ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ, ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ
ΠΛΗΡΟΦΟΡΙΚΗΣ

«Ασφαλείς, διαλειτουργικές και ανοιχτές αρχιτεκτονικές υπηρεσιών – Ασφαλείς επιχειρησιακές υπηρεσίες η-συναλλαγών»

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Αλέξανδρος Ι.Σ. Καλιοντζόγλου

Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών ΕΜΠ

ΑΘΗΝΑ, Σεπτέμβριος 2006

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ, ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ
ΠΛΗΡΟΦΟΡΙΚΗΣ

«Ασφαλείς, διαλειτουργικές και ανοιχτές αρχιτεκτονικές υπηρεσιών – Ασφαλείς επιχειρησιακές υπηρεσίες η-συναλλαγών»

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Αλέξανδρος Ι.Σ. Καλιοντζόγλου

Συμβουλευτική Επιτροπή : Ηλίας Κουκούτσης
Μιλτιάδης Αναγνώστου
Μιχάλης Θεολόγου

Εγκρίθηκε από την επταμελή εξεταστική επιτροπή την 20η Σεπτεμβρίου 2006.

.....	.....	.....
Ηλίας Κουκούτσης Επίκουρος Καθηγητής ΕΜΠ	Μιλτιάδης Αναγνώστου Καθηγητής ΕΜΠ	Μιχάλης Θεολόγου Καθηγητής ΕΜΠ
.....	.....	.....
Γεώργιος Στασινόπουλος Καθηγητής ΕΜΠ	Βασίλειος Μάγκλαρης Καθηγητής ΕΜΠ	Σωκράτης Κάτσικας Καθηγητής Πανεπιστημίου Αιγαίου
	.....	
	Δέσποινα Πολέμη Λέκτορας Πανεπιστημίου Πειραιά	

Αθήνα, Σεπτέμβριος 2006

Αφιερώνεται στη μάνα μου

.....
Αλέξανδρος Ι.Σ. Καλιοντζόγλου

Διδάκτωρ Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Ευχαριστίες

Αρχικά θα ήθελα να εκφράσω ένα μεγάλο ευχαριστώ στον επιβλέποντα καθηγητή μου κ. Ηλία Κουκούτση για την καθοδήγηση, το ενδιαφέρον και τον χρόνο του. Επίσης ευχαριστώ τους καθηγητές κ. Μιλτιάδη Αναγνώστου και Μιχάλη Θεολόγου για τις πολύτιμες συμβουλές τους καθ' όλη την διάρκεια της διατριβής. Οι παρατηρήσεις και τα σχόλια όλης της τριμελούς επιτροπής καθόρισαν σε πολύ μεγάλο βαθμό την αρτιότητα της διατριβής και με βοήθησαν να την βελτιώνω συνέχεια μέχρι την τελική μορφή της.

Για την Δρ. Δέσποινα Πολέμη, Λέκτορα Πανεπιστημίου Πειραιά, με σιγουριά μπορώ να πω είναι ότι αν δεν ήταν εκείνη, δεν θα είχε ξεκινήσει ποτέ η ακαδημαϊκή μου πορεία και κατ' επέκταση η ίδια η διατριβή. Την ευχαριστώ εγκάρδια για την τεράστια υπομονή και την επιμονή της και την υποστήριξή της ακόμα και όταν εγώ σκεφτόμουν να καταθέσω τα όπλα.

Τα έξι αυτά χρόνια που υπήρξα υποψήφιος διδάκτορας, με υποστήριξαν αρκετοί φίλοι και συνάδελφοι. Ο Παναγιώτης Σκλάβος και η Αθηνά Μπούρκα (και οι δύο διδάκτορες ΕΜΠ πια) ήταν απο εκείνους τους ανθρώπους που βρίσκονταν απο την αρχή στο πλευρό μου τόσο για να μου δώσουν συμβουλές για την διατριβή αλλά κυρίως ως φίλοι για να με βοηθήσουν με όποιο τρόπο μπορούσαν. Τους ευχαριστώ ολόψυχα και θέλω να τους εκφράσω πόσο τυχερός νιώθω που τους έχω γνωρίσει.

Σημαντικοί για μένα άνθρωποι με τους οποίους μπορούσα να μοιραστώ τις ανησυχίες, τις σκέψεις και τους προβληματισμούς μου και που θα ήθελα επίσης να ευχαριστήσω για την συμπαράσταση τους είναι ο Στέλιος Πανταζόπουλος, ο Jarkko Juntunen, ο Δημήτρης Φαρμάκης, η Τατιάνα Πεττεμερίδου, ο Λάμπρος Στραβελάκης και η Λίλα Δημοπούλου, όλοι πολύ καλοί φίλοι που αγαπώ πολύ.

Επίσης θέλω να ευχαριστήσω τους νέους φίλους και συνεργάτες Βασίλη Μενεκλή και Αλέξανδρο Σφάγγο για τις ιδέες και το ενδιαφέρον τους. Ελπίζω η φιλία μας να συνεχίσει και να βάλω και γω ένα λιθαράκι στην ολοκλήρωση των μεταπτυχιακών σπουδών τους.

Τέλος, ευχαριστώ την οικογένειά μου. Έχει παίξει ίσως τον σημαντικότερο ρόλο στο να μάθω να θέτω και να πραγματοποιώ στόχους στη ζωή μου και να προσπαθώ να βελτιώνομαι όσο μπορώ. Ελπίζω να τους έχω κάνει περήφανους.

Αλέξανδρος Καλιοντζόγλου
Αθήνα, Σεπτέμβριος 2006

Περιεχόμενα

1 Εισαγωγή

Τα τελευταία χρόνια παρατηρείται στην επιστημονική κοινότητα μια συνεχής προσπάθεια βελτίωσης του τρόπου επικοινωνίας υπολογιστικών συστημάτων με χρήση του Διαδικτύου. Στα πλαίσια αυτής της προσπάθειας, αναζητούνται μέθοδοι και πρωτόκολλα τα οποία θα καταστήσουν ευκολότερη την εδραίωση της επικοινωνίας και την μεταφορά δομημένων δεδομένων ανάμεσα σε κόμβους κατανεμημένων και ετερογενών πληροφοριακών συστημάτων, χωρίς όμως αυτό να οδηγεί σε απαγορευτική αύξηση του κόστους, τόσο σε πόρους όσο και σε υπολογιστικό φορτίο.
Μια βασική παράμετρος, η αμέλεια της οποίας αποτελούσε ανέκαθεν τροχοπέδη στην άμεση και γρήγορη εφαρμογή νέων τεχνολογιών που θα μπορούσαν να συντελέσουν την επίτευξη του παραπάνω στόχου, είναι η κατάλληλη ***ενσωμάτωση μηχανισμών και η χρήση υπηρεσιών ασφάλειας*** [Nash01, Adams99, Hartman03]. Η ανταλλαγή δεδομένων προσωπικού χαρακτήρα και οικονομικής φύσης, η οποία αποτελεί μέρος των επιχειρηματικών πρακτικών των προαναφερθέντων οργανισμών, απαιτεί ένα υψηλό επίπεδο ασφάλειας το οποίο θα εγγυάται ανάλογα με την περίπτωση τον έλεγχο ταυτότητας των εμπλεκόμενων οντοτήτων, την ορθή εξουσιοδότηση και απονομή δικαιωμάτων και το απόρρητο δεδομένων, λαμβάνοντας υπόψην και τις νομικές απαιτήσεις που διέπουν κάθε δραστηριότητα. Οι πρώιμες υλοποιήσεις πληροφοριακών συστημάτων, αγνοούσαν στο στάδιο του σχεδιασμού την ενσωμάτωση μηχανισμών ασφάλειας, καθιστώντας κατά τον τρόπο αυτό την μετέπειτα προσθήκη των ανωτέρω μηχανισμών μια επίπονη διαδικασία, που συνήθως δεν ήταν απόλυτα επιτυχής ή μέσα σε ικανοποιητικά επίπεδα απόδοσης. Γι' αυτό το λόγο, τα τελευταία χρόνια, έχει δοθεί μεγαλύτερη έμφαση στον τομέα της ασφάλειας, με σημαντικά ερευνητικά επιτεύγματα, τα οποία στοχεύουν, απο τη μια στη διευκόλυνση της υλοποίησης όσο το δυνατόν υψηλότερου επιπέδου υπηρεσιών ασφάλειας διατηρώντας σε χαμηλά επίπεδα το υπολογιστικό κόστος και αυξημένη την επίδοση, και απο την άλλη στην ενσωμάτωση όλων των παραμέτρων διαλειτουργικότητας και επεκτασιμότητας των συστημάτων.
Στην πράξη, η ασφαλής ανταλλαγή δεδομένων πρέπει να επιτυγχάνεται αποδοτικά ανάμεσα σε ένα ολοένα αυξανόμενο πλήθος φορέων με διαφοροποιούμενα πληροφοριακά συστήματα που αποτελούν κόμβους του διαδικτύου. Εκεί εμφανίζεται η ανάγκη για ένα υψηλό επίπεδο ***διαλειτουργικότητας***, ανάμεσα σε συστήματα, υπηρεσίες και εφαρμογές. Η επίτευξη της διαλειτουργικότητας είναι ένας απο τους σημαντικούς στόχους των σχεδιαστών συστημάτων τα τελευταία χρόνια, επειδή διευρύνονται τα σύνορα διαχειριστικών τομέων, κυρίως λόγω της επέκτασης του διαδικτύου και της ανάγκης για την διεκπεραίωση πολύπλοκων ηλεκτρονικών συναλλαγών ανάμεσα σε διαφορετικούς επιχειρηματικούς φορείς. Στην επιστημονική κοινότητα διερευνώνται οι τρόποι με τους οποίους ανομοιογενή συστήματα μπορούν να βρουν κοινούς κώδικες επικοινωνίας και μηνυμάτων, χωρίς να παίζουν ρόλο οι υποκείμενες πλατφόρμες ή γλώσσες προγραμματισμού υλοποίησης. Η διαλειτουργικότητα ως στόχος εισάγει ένα σύνολο προκλήσεων και δυσκολιών που έχουν να κάνουν τόσο με την πολυπλοκότητα των προσφερόμενων νέων ή υπαρχουσών υπηρεσιών όσο και με την προτυποποίηση, που φυσικά είναι το πρώτο βήμα για διαλειτουργικότητα.
Η βιβλιογραφία και ο επιχειρηματικός κόσμος έχουν να επιδείξουν μέχρι στιγμής ένα σύνολο ***προτύπων και πλαισίων αναφοράς*** που βοηθούν στην δημιουργία ασφαλών και

διαλειτουργικών συστημάτων, τόσο σε επίπεδο προδιαγραφής συγκεκριμένων υπηρεσιών, μηχανισμών ή πρωτοκόλλων, όσο και σε ένα συνολικότερο επίπεδο σχεδιασμού ολόκληρων αρχιτεκτονικών. Τα βήματα στον τομέα των νέων τεχνολογιών είναι ταχύτατα, οπότε οι σχεδιαστικές μέθοδοι που εφαρμόζονται πρέπει να είναι εύκολα προσαρμόσιμες και να λαμβάνουν υπόψην τα νέα επιτεύγματα.
Δυστυχώς, ένα μεγάλο μέρος των υπαρχόντων προτύπων αποτυγχάνουν στο να εξασφαλίσουν ικανοποιητικά επίπεδα διαλειτουργικότητας και ασφάλειας, καθώς και μιας τρίτης παραμέτρου, της ολοκληρωμένης ***προσέγγισης των επιχειρησιακών στόχων*** των οργανισμών που υιοθετούν τις αντίστοιχες υλοποιήσεις. Η ορθή αποτύπωση της επιχειρησιακής όψης ενός πληροφοριακού συστήματος αποτελεί έναν απο τους σημαντικότερους παράγοντες για την επιτυχή αφομοίωση των ηλεκτρονικών διαδικασιών του συστήματος απο τους χρήστες του. Οι επιμέρους στόχοι, που συνήθως δεν προσεγγίζονται ολοκληρωμένα απο υπάρχουσες μεθόδους σχεδιασμού, περιλαμβάνουν την ξεκάθαρη αποτύπωση των διαδικασιών, των κοινοτήτων χρηστών και των ρόλων τους, των πολιτικών και περιορισμών που διέπουν τις διαδικασίες και τους ρόλους, καθώς και των συγκεκριμένων αντικείμενων πληροφορίας που διακινούνται μέσα στις διαδικασίες.
Ο απώτερος σκοπός της βελτίωσης του τρόπου επικοινωνίας υπολογιστικών συστημάτων και παροχής η-υπηρεσιών είναι η αυτοματοποίηση, ενοποίηση και διαλειτουργικότητα αρχιτεκτονικών που υλοποιούν τις επιχειρηματικές δραστηριότητες διαφόρων κατηγοριών φορέων με τεχνολογική υποδομή, δηλαδή των δημόσιων και ιδιωτικών οργανισμών που δραστηριοποιούνται σε τομείς όπως η εκπαίδευση, το εμπόριο, η ιατρική φροντίδα, η δημόσια διοίκηση κ.α., λαμβάνοντας υπόψην τα αντίστοιχα πρότυπα του χώρου.
Με δεδομένη την ύπαρξη του διαδικτύου και των βασικών επικοινωνιακών πρωτοκόλλων που το διέπουν, η έρευνα οδήγησε σε τεχνολογίες που κατάφεραν να επιτύχουν ένα μέρος των προσδοκιών για διαλειτουργικότητα. Τέτοιες τεχνολογίες είναι η CORBA (Common Object Request Broker Architecture) [CORBA] του οργανισμού OMG (Object Management Group) και το DCOM (Distributed Component Object Model) [DCOM] της εταιρίας Microsoft. Οι τεχνολογίες αυτές όμως, αν και έχουν υιοθετηθεί σε κατανεμημένες αρχιτεκτονικές, μειονεκτούν στο ότι κάθε λύση που βασίζεται στα πρωτόκολλα που προδιαγράφουν θα πρέπει να εξαρτάται απο την υλοποίηση μιας συγκεκριμένης εταιρείας. Για παράδειγμα, αν κάποιος θέλει να χρησιμοποιήσει το DCOM, όλοι οι συμμετέχοντες κόμβοι στο κατανεμημένο περιβάλλον θα πρέπει να υποστηρίζουν ένα απο τα λειτουργικά συστήματα της Microsoft. Στην περίπτωση της CORBA, όλοι οι κόμβοι θα πρέπει να λειτουργούν το ίδιο προϊόν, το λεγόμενο ORB (Object Request Broker) [ORB]. Υπάρχουν βέβαια περιπτώσεις όπου ORB διαφορετικών εταιριών είναι διαλειτουργικά [Hugues02, Aleksy99], αλλά η διαλειτουργικότητα δεν επεκτείνεται και σε υψηλότερου επιπέδου υπηρεσίες, όπως η ασφάλεια και η διαχείριση συναλλαγών. Το DCOM και η CORBA θεωρούνται σήμερα ώριμες και λογικές λύσεις για επικοινωνία μεταξύ εξυπηρετητών σε ένα κλειστό περιβάλλον. Παρά ταύτα, η ανάγκη για ένα επιτυχημένο μοντέλο κατανεμημένων εφαρμογών, το οποίο να μπορεί να διασυνδέσει εφαρμογές πάνω απο το διαδίκτυο, παραμένει και απαιτεί λύσεις που να είναι ανεξάρτητες απο εταιρίες, πλατφόρμες και γλώσσες προγραμματισμού.

Ένα σημαντικό βήμα προόδου προς αυτό το σκοπό, ήταν η δημιουργία της XML (Extensible Markup Language) [XML]. Η XML συνδυάζει έναν ικανό αριθμό χαρακτηριστικών που την καθιστούν την πλέον κατάλληλη γλώσσα ανταλλαγής δεδομένων ανάμεσα σε πληροφοριακά συστήματα. Μέχρι πρόσφατα, αυτό που έλειπε ήταν ο συστηματικός και προτυποποιημένος τρόπος για την ανταλλαγή μηνυμάτων βασισμένων στην XML πάνω απο τα γνωστά και ευρύτατα χρησιμοποιούμενα πρωτόκολλα του διαδικτύου, όπως για παράδειγμα το HTTP [HTTP]. Το κενό αυτό ήρθαν να καλύψουν οι Υπηρεσίες Ιστού (Web Services).

Με τον όρο Υπηρεσίες Ιστού, στη βιβλιογραφία ορίζονται δύο έννοιες, μια συγκεκριμένη και μια ιδεατή [Kreger01, WSA]. Ως συγκεκριμένη έννοια, οι Υπηρεσίες Ιστού είναι ένα σύνολο ανερχόμενων προτύπων που περιγράφουν τα χαρακτηριστικά εφαρμογών για παροχή υπηρεσιών, βασιζόμενο σε διακριτά δομικά στοιχεία (component – based). Ως ιδεατή έννοια, οι Υπηρεσίες Ιστού αναπαριστούν ένα μοντέλο στο οποίο διακριτές λειτουργίες μέσα σε διαδικασίες ηλεκτρονικού επιχειρείν, κατανέμονται σε ένα δίκτυο συστημάτων.

Πέρα των προδιαγραφών που περιγράφουν την οργάνωση και επικοινωνία των Υπηρεσιών Ιστού, και κατ' επέκταση των αρχιτεκτονικών που βασίζονται σε αυτές, οι διεθνείς οργανισμοί προτυποποίησης και η ερευνητική κοινότητα, επικεντρώνουν την προσοχή τους στους μηχανισμούς εκείνους που θα προσδώσουν στις Υπηρεσίες Ιστού την απαραίτητη ασφάλεια, και κατά συνέπεια την ώθηση που χρειάζονται για να υιοθετηθούν ως μέρος κρίσιμων υποδομών πληροφοριακών συστημάτων. Προς αυτή την κατεύθυνση είναι σημαντική η προσπάθεια που επιτελείται προκειμένου οι Υπηρεσίες Ιστού να λειτουργούν σε συνδυασμό με τις Υποδομές Δημοσίου Κλειδιού [Adams99], στις οποίες ένα μεγάλο μέρος του επιχειρηματικού και κυβερνητικού κόσμου έχει επενδύσει παγκοσμίως. Ο συνδυασμός αυτός στοχεύει στην παροχή προδιαγραφών για σημαντικές υπηρεσίες ασφάλειας, όπως αυτές που επιτελούν έλεγχο πρόσβασης, διαχείρισης ταυτότητας, διαχείριση κλειδιών και πιστοποιητικών κ.α. Οι Υποδομές Δημοσίου Κλειδιού (ΥΔΚ) απο τη σύλληψη τους θεωρήθηκαν μια λύση ικανή να ενσωματώσει μηχανισμούς ασφάλειας σε πληροφοριακά συστήματα. Σήμερα όμως, αρκετά χρόνια μετά, είναι φανερό ότι υπάρχουν εγγενείς δυσκολίες στην ενσωμάτωση αυτή που έχουν να κάνουν με την οργανωτική πολυπλοκότητα των ΥΔΚ, το κόστος λειτουργίας τους, το χαμηλό επίπεδο ενσωμάτωσής τους σε επιχειρησιακές εφαρμογές, την έλλειψη εφαρμογών ικανών να τις στηρίξουν, το μικρό επίπεδο διαλειτουργικότητας και την έλλειψη εμπειρίας και τριβής των χρηστών με την συγκεκριμένη τεχνολογία, αλλά και τις τεχνολογίες ασφάλειας γενικότερα. Η κατάλληλη εφαρμογή της XML και των Υπηρεσιών Ιστού στις υπηρεσίες ΥΔΚ, θεωρείται πλέον ένας ικανός τρόπος για την αναίρεση των παραπάνω δυσκολιών.

Προχωρώντας το μοντέλο των Υπηρεσιών Ιστού ένα βήμα παραπέρα και δεσμεύοντάς το οργανωτικά στις επιχειρησιακές ανάγκες που ήρθαν να καλύψουν, η ερευνητική κοινότητα και η βιομηχανία έκαναν εισαγωγή της έννοιας της Αρχιτεκτονικής Προσανατολισμένης στις Υπηρεσίες - ΑΠΥ (Service Oriented Architecture) [High05]. Μια τέτοια αρχιτεκτονική αποτελεί μια ολιστική προσέγγιση για τον σχεδιασμό και την κατασκευή εφαρμογών που χρησιμοποιούν υπηρεσίες προσβάσιμες απο ένα δίκτυο, όπως για παράδειγμα το διαδίκτυο. Η Αρχιτεκτονική Προσανατολισμένη στις Υπηρεσίες προάγει το «χαλαρό» δέσιμο μεταξύ δομικών στοιχείων λογισμικού έτσι ώστε να είναι δυνατή η επαναχρησιμοποίησή τους και τα δομικά στοιχεία να βασίζονται σε καλώς

ορισμένες, δημοσιευμένες και προτυποποιημένες διεπαφές. Ο ορισμός αυτός στην ουσία «φωτογραφίζει» τις ιδιότητες των Υπηρεσιών Ιστού, οι οποίες θεωρούνται το καταλληλότερο δομικό στοιχείο για μια τέτοια αρχιτεκτονική, αν και μια Αρχιτεκτονική Προσανατολισμένη σε Υπηρεσίες μπορεί να χτιστεί και με άλλες τεχνολογίες [High04].
Οι διαδικασίες σχεδιασμού, υλοποίησης και διασύνδεσης Αρχιτεκτονικών Προσανατολισμένων στις Υπηρεσίες αποτελούν ένα νέο ερευνητικό πεδίο το οποίο εισάγει σημαντικές ανάγκες, καθώς:

- Δημιουργείται το ερώτημα, «πώς μπορεί κάποιος να επιτύχει τα απαραίτητα επίπεδα διαλειτουργικότητας και ασφάλειας σε νεοδημιουργηθείσες αρχιτεκτονικές υπηρεσιών ή σε ήδη υπάρχουσες οι οποίες επεκτείνονται με νέες επιχειρησιακές υπηρεσίες; Ποιες είναι οι παράμετροι που πρέπει να ληφθούν υπόψην ώστε μια Αρχιτεκτονική Προσανατολισμένη σε Υπηρεσίες να χαρακτηρίζεται ως ασφαλής, διαλειτουργική και ανοιχτή;»
- Εμφανίζεται η ανάγκη για δημιουργία συστηματικών κατασκευαστικών μεθόδων σχεδιασμού τέτοιων αρχιτεκτονικών που να λαμβάνουν υπόψην τα ιδιαίτερα χαρακτηριστικά τους, να επιτρέπουν τον σφαιρικό σχεδιασμό απο πολλές όψεις (π.χ. επιχειρησιακή, τεχνολογική) και να είναι συμβατές με διαδεδομένα πρότυπα του χώρου [Tang04]. Υπάρχοντα πλαίσια μπορούν να χρησιμοποιούν και στην περίπτωση της νέας γενιάς αρχιτεκτονικών υπηρεσιών, αλλά συνήθως είναι πολύ γενικά χωρίς να διατυπώνουν ακριβείς διαδικασίες (και άρα χρειάζεται πολύ περισσότερος χρόνος για να εφαρμοστούν), δεν δίνουν ιδιαίτερη σημασία στο πολύ σημαντικό θέμα της ασφάλειας ή την θεωρούν ως μεμονωμένη τεχνική λύση, απαιτούν συχνά την δημιουργία της αρχιτεκτονικής απο το μηδέν (και άρα δεν επιτρέπουν την αναβάθμιση ή την ενσωμάτωση υπαρχουσών υποδομών) και δεν παρέχουν συγκεκριμένα επαναχρησιμοποιήσιμα στοιχεία για εισαγωγή σε ένα πλήθος αρχιτεκτονικών με κοινά χαρακτηριστικά.
- Τέλος δημιουργείται το ερώτημα, «ποια είναι τέτοια κατάλληλα πρότυπα και μοντέλα αναφοράς που μπορούν να ληφθούν υπόψην για συμμόρφωση στις παραπάνω κατασκευαστικές μεθόδους, προκειμένου το αποτέλεσμα να είναι όντως μια ασφαλής, διαλειτουργική και ανοιχτή αρχιτεκτονική; Πως αυτά μπορούν να δώσουν συνολική επισκόπηση του αποτελέσματος; Πώς συντελούν στον σχεδιασμό διαφόρων ειδών υπηρεσιών (που είναι η καρδιά τέτοιου τύπου αρχιτεκτονικών) τόσο σε αρχιτεκτονικές που δημιουργούνται από την αρχή, όσο και σε ήδη υπάρχουσες που πρέπει να επεκταθούν με νέες επιχειρησιακές υπηρεσίες;»

Βάσει της παραπάνω υπάρχουσας κατάστασης και αναγκών, το **αντικείμενο μελέτης** της παρούσας διατριβής χωρίζεται σε τρία πεδία στα οποία υπάρχουν συγκεκριμένα προβλήματα και ελλείψεις:

- Το πρώτο πεδίο επικεντρώνεται στο πώς επιτυγχάνεται η ενσωμάτωση υπηρεσιών Υποδομών Δημοσίου Κλειδιού σε εφαρμογές η-επιχειρείν σε συνδυασμό με τεχνολογίες βασισμένες XML και σε Υπηρεσίες Ιστού, για μεγιστοποίηση της διαλειτουργικότητας.
- Το δεύτερο πεδίο μελέτης, εστιάζεται στους τρόπους συστηματικού σχεδιασμού Αρχιτεκτονικών Προσανατολισμένων σε Υπηρεσίες. Κατά την πορεία της διατριβής,

διαπιστώθηκε μια αδυναμία ολιστικής προσέγγισης του τρόπου με τον οποίο τεχνολογίες όπως οι προαναφερθείσες μπορούν να χρησιμοποιηθούν προκειμένου να χτιστούν αρχιτεκτονικές που καλύπτουν τις πραγματικές επιχειρηματικές ανάγκες των οργανισμών που τις υιοθετούν.

- Το τρίτο πεδίο επικέντρωσε σε ένα απο τα ισχύοντα πρότυπα / μοντέλα αναφοράς προδιαγραφών κατανεμημένων αρχιτεκτονικών, και πιο συγκεκριμένα το πρότυπο ISO-Reference Model for Object Distributed Processing (ISO/RM-ODP). Ειδικότερα εξετάστηκε ο τρόπος με τον οποίο το πρότυπο μπορεί να χρησιμοποιηθεί κατά τον σχεδιασμό μιας αρχιτεκτονικής υπηρεσιών, αλλά και στην μελέτη συγκεκριμένων υλοποιήσεων ανοιχτών αρχιτεκτονικών υπηρεσιών που βασίζονται στις ΥΔΚ, XML και Υπηρεσίες Ιστού, ως προς τη διαλειτουργικότητα και την ασφάλεια [Kaliontzoglou06b]. Το RM-ODP αναδεικνύεται ως ένα ιδιαίτερα χρήσιμο μοντέλο αναφοράς σε σχέση με άλλα πρότυπα του χώρου για πολλούς λόγους: είναι αρκετά γενικό αλλά ευέλικτο ως προς τις έννοιες που παρέχει για την αναπαράσταση ενός κατανεμημένου συστήματος, επιτρέπει την επισκόπηση και τον σχεδιασμό κατανεμημένων συστημάτων απο **διαφορετικές όψεις** (επιχειρησιακή, τεχνολογική και υπολογιστική καθώς και όψη πληροφορίας και μηχανικού), επιτρέπει τον έλεγχο συνέπειας ανάμεσα στις όψεις και στις προδιαγραφές, δεν επιβάλλει συγκεκριμένη σημειογραφία και είναι ευρέως διαδεδομένο με ένα σύνολο εφαρμογών του στην βιβλιογραφία.

Στο χώρο των παραπάνω ερευνητικών πεδίων, τα **αποτελέσματα και η συνεισφορά της διατριβής** συνοψίζονται ως εξής:

Α) Αρχικά μελετήθηκαν μεμονωμένες υπηρεσίες ασφάλειας και αναγνωρίστηκαν προβλήματα που παρουσιάζουν δύο απο αυτές κατά την ενσωμάτωσή τους σε υπηρεσίες η-επιχειρείν:

- Η υπηρεσία χρονοσφράγισης παρουσιάζει την αδυναμία υποστήριξης πρωτοκόλλων συμφωνίας συναλλαγών στα οποία εμπλέκονται άνω των δύο οντοτήτων.
- Η υπηρεσία ηλεκτρονικού ταχυδρομείου βάσει του πρωτοκόλλου S/MIME δεν υποστηρίζει την αυτόνομη υπογραφή συνημμένων εγγράφων και επίσης παρουσιάζει το πρόβλημα της "κρυφής προώθησης" το οποίο επιτρέπει σε κακόβουλους χρήστες να οδηγήσουν τον παραλήπτη ενός μηνύματος να πιστέψει ότι το έχει λάβει απο κάποιον άλλον ή να τον πείσει ότι για ένα μήνυμα αυτός ήταν όντως ο παραλήπτης ενώ ο αποστολέας του το προόριζε για κάποιον άλλο.

Η διατριβή προτείνει λύσεις στα παραπάνω προβλήματα με τον ορισμό ενός νέου μοντέλου συμφωνίας συναλλαγών που κάνει χρήση του πρωτοκόλλου χρονοσφράγισης, καθώς και την ενσωμάτωση συγκεκριμένων υποδομών XML στο πρωτόκολλο MIME με χρήση πολλαπλών υπογραφών και κρυπτογράφησης. Στη συνέχεια οι λύσεις εφαρμόστηκαν σε μεμονωμένες υπηρεσίες ηλεκτρονικού επιχειρείν.

Β) Υπο το πρίσμα των Αρχιτεκτονικών Προσανατολισμένων σε Υπηρεσίες (ΑΠΥ), τα συμπεράσματα απο την εφαρμογή των παραπάνω λύσεων ήταν τα ακόλουθα:

- Υπάρχει αδυναμία ολιστικής προσέγγισης του τρόπου με τον οποίο τεχνολογίες όπως η XML, οι Υπηρεσίες Ιστού και οι ΥΔΚ μπορούν να χρησιμοποιηθούν προκειμένου να χτιστούν αρχιτεκτονικές που καλύπτουν τις πραγματικές επιχειρηματικές ανάγκες των οργανισμών που τις υιοθετούν.
- Τα υπάρχοντα πλαίσια σχεδιασμού ΑΠΥ είναι πολύ γενικά και δεν αποτελούν τυπικές μεθόδους σχεδιασμού με διακριτά βήματα που να λαμβάνουν υπόψην τις ιδιαίτερες απαιτήσεις των ΑΠΥ, που έχουν να κάνουν με τις υπηρεσίες και την κατανομή τους και τις επιχειρησιακές ανάγκες των εμπλεκόμενων φορέων.
- Τα υπάρχοντα πλαίσια δεν εξασφαλίζουν ότι οι παρεχόμενες υπηρεσίες ασφάλειας είναι διαθέσιμες σε όλες τις υπόλοιπες υπηρεσίες της αρχιτεκτονικές που τις χρειάζονται.

Η διατριβή λύνει τα παραπάνω προβλήματα αρχικά εισάγοντας μια επέκταση του ορισμού των ΑΠΥ, ώστε να οριστεί η αναβαθμισμένη έννοια των **Ασφαλών, Διαλειτουργικών και Ανοιχτών Αρχιτεκτονικών Υπηρεσιών (ΑΔΑΑΥ)** και τα χαρακτηριστικά και οι απαιτήσεις που τις διέπουν.
Στη συνέχεια η διατριβή προδιαγράφει μια **πρωτότυπη συστηματική και δομημένη κατασκευαστική μέθοδο σχεδιασμού ασφαλών, διαλειτουργικών, ανοιχτών κατανεμημένων αρχιτεκτονικών προσανατολισμένων σε υπηρεσίες**. Οι σχεδιαζόμενες με την μέθοδο ΑΔΑΑΥ επιτυγχάνουν τα ακόλουθα χαρακτηριστικά:

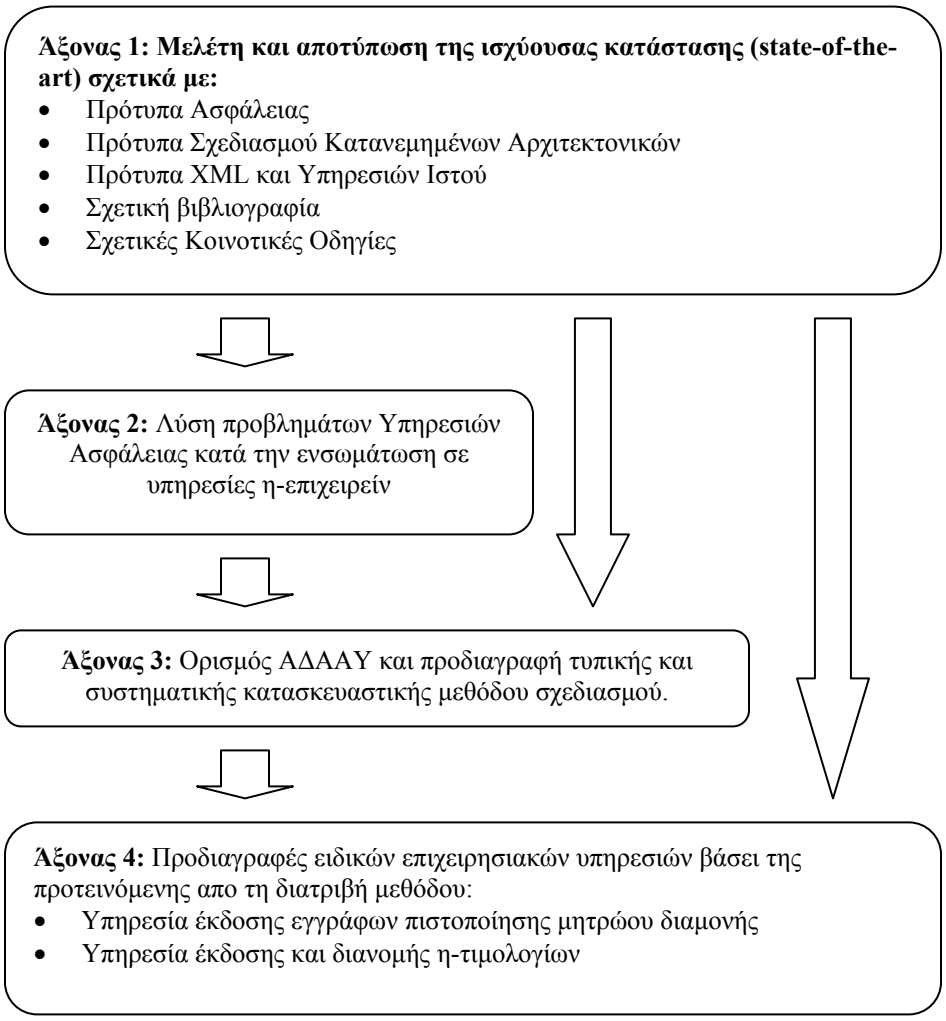
- Αποτελούνται απο υπηρεσίες / δομικές μονάδες που είναι επαναχρησιμοποιήσιμες εντός της ίδιας αρχιτεκτονικής αλλά και σε άλλες αρχιτεκτονικές.
- Οι υπηρεσίες συντονίζονται μέσα στην αρχιτεκτονική με έναν εύκολα διαχειρίσιμο τρόπο προκειμένου να προσομοιώσουν την επιχειρηματική λογική που η αρχιτεκτονική θέλει να προσεγγίσει.
- Η ασφάλεια υλοποιείται ως ο βέλτιστος συνδυασμός υπηρεσιών και μηχανισμών ασφάλειας οι οποίες είναι διαθέσιμες σε όλες τις υπηρεσίες της αρχιτεκτονικής που τις χρειάζονται μέσω κατάλληλων διεπαφών.

Η προτεινόμενη απο τη διατριβή μέθοδος συμμορφώνεται με το σύνολο των εννοιών του προτυποποιημένου μοντέλου αναφοράς ISO/Reference Model for Open Distributed Processing (RM-ODP) [RM-ODP]. Σε αντίθεση, όμως, με το πολύ γενικευμένο πλαίσιο του προτύπου, η μέθοδος χωρίζεται σε **στάδια τα οποία παρέχουν τα ακριβή βήματα** που πρέπει να ακολουθηθούν κατά τον σχεδιασμό, την απαραίτητη **σημειογραφία βάσει της UML** η οποία αναπαριστά ικανοποιητικά τις έννοιες του προτύπου, καθώς και συγκεκριμένα και επεκτάσιμα **επαναχρησιμοποιήσιμα δομικά στοιχεία** που μπορούν να ενσωματωθούν σε σχεδιαζόμενες αρχιτεκτονικές σε ένα ευρύ φάσμα επιχειρησιακών τομέων. Επιπρόσθετα η μέθοδος δίνει την δυνατότητα για σχεδιασμό τόσο ολοκληρωμένων αρχιτεκτονικών, όσο και υπηρεσιών που πρόκειται να εισαχθούν σε ήδη υπάρχουσες αρχιτεκτονικές, εφόσον αυτές έχουν καλώς ορισμένες διεπαφές στις υπηρεσίες τους.

Γ) Τέλος, με χρήση της παραπάνω κατασκευαστικής μεθόδου, η διατριβή ορίζει το σύνολο των προδιαγραφών δυο πρωτότυπων ασφαλών διασυνοριακών υπηρεσιών η-επιχειρείν και η-διακυβέρνησης ως παραδείγματα επιχειρησιακών υπηρεσιών που

μπορούν να φιλοξενηθούν σε μια ΑΔΑΑΥ. Οι υπηρεσίες επιλέχθηκαν επειδή υπάρχουσες προσεγγίσεις στις υλοποιήσεις τους επιδεικνύουν αδυναμίες στην παρούσα βιβλιογραφία και στις εργασίες οργανισμών προτυποποίησης, καθώς και επειδή παρουσιάζουν σημαντικές απαιτήσεις ως προς την ασφάλεια και τη διαλειτουργικότητα λόγω του διασυνοριακού χαρακτήρα συναλλαγών που επιτρέπουν [Kaliontzoglou05, Kaliontzoglou06a, Kaliontzoglou06c]. Ειδικότερα πρόκειται για μια **υπηρεσία έκδοσης και διανομής ηλεκτρονικών τιμολογίων** και μια **υπηρεσία έκδοσης πιστοποιητικών μητρώου διαμονής για δήμους**, οι οποίες έχουν την δυνατότητα να λειτουργήσουν σε ένα πανευρωπαϊκό δίκτυο φορέων, λαμβάνοντας υπόψην το κοινοτικό πλαίσιο που διέπει τέτοιες διασυνοριακές συναλλαγές.

Τα παραπάνω αποτελέσματα της διατριβής οργανώνονται σε τέσσερις βασικούς άξονες, όπως φαίνεται στο ακόλουθο σχήμα:



Σχήμα 1-1:Άξονες Διατριβής

Συνοπτικά, οι άξονες της Διατριβής είναι οι ακόλουθοι:

- **Άξονας 1**: Περιλαμβάνει την μελέτη των προτύπων και εργασιών που υποστηρίζουν την διατριβή στους τομείς των ΥΔΚ, της ασφάλειας XML και Υπηρεσιών Ιστού, καθώς και των μεθοδολογικών πλαισίων προδιαγραφής κατανεμημένων αρχιτεκτονικών και ΑΠΥ. Μελετήθηκαν επίσης συγκεκριμένες υλοποιήσεις αρχιτεκτονικών και υπηρεσιών η-επιχειρείν. Στον άξονα αυτό εντοπίστηκαν αδυναμίες και προβλήματα σε βασικές υπηρεσίες ασφάλειας κατά την εφαρμογή τους σε υπηρεσίες η-επιχειρείν.
- **Άξονας 2:** Στον άξονα δίνονται λύσεις προβλημάτων υπηρεσιών ασφάλειας κατά την ενσωμάτωσή τους σε υπηρεσίες η-επιχειρείν (χρονοσφράγιση, ηλεκτρονικό ταχυδρομείο). Οι λύσεις ενσωματώθηκαν σε μεμονωμένες υπηρεσίες η-επιχειρείν. Τα συμπεράσματα που εξήχθησαν στον άξονα αυτό, συνετέλεσαν στην αναγνώριση της αδυναμίας ολιστικής προσέγγισης του τρόπου με τον οποίο μπορούν σχεδιαστούν ΑΠΥ που καλύπτουν τις επιχειρησιακές απαιτήσεις οργανισμών και ενσωματώνουν την ασφάλεια ως υπηρεσίες και μηχανισμούς διαθέσιμες σε όλες τις υπηρεσίες της αρχιτεκτονικής που τις χρειάζονται.
- **Άξονας 3:** Αποτελείται απο την αναλυτική περιγραφή της δομημένης κατασκευαστικής μεθόδου προδιαγραφής ασφαλών, διαλειτουργικών και ανοιχτών αρχιτεκτονικών υπηρεσιών, βασιζόμενο στα αποτελέσματα της μελέτης του Άξονα 1 και των ειδικών δραστηριοτήτων του Άξονα 2.
- **Άξονας 4:** Αποτελείται απο τις ολοκληρωμένες προδιαγραφές των δύο επιχειρησιακών υπηρεσιών: μια υπηρεσία έκδοσης ψηφιακών εγγράφων πιστοποίησης μητρώου διαμονής για δήμους και μια υπηρεσία έκδοσης και διανομής η-τιμολογίων. Οι υπηρεσίες αυτές αποτελούν εφαρμογή της προτεινόμενης μεθοδολογίας στην η-διακυβέρνηση και το η-επιχειρείν σε πραγματικές συνθήκες και βοήθησαν στον εντοπισμό συγκεκριμένων προβλημάτων και δυνατών βελτιώσεων της μεθοδολογίας.

Συνακόλουθα με τους παραπάνω άξονες, ο σκελετός του κειμένου της διατριβής διαρθρώνεται ως εξής:

- Το **1ο κεφάλαιο** αποτελεί την παρούσα εισαγωγή.
- Στο **2ο κεφάλαιο** αποτυπώνεται η υπάρχουσα κατάσταση στο αντικείμενο μελέτης της διατριβής, που μαζί με το παράρτημα αποτελούν τον 1ο Άξονα της διατριβής.
- Στο **3ο κεφάλαιο** περιγράφονται οι ειδικές ερευνητικές δραστηριότητες που οδήγησαν στις προδιαγραφές και υλοποιήσεις αναβαθμισμένων υπηρεσιών ασφάλειας και προηγμένων υπηρεσιών η-επιχειρείν. (2ος Άξονας διατριβής)
- Στο **4ο κεφάλαιο** εισάγεται η έννοια των ΑΔΑΑΥ και των απαιτήσεών τους και παρουσιάζονται οι αναλυτικές προδιαγραφές της νέας κατασκευαστικής μεθόδου. (3ος Άξονας διατριβής)
- Στο **5ο κεφάλαιο** παρουσιάζονται οι αναλυτικές προδιαγραφές των δύο επιλεγμένων επιχειρησιακών υπηρεσιών, βάσει εφαρμογής της κατασκευαστικής μεθόδου του προηγούμενου κεφαλαίου. (4ος Άξονας διατριβής)
- Το **6ο κεφάλαιο** ολοκληρώνει τη διατριβή διατυπώνοντας τα συνολικά συμπεράσματα και μελλοντικές ερευνητικές κατευθύνσεις.
- Το **7ο κεφάλαιο / Παράρτημα Ι** στο τέλος της διατριβής καλύπτει την υπάρχουσα κατάσταση σε τεχνολογίες και πρότυπα αιχμής όσο αφορά στην ασφάλεια και τις

Υπηρεσίες Ιστού που μελετήθηκαν κατά την εκπόνηση της διατριβής καθώς και μια περιγραφή των βασικών στοιχείων του προτύπου RM-ODP.

Κάθε κεφάλαιο ολοκληρώνεται με παραγράφους για συμπεράσματα και παράθεση βιβλιογραφικών αναφορών.

1.1 Αναφορές

[Adams99] C. Adams, S. Lloyd, Understanding Public-Key Infrastructure – Concepts, Standards and Deployment Considerations, 1st Edition, Macmillan Technical Publishing, 1999

[Aleksy99] Aleksy, M. Schader, M. Tapper, C. (1999). "Interoperability and interchangeability of middleware components ina three-tier CORBA-environment-state of the art". Enterprise Distributed Object Computing Conference, 1999. EDOC '99. Proceedings.

[CORBA] Object Modelling Group/Common Object Request Broker Architecture, http://www.omg.org

[DCE] Open Software Foundations / Distributed Computing Environment, http://www.osf.org

[DCOM] M. Horstmann, M. Kirtland. (1997). "DCOM Architecture". Microsoft technical article, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dndcom/html/msdn_dcomarch.asp

[Hartman03] B. Hartman et al. (2003). Mastering Web Services Security, Wiley Publishing.

[High05] R. High, S. Kinder, S. Graham. (2005). "IBM's SOA Foundation – An architectural Introduction and Overview". http://www-128.ibm.com/developerworks/webservices/library/ws-soa-whitepaper/

[HTTP] R. Fielding et al. (1999). "Hypertext Transfer Protocol -- HTTP/1.1". RFC 2616, http://www.ietf.org/rfc/rfc2616.txt

[Hugues02] J. Hugues et al. (2002). "A case study of Middleware to Middleware: MOM and ORB interoperability." In Addendum to the proceedings of the 4th International Symposium on Distributed Objects and Applications (DOA'02), pages 29-32, Irvine, CA, USA, October 2002. University of California at Irvine.

[Kaliontzoglou05] A. Kaliontzoglou et al. (2005). "A secure e-Government platform architecture for small to medium sized public organizations", Electronic Commerce Research & Applications, Elsevier, Volume 4, No. 2, pp. 174-186

[Kaliontzoglou06a] A. Kaliontzoglou, P. Boutsi, D. Polemi. (2006). "eInvoke: Secure e-Invoicing based on Web Services", Electronic Commerce Research Journal, Springer, (Accepted for publication)

[Kaliontzoglou06b] A. Kaliontzoglou et al. (2006). "A formalized design method for building e-government architectures", (To appear in) Secure e-Government Web Services, Idea Group Publishing, Hershey, PA

[Kaliontzoglou06c] A. Kaliontzoglou, T. Karantjias, D. Polemi. (2006). "Building innovative, secure and interoperable e-government services", (To appear in) Secure e-Government Web Services, Idea Group Publishing, Hershey, PA

[Nash01] Nash, A. et al. (2001). PKI: Implementing & Managing E-Security, McGraw-Hill Osborn Media Publishing.

[ORB] OMG. (2004). “Common object request broker architecture: core specification v.3.0.3”. http://www.omg.org/technology/documents/formal/corba_2.htm
[RM-ODP]1. ITU-T Rec. X.901 | ISO/IEC 10746-1,2,3, “Reference Model for Open Distributed Processing – Part 1: Overview, Part 2 Foundations, Part 3 Architecture”, 1996-98
[Tang04] A. Tang, J. Han, and P. Chen. (2004). "A Comparative Analysis of Architecture Frameworks," Swinburne University of Technology SUTIT-TR2004.01
[WSA] D. Booth et al. (Editors). (2004). “Web Services Architecture”. W3C Working Group Note 11 February 2004, http://www.w3.org/TR/2004/NOTE-ws-arch-20040211
[Kreger01] H. Kreger. (2001). “Web Services Conceptual Architecture – WSCA 1.0”. White paper, http://www-3.ibm.com/software/solutions/webservices/pdf/KREGER01.pdf
[XML] T. Bray et al. (Editors). (2004). “Extensible Markup Language (XML) 1.0 (Third Edition)”. W3C Recommendation 04 February 2004.

2 Αποτύπωση υπάρχουσας κατάστασης στον τομέα των ασφαλών, διαλειτουργικών και ανοιχτών αρχιτεκτονικών

Το βασικό πεδίο ενδιαφέροντος της διατριβής εστιάζεται στους τρόπους σχεδιασμού διαλειτουργικών και ασφαλών αρχιτεκτονικών προσανατολισμένων στις υπηρεσίες που καλύπτουν τις ανάγκες των οργανισμών που τις υιοθετούν και βασίζονται στις Υ.Δ.Κ, την XML και τις Υπηρεσίες Ιστού. Σημαντικός στόχος ήταν οι αρχές σχεδιασμού που θα προταθούν να μπορούν να είναι εφαρμόσιμες ανεξαρτήτως του τομέα επιχειρησιακής δραστηριότητας και να σέβονται την εγγενή κατανομή των κόμβων και στοιχείων μιας τέτοιας αρχιτεκτονικής σε διαφορετικές περιοχές διαχείρισης, κάτι που οδήγησε στην μελέτη του Μοντέλου Αναφοράς για Ανοιχτές Κατανεμημένες Διεργασίες (Reference Model for Open Distributed Processing – RM-ODP).
Ως εκ τούτου, κατά την αποτύπωση της υπάρχουσας κατάστασης εξετάστηκαν τα ακόλουθα:

- Πρότυπα κρυπτογραφίας και ΥΔΚ.
- Μηχανισμοί ασφάλειας με χρήση της XML.
- Πρότυπα και τεχνολογίες Υπηρεσιών Ιστού και τα σχετικά πρότυπα ασφάλειας.
- Το πρότυπο RM-ODP και συναφή πλαίσια αναφοράς.
- Χαρακτηριστικά πλαισίων, μοντέλων και αρχιτεκτονικών που συνδυάζουν τα πρότυπα αυτά ή κάποιο υποσύνολό τους.

Τα παραπάνω παρουσιάζονται αναλυτικά στο παράρτημα της διατριβής. Σε κάθε ένα αναφέρονται οι στόχοι, οι λειτουργίες, τα χαρακτηριστικά και ανοιχτά θέματα που τα αφορούν, τα οποία λήφθηκαν υπόψην κατά την περαίωση της διατριβής. Το παρόν κεφάλαιο επικεντρώνει αρχικά στις μεθοδολογίες και πρότυπα σχεδιασμού ανοιχτών και κατανεμημένων αρχιτεκτονικών, στα χαρακτηριστικά του RM-ODP που επιλέχθηκε ως κατάλληλο πλαίσιο αναφοράς για την διατριβή και στις αντίστοιχες προσεγγίσεις και αποτυπώνονται αδυναμίες. Στη συνέχεια περιγράφονται τα προβλήματα υπαρχουσών αρχιτεκτονικών υπηρεσιών και των αντίστοιχων υλοποιήσεων.

2.1 Μεθοδολογίες και πρότυπα σχεδιασμού ανοιχτών και κατανεμημένων αρχιτεκτονικών

2.1.1 Εισαγωγή

Το οικοδόμημα των αρχιτεκτονικών που είναι προσανατολισμένες στις υπηρεσίες (service oriented architectures) στηρίζεται κυρίως στα πρότυπα και τις τεχνολογίες των Υπηρεσιών Ιστού. Ταυτόχρονα όμως, προκειμένου να χτιστεί μια αρχιτεκτονική προσανατολισμένη σε υπηρεσίες, θα πρέπει να ακολουθηθεί μια προτυποποιημένη διαδικασία σχεδιασμού και υλοποίησης η οποία να μπορεί να αποτυπώνει επαρκώς τις επιχειρησιακές απαιτήσεις που καλείται να καλύψει. Οι διαδικασίες αυτές είναι πολύπλοκες καθώς πρέπει να ικανοποιούν ένα δεδομένο σύνολο κριτηρίων:

- Θα πρέπει να λαμβάνουν υπόψην τα χαρακτηριστικά κατανεμημένων συστημάτων σε ετερογενή περιβάλλοντα, σεβόμενες τις απαιτήσεις ασφάλειας και διαλειτουργικότητας.
- Θα πρέπει να είναι ιδιαίτερα ευέλικτες ως προς τις έννοιες που παρέχουν για την αναπαράσταση ενός κατανεμημένου συστήματος. Σημαντική παράμετρος είναι η δυνατότητα σχεδιασμού απο διαφορετικές όψεις (π.χ. επιχειρησιακή, τεχνολογική).
- Στην αρχική φάση του σχεδιασμού, θα πρέπει να είναι τεχνολογικά ουδέτερες ώστε να δίνουν στον σχεδιαστή ελευθερία κινήσεων ως προς τις τεχνολογίες που θα υιοθετήσει για την υλοποίηση του συστήματος. Λόγω του ότι οι αρχιτεκτονικές αυτού του τύπου στοχεύουν σε υλοποιήσεις με πρότυπα Υπηρεσιών Ιστού, θεωρείται πλεονέκτημα η διαδικασία σχεδιασμού να μπορεί να λάβει εύκολα υπόψην τα πρότυπα αυτά όταν θα φτάσει στο σημείο επιλογής συγκεκριμένων τεχνολογιών.
- Θα πρέπει να δίνουν την δυνατότητα τόσο του σχεδιασμού ενός ολοκληρωμένου πληροφοριακού συστήματος για την αρχιτεκτονική υπηρεσιών απο την αρχή, όσο και του σχεδιασμού επιμέρους υπηρεσιών που ενδέχεται να προστεθούν σε ήδη υπάρχοντα συστήματα.
- Θα πρέπει να συμμορφώνονται με τις έννοιες ευρέως διαδεδομένων προτύπων και πλαισίων αναφοράς τόσο στην επιστημονική βιβλιογραφία όσο και στην βιομηχανία της πληροφορικής. Για τα πρότυπα αυτά θα πρέπει να υπάρχουν επιτυχημένα δείγματα εφαρμογής τους.

Όπως φαίνεται στην [Tang04], υπάρχει ένας αριθμός απο αρχιτεκτονικά πλαίσια που μπορούν να χρησιμοποιηθούν στην μοντελοποίηση αρχιτεκτονικών και παρέχουν μια δομημένη και συστηματική προσέγγιση στον σχεδιασμό συστημάτων. Τέτοια πλαίσια είναι:

- το Πλαίσιο Zachman για Επιχειρησιακές Αρχιτεκτονικές (Zachman Framework for Enterprise Architecture) [Zackman87],
- το Μοντέλο 4+1 Όψεων Αρχιτεκτονικών (4+1 View Model of Architecture) [Kruchten95],
- το Μοντέλο Αναφοράς για Ανοιχτές Κατανεμημένες Διεργασίες του ISO (ISO/Reference Model for Open Distributed Processing – ISO/RM-ODP) [RM-ODP],

- το Αρχιτεκτονικό Πλαίσιο του Open Group (Open Group Architecture Framework) [OGAF] και
- το Αρχιτεκτονικό Πλαίσιο του Τμήματος εθνικής άμυνας των Η.Π.Α (DoD Architecture Framework from the US Department of Defense) [DoDAF].

Επίσης, όπως έχει παρουσιαστεί στην [Costa01], το προαναφερθέν πρότυπο RM-ODP του οργανισμού ISO, η αρχιτεκτονική Common Object Request Broker Architecture (CORBA) του οργανισμού Object Modeling Group (OMG) [CORBA] και το περιβάλλον Distributed Computing Environment (DCE) του οργανισμού Open Software Foundation (OSF) [DCE], είναι παραδείγματα διαδεδομένων προτύπων για ανοιχτές κατανεμημένες διεργασίες που αντιμετωπίζουν την ετερογένεια και την ανοιχτότητα κατανεμημένων συστημάτων.
Υπο το πρίσμα των απαιτήσεων για μια κατασκευαστική διαδικασία ή μέθοδο που θα διευκολύνει έναν σχεδιαστή να σχεδιάσει και υλοποιήσει μια ασφαλή, διαλειτουργική και ανοιχτή αρχιτεκτονική υπηρεσιών, τα παραπάνω πλαίσια θεωρούνται αρκετά γενικά και δεν καλύπτουν τις απαιτήσεις βάσει των προαναφερθέντων κριτηρίων. Δεν αποτελούν δηλαδή μια τυπική μεθοδολογία με διακριτά βήματα, την οποία μπορεί κάποιος να εφαρμόσει προκειμένου να λάβει ως αποτέλεσμα τις πλήρεις προδιαγραφές μιας αρχιτεκτονικής υπηρεσιών. Επιπρόσθετα, μια αρχιτεκτονική υπηρεσιών απαιτεί την ενσωμάτωση ιδιαίτερων χαρακτηριστικών που έχουν να κάνουν με τις υπηρεσίες και την κατανομή τους και τις επιχειρησιακές ανάγκες των εμπλεκόμενων φορέων.
Απο τα παραπάνω πλαίσια, αυτό που προσεγγίζει περισσότερο τις απαιτήσεις και άρα θεωρήθηκε ένα ικανό πλαίσιο αναφοράς για την ανάπτυξη μιας αναλυτικής κατασκευαστικής μεθόδου είναι το ISO Reference Model for Open Distributed Systems ή RM-ODP όπως θα αναφέρεται στη συνέχεια. Το RM-ODP παρέχει ένα γενικό πλαίσιο αναφοράς για τον σχεδιασμό μιας κατανεμημένης αρχιτεκτονικής με βάσει πέντε διαφορετικές όψεις του συστήματος και ταυτόχρονα κύριος στόχος του είναι να επιτρέψει την πραγμάτωση όλων των προτερημάτων της κατανομής υπηρεσιών σε ένα περιβάλλον με ετερογενείς πόρους και πολλαπλές διαχειριστικές περιοχές (organization domains).
Η επιλογή του συγκεκριμένου προτύπου βασίστηκε σε τρεις λόγους:

- Ο πρώτος λόγος είναι ότι μια αρχιτεκτονική προσανατολισμένη στις υπηρεσίες είναι εξ ορισμού κατανεμημένη. Άρα μια μεθοδολογία που θα οδηγήσει στον σχεδιασμό της θα πρέπει να επικεντρώνεται γύρω απο την ορθή και αποτελεσματική κατανομή υπηρεσιών και διεργασιών.
- Ο δεύτερος λόγος έχει να κάνει με τα ιδιαίτερα χαρακτηριστικά του: είναι αρκετά γενικό αλλά παρ' όλα αυτά ιδιαίτερα ευέλικτο ως προς τις έννοιες που παρέχει για την αναπαράσταση ενός κατανεμημένου συστήματος. Συγκεκριμένα, παρέχει την δυνατότητα αποτύπωσης του συστήματος απο πέντε διαφορετικές όψεις (επιχειρησιακή, υπολογιστική, πληροφορίας, μηχανικού, τεχνολογική) επιτρέποντας τον έλεγχο συνέπειας ανάμεσα στις όψεις και προσδιορίζει τις γλώσσες που απαιτούνται για τις προδιαγραφές χωρίς να επιβάλλει συγκεκριμένη σημειογραφία (notation).
- Ο τρίτος λόγος είναι ότι το πρότυπο είναι ευρέως διαδεδομένο και υπάρχουν πρακτικές ως προς την εφαρμογή του, οι οποίες θα μπορούσαν να αποτελέσουν το

αρχικό υλικό για την προδιαγραφή μιας συστηματικής κατασκευαστικής μεθόδου σχεδιασμού εστιασμένης στις αρχιτεκτονικές προσανατολισμένες στις υπηρεσίες.

Όπως αναφέρθηκε, το RM-ODP δεν υποστηρίζει ρητά μια συγκεκριμένη σημειογραφία για χρήση σε συνδυασμό με τις όψεις του. Όπως διατυπώνεται στην [Costa01], υπάρχουν αρκετές τυπικές και ημι-τυπικές γλώσσες και σημειογραφίες που θα μπορούσαν να ληφθούν υπόψην για χρήση στις προδιαγραφές των όψεων. Ανάμεσα σε αυτές, η σημειογραφία που καλύτερα πληρώνει την απαίτηση για έλεγχο συνέπειας ανάμεσα στις όψεις των προδιαγραφών ενός κατανεμημένου συστήματος είναι η Unified Modeling Language (UML) [UML]. Σε σχέση με άλλες γλώσσες, η SDL [SDL] είναι επίσης αντικειμενοστρεφής και έχει γραφική αναπαράσταση των εννοιών αλλά της λείπει ο πλούτος σε έννοιες που έχει η UML και δεν υποστηρίζει μηχανισμούς επέκτασης όπως το *στερεότυπο* της UML. Οι Lotos [Lotos] και η Z [Z] είναι επίσης τυπικές γλώσσες, αλλά έχουν περιορισμένο σύνολο βασικών εννοιών και παρομοίως δεν διαθέτουν μηχανισμούς επέκτασης προκειμένου να ξεπεράσουν αυτή την αδυναμία.
Στο παρόν κεφάλαιο λοιπόν δίνεται αρχικά μια περιγραφή του προτύπου και στη συνέχεια μια επισκόπηση υπαρχουσών προσεγγίσεων στο πώς το πρότυπο έχει εφαρμοστεί για την παραγωγή των προδιαγραφών διαφόρων συστημάτων, κυρίως σε συνδυασμό με την UML για την παροχή της απαραίτητης σημειογραφίας.

2.1.2 Υπάρχουσες προσεγγίσεις χρήσης του RM-ODP και αδυναμίες

Στην παράγραφο αυτή συνοψίζονται τα χαρακτηριστικά ερευνητικών προσεγγίσεων μεθοδολογιών για την δημιουργία και τεκμηρίωση προδιαγραφών κατανεμημένων αρχιτεκτονικών βάσει του προτύπου RM-ODP. Σημειώνεται ότι καμία απο τις προσεγγίσεις δεν επικεντρώνει στα ιδιαίτερα χαρακτηριστικά μιας αρχιτεκτονικής προσανατολισμένης σε υπηρεσίες.
Στις περισσότερες προσεγγίσεις δεν περιγράφονται όλες οι όψεις του προτύπου, κάτι που επιδεικνύει την ισχύ του ως προς τα επίπεδα αφαίρεσης που προσφέρει στον σχεδιαστή. Αυτό σημαίνει ότι μπορεί να εφαρμοστεί ένα μέρος των όψεων για την παραγωγή προδιαγραφών ορισμένων υποσυστημάτων, χωρίς να χρειάζεται να προδιαγραφεί μια πλήρης αρχιτεκτονική.
Στην πλειοψηφία τους, οι προσεγγίσεις αντιστοιχούν ένα υποσύνολο των εννοιών του RM-ODP σε μια γλώσσα σημειογραφίας, την οποία το RM-ODP δεν προσφέρει. Η πλέον συνηθισμένη γλώσσα γι' αυτό το σκοπό είναι η UML ή κάποια παρόμοια σημειογραφία. Η UML θεωρείται η κατεξοχήν γλώσσα προδιαγραφών παγκοσμίως για αντικειμενοστρεφή συστήματα. Στην [Genniloud98] γίνεται προσπάθεια ανάλυσης των παραμετροποιήσιμων χαρακτηριστικών των εννοιών του RM-ODP για τον ορισμό επαναχρησιμοποιήσιμων αντικειμένων.
Αν και το πρότυπο το υποστηρίζει, μόνο ένα μικρό μέρος των προσεγγίσεων που έχουν μελετηθεί παρέχει μια άμεση αντιστοίχιση απο την μια όψη της αρχιτεκτονικής σε μια άλλη [Costa01, Nankman96] ή κάνουν χρήση των ορισμένων συναρτήσεων του RM-ODP [Nankman96]. Η αντιστοίχιση αυτή μειώνει την πιθανότητα να υπάρχει ασυνέπεια ανάμεσα στις όψεις και θεωρείται μια βασική απαίτηση για την ορθότητα μιας μεθοδολογίας.
Όσον αφορά συγκεκριμένα στο πώς προδιαγράφονται οι συγκεκριμένες όψεις σε σχέση με την σημειογραφία, οι προσεγγίσεις ποικίλουν:

- Για την επιχειρησιακή όψη χρησιμοποιείται η UML για την προδιαγραφή της έννοιας των κοινοτήτων και την στατική επισκόπηση των υψηλού επιπέδου σχέσεων μεταξύ ομαδοποιημένων οντοτήτων [Kande04, Costa01]. Οι διεργασίες σε ορισμένες περιπτώσεις περιγράφονται σε υψηλότερο επίπεδο με περιπτώσεις χρήσης [Kande04, Costa01, Bjerde98] ή και με διαγράμματα ακολουθίας [Costa01], δραστηριοτήτων [Bjerde98] και συνεργασίας [Blinov03, Bjerde98] για πιο αναλυτική περιγραφή και δυναμική αναπαράσταση τους [Costa01]. Διαγράμματα κλάσεων χρησιμοποιούνται για τον προσδιορισμό δραστών και ρόλων [Blinov03].
- Για την όψη πληροφορίας, χρησιμοποιούνται διαγράμματα κλάσεων UML για το στατικό σχήμα [Kande01, Costa01], διαγράμματα καταστάσεων για συμπεριφορά αντικειμένων πληροφορίας κατά την διάρκεια του κύκλου ζωής τους (δυναμικό σχήμα) [Costa01] καθώς και η OCL [OCL] για την περιγραφή περιορισμών [Bjerde98].
- Η υπολογιστική όψη συνήθως προσεγγίζεται με διαγράμματα κλάσεων UML για την δομή υπολογιστικών αντικειμένων, διεπαφών και σχέσεων μεταξύ τους [Kande04, Akerhurst04, Costa01, Blinov03] και διαγράμματα ακολουθίας UML για τις αλληλεπιδράσεις μεταξύ αντικειμένων με έμφαση στην χρονική ακολουθία των μηνυμάτων που ανταλλάσσονται [Kande04, Costa01, Blinov03, Bjerde98]. Οι σχέσεις μεταξύ υπολογιστικών αντικειμένων συνήθως προδιαγράφονται με διαγράμματα συνεργασίας UML [Kande04, Costa01, Bjerde98]. Επίσης ενδέχεται να προστίθενται διαγράμματα καταστάσεων για περιγραφή της λειτουργικής συμπεριφοράς των αντικειμένων καθώς και η OCL για περιορισμούς τους [Akerhurst04]. Μια ακόμη εναλλακτική για την περιγραφή αντικειμένων και τις διεπαφές τους αποτελεί η IDL [Nankman96].
- Η όψη μηχανικού συνήθως αναπαρίσταται με διαγράμματα εγκατάστασης UML για την κατανομή των αντικειμένων [Kande04, Akerhurst04, Bjerde98], ή με ελεύθερα διαγράμματα [Blinov03]. Επίσης μπορεί να χρησιμοποιηθεί η IDL για τον ορισμό των αντικειμένων και των διεπαφών τους [Nankman96].
- Τέλος, η τεχνολογική όψη συνήθως προσεγγίζεται με φυσική γλώσσα [Kande04, Nankman96] για την περιγραφή των τεχνολογιών που επιλέγονται ή διαγράμματα εγκατάστασης UML για την περιγραφή του υλικού και λογισμικού [Bjerde98].

Σημαντικές αδυναμίες των προσεγγίσεων που έχουν προταθεί μέχρι σήμερα είναι οι ακόλουθες:

- Οι μέθοδοι σχεδιασμού είναι αυστηρά δεμένες με τις εκάστοτε κατανεμημένες αρχιτεκτονικές που καλούνται να υλοποιήσουν. Πέραν των συγκεκριμένων προτάσεων για την αναπαράσταση εννοιών του RM-ODP με ορισμένα διαγράμματα σε UML, δεν έχουν γενικευμένη ισχύ ούτε παρουσιάζουν έναν παραμετροποιήσιμο τρόπο σχεδιασμού.
- Δεν αποτελούν πλήρεις προδιαγραφές τυπικής κατασκευαστικής μεθόδου με συγκεκριμένα και διακριτά στάδια και βήματα που μπορεί κάποιος να ακολουθήσει προκειμένου να φτάσει σε ένα αποτέλεσμα. Γίνεται απλή παράθεση των όψεων και της σημειογραφίας χωρίς να μπορούν αυτές να εφαρμοστούν είτε συνολικά για την

προδιαγραφή μιας νέας αρχιτεκτονικής, είτε τμηματικά για την προδιαγραφή μόνο συγκεκριμένων επιχειρησιακών υπηρεσιών ανάλογα με τις ανάγκες.

- Δεν ορίζονται αντικείμενα που να είναι παραμετροποιήσιμα και να μπορούν να επαναχρησιμοποιηθούν ή να επεκταθούν κατάλληλα σύμφωνα με κάποιες αρχές για τον σχεδιασμό άλλων κατανεμημένων αρχιτεκτονικών.
- Λόγω της γενικότητας και του εύρους του RM-ODP, συνήθως χρησιμοποιείται ένα υποσύνολο απο τις έννοιες και τις αρχές σχεδιασμού που περιλαμβάνει. Για παράδειγμα συνήθως αποφεύγεται να γίνει αναφορά στις διαφάνειες κατανομής του προτύπου και πώς αυτές υποστηρίζονται, ποιοι μηχανισμοί ή υπηρεσίες υλοποιούν τις συναρτήσεις του RM-ODP και πώς τίθενται *σημεία ελέγχου εφαρμογής των προδιαγραφών (conformance points)*. Όταν το υποσύνολο αυτό είναι μικρό, είναι μεγαλύτερες οι πιθανότητες οι προδιαγραφές που δημιουργούνται να εμπεριέχουν ένα υψηλό επίπεδο ασυνέπειας, η οποία θα οδηγήσει σε καθυστερήσεις κατά την υλοποίηση ενός συστήματος.
- Οι υπάρχουσες προσεγγίσεις, αν και αναφέρονται σε κατανεμημένα συστήματα και εφαρμογές, δεν λαμβάνουν υπόψην τα ιδιαίτερα χαρακτηριστικά και τις απαιτήσεις των αρχιτεκτονικών προσανατολισμένων σε υπηρεσίες, ιδιαίτερα σε σχέση με την διαλειτουργικότητα και την ασφάλεια.

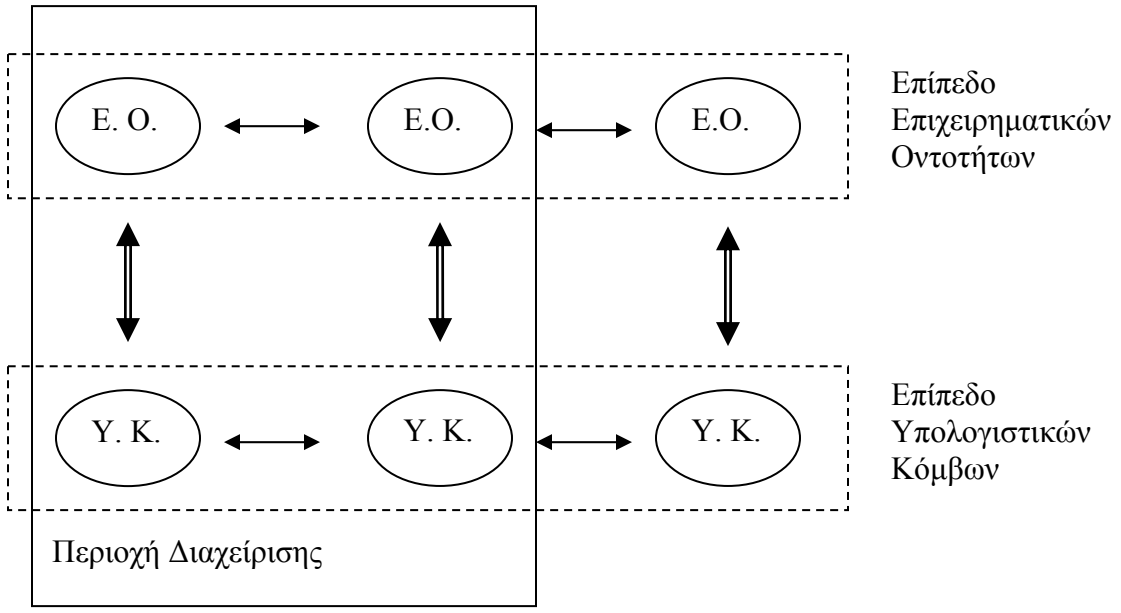
Τα παραπάνω συμπεράσματα λήφθηκαν υπόψην στην διατριβή, για την δημιουργία μιας νέας τυπικής και δομημένης κατασκευαστικής μεθόδου σχεδιασμού των προδιαγραφών αρχιτεκτονικών υπηρεσιών με έμφαση στην ασφάλεια και την διαλειτουργικότητα.

2.2 Υπάρχουσες Ανοιχτές Αρχιτεκτονικές Υπηρεσιών

Στην παράγραφο αυτή, περιγράφονται οι προσεγγίσεις ερευνητών παγκοσμίως στο πεδίο των ασφαλών αρχιτεκτονικών συστημάτων ηλεκτρονικών συναλλαγών και παροχής υπηρεσιών βασισμένων σε ΥΔΚ, XML και Υπηρεσίες Ιστού. Στο τέλος της παραγράφου παρατίθεται λίστα με τις ακριβείς αναφορές στις εργασίες αυτές.

2.2.1 Επίπεδα ασφάλειας αρχιτεκτονικών

Μια σύγχρονη αρχιτεκτονική που υποστηρίζει ηλεκτρονικές συναλλαγές θα πρέπει να σέβεται τόσο τις επιχειρηματικές απαιτήσεις του περιβάλλοντος στο οποίο πρόκειται να υλοποιηθεί όσο και τις απαιτήσεις διαλειτουργικότητας και ασφάλειας που απορρέουν απο το περιβάλλον και απο το σχετικό νομικό πλαίσιο. Η ανάγκη για διαλειτουργικότητα φαίνεται απο την στροφή προς αρχιτεκτονικές βασισμένες σε XML και Υπηρεσίες Ιστού. Σε μια ασφαλή αρχιτεκτονική, οι βασικές απαιτήσεις ασφάλειας (ιδιωτικότητα, ακεραιότητα, μη άρνηση συμμετοχής, αυθεντικοποίηση, έλεγχος πρόσβασης) εξασφαλίζονται συνήθως σε δύο επίπεδα, όπως φαίνεται και στο ακόλουθο σχήμα:



Σχήμα 2-1: Επίπεδα διάκρισης και υλοποίησης απαιτήσεων ασφάλειας

- Στο επίπεδο ανταλλαγής μηνυμάτων μεταξύ υπολογιστικών κόμβων (Υ. Κ.), όπου η εφαρμογή της XML, των ΥΔΚ και των Υπηρεσιών Ιστού εμφανίζεται συνήθως με την μορφή των προτύπων:
  - SSL/TLS,
  - Ψηφιακών Υπογραφών και Κρυπτογράφησης XML,
  - Ασφάλειας Υπηρεσιών Ιστού και
  - κάποιου μοντέλου Ελέγχου Πρόσβασης.
- Στο επίπεδο ανταλλαγής μηνυμάτων μεταξύ επιχειρηματικών οντοτήτων (Ε.Ο.) (οι οποίες για παράδειγμα μπορεί να είναι και οι ίδιοι οι χρήστες του συστήματος), όπου

οι απαιτήσεις ασφάλειας συνήθως είναι στενά δεμένες με το νομικό πλαίσιο και τις πολιτικές των οργανισμών που εμπεριέχουν τις οντότητες. Στο επίπεδο αυτό, το σύνολο των πιθανών εφαρμογών ΥΔΚ σήμερα περιορίζονται στην παροχή ψηφιακών πιστοποιητικών για την διεξαγωγή ασφαλούς η-ταχυδρομείου και των Ψηφιακών Υπογραφών και κρυπτογράφησης XML.

Μία *«Περιοχή Διαχείρισης» (Administration Domain)* αποτελεί στα πλαίσια της διατριβής το σύνολο των οντοτήτων που ανήκουν σε μια ομάδα την οποία διέπουν κοινοί κανόνες και επιχειρηματικές πολιτικές. Ανάλογα με το σύνολο των κανόνων που θα ορίσουμε, μια Περιοχή Διαχείρισης μπορεί να είναι π.χ. ένας οργανισμός και οι υπάλληλοί του, ή μια ολόκληρη χώρα και οι πολίτες της.
Όπως φαίνεται απο το σχήμα, Υ.Κ. και Ε.Ο. μπορεί να ανήκουν και να επικοινωνούν μέσα στην ίδια περιοχή διαχείρισης ή και να ανήκουν σε διαφορετικές περιοχές διαχείρισης.
Η βέλτιστη πρακτική σε μια ολοκληρωμένη αρχιτεκτονική είναι οι υπηρεσίες ασφάλειας που χρησιμοποιεί το άνω επίπεδο να χρησιμοποιούν τις μονάδες ασφάλειας του κάτω επιπέδου προκειμένου να έχουμε επαναχρησιμοποίηση πόρων.
Η μελέτη των εργασιών που ακολουθεί στόχο έχει να αποτυπώσει την υπάρχουσα κατάσταση και να αναδείξει αδυναμίες που υπάρχουν σε τέτοιου τύπου αρχιτεκτονικές.

2.2.2 Χαρακτηριστικά αρχιτεκτονικών και αδυναμίες

Στα πλαίσια της παρούσας διατριβής, οι αρχιτεκτονικές που μελετήθηκαν, αναλύονται ως προς τα χαρακτηριστικά που έχουν να κάνουν με την διαλειτουργικότητα και την ασφάλειά τους.
Πιο συγκεκριμένα, μελετήθηκε:

- Ο τρόπος επικοινωνίας των μηχανισμών και υπηρεσιών εντός των αρχιτεκτονικών, καθώς και των αρχιτεκτονικών με εξωτερικές οντότητες ως προς αυτές.
- Οι παρεχόμενοι μηχανισμοί και υπηρεσίες ασφάλειας, με έμφαση στην διαχείριση ταυτότητας, τον έλεγχο πρόσβασης, τις ψηφιακές και προηγμένες ηλεκτρονικές υπογραφές, την κρυπτογράφηση και την διαχείριση κλειδιών και πιστοποιητικών.

Σε όλες τις αρχιτεκτονικές που έχουν προταθεί χρησιμοποιείται είτε μόνο XML, είτε XML σε συνδυασμό με Υπηρεσίες Ιστού για την δημιουργία, αποστολή και αποθήκευση μηνυμάτων και εγγράφων προκειμένου να επιτευχθεί ανεξαρτησία απο το υποκείμενο σύστημα και διαλειτουργικότητα.
Ως προς την παροχή υπηρεσιών ασφάλειας για το επίπεδο υπολογιστικών κόμβων, στις περισσότερες αρχιτεκτονικές εφαρμόζονται ξεχωριστές διαδικασίες ασφάλειας στα μηνύματα (ψηφιακές υπογραφές, κρυπτογράφηση) προκειμένου να υπάρχει σαφής και διακριτή ενσωμάτωση της πληροφορίας ασφάλειας ανάλογα με τις απαιτήσεις της συναλλαγής (transaction). Επίσης παρέχεται ασφάλεια τόσο κατά την μετακίνηση μηνυμάτων όσο και κατά την αποθήκευσή τους. Παρ' όλα αυτά ακόμη δεν υποστηρίζεται ευρέως η ασφαλής επικοινωνία μεταξύ Υπηρεσιών Ιστού χρησιμοποιώντας τα τελευταία πρότυπα ασφάλειας για μηνύματα SOAP (ψηφιακές υπογραφές, κρυπτογράφηση, WS-Security) [Lee03].

Η ευέλικτη υλοποίηση πολιτικών ασφάλειας απαιτεί τον κατάλληλο διαχωρισμό των δομικών μονάδων έτσι ώστε να είναι εύκολο να χρησιμοποιείται κάθε φορά το κατάλληλο σύνολο μονάδων ανάλογα με τις απαιτήσεις ασφάλειας της περιοχής διαχείρισης στην οποία πρόκειται να εφαρμοστεί. Για παράδειγμα, ανάλογα με την πολιτική του οργανισμού που θα υιοθετήσει την αρχιτεκτονική, θα πρέπει να είναι δυνατόν να χρησιμοποιείται μόνο η υπηρεσία υπογραφής των μηνυμάτων SOAP, ή να χρησιμοποιούνται υπογραφές μόνο απο τη μία πλευρά, ή να χρησιμοποιούνται και απο τις δύο πλευρές σε συνδυασμό με κρυπτογράφηση κ.λ.π. Στην πλειοψηφία τους, οι μέχρι σήμερα προταθείσες αρχιτεκτονικές δεν παρέχουν την δυνατότητα αυτής της παραμετροποίησης [Lee03].
Προκειμένου να εξασφαλίσει την ακεραιότητα και αυθεντικότητα των εγγράφων XML που υπογράφονται στο σύστημα, σε κάποιες αρχιτεκτονικές λαμβάνεται υπόψην ότι οι ψηφιακές υπογραφές πρέπει να εκτελούνται στην πλευρά του χρήστη, και ενσωματώνει στο σχεδιασμό τις κατάλληλες μονάδες που τρέχουν στον φυλλομετρητή του χρήστη και επικοινωνούν με μια μονάδα ανάγνωσης έξυπνων καρτών, προκειμένου να χρησιμοποιηθούν τα κλειδιά και τα πιστοποιητικά που περιέχονται στην έξυπνη κάρτα του χρήστη. Αυτό υλοποιείται είτε με τεχνολογία Java Applets [Blobel03] είτε με στοιχεία ActiveX [diNatale04].
Μια σημαντική παράμετρος των προταθεισών αρχιτεκτονικών είναι ο τρόπος επίτευξης του ελέγχου πρόσβασης και διαχείρισης ταυτότητας. Στον τομέα αυτό υπάρχουν πολλές διαφορετικές προσεγγίσεις:

- Ενδέχεται να μην υλοποιούνται καθόλου υπηρεσίες ελέγχου πρόσβασης [Lee03]. Όταν υπάρχουν, συνήθως το μοντέλο ελέγχου πρόσβασης καθορίζει αναγνωριστικά χρηστών, ρόλους και τύπους πρόσβασης [Komathy03, Blobel03, Gritzalis04].
- Σε κάποιες αρχιτεκτονικές η μονάδα ελέγχου πρόσβασης βασίζεται σε μια μη προτυποποιημένη αρχιτεκτονική, η οποία σχεδιάστηκε κυρίως σύμφωνα με τις συγκεκριμένες ανάγκες της εκάστοτε αρχιτεκτονικής [Komathy03, Rezgui02, Fernandez02, diNatale04].
- Υπάρχουν αρχιτεκτονικές στις οποίες υλοποιείται μια Υποδομή Διαχείρισης Δικαιωμάτων (Privilege Management Infrastructure) με χρήση Πιστοποιητικών Χαρακτηριστικών (Attribute Certificates) και ένας εξυπηρετητής πολιτικών. Τα Πιστοποιητικά Χαρακτηριστικών χρησιμοποιούνται προκειμένου να οριστούν ρόλοι, ομάδες, ταυτότητες, και περιορισμοί για τους χρήστες στο σύστημα. Τα Πιστοποιητικά Χαρακτηριστικών εκδίδονται απο μια Αρχή έκδοσης Πιστοποιητικών Χαρακτηριστικών (Attribute Authority). Τα πιστοποιητικά αυτά χρησιμοποιούνται σε συνδυασμό με πιστοποιητικά X509 εκδιδόμενα απο μια Αρχή Πιστοποίησης. Τα πρώτα βεβαιώνουν τα χαρακτηριστικά και το ρόλο ενός χρήστη, ενώ τα δεύτερα την ταυτότητά του. Το σχήμα αυτό είναι αρκετά ευέλικτο και μπορεί να υλοποιήσει διάφορες μορφές μοντέλων ελέγχου πρόσβασης, όπως είναι το μοντέλο Ελέγχου Πρόσβασης βασισμένο σε Ρόλους [Blobel03].
- Ο αριθμός των αρχιτεκτονικών που έχουν υιοθετήσει πιο προηγμένα πρότυπα ασφάλειας για υπηρεσίες ιστού είναι ακόμη μικρός. Σε αυτές περιλαμβάνονται αρχιτεκτονικές όπου έλεγχος πρόσβασης βασίζεται στην γλώσσα XACML προκειμένου να συνδυαστούν τα έγγραφα με της πολιτικές ελέγχου πρόσβασης. Με την γλώσσα αυτή είναι δυνατή η εφαρμογή ελέγχου πρόσβασης και μεταξύ

διαφορετικών «περιοχών διαχείρισης» και συνδυάζεται με έναν μοντέλο Ελέγχου Πρόσβασης βασισμένο σε Ρόλους [Gritzalis04]. Το ίδιο ισχύει και για την περίπτωση της διαχείρισης κλειδιών και πιστοποιητικών με την χρήση του προτύπου XKMS, η οποία διευκολύνει την επικοινωνία των Υπηρεσιών Ιστού της αρχιτεκτονικής με την Αρχή Πιστοποίησης, προκειμένου να επιτευχθεί αυτόματα η εγγραφή κλειδιών και η έκδοση πιστοποιητικών, καθώς επίσης και ο έλεγχος εγκυρότητας των πιστοποιητικών που χρησιμοποιούνται απο τις υπηρεσίες ασφάλειας [Lee03].

- Σε ορισμένες προσεγγίσεις παρέχονται υπηρεσίες αυθεντικοποίησης, διαχείρισης διαπιστευτηρίων οντοτήτων και ελέγχου πρόσβασης σε κατανεμημένα συστήματα πάνω απο το διαδίκτυο, είτε με χρήση έξυπνων πρακτόρων (intelligent agents) [Gritzalis04] ή κινητών πρακτόρων [Rezgui02, Fernandez02].

Απο την μελέτη των παραπάνω, προέκυψαν ένα σύνολο απο αδυναμίες οι οποίες έχουν να κάνουν κυρίως με την τεχνική ολοκλήρωση των υπηρεσιών και μηχανισμών ασφάλειας μέσα σε μια αρχιτεκτονική. Οι αρχιτεκτονικές που μελετήθηκαν είναι ενδεικτικές προσπάθειες αντιμετώπισης της ασφάλειας ως μεμονωμένες τεχνικές λύσεις και όχι ως ένα συνολικό πλαίσιο.

Συγκεκριμένα συμπεράσματα που μπορούν να εξαχθούν είναι τα ακόλουθα:

- Σε όλες τις προσεγγίσεις η ασφάλεια στο επίπεδο ανταλλαγής μηνυμάτων μεταξύ Ε.Ο. βασίζεται σε απλές υπογραφές XML χωρίς να συνδυάζεται με ενσωματωμένη πολιτική υπογραφής και πληροφορία χρονοσήμανσης και άρα αποτυγχάνει να καλύψει την απαίτηση για μη-άρνηση συμμετοχής, τόσο στο επίπεδο μεταφοράς των μηνυμάτων XML, όσο και στο επίπεδο αποθήκευσής τους και μελλοντικής τους χρήσης.
- Στο μεγαλύτερο μέρος των αρχιτεκτονικών, δεν περιγράφεται καν το καθεστώς δημιουργίας των ψηφιακών υπογραφών, το οποίο συνήθως λαμβάνει χώρα στον εξυπηρετητή εφαρμογών της αρχιτεκτονικής, και άρα ο χρήστης δεν έχει κανέναν έλεγχο πάνω στο τι υπογράφεται.
- Οι υπηρεσίες ελέγχου πρόσβασης και διαχείρισης ταυτοτήτων αν και σε κάποιες αρχιτεκτονικές βασίζονται στην XML, συνήθως δεν λαμβάνουν υπόψην της πρότυπα του χώρου και άρα δεν αποτελούν διαλειτουργικές λύσεις προκειμένου να επιτευχθεί έλεγχος σε ευρύτερες «περιοχές διαχείρισης» (“administration domains”) και για κλιμάκωση σε μια αυξανόμενη κοινότητα χρηστών. Το μοντέλο χρήσης Πιστοποιητικών Χαρακτηριστικών [Blobel03] παρουσιάζει δυσκολίες στην περίπτωση ελέγχου πρόσβασης με χρήση αιτήσεων πρόσβασης που ξεπερνούν τα σύνορα «περιοχών διαχείρισης» και η χρήση κινητών πρακτόρων είναι ακόμη μια ανοιχτή περιοχή ειδικά στο θέμα της ασφάλειας, καθώς θεωρούνται ευπαθείς σε επιθέσεις αλλαγής κώδικα [Rezgui02, Fernandez02].
- Τέλος, αν και ένα μεγάλος μέρος των αρχιτεκτονικών χρησιμοποιεί ΥΔΚ, δεν προβλέπουν έναν πιο κλιμακούμενο και διαλειτουργικό τρόπο πρόσβασης στις υπηρεσίες αυτές προκειμένου να γίνεται διαφανής η εγγραφή στην ΥΔΚ και ο έλεγχος των πιστοποιητικών.

Επιπρόσθετα, η μελέτη συγκεκριμένων αρχιτεκτονικών ως προς την ασφάλεια, οδήγησε στην αναγνώριση συγκεκριμένων τεχνικών αδυναμιών, που έχουν άμεση σχέση με τη διαλειτουργικότητα, την διαφάνεια ως προς τις διαδικασίες ασφάλειας όπως τις αντιλαμβάνεται ο χρήστης, καθώς και την ικανοποίηση των επιχειρηματικών στόχων.

Συνοπτικά αυτές είναι οι ακόλουθες:

- Τα ηλεκτρονικά έγγραφα που διακινούνται ανάμεσα σε διαφορετικές οργανωτικές και διοικητικές περιοχές ή που καταλήγουν στα χέρια ενός χρήστη, στηρίζονται σε υπηρεσίες ασφάλειας του επιπέδου Υ.Κ., όπως παρουσιάστηκε στην εισαγωγή του κεφαλαίου. Παρ' όλα αυτά, η απαίτηση για μη άρνηση συμμετοχής επιβάλλει την επιπλέον χρησιμοποίηση υπηρεσιών χρονοσφράγισης σύμφωνα με μια προδιαγεγραμμένη πολιτική υπογραφών τόσο για τα διακινούμενα έγγραφα, όσο και για την ασφαλή αποθήκευση των εγγράφων.
- Προκειμένου να έχει νομική υπόσταση η υπογραφή ενός εγγράφου στο επίπεδο Ε.Ο., είναι απολύτως απαραίτητο οποιουδήποτε τύπου Ψηφιακή Υπογραφή να δημιουργείται στην πλευρά του ίδιου του χρήστη και στο ίδιο το επίπεδο Ε.Ο. και όχι στο επίπεδο των Υ.Κ. Αυτό που παρατηρείται να συμβαίνει στην πλειοψηφία των αρχιτεκτονικών, είναι η δημιουργία όλων των υπογραφών στους εξυπηρετητές με τους οποίους επικοινωνεί ο φυλλομετρητής ενός χρήστη, και όχι στο περιβάλλον του ίδιου του υπολογιστή του χρήστη όπου είναι συνδεδεμένη η έξυπνη κάρτα του. Στις περιπτώσεις που υιοθετείται το ορθό μοντέλο, αμελείται η πρώτη αδυναμία, οπότε δεν ικανοποιείται ούτως η άλλως ολοκληρωμένη υπηρεσία μη-άρνησης συμμετοχής.
- Η πλειοψηφία των αρχιτεκτονικών που έχουν μελετηθεί, υιοθετεί ένα μοντέλο ελέγχου πρόσβασης και διαχείρισης της ταυτότητας των χρηστών. Συνήθως όμως αυτό ακόμη και αν βασίζεται στην XML δεν αποτελεί μια προτυποποιημένη υλοποίηση, κάτι που δυσχεραίνει την επεκτασιμότητα της αρχιτεκτονικής και την επικοινωνία μεταξύ διαφορετικών Περιοχών Διαχείρισης.
- Οι αρχιτεκτονικές ως επί το πλείστον δεν δίνουν λύση στο θέμα της εύκολης και γρήγορης επικοινωνίας με την ΥΔΚ, προκειμένου να διευκολυνθεί η ενσωμάτωση των υπηρεσιών ασφάλειας με κύριες δραστηριότητες την εγγραφή στην Αρχή Πιστοποίησης και τον έλεγχο κλειδιών και πιστοποιητικών.

Τα συμπεράσματα αυτά έχουν ληφθεί υπόψην τόσο κατά την τεκμηρίωση του σχεδιασμού της κατασκευαστικής μεθόδου του κεφαλαίου 4, όσο και κατά τον σχεδιασμό των επιχειρησιακών υπηρεσιών (βάσει της μεθόδου) του κεφαλαίου 5.

2.3 Συμπεράσματα

Οι Υποδομές Δημοσίου Κλειδιού και οι υπηρεσίες που προσφέρουν, έχουν την ικανότητα να καλύψουν ένα μέρος των αναγκών σε ασφάλεια σύγχρονων πληροφοριακών συστημάτων που βασίζονται σε νέες τεχνολογίες. Είναι όμως αποδεκτό στη βιβλιογραφία αλλά και ως αποτέλεσμα ερευνών, ότι η επιτυχημένη χρήση των τεχνολογιών ΥΔΚ είναι περιορισμένη, παρά τις επενδύσεις που έχουν γίνει. Οι σημαντικότεροι λόγοι είναι το κόστος ενσωμάτωσης και χρήσης, η έλλειψη φιλικότητας προς τους χρήστες και κατανόησης των μηχανισμών των ΥΔΚ, η έμφαση περισσότερο στην τεχνολογία και όχι στην ανάγκη και η έλλειψη διαλειτουργικότητας των

εφαρμογών. Οι λόγοι αυτοί έχουν οδηγήσει στην ύπαρξη λίγων εφαρμογών που αντιμετωπίζουν συνολικά αυτά τα προβλήματα και στην έλλειψη ευρείας χρήσης ΥΔΚ και των συναφών τεχνολογιών ασφάλειας. Η XML αποτελεί μια τεχνολογία – ενδιάμεσο κρίκο – που μπορεί να προσδώσει στις ΥΔΚ θετική ώθηση και να λύσει το κομμάτι των προβλημάτων των σχετικών με τη διαλειτουργικότητα και το κόστος, αφού η ερευνητική κοινότητα αλλά και ο επιχειρηματικός κόσμος την χρησιμοποιούν ολοένα και περισσότερο για την προδιαγραφή και υλοποίηση εμπορικών προϊόντων, αλλά και προϊόντων ανοιχτού κώδικα. Υπάρχει λοιπόν ταυτόχρονα η απαίτηση για ενσωμάτωση υπηρεσιών ΥΔΚ και XML σε εφαρμογές με γνώμονα τις ανάγκες του χρήστη, και ταυτόχρονα για εξάλειψη οποιωνδήποτε υπαρχόντων ή νέων προβλημάτων που προκύπτουν από τον συνδυασμό αυτό.

Στην περιοχή των Υπηρεσιών Ιστού, η διαδικασία προτυποποίησης είναι ακόμη σε αρχικό στάδιο και τα ίδια τα πρότυπα παρουσιάζουν αδυναμίες Αυτό αφορά ακόμη περισσότερο το οικοδόμημα των αρχιτεκτονικών προσανατολισμένων σε υπηρεσίες, στις οποίες οι Υπηρεσίες Ιστού θεωρούνται ο ακρογωνιαίος λίθος. Οι ανάγκες που προκύπτουν στην έρευνα για διαδικασίες σχεδιασμού, υλοποίησης και διασύνδεσης αρχιτεκτονικών προσανατολισμένων στις υπηρεσίες σχετίζονται με τους τρόπους επίτευξης του απαραίτητου επίπέδου ασφάλειας και διαλειτουργικότητας σε νεοδημιουργηθείσες ή ήδη υπάρχουσες αρχιτεκτονικές υπηρεσιών.

Επιπρόσθετα, εμφανίζεται η ανάγκη για δημιουργία συστηματικών κατασκευαστικών μεθόδων σχεδιασμού τέτοιων αρχιτεκτονικών που να λαμβάνουν υπόψην τα ιδιαίτερα χαρακτηριστικά τους, να επιτρέπουν τον σφαιρικό σχεδιασμό απο πολλές όψεις (π.χ. επιχειρησιακή, τεχνολογική) και να είναι συμβατές με διαδεδομένα πρότυπα του χώρου. Ορισμένα πλαίσια που παρουσιάστηκαν στο παρόν κεφάλαιο [Zackman87, Kruchten95, RM-ODP, OGAF, DoDAF] είναι πολύ γενικά χωρίς να διατυπώνουν ακριβείς διαδικασίες, δεν δίνουν ιδιαίτερη σημασία στο πολύ σημαντικό θέμα της ασφάλειας ή την θεωρούν ως μεμονωμένη τεχνική λύση, απαιτούν συχνά την δημιουργία της αρχιτεκτονικής απο το μηδέν (και άρα δεν επιτρέπουν την αναβάθμιση ή την ενσωμάτωση υπαρχουσών υποδομών) και δεν παρέχουν συγκεκριμένα επαναχρησιμοποιήσιμα στοιχεία για εισαγωγή σε ένα πλήθος αρχιτεκτονικών με κοινά χαρακτηριστικά. Τέλος στην περίπτωση της δημιουργίας νέων μεθοδολογιών σχεδιασμού που αντιμετωπίζουν τις ανάγκες της νέας γενιάς αρχιτεκτονικών, τίθεται το ερώτημα πώς υπάρχοντα πλαίσια και πρότυπα συντελούν στον σχεδιασμό διαφόρων ειδών υπηρεσιών (που είναι η καρδιά τέτοιου τύπου αρχιτεκτονικών) τόσο σε αρχιτεκτονικές που δημιουργούνται από την αρχή, όσο και σε ήδη υπάρχουσες που πρέπει να επεκταθούν με νέες επιχειρησιακές υπηρεσίες.

Βάσει των παραπάνω, η διατριβή αρχικά επιχειρεί να δώσει λύσεις σε επιμέρους προβλήματα που μελετήθηκαν στην περιοχή της ασφάλειας με χρήση Υ.Δ.Κ και XML και την εφαρμογή της σε συγκεκριμένες επιχειρησιακές υπηρεσίες στους τομείς του η-επιχειρείν, και στη συνέχεια παρουσιάζει αναλυτικά μια νέα κατασκευαστική μεθοδολογία για τον συστηματικό σχεδιασμό ασφαλών και διαλειτουργικών αρχιτεκτονικών υπηρεσιών. Τέλος ως απόδειξη της εφαρμοσιμότητας της μεθόδου, παρουσιάζονται οι προδιαγραφές δύο συγκεκριμένων επιχειρησιακών υπηρεσιών η-συναλλαγών που έχουν υλοποιεί με τη φιλοσοφία αρχιτεκτονικών προσανατολισμένων σε υπηρεσίες.

2.4 Αναφορές

[Akerhurst04] D.H. Akerhurst, A.G. Waters, J. Derrick. (2004). "A Viewpoints Approach to Designing Group Based Applications", Design, Analysis and Simulation of Distributed Systems 2004, Advanced Simulation Technologies Conference, pages 83-93, Arlington, Virginia

[Bjerde98] L. Bjerde, A.J. Berre, J. Oldevik. (1998). "Describing a system from multiple viewpoints – using ISO/RM-ODP with OOram role modeling and UML", http://heim.ifi.uio.no/~trygver/1998/RM-ODP/Bjerde-ODP.doc

[Blinov03] M. Blinov, A. Patel. (2003). "An application of the reference model for open distributed processing to electronic brokerage", Computer Standards and Interfaces, Elsevier Science, pp. 411-425

[Blobel03] B. Blobel et al. (2003). "Using a privilege management infrastructure for secure web-based e-health applications". Computer Communications, Elsevier, Volume 26, Issue 16, pp. 1863-1872

[CIO] CIO-Council, "Federal Enterprise Architecture Framework version 1.1," 1999, http://www.cio.gov/archive/fedarch1.pdf.

[CORBA] Object Modelling Group / Common Object Request Broker Architecture, http://www.omg.org

[Costa01] C.A. Costa, J.A. Harding, R.I.M Young. (2001). "The application of UML and an open distributed process framework to information system design", Computers in Industry, Elsevier Science, pp. 33-48

[DCE] Open Software Foundations / Distributed Computing Environment, http://www.osf.org

[diNatale04] M. di Natale, T. Cucinotta, S. Kolachalam. (2004). "A Modular Open-Source Architecture for ICT Services in the Public Administration", Lecture Notes in Computer Science, Springer-Verlag GmbH, Volume 2739 / 2004, pp. 167 – 172

[DoDAF] US Department of Defense. (2003). "Department of Defense Architecture Framework Version 1.0 - Vol 1 Definition & Guideline and Vol 2 Product Descriptions". http://www.aitcnet.org/dodfw.

[Fernandez02] A. Fernandez. (2002). "Towards Interoperability amongst European Public Administrations", Electronic Government: First International Conference, EGOV 2002, Proceedings, Aix-en-Provence, France, September 2-5, Lecture Notes in Computer Science, Springer-Verlag GmbH, Volume 2456 / 2002, pp. 105 - 110

[Genilloud98] G. Genilloud. (1998). "Common domain objects in the RM-ODP viewpoints", Computer Standards & Interfaces, Elsevier Science, pp. 361-374

[Gritzalis04] D. Gritzalis, C. Lambrinoudakis. (2004). "A security architecture for interconnecting health information systems", International Journal of Medical Informatics, Elsevier, Volume 73, Issue 3, pp. 305-309

[Kande04] M. Kande et al. (2004). "Applying UML to Design an Inter-Domain Service Management application", Lecture Notes in Computer Science, Springer-Verlag GmbH, Volume 1618/2004, pp. 200-214

[Komathy03] K. Komathy, V. Ramachandran, P. Vivekanandan. (2003). "Security for XML messaging services: a component-based approach Source", Journal of Network and Computer Applications, ACM, Volume 26 , Issue 2, pp. 197 - 211

[Kruchten95] P. Kruchten. (1995). "The 4+1 View Model of Architecture," IEEE Software, vol. 12, pp. pp 42-50.

[Lee03] S. Lee et al. (2003). “TY*SecureWS: An Integrated Web Service Security Solution Based on Java”, E-Commerce and Web Technologies: 4th International Conference, Proceedings, Prague, Czech Repbulic, 2003, Lecture Notes in Computer Science, Springer-Verlag GmbH, Volume 2738 / 2003, pp. 186 - 195
[Lotos] ISO. (1989). “Lotos - Information processing systems -- Open Systems Interconnection - LOTOS - A formal description technique based on the temporal ordering of observational behaviour”. International Standard - IS 8807.
[Nankman96] M. A. Nankman, L. J.M. Nieuwenhuis. (1996). “Specification of a distributed storage system”, Computer Communications, Elsevier Science, 1996, pp. 30-38
[OCL] Object Management Group. (2005). “OCL 2.0 Specification”. http://www.omg.org/docs/ptc/05-06-06.pdf
[OGAF] The Open Group. (2003). "The Open Group Architecture Framework (ver 8.1 Enterprise Edition)". http://www.opengroup.org/architecture/togaf/#download.
[Rezgui02] A. Rezgui et al. (2002). “Preserving privacy in web services”, Proceedings of the 4th international workshop on Web information and data management, McLean, Virginia, USA, ACM, pp. 56 - 62
[RM-ODP] ITU-T Rec. X.901 | ISO/IEC 10746-1,2,3, “Reference Model for Open Distributed Processing – Part 1: Overview, Part 2 Foundations, Part 3 Architecture”, 1996-98
[SDL] ITU-T. (2000). “Formal description techniques (FDT) - Specification and Description Language (SDL)”. ITU-T Recommendation Z.100
[Tang04] A. Tang, J. Han, and P. Chen. (2004). "A Comparative Analysis of Architecture Frameworks," Swinburne University of Technology SUTIT-TR2004.01
[UML] Unified Modeling Language (UML), http://www.uml.org/
[Z] ISO. (2002). “Information Technology - Z Formal Specification Notation - Syntax, Type System and Semantics”. ISO/IEC 13568:2002
[Zackman87] J. Zachman. (1987). "A framework for Information Architecture," IBM Systems Journal, vol. 38.

3 Δημιουργία και εφαρμογή αναβαθμισμένων υπηρεσιών ασφάλειας & προηγμένων υπηρεσιών η-επιχειρείν

Βασική δραστηριότητα κατά τη διάρκεια της διατριβής ήταν η μελέτη υπαρχόντων τεχνολογικών προτύπων και πρωτοκόλλων, η εύρεση αδυναμιών και η πρόταση λύσεων. Στις παραγράφους που ακολουθούν, περιγράφονται τα αποτελέσματα της έρευνας σχετικά με τέτοιου τύπου αδυναμίες και οι λύσεις που προτάθηκαν για την αναίρεσή τους.

Παράλληλα με την προσπάθεια εύρεσης λύσεων σε αδυναμίες τεχνολογιών, προτύπων και πρωτοκόλλων, μελετήθηκαν και οι αδυναμίες και ελλείψεις σε εφαρμογές που βασικός τους στόχος είναι είτε αυτή καθεαυτή η παροχή ασφάλειας, είτε η εκτέλεση κάποιας επιχειρηματικής δραστηριότητας. Η μελέτη τέτοιων αδυναμιών και ελλείψεων εφαρμογών έγινε με μια οριζόντια λογική, έτσι ώστε να καλυφθούν όσο το δυνατόν περισσότεροι τομείς δραστηριοτήτων. Πιο συγκεκριμένα, η ερευνητική δραστηριότητα κάλυψε τους τομείς του η-εμπορίου, της η-διακυβέρνησης, της η-υγείας και του η-τουρισμού. Στις περιπτώσεις που έγινε υλοποίηση κάποιας εφαρμογής, η διαδικασία περιελάμβανε όλες τις απαραίτητες φάσεις: αποτύπωση απαιτήσεων χρηστών και ασφάλειας, καταγραφή προδιαγραφών, υλοποίηση και έλεγχο. Η ακολουθία αυτή διαδικασιών επαναλαμβανόταν μέχρι η εφαρμογή να φτάσει στην τελική της μορφή.

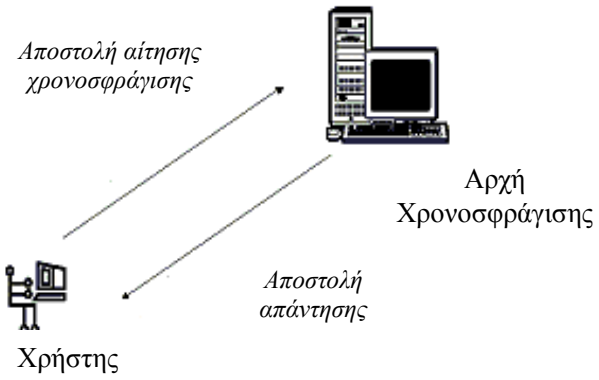
3.1 Αναβαθμισμένες υπηρεσίες ασφάλειας

Το παρόν κεφάλαιο περιλαμβάνει υπάρχουσες υπηρεσίες ασφάλειας που έχουν αναβαθμιστεί οι ίδιες ή ο τρόπος εφαρμογής τους προκειμένου να αποφευχθούν αδυναμίες που παρουσιάζουν.

3.1.1 Αναβαθμισμένη υπηρεσία Χρονοσφράγισης σε η-συναλλαγές

3.1.1.1 Υπάρχουσα κατάσταση

Χρονοσφράγιση (Time stamping) είναι μια υπηρεσία ΥΔΚ που συνδυάζει ψηφιακές υπογραφές και μια έμπιστη πηγή χρόνου προκειμένου να εξασφαλίσει ότι ορισμένα ψηφιακά δεδομένα υπάρχουν απο μια χρονική στιγμή και μετά. Το υπάρχον πρότυπο Χρονοσφράγισης IETF RFC 3161 περιγράφει το πρωτόκολλο επικοινωνίας μιας οντότητας που θέλει να χρονοσφραγίσει κάποια δεδομένα με την Αρχή Χρονοσφράγισης (Time-stamping Authority ή TSP).

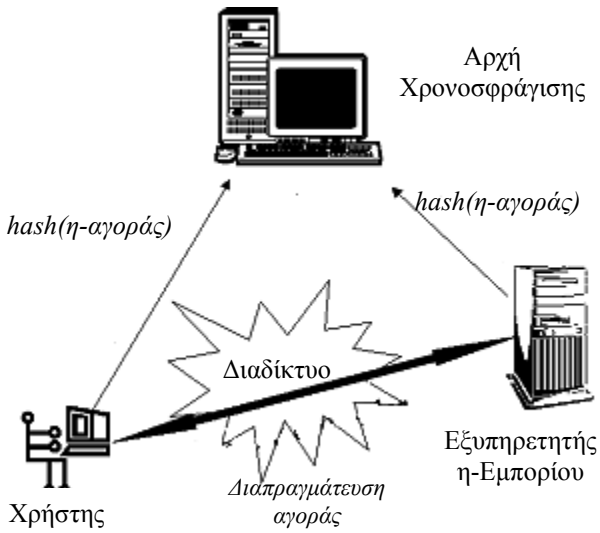


Σχήμα 3-1: Παραδοσιακό πρωτόκολλο χρονοσφράγισης

Η διαδικασία που περιγράφεται απο το πρωτόκολλο αυτό, περιλαμβάνει την εφαρμογή μιας συνάρτησης κατακερματισμού στο έγγραφο προς χρονοσφράγιση και αποστολή του αποτελέσματος της συνάρτησης στην Αρχή, η οποία αναλαμβάνει να το υπογράψει ψηφιακά συνδυάζοντάς το με την ώρα και την ημερομηνία που λαμβάνει απο μια παγκοσμίως έμπιστη πηγή χρόνου χρησιμοποιώντας κοινά πρωτόκολλα διαδικτύου (HTTP, TCP sockets). Το τελικό αποτέλεσμα είναι μια δομή δεδομένων χρονοσφράγισης (time stamp token) που επιστρέφεται στον χρήστη για αποθήκευση.

3.1.1.2 Χρονοσφράγιση σε η-συναλλαγές με περισσότερα των 2 μερών

Στην περίπτωση που θέλουμε να εφαρμόσουμε την Χρονοσφράγιση για να ασφαλίσουμε χρονικά μια ηλεκτρονική συναλλαγή στο διαδίκτυο, παρουσιάζεται η ανάγκη για την εμπλοκή στη διαδικασία περισσότερων οντοτήτων (π.χ. στην περίπτωση μιας εμπορικής συναλλαγής, του αγοραστή, του εμπόρου, της Αρχής Χρονοσφράγισης). Αυτό σημαίνει ότι θα πρέπει να διασφαλίζεται σε κάθε περίπτωση, ότι οι εμπλεκόμενοι θα πρέπει να συμφωνούν και να δεσμεύονται στην ίδια συμφωνία, προτού αυτή χρονοσφραγηθεί, όπως φαίνεται στο ακόλουθο σχήμα:



Σχήμα 3-2: Χρονοσφράγιση σε ηλεκτρονική συναλλαγή

Το πρόβλημα αυτό μελετήθηκε και σχεδιάστηκε ένα νέο σχήμα επικοινωνίας, κάνοντας όμως χρήση του υπάρχοντος πρωτοκόλλου χρονοσφράγισης προκειμένου να διασφαλιστεί η διαλειτουργικότητα της λύσης. Η λύση βασίστηκε σε XML για την προδιαγραφή των απαραίτητων μηνυμάτων που θα ανταλλαχθούν και σε κρυπτογραφία XML για την προστασία των μηνυμάτων απο τους εμπλεκόμενους φορείς προκειμένου να διασφαλιστεί η μη-άρνηση συμμετοχής τους στη συναλλαγή. Κατόπιν της εξασφάλισης της συμφωνίας ένα συνδυασμένο έγγραφο παράγεται και αποστέλλεται στην Αρχή Χρονοσφράγισης και το αποτέλεσμα επιστρέφεται στους εμπλεκόμενους φορείς προς φύλαξη.
Στα πλαίσια του προγράμματος "TSEC – Time stamping in e-Commerce" (ISIS 503166) ο Υ.Δ. συμμετείχε στην προδιαγραφή του νέου αυτού σχήματος χρονοσφράγισης. Το νέο πρωτόκολλο επικοινωνίας ενσωματώθηκε στο λογισμικό ενός υπάρχοντος συστήματος ηλεκτρονικού εμπορίου (ηλεκτρονικό κατάστημα). Πιο συγκεκριμένα, ο Υ.Δ. μελέτησε διαφορετικά σχήματα επικοινωνιών προκειμένου να επιτυγχάνεται η απαίτηση εξασφάλισης των δικαιωμάτων όλων των οντοτήτων. Αφού συμφωνήθηκε το σχήμα απο την ομάδα του έργου, ο Υ.Δ. σχεδίασε την δομή σε XML των μηνυμάτων που ανταλλάσσονται μεταξύ της εφαρμογής του πελάτη και του εξυπηρετητή του πωλητή και ανάμεσα στον εξυπηρετητή του πωλητή και την καινούργια οντότητα που αναλαμβάνει να επικοινωνήσει με την Αρχή Χρονοσφράγισης [Sklavos01]. Στη συνέχεια σχεδίασε και υλοποίησε τους μηχανισμούς εφαρμογής ψηφιακών υπογραφών XML και κρυπτογράφησης XML για τα μηνύματα αυτά. Επίσης διαμόρφωσε ανάλογα το ήδη υπάρχον πρωτόκολλο επικοινωνίας μεταξύ της εφαρμογής πελάτη και του εξυπηρετητή του πωλητή ώστε να είναι συμβατό με το καινούργιο πρωτόκολλο βασισμένο στην XML και την Χρονοσφράγιση.

3.1.2 Αναβαθμισμένη υπηρεσία ασφαλούς η-ταχυδρομείου

3.1.2.1 Υπάρχουσα κατάσταση

Ο συνηθισμένος τρόπος ανταλλαγής ψηφιακών δεδομένων σήμερα είναι το ηλεκτρονικό ταχυδρομείο. Όμως το πρωτόκολλο ασφάλειας στο ηλεκτρονικό ταχυδρομείο (S/MIME) δεν επιτρέπει την υπογραφή ενός συγκεκριμένου εγγράφου, παρά μόνο την υπογραφή του ηλεκτρονικού «γράμματος» στο σύνολό του.

3.1.2.2 Δημιουργία μεμονωμένων υπογεγραμμένων μηνυμάτων στο ασφαλές η-ταχυδρομείο

Προκειμένου να αντιμετωπιστεί η παραπάνω αδυναμία του S/MIME, ο Υ.Δ. προχώρησε στην αποτύπωση μιας αρχιτεκτονικής ενσωμάτωσης της απαραίτητης λειτουργικότητας σε εφαρμογές ανταλλαγής ηλεκτρονικών μηνυμάτων ώστε να μπορούν να παράγουν μεμονωμένα υπογεγραμμένα ηλεκτρονικά μηνύματα είτε σε δυαδική μορφή βάσει του PKCS#7 ή στην κρυπτογραφία XML. Η αρχιτεκτονική συνδυάζει ένα υπάρχον πρωτόκολλο επικοινωνίας όπως είναι το S/MIME, με τις ψηφιακές υπογραφές XML, αποθηκευτικά μέσα αναγνωριστικών (π.χ. έξυπνες κάρτες) και τις βασικές υπηρεσίες ΥΔΚ όπως είναι η εγγραφή και ο έλεγχος της εγκυρότητας πιστοποιητικών και υπογραφών καθώς και η χρονοσφράγιση.

Υπάρχουσες εφαρμογές η-ταχυδρομείου θα μπορούν να κάνουν χρήση του σχήματος με την εξωτερική υποστήριξη απο κάποια εφαρμογή παραγωγής υπογραφών ή κάποιο plug-in. Θα δίνουν όμως έτσι τη δυνατότητα σε οποιονδήποτε να υπογράφει κάθε είδος εγγράφου βάσει αναγνωρισμένων προτύπων και που θα είναι ανεξάρτητη του πρωτοκόλλου μεταφοράς του εγγράφου (ηλεκτρονικό ταχυδρομείο, FTP κλπ.).
Ο Υ.Δ. υλοποίησε μιας βιβλιοθήκη (και αντίστοιχη εφαρμογή που την χρησιμοποιεί) για υπογραφή μεμονωμένων εγγράφων, βασισμένη στην παραπάνω αρχιτεκτονική, ως συνοδευτική οποιασδήποτε εφαρμογής μεταφοράς ηλεκτρονικών εγγράφων, όπως το e-mail. Η βιβλιοθήκη θα μπορούσε να ενσωματωθεί στη λειτουργικότητα της εφαρμογής μεταφοράς για περισσότερη διαφάνεια. Η εφαρμογή με τη βιβλιοθήκη χρησιμοποιήθηκαν στα πλαίσια ενός ερευνητικού προγράμματος η-διακυβέρνησης (βλ. παράγραφο 3.2.2).

3.1.3 Υπογραφές XML στην λύση του προβλήματος «Κρυφής προώθησης»

3.1.3.1 Υπάρχουσα Κατάσταση

Στην βιβλιογραφία [Davis01] περιγράφεται το πρόβλημα «κρυφής προώθησης» (surreptitious forwarding) το οποίο είναι μια αδυναμία του πρωτοκόλλου S/MIME για την ανταλλαγή ασφαλούς ηλεκτρονικού ταχυδρομείου, παρά την εφαρμογή ψηφιακών υπογραφών και κρυπτογράφησης σε ένα μήνυμα. Το πρόβλημα μπορεί να συνοψιστεί στα εξής: ένας κακόβουλος χρήστης μπορεί να οδηγήσει τον παραλήπτη ενός μηνύματος να πιστέψει ότι το έχει λάβει απο κάποιον άλλον ή να τον πείσει ότι για ένα μήνυμα αυτός ήταν όντως ο παραλήπτης ενώ ο αποστολέας του το προόριζε για κάποιον άλλο.
Για μια πιο λεπτομερή παρουσίαση του προβλήματος, θεωρούμε ότι έχουμε τρεις χρήστες που επικοινωνούν με ηλεκτρονικό ταχυδρομείο, τους Α, Β, Γ. Όταν ο Α υπογράφει ένα μήνυμα, το αναπαριστούμε με ένα μικρό «α» δίπλα στο μήνυμα π.χ. $\{«\text{μήνυμα}»\}^{\alpha}$, ενώ όταν κρυπτογραφεί ένα μήνυμα το αναπαριστούμε με κεφαλαίο γράμμα του παραλήπτη του μηνύματος π.χ. $\{«\text{μήνυμα}»\}^{B}$ αν ο παραλήπτης είναι ο Β. Αντίστοιχο συμβολισμό θεωρούμε για τους Β και Γ. Η περιγραφή που ακολουθεί θεωρεί ότι χρησιμοποιούμε είτε τεχνική Υπογραφής και Κρυπτογράφησης (Sign & Encrypt) ή Κρυπτογράφησης και Υπογραφής (Encrypt & Sign), όπως συμβαίνει με τις περισσότερες εφαρμογές ηλεκτρονικού ταχυδρομείου σήμερα.
Στην πρώτη περίπτωση, ο Α υπογράφει και κρυπτογραφεί ένα μήνυμα για τον Β, αλλά ο Β επανακρυπτογραφεί το υπογεγραμμένο μήνυμα για τον Γ. Στο τέλος, ο Γ πιστεύει ότι ο Α του έστειλε απ' ευθείας το μήνυμα, και δεν μπορεί να εντοπίσει την ενδιάμεση παρέμβαση του Β. Ο Β θα μπορούσε να το κάνει αυτό για να φέρει σε δύσκολη θέση τον Α, τον Γ ή και τους δύο:

$A \rightarrow B \{ \{ «\text{άκρως απόρρητη πληροφορία}» \}^{\alpha} \}^{B}$

$B \rightarrow \Gamma \{ \{ «\text{άκρως απόρρητη πληροφορία}» \}^{\alpha} \}^{\Gamma}$

Στην περίπτωση αυτή ο Β έχει οδηγήσει τον Γ να πιστέψει ότι ο Α έστειλε ένα μήνυμα σ' αυτόν. Ο Α θα μπορούσε π.χ. να κατηγορηθεί για την αποκάλυψη μιας πολύ σημαντικής πληροφορίας.
Στην δεύτερη περίπτωση ο Α θέλει να στείλει ένα μήνυμα στον Β, αλλά ο Γ υποκλέπτει αυτό το μήνυμα. Ο Γ τώρα μπορεί να στείλει εκείνος το μήνυμα στον Β, χωρίς ο Β να

μπορεί να καταλάβει ότι το έχει στείλει ο Γ, και άρα ο Γ θεωρείται υπεύθυνος για την αποστολή του.
Αρχικό μήνυμα (που δεν φτάνει στον Β): $A \rightarrow B \{ \{ «η ιδέα μου» \}^{B} \}^{\alpha}$
Τελικό μήνυμα που φτάνει στον Β: $\Gamma \rightarrow \{ \{ «η ιδέα μου» \}^{B} \}^{\gamma}$
Ο Γ ενδέχεται να μην μπορεί καν να αποκρυπτογραφήσει το μήνυμα. Υπογράφει το κρυπτογραφημένο μήνυμα, οτιδήποτε και αν είναι αυτό.

3.1.3.2 Εφαρμογή XML στο ηλεκτρονικό ταχυδρομείο

Η μελέτη του προβλήματος οδήγησε στην λύση της εφαρμογής κρυπτογραφίας XML (ψηφιακές υπογραφές και κρυπτογράφηση) σε συνδυασμό με την κατάλληλη προδιαγραφή της δομής ενός μηνύματος ηλεκτρονικού ταχυδρομείου σε XML.
Ο Υ.Δ. συμμετείχε στη σχεδίαση και υλοποίηση μια πρότυπης εφαρμογής ηλεκτρονικού ταχυδρομείου βασισμένη στην XML. Η εργασία αυτή έγινε στα πλαίσια των μεταπτυχιακών μαθημάτων «Δίκτυα προστιθέμενης αξίας EDI και εφαρμογές ηλεκτρονικού εμπορίου» και «Αντικειμενοστρεφείς μεθοδολογίες ανάπτυξης λογισμικού». Πιο συγκεκριμένα, κατόπιν λήψης της απόφασης για τον πιο ενδεδειγμένο τρόπο λύσης του παραπάνω προβλήματος, ο Υ.Δ. έκανε τον συνολικό σχεδιασμό σε UML της εφαρμογής ηλεκτρονικού ταχυδρομείου (αρχιτεκτονική, διαγράμματα κλάσεων, δομικά στοιχεία και συσχετισμός τους, διαγράμματα ακολουθιών) και το μεγαλύτερο μέρος της υλοποίησης που περιελάμβανε κυρίως την διεπαφή με τον χρήστη, τον μηχανισμό χρήσης έξυπνης κάρτας, τους μηχανισμούς υπογραφών XML και της κρυπτογράφησης.

3.2 Προηγμένες υπηρεσίες η-επιχειρείν

Το παρόν κεφάλαιο καλύπτει ερευνητικές δραστηριότητες που έχουν να κάνουν με την δημιουργία ασφαλών υπηρεσιών σε διάφορους τομείς του η-επιχειρείν, οι οποίες συνδυάζουν της τεχνολογίες του παραρτήματος Ι, προκειμένου να επιτύχουν ασφαλώς συγκεκριμένους επιχειρηματικούς στόχους.

3.2.1 Ασφαλείς υπηρεσίες η-υγείας

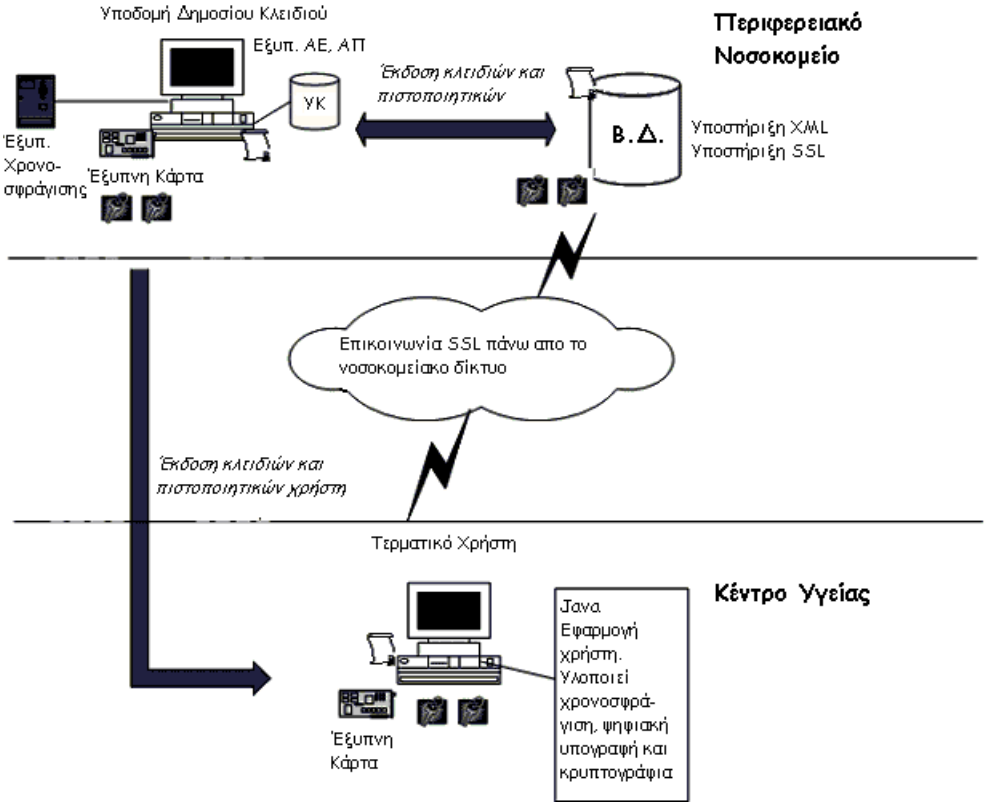
3.2.1.1 Υπάρχουσα κατάσταση

Μια ΥΔΚ είναι ένα πλαίσιο ασφάλειας, παρά μια τεχνική λύση, άρα η ασφάλεια που βασίζεται σε ΥΔΚ περιλαμβάνει αρκετές παραμέτρους που πρέπει να ληφθούν υπόψην για την ομαλή και επιτυχημένη ενσωμάτωση των υπηρεσιών του σε υπάρχοντα πληροφορικά δίκτυα σχετιζόμενα με τον τομέα της ιατρικής φροντίδας. Τέτοιες παράμετροι αφορούν: την τεχνική ενσωμάτωση μηχανισμών ασφάλειας ΥΔΚ σε ιατρικές εφαρμογές, την οργανωτική αναδόμηση πολιτικών, την εναρμόνιση με το νομικό πλαίσιο, την συμμετοχή του ιατρικού προσωπικού, καθώς και την εξασφάλιση της κατάλληλης επιχειρησιακής ροής πληροφοριών.
Παρόλο που οι τεχνικές υπηρεσίες ΥΔΚ όπως η Πιστοποίηση, η Εγγραφή, η Χρονοσφράγιση υλοποιούνται επαρκώς, οι παραπάνω παράμετροι στο σύνολό τους συνήθως αγνοούνται, παραλείπονται ή υποτιμώνται, οδηγώντας σε έλλειψη ολοκληρωμένων υπηρεσιών ΥΔΚ ή στην αδυναμία πραγματικής χρήσης τους στο ιατρικό περιβάλλον. Αυτό έχει σημαντικές επιπτώσεις στην ασφάλεια και αξιοπιστία του

πληροφοριακού συστήματος (Π.Σ.), κάτι που μειώνει την ποιότητα των προσφερόμενων υπηρεσιών.

3.2.1.2 Εφαρμογή υπηρεσιών ΥΔΚ και ασφάλειας XML στην Υγεία

Ο Υ.Δ. συμμετείχε στην έρευνα των επιπτώσεων των προαναφερθέντων παραμέτρων στην λειτουργία μια ΥΔΚ σε ιατρικό περιβάλλον ως μέρος του ερευνητικού Ευρωπαϊκού προγράμματος "RESHEN – Regional Secure Health Networks" (IST 2001-25354). Σχηματικά υλοποιημένη η υποδομή του πληροφοριακού συστήματος αναπαρίσταται στο επόμενο σχήμα:



Σχήμα 3-3: Π.Σ. σε ιατρικό περιβάλλον με χρήση υπηρεσιών ΥΔΚ

Στο έργο μελετήθηκαν και καταγράφηκαν οι ειδικές απαιτήσεις ασφάλειας ενός σύγχρονου Π.Σ. στον τομέα της υγείας. Κατόπιν άμεσης επαφής με ιατρικό προσωπικό, αναγνωρίστηκε το ανοιχτό πρόβλημα της ανάγκης για έγκυρη εξουσιοδότηση του ιατρικού προσωπικού στις εφαρμογές του Π.Σ. βάσει ελέγχου αυθεντικότητας έτσι ώστε να αποφευχθούν για παράδειγμα περιπτώσεις παράνομης έκδοσης ψηφιακών ιατρικών εγγράφων. Ως σημαντική επίσης αναγνωρίστηκε η εξασφάλιση της ακεραιότητας και εμπιστευτικότητας των ευαίσθητων ιατρικών δεδομένων τα οποία καλύπτονται απο ισχυρό νομικό πλαίσιο. Προκειμένου να καλυφθούν οι απαιτήσεις σχεδιάστηκε και υλοποιήθηκε εφαρμογή διακίνησης ηλεκτρονικών παραπεμπτικών και συνταγών χρησιμοποιώντας με αποδοτικό τρόπο την XML, υπηρεσίες μιας ΥΔΚ και έξυπνες κάρτες [Bourka03a].

Η *οργάνωση* της ΥΔΚ έγινε με βάση τις υπάρχουσες χρήσεις του δικτύου και περιελάμβανε την τεκμηρίωση μια Πολιτικής Εφαρμογής (application policy) για το κομμάτι της επιχειρηματικής ροής της παραπάνω υπηρεσίας διακίνησης η-εγγράφων.
Απο νομική σκοπιά, το Π.Σ. θα έπρεπε να εναρμονίζεται με το νομικό πλαίσιο και την εθνική νομοθεσία περί προστασίας προσωπικών δεδομένων και την Ευρωπαϊκή οδηγία για ψηφιακές υπογραφές. Οι απαιτήσεις αυτές λήφθηκαν υπόψην με τη χρήση των κατάλληλων μηχανισμών ασφάλειας στην επικοινωνία και την αποθήκευση, όσο ήταν δυνατόν. Η οδηγία περί ψηφιακών υπογραφών, αν είχε ήδη ενσωματωθεί στην Ελληνική νομοθεσία, την χρονική στιγμή υλοποίησης της υποδομής δεν υπήρχαν ακόμη οι απαραίτητες προδιαγραφές για έναν πλαίσιο διαπίστευσης στο Ελληνικό κράτος και δεν είχε οριστεί το καθεστώς που διέπει την εγκατάσταση και λειτουργία μιας Αρχής Πιστοποίησης.
Όσον αφορά στην συμμετοχή του ιατρικού προσωπικού, πραγματοποιήθηκε εκπαίδευση στις βασικές αρχές ασφάλειας του ισχύοντος θεσμικού και οργανωτικού πλαισίου, καθώς επίσης και στην χρήση των εφαρμογών η-παραπεμπτικών. Στη συνέχεια, διενεργήθηκε μια έρευνα βάσει ερωτηματολογίων και εξάχθηκαν συμπεράσματα σχετικά με την αποδοχή των ασφαλών ιατρικών εφαρμογών απο το προσωπικό. Τελικό συμπέρασμα ήταν ότι ενδεικτικά βήματα για την περαιτέρω ανάπτυξη στον τομέα περιλαμβάνουν την εμπλοκή του ιατρικού προσωπικού κατά το στάδιο της σχεδίασης, την συμμετοχή ειδικών σε θέματα υγείας μέσα στις συμβουλευτικές διαδικασίες και την εκπαίδευση και την παροχή ώριμων και τεχνικά ρεαλιστικών οργανωτικών σχημάτων [Bourka03b, Georgoulas03].
Στην παραπάνω λύση, ο Υ.Δ. συμμετείχε στις φάσεις της συλλογής απαιτήσεων, σχεδιασμού και υλοποίησης της ΥΔΚ και των εφαρμογών που την χρησιμοποιούν καθώς και της παρουσίασής τους στο ιατρικό προσωπικό ενός νοσοκομείου. Πιο συγκεκριμένα, σε επίπεδο υλοποίησης ανέλαβε το υπο-κομμάτι του σχεδιασμού σε UML της αρχιτεκτονικής της εφαρμογής η-παραπεμπτικών, που ήταν σχετικό με τους μηχανισμούς ασφάλειας (ψηφιακές υπογραφές XML και κρυπτογράφηση, Χρονοσφράγιση). Επίσης συνέβαλλε στην υλοποίηση των αντίστοιχων δομικών μονάδων της εφαρμογής.
Σε οργανωτικό επίπεδο, υλοποίησε και παραμετροποίησε ένα υπο-κομμάτι της ΥΔΚ (αρχιτεκτονική υποδομής, τύποι πιστοποιητικών, δικτυακή υποδομή) και ανέλαβε την προδιαγραφή των πολιτικών εφαρμογών. Επίσης ανέλαβε την οργάνωση ενός μέρους της διεξαγωγής της διαδικασίας αξιολόγησης (οργάνωση ερωτηματολογίων, επαφή με το ιατρικό προσωπικό).

3.2.2 Ασφαλείς υπηρεσίες η-διακυβέρνησης

3.2.2.1 Υπάρχουσα κατάσταση

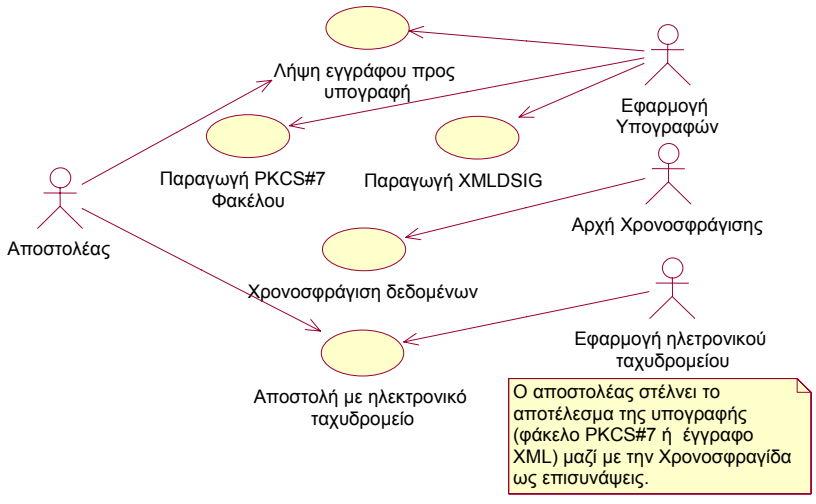
Η εφαρμογή ψηφιακών υπογραφών XML στην ηλεκτρονική διακυβέρνηση παρουσιάζει δυσκολίες λόγω της μικρής τριβής του προσωπικού των εμπλεκόμενων φορέων με τις νέες τεχνολογίες και την ασφάλεια. Παράλληλα, οι περισσότερες διαδικασίες σε δημόσιους οργανισμούς περιλαμβάνουν την διακίνηση εγγράφων που πρέπει να φέρουν υπογραφές, άρα και οι αντίστοιχες ψηφιακές αναπαραστάσεις τους θα πρέπει να φέρουν ψηφιακές υπογραφές. Ο συνηθισμένος τρόπος ανταλλαγής ψηφιακών δεδομένων στην ηλεκτρονική διακυβέρνηση σήμερα είναι το ηλεκτρονικό ταχυδρομείο. Συνεπώς ήταν απαραίτητο να ληφθεί υπόψην το πρόβλημα που αναφέρθηκε στην παράγραφο 3.1.2.

3.2.2.2 Εφαρμογή υπηρεσιών ΥΔΚ και ψηφιακών υπογραφών XML στην η διακυβέρνηση

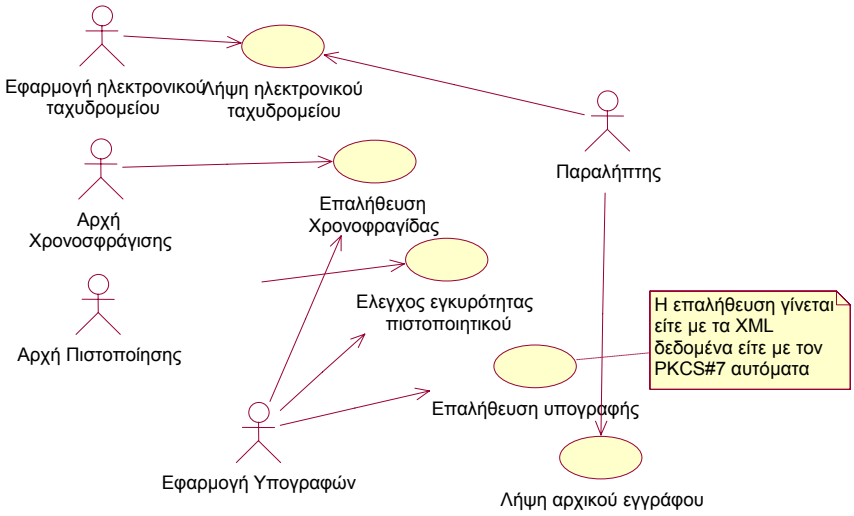
Το προαναφερθέν πρόβλημα ήταν εμφανές και στην περίπτωση του ερευνητικού έργου "La Mer – (IST-2001-33162)", όπου μελετήθηκε η συνολική υλοποίηση μιας ΥΔΚ βασισμένης σε έξυπνες κάρτες για την κάλυψη των αναγκών ασφάλειας Ευρωπαϊκών εμπορικών επιμελητηρίων. Στα πλαίσια του έργου ο Υ.Δ. συμμετείχε στην οργάνωση της ΥΔΚ και πιλοτική υποστήριξη ενός επιμελητηρίου.

Προκειμένου να αντιμετωπιστεί η παραπάνω αδυναμία του S/MIME, ο Υ.Δ. προχώρησε στο σχεδιασμό και υλοποίηση μιας απλής εφαρμογής που έκανε χρήση της βιβλιοθήκης της παραγράφου 3.1.2 και δίνει σε οποιονδήποτε τη δυνατότητα να υπογράφει κάθε είδος εγγράφου βάσει αναγνωρισμένων προτύπων. Έτσι, η εφαρμογή καθίσταται ανεξάρτητη του πρωτοκόλλου μεταφοράς του εγγράφου (ηλεκτρονικό ταχυδρομείο, FTP κλπ.). Πιο συγκεκριμένα η εφαρμογή παράγει ψηφιακές υπογραφές με χρήση δύο προτύπων: ψηφιακές υπογραφές XML για δεδομένα σε μορφή XML και υπογραφές με μια υλοποίηση του προτύπου PKCS#7 για οποιοδήποτε άλλο τύπο εγγράφου. Η εφαρμογή κάνει χρήση του προτύπου PKCS#11 για επικοινωνία με μια έξυπνη κάρτα, προκειμένου να έχει πρόσβαση στα κλειδιά του χρήστη και να υλοποιήσει το κρυπτογραφικό κομμάτι της διαδικασίας (υπογραφές RSA). Επίσης, έχει την δυνατότητα online πρόσβασης σε Λίστες Ανάκλησης Πιστοποιητικών, για να αποφανθεί αν οι υπογραφές που ελέγχει έχουν δημιουργηθεί με κλειδιά που αντιστοιχούν σε έγκυρα ψηφιακά πιστοποιητικά X509 και ενσωματώνει στο συνολικό μήνυμα την ψηφιακή αναπαράσταση μιας χρονοσφραγίδας [Karantjias03].

Η εφαρμογή παραγωγής υπογραφών είχε στόχο να εξοικειώσει το προσωπικό των επιμελητηρίων με τις ηλεκτρονικές υπογραφές και σημαντική παράμετρος κατά το σχεδιασμό ήταν η ευκολία στη χρήση και η απλότητα σε συνδυασμό με την απόδοση. Μέσα στο πρόγραμμα έγινε χρήση της εφαρμογής σε συνδυασμό με μια υπηρεσία χρονοσφράγισης και το ηλεκτρονικό ταχυδρομείο για την αποστολή υπογεγραμμένων εγγράφων ανάμεσα στα επιμελητήρια βάσει του σεναρίου που αναπαρίσταται στα ακόλουθα διαγράμματα χρήσης:



Σχήμα 3-4: Διάγραμμα χρήσης της εφαρμογής ηλεκτρονικών υπογραφών από τον αποστολέα



Σχήμα 3-5: Διάγραμμα χρήσης της εφαρμογής ηλεκτρονικών υπογραφών από τον παραλήπτη

Αποτελέσματα της εργασίας αυτής και μια συγκριτική μελέτη στην απόδοση των δύο μηχανισμών υπογραφής για διάφορα μεγέθη ψηφιακών εγγράφων παρουσιάζονται στις [Karantjias04].

3.2.3 Ψηφιακές υπογραφές XML στο η-εμπόριο

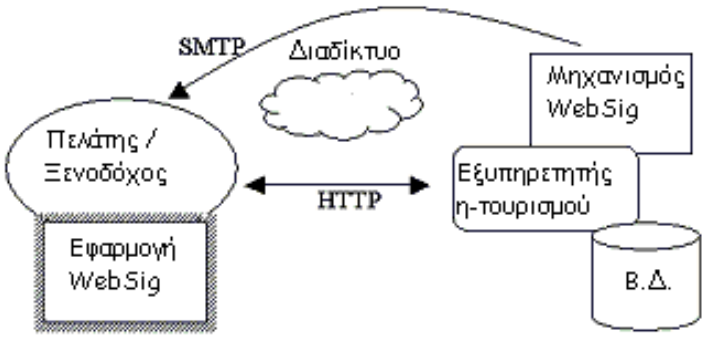
3.2.3.1 Υπάρχουσα κατάσταση

Στη φάση που οι ψηφιακές υπογραφές XML βάσει του προτύπου XML-DSIG ήταν ακόμη σε στάδιο προτυποποίησης, μελετήθηκε η εφαρμογή τους σε ένα τουριστικό σύστημα έκδοσης ψηφιακών αποδείξεων κρατήσεων (voucher). Το πρόβλημα ήταν η βελτίωση της αξιοπιστίας των συναλλαγών με το σύστημα. Η λύση που δόθηκε και παρουσιάζεται στην [Sklavos03] χρησιμοποιεί τις ψηφιακές υπογραφές XML προκειμένου να λάβουν οι εμπλεκόμενοι μια υπογεγραμμένη ψηφιακή απόδειξη.

3.2.3.2 Προτυποποίηση και εφαρμογή ψηφιακών υπογραφών XML

Η μελέτη έγινε στα πλαίσια του ευρωπαϊκού έργου “WebSig – Digital Signatures for Web Contents” (ISIS I4-06). Το έργο είχε ως στόχο την παραγωγή μιας βιβλιοθήκης παραγωγής και επαλήθευσης υπογραφών XML που να συμμορφώνεται με την τρέχουσα έκδοση του προτύπου.

Ο Υ.Δ. συμμετείχε στο σχεδιασμό της λύσης για την πλευρά του τουριστικού συστήματος και την υλοποίησή που περιλάμβανε τον προκαθορισμό μιας κατάλληλης μορφής ψηφιακής απόδειξης, την ενσωμάτωση των συναρτήσεων της βιβλιοθήκης στην διαδικασία έκδοσης των αποδείξεων καθώς και μιας απλής εφαρμογής για επαλήθευση των στοιχείων των υπογραφών. Η αρχιτεκτονική παρουσιάζεται στο ακόλουθο σχήμα:



Σχήμα 3.6: Αρχιτεκτονική συστήματος έκδοσης αποδείξεων

Η αρχιτεκτονική βασίστηκε σε ένα ήδη υπάρχον σύστημα για ηλεκτρονικές κρατήσεις ξενοδοχείων. Τα νέα στοιχεία που υλοποιήθηκαν, ενσωματώθηκαν διαφανώς στην υποδομή αυτή και ο τελικός χρήστης απλά έπρεπε να χρησιμοποιήσει την επιπλέον επιλογή για λήψη μιας ψηφιακής απόδειξης συναλλαγής. Όταν έκανε την επιλογή αυτή, η αντίστοιχη υπηρεσία στον εξυπηρετητή εφαρμογών αυτόματα παρήγαγε μια ψηφιακή απόδειξη σε XML με τα στοιχεία της κράτησης, την υπέγραφε και έκανε αποστολή στον χρήστη και τον αντιπρόσωπο του καταλύματος με ηλεκτρονικό ταχυδρομείο.
Με την λήψη της απόδειξης αυτής, ο χρήστης μπορούσε να τη σώσει σε μια δισκέτα ή CD και να την έχει μαζί του στην παρουσία του στο ξενοδοχείο. Εκεί ο αντίστοιχος υπάλληλος θα χρησιμοποιούσε την εφαρμογή που του έχει δοθεί για να επαληθεύσει τα στοιχεία της κράτησης και την υπογραφή πάνω τους.
Πιο συγκεκριμένα, η συμβολή του Υ.Δ. ήταν ο σχεδιασμός και η υλοποίηση όλου του μηχανισμού εφαρμογής των υπογραφών στον εξυπηρετητή του συστήματος, καθώς και της εφαρμογής επαλήθευσης ηλεκτρονικών υπογραφών για τους πελάτες / ξενοδόχους.

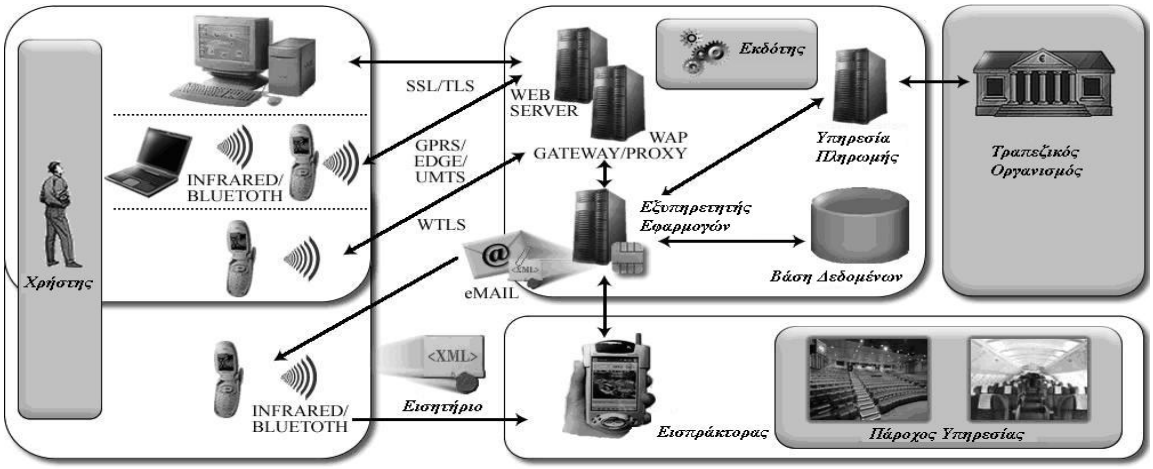
3.2.4 Ασφαλής υπηρεσία έκδοσης ηλεκτρονικών εισιτηρίων

3.2.4.1 Υπάρχουσα κατάσταση

Η έκδοση εισιτηρίων αποτελεί μια καθημερινή ανθρώπινη δραστηριότητα κυρίως στον τομέα των μεταφορών για συγκοινωνιακά μέσα, καθώς και για την είσοδο σε πολιτιστικά δρώμενα και τόπους διασκέδασης. Σε παγκόσμιο επίπεδο μελετώνται τρόποι μετάβασης σε ηλεκτρονικά ανάλογα υπηρεσιών έκδοσης ηλεκτρονικών εισιτηρίων, με έμφαση σε ασύρματα μέσα, λόγω της ευκολίας χρήσης που παρουσιάζουν.
Ο Υ.Δ. μελέτησε τις απαιτήσεις ενός συστήματος έκδοσης ηλεκτρονικών εισιτηρίων, απ' όπου έγινε φανερό ότι σε υπάρχουσες λύσεις υπάρχει αδυναμία πλήρους κάλυψης των δικαιωμάτων του χρήστη που λαμβάνει το εισιτήριο, ο οποίος δεν κρατά στα χέρια του ένα ηλεκτρονικό έγγραφο που να τον κατοχυρώνει νομικά, παρά μόνο έναν αριθμό ή έναν κωδικό.

3.2.4.2 Ασφαλής υπηρεσία έκδοσης ηλεκτρονικών εισιτηρίων

Στην [Mavroudis03] παρουσιάζεται μια αρχιτεκτονική ενός συστήματος ασφαλούς έκδοσης ηλεκτρονικών εισιτηρίων βασισμένη σε κρυπτογραφία XML για την πλήρη ψηφιοποίηση μιας τέτοιας υπηρεσίας.
Μια αναπαράσταση της αρχιτεκτονικής φαίνεται στο ακόλουθο σχήμα:



Σχήμα 3-6: Αρχιτεκτονική έκδοσης η-εισιτηρίων

Η έμφαση δόθηκε στην κάλυψη της ανάγκης του χρήστη να έχει ένα κρυπτογραφικά ενισχυμένο αποδεικτικό στοιχείο ως εισιτήριο, κάνοντας παράλληλα χρήση τεχνολογιών φιλικών και εύκολων προς αυτόν, όπως για παράδειγμα το κινητό του τηλέφωνο ως μέσο φύλαξης του ψηφιακού εισιτηρίου.
Ο Υ.Δ. στην εργασία αυτή μελέτησε τις απαιτήσεις ασφάλειας του συστήματος και πρότεινε τους κατάλληλους μηχανισμούς βασισμένους σε XML και ΥΔΚ για την ασφαλή δημιουργία , μεταφορά και επικύρωση του ηλεκτρονικού εισιτηρίου σε όλο τον κύκλο ζωής του.

3.3 Συμπεράσματα

Η εμπειρία των ερευνητικών εργασιών του παρόντος κεφαλαίου, οδήγησε στο συμπέρασμα ότι η ασφάλεια αποτελεί έναν στόχο άρρηκτα δεμένο με την λειτουργία επιχειρησιακών δραστηριοτήτων, που όμως είτε υποστηρίζεται ελλιπώς απο τα πρότυπα που υπάρχουν, είτε όταν υποστηρίζεται αποτελεί μεμονωμένη λύση σε συγκεκριμένα προβλήματα.
Στην περίπτωση των Υπηρεσιών Ιστού, και των αρχιτεκτονικών υπηρεσιών που αποτελούν την λογική συνέχεια ολοκλήρωσης Υπηρεσιών Ιστού για την πλήρη αναπαράσταση επιχειρησιακών υπηρεσιών με τεχνικά μέσα, είναι απαραίτητο οι αρχές ασφάλειας και διαλειτουργικότητας να εφαρμόζονται καθ' όλη την διάρκεια σχεδιασμού συστημάτων λογισμικού.
Οι ερευνητικές εργασίες που παρουσιάστηκαν και η μελέτη της σχετικής βιβλιογραφίας αποδεικνύουν ότι υπάρχει η ανάγκη για μια πιο συστηματική και ολιστική μέθοδο σχεδιασμού και υλοποίησης αρχιτεκτονικών υπηρεσιών, ώστε αυτές να βασίζονται σε ευρέως διαδεδομένα πρότυπα, ιδέες και αρχές και να ενσωματώνουν σε διακριτά βήματα τους απαραίτητους μηχανισμούς και υπηρεσίες ασφάλειας, ως ενιαίο σύνολο που απο τη μια καλύπτει τις απαιτήσεις ασφάλειας, και απο την άλλη αποτελεί φυσική και κατανοητή επέκταση των επιχειρησιακών διεργασιών που υλοποιούνται απο την άποψη των οντοτήτων που συμμετέχουν.

Μια τέτοια κατασκευαστική μέθοδος αποτελεί τον 3ο βασικό άξονα της διατριβής και παρουσιάζεται αναλυτικά στο επόμενο κεφάλαιο.

3.4 Αναφορές

[Bourka03a] A. Bourka et al. (2003). "Enriching healthcare applications with cryptographic mechanisms and XML-based security services", Technology and Healthcare, IOS Press, Issue 1, Vol. 11, pp. 61-76

[Bourka03b] A. Bourka et al. (2003). "PKI-based security of electronic healthcare documents", SSGRR 2003 Winter Conference, L'Aquilla, Italy

[Davis01] D.T. Davis. (2001). "Defective Sign & Encrypt in S/MIME, PKCS#7, MOSS, PEM, PGP, and XML.", proceedings of Usenix Tech. Conferenece 2001 *(Boston, Mass., June 25-30, 2001)*

[Georgoulas03] A. Georgoulas et al. (2003). "RESHEN, a best practice approach for secure healthcare networks in Europe", Advanced Health Telematics and Telemedicine - The Magdeburg Expert Summit Textbook, Vol. 96 in the "Studies in Health Technology and Informatics", IOS Press.

[Karantjias03] A. Karantjias et al. (2003). "Secure Applications for the Chambers of Commerce", SSGRR 2003 Winter Conference, L'Aquilla, Italy

[Karantjias04] A. Karantjias et al. (2004). "Secure applications for the Chambers of Commerce: functionality and technical assessment", Proceedings of EUROSEC' 2004 15th Forum on Information Systems and Security, Paris

[Mavroudis03] I. Mavroudis et al. (2003). "A mobile and secure ticketing service", Proceedings of e-Challenges 2003 conference, Bologna, IOS Press, pp. 85-92

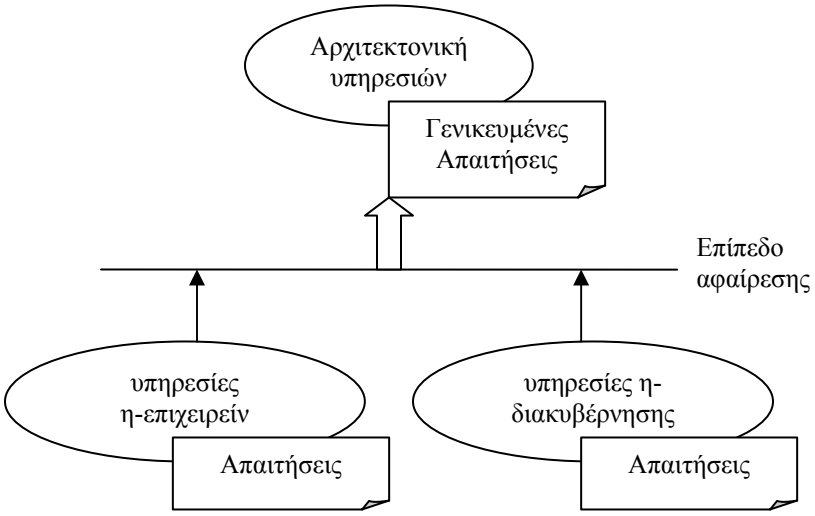
[Sklavos01] P. Sklavos et al. (2001). "Time stamping in e-commerce", Proceedings of E-Business E-work (EBEW 2001), Venice, IOS Press, pp. 546-552

[Sklavos03] P. Sklavos et al. (2003). "Applying XML Digital Signatures in electronic hotel reservations", SSGRR 2003 Winter Conference, L'Aquilla, Italy

4 Κατασκευαστική μέθοδος προδιαγραφής ασφαλών, διαλειτουργικών και ανοιχτών αρχιτεκτονικών υπηρεσιών

4.1 Εισαγωγή

Στους δύο πρώτους άξονες της διατριβής, έγινε μελέτη υπαρχουσών αρχιτεκτονικών υπηρεσιών και των υπηρεσιών που περιλαμβάνουν, απο την οποία έγινε φανερό ότι υπάρχουν κοινές απαιτήσεις απο συστήματα προσανατολισμένα στις υπηρεσίες, κυρίως όσον αφορά στη διαλειτουργικότητα και την ασφάλεια. Οι κοινές απαιτήσεις οδηγούν στο συμπέρασμα ότι μια γενίκευσή τους θα μπορούσε να καλύψει ένα ευρύτερο φάσμα αρχιτεκτονικών υπηρεσιών που έχουν ως κύριο στόχο την διεκπεραίωση η-συναλλαγών, όπως φαίνεται στο Σχήμα 4-1.



Σχήμα 4-1: Αφαίρεση γενικευμένων απαιτήσεων

Ως εκ τούτου, οι απαιτήσεις μπορούν να οδηγήσουν στην δημιουργία των προδιαγραφών μιας κατασκευαστικής μεθόδου σχεδιασμού αρχιτεκτονικών, που να μπορεί να χρησιμοποιηθεί για τον σχεδιασμό και την υλοποίηση ενός μεγάλου εύρους αντίστοιχων συστημάτων οριζόντια σε τομείς όπως η η-διακυβέρνηση, η-υγεία, η-εμπόριο κ.ο.κ. Η μέθοδος θα περιγράφει τα βήματα σχεδιασμού της αρχιτεκτονικής καθώς και τον τρόπο ορισμού των βασικών συνθετικών στοιχείων της. Επιπλέον, η μέθοδος θα ορίζει ένα σύνολο απο βασικές οντότητες ή στοιχεία τα οποία θα μπορούν να χρησιμοποιηθούν αυτούσια κατά τον σχεδιασμό μιας αρχιτεκτονικής, δίνοντας τη βάση της, ή να επεκταθούν κατάλληλα προκειμένου να καλυφθούν εξειδικευμένες απαιτήσεις ή πολιτικές της αρχιτεκτονικής.

Κύριο αντικείμενο του τρίτου άξονα λοιπόν της διατριβής είναι ανάπτυξη της παραπάνω μεθόδου με σκοπό την προδιαγραφή ασφαλών, διαλειτουργικών και ανοιχτών αρχιτεκτονικών υπηρεσιών. Η μεθοδολογία θα πρέπει να αντιμετωπίζει τις αδυναμίες που περιγράφηκαν στο δεύτερο κεφάλαιο και θα ευνοεί την ευέλικτη ενσωμάτωση επιχειρηματικών διεργασιών εντός μιας αρχιτεκτονικής.

Παρ' όλα αυτά, οι απαιτήσεις που προκύπτουν απο τους δύο πρώτους άξονες, δεν αρκούν απο μόνες τους για τις προδιαγραφές της μεθοδολογίας, αν αυτές δεν στηρίζονται σε ένα προτυποποιημένο πλαίσιο αναφοράς που να παρέχει ένα σύνολο αρχικών κανόνων και ορισμών. Η χρήση του πλαισίου αναφοράς κατά τον σχεδιασμό της κατασκευαστικής μεθόδου θα της προσθέσει αξία αν είναι αναγνωρισμένο απο την διεθνή επιστημονική κοινότητα. Το πλαίσιο αναφοράς που χρησιμοποιήθηκε στην διατριβή είναι το πρότυπο ISO/RM-ODP, σε συνδυασμό με την UML ως γλώσσα σημειογραφίας. Η UML επιλέχθηκε επειδή, όπως προκύπτει απο την βιβλιογραφία, είναι απο τη μια περισσότερο διαδεδομένη ως γλώσσα προδιαγραφής συστημάτων και απο την άλλη είναι ικανή να περιγράψει σε πολύ ικανοποιητικό βαθμό τις έννοιες και όψεις του RM-ODP.
Τα βήματα που ακολουθήθηκαν για την κατάρτιση των προδιαγραφών της μεθοδολογίας είναι τα ακόλουθα:

- ο ορισμός της έννοιας μιας ασφαλούς, διαλειτουργικής και ανοιχτής αρχιτεκτονικής υπηρεσιών και η αναλυτική καταγραφή των γενικευμένων απαιτήσεων την χαρακτηρίζουν.
- η προδιαγραφή της ίδιας της μεθοδολογίας, της οποίας ο σκελετός και η τεχνική περιγραφή παρουσιάζεται στο παρόν κεφάλαιο.

Μετά τη ολοκλήρωση της μεθοδολογίας, η δραστηριότητα του Άξονα 4 ήταν εφαρμογή της μεθοδολογίας για την παραγωγή των προδιαγραφών δύο επιχειρησιακών υπηρεσιών με αντικείμενο την υλοποίηση ηλεκτρονικών συναλλαγών μεταξύ φορέων σε πανευρωπαϊκό επίπεδο, όπως θα δούμε στο κεφάλαιο 5.

4.2 Επισκόπηση μεθοδολογίας

4.2.1 Βασικές έννοιες μεθοδολογίας

4.2.1.1 Ορισμός Ασφαλών, Διαλειτουργικών και Ανοιχτών Αρχιτεκτονικών Υπηρεσιών (ΑΔΑΑΥ)

Προκειμένου να γίνει κατανοητός ο στόχος της μεθοδολογίας, έπρεπε να οριστούν σαφώς τα είδη και τα χαρακτηριστικά των αρχιτεκτονικών που θα αποτελούν προϊόντα της.
Η εισαγωγή της διατριβής, παρουσίασε τον ορισμό της *Αρχιτεκτονικής προσανατολισμένης σε Υπηρεσίες (ΑΠΥ)* βάσει της βιβλιογραφίας. Όπως διαφαίνεται απο τον ορισμό, οι εφαρμογές που χρησιμοποιούν μια ΑΠΥ χτίζονται πάνω σε υπηρεσίες. Στην ΑΠΥ υπάρχουν τρία ιδεατά επίπεδα αφαίρεσης ξεκινώντας απο τις πιο στοιχειώδεις διεργασίες που επιτελούνται εντός της και ανεβαίνοντας προς τις πιο πολύπλοκες:

- *Λειτουργίες (operations)*: αποτελούν μεμονωμένες λογικές μονάδες εργασίας. Η εκτέλεση μιας λειτουργίας συνήθως προκαλεί την ανάγνωση, εγγραφή ή αλλαγή κάποιας αποθηκευμένης πληροφορίας. Οι λειτουργίες στην ΑΠΥ είναι άμεσα συγκρίσιμες με τις μεθόδους του αντικειμενοστρεφούς μοντέλου προγραμματισμού. Έχουν συγκεκριμένες, δομημένες διεπαφές και επιστρέφουν δομημένες απαντήσεις.

Η εκτέλεση μιας λειτουργίας μπορεί να εμπλέκει την κλήση άλλων επιμέρους λειτουργιών.

- *Υπηρεσίες (services)*: αναπαριστούν λογικές ομαδοποιήσεις λειτουργιών. Αποτελούν τη βασική ατομική έκφραση ενός επιχειρησιακού στόχου.
- *Επιχειρησιακές διεργασίες (business processes)*: αποτελούν ένα σύνολο πράξεων που επιτελούνται για την υλοποίηση μιας καλώς ορισμένης επιχειρηματικής δραστηριότητας. Οι επιχειρησιακές διεργασίες τυπικά εμπλέκουν την κλήση πολλαπλών υπηρεσιών.

Μια επιχειρησιακή διεργασία αποτελείται απο ένα σύνολο υπηρεσιών που εκτελούνται με μια συγκεκριμένη σειρά σύμφωνα με δεδομένους επιχειρησιακούς κανόνες και πολιτικές. Η σειριοποίηση, επιλογή και εκτέλεση των υπηρεσιών και κατά συνέπεια των λειτουργιών που αυτές περιέχουν ονομάζεται *συντονισμός (choreography)* [Peltz03].
Επεκτείνοντας τον παραπάνω ορισμό, μια *Ασφαλής, Διαλειτουργική και Ανοιχτή Αρχιτεκτονική Υπηρεσιών - ΑΔΑΑΥ*, αποτελεί μια αρχιτεκτονική βασισμένη στις αρχές των ΑΠΥ προκειμένου να επιτύχει την διαλειτουργικότητα και τους επιχειρηματικούς στόχους που καλείται να ικανοποιήσει, αλλά δίνει έμφαση και στις υπηρεσίες και μηχανισμούς ασφάλειας που πρέπει να ενσωματώνει, προκειμένου να καλύπτονται όλες οι βασικές απαιτήσεις ασφάλειας των στόχων αυτών.
Στη συνέχεια αποτυπώνονται και αναλύονται οι απαιτήσεις μιας ΑΔΑΑΥ όπως προκύπτουν απο την ανάλυση των γενικότερων απαιτήσεων οργανισμών που έχουν ως στόχο την υιοθέτηση τέτοιων αρχιτεκτονικών.

4.2.1.2 Απαιτήσεις ΑΔΑΑΥ

4.2.1.2.1 Διαλειτουργικότητα και κλιμάκωση

Η διαλειτουργικότητα είναι πρωταρχικός στόχος μιας ΑΔΑΑΥ, όπως και κάθε αρχιτεκτονικής που βασίζεται στο μοντέλο ΑΠΥ. Η έλλειψη διαλειτουργικότητας ανάμεσα σε αρχιτεκτονικές βασίζεται στην ανομοιογένεια των τεχνικών λύσεων που υιοθετούν και την υποδομή τους, όσο και στην έλλειψη καλά ορισμένων επιχειρηματικών δραστηριοτήτων που αυτές υποστηρίζουν.
Η διασύνδεση οργανισμών που χρησιμοποιούν διαφορετικές πλατφόρμες και συστήματα είναι ένα αρκετά δύσκολο πρόβλημα που απαιτεί την εύκολη αναγνώριση και δημοσίευση υποστηριζόμενων ηλεκτρονικών υπηρεσιών, και καθαρές διεπαφές για την εδραίωση ασφαλών και αξιόπιστων σημείων σύνδεσης [Kaliontzoglou05].
Συγκεκριμένες παράμετροι διαλειτουργικότητας που ενδέχεται να τίθενται ως απαιτήσεις απο μια ΑΔΑΑΥ είναι η υποστήριξη συγκεκριμένων προτύπων μορφών / δομών δεδομένων και μηνυμάτων, η δημοσίευση προδιαγραφών διεπαφών υπηρεσιών σε συγκεκριμένους καταλόγους και η χρήση λογισμικού ενδιάμεσης ολοκλήρωσης (wrapper) το οποίο υποστηρίζει προτυποποιημένες διεπαφές προς τις εξωτερικές οντότητες με τις οποίες επικοινωνεί η ΑΔΑΑΥ.
Η απαίτηση για εύκολη κλιμάκωση, τόσο διαχειριστικά όσο και σε επίπεδο πόρων, προέρχεται απο την ανάγκη για την παροχή υπηρεσιών σε ή την συνεργασία με ένα ολοένα αυξανόμενο αριθμό άλλων οντοτήτων (είτε αυτές είναι οι πελάτες μιας επιχείρησης, είτε οι πολίτες που επικοινωνούν με έναν δημόσιο οργανισμό κ.λ.π). Η διασύνδεση αυτή πρέπει να παρέχεται με ένα δεδομένο επίπεδο ποιότητας υπηρεσίας το

οποίο θα πρέπει να διατηρείται όσο γίνεται πιο σταθερό, όσο ο αριθμός των εμπλεκομένων οντοτήτων αυξάνει.
Συγκεκριμένες παράμετροι κλιμάκωσης που ενδέχεται να τίθενται ως απαιτήσεις απο μια ΑΔΑΑΥ είναι η υποστήριξη κατώτατων ορίων αριθμού συναλλαγών σε δεδομένο χρονικό διάστημα, κατώτατων ορίων αριθμού οντοτήτων με τις οποίες μπορεί να επικοινωνεί ταυτόχρονα η ΑΔΑΑΥ και κατώτατων ορίων αριθμού χρηστών που μπορεί να υποστηρίζει ταυτόχρονα.

4.2.1.2.2 Ασφάλεια και εμπιστοσύνη

Τα σημερινά δεδομένα υποδεικνύουν ότι προκειμένου μια ΑΠΥ να μπορεί να επιτύχει τους επιχειρηματικούς στόχους της, πρέπει οι υπηρεσίες που περιλαμβάνει να είναι απο όλες τις απόψεις ασφαλείς έμπιστες απο τις οντότητες με τις οποίες έρχεται σε επαφή. Μια σημαντική καινοτομία μιας ΑΔΑΑΥ, είναι ότι θεωρεί την ασφάλεια εξ αρχής ως αναπόσπαστο δομικό της συστατικό, και ότι την ενσωματώνει ως ένα σύνολο υπηρεσιών, παρά ως μεμονωμένους μηχανισμούς.
Οι ευρέως διαδεδομένες απαιτήσεις ασφάλειας που είναι αποτυπωμένες στη βιβλιογραφία και πρέπει να ικανοποιούνται απο μια ΑΔΑΑΥ είναι οι ακόλουθες:

- *Αυθεντικοποίηση*. Είναι η μέθοδος με την οποία αναγνωρίζεται μοναδικά μια οντότητα και επιβεβαιώνεται η ταυτότητά της.
- *Ακεραιότητα.* Η μέθοδος με την οποία εξασφαλίζεται ότι κάθε σύστημα, πόρος, αρχείο και γενικά κάθε πληροφορία μπορεί να τροποποιηθεί μόνο απο εξουσιοδοτημένες οντότητες.
- *Εμπιστευτικότητα και μυστικότητα.* Η μέθοδος με την οποία εξασφαλίζεται ότι πρόσβαση στο περιεχόμενο πληροφοριών έχουν μόνο εξουσιοδοτημένες οντότητες.
- *Μη άρνηση συμμετοχής*. Η μέθοδος με την οποία παράγονται κρυπτογραφικά δεδομένα που εξασφαλίζουν ότι μια οντότητα δεν μπορεί να αποποιηθεί τις πράξεις της.
- *Διαθεσιμότητα.* Μέθοδος που εξασφαλίζει ότι ένα σύστημα θα ικανοποιεί τους στόχους του με ένα δεδομένο επίπεδο ευστοχίας.

Προκειμένου να ικανοποιηθούν οι απαιτήσεις ασφάλειας, μια ΑΔΑΑΥ πρέπει να ενσωματώνει ένα κατάλληλο σύνολο απο *Υπηρεσίες Ασφάλειας*. Μια Υπηρεσία Ασφάλειας ικανοποιεί μια ή περισσότερες απαιτήσεις ασφάλειας, όπως θα παρουσιαστεί στην παράγραφο 4.3.3.3.3.
Συγκεκριμένες παράμετροι ασφάλειας που ενδέχεται να τίθενται ως απαιτήσεις απο μια ΑΔΑΑΥ είναι η κάλυψη όλων ή ενός συγκεκριμένου υποσυνόλου των παραπάνω με κάποια μορφή υπηρεσίας ή μηχανισμού, η υποστήριξη συγκεκριμένων προτύπων τεχνολογιών ασφάλειας ή αλγορίθμων, η υποστήριξη συγκεκριμένων κρυπτογραφικών χαρακτηριστικών και παραμέτρων (π.χ. μήκη κλειδιών κ.λ.π.) και η υποστήριξη δεδομένων επιπέδων ασφάλειας απο εφαρμογές ή υλικοτεχνική υποδομή (π.χ. σύμφωνα με τα common criteria κ.λ.π.).

