ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Ασφαλής διαχείριση σημασιολογικά συνδεδεμένων ψηφιακών αντικειμένων σε ετερογενή κατανεμημένα περιβάλλοντα

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Αζίζ Σ. Μούσας

Αθήνα, Σεπτέμβριος 2014

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Ασφαλής διαχείριση σημασιολογικά συνδεδεμένων ψηφιακών αντικειμένων σε ετερογενή κατανεμημένα περιβάλλοντα

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Αζίζ Σ. Μούσας

Συμβουλευτική Επιτροπή: Δήμητρα-Θεοδώρα Ι. Κακλαμάνη
Ιάκωβος Στ. Βενιέρης
Νικόλαος Κ. Ουζούνογλου

Εγκρίθηκε από την επταμελή εξεταστική επιτροπή την

.....	.....	.....
Δ.-Θ. Ι. Κακλαμάνη Καθηγήτρια Ε.Μ.Π.	Ι. Στ. Βενιέρης Καθηγητής Ε.Μ.Π.	Ν. Κ. Ουζούνογλου Καθηγητής Ε.Μ.Π.
.....	.....	.....
Κ. Κοντογιάννης Αναπληρωτής Καθηγητής Ε.Μ.Π.	Χ. Ζ. Πατρικάκης Επίκουρος Καθηγητής Τ.Ε.Ι. Πειραιά	Α.-Γ. Σταφυλοπάτης Καθηγητής Ε.Μ.Π.

.....
Χ. Δουληγέρης
Καθηγητής Παν. Πειραιώς

Αθήνα, Σεπτέμβριος 2014

.....
Αζίζ Σ. Μούσας
Διδάκτωρ Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Στην οικογένειά μου

Περίληψη

Η πρόοδος των Τεχνολογιών Πληροφορίας και Επικοινωνίας έχει δώσει την ώθηση για την ανάπτυξη και παροχή προηγμένων ηλεκτρονικών υπηρεσιών μέσω των οποίων καθίσταται δυνατή η ανταλλαγή κάθε είδους πληροφορίας. Κεντρική θέση στο διαδίκτυο έχουν πλέον το περιεχόμενο και οι υπηρεσίες μέσω των οποίων δίνεται η πρόσβαση σε αυτό, παρά οι κόμβοι που το αποτελούν. Παράλληλα, το μοντέλο παραγωγού-καταναλωτή πληροφορίας αναβαθμίζεται, με τους ρόλους να μην είναι τόσο διακριτοί, ενώ η μαζική παραγωγή πληροφοριών καθιστά δυνατή τη δημιουργία συναρπαστικών εφαρμογών που συνδυάζουν περιεχόμενο από διαφορετικές πηγές. Ωστόσο, το αναγκαίο βήμα για την περαιτέρω αλληλεπίδραση μεταξύ εταιριών, οργανισμών, χρηστών και περιεχομένου αφορά στη διασφάλιση των δεδομένων που διαμοιράζουν και των υπηρεσιών που τα παρέχουν.

Σε αυτό το πλαίσιο, με τις ανάγκες των τελικών χρηστών και των παραγωγών περιεχομένου να συγκλίνουν όλο και περισσότερο, βασικό ρόλο στην σημερινή επανάσταση των μέσων κατέχει η ευρεία υιοθέτηση διεθνών προτύπων. Η παρούσα διατριβή, ξεκινώντας από αυτή τη διαπίστωση, εξετάζει ζητήματα διαλειτουργικότητας στις δομές δεδομένων που ανταλλάσσονται μεταξύ διαφορετικών συστημάτων, στις πολιτικές προστασίας τους, αλλά και στην ελεγχόμενη πρόσβαση στις υπηρεσίες που τα προσφέρουν. Στη συνέχεια, προτείνει λύσεις οι οποίες βασίζονται στα διεθνή πρότυπα MPEG-21 και MPEG-M και ενισχύουν τη συνεργασία μεταξύ πληροφοριοκεντρικών εφαρμογών που δραστηριοποιούνται σε ετερογενή κατανεμημένα περιβάλλοντα.

Ειδικότερα, σε ότι αφορά τη διαλειτουργικότητα των δομών δεδομένων, στο πλαίσιο της διατριβής αξιολογείται η χρήση των ψηφιακών αντικειμένων του προτύπου MPEG-21 και προτείνεται μηχανισμός για την σημασιολογική συσχέτιση τους. Παράλληλα, εξετάζονται τα ζητήματα σημασιολογικής διαλειτουργικότητας τα οποία εγείρονται σε ετερογενή περιβάλλοντα και προτείνεται σύστημα για την υποστήριξη της το οποίο βασίζεται στη δομή των λεξικών διαλειτουργικότητας.

Όσον αφορά στη διαλειτουργικότητα των πολιτικών ασφαλείας και της προστασίας του ανταλλασσόμενου περιεχομένου, αναλύονται οι τρέχουσες τάσεις στον έλεγχο πρόσβασης σε ψηφιακό περιεχόμενο και προτείνεται σύστημα το οποίο ενοποιεί την πλατφόρμα του προτύπου MPEG-M με τις υποδομές της καινοτόμου μεθόδου Κρυπτογραφίας Βάσει Χαρακτηριστικών (ΚΒΧ).

Όσον αφορά στη διαλειτουργικότητας στον έλεγχο πρόσβασης των υπηρεσιών που προσφέρουν τα δεδομένα, αναλύονται οι υπάρχουσες λύσεις και οι περιορισμοί τους. Στη συνέχεια, προτείνεται σύστημα έλεγχου πρόσβασης διαδικτυακών υπηρεσιών τύπου REST, το οποίο κάνει χρήση ψηφιακών αντικειμένων για την περιγραφή της διεπαφής τους, ενώ τα δικαιώματα χρήσης των μεθόδων της διεπαφής περιγράφονται με την μορφή αδειών χρήσης. Οι τελευταίες επιβάλλονται με τη χρήση ΚΒΧ, δίνοντας πρόσβαση μονάχα στους εξουσιοδοτημένους χρήστες.

Τέλος, η διατριβή ολοκληρώνει το θεωρητικό πλαίσιο αξιολόγησης των προτεινόμενων μοντέλων συνεργασίας πληροφοριοκεντρικών εφαρμογών που δραστηριοποιούνται σε ετερογενή κατανεμημένα περιβάλλοντα, με την παρουσίαση ενός ολοκληρωμένου παραδείγματος χρήσης. Το παράδειγμα προέρχεται από τις ανάγκες του χώρου της υγείας και παρουσιάζει μια ολοκληρωμένη υπηρεσία διαχείρισης προσωπικών ιατρικών δεδομένων με ασφάλεια πάνω από περιβάλλον κινητού και διάχυτου υπολογισμού.

Λέξεις κλειδιά: Σημασιολογική διαλειτουργικότητα, προστασία περιεχομένου, κρυπτογραφία βάσει χαρακτηριστικών, διαδικτυακές υπηρεσίες REST, πρότυπες τεχνολογίες μεσισμικού.

Abstract

The advancement of Information and Communication Technologies has provided the basis for the development and delivery of advanced electronic services over which, massive information covering a wide range od topics can be exchanged. At the same time, the needs of information producers and consumers are converging and the mass generation of content enables the introduction of exciting applications that can exploit content from different sources. However, a necessary step for the further interaction between companies, organizations, users and the content itself, is the protection of both the shared data and the corresponding services.

In this context of rapid convergence of end users and content producers needs, essential role in today's media revolution holds the widespread adoption of international standards. Starting from the above observations, this dissertation examines interoperability issues at the level of data structures that are exchanged between heterogeneous systems, as well as the level of content protection policies, and access control mechanisms for content distribution services. Subsequently, solutions based on the MPEG-21 and MPEG-M international standards which strengthen the cooperation between content-centric applications that operate in heterogeneous distributed environments are proposed.

Specifically, regarding data structures interoperability, the dissertation evaluates the use of digital items of the MPEG-21 standard, and proposes a mechanism for their semantic linking. Additionaly, it examines the semantic interoperability issues that arise in heterogeneous environments and proposes a system for its support based on the underlying structure of the interoperability lexicons.

Regarding security policies and content protection interoperability it analyzes current trends in access control of digital content and proposes a system that unifies the MPEG-M standard platform with the infrastructure of the innovative Attribute-based Encryption cryptographic method (ABE).

Regarding the interoperability of access control methods of content distribution services, the dissertation analyzes existing solutions and their limitations and proposes an access control system for RESTful web services, which makes use of Digital Items for describing their interface and licenses for describing user rights on the methods of the interface. The latter are enforced by employing Attribute Based Encryption (ABE), enabling access only to authorized users.

The Dissertation concludes the theoretical framework for the assessment of the proposed cooperation models of content-centric applications operating in heterogeneous distributed environments, by presenting a complete use case scenario. The scenario stems from the needs of healthcare services and presents an integrated service for the secure management of personal medical records over pervasive mobile computing environments.

Keywords: Semantic interoperability, content protection, attribute-based encryption, RESTful web services, standard middleware technologies.

Ευχαριστίες

Η παρούσα διατριβή αποτελεί το επιστέγασμα της ερευνητικής μου δραστηριότητας στο Εργαστήριο Ευφυών Επικοινωνιών και Δικτύων Ευρείας Ζώνης του ΕΜΠ. Όλο αυτό το διάστημα, είχα τη χαρά και την τιμή να γνωρίσω και να συνεργαστώ με πολλούς ανθρώπους, τους οποίους θα ήθελα σε αυτό το σημείο να ευχαριστήσω για τη στήριξη, την καθοδήγηση και τη βοήθειά τους.

Αρχικά, θα ήθελα να ευχαριστήσω την επιβλέπουσα καθηγήτρια μου κύρια Δήμητρα - Θεοδώρα Κακλαμάνη, Καθηγήτρια ΕΜΠ, για την εμπιστοσύνη της στις ικανότητές μου, τις ευκαιρίες που μου έδωσε να ασχοληθώ με ενδιαφέροντα ερευνητικά θέματα, την καθοδήγηση, την υποστήριξη και την πίστη της σε μένα. Στη συνέχεια, τον κύριο Ιάκωβο Βενιέρη, Καθηγητή ΕΜΠ, για τη στήριξή του, τις συμβουλές του και την άψογη συνεργασία που είχαμε όλα αυτά τα χρόνια. Επίσης, θα ήθελα να ευχαριστήσω τον κύριο Χαράλαμπο Πατρικάκη, Επίκουρο Καθηγητή ΤΕΙ Πειραιά, για τη στενή συνεργασία και τη βοήθεια που μου προσέφερε. Επιπλέον, τον κύριο Νικόλαο Ουζούνογλου, Καθηγητή ΕΜΠ, και τον κύριο Κωνσταντίνο Κοντογιάννη, Αναπληρωτή Καθηγητή ΕΜΠ, που πάντοτε ευγενικοί στήριξαν τις προσπάθειές μου. Τέλος, θερμές ευχαριστίες στον κύριο Ανδρέα-Γεώργιο Σταφυλοπάτη, Καθηγητή ΕΜΠ, και τον κύριο Χρήστο Δουληγέρη, Καθηγητή Πανεπιστημίου Πειραιώς, που μου έκαναν την τιμή να συμπεριληφθούν στην επταμελή επιτροπή μου και να αξιολογήσουν το έργο μου.

Ένα μεγάλο ευχαριστώ οφείλω στον Άγγελο-Χρήστο Αναδιώτη για τη συνεργασία, την κατανόησή του και πάνω από όλα επειδή ήξερα ότι μπορώ να βασιστώ πάνω του. Όλα κύλισαν σύμφωνα με το κρυφό του σχέδιο για εμένα. Στο Γιώργο Λιουδάκη, που παρακολουθούσε σιωπηρά τη διαδρομή μου και ήταν πάντα εκεί όταν χρειάστηκα τη βοήθεια του για οποιονδήποτε λόγο. Στον Χρίστο Παππά, με τον οποίο υπήρχε πάντα κάτι ενδιαφέρον να συζητήσουμε, είτε όντας στο διπλανό γραφείο είτε στη διαδρομή προς το εργαστήριο. Στον Νίκο Δέλλα, ο οποίος μου έμαθε πως να γράφω σωστό κώδικα. Στον Φώτη Γώγουλο και την Άννα Αντωνακοπούλου για την καλύτερη ίσως από πολλές πλευρές συνεργασία που είχα αυτά τα χρόνια. Στον Παναγίωτη Γκόνη για την ευχάριστη συνεργασία και τις συμβουλές του. Μαζί με τους προαναφερθέντες, ευχαριστώ όλα τα παιδιά του εργαστηρίου, παλιότερους και νεότερους, για τις αλησμόνητες στιγμές που περάσαμε μαζί. Σε όλους αυτούς που έχω τη χαρά να αποκαλώ πλέον φίλους μου, τους εύχομαι να στοχεύουν

πάντα ψηλά.

Τέλος, μέσα από αυτές τις γραμμές θα ήθελα να εκφράσω τις εκ βαθέων ευχαριστίες μου στην πολυαγαπημένη μου οικογένεια που δεν έπαψε στιγμή να με στηρίζει. Από τους φίλους μου, τους οποίους ευχαριστώ για την κατανόηση τους, οφείλω να ξεχωρίσω τον Γιάννη Δροσινό, ο οποίος ήταν διαρκώς στο πλευρό μου. Χωρίς εσάς, τίποτα από ό,τι ακολουθεί δε θα υπήρχε.

Πίνακας Περιεχομένων

Πίνακας Σχημάτων

Σελ.

Κεφάλαιο 1

Εισαγωγή

Η εποχή μας χαρακτηρίζεται από τεχνολογικές εξελίξεις οι οποίες μεταμορφώνουν δραστικά τον τρόπο που ζούμε και εργαζόμαστε. Η πρόοδος των Τεχνολογιών Πληροφορίας και Επικοινωνίας έχει δώσει την ώθηση για την ανάπτυξη και παροχή προηγμένων ηλεκτρονικών υπηρεσιών μέσω των οποίων καθίσταται δυνατή η ανταλλαγή κάθε είδους πληροφορίας. Οι χρήστες του διαδικτύου κάνουν χρήση της πανταχού παρούσας συνδεσιμότητας και μοιράζονται τα δεδομένα τους σε όλες τις συσκευές τους σπάζοντας τα γεωγραφικά δεσμά που τους περιορίζουν χρησιμοποιώντας κατανεμημένες υπηρεσίες αποθήκευσης στο νέφος. Ενώ εταιρίες και οργανισμοί βρίσκονται διαρκώς σε σύνδεση μέσω διαδικτυακών υπηρεσιών.

Κεντρική θέση στο διαδίκτυο έχουν πλέον το περιεχόμενο και οι υπηρεσίες μέσω των οποίων δίνεται η πρόσβαση σε αυτό, παρά οι κόμβοι που το αποτελούν. Παράλληλα, το μοντέλο παραγωγού-καταναλωτή πληροφορίας αναβαθμίζεται, με τους ρόλους να μην είναι τόσο διακριτοί. Η ραγδαία ανάπτυξη των υπηρεσιών κοινωνικής δικτύωσης διευκολύνει το διαμοιρασμό του περιεχομένου και καθιστά τους χρήστες έναν από τους κύριους παραγωγούς πληροφορίας, ενώ ρόλο παραγωγού πληροφορίας λαμβάνουν και οι συσκευές τους, η αυξανόμενη διασύνδεση των οποίων γεννάει το διαδίκτυο των συσκευών.

1.1 Κίνητρο για την έρευνα

Η παραπάνω μαζική παραγωγή πληροφοριών καθιστά δυνατή τη δημιουργία συναρπαστικών εφαρμογών που συνδυάζουν περιεχόμενο από διαφορετικές πηγές. Ωστόσο, το αναγκαίο βήμα για την περαιτέρω αλληλεπίδραση μεταξύ εταιριών, οργανισμών, χρηστών και περιεχομένου αφορά στη διασφάλιση των δεδομένων που διαμοιράζουν και των υπηρεσιών που τα παρέχουν.

Για το παραπάνω ενδιαφέρονται προφανώς οι παραγωγοί ψηφιακού περιεχομένου, αλλά και οι καταναλωτές του. Οι πρώτοι επιθυμούν να διαμοιράσουν με ασφάλεια το περιεχόμενο τους χτίζοντας ad hoc έμπιστες σε αυτούς κοινότητες. Ενώ η ύπαρξη τεχνολογιών που θα τις υποστηρίζει, ενεργοποιεί την ευρεία κινητοποίηση της συνεργασίας μεταξύ συστημάτων που διαχειρίζονται από διαφορετικούς οργανισμούς και θα οδηγήσει στη δημιουργία εξελιγμένων και πρωτοποριακών πληροφοριοκεντρικών εφαρμογών προς όφελος των καταναλωτών.

Ωστόσο, το παραπάνω περιβάλλον χαρακτηρίζεται από ετερογένεια σε πολλούς τομείς. Από τη μια πλευρά, η δημιουργία ad hoc κοινοτήτων είναι προβληματική, αφού κατά κανόνα οι χρήστες είναι μέλη διαφορετικών οργανισμών και τα διαπιστευτήρια τους βασίζονται σε διαφορετικές τεχνολογίες. Από την άλλη πλευρά, οι πολιτικές προστασίας του περιεχομένου περιορίζουν την διάδοση του σε συγκεκριμένους τομείς ασφαλείας. Παράλληλα, οι μορφές παράδοσης των ψηφιακών περιεχομένων που επιλέγουν οι παραγωγοί τους είναι μη διαλειτουργικές, περιορίζοντας ακόμα περισσότερο την εμβέλεια του ψηφιακού περιεχομένου σε συγκεκριμένες συσκευές και πλατφόρμες. Το παραπάνω, έχει αρνητικές επιπτώσεις και στην διασύνδεση μεταξύ των περιεχομένων, η οποία οδηγεί τελικώς στην εύρεση τους από τους ενδιαφερόμενους χρήστες. Οι υπάρχοντες μηχανισμοί διασύνδεσης τους και η χρήση διαφορετικών λεξιλογίων οδηγούν σε παρερμηνείες, βλάπτοντας την ποιότητα μιας υπηρεσίας αλλά και την εμπειρία του τελικού χρήστη.

Οι νέες πληροφοριοκεντρικές εφαρμογές θα πρέπει να είναι ικανές να διαχειριστούν κάθε μορφής ψηφιακά περιεχόμενα, το κάθε ένα με τα δικά του χαρακτηριστικά και ανάγκες, τα οποία θα περιγράφονται από ευέλικτες δομές δεδομένων που θα εμπεριέχουν μεταδεδομένα που θα ενεργοποιούν την απρόσκοπτη επεξεργασία και προώθηση

τους. Στα τελευταία θα πρέπει να περιέχονται οι πολιτικές ασφαλείας τους, αλλά και πληροφορίες διασύνδεσης τους με άλλα ψηφιακά περιεχόμενα, ώστε να επιτρέπεται η εύκολη οργάνωση και αναζήτηση τους. Οι υπάρχουσες λύσεις, ωστόσο, είναι μη διαλειτουργικές και αναφέρονται μονάχα σε κλειστή κλάση τύπων δεδομένων, αφήνοντας ένα κενό στις ανάγκες της εποχής σχετικά με την παραγωγή, διαμοιρασμό και κατανάλωση ψηφιακού περιεχομένου.

1.2 Στόχοι της διατριβής

Σε αυτό το πλαίσιο, με τις ανάγκες των τελικών χρηστών και των παραγωγών περιεχομένου να συγκλίνουν όλο και περισσότερο, βασικό ρόλο στην σημερινή επανάσταση των μέσων κατέχει η ευρεία υιοθέτηση διεθνών προτύπων. Η παρούσα διατριβή, ξεκινώντας από αυτή τη διαπίστωση, εξετάζει ζητήματα διαλειτουργικότητας στις δομές δεδομένων που ανταλλάσσονται μεταξύ διαφορετικών συστημάτων, στις πολιτικές προστασίας τους, αλλά και στην ελεγχόμενη πρόσβαση στις υπηρεσίες που τα προσφέρουν. Στη συνέχεια, προτείνει λύσεις οι οποίες βασίζονται στα διεθνή πρότυπα MPEG-21 και MPEG-M και ενισχύουν τη συνεργασία μεταξύ πληροφοριοκεντρικών εφαρμογών που δραστηριοποιούνται σε ετερογενή κατανεμημένα περιβάλλοντα.

Ειδικότερα, σε ότι αφορά τη διαλειτουργικότητα των δομών δεδομένων, στο πλαίσιο της διατριβής αξιολογείται η χρήση των ψηφιακών αντικειμένων του προτύπου MPEG-21, και προτείνεται μηχανισμός για την σημασιολογική συσχέτισης τους. Παράλληλα, εξετάζονται τα ζητήματα σημασιολογικής διαλειτουργικότητας τα οποία εγείρονται σε ετερογενή περιβάλλοντα και προτείνεται σύστημα για την υποστήριξης της το οποίο βασίζεται στη δομή των λεξικών διαλειτουργικότητας.

Όσον αφορά στη διαλειτουργικότητα των πολιτικών ασφαλείας και της προστασίας του ανταλλασσόμενου περιεχομένου, αναλύονται οι τρέχουσες τάσεις στον έλεγχο πρόσβασης σε ψηφιακό περιεχόμενο και προτείνεται σύστημα το οποίο ενοποιεί την πλατφόρμα του προτύπου MPEG-M με τις υποδομές της καινοτόμου μεθόδου Κρυπτογραφίας Βάσει Χαρακτηριστικών (ΚΒΧ). Σε αυτό, η γλώσσα περιγραφής δικαιωμάτων MPEG-21 REL χρησιμοποιείται τόσο για την περιγραφή των πολιτικών προστασίας, όσο και για την εκ-

χώρηση χαρακτηριστικών από τις αρχές εκχώρησης χαρακτηριστικών. Ενώ, η επικοινωνία μεταξύ των διαφόρων οντοτήτων πραγματοποιείται μέσω των στοιχειωδών υπηρεσιών του προτύπου MPEG-M ενισχύοντας ακόμα περισσότερο τη διαλειτουργικότητα.

Όσον αφορά στη διαλειτουργικότητας στον έλεγχο πρόσβασης των υπηρεσιών που προσφέρουν τα δεδομένα, αναλύονται οι υπάρχουσες λύσεις και οι περιορισμοί τους. Στη συνέχεια προτείνεται σύστημα έλεγχου πρόσβασης διαδικτυακών υπηρεσιών τύπου REST, το οποίο κάνει χρήση ψηφιακών αντικειμένων για την περιγραφή της διεπαφής τους, ενώ τα δικαιώματα χρήσης των μεθόδων της διεπαφής περιγράφονται με την μορφή αδειών χρήσης. Οι τελευταίες επιβάλλονται με τη χρήση KBX, δίνοντας πρόσβαση μονάχα στους εξουσιοδοτημένους χρήστες.

Τέλος, η διατριβή ολοκληρώνει το θεωρητικό πλαίσιο αξιολόγησης των προτεινόμενων μοντέλων συνεργασίας πληροφοριοκεντρικών εφαρμογών που δραστηριοποιούνται σε ετερογενή κατανεμημένα περιβάλλοντα, με την παρουσίαση ενός ολοκληρωμένου παραδείγματος χρήσης. Το παράδειγμα προέρχεται από τις ανάγκες του χώρου της υγείας και παρουσιάζει μια ολοκληρωμένη υπηρεσία διαχείρισης προσωπικών ιατρικών δεδομένων με ασφάλεια πάνω από περιβάλλον κινητού και διάχυτου υπολογισμού.

1.3 Διάρθρωση της διατριβής

Η διατριβή αποτελείται από επτά κεφάλαια (συμπεριλαμβανομένου του παρόντος εισαγωγικού κεφαλαίου) τα οποία περιέχουν όλο το αναγκαίο υλικό για τη διατύπωση του προβλήματος, την περιγραφή των σχετικών τεχνολογιών, την ανασκόπηση των παρόμοιων ερευνητικών προσπαθειών μέχρι τώρα, την περιγραφή και την αξιολόγηση της προτεινόμενης λύσης. Πιο συγκεκριμένα:

Στο δεύτερο κεφάλαιο γίνεται αναφορά στο επίπεδο των δομών δεδομένων που παρέχει το πρότυπο MPEG-21 για ενθυλάκωση και προστασία της πληροφορίας. Πιο συγκεκριμένα, παρουσιάζονται τα ψηφιακά αντικείμενα (Digital Items), η γλώσσα περιγραφής δικαιωμάτων (Rights Expression Language), και τα εργαλεία προστασίας και διαχείρισης πνευματικής ιδιοκτησίας (Intellectual Property Management and Protection). Στη συνέ-

χεια, αναλύονται οι πρότυποι μηχανισμοί που παρέχει το MPEG-M, οι οποίοι αξιοποιούν τις παραπάνω δομές δεδομένων μέσα από ένα ενιαίο, αυστηρά καθορισμένο περιβάλλον, το οποίο επιτρέπει τη διασύνδεση ετερογενών συστημάτων. Ιδιαίτερη έμφαση δίνεται στις στοιχειώδεις υπηρεσίες και την αρχιτεκτονική του επεκτάσιμου μεσισμικού του MPEG-M, πάνω στα οποία στηρίζονται οι λύσεις που προτείνει η διατριβή.

Στο τρίτο κεφάλαιο παρουσιάζονται οι επικρατέστεροι μηχανισμοί συσχέτισης ψηφιακών εγγράφων του διαδικτύου και υπογραμμίζονται οι περιορισμοί τους. Στη συνέχεια, δίνεται έμφαση στη συσχέτιση μεταξύ ψηφιακών αντικειμένων του MPEG-21 και παρουσιάζεται ένας ευέλικτος μηχανισμός που υποστηρίζει την συσχέτιση τους εκμεταλλευόμενος τις τεχνολογίες του σημασιολογικού διαδικτύου για τη δημιουργία σημασιολογικά πλούσιων περιγραφών για αυτά. Ο μηχανισμός αυτός προτάθηκε και ενσωματώθηκε ως επέκταση στο τρίτο μέρος του πρότυπου MPEG-21, προτείνοντας μια βασική οντολογία για την περιγραφή των συσχετίσεων. Στο τέλος του κεφαλαίου παρουσιάζεται σύστημα υποστήριξης σημασιολογικής διαλειτουργικότητας που βασίζεται στα λεξικά διαλειτουργικότητας, δομές που δρουν ως σημασιολογικές γέφυρες μεταξύ εννοιών διαφορετικών οντολογιών, και παρουσιάζονται περιπτώσεις χρήσης του στο πλαίσιο των συσχετίσεων ψηφιακών αντικειμένων.

Στο τέταρτο κεφάλαιο περιγράφονται τα υπάρχοντα συστήματα ελέγχου πρόσβασης και ασφαλούς ανταλλαγής περιεχομένου σε κατανεμημένα και ετερογενή περιβάλλοντα και αναλύονται οι περιορισμοί τους. Στη συνέχεια ακολουθεί μια σύντομη εισαγωγή στην Κρυπτογραφία Βάσει Χαρακτηριστικών (Attribute-Based Encryption), η οποία αποτελεί μια πολλά υποσχόμενη τεχνολογία προστασίας περιεχομένου και έχει επιλεχθεί για την προστασία του περιεχομένου στα πλαίσια της προτεινόμενης αρχιτεκτονικής. Τα βασικά δομικά στοιχεία της αρχιτεκτονικής επικοινωνούν μεταξύ τους με τις στοιχειώδεις υπηρεσίες του MPEG-M και δημιουργούν μια ενοποιημένη πλατφόρμα ασφαλούς ανταλλαγής περιεχομένων που κρυπτογραφούνται βάσει χαρακτηριστικών, οι λειτουργίες της οποίας περιγράφονται λεπτομερώς και καλύπτουν πλήρως τον κύκλο κρυπτογράφησης του περιεχομένου. Στο σύστημα χρησιμοποιείται η γλώσσα περιγραφής δικαιωμάτων MPEG-21 REL τόσο για την περιγραφή των πολιτικών που θέτουν οι χρήστες για τον διαμοιρασμό των δεδομένων τους, όσο και για την εκχώρηση κατάλληλων χαρακτηριστι-

κών στους χρήστες, συνεισφέροντας με αυτόν τον τρόπο στην αντιμετώπιση της ετερογένειας των χρηστών, των πολιτικών διαμοιρασμού αλλά και στη διαλειτουργικότητα μεταξύ των αρχών εκχώρησης χαρακτηριστικών.

Στο πέμπτο κεφάλαιο περιγράφονται τα υπάρχοντα συστήματα ελέγχου πρόσβασης διαδικτυακών υπηρεσιών, οι οποίες αποτελούν τον επικρατέστερο τρόπο επικοινωνίας μεταξύ ετερογενών και κατανεμημένων συστημάτων. Στη συνέχεια, το κεφάλαιο εστιάζει στις διαδικτυακές υπηρεσίες που ακολουθούν την αρχιτεκτονική REST και προτείνει σύστημα ελέγχου πρόσβασης για αυτές. Το σύστημα κάνει χρήση ψηφιακών αντικειμένων για την περιγραφή των διεπαφών REST, αδειών χρήσης για την περιγραφή των κανόνων χρήσης των μεθόδων που ορίζουν, αλλά και χρήση KBX για την επιβολή των τελευταίων.

Το έκτο κεφάλαιο στοχεύει στην παρουσίαση των πλεονεκτημάτων των προτεινόμενων λύσεων μέσα από την επίδειξη ενός ολοκληρωμένου παραδείγματος χρήσης, το οποίο περιλαμβάνει ετερογενή σύνολα χρηστών που έχουν ως στόχο την συνεργασία και την ανταλλαγή περιεχομένου με ασφάλεια. Το παράδειγμα εστιάζει στην ασφαλή πρόσβαση και διαχείριση ιατρικών δεδομένων και λαμβάνει υπόψη του τις προσπάθειες προτυποποίησης στο χώρο της ηλεκτρονικής υγείας (e-health) όπως τα προσωπικά αρχεία υγείας. Εστιάζοντας στο πρόσφατο πρότυπο HL7 FHIR, το παράδειγμα χρήσης αναδεικνύει τα πλεονεκτήματα του μηχανισμού συσχέτισης ψηφιακών αντικειμένων, του συστήματος υποστήριξης σημασιολογικής διαλειτουργικότητας, του συστήματος ασφαλούς ανταλλαγής ψηφιακών αντικειμένων, αλλά και του συστήματος ασφαλούς συνεργασίας μέσω διαδικτυακών υπηρεσιών τύπου REST.

Τέλος, το έβδομο κεφάλαιο περιλαμβάνει τα συμπεράσματα που προκύπτουν από τη διατριβή και σκιαγραφεί τις πιθανές μελλοντικές κατευθύνσεις, που θα αποτελέσουν τους άξονες της συνέχισης της έρευνας έχοντας ως βάση τις λύσεις που προτείνει η διατριβή.

Κεφάλαιο 2

Ψηφιακά αντικείμενα και τεχνολογίες διαχείρισης τους

Το παρόν κεφάλαιο παρουσιάζει τις τεχνολογίες των προτύπων MPEG-21 και MPEG-M, τα οποία στοχεύουν στην υποστήριξη της διαλειτουργικότητας μεταξύ πολυμεσικών εφαρμογών. Πιο συγκεκριμένα, το MPEG-21 προδιαγράφει την αφηρημένη δομή των ψηφιακών αντικειμένων (§2.1.1), με την οποία μπορεί να περιγραφεί κάθε είδους περιεχόμενο. Επιπρόσθετα, το πρότυπο πλαισιώνει τα ψηφιακά αντικείμενα με τη γλώσσα περιγραφής δικαιωμάτων (§2.1.2), με την οποία μπορούν να ορισθούν οι κανόνες χρήσης τους. Η ανάγκη για προστασία του περιεχομένου, οδήγησε στην ανάπτυξη των εργαλείων προστασίας και διαχείρισης πνευματικής ιδιοκτησίας (§2.1.3), τα οποία αναλαμβάνουν τον ρόλο της επιβολής των αδειών χρήσης που αφορούν κάθε περιεχόμενο. Τις παραπάνω τεχνολογίες συμπληρώνει το πρότυπο MPEG-M προδιαγράφοντας τα τερματικά MPEG-M, τα οποία υποστηριζόμενα από το επεκτάσιμο μεσισμικό του MPEG-M (§2.2.2), προσφέρουν στοιχειώδεις υπηρεσίες (§2.2.1) σχετικές με τη δημιουργία, επεξεργασία και την κατανάλωση ψηφιακών αντικειμένων.

2.1 Το πρότυπο MPEG-21

Το πρότυπο MPEG-21 [7] στοχεύει στον ορισμό διαλειτουργικών μηχανισμών και τεχνολογιών για την υποστήριξη εφαρμογών που σχετίζονται με την παράδοση περιεχομένου σε ετερογενή δίκτυα και συσκευές. Στο πλαίσιο του MPEG-21, κάθε περιεχόμενο ενθυλακώνεται σε ψηφιακά αντικείμενα, τα οποία αποτελούν τη βασική μονάδα διαμοιρασμού περιεχομένου μεταξύ οντοτήτων. Βασισμένα στη γλώσσα XML και σε ευέλικτα XML σχήματα, τα ψηφιακά αντικείμενα αποτελούνται από το ψηφιακό περιεχόμενο, το οποίο μπορεί να ενσωματωθεί αυτούσιο ή ως σύνδεσμος, τα μεταδεδομένα που το περιγράφουν, αλλά και από τις πολιτικές χρήσης και προστασίας των μερών του.

Το MPEG-21 αποτελείται από δεκαοκτώ μέρη, περιγραφές των οποίων παρατίθενται παρακάτω, ενώ στις επόμενες παραγράφους αναλύονται με περισσότερη λεπτομέρεια εκείνα που λειτουργούν ως τεχνολογίες υποβάθρου για τη διατριβή. Κάθε μέρος του επικεντρώνει σε διαφορετικές πτυχές της διαχείρισης περιεχομένου, όπως την δημιουργία, παροχή, επεξεργασία, αποθήκευση, παράδοση και κατανάλωση του.

- **1ο Μέρος:** Όραμα, τεχνολογίες και στρατηγική (Vision, technologies and strategy). Ορίζει τη γωνία θέασης μέσω της οποίας οι τεχνολογίες της σουίτας MPEG-21 καθιστούν δυνατή τη διαφανή χρήση περιεχομένου σε ετερογενείς συσκευές και δίκτυα με τρόπο που να ικανοποιεί τις ανάγκες των χρηστών.

- **2ο Μέρος:** Διακήρυξη ψηφιακού αντικειμένου (Digital item declaration). Προδιαγράφει τις αφηρημένες έννοιες και τα στοιχεία από τα οποία συνίσταται ένα ψηφιακό αντικείμενο, το οποίο στοχεύει στην ψηφιακή αναπαράσταση παντός είδους περιεχομένου.

- **3ο Μέρος:** Ταυτοποίηση ψηφιακού αντικειμένου (Digital item identification). Προδιαγράφει δομές μέσω των οποίων πραγματοποιείται η ταυτοποίηση με μοναδικό τρόπο των ψηφιακών αντικειμένων όπως και των μερών τους.

- **4ο Μέρος:** Προστασία και διαχείριση πνευματικής ιδιοκτησίας (Intellectual property management and protection). Προδιαγράφει τα εργαλεία προστασίας ψηφιακών αντι-

κειμένων και ορίζει τα μηνύματα μέσω των οποίων καθίσταται δυνατή η μεταξύ τους επικοινωνία.

- **5ο Μέρος:** Γλώσσα περιγραφής δικαιωμάτων (Rights expression language). Παρέχει ευέλικτες δομές και λεξιλόγιο για τον σαφή ορισμό κανόνων χρήσης που αφορούν τη χρήση ενός ψηφιακού αντικειμένου.
- **6ο Μέρος:** Λεξικό δεδομένων δικαιωμάτων (Rights data dictionary). Παρέχει το λεξιλόγιο των δικαιωμάτων χρήσης ενός ψηφιακού αντικειμένου, ορίζοντας παράλληλα τους τρόπους με τους οποίους μπορεί να επεκταθεί.
- **7ο Μέρος:** Προσαρμογή ψηφιακού αντικειμένου (Digital item adaptation). Ορίζει τα εργαλεία προσαρμογής ψηφιακών αντικειμένων, τα οποία προσαρμόζουν τα περιεχόμενα τους κατάλληλα, με σκοπό να άρουν τους περιορισμούς που θέτουν οι συσκευές που τα καταναλώνουν και τα δίκτυα μέσω των οποίων μεταφορτώνονται.
- **8ο Μέρος:** Λογισμικό αναφοράς (Reference software). Παρέχει λογισμικό αναφοράς για τις τεχνολογίες του MPEG-21.
- **9ο Μέρος:** Μορφή αρχείου (File format). Ορίζει τη δομή αρχείου ενός ψηφιακού αντικειμένου.
- **10ο Μέρος:** Επεξεργασία ψηφιακού αντικειμένου (Digital item processing). Ορίζει εργαλεία για την επεξεργασία ψηφιακών αντικειμένων, με στόχο τη διαλειτουργικότητα στο επίπεδο της επεξεργασίας τους μέσω προκαθορισμένων τύπων επεξεργασίας.
- **11ο Μέρος:** Μέθοδοι αξιολόγησης για τεχνολογίες μόνιμης συσχέτισης (Evaluation tools for persistent association technologies). Παρέχει αξιολόγηση υπαρχόντων τεχνολογιών συσχέτισης και προτείνει μεθοδολογία αξιολόγησης τους.
- **12ο Μέρος:** Πλατφόρμα δοκιμών για την παράδοση MPEG-21 περιεχομένου (Test bed for MPEG-21 resource delivery). Παρέχει λογισμικό ελέγχου και αξιολόγησης της παράδοσης περιεχομένου στα πρότυπα του MPEG-21.
- **14ο Μέρος:** Έλεγχος συμμόρφωσης (Conformance testing). Ορίζει ελέγχους συμμόρφωσης στις τεχνολογίες του MPEG-21.

- **15ο Μέρος:** Αναφορές συμβάντων (Event reporting). Ορίζει δομές για την περιγραφή και τον διαμοιρασμό συμβάντων σχετικών με τη χρήση ψηφιακών αντικειμένων και του περιβάλλοντος χρήσης τους.
- **16ο Μέρος:** Μορφή δυαδικών αρχείων (Binary format). Ορίζει τις μεθόδους σειριοποίησης ενός αρχείου μορφής MPEG-21.
- **17ο Μέρος:** Ταυτοποίηση τμήματος περιεχομένου MPEG (Fragment identification of MPEG resources). Ορίζει συντακτικό για την ταυτοποίηση διαφορετικών τμημάτων ενός περιεχομένου MPEG.
- **18ο Μέρος:** Ροή ψηφιακού αντικειμένου (Digital item streaming). Προδιαγράφει εργαλεία που διευκολύνουν τη ροή ψηφιακών αντικειμένων, με βασικό σενάριο τον διαχωρισμό και την παράδοση εικόνας και ήχου οπτικοακουστικού περιεχομένου.

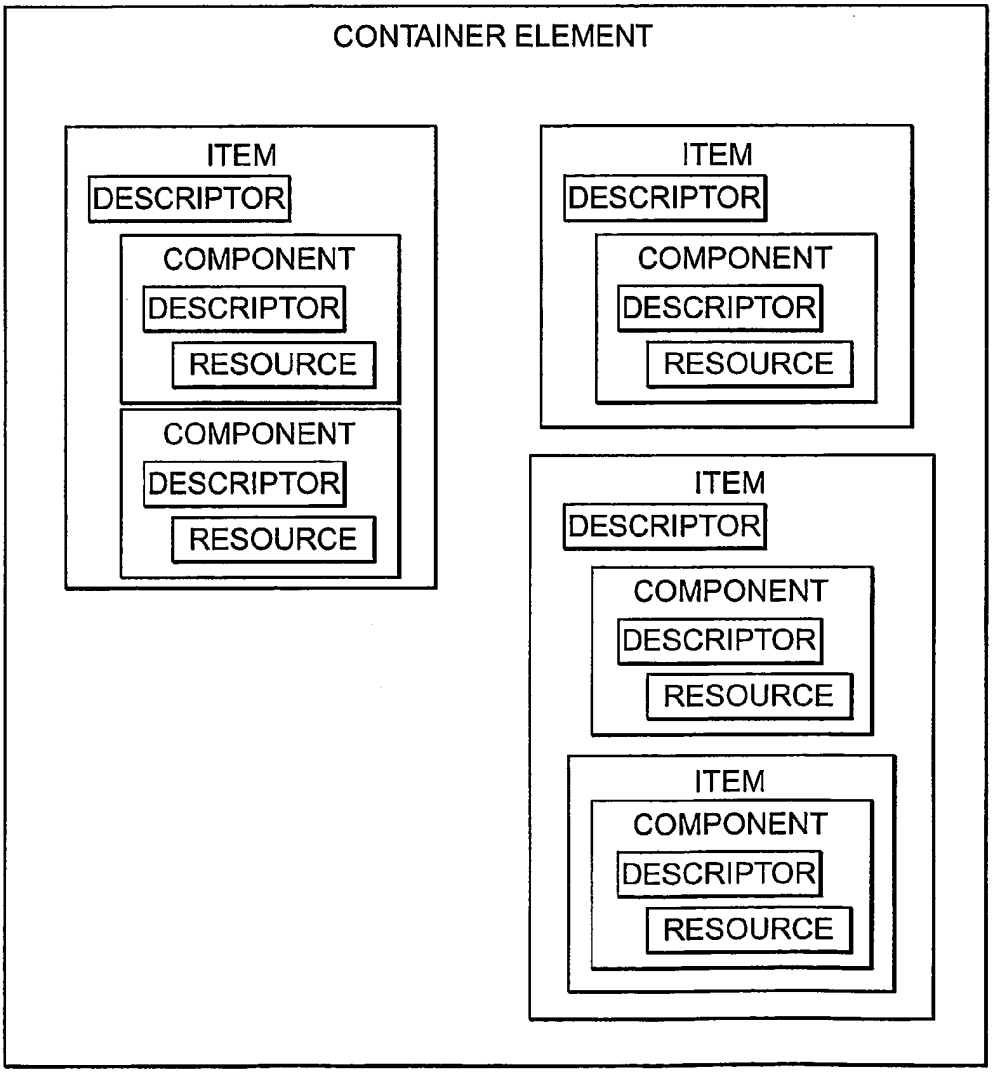
2.1.1 Ψηφιακά αντικείμενα

Τα ψηφιακά αντικείμενα, όπως ορίζονται από το δεύτερο μέρος της σουίτας προτύπων MPEG-21 [8], αποτελούν τη βασική δομή αναπαράστασης και διαμοιρασμού περιεχομένου. Τα ψηφιακά αντικείμενα στοχεύουν στην προτυποποίηση της περιγραφής κάθε είδους ψηφιακού περιεχομένου, με σκοπό την υποστήριξη της διαλειτουργικής χρήσης του σε ετερογενή συστήματα. Για το λόγο αυτό, τα ψηφιακά αντικείμενα προδιαγράφουν ευέλικτες δομές ώστε να συνδυάζουν περιεχόμενα (βίντεο, μουσική, εικόνες, ...), μεταδεδομένα (είδος περιεχομένου, ιδιοκτήτης, ...) και πληροφορίες προστασίας τους (άδειες χρήσης, κωδικοί προστασίας περιεχομένου) σε μια μονάδα πληροφορίας .

Τα βασικότερα τμήματα από τα οποία αποτελείται ένα ψηφιακό αντικείμενο παρουσιάζονται παρακάτω:

- Αντικείμενο (Item)

  Ένα αντικείμενο αποτελείται από την ομαδοποίηση ενός ή περισσοτέρων υπό-αντικειμένων τα οποία χαρακτηρίζονται από σχετικές περιγραφές. Το XML σχήμα των ψηφιακών αντικειμένων δίνει τη δυνατότητα να δηλωθούν τόσο αυτοτελείς μονάδες περιεχομένου, όπως μια φωτογραφία ή ένα τραγούδι, όσο και σύνολα περιεχομένων που



Σχήμα 1: Σχηματική αναπαράσταση ενός ψηφιακού αντικειμένου και των περιεχομένων του [1]

συνδέονται λογικά σε μια δομή, όπως μια συλλογή φωτογραφιών ή τραγουδιών. Τα αντικείμενα αποτελούν ουσιαστικά μια περιγραφική δομή που αναπαριστά ψηφιακά κάθε είδους περιεχόμενο.

