ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Σχεδιασμός και Ανάπτυξη Ηλεκτρονικής Ταυτότητας (eID) Πολίτη

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Στυλιανός Β. Γεωργιάδης

Κωνσταντίνος Χ. Μίχος

Επιβλέπων: Ιάκωβος Στ. Βενιέρης
Καθηγητής Ε.Μ.Π.

Αθήνα, Νοέμβριος 2018

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Σχεδιασμός και Ανάπτυξη Ηλεκτρονικής Ταυτότητας (eID) Πολίτη

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Στυλιανός Β. Γεωργιάδης

Κωνσταντίνος Χ. Μίχος

Επιβλέπων: Ιάκωβος Στ. Βενιέρης
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή επιτροπή την 7η Νοέμβρη 2018.

.....	.....	.....
Ι. Στ. Βενιέρης	Δ.-Θ. Ι. Κακλαμάνη	Γ. Κ. Ματσόπουλος
Καθηγητής Ε.Μ.Π.	Καθηγήτρια Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.

Αθήνα, Νοέμβριος 2018

.....

Στυλιανός Β. Γεωργιάδης

Κωνσταντίνος Χ. Μίχος

Διπλωματούχοι Ηλεκτρολόγοι Μηχανικοί και Μηχανικοί Υπολογιστών Ε.Μ.Π.

Περίληψη

Στη σύγχρονη εποχή, όλο και περισσότερες χώρες της Ευρωπαϊκής Ένωσης υιοθετούν τη χρήση Ηλεκτρονικής Ταυτότητας (eID) από τους πολίτες, ώστε να τους εξασφαλίζουν ασφαλή πρόσβαση σε υπηρεσίες Ηλεκτρονικής Διακυβέρνησης, συμβάλλοντας ταυτόχρονα και στη βελτίωση των παρεχόμενων υπηρεσιών. Παρότι τα πλεονεκτήματα που προσφέρει είναι αδιαμφισβήτητα, εγείρονται πολλά ζητήματα αναφορικά με την προστασία των προσωπικών δεδομένων και της ιδιωτικότητας των χρηστών. Για να μπορέσει εξ' ορισμού να υπάρξει η Ηλεκτρονική Ταυτότητα Πολίτη, είναι απαραίτητο να περιέχει προσωπικές πληροφορίες των πολιτών, που αποτελούν γι' αυτούς ταυτοποιητικά στοιχεία, όπως ΑΜΚΑ, ΑΦΜ, ΑΔΤ. Για τον λόγο αυτόν κρίνεται αναγκαία η ύπαρξη και χρήση μηχανισμών και δικλείδων ασφάλειας για την προστασία των προαναφερθέντων δεδομένων από πιθανή κακόβουλη χρήση τους, αλλά και διασφάλιση της ανωνυμίας των πολιτών όπου αυτή κρίνεται απαραίτητη, ακολουθώντας πιστά τις προτιμήσεις ιδιωτικότητας των πολιτών. Η παρούσα διπλωματική εργασία αφορά στον σχεδιασμό και την υλοποίηση ενός συστήματος Ηλεκτρονικής Διακυβέρνησης που βασίζεται στη χρήση Ηλεκτρονικής Ταυτότητας Πολίτη. Συγκεκριμένα, έπειτα από ενδελεχή μελέτη των τρεχουσών τεχνολογικών εξελίξεων στον τομέα, προτείνεται η χρήση έξυπνου κινητού τηλεφώνου που φέρει την Ηλεκτρονική Ταυτότητα Πολίτη και παρουσιάζεται ο τρόπος χρήσης της μέσω δύο πιλοτικών εφαρμογών και σεναρίων χρήσης που αναπτύχθηκαν στο πλαίσιο της παρούσας εργασίας. Βασικός στόχος του προτεινόμενου συστήματος είναι η διασφάλιση της προστασίας της ιδιωτικότητας του πολίτη κατά τη χρήση υπηρεσιών Ηλεκτρονικής Διακυβέρνησης.

Λέξεις κλειδιά: Ηλεκτρονική Διακυβέρνηση, Ηλεκτρονική Ταυτότητα Πολίτη, ασφάλεια, ιδιωτικότητα, αυθεντικοποίηση, ταυτοποίηση, έξυπνο κινητό τηλέφωνο, Android, FIDO, IRMA, Keycloak.

Abstract

Nowadays, more and more European Union countries adopt the use of an electronic IDentity (eID) by their citizens in order to ensure secure access to eGovernment services, while also contributing to the improvement of the services provided. Although the advantages that the eID offers are unquestionable, many issues arise regarding the protection of personal data and users' privacy. Each eID may contain personal information of the citizen, which constitutes identifying data, such as VAT number, etc. Therefore, it is necessary to use mechanisms so as to protect the abovementioned data against possible malicious use, but also to ensure anonymity of citizens when necessary, by also taking into account citizens' privacy preferences. This diploma thesis concerns the design and implementation of an eGovernment system based on the use of an electronic identity. Specifically, following a thorough study of the current technological developments in the respective research domain, the use of a smartphone which includes the electronic identity of each citizen is proposed and the functionality of the latter is tested in two pilot applications and use-case scenarios developed in the context of this thesis. The main objective of the proposed system is to ensure the protection of citizens' privacy while easily having access to eGovernment services.

Keywords: eGovernment, eID, security, privacy, authentication, identification, smartphone, Android, FIDO, IRMA, Keycloak.

Ευχαριστίες

Με την ολοκλήρωση της παρούσας διπλωματικής εργασίας γράφεται ο επίλογος ενός μεγάλου κεφαλαίου της προσωπικής μας πορείας, αυτού της ακαδημαϊκής μας ζωής. Για τον λόγο αυτόν θα θέλαμε να ευχαριστήσουμε όλους εκείνους τους ανθρώπους που συνέβαλαν σε αυτήν από την αρχή μέχρι το τέλος.

Αρχικά, θα θέλαμε να ευχαριστήσουμε ιδιαιτέρως τον Καθηγητή ΕΜΠ κ. Ιάκωβο Βενιέρη για την εμπιστοσύνη που μας έδειξε και την ευκαιρία που μας έδωσε να ασχοληθούμε με ένα τόσο ενδιαφέρον και σύγχρονο θέμα, που συνδυάζει ένα πλούσιο θεωρητικό υπόβαθρο με πολλές πρακτικές προεκτάσεις. Θα θέλαμε ακόμη να ευχαριστήσουμε θερμά τη Διδάκτορα ΕΜΠ κ. Μαρία–Ελευθερία Παπαδοπούλου, για την εποικοδομητική συνεργασία και τη διαρκή καθοδήγηση που μας παρείχε καθόλη τη διάρκεια εκπόνησης της διπλωματικής μας εργασίας.

Έπειτα, θα θέλαμε να ευχαριστήσουμε όλους μας τους φίλους, που στάθηκαν δίπλα μας καθόλη τη διάρκεια της παρούσας εργασίας και της φοιτητικής μας ζωής γενικά, μα πάνω από όλα θα θέλαμε να ευχαριστήσουμε από καρδιάς τις οικογένειές μας για την πλήρη στήριξη και αγάπη που μας παρείχαν απλόχερα όλα αυτά τα χρόνια.

Τέλος, λόγω της ιδιαίτερης φύσης της εργασίας που απαιτούσε δύο άτομα για την εκπόνησή της, θα θέλαμε να ευχαριστήσουμε ο ένας τον άλλο για την άψογη συνεργασία και αλληλοκατανόηση σε όλα τα ζητήματα που μας προέκυψαν κατά καιρούς.

Πίνακας Περιεχομένων

Ευρετήριο Σχημάτων

Ευρετήριο Πινάκων

Κεφάλαιο 1

Εισαγωγή

1.1 Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης και Διαχείριση Ταυτότητας

Η Ηλεκτρονική Διακυβέρνηση είναι ένα σύγχρονο και ενδιαφέρον θέμα προς μελέτη καθώς αποτελεί έναν ραγδαία εξελισσόμενο τομέα. Η χρήση τεχνολογικών μέσων στη Δημόσια Διοίκηση έχει προκαλέσει τη βελτίωση της ποιότητας των παρεχόμενων υπηρεσιών και τη μείωση του συνολικού κόστος λειτουργίας. Επιπροσθέτως, εξασφαλίζεται η αύξηση της διαφάνειας, η ενίσχυση των δημοκρατικών θεσμών, η συμμετοχή των πολιτών σε θέματα Δημόσιας Διοίκησης και η μείωση του φαινομένου της γραφειοκρατίας.

Τα τελευταία χρόνια, ο ελληνικός δημόσιος τομέας έχει καταβάλλει αξιόλογες προσπάθειες στην ενσωμάτωση των τεχνολογιών Ηλεκτρονικής Διακυβέρνησης, ωστόσο παραμένει χαμηλά συγκριτικά με τα υπόλοιπα κράτη μέλη της Ευρωπαϊκής Ένωσης. Η Ελλάδα πρέπει να εντείνει ακόμα περισσότερο τις προσπάθειές της ώστε να καλυφθεί το κενό των παρελθόντων ετών και να εκσυγχρονιστεί προς όφελος των πολιτών.

Η σχεδίαση πολύπλοκων πληροφοριακών συστημάτων μεταξύ των διαφόρων υπηρεσιών και η τάση αναδιαμόρφωσης των λειτουργιών του Δημόσιου Τομέα καθιστούν αναγκαία τη Διαχείρισης Ταυτότητας. Η Διαχείριση Ταυτότητας είναι ένα φλέγον ζήτημα που αν και αποτελεί απλοϊκή διαδικασία στην καθημερινή ζωή, η μεταφορά αντίστοιχων πρακτικών στο διαδίκτυο δημιουργεί μια επιπρόσθετη πολυπλοκότητα.

Η Ηλεκτρονική Διακυβέρνηση ως ιδέα τοποθετεί τον πολίτη στο επίκεντρο των δημόσιων υπηρεσιών, οι οποίες πάντα υπήρξαν οι βασικοί φορείς που απέδιδαν, διαχειρίζονταν και πιστοποιούσαν την ταυτότητα των πολιτών. Συνεπώς, η Διαχείριση Ταυτότητας στις υπηρεσίες Ηλεκτρονικής Διακυβέρνησης μπορεί να γίνει αντιληπτή ως ο έλεγχος των δεδομένων προσωπικού χαρακτήρα που αυθεντικοποιούν το άτομο και άρα δεν αφορά μόνο την ταυτοποίηση του πολίτη κατά τις συναλλαγές του, αλλά συμπεριλαμβάνει και τη γενικότερη εικόνα του ατόμου με πληθώρα ευαίσθητων πληροφοριών και δεδομένων.

1.2 Αντικείμενο της Διπλωματικής Εργασίας

Η παρούσα διπλωματική εργασία έχει ως βασικό στόχο την αναλυτική σχεδίαση και υλοποίηση της Ηλεκτρονικής Ταυτότητας Πολίτη, αφού πρώτα μελετηθούν σε βάθος οι ισχύουσες πολιτικές της Ευρωπαϊκής Ένωσης που δίνουν έμφαση στην ιδιωτικότητα και την ασφάλεια του χρήστη. Με χρήση του θεωρητικού υποβάθρου που

παρουσιάζεται αρχικά, προέκυψε η περιγραφή του προβλήματος με την καταγραφή των απαιτήσεων του συστήματος να ακολουθεί. Έπειτα, πραγματοποιήθηκε ο σχεδιασμός του συστήματος, η περιγραφή των οντοτήτων που θα το αποτελούν και εν τέλει η ενοποίηση τους σε ένα ολοκληρωμένο σύστημα καθορίζοντας τον τρόπο που όλα τα επιμέρους στοιχεία θα διαλειτουργούν μεταξύ τους. Πιο συγκεκριμένα, θα γίνει:

1. μελέτη της χρήσης της Ηλεκτρονικής Ταυτότητας Πολίτη στην παροχή υπηρεσιών Ηλεκτρονικής Διακυβέρνησης αλλά και των ταυτοποιητικών και όχι μόνο στοιχείων των πολιτών που αυτή θα φέρει.

2. διερεύνηση των τρόπων και των φυσικών μέσων που θα συμβάλλουν στην υλοποίησή της, σύμφωνα πάντα με τις τρέχουσες τεχνολογικές εξελίξεις (όπως χρήση έξυπνων καρτών, έξυπνων συσκευών/κινητών τηλεφώνων, ενδυτών συσκευών, και άλλων), αλλά θα συμβάλλουν και στην απαιτούμενη διαλειτουργικότητά της με υπάρχουσες πλατφόρμες Ηλεκτρονικής Διακυβέρνησης.

3. λεπτομερής εξέταση των μηχανισμών κρυπτογράφησης δεδομένων και έκδοσης ηλεκτρονικών πιστοποιητικών.

4. σχεδίαση, ανάπτυξη και σύγκριση πιλοτικών εφαρμογών και σεναρίων χρήσης, εξασφαλίζοντας πάντα την προστασία της ιδιωτικότητας του πολίτη κατά την πρόσβαση και χρήση των υπηρεσιών Ηλεκτρονικής Διακυβέρνησης στις συναλλαγές του με φορείς του δημοσίου.

5. εξαγωγή χρήσιμων συμπερασμάτων από την προσομοίωση, τόσο για το τρέχον επίπεδο ασφάλειας όσο και για μελλοντικές επεκτάσεις της προστασίας και των λειτουργιών που παρέχονται.

1.3 Διάρθρωση της Εργασίας

Το υπόλοιπο κείμενο της διπλωματικής εργασίας, πέραν της παρούσας Εισαγωγής, δομείται ως ακολούθως:

Στο Κεφάλαιο 2 αναλύεται η Ηλεκτρονική Διακυβέρνηση στη σύγχρονη εποχή και ο ρόλος της Ηλεκτρονικής Ταυτότητας Πολίτη σε αυτή. Διευκρινίζονται έννοιες και ορολογίες που χρησιμοποιούνται στην εργασία, γίνεται αναφορά στο νομικό πλαίσιο που πρέπει να τηρείται και παρουσιάζεται η βάση ενός τέτοιου συστήματος, δηλαδή η Διαχείριση Ταυτότητα. Ακολούθως δίνεται μία περιγραφή του προβλήματος που ανακύπτει, από την εφαρμογή όλων των παραπάνω σε ένα ενιαίο σύστημα.

Στο Κεφάλαιο 3 γίνεται η ανάλυση των απαιτήσεων του συστήματος και με βάση αυτό ακολουθεί μία αρχιτεκτονική υψηλού επιπέδου.

Στο Κεφάλαιο 4 περιγράφεται η σχεδίαση του συστήματος, λαμβάνοντας υπόψη την αρχιτεκτονική που προηγήθηκε καθώς και τις θεωρητικές λεπτομέρειες που δόθηκαν σχετικά με το φυσικό μέσο της ταυτότητας του πολίτη και τις απαιτήσεις που θα πρέπει να τηρούνται.

Στο Κεφάλαιο 5 παρουσιάζονται ενέργειες σχετικές με το αντικείμενο της παρούσας διπλωματικής, καθώς εδώ δίνεται η ανάπτυξη του συστήματος. Αναλύονται οι τεχνικές λεπτομέρειες σχετικά με τα πλαίσια (frameworks) που χρησιμοποιήθηκαν,

πως αυτά διαλειτουργούν μεταξύ τους στην πράξη και πως επικοινωνούν με τους servers που χρησιμοποιήθηκαν, αλλά και με την εφαρμογή για κινητό Android που υλοποιήθηκε. Στο τέλος του κεφαλαίου αυτού, δίνονται παραδείγματα χρήσης από την εκτέλεση πιλοτικών σεναρίων και συγκρίνονται μεταξύ τους.

Τέλος, στο Κεφάλαιο 6 γίνεται μία ανακεφαλαίωση των σταδίων από τα οποία πέρασε η παρούσα μελέτη και με αφορμή τη σύγκριση των πιλοτικών σεναρίων παρουσιάζονται πιθανές μελλοντικές επεκτάσεις της υπάρχουσας υλοποίησης.

Κεφάλαιο 2

Ηλεκτρονική Διακυβέρνηση και Ηλεκτρονική Ταυτότητα Πολίτη

2.1 Ρόλος και Κατευθύνσεις Ηλεκτρονικής Διακυβέρνησης

Στις μέρες μας, η ραγδαία ανάπτυξη του Διαδικτύου σε συνδυασμό με την εξέλιξη των υπολογιστικών συστημάτων έχει δημιουργήσει ένα ανεξάντλητο δίκτυο πληροφοριών. Το δίκτυο αυτό πλέον χρησιμοποιείται από όλους του τομείς ιδιωτικού και δημόσιου χαρακτήρα. Εστιάζοντας όμως στον δημόσιο τομέα, παρατηρείται μια συνεχώς αυξανόμενη ανάγκη για αξιοποίηση των Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ), όχι μόνο για τις εσωτερικές λειτουργίες των κρατικών υπηρεσιών αλλά κυρίως για τη βελτίωση της επικοινωνίας και των συναλλαγών του κράτους με τους πολίτες και τις επιχειρήσεις. Η δημόσια διοίκηση ωθείται προς τον ανασχεδιασμό των διαδικασιών και των οργανωτικών δομών της, ακολουθώντας ένα νέο μοντέλο λειτουργίας, περισσότερο αποτελεσματικό στην αντιμετώπιση των κοινωνικών προβλημάτων.

Η Ηλεκτρονική Διακυβέρνηση (ΗΔ), σύμφωνα με τον επίσημο ορισμό της Ευρωπαϊκής Ένωσης, ορίζεται ως «η διαδικασία αξιοποίησης των Τεχνολογιών Πληροφορικής και Επικοινωνιών στις δημόσιες διοικήσεις, σε συνδυασμό με οργανωτικές αλλαγές και νέες δεξιότητες, ώστε να βελτιωθούν η παροχή δημόσιων υπηρεσιών και οι δημοκρατικές διαδικασίες, καθώς και να ενισχυθεί η υποστήριξη των πολιτικών που ασκεί το δημόσιο» [1]. Βασικός στόχος, λοιπόν, είναι ο απλός πολίτης, μέσω αυτοματοποιημένων διαδικασιών, να επικοινωνεί και να διεκπεραιώνει άμεσα τις υποχρεώσεις του, χρησιμοποιώντας το διαδίκτυο ανά πάσα στιγμή, χωρίς να απαιτείται άσκοπη σπατάλη χρόνου, μειώνοντας παράλληλα και το φαινόμενο της γραφειοκρατίας.

Σχετικά με την ηλεκτρονική διακυβέρνηση, επικρατούν δύο φιλοσοφικές αντιλήψεις. Η πρώτη αναφέρεται στην εφαρμογή εργαλείων και τεχνικών στο ηλεκτρονικό εμπόριο και εστιάζει στην πρακτική αποδοτικότητα και τη μείωση του κόστους, όπως για παράδειγμα η ηλεκτρονική υποβολή της φορολογικής δήλωσης ή ο ηλεκτρονικός εφοδιασμός. Για κάποιους άλλους, η ηλεκτρονική διακυβέρνηση έχει τη δυναμική να «βελτιώσει τη δημοκρατική συμμετοχή» και να «υπερκεράσει την πολιτική αποστασιοποίηση». Η αντίληψη αυτή εστιάζει σε πρωτοβουλίες που θα φέρουν την αλληλεπίδραση μεταξύ των διαφόρων μορφών διακυβέρνησης και του πολίτη σε νέα επίπεδα.

- ***<u>Οφέλη της Ηλεκτρονικής Διακυβέρνησης</u>***

Οι προκλήσεις και τα νέα δεδομένα που αντιμετωπίζουν οι δημόσιες διοικήσεις των περισσότερων χωρών οδηγούν στη διερεύνηση της χρήσης των ΤΠΕ σε συνδυασμό

με νέες μορφές οργάνωσης και λειτουργίας. Συνεπώς, η τεχνολογία αποτελεί τον καταλύτη ριζοσπαστικών μετασχηματισμών των διαδικασιών, των οργανωτικών δομών, των δραστηριοτήτων, των στόχων των Δημόσιων Οργανισμών και του τρόπου επικοινωνίας τους με τους πολίτες και τις επιχειρήσεις, που βαθμιαία οδηγούν στη δημιουργία νέων λειτουργικών μοντέλων ηλεκτρονικής διακυβέρνησης, παρέχοντας αρκετά οφέλη τόσο στο δημόσιο τομέα όσο και στους πολίτες και τις επιχειρήσεις.

Η ανάπτυξη του ρόλου της ηλεκτρονικής διακυβέρνησης συνεισφέρει στην αποδοτικότερη αλληλεπίδραση μεταξύ δημόσιων υπηρεσιών και πολιτών με τη χρήση αυτοματοποιημένων διαδικασιών, απλοποιώντας σημαντικά τις υπάρχουσες υπηρεσίες του κράτους που παρέχονται στους πολίτες και τις επιχειρήσεις. Επιπρόσθετα, παρέχεται η δυνατότητα αναβάθμισης των εφαρμογών και των υπηρεσιών που σχετίζονται με τις εκπαιδευτικές και ερευνητικές δραστηριότητες. Οι εφαρμογές της ηλεκτρονικής διακυβέρνησης αυξάνουν την αποδοτικότητα και την αποτελεσματικότητα των δημόσιων υπαλλήλων, καθώς μειώνεται δραστικά ο χρόνος και το κόστος των υπηρεσιών προς τους πολίτες σε σχέση με τις παλαιότερες διαδικασίες. Το γεγονός αυτό οφείλεται στην άντληση και επεξεργασία πληροφοριών και δεδομένων από φορείς δημόσιας διοίκησης μέσα από τη χρήση κοινών πηγών.

Τα οφέλη ωστόσο αφορούν άμεσα και τον πολίτη, διότι η παροχή ηλεκτρονικών υπηρεσιών από το κράτος και τις επιχειρήσεις είναι ποιοτικότερη, καθώς δίνεται η δυνατότητα για πρόσβαση στις υπηρεσίες 24 ώρες την ημέρα, είναι δυνατή η συμπλήρωση φορμών για τη διεκπεραίωση αιτημάτων, αλλά παράλληλα δεν απαιτείται η φυσική του παρουσία προκειμένου να ολοκληρωθούν όλες οι διαδικασίες. Έτσι, η μείωση του χρόνου που απαιτείται για την ολοκλήρωση διαδικασιών είναι δεδομένη, ενώ η εξυπηρέτηση γίνεται γρηγορότερη, καλύτερη και πιο πλήρης, αφού ο πολίτης έχει καθολικό έλεγχο της συναλλαγής.

Πέρα από τους πολίτες, η ηλεκτρονική διακυβέρνηση είναι επωφελής και για τη βιωσιμότητα και λειτουργία των επιχειρήσεων. Η διεκπεραίωση των περισσότερων συναλλαγών τους με το δημόσιο, όπως εγγραφές σε επιμέρους τομείς, λήψη διαφόρων πιστοποιητικών από δημόσιους φορείς, υποβολή δηλώσεων και πραγματοποίηση πληρωμών, είναι άμεση και αποτελεσματική μειώνοντας το κόστος και τον χρόνο, συνεισφέροντας στην καταπολέμηση του φαινομένου της γραφειοκρατίας.