4.2.1.2.3 Ανοιχτότητα και κατανομή

Όπως υποδεικνύει και ο ορισμός της, μια ΑΔΑΑΥ πρέπει να είναι *ανοιχτή* και τα δομικά της στοιχεία *κατανεμημένα* [RM-ODP]. Μια ανοιχτή κατανεμημένη αρχιτεκτονική δίνει

την δυνατότητα για αλλαγή κόμβων μέσα της χωρίς να επηρεάζεται στο σύνολό της. Αυτό δίνει έναν βαθμό ελευθερίας στο τι είδη κόμβων περιέχει και τι δομικά στοιχεία περιέχει κάθε κόμβος. Η ανοιχτή αρχιτεκτονική επίσης εξασφαλίζει ευκολότερη διασύνδεση των στοιχειών αυτών.
Η ανοιχτότητα είναι βασική απαίτηση που πρέπει να λαμβάνεται στη φάση σχεδιασμού της ΑΔΑΑΥ. Ο σχεδιασμός θα πρέπει να συλλαμβάνει το επίπεδο ανοιχτότητας που χρειάζεται, να καθορίζει σαφώς τους κόμβους που θα περιέχονται, τις διεπαφές και τα κανάλια επικοινωνίας που υποστηρίζουν οι κόμβοι, προσφέροντας το απαραίτητο επίπεδο αφαίρεσης ως προς το τι ακριβώς περιέχει ο ίδιος ο κόμβος. Οι απαιτήσεις για διασφάλιση ανοιχτότητας και κατανομής επιβάλλουν την εφαρμογή προτυποποιημένων μεθόδων για τον σχεδιασμό ανοιχτών και κατανεμημένων αρχιτεκτονικών.
Συγκεκριμένες παράμετροι ανοιχτότητας και κατανομής που ενδέχεται να τίθενται ως απαιτήσεις απο μια ΑΔΑΑΥ είναι η επιβολή χρήσης αντικειμενοστρεφούς μοντέλου σχεδιασμού, η εφαρμογή συγκεκριμένων προτύπων για τον σχεδιασμό διεπαφών και συντονισμού υπηρεσιών και η υποστήριξη συγκεκριμένων μοντέλων κατανομής στα στοιχεία της αρχιτεκτονικής (π.χ. διαχείριση αντιγράφων δεδομένων σε πολλαπλές τοποθεσίες κ.λ.π.)

4.2.1.2.4 Σεβασμός της αντίληψης του χρήστη

Μια σημαντική απαίτηση που μια ΑΔΑΑΥ πρέπει να λαμβάνει υπόψη, είναι η φιλικότητα προς το χρήστη και ο σεβασμός στο πώς ο χρήστης αντιλαμβάνεται τις επιχειρηματικές υπηρεσίες και υπηρεσίες ασφάλειας που περιλαμβάνει η αρχιτεκτονική.
Η απαίτηση αυτή ικανοποιείται με τους εξής κυρίως τρόπους:

- Με την υποστήριξη εφαρμογών με τις οποίες ο χρήστης είναι ήδη εξοικειωμένος και για την χρήση τους δεν θα χρειαστεί επιπρόσθετη εκπαίδευση.
- Με την παροχή υψηλού επιπέδου διαφάνειας για τις πολύπλοκες διεργασίες, ώστε ο χρήστης να μην αντιλαμβάνεται χαμηλού επιπέδου τεχνικές λεπτομέρειες, χωρίς όμως να χάνει την αίσθηση του τι ακριβώς κάνει και γιατί το κάνει.

Η δεύτερη μέθοδος υλοποιείται πιο εύκολα σε μια αρχιτεκτονική υπηρεσιών, διότι μια πολύπλοκη διεργασία μπορεί να χωριστεί σε επιμέρους διεργασίες, και κάθε μια απο αυτές να αντιστοιχηθεί σε υπηρεσίες της αρχιτεκτονικής, με ελεγχόμενο επίπεδο αφαίρεσης και διαφάνειας ανάλογα με την περίπτωση.
Συγκεκριμένες παράμετροι φιλικότητας προς τους χρήστες που ενδέχεται να τίθενται ως απαιτήσεις απο μια ΑΔΑΑΥ είναι η υποστήριξη χαμηλών χρόνων απόκρισης, η επιβολή περιορισμών στον αριθμό των κινήσεων ή “clicks” του ποντικιού κατά την διενέργεια υπο-διεργασιών απο τους χρήστες και η υποστήριξη, προτυποποιημένων ή μη, εναλλακτικών διεπαφών και άτομα με ειδικές ανάγκες.

4.2.1.2.5 Ελαχιστοποίηση απαιτήσεων κόστους, πόρων - αυτοματοποίηση

Η ελαχιστοποίηση του κόστους για υλοποίηση, εγκατάσταση και λειτουργία ενός συστήματος που βασίζεται σε ΑΔΑΑΥ είναι μια σημαντική απαίτηση, που συνήθως είναι δύσκολο να καλυφθεί. Συνήθως οι πόροι τόσο σε ανθρώπινο, όσο και σε υλικοτεχνικό δυναμικό είναι περιορισμένοι.
Η απαίτηση αυτή καλύπτεται με τους ακόλουθους τρόπους:

- Την επαναχρησιμοποίηση πόρων, που είτε ήδη υπάρχουν, είτε δημιουργούνται για πρώτη φορά αλλά μπορούν να εφαρμοστούν σε πολλαπλά σημεία της αρχιτεκτονικής.
- Το σχεδιασμό επεκτάσιμων δομικών μονάδων που μπορούν εύκολα να προσαρμοστούν σε νέες συνθήκες με μικρό κόστος.
- Τη χρήση λογισμικού ανοιχτού κώδικα, και την υιοθέτηση ενός επιχειρηματικού μοντέλου που να διευκολύνει την υποστήριξη σε εφαρμογές ανοιχτού κώδικα. Για παράδειγμα, μια πλατφόρμα που βασίζεται σε μια ΑΔΑΑΥ και περιλαμβάνει εφαρμογές ανοιχτού κώδικα, θα μπορεί να υποστηριχθεί συνολικά απο τον πάροχο της για όλες τις εφαρμογές και δεν θα χρειάζεται ο οργανισμός που την υιοθετεί να λαμβάνει ξεχωριστά υποστήριξη για κάθε στοιχείο της πλατφόρμας.
- Την αυτοματοποίηση διαδικασιών χωρίς την απαραίτητη συμμετοχή ανθρώπινου παράγοντα.

Οι παραπάνω λύσεις υποστηρίζονται απο τις αρχιτεκτονικές υπηρεσιών, διότι οι υπηρεσίες είναι επί της ουσίας επαναχρησιμοποιούμενα στοιχεία, η διαχείριση των οποίων μπορεί να γίνει μεμονωμένα είτε ως σύνολο.
Συγκεκριμένες παράμετροι ελαχιστοποίησης κόστους που ενδέχεται να τίθενται ως απαιτήσεις απο μια ΑΔΑΑΥ είναι η επιβολή πολιτικών χρήσης λογισμικού ανοιχτού κώδικα, ο καθορισμός ανώτατου κόστους για συγκεκριμένες υπηρεσίες ή συστήματα και η χρήση μεθοδολογίας διαχείρισης αλλαγών κατά την εισαγωγή του νέου πληροφοριακού συστήματος.

4.2.1.2.6 Ενσωμάτωση υπαρχουσών υποδομών

Μια βασική απαίτηση είναι η υποστήριξη υπαρχουσών υποδομών και συστημάτων κατά την υιοθέτηση μια καινούργιας αρχιτεκτονικής. Η απαίτηση αυτή είναι πολύ έντονη στην η-διακυβέρνηση όπου δημόσιοι οργανισμοί δεν θέλουν να αλλάξουν εντελώς υπάρχουσες βάσεις δεδομένων ή άλλα συστήματα που ήδη έχουν.
Η πλέον αποδοτική λύση στον τομέα αυτό, είναι η υλοποίηση ενός ενδιάμεσου επιπέδου ολοκλήρωσης (integration layer) που επιτρέπει την επικοινωνία με υπάρχοντα συστήματα. Σε μια ΑΔΑΑΥ αυτό συνήθως περιλαμβάνει την υλοποίηση κατάλληλου λογισμικού (wrapper) που υλοποιεί μια υπηρεσία απο μόνο του, καθιστώντας την υπηρεσία διαθέσιμη στην υπόλοιπη αρχιτεκτονική.
Συγκεκριμένες παράμετροι ενσωμάτωσης υπαρχουσών υποδομών που ενδέχεται να τίθενται ως απαιτήσεις απο μια ΑΔΑΑΥ είναι η χρήση λογισμικού ενδιάμεσης ολοκλήρωσης (wrapper) το οποίο υποστηρίζει προτυποποιημένες διεπαφές προς τις εξωτερικές οντότητες με τις οποίες επικοινωνεί η ΑΔΑΑΥ, η υποστήριξη συγκεκριμένων διεπαφών και δομών μηνυμάτων και η κατάλληλη εφαρμογή κανόνων πολιτικών για την λήψη και αποθήκευση δεδομένων σε υπάρχουσες υποδομές

4.2.1.2.7 Σεβασμός στις επιχειρηματικές ανάγκες και τις πολιτικές του οργανισμού

Η ΑΔΑΑΥ θα πρέπει να επιτυγχάνει τον πρωταρχικό στόχο για τον οποίο ένας οργανισμός πρόκειται να την υιοθετήσει. Θα πρέπει να υλοποιεί τους επιχειρηματικούς

στόχους του οργανισμού, με σεβασμό στις όποιες πολιτικές, περιορισμούς και όρους αυτός θέτει.
Ο λόγος για τον οποίο ξεκίνησε η ιδέα των ΑΠΥ είναι ακριβώς αυτός: να εφαρμοστεί μια αντιστοίχηση των επιχειρηματικών δραστηριοτήτων του οργανισμού, που επιτυγχάνουν τους στόχους του, σε επιμέρους υπηρεσίες τις οποίες ο οργανισμός είναι ευκολότερο να ελέγξει και διαχειριστεί. Οι πολιτικές του οργανισμού διαμορφώνουν το περιβάλλον λειτουργίας κάθε μιας υπηρεσίας, κάνοντας ευκολότερο τον έλεγχο του ότι οι πολιτικές αυτές όντως εφαρμόζονται, είτε αυτές είναι πολιτικές ασφάλειας, επιχειρηματικής λογικής κ.λ.π.
Συγκεκριμένες παράμετροι ενσωμάτωσης υπαρχουσών υποδομών που ενδέχεται να τίθενται ως απαιτήσεις απο μια ΑΔΑΑΥ είναι η υλοποίηση των καταγεγραμμένων στόχων του επιχειρησιακού σχεδίου του οργανισμού που υιοθετεί την αρχιτεκτονική, ο ορισμός κριτηρίων επίτευξης των παραπάνω επιχειρησιακών στόχων και της μεθοδολογίας αξιολόγησης των κριτηρίων.

4.2.2 Απαιτήσεις μεθοδολογίας

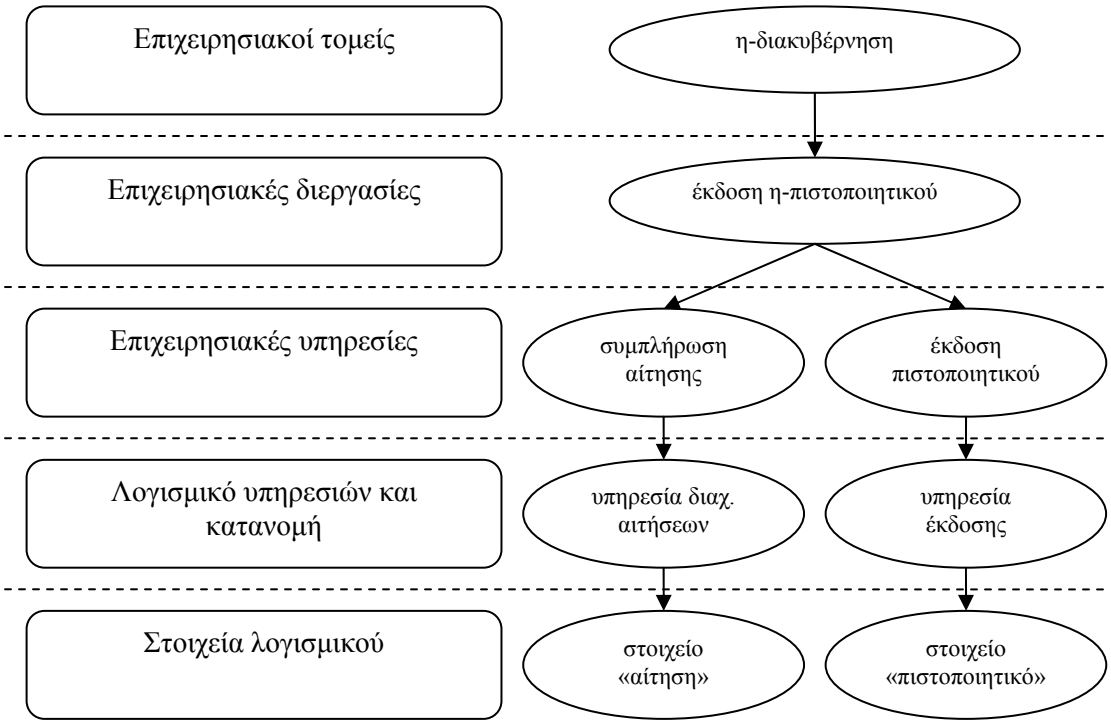
Οι απαιτήσεις που πρέπει να καλύπτονται απο τη μεθοδολογία είναι οι ακόλουθες:

- Οι αρχιτεκτονικές που προδιαγράφονται βάσει της μεθοδολογίας θα πρέπει να καλύπτουν τις απαιτήσεις των ΑΔΑΑΥ.
- Θα πρέπει να είναι γενικευμένη ως προς την έννοια των κατανεμημένων συστημάτων, αλλά να δίνει έμφαση στην υποστήριξη υπηρεσιών, όπως απαιτείται απο μια ΑΔΑΑΥ.
- Οι διαδικασίες και η σημειολογία πρέπει να καθορίζονται τυπικά. Ο σχεδιαστής που τη χρησιμοποιεί δεν θα πρέπει να ξεκινάει απο το μηδέν αλλά να μπορεί να χρησιμοποιεί ήδη υπάρχοντα στοιχεία, να μπορεί να τα επεκτείνει αν χρειάζεται και να δημιουργεί νέα.
- Πρέπει να παρέχει έναν δομημένο τρόπο για την αναπαράσταση των υπηρεσιών.
- Πρέπει να παρέχει καλώς ορισμένους παράγοντες ελέγχου ποιότητας των αποτελεσμάτων και βέλτιστες πρακτικές.
- Οι υπηρεσίες που ορίζονται θα πρέπει είναι επαναχρησιμοποιήσιμες.
- Θα πρέπει να διευκολύνει την μοντελοποίηση με υπάρχοντα εργαλεία.

Ένα μέρος των παραπάνω απαιτήσεων καλύπτεται απο το γεγονός ότι η μεθοδολογία χρησιμοποιεί το πρότυπο RM-ODP σε συνδυασμό με την UML. Οι υπόλοιπες καλύπτονται απο την διάρθρωση της ίδιας της μεθοδολογίας και τα περιεχόμενά της.

4.2.3 Ιεραρχία μεθοδολογίας και το πρότυπο RM-ODP

Προκειμένου η μεθοδολογία να καλύπτει όλες τις πλευρές του σχεδιασμού μιας ΑΔΑΑΥ θα πρέπει να επιτρέπει την ανάλυση όλων των επιπέδων που απαρτίζουν μια αρχιτεκτονική υπηρεσιών.
Το ακόλουθο σχήμα δίνει την αναπαράσταση της ιεραρχίας των επιπέδων της μεθοδολογίας, χρησιμοποιώντας ένα παράδειγμα απο τον επιχειρησιακό τομέα της η-διακυβέρνησης. Η ιεραρχία αυτή έχει προκύψει απο την μελέτη αντίστοιχων μεθοδολογιών και αρχιτεκτονικών πλαισίων [High05, Tang04].



Σχήμα 4-2: Ιεραρχία σχεδιαστικών επιπέδων μεθοδολογίας

Όπως φαίνεται απο το σχήμα, στο υψηλότερο επίπεδο γίνεται η αναγνώριση και διαχωρισμός των επιχειρησιακών τομέων στον οποίο θα ενταχθεί η προς σχεδιασμό ΑΔΑΑΥ. Κάθε τομέας εμπεριέχει έναν αριθμό κοινοτήτων με διακριτές ανάγκες για υπηρεσίες. Ένα παράδειγμα τομέα είναι η η-διακυβέρνηση και μια κοινότητα θα μπορούσε να είναι το σύνολο δήμων μιας περιφέρειας.

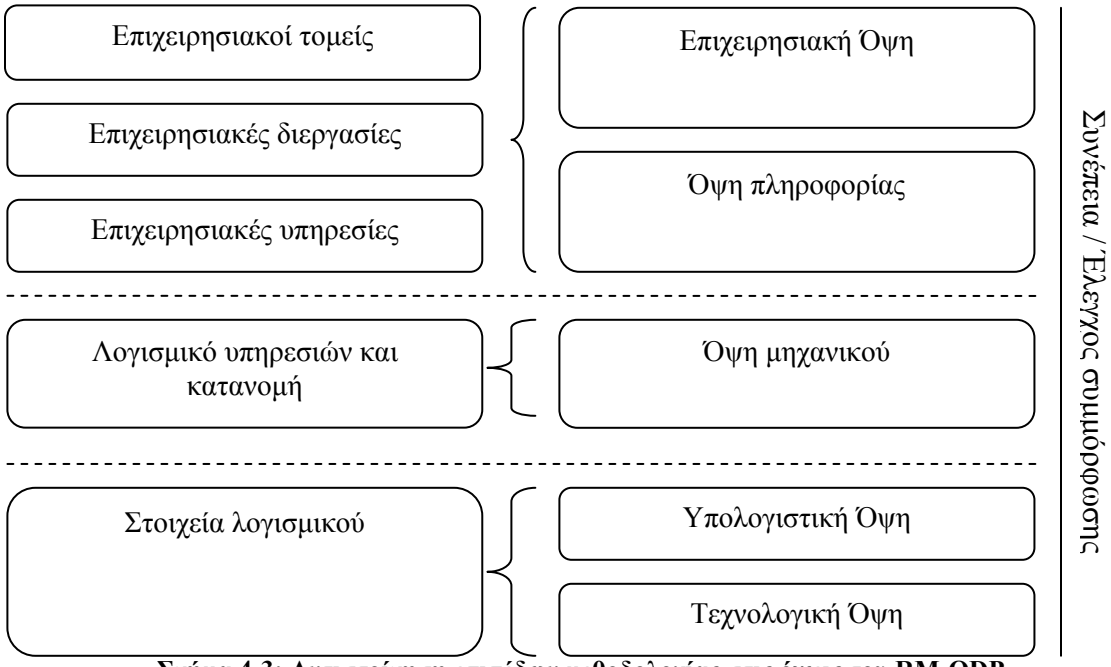
Στη συνέχεια αναγνωρίζονται μέσα στον τομέα οι επιχειρησιακές διεργασίες που πρέπει να παρέχονται, όπως για παράδειγμα η έκδοση ενός ηλεκτρονικού πιστοποιητικού[1]. Οι διεργασίες αναπαριστούν τις βασικές επιχειρηματικές δραστηριότητες που λαμβάνουν χώρα μέσα στις κοινότητες.

Κάθε επιχειρησιακή διεργασία χωρίζεται σε επιμέρους επιχειρησιακές υπηρεσίες, τις οποίες συντονίζει κατάλληλα προκειμένου να επιτελέσει τους επιχειρησιακούς στόχους της. Για παράδειγμα, η διεργασία έκδοσης του η-πιστοποιητικού θα περιλαμβάνει μια υπηρεσία για τη συμπλήρωση της αίτησης για το πιστοποιητικό απο έναν πολίτη και σε ένα μετέπειτα στάδιο την υπηρεσία για την πραγματική έκδοση του ηλεκτρονικού εγγράφου.

Ένα επίπεδο πιο κάτω, η κάθε επιχειρησιακή υπηρεσία αντιστοιχίζεται σε μια αντίστοιχη υπηρεσία που υλοποιείται με λογισμικό. Η έννοια της υπηρεσίας εδώ είναι πλέον τεχνική και όχι ιδεατή. Στο επίπεδο αυτό σχεδιάζεται η δομή της υπηρεσίας, οργανώνεται μέσα στην κατανεμημένη αρχιτεκτονική που αποτελεί η ΑΔΑΑΥ, αποφασίζονται οι διεπαφές της και η επικοινωνία με άλλες υπηρεσίες και επιλέγονται τεχνολογίες υλοποίησής της.

[1] Σημειώνεται ότι ένα αντίστοιχο παράδειγμα για την έκδοση ενός πιστοποιητικού θα χρησιμοποιείται τακτικά κατά την παρουσίαση της παρούσας μεθόδου για λόγους συνέπειας και καλύτερης κατανόησης.

Επίσης μια άλλη δραστηριότητα που σχεδιάζεται σε αυτό το επίπεδο είναι η εδραίωση του ακριβούς πλαισίου συντονισμού των διαφόρων υπηρεσιών μιας διεργασίας.
Στο τελευταίο επίπεδο, για κάθε υπηρεσία και μηχανισμό που απαιτείται στην αρχιτεκτονική, σχεδιάζονται τα εσωτερικά στοιχεία που τη απαρτίζουν. Ο σχεδιασμός των στοιχείων βασίζεται σε αντικειμενοστρεφείς μεθοδολογίες τεχνολογίας λογισμικού. Τα στοιχεία σχεδιάζονται και δομούνται έτσι ώστε να υλοποιούν τις διεπαφές της υπηρεσίας που έχουν ήδη καθοριστεί.
Προκειμένου να επιτευχθεί ο σχεδιασμός των παραπάνω επιπέδων, η μεθοδολογία αντιστοιχίζει τα επίπεδα σε όψεις του προτύπου RM-ODP. Η αντιστοίχηση αυτή φαίνεται στο ακόλουθο σχήμα.



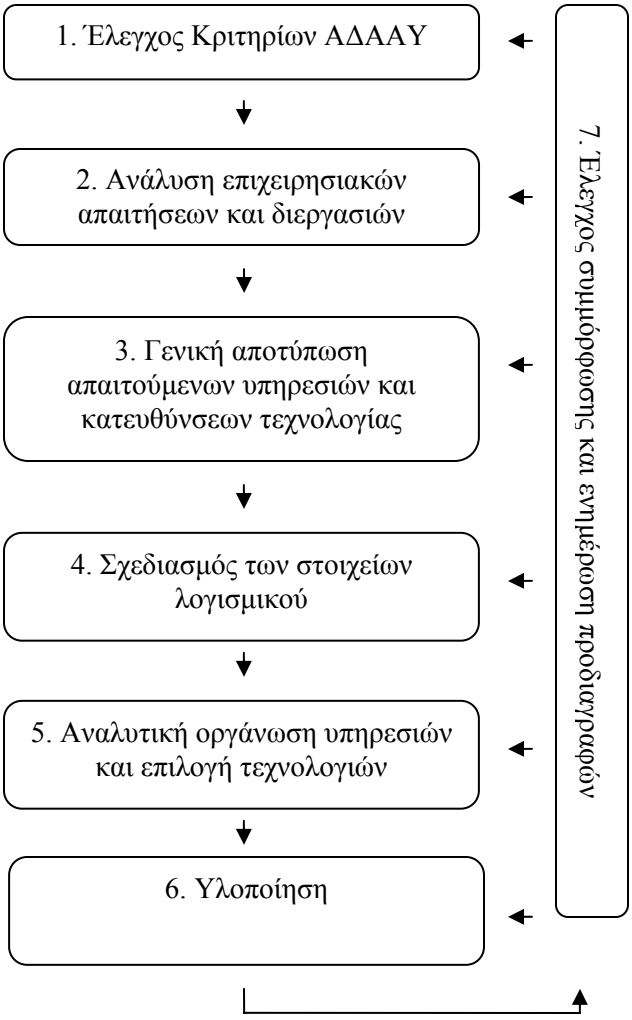
Σχήμα 4-3: Αντιστοίχηση επιπέδων μεθοδολογίας στις όψεις του RM-ODP

Όπως φαίνεται στο σχήμα, τα τρία πρώτα επίπεδα της μεθοδολογίας βασίζονται στην επιχειρησιακή όψη και την όψη πληροφορίας του προτύπου RM-ODP. Η επιχειρησιακή όψη περιγράφει τους τομείς στους οποίους αναφέρεται η προς σχεδιασμό αρχιτεκτονική, του στόχους της, της κοινότητες που περιλαμβάνει και τους ρόλους των αντικειμένων εντός των κοινοτήτων αυτών, τις πολιτικές που πρέπει να εφαρμόζονται, καθώς και τις διεργασίες που πρέπει να υλοποιούνται. Επίσης η επιχειρησιακή όψη αναγνωρίζει σε υψηλό επίπεδο τις υπηρεσίες απο τις οποίες απαρτίζεται κάθε επιχειρησιακή διεργασία στην αρχιτεκτονική, καθώς και τις γενικότερες υπηρεσίες της αρχιτεκτονικής που υλοποιούν βασικούς αλλά μη επιχειρησιακούς στόχους (π.χ. υπηρεσίες συντονισμού). Η όψη πληροφορίας χρησιμοποιείται για τον σχεδιασμό και την περιγραφή των αντικειμένων πληροφορίας που χρησιμοποιούν οι υπηρεσίες σε ιδεατό επίπεδο.
Το επίπεδο λογισμικού υπηρεσιών και κατανομής αντιστοιχίζεται στην Όψη Μηχανικού. Αυτό σημαίνει ότι οι υπηρεσίες αναγνωρίζονται ως επικοινωνούντα στοιχεία λογισμικού του συστήματος, και δίνεται ο τρόπος οργάνωσής τους. Επίσης η όψη σχεδιάζει τα

κανάλια μέσω των οποίων επικοινωνούν οι υπηρεσίες και τους κόμβους στους οποίους λειτουργούν.
Το τελευταίο επίπεδο της ιεραρχίας, σχεδιάζεται βάσει της υπολογιστικής και τεχνολογικής όψης. Κάθε στοιχείο λογισμικού που απαρτίζει μια υπηρεσία σχεδιάζεται με λεπτομέρεια χρησιμοποιώντας την λογική και της έννοιες του αντικειμενοστρεφούς προγραμματισμού. Ορίζονται οι διεπαφές του, η εσωτερική δομή τους και οι μέθοδοι που υποστηρίζει. Ο σχεδιασμός εδώ θα πρέπει να λαμβάνει υπόψη την συνολική όψη μηχανικού, χωρίς όμως να περιορίζεται. Βάσει της υπολογιστικής όψης, η όψη μηχανικού θα πρέπει να ανανεώνεται προκειμένου να αντικατοπτρίζονται λεπτομέρειες που δεν είναι ορατές σε υψηλό επίπεδο. Τέλος για κάθε ομάδα στοιχείων της υπολογιστικής όψης που αποτελούν μέρος υπηρεσιών, επιλέγεται μια τεχνολογία σύμφωνα με τις αρχές της τεχνολογικής όψης, και αυτή η τεχνολογία αντικατοπτρίζεται στην όψη μηχανικού και χρησιμοποιείται για την υλοποίηση των στοιχείων λογισμικού.
Ως κάθετος άξονας της μεθοδολογίας, ο οποίος επίσης βασίζεται στις έννοιες του RM-ODP, είναι ο συνεχής έλεγχος της συνέπειας του σχεδιασμού, δηλαδή ότι οι όψεις μεταξύ τους είναι συνεπείς και ο,τι προδιαγράφεται στη μια αντιστοιχεί σε ο,τι προδιαγράφεται σε μια άλλη. Επίσης, κάθετη δραστηριότητα είναι ο έλεγχος συμμόρφωσης της αρχιτεκτονικής που υλοποιείται σε σχέση με τις προδιαγραφές που έχουν προκύψει απο την εφαρμογή της μεθοδολογίας.

4.2.4 Επισκόπηση σταδίων μεθοδολογίας

Η μεθοδολογία αποτελείται απο επτά στάδια, τα οποία περιγράφονται συνοπτικά στις παραγράφους που ακολουθούν, τα οποία αναπαρίστανται στο ακόλουθο διάγραμμα:



Σχήμα 4-4: Τα επτά στάδια της κατασκευαστικής μεθόδου

Η αναλυτική περιγραφή της μεθόδου για κάθε στάδιο και συγκεκριμένα παραδείγματα περιλαμβάνονται στο κεφάλαιο 4.3.

4.2.4.1 1^{ο} στάδιο: Έλεγχος κριτηρίων ΑΔΑΑΥ

Στο στάδιο αυτό καταγράφεται αν οι απαιτήσεις της προς σχεδιασμό αρχιτεκτονική αποτελούν υποσύνολο των απαιτήσεων μιας γενικευμένης ΑΔΑΑΥ όπως αναφέρονται στην παράγραφο 4.2.1.2. Εάν ναι, τότε έχει νόημα να εφαρμοστεί η μεθοδολογία. Εάν η συγκεκριμένη αρχιτεκτονική έχει επιπλέον απαιτήσεις, οι οποίες δεν αποτελούν εξειδίκευση των απαιτήσεων της ΑΔΑΑΥ, τότε χρειάζεται περαιτέρω μελέτη για να αποφανθεί κάποιος αν η μεθοδολογία μπορεί να επεκταθεί κατάλληλα ώστε να τις καλύπτει. Σημειώνεται ότι οι απαιτήσεις της ΑΔΑΑΥ είναι αρκετά γενικές, ώστε να καλύπτουν ένα μεγάλο εύρος σύγχρονων ασφαλών, διαλειτουργικών και ανοιχτών αρχιτεκτονικών υπηρεσιών.

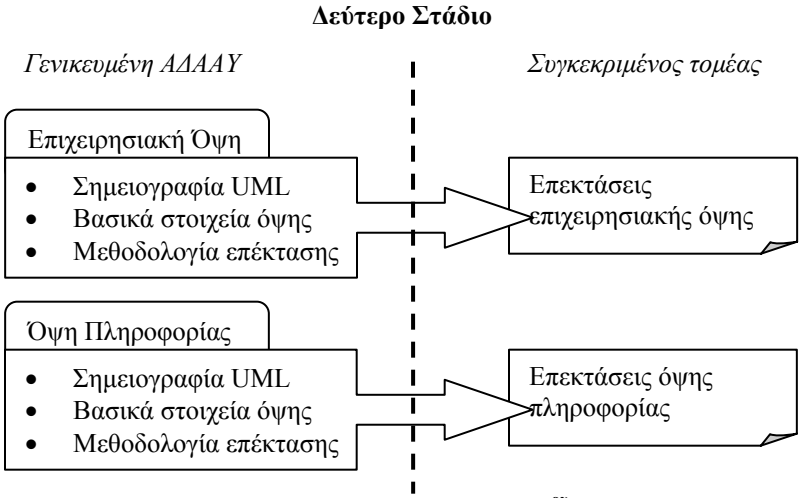
4.2.4.2 2^{ο} στάδιο: Ανάλυση επιχειρησιακών απαιτήσεων και διεργασιών

Στο στάδιο αυτό αναλύονται οι επιχειρησιακές απαιτήσεις του τομέα για τον οποίο προορίζεται η προς σχεδιασμό αρχιτεκτονική υπηρεσιών. Η ανάλυση προκύπτει μέσα απο τον σχεδιασμό των δύο πρώτων όψεων του RM-ODP, της επιχειρησιακής όψης και της όψης πληροφορίας.

Ως μέρος της επιχειρησιακής όψης αναλύονται οι κοινότητες που συμμετέχουν στην αρχιτεκτονική, οι οντότητες-αντικείμενα των κοινοτήτων και οι ρόλοι τους, οι διεργασίες στις οποίες συμμετέχουν και οι πολιτικές που διέπουν τις σχέσεις μεταξύ αντικειμένων και διεργασιών. Η ανάλυση αυτή επιτρέπει τον ορισμό σε υψηλό επίπεδο αφαίρεσης των υπηρεσιών που θα σχεδιαστούν ως μέρος των επιχειρησιακών διεργασιών.

Η όψη πληροφορίας καθορίζει σε ιδεατό επίπεδο τα αντικείμενα της αρχιτεκτονικής που αναπαριστούν κάποια πληροφορία και τις καταστάσεις απο τις οποίες αυτά περνούν ως μέρος των επιχειρησιακών διεργασιών.

Στο στάδιο αυτό η μεθοδολογία περιγράφει συνολικά το πως δομούνται η επιχειρησιακή όψη και η όψη πληροφορίας και δίνεται η σημειογραφία τους βάσει της UML. Ακολουθείται η γενική πρακτική που αποτυπώνεται στο ακόλουθο σχήμα.



Σχήμα 4-5: Σχηματική αναπαράσταση του 2^{ου} σταδίου της μεθοδολογίας

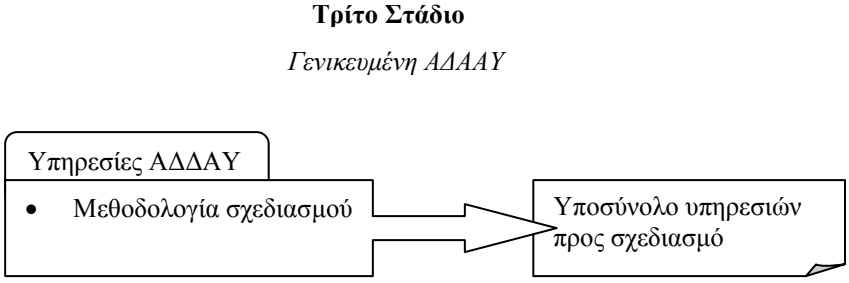
Κάθε μια απο τις δύο όψεις ως μέρος της μεθοδολογίας απαρτίζεται απο:

- ένα σύνολο *βασικών στοιχείων* που ενδέχεται να υπάρχουν σε μια ΑΔΑΑΥ και αποτελούν μέρος των προδιαγραφών της. Το χαρακτηριστικό αυτών των στοιχείων είναι ότι είναι επαναχρησιμοποιήσιμα, εξειδικεύουν έννοιες του RM-ODP μέσα στην ΑΔΑΑΥ, αλλά είναι και αρκετά γενικά ώστε να μπορούν να χρησιμοποιηθούν σε οποιαδήποτε ΑΔΑΑΥ.
- την περιγραφή της μεθοδολογίας επέκτασης των βασικών στοιχείων προκειμένου να ολοκληρωθεί η κάθε όψη για να αντικατοπτρίζει πληρέστερα το συγκεκριμένο περιβάλλον στο οποίο θα εφαρμοστεί η ΑΔΑΑΥ που σχεδιάζεται κάθε φορά, καθώς και την μεθοδολογία δημιουργίας καινούργιων αντικειμένων.

Απο την εφαρμογή της μεθοδολογίας σε αυτό το στάδιο λοιπόν, επιλέγονται στοιχεία της γενικευμένης ΑΔΑΑΥ που περιγράφουν το επιχειρησιακό επίπεδο της προς σχεδιασμό αρχιτεκτονικής, κάποια απο αυτά επεκτείνονται ώστε να αντικατοπτρίζουν την συγκεκριμένη περίπτωση και σχεδιάζονται και νέα.

4.2.4.3 3ο στάδιο: Γενική αποτύπωση απαιτούμενων υπηρεσιών και κατευθύνσεων τεχνολογίας

Στο στάδιο αυτό, επιλέγεται το υποσύνολο των υπηρεσιών που θα ενσωματωθούν στην αρχιτεκτονική απο ένα δεδομένο αρχικό σύνολο που δίνονται απο την μέθοδο και αποτυπώνονται οι αρχικές κατευθύνεις ως προς το συνολικό τεχνολογικό πλαίσιο που θα υιοθετηθεί (π.χ. αρχιτεκτονική J2EE κ.λ.π.).

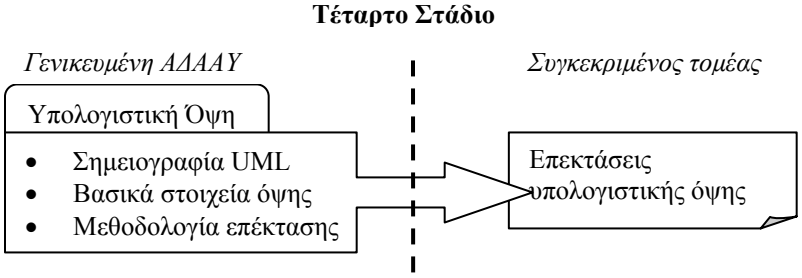


Σχήμα 4-6: Σχηματική αναπαράσταση του 3ου σταδίου της μεθοδολογίας

Στόχος σε αυτό το στάδιο είναι να δοθεί η γενική εικόνα του τι περιέχει η αρχιτεκτονική και προς τα που θα κατευθυνθεί ο σχεδιασμός των στοιχείων λογισμικού που απαρτίζουν τις υπηρεσίες στο επόμενο στάδιο.

4.2.4.4 4ο στάδιο: Σχεδιασμός στοιχείων λογισμικού

Στο στάδιο αυτό σχεδιάζεται κάθε στοιχείο των υπηρεσιών που έχουν επιλεγεί στο 3ο στάδιο, βάσει των αρχών σχεδιασμού κατασκευαστικής μεθόδου και των εννοιών της υπολογιστικής όψης του RM-ODP.
Στην υπολογιστική όψη ορίζονται επακριβώς οι διεπαφές κάθε υπηρεσίας, σχεδιάζονται τα συστατικά στοιχεία που υλοποιούν τις διεπαφές και τους στόχους της υπηρεσίας. Ο σχεδιασμός χρησιμοποιεί αντικειμενοστρεφείς αρχές και έννοιες ώστε όλα τα στοιχεία και οι υπηρεσίες που συνθέτουν να είναι επαναχρησιμοποιήσιμα.



Σχήμα 4-7: Σχηματική αναπαράσταση 4ου σταδίου μεθοδολογίας

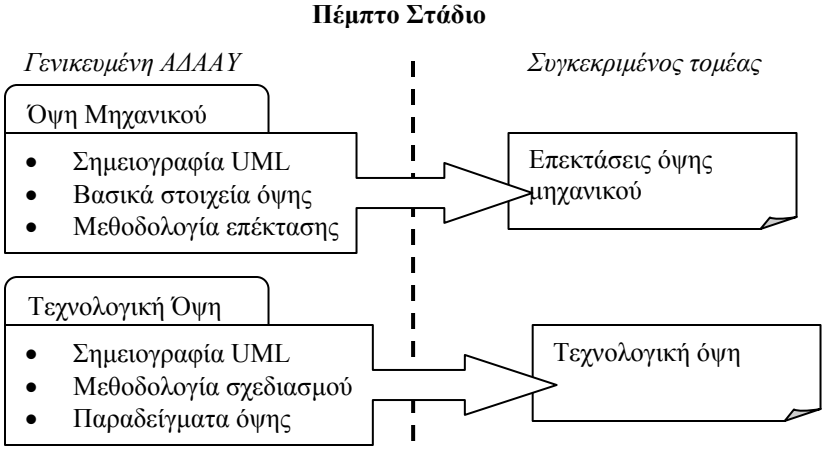
Όπως φαίνεται απο το σχήμα, όμοια με το δεύτερο στάδιο η όψη απαρτίζεται:

- απο ένα σύνολο επαναχρησιμοποιήσιμων σχεδιαστικών *βασικών στοιχείων* υπολογιστικής όψης που ενδέχεται να αποτελούν υπηρεσίες μιας ΑΔΑΑΥ.
- απο την περιγραφή της μεθοδολογίας επέκτασης των βασικών στοιχείων και ορισμού νέων.

Η μεθοδολογία επέκτασης περιγράφει τους συγκεκριμένους στόχους που πρέπει να επιτύχει η όψη, ποιες είναι οι αρχές και οι ιδέες που πρέπει να τηρούνται (βάσει του RM-ODP) και τι είδους διαγράμματα UML πρέπει να χρησιμοποιηθούν για να περιγραφούν οι ιδέες αυτές.

4.2.4.5 5^{ο} στάδιο: Αναλυτική οργάνωση υπηρεσιών και επιλογή τεχνολογιών

Στο πέμπτο στάδιο της μεθοδολογίας χρησιμοποιούνται οι αναλυτικές προδιαγραφές της υπολογιστικής όψης του προηγούμενου σταδίου ώστε να σχεδιαστεί η αναλυτική όψη μηχανικού σύμφωνα με το RM-ODP. Επίσης γίνεται επιλογή των τεχνολογιών που θα εφαρμοστούν στην συγκεκριμένη αρχιτεκτονική για την υλοποίηση των υπηρεσιών και των δομικών στοιχείων τους, και προκύπτει έτσι η τεχνολογική όψη, η οποία είναι άρρηκτα δεμένη με την όψη μηχανικού.



Σχήμα 4-8: Σχηματική αναπαράσταση 5ου σταδίου μεθοδολογίας

Και πάλι η μεθοδολογία περιγράφει τη σημειολογία βάσει της UML με την οποία προκύπτουν οι δύο όψεις και τα βήματα που πρέπει να ακολουθηθούν. Όσο αφορά στην τεχνολογική όψη, η μεθοδολογία περιγράφει και πάλι τους συγκεκριμένους στόχους που πρέπει να επιτύχει η όψη, ποιες είναι οι αρχές και οι ιδέες που πρέπει να τηρούνται (βάσει του RM-ODP) και τι είδους διαγράμματα πρέπει να χρησιμοποιηθούν για να περιγραφούν οι ιδέες αυτές, και επιπλέον συγκεκριμένα παραδείγματα τεχνολογιών αιχμής που θα μπορούσαν να χρησιμοποιηθούν ως «πρότυπα» (templates) για συγκεκριμένες ΑΔΑΑΥ, προκειμένου να καλύπτονται πληρέστερα οι γενικευμένες απαιτήσεις (για παράδειγμα η XML ή οι Υπηρεσίες Ιστού αποτελούν την πλέον ενδεδειγμένη λύση για την εξασφάλιση της διαλειτουργικότητας κ.ο.κ).

4.2.4.6 6ο Στάδιο: Υλοποίηση

Στο στάδιο αυτό υλοποιούνται βάσει των τεχνολογιών που έχουν επιλεγεί όλα στοιχεία λογισμικού της υπολογιστικής όψης και οργανώνονται σε υπηρεσίες σύμφωνα με την όψη μηχανικού.
Η ακριβής μεθοδολογία υλοποίησης δεν καλύπτεται απο την παρούσα διατριβή, αλλά η υπόθεση είναι ότι χρησιμοποιούνται συνήθεις πρακτικές τεχνολογίας λογισμικού για προγραμματισμό σε αντικειμενοστρεφή περιβάλλοντα με αντίστοιχα εργαλεία.

4.2.4.7 7ο στάδιο: Έλεγχος συμμόρφωσης και ενημέρωση προδιαγραφών

Στο τελευταίο στάδιο, επιτελούνται δύο διεργασίες:

- Σύμφωνα με τα κριτήρια συμμόρφωσης που έχουν τεθεί κατά τον σχεδιασμό βάσει του προτύπου RM-ODP, ελέγχεται αν η υλοποίηση της αρχιτεκτονικής ως σύστημα πλέον αντικατοπτρίζει της προδιαγραφές και συμμορφώνεται με αυτές.
- Οι προδιαγραφές όλων όψεων εκτός απο την τεχνολογική (μηχανικού, υπολογιστικής, πληροφορίας, επιχειρησιακής), επανελέγχονται με την αντίστροφη σειρά, διορθώνονται λάθη, ενσωματώνονται καινούργιες απαιτήσεις και γίνονται πιο λεπτομερείς, βάσει συμπερασμάτων που εξήχθησαν απο την υλοποίηση.

Με το πέρας του σταδίου αυτού υπάρχει μια πρώτη έκδοσης της συγκεκριμένης ΑΔΑΑΥ έτοιμη προς εγκατάσταση και λειτουργία.

4.2.5 Πλεονεκτήματα μεθοδολογίας

Τα πλεονεκτήματα της μεθοδολογίας σε σχέση με υπάρχουσες προσεγγίσεις είναι τα ακόλουθα:

- Είναι γενικευμένη και μπορεί να χρησιμοποιηθεί για την παραγωγή των προδιαγραφών ενός μεγάλου εύρους αρχιτεκτονικών υπηρεσιών, αποφεύγοντας τον ad-hoc σχεδιασμό λύσεων δεμένων με την εκάστοτε υλοποίηση.
- Είναι παραμετροποιήσιμη υπο την έννοια ότι μπορούν να εφαρμοστούν κατάλληλα υποσύνολά της για την παραγωγή των προδιαγραφών τόσο μιας ολόκληρης ΑΔΑΑΥ όσο και μιας συγκεκριμένης υπηρεσίας εντός μιας ΑΔΑΑΥ (π.χ. σχεδιασμός και υλοποίηση μόνο κάποιων επιχειρησιακών υπηρεσιών).
- Είναι δομημένη και παρέχει συγκεκριμένα βήματα που πρέπει να ακολουθηθούν σε κάθε στάδιο.
- Είναι βασισμένη σε ένα σημαντικό πρότυπο στον τομέα της προδιαγραφής κατανεμημένων αρχιτεκτονικών και τα αποτελέσματά της συμμορφώνονται στο πρότυπο, χωρίς να απαιτείται η εκκίνηση της διαδικασίας σχεδιασμού απο το μηδέν και τις πολύ γενικές έννοιες του RM-ODP. Επίσης η χρήση της UML επιτρέπει την κατανόηση των όψεων και των στόχων τους απο ένα κοινό το οποίο δεν είναι καθόλου εξοικειωμένο με το πρότυπο RM-ODP.
- Παρέχει ένα σύνολο απο παραμετροποιήσιμα κοινά αντικείμενα, απολύτως επαναχρησιμοποιήσιμα, για τον ορισμό των αντικειμένων κάθε αρχιτεκτονικής.
- Παρέχει υψηλό επίπεδο ανεξαρτησίας απο τεχνολογίες.

Θεωρείται επίσης σημαντικό να τονιστεί ότι η μεθοδολογία δεν προδιαγράφει τις λεπτομέρειες υλοποίησης του λογισμικού της ΑΔΑΑΥ και δεν επιβάλλει κάποια γλώσσα προγραμματισμού, αν και προδιαθέτει προς την χρήση εργαλείων και γλωσσών ανοιχτού κώδικα προκειμένου να καλύπτονται βέλτιστα ένα μέρος των γενικευμένων απαιτήσεων μιας ΑΔΑΑΥ.

4.3 Αναλυτική περιγραφή μεθοδολογίας

4.3.1 1ο στάδιο: Έλεγχος κριτηρίων ΑΔΑΑΥ

4.3.1.1 Στόχοι

Προκειμένου να αποφανθεί κάποιος αν έχει νόημα να εφαρμοστεί η μεθοδολογία, μπορεί να ελέγξει αν η αρχιτεκτονική που θέλει να σχεδιάσει και υλοποιήσει περιγράφεται απο τον ορισμό της ΑΔΑΑΥ και αν οι απαιτήσεις της είναι υποσύνολο των απαιτήσεων μιας ΑΔΑΑΥ, όπως αυτές περιγράφονται στο κεφάλαιο 4.2.1.2.

4.3.1.2 Μεθοδολογία σταδίου

Το παρόν στάδιο περιλαμβάνει τα ακόλουθα βήματα:

1. Ο σχεδιαστής μελετά όλες τις γενικευμένες απαιτήσεις που έχει μια ΑΔΑΑΥ όπως αυτές αναλύονται στην παράγραφο 4.2.1.2.
2. Μελετώνται οι γενικές απαιτήσεις της προς σχεδιασμό αρχιτεκτονικής, ως προς κάθε μία απο τις κατηγορίες των απαιτήσεων της ΑΔΑΑΥ, καθώς και αν η αρχιτεκτονική εμπίπτει στον ορισμό μιας ΑΔΑΑΥ.
3. Θεωρώντας ότι Χ = το σύνολο των απαιτήσεων της προς σχεδιασμό αρχιτεκτονικής και Α = το σύνολο των απαιτήσεων της ΑΔΑΑΥ, διακρίνουμε τις παρακάτω περιπτώσεις:
   - Α. Εάν $X \subseteq A$, τότε η μεθοδολογία μπορεί να εφαρμοστεί, όπως περιγράφεται στα στάδια που ακολουθούν.
   - Β. Εάν $X \cap A = \varnothing$, τότε η μεθοδολογία δεν μπορεί να εφαρμοστεί.
   - Γ. Εάν $A \subseteq X$, τότε η μεθοδολογία όπως περιγράφεται στα στάδια που ακολουθούν μπορεί να εφαρμοστεί ενδεχομένως για ένα υποσύνολο των προδιαγραφών.
4. Στις περιπτώσεις Α και Γ, καταγράφονται όλες οι απαιτήσεις που πρέπει να καλύπτονται χρησιμοποιώντας κατάλληλα σύνολα συγκεκριμένων παραμέτρων (όπως αυτά που αναφέρονται στην παράγραφο 4.2.1.2).

Στο πέρας του βήματος (4), ο σχεδιαστής έχει καταγράψει το σύνολο των βασικών απαιτήσεων της ΑΔΑΑΥ που θα σχεδιάσει προκειμένου να ληφθούν υπόψην κατά την ανάλυση των επιχειρησιακών απαιτήσεων στο στάδιο 2, καθώς και στην επιλογή των υπηρεσιών στο στάδιο 3.

4.3.2 2ο στάδιο: Ανάλυση επιχειρησιακών απαιτήσεων και διεργασιών

4.3.2.1 Στόχοι

Το 2ο στάδιο έχει στόχο σε πρώτη φάση να αποτυπώσει τις επιχειρησιακές απαιτήσεις της σχεδιαζόμενης αρχιτεκτονικής συμπεριλαμβανομένου αρχικά μιας υψηλού επιπέδου ανάλυσης των διεργασιών που υποστηρίζει και στην συνέχεια μια βαθύτερη ανάλυση τους, καθώς και τον διαχωρισμό κοινοτήτων και ρόλων των οντοτήτων που

συμμετέχουν. Σε δεύτερη φάση ορίζει τα αντικείμενα πληροφορίας που οι οντότητες ανταλλάσσουν και διαχειρίζονται προκειμένου να εκπληρώσουν τους στόχους τους.

4.3.2.2 Μεθοδολογία σταδίου

Στο στάδιο αυτό ο σχεδιασμός περιλαμβάνει τα ακόλουθα βήματα:

I. **Προδιαγράφεται η επιχειρησιακή όψη** της αρχιτεκτονικής βάσει των εννοιών και της σημειογραφίας του κεφαλαίου 4.3.2.3. Τα επιμέρους βήματα που ακολουθούνται είναι:
    1. Βάσει των απαιτήσεων της αρχιτεκτονικής προδιαγράφονται σε υψηλό επίπεδο οι επιχειρησιακές λειτουργίες που υλοποιεί σύμφωνα με τους κανόνες και τα στοιχεία της παραγράφου 4.3.2.3.3.1.
    2. Καθορίζονται οι κοινότητες που περιέχονται στην αρχιτεκτονική καθώς και αυτές που είναι εκτός της και με τις οποίες συναλλάσσεται. Εντός των κοινοτήτων ορίζονται επιχειρησιακά αντικείμενα και οι ρόλοι τους βάσει των στοιχείων και κανόνων της παραγράφου 4.3.2.3.3.2.
    3. Σχεδιάζονται με μεγαλύτερη λεπτομέρεια οι επιχειρησιακές διεργασίες που θα λαμβάνουν χώρα εντός της αρχιτεκτονικής και κατά την επικοινωνία της με εξωτερικούς φορείς βάσει των επιχειρησιακών λειτουργιών του βήματος (1) και των κανόνων της παραγράφου 4.3.2.3.3.3.
    4. Προδιαγράφονται οι πολιτικές που διέπουν κάθε διεργασία (περιορισμοί, δικαιώματα, επιχειρησιακοί κανόνες κ.λ.π) σύμφωνα με τους κανόνες της παραγράφου 4.3.2.3.3.4.

   Στο πέρας του βήματος (I), ο σχεδιαστής έχει ολοκληρώσει την πρώτη έκδοση της επιχειρησιακής όψης της αρχιτεκτονικής.

I. **Προδιαγράφεται η όψη πληροφορίας** της αρχιτεκτονικής βάσει των εννοιών και της σημειογραφίας του κεφαλαίου 4.3.2.4. Στο βήμα αυτό ορίζονται τα αντικείμενα πληροφορίας που δημιουργούνται και μεταφέρονται ως μέρος των διεργασιών του βήματος (I.3). Για κάθε αντικείμενο πληροφορίας ορίζεται:
    1. Το σταθερό του σχήμα σύμφωνα με τα βασικά στοιχεία και τους κανόνες της παραγράφου 4.3.2.4.3.1.
    2. Το δυναμικό σχήμα καταστάσεων του σύμφωνα με τα βασικά στοιχεία και τους κανόνες της παραγράφου 4.3.2.4.3.3.

   Η όψη πληροφορίας περιλαμβάνει και τους κανόνες προδιαγραφής στατικών σχημάτων αντικειμένων πληροφορίας στην παράγραφο 4.3.2.4.3.2, τα οποία χρησιμοποιούνται στα μετέπειτα στάδια της μεθοδολογίας.

Στο πέρας του βήματος (II), ο σχεδιαστής έχει ολοκληρώσει την πρώτη έκδοση της όψης πληροφορίας της αρχιτεκτονικής.

4.3.2.3 Προδιαγραφή Επιχειρησιακής Όψης

4.3.2.3.1 Εισαγωγή

Η επιχειρησιακή όψη σε μια ΑΔΑΑΥ περιλαμβάνει δύο θεμελιώδη στοιχεία, την γενική οργανωτική δομή της ΑΔΑΑΥ καθώς και τα οργανωτικά μοντέλα των υπηρεσιών και

εφαρμογών της. Στην όψη αυτή περιγράφεται το συνολικό περιβάλλον του συστήματος και ο σκοπός του. Επιπλέον, δίνονται οι απαιτήσεις για την αρχιτεκτονική, οι σχετικοί περιορισμοί, πράξεις που λαμβάνουν χώρα και ορίζονται οι πολιτικές ασφάλειας και επεξεργασίας απο επιχειρησιακή άποψη. Αυτό περιλαμβάνει τον ορισμό διαδικασιών, τους κανόνες που τις διέπουν καθώς και τους δράστες και τους ρόλους τους μέσα στις διαδικασίες.
Η αποτελεσματικότητα της εφαρμογής μεθοδολογιών πληροφορικής είναι άμεσα εξαρτώμενη απο την ολοκλήρωση όψεων. Αυτό σημαίνει ότι παρόλο που μια αρχιτεκτονική για ένα σύστημα έχει να κάνει με τεχνολογίες, αυτές δεν βγαίνουν στο προσκήνιο, αλλά το σύστημα και οι εφαρμογές του σε μια αρχιτεκτονική προσανατολισμένη στις υπηρεσίες περιγράφονται ως υπηρεσίες και διαδικασίες, και όχι ως τεχνικές λύσεις.
Οι υπηρεσίες περιγράφονται με τη μορφή μοντέλων διεργασιών. Αυτό σημαίνει ότι αναλύονται όλα τα βήματα της υπηρεσίας, απο την αρχή μέχρι το τέλος, όπως είναι για παράδειγμα η αναζήτηση απο τον πελάτη (πολίτη, επιχείρηση, δημόσιο οργανισμό κ.λ.π), η συμπλήρωση μιας φόρμας κ.ο.κ. Η παρούσα μεθοδολογία στόχο έχει στην επιχειρησιακή όψη να παρέχει τέτοια μοντέλα διεργασιών που αποτελούν κοινές υπηρεσίες σε ΑΔΑΑΥ, σε ένα επίπεδο με σχετικά υψηλό βαθμό αφαίρεσης, και να δώσει τους τρόπους επέκτασής τους, προκειμένου να μπορεί να προκύψει η ακριβής επιχειρησιακή όψη της προς σχεδιασμό αρχιτεκτονικής.

4.3.2.3.2 Έννοιες

Οι έννοιες που ορίζονται στο πρότυπο RM-ODP και χρησιμοποιούνται στη μεθοδολογία προδιαγραφής της επιχειρησιακής όψης είναι αυτές της παραγράφου 7.3.8.2.2.1.1.

4.3.2.3.3 Σημειογραφία

Στην παράγραφο αυτή καθορίζεται τι είδους διαγράμματα χρησιμοποιεί η μεθοδολογία για την αναπαράσταση των αντικειμένων της επιχειρησιακής όψης, και μπορούν να χρησιμοποιηθούν για την επέκταση της όψης. Όλα τα διαγράμματα βασίζονται στην UML.

- Διαγράμματα χρήσης (use case diagrams) χρησιμοποιούνται για την προδιαγραφή των λειτουργιών και στόχων του συστήματος.
- Διαγράμματα κλάσεων (class diagrams) και διαγράμματα συνεργασίας (collaboration diagrams) χρησιμοποιούνται για την περιγραφή ρόλων και τις σχέσεις αντικειμένων μέσα σε κοινότητες.
- Διαγράμματα δραστηριοτήτων (activity diagrams) ή διαγράμματα καταστάσεων (state machine diagrams) χρησιμοποιούνται για την περιγραφή διεργασιών.
- Η OCL ή φυσική γλώσσα χρησιμοποιείται για την περιγραφή πολιτικών και περιορισμών.

Οι παράγραφοι που ακολουθούν περιγράφουν πως χρησιμοποιείται η παραπάνω σημειογραφία ως μέρος της μεθοδολογίας.

4.3.2.3.3.1 Επιχειρησιακές λειτουργίες και συναρτήσεις

Σαν πρώτο βήμα απαιτείται η προδιαγραφή στο υψηλότερο επίπεδο των επιχειρησιακών στόχων που θα καλύψει η ΑΔΑΑΥ, για παράδειγμα η λήψη ενός εγγράφου απο έναν δημόσιο οργανισμό, η λήψη πληροφοριών απο μια βάση δεδομένων κ.λ.π.

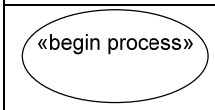
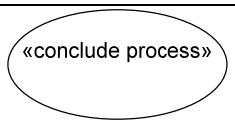
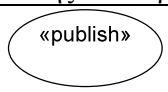
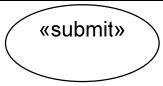
4.3.2.3.3.1.1 Μεθοδολογία προδιαγραφής

Η προδιαγραφή γίνεται με χρήση διαγραμμάτων χρήσης της UML. Κάθε επιχειρησιακός στόχος αναπαρίσταται με μια περίπτωση χρήσης (use case) της UML. Κάθε περίπτωση χρήσης συνοδεύεται απο αντικείμενα-δράστες (actors) οι οποίοι συμμετέχουν στην περίπτωση χρήσης κάνοντας διάφορες πράξεις, και ενδέχεται να προδιαγράφεται και ο ρόλος του κάθε δράστη. Παραδείγματα περιπτώσεων χρήσης που ενδέχεται να εμφανίζονται σε μια ΑΔΑΑΥ παρουσιάζονται στα βασικά στοιχεία και μπορούν να χρησιμοποιηθούν ως μέρος των προδιαγραφών. Κάθε διάγραμμα περιπτώσεων χρήσης συνοδεύεται απο μια υψηλού επιπέδου περιγραφή της επιχειρησιακής λειτουργίας που αναπαρίσταται στο διάγραμμα.

4.3.2.3.3.1.2 Βασικά στοιχεία όψης

Η παράγραφος αυτή περιέχει έτοιμα στοιχεία που μπορούν να χρησιμοποιηθούν ως μέρος των προδιαγραφών της επιχειρησιακής όψης. Όπως φαίνεται απο την προηγούμενη παράγραφο, αποτελούν στερεότυπα περιπτώσεων χρήσης [UML1.4] που απαντώνται συχνά σε μια ΑΔΑΑΥ με κάποια μορφή καθώς και στερεότυπα για αντικείμενα δράστες. Τα βασικά στοιχεία όψης με τη μορφή στερεοτύπων περιπτώσεων χρήσης της UML περιέχονται στον πίνακα που ακολουθεί:

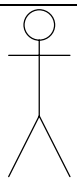
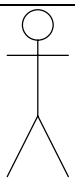
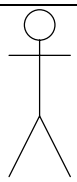
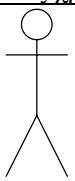
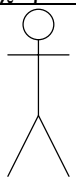
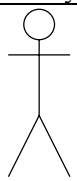
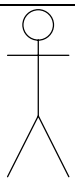
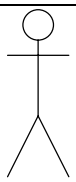
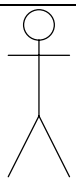
Πίνακας 4-1: Περιπτώσεις χρήσης / βασικά στοιχεία όψης για επιχειρησιακές λειτουργίες και συναρτήσεις

 Για την είσοδο ενός χρήστη σε ένα σύστημα.	 Για την έξοδο ενός χρήστη απο ένα σύστημα.	 Για την επιλογή μια επιχειρησιακής υπηρεσίας ή άλλης λειτουργίας.
 Για την εκκίνηση μιας διεργασίας.	 Για την περάτωση μιας διεργασίας.	 Για την δημοσίευση ενός αντικειμένου (εγγράφου κ.λ.π.)
 Για την διενέργεια ενός ελέγχου.	 Για την δημιουργία ενός αντικειμένου (εγγράφου, αίτησης κ.λ.π.)	 Για την αποστολή ενός αντικειμένου (εγγράφου, αίτησης κ.λ.π.)
 Για την αποθήκευση ενός αντικειμένου (εγγράφου, αίτησης κ.λ.π.)	 Για την εξέταση ενός αντικειμένου (εγγράφου, αίτησης κ.λ.π.)	 Για την έκδοση ενός αντικειμένου (εγγράφου, αίτησης κ.λ.π.)

«modify» Για την αλλαγή ενός αντικειμένου (εγγράφου, αίτησης κ.λ.π.).	«access registry» Για την πρόσβαση σε ένα αποθετήριο.	«perform query» Για την αποστολή ερωτήματος σε βάση δεδομένων και την λήψη απάντησης.
«administrate» Διαχείριση ενός αντικειμένου (πολιτικών ασφάλειας κ.λ.π.).	«forward» Για την προώθηση ενός αντικειμένου σε κατάλληλο παραλήπτη προς επεξεργασία.	«confirm reception» Για την επιβεβαίωση λήψης οποιουδήποτε μηνύματος.
«notify» Για την παροχή πληροφοριών κατάστασης ενός αντικειμένου ή διεργασίας.	«retrieve» Για την ανάκτηση ενός αντικειμένου (εγγράφου, αίτησης κ.λ.π.).	«activate» Για την ενεργοποίηση κάποιας δραστηριότητας.
«print» Για την εκτύπωση ενός εγγράφου.	«sign» Δημιουργία ψηφιακής υπογραφής.	«verify signature» Επαλήθευση ψηφιακής υπογραφής.
«authenticate» Αυθεντικοποίηση οντότητας.	«authorize» Πρόσβαση οντότητας βάσει ταυτότητας, χαρακτηριστικών και στοιχείων ελέγχου πρόσβασης.	«encrypt» Κρυπτογράφηση.
«decrypt» Αποκρυπτογράφηση.	«timestamp» Χρονοσφράγιση.	«deploy» Εγκατάσταση αντικειμένου ή υπηρεσίας,
«register» Για εγγραφή σε κάποια υπηρεσία ή σύστημα.	«receive» Για την λήψη κάποιου αντικείμενου.	

Τα αντίστοιχα βασικά στοιχεία όψης που έχουν τη μορφή δραστών της UML περιέχονται στον ακόλουθο πίνακα:

Πίνακας 4-2: Δράστες / βασικά στοιχεία όψης για επιχειρησιακές λειτουργίες και συναρτήσεις

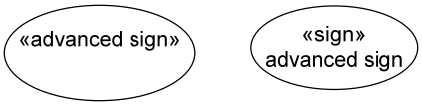
 «user» Για δράστη ο οποίος είναι απλός χρήστης.	 «administrator» Για δράστη ο οποίος είναι διαχειριστής συστήματος.	 «public organization» Για δράστη ο οποίος είναι δημόσιος οργανισμός.
 «citizen» Για δράστη ο οποίος είναι πολίτης.	 «employee» Για δράστη ο οποίος είναι υπάλληλος ενός οργανισμού.	 «enterprise» Για δράστη ο οποίος είναι μια εταιρία ή ιδιωτική επιχείρηση.
 «civil servant» Για δράστη ο οποίος είναι δημόσιος υπάλληλος.	 «IS» Για δράστη που αντιπροσωπεύει ένα πληροφοριακό σύστημα (information system).	 «TTP» Για δράστη που αποτελεί Έμπιστη Τρίτη Οντότητα - ΕΤΟ (Trusted Third Party - TTP).

Για κάθε περίπτωση χρήσης που δημιουργείται ως μέρος των προδιαγραφών, ελέγχεται εάν εμπίπτει στην γενική λογική κάποιου απο τα παραπάνω στερεότυπα. Αν εμπίπτει, τότε του δίνεται αυτό το στερεότυπο. Αν όχι, τότε ελέγχεται σύμφωνα με τους κανόνες επέκτασης αν πρέπει να δημιουργηθεί νέο στερεότυπο, το οποίο αποδίδεται στη νέα περίπτωση χρήσης.

4.3.2.3.3.1.3 Μεθοδολογία επέκτασης και παραδείγματα

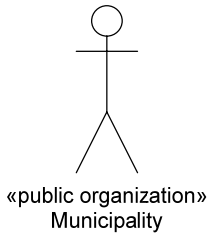
Τα βασικά στοιχεία της παραγράφου 4.3.2.3.3.1.2 μπορούν να επεκταθούν μόνο εάν το νέο στερεότυπο αποτελεί επίσης γενικευμένη επιχειρησιακή λειτουργία και δεν υπεισέρχεται σε τεχνικές λεπτομέρειες.

Για παράδειγμα, μια οντότητα ενδέχεται να θέλει να υπογράψει με προηγμένη ηλεκτρονική υπογραφή. Στην περίπτωση έχουμε την επιλογή είτε να δημιουργήσουμε ένα νέο στερεότυπο «Προηγμένη Υπογραφή» εάν πρόκειται να αποτελεί μια σημαντική επιχειρησιακή λειτουργία της ΑΔΑΑΥ ή απλά να δημιουργήσουμε τη νέα περίπτωση χρήσης με το ήδη υπάρχον βασικό στοιχείο «Υπογραφή» (Sign) εάν δεν αποτελεί γενική λειτουργία και απλά εμφανίζεται σε μια περίπτωση:



Σχήμα 4-9: Επιλογές επέκτασης βασικού στοιχείου

Ο ορισμός εντελώς νέων στερεοτύπων περιπτώσεων χρήσης ακολουθεί την λογική των βασικών στοιχείων και περιορίζεται μόνο στο ότι κάθε νέα περίπτωση πρέπει να αναφέρεται σε επιχειρησιακή λειτουργία. Η επέκταση στερεοτύπων δραστών ακολουθεί την ίδια λογική.
Ο απλός ορισμός ενός δράστη που αντιστοιχεί στην έννοια ενός δήμου δίνεται στο παράδειγμα του σχήματος που ακολουθεί:



Σχήμα 4-10: Παράδειγμα δράστη με χρήση του βασικού στοιχείου «δημόσιος οργανισμός»

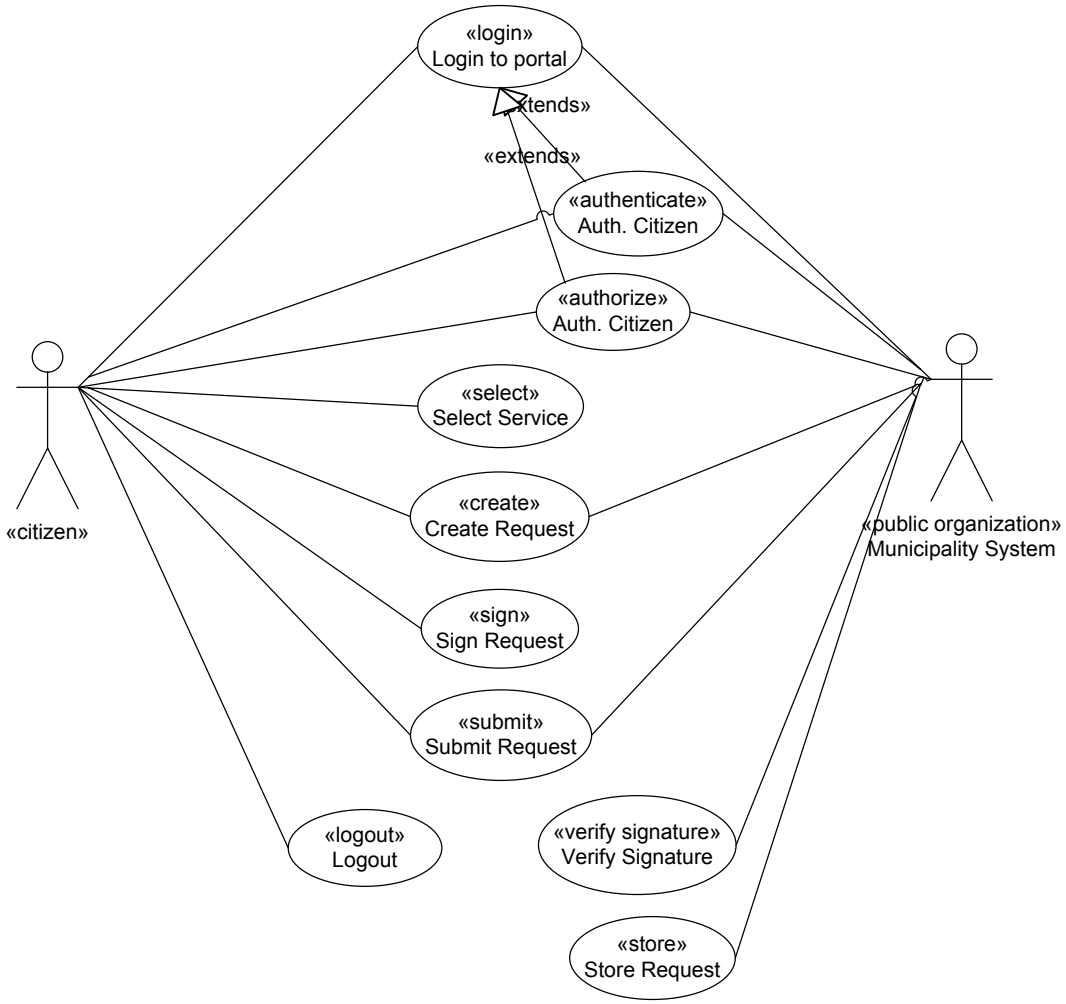
Όπως είναι φανερό ένας δήμος είναι ένας δημόσιος οργανισμός και άρα του αποδίδεται το σχετικό στερεότυπο.

Στο σημείο αυτό θα παρατεθεί ένα πιο πλήρες παράδειγμα των παραπάνω αρχών, για την ανάλυση σε αυτό το επίπεδο των προδιαγραφών μιας υπηρεσίας λήψης ενός ψηφιακού πιστοποιητικού γέννησης απο έναν δήμο.
Μια γενική περιγραφή της υπηρεσίας είναι η ακόλουθη:

«*Ένας **πολίτης** γνωρίζει την διαδικτυακή τοποθεσία του **δήμου** του, ο οποίος προσφέρει την **ηλεκτρονική υπηρεσία έκδοσης ενός ψηφιακού πιστοποιητικού γέννησης,** με προαιρετική **εκτύπωση** του εγγράφου. Ο πολίτης είναι **εγγεγραμμένος** στον δήμο και έχει λάβει μια **έξυπνη κάρτα** με **δύο ζεύγη κλειδιών** τα οποία μπορεί να χρησιμοποιεί για **αυθεντικοποίηση στον δήμο** και για την **υπογραφή ψηφιακών εγγράφων** (η έξυπνη κάρτα ενδέχεται να είναι και ηλεκτρονική ταυτότητα εκδιδόμενη απο το κράτος).*
*Αφότου επισκεφθεί τον δικτυακό τόπο του δήμο, ο πολίτης αυθεντικοποιείται μέσω της κάρτας του και επιλέγει την **υπηρεσία έκδοσης του πιστοποιητικού,** απο τις διαθέσιμες που του παρουσιάζονται βάσει του **ελέγχου πρόσβασης** με τα **διαπιστευτήριά** του. Εισάγει ένα σύνολο στοιχείων για την χρήση της υπηρεσίας (π.χ. ονοματεπώνυμο, ημερομηνία γέννησης, τύπος πιστοποιητικού), σε μια φόρμα **αίτησης** που του παρουσιάζεται, **υπογράφει την αίτηση** και την αποστέλλει.*
*Η **ΑΔΑΑΥ του δήμου** λαμβάνει την φόρμα μέσω των υπηρεσιών της και την **καταχωρεί**, μέχρι ένας **δημόσιος υπάλληλος**, ως μέρος των ημερήσιων καθηκόντων του, να την ζητήσει απο την υπηρεσία έκδοσης πιστοποιητικών. Ο δημόσιος υπάλληλος είναι επίσης εφοδιασμένος με μια **αντίστοιχη έξυπνη κάρτα**. Επίσης ο δήμος διαθέτει μια **κατάλληλη πολιτική υπογραφής** η οποία καθορίζει ότι ο δημόσιος υπάλληλος έχει την εξουσιοδότηση να υπογράφει εκπροσωπώντας τον δήμο.*

Ο δημόσιος υπάλληλος ελέγχει την αίτηση και ζητά απο την υπηρεσία να του επιστρέψει τα απαραίτητα ***στοιχεία*** *απο το* ***υπάρχον σύστημα του δήμου****, όπου είναι αποθηκευμένα τα στοιχεία των πιστοποιητικών γέννησης των εγγεγραμμένων πολιτών του δήμου.*
Τα στοιχεία ***ανακτώνται****, συντίθεται το* ***πιστοποιητικό*** *και* ***υπογράφεται απο τον δημόσιο υπάλληλο*** *ψηφιακά. Εάν έχει ζητηθεί, το πιστοποιητικό επίσης* ***εκτυπώνεται*** *και υπογράφεται και με τον παραδοσιακό τρόπο και αποστέλλεται ταχυδρομικώς. Στην συνέχεια αποστέλλεται μια* ***ειδοποίηση*** *στον πολίτη στο* ***ηλεκτρονικό του ταχυδρομείο****, προκειμένου να επανέλθει στο δικτυακό τόπο του δήμου και να λάβει το ψηφιακό ηλεκτρονικά υπογεγραμμένο πιστοποιητικό γέννησής του και να ενημερωθεί ότι θα το λάβει και εκτυπωμένο*.»

Οι λέξεις που έχουν σημειωθεί με έμφαση στο παραπάνω κείμενο δίνουν μια πρώτη εικόνα των σημαντικών δραστών που συμμετέχουν και επιχειρησιακών διαδικασιών και συναρτήσεων που ακολουθούνται στην συνολική διαδικασία, και που θα βοηθήσουν στην επιλογή των κατάλληλων βασικών στοιχείων της επιχειρησιακής όψης.
Μια πρώτη προσέγγιση των αντίστοιχων προδιαγραφών, για την χρονική στιγμή μέχρι την αποθήκευση της αίτησης του πολίτη, φαίνεται στο σχήμα που ακολουθεί:

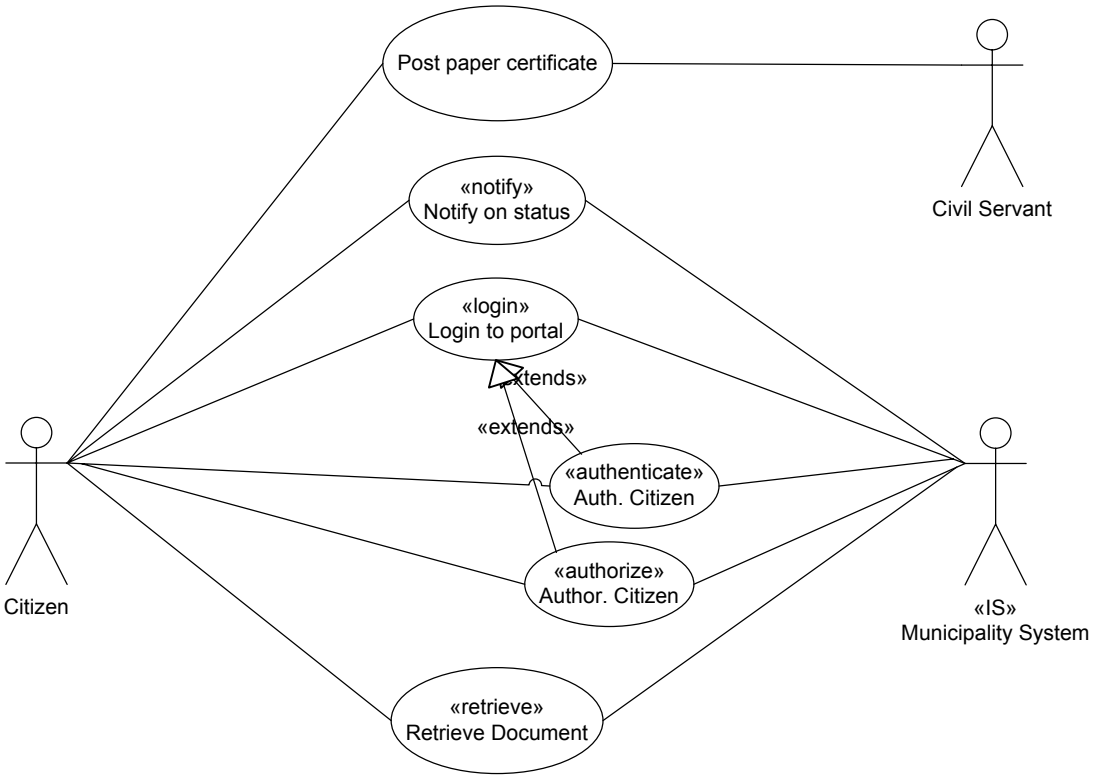


Σχήμα 4-11: Παράδειγμα προδιαγραφών για την συναλλαγή πολίτη-δήμου μέχρι την αποθήκευση της αίτησης

Στο Σχήμα 4-11 χρησιμοποιήθηκε ένα υποσύνολο των βασικών στοιχείων της προηγούμενης παραγράφου. Οι διαδικασίες αυθεντικοποίησης και ελέγχου πρόσβασης έχουν ενσωματωθεί στη διαδικασία εισόδου στο σύστημα, χρησιμοποιώντας τα κατάλληλα βέλη επέκτασης της UML. Κατόπιν των ελέγχων ασφάλειας, ο πολίτης επιλέγει την υπηρεσία που θέλει να χρησιμοποιήσει, δημιουργεί μια αίτηση σύμφωνα με τα δεδομένα που ζητά η υπηρεσία στο βήμα «Δημιουργία Αίτησης» (Create Request), την υπογράφει, και την αποστέλλει στην υπηρεσία στο βήμα «Αποστολή Αίτησης» (Submit Request). Απο το βήμα αυτό και ύστερα, ο πολίτης βγαίνει απο το σύστημα και το σύστημα του δήμου ελέγχει την υπογραφή και αποθηκεύει την αίτηση. Το επόμενο διάγραμμα, συνεχίζει το παράδειγμα, μέχρι να ολοκληρώσει την εργασία του ο δημόσιος υπάλληλος.

Σχήμα 4-12: Παράδειγμα προδιαγραφών συναλλαγής με τις δραστηριότητες του δημοσίου υπαλλήλου

Όπως φαίνεται στο σχήμα, ο δημόσιος υπάλληλος ακολουθεί μια παρόμοια με τον πολίτη διαδικασία προκειμένου να κάνει εισαγωγή στο σύστημα και να εκκινήσει την εργασία του. Στα πλαίσια της εργασίας αυτής ελέγχει αιτήσεις που έχει λάβει και για κάθε μια εκκινεί έναν έλεγχο στο υπάρχον σύστημα του δήμου (το οποίο εκπροσωπείται απο τον δράστη Existing System) προκειμένου να ψάξει για τα στοιχεία του συγκεκριμένου πολίτη, τα οποία θα μπουν στο ψηφιακό πιστοποιητικό γέννησης (Perform Query, Access Registry). Στη συνέχεια υπογράφει το πιστοποιητικό που εκδίδεται βάσει αυτών των στοιχείων, το εκτυπώνει εφόσον αυτό έχει ζητηθεί και εξέρχεται απο το σύστημα, το οποίο φροντίζει να αποθηκεύσει το υπογεγραμμένο έγγραφο.
Στη συνέχεια, ολοκληρώνεται η διαδικασία με το διάγραμμα που ακολουθεί:



Σχήμα 4-13: Παράδειγμα προδιαγραφών συναλλαγής με την λήψη του πιστοποιητικού απο τον πολίτη

Όπως φαίνεται στα τελευταία βήματα ο δημόσιος υπάλληλος υπογράφει με τον παραδοσιακό τρόπο και αποστέλλει ταχυδρομικώς την εκτυπωμένη μορφή του πιστοποιητικού. Ταυτόχρονα, ο πολίτης ειδοποιείται απο το σύστημα για να παραλάβει το πιστοποιητικό του, και εισέρχεται στο σύστημα όπως και πριν, προκειμένου να το κατεβάσει απο τον δικτυακό τόπο του δήμου.
Συνήθως στο υψηλό επίπεδο αυτό των προδιαγραφών, περιγράφεται ένα επιτυχές σενάριο συναλλαγής. Οι αναλυτικές προδιαγραφές που λαμβάνουν υπόψην και πιθανά λάθη ή αποτυχίες στην διαδικασία, υλοποιούνται σύμφωνα με τις αρχές της παραγράφου 4.3.2.3.3.3.

4.3.2.3.3.2 Κοινότητες, ρόλοι και σχέσεις αντικειμένων

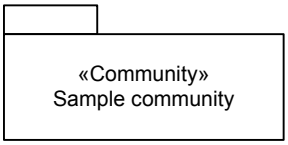
Κάθε ΑΔΑΑΥ περιλαμβάνει ένα σύνολο κοινοτήτων εντός της, και επικοινωνεί με κοινότητες εκτός της.

4.3.2.3.3.2.1 Μεθοδολογία προδιαγραφής

Σύμφωνα με τη μεθοδολογία, αρχικά οι κοινότητες και οι ρόλοι μπορούν να περιγραφούν συστηματικά με τη χρήση διαγραμμάτων κλάσεων. Αυτό σημαίνει ότι γίνεται ο διαχωρισμός των κοινοτήτων σύμφωνα με τον ορισμό της κοινότητας βάσει του RM-ODP και ομαδοποιούνται τα αντικείμενα που περιέχει. Κάθε αντικείμενο μέσα στην κοινότητα αναπαρίσταται απο μια κλάση της UML.
Πρότυπα στοιχεία της UML μπορούν να χρησιμοποιηθούν κατά βούληση για τις προδιαγραφές, όπως βέλη γενίκευσης (generalization) ή συσχετίσεως (association) κ.λ.π. Τα βέλη μπορούν να αναπαριστούν την *πολλαπλότητα (multiplicity)* των σχέσεων και οι ονομασίες που αποδίδονται στις άκρες των βελών αποδίδουν τους *ρόλους* που κάθε αντικείμενο λαμβάνει σε σχέση με άλλα. Τα όρια των κοινοτήτων καθορίζονται με πακέτα της UML.
Σε δεύτερο βήμα, οι σχέσεις των αντικειμένων δηλώνονται με διαγράμματα συνεργασίας, στα οποία εμφανίζονται όλες οι κλάσεις που έχουν ήδη δηλωθεί και φαίνεται με γραμμές συσχετίσεως UML (associations) ποια αντικείμενα έχουν σχέση με κάποια άλλα.

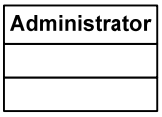
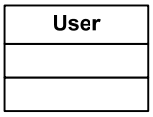
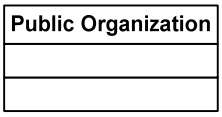
4.3.2.3.3.2.2 Βασικά στοιχεία όψης

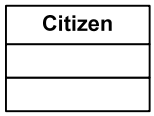
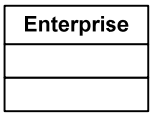
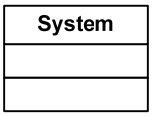
Τα επιχειρησιακά αντικείμενα των κοινοτήτων προκύπτουν απο τα αντικείμενα δράστες της παραγράφου 4.3.2.3.3.1 τα οποία ομαδοποιούνται μέσα σε πακέτα της UML για να αναπαρασταθούν οι κοινότητες. Τα αντικείμενα εδώ μετατρέπονται σε κλάσεις της UML προσδιορίζοντας τους ρόλους των επιχειρησιακών αντικειμένων ανάλογα με την κοινότητα που περιγράφεται.
Κάθε κοινότητα αναπαρίσταται όπως είπαμε με ένα πακέτο της UML που έχει το στερεότυπο «community»:



Βασικά στοιχεία εντός μιας τέτοια κοινότητας εδώ αποτελούν οι κλάσεις της UML στον πίνακα που ακολουθεί:

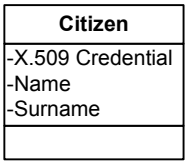
Πίνακας 4-3: Κλάσεις / βασικά στοιχεία όψης για επιχειρησιακές λειτουργίες και συναρτήσεις

 Για επιχειρησιακό αντικείμενο που αναπαριστά τον διαχειριστή συστήματος.	 Για επιχειρησιακό αντικείμενο που αναπαριστά τον χρήστη.	 Για επιχειρησιακό αντικείμενο που αναπαριστά τον δημόσιο οργανισμό.

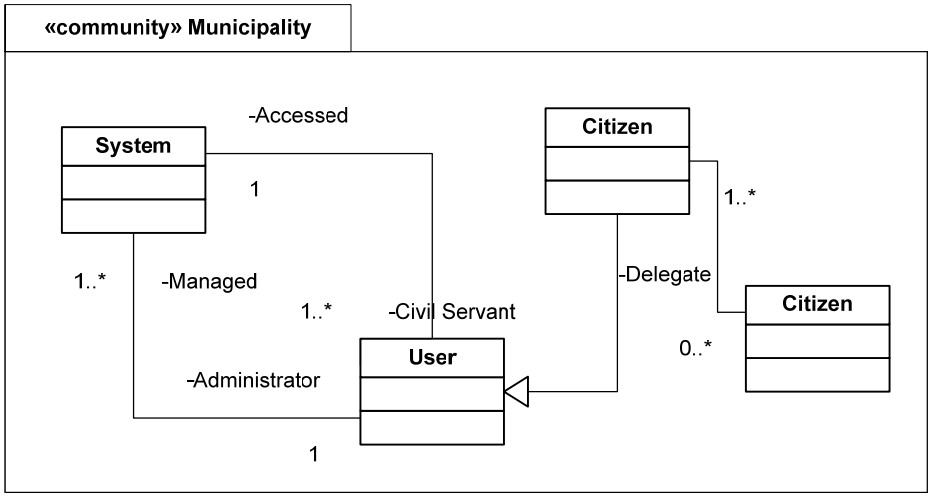
 Για επιχειρησιακό αντικείμενο που αναπαριστά τον πολίτη.	 Για επιχειρησιακό αντικείμενο που αναπαριστά την ιδιωτική επιχείρηση.	 Για ένα σύστημα.

4.3.2.3.3.2.3 Μεθοδολογία επέκτασης και παραδείγματα

Κάθε αντικείμενο επεκτείνεται με την προσθήκη περαιτέρω πληροφορίας με χαρακτηριστικά της UML (attributes) που προσδιορίζουν χαρακτηριστικά του. Για παράδειγμα, σε ένα αντικείμενο Πολίτη προστίθεται ο τύπος των διαπιστευτηρίων που χρησιμοποιεί και το ονοματεπώνυμό του:



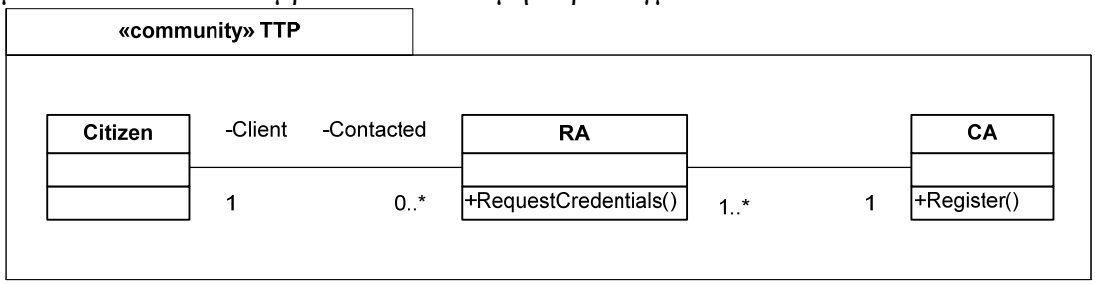
Όπως αναφέρθηκε στην προηγούμενη παράγραφο, τα αντικείμενα ενδέχεται να συνδέονται μεταξύ τους με βέλη γενίκευσης υποδεικνύοντας ότι το ένα είναι επέκταση του άλλου, ή με βέλη συσχέτισης ή εξάρτησης (dependency) κ.λ.π. χρησιμοποιώντας πρότυπη UML. Για παράδειγμα, αν θεωρήσουμε ότι μέσα στην κοινότητα του δήμου υπάρχει ένας γενικός «χρήστης» ο οποίος έχει ένα συγκεκριμένο σύνολο με ιδιότητες (π.χ. διαπιστευτήρια πρόσβασης στη σύστημα), τότε ένας πολίτης λαμβάνει τις ιδιότητες του χρήστη αλλά προσθέτει και κάποιες δικές του. Επίσης, ένας πολίτης μπορεί να έχει διάφορους εκπροσώπους (delegates) άλλους πολίτες που μπορούν να τον αντικαταστήσουν στις δραστηριότητες τους μέσα στον δήμο, όπως φαίνεται στο επόμενο σχήμα:



Σχήμα 4-14: Παράδειγμα κοινότητας και ρόλων

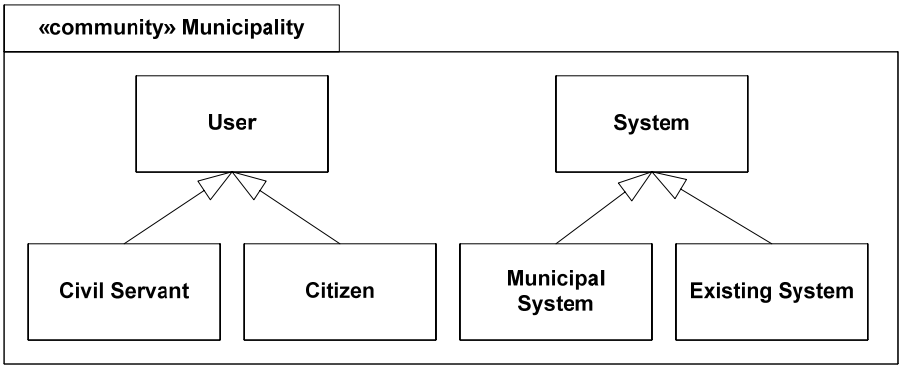
Όπως αναπαρίσταται, η γραμμή συσχέτισης ορίζει τον **ρόλο** του εκπροσώπου. Ένας εκπρόσωπος θα αναφέρεται τουλάχιστον σε έναν πολίτη, ενώ οποιοσδήποτε πολίτης

μπορεί να έχει άπειρους εκπροσώπους. Επιπρόσθετα, το σύστημα είναι προσβάσιμο (accessed) απο έναν χρήστη με τον **ρόλο** του Δημοσίου Υπαλλήλου (Civil Servant), και διαχειριζόμενο (managed) απο έναν χρήστη με τον **ρόλο** του Διαχειριστή (Administrator). Στο συγκεκριμένο παράδειγμα, ένας δημόσιος υπάλληλος μπορεί να έχει πρόσβαση σε ένα μόνο σύστημα, ενώ ένα σύστημα είναι προσβάσιμο απο πολλούς δημόσιους υπαλλήλους. Επίσης ένας διαχειριστής διαχειρίζεται πολλά συστήματα, ενώ ένα σύστημα είναι διαχειριζόμενο απο έναν και μόνο διαχειριστή. Για το σύνολο των προδιαγεγραμμένων επιχειρησιακών αντικειμένων δημιουργούνται παρόμοια διαγράμματα συνεργασίας επιδεικνύοντας ποια αντικείμενα συσχετίζονται και τον τρόπο με τον οποίο αυτό συμβαίνει. Ένα ακόμη παράδειγμα είναι το ακόλουθο:



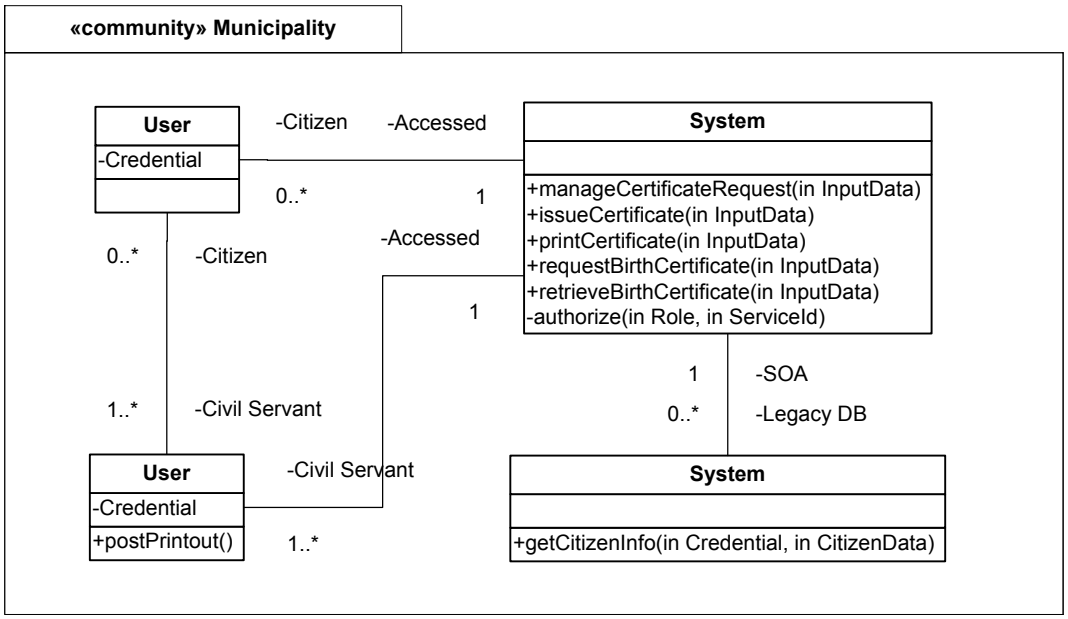
Σχήμα 4-15: Παράδειγμα διαγράμματος συνεργασίας μεταξύ επιχειρησιακών αντικειμένων

Στο παράδειγμα αυτό βλέπουμε πως ένας πολίτης σχετίζεται με μια Αρχή Εγγραφής εντός μιας κοινότητας Έμπιστων τρίτων οντοτήτων προκειμένου να αιτήσει ένα σύνολο διαπιστευτηρίων μέσω της προσφερόμενης μεθόδου RequestCredentials(). Η Αρχή Έγγραφής συνεργάζεται με την Αρχή Πιστοποίησης προκειμένου να εγγράψει τον πολίτη μέσω της μεθόδου Register().
Συνεχίζοντας το παράδειγμα της παραγράφου 4.3.2.3.3.1.3, η κοινότητα που περιλαμβάνει τις συμμετέχουσες οντότητες προδιαγράφεται στο σχήμα που ακολουθεί:



Σχήμα 4-16: Παράδειγμα επιχειρησιακών αντικειμένων για την κοινότητα Δήμος

Χρησιμοποιώντας τα βασικά στοιχεία της όψης, ο Πολίτης (Citizen) και ο Δημόσιος Υπάλληλος (Civil Servant) κληρονομούν τα χαρακτηριστικά του Χρήστη (User), ενώ το Πληροφοριακό Σύστημα του Δήμου (Municipal System) και η υπάρχουσα βάση δεδομένων (Existing System) κληρονομούν τα χαρακτηριστικά του Συστήματος (System). Επιπρόσθετα οι σχέσεις μεταξύ των αντικειμένων της κοινότητας διαφαίνονται στο ακόλουθο διάγραμμα συνεργασίας:



Σχήμα 4-17: Παράδειγμα διαγράμματος συνεργασίας για την κοινότητα Δήμος

Όπως φαίνεται ένας χρήστης με τον ρόλο του Πολίτη δημιουργεί αιτήσεις για πιστοποιητικά γέννησης στο δήμο μέσω του πληροφοριακού συστήματος και λαμβάνει τα πιστοποιητικά (βάσει των μεθόδων RequestBirthCertificate, RetrieveBirthCertificate), ενώ ο χρήστης με τον ρόλο του Δημοσίου υπαλλήλου ως μέρος της καθημερινής του εργασίας διαχειρίζεται τις αιτήσεις των πιστοποιητικών, δίνει τις εντολές για έκδοση των πιστοποιητικών και εκτυπώνει πιστοποιητικά (μέσω των μεθόδων ManageCertificateRequest, IsueCertificate, PrintCertificate). Το σύστημα ελέγχει την πρόσβαση των χρηστών σύμφωνα με την (ιδιωτική ως προς το αντικείμενο) μέθοδο ελέγχου πρόσβασης Authorize. Επιπρόσθετα, ο δημόσιος υπάλληλος αποστέλλει απευθείας στον πολίτη ταχυδρομικώς τα εκτυπωμένα πιστοποιητικά, εφόσον αυτό έχει ζητηθεί (όπως υποδεικνύει η μέθοδος PostPrintout). Τέλος, προκειμένου να δημιουργήσει τα πιστοποιητικά με τα σωστά στοιχεία, το πληροφοριακό σύστημα έρχεται σε επαφή με το υπάρχον σύστημα βάσης δεδομένων του δήμου (για να ζητήσει τα στοιχεία μέσω της μεθόδου GetCitizenInfo).

4.3.2.3.3.3 Διεργασίες

Κάθε επιχειρησιακός στόχος που έχει προδιαγραφεί στην παράγραφο 4.3.2.3.3.1 με διαγράμματα χρήσης, αναλύεται σε πιο λεπτομερείς επιμέρους διεργασίες που υλοποιούν το στόχο.

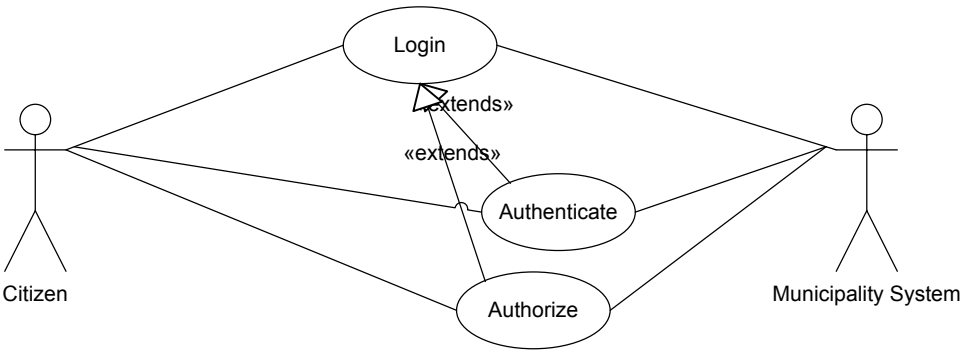
4.3.2.3.3.3.1 Μεθοδολογία προδιαγραφής

Η ανάλυση των διεργασιών γίνεται με διαγράμματα δραστηριοτήτων της UML, τα οποία απεικονίζουν τις δραστηριότητες στις οποίες συμμετέχουν τα αντικείμενα όλων των κοινοτήτων της παραγράφου 4.3.2.3.3.2. Ο αριθμός των διαγραμμάτων δραστηριοτήτων εξαρτάται απο τον αριθμό των διαγραμμάτων περιπτώσεων χρήσης και το επίπεδο της λεπτομέρειας που θέλουμε να αποδώσουμε. Στην περίπτωση που θέλουμε χαμηλό επίπεδο λεπτομέρειας, ένα διάγραμμα χρήσης περιλαμβάνει όσα περισσότερα διαγράμματα περιπτώσεων χρήσης γίνεται (με μέγιστο να υπάρχει ένα διάγραμμα

δραστηριοτήτων που περιλαμβάνει όλα τα διαγράμματα περιπτώσεων χρήσης, κάτι που όμως θα κάνει το διάγραμμα λιγότερο χρήσιμο και κατανοητό). Όταν θέλουμε υψηλό επίπεδο λεπτομέρειας, κάθε διάγραμμα δραστηριοτήτων περιλαμβάνει έναν μικρό αριθμό διαγραμμάτων περιπτώσεων χρήσης (με ελάχιστο κάθε διάγραμμα δραστηριοτήτων να περιγράφει στη μέγιστη λεπτομέρεια ένα και μόνο διάγραμμα περιπτώσεων χρήσης, οπότε και ο αριθμός των διαγραμμάτων δραστηριοτήτων είναι ο ίδιος με τον αριθμό των διαγραμμάτων περιπτώσεων χρήσης).
Η μεθοδολογία σε αυτό το σημείο δεν περιλαμβάνει βασικά στοιχεία διότι οι καταστάσεις που εμπεριέχει κάθε διεργασία είναι πολύ συγκεκριμένες και άρρηκτα δεμένες με τον συγκεκριμένο επιχειρησιακό στόχο. Οι δραστηριότητες που περιγράφονται είναι λεπτομερείς αναλύσεις των περιπτώσεων χρήσης που έχουν ήδη προδιαγραφεί και επιδεικνύουν πολλαπλές επιλογές ανάλογα με συγκεκριμένες συνθήκες.

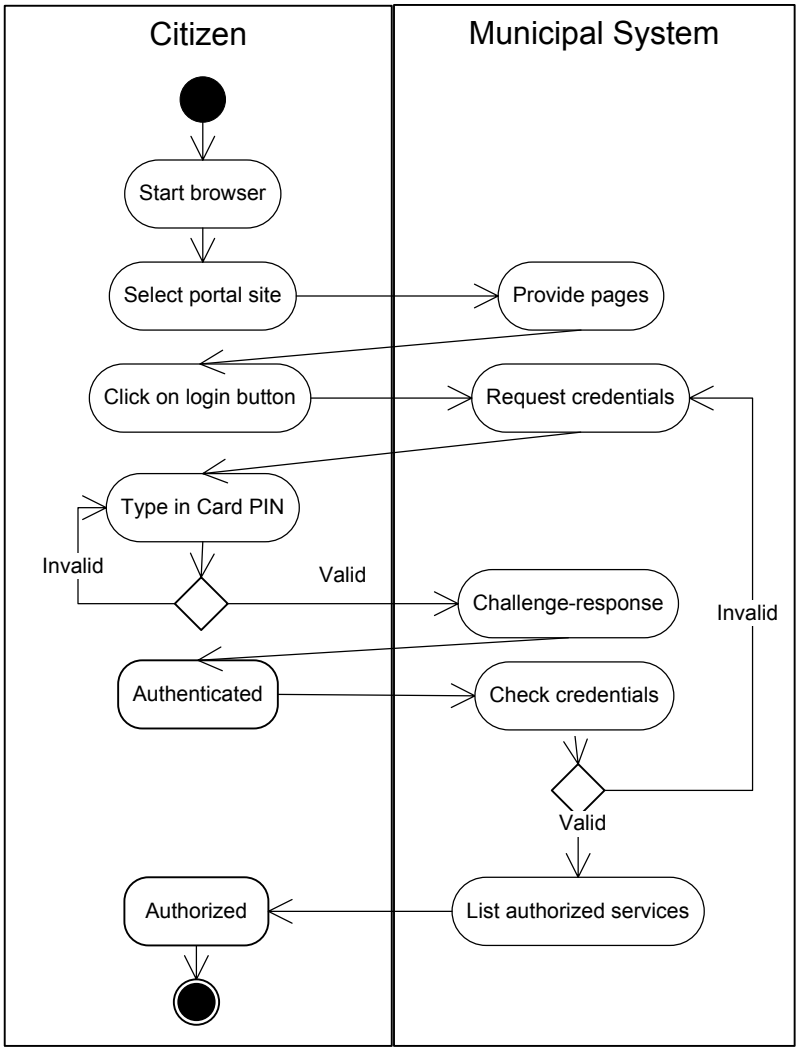
4.3.2.3.3.3.2 Παραδείγματα

Τα παραδείγματα που θα ακολουθήσουν βασίζονται στα διαγράμματα χρήσης και την κοινότητα «δήμος» που έχουμε ήδη δει στα παραδείγματα των προηγούμενων παραγράφων. Στην παρούσα παράγραφο θα αναλύσουμε περαιτέρω τις διαδικασίες που έχουν αναφερθεί στην υπηρεσία έκδοσης ενός πιστοποιητικού γέννησης και οι οποίες πιο συγκεκριμένα παρατέθηκαν στην παράγραφο 4.3.2.3.3.1.3. Οι διαδικασίες αυτές χωρίζονται σε μικρότερα υποσύνολα τα οποία σχεδιάζονται λεπτομερώς με διαγράμματα δραστηριοτήτων. Εάν ξεκινήσουμε με το παράδειγμα του διαγράμματος περιπτώσεων χρήσης που παρατίθεται στο Σχήμα 4-18,



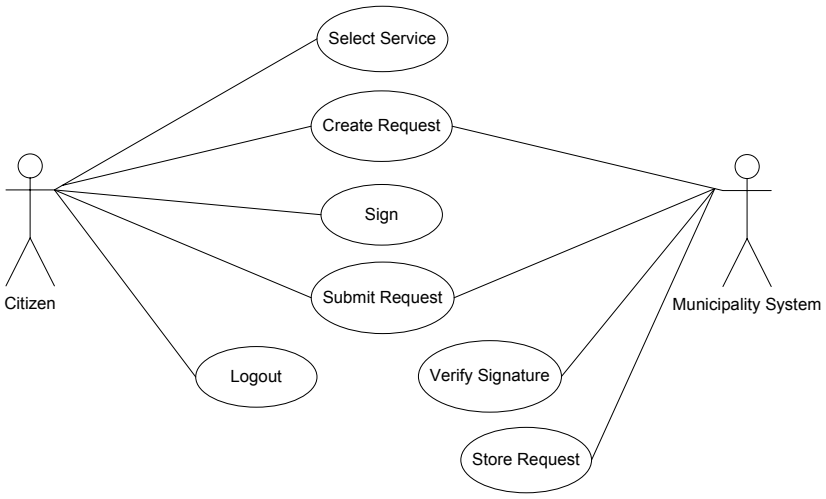
Σχήμα 4-18: Παράδειγμα διαγράμματος περιπτώσεων χρήσης για μια διαδικασία εισόδου στο σύστημα (login)

ένα πιθανό διάγραμμα δραστηριοτήτων που αυξάνει το επίπεδο λεπτομέρειας της διεργασίας είναι το ακόλουθο:



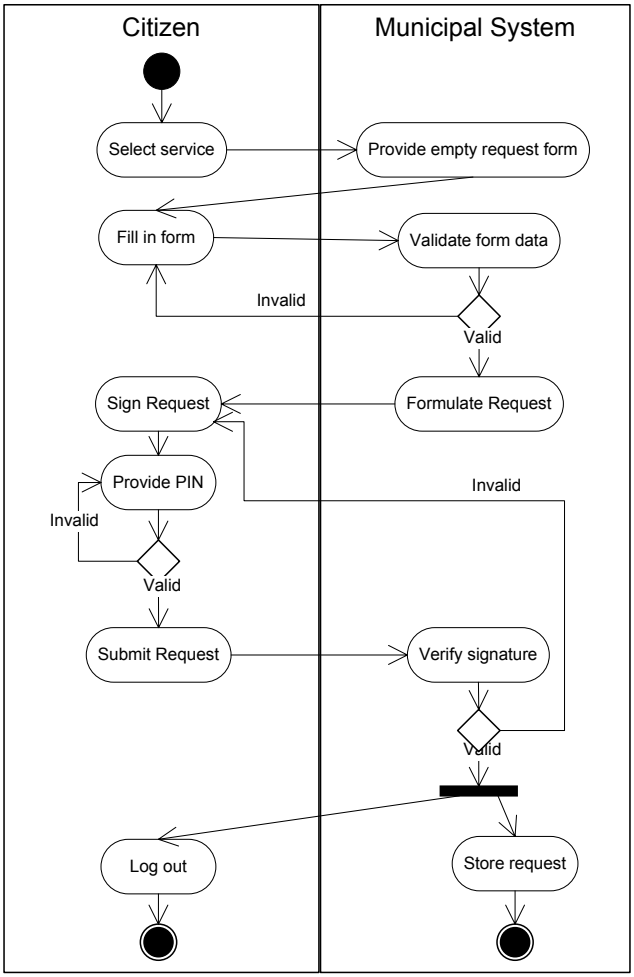
Σχήμα 4-19 : Διάγραμμα δραστηριοτήτων για το παράδειγμα του σχήματος Σχήμα 4-18

Όπως φαίνεται στο παραπάνω διάγραμμα, προκειμένου ο πολίτης να εισέρθει στο σύστημα επιλέγει την δικτυακή τοποθεσία του δήμου (select portal site), και το πληροφοριακό σύστημα του δήμου του επιστρέφει τις κατάλληλες σελίδες για είσοδο (provide pages). Ο πολίτης κάνει την κατάλληλη επιλογή εισόδου (click on login button) και στην συνέχεια το σύστημα του ζητά να αυθεντικοποιηθεί δίνοντας τα διαπιστευτήρια του, τα οποία βρίσκονται αποθηκευμένα στην έξυπνη κάρτα του (request credentials). Εκείνος δίνει τον κωδικό PIN προκειμένου η εφαρμογή πελάτης που χρησιμοποιεί να αποκτήσει πρόσβαση στο ιδιωτικό κλειδί και να υπογράψει τα απαραίτητα δεδομένα του πρωτοκόλλου αυθεντικοποίησης (challenge-response protocol). Μετά το πέρας του βήματος αυτού ο πολίτης έχει αυθεντικοποιηθεί. Τα στοιχεία του διασταυρώνονται με ήδη υπάρχοντα στο σύστημα και εάν ο έλεγχος είναι επιτυχής ο πολίτης εξουσιοδοτείται και του παρουσιάζονται οι κατάλληλες σελίδες επιλογής υπηρεσίας (list authorized services).
Η συνέχεια της διαδικασίας φαίνεται στο ακόλουθο διάγραμμα χρήσης:



Σχήμα 4-20: Παράδειγμα διαγράμματος χρήσης για την επιλογή υπηρεσίας και την αποστολή υπογεγραμμένης αίτησης

Το αναλυτικό διάγραμμα δραστηριοτήτων στην προκειμένη περίπτωση θα είναι:



Σχήμα 4-21: Διάγραμμα δραστηριοτήτων για το παράδειγμα του σχήματος Σχήμα 4-20

Όπως φαίνεται στην ανάλυση, ο πολίτης εφόσον έχει εξουσιοδοτηθεί, επιλέγει μια απο τις διαθέσιμες υπηρεσίες (select service) που στην προκειμένη περίπτωση είναι η υπηρεσία έκδοσης ψηφιακού πιστοποιητικού γέννησης. Το πληροφοριακό σύστημα του επιστρέφει την κατάλληλη άδεια φόρμα της αίτησης (provide empty request form) και ο πολίτης την συμπληρώνει με τα απαραίτητα στοιχεία (το ποια είναι αυτά τα στοιχεία θα αναλυθεί στο επόμενο στάδιο των προδιαγραφών, όπου θα γίνει ανάλυση των αντικειμένων πληροφορίας της δραστηριότητας). Το σύστημα ελέγχει τα δεδομένα που έχει συμπληρώσει ο χρήστης (validate request data) προκειμένου να αποφευχθούν λάθη και στη συνέχεια δημιουργεί την αίτηση προς υπογραφή (formulate request). Ο πολίτης, με μια παρόμοια διαδικασία με αυτή που ακολούθησε για την αυθεντικοποίηση, δίνει το PIN για την έξυπνη κάρτα του, υπογράφει (sign) και στέλνει την αίτηση (submit request). Εάν η υπογραφή είναι έγκυρη, η διαδικασία ολοκληρώνεται με την έξοδο του πολίτη απο το σύστημα (logout) και την αποθήκευση της αίτησης στο πληροφοριακό σύστημα (store request).
Το σύνολο των διαγραμμάτων δραστηριοτήτων που θα παραχθούν κατ' αυτόν τον τρόπο θα αναπαριστά όλες τις επιχειρησιακές δραστηριότητες που καλείται να καλύψει η σχεδιαζόμενη ΑΔΑΑΥ.

4.3.2.3.3.4 Πολιτικές

Οι επιχειρησιακοί στόχοι καθώς και οι διεργασίες στις οποίες αναλύονται, διέπονται απο ένα σύνολο πολιτικών. Μια πολιτική μπορεί να αποτελεί μια υποχρέωση, δικαίωμα ή απαγόρευση συσχετισμένη με κάποιο ρόλο και κάποιο αντικείμενο του συστήματος, ή ένα συγκεκριμένο συμβόλαιο ανάμεσα σε δύο επιχειρησιακά αντικείμενα.

4.3.2.3.3.4.1 Μεθοδολογία προδιαγραφής

Οι πολιτικές σύμφωνα με την παρούσα μεθοδολογία προδιαγράφονται είτε σε φυσική γλώσσα ή με την βοήθεια της επέκτασης της UML Object Constraints Language (OCL) [OCL], σε συνδυασμό με τα αντικείμενα που έχουν οριστεί στις κοινότητες της παραγράφου 4.3.2.3.3.2.
Οι πολιτικές και οι περιορισμοί που διέπουν το σύστημα καταγράφονται βάσει των απαιτήσεων του συστήματος και της περιγραφής των υπηρεσιών που πρόκειται να παραχθούν. Προκειμένου να αποφευχθούν αμφιβολίες στην ερμηνεία τους, θεωρείται καλή πρακτική να ενσωματώνονται στις προδιαγραφές με χρήση πιο συστηματικών γλωσσών όπως η OCL.

4.3.2.3.3.4.2 Παραδείγματα

Σαν συνέχεια του παραδείγματος της υπηρεσίας έκδοσης πιστοποιητικού γέννησης, αρχικά καταγράφονται οι ακόλουθες πολιτικές / περιορισμοί, σε φυσική γλώσσα:

1. Ο πολίτης που ζητά το πιστοποιητικό γέννησης θα πρέπει να αυθεντικοποιείται απο το σύστημα μετά την είσοδο του σε αυτό, και πριν την εκκίνηση της υπηρεσίας παραγωγής του πιστοποιητικού.
2. Ο πολίτης μπορεί να επιλέξει ανάμεσα σε ηλεκτρονική ή έντυπη αναπαράσταση του πιστοποιητικού, ή και τις δύο.

3. Η κάρτα κάθε χρήστη έχει δύο ζεύγη κλειδιών, ένα για ψηφιακή υπογραφή και ένα για αυθεντικοποίηση.
4. Η αυθεντικοποίηση κάθε χρήστη γίνεται μέσω της έξυπνης κάρτας του.
5. Ο έλεγχος πρόσβασης του χρήστη γίνεται βάσει των διαπιστευτηρίων στην κάρτα.
6. Ο πολίτης έχει πρόσβαση μόνο στην υπηρεσία έκδοσης ψηφιακών πιστοποιητικών γέννησης για αποστολή αίτησης και λήψη πιστοποιητικού.
7. Ο δημόσιος υπάλληλος έχει πρόσβαση μόνο στην υπηρεσία έκδοσης ψηφιακών πιστοποιητικών γέννησης για αποστολή αίτησης, λήψη πιστοποιητικού, έκδοσης πιστοποιητικού, εκτύπωση πιστοποιητικού.
8. Ο πολίτης πρέπει να υπογράφει ψηφιακά τις αιτήσεις που αποστέλλει.
9. Ο δημόσιος υπάλληλος πρέπει να υπογράφει ψηφιακά τα πιστοποιητικά που εκδίδει.
10. Ο δημόσιος υπάλληλος έχει πρόσβαση στα στοιχεία πολιτών του υπάρχοντος συστήματος μόνο μέσω της υπηρεσίας έκδοσης πιστοποιητικών.
11. Η έντυπη μορφή του πιστοποιητικού αποστέλλεται απο τον δημόσιο υπάλληλο στον πολίτη ταχυδρομικών εντός μιας εβδομάδας απο την έκδοση (και εκτύπωση) του.
12. Η έντυπη μορφή του πιστοποιητικού φέρει την κανονική σφραγίδα και υπογραφή του δήμου.

Όπως είναι φανερό, οι παραπάνω αποτελούν ένα σύνολο δηλώσεων παραδείγματα που απορρέουν απο την ανάλυση της περιγραφής της συγκεκριμένης υπηρεσίας στην παράγραφο 4.3.2.3.3.1.3.
Αν θέλουμε να δώσουμε ένα παράδειγμα σε OCL μπορούμε να θεωρήσουμε τις παραπάνω δηλώσεις πολιτικών 6 και 7. Βάσει του διαγράμματος στο Σχήμα 4-17, οι αντίστοιχες OCL δηλώσεις είναι οι ακόλουθες:

```
context System::authorize(role:Role, SID:ServiceId): Boolean
pre: role='civilservant' and Tuple { SID='manageCertificateRequest' or
SID='issueCertificate'       or       SID='printCertificate'       or
SID='requestBirthCertificate' or SID='retrieveBirthCertificate' }
post: result = true

context System::authorize(role:Role, SID:ServiceId): Boolean
pre: role='citizen' and Tuple { SID='requestBirthCertificate' or
SID='retrieveBirthCertificate' }
post: result = true
```

Η πρώτη απο τις παραπάνω δηλώσεις σε OCL αναπαριστά την πολιτική 7 και η δεύτερη την πολιτική 6.

4.3.2.4 Προδιαγραφή Όψης Πληροφορίας

4.3.2.4.1 Εισαγωγή

Η όψη αυτή καθορίζει την δομή και τη σημασιολογία των πληροφοριών που διακινούνται μέσα στο σύστημα. Επίσης περιλαμβάνει τον ορισμό των «πηγών»

πληροφορίας (αποστολέων) και «δεξαμενών» πληροφορίας (παραληπτών), καθώς και την επεξεργασία και μετασχηματισμό της πληροφορίας απο το σύστημα. Επιπρόσθετα περιγράφονται οι κανόνες ακεραιότητας και οι σταθερές.
Ο συνεπής ορισμός διεργασιών απαιτεί την χρησιμοποίηση γενικευμένων ορισμών δεδομένων για τις σημαντικές οντότητες και για τα δεδομένα που ανταλλάσσονται μεταξύ διεργασιών, εφαρμογών και υπηρεσιών. Η όψη πληροφορίας μοντελοποιεί τα δεδομένα και τις σχέσεις τους. Οι *οντότητες δεδομένων (data entities)* αναπαριστούν έννοιες στον τομέα του προβλήματος που καλείται να λύσει η ΑΔΑΑΥ και οι σχέσεις αναπαριστούν σχέσεις ανάμεσα στις έννοιες του προβλήματος. Το μοντέλο καθορίζει επί της ουσίας το λεξιλόγιο που χρησιμοποιείται για την περιγραφή του προβλήματος και αναπαριστά την δομή των αντικειμένων και τις βάσεις δεδομένων που χρησιμοποιούνται για την αναπαράσταση επιχειρησιακών εννοιών στους υπολογιστές.

4.3.2.4.2 Έννοιες

Οι έννοιες που ορίζονται στο πρότυπο RM-ODP και χρησιμοποιούνται στη μεθοδολογία προδιαγραφής της όψης πληροφορίας είναι αυτές της παραγράφου 7.3.8.2.2.1.2.

4.3.2.4.3 Σημειογραφία

Στην παράγραφο αυτή καθορίζεται τι είδους διαγράμματα χρησιμοποιεί η μεθοδολογία για την αναπαράσταση των αντικειμένων της όψης πληροφορίας, και μπορούν να χρησιμοποιηθούν για την επέκταση της όψης και πως ακριβώς χρησιμοποιούνται για το σκοπό αυτό. Τα διαγράμματα βασίζονται στην UML. Για την περιγραφή των σταθερών, στατικών και δυναμικών σχημάτων χρησιμοποιούνται διαγράμματα κλάσεων και διαγράμματα καταστάσεων. Οι παράγραφοι που ακολουθούν περιγράφουν πως χρησιμοποιείται η παραπάνω σημειολογία ως μέρος της μεθοδολογίας.

4.3.2.4.3.1 Σταθερό σχήμα

Για την προδιαγραφή ενός σταθερού σχήματος χρησιμοποιούνται διαγράμματα κλάσεων. Οι κλάσεις αναπαριστούν τα αντικείμενα πληροφορίας που δημιουργούνται, υπόκεινται επεξεργασία, μεταφέρονται και αποθηκεύονται στην ΑΔΑΑΥ. Οι κλάσεις και τα χαρακτηριστικά τους στο σταθερό σχήμα αποτελούν πάγια χαρακτηριστικά ενός αντικειμένου πληροφορίας τα οποία μένουν αναλλοίωτα ανεξάρτητα απο την κατάσταση στην οποία ενδέχεται να βρεθεί εντός του κύκλου ζωής του.

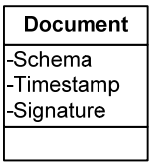
4.3.2.4.3.1.1 Μεθοδολογία προδιαγραφής

Το πρώτο βήμα της μεθοδολογίας είναι να αναγνωριστούν τα αντικείμενα πληροφορίας που απαιτούνται στο σύστημα, να καταγραφούν και να περιγραφούν ως κλάσεις σε σταθερό σχήμα, αναπαριστώντας μια αφαίρεση της οντότητας που πραγματικά δημιουργείται μέσα σε ένα σύστημα. Αυτά επιλέγονται απο τα βασικά στοιχεία όψης που περιγράφονται στη συνέχεια ή δημιουργούνται καινούργιες κλάσεις που αναπαριστούν πιο εξειδικευμένα αντικείμενα πληροφορίας ως επεκτάσεις των βασικών στοιχείων ή εντελώς νέα αντικείμενα.

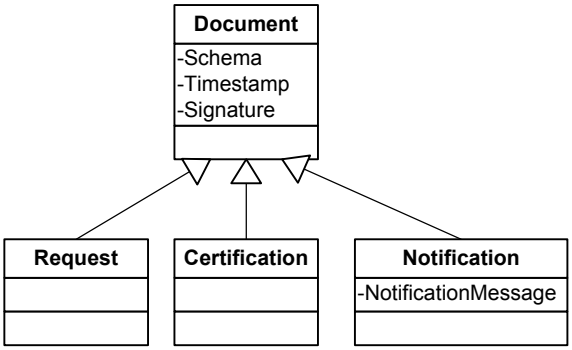
4.3.2.4.3.1.2 Βασικά στοιχεία όψης

Τα βασικά στοιχεία όψης στο στάδιο αυτό αποτελούν αντικείμενα πληροφορίας που είναι πιθανόν να απαιτούνται σε μια ΑΔΑΑΥ. Είναι τα ακόλουθα:

4.3.2.4.3.1.2.1 Έγγραφο



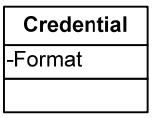
Αντικείμενο πληροφορίας που αναπαριστά ένα έγγραφο με νομική υπόσταση για την ΑΔΑΑΥ. Η δομή του εγγράφου βασίζεται σε ένα συγκεκριμένο σχήμα (schema)[2]. Προκειμένου να ικανοποιείται η απαίτηση για νομική υπόσταση των εγγράφων θα πρέπει να περιέχουν μια χρονοσφραγίδα και μια υπογραφή [ETSI101733].
Επαναχρησιμοποιήσιμα βασικά στοιχεία όψης που είναι απόγονοι του εγγράφου είναι τα αντικείμενα πληροφορίας που αναπαριστούν ένα έγγραφο πιστοποίησης, ένα έγγραφο αίτησης και ένα έγγραφο ειδοποίησης όπως φαίνεται στο ακόλουθο διάγραμμα:



Σχήμα 4-22: Απόγονοι του βασικού στοιχείου «Έγγραφο»

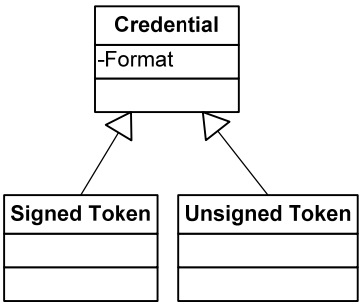
Η Πιστοποίηση (Certification) βεβαιώνει μια δήλωση εκ μέρους της οντότητας που την εκδίδει. Η Αίτηση (Request) συμπληρώνεται με τα απαιτούμενα στοιχεία για την εκπλήρωση μιας υπηρεσίας. Η Ειδοποίηση (Notification) χρησιμοποιείται για την μονόδρομη αποστολή ενός είδους πληροφορίας απο έναν αποστολέα σε έναν παραλήπτη και περιέχει ένα Μήνυμα Ειδοποίησης (NotificationMessage) το οποίο δίνει πληροφορίες για οποιοδήποτε θέμα στον παραλήπτη.

4.3.2.4.3.1.2.2 Διαπιστευτήριο



Αντικείμενο πληροφορίας που αναπαριστά ένα είδος διαπιστευτηρίου. Χαρακτηρίζεται απο μια μορφή. Ένα διαπιστευτήριο μπορεί να είναι υπογεγραμμένο ή μη-υπογεγραμμένο:

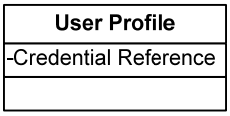
[2] Η λέξη «σχήμα» εδώ έχει να κάνει αυστηρά με τη δομή του εγγράφου και δεν πρέπει να συγχέεται με τα στατικά, δυναμικά και σταθερά σχήματα του RM-ODP.



Σχήμα 4-23: Απόγονοι του στοιχείου «Διαπιστευτήριο»

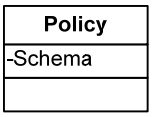
Ένα μη-υπογεγραμμένο διαπιστευτήριο δεν περιέχει κρυπτογραφική πληροφορία όπως είναι για παράδειγμα ο συνδυασμός ονόματος χρήστη / κωδικού (login / password). Ένα υπογεγραμμένο διαπιστευτήριο φέρει μια υπογραφή βάσει κρυπτογραφίας όπως είναι για παράδειγμα ένα εισιτήριο Kerberos [Neuman94] ή ένα πιστοποιητικό X509 [Housley02].

4.3.2.4.3.1.2.3 Προφίλ χρήστη



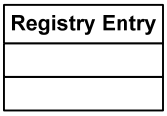
Αντικείμενο πληροφορίας που αναπαριστά μια δομή με στοιχεία ενός συγκεκριμένου χρήστη. Τα στοιχεία αυτά καθορίζονται απο τον σκοπό χρήσης του προφίλ αλλά εμπεριέχουν πάντα μια αναφορά σε ένα ή περισσότερα διαπιστευτήρια για λόγους αυθεντικοποίησης και ελέγχου πρόσβασης.

4.3.2.4.3.1.2.4 Πολιτική



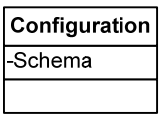
Αντικείμενο πληροφορίας που αναπαριστά μια πολιτική που εφαρμόζεται στην ΑΔΑΑΥ. Η δομή της πολιτικής και των κανόνων που ορίζει βασίζονται σε ένα συγκεκριμένο σχήμα.

4.3.2.4.3.1.2.5 Εγγραφή



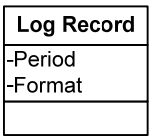
Αντικείμενο πληροφορίας που αναπαριστά μια εγγραφή σε ένα αποθετήριο πληροφορίας (για παράδειγμα μια βάση δεδομένων).

4.3.2.4.3.1.2.6 Αρχείο διαμόρφωσης



Αντικείμενο πληροφορίας που αναπαριστά ένα σύνολο παραμέτρων που χρησιμοποιούνται απο μηχανισμούς ή υπηρεσίες της αρχιτεκτονικής. Η δομή του βασίζεται σε ένα συγκεκριμένο σχήμα.

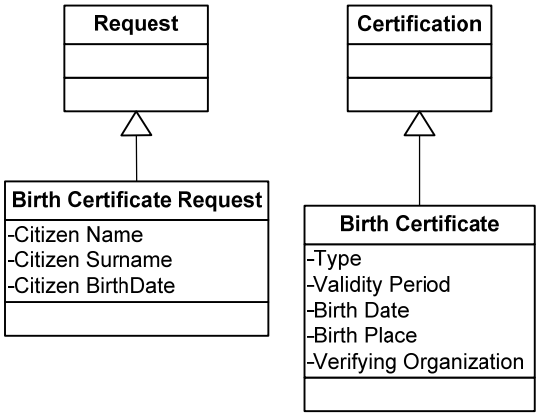
4.3.2.4.3.1.2.7 Αρχείο καταγραφής



Αντικείμενο πληροφορίας που αναπαριστά ένα σύνολο καταγεγραμμένων συμβάντων που λαμβάνουν χώρα στα διάφορα σημεία της αρχιτεκτονικής. Η δομή του βασίζεται σε μια συγκεκριμένη μορφή και έχει πάντα προδιαγεγραμμένη διάρκεια ζωής. Το τι πληροφορία περιέχει και σε τι καταστάσεις μεταπίπτει αφότου λήξει η διάρκεια ζωής του καθορίζεται απο μια πολιτική.

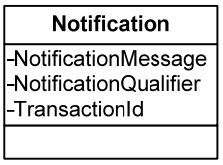
4.3.2.4.3.1.3 Μεθοδολογία επέκτασης και παραδείγματα

Τα αντικείμενα πληροφορίας επεκτείνονται αρχικά με την παραγωγή κλάσεων «παιδιών» των κλάσεων των βασικών στοιχείων, προκειμένου να παραχθούν σταθερά σχήματα αντικειμένων που περιέχουν πιο εξειδικευμένη πληροφορία και αναπαριστούν πιο συγκεκριμένα αντικείμενα πληροφορίας που απαντώνται στις συναλλαγές των υπηρεσιών της σχεδιαζόμενης αρχιτεκτονικής.
Στη συνέχεια κάθε αντικείμενο πληροφορίας σε σταθερό σχήμα επεκτείνεται ως προς τα χαρακτηριστικά του (attributes). Προστίθενται νέα χαρακτηριστικά τα οποία είναι συγκεκριμένα για το συγκεκριμένο πεδίο εφαρμογής της σχεδιαζόμενης ΑΔΑΑΥ και τις υπηρεσίες που καλείται να υποστηρίξει.
Συνεχίζοντας τα παραδείγματα της επιχειρησιακής όψης για την παραγωγή των προδιαγραφών της υπηρεσίας έκδοσης πιστοποιητικού γέννησης, βλέπουμε ότι το σύνολο των αντικειμένων πληροφορίας που απαιτούνται για την συγκεκριμένη υπηρεσία είναι τα ακόλουθα:
Δύο νέα αντικείμενα που αναπαριστούν την αίτηση για το πιστοποιητικό και το ίδιο το έγγραφο «πιστοποιητικό γέννησης», τα οποία επεκτείνουν τα βασικά στοιχεία όψης Αίτηση και Πιστοποίηση, όπως φαίνεται στο Σχήμα 4-24:



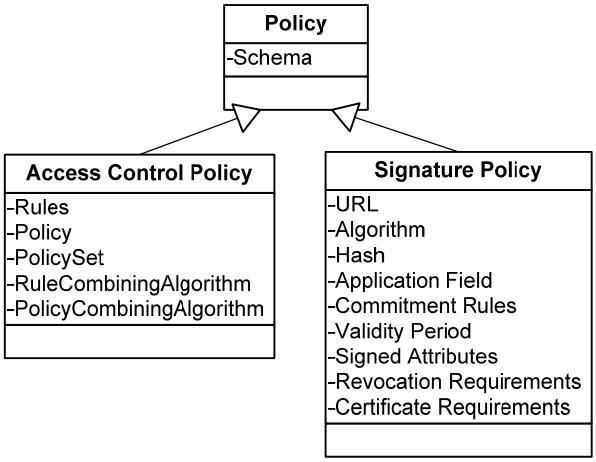
Σχήμα 4-24: Παραδείγματα επέκτασης των βασικών στοιχείων Αίτηση και Πιστοποίηση

Σημειώνεται εδώ ότι μια Αίτηση Πιστοποιητικού Γέννησης (Birth Certificate Request) και ένα Πιστοποιητικό Γέννησης (Birth Certificate) κληρονομούν όλα τα χαρακτηριστικά των κλάσεων απο τις οποίες προέρχονται. Αυτό σημαίνει ότι οι δομές τους περιγράφονται απο συγκεκριμένα σχήματα (που κατά πάσα πιθανότητα είναι επεκτάσεις των αντίστοιχων σχημάτων των κλάσεων «γονέων») και φέρουν υπογραφές του αιτούντα και του εκδότη αντίστοιχα.
Επίσης έχουν επεκταθεί με τα επιπρόσθετα χαρακτηριστικά που είναι απαραίτητα για την συγκεκριμένη υπηρεσία. Για παράδειγμα το πιστοποιητικό γέννησης φέρει την ημερομηνία γέννησης του αιτούντα, τον τόπο γέννησης και το όνομα του οργανισμού που τα πιστοποιεί (στην προκειμένη περίπτωση ο συγκεκριμένος Δήμος που το εκδίδει), τον τύπο και μια περίοδο ισχύος κ.ο.κ.
Άλλα βασικά στοιχεία σε σταθερό που χρειάζονται στην υπηρεσία έκδοσης του πιστοποιητικού γέννησης σύμφωνα με την περιγραφή της παραγράφου 4.3.2.3.3.1.3, είναι μια επέκταση της Ειδοποίησης με χαρακτηριστικά ως εξής:



Σχήμα 4-25: Επέκταση των χαρακτηριστικών του βασικού στοιχείου Ειδοποίηση

Το Αναγνωριστικό Ειδοποίησης (NotificationQualifier) χαρακτηρίζει το είδος της ειδοποίησης με έναν κωδικό (π.χ. κωδικός για επιτυχημένη έκδοση πιστοποιητικού κ.λ.π.), ενώ το Αναγνωριστικό Συναλλαγής (TransactionId) περιέχει τον κωδικό της συναλλαγής λόγω της οποίας δημιουργήθηκε η συγκεκριμένη ειδοποίηση. Επιπρόσθετα στο συγκεκριμένο παράδειγμα, σημαντικό ρόλο παίζουν οι επεκτάσεις του βασικού στοιχείου Πολιτική, όπως αυτές ορίζονται στο :



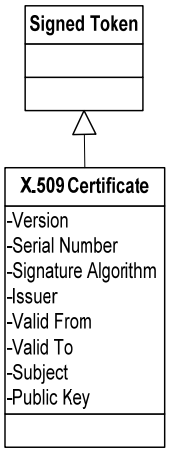
Σχήμα 4-26: Επεκτάσεις βασικού στοιχείου Πολιτική

Οι επεκτάσεις αυτές ορίζουν δύο αντικείμενα πολιτικών: μια Πολιτική Ελέγχου Πρόσβασης (Access Control Policy) και μια Πολιτική Υπογραφής (Signature Policy). Η πολιτική ελέγχου πρόσβασης θα χρησιμοποιηθεί απο την αντίστοιχη υπηρεσία της

αρχιτεκτονικής προκειμένου να αποφανθεί αν ο πολίτης δικαιούνται πρόσβαση στο σύστημα και ποιες υπηρεσίες μπορεί να χρησιμοποιήσει. Αποτελείται απο διάφορους κανόνες και επιμέρους πολιτικές (Rules, Policies, Policy Sets) τα οποία συνδυάζονται βάσει συνδυαστικών αλγορίθμων (RuleCombiningAlgorithm, PolicyCombiningAlgorithm) προκειμένου να ληφθούν αποφάσεις ελέγχου πρόσβασης πάνω σε πόρους.

Η πολιτική υπογραφής καθορίζει το πλαίσιο σύμφωνα με το οποίο ο δήμος δέχεται υπογεγραμμένες αιτήσεις και εκδίδει υπογεγραμμένα πιστοποιητικά γέννησης. Η πολιτική αυτή θα πρέπει να είναι δημοσιευμένη κάπου ώστε να μπορούν να την δουν (URL) και οι πολίτες που χρησιμοποιούν την υπηρεσία και το αναγνωριστικό της (το οποίο προκύπτει εφαρμόζοντας έναν αλγόριθμο κατακερματισμού (Algorithm) για την λήψη ενός Hash), θα πρέπει να ενσωματώνεται σε κάθε υπογεγραμμένο πιστοποιητικό γέννησης. Πιθανά χαρακτηριστικά της που φαίνονται στο παράδειγμα περιλαμβάνουν το Πεδίο Εφαρμογής (Application Field), τους Κανόνες Δέσμευσης (Commitment Rules) στην χρήση της υπηρεσίας, τα Χαρακτηριστικά που υπογράφονται σε κάθε πιστοποιητικό (Signed Attributes), τις απαιτήσεις για ενσωμάτωση δεδομένων ανακληθέντων πιστοποιητικών (Revocation Requirements) και τις απαιτήσεις απο τα πιστοποιητικά (ασφάλειας) που χρησιμοποιούνται για τις υπογραφές (Certificate Requirements). Για παράδειγμα μπορεί να είναι επιτρεπτά μόνο πιστοποιητικά που έχουν εκδοθεί απο μια συγκεκριμένη Αρχή Πιστοποίησης με συγκεκριμένο μήκος κλειδιών και συγκεκριμένες επεκτάσεις πιστοποιητικού.

Άλλα αντικείμενα πληροφορίας που χρειάζεται η υπηρεσία έκδοσης πιστοποιητικών γέννησης είναι τα ίδια τα διαπιστευτήρια που χρησιμοποιούνται. Στην προκειμένη υπηρεσία θεωρούμε ότι οι απαιτήσεις της υπηρεσίας καλύπτονται απο πιστοποιητικά X.509, τα οποία είναι επεκτάσεις των υπογεγραμμένων διαπιστευτηρίων:



Σχήμα 4-27: Ένα πιστοποιητικό X.509 ως επέκταση ενός υπογεγραμμένου διαπιστευτηρίου

Το πιστοποιητικό X.509 είναι ένα υπογεγραμμένο (απο μια Αρχή Πιστοποίησης) διαπιστευτήριο, με ένα σύνολο βασικών χαρακτηριστικών. Στο παράδειγμα της υπηρεσίας έκδοσης πιστοποιητικών γέννησης χρησιμοποιείται ως μέσο αυθεντικοποίησης.

Εντελώς νέα αντικείμενα πληροφορίας (τα οποία δεν έχουν σχέση με τα βασικά στοιχεία) είναι επίσης δυνατόν να δημιουργηθούν και να επεκταθούν σύμφωνα με τα παραπάνω και την λογική της παραγράφου 4.3.2.4.3.1.1.

4.3.2.4.3.2 Στατικό σχήμα

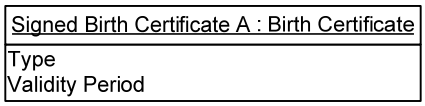
Το στατικό σχήμα ενός αντικειμένου πληροφορίας είναι άρρηκτα δεμένο με το σταθερό με την έννοια ότι αποτελεί ένα στιγμιότυπο του σταθερού υπο συγκεκριμένες συνθήκες και σε μια δεδομένη χρονική στιγμή. Υπόκειται φυσικά σε όλους τους περιορισμούς που προδιαγράφει το σταθερό σχήμα.

4.3.2.4.3.2.1 Μεθοδολογία προδιαγραφής

Ένα στατικό σχήμα προκύπτει ως στιγμιότυπο (instance) μιας κλάσης του σταθερού σχήματος που χρησιμοποιείται οπουδήποτε απαιτείται στις προδιαγραφές για να αναπαραστήσει ένα αντικείμενο πληροφορίας σε μια συγκεκριμένη κατάσταση.
Η μεθοδολογία δεν περιλαμβάνει βασικά στοιχεία όψης σε στατικό σχήμα, διότι όλα τα βασικά στοιχεία όψης της παραγράφου 4.3.2.4.3.1.2 μπορούν ανάλογα με τις ανάγκες σχεδιασμού να βρεθούν σε συγκεκριμένες καταστάσεις και άρα να γίνουν αντικείμενα (objects) της UML στιγμιότυπα των αντίστοιχων κλάσεων. Τα στατικά σχήματα αντικειμένων πληροφορίας χρησιμοποιούνται κατά το 4^{ο} στάδιο της μεθοδολογίας για τις προδιαγραφές των στοιχείων λογισμικού.

4.3.2.4.3.2.2 Παραδείγματα

Συνεχίζοντας τα παραδείγματα της παραγράφου 4.3.2.4.3.1.3, αν θέλουμε να αναπαραστήσουμε ένα συγκεκριμένο Πιστοποιητικό Γέννησης το οποίο μόλις έχει υπογραφεί μπορούμε να χρησιμοποιήσουμε το ακόλουθο στατικό σχήμα με αντικείμενο UML:



Σχήμα 4-28: Παράδειγμα στατικού σχήματος αντικειμένου πληροφορίας

Όπως φαίνεται στο παράδειγμα, το στατικό σχήμα του συγκεκριμένου υπογεγραμμένου Πιστοποιητικού Γέννησης Α είναι στιγμιότυπο της κλάσης Πιστοποιητικό Γέννησης και θα πρέπει να έχει συμπληρωμένο το χαρακτηριστικό Υπογραφή (Signature) που κληρονομεί απο την κλάση Έγγραφο.

4.3.2.4.3.3 Δυναμικό σχήμα

Το δυναμικό σχήμα ενός αντικειμένου πληροφορίας περιγράφει τις καταστάσεις στις οποίες μπορεί να βρεθεί το αντικείμενο μέσα στον κύκλο ζωής του.

4.3.2.4.3.3.1 Μεθοδολογία προδιαγραφής

Ένα δυναμικό σχήμα χρησιμοποιεί διαγράμματα καταστάσεων της UML για να προδιαγράψει τις μεταβάσεις απο μια κατάσταση σε μια άλλη και για την προδιαγραφή κάθε κατάστασης. Σημειώνεται ότι κάθε κατάσταση αντιστοιχεί σε ένα στατικό σχήμα

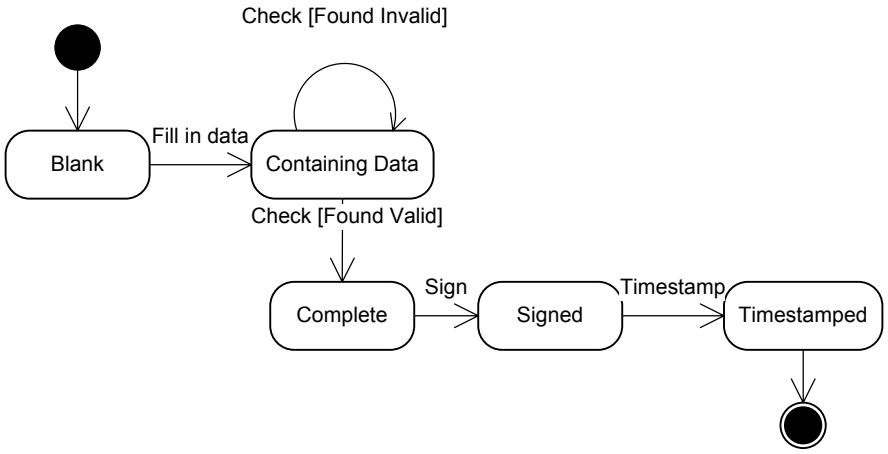
για το συγκεκριμένο αντικείμενο πληροφορίας, το οποίο θα χρησιμοποιηθεί σε επόμενο στάδιο των προδιαγραφών για την υλοποίηση των υπηρεσιών της ΑΔΑΑΥ.

4.3.2.4.3.3.2 Βασικά στοιχεία όψης

Τα βασικά στοιχεία όψης δυναμικών σχημάτων αποτελούν μέρη των κύκλων ζωής των βασικών στοιχείων όψης σταθερών σχημάτων της παραγράφου 4.3.2.4.3.1.2. Για κάθε ένα απο τα βασικά στοιχεία όψης σταθερών σχημάτων ενδέχεται να υπάρχουν περισσότερα του ενός δυναμικά σχήματα τα οποία είτε είναι επεκτάσεις των βασικών στοιχείων αυτής της παραγράφου είτε προδιαγράφουν έναν παράλληλο κύκλο ζωής για το αντικείμενο. Κάθε υλοποίηση βασικού στοιχείου θα πρέπει να λαμβάνει υπόψην τις καταστάσεις που προδιαγράφονται στην επόμενη παράγραφο.

4.3.2.4.3.3.2.1 Έγγραφο

Ένα έγγραφο περνάει απο τις ακόλουθες καταστάσεις: Κενό (blank), Συμπληρωμένο (Containing Data), Ολοκληρωμένο (Complete), Υπογεγραμμένο (Signed) και Χρονοσφραγισμένο (Timestamped):

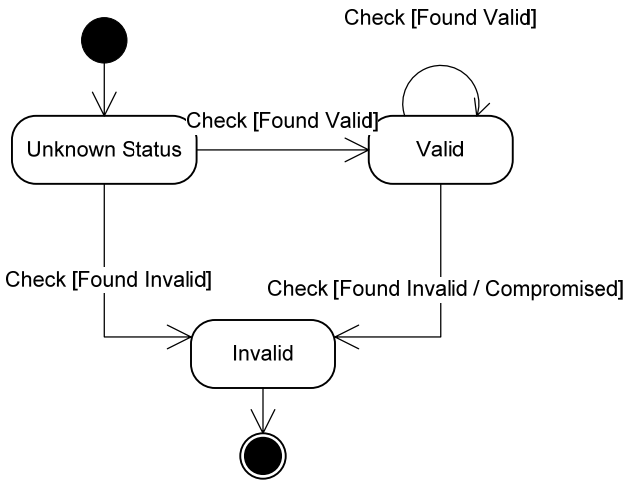


Σχήμα 4-29: Δυναμικό σχήμα του αντικειμένου Έγγραφο

Κατά την διάρκεια συμπλήρωσης των δεδομένων το Έγγραφο υπόκειται διαδοχικούς ελέγχους προκειμένου να εξασφαλίζεται ότι συμμορφώνεται με το σχήμα του και όποιες πολιτικές είναι σε ισχύ. Μόνο όταν είναι έγκυρο περνά στην κατάσταση Ολοκληρωμένο.

4.3.2.4.3.3.2.2 Διαπιστευτήριο

Ένα διαπιστευτήριο περνά στη ζωή του διαδοχικούς ελέγχους εγκυρότητας μέχρι να ακυρωθεί, είτε επειδή έχει λήξει η διάρκειά του είτε επειδή έχει παραβιαστεί η ασφάλειά του.

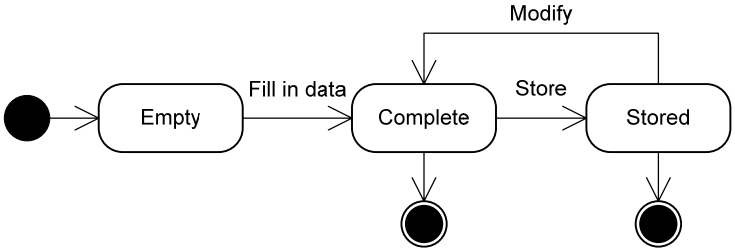


Σχήμα 4-30: Δυναμικό σχήμα του αντικειμένου Διαπιστευτήριο

Αρχικά κάθε η ισχύς κάθε διαπιστευτηρίου είναι Άγνωστη (Unknown Status). Αν ο έλεγχος της ισχύος του υποδείξει ότι είναι έγκυρο, τότε περνά στην κατάσταση Έγκυρο (Valid). Απο την κατάσταση αυτή, σύμφωνα με την ακολουθούμενη πολιτική, το διαπιστευτήριο ελέγχεται διαρκώς μέχρι είτε να λήξει η διάρκεια ζωής του, είτε να παραβιαστεί η ασφάλειά του. Οι έλεγχοι αυτοί είτε το αφήνουν στην ίδια κατάσταση, ή το μεταφέρουν στην κατάσταση Άκυρο (Invalid). Επίσης απο την αρχική κατάσταση, αν ο έλεγχος εγκυρότητας αποτύχει τότε το αντικείμενο πηγαίνει κατ' ευθείαν στην κατάσταση Άκυρο.

4.3.2.4.3.3.2.3 Προφίλ χρήστη

Ένα προφίλ χρήση συνήθως χρειάζεται για την μεταφορά μέσα στην αρχιτεκτονική διαφόρων στοιχείων για έναν χρήστη καθώς και την αποθήκευσή τους. Αρχικά κατασκευάζεται μια άδεια δομή του προφίλ (empty) σύμφωνα με την καθορισμένη πληροφορία που πρέπει να περιέχει το προφίλ, η οποία μπορεί να περιγράφεται με κάποιο σχήμα. Όπως φαίνεται απο το σταθερό σχήμα του αντικειμένου πληροφορίας, ένα προφίλ χρήστη επίσης πρέπει να περιέχει μια αναφορά σε συγκεκριμένα διαπιστευτήρια για τον χρήστη.



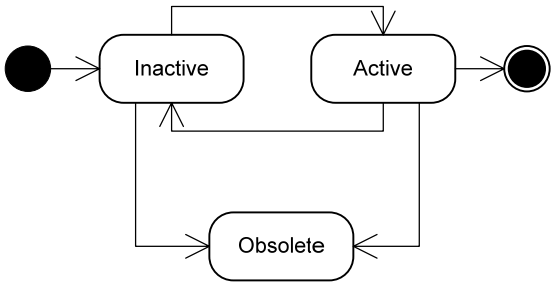
Σχήμα 4-31: Δυναμικό σχήμα προφίλ χρήστη

Τα δεδομένα του προφίλ λαμβάνονται απο τον ίδιο τον χρήστη. Όταν συμπληρωθούν τα στοιχεία, το αντικείμενο περνάει στην συμπληρωμένη κατάσταση (complete). Εάν κάποια πολιτική επιβάλλει την μη αποθήκευση του προφίλ, τότε όταν οι σχετικές διεργασίες σταματήσουν να χρειάζονται το προφίλ, αυτό καταστρέφεται.

Στην αντίθετη περίπτωση το προφίλ αποθηκεύεται και περνάει στην κατάσταση αποθηκευμένο (stored). Κατ' αυτόν τον τρόπο, την επόμενη φορά που ενδέχεται ο χρήσης να έχει πρόσβαση σε κάποια υπηρεσία, το προφίλ μπορεί να ανακτηθεί απο τον χώρο αποθήκευσης και ίσως να αλλάξει ή διαγραφεί εάν ο χρήστης το επιθυμεί.

4.3.2.4.3.3.2.4 Πολιτική

Μια πολιτική αρχικά σχεδιάζεται απο έναν διαχειριστή του συστήματος. Στην φάση του σχεδιασμού και μόλις ολοκληρωθεί βρίσκεται σε ανενεργή (inactive) κατάσταση.



Σχήμα 4-32: Δυναμικό σχήμα μιας πολιτικής

Όταν ληφθεί η απόφαση ενεργοποίησης, τότε η πολιτική περνάει στην ενεργοποιημένη φάση (active) και τότε λαμβάνεται υπόψην απο τις υπηρεσίες και μηχανισμούς εφαρμογής πολιτικών εντός της αρχιτεκτονικής.
Η πολιτική ενδέχεται να περνάει απο την μια κατάσταση στην άλλη για διάφορους λόγους:

- πρόκειται να αντικατασταθεί απο μια άλλη.
- πρόκειται να υποβληθεί σε παραμετροποίηση.
- πρόκειται να μείνει ανενεργή για ένα συγκεκριμένο χρονικό διάστημα.

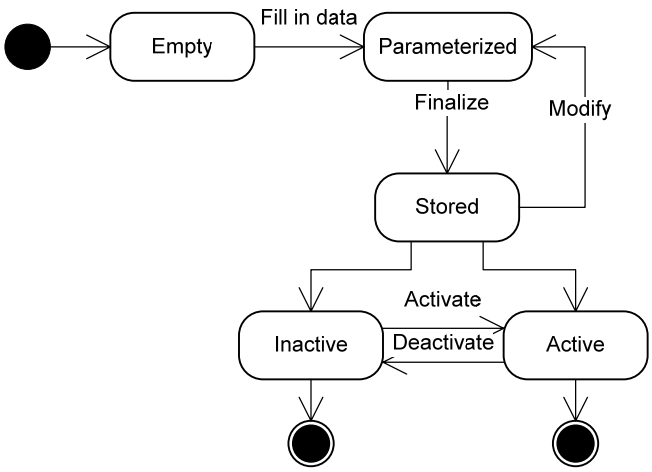
Είτε βρίσκεται σε ενεργοποιημένη είτε σε ανενεργή κατάσταση, όταν πρόκειται να αποσυρθεί περνάει στην κατάσταση «απαρχαιωμένη» (obsolete), που συνήθως σημαίνει ότι φυλάγεται σε ένα αρχείο πολιτικών.

4.3.2.4.3.3.2.5 Εγγραφή

Το αντικείμενο εγγραφή δεν έχει ένα συγκεκριμένο δυναμικό σχήμα διότι οι καταστάσεις και η επεξεργασία των εγγραφών μιας βάσης δεδομένων εξαρτώνται απο την συγκεκριμένη υλοποίηση της βάσης.

4.3.2.4.3.3.2.6 Αρχείο διαμόρφωσης

Το αρχείο διαμόρφωσης επηρεάζει στοιχεία λογισμικού της αρχιτεκτονικής, διότι καθορίζει την συμπεριφορά τους μέσω των παραμέτρων που περιέχει. Όπως φαίνεται στο Σχήμα 4-33, ξεκινά απο την άδεια (empty) κατάσταση στην οποία προστίθεται ένα σύνολο παραμέτρων για να καταλήξει στην παραμετροποιημένη κατάσταση (parameterized).

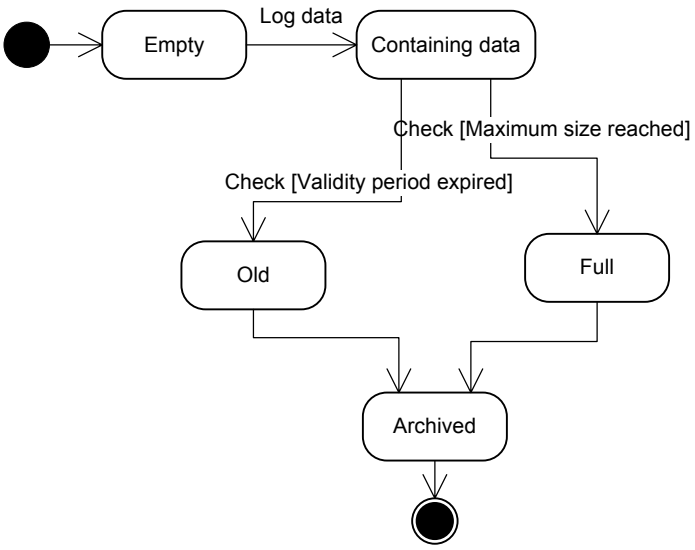


Σχήμα 4-33: Δυναμικό σχήμα αρχείου διαμόρφωσης

Το αρχείο διαμόρφωσης πάντα αποθηκεύεται (stored) προκειμένου να είναι διαθέσιμο σε κάθε εκκίνηση ενός συστήματος. Απο την αποθηκευμένη κατάσταση μπορεί να υποστεί αλλαγές, οπότε και περνά ξανά στην παραμετροποιημένη. Όταν οι αλλαγές ολοκληρωθούν αποθηκεύεται ξανά.
Αφότου περάσει στην αποθηκευμένη κατάσταση, τότε χαρακτηρίζεται είτε ως ενεργό (active) είτε ως ανενεργό (inactive). Στην δεύτερη περίπτωση, αν και αποθηκευμένο, δεν λαμβάνεται υπόψην απο το στοιχείο που το χρησιμοποιεί. Αυτό συμβαίνει διότι ενδέχεται να υπάρχουν περισσότερα του ενός αρχείων διαμορφώσεως για ένα συγκεκριμένο στοιχείο, και να πρέπει να λαμβάνεται υπόψην ένα υποσύνολο αυτών. Κάποια θα βρίσκονται λοιπόν στην ενεργή κατάσταση και κάποια στην ανενεργή. Η μετάβαση απο μια κατάσταση σε μια άλλη, μπορεί για παράδειγμα να υλοποιείται με την μεταφορά του αρχείου διαμόρφωσης απο έναν κατάλογο του συστήματος σε έναν άλλον.

4.3.2.4.3.3.2.7 Αρχείο καταγραφής

Το αρχείο καταγραφής συλλέγει συνεχώς πληροφορίες απο τα διάφορα γεγονότα του συστήματος. Ξεκινώντας τον κύκλο ζωής του, είναι στην κατάσταση «άδειο» (empty). Στην συνέχεια η υπηρεσία που είναι υπεύθυνη για την καταγραφή γεγονότων, προσθέτει δεδομένα στο αρχείο οπότε αυτό περνάει στην κατάσταση στην οποία εμπεριέχει ένα σύνολο απο αυτά (containing data).



Σχήμα 4-34 : Δυναμικό σχήμα αρχείου καταγραφής

Προκειμένου να περάσει σε επόμενη κατάσταση, συνήθως ελέγχονται δύο συνθήκες. Κάθε αρχείο καταγραφής έχει μια διάρκεια ισχύος. Όταν αυτή ξεπεραστεί τότε το αρχείο θεωρείται «παλαιωμένο» (old), αποθηκεύεται και περνά στην αρχειοθετημένη μορφή (archived), απο την οποία μπορούν να εξαχθούν πληροφορίες μελλοντικά. Η δεύτερη συνθήκη έχει να κάνει με το μέγεθος του αρχείου. Εάν ξεπεραστεί ένα κατώφλι, τότε το αρχείο περνά στην κατάσταση «πλήρες» (full) και απο εκεί πάλι καταλήγει στην αρχειοθετημένη μορφή.

4.3.2.4.3.3.3 Μεθοδολογία επέκτασης και παραδείγματα

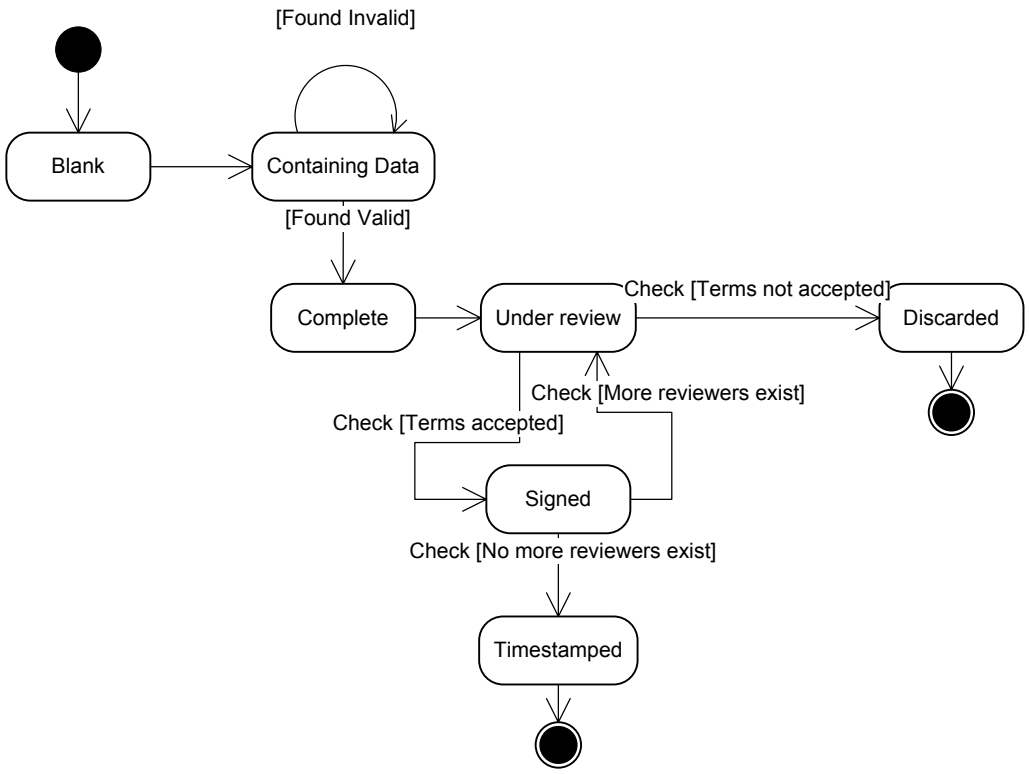
Η επέκταση των δυναμικών σχημάτων γίνεται με την προσθήκη νέων καταστάσεων στα διαγράμματα καταστάσεων ή την αλλαγή των ήδη υπαρχόντων. Επίσης για ένα αντικείμενο πληροφορίας ενδέχεται να υπάρχουν περισσότερα του ενός δυναμικά σχήματα σε παράλληλους άξονες.

Για παράδειγμα ένα αρχείο καταγραφής σε μια αρχιτεκτονική μπορεί να έχει και υπόσταση εγγράφου, οπότε να κληρονομεί και όλα τα χαρακτηριστικά (και άρα και δυναμικά σχήματα) του αντικειμένου «έγγραφο», δηλαδή να πρέπει να υπογράφεται και χρονοσφραγίζεται.

Επίσης κάθε νέο αντικείμενο πληροφορίας που εισάγεται, πρέπει να συνοδεύεται απο ένα η περισσότερα δυναμικά σχήματα, σύμφωνα με την λογική της παραπάνω μεθοδολογίας.

Ένα παράδειγμα επέκτασης είναι το ακόλουθο. Σε μια υπηρεσία μπορεί να απαιτείται η παραγωγή περισσότερων της μιας υπογραφής σε ένα συγκεκριμένο επιχειρησιακό έγγραφο προτού αυτό χρονοσφραγισθεί, για παράδειγμα σε ένα συμβόλαιο.

Το δυναμικό σχήμα του εγγράφου της παραγράφου 4.3.2.4.3.3.2.1 επεκτείνεται ως εξής:



Σχήμα 4-35: Παράδειγμα επέκτασης δυναμικού σχήματος εγγράφου

Όπως φαίνεται στο σχήμα, αφότου το έγγραφο φτάσει στην ολοκληρωμένη φάση (complete), ξεκινά ένας κύκλος ανασκοπήσεων. Όσο υπάρχουν οντότητες που πρέπει να το ελέγξουν και δέχονται τους όρους του συμβολαίου, τότε παράγονται νέες υπογραφές. Εάν κάποιος απο τους ελεγκτές δεν δεχτεί κάποιον όρο, τότε το έγγραφο απορρίπτεται (discarded). Εάν υπογράψουν όλοι, τότε μόνο το έγγραφο χρονοσφραγίζεται.

4.3.3 3^{ο} στάδιο: Γενική αποτύπωση απαιτούμενων υπηρεσιών και κατευθύνσεων τεχνολογίας

4.3.3.1 Στόχοι

Το στάδιο αυτό είναι προπαρασκευαστικό προκειμένου να αποφασιστεί το σύνολο των υπηρεσιών που θα ενσωματωθούν στην αρχιτεκτονική, με απώτερο στόχο να σχεδιαστούν τα υπομέρους στοιχεία λογισμικού στο 4^{ο} στάδιο και να εξασφαλιστεί το απαιτούμενο επίπεδο ασφάλειας.

4.3.3.2 Μεθοδολογία σταδίου

Ο σχεδιαστής ακολουθεί τα εξής επιμέρους βήματα:

1. Μελέτη των διαθέσιμων υπηρεσιών και μηχανισμών για την αρχιτεκτονική απο ένα αρχικό σύνολο που περιλαμβάνεται στην παράγραφο 4.3.3.3.
2. Επιλογή και καταγραφή των διαθέσιμων υπηρεσιών που απαιτούνται στην αρχιτεκτονική βάσει των αποτελεσμάτων του 2ου σταδίου προδιαγραφών.
3. Καταγραφή επιχειρησιακών στόχων που δεν καλύπτονται απο τις διαθέσιμες υπηρεσίες και προσθήκη νέων υπηρεσιών που τους καλύπτουν.
4. Επιλογή των συνολικών τεχνολογικών πλαισίων στα οποία θα κινηθεί η υλοποίηση της αρχιτεκτονικής.

Αν και μέχρι το στάδιο 5, η μεθοδολογία διατηρεί ανεξαρτησία απο συγκεκριμένες τεχνολογικές λύσεις ως προς τον σχεδιασμό, η μέχρι τώρα εμπειρία έχει αποδείξει ότι 100% ανεξαρτησία δεν μπορεί να επιτευχθεί. Το συνολικό τεχνολογικό πλαίσιο που θα υιοθετηθεί κατά την υλοποίηση (για παράδειγμα αν θα χρησιμοποιηθεί η αρχιτεκτονική Java Enterprise Architecture [J2EE] ή Microsoft .Net [dotNET] και τα δύο ή κάτι άλλο), θέτουν ένα σύνολο παραμέτρων τα οποία ενδέχεται να διευκολύνουν και την ανάλυση και τον σχεδιασμό εάν είναι γνωστά εκ των προτέρων. Γι'αυτό το λόγο, στο βήμα (4) του παρόντος σταδίου λαμβάνεται η απόφαση του γενικότερο πλαισίου που θα χρησιμοποιηθεί. Οι αρχιτεκτονικές υπηρεσιών επηρεάζονται λιγότερο απο αυτή την απόφαση δεδομένου ότι σε μεγάλο ποσοστό τους αποτελούνται απο Υπηρεσίες Ιστού, οι οποίες υποστηρίζονται απο όλα τα ευρέως διαδεδομένα πλαίσια υλοποίησης.
Το αποτέλεσμα του σταδίου 5 είναι μια λίστα με τις υπηρεσίες και τους μηχανισμούς που απαιτείται να σχεδιαστούν κατά τα στάδια 4 και 5, και να υλοποιηθούν στο στάδιο 6, καθώς και ένα σύνολο αποφάσεων για το γενικότερο πλαίσιο υλοποίησης που θα υιοθετηθεί στην αρχιτεκτονική.

4.3.3.3 Διαθέσιμες υπηρεσίες αρχιτεκτονικής

Η παράγραφος αυτή περιλαμβάνει ένα σύνολο υπηρεσιών που θεωρούνται υπηρεσίες «κορμού» για μια πλήρη αρχιτεκτονική υπηρεσιών προκειμένου να εξυπηρετεί βασικούς στόχους [Kaliontzoglou06, Meneklis05a, Meneklis05b].
Όλες οι υπηρεσίες μπορεί να υποστηρίζουν σύγχρονη ή ασύγχρονη επικοινωνία, και να είναι βασισμένες σε τεχνολογίες ανταλλαγής εγγράφων (document-centric) ή κλήσης μεθόδων (method-centric) [Kreger01].

4.3.3.3.1 Υπηρεσίες και μηχανισμοί διαχείρισης και συντονισμού

Οι *Υπηρεσίες Διαχείρισης και Συντονισμού* επιτελούν δύο πολύ σημαντικές λειτουργίες στο πλαίσιο της ΑΔΑΑΥ: διαχειρίζονται στο σύνολο τους άλλες υπηρεσίες και συντονίζουν τις Επιχειρησιακές Υπηρεσίες προκειμένου να επιτευχθούν οι επιχειρησιακοί στόχοι της ΑΔΑΑΥ.
Η ακριβής μεθοδολογία του συντονισμού Επιχειρησιακών Υπηρεσιών εξαρτάται απο τα σχετικά πρότυπα που υποστηρίζει η ΑΔΑΑΥ. Ο συντονισμός χρησιμοποιεί τα αποτελέσματα της ανάλυσης των Επιχειρησιακών στόχων του 2ου σταδίου, προκειμένου να τους διαιρέσει σε ατομικές υπο-διεργασίες που αναπαρίστανται απο Επιχειρησιακές Υπηρεσίες και κάνουν χρήση των Βασικών Υπηρεσιών και των Υπηρεσιών Ασφάλειας της αρχιτεκτονικής.

4.3.3.3.1.1 Υπηρεσίες πρόσβασης

Οι *Υπηρεσίες πρόσβασης* αναλαμβάνουν την διαχείριση των αιτήσεων πρόσβασης στην αρχιτεκτονική απο εξωτερικές οντότητες. Οι Υπηρεσίες πρόσβασης κάνουν άμεση χρήση των Υπηρεσιών Ασφάλειας στα πλαίσια της λειτουργίας τους.

4.3.3.3.1.2 Υπηρεσίες διαχείρισης διεργασιών

Οι *Υπηρεσίες διαχείρισης διεργασιών* αποτελούν τον πυρήνα της ΑΔΑΑΥ και διαχειρίζονται την δημιουργία και παράλληλη λειτουργία άλλων υπηρεσιών, την προσθήκη και αφαίρεση υπηρεσιών και την παρακολούθηση υπηρεσιών.