- Συστατικό (Component) και Περιεχόμενα (Resources)

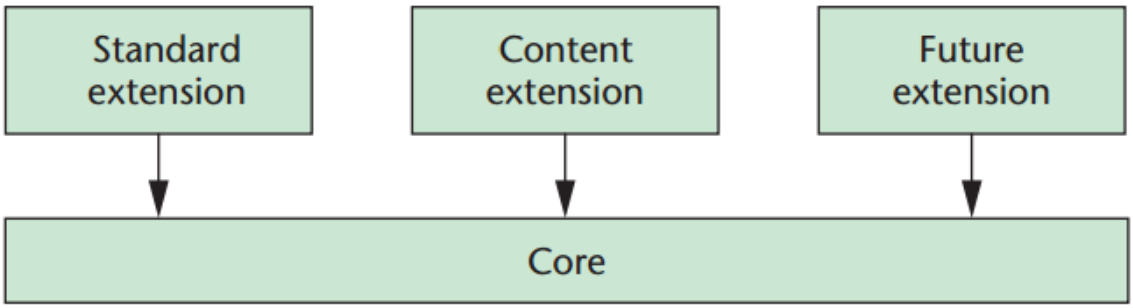
  Ένα συστατικό συνδέει το ψηφιακό περιεχόμενο που δηλώνεται σε ένα αντικείμενο με δηλώσεις που το αφορούν. Τυπικά, περιέχει πληροφορίες σχετικές με το περιεχόμενο (όπως κωδικοσελίδα για ένα έγγραφο κειμένου ή ρυθμό ροής bit για ένα βίντεο) και τον καθορισμό συνδέσμου για την πρόσβαση σε αυτό.

- Περιγραφή (Descriptor) και Δηλώσεις (Statements)

  Μια περιγραφή αποτελείται από την ομαδοποίηση μιας ή περισσοτέρων δηλώσεων που αφορούν σε ένα ψηφιακό περιεχόμενο. Η δήλωση αποτελεί ένα αφηρημένο στοιχείο στο οποίο μπορούν να συμπεριληφθούν πλήθος πληροφοριών σχετικές με ένα περιεχόμενο. Τυπικά, περιλαμβάνει μεταδεδομένα για το περιεχόμενο, πληροφορίες για την ψηφιακή ταυτότητα του περιεχομένου (αναγνωριστικό), τον τύπο του (mime type) και δηλώσεις όπως ο αριθμός αναθεώρησης του. Παραδείγματος χάρη, σε ένα ψηφιακό αντικείμενο που αφορά σε ένα βιβλίο, θα εμφανίζονταν δηλώσεις για τον τίτλο, συγγραφέα και αριθμό ISBN του. Τέλος, οι κανόνες που διέπουν τη χρήση του ψηφιακού αντικειμένου περιλαμβάνονται σε ειδική δήλωση σχετική με την προστασία και τη διαχείριση πνευματικής ιδιοκτησίας.

2.1.2 Γλώσσα περιγραφής δικαιωμάτων

Το πέμπτο μέρος της σουίτας προτύπων MPEG-21 προδιαγράφει το συντακτικό και το λεξιλόγιο της γλώσσας περιγραφής δικαιωμάτων (Rights Expression Language - REL - [9]), η οποία στοχεύει στην συμπερίληψη όλων των εννοιών, οντοτήτων και διαδικασιών που λαμβάνουν χώρα σε σενάρια διαμοιρασμού περιεχομένου και αφορούν στον καθορισμό των κανόνων χρήσης του περιεχομένου. Οι έννοιες και οι οντότητες που περιλαμβάνει η γλώσσα REL ομαδοποιούνται στις βασικές (core), τυπικές (standard) και πολυμεσικές (multimedia) έννοιες.



Σχήμα 2: Οι δομή των XML σχημάτων της MPEG-21 REL [2]

Οι δημιουργοί περιεχομένου μπορούν να εκφράσουν με τη REL τα δικαιώματα που

διέπουν τη χρήση του καθορίζοντας μέσω της βασικής δομής των *χορηγήσεων δικαιωμάτων* (grants), *ποιοι* μπορούν να χρησιμοποιήσουν το περιεχόμενο, *πως* μπορούν να το χρησιμοποιήσουν και κάτω από ποιους *όρους*. Σύμφωνα με το λεξιλόγιο της REL μια χορήγηση δικαιωμάτων αποτελείται από τον *χρήστη (principal)* στον οποίο χορηγείται το *δικαίωμα (right)* πάνω στο *περιεχόμενο (resource)*, που εξουσιοδοτείται ο χρήστης να πραγματοποιήσει πάνω στο περιεχόμενο και ποιες *συνθήκες (conditions)* πρέπει να πληρούνται τη στιγμή άσκησης του δικαιώματος χρήσης πάνω στο περιεχόμενο.

Οι χορηγήσεις δικαιωμάτων χρήσης που αφορούν σε ένα συγκεκριμένο περιεχόμενο, ομαδοποιούνται με τη μορφή αδειών χρήσης (license), οι οποίες μπορούν να συνοδεύουν το περιεχόμενο, και περιγράφουν με πληρότητα τα δικαιώματα που εκχωρεί ο δημιουργός στους χρήστες. Ενώ, για τη διασφάλιση της εγκυρότητας τους, οι άδειες χρήσης είναι δυνατό να υπογραφούν ψηφιακά από τον εκδότη τους (issuer).

Πέρα από τον καθορισμό κανόνων χρήσης περιεχομένου σε συγκεκριμένους χρήστες, με τη γλώσσα REL ο δημιουργός μπορεί να εκχωρήσει δικαιώματα χρήσης και σε ομάδες χρηστών που αναγνωρίζονται από τα χαρακτηριστικά τους. Με τον τρόπο αυτό, αποφεύγεται η ανάγκη για έκδοση νέων αδειών για κάθε χρήστη με την άδεια να αναφέρεται σε κατόχους χαρακτηριστικών (property possessors), οι οποίοι πρέπει να αποδεικνύουν την κατοχή των σχετικών χαρακτηριστικών προτού αποκτήσουν πρόσβαση στο περιεχόμενο.

Η γλώσσα REL παρέχει επίσης τη δυνατότητα για εκχώρηση χαρακτηριστικών στους χρήστες εκλαμβάνοντας την έννοια των χαρακτηριστικών (property) ως περιεχόμενο (resource). Μια τέτοια άδεια, έχει ως υποκείμενο συγκεκριμένο χρήστη αυστηρά καθορισμένο από το δημόσιο κλειδί του, ως δικαίωμα την κατοχή χαρακτηριστικού (possessesProperty) και ως αντικείμενο το συγκεκριμένο χαρακτηριστικό.

Τα βασικότερα στοιχεία της γλώσσας περιγραφής δικαιωμάτων του MPEG-21 παρουσιάζονται παρακάτω:

- Υποκείμενο (Principal) :

  Όπως αναφέρθηκε παραπάνω μια άδεια μπορεί να καθορίζει αυστηρά το υποκείμενο της με βάση το δημόσιο κλειδί του είτε ορίζοντας τα χαρακτηριστικά που πρέπει να κατέχει. Στην πρώτη περίπτωση το υποκείμενο ορίζεται ως ένας κάτοχος κλειδιού

(KeyHolder) που αναγνωρίζεται από το δημόσιο κλειδί του. Στη δεύτερη περίπτωση το υποκείμενο ορίζεται αφηρημένα ως κάτοχος χαρακτηριστικών (PropertyPossessor), τα οποία πιστοποιεί μια αρχή εμπιστοσύνης (TrustRoot).

- Δικαίωμα (Right) :

  Τα δικαιώματα αποτελούν *ρήματα* τα οποία δηλώνουν τη σχέση που επιτρέπεται να έχει το υποκειμένου με το αντικείμενο μιας χορήγησης άδειας. Τα ρήματα προέρχονται από το λεξικό δικαιωμάτων (Rights Data Dictionary - RDD - [10]) που αποτελεί το έκτο μέρος της σουίτας προτύπων MPEG-21. Το λεξικό αυτό είναι επεκτάσιμο και μπορεί να συμπεριλάβει νέα ρήματα που εμφανίζονται σε διάφορους τομείς εφαρμογών. Τα βασικότερα δικαιώματα που χρησιμοποιούνται στις άδειες χρήσεις αποτελούν η δυνατότητα αναπαραγωγής (play), ισχυρισμού κατοχής χαρακτηριστικού (possessesProperty), έκδοσης άδειας (issue), ακύρωσης άδειας (revoke), τροποποίησης (modify), επέκτασης (enhance), εκτύπωσης (print) και τέλος της αποθήκευσης (governedCopy).

- Περιεχόμενο (Resource) :

  Το περιεχόμενο αποτελεί ένα αφηρημένο στοιχείο της REL, με την έννοια πως μπορεί να αντιστοιχεί τόσο σε ένα ψηφιακό έγγραφο (digitalResource) αλλά και σε μια χορήγηση δικαιωμάτων (grant) η οποία χρησιμοποιείται σε συνδυασμό με το δικαίωμα χορήγησης του (issue). Οι βασικότεροι τύποι περιεχομένου που χρησιμοποιούνται σε άδειες χρήσεις αποτελούν η αντιστοίχιση σε υπηρεσίες (serviceReference), χαρακτηριστικά (propertyUri), ένα προστατευμένο ψηφιακό έγγραφο (protectedResource) και τέλος σε ένα ψηφιακό αντικείμενο (diReference).

- Συνθήκη (Condition) :

  Οι συνθήκες αφορούν στο περιβάλλον χρήσης στο οποίο επιτρέπεται το υποκείμενο μιας άδειας χρήσης να ασκήσει τα δικαιώματα του πάνω σε ένα περιεχόμενο. Οι δηλώσεις που μπορούν να πραγματοποιηθούν καλύπτουν ένα ευρύ φάσμα περιπτώσεων προστατευμένης χρήσης περιεχομένου και ορίζουν τόσο χρονικούς (validityInterval) και τοπικούς (territory) περιορισμούς όσο και περιορισμούς επανάληψης άσκησης δικαιώματος (exerciseMechanism), περιβάλλοντος χρήσης (securitySystem) και τέλος

χρέωσης ανά χρήση (feePerUse).

- Εκδότης (Issuer) :

  Ο εκδότης της άδειας χρήσης δηλώνεται με το δημόσιο κλειδί του, ενσωματώνοντας την ψηφιακή υπογραφή του περιεχομένου στα πρότυπα της κρυπτογράφησης XML εγγράφων (XML Digital Signature [11]) η οποία και αποδεικνύει την αυθεντικότητα της άδειας χρήσης.

2.1.3 Εργαλεία προστασίας και διαχείρισης πνευματικών δικαιωμάτων

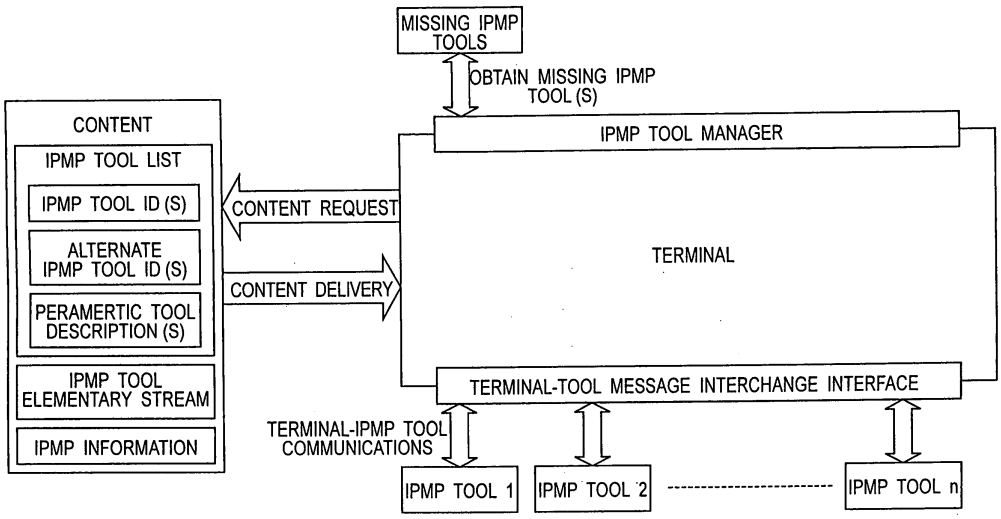
Το τέταρτο μέρος του προτύπου MPEG-21 [12] προδιαγράφει τις δομές που αφορούν στην προστασία των ψηφιακών αντικειμένων και στην επιβολή των αδειών χρήσης που περιλαμβάνονται στα ψηφιακά αντικείμενα. Για το λόγο αυτό, εισάγει τα εργαλεία προστασίας και διαχείρισης πνευματικών δικαιωμάτων (εργαλεία IPMP) που ως στόχο έχουν την επεξεργασία των αδειών χρήσης, τον έλεγχο της αυθεντικότητας τους, τον έλεγχο του περιβάλλοντος και του γενικότερου πλαισίου χρήσης προτού επιτρέψει την πρόσβαση στο περιεχόμενο.

Κάθε συσκευή η οποία παρέχει περιβάλλον εκτέλεσης στα εργαλεία IPMP ονομάζεται τερματικό IPMP. Το πρότυπο ορίζει τον τρόπο εκκίνησης των εργαλείων IPMP από το τερματικό και το πως αυτά δραστηριοποιούνται κατά την κατανάλωση του περιεχομένου. Ένα τερματικό IPMP έτσι παρέχει ένα ευέλικτο περιβάλλον για την ασφαλή κατανάλωση περιεχομένου προερχόμενο από διαφορετικούς δημιουργούς, οι οποίοι ενδέχεται να έχουν διαλέξει ετερογενείς τρόπους για την προστασία του περιεχομένου τους (π.χ. κρυπτογραφία ή υδατογραφήματα).

Η κατανάλωση ενός ψηφιακού αντικειμένου το οποίο προστατεύεται από ένα ή περισσότερα εργαλεία IPMP ξεκινάει με την επεξεργασία των πληροφοριών που περιέχονται στο σχετικό στοιχείο ελέγχου (IPMPGeneralInfoDescriptor). Αυτές ρυθμίζουν *ποιά ύπο-αντικείμενα* (resources) προστατεύουν, *ποια εργαλεία* είναι υπεύθυνα για κάθε ένα και *ποιές άδειες χρήσης* τους αντιστοιχούν. Το κατάλληλο εργαλείο IPMP, όπως ορίζεται από το μοναδικό αναγνωριστικό του, εάν δεν υπάρχει ήδη στο τερματικό, μπορεί να ληφθεί απομακρυσμένα. Η αρχικοποίηση του γίνεται μέσω των ρυθμίσεων (ConfigurationSettings)

που συμπεριλαμβάνονται στις πληροφορίες IPMP του ψηφιακού αντικειμένου παρέχοντας παράλληλα τις άδειες χρήσεις που αφορούν το κάθε ύπο-αντικείμενο (RightsDescriptor) ή την υπηρεσία έκδοσης και ελέγχου αδειών χρήσης (LicenseService). Εάν στις άδειες χρήσης καθορίζονται συγκεκριμένες επιτρεπόμενες πλατφόρμες χρήσης (SupportedPlatforms) ή τύποι τερματικών (TerminalID) το εργαλείο πρέπει να πραγματοποιήσει έλεγχο της συσκευής ώστε να δημιουργηθεί δεσμός αμοιβαίας εμπιστοσύνης μεταξύ τους. Η επικοινωνία αυτή ρυθμίζεται με αφηρημένα μηνύματα που ορίζει η διεπαφή του δρομολογητή μηνυμάτων εργαλείων (ToolMessageRouter - Εικόνα 3), ο οποίος λειτουργεί ως βάση διαλειτουργικότητας για την μεταξύ τους επικοινωνία.

Τα βασικότερα μηνύματα τα οποία προδιαγράφει το πρότυπο για την επικοινωνία με τον δρομολογητή μηνυμάτων εργαλείων αφορούν στην αμοιβαία ταυτοποίηση τερματικού και εργαλείων, στη ρύθμιση των μεθόδων προστασίας του περιεχομένου (αποκρυπτογράφηση, προσθήκη ή αφαίρεση υδατογραφήματος κτλ.) και τέλος στον ορισμό του σημείου ελέγχου (ControlPoint) στο οποίο απαιτείται η εκκίνηση του κάθε εργαλείου. Το τελευταίο ρυθμίζει τον τρόπο με τον οποίο το τερματικό καταναλώνει το περιεχόμενο, όπως και την προτεραιότητα ενεργοποίησης κάθε εργαλείου σε περίπτωση χρήσης περισσότερων του ενός.



Σχήμα 3: Επικοινωνία εργαλείων IPMP μέσω του δρομολογητή μηνυμάτων IPMP [3]

2.2 Το πρότυπο MPEG-M

Το πρότυπο MPEG-M [13] έχει ως στόχο τη διευκόλυνση της δημιουργίας, ανάπτυξης και διασύνδεσης εφαρμογών που έχουν στο επίκεντρο τους τον διαμοιρασμό πολυμεσικού περιεχομένου. Αυτό επιτυγχάνεται με δύο τρόπους. Από τη μια βασίζεται πάνω σε ήδη υπάρχοντα πρότυπα ευρέως διαδεδομένα (όπως οι τεχνολογίες του προτύπου MPEG-21) και από την άλλη ενσωματώνει με ευέλικτο τρόπο τις θεμελιώδεις διαδικασίες που εμφανίζονται σε εφαρμογές διαμοιρασμού περιεχομένου. Οι δομές που ορίζει είναι αρκετά αφηρημένες ώστε να μπορούν να εξειδικεύονται κατάλληλα από διαφορετικές εφαρμογές, αλλά εξακολουθούν να αποτελούν βάση για την εύκολη διασύνδεση τους. Αυτό έχει θετικές επιδράσεις τόσο στην πλευρά των παρόχων υπηρεσιών όσο και στην πλευρά των χρηστών τους. Οι πρώτοι είναι δυνατό να δημιουργούν εύκολα και γρήγορα υπηρεσίες διαμοιρασμού περιεχομένου και να τις διασυνδέσουν με άλλες υπηρεσίες που ακολουθούν τις προδιαγραφές του MPEG-M χωρίς επιπλέον κόστος. Οι χρήστες από την πλευρά τους, απολαμβάνουν με αυτόν τον τρόπο νέες, πιο ενδιαφέρουσες υπηρεσίες σε χαμηλότερο κόστος και με βελτιωμένη ποιότητα.

Το MPEG-M αποτελείται από πέντε μέρη, περιγραφές των οποίων παρατίθενται παρακάτω, ενώ στις επόμενες παραγράφους αναλύονται με περισσότερη λεπτομέρεια τα μέρη που λειτουργούν ως τεχνολογίες υποβάθρου για τη διατριβή.

- **1ο Μέρος:** Αρχιτεκτονική (Architecture). Προδιαγράφει την αρχιτεκτονική ενός τερματικού που ακολουθεί τα πρότυπα του MPEG-M. Εισάγεται ο όρος τερματικό MPEG-M, στο οποίο λειτουργεί το επεκτάσιμο μεσισμικό του MPEG και μέσω αυτού παρέχονται οι υπηρεσίες του MPEG-M.

- **2ο Μέρος:** Διεπαφή προγραμματισμού εφαρμογών επεκτάσιμου μεσισμικού του MPEG (MPEG extensible middleware API). Προδιαγράφει τις διεπαφές που προσφέρει το επεκτάσιμο μεσισμικό του MPEG, μέσω των οποίων οι πολυμεσικές εφαρμογές χρησιμοποιούν με διαφάνεια τις υπηρεσίες του τερματικού MPEG-M.

- **3ο Μέρος:** Λογισμικό αναφοράς και συμμόρφωση (Reference software and conformance). Προσφέρει λογισμικό αναφοράς για το επεκτάσιμο μεσισμικό και δίνει κατευθύνσεις

για την επέκταση του ώστε να διασφαλίζεται η διαλειτουργικότητα μεταξύ διαφορετικών υλοποιήσεων του.

- **4ο Μέρος:** Στοιχειώδεις υπηρεσίες (Elementary services). Εισάγει την έννοια των στοιχειωδών υπηρεσιών και προδιαγράφει πρωτόκολλα επικοινωνίας μεταξύ των οντοτήτων που τις προσφέρουν και αυτών που τις χρησιμοποιούν.

- **5ο Μέρος:** Ενοποιημένες υπηρεσίες (Aggregated services). Αφορά σε ενοποιημένες υπηρεσίες που μπορούν να προσφέρονται συνδυάζοντας στοιχειώδεις υπηρεσίες.

2.2.1 Στοιχειώδεις υπηρεσίες

Η πλατφόρμα παροχής υπηρεσιών του MPEG-M χτίζεται πάνω στη λεπτομερή ανάλυση των διαδικασιών που λαμβάνουν χώρα σε πολυμεσικές εφαρμογές με έμφαση στον διαμοιρασμό περιεχομένου. Αποτέλεσμα αυτής της ανάλυσης είναι η αναγνώριση των βασικών δομών που διακινούνται μεταξύ διαφορετικών οντοτήτων, αλλά και των στοιχειωδών λειτουργιών που πραγματοποιούν πάνω σε αυτές. Οι λειτουργίες που προσδιορίζονται θεωρούνται στοιχειώδεις, με την έννοια πως δεν μπορούν να αναλυθούν σε πιο απλές, ενώ από την άλλη είναι δυνατό να συνδυαστούν ώστε να δημιουργήσουν πιο σύνθετες προσαυξημένες υπηρεσίες όπως προδιαγράφει το 5ο μέρος του προτύπου.

Παρακάτω παρουσιάζονται οι βασικές δομές που προσδιορίζει το πρότυπο ως στοιχειώδεις :

- **Οντότητα (Entity):** Αφηρημένη έννοια η οποία λειτουργεί ως βάση διαλειτουργικότητας για οποιαδήποτε από τις παρακάτω.

- **Περιεχόμενο (Content):** Αναφέρεται στο μοναδικό αναγνωριστικό ενός ψηφιακού αντικειμένου είτε στην ακριβή XML μορφή του.

- **Συμβόλαιο (Contract):** Αντιστοιχεί σε αναφορά στο μοναδικό αναγνωριστικό ενός συμβολαίου είτε στην περιγραφή του με κείμενο, μεταδεδομένα και τα εμπλεκόμενα φυσικά ή νομικά πρόσωπα.

- **Συσκευή (Device):** Αναφέρεται στο μοναδικό αναγνωριστικό μιας συσκευής είτε σε περιγραφή της μέσω του υλικολογισμικού, της κεντρικής μονάδας επεξεργασίας ή μνήμης της κτλ. Η έννοια στοχεύει στην περιγραφή τόσο φυσικών συσκευών όσο και μονάδων λογισμικού, όπως τα εργαλεία IPMP.
- **Συμβάν (Event):** Αντιστοιχεί στην XML περιγραφή ενός συμβάντος μέσω του τύπου, χρόνου και τοποθεσίας έναρξης του αλλά και του σχετικού ψηφιακού αντικειμένου στο οποίο αναφέρεται.
- **Άδεια χρήσης (License):** Αναφέρεται στο μοναδικό αναγνωριστικό μιας άδειας χρήσης είτε στην XML μορφή της.
- **Υπηρεσία (Service):** Αντιστοιχεί σε αναφορά στο μοναδικό αναγνωριστικό μιας υπηρεσίας είτε στην περιγραφή της μέσω του τύπου της, των παραμέτρων που δέχεται και των αποτελεσμάτων που επιστρέφει.
- **Χρήστης (User):** Αναφέρεται στο μοναδικό αναγνωριστικό κάποιου χρήστη είτε στην περιγραφή του. Η έννοια στοχεύει στην δήλωση ενός φυσικού προσώπου, σε ομάδες φυσικών προσώπων ή οργανισμών.

Το πρότυπο ορίζει επίσης και τις στοιχειώδεις λειτουργίες που μπορούν να πραγματοποιηθούν πάνω στις παραπάνω δομές. Αυτές είναι ταυτοποίηση (authenticate), εξουσιοδότηση (authorize), έλεγχος (checkWith), δημιουργία (create), παράδοση (deliver), περιγραφή (describe), αναγνώριση (identify), διαπραγμάτευση (negotiate), πακετάρισμα (package), κοινοποίηση (post), παρουσίαση (present), επεξεργασία (process), αίτηση (request), ανάκληση (revoke), αναζήτηση (search), αποθήκευση (store), συναλλαγή (transact), επαλήθευση (verify).

Ο παρακάτω πίνακας παρουσιάζει τα πρωτόκολλα υπηρεσιών που προδιαγράφονται από το πρότυπο και συνδυάζουν τις στοιχειώδεις δομές με τις παραπάνω λειτουργίες.

	Περιεχόμενο	Συμβόλαιο	Συσκευή	Συμβάν	Άδεια	Υπηρεσία	Χρήστης
Ταυτοποίηση	X	X					X
Εξουσιοδότηση							X
Έλεγχος		X			X		

Δημιουργία	X	X			X		
Παράδοση	X	X					
Περιγραφή	X		X			X	X
Αναγνώριση	X	X	X		X		X
Διαπραγμάτευση		X			X		
Πακετάρισμα	X						
Κοινοποίηση	X						
Παρουσίαση		X			X		
Επεξεργασία	X				X		
Αίτηση	X	X	X	X	X		
Ανάκληση	X	X			X		
Αναζήτηση	X	X	X		X	X	X
Αποθήκευση	X	X		X	X		
Συναλλαγή	X				X		
Επαλήθευση		X	X		X		

Πίνακας 1: Στοιχειώδεις υπηρεσίες του MPEG-M [13]

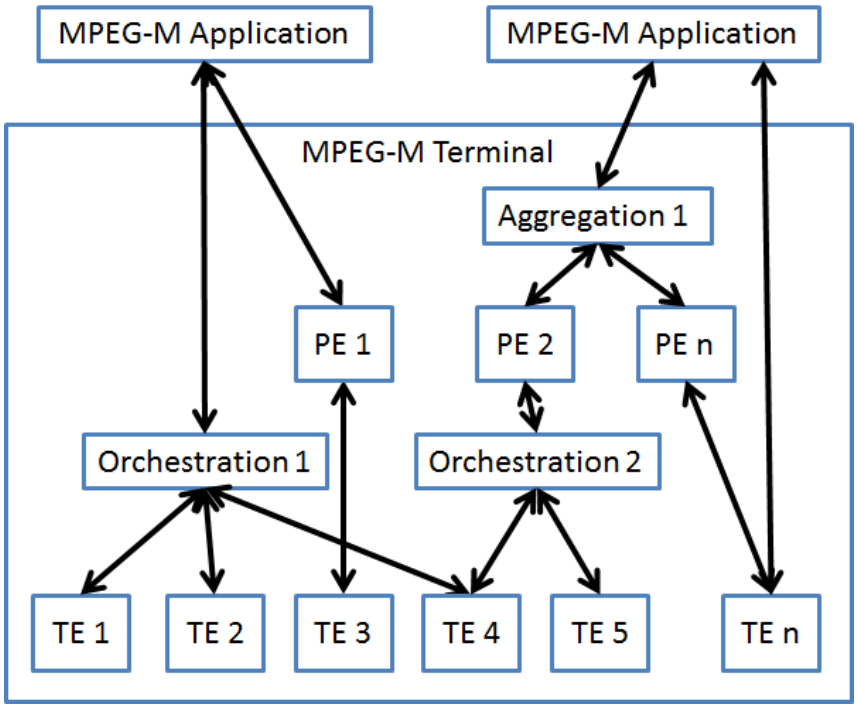
2.2.2 Επεκτάσιμο μεσισμικό

Το επεκτάσιμο μεσισμικό του MPEG-M [14] αποτελεί τη μονάδα λογισμικού μέσω της οποίας παρέχονται και καταναλώνονται στοιχειώδεις υπηρεσίες του MPEG-M. Εφαρμογές χτισμένες πάνω σε αυτό μπορούν να χρησιμοποιήσουν με διαφάνεια τις υπηρεσίες του MPEG-M χωρίς να εμπλέκονται σε βάθος στις τεχνολογίες που αυτές απαιτούν για τη λειτουργία τους, που πολλές φορές μπορεί να συμπεριλαμβάνουν και απομακρυσμένη επικοινωνία με διαδικτυακές υπηρεσίες. Αυτό επιτυγχάνεται με δύο τρόπους: Από τη μια εισάγεται η έννοια της μηχανής μεσισμικού, με κάθε μια να συγκεντρώνει τεχνολογίες και να παρέχει μέσω προγραμματιστικής διεπαφής λειτουργίες χρήσιμες σε όλα τα στάδια του κύκλου ζωής του περιεχομένου, από τη δημιουργία ως την κατανάλωση του. Από την άλλη, καλύπτονται οι απαιτήσεις κάθε εφαρμογής δίνοντας τη δυνατότητα για τον ορισμό και την εκτέλεση πολύπλοκων λειτουργικών αλυσίδων που αποτελούνται από υπηρεσίες που

παρέχουν οι διάφορες μηχανές μεσισμικού.

Οι μηχανές μεσισμικού χωρίζονται σε μηχανές τεχνολογιών και μηχανές πρωτοκόλλων. Οι τελευταίες αποτελούν το σημείο εισόδου στις στοιχειώδεις υπηρεσίες του MPEG-M και στηρίζονται στις μηχανές τεχνολογιών ώστε να εκτελέσουν τις λειτουργίες που απαιτεί κάθε στοιχειώδης υπηρεσία. Ωστόσο, οι μηχανές τεχνολογιών είναι δυνατό να χρησιμοποιηθούν και αυτόνομα.

Τέλος, μια εφαρμογή τυπικά χρειάζεται περισσότερες από μια κλήσεις προς το μεσισμικό ώστε να επιτελέσει μια λειτουργία υψηλού επιπέδου όπως η αναπαραγωγή περιεχομένου. Οι κλήσεις αυτές θα μπορούσαν να αφορούν είτε κλήσεις προς τις μηχανές τεχνολογίας είτε και προς τις μηχανές πρωτοκόλλου που παρέχουν τις στοιχειώδεις υπηρεσίες. Στην πρώτη περίπτωση το επεκτάσιμο μεσισμικό δίνει τη δυνατότητα να οριστούν ενορχηστρώσεις των κλήσεων προς τις μηχανές τεχνολογίας, ενώ στη δεύτερη μπορούν να οριστούν συνθέσεις των στοιχειωδών υπηρεσιών. Τα παραπάνω απεικονίζονται στο σχήμα που ακολουθεί, το οποίο παρουσιάζει ένα τερματικό MPEG-M, όπως ονομάζεται κάθε συσκευή στην οποία εκτελείται το επεκτάσιμο μεσισμικό.



Σχήμα 4: Αρχιτεκτονική επεκτάσιμου μεσισμικού του MPEG-M

Κεφάλαιο 3

Συσχέτιση ψηφιακών αντικειμένων

3.1 Εισαγωγή

Το διαδίκτυο σχεδιάστηκε στοχεύοντας στην υποστήριξη της επικοινωνίας μεταξύ υπολογιστικών συστημάτων. Ωστόσο η εξέλιξη του διαδικτύου [15] τοποθετεί τα υπολογιστικά συστήματα στο παρασκήνιο και βάζει στο προσκήνιο τα δεδομένα τα οποία ανταλλάσσουν μεταξύ τους, αλλά και τις υπηρεσίες που προσφέρουν [16]. Η διαθεσιμότητα πληροφορίας για τις σχέσεις που υφίστανται μεταξύ των δεδομένων αποτελεί μια θεμελιώδη απαίτηση για την εγκαθίδρυση του νέου αυτού παραδείγματος για το διαδίκτυο και τα πλεονεκτήματα που αυτό προσφέρει.

Ωστόσο, οι τρέχοντες μηχανισμοί για την περιγραφή των σχέσεων μεταξύ των δεδομένων έχουν περιορισμένη εκφραστικότητα, χαρακτηρίζονται από ακαμψία και πολλές φορές οδηγούν σε παρερμηνείες. Παραδείγματος χάρη, ο κύριος τρόπος με τον οποίο δηλώνεται η σχέση μεταξύ δύο ψηφιακών εγγράφων στο διαδίκτυο είναι η ενσωμάτωση αναφοράς του ενός στο άλλο χρησιμοποιώντας το URL τους. Στη γλώσσα HTML αυτό είναι δυνατό με τα στοιχεία <a> και <link>. Νέοι μηχανισμοί για τη σαφή περιγραφή τέτοιων σχέσεων, θα συνεισφέρουν στη σημασιολογική πληρότητα και ακρίβεια των περιγραφών, ενώ παράλληλα θα διευκολύνει την επεξεργασία και προσπέλαση των ψηφιακών εγγράφων.

Έχοντας τα παραπάνω κατά νου, σχεδιάστηκε ένας ευέλικτος μηχανισμός για τον

ορισμό σημασιολογικών σχέσεων μεταξύ ψηφιακών εγγράφων, χτίζοντας πάνω στα ψηφιακά αντικείμενα του προτύπου MPEG-21. Ο μηχανισμός αυτός, υιοθετεί τις σχετικές δομές που προσφέρει το πρότυπο και τις επεκτείνει με τη χρήση σημασιολογικών περιγραφών εκπεφρασμένων με τις τεχνολογίες του σημασιολογικού διαδικτύου RDF και OWL [17, 18]. Ο μηχανισμός αυτός επιτρέπει την πλήρη σημασιολογική περιγραφή των σχέσεων που προκύπτουν μεταξύ ψηφιακών αντικειμένων, ενώ ο μηχανισμός αυτός προτάθηκε και τελικώς ενσωματώθηκε ως επέκταση στο 3ο μέρος του προτύπου MPEG-21 [19, 20].

Η επόμενη παράγραφος φέρνει στην επιφάνεια τη διαρκώς αυξανόμενη ανάγκη για σαφή περιγραφή των σχέσεων που δημιουργούνται μεταξύ ψηφιακών εγγράφων, επισημαίνοντας την έλλειψη κατάλληλων εργαλείων. Στη συνέχεια, παρουσιάζονται τα ψηφιακά αντικείμενα του MPEG-21 και αναδεικνύονται οι περιορισμοί των μηχανισμών που προδιαγράφονται από το πρότυπο MPEG-21 σχετικά με την περιγραφή σχέσεων μεταξύ ψηφιακών αντικειμένων. Ακολούθως, περιγράφεται ο προτεινόμενος μηχανισμός και η προστιθέμενη αξία που προσφέρει σε τρεις χαρακτηριστικές περιπτώσεις χρήσης. Τέλος, παρουσιάζεται σύστημα υποστήριξης σημασιολογικής διαλειτουργικότητας το οποίο στηρίζεται στην προτεινόμενη δομή των λεξικών διαλειτουργικότητας.

3.2 Τρέχουσες τάσεις στην συσχέτιση ψηφιακών εγγράφων

Η επιτυχία σύγχρονων διαδικτυακών εφαρμογών εξαρτάται σε μεγάλο βαθμό από την ικανότητα τους να εκμεταλλευτούν και να χρησιμοποιήσουν προς όφελος των χρηστών τους τις σχέσεις που δημιουργούνται μεταξύ των κοινοτήτων των χρηστών τους με τα δεδομένα που μοιράζονται. Για παράδειγμα, το Facebook συλλέγει και χρησιμοποιεί τις σχέσεις φιλίας ή τις κοινοποιήσεις τύπου "Μου αρέσει!" (Like), το IEEExplore χρησιμοποιεί τις αναφορές των ερευνητών σε επιστημονικές εργασίες, ενώ η Amazon εξάγει συμπεράσματα σχετικά με τις καταναλωτικές συνήθειες των χρηστών τους δημιουργώντας προφίλ χρηστών ανάλογα με τα προϊόντα που αγοράζουν ή που απλά επισκέφτηκαν. Η αξιολόγηση του πλαισίου όπου οι παραπάνω σχέσεις δημιουργούνται γίνεται συνεπώς όλο και περισσότερο μια συμπαγής αναγκαιότητα.

Εν γένει, δύο εναλλακτικές στρατηγικές υπάρχουν σχετικά με τον τρόπο οπού μπο-

ρεί να εξαχθεί η πληροφορία για τις σχέσεις που δημιουργούνται μεταξύ δύο αφηρημένων οντοτήτων, έμμεσα ή άμεσα. Όταν χρησιμοποιούνται τεχνικές εξαγωγής συμπερασμάτων και τεχνητής νοημοσύνης έχουμε ουσιαστικά την σύνδεση των οντοτήτων με έμμεσο τρόπο, ενώ όταν οι ίδιοι οι χρήστες χρησιμοποιούν μηχανισμούς για να ορίσουν ρητά σημασιολογικά πλούσιες σχέσεις μεταξύ των οντοτήτων έχουμε τον ορισμό των σχέσεων με άμεσο τρόπο.

Η πρώτη στρατηγική έχει σημαντικές δυνατότητες, αφού για να λειτουργήσει δεν εξαρτάται στην ύπαρξη σχεσιακών μεταδεδομένων, αλλά ούτε και στην ποιότητα τους. Συνήθως χρησιμοποιούνται μηχανισμοί που βασίζονται στο περιεχόμενο ώστε να εξαχθούν χαμηλού επιπέδου συμπεράσματα που αφορούν στις ιδιότητες και τις σχέσεις των οντοτήτων που αναλύονται [21]. Ωστόσο, οι μηχανισμοί τεχνητής συμπερασματολογίας έχουν πολλές φορές αμφιλεγόμενα αποτελέσματα, τα οποία επιπρόσθετα είναι δύσκολο να επαληθευτούν [22].

Η δεύτερη στρατηγική προϋποθέτει την επένδυση των ίδιων των χρηστών στον ρητό καθορισμό των σχέσεων μεταξύ των οντοτήτων. Ωστόσο, μετά τον ορισμό των παραπάνω σχέσεων, αυτές μπορούν με απλότητα να χρησιμοποιηθούν καθολικά χωρίς κίνδυνο παρερμηνειών. Επί του παρόντος, είναι δυνατόν να βρεθούν τέτοιου είδους πληροφορίες σχετικά με τις οντότητες που μοιράζονται οι χρήστες με τη μορφή ετικετών τις οποίες ορίζουν οι χρήστες καθ' όλη τη διάρκεια του κύκλου ζωής περιεχομένου, από την παραγωγή του μέχρι την κατανάλωση του [23]. Ωστόσο, ακόμα και η παραπάνω τεχνική μπορεί να θεωρηθεί αναξιόπιστη καθότι εξαρτάται από υποκειμενικά κριτήρια και το γενικότερο πλαίσιο χρήσης των διαφόρων περιεχομένων.

Στην περίπτωση των ψηφιακών εγγράφων, ο ευκολότερος τρόπος για τον καθορισμό σχέσεων μεταξύ τους είναι η ενσωμάτωση ετεροαναφορών χρησιμοποιώντας το URL τους. Στη γλώσσα HTML αυτό είναι δυνατό με τα στοιχεία <a> και <link>. Οι προδιαγραφές των παραπάνω στοιχείων [24] περιλαμβάνουν υποστήριξη για τον ρητό καθορισμό του είδους της σχέσης μεταξύ δυο ψηφιακών εγγράφων, ωστόσο οι παρεχόμενοι τύποι σχέσεων είναι περιορισμένοι και μπορούν να οδηγήσουν σε σημασιολογικές παρερμηνείες. Τα παραπάνω είναι άλλωστε και οι λόγοι όπου ο μηχανισμός αυτός χρησιμοποιείται σε ελάχιστες περιπτώσεις και γενικότερα δεν αξιοποιείται ούτε από τους φυλλομετρητές αλλά ούτε

κι από τις μηχανές αναζήτησης [25].

Η τεχνολογία Microformats [26] προέκυψε ως λύση για την ενσωμάτωση μηχανικά αναγνώσιμων μεταδεδομένων σε HTML σελίδες, ενώ πρόσφατα κατέστη παρωχημένη από παρόμοιας λογικής τεχνολογίες όπως το W3C RDFa [27] και το schema.org [28] που αναπτύχθηκε και υποστηρίζεται από τις ισχυρότερες μηχανές αναζήτησης (Google, Yahoo, Bing). Η χρησιμοποίηση των παραπάνω τεχνολογιών καθιστά ικανή την μηχανική ανάγνωση και ανάλυση των σχετικών πληροφοριών και να συμβάλει στην συνδεσιμότητα μεταξύ των παντός είδους ψηφιακών εγγράφων.

Παράλληλα, αναπτύσσονται ραγδαία οι τεχνολογίες Σημασιολογικού Διαδικτύου (Semantic Web) και η πρωτοβουλία των Διασυνδεδεμένων Δεδομένων (Linked Data) [29] αποκτά μεγάλη απήχηση και προωθεί την εκμετάλλευση δομημένων μεταδεδομένων από εφαρμογές, ενώ έχει και ως ζητούμενο την διευκόλυνση των χρηστών στη δημιουργία μηχανικά αναγνώσιμων μεταδεδομένων. Προτείνεται η σύνδεση των διαφόρων οντοτήτων με πιο δομημένο τρόπο από την HTML, με την χρήση μεταδεδομένων που χαρακτηρίζονται από ακρίβεια, υποστηρίζουν μηχανικά υποστηριζόμενη εξαγωγή συμπερασμάτων και που ουσιαστικά θα καθιστούν την σημασιολογική αναζήτηση αποδοτική και συνεπώς χρήσιμη.

Το πρότυπο OAI-ORE (Open Archives Initiative Object Reuse and Exchange - [30]) χτίζει πάνω στη λογική των Διασυνδεδεμένων Δεδομένων και προδιαγράφει εργαλεία για τον ορισμό σημασιολογικών σχέσεων μεταξύ ψηφιακών εγγράφων, ωστόσο εστιάζει στην περιγραφή συλλογών τους. Πιο συγκεκριμένα, κάθε έγγραφο περιγράφεται ως μέλος μιας συλλογής εγγράφων και οι μεταξύ τους σχέσεις ορίζονται ως εσωτερικές σχέσεις που χαρακτηρίζουν τη συλλογή. Παραδείγματος χάρη, για τη δήλωση μιας σχέσης "διόρθωση" που υφίσταται μεταξύ δύο εγγράφων ο μηχανισμός προϋποθέτει τον ορισμό μιας συλλογής που τις περιέχει ώστε στη συνέχεια να τις συνδέσει με αυτή τη σχέση. Επιπλέον, το πρότυπο OAI-ORE δε στοχεύει στη δημιουργία αυτόνομων δομών για αυτές τα ψηφιακά έγγραφα και προτείνει την ανεξάρτητη διανομή του περιεχομένου από την περιγραφή του.

Αν και οι τελευταίες προτάσεις (W3C RDFa, Linked Data και OAI-ORE) έχουν οδηγήσει στην δημιουργία ενός εκτεταμένου δικτύου διασυνδεδεμένων δομημένων μεταδεδομένων, τα οποία περιγράφουν οντότητες παντός είδους και τις μεταξύ τους σχέσεις, αυτές

δεν έχουν υιοθετηθεί σε ευρεία κλίμακα. Επιπροσθέτως, στοχεύουν στην συμπλήρωση του σημασιολογικού κενού των ιστοσελίδων και όχι στη δημιουργία αυτοτελών εγγράφων με σημασιολογικά πλούσιες περιγραφές. Στην περίπτωση του RDFa τα μεταδεδομένα συνδυάζονται με τα δεδομένα, ενώ στην περίπτωση του OAI-ORE δεδομένα και μεταδεδομένα αποτελούν δύο ξεχωριστές δομές και διανέμονται χωριστά.

Από τα παραπάνω μπορεί κανείς να συμπεράνει πως οι υφιστάμενοι μηχανισμοί δεν καλύπτουν πλήρως τις σύγχρονες ανάγκες για αξιόπιστη και πρακτική σημασιολογική περιγραφή των σχέσεων μεταξύ αφηρημένων οντοτήτων, με τέτοιο τρόπο ώστε να μπορούν αυτές να αξιοποιηθούν χωρίς παρερμηνείες προς όφελος των χρηστών. Ένας τέτοιος μηχανισμός θα έπρεπε να απλουστεύει τη διάχυση των σημασιολογικών σχέσεων μεταξύ των οντοτήτων με έναν συνεκτικό τρόπο.