- ***<u>Κατηγορίες υπηρεσιών ΗΔ</u>***

Το φάσμα δραστηριοποίησης των ηλεκτρονικών υπηρεσιών είναι ιδιαιτέρως ευρύ, όμως τρεις διαφορετικές κατηγορίες περιεχομένων ξεχωρίζουν, ανάλογα με τη σχέση αλληλεπίδρασης των οντοτήτων που συμμετέχουν. Πρόκειται για τις υπηρεσίες τύπων «Κυβέρνηση-προς-Κυβέρνηση», «Κυβέρνηση-προς-Επιχειρήσεις» και «Κυβέρνηση-προς-Πολίτες». Μερικοί ερευνητές αναγνωρίζουν και έναν τέταρτο τομέα υπηρεσιών ΗΔ, ο οποίος είναι γνωστός ως «Κυβέρνηση-προς-Εργαζομένους». Ωστόσο, επειδή οι συγκεκριμένες διεργασίες που αφορούν το προαναφερθέν είδος υπηρεσιών πραγματοποιούνται εντός του ίδιου δημόσιου τομέα, μπορούν να θεωρηθούν υποσύνολο των «Κυβέρνηση-προς-Κυβέρνηση» υπηρεσιών. Συγκεκριμένα:

- **Κυβέρνηση-προς-Κυβέρνηση:** Οι υπηρεσίες τύπου «Κυβέρνηση-προς-Κυβέρνηση» αποτελούν τη «ραχοκοκαλιά» της ηλεκτρονικής διακυβέρνησης. Ερευνητές [2] προτείνουν οι κυβερνήσεις, τόσο σε εθνικό όσο και σε τοπικό επίπεδο διοίκησης, να βελτιώσουν και να αναβαθμίσουν τα εσωτερικά συστήματα και τις διαδικασίες προκειμένου να επιτευχθούν ηλεκτρονικές συναλλαγές με τους πολίτες και τις επιχειρήσεις. Οι υπηρεσίες αυτού του τύπου περιλαμβάνουν την ανταλλαγή πληροφοριών και δεδομένων μεταξύ των κυβερνητικών φορέων σε εθνική, περιφερειακή και τοπική κάλυψη.
- **Κυβέρνηση-προς-Επιχειρήσεις:** Οι ηλεκτρονικές υπηρεσίες τύπου «Κυβέρνηση-προς-Επιχειρήσεις» αποτελούν σημαντικό κομμάτι της ηλεκτρονικής διακυβέρνησης εξαιτίας του υψηλού ανταγωνισμού στον ιδιωτικό τομέα και της προοπτικής για μείωση του κόστους μέσα από τις ανανεωμένες υπηρεσίες που παρέχουν οι επιχειρήσεις. Οι υπηρεσίες αυτές περιλαμβάνουν την ηλεκτρονική ανταλλαγή πληροφοριών ανάμεσα στις κυβερνήσεις και τις επιχειρήσεις χρησιμοποιώντας το διαδίκτυο, έτσι ώστε η συνεργασία και η επικοινωνία μεταξύ αυτών να είναι πιο αποτελεσματική.
- **Κυβέρνηση-προς-Πολίτες:** Η παροχή υπηρεσιών τύπου «Κυβέρνηση-προς-Πολίτες» έχει ως βασικό στόχο την ταχύτερη και πιο αποτελεσματική διεκπεραίωση αιτημάτων που υποβάλλονται από τους πολίτες στις δημόσιες υπηρεσίες (όπως, η έκδοση διαφόρων πιστοποιητικών, πληρωμή τελών, φόρων κ.λπ.), αλλά με σημαντικότερο πλεονέκτημα αυτό της πρόσβασης σε πληροφορίες δημόσιου χαρακτήρα. Συγκεκριμένα, ο πολίτης μπορεί από μία και μόνο πύλη να επεξεργαστεί οποιοδήποτε αίτημά του στο πλαίσιο ενός ιδιαίτερα μεγάλου εύρους παρεχόμενων δημόσιων υπηρεσιών, χωρίς να απαιτείται η πρόσβαση σε ξεχωριστούς δημόσιους φορείς. Έτσι, η αμεσότητα που χαρακτηρίζει την ολοκλήρωση των προαναφερθέντων διαδικασιών συμβάλλει – εμμέσως αλλά καθοριστικά – στη συμμετοχή των πολιτών στις διοικητικές διαδικασίες και στη λήψη αποφάσεων, καθιστώντας τις υπηρεσίες «Κυβέρνηση-προς-Πολίτες» πρωτευούσης σημασίας.

2.2 Υφιστάμενη κατάσταση στην Ηλεκτρονική Διακυβέρνηση

2.2.1 Η Ηλεκτρονική Διακυβέρνηση στην Ευρώπη

Τα τελευταία χρόνια, οι Τεχνολογίες Πληροφορικής και Επικοινωνιών έχουν συνεισφέρει αρκετά στη βελτίωση των κοινωνικοοικονομικών σχέσεων μεταξύ των κυβερνήσεων, των πολιτών και των επιχειρήσεων. Το γεγονός αυτό οφείλεται στην ανάδειξη της ηλεκτρονικής διακυβέρνησης αλλά και στη σχεδίαση και ανάπτυξη κοινών μοντέλων διακυβέρνησης ανάμεσα στα κράτη μέλη, με στόχο την καθολική παροχή δημόσιων υπηρεσιών μέσω του διαδικτύου, προσφέροντας διαφάνεια και πλήρη έλεγχο του κυβερνητικού έργου. Τα μοντέλα αυτά περιλαμβάνουν όχι μόνο την απλή παροχή πληροφοριών ή πραγματοποίηση οικονομικών συναλλαγών, αλλά και τη συμμετοχή των πολιτών στις διαδικασίες ηλεκτρονικής δημοκρατίας.

Η εξέλιξη της τεχνολογίας σε παγκόσμιο επίπεδο είναι δεδομένη, όμως οι ρυθμοί ανάπτυξης των κρατών μελών της Ευρωπαϊκής Ένωσης (ΕΕ) είναι διαφορετικοί, καθιστώντας ουσιαστική την υιοθέτηση κοινών πολιτικών προκειμένου να υπάρχει ισορροπημένη ανάπτυξη των χωρών. Η Ευρωπαϊκή Επιτροπή έχει ως βασικό της στόχο τη διάδοση της ηλεκτρονικής διακυβέρνησης στα κράτη μέλη της ΕΕ και για τον λόγο αυτόν υπεύθυνος για την προώθησή της είναι ο Αντιπρόεδρος των Διοικητικών Υποθέσεων. Δύο από τα βασικότερα προγράμματα που εφαρμόζουν την κοινή στρατηγική είναι το IDABC και το ISA.

- ***IDABC***

Το IDABC [3] (Interoperable Delivery of european egovernment services to public Administrations, Businesses and Citizens) ήταν ένα πρόγραμμα της ΕΕ που ξεκίνησε το 2004 με σκοπό την προώθηση επωφελούς χρήσης των Τεχνολογιών Πληροφορικής και Επικοινωνιών μεταξύ των κρατών μελών. Στόχος του συγκεκριμένου προγράμματος ήταν η χρήση τεχνολογικών μέσων για την ανάπτυξη ηλεκτρονικών πλατφορμών παροχής υπηρεσιών δημόσιου χαρακτήρα για τους πολίτες και τις επιχειρήσεις, βελτιώνοντας την αποτελεσματικότητα της συνεργασίας ανάμεσα στις ευρωπαϊκές δημόσιες διοικήσεις και μετατρέποντας την Ευρώπη σε ένα ελκυστικό μέρος για να ζήσει, να εργαστεί και να επενδύσει ο καθένας.

Για να επιτευχθεί η διαλειτουργικότητα, σύμφωνα με το IDABC, αναπτύχθηκαν λύσεις και παρήχθησαν δομές που επέτρεπαν στις εθνικές και ευρωπαϊκές διοικήσεις να επικοινωνούν ηλεκτρονικά, καθώς σύγχρονες δημόσιες υπηρεσίες προσφέρονταν στις επιχειρήσεις και τους πολίτες. Το πρόγραμμα παρείχε επίσης την οικονομική υποστήριξη σε έργα που υιοθετούσαν τις απαιτήσεις της ευρωπαϊκής πολιτικής, ενώ βελτίωναν παράλληλα και τη συνεργασία των διοικήσεων των κρατών μελών.

Χρησιμοποιώντας τις Τεχνολογίες Πληροφορικής και Επικοινωνιών, αναπτύσσοντας κοινές λύσεις και υπηρεσίες και παρέχοντας παράλληλα μια πλατφόρμα για την ανταλλαγή πρακτικών μεταξύ των δημόσιων διοικήσεων, το IDABC συνεισέφερε στην πρωτοβουλία i2010 που αναβάθμισε σε μεγάλο βαθμό τον ευρωπαϊκό δημόσιο τομέα. Στις 31 Δεκεμβρίου 2009, το IDABC ολοκλήρωσε τον κύκλο του, με το πρόγραμμα ISA να το διαδέχεται.

- ***ISA***

Το πρόγραμμα ISA [4] (Interoperability Solutions for european public Administrations) είχε διάρκεια πέντε ετών (από το 2010 έως και το 2015) και αποτελεί τη συνέχεια του προγράμματος IDABC, όπως αυτό εγκρίθηκε από την Ευρωπαϊκή Βουλή τον Σεπτέμβριο του 2008. Το πρόγραμμα αυτό εστίαζε στην ανάπτυξη υποστηρικτικών συστημάτων που βελτίωναν την αλληλεπίδραση των δημόσιων διοικήσεων και την εφαρμογή των πολιτικών και δραστηριοτήτων της ΕΕ. Επιπρόσθετα, υποστήριζε τα διασυνοριακά έργα μεγάλης εμβέλειας υπό την στέγη του προγράμματος Πολιτικής Υποστήριξης των Τεχνολογιών Πληροφορικής και Επικοινωνιών.

- ***<u>Στρατηγική της Λισαβόνας</u>***

Τον Μάρτιο του 2000, τα κράτη μέλη της ΕΕ θέσπισαν μια δεκαετούς διάρκειας στρατηγική για να μετατρέψουν την ΕΕ στην «πιο ανταγωνιστική και δυναμική ένωση, μια κοινωνία βασισμένη στη γνώση, με βιώσιμη οικονομική ανάπτυξη, με όλο και περισσότερες ευκαιρίες εργασίας και ευρύτερη πολιτική συνοχή»[5]. Ο συγκεκριμένος στόχος συμπληρώθηκε προσθέτοντας μια περιβαλλοντολογική και βιώσιμης ανάπτυξης διάσταση, όπως αποφασίστηκε στο Γκέτεμποργκ έναν χρόνο αργότερα.

Η Στρατηγική της Λισαβόνας αποτέλεσε δέσμευση των ευρωπαϊκών κυβερνήσεων να συνεισφέρουν όλες τους τις προσπάθειες σε έναν γενικό στόχο: να επέλθει οικονομική, κοινωνική και περιβαλλοντολογική ανανέωση στην Ευρώπη. Σύμφωνα με την στρατηγική αυτή, μια ισχυρή οικονομία θα οδηγούσε στη δημιουργία θέσεων εργασίας μαζί με τις κοινωνικές και περιβαλλοντολογικές πολιτικές που θα εξασφάλιζαν βιώσιμη ανάπτυξη και κοινωνική σύμπτυξη.

Στη Λισαβόνα τέθηκαν οι πυλώνες που θα αποτελούσαν τις κατευθυντήριες οδηγίες για την αύξηση της ανταγωνιστικότητας. Ορισμένες από τις οδηγίες κινήθηκαν στο πλαίσιο υποστήριξης της ηλεκτρονικής διακυβέρνησης και αυτές ήταν οι παρακάτω:

- Πρώτος στόχος ήταν η δημιουργία μιας ψηφιακής οικονομίας που θα βασιζόταν στη γνώση και θα αποτελούνταν από νέα αγαθά και υπηρεσίες, συνιστώντας την κινητήρια δύναμη για την οικονομική ανάπτυξη, ανταγωνιστικότητα και δημιουργία θέσεων απασχόλησης.
- Με χρήση των Τεχνολογιών Πληροφορικής και Επικοινωνιών, η συγκρότηση ενός ενιαίου ευρωπαϊκού χώρου κρίθηκε απαραίτητη προκειμένου οι πολίτες να έχουν πρόσβαση σε υποδομές επικοινωνίας, κατάλληλες για την διεκπεραίωση όσο το δυνατόν περισσότερων αιτημάτων τους και κάλυψη των αναγκών τους. Κάθε πολίτης όφειλε να διαθέτει τις απαραίτητες ικανότητες και δεξιότητες που απαιτούνταν στην καθημερινότητά του ώστε να επωφελούνταν από τη διαμόρφωση της Κοινωνίας της Πληροφορίας (ΚτΠ). Το διαδίκτυο αποτελούσε ήδη ένα ευρέως χρησιμοποιούμενο και προσιτό μέσο, διευρύνοντας σε μεγάλο βαθμό τις δραστηριότητες των επιχειρήσεων και των πολιτών. Για την επίτευξη αυτού του στόχου απαιτούνταν αρκετές προϋποθέσεις, όπως η μείωση του κόστους πρόσβασης και χρήσης του διαδικτύου, η συστηματική χρήση του στα εκπαιδευτικά ιδρύματα και η κατάλληλη κατάρτιση των εκπαιδευτικών, η διασφάλιση της πρόσβασης των πολιτών στις ιστοσελίδες των δημόσιων φορέων, κ.ά.

- ***<u>eEurope 2002</u>***

Προκειμένου να ενισχυθεί η οικονομική πολιτική της Ευρωπαϊκής Ένωσης όπως προβλεπόταν από την Στρατηγικής της Λισαβόνας, θεσπίστηκε το σχέδιο δράσης eEurope 2002 [6] με τρεις βασικούς άξονες:

- <u>Φθηνότερο, ταχύτερο και ασφαλές διαδίκτυο:</u> Το 1998, παρά την απελευθέρωση των τηλεπικοινωνιακών υπηρεσιών, το διαδίκτυο δεν

αποτελούσε ένα προσιτό αγαθό. Για να την εξάπλωσή του, διαμορφώθηκε ένα νέο πλαίσιο ηλεκτρονικών επικοινωνιών που καθόριζε τις γενικές κατευθύνσεις πρόσβασης και αδειοδότησης, μεγαλώνοντας τον ανταγωνισμό στα τοπικά δίκτυα πρόσβασης και επέτρεπε τη δημιουργία νέων φορέων εκμετάλλευσης τηλεπικοινωνιών. Η οικονομικότερη και ταχύτερη πρόσβαση στο διαδίκτυο προσέφερε επίσης σημαντικά οφέλη στις επιστημονικές κοινότητες. Διατέθηκαν τα κατάλληλα χρηματοδοτικά μέσα για την διεκπεραίωση ερευνών βάσει του προγράμματος «Τεχνολογίες της Κοινότητας της Πληροφορίας», ενώ τα πανεπιστήμια απέκτησαν ενδοδίκτυα (intranets) υψηλών ταχυτήτων για αμεσότερη ανταλλαγή πληροφοριών.

- Επένδυση σε άτομα και δεξιότητες: Με το συγκεκριμένο σχέδιο δόθηκε έμφαση στη μετάβαση της νεολαίας στην ψηφιακή εποχή, καθώς τα σχολεία συνδέθηκαν με ερευνητικά δίκτυα, το διδακτικό προσωπικό ήταν καταρτισμένο ως προς τις νέες ψηφιακές τεχνολογίες και στα σχολικά προγράμματα ενσωματώθηκαν νέες μέθοδοι εκμάθησης της χρήσης των ΤΠΕ. Επιπρόσθετα, η εκπαίδευση των εργαζομένων όλων των ειδικοτήτων στις ψηφιακές τεχνολογίες σε συνάρτηση με τη σύσταση ευρωπαϊκών πιστοποιητικών βασικών δεξιοτήτων οδήγησε στη συμμετοχή όλων των πολιτών στην οικονομία της γνώσης και εξασφαλίστηκε η πρόσβαση στις τεχνολογίες πληροφοριών, σχεδιάζοντας παράλληλα προϊόντα που απευθύνονταν σε άτομα με ειδικές ανάγκες.
- Τόνωση της χρήσης του διαδικτύου: Ένας από τους βασικότερους παράγοντες επιτάχυνσης της διάδοσης του διαδικτύου αποτέλεσε το ηλεκτρονικό εμπόριο. Κρίθηκε αναγκαία η διαμόρφωση προτάσεων νομοθετικού περιεχομένου για τη διασφάλιση των αγορών με τη χρήση ηλεκτρονικών υπηρεσιών αλλά και την ενίσχυση της εμπιστοσύνης των καταναλωτών στα μέσα ηλεκτρονικού εμπορίου. Εκτός αυτού, η πρόσβαση στις δημόσιες υπηρεσίες, η υγειονομική περίθαλψη και συστήματα μεταφορών αποκτούν ηλεκτρονικό χαρακτήρα, προτρέποντας τους Ευρωπαίους να ενσωματώσουν τη δυναμική των τεχνολογιών και της πληροφορικής στην καθημερινότητά τους.

Στις αρχές του 2003, η Ευρωπαϊκή Επιτροπή δημοσιοποίησε μια αναφορά πεπραγμένων του σχεδίου eEurope 2002, χαρακτηρίζοντάς το σε ένα γενικό πλαίσιο επιτυχημένο και προτείνοντας το επόμενο βήμα για την ανάπτυξη της κοινωνίας της πληροφορίας στην Ευρώπη: το σχέδιο δράσης eEurope 2005.

- ***eEurope 2005***

Το σχέδιο δράσης eEurope 2005 [7] είχε ως βασικό σκοπό την ενίσχυση της παραγωγικότητας των οικονομικών δραστηριοτήτων, ενισχύοντας την υποδομή ευρυζωνικών επικοινωνιών. Μέχρι το 2005, η προσέγγιση που υιοθετήθηκε αφορούσε τους εξής άξονες:

- Σύγχρονες δικτυακές δημόσιες υπηρεσίες: Η Ηλεκτρονική Διακυβέρνηση (eGovernment), μέσω της χρήσης ευρυζωνικών δικτύων, επέτρεψε την πρόσβαση όλων των πολιτών στις δημόσιες διοικήσεις και τις παρεχόμενες

ηλεκτρονικές υπηρεσίες. Επιπρόσθετα, η εκπαίδευση εκσυγχρονίστηκε μέσω της εφαρμογής του σχεδίου δράσης της ηλεκτρονικής μάθησης (e-learning), προσφέροντας πρόσβαση στο διαδίκτυο σε όλα τα σχολεία και τα πανεπιστήμια, με άμεση συνεισφορά και στα διευρωπαϊκά ερευνητικά προγράμματα. Στο συγκεκριμένο σχέδιο αναπτύχθηκε και ο τομέας της υγείας μέσω της αναβάθμισης των ηλεκτρονικών υπηρεσιών και την εγκατάσταση δικτύου πληροφοριών υγείας μεταξύ των σημείων περίθαλψης.

- Δυναμικό περιβάλλον για το ηλεκτρονικό επιχειρείν (e-business): Η ανασκόπηση της σχετικής νομοθεσίας και η εγκατάσταση από την Ευρωπαϊκή Επιτροπή δικτύου υποστήριξης των μικρών και μεσαίων επιχειρήσεων εξασφάλισαν τη διάδοση του ηλεκτρονικού εμπορίου και την αναδιάρθρωση των επιχειρηματικών διεργασιών.
- Ασφαλής υποδομή πληροφοριών: Η ασφάλεια των δικτύων αποτέλεσε βασικό στόχο του προγράμματος eEurope 2005 και αυτό επετεύχθη συγκροτώντας επιχειρησιακή ομάδα υπεύθυνη για την ασφάλεια στον κυβερνοχώρο και την προστασία των προσωπικών δεδομένων, καθώς και τη διερεύνηση των δυνατοτήτων ασφαλούς ανταλλαγής πληροφοριών μεταξύ δημόσιων υπηρεσιών.
- Γενικευμένη διάθεση ευρυζωνικής πρόσβασης: Η χρήση ευρυζωνικών δικτύων συνεισέφερε στη διάδοση του περιεχομένου των δημόσιων υπηρεσιών σε διάφορες τεχνολογικές πλατφόρμες, χρησιμοποιώντας ένα νέο πλαίσιο κανονιστικών ρυθμίσεων που διέπουν την πολιτική σε ζητήματα ραδιοφάσματος.

Το σχέδιο eEurope 2005 περιείχε σαφείς οδηγίες για την ενίσχυση της ηλεκτρονικής διακυβέρνησης και τα αποτελέσματά του χαρακτηρίστηκαν ενθαρρυντικά σε έκθεση που παρουσιάστηκε από την Ευρωπαϊκή Επιτροπή στις 18 Φεβρουαρίου 2004. Ωστόσο, παρά τη σημαντική πρόοδο, παρέμειναν μεγάλες διαφορές μεταξύ των κρατών μελών τόσο σε ζητήματα ηλεκτρονικής διακυβέρνησης και εμπορίου όσο και σε θέματα ασφάλειας. Οι αδυναμίες που εντοπίστηκαν δεν επηρέασαν καθολικά την εφαρμογή του προγράμματος αλλά ελήφθησαν υπόψη στο πλαίσιο της πρωτοβουλίας i2010.

- ***i2010***

Το σχέδιο δράσης i2010 [8] αποτέλεσε το νέο στρατηγικό πλαίσιο της Ευρωπαϊκής Επιτροπής που καθόριζε τις γενικές κατευθύνσεις της κοινωνίας της πληροφορίας και των μέσων ενημέρωσης. Η επιτροπή έθεσε προτεραιότητα στην ανάπτυξη των παρακάτω αξόνων:

- Ενιαίος ευρωπαϊκός χώρος πληροφοριών: Η δημιουργία ενιαίου χώρου πληροφοριών θα βοηθούσε στην εξάπλωση των υπηρεσιών υψηλής ταχύτητας στην Ευρώπη, στη διάθεση νέων διαδικτυακών περιεχομένων αλλά και στην ενίσχυση της ασφάλειας του διαδικτύου. Για την επίτευξη του στόχου αυτού, το σχέδιο προέβλεπε την αναθεώρηση του κανονιστικού πλαισίου για τις ηλεκτρονικές επικοινωνίες και τον καθορισμό στρατηγικής για μια ασφαλή

ευρωπαϊκή κοινωνία της πληροφορίας. Η παροχή στήριξης στη δημιουργία περιεχομένου, όπως τα προγράμματα «eLearning» και «eContentplus», θεωρήθηκε αναγκαία για τη διαμόρφωση του χώρου πληροφοριών ως ολοκληρωμένη οντότητα.

- Καινοτομία και επενδύσεις στην έρευνα: Ο τομέας των Τεχνολογιών Πληροφορικής και Επικοινωνιών είχε περιθώρια βελτίωσης προκειμένου να μειωθεί η «απόσταση» της Ευρώπης από τους κύριους ανταγωνιστές της. Η μείωση της διαφοράς πραγματοποιήθηκε με την αύξηση των επενδύσεων στον τομέα των ΤΠΕ, τη δρομολόγηση πρωτοβουλιών έρευνας και τον ορισμό πολιτικών στον τομέα του ηλεκτρονικού εμπορίου, ώστε να ξεπεραστούν οι τεχνολογικοί, διαρθρωτικοί και νομικοί φραγμοί κυρίως στη λειτουργία των μικρομεσαίων επιχειρήσεων.
- Κοινωνική ένταξη, βελτίωση των δημόσιων υπηρεσιών και της ποιότητας ζωής: Η Ευρωπαϊκή Επιτροπή αποσκοπούσε στην ενίσχυση της κοινωνικής, οικονομικής και εδαφικής συνοχής μέσω της δημιουργίας μιας ευρωπαϊκής κοινωνίας της πληροφορίας. Προέτρεψε, λοιπόν, στη διάδοση της ιδέας της ηλεκτρονικής προσβασιμότητας, εγκρίνοντας παράλληλα σχέδιο δράσης ώστε οι δημόσιες υπηρεσίες να αναπτύξουν ένα σημαντικό υπόβαθρο που αφορούσε την ηλεκτρονική διοίκηση. Όσον αφορά την ποιότητα ζωής, δρομολογήθηκαν τρεις σημαντικές πράξεις, όπως η περίθαλψη ατόμων τρίτης ηλικίας, η κατασκευή «ευφυών αυτοκινήτων» και η δημιουργία ψηφιακών βιβλιοθηκών.
- Διακυβέρνηση: Τα κράτη μέλη δεσμεύτηκαν από τη δράση i2010 να μεταρρυθμίσουν τις τρέχουσες νομοθεσίες τους για να εναρμονιστούν με τα νέα κανονιστικά πλαίσια που αφορούσαν την ψηφιακή σύγκλιση. Εκτός αυτού, υποχρεώθηκαν να διαθέσουν μεγαλύτερο ποσοστό των εθνικών τους δαπανών στη δημιουργία σύγχρονων και διαλειτουργικών δημόσιων υπηρεσιών αλλά και να αναπτύξουν την κοινωνία της πληροφορίας σε εθνική κλίμακα.

- ***Σχέδιο δράσης 2011-2015***

Τον Νοέμβριο του 2009 στο Μάλμε της Σουηδίας, συγκροτήθηκε το Σχέδιο Δράσης 2011-2015 [9] ως μέρος της στρατηγικής «Ευρώπη 2020» που αποσκοπούσε στην ανασυγκρότηση του ευρωπαϊκού χώρου και στη δημιουργία μιας οικονομικής πραγματικότητας βασισμένης στη γνώση (βιώσιμη και χωρίς αποκλεισμούς). Οι προτεραιότητες του προγράμματος που είχαν τεθεί είναι οι παρακάτω:

- Ενδυνάμωση των πολιτών και των επιχειρήσεων: Η σχεδίαση υπηρεσιών που βασίζονται στις ανάγκες των πολιτών αποτέλεσε την πυξίδα του προγράμματος, ενώ η συνεργατική παραγωγή υπηρεσιών προσέδωσε αρκετά στη συνεργασία των διοικητικών διευθύνσεων. Ακόμη, επαναχρησιμοποιήθηκαν πληροφορίες του δημόσιου τομέα, προτρέποντας τους πολίτες και τις επιχειρήσεις να συμμετάσχουν στη διαμόρφωση των πολιτικών.
- Ενίσχυση της κινητικότητας στην ενιαία αγορά: Προκειμένου να επιτευχθεί η οικονομική ανάπτυξη στην Ευρώπη, και ιδιαίτερα εν μέσω της κρίσης που

υπήρχε, χρειάζονταν δράσεις οι οποίες θα επέτρεπαν στους πολίτες και τις επιχειρήσεις εντός της ηπείρου να δραστηριοποιούνται με τους ίδιους κανόνες και τις ίδιες πολιτικές σαν μία ενιαία οντότητα. Ήταν σημαντική, επομένως, η δημιουργία απρόσκοπτων υπηρεσιών για τις επιχειρήσεις, η προσωπική κινητικότητα, αλλά και η εφαρμογή διασυνοριακών υπηρεσιών και νέων υπηρεσιών σε επίπεδο Ευρωπαϊκής Ένωσης που θα οδηγούσε με σταθερό ρυθμό στην ενοποίηση της ευρωπαϊκής αγοράς.