4.3.3.3.1.3 Υπηρεσίες διαχείρισης χρηστών

Οι *Υπηρεσίες διαχείρισης χρηστών* αναλαμβάνουν να διαχειριστούν τα δεδομένα που ανταλλάσσονται με τις οντότητες που επικοινωνούν με την ΑΔΑΑΥ.

4.3.3.3.2 Βασικές υπηρεσίες και μηχανισμοί

Οι *Βασικές Υπηρεσίες* παρέχουν όπως υπονοεί η ονομασία τους βασικές λειτουργίες που χρησιμοποιούνται καθολικά στην αρχιτεκτονική προκειμένου να επιτευχθούν στοιχειώδεις διαδικασίες.

4.3.3.3.2.1 Υπηρεσίες διεπαφής χρηστών

Οι *Υπηρεσίες διεπαφής χρηστών* αναλαμβάνουν την επικοινωνία με τα διάφορα είδη φυλλομετρητών που χρησιμοποιούν οι χρήστες είτε εκτός είτε εντός της αρχιτεκτονικής. Οι υπηρεσίες αυτές λαμβάνουν και επεξεργάζονται τα μηνύματα απο τους ασφαλείς φυλλομετρητές και κάνουν χρήση των υπηρεσιών ασφάλειας όπου αυτό χρειάζεται, προκειμένου να επαληθεύσουν τις παραμέτρους ασφάλειας που ενδέχεται να συνοδεύουν τα μηνύματα.

4.3.3.3.2.2 Υπηρεσίες μετασχηματισμού μηνυμάτων

Οι *Υπηρεσίες μετασχηματισμού μηνυμάτων* επιτρέπουν την μετατροπή μηνυμάτων προκειμένου να μεταφερθούν ανάμεσα σε διαφορετικές περιοχές διαχείρισης, όπως για παράδειγμα ανάμεσα σε οργανισμούς σε διαφορετικές χώρες. Οι υπηρεσίες μετασχηματισμού πρέπει να σέβονται τις σημασιολογία του περιεχομένου των μηνυμάτων προκειμένου τα έγγραφα που ανταλλάσσονται να είναι αποδεκτά στο περιβάλλον κάθε περιοχής διαχείρισης.

4.3.3.3.2.3 Υπηρεσίες προώθησης μηνυμάτων

Οι *Υπηρεσίες προώθησης μηνυμάτων* αναλαμβάνουν την μεταφορά μηνυμάτων στο σωστό παραλήπτη εφαρμόζοντας την κατάλληλη πολιτική μεταφοράς. Γι’ αυτό το λόγο συνήθως κάνουν χρήση των Υπηρεσιών Ασφάλειας.

4.3.3.3.2.4 Υπηρεσίες δημοσίευσης και αναζήτησης σε καταλόγους Υπηρεσιών Ιστού

Οι *Υπηρεσίες δημοσίευσης και αναζήτησης σε καταλόγους Υπηρεσιών* επικοινωνούν με τους κατάλληλους καταλόγους προκειμένου είτε να δημοσιεύσουν μια Επιχειρησιακή Υπηρεσία της ΑΔΑΑΥ, ή κάποια άλλη διεπαφή της ΑΔΑΑΥ, ή και να αναζητήσουν περιγραφές άλλων υπηρεσιών στο διαδίκτυο.

4.3.3.3.2.5 Υπηρεσίες διαχείρισης αποθετηρίων

Οι *Υπηρεσίες διαχείρισης αποθετηρίων* ελέγχουν τις συναλλαγές με αποθετήρια (π.χ. βάσεις δεδομένων) που εμπεριέχονται στην αρχιτεκτονική. Στην περίπτωση που ένα αποθετήριο αποτελεί μέρος υπάρχουσας υποδομής, τότε η πρόσβαση σε αυτό γίνεται μέσω των Υπηρεσιών πρόσβασης σε υπάρχουσες υποδομές όπως περιγράφεται στην παράγραφο 4.3.3.3.5 που ακολουθεί.

4.3.3.3.2.6 Υπηρεσίες ειδοποιήσεων

Οι *Υπηρεσίες ειδοποιήσεων* αναλαμβάνουν να ειδοποιούν τις κατάλληλες οντότητες όταν αυτό επιβάλλεται απο κάποια Επιχειρησιακή Υπηρεσία που υποστηρίζει η ΑΔΑΑΥ. Οι μηχανισμοί που χρησιμοποιεί η υπηρεσία ειδοποιήσεων μπορεί να βασίζονται σε πολλαπλά ενσύρματα ή ασύρματα μέσα.

4.3.3.3.2.7 Υπηρεσίες εκτυπώσεων

Οι *Υπηρεσίες εκτυπώσεων* αναλαμβάνουν την εκτύπωση σε μέσα του οργανισμού όταν αυτό απαιτείται απο κάποια Επιχειρησιακή Υπηρεσία.

4.3.3.3.3 Υπηρεσίες και μηχανισμοί ασφάλειας

Η παράγραφος αυτή περιλαμβάνει υπηρεσίες που θεωρούνται βασικές για την παροχή του αποδεκτού επιπέδου ασφάλειας μιας ΑΔΑΑΥ, τόσο στο επίπεδο Επιχειρησιακών Οντοτήτων όσο και στο Επίπεδο Υπολογιστικών Κόμβων, όπως περιγράφεται στην παράγραφο **Error! Reference source not found.**.

4.3.3.3.3.1 Μηχανισμοί ψηφιακών υπογραφών

Οι *μηχανισμοί ψηφιακών υπογραφών* χρησιμοποιούν κρυπτογραφία προκειμένου να ενσωματώσουν την ταυτότητα μιας οντότητας με ένα σύνολο δεδομένων και να εξασφαλίσουν την ακεραιότητα των δεδομένων αυτών. Οι απλές ψηφιακές υπογραφές ικανοποιούν τις απαιτήσεις για αυθεντικοποίηση και ακεραιότητα.

4.3.3.3.3.2 Μηχανισμοί προηγμένων ηλεκτρονικών υπογραφών

Οι *μηχανισμοί προηγμένων ηλεκτρονικών* υπογραφών αναβαθμίζουν τις απλές ψηφιακές υπογραφές συνδυάζοντάς τις με χρονοσφραγίδες καθώς και το κρυπτογραφικό «δέσιμο» της υπογραφής με μια πολιτική υπογραφής που εδραιώνει τη νομική της αξία στα πλαίσια ενός οργανισμού. Καλύπτουν την απαίτηση για μη-άρνηση συμμετοχής.

4.3.3.3.3.3 Μηχανισμοί κρυπτογράφησης

Οι *μηχανισμοί κρυπτογράφησης* χρησιμοποιούν αλγόριθμους κρυπτογράφησης για να κρυπτογραφήσουν και αποκρυπτογραφήσουν δεδομένα. Καλύπτουν τις απαιτήσεις για ιδιωτικότητα και μυστικότητα.

4.3.3.3.3.4 Υπηρεσίες διαχείρισης ταυτότητας

Οι *Υπηρεσίες διαχείρισης ταυτότητας* διαχειρίζονται τις ταυτότητες των χρηστών, ανάλογα με τους επιχειρηματικούς στόχους της ΑΔΑΑΥ. Για παράδειγμα, μια υπηρεσία τέτοιου τύπου μπορεί να προσφέρει ανωνυμία στους χρήστες. Καλύπτουν την απαίτηση για αυθεντικοποίηση και συνήθως κάνουν χρήση της υπηρεσίας Ψηφιακών Υπογραφών.

4.3.3.3.3.5 Υπηρεσίες ελέγχου πρόσβασης

Οι *Υπηρεσίες ελέγχου πρόσβασης* διαχειρίζονται την πρόσβαση σε πόρους της αρχιτεκτονικής. Κάνουν χρήση της Υπηρεσίας Διαχείρισης Ταυτότητας, προκειμένου να επιτρέπει ή να απορρίπτει την οποιαδήποτε πρόσβαση ή επεξεργασία πόρων. Καλύπτουν τις απαιτήσεις για ακεραιότητα, ιδιωτικότητα και διαθεσιμότητα.

4.3.3.3.3.6 Υπηρεσίες χρονοσφράγισης

Οι *Υπηρεσίες χρονοσφράγισης* επιτρέπουν την επικοινωνία με μια Έμπιστη Τρίτη Οντότητα προκειμένου να ληφθούν πιστοποιημένα δεδομένα χρόνου που είναι κρυπτογραφικά δεμένα με ένα σύνολο δεδομένων. Σε συνδυασμό με τους μηχανισμούς προηγμένων ψηφιακών υπογραφών, καλύπτουν την απαίτηση για μη-άρνηση συμμετοχής.

4.3.3.3.3.7 Υπηρεσίες διαχείρισης κλειδιών και πιστοποιητικών

Οι *Υπηρεσίες διαχείρισης κλειδιών και πιστοποιητικών* αποτελούν τις υπηρεσίες που διαχειρίζονται κλειδιά και πιστοποιητικά των οντοτήτων που εμπλέκονται στην ΑΔΑΑΥ. Χρησιμοποιούνται απο τις υπηρεσίες διαχείρισης ταυτότητας και τους μηχανισμούς ψηφιακών υπογραφών και κρυπτογράφησης, για την λήψη κλειδιών και τον έλεγχο της εγκυρότητας υπογεγραμμένων δεδομένων.

4.3.3.3.4 Επιχειρησιακές υπηρεσίες

Οι *Επιχειρησιακές Υπηρεσίες* επιτελούν τις λειτουργίες για τις οποίες ένας οργανισμός υιοθετεί μια ΑΔΑΑΥ. Όπως αναφέρθηκε στην περιγραφή των Υπηρεσιών Διαχείρισης και Συντονισμού, οι Επιχειρησιακές Υπηρεσίες διαιρούνται σε ένα σύνολο ατομικών υπο-υπηρεσιών σύμφωνα με την ανάλυση των επιχειρηματικών στόχων όπως αποτυπώνεται στις προδιαγραφές της Επιχειρησιακής Όψης του 2^{ου} Σταδίου της μεθόδου. Αυτό επιτυγχάνει την καλύτερη διαχείρισή τους, και την επαναχρησιμοποίησή τους όπου είναι δυνατόν. Για παράδειγμα, μια ατομική επιχειρησιακή υπο-υπηρεσία, μπορεί να δέχεται μια συμπληρωμένη και ψηφιακά υπογεγραμμένη φόρμα απο τον χρήστη. Αυτή η υπο-υπηρεσία μπορεί να χρησιμοποιηθεί στη σύνθεση οποιασδήποτε Επιχειρησιακής Υπηρεσίας που περιλαμβάνει μια τέτοια διεργασία.

4.3.3.3.5 Υπηρεσίες υποστήριξης υπαρχουσών υποδομών

Οι *Υπηρεσίες υποστήριξης υπαρχουσών υποδομών* επί της ουσίας διαχειρίζονται το ενδιάμεσο επίπεδο ολοκλήρωσης της αρχιτεκτονικής το οποίο διασυνδέει την ΑΔΑΑΥ με αντίστοιχη υπηρεσία που λειτουργεί πάνω απο υπάρχουσες υποδομές ενός οργανισμού (π.χ. λογισμικό wrapper πάνω απο βάση δεδομένων κ.λ.π).
Κάθε υπάρχουσα υποδομή που υποστηρίζεται, αντιστοιχείται σε μια Υπηρεσία υποστήριξης υπαρχουσών υποδομών μέσα στην ΑΔΑΑΥ προκειμένου να είναι διαθέσιμη τις υπόλοιπες υπηρεσίες της αρχιτεκτονικής.

4.3.3.3.6 Παράδειγμα

Συνεχίζοντας το παράδειγμα της επιχειρησιακής υπηρεσίας έκδοσης ενός πιστοποιητικού γέννησης απο τα προηγούμενα στάδια, μπορούμε να συμπεράνουμε απο την περιγραφή της υπηρεσίας, ότι η ΑΔΑΑΥ που θα την φιλοξενήσει θα πρέπει κατ' ελάχιστο να υποστηρίζει το ακόλουθο υποσύνολο των παραπάνω υπηρεσιών:

- Υπηρεσίες και μηχανισμοί διαχείρισης και συντονισμού
    - Υπηρεσίες πρόσβασης
    - Υπηρεσίες διαχείρισης διεργασιών
    - Υπηρεσίες διαχείρισης χρηστών
- Βασικές υπηρεσίες και μηχανισμοί
    - Υπηρεσίες διεπαφής χρηστών
    - Υπηρεσίες δημοσίευσης και αναζήτησης σε καταλόγους Υπηρεσιών Ιστού
    - Υπηρεσίες διαχείρισης αποθετηρίων
    - Υπηρεσίες ειδοποιήσεων
    - Υπηρεσίες εκτυπώσεων
- Υπηρεσίες και μηχανισμοί ασφάλειας
    - Μηχανισμοί ψηφιακών υπογραφών
    - Μηχανισμοί προηγμένων ηλεκτρονικών υπογραφών
    - Υπηρεσίες διαχείρισης ταυτότητας
    - Υπηρεσίες ελέγχου πρόσβασης
    - Υπηρεσίες διαχείρισης κλειδιών και πιστοποιητικών
- Υπηρεσίες υποστήριξης υπαρχουσών υποδομών

Στην περίπτωση που σχεδιάζεται μόνο η επιχειρησιακή υπηρεσία έκδοσης πιστοποιητικών, αντί ολόκληρης της αρχιτεκτονικής (διότι για παράδειγμα η αρχιτεκτονική είναι ήδη διαθέσιμη), ο σχεδιαστής θα πρέπει να έχει εξασφαλίσει ότι οι παραπάνω υπηρεσίες υποστηρίζονται και έχουν σαφείς διεπαφές προκειμένου να ληφθούν υπόψην κατά τον σχεδιασμό.

4.3.4 4^{ο} στάδιο: Σχεδιασμός στοιχείων λογισμικού

4.3.4.1 Στόχοι

Ο στόχος του σταδίου είναι ο σχεδιασμός των προδιαγραφών όλων των στοιχείων λογισμικού που θα απαρτίσουν κάθε υπηρεσία και μηχανισμό που έχει επιλεχθεί στο προηγούμενο στάδιο. Για να επιτευχθεί αυτό προδιαγράφεται η υπολογιστική όψη κάθε στοιχείου.

4.3.4.2 Μεθοδολογία σταδίου

Το 4^{ο} στάδιο περιλαμβάνει τα εξής βήματα:

1. Για κάθε υπηρεσία ή μηχανισμό, η οποία υπάρχει ήδη στο σύνολο των υπηρεσιών του σταδίου 3, μελετάται το αντίστοιχο βασικό στοιχείο όψης της παραγράφου 4.3.4.3.3.2. Στη συνέχεια, το διάγραμμα δομικών στοιχείων του βασικού στοιχείου επεκτείνεται σύμφωνα με τις σχεδιαστικές αρχές της παραγράφου 4.3.4.3.3.1.1. Εάν θεωρηθεί απαραίτητο, λόγω αυξημένης πολυπλοκότητας, μια υπηρεσία ή μηχανισμός μπορεί να αναπαρασταθεί και με ένα σύνολο διαγραμμάτων δομικών στοιχείων που επικοινωνούν σε καλώς ορισμένα σημεία.
2. Για κάθε νέα υπηρεσία ή μηχανισμό που εισάγεται στην αρχιτεκτονική στο στάδιο 3, κατασκευάζεται ένα νέο διάγραμμα δομικών στοιχείων βάσει των σχεδιαστικών αρχών της παραγράφου 4.3.4.3.3.1.1.
3. Για κάθε διάγραμμα δομικών στοιχείων που έχει παραχθεί, κατασκευάζεται ένα διάγραμμα κλάσεων που αναλύει όλα τα δομικά στοιχεία, σύμφωνα με τις σχεδιαστικές αρχές της παραγράφου 4.3.4.3.3.1.2.
4. Για κάθε υπηρεσία ή μηχανισμό, σε συνδυασμό με τις κλάσεις που έχουν οριστεί στο προηγούμενο βήμα, παράγονται κατά βούληση διαγράμματα ακολουθίας τα οποία καλύπτουν όλες τις διεργασίες στις οποίες εμπλέκονται οι κλάσεις και υλοποιούν την επιθυμητή λειτουργικότητα της υπηρεσίας ή του μηχανισμού. Χρησιμοποιούνται οι σχεδιαστικές αρχές της παραγράφου 4.3.4.3.3.1.3.
5. Για κάθε υπηρεσία ή μηχανισμό, σε συνδυασμό με τις κλάσεις του βήματος (2) και τα αντικείμενα πληροφορίας του 2ου σταδίου, παράγονται κατά βούληση διαγράμματα συνεργασίας, προκειμένου να αντικατοπτρίζονται τα διάφορα πλαίσια αλληλεπίδρασης μεταξύ των κλάσεων και των αντικειμένων πληροφορίας, σύμφωνα με τις αρχές της παραγράφου 4.3.4.3.3.1.4.

Στο πέρας του 4ου σταδίου, ο σχεδιαστής θα έχει ολοκληρώσει την πρώτη έκδοση των προδιαγραφών όλων των επιμέρους στοιχείων λογισμικού της αρχιτεκτονικής καθώς και θα έχει ορίσει επακριβώς τις διεπαφές που υλοποιούν προκειμένου να μπορούν να συνδυαστούν.

4.3.4.3 Προδιαγραφή Υπολογιστικής Όψης

4.3.4.3.1 Εισαγωγή

Με την όψη αυτή, το σύστημα αποσυντίθεται σε λογικά και λειτουργικά στοιχεία που είναι κατάλληλα για κατανομή μέσα στην αρχιτεκτονική υπηρεσιών. Το αποτέλεσμα της διαδικασίας είναι αντικείμενα και οι διεπαφές τους καθώς και οι υπηρεσίες που χρησιμοποιούν.

4.3.4.3.2 Έννοιες

Οι έννοιες που ορίζονται στο πρότυπο RM-ODP και χρησιμοποιούνται στη μεθοδολογία προδιαγραφής της υπολογιστικής όψης είναι αυτές της παραγράφου 7.3.8.2.2.1.3.

4.3.4.3.3 Σημειογραφία

Στην παράγραφο αυτή καθορίζεται τι είδους διαγράμματα χρησιμοποιεί η μεθοδολογία για την αναπαράσταση των αντικειμένων της υπολογιστικής όψης, και μπορούν να

χρησιμοποιηθούν για την επέκταση της όψης. Όλα τα διαγράμματα βασίζονται στην UML.

- Διαγράμματα δομικών στοιχείων (component diagrams) για την εσωτερική οργάνωση μιας υπηρεσίας σε πακέτα, δομικά στοιχεία μέσα σε κάθε πακέτο και την επικοινωνία τους.
- Διαγράμματα κλάσεων για την περαιτέρω ανάλυση των δομικών στοιχείων που έχουν προδιαγραφεί, τον καθορισμό χαρακτηριστικών και μεθόδων.
- Διαγράμματα ακολουθίας για την προδιαγραφή των χρονικών ακολουθιών μηνυμάτων που ανταλλάσσονται ανάμεσα σε δομικά στοιχεία προκειμένου να επιτελέσουν τις λειτουργίες τους.
- Διαγράμματα συνεργασίας για την αποτύπωση των σχέσεων ανάμεσα σε αντικείμενα.

Οι παράγραφοι που ακολουθούν περιγράφουν πως χρησιμοποιείται η παραπάνω σημειολογία ως μέρος της μεθοδολογίας.

4.3.4.3.3.1 Μεθοδολογία προδιαγραφής

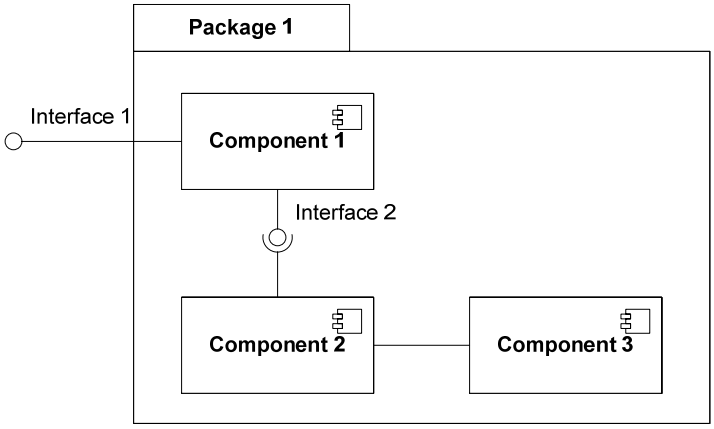
Η υπολογιστική όψη έχει σκοπό να αποτυπώσει όλα τα υπολογιστικά αντικείμενα που υπάρχουν στο σύστημα καθώς και τις διεπαφές που αυτά εκθέτουν, τόσο σε άλλα υπολογιστικά αντικείμενα μέσα στο ίδιο πακέτο, όσο και σε υπολογιστικά αντικείμενα σε άλλα πακέτα, επιτυγχάνοντας έτσι την επικοινωνία μεταξύ διαφορετικών δομικών στοιχειών.
Τα βασικά στοιχεία της υπολογιστικής όψης περιορίζονται σε μια υψηλού επιπέδου αφαίρεση των υπολογιστικών αντικειμένων, διότι οι ακριβείς προδιαγραφές είναι μέρος του σχεδιασμού μιας συγκεκριμένης ΑΔΑΑΥ. Στην παρούσα παράγραφο παρουσιάζονται οι αρχές σχεδιασμού που διέπουν την υπολογιστική όψη βάσει των εννοιών του RM-ODP και της UML. Προκειμένου να αναπαρασταθούν αρτιότερα και πιο ολοκληρωμένα οι έννοιες του RM-ODP, στις προδιαγραφές της υπολογιστικής όψης χρησιμοποιούνται διαγράμματα της 2^{ης} έκδοσης της UML (UML version 2.0) [UML2.0].

4.3.4.3.3.1.1 Διαγράμματα δομικών στοιχείων

Η ανάλυση μιας υπηρεσίας περιλαμβάνει αρχικά την κατάτμηση των λειτουργικών μονάδων της σε πακέτα της UML, με κάθε πακέτο να αναλαμβάνει ένα σύνολο συσχετιζόμενων λειτουργιών. Στη συνέχεια κάθε πακέτο συμπληρώνεται με ένα σύνολο δομικών στοιχείων της UML τα οποία ανήκουν στο πακέτο και επιτελούν την επιθυμητή λειτουργικότητα. Ένα δομικό στοιχείο ενδέχεται να υλοποιεί μια ή περισσότερες διεπαφές (interfaces) της UML. Κάθε διεπαφή έχει διττό ρόλο:

- δηλώνει ένα σύνολο συμπεριφορών (μεθόδων ή / και χαρακτηριστικών) που πρέπει να υποστηρίζονται απο το αντικείμενο που την υλοποιεί.
- εκθέτει την συμπεριφορά του αντικειμένου σε άλλα αντικείμενα (εντός ή εκτός του πακέτου) προκειμένου να είναι σε θέση να γνωρίζουν τι πρέπει να επιτελέσουν για να επικοινωνήσουν με το συγκεκριμένο αντικείμενο.

Το Σχήμα 4-36 επιδεικνύει τις παραπάνω σχεδιαστικές αρχές.



Σχήμα 4-36: Παράδειγμα χρήσης δομικών στοιχείων

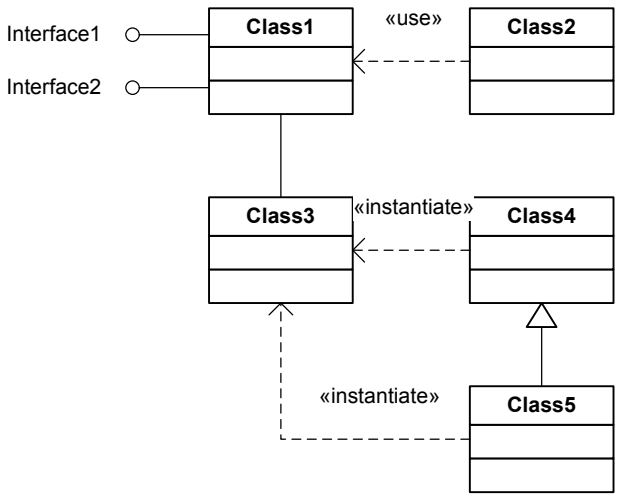
Όπως φαίνεται τρία δομικά στοιχεία περιλαμβάνονται στο Πακέτο 1 (Package 1), τα Στοιχείο 1, 2 και 3 (Components 1,2 και 3 αντίστοιχα). Το Στοιχείο 1 εκθέτει δύο Διεπαφές τις 1 και 2 (Interfaces 1,2). Η πρώτη διεπαφή είναι ορατή έξω απο το πακέτο προκειμένου να μπορεί να χρησιμοποιηθεί απο άλλα πακέτα (εντός της ίδιας ή άλλης υπηρεσίας ή μηχανισμού). Η δεύτερη χρησιμοποιείται εντός του πακέτου απο το Στοιχείο 2.

Τα διαγράμματα δομικών στοιχείων επιτυγχάνουν το πρώτο στάδιο αφαίρεσης των αντικειμένων της υπολογιστικής όψης και επιδεικνύουν τις ομάδες στοιχείων λογισμικού που θα υλοποιηθούν στο στάδιο 6.

4.3.4.3.3.1.2 Διαγράμματα κλάσεων

Ένα διάγραμμα κλάσεων αποτελεί την ανάλυση με μεγαλύτερη λεπτομέρεια των δομικών στοιχείων που έχουν ήδη προδιαγραφεί. Ένα δομικό στοιχείο μπορεί να αποτελείται απο μια ή περισσότερες κλάσεις που επικοινωνούν μεταξύ τους. Απο άποψη λειτουργικότητας, θα μπορούσαν να αντικαταστήσουν πλήρως το δομικό στοιχείο σε ένα διάγραμμα δομικών στοιχείων. Οι διεπαφές που υλοποιεί το δομικό στοιχείο προφανώς αντιστοιχίζονται σε μια απο τις κλάσεις που περιλαμβάνει.

Ένα παράδειγμα διαγράμματος κλάσεων παρατίθεται στο Σχήμα 4-37:

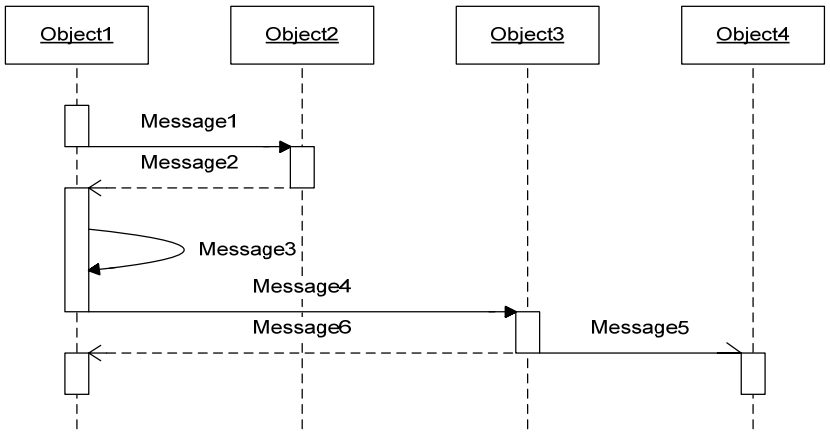


Σχήμα 4-37: Παράδειγμα διαγράμματος κλάσεων

Το παράδειγμα αυτό δίνει μια υποθετική ανάλυση του Στοιχείου 1 της προηγούμενης παραγράφου. Βλέπουμε ότι το στοιχείο αποτελείται απο πέντε κλάσεις με διάφορες σχέσεις και εξαρτήσεις μεταξύ τους. Και οι δύο διεπαφές του στοιχείου υλοποιούνται απο την Κλάση 1 (Class 1). Οι σχέσεις εξαρτήσεων στην προκειμένη περίπτωση χρησιμοποιούν τα πρότυπα «χρήσης» («use») και «δημιουργίας στιγμιότυπου» («instantiate»). Επίσης δυο κλάσεις σχετίζονται με σχέση κληρονομικότητας (οι 4 και 5). Γενικά σε ένα διάγραμμα κλάσεων στην υπολογιστική όψη μπορεί να χρησιμοποιηθεί όλο το εύρος των στοιχείων της UML για την αναπαράσταση των υπολογιστικών στοιχείων και οι συνήθεις πρακτικές τεχνολογίας λογισμικού.
Στην πρώτη φάση του σχεδιασμού, αναπαρίστανται μόνο κλάσεις σε ένα διάγραμμα, και τα βασικά χαρακτηριστικά και μέθοδοι. Στην συνέχεια (και κατά τη διάρκεια της υλοποίησης του σταδίου 6), οι κλάσεις διευρύνονται και γίνονται ακόμη πιο αναλυτικές και εμπλουτίζονται με περισσότερα χαρακτηριστικά και μεθόδους.

4.3.4.3.3.1.3 Διαγράμματα ακολουθίας

Αφότου οριστούν οι κλάσεις, το επόμενο βήμα είναι να οριστούν οι αλληλεπιδράσεις μεταξύ των κλάσεων και η χρονική ακολουθία αυτών των αλληλεπιδράσεων. Αυτό επιτυγχάνεται με διαγράμματα ακολουθίας της UML. Τα διαγράμματα ακολουθίας αναπαριστούν τα μηνύματα που ανταλλάσσονται μεταξύ αντικειμένων και την σειρά με την οποία γίνεται η ανταλλαγή προκειμένου τα υπολογιστικά αντικείμενα να επιτύχουν τους στόχους τους. Ένα παράδειγμα διαγράμματος ακολουθίας φαίνεται στο Σχήμα 4-38:



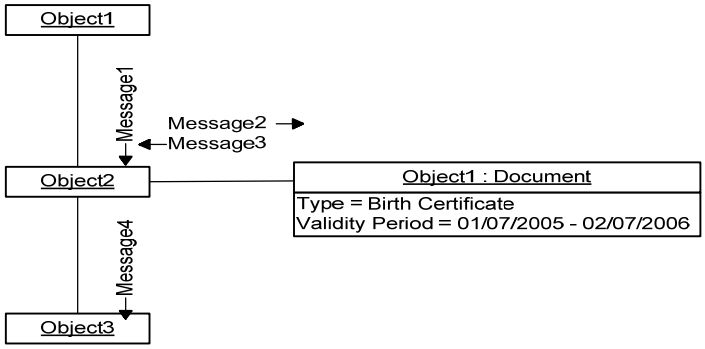
Σχήμα 4-38: Παράδειγμα διαγράμματος ακολουθίας

Σε ένα διάγραμμα ακολουθίας συνήθως παρατίθενται αντικείμενα, δηλαδή «στιγμιότυπα» κλάσεων[3]. Εντός των χρόνων δραστηριοποίησης των αντικειμένων (που διαφαίνονται με τα λευκά κουτάκια κατά μήκος των αξόνων), τα αντικείμενα στέλνουν και λαμβάνουν μηνύματα. Τα μηνύματα «κλήσεις» («calls») σύγχρονων μεθόδων αναπαρίστανται με συμπαγή βέλη με ολόκληρη την αιχμή τους, όπως τα μηνύματα 1, 3 και 4 του σχήματος. Τα ασύγχρονα μηνύματα αναπαρίστανται με συμπαγή βέλη με την μισή αιχμή τους, όπως το μήνυμα 5. Τέλος τα μηνύματα επιστροφής πληροφορίας αναπαρίστανται με βέλη διακεκομμένων γραμμών, όπως τα 2 και 6.

4.3.4.3.3.1.4 Διαγράμματα συνεργασίας

Ένα διάγραμμα συνεργασίας αναπαριστά το πως αντικείμενα-στιγμιότυπα με συγκεκριμένους ρόλους σχετίζονται σε ένα δεδομένο πλαίσιο καθώς και το σύνολο των μηνυμάτων που ανταλλάσσονται προκειμένου να επιτευχθεί ένα αποτέλεσμα. Στην αναπαράσταση αυτή δεν διαφαίνεται η συνιστώσα του χρόνου, όπως συμβαίνει σε ένα αντίστοιχο διάγραμμα ακολουθίας, και γι' αυτό το λόγο τα μηνύματα που ανταλλάσσονται αριθμούνται. Ένα παράδειγμα διαγράμματος συνεργασίας αποτυπώνεται στο Σχήμα 4-39:

[3] Μια περίπτωση στην οποία ενδέχεται να εμφανιστεί κλάση στο διάγραμμα και όχι αντικείμενο, είναι όταν καλείται κάποια στατική μέθοδος μιας στατικής κλάσης και άρα δεν μπορούν να δημιουργηθούν στιγμιότυπά της.



Σχήμα 4-39: Παράδειγμα διαγράμματος συνεργασίας

Στα πλαίσια της παρούσας μεθοδολογίας, τα διαγράμματα συνεργασίας χρησιμοποιούνται για την αποτύπωση καταστάσεων που συμβαίνουν σε υπολογιστικά αντικείμενα σε ένα δεδομένο πλαίσιο. Αυτό ενδέχεται να εμπλέκει την πιο συγκεκριμένη αναπαράσταση στιγμιότυπων που συνεργάζονται μεταξύ τους, καθώς και την αλληλεπίδρασή τους με αντικείμενα πληροφορίας, όπως αυτά έχουν οριστεί στο 2ο στάδιο.
Στο παραπάνω παράδειγμα, φαίνεται ότι τα αντικείμενα των τριών κλάσεων, ανταλλάσσουν μηνύματα μεταξύ τους βάσει της πληροφορίας που λαμβάνουν απο ένα αντικείμενο πληροφορίας της κλάσης Έγγραφο, και συμπεριφέρονται ανάλογα. Σημειώνεται ότι η αναπαράσταση του Εγγράφου γίνεται σε στατικό σχήμα, όπως περιγράφηκε στην παράγραφο 4.3.2.4.3.2.

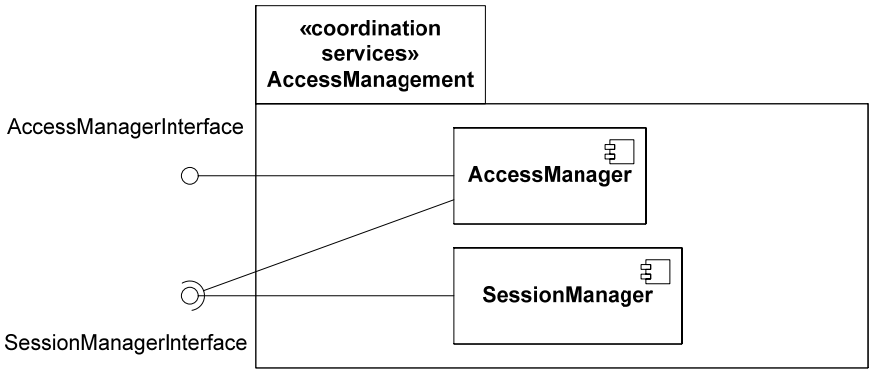
4.3.4.3.3.2 Βασικά στοιχεία όψης

Οι παράγραφοι που ακολουθούν περιγράφουν τα βασικά επαναχρησιμοποιήσιμα στοιχεία της υπολογιστικής όψης που θα αποτελέσουν την βάση της ΑΔΑΑΥ προς προδιαγραφή. Όπως έχει ήδη αναφερθεί, τα στοιχεία αυτά παρουσιάζονται σε ένα υψηλό επίπεδο αφαίρεσης και δίνονται μόνο οι αρχές με τις οποίες θα πρέπει να σχεδιαστούν, διότι ο ακριβής σχεδιασμός και η υλοποίησή τους είναι στενά δεμένη με την εκάστοτε αρχιτεκτονική. Όλες οι υπηρεσίες και μηχανισμοί αντιστοιχούν στις υπηρεσίες που παρουσιάστηκαν στο 3ο στάδιο.

4.3.4.3.3.2.1 Υπηρεσίες και μηχανισμοί διαχείρισης και συντονισμού

4.3.4.3.3.2.1.1 Υπηρεσία πρόσβασης

Η υπηρεσία πρόσβασης συντονίζει τους πόρους που απαιτούνται όταν κάποια οντότητα ζητά πρόσβαση στην αρχιτεκτονική. Αποτελείται απο δύο στοιχεία: τον *Διαχειριστή Πρόσβασης (AccessManager)* και τον *Διαχειριστή Συνόδων (SessionManager)*.

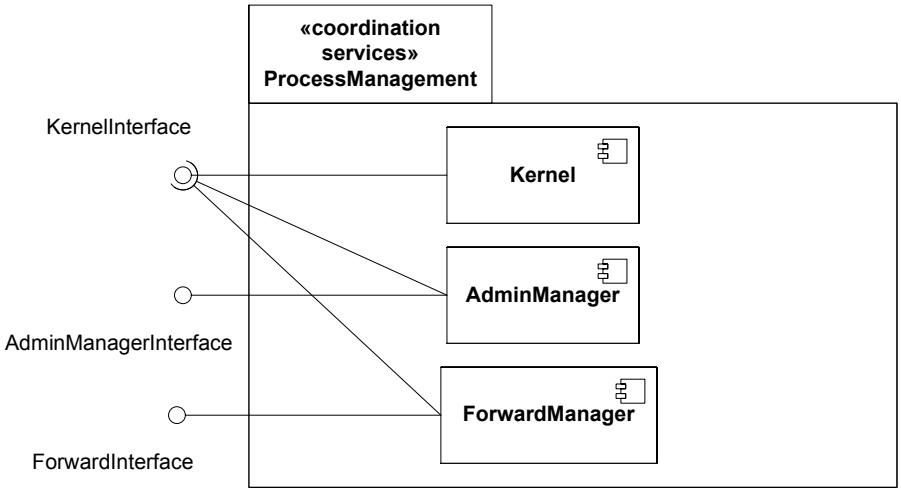


Σχήμα 4-40: Βασικό στοιχείο υπηρεσίας πρόσβασης

Ο Διαχειριστής Πρόσβασης είναι υπεύθυνος για την λήψη πληροφοριών χρηστών μέσω της υπηρεσίας διαχείρισης χρηστών, για την παράθεση όλων των διαθέσιμων υπηρεσιών αλλά και όλων των ενεργών υπηρεσιών, την έναρξη και λήξη συνόδων μέσων του Διαχειριστή Συνόδων, την προώθηση υπηρεσιών αν χρειάζεται σε άλλους διακομιστές μέσω της υπηρεσίας διαχείρισης διεργασιών και την έναρξη και λήξη υπηρεσιών. Ο Διαχειριστής Συνόδων έχει άμεση εποπτεία των σύνοδων πρόσβασης που υπάρχουν στο σύστημα. Μπορεί να ξεκινήσει ή να λήξει συνόδους, να παραθέσει πληροφορίες για τις συνόδους σε σχέση με τους χρήστες που τις έχουν ξεκινήσει.
Οι διεπαφές που υλοποιούνται είναι η *Διεπαφή Διαχείρισης Πρόσβασης (AccessManagerInterface)* απο τον Διαχειριστή Πρόσβασης, και η *Διεπαφή Διαχείρισης Συνόδων (SessionManagerInterface)* απο τον Διαχειριστή Συνόδων, η οποία χρησιμοποιείται και απο τον Διαχειριστή Πρόσβασης.

4.3.4.3.3.2.1.2 Υπηρεσία διαχείρισης διεργασιών

Η υπηρεσία διαχείρισης διεργασιών αποτελεί μια απο τις σημαντικότερες υπηρεσίες της αρχιτεκτονικής. Όπως φαίνεται στο Σχήμα 4-41, αποτελείται στο ελάχιστο απο τέσσερα στοιχεία: τον *Πυρήνα (Kernel)*, το *Γενικό Διαχειριστή (AdminManager)*, τον *Διαχειριστή Προώθησης (ForwardManager)* και τον *Εκκινητή Υπηρεσιών (Service Invoker)*.

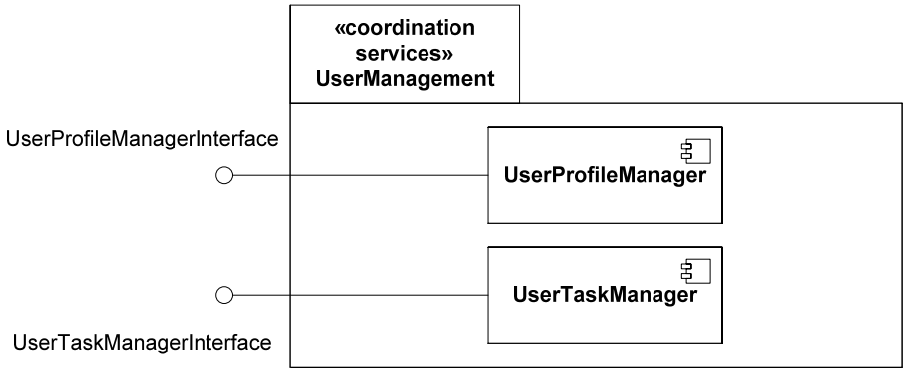


Σχήμα 4-41: Βασικό στοιχείο υπηρεσίας διαχείρισης διεργασιών

Ο Πυρήνας επιτελεί τις βασικές λειτουργίες αυθεντικοποίησης, δημιουργίας και διαγραφής συνόδων υπηρεσιών, την εγκατάσταση και απεγκατάσταση υπηρεσιών και την λήψη πληροφοριών για συνόδους, υπηρεσίες και χρήστες. Προκειμένου να επιτύχει τις λειτουργίες αυτές χρησιμοποιεί το μεγαλύτερο εύρος των υπολοίπων υπηρεσιών διαχείρισης και συντονισμού. Ο Πυρήνας συνήθως διατηρεί ένα αποθετήριο πληροφοριών που του επιτρέπει να επιτελεί τις λειτουργίες του. Ο Γενικός Διαχειριστής χρησιμοποιεί τον πυρήνα για την εποπτεία ορισμένων απο τις λειτουργίες του, και την παράθεση των λειτουργιών αυτών σε διαχειριστές του συστήματος. Οι δραστηριότητες που αναλαμβάνει περιέχουν την παράθεση των ενεργών συνόδων, την ρύθμισή τους, την εγκατάσταση νέων και την απεγκατάσταση υπαρχουσών υπηρεσιών και την φόρτωση αρχείων διαμόρφωσης. Ο Διαχειριστής Προωθήσεων λειτουργεί βοηθητικά για την προώθηση μηνυμάτων ή αντικειμένων εντός της αρχιτεκτονικής, όπου αυτό είναι απαραίτητο (σε αντίθεση με την υπηρεσία προώθησης μηνυμάτων που ακολουθεί και προωθεί μηνύματα εκτός της αρχιτεκτονικής).
Οι διεπαφές που υλοποιούνται στο βασικό στοιχείο διαχείρισης διεργασιών αποτελούνται απο την *Διεπαφή Πυρήνα (KernelInterface)*, την *Διεπαφή Γενικού Διαχειριστή (AdminManagerInterface)* και την *Διεπαφή Προώθησης (ForwardInterface)*. Η Διεπαφή Πυρήνα όπως φαίνεται χρησιμοποιείται απο τον Γενικό Διαχειριστή και τον Διαχειριστή Προωθήσεων, και ο κανόνας είναι να χρησιμοποιείται και απο ένα μεγάλο εύρος άλλων υπηρεσιών της αρχιτεκτονικής.

4.3.4.3.3.2.1.3 Υπηρεσία διαχείρισης χρηστών

Η υπηρεσία διαχείρισης χρηστών έχει κυρίως ως στόχο να διαχειρίζεται την πληροφορία που ενδέχεται να διακινείται στην αρχιτεκτονική σχετική με χρήστες, καθώς και τις διεργασίες χρηστών (user tasks). Όπως φαίνεται στο Σχήμα 4-42, αποτελείται απο τον *Διαχειριστή Προφίλ Χρηστών (UserProfileManager)* και τον *Διαχειριστή Διεργασιών Χρηστών (UserTaskManager)*.



Σχήμα 4-42: Βασικό στοιχείο υπηρεσίας διαχείρισης χρηστών

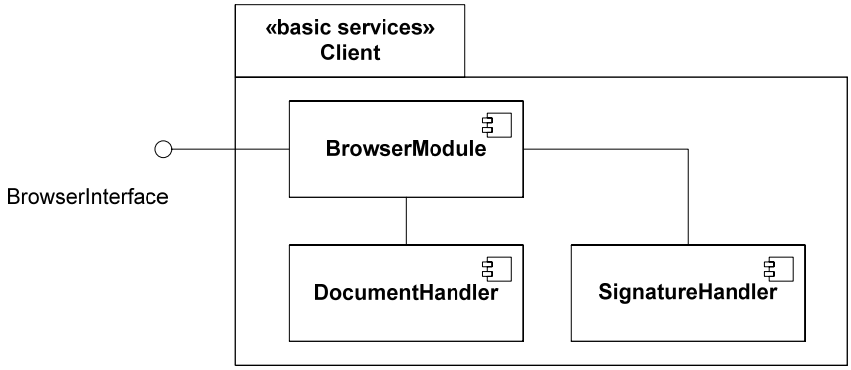
Ο Διαχειριστής Προφίλ Χρηστών καθορίζει και ανακτά προφίλ χρηστών, τα οποία είναι σαφώς ορισμένα ως αντικείμενα πληροφορίας στο στάδιο 2. Ο Διαχειριστής Διεργασιών Χρηστών επιστρέφει πληροφορίες σχετικά με τις διεργασίες που έχουν ξεκινήσει χρήστες (αναγνωριστικά και τύποι συνόδων, υπηρεσιών κ.λ.π). Για κάθε τύπο χρήστη ο Διαχειριστής Διεργασιών Χρηστών θα πρέπει να υποστηρίζει και μια υλοποίηση ενός αντίστοιχου Πελάτη Χρήστη που να εμπεριέχει την κατάλληλη πληροφορία διαχείρισης

μιας διεργασία (χρονικά σημεία εκκίνησης και περαίωσης, λίστα ενεργών διεργασιών κ.λ.π).
Οι διεπαφές που υλοποιούνται είναι η *Διεπαφή Διαχείρισης Προφίλ Χρήστη (UserProfileManagerInterface)* και η *Διεπαφή Διαχείρισης Διεργασιών Χρήστη (UserTaskManagerInterface)*.

4.3.4.3.3.2.2 Βασικές υπηρεσίες και μηχανισμοί

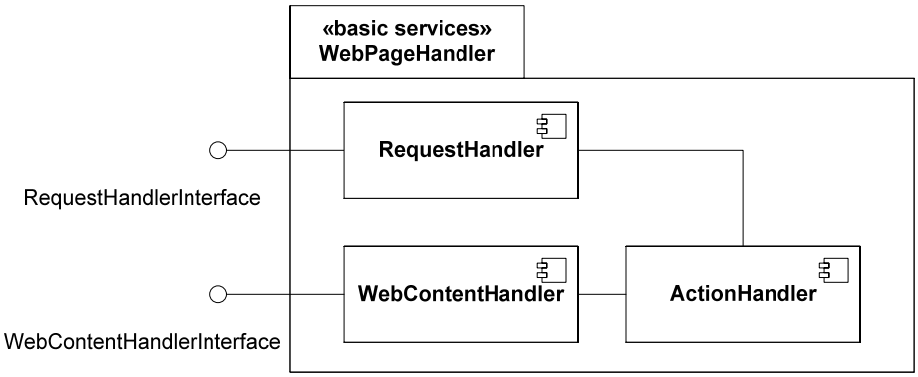
4.3.4.3.3.2.2.1 Υπηρεσία διεπαφής χρηστών

Η υπηρεσία διεπαφής αποτελείται απο δύο ομάδες στοιχείων. Τις σχετικές με τις εφαρμογές «πελάτες» που χρησιμοποιούν οι χρήστες προκειμένου να αλληλεπιδράσουν με την αρχιτεκτονική και τις υπόλοιπες υπηρεσίες της, καθώς και την υπηρεσία διαχείρισης του περιεχομένου των ιστοσελίδων δυναμικού και στατικού περιεχομένου που τροφοδοτούνται στις εφαρμογές πελάτες.
Τα βασικά στοιχεία που αποτελούν την υπο-υπηρεσία διεπαφής χρηστών για εφαρμογές πελάτες αποτυπώνονται στο σχήμα που ακολουθεί;



Σχήμα 4-43: Βασικό στοιχείο υπηρεσίας διεπαφής χρηστών για εφαρμογές «πελάτες»

Προκειμένου να επιτελούνται οι απαραίτητες λειτουργίες πλευρά του χρήστη, όπως για παράδειγμα είναι οι προηγμένες λειτουργίες ασφάλειας, είναι απαραίτητο να υποστηρίζονται απο την Δομική Μονάδα Φυλλομετρητή (BroswerModule). Η μονάδα αυτή είτε είναι μέρος του ίδιου του φυλλομετρτητή που χρησιμοποιείται, ή φορτώνεται σε αυτόν ως πρόγραμμα κατά την σύνδεση με τις υπηρεσίες της αρχιτεκτονικής ή είναι πρόσθετο κομμάτι λογισμικού που εγκαθίσταται σε έναν φυλλομετρητή (π.χ. ως plug-in).
Η Δομική Μονάδα Φυλλομετρητή χρησιμοποιεί δυο άλλα στοιχεία: τον Χειριστή Εγγράφων (DocumentHandler) και τον Χειριστή Υπογραφών (SignatureHandler). Ο Χειριστής Εγγράφων επιτρέπει την πρόσβαση στα έγγραφα XML που καταλήγουν στον φυλλομετρητή, την ανάγνωση των πεδίων τους και του περιεχομένου τους. Ο Χειριστής Υπογραφών αποτελεί ένα αντίγραφο του κατάλληλου μηχανισμού παραγωγής ψηφιακών υπογραφών XML, όπως θα περιγραφεί σε παράγραφο που ακολουθεί.
Όπως προαναφέρθηκε, το δεύτερο βασικό στοιχείο της υπηρεσίας διεπαφής χρηστών αποτελεί την υπηρεσία διαχείρισης των ιστοσελίδων.

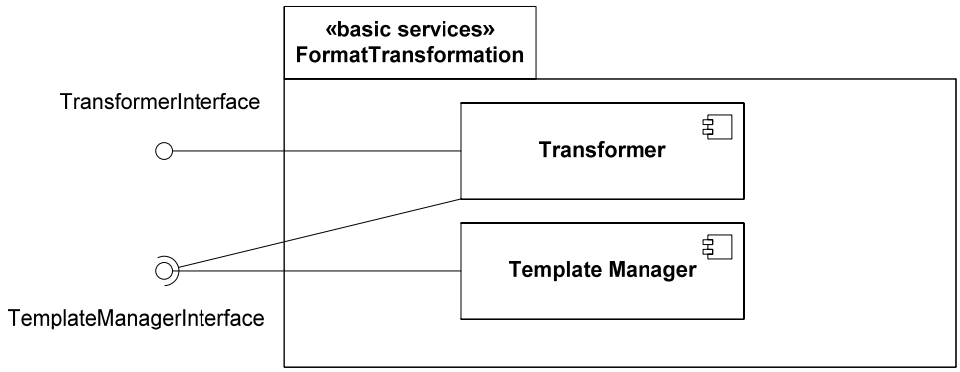


Σχήμα 4-44: Βασικό στοιχείο υπηρεσίας διεπαφής χρηστών για διαχείριση περιεχομένου

Το στοιχείο χρησιμοποιεί τον Χειριστή Αιτήσεων (Request Handler) για να δέχεται τις αιτήσεις για την εκκίνηση υπηρεσιών. Ο πυρήνας της υπηρεσία είναι ο Χειριστής Δράσεων (ActionHandler), ο οποίος αναλαμβάνει να επεξεργάζεται τις αιτήσεις, να επικοινωνεί με τις υπηρεσίες Πρόσβασης και Διαχείρισης Διεργασιών που παρουσιάστηκαν στην παράγραφο 4.3.4.3.3.2.1, και να προωθεί στην εφαρμογή «πελάτη» το κατάλληλο περιεχόμενο. Η προώθηση αυτή και η δημιουργία των ιστοσελίδων γίνεται μέσω του Χειριστή Περιεχομένου Ιστοσελίδων (WebContentHandler). Η υπηρεσία υλοποιεί δύο διεπαφές με τις οποίες επικοινωνούν οι φυλλομετρητές μέσω της Δομικής Μονάδας Φυλλομετρητή: την Διεπαφή Χειριστή Αιτήσεων (RequestHandlerInterface) και την Διεπαφή Χειριστή Περιεχομένου Ιστοσελίδων (WebContentHandlerInterface).

4.3.4.3.3.2.2.2 Υπηρεσία μετασχηματισμού μηνυμάτων

Η υπηρεσία μετασχηματισμού μηνυμάτων αποτελείται απο δύο βασικούς μηχανισμούς. Μια «μηχανή» μετασχηματισμών που χρησιμοποιεί πρότυπα μετασχηματισμών προκειμένου να μετατρέψει έγγραφα ή μηνύματα απο μια μορφή σε μια άλλη, και απο έναν διαχειριστή των προτύπων αυτών. Ο διαχειριστής των προτύπων είναι προσβάσιμος απο έναν διαχειριστή του συστήματος προκειμένου να προσθέσει, αφαιρέσει ή παραμετροποιήσει πρότυπα, αλλά και απο την ίδια την μηχανή μετασχηματισμών για την ανάκτηση προτύπων κατά την διαδικασία μετασχηματισμού.
Το βασικό στοιχείο της όψης φαίνεται στο ακόλουθο γενικό διάγραμμα δομικών στοιχείων:



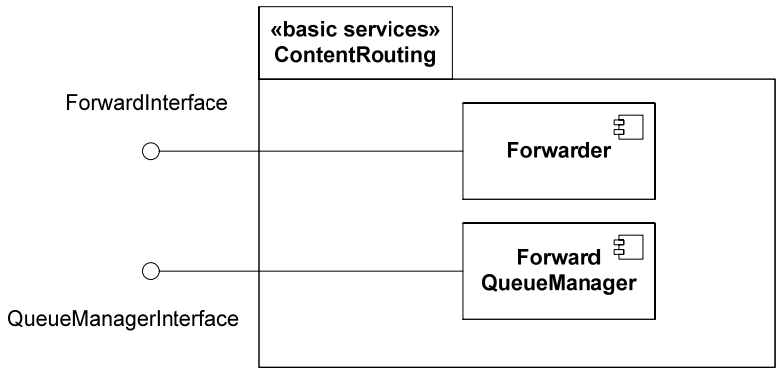
Σχήμα 4-45: Βασικό στοιχείο υπηρεσίας μετασχηματισμού

Η λειτουργία της μηχανής μετασχηματισμών επιτελείται απο το δομικό στοιχείο Μετασχηματιστής (Transformer) και η διαχείριση των προτύπων απο τον Διαχειριστή Προτύπων (Template Manager). Τα δομικά στοιχεία υλοποιούν δύο διεπαφές, την διεπαφή μετασχηματιστή (transformer interface) και την διεπαφή διαχείρισης προτύπων (template manager interface). Όπως φαίνεται στο σχήμα, η διεπαφή διαχείρισης προτύπων είναι διαθέσιμη προς χρήση τόσο απο εξωτερικές οντότητες / υπηρεσίες όσο και απο την ίδια την μηχανή μετασχηματισμών. Επίσης, ο Διαχειριστής Προτύπων επικοινωνεί με μια Υπηρεσία Διαχείρισης Αποθετηρίων προκειμένου να φυλάξει, μεταβάλλει και ανακτήσει πρότυπα μετασχηματισμού.

4.3.4.3.3.2.2.3 Υπηρεσία προώθησης μηνυμάτων

Η υπηρεσία προώθησης μηνυμάτων αποτελείται απο στοιχεία που αναγνωρίζουν το πλαίσιο μεταφοράς ενός μηνύματος και δημιουργούν τους κατάλληλους «φακέλους» SOAP προκειμένου να το αποστείλουν στη σωστή διεύθυνση, εφαρμόζοντας στην πορεία τους απαιτούμενους μηχανισμούς ασφάλειας, σύμφωνα με την πολιτική που έχει καθοριστεί.

Το ακόλουθο διάγραμμα δομικών στοιχείων επιδεικνύει τα δύο στοιχεία που αποτελούν την υπηρεσία, τον Διακομιστή (Forwarder) και τον Διαχειριστή της Ουράς Προώθησης (Forwarding Queue Manager):



Σχήμα 4-46: Βασικό στοιχείο υπηρεσίας προώθησης μηνυμάτων

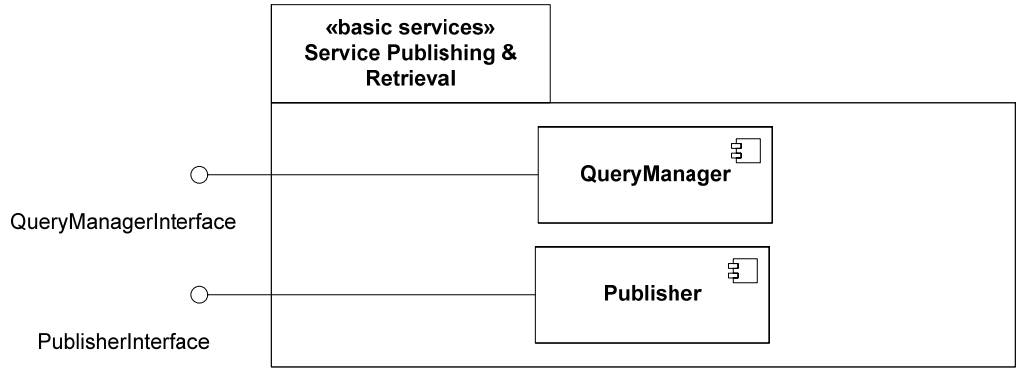
Ο Διακομιστής αναλαμβάνει να ανακτά κάθε φορά ένα μήνυμα που έχει αποθηκευτεί στην ουρά προώθησης, να φτιάχνει τον απαραίτητο φάκελο που το περιέχει, να ενσωματώνει όποια πληροφορία ασφάλειας απαιτείται και να το αποστέλλει στον παραλήπτη του. Για την περαίωση των παραπάνω διαδικασιών, ενδέχεται να επικοινωνεί με μια Υπηρεσία Διαχείρισης Αποθετηρίου όταν για την αποθήκευση της ουράς προώθησης χρησιμοποιείται ένα αποθετήριο, με διάφορες υπηρεσίες ασφάλειας (ή να χρησιμοποιεί μηχανισμούς ασφάλειας) ανάλογα με την πολιτική που ακολουθείται και με την Υπηρεσία Δημοσίευσης και αναζήτησης σε καταλόγους Υπηρεσιών Ιστού, όταν πρόκειται να αναζητηθεί η διεύθυνση ενός παραλήπτη, εάν δεν είναι γνωστή με άλλο τρόπο.

Ο Διαχειριστής της Ουράς Προώθησης δέχεται τα μηνύματα που πρόκειται να προωθηθούν, καθορίζει το πλαίσιο προώθησης κάθε μηνύματος και το αποθηκεύει στην ουρά. Άρα σε αναλογία με τα παραπάνω επίσης μπορεί να επικοινωνεί με την Υπηρεσία

Διαχείρισης Αποθετηρίου που είναι υπεύθυνη για το αποθετήριο που δρα ως ουρά προώθησης στην αρχιτεκτονική.
Η πρόσβαση στα δύο στοιχεία γίνεται μέσω των αντίστοιχων διεπαφών ForwardInterface και QueueManagerInterface.

4.3.4.3.3.2.2.4 Υπηρεσία δημοσίευσης και αναζήτησης σε καταλόγους Υπηρεσιών Ιστού

Η υπηρεσία δημοσίευσης και αναζήτησης σε καταλόγους Υπηρεσιών Ιστού επικοινωνεί με τέτοιους καταλόγους που υποστηρίζουν την τεχνολογία UDDI για να δημοσιεύσει της επιχειρησιακές υπηρεσίες που φιλοξενούνται στην αρχιτεκτονική καθώς και για την αναζήτηση νέων υπηρεσιών.

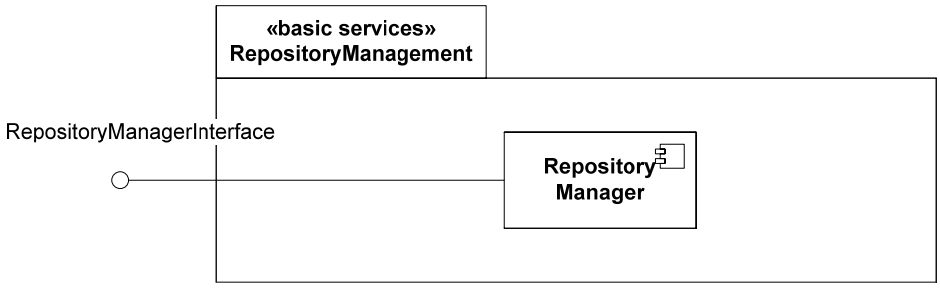


Σχήμα 4-47: Βασικό στοιχείο υπηρεσίας δημοσίευσης και αναζήτησης σε καταλόγους Υπηρεσιών Ιστού

Όπως φαίνεται στο σχήμα Σχήμα 4-47, η υπηρεσία αποτελείται απο δύο στοιχεία. Ο Διαχειριστής Αναζητήσεων (QueryManager) είναι διαθέσιμος μέσω της αντίστοιχης διεπαφής (QueryManagerInterface). Δέχεται συμβολοακολουθίες με λέξεις κλειδιά για υπηρεσίες και επιστρέφει τις περιγραφές τέτοιων υπηρεσιών που είναι καταχωρημένες σε έναν ή περισσότερους κεντρικούς καταλόγους UDDI. Ο Εκδότης (Publisher) δημοσιεύει μια υπηρεσία της αρχιτεκτονικής σε έναν κατάλογο UDDI. Δημοσιεύονται περιγραφικά στοιχεία της υπηρεσίας καθώς και οι προδιαγραφές WSDL της. Ο Εκδότης είναι διαθέσιμος μέσω της διεπαφής PublisherInterface.

4.3.4.3.3.2.2.5 Υπηρεσία διαχείρισης αποθετηρίων

Μια υπηρεσία διαχείρισης αποθετηρίου είναι υπεύθυνη για την εισαγωγή και εξαγωγή εγγράφων και πληροφορίας απο ένα αποθετήριο. Το βασικό δομικό στοιχείο της είναι ο Διαχειριστής Αποθετηρίου (Repository Manager) όπως φαίνεται στο Σχήμα 4-48.

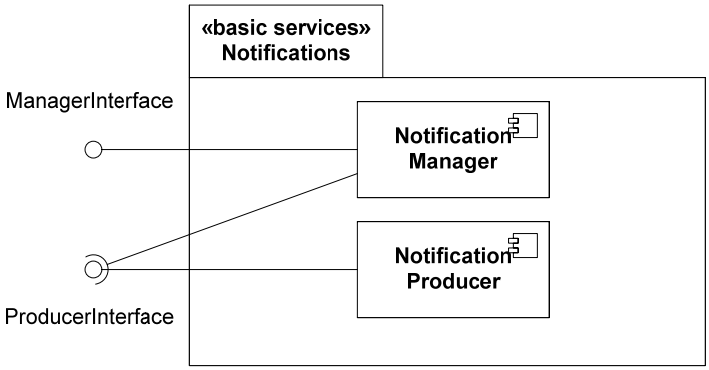


Σχήμα 4-48: Βασικό στοιχείο υπηρεσίας διαχείρισης αποθετηρίου

Ο Διαχειριστής Αποθετηρίου υλοποιεί την διεπαφή διαχείρισης αποθετηρίου (repository manager interface), η οποία είναι διαθέσιμη σε άλλες υπηρεσίες που θέλουν να εισάγουν ή να εξάγουν κάποιο έγγραφο απο το αποθετήριο, ή να κάνουν μια *ερώτηση (query)* για την λήψη πληροφοριών βάσει των ήδη υπαρχόντων εγγράφων.

4.3.4.3.3.2.2.6 Υπηρεσία ειδοποιήσεων

Η υπηρεσία ειδοποιήσεων αποτελείται απο δύο στοιχεία που επιτελούν βασικές λειτουργίες, τον Διαχειριστή Ειδοποιήσεων (Notification Manager), ο οποίος είναι υπεύθυνος για την λήψη αιτήσεων για αποστολή ειδοποίησης και την δημιουργία των κατάλληλων Κατασκευαστών Ειδοποιήσεων (Notification Producer). Ένας Κατασκευαστής Ειδοποιήσεων αναλαμβάνει να κατασκευάσει ένα αντικείμενο πληροφορίας Έγγραφο Ειδοποίησης, σύμφωνα με ένα δεδομένο σύνολο παραμέτρων.

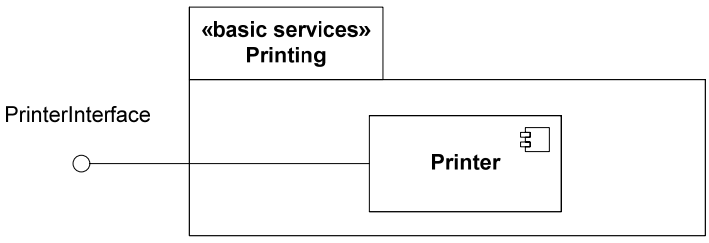


Σχήμα 4-49: Βασικό στοιχείο υπηρεσίας ειδοποιήσεων

Στην συνήθη περίπτωση, για κάθε είδος μέσου αποστολής μιας ειδοποίησης (π.χ. ηλεκτρονικό ταχυδρομείο, SMS κ.λ.π.) πρέπει να σχεδιαστεί και υλοποιηθεί ένας αντίστοιχος Κατασκευαστής Ειδοποιήσεων.
Ο Διαχειριστής Ειδοποιήσεων υλοποιεί την Διεπαφή Διαχείρισης (ManagerInterface), και ο Κατασκευαστής την Διεπαφή Κατασκευαστή (ProducerInterface). Όπως φαίνεται στο σχήμα, ο Διαχειριστής επίσης επικοινωνεί με έναν Κατασκευαστή μέσω της ίδιας Διεπαφής Κατασκευαστή.

4.3.4.3.3.2.2.7 Υπηρεσία εκτυπώσεων

Η υπηρεσία εκτυπώσεων επιτελεί την απλή διεργασία εκτυπώσεων των μηνυμάτων ή εγγραφών που αποστέλλονται σε αυτήν σε ένα εκτυπωτικό σύστημα που έχει παραμετροποιηθεί σε κάποιο αρχείο διαμόρφωσης το οποίο περιέχει.



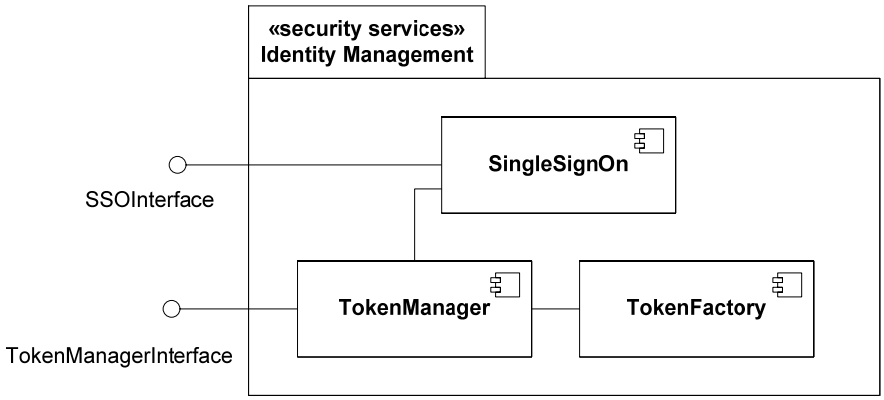
Σχήμα 4-50: Βασικό στοιχείο υπηρεσίας εκτυπώσεων

Όπως φαίνεται στο Σχήμα 4-50, η υπηρεσία υλοποιείται απο το δομικό στοιχείο Εκτυπωτής (Printer), το οποίο υλοποιεί την διεπαφή εκτυπωτής (printer interface), διαθέσιμη προς όλες τις άλλες υπηρεσίες που ενδέχεται να χρειαστούν να εκτυπώσουν κάποιο έγγραφο ή μήνυμα.

4.3.4.3.3.2.3 Υπηρεσίες και μηχανισμοί ασφάλειας

4.3.4.3.3.2.3.1 Υπηρεσία διαχείρισης ταυτότητας

Η υπηρεσία διαχείρισης ταυτότητας χρησιμοποιεί έννοιες βασισμένες στο πρότυπο SAML (βλ. παράγραφο 7.3.5), προκειμένου να δημιουργήσει *«σύμβολα» (tokens) ταυτοτήτων* που περιέχουν ισχυρισμούς (assertions) για οντότητες. Οι ισχυρισμοί αυτοί αποδίδουν στις ταυτότητες οντοτήτων (χρηστών, εξυπηρετητών κ.λ.π) χαρακτηριστικά αυθεντικοποίησης και ελέγχου πρόσβασης, τα οποία μέσω της υπηρεσίας διαχείρισης ταυτότητας μπορούν να αναλυθούν και να χρησιμοποιηθούν απο άλλες υπηρεσίες.



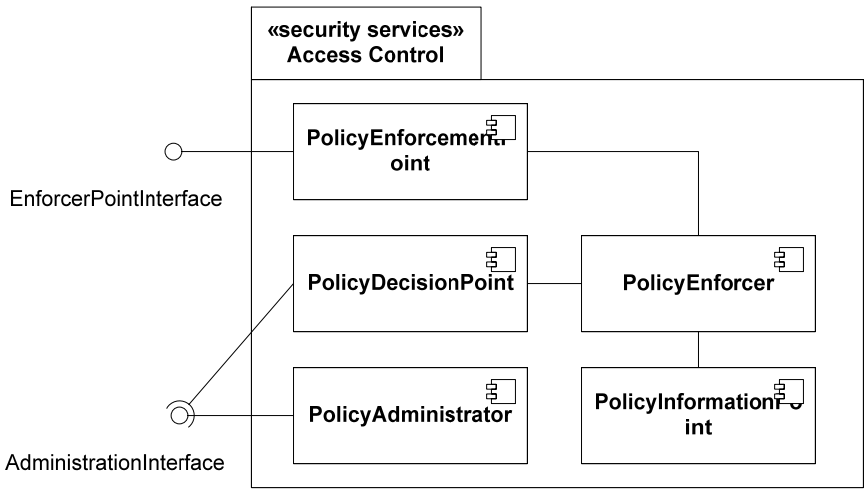
Σχήμα 4-51: Βασικό στοιχείο υπηρεσίας διαχείρισης ταυτότητας

Οι βασικές λειτουργίες που επιτελεί η υπηρεσία διαχείρισης ταυτότητας είναι να δημιουργεί και να επεξεργάζεται τέτοια σύμβολα. Αυτό το αναλαμβάνει ένας Διαχειριστής Συμβόλων (TokenManager), ο οποίος προκειμένου να δημιουργήσει σύμβολα ταυτοτήτων χρησιμοποιεί ένα «Εργοστάσιο» Συμβόλων (TokenFactory) και επικοινωνεί με εξωτερικές Αρχές για την συλλογή των απαραίτητων χαρακτηριστικών για τους ισχυρισμούς, όπως περιγράφεται στο πρότυπο της SAML. Παράλληλα, η υπηρεσία επιτελεί την λειτουργία Μοναδικής Εγγραφής (SingleSignOn) για τις οντότητες που συμμετέχουν στην αρχιτεκτονική.
Σημειώνεται ότι προκειμένου να παράγει και να ελέγχει υπογεγραμμένα σύμβολα ταυτοτήτων (για παράδειγμα μηνύματα XML με ισχυρισμούς SAML βασισμένα σε πιστοποιητικά X.509), η υπηρεσία κάνει χρήση του μηχανισμού ψηφιακών υπογραφών καθώς και της υπηρεσίας διαχείρισης κλειδιών και πιστοποιητικών.

4.3.4.3.3.2.3.2 Υπηρεσία ελέγχου πρόσβασης

Ο έλεγχος πρόσβασης στην αρχιτεκτονική σύμφωνα με την παρούσα μεθοδολογία βασίζεται απο πλευράς συνολικής αρχιτεκτονικής στις έννοιες που έχουν οριστεί στο πρότυπο XACML (βλ. παράγραφο 7.3.6). Χρησιμοποιούνται οι έννοιες του σημείου εφαρμογής πολιτικής, διαχείρισης πολιτικής και απόφασης πολιτικής, χωρίς όμως να

επιβάλλεται μια συγκεκριμένη υλοποίηση για τα σημεία αυτά. Το βασικό στοιχείο όψης φαίνεται στο Σχήμα 4-52:

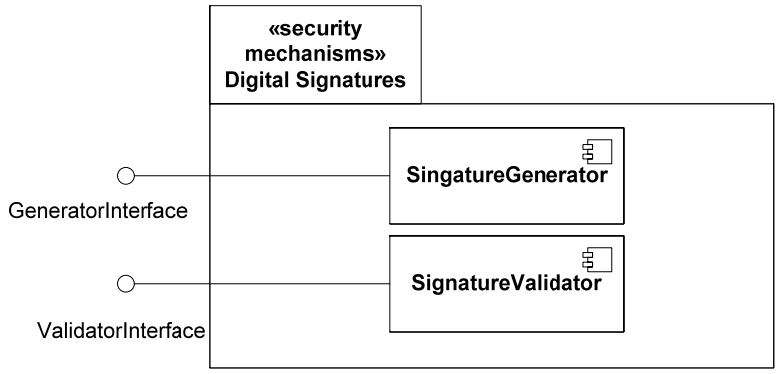


Σχήμα 4-52: Βασικό στοιχείο υπηρεσίας ελέγχου πρόσβασης

Η όλη υπηρεσία ελέγχου πρόσβασης συντονίζεται απο την μονάδα Εφαρμογής Πολιτικών (PolicyEnforcer). Το Σημείο Εφαρμογής Πολιτικών (PolicyEnforcementPoint) είναι το σημείο αλληλεπίδρασης των υπηρεσιών διαχείρισης και συντονισμού προκειμένου να εφαρμόσουν ελέγχους πρόσβασης. Ο διαχειριστής του συστήματος διαχειρίζεται τις πολιτικές ελέγχου πρόσβασης μέσω του Διαχειριστή Πολιτικών (PolicyAdministrator) και της διεπαφής που προσφέρει (AdministrationInterface). Την ίδια διεπαφή χρησιμοποιεί και το Σημείο Απόφασης Πολιτικής προκειμένου να αποφανθεί αν μια αίτηση ελέγχου πρόσβασης θα γίνει αποδεκτή ή όχι σύμφωνα με τις ισχύουσες πολιτικές. Η απάντηση θα προωθητή στο Σημείο Εφαρμογής Πολιτικής μέσω της μονάδα Εφαρμογής Πολιτικών που διαχειρίζεται την όλη διαδικασία και μεταφέρει τις απαραίτητες πληροφορίες στις επιμέρους μονάδες (αιτήσεις, απαντήσεις κ.λ.π). Οι πληροφορίες για τις ίδιες τις πολιτικές είναι αποθηκευμένες στο Σημείο Πληροφοριών Πολιτικών (PolicyInformationPoint). Το σημείο αυτό ενδέχεται να είναι μια βάση δεδομένων στην οποία αποθηκεύονται οι πολιτικές. Οι ακριβείς διαδικασίες που θα πρέπει να σχεδιαστούν και υλοποιηθούν για την συγκεκριμένη υπηρεσία προτείνεται να λαμβάνουν υπόψην τις προδιαγραφές του προτύπου XACML.

4.3.4.3.3.2.3.3 Μηχανισμός ψηφιακών υπογραφών

Ο μηχανισμός ψηφιακών υπογραφών χρησιμοποιεί το πρότυπο ψηφιακών υπογραφών XML (βλ. παράγραφο 7.2.2) για να παράγει και να επαληθεύσει ψηφιακές υπογραφές βάσει συγκεκριμένων κλειδιών και πιστοποιητικών που είναι αποθηκευμένα σε μια έξυπνη κάρτα ή έναν αποθηκευτικό χώρο στον δίσκο μιας μονάδας και ενός εγγράφου XML στο οποίο ενσωματώνεται η υπογραφή.

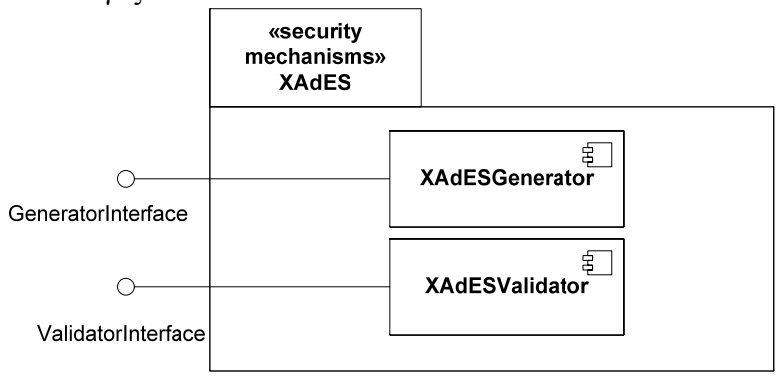


Σχήμα 4-53: Βασικό στοιχείο μηχανισμού ψηφιακών υπογραφών

Η δομή του βασικού στοιχείου είναι απλή. Αποτελείται απο τον Παραγωγό Υπογραφών (SignatureGenerator) ο οποίος δέχεται το έγγραφο προς υπογραφή και μια αναφορά στο χώρο αποθήκευσης του κρυπτογραφικού υλικού που θα χρησιμοποιηθεί (π.χ. ιδιωτικό κλειδί σε έξυπνη κάρτα) και παράγει το υπογεγραμμένο έγγραφο. Ο μηχανισμός μπορεί να παραμετροποιηθεί με κατάλληλα πρότυπα προκειμένου να παράγεται κάποιο απο τα τρία είδη υπογραφών (περικλείουσες, περικλειόμενες ή αποσπασμένες). Ο Ελεγκτής Υπογραφών (SignatureValidator) δέχεται ένα υπογεγραμμένο έγγραφο και κάνει όλους τους απαραίτητους ελέγχους προκειμένου να αποφανθεί εάν η υπογραφή είναι έγκυρη (π.χ. έλεγχο των χρησιμοποιούμενων πιστοποιητικών, κρυπτογραφική συνοχή των δεδομένων κ.λ.π) όπως προδιαγράφεται απο το πρότυπο. Γι' αυτό το λόγο ενδέχεται να επικοινωνεί με την υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών. Απο αρχιτεκτονικής άποψης, τα δύο στοιχεία θα μπορούσαν να ενοποιηθούν σε ένα που να περιλαμβάνει και τις δύο λειτουργίες.
Τα στοιχεία υλοποιούν τις αντίστοιχες διεπαφές Παραγωγού (GeneratorInterface) και Ελεγκτή (ValidatorInterface).

4.3.4.3.3.2.3.4 Μηχανισμός προηγμένων ηλεκτρονικών υπογραφών

Ο μηχανισμός προηγμένων ηλεκτρονικών υπογραφών βασίζεται στο πρότυπο XAdES (βλ. παράγραφο 7.2.3), για την παραγωγή και επαλήθευση υπογραφών XML που περιέχουν ένα ευρύτερο σύνολο πληροφοριών το οποίο τις καθιστά κατάλληλες για ηλεκτρονικές συναλλαγές.

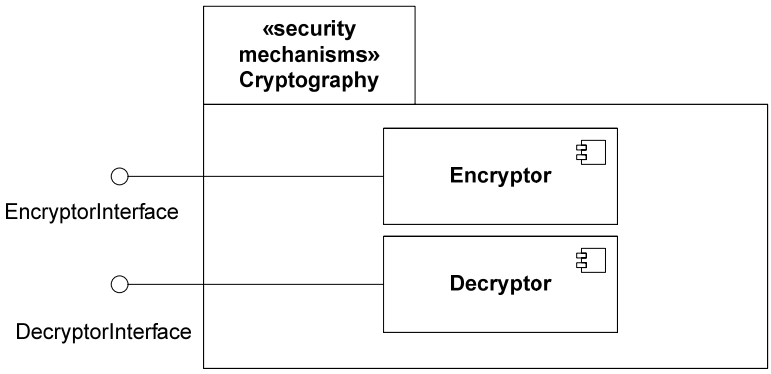


Σχήμα 4-54: Βασικό στοιχείο προηγμένων ηλεκτρονικών υπογραφών

Το βασικό στοιχείο του μηχανισμού αρχικά αποτελείται απο τον Παραγωγό XAdES (XAdESGenerator) ο οποίος συλλέγει τις κατάλληλες πληροφορίες για την παραγωγή της υπογραφές. Σύμφωνα με το πρότυπο αυτές είναι το έγγραφο προς υπογραφή, η πολιτική υπογραφής που ακολουθείται σε ηλεκτρονική μορφή, ένα σύνολο χαρακτηριστικών της υπογραφής (κάποια απο τα οποία υπογράφονται και κάποια όχι), χρονοσφραγίδες και δεδομένα ανάκλησης πιστοποιητικών. Προκειμένου να ενσωματώσει όλες αυτές τις πληροφορίες σε μια υπογραφή XAdES ο παραγωγός πρέπει να επικοινωνήσει τουλάχιστον με την υπηρεσία χρονοσφράγισης και την υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών. Επίσης κάνει χρήση του μηχανισμού απλών ψηφιακών υπογραφών της παραγράφου 4.3.4.3.3.2.3.3.
Ο Ελεγκτής XAdES (XAdESValidator) ελέγχει την εγκυρότητα της υπογραφής XAdES στο σύνολό της. Δηλαδή ελέγχει όλα τα επιμέρους συστατικά που την αποτελούν καθώς και την ίδια την απλή XML υπογραφή που περιέχει, κάνοντας χρήση του μηχανισμού ψηφιακών υπογραφών της παραγράφου 4.3.4.3.3.2.3.3. Η λειτουργικότητα του Ελεγκτή και Παραγωγού XAdES μπορεί να ενοποιηθεί σε μια μονάδα.

4.3.4.3.3.2.3.5 Μηχανισμός κρυπτογράφησης

Ο μηχανισμός κρυπτογράφησης υλοποιεί κρυπτογράφηση και αποκρυπτογράφηση ολόκληρων ή μέρους εγγράφων XML σύμφωνα με το αντίστοιχο πρότυπο (βλ. παράγραφο 7.2.1). Χρησιμοποιεί την υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών προκειμένου να εντοπίσει το κατάλληλο δημόσιο κλειδί που θα χρησιμοποιηθεί για την κρυπτογράφηση κάθε φορά.

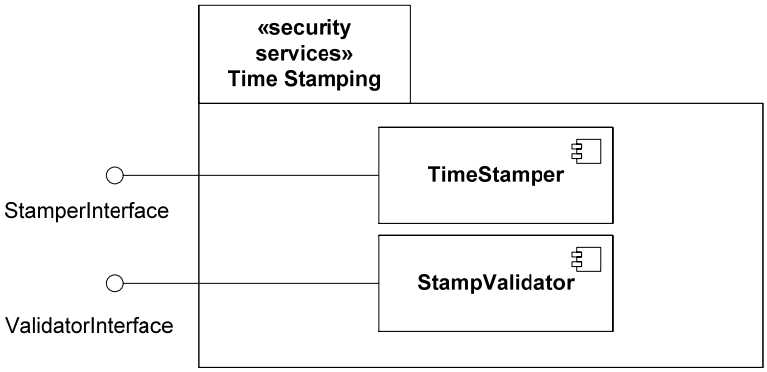


Σχήμα 4-55: Βασικό στοιχείο μηχανισμού κρυπτογράφησης

Ο μηχανισμός αποτελείται απο έναν Κρυπτογράφο (Encryptor) και έναν Αποκρυπτογράφο (Decryptor), ο οποίοι μπορεί να αποτελούν και ένα στοιχείο. Ο Κρυπτογράφος δέχεται το απλό έγγραφο, μια αναφορά σε ένα δημόσιο κλειδί και τις παραμέτρους κρυπτογράφησης (π.χ. αλγόριθμοι που θα χρησιμοποιηθούν). Εντοπίζει το κλειδί και υλοποιεί την διαδικασία κρυπτογράφησης σύμφωνα με το πρότυπο (χρησιμοποιώντας υβριδική κρυπτογραφία). Ο Αποκρυπτογράφος έχει πρόσβαση στον αποθηκευτικό χώρο που περιέχει το ιδιωτικό κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση.
Τα στοιχεία υλοποιούν τις αντίστοιχες διεπαφές Κρυπτογράφου (EncryptorInterface) και Αποκρυπτογράφου (DecryptorInterface).

4.3.4.3.3.2.3.6 Υπηρεσία χρονοσφράγισης

Η υπηρεσία χρονοσφράγισης αποτελεί επί της ουσίας μια υπηρεσία «wrapper» για την πραγματική υπηρεσία που βρίσκεται εκτός της αρχιτεκτονικής και παρέχεται απο μια Υποδομή Δημοσίου Κλειδιού. Στόχο έχει να λαμβάνει αιτήσεις για χρονοσφραγίδες σε έγγραφα απο τις υπηρεσίες που βρίσκονται εντός της αρχιτεκτονικής και να τις προωθεί στην πραγματική υπηρεσία για λήψη χρονοσφραγίδων.



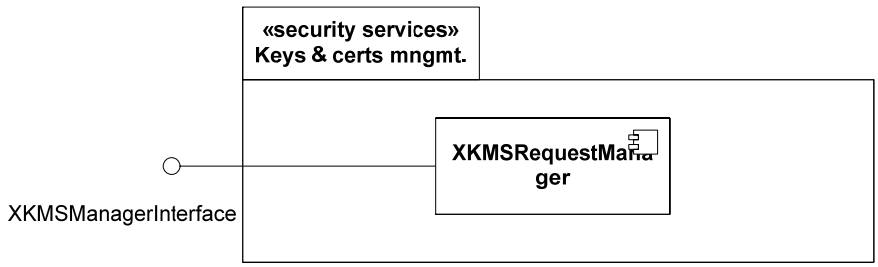
Σχήμα 4-56: Βασικό στοιχείο υπηρεσίας χρονοσφράγισης

Γι' αυτό το λόγο η αρχιτεκτονική του βασικού στοιχείου της υπηρεσίας είναι απλή. Ο Χρονοσφραγιστής (TimeStamper) λαμβάνει το έγγραφο προς χρονοσφράγιση και αναλαμβάνει να αποστείλει το hash του στην Αρχή Χρονοσφράγισης σύμφωνα με το πρότυπο χρονοσφράγισης RFC 3161. Επιστρέφει το δυαδικό αντικείμενο χρονοσφράγισης που του αποστέλλει η Αρχή Χρονοσφράγησης (χρονοσφραγίδα). Όταν μια υπηρεσία ζητά την επαλήθευση μιας τέτοια χρονοσφραγίδας, επικαλείται τον Ελεγκτή Χρονοσφραγίδων (StampValidator), ο οποίος ελέγχει την κρυπτογραφική υπόσταση της σφραγίδας και επικοινωνεί με την υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών για να ελέγξει αν είναι έγκυρο το πιστοποιητικό που χρησιμοποιήθηκε για την συγκεκριμένη χρονοσφραγίδα.
Τα στοιχεία υλοποιούν τις αντίστοιχες διεπαφές Χρονοσφραγιστή (StamperInterface) και Ελεγκτή Χρονοσφραγίδων (ValidatorInterface).

4.3.4.3.3.2.3.7 Υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών

Η υπηρεσία αυτή μπορεί να πάρει δύο μορφές: είτε να αποτελεί έναν εξυπηρετητή που υλοποιεί το πρότυπο XKMS, είτε μια ενδιάμεση υπηρεσία απλής προώθησης αναζητήσεων και εγγραφών κλειδιών, η οποία επικοινωνεί με έναν εξωτερικό εξυπηρετητή XKMS που παρέχεται απο μια Αρχή Πιστοποίησης. Στην πρώτη περίπτωση, ο σχεδιαστής της αρχιτεκτονικής θα πρέπει να σχεδιάσει και υλοποιήσει έναν δικό του εξυπηρετητή XKMS ή να εγκαταστήσει μια υπάρχουσα υλοποίηση που να υλοποιεί το πρότυπο. Στην δεύτερη περίπτωση, τα στοιχεία της υπηρεσίας απλά υλοποιούν ένα μέρος των διεπαφών που ορίζει το πρότυπο, ανάλογα με τις υπηρεσίες διαχείρισης που απαιτούνται. Για παράδειγμα, η υπηρεσία ίσως να χρειάζεται να δέχεται μηνύματα για αναζήτηση της κατάστασης ενός πιστοποιητικού (αν είναι έγκυρο ή έχει ανακληθεί) χωρίς να επιτρέπει την εγγραφή νέων ζευγών κλειδιών σε μια εξωτερική Αρχή Πιστοποίησης αυτόματα. Στην δεύτερη αυτή περίπτωση ο όγκος της εργασίας για τον σχεδιασμό και την υλοποίηση είναι μικρότερος. Χρειάζεται βέβαια και πάλι η γνώση

της παραγωγής των αντίστοιχων μηνυμάτων XKMS που υλοποιούν την επιθυμητή λειτουργικότητα.



Σχήμα 4-57: Βασικό στοιχείο υπηρεσίας διαχείρισης κλειδιών και πιστοποιητικών

Η ύπαρξη της υπηρεσίας επιτυγχάνει έναν κεντρικό έλεγχο της διαχείρισης των κλειδιών και των πιστοποιητικών και άρα ένα υψηλότερο επίπεδο ασφάλειας, αφού δεν επικοινωνεί με την Αρχή Πιστοποίησης κάθε υπηρεσία εντός της αρχιτεκτονικής απο μόνη της. Στην απλή της μορφή αποτελείται απο μια μονάδα Διαχείρισης Αιτήσεων XKMS (XKMSRequestManager) που αναλαμβάνει να δέχεται τις αιτήσεις για οποιαδήποτε εργασία διαχείρισης, είτε σε μια μορφή που είναι ήδη συμβατή με το XKMS είτε σε κάποια άλλη μορφή, να τις μετατρέπει σε μορφή XKMS αν απαιτείται, και να τις αποστέλλει στον εξυπηρετητή XKMS της Αρχής Πιστοποίησης με την οποία επικοινωνεί.
Η υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών ενδέχεται να χρησιμοποιεί τους μηχανισμούς ψηφιακών υπογραφών και κρυπτογραφίας στα μηνύματα που συνθέτει προς την Αρχή Πιστοποίησης.

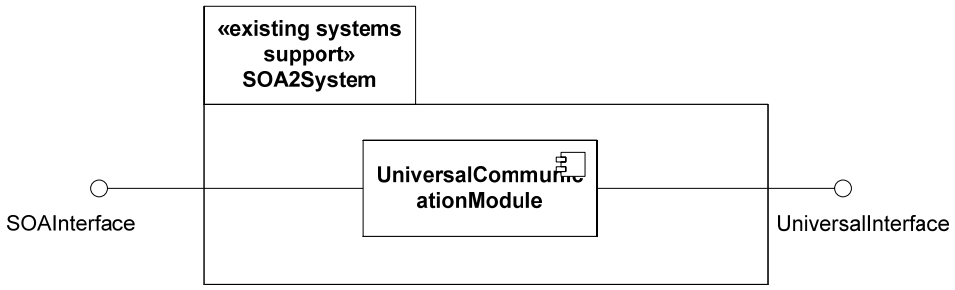
4.3.4.3.3.2.4 Επιχειρησιακές υπηρεσίες

Οι επιχειρησιακές υπηρεσίες που σχεδιάζονται και υλοποιούνται σε μια αρχιτεκτονική υπηρεσιών αποτελούν τις υπηρεσίες που δημοσιεύονται για χρήση απο εξωτερικές οντότητες και που επιτελούν τους επιχειρησιακούς στόχους του οργανισμού ή των οργανισμών που συμμετέχουν ή έχουν εγκαταστήσει την αρχιτεκτονική.
Οι επιχειρησιακές υπηρεσίες σχεδιάζονται σε όλα τα στάδια της παρούσας μεθοδολογίας. Βάσει των προηγούμενων σταδίων και των βασικών αρχών της παραγράφου 4.3.4.3.3.1 στο παρόν στάδιο σχεδιάζονται τα συστατικά στοιχεία λογισμικού των επιχειρησιακών υπηρεσιών, τα οποία όπως θα φανεί σε μετέπειτα στάδιο προτείνεται να υλοποιηθούν ως Υπηρεσίες Ιστού. Λόγω της γενικότητας της μεθοδολογίας, δεν υπάρχουν βασικά επαναχρησιμοποιήσιμα στοιχεία για τις επιχειρησιακές υπηρεσίες. Εκτενή παραδείγματα προδιαγραφών συγκεκριμένων επιχειρησιακών υπηρεσιών θα παρουσιαστούν στο επόμενο κεφάλαιο της παρούσας διατριβής.

4.3.4.3.3.2.5 Υπηρεσίες υποστήριξης υπαρχουσών υποδομών

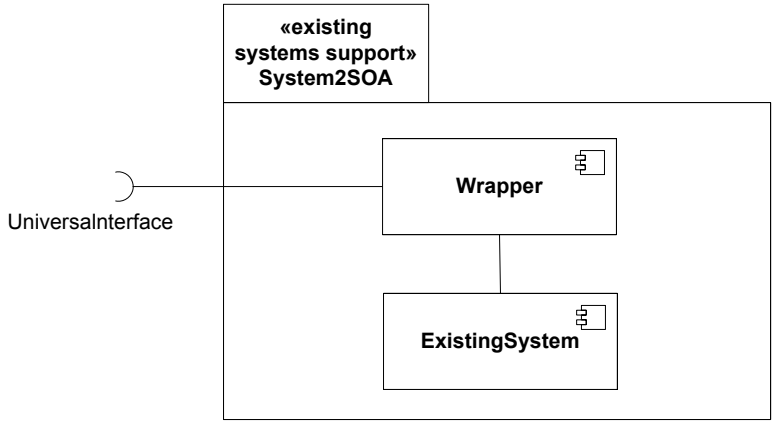
Οι υπηρεσίες υποστήριξης υπαρχουσών υποδομών έρχονται να καλύψουν την σημαντική απαίτηση για ενσωμάτωση σε μια καινούργια αρχιτεκτονική εφαρμογών, πληροφοριακών συστημάτων και βάσεων δεδομένων που ήδη έχει ένας οργανισμός και θέλει να διατηρήσει να χρησιμοποιεί. Στην παρούσα μεθοδολογία ακολουθείται η εξής προσέγγιση για τον σχεδιασμό των υπηρεσιών αυτών: απο την μεριά της προδιαγραφόμενης αρχιτεκτονικής υπάρχει μια μοναδική διεπαφή η οποία είναι ορατή

απο τις υπηρεσίες εντός της αρχιτεκτονικής. Απο την εξωτερική πλευρά, για κάθε υπάρχουσα υποδομή σχεδιάζεται και προδιαγράφεται λογισμικό "wrapper" που μπορεί απο τη μια να επικοινωνεί με την μια αυτή διεπαφή και απο την άλλη με την υπάρχουσα υποδομή. Έτσι επιτυγχάνεται μια ομογενοποιημένη τεχνική προσέγγιση, που επιτρέπει την χρήση πολλών διαφορετικών υπαρχουσών υποδομών απο την ίδια ΑΔΑΑΥ. Σχηματικά το βασικό στοιχείο της όψης παρατίθεται στο Σχήμα 4-58:



Σχήμα 4-58: Βασικό στοιχείο υπηρεσιών υποστήριξης υπαρχουσών υποδομών (πλευρά ΑΔΑΑΥ)

Το συγκεκριμένο πακέτο που περιέχει το βασικό στοιχείο ονομάζεται «ΑΔΑΑΥ προς Υπάρχον Σύστημα» (SOA2System), και αποτελεί το βασικό στοιχείο για την αρχιτεκτονική που σχεδιάζεται. Η Μονάδα Οικουμενικής Επικοινωνίας (UniversalCommunicationModule) εγγυάται ότι πληροφορίες απο οποιοδήποτε σύστημα απο την «εξωτερική» πλευρά της αρχιτεκτονικής μεταφέρονται μέσω της Οικουμενικής Διεπαφής (UniversalInterface) με ένα συγκεκριμένο τρόπο εντός της αρχιτεκτονικής και είναι διαθέσιμες μέσω της Διεπαφής ΑΔΑΑΥ (SOAInterface).
Φυσικά για κάθε υπάρχουσα υποδομή θα πρέπει να υπάρχει ένα αντίστοιχο σύνολο στοιχείων που χρησιμοποιεί την Οικουμενική Διεπαφή. Ένα δείγμα αντίστοιχου βασικού στοιχείου για την υποδομή είναι το ακόλουθο:

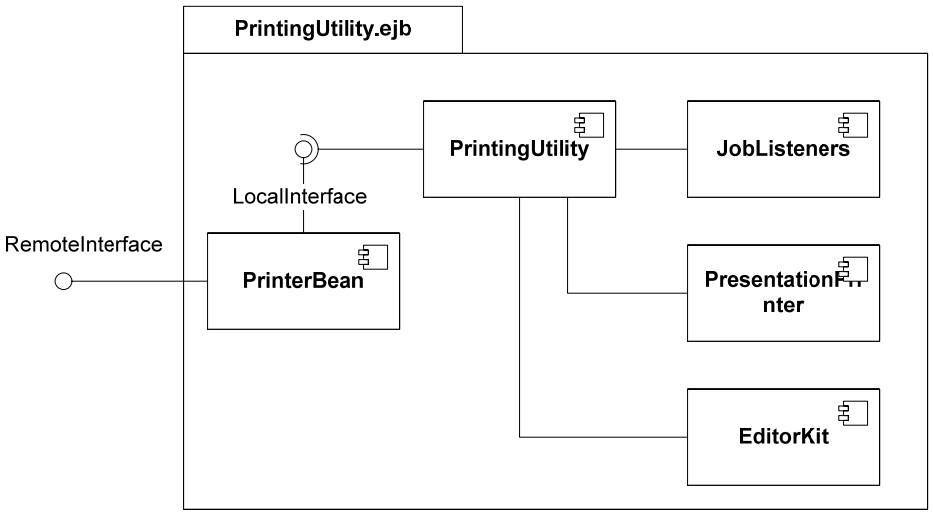


Σχήμα 4-59: Βασικό στοιχείο υπηρεσίας υπάρχουσας υποδομής (πλευρά υποδομής)

Όπως φαίνεται στο σχήμα, στο πακέτο «Υπάρχον Σύστημα προς ΑΔΑΑΥ» (System2SOA) υπάρχει μια μονάδα Wrapper που επικοινωνεί με την υπάρχουσα υποδομή (ExistingSystem) και επιτελεί τους κατάλληλους μετασχηματισμούς δεδομένων ώστε να επικοινωνήσει επιτυχώς με την ΑΔΑΑΥ μέσω της Οικουμενικής Διεπαφής.

4.3.4.3.3.3 Μεθοδολογία επέκτασης και παραδείγματα

Τα βασικά στοιχεία όψης που παρατέθηκαν, που αντιστοιχούν στις υπηρεσίες που έχουν επιλεγεί προς υλοποίηση στην σχεδιαζόμενη αρχιτεκτονική, καθώς και νέα στοιχεία τα οποία πρέπει να εισαχθούν επειδή έχουν επιλεγεί νέες υπηρεσίες απο το 3^{ο} στάδιο της μεθόδου, επεκτείνονται ή κατασκευάζονται βάσει των σχεδιαστικών αρχών της παραγράφου 4.3.4.3.3.1.
Συνεχίζοντας το παράδειγμα της επιχειρησιακής υπηρεσίας έκδοσης πιστοποιητικών γέννησης, παρατίθεται στην παρούσα παράγραφο ένας πιθανός σχεδιασμός της υπηρεσίας εκτύπωσης που θα πρέπει να υποστηρίζει η ΑΔΑΑΥ που φιλοξενεί την επιχειρησιακή υπηρεσία. Ο σχεδιασμός αυτός επεκτείνει το βασικό στοιχείο της παραγράφου 4.3.4.3.3.2.2.7 για την υπηρεσία εκτυπώσεων.
Ακολουθώντας τις αρχές της παραγράφου 4.3.4.3.3.1, σχεδιάζουμε το πρώτο στάδιο αφαίρεσης αναλύοντας περαιτέρω το βασικό στοιχείο της όψης. Αν και η μεθοδολογία μέχρι ένα επίπεδο υπόσχεται ανεξαρτησία απο την τεχνολογία υλοποίησης (οι λεπτομέρειες της οποίας επιλέγονται στο στάδιο 6), εάν υπάρχει ήδη μια ιδέα για το τι θα χρησιμοποιηθεί στην μετέπειτα υλοποίηση των στοιχειών, αυτή λαμβάνεται υπόψην προκειμένου να κατευθυνθεί ο σχεδιασμός προς τα εκεί. Στο σημείο αυτό λοιπόν χρησιμοποιείται ως δεδομένο το πλαίσιο υλοποίησης που έχει επιλεγεί στο στάδιο 4 της μεθόδου, και που για το συγκεκριμένο παράδειγμα θεωρείται ότι στην αρχιτεκτονική που χτίζεται θα χρησιμοποιηθεί Java και Enterprise Java Beans (EJBs). Αυτό βοηθά στο να σχεδιαστούν κάποια στοιχεία βάσει των κύριων χαρακτηριστικών της Java και των EJBs.
Επίσης κατά τον σχεδιασμό επιλέγεται ότι η τελική μορφή των κειμένων που θα εκτυπώνονται σε έναν εκτυπωτή θα είναι HTML, κάτι που δεν επηρεάζει οτιδήποτε άλλο, παρά μόνο τις βιβλιοθήκες της Java που θα χρησιμοποιηθούν.
Σύμφωνα με τα παραπάνω το πρώτο στάδιο αφαίρεσης μας δίνει τον σχεδιασμό του ακόλουθου σχήματος:



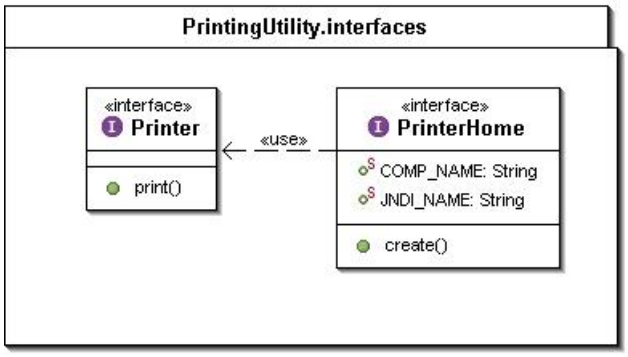
Σχήμα 4-60: Σχέδιο πρώτου σταδίου αφαίρεσης για ένα παράδειγμα υπηρεσίας εκτυπώσεων

Όπως φαίνεται στο σχήμα, η υπηρεσία αποτελείται απο:

- Ένα στοιχείο που βασίζεται στα EJB, ονομάζεται PrinterBean και είναι αυτό που υλοποιεί τις βασικές διεπαφές μέσω τον οποίων επιτυγχάνεται η πρόσβαση στην υπηρεσία.

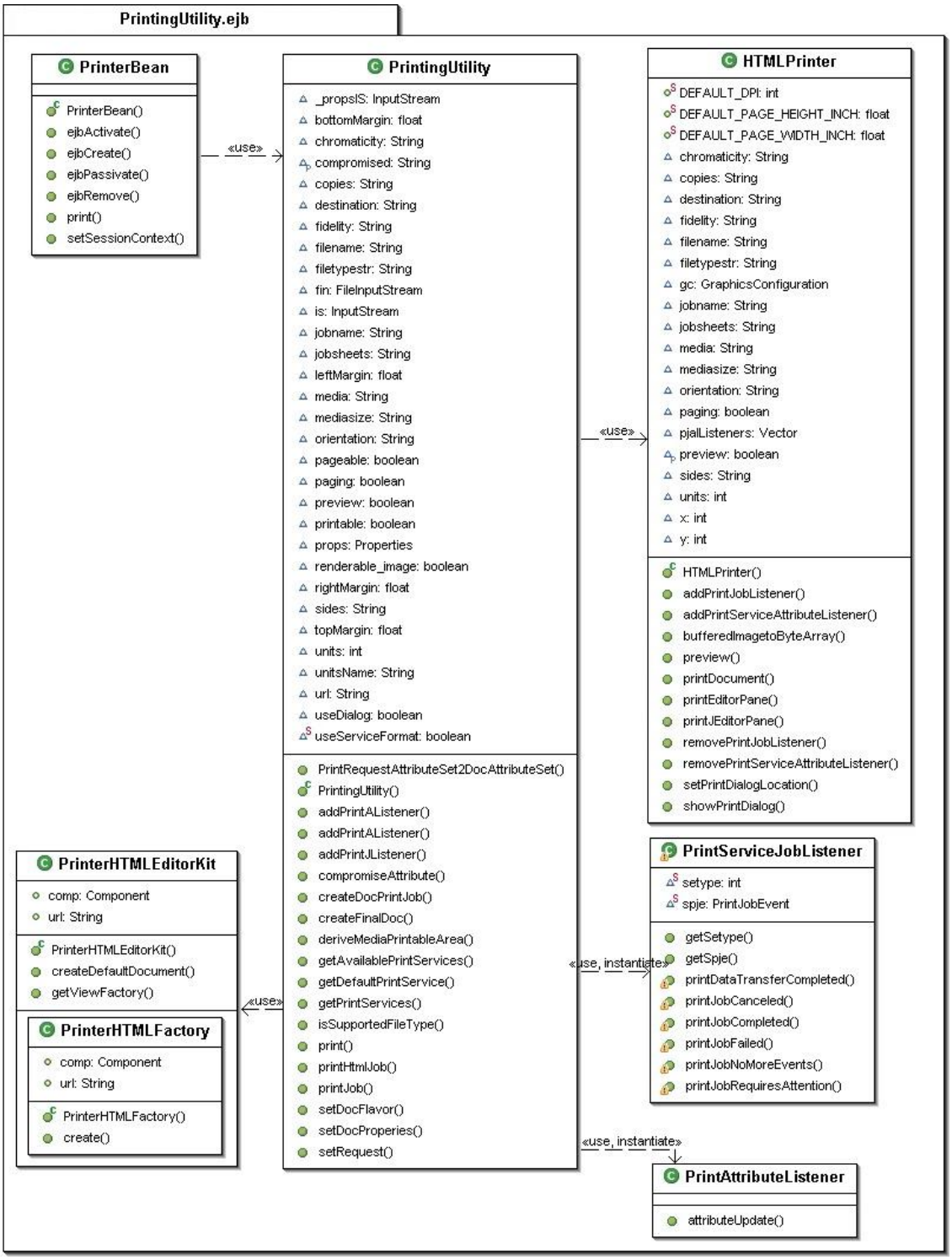
- Το στοιχείο PrintingUtility που είναι ο βασικός συντονιστής της υπηρεσίας. Χρησιμοποιεί τα υπόλοιπα στοιχεία προκειμένου να ολοκληρώσει μια εκτύπωση.
- Το στοιχείο JobListeners το οποίο εμπεριέχει την λειτουργικότητα για αποδοχή των διαφόρων «γεγονότων» της Java (events) τα οποία επηρεάζουν με ασύγχρονο τρόπο τις διάφορες εργασίες εκτύπωσης (π.χ. ασύγχρονα μηνύματα απο τον εκτυπωτή που χρησιμοποιείται για το πότε έχει ολοκληρωθεί μια εργασία εκτύπωσης κ.λ.π.)
- Το στοιχείο PresentationPrinter το οποίο αναλαμβάνει να μετατρέπει κάθε κείμενο που λαμβάνεται για εκτύπωση στην κατάλληλη μορφή (η οποία όπως αναφέρθηκε στο συγκεκριμένο παράδειγμα είναι HTML).
- Το στοιχείο EditorKit είναι μια μορφή plug-in για το αντικείμενο που διαχειρίζεται κείμενο, προκειμένου αυτό να υποστηρίζει την HTML.

Με βάσει τα παραπάνω ο σχεδιασμός προχωράει στην επόμενη φάση όπου τα παραπάνω στοιχεία αναλύονται σε κλάσεις. Επειδή χρησιμοποιούνται EJBs, οι διεπαφές που ορίστηκαν στο Σχήμα 4-60 κατά την υλοποίηση κατανέμομαι στο δικό τους πακέτο όπως φαίνεται στο Σχήμα 4-61:



Σχήμα 4-61: Πακέτο με κλάσεις διεπαφών για το παράδειγμα υπηρεσίας εκτυπώσεων

Αυτό συμβαίνει γιατί οι διεπαφές υλοποιούνται ως «interfaces» της Java, όπως φαίνεται στον ορισμό των κλάσεων. Στην συνέχεια αναλύεται το πακέτο PrintingUtility.ejb, όπως παρατέθηκε παραπάνω:



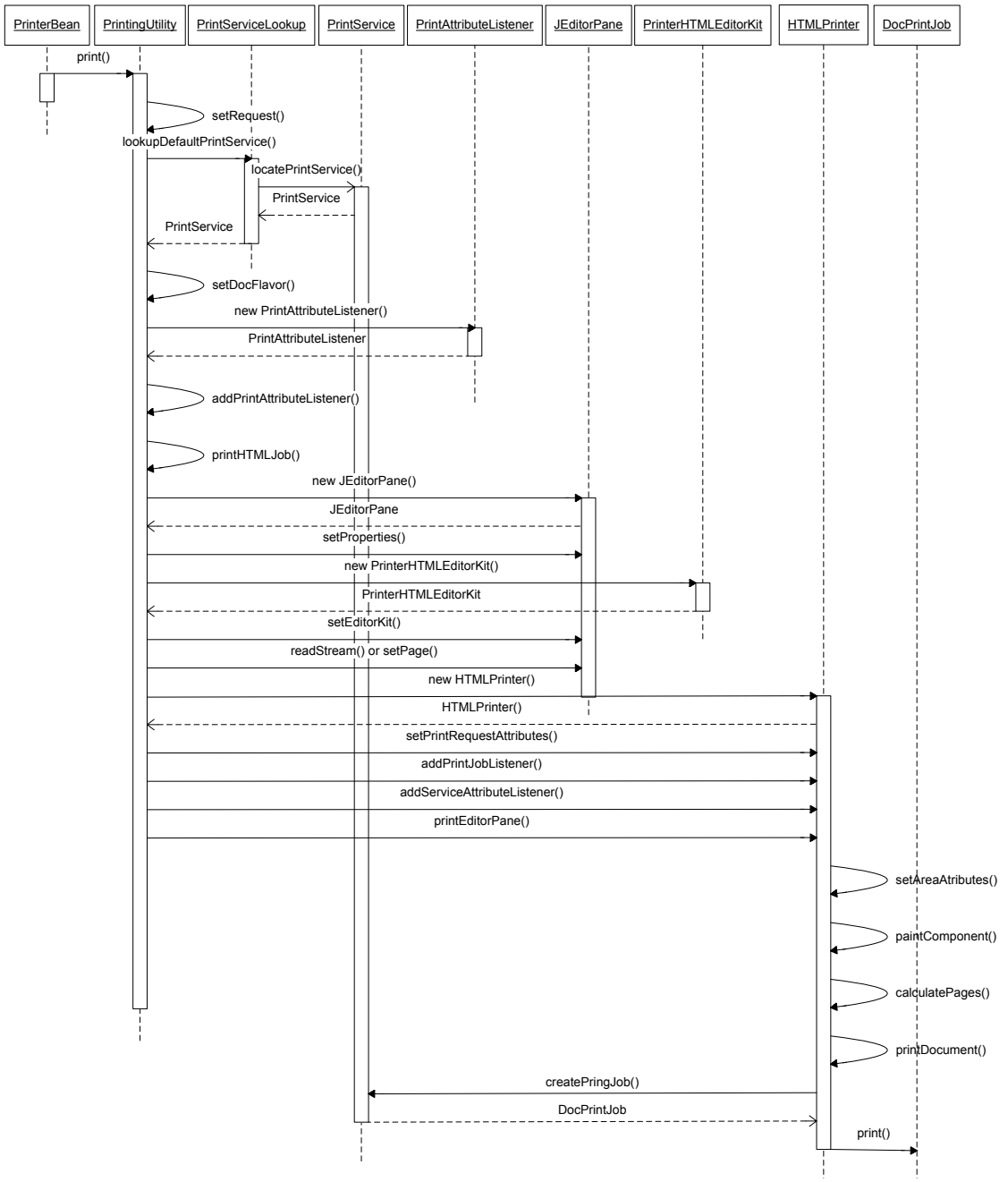
Σχήμα 4-62:Πακέτο με κλάσεις για το παράδειγμα υπηρεσίας εκτυπώσεων

Όπως φαίνεται στο σχήμα:

- το στοιχείο PrintingUtility αναλύθηκε σε μια και μόνη κλάση με το ίδιο όνομα και σε αυτήν έχουν προστεθεί τα χαρακτηριστικά και οι μέθοδοι που επιτελούν την λειτουργικότητα συντονισμού των εκτυπώσεων.
- το στοιχείο PrinterEJB αναλύθηκε επίσης σε μια κλάση με το ίδιο όνομα και υποστηρίζει τις βασικές μεθόδους δημιουργίας και διαχείρισης ενός EJB απο έναν εξυπηρετητή εφαρμογών που υποστηρίζει το πλαίσιο των EJBs.
- το στοιχείο JobListeners αναλύθηκε σε δύο κλάσεις, τις PrintServiceJobListener και PrintAttributeListener, οι οποίες δέχονται διαφορετικά είδη «γεγονότων» κατά την περαίωση εργασιών εκτύπωσης.
- το στοιχείο PresentationPrinter αναλύθηκε στην κλάση HTMLPrinter με τις βασικές μεθόδους για εγκατάσταση των listeners και την εκτύπωση ενός εγγράφου.
- το στοιχείο EditorKit αναλύθηκε στην κλάση PrinterHTMLEditorKit η οποία αναλαμβάνει την μορφοποίηση ενός κειμένου σε HTML και χρησιμοποιεί την εσωτερική κλάση PrinterHTMLFactory για την παραγωγή αντικειμένων τέτοιου τύπου.

Στη συνέχεια ορίζονται οι ακολουθίες μηνυμάτων που ανταλλάσσονται ανάμεσα σε αντικείμενα των παραπάνω κλάσεων βάσει διαγραμμάτων ακολουθίας. Ένα παράδειγμα τέτοιου διαγράμματος αποτελεί αυτό του σχήματος Σχήμα 4-63, στο οποίο φαίνονται χρονικά βήματα για την εκτέλεση μιας εκτύπωσης ανάμεσα σε στιγμιότυπα των κλάσεων που έχουν οριστεί.
Όπως φαίνεται στο σχήμα, η αντίστοιχη περιγραφή της διαδικασίας συνοπτικά είναι η ακόλουθη:

1. Η υπηρεσία εκτύπωσης είναι προσβάσιμη στην αρχιτεκτονική μέσω των διεπαφών της κλάσης PrinterBean, απο τις οποίες γίνεται κλήση στην μέθοδο print(). Η κλάση PrinterBean επί της ουσίας μεταφέρει τις παραμέτρους αυτούσιες στην κλήση της αντίστοιχης μεθόδου print() της συντονιστικής κλάσης PrintingUtility.
2. Η PrintingUtility εσωτερικά θέτει κάποια χαρακτηριστικά της αίτησης προς εκτύπωση με την setRequest() και αναζητά την προκαθορισμένη εκτυπωτική υπηρεσία του συστήματος μέσω της κλάσης PrintServiceLookup και της μεθόδου lookupDefaultPrintService(). Το αντικείμενο «εκτυπωτική υπηρεσία» PrintService εδώ αντικατοπτρίζει τον προκαθορισμένο εκτυπωτή του συστήματος στο οποίο τρέχει η υπηρεσία. Το αντικείμενο εντοπίζεται απο την PrintService και επιστρέφεται πίσω μέχρι την PrintingUtility.
3. Στη συνέχεια η PrintingUtility εσωτερικά θέτει ορισμένα χαρακτηριστικά του PrintService τα οποία έχουν να κάνουν με διάφορες παραμέτρους όπως π.χ. αν θα αποτελείται απο πολλές σελίδες, τι τύπου έγγραφο θα εκτυπωθεί κ.λ.π με την μέθοδο setDocFlavor().
4. Η PrintingUtility δημιουργεί έναν PrintAttributeListener προκειμένου να ενημερώνεται η κλάση αν υπάρχει κάποια αλλαγή σε ένα χαρακτηριστικό και ο PrintAttibuteListener προστίθεται στην κλάση μέσω της addPrintAttributeListener(). Έπειτα η PrintingUtility είναι σε θέση να καλέσει εσωτερικά την μέθοδο printHTMLJob().



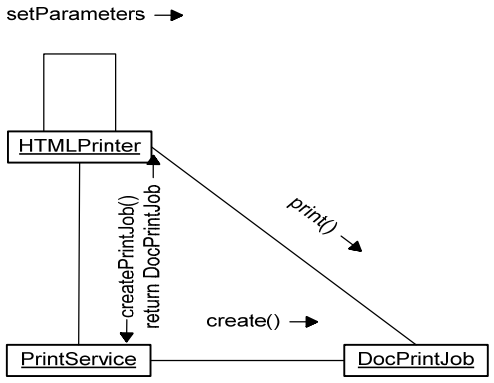
Σχήμα 4-63: Διάγραμμα ακολουθίας για μια διαδικασία εκτύπωσης στην υπηρεσία εκτυπώσεων

5. Εντός της printHTMLJob(), η PrintingUtility κατασκευάζει ένα αντικείμενο JEditorPane το οποίο θα αποτελέσει τη «βάση» αποθήκευσης για το κείμενο που θα εκτυπωθεί. Το αντικείμενο επιστρέφεται στην PrintingUtility, η οποία θέτει ένα σύνολο παραμέτρων του αντικειμένου.
6. Στη συνέχει η PrintingUtility κατασκευάζει ένα αντικείμενο PrinterHTMLEditorKit που αποτελεί επέκταση του αντικειμένου HTMLEditorKit της πρότυπης βιβλιοθήκης της Java, και το οποίο ενσωματώνεται στο JEditorPane που έχει δημιουργηθεί μέσω της μεθόδου setEditorKit() προκειμένου το

τελευταίο να υποστηρίζει τα χαρακτηριστικά μιας HTML σελίδας (γιατί ως τέτοιο θα τυπωθεί το κείμενο που προωθείται στην υπηρεσία εκτύπωσης). Η PrintingUtility διαβάζει το περιεχόμενο του κειμένου χρησιμοποιώντας την μέθοδο readStream() ή setPage() του JEditorPane, ανάλογα με τις παραμέτρους που έχουν οριστεί.

7. Στη συνέχεια η PrintingUtility περνά στην τελική φάση της διαδικασία δημιουργώντας ένα αντικείμενο HTMLPrinter στο οποίο παρέχει τα βασικά αντικείμενα που έχουν δημιουργηθεί ως τώρα (το JEditorPane, το PrintingService).
8. Στον HTMLPrinter τίθενται κάποια χαρακτηριστικά με την setPrintRequestAttributes(), προστίθενται δύο listeners με τις addPrintJobListener() και addServiceAttributeListener(), οι οποίοι επιβλέπουν τα γεγονότα που έχουν να κάνουν με την κατάσταση της εκτύπωσης. Έπειτα καλείται η printEditorPane() και ο έλεγχος περνά στο αντικείμενο HTMLPrinter().
9. Το HTMLPrinter θέτει τις τελικές παραμέτρους της εκτύπωσης με τις μεθόδους setAreaAttributes(), paintComponent(), calculatePages() και καλεί εσωτερικά την μέθοδο printDocument(), η οποία αναλαμβάνει να δημιουργήσει (για κάθε σελίδα που έχει οριστεί) μια διεργασία εκτύπωσης DocPrintJob στο υπάρχον PrintService μέσω μιας κλήσης στην createPrintJob(). Τέλος καλείται η print() κάθε αντικειμένου DocPrintJob() για να αποσταλεί η εκτύπωση στον εκτυπωτή.

Σημειώνεται ότι οι ακριβείς παράμετροι στις κλήσεις μεθόδων παραλείπονται στα πλαίσια του παραπάνω παραδείγματος. Το παράδειγμα ολοκληρώνεται με ένα στιγμιότυπο ενός διαγράμματος συνεργασίας που αντιστοιχεί σε ένα μέρος της προηγούμενης διαδικασίας.



Σχήμα 4-64: Παράδειγμα διαγράμματος συνεργασίας αντικειμένων της υπηρεσίας εκτυπώσεων

Στο παράδειγμα αυτό φαίνεται ότι το αντικείμενο HTMLPrinter αναλαμβάνει να ζητήσει απο το αντικείμενο PrintService δημιουργήσει ένα DocPrintJob για μια συγκεκριμένη εκτύπωση. Στη συνέχεια το HTMLPrinter θέτει κάποιες παραμέτρους και καλεί την μέθοδο print() του DocPrintJob για να εκκινήσει την εκτύπωση.

4.3.5 5^{ο} στάδιο: Αναλυτική οργάνωση υπηρεσιών και επιλογή τεχνολογιών

4.3.5.1 Στόχοι

Στο στάδιο αυτό, οργανώνονται όλες οι υπηρεσίες και οι μηχανισμοί που έχουν σχεδιαστεί μέχρι τώρα σε μια συγκεκριμένη αρχιτεκτονική. Σε πρώτη φάση ορίζονται αυστηρά τα επίπεδα της αρχιτεκτονικής, οι υπηρεσίες που προσφέρει κάθε επίπεδο και πως επικοινωνούν τα επίπεδα μεταξύ τους βάσει λογικών καναλιών. Σε δεύτερη φάση για κάθε δομικό στοιχείο και κανάλι επικοινωνίας λαμβάνεται η απόφαση για την συγκεκριμένη τεχνολογία υλοποίησής του, απο την απόφαση για το λογισμικό των λειτουργικών συστημάτων μέχρι τους τύπους των πρωτοκόλλων επικοινωνίας που θα χρησιμοποιηθούν. Η μεθοδολογία αναπαράστασης των αντικειμένων στο στάδιο αυτό έχει λάβει υπόψην ένα υποσύνολο των σχεδιαστικών αρχών της [Frankel03].
Εφόσον η μέθοδος εντοπίζεται στον σχεδιασμό ΑΔΑΑΥ, είναι προφανές ότι οι τεχνολογίες που θα αποτελούν φυσική επιλογή για την αρχιτεκτονική στην παρούσα χρονική στιγμή θα βασίζονται στην XML, τις Υπηρεσίες Ιστού καθώς και υλοποιήσεις ενός υποσυνόλου των προτύπων που έχουν παρατεθεί στο παράρτημα της διατριβής. Η μεθοδολογία πάντως δεν δεσμεύει τον σχεδιαστή να χρησιμοποιήσει κάτι άλλο μελλοντικά.

4.3.5.2 Μεθοδολογία σταδίου

Τα συγκεκριμένα βήματα που ακολουθούνται στο παρόν 5^{ο} στάδιο είναι τα ακόλουθα:

Ι. **Προδιαγράφεται η όψη μηχανικού** της αρχιτεκτονικής βάσει των εννοιών και της σημειογραφίας του κεφαλαίου 4.3.5.3. Τα επιμέρους βήματα που ακολουθούνται είναι:

1. Ορίζεται το είδος και ο αριθμός των επιπέδων στα οποία θα κατανεμηθούν οι κόμβοι της αρχιτεκτονικής σύμφωνα με τις αρχές της παραγράφου 4.3.5.3.3.1.3.1.
2. Για κάθε υπολογιστικό αντικείμενο ή ομάδα υπολογιστικών αντικειμένων (ανάλογα με το επίπεδο λεπτομέρειας που θέλουμε να επιτύχουμε) που έχει προδιαγραφεί στην υπολογιστική όψη του προηγούμενου σταδίου, σχεδιάζεται ένα αντίστοιχο (βασικό ή σύνθετο) μηχανικό αντικείμενο βάσει των αρχών της παραγράφου 4.3.5.3.3.1.3.3. Στο βήμα αυτό γίνεται απλή απαρίθμηση και αναπαράσταση των μηχανικών αντικειμένων, όχι αναλυτική περιγραφή τους.
3. Όλα τα μηχανικά αντικείμενα του βήματος (2) οργανώνονται σε κόμβους, και οι κόμβοι τοποθετούνται στα επίπεδα του βήματος (1), σύμφωνα με τις αρχές της παραγράφου 4.3.5.3.3.1.3.1.
4. Για κάθε ζεύγος μηχανικών αντικειμένων που επικοινωνούν απο διαφορετικούς κόμβους, σχεδιάζεται ένα κατάλληλο κανάλι μεταξύ τους σύμφωνα με τις αρχές της παραγράφου 4.3.5.3.3.1.3.2. Στο βήμα αυτό γίνεται απλή αναπαράσταση των καναλιών, όχι αναλυτική περιγραφή τους. Στο πέρας του βήματος αυτού, έχουν σχεδιαστεί οι πρώτες εκδόσεις των υψηλού επιπέδου συνολικών διαγραμμάτων εγκατάστασης.
5. Βάσει της υπολογιστικής όψης και των συνολικών διαγραμμάτων εγκατάστασης του βήματος (4), για κάθε μηχανικό αντικείμενο σχεδιάζεται ένα διάγραμμα λεπτομέρειας σύμφωνα με τις αρχές της παραγράφου 4.3.5.3.3.1.3.3.
6. Προαιρετικά εάν θεωρείται απαραίτητο, για κάθε κανάλι που έχει οριστεί στο βήμα (4) σχεδιάζεται ένα διάγραμμα λεπτομέρειας σύμφωνα με τις αρχές της παραγράφου 4.3.5.3.3.1.3.2.

Στο πέρας του βήματος (6), έχει ολοκληρωθεί η πρώτη έκδοση της όψης μηχανικού.

ΙΙ. **Προδιαγράφεται η τεχνολογική όψη** της αρχιτεκτονικής βάσει των εννοιών και της σημειογραφίας του κεφαλαίου 4.3.5.4. Τα επιμέρους βήματα που ακολουθούνται είναι:

1. Για κάθε συνολικό διάγραμμα εγκατάστασης και διάγραμμα λεπτομέρειας μηχανικού αντικειμένου της όψης μηχανικού, δημιουργείται ένα αντίγραφο που θα αποτελέσει μέρος της τεχνολογικής όψης. Τα διαγράμματα αυτά ενημερώνονται και αλλάζουν σύμφωνα με τις αρχές της τεχνολογικής όψης στα βήματα που ακολουθούν.
2. Για κάθε κόμβο του συστήματος επιλέγεται το είδος και η έκδοση του λειτουργικού συστήματος που θα τρέχει ο υπολογιστής και ενημερώνονται όλα τα διαγράμματα κόμβων σύμφωνα με τις αρχές της παραγράφου 4.3.5.4.4.1.1.1.
3. Για κάθε κανάλι που υπάρχει στην όψη μηχανικού επιλέγεται ο τύπος της τεχνολογίας που υποστηρίζει, αρχικά σύμφωνα με τα διαθέσιμα βασικά στοιχεία της παραγράφου 4.3.5.4.5.1. Εάν είναι απαραίτητο, ορίζονται καινούργιοι τύποι καναλιών (βασισμένα σε άλλες τεχνολογίες) σύμφωνα με την μεθοδολογία επέκτασης της παραγράφου 4.3.5.4.6.
4. Όλα τα κανάλια που εμφανίζονται σε συνολικά διαγράμματα εγκατάστασης της τεχνολογικής όψης, ενημερώνονται σύμφωνα με τις αρχές της παραγράφου 4.3.5.4.4.1.1.2.
5. Ενσωματώνονται στις προδιαγραφές τα αντίστοιχα βασικά στοιχεία όψης για τις τεχνολογίες καναλιών που επιλέχθηκαν στο βήμα (3).
6. Κάθε μηχανικό αντικείμενο σε συνολικό διάγραμμα εγκατάστασης και διάγραμμα λεπτομέρειας της τεχνολογικής όψης ενημερώνεται σύμφωνα με τις αρχές της παραγράφου 4.3.5.4.4.1.1.3. Αυτό συνεπάγεται την επιλογή προτύπων υλοποίησης, βιβλιοθήκες, προϊόντα και τεχνολογίες για κάθε αντικείμενο.

Στο πέρας του βήματος (6), έχει ολοκληρωθεί η πρώτη έκδοση της τεχνολογικής όψης.

4.3.5.3 Προδιαγραφή Όψης Μηχανικού

4.3.5.3.1 Εισαγωγή

Η όψη μηχανικού περιγράφει την υποστήριξη που χρειάζεται το σύστημα για να επιτρέψει την κατανομή των αντικειμένων που θα απαρτίζουν την υπολογιστική όψη. Αυτό περιλαμβάνει μονάδες όπου τα αντικείμενα λειτουργούν, όπως είναι οι υπολογιστικοί κόμβοι και οι υποδομές επικοινωνιών, καθώς και όλα τα ήδη πλατφορμών λογισμικού για κατανεμημένα συστήματα.

Η υποδομή αναφοράς για μια ΑΔΑΑΥ μοντελοποιείται με βάση τις έννοιες της όψης μηχανικού του RM-ODP και περιγράφει την ενθυλάκωση των μονάδων του συστήματος και των συνδέσεών τους. Παρόλο που οι τεχνολογίες και τα σχετικά πρότυπα δεν αποτελούν μέρος της όψης μηχανικού με την αυστηρή έννοια, είναι αλληλένδετα, γι' αυτό και η τεχνολογική όψη που ορίζεται στη συνέχεια της μεθοδολογίας, απορρέει άμεσα απο την όψη μηχανικού.

4.3.5.3.2 Έννοιες

Οι έννοιες που ορίζονται στο πρότυπο RM-ODP και χρησιμοποιούνται στη μεθοδολογία προδιαγραφής της όψης μηχανικού είναι αυτές της παραγράφου 7.3.8.2.2.1.4.

4.3.5.3.3 Σημειογραφία

Στην παράγραφο αυτή καθορίζεται τι είδους διαγράμματα χρησιμοποιεί η μεθοδολογία για την αναπαράσταση των αντικειμένων της όψης μηχανικού, και μπορούν να χρησιμοποιηθούν για την επέκταση της όψης. Όλα τα διαγράμματα βασίζονται στην UML.

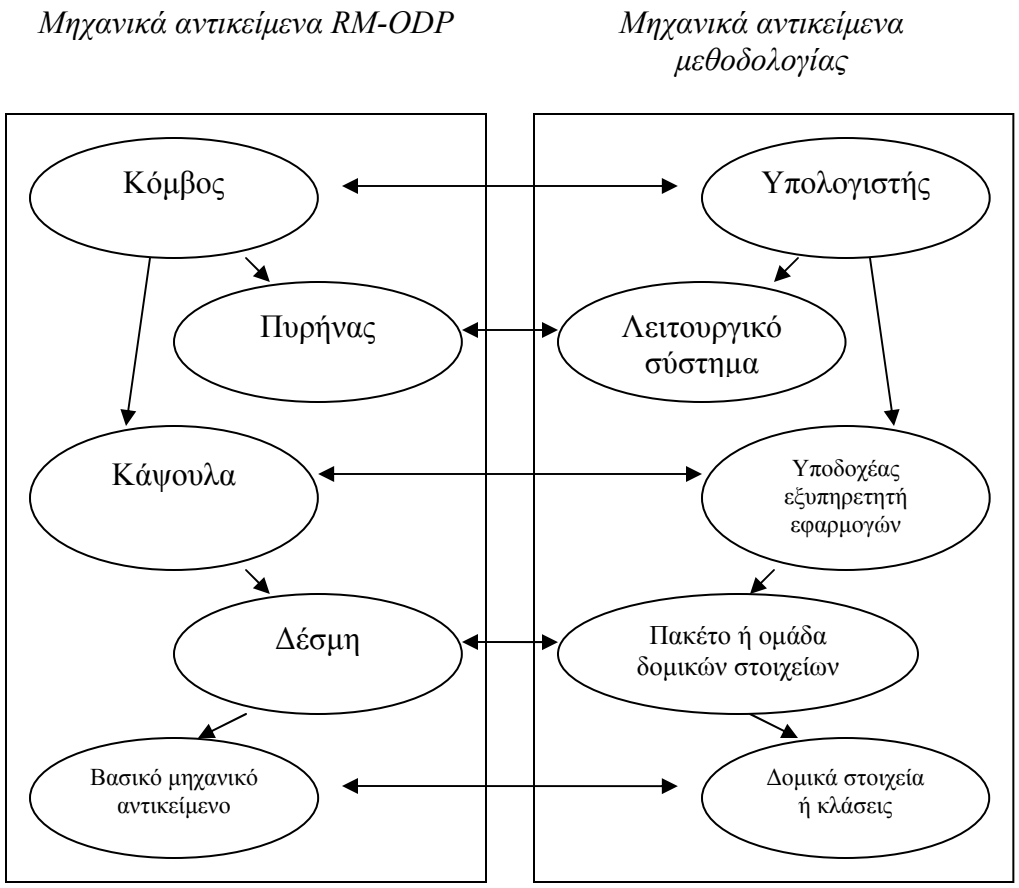
Ένα είδος διαγραμμάτων κυριαρχεί στην παρούσα όψη και αυτό είναι τα *διαγράμματα εγκατάστασης (deployment diagrams)*. Αποδίδουν ικανοποιητικά τόσο την συνολική κατανομή των κόμβων που περιέχουν τις υπηρεσίες στην αρχιτεκτονική, όσο και τον επιμέρους σχεδιασμό των περιεχόμενων καναλιών και των υπηρεσιών / μηχανισμών ως μηχανικά αντικείμενα (engineering objects), όπως αναφέρονται στις έννοιες που προηγήθηκαν.

Οι παράγραφοι που ακολουθούν περιγράφουν πως χρησιμοποιείται η παραπάνω σημειογραφία ως μέρος της μεθοδολογίας.

4.3.5.3.3.1 Μεθοδολογία προδιαγραφής

4.3.5.3.3.1.1 Αντιστοίχηση εννοιών RM-ODP σε στοιχεία της μεθόδου

Στην περίπτωση των αρχιτεκτονικών υπηρεσιών που αποτελούν το βασικό αντικείμενο της παρούσας μεθόδου, κάποιες απο τις έννοιες του προτύπου RM-ODP που παρουσιάστηκαν στην παράγραφο 4.3.5.3.2, αντιστοιχίζονται σε συγκεκριμένα συστατικά στοιχεία μιας ΑΔΑΑΥ και λαμβάνουν μια πιο συγκεκριμένη μορφή.



Σχήμα 4-65: Αντιστοιχία εννοιών μηχανικών αντικειμένων RM-ODP και μεθόδου

Η αντιστοιχία αυτή σχηματικά αναπαρίσταται στο Σχήμα 4-65 και επεξηγείται αναλυτικά στις παραγράφους που ακολουθούν.

4.3.5.3.3.1.1.1 Κόμβοι και πυρήνες

Στην τελική της μορφή μια ΑΔΑΑΥ περιλαμβάνει ένα σύνολο υπολογιστών. Κάθε υπολογιστής βρίσκεται σε ένα δεδομένο επίπεδο της αρχιτεκτονικής. Ένας κόμβος στην γλώσσα μηχανικού αντιστοιχεί σε έναν τέτοιο υπολογιστή. Επίσης, κάθε υπολογιστής αποτελεί ένα αυτοτελές υπολογιστικό σύστημα που διαχειρίζεται και κατανέμει τους πόρους των μηχανικών αντικειμένων που περιλαμβάνει. Όπως φαίνεται και στο Σχήμα 4-65, ένας υπολογιστής βρίσκεται υψηλά στην ιεραρχία των μηχανικών αντικειμένων και περιέχει κάψουλες. Η ακριβής αλληλεπίδραση και επικοινωνία μεταξύ κόμβων – υπολογιστών εξαρτάται απο τις ίδιες τις κάψουλες. Κάθε κόμβος εξαρτάται απο ένα ειδικό μηχανικό αντικείμενο που ονομάζεται πυρήνας, το οποίο αντιστοιχείται στο λειτουργικό σύστημα που τρέχει ο υπολογιστής.

4.3.5.3.3.1.1.2 Κάψουλες και διαχειριστές κάψουλων

Οι υπολογιστές περιέχουν διάφορα είδη εξυπηρετητών οι οποίοι φιλοξενούν τα μηχανικά αντικείμενα που επιτελούν τις επιθυμητές επιχειρησιακές λειτουργίες. Μια κάψουλα του RM-ODP αντιστοιχείται στον *υποδοχέα αντικειμένων ενός εξυπηρετητή εφαρμογών (application server container).* Κάθε κάψουλα κατέχει ένα χώρο αποθήκευσης και ένα

μέρος των υπολογιστικών πόρων του υπολογιστή. Επίσης την κάψουλα διαχειρίζεται ένας διαχειριστής κάψουλων που στην προκειμένη περίπτωση είναι ο ίδιος ο εξυπηρετητής.

4.3.5.3.3.1.1.3 Δέσμες και βασικά μηχανικά αντικείμενα

Τα πακέτα και γενικότερα οι ομάδες δομικών στοιχείων που έχουν οριστεί στο 4^{ο} στάδιο της μεθόδου αντιστοιχούν στις δέσμες της όψης μηχανικού του RM-ODP. Μια δέσμη αποτελεί την μικρότερη δυνατή ομαδοποίηση μηχανικών αντικειμένων ώστε αυτά να αποτελούν μια μονάδα επεξεργασίας. Ακολουθώντας την λογική αυτή, ένα βασικό μηχανικό αντικείμενο είναι είτε ένα δομικό στοιχείο ή μια κλάση.

4.3.5.3.3.1.1.4 Κανάλια

Η αλληλεπίδραση μεταξύ μηχανικών αντικειμένων επιτυγχάνεται και ελέγχεται μέσω των υποστηρικτικών μηχανισμών επικοινωνίας που ονομάζονται κανάλια. Η εδραίωση ενός καναλιού είναι απαραίτητη κάθε φορά που μηχανικά αντικείμενα που πρέπει να επικοινωνήσουν βρίσκονται σε διαφορετικούς κόμβους, οπότε και δημιουργείται μια *κατανεμημένη δέσμευση (distributed binding)*. Στην περίπτωση που η αλληλεπίδραση μεταξύ μηχανικών αντικειμένων συμβαίνει μέσα στον ίδιο κόμβο ή και μέσα στην ίδια δέσμη, τότε χρησιμοποιείται *τοπική δέσμευση (local binding)* και δεν απαιτείται κανάλι.
Ένα κανάλι επί της ουσίας αποτελεί μια διαμόρφωση απο στελέχη, δεσμευτές και αντικείμενα πρωτοκόλλων που διασυνδέουν ένα σύνολο απο μηχανικά αντικείμενα. Τα μηχανικά αντικείμενα που επικοινωνούν είναι τοπικά δεσμευμένα σε στελέχη. Ένα στέλεχος παρέχει την μετατροπή των δεδομένων που επιβάλλει η αλληλεπίδραση, εφαρμόζει ελέγχους, κρατάει αρχεία ασφάλειας και αλληλεπιδρά με άλλα μηχανικά αντικείμενα εκτός του καναλιού αν είναι απαραίτητο (π.χ. για λόγους ασφάλειας).
Ένας δεσμευτής διαχειρίζεται την απ' άκρο σ' άκρο ακεραιότητα του καναλιού, παρέχει την διαφάνεια τοποθεσίας και ενδέχεται να αλληλεπιδρά με μηχανικά αντικείμενα εκτός του καναλιού προκειμένου να επιτελέσει τις λειτουργίες του.
Ένα αντικείμενο πρωτοκόλλου παρέχει επικοινωνιακές συναρτήσεις, διαχειρίζεται πιθανά πρωτόκολλα που χρησιμοποιούνται στο κανάλι, και παρέχει πρόσβαση σε υποστηρικτικές υπηρεσίες, όπως για παράδειγμα καταλόγους ονομάτων για την μετάφραση διευθύνσεων αν αυτό είναι απαραίτητο.
Η γλώσσα μηχανικού αναφέρει τρεις τύπους καναλιών που αντιστοιχούν στους τρεις τύπους διεπαφών που χρησιμοποιούν τα υπολογιστικά αντικείμενα στην υπολογιστική όψη:

- Ένα *κανάλι λειτουργιών (operation channel)* αντιστοιχεί μια *διεπαφή λειτουργιών (operation interface)*. Για το κανάλι καθορίζεται ένα σύνολο λειτουργιών που υποστηρίζει η διεπαφή και το αν η διεπαφή έχει τον ρόλο του «πελάτη» ή του «εξυπηρετητή» για το σύνολο αυτό.
- Ένα *κανάλι ροής (stream channel)* αντιστοιχεί σε μια *διεπαφή ροής (stream interface)*. Για το κανάλι καθορίζεται ένα σύνολο ροών που υποστηρίζονται απο την διεπαφή και για κάθε ροή εάν η διεπαφή έχει τον ρόλο του «παραγωγού» ή του «καταναλωτή».

- Ένα *κανάλι σήματος (signal channel)* αντιστοιχεί σε μια *διεπαφή σήματος (signal interface)*. Για το κανάλι καθορίζεται ένα σύνολο σημάτων που υποστηρίζει η διεπαφή και για κάθε σήμα εάν η διεπαφή έχει το ρόλο του πομπού ή του αποδέκτη.

Όπως είναι φανερό, η λειτουργικότητα των μηχανικών αντικειμένων που επικοινωνούν καθορίζει τι είδους κανάλια χρειάζεται να εδραιωθούν μεταξύ τους. Σε αρχιτεκτονικές υπηρεσιών συνήθως απαντώνται τα κανάλια λειτουργικών, αλλά δεν αποκλείεται να χρειάζονται και κανάλια ροής στην περίπτωσης υπηρεσιών που έχουν να κάνουν με δεδομένα ήχου, βίντεο κ.λ.π.

4.3.5.3.3.1.2 Αντιστοίχηση αντικειμένων σε συναρτήσεις συστημάτων ODP

Όπως παρουσιάστηκε στην παράγραφο 7.3.8.2.3, τα ανοιχτά κατανεμημένα συστήματα που προδιαγράφονται σύμφωνα με το RM-ODP επιδεικνύουν ένα σύνολο συναρτήσεων οι οποίες καθορίζουν το επίπεδο της υλοποίησης διαφανειών κατανομής (που χρησιμοποιούν τις συναρτήσεις). Σύμφωνα με την παρουσίαση που έχει γίνει μέχρι τώρα ως προς τα συστατικά στοιχεία που προδιαγράφονται με την παρούσα κατασκευαστική μέθοδο, ο πίνακας που ακολουθεί περιγράφει τα είδη των συναρτήσεων που πρέπει να υλοποιούνται στο προς σχεδιασμό σύστημα και ποιό ακριβώς στοιχείο υλοποιεί κάθε συνάρτηση.

Πίνακας 4-4: Συναρτήσεις ODP και στοιχεία που τις υλοποιούν

Ομάδα συναρτήσεων	**Συνάρτηση**	**Στοιχείο που την υλοποιεί**
Διαχείρισης	Διαχείρισης κόμβου	Λειτουργικό σύστημα
	Διαχείρισης αντικειμένων	Λειτουργικό σύστημα, Εξυπηρετητής εφαρμογών, Υπηρεσία διαχείρισης διεργασιών, Υπηρεσία διαχείρισης χρηστών
	Διαχείρισης δεσμών	Εξυπηρετητής εφαρμογών, Υπηρεσία διαχείρισης διεργασιών, Υπηρεσία διαχείρισης χρηστών
	Διαχείρισης κάψουλων	Εξυπηρετητής εφαρμογών
Συντονισμού	Ειδοποίησης γεγονότων	Λειτουργικό σύστημα, Εξυπηρετητής εφαρμογών Υπηρεσία ειδοποιήσεων
	Παρακολούθησης σημείων ελέγχου και ανάκαμψης	Εξυπηρετητής εφαρμογών
	Απενεργοποίησης και επανενεργοποίησης	Εξυπηρετητής εφαρμογών
	Ομαδοποίησης	Υπηρεσία διαχείρισης (προαιρετικά)
	Αντιγραφής	Υπηρεσία διαχείρισης (προαιρετικά)
	Μετανάστευσης	Υπηρεσία διαχείρισης (προαιρετικά)

	Συναλλαγών	Υπηρεσία διαχείρισης εργασιών, Επιχειρησιακές υπηρεσίες
	Παρακολούθησης αναφορών διεπαφών μηχανικών αντικειμένων	Λειτουργικό σύστημα
Αποθετηρίων	Αποθήκευσης	Υπηρεσία διαχείρισης αποθετηρίων, Υπηρεσία δημοσίευσης και αναζήτησης σε καταλόγους Υπηρεσιών Ιστού, Υπηρεσία υποστήριξης υπαρχουσών υποδομών
	Οργάνωσης πληροφορίας	Υπηρεσία διαχείρισης αποθετηρίων, Υπηρεσία δημοσίευσης και αναζήτησης σε καταλόγους Υπηρεσιών Ιστού, Υπηρεσία υποστήριξης υπαρχουσών υποδομών
	Επανατοποθέτησης	Υπηρεσία διαχείρισης διεργασιών
	Αποθετηρίου τύπων	Υπηρεσία δημοσίευσης και αναζήτησης σε καταλόγους Υπηρεσιών Ιστού
	Αγοραπωλησίας	Υπηρεσία δημοσίευσης και αναζήτησης σε καταλόγους Υπηρεσιών Ιστού
Ασφάλειας	Ελέγχου πρόσβασης	Λειτουργικό σύστημα, Υπηρεσία ελέγχου πρόσβασης
	Ελέγχων ασφάλειας	Λειτουργικό σύστημα, Υπηρεσία ελέγχου πρόσβασης
	Αυθεντικοποίησης	Λειτουργικό σύστημα, Υπηρεσία διαχείρισης ταυτότητας
	Ακεραιότητας	Λειτουργικό σύστημα, Μηχανισμός ψηφιακών υπογραφών
	Εμπιστευτικότητας	Μηχανισμός κρυπτογράφησης
	Εξασφάλισης μη άρνησης συμμετοχής	Μηχανισμός προηγμένων ηλεκτρονικών υπογραφών
	Διαχείρισης κλειδιών	Υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών

Όπως φαίνεται απο τον παραπάνω πίνακα, οι συναρτήσεις των ODP συστημάτων κατανέμονται σε τρία επίπεδα:

- στο κατώτερο επίπεδο του λειτουργικού συστήματος των κόμβων
- στο επιχειρησιακό επίπεδο του εξυπηρετητή εφαρμογών,

- και στο ανώτερο επίπεδο των ίδιων των εφαρμογών οι οποίες υλοποιούνται ως μηχανισμοί ή υπηρεσίες μέσα στην αρχιτεκτονική.

Σε κάθε επίπεδο υλοποιείται ένα υποσύνολο των συναρτήσεων, και κάποια επίπεδα υλοποιούν και την ίδια συνάρτηση για διαφορετικά αντικείμενα.

4.3.5.3.3.1.3 Διαγράμματα εγκατάστασης

Στην παρούσα παράγραφο παρουσιάζεται ο τρόπος με τον οποίο χρησιμοποιούνται τα διαγράμματα εγκατάστασης της UML προκειμένου να αναπαρασταθούν τα μηχανικά αντικείμενα και τα κανάλια στην όψη μηχανικού.
Η παρούσα μέθοδος ορίζει δύο ειδών διαγράμματα για την όψη μηχανικού: *υψηλού επιπέδου συνολικά διαγράμματα εγκατάστασης* τα οποία αναπαριστούν τα μηχανικά αντικείμενα κατά την εγκατάστασή τους σε μια υλοποίηση της αρχιτεκτονικής (*high-level overall deployment diagrams*) και *διαγράμματα λεπτομέρειας (detail deployment diagrams)* τα οποία κατασκευάζονται για κάθε μηχανικό αντικείμενο .
Τα υψηλού επιπέδου διαγράμματα είναι συνήθως λίγα (ανάλογα με τους κόμβους της αρχιτεκτονικής και τα μηχανικά αντικείμενα που περιλαμβάνουν), επιδεικνύουν σαφώς τα επίπεδα της αρχιτεκτονικής και τους κόμβους του κάθε επιπέδου και χρησιμοποιούν όλες τις σχεδιαστικές αρχές της παραγράφου 4.3.5.3.3.1.3. Ο αριθμός των διαγραμμάτων λεπτομέρειας εξαρτάται απο τον αριθμό των μηχανικών αντικειμένων που θεωρεί ο σχεδιαστής πρέπει να αναπαρασταθούν λεπτομερώς και χρησιμοποιούν μόνο τις σχεδιαστικές αρχές που διέπουν το διάγραμμα του σχήματος Σχήμα 4-71.

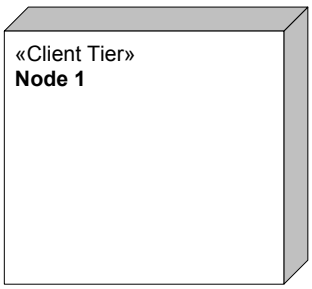
4.3.5.3.3.1.3.1 Επίπεδα αρχιτεκτονικής και κόμβοι

Τα επίπεδα που ορίζει η μεθοδολογία είναι τα ακόλουθα (σε συμφωνία με τις συνήθεις πρακτικές δόμησης πληροφοριακών συστημάτων):

- *Επίπεδο Πελάτη (Client Tier)*: αποτελεί το επίπεδο με το οποίο αλληλεπιδρούν οι χρήστες του συστήματος προκειμένου να χρησιμοποιήσουν τις υπηρεσίες της αρχιτεκτονικής
- *Επίπεδο Αλληλεπίδρασης (Interaction Tier)*: αποτελεί ένα ενδιάμεσο επίπεδο μεταξύ του επιπέδου πελάτη και του επιχειρησιακού επιπέδου. Λαμβάνει τις αιτήσεις απο το επίπεδο πελάτη, τις προωθεί στο επιχειρησιακό επίπεδο και επιστρέφει πίσω τις απαντήσεις κατάλληλα διαμορφωμένες για την εφαρμογή πελάτη που χρησιμοποιεί ένας χρήστης.
- *Επιχειρησιακό επίπεδο (Enterprise Tier)*: αποτελεί τον πυρήνα της αρχιτεκτονικής. Στο επίπεδο αυτό οργανώνονται και συντονίζονται όλες οι υπηρεσίες που περιλαμβάνει η αρχιτεκτονική.
- *Επίπεδο ολοκλήρωσης (Integration Tier)*: επιτελεί όλες τις απαραίτητες λειτουργίες για την διασύνδεση του επιχειρησιακού επιπέδου με υπάρχουσες ή παλαιότερες υποδομές των οργανισμών που συμμετέχουν στην αρχιτεκτονική.

Ένας κόμβος αναπαρίσταται με έναν κόμβο της UML, όπως φαίνεται στο Σχήμα 4-66. Η μεθοδολογία επιβάλλει κάθε κόμβος που συμμετέχει στην αρχιτεκτονική στα διαγράμματα της όψης μηχανικού να χαρακτηρίζεται με ένα πρότυπο της UML με ένα

απο τα παραπάνω επίπεδα για να είναι ξεκάθαρη η λειτουργικότητά του, όπως αναπαρίσταται στο Σχήμα 4-66

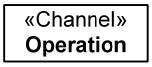


Σχήμα 4-66:Κόμβος της UML για την αναπαράσταση ενός κόμβου στην όψη μηχανικού

Όπως περιγράφηκε στις προηγούμενες παραγράφους, κάθε κόμβος αποτελεί μια διαμόρφωση μηχανικών αντικειμένων που σχηματίζουν μια μονάδα, και στον πραγματικό κόσμο αναπαριστά έναν ή περισσότερους υπολογιστές.
Στα πλαίσια της παρούσας μεθοδολογίας, κάθε κόμβος στην όψη μηχανικού απαριθμείται (1, 2 κ.λ.π) ή του δίνεται κάποιο κεφαλαίο γράμμα, ή κάποια συγκεκριμένη ονομασία, ανάλογα με την λειτουργία που επιτελεί. Επίσης κάθε κόμβος χαρακτηρίζεται με ένα πρότυπο της UML, που αντικατοπτρίζει το είδος του επίπεδου της αρχιτεκτονικής στο οποίο συμμετέχει. Τα είδη των προτύπων που χρησιμοποιούνται στην παρούσα μέθοδο περιγράφηκαν στην προηγούμενη παράγραφο.

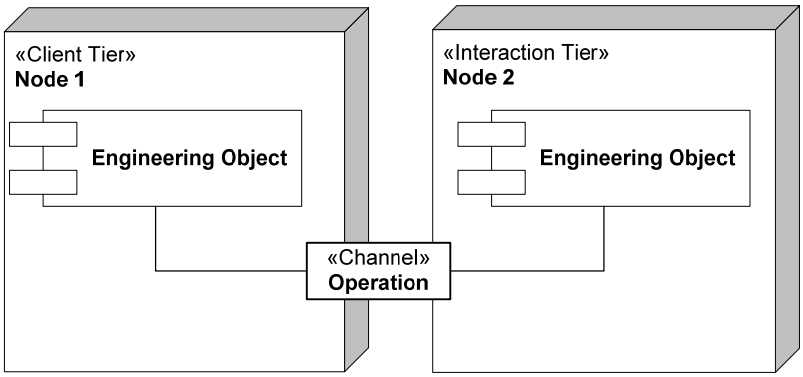
4.3.5.3.3.1.3.2 Κανάλια

Τα κανάλια χρησιμοποιούνται για να υποδείξουν τον τύπο και τα χαρακτηριστικά της επικοινωνίας ανάμεσα σε μηχανικά αντικείμενα που βρίσκονται σε **διαφορετικούς** κόμβους. Η αναπαράσταση ενός καναλιού γίνεται με χρήση ενός σχήματος αντικειμένου ή κλάσης της UML, στο οποίο αναγράφεται ο τύπος του καναλιού και του δίνεται το πρότυπο «κανάλι» («channel»), όπως φαίνεται στο παράδειγμα του σχήματος που ακολουθεί:



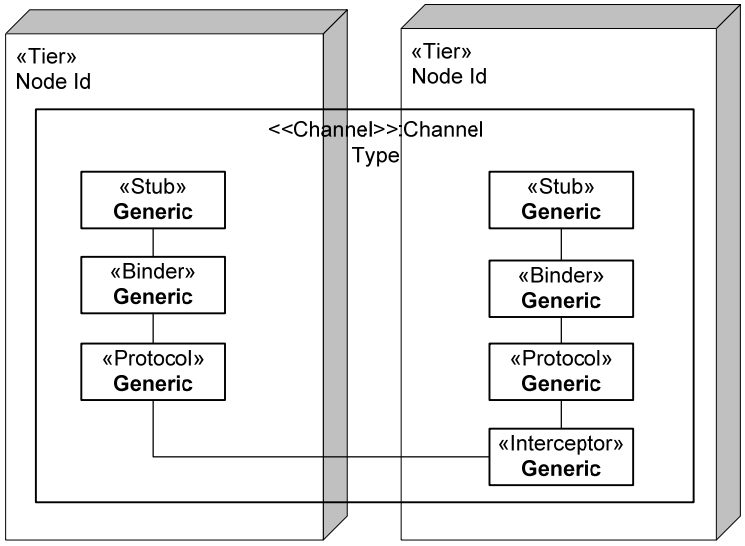
Σχήμα 4-67:Παράδειγμα αναπαράστασης ενός καναλιού λειτουργιών

Στα συνολικά διαγράμματα εγκατάστασης, τα κανάλια τοποθετούνται ανάμεσα σε δύο κόμβους και ενώνονται με γραμμές συσχετίσεως με τα μηχανικά αντικείμενα τα οποία ενώνουν, όπως φαίνεται στο Σχήμα 4-68:



Σχήμα 4-68: Τοποθέτηση καναλιών σε συνολικό διάγραμμα εγκατάστασης της όψης μηχανικού

Όπως αναφέρθηκε στην παράγραφο 4.3.5.3.3.1.1.4, ένα κανάλι στην όψη μηχανικού μπορεί να είναι λειτουργιών, ροής ή σημάτων. Όλοι οι τύποι καναλιών αναλύονται περαιτέρω σε ένα διάγραμμα λεπτομέρειας και περιέχουν κοινά στοιχεία. Ένα κανάλι έχει την γενικευμένη αναλυτική μορφή του ακόλουθου σχήματος:



Σχήμα 4-69: Ανάλυση ενός καναλιού σε διάγραμμα λεπτομέρειας της όψης μηχανικού

Όπως φαίνεται απο το σχήμα, κάθε κανάλι που εδραιώνεται ανάμεσα σε δυο μηχανικά αντικείμενα αποτελείται απο ένα στέλεχος, έναν δεσμευτή, ένα αντικείμενο πρωτοκόλλου και ενδεχομένως έναν αναχαιτιστή. Οι ορισμοί των παραπάνω εννοιών έχουν δοθεί στην παράγραφο 4.3.5.3.2, αλλά στο σημείο αυτό γίνεται μια περαιτέρω επεξήγηση προκειμένου να είναι κατανοητή η λειτουργικότητα τους, ώστε να αποδίδεται σωστά σε αντικείμενα που σχεδιάζονται:

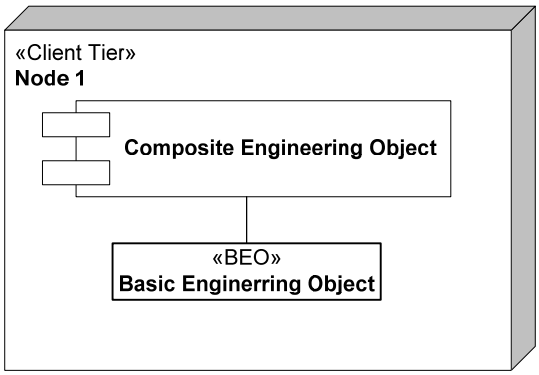
- Ένα στέλεχος συνήθως αναπαριστά στοιχεία ή λογισμικό που αναλαμβάνει να διαρθρώσει (κατά την αποστολή) και αποδιαρθρώσει (κατά την λήψη) τα δεδομένα που πρόκειται να μεταφερθούν στην κατάλληλη μορφή προκειμένου να αποτελούν μια μεταφέρσιμη δομή πάνω απο το κανάλι.

- Ένας δεσμευτής επιτυγχάνει την αντιστοίχηση της δομής που παράγει το στέλεχος σε ένα σε ένα (ή περισσότερα) δεδομένά πρωτόκολλα επικοινωνίας του δικτύου που χρησιμοποιείται κατά την μεταφορά.
- Το αντικείμενο πρωτοκόλλου είναι αυτό που επιτελεί την ίδια την επικοινωνία μεταφέροντας τα δεδομένα, σύμφωνα με το πρωτόκολλο που έχει επιλεγεί και στο οποίο τα έχει δεσμεύσει ο δεσμευτής.
- Τέλος, ένας αναχαίτισης χρησιμοποιείται προκειμένου να επιτευχθούν ενδεχόμενες μεταφράσεις των δεδομένων που ανταλλάσσουν μεταξύ τους αντικείμενα πρωτοκόλλου αν αυτό είναι απαραίτητο, λόγω περάσματος απο μια περιοχή διαχείρισης σε μια άλλη ή την εφαρμογή κάποιου πρωτοκόλλου μετατροπής σε χαμηλό επίπεδο (όπως π.χ. εάν έχουμε κρυπτογραφία στο κανάλι μεταφοράς).

Τα παραπάνω στοιχεία ενός καναλιού συνήθως επηρεάζονται απο την τεχνολογία που χρησιμοποιείται για την υλοποίηση του καναλιού. Για το λόγο αυτό, στις προδιαγραφές της όψης μηχανικού η έμφαση δίνεται στο ποια απο αυτά τα στοιχεία είναι παρόντα σε ένα κανάλι, και όχι τι αυτά αντιπροσωπεύουν. Οπότε ως μέρος των προδιαγραφών οργανώνονται σε «τύπους καναλιών» όλοι οι συνδυασμοί στοιχείων καναλιού που υπάρχουν στην αρχιτεκτονική και τα στοιχεία χαρακτηρίζονται με τον τίτλο «γενικευμένο» (generic) όπως ακριβώς στο σχήμα, και έπειτά παρατίθεται το σύνολο των καναλιών που χρησιμοποιούν κάθε τύπο.

4.3.5.3.3.1.3.3 Μηχανικά αντικείμενα

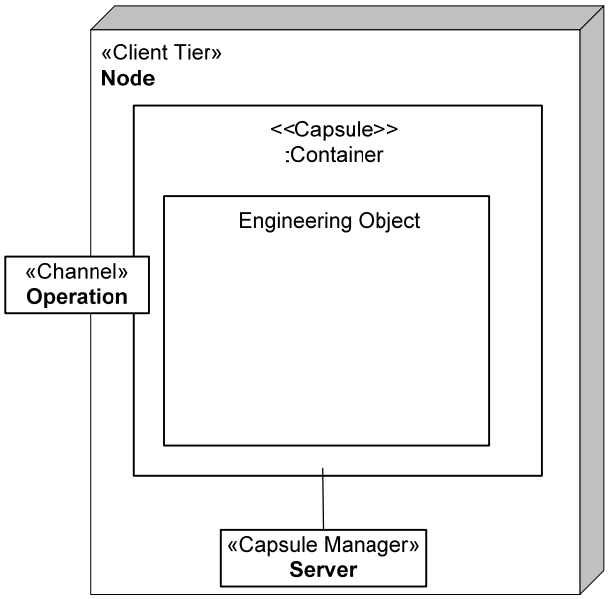
Όταν πρόκειται να σχεδιαστεί ένα συνολικό διάγραμμα εγκατάστασης της όψη μηχανικού, στο οποίο τοποθετούνται όλα τα μηχανικά αντικείμενα και φαίνονται οι διασυνδέσεις τους, τα μηχανικά αντικείμενα αναπαρίστανται είτε με ένα διάγραμμα στοιχείου της UML (component diagram) ή με μια απλή κλάση της UML:



Σχήμα 4-70: Αναπαράσταση μηχανικών αντικειμένων σε συνολικό διάγραμμα εγκατάστασης της όψης μηχανικού

Ένα διάγραμμα στοιχείου χρησιμοποιείται συνήθως για την αναπαράσταση ενός σύνθετου μηχανικού αντικειμένου που αποτελείται απο δύο ή περισσότερα βασικά μηχανικά αντικείμενα, ενώ η κλάση για ένα βασικό μηχανικό αντικείμενο που δεν διαχωρίζεται περαιτέρω σε άλλα αντικείμενα. Αυτό υποδεικνύεται με το πρότυπο «Βασικό Μηχανικό Αντικείμενο» («BEO»).

Μηχανικά αντικείμενα εντός του ίδιου κόμβου που συσχετίζονται, απλά διασυνδέονται με μια γραμμή συσχετίσεως της UML όπως φαίνεται στο Σχήμα 4-70, ενώ αν βρίσκονται σε διαφορετικούς κόμβους ανάμεσά τους παρεμβάλλεται το κατάλληλο κανάλι, όπως φαίνεται στο Σχήμα 4-68.
Κάθε μηχανικό αντικείμενο, αφού τοποθετηθεί σε συνολικό διάγραμμα εγκατάστασης, χρίζει και περαιτέρω ανάλυσης. Για το σκοπό αυτό, όπως έχει ήδη αναφερθεί, δημιουργούνται τα διαγράμματα λεπτομέρειας στα οποία χρησιμοποιείται ένα σχήμα όπως το ακόλουθο:



Σχήμα 4-71: Αναλυτική αναπαράσταση μηχανικού αντικειμένου σε διάγραμμα λεπτομέρειας της όψης μηχανικού

Στο σχήμα αυτό αναπαρίσταται η εξής πληροφορία για κάθε μηχανικό αντικείμενο:

- Ο κόμβος στον οποίο βρίσκεται.
- Τα κανάλια με τα οποία επικοινωνεί με άλλα μηχανικά αντικείμενα εκτός του κόμβου.
- Μηχανικά αντικείμενα απο τα οποία αποτελείται το συγκεκριμένο αντικείμενο. Προκειμένου να μην υπάρχει περίσσεια επικάλυψη και επανάληψη με τις προδιαγραφές της υπολογιστικής όψης, η αναπαράσταση μηχανικών αντικειμένων που αντιστοιχούν σε υπολογιστικά αντικείμενα, συνήθως περιορίζεται στις διεπαφές που υποστηρίζει και υλοποιεί το μηχανικό αντικείμενο.
- Το περιβάλλον λειτουργίας του αντικειμένου αν αυτό τρέχει σε έναν εξυπηρετητή εφαρμογών.

Η πληροφορία για το περιβάλλον λειτουργίας του αντικειμένου αναπαρίσταται τοποθετώντας το μηχανικό αντικείμενο μέσα σε ένα πλαίσιο το οποίο χαρακτηρίζεται ως Υποδοχέας Εξυπηρετητή Εφαρμογών (Container) με το πρότυπο «Κάψουλα» («Capsule»). Επίσης ο εξυπηρετητής στον οποίο ανήκει ο υποδοχέας ενώνεται με το τον υποδοχέα με μια γραμμή συσχετίσεως και έχει το πρότυπο «Διαχειριστής Κάψουλας»

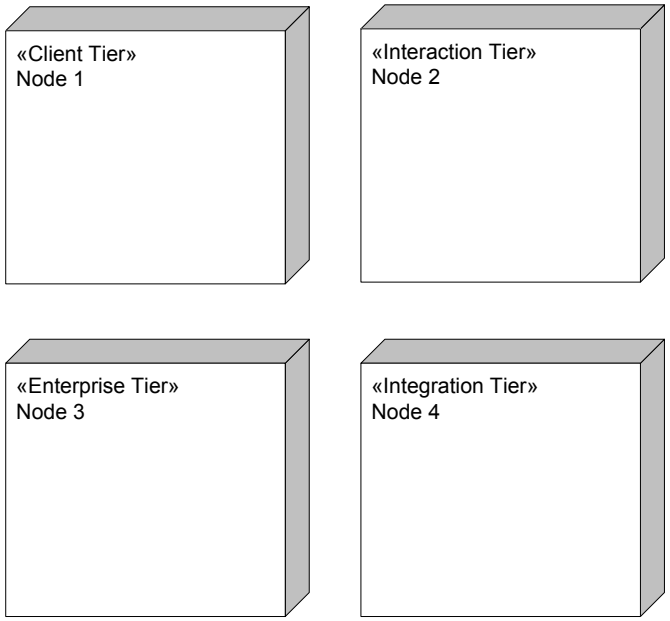
(«Capsule Manager») (η αντιστοίχηση των εννοιών του RM-ODP περιγράφηκε στην παράγραφο 4.3.5.3.3.1.1.2).

4.3.5.3.3.2 Βασικά στοιχεία όψης

Οι παράγραφοι που ακολουθούν περιγράφουν τα βασικά επαναχρησιμοποιήσιμα στοιχεία της όψης μηχανικού. Ο αριθμός των βασικών στοιχείων της συγκεκριμένης όψης είναι περιορισμένος διότι ο σχεδιασμός κάθε αντικειμένου είναι στενά δεμένη με την συγκεκριμένη εγκατάσταση που θα ακολουθηθεί σε μια σχεδιαζόμενη αρχιτεκτονική (αριθμός και είδος επιπέδων, αντικείμενα σε κάθε επίπεδο, σύνολο εξυπηρετητών (και άρα υποδοχέων που φιλοξενούν μηχανικά αντικείμενα), αριθμός και είδος καναλιών που υποστηρίζει κάθε αντικείμενο).

4.3.5.3.3.2.1 Κόμβοι

Υπάρχουν τεσσάρων ειδών κόμβοι σε ένα διάγραμμα εγκατάστασης της όψης μηχανικού που αντιστοιχούν στα είδη των επιπέδων που ορίζονται στην αρχιτεκτονική:

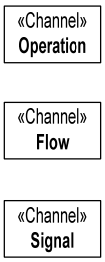


Σχήμα 4-72: Βασικά στοιχεία όψης για την αναπαράσταση κόμβων

Στη συνήθη πρακτική κόμβοι στο επίπεδο αλληλεπίδρασης παρεμβάλλονται πάντα μεταξύ κόμβων στο επίπεδο πελάτη και στο επιχειρησιακό επίπεδο. Επίσης οι κόμβοι του επιπέδου ολοκλήρωσης συνήθως είναι πάντα συνδεδεμένοι μόνο με το επιχειρησιακό επίπεδο και κανένα άλλο ώστε να υπάρχει αυστηρός έλεγχος των οντοτήτων που αλληλεπιδρούν με τα υπάρχοντα συστήματα.