3.3 Μηχανισμοί συσχέτισης ψηφιακών αντικειμένων

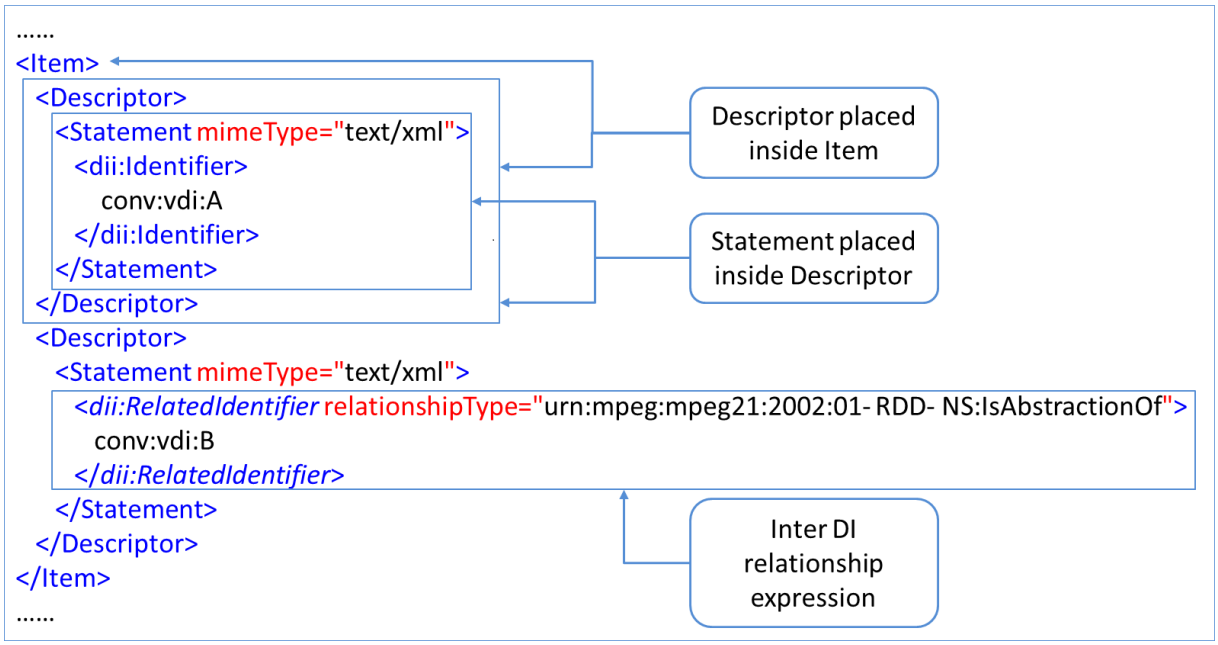
Τα ψηφιακά αντικείμενα αποτελούν μια σύγχρονη λύση για την ολοκληρωμένη περιγραφή και διαμοιρασμό δεδομένων. Τεχνολογίες όπως αυτή θα παίξουν καταλυτικό ρόλο στην υλοποίηση της στροφής που πραγματοποιούν οι υπηρεσίες σε πιο πληροφοριοκεντρικά μοντέλα. Τα ψηφιακά αντικείμενα ωστόσο αποτελούν σημαντικό καρπό των προσπαθειών της βιομηχανίας για την προτυποποίηση τους, κάτι που θα ενθαρρύνει τη διαδεδομένη υιοθέτηση τους.

Επιπρόσθετα, τα ψηφιακά αντικείμενα προσφέρουν τη δυνατότητα για την πολυδιάστατη περιγραφή δεδομένων, μετατρέποντας τα σε αυτοτελείς πληροφοριακές μονάδες. Οι ιδιότητες αυτές είναι συμβατές με τα σύγχρονα πληροφοριοκεντρικά μοντέλα, στα οποία οντότητες παντός είδους, όπως άνθρωποι, υπηρεσίες και αντικείμενα του πραγματικού κόσμου, έχουν μια ψηφιακή αναπαράσταση, η οποία περιγράφεται πλήρως από σημασιολογικά ακριβείς περιγραφές συμπεριλαμβανομένων των μεταξύ τους σχέσεων.

Επιπλέον, τα ψηφιακά αντικείμενα καλύπτουν πλήρως τις απαιτήσεις της στρατηγικής άμεσης συσχέτισης αυτοτελών δεδομένων, η οποία ούτως ή άλλως υπερέχει της στρατηγικής έμμεσης συσχέτισης τους (όπως παρουσιάστηκε και στην προηγούμενη πα-

ράγραφο) και αποτελούν ένα ευέλικτο εργαλείο για τη σύνδεση δεδομένων και μεταδεδομένων, διευκολύνοντας το διαμοιρασμό τους με έναν αξιόπιστο, διαφανή και συνεκτικό τρόπο. Ωστόσο, τα εργαλεία που προδιαγράφονται από το δεύτερο (Digital Item Declaration - DID - [8]) και το τρίτο (Digital Item Identification - DII - [31]) μέρος του προτύπου MPEG-21 επιτρέπουν μονάχα μια περιορισμένη και γενικά άκαμπτη περιγραφή των σχέσεων μεταξύ ψηφιακών αντικειμένων.

Το DID υποστηρίζει μονάχα την έμμεση έκφραση συμπερίληψης ή σύνθεσης μεταξύ ψηφιακών αντικειμένων ενθυλακώνοντας τα σχετικά στοιχεία XML, όπως θα υπαγόρευε μια αυστηρά γραμμική ιεραρχία (Σχήμα 5). Εναλλακτικά, τα στοιχεία του DID μπορούν να συμπεριλάβουν άλλα στοιχεία χρησιμοποιώντας το εργαλείο XInclude [32]. Ωστόσο, το XInclude καθιστά επίσης δυνατό μονάχα τον ορισμό της σχέσης της συμπερίληψης μεταξύ δύο ψηφιακών αντικειμένων.



Σχήμα 5: Συσχέτιση ψηφιακών αντικειμένων με χρήση του DII και DID [4]

Το DII προδιαγράφει το ρητό καθορισμό ενός περιορισμένου συνόλου συσχετίσεων μεταξύ ψηφιακών αντικειμένων μέσω της χρησιμοποίησης του στοιχείου RelatedIdentifier (σχετικό αναγνωριστικό) το οποίο ορίζει το χαρακτηριστικό relationshipType που υποδεικνύει το είδος της σχέσης (βλ. Σχήμα 5). Ο παραπάνω μηχανισμός είναι πιο ευέλικτος από αυτόν του DID, ωστόσο είναι ανεπαρκής για την έκφραση σχέσεων μεταξύ ψηφιακών αντι-

κειμένων που προκύπτουν φυσιολογικά.

Το τρίτο μέρος του προτύπου MPEG-21 , που αφορά στο DII επεκτάθηκε στο [33], έτσι ώστε το στοιχείο RelatedIdentifier να μπορεί να ορίζει και τη φύση των σχέσεων μεταξύ των ψηφιακών αντικειμένων, ωστόσο η διαθέσιμοι τύποι σχέσεων δεν καλύπτουν τις ανάγκες για πλήρη σημασιολογική περιγραφή αυτών των σχέσεων. Παράλληλα, η επέκταση απαιτεί την εγγραφή κάθε νέου τύπου σχέσης στην Αρχή Εγγραφών (Registration Authority) της διεθνούς οργάνωσης προτύπων ISO/IEC. Το παραπάνω είναι προφανώς μια μη αποδοτική προσέγγιση για τον ορισμό ταξινομήσεων σχέσεων και είναι σε καθαρά αντιδιαμετρικό σημείο από την προσέγγιση που θα ακολουθούσε φυσιολογικά κάποιος χρησιμοποιώντας το οντολογικά εργαλεία που προσφέρουν οι τεχνολογίες RDF και OWL, ώστε να περιγράψει με πληρότητα τη λογική σύνδεση μεταξύ των ψηφιακών αντικειμένων.

Οι μηχανισμοί που ορίζονται στο DID και DII είναι συνεπώς μη επαρκείς για την περιγραφή των σημασιολογικά πλούσιων σχέσεων που υφίστανται μεταξύ των ψηφιακών αντικειμένων. Η χρήση τους θα οδηγούσε σε περιορισμένες δυνατότητες εκμετάλλευσης των σχέσεων σε περίπτωση αναζήτησης σχετικών ψηφιακών αντικειμένων και θα δυσχέραινε τη χρήση κλασσικών και ευρέως διαδεδομένων εργαλείων ερωτήσεων όπως η γλώσσα SPARQL [34]. Επιπροσθέτως, δεν επιτρέπουν την περιγραφή πολύπλοκων σχέσεων όπως για παράδειγμα σχέσεων που χαρακτηρίζονται από τον χρόνο που δημιουργήθηκαν ή τον χρόνο που ισχύουν.

3.4 Επέκταση μηχανισμού συσχέτισης ψηφιακών αντικειμένων του MPEG-21

Η προτεινόμενη λύση βασίζεται και επεκτείνει τα ψηφιακά αντικείμενα προσθέτοντας έναν μηχανισμό που εκμεταλλεύεται τα πλεονεκτήματα των τεχνολογιών του σημασιολογικού διαδικτύου RDF και OWL και επιτρέπει την πλούσια και ακριβή περιγραφή των σχέσεων που προκύπτουν μεταξύ των ψηφιακών αντικειμένων. Η υιοθέτηση της από τους παραγωγούς περιεχομένου, θα έχει για αυτούς πολλαπλά πλεονεκτήματα, αφού θα

μπορούν με μια μοναδική δομή να πακετάρουν το περιεχόμενο τους μαζί με περιγραφικά μεταδεδομένα αλλά και τις σχέσεις που έχουν με άλλες δημιουργίες τους. Η λύση αυτή δημιουργεί ένα εύκολα επεξεργάσιμο και σημασιολογικά πλήρες πλαίσιο χρήσης για το περιεχόμενο, κάτι που θα συνεισφέρει στην αναβάθμιση του διαδικτύου και στον σημασιολογικό χειρισμό ψηφιακού περιεχομένου.

Έχοντας κατά νου τα συμπεράσματα της προηγούμενης παραγράφου, η προτεινόμενη λύση άρει τους περιορισμούς των υπαρχόντων μηχανισμών συσχέτισης ψηφιακών αντικειμένων που προδιαγράφει το πρότυπο MPEG-21 και επιτρέπει τη ρητή δήλωση σχέσεων μεταξύ ψηφιακών αντικειμένων με τη χρήση των τεχνολογιών σημασιολογικού διαδικτύου RDF και OWL. Ο προτεινόμενος μηχανισμός υλοποιείται ουσιαστικά με την προσθήκη ενός νέου στοιχείου με όνομα Relationships στο XML σχήμα του MPEG-21 DII, όπως απεικονίζεται στο πρώτο τμήμα του Σχήματος 6. Το στοιχείο αυτό θα περιέχει σε RDF μορφή τις περιγραφές για τις σχέσεις που μπορεί να έχει ένα ψηφιακό αντικείμενο και πρέπει να τοποθετείται μέσα σε ένα στοιχείο did:Descriptor.

Για τον ορισμό των παραπάνω σχέσεων με οντολογική μορφή προτάθηκε και μια βασική οντολογία για τις σχέσεις μεταξύ ψηφιακών αντικειμένων (MPEG-21 Core Ontology for DI Relationships - CODIR), η οποία απεικονίζεται στο δεύτερο τμήμα του Σχήματος 6. Η οντολογία αυτή, όπως και το στοιχείο Relationships προτάθηκαν και τελικώς ενσωματώθηκαν στο πρότυπο MPEG-21 ως επέκταση και προσφέρουν τις βάσεις ώστε να εκφράσει κάποιος τις σχέσεις που προκύπτουν μεταξύ ψηφιακών αντικειμένων. Πίο συγκεκριμένα, οι χρήστες καλούνται να επεκτείνουν την MPEG-21 CODIR οντολογία και να ορίσουν τις σχέσεις που εμφανίζονται στο καθορισμένο πεδίο της εφαρμογής τους. Οι οντολογίες αυτές δεν είναι απαραίτητο να δηλωθούν σε κάποια κεντρική αρχή, αντίθετα μπορούν να χρησιμοποιούνται ελεύθερα στο συγκεκριμένο πλαίσιο κάθε εφαρμογής. Τα παραπάνω απελευθερώνουν τη χρήση των σχέσεων τόσο από τις περιορισμένες σχέσεις που παρείχε το πρότυπο για το στοιχείο RelatedIdentifier, όσο κι από την εξάρτηση από κεντρική αρχή για δήλωση νέων σχέσεων.

Η παραπάνω λύση βρίσκεται σε συμφωνία με την πρωτοβουλία για τη διασύνδεση των δεδομένων Linked Data, αφού χρησιμοποιεί μοναδικά αναγνωριστικά URI για τα δεδομένα, δημιουργεί δομημένα μεταδεδομένα όπως και σημασιολογικές συνδέσεις μεταξύ

a

```
<xs:element name="Relationships">
  <xs:complexType mixed="true">
    <xs:sequence>
      <xs:element
        xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax- ns#"
        ref="rdf:RDF" minOccurs="1" maxOccurs="1"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
```

b

```
<rdf:RDF xmlns="mpeg21:corerelationalontology"
  xmlns:mpeg21coreRelOnt="mpeg21:corerelationalontology"
  ..............>

  <owl:Ontology rdf:about="mpeg21:corerelationalontology"/>

  <!-- Classes -->
  <owl:Class rdf:about="mpeg21:corerelationalontology;DigitalItem"/>
  <owl:Class rdf:about="&owl;Thing"/>

  <!-- Object Properties -->
  <owl:ObjectProperty rdf:about="&mpeg21coreRelOnt;interDIRelationship">
    <rdfs:domain rdf:resource="&mpeg21coreRelOnt;DigitalItem"/>
    <rdfs:range rdf:resource="&mpeg21coreRelOnt;DigitalItem"/>
  </owl:ObjectProperty>
</rdf:RDF>
```

c

```
<Descriptor>
  <Statement mimeType="text/xml">
    <dii:Relationships mimeType="application/rdf+xml">
      <rdf:RDF xmlns="individual:example:ontology#"
        xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">
        <DigitalItem rdf:about="DI_A">
          <rdf:type rdf:resource="&owl;DigitalItem"/>
          <correction rdf:resource="DI_B"/>
        </DigitalItem>
        <DigitalItem rdf:about="DI_B">
          <rdf:type rdf:resource="&owl;DigitalItem"/>
        </DigitalItem>
      </rdf:RDF>
    </dii:Relationships>
  </Statement>
</Descriptor>
```

Σχήμα 6: Οι προτεινόμενες επεκτάσεις του 3ου μέρους του προτύπου MPEG-21 [4]

των δεδομένων με την τεχνολογία RDF. Παράλληλα, η λύση είναι συμβατή και με το πρότυπο MPEG-21 αφού το επεκτείνει με την προσθήκη ενός νέου στοιχείου το οποίο θα περιέχει μεταδεδομένα σε μορφή RDF αποκλειστικά για τις σχέσεις μεταξύ ψηφιακών αντικειμένων.

Ένα παράδειγμα χρήσης του παραπάνω μηχανισμού θα ήταν το παρακάτω σενάριο : Έστω το ψηφιακό αντικείμενο A το οποίο θεωρείται διόρθωση του ψηφιακού αντικειμένου B. Τα δύο αυτά ψηφιακά αντικείμενα είναι λοιπόν συνδεδεμένα με την σχέση της διόρθωσης και σε μορφή τριάδας RDF αυτό σημαίνει πως το πρώτο αποτελεί το υποκείμενο (subject) της τριάδας, το δεύτερο αποτελεί το αντικείμενο (object) της τριάδας ενώ η σχέση "διόρθωση" αποτελεί το κατηγορούμενο (predicate) της τριάδας. Η τελευταία θα έχει δηλωθεί ως επέκταση της βασικής σχέσης interDIRelationship που ορίζεται από την MPEG-21 CODIR, ενώ τα δύο ψηφιακά αντικείμενα θα ορίζονται ως μέλος της κλάσης DigitalItem που συγκεντρώνει το σύνολο των ψηφιακών αντικειμένων. Το τρίτο μέρος του Σχήματος 6 απεικονίζει την παραπάνω περιγραφή όπως θα τοποθετούνταν στο υποκείμενο ψηφιακό αντικείμενο A.

3.5 Περιπτώσεις χρήσης

Σε αυτή την παράγραφο παρουσιάζονται πιθανά σενάρια χρήσης της προτεινόμενης λύσης και αναδεικνύεται η προστιθέμενη αξία που προσφέρει τόσο στην υποκειμενική αλλά και την αντικειμενική αντίληψη της ποιότητας εμπειρίας μιας εφαρμογής. Η χρήση του μηχανισμού προάγει την συμπερίληψη πληροφορίας που αφορά στις σχέσεις που υφίστανται μεταξύ των ψηφιακών αντικειμένων στα υπόλοιπα μεταδεδομένα που τα αφορούν. Η πληροφορία αυτή συνδέει τα ψηφιακά αντικείμενα μεταξύ τους δημιουργώντας γύρω τους έναν ιστό από σχετικά ψηφιακά αντικείμενα και επιτρέπει στις εφαρμογές την αυτόματη και ακριβή ανίχνευση των σχέσεων αυτών και την ευφυή χρησιμοποίηση αυτής της γνώσης –που διαφορετικά θα είχε διαφύγει– στην αναζήτηση, ανάκτηση, πρόσβαση και αλληλεπίδραση των των χρηστών με τα ψηφιακά αντικείμενα.

Παρακάτω παρουσιάζονται πιθανά σενάρια χρήσης του προτεινόμενου μηχανισμού συσχέτισης και εξετάζουν την προστιθέμενη αξία που προσφέρει η υιοθέτηση της.

3.5.1 Αναζήτηση περιεχομένου

Η ρητή δήλωση των σχέσεων μεταξύ ψηφιακών αντικειμένων έχει θετικά αποτελέσματα στην καταλογογράφηση τους (indexing) από τις μηχανές αναζήτησης, αφού δεν χρειάζεται πλέον να εξάγουν συμπεράσματα σχετικά με τις συνδέσεις που υφίστανται μεταξύ τους. Τα ποσοστά της ακρίβειας (precision) και της ανάκλησης (recall) των αναζητήσεων (κλασικές μετρικές για την ποιότητα ενός μηχανισμού αναζήτησης) βελτιώνονται εκμεταλλευόμενες τις σημασιολογικές συνδέσεις που περιγράφονται με οντολογικό τρόπο. Πιο συγκεκριμένα, μπορεί να υπολογιστεί η σημασιολογική συνάφεια μεταξύ δύο ψηφιακών αντικειμένων, χρησιμοποιώντας τις οντολογικές σχέσεις που τα συνδέουν είτε αυτές προέρχονται από την ίδια είτε από διαφορετική οντολογία. Αυτό καθίσταται δυνατό μέσω συνδέσεων που μπορεί να υπάρχουν μεταξύ των οντολογιών, όπως η rdf:subPropertyOf, skos:narrower ή owl:sameAS. Με τις δύο πρώτες μπορεί να δηλωθεί πως μια σχέση είναι πιο συγκεκριμένη από μια άλλη, ενώ με την τελευταία μπορεί να δηλωθεί η σημασιολογική ταύτιση δύο οντολογικών σχέσεων που έχουν οριστεί σε διαφορετικές οντολογίες. Παραδείγματος χάρη, η σχέση "διόρθωση" είναι πιο συγκεκριμένη από τη σχέση "σχολιασμός", και πιο ευρεία ως έννοια από τη σχέση "γραμματική_διόρθωση".

Η αναζήτηση βάσει των οντολογικών σχέσεων μεταξύ ψηφιακών αντικειμένων οδηγεί σε αποτελέσματα με μεγάλη ακρίβεια, ενώ εκμεταλλευόμενοι τις σχέσεις που υφίστανται μεταξύ των οντολογικών σχέσεων μπορεί να επιτευχθεί διεύρυνση των αποτελεσμάτων οδηγώντας σε υψηλότερη ανάκληση.

Για την αύξηση της ακρίβειας μιας αναζήτησης για τα σχετικά ψηφιακά αντικείμενα κάποιου ψηφιακό αντικειμένου, η ερώτηση αναζήτησης μπορεί να μετασχηματιστεί έτσι ώστε να αφορά σε πιο ειδικές σχέσεις από την ίδια οντολογία (που ενώνονται με rdf:subPropertyOf) ή πιο ειδικές σχέσεις από διαφορετικές οντολογίες (που ενώνονται με skos:narrower).

Όταν στην ερώτηση αναζήτησης σχετικών ψηφιακών αντικειμένων χρησιμοποιηθούν και σχέσεις οι οποίες είναι γενικότερες, τότε έχουμε αυτόματα διεύρυνση του πεδίου αναζήτησης και των ψηφιακών αντικειμένων που πληρούν τους όρους της αναζήτησης. Στην περίπτωση αυτή εκμεταλλευόμαστε σχέσεις όπως η owl:sameAs ή skos:broader.

Στην παρακάτω ερώτηση SPARQL (Σχήμα 7) χρησιμοποιείται η παραπάνω τεχνική ώστε να αυξηθούν τα αποτελέσματα που επιστρέφει η αναζήτηση. Πιο συγκεκριμένα, η ερώτηση αναζήτησης μετασχηματίζεται αντικαθιστώντας τη σχέση "σχολιασμός" (commenting) σε "απόκριση" (responding).

```
//Original Query
PREFIX rdf: <.....>
PREFIX bco: <.....>
PREFIX bco:instances <.....>

SELECT ?x WHERE
{   ?x rdf:type bco:WE-DID
    ?x bco:commenting ?y
    ?y rdf:type bco:WE-DID}

//Reformulated Query
PREFIX rdf: <.....>
PREFIX bco: <.....>
PREFIX bco:instances <.....>

SELECT ?x WHERE
{   ?x rdf:type bco:WE-DID
    ?x bco:responding ?y
    ?y rdf:type bco:WE-DID}
```

Σχήμα 7: Μετασχηματισμός ερώτησης αναζήτησης για αύξηση του ποσοστού ανάκτησης αποτελεσμάτων της αναζήτησης [4]

Οι παραπάνω μηχανισμοί επιτρέπουν την αύξηση των ποσοστών ακριβείας και ανάκτησης μιας αναζήτησης και ουσιαστικά συνεισφέρουν στην ποιότητα εμπειρίας μιας υπηρεσίας σχετικής με την ανακάλυψη περιεχομένου.

3.5.2 Παρουσίαση περιεχομένου

Οι σχέσεις που υπάρχουν μεταξύ ψηφιακών αντικειμένων μπορούν να χρησιμοποιηθούν για τη δημιουργία του γραφικού περιβάλλοντος μιας εφαρμογής. Έτσι, όταν κάποιο

ψηφιακό αντικείμενο βρίσκεται στο προσκήνιο, μαζί με αυτό μπορούν να εμφανίζονται και τα σχετικά με αυτό ψηφιακά αντικείμενα δίνοντας έτσι στο χρήστη μια πλήρη εικόνα των υπαρχόντων περιεχομένων μιας υπηρεσίας και επιτρέποντας του να έχει πλήρη εποπτεία κατά την εξερεύνηση περιεχομένων ενδιαφέροντος. Επιπρόσθετα, τα οντολογικά σχεδιασμένα γραφικά περιβάλλοντα [35] προωθούν τη δυναμική προσαρμογή και εξατομίκευση του γραφικού περιβάλλοντος ανάλογα με τις ανάγκες του κάθε χρήστη και παρέχουν άκρως διαδραστικό περιβάλλον για την εξερεύνηση και προσπέλαση του περιεχομένου. Για παράδειγμα, οι χρήστες μιας υπηρεσίας διαμοιρασμού βίντεο, μπορούν να σχολιάσουν το βίντεο ή να αποκριθούν σε αυτό με ένα δικό τους βίντεο. Έτσι, εάν κάποιος χρήστης βλέπει τη σελίδα του βίντεο με τα σχόλια που έχουν γίνει για αυτό, μπορεί να ενεργοποιήσει και την εμφάνιση των αποκρίσεων σε αυτό με βίντεο, διευρύνοντας τα προς εμφάνιση σχετικά ψηφιακά αντικείμενα.

3.5.3 Ταξινόμηση περιεχομένου

Οι σχέσεις μεταξύ των ψηφιακών αντικειμένων μπορούν να χρησιμοποιηθούν όμως και για την ταξινόμηση του περιεχομένου μιας ή περισσοτέρων εφαρμογών με παρόμοιο τρόπο όπως η τεχνική PageRank της Google [36]. Τα ψηφιακά αντικείμενα με τις περισσότερες εισερχόμενες σχέσεις θα θεωρούνται και τα πιο δημοφιλή και θα προωθούνται, ενώ οι χρήστες της υπηρεσίας θα ωφελούνται από την διαδικασία της ταξινόμησης. Επιπρόσθετα, η ρητή δήλωση του είδους της σχέσης δύο ψηφιακών αντικειμένων εξαλείφει την ανάγκη για εύρεση του τύπου αυτής της σχέσης και μπορεί να χρησιμοποιηθεί σε εκλεπτυσμένες μεθόδους ταξινόμησης, παραδείγματος χάρη ορίζοντας βάρη ανάλογα με το είδος της σχέσης [37] ή εκμεταλλευόμενοι το γράφο που δημιουργούν οι ιεραρχίες των σχέσεων των ψηφιακών αντικειμένων [38].

3.6 Σύστημα υποστήριξης σημασιολογικής διαλειτουργικότητας

Στις προηγούμενες παραγράφους παρουσιάστηκαν τα ζητήματα διασύνδεσης μεταξύ ψηφιακών αντικειμένων και προτάθηκε λύση βασισμένη σε διεθνή πρότυπα ώστε να υποστηρίζει και να διευκολύνει την ενσωμάτωση της από πολλαπλά συστήματα. Η λύση αυτή καλύπτει τις εκφραστικές ανάγκες για τη διασύνδεση των ψηφιακών αντικειμένων, εισάγοντας ευρύτατα διαδεδομένες τεχνολογίες του σημασιολογικού διαδικτύου. Στη βάση της λύσης βρίσκεται η οντολογία CODIR που ορίζει τις βασικές έννοιες για την περιγραφή των σχέσεων μεταξύ των ψηφιακών αντικειμένων και τα διάφορα συστήματα καλούνται να την επεκτείνουν ορίζοντας τις δικές τους οντολογίες με τις σχέσεις που εμφανίζονται στις δικές τους εφαρμογές. Η CODIR, δίνει ουσιαστικά τη βάση για τη διαλειτουργικότητα των προαναφερθέντων σχέσεων, ωστόσο προκύπτει σημασιολογικό κενό στη συσχέτιση των οντολογικών εννοιών που ορίζουν οι χρήστες.

Το σύστημα που παρουσιάζεται στις επόμενες παραγράφους προδιαγράφει αρχιτεκτονική η οποία στοχεύει να επιλύσει το παραπάνω ζήτημα και να υποστηρίξει την περαιτέρω διαλειτουργικότητα μεταξύ των οντολογιών που ορίζουν οι χρήστες. Για τον λόγο αυτό, ενσωματώνει τις οντολογίες των χρηστών και τις πρότυπες οντολογίες και ορίζει τα λεξικά διαλειτουργικότητας που δρουν ως σημασιολογικές γέφυρες μεταξύ των εννοιών διαφορετικών οντολογιών. Συγκεντρώνοντας τα παραπάνω σε μια βάση γνώσης, η οποία απεικονίζονται στο σχήμα 8 με τη μορφή πυραμίδας, το σύστημα παρέχει σημασιολογικές υπηρεσίες όπως η εύρεση σημασιολογικά ισοδύναμων εννοιών και η εύρεση σημασιολογικών εννοιών βάσει προθέματος. Οι παραπάνω υπηρεσίες μπορούν να βρουν εφαρμογή σε πολλαπλά σενάρια χρήσης, όπως στον ορισμό σημασιολογικών σχέσεων και περιγραφών και την επέκταση ήδη υπαρχόντων περιγραφών ή σημασιολογικών ερωτημάτων.

3.6.1 Λεξικό διαλειτουργικότητας

Τα λεξικά διαλειτουργικότητας αποτελούν μια δομή η οποία σχεδιάστηκε για να επιλύσει τα προβλήματα σημασιολογικής διαλειτουργικότητας που προκύπτουν στην εν-

Σχήμα 8: Η πυραμίδα των οντολογιών του συστήματος

σωμάτωση μεταδεδομένων μεταξύ διαφορετικών συστημάτων. Στην ουσία, τα λεξικά αποτελούν τα ίδια οντολογίες, όπως ακριβώς και οι οντολογίες χρηστών και οι πρότυπες οντολογίες. Σε αντίθεση όμως με τις υπόλοιπες οντολογίες, δεν στοχεύει στην περιγραφή των οντοτήτων και των μεταξύ τους σχέσεων που υφίστανται σε μια συγκεκριμένη θεματική περιοχή, αλλά στην σημασιολογική σύνδεση των εννοιών που ορίζονται σε διαφορετικές οντολογίες. Αυτό περιλαμβάνει σχέσεις ισοδυναμίας και σχέσεις που αφορούν στην ευρύτητα των εννοιών που ορίζονται στις οντολογίες. Για τον λόγο αυτό το λεξιλόγιο που χρησιμοποιούν τα λεξικά διαλειτουργικότητας προέρχεται από το σχήμα RDF, την γλώσσα OWL και το SKOS (Simple Knowledge Organisation System - Σύστημα Απλής Οργάνωσης Γνώσης - SKOS - [39]). Για παράδειγμα, εάν μια έννοια αποτελεί μέρος κάποιας άλλης έννοιας τότε μπορεί να προκύψει η σύνδεση τους με την σχέση rdf:subClassOf. Εάν δύο έννοιες δύο διαφορετικών οντολογιών έχουν ακριβώς το ίδιο νόημα τότε μπορούν να συνδεθούν με τη σχέση owl:sameAs. Ενώ εάν οι δύο αυτές έννοιες δεν μπορούν να συνδεθούν με τα παραπάνω, αλλά περιγράφουν σχετικές έννοιες σε διαφορετική κλίμακα ή ευρύτητα, αυτές

μπορούν να συνδεθούν με την σχέση skos:broader.

Το σχήμα 9 απεικονίζει αποσπάσματα από δύο οντολογίες οι οποίες περιγράφουν τη θεματική περιοχή των κινηματογραφικών ταινιών και το λεξικό διαλειτουργικότητας που τις συνδέει. Η οντολογία Movie Ontology [1](γραμμές 1–7) ορίζει την κλάση των ταινιών (γραμμή 2) και την σχέση τίτλος με το πεδίο ορισμού και τιμών της (γραμμή 3–6). Αντίστοιχους ορισμούς έχει και η οντολογία IMDB [40] (γραμμές 8–14). Τέλος, το λεξικό που τις συνδέει (γραμμές 15–22) ορίζει σχέσεις ισοδυναμίας μεταξύ των δύο κλάσεων ταινιών και των σχέσεων για τους τίτλους τους.

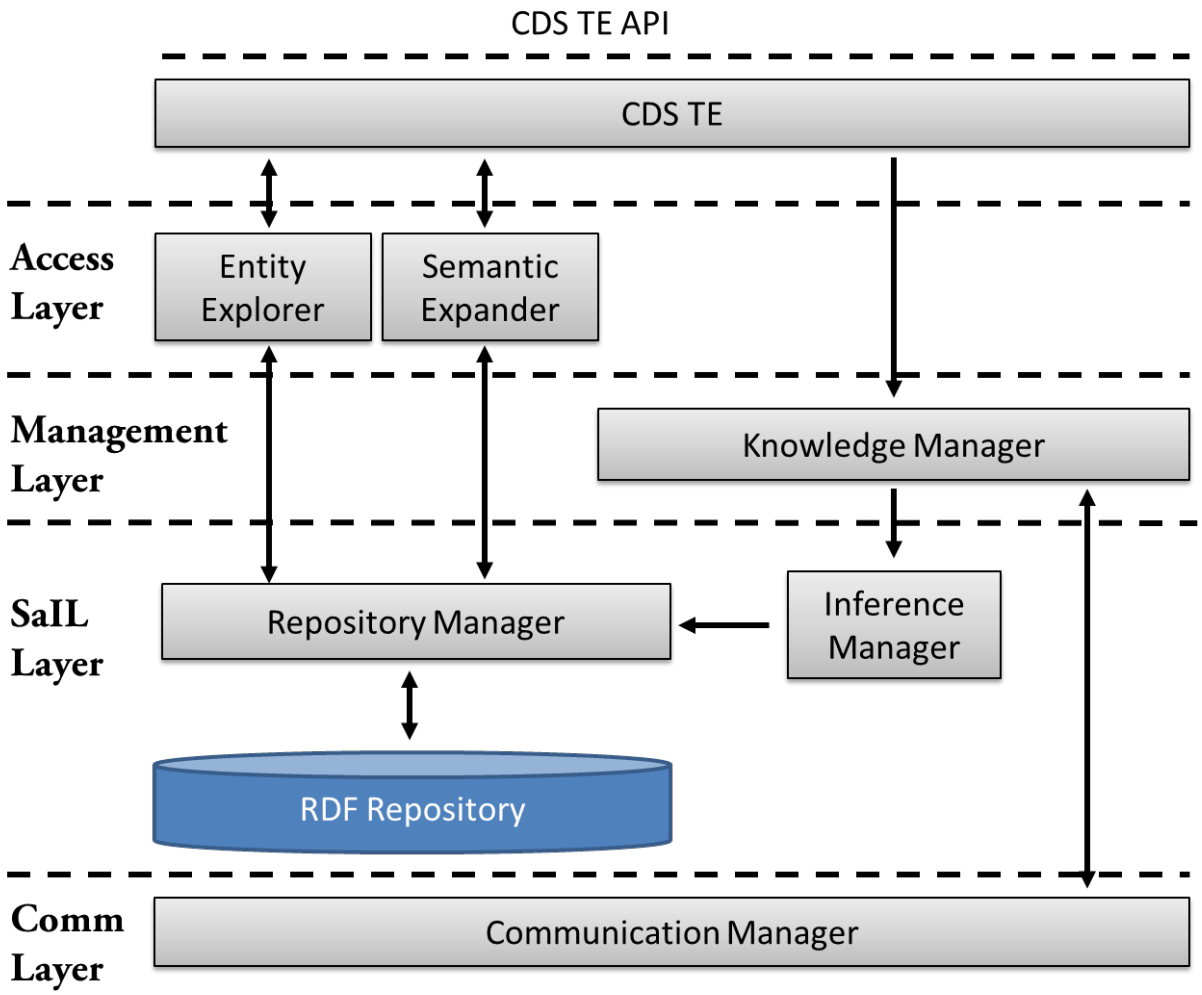
```
01 <!-------------MOVIE ONTOLOGY-------------->
02 <owl:Class rdf:about="&movieOntology;Movie"/>
03 <owl:DatatypeProperty rdf:about="&movieontology;title">
04   <rdfs:domain rdf:resource="&movieOntology;Movie"/>
05   <rdfs:range rdf:resource="&xsd;string"/>
06 </owl:DatatypeProperty>
07 ...
08 <!-------------IMDB ONTOLOGY-------------->
09 <owl:Class rdf:about="&imdb;Movie"/>
10 <owl:DatatypeProperty rdf:about="&imdb;title">
11   <rdfs:domain rdf:resource="&imdb;Movie"/>
12   <rdfs:range rdf:resource="&xsd;string"/>
13 </owl:DatatypeProperty>
14 ...
15 <!-------------IMDB2MOVIE ONTOLOGY DICTIONARY-------------->
16 <owl:Class rdf:about="&movieOntology;Movie">
17   <owl:equivalentClass rdf:resource"=&imdb;"Movie/>
18 </owl:Class>
19 <owl:DatatypeProperty rdf:about="&movieontology;title">
20   <owl:equivalentProperty rdf:resource"=&imdb;"title/>
21 </owl:DatatypeProperty>
22 ...
```

Σχήμα 9: Παράδειγμα λεξικού διαλειτουργικότητας (απόσπασμα)

3.6.2 Αρχιτεκτονική

Η αρχιτεκτονική του συστήματος χωρίζεται σε 4 επίπεδα, ανάλογα με το ρόλο που έχουν και τη λειτουργικότητα που προσφέρουν. Τα επίπεδα αυτά και οι αλληλεπιδράσεις τους απεικονίζονται στο σχήμα 10.

[1]www.movieontology.org



Σχήμα 10: Η αρχιτεκτονική της μηχανής τεχνολογίας CDS.

Ο ρόλος κάθε επιπέδου και των επιμέρους λειτουργικών τους μονάδων, επεξηγούνται στον παρακάτω Πίνακα 2.

Επίπεδο	**Λειτουργικές Μονάδες**
Πρόσβαση	Το επίπεδο αυτό παρέχει σημασιολογικές υπηρεσίες σχετικές με τις οντολογίες του συστήματος και αποτελείται από τις παρακάτω λειτουργικές μονάδες:

	SemanticExpander: Η μονάδα αυτή επεκτείνει τις RDF δηλώσεις που της παρέχονται και δημιουργεί σημασιολογικά ισοδύναμες περιγραφές, εκμεταλλευόμενη τις οντολογίες και τα λεξικά διαλειτουργικότητας του συστήματος. **EntityExplorer:** Η μονάδα αυτή επιτρέπει την αναζήτηση οντοτήτων των οντολογιών με πολλαπλά κριτήρια, όπως πρόθεμα της ετικέτας τους (label) ή της κλάσης στην οποία ανήκουν.
Διαχείριση	Το επίπεδο αυτό διαχειρίζεται τις οντολογίες και τα λεξικά του συστήματος σε υψηλό επίπεδο και αποτελείται από την παρακάτω λειτουργική μονάδα : **KnowledgeManager:** Η μονάδα αυτή αναλαμβάνει τη φόρτωση των οντολογιών και των λεξικών του συστήματος και εκκινεί τη διαδικασία λήψης απομακρυσμένων οντολογιών ή λεξικών εάν αυτά χρειάζονται στο σύστημα.
Αποθήκευση και Εξαγωγή Συμπερασμάτων	Το επίπεδο αυτό διαχειρίζεται την αποθήκευση των οντολογιών και των λεξικών του συστήματος και είναι υπεύθυνο για την εξαγωγή επιπρόσθετων συμπερασμάτων. Οι λειτουργικές του μονάδες είναι οι παρακάτω : **RepositoryManager:** Η μονάδα αυτή διαχειρίζεται την αποθήκευση των οντολογιών και των λεξικών με μορφή δηλώσεων RDF. Η χρήση των RDF δηλώσεων ως βασικής δομής επικοινωνίας με την συγκεκριμένη μονάδα του συστήματος, επιτρέπει τη δημιουργία διαφορετικών υλοποιήσεων για την αποθήκευση των δηλώσεων RDF, όπως αποθήκευση στη μνήμη, στο δίσκο ή σε σχεσιακή βάση. Παράλληλα, παρέχει μεθόδους για την ερώτηση της βάσης γνώσης στη γλώσσα ερωτήσεων SPARQL.

	InferenceEngine: Η μονάδα αυτή αναλαμβάνει την εξαγωγή συμπερασμάτων σχετικά με τις οντολογίες που διαχειρίζεται το σύστημα και με βασική δομή τα λεξικά διαλειτουργικότητας υλοποιεί (materialize) και επεκτείνει την συμπυκνωμένη γνώση των οντολογιών σε RDF δηλώσεις. Προτού αποθηκεύσει τη γνώση στη βάση γνώσης του συστήματος, ελέγχει την συνέπεια των εξαγόμενων συμπερασμάτων με την ήδη υπάρχουσα γνώση, έτσι ώστε να αποφευχθούν αντιφάσεις.
Επικοινωνία	Το επίπεδο αυτό διαχειρίζεται την απομακρυσμένη επικοινωνία με το σύστημα και αποτελείται από την παρακάτω λειτουργική μονάδα : **CommunicationManager:** Η μονάδα αυτή διαχειρίζεται την απομακρυσμένη επικοινωνία με το σύστημα και παρέχει πρόσβαση στις λειτουργίες του, όπως λήψη απομακρυσμένων οντολογιών ή λεξικών.

Πίνακας 2: Λειτουργικές μονάδες του συστήματος και οι αλληλεπιδράσεις τους

3.7 Σύνοψη

Ο μηχανισμός συσχέτισης ψηφιακών αντικειμένων που παρουσιάστηκε σε αυτό το κεφάλαιο προωθεί τη ρητή και ακριβή δήλωση του πλαισίου των σχέσεων που υφίστανται μεταξύ τους και επιτρέπει την χωρίς παρερμηνείες επεξεργασία τους. Το πλαίσιο αυτό παρέχεται με τρόπο που είναι συμβατός με τις εξελίξεις στο Σημασιολογικό Διαδίκτυο και δηλώνεται μέσα από τις υπάρχουσες δομές του διαδεδομένου προτύπου MPEG-21, το οποίο παρέχει εγγενώς υποστήριξη για την αναπαράσταση και συνδιαλλαγή πολύπλοκου ψηφιακού περιεχομένου.

Ο μηχανισμός με τη χρήση των τεχνολογιών του Σημασιολογικού Διαδικτύου προωθεί τη δημιουργία ενός παγκόσμιου πλέγματος που ενώνει μεταξύ του όλο το διαδικτυακό

περιεχόμενο, ενώ απλοποιεί τη δημιουργία πολύπλοκων συστημάτων οι οποίες εκμεταλλεύονται την επεκτασιμότητα και συνδεσιμότητα των περιγραφών των σχέσεων μέσω οντολογιών.

Οι σημασιολογικά πλούσιες περιγραφές των σχέσεων μεταξύ των ψηφιακών αντικειμένων επιτρέπουν την εκτέλεση έξυπνων αναζητήσεων, οι οποίες εκμεταλλεύονται αυτές τις σχέσεις αλλά και τις συνδέσεις μεταξύ αυτών καθεαυτών των σχέσεων (οι οποίες ορίζονται στα πλαίσια μίας ή περισσότερων οντολογιών). Επιτρέπει, παραδείγματος χάρη το μετασχηματισμό ενός ερωτήματος αναζήτησης σε πιο ειδικό ή πιο γενικό, διαλέγοντας έτσι ανάμεσα στο πλήθος ή την ποιότητα των αποτελεσμάτων που επιστρέφονται.

Η προσθήκη του παραπάνω μηχανισμού ενδυναμώνει το MPEG-21 και το καθιστά ταιριαστό εργαλείο για τον καθορισμό των σχεσιακού ιστού που συνδέει τα ψηφιακά αντικείμενα μεταξύ τους και βελτιώνει την επεξεργασία, ανακάλυψη και διανομή τους. Οι χρήστες πληροφοριοκεντρικών υπηρεσιών από την πλευρά τους λαμβάνουν γρηγορότερη και πιο ακριβή πρόσβαση στα περιεχόμενα που τους ενδιαφέρουν, κάτι που οδηγεί σε καλύτερη αλληλεπίδραση με την υπηρεσία και αντιστοιχεί σε καλύτερη πρόσληψη της ποιότητας της.

Τέλος, το σύστημα σημασιολογικής διαλειτουργικότητας υποστηρίζει τη σημασιολογική διαλειτουργικότητα μεταξύ περιγραφών που προκύπτουν από διαφορετικές οντολογίες, εισάγοντας τη δομή των λεξικών διαλειτουργικότητας, τα οποία δρουν ως σημασιολογικές γέφυρες μεταξύ των εννοιών διαφορετικών οντολογιών και βάσει αυτών παρέχονται σημασιολογικές υπηρεσίες χρήσιμες σε κάθε είδους πληροφοριοκεντρικές εφαρμογές.

Κεφάλαιο 4

Ασφαλής διαχείριση ψηφιακών αντικειμένων

4.1 Εισαγωγή

Η πληροφορία καθίσταται όλο και πιο περισσότερο ένα πολύτιμο αγαθό για παντός είδους οργανισμούς. Η χάραξη στρατηγικών και η λήψη αποφάσεων επηρεάζονται άμεσα τόσο από τους μηχανισμούς εξαγωγής γνώσης, όσο και της ποιότητας των εισερχόμενων πληροφοριών. Επιπρόσθετα, οι αλυσίδες παροχής υπηρεσιών γίνονται όλο και πιο πολύπλοκες, περιλαμβάνοντας πολλούς και ετερογενείς χρήστες, προϋποθέτοντας την ανταλλαγή πληροφοριών μεταξύ τους με δυναμικό ad hoc τρόπο, δημιουργώντας προσωρινές κοινότητες.