- Αποδοτικότητα και αποτελεσματικότητα: Το σχέδιο δράσης 2011-2015 συμπεριλάμβανε και σημαντικές κατευθύνσεις προς τη μεγιστοποίηση της αποδοτικότητας και της αποτελεσματικότητας, τόσο σε επίπεδο επιχειρήσεων όσο και σε επίπεδο διοικητικών υπηρεσιών, όπως τη βελτίωση των οργανωτικών διαδικασιών, τη μείωση του διοικητικού φόρτου και την εφαρμογή του θέματος της «πράσινης κυβέρνησης».
- Βασικοί ενεργοποιητές και προϋποθέσεις: Οι καινοτόμες δράσεις στην ηλεκτρονική διακυβέρνηση μαζί με τις ανοιχτές προδιαγραφές για διαλειτουργικότητα ήταν η κινητήριος δύναμη ώστε να ενεργοποιηθούν οι επιχειρησιακοί και διοικητικοί παράγοντες. Αφήνοντας, δηλαδή, τις χειριστικές διαδικασίες και αναπτύσσοντας νέα σχέδια και δράσεις με τη βοήθεια των τεχνολογικών μέσων, η Ευρώπη προσπάθησε να ανασυγκροτηθεί και να αναγεννηθεί σε μία ισχυρή οικονομική, πολιτική και τεχνολογική παρουσία.

- ***Σχέδιο δράσης 2016-2020***

Σύμφωνα με την στρατηγική «Ευρώπη 2020» [10], μέχρι την ολοκλήρωσή της, οι δημόσιοι διοικητικοί οργανισμοί θα πρέπει να είναι ανοιχτοί, αποδοτικοί και αποτελεσματικοί, παρέχοντας σε όλους τους ευρωπαίους πολίτες και σε όλες τις επιχειρήσεις φιλικές και εξατομικευμένες ψηφιακές υπηρεσίες. Επιπρόσθετα, θα εφαρμόζεται καινοτόμος σχεδιασμός και υλοποίηση ηλεκτρονικών υπηρεσιών, ανάλογων των αναγκών και των απαιτήσεων πολιτών και επιχειρήσεων. Οι προτεραιότητες που τέθηκαν για την εφαρμογή της παραπάνω πολιτικής είναι οι εξής:

- Εκσυγχρονισμός της δημόσιας διοίκησης με ΤΠΕ: Οι δημόσιες αρχές οφείλουν να μετασχηματίσουν τις υποστηρικτικές τους υπηρεσίες, ενώ παράλληλα να σχεδιάσουν εκ νέου τις υφιστάμενες διαδικασίες, έχοντας σαν γνώμονα την κοινή ερμηνεία της διαλειτουργικότητας σε ολόκληρη την Ευρωπαϊκή Ένωση. Η Ευρωπαϊκή Επιτροπή θα επιτρέψει τη μετάβαση των μελών της προς τις πλήρως ηλεκτρονικές δημόσιες συμβάσεις μέχρι τα τέλη του 2019, καθώς και θα διασφαλίσει την ανάπτυξη της υποδομής διασυνοριακών ψηφιακών συναλλαγών. Η χρήση ηλεκτρονικής ταυτοποίησης και η αναθεώρηση του ευρωπαϊκού πλαισίου διαλειτουργικότητας θα αποτελέσει σημαντικό βήμα ενόψει του ψηφιακού μετασχηματισμού.
- Διευκόλυνση της διασυνοριακής κινητικότητας με διαλειτουργικές, ψηφιακές δημόσιες υπηρεσίες: Μέχρι το 2017, είχαν προγραμματιστεί η δημιουργία μιας ενιαίας ψηφιακής πύλης, η διασύνδεση όλων των μητρώων επιχειρήσεων των

κρατών μελών, η υποβολή νομοθετικής πρότασης σχετικά με την εφαρμογή ενιαίου μηχανισμού για την καταχώρηση και την καταβολή του ΦΠΑ, η δημιουργία ειδικής πύλης για την καταγραφή επαγγελματικής κινητικότητας του δικτύου αλλά και η ανάπτυξη μίας ανεξάρτητης διασυνοριακής υπηρεσίας υγείας.

- Διευκόλυνση της ψηφιακής αλληλεπίδρασης μεταξύ των διοικήσεων και των πολιτών-επιχειρήσεων για την παροχή δημόσιων υπηρεσιών υψηλής ποιότητας: Στο πλαίσιο των προτεραιοτήτων που έχουν τεθεί από την επιτροπή, πραγματοποιείται μετασχηματισμός των ιστοτόπων της για την υποστήριξη της ενίσχυσης της δέσμευσης και της συμμετοχής των επιχειρήσεων και των πολιτών σε προγράμματα και διαδικασίες χάραξης πολιτικών της Ευρωπαϊκής Ένωσης. Επιπροσθέτως, έως τα τέλη του 2020 έχει προβλεφθεί η ολοκλήρωση και υιοθέτηση υποδομής χωρικών δεδομένων, όπως χαρακτηριστικά αναφέρεται στην οδηγία INSPIRE[11].

Δύο χώρες που ακολούθησαν αρκετές από τις δράσεις των παραπάνω σχεδίων είναι η Εσθονία και το Ηνωμένο Βασίλειο:

Εσθονία

Η Εσθονία ξεχωρίζει ως μία από τις χώρες που έχει εφαρμόσει σχεδόν πλήρως την ηλεκτρονική διακυβέρνηση σε εθνικό επίπεδο [12]. Το γεγονός ότι κατέχει υψηλές θέσεις στους πίνακες με τους σχετικούς δείκτες, την κάνουν λαμπρό παράδειγμα εφαρμογής των πρακτικών της ηλεκτρονικής διακυβέρνησης. Πιο συγκεκριμένα, στην Εσθονία όλες οι δραστηριότητες που αφορούν τον δημόσιο τομέα στη χώρα διεκπεραιώνονται μέσω των ηλεκτρονικών υπηρεσιών. Εξαιρέσεις σε αυτόν τον κανόνα αποτελούν οι περιπτώσεις διαδικασιών που αφορούν τον γάμο, το διαζύγιο και την αγοραπωλησία ακινήτων που απαιτούν τη φυσική παρουσία των πολιτών. Επακόλουθα, όλες αυτές οι διευκολύνσεις οδηγούν στην αυξημένη ικανοποίηση των πολιτών λόγω της άμεσης εξυπηρέτησής τους, αλλά ταυτόχρονα και στην καλύτερη λειτουργία του δημόσιου τομέα λόγω μειωμένης γραφειοκρατίας και εξοικονόμησης πόρων. Την εξαγωγή των απαιτήσεων του συστήματος ηλεκτρονικής διακυβέρνησης και τον σχεδιασμό του αναλαμβάνει ο κρατικός τομέας, ενώ η υλοποίησή του γίνεται από τον ιδιωτικό τομέα. Ωστόσο, είτε ο δημόσιος είτε ο ιδιωτικός τομέας μπορεί να αναλάβει τη λειτουργία ενός τέτοιου κρίσιμου συστήματος, ανάλογα φυσικά με τις απαιτήσεις του και τον αντίστοιχο σχεδιασμό του.

Απαραίτητο «εργαλείο» – «κλειδί» για τη χρήση των ηλεκτρονικών υπηρεσιών που παρέχονται από το κράτος της Εσθονίας είναι η κάρτα – ταυτότητα του πολίτη που εκδίδεται από το Εθνικό Σύστημα Ταυτοτήτων. Λόγω του ενσωματωμένου μικροκυκλώματος (chip) που φέρει (και άρα της ασφάλειας που προσφέρει), η κάρτα αυτή χρησιμοποιείται ευρέως ως εθνική ταυτότητα, ταξιδιωτικό έγγραφο στην Ε.Ε., ως κάρτα ασφάλισης, κάρτα μεταφοράς για τη χρήση Μ.Μ.Μ., ως ψηφιακή υπογραφή, σε ηλεκτρονικές ψηφοφορίες και σε τραπεζικές συναλλαγές, κ.ά. Επιπρόσθετα, σημαντικό βάσει των ραγδαίων τεχνολογικών εξελίξεων στον τομέα των «έξυπνων» κινητών

τηλεφώνων (smartphones) είναι το γεγονός ότι η ταυτοποίηση των πολιτών μπορεί να γίνει και μέσω του κινητού τους τηλεφώνου. Τέλος, αξίζει να αναφερθεί και ο νέος θεσμός του "Service Owner" στο εσθονικό σύστημα που ορίζεται ως ένα άτομο μέσα σε έναν κρατικό οργανισμό που έχει την ευθύνη της διασφάλισης της ποιότητας των προσφερόμενων υπηρεσιών.

Σε όλα τα παραπάνω, όμως, θα πρέπει να λάβουμε σοβαρά υπόψη τις συνθήκες κάτω από τις οποίες σχεδιάστηκε και δημιουργήθηκε αυτό το τόσο πετυχημένο μοντέλο Ηλεκτρονικής Διακυβέρνησης. Η Εσθονία αποτελεί ένα σχετικά καινούριο κράτος αφού ανεξαρτητοποιήθηκε το 1991, και συνάμα μικρό καθώς ο πληθυσμός της δεν υπερβαίνει το 1,5 εκατομμύριο κατοίκους. Εκμεταλλευόμενη, έτσι, την ευκαιρία δόμησης του δημόσιου τομέα της από το μηδέν, χωρίς τις δυσλειτουργίες και τη γραφειοκρατία που εμφανίζουν άλλα κράτη, πέτυχε τον συνδυασμό δημόσιου και ιδιωτικού τομέα σε ένα – πλήρως σύγχρονο – ηλεκτρονικό σύστημα διακυβέρνησης.

Ηνωμένο Βασίλειο

Το Ηνωμένο Βασίλειο είναι χαρακτηριστικό παράδειγμα της εφαρμογής της ανοικτής Ηλεκτρονικής Διακυβέρνησης [12]. Συνέβαλε στην ίδρυση του "Open Government Partnership" το 2011 και πλέον εφαρμόζει το 3ο Εθνικό Σχέδιο Δράσης. Σύμφωνα με αυτό, υπάρχουν 5 βασικοί πυλώνες δράσεων που πρέπει να εφαρμόζονται: η πρόσβαση σε πληροφορίες, η καταπολέμηση της διαφθοράς, η συμμετοχή των πολιτών, τα ανοιχτά δεδομένα και η δημόσια λογοδοσία. Συνάμα με αυτό το πλαίσιο έχει δημοσιευτεί το «Πρότυπο Ψηφιακών Υπηρεσιών» που περιλαμβάνει 18 κριτήρια που μία υπηρεσία θα πρέπει να πληροί, ώστε να είναι άξια χρήσης από τους πολίτες και άρα να είναι πλέον διαθέσιμη στους τελευταίους. Το προαναφερθέν πρότυπο αποτελεί τον οδηγό των υπουργείων για τον σχεδιασμό, την υλοποίηση και την εφαρμογή των ηλεκτρονικών υπηρεσιών.

Άλλα σημεία στα οποία το Ηνωμένο Βασίλειο πρωτοπόρησε είναι ο ορισμός «Κυβερνητικού Διευθυντή Δεδομένων» και η άδεια χρήσης Ανοικτής Διακυβέρνησης στην εθνική υπηρεσία χαρτογράφησης που συνέβαλε στην επαναξιοποίηση χαρτογραφικών δεδομένων και στη διασύνδεση με άλλες κρατικές πηγές αντίστοιχων δεδομένων. Μία ακόμα καινοτομία που εφάρμοσε ο οργανισμός Εθνικών Αρχείων είναι η δημιουργία του πρώτου καταλόγου του δημόσιου τομέα με απώτερο στόχο τη μακροχρόνια διατήρηση των πληροφοριών σε ψηφιακή μορφή. Ωστόσο, επειδή είναι ξεκάθαρο ότι η παροχή τέτοιων διευκολύνσεων πρέπει να γίνεται με γνώμονα τους ίδιους τους πολίτες, τους δίνεται το δικαίωμα και παροτρύνονται να καταθέσουν τις απόψεις τους σχετικά με το σύστημα, τους κανονισμούς του, τους περιορισμούς του και τις αδυναμίες που μπορεί να έχει με σκοπό τη συνεχή εξέλιξη και βελτίωσή του. Σε ό,τι αφορά τους δημόσιους υπαλλήλους οι οποίοι είναι επιφορτισμένοι με την εξυπηρέτηση των πολιτών και έρχονται σε επαφή μαζί τους, έχει θεσπιστεί ένας «Κώδικας Συμπεριφοράς» που πρέπει να τηρείται καθολικά από όλους.

Τέλος, θα πρέπει να αναφερθούμε στην κυβερνητική πύλη[1] του Ηνωμένου Βασιλείου που συγκεντρώνει όλη τη δημόσια πληροφορία από περισσότερες από 400 ιστοσελίδες, μειώνοντας αισθητά τη γραφειοκρατία και την αναζήτηση πληροφοριών σε τεράστιο όγκο δεδομένων και βοηθώντας ουσιαστικά με τον τρόπο αυτό τους πολίτες. Για τη διασφάλιση της εξουσιοδοτημένης χρήσης των πληροφοριών αυτών αλλά και των υπόλοιπων παρεχόμενων υπηρεσιών μέσω της προαναφερθείσας πύλης, υιοθετήθηκε το ενιαίο σύστημα διασφάλισης ταυτότητας των πολιτών (Gov.UK Verify) για την παροχή μίας ολοκληρωμένης ηλεκτρονικής εμπειρίας. Μαζί με αυτήν την καινοτομία έχει μπει στη ζωή των πολιτών του Ηνωμένου Βασιλείου και η Ψηφιακή Αγορά αναφορικά με τις προμήθειες των δημόσιων φορέων για τον μετασχηματισμό των ηλεκτρονικών υπηρεσιών.

2.2.2 Η Ηλεκτρονική Διακυβέρνηση στην Ελλάδα

Προκειμένου η ελληνική πραγματικότητα να ανταπεξέλθει στις συνεχόμενες αλλαγές, η Δημόσια Διοίκηση βρίσκεται σε φάση ολοκληρωτικής αναδιάρθρωσης. Βασικός σκοπός είναι η εξυπηρέτηση των πολιτών και των επιχειρήσεων όσο καλύτερα και αποτελεσματικότερα γίνεται. Ο εκσυγχρονισμός της Ηλεκτρονικής Διακυβέρνησης στην Ελλάδα βασίστηκε σε δύο πυλώνες παρεμβάσεων. Ο πρώτος αφορούσε την υλοποίηση των έργων πληροφορικής για την ηλεκτρονική διακυβέρνηση και ο δεύτερος τα μέτρα θεσμικού περιεχομένου για την εξοικείωση των πολιτών στις νέες τεχνολογικές υπηρεσίες [13].

Η χρηματοδότηση του μεγάλου αυτού έργου δόθηκε από την Ευρωπαϊκή Ένωση μέσω των Κοινοτικών Πλαισίων Στήριξης. Αξιοποιώντας τα κονδύλια, η Ελλάδα προσπάθησε να υλοποιήσει και να εδραιώσει τις υπηρεσίες Ηλεκτρονικής Διακυβέρνησης. Το πρώτο πρόγραμμα που τέθηκε σε ισχύ ήταν το «Κλεισθένης» με ορίζοντα έναρξης το έτος 1994. Η διάρκειά του ήταν έξι χρόνια και βασικός σκοπός ήταν η εισαγωγή νέων τεχνολογιών στους κλάδους Τοπικής Αυτοδιοίκησης και Δημόσιου Τομέα.

Εν συνεχεία, το 1999 ψηφίστηκε το επιχειρησιακό πρόγραμμα του Υπουργείου Οικονομικών «Κοινωνία της Πληροφορίας» (ΚτΠ) με το οποίο ενισχύθηκαν οι τεχνικές υποδομές των παρεχόμενων ηλεκτρονικών υπηρεσιών σε βασικούς κλάδους της δημόσιας διοίκησης, όπως η υγεία και η παιδεία. Οι γενικοί στρατηγικοί στόχοι του προγράμματος εστίαζαν στην εξυπηρέτηση του πολίτη και τη βελτίωση της ποιότητας ζωής του, καθώς και την ανάπτυξη του ανθρώπινου δυναμικού. Μερικές από τις σημαντικότερες δράσεις που πραγματοποιήθηκαν στο πλαίσιο επίτευξης των στόχων του προγράμματος ΚτΠ είναι οι εξής [13]:

- Αναβάθμιση του εξοπλισμού υπολογιστικών συστημάτων στα σχολεία και τα εκπαιδευτικά ιδρύματα.
- Ολοκλήρωση του Πανελλήνιου Εκπαιδευτικού Δικτύου ενοποιώντας όλες τις σχολικές μονάδες σε ένα ενδοδίκτυο (intranet).

[1] https://www.gov.uk/

- Ψηφιοποίηση της πολιτιστικής κληρονομιάς και εξέλιξη κόμβων πληροφόρησης με ελληνικό πολιτιστικό περιεχόμενο.
- Βελτίωση της ποιότητας των παρεχόμενων υπηρεσιών σε διοικητικό επίπεδο.
- Χρησιμοποίηση των ΤΠΕ προκειμένου να βελτιωθούν οι υπηρεσίες υγείας και πρόνοιας για όλους του Έλληνες πολίτες.
- Ενσωμάτωση νέων τεχνολογιών στους τρεις τομείς της οικονομίας (πρωτογενής, δευτερογενής και τριτογενής) και ανάπτυξη του ηλεκτρονικού εμπορίου.
- Στήριξη της διαδικασίας απελευθέρωσης της τηλεπικοινωνιακής αγοράς.
- Ενίσχυση πρόσβασης στην Κοινωνία της Πληροφορίας από κατοίκους λιγότερο ανεπτυγμένων περιοχών.

Το πρόγραμμα που τέθηκε έπειτα σε εφαρμογή ήταν το «Πολιτεία». Λειτούργησε συμπληρωματικά του ΚτΠ και στόχοι του ήταν οι εξής:

- Συμμετοχικότητα.
- Αξιοκρατία και παροχή ίσων ευκαιριών σε όλους τους πολίτες.
- Διαφάνεια στην εφαρμογή δράσεων της Δημόσιας Διοίκησης.
- Αναβάθμιση της ποιότητας παρεχόμενων υπηρεσιών.

Το επόμενο σημαντικό έργο που υλοποιήθηκε από το Υπουργείο Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης ήταν το «Σύζευξις». Πρόκειται για ένα τυπικό έργο παροχής τηλεπικοινωνιών και τηλεματικών υπηρεσιών μεγάλης κλίμακας. Δημιουργήθηκε ένα ενιαίο δίκτυο πρόσβασης των φορέων του Ελληνικού Δημοσίου, ώστε να απλοποιηθεί η επικοινωνία μεταξύ τους αλλά και να επεκταθούν οι υπηρεσίες εικόνας, δεδομένων και φωνής.

Ένα σημαντικό έργο δημόσιας διοίκησης είναι η πύλη "Ermis"[2] η οποία αποτελεί την κεντρική Κυβερνητική Διαδικτυακή Πύλη της Ελλάδας, παρέχοντας υπηρεσίες ενημέρωσης πολιτών με τη χρήση κλιμακούμενων μεθόδων αυθεντικοποίησης. Μέσω της συγκεκριμένης πύλης προσφέρεται η δυνατότητα χρήσης υπηρεσιών δύο μεγάλων κατηγοριών:

1. οι υπηρεσίες εκείνες που μπορεί να παραλάβει ο χρήστης είτε στην ηλεκτρονική του θυρίδα είτε από τα Κέντρα Εξυπηρέτησης Πολιτών (ΚΕΠ), όπως το πιστοποιητικό γέννησης, το πιστοποιητικό οικογενειακής κατάστασης, το αντίγραφο ποινικού του μητρώου, κ.λπ.
2. οι υπηρεσίες που μπορεί να παραλάβει ο χρήστης μόνο στην ηλεκτρονική του θυρίδα, όπως η ασφαλιστική του ενημερότητα, απόσπασμα του ατομικού λογαριασμού του στο Ίδρυμα Κοινωνικών Ασφαλίσεων (ΙΚΑ), κ.ο.κ.

Το 2016 ιδρύθηκε η Γενική Γραμματεία Ψηφιακής Πολιτικής (ΓΓΨΠ) υπό την αιγίδα του τότε νεοσύστατου υπουργείου Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης. Σκοπός της ήταν ο σχεδιασμός, ο συντονισμός και η υλοποίηση έργων ΤΠΕ στο ελληνικό δημόσιο αλλά και γενικά σε όλη τη χώρα. Για να υλοποιηθούν σωστά

[2] www.ermis.gov.gr

οι πρωτοβουλίες της Ευρωπαϊκής Επιτροπής όπως αναφέρθηκαν παραπάνω, διαμορφώθηκε η Εθνική Ψηφιακή Στρατηγική (ΕΨΣ) που έχει ως αποκλειστικό στόχο την ψηφιακή ανάπτυξη της χώρας, την αξιοποίηση των ΤΠΕ προς όφελος της κοινωνίας και της οικονομίας και την άρση των γεωγραφικών αποκλεισμών.

Οι επτά (7) τομείς παρέμβασης που καθορίζονται από την ΕΨΣ είναι οι εξής [13]:

1. Ανάπτυξη εθνικών υποδομών συνδεσιμότητας νέας γενιάς.
2. Επιτάχυνση της ψηφιοποίησης της οικονομίας.
3. Ώθηση του κλάδου ΤΠΕ για την ανάπτυξη της ψηφιακής οικονομίας και της απασχόλησης.
4. Ενδυνάμωση του ανθρώπινου δυναμικού με ψηφιακές δεξιότητες.
5. Ριζική αναθεώρηση του τρόπου παροχής Ψηφιακών Υπηρεσιών του Δημοσίου.
6. Άρση των αποκλεισμών και διάχυση των ωφελειών της ψηφιακής οικονομίας.
7. Ενίσχυση ασφάλειας και εμπιστοσύνης.

Από την εισήγηση της ηλεκτρονικής διακυβέρνησης στην Ελλάδα, πολλά από τα έργα ΤΠΕ αποτέλεσαν Ολοκληρωμένα Πληροφοριακά Συστήματα και, ως αποτέλεσμα, ακολουθούσαν τη συμβατική γραμμική μεθοδολογία (καταρράκτη – waterfall) που δεν ανταποκρινόταν στις σύγχρονες απαιτήσεις και αρκετές φορές οδηγούσε σε αποτυχίες. Ο λόγος αυτός οδήγησε στην υιοθέτηση μεθοδολογίας ευέλικτης υλοποίησης (agile development), αξιοποιώντας τις ΤΠΕ στο δημόσιο με τον περιορισμό της σπατάλης και επαναχρησιμοποιώντας τους όποιους πόρους χρειάζονταν.

Παρακάτω παρουσιάζεται ένας συνοπτικός πίνακας των ολοκληρωμένων ή εν εξελίξει έργων ηλεκτρονικής διακυβέρνησης στην Ελλάδα. Τα συγκεκριμένα έργα επηρεάζουν έμμεσα και άμεσα μεγάλη μερίδα του ελληνικού πληθυσμού. Τέλος, πρέπει να σημειωθεί ότι τα περισσότερα από τα παρακάτω έργα έχουν υλοποιηθεί ως επί το πλείστον μετά το 2010.