4.3.5.3.3.2.2 Κανάλια

Τα κανάλια στην μηχανική όψη όπως έχει περιγραφεί είναι τριών ειδών, οπότε προκύπτουν αντίστοιχα και τρία βασικά στοιχεία όψης για τα υψηλού επιπέδου συνολικά διαγράμματα εγκατάστασης:



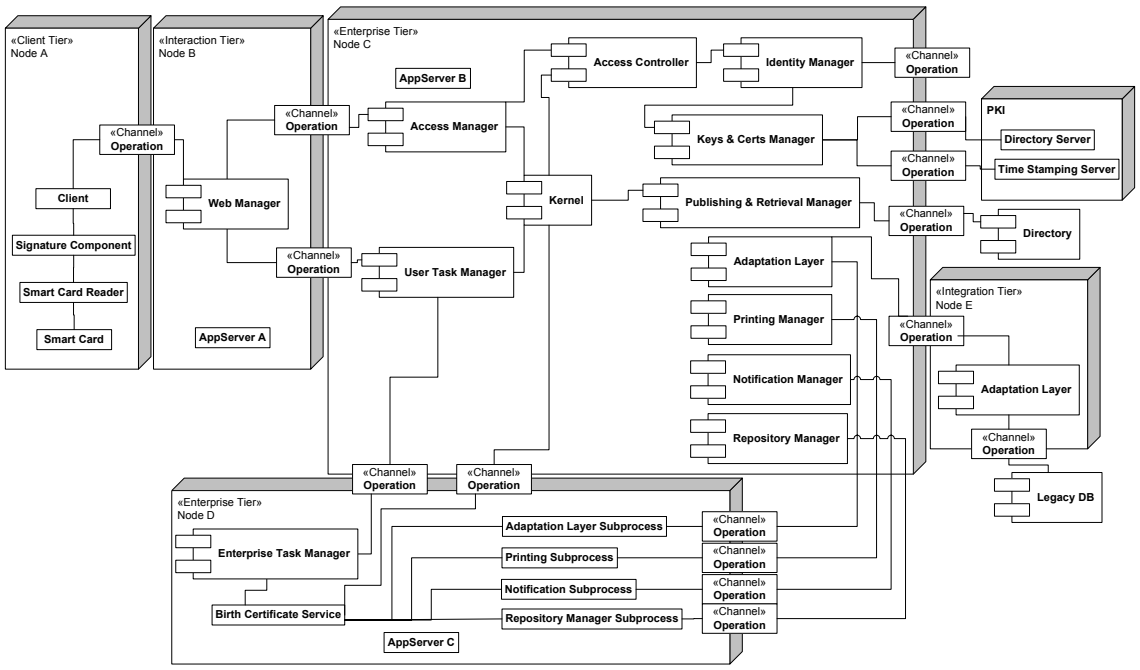
Σχήμα 4-73: Βασικά στοιχεία όψης για την αναπαράσταση καναλιών

Τα αντίστοιχα διαγράμματα λεπτομέρειας που αντιστοιχούν σε κάποιο κανάλι μέσα σε μια συγκεκριμένη αρχιτεκτονική εξαρτώνται απο το είδος των μηχανικών αντικειμένων που επικοινωνούν μέσω του καναλιού και τα δεδομένα που ανταλλάσσονται (το οποίο π.χ. επηρεάζει αν θα υπάρχουν αναχαιτιστές ή όχι κ.λ.π.).

4.3.5.3.3.3 Μεθοδολογία επέκτασης και παραδείγματα

Στην περίπτωση που σε μια αρχιτεκτονική χρειάζεται να οριστούν νέα επίπεδα, τότε αυτό γίνεται με τον ορισμό νέων προτύπων της UML τα οποία αποδίδονται ανάλογα σε κόμβους που σχεδιάζονται. Το ίδιο δεν ισχύει στην περίπτωση των καναλιών, προκειμένου να υπάρχει μια στενή σχέση με τις έννοιες του RM-ODP, το οποίο ορίζει αυστηρά τρεις τύπους καναλιών. Ενδέχεται όμως να υπάρχουν διαφορετικοί συνδυασμοί εσωτερικών στοιχείων για κάθε κανάλι, όπως περιγράφηκε στην παράγραφο 4.3.5.3.3.1.3.2.

Στόχος της παρούσας παραγράφου είναι να δώσει ένα παράδειγμα πρώτα ενός συνολικού διαγράμματος εγκατάστασης και στη συνέχεια να αναλύσει κάποιο απο τα στοιχεία του, σύμφωνα με τις αρχές προδιαγραφής της όψης μηχανικού. Για το λόγο αυτό, και για να είναι πιο κατανοητό το παράδειγμα, συνεχίζεται το αντίστοιχο με την υπηρεσία έκδοσης ενός πιστοποιητικού γέννησης που ακολουθείται σε όλα τα προηγούμενα στάδια. Στην όψη μηχανικού που παρατίθεται στο Σχήμα 4-74 παρουσιάζεται μια απλοποιημένη συνολική πιθανή αρχιτεκτονική που θα μπορούσε να υποστηρίξει την εν λόγω υπηρεσία, σύμφωνα με το σύνολο των υπηρεσιών που προ-απαιτούνται όπως παρουσιάστηκε στο παράδειγμα του σταδίου 3 στην παράγραφο 4.3.3.3.6.



Σχήμα 4-74: Παράδειγμα συνολικού διαγράμματος εγκατάστασης όψης μηχανικού για μια ΑΔΑΑΥ που φιλοξενεί την υπηρεσία έκδοσης πιστοποιητικών γέννησης

Το σχήμα αποτελεί ένα συνολικό διάγραμμα εγκατάστασης που επιδεικνύει την οργάνωση της ΑΔΑΑΥ για τον δήμο σε πέντε επίπεδα με έναν κόμβο σε κάθε επίπεδο και έναν κόμβο εκτός της αρχιτεκτονικής που εκπροσωπεί την ΥΔΚ, σύμφωνα με τις αρχές της μεθόδου της παραγράφου 4.3.5.3.3.1.3. Οι συγκεκριμένοι κόμβοι συγκεκριμένα επίπεδα και τα μηχανικά αντικείμενα που περιέχουν αναλύονται ως εξής:

1. *Κόμβος Α* στο επίπεδο πελάτη. Στον κόμβο βρίσκεται η *Εφαρμογή πελάτη (Client)* με την οποία αλληλεπιδρούν οι πολίτες και οι δημόσιοι υπάλληλοι του παραδείγματος και αποτελεί το ένα μέρος της υπηρεσίας διεπαφής χρηστών (βλ. και παραγράφους 4.3.3.3.2.1 και 4.3.4.3.3.2.2.1). Το μηχανικό αντικείμενο εφαρμογής πελάτη επικοινωνεί με το αντικείμενο διαχειριστή ιστοσελίδων στον κόμβο Β μέσω ενός καναλιού λειτουργιών. Στο επίπεδο αυτό επίσης περιλαμβάνεται ένα μηχανικό αντικείμενο που υλοποιεί τους μηχανισμούς ψηφιακών και προηγμένων ηλεκτρονικών υπογραφών *(Signature component)* (βλ. και παραγράφους 4.3.3.3.3.1,4.3.3.3.3.2 και 4.3.4.3.3.2.3.3, 4.3.4.3.3.2.3.4) με χρήση ενός *Αναγνώστη κάρτας (Smart card reader)* και της *Έξυπνης κάρτας (Smart card)* του κάθε χρήστη.
2. *Κόμβος Β* στο επίπεδο αλληλεπίδρασης. Ο κόμβος περιέχει τον *Εξυπηρετητή εφαρμογών Α (App Server A)* και τον *Διαχειριστή ιστοσελίδων (Web manager)* που δέχεται τις αιτήσεις πρόσβασης απο τις εφαρμογές πελάτες, τις αποδομεί κατάλληλα και τις αποστέλλει στο το πρώτο επιχειρησιακό επίπεδο στον κόμβο C, προκειμένου να λάβει τις απαραίτητες απαντήσεις. Τις απαντήσεις τις δομεί σε ιστοσελίδες ή άλλου τύπου έγγραφα, όπως για παράδειγμα XML, και τις επιστρέφει στους πελάτες. Το αντικείμενο διαχείρισης ιστοσελίδων αποτελεί το δεύτερο μέρος της υπηρεσίας διεπαφής χρηστών (βλ. και παραγράφους 4.3.3.3.2.1 και 4.3.4.3.3.2.2.1) και επικοινωνεί απο την μια πλευρά με το αντικείμενο εφαρμογής πελάτη στον κόμβο Α

και με τα αντικείμενα διαχειριστή πρόσβασης και εργασιών χρηστών στον κόμβο C μέσω καναλιών λειτουργιών.

3. *Κόμβος C* στο πρώτο επιχειρησιακό επίπεδο, ο οποίος περιέχει τον *Εξυπηρετητή εφαρμογών B (App Server B)*. Ο κόμβος αυτός αποτελεί την καρδιά της συγκεκριμένης αρχιτεκτονικής όπου φιλοξενείται το μεγαλύτερο μέρος των υπηρεσιών διαχείρισης καθώς και οι βασικές υπηρεσίες, οι υπηρεσίες υποστήριξης υπαρχουσών υποδομών οι υπηρεσίες ασφάλειας. Πιο συγκεκριμένα, τα μηχανικά αντικείμενα που περιλαμβάνονται και υλοποιούν τις παραπάνω υπηρεσίες είναι τα ακόλουθα (σε συμφωνία με τα βασικά στοιχεία της υπολογιστικής όψης που παρουσιάστηκαν στην παράγραφο 4.3.4.3.3.2 και το παράδειγμα της παραγράφου 4.3.3.3.6):
   - Υπηρεσίες και μηχανισμοί διαχείρισης και συντονισμού:
     - Ο *Διαχειριστής πρόσβασης (Access Manager)* υλοποιεί την υπηρεσία πρόσβασης (βλ. και παραγράφους 4.3.3.3.1.1 και 4.3.4.3.3.2.1.1). Δέχεται τις αιτήσεις μέσω του επιπέδου αλληλεπίδρασης, επικοινωνεί με την υπηρεσία ελέγχου πρόσβασης για τις κατάλληλες εξουσιοδοτήσεις και με τον πυρήνα για τις εκκινήσεις διεργασιών που απαιτούνται σύμφωνα με τις αιτήσεις. Επικοινωνεί με τον διαχειριστή ιστοσελίδων στον κόμβο B μέσω ενός καναλιού λειτουργιών,
     - Ο *Πυρήνας (Kernel)* υλοποιεί το βασικό μέρος της υπηρεσίας διαχείρισης διεργασιών με όλες τις λειτουργίες που αναφέρθηκαν στις παραγράφους 4.3.3.3.1.2 και 4.3.4.3.3.2.1.2, εκτός απο τις σχετικές με τον σχεδιασμό, τον συντονισμό, την εγκατάσταση και απεγκατάσταση των επιχειρησιακών υπηρεσιών, οι οποίες συντελούνται στο δεύτερο επιχειρησιακό επίπεδο.
     - Ο *Διαχειριστής εργασιών χρηστών (User task Manager)* υλοποιεί την υπηρεσία διαχείρισης χρηστών με όλες τις λειτουργίες που αναφέρθηκαν στις παραγράφους 4.3.3.3.1.3 και 4.3.4.3.3.2.1.3. Επικοινωνεί με τον διαχειριστή ιστοσελίδων στον κόμβο B μέσω ενός καναλιού λειτουργιών.
   - Βασικές υπηρεσίες και μηχανισμοί
     - Ο *Διαχειριστής δημοσίευσης και ανάκτησης (Publishing & retrieval manager)* υλοποιεί μια υπηρεσία δημοσίευσης και αναζήτησης σε καταλόγους υπηρεσιών ιστού, με όλες τις λειτουργίες που αναφέρθηκαν στις παραγράφους 4.3.3.3.2.4 και 4.3.4.3.3.2.2.4. Επικοινωνεί με έναν κατάλογο υπηρεσιών ιστού UDDI μέσω ενός καναλιού λειτουργιών. Όσο αφορά στη συγκεκριμένη επιχειρησιακή υπηρεσία του παραδείγματος (έκδοση πιστοποιητικών γέννησης), ο διαχειριστής δημοσίευσης βοηθά στο να την βρουν πολίτες που ενδιαφέρονται για υπηρεσίες που προσφέρει ο δήμος τους (καθώς και τις μετέπειτα ενημερώσεις της υπηρεσίας στον κατάλογο υπηρεσιών ιστού).
     - Ο *Διαχειριστής αποθετηρίων (Repository Manager)* υλοποιεί μια υπηρεσία διαχείρισης αποθετηρίων σύμφωνα με τις περιγραφές των παραγράφων 4.3.3.3.2.5 και 4.3.4.3.3.2.2.5. Πιο συγκεκριμένα ο διαχειριστής επιτρέπει την πρόσβαση και αναζήτηση σε βάσεις δεδομένων που ενδεχομένως απαιτούν οι υπηρεσίες τις αρχιτεκτονικής (π.χ. για την αποθήκευση των εκκρεμών αιτήσεων ή πιστοποιητικών γέννησης) εκτός απο την ήδη

υπάρχουσα βάση του δήμου, η οποία είναι προσβάσιμη μέσω της υπηρεσίας υποστήριξης υπαρχουσών υποδομών. Ο διαχειριστής ελέγχεται απο μια αντίστοιχη επιχειρησιακή υπο-διεργασία στον κόμβο D μέσω ενός καναλιού λειτουργιών.

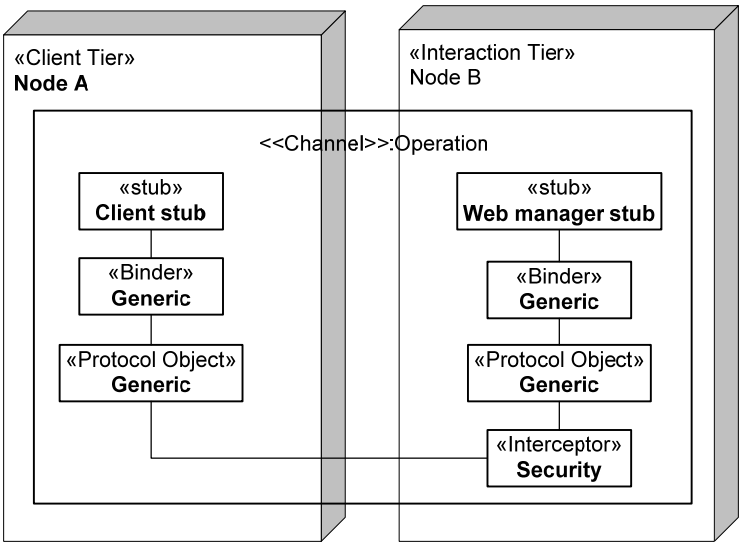
- Ο *Διαχειριστής ειδοποιήσεων (Notification manager)* υλοποιεί μια υπηρεσία ειδοποιήσεων σύμφωνα με τις περιγραφές των παραγράφων 4.3.3.3.2.6 και 4.3.4.3.3.2.2.6. Στο συγκεκριμένο παράδειγμα επιχειρησιακής υπηρεσίας, ο διαχειριστής ειδοποιήσεων χρειάζεται μόνο να μπορεί να αποστείλει αυτοματοποιημένα μηνύματα ηλεκτρονικού ταχυδρομείου σε συγκεκριμένες φάσεις της όλης διαδικασίας (για κάποιο λάθος της αίτησης ή ότι το έγγραφο είναι έτοιμο προς παραλαβή). Ο διαχειριστής ελέγχεται απο μια αντίστοιχη επιχειρησιακή υπο-διεργασία στον κόμβο D μέσω ενός καναλιού λειτουργιών.
- Ο *Διαχειριστής εκτυπώσεων (Printing Manager)* υλοποιεί μια υπηρεσία εκτυπώσεων με όλες τις λειτουργίες που αναφέρθηκαν στις παραγράφους 4.3.3.3.2.7 και 4.3.4.3.3.2.2.7. Ο διαχειριστής εκτυπώνει στον κεντρικό εκτυπωτή του αντίστοιχου τμήματος του δήμου τα πιστοποιητικά που πρέπει να αποσταλούν ταχυδρομικώς, εάν το έχει ζητήσει στην αντίστοιχη αίτησή του κάποιος πολίτης. Ο διαχειριστής ελέγχεται απο μια αντίστοιχη επιχειρησιακή υπο-διεργασία στον κόμβο D μέσω ενός καναλιού λειτουργιών.

- Υπηρεσίες ασφάλειας
  - Ο *Ελεγκτής πρόσβασης (Access controller)* υλοποιεί την υπηρεσία ελέγχου πρόσβασης με την λειτουργικότητα που περιγράφεται στις παραγράφους 4.3.3.3.3.5 και 4.3.4.3.3.2.3.2. Ο ελεγκτής κάνει ελέγχους σύμφωνα με τους κανόνες προκαθορισμένων πολιτικών πρόσβασης και τα διαπιστευτήρια που του δίνονται μέσω του διαχειριστή πρόσβασης (για πολίτες και δημοσίους υπαλλήλους) και τα οποία ελέγχει μέσω του διαχειριστή ταυτοτήτων.
  - Ο *Διαχειριστής ταυτοτήτων (Identity manager)* υλοποιεί μια υπηρεσία διαχείρισης ταυτότητας με τις λειτουργίες που περιγράφονται στις παραγράφους 4.3.3.3.3.4 και 4.3.4.3.3.2.3.1, προκειμένου να ελέγχει οποιαδήποτε αίτηση για έλεγχο ταυτότητας λαμβάνει απο τον ελεγκτή πρόσβασης. Προκειμένου να διαχειριστεί ταυτότητες, το μηχανικό αυτό αντικείμενο αντλεί πληροφορίες απο δύο πηγές: απο εξωτερικές Αρχές που δημιουργούν και επικυρώνουν διαπιστευτήρια (σύμφωνα με μια αρχιτεκτονική SAML) μέσω ενός καναλιού λειτουργιών και απο την εσωτερική υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών.
  - Ο *Διαχειριστής κλειδιών και πιστοποιητικών (Keys & Certificates Manager)* υλοποιεί μια υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών με την λειτουργικότητα που περιγράφεται στις παραγράφους 4.3.3.3.3.7 και 4.3.4.3.3.2.3.7. Όπως φαίνεται στο Σχήμα 4-74, οι μέθοδοι που υλοποιεί το αντικείμενο αυτό (έλεγχος κατάστασης πιστοποιητικών και λήψη χρονοσφραγίδων) συντελούνται σύμφωνα με τα δεδομένα που ανταλλάζει με μια εξωτερική ΥΔΚ με την οποία επικοινωνεί μέσω δύο καναλιών λειτουργιών.

- Μια υπηρεσία υποστήριξης υπαρχουσών υποδομών υλοποιείται απο ένα μηχανικό αντικείμενο που δρα ως *Ενδιάμεσο επίπεδο προσαρμογής (Adaptation layer)*. Το αντικείμενο αυτό αποτελεί το κομμάτι της υπηρεσίας απο την πλευρά της αρχιτεκτονικής και επικοινωνεί με το αντίστοιχο αντικείμενο που αποτελεί το κομμάτι της υπηρεσίας που περιλαμβάνεται στον κόμβο Ε, σύμφωνα με την λογική των παραγράφων 4.3.3.3.5 και 4.3.4.3.3.2.5. Τα δύο μέρη της υπηρεσίας επικοινωνούν μέσω ενός καναλιού λειτουργιών.

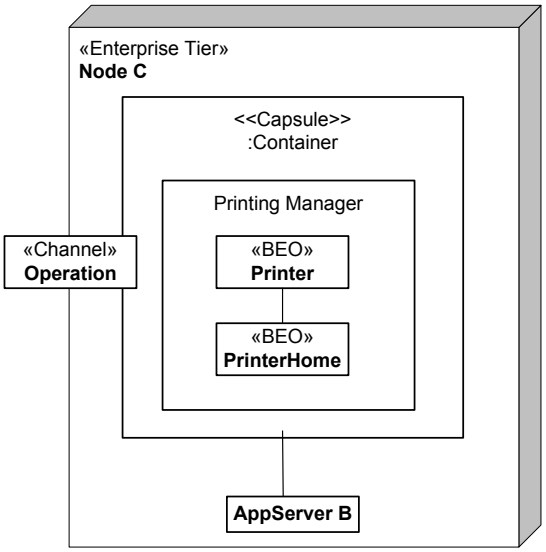
4. *Κόμβος D* στο δεύτερο επιχειρησιακό επίπεδο, ο οποίος περιέχει τον *Εξυπηρετητή εφαρμογών C (App Server C)*. Αυτός ο κόμβος περιλαμβάνει το αντικείμενο *Διαχειριστή επιχειρησιακών διεργασιών (Enterprise Task Manager)*, ο οποίος επιτελεί τις διαχειριστικές εργασίες τις σχετικές με τον σχεδιασμό, συντονισμό, εγκατάσταση και απεγκατάσταση των επιχειρησιακών υπηρεσιών και υπο-υπηρεσιών. Οι υπο-υπηρεσίες αποτελούν υπηρεσίες ιστού που επικοινωνούν μέσω καναλιών λειτουργιών με τις πραγματικές αντίστοιχες βασικές υπηρεσίες στο πρώτο επιχειρησιακό επίπεδο και τις διαχειρίζονται (ως ένα είδος wrappers). Αυτό σημαίνει ότι ο σχεδιαστής έχει την ευχέρεια καθορίζοντας την λειτουργικότητα της *Υπηρεσίας έκδοσης πιστοποιητικών γέννησης (Birth certificate service)*, να συνθέσει κάποιες απο τις φάσεις της χρησιμοποιώντας το κατάλληλο σύνολο υπο-υπηρεσιών (στην προκειμένη περίπτωση *υπο-υπηρεσία εκτύπωσης, υπο-υπηρεσία ειδοποιήσεων, υπο-υπηρεσία υπάρχουσας υποδομής* και *υπο-υπηρεσία διαχείρισης αποθετηρίου*). Τόσο ο Διαχειριστής επιχειρησιακών διεργασιών όσο και η κάθε επιχειρησιακή υπηρεσία που εγκαθίσταται στην συγκεκριμένη αρχιτεκτονική πρέπει να επικοινωνεί μέσω καναλιών λειτουργιών και με τον πυρήνα στον κόμβο C προκειμένου να υποστηρίζονται οι βασικές λειτουργίες εγκαθιδρύσεως συνόδων και η χρησιμοποίηση των μηχανισμών ασφάλειας, ο οποίες είναι διαθέσιμές μόνο μέσω του πυρήνα.
5. *Κόμβος E* στο επίπεδο ολοκλήρωσης. Στον κόμβο Ε περιλαμβάνεται το κομμάτι της υπηρεσίας υποστήριξης υπαρχουσών υποδομών που ολοκληρώνει το υπάρχον σύστημα του δήμου (*Βάση δεδομένων (Legacy DB)* με στοιχεία των πολιτών). Η υπηρεσία υλοποιείται απο ένα αντικείμενο *Ενδιάμεσου επιπέδου προσαρμογής (Adaptation layer)*, το οποίο γνωρίζει πως να επικοινωνεί απο τη μια πλευρά με το αντίστοιχο αντικείμενο στον κόμβο C μέσω ενός καναλιού λειτουργιών, και απο την άλλη με το υπάρχον σύστημα μέσω ενός άλλου καναλιού λειτουργιών.

Όπως φαίνεται απο την παραπάνω ανάλυση, στο συγκεκριμένο παράδειγμα χρησιμοποιούνται μόνο κανάλια λειτουργιών. Ένα παράδειγμα διαγράμματος λεπτομέρειας για ένα κανάλι αποτελεί το ακόλουθο για το κανάλι μεταξύ της εφαρμογής πελάτη και του διαχειριστή ιστοσελίδων:



Σχήμα 4-75: Παράδειγμα διαγράμματος λεπτομέρειας του καναλιού ανάμεσα στην εφαρμογή πελάτη και τον διαχειριστή ιστοσελίδων

Το σχήμα επιδεικνύει την γενική μορφή του καναλιού στην όψη μηχανικού. Τα σημεία στα οποία πρέπει να δοθεί έμφαση είναι δύο: πρώτον ότι τα στελέχη για στο υψηλότερο επίπεδο επικοινωνίας υλοποιούνται απο τα μηχανικά αντικείμενα που επικοινωνούν και δεύτερον ότι το κανάλι απαιτεί την ύπαρξη ενός αναχαιτιστή για την παροχή σε χαμηλό επίπεδο κατάλληλων μηχανισμών ασφάλειας (και άρα την κατάλληλη μετάφραση των δεδομένων ανάμεσα στα δύο αντικείμενα πρωτοκόλλου ώστε το ένα να αποδέχεται και να κατανοεί τα ασφαλή δεδομένα που του στέλνει το άλλο).
Το παράδειγμα ολοκληρώνεται με ένα διάγραμμα λεπτομέρειας στην όψη μηχανικού για το αντικείμενο Διαχειριστή εκτυπώσεων σε πλήρη αντιστοίχηση με το παράδειγμα που παρατέθηκε στην περιγραφή της υπολογιστικής όψης στην παράγραφο 4.3.4.3.3.3. Το συγκεκριμένο διάγραμμα λεπτομέρειας φαίνεται στο Σχήμα 4-76:



Σχήμα 4-76: Παράδειγμα διαγράμματος λεπτομέρειας για το μηχανικό αντικείμενο Διαχειριστής εκτυπώσεων στην όψη μηχανικού

Σε αντιστοιχία με τις προδιαγραφές της υπολογιστικής όψης και τις σχεδιαστικές αρχές της παραγράφου 4.3.5.3.3.1.3.3, παρατηρούμε ότι:

- Το αντικείμενο βρίσκεται στον κόμβο C.
- Χρησιμοποιεί ένα κανάλι λειτουργιών προκειμένου να επικοινωνήσει με άλλα μηχανικά αντικείμενα εκτός του κόμβου C.
- Εμπεριέχει δύο βασικά μηχανικά αντικείμενα (με το πρότυπο BEO) τα οποία αντιπροσωπεύουν τις δύο διεπαφές του: το αντικείμενο Printer και το PrinterHome.
- Το αντικείμενο λειτουργεί στον υποδοχέα του εξυπηρετητή εφαρμογών B.

Προκειμένου να ολοκληρώσει τις προδιαγραφές του παραδείγματος, ο σχεδιαστής θα πρέπει να αναλύσει με αντίστοιχο τρόπο όλα τα μηχανικά αντικείμενα του σχήματος Σχήμα 4-74 και να δώσει τον ορισμό διαγραμμάτων λεπτομέρειας πιθανών καναλιών που δεν υπακούουν στην γενική όψη του σχήματος Σχήμα 4-75.

4.3.5.4 Προδιαγραφή Τεχνολογικής Όψης

4.3.5.4.1 Εισαγωγή

Η όψη αυτή περιγράφει τις ακριβείς τεχνολογίες που επιλέγονται για την υλοποίηση του συστήματος. Είναι στενά δεμένη με την όψη μηχανικού διότι αντιστοιχεί κάθε στοιχείο της σε μια τεχνολογία. Περιέχει την διαμόρφωση των μηχανικών αντικειμένων αναπαριστώντας τόσο τα στοιχεία υλικού όσο και λογισμικού.

4.3.5.4.2 Έννοιες

Οι έννοιες που ορίζονται στο πρότυπο RM-ODP και χρησιμοποιούνται στη μεθοδολογία προδιαγραφής της τεχνολογικής όψης είναι αυτές της παραγράφου 7.3.8.2.2.1.5.

4.3.5.4.3 Σημειογραφία

Στην παράγραφο αυτή καθορίζεται τι είδους διαγράμματα χρησιμοποιεί η μεθοδολογία για την αναπαράσταση των αντικειμένων της τεχνολογικής όψης, και μπορούν να χρησιμοποιηθούν για την επέκταση της όψης. Όλα τα διαγράμματα βασίζονται στην UML.

Ένα είδος διαγραμμάτων κυριαρχεί και στην τεχνολογική όψη και αυτό είναι και πάλι τα διαγράμματα εγκατάστασης. Αυτό οφείλεται στο γεγονός ότι η τεχνολογική όψη έχει μια «ένα-προς-ένα» αντιστοίχιση με την όψη μηχανικού. Κάθε κόμβος, μηχανικό αντικείμενο και κανάλι της όψης μηχανικού εμφανίζεται και στην τεχνολογική όψη, χαρακτηρισμένο όμως απο μια συγκεκριμένη τεχνολογία ή εναλλακτικές τεχνολογίες αν αυτό είναι επιθυμητό.

Οι παράγραφοι που ακολουθούν περιγράφουν πως χρησιμοποιείται η παραπάνω σημειογραφία ως μέρος της μεθοδολογίας.

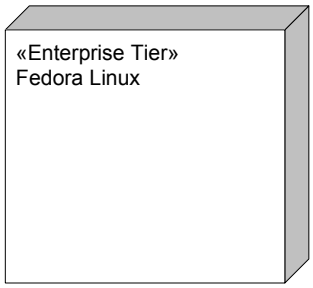
4.3.5.4.4 Μεθοδολογία προδιαγραφής

4.3.5.4.4.1.1 Διαγράμματα εγκατάστασης

Στην παρούσα παράγραφο παρουσιάζεται ο τρόπος με τον οποίο χρησιμοποιούνται τα διαγράμματα εγκατάστασης της UML προκειμένου να αναπαρασταθούν οι τεχνολογικές επιλογές για κάθε αντικείμενο της όψης μηχανικού.
Εφόσον η τεχνολογική όψη είναι επί της ουσίας επέκταση της όψης μηχανικού, η μέθοδος χρησιμοποιεί και πάλι τα υψηλού επιπέδου συνολικά διαγράμματα εγκατάστασης και τα διαγράμματα λεπτομέρειας που έχουν ήδη οριστεί και αλλάζει το είδος της πληροφορίας που αυτά παρέχουν προκειμένου να γίνουν εμφανείς οι τεχνολογικές επιλογές.

4.3.5.4.4.1.1.1 Κόμβοι

Οι κόμβοι που έχουν οριστεί στην όψη μηχανικού και αντιστοιχούν σε υπολογιστές πλέον χαρακτηρίζονται απο ένα λειτουργικό σύστημα. Ο αριθμός του κάθε κόμβου αντικαθίσταται απο το είδος του λειτουργικού συστήματος, όπως στο παράδειγμα του σχήματος που ακολουθεί.



Σχήμα 4-77: Αναπαράσταση ενός κόμβου στην τεχνολογική όψη

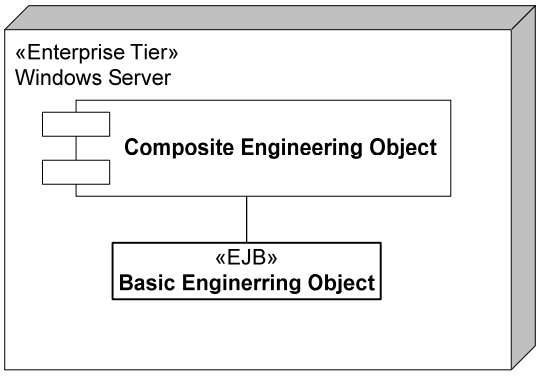
Το πρότυπο UML που χαρακτηρίζει σε ποιό επίπεδο της αρχιτεκτονικής βρίσκεται ο κόμβος παραμένει αναλλοίωτο (π.χ. στο συγκεκριμένο παράδειγμα ο κόμβος βρίσκεται στο επιχειρησιακό επίπεδο οπότε έχει το πρότυπο «Enterprise Tier»).

4.3.5.4.4.1.1.2 Κανάλια

Στην τεχνολογική όψη κάθε κανάλι σημειώνεται όπως και στην όψη μηχανικού με τη διαφορά ότι αντικαθίσταται πλέον ο τύπος του καναλιού (λειτουργίας, σήματος ή ροής) με την πραγματική τεχνολογία που το υποστηρίζει. Το ίδιο συμβαίνει και για τα διαγράμματα λεπτομέρειας για κάθε κανάλι, όπου αντικαθίστανται οι «γενικευμένες» αναπαραστάσεις των εσωτερικών στοιχείων με τα τεχνολογικά ανάλογά τους. Παραδείγματα αναπαράστασης των καναλιών στην τεχνολογική όψη αποτελούν τα βασικά στοιχεία της όψης που παρατίθενται στην παράγραφο 4.3.5.4.5.1.

4.3.5.4.4.1.1.3 Μηχανικά αντικείμενα

Τα βασικά μηχανικά αντικείμενα στην τεχνολογική όψη χαρακτηρίζονται απο ένα πρότυπο που παραπέμπει σε μια συγκεκριμένη τεχνολογία, όπως για παράδειγμα αν είναι EJB ή Υπηρεσία Ιστού, όπως φαίνεται στο σχήμα που ακολουθεί.

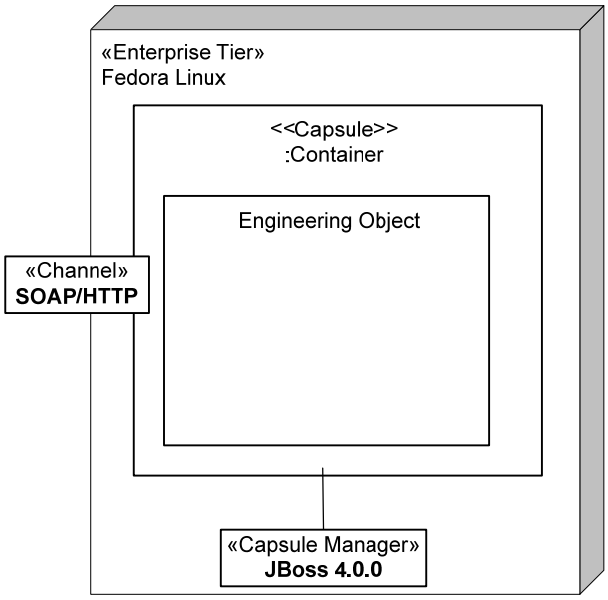


Σχήμα 4-78: Αναπαράσταση μηχανικών αντικειμένων σε συνολικό διάγραμμα εγκατάστασης της τεχνολογικής όψης

Τα σύνθετα μηχανικά αντικείμενα παραμένουν ως έχουν στο συνολικό διάγραμμα εγκατάστασης και περισσότερες λεπτομέρειες τεχνολογιών επιλογών που τα αφορούν παρατίθενται στα διαγράμματα λεπτομέρειας.

Επιπρόσθετα, κάθε μηχανικό αντικείμενο το οποίο μέχρι τώρα έχει ένα όνομα που περιγράφει την γενική λειτουργία του, όπως αυτή προκύπτει απο την αντιστοίχηση των υπολογιστικών αντικειμένων, στην τεχνολογική όψη ενδέχεται να λάβει μια πιο συγκεκριμένη ονομασία που σχετίζεται με κάποια συγκεκριμένη τεχνολογία που χρησιμοποιείται για το αντικείμενο ή βιβλιοθήκη ή προϊόν. Για παράδειγμα μια «δομική μονάδα φυλλομετρητή» (βλ. βασικά στοιχεία υπολογιστικής όψης στην παράγραφο 4.3.4.3.3.2.2.1) μπορεί να είναι ένα Java Applet ή ένα στοιχείο ActiveX, και αυτή η ονομασία θα χρησιμοποιηθεί στην τεχνολογική όψη. Η συσχετίσεις ανάμεσα στα στοιχεία στην τεχνολογική όψη σχεδιάζονται με τον ίδιο τρόπο όπως στην όψη μηχανικού.

Η περαιτέρω ανάλυση των αντικειμένων στην τεχνολογική όψη γίνεται βάσει διαγραμμάτων αντίστοιχων των διαγραμμάτων λεπτομέρειας της όψης μηχανικού. Στα διαγράμματα αυτά πλέον τοποθετείται πληροφορία σχετικά με την συγκεκριμένη υλοποίηση όπως στο παράδειγμα του σχήματος:



Σχήμα 4-79: Διάγραμμα λεπτομέρειας μηχανικού αντικειμένου στην τεχνολογική όψη

Στο σχήμα αυτό και στην ανάλυση του που το συνοδεύει ως μέρος του σχεδιασμού, αναπαρίσταται η εξής πληροφορία για κάθε μηχανικό αντικείμενο:

- Το λειτουργικό σύστημα που υποστηρίζει ο κόμβος στον οποίο βρίσκεται.
- Η τεχνολογία που υποστηρίζουν τα κανάλια με τα οποία επικοινωνεί με άλλα μηχανικά αντικείμενα εκτός του κόμβου.
- Τεχνολογικά χαρακτηριστικά μηχανικών αντικειμένων απο τα οποία αποτελείται το συγκεκριμένο αντικείμενο (κυρίως διεπαφών).
- Το είδος του εξυπηρετητή εφαρμογών στο οποίο ενδέχεται να βρίσκεται το αντικείμενο (συγκεκριμένο προϊόν και έκδοσή του).
- Βιβλιοθήκες, άλλα προϊόντα ή τεχνολογίες που χρησιμοποιεί το αντικείμενο και πρότυπα υλοποίησης με τα οποία συμμορφώνεται.

Η παραπάνω πληροφορία καθορίζει επακριβώς τι θα χρησιμοποιηθεί απο τους προγραμματιστές που θα κληθούν να υλοποιήσουν τα στοιχεία της αρχιτεκτονικής και να συνθέσουν τις υπηρεσίες της στο επόμενο στάδιο της μεθόδου.

4.3.5.4.5 Βασικά στοιχεία όψης

Η μέθοδος ορίζει ένα σύνολο βασικών στοιχείων για διάφορα είδη καναλιών που είναι ευρέως διαδεδομένα στην υλοποίηση αρχιτεκτονικών υπηρεσιών και στην ασφαλή επικοινωνία μεταξύ οντοτήτων. Δεν ορίζονται βασικά στοιχεία για τα μηχανικά αντικείμενα για τους ίδιου λόγους που αναφέρθηκαν στην αντίστοιχη παράγραφο 4.3.5.3.3.2 της όψης μηχανικού.

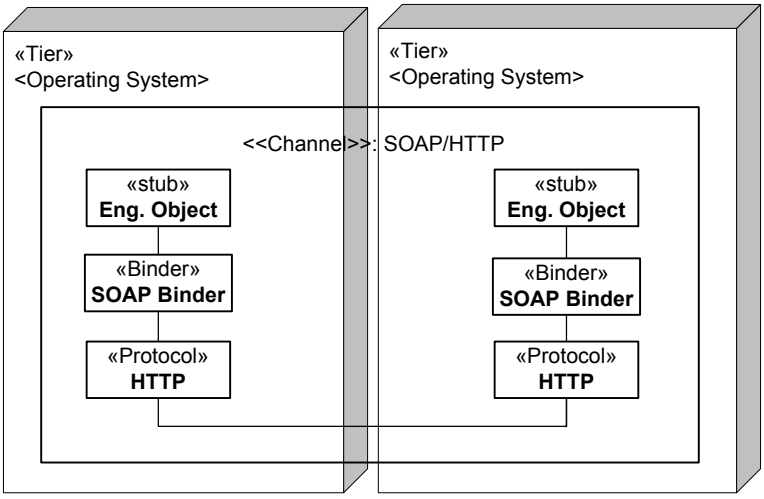
4.3.5.4.5.1 Κανάλια

4.3.5.4.5.1.1 SOAP/HTTP

Ο πλέον συνηθισμένος τύπος καναλιού στις αρχιτεκτονικές υπηρεσιών είναι αυτός που βασίζεται στο πρωτόκολλο SOAP/HTTP [Mitra03], οποίος σε συνολικό διάγραμμα εγκατάστασης συμβολίζεται με το ακόλουθο σχήμα:

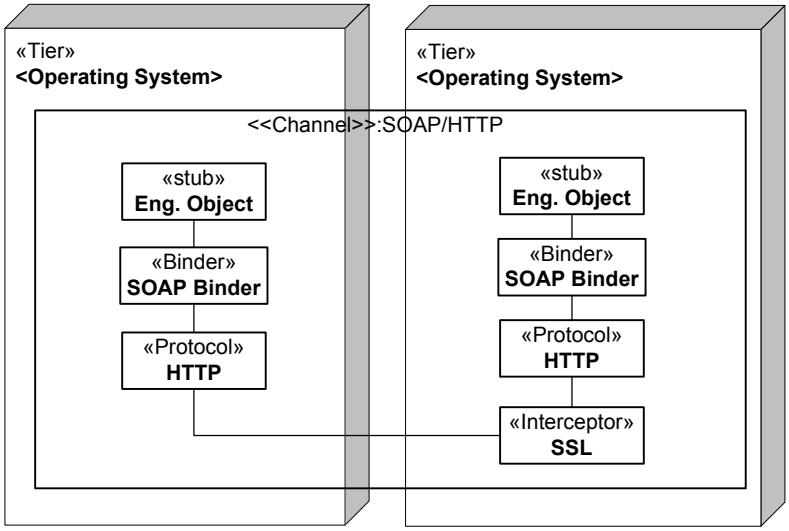
Σχήμα 4-80: Βασικό στοιχείο καναλιού SOAP/HTTP για συνολικό διάγραμμα εγκατάστασης

Στην περίπτωση ενός τέτοιου καναλιού, το κομμάτι του κώδικα που είναι υπεύθυνο για την διάρθρωση και αποδιάρθρωση δεδομένων στο σχήμα του SOAP είναι το στέλεχος στο κανάλι επικοινωνίας ανάμεσα σε δύο μηχανικά αντικείμενα. Ο δεσμευτής είναι το κομμάτι του κώδικα που δένει το SOAP με το πρωτόκολλο HTTP προκειμένου να επιτύχει την επικοινωνία. Τέλος, το αντικείμενο πρωτοκόλλου είναι το στοιχείο που υλοποιεί το ίδιο το πρωτόκολλο HTTP. Τα παραπάνω φαίνεται στο Σχήμα 4-81:



Σχήμα 4-81: Βασικό στοιχείο καναλιού SOAP/HTTP για διάγραμμα λεπτομέρειας

Τα μηχανικά αντικείμενα που επικοινωνούν υλοποιούν τα κατάλληλα στελέχη για την δημιουργία μηνυμάτων SOAP. Στο βασικό στοιχείο αποτυπώνονται επίσης οι κόμβοι στους οποίους βρίσκονται τα αντικείμενα που επικοινωνούν.
Στη περίπτωση που ανάμεσα στα αντικείμενα απαιτείται η εδραίωση και κάποιου ειδικού τύπου «μετάφρασης», όπως για παράδειγμα όταν χρησιμοποιείται κρυπτογράφηση, τότε προστίθεται και ένα κατάλληλος αναχαίτισης στο βασικό στοιχείο και αυτό παίρνει την μορφή:



Σχήμα 4-82: Βασικό στοιχείο καναλιού SOAP/HTTP με παράδειγμα αναχαιτιστή

Η επικοινωνία σε ένα κανάλι RMI/IIOP μπορεί να είναι σύγχρονη ή ασύγχρονη.

4.3.5.4.5.1.2 Κλήση απομακρυσμένης μεθόδου - Remote Method Invocation (RMI)

Οι εφαρμογές που βασίζονται στο RMI [RMI] υλοποιούν τις αλληλεπιδράσεις μεταξύ τους βασιζόμενες στο παράδειγμα εφαρμογών «πελάτη-εξυπηρετητή». Μια εφαρμογή εξυπηρετητής δημιουργεί απομακρυσμένα αντικείμενα, καθιστά προσβάσιμες τις αναφορές στα αντικείμενα αυτά και περιμένει εφαρμογές πελάτες να καλέσουν μεθόδους πάνω στα αντικείμενα. Το RMI προσφέρει έναν μηχανισμό με τον οποίο οι εφαρμογές εξυπηρετητή και πελάτη μπορούν να επικοινωνήσουν και να μεταφέρουν πληροφορία εκατέρωθεν.

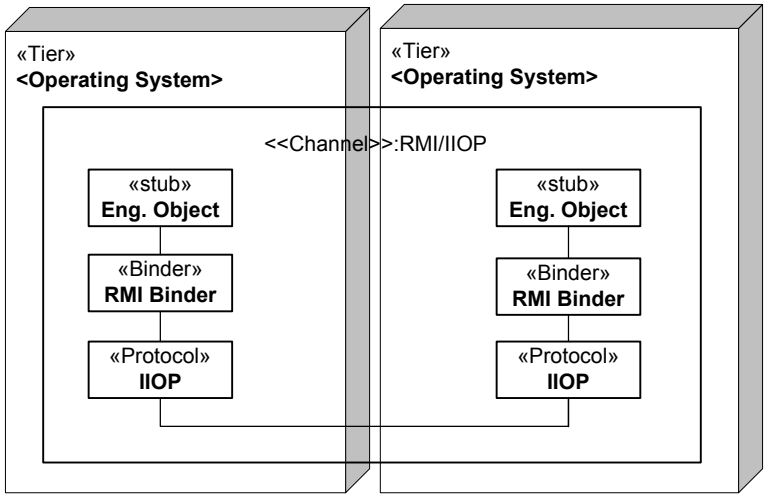
Ένα *Απομακρυσμένο Αντικείμενο (Remote Object)* αποτελεί ένα αντικείμενο Java του οποίου οι μέθοδοι μπορούν να κληθούν απο (και σε) μια *Εικονική Μηχανή Java (Java Virtual Machine),* που ενδεχομένως να βρίσκεται στον ίδιο ή σε άλλον κόμβο σε σχέση με το αντικείμενο. Ένα Απομακρυσμένο Αντικείμενο περιγράφεται απο *Απομακρυσμένες Διεπαφές (Remote Interfaces)* οι οποίες καθορίζουν τις μεθόδους του Απομακρυσμένου Αντικειμένου. Η πράξη κλήσης μιας μεθόδου ενός Απομακρυσμένου Αντικειμένου απο ένα άλλο αντικείμενο της Java ονομάζεται *Κλήση Απομακρυσμένης Μεθόδου (Remote Method Invocation)*.

Ο μηχανισμός RMI χρησιμοποιεί *στελέχη (stubs)* και *σκελετούς (skeletons)* για την σύνδεση και αποσύνδεση της πληροφορίας που ανταλλάσσεται μεταξύ των αντικειμένων. Ένα στέλεχος (στην ορολογία του Java RMI) δρα ως ένας τοπικός αντιπρόσωπος του Απομακρυσμένου Αντικειμένου. Ο πελάτης καλεί την μέθοδο στο τοπικό στέλεχος, το οποίο είναι υπεύθυνο για την εκτέλεση της κλήσης της μεθόδου στο Απομακρυσμένο Αντικείμενο. Ένας σκελετός στην άλλη πλευρά είναι υπεύθυνος για την αποστολή της κλήσης στην πραγματική υλοποίηση του Απομακρυσμένου Αντικειμένου. Μεταξύ άλλων, ένα στέλεχος εκκινεί την σύνδεση με την απομακρυσμένη Εικονική Μηχανή Java, διορθώνει τις παραμέτρους που τροφοδοτεί την Μηχανή και αποδιαρθρώνει την τιμή επιστροφής ή το αντικείμενο λάθους που επιστρέφεται. Ένας

σκελετός αποδιαρθρώνει τις παραμέτρους που τροφοδοτούνται στην απομακρυσμένη μέθοδο και διαρθρώνει το αποτέλεσμα του καλούντο.
Σε ένα συνολικό διάγραμμα εγκατάστασης ένα κανάλι βασισμένο στο RMI αναπαρίσταται ως εξής:

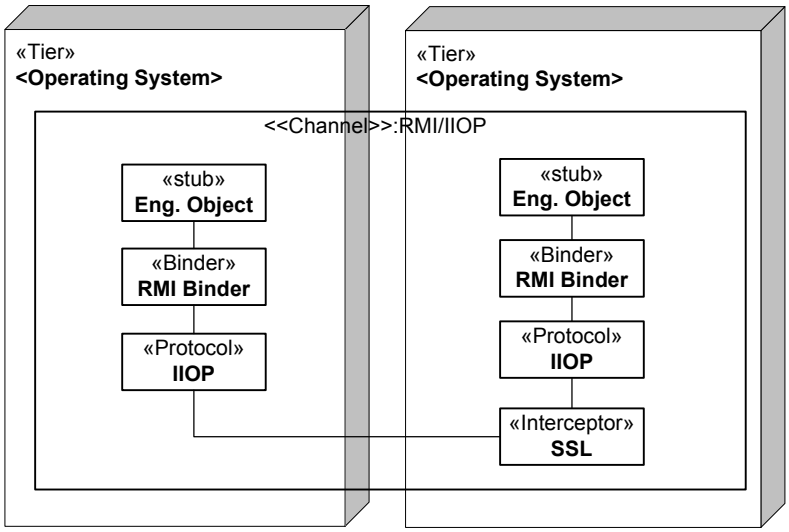
Σχήμα 4-83: Βασικό στοιχείο όψης καναλιού RMI/IIOP για συνολικό διάγραμμα εγκατάστασης

Με όρους του RM-ODP, τα στελέχη και σκελετοί του RMI επιτελούν το έργο των στελεχών καναλιών. Ο ρόλος των αντικειμένων πρωτοκόλλου επιτελείται απο το πρωτόκολλο IIOP και ο ρόλος του δεσμευτή ενός καναλιού αναλαμβάνεται απο δεσμευτές του RMI. Η αναπαράσταση του βασικού αντικειμένου ενός καναλιού βασισμένου στο RMI φαίνεται στο σχήμα που ακολουθεί:



Σχήμα 4-84: Βασικό στοιχείο καναλιού RMI/IIOP για διάγραμμα λεπτομέρειας

Όπως φαίνεται στο σχήμα, το βασικό στοιχείο καθορίζεται περαιτέρω απο τους κόμβους στους οποίους βρίσκονται τα μηχανικά αντικείμενα που επικοινωνούν. Επιπρόσθετα, τα στελέχη σε κάθε πλευρά του καναλιού υλοποιούνται ως μέρη των μηχανικών αντικειμένων.
Στη περίπτωση που ανάμεσα στα αντικείμενα απαιτείται η εδραίωση και κάποιου ειδικού τύπου «μετάφρασης», όπως για παράδειγμα όταν χρησιμοποιείται κρυπτογράφηση, τότε προστίθεται και ένα κατάλληλος αναχαίτισης στο βασικό στοιχείο και αυτό παίρνει την μορφή:



Σχήμα 4-85: Βασικό στοιχείο καναλιού RMI/IIOP με παράδειγμα αναχαιτιστή

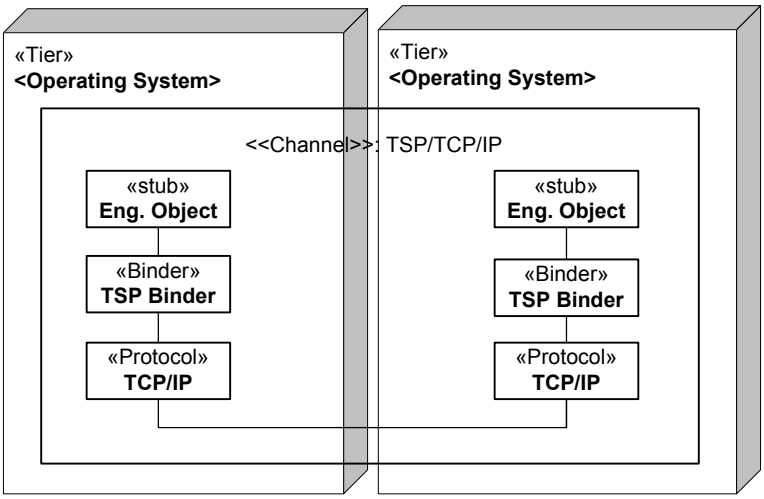
Η επικοινωνία σε ένα κανάλι RMI/IIOP μπορεί να είναι σύγχρονη ή ασύγχρονη.

4.3.5.4.5.1.3 Πρωτόκολλο χρονοσφράγισης πάνω απο TCP/IP

Στην περίπτωση επικοινωνίας με μια Αρχής Χρονοσφράγισης με στόχο την λήψη μιας χρονοσφραγίδας για ένα έγγραφο χρησιμοποιείται το πρωτόκολλο χρονοσφράγισης (time stamping protocol) το οποίο είναι προδιαγεγραμμένο στο RFC 3161 [Adams01]. Σε συνολικό διάγραμμα εγκατάστασης ένα τέτοιου τύπου κανάλι συμβολίζεται ως εξής:

Σχήμα 4-86: Βασικό στοιχείο καναλιού TSP/TCP/IP για συνολικό διάγραμμα εγκατάστασης

Το κομμάτι του κώδικα που είναι υπεύθυνο για την διόρθωση και αποδιάρθρωση των δεδομένων στην κατάλληλη δυαδική μορφή του πρωτοκόλλου χρονοσφράγισης (time-stamping protocol) είναι τα στελέχη που υλοποιούνται απο τα μηχανικά αντικείμενα που επικοινωνούν. Ο δεσμευτής είναι το κομμάτι του κώδικα που «δένει» αντικείμενα του πρωτοκόλλου χρονοσφράγισης στο υποκείμενο πρωτόκολλο TCP/IP για μεταφορά τους πάνω στο διαδίκτυο. Τέλος, το αντικείμενο πρωτοκόλλου είναι το κομμάτι του κώδικα που υλοποιεί το TCP/IP. Αυτό φαίνεται στο σχήμα που ακολουθεί:



Σχήμα 4-87: Βασικό στοιχείο καναλιού TSP/TCP/IP για διάγραμμα λεπτομέρειας

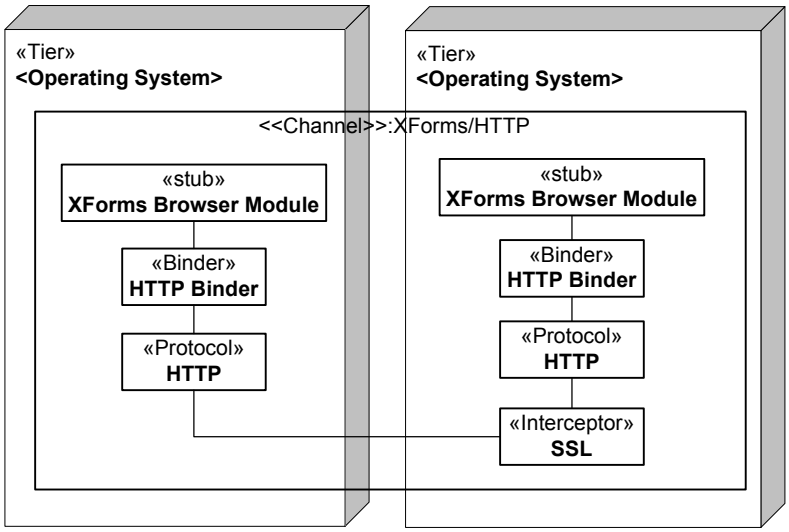
Η μονάδα που θα εμπεριέχει το μηχανικό στοιχείο απο την μια εκ των δύο πλευρών προφανώς θα φιλοξενείται απο την Αρχή Χρονοσφράγισης.
Η επικοινωνία με κανάλι αυτού του τύπου είναι πάντοτε σύγχρονη.

4.3.5.4.5.1.4 XForms πάνω απο HTTP

Το πρωτόκολλο XForms [Boyer06] λειτουργεί σε υψηλό επίπεδο εφαρμογής προκειμένου να μεταφερθούν δεδομένα XML που αναπαριστούν την δομή μιας φόρμας πάνω απο HTTP. Σε συνολικό διάγραμμα εγκατάστασης ένα τέτοιου τύπου κανάλι συμβολίζεται ως εξής:

Σχήμα 4-88: Βασικό στοιχείο καναλιού Xforms/HTTP για συνολικό διάγραμμα εγκατάστασης

Το κομμάτι του κώδικα που είναι υπεύθυνο για την διόρθωση και αποδιάρθρωση των δεδομένων σε μορφή XML που συμμορφώνεται με το πρότυπο Xforms είναι τα στελέχη που υλοποιούνται απο τα μηχανικά αντικείμενα που επικοινωνούν, και που βρίσκονται είτε σε έναν φυλλομετρητή που υλοποιεί το πρωτόκολλο XForms (αυτόνομα ή μέσω κάποιας ενδιάμεσης εφαρμογής στον φυλλομετρητή – browser plug-in) είτε σε έναν εξυπηρετητή διαδικτύου του επιπέδου αλληλεπίδρασης. Ο δεσμευτής είναι το κομμάτι του κώδικα που «δένει» αντικείμενα του πρωτοκόλλου στο υποκείμενο πρωτόκολλο HTTP για μεταφορά τους πάνω στο διαδίκτυο. Τέλος, το αντικείμενο πρωτοκόλλου είναι το κομμάτι του κώδικα που υλοποιεί το HTTP Post request. Αυτό φαίνεται στο σχήμα που ακολουθεί:



Σχήμα 4-89: Βασικό στοιχείο καναλιού XForms/HTTP για διάγραμμα λεπτομέρειας

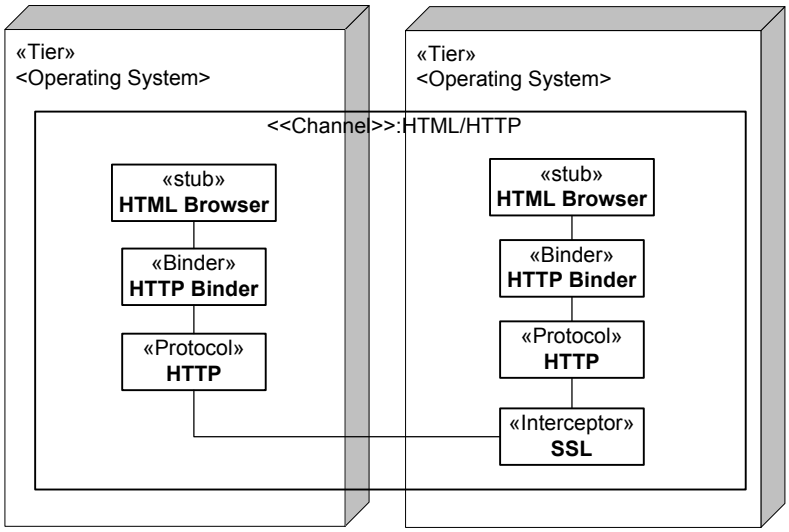
Ένας XForms φυλλομετρητής έχει την δυνατότητα να επικοινωνεί είτε με συνηθισμένους εξυπηρετητές ιστού, οι οποίοι αναλαμβάνουν να μεταφράσουν τα XML δεδομένα, είτε απ' ευθείας με Υπηρεσίες Ιστού, με τους οποίους τα δεδομένα XML θα πρέπει εκτός απο το πρότυπο XForms να συμμορφώνονται και με το πρότυπο SOAP.
Η επικοινωνία με κανάλι αυτού του τύπου μπορεί να είναι σύγχρονη ή ασύγχρονη.

4.3.5.4.5.1.5 HTML πάνω απο HTTP

Το πρωτόκολλο HTML αποτελεί τον πλέον διαδεδομένο τρόπο μεταφοράς δεδομένων ιστοσελίδων πάνω απο το HTTP. Σε συνολικό διάγραμμα εγκατάστασης ένα τέτοιου τύπου κανάλι συμβολίζεται ως εξής:

Σχήμα 4-90: Βασικό στοιχείο καναλιού HTML/HTTP για συνολικό διάγραμμα εγκατάστασης

Το κομμάτι του κώδικα που είναι υπεύθυνο για την διόρθωση και αποδιάρθρωση των δεδομένων σε μορφή HTML είναι τα στελέχη που υλοποιούνται απο τα μηχανικά αντικείμενα που επικοινωνούν, και που βρίσκονται είτε σε έναν φυλλομετρητή που υλοποιεί το πρωτόκολλο HTML (όπως όλοι οι σύγχρονοι φυλλομετρητές), είτε σε έναν εξυπηρετητή διαδικτύου στο επίπεδο αλληλεπίδρασης. Ο δεσμευτής είναι το κομμάτι του κώδικα που «δένει» αντικείμενα του πρωτοκόλλου στο υποκείμενο πρωτόκολλο HTTP για μεταφορά τους πάνω στο διαδίκτυο. Τέλος, το αντικείμενο πρωτοκόλλου είναι το κομμάτι του κώδικα που υλοποιεί το HTTP Post request. Αυτό φαίνεται στο σχήμα που ακολουθεί:



Σχήμα 4-91: Βασικό στοιχείο καναλιού HTML/HTTP για διάγραμμα λεπτομέρειας

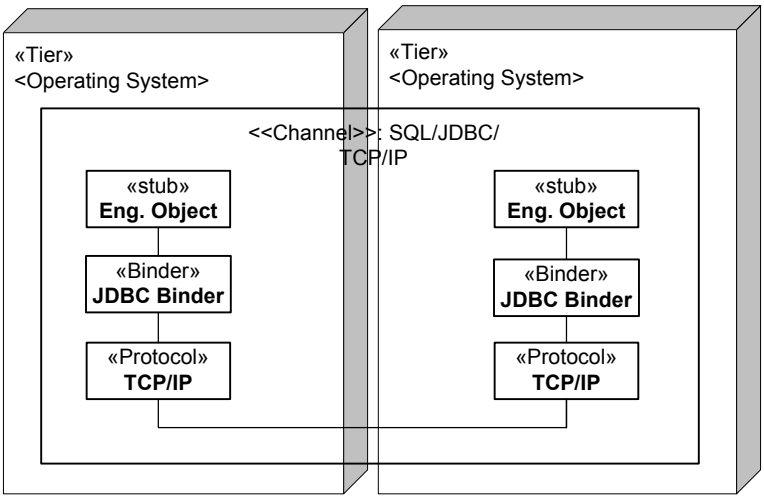
Η επικοινωνία με κανάλι αυτού του τύπου μπορεί να είναι σύγχρονη ή ασύγχρονη.

4.3.5.4.5.1.6 SQL με χρήση JDBC πάνω απο TCP/IP

Το πρωτόκολλο JDBC [Bales03] αποτελεί έναν διαδεδομένο τρόπο μεταφοράς δεδομένων σχεσιακών βάσεων δεδομένων (SQL) πάνω απο το διαδίκτυο. Σε συνολικό διάγραμμα εγκατάστασης ένα τέτοιου τύπου κανάλι συμβολίζεται ως εξής:

Σχήμα 4-92: Βασικό στοιχείο καναλιού SQL/JDBC/TCP/IP για συνολικό διάγραμμα εγκατάστασης

Το κομμάτι του κώδικα που είναι υπεύθυνο για την διόρθωση και αποδιάρθρωση των δεδομένων SQL σε μορφή JDBC είναι τα στελέχη που υλοποιούνται απο τα μηχανικά αντικείμενα που επικοινωνούν, και που απο τη μια πλευρά αποτελούν πάντα μια σχεσιακή βάση δεδομένων. Ο δεσμευτής είναι το κομμάτι του κώδικα που «δένει» αντικείμενα του πρωτοκόλλου στο υποκείμενο πρωτόκολλο TCP/IP για μεταφορά τους πάνω στο διαδίκτυο. Τέλος, το αντικείμενο πρωτοκόλλου είναι το κομμάτι του κώδικα που υλοποιεί το TCP/IP. Αυτό φαίνεται στο σχήμα που ακολουθεί:



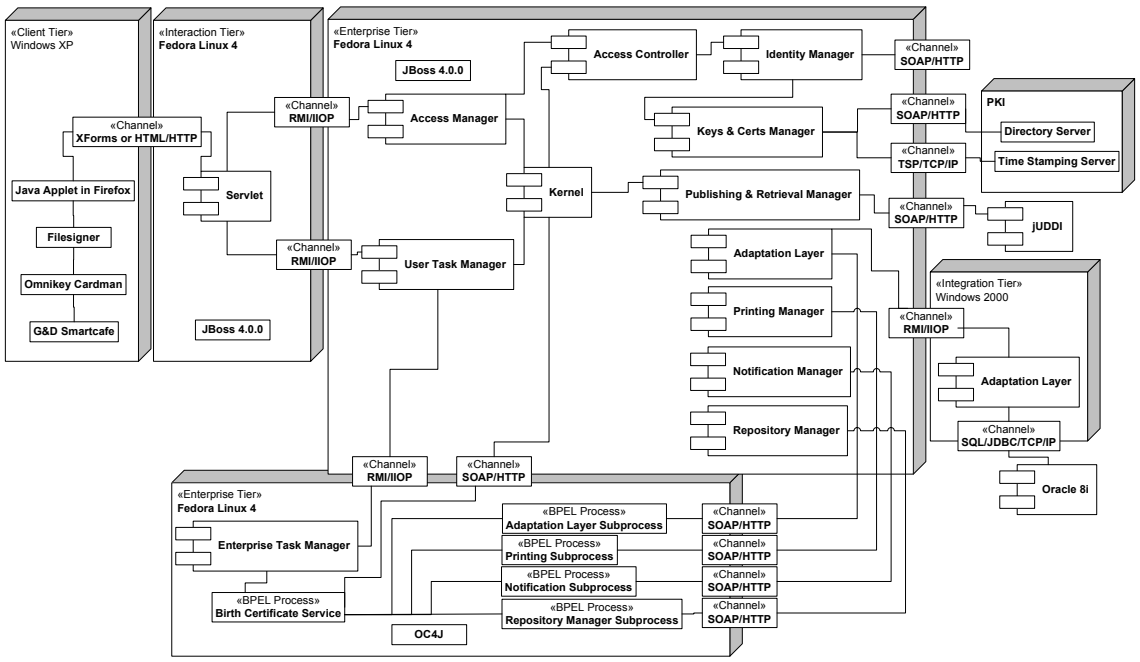
Σχήμα 4-93: Βασικό στοιχείο καναλιού HTML/HTTP για διάγραμμα λεπτομέρειας

Η επικοινωνία με κανάλι αυτού του τύπου είναι πάντα σύγχρονη.

4.3.5.4.6 Μεθοδολογία επέκτασης και παραδείγματα

Τα βασικά στοιχεία της προηγούμενης παραγράφου μπορούν να επεκταθούν αναγνωρίζοντας τα κατάλληλα στοιχεία που αποτελούν ένα νέο κανάλι που χρειάζεται να προστεθεί στα ήδη υπάρχοντα. Για το σκοπό αυτό, το προς σχεδιασμό κανάλι πρέπει να μελετηθεί και να εξαχθούν τα στοιχεία που αναπαριστούν ή παίζουν το ρόλο των στελεχών, των δεσμευτών, των αντικειμένων πρωτοκόλλου και ενδεχόμενων αναχαιτιστών που περιλαμβάνει σύμφωνα με τους ορισμούς των εννοιών της όψης μηχανικού και τις περιγραφές της παραγράφου 4.3.5.3.3.1.3.2. Αφότου αποφασιστούν ποια απο τα παραπάνω στοιχεία υπάρχουν στο σχεδιαζόμενο κανάλι (στην πλειονότητα των περιπτώσεων θα περιλαμβάνονται τουλάχιστον τα τρία πρώτα) και ποιες τεχνολογίες τα υλοποιούν, τότε σχεδιάζονται ένα συνοπτικό διάγραμμα για να περιληφθεί σε συνολικά διαγράμματα εγκατάστασης (παρόμοιο με αυτό του σχήματος Σχήμα 4-80) και ένα διάγραμμα λεπτομέρειας (παρόμοιο με αυτό του σχήματος Σχήμα 4-81).

Στη συνέχεια της παραγράφου δίνεται ένα συγκεκριμένο παράδειγμα προδιαγραφής της τεχνολογικής όψης για την αρχιτεκτονική που παρατέθηκε στο αντίστοιχο παράδειγμα της όψης μηχανικού και φιλοξενεί την υπηρεσία έκδοσης πιστοποιητικών γέννησης. Στο συνολικό διάγραμμα εγκατάστασης τεχνολογικής όψης που παρατίθεται στο Σχήμα 4-94 παρουσιάζεται το παράδειγμα της αρχιτεκτονικής με επιλεγμένες συγκεκριμένες τεχνολογίες για την υλοποίηση.



Σχήμα 4-94: Παράδειγμα συνολικού διαγράμματος εγκατάστασης τεχνολογικής όψης για μια ΑΔΑΑΥ που φιλοξενεί την υπηρεσία έκδοσης πιστοποιητικών γέννησης

Οι τεχνολογικές επιλογές που έχουν γίνει αναλύονται για κάθε κόμβο ως εξής:

1. Ο κόμβος Α στο επίπεδο πελάτη χρησιμοποιεί λειτουργικό Windows XP. Η Εφαρμογή πελάτη (Client) θα υλοποιηθεί ως ένα java applet το οποίο θα τρέχει στους χρησιμοποιούμενους φυλλομετρητές που στην προκειμένη περίπτωση θα είναι Mozilla Firefox 1.0.4. Το applet επικοινωνεί με το servlet διαχείρισης ιστοσελίδων στον κόμβο Β ανταλλάσσοντας απλές HTML σελίδες πάνω απο HTTP ή φόρμες βασισμένες στο πρότυπο XForms (όπως φαίνεται απο το αντίστοιχο κανάλι στο σχήμα) (βλ. και παραγράφους 4.3.5.4.5.1.4 και 4.3.5.4.5.1.5). Το applet χρησιμοποιεί την βιβλιοθήκη Filesigner (βλ. και παράγραφο 3.2.2) για την παραγωγή ψηφιακών και προηγμένων ηλεκτρονικών υπογραφών με χρήση ενός αναγνώστη κάρτας Omnikey Cardman και μιας έξυπνης κάρτας G&D Smartcafe.
2. Ο κόμβος Β στο επίπεδο αλληλεπίδρασης χρησιμοποιεί λειτουργικό σύστημα Fedora Linux 4. Ο κόμβος περιέχει έναν εξυπηρετητή εφαρμογών JBoss 4.0.0 στον οποίο ο Διαχειριστής ιστοσελίδων υλοποιείται με java servlets που δέχονται τις αιτήσεις πρόσβασης απο τα applets των χρηστών μέσω του καναλιού XForms/HTTP ή HTML/HTTP . Απο την άλλη πλευρά, τα servlets ανταλλάσσουν δεδομένα με τις εφαρμογές που τρέχουν στον εξυπηρετητή εφαρμογών του κόμβου C μέσω καναλιών RMI/IIOP (βλ. παράγραφο 4.3.5.4.5.1.2).
3. Ο κόμβος C στο πρώτο επιχειρησιακό επίπεδο χρησιμοποιεί λειτουργικό σύστημα Linux Fedora 4 και περιέχει επίσης έναν εξυπηρετητή εφαρμογών JBoss 4.0.0. Όπως αναλύθηκε στο παράδειγμα της παραγράφου 4.3.5.3.3.3 για την όψη μηχανικού, ο κόμβος αυτός φιλοξενεί το μεγαλύτερο μέρος των υπηρεσιών διαχείρισης, τις βασικές υπηρεσίες, τις υπηρεσίες υποστήριξης υπαρχουσών υποδομών και τις υπηρεσίες ασφάλειας. Οι τεχνολογικές επιλογές (βιβλιοθήκες, πρότυπα, προϊόντα) που θα χρησιμοποιηθούν στην υλοποίηση κάθε αντικειμένου θα πρέπει να αναλυθούν

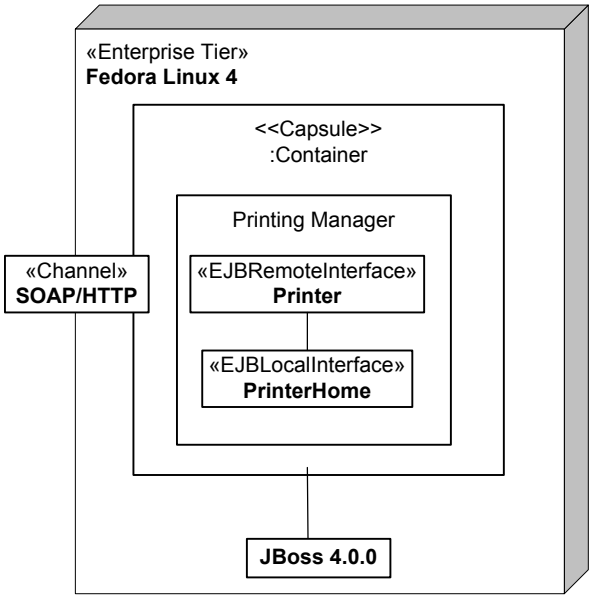
στα αντίστοιχα διαγράμματα λεπτομέρειας. Ως μέρος του παρόντος παραδείγματος αναλύονται τα κανάλια που χρησιμοποιούνται απο τα διάφορα μηχανικά αντικείμενα, καθώς και οι τεχνολογικές επιλογές που είναι εμφανής στο συνολικό διάγραμμα εγκατάστασης του σχήματος Σχήμα 4-94:

- Υπηρεσίες και μηχανισμοί διαχείρισης και συντονισμού:
  - Ο Διαχειριστής πρόσβασης επικοινωνεί με τα servlets του διαχειριστή ιστοσελίδων στον κόμβο Β μέσω ενός καναλιού RMI/IIOP.
  - Ο Διαχειριστής εργασιών χρηστών επικοινωνεί με τον διαχειριστή ιστοσελίδων στον κόμβο Β μέσω ενός καναλιού RMI/IIOP.
- Βασικές υπηρεσίες και μηχανισμοί
  - Ο Διαχειριστής δημοσίευσης και ανάκτησης επικοινωνεί με έναν κατάλογο υπηρεσιών ιστού UDDI μέσω ενός καναλιού SOAP/HTTP (βλ. παράγραφο 4.3.5.4.5.1.1). Ο κατάλογος UDDI που χρησιμοποιείται είναι μια υλοποίηση του λογισμικού ανοιχτού κώδικα jUDDI [jUDDI].
  - Ο Διαχειριστής αποθετηρίων ελέγχεται απο μια επιχειρησιακή υπο-διεργασία στον κόμβο D μέσω ενός καναλιού SOAP/HTTP.
  - Ο Διαχειριστής ειδοποιήσεων ελέγχεται απο μια επιχειρησιακή υπο-διεργασία στον κόμβο D μέσω ενός καναλιού SOAP/HTTP.
  - Ο Διαχειριστής εκτυπώσεων ελέγχεται απο μια επιχειρησιακή υπο-διεργασία στον κόμβο D μέσω ενός καναλιού SOAP/HTTP.
- Υπηρεσίες ασφάλειας
  - Ο Διαχειριστής ταυτοτήτων επικοινωνεί με εξωτερικές Αρχές που δημιουργούν και επικυρώνουν διαπιστευτήρια και ισχυρισμούς σύμφωνα με το πρότυπο SAML μέσω ενός καναλιού SOAP/HTTP.
  - Ο Διαχειριστής κλειδιών και πιστοποιητικών χρησιμοποιεί το πρότυπο XKMS για να επικοινωνήσει με την ΥΔΚ μέσω ενός καναλιού SOAP/HTTP και το πρότυπο RFC 3161 για το πρωτόκολλο χρονοσφράγισης πάνω απο ένα κανάλι TSP/TCP/IP (βλ. παράγραφο 4.3.5.4.5.1.3).
- Τα αντικείμενα που υλοποιούν τα Ενδιάμεσα επίπεδα προσαρμογής στους κόμβους C και E επικοινωνούν μέσω ενός καναλιού RMI/IIOP.

4. Ο κόμβος D στο δεύτερο επιχειρησιακό επίπεδο χρησιμοποιεί λειτουργικό σύστημα Fedora Linux 4 και περιέχει έναν εξυπηρετητή εφαρμογών Oracle με υποδοχέα εφαρμογών J2EE (*Oracle application server container for J2EE – OC4J*). Ο Διαχειριστής επιχειρησιακών διεργασιών αποτελεί μια μηχανή BPEL της Oracle (Oracle BPEL engine), ο οποίος επιτελεί τις διαχειριστικές εργασίες τις σχετικές με τον σχεδιασμό, συντονισμό, εγκατάσταση και απεγκατάσταση των επιχειρησιακών υπηρεσιών και υπο-υπηρεσιών. Τόσο ο Διαχειριστής επιχειρησιακών διεργασιών όσο και η κάθε επιχειρησιακή υπηρεσία που εγκαθίσταται στην συγκεκριμένη αρχιτεκτονική επικοινωνεί μέσω καναλιών SOAP/HTTP με τον πυρήνα στον κόμβο C. Επίσης ο Διαχειριστής επιχειρησιακών διεργασιών επικοινωνεί με ένα κανάλι RMI/IIOP με τον διαχειριστή εργασιών χρηστών στον κόμβο C.
5. Ο κόμβος E στο επίπεδο ολοκλήρωσης χρησιμοποιεί λειτουργικό σύστημα Windows 2000. Το Ενδιάμεσο επίπεδο προσαρμογής επικοινωνεί απο τη μια πλευρά με το αντίστοιχο αντικείμενο στον κόμβο C μέσω ενός καναλιού RMI/IIOP, και απο την άλλη με την υπάρχουσα βάση δεδομένων μέσω ενός καναλιού SQL/JDBC/TCP/IP

(βλ. παράγραφο 4.3.5.4.5.1.6). Η υπάρχουσα βάση δεδομένων του δήμου του παραδείγματος είναι μια Oracle 8i.

Όπως φαίνεται απο την παραπάνω ανάλυση, στο συγκεκριμένο παράδειγμα χρησιμοποιούνται τα διάφορα κανάλια που έχουν παρατεθεί ως βασικά στοιχεία της όψης στην παράγραφο 4.3.5.4.5.1 και δεν χρειάστηκε να οριστούν νέοι τύποι καναλιών που χρησιμοποιούν άλλες τεχνολογίες.
Το παράδειγμα ολοκληρώνεται με ένα διάγραμμα λεπτομέρειας στην τεχνολογική όψη για το αντικείμενο Διαχειριστή εκτυπώσεων σε πλήρη αντιστοίχηση με τα παραδείγματα που παρατέθηκαν στην περιγραφή της υπολογιστικής όψης και της όψης μηχανικού στις παραγράφους 4.3.4.3.3.3 και 4.3.5.3.3.3 αντίστοιχα. Το συγκεκριμένο διάγραμμα λεπτομέρειας φαίνεται στο Σχήμα 4-95:



Σχήμα 4-95: Παράδειγμα διαγράμματος λεπτομέρειας για το μηχανικό αντικείμενο Διαχειριστής εκτυπώσεων στην τεχνολογική όψη

Σε αντιστοιχία με τις προδιαγραφές της υπολογιστικής όψης και τις σχεδιαστικές αρχές της παραγράφου 4.3.5.4.4.1.1.3, παρατηρούμε ότι:

- Το λειτουργικό σύστημα στον κόμβο που βρίσκεται το αντικείμενο είναι Fedora Linux 4.
- Το αντικείμενο επικοινωνεί με άλλα αντικείμενα εκτός του κόμβου του μέσω ενός καναλιού SOAP/HTTP.
- Το αντικείμενο υλοποιεί την διεπαφή Printer που είναι μια διεπαφή απομακρυσμένης πρόσβασης (το οποίο δηλώνεται ορίζοντας το αντίστοιχο πρότυπο UML EJBRemoteInterface) και την διεπαφή PrinterHome που είναι μια διεπαφή τοπικής πρόσβασης (το οποίο δηλώνεται ορίζοντας το αντίστοιχο πρότυπο UML EJBLocalInterface) για την αρχιτεκτονική J2EE.
- Ο εξυπηρετητής εφαρμογών στον υποδοχέα του οποίου φιλοξενείται το αντικείμενο είναι ο JBoss 4.0.0.

- Η υλοποίηση του Διαχειριστή εκτυπώσεων χρησιμοποιεί το API υπηρεσιών εκτύπωσης της Java (Java Print Service API), το οποίο περιλαμβάνει ένα σύνολο επεκτάσιμων χαρακτηριστικών για εκτυπώσεις που βασίζονται στα προτυποιημένα χαρακτηριστικά που καθορίζονται στο Πρωτόκολλο Διαδικτυακών Εκτυπώσεων (Internet Printing Protocol – IPP) έκδοση 1.1 του οργανισμού IETF [Herriot00].

Προκειμένου να ολοκληρώσει τις προδιαγραφές του παραδείγματος, ο σχεδιαστής θα πρέπει να αναλύσει με αντίστοιχο τρόπο όλα τα μηχανικά αντικείμενα του σχήματος Σχήμα 4-94.

4.3.6 6ο στάδιο:Υλοποίηση

4.3.6.1 Μεθοδολογία σταδίου

Το στάδιο αυτό περιλαμβάνει τη διαδικασία υλοποίησης των στοιχείων που έχουν σχεδιαστεί στα προηγούμενα στάδια των προδιαγραφών. Πιο συγκεκριμένα υλοποιούνται με τις τεχνολογίες που έχουν επιλεγεί στην τεχνολογική όψη όλα τα στοιχεία της υπολογιστικής όψης, χρησιμοποιώντας τα αντικείμενα πληροφορίας που έχουν οριστεί στην όψη πληροφορίας και υλοποιώντας τις επιχειρησιακές διεργασίες που έχουν οριστεί στην επιχειρησιακή όψη. Τέλος οργανώνονται και εγκαθίστανται τα στοιχεία αυτά όπως έχει οριστεί στην όψη μηχανικού.
Η παρούσα μεθοδολογία, δεν προδιαγράφει συγκεκριμένη μέθοδο τεχνολογίας λογισμικού ή εργαλεία υλοποίησης τα οποία θα χρησιμοποιηθούν κατά την υλοποίηση και τον προγραμματισμό. Η επιλογή για κάποια μέθοδο ή μεθόδους αφήνεται στον σχεδιαστή της αρχιτεκτονικής.
Κατά την διάρκεια της υλοποίησης, ενδέχεται ορισμένες αποφάσεις που έχουν ληφθεί στον σχεδιασμό να οδηγούν σε αδιέξοδο, να εντοπίζονται πιο συμφέρουσες λύσεις ή να εμφανίζονται καινούργιες προδιαγραφές που δεν ήταν ξεκάθαρες ή ορατές στην αρχή (κάτι το οποίο είναι ο κανόνας και όχι η εξαίρεση στον σχεδιασμό και την υλοποίηση σύνθετων συστημάτων). Οι αλλαγές των προδιαγραφών που ενδέχεται να χρειάζονται, συλλέγονται και τεκμηριώνονται. Ανα τακτά χρονικά διαστήματα κατά την διάρκεια υλοποίησης οι αλλαγές αυτές ενσωματώνονται στις προδιαγραφές, και έτσι προκύπτουν επόμενες εκδόσεις τους πέραν της πρώτης, που έχουν ήδη προκύψει απο την εφαρμογή των σταδίων 2 με 5.

4.3.7 7ο στάδιο: Έλεγχος συμμόρφωσης και ενημέρωση προδιαγραφών

4.3.7.1 Στόχοι

Το παρόν στάδιο έχει στόχο να θέσει τα σημεία αναφοράς της αρχιτεκτονικής (όπως ορίζονται απο το πρότυπο) να καθορίσει και να καθορίσει ποια απο αυτά είναι σημεία συμμόρφωσης. Στην συνέχεια επιτελείται ο έλεγχος των σημείων αυτών όπως περιγράφονται στις προδιαγραφές προκειμένου να εντοπιστούν τα σημεία στα οποία το υλοποιημένο σύστημα δεν συμμορφώνεται στις προδιαγραφές για να διορθωθεί.

4.3.7.2 Μεθοδολογία σταδίου

Ο καθορισμός των σημείων αναφοράς και συμμόρφωσης χρονικά γίνεται κατά την διάρκεια των σταδίων 2, 4 και 5 της παρούσας μεθόδου. Κάθε ένα απο αυτά τα στάδια (και οι επιμέρους προδιαγραφές όψεων που περιέχει) χρησιμοποιούν τις αρχές του παρόντος σταδίου προκειμένου να ορίσουν τις απαραίτητες δηλώσεις συμμόρφωσης. Μετά το πέρας του σταδίου 6 και την υλοποίηση του συστήματος, επιτελείται στο παρόν στάδιο ο έλεγχος συμμόρφωσης βάσει αυτών των σημείων. Τα αποτελέσματα του ελέγχου επιδεικνύουν απο τη μία πλευρά ποια κομμάτια των προδιαγραφών πρέπει να βελτιωθούν ή ενημερωθούν, και ποια στοιχεία του υλοποιημένου συστήματος να διορθωθούν.

Τα βήματα που ακολουθούνται είναι τα εξής:

Ι. Στην αρχή καταγράφονται τα σημεία συμμόρφωσης σε κάθε όψη, με την ακόλουθη σειρά:

1. Κατά την διάρκεια σχεδιασμού των προδιαγραφών της Όψης Μηχανικού, καθορίζονται πρώτα τα πιθανά σημεία αναφοράς σύμφωνα με τις αρχές της παραγράφου 4.3.7.3.1. Στη συνέχεια επιλέγεται ένα υποσύνολο αυτών των σημείων αναφοράς που αναγνωρίζονται ως σημεία συμμόρφωσης.

2. Κατά την διάρκεια σχεδιασμού των προδιαγραφών της Υπολογιστικής Όψης, καταγράφονται τα πιθανά σημεία αναφοράς σύμφωνα με τις αρχές της παραγράφου 4.3.7.3.2. Στη συνέχεια επιλέγονται ποια απο τα σημεία αυτά αναγνωρίζονται ως σημεία συμμόρφωσης. Επίσης, τα σημεία αναφοράς στην Υπολογιστική Όψη που αντιστοιχούν σε σημεία αναφοράς στην Όψη Μηχανικού και αναφέρουν χαρακτηριστικά διαφάνειας που εφαρμόζονται σε αυτά, γίνεται αυτόματα σημεία συμμόρφωσης.

3. Γίνεται καταγραφή των σημείων αναφοράς της Όψης Μηχανικού και της Υπολογιστικής Όψης που σχετίζονται με σταθερά, δυναμικά και στατικά σχήματα αντικειμένων πληροφορίας. Καθορίζεται ποια απο τα σημεία αυτά θεωρούνται σημεία συμμόρφωσης εκφραζόμενα με όρους της Όψης Πληροφορίας.

4. Γίνεται καταγραφή των σημείων αναφοράς της Όψης Μηχανικού και της Υπολογιστικής Όψης που σχετίζονται με επιχειρησιακούς στόχους της αρχιτεκτονικής και πολιτικές. Καθορίζεται ποια απο τα σημεία αυτά θεωρούνται σημεία συμμόρφωσης εκφραζόμενα με όρους της Επιχειρησιακής Όψης.

ΙΙ. Σε δεύτερη φάση, γίνεται ο έλεγχος των προδιαγραφών:

1. Για κάθε προγραμματιστικό σημείο συμμόρφωσης, ελέγχεται αν η υλοποίηση της αρχιτεκτονικής έχει την καθορισμένη συμπεριφορά ως προς την αλληλεπίδραση μεταξύ προγραμματιστικών διεπαφών.
2. Για κάθε αντιληπτικό σημείο συμμόρφωσης, ελέγχεται αν η υλοποίηση της αρχιτεκτονικής έχει την καθορισμένη συμπεριφορά ως προς την αλληλεπίδραση των υπηρεσιών με οντότητες του εξωτερικού κόσμου (π.χ. ανθρώπους κ.λ.π.)
3. Για κάθε διαλειτουργικό σημείο συμμόρφωσης, ελέγχεται αν η υλοποίηση της αρχιτεκτονικής έχει την καθορισμένη συμπεριφορά ως προς την διακίνηση και ανταλλαγή πληροφορίας με μεταξύ δύο ή περισσότερων συστημάτων μέσα στην αρχιτεκτονική ή και εκτός αυτής.
4. Για κάθε σημείο αναφοράς συνδιαλλαγής, ελέγχεται αν η υλοποίηση της αρχιτεκτονικής έχει την καθορισμένη συμπεριφορά ως προς τις μεθόδους πρόσβασης σε φυσικά μέσα αποθήκευσης και μεταφοράς πληροφορίας.

ΙΙΙ. Η Τρίτη φάση του παρόντος σταδίου έχει να κάνει με την ενημέρωση των προδιαγραφών και την διόρθωση της υλοποίησης.

1. Για κάθε σημείο συμμόρφωσης που ο έλεγχος είναι αρνητικός μελετώνται οι προδιαγραφές και:
   - Είτε ενημερώνονται κατάλληλα οι προδιαγραφές, διορθώνεται η υλοποίηση ώστε να συμμορφώνεται με τις νέες προδιαγραφές και επαναλαμβάνεται ο έλεγχος.
   - Είτε οι προδιαγραφές παραμένουν αμετάβλητες, διορθώνεται η υλοποίηση ώστε να συμμορφώνεται με αυτές και επαναλαμβάνεται ο έλεγχος.

Οι φάσεις I, II και III του παρόντος σταδίου, εφαρμόζονται τόσες φορές, όσες χρειάζεται προκειμένου να σταθεροποιηθούν οι προδιαγραφές του συστήματος και όλοι οι έλεγχοι της υλοποίησης στα σημεία συμμόρφωσης να είναι πετυχημένοι. Στο πέρας αυτής της διαδικασία έχει υλοποιηθεί επιτυχώς η αρχιτεκτονική.

4.3.7.3 Έλεγχος συμμόρφωσης

Σε πρώτη φάση ο έλεγχος συμμόρφωσης απαιτεί την καταγραφή και ορισμό των σημείων αναφοράς (όπως αναφέρονται στο πρότυπο RM-ODP) σε κάθε όψη. Επειδή τα σημεία αναφοράς της επιχειρησιακής όψης και της όψης πληροφορίας βασίζονται στα σημεία αναφοράς της υπολογιστικής όψης και κυρίως της όψης μηχανικού, η μέθοδος (όπως φαίνεται απο την προηγούμενη παράγραφο) ορίζει πρώτα τα σημεία αναφοράς σε αυτές τις όψεις (ανάποδα δηλαδή απο την σειρά προδιαγραφής τους). Η τεχνολογική όψη δεν έχει σημεία αναφοράς. Εάν αυτό είναι θεμιτό, ο σχεδιαστής θα πρέπει να ελέγχει κατά το στάδιο της συμμόρφωσης αν οι τεχνολογικές λύσεις που έχει επιλέξει συμμορφώνονται με τα επιμέρους τεχνολογικά πρότυπα στα οποία αντιστοιχούν (αν αυτά υπάρχουν). Στην παρούσα παράγραφο περιγράφεται πως καταγράφονται τα σημεία αναφοράς στις όψεις.

4.3.7.3.1 Σημεία αναφοράς στην όψη μηχανικού

Τα ακόλουθα θεωρούνται σημεία αναφοράς, και άρα πιθανά σημεία συμμόρφωσης, στην όψη μηχανικού:

Πιθανά προγραμματιστικά σημεία αναφοράς:
- Ανάμεσα σε βασικά μηχανικά αντικείμενα που επικοινωνούν (κλάσεις).
- Ανάμεσα σε βασικά μηχανικά αντικείμενα και το λειτουργικό σύστημα.
- Ανάμεσα σε βασικά μηχανικά αντικείμενα και στελέχη καναλιών.
- Ανάμεσα σε στελέχη καναλιών.
- Ανάμεσα σε στελέχη και δεσμευτές.
- Ανάμεσα σε δεσμευτές.
- Ανάμεσα σε δεσμευτές και αντικείμενα πρωτοκόλλου.
- Ανάμεσα σε αντικείμενα πρωτοκόλλου και άλλα αντικείμενα πρωτοκόλλου στον ίδιο κόμβο.
- Διεπαφές ελέγχου στελεχών, δεσμευτών, αντικειμένων πρωτοκόλλου και αναχαιτιστών.

Πιθανά αντιληπτικά σημεία αναφοράς:
- Διεπαφή ενός αντικειμένου.

Πιθανά διαλειτουργικά σημεία αναφοράς:
- Ανάμεσα σε αντικείμενα πρωτοκόλλου που βρίσκονται σε διαφορετικούς κόμβους.

Πιθανά σημεία αναφοράς συνδιαλλαγών:
- Διεπαφή ενός αντικειμένου.

Ο ορισμός των διαλειτουργικών σημείων αναφοράς ως σημεία συμμόρφωσης, επιτρέπει την διαλειτουργικότητα ανάμεσα σε συστήματα.
Ο ορισμός των προγραμματιστικών σημείων αναφοράς ως σημεία συμμόρφωσης, επιτρέπει την μεταφερσιμότητα μηχανικών αντικειμένων ανάμεσα σε συστήματα, και προωθεί την ανοιχτότητα της αρχιτεκτονικής.
Η καταγραφή των σημείων αναφοράς και η επιλογή τους ως σημεία συμμόρφωσης μπορεί να γίνει με τον ακόλουθο (ή κάποιον παρόμοιο) πίνακα:

Κατηγορία σημείου	**Αναγνωριστικό σημείου**	**Περιγραφή σημείου**	**Περιγραφή επιθυμητής λειτουργικότητας**	**Αποδοχή ως σημείο συμμόρφωσης**

Πίνακας 4-5: Πρότυπο πίνακα καταγραφής σημείων αναφοράς της όψης μηχανικού

Η στήλη κατηγορία περιέχει την κατηγορία του συγκεκριμένου σημείου αναφοράς: αν είναι προγραμματιστικό, αντιληπτικό, συνδιαλλαγής ή διαλειτουργικό. Η στήλη αναγνωριστικό σημείου περιέχει έναν κωδικό για το σημείο. Προτείνεται η ακόλουθη σημειογραφία: αρχικά όψης, κατηγορία σημείου, αύξων αριθμός. Για παράδειγμα το πρώτο προγραμματιστικό σημείο της όψης μηχανικού θα έχει το αναγνωριστικό ΟΜΠ00.
Η περιγραφή σημείου περιέχει τα αντικείμενα τα οποία βρίσκονται στα δύο άκρα του σημείου αναφοράς. Η περιγραφή της επιθυμητής λειτουργικότητας περιγράφει τις απαιτήσεις συμμόρφωσης για το σημείο. Η τελευταία στήλη «αποδοχή ως σημείο συμμόρφωσης» καθορίζει αν το συγκεκριμένο γίνεται αποδεκτό ως σημείο συμμόρφωσης για τον έλεγχο των προδιαγραφών.

4.3.7.3.2 Σημεία αναφοράς στην υπολογιστική όψη

Στην υπολογιστική όψη, υπάρχει ένα σημείο αναφοράς σε κάθε διεπαφή ενός υπολογιστικού αντικειμένου. Το αν το σημείο αυτό θα θεωρηθεί προγραμματιστικό, αντιληπτικό, διαλειτουργικό ή συνδιαλλαγής εξαρτάται απο τις απαιτήσεις συμπεριφοράς που απαιτείται να καλυφθούν όταν αυτό ορίζεται ως σημείο συμμόρφωσης μέσα στις προδιαγραφές.
Η υλοποίηση που θέλει να συμμορφώνεται στις προδιαγραφές της υπολογιστικής όψης πρέπει να παραθέσει τα σημεία αναφοράς της όψης μηχανικού που αντιστοιχούν σε σημεία αναφοράς της υπολογιστικής όψης και να δηλώσει ποιες δομές διαφάνειας και μηχανικών αντικειμένων τα χαρακτηρίζουν. Κατ' αυτόν τον τρόπο τα συγκεκριμένα σημεία αναφοράς γίνονται σημεία συμμόρφωσης.
Η συμμόρφωση ενός αντικειμένου σε ένα προγραμματιστικό σημείο αναφοράς μπορεί να ελεγχθεί σε σχέση με την προτυποποιημένη μορφή μιας διεπαφής σε μια γλώσσα που ικανοποιεί τους κανόνες μεταφερσιμότητας. Η συμμόρφωση ενός αντικειμένου σε ένα διαλειτουργικό σημείο αναφοράς μπορεί να ελεγχθεί με τις αλληλεπιδράσεις που εμφανίζονται σε πρωτόκολλα επικοινωνίας στα οποία συμμετέχει η διεπαφή.
Η καταγραφή των σημείων αναφοράς και η επιλογή τους ως σημεία συμμόρφωσης γίνεται με έναν πίνακα παρόμοιο με αυτόν της προηγούμενης παραγράφου:

Κατηγορία σημείου	**Αναγνωριστικό**	**Περιγραφή σημείου**	**Περιγραφή επιθυμητής λειτουργικότητας**	**Αντίστοιχο σημείο**	**Αποδοχή ως σημείο συμμόρφωσης**

	σημείου			όψης μηχανικού	

Στον πίνακα αυτό έχει προστεθεί η στήλη «αντίστοιχο σημείο όψης μηχανικού» στην οποία καταγράφονται τα αναγνωριστικά των σημείων αναφοράς της όψης μηχανικού που έχουν καταγραφεί και σχετίζονται με το συγκεκριμένο σημείο αναφοράς της υπολογιστικής όψης.

4.3.7.3.3 Σημεία αναφοράς στην όψη πληροφορίας

Στην όψη πληροφορίας οι δηλώσεις συμμόρφωσης απαιτούν ότι η συμπεριφορά του κατανεμημένου συστήματος συμμορφώνεται με ένα συγκεκριμένο σύνολο απο σταθερά, δυναμικά και στατικά σχήματα.

Η υλοποίηση που θέλει να συμμορφώνεται στις προδιαγραφές της όψης πληροφορίας πρέπει να παραθέσει τα σημεία αναφοράς της όψης μηχανικού και της υπολογιστικής όψης που αντιστοιχούν σε σημεία αναφοράς της όψης πληροφορίας. Κατ' αυτόν τον τρόπο τα συγκεκριμένα σημεία αναφοράς γίνονται σημεία συμμόρφωσης. Οι αλληλεπιδράσεις στα σημεία αυτά μπορούν να εκφραστούν σε όρους της όψης πληροφορίας προκειμένου να ελεγχθεί ότι είναι συνεπή με σταθερά, στατικά και δυναμικά σχήματα.

Σημεία αναφοράς της όψης πληροφορίας μπορεί να είναι και των τεσσάρων ειδών. Η καταγραφή των σημείων αναφοράς και η επιλογή τους ως σημεία συμμόρφωσης γίνεται με έναν πίνακα παρόμοιο με αυτόν της προηγούμενης παραγράφου:

Κατηγορία σημείου	**Αναγνωριστικό σημείου**	**Περιγραφή σημείου**	**Περιγραφή επιθυμητής λειτουργικότητας**	**Αντίστοιχο σημείο όψης μηχανικού ή υπολογιστικής όψης**	**Αποδοχή ως σημείο συμμόρφωσης**

Στον πίνακα αυτό έχει προστεθεί η στήλη «αντίστοιχο σημείο όψης μηχανικού ή υπολογιστικής όψης» στην οποία καταγράφονται τα αναγνωριστικά των σημείων αναφοράς της όψης μηχανικού ή της υπολογιστικής όψης που έχουν καταγραφεί και σχετίζονται με το συγκεκριμένο σημείο αναφοράς της όψης πληροφορίας.

4.3.7.3.4 Σημεία αναφοράς στην επιχειρησιακή όψη

Στην επιχειρησιακή όψη οι δηλώσεις συμμόρφωσης απαιτούν ότι η συμπεριφορά του κατανεμημένου συστήματος συμμορφώνονται με ένα συγκεκριμένο σύνολο απο στόχους και πολιτικές.

Η υλοποίηση που θέλει να συμμορφώνεται στις προδιαγραφές της επιχειρησιακής όψης πρέπει να παραθέσει τα σημεία αναφοράς της όψης μηχανικού, της υπολογιστικής όψης και της όψης πληροφορίας που αντιστοιχούν σε σημεία αναφοράς της επιχειρησιακής όψης. Κατ' αυτόν τον τρόπο τα συγκεκριμένα σημεία αναφοράς γίνονται σημεία συμμόρφωσης. Οι αλληλεπιδράσεις στα σημεία αυτά μπορούν να εκφραστούν σε όρους

της επιχειρησιακής όψης προκειμένου να ελεγχθεί ότι δεν παραβιάζονται οι προδιαγραφές της επιχειρησιακή όψης. Τα σημεία αναφοράς που καταγράφονται θα πρέπει να καλύπτουν κατ' ελάχιστο τις πολιτικές που έχουν προδιαγραφεί στην επιχειρησιακή όψη.
Σημεία αναφοράς της όψης πληροφορίας μπορεί να είναι και των τεσσάρων ειδών. Η καταγραφή των σημείων αναφοράς και η επιλογή τους ως σημεία συμμόρφωσης γίνεται με έναν πίνακα παρόμοιο με αυτόν της προηγούμενης παραγράφου:

Κατηγορία σημείου	**Αναγνωριστικό σημείου**	**Περιγραφή σημείου**	**Περιγραφή επιθυμητής λειτουργικότητας**	**Αντίστοιχο σημείο όψης μηχανικού ή υπολογιστικής όψης ή όψης πληροφορίας**	**Αποδοχή ως σημείο συμμόρφωσης**

Στον πίνακα αυτό έχει προστεθεί η στήλη «αντίστοιχο σημείο όψης μηχανικού ή υπολογιστικής όψης ή όψης πληροφορίας» στην οποία καταγράφονται τα αναγνωριστικά των σημείων αναφοράς της όψης μηχανικού ή της υπολογιστικής όψης ή της όψης πληροφορίας που έχουν καταγραφεί και σχετίζονται με το συγκεκριμένο σημείο αναφοράς της επιχειρησιακής όψης.

4.4 Συμπεράσματα

Το παρόν κεφάλαιο εισήγαγε την έννοια της ασφαλούς, διαλειτουργικής και ανοιχτής αρχιτεκτονικής υπηρεσιών (ΑΔΑΑΥ) και παρουσίασε αναλυτικά μια πρωτότυπη κατασκευαστική μέθοδο σχεδιασμού τέτοιου τύπου αρχιτεκτονικών, η οποία βασίζεται στο σύνολο των εννοιών που ορίζονται στο προτυποποιημένο πλαίσιο αναφοράς ISO / RM-ODP. Η μέθοδος φιλοδοξεί να καλύψει τις σχεδιαστικές ανάγκες της νέας γενιάς αρχιτεκτονικών υπηρεσιών που έχουν κάνει την εμφάνισή τους στην ερευνητική κοινότητα και στον επιχειρηματικό κόσμο παγκοσμίως τα τελευταία 2 χρόνια.
Προκειμένου να επαληθευτεί η αξία και η εφαρμοσιμότητα της μεθόδου, οι αρχές της έχουν ήδη εφαρμοστεί στους τομείς του η-επιχειρείν και της η-διακυβέρνησης με την παραγωγή των προδιαγραφών δύο καινοτόμων επιχειρησιακών υπηρεσιών. Οι προδιαγραφές αυτές παρουσιάζονται στο επόμενο κεφάλαιο και αποτελούν τον $4^{ο}$ άξονα της παρούσας διατριβής. Σημειώνεται ότι ένα μέρος της κατασκευαστικής μεθόδου έχει ήδη χρησιμοποιηθεί στα πλαίσια ενός Ευρωπαϊκού ερευνητικού έργου για την παραγωγή των προδιαγραφών και την υλοποίηση μιας πλήρους αρχιτεκτονικής η-διακυβέρνησης.

4.5 Αναφορές

[ActiveX] D. Chappell. (1999). "Understanding ActiveX and OLE". Microsoft Press.
[Adams01] C. Adams et al. (2001). "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)". IETF RFC 3161, http://www.ietf.org/rfc/rfc3161.txt
[Applet] SUN Microsystems. Java Applets. http://java.sun.com/applets/

[Bales03] D. Bales. (2003). "JDBC Pocket Reference". O' Reilly publications.
[Boyer06] J. Boyer et al. (Editors). (2006). "XForms 1.0". W3C Recommendation. http://www.w3.org/TR/xforms/
[dotNet] Microsoft. (2006). Microsoft .NET. http://www.microsoft.com/net/.
[ETSI101733] ETSI Technical Specification. (2002). "Electronic signature and infrastructures; Electronic signature formats". ETSI TS 101 733 V1.4.0, http://portal.etsi.org
[Frankel03] D. Frankel Consulting. (2003). "Applying EDOC and MDA to the RM-ODP Engineering and Technology Viewpoints: An architectural perspective", v. 01-00
[Herriot00] R. Herriot et al. (Editor). (2000). "Internet Printing Protocol/1.1: Encoding and Transport". IETF RFC 2910, http://www.ietf.org/rfc/rfc2910.txt
[High05] R. High, S. Kinder, S. Graham. (2005). "IBM's SOA Foundation – An architectural Introduction and Overview". http://www-128.ibm.com/developerworks/webservices/library/ws-soa-whitepaper/
[Housley02] R. Housley, W. Polk, W. Ford, D. Solo. (2002). "RFC 3280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".
[J2EE] SUN Microsystems. Java 2 Platform, Enterprise Edition (J2EE). Specification, SUN Microsystems.
[jUDDI] Apache. jUDDI. http://ws.apache.org/juddi/
[Kaliontzoglou05] A. Kaliontzoglou et al. (2005). "A secure e-Government platform architecture for small to medium sized public organizations", Electronic Commerce Research & Applications, Elsevier, Volume 4, No. 2, pp. 174-186
[Kaliontzoglou06] A. Kaliontzoglou et al. (2006). "A formalized design method for building e-government architectures", (To appear in) Secure e-Government Web Services, Idea Group Publishing, Hershey, PA
[Karantjias03] A. Karantjias et al. (2003). "Secure Applications for the Chambers of Commerce", SSGRR 2003 Winter Conference, 2003, L'Aquilla, Italy
[Kreger01] H. Kreger. (2001). "Web Services Conceptual Architecture – WSCA 1.0". White paper, http://www-3.ibm.com/software/solutions/webservices/pdf/KREGER01.pdf
[Meneklis05a] Meneklis et al. (2005). "Engineering and Technology aspects of an e-government architecture based on Web Services", (to appear in) proceedings of 3rd IEEE European Conference on Web Services, Växjö, Sweden
[Meneklis05b] B. Meneklis et al. (2005). "Applying the ISO RM-ODP standard in e-Government", E-Government: Towards Electronic Democracy: International Conference, TCGOV 2005, Bolzano, Italy, Proceedings, Lecture Notes in Computer Science, Springer-Verlag GmbH, Volume 3416 / 2005, pp. 213
[Mitra03] N. Mitra. (Editor). (2003). "SOAP version 1.2 Part0: Primer". W3C Recommendation, http://www.w3.org/TR/soap12-part0/
[Neuman94] B. C. Neuman, T. Ts'o. (1994). "Kerberos: An Authentication Service for Computer Networks". *IEEE Communications*, 32(9):33-38. September 1994
[OC4J] Oracle. (2006). "Oracle Application Server 10gR3, New Features Overview". Oracle white paper, http://www.oracle.com/technology/tech/java/oc4j/1013/OracleAS-NF-1013.pdf
[OCL] Object Management Group. (2005). "OCL 2.0 Specification". http://www.omg.org/docs/ptc/05-06-06.pdf

[Peltz03] C. Peltz. (2003). “Web services orchestration and choreography”. IEEE Computer, Vol 36, Issue 10, pp. 46- 52
[RMI] SUN Microsystems. (2003). “Java RMI Specification”. http://java.sun.com/j2se/1.4.2/docs/guide/rmi/spec/rmiTOC.html
[RM-ODP] ITU-T Rec. X.901 | ISO/IEC 10746-1,2,3, “Reference Model for Open Distributed Processing – Part 1: Overview, Part 2 Foundations, Part 3 Architecture”, 1996-98
[Tang04] A. Tang, J. Han, and P. Chen. (2004). "A Comparative Analysis of Architecture Frameworks," Swinburne University of Technology SUTIT-TR2004.01
[UML1.4] Unified Modeling Language (UML) 1.4, http://www.omg.org/cgi-bin/doc?formal/01-09-67
[UML2.0] Unified Modeling Language (UML) 2.0, http://www.omg.org/technology/documents/formal/uml.htm

5 Εφαρμογή κατασκευαστικής μεθόδου για την προδιαγραφή υπηρεσιών η-συναλλαγών βασισμένων σε ΑΔΑΑΥ

5.1 Εισαγωγή

Το παρόν κεφάλαιο στοχεύει στο να επαληθεύσει την ορθότητα και εφαρμοσιμότητα της κατασκευαστικής μεθόδου του κεφαλαίου 4, με την εφαρμογή της για την παραγωγή των προδιαγραφών δυο σημαντικών υπηρεσιών η-συναλλαγών που βασίζονται στην έννοια των ΑΔΑΑΥ. Στην περιγραφή κάθε επιχειρησιακής υπηρεσίας αρχικά αιτιολογείται ο λόγος επιλογής της, δίνεται μια ακριβής περιγραφή της στα πλαίσια ενός οργανισμού ο οποίος θα μπορούσε να την προσφέρει, παρέχεται η τρέχουσα κατάσταση της υπηρεσίας σε διάφορα επίπεδα και στη συνέχεια εφαρμόζονται κατάλληλα ένα προς ένα τα στάδια που έχουν περιγραφεί για την παραγωγή των προδιαγραφών.

5.2 Υπηρεσία έκδοσης ηλεκτρονικών τιμολογίων

5.2.1 Εισαγωγή

Ένα εμπορικό τιμολόγιο είναι το πλέον σημαντικό έγγραφο που ανταλλάσσεται ανάμεσα σε εμπορικούς εταίρους. Πέραν της αξίας του ως επιχειρησιακό έγγραφο, ένα τιμολόγιο αποτελεί και ένα έγγραφο λογιστικό με νομική αξία και αποτελεί τη βάση για την δήλωση και απόδοση Φόρου Προστιθέμενης Αξίας (ΦΠΑ), την δήλωση στατιστικών στοιχείων για το εμπόριο ανάμεσα σε χώρες-μέλη της Ευρωπαϊκής Ένωσης και τις δηλώσεις εισαγωγών και εξαγωγών με χώρες εκτός της Ένωσης. Επομένως τα τιμολόγια έχουν κρίσιμη σημασία στο σύστημα ΦΠΑ κάθε χώρας μέλους. Καθορίζουν την δυνατότητα απόδοσης ΦΠΑ απο τον παραλήπτη του τιμολογίου και το καθεστώς ΦΠΑ που εφαρμόζεται σε κάθε περίπτωση. Με την πιο συστηματική χρήση των τιμολογίων, οι φορολογικές αρχές μπορούν να υλοποιήσουν νέες μεθόδους και εργαλεία για την διεξαγωγή εναλλακτικών ελέγχων που είναι λιγότερο παρεισφρητικοί στους συναλλασσόμενους οργανισμούς.

Η Οδηγία της Ευρωπαϊκής Ένωσης για την νομοθεσία του ΦΠΑ σχετικά με την ηλεκτρονική τιμολόγηση και την ηλεκτρονική αποθήκευση τιμολογίων ήρθε σε ισχύ σε κράτη μέλη τον Ιανουάριο του 2004 και θα πρέπει να υιοθετηθεί απο όλες της χώρες της Ένωσης μέχρι το 2008. Επομένως, η εγκατάσταση υπηρεσιών η-τιμολόγησης είναι μια νέα πανευρωπαϊκή ανάγκη. Παρ' όλα αυτά, προκειμένου υλοποιήσεις η-τιμολόγησης να είναι επιτυχείς, θα πρέπει να συμμορφώνονται με τις απαιτήσεις της συγκεκριμένης Οδηγίας, δηλαδή να είναι διαλειτουργικές, ασφαλής, οικονομικές και αποδεκτές απο την πλειοψηφία των επιχειρήσεων και των οργανισμών που δρουν στα Ευρωπαϊκά κράτη μέλη.

Οι περισσότερες υλοποιήσεις η-τιμολόγησης σήμερα βασίζονται στο EDI, το οποίο αποτελεί μια τεχνολογική λύση που καλύπτεται απο την Οδηγία. Η δεύτερη επιλογή, είναι η χρήση προηγμένων υπογραφών, αλλά η υιοθέτησή τους δεν είναι ευρεία αυτή τη στιγμή. Πιο συγκεκριμένα, η Οδηγία δηλώνει: «... τιμολόγια που αποστέλλονται με ηλεκτρονικά μέσα θα είναι αποδεκτά απο τα κράτη μέλη δεδομένου ότι εξασφαλίζεται η

αυθεντικοποίηση και η ακεραιότητα των περιεχομένων με την χρήση προηγμένων ηλεκτρονικών υπογραφών...».
Ανάμεσα σε άλλα σημεία στα οποία δίνεται έμφαση, η Οδηγία καθορίζει την ασφαλή αποθήκευση και διατήρηση των τιμολογίων: «... μια οντότητα που υπόκειται σε φορολογικό καθεστώς θα εξασφαλίζει ότι αντίγραφα των τιμολογίων που εκδίδονται, αποστέλλονται και λαμβάνονται διαφυλάττονται. ... η αυθεντικοποίηση, ακεραιότητα και αναγνωσιμότητα των εγγράφων θα εξασφαλίζεται καθ' όλη τη διάρκεια της φύλαξής τους...».

5.2.2 Τρέχουσα κατάσταση και νομικό πλαίσιο υπηρεσιών η-τιμολόγησης

Η παράγραφος αυτή παρουσιάζει την σχετική Ευρωπαϊκή νομοθεσία για συστήματα ασφαλούς η-τιμολόγησης, περιγράφει τις απαιτήσεις ασφάλειας που απορρέουν απο αυτή. Επίσης παρουσιάζονται υλοποιήσεις τέτοιων συστημάτων.

5.2.2.1 Νομικό πλαίσιο

Οι οδηγίες της Ευρωπαϊκής Επιτροπής επιταχύνουν την προσδοκώμενη εναρμόνιση των εθνικών νομικών πλαισίων των χωρών μελών, προκειμένου να παρασχεθεί ένα ομοιόμορφο πλαίσιο για την Ευρωπαϊκή αγορά, υπο την οποία η ηλεκτρονική τιμολόγηση θα προτυποποιηθεί και θα είναι εφαρμόσιμη σε κάθε κράτος μέλος. Το άμεσο αποτέλεσμα αυτής της προσπάθειας είναι η διευκόλυνση των εμπορικών συναλλαγών ανάμεσα σε κράτη μέλη, με την ανταλλαγή η-τιμολογίων. Η προαναφερθείσα εναρμόνιση θα επιτευχθεί με την εισαγωγή των ακόλουθων οδηγιών:

- Οδηγία 2001/115/EC της 20ης Δεκεμβρίου του 2001, η οποία βελτιώνει την Οδηγία 77/388/EEC με στόχο την απλοποίηση, εκσυγχρονισμό και εναρμόνιση των συνθηκών για τιμολόγηση σε σχέση με τον Φόρο Προστιθέμενης Αξίας [E01115]. Η Οδηγία αυτή ξεκαθαρίζει την υλοποίηση της η-τιμολόγησης στα κράτη-μέλη και σκοπεύει να εισάγει εναρμονισμένες διαδικασίες για την τιμολόγηση (σε χαρτί ή ηλεκτρονική) διαμέσου συνόρων κρατών. Σύμφωνα με την Οδηγία, οι επιχειρήσεις που λειτουργούν σε κράτη μέλη πρέπει να έχουν απλοποιημένους κανονισμούς περί τιμολόγησης και διαδικασίες εναρμονισμένες σε κοινοτικό επίπεδο απο τον Ιανουάριο του 2004. Η Οδηγία επιπρόσθετα προάγει την χρήση των ΥΔΚ υποχρεώνοντας τις Ευρωπαϊκές χώρες να αποδέχονται ψηφιακά υπογεγραμμένα ηλεκτρονικά έγγραφα.
- Οδηγία 1999/93/EC της 13ης Δεκεμβρίου 1999 πάνω στο κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές [EC9993]. Η Οδηγία διευκολύνει την χρήση ηλεκτρονικών υπογραφών στην κοινότητα, συνεισφέρει στην νομική αναγνώρισή τους και εδραιώνει το νομοθετικό πλαίσιο για ηλεκτρονικές υπογραφές και παροχείς υπηρεσιών πιστοποίησης και εξασφαλίζει την κατάλληλη λειτουργία των εσωτερικών αγορών σε στις υπηρεσίες πιστοποίησης και η-υπογραφές. Σύμφωνα με την Οδηγία «... μια προηγμένη ηλεκτρονική υπογραφή μπορεί να εγγυηθεί την αυθεντικότητα της προέλευσης και την ακεραιότητα των [υπογεγραμμένων]περιεχομένων...». Τα κράτη μέλη παρ' όλα αυτά, μπορεί να απαιτήσουν οι προηγμένες ηλεκτρονικές υπογραφές να βασίζονται σε αναγνωρισμένα πιστοποιητικά και να δημιουργούνται με ασφαλή συσκευή υπογραφών, σύμφωνα με το Άρθρο 2 (6) και (10) της Οδηγίας.

- Οδηγία 95/46/EC της 24ης Οκτωβρίου του 1995 για την προστασία προσώπων σε σχέση με τα προσωπικά δεδομένα και την ελεύθερη διακίνηση τέτοιων δεδομένων [EC9546].
- Οδηγία 96/9/EC της 11ης Μαρτίου του 1996 πάνω στην νομική προστασία βάσεων δεδομένων [EC969].
- Οδηγία 97/66/EC της 15ης Δεκεμβρίου του 1997 σχετικά με την επεξεργασία των προσωπικών δεδομένων και την προστασία της ιδιωτικότητας στον τομέα των τηλεπικοινωνιών [EC9766].
- Οδηγία 2002/58/EC της 12ης Ιουλίου του 2002 σχετικά με την επεξεργασία προσωπικών δεδομένων και την προστασία της ιδιωτικότητας στον τομέα των ηλεκτρονικών επικοινωνιών [EC0258].
- Ρύθμιση (EC) 45/2001 της 18ης Δεκεμβρίου του 2000 σχετικά με την προστασία προσώπων σε σχέση με την επεξεργασία προσωπικών δεδομένων απο ινστιτούτα και οργανισμούς της κοινότητας και την ελεύθερη διακίνηση τέτοιων δεδομένων [EC0145].

Οι παραπάνω οδηγίες και ρυθμίσεις επιβάλλουν περιορισμούς, στους οποίους πρέπει να συμμορφώνονται οι υλοποιήσεις η-τιμολόγησης προκειμένου να είναι συμβατές με το κοινοτικό πλαίσιο.

5.2.2.2 Απαιτήσεις ασφάλειας η-τιμολόγησης

Προκειμένου η η-τιμολόγηση να αποτελέσει μέρος των οικονομικών και νομικών πρακτικών ενός οργανισμού, είναι σημαντικό να ικανοποιεί αυστηρές απαιτήσεις ασφάλειας [Kaliontzoglou03]. Η παράγραφος αυτή παρουσιάζει λεπτομερώς τις βασικές απαιτήσεις ασφάλειας, οι οποίες οδήγησαν στην δημιουργία και ενσωμάτωση μιας τέτοιας υπηρεσίας ως υπηρεσία μιας ΑΔΑΑΥ. Η πλειοψηφία των απαιτήσεων αυτών επιβάλλεται απο την Οδηγία 2001/115/EC.

- Η αυθεντικοποίηση προέλευσης εξασφαλίζει ότι οι αποστολείς τιμολογίων είναι πραγματικά αυτοί που ισχυρίζονται. Η αυθεντικοποίηση οντοτήτων εμπλεκόμενων σε μια συναλλαγή η-τιμολογίων είναι απαραίτητη ώστε οι φορολογικές αρχές να μπορούν μοναδικά και οριστικά να αναγνωρίσουν τις οντότητες αυτές.
- Η ακεραιότητα του περιεχομένου των τιμολογίων εξασφαλίζει ότι τα τιμολόγια δεν είναι δυνατόν να μεταβληθούν σκόπιμα ή ακούσια κατά την μεταφορά ή την αποθήκευση.
- Η μη-άρνηση αποστολής και λήψης των τιμολογίων εξασφαλίζει ότι ούτε ο αποστολέας ούτε ο παραλήπτης μπορούν να αρνηθούν ότι η ανταλλαγή του τιμολογίου έχει συμβεί.
- Η μυστικότητα και ιδιωτικότητα εξασφαλίζουν ότι κανένας άλλος εκτός απο τον αποστολέα και τον καθορισμένο παραλήπτη μπορούν να αναγνώσουν το η-τιμολόγιο.
- Η ακεραιότητα στην σειρά των τιμολογίων βοηθά την αποφυγή οποιονδήποτε κενών στη σειριοποίηση των αποστελλόμενων τιμολογίων και στην ενδυνάμωση του ελέγχου απο τον οργανισμό που εκδίδει το τιμολόγιο και τις φορολογικές αρχές.
- Η διαθεσιμότητα εξασφαλίζει ότι οι οργανισμοί μπορούν να χρησιμοποιήσουν μια υπηρεσία η-τιμολόγησης οποιαδήποτε στιγμή χωρίς να υπάρχει διατάραξη των λογιστικών πρακτικών. Απο τη μια πλευρά το σύστημα θα πρέπει να είναι εύρωστο

και προστατευμένο απο εισβολές και απο την άλλη να διαθέτει έναν σταθερό τρόπο δημοσίευσης των υπηρεσιών που υποστηρίζει.
- Οι συνθήκες που σχετίζονται με την ηλεκτρονική αποθήκευση η-τιμολογίων και οι τεχνικές απαιτήσεις του συστήματος αποθήκευσης είναι στοιχειώδη στοιχεία των απαιτήσεων ασφάλειας. Η αυθεντικοποίηση, ακεραιότητα και αναγνωσιμότητα θα πρέπει να εξασφαλίζονται καθ' όλη την διάρκεια αποθήκευσης, σύμφωνα με την Οδηγία.

Οποιαδήποτε υπηρεσία η-τιμολόγησης θα πρέπει να συνοδεύεται απο μια πολιτική ασφάλειας που θα καθορίζει τους περιορισμούς στην παροχή της υπηρεσίας. Επίσης η πολιτική ασφάλειας θα πρέπει να περιέχει την πολιτική υπογραφής (πως και γιατί οι ηλεκτρονικές υπογραφές χρησιμοποιούνται στο πλαίσιο της υπηρεσίας).

5.2.2.3 Υπάρχουσες υλοποιήσεις υπηρεσιών η-τιμολόγησης

Υπάρχουν διάφορες λύσεις η-τιμολόγησης, οι οποίες προσπαθούν να εξασφαλίσουν συμβατότητα με υπάρχουσες οικονομικές εφαρμογές με διάφορους τρόπους, αλλά αποτυγχάνουν στην ικανοποίηση όλων των απαιτήσεων της προηγούμενης παραγράφου [Kaliontzoglou06a]:

- Σε κάποιες λύσεις, τα τιμολόγια αποθηκεύονται και υπόκεινται διαχείριση κεντρικά απο τις εταιρίες που παρέχουν την υπηρεσία τιμολογίων, και άρα υπο μια έννοια δρουν ως Έμπιστες Τρίτες Οντότητες. Κάποιες απο τις εταιρίες αυτές παρέχουν υπηρεσίες μετασχηματισμού απο μια μορφή τιμολογίου σε μια άλλη.
- Τα ηλεκτρονικά τιμολόγια δημιουργούνται απο μια μονάδα μιας ομάδας εφαρμογών που λειτουργεί ο εκδότης των τιμολογίων, ή μέσω κάποιας επιπρόσθετης μονάδας λογισμικού (plug-in) στο ήδη υπάρχον πακέτο λογισμικού, ή ακόμη και με κάποια αυτόνομη διαδικτυακή υπηρεσία η-τιμολόγησης.
- Η ανταλλαγή των η-τιμολογίων επιτυγχάνεται είτε πάνω απο ασφαλείς μισθωμένες γραμμές, ή πάνω απο το διαδίκτυο με χρήση Κωδικών Αυθεντικοποίησης Μηνυμάτων (Message Authentication Code - MAC) και το SSL [Nash01], προκειμένου να διασφαλιστεί η ακεραιότητα, ιδιωτικότητα και αυθεντικοποίηση του καναλιού κατά την διάρκεια της ανταλλαγής των τιμολογίων.
- Κάποιες λύσεις προσπαθούν να επιτύχουν μη-άρνηση της συμμετοχής με χρήση ΥΔΚ και ψηφιακών υπογραφών XML. Κάποιες επιπρόσθετα παρέχουν την δυνατότητα για πρόσβαση σε κεντρικά αποθηκευμένα ιδιωτικά κλειδιά και πιστοποιητικά προκειμένου να υπάρχει ένας τρόπος για ψηφιακή υπογραφή των η-τιμολογίων απο οποιοδήποτε σημείο πρόσβασης.
- Κάποιες λύσεις εμπλέκουν την αποστολή ειδοποιήσεων με ηλεκτρονικό ταχυδρομείο ανάμεσα στους φορείς που ανταλλάσσουν η-τιμολόγια προκειμένου να εκκινήσουν μια χειροκίνητη ανάκτηση των τιμολογίων. Επομένων μειώνουν την πολυπλοκότητα της υποδομής ασφάλειας που απαιτείται απο άλλες προσεγγίσεις, παρέχοντας πρόσβαση σε έναν ασφαλή εξυπηρετητή όπου δημιουργείται το τιμολόγιο.
- Μια μερίδα των λύσεων συμμορφώνεται με το πρότυπο EDI ή παρέχει μεταφραστές γι' αυτό.
- Μια υπηρεσία η-τιμολόγησης βασίζεται στο πρότυπο των Προηγμένων Ηλεκτρονικών Υπογραφών XML ETSI TS 101 903 προκειμένου να επιτύχει την

μακροπρόθεσμη δυνατότητα επαλήθευσης των ηλεκτρονικά υπογεγραμμένων εγγράφων.
- Υπάρχουν αρκετές λύσεις τιμολογίων που δεν μεταφέρουν κάποιο είδος ηλεκτρονικών δεδομένων. Διαχειρίζονται τα δεδομένα των τιμολογίων σε ηλεκτρονική μορφή αφότου όμως έχουν σκανάρει τα τιμολόγια απο το χαρτί [Klein04].

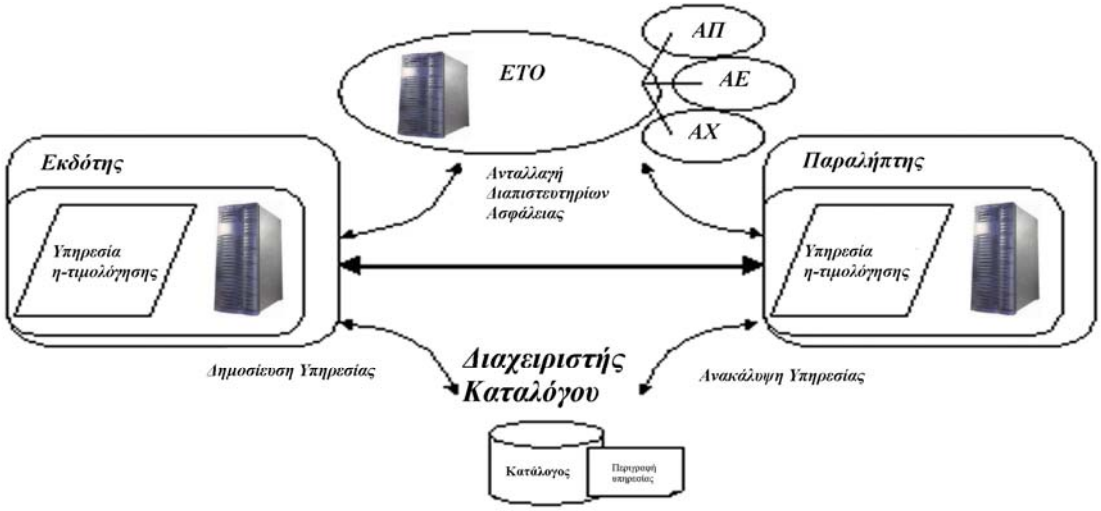
Παρόλο που υπάρχουν συστήματα ηλεκτρονικής τιμολόγησης που χρησιμοποιούν προηγμένες η-υπογραφές, δεν υπάρχουν υλοποιήσεις που εξασφαλίζουν μια εύρωστη και διαλειτουργική παροχή της υπηρεσίας και την ίδια στιγμή κάλυψη των απαιτήσεων ασφάλειας στην ανταλλαγή και διαχείριση των τιμολογίων.
Ένα μέρος των χαρακτηριστικών που προαναφέρθηκαν, καλύπτουν ένα υποσύνολο των απαιτήσεων που αναφέρονται στην Οδηγία, ενώ άλλα δεν καλύπτουν όλες τις απαιτήσεις ασφάλειας. Οι περισσότερες απο τις παραπάνω λύσεις επίσης είναι κλειστές και μη διαλειτουργικές.

5.2.3 Προδιαγραφές ασφαλούς επιχειρησιακής υπηρεσίας η-τιμολόγησης

Η παρούσα παράγραφος έχει στόχο να παρουσιάσει τις προδιαγραφές μιας προηγμένης και καινοτόμου υπηρεσίας η-τιμολόγησης που καλύπτει τις απαιτήσεις για διαλειτουργικότητα και ασφάλεια που προκύπτουν τόσο απο την ανάγκη για ανταλλαγή η-τιμολογίων ανάμεσα σε συναλλασσόμενους οργανισμούς, όσο και απο τις υποδείξεις των σχετικών Ευρωπαϊκών οδηγιών [Kaliontzoglou06c].
Για τον σχεδιασμό της υπηρεσίας χρησιμοποιείται το κατάλληλο υποσύνολο της κατασκευαστικής μεθόδου του κεφαλαίου 5, με γνώμονα το ότι προσπαθούμε να χτίσουμε μια νέα επιχειρησιακή υπηρεσία που θα ενσωματωθεί σε μια υπάρχουσα ΑΔΑΑΥ. Όπως θα δούμε ήδη απο το πρώτο στάδιο που ακολουθεί, η υπηρεσία αυτή όντως καλύπτει τα απαραίτητα κριτήρια ώστε να έχει νόημα η εφαρμογή της μεθοδολογίας για τον σχεδιασμό της. Προτού προχωρήσουμε όμως στον σχεδιασμό, δίνεται η αναλυτική περιγραφή της υπηρεσίας η-τιμολόγησης.

5.2.3.1 Περιγραφή υπηρεσίας

Μια υπηρεσία η-τιμολόγησης έχει βασικό στόχο την διαχείριση και ανταλλαγή μεταξύ οργανισμών **ηλεκτρονικών εγγράφων** που αναπαριστούν **ηλεκτρονικά τιμολόγια**. Ως γνωστόν, ένα τιμολόγιο εκδίδεται απο ένα οργανισμό προκειμένου να χρεώσει έναν δεύτερο οργανισμό για υπηρεσίες ή προϊόντα που του έχει διαθέσει.
Ένα η-τιμολόγιο πρέπει να αποτελεί μια ακριβή αναπαράσταση του χάρτινου τιμολογίου που χρησιμοποιείται σήμερα, και να έχει την δυνατότητα να περιέχει όλους τους τύπους δεδομένων που εμφανίζονται εκεί.
Οι οντότητες που εμπλέκονται στην η-τιμολόγηση φαίνονται στο σχήμα που ακολουθεί:



Σχήμα 5-1 : Μια συναλλαγή η-τιμολόγησης

Οι οντότητες είναι:

- Ο *Εκδότης*, ο οποίος λειτουργεί ένα πληροφοριακό σύστημα που υποστηρίζει μια υπηρεσία η-τιμολόγησης και ακολουθεί τα κατάλληλα βήματα προκειμένου να την δημοσιεύσει σε έναν κατάλογο, ώστε να είναι διαθέσιμη σε άλλους οργανισμούς. Επικοινωνεί με μια ΕΤΟ για να λάβει τα απαραίτητα διαπιστευτήρια ασφάλειας (κλειδιά και πιστοποιητικά).
- Ο *Παραλήπτης*, ο οποίος λειτουργεί ένα πληροφοριακό σύστημα που υποστηρίζει την ίδια υπηρεσία, ή μια εντελώς ανεξάρτητη υπηρεσία η-τιμολόγησης. Στην δεύτερη περίπτωση, είναι απαραίτητο οι δύο υπηρεσίες (του παραλήπτη και του αποστολέα) να υποστηρίζουν τουλάχιστον έναν κοινό τύπο η-τιμολογίου. Ο παραλήπτης πρέπει να έχει λάβει διαπιστευτήρια ασφαλείας απο μια ΕΤΟ και να υπάρχει σε ισχύ διαπίστευση των ΕΤΟ του παραλήπτη και του εκδότη ή οι δυο ΕΤΟ να ταυτίζονται.
- Η *Έμπιστη Τρίτη Οντότητα – ΕΤΟ,* η οποία πρέπει να αποτελείται κατ' ελάχιστο απο μια Αρχή Πιστοποίησης και μια Αρχή Εγγραφής που προσφέρουν υπηρεσίες εγγραφής, πιστοποίησης και ανάκλησης, καθώς και μια Αρχή Χρονοσφράγισης η οποία προσφέρει χρονοσφραγίδες. Πριν λάβει χώρα οποιαδήποτε ασφαλής επικοινωνία, οι συμμετέχοντες οργανισμοί απαιτείται να έχουν εδραιώσει το κατάλληλο πλαίσιο ασφάλειας βασισμένο σε Έμπιστες Τρίτες Οντότητες και ΥΔΚ.
- Ο *Διαχειριστής καταλόγου υπηρεσιών*, ο οποίος λειτουργεί έναν κατάλογο όπου δημοσιεύονται και γίνονται δημοσίως διαθέσιμες οι περιγραφές υπηρεσιών η-τιμολόγησης (ή στην γενική περίπτωση οποιονδήποτε υπηρεσιών).

Οι λειτουργίες που πρέπει να υποστηρίζονται απο την υπηρεσία είναι οι ακόλουθες:

- Σύνθεση, επεξεργασία, υπογραφή και αποθήκευση η-τιμολογίων.
- Ασφαλής ανταλλαγή η-τιμολογίων.

- Διαχωρισμός ρόλων χρηστών οργανισμού σε διοικητικούς (με δυνατότητα σύνθεσης, επεξεργασίας, υπογραφής και αποστολής τιμολογίων) και απλούς χρήστες (με δυνατότητα μόνο σύνθεσης και επεξεργασίας).
- Υποστήριξη διαπιστευτηρίων ΕΤΟ.
- Τα δεδομένα για την σύνθεση και διαχείριση τιμολογίων θα πρέπει να μπορούν να ληφθούν απο ήδη υπάρχοντα συστήματα που έχουν τα απαραίτητα δεδομένα.

Όλες οι παραπάνω λειτουργίες θα πρέπει να επιτελούνται σεβόμενες τις απαιτήσεις ασφάλειας και διαλειτουργικότητας που αντικατοπτρίζονται απο τις Ευρωπαϊκές οδηγίες και περιγράφονται στην παράγραφο 5.2.2.2.

5.2.3.2 1ο Στάδιο: Έλεγχος κριτηρίων ΑΔΑΑΥ

Κατά το πρώτο στάδιο της μεθόδου ελέγχουμε αν η συγκεκριμένη υπηρεσία βάσει της περιγραφής και των απαιτήσεών της όντως εμπίπτει στην κατηγορία επιχειρησιακών υπηρεσιών που έχει νόημα να φιλοξενηθεί σε μια ΑΔΑΑΥ.

5.2.3.2.1 Διαλειτουργικότητα και κλιμάκωση

Η υπηρεσία η-τιμολόγησης έχει ξεκάθαρες απαιτήσεις διαλειτουργικότητας δεδομένου ότι χρειάζεται μια υποδομή επικοινωνίας μεταξύ διαφορετικών οντοτήτων που οφείλουν να «αντιλαμβάνονται» κοινές μορφές δεδομένων αναπαράστασης των η-τιμολογίων. Επιπλέον ο αριθμός οντοτήτων που πρέπει να υποστηρίζει περιορίζεται μόνο απο τον αριθμό των φορέων με τους οποίους ο οργανισμός έχει εμπορικές συναλλαγές. Αυτός μπορεί να κυμαίνεται απο μερικές δεκάδες μέχρι χιλιάδες οντότητες (ανάλογα με το μέγεθος και την φύση των δραστηριοτήτων του οργανισμού), και άρα η υπηρεσία έχει αυξημένες απαιτήσεις κλιμάκωσης.
Στην συγκεκριμένη περίπτωση οι απαιτήσεις που τίθενται είναι υποστήριξη για τουλάχιστον 1000 εταιρίες – πελάτες και 35.000 συναλλαγές ημερησίως, βάσει του γεγονότος ότι απευθύνεται κυρίως σε μικρομεσαίες επιχειρήσεις και όχι μεγάλους οργανισμούς. Η υπηρεσία αυτή δεν χαρακτηρίζεται κρίσιμη οπότε μια απαίτηση για διαθεσιμότητα της τάξεως του 90% θεωρείται κατάλληλη.

5.2.3.2.2 Ασφάλεια και εμπιστοσύνη

Οι απαιτήσεις για ασφάλεια και εμπιστοσύνη προκύπτουν τόσο απο τις επιβολές των Ευρωπαϊκών οδηγιών, όσο και απο την περιγραφή της ίδιας της υπηρεσίας. Όπως περιγράφηκε στην παράγραφο 5.2.2.2 απαιτείται κατ' ελάχιστο η παροχή υπηρεσιών και μηχανισμών που υποστηρίζουν αυθεντικοποίηση προέλευσης δεδομένων και οντοτήτων, ακεραιότητα του περιεχομένου των τιμολογίων, μη-άρνηση αποστολής και λήψης των τιμολογίων, μυστικότητα και ιδιωτικότητα, ακεραιότητα στην σειρά των τιμολογίων, διαθεσιμότητα της υπηρεσίας, και ασφαλή αποθήκευση των τιμολογίων.

5.2.3.2.3 Ανοιχτότητα και κατανομή

Η υπηρεσία η-τιμολόγησης έχει απαιτήσεις ανοιχτότητας όσο αφορά στην διασύνδεση των δομικών της στοιχείων μεταξύ τους καθώς και με τις υπόλοιπες υπηρεσίες που χρειάζεται και πρέπει να παρέχονται απο την αρχιτεκτονική που την φιλοξενεί (όπως π.χ. υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών, ελέγχου πρόσβασης, ενδεχομένως εκτυπώσεων, πρόσβασης σε καταλόγους υπηρεσιών κ.λ.π.). Επίσης είναι σημαντικό να

διευκολύνεται η αλλαγή δομικών στοιχείων της ίδιας της υπηρεσίας χωρίς να επηρεάζεται όσο το δυνατόν η υπηρεσία στο σύνολό της.

5.2.3.2.4 Σεβασμός της αντίληψης του χρήστη

Ο σεβασμός της αντίληψης του χρήστη για την συγκεκριμένη υπηρεσία είναι σημαντική παράμετρος κυρίως ως προς δυο χαρακτηριστικά της. Κατά πρώτον, πρέπει να είναι εξαιρετικά φιλική στις βασικές λειτουργίες σύνθεσης, διαχείρισης και αποστολής η-τιμολογίων. Κατά δεύτερον, θα πρέπει να δίνει στον χρήστη να κατανοεί την εφαρμογή των προηγμένων ηλεκτρονικών υπογραφών που απαιτούνται απο την σχετική Οδηγία (π.χ. να μπορεί ανα πάσα στιγμή να γνωρίζει τι υπογράφει), χωρίς να τον εμπλέκει σε τεχνικές λεπτομέρειες.

5.2.3.2.5 Ελαχιστοποίηση απαιτήσεων κόστους, πόρων - αυτοματοποίηση

Η παραδοσιακή τιμολόγηση είναι μια υπηρεσία που απαιτεί την ύπαρξη των τιμολογίων σε χαρτί. Η η-τιμολόγηση αποτελεί μια χαρακτηριστική περίπτωση ηλεκτρονικής υπηρεσίας που μειώνει το κόστος σε πρώτη φάση λόγω της μείωσης της απαίτησης για ύπαρξη των τιμολογίων σε χάρτινη μορφή. Επίσης η υπηρεσία έχει ως στόχο την αυτοματοποίηση των διαδικασιών παραγωγής και αποστολής τιμολογίων ακόμη και μαζικά.

Σημειώνεται όμως, ότι λόγω των περιορισμών που τίθενται ως προς τις αναγνωρισμένες ηλεκτρονικές υπογραφές (ότι ο υπογράφων θα πρέπει να είναι παρών κατά την παραγωγή της υπογραφής και να βάζει το PIN της έξυπνης κάρτας του), μια τέτοια υπηρεσία δεν θα μπορεί να αυτοματοποιήσει συνολικά την διαδικασία, απο τη στιγμή που ένα τιμολόγιο είναι έτοιμο μέχρι την αποστολή του. Ο ανθρώπινος παράγοντας επιβάλλεται να υπάρχει στη διαδικασία λόγω της νομικής φύσης των υπογραφών

5.2.3.2.6 Ενσωμάτωση υπαρχουσών υποδομών

Όπως διατυπώνεται και στην περιγραφή της υπηρεσίας, είναι θεμιτό να είναι διαθέσιμη η υπάρχουσα πληροφορία για εμπορεύματα, υπηρεσίες και ενδεχομένως πελάτες, που ένας οργανισμός έχει ήδη στην κατοχή του, σε υπάρχοντα πληροφοριακά συστήματα ή βάσεις δεδομένων. Επομένως η υπηρεσία θα πρέπει να δίνει τη δυνατότητα για άντληση των δεδομένων αυτών απο υπάρχουσες υποδομές.

5.2.3.2.7 Σεβασμός στις επιχειρηματικές ανάγκες και τις πολιτικές του οργανισμού

Η υπηρεσία η-τιμολόγησης ενδέχεται να αποτελέσει μια βασική υπο-υπηρεσία που αντιστοιχεί σε μια επιχειρηματική ανάγκη οποιουδήποτε εμπορικού οργανισμού. Επίσης υπάρχει ένα σύνολο πολιτικών και περιορισμών που επιβάλλονται σε αυτή απο το σχετικό κοινοτικό πλαίσιο που πρέπει να σέβονται οι οργανισμοί που δρουν στην Ευρωπαϊκή Ένωση [Kaliontzoglou06b].

Όπως φαίνεται απο τα παραπάνω, το σύνολο των απαιτήσεων της υπηρεσίας η-τιμολόγησης είναι υποσύνολο των απαιτήσεων της ΑΔΑΑΥ όπως παρουσιάζονται στην μεθοδολογία. Άρα αποφαινόμαστε ότι η υπηρεσία η-τιμολόγησης είναι κατάλληλη για ενσωμάτωση σε μια ΑΔΑΑΥ. Η ΑΔΑΑΥ όπως περιγράφηκε στο προηγούμενο κεφάλαιο μπορεί να εμπεριέχει όλες εκείνες τις υπηρεσίες πάνω στις οποίες μπορεί να βασιστεί και

να χρησιμοποιήσει η υπηρεσία η-τιμολόγησης προκειμένου να καλύψει όλες τις απαιτήσεις της Οδηγίας. Στην συνέχεια της ανάλυσης τον προδιαγραφών λοιπόν, θεωρούμε ότι **η υπηρεσία φιλοξενείται σε μια ΑΔΑΑΥ που παρέχει ένα δεδομένο σύνολο υπηρεσιών**. Το ακριβές σύνολο θα προδιαγραφεί στο 3^{ο} στάδιο της μεθόδου, βάσει της περιγραφής της υπηρεσίας και της ανάλυσης των επιχειρησιακών απαιτήσεων και διεργασιών που ακολουθεί (2^{ο} στάδιο).

5.2.3.3 2^{ο} Στάδιο: Ανάλυση επιχειρησιακών απαιτήσεων και διεργασιών

Ακολουθώντας τα βήματα της μεθόδου πρέπει πρώτα να προδιαγράψουμε την επιχειρησιακή όψη της υπηρεσίας η-τιμολόγησης και στη συνέχεια την όψη πληροφορίας.

5.2.3.3.1 Επιχειρησιακή όψη

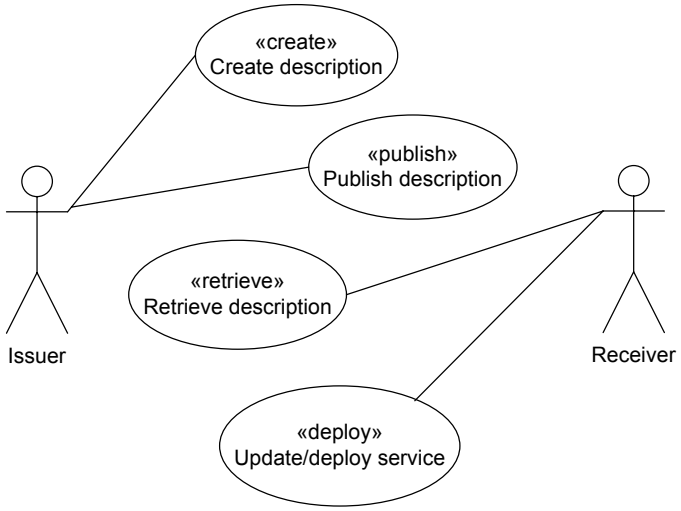
5.2.3.3.1.1 Επιχειρησιακές λειτουργίες και συναρτήσεις

Στην φάση αυτή χρησιμοποιούμε και επεκτείνουμε τα βασικά στοιχεία της παραγράφου 4.3.2.3.3.1.2 για να παράγουμε τα αντίστοιχα διαγράμματα χρήσης της UML που αντικατοπτρίζουν σε υψηλό επίπεδο τις επιχειρησιακές λειτουργίες που παρέχει η υπηρεσία.

Για το λόγο αυτό διαιρούμε την συνολική υπηρεσία σε τέσσερις φάσεις: προ-τιμολόγησης, έκδοσης, αποστολής / λήψης και αποθήκευσης.

5.2.3.3.1.1.1 Φάση προ-τιμολόγησης

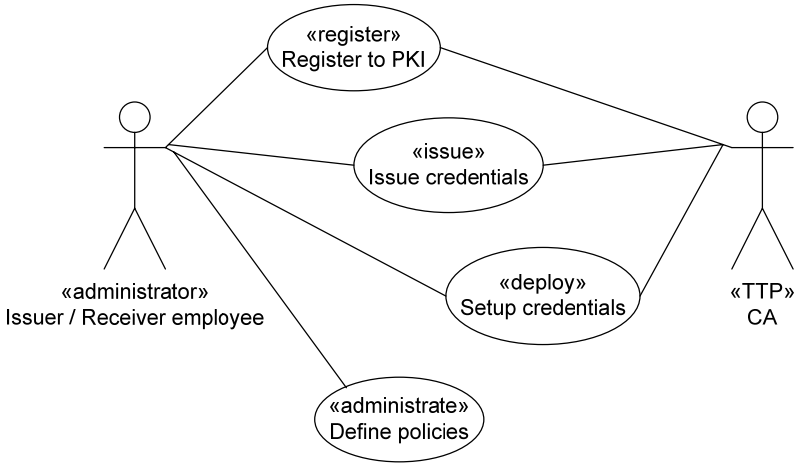
Τα βήματα που λαμβάνουν χώρα στη φάση αυτή περιλαμβάνουν την προαιρετική επικοινωνία με την υπηρεσία καταλόγου για την δημοσίευση και ανάκτηση της περιγραφής της υπηρεσίας απο τον Εκδότη και τον Παραλήπτη αντίστοιχα (βλ. Σχήμα 5-2), καθώς και επικοινωνία με την ΕΤΟ για την απόκτηση διαπιστευτηρίων ασφάλειας (βλ. Σχήμα 5-3).



Σχήμα 5-2. Δημοσίευση και ανάκτηση υπηρεσίας

Κατά την δημοσίευση, ο Εκδότης δημοσιεύει την περιγραφή της υπηρεσίας στον δημόσιο κατάλογο. Ο Παραλήπτης ψάχνει στον κατάλογο και ανακτά την περιγραφή.

Έπειτα διαμορφώνει την υπηρεσία του ώστε να συμμορφώνεται με την περιγραφή αυτή (Σχήμα 5-2).
Προκειμένου να μπορούν να επικοινωνήσουν ασφαλώς, πρέπει και ο Εκδότης και ο Παραλήπτης να συμμετέχουν σε διαδικασίες εγγραφής και πιστοποίησης (Σχήμα 5-3) όπως επιβάλλεται απο το Έγγραφο Πρακτικών Πιστοποίησης της σχετικής ΕΤΟ, για να αποκτήσουν τα απαραίτητα διαπιστευτήρια (κατά πάσα πιθανότητα με τη μορφή μιας έξυπνης κάρτας).



Σχήμα 5-3: Διαδικασία λήψης και εγκατάστασης διαπιστευτηρίων

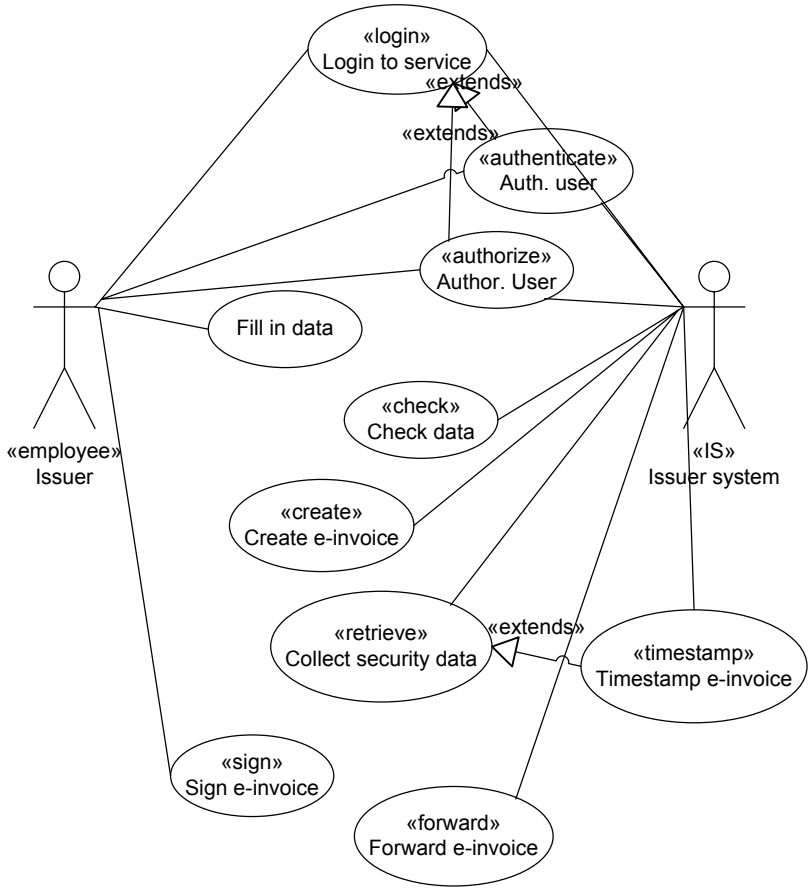
Επιπρόσθετα, είναι σημαντικό οι οργανισμοί να καθορίσουν τις απαραίτητες πολιτικές υπογραφών που θα αναφέρονται κατά την παραγωγή και επαλήθευση προηγμένων υπογραφών, όπως υποδεικνύεται απο τα σχετικά πρότυπα.

5.2.3.3.1.1.2 Φάση έκδοσης η-τιμολογίου

Η διαδικασία η-τιμολόγησης ξεκινά απο τον Εκδότη. Αρχικά αυθεντικοποιείται μέσω της έξυπνης κάρτας του και του PIN μέσα απο την διεπαφή χρήστη. Βάσει των διαπιστευτηρίων ασφάλειας το σύστημα κάνει έναν έλεγχο πρόσβασης.
Η διεπαφή χρήστη επιτρέπει στον χρήστη να δημιουργήσει ένα καινούργιο τιμολόγιο και να συμπληρώσει τα απαραίτητα δεδομένα για την ολοκλήρωση του τιμολογίου ή να διαχειριστεί ήδη υπάρχοντα τιμολόγια (για παράδειγμα τιμολόγια που έχουν ήδη ληφθεί, πρόχειρα κ.λ.π.) Τα δεδομένα ελέγχονται αυτόματα για πιθανά λάθη σύμφωνα με τις ισχύουσες πολιτικές. Σύμφωνα με τα χαρακτηριστικά του χρήστη και τα δικαιώματά του (attributes & privileges) ο χρήστης έχει διαθέσιμες ή όχι τις επιλογές για υπογραφή και αποστολή του η-τιμολογίου. Τα βήματα που διαφανώς επιτελούνται είναι τα ακόλουθα:

- Τα δεδομένα της φόρμας συλλέγονται και χρησιμοποιούνται για να δομηθεί ένα τιμολόγιο.
- Συλλέγονται τα δεδομένα ασφάλειας (π.χ. χρονοσφραγίδες).
- Δημιουργείται η προηγμένη υπογραφή βάσει αυτών των δεδομένων και τα κρυπτογραφικά στοιχεία στην έξυπνη κάρτα.

Η διάκριση ανάμεσα σε τύπους χρηστών παρέχει την ευελιξία που απαιτεί η περιγραφή της υπηρεσίας για τον διαχωρισμό σε υπαλλήλους που απλά παρέχουν δεδομένα και σε διοικητικούς υπαλλήλους υπεύθυνους για την υπογραφή των τιμολογίων.

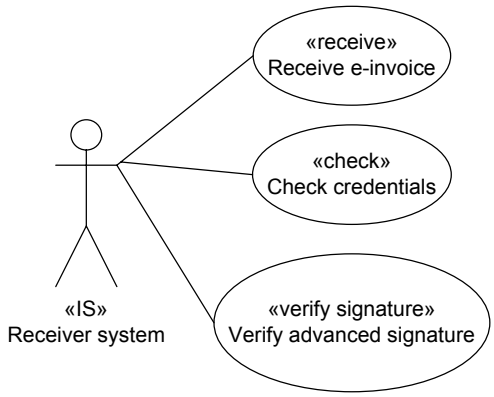


Σχήμα 5-4: Φάση έκδοσης η-τμολογίου

Τα πιστοποιητικά που χρησιμοποιούνται για την υπογραφή και αυθεντικοποίηση μπορεί να είναι διαφορετικά ή τα ίδια, κάτι που καθορίζεται απο την πολιτική ασφάλειας του οργανισμού. Στην περίπτωση που είναι διαφορετικά, στον χρήστη δίνεται η δυνατότητα επιλογής.
Στο τέλος αυτής της φάσης, το η-τιμολόγιο προωθείται για αποστολή στον οργανισμό παραλήπτη.

5.2.3.3.1.1.3 Φάση αποστολής / λήψης η-τιμολογίου

Μετά την επιτυχή δημιουργία της υπογραφής, το η-τιμολόγιο αποστέλλεται με ασφαλή τρόπο σε μια αντίστοιχη υπηρεσία στον οργανισμό παραλήπτη.

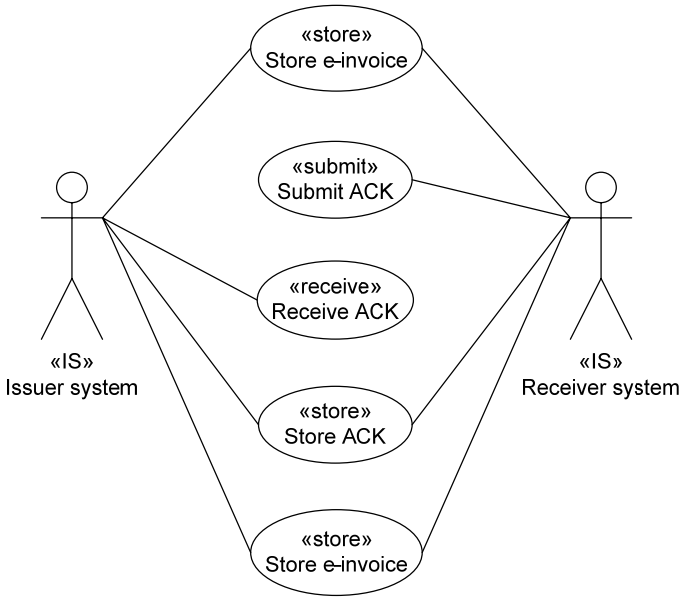


Σχήμα 5-5: Φάση αποστολής / λήψης η-τιμολογίου

Η λήψη του τιμολογίου είναι μια πλήρως αυτοματοποιημένη διαδικασία που δεν απαιτεί την ανθρώπινη παρέμβαση. Εκτελείται η επαλήθευση της κρυπτογραφικής πληροφορίας των διαπιστευτηρίων που χρησιμοποιήθηκαν για την υπογραφή του τιμολογίου, καθώς και οποιασδήποτε χρονοσφραγίδας αυτό περιέχει. Στη συνέχει επαληθεύεται η ίδια η προηγμένη υπογραφή.

5.2.3.3.1.1.4 Φάση αποθήκευσης η-τιμολογίου

Εάν όλες οι επαληθεύσεις της φάσης Γ είναι επιτυχείς, το η-τιμολόγιο αρχικά αποθηκεύεται στην βάση του Παραλήπτη, όπως φαίνεται στο Σχήμα 5-31. Αυτό το καθιστά διαθέσιμο απο οποιαδήποτε εφαρμογή η-τιμολόγησης έχει ο οργανισμός Παραλήπτης. Η διαδικασία ολοκληρώνεται απο την αποστολή μιας απόδειξης πίσω στον εκδότη, που αντικατοπτρίζει το τιμολόγιο που μόλις έχει ληφθεί, και περιλαμβάνει την κατάσταση όλης της διαδικασίας. Όταν η υπηρεσία του Εκδότη λάβει την απόδειξη και την επαληθεύσει, την φυλάει στην δική της βάση μαζί με το αντίστοιχο τιμολόγιο.

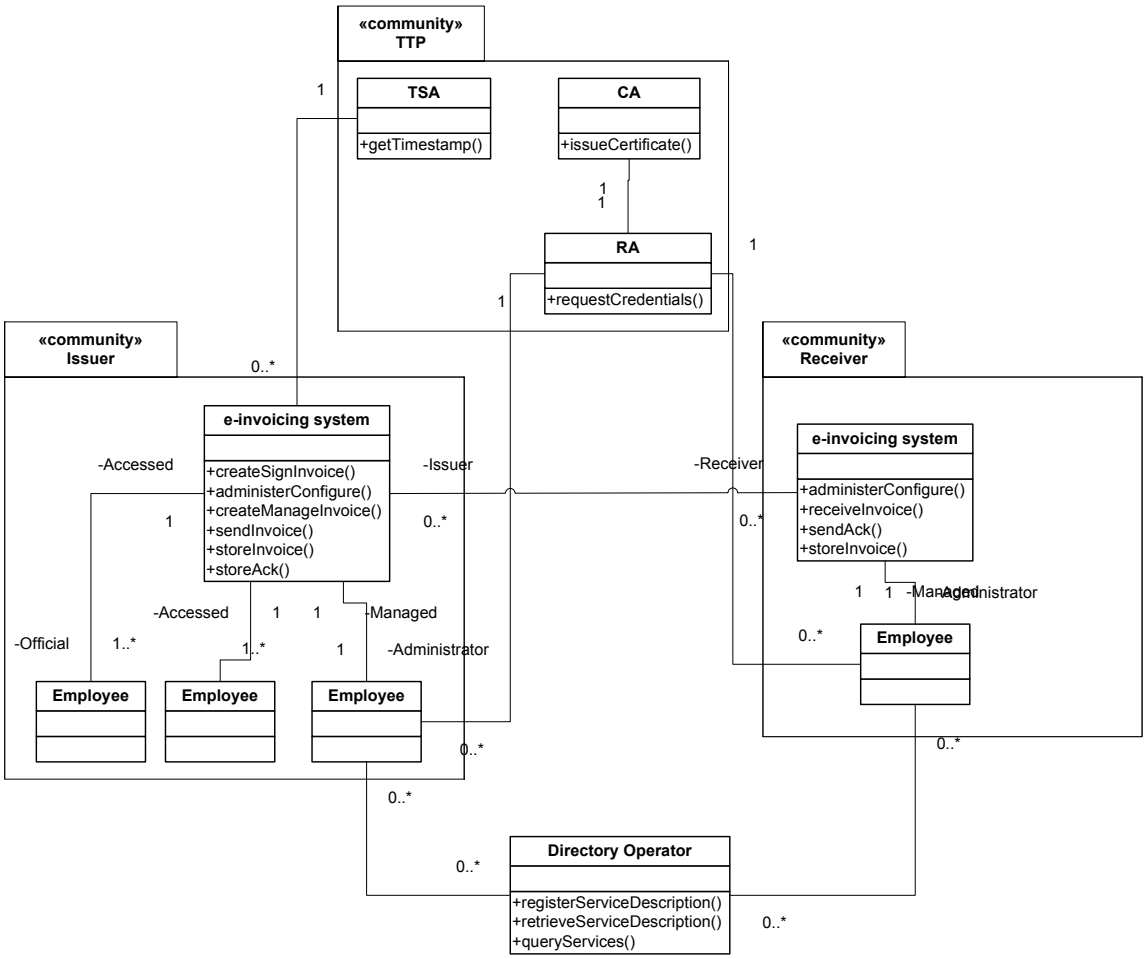


Σχήμα 5-6: Φάση αποθήκευσης η-τιμολογίου

Η πλήρης αυτοματοποίηση της διαδικασία για την μαζική αποστολή τιμολογίων είναι μια απαίτηση που ενδέχεται να υπάρχει απο τον οργανισμό που υιοθετεί την υπηρεσία, αλλά έρχεται εν μέρει σε αντίφαση με την Οδηγία και την εφαρμογή των αναγνωρισμένων προηγμένων υπογραφών. Αυτό είναι ένα ανοιχτό θέμα στην η-τιμολόγηση γενικότερα.

5.2.3.3.1.2 Κοινότητες, ρόλοι και σχέσεις αντικείμενων

Η πλήρης ανάλυση των κοινοτήτων και των ρόλων που ορίζονται ως μέρος των προδιαγραφών για την συγκεκριμένη υπηρεσία φαίνονται στο διάγραμμα συνεργασίας που ακολουθεί:



Σχήμα 5-7: Κοινότητες, ρόλοι και σχέσεις τους για την υπηρεσία η-τιμολόγησης

Το σχήμα περιλαμβάνει όλες τις επιμέρους κοινότητες και αντικείμενα που συμμετέχουν σε μια συναλλαγή που απαιτεί την έκδοση και αποστολή ενός τιμολογίου.
Οι επιμέρους κοινότητες είναι:

- Η κοινότητα *Εκδότης (Issuer)* περιλαμβάνει αντικείμενα με δεδομένους ρόλους που συντελούν στην παραμετροποίηση της υπηρεσίας και την διαχείριση των τιμολογίων. Αυτοί είναι:

- Ο *Υπάλληλος (Employee)*, ο οποίος είναι υπεύθυνος για την δημιουργία και διαχείριση η-τιμολογίων βάσει της υπηρεσίας, αλλά δεν έχει δικαίωμα να υπογράψει και να αποστείλει τιμολόγια. Αποτελεί τον προκαθορισμένο ρόλο στην χρήση της υπηρεσία.
- Ο *Διοικητικός Υπάλληλος (Official)*, ο οποίος αποτελεί έναν υπάλληλο με τον επιπρόσθετο ρόλο να μπορεί να υπογράψει (με χρήση της έξυπνης κάρτας του) και να αποστείλει τιμολόγια.
- Ο *Διαχειριστής (Administrator)* είναι επίσης Υπάλληλος, ο οποίος είναι υπεύθυνος για την αίτηση και λήψη διαπιστευτηρίων απο τις ΕΤΟ και την εγκατάστασή τους στην υπηρεσία, και την συνολική διαχείριση της υπηρεσίας στον Εκδότη. Επίσης είναι υπεύθυνος για την δημοσίευση της υπηρεσία στον κατάλογο υπηρεσιών.
- Το ίδιο το *Σύστημα η-τιμολόγησης (E-Invoicing System)*, που ανταλλάσσει τα κατάλληλα μηνύματα με αντίστοιχες υπηρεσίες σε οργανισμούς Παραλήπτες, προκειμένου να επιτύχει ασφαλείς και ολοκληρωμένες συναλλαγές η-τιμολογίων.

- Η κοινότητα *Παραλήπτης (Receiver)* περιλαμβάνει όλους τους ρόλους σχετικά με την παραμετροποίηση της υπηρεσίας για την ασφαλή λήψη και αποθήκευση η-τιμολογίων. Οι ρόλοι αυτοί είναι:
  - Ο *Διαχειριστής (Administrator)*, ο οποίος είναι υπεύθυνος για την αίτηση και λήψη διαπιστευτηρίων απο τις ΕΤΟ και την εγκατάστασή τους στην υπηρεσία, και την συνολική διαχείριση της υπηρεσίας στον Παραλήπτη. Επίσης είναι υπεύθυνος για την ανάκτηση της περιγραφής μιας υπηρεσίας η-τιμολόγησης απο κατάλογο υπηρεσιών και παραμετροποίησης του συστήματος του Παραλήπτη για διαλειτουργική επικοινωνία.
  - Το *Σύστημα η-τιμολόγησης (E-Invoicing System)*, που ανταλλάσσει τα κατάλληλα μηνύματα με αντίστοιχες υπηρεσίες σε οργανισμούς Εκδότες, προκειμένου να επιτύχει ασφαλείς και ολοκληρωμένες συναλλαγές η-τιμολογίων.
- Η *Κοινότητα ΕΤΟ (TTP)* περιλαμβάνει τους οργανισμούς που υποστηρίζουν ΥΔΚ και προσφέρουν κατ' ελάχιστο τις υπηρεσίες πιστοποίησης και χρονοσφράγισης (σύμφωνα με τις απαιτήσεις της υπηρεσίας). Ο ρόλοι που εμπεριέχει είναι λοιπόν:
  - Μια ΑΠ (CA), με όλες τα χαρακτηριστικά περιγράφονται στο Παράρτημα.
  - Μια ΑΕ (RA), με όλες τα χαρακτηριστικά που περιγράφονται στο Παράρτημα.
  - Μια Αρχή Χρονοσφράγισης (TSA), η οποία μπορεί να παράγει χρονοσφραγίδες για έγγραφα με βάσει μια έμπιστη πηγή χρόνου.

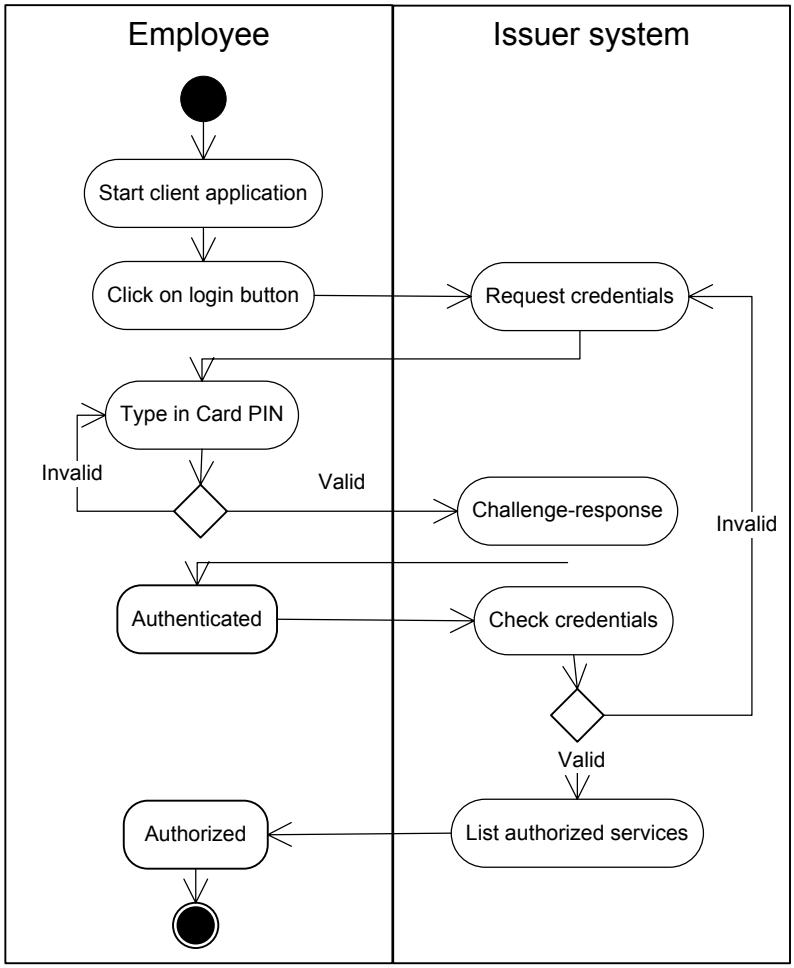
Οι παραπάνω κοινότητες συμπληρώνονται απο τον ρόλο του *Διαχειριστή Καταλόγου (Directory Operator)*, ο οποίος διαχειρίζεται τα δημόσια δεδομένα περιγραφών υπηρεσιών.
Όπως φαίνεται στο διάγραμμα και ορίζεται απο την μεθοδολογία, οι κοινότητες έχουν το στερεότυπο «Community» και οι ρόλοι αναπαρίστανται με κλάσεις της UML, συμπεριλαμβανομένου κάποιων βασικών στοιχείων όψης που έχουν χρησιμοποιηθεί.

5.2.3.3.1.3 Διεργασίες

Οι διεργασίες που περιλαμβάνονται στην φάση προ-τιμολόγησης και περιγράφονται στην παράγραφο 5.2.3.3.1.1 δεν χρήζουν περαιτέρω ανάλυσης γιατί αποτελούν οργανωτικές διαδικασίες και δεν αποτελούν εγγενείς διαδικασίες της υπηρεσίας που σχεδιάζεται. Επίσης σχετίζονται με την υπάρχουσα υποδομή που θα φιλοξενήσει την υπηρεσία (ως προς τον τρόπο παραμετροποίησής της και εγκατάστασης της υπηρεσίας), καθώς και τις υποδομές των Έμπιστων Τρίτων Οντοτήτων που συμμετέχουν.
Ως μέρος των προδιαγραφών της παρούσας παραγράφου θα δοθούν οι διεργασίες που λαμβάνουν χώρα στις τρεις υπόλοιπες φάσεις της η-τιμολόγησης.