Αυτή η τάση οδήγησε στην ανάπτυξη νέων παραδειγμάτων επικοινωνίας όπως τα συστήματα δημοσίευσης/συνδρομής (publish/subscribe systems- [41]) και υποδομών βασισμένων στο σύννεφο (cloud-based systems - [42]) τα οποία υιοθετούν την έννοια της παντοχού παρούσας πληροφορίας. Παράλληλα εμφανίστηκαν και νέες πηγές δεδομένων όπως για παράδειγμα τα ασύρματα δίκτυα αισθητήρων (Wireless Sensors Networks - WSN - [43]) και το Διαδίκτυο των Πραγμάτων (Internet of Things - IoT - [44]). Επιπλέον, ο προσανατολισμός προς υπηρεσιοκεντρικό σχεδιασμό των εφαρμογών κατέστησε κυρίαρχη τη χαλαρή σύνδεση και αλληλεπίδραση μεταξύ των μερών ενός συστήματος [45].

Η νέα αυτή εποχή ζητά τη συνεργασία μεταξύ οργανισμών, με την *εμπιστοσύνη* μεταξύ των εταίρων να βρίσκεται στο κέντρο της προσοχής. Βασικές απαιτήσεις για τις μεταξύ τους συναλλαγές αποτελούν η προστασία τόσο της πληροφορίας όσο και της ιδιωτικότητας. Από τη μια, οι οργανισμοί καλούνται να εμπιστευθούν πληροφορίες και δεδομένα που δεν προέρχονται από τους ίδιους και συνεπώς να εμπιστευθούν και τους οργανισμούς που τα παράγουν. Από την άλλη, τα ουκ ολίγα περιστατικά παραβίασης της ασφάλειας και της ιδιωτικότητας των χρηστών έχουν οδηγήσει τις εταιρίες στην αντίθετη κατεύθυνση. Παράλληλα, αυτή η διστακτικότητα για συνεργασία μεταξύ διαφορετικών οργανισμών οδηγεί σε ύφεση της παγκόσμιας ψηφιακής οικονομίας.

Σε αυτό το πλαίσιο, ο αποδοτικός έλεγχος πρόσβασης στη διακινούμενη πληροφορία είναι κρίσιμος παράγοντας για την προστασία της και ως εκ τούτου, η εξέλιξη των πολιτικών ασφαλείας έφερε τον έλεγχο πρόσβασης στο προσκήνιο συστημάτων που προστατεύουν τόσο την ασφάλεια όσο την ιδιωτικότητα των χρηστών τους. Πέρα από τα υπάρχοντα μοντέλα ελέγχου πρόσβασης [46], έχουν υπάρξει ποικίλες προσεγγίσεις στο θέμα αυτό οι οποίες εισάγουν αρκετά νέα χαρακτηριστικά. Αρκετές διακεκριμένες λύσεις προτείνουν βελτιώσεις του μοντέλου ελέγχου πρόσβασης βάσει ρόλων (Role-Based Access Control - RBAC - [47]) ώστε να συμπεριλάβουν περισσότερα κριτήρια στη λήψη αποφάσεων ελέγχου πρόσβασης πέρα από το *ποιός χρήστης* έχοντας *κάποιον ρόλο* θέλει να εκτελέσει *μια ενέργεια σε κάποιο αντικείμενο*. Εν προκειμένω, νέα μοντέλα ελέγχου πρόσβασης έχουν υιοθετήσει έννοιες όπως οργανισμοί [48] και πλαίσιο χρήσης [49], ενώ εμφανίστηκαν συστήματα ελέγχου πρόσβασης που προστατεύουν την ιδιωτικότητα των χρηστών [50] εστιάζοντας στην προστασία των προσωπικών τους δεδομένων.

Ωστόσο, θεωρώντας ένα κατανεμημένο περιβάλλον που αποτελείται από μεγάλο αριθμό ετερογενών συμμετεχόντων οι οποίοι σχετίζονται χαλαρά και αλληλεπιδρούν με δυναμικό τρόπο, ενώ βρίσκονται υπό την εποπτεία διαφορετικών οντοτήτων, δύο ζητήματα κάνουν την εμφάνιση τους αυτόματα: διαλειτουργικότητα των πολιτικών ασφαλείας και της επιβολής τους. Σε ότι αφορά τη διαλειτουργικότητα, οι προσπάθειες προτυποποίησης (βλ. [51][52]) δεν έχουν παράξει αποδοτικές λύσεις, όπως αναλύεται και στην παράγραφο 4.2, ενώ προσεγγίσεις που χρησιμοποιούν τις τεχνολογίες του Σημασιολογικού Διαδικτύου για τον έλεγχο πρόσβασης (βλ. [53] για μια επισκόπηση) υπόσχονται διαλειτουργι-

κότητα μόνο στο σημασιολογικό επίπεδο. Σε ότι αφορά το ζήτημα της επιβολής των πολιτικών ασφαλείας, οι προσεγγίσεις περιορίζονται στο παράδειγμα PDP–PEP (Policy Decision Point–Policy Enforcement Point, Σημείο Εξέτασης Πολιτικών–Σημείο Επιβολής Πολιτικών - [54]), το οποίο δεν ταιριάζει στο αναλυθέν περιβάλλον. Όταν τα δεδομένα εκτεθούν "σε κοινή θέα", το παράδειγμα PDP–PEP δεν μπορεί να διασφαλίσει την επιβολή των σχετικών πολιτικών, ενώ λύσεις όπως οι "κολλώδεις πολιτικές" (sticky policies - [55]) δεν είναι αποδοτικές, αφού η τήρηση τους στηρίζεται στην καλή θέληση του χρήστη που λαμβάνει τα δεδομένα.

Υπό το φως αυτών των ζητημάτων, σχεδιάστηκε και υλοποιήθηκε αρχιτεκτονική που στοχεύει στη προστασία της πληροφορίας σε κατανεμημένα ετερογενή περιβάλλοντα και απαντάει στα παραπάνω ζητήματα με έναν ολοκληρωμένο τρόπο. Η προστασία της διακινούμενης πληροφορίας πραγματοποιείται με χρήση κρυπτογραφίας. Η πληροφορία κρυπτογραφείται με τη σύγχρονη μέθοδο κρυπτογραφίας βάσει χαρακτηριστικών (πιο συγκεκριμένα με μέθοδο που βασίζεται σε πολιτικές κρυπτογραφήματος - Ciphertext-Policy Attribute-Based Encryption - CP-ABE - [56]) και μεταφράζει τις πολιτικές ελέγχου πρόσβασης σε δέντρα πρόσβασης που αποτελούνται από λογικές σχέσεις μεταξύ των χαρακτηριστικών που πρέπει να έχουν στην κατοχή τους οι χρήστες ώστε να μπορούν να αποκρυπτογραφήσουν τα δεδομένα. Στην πραγματικότητα, αυτά τα χαρακτηριστικά εκχωρούνται ασύγχρονα και από διαφορετικές αρχές που δραστηριοποιούνται σε ποικίλους και συχνά ασύνδετους τομείς ασφαλείας. Το γεγονός αυτό επεκτείνει περαιτέρω την έννοια της ετερογένειας που υφίσταται στο τυπικό σενάριο διακίνησης πληροφορίας και αφορά στην ετερογένεια των παραγωγών πληροφορίας, εισάγοντας τον ρόλο των διαφορετικών *Αρχών Χαρακτηριστικών*.

Η προτεινόμενη αρχιτεκτονική απαντάει στις δύο αυτές μορφές ετερογένειας χρησιμοποιώντας τεχνολογίες που προδιαγράφονται στα πρότυπα MPEG-21 [7] και MPEG-M [13]. Αρχικά υιοθετούνται τα ψηφιακά αντικείμενα ως η δομή που ενθυλακώνει την πληροφορία που ανταλλάσσεται μεταξύ των χρηστών του συστήματος. Σε κάθε ψηφιακό αντικείμενο ενσωματώνονται οι άδειες χρήσης του περιεχομένου εκπεφρασμένες στη γλώσσα MPEG-21 REL [9], η οποία πέρα από την προαναφερθείσα λειτουργία της χρησιμοποιείται και ως ένας ασφαλής και ενοποιημένος φορέας για τον ορισμό και την εκχώρηση χαρα-

κτηριστικών στους χρήστες. Τέλος, το σύστημα υιοθετεί την πλατφόρμα και την αρχιτεκτονική λογισμικού του προτύπου MPEG-M, στο οποίο έχουν πραγματοποιηθεί συνεισφορές με τη μορφή σχολίων και προτάσεων σε σειρά συνεδριάσεων του διεθνούς οργανισμού MPEG [57] [58] [59] [60] [61] [62], και την ενσωματώνει με υποδομή ABE (Attribute-based Encryption - Κρυπτογραφία βάσει χαρακτηριστικών) η οποία υποστηρίζει τις κρυπτογραφικές λειτουργίες του συστήματος για την προστασία του περιεχομένου.

Η παράγραφος 4.2 παρουσιάζει τις τρέχουσες προσεγγίσεις στην ευρύτερη ερευνητική περιοχή αναδεικνύοντας τους περιορισμούς και τις αδυναμίες τους. Ακολουθεί περιγραφή της κρυπτογραφίας βάσει χαρακτηριστικών και των υποδομών στις οποίες στηρίζεται και τέλος στην παράγραφο 4.4 παρουσιάζεται αναλυτικά το προτεινόμενο σύστημα και οι λειτουργίες του.

4.2 Τρέχουσες τάσεις στον έλεγχο πρόσβασης ψηφιακού περιεχομένου

Το προτεινόμενο σύστημα στοχεύει στην ασφαλή διαμοίραση παντός είδους πληροφορίας σε μεγάλης κλίμακας ετερογενή περιβάλλοντα. Σε αυτό το πλαίσιο, αντλεί έμπνευση από επιστημονικές εργασίες στον τομέα του ελέγχου πρόσβασης [47][63][46][53][64][50], ωστόσο η οικογένεια των μοντέλων ελέγχου πρόσβασης βάσει χαρακτηριστικών (Attribute-based Access Control - ABAC - [49][65][66][67]) είναι πιο κοντά στο παρόν σύστημα. Σε ανοικτά, κατανεμημένα περιβάλλοντα, όπου ο παραγωγός περιεχομένου και οι καταναλωτές του βρίσκονται εν γένει σε διαφορετικούς τομείς ασφαλείας, οι οποίοι διοικούνται από διαφορετικές αρχές και τεχνολογίες ελέγχου πρόσβασης που δεν είναι γνωστές στους υπόλοιπους τομείς, μια λύση που ταιριάζει στο ABAC μοντέλο ελέγχου πρόσβασης θα ήταν η χρησιμοποίηση ψηφιακών διαπιστευτηρίων, όπως τα ψηφιακά πιστοποιητικά X.509 [68], για τη βεβαίωση των χαρακτηριστικών των χρηστών που ζητούν πρόσβαση στα δεδομένα. Το παρόν σύστημα δεν είναι άμεσα συγκρίσιμο αλλά αντιθέτως συμπληρωματικό σε αυτά. Αντί να ορίζει μια γλώσσα για τον έλεγχο πρόσβασης, παρέχει τα εργαλεία για την ασφαλή διαμοίραση του περιεχομένου και την απομακρυσμένη επιβολή ελέγχου πρόσβασης σε αυτό,

οπότε μπορεί να χρησιμοποιηθεί σε συνδυασμό με αυτά.

Η XACML (eXtensible Access Control Markup Language - Επεκτάσιμή γλώσσα σήμανσης ελέγχου πρόσβασης - [51]) αποτελεί μια ευρέως διαδεδομένη πρωτοβουλία προτυποποίησης στην περιοχή του ελέγχου πρόσβασης. Το πρότυπο προδιαγράφει ένα γενικού σκοπού πλαίσιο ελέγχου πρόσβασης, το οποίο περιλαμβάνει ένα μοντέλο αρχιτεκτονικής που βασίζεται στο παράδειγμα PDP–PEP (Policy Decision Point–Policy Enforcement Point, Σημείο Εξέτασης Πολιτικών–Σημείο Επιβολής Πολιτικών - [54]) για την επιβολή των πολιτικών ελέγχου πρόσβασης. Η XACML αποτελεί κατάλληλο εργαλείο για την περιγραφή πολιτικών, αλλά δεν εξετάζει τον τρόπο όπου πραγματοποιείται η εκχώρηση και διαχείριση των χαρακτηριστικών των χρηστών. Ώς εκ τούτου, θεωρείται συμπληρωματική με το προτεινόμενο σύστημα. Το παραπάνω πρόβλημα καλύπτεται μερικώς με την χρησιμοποίηση της τεχνολογίας SAML (Security Assertion Markup Language - Γλώσσα σήμανσης βεβαιώσεων ασφαλείας -[52]), η οποία σχεδιάστηκε για την ανταλλαγή πληροφοριών ασφαλείας μεταξύ έμπιστων οντοτήτων, σε μορφή βεβαιώσεων (assertions) σε γλώσσα XML. Ωστόσο, σε ετερογενή περιβάλλοντα, όπου οι ad hoc σχέσεις μεταξύ των χρηστών είναι ο κανόνας, αυτό είναι δύσκολο, αφού ένα σύστημα SAML θα καλείται να επεξεργάζεται και να ενσωματώνει πολλαπλούς τύπους διαπιστευτηρίων σε SAML βεβαιώσεις. Αντιθέτως, η προτεινόμενη προσέγγιση χρησιμοποιεί μια τεχνολογία για όλες τις διαδικασίες ελέγχου πρόσβασης, τη διαχείριση των χαρακτηριστικών των χρηστών και την περιγραφή πολιτικών πρόσβασης για το διακινούμενο περιεχόμενο.

Το προτεινόμενο σύστημα μοιράζεται σε κάποιο βαθμό τους ίδιους στόχους με συστήματα που υιοθετούν την έννοια των Εικονικών Οργανισμών (Virtual Organisation - VO - [69] [70] [71] [72]). Ένας VO αποτελεί τον συνασπισμό ετερογενών οργανισμών που αν και χρησιμοποιούν διαφορετικές πολιτικές μπορούν να συνεργάζονται μέσω ενοποιημένων εικονικών πολιτικών. Ωστόσο, τέτοιου είδους προσεγγίσεις εκτός του ότι δεν ταιριάζουν σε δυναμικές ad hoc συνεργασίες, χαρακτηρίζονται από μεγάλο κόστος στη διαχείριση τους. Αντίθετα, το προτεινόμενο σύστημα υιοθετεί χαλαρότερες σχέσεις μεταξύ των συνεργαζόμενων οντοτήτων.

Τέλος, το προτεινόμενο σύστημα χτίζει πάνω σε λύσεις όπου χρησιμοποιούν κρυπτογραφία για την επιβολή των πολιτικών πρόσβασης του περιεχόμενου στο επίπεδο των

δεδομένων αυτών καθεαυτών. Λύσεις που βασίζονται στη συμμετρική και ασύμμετρη κρυπτογραφία [73] [74] [75] [76] [77] [78] επιφέρουν μεγάλη πολυπλοκότητα στη διαχείριση των κλειδιών αποκρυπτογράφησης όταν πραγματοποιούν εκλεπτυσμένο έλεγχο πρόσβασης. Τα πρώτα έχουν μεγάλο κόστος στη διαμοίραση των κλειδιών, ενώ τα τελευταία απαιτούν την *a priori* γνώση των δημόσιων κλειδιών των αποδεκτών καταναλωτών της πληροφορίας. Για τον λόγο αυτό, το προτεινόμενο σύστημα χρησιμοποιεί τη μέθοδο κρυπτογράφησης βάσει χαρακτηριστικών (Attribute-Based Encryption - ABE - [79]) και πιο συγκεκριμένα την τεχνική που κρυπτογραφεί με βάση πολιτικές κρυπτογραφήματος (Ciphertext-Policy Attribute-Based Encryption - CP-ABE - [56]). Η κρυπτογράφηση με ABE έχει υποστηριχθεί σε πολλά πρόσφατα συστήματα με πολυποίκιλα πεδία εφαρμογής στα οποία απαιτείται έλεγχος πρόσβασης στην διακινούμενη πληροφορία [80] [81] [82] [83] [84], ωστόσο καμία υπάρχουσα προσέγγιση δεν ενσωματώνει τη διαχείριση των χαρακτηριστικών των χρηστών σε συνδυασμό με ένα σύστημα ABE, προσφέροντας ένα ολοκληρωμένο σύστημα ελέγχου πρόσβασης δίχως σύνδεση σε δυναμικά ετερογενή περιβάλλοντα. Αυτό είναι ένα σημαντικό πλεονέκτημα του προτεινόμενου συστήματος το οποίο αναλύεται στις επόμενες παραγράφους.

4.3 Κρυπτογραφία βάσει χαρακτηριστικών

Η Κρυπτογραφία Βάσει Χαρακτηριστικών (Attribute-Based Encryption - ABE [79]) αποτελεί μια καινοτόμο μέθοδο κρυπτογράφησης η οποία βασίζεται στην Κρυπτογραφία Βάσει Ταυτότητας (Identity-Based Encryption - IBE - [85]) και την επεκτείνει εκλαμβάνοντας την ταυτότητα ενός χρήστη ως ένα εκ των ιδιοτήτων του που τον χαρακτηρίζουν. Πιο συγκεκριμένα, η κρυπτογράφηση με IBE αποφεύγει τη χρησιμοποίηση πιστοποιητικών για την επικοινωνία του δημόσιου κλειδιού του αποδέκτη ενός μηνύματος, με τη θέση του δημοσίου κλειδιού να λαμβάνει το μοναδικό αναγνωριστικό - ταυτότητα του, όπως παραδείγματος χάρη η διεύθυνση ηλεκτρονικού ταχυδρομείου του. Η κρυπτογράφηση με ABE από την πλευρά της, εκμεταλλεύεται τα αναγνώσιμα δημόσια κλειδιά που προτείνει η IBE και περιγράφει τον αποδέκτη μέσω των χαρακτηριστικών του, επιτρέποντας παράλληλα τον ορισμό πολύπλοκων συνδυασμών μεταξύ των χαρακτηριστικών, τα λεγόμενα δέντρα

πρόσβασης ABE, χρησιμοποιώντας λογικές σχέσεις σύζευξης ή διάζευξης.

Η κρυπτογραφία ABE ωστόσο, εμφανίζεται με δύο μορφές : την KP-ABE (Key-Policy ABE - [86]) και την CP-ABE (Ciphertext-Policy ABE - [87][88]). Η διαφορά τους έγκειται στην τοποθέτηση των χαρακτηριστικών (αντίστοιχα του δέντρου πρόσβασης) στο κρυπτογραφημένο μήνυμα είτε στο κλειδί αποκρυπτογράφησης. Στην KP-ABE ακολουθείται η πρώτη προσέγγιση, δηλαδή τα χαρακτηριστικά ενσωματώνονται στο μήνυμα, ενώ οι αποδέκτες απαιτείται να ενημερώσουν τα κλειδιά αποκρυπτογράφησης τους με το νέο δέντρο πρόσβασης. Η CP-ABE ακολουθεί τη δεύτερη προσέγγιση και ενσωματώνει το δέντρο πρόσβασης στο κρυπτογραφημένο μήνυμα, ενώ τα κλειδιά αποκρυπτογράφησης των χρηστών, τα οποία περιέχουν τα χαρακτηριστικά τους, δεν χρειάζεται να ενημερωθούν εκ νέου.

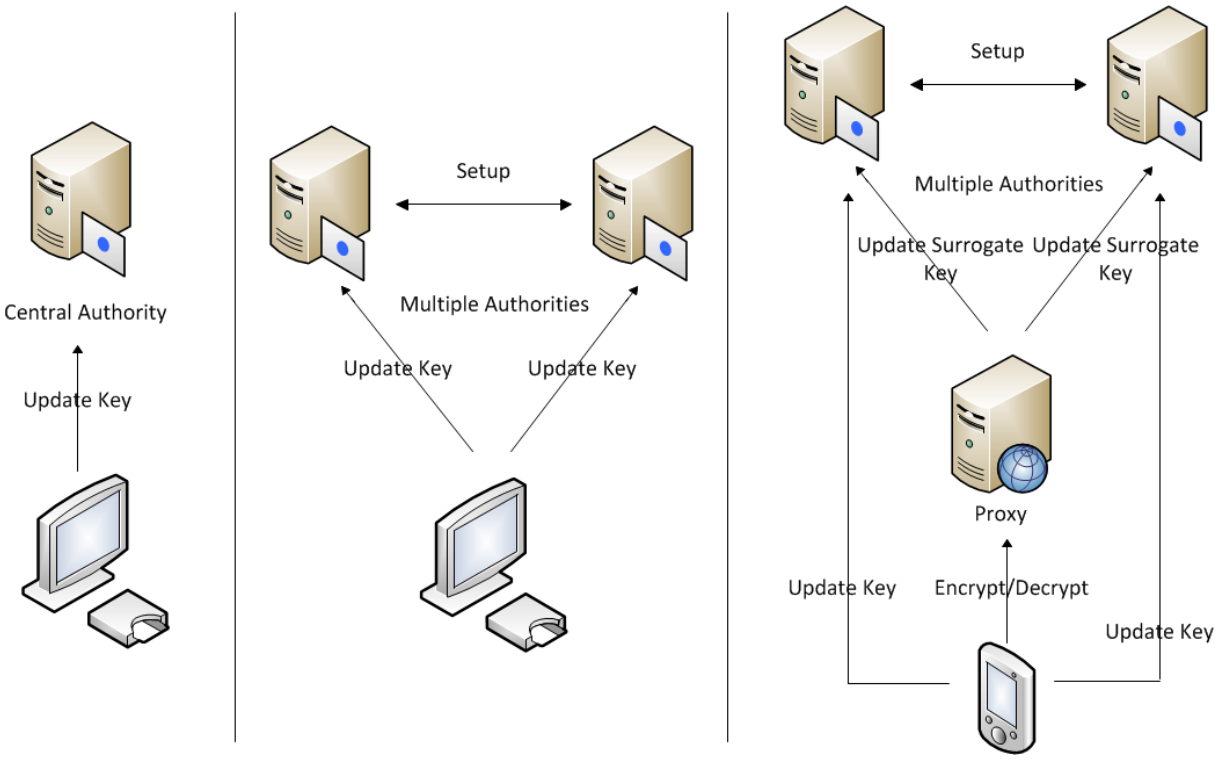
Τα τελευταίο, καθιστά την CP-ABE ένα ιδανικό ταίριασμα με μοντέλα ελέγχου πρόσβασης που βασίζονται σε χαρακτηριστικά (Attribute-based Access Control - ABAC). Από τη μια κάθε χαρακτηριστικό μπορεί να χρησιμοποιηθεί ως προαπαιτούμενο για την πρόσβαση στα κρυπτογραφημένα μηνύματα και μονάχα οι κάτοχοι του να μπορούν να το αποκρυπτογραφούν. Από την άλλη, τα δέντρα πρόσβασης ABE προσφέρουν μεγάλη ευελιξία στον ορισμό των κανόνων πρόσβασης και επιτρέπουν τον σχηματισμό πολύπλοκων κανόνων πρόσβασης. Παράλληλα, η κρυπτογράφηση των μηνυμάτων γίνεται μια φορά και αναφέρεται σε πολλαπλούς αποδέκτες, οι οποίοι δεν είναι απαραίτητο να είναι γνωστοί a priori.

Τα παραπάνω ελκυστικά χαρακτηριστικά της CP-ABE είναι άλλωστε που έχουν οδηγήσει στη χρήση της σε πολλές πρακτικές εφαρμογές. Με χαρακτηριστικά παραδείγματα τη χρήση της σε ασύρματα δίκτυα σενσόρων [83][82], προστασίας δημοσιεύσεων σε κοινωνικά δίκτυα [80], στη διαχείριση ιατρικών δεδομένων [89] και στην προστασία ψηφιακού περιεχομένου σε συστήματα συνδρομητικής τηλεόρασης [90].

Στη συνέχεια όπου αναφέρεται η Κρυπτογραφία Βάσει Χαρακτηριστικών, θα αναφερόμαστε στην CP-ABE.

4.3.1 Αρχιτεκτονική συστήματος κρυπτογραφίας βάσει χαρακτηριστικών

Τα συστήματα ABE της βιβλιογραφίας χωρίζονται στις εξής τρεις κατηγορίες ανάλογα με τις υποδομές που απαιτούν και τις λειτουργίες που προσφέρουν :



Σχήμα 11: Αρχιτεκτονική συστήματος κρυπτογραφίας βάσει χαρακτηριστικών

- **Κεντρική αρχή** :

  Συστήματα που ακολουθούν αυτό το μοντέλο [56][87], θεωρούν μια πλήρως έμπιστη κεντρική αρχή η οποία είναι επιφορτισμένη με το έργο της έκδοσης και διαχείρισης των κλειδιών των χρηστών. Από τη μια, έχοντας συγκεντρωμένη ανά πάσα στιγμή σε ένα σημείο τη γνώση των χαρακτηριστικών των χρηστών, διευκολύνεται η διασφάλιση της κατασκευής κλειδιών τα οποία δεν μπορούν να συνδυαστούν μεταξύ τους, αλλά και η διαχείριση ανακλήσεων χαρακτηριστικών των χρηστών. Ωστόσο, από την άλλη πλευρά, η ύπαρξη μιας μοναδικής κεντρικής αρχής εγείρει ζητήματα ασφαλείας και ιδιωτικότητας των δεδομένων των χρηστών, καθώς σε περίπτωση ρήγματος ασφαλείας, είναι δυνατό να αποκτηθεί πρόσβαση στα κλειδιά και επομένως και τα δεδομένα των χρηστών.

- **Πολλαπλές αρχές** :

  Συστήματα που θεωρούν πολλαπλές αρχές έκδοσης κλειδιών αποκρυπτογράφησης ABE [91][92][93], στηρίζονται στη κατανεμημένη δημιουργία των κλειδιών των χρηστών, ώστε να αποφύγουν τα ζητήματα ασφάλειας που ανακύπτουν σε συστήματα με μια μοναδική πλήρως έμπιστη κεντρική αρχή. Ωστόσο, από τη στιγμή που κάθε αρχή λειτουργεί αυτόνομα ύστερα από την αρχικοποίηση του συστήματος, η διασφάλιση της μη σύμπραξης των κλειδιών των χρηστών είναι αρκετά πολύπλοκη υπόθεση. Το ζήτημα αυτό λύνεται μέσω της χρήσης μοναδικού αναγνωριστικού για κάθε χρήστη, το οποίο χρησιμοποιείται με τέτοιον τρόπο ώστε κάθε χαρακτηριστικό που λαμβάνει κάποιος χρήστης να δένεται με το μοναδικό του αναγνωριστικό. Παράλληλα, ένα επιπλέον πλεονέκτημα των συστημάτων που στηρίζονται σε πολλαπλές αρχές είναι η διατήρηση της ασφάλειας του συστήματος ακόμα και μετά από την έκθεση των μυστικών κλειδιών ενός πεπερασμένου πλήθους αρχών.

- **Κρυπτογράφηση ABE μέσω αντιπροσώπου** :

  Συστήματα που προσφέρουν κρυπτογραφικές υπηρεσίες μέσω αντιπροσώπων [94][95] στοχεύουν στην ασφαλή μετακύλιση του κόστους των κρυπτογραφικών εργασιών σε πληρεξούσιους εξυπηρετητές. Οι τελευταίοι θεωρούνται ημιέμπιστοι και πέρα από την εγγενή υποστήριξη συσκευών με περιορισμένη υπολογιστική ισχύ, διευκολύνουν την ανάκληση χαρακτηριστικών είτε αναλαμβάνοντας την επικαιροποίηση των κλειδιών και των διαθέσιμων λιστών ανάκλησης, είτε παρέχοντας υπηρεσίες επανακρυπτογράφησης.

Ένα βασικό σύστημα κρυπτογραφίας βάσει χαρακτηριστικών προσφέρει τις παρακάτω μεθόδους :

- **Αρχικοποίηση** (παράμετρος ασφάλειας, σύνολο χαρακτηριστικών) -> δημόσιες παράμετροι, μυστικό κλειδί αρχής.

  Η αρχικοποίηση της αρχής έκδοσης κλειδιών περιλαμβάνει τον ορισμό της παραμέτρου ασφάλειας, βάσει της οποίας κατασκευάζονται οι δημόσιες παράμετροι για κάθε χαρακτηριστικό και το μυστικό κλειδί της αρχής.

- **Έκδοση κλειδιού** (μυστικό κλειδί, χαρακτηριστικά) -> κλειδί αποκρυπτογράφησης.

  Η αρχή έκδοσης κλειδιών αποκρυπτογράφησης χρησιμοποιεί το μυστικό κλειδί της ώστε να εκδώσει ένα νέο κλειδί για κάποιον χρήστη, ανάλογα με τα χαρακτηριστικά του.

- **Κρυπτογράφηση** (δημόσιες παράμετροι, δέντρο πρόσβασης, μήνυμα) -> κρυπτογραφημένο μήνυμα.

  Για την κρυπτογράφηση ενός μηνύματος απαιτείται ο ορισμός του δέντρου πρόσβασης, που ορίζει τα χαρακτηριστικά που πρέπει να έχουν στην κατοχή τους οι αποδέκτες του, και χρησιμοποιεί τις δημόσιες παραμέτρους για κάθε χρησιμοποιούμενο χαρακτηριστικό, ώστε να κατασκευάσει το τελικό κρυπτογραφημένο μήνυμα.

- **Αποκρυπτογράφηση** (δημόσιες παράμετροι, κλειδί αποκρυπτογράφησης, κρυπτογραφημένο μήνυμα) -> αποκρυπτογραφημένο μήνυμα.

  Για την αποκρυπτογράφηση ενός μηνύματος απαιτείται το κλειδί αποκρυπτογράφησης του χρήστη και οι δημόσιες παράμετροι για κάθε χαρακτηριστικό. Η διαδικασία είναι επιτυχής μόνο όταν το κλειδί αποκρυπτογράφησης περιέχει τα χαρακτηριστικά τα οποία ορίζει το δέντρο πρόσβασης το οποίο χρησιμοποιήθηκε για την κρυπτογράφηση του μηνύματος.

Συστήματα ABE με πολλαπλές αρχές έκδοσης κλειδιών απαιτούν την αρχικοποίηση των καθολικών παραμέτρων του συστήματος και της χρήσης τους σε κάθε μια από τις παραπάνω μεθόδους. Ενώ, σε συστήματα που υποστηρίζουν ανάκληση χαρακτηριστικών [94][95], προστίθενται μέθοδοι για την επανέκδοση κλειδιών ή ακόμα και την επανακρυπτογράφηση μηνυμάτων.

4.3.2 Προκλήσεις και ανοικτά θέματα

Τα ελκυστικά στοιχεία που προσφέρει η κρυπτογραφία βάσει χαρακτηριστικών, έχουν στρέψει το ενδιαφέρον πολλών ερευνητών στην προσπάθεια εμπλουτισμού των δυνατοτήτων της με στόχο τη δημιουργία ασφαλών συστημάτων και της εφαρμογής της σε πολλά πρακτικά σενάρια.

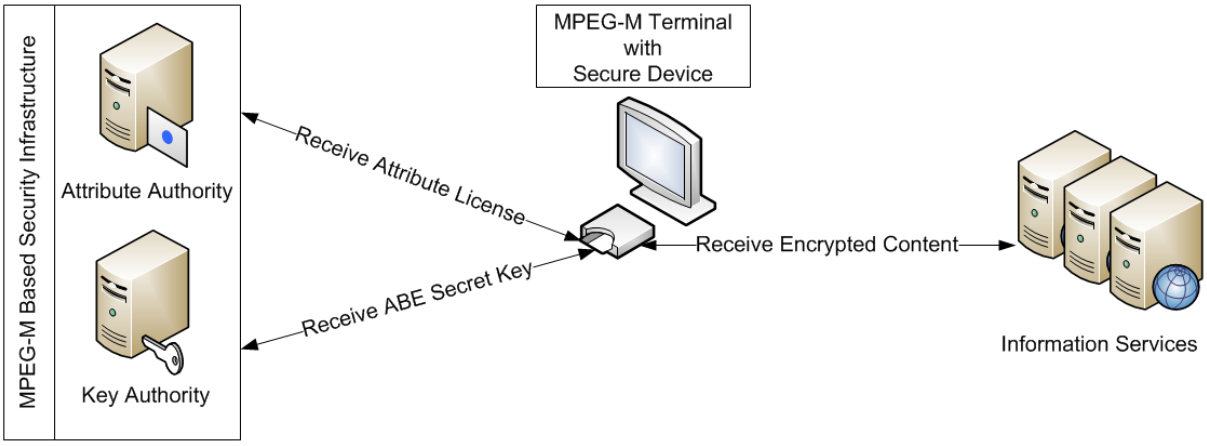
Πιο συγκεκριμένα, στο πλαίσιο της εκφραστικότητας των δέντρων πρόσβασης, η έρευνα στοχεύει στη διεύρυνση της προσθέτοντας τη σχέση λογικής άρνησης [96], διατηρώντας βεβαίως την ασφάλεια της κρυπτογράφησης. Το παραπάνω ωστόσο ενδέχεται να επιβαρύνει το κόστος κρυπτογράφησης και αποκρυπτογράφησης, η μείωση του οποίου αποτελεί και τον σημαντικότερο παράγοντα για την υιοθέτηση της μεθόδου από πραγματικές εφαρμογές [97].

Παράλληλα, εμφανίζονται συστήματα που ελαχιστοποιούν τις απαιτήσεις για πλήρως έμπιστες αρχές [98][95], αντικαθιστώντας τις με ημιέμπιστες, ενώ εισάγονται και ενδιάμεσοι πληρεξούσιοι κόμβοι με αποκλειστικό ρόλο να παρέχουν κρυπτογραφικές υπηρεσίες με ασφαλή τρόπο. Οι τελευταίοι ενισχύουν την υποστήριξη συσκευών με περιορισμένη υπολογιστική ισχύ και επιπροσθέτως διευκολύνουν τη διαδικασία ανάκλησης χαρακτηριστικών των χρηστών. Έτσι, σε περίπτωση που κάποιος χρήστης παύει να έχει στην κατοχή του ένα χαρακτηριστικό, αυτός ενώ είχε πρόσβαση σε μηνύματα που το απαιτούσαν, θα πρέπει πλέον να μην είναι δυνατό να έχει πρόσβαση σε αυτά, υπηρετώντας με αυτό τον τρόπο τη διασφάλιση τόσο της πρότερης όσο και μελλοντικής μυστικότητας των κρυπτογραφημένων μηνυμάτων. Το παραπάνω ωστόσο επιβάλει είτε την την επάνακρυπτογράφηση των δεδομένων και την επικαιροποίηση των κλειδιών αποκρυπτογράφησης των σχετικών χρηστών, είτε την ακύρωση του κλειδιού του συγκεκριμένου χρήστη, έτσι ώστε αυτό να μην είναι διαθέσιμο σε αυτόν με κανένα τρόπο.

4.4 Σύστημα ασφαλούς διαχείρισης ψηφιακών αντικειμένων

Η προτεινόμενη λύση σχεδιάστηκε στοχεύοντας στην υποστήριξη έλεγχου πρόσβασης χωρίς σύνδεση σε ετερογενή και κατανεμημένα περιβάλλοντα. Η ετερογένεια υποστηρίζεται με τη χρήση των δομών δεδομένων και υπηρεσιών που προδιαγράφονται στα διεθνή πρότυπα MPEG-21 [7] και MPEG-M [13], ενώ ο έλεγχος πρόσβασης χωρίς σύνδεση γίνεται εφικτός με τη χρησιμοποίηση της πρωτότυπης μεθόδου κρυπτογράφησης βάσει χαρακτηριστικών (Attribute-based Encryption - ABE - [56]) για την προστασία της πληροφορίας. Η προτεινόμενη αρχιτεκτονική αποσκοπεί στην ενσωμάτωση των παραπάνω σε ένα ολοκληρωμένο σύστημα, του οποίου οι κύριοι χρήστες μαζί με τις αλληλεπιδράσεις

μεταξύ τους αναπαριστώνται στο Σχήμα 12.



Σχήμα 12: Αρχιτεκτονική συστήματος offline ελέγχου πρόσβασης [5]

Λαμβάνοντας υπόψη τόσο την ετερογένεια των χρηστών όσο και των πληροφοριοκεντρικών υπηρεσιών που εκείνοι επιθυμούν να χρησιμοποιήσουν, προκύπτει η ανάγκη για μια κοινή δομή δεδομένων που θα ενθυλακώνει την πληροφορία και θα λειτουργεί ως γέφυρα διαλειτουργικότητας. Επιπρόσθετα, αυτή η δομή δεδομένων πρέπει να μπορεί να υποστηρίζει την προστασία της πληροφορίας υπολογίζοντας και την ετερογένεια των χρηστών που παίρνουν μέρος στο πλαίσιο των λειτουργιών του συστήματος.

Έχοντας τα παραπάνω κατά νου, προτείνεται η χρήση των ψηφιακών αντικειμένων ως η βασική δομή δεδομένων για την ενθυλάκωση της πληροφορίας. Τα ψηφιακά αντικείμενα πέρα από τη διαλειτουργικότητα που προσφέρουν στον διαμοιρασμό της πληροφορίας μεταξύ ανεξάρτητων συστημάτων, παρέχουν επίσης τη δυνατότητα για την συμπερίληψη τόσο περιγραφικών μεταδεδομένων για αυτή, αλλά και κανόνων που διέπουν τη χρήση της. Τα παραπάνω καθιστούν τα ψηφιακά αντικείμενα μια αυτόνομη και αυτοπεριγραφόμενη δομή ιδανική για τη χρήση της σε παντός είδους κατανεμημένα περιβάλλοντα.

Ακολουθώντας τις προδιαγραφές του προτύπου MPEG-21 για την προστασία ενός ψηφιακού αντικειμένου, περιγράφονται οι κανόνων χρήσης τους στη γλώσσα περιγραφής δικαιωμάτων χρήσης MPEG-21 REL. Οι κανόνες αυτοί ενδέχεται να αναφέρονται είτε σε συγκεκριμένη οντότητα είτε σε κλάση οντοτήτων που αναγνωρίζονται με βάση τα χαρακτηριστικά τους. Το σύνολο των κανόνων χρήσης ενός ψηφιακού αντικειμένου, που αποτελούν ουσιαστικά την πολιτική ασφαλείας του, κωδικοποιούνται σε μια ή περισσότερες

άδειες χρήσης εκπεφρασμένες στη γλώσσα REL. Η προστασία της πληροφορίας πραγματοποιείται με την κρυπτογράφηση της εφαρμόζοντας τις άδειες χρήσης πάνω στην πληροφορία με τέτοιον τρόπο ώστε μόνο οι εξουσιοδοτημένες οντότητες να μπορούν να την ανακτήσουν. Πιο συγκεκριμένα η πληροφορία κρυπτογραφείται με χρήση της μεθόδου κρυπτογράφησης CP-ABE με δέντρο πρόσβασης (access tree) που σχηματίζεται από τις άδειες χρήσης. Η παραπάνω διαδικασία περιγράφεται αναλυτικά στην παράγραφο 4.4.2.

Όπως διαφαίνεται από τα παραπάνω, η προστασία της πληροφορίας προϋποθέτει τη λήψη REL αδειών από τους χρήστες του συστήματος ώστε να μπορούν να ανακτήσουν την πληροφορία. Πιο συγκεκριμένα, προτού οι χρήστες λάβουν κλειδί αποκρυπτογράφησης που να αντιστοιχεί στις ιδιότητες τους, έχουν ήδη αποκτήσει REL άδειες που πιστοποιούν τα χαρακτηριστικά τους. Οι δύο αυτές διαδικασίες αν και βασικές για ένα σύστημα που στηρίζεται στην τεχνολογία ABE, δεν εξετάζονται ενδελεχώς από τα συστήματα ABE της βιβλιογραφίας, τα οποία και εστιάζουν στην παραγωγή ασφαλών κλειδιών αποκρυπτογράφησης για τους χρήστες. Για το λόγο αυτό, εισάγεται ο ρόλος της Αρχής Χαρακτηριστικών (ΑΧ) και της Αρχής Κλειδιών (ΑΚ). Ο πρώτος είναι υπεύθυνος για την έκδοση REL αδειών που να πιστοποιούν τα χαρακτηριστικά των χρηστών, ενώ ο δεύτερος αναλαμβάνει την έκδοση ABE κλειδιών αποκρυπτογράφησης που να αντιστοιχούν στις REL άδειες των χρηστών. Αναλυτικότερα, κάθε REL άδεια δημιουργείται χρησιμοποιώντας την στοιχειώδη υπηρεσία `CreateLicense` και είναι ψηφιακά υπογεγραμμένη από την εκδούσα αρχή. Οι κάτοχοι των REL αδειών μπορούν να τις χρησιμοποιήσουν ως πιστοποίηση των χαρακτηριστικών τους σε διαφορετικές ΑΚ, οι οποίες έχουν τη δυνατότητα να ελέγξουν την εγκυρότητα τους επικοινωνώντας με τις αντίστοιχες ΑΧ χρησιμοποιώντας την στοιχειώδη υπηρεσία `VerifyLicense`.

Οι REL άδειες των χρηστών που περιέχουν τα χαρακτηριστικά τους, αποθηκεύονται στην ασφαλή συσκευή του χρήστη. Αυτή θα μπορούσε να είναι μια έξυπνη κάρτα, μια Μονάδα Έμπιστης Πλατφόρμας (Trusted Platform Module - TPM), μια κάρτα SIM κινητού τηλεφώνου κτλ. Η αποθήκευση των REL αδειών πραγματοποιείται με τη στοιχειώδη υπηρεσία `StoreLicense` η οποία υλοποιείται τοπικά στο τερματικό του χρήστη.

Για να λάβει ο χρήστης το ABE κλειδί που αντιστοιχεί στα χαρακτηριστικά που έχει αποθηκευμένα στην ασφαλή συσκευή του, προμηθεύει την Αρχή Κλειδιών με τις αντί-

στοιχες REL άδειες χρησιμοποιώντας τη στοιχειώδη υπηρεσία `AuthorizeUser` την οποία και προσφέρει η AK. Αφού η AK ελέγξει την εγκυρότητα των REL αδειών χρησιμοποιώντας τη στοιχειώδη υπηρεσία `VerifyLicense` για την επικοινωνία της με την αντίστοιχη Αρχή Χαρακτηριστικών, η AK παράγει το ABE κλειδί και το επιστρέφει στο χρήστη στο μήνυμα απάντησης. Τέλος, το ABE κλειδί αποκρυπτογράφησης του χρήστη αποθηκεύεται στην ασφαλή συσκευή του χρήστη.

Έχοντας ο χρήστης αποθηκευμένο στη συσκευή του το ABE κλειδί του, μπορεί να καταναλώσει δεδομένα προερχόμενα από παντός είδους πληροφοριοκεντρικές υπηρεσίες. Τα δεδομένα αυτά συνοδεύονται από τους REL κανόνες χρήσης, βάσει των οποίων έχουν κρυπτογραφηθεί ώστε μόνο οι εξουσιοδοτημένοι χρήστες να μπορούν να τα προσπελάσουν. Στη συνέχεια, θα χρησιμοποιηθεί το ABE κλειδί του χρήστη για την αποκρυπτογράφηση των δεδομένων και σε περίπτωση που η αποκρυπτογράφηση αποτύχει αυτό συνεπάγεται την μη ικανοποίηση του CP-ABE δέντρου πρόσβασης του κρυπτογραφήματος από το ABE κλειδί του χρήστη, δηλαδή την απουσία ενός ή περισσοτέρων αναγκαίων χαρακτηριστικών. Τα χαρακτηριστικά αυτά ο χρήστης μπορεί να τα αποκτήσει επικοινωνώντας με κατάλληλες Αρχές Χαρακτηριστικών όπως έχουν καθοριστεί στους REL κανόνες χρήσης των δεδομένων.