Πίνακας 1. Ολοκληρωμένα Έργα Ηλεκτρονικής Διακυβέρνησης [12]

Έργο	**Φορέας Διαχείρισης**	**Αποδέκτες**	**Διεύθυνση ιστοτόπου (URL)**
Φορολογία και τελωνεία (Taxisnet, Icisnet, Συστήματα Περιουσιολογίου Ε9)	Ανεξάρτητη Αρχή Δημοσίων Εσόδων (ΑΑΔΕ), Γενική Γραμματεία Πληροφορικών Συστημάτων (ΓΓΠΣ)	Πολίτες, επιχειρήσεις, άλλες υπηρεσίες του Υπ. Οικονομικών, Ενοποιημένο Τελειωνειακό Σύστημα στην ΕΕ	https://www.aade.gr/ http://gsis.gr/gsis/info/gsis_site/index.html https://portal.gsis.gr/portal/page/portal/ICISnet

Ενιαίο Δημοτολόγιο Ληξιαρχείο	Υπουργείο Εσωτερικών (Κύριος των έργων και Φορέας Λειτουργίας). Υλοποίηση ΚτΠ ΑΕ	Δήμοι, Υπηρεσίες Δημοτολογίου, Ληξιαρχεία	http://www.ypes.gr/el/Ministry/Actions
Κτηματολόγιο	Εθνικό Κτηματολόγιο και Χαρτογράφηση ΑΕ (ΕΚΧΑ ΑΕ)	Κτηματολογικά γραφεία, πολίτες, επιχειρήσεις	http://www.ktimatologio.gr
Στρατολογία	Υπουργείο Εθνικής Άμυνας, Γενικό Επιτελείο Εθνικής Άμυνας, Γενικό Επιτελείο Στρατού	Πολίτες σχετικά με τα στρατολογικά τους θέματα	https://www.stratologia.gr/ https://katataxi.army.Gr
Διαύγεια	Υπουργείο Διοικητικής Ανασυγκρότησης (Κύριος και Φορέας Λειτουργίας). Υλοποίηση ΚτΠ ΑΕ	Δημόσιο, Πολίτες, επιχειρήσεις	https://diavgeia.gov.gr/
Open Gov και Open data	Υπουργείο Διοικητικής Ανασυγκρότησης Εθνικό Κέντρο Δημόσιας Διοίκησης και Αυτοδιοίκησης (ΕΚΔΔΑ)	Πολίτες, επιχειρήσεις, δημόσιο	http://opengov.gr/ http://data.gov.gr
Μητρώο Ανθρώπινου Δυναμικού του Ελληνικού Δημοσίου	Υπουργείο Διοικητικής Ανασυγκρότησης και ΓΓΠΣ Υπ. Οικονομικών	Δημόσιο, δημόσιοι υπάλληλοι	https://apografi.gov.gr
Ενιαία Αρχή Πληρωμής	ΓΓΠΣ Υπουργείο Οικονομικών	Δημόσιο, δημόσιοι υπάλληλοι	http://www.gsis.gr/gsis/info/gsis_site/Services/DimosiaDioikisi/epsp. Html
Κεντρικό Ηλεκτρονικό Μητρώο Δημοσίων Συμβάσεων (ΚΗΜΔΗΣ)	Υπουργείο Ανάπτυξης και ΑνταγωνιστικότηταςΓενική Γραμματεία Εμπορίου	Δημόσιοι Φορείς, Οικονομικοί Φορείς που συμμετέχουν σε διαγωνισμούς του δημοσίου, διενέργεια ηλεκτρονικών διαγωνισμών από 60.000 ευρώ και άνω	www.promitheus.gov.gr

		για προμήθειες και υπηρεσίες Και ανάρτηση των δημοσίων συμβάσεων στο ΚΗΜΔΗΣ	
Εργάνη	Υπουργείο Εργασίας, Κοινωνικής Ασφάλισης & Κοινωνικής Αλληλεγγύης	Πολίτες, επιχειρήσεις, εργαζόμενοι, άνεργοι	http://eservices.yeka.gr/
Ήλιος Ενιαίο Σύστημα Ελέγχου Πληρωμών Συντάξεων	Υπουργείο Εργασίας, Κοινωνικής Ασφάλισης & Κοινωνικής Αλληλεγγύης ΗΔΙΚΑ	Πολίτες συνταξιοδοτούμενοι	http://www.yeka.gr/
«Απλό»	Υπουργείο Εργασίας, Κοινωνικής Ασφάλισης & Κοινωνικής Αλληλεγγύης	Αιτήσεις πολιτών για βεβαιώσεις ασφάλειας και υγείας	https://aplo.yeka.gr/
Ηλεκτρονική Συνταγογράφηση	Υπουργείο Εργασίας, Κοινωνικής Ασφάλισης & Κοινωνικής Αλληλεγγύης, ΗΔΙΚΑ	Γιατροί, φαρμακοποιοί, πολίτες	https://www.e-prescription.gr/
Ηλεκτρονικά ραντεβού e-RDV	ΗΔΙΚΑ	Πολίτες	https://www.e-syntagografisi.gr/p-rv/p
Γεωχωρικά δεδομένα ΓΥΣ	Υπουργείο Εθνικής Άμυνας Γεωγραφική Υπηρεσία Στρατού	E-shop για γεωχωρικά δεδομένα της ΓΥΣ	http://web.gys.gr/portal
Εθνικό Τυπογραφείο	Υπουργείο Διοικητικής Ανασυγκρότησης Εθνικό Τυπογραφείο	Πολίτες, επιχειρήσεις, δημόσιο	http://www.et.gr/
ΣΥΖΕΥΞΙΣ	Υπουργείο Διοικητικής Ανασυγκρότησης ΚτΠ ΑΕ	Εθνικό Δίκτυο Δημόσιας Διοίκησης	http://www.syzefxis.gov.gr/
G-cloud Υπηρεσίες government cloud	ΚτΠ ΑΕ -ΓΓΠΣ Έργο σε εξέλιξη	Φορείς Δημοσίου	http://www.ktpae.gr/
Σύστημα Ηλεκτρονικής Διαχείρισης	Υπουργείο Διοικητικής Ανασυγκρότησης	Πολίτες, επιχειρήσεις, δημόσιο	http://aped.gov.gr/

Εγγράφων - ψηφιακή υπογραφή	Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ)		
Ηλεκτρονικό Σύστημα του Ανώτατου Συμβουλίου Επιλογής Προσωπικού (ΑΣΕΠ)	ΑΣΕΠ (Κύριος του έργου και Φορέας Λειτουργίας), υλοποίηση από την ΚτΠ ΑΕ	Πολίτες, Φορείς του Δημοσίου για πρόσληψη προσωπικού	http://www.asep.gr/
Ηλεκτρονικό Σύστημα Υποβολής και επεξεργασίας δηλώσεων ΠΟΘΕΝ ΕΣΧΕΣ	Επιθεωρητής Δημόσιας Διοίκησης και άλλοι ελεγκτικοί Φορείς του Δημοσίου, Φορέας Λειτουργίας ΓΓΠΣ, υλοποίηση από την ΚτΠ ΑΕ	Πολίτες που υποχρεούνται σε δήλωση ΠΟΘΕΝ ΕΣΧΕΣ, Ελεγκτικοί Φορείς των δηλώσεων.	https://www.pothen.gr/
Ολοκληρωμένο Σύστημα Διαχείρισης Δικαστικών Υποθέσεων (ΟΣΔΔΥ-ΠΠ)	Υπουργείο Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων Έργο σε εξέλιξη / πιλοτική λειτουργία	Ειρηνοδικεία, πταισματοδικεία, πρωτοδικεία, εισαγγελίες πρωτοδικών, εφετεία, εισαγγελίες εφετών, Άρειος Πάγων, εισαγγελία Αρείου Πάγου, δικηγόροι και πολίτες	https://www.solon.gov.gr/

2.3 Πλαίσια Διαλειτουργικότητας Ηλεκτρονικής Διακυβέρνησης και Ευρωπαϊκά Πρότυπα

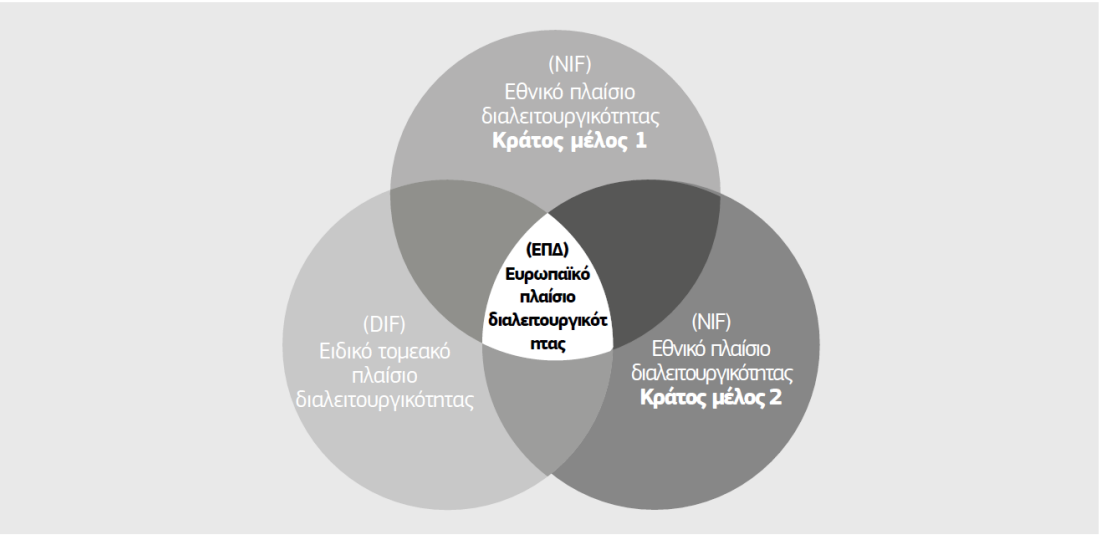
Η Ευρωπαϊκή Ένωση ιδρύθηκε προκειμένου να ενοποιηθούν τα κράτη-μέλη της, εγγυώμενη τέσσερις «ελευθερίες»: την ελεύθερη κυκλοφορία κεφαλαίων, εμπορευμάτων, υπηρεσιών και προσώπων. Οι πολίτες έχουν τη δυνατότητα να μετακινούνται, να δραστηριοποιούνται και να πραγματοποιούν συναλλαγές σε όλα τα κράτη της ΕΕ. Όμως, για να επιτευχθεί η δράση αυτή κρίθηκε απαραίτητο να θεσμοθετηθούν οι κανόνες που διασφαλίζουν τις ελευθερίες των ευρωπαίων πολιτών.

Η ελεύθερη διακίνηση προϊόντων και υπηρεσιών σε συνδυασμό με τη συνεχώς αυξανόμενη ανάπτυξη των ΤΠΕ οδήγησε στη εισαγωγή ψηφιακών δημόσιων υπηρεσιών, αποφεύγοντας τον τυχόν ψηφιακό κατακερματισμό. Η κοινή πολιτική και οι ταυτόσημες νομοθεσίες των κρατών-μελών της ΕΕ αποτελούν στοιχεία ζωτικής σημασίας για τη συγκρότηση και την ανάπτυξη της Ένωσης. Η Ευρωπαϊκή Επιτροπή έθεσε το Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας (ΕΠΔ) ώστε να παρέχει συστάσεις

και κατευθύνσεις στις δημόσιες διοικήσεις, βελτιώνοντας έτσι τις απαιτούμενες δραστηριότητες διαλειτουργικότητας.

Ο ορισμός που δίνεται από την Ευρωπαϊκή Επιτροπή για το ΕΠΔ είναι [14]: «το ευρωπαϊκό πλαίσιο διαλειτουργικότητας είναι μια από κοινού συμφωνημένη προσέγγιση για την παροχή ευρωπαϊκών δημόσιων υπηρεσιών με διαλειτουργικό τρόπο. Ορίζει τις βασικές κατευθυντήριες γραμμές για τη διαλειτουργικότητα με τη μορφή κοινών αρχών, μοντέλων και συστάσεων». Σκοπός του είναι ο σχεδιασμός ευρωπαϊκών δημόσιων υπηρεσιών προς άλλες δημόσιες διοικήσεις, πολίτες και επιχειρήσεις, καθώς και να παρέχει κατευθύνσεις προς τις δημόσιες διοικήσεις όσον αφορά τον σχεδιασμό και την επικαιροποίηση των εθνικών πλαισίων διαλειτουργικότητας (National Interoperability Framework - NIF), συμβάλλοντας παράλληλα και στην καθιέρωση της ενιαίας ψηφιακής αγοράς.

Θεωρώντας δεδομένο το γεγονός ότι όλα τα κράτη μέλη έχουν διαφορετικά διοικητικά και πολιτικά συστήματα, για τον ορισμό του εκάστοτε ΕΠΔ λαμβάνονται υπόψη οι τυχόν εθνικές ιδιαιτερότητες που είναι πιθανό να υπάρχουν. Επιπλέον, τα ειδικά τομεακά πλαίσια διαλειτουργικότητας (Domain-specific Interoperability Framework - DIF) οφείλουν να συμβαδίζουν με την εφαρμογή του ΕΠΔ, καλύπτοντας τις ανάγκες διαλειτουργικότητας του εν λόγω τομέα. Παρακάτω απεικονίζεται η σχέση δύο NIF κρατών μελών του DIF και πώς το ΕΠΔ παρέχει έναν κοινό πυρήνα αλληλεπίδρασης [14].



Εικόνα 1. Σχέση μεταξύ ΕΠΔ, NIF και DIF[14]

Δύο κατευθύνσεις ορίζονται από το ΕΠΔ ώστε να αναπτυχθεί ένα ευρωπαϊκό οικοσύστημα δημόσιων υπηρεσιών, το οποίο θα εξυπηρετεί τους πολίτες, τις επιχειρήσεις και τον δημόσιο τομέα και θα υποστηρίζει την ενιαία ψηφιακή αγορά εντός ΕΕ:

- *από κάτω προς τα πάνω*, στην περίπτωση που το NIF αναπροσαρμόζεται και εναρμονίζεται με το ΕΠΔ παρέχοντας δημόσιες υπηρεσίες σε όλες τις εθνικές διοικήσεις.
- *από πάνω προς τα κάτω*, στην περίπτωση που η νομοθεσία και οι τομείς πολιτικής της ΕΕ λαμβάνουν υπόψη και εναρμονίζονται με το ΕΠΔ μέσω παραπομπών επί τούτω, χρησιμοποιώντας κατάλληλα το DIF.

Το ΕΠΔ ορίζει με σαφήνεια συνολικά δώδεκα (12) βασικές αρχές που ομαδοποιούνται σε τέσσερις (4) μεγαλύτερες κατηγορίες:

I. Αρχή που καθορίζει το πλαίσιο των δράσεων της ΕΕ για τη διαλειτουργικότητα

1. Επικουρικότητα και αναλογικότητα: Η αρχή της επικουρικότητας προϋποθέτει την εφαρμογή αποφάσεων και μέτρων της ΕΕ που ταυτίζονται με τις ανάγκες του πολίτη και είναι αποτελεσματικότερα από τη λήψη μέτρων σε εθνικό επίπεδο. Αναφορικά με την αρχή της αναλογικότητας, η αρχή αυτή περιορίζει τις δράσεις της ΕΕ προκειμένου να επιτευχθούν άμεσα οι στόχοι των συνθηκών. Συγκεκριμένα, τα NIF προσαρμόζονται και επεκτείνονται ανάλογα με τις εθνικές ιδιαιτερότητες, έχοντας παράλληλα και τις συστάσεις του ΕΠΔ.

II. Βασικές αρχές διαλειτουργικότητας

1. Ανοιχτός χαρακτήρας: Η έννοια του ανοιχτού χαρακτήρα εστιάζει κυρίως στα δεδομένα, τις προδιαγραφές και το λογισμικό. Η γενική ιδέα είναι πως τα δημόσια δεδομένα πρέπει να διατίθενται ελεύθερα για οποιαδήποτε χρήση, χωρίς βέβαια να υπερβαίνουν τους ισχύοντες περιορισμούς, όπως, για παράδειγμα, η προστασία δεδομένων προσωπικού χαρακτήρα για λόγους απορρήτου ή λόγω δικαιωμάτων πνευματικής ιδιοκτησίας. Η πρωτοβουλία INSPIRE προβλέπει, εκτός άλλων, την κοινή χρήση των υπηρεσιακών χωρικών δεδομένων μεταξύ των δημόσιων υπηρεσιών, ώστε οι διοικήσεις να λαμβάνουν αποφάσεις αμεσότερα και αποτελεσματικότερα, εφαρμόζοντας κάθε αρχή διαφάνειας στην πράξη. Η χρήση των ΤΠΕ επιτρέπει την εφαρμογή του ανοιχτού χαρακτήρα σε ευρωπαϊκό και εθνικό επίπεδο, καθώς εξοικονομείται μεγάλο κόστος ανάπτυξης για τα λογισμικά ανοιχτής πηγής. Ένα ακόμη σημαντικό στοιχείο είναι η χρήση ανοιχτών προδιαγραφών, αφότου βέβαια ληφθεί υπόψη η κάλυψη των λειτουργικών αναγκών, η ωριμότητα και η υποστήριξη της αγοράς μαζί με την καινοτομία.

2. Διαφάνεια: Η διαφάνεια αποτελεί μία από τις βασικότερες αρχές του ΕΠΔ και αφορά τη δυνατότητα προβολής (εντός του διοικητικού περιβάλλοντος) μιας δημόσιας διοίκησης. Θα πρέπει, δηλαδή, οι άλλες διοικήσεις, οι πολίτες και οι επιχειρήσεις να έχουν τη δυνατότητα παρακολούθησης των διαδικασιών, των κανόνων, των δεδομένων και των υπηρεσιών για να συνεισφέρουν στη διαδικασία λήψης αποφάσεων. Επίσης, η αρχή της διαφάνειας αναφέρεται και στη διασφάλιση διαλειτουργικότητας μεταξύ των επιμέρους πληροφοριακών

συστημάτων ηλεκτρονικής διακυβέρνησης, διότι οι δημόσιες διοικήσεις χρησιμοποιούν διάσπαρτα και ανομοιογενή συστήματα για τη διεκπεραίωση βασικών λειτουργιών. Τέλος, μέσω της διαφάνειας διασφαλίζεται το δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα, όπως διαμορφώνεται και από το νέο νομοθετικό πλαίσιο για τους μεγάλους όγκους προσωπικών δεδομένων των πολιτών που διαχειρίζονται όλες οι δημόσιες υπηρεσίες.

3. Δυνατότητα επαναχρησιμοποίησης: Ο όρος της επαναχρησιμοποίησης αναφέρεται στο ότι οι δημόσιες διοικήσεις που αντιμετωπίζουν ποικίλα ζητήματα επιδιώκουν να επωφεληθούν από τα υπόλοιπα έργα, αξιολογώντας τη χρησιμότητα των διαθέσιμων στοιχείων, όπως λογισμικά συστήματα ή/και πρότυπα. Επιπρόσθετα, με τον τρόπο αυτόν εξοικονομούνται χρήματα και χρόνος. Η επαναχρησιμοποίηση και η ανταλλαγή πληροφοριών και δεδομένων κατά την υλοποίηση ευρωπαϊκών δημόσιων υπηρεσιών πραγματοποιείται πάντα με γνώμονα τον σεβασμό του ιδιωτικού απορρήτου και την εμπιστευτικότητα.

4. Τεχνολογική ουδετερότητα και φορητότητα των δεδομένων: Κατά τη δημιουργία των ευρωπαϊκών δημόσιων υπηρεσιών είναι απαραίτητο οι υπηρεσίες να εστιάσουν στις λειτουργικές ανάγκες και να καθυστερήσουν τις αποφάσεις που αφορούν την τεχνολογία, προκειμένου να ελαχιστοποιηθούν τυχόν τεχνολογικές εξαρτήσεις, να μην χρησιμοποιηθούν ειδικές τεχνικές εφαρμογές και να είναι σε θέση οι υπηρεσίες αυτές να προσαρμόζονται στο συνεχώς μεταβαλλόμενο τεχνολογικό περιβάλλον. Η φορητότητα των δεδομένων θα πρέπει να επιτρέπει τη μεταφορά των πληροφοριών μεταξύ συστημάτων και εφαρμογών, χωρίς αδικαιολόγητους περιορισμούς, εφόσον δεν υπάρχει νομικό κώλυμα.

III. Αρχές που αφορούν τις γενικές ανάγκες και προσδοκίες των χρηστών

1. Λειτουργία με επίκεντρο τον χρήστη: Χρήστες των ευρωπαϊκών δημόσιων υπηρεσιών μπορεί να είναι πολίτες, δημόσιες διοικήσεις και επιχειρήσεις. Οι ανάγκες και οι απαιτήσεις των χρηστών πρέπει να αποτελούν την πυξίδα για τον σχεδιασμό και την ανάπτυξη υπηρεσιών ΗΔ. Η πρόσβαση στις υπηρεσίες πρέπει να πραγματοποιείται μέσα από πολλαπλά κανάλια, δίνοντας στον χρήστη τη δυνατότητα επιλογής, ενώ η δημιουργία ενιαίου κόμβου κρίνεται απαραίτητη προκειμένου οι πολίτες να μην αναγνωρίζουν την εσωτερική πολυπλοκότητα των διοικητικών συστημάτων. Ακόμη, οι χρήστες οφείλουν να συμμετέχουν στην αξιολόγηση των υπηρεσιών ώστε οι τελευταίες να βελτιώνονται συνεχώς.

2. Ένταξη και προσβασιμότητα: Η έννοια της ένταξης εστιάζει στη δυνατότητα του συνόλου του ευρωπαϊκού πληθυσμού να επωφεληθεί πλήρως από τις ευκαιρίες που προσφέρονται από τις νέες τεχνολογίες των δημόσιων υπηρεσιών, χωρίς να υπολογίζονται κοινωνικές ή/και οικονομικές διαφορές. Αντιστοίχως, η προσβασιμότητα εξασφαλίζει ότι τα άτομα με ειδικές ανάγκες, οι ηλικιωμένοι καθώς και οι μειονεκτούσες ομάδες μπορούν να χρησιμοποιούν καθολικά και σε όλα τα επίπεδα τις ευρωπαϊκές δημόσιες υπηρεσίες.

3. Ασφάλεια και προστασία της ιδιωτικότητας: Στην Ευρώπη είναι πολύ σημαντικό οι πολίτες και οι επιχειρήσεις να είναι βέβαιοι ότι κατά την αλληλεπίδραση με τις δημόσιες αρχές βρίσκονται σε ένα ασφαλές και αξιόπιστο περιβάλλον, συμμορφωμένο με τους σχετικούς κανονισμούς. Η προστασία της ιδιωτικότητας συνιστά πρωταρχικής σημασίας στόχο που καθορίζεται από το ΕΠΔ, οπότε η διαμόρφωση κοινού πλαισίου ασφάλειας και προστασίας της ιδιωτικότητας και η δημιουργία διαδικασιών για την αξιόπιστη ανταλλαγή δεδομένων μεταξύ των διοικήσεων αποτελεί βασικό στόχο της Ευρωπαϊκής Επιτροπής.

4. Πολυγλωσσία: Οι ευρωπαϊκές υπηρεσίες οφείλουν να συμμορφώνονται με τα πλαίσια πολυγλωσσίας εντός της ΕΕ διότι μπορούν να χρησιμοποιηθούν από οποιονδήποτε πολίτη οποιουδήποτε κράτους μέλους. Είναι σημαντικό να υπάρχει μια ισορροπία μεταξύ των προσδοκιών των πολιτών και των επιχειρήσεων και της ικανότητας των δημόσιων διοικήσεων να προσφέρουν τις υπηρεσίες τους σε όλες τις γλώσσες που μιλούνται στην Ευρώπη.

IV. Θεμελιώδεις αρχές για τη συνεργασία μεταξύ δημόσιων διοικήσεων

1. Διοικητική απλούστευση: Η διοικητική απλούστευση και η χρήση ψηφιακών καναλιών βοηθάει τους πολίτες και τις επιχειρήσεις να μειώσουν τη διοικητική επιβάρυνση, παρέχοντας υψηλής ποιότητας υπηρεσίες και μειώνοντας τις διαδικασίες που απαιτούνται για την διεκπεραίωση συγκεκριμένων εργασιών. Η ψηφιοποίηση των δημόσιων υπηρεσιών πρέπει να γίνεται κατά περίπτωση (digital-by-default) ώστε να υπάρχει διαθέσιμο κανάλι για τη χρήση μιας συγκεκριμένης υπηρεσίας και να δίνεται προτεραιότητα στα ψηφιακά κανάλια έναντι των συμβατών (digital-first).

2. Διατήρηση των πληροφοριών: Η διαμόρφωση μακροπρόθεσμης πολιτικής διατήρησης πληροφοριών σχετικά με τις ευρωπαϊκές δημόσιες υπηρεσίες αποτελεί σύσταση του ΕΠΔ, ώστε τα αρχεία και τα δεδομένα που βρίσκονται σε ηλεκτρονική μορφή να διατηρούν τον ευανάγνωστο, αξιόπιστο και αδιάβλητο χαρακτήρα τους και να είναι προσβάσιμα όταν αυτό απαιτείται. Συστήνεται επίσης και η κατάλληλη «πολιτική διατήρησης» σε ζητήματα που δεν είναι εθνικής αλλά ευρωπαϊκής σημασίας και αφορούν παραπάνω από ένα κράτη μέλη.

3. Αξιολόγηση της αποτελεσματικότητας και της αποδοτικότητας: Όλες οι τεχνολογικές λύσεις που προτείνονται από την Ευρωπαϊκή Επιτροπή πρέπει να αξιολογούνται με συγκεκριμένες εκτιμήσεις, όπως η απόδοση των επενδύσεων, το συνολικό κόστος ιδιοκτησίας, η μείωση του διοικητικού φόρτου, η διαφάνεια, η αποδοτικότητα και η απλοποίηση. Προφανώς, λαμβάνονται υπόψη όχι μόνο οι ανάγκες των χρηστών αλλά και η αναλογικότητα και η ισορροπία μεταξύ κόστους και οφέλους.