5.2.3.3.1.3.1 Φάση έκδοσης η-τιμολογίου

Αρχικά, αναλύουμε περαιτέρω το διάγραμμα περιπτώσεων χρήσης στο Σχήμα 5-4 χωρίζοντάς το στη *διεργασία αυθεντικοποίησης και ελέγχου πρόσβασης* και στη *διεργασία συμπλήρωσης στοιχείων και υπογραφής*. Η διεργασία αυθεντικοποίησης και ελέγχου φαίνεται στο ακόλουθο σχήμα:

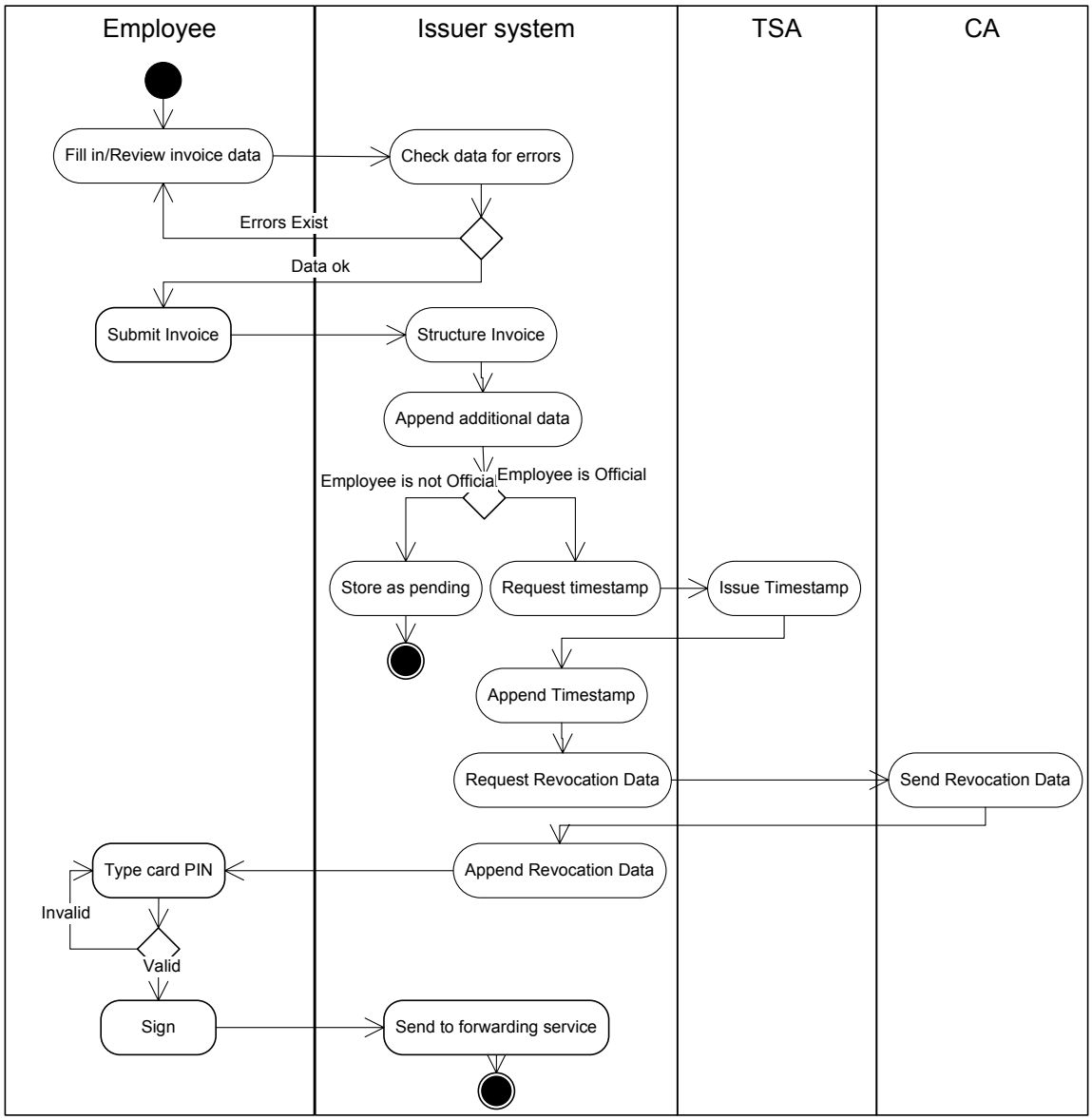


Σχήμα 5-8: Διεργασία αυθεντικοποίησης και ελέγχου πρόσβασης υπαλλήλου στον εκδότη

Κατά τη διεργασία αυτή, ο Υπάλληλος εκκινεί την εφαρμογή που του επιτρέπει είσοδο στην υπηρεσία. Μέσω της υπηρεσίας ελέγχου πρόσβασης γίνονται τα εξής:

1. Ζητούνται τα διαπιστευτήρια του χρήστη.
2. Ο χρήστης εισάγει το PIN για πρόσβαση στα διαπιστευτήρια.
3. Εάν η πρόσβαση είναι επιτυχής, διενεργείται ένα πρωτόκολλο πρόκλησης-απάντησης.
4. Εάν είναι επιτυχές, ο χρήστης θεωρείται αυθεντικοποιημένος.
5. Ελέγχονται τα διαπιστευτήρια σε σχέση με τις ισχύουσες πολιτικές πρόσβασης.
6. Εάν ο έλεγχος είναι επιτυχής, ο χρήστης αποκτά πρόσβαση σε ο,τι είναι διαθέσιμο βάσει των διαπιστευτηρίων του και της πολιτικής.

Εφόσον σύμφωνα με το διάγραμμα ρόλων της προηγούμενης παραγράφου, ο Διοικητικός Υπάλληλος είναι επίσης Υπάλληλος (η κλάση Υπάλληλος αποτελεί γενίκευση), ακολουθεί επίσης την ίδια διαδικασία εισαγωγής στο σύστημα, αλλά του αποδίδονται διαφορετικά δικαιώματα. Το ίδιο ισχύει για τον Διαχειριστή.
Στη συνέχεια εκτελείται η διεργασία συμπλήρωσης και υπογραφής, όπως φαίνεται στο Σχήμα 5-9:



Σχήμα 5-9: Διεργασία συμπλήρωσης και υπογραφής

Τα βήματα της διεργασίας είναι τα ακόλουθα:

1. Ο Υπάλληλος είτε ελέγχει και μεταβάλλει τα στοιχεία ενός υπάρχοντος τιμολογίου (προς αποστολή) είτε δημιουργεί ένα νέο και συμπληρώνει τα στοιχεία του.
2. Το σύστημα ελέγχει παράλληλα τα δεδομένα για λάθη (π.χ. λάθος τύπος πληροφορίας, υποχρεωτικά πεδία που είναι κενά κ.λ.π.). Όσο υπάρχουν λάθη ο Υπάλληλος τα διορθώνει.
3. Όταν δεν υπάρχον λάθη, το τιμολόγιο δομείται σύμφωνα με τα ληφθέντα στοιχεία και επιπλέον στοιχεία που ίσως χρειάζονται απο μια βάση δεδομένων ή μια υπάρχουσα υποδομή (υπάρχον πληροφοριακό σύστημα).
4. Εάν ο Υπάλληλος δεν είναι Διοικητικός, το τιμολόγιο αποθηκεύεται.

5. Εάν ο Υπάλληλος είναι Διοικητικός, τότε ζητείται μια χρονοσφραγίδα για το η-τιμολόγιο απο την Αρχή χρονοσφράγισης, και αυτή ενσωματώνεται στο τιμολόγιο.
6. Επίσης ζητούνται τα κατάλληλα δεδομένα ελέγχου κατάστασης των διαπιστευτηρίων απο την Αρχή Πιστοποίησης, και ενσωματώνονται επίσης στο τιμολόγιο.
7. Τέλος, ζητείται απο τον Διοικητικό Υπάλληλο να εισάγει το PIN του για την κάρτα, προκειμένου να υλοποιηθεί προηγμένη ηλεκτρονική υπογραφή στα δεδομένα. Μόλις η υπογραφή είναι επιτυχής, το η-τιμολόγιο αποστέλλεται στην υπηρεσία προώθησης.

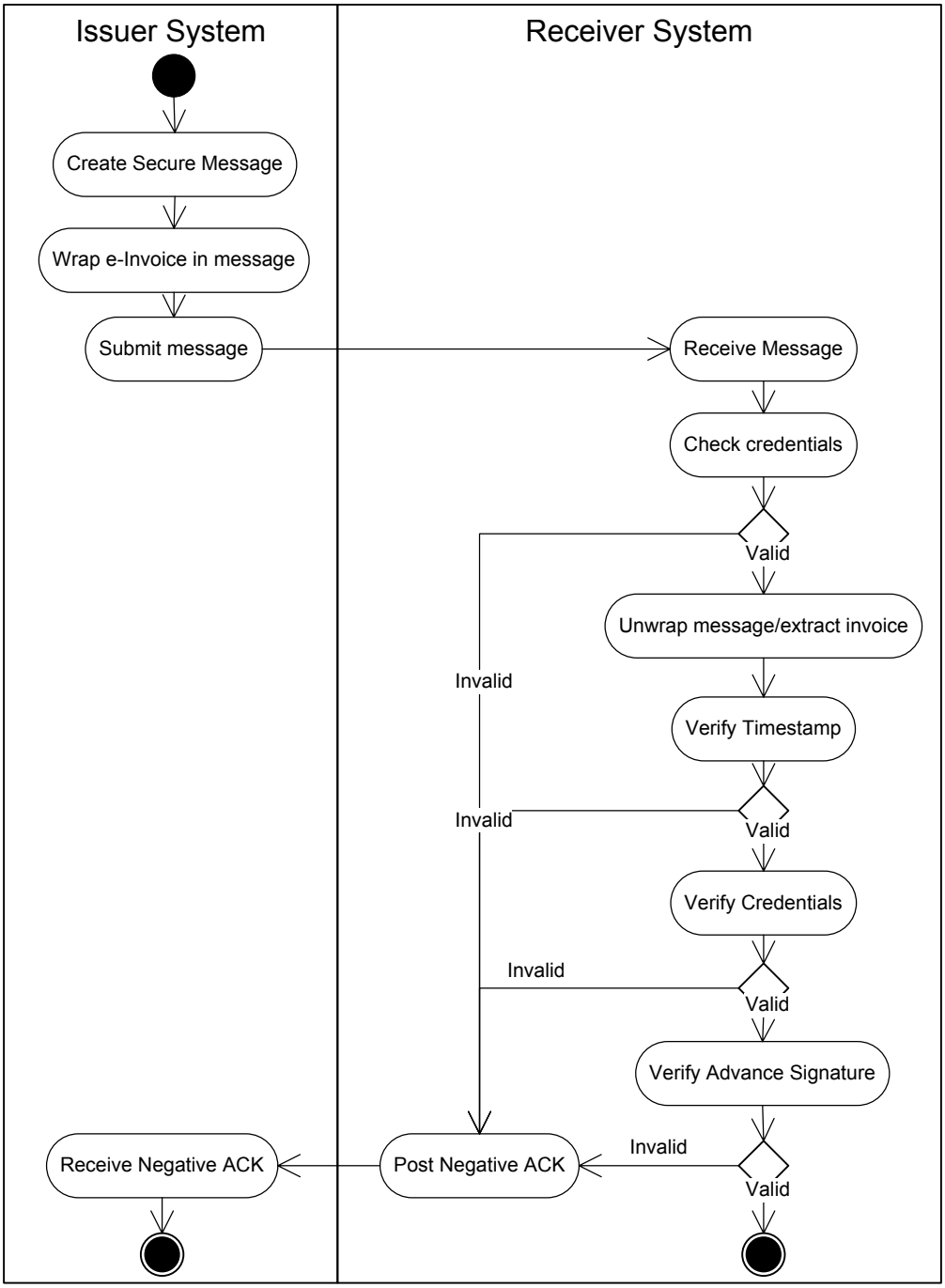
Όπως φαίνεται ήδη απο την παραπάνω ανάλυση, η υπηρεσία η-τιμολόγησης απαιτεί την επικοινωνία με ένα υποσύνολο των υπηρεσιών της ΑΔΑΑΥ που θα πρέπει να την φιλοξενήσει. Οι προδιαγραφές της επιχειρησιακής όψης υποδεικνύουν ποιες είναι αυτές οι υπηρεσίες που θα επιλεγούν στο επόμενο στάδιο της μεθόδου ως προαπαιτούμενες.

5.2.3.3.1.3.2 Φάση αποστολής / λήψης η-τιμολογίου

Η φάση αυτή αναλύεται με μια διεργασία η οποία αντιστοιχεί στο διάγραμμα περιπτώσεων χρήσης (που έχει ήδη αναπαρασταθεί στο Σχήμα 5-5). Απο την πλευρά του Εκδότη η διεργασία επί της ουσίας περιλαμβάνει την δημιουργία ενός κατάλληλου ασφαλούς μηνύματος προς αποστολή, το οποίο περιλαμβάνει το η-τιμολόγιο που έχει παραχθεί.
Όπως φαίνεται στο Σχήμα 5-10, όταν το σύστημα του Παραλήπτη λάβει το μήνυμα αυτό, το πρώτο βήμα είναι να ελέγχει τα διαπιστευτήρια του ίδιου του μηνύματος. Εάν αυτά είναι έγκυρα, τότε το εξάγεται το ίδιο το η-τιμολόγιο απο το μήνυμα. Στη συνέχεια διενεργούνται τρεις βασικοί έλεγχοι για την προηγμένη ηλεκτρονική υπογραφή:

1. Η εγκυρότητα της χρονοσφραγίδας που περιέχει.
2. Η εγκυρότητα των διαπιστευτηρίων που χρησιμοποιήθηκαν για την παραγωγή της υπογραφής των τιμολογίων, σε σχέση με το χρόνο που υποδηλώνει η χρονοσφραγίδα.
3. Η εγκυρότητα της ίδιας της υπογραφής.

Εάν κάποιος απο όλους τους παραπάνω ελέγχους αποτύχει, τότε στον Εκδότη αποστέλλεται μια αρνητική επιβεβαίωση με την αιτιολογία της απόρριψης.



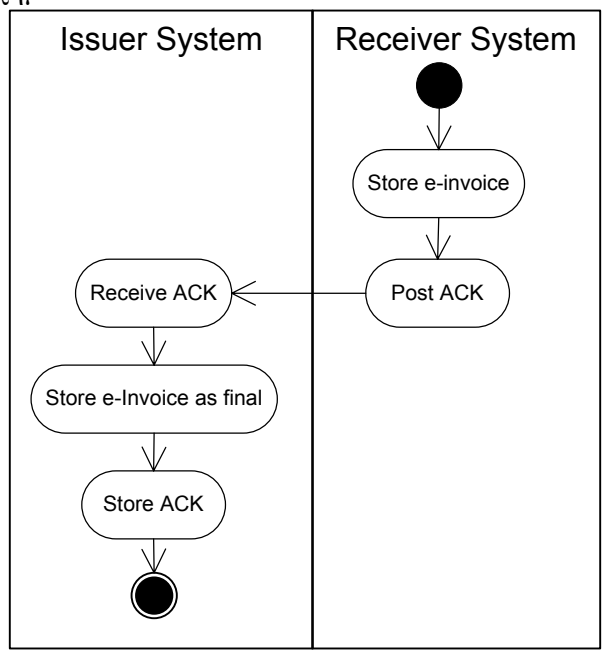
Σχήμα 5-10: Διεργασία αποστολής και λήψης του η-τιμολογίου

Εάν αντίθετα, όλοι οι έλεγχοι είναι επιτυχείς, τότε η διαδικασία προχωράει κανονικά στην επόμενη φάση, αυτή της αποθήκευσης του η-τιμολογίου.

5.2.3.3.1.3.3 Φάση αποθήκευσης η-τιμολογίου

Η τελική φάση αντικατοπτρίζεται σε μια απλή διεργασία που περιλαμβάνει τα βήματα της αποθήκευσης του τιμολογίου απο τον Παραλήπτη και της δημιουργίας ενός θετικού

μηνύματος επιβεβαίωσης, το οποίο αποστέλλεται απο τον Παραλήπτη στον Εκδότη, όπως φαίνεται στο Σχήμα 5-11:



Σχήμα 5-11: Διεργασία αποθήκευσης η-τιμολογίου

Μόλις ο Εκδότης λάβει την επιβεβαίωση, προχωρά επίσης στην αποθήκευση τόσο της τελικής μορφής του τιμολογίου, όσο και της ίδιας της επιβεβαίωσης, για οποιαδήποτε μελλοντική χρήση.

5.2.3.3.1.4 Πολιτικές

Οι πολιτικές / περιορισμοί που θα πρέπει να βρίσκονται σε ισχύ για την υπηρεσία η-τιμολόγησης είναι οι ακόλουθες:

- Το η-τιμολόγιο θα πρέπει να εμπεριέχει την ελάχιστη ποσότητα και είδος πληροφορίας που απαιτείται απο την Οδηγία.
- Η δομή του η-τιμολογίου θα πρέπει να βασίζεται σε όσο το δυνατόν περισσότερα διαδεδομένα πρότυπα του χώρου του η-επιχειρείν.
- Η δομή του η-τιμολογίου θα πρέπει να είναι ορισμένη σε XML.
- Η υπηρεσία θα πρέπει να κάνει χρήση πιστοποιητικών X.509 αποθηκευμένων σε κάρτες για τις ηλεκτρονικές υπογραφές, είτε αυτόνομα είτε μέσω μιας κατάλληλης υπηρεσίας μιας ΑΔΑΑΥ.
- Η υπηρεσία θα πρέπει να χρησιμοποιεί προηγμένες ηλεκτρονικές υπογραφές για την υπογραφή των η-τιμολογίων.
- Η υπηρεσία θα πρέπει να υποστηρίζει την σύνθεση, επεξεργασία, υπογραφή, αποθήκευση και ασφαλή ανταλλαγή τιμολογίων.
- Η υπηρεσία θα πρέπει να ικανοποιεί όλες τις απαιτήσεις ασφάλειας της Οδηγίας για αυθεντικοποίηση προέλευσης και αυθεντικοποίηση οντοτήτων, ακεραιότητα του περιεχομένου των τιμολογίων, μη-άρνηση αποστολής και λήψης των τιμολογίων,

μυστικότητα και ιδιωτικότητα, ακεραιότητα στην σειρά των τιμολογίων, διαθεσιμότητα και ασφαλή αποθήκευση.

- Η υπηρεσία θα πρέπει να υποστηρίζει τον διαχωρισμό ρόλων των χρηστών σε διοικητικούς (με δυνατότητα σύνθεσης, επεξεργασίας, υπογραφής και αποστολής η-τιμολογίων) και σε απλούς εργαζόμενους (με δυνατότητα σύνθεσης, επεξεργασίας και προσωρινής αποθήκευσης).
- Τα δεδομένα για την σύνθεση και διαχείριση τιμολογίων θα μπορούν να ληφθούν απο υπάρχοντα συστήματα μέσω υπηρεσιών υποστήριξης υπαρχουσών υποδομών που πρέπει να φιλοξενεί η ΑΔΑΑΥ που θα υποστηρίξει και την υπηρεσία η-τιμολόγησης.

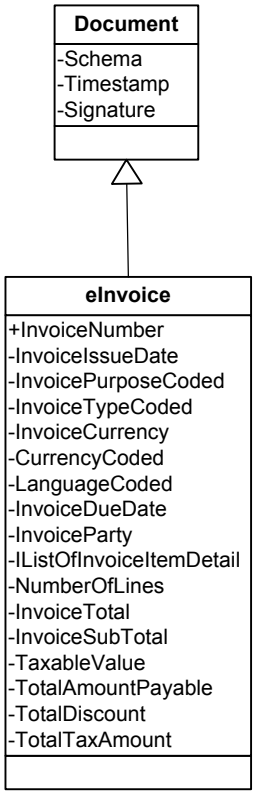
5.2.3.3.2 Όψη πληροφορίας

Στην παρούσα παράγραφο, παρατίθενται όλα τα αντικείμενα πληροφορίας που υπάρχουν στην υπηρεσία η-τιμολόγησης και είτε δημιουργούνται και μεταφέρονται προκειμένου να επιτελεστούν οι διεργασίες που έχουν ήδη περιγραφεί, είτε επηρεάζουν την υπηρεσία κατά τη διάρκεια της ζωής τους. Ως μέρος της όψης προδιαγράφονται τα σταθερά και δυναμικά σχήματα των αντικείμενων αυτών. Όπου είναι δυνατό, χρησιμοποιούνται και επεκτείνονται τα βασικά στοιχεία της όψης, όπως έχουν παρουσιαστεί στο κεφάλαιο 4.3.2.4.3.1.2.

5.2.3.3.2.1 Το η-τιμολόγιο

5.2.3.3.2.1.1 Σταθερό σχήμα

Το ηλεκτρονικό τιμολόγιο είναι μια μορφή ηλεκτρονικού εγγράφου. Επομένως αποτελεί επέκταση του βασικού στοιχείου Έγγραφο, της παραγράφου 4.3.2.4.3.1.2.1. Το σταθερό σχήμα του τιμολογίου φαίνεται στο ακόλουθο σχήμα:



Σχήμα 5-12: Σταθερό σχήμα η-τιμολογίου

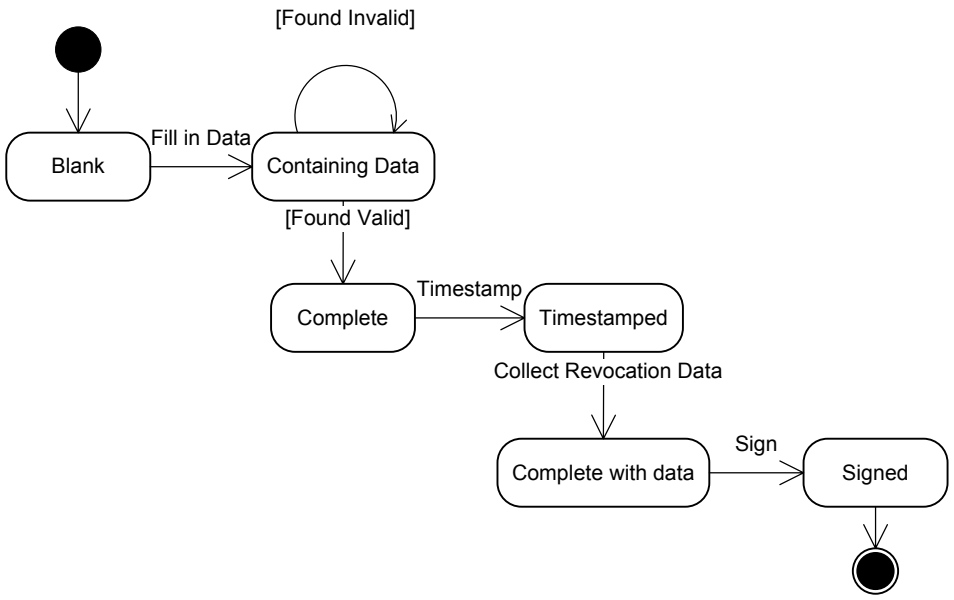
Το βασικό στοιχείο Έγγραφο έχει επεκταθεί με ένα σύνολο πεδίων που πρέπει να περιέχονται σε κάθε τιμολόγιο. Όπως κάθε Έγγραφο ένα η-τιμολόγιο περιγράφεται απο ένα σχήμα. Προκειμένου να διασφαλιστεί η διαλειτουργικότητα μεταξύ διαφορετικών υπηρεσιών η-τιμολόγησης, είναι απαραίτητο η υπηρεσία να υποστηρίζει ορισμένα συγκεκριμένα σχήματα XML που καθορίζουν επακριβώς το περιεχόμενο ενός η-τιμολογίου. Πρότυπα που μπορούν να χρησιμοποιηθούν γι' αυτό το σκοπό είναι τα ακόλουθα:

- Η XML Common Business Library έκδοση 4.0 (xCBL 4.0) [xCBL03]
- Το πρότυπο electronic Business Interchange using XML (eBis-XML suite) [BASDA] του οργανισμού Business Application Software Developers Association (BASDA)
- Η Universal Business Language (UBL) [UBL1.0] του OASIS
- Οι προδιαγραφές του Open Applications Group Integration (OAGIS) [Rowell02]

Όσο περισσότερα απο τέτοιου τύπου πρότυπα υποστηρίζονται κατά την παραγωγή η-τιμολογίων τόσο περισσότερο αυξάνεται το επίπεδο διαλειτουργικότητας της υπηρεσίας.

5.2.3.3.2.1.2 Δυναμικό σχήμα

Το δυναμικό σχήμα του η-τιμολογίου αποτελεί μια επέκταση του δυναμικού σχήματος ενός Εγγράφου, όπως φαίνεται στο επόμενο σχήμα:



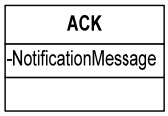
Σχήμα 5-13: Δυναμικό σχήμα η-τιμολογίου

Προκειμένου να τηρούνται οι απαιτήσεις απο την Οδηγία, το η-τιμολόγιο πρέπει να υπογραφεί με προηγμένη υπογραφή. Άρα εκτός απο την χρονοσφραγίδα πρέπει να του προστεθούν και τα δεδομένα ανάκλησης των σχετικών διαπιστευτηρίων σε σχέση με τον χρόνο που υποδηλώνει η χρονοσφραγίδα, και έπειτα να τελεστεί η υπογραφή.

5.2.3.3.2.2 Μήνυμα επιβεβαίωσης

5.2.3.3.2.2.1 Σταθερό σχήμα

Το Μήνυμα Επιβεβαίωσης αποτελεί μια μορφή του βασικού στοιχείου Ειδοποίηση, όπως έχει προδιαγραφεί στην παράγραφο 4.3.2.4.3.1.2.1, επομένως έχει το ίδιο σταθερό σχήμα.

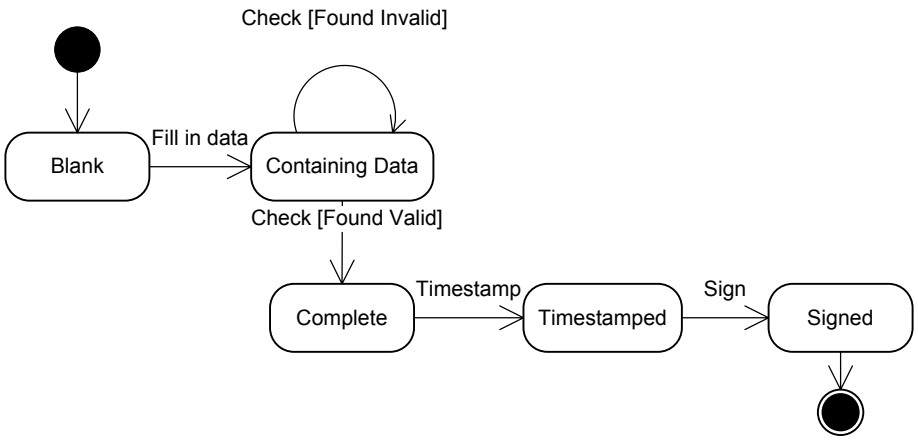


Σχήμα 5-14: Σταθερό σχήμα Μηνύματος Επιβεβαίωσης

Το μήνυμα που του αποδίδεται κάθε φορά έχει να κάνει με το είδος της επιβεβαίωσης θέλουμε να αποσταλεί απο τον Παραλήπτη στον εκδότη, όπως περιγράφηκε στις διεργασίες αποστολής / λήψης και αποθήκευσης του η-τιμολογίου στις παραγράφους 5.2.3.3.1.3.2 και 5.2.3.3.1.3.3 αντίστοιχα.

5.2.3.3.2.2.2 Δυναμικό σχήμα

Το δυναμικό σχήμα του αντικειμένου είναι ίδιο με το σχήμα του βασικού στοιχείου Ειδοποίηση (και του Εγγράφου, απο το οποίο παράγεται η Ειδοποίηση):



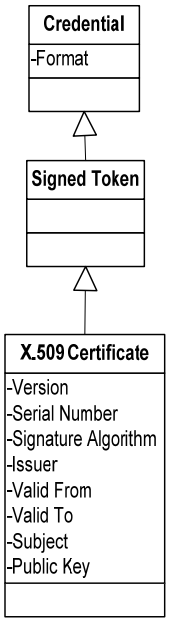
Σχήμα 5-15: Δυναμικό σχήμα Μηνύματος Επιβεβαίωσης

Σημειώνεται ότι το συγκεκριμένο αντικείμενο πληροφορίας δεν έχει απαίτηση για προηγμένη ηλεκτρονική υπογραφή, όποτε μια απλή ψηφιακή υπογραφή καλύπτει τις απαιτήσεις ασφάλειας του.

5.2.3.3.2.3 Διαπιστευτήριο

5.2.3.3.2.3.1 Σταθερό σχήμα

Στην προκειμένη περίπτωση, τα διαπιστευτήρια που θα χρησιμοποιηθούν στην υπηρεσία θα αποτελούν υπογεγραμμένες οντότητες και θα υπακούουν στο πρότυπο X.509. Οπότε επεκτείνουμε κατάλληλα το βασικό στοιχείο της παραγράφου 4.3.2.4.3.1.2.2 για να λάβουμε το αντίστοιχο σταθερό σχήμα:

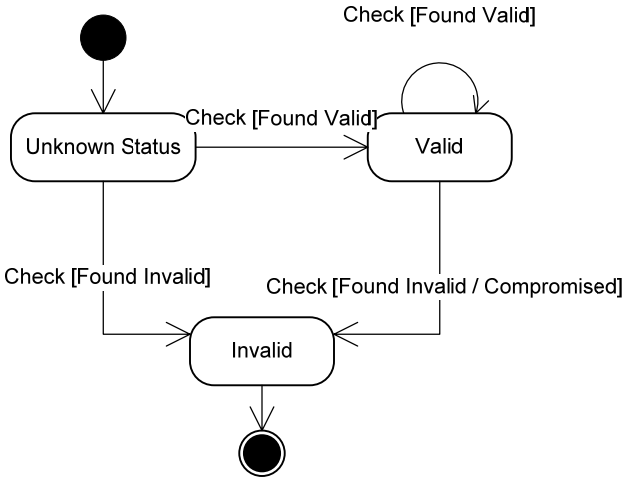


Σχήμα 5-16: Σταθερό σχήμα Διαπιστευτηρίου

Στο αντικείμενο πληροφορίας έχει επεκταθεί με το σύνολο των πεδίων που προδιαγράφονται απο το πρότυπο X.509, όπως έχει περιγραφεί ήδη στο παράδειγμα της παραγράφου 4.3.2.4.3.1.3.

5.2.3.3.2.3.2 Δυναμικό σχήμα

Το δυναμικό σχήμα του αντικειμένου είναι ίδιο με το δυναμικό σχήμα που προδιαγράφεται για το Διαπιστευτήριο στην παράγραφο 4.3.2.4.3.3.2.2:



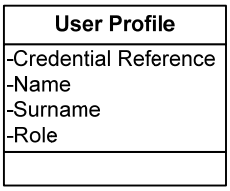
Σχήμα 5-17: Δυναμικό σχήμα Διαπιστευτηρίου

Όπως και το βασικό στοιχείο όψης, το αντικείμενο περνάει απο τις διάφορες καταστάσεις σε σχέση με την εγκυρότητά του.

5.2.3.3.2.4 Προφίλ χρήστη

5.2.3.3.2.4.1 Σταθερό σχήμα

Το σταθερό σχήμα για το προφίλ χρήστη που θα χρησιμοποιηθεί στην υπηρεσία η-τιμολόγησης αποτελεί μια επέκταση του σταθερού σχήματος του βασικού στοιχείου όψης της παραγράφου 4.3.2.4.3.1.2.3, όπως φαίνεται στο ακόλουθο σχήμα:

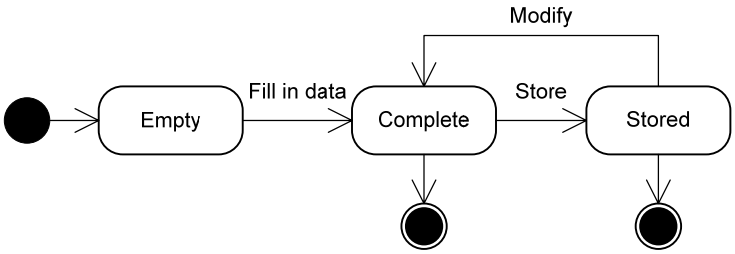


Σχήμα 5-18: Σταθερό σχήμα Προφίλ χρήστη

Η επέκταση περιλαμβάνει τα πεδία Όνομα (Name), Επώνυμο (Surname) και Ρόλος (Role), που θα χρησιμοποιηθούν απο την υπηρεσία προκειμένου να κα γνωρίζει στοιχεία που της χρησιμεύουν για έναν χρήστη που έχει ήδη αυθεντικοποιηθεί.

5.2.3.3.2.4.2 Δυναμικό σχήμα

Το δυναμικό σχήμα του αντικειμένου είναι ίδιο με το δυναμικό σχήμα που προδιαγράφεται για το Προφίλ Χρήστη στην παράγραφο 4.3.2.4.3.3.2.3:



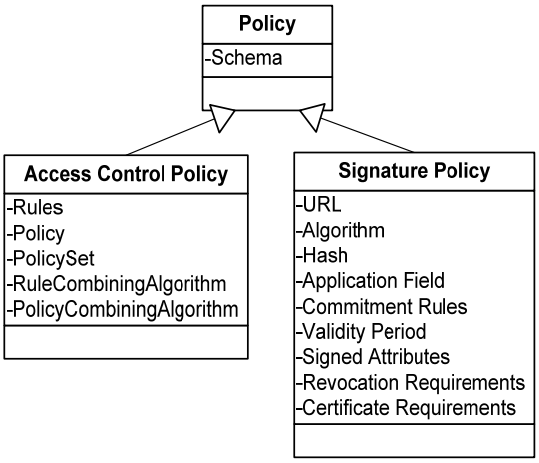
Σχήμα 5-19: Δυναμικό σχήμα Προφίλ χρήστη

Όπως και το βασικό στοιχείο όψης, το αντικείμενο συμπληρώνεται με τα στοιχεία του χρήστη κατά την δημιουργία του και ενημερώνεται αν αυτά αλλάξουν. Σε οποιαδήποτε περίπτωση, κάθε φορά αποθηκεύεται στο σύστημα.

5.2.3.3.2.5 Πολιτική

5.2.3.3.2.5.1 Σταθερό σχήμα

Η περιγραφή της υπηρεσίας και οι πολιτικές της Επιχειρησιακής Όψης επιβάλλουν τον ορισμό δύο ειδών πολιτικών, μιας Πολιτικής Ελέγχου Πρόσβασης και μιας Πολιτικής Υπογραφής. Χρησιμοποιούνται τα ακόλουθα σταθερά σχήματα για τα είδη των πολιτικών, που προκύπτουν απο το βασικό στοιχείο όψης της παραγράφου 4.3.2.4.3.1.2.4:



Σχήμα 5-20: Σταθερό σχήμα για τις Πολιτικές της υπηρεσίας

Η πολιτική ελέγχου πρόσβασης θα χρησιμοποιηθεί απο την υπηρεσία της αρχιτεκτονικής που φιλοξενεί την υπηρεσία η-τιμολόγησης προκειμένου να αποφανθεί αν ο χρήστης δικαιούνται πρόσβαση στο σύστημα και ποιες υπηρεσίες μπορεί να χρησιμοποιήσει. Αποτελείται απο διάφορους κανόνες και επιμέρους πολιτικές (Rules, Policies, Policy Sets) τα οποία συνδυάζονται βάσει συνδυαστικών αλγορίθμων (RuleCombiningAlgorithm, PolicyCombiningAlgorithm) προκειμένου να ληφθούν αποφάσεις ελέγχου πρόσβασης πάνω σε πόρους.

Στην συγκεκριμένη υπηρεσία θα υπάρχει ένα Σύνολο Πολιτικών (PolicySet) με δυο Πολιτικές (Policy), μια για κάθε ρόλο χρήστη που σχετίζεται άμεσα με την συγκεκριμένη υπηρεσία:

- Για τον Υπάλληλο, ο Κανόνας (Rule) που ισχύει είναι: έχει πρόσβαση σε όλες τις λειτουργίες της υπηρεσίας εκτός απο την υπογραφή και την αποστολή.
- Για τον Διοικητικό Υπάλληλο, ο Κανόνας είναι: έχει πρόσβαση σε όλες τις λειτουργίες της υπηρεσίας.

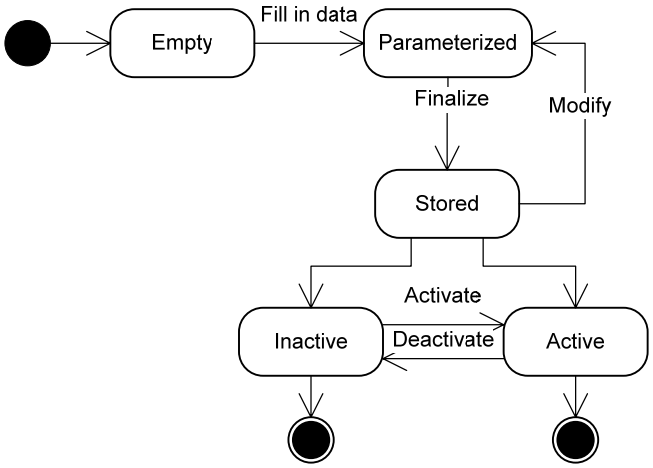
Οι κανόνες για τον ρόλο του Διαχειριστή ορίζονται στις πολιτικές που αναφέρονται στην συνολική ΑΔΑΑΥ που φιλοξενεί την υπηρεσία και δεν αποτελούν μέρος των προδιαγραφών της υπηρεσίας η-τιμολόγησης.
Η πολιτική υπογραφής καθορίζει το πλαίσιο σύμφωνα με το οποίο ο υπογράφονται τα ψηφιακά τιμολόγια. Θα πρέπει να είναι δημοσιευμένη κάπου ώστε να μπορούν να την δουν (URL) όλοι οι συμμετέχοντες στις κοινότητες που έχουν οριστεί. Το αναγνωριστικό της (το οποίο προκύπτει εφαρμόζοντας έναν αλγόριθμο κατακερματισμού (Algorithm) για την λήψη ενός Hash), θα πρέπει να ενσωματώνεται σε κάθε υπογεγραμμένο πιστοποιητικό γέννησης. Πιθανά χαρακτηριστικά της που φαίνονται στο παράδειγμα περιλαμβάνουν το Πεδίο Εφαρμογής (Application Field), τους Κανόνες Δέσμευσης (Commitment Rules) στην χρήση της υπηρεσίας, τα Χαρακτηριστικά που υπογράφονται σε κάθε πιστοποιητικό (Signed Attributes), τις απαιτήσεις για ενσωμάτωση δεδομένων ανακληθέντων πιστοποιητικών (Revocation Requirements) και τις απαιτήσεις απο τα πιστοποιητικά (ασφάλειας) που χρησιμοποιούνται για τις υπογραφές (Certificate Requirements).
Τα παραπάνω χαρακτηριστικά προκύπτουν απο τους περιορισμούς που έχουν οριστεί για την υπηρεσία στην 5.2.3.3.1.4 και είναι οι ακόλουθοι:

- Το URL επιλέγεται απο τον φορέα που παράγει τις υπογραφές.
- Ο αλγόριθμος κατακερματισμού είναι ο SHA-1.
- Το πεδίο εφαρμογής ορίζεται ως «Η-τιμολόγηση» (e-invoicing).
- Οι κανόνες δέσμευσης ορίζουν ότι ένα υπογεγραμμένο η-τιμολόγιο απο έναν οργανισμό αποτελεί νομικά κατοχυρωμένο έγγραφο που ορίζει ότι ο οργανισμός χρεώνει με ένα ποσό έναν άλλο οργανισμό για ένα δεδομένο σύνολο υπηρεσιών ή προϊόντων.
- Τα χαρακτηριστικά που υπογράφονται είναι όλο το τιμολόγιο, η χρονοσφραγίδα στα δεδομένα του και τα δεδομένα ανακληθέντων πιστοποιητικών.
- Οι απαιτήσεις ενσωμάτωσης δεδομένων ανακληθέντων πιστοποιητικών ορίζουν ότι τα δεδομένα αυτά είναι υποχρεωτικό να περιλαμβάνονται στην υπογραφή.
- Οι απαιτήσεις πιστοποιητικών ορίζουν ότι τα κλειδιά και τα αντίστοιχα πιστοποιητικά που χρησιμοποιούνται θα πρέπει να είναι διαπιστευμένα απο τις Αρχές Πιστοποίησης των συμμετεχουσών κοινοτήτων.

Ορισμένα απο τα παραπάνω χαρακτηριστικά ενδέχεται να οριστικοποιούνται λίγο πριν την έναρξη λειτουργίας της υπηρεσίας.

5.2.3.3.2.5.2 Δυναμικό σχήμα

Το δυναμικό σχήμα για τις όλες τις παραπάνω πολιτικές ακολουθεί το αντίστοιχο σχήμα του βασικού στοιχείου της παραγράφου 4.3.2.4.3.3.2.4:



Σχήμα 5-21: Δυναμικό σχήμα Πολιτικής

Κάθε πολιτική, αφότου παραμετροποιηθεί, αποθηκεύεται στο σύστημα σε ηλεκτρονική μορφή, ενεργοποιείται και είναι προσβάσιμη απο τις υπηρεσίες και τους μηχανισμούς που την χρειάζονται. Η πολιτική υπογραφής, όσο είναι σε ενεργή κατάσταση, είναι δημοσιευμένη και στο διαδίκτυο.

5.2.3.4 3ο Στάδιο: Γενική αποτύπωση απαιτούμενων υπηρεσιών και κατευθύνσεων τεχνολογίας

Ακολουθώντας τα βήματα που ορίζει η μεθοδολογία του σταδίου, προκύπτουν οι προδιαγραφές που ακολουθούν.

5.2.3.4.1 Απαραίτητες Υπηρεσίες ΑΔΑΑΥ

Οι υπηρεσίες που θα πρέπει να υποστηρίζει κατ' ελάχιστο η ΑΔΑΑΥ που θα φιλοξενήσει την επιχειρησιακή υπηρεσία η-τιμολόγησης σύμφωνα με τις μέχρι τώρα προδιαγραφές και τα βασικά στοιχεία όψης του σταδίου είναι οι ακόλουθες:

- Υπηρεσίες και μηχανισμοί διαχείρισης και συντονισμού
    - Υπηρεσία πρόσβασης
    - Υπηρεσία διαχείρισης διεργασιών
- Βασικές υπηρεσίες και μηχανισμοί
    - Υπηρεσία διεπαφής χρηστών
    - Υπηρεσία μετασχηματισμού μηνυμάτων
    - Υπηρεσία προώθησης μηνυμάτων
    - Υπηρεσία δημοσίευσης και αναζήτησης σε καταλόγους Υπηρεσιών Ιστού
    - Υπηρεσία διαχείρισης αποθετηρίων
- Υπηρεσίες και μηχανισμοί ασφάλειας
    - Μηχανισμοί ψηφιακών υπογραφών
    - Μηχανισμοί προηγμένων ηλεκτρονικών υπογραφών

- Μηχανισμοί κρυπτογράφησης
- Υπηρεσίες ελέγχου πρόσβασης
- Υπηρεσίες χρονοσφράγισης
- Υπηρεσίες διαχείρισης κλειδιών και πιστοποιητικών

- Υπηρεσίες υποστήριξης υπαρχουσών υποδομών

Για κάθε υπάρχον σύστημα που κρατάει δεδομένα τιμολογίων θα πρέπει να σχεδιαστεί μια αντίστοιχη Υπηρεσία Υποστήριξης Υπαρχουσών Υποδομών, έτσι ώστε να κάνει διαθέσιμα τα δεδομένα αυτά στην υπηρεσία η-τιμολόγησης.
Οι προδιαγραφές των σταδίων που ακολουθούν λαμβάνουν υπόψην ότι παρέχονται όλες οι παραπάνω υπηρεσίες.

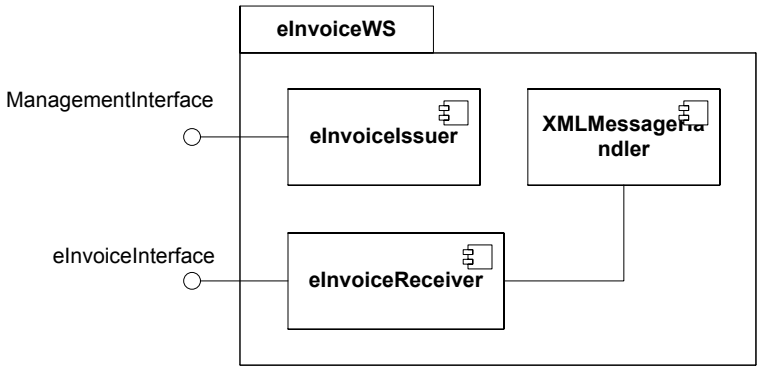
5.2.3.4.2 Συνολικό τεχνολογικό πλαίσιο

Όσο αφορά στο συνολικό τεχνολογικό πλαίσιο που θα ακολουθηθεί, η συγκεκριμένη υπηρεσία πρόκειται να υλοποιηθεί σε περιβάλλον J2EE.

5.2.3.5 4ο Στάδιο: Σχεδιασμός στοιχείων λογισμικού

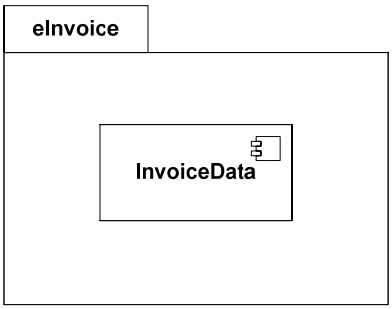
5.2.3.5.1 Διαγράμματα δομικών στοιχείων

Η υπηρεσία η-τιμολόγησης είναι μια νέα επιχειρησιακή υπηρεσία που θέλουμε να σχεδιάσουμε, επομένως δεν υπάρχει κάποιο έτοιμο βασικό στοιχείο όψης που θα χρησιμοποιηθεί ως βάση. Κατασκευάζουμε λοιπόν τα νέα διαγράμματα δομικών στοιχείων που αναπαριστούν την δομή της υπηρεσίας:



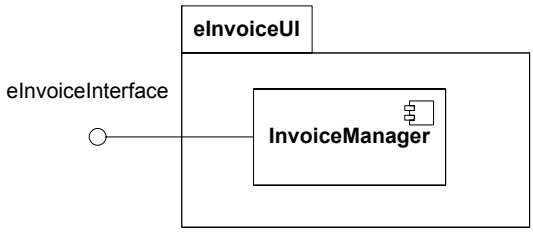
Σχήμα 5-22: Διάγραμμα δομικών στοιχειών Υπηρεσίας Ιστού η-τιμολόγησης

Το πρώτο διάγραμμα παρουσιάζει το βασικό πακέτο eInvoiceWS, το οποίο αποτελείται απο τρία βασικά δομικά στοιχεία: την Υ.Ι. eInvoiceIssuer που επιτελεί τις βασικές επιχειρησιακές λειτουργίες και συναρτήσεις της υπηρεσίας που σχεδιάζεται ως προς την δημιουργία, διαχείριση, υπογραφή και αποστολή, την eInvoiceReceiver που αποτελεί την Ι.Υ. «σημείο λήψης» εισερχόμενων μηνυμάτων της υπηρεσίας και το δομικό στοιχείο XMLMessageHandler που χρησιμεύει ως διαχειριστής μηνυμάτων και εγγράφων XML.
Το δεύτερο διάγραμμα eInvoice στο Σχήμα 5-23 περιλαμβάνει το βασικό δομικό στοιχείο InvoiceData το οποίο αναπαριστά το αντίστοιχο αντικείμενο πληροφορίας και τα περιεχόμενά του.



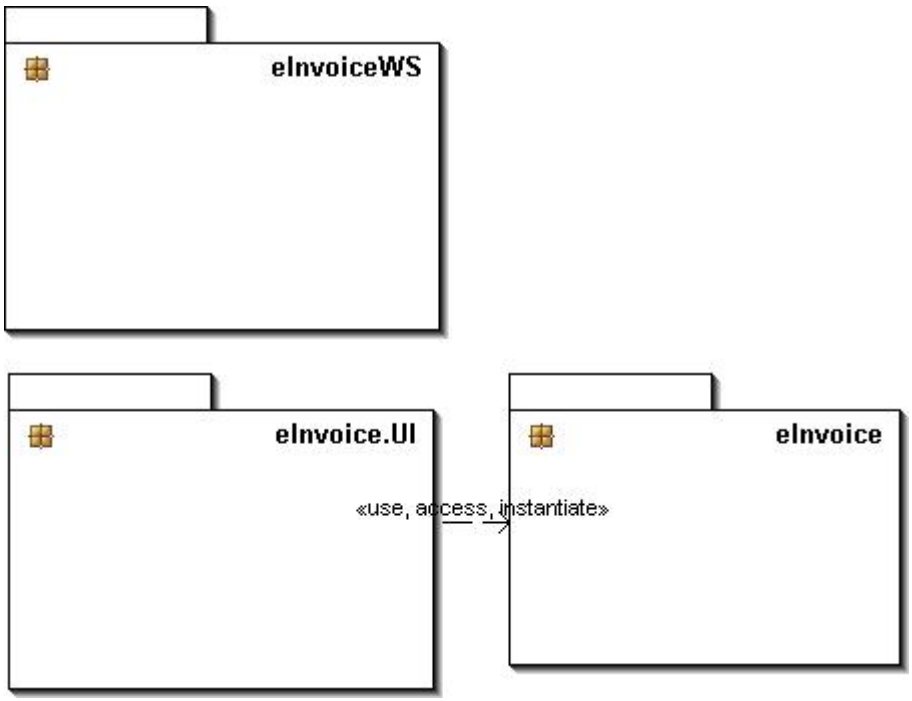
Σχήμα 5-23: Διάγραμμα δομικών στοιχείων για την αναπαράσταση του αντικειμένου πληροφορίας Τιμολόγιο

Το δομικό στοιχείο InvoiceData θα αναλυθεί περαιτέρω στη συνέχεια προκειμένου να γίνεται πλήρης διαχείρισης των δεδομένων που περιέχει βάσει του σχήματός του.
Το τελευταίο διάγραμμα δομικών στοιχείων θα αποτελέσει μέρος της Υπηρεσίας Διεπαφής Χρηστών της αρχιτεκτονικής, για την πρόσβαση στη συγκεκριμένη επιχειρησιακή υπηρεσία.



Σχήμα 5-24: Διάγραμμα δομικών στοιχείων για την υπο-υπηρεσία Διεπαφής Χρηστών

Οι λειτουργίες της γραφικής διεπαφής χρηστών διαχειρίζεται το δομικό στοιχείο InvoiceManager. Η συνολική σχέση μεταξύ των παραπάνω διαγραμμάτων φαίνεται στο ακόλουθο σχήμα:

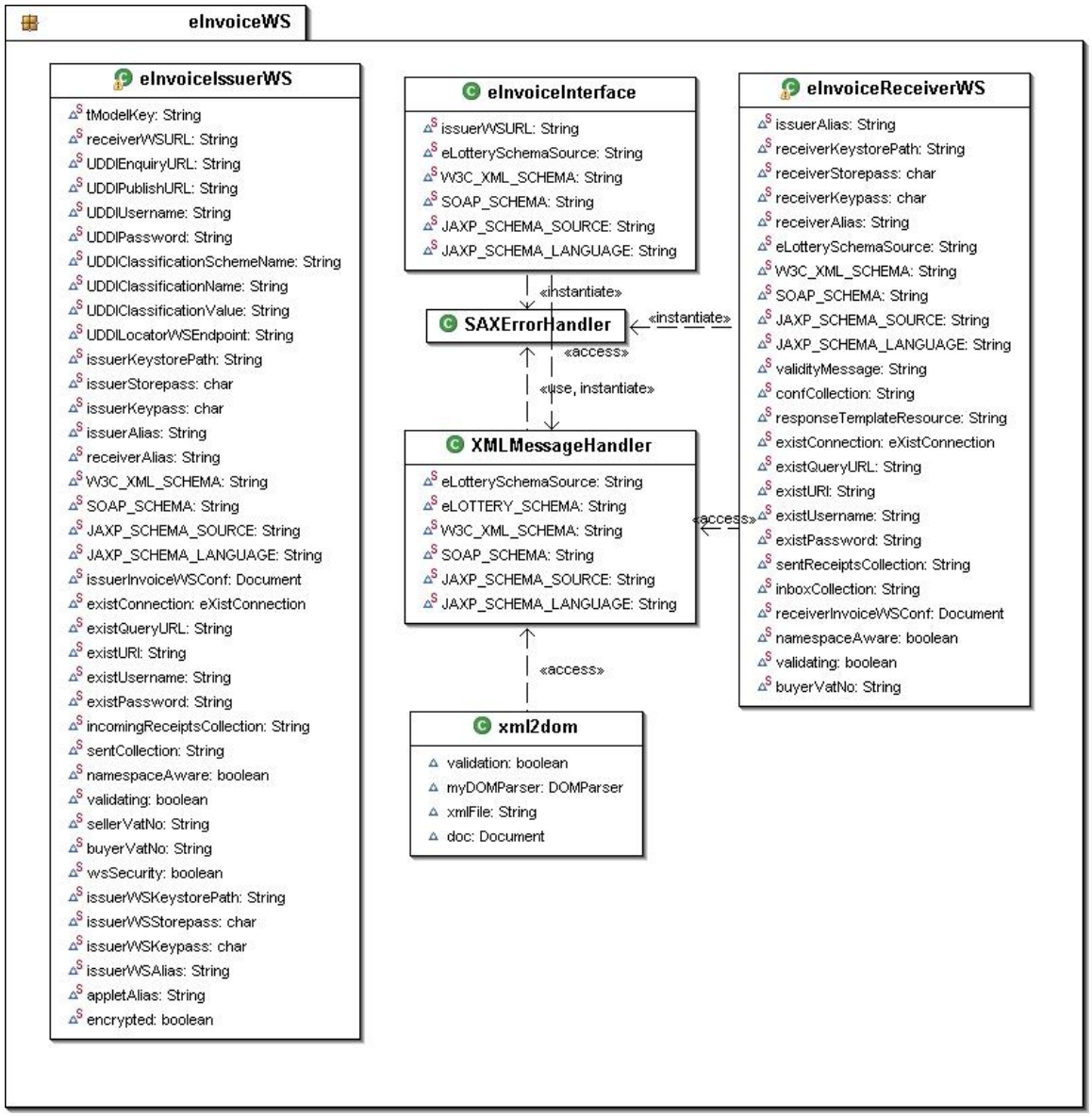


Σχήμα 5-25: Σχέση μεταξύ των διαγραμμάτων δομικών στοιχείων της επιχειρησιακής υπηρεσίας

Όπως φαίνεται, το πακέτο για την γραφική διεπαφή χρήστη χρησιμοποιεί την αναπαράσταση του αντικειμένου πληροφορίας στο πακέτο eInvoice.

5.2.3.5.2 Διαγράμματα κλάσεων

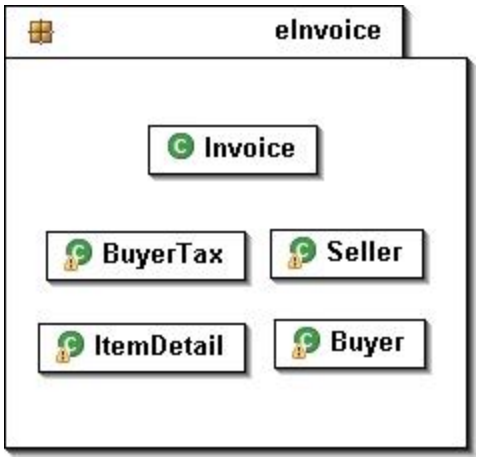
Στη συνέχεια παράγονται διαγράμματα κλάσεων που αντιστοιχούν στα παραπάνω διαγράμματα δομικών στοιχείων.
Το διάγραμμα κλάσεων για την Υ.Ι. είναι το ακόλουθο:



Σχήμα 5-26: Διάγραμμα κλάσεων Υ.Ι. η-τιμολόγησης

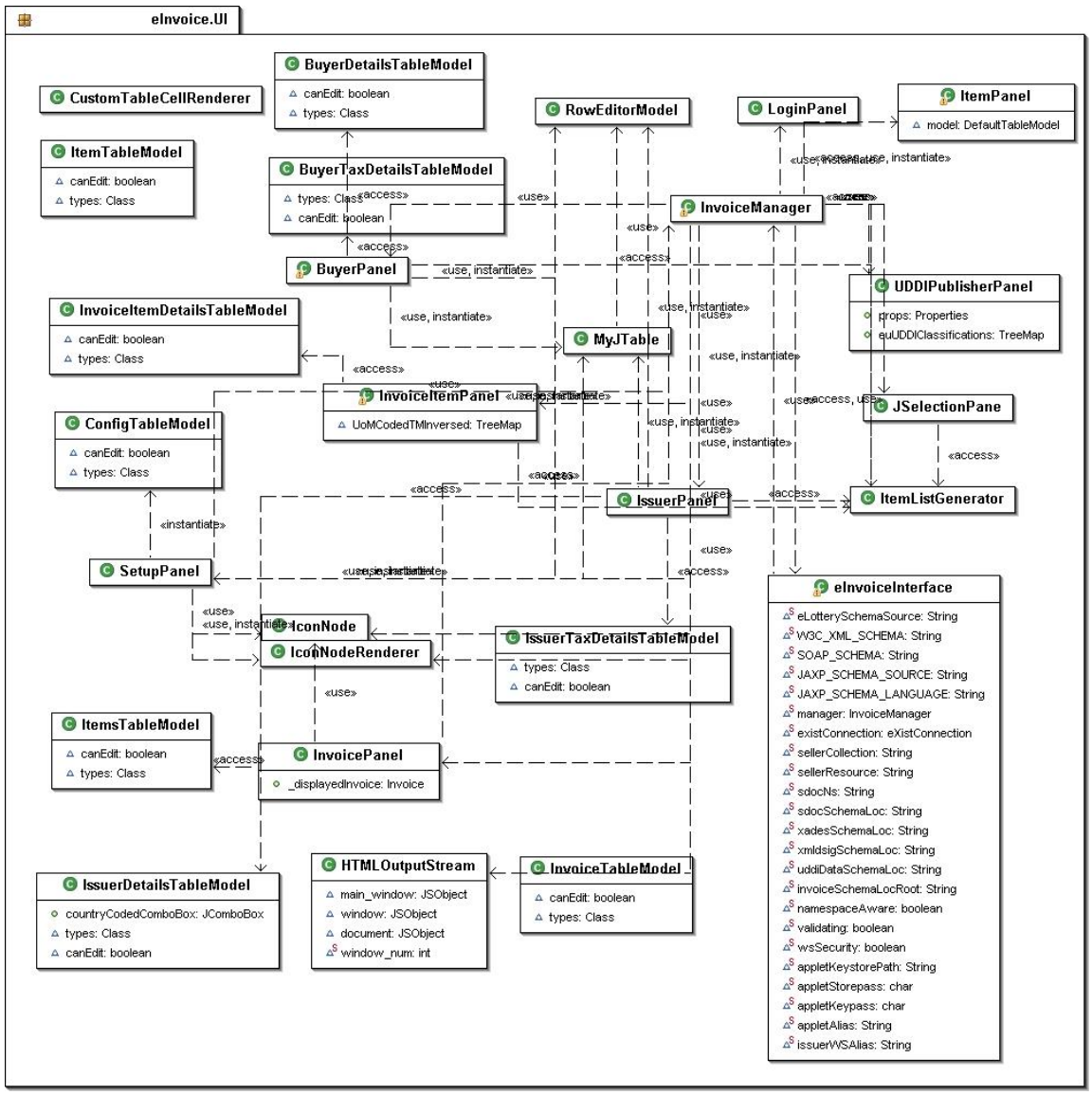
Το δομικό στοιχείο eInvoiceIssuer αναλύεται στην κλάση eInvoiceIssuerWS η οποία αναλαμβάνει να υλοποιεί τις βασικές επιχειρησιακές λειτουργίες της υπηρεσίας. Το δομικό στοιχείο eInvoiceReceiver υλοποιείται απο την κλάση eInvoiceReceiverWS, η οποία λειτουργεί ως σημείο διαχείρισης των μηνυμάτων με η-τιμολόγια ή επιβεβαιώσεων που λαμβάνονται, και αναλαμβάνει να αναλύει τα μηνύματα αυτά στα συστατικά τους. Για το λόγο αυτό, η κλάση χρησιμοποιεί το σύνολο των κλάσεων του δομικού στοιχείου XMLMessageHandler, οι οποίες όπως φαίνεται στο σχήμα είναι οι SAXErrorHandler για την διαχείριση λαθών, XMLMessageHandler που υλοποιεί την βασική λειτουργικότητα ανάγνωσης των μηνυμάτων και αναπαράστασής τους για διαχείριση σε μια δενδρική δομή DOM [DOM] με χρήση της κλάσης xml2dom. Τέλος, η πρόσβαση στο eInvoiceReceiverWS γίνεται μέσω της κλάσης – διεπαφής eInvoiceInterface.

Η διεπαφή eInvoiceInterface υλοποιείται ως μια κλάση επίσης, με την οποία θα επικοινωνεί κάθε αντικείμενο που θέλει να στείλει μήνυμα στο eInvoiceReceiverWS. Αυτή η διεπαφή δημοσιεύεται στους καταλόγους Y.I.
Σημειώνεται ότι στην παρούσα ενότητα στον αναλυτικό σχεδιασμό της υπηρεσίας περιλαμβάνεται και ένα σύνολο επιμέρους κλάσεων και οι περιγραφές τους, οι οποίες δεν παρατίθενται στην διατριβή, λόγω όγκου και λόγω του ότι δεν προσφέρουν κάτι ως προς την τεκμηρίωση της ορθότητας της κατασκευαστικής μεθόδου.
Το διάγραμμα δομικών στοιχείων του eInvoice στο Σχήμα 5-23 αναλύεται στις ακόλουθες κλάσεις:



Σχήμα 5-27: Διάγραμμα κλάσεων για το δομικό στοιχείο eInvoice (αντικείμενο πληροφορίας)

Όπως φαίνεται στο σχήμα, η βασική κλάση που αναπαριστά το η-τιμολόγιο λέγεται Invoice και χρησιμοποιεί κλάσεις που αναπαριστούν διαφορετικά υπο-κομμάτια του τιμολογίου σύμφωνα με το σχήμα του: BuyerTax, Seller, ItemDetail, Buyer (βλ. και παράγραφο 5.2.3.3.2.1.1).
Το τρίτο διάγραμμα δομικών στοιχείων αναλύεται ως εξής:



Σχήμα 5-28: Διάγραμμα κλάσεων για την γραφική διεπαφή με τους χρήστες

Η βασική κλάση που αντιστοιχεί στον InvoiceManager στο Σχήμα 5-28 ονομάζεται επίσης InvoiceManager. Χρησιμοποιεί ένα σύνολο απο στοιχεία γραφικών του Framework της Java για την υλοποίηση των διαφόρων φορμών δημιουργίας, επεξεργασίας και αποστολής των τιμολογίων που βασίζονται στις κλάσεις TableModel, JPane, και EditorModel. Η κλάση αυτή αναλαμβάνει να δέχεται τις πληροφορίες απο την διεπαφή χρήστη προκειμένου να καλεί τις κατάλληλες μεθόδους στην Y.I. που υλοποιεί την επιχειρησιακή υπηρεσία. Οι αναλυτικές προδιαγραφές των παραπάνω κλάσεων θεωρούνται εκτός ενδιαφέροντος της διατριβής.

5.2.3.5.3 Διαγράμματα ακολουθίας

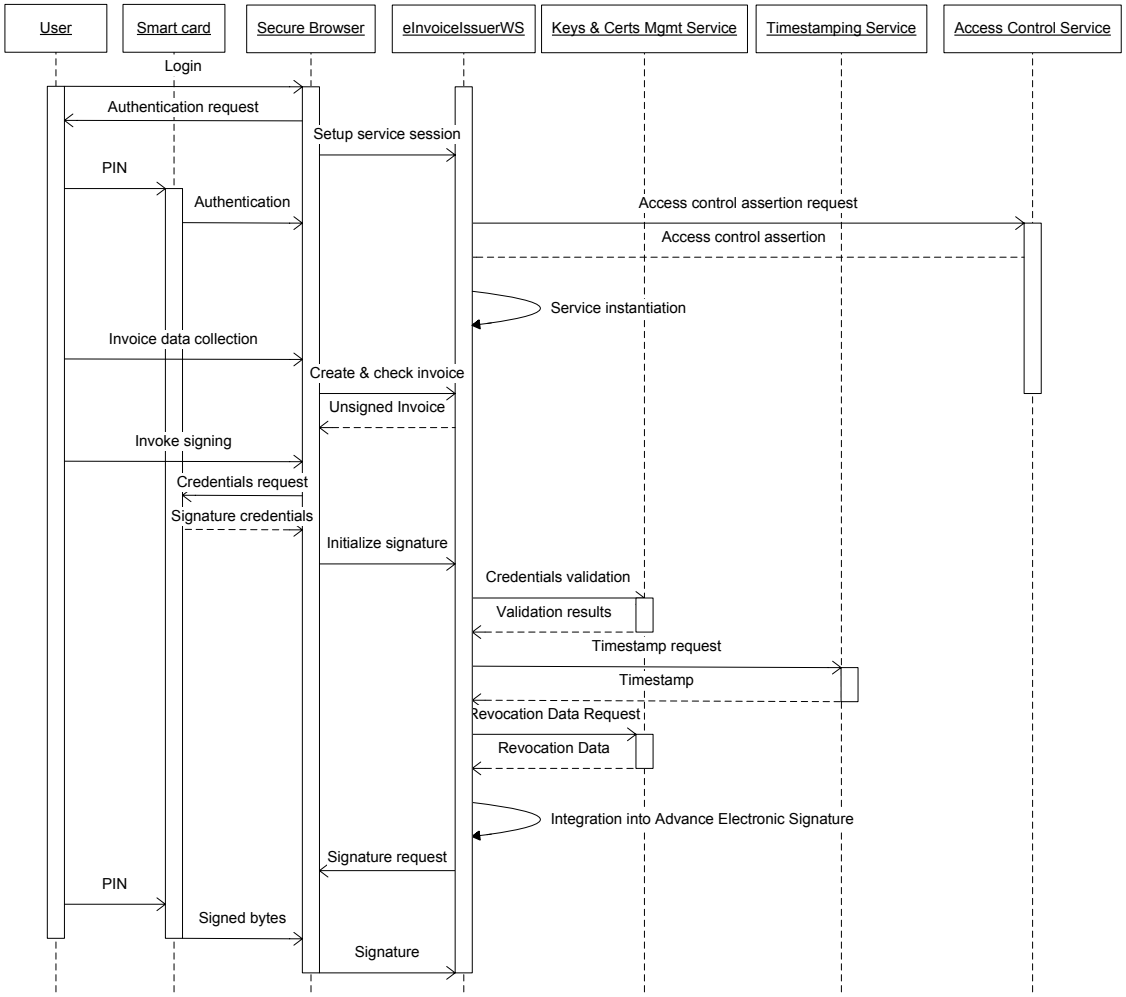
Με βάση τις κλάσεις που έχουμε ορίσει, συμπληρώνουμε αρχικά τις προδιαγραφές με διαγράμματα ακολουθίας. Προδιαγράφεται ένα διάγραμμα ακολουθίας για κάθε φάση

της η-τιμολόγησης, σύμφωνα με τις προδιαγραφές των διεργασιών της παραγράφου 5.2.3.3.1.3.

5.2.3.5.3.1 Φάση έκδοσης

Όπως φαίνεται στο διάγραμμα ακολουθίας στο Σχήμα 5-29, ένας υπάλληλος του οργανισμού Εκδότη (εκπροσωπούμενος απο την κλάση «User» στο διάγραμμα) ξεκινά τη διαδικασία η-τιμολόγησης. Αρχικά αυθεντικοποιείται μέσω της έξυπνης κάρτας του και του PIN μέσα απο την ασφαλή διεπαφή χρήστη (Secure browser). Βάσει των διαπιστευτηρίων ασφάλειας το σύστημα κάνει έναν έλεγχο πρόσβασης.
Η διεπαφή χρήστη επιτρέπει στον χρήστη να δημιουργήσει ένα καινούργιο τιμολόγιο και να συμπληρώσει τα απαραίτητα δεδομένα για την ολοκλήρωση του τιμολογίου ή να διαχειριστεί ήδη υπάρχοντα τιμολόγια (για παράδειγμα τιμολόγια που έχουν ήδη ληφθεί, πρόχειρα κ.λ.π.) Τα δεδομένα ελέγχονται αυτόματα για πιθανά λάθη σύμφωνα με τις ισχύουσες πολιτικές. Σύμφωνα με τα χαρακτηριστικά του χρήστη και τα δικαιώματά του (attributes & privileges) ο χρήστης έχει διαθέσιμες ή όχι τις επιλογές για υπογραφή και αποστολή του η-τιμολογίου. Τα βήματα που διαφανώς επιτελούνται είναι τα ακόλουθα:

- Τα δεδομένα της φόρμας συλλέγονται και χρησιμοποιούνται για να δομηθεί ένα τιμολόγιο.
- Οι χρονοσφραγίδες και η πληροφορία ανάκλησης πιστοποιητικών συλλέγονται απο τις πηγές τους μέσω των αντίστοιχων υπηρεσιών Χρονοσφράγισης και Διαχείρισης Κλειδιών και Πιστοποιητικών της ΑΔΑΑΥ
- Δημιουργείται η προηγμένη ηλεκτρονική υπογραφή βάσει αυτών των δεδομένων και τα κρυπτογραφικά στοιχεία στην έξυπνη κάρτα του.

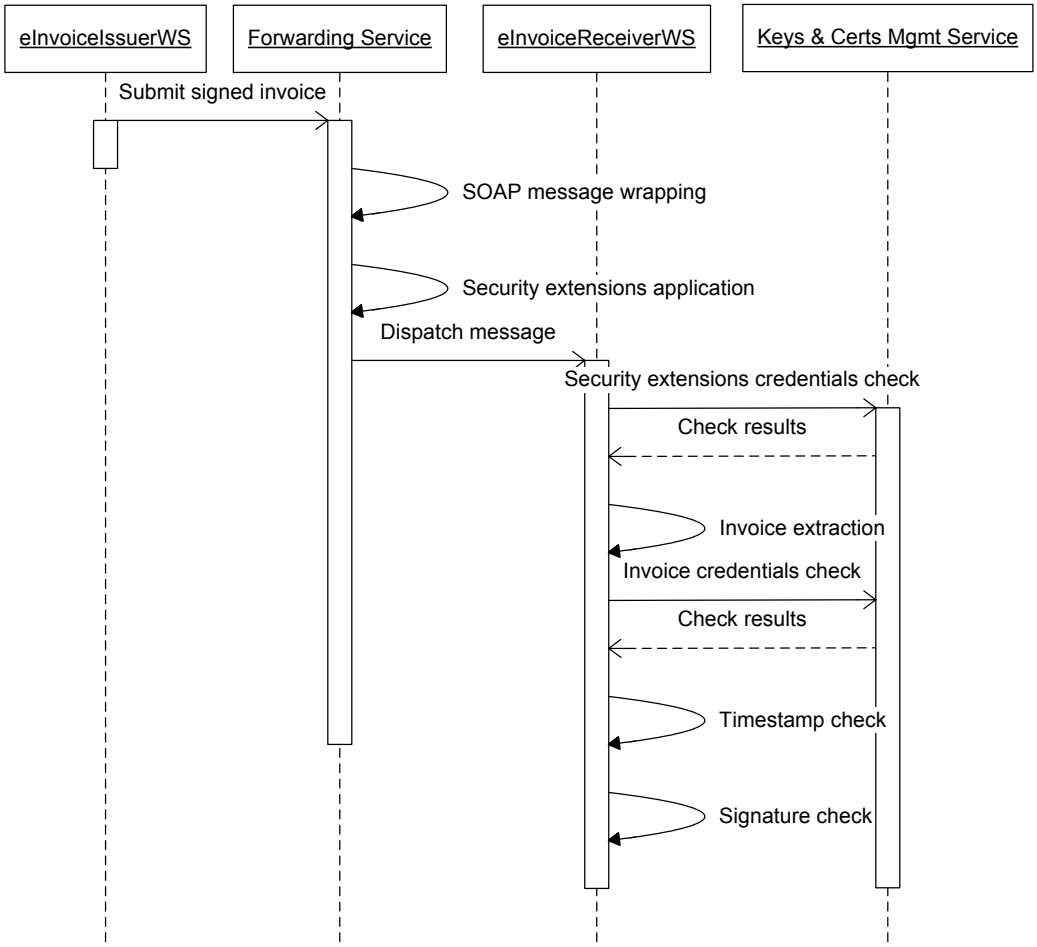


Σχήμα 5-29: Φάση έκδοσης η-τιμολογίου

Τα πιστοποιητικά που χρησιμοποιούνται για την υπογραφή και αυθεντικοποίηση μπορεί να είναι διαφορετικά ή τα ίδια, κάτι που καθορίζεται απο την πολιτική ασφάλειας του οργανισμού. Στην περίπτωση που είναι διαφορετικά, στον χρήστη δίνεται η δυνατότητα επιλογής, ανάλογα με την χρήση μια δεδομένη χρονική στιγμή.

5.2.3.5.3.2 Φάση αποστολής / λήψης

Μετά την επιτυχή δημιουργία της προηγμένης ηλεκτρονικής υπογραφής, το τιμολόγιο ενσωματώνεται σε ένα μήνυμα SOAP και αποστέλλεται στην Υπηρεσία Προώθησης της ΑΔΑΑΥ του οργανισμού, όπως διαφαίνεται στο Σχήμα 5-30. Η Υπηρεσία Προώθησης αναλαμβάνει να εξάγει το τιμολόγιο, και να το πακετάρει σε ένα νέο μήνυμα, προσθέτοντάς του τις κατάλληλες επεκτάσεις ασφάλειας, χρησιμοποιώντας μηχανισμούς Ψηφιακών Υπογραφών και Κρυπτογράφησης. Το ασφαλές πλέον μήνυμα SOAP αποστέλλεται σε μια αντίστοιχη υπηρεσία στον οργανισμό παραλήπτη.



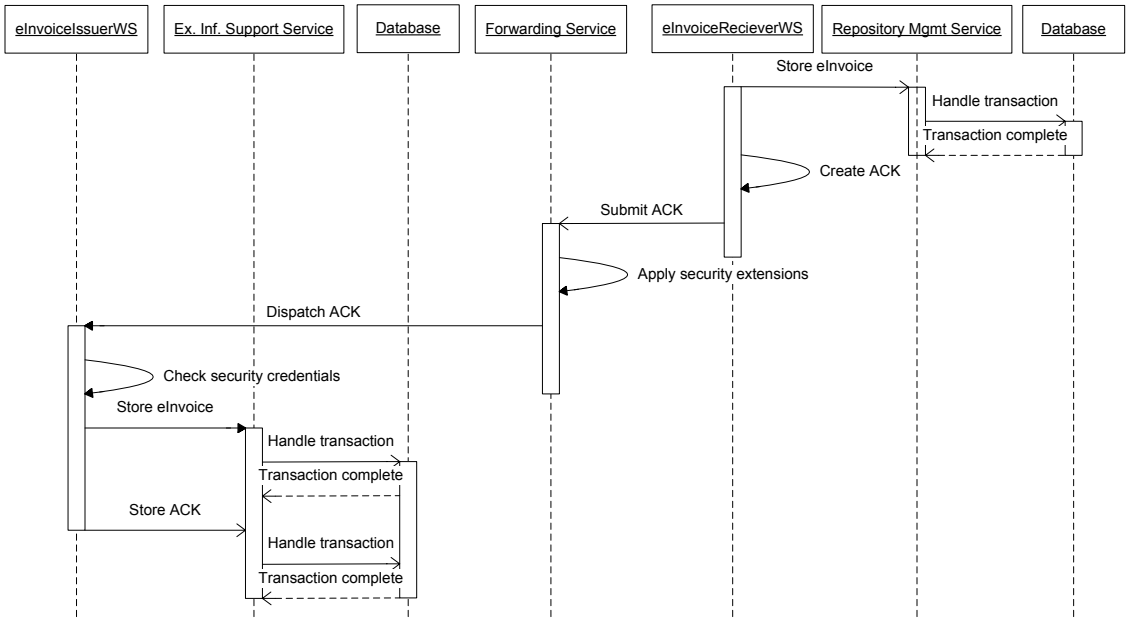
Σχήμα 5-30: Φάση αποστολής / λήψης η-τιμολογίου

Η λήψη του τιμολογίου είναι μια πλήρως αυτοματοποιημένη διαδικασία που δεν απαιτεί την ανθρώπινη παρέμβαση. Το μήνυμα SOAP που περιέχει το τιμολόγιο αποκρυπτογραφείται και επαληθεύονται τα διαπιστευτήρια του συνολικού μηνύματος με επικοινωνία με την Υπηρεσία Διαχείρισης Κλειδιών και Πιστοποιητικών.
Στη συνέχεια εξάγεται το ίδιο το τιμολόγιο, και εκτελείται η επαλήθευση της κρυπτογραφικής πληροφορίας των διαπιστευτηρίων που χρησιμοποιήθηκαν για την υπογραφή του, καθώς και οποιασδήποτε χρονοσφραγίδας αυτό περιέχει. Στη συνέχεια επαληθεύεται η ίδια η προηγμένη ηλεκτρονική υπογραφή.

5.2.3.5.3.3 Φάση αποθήκευσης

Εάν όλες οι επαληθεύσεις της προηγούμενης φάσης είναι επιτυχείς, το η-τιμολόγιο αρχικά αποθηκεύεται στην βάση του Παραλήπτη, όπως φαίνεται στο Σχήμα 5-31, μέσω μιας Υπηρεσία Υποστήριξης Υπαρχουσών Υποδομών (αν το σύστημα στο οποίο αποθηκεύονται είναι υπάρχον) είτε μέσω μιας Υπηρεσίας Διαχείρισης Αποθετηρίων αν έχει φτιαχτεί εκ νέου για την υπηρεσία. Στην προκειμένη περίπτωση του σχήματος χρησιμοποιείται το πρώτο απο τον Εκδότη ενώ το δεύτερο απο τον Παραλήπτη. Η

διαδικασία ολοκληρώνεται απο την αποστολή μιας απόδειξης SOAP πίσω στον εκδότη, που αντικατοπτρίζει το τιμολόγιο που μόλις έχει ληφθεί, και περιλαμβάνει την κατάσταση όλης της διαδικασίας.

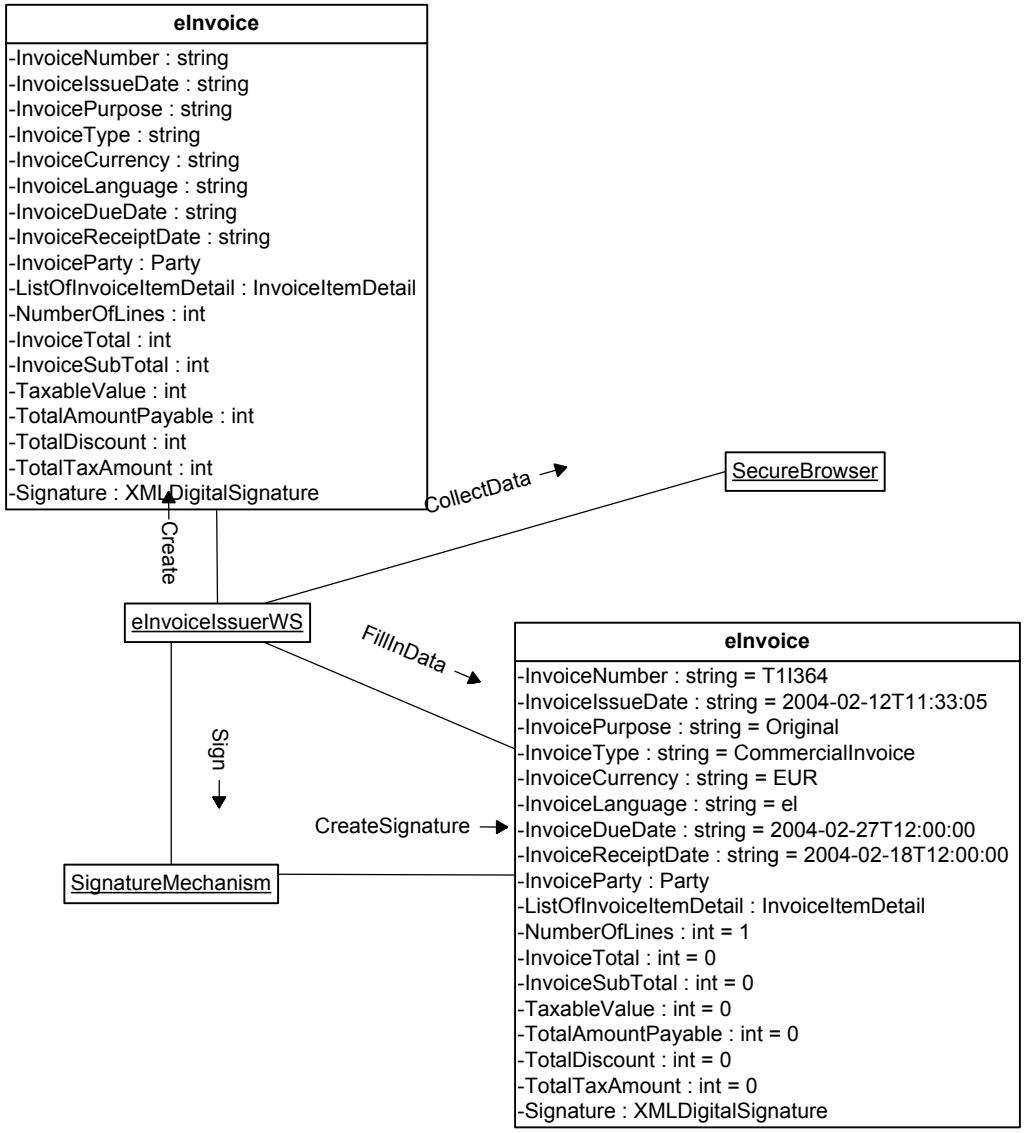


Σχήμα 5-31: Φάση αποθήκευσης η-τιμολογίου

Η απάντηση αυτή είναι υπογεγραμμένη μόνο σύμφωνα με τις επεκτάσεις ασφάλειας για μηνύματα SOAP. Όταν η υπηρεσία του Εκδότη λάβει την απόδειξη και την επαληθεύσει, την φυλάει στην δική της βάση μαζί με το αντίστοιχο τιμολόγιο.

5.2.3.5.4 Διαγράμματα συνεργασίας

Σύμφωνα με την μεθοδολογία, ως τελευταίο κομμάτι των προδιαγραφών της υπολογιστικής όψης, σχεδιάζονται κατάλληλα διαγράμματα συνεργασίας για περαιτέρω ανάλυση και διευκρίνιση των σχέσεων των κλάσεων και των αντικειμένων που απορρέουν απο αυτές. Στην ανάλυση αυτή χρησιμοποιούνται όπου χρειάζεται στατικά σχήματα αντικειμένων πληροφορίας που ανταλλάσσονται. Στην προκειμένη περίπτωση θεωρείται απαραίτητο να διευκρινιστεί η επεξεργασία που υπόκειται ένα η-τιμολόγιο κατά τη φάση της δημιουργίας και υπογραφής του (στην φάση έκδοσης παραπάνω).
Το διάγραμμα συνεργασίας που ακολουθεί χρησιμοποιεί στατικά σχήματα του αντικείμενου η-τιμολόγιο για να δείξει το πως συμπληρώνεται με στοιχεία:



Σχήμα 5-32: Διάγραμμα συνεργασίας για την δημιουργία ενός η-τιμολογίου

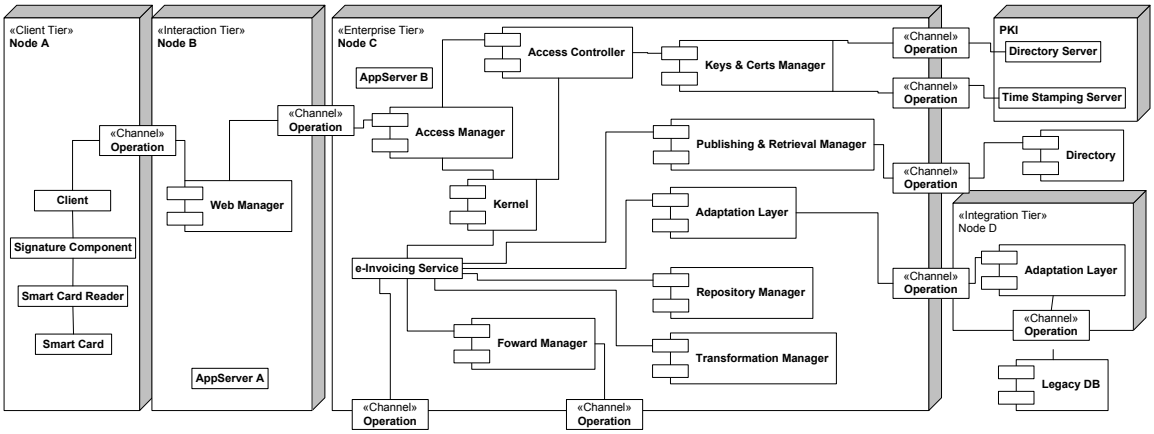
Όπως φαίνεται στο σχήμα, η δημιουργία του τιμολογίου συντελείται απο την κλάση eInvoiceIssuerWS. Αρχικά δημιουργείται ένα κενό τιμολόγιο έχοντας όλα τα πεδία που απαιτούνται απο το σχήμα. Στη συνέχεια αλληλεπιδρά με τον χρήστη μέσω του φυλλομετρητή προκειμένου να λάβει το απαραίτητο μέρος της πληροφορίας που απαιτείται για την συμπλήρωση του τιμολογίου. Ένα μέρος της πληροφορίας που είναι ήδη στο σύστημα (π.χ. στοιχεία των συμμετεχουσών οντοτήτων όπως η διεύθυνση κ.λ.π.) συμπληρώνονται αυτόματα, οπότε προκύπτει μια συμπληρωμένη μορφή του τιμολογίου, όπως φαίνεται στο σχήμα. Τέλος το eInvoiceIssuerWS χρησιμοποιεί τον μηχανισμό ηλεκτρονικών υπογραφών στέλνοντάς του το συμπληρωμένο τιμολόγιο προκειμένου να προκύψει μια ολοκληρωμένη ηλεκτρονική υπογραφή η οποία περικλείει τα δεδομένα του τιμολογίου και όλη την απαραίτητη πληροφορία (χρονοσφραγίδα, δεδομένα ανάκλησης πιστοποιητικών).

5.2.3.6 5ο Στάδιο: Αναλυτική οργάνωση υπηρεσιών και επιλογή τεχνολογιών

Το στάδιο αυτό περιλαμβάνει την δημιουργία των προδιαγραφών της Όψης Μηχανικού και της Τεχνολογικής Όψης. Και οι δύο αυτές όψεις θεωρούν ότι η υπηρεσία η-τιμολόγησης εγκαθίσταται σε μια συνολική αρχιτεκτονική ΑΔΑΑΥ η οποία προσφέρει τις υπηρεσίες που έχουν επιλεγεί στο 3ο στάδιο. Η υπηρεσία η-τιμολόγησης κάνει χρήση των υπηρεσιών αυτών προκειμένου να υλοποιήσει τις επιχειρησιακές διεργασίες. Οι όψεις του παρόντος σταδίου αποδίδουν πως θα πρέπει κατανέμονται σε κόμβους τα μηχανικά αντικείμενα **όλων** των υπηρεσιών που χρησιμοποιούνται και ποιες τεχνολογίες χρησιμοποιούνται σε κάθε υπηρεσία.

5.2.3.6.1 Όψη Μηχανικού

Προκειμένου να λειτουργήσει η υπηρεσία, θεωρούμε ότι η συνολική αρχιτεκτονική αποτελείται απο τέσσερα βασικά επίπεδα στα οποία κατανέμονται οι κόμβοι: ένα επίπεδο πελάτη, ένα επίπεδο αλληλεπίδρασης, ένα επιχειρησιακό επίπεδο και ένα επίπεδο ολοκλήρωσης. Ορίζεται ένα μηχανικό αντικείμενο που αναπαριστά στην υπηρεσία η-τιμολόγησης και ένα μηχανικό αντικείμενο για κάθε μια απο τις απαραίτητες υπηρεσίες της ΑΔΑΑΥ. Η κατανομή όλων των μηχανικών αντικειμένων φαίνεται στο συνολικό διάγραμμα εγκατάστασης στο Σχήμα 5-33:



Σχήμα 5-33: Συνολικό διάγραμμα εγκατάστασης αρχιτεκτονικής η-τιμολόγησης

Στο σχήμα έχουν ήδη τοποθετηθεί και όλα τα απαραίτητα κανάλια επικοινωνίας με τα οποία μηχανικά αντικείμενα που βρίσκονται σε διαφορετικούς κόμβους επικοινωνούν μεταξύ τους καθώς και με άλλες υπηρεσίες σε εξωτερικές αρχιτεκτονικές ή με εξωτερικές οντότητες. Το συνολικό διάγραμμα εγκατάστασης αναλύεται ως εξής:

1. *Κόμβος Α* στο επίπεδο πελάτη. Στον κόμβο βρίσκεται η *Εφαρμογή πελάτη (Client)* με την οποία αλληλεπιδρούν οι χρήστες (Υπάλληλοι και Διοικητικοί Υπάλληλοι) και αποτελεί το ένα μέρος της υπηρεσίας διεπαφής χρηστών (βλ. και παραγράφους 4.3.3.3.2.1 και 4.3.4.3.3.2.2.1). Το μηχανικό αντικείμενο εφαρμογής πελάτη επικοινωνεί με το αντικείμενο διαχειριστή ιστοσελίδων στον κόμβο Β μέσω ενός καναλιού λειτουργιών. Στο επίπεδο αυτό επίσης περιλαμβάνεται ένα μηχανικό

αντικείμενο που υλοποιεί τους μηχανισμούς ψηφιακών και προηγμένων ηλεκτρονικών υπογραφών *(Signature component)* (βλ. και παραγράφους 4.3.3.3.3.1,4.3.3.3.3.2 και 4.3.4.3.3.2.3.3, 4.3.4.3.3.2.3.4) με χρήση ενός *Αναγνώστη κάρτας (Smart card reader)* και της *Έξυπνης κάρτας (Smart card)* του κάθε χρήστη.

2. *Κόμβος Β* στο επίπεδο αλληλεπίδρασης. Ο κόμβος περιέχει τον *Εξυπηρετητή εφαρμογών Α (App Server A)* και τον *Διαχειριστή ιστοσελίδων (Web manager)* που δέχεται τις αιτήσεις πρόσβασης απο τις εφαρμογές πελάτες, τις αποδομεί κατάλληλα και τις αποστέλλει στο επιχειρησιακό επίπεδο στον κόμβο C, προκειμένου να λάβει τις απαραίτητες απαντήσεις. Τις απαντήσεις τις δομεί σε ιστοσελίδες ή άλλου τύπου έγγραφα, όπως για παράδειγμα XML, και τις επιστρέφει στις εφαρμογές πελάτες. Το αντικείμενο διαχείρισης ιστοσελίδων αποτελεί το δεύτερο μέρος της υπηρεσίας διεπαφής χρηστών (βλ. και παραγράφους 4.3.3.3.2.1 και 4.3.4.3.3.2.2.1) και επικοινωνεί απο την μια πλευρά με το αντικείμενο εφαρμογής πελάτη στον κόμβο Α και με το αντικείμενο διαχειριστή πρόσβασης στον κόμβο C μέσω καναλιών λειτουργιών.
3. *Κόμβος C* στο επιχειρησιακό επίπεδο, ο οποίος περιέχει τον *Εξυπηρετητή εφαρμογών Β (App Server B)*. Ο κόμβος αυτός αποτελεί την καρδιά της συγκεκριμένης αρχιτεκτονικής όπου φιλοξενείται το μεγαλύτερο μέρος των υπηρεσιών διαχείρισης καθώς και οι βασικές υπηρεσίες, οι υπηρεσίες υποστήριξης υπαρχουσών υποδομών, οι υπηρεσίες ασφάλειας και η επιχειρησιακή υπηρεσία η-τιμολόγησης που σχεδιάζεται. Πιο συγκεκριμένα, τα μηχανικά αντικείμενα που περιλαμβάνονται και υλοποιούν τις παραπάνω υπηρεσίες είναι τα ακόλουθα (σε συμφωνία με τα βασικά στοιχεία της υπολογιστικής όψης που παρουσιάστηκαν στην παράγραφο 4.3.4.3.3.2 και τα αποτελέσματα του 3^{ου} σταδίου):
   - Υπηρεσίες και μηχανισμοί διαχείρισης και συντονισμού:
     - Ο *Διαχειριστής πρόσβασης (Access Manager)* υλοποιεί την υπηρεσία πρόσβασης (βλ. και παραγράφους 4.3.3.3.1.1 και 4.3.4.3.3.2.1.1). Δέχεται τις αιτήσεις μέσω του επιπέδου αλληλεπίδρασης, επικοινωνεί με την υπηρεσία ελέγχου πρόσβασης για τις κατάλληλες εξουσιοδοτήσεις και με τον πυρήνα για τις εκκινήσεις διεργασιών που απαιτούνται σύμφωνα με τις αιτήσεις. Επικοινωνεί με τον διαχειριστή ιστοσελίδων στον κόμβο Β μέσω ενός καναλιού λειτουργιών,
     - Ο *Πυρήνας (Kernel)* υλοποιεί το βασικό μέρος της υπηρεσίας διαχείρισης διεργασιών με όλες τις λειτουργίες που αναφέρθηκαν στις παραγράφους 4.3.3.3.1.2 και 4.3.4.3.3.2.1.2, εκτός απο τις σχετικές με τον σχεδιασμό, τον συντονισμό, την εγκατάσταση και απεγκατάσταση των επιχειρησιακών υπηρεσιών, οι οποίες συντελούνται στο δεύτερο επιχειρησιακό επίπεδο.
   - Βασικές υπηρεσίες και μηχανισμοί
     - Ο *Διαχειριστής δημοσίευσης και ανάκτησης (Publishing & retrieval manager)* υλοποιεί μια υπηρεσία δημοσίευσης και αναζήτησης σε καταλόγους υπηρεσιών ιστού, με όλες τις λειτουργίες που αναφέρθηκαν στις παραγράφους 4.3.3.3.2.4 και 4.3.4.3.3.2.2.4. Επικοινωνεί με έναν κατάλογο υπηρεσιών ιστού UDDI μέσω ενός καναλιού λειτουργιών. Όσο αφορά στην υπηρεσία η-τιμολόγησης, ο διαχειριστής δημοσίευσης βοηθά

στο να την βρουν επιχειρήσεις που ενδιαφέρονται να ανταλλάξουν ηλεκτρονικά τιμολόγια με τον οργανισμό που λειτουργεί την υπηρεσία.

- Ο *Διαχειριστής αποθετηρίων (Repository Manager)* υλοποιεί μια υπηρεσία διαχείρισης αποθετηρίων σύμφωνα με τις περιγραφές των παραγράφων 4.3.3.3.2.5 και 4.3.4.3.3.2.2.5. Πιο συγκεκριμένα ο διαχειριστής επιτρέπει την πρόσβαση και αναζήτηση στη βάση δεδομένων που φυλάσσονται τα η-τιμολόγια και όλες οι επιβεβαιώσεις.
- Ο *Διαχειριστής Μετασχηματισμού (Transformation Manager)* υλοποιεί μια υπηρεσία μετασχηματισμού μηνυμάτων σύμφωνα με τις προδιαγραφές των παραγράφων 4.3.3.3.2.2 και 4.3.4.3.3.2.2.2. Ο Διαχειριστής αυτός εξασφαλίζει ότι η υπηρεσία η-τιμολόγησης θα μπορεί να κατανοεί τα η-τιμολόγια που υπακούουν σε διαφορετικά σχήματα και θα μπορεί να μεταφράζει τιμολόγια απο ένα σχήμα σε ένα άλλο.
- Ο *Διαχειριστής Προώθησης (Forward Manager)* υλοποιεί μια υπηρεσία προώθησης μηνυμάτων σύμφωνα με τις προδιαγραφές των παραγράφων 4.3.3.3.2.3 και 4.3.4.3.3.2.2.3. Ο Διαχειριστής αυτός λαμβάνει όλα τα μηνύματα που εμπεριέχουν η-τιμολόγια και τα αποστείλει στο σωστό προορισμό τους (σε άλλους οργανισμούς) χρησιμοποιώντας τους κατάλληλους μηχανισμούς ασφάλειας.

• Υπηρεσίες ασφάλειας

- Ο *Ελεγκτής πρόσβασης (Access controller)* υλοποιεί την υπηρεσία ελέγχου πρόσβασης με την λειτουργικότητα που περιγράφεται στις παραγράφους 4.3.3.3.3.5 και 4.3.4.3.3.2.3.2. Ο ελεγκτής κάνει ελέγχους σύμφωνα με τους κανόνες πολιτικών πρόσβασης των παραγράφων 5.2.3.3.1.4 και 5.2.3.3.2.5 και τα διαπιστευτήρια που του δίνονται μέσω του διαχειριστή πρόσβασης και τα οποία ελέγχει μέσω του Διαχειριστή Κλειδιών και Πιστοποιητικών.
- Ο *Διαχειριστής κλειδιών και πιστοποιητικών (Keys & Certificates Manager)* υλοποιεί μια υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών με την λειτουργικότητα που περιγράφεται στις παραγράφους 4.3.3.3.3.7 και 4.3.4.3.3.2.3.7. Όπως φαίνεται στο Σχήμα 5-33, οι μέθοδοι που υλοποιεί το αντικείμενο αυτό (έλεγχος κατάστασης πιστοποιητικών και λήψη χρονοσφραγίδων) συντελούνται σύμφωνα με τα δεδομένα που ανταλλάζει με μια εξωτερική ΥΔΚ με την οποία επικοινωνεί μέσω δύο καναλιών λειτουργιών.

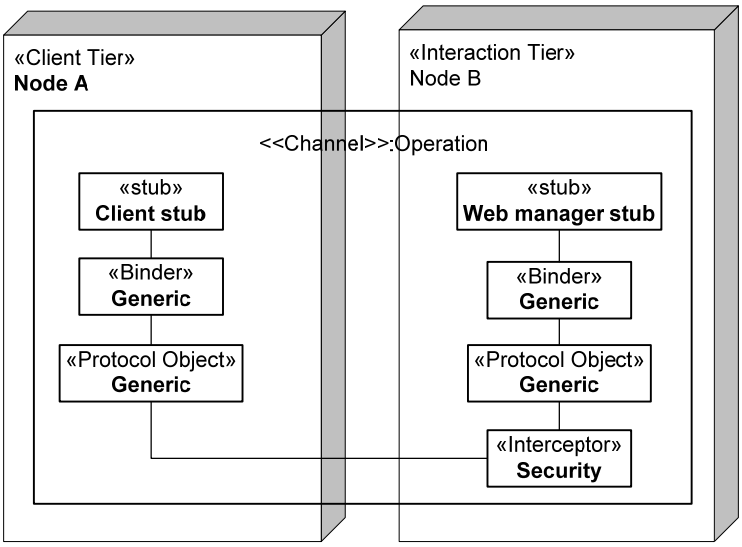
• *Επιχειρησιακή υπηρεσία η-τιμολόγησης*. Στο επίπεδο αυτό φιλοξενείται το μηχανικό αντικείμενο που υλοποιεί την επιχειρησιακή υπηρεσία η-τιμολόγησης. Το αντικείμενο επικοινωνεί με τον πυρήνα και τις βασικές υπηρεσίες της ΑΔΑΑΥ προκειμένου να υλοποιήσει τις προδιαγραφές της υπολογιστικής όψης του 4ου σταδίου. Επίσης, εξωτερικές οντότητες επικοινωνούν με την υπηρεσία μέσω ενός καναλιού λειτουργιών προκειμένου να της αποστείλουν η-τιμολόγια.

• Μια υπηρεσία υποστήριξης υπαρχουσών υποδομών υλοποιείται απο ένα μηχανικό αντικείμενο που δρα ως *Ενδιάμεσο επίπεδο προσαρμογής (Adaptation layer)*. Το αντικείμενο αυτό αποτελεί το κομμάτι της υπηρεσίας απο την πλευρά της αρχιτεκτονικής και επικοινωνεί με το αντίστοιχο αντικείμενο που αποτελεί το κομμάτι της υπηρεσίας που περιλαμβάνεται στον κόμβο D, σύμφωνα με την λογική

των παραγράφων 4.3.3.3.5 και 4.3.4.3.3.2.5. Τα δύο μέρη της υπηρεσίας επικοινωνούν μέσω ενός καναλιού λειτουργιών.

4. *Κόμβος D* στο επίπεδο ολοκλήρωσης. Στον κόμβο Ε περιλαμβάνεται το κομμάτι της υπηρεσίας υποστήριξης υπαρχουσών υποδομών που ολοκληρώνει οποιοδήποτε υπάρχον σύστημα / *Βάση δεδομένων (Legacy DB)* με στοιχεία για τιμολόγια. Η υπηρεσία υλοποιείται απο ένα αντικείμενο *Ενδιάμεσου επιπέδου προσαρμογής (Adaptation layer)*, το οποίο γνωρίζει πως να επικοινωνεί απο τη μια πλευρά με το αντίστοιχο αντικείμενο στον κόμβο C μέσω ενός καναλιού λειτουργιών, και απο την άλλη με το υπάρχον σύστημα μέσω ενός άλλου καναλιού λειτουργιών.

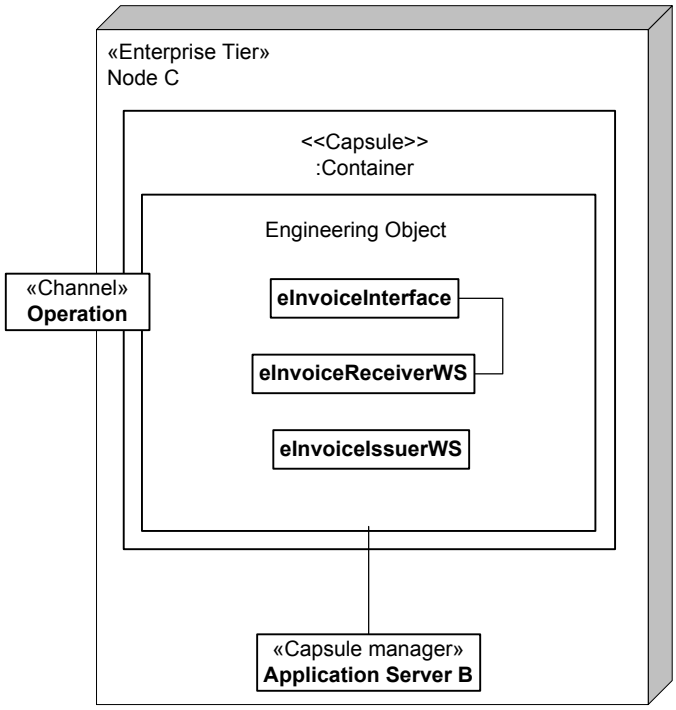
Όπως φαίνεται απο την παραπάνω ανάλυση, στο συγκεκριμένο παράδειγμα χρησιμοποιούνται μόνο κανάλια λειτουργιών. Το διάγραμμα λεπτομέρειας για το κανάλι μεταξύ της εφαρμογής πελάτη και του διαχειριστή ιστοσελίδων:



Σχήμα 5-34: Διαγράμματος λεπτομέρειας του καναλιού ανάμεσα στην εφαρμογή πελάτη και τον διαχειριστή ιστοσελίδων

Το σχήμα επιδεικνύει την γενική μορφή του καναλιού στην όψη μηχανικού σύμφωνα με τις αρχές της παραγράφου 4.3.5.3.3.1.3.2. Τα στελέχη για στο υψηλότερο επίπεδο επικοινωνίας υλοποιούνται απο τα μηχανικά αντικείμενα που επικοινωνούν και το κανάλι απαιτεί την ύπαρξη ενός αναχαιτιστή για την παροχή σε χαμηλό επίπεδο κατάλληλων μηχανισμών ασφάλειας (και άρα την κατάλληλη μετάφραση των δεδομένων ανάμεσα στα δύο αντικείμενα πρωτοκόλλου ώστε το ένα να αποδέχεται και να κατανοεί τα ασφαλή δεδομένα που του στέλνει το άλλο). **Όλα** τα κανάλια που περιέχονται στο συνολικό διάγραμμα εγκατάστασης έχουν την ίδια μορφή με το παραπάνω, και δεν επαναλαμβάνονται.

Οι προδιαγραφές της όψης μηχανικού ολοκληρώνονται με ένα διάγραμμα λεπτομέρειας στην όψη μηχανικού για το αντικείμενο της υπηρεσίας η-τιμολόγησης σε πλήρη αντιστοίχηση με τις προδιαγραφές της υπολογιστικής όψης, όπως φαίνεται στο :



Σχήμα 5-35: Διάγραμμα λεπτομέρειας για το μηχανικό αντικείμενο υπηρεσίας η-τιμολόγησης

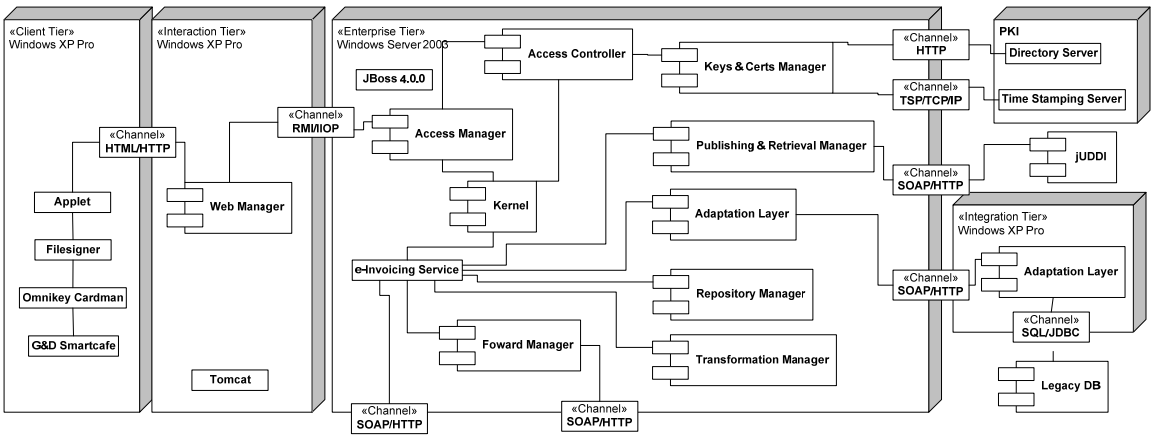
Παρατηρούμε ότι:

- Το αντικείμενο βρίσκεται στον κόμβο C.
- Εμπεριέχει τα τρία βασικά στοιχεία eInvoiceInterface, eInvoiceReceiverWS και eInvoiceIssuerWS, σε πλήρη αντιστοιχία με τα στοιχεία της υπολογιστικής όψης.
- Το αντικείμενο επικοινωνεί με τις απαραίτητες υπηρεσίες της αρχιτεκτονικής εσωτερικά στον κόμβο C, οπότε δεν εδραιώνονται κανάλια για αυτή την επικοινωνία. Η εξωτερική πρόσβαση στο eInvoiceReceiverWS γίνεται μέσω του eInvoiceInterface το οποίο δέχεται μηνύματα πάνω απο ένα κανάλι λειτουργιών.
- Το αντικείμενο λειτουργεί στον υποδοχέα του εξυπηρετητή εφαρμογών B.

Οι προδιαγραφές των μηχανικών αντικειμένων όλων των υπόλοιπων υπηρεσιών θεωρούνται δεδομένες και δεν αποτελούν μέρος της διατριβής.

5.2.3.6.2 Τεχνολογική Όψη

Το συνολικό διάγραμμα εγκατάστασης της τεχνολογικής όψης προκύπτει απο το διάγραμμα στο Σχήμα 5-33 το οποίο έχει εμπλουτιστεί με τεχνολογίες, όπως φαίνεται στο ακόλουθο σχήμα:



Σχήμα 5-36: Συνολικό διάγραμμα εγκατάστασης τεχνολογικής όψης αρχιτεκτονικής η-τιμολόγησης

Οι τεχνολογικές επιλογές που έχουν γίνει αναλύονται για κάθε κόμβο ως εξής:

1. Ο κόμβος Α στο επίπεδο πελάτη χρησιμοποιεί λειτουργικό Windows XP Pro. Η Εφαρμογή πελάτη (Client) θα υλοποιηθεί ως ένα java applet το οποίο θα τρέχει στους χρησιμοποιούμενους φυλλομετρητές που στην προκειμένη περίπτωση θα είναι Mozilla Firefox 1.5. Το applet επικοινωνεί με το servlet διαχείρισης ιστοσελίδων στον κόμβο Β ανταλλάσσοντας απλές HTML σελίδες πάνω απο HTTP. Το applet χρησιμοποιεί την βιβλιοθήκη Filesigner (βλ. και παράγραφο 3.2.2) για την παραγωγή ψηφιακών και προηγμένων ηλεκτρονικών υπογραφών με χρήση ενός αναγνώστη κάρτας Omnikey Cardman και μιας έξυπνης κάρτας G&D Smartcafe.
2. Ο κόμβος Β στο επίπεδο αλληλεπίδρασης χρησιμοποιεί λειτουργικό σύστημα Windows XP Pro. Ο κόμβος περιέχει έναν εξυπηρετητή εφαρμογών Tomcat στον οποίο ο Διαχειριστής ιστοσελίδων υλοποιείται με java servlets που δέχονται τις αιτήσεις πρόσβασης απο τα applets των χρηστών μέσω του καναλιού HTML/HTTP . Απο την άλλη πλευρά, τα servlets ανταλλάσσουν δεδομένα με τις εφαρμογές που τρέχουν στον εξυπηρετητή εφαρμογών του κόμβου C μέσω καναλιών RMI/IIOP (βλ. παράγραφο 4.3.5.4.5.1.2).
3. Ο κόμβος C στο πρώτο επιχειρησιακό επίπεδο χρησιμοποιεί λειτουργικό σύστημα Windows Server 2003 και περιέχει επίσης έναν εξυπηρετητή εφαρμογών JBoss 4.0.0. Ο κόμβος αυτός φιλοξενεί το μεγαλύτερο μέρος των υπηρεσιών διαχείρισης, τις βασικές υπηρεσίες, τις υπηρεσίες υποστήριξης υπαρχουσών υποδομών και τις υπηρεσίες ασφάλειας και οι τεχνολογικές επιλογές (βιβλιοθήκες, πρότυπα, προϊόντα) θεωρούνται αναλυμένα στις προδιαγραφές της συνολικής ΑΔΑΑΥ που φιλοξενεί την υπηρεσία η-τιμολόγησης. Συνοπτικά οι τεχνολογίες που προτείνονται για μια πιθανή ΑΔΑΑΥ είναι οι ακόλουθες:
   - Υπηρεσίες και μηχανισμοί διαχείρισης και συντονισμού:
     - Ο Διαχειριστής πρόσβασης επικοινωνεί με τα servlets του διαχειριστή ιστοσελίδων στον κόμβο Β μέσω ενός καναλιού RMI/IIOP.
   - Βασικές υπηρεσίες και μηχανισμοί
     - Ο Διαχειριστής δημοσίευσης και ανάκτησης επικοινωνεί με έναν κατάλογο υπηρεσιών ιστού UDDI μέσω ενός καναλιού SOAP/HTTP (βλ. παράγραφο 4.3.5.4.5.1.1). Ο κατάλογος UDDI που χρησιμοποιείται είναι μια υλοποίηση του λογισμικού ανοιχτού κώδικα jUDDI [jUDDI].

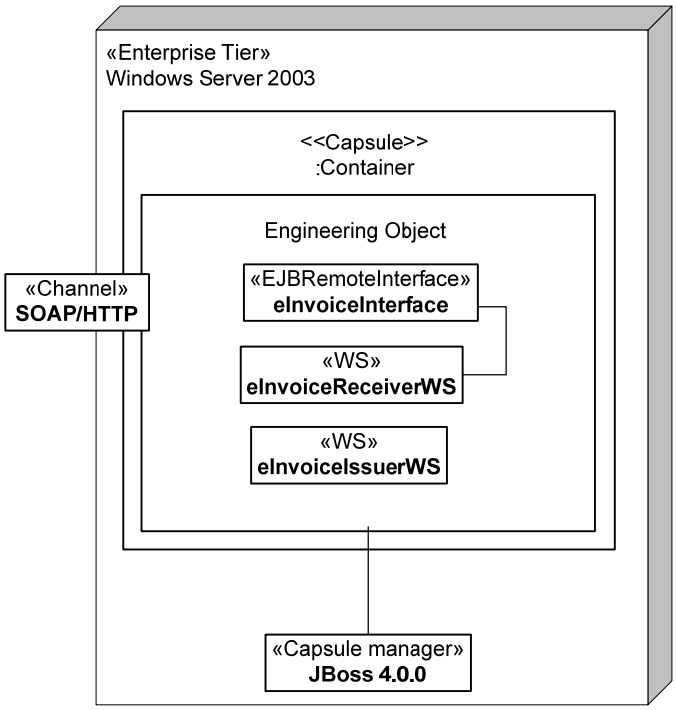
- Ο Διαχειριστής αποθετηρίων ελέγχεται απο μια επιχειρησιακή υπο-διεργασία στον κόμβο D μέσω ενός καναλιού SOAP/HTTP.

• Υπηρεσίες ασφάλειας
  - Ο Διαχειριστής κλειδιών και πιστοποιητικών χρησιμοποιεί το πρότυπο XKMS για να επικοινωνήσει με την ΥΔΚ μέσω ενός καναλιού SOAP/HTTP και το πρότυπο RFC 3161 για το πρωτόκολλο χρονοσφράγισης πάνω απο ένα κανάλι TSP/TCP/IP (βλ. παράγραφο 4.3.5.4.5.1.3).
  - Ο Διαχειριστής ελέγχου πρόσβασης χρησιμοποιεί το πρότυπο XACML για την διαχείριση και εφαρμογή των πολιτικών ελέγχου πρόσβασης.

• Η επιχειρησιακή υπηρεσία η-τιμολόγησης επικοινωνεί με αντικείμενα μέσα στον κόμβο αυτό για πρόσβαση στις εσωτερικές υπηρεσίες χωρίς την χρήση καναλιών. Ένα κανάλι SOAP/HTTP χρησιμοποιείται απο εξωτερικές οντότητες για να αποστείλουν η-τιμολόγια στην διεπαφή eInvoiceInterface της υπηρεσίας.

4. Ο κόμβος D στο επίπεδο ολοκλήρωσης χρησιμοποιεί λειτουργικό σύστημα Windows XP Pro. Το Ενδιάμεσο επίπεδο προσαρμογής επικοινωνεί απο τη μια πλευρά με το αντίστοιχο αντικείμενο στον κόμβο C μέσω ενός καναλιού RMI/IIOP, και απο την άλλη με την υπάρχουσα βάση δεδομένων μέσω ενός καναλιού SQL/JDBC/TCP/IP (βλ. παράγραφο 4.3.5.4.5.1.6).

Η παραπάνω ανάλυση θεωρεί ότι τα διαγράμματα λεπτομέρειας των καναλιών που αναφέρονται ότι χρησιμοποιούνται, είναι όπως παρουσιάζονται ως βασικά στοιχεία όψης στην παράγραφο 4.3.5.4.5.1.
Η τεχνολογική όψη του διαγράμματος λεπτομέρειας του σύνθετου αντικειμένου της υπηρεσίας τιμολόγησης είναι η ακόλουθη:



Σχήμα 5-37: Διάγραμμα λεπτομέρειας τεχνολογικής όψης αντικειμένου υπηρεσίας η-τιμολόγησης

Οι τεχνολογικές λεπτομέρειες του αντικειμένου της υπηρεσίας αναλύονται ως εξής:

- Το λειτουργικό σύστημα στον κόμβο που βρίσκεται το αντικείμενο είναι Windows Server 2003.
- Το αντικείμενο επικοινωνεί με άλλα αντικείμενα εκτός του κόμβου του μέσω ενός καναλιού SOAP/HTTP.
- Το αντικείμενο υλοποιεί την διεπαφή eInvoiceInterface που είναι μια διεπαφή απομακρυσμένης πρόσβασης (στο οποίο αποδίδεται το αντίστοιχο πρότυπο UML EJBRemoteInterface της αρχιτεκτονικής J2EE).
- Ο εξυπηρετητής εφαρμογών στον υποδοχέα του οποίου φιλοξενείται το αντικείμενο είναι ο JBoss 4.0.0.
- Στην υλοποίηση της υπηρεσίας η-τιμολόγησης έχουν χρησιμοποιηθεί οι ακόλουθες τεχνολογίες/πρότυπα/βιβλιοθήκες: η βιβλιοθήκη xCBL [xCBL03] για τον καθορισμό των σχημάτων των μηνυμάτων που ανταλλάσσονται ώστε να καλύπτεται η απαραίτητη πληροφορία που επιβάλλεται απο την οδηγία 2001/115/EC, την ανοιχτού κώδικα βιβλιοθήκη που έχει παραχθεί σε ένα πρόγραμμα η-διακυβέρνησης στην Εσθονία [EID03] για την παραγωγή προηγμένων ηλεκτρονικών υπογραφών (η βιβλιοθήκη έχει αναβαθμιστεί και τροποποιηθεί προκειμένου να συμμορφώνεται πλήρως με το πρότυπο XAdES [XAdES02]), το πρότυπο SOAP και οι επεκτάσεις ασφαλείας του WS-Security, και η εγγενής XML βάση δεδομένων eXist [Meier02] για την μακροπρόθεσμη αποθήκευση των τιμολογίων στην μορφή με την οποία έχουν αποσταλεί και ληφθεί.

Σημειώνεται ότι το παραπάνω διάγραμμα αντιστοιχεί πλήρως σε αυτό στο Σχήμα 5-35, ώστε να εξασφαλίζεται η συνέπεια ανάμεσα στην Όψη μηχανικού και την Τεχνολογική όψη.

5.2.3.7 6^{ο} Στάδιο: Υλοποίηση

Η υπηρεσία που προδιαγράφεται στο παρόν κεφάλαιο έχει υλοποιηθεί με την χρήση των ακόλουθων εργαλείων και περιβαλλόντων δημιουργίας λογισμικού σε Java:

- NetBeans IDE 5.0
- Eclipse IDE 3.1

Δημοσιεύσεις σχετικές με τον σχεδιασμό και την υλοποίηση είναι οι [Kaliontzoglou03, Kaliontzoglou06a, Kaliontzoglou06b, Kaliontzoglou06c]. Η αρχιτεκτονική της υπηρεσίας έχει επίσης συμπεριληφθεί στην αναφορά για την Ευρωπαϊκή ένωση της ομάδας εργασίας για την η-τιμολόγηση του οργανισμού CEN/ISSS [CEN03].

5.2.3.8 7^{ο} Στάδιο: Έλεγχος συμμόρφωσης και ενημέρωση προδιαγραφών

Το τελευταίο στάδιο εφαρμόζει το τελευταίο στάδιο της μεθοδολογίας προκειμένου να καταγράψει τα σημεία συμμόρφωσης της υπηρεσίας τιμολόγησης προκειμένου να μπορεί να αξιολογηθεί κατά πόσο η υλοποίηση της υπηρεσίας ανταποκρίνεται στις παρούσες

προδιαγραφές. Σύμφωνα με την μεθοδολογία η αποτύπωση αρχικά των σημείων αναφοράς ξεκινά με την όψη μηχανικού και συνεχίζει με την υπολογιστική όψη, την όψη πληροφορίας και την επιχειρησιακή όψη, με αυτή τη σειρά.

5.2.3.8.1 Σημεία συμμόρφωσης όψης μηχανικού

Ο παρακάτω πίνακας αναλύει τα σημεία αναφοράς της όψης μηχανικού και δηλώνει ποια απο αυτά καταγράφονται ως σημεία συμμόρφωσης.

Κατηγορία σημείου	**Αναγνωριστικό σημείου**	**Περιγραφή σημείου**	**Περιγραφή επιθυμητής λειτουργικότητας**	**Αποδοχή ως σημείο συμμόρφωσης**
Προγραμματιστικά	ΟΜΠ00	Ανάμεσα στο αντικείμενο eInvoiceInterface και το eInvoiceReceiverWS.		Ναι
	ΟΜΠ01	Ανάμεσα στο αντικείμενο eInvoiceInterface και τον εξυπηρετητή εφαρμογών Β.	Η εκκίνηση του αντικειμένου μέσα στον εξυπηρετητή γίνεται ομαλά.	Όχι
	ΟΜΠ02	Ανάμεσα στο αντικείμενο eInvoiceReceiverWS και τον εξυπηρετητή εφαρμογών Β.	Η εκκίνηση του αντικειμένου μέσα στον εξυπηρετητή γίνεται ομαλά.	Όχι
	ΟΜΠ03	Ανάμεσα στο αντικείμενο eInvoiceIssuerWS και τον εξυπηρετητή εφαρμογών Β.	Η εκκίνηση του αντικειμένου μέσα στον εξυπηρετητή γίνεται ομαλά.	Όχι
	ΟΜΠ04	Ανάμεσα στην υπηρεσία η-τιμολόγησης και τον πυρήνα της αρχιτεκτονικής.	Η υπηρεσία χρησιμοποιεί επιτυχώς όλες τις σχετικές μεθόδους του πυρήνα για την εκκίνησή της.	Ναι
	ΟΜΠ05	Ανάμεσα στην υπηρεσία η-τιμολόγησης και τον διαχειριστή δημοσίευσης και αναζήτησης.	Η υπηρεσία χρησιμοποιεί επιτυχώς όλες τις μεθόδους του διαχειριστή για αναζήτηση των περιγραφών άλλων υπηρεσιών.	Ναι
	ΟΜΠ06	Ανάμεσα στην υπηρεσία η-τιμολόγησης και το αντικείμενο ενδιάμεσου επιπέδου προσαρμογής.	Η υπηρεσία χρησιμοποιεί επιτυχώς όλες τις μεθόδους του ενδιάμεσου επιπέδου για αποστολή και λήψη πληροφοριών απο υπάρχουσες υποδομές.	Ναι
	ΟΜΠ07	Ανάμεσα στην υπηρεσία η-τιμολόγησης και τον διαχειριστή αποθετηρίων.	Η υπηρεσία χρησιμοποιεί επιτυχώς τις μεθόδους και λήψη	Ναι

			και αποθήκευση πληροφοριών σε αποθετήρια.	
	ΟΜΠ08	Ανάμεσα στην υπηρεσία η-τιμολόγησης και τον διαχειριστή μετασχηματισμού.	Η υπηρεσία χρησιμοποιεί επιτυχώς τις μεθόδους μετασχηματισμού.	Ναι
	ΟΜΠ09	Ανάμεσα στην υπηρεσία η-τιμολόγησης και τον διαχειριστή προώθησης.	Η υπηρεσία χρησιμοποιεί επιτυχώς τις μεθόδους προώθησης μηνυμάτων.	Ναι
	ΟΜΠ10	Ανάμεσα στα αντικείμενα πρωτοκόλλου του καναλιού λειτουργιών που χρησιμοποιεί η υπηρεσία η-τιμολόγησης και μια εξωτερική υπηρεσία.	Τα αντικείμενα πρωτοκόλλου ανταλλάσσουν επιτυχώς τα απαραίτητα μηνύματα.	Ναι
	ΟΜΠ11	Ανάμεσα στο αντικείμενο πρωτοκόλλου και τον δεσμευτή του καναλιού λειτουργιών που χρησιμοποιεί η υπηρεσία η-τιμολόγησης.	Ο δεσμευτής δεσμεύει επιτυχώς το στέλεχος στο αντικείμενο πρωτοκόλλου.	Ναι
	ΟΜΠ12	Ανάμεσα στο στέλεχος και τον δεσμευτή του καναλιού λειτουργιών που χρησιμοποιεί η υπηρεσία η-τιμολόγησης.	Ο δεσμευτής λαμβάνει επιτυχώς δεδομένα απο το στέλεχος.	Ναι
	ΟΜΠ13	Ανάμεσα στη διεπαφή eInvoiceInterface και το στέλεχος του καναλιού λειτουργιών που χρησιμοποιεί η υπηρεσία η-τιμολόγησης.	Οι μέθοδοι της διεπαφής ενεργοποιούνται επιτυχώς απο το στέλεχος σύμφωνα με τα δεδομένα που λαμβάνει.	Ναι
Διαλειτουργικά	ΟΜΔ00	Ανάμεσα στα αντικείμενα πρωτοκόλλου του καναλιού λειτουργιών που χρησιμοποιεί η υπηρεσία η-τιμολόγησης και μια εξωτερική υπηρεσία.	Τα μηνύματα που ανταλλάσσονται ανάμεσα στα δύο αντικείμενα είναι κατανοητά και απο τα δύο.	Ναι

Πίνακας 5-1: Σημεία συμμόρφωσης της Όψης Μηχανικού

5.2.3.8.2 Σημεία συμμόρφωσης υπολογιστικής όψης

Ο παρακάτω πίνακας αναλύει τα σημεία αναφοράς της υπολογιστικής όψης και δηλώνει ποια απο αυτά καταγράφονται ως σημεία συμμόρφωσης.

Κατηγορία σημείου	**Αναγνωριστικό σημείου**	**Περιγραφή σημείου**	**Περιγραφή επιθυμητής λειτουργικότητας**	**Αντίστοιχο σημείο όψης μηχανικού**	**Αποδοχή ως σημείο συμμόρφωσης**
Προγραμματιστικά	ΥΟΠ00	Ανάμεσα στην κλάση eInvoiceReceiverWS και την	Η κλάση eInvoiceReceiverWS χρησιμοποιεί επιτυχώς και με	ΟΜΠ04	Ναι

		κλάση XMLMessageHandler.	τα κατάλληλα ορίσματα τις μεθόδους της κλάσης XMLMessageHandler.		
	ΥΟΠ01	Ανάμεσα στην κλάση eInvoiceInterface και την κλάση XML MessageHandler.	Η κλάση eInvoiceInterface χρησιμοποιεί επιτυχώς και με τα κατάλληλα ορίσματα τις μεθόδους της κλάσης XMLMessageHandler.	ΟΜΠ04	Ναι
	ΥΟΠ02	Ανάμεσα στην κλάση InvoiceManager και στην κλάση eInvoice interface.	Και οι δύο κλάσεις χρησιμοποιούν επιτυχώς τις μεθόδους η μια της άλλης.	-	Ναι
Αντιληπτικά	ΥΟΑ00	Ανάμεσα στην κλάση InvoiceManager και την κλάση LoginPanel.	Ο χρήστης μπορεί να εισάγει επιτυχώς το PIN για την αυθεντικοποίησή του.	-	Ναι
	ΥΟΑ01	Ανάμεσα στην κλάση InvoiceManager και την κλάση ItemPanel.	Ο χρήστης μπορεί να διαχειριστεί επιτυχώς τις υπηρεσίες / προϊόντα που μπορούν να εισαχθούν σε ένα τιμολόγιο.	ΟΜΠ07, ΟΜΠ06	Ναι
	ΥΟΑ02	Ανάμεσα στην κλάση InvoiceManager και την κλάση UDDIPublisherPanel.	Ο χρήστης μπορεί να διαχειριστεί επιτυχώς την δημοσίευση της υπηρεσίας στον κατάλογο υπηρεσιών.	ΟΜΠ05	Ναι
	ΥΟΑ03	Ανάμεσα στην κλάση InvoiceManager και την κλάση BuyerPanel.	Ο χρήστης μπορεί να διαχειριστεί επιτυχώς τα στοιχεία των οργανισμών – παραληπτών τιμολογίων.	ΟΜΠ07, ΟΜΠ06	Ναι
	ΥΟΑ04	Ανάμεσα στην κλάση InvoiceManager και την κλάση InvoiceItemPanel.	Ο χρήστης μπορεί να διαχειριστεί επιτυχώς τις υπηρεσίες / προϊόντα που προστίθενται σε ένα συγκεκριμένο τιμολόγιο.	-	Ναι
	ΥΟΑ05	Ανάμεσα στην κλάση InvoiceManager και την κλάση IssuerPanel.	Ο χρήστης μπορεί να διαχειριστεί επιτυχώς τα στοιχεία του δικού του οργανισμού και πως αυτά αποθηκεύονται στον κατάλογο υπηρεσιών.	ΟΜΠ5	Ναι
	ΥΟΑ06	Ανάμεσα στην κλάση InvoiceManager και την κλάση SetupPanel.	Ο χρήστης μπορεί να διαχειριστεί επιτυχώς όλες τις παραμέτρους της υπηρεσίας.	-	Ναι
	ΥΟΑ07	Ανάμεσα στην κλάση InvoiceManager και την κλάση InvoicePanel.	Ο χρήστης μπορεί να διαχειριστεί επιτυχώς τα στοιχεία που εισάγονται σε ένα συγκεκριμένο τιμολόγιο.	-	Ναι

Πίνακας 5-2: Σημεία συμμόρφωσης της Υπολογιστικής Όψης

5.2.3.8.3 Σημεία συμμόρφωσης όψης πληροφορίας

Ο παρακάτω πίνακας αναλύει τα σημεία αναφοράς της όψης πληροφορίας και δηλώνει ποια απο αυτά καταγράφονται ως σημεία συμμόρφωσης.

Κατηγορία σημείου	Αναγνωριστικό σημείου	Περιγραφή σημείου	Περιγραφή επιθυμητής λειτουργικότητας	Αντίστοιχο σημείο όψης μηχανικού ή υπολογιστικής όψης	Αποδοχή ως σημείο συμμόρφωσης
Προγραμματιστικά	ΟΠΠ00	Ανάμεσα στην υπηρεσία η-τιμολόγησης και το αντικείμενο πληροφορίας η-τιμολόγιο.	Η δομή του η-τιμολογίου συμμορφώνεται στο σχήμα που έχει οριστεί.	ΟΜΠ07, ΟΜΠ06, ΥΟΑ07, ΟΜΠ09, ΥΟΑ01, ΥΟΑ03, ΥΟΑ04, ΥΟΑ05	Ναι
	ΟΠΠ01	Ανάμεσα στην υπηρεσία η-τιμολόγησης και το αντικείμενο πληροφορίας Μήνυμα Επιβεβαίωσης.	Η δομή του μηνύματος επιβεβαίωσης συμμορφώνεται με το σχήμα που έχει οριστεί.	ΟΜΠ09, ΟΜΠ07	Ναι
Διαλειτουργικά	ΟΠΔ00	Ανάμεσα σε δύο υπηρεσίες τιμολόγησης.	Οι δύο υπηρεσίες μπορούν να επεξεργαστούν επιτυχώς τα τιμολόγια που ανταλλάσσουν.	ΟΜΠ07, ΟΜΠ08, ΟΜΠ09, ΟΜΔ00	Ναι
	ΟΠΔ01	Ανάμεσα σε δύο υπηρεσίες τιμολόγησης.	Οι δύο υπηρεσίες μπορούν να επεξεργαστούν επιτυχώς τα μηνύματα επιβεβαίωσης που ανταλλάσσουν.	ΟΜΠ07, ΟΜΠ08, ΟΜΠ09, ΟΜΔ00	Ναι

Πίνακας 5-3: Σημεία συμμόρφωσης της Όψης Μηχανικού

5.2.3.8.4 Σημεία συμμόρφωσης επιχειρησιακής όψης

Ο παρακάτω πίνακας αναλύει τα σημεία αναφοράς της επιχειρησιακής όψης και δηλώνει ποια απο αυτά καταγράφονται ως σημεία συμμόρφωσης.

Κατηγορία σημείου	Αναγνωριστικό σημείου	Περιγραφή σημείου	Περιγραφή επιθυμητής λειτουργικότητας	Αντίστοιχο σημείο όψης μηχανικού ή υπολογιστικής όψης ή όψης πληροφορίας	Αποδοχή ως σημείο συμμόρφωσης
Προγραμματιστικά	ΕΟΠ00	Ανάμεσα στην υπηρεσία και το η-τιμολόγιο.	Το η-τιμολόγιο πρέπει να περιέχει την ελάχιστη ποσότητα και είδος πληροφορίας που απαιτείται απο την οδηγία.	ΟΠΠ00	Ναι
	ΕΟΠ01	Ανάμεσα στην υπηρεσία και τον μηχανισμό προηγμένων ηλεκτρονικών υπογραφών.	Η υπηρεσία θα πρέπει να χρησιμοποιεί προηγμένες ηλεκτρονικές υπογραφές για την υπογραφή των η-τιμολογίων.	ΥΟΑ00	Ναι
	ΕΟΠ02	Ανάμεσα στην υπηρεσία και το η-τιμολόγιο.	Η δομή του η-τιμολογίου θα πρέπει να είναι ορισμένη σε XML.	ΟΠΠ00	Ναι
	ΕΟΠ03	Ανάμεσα στην υπηρεσία και τους μηχανισμούς ψηφιακών υπογραφών και προηγμένων	Η υπηρεσία θα πρέπει να κάνει χρήση πιστοποιητικών X.509 αποθηκευμένων σε	ΥΟΑ00	Ναι

		ηλεκτρονικών υπογραφών.	κάρτες για τις ηλεκτρονικές υπογραφές, είτε αυτόνομα είτε μέσω κατάλληλης υπηρεσίας ΑΔΑΑΥ.		
	ΕΟΠ04	Ανάμεσα στην υπηρεσία και τους μηχανισμούς ψηφιακών υπογραφών και προηγμένων ηλεκτρονικών υπογραφών.	Η υπηρεσία θα πρέπει να ικανοποιεί τις απαιτήσεις ασφάλειας της οδηγίας για αυθεντικοποίηση προέλευσης και οντοτήτων, ακεραιότητα του περιεχομένου των τιμολογίων και μη-άρνηση συμμετοχής.	ΥΟΑ00	Ναι
	ΕΟΠ05	Ανάμεσα στην υπηρεσία και τον μηχανισμό κρυπτογράφησης.	Η υπηρεσία θα πρέπει να ικανοποιεί τις απαιτήσεις ασφάλειας της οδηγίας για μυστικότητα και ιδιωτικότητα.	-	Ναι
	ΕΟΠ06	Ανάμεσα στην υπηρεσία και τον διαχειριστή αποθετηρίων.	Η υπηρεσία θα πρέπει να ικανοποιεί την απαίτηση ασφάλειας της οδηγίας για ασφαλή αποθήκευση.	ΟΜΠ07	Ναι
	ΕΟΠ07	Ανάμεσα στην υπηρεσία και το ενδιάμεσο επίπεδο ολοκλήρωσης.	Η υπηρεσία θα πρέπει να ικανοποιεί την απαίτηση ασφάλειας της οδηγίας για ασφαλή αποθήκευση.	ΟΜΠ06	Ναι
	ΕΟΠ08	Ανάμεσα στην υπηρεσία και το δικτυακό περιβάλλον.	Η υπηρεσία θα πρέπει να ικανοποιεί την απαίτηση ασφάλειας της οδηγία για διαθεσιμότητα.	-	Ναι
	ΕΟΠ09	Ανάμεσα στην υπηρεσία και τον πυρήνα της αρχιτεκτονικής.	Η υπηρεσία θα πρέπει να επιτρέπει τον διαχωρισμό και την χρήση δυο διακριτών ρόλων.	ΟΜΠ04	Ναι
	ΕΟΠ10	Ανάμεσα στην υπηρεσία και το ενδιάμεσο επίπεδο ολοκλήρωσης.	Τα δεδομένα για τη σύνθεση και διαχείριση τιμολογίων θα μπορούν να ληφθούν απο υπάρχοντα συστήματα μέσω υπηρεσιών υποστήριξης υπαρχουσών υποδομών.	ΟΜΠ06	Ναι
Αντιληπτικά	ΕΟΑ00	Ανάμεσα στην υπηρεσία και τον χρήστη.	Η υπηρεσία θα πρέπει να υποστηρίζει την σύνθεση τιμολογίων και επεξεργασία τιμολογίων.	ΥΟΑ04, ΥΟΑ07	Ναι
	ΕΟΑ01	Ανάμεσα στην υπηρεσία και τον χρήστη.	Η υπηρεσία θα πρέπει να υποστηρίζει την αποθήκευση τιμολογίων.	ΟΜΠ06, ΟΜΠ07	Ναι
	ΕΟΑ02	Ανάμεσα στην υπηρεσία και τον χρήστη.	Η υπηρεσία θα πρέπει να υποστηρίζει την υπογραφή τιμολογίων.	ΥΟΑ00	Ναι
	ΕΟΑ03	Ανάμεσα στην υπηρεσία και τον χρήστη.	Η υπηρεσία θα πρέπει να υποστηρίζει την δημοσίευσή	ΥΟΑ02, ΟΜΠ05	Ναι

			της σε καταλόγους υπηρεσιών.		
	ΕΟΑ04	Ανάμεσα την υπηρεσία και τον χρήστη.	Η υπηρεσία θα πρέπει να υποστηρίξει την επεξεργασία οργανισμών παραληπτών τιμολογίων.	ΥΟΑ03	Ναι
	ΕΟΑ05	Ανάμεσα στην υπηρεσία και τον χρήστη.	Η υπηρεσία θα πρέπει να υποστηρίζει την επεξεργασία των υπηρεσιών / προϊόντων που μπορούν να συμπεριληφθούν σε ένα τιμολόγιο.	ΥΟΑ04	Ναι
Διαλειτουργικά	ΕΟΔ01	Ανάμεσα στην υπηρεσία και το η-τιμολόγιο.	Η δομή του η-τιμολογίου πρέπει να βασίζεται σε όσο το δυνατόν περισσότερα διαδεδομένα πρότυπα του ΄χωρου.	ΟΠΠ00	Ναι
	ΕΟΔ01	Ανάμεσα σε δύο υπηρεσίες η-τιμολόγησης.	Η υπηρεσία θα πρέπει να υποστηρίζει την ασφαλή ανταλλαγή τιμολογίων.	ΟΜΠ10, ΟΜΔ00	Ναι

Πίνακας 5-4: Σημεία συμμόρφωσης της Όψης Μηχανικού

Μετά την ολοκλήρωση της υλοποίησης, ο σχεδιασμός επιβάλλει τον έλεγχο όλων των σημείων που έχουν χαρακτηριστεί ως σημεία συμμόρφωσης στους παραπάνω πίνακες. Η συμμόρφωση ή μη σε κάποιο σημείο μπορεί να έχει ένα απο τα παρακάτω αποτελέσματα:

- Την διόρθωση της υλοποίησης ώστε να συμμορφώνεται πλήρως με τα παραπάνω.
- Την διόρθωση των προδιαγραφών και κατά συνέπεια την διόρθωση της υλοποίησης, χωρίς να επηρεαστούν τα σημεία συμμόρφωσης.
- Την διόρθωση των προδιαγραφών και κατά συνέπεια την διόρθωση της υλοποίησης, με ταυτόχρονη ενημέρωση των σημείων συμμόρφωσης.

Τα παραπάνω συνεχίζονται ως ότου η υλοποίηση συμμορφώνεται πλήρως με τις προδιαγραφές.

5.3 Υπηρεσία έκδοσης εγγράφων πιστοποίησης μητρώου διαμονής για Δήμους

5.3.1 Εισαγωγή

Με τον όρο *Μικρομεσαίοι Δημόσιοι Οργανισμοί (ΜΔΟ)* αναφερόμαστε σε δημόσιους οργανισμούς που έχουν τα ακόλουθα χαρακτηριστικά [Kaliontzoglou05]:
Οργανισμοί που καλύπτουν μια γεωγραφική περιοχή που εξυπηρετεί αρκετές χιλιάδες πολιτών και μπορεί να βρίσκεται σε αγροτικές ή απομακρυσμένες περιοχές. Ένα παράδειγμα είναι ένας δήμος σε ένα νησί.

- Οργανισμοί που καλύπτουν μια γεωγραφική περιοχή που εξυπηρετεί περίπου 500.000 πολίτες και που συνήθως βρίσκονται σε αστικές περιοχές. Παραδείγματα τέτοιων οργανισμών είναι μεγαλύτεροι δήμοι σε πόλεις ή επιμελητήρια που λειτουργούν υπό νομικό καθεστώς δημοσίου.
- Οργανισμοί που αλληλεπιδρούν συχνά με πολίτες ή / και επιχειρήσεις προκειμένου να παρέχουν υπηρεσίες, ηλεκτρονικές ή βασισμένες στο χαρτί, διαθέτοντας έναν περιορισμένο αριθμό διαθέσιμων πόρων (σε εργαζομένους και χρήματα).
- Οργανισμοί που αλληλεπιδρούν μεταξύ τους σε τοπικές ή διασυνοριακές συναλλαγές, προκειμένου να ανταλλάξουν πληροφορίες εκ μέρους πολιτών, επιχειρήσεων ή του ίδιου του κράτους.

Ο αριθμός των μικρομεσαίων δημόσιων οργανισμών σε σύγχρονες δομές είναι μεγάλος διότι απο τη φύση τους είναι κατανεμημένοι και καλύπτουν μικρές περιοχές δημόσιας διοίκησης. Οι ΜΔΟ εξυπηρετούν ως ο σύνδεσμος με τα υψηλότερα επίπεδα της διακυβέρνησης που αποτελούνται απο μεγαλύτερους δημόσιους οργανισμούς όπως είναι τα υπουργία. ΜΔΟ που είναι επαρκώς εξοπλισμένοι και καλώς οργανωμένοι μπορούν να εξασφαλίσουν ότι όλοι οι πολίτες σε αγροτικές και μητροπολιτικές περιοχές λαμβάνουν υπηρεσίες υψηλής ποιότητας.
Προκειμένου να υποστηρίξουν την ποιότητα των υπηρεσιών, οι ΜΔΟ πρέπει να λύσουν το πρόβλημα της αποδοτικής και ασφαλούς ηλεκτρονικής ανταλλαγής δεδομένων και δημοσίων εγγράφων, με έναν τρόπο που είναι εύκολα προσβάσιμος απο τους πολίτες, τις επιχειρήσεις και άλλους δημόσιους οργανισμούς.
Ένας απο τους πλέον σημαντικούς ΜΔΟ που υπάρχει σε κάθε σύγχρονη και κοινωνία είναι ο δήμος. Τα τελευταία χρόνια οι δήμοι έχουν έρθει στο προσκήνιο της η-διακυβέρνησης παγκοσμίως λόγω της συχνότατης επικοινωνίας που έχουν με πολίτες και της αναγνωρισμένης παραπάνω ανάγκης για αναβάθμιση των υπηρεσιών τους.
Πιο συγκεκριμένα, η έκδοση και διανομή δημόσιων εγγράφων πιστοποίησης (π.χ. πιστοποιητικό γάμου, θανάτου, γέννησης, διαμονής κ.λ.π) κατατάσσεται ανάμεσα στις πρώτες προτεραιότητες για παροχή απο δήμους παγκοσμίως, κάτι που φαίνεται απο τα αποτελέσματα σημαντικών πρωτοβουλιών όπως το e-Gif που λειτουργεί απο το UK Office of the e-Envoy [Govtalk], το SAGA στη Γερμανία [SAGA03], καθώς και τα αποτελέσματα ερευνών που έχουν διεξαχθεί όπως το eMayor [eMayorD2.1] και το FASME [FASME].

5.3.2 Τρέχουσα κατάσταση υπηρεσιών η-διακυβέρνησης για ΜΔΟ

Οι αρχικές προσεγγίσεις στην περιοχή της παροχής υπηρεσιών η-διακυβέρνησης για ΜΔΟ έγινε σε παγκόσμια κλίμακα με κεντροποιημένες εγκαταστάσεις όπως είναι οι Πύλες Διαδικτύου (Web Portals). Μια τέτοια προσέγγιση είναι κατάλληλη για περιπτώσεις που επικεντρώνονται στην διανομή και αναζήτηση περιεχόμενου. Είναι παρ' όλα αυτά δύσκολο να υλοποιηθούν υπηρεσίες με πολύπλοκη ροή εργασιών ή υπηρεσίες με προηγμένα χαρακτηριστικά ασφάλειας όπως είναι οι ψηφιακές υπογραφές (κυρίως λόγω των περιορισμένων δυνατοτήτων των φυλλομετρητών).
Οι κατανεμημένες εγκαταστάσεις υπηρεσιών η-διακυβέρνησης είναι πιο κατάλληλες για να αντιμετωπίσουν τέτοιου είδους θέματα. Οι πλατφόρμες η-διακυβέρνησης που περιέχουν κατανεμημένα στοιχεία (όπως συγκεκριμένες εφαρμογές, πύλες, εξυπηρετητές, βάσεις δεδομένων) είναι σε θέση να διαχειριστούν πολύπλοκες διαδικασίες ροής εργασιών. Στην Ευρώπη υπάρχουν αρκετές τέτοιες προσεγγίσεις [Kaliontzoglou05] που δεν αντιμετωπίζουν όμως πλήρως τις ακόλουθες απαιτήσεις:

- Την διαλειτουργικότητα ανάμεσα σε σύγχρονες και μελλοντικές πλατφόρμες η-διακυβέρνησης με την χρήση ευρέως διαδεδομένων προτύπων. Πολλές υλοποιήσεις είναι καθαρά τοπικού χαρακτήρα.
- Την ευελιξία να καλύψουν τις ιδιαίτερες απαιτήσεις οργανισμών που είναι ΜΔΟ, επειδή όλες οι υλοποιήσεις προϋποθέτουν ότι όλοι οι δημόσιοι οργανισμοί έχουν τις ίδιες ανάγκες ανεξάρτητα απο το μέγεθός τους, την θέση τους και τον τύπο των υπηρεσιών που προσφέρουν.
- Την εδραίωση διασυνοριακών αλυσίδων υπηρεσιών και εμπιστοσύνης, στις οποίες οι υπηρεσίες η-διακυβέρνησης μπορούν να προσφερθούν μέσα απο την κατάλλήλη χρήση τεχνολογιών ασφάλειας όπως είναι οι ΥΔΚ στις οποίες πολλές κυβερνήσεις έχουν επενδύσει.
- Την συμμόρφωση με τα σχετικά πλαίσια πολιτικών και θεσμών που κυβερνούν όλες τις λύσεις τέτοιου τύπου στις χώρες που εφαρμόζονται, καθώς και με πλαίσια άλλων χωρών με τις οποίες είναι επιθυμητές οι διασυνοριακές συναλλαγές.

Ένας απο τους ΜΔΟ που απαντώνται σε όλες σύγχρονες κοινωνίες και που έχει όλες τις παραπάνω απαιτήσεις είναι ο δήμος. Σε ευρωπαϊκό επίπεδο, αρκετοί δήμοι έχουν συμμετέχει τα τελευταία χρόνια στην προσπάθεια εκσυγχρονισμού στα πλαίσια των κυβερνητικών προσπαθειών για η-δημοκρατία και η-διακυβέρνηση. Τα χαρακτηριστικά που αναφέρθηκαν παραπάνω για τους ΜΔΟ καθώς και των υπαρχουσών προσεγγίσεων οδηγούν στο συμπέρασμα ότι ένας δήμος μπορεί να επωφεληθεί απο την υιοθέτηση μιας ΑΔΑΑΥ η οποία θα αναλάβει:

- να φιλοξενήσει τις επιχειρησιακές υπηρεσίες του δήμου, τόσο για την διενέργεια των εσωτερικών του διεργασιών, όσο και για την παροχή υπηρεσιών σε πολίτες και επιχειρήσεις.
- την επικοινωνία με άλλους δήμους για ανταλλαγή πληροφοριών, τόσο σε τοπικό επίπεδο στην ίδια πόλη, όσο και ανάμεσα σε διαφορετικές πόλεις στην ίδια χώρα ή και σε διαφορετικές χώρες.
- την υποστήριξη υπαρχουσών υποδομών που ενδεχομένως ήδη διαθέτει ο δήμος.

- την παροχή του απαραίτητου επιπέδου ασφάλειας σε όλες τις διεργασίες και συναλλαγές.

Στα πλαίσια αυτά, το παρόν κεφάλαιο παρουσιάζει τις προδιαγραφές μιας προηγμένης ασφαλούς επιχειρησιακής υπηρεσίας έκδοσης εγγράφων πιστοποίησης μητρώου διαμονής, οι οποίες προκύπτουν με εφαρμογή της μεθόδου του κεφαλαίου 4. Η υπηρεσία αυτή μπορεί να διαμορφωθεί κατάλληλα και να γενικευθεί ώστε να υποστηρίζει κάθε είδος πιστοποιητικού που έχει αντίστοιχες απαιτήσεις ή εμπλέκεται σε παρόμοιες διαδικασίες, όπως πιστοποιητικά γέννησης, γάμου κ.λ.π., κάτι που αντιπροσωπεύει σημαντικό κομμάτι των επιχειρησιακών διεργασιών που επιτελούνται σε έναν δήμο.

5.3.3 Προδιαγραφές ασφαλούς επιχειρησιακής υπηρεσίας έκδοσης εγγράφων πιστοποίησης μητρώου διαμονής για Δήμους

5.3.3.1 Περιγραφή υπηρεσίας

Η υπηρεσία υλοποιεί την ασφαλή έκδοση και διανομή εγγράφων πιστοποίησης μητρώου διαμονής. Στην παρούσα περιγραφή χρησιμοποιείται ο όρος «έγγραφο πιστοποίησης» για την απόδοση της έννοιας ενός πιστοποιητικού μητρώου διαμονής, προκειμένου να μην υπάρχει σύγχυση με τα πιστοποιητικά ασφάλειας μιας υποδομής δημοσίου κλειδιού όπως για παράδειγμα αυτά που συμμορφώνονται με το πρότυπο X.509.
Η υπηρεσία επιτρέπει την ασφαλή δημιουργία, έκδοση και παράδοση (σε πολίτες ή άλλους δήμους) ψηφιακά υπογεγραμμένων εγγράφων πιστοποίησης μητρώου διαμονής. Ο σκοπός της είναι να επιτρέψει σε έναν πολίτη ή έναν αντιπρόσωπό του (που μπορεί να είναι ένας άλλος πολίτης ή ένας δημόσιος υπάλληλος) να ολοκληρώσει ηλεκτρονικά μια ασφαλή αίτηση για ένα έγγραφο πιστοποίησης, άσχετα με το που ο πολίτης αυτός βρίσκεται.
Οι διαδικασίες που υλοποιούνται στην υπηρεσία πρέπει να είναι οι ακόλουθες:

- Κάθε χρήστης της υπηρεσίας έχει πρόσβαση σε αυτήν απο τον δικτυακό τόπο του δήμου που την φιλοξενεί και προκειμένου να την χρησιμοποιήσει υπόκειται σε διαδικασίες αυθεντικοποίησης και ελέγχου πρόσβασης σύμφωνα με διαπιστευτήρια που περιέχονται στην έξυπνη κάρτα που διαθέτει. Την κάρτα μπορεί να του την παρέχει ο δήμος ή κάποια άλλη δημόσια ή ιδιωτική Αρχή Πιστοποίησης.
- Ο πολίτης συμπληρώνει μια συγκεκριμένη φόρμα που αναπαριστά την αίτηση για το έγγραφο πιστοποίησης, την υπογράφει ψηφιακά με χρήση των κλειδιών που περιέχονται στην έξυπνη κάρτα του.
- Ο πολίτης στην αίτησή του συμπληρώνει το ονοματεπώνυμο του ατόμου για το οποίο θα δημιουργηθεί το πιστοποιητικό, την ηλικία του, καθώς και τον δήμο απο τον οποίο θέλει να εκδοθεί το έγγραφο πιστοποίησης και απο ποιον δήμο θέλει να το λάβει. Αυτό καλύπτει την περίπτωση στην οποία ο πολίτης βρίσκεται (χωρικά) σε άλλο δήμο απο αυτόν που μπορεί να εκδώσει το πιστοποιητικό εντός της ίδιας χώρας ή και σε διαφορετική χώρα. Στην τελευταία περίπτωση, μαζί με το αρχικό έγγραφο πιστοποίησης, η υπηρεσία παραδίδει και μια πιστή υπογεγραμμένη μετάφραση του

εγγράφου στην μορφή και γλώσσα του δήμου και της χώρας στην οποία αυτό παραδίδεται για χρήση.

- Η υπηρεσία προωθεί την αίτηση είτε σε έναν δημόσιο υπάλληλο στην ίδιο τον δήμο για εξυπηρέτηση, ή σε μια αντίστοιχη υπηρεσία σε έναν άλλο δήμο αν έτσι ορίζεται στην αίτηση.
- Ένας δημόσιος υπάλληλος που εργάζεται στο δήμο και είναι υπεύθυνος για την διεκπεραίωση τέτοιων υποθέσεων λαμβάνει την αίτηση και βάσει των στοιχείων που περιέχει την αποδέχεται ή την απορρίπτει. Στην δεύτερη περίπτωση αιτιολογεί την απόφασή του με εκκίνηση της έκδοσης ενός *έγγράφου πιστοποίησης αρνητικής απάντησης*.
- Όταν λάβει μια εγκεκριμένη αίτηση για έγγραφο πιστοποίησης, η υπηρεσία αναλαμβάνει να δημιουργήσει μια αναζήτηση στο σύστημα του δήμου (βάση δεδομένων) που περιέχει τα στοιχεία όλων των πολιτών για τα οποία είναι υπεύθυνος ο συγκεκριμένος δήμος. Αν βρει τον συγκριμένο πολίτη, δημιουργεί το αντίστοιχο *έγγραφο πιστοποίησης (θετικής απάντησης)* και το προωθεί στον δημόσιο υπάλληλο για υπογραφή. Αν όχι δημιουργεί ένα έγγραφο πιστοποίησης αρνητικής απάντησης που πιστοποιεί ότι ο συγκεκριμένος πολίτης δεν είναι εγγεγραμμένος στον δήμο και το προωθεί επίσης στον δημόσιο υπάλληλο για υπογραφή.
- Ο δημόσιος υπάλληλος που λαμβάνει έγγραφα πιστοποίησης, είτε με τα στοιχεία διαμονής (θετικής απάντησης) είτε με την ένδειξη ότι ο πολίτης δεν είναι καταχωρημένος ή κάποιον άλλο λόγο απόρριψης (αρνητικής απάντησης), τα υπογράφει και επιλέγει την πρόοδο στο επόμενο στάδιο της εξυπηρέτησης: η υπηρεσία είτε αποθηκεύει το έγγραφο ή το προωθεί σε αντίστοιχη υπηρεσία τον δήμο απο τον οποίο έχει οριστεί να ληφθεί το έγγραφο.
- Όταν ένα έγγραφο προωθείται απο έναν δήμο σε έναν άλλο, τότε μετατρέπεται σε μια μορφή κοινή σε όλες τις σχετικές υπηρεσίες η οποία αποστέλλεται μαζί με την αρχική (υπογεγραμμένη μορφή του εγγράφου). Η υπηρεσία στον δήμο που την λαμβάνει την μετατρέπει αυτόματα στην τοπική μορφή του δήμου και προωθεί αυτή την μετάφραση σε έναν δημόσιο υπάλληλο για υπογραφή.
- Όταν ένα έγγραφο πιστοποίησης αποθηκεύεται, η υπηρεσία αυτόματα στέλνει μια ειδοποίηση στον ενδιαφερόμενο πολίτη, για να τον ενημερώσει ότι μπορεί να λάβει ηλεκτρονικά το έγγραφο χρησιμοποιώντας την ίδια την υπηρεσία.
- Ο πολίτης εφόσον έχει λάβει την αντίστοιχη ειδοποίησης μπορεί να λάβει το έγγραφο πιστοποίησης και να το κατεβάσει στον υπολογιστή του.

Συγκεκριμένοι περιορισμοί της υπηρεσίας είναι οι ακόλουθοι:

- Οι υπογραφές των εγγράφων υπηρεσία πρέπει να υπακούουν στο πρότυπο των προηγμένων ηλεκτρονικών υπογραφών με μια δεδομένη πολιτική υπογραφής.
- Κάθε έγγραφο που έχει εκδοθεί, παραμένει αποθηκευμένο για 10 μέρες απο την υπηρεσία. Στην συνέχεια διαγράφεται. Ο πολίτης θα ενημερώνεται για το διάστημα αυτό με την ειδοποίηση που λαμβάνει.

Στην συνέχεια παρουσιάζονται τα επτά στάδια εφαρμογής της μεθόδου του κεφαλαίου 4, με τις προδιαγραφές που προκύπτουν απο κάθε στάδιο.

5.3.3.2 1ο Στάδιο: Έλεγχος κριτηρίων ΑΔΑΑΥ

Στο στάδιο αυτό ελέγχεται αν η υπηρεσία εμφανίζει όλες εκείνες τις απαιτήσεις που χαρακτηρίζουν μια επιχειρησιακή υπηρεσία που μπορεί να σχεδιαστεί με βάση της αρχές μιας ΑΔΑΑΥ και μπορεί να φιλοξενηθεί σε αυτήν.

5.3.3.2.1 Διαλειτουργικότητα και κλιμάκωση

Οι απαιτήσεις διαλειτουργικότητας της υπηρεσίας μπορούν να διαχωριστούν σε απαιτήσεις για επικοινωνία με άλλες οντότητες (πολίτες μέσω φυλλομετρητών, επιχειρήσεις μέσω φυλλομετρητών ή Υπηρεσιών Ιστού, άλλοι δημόσιοι οργανισμοί στην ίδια ή σε άλλη χώρα μέσω φυλλομετρητών ή Υπηρεσιών Ιστού) που περιλαμβάνει τις δομές των ανταλλασσόμενων μηνυμάτων και τα πρωτόκολλα που χρησιμοποιούνται σε όλα τα επίπεδα επικοινωνίας, σε απαιτήσεις για διαλειτουργικότητα ηλεκτρονικών υπογραφών και των αντίστοιχων πολιτικών ιδιωτικότητας.

Επίσης δεδομένου ότι ο αριθμός τόσο των δήμων όσο και των οντοτήτων που συναλλάσσονται μαζί τους είναι αυξανόμενος, είναι απαραίτητη η μελέτη των παραμέτρων κλιμάκωσης της επιχειρησιακής υπηρεσίας. Ανάλογα με το μέγεθος του δήμου που θα την φιλοξενήσει, η υπηρεσία θα πρέπει να μπορεί να υποστηρίζει μέχρι και 20.000 συναλλαγές ημερησίως, σε 24ωρη βάση. Η υπηρεσία αυτή δεν θεωρείται κρίσιμη παρ' όλα αυτά, οπότε μια διαθεσιμότητα της τάξεως του 90% θεωρείται κατάλληλη.

5.3.3.2.2 Ασφάλεια και εμπιστοσύνη

Οι απαιτήσεις για ασφάλεια προκύπτουν απο τις βέλτιστες πρακτικές στον τομέα της η-διακυβέρνησης, τις επιταγές τις Ευρωπαϊκής Ένωσης στην περιοχή των ηλεκτρονικών υπογραφών και την περιγραφή της ίδιας της υπηρεσίας. Κατ' ελάχιστο, θα πρέπει να υποστηρίζεται η αυθεντικοποίηση οντοτήτων, η ακεραιότητα, η μη-άρνηση συμμετοχής σε συναλλαγές, η μυστικότητα και η ιδιωτικότητα.

5.3.3.2.3 Ανοιχτότητα και κατανομή

Η υπηρεσία έχει απαιτήσεις ανοιχτότητας όσο αφορά στην διασύνδεση των δομικών της στοιχείων μεταξύ τους καθώς και με τις υπόλοιπες υπηρεσίες που χρειάζεται και πρέπει να παρέχονται απο την αρχιτεκτονική που την φιλοξενεί (όπως π.χ. υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών, ελέγχου πρόσβασης, πρόσβασης σε καταλόγους υπηρεσιών κ.λ.π.). Επίσης είναι σημαντικό να διευκολύνεται η αλλαγή δομικών στοιχείων της ίδιας της υπηρεσίας χωρίς να επηρεάζεται όσο το δυνατόν η υπηρεσία στο σύνολό της.

5.3.3.2.4 Σεβασμός της αντίληψης του χρήστη

Ο σεβασμός της αντίληψης του χρήστη (είτε είναι πολίτης είτε δημόσιος υπάλληλος) για την συγκεκριμένη υπηρεσία είναι σημαντική παράμετρος ως προς τα ακόλουθα χαρακτηριστικά:

- πρέπει να είναι εξαιρετικά φιλική στις βασικές λειτουργίες δημιουργίας μιας αίτησης, διαχείρισης (αποδοχής / απόρριψης) και λήψης εγγράφου πιστοποίησης.
- πρέπει να δίνει στον χρήστη να κατανοεί την εφαρμογή των προηγμένων ηλεκτρονικών υπογραφών που απαιτούνται απο την σχετική Οδηγία (π.χ. να μπορεί ανα πάσα στιγμή να γνωρίζει τι υπογράφει), χωρίς να τον εμπλέκει σε τεχνικές λεπτομέρειες.

- εφόσον αναφέρεται στο σύνολο του πληθυσμού μιας χώρας, πρέπει να λαμβάνει υπόψην τις απαιτήσεις ομάδων πολιτών με ιδιαίτερα χαρακτηριστικά, όπως ηλικιωμένους, ανθρώπους με κινητικές δυσκολίες, ανθρώπους με χαμηλή επαφή με την τεχνολογία.
- θα πρέπει να υποστηρίζει την εύκολη παραμετροποίηση σε άλλες γλώσσες εφόσον στοχεύει στην υλοποίηση διασυνοριακών συναλλαγών εγγράφων πιστοποίησης.

Σημαντική παράμετρος είναι ότι σε κάθε επαφή με χρήστη πρέπει να χρησιμοποιούνται αποκλειστικά όλοι ευρέως διαδεδομένοι φυλλομετρητές ιστού, προκειμένου ο χρήστης να μην χρειάζεται να εκπαιδευτεί σε νέες εφαρμογές. Επιπλέον λογισμικό στην πλευρά του χρήστη επιτρέπεται αλλά θα πρέπει να περιοριστεί στο ελάχιστο δυνατό, και να είναι εξαιρετικά απλή η λήψη και εγκατάστασή του.

5.3.3.2.5 Ελαχιστοποίηση απαιτήσεων κόστους, πόρων - αυτοματοποίηση

Η ελαχιστοποίηση απαιτήσεων κόστους αποτελεί σημαντική απαίτηση για κάθε ΜΔΟ, λόγω του μικρού αριθμού διαθέσιμων πόρων που χαρακτηρίζουν τέτοιους οργανισμούς, τόσο σε ανθρώπινο δυναμικό (διεκπεραίωση διεργασιών, τεχνογνωσία) όσο και σε υλικό (υποδομή, ηλεκτρονικά μέσα). Η παρούσα υπηρεσία έχει την δυνατότητα να αυξήσει την αποδοτικότητα μιας αντίστοιχης μεθόδου που βασίζεται αποκλειστικά στο χαρτί, ειδικά στην περίπτωση που ως μέρος της επιλογής τεχνολογιών χρησιμοποιείται λογισμικό ανοιχτού κώδικα. Επίσης υπάρχει το γεγονός ότι η υπηρεσία είναι εύκολα παραμετροποιήσιμη, την καθιστά εξαιρετικά φιλική ως προς το κόστος για έναν δήμο, εφόσον μπορεί να χρησιμοποιηθεί για την παραγωγή ενός συνόλου άλλων αντίστοιχων υπηρεσιών που έχουν ως στόχο την παραγωγή ψηφιακά υπογεγραμμένων εγγράφων πιστοποίησης για διάφορους σκοπούς. Τέλος ανήκει στην κατηγορία των υπηρεσιών που οδηγούν σε αυτοματοποίηση των διαδικασιών που επιτελούν εφόσον ένα κομμάτι της επιχειρησιακής δραστηριότητας που αντικαθιστά, επιτελείται αποκλειστικά απο αυτήν (αναζήτηση ε βάσεις δεδομένων, ενημέρωση χρηστών για αποτελέσματα διαδικασίας κ.λ.π).

5.3.3.2.6 Ενσωμάτωση υπαρχουσών υποδομών

Δήμοι που έχουν ήδη εγκαταστήσει παλαιότερες υποδομές, φυλάσσουν σε αυτές την πληροφορία για τα στοιχεία διαμονής των πολιτών. Τα στοιχεία αυτά είναι απαραίτητα στην παρούσα υπηρεσία προκειμένου να συντάξει ένα έγγραφο πιστοποίησης μητρώου διαμονής. Επομένως η υπηρεσία θα πρέπει να δίνει τη δυνατότητα για άντληση των αντίστοιχων δεδομένων απο τις υπάρχουσες αυτές υποδομές.

5.3.3.2.7 Σεβασμός στις επιχειρηματικές ανάγκες και τις πολιτικές του οργανισμού

Το νομικό πλαίσιο που διέπει τις δραστηριότητες ενός δήμου είναι πολύπλοκο, και πρέπει να μελετηθεί εξονυχιστικά εάν πρόκειται να υιοθετηθεί μια τέτοια υπηρεσία, προκειμένου να μην υπάρχουν διαφωνίες με το υπάρχον νομικό και θεσμικό πλαίσιο. Η παροχή της υπηρεσίας αυτής για διασυνοριακές συναλλαγές υπαγορεύει μια προεργασία ανάμεσα στους δήμους που θέλουν να συνδεθούν ώστε οι πολιτικές που εφαρμόζει ο καθένας να ταιριάζουν (αυτό αποτελεί σημαντικό πρόβλημα σε κάθε τέτοιου είδους

συναλλαγή και επί του παρόντος υπαγορεύει πολλές φορές την αλλαγή του θεσμικού πλαισίου, κάτι που είναι εκτός ενδιαφέροντος της παρούσας διατριβής).
Το διαδικαστικό κομμάτι της υπηρεσίας έκδοσης των εγγράφων πιστοποίησης μητρώου διαμονής μπορεί να αποτυπωθεί με ακρίβεια και να βελτιωθεί ώστε να καλύπτονται πλήρως οι επιχειρηματικές ανάγκες του δήμου ως προς την συγκεκριμένη υπηρεσία.

Όπως φαίνεται απο τα παραπάνω, το σύνολο των απαιτήσεων της υπηρεσίας έκδοσης εγγράφων πιστοποίησης μητρώου διαμονής για δήμους, είναι υποσύνολο των απαιτήσεων της ΑΔΑΑΥ όπως παρουσιάζονται στην μεθοδολογία. Άρα αποφαινόμαστε ότι η υπηρεσία είναι κατάλληλη για ενσωμάτωση σε μια ΑΔΑΑΥ. Η ΑΔΑΑΥ όπως περιγράφηκε στο προηγούμενο κεφάλαιο μπορεί να εμπεριέχει όλες εκείνες τις υπηρεσίες πάνω στις οποίες μπορεί να βασιστεί και να χρησιμοποιήσει η υπηρεσία δόσης εγγράφων προκειμένου να καλύψει όλες τις απαιτήσεις της. Στην συνέχεια της ανάλυσης τον προδιαγραφών λοιπόν, θεωρούμε ότι **η υπηρεσία φιλοξενείται σε μια ΑΔΑΑΥ που παρέχει ένα δεδομένο σύνολο υπηρεσιών**. Το ακριβές σύνολο θα προδιαγραφεί στο 3^{ο} στάδιο της μεθόδου, βάσει της περιγραφής της υπηρεσίας και της ανάλυσης των επιχειρησιακών απαιτήσεων και διεργασιών που ακολουθεί (2^{ο} στάδιο).

5.3.3.3 2ο Στάδιο: Ανάλυση επιχειρησιακών απαιτήσεων και διεργασιών

Ακολουθώντας τα βήματα της μεθόδου πρέπει πρώτα να προδιαγράψουμε την επιχειρησιακή όψη της υπηρεσίας έκδοσης εγγράφων πιστοποίησης και στη συνέχεια την όψη πληροφορίας.

5.3.3.3.1 Επιχειρησιακή όψη

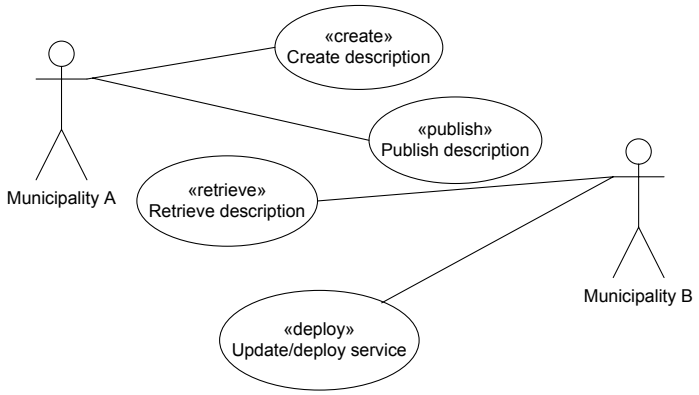
5.3.3.3.1.1 Επιχειρησιακές λειτουργίες και συναρτήσεις

Στην φάση αυτή χρησιμοποιούμε και επεκτείνουμε τα βασικά στοιχεία της παραγράφου 4.3.2.3.3.1.2 για να παράγουμε τα αντίστοιχα διαγράμματα χρήσης της UML που αντικατοπτρίζουν σε υψηλό επίπεδο τις επιχειρησιακές λειτουργίες που παρέχει η υπηρεσία.
Για το λόγο αυτό διαιρούμε την συνολική υπηρεσία σε τέσσερις φάσεις: διασύνδεσης δήμων, αίτησης & έκδοσης, μεταφοράς & μετάφρασης και λήψης.