4.4.1 Δημιουργία έμπιστων κοινοτήτων

Η απόκτηση χαρακτηριστικών και κλειδιών αποκρυπτογράφησης από τους χρήστες είναι διαδικασίες που λαμβάνουν χώρα ασύγχρονα, με την έννοια πως εάν και αποτελούν απαραίτητα μέρη στον κύκλο ζωής της πληροφορίας, πραγματοποιούνται ανεξάρτητα από την παραγωγή και κατανάλωση της πληροφορίας. Τα χαρακτηριστικά αποκτώνται από διαφορετικές Αρχές Χαρακτηριστικών με τη μορφή REL αδειών, οι οποίες στη συνέχεια προωθούνται σε μια Αρχή Κλειδιών ώστε να αποκτήσουν το ενημερωμένο ABE κλειδί τους.

Η ύπαρξη περισσότερων από μια Αρχές Χαρακτηριστικών έρχεται φυσιολογικά, λόγω του ότι διαφορετικοί οργανισμοί χορηγούν διαφορετικά χαρακτηριστικά. Για παράδειγμα ένας χρήστης μπορεί να λάβει από το Υπουργείο Παιδείας το χαρακτηριστικό 'φοι-

τητής", και παράλληλα να έχει αποκτήσει από μια διαδικτυακή υπηρεσία ροής βίντεο, η οποία λειτουργεί εδώ ως Αρχή Χαρακτηριστικών, το χαρακτηριστικό πως είναι συνδρομητής της.

Τα χαρακτηριστικά αποτελούν τα τεκμήρια για τη πρόσβαση στα δεδομένα και τις υπηρεσίες. Ωστόσο, οι υπηρεσίες χαρακτηρίζονται, μαζί με τους παραγωγούς και τους παρόχους των, από μεγάλο διασκορπισμό και ετερογένεια, κάνοντας την διαχείριση των χαρακτηριστικών ιδιαίτερα περίπλοκη διαδικασία. Για την αντιμετώπιση της ετερογένειας, είναι αναγκαίος ένας ομοιόμορφος τρόπος τόσο για την αναπαράσταση των χαρακτηριστικών αυτών καθεαυτών όσο και για τον έλεγχο της εγκυρότητας τους. Η ομοιόμορφη αναπαράσταση των χαρακτηριστικών είναι σημαντική για τη διαλειτουργικότητα μεταξύ των διαφόρων υπηρεσιών. Οι εμπλεκόμενες οντότητες πρέπει να είναι ικανές να προσδιορίσουν με ακρίβεια εάν κάποιος χρήστης είναι κάτοχος κάποιου χαρακτηριστικού και προφανώς να μπορούν να αντιληφθούν τη μορφή στην οποία αυτό τους προωθείται. Από την άλλη, ο έλεγχος εγκυρότητας των χαρακτηριστικών των χρηστών είναι επίσης επιτακτική ανάγκη, ώστε να μπορούν οι διάφορες οντότητες να ελέγχουν εάν κάποιος είναι νόμιμος κάτοχος κάποιου χαρακτηριστικού.

Έχοντας κατά νου την αρχιτεκτονική, το σχήμα 13 παρουσιάζει ένα παράδειγμα REL άδειας που έχει εκδοθεί από το Υπουργείο Παιδείας (γραμμές 2–10) και πιστοποιεί πως ένας χρήστης (γραμμές 12–17) είναι 'φοιτητής" (γραμμή 22). Όποιος κατέχει αυτή την REL άδεια θα μπορεί να έχει πρόσβαση σε δεδομένα που είναι αποκλειστικά για 'φοιτητές", όπως περιγράφεται στην παράγραφο 4.4.3.

Οι χρήστες λαμβάνουν το ABE κλειδί τους προωθώντας τις REL άδειες τους στις Αρχές Κλειδιών. Αυτό το κλειδί συγκεντρώνει τα χαρακτηριστικά του χρήστη και είναι δυνατό να αποκρυπτογραφεί δεδομένα που έχουν κρυπτογραφηθεί με οποιοδήποτε υποσύνολο ή από αυτά.

4.4.2 Προστασία ψηφιακών αντικειμένων

Προστασία της πληροφορίας πραγματοποιείται με την κρυπτογράφηση των δεδομένων βάσει των καθορισμένων πολιτικών χρήσης που εκφράζονται με χρήση της MPEG-

```
01 <rel-r:License>
02   <rel-r:issuer>
03     <dsig:Signature>
04       <dsig:SignatureValue>...</dsig:SignatureValue>
05       <dsig:KeyInfo>
06         <dsig:KeyName>ΤΠΟΤΡΓΕΙΟ ΠΑΙΔΕΙΑΣ</dsig:KeyName>
07         <dsig:KeyValue>...</dsig:KeyValue>
08       </dsig:KeyInfo>
09     </dsig:Signature>
10   </rel-r:issuer>
11   <rel-r:inventory>
12     <rel-r:keyHolder licensePartId="user">
13       <dsig:KeyInfo>
14         <dsig:KeyName>ONOMA ΧΡΗΣΤΗ</dsig:KeyName>
15         <dsig:KeyValue>...</dsig:KeyValue>
16       </dsig:KeyInfo>
17     </rel-r:keyHolder>
18   </rel-r:inventory>
19   <rel-r:grant>
20     <rel-r:principal licensePartIdRef="user"/>
21     <rel-r:possessesProperty/>
22     <rel-sx:propertyUri definition="ΦΟΙΤΗΤΗΣ"/>
23   </rel-r:grant>
24 </rel-r:License>
```

Σχήμα 13: REL άδεια χρήσης (απόσπασμα)

21 REL και ρυθμίζουν ποιοι χρήστες μπορούν να προσπελάσουν τα δεδομένα ανάλογα με τα χαρακτηριστικά που κατέχουν.

Για παράδειγμα, έστω μια διαδικτυακή υπηρεσία ροής βίντεο η οποία χωρίζει τους χρήστες της σε "χρυσούς" και "ασημένιους" συνδρομητές, ανάλογα με τη συνδρομή που έχουν προμηθευτεί. Έστω επίσης και μια προωθητική ενέργεια η οποία προσφέρει στους "φοιτητές" που έχουν "ασημένια" συνδρομή την δυνατότητα να έχουν πρόσβαση σε βίντεο υψηλής ανάλυσης, κάτι που έχουν και οι χρυσοί συνδρομητές. Η πολιτική χρήσης όπως διαμορφώνεται από τα παραπάνω είναι η εξής :

ΧΡΥΣΟΣ-ΣΥΝΔΡΟΜΗΤΗΣ OR

(ΦΟΙΤΗΤΗΣ AND ΑΣΗΜΕΝΙΟΣ-ΣΥΝΔΡΟΜΗΤΗΣ)

Η παραπάνω πολιτική θα μεταφραστεί σε δύο χορηγήσεις άδειας (license grants) και θα ενσωματωθούν σε ένα ψηφιακό αντικείμενο με τη μορφή μιας άδειας χρήσης, η οποία στη συνέχεια θα οδηγήσει την κρυπτογράφηση των δεδομένων. Η άδεια χρήσης του παραδείγματος παρατίθεται στο σχήμα 14, με τις χορηγήσεις άδειας να βρίσκονται στις γραμμές 35–50 με το δικαίωμα χρήσης που εξουσιοδοτούν να είναι αυτό της *αναπαραγωγής*, όπως αυτό δηλώνεται από το στοιχείο `<rel-r:play>` (γραμμές 38, 46). Το μοναδικό

αναγνωριστικό της άδειας χρήσης βρίσκεται στη γραμμή 1 (*play-vid-202621*), ενώ η άδεια αναφέρεται στο ψηφιακό αντικείμενο με αναγνωριστικό (*hd-vid-124353* - γραμμές 40, 48) το οποίο παρουσιάζεται παρακάτω.

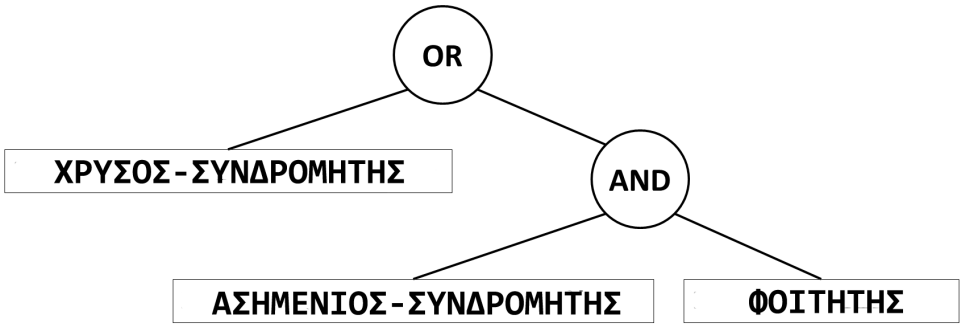
```
01 <rel-r:License licenseId="hd-vid-lic-202621">
02   <rel-r:issuer>
03     <dsig:Signature>
04       <dsig:SignatureValue>...</dsig:SignatureValue>
05       <dsig:KeyInfo>
06         <dsig:KeyName>ΤΠΗΡΕΣΙΑ ΡΟΗΣΒΙΝΤΕΟ </dsig:KeyName>
07         <dsig:KeyValue>...</dsig:KeyValue>
08       </dsig:KeyInfo>
09     </dsig:Signature>
10   </rel-r:issuer>
11   <rel-r:inventory>
12     <rel-r:forAll licensePartId="gold-policy">
13       <rel-r:propertyPossessor>
14         <rel-sx:propertyUri definition="ΧΡΤΣΟΣΣΤΝΔΡΟΜΗΤΗΣ-"/>
15         <rel-r:trustRoot>
16           <rel-r:keyHolder>ΤΠΗΡΕΣΙΑ ΡΟΗΣΒΙΝΤΕΟ </rel-r:keyHolder>
17         </rel-r:trustRoot>
18       </rel-r:propertyPossessor>
19     </rel-r:forAll>
20      <rel-r:forAll licensePartId="promo-policy">
21       <rel-r:propertyPossessor>
22         <rel-sx:propertyUri definition="ΑΣΗΜΕΝΙΟΣΣΤΝΔΡΟΜΗΤΗΣ-"/>
23         <rel-r:trustRoot>
24           <rel-r:keyHolder>ΤΠΗΡΕΣΙΑ ΡΟΗΣΒΙΝΤΕΟ </rel-r:keyHolder>
25         </rel-r:trustRoot>
26       </rel-r:propertyPossessor>
27        <rel-r:propertyPossessor>
28         <rel-sx:propertyUri definition="ΦΟΙΤΗΤΗΣ"/>
29         <rel-r:trustRoot>
30           <rel-r:keyHolder>ΤΠΟΤΡΓΕΙΟ ΠΑΙΔΕΙΑΣ</rel-r:keyHolder>
31         </rel-r:trustRoot>
32       </rel-r:propertyPossessor>
33     </rel-r:forAll>
34   </rel-r:inventory>
35   <rel-r:grant>
36     <rel-r:forAll licensePartIdRef="gold-policy" varName="x"/>
37     <rel-r:principal varRef="x"/>
38     <rel-r:play/>
39     <rel-mx:diReference>
40       hd-vid-124353
41     </rel-mx:diReference>
42   </rel-r:grant>
43   <rel-r:grant>
44     <rel-r:forAll licensePartIdRef="promo-policy" varName="y"/>
45     <rel-r:principal varRef="y"/>
46     <rel-r:play/>
47     <rel-mx:diReference>
48       hd-vid-124353
49     </rel-mx:diReference>
50   </rel-r:grant>
51 </rel-r:License>
```

Σχήμα 14: REL άδεια χρήσης που ρυθμίζει την πρόσβαση στην υπηρεσία βίντεο υψηλής ποιότητας (απόσπασμα)

Σε αυτό το σημείο πρέπει να σημειωθεί πως οι κανόνες χρήσης του ψηφιακού αντικειμένου, πρέπει να εκφραστούν σε Διαζευκτική Κανονική Μορφή (Disjunctive Normal Form

- DNF) ώστε να μπορούν να μεταφραστούν σε χορηγήσεις δικαιωμάτων χρήσης REL. Αυτό συμβαίνει λόγω του σχήματος της MPEG-21 REL που δεν επιτρέπει τον ορισμό πολύπλοκων λογικών εκφράσεων στους κανόνες χρήσης. Ωστόσο, δεν προκύπτει κάποιος περιορισμός ως προς την εκφραστικότητα που μπορούμε να χρησιμοποιήσουμε αφού κάθε λογική έκφραση μπορεί να γραφεί σε μορφή DNF. Στο παραπάνω παράδειγμα δεν ήταν αναγκαίος ο μετασχηματισμός της λογικής έκφρασης, αλλά σε πολλές περιπτώσεις πραγματοποιείται ένα ενδιάμεσο βήμα για την παραγωγή της DNF μορφής του κανόνα χρήσης.

Οι παραχθείσα άδεια χρήσης του ψηφιακού αντικειμένου χρησιμοποιείται στη συνέχεια για την παραγωγή ενός CP-ABE δέντρου πρόσβασης βάσει του οποίου θα κρυπτογραφηθούν τα δεδομένα. Το σχήμα 15 απεικονίζει το δέντρο πρόσβασης που αντιστοιχεί στην άδεια χρήσης του σχήματος 14.



Σχήμα 15: Κρυπτογραφική πολιτική σε μορφή δέντρου πρόσβασης

Την κρυπτογράφηση των δεδομένων που ορίζει το ψηφιακό αντικείμενο αναλαμβάνει το εργαλείο ABE που επιλέγει ο παραγωγός. Το τελευταίο καταγράφεται στο ψηφιακό αντικείμενο σύμφωνα με τις προδιαγραφές του διεθνούς προτύπου για τη Διαχείριση και Προστασία της Πνευματικής Ιδιοκτησίας (Intellectual Property Management and Protection - IPMP - [31]), ώστε να μπορούν οι πιθανοί παραλήπτες των δεδομένων να αποκρυπτογραφήσουν τα δεδομένα. Αυτό φαίνεται στο σχήμα 16, όπου στις γραμμές 16–18 ορίζεται το εργαλείο IPMP (`gr.ntua.icbnet.security.ABETool`) που χρησιμοποιήθηκε για την κρυπτογράφηση των δεδομένων. Σημειώνεται πως στις γραμμές 20–24 έχει ενσωματωθεί και παραπομπή για την άδεια χρήσης (σχήμα 14) που διέπει τα δεδομένα.

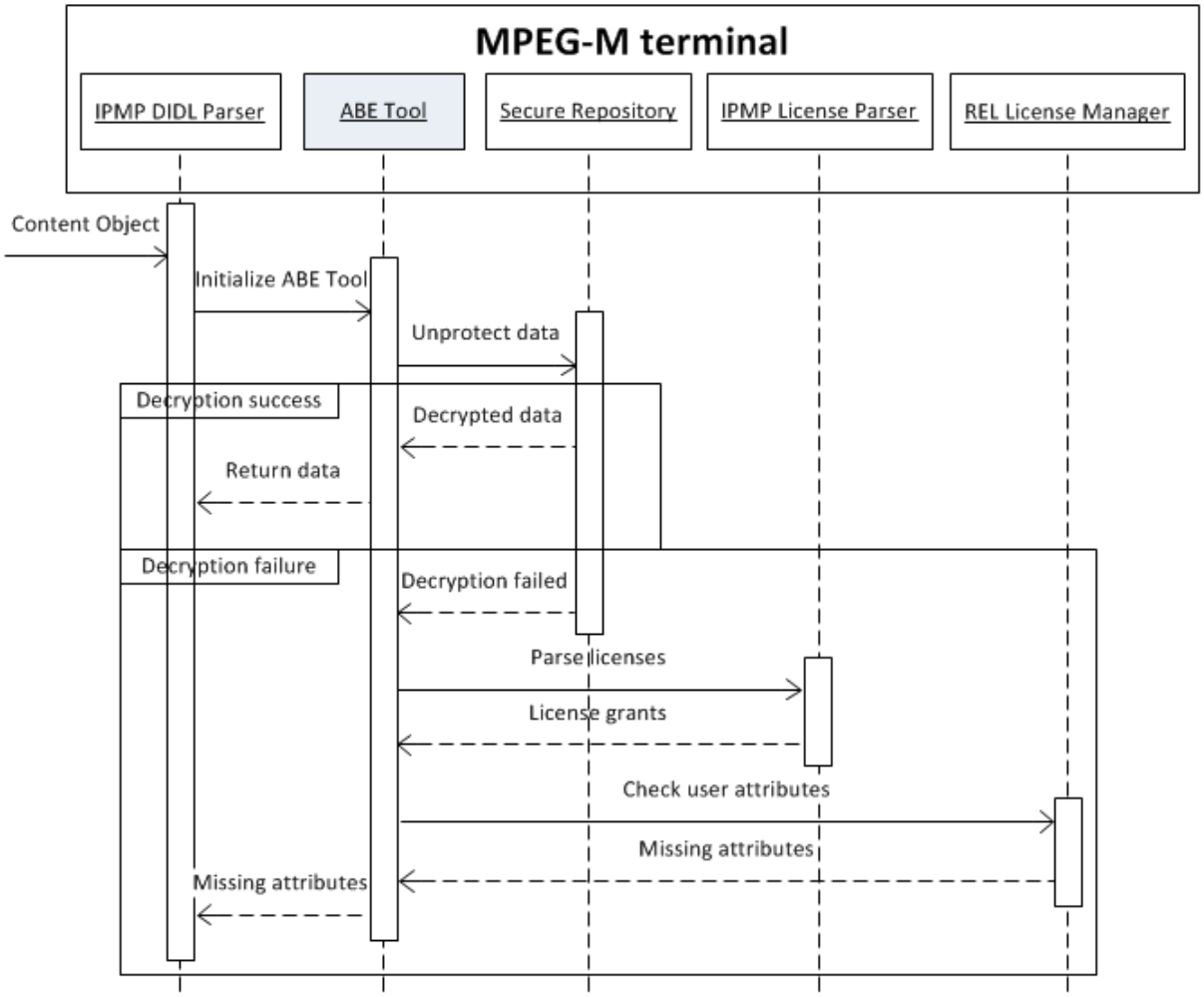
```
01 <didl:Item>
02   <didl:Descriptor>
03     <didl:Statement>
04       <dii:Identifier>
05              hd-vid-124353
06       </dii:Identifier>
07     </didl:Statement>
08   </didl:Descriptor>
09   <didl:Component>
10     <ipmpdidl:Resource mimeType="text/plain"
11           ref="https://hd.vid.com:8080/stream?vidId=124353">
12       <ipmpinfo:Info>
13         <ipmpinfo:IPMPInfoDescriptor>
14           <ipmpinfo:Tool>
15             <ipmpinfo:ToolBaseDescription>
16               <ipmpinfo:IPMPToolID>
17                     gr.ntua.icbnet.security.ABETool
18               </ipmpinfo:IPMPToolID>
19             </ipmpinfo:ToolBaseDescription>
20             <ipmpinfo:RightsDescriptor>
21               <ipmpinfo:LicenseReference>
22                     hd-vid-lic-202621
23               </ipmpinfo:LicenseReference>
24             </ipmpinfo:RightsDescriptor>
25           </ipmpinfo:Tool>
26         </ipmpinfo:IPMPInfoDescriptor>
27       </ipmpinfo:Info>
28     </ipmpdidl:Resource>
29   </didl:Component>
30 </didl:Item>
```

Σχήμα 16: Ψηφιακό αντικείμενο ροής βίντεο υψηλής ανάλυσης (απόσπασμα)

4.4.3 Πρόσβαση στα ψηφιακά αντικείμενα

Εφόσον τα δεδομένα που κυκλοφορούν στο σύστημα περιγράφονται από ένα ψηφιακό αντικείμενο και έχουν κρυπτογραφηθεί με βάση την άδεια χρήσης που συμπεριλαμβάνεται σε αυτό, οι χρήστες που επιθυμούν να αποκτήσουν πρόσβαση στα δεδομένα πρέπει να χρησιμοποιήσουν το ABE κλειδί αποκρυπτογράφησης τους το οποίο έχουν αποθηκευμένο στην ασφαλή συσκευή τους και έχουν αποκτήσει σύμφωνα με τη διαδικασία που περιγράφεται στην παράγραφο 4.4.1. Το σχήμα 17 απεικονίζει την ροή εργασίας που λαμβάνει χώρα στο τερματικό MPEG-M για την πρόσβαση στα κρυπτογραφημένα δεδομένα.

Αρχικά, εξάγονται από το ψηφιακό αντικείμενο η άδεια χρήσης που προστατεύει τα δεδομένα, όπως και το IPMP εργαλείο το οποίο πρέπει να χρησιμοποιηθεί για την αποκρυπτογράφηση των δεδομένων. Σε περίπτωση που το τερματικό δεν έχει στη διάθεση του το συγκεκριμένο εργαλείο, το μεταφορτώνει και το αποθηκεύει στην ασφαλή συσκευή του χρήση για επόμενη χρήση του. Στη συνέχεια, το εργαλείο IPMP θα χρησιμοποιήσει το ABE



Σχήμα 17: Ροή εργασιών πρόσβασης στα δεδομένα [5]

κλειδί του χρήστη και θα προσπαθήσει να αποκρυπτογραφήσει τα δεδομένα.

Αυτή η διαδικασία θα είναι επιτυχής, εκτός κι αν ο χρήστης δεν έχει στην κατοχή του ένα ή περισσότερα χαρακτηριστικά από αυτά που καθιστά αναγκαία η άδεια χρήσης του ψηφιακού αντικειμένου και το κρυπτογραφικό δέντρο πρόσβασης. Τα χαρακτηριστικά αυτά μπορεί να λείπουν είτε διότι ο χρήστης δεν τα είχε είτε διότι η εγκυρότητα τους έχει λήξει. Σε κάθε περίπτωση, το εργαλείο IPMP θα ελέγξει την άδεια χρήσης με τις REL άδειες του χρήστη και θα τον ειδοποιήσει αντίστοιχα για τον λόγο της αποτυχίας αποκρυπτογράφησης των δεδομένων.

Γυρνώντας πίσω στο παράδειγμα με την υπηρεσία ροής βίντεο, έστω ότι η συνδρομή του χρήστη που ίσχυε για έναν μήνα έχει λήξει. Η προαναφερθείσα REL άδεια απεικονίζεται στο σχήμα 18, με την περίοδο εγκυρότητας να ορίζεται στις γραμμές 23–26. Αν ο χρή-

στης δεν έχει κάνει τις απαραίτητες ενέργειες για να ανανεώσει την συνδρομή του μετά την λήξη της, το εργαλείο IPMP θα τον ειδοποιήσει για τη λήξη της και ο χρήστης θα μπορεί να την ανανεώσει και να λάβει το ενημερωμένο ABE κλειδί του που θα καθιστά ικανή την αποκρυπτογράφηση των δεδομένων.

```
01 <rel-r:License licenseId="gold-license-789364">
02   <rel-r:issuer>
03     <dsig:Signature>
04       <dsig:SignatureValue>...</dsig:SignatureValue>
05       <dsig:KeyInfo>
06         <dsig:KeyName>ΤΠΗΡΕΣΙΑ ΡΟΗΣΒΙΝΤΕΟ </dsig:KeyName>
07         <dsig:KeyValue>...</dsig:KeyValue>
08       </dsig:KeyInfo>
09     </dsig:Signature>
10   </rel-r:issuer>
11   <rel-r:inventory>
12     <rel-r:keyHolder licensePartId="x">
13       <dsig:KeyInfo>
14         <dsig:KeyName>ONOMA ΧΡΗΣΤΗ</dsig:KeyName>
15         <dsig:KeyValue>...</dsig:KeyValue>
16       </dsig:KeyInfo>
17     </rel-r:keyHolder>
18   </rel-r:inventory>
19   <rel-r:grant>
20     <rel-r:principal licensePartIdRef="x"/>
21     <rel-r:possessesProperty/>
22     <rel-sx:propertyUri definition="ΑΣΗΜΕΝΙΟΣΣΤΝΔΡΟΜΗΤΗΣ-"/>
23     <rel-r:validityInterval>
24       <rel-r:notBefore>2013-09-01T00:00:00</rel-r:notBefore>
25       <rel-r:notAfter>2013-10-01T00:00:00</rel-r:notAfter>
26     </rel-r:validityInterval>
27   </rel-r:grant>
28 </rel-r:License>
```

Σχήμα 18: Άδεια χρήσης με περίοδο εγκυρότητας (απόσπασμα)

4.5 Σύνοψη

Σε αυτό το κεφάλαιο παρουσιάστηκε μια ενοποιημένη αρχιτεκτονική που εστιάζει στην επίλυση των ζητημάτων που προκύπτουν σε ετερογενή κατανεμημένα συστήματα διαμοιρασμού πληροφορίας. Σε αυτά λαμβάνουν μέρος από τη μια, παραγωγοί περιεχομένου οι οποίοι κατά κανόνα ακολουθούν τις δικές τους πρακτικές για το πακετάρισμα, την προώθηση, τον διαμοιρασμό και την προστασία του περιεχομένου τους. Από την άλλη, οι καταναλωτές περιεχομένου συνιστούν ένα δυναμικό σύνολο από χρήστες οι οποίοι τυπικά βρίσκονται σε διαφορετικούς τομείς ασφαλείας από τους παραγωγούς περιεχομένου. Οι παραπάνω μορφές ετερογένειας, των δομών που διαμοιράζονται και των πολιτικών προστασίας τους, περιορίζουν την εμβέλεια του περιεχομένου αλλά και τη διάχυση της πλη-

ροφορίας.

Έχοντας τα παραπάνω κατά νου, η προτεινόμενη λύση βασίζεται πάνω στις τεχνολογίες του προτύπου MPEG-21 για την περιγραφή και την προστασία των διακινούμενων περιεχομένων. Πιο συγκεκριμένα, υιοθετούνται τα ψηφιακά αντικείμενα ως η βασική μονάδα ανταλλαγής περιεχομένου, ενώ οι κανόνες χρήσης τους εκφράζονται με τη γλώσσα περιγραφής δικαιωμάτων. Επιπρόσθετα, το σύστημα επιβάλει τους κανόνες χρήσης των περιεχομένων με χρήση της καινοτόμου μεθόδου Κρυπτογραφίας Βάσει Χαρακτηριστικών (ΚΒΧ). Το περιεχόμενο κρυπτογραφείται με βάση τους κανόνες χρήσης, αφού πρώτα αυτοί μετασχηματιστούν σε κατάλληλο δέντρο πρόσβασης. Τα παραπάνω υποστηρίζονται από εργαλείο προστασίας και διαχείρισης πνευματικών δικαιωμάτων το οποίο είναι επιφορτισμένο με τη διαχείριση των κλειδιών αποκρυπτογράφησης των χρηστών και χρησιμοποιώντας τις στοιχειώδεις υπηρεσίες του MPEG-M ως πρωτόκολλα επικοινωνίας με τις υποδομές της ΚΒΧ.

Κεφάλαιο 5

Διαχείριση ελέγχου πρόσβασης σε διαδικτυακές υπηρεσίες REST

5.1 Εισαγωγή

Το βασικό παράδειγμα επικοινωνίας μεταξύ διαδικτυακών εφαρμογών έχει πλέον μετατοπιστεί από την υπηρεσιοκεντρική προσέγγιση και έχει κατευθυνθεί στην πληροφοριοκεντρική προσέγγιση [99]. Οι υπηρεσιοκεντρικές αρχιτεκτονικές (Service-Oriented Architectures - SOA) παρέχουν σημαντικά πλεονεκτήματα στους οργανισμούς, επιτρέποντας την επικοινωνία μεταξύ διαφορετικών εφαρμογών εκθέτοντας η κάθε μια σύνολα υπηρεσιών μαζί με τις περιγραφές τους χρησιμοποιώντας τη γλώσσα περιγραφής δικτυακών υπηρεσιών (Web Service Description Language - WSDL - [100]). Οι υπηρεσίες αυτές καλούνται με το πρωτόκολλο SOAP (Simple Object Access Protocol - [101]) και ουσιαστικά καθιστούν δυνατή την αποδοτική επικοινωνία ανεξάρτητα από την υλοποίηση τους.

Ωστόσο, οι υπηρεσίες που αναπτύσσονται με τον παραπάνω τρόπο δεν είναι ενσωματωμένες με το διαδίκτυο παρά το χρησιμοποιούν ως μέσο. Το τελευταίο το καταφέρνουν οι υπηρεσίες που ακολουθούν την πληροφοριοκεντρική προσέγγιση Resource-Oriented Architecture (ROA), με το ίδιο το διαδίκτυο να αποτελεί το καλύτερο παράδειγμα. Στην πληροφοριοκεντρική προσέγγιση οι εφαρμογές επικοινωνούν μεταξύ τους ανταλλάσσοντας δομές πληροφορίας οι οποίες έχουν μοναδικό αναγνωριστικό και μπορούν να

περιέχουν εκτός από δεδομένα και μεταδεδομένα κατάστασης, ελέγχου και παρουσίασης.

Η πληροφοριοκεντρική αρχιτεκτονική REST (REpresentational State Transfer - REST - [102]) έχει τύχει τα τελευταία χρόνια ευρείας αποδοχής λόγο της απλότητας και ευελιξίας την οποία προσφέρει στην ανάπτυξη μιας διαδικτυακής υπηρεσίας. Οι βασικές σχεδιαστικές αρχές μιας υπηρεσίας REST εντοπίζονται στην διευθυνσιοδότηση, την ομοιόμορφη διεπαφή και την έλλειψη καταγραφής κατάστασης [103]. Κάθε ουσιαστικό τμήμα πληροφορίας λαμβάνει μοναδικό αναγνωριστικό και διεύθυνση πρόσβασης. Παράλληλα, ανεξάρτητα από το διαφορετικό μέρος πληροφορίας και των λειτουργιών που εκτίθεται μέσω μιας διεπαφής REST, η διεύθυνση πρόσβασης ακολουθεί συνήθως συγκεκριμένο πρότυπα οδηγώντας σε οικίες και ομοιόμορφες διεπαφές για την υπηρεσία, βασισμένες στις μεθόδους του πρωτοκόλλου HTTP (GET/POST/PUT/DELETE). Επιπρόσθετα, κάθε κλήση προς τη διεπαφή είναι ανεξάρτητη από τις προηγούμενές και έτσι δεν επιβάλει την καταγραφή κατάστασης από τον εξυπηρετητή. Τα παραπάνω, καθιστούν την αρχιτεκτονική διαδικτυακών υπηρεσιών REST ιδανική για μεγάλης κλίμακας εφαρμογές οι οποίες αναπτύσσονται σε πολλαπλούς τομείς, αφού πετυχαίνει ενίσχυση της διαλειτουργικότητας, μείωση του κόστους ενσωμάτωσης σε υπάρχουσες εφαρμογές και ακόμα πιο χαλαρή σύζευξη τόσο μεταξύ άλλων υπηρεσιών αλλά και από τα συνεχώς εξελισσόμενα τεχνολογικά πρότυπα.

Σε αυτό το πλαίσιο, ο αποδοτικός έλεγχος πρόσβασης στις διαδικτυακές υπηρεσίες αποτελεί κρίσιμη παράμετρο για την περαιτέρω εξέλιξη τους. Πέρα από τα υπάρχοντα κεντρικοποιημένα μοντέλα ελέγχου πρόσβασης που βασίζονται στον ρητό ορισμό των εξουσιοδοτημένων χρηστών με τη μορφή λιστών (Access Control Lists) ή στον έλεγχο πρόσβασης βάσει των ρόλων των χρηστών (Role-Based Access Control - RBAC), έχουν εμφανιστεί και αρχιτεκτονικές οι οποίες στοχεύουν σε κατανεμημένα περιβάλλοντα και στην κατανεμημένη λήψη αποφάσεων εξουσιοδότησης. Οι λύσεις αυτές υποστηρίζουν μεγάλο αριθμό ετερογενών συμμετεχόντων οι οποίοι σχετίζονται χαλαρά και αλληλεπιδρούν με δυναμικό τρόπο, ενώ βρίσκονται υπό την εποπτεία διαφορετικών οντοτήτων.

Σε ένα κατανεμημένο περιβάλλον ωστόσο, δύο ζητήματα κάνουν την εμφάνιση τους αυτόματα, τόσο η διαλειτουργικότητα των πολιτικών ασφαλείας όσο και η επιβολή τους. Σε ότι αφορά την διαλειτουργικότητα, οι προσπάθειες προτυποποίησης (βλ. [51][52]) προσφέρουν σημαντικά εργαλεία, ωστόσο η επιβολή των διαφόρων πολιτικών περιορίζε-

ται στο παράδειγμα PDP–PEP (Policy Decision Point–Policy Enforcement Point, Σημείο Εξέτασης Πολιτικών–Σημείο Επιβολής Πολιτικών - [54]), το οποίο από τη μια απαιτεί την αποκάλυψη των διαπιστευτηρίων των χρηστών αλλά και τον συνεχή έλεγχο της εγκυρότητας τους.

Η προτεινόμενη λύση που παρουσιάζεται σε αυτό το κεφάλαιο στοχεύει στην επίλυση των προαναφερθέντων ζητημάτων και στη προστασία διαδικτυακών υπηρεσιών που ακολουθούν την αρχιτεκτονική REST με έναν ολοκληρωμένο τρόπο. Αρχικά, χρησιμοποιείται ένα μοναδικό ψηφιακό αντικείμενο για την περιγραφή των μεθόδων της διεπαφής. Στη συνέχεια με χρήση της γλώσσας περιγραφής δικαιωμάτων MPEG-21 REL εκφράζονται τα δικαιώματα χρήσης που πρέπει να έχουν οι χρήστες για να αποκτήσουν πρόσβαση σε κάποια μέθοδο. Κάθε χρήστης δεν ορίζεται ωστόσο ρητά μέσω κάποιου μοναδικού αναγνωριστικού, αλλά βάσει των χαρακτηριστικών που πρέπει να έχει στην κατοχή του. Με αυτόν τον τρόπο υποστηρίζονται δυναμικά σύνολα χρηστών αλλά και ετερογενείς οργανισμοί πιστοποίησης χαρακτηριστικών. Πιο συγκεκριμένα, οι χρήστες λαμβάνουν REL άδειες οι οποίες πιστοποιούν την κατοχή κάποιου χαρακτηριστικού και με αυτές λαμβάνουν το προσωπικό τους κλειδί αποκρυπτογράφησης ABE. Ακολουθώντας τις προδιαγραφές του προηγούμενου κεφαλαίου, πραγματοποιείται κρυπτογράφηση κοινόχρηστου κλειδιού (βάσει του οποίου πραγματοποιείται ο έλεγχος πρόσβασης) που αντιστοιχεί σε κάθε μέθοδο και ενέργεια της διεπαφής REST ξεχωριστά.

Η ακόλουθη παράγραφος παρουσιάζει τις τρέχουσες προσεγγίσεις στον έλεγχο πρόσβασης σε διαδικτυακές υπηρεσίες αναδεικνύοντας τους περιορισμούς και τις αδυναμίες τους. Στη συνέχεια παρουσιάζεται η αρχιτεκτονική της προτεινόμενης λύσης και λεπτομερής περιγραφή των επιμέρους τμημάτων της. Πιο συγκεκριμένα, αναλύεται η δημιουργία ψηφιακού αντικειμένου για την περιγραφή διεπαφής REST, αλλά και η άδεια χρήσης της. Ενώ, τέλος, παρουσιάζεται ο μηχανισμός με τον οποίο πραγματοποιείται ο έλεγχος πρόσβασης στην διεπαφή με βάση τα παραπάνω στοιχεία.

5.2 Τρέχουσες τάσεις στον έλεγχο πρόσβασης διαδικτυακών υπηρεσιών

Το προτεινόμενο σύστημα στοχεύει στην προστασία διαδικτυακών υπηρεσιών σε μεγάλης κλίμακας ετερογενή περιβάλλοντα. Σε αυτό το πλαίσιο, εμφανίζονται προβλήματα διαλειτουργικότητας τόσο στις πολιτικές ασφαλείας των διαδικτυακών υπηρεσιών, αλλά και στον τρόπο με τον οποίο πραγματοποιείται η ταυτοποίηση των χρηστών για την κατανάλωση των υπηρεσιών.

Ακρογωνιαίος λίθος για την ασφάλεια διαδικτυακών υπηρεσιών που στηρίζονται στην τεχνολογία SOAP αποτελεί η σουίτα προτύπων WS-* του οργανισμού OASIS [104], στα οποία προδιαγράφονται τεχνολογικές λύσεις για τον ορισμό, την ανάπτυξη και προστασία τους. Αρχικά, το πρότυπο WS-Security στοχεύει στην προστασία και την ακεραιότητα των μηνυμάτων SOAP που στέλνονται μεταξή πελάτη-υπηρεσίας. Για το λόγο αυτό, χρησιμοποιεί το πρότυπο XML Encryption [105] για την κρυπτογράφηση τμημάτων των μηνυμάτων, αλλά και το πρότυπο XML Digital Signature [11] για την ψηφιακή υπογραφή τους. Παράλληλα, εισάγει την έννοια των διαπιστευτηρίων ασφαλείας (security tokens), όπως οι ευρέως διαδεδομένες τεχνολογίες SAML, X.509 αλλά και άδειες χρήσης στη γλώσσα MPEG-21 REL, βάση των οποίων γίνεται η ταυτοποίηση των χρηστών. Στη συνέχεια, το πρότυπο WS-Trust [106] εισάγει τις υπηρεσίες διαπιστευτηρίων ασφαλείας (Security Token Service - STS), οι οποίες είναι υπεύθυνες για την έκδοση security tokens, και προδιαγράφει τα πρωτόκολλα με τα οποία πραγματοποιείται η επικοινωνία για την έκδοση νέου security token, την ανανέωση του, αλλά και του ελέγχου της εγκυρότητας του. Τέλος, το πρότυπο WS-SecurityPolicy [107] προδιαγράφει τον τρόπο με τον οποίο δηλώνονται οι πολιτικές ασφαλείας της υπηρεσίας. Πιο συγκεκριμένα, οι πολιτικές ενσωματώνονται στην περιγραφή WSDL της υπηρεσίας και καθορίζουν τα διαπιστευτήρια ασφαλείας που απαιτούνται για την πρόσβαση σε κάθε μέθοδο της διεπαφής, αλλά και τα σημεία των μηνυμάτων SOAP που πρέπει να προστατεύονται.

Η ασφάλεια και οι δυνατότητες που προσφέρει η σουίτα προτύπων WS-* κατοχυρώνονται μέσω της ευρείας υιοθέτησης τους και της χρήσης τους σε σενάρια ιδιαίτερης κρισιμότητας και απαιτήσεων ασφαλείας. Ωστόσο, η εμφάνιση της αρχιτεκτονικής διαδι-

κτυακών υπηρεσιών REST, έκανε έκδηλη την πολυπλοκότητα και τις δυσκολίες ανάπτυξης μιας διαδικτυακής υπηρεσίας με την τεχνολογία SOAP και πλέον, η πλειοψηφία των διαδικτυακών υπηρεσιών σχεδιάζονται ακολουθώντας την αρχιτεκτονική REST.

Το γεγονός όμως πως η αρχιτεκτονική REST δεν εξετάζει ζητήματα ελέγχου πρόσβασης στις μεθόδους μιας υπηρεσίας, αλλά και η απουσία πρόβλεψης εισαγωγής πολιτικών ασφαλείας στη γλώσσας περιγραφής υπηρεσιών REST (WADL - Web Application Description Language) [108], έχει οδηγήσει στην ανάπτυξη μη διαλειτουργικών υπηρεσιών REST.

Η διεπαφή REST της δημοφιλούς υπηρεσίας αποθήκευσης αρχείων Drive της Google [2], προστατεύεται βασιζόμενη σε λίστες ελέγχου πρόσβασης [3]. Πιο συγκεκριμένα, ο κάτοχος ενός εικονικού δίσκου στο σύννεφο του Drive, πρέπει να εξουσιοδοτήσει ρητά τους χρήστες που θα έχουν πρόσβαση σε κάποιο αρχείο, χωρίς να μπορεί να καθορίσει τους εξουσιοδοτημένους χρήστες με έμμεσο τρόπο μέσω των χαρακτηριστικών τους. Παράλληλα, παρέχεται δυνατότητα για καθορισμό των ενεργειών που μπορούν να πραγματοποιούν οι χρήστες πάνω σε κάθε αρχείο. Ωστόσο, κάθε εξουσιοδοτημένος χρήστης πρέπει να είναι ήδη εγγεγραμμένος στην Google, αφού δεν υποστηρίζει κάποιον άλλο τρόπο ταυτοποίησης του.

Για την πρόσβαση στις διαδικτυακές υπηρεσίες REST που προσφέρει η Amazon [4] για τα προϊόντα της, είναι απαραίτητη η λήψη προσωρινού secure token από τον STS εξυπηρετητή της. Πριν τη λήψη του secure token έχει προηγηθεί είσοδος στην υπηρεσία μέσω των υποστηριζόμενων πρωτοκόλλων Oauth2 [109] ή SAML ώστε ο εξυπηρετητής να χτίσει το τρέχον πλαίσιο ασφαλείας (security context). Στη συνέχεια, κάθε κλήση προς τη διεπαφή συνοδεύεται από την ψηφιακή υπογραφή της, που έχει προκύψει χρησιμοποιώντας το secure token. Με βάση το μοναδικό αναγνωριστικό του secure token, ο εξυπηρετητής ταυτοποιεί τον χρήστη και ελέγχει εάν τα χαρακτηριστικά, οι ρόλοι και τα δικαιώματα του πληρούν τις πολιτικές χρήσης της υπηρεσίας. Ωστόσο, οι τελευταίες δεν βασίζονται σε κάποιο υπάρχον πρότυπο, αλλά στο μοντέλο πολιτικών ασφαλείας της υπηρεσίας IAM

[2] http://drive.google.com
[3] https://support.google.com/drive/answer/2494822?hl=en&ref_topic=2525251
[4] http://aws.amazon.com/

(Amazon Identity and Access Management [5] - Διαχείριση Ταυτότητας και Πρόσβασης).

Τέλος, η ανάγκη για ασφαλείς διαδικτυακές υπηρεσίες REST, οδήγησε στην ανάπτυξη ξεχωριστής λειτουργικής μονάδας ελέγχου πρόσβασης για τη δημοφιλή βιβλιοθήκη ανάπτυξης διαδικτυακών υπηρεσιών Django [6]. Το αντικειμενοστραφές μοντέλο της μονάδας ελέγχου πρόσβασης στοχεύει στην αναπαράσταση πολιτικών ασφαλείας και της σύνδεσης τους με τις μεθόδους της διεπαφής, ωστόσο αυτό καλύπτει μονάχα τις βασικές περιπτώσεις ελέγχου πρόσβασης και χρειάζεται επέκταση. Πιο συγκεκριμένα, τα αντικείμενα (Resources) που ανταλλάσσονται μέσω της διεπαφής, ενσωματώνονται σε μοντέλα πληροφορίας (Model) πάνω στα οποία ένας χρήστης (User) μπορεί να πραγματοποιήσει μια εργασία (Task). Ο προγραμματιστής έχει τη δυνατότητα να σχεδιάσει το επιθημητό μοντέλο ελέγχου πρόσβασης, και αφού ταυτοποιήσει τον χρήστη (π.χ. μέσω LDAP (Lightweight Directory Access Protocol [110])) να ελέγξει προγραμματιστικά εάν πληροί τις προϋποθέσεις εκτέλεσης της εργασίας.

5.3 Σύστημα ελέγχου πρόσβασης διαδικτυακών υπηρεσιών REST

Το προτεινόμενο σύστημα αφορά στην υποστήριξη διαδικτυακών υπηρεσιών που ακολουθούν την αρχιτεκτονική REST, και στοχεύει στον χωρίς σύνδεση έλεγχο πρόσβασης σε διεπαφές REST. Το παραπάνω καθίσταται δυνατό αναπαριστώντας μια διεπαφή REST με ένα ψηφιακό αντικείμενο το οποίο καθορίζει τις μεθόδους που αυτή προσφέρει αλλά και τους χρήστες που είναι εξουσιοδοτημένοι να τις χρησιμοποιήσουν. Οι χρήστες περιγράφονται με βάση τα χαρακτηριστικά τα οποία πρέπει να έχουν στην κατοχή τους, ενώ ο χωρίς σύνδεση έλεγχος πρόσβασης στα χαρακτηριστικά που κατέχουν, πραγματοποιείται με τη χρήση κρυπτογραφίας βάσει χαρακτηριστικών.