2.4 Συστήματα Διαχείρισης Ψηφιακών Ταυτοτήτων

Στη σύγχρονη εποχή τα Συστήματα Διαχείρισης Ταυτότητας βρίσκονται στην καρδιά οποιουδήποτε δημόσιου, ιδιωτικού ή υβριδικού αυτόνομου φορέα. Είναι πλέον αναγκαίο οι οργανισμοί να αναπτύσσουν υποδομές πληροφοριακών συστημάτων, ώστε να βελτιώσουν την απόδοση των τελευταίων. Το αυξανόμενο ενδιαφέρον στη χρήση διαδικτυακών περιβαλλόντων για την παράδοση και βελτίωση της προστιθέμενης αξίας των υπηρεσιών τους, όπως για παράδειγμα η «ενορχήστρωση» υπηρεσιών που προσφέρουν πολλοί διαφορετικοί αυτόνομοι οργανισμοί, αποτελεί βασικό λόγο και κίνητρο για την ανάπτυξη τέτοιων υποδομών. Ουσιαστικά, το κλειδί για να πετύχουν τα παραπάνω είναι το σύστημα που θα σχεδιαστεί να παρέχει ταυτοποίηση και αυθεντικοποίηση (identification and authentication) των χρηστών με ταυτόχρονη παροχή εξουσιοδότησης (authorization) αναφορικά με τα δικαιώματά τους πρόσβασης σε δεδομένα και υπηρεσίες, διατηρώντας ωστόσο σε λογικά πλαίσια το λειτουργικό κόστος για τον εκάστοτε οργανισμό. Τα συστήματα αυτά, λοιπόν, μέσω των οποίων πραγματοποιούνται τέτοιες διαδικασίες ονομάζονται Συστήματα Διαχείρισης Ταυτότητας (Identity Management Systems - IMS).

Ιστορικά, στον σχεδιασμό Συστημάτων Διαχείρισης Ταυτότητας έχουν χρησιμοποιηθεί τρία (3) διαφορετικά μοντέλα: οργανισμο-κεντρικά, χρηστοκεντρικά και ομοσπονδιακά, ανάλογα με το ποιος κατέχει τις πληροφορίες του χρήστη. Συγκεκριμένα:

- *Οργανισμο-κεντρικά*: ο εκάστοτε οργανισμός διατηρεί και διαχειρίζεται τις προσωπικές πληροφορίες του χρήστη, ακόμα και μεταξύ άλλων φορέων.
- *Χρηστοκεντρικά*: ο χρήστης έχει τον έλεγχο των προσωπικών του πληροφοριών.
- *Ομοσπονδιακά*: η ταυτότητα του κάθε χρήστη είναι αποθηκευμένη σε διάφορα συστήματα διαχείρισης ταυτότητας με τα οποία επικοινωνεί κάθε φορά ανάλογα με το ποιες πληροφορίες του χρήστη ζητούνται.

Και οι τρεις παραπάνω προσεγγίσεις μπορούν να προκύψουν με ανάπτυξη διαδικτυακής υποδομής που θα δίνει τη δυνατότητα στους χρήστες να ταυτοποιούνται μία μόνο φορά, ώστε να εισέλθουν στο αυτόνομο σύστημα που τους ενδιαφέρει (Single Sign-On). Από τη μία πλευρά, τα οργανισμο-κεντρικά μοντέλα βασίζονται σε ιεραρχικούς κανόνες με βάση τους οποίους ελέγχουν την εγκυρότητα μίας ταυτότητας, γεγονός που δυσκολεύει την εφαρμογή τους στα διάφορα αυτόνομα συστήματα που θα άξιζε να χρησιμοποιηθούν. Από την άλλη πλευρά, τα χρηστο-κεντρικά μοντέλα επικεντρώνονται ιδιαιτέρως στα όρια που χωρίζουν την ιδιωτικότητα από την αποκάλυψη στοιχείων ταυτότητας περισσότερων από όσα πρέπει. Για τον λόγο αυτό, θα μπορούσε να θεωρηθεί το μοντέλο αυτό ως μία συμπληρωματική προσέγγιση στα άλλα δύο μοντέλα στα σημεία που «πάσχουν». Σε ό,τι αφορά το τρίτο μοντέλο, το ομοσπονδιακό μοντέλο φαίνεται να αποτελεί κατάλληλη προσέγγιση για τη διαχείριση της ταυτοποίησης και εξουσιοδότησης χρηστών στα διάφορα αυτόνομα συστήματα, καθώς σε κάθε ένα από αυτά υπάρχει δικό του τοπικό σύστημα διαχείρισης ταυτότητας. Αυτό από μόνο του

σημαίνει ότι κάθε ένα τέτοιο τοπικό σύστημα έχει ανεξάρτητο σχήμα ταυτότητας για τα στοιχεία του ατόμου που διαχειρίζεται, άρα συμβάλλει στον συνδυασμό της διαλειτουργικότητας με την αυτονομία των Συστημάτων Διαχείρισης Ταυτότητας. Στο πλαίσιο λειτουργίας ενός τέτοιου συνεργατικού συστήματος δίνονται αμοιβαίες άδειες για την αποκάλυψη στοιχείων ταυτότητας μεταξύ των οργανισμών που συμμετέχουν σε αυτό μέσα από συμφωνίες εμπιστοσύνης. Τέτοιες συμφωνίες επιβεβαιώνουν στην πράξη τον «κύκλο εμπιστοσύνης» στα συνεργατικά συστήματα.

Πιο συγκεκριμένα, στα Ομοσπονδιακά Συστήματα Διαχείρισης Ταυτότητας υπάρχουν δύο βασικά είδη οντοτήτων: οι πάροχοι υπηρεσιών (Service Providers - SPs) και οι πάροχοι ταυτότητας (Identity Providers - IdPs). Από τη μία πλευρά, οι πάροχοι υπηρεσιών προσφέρουν τις υπηρεσίες τους όταν ο εκάστοτε χρήστης πληροί τις απαιτήσεις πολιτικής που σχετίζονται με εκείνον και τις υπηρεσίες που θέλει να χρησιμοποιήσει. Από την άλλη πλευρά, οι πάροχοι ταυτότητας διαχειρίζονται τις πληροφορίες χρήστη με σχετικές με την ταυτότητα και την αυθεντικοποίησή του στο σύστημα. Πολλές φορές, κάθε οργανισμός που εφαρμόζει ομοσπονδιακό σύστημα έχει και τους δύο ρόλους παρόχου (υπηρεσιών και ταυτότητας) και πετυχαίνει την ταυτοποίηση των χρηστών με χρήση SSO τεχνολογίας. Με τη χρήση του SSO γίνεται εφικτή η πρόσβαση του χρήστη με όνομα χρήστη (username) και κωδικό χρήστη (password) σε πολλές υπηρεσίες είτε ενός είτε πολλών οργανισμών.

Μία ταυτότητα που χρησιμοποιείται σε ομοσπονδιακά συστήματα περιλαμβάνει όχι μόνο τα στοιχεία εισόδου του χρήστη, αλλά και τις ιδιότητες του χρήστη καθώς και διάφορα άλλα ταυτοποιητικά στοιχεία του. Έτσι, αν θεωρήσουμε τους παρόχους ταυτότητας ως απλούς κανονικούς παρόχους υπηρεσιών, τότε ο μηχανισμός διατήρησης ιδιωτικότητας θα πρέπει να μπορεί να ανακτά τα χαρακτηριστικά ταυτότητας χρήστη και από άλλους παρόχους υπηρεσιών [15][1].

2.4.1 Η Έννοια της Διαχείρισης Ταυτότητας

Από την πρώτη στιγμή δημιουργίας των ψηφιακών ταυτοτήτων εμφανίστηκε η ανάγκη διαχείρισής τους στα διάφορα πλαίσια στα οποία αυτές χρησιμοποιούνταν. Με άλλα λόγια, από την αρχή χρειάστηκε να καθοριστεί η πληροφορία που μία ψηφιακή ταυτότητα εμπεριέχει, με ποιες άλλες ταυτότητες συσχετίζεται, σε ποια πλαίσια (δίκτυα, διοικητικές περιοχές, κ.ά.) είναι αποδεκτή, τι μορφή (format) ακολουθεί, και μία σειρά από άλλα χαρακτηριστικά και ιδιότητες οι οποίες την καθιστούν λειτουργική. Η διαχείρισή τους, μέχρι και πριν από λίγα χρόνια, ήταν αρκετά εύκολη, αφού τα μέχρι πρόσφατα απομονωμένα δίκτυα και υπηρεσίες καθόριζαν από μόνα τους τη μορφή και τη λειτουργία των ψηφιακών ταυτοτήτων που χρησιμοποιούσαν. Ο καθορισμός των ταυτοτήτων δεν γινόταν με βάση κάποια πρότυπα αλλά, κατά κύριο λόγο, βασιζόταν σε εσωτερικές αποφάσεις που έπαιρνε αυτόνομα το εκάστοτε δίκτυο. Το αποτέλεσμα αυτού ήταν η δημιουργία μιας πολύ μεγάλης γκάμας διαφορετικών ψηφιακών ταυτοτήτων με διαφορετικά χαρακτηριστικά, ιδιότητες και λειτουργικότητα.

2.4.2 Βασικά Ζητήματα Διαχείρισης Ταυτότητας

Με τη ραγδαία εξάπλωση του Διαδικτύου, η διαφορετικότητα των ψηφιακών ταυτοτήτων άρχισε να δημιουργεί προβλήματα διαλειτουργικότητας και συνεργασίας μεταξύ δικτύων, υπηρεσιών και πλαισίων, όχι μόνο διαφορετικής τεχνολογίας αλλά και συστημάτων ίδιας τεχνολογίας που είχαν σχεδιαστεί σε διαφορετικές διοικητικές περιοχές και σε διαφορετικούς τομείς. Χαρακτηριστικό παράδειγμα αποτελούν τα κοινωνικά δίκτυα (social networks) όπου, ακόμα και σήμερα, θεωρείται ιδιαίτερα δύσκολη ως και αδύνατη η μεταξύ τους συνεργασία και η ανταλλαγή πληροφοριών. Παρότι το πρόβλημα άρχισε να διαφαίνεται από νωρίς, η κοινότητα του διαδικτύου συνεχώς ανέβαλε την αντιμετώπισή του. Οι αρχικές προσπάθειες που έγιναν προς τη λύση του προβλήματος κατέληγαν στη διαπίστωση της εξαιρετικά μεγάλης πολυπλοκότητας του προβλήματος. Κάθε διαφορετικό πλαίσιο απαιτούσε διαφορετική λύση, αφού η διαχείριση των ψηφιακών ταυτοτήτων του βασιζόταν σε διαφορετικές προϋποθέσεις και λειτουργούσε υπό διαφορετικές συνθήκες.

Πολλές προσπάθειες γίνονται πλέον ώστε να αντιμετωπιστούν τα προβλήματα που διαρκώς εμφανίζονται στον τομέα της διαχείρισης ταυτοτήτων. Παρόλα αυτά, επειδή πίσω από το διαδίκτυο και τις υπηρεσίες του έχει αναπτυχθεί πλέον μια τεράστια οικονομία, πολλές φορές τα εμπλεκόμενα μέρη δεν επιδιώκουν την ανάπτυξη μιας ενιαίας λύσης παρά σχεδιάζουν εξειδικευμένες λύσεις για τη δική τους περίπτωση. Έτσι, παρότι πολλές ερευνητικές ομάδες, τόσο από εταιρείες αλλά και από πανεπιστήμια, έχουν προτείνει μια σειρά από λύσεις, παρατηρείται το φαινόμενο αυτές οι λύσεις να είναι εφαρμόσιμες μόνο υπό συγκεκριμένες συνθήκες και πλαίσια χωρίς να είναι δυνατή η ενσωμάτωσή τους σε άλλα ή η μεταξύ τους συνεργασία. Συγκεκριμένα, τα συστήματα διαχείρισης ψηφιακών ταυτοτήτων που έχουν παρουσιαστεί ως τώρα (σχεδόν στο σύνολό τους) είναι σχεδιασμένα με τέτοιο τρόπο ώστε να λαμβάνουν υπόψη μόνο τις απαιτήσεις που προκύπτουν από έναν περιορισμένο αριθμό σεναρίων χρήσης. Σε αυτά τα σενάρια συνήθως εξετάζεται ένα υποσύνολο του προβλήματος που αντιμετωπίζει κάποια κοινότητα (για παράδειγμα, πάροχοι υπηρεσιών που συνεργάζονται, οργανισμοί, εταιρείες τηλεπικοινωνιών, κ.τ.λ.) κατά την παροχή κάποιων υπηρεσιών. Κάθε περίπτωση από αυτές είναι διαφορετική, βασίζεται σε διαφορετικές τεχνολογικές απαιτήσεις και εξυπηρετεί υπηρεσίες διαφορετικού σκοπού. Παράλληλα, οι απαιτήσεις ιδιωτικότητας, εμπιστοσύνης και ασφάλειας όχι μόνο είναι διαφορετικές κάθε φορά αλλά και μεταβάλλονται δυναμικά κατά το πέρασμα του χρόνου.

Το αποτέλεσμα αυτών των ανεξάρτητων προσπαθειών, είναι η δημιουργία ενός μεγάλου αριθμού διαφορετικών IdM συστημάτων, τα οποία ουσιαστικά ορίζουν την δική τους αποκλειστική «IdM κοινότητα» (επονομαζόμενη ως ομοσπονδία - Federation ή κύκλος εμπιστοσύνης- Circle of Trust κ.λπ.) που αποτελείται μόνο από εκείνα τα μέρη που ικανοποιούν το υποσύνολο των απαιτήσεων, βάση του οποίου σχεδιάστηκε το συγκριμένο IdM σύστημα. Λύσεις που αφορούν τη διαχείριση ταυτοτήτων παρέχονται μόνο στα μέλη αυτής της κοινότητας, εφόσον αυτά παραμένουν εντός των προκαθορισμένων ορίων της. Αυτή η πρακτική έχει οδηγήσει στον σχηματισμό απομονωμένων «IdM νησιών» με σοβαρά ζητήματα διαλειτουργικότητας. Προσπάθειες

για να συνδεθούν και να συνεργαστούν αυτά τα απομονωμένα συστήματα έχουν ήδη προταθεί, όμως και πάλι οι λύσεις τείνουν να ακολουθήσουν την ίδια πρακτική. Συγκεκριμένα, ορίζεται ένα νέο μεγαλύτερο πλαίσιο και μέσα σε αυτό σχεδιάζονται νέες στατικές διαδικασίες αντιστοίχισης - συσχέτισης εννοιών και δεδομένων ταυτότητας που είναι λειτουργικές μόνο μέσα στα νέα «σύνορα». Με άλλα λόγια, δημιουργείται και πάλι μία νέα IdM κοινότητα – ομοσπονδία, μόνο που είναι μεγαλύτερη αυτή τη φορά [16].

2.4.2.1 Νομικό Πλαίσιο και Προστασία Δεδομένων – Ιδιωτικότητα Χρήστη

Τα προσωπικά δεδομένα στο διαδίκτυο αποτελούν μία έννοια αρκετά αφηρημένη, η οποία διαφοροποιείται κατά ένα ποσοστό μεταξύ των χωρών και άρα ταξινομείται σε κατηγορίες ανάλογα με το είδος αυτών των δεδομένων. Συχνά στο διαδίκτυο η κατηγοριοποίηση των προσωπικών δεδομένων γίνεται με διάφορους τρόπους, ενώ το γεγονός ότι αποτελεί αφηρημένη και γενική έννοια οδηγεί στο να συγχέεται με την έννοια της ιδιωτικότητας του χρήστη.

Σύμφωνα με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ο όρος «Προσωπικά Δεδομένα» περιλαμβάνει κάθε πληροφορία που χαρακτηρίζει και ταυτοποιεί ένα φυσικό πρόσωπο, όπως το ονοματεπώνυμο, η διεύθυνση, το τηλέφωνο, το επάγγελμα, το μορφωτικό επίπεδο, η περιουσιακή και οικογενειακή κατάσταση. Τα παραπάνω χαρακτηριστικά ανήκουν στα λεγόμενα «απλά» προσωπικά δεδομένα, ενώ υπάρχουν, ακόμη, δεδομένα που αφορούν ιδιαίτερα «ευαίσθητα» προσωπικά δεδομένα της ιδιωτικής του ζωής, όπως το θρήσκευμα, οι πολιτικές πεποιθήσεις, η κατάσταση της υγείας του, η εθνική του καταγωγή, τα γενετικά του δεδομένα και άλλα.

Πρακτικά, ο διαχωρισμός των απλών από τα ευαίσθητα προσωπικά δεδομένα σχετίζεται με τον τρόπο συλλογής και επεξεργασίας τους. Σχετικά με τα απλά δεδομένα αρκεί η προφορική συγκατάθεση του υποκειμένου για τη νομική τους επεξεργασία, ενώ για τα ευαίσθητα δεδομένα χρειάζεται γραπτή έγκριση/συγκατάθεσή του.

Σε ό,τι αφορά την ιδιωτικότητα του χρήστη ή αλλιώς προστασία της ιδιωτικής ζωής, παρουσιάζεται συχνά συνυφασμένη με την προστασία των προσωπικών δεδομένων του χρήστη. Με τον όρο «ιδιωτικότητα» εννοούμε το «δικαίωμα στην απομόνωση» (the right to be let alone), που σχετίζεται με την απομόνωση, την μυστικότητα και την αυτονομία. Εναλλακτικά, η ιδιωτικότητα χρησιμοποιείται για την περιγραφή της κατάστασης του να μπορεί κάποιος να είναι μόνος και να μην μπορεί κάποιος άλλος να τον δει ή να τον ακούσει.

Στο πλαίσιο του Διαδικτύου, οι παραπάνω όροι έχουν αντίστοιχη σημασία και υπόσταση. Έτσι, η διαδικτυακή ιδιωτικότητα αναφέρεται στο δικαίωμα διατήρησης της προσωπικής ιδιωτικότητας σε σχέση με την αποθήκευση, μετατροπή, διάθεση σε τρίτους και επίδειξη πληροφοριών που αφορούν ένα άτομο μέσω του διαδικτύου. Η ιδιωτικότητα στο διαδίκτυο είναι μέρος της ιδιωτικότητας των πληροφοριών (Information Privacy) που σχετίζεται με τη γενική απαίτηση των ατόμων να μην είναι διαθέσιμα τα προσωπικά τους δεδομένα σε τρίτα άτομα και οργανισμούς, αλλά και αν είναι, τότε η ιδιωτικότητα συμβολίζει τη δυνατότητα του ατόμου να ασκεί σε σημαντικό

βαθμό έλεγχο πάνω στη χρήση των προσωπικών του δεδομένων. Να σημειωθεί εδώ, πως ο όρος «προσωπικά δεδομένα» στο διαδίκτυο δε διαφέρει από την γενικότερη περιγραφή που δόθηκε. Ωστόσο, στο διαδίκτυο ο προαναφερθέν όρος θεωρείται οποιαδήποτε πληροφορία σχετίζεται και είναι ικανή να ταυτοποιήσει ένα άτομο [17].

Ένας βασικός στόχος για την καθιέρωση ενός ηλεκτρονικού συστήματος διαχείρισης ταυτότητας είναι η εξασφάλιση μεγαλύτερης εμπιστοσύνης για την ταυτότητα του χρήστη. Ανάλογα με τον τρόπο με τον οποίο υλοποιείται ένα τέτοιο σύστημα διαχείρισης ηλεκτρονικής ταυτότητας, το σύστημα αυτό θα μπορούσε να παρέχει τη δυνατότητα παρακολούθησης άκρως προσωπικών πληροφορίων των πολιτών. Για αυτούς τους λόγους, τα συστήματα διαχείρισης ταυτότητας συχνά απαιτούν υψηλά επίπεδα εμπιστοσύνης στον πάροχο ταυτότητας (φορείς της κυβέρνησης συνήθως) για να γίνουν αποδεκτά. Επιπρόσθετα, δεν παρουσιάζουν όλες οι κοινωνίες τα ίδια επίπεδα εμπιστοσύνης στις κυβερνήσεις τους για να εκπληρώσουν αυτόν τον ρόλο. Οι κυβερνήσεις στο Ηνωμένο Βασίλειο, στις ΗΠΑ, στον Καναδά, στη Νέα Ζηλανδία και στην Αυστραλία ειδικότερα αντιμετώπισαν μοναδικές προκλήσεις όσον αφορά την εφαρμογή νέων συστημάτων διαχείρισης ταυτότητας σε σύγκριση με άλλες χώρες. Οι πολίτες φαινομενικά δεν επιθυμούν να εμπιστεύονται τις προθέσεις της κυβέρνησης, καθώς τις περισσότερες φορές αυτές οι προθέσεις σχετίζονται με το να ασκούν ισχυρό δημόσιο έλεγχο και αντικρούουν τις απαιτήσεις για μεγαλύτερο έλεγχο από την πλευρά των πολιτών και για ισχυρά μέτρα προστασίας της ιδιωτικής ζωής. Αντίθετα, οι σκανδιναβικές χώρες έχουν εφαρμόσει συστήματα διαχείρισης ταυτότητας με μοναδικά αναγνωριστικά στοιχεία τα οποία δεν ακολουθούν ισχυρά μοντέλα που βασίζονται στο ιδιωτικό απόρρητο, βασισμένα στον έλεγχο των χρηστών, χωρίς να προκαλούν διαμάχες. Παρομοίως, η Σιγκαπούρη και άλλα ασιατικά έθνη έχουν εφαρμόσει με επιτυχία συστήματα τα οποία δεν θεωρούνται συμβατά με ένα ισχυρό μοντέλο που βασίζεται στην προστασία της ιδιωτικής ζωής και του χρήστη [18].

Σημαντική προσθήκη στο ισχύον νομικό πλαίσιο είναι ο νέος Γενικός Κανονισμός για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα (General Data protection Regulation – GDPR). Το GDPR είναι μια νέα νομοθεσία για την ασφάλεια των δεδομένων και της ιδιωτικής ζωής που αναπτύχθηκε από το Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο για την προστασία των δικαιωμάτων των πολιτών της ΕΕ που σχετίζονται με τα προσωπικά τους δεδομένα. Οι εταιρείες (συμπεριλαμβανομένων των ιστοτόπων, εφαρμογών για κινητά και υπολογιστές, κ.λπ.) που πραγματοποιούν επιχειρηματικές συναλλαγές με πολίτες της ΕΕ επηρεάζονται ήδη από τον κανονισμό αυτό. Στις 25 Μαΐου 2018 το GDPR αντικατέστησε τον υφιστάμενο νόμο για την προστασία των δεδομένων, δηλαδή την οδηγία για την προστασία των δεδομένων που ισχύει από το 1998. Ένας από τους βασικούς στόχους και απαιτήσεις του GDPR είναι να ενημερώνονται οι πολίτες της ΕΕ για τον τρόπο συλλογής, χρήσης, διαμοιρασμού, ασφάλειας και επεξεργασίας των προσωπικών τους δεδομένων. Θα δώσει έτσι τον έλεγχο πάνω στα δεδομένα του ατόμου στο ίδιο το άτομο, απλοποιώντας το κανονιστικό νομικό πλαίσιο των διεθνών επιχειρήσεων, αφού θα έχει ενοποιήσει τον κανονισμό εντός της Ε.Ε. [19].

Συμπερασματικά, ο βασικός παράγοντας που κάνει τη διαφορά εδώ είναι οι σχέσεις των πολιτών με τις κυβερνήσεις τους. Όταν οι πολίτες είναι πεπεισμένοι ότι η κυβέρνησή τους είναι αξιόπιστη και οι πληροφορίες τους διακινούνται και τίθενται σε επεξεργασία υπό τον κατάλληλο έλεγχο, είναι λιγότερο πιθανό να ζητήσουν τον άμεσο έλεγχο αυτών των πληροφοριών. Αντίθετα, όταν οι πολίτες είναι λιγότερο σίγουροι για την αξιοπιστία της κυβέρνησης και ανησυχούν ότι οι ιδιωτικές πληροφορίες σε κυβερνητικά χέρια θα μπορούσαν να καταστρατηγηθούν, να χρησιμοποιηθούν για άσχετους σκοπούς ή να μην προστατευθούν σωστά, ίσως είναι πιο πιθανό να απαιτήσουν άμεσο έλεγχο των πολιτών για τη διαχείριση της ταυτότητας. Αναπόφευκτα, λοιπόν, οι πολίτες, για να μπορέσουν να εμπιστευτούν τις κυβερνήσεις τους και τα νέα συστήματα διαχείρισης ταυτότητας που αυτές θέλουν να εισάγουν, έχουν την ανάγκη να καλύπτονται από το κατάλληλο νομικό πλαίσιο σχετικά με την προστασία των δεδομένων τους.