5.3.3.3.1.1.1 Φάση διασύνδεσης δήμων

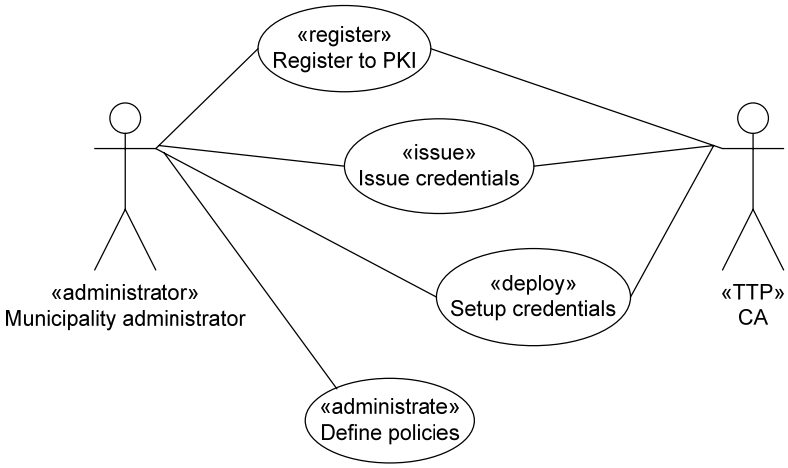
Τα βήματα που λαμβάνουν χώρα στη φάση αυτή πρέπει να συμβούν προτού η υπηρεσία είναι διαθέσιμη σε οποιονδήποτε πολίτη ή επιχείρηση, προκειμένου να εδραιωθούν οι κατάλληλοι μηχανισμοί επικοινωνίας μεταξύ δήμων που διαθέτουν την υπηρεσία. Σε τεχνικό επίπεδο, κάθε δήμος που υιοθετεί σε μια ΑΔΑΑΥ την υπηρεσία έκδοσης των εγγράφων πιστοποίησης δημοσιεύει την περιγραφή της υπηρεσίας σε έναν κατάλογο υπηρεσιών, ώστε άλλοι δήμοι να μπορούν να γνωρίζουν τις διεπαφές με τις οποίες αντίστοιχες δικές τους υπηρεσίες θα μπορούν να επικοινωνήσουν (βλ. Σχήμα 5-38). Η φάση αυτή θα πρέπει περιλαμβάνει και μια συμφωνία νομικής φύσεως δεδομένου ότι η υπηρεσία υποστηρίζει την διασυνοριακή ανταλλαγή προσωπικών δεδομένων, καθώς και μεταφράσεών τους. Το δεύτερο βήμα της φάσης είναι η εδραίωση μιας αλυσίδας διαπίστευσης των πιστοποιητικών ασφάλειας που πρόκειται να χρησιμοποιούν για την

δημιουργία ηλεκτρονικών υπογραφών, βάση διαθέσιμων ΕΤΟ (που μπορεί να έχει ήδη γίνει ή όχι) (βλ. Σχήμα 5-39).



Σχήμα 5-38. Δημοσίευση και ανάκτηση υπηρεσίας

Κατά την δημοσίευση, ο δήμος δημοσιεύει την περιγραφή της υπηρεσίας στον δημόσιο κατάλογο. Ένας άλλος δήμος μπορεί να ψάξει στον κατάλογο και να ανακτήσει την περιγραφή. Έπειτα διαμορφώνει την υπηρεσία του ώστε να συμμορφώνεται με την περιγραφή αυτή (Σχήμα 5-38).
Προκειμένου να μπορούν να επικοινωνήσουν ασφαλώς, πρέπει οι συμμετέχοντες δήμοι (αν αυτό δεν ισχύει ήδη) να συμμετέχουν σε διαδικασίες εγγραφής και πιστοποίησης (Σχήμα 5-39) όπως επιβάλλεται απο το Έγγραφο Πρακτικών Πιστοποίησης της σχετικής ΕΤΟ, για να αποκτήσουν τα απαραίτητα διαπιστευτήρια για τους δημοσίους υπαλλήλους τους (με τη μορφή μιας έξυπνης κάρτας).



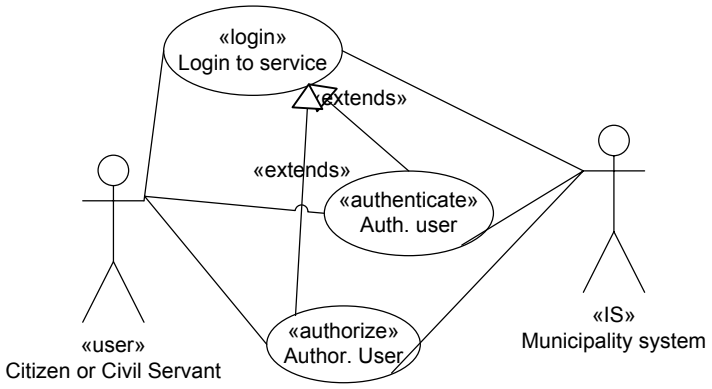
Σχήμα 5-39: Διαδικασία λήψης και εγκατάστασης διαπιστευτηρίων

Επιπρόσθετα, είναι σημαντικό οι οργανισμοί να καθορίσουν τις απαραίτητες πολιτικές υπογραφών που θα αναφέρονται κατά την παραγωγή και επαλήθευση προηγμένων υπογραφών, όπως υποδεικνύεται απο τα σχετικά πρότυπα.

5.3.3.3.1.1.2 Φάση αίτησης και έκδοσης

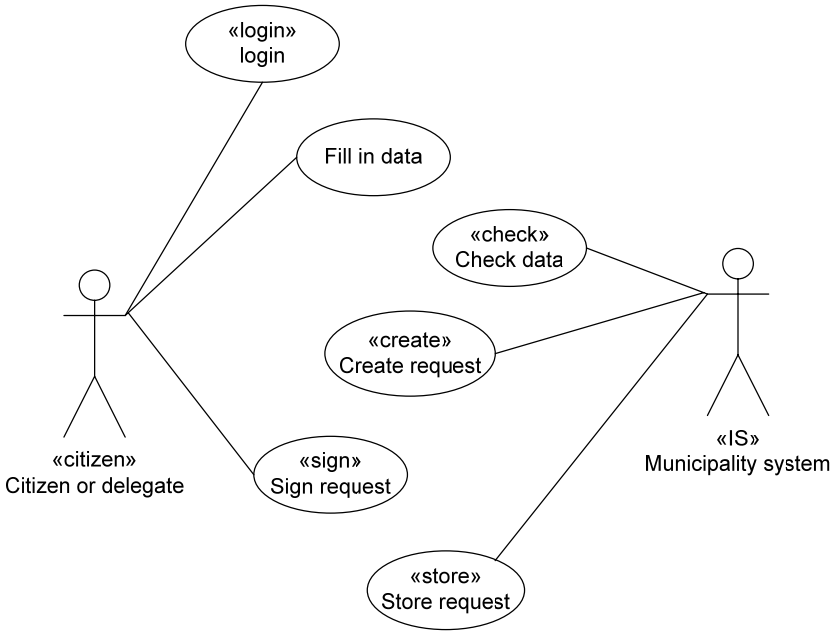
Οι φάσεις της υπηρεσίας εμπεριέχουν την είσοδο ενός χρήστη (πολίτη, δημοσίου υπαλλήλου κ.λ.π) στο σύστημα και την αυθεντικοποίηση του βάσει της έξυπνης κάρτας

του, καθώς και τον αντίστοιχο έλεγχο πρόσβασης ο οποίος επηρεάζει τι μπορεί ο συγκεκριμένος χρήστης να επιλέξει.



Σχήμα 5-40: Είσοδος στο σύστημα, αυθεντικοποίηση και έλεγχος πρόσβασης

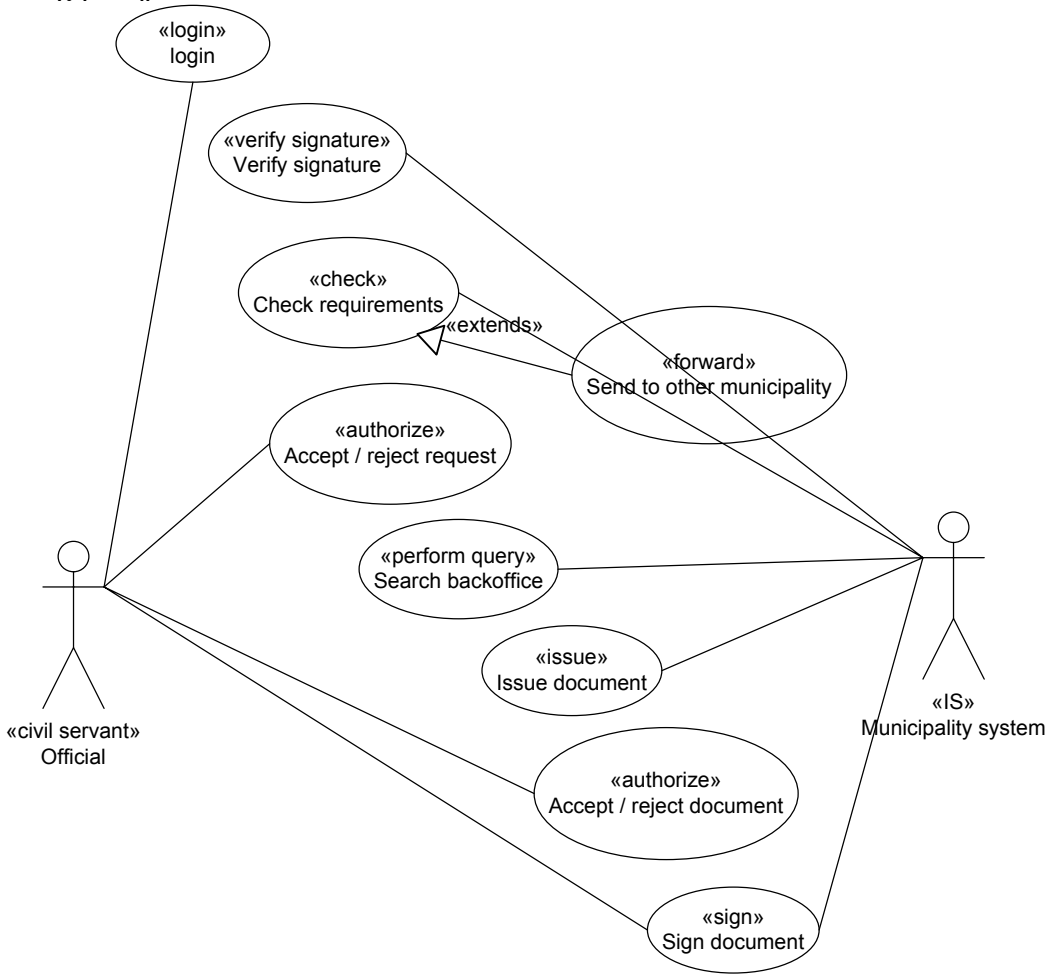
Κάθε στιγμιότυπο αυτής της διαδικασίας ακολουθεί τα βήματα του παραπάνω σχήματος (Σχήμα 5-40). Τα βήματα αυτά συνοψίζονται στην περίπτωση χρήσης login στην συνέχεια της περιγραφής.
Στην παρούσα φάση, ο πολίτης αρχικά εισέρχεται στο σύστημα, επιλέγει την υπηρεσία έκδοσης πιστοποιητικού μητρώου διαμονής και συμπληρώνει τα στοιχεία της αίτησής του σε μια φόρμα, όπως φαίνεται στο ακόλουθο διάγραμμα χρήσης:



Σχήμα 5-41: Φάση αίτησης & έκδοσης: δημιουργία αίτησης

Στη συνέχει α η υπηρεσία ελέγχει τα δεδομένα αυτά, δημιουργεί το έγγραφο της αίτησης στην εφαρμογή πελάτη και ο πολίτης την υπογράφει. Η αίτηση αποθηκεύεται για περαιτέρω επεξεργασία.

Στη συνέχεια της φάσης αυτής, όταν ο υπεύθυνος για την υπηρεσία δημόσιος υπάλληλος εισέρχεται στο σύστημα, του παρουσιάζονται οι διαθέσιμες αποθηκευμένες αιτήσεις και τα στοιχεία ασφάλειας αυτών (αφότου έχει προηγηθεί έλεγχος των υπογραφών που φέρουν). Ο υπάλληλος μπορεί να αποδεχθεί ή να απορρίψει κάποια αίτηση, δίνοντας μια αιτιολόγηση.
Εάν η αίτηση είναι αποδεκτή, ελέγχεται εάν μπορεί να ικανοποιηθεί στο σύστημα του παρόντος δήμου (δηλαδή, αν τα στοιχεία που απαιτούνται για το έγγραφο πιστοποίησης είναι διαθέσιμα στον παρόν δήμο ή όχι). Αν όχι προωθείται στον κατάλληλο δήμο, σε μια αντίστοιχη υπηρεσία.



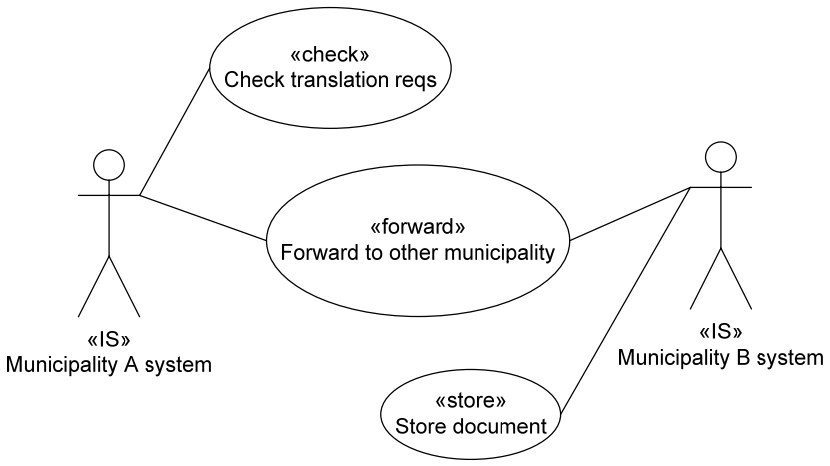
Σχήμα 5-42: Φάση αίτησης και έκδοσης: έκδοση εγγράφου πιστοποίησης

Αν ναι, τότε το σύστημα αναζητά την κατάλληλη πληροφορία για τα στοιχεία διαμονής του ατόμου που περιέχονται στην αίτηση στην βάση δεδομένων του δήμου, και δημιουργεί το αντίστοιχο έγγραφο πιστοποίησης μητρώου διαμονής, το οποίο επίσης παρουσιάζεται στον δημόσιο υπάλληλο για έλεγχο και υπογραφή, όπως φαίνεται στο Σχήμα 5-42.

5.3.3.3.1.1.3 Φάση μεταφοράς και μετάφρασης

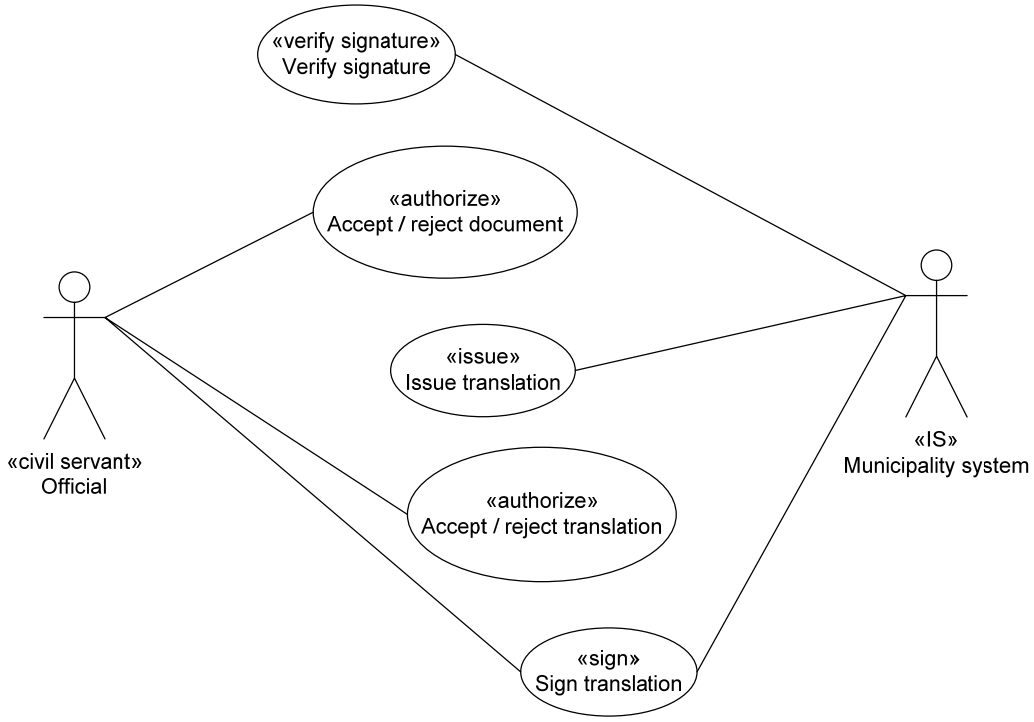
Στην περίπτωση που ένα έγγραφο χρειάζεται να μεταφραστεί σε μια άλλη μορφή ή μια άλλη δομή, και αυτό δεν μπορεί να γίνει στον παρόν δήμο, τότε μεταφέρεται στον δήμο

που μπορεί να επιτελέσει την μετάφραση / μετατροπή, όπου και αποθηκεύεται, όπως στο ακόλουθο σχήμα:



Σχήμα 5-43: Φάση μεταφοράς και μετάφρασης: μεταφορά εγγράφου προς μετάφραση

Στον δήμο αυτό, ελέγχεται η υπογραφή του εγγράφου, και ένας δημόσιος υπάλληλος που ελέγχει τις μεταφράσεις, αποδέχεται να γίνει ή όχι η μετάφραση του εγγράφου.

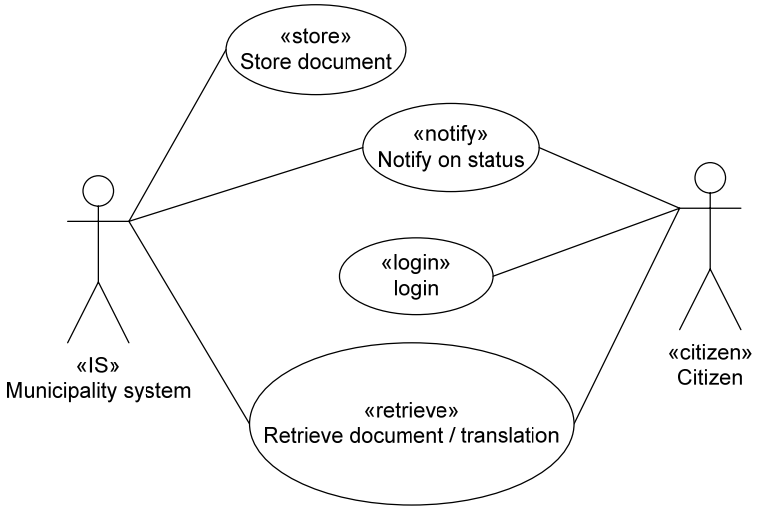


Σχήμα 5-44: Φάση μεταφοράς και μετάφρασης: μετάφραση εγγράφου

Στην αποδοχή, εκδίδεται μια μετάφραση του εγγράφου και ο δημόσιος υπάλληλος είτε την απορρίπτει, ή την αποδέχεται και την υπογράφει. Εάν η μετάφραση πρέπει να παραδοθεί σε άλλο δήμο, τότε επιστρέφεται, αλλιώς αποθηκεύεται στον παρόν.

5.3.3.3.1.1.4 Φάση λήψης

Στην τελική φάση της υπηρεσίας, ο πολίτης που έκανε την αίτηση ενημερώνεται με μια ειδοποίηση ότι το έγγραφο που ζήτησε και ενδεχομένως η μετάφρασή του, είναι διαθέσιμα προς λήψη.

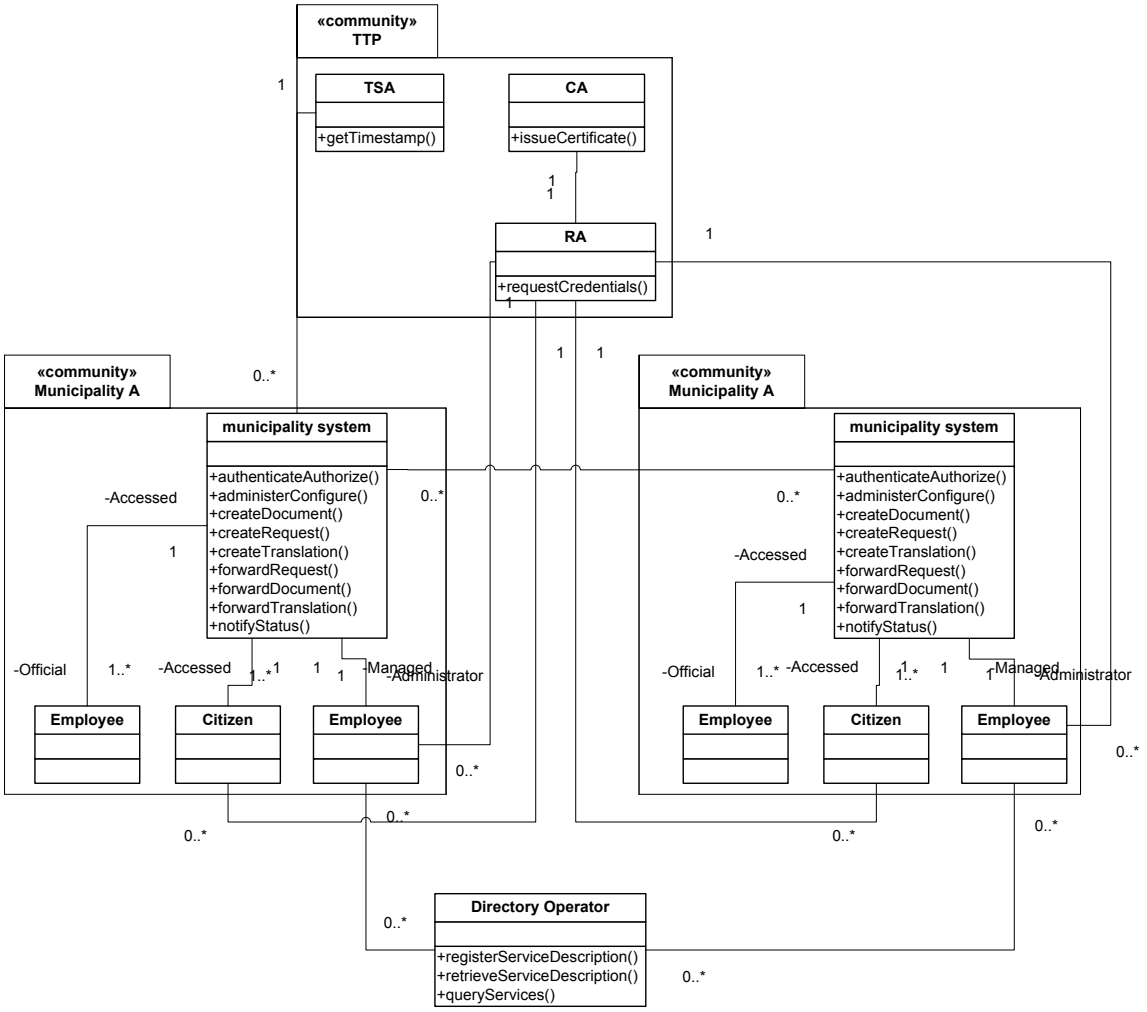


Σχήμα 5-45: Φάση και λήψης εγγράφου και μετάφρασης

Μπορεί να κάνει εισαγωγή στο σύστημα και να τα κατεβάσει στον υπολογιστή του.

5.3.3.3.1.2 Κοινότητες, ρόλοι και σχέσεις αντικείμενων

Η πλήρης ανάλυση των κοινοτήτων και των ρόλων που ορίζονται ως μέρος των προδιαγραφών για την συγκεκριμένη υπηρεσία φαίνονται στο διάγραμμα συνεργασίας που ακολουθεί:



Σχήμα 5-46: Κοινότητες, ρόλοι και σχέσεις τους για την υπηρεσία έκδοσης εγγράφων πιστοποίησης μητρώου διαμονής

Το σχήμα περιλαμβάνει όλες τις επιμέρους κοινότητες και αντικείμενα που συμμετέχουν στην έκδοση, δημιουργία και μετάφραση εγγράφων πιστοποίησης μητρώου διαμονής.
Οι επιμέρους κοινότητες είναι:

- Η κοινότητα *Δήμος Α (Municipality A)* περιλαμβάνει αντικείμενα με δεδομένους ρόλους που συντελούν στην παραμετροποίηση της υπηρεσίας, την λήψη αιτήσεων για έγγραφα και την διαχείριση και έκδοση εγγράφων πιστοποίησης και των μεταφράσεών τους. Αυτοί είναι:
    - Ο Πολίτης *(Citizen)*, ο οποίος είναι υπεύθυνος για την δημιουργία μιας αίτησης, υπογραφής και αποστολής της στο σύστημα.
    - Ο *Διοικητικός Υπάλληλος (Official)*, ο οποίος ελέγχει και αποδέχεται ή απορρίπτει αιτήσεις, έγγραφα πιστοποίησης και μεταφράσεις τους. Επίσης μπορεί να λάβει τον ρόλο του πολίτη (και να τον εκπροσωπήσει) δημιουργώντας μια αίτηση γι' αυτόν.
    - Ο *Διαχειριστής (Administrator)* είναι υπεύθυνος για την αίτηση και λήψη διαπιστευτηρίων απο τις ΕΤΟ και την εγκατάστασή τους στην υπηρεσία,

και την συνολική διαχείριση της υπηρεσίας στον Δήμο. Επίσης είναι υπεύθυνος για την δημοσίευση της υπηρεσίας στον κατάλογο υπηρεσιών.
    - Το ίδιο το *Σύστημα του Δήμου (Municipality System)*, που ανταλλάσσει τα κατάλληλα μηνύματα με αντίστοιχες υπηρεσίες σε άλλους Δήμους, προκειμένου να επιτύχει ασφαλείς και ολοκληρωμένες συναλλαγές αιτήσεων, εγγράφων πιστοποίησης ή μεταφράσεων τους.
- Η κοινότητα *Δήμος Β (Municipality B)* είναι πανομοιότυπη του Δήμου Α και λειτουργεί μια αντίστοιχη υπηρεσία. Είναι παρούσα στο διάγραμμα, για να δηλωθεί ότι ένα έγγραφο ή μια μετάφραση ενδέχεται να εκδίδονται σε δήμο διαφορετικό απο αυτόν στον οποίο γίνεται η αίτηση. Εμπεριέχει αντίστοιχους ρόλους με τον Δήμο Α.
- Η *Κοινότητα ΕΤΟ (TTP)* περιλαμβάνει τους οργανισμούς που υποστηρίζουν ΥΔΚ και προσφέρουν κατ' ελάχιστο τις υπηρεσίες πιστοποίησης και χρονοσφράγισης (σύμφωνα με τις απαιτήσεις της υπηρεσίας). Ο ρόλοι που εμπεριέχει είναι λοιπόν:
    - Μια ΑΠ (CA), με όλες τα χαρακτηριστικά που περιγράφονται στο Παράρτημα.
    - Μια ΑΕ (RA), με όλες τα χαρακτηριστικά που περιγράφονται στο Παράρτημα.
    - Μια Αρχή Χρονοσφράγισης (TSA), η οποία μπορεί να παράγει χρονοσφραγίδες για έγγραφα με βάσει μια έμπιστη πηγή χρόνου.

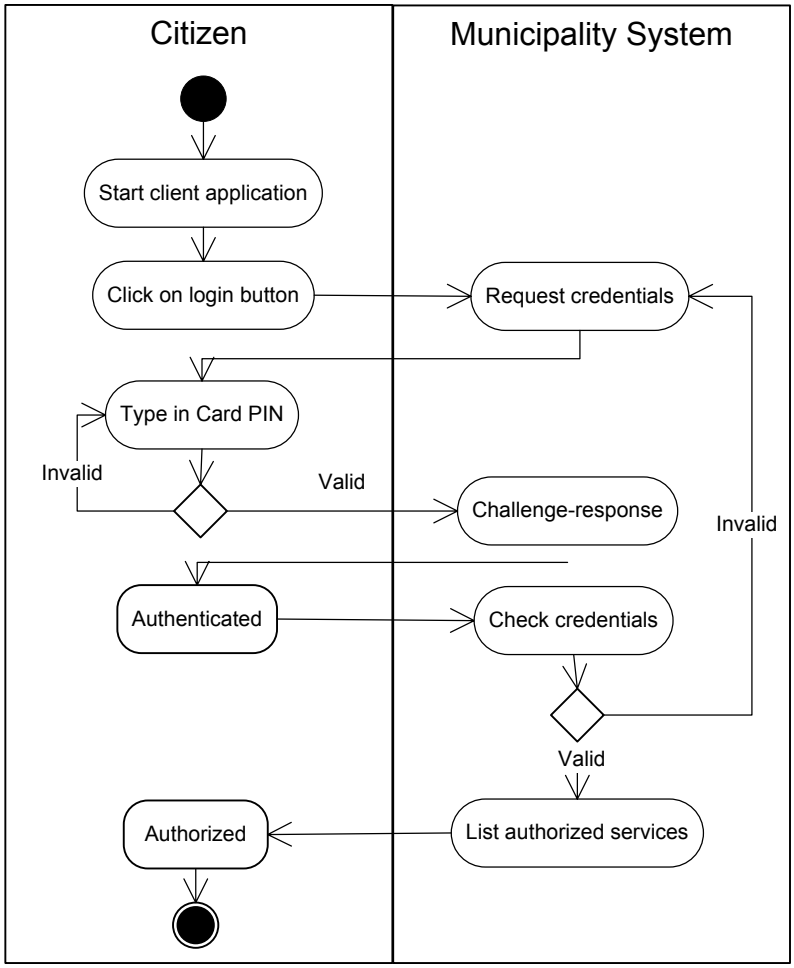
Οι παραπάνω κοινότητες συμπληρώνονται απο τον ρόλο *Διαχειριστή Καταλόγου (Directory Operator)*, ο οποίος διαχειρίζεται τα δημόσια δεδομένα περιγραφών υπηρεσιών.
Όπως φαίνεται στο διάγραμμα και ορίζεται απο την μεθοδολογία, οι κοινότητες έχουν το στερεότυπο «Community» και οι ρόλοι αναπαρίστανται με κλάσεις της UML, συμπεριλαμβανομένου κάποιων βασικών στοιχείων όψης που έχουν χρησιμοποιηθεί.

5.3.3.3.1.3 Διεργασίες

Οι διεργασίες που περιλαμβάνονται στην Φάση διασύνδεσης δήμων και περιγράφονται στην παράγραφο 5.3.3.3.1.1.1 δεν χρήζουν περαιτέρω ανάλυσης γιατί αποτελούν οργανωτικές διαδικασίες και δεν αποτελούν εγγενείς διαδικασίες της υπηρεσίας που σχεδιάζεται. Επίσης σχετίζονται με την υπάρχουσα υποδομή που θα φιλοξενήσει την υπηρεσία (ως προς τον τρόπο παραμετροποίησής της και εγκατάστασης της υπηρεσίας), καθώς και τις υποδομές των Έμπιστων Τρίτων Οντοτήτων που συμμετέχουν.
Ως μέρος των προδιαγραφών της παρούσας παραγράφου θα δοθούν οι διεργασίες που λαμβάνουν χώρα στις υπόλοιπες φάσεις της υπηρεσίας.

5.3.3.3.1.3.1 Φάση αίτησης

Αρχικά, αναλύουμε περαιτέρω το διάγραμμα περιπτώσεων χρήσης στο Σχήμα 5-4 χωρίζοντάς το στη *διεργασία αυθεντικοποίησης και ελέγχου πρόσβασης* και στη *διεργασία συμπλήρωσης στοιχείων αίτησης και υπογραφής*. Η διεργασία αυθεντικοποίησης και ελέγχου φαίνεται στο ακόλουθο σχήμα:

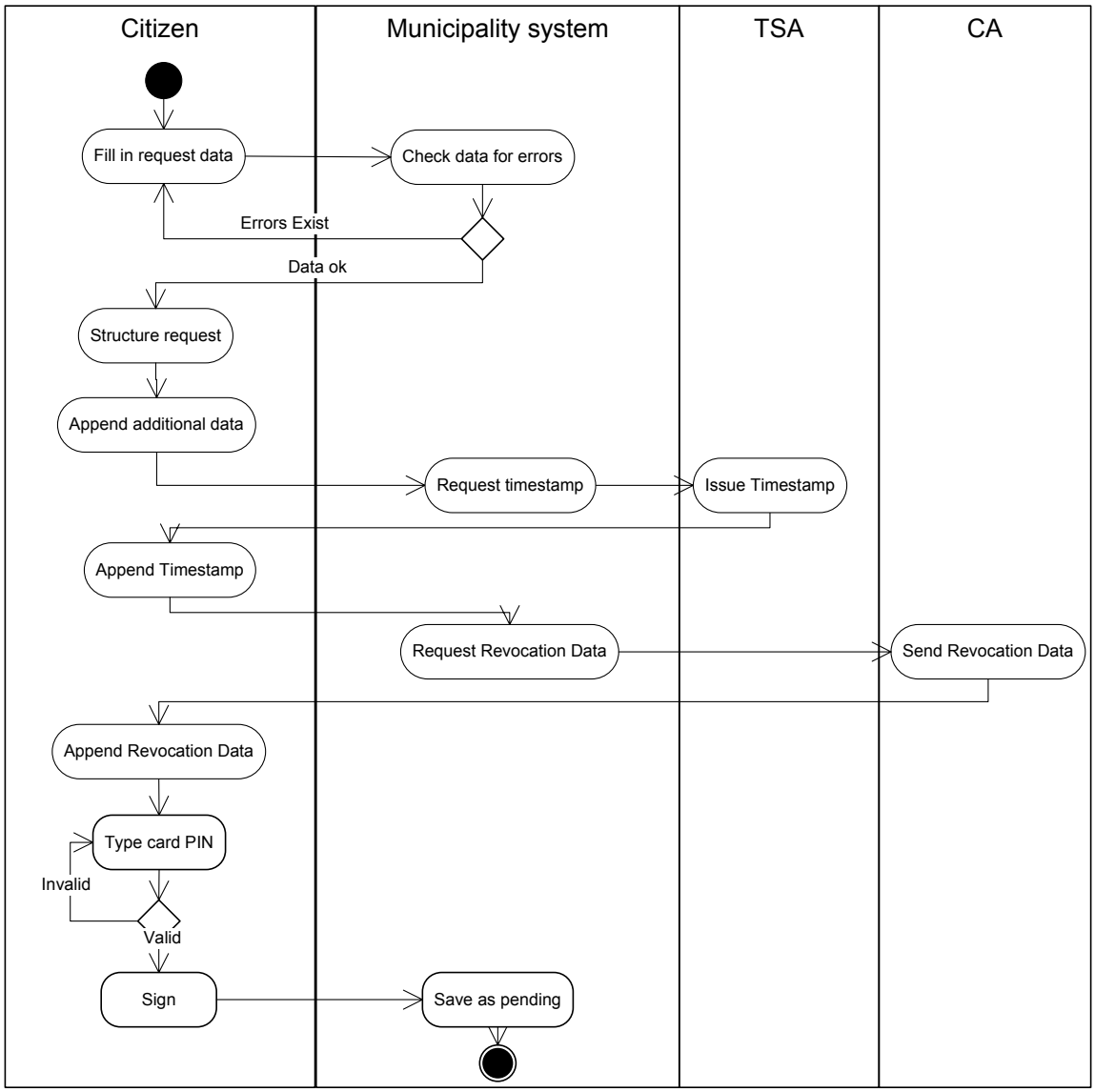


Σχήμα 5-47: Διεργασία αυθεντικοποίησης και ελέγχου πρόσβασης πολίτη στο Π.Σ. ενός δήμου

Κατά τη διεργασία αυτή, ο χρήστης εκκινεί την εφαρμογή που του επιτρέπει είσοδο στην υπηρεσία. Μέσω της υπηρεσίας ελέγχου πρόσβασης γίνονται τα εξής:

1. Ζητούνται τα διαπιστευτήρια του χρήστη.
2. Ο χρήστης εισάγει το PIN για πρόσβαση στα διαπιστευτήρια.
3. Εάν η πρόσβαση είναι επιτυχής, διενεργείται ένα πρωτόκολλο πρόκλησης-απάντησης.
4. Εάν είναι επιτυχές, ο χρήστης θεωρείται αυθεντικοποιημένος.
5. Ελέγχονται τα διαπιστευτήρια σε σχέση με τις ισχύουσες πολιτικές πρόσβασης.
6. Εάν ο έλεγχος είναι επιτυχής, ο χρήστης αποκτά πρόσβαση σε ο,τι είναι διαθέσιμο βάσει των διαπιστευτηρίων του και της πολιτικής.

Η ίδια διαδικασία εισαγωγής στο σύστημα ακολουθείται και απο έναν Δημόσιο Υπάλληλο και τον Διαχειριστή, αλλά του αποδίδονται διαφορετικά δικαιώματα. Το ίδιο ισχύει για τον Διαχειριστή.
Στη συνέχεια εκτελείται η διεργασία συμπλήρωσης στοιχείων αίτησης και υπογραφής, όπως φαίνεται στο Σχήμα 5-9:



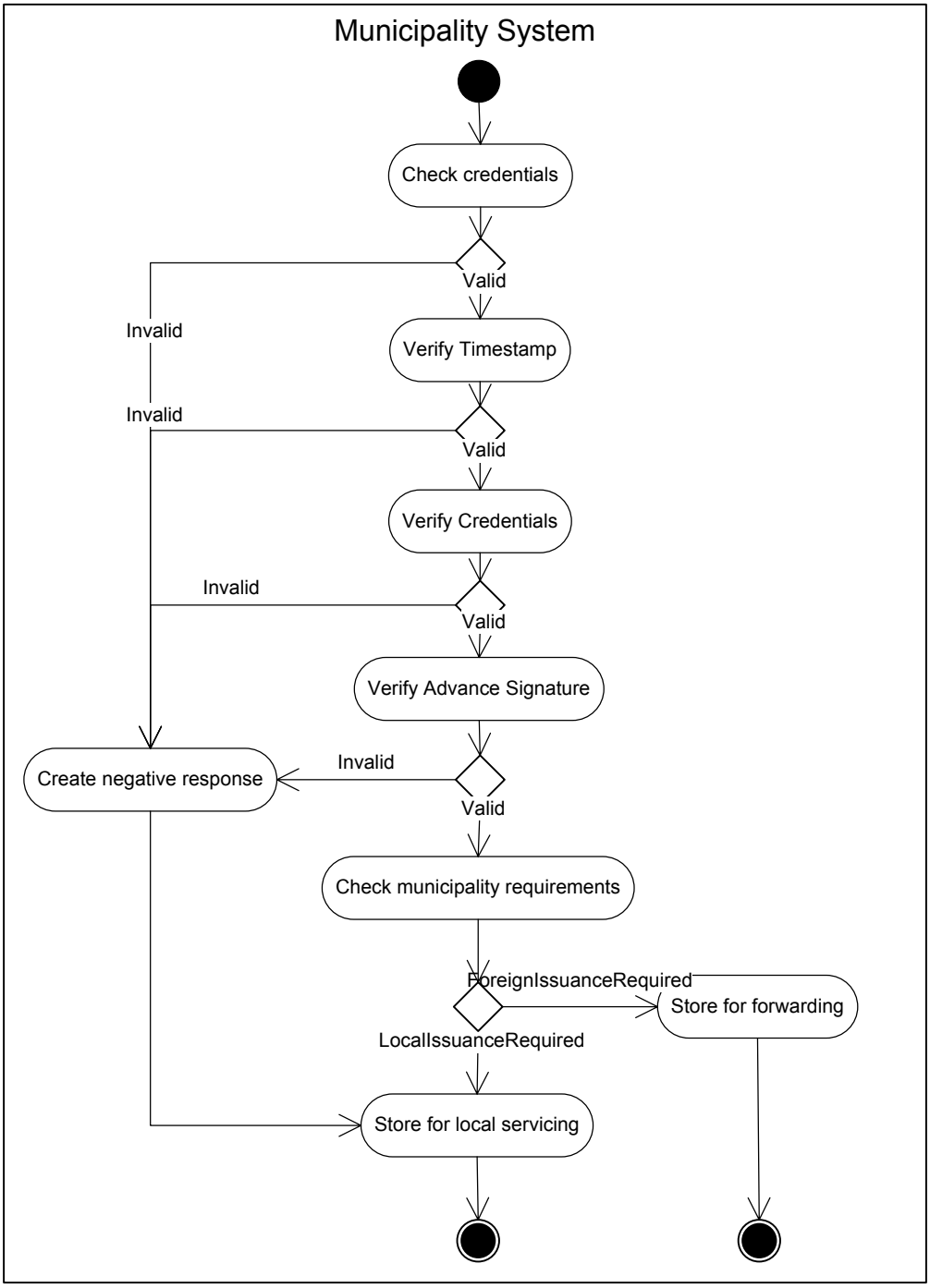
Σχήμα 5-48: Διεργασία συμπλήρωσης αίτησης και υπογραφής

Τα βήματα της διεργασίας είναι τα ακόλουθα:

1. Ο χρήστης είτε συμπληρώνει τα στοιχεία της φόρμας της αίτησης.
2. Το σύστημα ελέγχει παράλληλα τα δεδομένα για λάθη (π.χ. λάθος τύπος πληροφορίας, υποχρεωτικά πεδία που είναι κενά κ.λ.π.). Όσο υπάρχουν λάθη, ο χρήστης τα διορθώνει. Τα περιεχόμενα της αίτησης θα καθοριστούν στην Όψη Πληροφορίας.
3. Όταν δεν υπάρχουν λάθη, η αίτηση δομείται στην εφαρμογή πελάτη σύμφωνα με τα ληφθέντα στοιχεία.
4. Μέσω της κατάλληλης υπηρεσίας του συστήματος, ζητείται μια χρονοσφραγίδα απο την Αρχή χρονοσφράγισης, και αυτή ενσωματώνεται στην δομή που θα υπογραφεί.

5. Μέσω της κατάλληλης υπηρεσίας του συστήματος, ζητούνται τα δεδομένα ελέγχου κατάστασης των διαπιστευτηρίων απο την Αρχή Πιστοποίησης, και ενσωματώνονται επίσης στη δομή που θα υπογραφεί.
6. Τέλος, ζητείται απο τον χρήστη να εισάγει το PIN του για την κάρτα, προκειμένου να υλοποιηθεί προηγμένη ηλεκτρονική υπογραφή στα δεδομένα. Μόλις η υπογραφή είναι επιτυχής, το έγγραφο της αίτησης αποθηκεύεται στο σύστημα.

Ένας δημόσιος υπάλληλος που θέλει να εισάγει τα στοιχεία μιας αίτησης ως εκπρόσωπος ενός πολίτη ακολουθεί ακριβώς την ίδια διαδικασία. Στη συνέχεια ακολουθούνται τα παρακάτω βήματα προκειμένου να αναγνωριστεί πώς θα γίνει η επεξεργασία της αίτησης:



Σχήμα 5-49: Έλεγχος υπογραφής και αρχική επεξεργασία αίτησης

1. Αρχικά γίνεται έλεγχος της πληροφορίας ασφάλειας που εμπεριέχεται στην υπογεγραμμένη αίτηση: της χρονοσφραγίδας, των δεδομένων ανάκλησης πιστοποιητικών σχετικών με τα διαπιστευτήρια που έχουν χρησιμοποιηθεί και της ίδιας της υπογραφής. Εάν οποιοσδήποτε έλεγχος αποτύχει, τότε δημιουργείται ένα έγγραφο αρνητικής απάντησης, το οποίο αποθηκεύεται για περαιτέρω επεξεργασία.

2. Εάν όλοι οι έλεγχοι επιτύχουν, τότε ελέγχεται εάν ο δήμος που θα εκδώσει το έγγραφο πιστοποίησης είναι ο παρών ή κάποιος άλλος. Στην πρώτη περίπτωση η αίτηση αποθηκεύεται για περαιτέρω τοπική επεξεργασία.
3. Στην περίπτωση που το έγγραφο πιστοποίησης πρέπει να εκδοθεί απο άλλο δήμο, τότε αποθηκεύεται προς προώθηση.

Όπως φαίνεται ήδη απο την παραπάνω ανάλυση, η υπηρεσία απαιτεί την επικοινωνία με ένα υποσύνολο των υπηρεσιών της ΑΔΑΑΥ που θα πρέπει να την φιλοξενήσει. Οι προδιαγραφές της επιχειρησιακής όψης υποδεικνύουν ποιες είναι αυτές οι υπηρεσίες που θα επιλεγούν στο επόμενο στάδιο της μεθόδου ως προαπαιτούμενες.

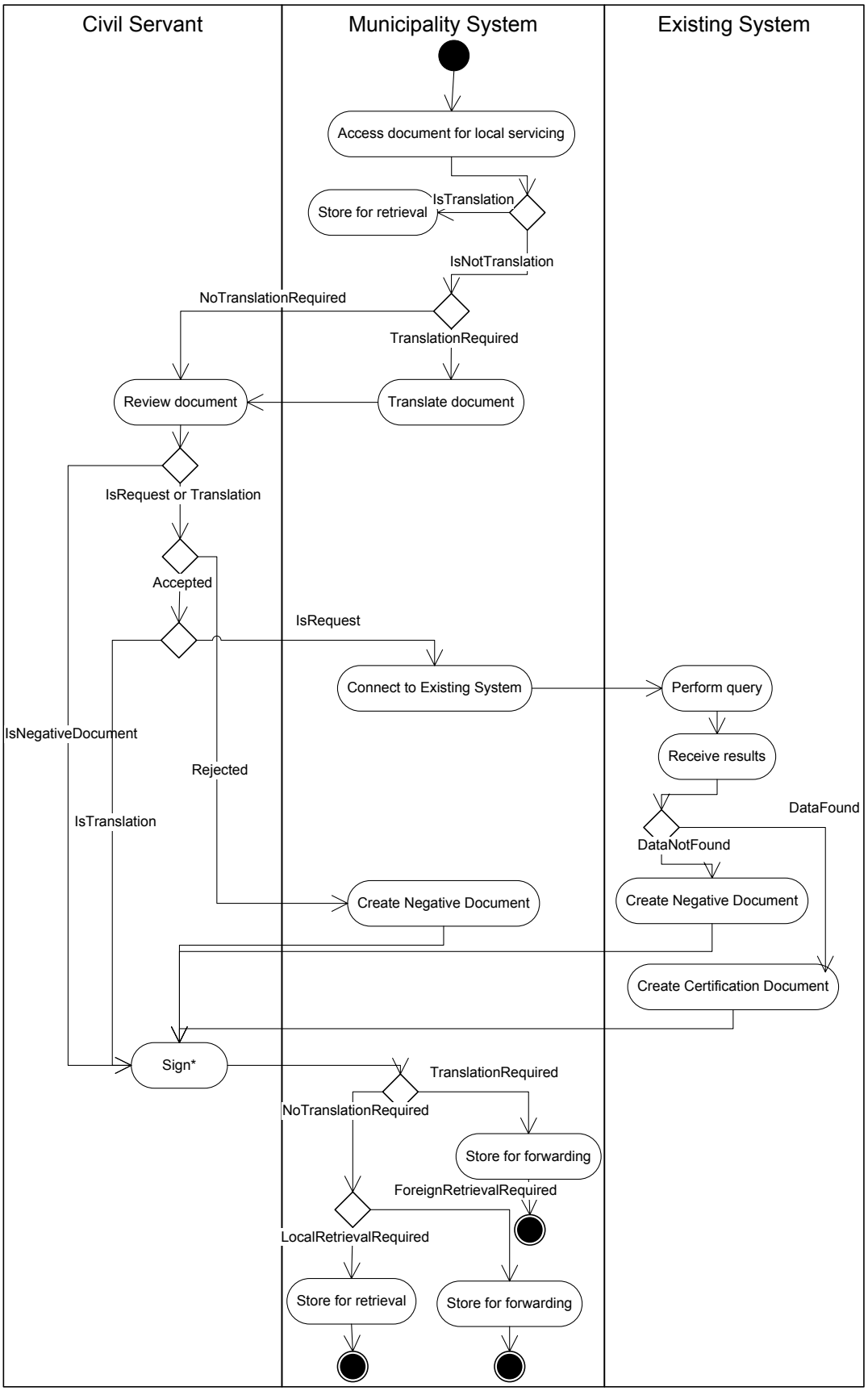
5.3.3.3.1.3.2 Φάση επεξεργασία / έκδοσης εγγράφου πιστοποίησης

Η φάση αυτή εξελίσσεται ανάλογα με το τι είδους έγγραφα είναι αποθηκευμένα στο σύστημα και προωθούνται σε έναν δημόσιο υπάλληλο προς επεξεργασία. Τα πιθανά ήδη εγγράφων που ενδέχεται να βρίσκονται αποθηκευμένα είναι:

- Μια αίτηση για έγγραφο πιστοποίησης
- Ένα έγγραφο πιστοποίησης (θετική απάντηση)
- Ένα αρνητικό έγγραφο πιστοποίησης (αρνητική απάντηση)
- Ένα έγγραφο πιστοποιημένης μετάφρασης

Οι έλεγχοι και διεργασίες που επιτελούνται είναι οι ακόλουθοι:

1. Ελέγχεται αν το εισερχόμενο έγγραφο πρέπει να μεταφραστεί και αν ναι υπόκειται μετάφραση. Σημειώνεται ότι εάν το έγγραφο είναι έγγραφο πιστοποίησης τότε απαιτείται σίγουρα μετάφρασή του (δεν υπάρχει περίπτωση να συνεχίσει έγγραφο σε έλεγχο απο δημόσιο υπάλληλο στη φάση αυτή).
2. Εάν το έγγραφο είναι ήδη αρνητικό, τότε απλά παρουσιάζεται στον δημόσιο υπάλληλο προς υπογραφή.
3. Εάν το έγγραφο είναι μια αίτηση ή μια μετάφραση παρουσιάζεται για λήψη απόφασης αν θα συνεχιστεί η επεξεργασία του ή όχι. Αν όχι, εκδίδεται ένα κατάλληλο αρνητικό έγγραφο πιστοποίησης και υπογράφεται αυτό.
4. Εάν ο δημόσιος υπάλληλος αποφασίσει να συνεχιστεί, τότε εάν αυτό είναι μια αίτηση, γίνεται η κατάλληλη ερώτηση στο υπάρχον σύστημα με την πληροφορία του μητρώου διαμονής. Εάν είναι μετάφραση τότε πάει κατ' ευθείαν προς υπογραφή.
5. Εάν η ερώτηση στο μητρώο δεν δώσει απάντηση (δηλαδή τα δεδομένα της αίτησης δεν βρίσκονται στην συγκεκριμένη βάση), τότε δημιουργείται πάλι ένα αρνητικό έγγραφο και αποστέλλεται προς υπογραφή. Διαφορετικά δημιουργείται το έγγραφο πιστοποίησης με τα δεδομένα, και υπογράφεται αυτό.
6. Ο τελικός έλεγχος μετά την υπογραφή είναι εάν το έγγραφο (αν είναι θετική ή αρνητική απάντηση) πρέπει να μεταφραστεί. Στην περίπτωση αυτή αποθηκεύεται προς μετάφραση, διαφορετικά αποθηκεύεται προς λήψη απο τον πολίτη.


Civil Servant
Municipality System
Existing System
Access document for local servicing
IsTranslation
Store for retrieval
IsNotTranslation
NoTranslationRequired
TranslationRequired
Review document
Translate document
IsRequest or Translation
Accepted
IsRequest
Connect to Existing System
Perform query
IsNegativeDocument
Receive results
Rejected
DataFound
IsTranslation
DataNotFound
Create Negative Document
Create Negative Document
Create Certification Document
Sign*
TranslationRequired
NoTranslationRequired
Store for forwarding
ForeignRetrievalRequired
LocalRetrievalRequired
Store for retrieval
Store for forwarding

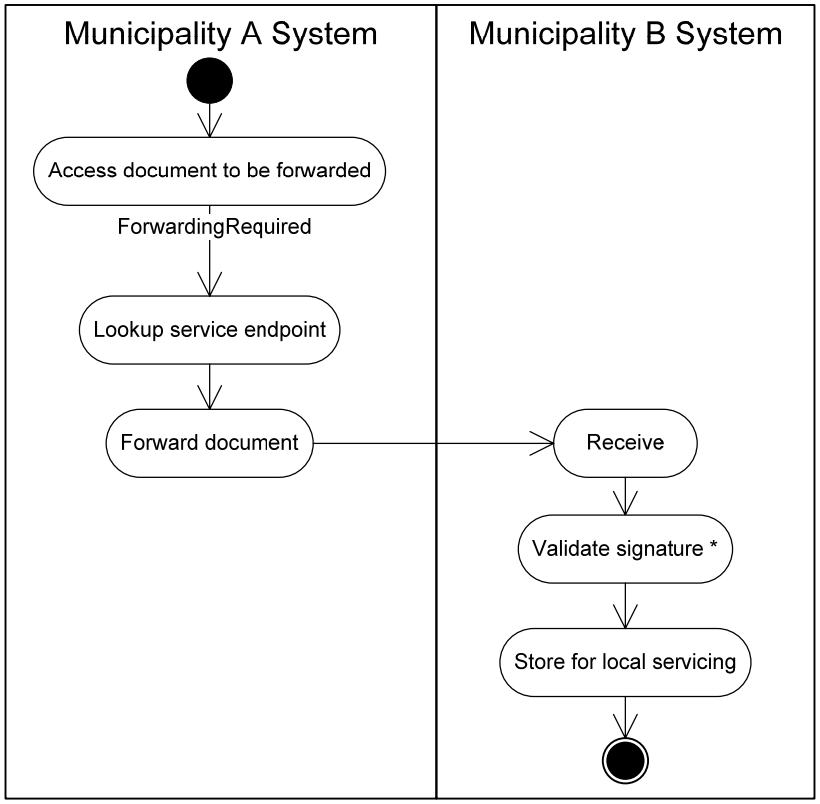
Σχήμα 5-50: Επεξεργασία και έκδοση εγγράφων πιστοποίησης

Ο αστερίσκος στην πράξη της υπογραφής στο σχήμα υποδηλώνει ότι η υπογραφή απαιτεί όλες τις επιμέρους διεργασίες που έχουν ήδη παρουσιαστεί στην προηγούμενη φάση και δεν επαναλαμβάνονται εδώ.

5.3.3.3.1.3.3 Φάση μεταφοράς και λήψης

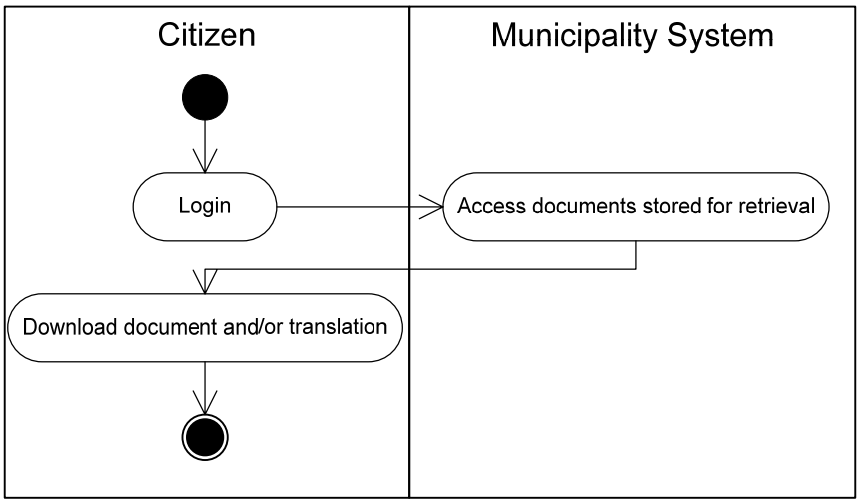
Η φάση αυτή λαμβάνει χώρα όταν ένα έγγραφο (οποιουδήποτε τύπου) μεταφέρεται απο έναν δήμο σε έναν άλλο. Τα βήματα που λαμβάνουν χώρα είναι τα ακόλουθα (Σχήμα 5-51):

1. Αρχικά λαμβάνονται τα έγγραφο προς μεταφορά.
2. Στη συνέχεια ελέγχεται σε μια υπηρεσία καταλόγου η διεύθυνση προορισμού (στην περιγραφή της υπηρεσίας).
3. Βάσει αυτής της διεύθυνση προωθείται το έγγραφο απο τον δήμο Α στον δήμο Β προορισμού.
4. Ο δήμος Β λαμβάνει το έγγραφο και ελέγχει την υπογραφή του.
5. Στη συνέχεια το αποθηκεύει για τοπική επεξεργασία, σύμφωνα με τα βήματα της προηγούμενης φάσης.



Σχήμα 5-51: Μεταφορά εγγράφου μεταξύ δύο υπηρεσιών

Σημειώνεται ότι ο αστερίσκος στο βήμα της επαλήθευσης της υπογραφής υπονοεί όλα τα βήματα επαλήθευσης που έχουν παρουσιαστεί στο Σχήμα 5-49 τα οποία δεν επαναλαμβάνονται στο παραπάνω σχήμα.
Το τελικό βήμα σε κάθε συναλλαγή είναι η λήψη εγγράφων απο τον πολίτη (ή αντιπρόσωπό του), όπως φαίνεται στο ακόλουθο σχήμα:



Σχήμα 5-52: Λήψη εγγράφων

Ο πολίτης εισέρχεται στο σύστημα σύμφωνα με την διαδικασία που παρατέθηκε στο Σχήμα 5-47. Το σύστημα ελέγχει τα έγγραφα που υπάρχουν προς λήψη, τα παραθέτει στον πολίτη και εκείνος τα κατεβάζει (είτε είναι ένα θετικό έγγραφο πιστοποίησης, ή ένα αρνητικό ή ένα έγγραφο και η πιστοποιημένη μετάφρασή του).

5.3.3.3.1.4 Πολιτικές

Οι πολιτικές / περιορισμοί που θα πρέπει να βρίσκονται σε ισχύ για την υπηρεσία έκδοσης εγγράφων πιστοποίησης μητρώου διαμονής είναι οι ακόλουθες:

- Τα ακόλουθα έγγραφα που διακινούνται στο σύστημα πρέπει πάντα να φέρουν προηγμένη ηλεκτρονική υπογραφή: οι αιτήσεις, τα έγγραφα πιστοποίησης θετικής και αρνητικής απάντησης και οι μεταφράσεις.
- Δικαίωμα δημιουργίας και υπογραφής αίτησης εγγράφου πιστοποίησης έχουν οι: πολίτες, εκπρόσωποι πολιτών, δημόσιοι υπάλληλοι (που επίσης μπορούν να δράσουν ως εκπρόσωποι πολιτών).
- Τα έγγραφα πιστοποίησης θετικής και αρνητικής απάντησης και οι μεταφράσεις δημιουργούνται αυτόματα απο το σύστημα κάθε δήμου σύμφωνα με δεδομένα που είναι αποθηκευμένα στις υπάρχουσες βάσεις δεδομένων.
- Δικαίωμα ελέγχου, προσθήκης σχολίων και υπογραφής στα έγγραφα πιστοποίησης θετικής και αρνητικής απάντησης και στις μεταφράσεις έχουν μόνο οι δημόσιοι υπάλληλοι των εμπλεκομένων δήμων.
- Όλοι οι χρήστες του συστήματος πρέπει να κατέχουν έξυπνη κάρτα με τα διαπιστευτήρια κάθε χρήστη και κλειδιά για τις ηλεκτρονικές υπογραφές.

- Όλοι οι χρήστες του συστήματος πρέπει να υπόκεινται σε διαδικασίες αυθεντικοποίησης και ελέγχου πρόσβασης βάσει των διαπιστευτηρίων τους.
- Τα **ελάχιστα απαραίτητα στοιχεία** που πρέπει να συμπληρωθούν σε μια αίτηση είναι το ονοματεπώνυμο του προσώπου για το οποίο θα εκδοθεί το έγγραφο πιστοποίησης, η ημερομηνία γέννησής του, ο τρόπος με τον οποίο ο αιτών θέλει να λαμβάνει ειδοποιήσεις απο το σύστημα και η αντίστοιχη διεύθυνση (ή τηλέφωνο) για τις ειδοποιήσεις, *ο δήμος έκδοσης* του εγγράφου και ο *δήμος λήψης* του.
- Ο δήμος που θα εκδώσει ένα έγγραφο πιστοποίησης πρέπει πάντα να ταυτίζεται με τον δήμο έκδοσης που έχει δηλωθεί στην αίτηση. Ο δήμος που θα μεταφράσει ένα έγγραφο πιστοποίησης (αρνητικής ή θετικής απάντησης) πρέπει πάντα να ταυτίζεται με τον δήμο λήψης που έχει δηλωθεί στην αίτηση.
- Ένας δημόσιος υπάλληλος πρέπει πάντα να ελέγχει κάθε αίτηση, έγγραφο πιστοποίησης και μετάφραση που το σύστημα λαμβάνει ή παράγει. Έχει δικαίωμα να αποδεχτεί ή να απορρίψει κάθε έγγραφο. Στην περίπτωση της απόρριψης, πρέπει να δώσει διευκρινίσεις σε κατάλληλο χώρο πληροφορίας εντός του εγγράφου πιστοποίησης αρνητικής απάντησης που δημιουργείται.
- Εάν τα στοιχεία ενός πολίτη που περιέχονται σε μια αίτηση δεν υπάρχουν στη βάση δεδομένων του καθορισμένου (στην αίτηση) δήμου έκδοσης, τότε πάντα εκδίδεται ένα έγγραφο πιστοποίησης αρνητικής απάντησης.
- Όταν οποιοδήποτε έγγραφο που παράγει η υπηρεσία είναι έτοιμο για λήψη, τότε πρέπει πάντα να ειδοποιείται ο αντίστοιχος πολίτης με μια διευκρινιστική ειδοποίηση προκειμένου να επανέλθει στο σύστημα για να λάβει τα έγγραφά του.
- Τα έγγραφα θα παραμένουν στο σύστημα για ένα δεδομένο αριθμό ημερών, κατόπιν απόφασης του κάθε δήμου. Στην συγκεκριμένη υπηρεσία (όπως έχει οριστεί στην περιγραφή της) ο αριθμός αυτός είναι 10 ημέρες. Μετά το πέρας του χρόνο αυτού, τα έγγραφα διαγράφονται.

Στην υλοποίηση της συγκεκριμένης υπηρεσίας όλες οι παραπάνω πολιτικές πρέπει να ισχύουν κάθε στιγμή.

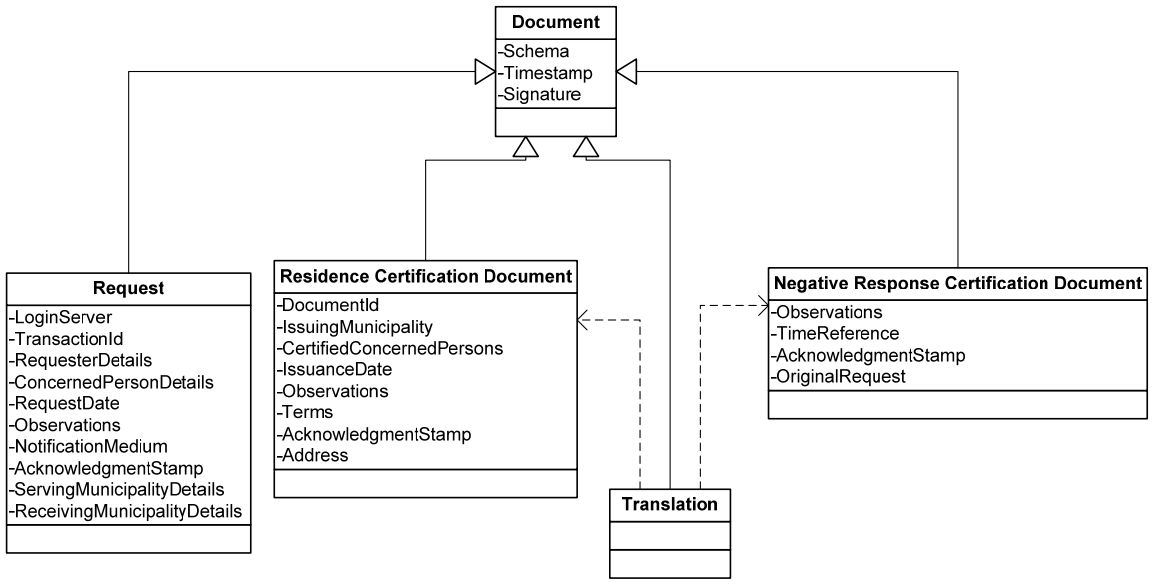
5.3.3.3.2 Όψη πληροφορίας

Στην παρούσα παράγραφο, παρατίθενται όλα τα αντικείμενα πληροφορίας που υπάρχουν στην υπηρεσία και είτε δημιουργούνται και μεταφέρονται προκειμένου να επιτελεστούν οι διεργασίες που έχουν ήδη περιγραφεί, είτε επηρεάζουν την υπηρεσία κατά τη διάρκεια της ζωής τους. Ως μέρος της όψης προδιαγράφονται τα σταθερά και δυναμικά σχήματα των αντικείμενων αυτών. Όπου είναι δυνατό, χρησιμοποιούνται και επεκτείνονται τα βασικά στοιχεία της όψης, όπως έχουν παρουσιαστεί στο κεφάλαιο 4.3.2.4.3.1.2.

5.3.3.3.2.1 Τα η-έγγραφα: Η αίτηση, το έγγραφο πιστοποίησης μητρώου διαμονής (θετική απάντηση), το έγγραφο πιστοποίησης αρνητικής απάντησης και η μετάφραση

5.3.3.3.2.1.1 Σταθερό σχήμα

Όλα τα παραπάνω έγγραφα αποτελούν επεκτάσεις του βασικού στοιχείου Έγγραφο, της παραγράφου 4.3.2.4.3.1.2.1. Τα σταθερά τους σχήματα φαίνονται στα σχήματα που ακολουθούν:



Σχήμα 5-53: Σταθερά σχήματα η-εγγράφων

Το βασικό στοιχείο Έγγραφο έχει επεκταθεί με ένα σύνολο πεδίων που πρέπει να περιέχονται σε κάθε ένα απο τα η-έγγραφα. Πιο συγκεκριμένα, η αίτηση εμπεριέχει τα ακόλουθα πεδία / δομές:

- Το αναγνωριστικό του εξυπηρετητή στον οποίο δημιουργείται (LoginServer).
- Το αναγνωριστικό της συναλλαγής (TransactionId).
- Τα στοιχεία του χρήστη που συμπληρώνει την αίτηση (ονοματεπώνυμο κ.λ.π.) (RequesterDetails)
- Τα στοιχεία του πολίτη για τον οποίο θα εκδοθεί το έγγραφο πιστοποίησης (ConcernedPersonDetails).
- Την ημερομηνία δημιουργίας της αίτησης (RequestDate).
- Παρατηρήσεις απο τον αιτούντα (Observations).
- Το είδος του μέσου λήψης ειδοποιήσεων (NotificationMedium).
- Έναν αριθμό πρωτοκόλλου (AcknowledgmentStamp).
- Το αναγνωριστικό του δήμου έκδοσης (ServingMunicipalityDetails).
- Το αναγνωριστικό του δήμου λήψης (ReceivingMunicipalityDetails).

Το έγγραφο πιστοποίησης μητρώου διαμονής περιέχει τα ακόλουθα πεδία / δομές:

- Ένα αναγνωριστικό για το ίδιο το έγγραφο (DocumentId).
- Το αναγνωριστικό του δήμου έκδοσής του (IssuingMunicipality).
- Τα στοιχεία των πολιτών για τους οποίους πιστοποιεί τα δεδομένα διαμονής (CertifiedConcernedPersons).
- Την ημερομηνία έκδοσής του (IssuanceDate).
- Παρατηρήσεις απο τον δημόσιο υπάλληλο που το ελέγχει (Observations).
- Όρους έκδοσής του, αν υπάρχουν (Terms).

- Έναν αριθμό πρωτοκόλλου (AcknowledgmentStamp).
- Την διεύθυνση των πολιτών, δηλαδή τα δεδομένα πιστοποίησης (Address).

Το έγγραφο πιστοποίησης αρνητικής απάντησης περιέχει τα ακόλουθα πεδία / δομές:

- Παρατηρήσεις απο τον δημόσιο υπάλληλο που το ελέγχει (Observations).
- Την ώρα έκδοσής του (TimeReference).
- Έναν αριθμό πρωτοκόλλου (AcknowledgmentStamp).
- Την αρχική αίτηση (OriginalRequest) που είτε απορρίφθηκε ή δεν ήταν δυνατό να εκπληρωθεί επιτυχώς.

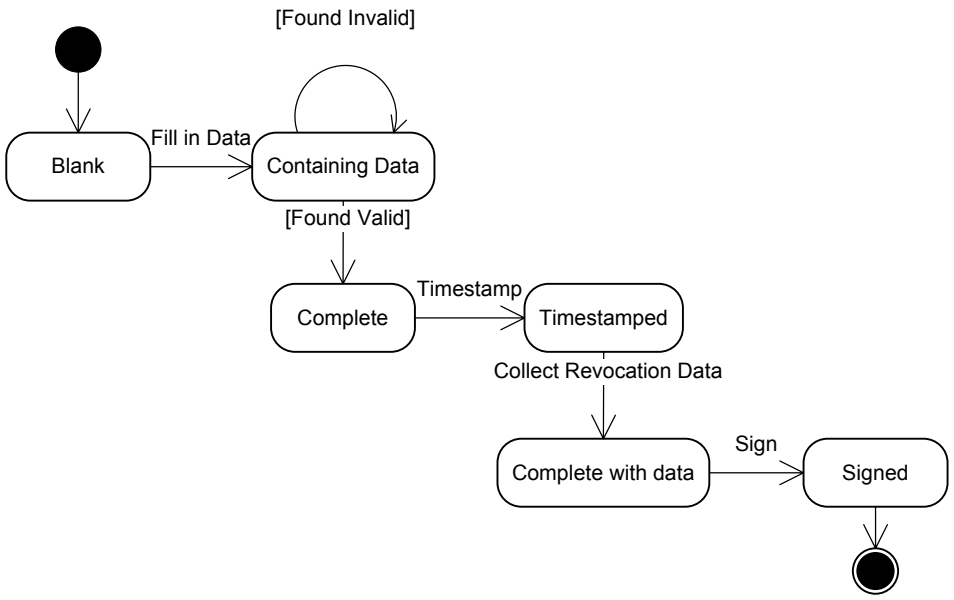
Το αντικείμενο πληροφορίας Μετάφραση εξαρτάται απο τα έγγραφα πιστοποίησης θετικής και αρνητικής απάντησης, διότι τα περιεχόμενα του πάντα αποτελούν μεταφράσεις των περιεχομένων των δύο αυτών στοιχείων (είτε σε επίπεδο δομής, είτε σε επίπεδο γλώσσας).
Προκειμένου να διασφαλιστεί η διαλειτουργικότητα μεταξύ διαφορετικών υπηρεσιών, είναι απαραίτητο η υπηρεσία να υποστηρίζει ένα σύνολο σχημάτων XML που εμπεριέχουν δεδομένα αποτύπωσης προσωπικών στοιχείων (ονοματεπώνυμο κ.λ.π.) και διευθύνσεων που είναι ευρέως διαδεδομένα στην η-διακυβέρνηση. Πρότυπα που μπορούν να χρησιμοποιηθούν γι' αυτό το σκοπό είναι τα ακόλουθα:

- Σχήματα που έχουν δημιουργηθεί υπο την αιγίδα της πρωτοβουλίας e-Gif στο Ηνωμένο Βασίλειο [Hunter04, Kent03]
- Τα σχήματα της βιβλιοθήκης OASIS Universal Business Language (UBL) [UBL1.0],
- Σχήματα που έχουν δημιουργηθεί στο πρόγραμμα eGov – GovML [Kavvadias02]
- Η πρωτοβουλία του IDA για e-procurement XML schemas [IDA04]

Όσο περισσότερα απο τέτοιου τύπου πρότυπα υποστηρίζονται τόσο περισσότερο αυξάνεται το επίπεδο διαλειτουργικότητας της υπηρεσίας.

5.3.3.3.2.1.2 Δυναμικό σχήμα

Όλα τα παραπάνω έγγραφα έχουν το ίδιο δυναμικό σχήμα που αποτελεί μια επέκταση του δυναμικού σχήματος ενός Εγγράφου, όπως φαίνεται στο επόμενο σχήμα:



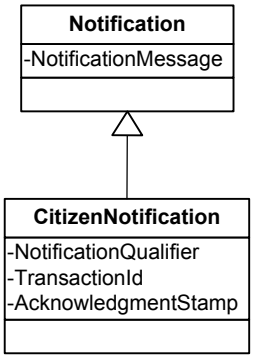
Σχήμα 5-54: Δυναμικό σχήμα η-εγγράφων

Σύμφωνα με τις πολιτικές που έχουν τεθεί, κάθε η-έγγραφο πρέπει να υπογραφεί με προηγμένη ηλεκτρονική υπογραφή. Άρα εκτός απο την χρονοσφραγίδα πρέπει να του προστεθούν και τα δεδομένα ανάκλησης των σχετικών διαπιστευτηρίων σε σχέση με τον χρόνο που υποδηλώνει η χρονοσφραγίδα, και έπειτα να τελεστεί η υπογραφή.

5.3.3.3.2.2 Ειδοποίηση

5.3.3.3.2.2.1 Σταθερό σχήμα

Η υπηρεσία απαιτεί την αποστολή ειδοποιήσεων στους πολίτες που έχουν να λάβουν κάποιο έγγραφο απο αυτήν. Κάθε ειδοποίηση επεκτείνει το βασικό στοιχείο Ειδοποίηση, όπως έχει προδιαγραφεί στην παράγραφο 4.3.2.4.3.1.2.1, κατά τον ακόλουθο τρόπο:

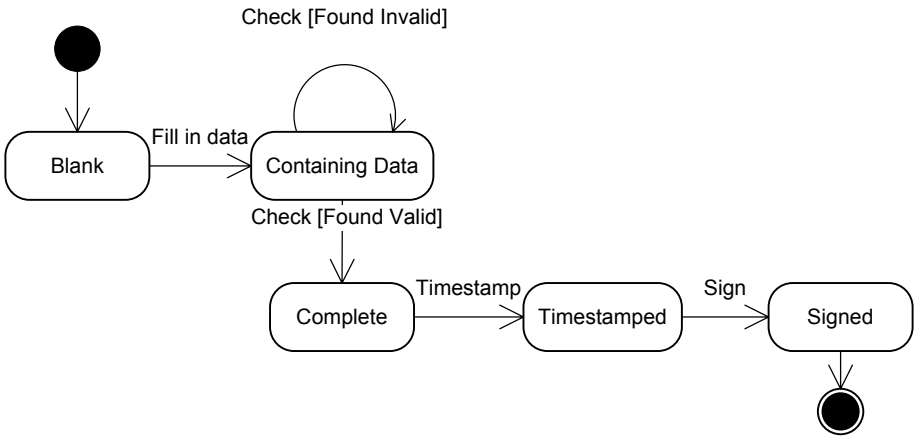


Σχήμα 5-55: Σταθερό σχήμα Ειδοποίησης

Κάθε ειδοποίηση είναι χαρακτηρίζεται απο κάποιο αναγνωριστικό (NotificationQualifier) και είναι δεμένη με μια συγκεκριμένη συναλλαγή (TransactionId). Επίσης περιέχει έναν αριθμό πρωτοκόλλου (AcknowledgmentStamp).

5.3.3.3.2.2.2 Δυναμικό σχήμα

Το δυναμικό σχήμα του αντικειμένου είναι ίδιο με το σχήμα του βασικού στοιχείου Ειδοποίηση (και του Εγγράφου, απο το οποίο παράγεται η Ειδοποίηση):



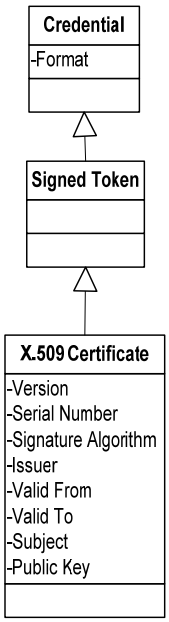
Σχήμα 5-56: Δυναμικό σχήμα Μηνύματος Επιβεβαίωσης

Σημειώνεται ότι το συγκεκριμένο αντικείμενο πληροφορίας δεν έχει απαίτηση για προηγμένη ηλεκτρονική υπογραφή, όποτε μια απλή ψηφιακή υπογραφή καλύπτει τις απαιτήσεις ασφαλείας του.

5.3.3.3.2.3 Διαπιστευτήριο

5.3.3.3.2.3.1 Σταθερό σχήμα

Στην προκειμένη περίπτωση, τα διαπιστευτήρια που θα χρησιμοποιηθούν στην υπηρεσία θα αποτελούν υπογεγραμμένες οντότητες και θα υπακούουν στο πρότυπο X.509. Οπότε επεκτείνουμε κατάλληλα το βασικό στοιχείο της παραγράφου 4.3.2.4.3.1.2.2 για να λάβουμε το αντίστοιχο σταθερό σχήμα:

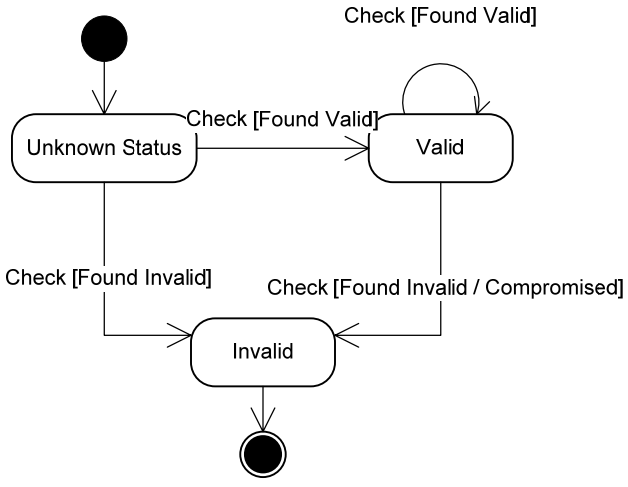


Σχήμα 5-57: Σταθερό σχήμα Διαπιστευτηρίου

Στο αντικείμενο πληροφορίας έχει επεκταθεί με το σύνολο των πεδίων που προδιαγράφονται απο το πρότυπο X.509, όπως έχει περιγραφεί ήδη στο παράδειγμα της παραγράφου 4.3.2.4.3.1.3.

5.3.3.3.2.3.2 Δυναμικό σχήμα

Το δυναμικό σχήμα του αντικειμένου είναι ίδιο με το δυναμικό σχήμα που προδιαγράφεται για το Διαπιστευτήριο στην παράγραφο 4.3.2.4.3.3.2.2:



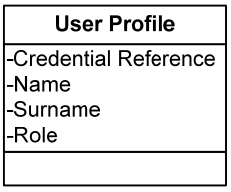
Σχήμα 5-58: Δυναμικό σχήμα Διαπιστευτηρίου

Όπως και το βασικό στοιχείο όψης, το αντικείμενο περνάει απο τις διάφορες καταστάσεις σε σχέση με την εγκυρότητά του.

5.3.3.3.2.4 Προφίλ χρήστη

5.3.3.3.2.4.1 Σταθερό σχήμα

Το σταθερό σχήμα για το προφίλ χρήστη που θα χρησιμοποιηθεί στην υπηρεσία αποτελεί μια επέκταση του σταθερού σχήματος του βασικού στοιχείου όψης της παραγράφου 4.3.2.4.3.1.2.3, όπως φαίνεται στο ακόλουθο σχήμα:

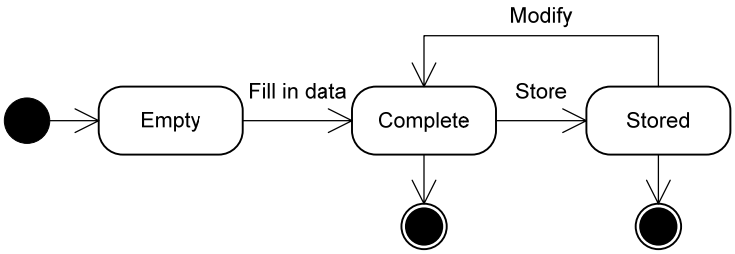


Σχήμα 5-59: Σταθερό σχήμα Προφίλ χρήστη

Η επέκταση περιλαμβάνει τα πεδία Όνομα (Name), Επώνυμο (Surname) και Ρόλος (Role), που θα χρησιμοποιηθούν απο την υπηρεσία προκειμένου να κα γνωρίζει στοιχεία που της χρησιμεύουν για έναν χρήστη που έχει ήδη αυθεντικοποιηθεί.

5.3.3.3.2.4.2 Δυναμικό σχήμα

Το δυναμικό σχήμα του αντικειμένου είναι ίδιο με το δυναμικό σχήμα που προδιαγράφεται για το Προφίλ Χρήστη στην παράγραφο 4.3.2.4.3.3.2.3:



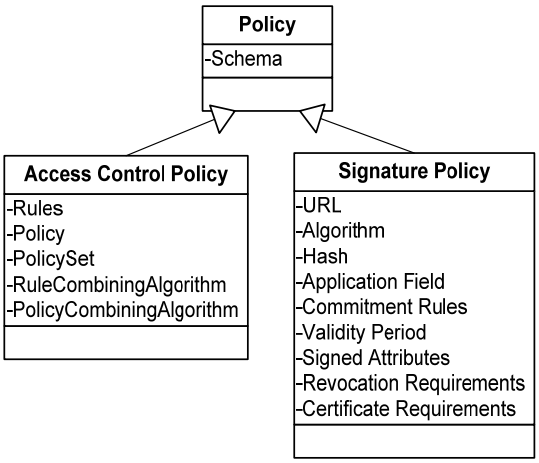
Σχήμα 5-60: Δυναμικό σχήμα Προφίλ χρήστη

Όπως και το βασικό στοιχείο όψης, το αντικείμενο συμπληρώνεται με τα στοιχεία του χρήστη κατά την δημιουργία του και ενημερώνεται αν αυτά αλλάξουν. Σε οποιαδήποτε περίπτωση, κάθε φορά αποθηκεύεται στο σύστημα.

5.3.3.3.2.5 Πολιτική

5.3.3.3.2.5.1 Σταθερό σχήμα

Η περιγραφή της υπηρεσίας και οι πολιτικές της Επιχειρησιακής Όψης επιβάλλουν τον ορισμό δύο ειδών πολιτικών, μιας Πολιτικής Ελέγχου Πρόσβασης και μιας Πολιτικής Υπογραφής. Χρησιμοποιούνται τα ακόλουθα σταθερά σχήματα για τα είδη των πολιτικών, που προκύπτουν απο το βασικό στοιχείο όψης της παραγράφου 4.3.2.4.3.1.2.4:



Σχήμα 5-61: Σταθερό σχήμα για τις Πολιτικές της υπηρεσίας

Η πολιτική ελέγχου πρόσβασης θα χρησιμοποιηθεί απο την υπηρεσία της αρχιτεκτονικής που φιλοξενεί την υπηρεσία προκειμένου να αποφανθεί αν ο χρήστης δικαιούνται πρόσβαση στο σύστημα και ποιες υπηρεσίες μπορεί να χρησιμοποιήσει. Αποτελείται απο διάφορους κανόνες και επιμέρους πολιτικές (Rules, Policies, Policy Sets) τα οποία συνδυάζονται βάσει συνδυαστικών αλγορίθμων (RuleCombiningAlgorithm, PolicyCombiningAlgorithm) προκειμένου να ληφθούν αποφάσεις ελέγχου πρόσβασης πάνω σε πόρους.
Στην συγκεκριμένη υπηρεσία θα υπάρχει ένα Σύνολο Πολιτικών (PolicySet) με δυο Πολιτικές (Policy), μια για κάθε ρόλο χρήστη που σχετίζεται άμεσα με την συγκεκριμένη υπηρεσία:

- Για τον Πολίτη, ο Κανόνας (Rule) που ισχύει είναι: μπορεί να δημιουργήσει και να υπογράψει μια αίτηση, και να κατεβάσει στον υπολογιστή του έγγραφα που έχουν αποθηκευθεί για αυτόν.
- Για τον Δημόσιο Υπάλληλο, ο Κανόνας είναι: μπορεί να δημιουργήσει και να υπογράψει μια αίτηση, να ελέγξει και να υπογράψει ένα έγγραφο πιστοποίησης μητρώου διαμονής (θετική απάντηση) ή ένα έγγραφο πιστοποίησης αρνητικής απάντησης ή μια μετάφραση .

Οι κανόνες για τον ρόλο του Διαχειριστή ορίζονται στις πολιτικές που αναφέρονται στην συνολική ΑΔΑΑΥ που φιλοξενεί την υπηρεσία και δεν αποτελούν μέρος των προδιαγραφών της παρούσας υπηρεσίας.
Η πολιτική υπογραφής καθορίζει το πλαίσιο σύμφωνα με το οποίο ο υπογράφονται τα η-έγγραφα. Θα πρέπει να είναι δημοσιευμένη κάπου ώστε να μπορούν να την δουν (URL) όλοι οι συμμετέχοντες στις κοινότητες που έχουν οριστεί. Το αναγνωριστικό της (το οποίο προκύπτει εφαρμόζοντας έναν αλγόριθμο κατακερματισμού (Algorithm) για την λήψη ενός Hash), θα πρέπει να ενσωματώνεται σε κάθε υπογεγραμμένο πιστοποιητικό γέννησης. Πιθανά χαρακτηριστικά της που φαίνονται στο παράδειγμα περιλαμβάνουν το Πεδίο Εφαρμογής (Application Field), τους Κανόνες Δέσμευσης (Commitment Rules) στην χρήση της υπηρεσίας, τα Χαρακτηριστικά που υπογράφονται σε κάθε πιστοποιητικό (Signed Attributes), τις απαιτήσεις για ενσωμάτωση δεδομένων

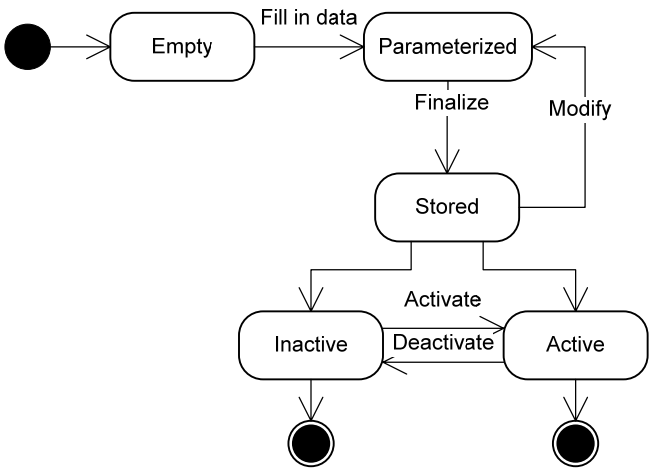
ανακληθέντων πιστοποιητικών (Revocation Requirements) και τις απαιτήσεις απο τα πιστοποιητικά (ασφάλειας) που χρησιμοποιούνται για τις υπογραφές (Certificate Requirements).
Τα παραπάνω χαρακτηριστικά προκύπτουν απο τους περιορισμούς που έχουν οριστεί για την υπηρεσία και είναι οι ακόλουθοι:

- Το URL επιλέγεται απο τον φορέα που παράγει τις υπογραφές.
- Ο αλγόριθμος κατακερματισμού είναι ο SHA-1.
- Το πεδίο εφαρμογής ορίζεται ως «έκδοση εγγράφων πιστοποίησης μητρώου διαμονής».
- Οι κανόνες δέσμευσης ορίζουν ότι ένα υπογεγραμμένο η-έγγραφο απο έναν οργανισμό αποτελεί νομικά κατοχυρωμένο έγγραφο που πιστοποιεί κάθε φορά:
    - Στην περίπτωση της αίτησης, ότι ένας πολίτης ή εκπρόσωπός του ζητά ένα έγγραφο πιστοποίησης μητρώου διαμονής για ένα πρόσωπο.
    - Στην περίπτωση του εγγράφου πιστοποίησης μητρώου διαμονής, ότι αυτό πιστοποιεί ότι ένα πρόσωπο διαμένει σε μια συγκεκριμένη οδό σύμφωνα με τα δεδομένα του δήμου.
    - Στην περίπτωση εγγράφου πιστοποίησης αρνητικής απάντησης, ότι αυτό πιστοποιεί πώς ο συγκεκριμένος πολίτης δεν βρέθηκε στον δήμο αναζήτησης ή ότι υπήρχε κάποιο άλλο πρόβλημα με την αίτηση.
    - Στην περίπτωση της μετάφρασης, ότι αυτή αποτελεί πιστή μετάφραση σε τοπική μορφή ενός εγγράφου πιστοποίησης (θετικής ή αρνητικής απάντησης) που έχει εκδοθεί σε έναν άλλο δήμο.
- Τα χαρακτηριστικά που υπογράφονται είναι όλο το εκάστοτε η-έγγραφο, η χρονοσφραγίδα στα δεδομένα του και τα δεδομένα ανακληθέντων πιστοποιητικών.
- Οι απαιτήσεις ενσωμάτωσης δεδομένων ανακληθέντων πιστοποιητικών ορίζουν ότι τα δεδομένα αυτά είναι υποχρεωτικό να περιλαμβάνονται στην υπογραφή.
- Οι απαιτήσεις πιστοποιητικών ορίζουν ότι τα κλειδιά και τα αντίστοιχα πιστοποιητικά που χρησιμοποιούνται θα πρέπει να είναι διαπιστευμένα απο τις Αρχές Πιστοποίησης των συμμετεχουσών κοινοτήτων.

Ορισμένα απο τα παραπάνω χαρακτηριστικά ενδέχεται να οριστικοποιούνται λίγο πριν την έναρξη λειτουργίας της υπηρεσίας.

5.3.3.3.2.5.2 Δυναμικό σχήμα

Το δυναμικό σχήμα για τις όλες τις παραπάνω πολιτικές ακολουθεί το αντίστοιχο σχήμα του βασικού στοιχείου της παραγράφου 4.3.2.4.3.3.2.4:



Σχήμα 5-62: Δυναμικό σχήμα Πολιτικής

Κάθε πολιτική, αφότου παραμετροποιηθεί, αποθηκεύεται στο σύστημα σε ηλεκτρονική μορφή, ενεργοποιείται και είναι προσβάσιμη απο τις υπηρεσίες και τους μηχανισμούς που την χρειάζονται. Η πολιτική υπογραφής, όσο είναι σε ενεργή κατάσταση, είναι δημοσιευμένη και στο διαδίκτυο.

5.3.3.4 3ο Στάδιο: Γενική αποτύπωση απαιτούμενων υπηρεσιών και κατευθύνσεων τεχνολογίας

Ακολουθώντας τα βήματα που ορίζει η μεθοδολογία του σταδίου, προκύπτουν οι προδιαγραφές που ακολουθούν.

5.3.3.4.1 Απαραίτητες Υπηρεσίες ΑΔΑΑΥ

Οι υπηρεσίες που θα πρέπει να υποστηρίζει κατ' ελάχιστο η ΑΔΑΑΥ που θα φιλοξενήσει την επιχειρησιακή υπηρεσία σύμφωνα με τις μέχρι τώρα προδιαγραφές και τα βασικά στοιχεία όψης του σταδίου είναι οι ακόλουθες:

- Υπηρεσίες και μηχανισμοί διαχείρισης και συντονισμού
    - Υπηρεσίες πρόσβασης
    - Υπηρεσίες διαχείρισης διεργασιών
    - Υπηρεσίες διαχείρισης χρηστών
- Βασικές υπηρεσίες και μηχανισμοί
    - Υπηρεσίες διεπαφής χρηστών
    - Υπηρεσίες μετασχηματισμού μηνυμάτων
    - Υπηρεσίες προώθησης μηνυμάτων
    - Υπηρεσίες δημοσίευσης και αναζήτησης σε καταλόγους Υπηρεσιών Ιστού
    - Υπηρεσίες διαχείρισης αποθετηρίων
    - Υπηρεσίες ειδοποιήσεων
- Υπηρεσίες και μηχανισμοί ασφάλειας
    - Μηχανισμοί ψηφιακών υπογραφών
    - Μηχανισμοί προηγμένων ηλεκτρονικών υπογραφών
    - Μηχανισμοί κρυπτογράφησης

- Υπηρεσίες διαχείρισης ταυτότητας
- Υπηρεσίες ελέγχου πρόσβασης
- Υπηρεσίες χρονοσφράγισης
- Υπηρεσίες διαχείρισης κλειδιών και πιστοποιητικών

- Υπηρεσίες υποστήριξης υπαρχουσών υποδομών

Για κάθε υπάρχον σύστημα που κρατάει δεδομένα διαμονής πολιτών του δήμου θα πρέπει να σχεδιαστεί μια αντίστοιχη Υπηρεσία Υποστήριξης Υπαρχουσών Υποδομών, έτσι ώστε να κάνει διαθέσιμα τα δεδομένα αυτά στην υπηρεσία έκδοσης εγγράφων πιστοποίησης.
Οι προδιαγραφές των σταδίων που ακολουθούν λαμβάνουν υπόψην ότι παρέχονται όλες οι παραπάνω υπηρεσίες.

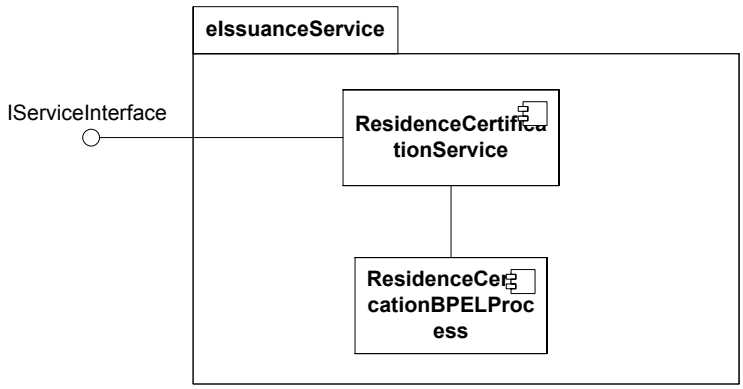
5.3.3.4.2 Συνολικό τεχνολογικό πλαίσιο

Όσο αφορά στο συνολικό τεχνολογικό πλαίσιο που θα ακολουθηθεί, η συγκεκριμένη υπηρεσία πρόκειται να υλοποιηθεί σε περιβάλλον J2EE.

5.3.3.5 4ο Στάδιο: Σχεδιασμός στοιχείων λογισμικού

5.3.3.5.1 Διαγράμματα δομικών στοιχείων

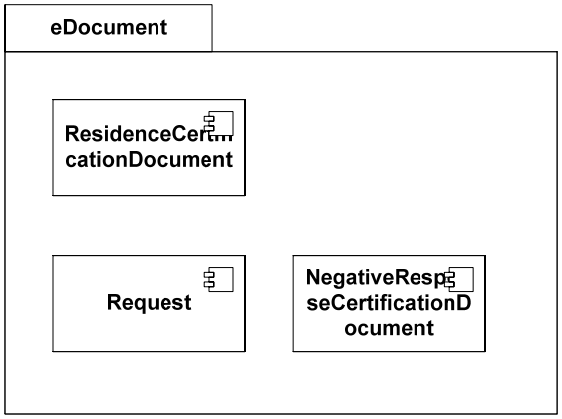
Η υπηρεσία έκδοσης εγγράφων πιστοποίησης μητρώου διαμονής αποτελεί μια νέα επιχειρησιακή υπηρεσία, επομένως δεν υπάρχει κάποιο έτοιμο βασικό στοιχείο όψης που θα χρησιμοποιηθεί ως βάση. Κατασκευάζουμε τα νέα διαγράμματα δομικών στοιχείων που αναπαριστούν την δομή της υπηρεσίας:



Σχήμα 5-63: Διάγραμμα δομικών στοιχειών Υπηρεσίας έκδοσης εγγράφων πιστοποίησης

Το πρώτο διάγραμμα παρουσιάζει το βασικό πακέτο eIssuanceService, το οποίο αποτελείται απο δύο βασικά δομικά στοιχεία: την υπηρεσία ResidenceCertificationService που επιτελεί τις βασικές επιχειρησιακές λειτουργίες και συναρτήσεις της υπηρεσίας που σχεδιάζεται ως προς την δημιουργία, επεξεργασία και διαχείριση των σχετικών με την υπηρεσία ηλεκτρονικών εγγράφων καθώς και το στοιχείο περιγραφής της κατάλληλης διεργασίας (ResidenceCertificationBPELProcess) που χρησιμοποιεί τις λειτουργίες τις υπηρεσίες και άλλες διαθέσιμες υπηρεσίες στην αρχιτεκτονική που την φιλοξενεί προκειμένου να τις συντονίσει συνολικά για να

επιτευχθούν οι επιχειρησιακοί στόχοι και να υλοποιηθούν οι διεργασίες της παραγράφου 5.3.3.3.1.3.
Το δεύτερο διάγραμμα eInvoice στο Σχήμα 5-64 περιλαμβάνει τα βασικά δομικά στοιχεία ResidenceCertificationDocument, Request και NegativeResponseCertificationDocument τα οποία αναπαριστούν τα αντίστοιχα αντικείμενα πληροφορίας και τα περιεχόμενά τους. Σημειώνεται ότι το αντικείμενο πληροφορίας Μετάφραση ("Translation") έχει την δομή του ResidenceCertificationDocument, με την διαφορά ότι τα πεδία του είναι σε διαφορετική γλώσσα.

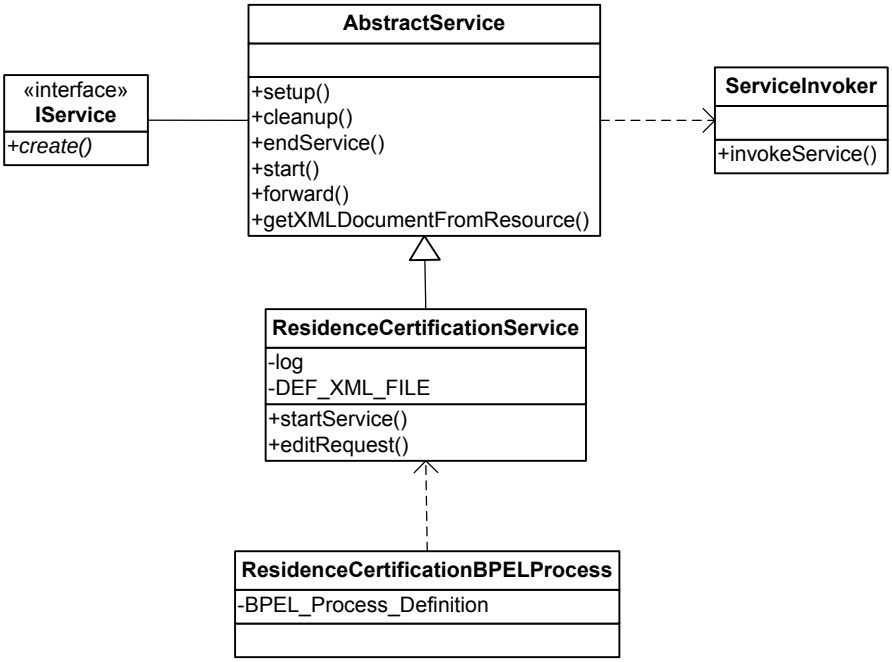


Σχήμα 5-64: Διάγραμμα δομικών στοιχείων για την αναπαράσταση των αντικειμένων πληροφορίας

Το παραπάνω δομικά στοιχεία θα αναλυθούν περαιτέρω στη συνέχεια προκειμένου να γίνει πλήρης αναπαράσταση των δεδομένων που περιέχουν βάσει του σχήματός τους.

5.3.3.5.2 Διαγράμματα κλάσεων

Στη συνέχεια παράγονται διαγράμματα κλάσεων που αντιστοιχούν στα παραπάνω διαγράμματα δομικών στοιχείων.
Το διάγραμμα κλάσεων για την υπηρεσία. είναι το ακόλουθο:



Σχήμα 5-65: Διάγραμμα κλάσεων υπηρεσία έκδοσης πιστοποιητικών

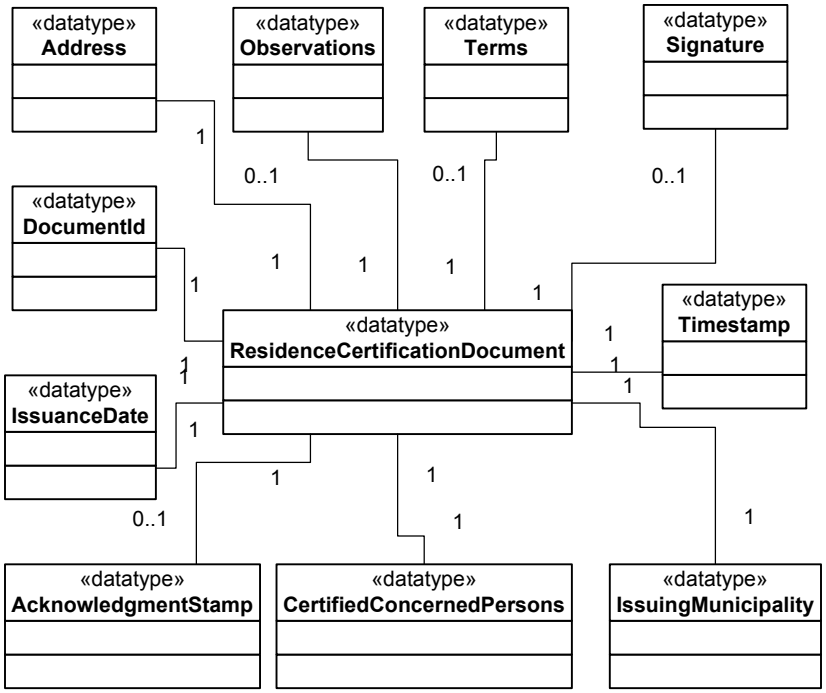
Το δομικό στοιχείο ResidenceCertificationService αποτελεί μια εξειδικευμένη κλάση που βασίζεται στην κλάση AbstractService η οποία υποστηρίζεται απο το μοντέλο διαχείρισης υπηρεσιών της συγκεκριμένης ΑΔΑΑΥ. Κάθε τέτοια υπηρεσία πρέπει να υλοποιεί την διεπαφή IService προκειμένου να είναι προσβάσιμη απο άλλες υπηρεσίες στην αρχιτεκτονική και εξαρτάται απο τον μηχανισμό κλήσης των υπηρεσιών ServiceInvoker.

Τα χαρακτηριστικά log και DEF_XML_FILE καθορίζουν την κλάση που θα υλοποιεί την καταγραφή συμβάντων της υπηρεσίας και το αρχείο καθορισμού του αρχείου XML που αναπαριστά ένα πιστοποιητικό μητρώου διαμονής αντίστοιχα. Οι μέθοδοι startService() και editRequest() υλοποιούν τις διαδικασίες εκκίνησης της υπηρεσίας και επεξεργασίας μιας αίτησης.

Η κλάση ResidenceCertificationBPELProcess αναπαριστά την προδιαγραφή στην γλώσσα BPEL [Arkin05] των δράσεων που λαμβάνουν χώρα κατά την λειτουργία της υπηρεσίας. Κάθε δράση δηλώνει τις παραμέτρους δεδομένων που εισάγονται και εξάγονται και ποιες υπο-υπηρεσίες χρησιμοποιούνται με είσοδο και έξοδο αυτά τα δεδομένα αντίστοιχα. Η διεργασία περιγράφεται σε ένα αρχείο XML που συμμορφώνεται με το πρότυπο BPEL.

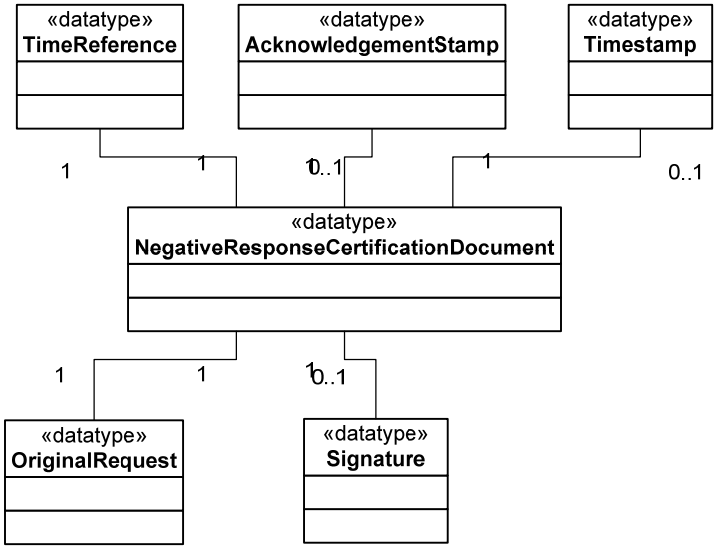
Σημειώνεται ότι στην παρούσα ενότητα στον αναλυτικό σχεδιασμό της υπηρεσίας περιλαμβάνεται και ένα σύνολο επιμέρους κλάσεων και οι περιγραφές τους, οι οποίες δεν παρατίθενται στην διατριβή, λόγω όγκου και λόγω του ότι δεν προσφέρουν κάτι ως προς την τεκμηρίωση της ορθότητας της κατασκευαστικής μεθόδου.

Τα διαγράμματα κλάσεων των αντικειμένων πληροφορίας είναι τα ακόλουθα:



Σχήμα 5-66: Διάγραμμα κλάσεων για το δομικό στοιχείο ResidenceCertificationDocument (αντικείμενο πληροφορίας)

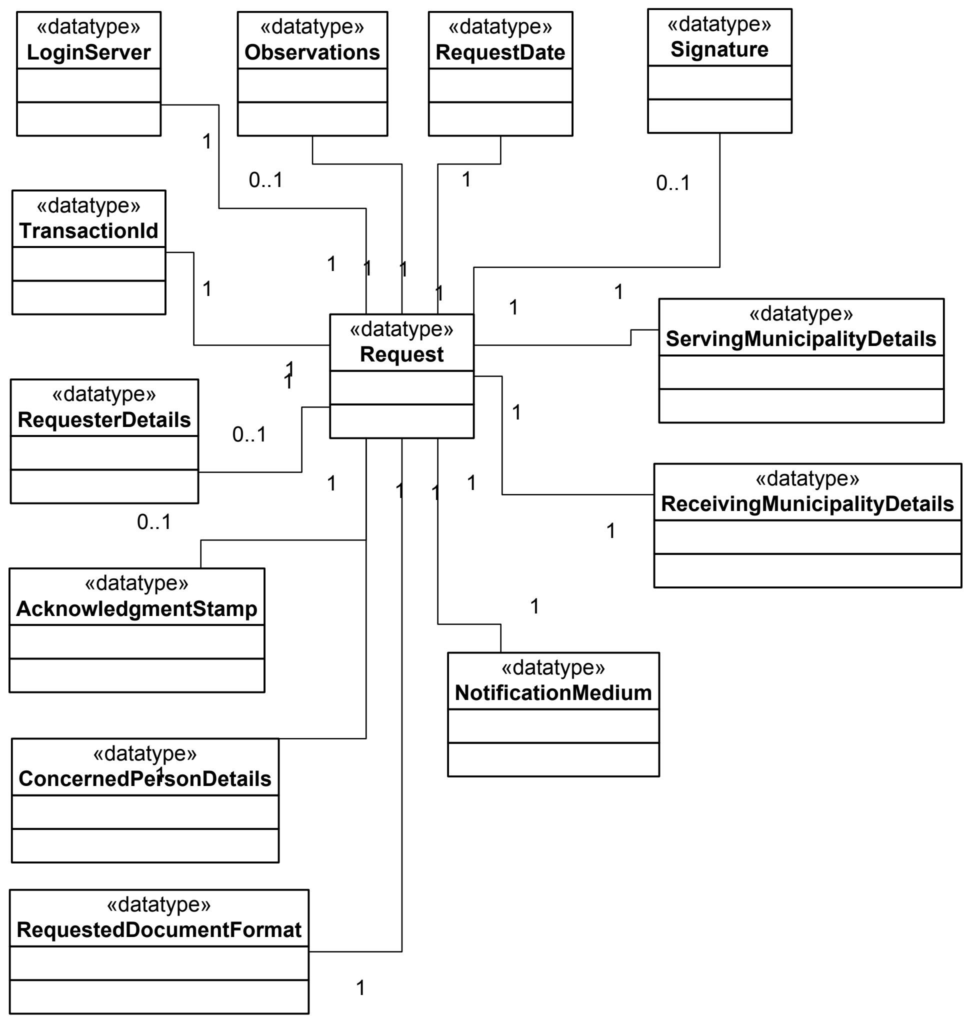
Όπως φαίνεται στο σχήμα, η βασική κλάση που αναπαριστά το έγγραφο πιστοποίησης μητρώου διαμονής ονομάζεται ResidenceCertificationDocument και χρησιμοποιεί κλάσεις που αναπαριστούν διαφορετικά υπο-κομμάτια του εγγράφου σύμφωνα με το σχήμα του: Address, Observations, Terms, Signature, Timestamp, IssuingMunicipality, CertifiedConcernedPersons, AcknowledgementStamp, IssuanceDate, DocumentId (βλ. και παράγραφο 5.3.3.3.2.1).
Στο επόμενο σχήμα αναλύεται η κλάση του αρνητικού εγγράφου πιστοποίησης:



Σχήμα 5-67: Διάγραμμα κλάσεων για το δομικό στοιχείο NegativeResponseCertificationDocument

Η βασική κλάση που αναπαριστά το έγγραφο ονομάζεται NegativeResponseCertificationDocument και χρησιμοποιεί κλάσεις που αναπαριστούν διαφορετικά υπο-κομμάτια του εγγράφου σύμφωνα με το σχήμα του: TimeReference, AcknowledgmentStamp, Timestamp, OriginalRequest, Signature (βλ. και παράγραφο 5.3.3.3.2.1).

Στο επόμενο σχήμα αναλύεται η κλάση της αίτησης:



Σχήμα 5-68: Διάγραμμα κλάσεων για το δομικό στοιχείο Request

Η βασική κλάση που αναπαριστά το έγγραφο ονομάζεται Request και χρησιμοποιεί κλάσεις που αναπαριστούν διαφορετικά υπο-κομμάτια του εγγράφου σύμφωνα με το σχήμα του: LoginServer, Observations, RequestDate, Singnature, TransactionId, ServiceMunicipalityDetails, ReceivingMunicipalityDetails, NotificationMedium, RequesterDetails, AcknowledgementStamp, ConcernedPersonDetails, RequestedDocumentFormat(βλ. και παράγραφο 5.3.3.3.2.1).

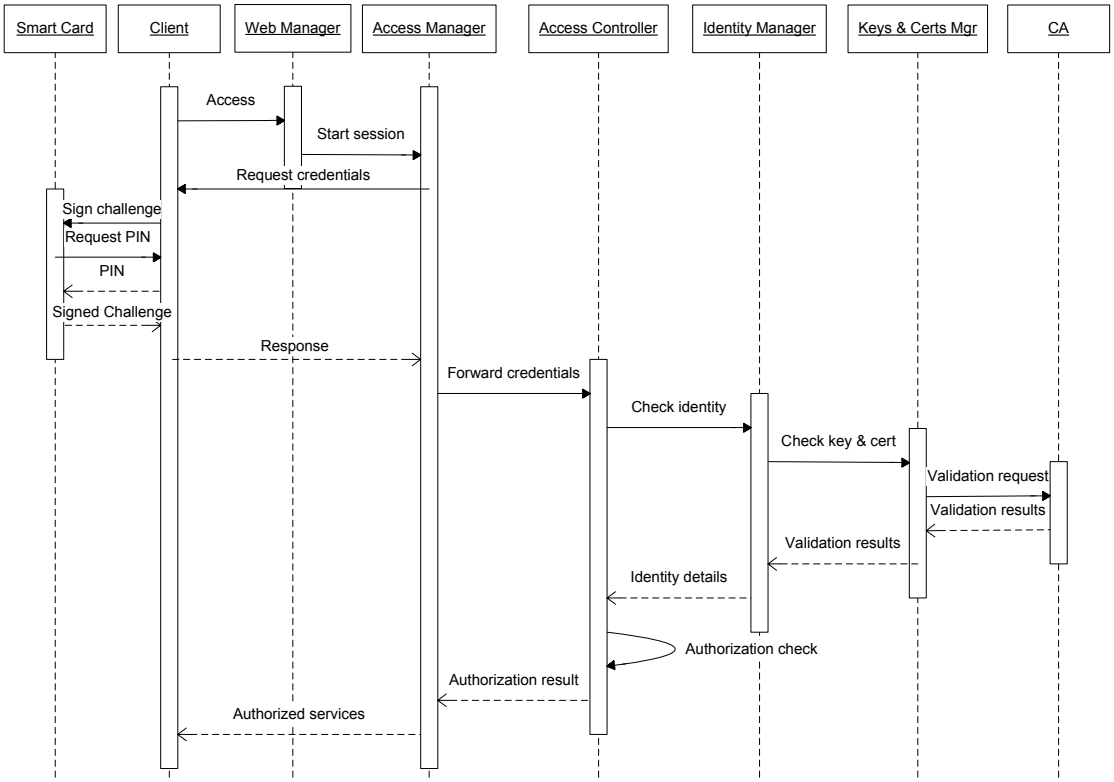
5.3.3.5.3 Διαγράμματα ακολουθίας

Με βάση τις κλάσεις που έχουμε ορίσει, συμπληρώνουμε αρχικά τις προδιαγραφές με διαγράμματα ακολουθίας. Προδιαγράφεται ένα διάγραμμα ακολουθίας για κάθε φάση

της υπηρεσίας, σύμφωνα με τις προδιαγραφές των διεργασιών της παραγράφου 5.3.3.3.1.3.

5.3.3.5.3.1 Φάση αίτησης

Όπως φαίνεται στο διάγραμμα ακολουθίας στο Σχήμα 5-69, ο πολίτης που θέλει πρόσβαση στο σύστημα χρησιμοποιεί μια εφαρμογή «πελάτη» προκειμένου να εκκινήσει τη διαδικασία αυθεντικοποίησης. Οι οντότητες που φαίνονται στο σχήμα εκπροσωπούν τις αντίστοιχες υπηρεσίες της ΑΔΑΑΥ που φιλοξενεί την υπηρεσία η-τιμολόγησης και οι οποίες είναι υπεύθυνες για των έλεγχο των διαπιστευτηρίων του πολίτη (που είναι αποθηκευμένα στην έξυπνη κάρτα του). Τα βήματα που λαμβάνουν χώρα είναι τα ακόλουθα:

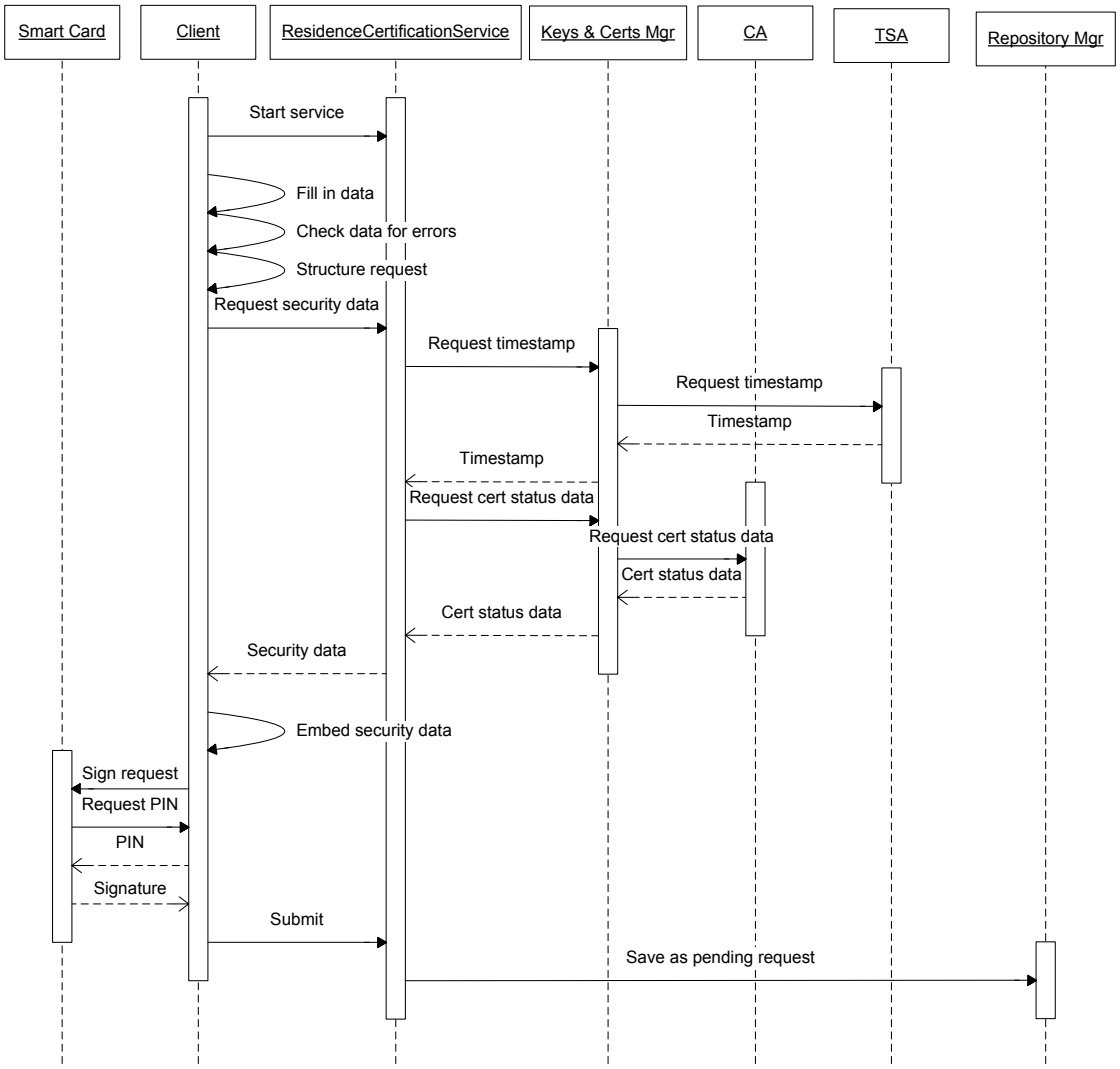


Σχήμα 5-69: Αυθεντικοποίηση και έλεγχος πρόσβασης στο σύστημα

Η εφαρμογή πελάτης εκκινεί την πρόσβαση στο σύστημα μέσω του Web Manager, ο οποίος δίνει την εντολή για δημιουργία νέας συνόδου στον Access Manager. Ο Access Manager δημιουργεί την σύνοδο και κάνει την αίτηση για τα διαπιστευτήρια του πολίτη στην εφαρμογή πελάτη (συνοδευόμενη απο δεδομένα «πρόκλησης» για την διενέργεια ενός πρωτοκόλλου «πρόκλησης-απάντησης»). Η αυθεντικοποίηση βασίζεται στο πρωτόκολλο και την υπογραφή των δεδομένων της απάντησης βάσει των ιδιωτικών κλειδιών που βρίσκονται στην έξυπνη κάρτα.

Εφόσον το πρωτόκολλο ολοκληρωθεί επιτυχώς, το πιστοποιητικό του πολίτη προωθείται μέσω του Access Controller, του Identity Manager στην υπηρεσία Keys & Certificates Manager, η οποία είναι υπεύθυνη για την επικοινωνία με την ΥΔΚ προκειμένου να

ελέγξει την κατάσταση του πιστοποιητικού. Η απάντηση επιστρέφεται στον Access Controller ο οποίος (εφόσον το πιστοποιητικό είναι έγκυρο) ελέγχει της ισχύουσες πολιτικές και επιστρέφει στην εφαρμογή πελάτη του πολίτη τις υπηρεσίες για τις οποίες είναι εξουσιοδοτημένος να χρησιμοποιεί. Στην προκειμένη περίπτωση στον χρήστη δίνεται η δυνατότητα για συμπλήρωση και υπογραφή της αίτησης για έγγραφο πιστοποίησης μητρώου διαμονής.
Η διαδικασία συμπλήρωσης και υπογραφής της αίτησης αναπαρίσταται στο επόμενο διάγραμμα ακολουθίας:

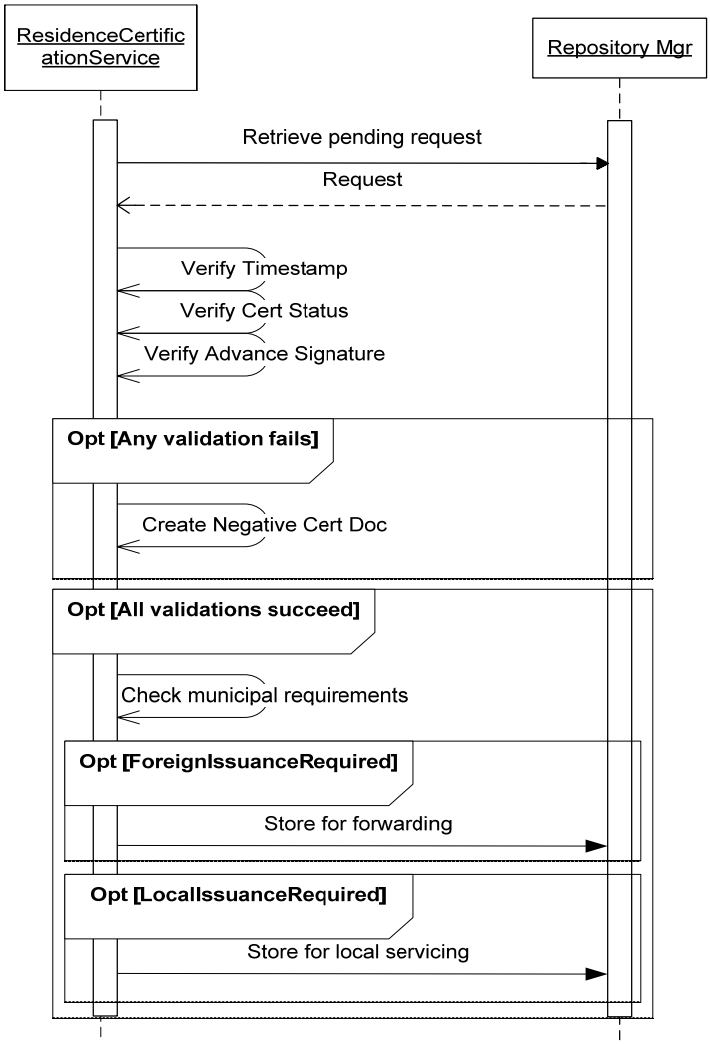


Σχήμα 5-70: Συμπλήρωση αίτησης και ηλεκτρονική υπογραφή

Τα βήματα που ακολουθούνται για την συμπλήρωση της αίτησης, όπως ορίζει η υπηρεσία έκδοσης των εγγράφων πιστοποίησης (ResidenceCertificationService στο σχήμα) είναι τα ακόλουθα:

1. Μέσω της εφαρμογής πελάτη, ο εξουσιοδοτημένος πλέον χρήστης εκκινεί την υπηρεσία, η οποία του παρουσιάζει μια φόρμα αίτησης. Ο πολίτης συμπληρώνει τα απαραίτητα στοιχεία (όπως έχουν οριστεί στο σχήμα πληροφορίας). Η εφαρμογή ταυτόχρονα διενεργεί έλεγχο εάν τα στοιχεία που συμπληρώνονται έχουν την κατάλληλη μορφή και ενημερώνει τον χρήστη για τυχόν λάθη.
2. Εφόσον η αίτηση συμπληρωθεί, ο χρήστης ενεργοποιεί την διαδικασία υπογραφής της. Προκειμένου να δημιουργηθεί μια προηγμένη ηλεκτρονική υπογραφή, αποστέλλεται αρχικά μέσω του Keys & Certificates Manager μια αίτηση για χρονοσφραγίδα σε μια Αρχή Χρονοσφράγισης (TSA). Η αρχή επιστρέφει τα δεδομένα της χρονοσφραγίδας.
3. Στη συνέχεια, και πάλι μέσω του Keys & Certificates Manager, ζητούνται τα δεδομένα κατάστασης του πιστοποιητικού που χρησιμοποιείται για την υπογραφή απο την αντίστοιχη Αρχή Πιστοποίησης. Η αρχή επιστρέφει τα δεδομένα αυτά.
4. Τα συνολικά δεδομένα ασφάλειας (χρονοσφραγίδα και δεδομένα κατάστασης πιστοποιητικού) προωθούνται στην εφαρμογή πελάτη η οποία τα συνδυάζει με την αίτηση και τα υπογράφει σύμφωνα με το πρότυπο προηγμένων ηλεκτρονικών υπογραφών, βάσει των ιδιωτικών κλειδιών που περιλαμβάνονται στην έξυπνη κάρτα του χρήστη (αφού ο χρήστης δώσει το σχετικό PIN).
5. Ως τελικό βήμα, η υπογεγραμμένη πλέον αίτηση προωθείται στην υπηρεσία έκδοσης, η οποία την αποθηκεύει χρησιμοποιώντας την υπηρεσία Repository Manager της ΑΔΑΑΥ ως *«αίτηση σε αναμονή» (pending request)*.

Σημειώνεται επίσης, ότι, τα πιστοποιητικά που χρησιμοποιούνται για την υπογραφή και αυθεντικοποίηση μπορεί να είναι διαφορετικά ή τα ίδια, κάτι που καθορίζεται απο την πολιτική ασφάλειας του οργανισμού. Στην περίπτωση που είναι διαφορετικά, στον χρήστη δίνεται η δυνατότητα επιλογής, ανάλογα με την χρήση μια δεδομένη χρονική στιγμή.
Στο Σχήμα 5-71 παρατίθενται τα βήματα που διενεργούνται προκειμένου να ελεγχθεί εάν η προηγμένη ηλεκτρονική υπογραφή του εγγράφου (αίτηση) που έχει αποθηκευθεί είναι έγκυρη.



Σχήμα 5-71: Επαλήθευση της προηγμένης ηλεκτρονικής υπογραφής και αρχικοί έλεγχοι αίτησης

Τα βήματα είναι τα ακόλουθα:

1. Ελέγχεται η κρυπτογραφική εγκυρότητα της χρονοσφραγίδας στα δεδομένα της αίτησης.
2. Ελέγχεται η εγκυρότητα του πιστοποιητικού που χρησιμοποιήθηκε στην υπογραφή κατά την χρονική στιγμή που έλαβε χώρα η υπογραφή, σύμφωνα με τα περιλαμβανόμενα δεδομένα κατάστασης.
3. Ελέγχεται η κρυπτογραφική εγκυρότητα της ίδιας της υπογραφής για τα δεδομένα της αίτησης, καθώς και οποιαδήποτε άλλα δεδομένα ορίζει το πρότυπο της προηγμένης ηλεκτρονικής υπογραφής.

4. Εάν οποιοδήποτε έλεγχος αποτύχει, τότε δημιουργείται ένα έγγραφο αρνητικής απάντησης, το οποίο αποθηκεύεται ως *«έγγραφο για τοπική επεξεργασία» (stored for local servicing)*.
5. Εάν όλοι έλεγχοι επιτύχουν, τότε γίνεται έλεγχος εάν η αίτηση θα υποστεί επεξεργασία τοπικά, ή αν πρέπει να προωθηθεί σε κάποιον άλλο δήμο. Στην πρώτη περίπτωση αποθηκεύεται ως «έγγραφο για τοπική επεξεργασία», στην δεύτερη ως *«έγγραφο για προώθηση» (stored for forwarding)*.

Οι παραπάνω διαδικασίες για την παραγωγή προηγμένης ηλεκτρονικής υπογραφής και της επαλήθευσή της υπονοούνται στη συνέχεια των προδιαγραφών κάθε φορά που γίνεται χρήση αυτού του μηχανισμού και δεν αναλύονται εκ νέου.

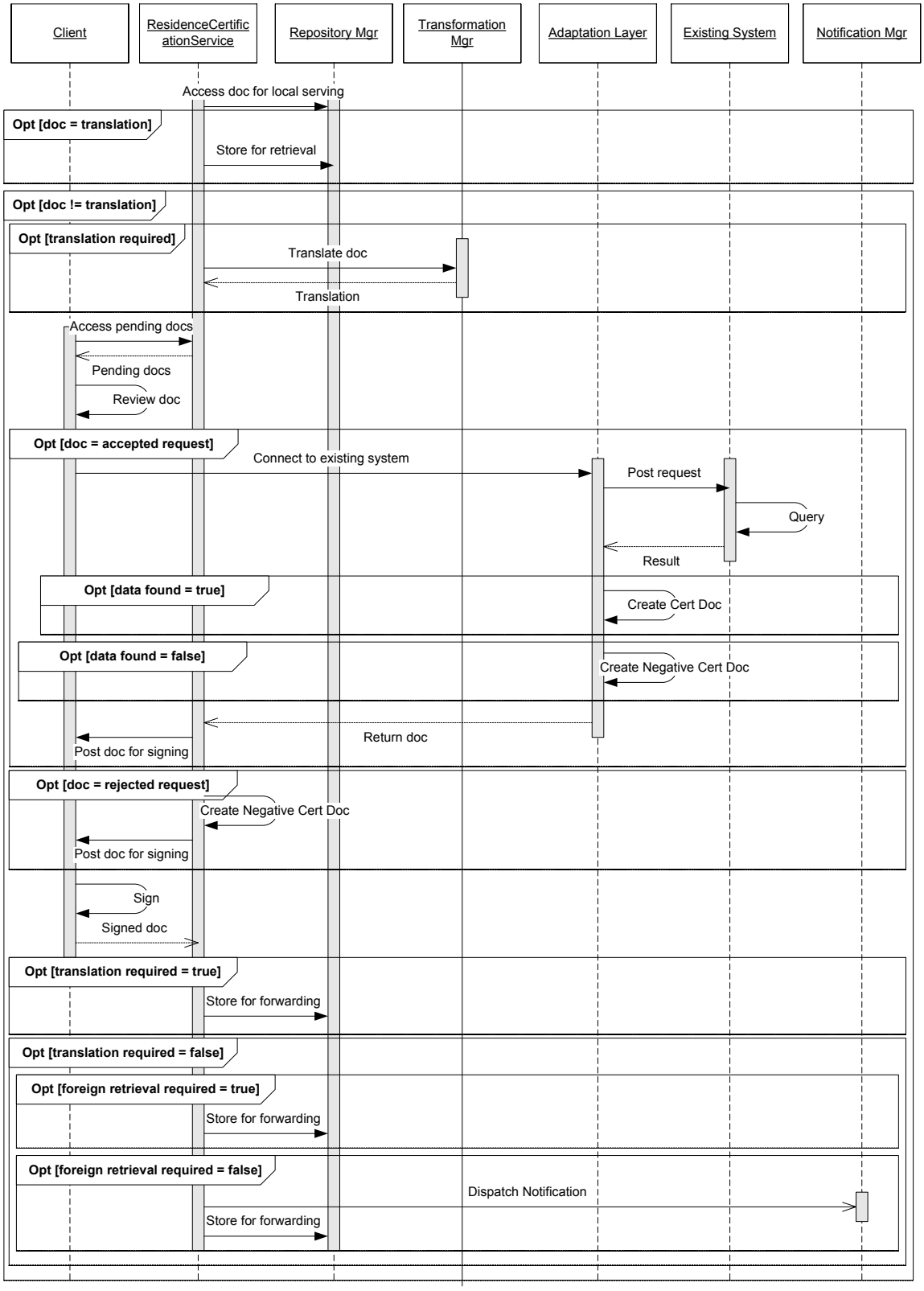
5.3.3.5.3.2 Φάση επεξεργασίας / έκδοσης εγγράφου πιστοποίησης

Στην φάση αυτή πέραν της εφαρμογής πελάτη και της υπηρεσία έκδοσης εμπλέκονται και οι υπηρεσίες μετασχηματισμού μηνυμάτων, επικοινωνίας με υπάρχουσες υποδομές και ειδοποιήσεων. Η διαδικασία αναλύεται στο διάγραμμα ροής στο Σχήμα 5-72. Η υπηρεσία έκδοσης μέσω του Repository Manager ανακτά έγγραφα που έχουν αποθηκευτεί και είναι «έγγραφα για τοπική επεξεργασία». Τα βήματα της διαδικασίας εξαρτώνται απο τον τύπο του εγγράφου που ανακτάται.

- Εάν το έγγραφο είναι μια μετάφραση ή γενικά ένα μετασχηματισμένο έγγραφο, τότε επαναποθηκεύεται αλλά αυτή τη φορά ως *«έγγραφο για ανάκτηση» (stored for retrieval)*.
- Εάν το έγγραφο πρέπει να μετασχηματιστεί, τότε καλείται η υπηρεσία Transformation Manager με τις κατάλληλες παραμέτρους προκειμένου να ληφθεί μια κατάλληλα μετασχηματισμένη μορφή του εγγράφου.

Στη συνέχεια:

- Εάν το έγγραφο είναι έγγραφο αρνητικής απάντησης, τότε προωθείται προς υπογραφή.
- Εάν είναι αίτηση ή ένα μόλις μετασχηματισμένο έγγραφο, προωθείται για έλεγχο απο έναν δημόσιο υπάλληλο μέσω της εφαρμογής πελάτη. Ο Δημόσιος υπάλληλος μπορεί να αποδεχθεί ή να απορρίψει την αίτηση.
    - Σε περίπτωση απόρριψης δημιουργείται ένα έγγραφο αρνητικής απάντησης και προωθείται πάλι προς υπογραφή.
    - Σε περίπτωση αποδοχής, τότε μέσω της υπηρεσίας Adaptation Layer το σύστημα επικοινωνεί με το υπάρχον σύστημα του δήμου με τα μητρώα των πολιτών και ψάχνει για να βρει τα στοιχεία διαμονής. Εάν τα βρει, τότε δημιουργεί ένα έγγραφο πιστοποίησης και το προωθεί για υπογραφή. Εάν όχι, τότε και πάλι δημιουργείται ένα έγγραφο αρνητικής απάντησης και προωθείται αυτό για υπογραφή.



Σχήμα 5-72: Επεξεργασία και έκδοση εγγράφων πιστοποίησης

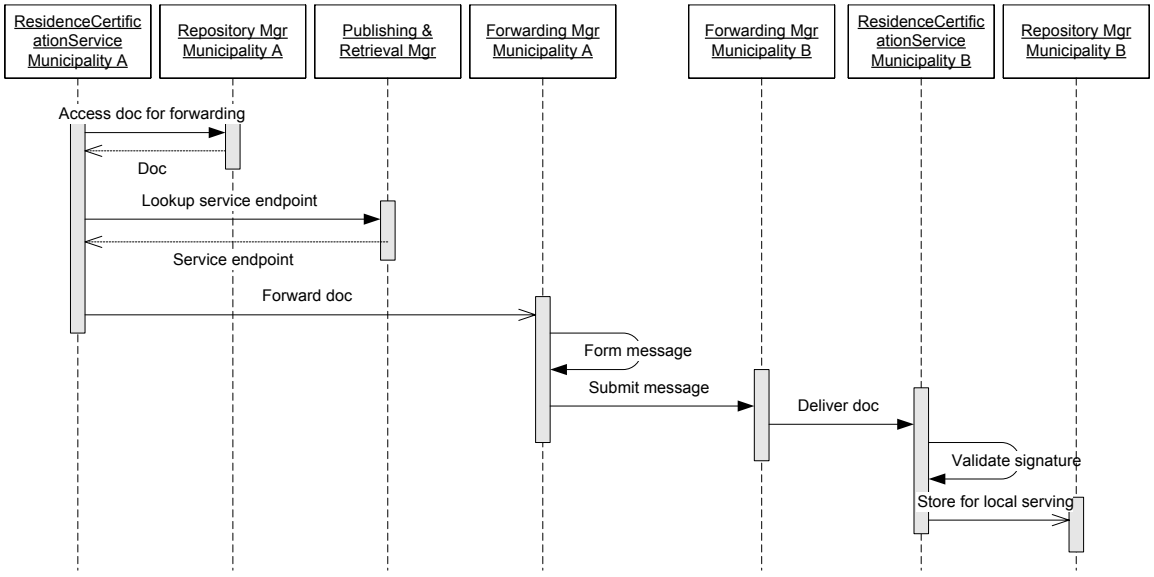
Σε κάθε περίπτωση τα τελικά βήματα του σταδίου είναι ο έλεγχος αν το έγγραφο χρειάζεται περαιτέρω μετασχηματισμούς:

- Αν χρειάζεται (κάτι που σημαίνει ότι πρέπει να προωθηθεί σε άλλο δήμο για να υποστεί τον μετασχηματισμό), τότε αποθηκεύεται ως «έγγραφο για προώθηση».
- Αν όχι, τότε ελέγχεται αν πρέπει να το λάβει ένας πολίτης τοπικά ή απο άλλο δήμο. Στην πρώτη περίπτωση αποθηκεύεται ως «έγγραφο για λήψη» ενώ στη δεύτερη ως «έγγραφο για προώθηση».

Οι υπογραφές που αναφέρονται στη διαδικασία είναι όλες προηγμένες ηλεκτρονικές υπογραφές και πραγματοποιούνται όπως περιγράφηκε στην προηγούμενη φάση για την αίτηση.

5.3.3.5.3.3 Φάση μεταφοράς και λήψης

Η φάση αναλύεται στο Σχήμα 5-73. Εμπλέκονται εκτός της βασικής υπηρεσίας έκδοσης οι υπηρεσίες Repository Manager, Publishing & Retrieval Manager και Forwarding Manager.



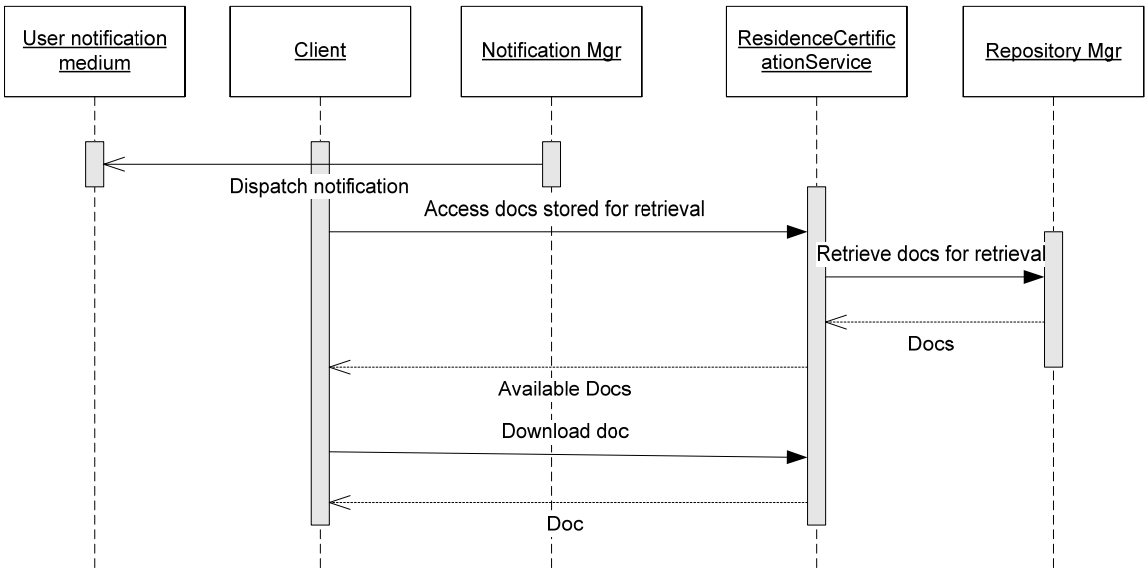
Σχήμα 5-73: Προώθηση εγγράφου απο έναν δήμο σε έναν άλλο

Τα βήματα που ακολουθούνται είναι τα εξής:

- Η υπηρεσία έκδοσης μέσω του Repository Manager λαμβάνει τα έγγραφα που έχουν αποθηκευτεί ως «έγγραφα για προώθηση».
- Βάσει της πληροφορίας για το σε ποιόν δήμο πρέπει να προωθηθεί το έγγραφο, αναζητείται η διεύθυνση της υπηρεσίας (service endpoint) μέσω του Publishing & Retrieval Manager.
- Αποστέλλεται στον Forwarding Manager το έγγραφο και αυτό προωθείται στην αντίστοιχη υπηρεσία του άλλου δήμου. Στο σημείο αυτό ενδέχεται να εφαρμόζονται περαιτέρω μηχανισμοί ασφάλειας στο μήνυμα, σύμφωνα με τις πολιτικές της υπηρεσίας.

- Στην πλευρά του άλλου δήμου, το μήνυμα λαμβάνεται, επαληθεύονται τα στοιχεία ασφάλειας του και αποθηκεύεται ως «έγγραφο για τοπική επεξεργασία».

Η επαλήθευση της προηγμένης ηλεκτρονικής υπογραφής βασίζεται στη διαδικασία που έχει περιγραφεί στην παράγραφο 5.3.3.5.3.1 για την αίτηση.
Η τελική φάση αναπαρίσταται στο διάγραμμα ακολουθίας στο Σχήμα 5-74:

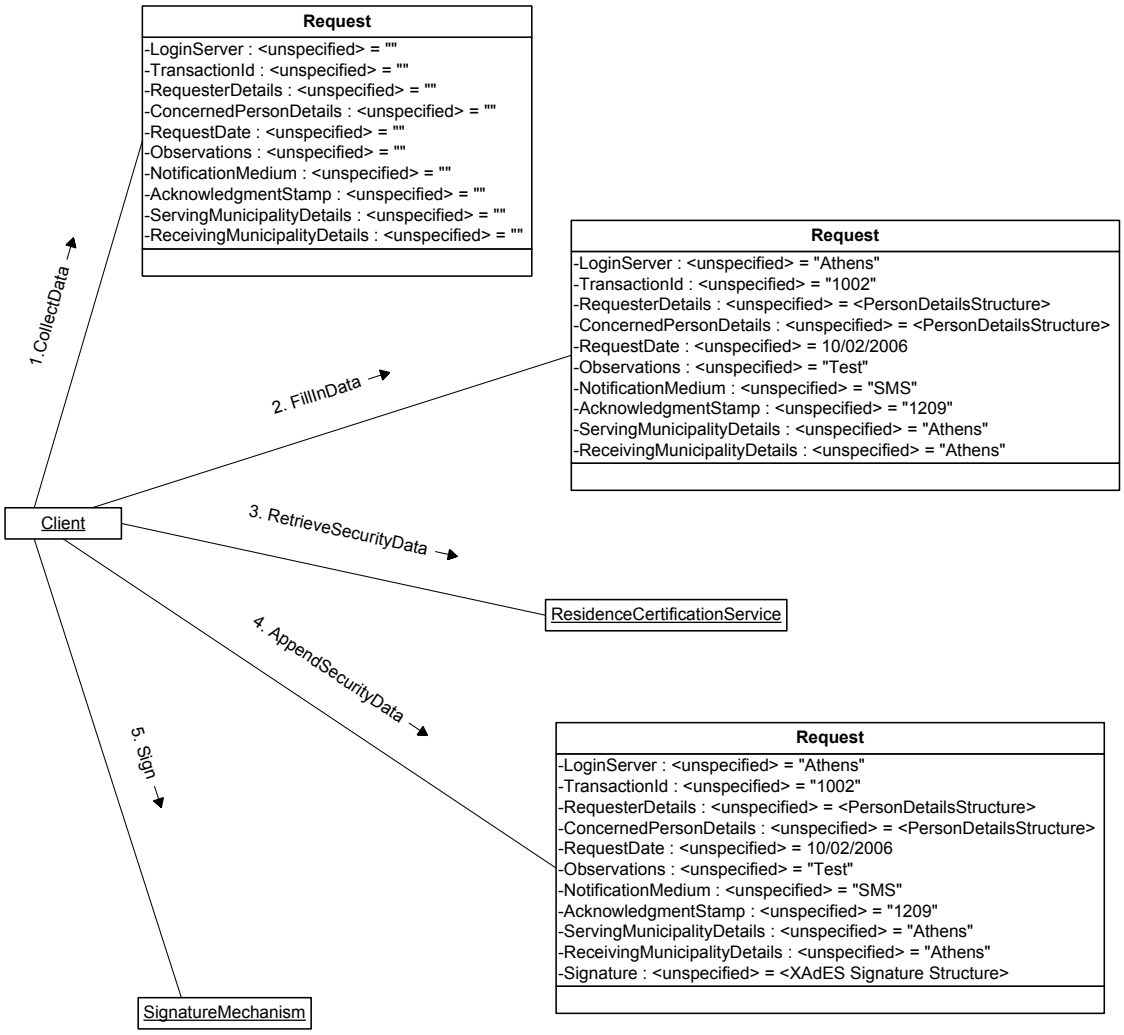


Σχήμα 5-74: Ειδοποίηση πολίτη και λήψη εγγράφων

Ο Notification Manager αποστέλλει την κατάλληλη μορφή ειδοποίησης στον πολίτη σύμφωνα με το τι αυτός είχε δηλώσει στην αίτησή του. Στη συνέχεια ο πολίτης εισέρχεται για μια ακόμη φορά στο σύστημα και λαμβάνει τα έγγραφα που έχουν αποθηκευτεί για λογαριασμό του.

5.3.3.5.4 Διαγράμματα συνεργασίας

Σύμφωνα με την μεθοδολογία, ως τελευταίο κομμάτι των προδιαγραφών της υπολογιστικής όψης, σχεδιάζονται κατάλληλα διαγράμματα συνεργασίας για περαιτέρω ανάλυση και διευκρίνιση των σχέσεων των κλάσεων και των αντικειμένων που απορρέουν απο αυτές. Στην ανάλυση αυτή χρησιμοποιούνται όπου χρειάζεται στατικά σχήματα αντικειμένων πληροφορίας που ανταλλάσσονται.
Το σχήμα που ακολουθεί επιδεικνύει τις καταστάσεις απο τις οποίες περνάει μια αίτηση κατά την διάρκεια της επεξεργασίας της, με χρήση κατάλληλων στατικών σχημάτων:



Σχήμα 5-75: Συνεργασία αντικειμένων για την δημιουργία, συμπλήρωση και υπογραφή ενός εγγράφου «αίτηση»

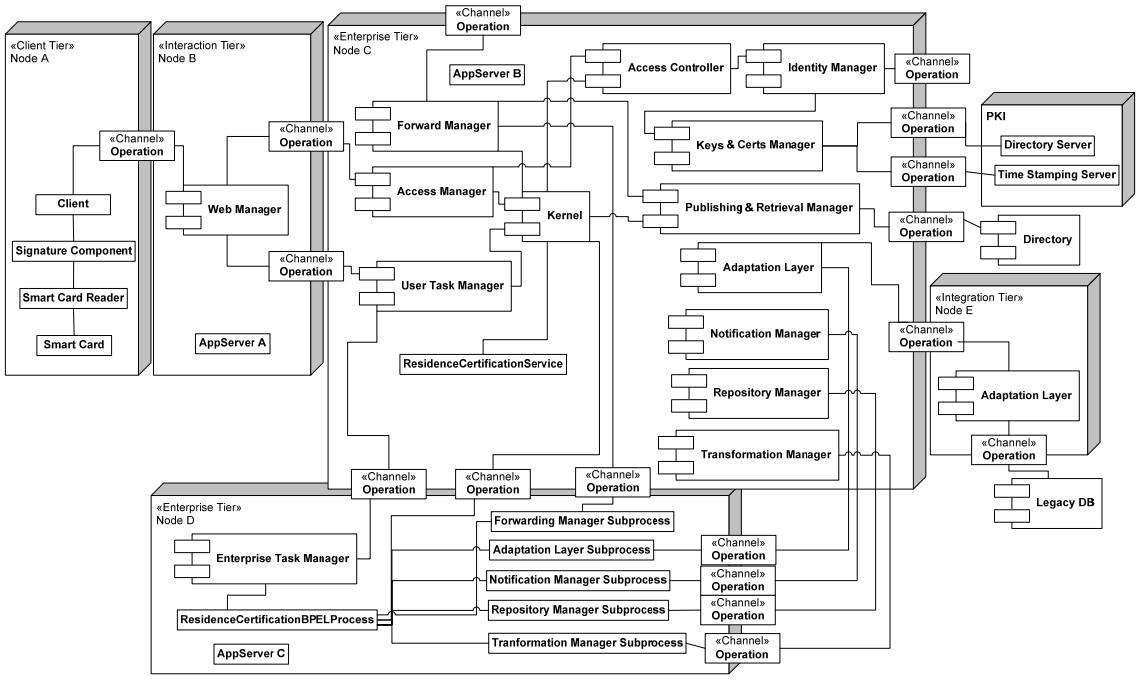
Όπως φαίνεται απο το σχήμα, και σε συμφωνία με τα διαγράμματα ακολουθίας των προηγούμενων παραγράφων, η εφαρμογή πελάτης διαχειρίζεται την κατάσταση μιας αίτησης. Αρχικά δημιουργεί μια άδεια δομή, στην συνέχεια την συμπληρώνει σύμφωνα με τις επιλογές του χρήστη, λαμβάνει τα απαραίτητα δεδομένα ασφάλειας μέσω της ίδιας της υπηρεσίας έκδοσης, τα ενσωματώνει στην δομή του εγγράφου σύμφωνα με το πρότυπο των προηγμένων ηλεκτρονικών υπογραφών και τέλος υλοποιεί και την ίδια την υπογραφή χρησιμοποιώντας τον μηχανισμό υπογραφών και τα κλειδιά στην έξυπνη κάρτα του χρήστη. Η επεξεργασία των υπόλοιπων τύπων η-εγγράφων είναι αντίστοιχη, με τη διαφορά ότι ένα μέρος της πληροφορίας λαμβάνεται απο το υπάρχον σύστημα με το μητρώο των πολιτών και ένα μέρος συμπληρώνεται απο τον εκάστοτε δημόσιο υπάλληλο.

5.3.3.6 5ο Στάδιο: Αναλυτική οργάνωση υπηρεσιών και επιλογή τεχνολογιών

Το στάδιο αυτό περιλαμβάνει την δημιουργία των προδιαγραφών της Όψης Μηχανικού και της Τεχνολογικής Όψης. Και οι δύο αυτές όψεις θεωρούν ότι η υπηρεσία έκδοσης εγγράφων πιστοποίησης μητρώου διαμονής εγκαθίσταται σε μια συνολική αρχιτεκτονική ΑΔΑΑΥ η οποία προσφέρει τις υπηρεσίες που έχουν επιλεγεί στο 3ο στάδιο. Η υπηρεσία κάνει χρήση των υπηρεσιών αυτών προκειμένου να υλοποιήσει τις επιχειρησιακές διεργασίες. Οι όψεις του παρόντος σταδίου αποδίδουν πως θα πρέπει κατανέμονται σε κόμβους τα μηχανικά αντικείμενα **όλων** των υπηρεσιών που χρησιμοποιούνται και ποιες τεχνολογίες χρησιμοποιούνται σε κάθε υπηρεσία.

5.3.3.6.1 Όψη Μηχανικού

Προκειμένου να λειτουργήσει η υπηρεσία, θεωρούμε ότι η συνολική αρχιτεκτονική αποτελείται απο πέντε βασικά επίπεδα στα οποία κατανέμονται οι κόμβοι: ένα επίπεδο πελάτη, ένα επίπεδο αλληλεπίδρασης, δύο επιχειρησιακά επίπεδα και ένα επίπεδο ολοκλήρωσης. Ορίζεται ένα μηχανικό αντικείμενο που αναπαριστά στην υπηρεσία έκδοσης εγγράφων και ένα μηχανικό αντικείμενο για κάθε μια απο τις απαραίτητες υπηρεσίες της ΑΔΑΑΥ. Η κατανομή όλων των μηχανικών αντικειμένων φαίνεται στο συνολικό διάγραμμα εγκατάστασης στο επόμενο σχήμα:



Σχήμα 5-76: Συνολικό διάγραμμα εγκατάστασης όψης μηχανικού αρχιτεκτονικής υποστήριξης της υπηρεσίας έκδοσης εγγράφων πιστοποίησης μητρώου διαμονής

Το σχήμα αποτελεί ένα συνολικό διάγραμμα εγκατάστασης που επιδεικνύει την οργάνωση της ΑΔΑΑΥ για τον δήμο σε πέντε επίπεδα με έναν κόμβο σε κάθε επίπεδο και έναν κόμβο εκτός της αρχιτεκτονικής που εκπροσωπεί την ΥΔΚ, σύμφωνα με τις

αρχές της μεθόδου της παραγράφου 4.3.5.3.3.1.3. Στο σχήμα έχουν τοποθετηθεί και όλα τα απαραίτητα κανάλια επικοινωνίας με τα οποία μηχανικά αντικείμενα που βρίσκονται σε διαφορετικούς κόμβους επικοινωνούν μεταξύ τους καθώς και με άλλες υπηρεσίες σε εξωτερικές αρχιτεκτονικές ή με εξωτερικές οντότητες. Οι συγκεκριμένοι κόμβοι συγκεκριμένα επίπεδα και τα μηχανικά αντικείμενα που περιέχουν αναλύονται ως εξής:

1. *Κόμβος Α* στο επίπεδο πελάτη. Στον κόμβο βρίσκεται η *Εφαρμογή πελάτη (Client)* με την οποία αλληλεπιδρούν οι πολίτες και οι δημόσιοι υπάλληλοι του παραδείγματος και αποτελεί το ένα μέρος της υπηρεσίας διεπαφής χρηστών (βλ. και παραγράφους 4.3.3.3.2.1 και 4.3.4.3.3.2.2.1). Το μηχανικό αντικείμενο εφαρμογής πελάτη επικοινωνεί με το αντικείμενο διαχειριστή ιστοσελίδων στον κόμβο Β μέσω ενός καναλιού λειτουργιών. Στο επίπεδο αυτό επίσης περιλαμβάνεται ένα μηχανικό αντικείμενο που υλοποιεί τους μηχανισμούς ψηφιακών και προηγμένων ηλεκτρονικών υπογραφών *(Signature component)* (βλ. και παραγράφους 4.3.3.3.3.1,4.3.3.3.3.2 και 4.3.4.3.3.2.3.3, 4.3.4.3.3.2.3.4) με χρήση ενός *Αναγνώστη κάρτας (Smart card reader)* και της *Έξυπνης κάρτας (Smart card)* του κάθε χρήστη.
2. *Κόμβος Β* στο επίπεδο αλληλεπίδρασης. Ο κόμβος περιέχει τον *Εξυπηρετητή εφαρμογών Α (App Server A)* και τον *Διαχειριστή ιστοσελίδων (Web manager)* που δέχεται τις αιτήσεις πρόσβασης απο τις εφαρμογές πελάτες, τις αποδομεί κατάλληλα και τις αποστέλλει στο το πρώτο επιχειρησιακό επίπεδο στον κόμβο C, προκειμένου να λάβει τις απαραίτητες απαντήσεις. Τις απαντήσεις τις δομεί σε ιστοσελίδες ή άλλου τύπου έγγραφα, όπως για παράδειγμα XML, και τις επιστρέφει στους πελάτες. Το αντικείμενο διαχείρισης ιστοσελίδων αποτελεί το δεύτερο μέρος της υπηρεσίας διεπαφής χρηστών (βλ. και παραγράφους 4.3.3.3.2.1 και 4.3.4.3.3.2.2.1) και επικοινωνεί απο την μια πλευρά με το αντικείμενο εφαρμογής πελάτη στον κόμβο Α και με τα αντικείμενα διαχειριστή πρόσβασης και εργασιών χρηστών στον κόμβο C μέσω καναλιών λειτουργιών.
3. *Κόμβος C* στο πρώτο επιχειρησιακό επίπεδο, ο οποίος περιέχει τον *Εξυπηρετητή εφαρμογών Β (App Server B)*. Ο κόμβος αυτός αποτελεί την καρδιά της συγκεκριμένης αρχιτεκτονικής όπου φιλοξενείται το μεγαλύτερο μέρος των υπηρεσιών διαχείρισης καθώς και οι βασικές υπηρεσίες, οι υπηρεσίες υποστήριξης υπαρχουσών υποδομών οι υπηρεσίες ασφάλειας. Πιο συγκεκριμένα, τα μηχανικά αντικείμενα που περιλαμβάνονται και υλοποιούν τις παραπάνω υπηρεσίες είναι τα ακόλουθα (σε συμφωνία με τα βασικά στοιχεία της υπολογιστικής όψης που παρουσιάστηκαν στην παράγραφο 4.3.4.3.3.2):
   - Υπηρεσίες και μηχανισμοί διαχείρισης και συντονισμού:
     - Ο *Διαχειριστής πρόσβασης (Access Manager)* υλοποιεί την υπηρεσία πρόσβασης (βλ. και παραγράφους 4.3.3.3.1.1 και 4.3.4.3.3.2.1.1). Δέχεται τις αιτήσεις μέσω του επιπέδου αλληλεπίδρασης, επικοινωνεί με την υπηρεσία ελέγχου πρόσβασης για τις κατάλληλες εξουσιοδοτήσεις και με τον πυρήνα για τις εκκινήσεις διεργασιών που απαιτούνται σύμφωνα με τις αιτήσεις. Επικοινωνεί με τον διαχειριστή ιστοσελίδων στον κόμβο Β μέσω ενός καναλιού λειτουργιών.
     - Ο *Πυρήνας (Kernel)* υλοποιεί το βασικό μέρος της υπηρεσίας διαχείρισης διεργασιών με όλες τις λειτουργίες που αναφέρθηκαν στις παραγράφους 4.3.3.3.1.2 και 4.3.4.3.3.2.1.2, εκτός απο τις σχετικές με τον σχεδιασμό,

τον συντονισμό, την εγκατάσταση και απεγκατάσταση των επιχειρησιακών υπηρεσιών, οι οποίες συντελούνται στο δεύτερο επιχειρησιακό επίπεδο.

- Ο *Διαχειριστής εργασιών χρηστών (User task Manager)* υλοποιεί την υπηρεσία διαχείρισης χρηστών με όλες τις λειτουργίες που αναφέρθηκαν στις παραγράφους 4.3.3.3.1.3 και 4.3.4.3.3.2.1.3. Επικοινωνεί με τον διαχειριστή ιστοσελίδων στον κόμβο Β μέσω ενός καναλιού λειτουργιών.

- Βασικές υπηρεσίες και μηχανισμοί
  - Ο *Διαχειριστής δημοσίευσης και ανάκτησης (Publishing & retrieval manager)* υλοποιεί μια υπηρεσία δημοσίευσης και αναζήτησης σε καταλόγους υπηρεσιών ιστού, με όλες τις λειτουργίες που αναφέρθηκαν στις παραγράφους 4.3.3.3.2.4 και 4.3.4.3.3.2.2.4. Επικοινωνεί με έναν κατάλογο υπηρεσιών ιστού UDDI μέσω ενός καναλιού λειτουργιών. Όσο αφορά στη συγκεκριμένη επιχειρησιακή υπηρεσία που σχεδιάζουμε, ο διαχειριστής δημοσίευσης βοηθά στο να την βρουν δήμοι που προφέρουν αντίστοιχες υπηρεσίες, προκειμένου να διασυνδεθούν μεταξύ τους.
  - Ο *Διαχειριστής αποθετηρίων (Repository Manager)* υλοποιεί μια υπηρεσία διαχείρισης αποθετηρίων σύμφωνα με τις περιγραφές των παραγράφων 4.3.3.3.2.5 και 4.3.4.3.3.2.2.5. Πιο συγκεκριμένα ο διαχειριστής επιτρέπει την πρόσβαση και αναζήτηση σε βάσεις δεδομένων που απαιτούν οι υπηρεσίες τις αρχιτεκτονικής (π.χ. για την αποθήκευση των εκκρεμών αιτήσεων ή εγγράφων πιστοποίησης) εκτός απο την ήδη υπάρχουσα βάση του δήμου, η οποία είναι προσβάσιμη μέσω της υπηρεσίας υποστήριξης υπαρχουσών υποδομών. Ο διαχειριστής ελέγχεται απο μια αντίστοιχη επιχειρησιακή υπο-διεργασία στον κόμβο D μέσω ενός καναλιού λειτουργιών.
  - Ο *Διαχειριστής ειδοποιήσεων (Notification manager)* υλοποιεί μια υπηρεσία ειδοποιήσεων σύμφωνα με τις περιγραφές των παραγράφων 4.3.3.3.2.6 και 4.3.4.3.3.2.2.6. Ο διαχειριστής ειδοποιήσεων στέλνει αυτοματοποιημένα μηνύματα ηλεκτρονικού ταχυδρομείου σε πολίτες ότι το έγγραφο είναι έτοιμο προς παραλαβή. Ο διαχειριστής ελέγχεται απο μια αντίστοιχη επιχειρησιακή υπο-διεργασία στον κόμβο D μέσω ενός καναλιού λειτουργιών.
  - Ο *Διαχειριστής μετασχηματισμών (Transformation manager)* υλοποιεί μια υπηρεσία μετασχηματισμού μηνυμάτων με την λειτουργικότητα που περιγράφεται στις παραγράφους 4.3.3.3.2.2 και 4.3.4.3.3.2.2.2. Ο διαχειριστής ελέγχεται απο μια αντίστοιχη επιχειρησιακή υπο-διεργασία στον κόμβο D μέσω ενός καναλιού λειτουργιών.
  - Ο *Διαχειριστής Προώθησης (Forward Manager)* υλοποιεί μια υπηρεσία προώθησης μηνυμάτων σύμφωνα με τις προδιαγραφές των παραγράφων 4.3.3.3.2.3 και 4.3.4.3.3.2.2.3. Ο Διαχειριστής αυτός λαμβάνει όλα τα μηνύματα με η-έγγραφα και τα αποστέλλει στο σωστό προορισμό τους (σε άλλους οργανισμούς) χρησιμοποιώντας τους κατάλληλους μηχανισμούς ασφάλειας.

- Υπηρεσίες ασφάλειας

- Ο *Ελεγκτής πρόσβασης (Access controller)* υλοποιεί την υπηρεσία ελέγχου πρόσβασης με την λειτουργικότητα που περιγράφεται στις παραγράφους 4.3.3.3.3.5 και 4.3.4.3.3.2.3.2. Ο ελεγκτής κάνει ελέγχους σύμφωνα με τους κανόνες προκαθορισμένων πολιτικών πρόσβασης και τα διαπιστευτήρια που του δίνονται μέσω του διαχειριστή πρόσβασης (για πολίτες και δημοσίους υπαλλήλους) και τα οποία ελέγχει μέσω του διαχειριστή ταυτοτήτων.
- Ο *Διαχειριστής ταυτοτήτων (Identity manager)* υλοποιεί μια υπηρεσία διαχείρισης ταυτότητας με τις λειτουργίες που περιγράφονται στις παραγράφους 4.3.3.3.3.4 και 4.3.4.3.3.2.3.1, προκειμένου να ελέγχει οποιαδήποτε αίτηση για έλεγχο ταυτότητας λαμβάνει απο τον ελεγκτή πρόσβασης. Προκειμένου να διαχειριστεί ταυτότητες, το μηχανικό αυτό αντικείμενο αντλεί πληροφορίες απο δύο πηγές: απο εξωτερικές Αρχές που δημιουργούν και επικυρώνουν διαπιστευτήρια μέσω ενός καναλιού λειτουργιών και απο την εσωτερική υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών.
- Ο *Διαχειριστής κλειδιών και πιστοποιητικών (Keys & Certificates Manager)* υλοποιεί μια υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών με την λειτουργικότητα που περιγράφεται στις παραγράφους 4.3.3.3.3.7 και 4.3.4.3.3.2.3.7. Όπως φαίνεται στο Σχήμα 5-76, οι μέθοδοι που υλοποιεί το αντικείμενο αυτό (έλεγχος κατάστασης πιστοποιητικών και λήψη χρονοσφραγίδων) συντελούνται σύμφωνα με τα δεδομένα που ανταλλάζει με μια εξωτερική ΥΔΚ με την οποία επικοινωνεί μέσω δύο καναλιών λειτουργιών.

• Μια υπηρεσία υποστήριξης υπαρχουσών υποδομών υλοποιείται απο ένα μηχανικό αντικείμενο που δρα ως *Ενδιάμεσο επίπεδο προσαρμογής (Adaptation layer)*. Το αντικείμενο αυτό αποτελεί το κομμάτι της υπηρεσίας απο την πλευρά της αρχιτεκτονικής και επικοινωνεί με το αντίστοιχο αντικείμενο που αποτελεί το κομμάτι της υπηρεσίας που περιλαμβάνεται στον κόμβο Ε, σύμφωνα με την λογική των παραγράφων 4.3.3.3.5 και 4.3.4.3.3.2.5. Τα δύο μέρη της υπηρεσίας επικοινωνούν μέσω ενός καναλιού λειτουργιών.

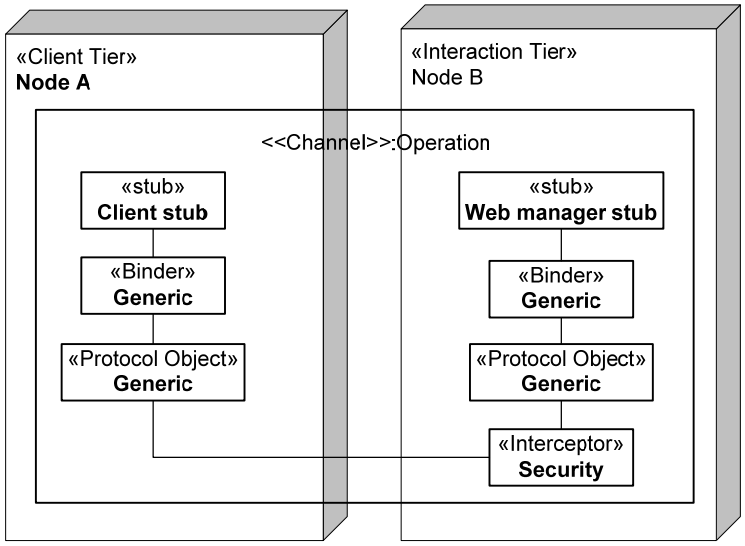
• Ένα στιγμιότυπο της υπηρεσίας ResidenceCertificationService δημιουργείται κάθε φορά που επιλέγεται απο έναν χρήστη η υπηρεσία έκδοσης εγγράφων πιστοποίησης μητρώου διαμονής και τρέχει στον εξυπηρετητή υλοποιώντας όλες τις βασικές διεπαφές που μια τέτοια υπηρεσία πρέπει να διαθέτει προκειμένου να ελέγχεται ο κύκλος ζωής της απο τον πυρήνα (εκκίνηση και διακοπή της υπηρεσίας κ.λ.π). Οι πραγματικές επιχειρησιακές λειτουργίες και ο απαραίτητος συντονισμός και χρονισμός επιτυγχάνονται απο την υλοποίηση της διεργασίας BPEL στο δεύτερο επιχειρησιακό επίπεδο όπως περιγράφεται στον επόμενο κόμβο.

4. *Κόμβος D* στο δεύτερο επιχειρησιακό επίπεδο, ο οποίος περιέχει τον *Εξυπηρετητή εφαρμογών C (App Server C)*. Αυτός ο κόμβος περιλαμβάνει το αντικείμενο *Διαχειριστή επιχειρησιακών διεργασιών (Enterprise Task Manager)*, ο οποίος επιτελεί τις διαχειριστικές εργασίες τις σχετικές με τον σχεδιασμό, συντονισμό, εγκατάσταση και απεγκατάσταση των επιχειρησιακών υπηρεσιών και υπο-υπηρεσιών. Οι υπο-υπηρεσίες αποτελούν υπηρεσίες ιστού που επικοινωνούν μέσω καναλιών λειτουργιών με τις πραγματικές αντίστοιχες βασικές υπηρεσίες στο πρώτο

επιχειρησιακό επίπεδο και τις διαχειρίζονται (ως ένα είδος wrappers). Αυτό σημαίνει ότι ο σχεδιαστής έχει την ευχέρεια καθορίζοντας την λειτουργικότητα της *Υπηρεσίας έκδοσης εγγράφων πιστοποίησης μητρώου διαμονής (ResidenceCertificationBPELProcess)*, να συνθέσει κάποιες απο τις φάσεις της χρησιμοποιώντας το κατάλληλο σύνολο υπο-υπηρεσιών (στην προκειμένη περίπτωση *υπο-υπηρεσία προώθησης μηνυμάτων*, *υπο-υπηρεσία ειδοποιήσεων, υπο-υπηρεσία υπάρχουσας υποδομής*, *υπο-υπηρεσία διαχείρισης αποθετηρίου* και *υπο-υπηρεσία μετασχηματισμού μηνυμάτων*). Ο Διαχειριστής επιχειρησιακών διεργασιών και σχεδιαζόμενη υπηρεσία επικοινωνεί μέσω καναλιών λειτουργιών με τον πυρήνα στον κόμβο C προκειμένου να υποστηρίζονται οι βασικές λειτουργίες εγκαθιδρύσεως συνόδων και η χρησιμοποίηση των μηχανισμών ασφάλειας, ο οποίες είναι διαθέσιμές μόνο μέσω του πυρήνα.