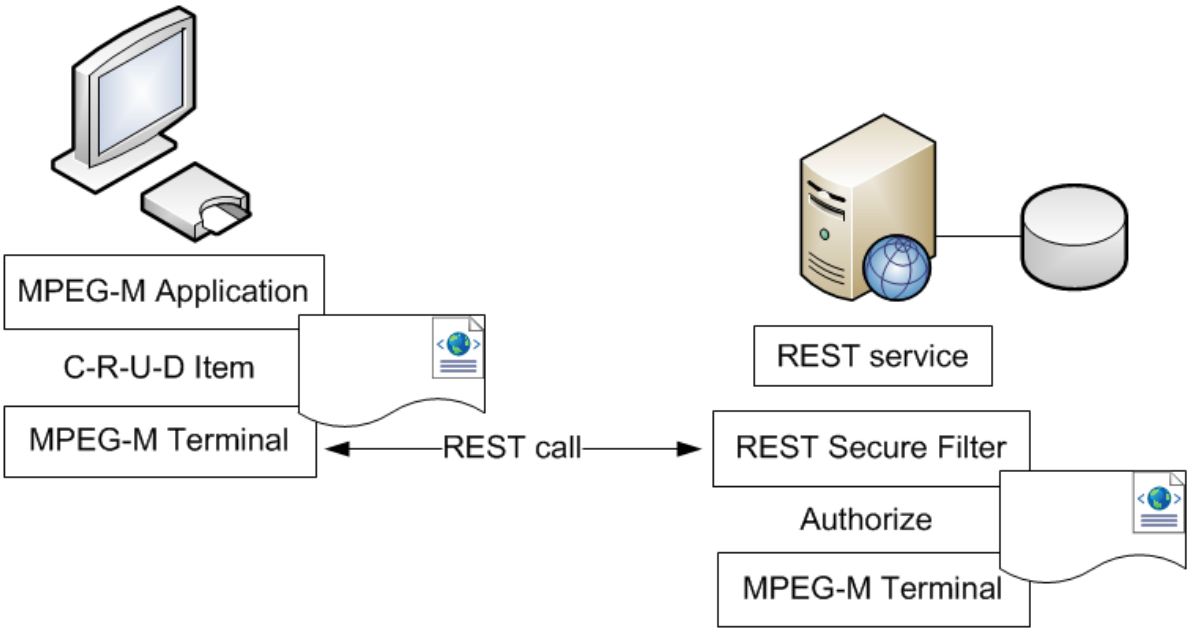
Το ψηφιακό αντικείμενο καθορίζει πλήρως τις μεθόδους της διεπαφής, με τρόπο που τόσο οι καλούντες όσο και ο εξυπηρετητής μπορούν να επεξεργάζονται. Πιο συγκεκριμένα, οι διευθύνσεις URL της διεπαφής συνδυάζονται με πολιτικές ελέγχου πρόσβασης που ενσωματώνουν κοινόχρηστο κλειδί κρυπτογραφημένο βάσει των χαρακτηριστι-

[5] http://docs.aws.amazon.com/IAM/latest/UserGuide/PoliciesOverview.html
[6] https://code.google.com/p/implementing-rest/wiki/DjangoRESTframework

κών τους. Σε κάθε κλήση προς τον εξυπηρετητή προστίθεται το αντίστοιχο αποκρυπτογραφημένο κλειδί, ενώ ο εξυπηρετητής δίνει πρόσβαση στην εισερχόμενη αίτηση μονάχα εάν το κοινόχρηστο κλειδί βρίσκεται σε συμφωνία με την άδεια χρήσης.

Στο σημείο αυτό, αξίζει να σημειωθεί πως το παρόν σύστημα ακολουθεί τις προδιαγραφές του συστήματος του προηγούμενου κεφαλαίου σε ότι αφορά τη λήψη κλειδιών ABE και την κρυπτογράφηση. Άλλωστε, τα δύο συστήματα μοιράζονται τις ίδιες θεμελιώδεις αρχές, δηλαδή έλεγχο πρόσβασης βάσει χαρακτηριστικών, χρήση της γλώσσας περιγραφής δικαιωμάτων τόσο για πιστοποίηση χαρακτηριστικών αλλά και για δήλωση πολιτικών πρόσβασης και επιβολή τους με κρυπτογραφία βάσει χαρακτηριστικών.

Στο ακόλουθο σχήμα, απεικονίζεται η αρχιτεκτονική του συστήματος και παρουσιάζεται η επικοινωνία μιας εφαρμογής βασισμένης στο MPEG-M με διεπαφή REST. Πιο συγκεκριμένα, οι αλληλεπιδράσεις της εφαρμογής με το ψηφιακό αντικείμενο που περιγράφει τη διεπαφή, μεταφράζονται σε κλήσεις REST, δίχως η εφαρμογή να έχει γνώση των υποκείμενων τεχνολογιών που την καθιστούν δυνατή. Παράλληλα, στην πλευρά του εξυπηρετητή, ο έλεγχος πρόσβασης πραγματοποιείται με την προσθήκη ενός φίλτρου στις εισερχόμενες κλήσεις REST, η λειτουργία του οποίου παρουσιάζεται αναλυτικά στην παράγραφο 5.3.3.



Σχήμα 19: Αρχιτεκτονική συστήματος offline ελέγχου πρόσβασης σε διαδικτυακές υπηρεσίες REST

Βασικά πλεονεκτήματα της αρχιτεκτονικής του συστήματος αποτελούν η διαφάνεια που προσφέρει στην πλευρά της εφαρμογής όταν αυτή αλληλεπιδρά με την υπηρεσία, αλλά και η ευκολία ενσωμάτωσης της λύσης στην πλευρά του εξυπηρετητή. Τα παραπάνω διευκολύνουν την ανάπτυξη ασφαλών πληροφοριοκεντρικών εφαρμογών και επιτρέπουν την πλήρη εστίαση τους στο περιεχόμενο.

Στις παραγράφους που ακολουθούν χρησιμοποιείται ως παράδειγμα η διεπαφή REST που προσφέρει το διαδεδομένο σύστημα διαχείρισης ψηφιακής βιβλιοθήκης DSpace [7], το οποίο δίνει τη δυνατότητα προσθήκης νέων ψηφιακών εγγράφων, επεξεργασία των ήδη υπαρχόντων αλλά και τη δημιουργία συλλογών από έγγραφα. Πιο συγκεκριμένα, θα περιγραφούν οι μέθοδοι που ορίζει το DSpace για την εισαγωγή, την αντικατάσταση, την ενημέρωση και τη διαγραφή ενός ψηφιακού εγγράφου.

5.3.1 Ορισμός και ανάπτυξη διεπαφής REST στον εξυπηρετητή

Ο ορισμός μια διεπαφής REST πραγματοποιείται με ένα μοναδικό ψηφιακό αντικείμενο το οποίο συνοδεύεται από την άδεια χρήσης που το προστατεύει. Στο ψηφιακό αντικείμενο περιλαμβάνονται οι διευθύνσεις εισόδου στη διεπαφή, ενώ η άδεια χρήσης περιγράφει τις μεθόδους που υποστηρίζει κάθε διεύθυνση URL π.χ. POST, και τους κανόνες ελέγχου πρόσβασης που τις αφορούν. Ουσιαστικά, το δημιουργηθέν ψηφιακό αντικείμενο περιλαμβάνει όλη την πληροφορία που χρειάζεται κάποιος για να αποκτήσει πρόσβαση στη διεπαφή.

Στο παρακάτω σχήμα περιγράφεται το μέρος της διεπαφής REST του DSpace και αφορά στην προστασία των μεθόδων που αφορούν τη διαχείριση των ψηφιακών εγγράφων της βιβλιοθήκης. Αρχικά, κάθε διεύθυνση εισόδου της διεπαφής REST αναπαριστάται ως ένα τμήμα (Component) του ψηφιακού αντικειμένου. Στη γραμμή 10 δηλώνεται η διεύθυνση URL της διεπαφής, η οποία προστατεύεται από το εργαλείο προστασίας και διαχείρισης πνευματικών δικαιωμάτων RESTTool, σύμφωνα με τους κανόνες χρήσης που ορίζει η άδεια χρήσης της γραμμής 21.

Η ανάπτυξη της διεπαφής REST στον εξυπηρετητή μπορεί να ακολουθεί δύο μο-

[7] http://wiki.duraspace.org/display/DSDOC4x/REST+API

```
01 <didl:Item>
02   <didl:Descriptor>
03     <didl:Statement>
04       <dii:Identifier>
05              ntua-dspace-rest
06       </dii:Identifier>
07     </didl:Statement>
08   </didl:Descriptor>
09   <didl:Component>
10     <ipmpdidl:Resource id="ITEMS" ref="https://dspace.lib.ntua.gr/rest/items/*">
11       <ipmpinfo:Info>
12         <ipmpinfo:IPMPInfoDescriptor>
13           <ipmpinfo:Tool>
14             <ipmpinfo:ToolBaseDescription>
15               <ipmpinfo:IPMPToolID>
16                      gr.ntua.icbnet.security.RESTTool
17               </ipmpinfo:IPMPToolID>
18             </ipmpinfo:ToolBaseDescription>
19             <ipmpinfo:RightsDescriptor>
20               <ipmpinfo:LicenseReference>
21                      ntua-dspace-rest-lic
22               </ipmpinfo:LicenseReference>
23             </ipmpinfo:RightsDescriptor>
24           </ipmpinfo:Tool>
25         </ipmpinfo:IPMPInfoDescriptor>
26       </ipmpinfo:Info>
27     </ipmpdidl:Resource>
28   </didl:Component>
29 </didl:Item>
```

Σχήμα 20: Αναπαράσταση διεπαφής REST με ένα ψηφιακό αντικείμενο (απόσπασμα)

ντέλα. Από τη μια μπορεί να υπάρχει ήδη υπάρχουσα διεπαφή REST η οποία καλείται να προστατευθεί, όποτε σε αυτή την περίπτωση το ψηφιακό αντικείμενο και η άδεια χρήσης χρησιμοποιούνται ώστε να ελέγξουν την πρόσβαση στην διεπαφή. Από την άλλη, το ψηφιακό αντικείμενο μπορεί να χρησιμοποιηθεί ώστε να αναπτυχθεί μια νέα διεπαφή στον εξυπηρετητή την οποία μπορούν να χρησιμοποιούν με ασφάλεια οι χρήστες που περιγράφει η άδεια χρήσης. Το πρώτο μοντέλο μπορεί να χρησιμοποιηθεί για την διασφάλιση οποιαδήποτε υπηρεσίας REST, ενώ το τελευταίο ενισχύει την ασφαλή συνεργασία μεταξύ πολλαπλών οντοτήτων.

Τα παραπάνω καθίστανται δυνατά δηλώνοντας στον εξυπηρετητή τα ψηφιακά αντικείμενα και τις άδειες χρήσης τους χρησιμοποιώντας τις στοιχειώδεις υπηρεσίες του MPEG-M (StoreContent και StoreLicense). Αυτά στη συνέχεια επεξεργάζονται από φίλτρο εισερχόμενων HTTP αιτήσεων, του οποίου η λειτουργία θα παρουσιαστεί στην παράγραφο 5.3.3, ώστε να γίνει έλεγχος πρόσβασης στη διεπαφή REST.

5.3.2 Ορισμός κανόνων χρήσης διεπαφής REST

Οι κανόνες χρήσης μιας διεπαφής REST περιγράφονται με τη μορφή αδειών χρήσης της γλώσσας MPEG-21 REL. Κάθε εκχώρηση δικαιωμάτων χρήσης (grant) της άδειας αναφέρεται σε συγκεκριμένη διεύθυνση URL και HTTP μέθοδο, ο συνδυασμός των οποίων ουσιαστικά ορίζει μια ατομική ενέργεια σε ένα περιεχόμενο (resource). Για κάθε εκχώρηση χρήσης απαιτούνται τα παρακάτω:

- Ο ορισμός του υποκειμένου κάθε εκχώρησης χρήσης πραγματοποιείται περιγραφικά, με βάση τα χαρακτηριστικά που πρέπει να έχει στην κατοχή του κάποιος χρήστης (σύμφωνα με τις προδιαγραφές που περιγράφονται στην παράγραφο 4.4.2), κι όχι ρητά με βάση το δημόσιο κλειδί των χρηστών. Αυτό δίνει τη δυνατότητα να υποστηριχθούν δυναμικά σύνολα χρηστών, αλλά και να συμπεριληφθούν πολλαπλές αρχές έκδοσης χαρακτηριστικών.

- Ο ορισμός του δικαιώματος χρήσης (right) κάθε εκχώρησης δικαιωμάτων χρήσης καθορίζει την HTTP μέθοδο (GET, POST, PUT, DELETE) που θα χρησιμοποιηθεί για την κλήση της διεπαφής REST. Στον παρακάτω πίνακα φαίνονται οι αντιστοιχίες για τις βασικές μεθόδους CRUD μιας διεπαφής REST, ωστόσο η τελευταία μπορεί να παρέχει κι άλλες μεθόδους όπως αναζήτηση. Σε αυτή την περίπτωση, μπορούν να χρησιμοποιηθούν υπάρχοντα ρήματα τα οποία προσφέρει η γλώσσα περιγραφής δικαιωμάτων, αλλά και καθορισμός νέων ρημάτων με βάση το λεξικό δικαιωμάτων.

Ενέργεια	Δικαίωμα χρήσης	Μέθοδος HTTP
CREATE	rel-r:issue	POST
READ	rel-mx:play	GET
UPDATE	rel-mx:modify	PUT
DELETE	rel-r:revoke	DELETE
SEARCH	rel-m1x:enlist	GET

Πίνακας 3: Αντιστοίχιση ενεργειών με δικαιώματα χρήσης και HTTP μέθοδο

- Αντικείμενο της εκχώρησης χρήσης αποτελεί η πρόσβαση σε κάποια συγκεκριμένη

διεύθυνση URL και το περιεχόμενο που αυτή προστατεύει, εάν πρόκειται για μέθοδο GET. Αυτή μοντελοποιείται ως προστατευμένο περιεχόμενο (protectedResource) το οποίο συμπεριλαμβάνει τον ορισμό του περιεχομένου που προστατεύεται, π.χ. μια εικόνα, τα αποτελέσματα μιας αναζήτησης ή ακόμα κι ένα ψηφιακό αντικείμενο.

Στο παρακάτω σχήμα παρατίθεται μέρος της άδειας χρήσης που αφορά στην προστασία των μεθόδων διαχείρισης ψηφιακών εγγράφων της διεπαφής του DSpace. Πιο συγκεκριμένα, αντικατοπτρίζει την πολιτική που πρέπει να διέπει την προσθήκη νέων εγγράφων στην ψηφιακή βιβλιοθήκη, με το γραμματειακό προσωπικό να είναι υπεύθυνο για την διαδικασία. Η πολιτική αυτή διασφαλίζεται με τη βοήθεια του κοινόχρηστου κλειδιού που ορίζεται στη γραμμή 16, το οποίο έχει κρυπτογραφηθεί με βάση τα χαρακτηριστικά που πρέπει να κατέχει ο χρήστης που καλεί την υπηρεσία. Στην συγκεκριμένη περίπτωση λοιπόν, κρυπτογραφείται με βάση το χαρακτηριστικό *NTUA:SCHOOL-SECRETARY* αλλά και το χαρακτηριστικό του συστήματος *system:access_control*, το οποίο έχει στην κατοχή του ο εξυπηρετητής.

```
01 <rel-r:License licenseId="ntua-dspace-rest-lic">
02   <rel-r:grant>
03     <rel-r:forAll varName="grammateia">
04       <rel-r:propertyPossessor>
05         <rel-sx:propertyUri definition="NTUA:SCHOOL-SECRETARY"/>
06       </rel-r:propertyPossessor>
07     </rel-r:forAll>
08     <rel-r:principal varRef="grammateia"/>
09     <rel-r:issue/>
10     <rel-m1x:protectedResource>
11       <rel-r:digitalResource>
12         <rel-r:secureIndirect URI="#ITEMS"/>
13       </rel-r:digitalResource>
14           <xenc:encryptedKey MimeType="">
15         <xenc:CipherData>
16           <xenc:CipherValue>ABC...</xenc:CipherValue
17         </xenc:CipherData>
18       </xenc:encryptedKey>
19     </rel-m1x:protectedResource>
20   </rel-r:grant>
21 </rel-r:License>
```

Σχήμα 21: Άδεια χρήσης που ρυθμίζει την πρόσβαση στην υπηρεσία REST (απόσπασμα)

5.3.3 Ελεγχόμενη πρόσβαση σε διεπαφές REST

Ο έλεγχος πρόσβασης σε μια διεπαφή REST πραγματοποιείται σε δύο φάσεις. Η πρώτη φάση λαμβάνει χώρα στο περιβάλλον του χρήστη της υπηρεσίας REST και ξεκινάει

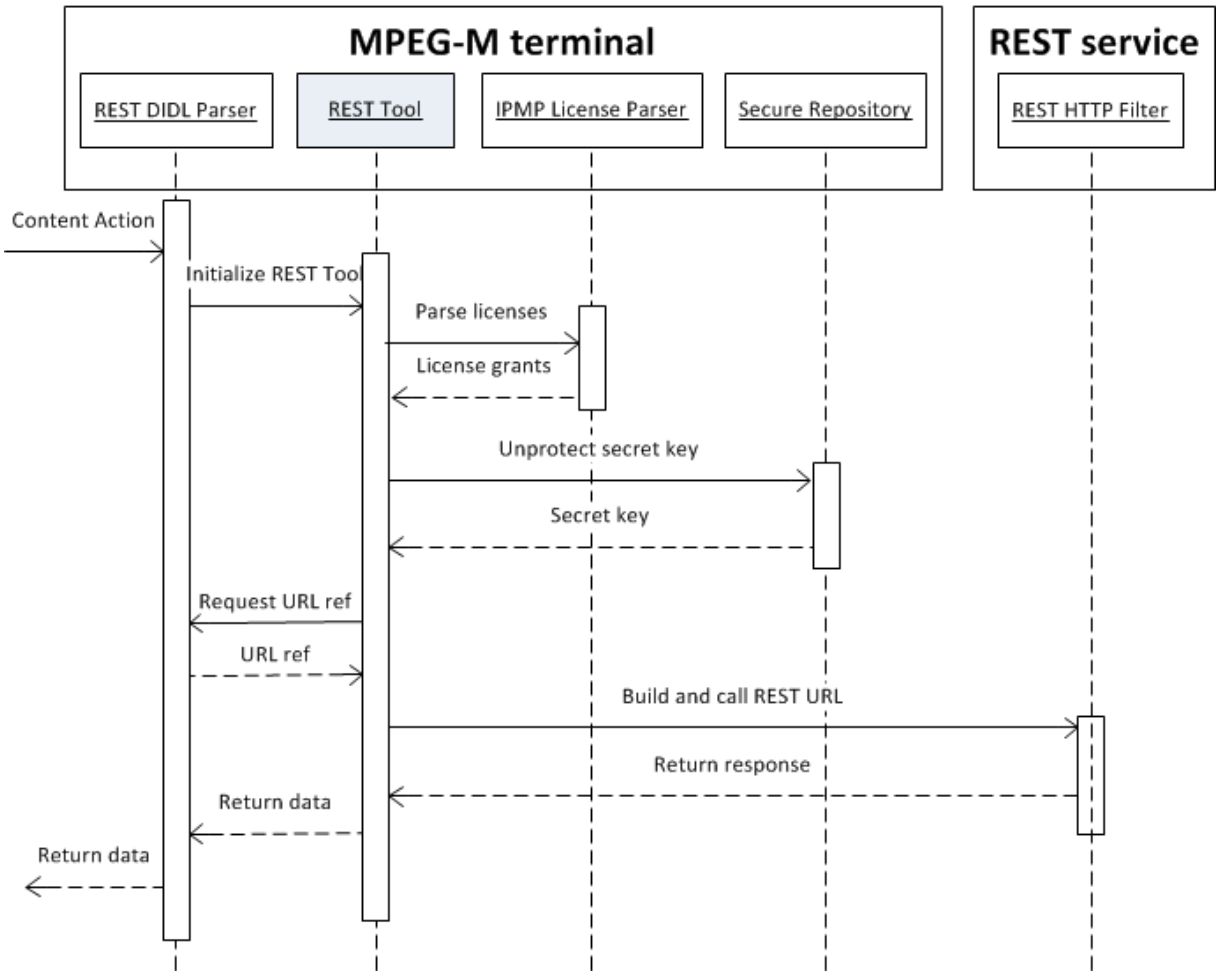
με την επεξεργασία του ψηφιακού αντικειμένου που περιγράφει τη διεπαφή, ενώ η δεύτερη λαμβάνει χώρα στον εξυπηρετητή όπου και δίνεται η εξουσιοδότηση για την χρήση της.

Αρχικά, ας θεωρήσουμε την διεπαφή REST του DSpace, η οποία περιγράφεται από το ψηφιακό αντικείμενο του σχήματος 29. Έστω επίσης πως γραμματέας της Σ.Η.Μ.Μ.Υ. επιθυμεί να προσθέσει μια διδακτορική διατριβή στην ψηφιακή βιβλιοθήκη του Ε.Μ.Π.. Για να πραγματοποιήσει την παραπάνω ενέργεια, η γραμματέας θα χρησιμοποιήσει την εφαρμογή διαχείρισης συγγραμμάτων της βιβλιοθήκης η οποία βασίζεται στο μεσισμικό του MPEG-M ώστε να χρησιμοποιήσει τις υπηρεσίες που περιγράφονται στο ψηφιακό αντικείμενο της υπηρεσίας REST του DSpace. Πιο συγκεκριμένα, οι λειτουργίες της εφαρμογής αντιστοιχούν σε χρήση τμημάτων του ψηφιακών αντικειμένων, π.χ. η προσθήκη αντιστοιχεί στην δημιουργία (rel-r:issue) ενός νέου εγγράφου (αντικείμενο με id 'ITEMS').

Το αντικείμενο 'ITEMS' προστατεύεται ωστόσο από το εργαλείο διαχείρισης και προστασίας πνευματικών δικαιωμάτων 'gr.ntua.icbnet.security.RESTTool'. Το RESTTool ενορχηστρώνει τη χρήση του αντικειμένου και ουσιαστικά κρύβει τις υποκείμενες τεχνολογίες με τις οποίες θα πραγματοποιηθεί η επικοινωνία με τον εξυπηρετητή της βιβλιοθήκης. Με άλλα λόγια, η εφαρμογή διαχείρισης των ψηφιακών εγγράφων της βιβλιοθήκης ασχολείται μονάχα με τις δομές που ορίζει το DSpace (έγγραφα (items), συλλογές (collections) κτλ.). Ενώ κάθε ενέργεια που επιθυμεί να πραγματοποιήσει κάποιος χρήστης περιγράφεται από την τετράδα **ΕΝΕΡΓΕΙΑ - ΑΝΤΙΚΕΙΜΕΝΟ - ΠΑΡΑΜΕΤΡΟΙ - ΔΕΔΟΜΕΝΑ**, τα οποία αποτελούν και την είσοδο του RESTTool.

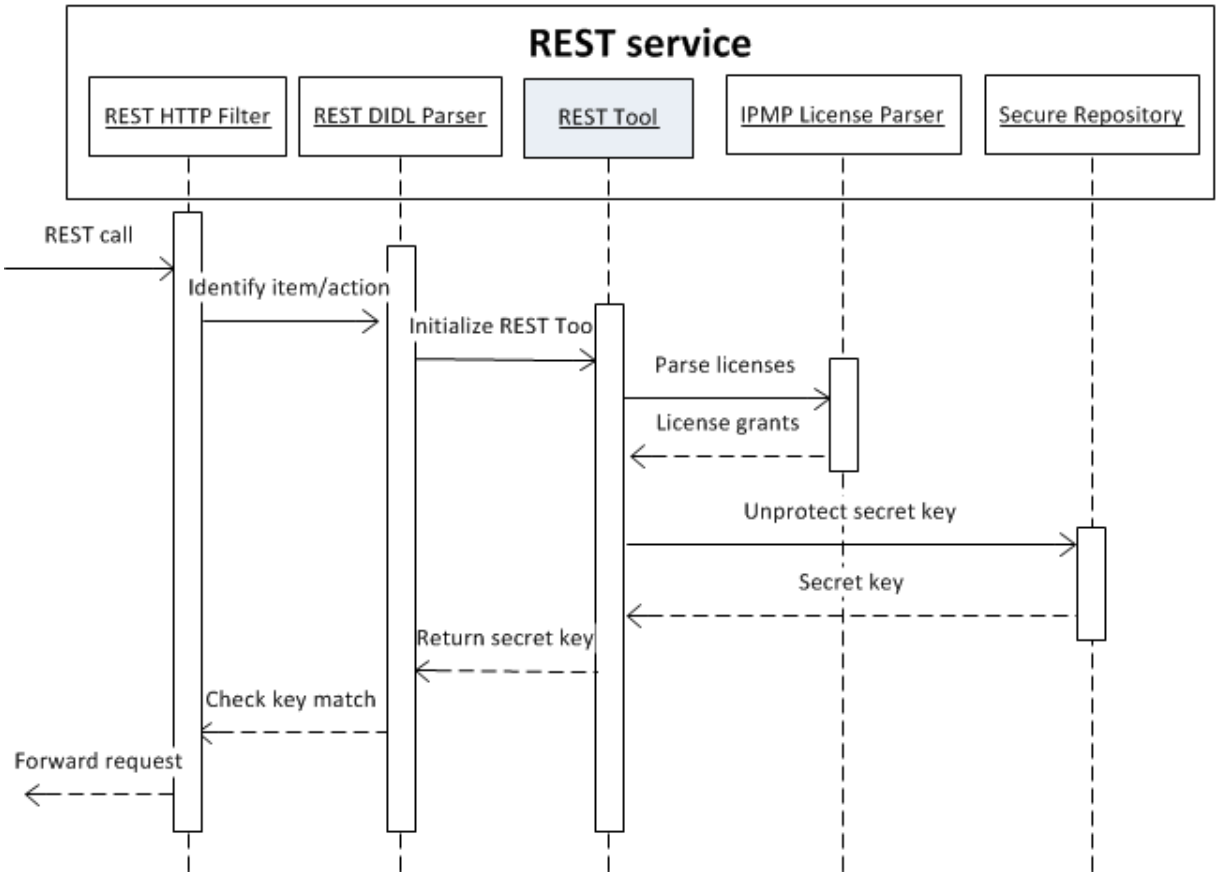
Γυρνώντας στο παράδειγμα, το RESTTool χτίζει και πραγματοποιεί την κλήση προς την υπηρεσία REST της βιβλιοθήκης, έχοντας ως είσοδο την ενέργεια rel-r:issue, το αντικείμενο ITEMS και το νέο έγγραφο στη μορφή που ορίζει το DSPace. Το RESTTool αρχικά επεξεργάζεται την άδεια χρήσης με αναγνωριστικό *ntua-dspace-rest-lic* που προστατεύει το αντικείμενο 'ITEMS' και εντοπίζει σε αυτή τη χορήγηση χρήσης που αντιστοιχεί στην ενέργεια 'rel-r:issue'. Στις γραμμές 10–19 ορίζεται το αντικείμενο ως προστατευμένο περιεχόμενο με κλειδί το οποίο έχει κρυπτογραφηθεί βάσει των χαρακτηριστικών που ορίζονται στη χορήγηση χρήσης. Αποκρυπτογραφώντας το, το RESTTool αποκτά το κρυφό κλειδί το οποίο ουσιαστικά αποδεικνύει πως ο χρήστης είναι κάτοχος των απαιτούμενων χαρακτηριστικών. Τέλος, το URL της μεθόδου χτίζεται αντικαθιστώντας τους αστερίσκους του συν-

δέσμου που ορίζει το ψηφιακό αντικείμενο με τις παραμέτρους που έχει δηλώσει ο χρήστης και το κρυφό κλειδί. Τέλος, συμβουλεύεται τον πίνακα 3 ώστε να αντιστοιχεί την ενέργεια 'rel-r:issue' σε μέθοδο HTTP.



Σχήμα 22: Ροή εργασιών πρόσβασης στην υπηρεσία REST μέσω του RESTTool

Ο εξυπηρετητής λαμβάνοντας την κλήση στο φίλτρο αιτήσεων HTTP, αρχικά λαμβάνει υπόψη το ψηφιακό αντικείμενο που περιγράφει την υπηρεσία REST, εντοπίζει το αντικείμενο στο οποίο αντιστοιχεί το URL της κλήσης, αλλά και την άδεια χρήσης που το προστατεύει. Στη συνέχεια, αναζητεί τη χορήγηση άδειας που αναφέρεται στο αντικείμενο και ταιριάζει με την HTTP μέθοδο της κλήσης. Στο σημείο αυτό, αποκρυπτογραφεί το κρυφό κλειδί, αφού είναι κάτοχος του χαρακτηριστικού system:access_control, και ελέγχει εάν είναι ίδιο με αυτό που έχει σταλθεί. Στην περίπτωση που ταυτίζονται τα κλειδιά, το φίλτρο επιτρέπει την συνέχιση της κλήσης, ενώ σε διαφορετική περίπτωση επιστρέφει σφάλμα.



Σχήμα 23: Ροή εργασιών ελέγχου πρόσβασης υπηρεσίας REST

5.4 Σύνοψη

Οι διαδικτυακές υπηρεσίες αποτελούν τον κύριο τρόπο επικοινωνίας μεταξύ ετερογενών συστημάτων, ως εκ τούτου ο έλεγχος πρόσβασης σε αυτές έχει τύχει εκτενούς έρευνας. Ακρογωνιαίο λίθο στο πεδίο αυτό αποτελεί η σουίτα προτύπων WS-* του οργανισμού OASIS. Οι δομές που ορίζει σε ότι αφορά τις πολιτικές ασφαλείας και η υποστήριξη πολλαπλών διαπιστευτηρίων χρηστών διασφαλίζουν την διαλειοτυργικοτητα τους.

Ωστόσο, ο έλεγχος πρόσβασης στην ανερχόμενη αρχιτεκτονική ανάπτυξης διαδικτυακών υπηρεσιών REST δεν έχει ερευνηθεί εκτενώς. Η αρχιτεκτονική REST δεν εξετάζει ζητήματα ασφάλειας, ενώ παράλληλα η γλώσσα περιγραφής WADL δεν προβλέπει στοιχεία για την συμπερίληψη πολιτικών ασφαλείας που προστατεύουν τις μεθόδους των διεπαφών. Τα παραπάνω οδηγούν σε ανάπτυξη μη διαλειτουργικών λύσεων σε ότι αφορά την υλοποίηση ελέγχου πρόσβασης σε κάθε υπηρεσία ξεχωριστά.

Στο κεφάλαιο αυτό παρουσιάστηκε αρχιτεκτονική που στοχεύει στην υποστήριξη ελέγχου πρόσβασης βάσει χαρακτηριστικών σε διεπαφές REST, χρησιμοποιώντας τις πρότυπες τεχνολογίες του MPEG-21 και τη μέθοδο κρυπτογράφησης CP-ABE. Το κεφάλαιο προτείνει την περιγραφή μιας διεπαφής REST με ένα μοναδικό ψηφιακό αντικείμενο, αλλά και την περιγραφή των πολιτικών προστασίας κάθε μεθόδου της με τη γλώσσα περιγραφής δικαιωμάτων MPEG-21 REL. Στη συνέχεια, το εργαλείο διαχείρισης και προστασίας πνευματικών δικαιωμάτων RESTTool επιβάλει από τη μια τον έλεγχο πρόσβασης στην διεπαφή χρησιμοποιώντας κρυπτογραφημένο κοινόχρηστο κλειδί το οποίο μόνο εξουσιοδοτημένοι χρήστες μπορούν να αποκρυπτογραφήσουν. Ενώ, από την άλλη διευκολύνει την ανάπτυξη ασφαλών εφαρμογών βασισμένων στο πρότυπο MPEG-M, κρύβοντας τόσο τις υποκείμενες τεχνολογίες επικοινωνίας και προστασίας με διεπαφές REST, μοντελοποιώντας τις ως αλληλεπιδράσεις με τμήματα του ψηφιακού αντικειμένου που περιγράφει τη διεπαφή.

Κεφάλαιο 6

Μελέτη περίπτωσης: Ασφαλής διαχείριση προσωπικών αρχείων υγείας

6.1 Εισαγωγή

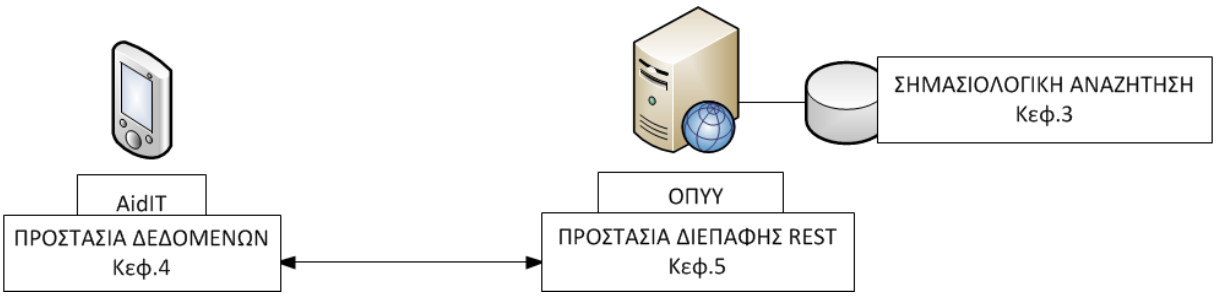
Η εφαρμογή που παρουσιάζεται στο παρόν κεφάλαιο αποτελεί την πρότυπη υλοποίηση ενός συστήματος ασφαλούς διαχείρισης προσωπικών αρχείων υγείας σε ένα δυναμικό περιβάλλον, τόσο ως προς τους χρήστες και τους ρόλους τους, όσο και των συστημάτων που αλληλεπιδρούν στο πλαίσιο σεναρίων ιατρικού ενδιαφέροντος. Η εφαρμογή λαμβάνει υπόψη της τόσο τα προσωπικού χαρακτήρα δεδομένα τα οποία διακινούνται, προστατεύοντας τα ανάλογα, αλλά και την ανάγκη συνεργασίας ετερογενών συστημάτων για την υποστήριξη ουσιαστικών σεναρίων χρήσης.

Κεντρικό ρόλο στην εφαρμογή έχει το πρότυπο HL7 FHIR [6], στο οποίο ορίζονται οι βασικές μονάδες πληροφορίας που ανταλλάσσονται μεταξύ πληροφοριακών συστημάτων υγείας, ενώ το πρότυπο ορίζει διεπαφή REST για την επικοινωνία τους. Παρακάτω παρουσιάζεται το χαρακτηριστικό σενάριο χρήσης το οποίο υποστηρίζεται κατάλληλα αξιοποιώντας τις λύσεις που προτείνει η διατριβή τόσο ως προς την σημασιολογική διαλειτουργικότητα κατά τη χρήση ψηφιακών αντικειμένων, όσο και την ασφαλή διαχείριση τους μέσω

διεπαφής REST.

Ασθενής επισκέπτεται ορθοπεδικό λόγω προβλημάτων που αντιμετωπίζει στη μέση. Ο ιατρός αφού ελέγξει την καρτέλα του ασθενή για παλαιότερες παθήσεις στο ίδιο σημείο και τις σημειώσεις των προηγούμενων ορθοπεδικών, εξετάζει τον ασθενή και κρίνει πως η κατάσταση μπορεί να αντιμετωπιστεί με συντηρητική -μη παρεμβατική- θεραπεία. Για τον λόγο αυτό, ενημερώνει την καρτέλα του ασθενή προσθέτοντας ένα πρόγραμμα φροντίδας με στόχο να χάσει ο ασθενής 5 κιλά, ενώ θέτει ως φαρμακευτική αγωγή την λήψη ενός μυοχαλαρωτικού χαπιού κάθε βράδυ. Ο ασθενής φεύγοντας από το ιατρείο επισκέπτεται φαρμακείο, στο οποίο ο φαρμακοποιός διαβάζοντας την καρτέλα του ασθενή, λαμβάνει υπόψη τις αλλεργίες του και τον προμηθεύει με ένα ασφαλές φάρμακο για αυτόν.

Στο σενάριο δραστηριοποιούνται τρεις χρήστες, ο ασθενής, ο ιατρός και ο φαρμακοποιός γύρω από την βασική δομή της καρτέλας του ασθενή η οποία παρουσιάζεται στην επόμενη παράγραφο. Και οι τρεις, για τις ανάγκες του παραδείγματος, αποτελούν μέλη ενός οργανισμού παροχής υπηρεσιών (ΟΠΥΥ), που για την Ελλάδα θα μπορούσε να είναι ο ΕΟΠΥΥ, και έχουν λάβει τις απαραίτητες πιστοποιήσεις ώστε να μπορούν να χρησιμοποιούν την εφαρμογή AidIT. Με αυτόν τον τρόπο, εξουσιοδοτούνται να διαβάζουν και να ενημερώνουν την καρτέλα του ασθενή επικοινωνώντας με τον εξυπηρετητή του ΟΠΥΥ. Στο παρακάτω σχήμα φαίνεται η αρχιτεκτονική της εφαρμογής μαζί με τις προτεινόμενες λύσεις της διατριβής από τις οποίες υποστηρίζεται.



Σχήμα 24: Αρχιτεκτονική εφαρμογής AidIT

6.2 Το πρότυπο HL7 FHIR

Ο οργανισμός Health Level 7 (HL7) αποτελεί μια διεθνή κοινότητα εμπειρογνωμόνων οι οποίοι δραστηριοποιούνται στην περιοχή της προτυποποίησης των συναλλαγών, της διαχείρισης και διαλειτουργικότητας μεταξύ ιατρικών πληροφοριακών συστημάτων, και έχει παράξει σειρά προτύπων με κυριότερα εξ αυτών τα HL7 v2.x, 3.x και το FHIR.

Το πρότυπο HL7 v2.x, η πρώτη έκδοση του οποίου χρονολογείται το 1989, έχει υιοθετηθεί ευρέως από εθνικούς αλλά και ιδιωτικούς οργανισμούς που δραστηριοποιούνται στο χώρο της υγείας (ασφαλιστικοί φορείς, ιδιωτικές κλινικές κτλ.). Ωστόσο η ευελιξία των μηνυμάτων τα οποία ορίζει οδηγεί σε παρερμηνείες των δομών τους, με αποτέλεσμα πολλές φορές η επικοινωνία μεταξύ δύο συστημάτων τα οποία στηρίζονται στο πρότυπο HL7 v2.x να απαιτεί σημαντική προσπάθεια.

Το πρότυπο HL7 v3.x, η πρώτη έκδοση του οποίου χρονολογείται το 2005, προσπαθεί να λύσει το παραπάνω πρόβλημα ορίζοντας πιο αυστηρές δομές βασισμένες στη γλώσσα XML και το Reference Information Model [111] περιγράφει τα δεδομένα που χρειάζονται σε κλινικά αλλά και διαχειριστικά περιβάλλοντα. Ωστόσο, η πολυπλοκότητα του RIM αποτελεί σημαντική τροχοπέδη στην υιοθέτηση του προτύπου από τα ιατρικά πληροφοριακά συστήματα.

Το πρότυπο HL7 FHIR (Fast Healthcare Interoperability Resources), η πρώτη έκδοση του οποίου χρονολογείται το 2012, προσεγγίζει τα προβλήματα διαλειτουργικότητας μεταξύ ιατρικών πληροφοριακών συστημάτων με διαφορετικό τρόπο, σκοπεύοντας στην γρήγορη ενσωμάτωση του προτύπου. Αρχικά, ορίζει ευέλικτες δομές για την περιγραφή των ιατρικών δεδομένων και προωθεί τη χρήση σύγχρονων τεχνολογιών επικοινωνίας μεταξύ πληροφοριακών συστημάτων ορίζοντας διεπαφή διαδικτυακών υπηρεσιών REST. Οι προσπάθειες προτυποποίησης στο πλαίσιο του HL7 FHIR στοχεύουν στην κάλυψη των πιο κοινών διαδικασιών, ενώ οι πιο πολύπλοκες μπορούν να καλυφθούν με επέκταση των δομών του, κάτι που διευκολύνεται με τη χρήση οντολογικών μοντέλων για την αναπαράσταση λεπτομερών ιατρικών δεδομένων.

Το παρακάτω παράδειγμα παρουσιάζει μια ιατρική συνταγή φαρμάκων με το στοι-

χείο MedicationPrescription, ενώ το πρότυπο ορίζει δομές για όλες τις οντότητες που δραστηριοποιούνται σε υγειονομικά σενάρια, όπως ασθενής, προμηθευτής υγείας, οργανισμός αλλά και πολλές κλινικές διαδικασίες, όπως ιατρικές εξετάσεις, φαρμακευτική αγωγή, περίθαλψη κτλ. Η σχεδίαση ωστόσο των παραπάνω, οδηγείται από την απαίτηση για αυτοτελείς, συμπαγείς, ανεξάρτητα διαχειρίσιμες και συνδυάσιμες δομές, ώστε να είναι σύμφωνες με την αρχιτεκτονική διαδικτυακών υπηρεσιών REST που ορίζει [8], η οποία διευκολύνει την επικοινωνία μεταξύ πληροφοριακών συστημάτων με τρόπο ταιριαστό με τις σύγχρονες τάσεις ανάπτυξης εφαρμογών.

```
<MedicationPrescription xmlns="http://hl7.org/fhir">
  <text> Theophylline 200mg twice a day </text>
    <Medication id="med1">
      <name value="Theophylline 200mg"/>
      <system value="http:/snomed.org"/>
      <code value="66493003"/>
    </Medication>
  <patient>
    <reference value="Patient/1028"/>
    <display value="Peter Patient"/>
  </patient>
  <prescriber>
    <reference value="Practitioner/example"/>
    <display value="Peter Practitioner"/>
  </prescriber>
  <reasonResource>
    <reference value="Condition/f201"/>
    <display value="fever"/>
  </reasonResource>
  <medication>
    <reference value="Medication/example"/>
    <display value="Theophylline 200mg BD"/>
  </medication>
  <dosageInstruction>
    <text value="Take with Food"/>
    <timingSchedule>
      <repeat>
        <frequency value="2"/>
        <duration value="1"/>
        <units value="d"/>
      </repeat>
    </timingSchedule>
    <route>
      <system value="http://snomed.info/sct"/>
      <code value="394899003"/>
      <display value="oral administration of treatment"/>
    </route>
    <doseQuantity>
      <value value="1"/>
      <units value="tablet"/>
    </doseQuantity>
  </dosageInstruction>
</MedicationPrescription>
```

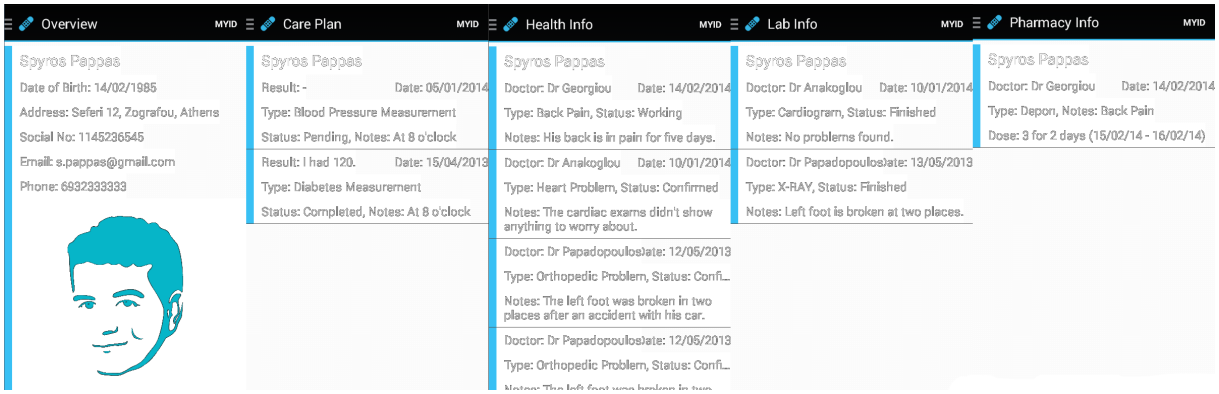
Σχήμα 25: Παράδειγμα συνταγής ιατρού με τη δομή MedicationPrescription του προτύπου HL7 FHIR

[8]http://hl7.org/implement/standards/fhir/http.html

6.3 Η καρτέλα ασθενή

Η καρτέλα του ασθενή, αποτελεί τη βασική δομή γύρω από την οποία συναλλάσσονται οι χρήστες του συστήματος. Η δομή αυτή αναφέρεται σε συγκεντρωτικά δεδομένα που αφορούν τον ασθενή και περιλαμβάνει τα παρακάτω :

- Στοιχεία ασθενή: βασικές πληροφορίες, όπως διεύθυνση κατοικίας, τηλέφωνο επικοινωνίας και φωτογραφία, αλλά και πληροφορίες που αφορούν την υπόσταση του ως ασφαλιζόμενος, π.χ. Αριθμός Μητρώου Κοινωνικής Ασφάλισης.
- Στοιχεία ασθενειών: γενικές πληροφορίες για το ιστορικό υγείας του ασθενή, όπως η ύπαρξη κάποιας αλλεργίας, τραυματισμού ή χρόνιας ασθένειας.
- Ιατρικές εντολές: ιστορικό ιατρικών διαγνώσεων και εργαστηριακών μετρήσεων, όπως διάγνωση για αναιμία ή μέτρηση λευκών αιμοσφαιρίων και αιματοκρίτη.
- Φαρμακευτική αγωγή: ιστορικό φαρμάκων τα οποία λαμβάνει ο ασθενής.
- Πλάνο φροντίδας: καθημερινές ενέργειες που πρέπει να επιτελέσει ο ασθενής και προσωπικοί στόχοι υγείας, όπως λήψη κάποιου χαπιού ή μείωση βάρους κάτω από μια συγκεκριμένη τιμή.