2.4.3 Αυθεντικοποίηση

Παραδοσιακά, οι διαδικτυακοί χρήστες μίας υπηρεσίας αποτελούν έναν αδύναμο σύνδεσμο του «έξω κόσμου» με το σύστημα της υπηρεσίας από την άποψη της ασφάλειας. Παρότι είναι απαραίτητοι για την ύπαρξή της, οι χρήστες της μπορούν να δημιουργήσουν προβλήματα στο δίκτυο της υπηρεσίας και για τον λόγο αυτόν θεωρείται υψίστης σημασίας ο αποτελεσματικός έλεγχος εισόδου χρηστών. Αυτό μπορεί να επιτευχθεί μέσω της αυθεντικοποίησης των χρηστών. Η «Αυθεντικοποίηση» ορίζεται ως η απόδειξη ότι ο ισχυρισμός ενός χρήστη για την ταυτότητά του είναι έγκυρος και αυθεντικός και για να γίνει αυτό χρειάζεται «αποδείξεις ταυτότητας». Σε διαδικτυακές τεχνολογίες, τα φυσικά μέσα δε μπορούν να χρησιμοποιηθούν από μόνα τους ως ταυτότητες (όπως, η άδεια οδήγησης που αυθεντικοποιεί κάποιον ως οδηγό), άρα χρειάζεται να παρουσιάσει κάτι διαφορετικό ο χρήστης για να ταυτοποιηθεί. Αυτό τυπικά σημαίνει ότι ο χρήστης θα πρέπει να «απαντήσει» με τα προσωπικά του στοιχεία-credentials όταν ζητήσει πρόσβαση στην υπηρεσία που θέλει. Γενικά, για τους σκοπούς διαδικτυακής αυθεντικοποίησης, ως προσωπικά στοιχεία-credentials ενός χρήστη θεωρούνται κάτι που μπορεί να ξέρει, να έχει ή να είναι ένας χρήστης. Να σημειωθεί, ωστόσο, ότι μετά τη διαδικασία της αυθεντικοποίησης, πρέπει από τη μία να δοθεί εξουσιοδότηση (authorization) και από την άλλη να καταγραφούν όλες αυτές οι επικοινωνίες με την υπηρεσία σε μία βάση δεδομένων (accounting).

Αναλυτικότερα, σε ό,τι αφορά τα προσωπικά στοιχεία-credentials του χρήστη και τις κατηγορίες τους, έχουμε τις εξής:

- *Τι ξέρει ο χρήστης*: Οι άνθρωποι-χρήστες μίας υπηρεσίας γνωρίζουν με πολλές λεπτομέρειες πληροφορίες για τη ζωή τους (γενέθλια, επετείους, σημαντικές ημερομηνίες, ονόματα και άλλα) που μπορούν να τις χρησιμοποιήσουν ως στοιχεία απλής αυθεντικοποίησης, καθώς αυτό είναι βολικό αφού μπορούν να τα θυμούνται εύκολα. Αυτό όμως που οι απλοί χρήστες δεν αντιλαμβάνονται εύκολα είναι ότι τέτοιες πληροφορίες δεν είναι ασφαλείς. Στο διαδίκτυο

χρησιμοποιούνται ευρέως τέτοιου είδους κωδικοί και PIN λόγω ευκολίας απομνημόνευσης, αλλά, αν δεν έχουν προδιαγραφεί με συγκεκριμένους κανόνες, π.χ., για ελάχιστο αριθμό χαρακτήρων ή απαραίτητο συνδυασμό πεζών-κεφαλαίων-αριθμών-συμβόλων, προσφέρουν λίγη έως καμία ασφάλεια. Πολλοί οργανισμοί, δυστυχώς, για ελάττωση του κόστους, επιτρέπουν τη χρήση τέτοιων απλών κωδικών, εξασφαλίζοντας εύκολη πρόσβαση αλλά με αδύναμα credentials. Επιπροσθέτως, λόγω της αυξανόμενης ανάγκης για χρήση όλο και περισσότερων τέτοιων κωδικών στο διαδίκτυο, πολλοί χρήστες τους σημειώνουν κοντά/μπροστά στον υπολογιστή τους, μειώνοντας κι άλλο την ασφάλεια, καθώς κάποιος με απλή πρόσβαση στον χώρο του υπολογιστή αποκτά ταυτόχρονη πρόσβαση στον λογαριασμό του χρήστη στην υπηρεσία.

- *Τι έχει ο χρήστης*: Σε αυτήν την κατηγορία ανήκουν αυτά που ένας άνθρωπος μπορεί να αποκτήσει κατά τη διάρκεια της ζωής του και είναι τεχνητά επίκτητα. Δηλαδή, για να ελεγχθεί καλύτερα η αυθεντικοποίηση ενός χρήστη σε ένα σύστημα, συνηθίζεται πλέον να δίνεται στους χρήστες μία προσωπική «συσκευή» την οποία γνωρίζει ο υπεύθυνος διακομιστής αυθεντικοποίησης (authentication server) της υπηρεσίας. Όταν αυτή η συσκευή χρησιμοποιηθεί προς το δίκτυο από τον χρήστη, τον αυθεντικοποιεί δίνοντάς του πρόσβαση. Τέτοιου είδους συσκευές είναι τα έξυπνα κινητά τηλέφωνα (smartphones), οι έξυπνες κάρτες (smart cards), φορητά μέσα αποθήκευσης δεδομένων (usb sticks) και άλλες πολλές, είτε μόνο σε φυσική μορφή (hardware) είτε μόνο σε ηλεκτρονική (software). Αυτές οι ηλεκτρονικές, κατά κύριο λόγο, συσκευές εκμεταλλεύονται τη δυνατότητα αποθήκευσης σε αυτές κρυπτογραφημένων κλειδιών, των οποίων τον αλγόριθμο κρυπτογράφησης γνωρίζει ο διακομιστής αυθεντικοποίησης, δημιουργώντας έτσι One-Time-Passwords (OTPs), τα οποία χρησιμοποιούνται για την είσοδο του χρήστη στο σύστημα.
- *Τι είναι ο χρήστης*: Σε επόμενο στάδιο, με την πρόοδο της τεχνολογίας αλλά και της βιοϊατρικής, έχουν δημιουργηθεί μέσα που ταυτοποιούν έναν άνθρωπο ως οντότητα σε σχέση με κάτι μοναδικό που είναι/έχει εκ γενετής, όπως το δακτυλικό του αποτύπωμα, το πρόσωπό του, η φωνή του ή η ίριδα του ματιού του. Αυτά τα μέσα παρέχουν πολύ μεγάλη ασφάλεια σε ένα σύστημα που τα χρησιμοποιεί, γι' αυτό και παρουσιάζουν αυξημένο κόστος, καθώς απαιτούνται οι ειδικοί αναγνώστες/σαρωτές αποτυπώματος, προσώπου, φωνής ή/και ίριδας [20].

2.4.3.1 Μέθοδοι Αυθεντικοποίησης

Όπως αναφέρθηκε, η αυθεντικοποίηση είναι η μέθοδος που χρησιμοποιείται ώστε να επιβεβαιωθεί ότι ένας χρήστης είναι αυτός που ισχυρίζεται ότι είναι. Για να επιτευχθεί αυτός ο έλεγχος, το εκάστοτε σύστημα παρουσιάζει μία ή παραπάνω «δοκιμασίες» στον χρήστη: για κάτι που ξέρει ή/και για κάτι που έχει ή/και για κάτι που είναι.

Συχνά, μία μόνο κατηγορία από τις δοκιμασίες αυτές δεν είναι αρκετή καθώς ένας κωδικός μπορεί να υποκλαπεί, μία συσκευή (token) μπορεί να κλαπεί ή το αποτύπωμα μπορεί να συλλεχτεί από ένα αντικείμενο για παράδειγμα. Έτσι, για να παρέχεται μεγαλύτερη ασφάλεια και ισχυρότερη αυθεντικοποίηση, ένα σύστημα μπορεί να παρουσιάσει στον χρήστη έναν συνδυασμό δοκιμασιών που απαιτούνται να περάσει ώστε να αυθεντικοποιηθεί, όπως, παραδείγματος χάριν, χρήση κωδικού πρόσβασης (password) και συσκευής (token). Το ρίσκο που εμπεριέχει, βέβαια, ένας συνδυασμός μεθόδων αυθεντικοποίησης είναι η αύξηση του κόστους του συστήματος που θα κληθεί να υποστηρίξει ένα τέτοιο πρωτόκολλο. Αυτό το πρωτόκολλο ονομάζεται «Αυθεντικοποίηση Δύο Παραγόντων» (Two-Factor Authentication).

Παρακάτω, αναφέρονται πιο αναλυτικά διάφορες μέθοδοι αυθεντικοποίησης που χρησιμοποιούνται από σύγχρονα συστήματα που χρειάζονται έγκυρη αυθεντικοποίηση των χρηστών τους, υπό τη μορφή θετικών και αρνητικών στοιχείων του καθενός.

- Κωδικός πρόσβασης (Password)

Θετικά:

- απαίτηση κανόνων κατά την εγγραφή για επίτευξη πολυπλοκότητας (ελάχιστος αριθμός χαρακτήρων, συνδυασμός πεζών-κεφαλαίων γραμμάτων και συμβόλων, κ.λπ.).
- γενικά εύκολο στη χρήση και οι χρήστες είναι συνηθισμένοι σε αυτήν τη μέθοδο.
- η χρήση φράσης πρόσβασης (passphrase) αποτελεί ένα ισχυρό εργαλείο ταυτοποίησης.

Αρνητικά:

- χρειάζεται εγγραφή (registration) είτε από τον χρήστη είτε από τον διαχειριστή.
- συχνά είναι συνδυασμός του ονοματεπωνύμου του χρήστη, άρα εύκολα μαντεύεται (πρόβλημα ασφάλειας).
- συχνά δημιουργούνται πολύ αδύναμα passwords (π.χ., αριθμός κινητού τηλεφώνου, ημερομηνίες γέννησης, κ.λπ.).
- τα ισχυρά passwords μπορεί να ξεχαστούν ή να κλαπούν (αν σημειωθούν κάπου για να μην ξεχαστούν).

- Κωδικός πρόσβασης μίας χρήσης (One-Time Password)

Θετικά:

- υπάρχουν διάφοροι τύποι OTP: Paper Tokens, Hard Tokens, SMS Text, Soft Tokens (Mobile Apps).
- μπορεί να παραχθεί και να χρησιμοποιηθεί εύκολα και άμεσα είτε από μία απλή συσκευή ή ακόμα και από ένα πρόγραμμα (εφαρμογή) σε υπολογιστή ή κινητό.

- ο συγχρονισμός μπορεί να γίνει με βάση την ώρα, κάτι που διευκολύνει αρκετά την υλοποίησή του αλλά προστατεύει το σύστημα από τυχόν αποσυγχρονισμούς.

Αρνητικά:

- η υλοποίηση κάποιων μεθόδων αυθεντικοποίησης μπορεί να είναι δαπανηρή, όπως η αποστολή OTP μέσω SMS ή η απόκτηση συσκευής παραγωγής OTP.
- υπάρχει περίπτωση ο μηχανισμός που παράγει τον OTP να αποσυγχρονιστεί και μετά ο χρήστης να μην έχει δυνατότητα ταυτοποίησης .
- λόγω του συγχρονισμού, δεν υπάρχει η δυνατότητα παραπάνω από μία συσκευές να παράγουν OTP για συγκεκριμένο χρήστη.
- μπορεί να γίνει αποκρυπτογράφηση του αλγορίθμου παραγωγής του OTP.

➢ Βιομετρικά (Biometrics)

Θετικά:

- τα βιομετρικά χαρακτηριστικά του κάθε ατόμου είναι μοναδικά, οπότε δεν μπορούν να αντιγραφούν.
- δεν απαιτείται η τακτική αλλαγή των βιομετρικών στοιχείων ταυτοποίησης σε αντίθεση με έναν κοινό κωδικό.
- δεν απαιτεί μεγάλη προσπάθεια από τον χρήστη για την ταυτοποίησή του (π.χ., ίριδα ματιού ή δακτυλικό αποτύπωμα).

Αρνητικά:

- τα βιομετρικά χαρακτηριστικά είναι προσωπικά και αποθηκεύονται για το κάθε άτομο ξεχωριστά, υπάρχει κίνδυνος διαρροής τους σε περίπτωση υποκλοπής δεδομένων.
- υπάρχει περίπτωση αποτυχίας ταυτοποίησης λόγω προβληματικής συσκευής αναγνώρισης.
- υψηλό κόστος κατασκευής και υλοποίησης μηχανισμού βιομετρικών χαρακτηριστικών.
- σύνθετη ενσωμάτωση βιομετρικού ελέγχου σε σύστημα ταυτοποίησης χρηστών.

2.4.4 Διαχείριση Ταυτοτήτων στην Ηλεκτρονική Διακυβέρνηση

Τα Συστήματα Διαχείρισης Ταυτότητας μπορούν να προσδώσουν αρκετά πλεονεκτήματα σε ένα συνεργατικό αυτόνομο σύστημα που θα τα χρησιμοποιήσει. Ενδιαφέρον παρουσιάζει η περίπτωση ενός τέτοιου συστήματος του δημόσιου τομέα, αυτού της Ηλεκτρονικής Διακυβέρνησης (eGovernment). Βασικό ζήτημα στο οποίο πρέπει να δοθεί προσοχή κατά τον σχεδιασμό είναι η ετερογένεια και διαφορετικότητα των διαδικασιών, των δεδομένων και όλης της υποδομής μεταξύ των τοπικών και των κεντρικών υπηρεσιών διαχείρισης μίας χώρας (π.χ., δήμοι και κρατική κυβέρνηση), που είναι και αρκετά πιθανό να επιδεινώνονται από μικροπολιτικές σκοπιμότητες. Λόγω αυτών, παρουσιάζονται αρκετές προκλήσεις στον σχεδιασμό ενός Συστήματος

Διαχείρισης Ταυτότητας που θα κληθεί να υποστηρίξει την ΗΔ. Επιπρόσθετα, το ομοσπονδιακό μοντέλο θεωρείται απαραίτητο, καθώς η πολυεπίπεδη-κάθετη διαλειτουργικότητα που παρέχει ταιριάζει απόλυτα με τις ανάγκες της Ηλεκτρονικής Διακυβέρνησης.

Η Ομοσπονδιακή Ταυτότητα είναι ένα σύνολο μηχανισμών μέσω των οποίων οι οργανισμοί μπορούν να μοιράζονται πληροφορίες ταυτότητας μεταξύ τομέων ασφάλειας. Έτσι, οι οργανισμοί αυτοί έχουν τη δυνατότητα να αναπτύξουν εφαρμογές που βασίζονται στην ταυτότητα των χρηστών και έτσι να αυξήσουν την αποδοτικότητά τους σε ό,τι αφορά την ανταλλαγή πληροφοριών «εκτός συνόρων» του κάθε φορέα. Για τον λόγο αυτόν, η Ομοσπονδιακή Ταυτότητα βρίσκει εφαρμογή σε ένα μεγάλο εύρος φορέων και οργανισμών, δημόσιων και ιδιωτικών. Η διαφορά μεταξύ δημόσιου και ιδιωτικού φορέα, όμως, έγκειται στο γεγονός ότι ο δημόσιος θεσμός πρέπει να συνυπολογίσει πολλά ζητήματα, όπως την αναγκαία ένταξη, συνέχεια και διαλειτουργικότητα, αφού θα πρέπει να εξυπηρετεί ολόκληρο τον πληθυσμό στο πλαίσιο της Ηλεκτρονικής Διακυβέρνησης και όχι συγκεκριμένη μερίδα του, όπως με μια ιδιωτική υπηρεσία που δε θα τη χρησιμοποιούν όλοι οι πολίτες ενός κράτους.

Για τον εκσυγχρονισμό ενός κράτους, η διαχείριση ταυτότητας στην Ηλεκτρονική Διακυβέρνηση μπορεί να προσφέρει αποδοτικά, μέσω διαδικτύου, παροχή υπηρεσιών στους πολίτες και να συνεισφέρει στην επιβολή του νόμου σε ζητήματα εθνικής ασφάλειας. Συνεπώς, τα τελευταία χρόνια αρκετές κυβερνήσεις προσπαθούν να εγκρίνουν οδηγίες για την ανάπτυξη υπηρεσιών Ηλεκτρονικής Διακυβέρνησης, καθώς και μέτρα που αφορούν τον έλεγχο πρόσβασης στα ιστορικά, ατομικά στοιχεία των πολιτών, γεγονός που αποτελεί πρόκληση για μία σύγχρονη κυβέρνηση. Αυτό είναι εμφανές και από το γεγονός ότι μερικές χώρες επιλέγουν άλλες προσεγγίσεις στη διαχείριση ταυτότητας που εφαρμόζουν. Αυτές διαφοροποιούνται συνήθως ως προς το σχήμα ταυτότητας που υιοθετούν, την κουλτούρα και τις συνήθειες κάθε λαού και γενικότερα τις σχέσεις της κεντρικής κυβέρνησης με τους τοπικούς θερμούς, καθώς και της ικανότητάς τους να τις εφαρμόσουν [15].

2.5 Περιγραφή του προβλήματος

Σε ένα γενικό πλαίσιο, λοιπόν, η «Ηλεκτρονική Ταυτότητα» είναι το μέσο που χρησιμοποιεί ένας πολίτης ώστε να αποδείξει ηλεκτρονικά ότι είναι αυτός που ισχυρίζεται ότι είναι και άρα να αποκτήσει πρόσβαση σε ένα σύνολο από ηλεκτρονικές υπηρεσίες ΗΔ. Αυτή η ταυτότητα επιτρέπει σε μία οντότητα (πολίτης, επιχείρηση, διοίκηση) να ταυτοποιηθεί μοναδικά από οποιαδήποτε άλλη.

Όλες αυτές οι οντότητες αντιμετωπίζουν το ίδιο πρόβλημα σχετικά με την ηλεκτρονική τους παρουσία. Όλοι πρέπει να έχουν ηλεκτρονική παρουσία, να προστατεύονται από την κατάχρησή της, επιβεβαιώνοντας με αδιαμφισβήτητα στοιχεία το «ποιος συμμετέχει» στις ηλεκτρονικές συναλλαγές. Η ηλεκτρονική ταυτότητά τους θα πρέπει επίσης να μπορεί να λαμβάνει διάφορες μορφές ανάλογα με τις επιθυμίες των πολιτών. Σε ορισμένες περιπτώσεις, ένα άτομο μπορεί να επιθυμεί να παρουσιαστεί ως

διευθύνων σύμβουλος μιας εταιρείας και σε ξεχωριστό πλαίσιο ως δικαιούχος ασφαλιστικής κάλυψης υγείας. Ακόμη, όλοι πρέπει να έχουν διαθέσιμες περιγραφές για τον εαυτό τους. Είτε πρόκειται για έναν πολίτη που συμπληρώνει ένα ηλεκτρονικό διοικητικό έντυπο, είτε για μια επιχείρηση που προσφέρει μια υπηρεσία ή την προετοιμασία μιας προσφοράς, είτε για μια διοίκηση που επιθυμεί να μοιραστεί πληροφορίες, θα πρέπει να μην απαιτείται συνεχώς η ίδια σπατάλη χρόνου και χρημάτων που προκύπτει από την απάντηση στα ίδια ερωτήματα σε όλο και περισσότερες μορφές. Είναι επίσης σκόπιμο τα εμπιστευτικά δεδομένα να είναι αξιόπιστα και να θεωρούνται αυθεντικά.

Η δυνατότητα σύνδεσης ενός συνόλου πληροφοριών με έναν χρήστη (πολίτη, επιχείρηση, διοίκηση) και η αποτελεσματική και ασφαλής διαχείριση των δεδομένων που σχετίζονται με τους χρήστες είναι ουσιώδεις για πολλές διαφορετικές αλληλεπιδράσεις. Για τον σκοπό αυτό αναπτύσσονται οργανωτικές και τεχνικές υποδομές για τον καθορισμό, τον προσδιορισμό και τη διαχείριση της ταυτότητας που σχετίζεται με συγκεκριμένες ομάδες ατόμων, όπως πελάτες, ασθενείς ή πολίτες. Αυτές οι υποδομές είναι τα Συστήματα Διαχείρισης Ταυτότητας που αναλύσαμε παραπάνω. Στα σύγχρονα κράτη-μέλη της Ευρωπαϊκής Ένωσης έχουν δοθεί κίνητρα με σκοπό να εισάγουν την Ηλεκτρονική Ταυτότητα (eID) του πολίτη στις δημόσιες υπηρεσίες τους μέσω κάποιας Κεντρικής Διαδικτυακής Πύλης (portal) στις ηλεκτρονικές υπηρεσίες του εκάστοτε κράτους. Σε ευρωπαϊκό επίπεδο, υπάρχει η φιλοδοξία κάθε πολίτης να μπορεί να διασχίζει τα ευρωπαϊκά σύνορα και να έχει πρόσβαση σε τοπικές υπηρεσίες, ακόμα και μέσω του κινητού τηλεφώνου του. Πρακτικά, υπάρχει η ανάγκη για ένα διαλειτουργικό πλαίσιο το οποίο θα διευθετεί τα ζητήματα που ανακύπτουν σχετικά με τις απαιτήσεις της ηλεκτρονικής ταυτότητας σε ευρωπαϊκό επίπεδο και ουσιαστικά θα εκφράζει το πλάνο εφαρμογής της ηλεκτρονικής διακυβέρνησης. Πολλοί τομείς εφαρμογής της ηλεκτρονικής διακυβέρνησης αποτελούν υποψήφια πεδία ενσωμάτωσης σε αυτό το πλαίσιο ευρωπαϊκής ηλεκτρονικής διακυβέρνησης, γι' αυτό και είναι αναγκαία η ύπαρξη ενός διαλειτουργικού μηχανισμού ταυτότητας σε διασυνοριακή βάση. Τέτοιοι τομείς είναι η απλή ταυτότητα πολίτη, η κοινωνική ασφάλιση, η σύνταξη, η υγεία και νοσοκομειακή περίθαλψη, η έκδοση πιστοποιητικών και αδειών (οδήγησης και ασκήσεως επαγγέλματος), η φορολογία και άλλοι.

Συμπερασματικά, λοιπόν, είναι αναγκαίο να οργανωθεί ένα σύστημα που θα καλύπτει όλες αυτές τις ανάγκες των πολιτών μιας χώρας ηλεκτρονικά και σύγχρονα, τηρώντας ταυτόχρονα και όλες τις απαιτήσεις ασφάλειας των προσωπικών δεδομένων των πολιτών. Καθώς ένας πολίτης εμπλέκεται σε πολλούς τομείς της δημόσιας ζωής (φορολογία, κοινωνική ασφάλιση, εκπαίδευση, οικογένεια, κ.ά.) και ταυτόχρονα διαδραματίζει πολλαπλούς ρόλους (απλός πολίτης, δικηγόρος, πατέρας, κ.ά.), οι πληροφορίες που σχετίζονται με αυτόν πρέπει να διαχειρίζονται με ανεξάρτητο τρόπο. Αυτός ο τρόπος θα ορίζεται σε κατάλληλο νομικό πλαίσιο που θα διασφαλίζει σαφώς την προστασία των προσωπικών δεδομένων, αλλά και τον πλήρη προσωπικό έλεγχο του κάθε πολίτη πάνω στα δεδομένα που τον αφορούν.

Κεφάλαιο 3

Ανάλυση Απαιτήσεων Συστήματος και Αρχιτεκτονική

3.1 Απαιτήσεις Φυσικού Μέσου και Συστήματος Διαχείρισης Ταυτοτήτων

Το γεγονός ότι αυτό το πρωτοπόρο σύστημα "Ηλεκτρονικής Ταυτότητας Πολίτη" σχεδιάζεται ώστε να εφαρμοστεί στην ηλεκτρονική διακυβέρνηση καθορίζει τις απαιτήσεις και τις προϋποθέσεις που πρέπει να πληρούνται, ώστε να επιτελεί το σκοπό του. Πιο συγκεκριμένα, το φυσικό μέσο που θα παίζει το ρόλο της ταυτότητας ενός πολίτη σε μία ηλεκτρονική υπηρεσία θα έχει ισχύ αντίστοιχη με αυτήν της αστυνομικής του ταυτότητας, όταν προσέρχεται σε μία φυσική κρατική υπηρεσία. Δηλαδή θα έχει καίρια θέση σε μία πληθώρα κρατικών υπηρεσιών, διευκολύνοντας τόσο τους πολίτες στη χρήση τους, όσο και το κράτος στη διαχείρισή τους, μειώνοντας αρκετά γραφειοκρατικά ζητήματα της καθημερινότητας.