5. *Κόμβος Ε* στο επίπεδο ολοκλήρωσης. Στον κόμβο Ε περιλαμβάνεται το κομμάτι της υπηρεσίας υποστήριξης υπαρχουσών υποδομών που ολοκληρώνει το υπάρχον σύστημα του δήμου (*Βάση δεδομένων (Legacy DB)* με στοιχεία μητρώου διαμονής των πολιτών). Η υπηρεσία υλοποιείται απο ένα αντικείμενο *Ενδιάμεσου επιπέδου προσαρμογής (Adaptation layer)*, το οποίο γνωρίζει πως να επικοινωνεί απο τη μια πλευρά με το αντίστοιχο αντικείμενο στον κόμβο C μέσω ενός καναλιού λειτουργιών, και απο την άλλη με το υπάρχον σύστημα μέσω ενός άλλου καναλιού λειτουργιών.

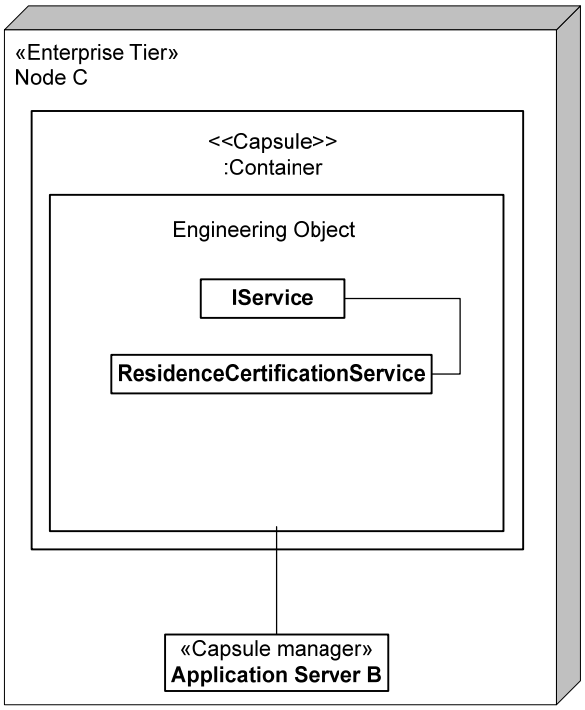
Το διάγραμμα λεπτομέρειας για το κανάλι μεταξύ της εφαρμογής πελάτη και του διαχειριστή ιστοσελίδων είναι όπως στο ακόλουθο σχήμα:



Σχήμα 5-77: Διαγράμματος λεπτομέρειας του καναλιού ανάμεσα στην εφαρμογή πελάτη και τον διαχειριστή ιστοσελίδων

Το σχήμα επιδεικνύει την γενική μορφή του καναλιού στην όψη μηχανικού σύμφωνα με τις αρχές της παραγράφου 4.3.5.3.3.1.3.2. Τα στελέχη για στο υψηλότερο επίπεδο επικοινωνίας υλοποιούνται απο τα μηχανικά αντικείμενα που επικοινωνούν και το κανάλι απαιτεί την ύπαρξη ενός αναχαιτιστή για την παροχή σε χαμηλό επίπεδο κατάλληλων μηχανισμών ασφάλειας (και άρα την κατάλληλη μετάφραση των δεδομένων

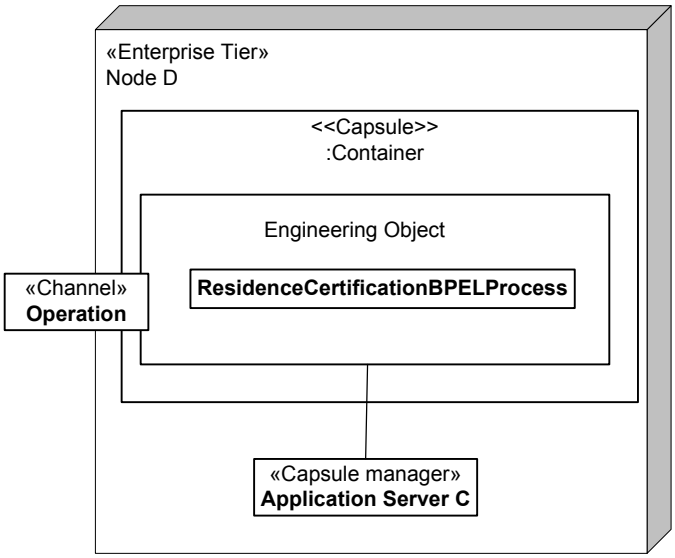
ανάμεσα στα δύο αντικείμενα πρωτοκόλλου ώστε το ένα να αποδέχεται και να κατανοεί τα ασφαλή δεδομένα που του στέλνει το άλλο). **Όλα** τα κανάλια που περιέχονται στο συνολικό διάγραμμα εγκατάστασης έχουν την ίδια μορφή με το παραπάνω, και δεν επαναλαμβάνονται.
Οι προδιαγραφές της όψης μηχανικού ολοκληρώνονται με ένα διάγραμμα λεπτομέρειας στην όψη μηχανικού για το αντικείμενο της υπηρεσίας έκδοσης εγγράφων πιστοποίησης σε πλήρη αντιστοίχηση με τις προδιαγραφές της υπολογιστικής όψης, όπως φαίνεται στο Σχήμα 5-78 και το :



Σχήμα 5-78: Διάγραμμα λεπτομέρειας για το μηχανικό αντικείμενο υπηρεσίας έκδοσης εγγράφων πιστοποίησης μητρώου διαμονής

Παρατηρούμε ότι:

- Το αντικείμενο βρίσκεται στον κόμβο C.
- Εμπεριέχει τα δύο βασικά στοιχεία IService (διεπαφή) και ResidenceCertificationService, σε πλήρη αντιστοιχία με τα στοιχεία της υπολογιστικής όψης.
- Το αντικείμενο επικοινωνεί με τις απαραίτητες υπηρεσίες της αρχιτεκτονικής εσωτερικά στον κόμβο C, οπότε δεν εδραιώνονται κανάλια για αυτή την επικοινωνία.
- Το αντικείμενο λειτουργεί στον υποδοχέα του εξυπηρετητή εφαρμογών B.



Σχήμα 5-79: Διάγραμμα λεπτομέρειας για το μηχανικό αντικείμενο ResidenceCertificationServiceBPELProcess

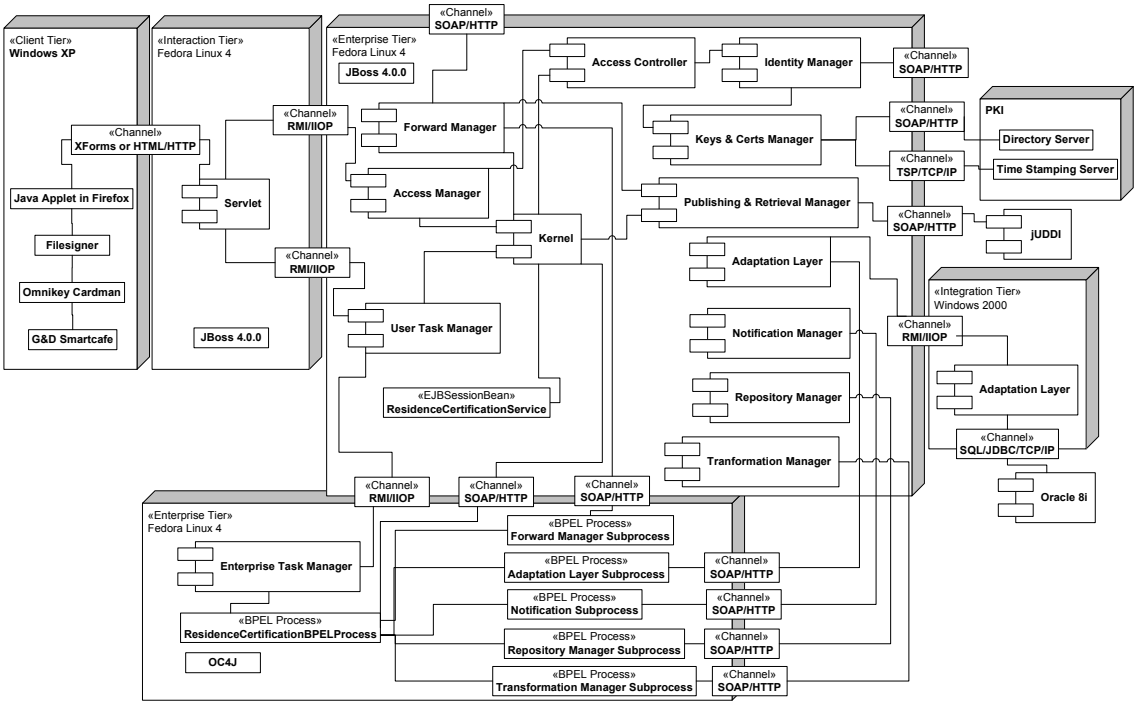
Για το αντικείμενο αυτό παρατηρούμε ότι:

- Βρίσκεται στον κόμβο D.
- Εμπεριέχει το βασικό στοιχείο ResidenceCertificationServiceBPELProcess, σε πλήρη αντιστοιχία με τα στοιχεία της υπολογιστικής όψης.
- Το αντικείμενο επικοινωνεί με τις απαραίτητες υπηρεσίες της αρχιτεκτονικής εσωτερικά στον κόμβο D (συμπεριλαμβανομένου υπο-διεργασίες BPEL), οπότε δεν εδραιώνονται κανάλια για αυτή την επικοινωνία. Η εξωτερική πρόσβαση με την αντίστοιχη υπηρεσία BPEL στο πρώτο επιχειρησιακό επίπεδο γίνεται μέσω ενός καναλιού λειτουργιών.
- Το αντικείμενο λειτουργεί στον υποδοχέα του εξυπηρετητή εφαρμογών C.

Οι προδιαγραφές των μηχανικών αντικειμένων όλων των υπόλοιπων υπηρεσιών θεωρούνται δεδομένες και δεν αποτελούν μέρος της διατριβής.

5.3.3.6.2 Τεχνολογική Όψη

Το συνολικό διάγραμμα εγκατάστασης της τεχνολογικής όψης προκύπτει απο το διάγραμμα στο Σχήμα 5-76, το οποίο έχει εμπλουτιστεί με τεχνολογίες, όπως φαίνεται στο ακόλουθο σχήμα:



Σχήμα 5-80: Συνολικό διάγραμμα εγκατάστασης τεχνολογικής όψης αρχιτεκτονικής υπηρεσίας έκδοσης εγγράφων πιστοποίησης μητρώου διαμονής

Οι τεχνολογικές επιλογές που έχουν γίνει αναλύονται για κάθε κόμβο ως εξής:

1. Ο κόμβος Α στο επίπεδο πελάτη χρησιμοποιεί λειτουργικό Windows XP. Η Εφαρμογή πελάτη (Client) θα υλοποιηθεί ως ένα java applet το οποίο θα τρέχει στους χρησιμοποιούμενους φυλλομετρητές που στην προκειμένη περίπτωση θα είναι Mozilla Firefox 1.5. Το applet επικοινωνεί με το servlet διαχείρισης ιστοσελίδων στον κόμβο Β ανταλλάσσοντας απλές HTML σελίδες πάνω απο HTTP ή φόρμες βασισμένες στο πρότυπο XForms (όπως φαίνεται απο το αντίστοιχο κανάλι στο σχήμα) (βλ. και παραγράφους 4.3.5.4.5.1.4 και 4.3.5.4.5.1.5). Το applet χρησιμοποιεί την βιβλιοθήκη Filesigner (βλ. και παράγραφο 3.2.2) για την παραγωγή ψηφιακών και προηγμένων ηλεκτρονικών υπογραφών με χρήση ενός αναγνώστη κάρτας Omnikey Cardman και μιας έξυπνης κάρτας G&D Smartcafe.
2. Ο κόμβος Β στο επίπεδο αλληλεπίδρασης χρησιμοποιεί λειτουργικό σύστημα Fedora Linux 4. Ο κόμβος περιέχει έναν εξυπηρετητή εφαρμογών JBoss 4.0.0 στον οποίο ο Διαχειριστής ιστοσελίδων υλοποιείται με java servlets που δέχονται τις αιτήσεις πρόσβασης απο τα applets των χρηστών μέσω του καναλιού XForms/HTTP ή HTML/HTTP . Απο την άλλη πλευρά, τα servlets ανταλλάσσουν δεδομένα με τις εφαρμογές που τρέχουν στον εξυπηρετητή εφαρμογών του κόμβου C μέσω καναλιών RMI/IIOP (βλ. παράγραφο 4.3.5.4.5.1.2).
3. Ο κόμβος C στο πρώτο επιχειρησιακό επίπεδο χρησιμοποιεί λειτουργικό σύστημα Linux Fedora 4 και περιέχει επίσης έναν εξυπηρετητή εφαρμογών JBoss 4.0.0. Ο κόμβος αυτός φιλοξενεί το μεγαλύτερο μέρος των υπηρεσιών διαχείρισης, τις βασικές υπηρεσίες, τις υπηρεσίες υποστήριξης υπαρχουσών υποδομών και τις υπηρεσίες ασφάλειας και οι τεχνολογικές επιλογές (βιβλιοθήκες, πρότυπα, προϊόντα)

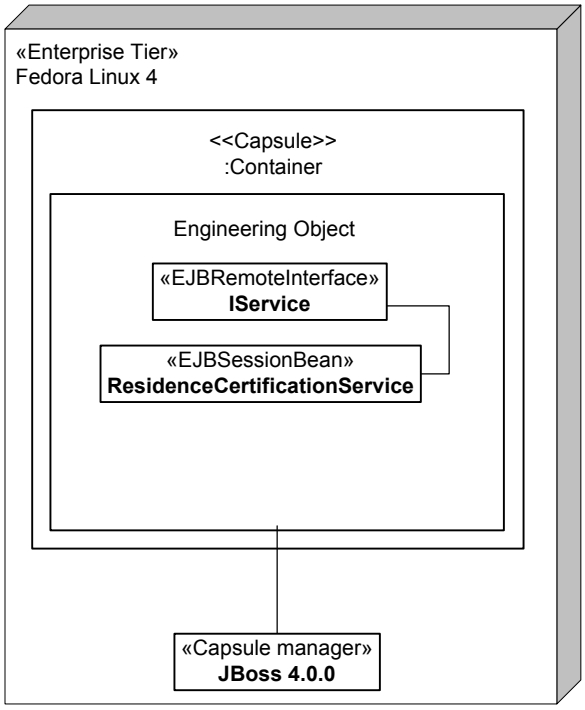
θεωρούνται αναλυμένες στις προδιαγραφές της συνολικής ΑΔΑΑΥ που φιλοξενεί την υπηρεσία έκδοσης εγγράφων πιστοποίησης μητρώου διαμονής. Συνοπτικά οι τεχνολογίες που προτείνονται για μια πιθανή ΑΔΑΑΥ είναι οι ακόλουθες:

- Υπηρεσίες και μηχανισμοί διαχείρισης και συντονισμού:
  - Ο Διαχειριστής πρόσβασης επικοινωνεί με τα servlets του διαχειριστή ιστοσελίδων στον κόμβο Β μέσω ενός καναλιού RMI/IIOP.
  - Ο Διαχειριστής εργασιών χρηστών επικοινωνεί με τον διαχειριστή ιστοσελίδων στον κόμβο Β μέσω ενός καναλιού RMI/IIOP.
- Βασικές υπηρεσίες και μηχανισμοί
  - Ο Διαχειριστής δημοσίευσης και ανάκτησης επικοινωνεί με έναν κατάλογο υπηρεσιών ιστού UDDI μέσω ενός καναλιού SOAP/HTTP (βλ. παράγραφο 4.3.5.4.5.1.1). Ο κατάλογος UDDI που χρησιμοποιείται είναι μια υλοποίηση του λογισμικού ανοιχτού κώδικα jUDDI [jUDDI].
  - Ο Διαχειριστής αποθετηρίων ελέγχεται απο μια επιχειρησιακή υπο-διεργασία στον κόμβο D μέσω ενός καναλιού SOAP/HTTP.
  - Ο Διαχειριστής ειδοποιήσεων ελέγχεται απο μια επιχειρησιακή υπο-διεργασία στον κόμβο D μέσω ενός καναλιού SOAP/HTTP.
  - Ο Διαχειριστής μετασχηματισμού μηνυμάτων ελέγχεται απο μια επιχειρησιακή υπο-διεργασία στον κόμβο D μέσω ενός καναλιού SOAP/HTTP.
  - Ο Διαχειριστής προώθησης μηνυμάτων ελέγχεται απο μια επιχειρησιακή υπο-διεργασία στον κόμβο D μέσω ενός καναλιού SOAP/HTTP.
- Υπηρεσίες ασφάλειας
  - Ο Διαχειριστής ταυτοτήτων επικοινωνεί με εξωτερικές Αρχές που δημιουργούν και επικυρώνουν διαπιστευτήρια και ισχυρισμούς σύμφωνα με το πρότυπο SAML μέσω ενός καναλιού SOAP/HTTP.
  - Ο Διαχειριστής κλειδιών και πιστοποιητικών χρησιμοποιεί το πρότυπο XKMS για να επικοινωνήσει με την ΥΔΚ μέσω ενός καναλιού SOAP/HTTP και το πρότυπο RFC 3161 για το πρωτόκολλο χρονοσφράγισης πάνω απο ένα κανάλι TSP/TCP/IP (βλ. παράγραφο 4.3.5.4.5.1.3).
- Τα αντικείμενα που υλοποιούν τα Ενδιάμεσα επίπεδα προσαρμογής στους κόμβους C και E επικοινωνούν μέσω ενός καναλιού RMI/IIOP.
- Το αντικείμενο ResidenceCertificationService που υλοποιεί την διεπαφή των υπηρεσιών της αρχιτεκτονικής και είναι υλοποιημένο ως Session EJB.

4. Ο κόμβος D στο δεύτερο επιχειρησιακό επίπεδο χρησιμοποιεί λειτουργικό σύστημα Fedora Linux 4 και περιέχει έναν εξυπηρετητή εφαρμογών Oracle με υποδοχέα εφαρμογών J2EE (*Oracle application server container for J2EE – OC4J*) [OC4J]. Ο Διαχειριστής επιχειρησιακών διεργασιών αποτελεί μια μηχανή BPEL της Oracle (Oracle BPEL engine), ο οποίος επιτελεί τις διαχειριστικές εργασίες τις σχετικές με τον σχεδιασμό, συντονισμό, εγκατάσταση και απεγκατάσταση των επιχειρησιακών υπηρεσιών και υπο-υπηρεσιών. Ο Διαχειριστής επιχειρησιακών διεργασιών και η υπηρεσία έκδοσης εγγράφων πιστοποίησης μητρώου διαμονής επικοινωνεί μέσω καναλιών SOAP/HTTP με τον πυρήνα στον κόμβο C. Επίσης ο Διαχειριστής επιχειρησιακών διεργασιών επικοινωνεί με ένα κανάλι RMI/IIOP με τον διαχειριστή εργασιών χρηστών στον κόμβο C.

5. Ο κόμβος Ε στο επίπεδο ολοκλήρωσης χρησιμοποιεί λειτουργικό σύστημα Windows 2000. Το Ενδιάμεσο επίπεδο προσαρμογής επικοινωνεί απο τη μια πλευρά με το αντίστοιχο αντικείμενο στον κόμβο C μέσω ενός καναλιού RMI/IIOP, και απο την άλλη με την υπάρχουσα βάση δεδομένων μέσω ενός καναλιού SQL/JDBC/TCP/IP (βλ. παράγραφο 4.3.5.4.5.1.6). Η υπάρχουσα βάση δεδομένων του δήμου του παραδείγματος είναι μια Oracle 8i.

Η παραπάνω ανάλυση θεωρεί ότι τα διαγράμματα λεπτομέρειας των καναλιών που αναφέρονται ότι χρησιμοποιούνται, είναι όπως παρουσιάζονται ως βασικά στοιχεία όψης στην παράγραφο 4.3.5.4.5.1.
Η τεχνολογική όψη του διαγράμματος λεπτομέρειας του σύνθετου αντικειμένου της υπηρεσίας έκδοσης εγγράφων πιστοποίησης είναι η ακόλουθη:



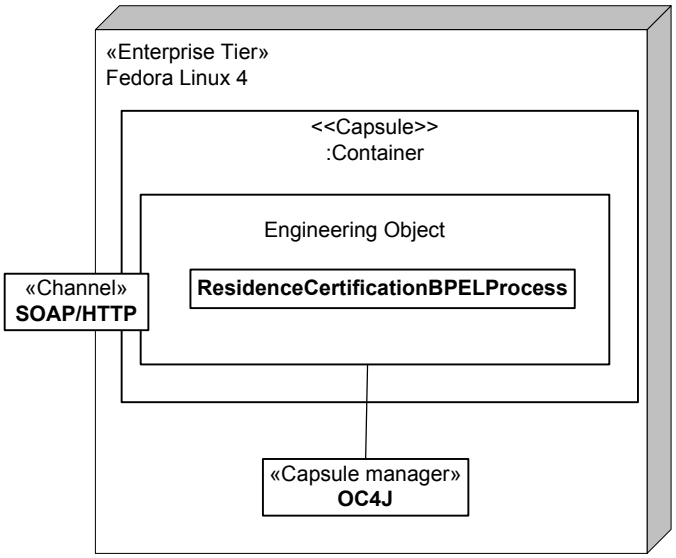
Σχήμα 5-81: Διάγραμμα λεπτομέρειας τεχνολογικής όψης αντικειμένου υπηρεσίας έκδοσης εγγράφων πιστοποίησης μητρώου διαμονής

Οι τεχνολογικές λεπτομέρειες του αντικειμένου της υπηρεσίας αναλύονται ως εξής:

- Το λειτουργικό σύστημα στον κόμβο που βρίσκεται το αντικείμενο είναι Fedora Linux 4.
- Το αντικείμενο επικοινωνεί με άλλα αντικείμενα εκτός του κόμβου του μέσω ενός καναλιού SOAP/HTTP.
- Το αντικείμενο υλοποιεί την διεπαφή IService που είναι μια διεπαφή απομακρυσμένης πρόσβασης, ενώ η ίδια η υπηρεσία αποτελεί ένα EJBSessionBean σύμφωνα με τις αρχές μιας αρχιτεκτονικής J2EE.
- Ο εξυπηρετητής εφαρμογών στον υποδοχέα του οποίου φιλοξενείται το αντικείμενο είναι ο JBoss 4.0.0.

- Στην υλοποίηση της υπηρεσίας έκδοσης εγγράφων πιστοποίησης μητρώου διαμονής έχουν χρησιμοποιηθεί οι ακόλουθες τεχνολογίες/πρότυπα/βιβλιοθήκες: η βιβλιοθήκη UBL [UBL1.0] και τα αποτελέσματα προτυποποίησης των εργασιών του e-GIF [Hunter04] για τον καθορισμό των σχημάτων των μηνυμάτων που ανταλλάσσονται ώστε να καλύπτεται η απαραίτητη πληροφορία για τα η-έγγραφα που έχουν οριστεί, την ανοιχτού κώδικα βιβλιοθήκη που έχει παραχθεί στο κρατικό πρόγραμμα η-διακυβέρνησης στην Εσθονία [EID03] για την παραγωγή προηγμένων ηλεκτρονικών υπογραφών (η βιβλιοθήκη έχει αναβαθμιστεί και τροποποιηθεί προκειμένου να συμμορφώνεται πλήρως με το πρότυπο XAdES), το πρότυπο SOAP, η υλοποίηση κρυπτογραφίας XML του Apache Group, το περιβάλλον υλοποίησης J2EE v. 1.5.0_06 και οι σχετικές βιβλιοθήκες για την παραγωγή μηνυμάτων SOAP και ο JBoss 4.0.0 ως εξυπηρετητής εφαρμογών.

Όσο αφορά στο δεύτερο αντικείμενο που έχει οριστεί στο διάγραμμα στο Σχήμα 5-79, οι αντίστοιχες προδιαγραφές στην τεχνολογική όψη είναι οι εξής:



Σχήμα 5-82: Διάγραμμα λεπτομέρειας τεχνολογικής όψης αντικειμένου ResidenceCertificationServiceBPELProcess

Οι τεχνολογικές λεπτομέρειες του αντικειμένου αναλύονται ως εξής:

- Το λειτουργικό σύστημα στον κόμβο που βρίσκεται το αντικείμενο είναι Fedora Linux 4.
- Το αντικείμενο επικοινωνεί με άλλα αντικείμενα εκτός του κόμβου του μέσω ενός καναλιού SOAP/HTTP.
- Το αντικείμενο αποτελεί μια διεργασία BPEL σύμφωνα με τις αρχές του αντίστοιχου προτύπου.
- Ο εξυπηρετητής εφαρμογών στον υποδοχέα του οποίου φιλοξενείται το αντικείμενο είναι ο OC4J της Oracle.
- Στην υλοποίηση της διεργασίας BPEL έχουν χρησιμοποιηθεί οι ακόλουθες τεχνολογίες/πρότυπα/βιβλιοθήκες: το πρότυπο SOAP, η γλώσσα BPEL, το λογισμικό

του εξυπηρετητή OC4J και η υλοποίηση της Oracle ενός εξυπηρετητή διεργασιών BPEL (BPEL Process Manager 10.1.2)

Σημειώνεται ότι τα παραπάνω διαγράμματα αντιστοιχούν πλήρως σε αυτά της όψης μηχανικού, ώστε να εξασφαλίζεται η συνέπεια ανάμεσα στην Όψη μηχανικού και την Τεχνολογική όψη.

5.3.3.7 6ο Στάδιο: Υλοποίηση

Η υπηρεσία που προδιαγράφεται στο παρόν κεφάλαιο έχει υλοποιηθεί με την χρήση των ακόλουθων εργαλείων και περιβαλλόντων δημιουργίας λογισμικού σε Java:

- Eclipse IDE 3.1
- Oracle BPEL Designer

Η υλοποίηση της υπηρεσίας έχει γίνει στα πλαίσια του Ευρωπαϊκού έργου eMayor [eMayorD3.1, eMayorD4.1], στο οποίο χρησιμοποιήθηκε ένα μέρος της μεθοδολογίας της παρούσας διατριβής για τον σχεδιασμό. Ένα παράδειγμα μιας διεργασίας BPEL που αντιστοιχεί στην επιχειρησιακή υπηρεσία έκδοσης των εγγράφων πιστοποίησης παρατίθεται στο επόμενο σχήμα:

Σχήμα 5-83: Σχεδιασμός διεργασίας BPEL

Όπως φαίνεται στο σχήμα, τα εργαλεία σχεδιασμού επιτρέπουν την πλήρη αναπαράσταση μιας διεργασίας BPEL γραφικά και τον αυτόματο ορισμό των αντίστοιχων Υπηρεσιών Ιστού, καθώς και την εγκατάστασή τους στον κατάλληλο εξυπηρετητή εφαρμογών του δευτέρου επιχειρησιακού επιπέδου των προδιαγραφών.
Δημοσιεύσεις σχετικές με τον σχεδιασμό και την υλοποίηση της υπηρεσίας είναι οι [Kaliontzoglou05, Kaliontzoglou06c, Kaliontzoglou06d, Oikonomidis05, Meneklis05a, Meneklis05b, Meneklis06].

5.3.3.8 7ο Στάδιο: Έλεγχος συμμόρφωσης και ενημέρωση προδιαγραφών

Το τελευταίο στάδιο εφαρμόζει το τελευταίο στάδιο της μεθοδολογίας προκειμένου να καταγράψει τα σημεία συμμόρφωσης της υπηρεσίας τιμολόγησης προκειμένου να μπορεί να αξιολογηθεί κατά πόσο η υλοποίηση της υπηρεσίας ανταποκρίνεται στις παρούσες προδιαγραφές. Σύμφωνα με την μεθοδολογία η αποτύπωση αρχικά των σημείων αναφοράς ξεκινά με την όψη μηχανικού και συνεχίζει με την υπολογιστική όψη, την όψη πληροφορίας και την επιχειρησιακή όψη, με αυτή τη σειρά.

5.3.3.8.1 Σημεία συμμόρφωσης όψης μηχανικού

Ο παρακάτω πίνακας αναλύει τα σημεία αναφοράς της όψης μηχανικού και δηλώνει ποια απο αυτά καταγράφονται ως σημεία συμμόρφωσης.

Κατηγορία σημείου	Αναγνωριστικό σημείου	Περιγραφή σημείου	Περιγραφή επιθυμητής λειτουργικότητας	Αποδοχή ως σημείο συμμόρφωσης

Προγραμματιστικά	ΟΜΠ00	Ανάμεσα στο αντικείμενο IService και το ResidenceCertificationService.	Το ResidenceCertificationService χρησιμοποιεί επιτυχώς τις μεθόδους που ορίζει η διεπαφή IService (κοινή για όλες τις υπηρεσίες της πλατφόρμας)	Ναι
	ΟΜΠ01	Ανάμεσα στο αντικείμενο IService και τον εξυπηρετητή εφαρμογών Β.	Ο έλεγχος του κύκλου ζωής του αντικειμένου γίνεται επιτυχώς.	Όχι
	ΟΜΠ02	Ανάμεσα στο αντικείμενο ResidenceCertifictionService και τον εξυπηρετητή εφαρμογών Β.	Ο έλεγχος του κύκλου ζωής του αντικειμένου γίνεται επιτυχώς.	Όχι
	ΟΜΠ03	Ανάμεσα στο αντικείμενο ResidenceCertificationServiceBPELProcess και τον εξυπηρετητή εφαρμογών C.	Ο έλεγχος του κύκλου ζωής του αντικειμένου γίνεται επιτυχώς.	Όχι
	ΟΜΠ04	Ανάμεσα στο αντικείμενο ResidenceCertificationService και τον πυρήνα της αρχιτεκτονικής.	Η υπηρεσία χρησιμοποιεί επιτυχώς όλες τις μεθόδους του πυρήνα για την εκκίνησή της.	Ναι
	ΟΜΠ05	Ανάμεσα στο αντικείμενο ResidenceCertificationBPELProcess και τον πυρήνα της αρχιτεκτονικής.	Η διεργασία BPEL χρησιμοποιεί επιτυχώς όλες τις μεθόδους του πυρήνα για τον έλεγχο του κύκλου ζωής του αντικειμένου ResidenceCertificationService.	Ναι
	ΟΜΠ06	Ανάμεσα στο αντικείμενο ResidenceCertificationBPELProcess και το αντικείμενο EnterpriseTaskManager.	Το αντικείμενο EnterpriseTaskManager ελέγχει επιτυχώς την διεργασία BPEL.	Ναι
	ΟΜΠ07	Ανάμεσα στο αντικείμενο ResidenceCertificationBPELProcess και την υπο-διεργασία Adaptation Layer Subprocess.	Η διεργασία ResidenceCertificationBPELProcess ελέγχει και καλεί επιτυχώς την υπο-υπηρεσία σύμφωνα με την επιχειρησιακή λογική.	Ναι
	ΟΜΠ08	Ανάμεσα στο αντικείμενο ResidenceCertificationBPELProcess και την υπο-διεργασία Notification Subprocess.	Η διεργασία ResidenceCertificationBPELProcess ελέγχει και καλεί επιτυχώς την υπο-υπηρεσία σύμφωνα με την επιχειρησιακή λογική.	Ναι
	ΟΜΠ09	Ανάμεσα στο αντικείμενο ResidenceCertificationBPELProcess και την υπο-διεργασία Repository Manager Subprocess.	Η διεργασία ResidenceCertificationBPELProcess ελέγχει και καλεί επιτυχώς την υπο-υπηρεσία σύμφωνα με την	Ναι

			επιχειρησιακή λογική.	
	ΟΜΠ10	Ανάμεσα στο αντικείμενο ResidenceCertificationBPELProcess και την υπο-διεργασία Transformation Manager Subprocess.	Η διεργασία ResidenceCertificationBPELProcess ελέγχει και καλεί επιτυχώς την υπο-υπηρεσία σύμφωνα με την επιχειρησιακή λογική.	Ναι
	ΟΜΠ11	Ανάμεσα στο αντικείμενο ResidenceCertificationBPELProcess και την υπο-υπηρεσία Forward Manager Subprocess.	Η διεργασία ResidenceCertificationBPELProcess ελέγχει και καλεί επιτυχώς την υπο-υπηρεσία σύμφωνα με την επιχειρησιακή λογική.	Ναι
	ΟΜΠ12	Ανάμεσα στα αντικείμενα πρωτοκόλλου του καναλιού λειτουργιών που χρησιμοποιεί το αντικείμενο ResidenceCertificationBPELProcess και ο πυρήνας.	Τα αντικείμενα πρωτοκόλλου ανταλλάσσουν επιτυχώς τα απαραίτητα μηνύματα.	Ναι
	ΟΜΠ13	Ανάμεσα στο αντικείμενο πρωτοκόλλου και τον δεσμευτή του καναλιού λειτουργιών που χρησιμοποιεί η υπηρεσία έκδοσης.	Ο δεσμευτής δεσμεύει επιτυχώς το στέλεχος στο αντικείμενο πρωτοκόλλου.	Ναι
	ΟΜΠ14	Ανάμεσα στο στέλεχος και τον δεσμευτή του καναλιού λειτουργιών που χρησιμοποιεί η υπηρεσία έκδοσης.	Ο δεσμευτής λαμβάνει επιτυχώς τα δεδομένα απο το στέλεχος.	Ναι
Διαλειτουργικά	ΟΜΔ00	Ανάμεσα στα αντικείμενα πρωτοκόλλου του καναλιού λειτουργιών που χρησιμοποιεί η υπηρεσία έκδοσης και ο πυρήνας.	Τα μηνύματα που ανταλλάσσονται ανάμεσα στα δύο αντικείμενα είναι κατανοητά και απο τα δύο.	Ναι

Πίνακας 5-5: Σημεία συμμόρφωσης της Όψης Μηχανικού

5.3.3.8.2 Σημεία συμμόρφωσης υπολογιστικής όψης

Ο παρακάτω πίνακας αναλύει τα σημεία αναφοράς της υπολογιστικής όψης και δηλώνει ποια απο αυτά καταγράφονται ως σημεία συμμόρφωσης.

Κατηγορία σημείου	**Αναγνωριστικό σημείου**	**Περιγραφή σημείου**	**Περιγραφή επιθυμητής λειτουργικότητας**	**Αντίστοιχο σημείο όψης μηχανικού**	**Αποδοχή ως σημείο συμμόρφωσης**
Προγραμματιστικά	ΥΟΠ00	Ανάμεσα στην κλάση IService και την κλάση ResidenceCertificationService.	Η κλάση ResidenceCertificationservice υλοποιεί όλες τις μεθόδους της διεπαφής IService.	ΟΜΠ00	Ναι

Πίνακας 5-6: Σημεία συμμόρφωσης της Υπολογιστικής Όψης

5.3.3.8.3 Σημεία συμμόρφωσης όψης πληροφορίας

Ο παρακάτω πίνακας αναλύει τα σημεία αναφοράς της όψης πληροφορίας και δηλώνει ποια απο αυτά καταγράφονται ως σημεία συμμόρφωσης.

Κατηγορία σημείου	**Αναγνωριστικό σημείου**	**Περιγραφή σημείου**	**Περιγραφή επιθυμητής λειτουργικότητας**	**Αντίστοιχο σημείο όψης μηχανικού ή υπολογιστικής όψης**	**Αποδοχή ως σημείο συμμόρφωσης**
Προγραμματιστικά	ΟΠΠ00	Ανάμεσα στην υπηρεσία έκδοσης εγγράφων πιστοποίησης το αντικείμενο πληροφορίας η-έγγραφο πιστοποίησης μητρώου διαμονής (ResidenceCertificationDocument).	Η δομή του εγγράφου συμμορφώνεται στο σχήμα που έχει οριστεί.	ΟΜΠ07	Ναι
	ΟΠΠ01	Ανάμεσα στην υπηρεσία έκδοσης εγγράφων πιστοποίησης το αντικείμενο πληροφορίας (Request).	Η δομή του εγγράφου συμμορφώνεται στο σχήμα που έχει οριστεί.	ΟΜΠ07	Ναι
	ΟΠΠ02	Ανάμεσα στην υπηρεσία έκδοσης εγγράφων πιστοποίησης το αντικείμενο πληροφορίας έγγραφο αρνητικής απάντησης (NegativeResponseCertificationDocument).	Η δομή του εγγράφου συμμορφώνεται στο σχήμα που έχει οριστεί.	ΟΜΠ07	Ναι
	ΟΠΠ03	Ανάμεσα στην υπηρεσία έκδοσης εγγράφων πιστοποίησης το αντικείμενο πληροφορίας μετάφραση (Translation).	Η δομή του εγγράφου συμμορφώνεται στο σχήμα που έχει οριστεί.	ΟΜΠ07	Ναι
Διαλειτουργικά	ΟΠΔ00	Ανάμεσα σε δύο υπηρεσίες έκδοσης εγγράφων πιστοποίησης.	Οι δύο υπηρεσίες μπορούν να επεξεργαστούν επιτυχώς όλα τα η-έγγραφα που ανταλλάσσουν.	ΟΜΠ11	Ναι

Πίνακας 5-7: Σημεία συμμόρφωσης της Όψης Μηχανικού

5.3.3.8.4 Σημεία συμμόρφωσης επιχειρησιακής όψης

Ο παρακάτω πίνακας αναλύει τα σημεία αναφοράς της επιχειρησιακής όψης και δηλώνει ποια απο αυτά καταγράφονται ως σημεία συμμόρφωσης.

Κατηγορία σημείου	**Αναγνωριστικό σημείου**	**Περιγραφή σημείου**	**Περιγραφή επιθυμητής λειτουργικότητας**	**Αντίστοιχο σημείο όψης μηχανικού ή υπολογιστικής όψης ή όψης πληροφορίας**	**Αποδοχή ως σημείο συμμόρφωσης**
Προγραμματιστικά	ΕΟΠ00	Ανάμεσα στην διεργασία ResidenceCertificationBPELP	Τα ακόλουθα έγγραφα που διακινούνται στο σύστημα	ΟΠΠ01, ΟΠΠ02, ΟΠΠ03, ΟΠΠ04	Ναι

		rocess και τον μηχανισμό προηγμένων ηλεκτρονικών υπογραφών.	πρέπει πάντα να φέρουν προηγμένη ηλεκτρονική υπογραφή: οι αιτήσεις, τα έγγραφα πιστοποίησης θετικής και αρνητικής απάντησης και οι μεταφράσεις.		
	ΕΟΠ01	Ανάμεσα στο αντικείμενο ResidenceCertificationBPELP rocess και τον πυρήνα της αρχιτεκτονικής.	Δικαίωμα δημιουργίας και υπογραφής αίτησης εγγράφου πιστοποίησης έχουν οι πολίτες, οι εκπρόσωποι πολιτών και οι δημόσιοι υπάλληλοι.	ΟΜΠ05	Ναι
	ΕΟΠ02	Ανάμεσα στο αντικείμενο ResidenceCertificationBPELP Rocess και το AdaptationLayerSubprocess.	Τα έγγραφα πιστοποίησης θετικής και αρνητικής απάντησης και οι μεταφράσεις δημιουργούνται αυτόματα απο το σύστημα κάθε δήμου σύμφωνα με δεδομένα που είναι αποθηκευμένα στις υπάρχουσες βάσεις δεδομένων.	ΟΜΠ07	Ναι
	ΕΟΠ03	Ανάμεσα στο αντικείμενο ResidenceCertificationBPELP rocess και τον πυρήνα της αρχιτεκτονικής.	Δικαίωμα ελέγχου, προσθήκης σχολίων και υπογραφής στα έγγραφα πιστοποίησης θετικής και αρνητικής απάντησης και στις μεταφράσεις έχουν μόνο οι δημόσιοι υπάλληλοι των εμπλεκομένων δήμων.	ΟΜΠ05	Ναι
	ΕΟΠ04	Ανάμεσα στο αντικείμενο ResidenceCertificationBPELP rocess και τον πυρήνα της αρχιτεκτονικής.	Όλοι οι χρήστες του συστήματος πρέπει να κατέχουν έξυπνη κάρτα με τα διαπιστευτήρια κάθε χρήστη και κλειδιά για τις ηλεκτρονικές υπογραφές.	ΟΜΠ05	Ναι
	ΕΟΠ05	Ανάμεσα στο αντικείμενο ResidenceCertificationBPELP rocess και το αντικείμενο αίτηση.	Τα ελάχιστα απαραίτητα στοιχεία που πρέπει να συμπληρωθούν σε μια αίτηση είναι το ονοματεπώνυμο του προσώπου για το οποίο θα εκδοθεί το έγγραφο πιστοποίησης, η ημερομηνία γέννησής του, ο τρόπος με τον οποίο ο αιτών θέλει να λαμβάνει ειδοποιήσεις και η αντίστοιχη διεύθυνση ή τηλέφωνο για τις ειδοποιήσεις, ο δήμος έκδοσης του εγγράφου και ο δήμος λήψης του.	ΟΠΠ01	Ναι
	ΕΟΠ06	Ανάμεσα στο αντικείμενο	Ο δήμος που θα εκδώσει ένα	ΟΜΠ07, ΟΜΠ11	Ναι

		ResidenceCertificationBPELProcess και τις υπο-διεργασίες διαχείρισης υπαρχουσών υποδομών και προώθησης.	έγγραφο πιστοποίησης πρέπει πάντα να ταυτίζεται με τον δήμο έκδοσης που έχει δηλωθεί στην αίτηση.		
	ΕΟΠ07	Ανάμεσα στο αντικείμενο ResidenceCertificationBPELProcess και τις υπο-διεργασίες προώθησης και μετασχηματισμού μηνυμάτων.	Ο δήμος που θα μεταφράσει ένα έγγραφο πιστοποίησης (αρνητικής ή θετικής απάντησης) πρέπει πάντα να ταυτίζεται με τον δήμο λήψης που έχει δηλωθεί στην αίτηση.	ΟΜΠ10, ΟΜΠ11	Ναι
	ΕΟΠ08	Ανάμεσα στο αντικείμενο ResidenceCertificationBPELProcess και την υπο-διεργασία διαχείρισης υπαρχουσών υποδομών.	Εάν τα στοιχεία του πολίτη που περιέχονται στην αίτηση δεν υπάρχουν στο σύστημα του καθορισμένου δήμου έκδοσης, τότε πάντα εκδίδεται ένα έγγραφο πιστοποίησης αρνητικής απάντησης.	ΟΜΠ07	Ναι
	ΕΟΠ09	Ανάμεσα στο αντικείμενο ResidenceCertificationBPELProcess και την υπο-διεργασία ειδοποιήσεων.	Όταν οποιοδήποτε έγγραφο που παράγει η υπηρεσία είναι έτοιμο για λήψη, τότε πρέπει πάντα να ειδοποιείται ο αντίστοιχος πολίτης με μια διευκρινιστική ειδοποίηση.	ΟΜΠ08	Ναι
	ΕΟΠ10	Ανάμεσα στο αντικείμενο ResidenceCertificationBPELProcess και την υπο-διεργασία διαχείρισης αποθετηρίων.	Τα έγγραφα θα παραμένουν στο σύστημα για ένα δεδομένο αριθμό ημερών, στην προκειμένη περίπτωση 10 ημέρες. Μετά το πέρας του χρονικού αυτού διαστήματος διαγράφονται.	ΟΜΠ09	Ναι
Αντιληπτικά	ΕΟΑ00	Ανάμεσα στο αντικείμενο ResidenceCertificationBPELProcess και τους χρήστες.	Όλοι οι χρήστες πρέπει να υπόκεινται σε διαδικασίες αυθεντικοποίησης και ελέγχου πρόσβασης βάσει των διαπιστευτηρίων τους.	ΟΜΠ05	Ναι
	ΕΟΑ01	Ανάμεσα στο αντικείμενο ResidenceCertificationBPELProcess και τους χρήστες.	Ένας δημόσιος υπάλληλος πρέπει πάντα να ελέγχει κάθε αίτηση, έγγραφο πιστοποίησης και μετάφραση που λαμβάνει το σύστημα ή παράγει. Έχει δικαίωμα να αποδεχτεί ή να απορρίψει κάθε έγγραφο. Στην περίπτωση απόρριψης, πρέπει να δώσει διευκρινίσεις κατάλληλο χώρο πληροφορίας εντός του εγγράφου πιστοποίησης αρνητικής απάντησης που δημιουργείται.	ΟΜΠ05, ΟΠΠ02	Ναι
Διαλειτουργικά	ΕΟΔ00	Ανάμεσα σε δύο αντικείμενα ResidenceCertificationBPELP	Όταν ένα έγγραφο προωθείται απο έναν δήμο σε έναν άλλο,	ΟΜΠ10, ΟΠΠ00, ΟΠΠ01, ΟΠΠ02,	Ναι

		rocess	τότε μετατρέπεται σε μια μορφή κοινή σε όλες τις σχετικές υπηρεσίες η οποία αποστέλλεται μαζί με την αρχική (υπογεγραμμένη) μορφή του εγγράφου. Η υπηρεσία που την λαμβάνει την μετατρέπει αυτόματα στην τοπική μορφή του δήμου.	ΟΠΠ03, ΟΜΠ11, ΟΜΔ00	

Πίνακας 5-8: Σημεία συμμόρφωσης της Όψης Μηχανικού

Μετά την ολοκλήρωση της υλοποίησης, ο σχεδιασμός επιβάλλει τον έλεγχο όλων των σημείων που έχουν χαρακτηριστεί ως σημεία συμμόρφωσης στους παραπάνω πίνακες.

5.4 Συμπεράσματα

Στο παρόν κεφάλαιο της διατριβής παρουσιάστηκαν αναλυτικά οι προδιαγραφές επιχειρησιακών υπηρεσιών οι οποίες παρήχθησαν με πιστή εφαρμογή της κατασκευαστικής μεθόδου του κεφαλαίου 4. Οι υπηρεσίες αυτές επιτελούν σημαντικούς επιχειρησιακούς στόχους όπως διαφαίνεται απο την βιβλιογραφία και τις τρέχουσες ερευνητικές και επιχειρηματικές δραστηριότητες για τους οργανισμούς που τις υιοθετούν, τόσο στον τομέα του η-επιχειρείν, όσο και της η-διακυβέρνησης.
Οι προδιαγραφές των υπηρεσιών συμμορφώνονται με το πρότυπο RM-ODP και εμπεριέχουν το απαραίτητο πλαίσιο βελτίωσης και ελέγχου τους προκειμένου να μπορούν να αναβαθμιστούν αν απαιτηθεί μελλοντικά.
Ο σχεδιασμός και η υλοποίηση της υπηρεσίας η-τιμολόγησης οδήγησε στην αναγνώριση των παρακάτω θεμάτων:

- Η περίοδος ισχύος των προηγμένων ηλεκτρονικών υπογραφών εξασφαλίζει ότι μια υπογραφή μπορεί να ελεγχθεί βάση μιας χρονοσφραγίδας αρχείου (βλ. και την περιγραφή του προτύπου στο παράρτημα). Η χρονοσφραγίδα αρχείου ενδέχεται να δημιουργήσει προβλήματα απόδοσης όταν χρησιμοποιείται συχνά ως μέρος ενός ηλεκτρονικού αποθετηρίου με μεγάλο όγκο δεδομένων (όπως αυτός της συγκεκριμένης υπηρεσίας) [Bradner02]. Χρειάζονται επομένως μέτρα προκειμένου να επιταχυνθεί η διαδικασία ανανέωσης προηγμένων ηλεκτρονικών υπογραφών και η λήψη και ενσωμάτωση χρονοσφραγίδων.
- Δεν υπάρχει μέχρι αυτή τη στιγμή ένα πρωτόκολλο χρονοσφράγισης που χρησιμοποιεί αμιγώς δεδομένα XML [Apvrille02, Wouters 02] και γι' αυτό το λόγο σε κάθε υλοποίηση υπάρχει η ανάγκη για επιπλέον μετασχηματισμούς απο και σε μορφή Base64.
- Ένα σημαντικό θέμα για τη συγκεκριμένη υπηρεσία είναι να βρεθεί ο πλέον αποδοτικός τρόπος διαχείρισης διαφορετικών μορφών η-τιμολογίων, ώστε να είναι σεβαστές όλες οι πολιτικές ιδιωτικότητας, να χρησιμοποιείται ο ελάχιστος δυνατός αριθμός ψηφιακών υπογραφών και να επιτυγχάνεται η μεγαλύτερη δυνατή διαλειτουργικότητα με την υποστήριξη όσο των δυνατόν περισσότερων σχημάτων (προτυποποιημένων ή μη).

Η υπηρεσία έκδοσης εγγράφων πιστοποίησης μητρώου διαμονής έχει ήδη δοκιμαστεί σε συνεργασία με Ευρωπαϊκούς δήμους. Απο την αξιολόγηση που έχει γίνει, ανοιχτά μελλοντικά θέματα που διαφαίνονται είναι τα ακόλουθα:

- Υπάρχουν ανοιχτά ερωτήματα σχετικά με την κατανόηση απο τους τελικούς χρήστες της έννοιας της ψηφιακής ταυτότητας και επιχειρησιακούς κανόνες ή πολιτικές σχετικές με την διαχείριση λαθών, την ασφάλεια και την ιδιωτικότητα. Στις παραπάνω περιοχές οι εμπλεκόμενοι φορείς που υιοθετούν την επιχειρησιακή υπηρεσία αδυνατούν να δώσουν ξεκάθαρες απαιτήσεις για τον σχεδιασμό της επιχειρησιακής όψης και της όψης πληροφορίας. Αυτό μπορεί να οδηγήσει σε κρίσιμα «κενά γνώσης» κατά την εφαρμογή της μεθοδολογίας, συμπεριλαμβανομένου κενών σε νομικά θέματα.
- Αναγνωριστικά κενά ανάμεσα στην θεωρία (δηλαδή τις προδιαγραφές που προέκυψαν βάσει της μεθοδολογίας) και την πρακτική (δηλαδή το υλοποιημένο λογισμικό της υπηρεσίας) σχετικά με τα επίπεδα πελάτη και αλληλεπίδρασης. Το πρότυπο XForms αν και έχει σχεδιαστεί για να καλύπτει αυτό το κενό, αποδείχτηκε ιδιαίτερα πολύπλοκο και «βαρύ» και χρίζει περαιτέρω έρευνας.
- Ο σχεδιασμός της υπηρεσίας λαμβάνει υπόψην την ύπαρξη μιας κεντρικοποιημένης υπηρεσίας ελέγχου πρόσβασης και εφαρμογής πολιτικής. Η λύση αυτή αποδεικνύεται πραγματοποιήσιμη, αλλά δεν έγινε ξεκάθαρο εάν η χρήση της XACML στον τομέα αυτό είναι η πλέον κατάλληλη και αν μπορεί να καλύψει την πιο γενικευμένη προδιαγραφή πολιτικών των διαχειριστικών συναλλαγών [eMayorD4.1]. Επίσης ιδιαίτερο ενδιαφέρον παρουσιάζει η μελέτη του αντίκτυπου στην απόδοση, η οποία δεν πρέπει να αποτελεί τροχοπέδη για την κλιμάκωση της αρχιτεκτονικής. Πιο συγκεκριμένα, η απόδοση στην υλοποίηση επηρεάζεται απο τον υψηλό αριθμό των απομακρυσμένων κλήσεων μεθόδων εντός της αρχιτεκτονικής και απο τις διαφορές στην απόδοση μεταξύ κρίσιμων στοιχείων της αρχιτεκτονικής, και ειδικά των στοιχείων που σχετίζονται με τον συντονισμό των υπηρεσιών με το πρότυπο BPEL.

Παρ' όλα αυτά, οι υπηρεσίες καλύπτουν όλες τις προδιαγραφές που τίθενται απο τη σχετική νομοθεσία και τη λειτουργικότητα που απαιτείται. Σημαντικό είναι να αναφερθεί ότι οι προδιαγραφές δεν αντικατοπτρίζουν πιστή μεταφορά του επιχειρηματικού μοντέλου των αντίστοιχων υπηρεσιών που βασίζονται σήμερα στο χαρτί, αλλά το μοντέλου που αναπαριστούν έχει ρυθμιστεί, αναθεωρηθεί και βελτιωθεί ώστε να καλύπτει τις απαιτήσεις και ταυτόχρονα να εκμεταλλεύεται τις ιδιαιτερότητες, δυνατότητες και υπηρεσίες μιας ασφαλούς, διαλειτουργικής και ανοιχτής αρχιτεκτονικής υπηρεσιών.

5.5 Αναφορές

[Apvrille02] A. Apvrille, V.Girier. (2002). "XML Security Time Stamping Protocol", In Proceedings of Information Security Solutions Europe Conference (ISSE 2002), Paris, France.

[Arkin05] A. Arkin et al. (Editors). (2005). "Web Services Business Process Execution Language, version 2.0", OASIS standard, http://www.oasis-open.org/committees/download.php/16024/wsbpel-specification-draft-Dec-22-2005.htm

[BASDA] eBIS-XML Specifications, Business Application Software Developers Association (BASDA), basda.net/twiki/pub/Core/DownloadTheSuite/eBIS-XML-3.05.zip.
[Brandner02] R. Brandner, U. Pordesch. (2002). "Long-term conservation of provability of electronically signed documents", In Proceedings of the Information Security Solutions Europe Conference (ISSE 2002), Paris, France.
[CEN03] CEN/ISSS e-Invoicing Focus Group. (2003). "Report and Recommendations of CEN/ISSS e-Invoicing Focus Group on Standards and Developments on electronic invoicing", www.cenorm.be/isss/Projects/e-Invoicing.
[DOM] W3C Document Object Model – DOM, http://www.w3.org/DOM/
[EC01115] Council The European Parliament. (2001). Directive 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with view to simplifying, modernizing and harmonizing the conditions laid down for invoicing in respect of value added tax http://europa.eu.int/comm/taxation_customs/law_en.htm
[EC0145] The European Parliament. (2001). "Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data."
[EC0258] Council The European Parliament. (2002). Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) http://www.etsi.org/frameset/home.htm?/public-interest/EC_Directives.htm
[EC9546] Council The European Parliament. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
[EC969] Council The European Parliament. (1996). Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases http://europa.eu.int/ISPO/infosoc/legreg/docs/969ec.html
[EC9993] Council The European Parliament. (1999). Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures
[EID03] AS Sertifitseerimiskeskus, (2003). "The Esthonian ID Card and digital signature concepts: Principles and Solutions", white paper, www.id.ee/file.php?id=122
[eMayorD2.1] eMayor consortium. (2004). "Deliverable D2.1: Municipal Services – Analysis, Requirements and Usage scenarios", eMayor project, IST-2004-507217, http://www.emayor.org
[eMayorD3.1] eMayor consortium. (2004). "Deliverable D3.1: eMayor – System Design", eMayor project, IST-2004-507217, http://www.emayor.org
[eMayorD4.1] eMayor consortium. (2005). "Deliverable D4.1: eMayor development", eMayor project, IST-2004-507217, http://www.emayor.org
[FASME] The FASME Project ("Facilitating Administrative Services for Mobile Europeans"), www.fasme.org
[Govtalk] UK Office of the e-Envoy, UK GovTalk portal, www.govtalk.gov.uk
[Hartman03] B. Hartman et al. (2003). Mastering Web Services Security, Wiley Publishing.

[Hunter04] R. Hunter. (Editor). (2004). “e-Government Schema Guidelines for XML”, Office of the e-Envoy, v3.1, January 2004, http://www.govtalk.gov.uk/documents/schema-guidelines-3_1.pdf
[IDA04] IDA. (2004). ”IDA e-procurement XML schemas initiative - e-Ordering and e-Invoicing phases”, v 2.0, http://europa.eu.int/ida/servlets/Doc?id=18083
[jUDDI] Apache. jUDDI. http://ws.apache.org/juddi/
[Kaliontzoglou03] A. Kaliontzoglou et al. (2003). “Secure e-Invoicing Service based on Web Services”, In Proceedings of the 1st Hellenic Conference on Electronic Democracy, Athens, Greece.
[Kaliontzoglou05] A. Kaliontzoglou et al. (2005). “A secure e-Government platform architecture for small to medium sized public organizations”, Electronic Commerce Research & Applications, Elsevier, Volume 4, No. 2, pp. 174-186
[Kaliontzoglou06a] A. Kaliontzoglou, P. Boutsi, D. Polemi. (2006). “eInvoke: Secure e-Invoicing based on Web Services”, Electronic Commerce Research Journal, Springer, (Accepted for publication)
[Kaliontzoglou06b] A. Kaliontzoglou et al. (2006). “Secure electronic eInvoicing with the SELIS architecture: technical overview, market trends and deployment models”, Proceedings of 2nd Conference on Electronic Democracy, Athens, 2006
[Kaliontzoglou06c] A. Kaliontzoglou, T. Karantjias, D. Polemi. (2006). “Building innovative, secure and interoperable e-government services”, (To appear in) Secure e-Government Web Services, Idea Group Publishing, Hershey, PA
[Kaliontzoglou06d] A. Kaliontzoglou et al. (2006). “A formalized design method for building e-government architectures”, (To appear in) Secure e-Government Web Services, Idea Group Publishing, Hershey, PA
[Karantjias04] A. Karantjias et al. (2004). "Secure applications for the Chambers of Commerce: functionality and technical assessment", Proceedings of EUROSEC' 2004 15th Forum on Information Systems and Security, Paris
[Kavvadias02] G. Kavvadias, E. Spanos, E. Tambouris. (Editors). (2002). “Deliverable D2.3.1 GovML syntax and filters implementation”, the eGov project, IST-2000-28471, http://www.egov-project.org/egovsite/eGOV_D231.zip
[Kent03] A. Kent. (Editor). (2003). “Address and Personal Details Schema”, Office of the e-Envoy, v1.3, http://www.govtalk.gov.uk/documents/APD-v1-3.zip
[Klein04] B. Klein, S. Agne, A. Dengel. (2004). “Results of a Study on Invoice-Reading Systems in Germany”, Document Analysis Systems VI: 6th International Workshop, Florence, Italy,. Proceedings, Lecture Notes in Computer Science, Springer-Verlag GmbH, Volume 3163/2004, 451
[Meier02] W. Meier. (2002). “eXist: An Open Source Native XML Database”, In Lecture Notes In Computer Science, Revised Papers from the NODe 2002 Web and Database-Related Workshops on Web, Web-Services, and Database Systems, Springer-Verlag, 169-183
[Meneklis05a] B. Meneklis et al. (2005). “Applying the ISO RM-ODP standard in e-Government”, E-Government: Towards Electronic Democracy: International Conference, TCGOV 2005, Bolzano, Italy, Proceedings, Lecture Notes in Computer Science, Springer-Verlag GmbH, Volume 3416 / 2005, pp. 213

[Meneklis05b] B. Meneklis et al. (2005). “Engineering and Technology aspects of an e-government architecture based on Web Services”. Proceedings of 3rd IEEE European Conference on Web Services, Växjö, Sweden, pp. 118-129
[Meneklis06] B. Meneklis et al. (2006). “Issues and experiences in deploying secure and interoperable e-government transactions and services”, Proceedings of 2nd Conference on Electronic Democracy, Athens
[Nash01] A. Nash et al. (2001). PKI: Implementing & Managing E-Security, McGraw-Hill Osborn Media Publishing.
[OC4J] Oracle. (2006). “Oracle Application Server 10gR3, New Features Overview”. Oracle white paper, http://www.oracle.com/technology/tech/java/oc4j/1013/OracleAS-NF-1013.pdf
[Oikonomidis05] N. Oikonomidis et al. (2005). “Design Principles and Aspects for Cross-Border Municipal Services Deployment”, (To appear in) Proceedings of “EGOV05 – International Conference on E-Government”, Copenhagen, Denmark
[Rowell02] M. Rowell. (Editor). (2002). ”OAGIS - A “Canonical” Business Language”, Open Applications Group white paper, version 1.0, www.openapplications.org/downloads/whitepapers/whitepaperdocs/20020429_OAGIS_A_Canonical_Business_Langugage-PDF.zip.
[SAGA03]German Federal Ministry of Interior. (2003). “SAGA - Standards and Architectures for e-government Applications, version 2.0”.
[UBL1.0] OASIS, “Universal Business Language UBL 1.0”, ver. 1.0, Official OASIS Standard, http://docs.oasis-open.org/ubl/cd-UBL-1.0.zip
[Wouters02] K. Wouters et al. (2002). “Towards an XML Format for Time-Stamps”, In Proceedings of ACM Workshop on XML Security, ACM Press, Fairfax, Virginia, 61-70.
[XAdES02] ETSI Technical Specification. (2002). “ETSI TS 101 903 V1.1.1 - XML Advanced Electronic Signatures (XAdES)”.
[xCBL03] xCBL.org, (2003), XML Common Business Library version 4.00 (xCBL v4.00). www.xcbl.org/xcbl40/xcbl40.html.

6 Συμπεράσματα

Στην παρούσα διατριβή αρχικά μελετήθηκαν μεμονωμένα προβλήματα στην περιοχή της ενσωμάτωσης υπηρεσιών ασφάλειας βασισμένων σε Υ.Δ.Κ σε εφαρμογές XML και Υπηρεσιών Ιστού και προτάθηκαν λύσεις. Τα προβλήματα αυτά σε συνδυασμό με την μελέτη πλαισίων σχεδιασμού κατανεμημένων συστημάτων και ήδη υπαρχουσών αρχιτεκτονικών υπηρεσιών ηλεκτρονικών συναλλαγών, οδήγησαν στην αναγνώριση της έλλειψης ολιστικών συστηματικών μεθόδων σχεδιασμού αρχιτεκτονικών προσανατολισμένων στις υπηρεσίες.
Οι αρχές που διέπουν αυτόν τον τύπο αρχιτεκτονικών βρίσκονται ακόμη σε πολύ αρχικό στάδιο στην βιβλιογραφία και υπάρχει η ανάγκη για τον προσδιορισμό μιας καινοτόμου μεθοδολογίας σχεδιασμού συστημάτων που βασίζονται σε δομικά στοιχεία-υπηρεσίες και ταυτόχρονα δίνει έμφαση στο πολύ σημαντικό θέμα της ασφάλειας. Στο πλαίσιο αυτό, η παρούσα διατριβή όρισε την έννοια της Ασφαλούς, Διαλειτουργικής και ανοιχτής Αρχιτεκτονικής Υπηρεσιών και διατύπωσε μια κατασκευαστική μεθοδολογία που:

- Λαμβάνει υπόψην τις ιδιαιτερότητες των ΑΔΑΑΥ.
- Ικανοποιεί τις απαιτήσεις των ΑΔΑΑΥ, με έμφαση στην διαλειτουργικότητα και την ασφάλεια.
- Βασίζεται σε διεθνή ανοιχτά πρότυπα.

Η μεθοδολογία καλύπτει αδυναμίες και ανοιχτά προβλήματα στην περιοχή των πλαισίων σχεδιασμού αρχιτεκτονικών υπηρεσιών παρέχοντας ταυτόχρονα όλα τα ακόλουθα πλεονεκτήματα:

- Την αποφυγή χρήσης ad-hoc σχεδιασμού λύσεων δεμένων με την εκάστοτε υλοποίηση.
- Την παροχή υψηλού επιπέδου παραμετροποιησιμότητας με την εφαρμογή κατάλληλου υποσυνόλου των σταδίων της μεθοδολογίας.
- Την παροχή συγκεκριμένων και αναλυτικών βημάτων που πρέπει να ακολουθηθούν σε κάθε στάδιο με χρήση εκτενών παραδειγμάτων.
- Την συμμόρφωση με το RM-ODP και την UML.
- Την παροχή ενός συνόλου απο παραμετροποιήσιμα και επαναχρησιμοποιήσιμα κοινά αντικείμενα
- Την παροχή υψηλού επιπέδου ανεξαρτησίας απο τεχνολογίες.

Στη συνέχεια η διατριβή παρουσίασε δύο επιχειρησιακές υπηρεσίες που σχεδιάστηκαν με εφαρμογή της παραπάνω μεθοδολογίας. Οι επιχειρησιακές υπηρεσίες είναι μια υπηρεσία ηλεκτρονικής τιμολόγησης και μια υπηρεσία έκδοσης εγγράφων πιστοποίησης μητρώου διαμονής για δήμους λόγω του επιχειρηματικού ενδιαφέροντός τους, των αδυναμιών τέτοιου τύπου υπαρχουσών υπηρεσιών που υπάρχουν στην βιβλιογραφία, την βιομηχανία και στις εργασίες οργανισμών προτυποποίησης, καθώς και επειδή παρουσιάζουν σημαντικές απαιτήσεις ως προς την ασφάλεια και τη διαλειτουργικότητα λόγω του διασυνοριακού χαρακτήρα συναλλαγών που επιτρέπουν.

Μελλοντικές ερευνητικές δραστηριότητες και κατευθύνσεις που μπορούν να βασιστούν στην παρούσα διατριβή και προκύπτουν απο προβλήματα που συναντήθηκαν είναι οι ακόλουθες:

- Μια επέκταση της διατριβής θα μπορούσε να είναι η ενσωμάτωση μιας μεθοδολογίας βελτίωσης της απόδοσης σε υλοποιήσεις λόγω του αριθμού των απομακρυσμένων κλήσεων μεθόδων εντός της αρχιτεκτονικής και απο τις διαφορές στην απόδοση μεταξύ κρίσιμων στοιχείων της αρχιτεκτονικής.
- Η εμπειρία δείχνει ότι τα αποτελέσματα εφαρμογής μιας τέτοιας μεθοδολογίας βελτιώνονται εάν σε κατάλληλα σημεία υπεισέρχονται εσωτερική έλεγχοι (audits) των διαδικασιών και των προδιαγραφών απο ειδικούς στον σχεδιασμό συστημάτων πληροφορικής. Μια πρώτη εκτίμηση του πότε πρέπει να γίνουν οι έλεγχοι είναι στην αρχή της διαδικασίας, μετά το πέρας του σχεδιασμού της πρώτης έκδοσης του πυρήνα της αρχιτεκτονικής (στα πλαίσια της υπολογιστικής όψης), πριν την έναρξη της υλοποίησης και μετά τη λήξη της. Μένει να διερευνηθεί το αντίστοιχο μεθοδολογικό πλαίσιο και ο ακριβής χρονισμός τέτοιων ελέγχων καθώς και ο πλέον αποδοτικός τρόπος ενσωμάτωσής τους στην μεθοδολογία.
- Στην περίπτωση που σχεδιάζεται αρχικά μια γενικευμένη αρχιτεκτονική για έναν οργανισμό (generic reference architecture) είναι σημαντικό να αναδειχθεί ένας τρόπος υπολογισμού και εκτίμησης των πόρων που θα πρέπει να καλύψει ένας οργανισμός προκειμένου να συνδεθεί στην αρχιτεκτονική.
- Πέραν του πλαισίου ελέγχου συμμόρφωσης που περιλαμβάνει η μεθοδολογία στο τελευταίο στάδιο, είναι σημαντικό να προσδιοριστούν και να καθοριστούν συγκεκριμένες παράμετροι εξασφάλισης ποιότητας και το αντίστοιχο πλαίσιο διαχείρισης της ποιότητας ως προς τα αποτελέσματα εφαρμογής της μεθοδολογίας. Πολλές φορές συναντάται το φαινόμενο οι προδιαγραφές να είναι πολύ γενικές (ιδιαίτερα στην επιχειρησιακή όψη) και οι παράμετροι ποιότητας θα πρέπει να καθορίζουν και να θέτουν τα επίπεδα της «αυστηρότητας» του σχεδιασμού.

Στις μελλοντικές κατευθύνσεις επίσης περιλαμβάνονται όλες οι επιμέρους ερευνητικές δραστηριότητες που αναφέρονται στις παραγράφους των συμπερασμάτων των κεφαλαίων 4 και 5.

7 Παράρτημα Ι

7.1 Πρότυπα Κρυπτογραφίας και Υποδομών Δημοσίου Κλειδιού

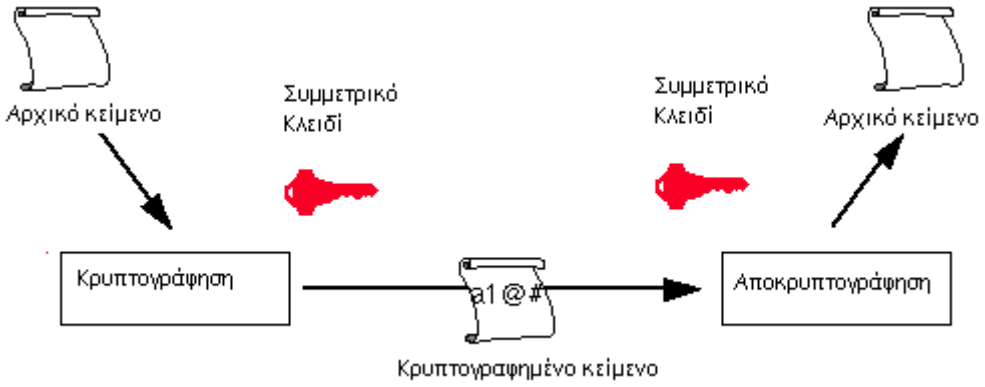
Στο παρόν κεφάλαιο αποτυπώνονται οι βασικές έννοιες των Υποδομών Δημοσίου Κλειδιού και τα πρότυπα που τις υποστηρίζουν.

7.1.1 Εισαγωγή στην κρυπτογραφία

Η *κρυπτογραφία* μπορεί να χρησιμοποιηθεί προκειμένου μηνύματα που κινούνται πάνω απο ανοιχτά δίκτυα να προστατευθούν απο υποκλοπή. Αυτό σημαίνει ότι ένα κρυπτογραφημένο μήνυμα αποτρέπει οποιονδήποτε να διαβάσει το μήνυμα καθώς αυτό περνάει απο τους διάφορους κόμβους του δικτύου μέχρι να φτάσει στον παραλήπτη του. Η κρυπτογραφία επίσης μπορεί να εξασφαλίσει την ακεραιότητα του μηνύματος, δηλαδή μπορεί να αποτρέψει κάποιον απο το να μεταβάλλει, διαγράψει ή εισάγει bits στα δεδομένα ενός μηνύματος χωρίς αυτό να γίνει αντιληπτό απο τον παραλήπτη. Τα *κρυπτογραφικά κλειδιά* είναι επί της ουσίας μεγάλοι τυχαίοι αριθμοί που ελέγχουν την διαδικασία της κρυπτογράφησης.

7.1.1.1 Συμμετρική κρυπτογραφία

Στην παραδοσιακή κρυπτογραφία, το ίδιο κρυπτογραφικό κλειδί χρησιμοποιείται για να κρυπτογραφήσει και να αποκρυπτογραφήσει πληροφορία. Αυτό είναι πλέον γνωστό ως *μυστικό κλειδί (secret key)* και ο τύπος της κρυπτογραφία ως *συμμετρική κρυπτογραφία* επειδή δύο οντότητες που θέλουν να επικοινωνήσουν ασφαλώς, χρησιμοποιούν το ίδιο κλειδί για να την υλοποιήσουν. Ειδικότερα, οι οντότητες λαμβάνουν και οι δύο τα κλειδιά τους με χρήση ενός ασφαλούς μέσου (ίσως και εκτός δικτύου) και πρέπει να τα προστατεύσουν προκειμένου να εξασφαλίσουν ότι μόνο εξουσιοδοτημένες οντότητες μπορούν να χρησιμοποιήσουν την πληροφορία.



Σχήμα 7-1: Συμμετρική κρυπτογράφηση

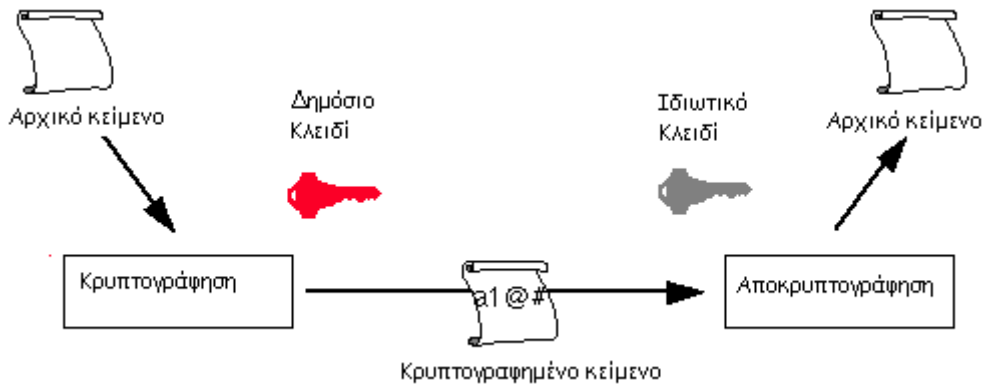
Η συμμετρική κρυπτογραφία διακρίνεται απο δύο προβλήματα:

α) όσο μεγαλώνει ο αριθμός των εμπλεκόμενων οντοτήτων, η διαχείριση των κλειδιών γίνεται όλο και πιο δύσκολη και
β) επειδή και οι δύο οντότητες χρησιμοποιούν το ίδιο κλειδί, δεν μπορεί κάποιος να αποδείξει απο που ξεκίνησε το κρυπτογραφημένο μήνυμα.

Συνηθισμένοι αλγόριθμοι συμμετρικής κρυπτογραφίας είναι ο Data Encryption Standard – DES (NIST 1988) [DES], ο Triple DES – 3DES [Barker04], ο Advanced Encryption Standard – AES (NIST 2001) [AES].

7.1.1.2 Κρυπτογραφία δημοσίου κλειδιού

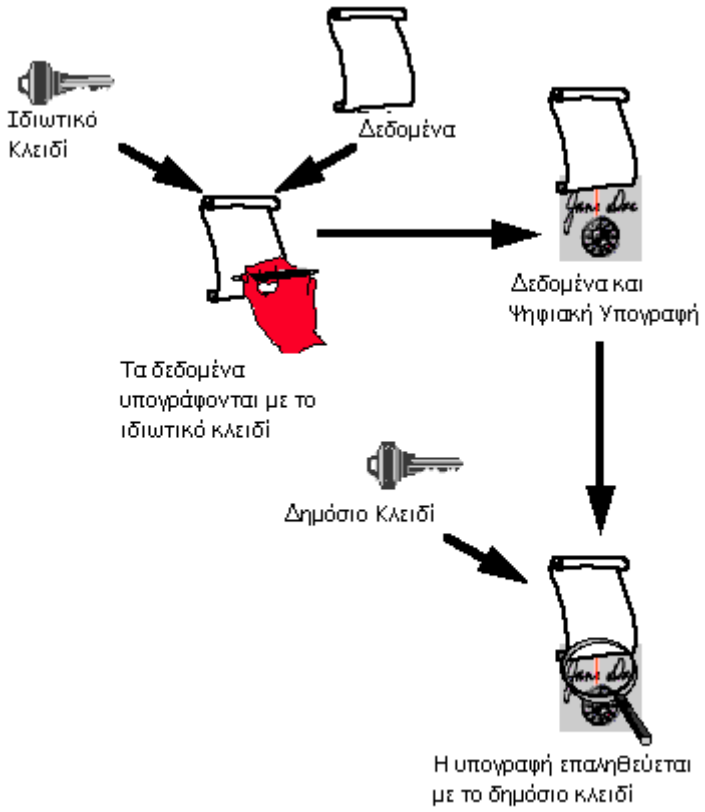
Μια διαφορετική προσέγγιση της κρυπτογραφίας ονομάζεται *κρυπτογραφία δημοσίου κλειδιού ή ασύμμετρη κρυπτογραφία*. Αυτή η μορφή, χρησιμοποιεί δύο διαφορετικά αλλά μαθηματικά συσχετιζόμενα κλειδιά. Το ένα μπορεί να χρησιμοποιηθεί χωρίς να μπορεί να αποκαλυφθεί το άλλο. Με την κρυπτογραφία δημοσίου κλειδιού, το *δημόσιο κλειδί* μπορεί, όπως λέει και το όνομά του, να δημοσιοποιηθεί σε οποιονδήποτε θέλει να κάνει μια συναλλαγή με την οντότητα που κρατάει το *ιδιωτικό κλειδί*. Η διανομή του δημοσίου κλειδιού είναι εύκολη, για παράδειγμα μέσω της δημοσίευσης σε κεντρικούς καταλόγους. Το ιδιωτικό κλειδί πρέπει να κρατηθεί κρυφό και να μπορεί να το χρησιμοποιήσει μόνο ο ιδιοκτήτης του. Ένας δημοφιλής αλγόριθμος κρυπτογραφίας δημοσίου κλειδιού είναι ο RSA, τον οποίον ανακάλυψαν ο R. Rivest, ο A. Shamir και ο L. Adleman [Kaliski98].
Στην κρυπτογραφία δημοσίου κλειδιού προκειμένου να κρυπτογραφηθούν κάποια δεδομένα, γίνεται χρήση του δημοσίου κλειδιού και το ιδιωτικό κλειδί χρησιμοποιείται μόνο για την αποκρυπτογράφησή τους. Οποιαδήποτε απο τις οντότητες που γνωρίζουν το δημόσιο κλειδί μπορεί να κρυπτογραφήσει δεδομένα με παραλήπτη τον ένα και μοναδικό κάτοχο του ιδιωτικού κλειδιού.



Σχήμα 7-2: Κρυπτογράφηση με κρυπτογραφία δημοσίου κλειδιού

Η κρυπτογραφία δημοσίου κλειδιού μπορεί επίσης να χρησιμοποιηθεί για τη δημιουργία μη παραποιούμενων *ψηφιακών υπογραφών* βασισμένων στο ιδιωτικό κλειδί κάποιου χρήστη. Το γεγονός ότι το ιδιωτικό κλειδί το έχει μόνο ο ιδιοκτήτης του, σημαίνει ότι το αποτέλεσμα οποιασδήποτε συνάρτησης χρησιμοποιεί το κλειδί αυτό, μπορεί να θεωρηθεί ότι έχει επιτελεστεί απο τον συγκεκριμένο ιδιοκτήτη και κανέναν άλλο. Μια ψηφιακή υπογραφή δημιουργείται απο την χρήση του ιδιωτικού κλειδιού προκειμένου να

«υπογραφούν» ηλεκτρονικά δεδομένα με τέτοιο τρόπο που να μην μπορεί να πλαστογραφηθεί.



Σχήμα 7-3: Παραγωγή ψηφιακών υπογραφών με κρυπτογραφία δημοσίου κλειδιού

Οι ψηφιακές υπογραφές είναι ισχυρότερες απο τις γραπτές διότι η υπογραφή είναι μαθηματικά δεμένη με τα υπογεγραμμένα δεδομένα. Η ψηφιακή υπογραφή δεν μπορεί να μεταφερθεί απο ένα κείμενο σε άλλο και οποιαδήποτε αλλαγή στα υπογεγραμμένα δεδομένα, ακυρώνει την υπογραφή. Η ψηφιακή υπογραφή δημιουργείται απο τα προς υπογραφή δεδομένα και το ιδιωτικό κλειδί και προστίθεται στο μήνυμα. Οποιοσδήποτε λαμβάνει το μήνυμα εκτελεί μια διαφορετική συνάρτηση που χρησιμοποιεί το δημόσιο κλειδί και την υπογραφή ή τα δεδομένα ως είσοδο, ανάλογα με τον αλγόριθμο. Εάν η εφαρμογή αυτής της συνάρτησης δίνει το αναμενόμενο αποτέλεσμα, η υπογραφή θεωρείται έγκυρη.

Οι ψηφιακές υπογραφές υλοποιούν έναν αριθμό υπηρεσιών ασφάλειας. Ειδικότερα, προσδίδουν έλεγχο αυθεντικότητας ή *αυθεντικοποίηση* σε ένα μήνυμα, εξασφαλίζοντας ότι αυτό έχει προέλθει απο έναν συγκεκριμένο χρήστη, ο οποίος είναι ο μοναδικός κάτοχος του ιδιωτικού κλειδιού. Η ψηφιακή υπογραφή προστατεύει το μήνυμα απο μη εξουσιοδοτημένη μεταποίηση προσδίνοντας έναν έλεγχο ακεραιότητας. Παρόλο που απο μόνη της η υπογραφή δεν είναι αρκετή για να επιτύχει την υπηρεσία *μη-άρνησης συμμετοχής (non-repudiation)*, μια ψηφιακή υπογραφή κατασκευασμένη σε συνδυασμό με κατάλληλα δεδομένα μπορεί να παρέχει ένα μέρος της υπηρεσίας μη-άρνησης.

Το αρνητικό χαρακτηριστικό της κρυπτογραφίας δημοσίου κλειδιού είναι το αυξημένο υπολογιστικό κόστος της. Ακόμη και με σύγχρονους υπολογιστές, θεωρείται αργή λόγω των πολύπλοκων υπολογισμών που περιλαμβάνει. Γι' αυτό το λόγο, στην πράξη, αλγόριθμοι κρυπτογραφίας δημοσίου κλειδιού χρησιμοποιούνται μόνο για την κρυπτογράφηση περιορισμένου μεγέθους πληροφορίας, όπως για παράδειγμα ένα κλειδί συμμετρικού αλγορίθμου όπως ο DES ή ο 3DES. Το δεύτερο αυτό κλειδί χρησιμοποιείται με έναν αλγόριθμο συμμετρικής κρυπτογραφίας ο οποίος αναλαμβάνει να κρυπτογραφήσει μεγαλύτερους όγκους δεδομένων με πιο αποδοτικό τρόπο.
Προκειμένου να λειτουργήσει σωστά η κρυπτογραφία δημοσίου κλειδιού, τα ιδιωτικά κλειδιά πρέπει να προστατεύονται. Έχουν βρεθεί διάφοροι τρόποι προκειμένου να υπάρχει αυξημένο επίπεδο προστασίας, ώστε ένας χρήστης να μπορεί να μεταφέρει ασφαλώς το ιδιωτικό κλειδί του. Οι *έξυπνες κάρτες* είναι ένας απ' αυτούς που θεωρούνται αποτελεσματικοί τρόποι. Οι τεχνολογίες για έξυπνες κάρτες και αναγνώστες έξυπνων καρτών για προσωπικούς υπολογιστές είναι ήδη διαθέσιμες και μέσα σε λογικά πλαίσια κόστους.

7.1.2 Βασικοί μηχανισμοί και διαδικασίες ασφάλειας

Η παράγραφος αυτή έχει ως στόχο την συνοπτική περιγραφή των βασικών μηχανισμών και διαδικασιών εκείνων που λαμβάνουν χώρα κατά την διεκπεραίωση κρυπτογραφικών λειτουργιών. Συνήθως η χρήση των μηχανισμών αυτών αποτελεί στοιχειώδες βήμα μιας συνολικότερης κρυπτογραφικής λειτουργίας. Οι μηχανισμοί που περιγράφονται εδώ είναι βασισμένοι σε ευρέως διαδεδομένα πρότυπα.

7.1.2.1 Συμφωνία κλειδιών

Με τον όρο συμφωνία κλειδιών εννοούμε την διαδικασία επίλυσης του ακόλουθου προβλήματος: δύο οντότητες θέλουν να συμφωνήσουν στην πληροφορία κρυπτογραφικών κλειδιών μυστικά πάνω απο ένα ανοιχτό κατανεμημένο δίκτυο. Προκειμένου να επιτευχθεί η ασφαλής συμφωνία χρησιμοποιούνται *πρωτόκολλα συμφωνίας κλειδιών (key agreement protocols)*. Ένα τέτοιο πρωτόκολλο χρησιμοποιεί την έννοια της *συνόδου (session)* η οποία αποτελεί μια σειρά αλληλεπιδράσεων μεταξύ δύο οντοτήτων που συμβαίνουν κατά τη διάρκεια μιας σύνδεσης με σκοπό την συμφωνία των κλειδιών. Τα θεμιτά χαρακτηριστικά τέτοιων πρωτοκόλλων είναι τα ακόλουθα:

- Γνωστά κλειδιά συνόδου: ένα πρωτόκολλο επιτυγχάνει το στόχο του παρά το γεγονός ότι κάποιος έχει υποκλέψει κάποια απο τα κλειδιά προηγούμενων συνόδων.
- *(Τέλεια) πρόσθια μυστικότητα (perfect forward secrecy)*: Εάν κάποιο απο τα κρυπτογραφικά μυστικά που χρησιμοποιούνται για μια ή περισσότερες οντότητες υποκλαπούν, η μυστικότητα προηγούμενων κλειδιών συνόδων δεν επηρεάζεται.
- Άγνωστο μοίρασμα κλειδιού: η οντότητα i δεν μπορεί να εξαναγκαστεί να μοιραστεί τον κλειδί της με την οντότητα j χωρίς η i να το γνωρίζει, για παράδειγμα όταν η i πιστεύει ότι το κλειδί το μοιράζεται με μια οντότητα l που είναι διαφορετική της j.
- Απομίμηση με υποκλοπή κλειδιού: Εάν υποθέσουμε ότι το κρυπτογραφικό μυστικό (αρχικά δεδομένα παραμέτρων) του i, που χρησιμοποιείται στην συμφωνία υποκλέπτεται, τότε ο υποκλοπέας που γνωρίζει την τιμή του μπορεί να υποδυθεί τον i, εφόσον αυτή η τιμή ακριβώς χαρακτηρίζει τον i. Ενδέχεται παρ' όλα αυτά, ότι αυτή

η απώλεια δεν επιτρέπει στον υποκλοπέα να υποδυθεί τον ρόλο άλλων οντοτήτων πέραν του i.

- Απώλεια πληροφορίας: Η υποκλοπή άλλης πληροφορίας που δεν θα ήταν υπο κανονικές συνθήκες διαθέσιμη στον υποκλοπέα, δεν επηρεάζει την ασφάλεια του πρωτοκόλλου.
- Ανεξαρτησία μηνυμάτων: Ανεξάρτητες ροές μηνυμάτων ενός πρωτοκόλλου συμφωνίας που έχουν εδραιωθεί ανάμεσα σε δύο έντιμες οντότητες είναι άσχετες μεταξύ τους (δηλαδή δεν τυχαίνει να υπάρχουν ίδιες ροές μηνυμάτων ανάμεσα σε διαφορετικές οντότητες).

Ένα απο τα πιο γνωστά πρωτόκολλα συμφωνία κλειδιών είναι αυτό των Diffie-Helman το οποίο περιγράφεται στο RFC 2631 (Diffie-Hellman Key Agreement Method) [DH].

7.1.2.2 Συναρτήσεις κατακερματισμού

Μια συνάρτηση *κατακερματισμού Η (hash function)* είναι ένας μετασχηματισμός που λαμβάνει μια είσοδο μεταβλητού μήκους m και επιστρέφει μια συμβολοακολουθία σταθερού μήκους, που ονομάζεται *τιμή της συνάρτησης* h, δηλαδή h = H(m). Οι συναρτήσεις κατακερματισμού με αυτή την ιδιότητα βρίσκουν εφαρμογή σε μια πληθώρα περιπτώσεων, αλλά όταν χρησιμοποιούνται στην κρυπτογραφία συνήθως επιλέγονται ώστε να διαθέτουν και επιπλέον ιδιότητες.
Οι βασικές απαιτήσεις απο μια κρυπτογραφική συνάρτηση κατακερματισμού είναι οι ακόλουθες:

- Η είσοδος να είναι οσοδήποτε μήκους.
- Η έξοδος να έχει σταθερό μέγεθος.
- Η H(x) να είναι εύκολο να υπολογιστεί για οποιοδήποτε δεδομένο x.
- Η H(x) είναι *μονόδρομη (one-way)*.
- Η H(x) είναι *ανθεκτική σε συγκρούσεις (collision-free)*.

Μια συνάρτηση κατακερματισμού Η είναι μονόδρομη όταν είναι δύσκολο να αντιστραφεί, όπου ο όρος «δύσκολο» σημαίνει ότι για μια δεδομένη τιμή της συνάρτηση h, είναι υπολογιστικά αδύνατο να βρεθεί κάποια είσοδος x έτσι ώστε H(x)=h.
Εάν για **ένα** συγκεκριμένο μήνυμα x, είναι υπολογιστικά αδύνατο να βρεθεί ένα μήνυμα y το οποίο είναι διαφορετικό απο το x έτσι ώστε H(x) = H(y), τότε η Η χαρακτηρίζεται ως μια συνάρτηση κατακερματισμού *ασθενώς ανθεκτική στις συγκρούσεις (weakly collision-free)*.
Μια *ισχυρά ανθεκτική στις συγκρούσεις (strongly collision-free)* συνάρτηση κατακερματισμού Η χαρακτηρίζεται αυτή για την οποία είναι υπολογιστικά αδύνατο να βρεθούν **οποιαδήποτε** δύο μηνύματα x και y για τα οποία H(x)=H(y).
Η τιμή της συνάρτησης κατακερματισμού (η οποία αναφέρεται στην βιβλιογραφία και ως hash ή message digest) αναπαριστά με συνέπεια το μήνυμα ή έγγραφο απο το οποίο υπολογίστηκε. Κάποιος θα μπορούσε να θεωρήσει την τιμή αυτή ως ένα «ψηφιακό δακτυλικό αποτύπωμα» του εγγράφου. Παραδείγματα των πλέον διαδεδομένων συναρτήσεων κατακερματισμού είναι οι MD2 [Kaliski92], MD5 [Rivest92] και SHA1 [Eastlake01].

Ο κύριος ρόλος των κρυπτογραφικών συναρτήσεων κατακερματισμού είναι στην δημιουργία ψηφιακών υπογραφών όπως περιγράφηκαν στην παράγραφο 7.1.1.2. Επιπλέον η τιμή μιας συνάρτησης μπορεί να δημοσιευθεί χωρίς να αποκαλύπτονται τα περιεχόμενα του εγγράφου απο το οποίο προκύπτει. Αυτό βρίσκει εφαρμογή στην *ψηφιακή χρονοσφράγιση (digital timestamping)*, όπου χρησιμοποιώντας συναρτήσεις κατακερματισμού, κάποιος μπορεί να λάβει ένα χρονοσφραγισμένο έγγραφο χωρίς να αποκαλύπτει τα περιεχόμενα του εγγράφου στην υπηρεσία χρονοσφράγισης.

7.1.2.3 Αλγόριθμοι κρυπτογράφησης βασισμένοι Σε Τμήματα

Οι *αλγόριθμοι κρυπτογράφησης βασισμένοι σε τμήματα (block ciphers)* είναι ένας τύπος αλγόριθμου συμμετρικής κρυπτογράφησης που μετατρέπει ένα block *μη κρυπτογραφημένου κειμένου (plaintext)* καθορισμένου μήκους, σε block *κρυπτογραφημένου κειμένου (ciphertext)* του ίδιου μήκους. Αυτός ο μετασχηματισμός πραγματοποιείται με την βοήθεια ενός μυστικού κλειδιού που χορηγείται από τον χρήστη. Η αποκρυπτογράφηση γίνεται με την εφαρμογή του αντίστροφου μετασχηματισμού στο κρυπτογραφημένο κείμενο χρησιμοποιώντας το ίδιο μυστικό κλειδί. Το καθορισμένο μήκος καλείται *μέγεθος τμήματος (block size)*.
Οι block ciphers λειτουργούν επαναληπτικά, κρυπτογραφώντας ένα block διαδοχικά αρκετές φορές. Σε κάθε γύρο, ο ίδιος μετασχηματισμός εφαρμόζεται στα δεδομένα χρησιμοποιώντας ένα υπο-κλειδί. Το σύνολο των υπο-κλειδιών προέρχεται από το μυστικό κλειδί που χορήγησε ο χρήστης, με ειδική συνάρτηση. Το σύνολο των υπο-κλειδιών καλείται πρόγραμμα κλειδιών.
Ο αριθμός των επαναλήψεων του block cipher εξαρτάται από το επίπεδο της επιθυμητής ασφάλειας και την απόδοση του συστήματος. Στις περισσότερες περιπτώσεις, ο αυξημένος αριθμός επαναλήψεων βελτιώνει την προσφερόμενη ασφάλεια, αλλά για μερικούς αλγορίθμους ο αριθμός των επαναλήψεων πρέπει να είναι πολύ μεγάλος ώστε να επιτευχθεί ικανοποιητική ασφάλεια.
Οι Feistel ciphers [Feistel88] είναι ειδικές περιπτώσεις block ciphers όπου το κρυπτογραφημένο κείμενο υπολογίζεται ως εξής: το κείμενο χωρίζεται στο μισό. Η συνάρτηση f εφαρμόζεται στο ένα μισό με χρήση ενός υπο-κλειδιού και η έξοδος της f περνάει από λογική πράξη X-OR με το άλλο μισό. Έπειτα, το αποτέλεσμα της λογικής πράξης γίνεται είσοδος της f και το προηγούμενο μισό το οποίο μετασχηματίστηκε γίνεται μία από τις εισόδους της επόμενης X-OR. Η άλλη είσοδος της X-OR είναι το αποτέλεσμα του δεύτερου μετασχηματισμού, ο οποίος χρησιμοποιεί νέο υπο-κλειδί. Ο αλγόριθμος συνεχίζεται με το ίδιο τρόπο. Στο τέλος της τελευταίας επανάληψης, τα δύο κρυπτογραφημένα μισά συνενώνονται.
Ένα σημαντικό χαρακτηριστικό του Feistel είναι ότι η αποκρυπτογράφηση είναι δομικά ταυτόσημη με την κρυπτογράφηση. Τα υπο-κλειδιά χρησιμοποιούνται σε αντίστροφη σειρά στην αποκρυπτογράφηση. Οι Feistel ciphers καλούνται και DES-like ciphers.

7.1.2.4 Αλγόριθμοι κρυπτογράφησης βασισμένοι σε Ροές

Ένας *αλγόριθμος κρυπτογράφησης βασισμένος σε ροές (Stream cipher)* είναι ένας τύπος αλγόριθμου συμμετρικής κρυπτογράφησης με εξαιρετική ταχύτητα (πολύ ταχύτεροι από τους block ciphers). Σε αντίθεση με τους block ciphers που λειτουργούν με μεγάλα κομμάτια δεδομένων (blocks), οι stream ciphers τυπικά λειτουργούν με μικρότερες μονάδες απλού κειμένου, συνήθως με bits. Η κρυπτογράφηση ενός συγκεκριμένου

κειμένου με έναν block cipher θα καταλήγει πάντα στο ίδιο αποτέλεσμα όταν χρησιμοποιείται το ίδιο κλειδί. Με έναν stream cipher, ο μετασχηματισμός των μικρότερων αυτών μονάδων θα ποικίλει, ανάλογα με πως υπόκεινται επεξεργασία κατά την διάρκεια της κρυπτογράφησης.

Ένας stream cipher παράγει μια ακολουθία από bits που χρησιμοποιείται σαν κλειδί και καλείται *ροή-κλειδί (keystream)*. Η κρυπτογράφηση επιτυγχάνεται με τον συνδυασμό του keystream με το plaintext, συνήθως μέσω μιας πράξης X-OR. Η παραγωγή του keystream μπορεί να είναι ανεξάρτητη του plaintext και του ciphertext (*οπότε μιλάμε για σύγχρονο αλγόριθμο – synchronous stream cipher*) ή μπορεί να εξαρτάται από αυτά (οπότε μιλάμε για *αυτοσυγχρονιζόμενο αλγόριθμο - self-synchronizing stream cipher*). Οι περισσότεροι stream ciphers είναι σύγχρονοι.

Οι stream ciphers βασίζονται στις θεωρητικές ιδιότητες ενός *one-time pad*. One-time pads (καμιά φορά καλούνται και Vernam ciphers [Vernam]) είναι αλγόριθμοι που χρησιμοποιούν ως κλειδί μια ακολουθία bits (keystream) που παράγεται τελείως στην τύχη. Το keystream είναι του ίδιου μήκους με το μη κρυπτογραφημένο κείμενο (plaintext) και συνδυάζεται μέσω μιας X-OR πράξης με αυτό για την παραγωγή του κρυπτογραφημένου κειμένου (ciphertext). Επειδή το keystream είναι τελείως τυχαίο και είναι του ίδιου μήκους με το plaintext, η εύρεση του αρχικού κειμένου είναι αδύνατη ακόμα και με την διάθεση τεράστιας υπολογιστικής ισχύος. Ένας τέτοιος αλγόριθμος προσφέρει τέλεια μυστικότητα και ασφάλεια και έχει χρησιμοποιηθεί σε μεγάλη κλίμακα σε καιρό πολέμου για την διασφάλιση διπλωματικών καναλιών. Το γεγονός, όμως, ότι το μυστικό κλειδί (δηλαδή το keystream), που χρησιμοποιείται μόνο μία φορά, είναι του ίδιου μήκους με του μήνυμα, εισάγει σημαντικό πρόβλημα στην διαχείριση του κλειδιού. Παρ' όλη την ασφάλεια που προσφέρει, ο one-time pad δεν μπορεί να εφαρμοστεί στην πράξη.

Οι stream ciphers αναπτύχθηκαν σαν μια προσέγγιση της λειτουργίας ενός one-time pad. Αν και δεν είναι σε θέση να παρέχουν την θεωρητική ασφάλεια ενός time-pad, είναι αρκετά πρακτικοί. Ο πιο ευρέως χρησιμοποιούμενος stream cipher είναι ο RC4 [Kelsey96]. Ενδιαφέρον παρουσιάζει το γεγονός ότι συγκεκριμένοι τρόποι λειτουργίας ενός block cipher προσομοιάζουν ένα stream cipher όπως για παράδειγμα ο DES σε CFB και OFB τρόπους λειτουργίας. Ακόμα και έτσι, οι αυθεντικοί stream ciphers είναι αρκετά ταχύτεροι.

Ένας μηχανισμός για την παραγωγή του keystream είναι ο *Καταχωρητής Γραμμικής Ολίσθησης με Ανάδραση (Linear Feedback Shift Register – LFSR)*. Ο καταχωρητής αποτελείται από μία σειρά κελιών (cells) το καθένα από τα οποία αποτελείται από ένα bit. Τα περιεχόμενα των κελιών καθορίζονται από ένα *Διάνυσμα Αρχικοποίησης (Initialization Vector)* που λειτουργεί σαν το μυστικό κλειδί. Το keystream δεν αποτελεί πλέον το μυστικό κλειδί (όπως στους one-time pads) λόγω του μεγέθους του. Η συμπεριφορά του καταχωρητή ρυθμίζεται από ένα ρολόι και σε κάθε χρονική στιγμή τα bits μετακινούνται μία θέση δεξιά, την στιγμή που το X-OR αποτέλεσμα μερικών από αυτών τοποθετείται στο αριστερότερο κελί. Κάθε αλλαγή του ρολογιού δίνει ένα bit εξόδου.

Η κατασκευή των LFSR είναι εύκολη τόσο υπό μορφή λογισμικού όσο και υπό μορφή υλικού, ενώ η λειτουργία τους είναι ταχύτατη. Οι ακολουθίες bit, όμως, που δημιουργούνται από ένα και μοναδικό LFSR δεν είναι ασφαλείς καθ' ότι τον τελευταίο καιρό έχει αναπτυχθεί μια δυνατή μαθηματική φόρμουλα που επιτρέπει την ανάλυση του

μηχανισμού και εύρεση του keystream. Απαιτείται, λοιπόν, η συνδυασμένη χρήση πολλών LFSRs.
Ένας συνδυασμός LFSRs είναι ο Shift Register Cascade που αποτελείται από ένα σύνολο από LFSRs που συνδέονται μεταξύ τους με τέτοιο τρόπο ώστε η συμπεριφορά του ενός να εξαρτάται από την συμπεριφορά του άλλου. Αυτό επιτυγχάνεται συνήθως με την χρήση του ενός LFSR έτσι ώστε να ελέγχει το ρολόι του άλλου. Άλλο παράδειγμα τέτοιου συνδυασμού είναι ο *Shrinking Generator* [Coppersmith93] που αναπτύχθηκε από τους Coppersmith, Krawczyk και Mansur που βασίζεται στην αλληλεπίδραση των εξόδων δύο LFSRs. Ειδικότερα, τα bits της μιας εξόδου χρησιμοποιούνται για να καθορίσουν, μέσω κατάλληλης τεχνικής, εάν τα bits της δεύτερης εξόδου θα συμπεριληφθούν στο keystream. Ο Shrinking Generator χαρακτηρίζεται για την απλότητα ασφάλεια που προσφέρει.

7.1.2.5 Κώδικες Αυθεντικοποίησης μηνυμάτων

Ένας *Κώδικας Αυθεντικοποίησης Μηνύματος ΚΑΜ (Message Authentication Code – MAC)* είναι μια ετικέτα αυθεντικοποίησης (ή αλλιώς άθροισμα ελέγχου) που παράγεται απο την εφαρμογή σε ένα μήνυμα μιας διαδικασίας αυθεντικοποίησης, μαζί με ένα μυστικό κλειδί. Οι ΚΑΜ υπολογίζονται και επαληθεύονται με το ίδιο κλειδί, οπότε μπορούν να επαληθευτούν μόνο απο τον παραλήπτη που το έχει, σε αντίθεση με τις ψηφιακές υπογραφές που μπορούν να επαληθευτούν απο οποιονδήποτε. Οι ΚΑΜ μπορούν να κατηγοριοποιηθούν ως:

- Ασφαλείς χωρίς συνθήκες
- Βασισμένοι σε συναρτήσεις κατακερματισμού
- Βασισμένοι σε αλγορίθμους ροής (stream ciphers)
- Βασισμένοι σε αλγορίθμους τμημάτων (block ciphers)

Οι Simmons και Stinson πρότειναν έναν ασφαλή χωρίς συνθήκες ΚΑΜ που βασίζεται σε κρυπτογράφηση με χρήση ενός one-time pad. Το κρυπτογραφημένο κείμενο του μηνύματος αυθεντικοποιεί τον εαυτό του εφόσον κανένας άλλος δεν έχει πρόσβαση στο one-time pad. Παρ' όλα αυτά, θα πρέπει να υπάρχει πλεονασμός πληροφορίας στο μήνυμα. Ένας ασφαλής ΚΑΜ χωρίς συνθήκες μπορεί να ληφθεί επίσης με την χρήση ενός μυστικού κλειδιού μιας χρήσης (one-time secret key).
Οι ΚΑΜ βασισμένοι σε συναρτήσεις κατακερματισμού χρησιμοποιούν ένα ή περισσότερα κλειδιά σε συνδυασμό με μια συνάρτηση κατακερματισμού για να παράγουν ένα άθροισμα ελέγχου που προστίθεται στο μήνυμα. Ένα παράδειγμα είναι ο αλγόριθμος keyed-MD5 [Metzger95].
Οι Lai, Rueppel και Woolven πρότειναν έναν ΚΑΜ βασισμένο σε αλγόριθμους ροών [Lai92]. Στον αλγόριθμό τους, ένας αποδεδειγμένα ασφαλής stream cipher χρησιμοποιείται για να χωρίσει ένα μήνυμα σε δύο υπο-ροές, και κάθε υπο-ροή τροφοδοτείται σε ένα LFSR. Το άθροισμα ελέγχου είναι η τελική κατάσταση των δύο LFSR.
ΚΑΜ μπορούν να προκύψουν και με απο αλγορίθμους βασισμένους σε τμήματα (block ciphers). Ο DES-CBC είναι ευρέως διαδεδομένος. Η βασική ιδέα είναι ότι κρυπτογραφούνται τα τμήματα του μηνύματος με τον DEC_CBC και το τελικό τμήμα του cipthertext χρησιμοποιείται ως το άθροισμα ελέγχου.

7.1.2.6 Μετασχηματισμός base64

Ο *μετασχηματισμός base64 (base64 encoding)* αποτελεί ένα σχήμα κωδικοποίησης με το οποίο δυαδικά δεδομένα μετατρέπονται σε εκτυπώσιμους χαρακτήρες ASCII [ASCII]. Ο μετασχηματισμός αυτός έχει οριστεί ως η κωδικοποίηση που χρησιμοποιείται για την μεταφορά περιεχομένου MIME [Freed96] στο ηλεκτρονικό ταχυδρομείο. Οι μόνοι χαρακτήρες που χρησιμοποιούνται είναι οι κεφαλαίοι και μικροί χαρακτήρες του λατινικού αλφαβήτου, οι αριθμοί, τα σύμβολα «+» και «/», και το σύμβολο «=» ως σύμβολο ειδικής επέκτασης.
Οι πλήρεις προδιαγραφές του base64 περιέχονται στα RFC 1421 και 2045. Το σχήμα κωδικοποίησης καθορίζεται μόνο για δεδομένα που το αρχικό τους μήκος είναι πολλαπλάσιο των 8 bits, μια απαίτηση που καλύπτεται απο τα περισσότερα είδη αρχείων σε υπολογιστές. Τα κωδικοποιημένα σε base64 δεδομένα που προκύπτουν έχουν ένα μήκος που είναι περίπου 33% μεγαλύτερο απο τα αρχικά δεδομένα, και εμφανίζονται ως ένα σύνολο τυχαίων χαρακτήρων.
Για να μετατραπούν δεδομένα σε base64, αποθηκεύονται σε μια αποθήκη στοιχείων των 24-bits ανά τρία bytes. Τα πρώτα 8 bits της αποθήκης αντιστοιχούν στο πρώτο byte, τα μεσαία 8 στο δεύτερο και τα τελευταία 8 στο τρίτο. Εάν υπάρχουν λιγότερα απο τρία bytes για να κωδικοποιηθούν τότε τα αντίστοιχα bits στον αποθηκευτικό χώρο συμπληρώνονται με 0.
Στην συνέχεια λαμβάνονται απο τον αποθηκευτικό χώρο τα bits ανά έξι, αντιστοιχώντας σε έναν απο τους ακόλουθους χαρακτήρες:

ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/

Αυτό επαναλαμβάνεται με διαδοχικές τριάδες bytes μέχρι να τελειώσει το δυαδικό αρχείο. Εάν το μέγεθος των αρχικών δεδομένων είναι πολλαπλάσιο του τρία, η διαδικασία ολοκληρώνεται ομαλά. Εάν δεν είναι, κατά την τελευταία επανάληψη στην αποθήκη στοιχείων μπορεί να καταλήξουν ένα ή δύο bytes. Στην περίπτωση αυτή, καθώς για την κωδικοποίηση απαιτούνται τρία bytes, προστίθενται αρκετά bits με τιμή μηδέν, ώστε να δημιουργηθεί πάλι ομάδα των τριών bytes. Ειδικότερα, δύο τέτοια bytes μηδενικών προστίθενται αν έχουμε στο τέλος ένα byte αρχικών δεδομένων, ή ένα byte μηδενικών προστίθεται αν έχουμε δύο bytes αρχικών δεδομένων. Καθώς τα μηδενικά που προστίθενται δεν μπορούν να αναπαρασταθούν κωδικοποιώντας τα σε κάποιον απο τους παραπάνω ASCII χαρακτήρες, αναπαρίστανται με έναν 65^{o} χαρακτήρα, ο οποίος είναι ο «=». Ως λογική συνέπεια, ο χαρακτήρας αυτός μπορεί να εμφανιστεί μόνο στο τέλος των κωδικοποιημένων δεδομένων.

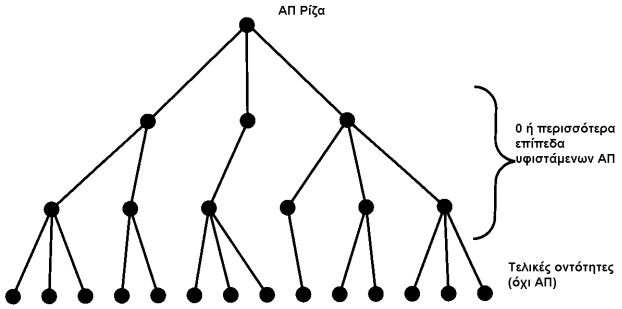
7.1.3 Ψηφιακά πιστοποιητικά – Αρχές Πιστοποίησης

Προκειμένου ένα σύστημα βασισμένο στην κρυπτογραφία δημοσίου κλειδιού να λειτουργήσει σωστά, θα πρέπει οι κάτοχοι δημόσιων κλειδιών να μπορούν να είναι σίγουροι ποιος είναι ο κάτοχος ενός τέτοιου κλειδιού και ότι το κλειδί αυτό είναι σωστό και δεν έχει αλλοιωθεί. Η ταυτοποίηση αυτή, αποτέλεσε το κίνητρο για την δημιουργία των *ψηφιακών πιστοποιητικών δημοσίου κλειδιού*. Τα πιστοποιητικά παρέχουν ένα ισχυρό δέσιμο ανάμεσα στο δημόσιο κλειδί και τον ιδιοκτήτη του, έτσι ώστε χρήστες να είναι σίγουροι ότι χρησιμοποιούν όντως ένα δημόσιο κλειδί που ανήκει στην οντότητα στην οποία θέλουν να στείλουν ένα κρυπτογραφημένο μήνυμα. *Η Αρχή Πιστοποίησης –*

ΑΠ (Certification Authority – CA) αποτελεί έναν εκδότη πιστοποιητικών τον οποίο καλούνται να εμπιστευθούν οι χρήστες και εγγυάται για τις ταυτότητες που περιέχονται μέσα στα πιστοποιητικά.
Η ΑΠ διατηρεί μια βάση δεδομένων για όλα τα δημόσια κλειδιά που έχουν δημοσιευθεί και διανέμει πιστοποιητικά δημοσίου κλειδιού. Κάθε πιστοποιητικό είναι επί της ουσίας μια δήλωση της Αρχής που περιγράφει το δημόσιο κλειδί ενός χρήστη και περιλαμβάνει το όνομά του και το δημόσιο κλειδί. Η ΑΠ υπογράφει κάθε πιστοποιητικό με το δικό της ιδιωτικό κλειδί. Ανάλογα με την πολιτική που ακολουθείται, η υπογραφή μπορεί να μεταδίδει και επιπρόσθετη πληροφορία, όπως για παράδειγμα την εγγύηση για την φερεγγυότητα του χρήστη ως προς την πίστωση χρημάτων. Το υπογεγραμμένο πιστοποιητικό επίσης αποτρέπει την μη ανιχνεύσιμη αλλοίωση του δημοσίου κλειδιού κάποιου χρήστη. Αν κάποιος χρήστης έχει στα χέρια του ένα πιστοποιητικό που έχει προέλθει απο μια ΑΠ, και η υπογραφή της ΑΠ στο πιστοποιητικό είναι έγκυρη, τότε ο χρήστης αυτός μπορεί να είναι σίγουρος ότι το δημόσιο κλειδί όντως ανήκει στο πρόσωπο ή τον οργανισμό που αναφέρεται μέσα του και ότι το κλειδί είναι σωστό.
Κάθε ΑΠ πρέπει να έχει μια *Δήλωση Πρακτικών Πιστοποίησης – ΔΠΠ (Certification Practice Statement – CPS)* που αποτελεί μια δήλωση των πρακτικών που εφαρμόζει η Αρχή προκειμένου να εκδώσει πιστοποιητικά. Η ΔΠΠ περιγράφει την λειτουργία της ΑΠ, τον τρόπο ελέγχου της ταυτότητας των οντοτήτων που ζητούν πιστοποιητικά πριν την έκδοση των τελευταίων, καθώς και το είδος των υποχρεώσεων και υπευθυνοτήτων που αναλαμβάνει. Επιπρόσθετα, κάθε ΑΠ υποστηρίζει μια ή περισσότερες *Πολιτικές Πιστοποιητικού – ΠΠ (Certificate Policy - CP)*. Μια πολιτική πιστοποιητικού αποτελεί ένα σύνολο απο κανόνες που καθορίζουν την καταλληλότητα ενός πιστοποιητικού για μια συγκεκριμένη κοινότητα ή κλάση εφαρμογών με κοινές απαιτήσεις ασφάλειας.
Μια ΔΠΠ αποτελεί μια αναλυτική δήλωση απο την ΑΠ για τις πρακτικές της που θα πρέπει να είναι κατανοητή απο τους εγγεγραμμένους χρήστες. Παρ' όλο που το επίπεδο της λεπτομέρειας μπορεί να διαφέρει απο ΔΠΠ σε ΔΠΠ, συνήθως είναι πιο λεπτομερείς απο μια ΠΠ. Μια ΠΠ απο την άλλη, αποτελεί κυρίως το όχημα για την εξασφάλιση της διαλειτουργικότητας σε παγκόσμια βάση. Μια ΑΠ μέσα σε μια μοναδική ΔΠΠ μπορεί να υποστηρίζει πολλαπλές ΠΠ (που χρησιμοποιούνται για διαφορετικούς σκοπούς εφαρμογών ή διαφορετικές κοινότητες χρηστών). Επίσης διαφορετικές ΑΠ, με διαφορετικές ΔΠΠ, μπορούν να υποστηρίζουν μια κοινή ΠΠ.
Θεωρείται απίθανο ένας οργανισμός ΑΠ σε μια μεγάλη κοινότητα χρηστών να μπορεί να γνωρίζει όλους τους πιθανούς χρήστες που θέλουν να επικοινωνήσουν ασφαλώς. Αυτό οδηγεί στην ανάγκη για δημιουργία περισσότερων ΑΠ, οι οποίες υποστηρίζουν ένα *μοντέλο εμπιστοσύνης (trust model),* το οποίο αποτελεί έναν τρόπο οργάνωσης ΑΠ που υποδεικνύει ποιες οντότητες μπορεί να εμπιστευτεί ένας χρήστης. Ένα μοντέλο εμπιστοσύνης καθορίζει πως μέσα σε μια συγκεκριμένη κοινότητα μπορούν οι ΑΠ να οργανώνονται σε μια *ιεραρχία*. Οποιοσδήποτε μέσα στην ιεραρχία, μπορεί να χρησιμοποιήσει ένα πιστοποιητικό που έχει προέλθει απο μια ΑΠ της ιεραρχίας προκειμένου να στείλει ένα κρυπτογραφημένο μήνυμα σε κάποιον που επίσης ανήκει στην ιεραρχία (και άρα τον εμπιστεύεται). Τα πιο διαδεδομένα μοντέλα εμπιστοσύνης ακολουθούν.

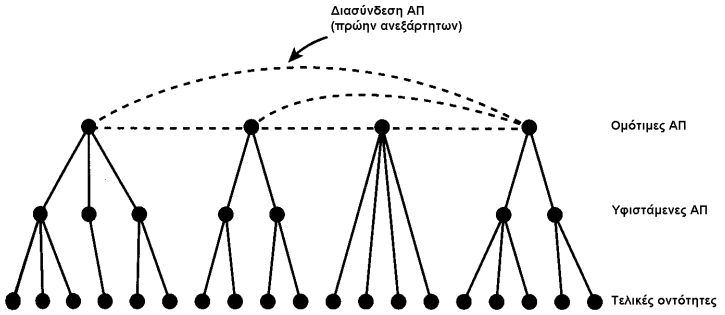
- Η πιο συνηθισμένη μορφή οργάνωσης των ΑΠ είναι το *αυστηρά ιεραρχικό μοντέλο (strict hierarchy model)*, όπου η ιεραρχία έχει τη μορφή ενός δέντρου, με μια συγκεκριμένη ΑΠ να παίζει το ρόλο του *κόμβου ρίζα (root CA)* και να αποτελεί την αρχή της εμπιστοσύνης για όλες τις οντότητες που συμμετέχουν. Κάτω απο τη ρίζα

υπάρχουν ένα η περισσότερα επίπεδα *υφιστάμενων ΑΠ (subordinate CAs)* και τα φύλλα του δέντρου είναι οι τελικές οντότητες που λαμβάνουν τα πιστοποιητικά. Όλες οι οντότητες στην κοινότητα θεωρούν το δημόσιο κλειδί της ΑΠ ρίζας ως την αρχή εμπιστοσύνης και το αρχικό ή τελικό σημείο για όλους τους ελέγχους εγκυρότητας πιστοποιητικών ως προς την εμπιστοσύνη. Ένα παράδειγμα τέτοιας ιεραρχίας αναπαρίσταται στο ακόλουθο σχήμα.



Σχήμα 7-4: Αυστηρά ιεραρχικό μοντέλο εμπιστοσύνης

- Μια άλλη μορφή οργάνωσης είναι το *κατανεμημένο μοντέλο εμπιστοσύνης (distribute trust model)* όπου επί της ουσίας υπάρχουν μικρότερες κοινότητες βασισμένες στο αυστηρά ιεραρχικό μοντέλο και οι ΑΠ ρίζες τους διαπιστεύουν η μια την άλλη, όπως φαίνεται στο σχήμα 5:



Σχήμα 7-5: Κατανεμημένο μοντέλο εμπιστοσύνης

- Στο *πλήρες διασυνδεδεμένο μοντέλο (mesh model)* όλες οι συμμετέχουσες ΑΠ διαπιστεύουν η μια την άλλη. Στο *μοντέλο κεντρικού σημείου (hub-and-spoke model)* έχουμε πάλι διαφορετικές κοινότητες, όπου όμως η κάθε ΑΠ διαπιστεύεται μόνο με μια κεντρική ΑΠ, της οποίας αποκλειστική ευθύνη είναι να διευκολύνει την μεταξύ ΑΠ μεταφορά εμπιστοσύνης. Αυτή η μορφή ονομάζεται στη βιβλιογραφία και *«ΑΠ γέφυρα» (bridge CA)* διότι γεφυρώνει το κενό επικοινωνίας ανάμεσα σε ζευγάρια ΑΠ ριζών.
- Το *μοντέλο διαδικτύου (web model)* έχει πάρει το όνομά του απο την μέθοδο που έχει χρησιμοποιηθεί στους πλέον διαδεδομένους φυλλομετρητές Ιστού (web browsers) μέχρι τώρα. Στο μοντέλο αυτό, ένας αριθμός απο δημόσια κλειδιά και πιστοποιητικά είναι προεγκατεστημένα στις εφαρμογές που θα τα χρησιμοποιήσουν (ως επί το πλείστον φυλλομετρητές και εφαρμογές ηλεκτρονικού ταχυδρομείου) απο τον κατασκευαστή τους, και αυτά καθορίζουν ποιες ΑΠ ο χρήστης της εφαρμογής εμπιστεύεται αρχικά. Το σύνολο των πιστοποιητικών αυτών μπορεί να αλλάξει, και ο χρήστης να προσθέσει ή αφαιρέσει ΑΠ κατά βούληση. Επιπρόσθετα, οι εφαρμογές συνήθως παρέχουν τρόπους

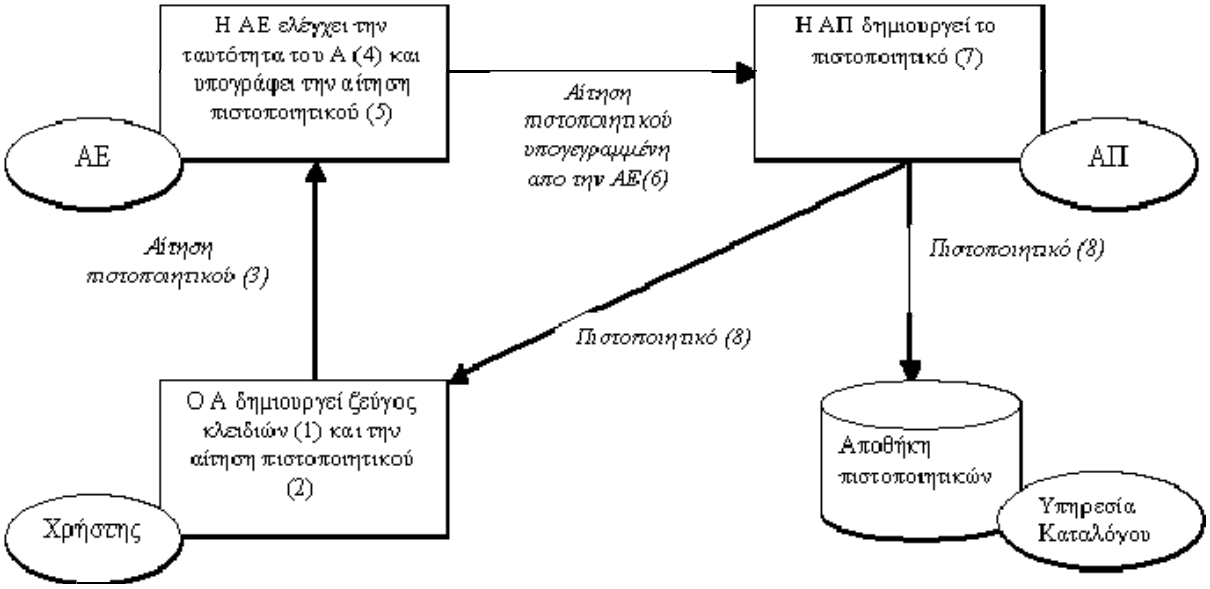
για ανανέωση των πιστοποιητικών ΑΠ που διαθέτουν απο μια κεντρική πηγή ανά τακτά χρονικά διαστήματα.

- Τέλος υπάρχει το λεγόμενο *μοντέλο εμπιστοσύνης βασισμένο στον χρήστη (user centric trust model)* όπου κάθε χρήστης είναι άμεσα και συνολικά υπεύθυνος για τα πιστοποιητικά που εμπιστεύεται ή απορρίπτει. Το πιο διαδεδομένο παράδειγμα υλοποίησης του μοντέλου αυτού είναι το PGP (Pretty Good Privacy) [Callas98].

Μία οντότητα μπορεί να επιλέξει να ανήκει σε περισσότερες της μιας ιεραρχίες. Μια ιεραρχία μπορεί να εφαρμόζει αυστηρότερους κανόνες στην ταυτοποίηση ενός χρήστη απο άλλες προτού εκδώσει ένα πιστοποιητικό. Μια ιεραρχία μπορεί να υποστηρίζει τους χρήστες μόνο μιας συγκεκριμένης εφαρμογής. Για παράδειγμα το πιστοποιητικό που έχει εκδοθεί απο έναν τραπεζικό οργανισμό θα μπορούσε να χρησιμοποιηθεί και για οικονομικές συναλλαγές.
Ένα άτομο που ανήκει σε μια ιεραρχία είναι πιθανό να θέλει να επικοινωνήσει με ένα άτομο που ανήκει σε μια διαφορετική ιεραρχία. Το άτομο αυτό μπορεί να επιλέξει αν θέλει να ανήκει και στις δύο ιεραρχίες (αν γίνεται). Μια άλλη επιλογή είναι δυο κόμβοι ΑΠ μέσα στις ιεραρχίες αυτές (για παράδειγμα οι κόμβοι στην κορυφή των ιεραρχιών αν υπάρχουν) να διαπιστεύσουν ο ένας τον άλλον. Διαμέσου της *διαπίστευσης (cross-certification)*, οι κόμβοι παρέχουν έναν τρόπο σε κατόχους πιστοποιητικών της μιας ιεραρχίας να επιβεβαιώσουν την εγκυρότητα πιστοποιητικών της άλλης ιεραρχίας. Η διαπίστευση πρέπει να γίνει προσεκτικά προκειμένου να διασφαλιστεί ότι οι πολιτικές που εφαρμόζονται απο τις ΑΠ είναι συμβατές.
Η εδραίωση μια ιεραρχίας ΑΠ πρέπει να λάβει υπόψην παραμέτρους όπως το κόστος, η απόδοση και η προσφερόμενη λειτουργικότητα. Επιπρόσθετα, υπάρχει το ζήτημα της υπευθυνότητας που πρέπει να παρέχει η ΑΠ. Κάποιες ΑΠ ενδέχεται να πρέπει να υποστηρίξουν τα πιστοποιητικά τους με χρηματικές εγγυήσεις. Αυτό σημαίνει ότι στην περίπτωση που ένας χρήστης πιστοποιητικών υποστεί κακόβουλη ενέργεια για την οποία ευθύνεται η ΑΠ (λόγω π.χ. κακής διενέργειας της διαδικασίας εγγραφής για ένα πιστοποιητικό που χρησιμοποιείται για χρηματικές συναλλαγές), θα πρέπει η ΑΠ να μπορεί να αποζημιώσει τον χρήστη. Στην περίπτωση αυτή θα πρέπει να ορίζει εξ αρχής τι χρηματική εγγύηση συνδέεται με κάθε τύπο πιστοποιητικού που παρέχει. Όσο υψηλότερο είναι το επίπεδο ασφάλειας που παρέχεται, τόσο υψηλότερο είναι και το ποσό της χρηματικής εγγύησης (και τόσο δυσκολότερο να παρακαμφθεί η ασφάλεια που παρέχει το πιστοποιητικό απο κάποιον κακόβουλο χρήστη).

7.1.4 Υποδομές Δημοσίου Κλειδιού (ΥΔΚ)

Τα πιστοποιητικά δημοσίου κλειδιού απαιτούν μια υποδομή διαχείρισης προκειμένου να υποστηριχθεί η δημιουργία, διανομή και ανάκλησή τους. Μια τέτοιου είδους υποδομή είναι η *Υποδομή Δημοσίου Κλειδιού – ΥΔΚ (Public Key Infrastructure – PKI)*. Η ΥΔΚ περιλαμβάνει έναν αριθμό δομικών στοιχείων, με βασικότερο την ΑΠ όπως περιγράφηκε στην προηγούμενη παράγραφο. Επιπρόσθετα μπορεί να περιλαμβάνει μια *Αρχή Εγγραφής – ΑΕ (Registration Authority – RA)* και μια υπηρεσία καταλόγου. Πέρα απο τα στοιχεία λογισμικού, υπάρχει επίσης μια ΔΠΠ, όπως αναφέρεται στην παράγραφο 2.1.2, που περιγράφει την λειτουργία της ΥΔΚ, τα μέτρα ασφαλείας της, και την έκταση των ευθυνών της καθώς και μια ή περισσότερες ΠΠ, για τα διάφορα είδη πιστοποιητικών που εκδίδονται στα πλαίσια της ΥΔΚ. Μια ΥΔΚ ενδέχεται να λειτουργεί με διάφορους τρόπους. Στο σχήμα που ακολουθεί αναπαρίσταται ένας τέτοιος τρόπος, που είναι και απο τους πλέον διαδεδομένους.



Σχήμα 7-6: Διαδικασία έκδοσης ψηφιακού πιστοποιητικού

1. Ο χρήστης Α ξεκινά την διαδικασία δημιουργώντας ένα ζεύγος κλειδιών (δημοσίου – ιδιωτικού), πιθανόν πάνω σε μια έξυπνη κάρτα.
2. Το λογισμικό στο σύστημα του Α δημιουργεί μια *αίτηση πιστοποιητικού* βάσει του δημοσίου κλειδιού. Η αίτηση πιστοποιητικού υπογράφεται με το ιδιωτικό κλειδί του Α (που φυσικά σχετίζεται με το αντίστοιχο δημόσιο που περιέχεται στην αίτηση).
3. Η αίτηση μαζί με οποιαδήποτε άλλα απαιτούμενα δεδομένα και στοιχεία, αποστέλλονται στην ΑΕ.
4. Προτού η ΑΠ εκδώσει το πιστοποιητικό, ο χρήσης Α πρέπει να πείσει την ΑΕ (η οποία επέχει το ρόλο έμπιστου πράκτορα της ΑΠ) ότι είναι όντως αυτός που ισχυρίζεται. Στη συνηθισμένη περίπτωση η ΑΕ αποτελείται απο προσωπικό και το απαραίτητο λογισμικό που επεξεργάζεται αιτήσεις πιστοποιητικών. Το προσωπικό ελέγχει τα στοιχεία που δίνει ο Α και αν συμφωνούν με την αίτηση που έχει κάνει.
5. Εάν η επαλήθευση της ταυτότητας του Α είναι επιτυχής, η ΑΕ υπογράφει ξανά την αίτηση πιστοποιητικού που έχει ήδη υπογράψει ο Α. Εναλλακτικά η αίτηση πιστοποιητικού αποστέλλεται με την αρχική υπογραφή του Α (και μόνο) στην ΑΠ. Η υπογραφή του Α στην αρχική αίτηση αποδεικνύει ότι ο Α κατέχει το ιδιωτικό κλειδί που ταιριάζει στο δημόσιο που περιλαμβάνει η αίτηση. Σε μερικές περιπτώσεις, προκειμένου να εξασφαλιστεί η ακεραιότητα της διαδικασίας, τα κλειδιά δημιουργούνται παρουσία της ΑΕ.
6. Η ΑΕ αποστέλλει την αίτηση πιστοποιητικού στην ΑΠ.
7. Η ΑΠ ελέγχει την υπογραφή της ΑΕ στην αίτηση και ότι η συγκεκριμένη ΑΕ είναι εξουσιοδοτημένη να κάνει την συγκεκριμένη αίτηση. Αν ο έλεγχος αυτός είναι επιτυχημένος, η ΑΠ λαμβάνει το δημόσιο κλειδί που περιέχεται στην αίτηση, δημιουργεί ένα πιστοποιητικό με αυτό και το υπογράφει.
8. Το πιστοποιητικό επιστρέφεται στον Α, ο οποίος το εισάγει στο λογισμικό που χρησιμοποιεί και που ενδέχεται να υλοποιεί μορφές υπηρεσιών ασφάλειας βασισμένων σε ΥΔΚ, για παράδειγμα την αποστολή *ασφαλούς ηλεκτρονικού ταχυδρομείου (secure e-mail)*. Ένας χρήστης Β αποδέκτης ενός ψηφιακά υπογεγραμμένου e-mail, μπορεί να ελέγξει την υπογραφή βάσει του δημοσίου κλειδιού που περιλαμβάνεται στο

πιστοποιητικό (το οποίο ενδέχεται να το έχει απο προηγούμενη επικοινωνία ή περιλαμβάνεται στο ίδιο το μήνυμα).
9. Η ΑΠ αρχειοθετεί το πιστοποιητικό σε έναν δημόσιο κατάλογο, έτσι ώστε οποιοσδήποτε θέλει να επικοινωνήσει ασφαλώς με τον Α, ή να επιβεβαιώσει μια υπογραφή του να μπορεί να ανακτήσει το πιστοποιητικό του Α απο εκεί, ανεξαρτήτως της άμεσης μεθόδου επικοινωνίας μεταξύ τους.
Αν για κάποιο λόγο, τα κλειδιά του Α υποκλαπούν, ή το πιστοποιητικό του Α αλλοιωθεί, η ΑΠ πρέπει να ειδοποιηθεί, προκειμένου να ανακληθεί το πιστοποιητικό. Μόλις η ΑΠ ειδοποιηθεί ότι το πιστοποιητικό δεν είναι πλέον έγκυρο, το τοποθετεί σε μία *Λίστα Ανάκλησης Πιστοποιητικών – ΛΑΠ (Certificate Revocation List – CRL)* [Housley02] μαζί με την ημερομηνία και την ώρα απο την οποία το πιστοποιητικό έπαψε να είναι έγκυρο. Μηνύματα που έχουν υπογραφεί ή κρυπτογραφηθεί πριν την συγκεκριμένη ώρα και μέρα θεωρούνται έγκυρα. Μηνύματα που έχουν κρυπτογραφηθεί κατόπιν του χρονικού αυτού σημείου, υπάρχει το ενδεχόμενο να έχουν παραποιηθεί. Η ΑΠ ανανεώνει την ΛΑΠ και την δημοσιοποιεί συνήθως κάνοντας χρήση ενός *καταλόγου LDAP (Lightweight Directory Access Protocol)* [Hodges02], ο οποίος περιλαμβάνει πιστοποιητικά και ΛΑΠ σε μια δενδροειδή οργανωτική δομή. Οντότητες που θέλουν να επικοινωνήσουν ασφαλώς με κάποιον χρήστη στην ιεραρχία, μπορούν να ψάξουν και να λάβουν το πιστοποιητικό του απο τον κατάλογο και ταυτόχρονα να ελέγξουν την εγκυρότητά του απο την ΛΑΠ. Στη θεωρία, οποιοσδήποτε θέλει να χρησιμοποιήσει το δημόσιο κλειδί του Α θα πρέπει πρώτα να συμβουλευτεί την ΛΑΠ. Στην πράξη όμως, ο προσδιορισμός και η πρόσβαση στον κατάλογο μιας ΑΠ μπορεί να είναι δυσχερής (όπως συμβαίνει με τις σύγχρονες εφαρμογές που κάνουν χρήση υπηρεσιών ΥΔΚ οι οποίες δεν υλοποιούν αυτό το χαρακτηριστικό). Αυτό δημιουργεί ένα κενό στην ασφάλεια του όλου συστήματος.

7.2 Πρότυπα ασφάλειας XML

Η XML αποτελεί ένα υποσύνολο της *Standard Generalized Markup Language (SGML)*. Απο κατασκευής, έγγραφα XML συμμορφώνονται στην SGML. Η XML είναι μια δομημένη γλώσσα, κάτι που σημαίνει ότι ένα έγγραφο XML δεν περιέχει μόνο δεδομένα αλλά καθορίζει επίσης τις δομικές σχέσεις ανάμεσα στα δεδομένα αυτά. Αυτή είναι η δύναμη της XML, που επιτρέπει την αναπαράσταση οποιουδήποτε είδους δεδομένων, εφόσον έχει οριστεί το δομικό τους σχήμα. Οι προδιαγραφές της δομής ενός εγγράφου XML μπορούν να επιτευχθούν με την βοήθεια μοντέλων. Ειδικότερα μπορεί να χρησιμοποιηθεί είτε με το *μοντέλο Ορισμού Τύπων Εγγράφου (Document Type Definitions – DTD)* [Bray00] ή τα *Σχήματα XML (XML Schemas)* [Fallside04], τα οποία εξασφαλίζουν ότι δύο ή περισσότερα έγγραφα είναι του ίδιου «τύπου». Σε ότι αφορά στην αναπαράσταση της πληροφορίας μέσα σε ένα έγγραφο, η XML χαρακτηρίζεται απο ανεξαρτησία απο υποκείμενες πλατφόρμες, διότι όλη η πληροφορία αποθηκεύεται σε μορφή απλού κειμένου. Αυτή είναι μια απο τις πολύ ισχυρές της ιδιότητες, που κάνει τα έγγραφα XML αναγνώσιμα και απο μηχανές και απο ανθρώπους και εύκολα ενσωματώσιμα σε *ροές εργασιών (workflows)*.

Σύμφωνα με τα παραπάνω, η XML σε ένα σύστημα χρησιμοποιείται για να προδιαγραφούν έγγραφα και μηνύματα που ανταλλάσσονται μεταξύ οντοτήτων. Αυτό συνεπάγεται ότι η ασφάλεια XML ασχολείται με την ασφάλεια σε επίπεδο μηνυμάτων και οι κύριες τεχνικές που χρησιμοποιούνται είναι η κρυπτογράφηση και οι ψηφιακές υπογραφές. Παρόλο που υπάρχουσες τεχνικές για κρυπτογράφηση ηλεκτρονικού ταχυδρομείου ή αρχείων μπορούν να χρησιμοποιηθούν και για μηνύματα XML, τεχνικές που είναι εξειδικευμένες για την XML θεωρούνται πιο κατάλληλες γι' αυτό το σκοπό. Την προσπάθεια προτυποποίησης στον τομέα αυτό οδηγεί ο οργανισμός W3C. Ένα πρότυπο για την παραγωγή ψηφιακών υπογραφών σε XML υπάρχει στη μορφή σύστασης του W3C (W3C recommendation) [XMLSIG] καθώς και ως RFC απο την IETF (RFC 3275 XML-Signature Syntax and Processing) [RFC3275]. Υπάρχει επίσης μια υποψήφια σύσταση του W3C για κρυπτογράφηση XML [XMLENC]. Σε Ευρωπαϊκό επίπεδο, ο οργανισμός προτυποποίησης ETSI έχει εκδώσει το πρότυπο "XML Advanced Electronic Signatures – XAdES" [XAdES, XAdESW3C], το οποίο κάνει χρήση του παραπάνω προτύπου του W3C για ψηφιακές υπογραφές XML και έχει ως στόχο την δημιουργία προηγμένων υπογραφών που εμπεριέχουν τα απαραίτητα δεδομένα, όπως *χρονοσφραγίδες (timestamps)*, προκειμένου να μπορούν να επαληθευτούν μακροπρόθεσμα.

7.2.1 Κρυπτογράφηση XML

Το υποψήφιο πρότυπο για *Σύνταξη και Επεξεργασία Κρυπτογράφησης XML (XML Encryption Syntax and Processing)* περιγράφει μια διαδικασία για την κρυπτογράφηση ψηφιακών δεδομένων και τον τρόπο με τον οποίο το αποτέλεσμα της κρυπτογράφησης θα έπρεπε να αναπαρασταθεί σε XML. Η μέθοδος αυτή είναι πιο κατάλληλη για την κρυπτογράφηση των ίδιων των δεδομένων XML, αλλά μπορεί να εφαρμοστεί και στην γενική περίπτωση για οποιονδήποτε άλλο τύπο δεδομένων. Η Κρυπτογράφηση XML υποστηρίζει την κρυπτογράφηση ενός ολόκληρου κειμένου XML ή μόνο επιλεγμένων κομματιών του. Η μικρότερη μονάδα πληροφορίας που μπορεί να κρυπτογραφηθεί είναι ένα *στοιχείο XML (XML element)*. Υποστηρίζεται επίσης η επανακρυπτογράφηση

δεδομένων, δηλαδή δεδομένα που έχουν ήδη κρυπτογραφηθεί μια φορά μπορούν να επανακρυπτογραφηθούν. Η μέθοδος επίσης παρέχει την αναγνώριση ή τη μεταφορά πληροφορίας για τα κλειδιά αποκρυπτογράφησης.
Η πρόταση του W3C επικεντρώνει στον καθορισμό της διαδικασίας δημιουργίας και αναπαράστασης των κρυπτογραφημένων δεδομένων XML, καθώς φυσικά και της διαδικασίας αποκρυπτογράφησης. Δεν προδιαγράφει νέους αλγορίθμους. Αντίθετα, χρησιμοποιεί υπάρχοντες αλγορίθμους για την κρυπτογράφηση / αποκρυπτογράφηση, την συμφωνία κλειδιών, τις συναρτήσεις κατακερματισμού, την αυθεντικοποίηση μηνυμάτων και άλλες κρυπτογραφικές εφαρμογές (εκτός απο την διαδικασία παραγωγής ψηφιακών υπογραφών που καλύπτονται απο άλλο πρότυπο) όπως περιγράφονται στην παράγραφο 7.1.2. Η πρόταση περιγράφει την χρήση συμμετρικής και ασύμμετρης κρυπτογραφίας.

7.2.1.1 Μορφή / Δομή

Τα έγγραφα XML αποτελούνται απο ένα σύνολο *στοιχείων (tags)* τα οποία απαρτίζουν την δομή του εγγράφου. Σύμφωνα με το πρότυπο για την κρυπτογράφηση, τα κρυπτογραφημένα δεδομένα περιέχονται στο στοιχείο EncryptedData, που επί της ουσίας αντικαθιστά τα προς κρυπτογράφηση δεδομένα μέσα στο έγγραφο. Η δομή του EncryptedData βασίζεται στο σχήμα του στοιχείου EncryptedType, όπως φαίνεται στο επόμενο σχήμα:

```
<complexType name='EncryptedType' abstract='true'>
  <sequence>
    <element name='EncryptionMethod' type='xenc:EncryptionMethodType'
             minOccurs='0'/>
    <element ref='ds:KeyInfo' minOccurs='0'/>
    <element ref='xenc:CipherData'/>
    <element ref='xenc:EncryptionProperties' minOccurs='0'/>
  </sequence>
  <attribute name='Id' type='ID' use='optional'/>
  <attribute name='Type' type='anyURI' use='optional'/>
  <attribute name='MimeType' type='string' use='optional'/>
  <attribute name='Encoding' type='anyURI' use='optional'/>
 </complexType>
```

Σχήμα 7-7: Το σχήμα για τον τύπο EncryptedType

Το στοιχείο EncryptedData κατ' ελάχιστον αποτελείται απο τα κρυπτογραφημένα δεδομένα εντός ενός στοιχείου CipherData.

```
<element name='CipherData' type='xenc:CipherDataType'/>
<complexType name='CipherDataType'>
   <choice>
     <element name='CipherValue' type='base64Binary'/>
     <element ref='xenc:CipherReference'/>
   </choice>
 </complexType>
```

Σχήμα 7-8 : Το σχήμα για το στοιχείο CipherData

Επιπρόσθετα μπορεί να περιλαμβάνει τα στοιχεία EncryptionMethod, KeyInfo και EncryptionProperties, τα οποία είναι όλα προαιρετικά και περιγράφονται στην συνέχεια της παρούσας παραγράφου.
Όπως φαίνεται απο το σχήμα Σχήμα 7-8, το στοιχείο CipherData μπορεί να αναπαρασταθεί με δύο τρόπους. Ο πρώτος είναι να περιέχει το ίδιο το κρυπτογραφημένο κείμενο ως XML, που είναι και η πιο συνηθισμένη περίπτωση. Τα κρυπτογραφημένα δεδομένα δεν είναι πλέον κατανοητά αφού το κείμενο είναι κωδικοποιημένο σε μορφή base64 (βλ. παράγραφο 7.1.2.6). Ο δεύτερος τρόπος είναι η δομή CipherData να περιέχει μια *αναφορά (Reference)* στο κρυπτογραφημένο αντικείμενο και όχι το ίδιο το αντικείμενο.
Το στοιχείο EncryptionMethod περιέχει τον αλγόριθμο κρυπτογράφησης και το μέγεθος του κλειδιού. Ο τύπος στον οποίο βασίζεται είναι ο EncryptedMethodType ο οποίος φαίνεται στο ακόλουθο σχήμα:

```
<complexType name='EncryptionMethodType' mixed='true'>
  <sequence>
    <element name='KeySize' minOccurs='0' type='xenc:KeySizeType'/>
    <element name='OAEPparams' minOccurs='0' type='base64Binary'/>
    <any namespace='##other' minOccurs='0' maxOccurs='unbounded'/>
  </sequence>
  <attribute name='Algorithm' type='anyURI' use='required'/>
</complexType>
```

Σχήμα 7-9: Ο τύπος EncryptionMethodType

Το στοιχείο KeyInfo παρέχει την πληροφορία που απαιτείται απο την εφαρμογή του παραλήπτη προκειμένου να αποκρυπτογραφήσει τα δεδομένα. Εάν παραλείπεται, αναμένεται απο την εφαρμογή να γνωρίζει πώς θα υλοποιήσει την αποκρυπτογράφηση, συμπεριλαμβανομένης της επιλογής του κλειδιού που θα χρησιμοποιήσει.

```
<element name="KeyInfo" type="ds:KeyInfoType"/>
<complexType name="KeyInfoType" mixed="true">
  <choice maxOccurs="unbounded">
    <element ref="ds:KeyName"/>
    <element ref="ds:KeyValue"/>
    <element ref="ds:RetrievalMethod"/>
    <element ref="ds:X509Data"/>
    <element ref="ds:PGPData"/>
    <element ref="ds:SPKIData"/>
    <element ref="ds:MgmtData"/>
    <any processContents="lax" namespace="##other"/>
    <!-- (1,1) elements from (0,unbounded) namespaces -->
  </choice>
  <attribute name="Id" type="ID" use="optional"/>
</complexType>
```

Σχήμα 7-10: Το σχήμα για το στοιχείο KeyInfo

Η Κρυπτογράφηση XML επιτρέπει στον αποστολέα και τον παραλήπτη των κρυπτογραφημένων δεδομένων να προεπιλέξουν κρυπτογραφικές παραμέτρους, συμπεριλαμβανομένου των κλειδιών , έτσι ώστε οι παράμετροι να μην χρειάζονται να ανταλλαχθούν την ίδια τη στιγμή που επιτελείται η κρυπτογράφηση. Επιπρόσθετα, υποστηρίζει όλες τις επιλογές που προδιαγράφονται απο το πρότυπο Ψηφιακής

Υπογραφής XML για τον προσδιορισμό των κλειδιών. Ο προσδιορισμός μπορεί να επιτευχθεί με ένα αναγνωριστικό κλειδιού, το ίδιο το κλειδί αποκρυπτογράφησης, μια αναφορά σε μια τοποθεσία όπου βρίσκεται το κλειδί, ή το πιστοποιητικό δημοσίου κλειδιού του παραλήπτη που χρησιμοποιήθηκε για την κρυπτογράφηση των δεδομένων. Υποστηρίζονται διάφοροι τύποι πιστοποιητικών, συμπεριλαμβανομένου των X509. Παρ' όλα αυτά, ορισμένες αναπαραστάσεις κλειδιών δεν είναι χρήσιμες στην περίπτωση της Κρυπτογράφησης XML. Για παράδειγμα, η αποστολή του ίδιου του κλειδιού αποκρυπτογράφησης μαζί με τα δεδομένα που αυτό αποκαλύπτει προφανώς δεν ωφελεί. Ως εναλλακτική λύση, η Κρυπτογράφηση XML επεκτείνει τις επιλογές της Ψηφιακής Υπογραφής XML και προσθέτει την επιλογή για ένα EncryptedKey. Εάν η δομή KeyInfo δεν περιλαμβάνεται, η εφαρμογή του παραλήπτη θα πρέπει να γνωρίζει ποιο κλειδί να χρησιμοποιήσει για να αποκρυπτογραφήσει το μήνυμα. Εν κατακλείδι, το στοιχείο EncryptionProperties περιέχει επιπρόσθετες πληροφορίες σχετικές με την διαδικασία.

7.2.1.2 Διαδικασία κρυπτογράφησης και αποκρυπτογράφησης

Για να κρυπτογραφηθούν στοιχεία XML ακολουθείται η παρακάτω διαδικασία:

1. Επιλέγεται ο αλγόριθμος κρυπτογράφησης και οι παράμετροί του.
2. Ανακτάται το κλειδί. Αν το κλειδί πρόκειται να αναγνωριστεί, δημιουργείται ένα στοιχείο KeyInfo. Αν πρόκειται να αποσταλεί μαζί με τα κρυπτογραφημένα δεδομένα, κρυπτογραφείται και δημιουργείται ένα στοιχείο EncryptedKey, το οποίο τοποθετείται μέσα στο στοιχείο KeyInfo, ή κάποιο άλλο σημείο μέσα στο έγγραφο.
3. Κρυπτογραφούνται τα δεδομένα. Για δεδομένα XML αυτό μπορεί να εμπεριέχει την κωδικοποίηση σε UTF-8 [UTF8] και σειριοποίηση, δηλαδή την μετατροπή της δομής σε μια ακολουθία απο bytes. Το αποτέλεσμα είναι ένα octet string.
4. Δημιουργείται το στοιχείο EncryptedData. Στην περίπτωση που τα κρυπτογραφημένα δεδομένα αποθηκεύονται μέσα στο έγγραφο (αντί να υπάρχει απλά μια αναφορά σε αυτά), τότε πρέπει να είναι κωδικοποιημένα στη μορφή base64.
5. Αντικαθίστανται τα προς κρυπτογράφηση δεδομένα μέσα στο ίδιο το έγγραφο XML, με το στοιχείο EncryptedData.

Προκειμένου να επιτευχθεί η αποκρυπτογράφηση των δεδομένων, ακολουθούνται τα επόμενα βήματα.

1. Γίνεται επεξεργασία του στοιχείου EncryptedData. Απροσδιόριστες παράμετροι, παρέχονται απο την εφαρμογή.
2. Ανακτάται το κλειδί αποκρυπτογράφησης. Αυτό μπορεί να περιλαμβάνει πρώτα την αποκρυπτογράφηση ενός συμμετρικού κλειδιού απο ένα ιδιωτικό ή την ανάκτηση απο μια τοπική αποθήκη κλειδιών, στο δίσκο του χρήστη ή μια έξυπνη κάρτα.
3. Αποκρυπτογραφούνται τα δεδομένα στη δομή CipherData.
4. Γίνεται επεξεργασία των αποκρυπτογραφημένων δεδομένων. Αυτό μπορεί να απαιτεί την επαναφορά των δεδομένων, που έχουν κωδικοποιηθεί ως UTF-8, στην αρχική τους μορφή. Επίσης, γίνεται αντικατάσταση των δεδομένων στην αρχική τους θέση μέσα στη δομή του εγγράφου XML. Σε μερικές περιπτώσεις, ενδέχεται να απαιτείται και περαιτέρω επεξεργασία.

7.2.1.3 Παράδειγμα

Το κομμάτι κώδικα που ακολουθεί είναι ένα παράδειγμα κρυπτογραφημένου περιεχομένου.

```
<PaymentInfo xmlns='http://example.org/paymentv2'>
      <Name>John Smith</Name>
      <CreditCard Limit='5,000' Currency='USdollars'>
      <EncryptedData xmlns='http://www.w3.org/2001/04/xmlenc#'
Type='http://www.w3.org/2001/04/xmlenc#Content'>
           <EncryptionMethod
Algorithm='http://www.w3.org/2001/04/xmlenc#3des-cbc'/>
                <ds:KeyInfo
xmlns:ds='http://www.w3.org/2000/09/xmldsig#'>
                     <ds:KeyName>mykey</ds:KeyName>
                </ds:KeyInfo>
                <CipherData>
                     <CipherValue>423EE256</CipherValue>
                </CipherData>
      </EncryptedData>
</PaymentInfo>
```

Σχήμα 7-11 :Παράδειγμα κρυπτογράφησης XML

Το κρυπτογραφημένο περιεχόμενο αντικαθιστά το αρχικό μέσα στο έγγραφο XML. Στην περίπτωση του παραδείγματος, το κρυπτογραφημένο κομμάτι αναπαριστά ευαίσθητη πληροφορία για μια πληρωμή. Το ονοματεπώνυμο στην πιστωτική κάρτα και το όριο, μεταδίδονται χωρίς επεξεργασία, ενώ ο αριθμός της κάρτας είναι κρυπτογραφημένος. Ο αλγόριθμος κρυπτογράφησης που χρησιμοποιείται είναι ο 3DES σε μορφή cipher block chaining – CBC. Το κλειδί που θα χρησιμοποιηθεί για να αποκρυπτογραφηθούν τα δεδομένα ονομάζεται mykey. Στην περίπτωση αυτή, θεωρείται ότι ο παραλήπτης του μηνύματος γνωρίζει το κλειδί απο προηγούμενη επικοινωνία. Τα κρυπτογραφημένα δεδομένα εμφανίζονται μέσα στη δομή CipherValue.

7.2.2 Ψηφιακή Υπογραφή XML

Το πρότυπο Ψηφιακής Υπογραφής XML καθορίζει πώς ψηφιακά δεδομένα υπογράφονται και πως το αποτέλεσμα της υπογραφής μπορεί να αναπαρασταθεί σε XML. Η Ψηφιακή Υπογραφή XML προορίζεται κυρίως για δεδομένα XML, αλλά μπορεί να εφαρμοστεί και γενικότερα με όλες τις μορφές ψηφιακών δεδομένων. Με την Ψηφιακή Υπογραφή XML μπορεί να υπογραφεί ένα ολόκληρο έγγραφο XML ή επιλεγμένα κομμάτια του.

Το πρότυπο καθορίζει την διαδικασία για την δημιουργία και αναπαράσταση μιας υπογραφής XML και την επαλήθευση της εγκυρότητάς της, βασιζόμενο σε υπάρχοντες αλγορίθμους για υπογραφή, συναρτήσεις κατακερματισμού, και Κώδικες Αυθεντικοποίησης Μηνυμάτων – ΚΑΜ (message authentication codes - MACs) (βλ. παράγραφο 7.1.2.5). Το πρότυπο μπορεί να συνδυαστεί με αρκετά ευρέως διαδεδομένα είδη πιστοποιητικών, συμπεριλαμβανομένου των πιστοποιητικών X509. Επίσης, μπορεί επίσης να χρησιμοποιηθεί χωρίς πιστοποιητικά, κάτι που αποκλίνει απο την γενική περίπτωση κρυπτοσυστημάτων δημοσίου κλειδιού, αλλά που μπορεί να δικαιολογηθεί υπό ορισμένες προϋποθέσεις. Το πρότυπο κάνει αναφορά σε άλλα πρότυπα για μετασχηματισμούς όπως είναι η *κανονικοποίηση*, η οποία φέρνει τα δεδομένα σε μια

πρότυπη μορφή που εξαλείφει οποιεσδήποτε δευτερεύουσες και ασήμαντες διαφορές στην αναπαράσταση και κωδικοποίηση.
Οι ψηφιακές υπογραφές είναι αρκετά πιο πολύπλοκες στην υλοποίηση απο την κρυπτογράφηση. Η δημιουργία τους πρέπει να γίνεται με ιδιαίτερη προσοχή, διότι είναι άρρηκτα δεμένες με την αναπαράσταση των δεδομένων που υπογράφονται. Αυτό σημαίνει ότι η αναπαράσταση των υπογεγραμμένων δεδομένων και των δεδομένων που διαβάζονται προκειμένου να επαληθευτεί η υπογραφή πρέπει να είναι συνεπή. Η επεξεργασία της υπογραφής είναι πολύ ευαίσθητη σε αλλαγές στην αναπαράσταση των δεδομένων και την διάταξη των βημάτων επεξεργασίας. Ακόμη και αν η υπογραφή ήταν έγκυρη τη στιγμή της δημιουργίας της, υπάρχει το ενδεχόμενο να μην μπορεί να επαληθευτεί στη συνέχεια απο τον παραλήπτη, λόγω αλλαγών που συνέβησαν κατά τη μεταφορά ενός μηνύματος.

7.2.2.1 Μορφή / Δομή

Μια Υπογραφή XML αποτελείται απο δυο απαραίτητα στοιχεία XML, το στοιχείο SignedInfo και το στοιχείο SignatureValue όπως φαίνεται στο ακόλουθο σχήμα XML:

```
<element name="Signature" type="ds:SignatureType"/>
<complexType name="SignatureType">
  <sequence>
    <element ref="ds:SignedInfo"/>
    <element ref="ds:SignatureValue"/>
    <element ref="ds:KeyInfo" minOccurs="0"/>
    <element ref="ds:Object" minOccurs="0" maxOccurs="unbounded"/>
  </sequence>
  <attribute name="Id" type="ID" use="optional"/>
</complexType>
```

Σχήμα 7-12:Το σχήμα του στοιχείου Signature

Υπάρχουν επίσης και δυο προαιρετικά στοιχεία, τα KeyInfo και Object.

SignedInfo. Περιλαμβάνει το στοιχείο CanonicalizationMethod, που είναι στην ουσία η μέθοδος κανονικοποίησης που θα εφαρμοστεί στο ίδιο το στοιχείο SignedInfo, στους αλγορίθμους που χρησιμοποιούνται για την παραγωγή της υπογραφής (συνήθως έναν αλγόριθμο κατακερματισμού και έναν αλγόριθμο ψηφιακής υπογραφής), και σε μια ή περισσότερες αναφορές (δηλ. στοιχεία Reference) στα δεδομένα που υπογράφονται.

```
<element name="SignedInfo" type="ds:SignedInfoType"/>
<complexType name="SignedInfoType">
  <sequence>
    <element ref="ds:CanonicalizationMethod"/>
    <element ref="ds:SignatureMethod"/>
    <element ref="ds:Reference" maxOccurs="unbounded"/>
  </sequence>
  <attribute name="Id" type="ID" use="optional"/>
</complexType>
```

Σχήμα 7-13:Το σχήμα του στοιχείου SignedInfo

Κάθε στοιχείο αναφοράς Reference περιλαμβάνει ένα URI που αναγνωρίζει τα δεδομένα που υπογράφονται, τους μετασχηματισμούς που αυτά υπόκεινται (κάποιοι απο τους οποίους αναλύονται στη συνέχεια), ένα αναγνωριστικό του αλγορίθμου μετασχηματισμού που θα χρησιμοποιηθεί στα προς μετασχηματισμό δεδομένα και την τιμή του αποτελέσματος της συνάρτησης κατακερματισμού.
SignatureValue. Αποτελεί την τιμή της ψηφιακής υπογραφής.

```
<element name="SignatureValue" type="ds:SignatureValueType"/>
<complexType name="SignatureValueType">
  <simpleContent>
    <extension base="base64Binary">
      <attribute name="Id" type="ID" use="optional"/>
    </extension>
  </simpleContent>
</complexType>
```

Σχήμα 7-14:Το σχήμα του στοιχείου SignatureValue

Όπως φαίνεται απο το σχήμα, η τιμή είναι κωδικοποιημένη στη μορφή base64.
KeyInfo. Παρέχει την πληροφορία που χρειάζεται απο την εφαρμογή του παραλήπτη για να επαληθεύσει την υπογραφή και το XML σχήμα του έχει ήδη παρουσιαστεί στο σχήμα Σχήμα 7-10. Εάν παραληφθεί, θεωρείται ότι η εφαρμογή γνωρίζει τον τρόπο για την επαλήθευση. Για παράδειγμα, μπορεί δύο συνεργάτες να έχουν προ-ανταλλάξει δημόσια κλειδιά με κάποιον άλλο τρόπο, εξαλείφοντας την ανάγκη για εισαγωγή του δημοσίου κλειδιού ως στοιχείο-παιδί του KeyInfo. Αν αυτό δεν έχει συντελεστεί, το KeyInfo μπορεί να περιλαμβάνει ένα αναγνωριστικό κλειδιού, ή το δημόσιο κλειδί του υπογράφοντος, ή μια αναφορά στην τοποθεσία όπου το κλειδί είναι διαθέσιμο, ή το ίδιο το ψηφιακό πιστοποιητικό δημοσίου κλειδιού. Υποστηρίζεται ένας ικανός αριθμός τύπων πιστοποιητικών.
Object. Είναι μια δομή που μπορεί να περιέχει οποιασδήποτε άλλης μορφής πληροφορία για την υποστήριξη της υπογραφής και είναι ιδιαίτερα χρήσιμη στην περίπτωση των Προηγμένων Ηλεκτρονικών Υπογραφών XML XAdES, οι οποίες παρουσιάζονται σε επόμενο κεφάλαιο.

7.2.2.2 Μετασχηματισμοί

Προτού τα δεδομένα υπογραφούν, υπόκεινται συνήθως σε μια ή περισσότερες διαδικασίες μετασχηματισμού. Οι μετασχηματισμοί αυτοί καθιστούν τα δεδομένα κατάλληλα προς υπογραφή. Για παράδειγμα, ένας πολύ γνωστός μετασχηματισμός, ο οποίος αρχικά χρησιμοποιήθηκε για το ηλεκτρονικό ταχυδρομείο, είναι η αποκωδικοποίηση base64. Η αποκωδικοποίηση base64 χρησιμοποιείται προκειμένου να υπογραφεί η αρχική έκδοση δεδομένων που έχουν κωδικοποιηθεί με base64 (βλ. παράγραφο 7.1.2.6). Για παράδειγμα, προκειμένου να εισαχθούν δυαδικά δεδομένα στο XML έγγραφο, αυτά κωδικοποιούνται με base64 και μετατρέπονται σε μια συμβολοσειρά. Συνήθως όμως σε συναρτήσεις κατακερματισμού θέλουμε να δώσουμε ως όρισμα την αρχική δυαδική μορφή των δεδομένων, άρα είναι απαραίτητο αυτά να περάσουν απο έναν μετασχηματισμό αποκωδικοποίησης base64. Επιπρόσθετα, υπάρχουν αρκετοί ακόμη μετασχηματισμοί που είναι σημαντικοί για την XML και τις Υπογραφές XML. Θα αναλυθούν στη συνέχεια οι μετασχηματισμοί *XPath (XPath Transform)*,

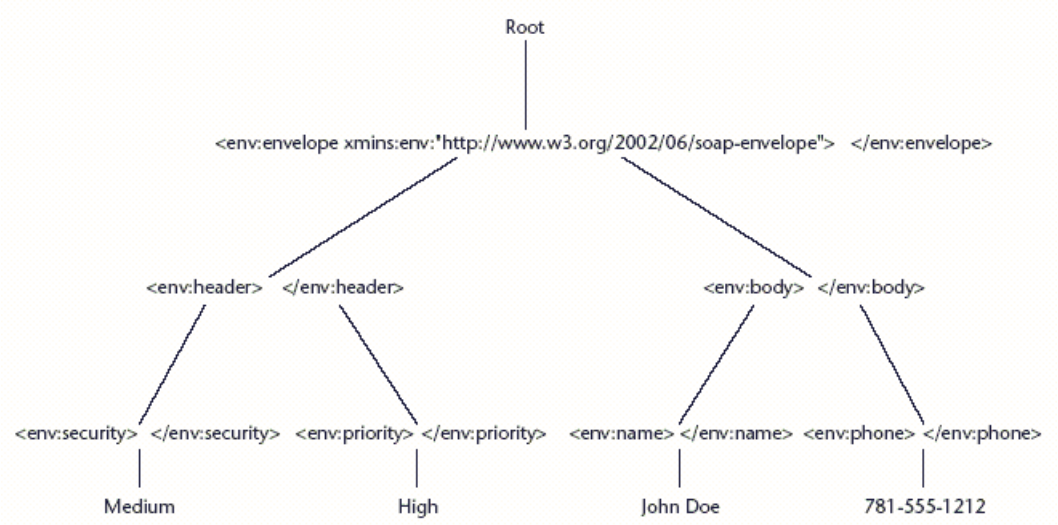
Κανονικοποίησης XML (Canonical XML Transform), και ο *Μετασχηματισμός Αποκρυπτογράφησης για την Υπογραφή XML (Decryption Transform for XML Signature)*.

Ο μετασχηματισμός κανονικοποίησης XML μπορεί να εφαρμοστεί στο στοιχείο SignedInfo. Επιπρόσθετα, κάθε στοιχείο Reference μέσα στο SingedInfo ενδέχεται να περιέχει μετασχηματισμούς που καθορίζονται στο ίδιο το στοιχείο. Η παράμετρος εισόδου στον πρώτο μετασχηματισμό είναι τα δεδομένα που καθορίζονται απο το URI του SignedInfo. Η έξοδος του μετασχηματισμού αυτού, γίνεται είσοδος του επόμενου, και ούτω καθεξής, μέχρι η έξοδος του τελευταίο μετασχηματισμού να γίνει είσοδος της συνάρτησης κατακερματισμού.
Παρόλο που η Υπογραφή XML δεν επιβάλει την χρήση των συγκεκριμένων αυτών μετασχηματισμών, η λειτουργικότητα που προσφέρουν είναι απαραίτητη προκειμένου να εκτελεστεί σωστά η συνάρτηση της υπογραφής. Ακόμη και αν ο σχεδιαστής μιας εφαρμογής δεν θέλει να χρησιμοποιήσει τους συγκεκριμένους αλγορίθμους, θα πρέπει να βρει κάτι αντίστοιχο με παρόμοια λειτουργικότητα. Η χρήση εναλλακτικών λύσεων αποθαρρύνεται γενικότερα διότι μειώνει την διαλειτουργικότητα των Υπογραφών XML.

7.2.2.3 XPath / XPointer

Υπάρχει η ανάγκη για επιλεκτική υπογραφή περιοχών μέσα στο έγγραφο XML. Σε αντίθεση με το ηλεκτρονικό ταχυδρομείο ή αρχεία, όπου ολόκληρα τα έγγραφα προορίζονται για έναν παραλήπτη, στην περίπτωση των εγγράφων XML, υπάρχει το ενδεχόμενο πολλοί παραλήπτες να πρέπει να επεξεργαστούν ένα έγγραφο, και κάθε ένας να πρέπει να υπογράψει ή να επαληθεύσει ένα συγκεκριμένο μέρος του. Αυτό είναι διαφορετικό απο την ιδιότητα επιλεκτικής απόκρυψης της Κρυπτογράφησης XML. Με την Κρυπτογράφηση XML, τα κρυπτογραφημένα δεδομένα παίρνουν την θέση των αρχικών μέσα στο έγγραφο και είναι εμφανές τι είναι κρυπτογραφημένο. Στις ψηφιακές υπογραφές XML, τα υπογεγραμμένα δεδομένα δεν αντικαθιστούν κάτι. Άντ' αυτού, δημιουργείται μια επιπρόσθετη δομή και προστίθεται μέσα στο έγγραφο, πολύ πιθανόν σε κάποιο άλλο σημείο. Χρειάζεται λοιπόν μια μέθοδος αναγνώρισης των στοιχείων του εγγράφου που έχουν υπογραφεί, καθώς και το ποια υπογραφή αντιστοιχεί σε αυτά. Γι' αυτό το σκοπό χρησιμοποιείται η γλώσσα XPath [XPath]. Η XPath μπορεί να χρησιμοποιηθεί για διάφορες λειτουργίες, αλλά οι Ψηφιακές Υπογραφές XML την χρησιμοποιούν προκειμένου να αναγνωρίσουν τους υπογεγραμμένους κόμβους.
Η γλώσσα XPath (XML Path Language – XPath) είναι μια γλώσσα αναζητήσεων, η οποία ψάχνει, βρίσκει και αναγνωρίζει κομμάτια ενός εγγράφου XML. Αρχικά υλοποιήθηκε για χρήση σε συνδυασμό με την Επεκτάσιμη Γλώσσα Μετασχηματισμών Διαμόρφωσης (Extensible StyleSheet Language Transformations – XSLT) [XSLT]. Το αναγνωριστικό της XPath είναι http://www.w3.org/TR/1999/REC-xpath-1999116. Επίσης επιτελείται εργασία πάνω στο Φίλτρο XPath Ψηφιακής Υπογραφής (XML Signature XPath Filter) [XPathFilter], το οποίο είναι μια εξειδικευμένη έκδοση της XPath για την εφαρμογή της σε ψηφιακές υπογραφές. Η ανάλυση που ακολουθεί αναφέρεται στην έκδοση 1.0 της XPath.
Προκειμένου να λειτουργήσει η XPath, το έγγραφο XML θα πρέπει να είναι οργανωμένο σε δενδρική δομή. Στο Σχήμα 7 έχει μοντελοποιηθεί ένα έγγραφο XML ως ένα τέτοιο δέντρο. Τα περιεχόμενα αυτό το δέντρου είναι παρόμοια αλλά όχι ακριβώς ίδια με το αρχικό έγγραφο XML. Περιέχει τα στοιχεία, σχόλια, χώρους ονομάτων και εντολές

επεξεργασίας του εγγράφου XML. Έχει επίσης έναν κόμβο ρίζα, ο οποίος βρίσκεται λογικά πάνω απο αυτό που θεωρούμε ρίζα του εγγράφου. Αυτό μας επιτρέπει να συμπεριλάβουμε σχόλια που εμφανίζονται πριν απο την αρχή του εγγράφου XML. Παρ' όλα αυτά, δεν περιέχει την δήλωση της XML <?xml version="1.0"?>.



Σχήμα 7-15: Δέντρο XML

Το *μονοπάτι εύρεσης θέσης* αναγνωρίζει έναν κόμβο μέσα στο δέντρο καθορίζοντας διαδρομές για να φτάσουμε στον κόμβο αυτό απο έναν άλλον αρχικό κόμβο. Το μονοπάτι θέσης μπορεί να είναι απόλυτο ή σχετικό. Εάν είναι απόλυτο, ξεκινά απο τον κόμβο ρίζα του εγγράφου. Αν είναι σχετικό, ξεκινά απο έναν άλλο κόμβο, ο οποίος καλείται συναφής κόμβος στο δέντρο.
Απο το σημείο αυτό, η XPath προχωράει μέσα στο δέντρο για να εντοπίσει κόμβους που μας ενδιαφέρουν. Κάθε βήμα αποτελείται απο μια κατεύθυνση, που ονομάζεται άξονας, για αναζήτηση με σημείο αναφοράς τον συναφή κόμβο. Αναζητήσεις μπορεί να κατευθύνονται προς τα πάνω ή προς τα κάτω σε σχέση με τον αρχικό κόμβο και έτσι λαμβάνονται συγκεκριμένες σχέσεις. Για ψηφιακές υπογραφές, οι μόνοι κόμβοι που μας ενδιαφέρουν είναι οι απόγονοι του συναφή κόμβου. Σε κάθε βήμα επίσης γίνεται ένας έλεγχος του κόμβου και εφαρμόζονται λογικοί τελεστές (ίσον, άνισο, μεγαλύτερο από κλπ). Με χρήση των τελεστών αυτών ελέγχεται το περιεχόμενο των κόμβων. Τα αποτελέσματα ενός ελέγχου μπορεί να τροφοδοτηθούν σε έναν επόμενο κ.ο.κ.
Το πρότυπο XPointer [XPointer] αποτελεί επίσης Recommendation του W3C και επεκτείνει το XPath προκειμένου να μπορεί να γίνει χρήση των αναγνωριστικών URI στις αναζητήσεις. Το πιο ενδιαφέρον στοιχείο του Xpointer είναι η *μορφή «απλού ονόματος» (bare name)*. Ένα «απλό όνομα» κάνει αναφορά σε ένα στοιχείο μέσα στο έγγραφο το οποίο έχει ένα χαρακτηριστικό (attribute) ID με το ίδιο όνομα. Στο παράδειγμα που ακολουθεί, το στοιχείο Test έχει ένα χαρακτηριστικό ID με το όνομα referencedNode. Κατ' αυτόν τον τρόπο, η αναφορά στο στοιχείο Test γίνεται μέσω του referencedNode:

Δήλωση στοιχείου Test:

```
<Test ID =”referencedNode”>
…
</Test>
```

Αναφορά στο στοιχείο Test:

```
<signedInfoRef URI=”#referencedNode”>
…
</signedInfoRef >
```

Η μορφή αυτή «απλού ονόματος» του XPointer χρησιμοποιείται μόνο όταν η αναφορά στο referencedNode βρίσκεται μέσα στο ίδιο έγγραφο που βρίσκεται και το Test. Όταν ο κόμβος είναι σε εξωτερικό έγγραφο, τότε το «απλό όνομα» προστίθεται στο URI που αναγνωρίζει το εξωτερικό έγγραφο. Ο XPointer «απλού ονόματος» χρησιμεύει στον προσδιορισμό των υπογεγραμμένων στοιχείων μέσα στο έγγραφο XML.