Σχήμα 26: Στιγμιότυπα από την καρτέλα του ασθενή

Η κατηγοριοποίηση των πληροφοριών του ασθενή σε αυτές τις 5 κατηγορίες δίνει τη δυνατότητα για εξατομικευμένη αλληλεπίδραση με την καρτέλα του ασθενή ανάλογα με τον ρόλο του χρήστη που την προσπελάζει. Για παράδειγμα, ο ασθενής έχει κατά κύριο

λόγο δικαιώμα διαβάσματος της καρτέλας του, ενώ ο ιατρός του έχει δικαίωμα να ορίσει την φαρμακευτική του αγωγή ή να αλλάξει το πλάνο φροντίδας του. Στον παρακάτω πίνακα φαίνονται οι δυνατές αλληλεπιδράσεις (C - Create - Δημιουργία, R - Read - Διάβασμα, U - Update - Ενημέρωση, D - Delete - Διαγραφή) των χρηστών με κάθε μια από τις κατηγορίες πληροφοριών :

	Στοιχεία ασθενή				**Στοιχεία ασθενειών**				**Ιατρικές εντολές**				**Φαρ/κή αγωγή**				**Πλάνο φροντίδας**			
Ρόλος	C	R	U	D	C	R	U	D	C	R	U	D	C	R	U	D	C	R	U	D
Ασθενής		X			X	X				X				X	X			X	X	
Ιατρός		X			X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Φαρμακοποιός		X				X				X				X	X					

Πίνακας 4: Διακαιώματα χρήσης της καρτέλας ασθενή

6.4 Ασφαλής πρόσβαση και διαχείριση προσωπικών αρχείων υγείας

Σε αυτή την παράγραφο παρουσιάζονται οι βασικές λειτουργικότητες της εφαρμογής, εξετάζοντας μέρη του σεναρίου που χρήζουν ιδιαίτερης προσοχής. Αρχικά, περιγράφονται οι άδειες χρήσης που ρυθμίζουν τις δυνατές αλληλεπιδράσεις των χρηστών με τα προσωπικά αρχεία υγείας. Ακολουθεί, περιγραφή των τρόπων όπου οι χρήστες της εφαρμογής αλληλεπιδρούν με την καρτέλα του ασθενή ανάλογα με τα δικαιώματα τους. Στη συνέχεια παρουσιάζεται ο μηχανισμός αναζήτησης του συστήματος, ο οποίος χρησιμοποιεί υποδομές σημασιολογικής διαλειτουργικότητας. Τέλος, παρουσιάζεται ο μηχανισμός εξουσιοδότησης χρηστών για προσπέλαση της καρτέλας του ασθενή.

6.4.1 Άδεια χρήσης προσωπικών αρχείων υγείας

Η προστασία των προσωπικών αρχείων υγείας, βασίζεται σε άδειες χρήσης οι οποίες περιγράφουν τους χρήστες που μπορούν να έχουν πρόσβαση σε αυτά. Στην περίπτωση της εφαρμογής, οι άδειες χρήσεις δημιουργούνται αυτόματα και αντικατοπτρίζουν τα δικαιώ-

ματα χρήσης της καρτέλας του ασθενή, όπως αυτά περιγράφηκαν στην προηγούμενη παράγραφο. Ουσιαστικά, η αλληλεπίδραση με κάθε καρτέλα καθορίζεται από την ύπαρξη ή μη χαρακτηριστικού που αναφέρεται στην συγκεκριμένη καρτέλα, π.χ. pharmacy για την καρτέλα φαρμακευτικής αγωγής. Η μοναδικότητα κάθε χαρακτηριστικού, διασφαλίζεται μέσω της χρησιμοποίησης του μοναδικού αναγνωριστικού κάθε χρήστη ως πρόθεμα του χαρακτηριστικού π.χ. JohnDoe:pharmacy. Το συγκεκριμένο χαρακτηριστικό ωστόσο συνδέεται και με το δικαίωμα χρήσης που πρέπει να έχει ο κάτοχος αυτού του χαρακτηριστικού, όπως δικαίωμα δημιουργίας ή διαβάσματος. Τα παραπάνω παρουσιάζονται στο ακόλουθο απόσπασμα άδεια χρήσης η οποία αφορά τα δικαιώματα χρήσης της καρτέλας φαρμακευτικής αγωγής.

```
11   <rel-r:inventory>
20         <rel-r:forAll licensePartId="own-policy">
27           <rel-r:propertyPossessor>
28         <rel-sx:propertyUri definition="JohnDoeΦΑΡΜΑΚΑ:"/>
32       </rel-r:propertyPossessor>
33     </rel-r:forAll>
20         <rel-r:forAll licensePartId="break-glass-policy">
27           <rel-r:propertyPossessor>
28         <rel-sx:propertyUri definition="ΕΟΠΤΤ:break\_glass"/>
32       </rel-r:propertyPossessor>
33     </rel-r:forAll>
20         <rel-r:forAll licensePartId="pharmacist-policy">
21       <rel-r:propertyPossessor>
22         <rel-sx:propertyUri definition="JohnDoeΦΑΡΜΑΚΑ:"/>
26       </rel-r:propertyPossessor>
27           <rel-r:propertyPossessor>
28         <rel-sx:propertyUri definition="ΕΟΠΤΤΦΑΡΜΑΚΟΠΟΙΟΣ:"/>
32       </rel-r:propertyPossessor>
33     </rel-r:forAll>
20         <rel-r:forAll licensePartId="doctor-policy">
21       <rel-r:propertyPossessor>
22         <rel-sx:propertyUri definition="JohnDoeΦΑΡΜΑΚΑ:"/>
26       </rel-r:propertyPossessor>
27           <rel-r:propertyPossessor>
28         <rel-sx:propertyUri definition="ΕΟΠΤΤΙΑΤΡΟΣ:"/>
32       </rel-r:propertyPossessor>
33     </rel-r:forAll>
34   </rel-r:inventory>
```

Σχήμα 27: Πολιτικές προστασίας διαδικτυακής υπηρεσίας HL7 FHIR (απόσπασμα)

Τα δικαιώματα κάθε χρήστη δένονται με τις πολιτικές στο ακόλουθο απόσπασμα άδεια χρήσης, η οποία έχει ιδιαίτερο ενδιαφέρον, διότι ο κάθε χρήστης έχει διαφορετικά δικαιώματα ως προς τις λειτουργίες που μπορεί να πραγματοποιήσει.

```
01 <rel-r:License licenseId="john-doe-pharmacy-lic">
02   <rel-r:issuer>
03     <dsig:Signature>
04       <dsig:SignatureValue>...</dsig:SignatureValue>
06       <dsig:KeyName>John Doe</dsig:KeyName>
09     </dsig:Signature>
10   </rel-r:issuer>
     <rel-r:inventory>
     ...
34   </rel-r:inventory>
     <rel-r:grantGroup>
36     <rel-r:forAll licensePartIdRef="own-policy" varName="x"/>
36     <rel-r:forAll licensePartIdRef="doctor-policy" varName="y"/>
           <rel-r:forAll licensePartIdRef="pharmacist-policy" varName="z"/>
           <rel-r:forAll licensePartIdRef="break-glass-policy" varName="w"/>
<!-- READ --> <!-- SEARCH -->
35     <rel-r:grant>
37       <rel-r:allPrincipals>
           <rel-r:principal varRef="x"/>
           <rel-r:principal varRef="y"/>
           <rel-r:principal varRef="z"/>
         </rel-r:allPrincipals>
38       <rel-r:play/> <!-- <rel-r:enlist/> -->
10     <rel-m1x:protectedResource>
11       <rel-r:digitalResource>
12         <rel-r:secureIndirect URI="#ITEMS"/>
13       </rel-r:digitalResource>
14           <xenc:encryptedKey MimeType="">
16           <xenc:CipherValue>ABC...</xenc:CipherValue
18       </xenc:encryptedKey>
19     </rel-m1x:protectedResource>
42     </rel-r:grant>

<!-- CREATE --> <!-- UPDATE --> <!-- DELETE -->
35     <rel-r:grant>
         <rel-r:principal varRef="y"/>
38       <rel-r:issue/> <!-- <rel-mx:modify/> --> <!-- <rel-r:revoke/> -->
10     <rel-m1x:protectedResource>
11       <rel-r:digitalResource>
12         <rel-r:secureIndirect URI="#ITEMS"/>
13       </rel-r:digitalResource>
14           <xenc:encryptedKey MimeType="">
16           <xenc:CipherValue>ABC...</xenc:CipherValue
18       </xenc:encryptedKey>
19     </rel-m1x:protectedResource>
42     </rel-r:grant>

<!-- BREAK GLASS READ -->
35     <rel-r:grant>
         <rel-r:principal varRef="w"/>
38       <rel-r:play/>
10     <rel-m1x:protectedResource>
11       <rel-r:digitalResource>
12         <rel-r:secureIndirect URI="#ITEMS"/>
13       </rel-r:digitalResource>
14           <xenc:encryptedKey MimeType="">
16           <xenc:CipherValue>ABC...</xenc:CipherValue
18       </xenc:encryptedKey>
19     </rel-m1x:protectedResource>
42     </rel-r:grant>
     </rel-r:grantGroup>
51 </rel-r:License>
```

Σχήμα 28: Άδεια χρήσης που ρυθμίζει την πρόσβαση στην φαρμακευτική αγωγή του ασθενή (απόσπασμα)

Στην άδεια χρήσης του παραδείγματος πέρα από το χαρακτηριστικό pharmacy, το οποίο πιστοποιεί ο ασθενής κατά βούληση, γίνεται αυτόματα χρήση και των χαρακτηριστικών του συστήματος, system:access_control, το οποίο χρησιμοποιείται από τον εξυπηρετητή της υπηρεσίας REST για να πραγματοποιήσει έλεγχο πρόσβασης στη διεπαφή, αλλά και του system:break_glass το οποίο χρησιμοποιείται σε περιπτώσεις όπου ο χρήστης είναι φυσικά αδύνατο να δώσει εξουσιοδότηση πρόσβασης στα προσωπικά αρχεία υγείας του. Τότε, ο εξυπηρετητής καταγράφει (audit) τις ενέργειες που πραγματοποιούνται με βάση το συγκεκριμένο χαρακτηριστικό, το οποίο είναι δυνατό λόγο της ύπαρξης ιδιαίτερων χορηγήσεων χρήσης στην άδεια. Το χαρακτηριστικό αυτό είναι βεβαίως εξαιρετικά κρίσιμο και δίνεται για μικρό χρονικό διάστημα μονάχα σε εξουσιοδοτημένο προσωπικό, το οποίο μπορεί και να διωχθεί νομικά σε ενδεχόμενη κακή χρήση του.

6.4.2 Διαχείριση και προστασία προσωπικών αρχείων υγείας

Στην εφαρμογή AidIT, η διαχείριση των προσωπικών αρχείων υγείας ενός ασθενή δεν αποτελεί ατομική διαδικασία αλλά συνεργατική. Παραδείγματος χάρη, ο ιατρός ενός ασθενή μπορεί να προσθέσει μια νέα διάγνωση ή να αλλάξει τη φαρμακευτική αγωγή που λαμβάνει ο ασθενής. Χρησιμοποιώντας τις δομές δεδομένων και την υπηρεσία REST που ορίζει το πρότυπο HL7 FHIR είναι δυνατή η επικοινωνία διαφορετικών συστημάτων όπως νοσοκομεία, φαρμακεία και ιδιώτες ιατροί. Παρακάτω παρουσιάζονται τα βήματα με τα οποία εκτελείται το προαναφερθέν παράδειγμα.

Αρχικά, ο ασθενής με την έγγραφή του στο σύστημα αποκτά το δικαίωμα χρήσης της εφαρμογής AidIT, μέσω της οποίας διαχειρίζεται τα προσωπικά του αρχεία υγείας. Μετά τον ορισμό της άδειας χρήσης της καρτέλας του ασθενή, όπως αυτή παρουσιάστηκε στην προηγούμενη παράγραφο, η εφαρμογή AidIT χρησιμοποιώντας τις στοιχειώδεις υπηρεσίες του MPEG-M (StoreLicense και StoreContent) δηλώνει στον εξυπηρετητή του ΟΠΥΥ τις διευθύνσεις εισόδου για τα ιατρικά δεδομένα του χρήστη. Το παρακάτω ψηφιακό αντικείμενο αναπαριστά την προστατευμένη διεπαφή REST την οποία θα ενεργοποιήσει ο εξυπηρετητής μετά τη λήψη του.

```
01 <didl:Item>
02   <didl:Descriptor>
03     <didl:Statement>
04       <dii:Identifier>
05              john-doe-aidit-rest
06       </dii:Identifier>
07     </didl:Statement>
08   </didl:Descriptor>
09   <didl:Component>
10     <ipmpdidl:Resource id="MEDICATIONS"
11 ref="https://aidit.opyy.gov.gr/rest/123456789012/medications/*">
12       <ipmpinfo:Info>
13         <ipmpinfo:IPMPInfoDescriptor>
14           <ipmpinfo:Tool>
15             <ipmpinfo:ToolBaseDescription>
16               <ipmpinfo:IPMPToolID>
17                     gr.ntua.icbnet.security.RESTTool
18               </ipmpinfo:IPMPToolID>
19             </ipmpinfo:ToolBaseDescription>
20             <ipmpinfo:InitializationSettings>
22               <ipmpmsg:ControlPointAddress>
23                   <ID>08</ID> <!--CONTROL_POINT_BEFORE_TRANSFERRING-->
24               </ipmpmsg:ControlPointAddress>
26             </ipmpinfo:InitializationSettings>
27           </ipmpinfo:Tool>
42           <ipmpinfo:RightsDescriptor>
43             <ipmpinfo:LicenseReference>
44               john-doe-aidit-rest-lic
45             </ipmpinfo:LicenseReference>
46           </ipmpinfo:RightsDescriptor>
47         </ipmpinfo:IPMPInfoDescriptor>
48       </ipmpinfo:Info>
49     </ipmpdidl:Resource>
50   </didl:Component>
51 </didl:Item>
```

Σχήμα 29: Αναπαράσταση διεπαφής REST για πρόσβαση στα προσωπικά αρχεία υγείας ασθενή με ψηφιακό αντικείμενο (απόσπασμα)

Το ψηφιακό αντικείμενο της υπηρεσίας REST συνοδευόμενο με μια μοναδική άδεια χρήσης, προστατεύει την πρόσβαση στην υπηρεσία REST. Πιο συγκεκριμένα, η γραμμή 23 ορίζει την ενεργοποίηση του RESTTool το οποίο και θα πραγματοποιήσει την επικοινωνία με την διεπαφή.

Επιστρέφοντας στο παράδειγμα, ο ιατρός χρησιμοποιώντας την εφαρμογή θα προσθέσει στην ενεργό φαρμακευτική αγωγή του ασθενή ένα νέο φάρμακο. Δημιουργώντας τη δομή MedicationsPrescription του HL7 FHIR που περιγράφει τις συνταγές φαρμάκων, η εφαρμογή θα δημιουργήσει ένα ψηφιακό αντικείμενο το οποίο θα έχει ως προστατευμένο περιεχόμενο το HL7 μήνυμα με την ιατρική συνταγή. Όπως φαίνεται και στο παρακάτω σχήμα, το περιεχόμενο του ψηφιακού αντικείμενου προστατεύεται από την άδεια χρήσης που έχει ορίσει ο ασθενής και η οποία επιβάλλεται από το ABETool, το οποίο ενορχηστρώνει την αποκρυπτογράφηση των δεδομένων πριν το διάβασμα τους. Η προστασία των αρ-

χείων υγείας μέσω κρυπτογράφησης διασφαλίζει τα δεδομένα από πιθανό ρήγμα στην ασφάλεια του εξυπηρετητή του ΟΠΥΥ και ενδεχόμενη κακόβουλη χρήση τους. Τέλος, στο πεδίο των συσχετίσεων με άλλα ψηφιακά αντικείμενα, προστίθεται πληροφορίες για το φάρμακο και την αιτία συνταγογράφησης. Αυτές, δεν είναι κρυπτογραφημένες ώστε να καταστήσουν δυνατή την υποστήριξη υπηρεσιών αναζήτησης.

```
01 <didl:Item>
02   <didl:Descriptor>
03     <didl:Statement>
04       <dii:Identifier>
05              john-doe-medication-prescription-234
06       </dii:Identifier>
07     </didl:Statement>
08   </didl:Descriptor>
02   <didl:Descriptor>
03     <didl:Statement>
04       <dii:Relationships mimeType="application/rdf+xml">
05         <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">
06           <DigitalItem rdf:about="john-doe-medication-prescription-234">
07             <reasonResource rdf:resource="http://snomed.info/sct/249921008">
08         <!-- Clinical finding / Finding of body region / Finding of back / Stiff back -->
09             <medication rdf:resource="http://www.opyy.org/muscle-relaxant/12345">
10           </DigitalItem>
11          </rdf:RDF>
06       </dii:Relationships>
07     </didl:Statement>
08   </didl:Descriptor>
09   <didl:Component>
10     <ipmpdidl:Resource id="MEDICATIONS">
12       <ipmpinfo:Info>
13         <ipmpinfo:IPMPInfoDescriptor>
14           <ipmpinfo:Tool>
15             <ipmpinfo:ToolBaseDescription>
16               <ipmpinfo:IPMPToolID>
17                      gr.ntua.icbnet.security.ABETool
18               </ipmpinfo:IPMPToolID>
19             </ipmpinfo:ToolBaseDescription>
20             <ipmpinfo:InitializationSettings>
22               <ipmpmsg:ControlPointAddress>
23                 <ID>07</ID> <!--CONTROL_POINT_BEFORE_PLAYBACK-->
24               </ipmpmsg:ControlPointAddress>
26             </ipmpinfo:InitializationSettings>
27           </ipmpinfo:Tool>
42           <ipmpinfo:RightsDescriptor>
43             <ipmpinfo:LicenseReference>
44               john-doe-aidit-rest-lic
45             </ipmpinfo:LicenseReference>
46           </ipmpinfo:RightsDescriptor>
47         </ipmpinfo:IPMPInfoDescriptor>
48       </ipmpinfo:Info>
         <ipmpinfo:Contents>
         ...
         </ipmpinfo:Contents>
49     </ipmpdidl:Resource>
50   </didl:Component>
51 </didl:Item>
```

Σχήμα 30: Ψηφιακό αντικείμενο με με κρυπτογραφημένη συνταγή ιατρού (HL7 FHIR MedicationPrescription) (απόσπασμα)

6.4.3 Αναζήτηση στοιχείων της καρτέλας του ασθενή

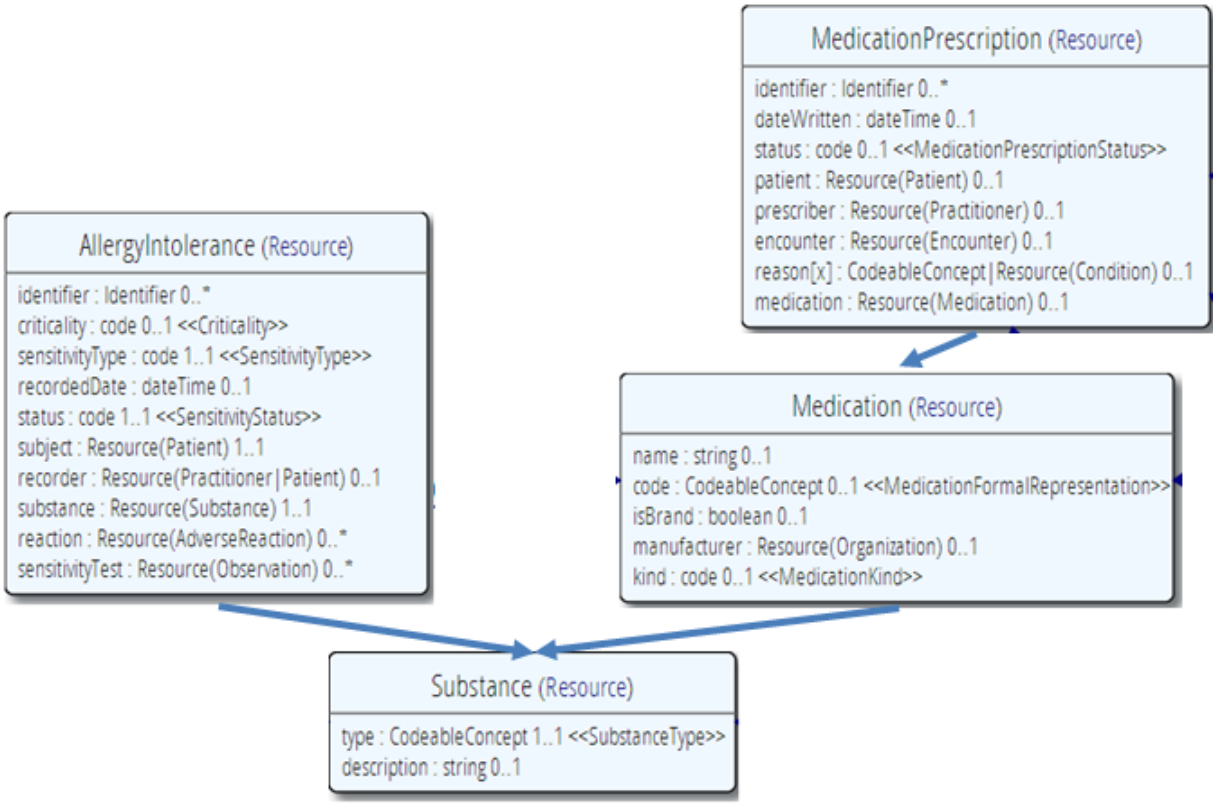
Από τη στιγμή που τα ιατρικά δεδομένα των ασθενών, τα οποία διαμοιράζονται μέσω του εξυπηρετητή του ΟΠΥΥ είναι κρυπτογραφημένα, δεν θα ήταν δυνατό να προσφέρονται υπηρεσίες αναζήτησης για αυτά. Ωστόσο, η εφαρμογή AidIT εκμεταλλεύεται τις δομές και τους μηχανισμούς που προσφέρουν τα ψηφιακά αντικείμενα, ώστε χωρίς να βλάψει την ασφάλεια των δεδομένων και την ιδιωτικότητα των ασθενών, να συμπεριλαμβάνει σε αυτά πληροφορίες που μπορούν να χρησιμοποιηθούν για την διευκόλυνση της περιήγησης στα ιατρικά δεδομένα των ασθενών.

Για παράδειγμα, έστω ασθενής ο οποίος επισκέπτεται φαρμακείο για να προμηθευτεί την φαρμακευτική αγωγή που του έχει συνταγογραφήσει ο ιατρός του. Λαμβάνοντας υπόψη πως η συνταγογράφηση φαρμάκου γίνεται βάση δραστικής ουσίας, ο φαρμακοποιός είναι απαραίτητο να επιλέξει φάρμακο που περιέχει τη δραστική ουσία, αλλά θα πρέπει να διασφαλίσει πως ο ασθενής δεν έχει αλλεργία σε κάποια από τις υπόλοιπες ουσίες του φαρμάκου. Για αυτό, θα πρέπει προτού προμηθεύσει τον ασθενή με κάποιο φάρμακο, να αναζητήσει στα προσωπικά αρχεία υγείας του πιθανή αλλεργία. Στο παρακάτω σχήμα παρουσιάζεται η συσχέτιση που υπάρχει μεταξύ συνταγογραφούμενων φαρμάκων και αλλεργιών, η οποία γίνεται μέσω της δραστικής ουσίας.

Η αναζήτηση για αλλεργία του ασθενή σε κάποιο φάρμακο μεταφράζεται σε μια αίτηση SPARQL (σχήμα 32), την οποία ο εξυπηρετητής μπορεί να εκτελέσει πάνω στα μεταδεδομένα που έχει συλλέξει από τις συσχετίσεις των υπαρχόντων ψηφιακών αντικειμένων (φάρμακα, δραστική ουσία, αλλεργίες).

Η επιτυχής λειτουργία της αναζήτησης ωστόσο στηρίζεται στη διασύνδεση του συστήματος ελέγχου προμηθειών του φαρμακείου με την εφαρμογή AidIT και το μοντέλο πληροφορίας του ΟΠΥΥ. Πιο συγκεκριμένα, η κατασκευάστρια εταιρία εξέδωσε λεξικό διαλειτουργικότητας, απόσπασμα του οποίου ακολουθεί, και το οποίο περιέχει σημασιολογικές συσχετίσεις μεταξύ των οντολογιών του λογισμικού και του ΟΠΥΥ σχετικά με το ιατροφαρμακευτικό υλικό.

Το λεξικό χρησιμοποιείται τόσο στο πλαίσιο της αναζήτησης, όσο και της παρουσίασης των αποτελεσμάτων της. Παραδείγματος χάρη, όταν ο φαρμακοποιός αναζητήσει



Σχήμα 31: Συσχέτιση ψηφιακών αντικειμένων αλλεργιών και συνταγογραφούμενων φαρμάκων [6]

```
SELECT ?id
WHERE
{
?a rdf:isA eopyy:AllergyIntolerence .
?a rdf:id ?id .
?a oppy:hasSubstance ?b .
?c opyy:hasSubstance ?b .
?c opyy:hasBarcode ABCDEF .
}
```

Σχήμα 32: Αίτηση SPARQL για εύρεση υφιστάμενων αλλεργιών ασθενή σε κάποιο φάρμακο

```
opyy:hasKAK equivalentProperty pharm:producerCanonicalName
opyy:hasATCCode equivalentProperty pharm:substanceCode
opyy:description equivalentProperty pharm:desc
opyy:hasBarcode equivalentProperty pharm:barcode
```

Σχήμα 33: Λεξικό διαλειτουργικότητας σημασιολογικών μοντέλων ΟΠΠΥ-λογισμικού προμηθειών φαρμάκων

φάρμακο με την δραστική ουσία που έχει συνταγογραφήσει ο ιατρός, θα χρησιμοποιήσει τη διμερή συσχέτιση που αφορά τον κωδικό Ανατομικής Θεραπευτικής Χημικής ουσίας (Anatomical Therapeutic Chemical - ATC) ώστε να σχηματίσει το αίτημα προς το λογισμικό

προμηθειών. Ενώ, στη συνέχεια θα χρησιμοποιήσει τη συσχέτιση που αφορά τον γραμμωτό κώδικα (barcode) του φαρμάκου ώστε να κάνει την αναζήτηση για πιθανή ύπαρξη αλλεργίας σε άλλη ουσία του φαρμάκου.

6.4.4 Εξουσιοδότηση για πρόσβαση στην καρτέλα του ασθενή

Η πρόσβαση στην καρτέλα του ασθενή ελέγχεται από την ύπαρξη ή μη των χαρακτηριστικών που έχει ορίσει ο χρήστης στην άδεια χρήσης της καρτέλας. Ωστόσο, πέρα από τα χαρακτηριστικά που πιστοποιεί ο ΟΠΥΥ, όπως αυτό του ιατρού ή του φαρμακοποιού, για την πρόσβαση στην καρτέλα του ασθενή απαιτείται και η ρητή έγκριση του ασθενή. Η τελευταία έχει τη μορφή άδειας χρήσης, η οποία πιστοποιεί πως κάποιος χρήστης κατέχει το χαρακτηριστικό που καθορίζει την πρόσβαση σε κάποια καρτέλα. Με αυτή είναι δυνατό ο χρήστης να ανανεώσει το κλειδί αποκρυπτογράφησης του και να έχεις συνεπώς πρόσβαση στις υπηρεσίες του ΟΠΥΥ αλλά και αλληλεπίδρασης με τα ιατρικά δεδομένα του ασθενή.

Στην εφαρμογή AidIT η παραπάνω διαδικασία πραγματοποιείται με τη χρήση κωδικών QR, οι οποίοι οπτικοποιούν την ψηφιακή μορφή της άδειας χρήσης, ενώ η σάρωση τους ουσιαστικά ισοδυναμεί με την μεταφορά τους. Η πλήρης διαδικασία εξουσιοδότησης παρόλα αυτά εκκινείται με την επίδειξη από τον χρήστη της άδειας χρήσης που έχει εκδώσει ο ΟΠΥΥ και πιστοποιεί τον ρόλο του. Και σε αυτή την περίπτωση η άδεια χρήσης οπτικοποιείται με τη χρήση κωδικού QR, ο οποίος αφού σαρωθεί χρησιμοποιείται ώστε να καθορίσει τον χρήστη που θα αποκτήσει πρόσβαση στις καρτέλες του. Στο παρακάτω σχήμα εμφανίζεται στιγμιότυπο της οπτικοποίησης της άδειας χρήσης ενός ιατρού.

```
<rel-r:License>
  <rel-r:issuer>
    <dsig:Signature>
      <dsig:SignatureValue>...</dsig:SignatureValue>
      <dsig:KeyInfo>
        <dsig:KeyName>ΕΟΠΥΥ</dsig:KeyName>
        <dsig:KeyValue>...</dsig:KeyValue>
      </dsig:KeyInfo>
    </dsig:Signature>
  </rel-r:issuer>
  <rel-r:inventory>
    <rel-r:keyHolder licensePartId="doctor">
      <dsig:KeyInfo>
        <dsig:KeyName>ΚΩΣΤΑΣ ΠΕΤΡΟΠΟΥΛΟΣ</dsig:KeyName>
        <dsig:KeyValue>...</dsig:KeyValue>
      </dsig:KeyInfo>
    </rel-r:keyHolder>
  </rel-r:inventory>
  <rel-r:grant>
    <rel-r:principal licensePartIdRef="doctor"/>
    <rel-r:possessesProperty/>
    <rel-sx:propertyUri definition="ΕΟΠΥΥ:ΙΑΤΡΟΣ"/>
  </rel-r:grant>
</rel-r:License>
```

Σχήμα 34: Οπτικοποίηση πιστοποιητικού ιατρού με κωδικό QR

6.5 Σύνοψη

Κεντρικό ρόλο στην παροχή υπηρεσιών υγείας κατέχει η ανταλλαγή ιατρικών δεδομένων μεταξύ των φορέων υγείας. Ωστόσο, η ετερογένεια των εμπλεκόμενων χρηστών αλλά και των κλινικών δεδομένων, μετατρέπουν την ανταλλαγή τους σε ένα πολύπλοκο εγχείρημα. Η έλλειψη συνεργασίας μεταξύ των παρόχων υγείας μπορεί να οδηγήσει σε αναποτελεσματικές θεραπευτικές αγωγές και να αυξήσει το κόστος υγειονομικής περίθαλψης θέτοντας σημαντικές επιβαρύνσεις στις εθνικές οικονομίες σε όλον τον κόσμο. Όπως φαίνεται στο [112], η επίτευξη της διαλειτουργικότητας μεταξύ ιατρικών πληροφοριακών συστημάτων υγειονομικής περίθαλψης μπορεί να περιορίσει σημαντικά τα κόστη της, ενώ στις Η.Π.Α. το όφελος εκτιμάται περίπου στα 80 δισεκατομμύρια δολάρια.

Η εφαρμογή AidIT έχει ως στόχο να ενισχύσει την αλληλεπίδραση μεταξύ επαγγελματιών υγείας και ασθενών, παρέχοντάς τους ένα διαδραστικό εργαλείο για την ασφαλή και αποτελεσματική ανταλλαγή πληροφοριών για την υγεία τους. Η εφαρμογή αξιοποιεί το ανερχόμενο πρότυπο ηλεκτρονικής υγείας HL7 FHIR, προκειμένου να στηρίξει τη συνδεσιμότητα μεταξύ των παρόχων υγειονομικής περίθαλψης, καθώς και να κάνει διαθέσιμο στους ασθενείς το πλήρες ιατρικό ιστορικό τους, τόσο στο σημείο παροχής ιατρικών υπηρεσιών όσο και στο σπίτι. Αυτό επιτρέπει στους ασθενείς να ελέγχουν και να παρακολουθούν την υγεία τους, ενισχύοντας παράλληλα τους επαγγελματίες της υγείας για

παροχή περισσότερο εξατομικευμένων υπηρεσιών και τη μείωση των ιατρικών σφαλμάτων.

Για να πετύχει τα παραπάνω, η εφαρμογή AidIT αξιοποιεί τις λύσεις που προτείνει η διατριβή ώστε να προσφέρει ασφαλή διαχείριση σε σημασιολογικά συνδεδεμένα ιατρικά δεδομένα. Τα τελευταία αναπαριστώνται ως ψηφιακά αντικείμενα, κάτι που από τη μια διευκολύνει τη δημιουργία υγειονομικών εφαρμογών που θα συνδυάζουν δεδομένα προερχόμενα από διάφορες πηγές, όπως παραδείγματος χάρη ένδυτες συσκευές. Από την άλλη τα ψηφιακά αντικείμενα προσφέρουν στις εφαρμογές διαφανείς διεπαφές για την αλληλεπίδραση μαζί τους, καθορίζοντας τόσο τους τρόπους όσο και τις τεχνολογίες που απαιτούν για την κατανάλωση τους.

Από την πλευρά της ασφαλούς ανταλλαγής των ευαίσθητων ιατρικών δεδομένων, η συμπερίληψη στα ψηφιακά αντικείμενα των κανόνων χρήσης τους, καθιστά δυνατό τον ευέλικτο καθορισμό των εξουσιοδοτημένων φορέων που έχουν πρόσβαση στα ιατρικά δεδομένα των χρηστών. Οι άδειες χρήσεις, που έχουν δηλωθεί με τη γλώσσα περιγραφής δικαιωμάτων, χρησιμοποιούνται τόσο για την προστασία της διεπαφής REST που προδιαγράφει το πρότυπο HL7 FHIR, αλλά και για την κρυπτογράφηση των ιατρικών δεδομένων με βάσει τα χαρακτηριστικά που καλούνται να πληρούν όσοι επιθυμούν να αποκτήσουν πρόσβαση σε αυτά. Με αυτόν τον τρόπο, τα ιατρικά δεδομένα είναι διασφαλισμένα ακόμα και σε πιθανή παραβίαση του εξυπηρετητή της εφαρμογής, στον οποίο και βρίσκονται αποθηκευμένα, αφού εξ αρχής ο εξυπηρετητής θεωρείται ημιέμπιστος. Επιπρόσθετα, σε περιπτώσεις έκτακτης ανάγκης η εφαρμογή φροντίζει να άρει τους περιορισμούς ασφαλείας, προσφέροντας πρόσβαση στα ιατρικά δεδομένα των ασθενών, καταγράφοντας παράλληλα στο παρασκήνιο τις μη ρητά εξουσιοδοτημένες ενέργειες.

Τέλος, η εφαρμογή προσφέρει εξελιγμένες υπηρεσίες αναζήτησης στα ιατρικά δεδομένα των ασθενών, βασιζόμενη στη διασύνδεση τους αλλά και το σύστημα σημασιολογικής διαλειτουργικότητας, το οποίο προσφέρει την κατάλληλη υποδομή για την ενσωμάτωση ιατρικών δεδομένων που προέρχονται από διαφορετικούς οργανισμούς που χρησιμοποιούν ετερογενή λεξιλόγια για την περιγραφή των ασθενειών.

Κεφάλαιο 7

Συμπεράσματα - Προτάσεις για μελλοντική έρευνα

7.1 Συμπεράσματα

Η παρούσα διδακτορική διατριβή επικεντρώνεται στην υποστήριξη της διαλειτουργικότητας στις συναλλαγές μεταξύ κατανεμημένων συστημάτων που χαρακτηρίζονται από ετερογένεια. Πάνω σε αυτό το πλαίσιο, εξετάζει το ζήτημα της σημασιολογικής διαλειτουργικότητας των δεδομένων που ανταλλάσσονται μεταξύ των συστημάτων, αλλά και το ζήτημα της διαλειτουργικότητας των πολιτικών προστασίας τους. Η ενίσχυση της πρώτης είναι αναγκαία για την δημιουργία εξελιγμένων και πρωτοποριακών πληροφοριοκεντρικών εφαρμογών, ενώ η ανάπτυξη των τεχνολογιών που υποστηρίζουν τη δεύτερη είναι απαραίτητη για την ευρεία κινητοποίηση της συνεργασίας μεταξύ συστημάτων τα οποία βρίσκονται υπό την εποπτεία διαφορετικών οργανισμών. Η διατριβή προτείνει λύσεις στα παραπάνω ζητήματα, τα συμπεράσματα της οποίας συνοψίζονται παρακάτω :

- Συσχέτιση ψηφιακών αντικειμένων. Η διαρκής αλληλεπίδραση μεταξύ του πραγματικού και του ψηφιακού κόσμου, απαιτεί τόσο την ύπαρξη συνεκτικών και καθολικών τρόπων για την ψηφιακή αναπαράσταση αντικειμένων του πραγματικού κόσμου, αλλά και την ανάπτυξη σημασιολογικών εργαλείων βάσει των οποίων μπορούν να δηλωθούν οι σχέσεις μεταξύ τους με ακρίβεια. Το πρότυπο MPEG-21 καθιστά

δυνατή την ψηφιακή αναπαράσταση αντικειμένων, ωστόσο οι μηχανισμοί συσχέτισης μεταξύ τους είναι ελλείπείς. Έτσι, παρουσιάστηκαν οι επικρατέστεροι μηχανισμοί συσχέτισης ψηφιακών εγγράφων του διαδικτύου και υπογραμμίστηκαν οι περιορισμοί τους. Δόθηκε έμφαση στη συσχέτιση μεταξύ ψηφιακών αντικειμένων του MPEG-21 και παρουσιάστηκε ένας ευέλικτος μηχανισμός που υποστηρίζει την συσχέτιση τους εκμεταλλευόμενος τις τεχνολογίες του σημασιολογικού διαδικτύου για τη δημιουργία σημασιολογικά πλούσιων περιγραφών για αυτά. Ο μηχανισμός αυτός ορίζει οντολογικό μοντέλο το οποίο δρα ως βάση για τις περιγραφές των συσχετίσεων, ενώ προτάθηκε και τελικώς ενσωματώθηκε ως επέκταση στο τρίτο μέρος του πρότυπου MPEG-21 (Digital Item Identification).

- Σημασιολογική διαλειτουργικότητα. Κεντρική θέση σε πληροφοριοκεντρικές εφαρμογές έχει το μοντέλο πληροφορίας πάνω στο οποίο λειτουργούν, από το οποίο άλλωστε πηγάζουν πολλά από τα πλεονέκτημα που έχουν έναντι άλλων παρόμοιων εφαρμογών. Ωστόσο, η ετερογένεια που εμφανίζεται εδώ δυσχεραίνει τη διασύνδεση τους με άλλες εφαρμογές με στόχο τη δημιουργία συναρπαστικών νέων εφαρμογών προς όφελος των χρηστών. Η άνθηση των τεχνολογιών του σημασιολογικού διαδικτύου και των οντολογιών προσφέρει τη βάση για τη συντακτική διαλειτουργικότητα των παραπάνω μοντέλων, αλλά η σημασιολογική διαλειτουργικότητα εξακολουθεί να αποτελεί εμπόδιο. Για την προώθηση της σημασιολογικής διαλειτουργικότητας, η διατριβή προτείνει σύστημα που την υποστηρίζει βασιζόμενο στις δομή των λεξικών σημασιολογικής διαλειτουργικότητας, τα οποία δρουν ως σημασιολογικές γέφυρες μεταξύ εννοιών διαφορετικών οντολογιών και βάσει αυτών παρέχονται σημασιολογικές υπηρεσίες χρήσιμες σε κάθε είδους πληροφοριοκεντρικές εφαρμογές.

- Ασφαλής διαχείριση ψηφιακών αντικειμένων. Τα ζητήματα ασφάλειας που εμφανίζονται σε σενάρια ανταλλαγής περιεχομένου μεταξύ ετερογενών κατανεμημένων συστημάτων, στα οποία οι παραγωγοί περιεχομένου από τη μια επιθυμούν την προστασία του, ενώ από την άλλη θέλουν να περιορίσουν τις επιπτώσεις που έχουν οι πολιτικές ασφαλείας στην διάδοση του, απαιτούν την δημιουργία λύσεων που να βασίζονται πάνω σε πρότυπα ώστε να είναι ευρεία η ενσωμάτωση τους. Έτσι, περιγράφηκαν υπάρχοντα συστήματα ελέγχου πρόσβασης και ασφαλούς ανταλλαγής περιε-

χομένου σε κατανεμημένα και ετερογενή περιβάλλοντα και αναλύθηκαν οι περιορισμοί τους. Παρουσιάστηκε η Κρυπτογραφία Βάσει Χαρακτηριστικών (Attribute-Based Encryption), η οποία αποτελεί μια πολλά υποσχόμενη τεχνολογία προστασίας περιεχομένου η οποία και επιλέχθηκε για την προστασία του στα πλαίσια της προτεινόμενης αρχιτεκτονικής. Τα βασικά δομικά στοιχεία της αρχιτεκτονικής επικοινωνούν μεταξύ τους με τις στοιχειώδεις υπηρεσίες του MPEG-M και δημιουργούν μια ενοποιημένη πλατφόρμα ασφαλούς ανταλλαγής περιεχομένων που κρυπτογραφούνται βάσει χαρακτηριστικών, οι λειτουργίες της οποίας περιγράφονται λεπτομερώς και καλύπτουν πλήρως τον κύκλο ζωής του περιεχομένου. Στο σύστημα χρησιμοποιείται η γλώσσα περιγραφής δικαιωμάτων MPEG-21 REL τόσο για την περιγραφή των πολιτικών που θέτουν οι χρήστες για τον διαμοιρασμό των δεδομένων τους, όσο και για την εκχώρηση κατάλληλων χαρακτηριστικών στους χρήστες, συνεισφέροντας με αυτόν τον τρόπο στην αντιμετώπιση της ετερογένειας των χρηστών, των πολιτικών διαμοιρασμού αλλά και στη διαλειτουργικότητα μεταξύ των αρχών εκχώρησης χαρακτηριστικών.