Έχοντας ορίσει και περιγράψει σαφώς την ηλεκτρονική ταυτότητα και το πλαίσιο του συστήματος που θα τη διαχειρίζεται, έχουν γίνει σαφείς οι περιορισμοί που θέτονται. Σε ό,τι αφορά την ιδιωτικότητα του πολίτη καθώς και τα προσωπικά του δεδομένα είναι ύψιστης σημασίας για το συγκεκριμένο σύστημα. Μόνο στην περίπτωση που μπορεί το κράτος να εγγυηθεί την εχεμύθεια και την σωστή χρήση όλων αυτών των δεδομένων των πολιτών, θα μπορέσουν και αυτοί με τη σειρά τους να εμπιστευτούν ένα τέτοιο σύστημα και να αρχίσουν να το χρησιμοποιούν, με τελικό σκοπό να βελτιώσει τις υπηρεσίες που λαμβάνουν. Ένα τέτοιο κρίσιμης σημασίας σύστημα για ένα κράτος πρέπει να προδιαγραφεί σωστά και με αυστηρό τρόπο, ώστε να προβλεφθούν όλες οι ειδικές περιπτώσεις πολιτών, ώστε να συμπεριφέρεται σωστά το σύστημα, να παραμένει αδιάβλητο και με σαφώς όσο το δυνατόν μικρότερο κόστος κατασκευής και συντήρησης. Τέτοια ζητήματα, λοιπόν, αποτελούν τις λειτουργικές και μη λειτουργικές απαιτήσεις του συστήματος διαχείρισης ηλεκτρονικών ταυτοτήτων. Ακόμη, πρέπει να ληφθούν σοβαρά υπόψιν οι διαθέσιμες επιλογές σχετικά με τα φυσικά μέσα που θα "γίνουν" εν τέλει η ίδια η ηλεκτρονική ταυτότητα. Τέλος, όλα τα παραπάνω θα πρέπει να λειτουργούν με γνώμονα τους πολίτες ανεξαρτήτως ηλικίας και μόρφωσης, δηλαδή θα πρέπει να προβλεφθεί η καθολική και εύκολη μετάβαση σε αυτό το πλαίσιο ηλεκτρονικής ταυτοποίησης, παρέχοντας τελικά μια απροβλημάτιστη και απρόσκοπτη αλληλεπίδραση με τους χρήστες.

Τα παραπάνω αποτελούν μία γενική, ποιοτική περιγραφή των απαιτήσεων του συστήματος και στη συνέχεια του κεφαλαίου ακολουθεί ανάλυση σε βάθος όσων προηγήθηκαν.

3.1.1 Απαιτήσεις ασφάλειας και προστασίας της ιδιωτικότητας

Μέσω της ηλεκτρονικής διακυβέρνησης πρέπει, λοιπόν, να διασφαλίζεται η διαφάνεια και η αποτελεσματικότητα των κυβερνητικών διαδικασιών και υπηρεσιών. Γίνεται χρήση τεχνολογιών πληροφορίας και επικοινωνίας, κι έτσι παρέχεται στους πολίτες ένα σύνολο ηλεκτρονικών υπηρεσιών σε πραγματικό χρόνο από τους δημόσιους οργανισμούς. Ωστόσο, αυτή η συνεργασία μεταξύ δημόσιων υπηρεσιών και ηλεκτρονικών συναλλαγών προϋποθέτει και απαιτεί την ανταλλαγή πολλών, προσωπικών και κυρίως ευαίσθητων δεδομένων των πολιτών, γεγονός που την καθιστά τη μεγαλύτερη ανησυχία των πολιτών ως προς τη χρήση τους. Είναι αναγκαίο για τους πολίτες να έχουν τον απόλυτο έλεγχο πάνω σε όλων των ειδών τις πληροφορίες που τους αφορούν και γενικότερα, να μην τίθεται σε κανένα κίνδυνο έκθεσης η ιδιωτικότητά τους. Προφανώς, για την ουσιαστική λειτουργία αυτών των υπηρεσιών απαιτείται η συγκέντρωση μεγάλου όγκου πληροφοριών για κάθε πολίτη γι' αυτό και οποιαδήποτε αποκάλυψη μπορεί να οδηγήσει στην ταυτοποίησή του και κατ' επέκταση στην παραβίαση της ιδιωτικότητάς του. Γίνεται σαφές, άρα, ότι το ζήτημα προστασίας των δεδομένων των πολιτών έχει ιδιαίτερη βαρύτητα στην τελική εφαρμογή των υπηρεσιών ηλεκτρονικής διακυβέρνησης, αφού ο τρόπος με τον οποίο θα διαφυλαχτεί τελικά αυτή, επηρεάζει την αποτελεσματικότητα των υπηρεσιών αυτών.

Οι υπηρεσίες ηλεκτρονικής διακυβέρνησης έχουν κάποια διαφοροποιητικά στοιχεία που τις ξεχωρίζουν από άλλες ηλεκτρονικές υπηρεσίες που σχετίζονται με την προστασία της ιδιωτικότητας. Πιο συγκεκριμένα:

- Πολλά από τα δεδομένα που ανταλλάσσονται κατά τη χρήση υπηρεσιών ηλεκτρονικής διακυβέρνησης είναι υψίστου σημασίας και ευαισθησίας, όπως οικονομικά και φορολογικά δεδομένα, δεδομένα υγείας, το ποινικό μητρώο και άλλα.
- Υπάρχουν τύποι δεδομένων από αυτά που ανταλλάσσονται που αποτελούν ταυτοποιητικά στοιχεία για τους πολίτες, όπως ο αριθμός δελτίου ταυτότητας, ο αριθμός φορολογικού μητρώου, και άλλοι, γι' αυτό το λόγο και η συνδεσιμότητα μεταξύ των δεδομένων που χρησιμοποιούνται πρέπει να είναι άμεση.
- Μερικές από τις υπηρεσίες ηλεκτρονικής διακυβέρνησης για να μπορέσουν να αξιοποιηθούν, χρειάζονται μία αρκετά συγκεκριμένη ροή διαδικασιών και δεδομένων μεταξύ των διαφόρων συστημάτων, γεγονός που αυξάνει τη συνολική αλληλεπίδραση πολλαπλών ετερογενών φορέων και δομών με σκοπό την ανταλλαγή και τον διαμοιρασμό αρχείων.
- Συγκεκριμένοι τύποι ροών εργασιών και δεδομένων είναι πιθανόν να απαιτούν αλληλεπίδραση με φορείς εκτός των συνόρων μια χώρας.
- Συνήθως, το σύνολο τέτοιων υπηρεσιών παρέχονται από ένα κεντρικό σημείο πρόσβασης των πολιτών στις υπηρεσίες ηλεκτρονικής διακυβέρνησης, δηλαδή μέσω μίας κεντρικής διαδικτυακής πύλης, και δημιουργεί αναπόφευκτα νέα ζητήματα προστασίας δεδομένων των πολιτών, αφού αυτή είναι ουσιαστικά ο

μεσολαβητής και άρα συγκεντρώνει διαφορετικά δεδομένα και επιτελεί κρίσιμες διαδικασίες όπως αυτή της ταυτοποίησης των πολιτών.

- Συχνά, εμφανίζονται αντιθέσεις ή ζητήματα που χρήζουν αποσαφήνισης σχετικά με το υφιστάμενο πλαίσιο για την προστασία των προσωπικών δεδομένων και με αυτό που πρέπει να εφαρμόζεται από υπηρεσίες ηλεκτρονικής διακυβέρνησης.

Με βάση τα παραπάνω κρίνεται αναγκαία η ανάπτυξη και η χρήση εξελιγμένων τεχνολογιών που θα διασφαλίζουν ότι όλα τα προσωπικά και ευαίσθητα δεδομένα των πολιτών είναι απόλυτα προστατευμένα και διασφαλισμένα. Για να γίνει βέβαια αυτό πρέπει να ληφθούν ιδιαιτέρως σοβαρά υπόψιν τα χαρακτηριστικά που διέπουν τις υπηρεσίες ηλεκτρονικής διακυβέρνησης, με απώτερο σκοπό την επίλυση όλων των ζητημάτων ιδιωτικότητας που αναφέρθηκαν.

3.1.2 Λειτουργικές και μη λειτουργικές απαιτήσεις του συστήματος

Ο διαδικτυακός τόπος που θα αποτελεί την πύλη εισόδου των πολιτών στις υπηρεσίες ηλεκτρονικής διακυβέρνησης ή και των επιχειρήσεων ή άλλων φορέων θα πρέπει γενικά να συμμορφώνεται και να διέπεται από κάποιες συγκεκριμένες θεμελιώδεις αρχές. Με βάση αυτές θα μπορέσουμε στη συνέχεια να εξάγουμε πιο συγκεκριμένες λειτουργικές και μη λειτουργικές απαιτήσεις για το σύστημα μας. Αναλυτικότερα έχουμε την:

- Αρχή της ισότητας και της ισονομίας: Οι φορείς της δημόσιας διοίκησης θα πρέπει να περιορίζουν αποτελεσματικά την πρόσβαση στις πληροφορίες και στις υπηρεσίες που παρέχουν μέσω των διαδικτυακών τους τόπων, εξασφαλίζοντας κυρίως: την τεχνολογική ανεξαρτησία στην πρόσβαση στην πλατφόρμα, την κάλυψη αναγκών ειδικών ομάδων όπως άτομα με αναπηρία και κυρίως την προστασία των ανθρώπινων δικαιωμάτων.
- Αρχή της πληρότητας και της αξιοπιστίας: Οι πληροφορίες που παρέχονται στους πολίτες μέσω των υπηρεσιών ηλεκτρονικής διακυβέρνησης, των φορέων δηλαδή της δημόσιας διοίκησης πρέπει να είναι ορθές, πλήρεις και επικαιροποιημένες.
- Αρχή της εμπιστοσύνης: Καθώς η πρόσβαση στις παρεχόμενες υπηρεσίες θα γίνεται μέσω της κεντρικής διαδικτυακής πύλης θα πρέπει αυτή να συμβάλλει στη δημιουργία σχέσης εμπιστοσύνης με τους πολίτες που επισκέπτονται τον ιστότοπο και τον χρησιμοποιούν, εφαρμόζοντας έμπρακτα τους κατάλληλους και εξελιγμένους μηχανισμούς ασφάλειας και προστασίας προσωπικών δεδομένων.
- Αρχή της σωστής διαχείρισης δημόσιων πόρων: Σαφώς, για την ανάπτυξη, εφαρμογή, υποστήριξη και συντήρηση ενός τέτοιου καθολικού συστήματος στη δημόσια διοίκηση απαιτείται μία μεγάλη επένδυση, η οποία πρέπει να δικαιολογείται από το πόσο θα ωφεληθούν οι πολίτες από τη χρήση αυτής της

δημόσιας Κεντρικής Διαδικτυακής Πύλης και των υπηρεσιών που αυτή θα παρέχει.

- Αρχή της ανοιχτής διάθεσης και χρήσης δημόσιων πληροφοριών: Όσες από τις πληροφορίες θα διατίθενται από τη χρήση και λειτουργία αυτού του διαδικτυακού τόπου της δημόσιας διοίκησης θα πρέπει να είναι διαθέσιμες χωρίς τεχνικούς ή νομικούς περιορισμούς, να είναι μηχαναγνώσιμο και να του αντιστοιχούν κυβερνητικές άδειας με όρους χρήσης.

Με βάση τις παραπάνω αρχές, πλέον, μπορούμε να εξάγουμε τις απαιτήσεις ενός συστήματος παροχής υπηρεσιών Ηλεκτρονικής Διακυβέρνησης:

Λειτουργικές Απαιτήσεις:

- Εξουσιοδότηση (Authorization)
- Έλεγχος ταυτότητας (Identification – Authentication)

Μη Λειτουργικές Απαιτήσεις:

- Απαιτήσεις ασφάλειας (Security Requirements)
- Ακεραιότητα (Integrity)
- Εμπιστευτικότητα (Confidentiality)
- Διαθεσιμότητα (Availability)
- Εμπιστοσύνη (Trust)
- Μη-Αποποίηση Ευθύνης (Non-Repudiation)
- Προστασία των δεδομένων (Data protection)
- Αυθεντικότητα (Authenticity)
- Απόδοση Συστήματος (System Efficiency)
- Αξιοπιστία Συστήματος (System Reliability)
- Επεκτασιμότητα (Scalability)
- Διαλειτουργικότητα (Interoperability)
- Χρηστικότητα (Usability)
- Φιλικότητα προς το χρήστη (User Friendliness)
- Εξοικονόμηση κόστους – χρόνου (Cost-Time Efficiency)

3.1.3 Περιγραφή των φυσικών μέσων που μπορούν να χρησιμοποιηθούν ως eID και σύγκριση αυτών

Οποιαδήποτε εξέλιξη της τεχνολογίας οδηγεί συνεχώς σε αυξανόμενες εναλλακτικές σε φυσικά μέσα, που ενσωματώνουν νέες και καινοτόμες τεχνογνωσίες, τα οποία μπορούν να χρησιμοποιηθούν ως ηλεκτρονικές ταυτότητες για τους πολίτες. Κάθε μία κατηγορία από τα διαφορετικά είδη φυσικών μέσων έχει προφανώς συγκεκριμένα πλεονεκτήματα και μειονεκτήματα κατά τη χρήση της ή κατά τη διαδικασία εφαρμογής της χρήσης της από το ευρύ κοινό. Παρακάτω παρουσιάζονται οι σύγχρονες λύσεις που θα μπορούσαν να χρησιμοποιηθούν σε ένα σύστημα Ηλεκτρονικής Ταυτότητας Πολίτη, μαζί με μία λίστα από πλεονεκτήματα και μειονεκτήματα κάθε μίας από αυτές, ώστε να μελετηθούν και να ερευνηθούν. Τελικός

σκοπός αυτής της μελέτης, σε συνδυασμό με τις άλλες παραμέτρους σχετικά με το σχεδιασμό ενός τέτοιου πολύπλοκου και απαιτητικού συστήματος, είναι η επιλογή του καταλληλότερου μέσου για να επιτελέσει στην πράξη την "Ηλεκτρονική Ταυτότητα Πολίτη".

1. RFID (tags - παθητικές ετικέτες)

Πλεονεκτήματα:

- Τα δεδομένα της ετικέτας μπορούν να μεταβάλλονται συνεχώς δεν απαιτείται η τακτική αλλαγή των βιομετρικών στοιχείων ταυτοποίησης σε αντίθεση με ένα κοινό κωδικό.
- Ταχύτερη συλλογή δεδομένων και λειτουργία χωρίς να χρειάζεται επαφή.
- Σε περίπτωση απώλειας της ετικέτας, η αντικατάστασή της είναι οικονομική.
- Για την αποφυγή συμβάντων παρανομίας, κάποια συστήματα συνδυάζουν τον σειριακό αριθμό με ένα απλό πρωτόκολλο πρόκλησης-απόκρισης.

Μειονεκτήματα:

- Παρουσιάζονται αρκετά προβλήματα στην ασφάλεια και στην ιδιωτικότητα (απαιτείται PIN για να είναι ασφαλές).
- Το κόστος υλοποίησης της τεχνολογίας RFID είναι υψηλό καθώς απαιτείται εκτός από την ετικέτα και ο αναγνώστης.
- Υπάρχει το ενδεχόμενο να παρουσιαστούν προβλήματα κατά την ανάγνωση της ετικέτας διότι η εμβέλεια της ανάγνωσης είναι συνήθως μικρή.
- Κάποια συστήματα έχουν χαμηλές ταχύτητες μετάδοσης δεδομένων από την ετικέτα στον αναγνώστη.
- Επειδή η τεχνολογία RFID βασίζεται στα ραδιοκύματα, θα πρέπει να λαμβάνονται υπόψη διάφορα συνήθη ζητήματα που αφορούν τις ραδιοσυχνότητες, όπως η αντανάκλαση, περίθλαση/παράθλαση, εξασθένηση και παρεμβολή.

2. Κάρτες (smart cards)

Πλεονεκτήματα:

- Είναι εύχρηστες.
- Οι έξυπνες κάρτες διαθέτουν εκτός από CPU και μνήμη ROM για την αποθήκευση του λειτουργικού συστήματος, μνήμη RAM ια γρήγορη εκτέλεση υπολογισμών και μνήμη EEPROM για την αποθήκευση εφαρμογών και δεδομένων.
- Οι περισσότερες κάρτες χρησιμοποιούν κρυπτογραφημένα δεδομένα.
- Ο μικροεπεξεργαστής της κάρτας απαιτεί την χρήση αναγνώστη, οπότε και μπορεί η κάρτα να προγραμματιστεί ώστε να αναγνωρίζεται από συγκεκριμένους αναγνώστες.
- Σε περίπτωση απώλειας, η αντικατάστασή της είναι οικονομική.

- Για ανάγκες υψηλότερης ασφάλειας και πρόσβαση σε συγκεκριμένες υπηρεσίες ή πληροφορίες, μία έξυπνη κάρτα μπορεί να αποτελέσει μια συσκευή για την αποθήκευση πληροφοριών όπως η εικόνα ή άλλα βιομετρικά χαρακτηριστικά του χρήστη (π.χ. τα δαχτυλικά αποτυπώματα).
- Ως επί το πλείστον είναι επαναπρογραμματιζόμενες.
- Είναι συμβατές με φορητές ηλεκτρονικές συσκευές.
- Επιτρέπουν μεγάλη ασφάλεια, και αυτό οφείλεται στις πολύπλοκες κρυπτογραφικές τεχνικές που χρησιμοποιούνται για να κωδικοποιούν και να αποκωδικοποιούν τις πληροφορίες μεταξύ των καρτών και των άλλων συσκευών.

Μειονεκτήματα:

- Απαιτείται η χρήση ακριβού αναγνώστη ώστε να γίνει η ταυτοποίηση.
- Ο αναγνώστης πρέπει να συνδεθεί σε υπολογιστή εκτός και αν είναι ασύρματος (bluetooth), με το κόστος να αυξάνεται αρκετά.
- Εύκολα μπορεί να χαθούν.
- Δημιουργούν προβλήματα ασφάλειας σε περιπτώσεις απωλειών και κλοπών.

3. USB stick

Πλεονεκτήματα:

- Εύχρηστο και φορητό.
- Δε χρειάζεται ειδικό αναγνώστη.
- Μικρό κόστος απόκτησης.

Μειονεκτήματα:

- Απαιτείται ειδικό λογισμικό για την απαραίτητη κρυπτογράφηση.
- Σε περίπτωση απώλειας υπάρχει θέμα ασφάλειας (εκτός και αν για την ταυτοποίηση απαιτείται και PIN).
- Μπορεί να χρησιμοποιηθεί μόνο σε συνδυασμό με υπολογιστή, όχι με κινητό (εκτός και αν υπάρξει ειδική σύνδεση).

4. Εφαρμογή σε κινητό

Πλεονεκτήματα:

- Εύχρηστο και φορητό, ευρέως διαδεδομένο.
- Μηδενικό κόστος πέραν από τη συγγραφή της εφαρμογής.
- Ευελιξία στο είδος ταυτοποίησης και αυθεντικοποίησης που μπορεί να υποστηριχθεί (δαχτυλικό αποτύπωμα, username/password, PIN, κλπ.).
- Σε περίπτωση απώλειας, όποιος το βρει/κλέψει δε μπορεί χωρίς τα credentials του χρήστη ή το δακτυλικό του αποτύπωμα να ταυτοποιηθεί.
- Σε περίπτωση απώλειας επίσης μπορεί να γίνει απομακρυσμένο κλείδωμα του κινητού, αποτρέποντας οποιαδήποτε λειτουργία, άρα και διαρροή πληροφοριών του χρήστη.

Μειονεκτήματα:

- Εξάρτηση από τη μπαταρία.
- Απαραίτητη η χρήση smartphone και όχι οποιουδήποτε κινητού.
- Δυσκολία στην προσαρμογή μεγαλύτερων ανθρώπων (αναγκαία η περίοδος προσαρμογής).

5. Wearable συσκευές

Πλεονεκτήματα:

- Εύχρηστες, με δυνατότητα φορητότητας.
- Αμεσότητα στη χρήση, καθώς είναι σχεδιασμένες να εκτελούν συγκεκριμένες λειτουργίες.
- Ευκολία στην επικοινωνία δεδομένων και πληροφοριών.

Μειονεκτήματα:

- Περιορισμένες δυνατότητες, ιδιαίτερα στα είδη ταυτοποίησης και αυθεντικοποίησης που μπορούν να υποστηρίξουν.
- Μικρές στο μέγεθος, με αποτέλεσμα να αυξάνεται η πιθανότητα απώλειας τους
- Η διάρκεια της μπαταρίας είναι αρκετά περιορισμένη.
- Η αγορά μιας wearable συσκευής μπορεί να ξεπεράσει τις μερικές εκατοντάδες ευρώ.
- Αντίξοες καιρικές συνθήκες όπως ζέστη και υγρασία, μπορούν να προκαλέσουν μόνιμες βλάβες στις συσκευές.

3.1.4 Αλληλεπίδραση με το χρήστη

Στόχος της Ηλεκτρονικής Διακυβέρνησης και των υπηρεσιών που θα παρέχονται μέσω αυτής είναι να αξιοποιηθεί σωστά και αποδοτικά η τεχνολογία σχετικά με τις πληροφορίες και τις επικοινωνίες σήμερα, ώστε να αναβαθμιστούν ουσιαστικά οι υπηρεσίες εξυπηρέτησης και πληροφόρησης προς όλους τους πολίτες (άτομα ή επιχειρήσεις) που συναλλάσσονται με τη Δημόσια Διοίκηση, ελαχιστοποιώντας τα γραφειοκρατικά προβλήματα. Όλη η αλληλεπίδραση ενός χρήστη στις ηλεκτρονικά παρεχόμενες υπηρεσίες γίνεται μέσω της Κεντρικής Διαδικτυακής Πύλης (ΚΔΠ), η οποία θα πρέπει:

- Να παρέχει εύκολη και ασφαλή πρόσβαση στις υπηρεσίες εξυπηρέτησης των πολιτών.
- Να έχει ένα φιλικό προς τον χρήστη πρόσωπο (user friendly interface).
- Να γίνει μέρος της καθημερινότητας των πολιτών και να την προτιμάνε καθημερινά όλο και περισσότεροι πολίτες.
- Ανάλογα με τον κάθε χρήστη (πολίτης ή επιχείρηση) να παρέχει προσαρμοσμένο περιεχόμενο στις ανάγκες του καθενός.

Όπως έχουμε αναφέρει, το πλαίσιο διαλειτουργικότητας που θα πρέπει να εφαρμόζει η Κεντρική Διαδικτυακή Πύλη του συστήματος της Ηλεκτρονικής

Διακυβέρνησης ορίζει ότι η πύλη αυτή θα πρέπει να είναι το κεντρικό σημείο επαφής των πολιτών με τις υπηρεσίες που θα θέλουν να χρησιμοποιήσουν. Έτσι, θα πρέπει να προσφέρεται από την πύλη:

- Ένα μοναδικό σημείο που θα συγκεντρώνει και θα παρέχει στον χρήστη την ζητούμενη πληροφορία που είναι διαθέσιμη από τον εκάστοτε φορέα .
- Ένα σημείο κεντρικής ενημέρωσης των πολιτών για τις πρωτοβουλίες και τις δραστηριότητες της πολιτικής ηγεσίας.
- Ένα χώρο πρόσβασης που θα παρέχει οδηγίες προς τους πολίτες για πρακτικά ζητήματα χρήσης και αρμοδιότητας του κάθε φορέα.
- Σε περιπτώσεις που ένας φορέας, διαρθρώνεται σε πολλούς επιμέρους που παρέχονται μέσω της πύλης, χρειάζεται ένα κεντρικό σημείο πρόσβασης στο βασικό φορέα και μέσω αυτού θα δίνεται η πρόσβαση στους επιμέρους.

Για να εκπληρωθεί, λοιπόν, ο σκοπός χρειάζεται απαραιτήτως κλίμα εμπιστοσύνης και ασφάλειας στους πολίτες-χρήστες των υπηρεσιών. Για να εξασφαλιστεί αυτή η εμπιστοσύνη χρειάζεται οι χρήστες να αποκομίζουν μια καλή εμπειρία χρήσης από τις επισκέψεις τους στην πύλη. Για το λόγο αυτό, η χρηστικότητα και η λειτουργικότητά της πρέπει να ληφθούν πολύ σοβαρά υπόψη κατά το σχεδιασμό και την υλοποίηση των υπηρεσιών Ηλεκτρονικής Διακυβέρνησης και της Κεντρικής Διαδικτυακής Πύλης. Πιο συγκεκριμένα, η πύλη θα πρέπει:

- Να μην αποτελεί μια στείρα πηγή πληροφοριών προς τους χρήστες, αλλά να σχεδιαστεί κατάλληλα δίνοντας προτεραιότητα στις ανάγκες και τα ενδιαφέροντα των χρηστών, όπως αυτά έχουν καθοριστεί.
- Αναλόγως την κατηγορία του χρήστη που πρόκειται να τη χρησιμοποιήσει, να μπορεί να τους παρέχει προσωποποιημένες υπηρεσίες, αφού πρώτα ρυθμιστεί το ζήτημα της εγγραφής των χρηστών και κατ' επέκταση δημιουργηθεί κοινότητα χρηστών της πύλης.
- Να αποτελεί για τους χρήστες το μοναδικό, εγκεκριμένο από το κράτος σημείο παροχής πληροφοριών του συγκεκριμένου φορέα, αλλά και το μοναδικό σημείο εισόδου στις ηλεκτρονικές υπηρεσίες που προσφέρει ο φορέας αυτός.
- Να σχεδιαστεί κατάλληλα ώστε να επιτρέπει συνεχείς ενημερώσεις περιεχομένου, αλλά και έλεγχο του περιεχομένου που ήδη έχει ανεβαστεί εκεί.
- Να τηρεί όλα τα πλαίσια διαφάνειας προς το χρήστη που τη χρησιμοποιεί για το περιεχόμενο και τις υπηρεσίες που του παρέχει.