7.2.2.4 Κανονικοποίηση XML

Όπως προαναφέρθηκε, οι ψηφιακές υπογραφές εξαρτώνται απο την αναπαράσταση των δεδομένων που υπογράφονται. Για παράδειγμα, η προσθήκη ενός κατά τ’ άλλα ασήμαντου χαρακτήρα σε ένα έγγραφο, όπως είναι ένα κενό, θα θεωρηθεί απο μια εφαρμογή επαλήθευσης ως αλλαγή του υπογεγραμμένου εγγράφου και η επαλήθευση της υπογραφής θα αποτύχει. Για να αποφύγουμε τέτοιες καταστάσεις, τα έγγραφα XML μετασχηματίζονται σε μια πρότυπη μορφή προτού υπογραφούν και προτού γίνει η επαλήθευση της υπογραφής.

Η *Κανονικοποιημένη XML (Canonical XML)* [Boyer01] παρέχει έναν πρότυπο τρόπο ώστε να αποφανθεί κάποιος αν δύο έγγραφα είναι όμοια. Καθορίζει κανόνες προκειμένου να μετασχηματιστεί ένα έγγραφο XML σε μια πρότυπη αναπαράσταση. Ένα άλλο έγγραφο με την ίδια κανονικοποιημένη αναπαράσταση θεωρείται όμοιο με το πρώτο. Υπάρχουν δύο παραλλαγές της Κανονικοποιημένης XML. Μια έκδοση δεν περιλαμβάνει σχόλια και το αναγνωριστικό της είναι http://www.w3.org/TR/2001/REC-xml-c14-20010315. Η άλλη έκδοση περιλαμβάνει σχόλια και το αναγνωριστικό της είναι http://www.w3.org/TR/2001/REC-xml-c14-20010315#WithComments.

Ένα δεύτερο πρότυπο, η *Αποκλειστική Κανονικοποίηση XML (Exclusive XML Canonicalization)* [Boyer02] είναι ακόμη υπό προτυποποίηση και καλύπτει την ανάγκη για την υπογραφή κομματιών ενός εγγράφου με τέτοιο τρόπο ώστε το υπογεγραμμένο κομμάτι να μπορεί να εξαχθεί και να τοποθετηθεί σε ένα άλλο έγγραφο. Για παράδειγμα, αν το υπογεγραμμένο κομμάτι του εγγράφου χρησιμοποιεί έναν προκαθορισμένο *χώρο ονομάτων (namespace)*, η Αποκλειστική Κανονικοποίηση XML αντιγράφει τον χώρο ονομάτων στο υπο-κομμάτι του εγγράφου που υπογράφεται.

Η κανονικοποιημένη μορφή ενός εγγράφου είναι αυτή που τελικά υπογράφεται, επειδή οι κανόνες της κανονικοποίησης που έχουν εφαρμοστεί στο ληφθέν έγγραφο XML εξαλείφουν αλλαγές που τυχόν μπορεί να συμβούν κατά τη μεταφορά διαμέσου κόμβων και διατηρούν μια σταθερή μορφή του εγγράφου.

Η Κανονικοποίηση XML μετατρέπει τα δεδομένα χρησιμοποιώντας ένα σταθερό σύνολο χαρακτήρων, το UTF-8. Κανονικοποιεί γραμμές και χαρακτηριστικά, αντικαθιστά αναφορές, αφαιρεί περιττές αναφορές χώρων ονομάτων, προσθέτει προκαθορισμένα χαρακτηριστικά και εφαρμόζει όλες εκείνες τις συναρτήσεις που εξαλείφουν περιττές δομές και ξεκαθαρίζουν διφορούμενες εκφράσεις.

Όταν χρησιμοποιείται με τις ψηφιακές υπογραφές, η κανονικοποίηση πρέπει να μετασχηματίσει τα δεδομένα πριν εκτελεστεί η υπογραφή. Επίσης χρησιμοποιείται για να μετασχηματίσει τα δεδομένα πριν γίνει και η επαλήθευση της υπογραφής. Επειδή η κανονικοποίηση μπορεί να έχει υψηλό κόστος σε υπολογιστικούς πόρους, μόνο τα κομμάτια του εγγράφου που πρόκειται να υπογραφούν κανονικοποιούνται.

7.2.2.5 Μετασχηματισμός Αποκρυπτογράφησης για την Ψηφιακή Υπογραφή XML

Όταν η ψηφιακή υπογραφή συνδυάζεται με κρυπτογράφηση, είναι απαραίτητο να γνωρίζουμε αν η υπογραφή εφαρμόστηκε σε κρυπτογραφημένα δεδομένα ή αν ήταν αναγνώσιμα δεδομένα που υπεγράφησαν και κρυπτογραφήθηκαν στη συνέχεια. Στην πρώτη περίπτωση, τα κρυπτογραφημένα δεδομένα πρέπει να παραμείνουν ως έχουν προκειμένου να επαληθευτεί η υπογραφή. Στην δεύτερη περίπτωση, πρέπει πρώτα να επιτελεστεί η αποκρυπτογράφηση πριν γίνει η επαλήθευση. Ο Μετασχηματισμός Αποκρυπτογράφησης για την Ψηφιακή Υπογραφή XML [Hughes02] είναι μια υπό προτυποποίηση πρόταση του W3C που καθορίζει πώς ο υπογράφων ένα έγγραφο μπορεί να πληροφορήσει τον παραλήπτη που θα επαληθεύσει την υπογραφή, ποια υπογεγραμμένα τμήματα του εγγράφου πρέπει να παραμείνουν κρυπτογραφημένα πριν την επαλήθευση. Όλα τα υπόλοιπα τμήματα πρέπει να αποκρυπτογραφηθούν και μετά ο παραλήπτης να προχωρήσει σε επαλήθευση.
Η διαδικασία δεν είναι ένας ξεχωριστός μετασχηματισμός. Αντίθετα, είναι μια οδηγία στην εφαρμογή επαλήθευσης που χρησιμοποιείται κατά την διάρκεια του μετασχηματισμού αποκρυπτογράφησης. Συνεπώς, ένα στοιχείο που περιλαμβάνει έναν κρυπτογραφημένο κόμβο που εξαιρείται, πρέπει να εισαχθεί ας στοιχείο-παιδί στο στοιχείο του μετασχηματισμού. Ένα παράδειγμα είναι το ακόλουθο:

```
<Transform Algorithm=”http://www.w3.org/2001/04/decrypt#”>
      <Except xmlns=http://www.w3.org/2001/04/decrypt# URI=”#enc1”/>
</Transform>
```

Στο παράδειγμα αυτό, ο κόμβος enc1 κρυπτογραφήθηκε πριν λάβει χώρα η υπογραφή. Άλλα τμήματα του εγγράφου κρυπτογραφήθηκαν μετά την υπογραφή. Για να γίνει η επαλήθευση της υπογραφής, όλα τα άλλα τμήματα πρέπει πρώτα να αποκρυπτογραφηθούν, αλλά ο κόμβος enc1 πρέπει να αφεθεί άθικτος μέχρι να έχει τελειώσει η διαδικασία επαλήθευσης. Αν χρειάζεται, στα πλαίσια της εκάστοτε εφαρμογής, ο κόμβος enc1 μπορεί να αποκρυπτογραφηθεί κατόπιν της ολοκλήρωσης της διαδικασίας επαλήθευσης.

7.2.2.6 Διαδικασία δημιουργίας / επαλήθευσης Υπογραφής

Για τη δημιουργία μιας Ψηφιακής Υπογραφής XML επιτελούνται τα ακόλουθα βήματα:

1. Εφαρμόζονται οι επιλεγμένοι μετασχηματισμοί στα αντικείμενα που πρόκειται να υπογραφούν. Οι μετασχηματισμοί εφαρμόζονται στη σειρά που έχει προδιαγραφεί.
2. Υπολογίζεται η τιμή της συνάρτησης κατακερματισμού στο αποτέλεσμα των μετασχηματισμών.

3. Δημιουργείται ένα στοιχείο αναφοράς που περιλαμβάνει το URI των προς υπογραφή δεδομένων και τα αναγνωριστικά των μετασχηματισμών που χρησιμοποιήθηκαν, τη συνάρτηση κατακερματισμού καθώς επίσης και την τιμή της τελευταίας. Αυτό συμβαίνει αν η υπογραφή καλύπτει περισσότερους απο έναν κόμβους μέσα στο έγγραφο XML.
4. Δημιουργείται το στοιχείο SignedInfo. Περιλαμβάνεται η μέθοδος υπογραφής με ένα στοιχείο SignatureMethod, η μέθοδος κανονικοποίησης με το στοιχείο CanonicalizationMethod και όλες οι αναφορές που δημιουργήθηκαν προηγουμένως.
5. Εφαρμόζεται η μέθοδος κανονικοποίησης στο στοιχείο SignedInfo.
6. Χρησιμοποιούνται οι αλγόριθμοι που καθορίστηκαν στο στοιχείο SignatureMethod για να δημιουργηθεί η υπογραφή. Αυτό συνήθως σημαίνει την εφαρμογή μιας συνάρτησης κατακερματισμού στο κανονικοποιημένο στοιχείο SignedInfo και υπογραφή της τιμής που προκύπτει.
7. Δημιουργείται το στοιχείο Signature που περιλαμβάνει το στοιχείο SignedInfo, το στοιχείο SignatureValue (στο οποίο τοποθετείται η τιμή που προκύπτει απο το βήμα 6), καθώς και τα προαιρετικά στοιχεία KeyInfo και Object.
8. Επισημαίνεται ότι σε κάθε στοιχείο στο οποίο γίνεται αναφορά, ενδέχεται να εφαρμοστεί διαφορετικός αλγόριθμος συνάρτησης κατακερματισμού ή κανονικοποίησης.

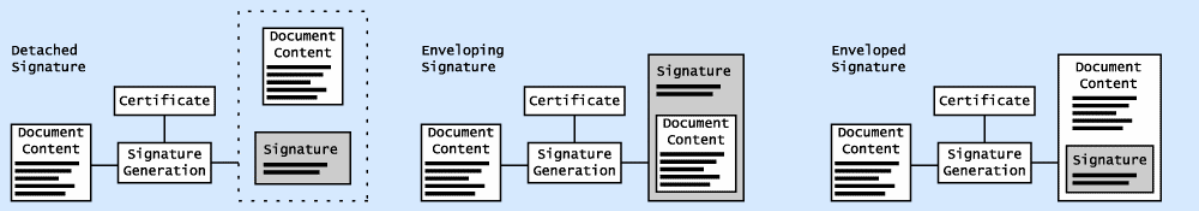
Για να επαληθευθεί μια υπογραφή εκτελούνται οι ακόλουθες διαδικασίες:

1. Κανονικοποιείται το στοιχείο SignedInfo σύμφωνα με την μέθοδο κανονικοποίησης που αναφέρεται στο στοιχείο CanonicalizationMethod (που περιέχεται στο SignedInfo).
2. Για κάθε στοιχείο αναφοράς Reference, λαμβάνονται τα αντικείμενα στα οποία γίνεται η αναφορά.
3. Γίνεται επεξεργασία κάθε αντικειμένου σύμφωνα με τους μετασχηματισμούς που έχουν προδιαγραφεί.
4. Στο αποτέλεσμα εφαρμόζεται η συνάρτηση κατακερματισμού όπως έχει καθοριστεί. Γίνεται σύγκριση του αποτελέσματος με την τιμή που είναι αποθηκευμένη στο αντίστοιχο στοιχείο Reference. Αν οι δύο τιμές δεν είναι ίδιες, η επαλήθευση αποτυγχάνει.
5. Ανακτάται η απαραίτητη πληροφορία για τα κλειδιά που πρέπει να χρησιμοποιηθούν. Μπορεί να περιέχεται σε ένα στοιχείο KeyInfo, ή να είναι ήδη διαθέσιμη με κάποιον άλλο τρόπο.
6. Εφαρμόζεται η μέθοδος υπογραφής με χρήση του κλειδιού και το αποτέλεσμα συγκρίνεται με την τιμή υπογραφής του στοιχείου SignatureValue στο κανονικοποιημένο SignedInfo. Και πάλι αν τα αποτελέσματα δεν είναι τα ίδια, η επαλήθευση αποτυγχάνει.

7.2.2.7 Είδη Ψηφιακής Υπογραφής XML

Το πρότυπο Ψηφιακών Υπογραφών XML ενσωματώνει την λειτουργικότητα των υπογραφών στα έγγραφα μέσα απο τρία ισότιμα σχήματα: περικλειόμενες (enveloped), περικλείουσες (enveloping) και αποσπασμένες (detached) υπογραφές.

Σχηματικά, τα τρία είδη των υπογραφών αναπαρίστανται στο ακόλουθο διάγραμμα:



Σχήμα 7-16: Αποσπασμένες, περικλείουσες και περικλειόμενες υπογραφές XML

Περικλειόμενες υπογραφές: Αποτελούν τον μηχανισμό υπογραφών που είναι πιο κοντά στην ανθρώπινη λογική. Όταν μια ιδιόχειρη υπογραφή μπαίνει σε ένα έγγραφο, το ίδιο το έγγραφο παραμένει εμφανές και χρησιμοποιήσιμο, και η υπογραφή είναι εμφανής (ενσωματωμένη) πάνω του. Το πρότυπο Ψηφιακών Υπογραφών XML επιτρέπει την παραγωγή περικλειόμενων υπογραφών, όπου το ίδιο έγγραφο περικλείει την υπογραφή. Το πλεονέκτημα αυτής της λύσης είναι ότι το έγγραφο παραμένει στην μορφή που ήταν και πριν και μπορεί να υποστεί επεξεργασία. Αυτό επιτρέπει σε συστήματα να συνεχίζουν να το χρησιμοποιούν όπως και πριν, έχοντας τώρα μια επιπλέον παράμετρο ασφάλειας.
Περικλείουσες υπογραφές: Οι περικλείουσες υπογραφές αποτελούν ένα «δοχείο» για το ίδιο το έγγραφο που υπογράφεται. Το βασικό έγγραφο είναι η ίδια η υπογραφή, που περιλαμβάνει το υπογεγραμμένο έγγραφο ως βασικό κομμάτι της. Το κύριο πρόβλημα αυτής της προσέγγισης είναι ότι τα υπογεγραμμένα δεδομένα πρέπει να εξαχθούν απο το «δοχείο» αυτό πριν γίνει η επεξεργασία τους απο μια εφαρμογή. Μια περικλείουσα υπογραφή είναι παρόμοια με σύγχρονα συστήματα παραγωγής υπογραφών όπως αυτά που βασίζονται στο PGP ή το S/MIME.
Αποσπασμένες υπογραφές: Οι αποσπασμένες υπογραφές αφήνουν το υπογεγραμμένο έγγραφο όπως ακριβώς είναι στην αρχική του μορφή, και τα δεδομένα της υπογραφής παρέχονται ξεχωριστά, σε άλλο έγγραφο. Οι δύο οντότητες, έγγραφο και υπογραφή, πρέπει να μεταφέρονται μαζί. Σε όρους συστήματος αρχείων, η υπογραφή αποθηκεύεται σε ένα ξεχωριστό αρχείο. Οι εφαρμογές μπορούν να επεξεργάζονται το αρχείο του υπογεγραμμένου εγγράφου όπως και πριν την παραγωγή της υπογραφής. Η χρήση ενός ξεχωριστού αντικειμένου για την υπογραφή μειονεκτεί στο ότι αυξάνει την πολυπλοκότητα της ενσωμάτωσης της ασφάλειας που προσφέρουν στο σύστημα λόγω του ότι πρέπει κάθε στιγμή να μεταφέρονται δύο διαφορετικά αρχεία.

7.2.2.8 Παράδειγμα

Το απόσπασμα κειμένου XML που ακολουθεί αποτελεί ένα παράδειγμα μιας αποσπασμένης Υπογραφής XML.

```
<Signature xmlns=”http://www.w3.org/2000/09/xmldsig#”>
      <SignedInfo>
         <CanonicalizationMethod Algorithm=”http://www.w3.org/TR/2001/RECxml-
c14n-20010315”/>
         <SignatureMethod
Algorithm=”http://www.w3.org/2000/09/xmldsig#dsasha1”/>
         <Reference URI=”http://www.mycompany.com/order/”>
            <Transforms>
```

```
                <Transform Algorithm="http://www.w3.org/TR/2001/REC-xmlc14n-
20010315"/>
             </Transforms>
             <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
          </Reference>
       </SignedInfo>
       <SignatureValue>MC0CFFrVLtRlk=...</SignatureValue>
       <KeyInfo>
          <KeyValue>
            <DSAKeyValue>
              <P>...</P>
              <Q>...</Q>
              <G>...</G>
              <Y>...</Y>
            </DSAKeyValue>
            </KeyValue>
       </KeyInfo>
</Signature>
```

Σχήμα 7-17 : Παράδειγμα αποσπασμένης υπογραφής XML με DSA

Το στοιχείο SignatureMethod καθορίζει τον αλγόριθμο της υπογραφής και της συνάρτησης κατακερματισμού που στην προκειμένη περίπτωση είναι οι DSA και SHA-1 αντιστοίχως. Καθορίζεται επίσης ο μετασχηματισμός κανονικοποίησης. Τα δεδομένα που υπογράφονται αναγνωρίζονται απο το χαρακτηριστικό URI του στοιχείου αναφοράς Reference. Στο παράδειγμα υπάρχει μόνο ένα στοιχείο Reference και αναγνωρίζει ένα άλλο έγγραφο (ανεξάρτητο) που ονομάζεται order. Η συνάρτηση κατακερματισμού και ο μετασχηματισμός που εφαρμόζονται, περιέχονται σε στοιχεία παιδιά του στοιχείου αναφοράς. Επιπρόσθετα, το δημόσιο κλειδί DSA που θα χρησιμοποιηθεί για να επαληθευτεί η υπογραφή, είναι επίσης παρόν. Τονίζεται ότι το απλό αυτό παράδειγμα χρησιμοποιεί μόνο το κλειδί για την επαλήθευση και όχι ένα ολόκληρο πιστοποιητικό. Με τον τρόπο αυτό επιτυγχάνεται η ελάχιστη ασφάλεια για την υπογραφή, αφού ο παραλήπτης του μηνύματος δεν έχει κάποιο τρόπο να επιβεβαιώσει ότι ο υπογράφων είναι κάποιο πρόσωπο που εμπιστεύεται. Στην περίπτωση που η χρήση μιας Υποδομής Δημοσίου Κλειδιού θεωρείται πολύπλοκη και δαπανηρή, ένας καλύτερος τρόπος χειρισμού του συγκεκριμένου μηνύματος είναι να έχει προηγηθεί η ανταλλαγή του κλειδιού με τον παραλήπτη και στο μήνυμα να υπάρχει μόνο μια αναφορά στο κλειδί.

7.2.3 Προηγμένες Ηλεκτρονικές Υπογραφές XML – XAdES

7.2.3.1 Τα πρότυπα ETSI TS 101 733 και ETSI 101 903

Η Ευρωπαϊκή Οδηγία για το κοινοτικό πλαίσιο Ηλεκτρονικών Υπογραφών, καθορίζει την ηλεκτρονική υπογραφή ως: «δεδομένα σε ηλεκτρονική μορφή που είναι ενσωματωμένα ή είναι λογικά συσχετισμένα με άλλα ηλεκτρονικά δεδομένα και εξυπηρετούν ως ένα μέσο αυθεντικοποίησης.»
Το πρότυπο του ETSI TS 101 733 [ETSI101733], δημιουργήθηκε με σκοπό να καλύψει την παραγωγή και επαλήθευση ηλεκτρονικών υπογραφών για διάφορους τύπους συναλλαγών, συμπεριλαμβανομένων των εμπορικών συναλλαγών (για παράδειγμα αγορά, δημιουργία συμβολαίου ή τιμολογίων). Το πρότυπο μπορεί να χρησιμοποιηθεί για οποιαδήποτε συναλλαγή ανάμεσα σε έναν ιδιώτη και μια εταιρία, ανάμεσα σε δύο εταιρίες, έναν ιδιώτη και έναν δημόσιο οργανισμό κλπ.

Μια ηλεκτρονική υπογραφή που παράγεται σύμφωνα με το ETSI TS 101 733, παρέχει αποδεικτικά στοιχεία τα οποία μπορούν να υποστούν επεξεργασία προκειμένου να είναι κάποιος σίγουρος ότι μια συγκεκριμένη δέσμευση έχει γίνει αποδεκτή κάτω από μια δεδομένη *πολιτική υπογραφής*, σε μια δεδομένη χρονική στιγμή, από έναν υπογράφοντα με δεδομένο αναγνωριστικό όπως είναι ένα όνομα ή ένα ψευδώνυμο και προαιρετικά ένα ρόλο. Η πολιτική υπογραφής καθορίζει τις τεχνικές και διαδικαστικές απαιτήσεις για τη δημιουργία και επαλήθευση της υπογραφής προκειμένου να καλύπτεται μια συγκεκριμένη επιχειρηματική ανάγκη. Το υποκείμενο νομικό πλαίσιο μπορεί να αναγνωρίζει μια συγκεκριμένη πολιτική υπογραφής ως κατάλληλη γι' αυτό. Για παράδειγμα, μια συγκεκριμένη πολιτική υπογραφής μπορεί να αναγνωρίζεται από ένα δικαστήριο ως κατάλληλη για να καλύψει της ανάγκες της Ευρωπαϊκής Οδηγίας για το ηλεκτρονικό εμπόριο.
Το πρότυπο ETSI TS 101 733 καθορίζει τη μορφή των προηγμένων ηλεκτρονικών υπογραφών που παραμένουν έγκυρες για μεγάλα χρονικά διαστήματα, συμμορφώνονται με την Ευρωπαϊκή Οδηγία και ενσωματώνουν επιπρόσθετη χρήσιμη πληροφορία για συχνές και συνηθισμένες περιπτώσεις. Επί του παρόντος, το πρότυπο χρησιμοποιεί την Abstract Syntax Notation 1 (ASN.1) [ASN.1] και βασίζεται στην δομή που καθορίζεται στο RFC 2630.
Όπως παρουσιάστηκε στο προηγούμενο κεφάλαιο, η Ομάδα Εργασίας του W3C για τις υπογραφές XML, έχει παράγει μια σύνταξη για τις Ψηφιακές Υπογραφές XML. Η σύνταξη αυτή παρέχει την βασική λειτουργικότητα για την ταυτόχρονη υπογραφή αρκετών αντικειμένων δεδομένων. Παρέχει επίσης τα βασικά μέσα για την ενσωμάτωση οποιασδήποτε επιπρόσθετης χαρακτηρίζουσας πληροφορίας.
Το πρότυπο ETSI TS 101 903 [XAdES02] με τη σειρά του, καθορίζει μορφές εγγράφων XML για προηγμένες ηλεκτρονικές υπογραφές που παραμένουν έγκυρες μετά από μεγάλες χρονικές περιόδους, συμμορφώνονται με την Ευρωπαϊκή Οδηγία και ενσωματώνουν επιπρόσθετη χρήσιμη πληροφορία για συχνές και συνηθισμένες περιπτώσεις, υλοποιώντας τα εξής:

- ✓ Προτείνοντας τους ορισμούς ενός Σχήματος XML για νέους τύπους XML που θα μπορούν να περιέχουν την πληροφορία για να καλύψουν την απαίτηση για μακροπρόθεσμη εγκυρότητα καθώς και τις απαιτήσεις που επιβάλλονται από σύγχρονες επιχειρηματικές διαδικασίες και την Ευρωπαϊκή Οδηγία. Οι υπογραφές αυτές χτίζονται πάνω στο πρότυπο των Ψηφιακών Υπογραφών XML με την προσθήκη της παραπάνω πληροφορίας χρησιμοποιώντας το στοιχείο XML Object, όπως αυτό ορίστηκε στο πρότυπο των Ψηφιακών Υπογραφών XML.
- ✓ Καθορίζοντας τους μηχανισμούς που χρησιμοποιούνται για την παραγωγή της προαναφερθείσας επιπρόσθετης χαρακτηρίζουσας πληροφορίας.

Το πρότυπο ETSI TS 101 903 (γνωστό και ως Προηγμένες Ψηφιακές Υπογραφές XML – XML Advanced Electronic Signatures ή XAdES), καθορίζει δύο βασικούς τύπους ιδιοτήτων: *υπογεγραμμένες ιδιότητες (signed properties)* και *μη υπογεγραμμένες ιδιότητες (unsigned properties)*. Οι πρώτες είναι πρόσθετα αντικείμενα δεδομένων που επίσης διασφαλίζονται από την υπογραφή που παράγεται από τον υπογράφοντα στο στοιχείο SignedInfo (βλ. και παράγραφο 2.2.2.1), κάτι που υπονοεί ότι ο υπογράφων έχει αυτά τα αντικείμενα δεδομένων, εφαρμόζει μια κρυπτογραφική συνάρτηση κατακερματισμού

πάνω σε όλα και παράγει ένα αντίστοιχο στοιχείο αναφοράς Reference. Οι μη υπογεγραμμένες ιδιότητες είναι αντικείμενα δεδομένων που προστίθενται από τον υπογράφοντα, από τον επαληθεύοντα την υπογραφή ή άλλες οντότητες μετά την παραγωγή της υπογραφής. Δεν διασφαλίζονται από την υπογραφή στο στοιχείο Signature (που παράγεται από τον υπογράφοντα). Παρ' όλα αυτά, υπάρχει το ενδεχόμενο να υπογραφούν από άλλες οντότητες (χρονοσφραγίδες, πρόσθετες υπογραφές, πιστοποιητικά και λίστες ανάκλησης πιστοποιητικών ΛΑΣ είναι πιθανά περιεχόμενα των μη υπογεγραμμένων ιδιοτήτων).
Η επαλήθευση μια προηγμένης ηλεκτρονικής υπογραφής βάσει του XAdES απαιτεί:

- ✓ Μια προηγμένη ηλεκτρονική υπογραφή που έχει δημιουργηθεί βάσει του προτύπου Ψηφιακών Υπογραφών XML του W3C όπως περιγράφεται στο κεφάλαιο 2.2.2 με την ενσωμάτωση της επιπρόσθετης χαρακτηρίζουσας πληροφορίας. Αυτή είναι:
  - Οι αναφορές στα **υπογεγραμμένα αντικείμενα**.
  - Οι **υπογεγραμμένες ιδιότητες** (που παρέχονται από τον υπογράφοντα).
  - Η ίδια η **υπογραφή** όπως καθορίζεται στο πρότυπο Ψηφιακών Υπογραφών XML.
- ✓ Δεδομένα επαλήθευσης, που αποτελούν τα επιπρόσθετα δεδομένα που απαιτούνται για την επαλήθευση της ηλεκτρονικής υπογραφής. Περιλαμβάνουν:
  - Ψηφιακά πιστοποιητικά.
  - Πληροφορία ανάκλησης πιστοποιητικών.
  - Χρονοσφραγίδες από Αρχές Χρονοσφράγισης.

Τα **υπογεγραμμένα αντικείμενα** αποτελούν τα έγγραφα, στοιχεία, κλπ που ο χρήστης ήθελε να υπογράψει.
Οι **υπογεγραμμένες ιδιότητες** περιλαμβάνουν οποιαδήποτε επιπρόσθετη πληροφορία που θα υπογραφεί από τον χρήστη προκειμένου να είναι συμβατή με την ακολουθούμενη πολιτική υπογραφής ή το ίδιο το πρότυπο (π.χ. τον χρόνο παραγωγής της υπογραφής).
Τα **δεδομένα επαλήθευσης** ενδέχεται να συλλέγονται είτε από τον υπογράφοντα ή από τον επαληθεύοντα ή και τους δύο και θα καλύπτουν τις απαιτήσεις της πολιτικής υπογραφής. Τα δεδομένα αυτά περιλαμβάνουν πιστοποιητικά ΑΠ και πληροφορία κατάστασης ανάκλησης πιστοποιητικών με τη μορφή ΛΑΠ ή πληροφορία όπως λαμβάνεται από μια online υπηρεσία (π.χ. μέσω των πρωτοκόλλων OCSP (Online Certificate Status Protocol) [Myers99] ή SCVP (Standard Certificate Validation Protocol) [Freeman06]). Επιπρόσθετα δεδομένα είναι χρονοσφραγίδες. Από το πρότυπο απαιτείται ως ελάχιστο, ότι είτε ο υπογράφοντας είτε ο επαληθεύων ζητούν μια χρονοσφραγίδα πάνω στα δεδομένα της υπογραφής.

7.2.3.2 Μορφή / Δομή

Το πρότυπο καθορίζει έξι μορφές προηγμένων ηλεκτρονικών υπογραφών XML με αυξανόμενο επίπεδο πολυπλοκότητας.
Οι τρεις πρώτες πιο απλές μορφές είναι:

- ✓ Η *Προηγμένη Ηλεκτρονική Υπογραφή XML (XML Advanced Electronic Signature – XAdES)*.
- ✓ Η *XAdES με Χρονοσφραγίδα (XAdES with Time-Stamp ή XAdES-T)*.

- ✓ Η *XAdES με πλήρη Δεδομένα Επαλήθευσης (XAdES with Complete Validation Data ή XAdES-C)*.

Οι δύο επόμενες μορφές καλύπτουν ένα πιο αυξημένο σύνολο απαιτήσεων και ονομάζονται *XAdES-X* και *XAdES-X-L* και θα περιγραφούν συνοπτικά στη συνέχεια. Το τελευταίο είδος ονομάζεται *XAdES-A* και αποτελεί μια μορφή για την ασφαλή αποθήκευση υπογραφών κατά έναν τρόπο ώστε να προστατεύονται αν η κρυπτογραφική πληροφορία αποδυναμωθεί (π.χ. με το σπάσιμο ενός αλγορίθμου κλπ.).

7.2.3.2.1 Προηγμένη Ηλεκτρονική Υπογραφή XML – XAdES

Η σχηματική αναπαράσταση της δομή μιας υπογραφής XAdES είναι η ακόλουθη:

Σχήμα 7-18: Προηγμένη Ηλεκτρονική Υπογραφή XML - XAdES

Όπως είναι φανερό, τα βασικά στοιχεία της υπογραφής SignedInfo, Signature και KeyInfo είναι όπως έχουν περιγραφεί στο κεφάλαιο των Ψηφιακών Υπογραφών XML. Η υπογραφή XAdES προσθέτει τα στοιχεία SignedProperties και UnsignedProperties για να περιληφθούν οι υπογεγραμμένες και μη υπογεγραμμένες πληροφορίες σύμφωνα με το πρότυπο.
Συνοπτικά τα στοιχεία που απαρτίζουν τις υπογεγραμμένες ιδιότητες είναι τα εξής:

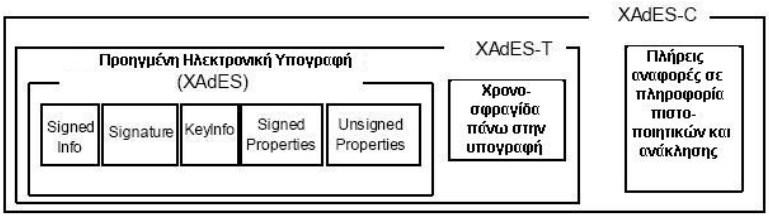
- ✓ Ο χρόνος υπογραφής (στοιχείο SigningTime).
- ✓ Το πιστοποιητικό υπογραφής (στοιχείο SigningCertificate).
- ✓ Το αναγνωριστικό της χρησιμοποιούμενης πολιτικής υπογραφής (στοιχείο SignaturePolicyIdentifier).
- ✓ Τα στοιχεία του τόπου παραγωγής της υπογραφής (στοιχείο SignatureProductionPlace).
- ✓ Ο ρόλος του υπογράφοντα (στοιχείο SingerRole).
- ✓ Μια χρονοσφραγίδα πάνω σε όλες τις αναφορές των υπογεγραμμένων δεδομένων (στοιχείο AllDataObjectsTimeStamp) ή εναλλακτικά μια χρονοσφραγίδα πάνω σε αναφορές ορισμένων από τα υπογεγραμμένα δεδομένα (IndividualDataObjectsTimeStamp).
- ✓ Τα χαρακτηριστικά των υπογεγραμμένων δεδομένων (στοιχείο DataObjectFormat).
- ✓ Τον τύπο της δέσμευσης (στοιχείο CommitmentTypeIndication).

Οι μη υπογεγραμμένες ιδιότητες περιλαμβάνουν μια υπογραφή αντισυμβαλλόμενου (στοιχείο CounterSignature).

Η μορφή XAdES καλύπτει τις νομικές προϋποθέσεις για προηγμένες ηλεκτρονικές υπογραφές όπως καθορίζονται στην Οδηγία της Ευρωπαϊκής Επιτροπής για ηλεκτρονικές υπογραφές. Παρέχει βασική αυθεντικοποίηση και προστασία ακεραιότητας και μπορεί να δημιουργηθεί χωρίς την πρόσβαση σε online υπηρεσίες Χρονοσφράγισης. Παρ' όλα αυτά χωρίς την προσθήκη μιας χρονοσφραγίδας στην υπογραφή ή ένα άλλο ασφαλές αρχείο χρόνου, η ηλεκτρονική υπογραφή δεν προστατεύει ενάντια στην απειλή ο υπογράφων αργότερα να αρνηθεί ότι δημιούργησε την υπογραφή, δηλαδή δεν παρέχει την μη-άρνηση συμμετοχής (non-repudiation).

7.2.3.2.2 XAdES με Χρονοσφραγίδα - XAdES-T και XAdES με Πλήρη Δεδομένα Επαλήθευσης – XAdES-C

Η Προηγμένη Ηλεκτρονική Υπογραφή με Χρονοσφραγίδα XAdES-T προσθέτει στη XAdES μια χρονοσφραγίδα, προκειμένου ο υπογράφων να κάνει τα πρώτα βήματα για την παροχή μακροπρόθεσμης επαλήθευσης. Αυτή η μορφή ή κάποιο άλλο στοιχείο χρόνου θα πρέπει να δημιουργείται κοντά στη χρονική στιγμή της παραγωγής της υπογραφής για να παρασχεθεί προστασία από άρνηση δημιουργίας της.
Η Προηγμένη Ηλεκτρονική Υπογραφή με Πλήρη Δεδομένα Επαλήθευσης – XAdES-C προσθέτει στην XAdES-T τις αναφορές σε ένα σύνολο δεδομένων που υποστηρίζουν την εγκυρότητα της υπογραφής, για παράδειγμα τις αναφορές σε πιστοποιητικά και την αντίστοιχη πληροφορία ανάκλησης των πιστοποιητικών αν υπάρχει. Σημειώνεται ότι στην υπογραφή ενσωματώνονται μόνο **αναφορές** στην πληροφορία και όχι το ίδιο το περιεχόμενο της πληροφορίας, που θα ήταν πολύ μεγαλύτερο.
Η σχηματική αναπαράσταση της XAdES-T και της XAdES-C είναι η ακόλουθη:



Σχήμα 7-19: XAdES-T και XAdES-C

Η XAdES-T όπως προαναφέρθηκε θα πρέπει να δημιουργείται κοντά στο χρονικό σημείο που δημιουργήθηκε η XAdES για προστασία από άρνηση συμμετοχής στη δημιουργία της αργότερα. Στο χρονικό αυτό σημείο ενδέχεται να μην είναι διαθέσιμη ακόμη η πληροφορία για συνολική επαλήθευση της υπογραφής, ή να είναι διαθέσιμο κάποιο μέρος της με το οποίο μπορούν να γίνουν κάποιοι αρχικοί έλεγχοι.
Και για τις δύο περιπτώσεις υπογραφών, αν ο υπογράφων δημιουργήσει μόνο την βασική XAdES υπογραφή, ο επαληθεύων την υπογραφή θα πρέπει να δημιουργήσει τις XAdES-T και XAdES-C μορφές με την πρώτη ευκαιρία. Αυτό θα παρέχει τα επιπρόσθετα δεδομένα τουλάχιστον την στιγμή που πρώτη φορά η υπογραφή επαληθεύεται και η οποία θεωρητικά είναι κοντά στην στιγμή της δημιουργίας της.

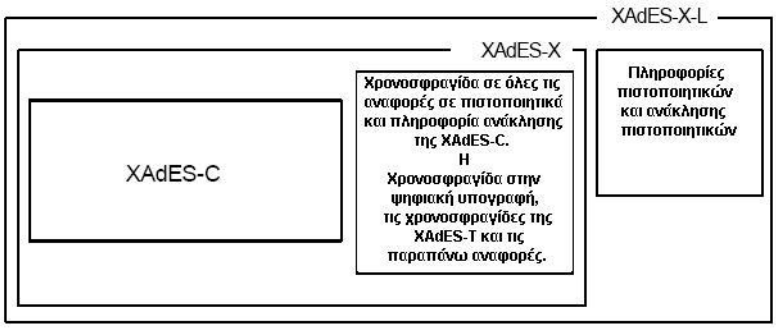
7.2.3.2.3 Επεκτάσιμες μορφές XadES

Η πρώτη επεκτάσιμη μορφή XAdES είναι η XAdES-X ή XAdES με Εκτεταμένα Δεδομένα Επαλήθευσης (XAdES with eXtended Validation Data).

Οι μορφές αυτές δημιουργούνται στις παρακάτω περιπτώσεις:

- ✓ Αν υπάρχει κίνδυνος ότι κάποια από τα κλειδιά που χρησιμοποιούνται στην αλυσίδα πιστοποιητικών ή στην πληροφορία ανάκλησης πιστοποιητικών έχουν αποκαλυφθεί. Η περίπτωση ενός σπασμένου αλγορίθμου είναι διαφορετική και καλύπτεται στη συνέχεια από την μορφή XAdES-A. Για την μορφή XAdES-X είναι απαραίτητο να χρονοσφραγισθούν όλες οι αναφορές σε πιστοποιητικά και πληροφορία ανάκλησης πιστοποιητικών που περιέχονται στη XAdES-C. Εναλλακτικά, η χρονοσφραγίδα μπορεί να εφαρμοστεί στην ψηφιακή υπογραφή (το στοιχείο Signature), τις χρονοσφραγίδες που εμφανίζονται στην μορφή XAdES-T και τις παραπάνω αναφορές.
- ✓ Αν τα δεδομένα πιστοποιητικών και η πληροφορία ανάκλησης πιστοποιητικών δεν αποθηκεύονται για μεγάλο χρονικό διάστημα, τότε επιβάλλεται να προστεθούν στην ίδια την υπογραφή. Έτσι προκύπτει η XAdES-X-L μορφή.

Σχηματικά αναπαρίστανται στο ακόλουθο σχήμα:

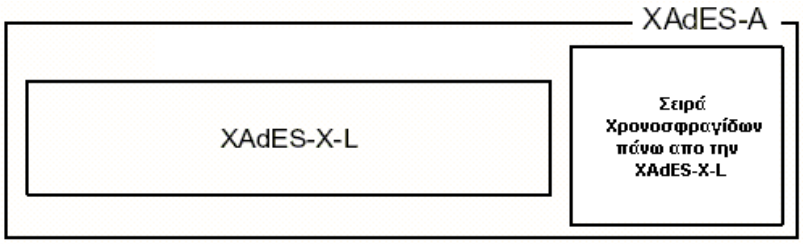


Σχήμα 7-20: XAdES-X και XAdES-X-L

Οι προδιαγραφές του προτύπου καθορίζουν ότι η χρονοσφραγίδα πάνω στις αναφορές των πιστοποιητικών και πληροφορίας ανάκλησης μπορεί να παραληφθεί και να προστεθούν τα ίδια τα δεδομένα των πιστοποιητικών και ανάκλησης.
Η μορφή XAdES-X-L παράγεται επί της ουσίας με την ενσωμάτωση των δεδομένων αυτών ως στοιχεία XML αφότου μετασχηματιστούν κατά base64, εφόσον είναι δυαδικά δεδομένα τύπου ΛΑΠ ή απάντησης ενός εξυπηρετητή OCSP.

7.2.3.2.4 Μορφή XAdES Αρχειοθέτησης Δεδομένων Επαλήθευσης

Η μορφή Αρχειοθέτησης Δεδομένων Επαλήθευσης XAdES-A (Archive Validation Data) παρουσιάζεται στο ακόλουθο σχήμα:



Σχήμα 7-21: XAdES-A

Προτού αλγόριθμοι, κλειδιά και τα υπόλοιπα κρυπτογραφικά δεδομένα που έχουν χρησιμοποιηθεί στη μορφή XAdES-C γίνουν παρωχημένα ή αδύναμα, η μορφή XAdES-X-L θα πρέπει να χρονοσφραγηθεί. Εάν είναι δυνατόν, αυτό θα πρέπει να γίνει με την εφαρμογή ισχυρότερων αλγορίθμων (ή μεγαλύτερα μήκη κλειδιών) από τα ήδη χρησιμοποιημένα για την παραγωγή των αρχικών χρονοσφραγίδων. Τα επιπρόσθετα αυτά δεδομένα και η χρονοσφραγίδα ονομάζονται μορφή Αρχειοθέτησης Δεδομένων Επαλήθευσης ή XAdES-A Η διαδικασία αυτή μπορεί να επαναλαμβάνεται κάθε φορά που η προστασία που χρησιμοποιήθηκε για την χρονοσφράγιση της προηγούμενης XAdES-A αποδυναμώνεται. Συνεπώς η XAdES-A μπορεί να φέρει πολλαπλές ενσωματωμένες χρονοσφραγίδες. Η υποστήριξη μια υλοποίησης του XAdES για την μορφή XAdES-A είναι προαιρετική.

7.3 Πρότυπα Υπηρεσιών Ιστού

7.3.1 Το πρότυπο SOAP

7.3.1.1 Εισαγωγή

Το *SOAP* [Mitra03] (που αρχικά αποτελούσε ακρωνύμιο των όρων Απλό Πρωτόκολλο Πρόσβασης σε Αντικείμενα – Simple Object Access Protocol, αλλά στη συνέχεια παρέμεινε στην βιβλιογραφία απλά ως SOAP), είναι ένα πρωτόκολλο ανταλλαγής μηνυμάτων βασισμένο στην XML. Δημιουργήθηκε για να δώσει λύση σε προβλήματα διαλειτουργικότητας ανάμεσα σε κατανεμημένες εφαρμογές. Οι προδιαγραφές του μεγάλωσαν τα τελευταία τέσσερα χρόνια και αυτή τη στιγμή βρίσκεται στην έκδοση 1.2. Οι προδιαγραφές του επίσης έχουν κατατεθεί στο W3C προκειμένου να αποτελέσει πρότυπο παρόμοια με το HTTP και την XML.
Το βασικό χαρακτηριστικό του SOAP είναι η απλότητά του. Είναι σχετικά εύκολο για κάποιον να υλοποιήσει μια απλή εφαρμογή που να υποστηρίζει το SOAP χρησιμοποιώντας μια απο τις διαδεδομένες γλώσσες προγραμματισμού και να έχει πρόσβαση σε μια άλλη εφαρμογή εξυπηρετητή που υποστηρίζει SOAP και είναι γραμμένη σε μια άλλη γλώσσα.

7.3.1.2 Σκοπός

Το SOAP είναι μια μέθοδος για την αποστολή και λήψη πληροφορίας πάνω απο ένα δίκτυο, όπως το διαδίκτυο, με χρήση της XML. Υπάρχουν διαφορετικοί τρόποι για να χρησιμοποιήσει κάποιος το SOAP. Στην πιο απλή μορφή του, μπορεί κάποιος να χρησιμοποιήσει έναν συνηθισμένο φυλλομετρητή ιστού για να αποκτήσει πρόσβαση στον εξυπηρετητή ιστού μιας δικτυακής τοποθεσίας που προσφέρει μια διεπαφή για την κλήση αντικειμένων. Η τεχνική λύση που υποστηρίζει το SOAP είναι κρυμμένη πίσω απο την διεπαφή αυτή, οπότε ο φυλλομετρητής δεν χρειάζεται να γνωρίζει πως να χρησιμοποιεί άμεσα το ίδιο το πρωτόκολλο SOAP.
Ένας εναλλακτικός τρόπος χρήσης του SOAP είναι η ενσωμάτωσή του σε μια εφαρμογή η οποία χρησιμοποιεί μηνύματα XML για να αποστείλει πληροφορία σε έναν εξυπηρετητή που περιέχει αντικείμενα που χρησιμοποιούνται απο την εφαρμογή. Η εφαρμογή αποτελεί ένα «κέλυφος» που βρίσκεται στον τοπικό υπολογιστή και επιτρέπει

τις κλήσεις στον εξυπηρετητή όπου βρίσκονται τα αντικείμενα και τα δεδομένα. Κατ' αυτόν τον τρόπο, οι εφαρμογές «πελάτες» δεν χρειάζεται να τροποποιούνται κάθε φορά που γίνονται αλλαγές στα αντικείμενα. Επίσης έτσι εξασφαλίζεται ότι τα δεδομένα αποθηκεύονται σε ένα ασφαλές περιβάλλον και ελέγχεται η πρόσβαση σε αυτά.
Το SOAP έχει σχεδιαστεί με τρεις βασικούς σχεδιαστικούς στόχους:

- Να παρέχει ένα προτυποποιημένο πρωτόκολλο κλήσης αντικειμένων βασισμένο σε άλλα πρότυπα του Διαδικτύου, χρησιμοποιώντας το HTTP για μεταφορά και την XML για την δόμηση των δεδομένων.
- Να αποτελεί ένα επεκτάσιμο πρωτόκολλο και μορφή δεδομένων μηνυμάτων που μπορεί να εξελιχθεί.
- Να είναι απλό.

Ο πρώτος στόχος κάνει το SOAP ευέλικτο ώστε να μπορεί να ενσωματωθεί σε συστήματα και να υποστηριχθούν οι Υπηρεσίες Ιστού που έχουν υλοποιηθεί σε διαφορετικές πλατφόρμες και με διαφορετικές γλώσσες προγραμματισμού. Το οικοδόμημα των Υπηρεσιών Ιστού βασίζεται στην ικανότητα ακριβώς της αποστολής και λήψης μηνυμάτων σε μια προτυποποιημένη μορφή κατανοητή απο όλα τα συστήματα.

7.3.1.3 Μορφή / Δομή

Μια διαδικασία, για παράδειγμα, που επιδεικνύει την δημιουργία και αποστολή ενός σύγχρονου μηνύματος SOAP περιλαμβάνει πέντε βήματα:

1. Δημιουργία της σύνδεσης SOAP.
2. Δημιουργία του μηνύματος SOAP.
3. Συμπλήρωση του μηνύματος με δεδομένα.
4. Αποστολή του μηνύματος.
5. Λήψη της απάντησης.

Οι κανόνες κωδικοποίησης που ορίζονται για διάφορους τύπους δεδομένων μπορούν να σειριοποιηθούν με χρήση *αιτήσεων SOAP (SOAP requests)*. Οι προδιαγραφές 1.1 του SOAP βασίζουν την κωδικοποίηση δεδομένων σε δομές Σχημάτων XML και τύπους δεδομένων Σχημάτων XML, αλλά επιτρέπουν και κωδικοποιήσεις όπως η RDF [Klyne04]. Οι υποστηριζόμενοι τύποι περιλαμβάνουν απλούς τύπους όπως είναι οι συμβολοακολουθίες (strings), καθώς και πολύπλοκους τύπους όπως είναι οι δομές (structures) και οι πίνακες (arrays). Οι προδιαγραφές επίσης περιγράφουν μια σύμβαση για την υλοποίηση αλληλεπιδράσεων RPC με χρήση της XML. Τα μηνύματα SOAP μπορούν να αποσταλούν πάνω απο οποιοδήποτε πρωτόκολλο μεταφοράς συμπεριλαμβανομένων των HTTP(S), SMTP [Postel82] και FTP [Postel85].
Ένα μήνυμα SOAP περιέχει τρία βασικά τμήματα:

- έναν *φάκελο (envelope)*
- μια *επικεφαλίδα (header)* για την προσθήκη στο μήνυμα SOAP χαρακτηριστικών που εξαρτώνται απο την εκάστοτε εφαρμογή (για παράδειγμα πληροφορίες αυθεντικοποίησης)

- ένα *σώμα (body)* που περιέχει την πληροφορία που ενδιαφέρει τον παραλήπτη του μηνύματος

Το Σχήμα 7-22 επιδεικνύει πως θα μπορούσε να γραφτεί σε SOAP ένα παράδειγμα αίτησης και απάντησης απο μια υπηρεσία:

Request

```
POST /StockQuote HTTP/1.1
Host: www.stockquoteserver.com
Content-Type: text/xml
Content-Length: nnnn
SOAPAction: "Some-URI"

<SOAP:Envelope
xmlns:SOAP="urn:schemas.xmlsoap.org:soap.v1">
<SOAP:Header>
       <t:Transaction xmlns:t="URI"
mustUnderstand="1">5</t:Transaction>
     </SOAP:Header>
     <SOAP:Body>
          <m:GetLastTradePrice
xmlns:m="URI">
               <symbol>DIS</symbol>
          </m:GetLastTradePrice>
     </SOAP:Body>
</SOAP:Envelope>
```

Response

```
HTTP/1.1 200 OK
Content-Type: text/xml
Content-Length: nnnn

<SOAP:Envelope
xmlns:SOAP="urn:schemas.xmlsoap.org:soap.v1">
    <SOAP:Header>
       <t:Transaction xmlns:t="URI"
xsi-type="xsd:int"
mustUnderstand="=">5</t:Transaction>
</SOAP:Header>
<SOAP:Body>
<m:GetLastTradePriceResponse
xmlns:m="URI">
<return>34.5</return>
</m:GetLastTradePriceResponse>
</SOAP:Body>
</SOAP:Envelope>
```

Σχήμα 7-22: Ένα παράδειγμα αίτησης και απάντησης με SOAP

Ένας εξυπηρετητής εφαρμογών που λαμβάνει ένα μήνυμα SOAP πρέπει να αναγνωρίσει όλα τα κομμάτια που περιέχει, να επαληθεύσει ότι είναι ολοκληρωμένα και να τα επεξεργαστεί. Επειδή ένα μήνυμα SOAP μπορεί να ταξιδέψει διαμέσου πολλών ενδιάμεσων σταθμών, ένα *χαρακτηριστικό δράστη (actor attribute)* χρησιμοποιείται για να υποδειχθεί ο τελικός παραλήπτης του μηνύματος. Οι προδιαγραφές επίσης καθορίζουν ένα *χαρακτηριστικό υποχρεωτικής κατανόησης (mustUnderstand attribute)*, το οποίο καθορίζει εάν μια συγκεκριμένη καταχώρηση στην επικεφαλίδα πρέπει να είναι κατανοητή και να υποστεί επεξεργασία από τον παραλήπτη.

7.3.1.4 Ανοιχτά Θέματα

Παρόλο που έχουν γίνει αρκετές προσπάθειες γύρω απο την υλοποίηση του SOAP, υπάρχουν ακόμη ανοιχτά θέματα που πρέπει να μελετηθούν, διαφορετικά μια αλόγιστη χρήση του SOAP θα μπορούσε να οδηγήσει σε πτώση της απόδοσης και ταχύτητας ενός συστήματος:

- Είναι ακριβή η δόμηση και αποδόμηση ενός μηνύματος: η χρήση των κανόνων κωδικοποίησης του SOAP έχουν υπολογιστικό κόστος μεγαλύτερο απο για παράδειγμα αυτήν του RMI/IIOP. Το SOAP είναι ένα πρωτόκολλο βασισμένο στο ASCII οπότε τα δεδομένα πρέπει να μετατρέπονται σε συμβολοακολουθίες αντί να μεταδίδονται στην δυαδική μορφή τους. Αυτή η διαδικασία μετατροπής καταναλώνει υπολογιστική ισχύ.
- Το SOAP απαιτεί περισσότερη μνήμη: το χτίσιμο συμβολοακολουθιών XML και η ανάλυσή τους χρησιμοποιεί περισσότερη μνήμη και πιθανώς παράγει και περισσότερα «σκουπίδια» στη μνήμη.

- Απαιτεί περισσότερη εργασία απο την πλευρά των προγραμματιστών: απαιτεί το γράψιμο κώδικα για την αντιστοίχηση των μηνυμάτων SOAP σε αντικείμενα.
- Το γεγονός ότι η χρήση του SOAP βασίζεται κυρίως σε διαδικτυακή κίνηση HTTP, σημαίνει ότι ξεπερνάει με ευκολία την προστασία firewalls. Αυτό έχει τεθεί ως πιθανός κίνδυνος ασφάλειας για τις εφαρμογές που προστατεύονται πίσω απο αυτό.

Παρά τα παραπάνω, δεν είναι απαγορευτική η υλοποίηση εφαρμογών και υπηρεσιών που βασίζονται στο SOAP, διότι αν ειδωθούν μέσα στο πραγματικό πλαίσιο διαστάσεών τους, η υλοποίηση δεν επηρεάζεται ιδιαίτερα. Επιπρόσθετα, τα ισχυρά πλεονεκτήματα του SOAP (απλότητα, ευελιξία, ανεξαρτησία απο πλατφόρμες) μπορούν να ξεπεράσουν τις πιθανές δυσκολίες.

7.3.2 Γλώσσα Περιγραφής Υπηρεσιών Ιστού

7.3.2.1 Εισαγωγή

Η *Γλώσσα Περιγραφής Υπηρεσιών Ιστού (Web Services Description Language - WSDL)* [Christensen01] αποτελεί μια μορφή εγγράφου σε XML για την περιγραφή υπηρεσιών δικτύου ως ένα σύνολο απο *σημεία τερματισμού (endpoints)* βασιζόμενων σε μηνύματα που περιέχουν είτε πληροφορία *προσανατολισμένη σε έγγραφα (document-oriented)* είτε πληροφορία *προσανατολισμένη σε διαδικασίες (procedure-oriented)*. Τα έγγραφα WSDL περιγράφουν ορισμένες αφηρημένες και ορισμένες συγκεκριμένες λεπτομέρειες των υπηρεσιών δικτύου. Οι αφηρημένες λεπτομέρειες περιγράφουν λειτουργίες και χαρακτηριστικά μηνυμάτων των υπηρεσιών δικτύου που ισχύουν ανεξάρτητα απο την εκάστοτε υλοποίηση. Οι συγκεκριμένες λεπτομέρειες δεσμεύουν τις αφηρημένες σε ένα συγκεκριμένο δικτυακό πρωτόκολλο και μορφή μηνύματος, προκειμένου να ορίσουν το σημείο τερματισμού. Συνδυασμένα συσχετιζόμενα σημεία τερματισμού σχηματίζουν την δικτυακή υπηρεσία. Η WSDL είναι επεκτάσιμη για να επιτρέπει την περιγραφή των σημείων τερματισμού ανεξάρτητα απο την μορφή των μηνυμάτων ή το πρωτόκολλο επικοινωνίας. Οι προδιαγραφές *δεσμεύσεων (bindings)* που υπάρχουν μέχρι στιγμής, περιγράφουν πώς μπορεί να χρησιμοποιηθεί η WSDL σε συνδυασμό με το SOAP, HTTP GET/POST και το MIME.
Η WSDL (αυτή τη στιγμή στην έκδοση 2.0) είναι προσχέδιο προτύπου του W3C το οποίο έχει κατατεθεί απο τις Ariba, IBM και Microsoft ως πρόταση περιγραφής υπηρεσιών. Παρ' όλο που η τεχνολογία είναι ακόμη υπό σχεδιασμό, σχεδόν όλοι οι οργανισμοί που ασχολούνται με τις υπηρεσίες ιστού παρέχουν υποστήριξη για την WSDL και διαθέτουν εργαλεία για την παραγωγή αρχείων WSDL.

7.3.2.2 Σκοπός

Προτού μια εφαρμογή μπορέσει να έχει πρόσβαση σε μια υπηρεσία ιστού, θα πρέπει να μάθει με έναν δομημένο τρόπο τις διαθέσιμες λειτουργίες που προσφέρονται και τις δομές μηνυμάτων που χρησιμοποιούνται απο την υπηρεσία. Τα έγγραφα WSDL καλύπτουν αυτή την ανάγκη περιγραφής της διεπαφής ενός μηνύματος SOAP, παρέχοντας σε ένα έγγραφο XML τεχνικές πληροφορίες για τις λεπτομέρειες κλήσης μιας υπηρεσίας ιστού, την τοποθεσία της στο δίκτυο και τον ορισμό της δομής των μηνυμάτων που κατανοεί. Στα έγγραφα WSDL γίνεται αναφορά μέσω αναγνωριστικών

URL που αποθηκεύονται σε κεντρικές βάσεις δεδομένων στις οποίες κάποιος μπορεί να αναζητήσει υπηρεσίες.
Τα έγγραφα WSDL παίζουν έναν σημαντικό ρόλο στις αλληλεπιδράσεις ανάμεσα σε υπηρεσίες ιστού. Όταν μια υπηρεσία ιστού δημοσιεύεται, ένας διαχειριστής τοποθετεί έναν δεσμό στην περιγραφή WSDL της υπηρεσίας σε μια σχετική βάση δεδομένων. Κατ' αυτό τον τρόπο, η περιγραφή WSDL είναι διαθέσιμη ως αποτέλεσμα σε αναζητήσεις εφαρμογών πελατών που ψάχνουν στην βάση για μια υπηρεσία. Μια εφαρμογή πελάτης αποκτά πρόσβαση στην περιγραφή WSDL για να βρει πληροφορίες για μια υπηρεσία και να μπορέσει να δημιουργήσει ένα μήνυμα SOAP με την κατάλληλη δομή. Στην συνέχεια, η εφαρμογή πελάτης καλεί την υπηρεσία.

7.3.2.3 Δομή

Ένα έγγραφο WSDL χρησιμοποιεί τα ακόλουθα στοιχεία για τον ορισμό υπηρεσιών ιστού:

- *Αφηρημένοι ορισμοί*
  Type: παρέχει ορισμούς για τους τύπους δεδομένων που περιέχουν μηνύματα SOAP.
  Message: παρέχει έναν ορισμό του μηνύματος που μεταφέρεται σε μια επικοινωνία.
  Operation: παρέχει την περιγραφή μιας πράξης που υποστηρίζεται απο την υπηρεσία.
  PortType: καθορίζει την διεπαφή υπηρεσιών των λειτουργιών που υποστηρίζει η υπηρεσία ιστού.
- *Συγκεκριμένοι ορισμοί*
  Binding: προδιαγράφει το πρωτόκολλο και την μορφή των δεδομένων για ένα συγκεκριμένο PortType.
  Port: προδιαγράφει την διεύθυνση μια συγκεκριμένης δέσμευσης.
  Service: προδιαγράφει την τοποθεσία URL της υπηρεσίας ιστού στον εξυπηρετητή που την φιλοξενεί.

Το Σχήμα 7-23 παραθέτει ένα παράδειγμα μιας περιγραφής WSDL μιας υπηρεσίας για μετοχές χρηματιστηρίου. Η υπηρεσία ονομάζεται GetTradePrice και είναι βασισμένη σε κωδικοποίηση SOAP. Η αίτηση λαμβάνει ένα σύμβολο τύπου συμβολοακολουθίας string και επιστρέφει την τιμή μιας μετοχής ως αριθμό κινητής υποδιαστολής float.

```
<?xml version="1.0"?>
<definitions name="StockQuote"
        targetNamespace="http://example.com/stockquote.wsdl"
        xmlns:tns="http://example.com/stockquote.wsdl"
        xmlns:xsd="http://www.w3.org/2000/10/XMLSchema"
        xmlns:xsd1="http://example.com/stockquote.xsd"
        xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
        xmlns="http://schemas.xmlsoap.org/wsdl/">
   <message name="GetTradePriceInput">
      <part name="tickerSymbol" element="xsd:string"/>
      <part name="time" element="xsd:timeInstant"/>
   </message>
```

```
   <message name="GetTradePriceOutput">
      <part name="result" type="xsd:float"/>
   </message>
   <portType name="StockQuotePortType">
      <operation name="GetTradePrice">
        <input message="tns:GetTradePriceInput"/>
        <output message="tns:GetTradePriceOutput"/>
      </operation>
   </portType>
   <binding name="StockQuoteSoapBinding"type="tns:StockQuotePortType">
         <soap:binding style="rpc" transport="http://schemas.xmlsoap.org/soap/http"/>
    <operation name="GetTradePrice">
         <soap:operation soapAction="http://example.com/GetTradePrice"/>
         <input>
<soap:body use="encoded" namespace="http://example.com/stockquote"
encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
         </input>
         <output>
          <soap:body use="encoded" namespace="http://example.com/stockquote"
            encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
         </output>
   </operation>
   </binding>
   <service name="StockQuoteService">
      <documentation>My first service</documentation>
      <port name="StockQuotePort" binding="tns:StockQuoteBinding">
        <soap:address location="http://example.com/stockquote"/>
      </port>
   </service>
</definitions>
```

Σχήμα 7-23: Παράδειγμα εγγράφου περιγραφής WSDL

Είναι εύκολο να διαπιστωθεί ότι το έγγραφο WSDL σε σύγκριση με την περιγραφή της διεπαφής SOAP είναι αρκετά μεγαλύτερο. Αυτό οφείλεται στην πλεονάζουσα πληροφορία που οφείλεται στα ξεχωριστά οριζόμενα στοιχεία και την XML.

7.3.2.4 Ανοιχτά θέματα

Έχουν προταθεί βελτιώσεις του WSDL προκειμένου να αντιμετωπιστούν κυρίως κάποια θέματα ασφάλειας. Η ασφάλεια σχετικά με την WSDL αναφέρεται σε τρεις ξεχωριστές αλλά συσχετιζόμενες περιοχές: ασφάλεια την βάση δεδομένων των υπηρεσιών, ασφάλεια σε συναλλαγές και ασφάλεια στην σχετική υποκείμενη υποδομή.

Η ασφάλεια της βάσης δεδομένων εξασφαλίζει ότι οι χρήστες που αναζητούν υπηρεσίες λαμβάνουν έμπιστα δεδομένα.

Η ασφάλεια συναλλαγών εξασφαλίζει ότι τόσο ο αιτών την υπηρεσία όσο και ο πάροχός της που είναι καταχωρημένος στην βάση, βεβαιώνονται ότι η εμπορική συναλλαγή θα εκτελεστεί με ασφαλή τρόπο. Αυτό σημαίνει ότι οι παράμετροι εμπιστοσύνης της

υπηρεσίας ιστού θα πρέπει να είναι διαθέσιμες σε όλες τις εμπλεκόμενες οντότητες πριν γίνει εκτέλεση της υπηρεσίας και η εμπιστοσύνη θα πρέπει να διασφαλίζεται καθ' όλη τη διάρκεια της συναλλαγής.
Η ασφάλεια στην υποκείμενη υποδομή εξασφαλίζει ότι η απαιτούμενη υποδομή για την εμπιστοσύνη στο περιβάλλον ανακάλυψης και περιγραφής των υπηρεσιών μπορεί να κατανοηθεί και να χρησιμοποιηθεί απο όλους τους συμμετέχοντες.

7.3.3 Πρωτόκολλο Περιγραφής, Ανακάλυψης και Ολοκλήρωσης

7.3.3.1 Εισαγωγή

Οι προδιαγραφές του *Πρωτοκόλλου Περιγραφής, Ανακάλυψης και Ολοκλήρωσης (Universal Description Discovery & Integration - UDDI)* [Clement04] παρέχουν ένα σύστημα για την εγγραφή και εύρεση της πληροφορίας που απαιτείται για την χρήση μιας υπηρεσίας ιστού και της πληροφορίας για τον παροχέα της υπηρεσίας. Η έμφαση στο UDDI δίνεται στον ορισμό ενός συνόλου υπηρεσιών που υποστηρίζουν την περιγραφή και αναζήτηση

1. επιχειρήσεων, οργανισμών και άλλων παρόχων υπηρεσιών ιστού,
2. των υπηρεσιών που αυτοί διαθέτουν και
3. των προγραμματιστικών διεπαφών που μπορούν να χρησιμοποιηθούν για πρόσβαση στις υπηρεσίες.

Τα δεδομένα οργανώνονται με τέτοιο τρόπο ώστε οι επιχειρήσεις να μπορούν να προσφέρουν πολλαπλές υπηρεσίες και μια υπηρεσία να μπορεί να προσφερθεί απο πολλές επιχειρήσεις. Κάθε μια απο τις οντότητες που εμπεριέχονται σε ένα σύστημα UDDI αναγνωρίζεται μοναδικά απο ένα μοναδικό κλειδί προκειμένου να διευκολύνονται αναζητήσεις και ενημερώσεις της πληροφορίας που σχετίζεται με κάθε οντότητα.
Μια κοινοπραξία εταιριών, συμπεριλαμβανομένου της IBM, της Microsoft και της Ariba ξεκίνησαν την δημιουργία της ιδέας για έναν επιχειρηματικό κατάλογο στο διαδίκτυο που να καθορίζει βάσεις μέσα στις οποίες εταιρίες μπορούν να δημοσιεύσουν πληροφορίες για τις ίδιες και τις υπηρεσίες που προσφέρουν. Το αποτέλεσμα ήταν το έργο UDDI που κατατέθηκε στον οργανισμό OASIS για προτυποποίηση. Οι προδιαγραφές του UDDI έκδοση 2 έχουν ήδη γίνει πρότυπο του OASIS. Αυτή τη στιγμή είναι σε φάση σχεδιασμού η τρίτη έκδοση του προτύπου απο την αντίστοιχη τεχνική επιτροπή.

7.3.3.2 Σκοπός

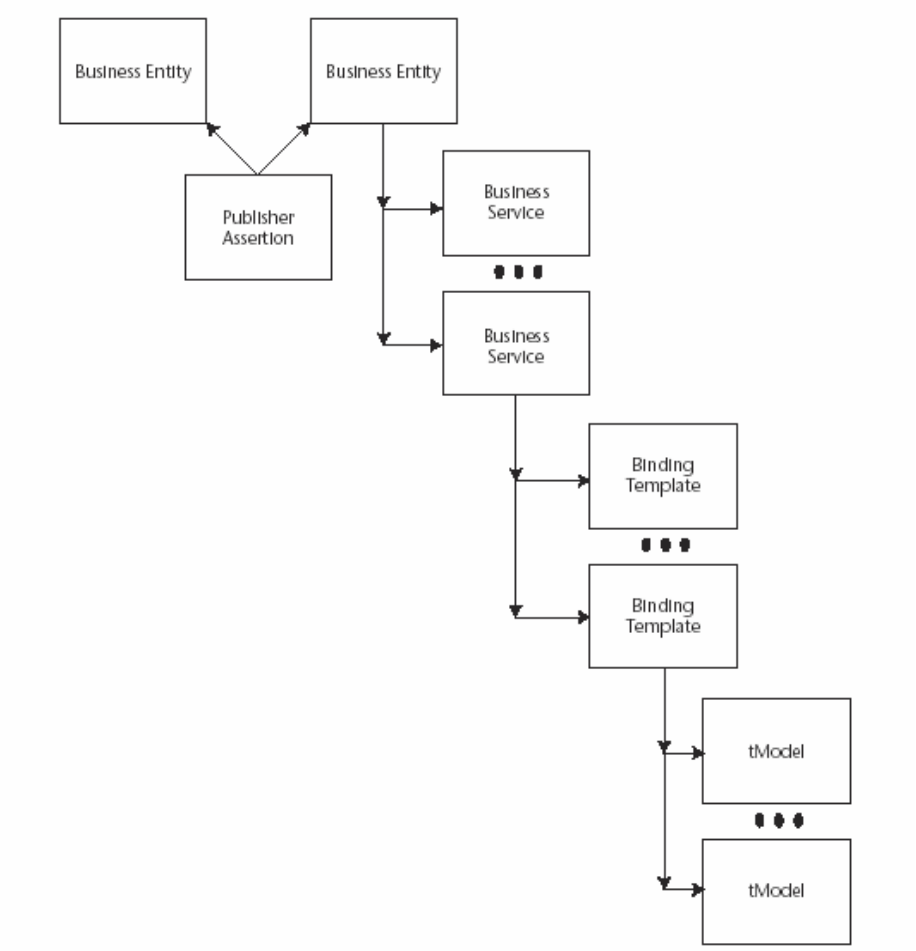
Το UDDI αντιμετωπίζει το πρόβλημα του εντοπισμού κατάλληλων υπηρεσιών ιστού για κατανάλωση απο άλλες υπηρεσίες ή εφαρμογές. Αυτό επιτυγχάνεται με τον καθορισμό βάσεων που είναι ικανές να διαχειριστούν περιγραφές επιχειρησιακών δεδομένων. Τέτοιες βάσεις επίσης παρέχουν λειτουργίες όπως δυνατότητες αναζήτησης, προγραμματιστική πρόσβαση σε απομακρυσμένες εφαρμογές και μηχανισμούς που αμβλύνουν προβλήματα που συμβαίνουν κατά την πρόσβαση σε εγγεγραμμένες υπηρεσίες ιστού. Με την χρήση συστημάτων UDDI, μια οντότητα μπορεί να ανακαλύψει και να συγκρίνει τις υπηρεσίες ιστού που παρέχουν την ίδια λειτουργικότητα. Για παράδειγμα, μια εφαρμογή μπορεί να ανακαλύψει τις υπηρεσίες ιστού που παρέχουν

επεξεργασία δεδομένων πληρωμών πιστωτικών καρτών, και συγκρίνοντάς τες να επιλέξει και χρησιμοποιήσει την πιο κατάλληλη.

7.3.3.3 Δομή

Τα δεδομένα ενός μητρώου UDDI βασίζονται στο HTTP και το SOAP και είναι προσβάσιμα μέσω δύο συνόλων διεπαφών SOAP. Η μια διεπαφή υποστηρίζει πιθανούς συνδρομητές που ανακαλύπτουν επιθυμητές υπηρεσίες και λαμβάνουν τις λεπτομέρειές τους, και η άλλη υποστηρίζει τους παρόχους υπηρεσιών ώστε να μπορούν να διαχειρίζονται την δημοσίευση των υπηρεσιών τους στο μητρώο.

Για τα μητρώα UDDI έχουν καθοριστεί πέντε δομές:
businessEntity: αναπαριστά την επιχείρηση / οργανισμό και παρέχει πληροφορίες όπως το μοναδικό *αναγνωριστικό της (UUID)*, το όνομα της εταιρίας, μια περιγραφή και τις σχετικές επαφές.
businessService: περιλαμβάνεται στην businessEntity και παρέχει δεδομένα για την συγκεκριμένη υπηρεσία που παρέχεται απο την επιχείρηση. Η δομή περιλαμβάνει ένα μοναδικό αναγνωριστικό, την περιγραφή της υπηρεσίας και την κατηγορία της.
bindingTemplate: περιλαμβάνεται στην businessService και αναγνωρίζει πώς και πού μπορεί κάποιος να αποκτήσει πρόσβαση στην υπηρεσία. Η δομή περιέχει ένα μοναδικό αναγνωριστικό και την διεύθυνση της υπηρεσίας ιστού (URL ή e-mail).
tModel: περιλαμβάνεται στο bindingTemplate και περιλαμβάνει τις τεχνικές προδιαγραφές της διεπαφής της υπηρεσίας ιστού. Η δομή περιέχει ένα μοναδικό αναγνωριστικό, ένα όνομα, μια περιγραφή και τα *αναγνωριστικά κατηγορίας (category descriptors)*.
publisherAssertion: παρέχει έναν τρόπο για δύο οντότητες να μπορέσουν να αποκτήσουν μια σχέση μεταξύ τους.



Σχήμα 7-24: Δομή UDDI

Το Σχήμα 7-24 παρουσιάζει την σχέση μεταξύ των παραπάνω δομών.

7.3.3.4 Ανοιχτά θέματα

Η έλλειψη μηχανισμών ποιότητας υπηρεσίας (quality of service – QoS) είναι ένα ανοιχτό θέμα για το UDDI. Οι προδιαγραφές UDDI δεν απαντούν σε ερωτήματα ποιότητας υπηρεσίας όπως για παράδειγμα «πόσο συχνά μπορεί κάποιος να έχει πρόσβαση στην υπηρεσία;» ή «προσφέρει υποστήριξη ο συγκεκριμένος πάροχος;».

Επιπρόσθετα υπάρχουν ζητήματα αξιοπιστίας των δεδομένων που έχουν να κάνουν με τις ενημερώσεις της πληροφορίας σε διαφορετικά μητρώα UDDI. Όλα τα μητρώα UDDI που φιλοξενούν μια υπηρεσία ιστού θα πρέπει να αντικατοπτρίζουν την πιο πρόσφατη περιγραφή της υπηρεσίας.

Η τρίτη έκδοση των προδιαγραφών περιλαμβάνει υποστήριξη για ψηφιακές υπογραφές στα αποθηκευμένα δεδομένα κάτι που επιτρέπει στους ιδιοκτήτες τους να υπογράφουν τις εγγραφές που καταχωρούν σε ένα μητρώο. Αυτό όμως δεν αρκεί για την κάλυψη της απαίτησης για συνεχή αυθεντικοποίηση των δεδομένων. Οι ψηφιακές υπογραφές και απο τους ίδιους τους διαχειριστές των μητρώων θα αναβαθμίσει την παροχή αυθεντικότητας των δεδομένων.

Άλλα ανοιχτά θέματα περιλαμβάνουν την έλλειψη μιας προτυποποιημένης σύνταξης για πολιτικές ελέγχου πρόσβασης και σχημάτων αυθεντικοποίησης.

7.3.4 Προδιαγραφές Διαχείρισης Κλειδιών με XML

7.3.4.1 Εισαγωγή

Το πρότυπο *Διαχείρισης Κλειδιών με XML (XML Key Management Specifications – XKMS)* [Hallam-Baker05] αποτελεί προδιαγραφές για την εγγραφή και διανομή δημόσιων κλειδιών. Είναι μια τεχνολογία βασισμένη στην XML με σκοπό την διευκόλυνση της ενσωμάτωσης ΥΔΚ κάνοντας ευκολότερη την παραμετροποίηση, χρήση και διαχείρισή της. Αυτό επιτυγχάνεται αποφορτίζοντας την ΥΔΚ απο πολύπλοκες εργασίες διαχείρισης κλειδιών και την εδραίωση επικοινωνίας με την ΥΔΚ μέσω της XML, δίνοντας αντίστοιχες δυνατότητες ακόμα και σε ασύρματες συσκευές (κινητά τηλέφωνα κ.λ.π). Το πρότυπο XKMS σχεδιάστηκε για χρήση σε συνδυασμό με τις Ψηφιακές Υπογραφές XML και την Κρυπτογράφηση XML, αλλά και με μελλοντικά πρότυπα. Η συνδυασμένη χρήση της Ψηφιακής Υπογραφής XML και της Κρυπτογράφησης XML παρέχει ακεραιότητα και ιδιωτικότητα, αλλά δεν αντιμετωπίζει τα θέματα εμπιστοσύνης που έχουν να κάνουν με την διαχειρίση κλειδιών. Αυτά τα θέματα αντιμετωπίζονται απο το XKMS.

Το πρότυπο XMKS αποτελείται απο δύο κομμάτια:

- Τις *Προδιαγραφές Παροχής Υπηρεσιών Πληροφοριών με XML (XML Key Information Services Specification X-KISS)*: Καθορίζουν ένα πρωτόκολλο για μια υπηρεσία εμπιστοσύνης που τρέχει σαν Υπηρεσία Ιστού και επιστρέφει την πληροφορία που είναι σχετική με τα στοιχεία KeyInfo που περιέχονται στις δομές Ψηφιακών Υπογραφών XML και Κρυπτογράφησης XML (βλ. Παραγράφους 7.2.1.1 και 7.2.2.1).
- Τις *Προδιαγραφές Παροχής Υπηρεσιών Εγγραφής με XML (XML Key Registration Service Specification X-KRSS)*: Καθορίζουν ένα πρωτόκολλο για μια Υπηρεσία Ιστού που δέχεται πληροφορίες για εγγραφή, ανάκληση και ανάκτηση δημόσιων κλειδιών.

Η αρχικές προδιαγραφές του XKMS δόθηκαν απο την Microsoft, τη Verisign και την WebMethods, αλλά αποτελούν πλέον μια Σημείωση του W3C.

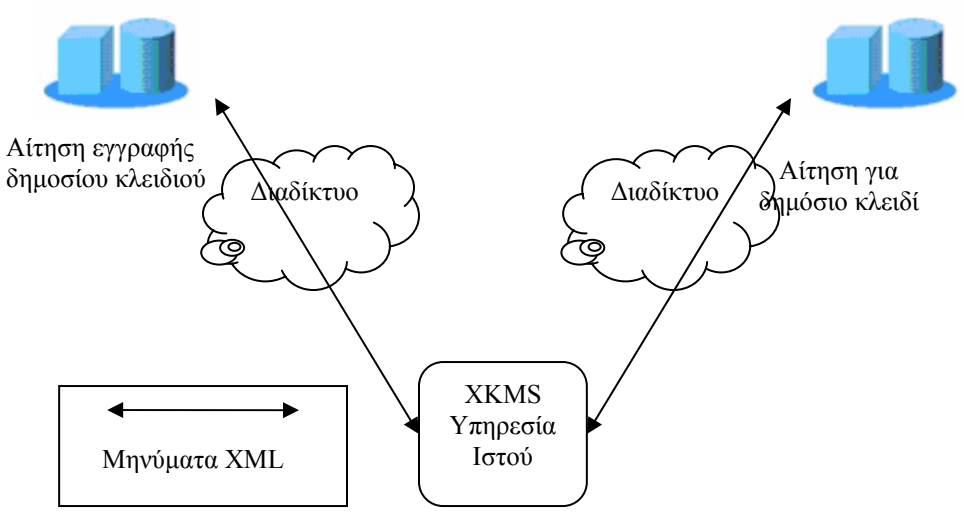
7.3.4.2 Διεργασίες XKMS

Το XKMS απλουστεύει σύνθετες διεργασίες μιας ΥΔΚ ορίζοντας Προγραμματιστικές Διεπαφές (APIs), οι οποίες μπορούν να χρησιμοποιηθούν απο Υπηρεσίες Ιστού. Οι λειτουργίες που προσφέρονται απο της Υπηρεσίες Ιστού που υποστηρίζουν το XKMS περιλαμβάνουν τα εξής:

- Εγγραφή ενός δημόσιου κλειδιού (Πρωτόκολλο X-KRSS)
- Ανάκληση ενός κλειδιού (Πρωτόκολλο X-KRSS)
- Ανάκτηση ενός κλειδιού (Πρωτόκολλο X-KRSS)
- Εντοπισμός ενός κλειδιού (Πρωτόκολλο X-KISS)

- Έλεγχος εγκυρότητας ενός κλειδιού (Πρωτόκολλο X-KISS)

Οι μόνες κρυπτογραφικές λειτουργίες που πρέπει να υποστηρίζονται απο μια εφαρμογή είναι αυτές της Ψηφιακής Υπογραφής XML και της Κρυπτογράφησης XML. Η διαμόρφωση μιας τοπολογίας XKMS είναι όπως φαίνεται στο ακόλουθο σχήμα:



Σχήμα 7-25: Διαμόρφωση τοπολογίας XKMS

Ο βασικός στόχος του πρωτοκόλλου X-KISS είναι η ελαχιστοποίηση της πολυπλοκότητας που συναντά μια εφαρμογή-πελάτης με το να μεταβιβάζει ένα μέρος των διεργασιών που χρειάζονται για την επεξεργασία ενός στοιχείου KeyInfo μιας δομής Ψηφιακής Υπογραφής XML ή Κρυπτογράφησης XML σε μια υπηρεσία εμπιστοσύνης. Ο υπογράφων μπορεί να συμπεριλάβει είτε ένα στοιχείο KeyInfo που καθορίζει το ίδιο το κλειδί (το όνομα ενός κλειδιού, ένα πιστοποιητικό X509, ένα αναγνωριστικό PGP κ.λ.π.) ή μια αναφορά στην τοποθεσία όπου τα πλήρη δεδομένα του στοιχείου KeyInfo μπορούν να βρεθούν. Στην περίπτωση της κρυπτογράφησης, η εφαρμογή-πελάτης μπορεί να μην γνωρίζει καν το δημόσιο κλειδί του παραλήπτη.
Το X-KRSS περιγράφει ένα πρωτόκολλο για την υποστήριξη της εγγραφής πληροφορίας ενός δημοσίου κλειδιού και του ιδιοκτήτη του σε μια υπηρεσία εμπιστοσύνης. Οι προδιαγραφές υποστηρίζουν την διαδικασία εγγραφής που υλοποιείται προκειμένου να δεθεί πληροφορία με ένα ζεύγος κλειδιών που έχουν δημιουργηθεί είτε απο τον πελάτη είτε απο τον εξυπηρετητή που παρέχει την υπηρεσία εμπιστοσύνης.

7.3.4.3 Παράδειγμα

Ένα παράδειγμα μια αίτησης για εγγραφή σε έναν εξυπηρετητή X-KRSS φαίνεται στο σχήμα που ακολουθεί, όπου το ζεύγος κλειδιών έχει δημιουργηθεί απο τον πελάτη.

```
<Register>
  <Prototype Id="keybinding">
    <Status>Valid</Status>
    <KeyID>mailto:Alice@cryptographer.test</KeyID>
```

```
    <ds:KeyInfo>
      <ds:KeyValue>
        <ds:RSAKeyValue>
          <ds:Modulus>
          998/T2PUN8HQlnhf9YIKdMHHGM7HkJwA56UD0a1oYq7E
          fdxSXAidruAszNqBoOqfarJIsfcVKLob1hGnQ/l6xw
          </ds:Modulus>
          <ds:Exponent>AQAB</ds:Exponent>
        </ds:RSAKeyValue>
      </ds:KeyValue>
      <ds:KeyName>mailto:Alice@cryptographer.test</ds:KeyName>
    </ds:KeyInfo>
    <PassPhrase>Pass</PassPhrase>
  </Prototype>
  <AuthInfo>
    <AuthUserInfo>
      <ProofOfPossession>
        <ds:Signature URI="#keybinding"
            [RSA-Sign (KeyBinding, Private)] />
      </ProofOfPossession>
      <KeyBindingAuth>
        <ds:Signature  URI="#keybinding"
            [HMAC-SHA1 (KeyBinding, Auth)] />
      </KeyBindingAuth>
    </AuthUserInfo>
  </AuthInfo>
  <Respond>
    <string>KeyName<string>
    <string>KeyValue</string>
    <string>RetrievalMethod</string>
  </Respond>
</Register>
```

Σχήμα 7-26: Αίτηση εγγραφής ενός ζεύγους κλειδιών δημιουργημένων στην πλευρά του χρήστη

Τα στοιχεία της αίτησης εγγραφής είναι τα ακόλουθα:

Register: Περιέχει όλη την πληροφορία που είναι σχετική με το δημόσιο κλειδί και τον ιδιοκτήτη του.
Status: Καθορίζει την τρέχουσα κατάσταση του δημόσιου κλειδιού. Όταν το κλειδί εγγράφεται, το στοιχείο αυτό παίρνει την τιμή valid.
KeyID: Περιέχει ένα όνομα ή μια τοποθεσία που αναγνωρίζει μοναδικά το κλειδί.
PassPhrase: Περιέχει το αποτέλεσμα μια συνάρτησης κατακερματισμού πάνω στον κωδικό του χρήστη.
AthInfo: Περιέχει τα στοιχεία που αυθεντικοποιούν την αίτηση εγγραφής.
ProofOfPossesion: Περιέχει το στοιχείο Signature της Ψηφιακής Υπογραφής που αποδεικνύει την κατοχή του ιδιωτικού κλειδιού.

KeyBindingAuth: Περιέχει την αίτηση δέσμευσης του κλειδιού, αυθεντικοποιημένη απο μια υπογραφή.
Response: Καθορίζει πως θα πρέπει να απαντήσει ο εξυπηρετητής. Ο εξυπηρετητής επιστρέφει το όνομα του κλειδιού, την τιμή του και την μέθοδο ανάκτησης.

7.3.5 Γλώσσα Προδιαγραφής Ισχυρισμών Ασφάλειας

7.3.5.1 Εισαγωγή

Η *Γλώσσα Προδιαγραφής Ισχυρισμών Ασφάλειας (Security Assertion Markup Language – SAML)* [Cantor05] είναι ένα πλαίσιο βασισμένο στην XML που χρησιμοποιείται για την ανταλλαγή πληροφορία ασφάλειας στην μορφή *«ισχυρισμών» (assertions)* ασφάλειας για ταυτότητες οντοτήτων σε μια συγκεκριμένη διαχειριστική περιοχή ασφάλειας. Ένας ισχυρισμός SAML μπορεί να περιέχει πληροφορία για πράξεις *αυθεντικοποίησης (authentication assertion)* που επιτελούνται απο ταυτότητες, *χαρακτηριστικά ταυτοτήτων (attribute assertion)* και *αποφάσεις για έλεγχο πρόσβασης (authorization assertion)* σε συγκεκριμένους πόρους μιας περιοχής ασφάλειας. Ένα παράδειγμα ισχυρισμού χαρακτηριστικών φαίνεται στο ακόλουθο σχήμα:

```
<saml:assertion
 xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
 MajorVersion="1" MinorVersion="1"
 Issuer="https://idp.edu/saml/" ...>
 <saml:Conditions NotBefore="..." NotAfter="..."/>
 <saml:AuthenticationStatement
   AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:X509-PKI"
   AuthenticationInstant="...">
   <saml:Subject>...</saml:Subject>
 </saml:AuthenticationStatement>
 <saml:AttributeStatement>
   <saml:Subject>...</saml:Subject>
   <saml:Attribute
     AttributeName="urn:mace:dir:attribute-
def:eduPersonScopedAffiliation"

AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
     <saml:AttributeValue Scope="idp.edu">
       member
     </saml:AttributeValue>
     <saml:AttributeValue Scope="idp.edu">
       student
     </saml:AttributeValue>
   </saml:Attribute>
 </saml:AttributeStatement>
</saml:Assertion>
```

Σχήμα 7-27: Παράδειγμα ισχυρισμού SAML

Στο παράδειγμα του σχήματος, γίνεται μια δήλωση χαρακτηριστικού η οποία μπορεί να υποδεικνύει ή όχι ότι ένα υποκείμενο έχει μια σχέση τύπου «μαθητής», την οποία κάποιος θα μπορούσε να χρησιμοποιήσει προκειμένου να επιτρέψει ή να απορρίψει την πρόσβαση σε ένα σύστημα.

Οι ισχυρισμοί εκδίδονται απο *αρχές SAML*, που μπορεί να δρουν ως *αρχές αυθεντικοποίησης, αρχές χαρακτηριστικών ή σημεία αποφάσεων πολιτικών*. Η SAML καθορίζει ένα πρωτόκολλο με το οποίο εφαρμογές-πελάτες μπορούν να ζητούν ισχυρισμούς απο Αρχές SAML και να λαμβάνουν απαντήσεις απο αυτές. Επιπρόσθετα, η SAML περιγράφει πως οι ισχυρισμοί μπορούν να μεταδοθούν απο εφαρμογές κάνοντας χρήση κάποιων προφίλ και «δεσμεύσεων» (bindings). Οι δεσμεύσεις περιγράφουν τον τρόπο με τον οποίο κάποιος κάνει μια αίτηση και λαμβάνει ισχυρισμούς απο μια Αρχή SAML, ενώ τα προφίλ περιγράφουν τον τρόπο με τον οποίο οι ισχυρισμοί SAML μπορούν να υποστηρίξουν την ασφάλεια συναλλαγών μεταξύ εφαρμογών. Οι προδιαγραφές της SAML αυτή τη στιγμή ορίζουν δεσμεύσεις μόνο για το SOAP και το HTTP POST.
Το πρωτόκολλο της SAML έχει προδιαγραφεί με το συνδυασμό της AuthXML της εταιρίας Securant Techonolgies και της γλώσσας Security Services Markup Language της Netegrity. Αυτή τη στιγμή είναι ένα πρότυπο του OASIS που παράγεται απο την Τεχνική Επιτροπή για τις Υπηρεσίες Ασφάλειας.

7.3.5.2 Σκοπός

Ο σκοπός της SAML είναι να καθορίσει μια πρότυπη αναπαράσταση δεδομένων ασφάλειας αναγνωρίσιμων απο διαφορετικές εφαρμογές υπηρεσιών ασφάλειας, ανεξάρτητα απο τις τεχνολογίες ασφάλειας ή τις πολιτικές που χρησιμοποιούν. Η SAML είναι ένα είδος *Υποδομής Διαχείρισης Δικαιωμάτων (Permission Management Infrastructure – PMI)* [Lorch03]. Πριν απο την SAML, οι υλοποιήσεις τέτοιων υποδομών έπρεπε να βασιστούν σε πολύπλοκα και ασύμβατα πακέτα λογισμικού απο διάφορες εταιρίες.

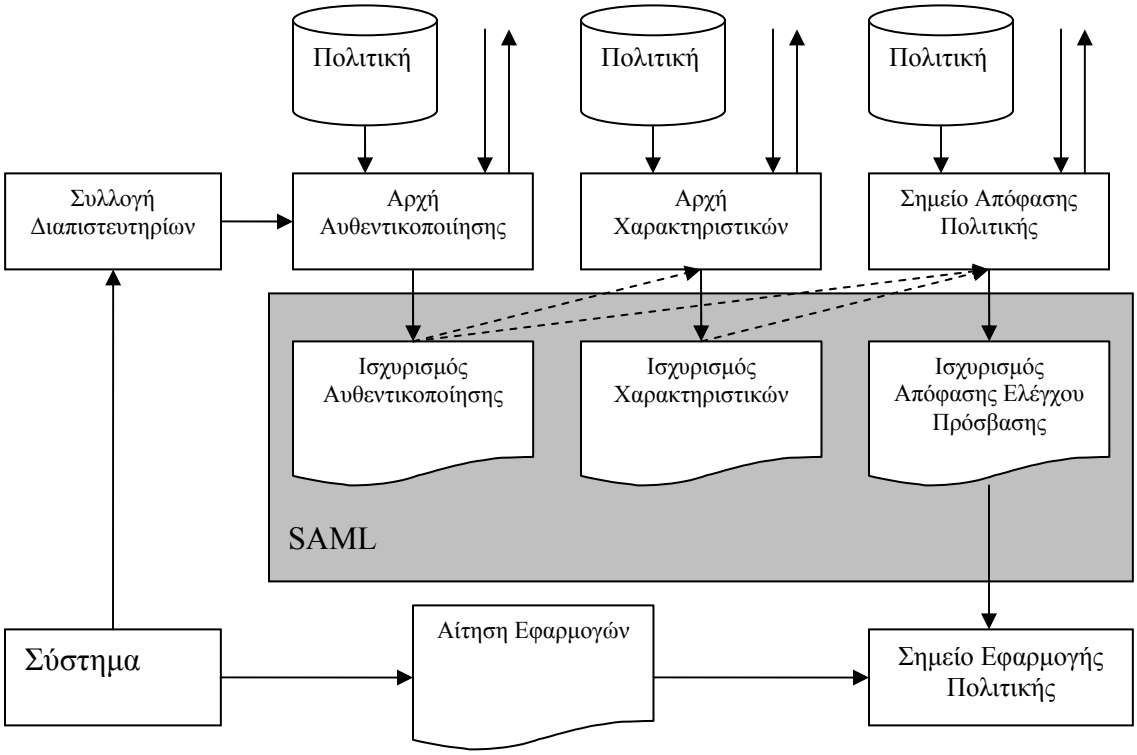
Η SAML καθορίζει τρία διαφορετικά είδη δηλώσεων ισχυρισμών που μπορούν να δημιουργηθούν απο μια Αρχή SAML:

- Αυθεντικοποίηση: Υποδεικνύει ότι η καθορισμένη ταυτότητα έχει αυθεντικοποιηθεί απο μια δεδομένη Αρχή σε ένα δεδομένο χρόνο.
- Χαρακτηριστικό: Η καθορισμένη ταυτότητα είναι συνδεδεμένη με τα καθορισμένα χαρακτηριστικά.
- Απόφαση ελέγχου πρόσβασης: Μια συγκεκριμένη απόφαση ελέγχου πρόσβασης σε έναν πόρο βασισμένη σε μια αίτηση ελέγχου πρόσβασης.

Κάθε δήλωση ισχυρισμού επιστρέφεται στην οντότητα που την αιτεί, κατόπιν αποστολής μιας αίτησης αυθεντικοποίησης, ή χαρακτηριστικών ή ελέγχου πρόσβασης προς μια υπηρεσία έμπιστης τρίτης οντότητας. Η SAML είναι γραμμένη στην XML και ενσωματώνει όλα τα πλεονεκτήματα της XML για ανεξαρτησία απο πλατφόρμες και γλώσσες προγραμματισμού.

7.3.5.3 Διαδικασία χρήσης SAML

Το ακόλουθο σχήμα επιδεικνύει πως η SAML μπορεί να επιτρέψει σε μια οντότητα ενός συστήματος να επιτελέσει μια δραστηριότητα πάνω σε έναν συγκεκριμένο πόρο:



Σχήμα 7-28: Μοντέλο διαχείρισης SAML

Τα βήματα που λαμβάνουν χώρα είναι τα ακόλουθα:

1. Ο πελάτης αυθεντικοποιείται και ζητά απο την αρχή αυθεντικοποίησης να του επιστρέψει έναν ισχυρισμό SAML ως απόδειξη της αυθεντικοποίησης.
2. Ο πελάτης εκδίδει μια αίτηση πρόσβασης στον πόρο και την στέλνει στον οργανισμό που διαχειρίζεται τον πόρο μαζί με τον ισχυρισμό αυθεντικοποίησης του βήματος 1.
3. Ο οργανισμός που θα δεχτεί την αίτηση, πρώτα εξετάζει τον ισχυρισμό αυθεντικοποίησης και έπειτα επικοινωνεί με την Αρχή Χαρακτηριστικών SAML, για να της δώσει τον ισχυρισμό αυθεντικοποίησης και να ζητήσει έναν ισχυρισμό χαρακτηριστικών.
4. Ο οργανισμός αποστέλλει μια αίτηση ελέγχου πρόσβασης SAML στην Αρχή Ελέγχου Πρόσβασης (σημείο ελέγχου πολιτικής) μαζί με τον πόρο στον οποίο ζητά πρόσβαση ο πελάτης και τον ισχυρισμό χαρακτηριστικών.
5. Η Αρχή Ελέγχου Πρόσβασης αποφαίνεται για το αν θα δώσει πρόσβαση ή όχι και επιστέφει μια απόφαση αποδοχής ή απόρριψης στη μορφή ενός ισχυρισμού απόφασης ελέγχου πρόσβασης.

Η SAML είναι ένα πρότυπο ανεξάρτητο απο τις υλοποιήσεις εταιριών και βασίζεται σε ευρέως αποδεκτά πρότυπα και πρωτόκολλα βασισμένα στην XML προκειμένου να επιτυγχάνει διαλειτουργικότητα ανάμεσα σε εφαρμογές.

7.3.5.4 Ανοιχτά θέματα

Οι προδιαγραφές της SAML δεν περιγράφουν όλες τις πλευρές και υποστηριζόμενες υπηρεσίες σε ένα περιβάλλον SAML. Στο Σχήμα 7-28 οι προδιαγραφές καλύπτουν το σκιασμένο κομμάτι. Οι υπόλοιπες υπηρεσίες της αρχιτεκτονικής δεν καθορίζονται απο τις προδιαγραφές, κάτι που μπορεί να επηρεάσει την διαλειτουργικότητα της χρήσης της SAML.

7.3.6 Επεκτάσιμη Γλώσσα Ελέγχου Πρόσβασης

7.3.6.1 Εισαγωγή

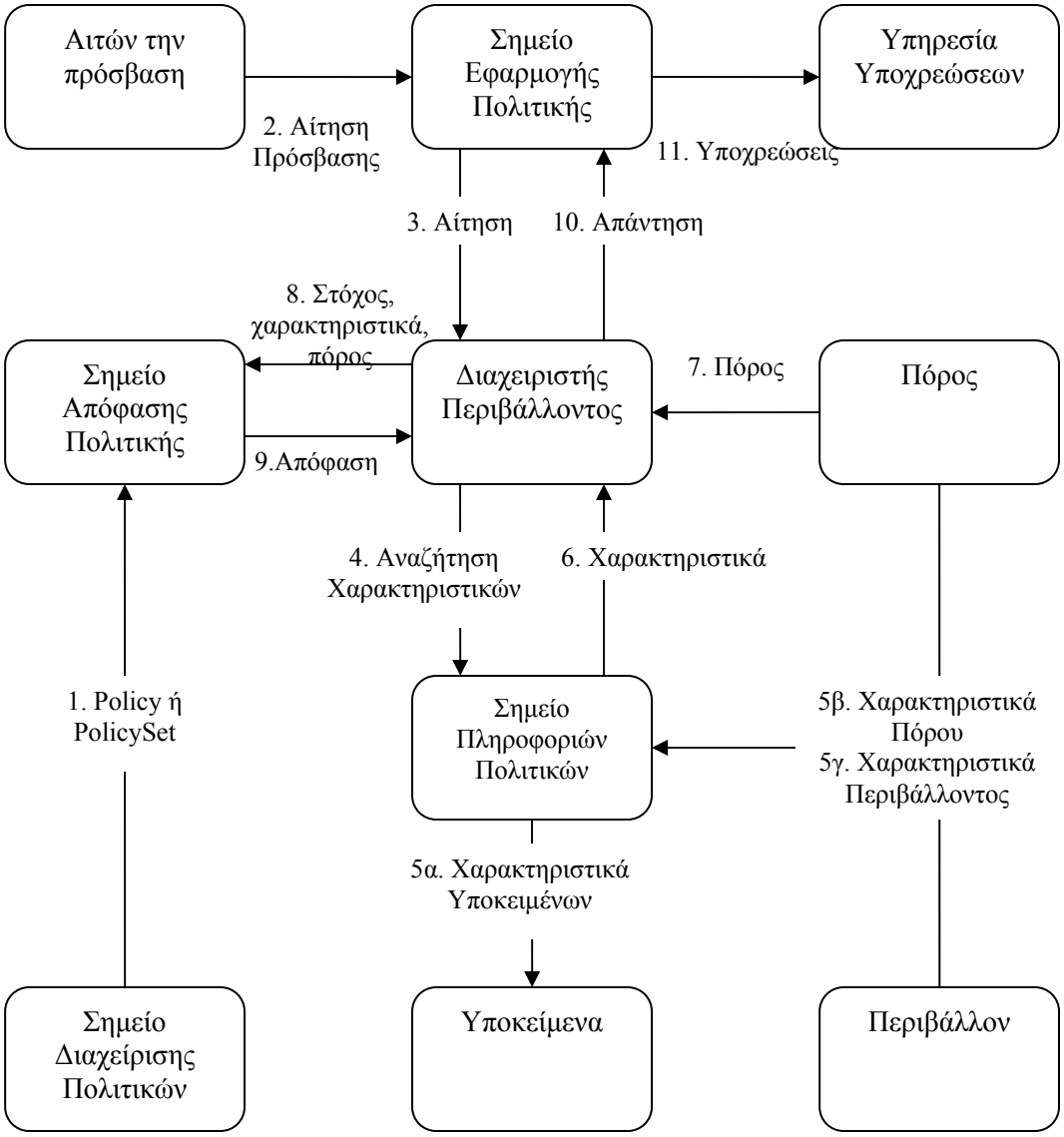
Η *Επεκτάσιμη Γλώσσα Ελέγχου Πρόσβασης (eXtensible Access Control Markup Language - XACML)* [Moses05] είναι μια γενικευμένη γλώσσα προδιαγραφής πολιτικών που βασίζεται στην XML για την έκφραση πληροφορίας ασφάλειας. Η XACML εστιάζει στην δημιουργία μιας πλούσιας γλώσσας για *πολιτικές ασφάλειας* και ένα *μοντέλο για έλεγχο πρόσβασης*, προσφέροντας μια μέθοδο για συνδυασμό μεμονωμένων κανόνων και πολιτικών σε ένα μοναδικό σύνολο πολιτικών που εφαρμόζεται προκειμένου να ληφθεί μια απόφαση για μια συγκεκριμένη αίτηση. Η πολιτική που μπορεί να εφαρμοστεί σε μια αίτηση απόφασης μπορεί να συντεθεί απο έναν αριθμό ανεξάρτητων κανόνων η πολιτικών.

7.3.6.2 Σκοπός

Η XACML είναι μια γλώσσα που επιτρέπει σε οργανισμούς να επικοινωνούν τις πολιτικές τους προς απόκτηση πρόσβασης σε πληροφορίες και πόρους.
Καθορίζει τρία στοιχεία πολιτικής υψηλότερου επιπέδου: τα Rule, Policy και PolicySet. Το στοιχείο Rule περιέχει μια έκφραση Boolean που μπορεί να αποτιμηθεί μεμονωμένα, το στοιχείο Policy περιέχει ένα σύνολο απο στοιχεία Rule και μια συγκεκριμένη διαδικασία για τον συνδυασμό των αποτελεσμάτων των αποτιμήσεών τους, και το στοιχείο PolicySet περιλαμβάνει ένα σύνολο απο στοιχεία Policy ή άλλα στοιχεία PolicySet και μια συγκεκριμένη διαδικασία για το συνδυασμό των αποτελεσμάτων των αποτιμήσεών τους.
Η XACML επίσης καθορίζει έναν αριθμό απο συνδυαστικούς αλγόριθμους που μπορούν να αναγνωριστούν απο τα χαρακτηριστικά RuleCombiningAlgId ή PolicyCombiningAlgId των στοιχείων Policy και PolicySet αντίστοιχα. Ο αλγόριθμος συνδυασμού των στοιχείων Rule και ο αλγόριθμος συνδυασμού των στοιχείων Policy καθορίζουν μια διαδικασία προκειμένου να ληφθεί μια απόφαση δεδομένου των μεμονωμένων αποτελεσμάτων της αποτίμησης των συνόλων απο κανόνες και πολιτικές αντίστοιχα.

7.3.6.3 Διαδικασίες χρήσης XACML

Οι κύριες οντότητες που εμπλέκονται σε μια περιοχή διαχείρισης που χρησιμοποιεί XACML φαίνονται στο ακόλουθο σχήμα:



Σχήμα 7-29:Διάγραμμα ροής XACML

Η διαδικασία που φαίνεται στο σχήμα είναι η ακόλουθη:

1. Το Σημείο Διαχείρισης Πολιτικών – ΣΔΠ (Policy Administration Point – PAP) γράφει πολιτικές για τους πόρους που διαχειρίζεται και τις γνωστοποιεί στο Σημείο Απόφασης Πολιτικής – ΣΑΠ (Policy Decision Point – PDP), το οποίο αποτιμά τις πολιτικές και παίρνει τις αποφάσεις ελέγχου πρόσβασης.
2. Η οντότητα που ζητά την πρόσβαση σε κάποιο πόρο στέλνει μια αίτηση πρόσβασης στο Σημείο Εφαρμογής Πολιτικής - ΣΕΠ (Policy Enforcement Point – PEP) προκειμένου να υλοποιηθεί ο έλεγχος πρόσβασης.
3. Το ΣΕΠ αποστέλλει την αίτηση για πρόσβαση στον διαχειριστή περιβάλλοντος (context handler) σε μια μορφή που αυτός καταλαβαίνει. Ο διαχειριστής

περιβάλλοντος κατασκευάζει μια αίτηση XACML βάσει της πληροφορίας που περιέχεται στην αίτηση.

4. Πληροφορίες για τον πόρο προς πρόσβαση και χαρακτηριστικά του περιβάλλοντος ενδέχεται να ζητηθούν απο έναν Σημείο Πληροφοριών Πολιτικών – ΣΠΠ (Policy Information Point – PIP), το οποίο τελεί χρέη πηγής τιμών χαρακτηριστικών.
5. Το ΣΠΠ αναζητά και λαμβάνει τα χαρακτηριστικά του υποκειμένου που ζητά πρόσβαση, τον πόρο που ζητείται προς πρόσβαση και το περιβάλλον.
6. Το ΣΠΠ επιστρέφει τα χαρακτηριστικά που έχουν ζητηθεί στον διαχειριστή περιβάλλοντος.
7. Ο διαχειριστής περιβάλλοντος ενδέχεται να συμπεριλάβει τον πόρο στην αίτηση.
8. Ο διαχειριστής περιβάλλοντος στέλνει την αίτηση για απόφαση πρόσβασης στο ΣΑΠ για να αποτιμήσει την πολιτική.
9. Το ΣΑΠ επιστρέφει την απάντηση.
10. Ο διαχειριστής περιβάλλοντος μεταφράζει την απάντηση απο XACML στην μορφή που κατανοεί το ΣΕΠ. Αποστέλλει την απάντηση αυτή στο ΣΕΠ.
11. Το ΣΕΠ εφαρμόζει την πολιτική. Εάν η πρόσβαση επιτρέπεται σύμφωνα με την απάντηση, τότε το ΣΕΠ επιτρέπει πρόσβαση στον πόρο, αλλιώς απορρίπτει την αίτηση πρόσβασης.

7.3.6.4 Ανοιχτά θέματα

Το βασικό κομμάτι της γλώσσας XACML είναι απομονωμένο απο το περιβάλλον των εφαρμογών μέσω του διαχειριστή περιβάλλοντος. Οι υλοποιήσεις της XACML πρέπει να μεταφράζουν τις αναπαραστάσεις των χαρακτηριστικών απο το περιβάλλον των εφαρμογών στις αναπαραστάσεις των χαρακτηριστικών στο περιβάλλων της XACML. Η μετάφραση αυτή δεν περιγράφεται απο τις προδιαγραφές της XACML.

7.3.7 Ασφάλεια Υπηρεσιών Ιστού

7.3.7.1 Εισαγωγή

Το πρότυπο Ασφάλειας Υπηρεσιών Ιστού (WS-Security) [Nadalin06] καθορίζει επεκτάσεις στο πρότυπο SOAP (βλ. παράγραφο 7.3.1) για να ενσωματώσει πληροφορία κρυπτογράφησης και ψηφιακών υπογραφών, συμπεριλαμβανομένων διαπιστευτηρίων ασφάλειας όπως πιστοποιητικά ΥΔΚ και *«εισιτήρια» Kerberos (Kerberos tickets)* [Neuman94], σε ένα μήνυμα SOAP. Η πρώτη του έκδοση ήταν τον Απρίλιο του 2002 και στη συνέχεια υιοθετήθηκε ως πρότυπο του οργανισμού OASIS.

Η ασφάλεια που προσδίδει το πρότυπο στο επίπεδο αυτό (επίπεδο ανταλλαγής μηνυμάτων) είναι ανεξάρτητη απο κρυπτογράφηση στο «επίπεδο μεταφοράς» (transport layer) όπως αυτή που επιτυγχάνεται με το SSL, οπότε μπορεί να χρησιμοποιηθεί για παράδειγμα σε ένα εσωτερικό εταιρικό δίκτυο σαν μια κανονική σύνδεση HTTP.

Οι προδιαγραφές του WS-Security αναφέρονται στην ασφάλεια ενός μηνύματος, απο-άκρη-σε-άκρη (end-to-end). Περιγράφουν βελτιώσεις της διαδικασίας ανταλλαγής μηνυμάτων SOAP για την παροχή προστασίας με εξασφάλιση της ακεραιότητας, ιδιωτικότητας και αυθεντικοποίησης ενός μοναδικού μηνύματος SOAP. Το πρότυπο επίσης παρέχει έναν γενικής χρήσης μηχανισμό για την σύνδεση διαπιστευτηρίων ασφάλειας με μηνύματα και περιγράφει πώς κωδικοποιούνται τέτοια δυαδικά διαπιστευτήρια.

7.3.7.2 Μηχανισμοί WS-Security

Οι προδιαγραφές παρέχουν τρεις κύριους μηχανισμούς: μετάδοση διαπιστευτηρίων ασφάλειας, ακεραιότητα μηνυμάτων και ιδιωτικότητα μηνυμάτων. Οι μηχανισμοί αυτοί απο μόνοι τους δεν παρέχουν μια ολοκληρωμένη λύση ασφάλειας. Αποτελούν αντίθετα ένα συστατικό που μπορεί να χρησιμοποιηθεί σε συνδυασμό με άλλες επεκτάσεις Υπηρεσιών Ιστού και υψηλότερου επιπέδου πρωτόκολλα εφαρμογών προκειμένου να ικανοποιηθεί ένα ευρύ σύνολο μοντέλων ασφάλειας και τεχνολογιών κρυπτογράφησης. Οι μηχανισμοί αυτοί μπορούν να χρησιμοποιηθούν ανεξάρτητα ή όλοι μαζί.
Το πρότυπο παρέχει έναν μηχανισμό για τον καθορισμό κωδικοποιημένων δυαδικών διαπιστευτηρίων ασφάλειας και έναν γενικής χρήσης μηχανισμό για την σύνδεση των διαπιστευτηρίων αυτών με μηνύματα. Πιο συγκεκριμένα περιγράφει πώς να κωδικοποιηθούν πιστοποιητικά X509 και «εισιτήρια» Kerberos καθώς και το πώς να συμπεριληφθούν σε ένα μήνυμα κρυπτογραφημένα κλειδιά. Οι προδιαγραφές καθορίζουν ένα μοντέλο ασφάλειας μηνυμάτων με την έννοια των διαπιστευτηρίων ασφάλειας συνδυασμένων με ψηφιακές υπογραφές ως απόδειξη κατοχής του διαπιστευτηρίου.
Η ακεραιότητα μηνυμάτων επιτυγχάνεται χρησιμοποιώντας τις ψηφιακές υπογραφές XML σε συνδυασμό με διαπιστευτήρια ασφάλειας, για την εξασφάλιση ότι τα μηνύματα μεταδίδονται χωρίς αλλοιώσεις. Οι μηχανισμοί ακεραιότητας είναι σχεδιασμένοι κατά τέτοιο τρόπο ώστε να μπορούν να υποστηρίξουν πολλαπλές υπογραφές και είναι επεκτάσιμοι ώστε να μπορούν να υποστηρίξουν επιπρόσθετες μορφές υπογραφών. Οι μηχανισμοί κρυπτογράφησης υποστηρίζουν επιπρόσθετες τεχνολογίες και διαδικασίες κρυπτογραφίας και λειτουργίες απο πολλαπλούς δράστες.

7.3.7.3 Μορφή / Δομή

Το πρότυπο καθορίζει ένα στοιχείο ασφάλειας για ένα μήνυμα SOAP. Το στοιχείο ασφάλειας περιέχεται στην επικεφαλίδα του μηνύματος SOAP και αναφέρεται σε έναν συγκεκριμένο ρόλο. Αυτό σημαίνει ότι μπορούν να υπάρχουν περισσότερα του ενός στοιχεία ασφάλειας σε μια επικεφαλίδα. Το στοιχείο ασφάλειας Security περιέχει όλους τους ισχυρισμούς ή άλλο είδος πληροφορίας που είναι σχετική με τον ρόλο, όπως στοιχεία Signature και EncryptedKey. Το στοιχείο EncryptedKey πρέπει να περιλαμβάνει ένα στοιχείο ReferenceList έτσι ώστε ο παραλήπτης του μηνύματος να μπορεί να συνδέσει κλειδιά με τα αντίστοιχα κρυπτογραφημένα δεδομένα.
Το στοιχείο Security περιλαμβάνει τα ακόλουθα υπο-στοιχεία: UsernameToken, BinarySecurityToken, SecurityTokenReference, KeyInfo, Signature, ReferenceList και EncryptedData. Το στοιχείο UserNameToken χρησιμοποιείται για να συμπεριληφθεί το όνομα του χρήστη και ένας προαιρετικός κωδικός. Το στοιχείο BinarySecurityToken είναι ένα διαπιστευτήριο ασφάλειας (όχι σε μορφή XML), όπως ένα πιστοποιητικό X509 ή ένα «εισιτήριο» Kerberos. Το στοιχείο SecurityTokenReference περιλαμβάνει ένα σύνολο απο ισχυρισμούς ή μια αναφορά σε ισχυρισμούς. Τέλος το στοιχείο ReferenceList χρησιμοποιείται για να αναγνωριστούν τα κρυπτογραφημένα στοιχεία μέσα σε ένα μήνυμα που έχει κρυπτογραφηθεί με το ίδιο κλειδί.
Ο κύριος σκοπός των προδιαγραφών Ασφάλειας Υπηρεσιών Ιστού είναι να δώσουν σε εφαρμογές την ικανότητα να κατασκευάζουν ασφαλή μηνύματα SOAP και να παρέχουν

ένα ευέλικτο σύνολο μηχανισμών που μπορούν να χρησιμοποιηθούν για να υλοποιηθεί ένα εύρος πρωτοκόλλων ασφάλειας.
Οι προδιαγραφές Ασφάλειας Υπηρεσιών Ιστού καθορίζουν πώς χρησιμοποιούνται οι Ψηφιακές Υπογραφές XML και η Κρυπτογράφηση XML σε επικεφαλίδες μηνυμάτων SOAP. Οι ψηφιακές υπογραφές απο μόνες τους δεν μπορούν να δώσουν αυθεντικοποίηση μηνυμάτων, θα πρέπει να συνδυαστούν και με κατάλληλα μέσα που θα εξασφαλίζουν την μοναδικότητα των μηνυμάτων, όπως χρονοσφραγίδες ή σειριακοί αριθμοί. Έτσι μπορεί να αποφευχθούν επιθέσεις «επανάληψης». Οι υλοποιήσεις του προτύπου θα πρέπει να είναι επίσης ευαίσθητες στα θέματα που μπορεί να προκύψουν απο τη χρήση της Ψηφιακής Υπογραφής γενικότερα. Διαπιστευτήρια που μεταφέρονται με μηνύματα θα πρέπει να είναι και τα ίδια υπογεγραμμένα ώστε να εξασφαλίζεται η ακεραιότητά τους. Τέλος, ιδιαίτερη προσοχή θα πρέπει να δίνεται στον συνδυασμό υπογραφών με κρυπτογράφηση στα ίδια δεδομένα, διότι ο συνδυασμός αυτός ενδέχεται να δημιουργήσει κρυπτογραφική αδυναμία.
Η Ασφάλεια Υπηρεσιών Ιστού ξεπερνάει τα δύο πρότυπα των Ψηφιακών Υπογραφών XML και Κρυπτογράφησης XML, εφαρμόζοντάς τα πάνω σε μηνύματα SOAP. Με άλλα λόγια καλύπτει κάποια απο τα κενά που αφήνουν τα δύο αυτά πρότυπα όταν χρησιμοποιούνται με το SOAP και παρέχει επιπρόσθετες οδηγίες εφαρμογής.

7.3.8 Το πρότυπο ISO/RM-ODP

7.3.8.1 Εισαγωγή

Ο οργανισμός προτυποποίησης ISO και η ITU-T, ένωσαν τις προσπάθειες τους για την δημιουργία ενός κοινού πλαισίου υλοποίησης συστημάτων *Ανοιχτών Κατανεμημένων Διεργασιών (Open Distributed Processing – ODP)* που ωφελούνται απο την κατανομή υπηρεσιών επεξεργασίας της πληροφορίας σε περιβάλλοντα με ετερογενείς τεχνολογίες και πολλαπλές περιοχές διαχείρισης. Το *Μοντέλο Αναφοράς Ανοιχτών Κατανεμημένων Διεργασιών (ODP Reference Model – RM-ODP)* είναι το αποτέλεσμα αυτής της προσπάθειας. Το RM-ODP δημιουργεί μια αρχιτεκτονική που ενσωματώνει υποστήριξη για κατανομή, διαλειτουργικότητα και μεταφερσιμότητα και περιγράφει συστήματα που υποστηρίζουν ετερογενείς διεργασίες καθώς και την ανταλλαγή πληροφοριών μεταξύ ομάδων μέσα σε έναν οργανισμό αλλά και ανάμεσα σε συνεργαζόμενους οργανισμούς.
Το RM-ODP καθορίζει τις βασικές έννοιες της κατανεμημένης διεργασίας, αναγνωρίζει τα χαρακτηριστικά που πρέπει να έχει ένα σύστημα ανοιχτών κατανεμημένων διεργασιών και εισάγει **πέντε *όψεις (viewpoints)*** (επιχειρησιακή, πληροφορίας, υπολογιστική, μηχανικού, τεχνολογική) που χρησιμοποιούνται προκειμένου να καθοριστεί το ODP σύστημα. Μια όψη σε ένα σύστημα είναι μια αφαίρεση του συστήματος (ή ενός κομματιού του συστήματος) που παρέχει προδιαγραφές του όλου (ή του κομματιού) σχετικές με ένα συγκεκριμένο σύνολο ενδιαφερόντων. Το πρότυπο επίσης καθορίζει μια γλώσσα που μπορεί να χρησιμοποιηθεί για την περιγραφή κάθε όψης. Επί της ουσίας, κάθε γλώσσα όψης παρέχει ένα σύνολο απο ορισμούς εννοιών και κανόνων που επιτρέπουν την προδιαγραφή του συστήματος απο την αντίστοιχη όψη. Επιπρόσθετα, το RM-ODP παρέχει ένα πλαίσιο για τον έλεγχο της συμμόρφωσης στις προδιαγραφές και την συνέπεια ανάμεσα σε διαφορετικές όψεις και καθορίζει συγκεκριμένες συναρτήσεις που πρέπει να υποστηρίζονται απο το σύστημα ODP. Τέλος, παρουσιάζει μια αρχιτεκτονική συστήματος που παρέχει διαφάνειες κατανομής μεταξύ

εφαρμογών του συστήματος. Οι διαφάνειες κατανομής επιτρέπουν το κρύψιμο της πολυπλοκότητας που συνοδεύει την κατανομή του συστήματος απο τις διάφορες εφαρμογές, όταν η πολυπλοκότητα αυτή είναι άσχετη με τον σκοπό της εφαρμογής.
Η προδιαγραφή του συστήματος με το RM-ODP βασίζεται σε ένα αντικειμενοστρεφές μοντέλο. Η προσέγγιση αυτή παρέχει μια τυποποίηση ήδη εδραιωμένων πρακτικών σχεδιασμού αφαίρεσης και ενθυλάκωσης (encapsulation).
Το σύνολο των εγγράφων που απαρτίζουν το RM-ODP αποτελείται απο τέσσερα μέρη:

- Μέρος 1ο: *ISO 10746-1/ITU-T X.901: Επισκόπηση (Overview)*.
- Μέρος 2ο: *ISO 10746-2/ITU-T X.902: Βάσεις (Foundations)*.
- Μέρος 3ο: *ISO 10746-3/ITU-T X.903: Αρχιτεκτονική (Architecture)*.
- Μέρος 4ο: *ISO 10746-4/ITU-T X.904: Σημασιολογία αρχιτεκτονικών (Architectural semantics)*.

Το πρώτο μέρος περιέχει μια επισκόπηση των στόχων του προτύπου δίνοντας την εμβέλεια, την τεκμηρίωση και την εξήγηση των βασικών ιδεών και μια περίληψη της αρχιτεκτονικής του.
Το δεύτερο μέρος περιέχει τους ορισμούς των εννοιών και το αναλυτικό πλαίσιο για την περιγραφή κατανεμημένων συστημάτων. Τα περιεχόμενα είναι τόσο λεπτομερή όσο χρειάζεται για να υποστηριχθεί το τρίτο μέρος και να εδραιωθούν απαιτήσεις για νέες τεχνικές προδιαγραφών.
Το τρίτο μέρος περιέχει τις προδιαγραφές των απαραίτητων χαρακτηριστικών που καθιστούν ένα κατανεμημένο σύστημα ανοιχτό. Αποτελούν περιορισμούς που πρέπει να λαμβάνουν υπόψην τα πρότυπα ανοιχτών κατανεμημένων διεργασιών. Χρησιμοποιεί τις περιγραφικές τεχνικές του δεύτερου μέρους.
Το τέταρτο μέρος περιέχει μια επίσημη περιγραφή των εννοιών του δευτέρου μέρους και μια φορμαλιστική περιγραφή των γλωσσών όψεων του τρίτου μέρους. Η τυποποίηση επιτυγχάνεται με την εξήγηση όλων των εννοιών των δομών κάθε διαφορετικής προτυποποιημένης τεχνικής προδιαγραφών.
Όλα τα μέρη του RM-ODP επεξηγούνται με χρήση αντικειμενοστρεφών εννοιών. Το αντικειμενοστρεφές μοντέλο παίζει έναν σημαντικό ρόλο στην μοντελοποίηση ανοιχτών κατανεμημένων συστημάτων καθώς παρέχει το απαιτούμενο επίπεδο αφαίρεσης για την απόκρυψη της εγγενούς πολυπλοκότητας τέτοιου είδους συστημάτων.

7.3.8.2 Στοιχεία του RM-ODP

Το πρότυπο RM-ODP βασίζεται σε τέσσερα σημαντικά στοιχεία:

- Μια μοντελοποίηση των αντικειμένων της αρχιτεκτονικής.
- Την προδιαγραφή του συστήματος με χρήση ξεχωριστών αλλά συσχετισμένων όψεων.
- Τον ορισμό της υποδομής του συστήματος με την χρήση *διαφανειών κατανομής (distribution transparencies)* για εφαρμογές.
- Ένα πλαίσιο για τον έλεγχο της συμμόρφωσης προς τις προδιαγραφές που έχουν σχεδιαστεί.

Περισσότερες λεπτομέρειες γι' αυτά τα στοιχεία δίνονται στη συνέχεια.

7.3.8.2.1 Μοντελοποίηση αντικειμένων

Η μοντελοποίηση αντικειμένων παρέχει μια τυποποίηση ευρέως εδραιωμένων πρακτικών σχεδιασμού για *αφαίρεση και ενθυλάκωση*. Η αφαίρεση επιτρέπει την περιγραφή της λειτουργικότητας του συστήματος ξεχωριστά απο τις λεπτομέρειες υλοποίησης. Η ενθυλάκωση επιτρέπει την απόκρυψη της ετερογένειας και λεπτομερειών ασφάλειας και μηχανισμών παροχής υπηρεσιών απο τον χρήστη του συστήματος.

Οι έννοιες της μοντελοποίησης αντικειμένων καλύπτουν:

- *Βασικές έννοιες μοντελοποίησης (Basic modeling concepts)* – Παρέχουν αυστηρούς ορισμούς ενός ελάχιστου συνόλου απο έννοιες (πράξη, αντικείμενο, αλληλεπίδραση και διεπαφή) που αποτελούν την βάση των περιγραφών ανοιχτών κατανεμημένων συστημάτων και είναι εφαρμόσιμες σε όλες τις όψεις.
- *Έννοιες προδιαγραφών (Specification concepts)* – Καλύπτουν τις έννοιες του τύπου και της κλάσης που είναι απαραίτητες για την λογική των προδιαγραφών και τις σχέσεις μεταξύ προδιαγραφών, παρέχουν γενικά εργαλεία για σχεδιασμό και εδραιώνουν τις απαιτήσεις των γλωσσών.
- *Έννοιες δόμησης (Structuring concepts)* – Στηρίζονται στις βασικές έννοιες μοντελοποίησης και τις έννοιες προδιαγραφών για να καλύψουν τις επαναλαμβανόμενες δομές σε κατανεμημένα συστήματα, και περιοχές όπως οι πολιτικές, η ονοματολογία, οι συμπεριφορές, οι εξαρτήσεις και η επικοινωνία.

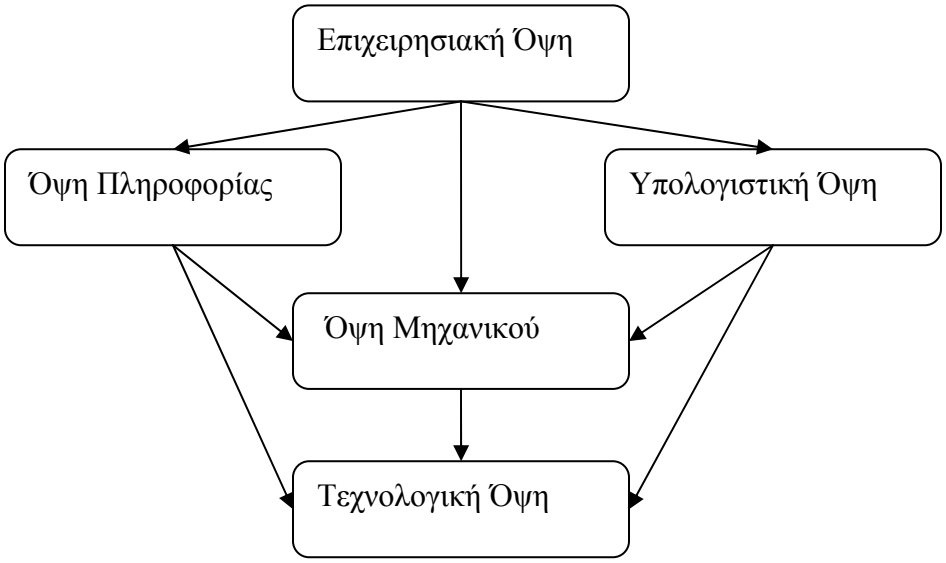
7.3.8.2.2 Προδιαγραφές όψεων

Μια όψη (ενός συστήματος) αποτελεί μια αφαίρεση που αποδίδει τις προδιαγραφές του συστήματος σχετικά με ένα συγκεκριμένο σύνολο αναγκών. Οι πέντε όψεις και οι αντίστοιχες γλώσσες, όπως καθορίζονται στο πρότυπο, που χρησιμοποιούνται για τον προσδιορισμό του συστήματος είναι οι ακόλουθες:

- *Η Επιχειρησιακή Όψη (Enterprise Viewpoint)*, που επικεντρώνει στις πολιτικές που καθορίζουν την συμπεριφορά αντικειμένων μέσα στο σύστημα καθώς και τον σκοπό λειτουργίας και εμβέλειας του συστήματος. Η όψη αυτή περιγράφει το σύστημα απο την πλευρά του τι απαιτείται αυτό να κάνει. Η *Επιχειρησιακή Γλώσσα* χρησιμοποιείται για να περιγράψει την Επιχειρησιακή Όψη.
- *Η Όψη Πληροφορίας (Information Viewpoint)*, περιγράφει τις οντότητες πληροφορίας που μεταφέρονται, αποθηκεύονται και υπόκεινται σε επεξεργασία μέσα στο σύστημα. Η *Γλώσσα Πληροφορίας* χρησιμοποιείται για να περιγραφεί η Όψη Πληροφορίας.
- *Η Υπολογιστική Όψη (Computational Viewpoint)*, επικεντρώνεται στο πως επιτυγχάνεται η κατανομή των διεργασιών. Η *Υπολογιστική Γλώσσα* χρησιμοποιείται για την περιγραφή της Υπολογιστικής Όψης.
- *Η Όψη Μηχανικού (Engineering Viewpoint)*, επικεντρώνει στον τρόπο με τον οποίο διαφορετικά αντικείμενα μέσα στο σύστημα επικοινωνούν μεταξύ τους και στους πόρους που απαιτούνται για να επιτευχθεί αυτή η επικοινωνία. Η *Γλώσσα Μηχανικού* χρησιμοποιείται για να περιγραφεί η Όψη Μηχανικού.

- *Η Τεχνολογική Όψη (Technology Viewpoint)*, επικεντρώνεται στην επιλογή τεχνολογίας για το σύστημα. Η *Τεχνολογική Γλώσσα* χρησιμοποιείται για να περιγραφεί η Τεχνολογική Όψη.

Οι σχέσεις ανάμεσα στις όψεις φαίνονται στο Σχήμα 7-30:



Σχήμα 7-30: Σχέσεις ανάμεσα στις όψεις του συστήματος βάσει RM-ODP

Οι έννοιες της μοντελοποίησης αντικειμένων δίνουν μια κοινή βάση για τις γλώσσες όψεων και καθιστούν δυνατή την αναγνώριση σχέσεων μεταξύ των διαφορετικών προδιαγραφών όψεων και την αντιστοίχιση ανάμεσα στις αναπαραστάσεις του συστήματος σε διαφορετικές όψεις.

7.3.8.2.2.1 Έννοιες RM-ODP για τις όψεις

Οι έννοιες που ορίζονται στο πρότυπο RM-ODP για κάθε όψη είναι οι ακόλουθες:

7.3.8.2.2.1.1 Έννοιες επιχειρησιακής όψης

- *Οντότητα (entity)*: οποιαδήποτε συγκεκριμένη ή αφηρημένη έννοια με ενδιαφέρον. Μπορεί να χαρακτηρίσει οτιδήποτε στον χώρο τον οποίο θέλουμε να μοντελοποιήσουμε ή να σχεδιάσουμε.
- *Αφαίρεση (abstraction)*: η διαδικασία με την οποία αποσιωπούμε άσχετες λεπτομέρειες με σκοπό την απλοποίηση του μοντέλου, ή το αποτέλεσμα αυτής της διαδικασίας.
- *Σύστημα (system)*: κάτι που θεωρείται σημαντικό στο σύνολό του ή ως σύνθεση στοιχείων.
- *Αντικείμενο (object)*: το μοντέλο μιας οντότητας. Ένα αντικείμενο χαρακτηρίζεται απο την συμπεριφορά του και την κατάστασή του. Ένα αντικείμενο είναι διαφορετικό απο ένα άλλο αντικείμενο. Ένα αντικείμενο είναι ενθυλακωμένο, δηλαδή οποιαδήποτε αλλαγή στην κατάστασή του είναι το αποτέλεσμα είτε μιας εσωτερικής αλλαγής του αντικειμένου ή μιας αλληλεπίδρασης με το περιβάλλον του.

Ένα αντικείμενο αλληλεπιδρά με το περιβάλλον του σε προκαθορισμένα σημεία αλληλεπίδρασης.

- *Περιβάλλον ενός αντικειμένου (environment of an object)*: το κομμάτι ενός μοντέλου που δεν αποτελεί μέρος ενός αντικειμένου.
- *Πράξη (action)*: κάτι που συμβαίνει.
- *Συμπεριφορά ενός αντικειμένου (behavior of an object)*: Ένα σύνολο απο πράξεις ενός αντικειμένου και περιορισμοί για το πότε μπορούν να συμβούν.
- *Διεπαφή (interface)*: Μια αφαίρεση της συμπεριφοράς ενός αντικειμένου που αποτελείται απο ένα υποσύνολο απο αλληλεπιδράσεις του αντικειμένου, μαζί με ένα σύνολο απο περιορισμούς για το πότε μπορούν να λάβουν χώρα οι αλληλεπιδράσεις αυτές.
- *Σημείο αλληλεπίδρασης (interaction point)*: ένα σημείο στο οποίο υπάρχει ένα σύνολο απο διεπαφές.
- *Σύνθεση αντικειμένων (composition of objects)*: ο συνδυασμός δύο ή περισσότερων αντικειμένων απο τον οποίο προκύπτει ένα νέο αντικείμενο, σε διαφορετικό επίπεδο αφαίρεσης. Τα χαρακτηριστικά του νέου αντικειμένου καθορίζονται απο τα συνδυαζόμενα αντικείμενα-συνιστώσες και τον τρόπο με τον οποίο έχουν συνδυαστεί. Η συμπεριφορά του *σύνθετου αντικειμένου* είναι η αντίστοιχη σύνθεση των συμπεριφορών των αντικείμενων-συνιστωσών.
- *Σύνθεση συμπεριφορών (composition of behaviors)*: ο συνδυασμός δύο ή περισσότερων συμπεριφορών απο τον οποίο προκύπτει μια νέα συμπεριφορά. Τα χαρακτηριστικά της νέα συμπεριφοράς καθορίζονται απο τις συμπεριφορές που την απαρτίζουν και τον τρόπο με τον οποίο συνδυάζονται.
- *Τύπος ενός <X> (type of an <X>)*: ένα κατηγόρημα που χαρακτηρίζει μια συλλογή απο <X>. Το <X> είναι αυτού του τύπου, ή ικανοποιεί τον τύπο, αν το κατηγόρημα είναι αληθές γι' αυτό το <X>. Στο RM-ODP τύποι ορίζονται για αντικείμενα, διεπαφές και πράξεις.
- *Πρότυπο <X> (template <X>)*: Οι προδιαγραφές των κοινών χαρακτηριστικών μιας συλλογής απο <X> με τόση λεπτομέρεια ώστε το <X> να μπορεί να υλοποιηθεί απο αυτές. Το <X> μπορεί να είναι οτιδήποτε έχει τύπο.
- *Ρόλος (role)*: αναγνωριστικό μιας συμπεριφοράς που σχετίζεται με τις συνιστώσες ενός σύνθετου αντικειμένου. Ο ρόλος μπορεί να εμφανίζεται ως παράμετρος ενός προτύπου για ένα σύνθετο αντικείμενο.
- *Τομέας <X> (domain <X>)*: Ένα σύνολο απο αντικείμενα, τα οποία είναι συσχετιζόμενα βάσει μιας χαρακτηρίζουσας σχέσης <X> με ένα *αντικείμενο ελέγχου (controlling object)*. Κάθε τομέας έχει ένα αντικείμενο ελέγχου.
- *Συμβόλαιο (contract)*: μια συμφωνία που συντονίζει την συλλογική συμπεριφορά ενός συνόλου αντικειμένων. Ένα συμβόλαιο καθορίζει υποχρεώσεις, δικαιώματα και απαγορεύσεις για τα εμπλεκόμενα αντικείμενα.
- *Υποχρέωση (obligation)*: ο καθορισμός ότι απαιτείται μια συγκεκριμένη συμπεριφορά. Η υποχρέωση ικανοποιείται όταν συντελείται η καθορισμένη συμπεριφορά.
- *Δικαίωμα (permission)*: ο καθορισμός ότι μια συγκεκριμένη συμπεριφορά μπορεί να επιτραπεί. Είναι ισοδύναμο με το να μην υπάρχει υποχρέωση να μην συμβεί η συμπεριφορά.

- *Απαγόρευση (prohibition)*: ο καθορισμός ότι μια συγκεκριμένη συμπεριφορά δεν πρέπει να συμβεί. Είναι ισοδύναμη με το να υπάρχει υποχρέωση να μην συμβεί η συμπεριφορά.
- *Πολιτική (policy)*: ένα σύνολο κανόνων σχετικών με ένα συγκεκριμένο σκοπό. Ένας κανόνας μπορεί να εκφραστεί ως υποχρέωση, δικαίωμα ή απαγόρευση.
- *Κοινότητα (community)*: ένας συνδυασμός αντικειμένων δομημένος ώστε να επιτυγχάνει ένα συγκεκριμένο στόχο. Ο στόχος περιγράφεται ως ένα συμβόλαιο που καθορίζει πως μπορεί να επιτευχθεί ο στόχος αυτός.
- *Ομοσπονδία <X> τομέων (federation of <X> domains)*: μία κοινότητα απο <X> τομείς.

7.3.8.2.2.1.2 Έννοιες όψης πληροφορίας

- *Σταθερό σχήμα (invariant schema)*: ένα σύνολο απο κατηγορήματα για ένα ή περισσότερα αντικείμενα πληροφορίας που πρέπει να αληθεύουν πάντα. Τα κατηγορήματα περιορίζουν τις πιθανές καταστάσεις και αλλαγές καταστάσεων των αντικειμένων στα οποία εφαρμόζονται.
- *Στατικό σχήμα (static schema)*: η προδιαγραφή μιας κατάστασης ενός ή περισσότερων αντικειμένων πληροφορίας, σε κάποια δεδομένη χρονική στιγμή, η οποία υπόκειται στους περιορισμούς ορισμένων σταθερών σχημάτων.
- *Δυναμικό σχήμα (dynamic schema):* η προδιαγραφή των επιτρεπόμενων αλλαγών καταστάσεων ενός ή περισσότερων αντικειμένων πληροφορίας, που υπόκειται στους περιορισμούς ορισμένων σταθερών σχημάτων.

7.3.8.2.2.1.3 Έννοιες υπολογιστικής όψης

- *Σήμα (signal)*: μια ατομική μοιρασμένη πράξη που οδηγεί σε μονόδρομη επικοινωνία απο ένα αντικείμενο που την εκκινεί σε ένα αντικείμενο που την δέχεται.
- *Ανακοίνωση (announcement)*: μια αλληλεπίδραση, η *επίκληση (invocation)*, που εκκινείται απο ένα αντικείμενο «πελάτη» και που οδηγεί στην μεταβίβαση πληροφορίας απο το αντικείμενο αυτό σε ένα αντικείμενο «εξυπηρετητή», ζητώντας απο το αντικείμενο «εξυπηρετητή» να εκτελέσει κάποια συνάρτηση.
- *Ανάκριση (interrogation)*: μια αλληλεπίδραση που αποτελείται απο:
    - Μια αλληλεπίδραση, η επίκληση, που εκκινείται απο ένα αντικείμενο «πελάτη» και που οδηγεί στην μεταβίβαση πληροφορίας απο το αντικείμενο αυτό σε ένα αντικείμενο «εξυπηρετητή», ζητώντας απο το αντικείμενο «εξυπηρετητή να εκτελέσει κάποια συνάρτηση και που συνοδεύεται απο
    - Μια δεύτερη αλληλεπίδραση, ο *τερματισμός (termination)*, η οποία εκκινείται απο το αντικείμενο «εξυπηρετητή» και που οδηγεί στην μεταβίβαση πληροφορίας απο το αντικείμενο αυτό στο αντικείμενο «πελάτη» ως απάντηση στην επίκληση.
- *Λειτουργία (operation)*: μια αλληλεπίδραση ανάμεσα σε ένα αντικείμενο «πελάτη» και ένα αντικείμενο «εξυπηρετητή» που είναι είτε μια ανάκριση (interrogation) ή μια ανακοίνωση (announcement).
- *Ροή (flow)*: μια αφαίρεση μιας σειράς αλληλεπιδράσεων, που οδηγεί στην μεταβίβαση πληροφορίας απο ένα αντικείμενο «παραγωγό» σε ένα αντικείμενο «καταναλωτή» (όπως ορίζονται αυτά στο πρότυπο ITU-T Rec. X.902 I ISOAEC 10746-2).

- *Διεπαφή σημάτων (signal interface)*: μια διεπαφή στην οποία όλες οι αλληλεπιδράσεις είναι σήματα.
- *Διεπαφή λειτουργιών (operation interface)*: μια διεπαφή στην οποία όλες οι αλληλεπιδράσεις είναι λειτουργίες.
- *Διεπαφή ροών (stream interface)*: μια διεπαφή στην οποία όλες οι αλληλεπιδράσεις είναι ροές.

7.3.8.2.2.1.4 Έννοιες όψης μηχανικού

- *Βασικό μηχανικό αντικείμενο (basic engineering object)*: ένα μηχανικό αντικείμενο που απαιτεί την υποστήριξη μιας κατανεμημένης υποδομής.
- *Δέσμη (cluster)*: μια διαμόρφωση απο βασικά μηχανικά αντικείμενα που σχηματίζουν μια μονάδα με σκοπό την απενεργοποίηση, εφαρμογή σημείων ελέγχου, επανενεργοποίηση, ανάκτηση και μεταφορά.
- *Κάψουλα (capsule)*: μια διαμόρφωση μηχανικών αντικειμένων σχηματίζουν μια μονάδα με σκοπό την ενθυλάκωση των διεργασιών και την αποθήκευση.
- *Πυρήνας (nucleus)*: ένα μηχανικό αντικείμενο που συντονίζει τις διεργασίες, την αποθήκευση και τις λειτουργίες επικοινωνιών προκειμένου να χρησιμοποιηθούν απο άλλα μηχανικά αντικείμενα μέσα στον κόμβο στον οποίο ανήκουν.
- *Κόμβος (node)*: μια διαμόρφωση μηχανικών αντικειμένων που σχηματίζουν μια μονάδα με σκοπό την χωρική τοποθέτηση. Ο κόμβος ενσωματώνει ένα σύνολο συναρτήσεων διεργασιών, αποθήκευσης και επικοινωνίας.
- *Στέλεχος (stub)*: ένα μηχανικό αντικείμενο σε ένα κανάλι, το οποίο ερμηνεύει τις αλληλεπιδράσεις που μεταβιβάζονται απο το κανάλι, και επιτελεί οποιουσδήποτε απαραίτητους μετασχηματισμούς ή συντονισμούς επιβάλλονται απο την ερμηνεία.
- *Δεσμευτής (binder)*: ένα μηχανικό αντικείμενο μέσα σε ένα κανάλι, το οποίο διατηρεί μια κατανεμημένη δέσμευση ανάμεσα σε αλληλεπιδρώντα βασικά μηχανικά αντικείμενα.
- *Αναχαιτιστής «Χ» (interceptor «Χ»)*: ένα μηχανικό αντικείμενο σε ένα κανάλι, που τοποθετείται στο σύνορο ανάμεσα σε τομείς «Χ». Ο αναχαιτιστής «Χ»:
    - κάνει ελέγχους για να εφαρμόσει ή να παρακολουθήσει πολιτικές σε επιτρεπόμενες αλληλεπιδράσεις ανάμεσα σε βασικά μηχανικά αντικείμενα διαφορετικών τομέων.
    - κάνει μετατροπές για να αποκρύψει διαφορές στη μετάφραση των δεδομένων απο βασικά μηχανικά αντικείμενα διαφορετικών τομέων.
- *Αντικείμενο πρωτοκόλλου (protocol object)*: ένα μηχανικό αντικείμενο σε ένα κανάλι, που επικοινωνεί με άλλα αντικείμενα πρωτοκόλλου στο ίδιο κανάλι για να επιτευχθεί η αλληλεπίδραση ανάμεσα σε βασικά μηχανικά αντικείμενα (τα οποία ενδέχεται να βρίσκονται σε διαφορετικές δέσμες, κάψουλες ή κόμβους).
- *Κανάλι (channel)*: μια διαμόρφωση απο στελέχη, δεσμευτές, αντικείμενα πρωτοκόλλου και αναχαιτιστές που παρέχουν ένα δέσιμο ανάμεσα σε ένα σύνολο απο διεπαφές στα βασικά μηχανικά αντικείμενα. Μέσα απο το δέσιμο αυτό μπορούν να επιτευχθούν αλληλεπιδράσεις.

7.3.8.2.2.1.5 Έννοιες τεχνολογικής όψης

- *Πρότυπο υλοποίησης (implementable standard)*: ένα πρότυπο για ένα τεχνολογικό αντικείμενο.
- *Υλοποίηση (implementation)*: η διαδικασία πραγμάτωσης, η εγκυρότητα της οποία μπορεί να ελεγχθεί.

7.3.8.2.3 Συναρτήσεις των ODP συστημάτων

Το πρότυπο σκιαγραφεί τις περιγραφές ενός συνόλου *συναρτήσεων (functions)* συστημάτων ODP. Οι συναρτήσεις είναι είτε θεμελιώδεις ή ευρέως εφαρμόσιμες στην κατασκευή συστημάτων ανοιχτών κατανεμημένων. Το σύνολο των συναρτήσεων αυτών χωρίζεται σε τέσσερις ομάδες:

- *Συναρτήσεις διαχείρισης (management functions)*.
- *Συναρτήσεις συντονισμού (coordination functions).*
- *Συναρτήσεις αποθετηρίων (repository functions).*
- *Συναρτήσεις ασφάλειας (security functions).*

Οι περιγραφές των επιμέρους συναρτήσεων που απαρτίζουν κάθε ομάδα δίνονται στη συνέχεια.

7.3.8.2.3.1 Συναρτήσεις διαχείρισης

Οι συναρτήσεις διαχείρισης περιλαμβάνουν:

- Την *συνάρτηση διαχείρισης κόμβου (node management function)*, η οποία παρέχεται απο τον πυρήνα ενός κόμβου και είναι υπεύθυνη για τον έλεγχο των συναρτήσεων διεργασίας, αποθήκευσης και επικοινωνίας εντός του κόμβου. Πιο συγκεκριμένα ασχολείται με την διαχείριση «νημάτων» διεργασιών, την δημιουργία καναλιών και την διαχείριση διεπαφών, την δημιουργία και διαγραφή κάψουλων.
- Την *συνάρτηση διαχείρισης αντικειμένων (object management function)*, η οποία παρέχεται όπου απαιτείται απο ένα αντικείμενο και επιτρέπει την παρακολούθηση *σημείων ελέγχου (checkpoints)* και την διαγραφή αντικειμένων.
- Την *συνάρτηση διαχείρισης δεσμών (cluster management function)*, η οποία παρέχεται απο έναν διαχειριστή δέσμης και επιτρέπει την παρακολούθηση σημείων ελέγχου, την ανάκαμψη, την μετανάστευση, την απενεργοποίηση ή την διαγραφή μιας δέσμης.
- Την *συνάρτηση διαχείρισης κάψουλων (capsule management function)*, η οποία παρέχεται απο έναν διαχειριστή κάψουλας και επιτρέπει την δημιουργία (συμπεριλαμβανόμενων της ανάκαμψης και της επανενεργοποίησης), την παρακολούθηση σημείων ελέγχου, την απενεργοποίηση και την διαγραφή όλων των δεσμών σε μια κάψουλα, καθώς και την διαγραφή της ίδιας της κάψουλας.

7.3.8.2.3.2 Συναρτήσεις συντονισμού

Οι συναρτήσεις συντονισμού περιλαμβάνουν:

- Την *συνάρτηση ειδοποίησης γεγονότων (event notification function)*, η οποία καταγράφει και καθιστά διαθέσιμα τα ιστορικά γεγονότων.

- Την *συνάρτηση παρακολούθησης σημείων ελέγχου και ανάκαμψης (checkpoint and recovery function)*, η οποία συντονίζει την παρακολούθηση σημείων ελέγχου δεσμών και την ανάκαμψη δεσμών απο αποτυχίες βάσει των σημείων αυτών. Ο καθορισμός των σημείων αυτός γίνεται βάσει αντίστοιχων πολιτικών.
- Την *συνάρτηση απενεργοποίησης και επανενεργοποίησης (deactivation and reactivation function)*, η οποία συντονίζει την απενεργοποίηση και την επανενεργοποίηση δεσμών. Οι δραστηριότητες αυτές γίνονται βάσει πολιτικών. Οι πολιτικές αυτές ορίζουν και το πότε θα πρέπει να αποθηκεύονται τα σχετικά σημεία ελέγχου.
- Την *συνάρτηση ομαδοποίησης (group function)*, η οποία παρέχει τους απαραίτητους μηχανισμούς για τον συντονισμό των αλληλεπιδράσεων αντικειμένων σε μια *δέσμευση πολλαπλών μερών (multiparty binding)*.
- Την *συνάρτηση αντιγραφής (replication function)*, η οποία είναι υπεύθυνη για την ειδική περίπτωση μιας ομάδας όπου τα αντικείμενα είναι συμβατά απο άποψη συμπεριφοράς. Παρέχει τους μηχανισμούς που εξασφαλίζουν ότι η ομάδα εμφανίζεται προς άλλα αντικείμενα σαν να ήταν ένα αντικείμενο και συντονίζει την προσθήκη και αφαίρεση μελών της ομάδας.
- Την *συνάρτηση μετανάστευσης (migration function)*, η οποία συντονίζει την μετανάστευση μιας δέσμης απο μια κάψουλα σε μια άλλη. Λειτουργεί είτε αντιγράφοντας την δέσμη, χρησιμοποιώντας την συνάρτηση αντιγραφής, είτε απενεργοποιώντας την δέσμη και επανενεργοποιώντας την στη νέα τοποθεσία, χρησιμοποιώντας την συνάρτηση απενεργοποίησης και επανενεργοποίησης.
- Την *συνάρτηση συναλλαγών (transaction function)*, η οποία συντονίζει και ελέγχει ένα σύνολο απο συναλλαγές προκειμένου να επιτύχει το επιθυμητό επίπεδο ορατότητας και σταθερότητας σύμφωνα με τις αντίστοιχες πολιτικές. Μια συναλλαγή ACID είναι μια ειδική περίπτωση της συνάρτησης συναλλαγής.
- Την συνάρτηση παρακολούθησης αναφορών διεπαφών μηχανικών αντικειμένων (engineering interface reference tracking function), η οποία παρακολουθεί την μεταφορά αναφορών σε διεπαφές ανάμεσα σε μηχανικά αντικείμενα σε διαφορετικές δέσμες, προκειμένου να καθορίζεται πότε δεν χρειάζεται πλέον η υποστηρίζουσα υποδομή για την αναφορά, επειδή δεν μπορεί κάποιο αντικείμενο ή δέσμη να δεσμευτεί πλέον με τη συγκεκριμένη διεπαφή.

7.3.8.2.3.3 Συναρτήσεις αποθετηρίων

Οι συναρτήσεις αποθετηρίων περιλαμβάνουν:

- Την *συνάρτηση αποθήκευσης (storage function)*, η οποία αποθηκεύει δεδομένα.
- Την *συνάρτηση οργάνωσης πληροφορίας (information organization function)*, η οποία διαχειρίζεται ένα αποθετήριο πληροφορίας που περιγράφεται απο ένα σχήμα και επιτρέπει την τροποποίηση και ενημέρωση τόσο του σχήματος όσο και των ίδιων των δεδομένων, καθώς και την διενέργεια ερωτήσεων στο αποθετήριο.
- Την *συνάρτηση επανατοποθέτησης (relocation function)*, η οποία διαχειρίζεται ένα αποθετήριο με αναφορές για τις θέσεις διεπαφών και επιμέρους διαχειριστικές συναρτήσεις για δέσμες που υποστηρίζουν αυτές τις διεπαφές.
- Την *συνάρτηση αποθετηρίου τύπων (type repository function)*, η οποία διαχειρίζεται ένα αποθετήριο με προδιαγραφές τύπων και σχέσεις τύπων.

- Την *συνάρτηση αγοραπωλησίας (trading function)*, η οποία υποστηρίζει την εξαγωγή προσφορών υπηρεσιών υπο την έννοια της πληροφορίας για τις διεπαφές στις οποίες προσφέρεται μια υπηρεσία, και την εισαγωγή απο χρήστες της υπηρεσίας σύμφωνα με συγκεκριμένες προδιαγραφές.

7.3.8.2.3.4 Συναρτήσεις ασφάλειας

Οι συναρτήσεις ασφάλειας καλύπτουν τις απαιτήσεις για εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα και ελεγξιμότητα. Περιλαμβάνουν:

- Την *συνάρτηση ελέγχου πρόσβασης (access control function)*, η οποία αποτρέπει τις μη εξουσιοδοτημένες αλληλεπιδράσεις με ένα αντικείμενο.
- Την *συνάρτηση ελέγχων ασφάλειας (security audit function)*, η οποία παρακολουθεί και συλλέγει πληροφορίες για τις σχετικές με ασφάλεια πράξεις στην αρχιτεκτονική, και επιτρέπει την ανάλυση της πληροφορίας για την εξέταση πολιτικών, ελέγχων και διαδικασιών.
- Την *συνάρτηση αυθεντικοποίησης (authentication function)*, η οποία παρέχει επιβεβαίωση της δηλωθείσας ταυτότητας για ένα αντικείμενο.
- Την *συνάρτηση ακεραιότητας (integrity function)*, η οποία αναγνωρίζει και/ή αποτρέπει την μη εξουσιοδοτημένη δημιουργία, μεταβολή ή διαγραφή δεδομένων.
- Την *συνάρτηση εμπιστευτικότητας (confidentiality function)*, η οποία αποτρέπει την μη εξουσιοδοτημένη αποκάλυψη πληροφορίας.
- Την *συνάρτηση εξασφάλισης της μη άρνησης συμμετοχής (non-repudation function)*, η οποία αποτρέπει ένα αντικείμενο σε μια αλληλεπίδραση απο το να αρνηθεί την συμμετοχή του στην αλληλεπίδραση.
- Την *συνάρτηση διαχείρισης κλειδιών (key management function)*, η οποία παρέχει δυνατότητες για την διαχείριση κρυπτογραφικών κλειδιών.

Οι συναρτήσεις μπορούν να εφαρμοστούν και σε αντικείμενα και στις αλληλεπιδράσεις μεταξύ αντικείμενων.

7.3.8.2.4 Διαφάνειες κατανομής

Οι *διαφάνειες κατανομής* επιτρέπουν την απόκρυψη της πολυπλοκότητας που σχετίζεται με την κατανομή του συστήματος απο εφαρμογές όταν αυτή είναι άσχετη με τους στόχους της ίδιας της εφαρμογής. Για παράδειγμα:

- Η *διαφάνεια πρόσβασης (access transparency)* αποκρύπτει τις διαφορές στην αναπαράσταση δεδομένων και τους μηχανισμούς κλήσης για υπηρεσίες ανάμεσα σε συστήματα.
- Η *διαφάνεια αποτυχίας (failure transparency)* αποκρύπτει απο ένα υπολογιστικό αντικείμενο την αποτυχία και πιθανή ανάνηψη άλλων υπολογιστικών αντικείμενων ή το ίδιο το αντικείμενο. Μπορεί να υλοποιηθεί με μια εξειδικευμένη υποδομή γι' αυτό το σκοπό. Διαφορετικά υποστηρίζεται απο τις συναρτήσεις σημείου ελέγχου και ανάνηψης ή απο την συνάρτηση αντιγραφής σε συνδυασμό με την συνάρτηση επαναποτοποθέτησης.
- Η *διαφάνεια τοποθεσίας (location transparency)* αποκρύπτει την ανάγκη μιας εφαρμογής να γνωρίζει πληροφορίες τοποθεσίας μιας υπηρεσίας προκειμένου να την

καλέσει. Αυτό προϋποθέτει ότι οι διεπαφές αντικειμένων μπορούν να αναγνωριστούν οικουμενικά στην αρχιτεκτονική.

- Η *διαφάνεια μετανάστευσης (migration transparency)* αποκρύπτει απο ένα υπολογιστικό αντικείμενο το γεγονός ότι έχει μετακινηθεί. Υποστηρίζεται απο μια συνάρτηση μετανάστευσης.
- Η *διαφάνεια σταθερής αποθήκευσης (persistence transparency)* αποκρύπτει απο υπολογιστικά αντικείμενα την κατανομή και αποδέσμευση πόρων σε δέσμες. Υποστηρίζεται απο τις συναρτήσεις ενεργοποίησης και απενεργοποίησης.
- Η *διαφάνεια επανατοποθέτησης (relocation transparency)* αποκρύπτει απο ένα υπολογιστικό αντικείμενο το γεγονός ότι οι διεπαφές με τις οποίες επικοινωνεί έχουν αλλάξει θέση. Υποστηρίζεται απο μια συνάρτηση επανατοποθέτησης.
- Η *διαφάνεια αντιγραφής (replication transparency)* αποκρύπτει το γεγονός ότι υπάρχουν πολλαπλά αντίγραφα μιας υπηρεσίας προκειμένου να παρέχεται αξιοπιστία και διαθεσιμότητα.
- Η *διαφάνεια συναλλαγής (transaction transparency)* χρειάζεται λόγω της πολυπλοκότητας που επιφέρει το γεγονός ότι ο συντονισμός συναλλαγών εμπλέκει τον προγραμματισμό, την παρακολούθηση και την ανάνηψη των πράξεων εντός των συναλλαγών αυτών. Για να επιτευχθεί ο απαραίτητος έλεγχος απαιτείται αλληλεπίδραση ανάμεσα στα υπολογιστικά αντικείμενα που συμμετέχουν στις πράξεις μιας συναλλαγής και τα υπολογιστικά αντικείμενα που πραγματοποιούν την συνάρτηση συναλλαγής. Οι διεργασίες συναλλαγών είναι εξαιρετικά πολύπλοκες και είναι γενικά ανεπιθύμητη η εμπλοκή του ελέγχου τους στην λειτουργικότητα των σχεδιαζόμενων εφαρμογών. Η διαφάνεια συναλλαγής λοιπόν αποτελεί την παροχή μιας αυτόματης διαδικασίας που μετατρέπει τις προδιαγραφές της υπολογιστικής όψης με έλεγχο συναλλαγών σε προδιαγραφές χωρίς έλεγχο συναλλαγών.

Όπως φαίνεται απο τα παραπάνω, η υλοποίηση των διαφανειών κατανομής στηρίζεται απο τις συναρτήσεις της προηγούμενης παραγράφου. Παρ' όλα αυτά, υπάρχουν διάφορα κόστη στην απόδοση του συστήματος που σχετίζονται με κάθε διαφάνεια και μόνο επιλεγμένες διαφάνειες είναι απαραίτητες σε κάθε περίπτωση. Γι' αυτό το λόγο, ένα σύστημα που συμμορφώνεται στο πρότυπο δεν είναι απαραίτητο να υλοποιεί όλα τα είδη διαφανειών.

7.3.8.2.5 Συμμόρφωση προς τις προδιαγραφές

Τα βασικά χαρακτηριστικά ετερογένειας και εξέλιξης υπονοούν ότι διαφορετικά μέρη ενός κατανεμημένου συστήματος μπορούν να ληφθούν ξεχωριστά, απο διαφορετικές οντότητες. Είναι λοιπόν πολύ σημαντικό οι συμπεριφορές των διαφορετικών μερών του συστήματος να είναι σαφώς ορισμένες και να είναι δυνατόν να αποδίδεται ευθύνη για κάθε αποτυχία του συστήματος να συμμορφωθεί στις προδιαγραφές του.
Η συμμόρφωση προς τις προδιαγραφές (conformance) είναι ένα σύνολο δηλώσεων που αναγνωρίζουν *σημεία συμμόρφωσης (conformance points)* στις προδιαγραφές του σχεδιαζόμενου συστήματος και την συμπεριφορά που πρέπει να ικανοποιείται στα σημεία αυτά. Τα σημεία συμμόρφωσης πρόκειται να ελεγχθούν κατά τον έλεγχο του συστήματος, κατά την διάρκεια της υλοποίησης και της λειτουργίας του.

Το πλαίσιο που καθορίζεται απο το πρότυπο για την αξιολόγηση της συμμόρφωσης προς τις προδιαγραφές (που προκύπτουν με εφαρμογή των αρχών του προτύπου) αντιμετωπίζει αυτά τα θέματα. Το πλαίσιο αυτό καλύπτει:

- Την αναγνώριση σημείων συμμόρφωσης μέσα στα σύνολα των όψεων στα οποία μπορούν να γίνουν παρατηρήσεις συμμόρφωσης.
- Τον καθορισμό των κλάσεων ενός σημείου συμμόρφωσης.
- Τις προδιαγραφές της φύσης των δηλώσεων συμμόρφωσης που γίνονται σε κάθε όψη και τις σχέσεις που υπάρχουν μεταξύ τους.

Σε κάθε επίπεδο αφαίρεσης, ένας έλεγχος (test) είναι μια σειρά απο παρατηρούμενες επιδράσεις και γεγονότα, που διαδραματίζονται σε προδιαγεγραμμένα σημεία, τα οποία ονομάζονται *σημεία αναφοράς (reference points)*. Τα σημεία αναφοράς αποτελούν προσβάσιμες διεπαφές. Ένα στοιχείο του συστήματος για το οποίο ελέγχεται η συμμόρφωση μελετάται ως «μαύρο κουτί», το οποίο ελέγχεται μόνο στις εξωτερικές του συνδέσεις.
Ένα σημείο συμμόρφωσης αποτελεί ένα σημείο αναφοράς στο οποίο μπορεί να γίνει ένας έλεγχος για να αποφανθεί κάποιος αν το σύστημα ικανοποιεί ένα σύνολο απο κριτήρια συμμόρφωσης. Μια δήλωση συμμόρφωσης πρέπει να αναγνωρίζει πού βρίσκονται τα σημεία συμμόρφωσης και ποια κριτήρια πρέπει να ικανοποιούνται σε αυτά τα σημεία. Στο πρότυπο ορίζονται τέσσερις κατηγορίες σημείων αναφοράς στα οποία μπορούν να διεξαχθούν έλεγχοι συμμόρφωσης:

- *Προγραμματιστικό σημείο αναφοράς (Programmatic reference point):* Ένα σημείο αναφοράς στο οποίο μια προγραμματιστική διεπαφή μπορεί να εδραιωθεί για να επιτρέψει την πρόσβαση σε μια συνάρτηση / μέθοδο. Μια προγραμματιστική απαίτηση συμμόρφωσης δηλώνεται έχοντας στο μυαλό την συμβατότητα ως προς την συμπεριφορά της διεπαφής, στην περίπτωση που το αντικείμενο που την εκθέτει αλλάξει.
- *Αντιληπτικό σημείο αναφοράς (Perceptual reference point):* Αποτελεί σημείο αναφοράς στο οποίο συντελείται μια αλληλεπίδραση ανάμεσα στο σύστημα και τον φυσικό κόσμο.
- *Διαλειτουργικό σημείο αναφοράς (Interworking reference point):* Ένα σημείο αναφοράς στο οποίο μια διεπαφή μπορεί να εδραιωθεί προκειμένου να επιτραπεί η επικοινωνία ανάμεσα σε δύο η περισσότερα συστήματα. Μια διαλειτουργική απαίτηση συμμόρφωσης δηλώνεται σε σχέση με την ανταλλαγή πληροφορίας ανάμεσα σε δύο ή περισσότερα συστήματα. Η διαλειτουργική συμμόρφωση περιλαμβάνει την διασύνδεση σημείων αναφοράς.
- *Σημείο αναφοράς συνδιαλλαγής (Interchange reference point):* Αποτελεί ένα σημείο αναφοράς στο οποίο μπορεί να εισαχθεί στο σύστημα ένα εξωτερικό μέσο αποθήκευσης. Μια απαίτηση συμμόρφωσης συνδιαλλαγής δηλώνεται σε σχέση με την συμπεριφορά (μέθοδοι και μορφές πρόσβασης) κάποιου φυσικού μέσου ώστε να καταγράφεται πληροφορία σε ένα σύστημα και να μπορεί να μεταφερθεί σε ένα άλλο.

Η *διαδικασία ελέγχου της συμμόρφωσης (conformance testing)* χρησιμοποιεί τα σημεία συμμόρφωσης που έχουν οριστεί στις προδιαγραφές, βάσει των παραπάνω σημείων αναφοράς.

7.4 Αναφορές

[DES] US Department of Commerce. (1999). "Data Encryption Standard". *Federal Information Processing Standards Publication-FIPS PUB 46-3*.

[Barker04] W. C. Barker. (2004). "Recommendation for the Triple Data Encryption Algorithm Block Cipher". *NIST*.

[AES] NIST. (2001). "Advanced Encryption Standard (AES)". *Federal Information Processing Standards Publication-FIPS PUB 197*.

[Kaliski98] B. Kaliski, S. Staddon. (1998). "RFC 2437 - PKCS #1: RSA Cryptography Specifications Version 2.0". *RSA Laboratories.*

[DH] RSA Laboratories. (1993). "Diffie-Hellman Key-Agreement Standard, Version 1.4". PKCS #3.

[Kaliski92] B.S. Kaliski. (1992). *"*RFC 1319: The MD2 Message-Digest Algorithm*"*. *RSA Laboratories*.

[Rivest92] R.L. Rivest. (1992). *"*RFC 1321: The MD5 Message-Digest Algorithm". *Internet Activities Board*.

[Eastlake01] D. Eastlake, P. Jones. (2001). "RFC 3174 - US Secure Hash Algorithm 1 (SHA1)".

[Feistel88] M. Luby, C. Rackoff. (1988). "How to Construct Pseudorandom Permutations and Pseudorandom Functions". In *SIAM J. Comput.,* vol. 17, 1988, pp. 373-386.

[Vernam] Gilbert S. Vernam, "Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications". Journal of the IEEE, Vol 55, pp109-115

[Kelsey96] J. Kelsey, B. Schneier, D. Wagner. (1996). "Key-Schedule Cryptanalysis of 3-WAY, IDEA, G-DES, RC4, SAFER, and Triple-DES". *Advances in Cryptology-CRYPTO '96 Proceedings*, Springer-Verlag (1996), 237-251.

[Coppersmith93] D. Coppersmith, H. Krawczyk, Y. Mansour. (1993). "The shrinking generator". *In Advances in Cryptology,* Proc. CRYPTO `93, 1994, pp. 22--39.

[Metzger95] P. Metzger, W. Simpson. (1995). "IP Authentication using Keyed MD5". *RFC 1828*.

[Lai92] Lai XJ, RA Rueppel, J Woolven, (1992). "A Fast Cryptographic Checksum Algorithm Based on Stream Ciphers". *In Proceedings of Auscrypt 92*.

[ASCII] International Organization for Standardization. (1975). "The set of control characters for ISO 646". *Internet Assigned Numbers Authority Registry*.

[Freed96] N. Freed, N. Borenstein. (1996). "RFC 2045 - Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies". (Obsoletes RFC 1521, RFC 1522, RFC 1590) (Updated by RFC 2184, RFC 2231)

[Callas98] J. Callas, L. Donnerhacke, H. Finney, R. Thayer. (1998). "RFC 2440 – OpenPGP Message Format".

[Housley02] R. Housley, W. Polk, W. Ford, D. Solo. (2002). "RFC 3280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[Hodges02] J. Hodges, R. Morgan. (2002). "RFC 3377 – Lightweight Directory Access Protocol (v3): Technical Specification".

[Bray00] T. Bray et al. (2000). ”Extensible Markup Language (XML) 1.0 (Second Edition)”. http://www.w3.org/TR/2000/REC-xml-20001006
[Fallside04] D. C. Fallside, P. Walmsley. (2004). “XML Schema Part 0: Primer Second Edition”. http://www.w3.org/TR/2004/REC-xmlschema-0-20041028
[Hughes02] M. Hughes, T. Imamura, H. Maruyama. (Editors). (2002). “Decryption Transform for XML Signature”. W3C Recommendation, http://www.w3.org/TR/xmlenc-decrypt
[ETSI101733] ETSI Technical Specification. (2002). “Electronic signature and infrastructures; Electronic signature formats“. ETSI TS 101 733 V1.4.0, http://portal.etsi.org
[XAdES02] ETSI Technical Specification. (2002). “ETSI TS 101 903 V1.1.1 - XML Advanced Electronic Signatures (XAdES)”.
[ASN.1] ISO. (2002). Abstract Syntax Notation One (ASN.1), Specification of Basic Notation
ITU-T Rec. X.680 (2002) | ISO/IEC 8824-1:2002
[Myers99] M. Myers et al. (Editors). (1999). “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP”. RFC 2560, http://rfc.net/rfc2560.html
[Freeman06] T. Freeman et. al. (2006). “Standard Certificate Validation Protocol (SCVP)”. Internet draft, http://www.ietf.org/internet-drafts/draft-ietf-pkix-scvp-23.txt
[Mitra03] N. Mitra. (Editor). (2003). “SOAP version 1.2 Part0: Primer”. W3C Recommendation, http://www.w3.org/TR/soap12-part0/
[Klyne04] G. Klyne, J. J. Carroll. (Editors). (2004). “Resource Description Framework (RDF): Concepts and Abstract Syntax”. W3C Recommendation, http://www.w3.org/TR/2004/REC-rdf-concepts-20040210/
[Postel82] J. B. Postel. (1982). “Simple mail transfer protocol”. IETF RFC 821, http://www.ietf.org/rfc/rfc0821.txt
[Postel85] J. Postel. (1985). “File transfer protocol (FTP)”. IETF RFC 959, http://www.ietf.org/rfc/rfc959.txt
[Christensen01] E. Christensen et al. (2001). “Web Services Description Language (WSDL) 1.1”. W3C Note, http://www.w3.org/TR/wsdl
[Clement04] L. Clement et al. (Editors). (2004). “UDDI Version 3.0.2”. OASIS UDDI Spec Technical Committee Draft http://uddi.org/pubs/uddi-v3.0.2-20041019.htm
[Hallam-Baker05] P. Hallam-Baker, S. H. Mysore. (Editors). (2005). “XML Key Management Specification (XKMS 2.0) Version 2.0”. W3C Recommendation, http://www.w3.org/TR/xkms2/
[Cantor05] S. Cantor et al. (Editors). (2005). “Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0”. OASIS Standard, http://docs.oasis-open.org/security/saml/v2.0/
[Lorch03] M. Lorch, D. Kafura, S. Shah. (2003). “An XACML-based policy management and authorization service for globus resources”. Proceedings of Fourth International Workshop on Grid Computing, pp. 208- 210
[Moses05] T. Moses. (Editor). (2005). “eXtensible Access Control Markup Language (XACML) Version 2.0”. OASIS Standard, http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf
[Nadalin06] A. Nadalin et al. (Editors). (2006). “Web Services Security: SOAP Message Security 1.1”. OASIS Standard Specification, http://docs.oasis-open.org/wss/v1.1/

[Neuman94] B. C. Neuman, T. Ts'o. (1994). “Kerberos: An Authentication Service for Computer Networks”. *IEEE Communications*, 32(9):33-38. September 1994