- Έλεγχος πρόσβασης διαδικτυακών υπηρεσιών REST. Οι διαδικτυακές υπηρεσίες αποτελούν τον κύριο τρόπο επικοινωνίας μεταξύ ετερογενών συστημάτων, ως εκ τούτου ο έλεγχος πρόσβασης σε αυτές έχει τύχει εκτενούς έρευνας. Ωστόσο, ο έλεγχος πρόσβασης στην ανερχόμενη αρχιτεκτονική ανάπτυξης διαδικτυακών υπηρεσιών REST δεν έχει ερευνηθεί εκτενώς, ενώ οι προσπάθειες προτυποποίησης της περιγραφής διεπαφών REST δεν έχουν οδηγήσει σε σημαντικά αποτελέσματα. Τα παραπάνω, οδηγούν στην ανάπτυξη μη διαλειτουργικών διαδικτυακών υπηρεσιών REST σε ότι αφορά την υλοποίηση ελέγχου πρόσβασης σε κάθε μια ξεχωριστά. Έτσι, παρουσιάστηκε σύστημα για τον έλεγχο πρόσβασης βάσει χαρακτηριστικών σε διεπαφές REST, το οποίο προτείνει την περιγραφή κάθε μεθόδου της διεπαφής ως ενός ψηφιακού αντικειμένου, του οποίου οι πολιτικές χρήσης δηλώνονται στη γλώσσα περιγραφής δικαιωμάτων MPEG-21 REL, οι οποίες επιβάλλονται με τη χρήση κρυπτογραφίας βάσει χαρακτηριστικών. Το σύστημα βασισμένο σε πρότυπα, επιτυγχάνει να προσφέρει μια διαλειτουργική λύση για την προστασία διεπαφών REST και προάγει την ασφαλή συνεργασία εφαρμογών μέσω αυτών.

- Ασφαλής συνεργασία προμηθευτών υγείας και υποστήριξη τηλεϊατρικών υπηρεσιών. Στην εποχή μας όπου η διασύνδεση μεταξύ συσκευών και ανθρώπων είναι πανταχού παρούσα, γίνεται δυνατή η αλλαγή του παραδείγματος παροχής υπηρεσιών υγείας και η ενίσχυση του προνοιακού και προληπτικού χαρακτήρα της μέσω της συνεχούς παρακολούθησης των ασθενών, το οποίο πέρα από τη βελτίωση των παρεχόμενων υπηρεσιών υγείας θα έχει φυσικά και οφέλη στη εξοικονόμηση οικονομικών και όχι μόνο πόρων. Ωστόσο, ζητούμενο για τα παραπάνω είναι η διασύνδεση μεταξύ των ετερογενών συστημάτων των παρόχων υγείας (ασφαλιστικοί φορείς, νοσοκομεία, ιατροί, φαρμακεία) και η διασφάλιση των προσωπικού χαρακτήρα δεδομένων τα οποία θα ανταλλάσσονται. Σημαντικό βήμα κάνει η πρωτοβουλία HL7 FHIR στην προτυποποίηση των παραπάνω δεδομένων και διαδικασιών, ωστόσο δεν λαμβάνει υπόψη της ζητήματα ασφαλείας. Η εφαρμογή AidIT, στηριζόμενη στο πρότυπο HL7 FHIR και στις λύσεις της διατριβής προσφέρει την ασφαλή συνεργασία μεταξύ των παρόχων υγείας και ενεργοποιεί το όραμα για μετατροπή των κινητών συσκευών σε προσωπικούς βοηθούς υγείας.

7.2 Μελλοντικές ερευνητικές κατευθύνσεις

Παρακάτω παρατίθενται προτάσεις για μελλοντική έρευνα στα πλαίσια που προδιαγράφει η διατριβή. Αυτές αφορούν σε επεκτάσεις των λύσεων που προτείνονται τόσο για την υποστήριξη της σημασιολογικής διαλειτουργικότητας, την ασφαλή διαχείριση ψηφιακών αντικειμένων αλλά και την προστασία διαδικτυακών υπηρεσιών REST. Συγκεκριμένα, έχουν αναγνωριστεί οι ακόλουθοι βασικοί άξονες :

- Επέκταση του συστήματος σημασιολογικής διαλειτουργικότητας σε ότι αφορά τη δημιουργία των λεξικών σημασιολογικής διαλειτορυγικότητας. Η παρούσα διατριβή προτείνει τη δομή των λεξικών σημασιολογικής διαλειτουργικότητας, ωστόσο δεν ορίζει ημιαυτόματους ή αυτόματους τρόπους δημιουργίας και επέκτασης τους. Στο σημείο αυτό και θεωρώντας σενάριο διαμοιρασμού ψηφιακών αντικειμένων του MPEG-21 από ετερογενείς χρήστες μέσω τερματικού MPEG-M, προτείνεται να επεκταθεί το σύστημα σημασιολογικής διαλειτουργικότητας ώστε να δημιουργεί τα λεξικά με αυ-

τόματο τρόπο έχοντας ως είσοδο τη δραστηριότητα κάθε χρήστη. Οι μηχανισμοί που θα πραγματοποιούν το παραπάνω θα λαμβάνουν υπόψη τους τα ψηφιακά αντικείμενα που καταναλώνει και μοιράζεται ο χρήστης και μεταξύ άλλων θα μπορούσαν να χρησιμοποιηθούν τεχνικές συσχέτισης οντολογιών για την δημιουργία των λεξικών. Επιπρόσθετα, θα μπορούσε να εξεταστεί η κατανεμημένη δημιουργία των λεξικών με βάση το σύνολο των ψηφιακών αντικειμένων που διακινούνται στο σύστημα.

- Επέκταση του συστήματος σημασιολογικής διαλειτουργικόττηας σε ότι αφορά την αξιολόγηση των λεξικών σημασιολογικής διαλειτουργικότητας. Στο σημείο αυτό προτείνεται, με βάση την παραπάνω πρόταση, να επεκταθεί το σύστημα ώστε από τη μια να αξιολογεί την ποιότητα των δημιουργημένων λεξικών και από την άλλη, έχοντας κατά νου πως τα λεξικά αποτελούνται από συσχετίσεις αποκλειστικά δύο οντολογιών, να χρησιμοποιούνται οι παραπάνω αξιολογήσεις ώστε κατά την παροχή των υπηρεσιών σημασιολογικής διαλειτουργικότητας του συστήματος και σε περίπτωση μη ύπαρξης διαθέσιμου λεξικού, το σύστημα να ακολουθεί τη βέλτιστη σημασιολογική διαδρομή μεταξύ δύο οντολογιών, επιλέγοντας τις σημασιολογικές γέφυρες-λεξικά που θα οδηγήσουν από την οντολογία-αφετηρία στην οντολογία-προορισμό με την ελάχιστη σημασιολογική απόσταση.

- Επέκταση του συστήματος σημασιολογικής διαλειτουργικότητας σε ότι αφορά την αξιοποίηση των λεξικών διαλειτουργικότητας. Ένας από τους τρόπους με τους οποίους μπορεί να αξιοποιηθεί το σύστημα και τα λεξικά σημασιολογικής διαλειτουργικότητας αποτελεί η παρουσίαση ενός ψηφιακού αντικειμένου στον χρήστη. Στο σημείο αυτό και θεωρώντας σενάριο διαμοιρασμού ψηφιακών αντικειμένων του MPEG-21 από ετερογενείς χρήστες μέσω τερματικού MPEG-M, προτείνεται η επέκταση του συστήματος ώστε να παρέχει εξατομικευμένη παρουσίαση των ψηφιακών αντικειμένων σε κάθε χρήστη. Λαμβάνοντας υπόψη τα ψηφιακά αντικείμενα που μοιράζεται ο χρήστης, θα μπορούσε να δημιουργηθεί η οντολογία του χρήστη, που θα αποτελεί την δική του θέαση για τον κόσμο. Ενώ, όταν ο χρήστης καταναλώνει ένα ψηφιακό αντικείμενο, το σύστημα θα δημιουργεί αυτόματα λεξικό σημασιολογικής διαλειτουργικότητας από την οντολογία του ψηφιακού αντικειμένου στην οντολογία του χρήστη και θα παρουσιάζει το ψηφιακό αντικείμενο σύμφωνα με την τελευταία. Το

παραπάνω προτείνεται να υλοποιηθεί με βάση τις προδιαγραφές του 7ου μέρους του προτύπου MPEG-21 (Digital Item Adaptation - Προσαρμογή ψηφιακών αντικειμένων - [113]), το οποίο καλείται να επιλύσει τα ζητήματα ετερογένειας των συσκευών αναπαραγωγής ψηφιακών αντικειμένων παρέχοντας μηχανισμούς για την προσαρμογή τους σύμφωνα με τις δυνατότητες της συσκευής, ωστόσο εδώ θα χρησιμοποιηθεί για την προσαρμογή του ψηφιακού αντικειμένου στον χρήστη.

- Επέκταση του συστήματος ασφαλούς διαχείρισης ψηφιακών αντικειμένων με στόχο την υποστήριξη μοντέλου ελέγχου πρόσβασης το οποίο βασίζεται σε οντολογίες. Πιο συγκεκριμένα, προτείνεται η χρήση οντολογικών χαρακτηριστικών στις άδειες χρήσης της γλώσσας περιγραφής δικαιωμάτων και η επέκταση του μηχανισμού μετάφρασης των τελευταίων σε δέντρα πρόσβασης κρυπτογραφίας βάσει χαρακτηριστικών. Αυτή η προσέγγιση, αναμένεται να επεκτείνει ακόμα περισσότερο την ευελιξία του προτεινόμενου συστήματος, αφού κάθε εμπλεκόμενη οντότητα θα μπορεί να χρησιμοποιεί το δικό της λεξιλόγιο για την περιγραφή των χαρακτηριστικών των πολιτικών πρόσβασης.

- Επέκταση του συστήματος προστασίας διαδικτυακών υπηρεσιών REST, ώστε κάθε κλήση στην διεπαφή να μπορεί να δημιουργεί αναφορές συμβάντων που βασίζονται στο 15ο μέρος του προτύπου MPEG-21 (Event Reporting - [114]). Η συγκεκριμένη προσθήκη θα παρείχε προστιθέμενη αξία σε περιπτώσεις όπου απαιτείται η διαλειτουργική ενημέρωση της χρήσης της διεπαφής σε περισσότερα από ένα συστήματα. Με βάση αυτό το σύστημα και χρησιμοποιώντας το 19ο μέρος του προτύπου MPEG-21 που προδιαγράφει την οντολογία αλυσίδας αξιών μέσων (Media Value Chain Ontology - [115]) θα μπορούσε να υποστηριχθεί η ασφαλής εκτέλεση ροών εργασιών οι οποίες στηρίζονται στη διαχείριση, επεξεργασία και διαμοιρασμό ψηφιακών αντικειμένων και απαιτούν την ασύγχρονη εκτέλεση τους.

Βιβλιογραφία

[1] A. Vetro, "Consistent digital item adaption for mpeg-21 multimedia systems," Dec. 27 2006. EP Patent 1,362,484.

[2] ContentGuard, "Profiling mpeg rights expression language: Concept, approach and application." `http://www.xrml.org/reference/MPEG-REL-Profling.pdf`, 2003.

[3] Z. Huang, M. Ji, S. Shen, and T. Senoh, "Method for implementing mpeg-21 ipmp," July 15 2004. US Patent App. 10/474,028.

[4] H. Castro, M. Andrade, F. Almeida, G. Tropea, N. Melazzi, A. Mousas, D. Kaklamani, L. Chiariglione, and A. Difino, "Semantically connected web resources with mpeg-21," *Multimedia Tools and Applications*, pp. 1–24, 2014.

[5] A. S. Mousas, A.-C. Anadiotis, G. Lioudakis, J. Papanis, P. Gkonis, D. Kaklamani, and I. Venieris, "On supporting secure information distribution in heterogeneous systems using standard technologies," *Wireless Personal Communications*, vol. 76, no. 1, pp. 99–119, 2014.

[6] HL7, "Fast healthcare integration resources." `http://www.hl7.org/implement/standards/fhir/`, February 2014.

[7] International Standards Organization, "ISO/IEC TR 21000-1:2004 Information technology – Multimedia framework (MPEG-21) – Part 1: Vision, Technologies and Strategy," November 2004.

[8] International Standards Organization, "ISO/IEC 21000-2:2005 Information technology – Multimedia framework (MPEG-21) – Part 2: Digital Item Declaration," October 2005.

[9] International Standards Organization, "ISO/IEC 21000-5:2004 Information technology – Multimedia framework (MPEG-21) – Part 5: Rights Expression Language," April 2004.

[10] International Standards Organization, "ISO/IEC 21000-6:2004 Information technology – Multimedia framework (MPEG-21) – Part 6: Rights Data Dictionary," May 2004.

[11] W. X. S. W. Group, "Xml signature syntax and processing." http://www.w3.org/TR/xmldsig-core/, 2008. (Online). Last accessed: 4 Apr. 2014.

[12] International Standards Organization, "ISO/IEC 21000-4:2006 Information technology – Multimedia framework (MPEG-21) – Part 4: Intellectual Property Management and Protection Components," April 2006.

[13] International Standards Organization, "ISO/IEC 23006-1:2013 Information technology – Multimedia service platform technologies – Part 1: Architecture," May 2013.

[14] International Standards Organization, "ISO/IEC 23006-3:2013 Information technology - Multimedia service platform technologies – Part 3: Conformance and reference software," September 2013.

[15] T. Zahariadis, P. Daras, J. Bouwen, N. Niebert, D. Griffin, F. Alvarez, and G. Camarillo, "Towards a content-centric internet," *Towards the Future Internet - A European Research Perspective*, pp. 1–256, 2010.

[16] E. Aitenbichler, A. Behring, D. Bradler, M. Hartmann, L. Martucci, M. Mühlhäuser, S. Ries, D. Schnelle-Walka, D. Schreiber, J. Steimle, and T. Strufe, "Shaping the future internet," in *Shaping the Future Internet*, 2009.

[17] World Wide Web Consortium (W3C), "Resource Description Framework (RDF): Concepts and Abstract Syntax." http://www.w3.org/TR/2004/REC-rdf-syntax-grammar-20040210/, February 2004. W3C Recommendation.

[18] W. W. W. C. (W3C), "Owl 2 web ontology language." http://www.w3.org/TR/owl2-overview/, December 2012. W3C Recommendation.

[19] H. Castro, T. Andrade, G. Tropea, A. S. Mousas, and E. Radica, "Information technology - multimedia framework (mpeg-21) - part 3: Digital item identification, amendment 2: Digital item semantic relationships," November 2011. Input document to the International Standards Organization, ISO/IEC JTC 1/SC 29/WG 11 (MPEG).

[20] H. Castro, T. Andrade, G. Tropea, A. S. Mousas, and E. Radica, "Proposal to extend mpeg-21 dii with means to support a semantically explicit declaration of relationships between digital items," July 2011. Input document to the International Standards Organization, ISO/IEC JTC 1/SC 29/WG 11 (MPEG).

[21] C. H. Chang, M. Kayed, M. Girgis, and K. Shaalan, "A survey of web information extraction systems," *Knowledge and Data Engineering, IEEE Transactions on*, vol. 18, no. 10, pp. 1411–1428, 2006.

[22] W. F. Clocksin, "Artificial intelligence and the future," *Philosophical Transactions*, pp. 1721–1748, 2003.

[23] M. Gupta, R. Li, Z. Yin, and J. Han, "Survey on social tagging techniques," *SIGKDD Explor. Newsl.*, vol. 12, pp. 58–72, Nov. 2010.

[24] W. H. W. Group, "W3C HTML 4.01 Specification, Section 12–Links." `http://www.w3.org/TR/html401/struct/links.html`, 1997. (Online). Last accessed: 6 Dec. 2013.

[25] N. Shadbolt, W. Hall, and T. Berners-Lee, "The semantic web revisited," *Intelligent Systems, IEEE*, vol. 21, no. 3, pp. 96–101, 2006.

[26] R. Khare, "Microformats: the next (small) thing on the semantic web?," *Internet Computing, IEEE*, vol. 10, no. 1, pp. 68–75, 2006.

[27] W. X. W. Group, "RDFa Use Cases: Scenarios for embedding RDF in HTML." `http://www.w3.org/TR/xhtml-rdfa-scenarios`, 2007. (Online). Last accessed: 6 Dec. 2013.

[28] M. Y. W. Google, Yahoo, "Schema.org vocabulary." `http://schema.org`, 2011. (Online). Last accessed: 6 Dec. 2013.

[29] W. S. W. Education and O. Group, "Linked Data - Connect Distributed Data across the Web." `http://linkeddata.org`, 2006. (Online). Last accessed: 6 Dec. 2013.

[30] O. A. Initiative, "Open Archives Initiative Object Reuse and Exchange." `http://www.openarchives.org/ore`, 2008. (Online). Last accessed: 6 Dec. 2013.

[31] International Standards Organization, "ISO/IEC 21000-3:2003 Information technology – Multimedia framework (MPEG-21) – Part 3: Digital Item Identification," April 2003.

[32] W. X. C. W. Group, "XML Inclusions (XInclude) Version 1.0." `http://www.w3.org/TR/xinclude/`, 2006. (Online). Last accessed: 6 Dec. 2013.

[33] International Standards Organization, "ISO/IEC 21000-3:2003/FDAM 1:2007(E) MPEG-21 - Part 3: Digital Item Identification, AMENDMENT 1: Related identifier types.," October 2007.

[34] W. W. W. C. (W3C), "Sparql." `http://www.w3.org/TR/sparql11-overview/`, March 2013. W3C Recommendation.

[35] H. Paulheim and F. Probst, "Ontology-enhanced user interfaces: A survey.," *Int. J. Semantic Web Inf. Syst.*, vol. 6, no. 2, pp. 36–59, 2010.

[36] S. Brin and L. Page, "The Anatomy of a Large-Scale Hypertextual Web Search Engine," *Computer Networks and ISDN Systems*, vol. 30, pp. 107–117, April 1998.

[37] B. Aleman-Meza, I. B. Arpinar, M. V. Nural, and A. P. Sheth, "Ranking documents semantically using ontological relationships," in *Proceedings of the 2010 IEEE Fourth International Conference on Semantic Computing*, ICSC '10, (Washington, DC, USA), pp. 299–304, IEEE Computer Society, 2010.

[38] M. Kahng, S. Lee, and S.-g. Lee, "Ranking objects by following paths in entity-relationship graphs," in *Proceedings of the 4th Workshop on Workshop for Ph.D. Students in Information & Knowledge Management*, PIKM '11, (New York, NY, USA), pp. 11–18, ACM, 2011.

[39] W. S. W. D. W. Group, "SKOS Simple Knowledge Organization System." `http://www.w3.org/TR/skos-reference/skos.rdf`, 2009. (Online). Last accessed: 6 Dec. 2013.

[40] G. Grimnes, "The IMDB Mapping Movie Ontology." `http://www.csd.abdn.ac.uk/~ggrimnes/dev/imdb/IMDB.rdfs`. (Online). Last accessed: 6 Dec. 2013.

[41] P. T. Eugster, P. A. Felber, R. Guerraoui, and A.-M. Kermarrec, "The many faces of publish/subscribe," *ACM Computing Surveys*, vol. 35, pp. 114–131, June 2003.

[42] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," *Journal of Internet Services and Applications*, vol. 1, no. 1, pp. 7–18, 2010.

[43] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, 2002.

[44] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, pp. 2787–2805, Oct. 2010.

[45] M. P. Papazoglou and W.-J. Heuvel, "Service oriented architectures: approaches, technologies and research issues," *The VLDB Journal*, vol. 16, pp. 389–415, July 2007.

[46] S. De Capitani di Vimercati, P. Samarati, and R. Sandhu, "Access control," in *Computer Science Handbook (3rd edition) - Information Systems and Information Technology* (A. Tucker and H. Topi, eds.), Taylor and Francis Group, 2014. (to appear).

[47] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed nist standard for role-based access control," *ACM Transactions on Information and System Security*, vol. 4, no. 3, pp. 224–274, 2001.

[48] A. Kalam, R. Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, A. Miege, C. Saurel, and G. Trouessin, "Organization based access control," in *Proceedings of the 4th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY 2003)*, pp. 120–131, 2003.

[49] E. Yuan and J. Tong, "Attributed based access control (ABAC) for web services," in *Proceedings of the IEEE International Conference on Web Services (ICWS 2005)*, 2005.

[50] A. Antonakopoulou, G. V. Lioudakis, F. Gogoulos, D. I. Kaklamani, and I. S. Venieris, "Leveraging access control for privacy protection: A survey," in *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards* (G. Yee, ed.), pp. 65–94, IGI Global, 2012.

[51] Organization for the Advancement of Structured Information Standards (OASIS), "eXtensible Access Control Markup Language (XACML) Version 2.0." `http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf`, February 2005. OASIS Standard.

[52] Organization for the Advancement of Structured Information Standards (OASIS), "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) Version 2.0." `http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf`, March 2005. OASIS Standard.

[53] E. I. Papagiannakopoulou, M. N. Koukovini, G. V. Lioudakis, N. M. Dellas, D. I. Kaklamani, and I. S. Venieris, "Leveraging Semantic Web Technologies for Access Control," in *Emerging Trends in Information and Communication Technologies Security* (B. Akhgar and H. Arabnia, eds.), Morgan Kaufmann, 2014. (to appear).

[54] A. Westerinen, J. Schnizlein, J. Strassner, M. Scherling, B. Quinn, S. Herzog, A. Huynh, M. Carlson, J. Perry, and S. Waldbusser, "Terminology for Policy-Based Management." RFC 3198 (Informational), Nov. 2001.

[55] G. Karjoth, M. Schunter, and M. Waidner, "Platform for enterprise privacy practices: privacy-enabled management of customer data," in *Proceedings of the 2nd International Conference on Privacy Enhancing Technologies (PET 2002)*, vol. 2482 of *Lecture Notes in Computer Science*, (Berlin, Heidelberg), pp. 69–84, Springer-Verlag, 2003.

[56] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP 2007)*, pp. 321–334, 2007.

[57] A. Difino, A. S. Mousas, and A.-C. Anadiotis, "Proposed revised version of MPEG-M part3," July 2012. Input document to the International Standards Organization, ISO/IEC JTC 1/SC 29/WG 11 (MPEG).

[58] A. Difino, A. S. Mousas, and A.-C. Anadiotis, "Proposed revised version of MPEG-M part2," July 2012. Input document to the International Standards Organization, ISO/IEC JTC 1/SC 29/WG 11 (MPEG).

[59] A. Difino, A. S. Mousas, A.-C. Anadiotis, B. Ardeleanu, and P. Gkonis, "Proposal for a refactored version of mxm for mpeg-m purpose," April 2012. Input document to the International Standards Organization, ISO/IEC JTC 1/SC 29/WG 11 (MPEG).

[60] A. Difino, A. S. Mousas, A.-C. Anadiotis, B. Ardeleanu, and P. Gkonis, "Proposed revised version of MPEG-M part3," April 2012. Input document to the International Standards Organization, ISO/IEC JTC 1/SC 29/WG 11 (MPEG).

[61] A. Difino, A. S. Mousas, A.-C. Anadiotis, B. Ardeleanu, and P. Gkonis, "Proposed revised version of MPEG-M part2," April 2012. Input document to the International Standards Organization, ISO/IEC JTC 1/SC 29/WG 11 (MPEG).

[62] A.-C. Anadiotis, A. Difino, A. S. Mousas, S. Signorello, and G. Tropea, "An mpeg-m use case: The mpm photo sharing service," February 2012. Input document to the International Standards Organization, ISO/IEC JTC 1/SC 29/WG 11 (MPEG).

[63] F. Cuppens and N. Cuppens-Boulahia, "Modeling Contextual Security Policies," *International Journal of Information Security*, vol. 7, no. 4, pp. 285–305, 2008.

[64] R. Zhang, F. Giunchiglia, B. Crispo, and L. Song, "Relation-based access control: An access control model for context-aware computing environment," *Wireless Personal Communications*, vol. 55, no. 1, pp. 5–17, 2010.

[65] R. Hebig, C. Meinel, M. Menzel, I. Thomas, and R. Warschofsky, "A web service architecture for decentralised identity- and attribute-based access control," in *Proceedings of the IEEE 2009 International Conference on Web Services (ICWS 2009)*, pp. 551–558, 2009.

[66] L. Wang, D. Wijesekera, and S. Jajodia, "A logic-based framework for attribute based access control," in *Proceedings of the 2004 ACM workshop on Formal methods in security engineering (FMSE 2004)*, (New York, NY, USA), pp. 45–55, ACM, 2004.

[67] H. Shen, "A semantic-aware attribute-based access control model for web services," in *Algorithms and Architectures for Parallel Processing* (A. Hua and S.-L. Chang, eds.), vol. 5574 of *Lecture Notes in Computer Science*, pp. 693–703, Springer Berlin Heidelberg, 2009.

[68] International Telecommunication Union (ITU) – Telecommunication Standardization Sector, "Information technology – Open Systems Interconnection – The Directory: Public-key and Attribute Certificate Frameworks," August 2005. ITU-T Recommendation X.509.

[69] L. Camarinha-Matos, I. Silveri, H. Afsarmanesh, and A. Oliveira, "Towards a framework for creation of dynamic virtual organizations," in *Collaborative Networks and Their Breeding Environments* (L. Camarinha-Matos, H. Afsarmanesh, and A. Ortiz, eds.), vol. 186 of *IFIP – The International Federation for Information Processing*, pp. 69–80, Springer US, 2005.

[70] F. Kerschbaum and P. Robinson, "Security architecture for virtual organizations of business web services," *Journal of Systems Architecture*, vol. 55, no. 4, pp. 224–232, 2009.

[71] R. Alfieri, R. Cecchini, V. Ciaschini, L. dell'Agnello, A. Frohner, A. Gianoli, K. LÃµrentey, and F. Spataro, "VOMS, an authorization system for virtual organizations," in *Grid Computing* (F. FernÃ¡ndez Rivera, M. Bubak, A. GÃ³mez Tato, and R. Doallo, eds.), vol. 2970 of *Lecture Notes in Computer Science*, pp. 33–40, Springer Berlin Heidelberg, 2004.

[72] S. Ayed, N. Cuppens-Boulahia, and F. Cuppens, "Managing access and flow control requirements in distributed workflows," in *Proceedings of the 2008 IEEE/ACS International Conference on Computer Systems and Applications (AICCSA 2008)*, (Washington, DC, USA), pp. 702–710, IEEE Computer Society, 2008.

[73] S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: management of access control evolution on outsourced data," in *Proceedings of the 33rd international conference on Very Large Databases (VLDB 2007)*, pp. 123–134, VLDB Endowment, 2007.

[74] W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and efficient access to outsourced data," in *Proceedings of the 2009 ACM workshop on Cloud computing security (CCSW 2009)*, (New York, NY, USA), pp. 55–66, ACM, 2009.

[75] N. Subramanian, C. Yang, and W. Zhang, "Securing distributed data storage and retrieval in sensor networks," in *Proceedings of the 5th IEEE International Conference on Pervasive Computing and Communications (PerCom 2007)*, pp. 191–200, 2007.

[76] D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," in *Advances in Cryptology â˘ş- CRYPTO 2005* (V. Shoup, ed.), vol. 3621 of *Lecture Notes in Computer Science*, pp. 258–275, Springer Berlin Heidelberg, 2005.

[77] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in *Proceedings of the 2009 ACM workshop on Cloud computing security (CCSW 2009)*, (New York, NY, USA), pp. 103–114, ACM, 2009.

[78] C. Dong, G. Russello, and N. Dulay, "Shared and searchable encrypted data for untrusted servers," in *Data and Applications Security XXII* (V. Atluri, ed.), vol. 5094 of *Lecture Notes in Computer Science*, pp. 127–143, Springer Berlin Heidelberg, 2008.

[79] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proceedings of the 24th annual international conference on Theory and Applications of Cryptographic Techniques*, EUROCRYPT'05, (Berlin, Heidelberg), pp. 457–473, Springer-Verlag, 2005.

[80] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin, "Persona: an online social network with user-defined privacy," *SIGCOMM Computer Communication Review*, vol. 39, pp. 135–146, Aug. 2009.

[81] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131–143, 2013.

[82] S. Yu, K. Ren, and W. Lou, "FDAC: Toward fine-grained distributed data access control in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 4, pp. 673–686, 2011.

[83] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless Communications*, vol. 17, no. 1, pp. 51–58, 2010.

[84] D. Huang and M. Verma, "ASPE: attribute-based secure policy enforcement in vehicular ad hoc networks," *Ad Hoc Networks*, vol. 7, pp. 1526–1535, Nov. 2009.

[85] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in cryptology*, pp. 47–53, Springer, 1985.

[86] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM conference on Computer and communications security*, pp. 89–98, ACM, 2006.

[87] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Public Key Cryptography–PKC 2011*, pp. 53–70, Springer, 2011.

[88] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Security and Privacy, 2007. SP'07. IEEE Symposium on*, pp. 321–334, IEEE, 2007.

[89] J. A. Akinyele, M. W. Pagano, M. D. Green, C. U. Lehmann, Z. N. Peterson, and A. D. Rubin, "Securing electronic medical records using attribute-based encryption on mobile devices," in *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*, pp. 75–86, ACM, 2011.

[90] P. Traynor, K. R. Butler, W. Enck, and P. McDaniel, "Realizing massive-scale conditional access systems through attribute-based cryptosystems.," in *NDSS*, 2008.

[91] M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in *Proceedings of the 16th ACM conference on Computer and communications security*, pp. 121–130, ACM, 2009.

[92] V. Božović, D. Socek, R. Steinwandt, and V. I. Villányi, "Multi-authority attribute-based encryption with honest-but-curious central authority," *International Journal of Computer Mathematics*, vol. 89, no. 3, pp. 268–283, 2012.

[93] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Advances in Cryptology–EUROCRYPT 2011*, pp. 568–588, Springer, 2011.

[94] K. Yang, X. Jia, K. Ren, and B. Zhang, "Dac-macs: Effective data access control for multi-authority cloud storage systems," in *INFOCOM, 2013 Proceedings IEEE*, pp. 2895–2903, IEEE, 2013.

[95] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, pp. 261–270, ACM, 2010.

[96] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proceedings of the 14th ACM conference on Computer and communications security*, pp. 195–203, ACM, 2007.

[97] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute-based systems," *Journal of Computer Security*, vol. 18, no. 5, pp. 799–837, 2010.

[98] S. Müller, S. Katzenbeisser, and C. Eckert, "On multi-authority ciphertext-policy attribute-based encryption," *Bulletin of the Korean Mathematical Society*, vol. 46, no. 4, pp. 803–819, 2009.

[99] M. Athanasopoulos, K. Kontogiannis, and C. Brealey, "Considerations of adapting service-offering components to restful architectures," *Migrating Legacy Applications: Challenges in Service Oriented Architecture and Cloud Computing Environments*, pp. 303–323, 2013.

[100] W. W. W. C. (W3C), "Web services description language." `http://www.w3.org/TR/wsdl`, March 2001. W3C Recommendation.

[101] W. W. W. C. (W3C), "Soap version 1.2." `http://www.w3.org/TR/soap12-part1/`, April 2007. W3C Recommendation.

[102] R. T. Fielding, *Architectural styles and the design of network-based software architectures*. PhD thesis, University of California, 2000.

[103] L. Richardson and S. Ruby, *RESTful web services*. O'Reilly Media, Inc., 2008.

[104] OASIS, "Web services security version 1.2." `http://docs.oasis-open.org/wss/v1.1/`, February 2004.

[105] W. X. E. W. Group, "Xml encryption syntax and processing." `http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/`, 2002. (Online). Last accessed: 5 Apr. 2014.

[106] OASIS, "Ws-trust 1.3." `http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.html`, March 2007.

[107] OASIS, "Ws-securitypolicy 1.2." http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-spec-os.html, July 2007.

[108] W. W. W. C. (W3C), "Web application description language." http://www.w3.org/Submission/wadl/, August 2009.

[109] IETF, "Oauth 2.0." http://tools.ietf.org/html/rfc6749, October 2012.

[110] IETF, "Lightweight directory access protocol." http://tools.ietf.org/html/rfc4510, June 2006.

[111] HL7, "Reference information model." http://www.hl7.org/implement/standards/rim.cfm, November 2012.

[112] B. Middleton, "The value of healthcare information exchange and interoperability," in *2004 HIMSS Annual Conference and Exhibition. Orange County Convention Center, Orlando, FL*, vol. 23, 2004.

[113] I. S. Organization, "Information technology – multimedia framework (mpeg-21) – part 7: Digital item adaptation," March 2013.

[114] I. S. Organization, "Information technology – multimedia framework (mpeg-21) – part 15: Event reporting," December 2011.

[115] I. S. Organization, "Information technology – multimedia framework (mpeg-21) – part 19: Media value chain ontology," June 2010.

[116] J. P. Papanis, S. I. Papapanagiotou, A. S. Mousas, G. V. Lioudakis, D. I. Kaklamani, and I. S. Venieris, "On the use of attribute-based encryption for multimedia content protection over information-centric networks," *Transactions on Emerging Telecommunications Technologies*, vol. 25, no. 4, pp. 422–435, 2014.

[117] F. Almeida, H. Castro, M. T. Andrade, G. Tropea, N. B. Melazzi, S. Signorello, A. Mousas, A. Anadiotis, D. Kaklamani, I. Venieris, S. Minelli, and A. Difino, "Digital forgetting in information-centric networks—the convergence perspective," *New Review of Hypermedia and Multimedia*, vol. 20, no. 2, pp. 169–187, 2014.

[118] F. I. Gogoulos, A. Antonakopoulou, G. V. Lioudakis, A. S. Mousas, D. I. Kaklamani, and I. S. Venieris, "On the design of a privacy aware authorization engine for collaborative environments," *Electronic Markets*, vol. 24, no. 2, pp. 101–112, 2014.

[119] F. I. Gogoulos, A. Antonakopoulou, G. V. Lioudakis, A. S. Mousas, D. I. Kaklamani, and I. S. Venieris, "An authorization model for cross-enterprise collaborations," *Security and Communication Networks*, 2014.

[120] A. Antonakopoulou, F. I. Gogoulos, G. V. Lioudakis, A. S. Mousas, D. I. Kaklamani, and I. S. Venieris, "An ontology for privacy-aware access control in network monitoring environments," *Journal of Research and Practice in Information Technology*, 2013.

[121] G. Tropea, G. Bianchi, N. Blefari-Melazzi, H. Castro, L. Chiariglione, A. Difino, T. Huebner, A.-C. Anadiotis, and A. S. Mousas, "The adoption of rights expression language in convergence," in *Enhancing the Internet with the CONVERGENCE System* (F. Almeida, M. Andrade, N. Melazzi, R. Walker, H. Hussmann, and I. Venieris, eds.), Enhancing the Internet with the CONVERGENCE System, ch. 7, pp. 165–195, Springer, 2014.

[122] A.-C. Anadiotis, A. S. Mousas, A. Difino, and C. Patrikakis, "The content level (comid)," in *Enhancing the Internet with the CONVERGENCE System* (F. Almeida, M. Andrade, N. Melazzi, R. Walker, H. Hussmann, and I. Venieris, eds.), Enhancing the Internet with the CONVERGENCE System, ch. 4, pp. 73–102, Springer, 2014.

[123] F. Gogoulos, A. Antonakopoulou, A. Mousas, G. Lioudakis, D. Kaklamani, and I. Venieris, "Privacy-aware passive network monitoring," in *Informatics, 2009. PCI '09. 13th Panhellenic Conference on*, pp. 171–175, 2009.

[124] G. Lioudakis, F. Gogoulos, A. Antonakopoulou, A. Mousas, I. Venieris, and D. Kaklamani, "An access control approach for privacy-preserving passive network monitoring," in *Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for*, pp. 1–8, 2009.

[125] F. Gogoulos, A. Antonakopoulou, G. Lioudakis, A. Mousas, D. Kaklamani, and I. Venieris, "Privacy-aware access control and authorization in passive network monitoring infrastructures," in *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*, pp. 1114–1121, 2010.

[126] A. Mousas, A. Antonakopoulou, F. Gogoulos, G. Lioudakis, D. Kaklamani, and I. Venieris, "Visualising access control: The prism approach," in *Informatics (PCI), 2010 14th Panhellenic Conference on*, pp. 107–111, 2010.

[127] A. Antonakopoulou, F. Gogoulos, G. Lioudakis, A. Mousas, D. Kaklamani, and I. Venieris, "Semantic information model for privacy-aware access control," in *Informatics (PCI), 2010 14th Panhellenic Conference on*, pp. 130–134, 2010.

[128] H. Castro, M. Andrade, F. Almeida, G. Tropea, N. Melazzi, L. Chiariglione, A. Mousas, and D. Kaklamani, "Exploring semantic relationships across internet resources," in *Next Generation Web Services Practices (NWeSP), 2011 7th International Conference on*, pp. 80–85, 2011.

[129] N. Melazzi, S. Salsano, A. Detti, G. Tropea, L. Chiariglione, A. Difino, A. Anadiotis, A. Mousas, I. Venieris, and C. Patrikakis, "Publish/subscribe over information centric networks: A standardized approach in convergence," in *Future Network Mobile Summit (FutureNetw), 2012*, pp. 1–8, 2012.

[130] G. Lioudakis, A. Anadiotis, A. Mousas, C. Patrikakis, D. Kaklamani, and I. Venieris, "Routing in content-centric networks: From names to concepts," in *New Technologies, Mobility and Security (NTMS), 2012 5th International Conference on*, pp. 1–5, 2012.

Δημοσιεύσεις

Διεθνή Περιοδικά

- A. S. Mousas, A.-C. Anadiotis, G. Lioudakis, J. Papanis, P. Gkonis, D. Kaklamani, and I. Venieris, "On supporting secure information distribution in heterogeneous systems using standard technologies," *Wireless Personal Communications*, vol. 76, no. 1, pp. 99–119, 2014
- H. Castro, M. Andrade, F. Almeida, G. Tropea, N. Melazzi, A. Mousas, D. Kaklamani, L. Chiariglione, and A. Difino, "Semantically connected web resources with mpeg-21," *Multimedia Tools and Applications*, pp. 1–24, 2014
- J. P. Papanis, S. I. Papapanagiotou, A. S. Mousas, G. V. Lioudakis, D. I. Kaklamani, and I. S. Venieris, "On the use of attribute-based encryption for multimedia content protection over information-centric networks," *Transactions on Emerging Telecommunications Technologies*, vol. 25, no. 4, pp. 422–435, 2014
- F. Almeida, H. Castro, M. T. Andrade, G. Tropea, N. B. Melazzi, S. Signorello, A. Mousas, A. Anadiotis, D. Kaklamani, I. Venieris, S. Minelli, and A. Difino, "Digital forgetting in information-centric networks—the convergence perspective," *New Review of Hypermedia and Multimedia*, vol. 20, no. 2, pp. 169–187, 2014
- F. I. Gogoulos, A. Antonakopoulou, G. V. Lioudakis, A. S. Mousas, D. I. Kaklamani, and I. S. Venieris, "On the design of a privacy aware authorization engine for collaborative environments," *Electronic Markets*, vol. 24, no. 2, pp. 101–112, 2014
- F. I. Gogoulos, A. Antonakopoulou, G. V. Lioudakis, A. S. Mousas, D. I. Kaklamani, and I. S. Venieris, "An authorization model for cross-enterprise collaborations," *Security and Communication Networks*, 2014
- A. Antonakopoulou, F. I. Gogoulos, G. V. Lioudakis, A. S. Mousas, D. I. Kaklamani, and I. S. Venieris, "An ontology for privacy-aware access control in network monitoring environments," *Journal of Research and Practice in Information Technology*, 2013

Κεφάλαια βιβλίων

- G. Tropea, G. Bianchi, N. Blefari-Melazzi, H. Castro, L. Chiariglione, A. Difino, T. Huebner, A.-C. Anadiotis, and A. S. Mousas, "The adoption of rights expression language in convergence," in *Enhancing the Internet with the CONVERGENCE System* (F. Almeida, M. Andrade, N. Melazzi, R. Walker, H. Hussmann, and I. Venieris, eds.), Enhancing the Internet with the CONVERGENCE System, ch. 7, pp. 165–195, Springer, 2014

- A.-C. Anadiotis, A. S. Mousas, A. Difino, and C. Patrikakis, "The content level (comid)," in *Enhancing the Internet with the CONVERGENCE System* (F. Almeida, M. Andrade, N. Melazzi, R. Walker, H. Hussmann, and I. Venieris, eds.), Enhancing the Internet with the CONVERGENCE System, ch. 4, pp. 73–102, Springer, 2014

Πρακτικά Συνεδρίων

- F. Gogoulos, A. Antonakopoulou, A. Mousas, G. Lioudakis, D. Kaklamani, and I. Venieris, "Privacy-aware passive network monitoring," in *Informatics, 2009. PCI '09. 13th Panhellenic Conference on*, pp. 171–175, 2009

- G. Lioudakis, F. Gogoulos, A. Antonakopoulou, A. Mousas, I. Venieris, and D. Kaklamani, "An access control approach for privacy-preserving passive network monitoring," in *Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for*, pp. 1–8, 2009

- F. Gogoulos, A. Antonakopoulou, G. Lioudakis, A. Mousas, D. Kaklamani, and I. Venieris, "Privacy-aware access control and authorization in passive network monitoring infrastructures," in *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*, pp. 1114–1121, 2010

- A. Mousas, A. Antonakopoulou, F. Gogoulos, G. Lioudakis, D. Kaklamani, and I. Venieris, "Visualising access control: The prism approach," in *Informatics (PCI), 2010 14th Panhellenic Conference on*, pp. 107–111, 2010

- A. Antonakopoulou, F. Gogoulos, G. Lioudakis, A. Mousas, D. Kaklamani, and I. Venieris, "Semantic information model for privacy-aware access control," in *Informatics (PCI), 2010 14th Panhellenic Conference on*, pp. 130–134, 2010

- H. Castro, M. Andrade, F. Almeida, G. Tropea, N. Melazzi, L. Chiariglione, A. Mousas, and D. Kaklamani, "Exploring semantic relationships across internet resources," in *Next Generation Web Services Practices (NWeSP), 2011 7th International Conference on*, pp. 80–85, 2011

- N. Melazzi, S. Salsano, A. Detti, G. Tropea, L. Chiariglione, A. Difino, A. Anadiotis, A. Mousas, I. Venieris, and C. Patrikakis, "Publish/subscribe over information centric networks: A standardized approach in convergence," in *Future Network Mobile Summit (FutureNetw), 2012*, pp. 1–8, 2012
- G. Lioudakis, A. Anadiotis, A. Mousas, C. Patrikakis, D. Kaklamani, and I. Venieris, "Routing in content-centric networks: From names to concepts," in *New Technologies, Mobility and Security (NTMS), 2012 5th International Conference on*, pp. 1–5, 2012

Συνεισφορά σε Πρότυπα

- A. Difino, A. S. Mousas, and A.-C. Anadiotis, "Proposed revised version of MPEG-M part3," July 2012. Input document to the International Standards Organization, ISO/IEC JTC 1/SC 29/WG 11 (MPEG)
- A. Difino, A. S. Mousas, and A.-C. Anadiotis, "Proposed revised version of MPEG-M part2," July 2012. Input document to the International Standards Organization, ISO/IEC JTC 1/SC 29/WG 11 (MPEG)
- A. Difino, A. S. Mousas, A.-C. Anadiotis, B. Ardeleanu, and P. Gkonis, "Proposal for a refactored version of mxm for mpeg-m purpose," April 2012. Input document to the International Standards Organization, ISO/IEC JTC 1/SC 29/WG 11 (MPEG)
- A. Difino, A. S. Mousas, A.-C. Anadiotis, B. Ardeleanu, and P. Gkonis, "Proposed revised version of MPEG-M part3," April 2012. Input document to the International Standards Organization, ISO/IEC JTC 1/SC 29/WG 11 (MPEG)
- A. Difino, A. S. Mousas, A.-C. Anadiotis, B. Ardeleanu, and P. Gkonis, "Proposed revised version of MPEG-M part2," April 2012. Input document to the International Standards Organization, ISO/IEC JTC 1/SC 29/WG 11 (MPEG)
- A.-C. Anadiotis, A. Difino, A. S. Mousas, S. Signorello, and G. Tropea, "An mpeg-m use case: The mpm photo sharing service," February 2012. Input document to the International Standards Organization, ISO/IEC JTC 1/SC 29/WG 11 (MPEG)
- H. Castro, T. Andrade, G. Tropea, A. S. Mousas, and E. Radica, "Information technology - multimedia framework (mpeg-21) - part 3: Digital item identification, amendment 2: Digital item semantic relationships," November 2011. Input document to the International Standards Organization, ISO/IEC JTC 1/SC 29/WG 11 (MPEG)
- H. Castro, T. Andrade, G. Tropea, A. S. Mousas, and E. Radica, "Proposal to extend mpeg-21 dii with means to support a semantically explicit declaration of relationships between digital items,"

July 2011. Input document to the International Standards Organization, ISO/IEC JTC 1/SC 29/WG 11 (MPEG)