3.2 Συνολική περιγραφή της αρχιτεκτονικής του συστήματος

Οι πάροχοι ηλεκτρονικών υπηρεσιών θα προσφέρουν τις υπηρεσίες τους μέσω μίας Κεντρικής Διαδικτυακής Πύλης, αφού πρώτα δηλώσουν τις απαιτήσεις τους όσον αφορά στο επίπεδο αυθεντικοποίησης (π.χ., χρήση username/password, Ψηφιακό Πιστοποιητικό, Βιομετρικά κλπ.) για κάθε υπηρεσία, καθώς επίσης και τα όποια απαιτούμενα δικαιολογητικά πρέπει οι χρήστες να υποβάλουν κατά τη διαδικασία εγγραφής. Οι τελικοί χρήστες, αφού αρχικά εγγραφούν στην ηλεκτρονική υπηρεσία

μέσω της πύλης, μπορούν να αξιοποιήσουν τις προσφερόμενες ηλεκτρονικές υπηρεσίες αφού πρώτα ελεγχθεί και διαπιστωθεί η ορθότητα της ηλεκτρονικής τους ταυτότητας (αυθεντικοποίηση).

Δεδομένης της ύπαρξης της πύλης ως διαμεσολαβητή μεταξύ χρήστη και εξυπηρετητή κάθε ηλεκτρονικής υπηρεσίας, είναι επιτακτική η ανάγκη για την οικοδόμηση μιας σχέσης εμπιστοσύνης μεταξύ αυτής και του αντίστοιχου εξυπηρετητή, έτσι ώστε να επιτυγχάνεται η απαιτούμενη βεβαιότητα για τις "ταυτότητες" των οντοτήτων αυτών. Η δημιουργία της σχέσης αυτής βασίζεται στην ανταλλαγή ενός διακριτικού (token) που αξιοποιείται για την ταυτοποίηση και αυθεντικοποίησή τους. Επίσης, η δημιουργία ενός Εικονικού Ιδιωτικού Δικτύου (Virtual Private Network) μεταξύ τους μπορεί να διασφαλίσει μεταξύ άλλων και την εμπιστευτικότητα και ακεραιότητα των δεδομένων τα οποία ανταλλάσσονται πάνω από το ασφαλές κανάλι επικοινωνίας (secure communication channel) το οποίο δημιουργείται. Επιπλέον ενδέχεται να απαιτούνται και υπηρεσίες μη αποποίησης αποστολής και λήψης μηνύματος, καθώς και υπηρεσίες χρονοσήμανσης.

Για να μπορέσει ένας πολίτης να χρησιμοποιήσει μία ηλεκτρονική υπηρεσία, θα πρέπει πρώτα να εγγραφεί στην Κεντρική Διαδικτυακή Πύλη. Συγκεκριμένα, ο αιτών χρήστης συμπληρώνει την αίτηση εγγραφής δηλώνοντας τα στοιχεία του, επιλέγει μία προς μία τις ηλεκτρονικές υπηρεσίες που επιθυμεί να χρησιμοποιήσει, δηλώνει τα μοναδικά αναγνωριστικά που αντιστοιχούν στις υπηρεσίες που επέλεξε (π.χ., ΑΦΜ για την περίπτωση οικονομικών υπηρεσιών) και δηλώνει αν επιθυμεί, ανά παρεχόμενη υπηρεσία, να αποθηκευτεί στην πύλη το ανά περίπτωση απαιτούμενο αναγνωριστικό. Η Κεντρική Διαδικτυακή Πύλη δημιουργεί μία σχέση εμπιστοσύνης με τον εξυπηρετητή της κάθε υπηρεσίας που επιθυμεί να εγγραφεί ο αιτών χρήστης, ελέγχει τα στοιχεία του και κατά πόσο έχει δικαίωμα χρήσης της ηλεκτρονικής υπηρεσίας. Εφόσον τα αποτελέσματα των παραπάνω ελέγχων είναι σωστά, ο χρήστης ενημερώνεται για την επιτυχημένη εγγραφή του στην πύλη και τις ηλεκτρονικές υπηρεσίες και ακολούθως παραλαμβάνει τα διαπιστευτήριά του (π.χ., username και password ή ψηφιακό πιστοποιητικό), σύμφωνα με το επίπεδο αυθεντικοποίησης που έχει οριστεί για κάθε παρεχόμενη ηλεκτρονική υπηρεσία.

Ακολούθως, προκειμένου να χρησιμοποιήσει κάποια ηλεκτρονική υπηρεσία, ο χρήστης επισκέπτεται την πύλη και επιλέγει την υπηρεσία αυτή. Η πύλη, γνωρίζοντας το επίπεδο αυθεντικοποίησης που απαιτείται για τους αιτούντες προσπέλασης στην υπηρεσία αυτή, ενημερώνει το χρήστη για τα διαπιστευτήρια που απαιτείται να παρουσιάσει προκειμένου να του επιτραπεί η πρόσβαση. Ο χρήστης εισάγει τα διαπιστευτήριά του και εφόσον το αποτέλεσμα του σχετικού ελέγχου είναι θετικό, μπορεί να κάνει πλέον χρήση της αιτούμενης υπηρεσίας. Για την υποστήριξη παροχής επιπρόσθετων υπηρεσιών μη-αποποίησης, η πύλη θα πρέπει να διατηρεί αρχείο καταγραφής (log file) κάθε προσπάθειας αυθεντικοποίησης. Σε περίπτωση που η προσπάθεια είναι επιτυχημένη, το αρχείο περιλαμβάνει την ώρα, την ημερομηνία, το όνομα του χρήστη (username) και τα διαπιστευτήρια που αντιστοιχούν στη

συγκεκριμένη σύνοδο. Σε περίπτωση που αυτή είναι αποτυχημένη, το αρχείο περιλαμβάνει μόνον την ώρα, την ημερομηνία και το όνομα του χρήστη (username).

Οι πολίτες που επιθυμούν να έχουν πρόσβαση σε κάποια από αυτές τις υπηρεσίες δε χρειάζεται να εγγραφούν σε κάθε μία από αυτές ξεχωριστά, καθώς το σύστημα θα υποστηρίζει εφάπαξ πιστοποίηση ταυτότητας και την εν συνεχεία διάφανη διαβίβαση της πιστοποίησης του χρήστη σε πολλαπλούς παρόχους (Single Sign-On) για την εξυπηρέτηση των αιτημάτων τους. Για την ταυτοποίηση και αυθεντικοποίησή του στην πύλη απαιτείται η χρήση της προσωπικής ηλεκτρονικής ταυτότητάς του (eID).

Για να προμηθευτεί ο χρήστης την ηλεκτρονική ταυτότητά του, επικοινωνεί αρχικά με την αρμόδια Αρχή Εγγραφών (Registration Authority) καταθέτοντας μία αίτηση για έκδοση ενός πιστοποιητικού. Αυτή ελέγχει την εγκυρότητα της αίτησης και εφόσον είναι ορθή την προωθεί στην Αρχή Πιστοποιητικών (Certification Authority), η οποία δημιουργεί ένα δημόσιο κλειδί και εκδίδει ένα πιστοποιητικό που το αντιστοιχίζει σε αυτόν. Όταν ο χρήστης δοκιμάζει να χρησιμοποιήσει μία υπηρεσία, χρησιμοποιεί αυτό το πιστοποιητικό. Έτσι, για το σύνολο των υπηρεσιών Ηλεκτρονικής Διακυβέρνησης, ο χρήστης παραλαμβάνει την ηλεκτρονική ταυτότητά του από την ανώτατη όλων αρμόδια Αρχή Πιστοποίησης, έτσι ώστε η ταυτότητα να περιέχει όλα τα απαραίτητα πιστοποιητικά για πρόσβαση στην πληθώρα των προαναφερθέντων υπηρεσιών. Τα στοιχεία που θα περιέχει η ηλεκτρονική ταυτότητά του, πέραν των απαραίτητων κλειδιών για την αυθεντικοποίησή του, είναι, για παράδειγμα: Ονοματεπώνυμο, Αριθμός Δελτίου Ταυτότητας (Α.Δ.Τ.), Αριθμός Φορολογικού Μητρώου (Α.Φ.Μ.), Αριθμός Μητρώου Κοινωνικής Ασφάλισης (Α.Μ.Κ.Α.), Φωτογραφία κατόχου.

3.3 Σενάρια Χρήσης

3.3.1 Κριτήρια επιλογής του τελικού σεναρίου χρήσης

Έχοντας αναλύσει και αιτιολογήσει με τις περιγραφές μας παραπάνω τις επιλογές που κάναμε στις απαιτήσεις του συστήματος και την αρχιτεκτονική που θα ακολουθήσουμε, πρέπει να ορίσουμε και τα σενάρια χρήσης που θα ακολουθήσουμε για να καταλήξουμε τελικά σε συμπεράσματα. Ωστόσο, για να γίνει αυτό είναι απαραίτητο να αναφέρουμε τον τρόπο σκέψης και γενικά τα κριτήρια επιλογής που θα εφαρμόσουμε στον καθορισμό των σεναρίων χρήσης.

Όπως είδαμε, καταλυτικό ρόλο σε οποιαδήποτε προσπάθεια κατασκευής τέτοιου συστήματος Ηλεκτρονικής Ταυτότητας Πολίτη, που θα συμπεριλαμβάνει και σύστημα διαχείρισης ταυτοτήτων, παίζει η ευαισθησία (sensitivity) των δεδομένων που ανταλλάσσονται μεταξύ πολιτών και ηλεκτρονικών υπηρεσιών. Καθώς οι υπηρεσίες θα συγκεντρωθούν σε ένα κοινό σημείο, την Κεντρική Διαδικτυακή Πύλη της Ηλεκτρονικής Διακυβέρνησης του κράτους, πρέπει να δοθεί εξαιρετική προσοχή στο χειρισμό κάποιων δεδομένων των πολιτών που αφορούν συγκεκριμένες υπηρεσίες. Βασικότερες από αυτές είναι οι υπηρεσίες από αφορούν την υγεία και την εφορία. Είναι σαφές και αδιαμφισβήτητο ότι τα δεδομένα υγείας, είναι απολύτως προσωπικά, και

πρέπει να τα διαχειρίζεται ο εκάστοτε φορέας με αυστηρότητα και σοβαρότητα ως προς το που, πως και σε ποιον εμφανίζονται. Τέτοια δεδομένα μπορεί να έχουν άμεσο αντίκτυπο στην εργασία ενός ατόμου (πχ. εγκυμοσύνη για τις γυναίκες) και γενικότερα στη συμπεριφορά του περιγύρου του ως προς αυτόν. Αντίστοιχα, αυστηρώς προσωπικά πρέπει να θεωρούνται και οτιδήποτε δεδομένα σχετίζονται με την οικονομική κατάσταση ενός ατόμου και τα φορολογικά του στοιχεία. Και αυτά είναι ικανά να δημιουργήσουν αρνητικά κοινωνικά φαινόμενα ως προς το άτομο, αλλά και σε πιο πρακτικό επίπεδο όπως πχ στην εργασία του.

Η κρισιμότητα (criticality), λοιπόν, των προσωπικών δεδομένων των ατόμων είναι τεράστια και σίγουρα θα διαμορφώσει σε πολύ μεγάλο βαθμό όποιες αποφάσεις ληφθούν για τα πιθανά σενάρια χρήσης, τόσο σε πραγματικά δεδομένα, όσο και στα πλαίσια της παρούσας εργασίας που στόχος της είναι η μελέτη και η εξαγωγή χρήσιμων συμπερασμάτων για το παρόν και το μέλλον.

Τέλος, και οι ίδιες οι ηλεκτρονικές υπηρεσίες που θα παρέχονται από την Κεντρική Διαδικτυακή Πύλη παίζουν το δικό τους ρόλο για την επιλογή των τελικών σεναρίων χρήσης. Ειδικότερα και σε αντιστοιχία με τα σημερινά δεδομένα, προβλέπεται να συμμετέχουν υπηρεσίες υγείας, εφορίας, ληξιαρχείου, έκδοσης πιστοποιητικών, εκλογικών και στρατολογικών διαδικασιών, γραμματείες πανεπιστημίων και άλλες. Καθώς, αυτές κάνουν χρήση διαφόρων τεχνολογιών παλιών και νέων, η συνολική ενσωμάτωση τους σε ένα σύστημα είναι πολύπλοκη διαδικασία και ασφαλώς πρέπει να ληφθεί και αυτή σοβαρά υπόψιν, κατά την επιλογή και περιγραφή των σεναρίων χρήσης που ακολουθούν.

3.3.2 Σενάριο χρήσης

Άρα, συνυπολογίζοντας όλα τα παραπάνω μπορούμε να καταλήξουμε σε βασικά σενάρια χρήσης της Κεντρικής Διαδικτυακής Πύλης σε συνδυασμό με την Ηλεκτρονική Ταυτότητα του Πολίτη για την ταυτοποίησή του και τη χρήση των ηλεκτρονικών υπηρεσιών. Ωστόσο, επιβάλλεται να αναφέρουμε ότι για την λογική συνέχεια και συνέπεια των σεναρίων, έχουν γίνει κάποιες παραδοχές που αφορούν ενέργειες σχετικές με την εγγραφή του χρήστη στο σύστημα και γενικά με την έκδοση της ηλεκτρονικής του ταυτότητας και την εγκατάσταση των πιστοποιητικών που τη συνοδεύουν στο φυσικό μέσο που θα επιλεχτεί.

3.3.2.1 Γενική περιγραφή πρώτου σεναρίου χρήσης

Ο χρήστης εισέρχεται στο διαδικτυακό ιστότοπο της Κεντρικής Διαδικτυακής Πύλης, στην οποία εμφανίζονται οι διαθέσιμες επιλογές σε υπηρεσίες ηλεκτρονικής διακυβέρνησης. Αφού πλοηγηθεί και βρει ο χρήστης την υπηρεσία που τον αφορά και θέλει να χρησιμοποιήσει, την επιλέγει. Τότε του ζητείται να εισάγει το μοναδικό του username που του έχει δοθεί και του αντιστοιχεί από την έκδοση της Ηλεκτρονικής του Ταυτότητας. Στη συνέχεια, ειδοποιείται με κατάλληλο μήνυμα, πως θα πρέπει να κάνει χρήση του φυσικού μέσου της ηλεκτρονικής του ταυτότητας, ώστε να ταυτοποιηθεί .

Αφού προχωρήσει με αυτό το βήμα, τότε ο ιστότοπος ανανεώνεται και τον ανακατευθύνει στο περιβάλλον της ηλεκτρονικής υπηρεσίας που επέλεξε και ως επίσημα ταυτοποιημένος χρήστης της μπορεί να την χρησιμοποιήσει άμεσα.

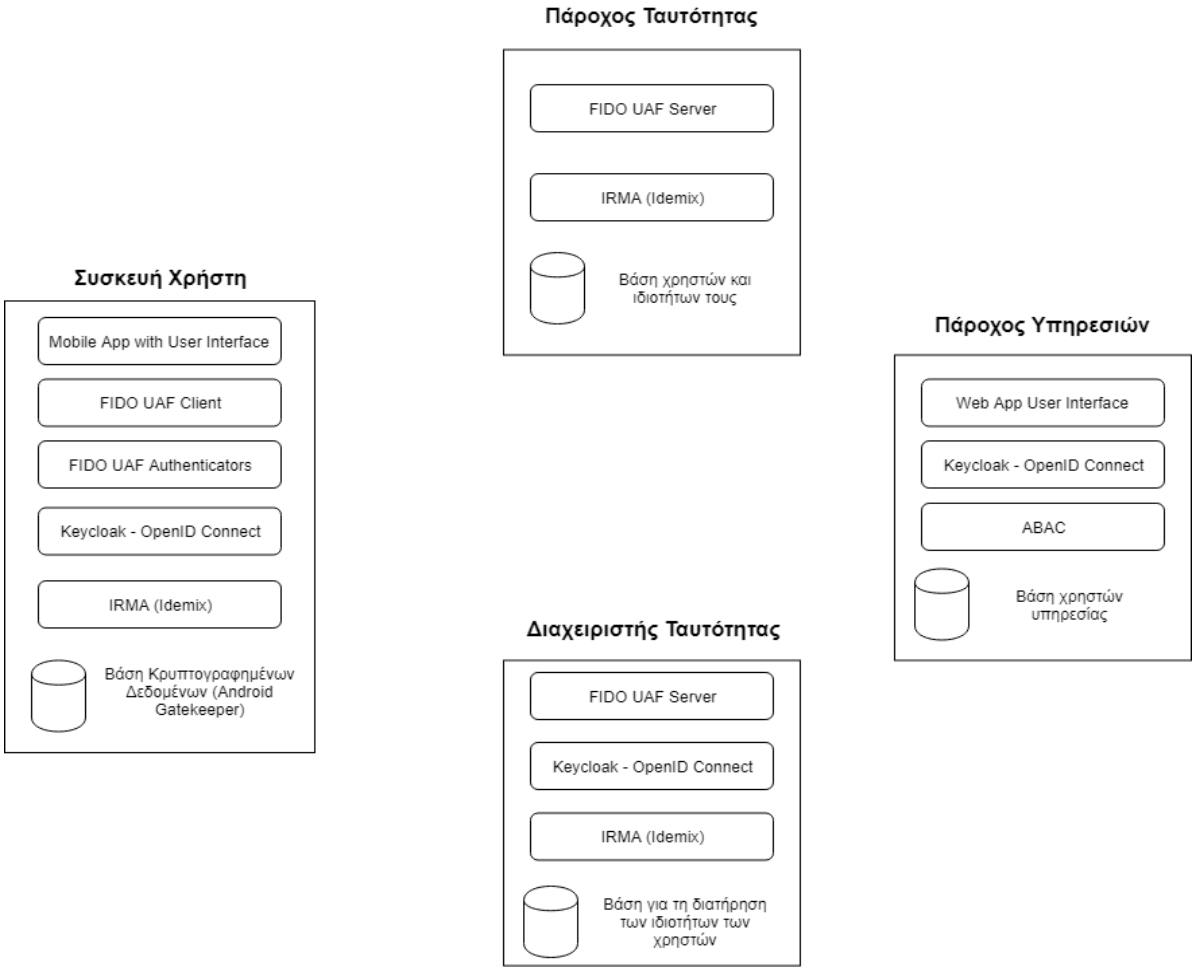
3.3.2.2 Γενική περιγραφή δεύτερου σεναρίου χρήσης

Ομοίως με πριν, ο χρήστης εισέρχεται στο διαδικτυακό ιστότοπο της Κεντρικής Διαδικτυακής Πύλης, πλοηγείται στις υπηρεσίες ηλεκτρονικής διακυβέρνησης που παρέχονται και επιλέγει την υπηρεσία που επιθυμεί. Τότε εμφανίζεται στον χρήστη κατάλληλη υπόδειξη για να χρησιμοποιήσει το κινητό του και να σκανάρει το QR code που έχει εμφανιστεί στην οθόνη. Σε αυτό το QR code έχει κωδικοποιηθεί μία σειρά ερωτήσεων των χαρακτηριστικών του χρήστη που απαιτεί η υπηρεσία να της αποκαλυφθούν, ώστε να επιτρέψει στο χρήστη να τη χρησιμοποιήσει και να φορτώσει το προφίλ του. Αφού το σκανάρει, τότε στο κινητό του εμφανίζονται τα ερωτήματα προς το χρήστη και ρωτάται αν αποδέχεται την αποκάλυψή τους. Αν τη δεχτεί, επιστρέφει στον ιστότοπο της Κεντρικής Διαδικτυακής Πύλης και πατώντας το κουμπί επαλήθευσης ταυτότητας, εισάγεται στην υπηρεσία που επέλεξε. Έτσι, όντας επισήμως ταυτοποιημένος χρήστης της υπηρεσίας με τα συγκεκριμένα χαρακτηριστικά και μπορεί πλέον να τη χρησιμοποιήσει άμεσα.

Κεφάλαιο 4

Σχεδίαση Συστήματος

Το παρόν κεφάλαιο πραγματεύεται και παρουσιάζει την σχεδίαση του συστήματος. Προηγήθηκε η ανάλυση των απαιτήσεων που θα πρέπει να πληροί, καθώς και η επιλογή του φυσικού μέσου που θα διαδραματίσει το ρόλο της Ηλεκτρονικής Ταυτότητας Πολίτη, ενώ περιγράφηκαν και τα βασικά σενάρια χρήσης. Με βάση τα παραπάνω, στο σχήμα που δίνεται παρακάτω φαίνεται η σχεδίαση του συστήματος σε μορφή οντοτήτων που θα το αποτελούν. Όπως είναι διακριτό, πολλές υπο-οντότητες αναφέρονται σε παραπάνω οντότητες από μία, γεγονός που φανερώνει τη στενή σύνδεση μεταξύ τους και το ότι θα πρέπει να διαλειτουργούν και να επικοινωνούν άμεσα. Πιο συγκεκριμένα, διακρίνουμε τις εξής οντότητες: Συσκευή Χρήστη (ΣΧ), Πάροχος Ταυτότητας (ΠΤ), Διαχειριστής Ταυτότητας (ΔΤ) και Πάροχος Υπηρεσιών (ΠΥ) που αναλύονται στη συνέχεια του κεφαλαίου.



Εικόνα 2. Οντότητες του Συστήματος

4.1 Ηλεκτρονική Ταυτότητα Πολίτη

4.1.1 Φυσικό μέσο και περιεχόμενα αυτού

Λαμβάνοντας υπόψιν όλες τις σύγχρονες και διαθέσιμες επιλογές, που παρουσιάστηκαν στο κεφάλαιο 3 της παρούσας μελέτης, σχετικά με το φυσικό μέσο που μπορεί να διαδραματίσει το ρόλο της Ηλεκτρονικής Ταυτότητας Πολίτη (eID) επιλέχθηκε αυτό της εφαρμογής σε κινητό τηλέφωνο. Στην επιλογή αυτή συνυπολογίστηκαν όλα τα πλεονεκτήματα και τα πιθανά μειονεκτήματα αυτού του μέσου, σε άμεση σύγκριση με τα υπόλοιπα.

Μελετώντας τα θετικά και τα αρνητικά αυτής της επιλογής βλέπουμε σαφώς τα σημεία στα οποία υπερτερεί, αλλά και ότι τα αρνητικά που παρουσιάζονται εύκολα ξεπερνιούνται. Πιο συγκεκριμένα, λόγω της ραγδαίας εξάπλωσης της τεχνολογίας στον τομέα των «έξυπνων» κινητών τηλεφώνων μία τέτοια λύση είναι διαδεδομένη στους πολίτες και εντελώς φορητή και εύχρηστη, καθώς το κινητό είναι πλέον αναπόσπαστο μέρος της καθημερινότητας των περισσότερων πολιτών. Ανάλογα με το είδος και τις τεχνολογίες των αισθητήρων που φέρει, μπορεί να γίνει ταυτοποίηση και αυθεντικοποίηση των χρηστών με δαχτυλικό αποτύπωμα ή αναγνώριση προσώπου/φωνής, πέραν των βασικών username/password και PIN. Ακόμη, σημαντικό είναι το γεγονός ότι σε περίπτωση απώλειας, χωρίς τα credentials αλλά και το βιομετρικό που έχει χρησιμοποιήσει ο χρήστης, δε μπορεί να γίνει πλαστοπροσωπία και να ταυτοποιηθεί κάποιος χωρίς να είναι ο ίδιος ο κάτοχος της ταυτότητας αυτής. Επιπλέον δικλείδα ασφάλειας σε περίπτωση απώλειας, είναι ότι μπορούν απομακρυσμένα να διαγραφούν τα δεδομένα, αλλά και να κλειδώσει το κινητό, αποτρέποντας οποιαδήποτε διαρροή προσωπικών δεδομένων του χρήστη.

Σαφώς, υπάρχουν και κάποια μειονεκτήματα για τα οποία θα παρουσιάσουμε κάποιες λύσεις ώστε να μην επηρεάζουν τόσο την εγκυρότητα και ευχρηστία της ηλεκτρονικής ταυτότητας με τη μορφή εφαρμογής σε κινητό. Η εξάρτηση από τη μπαταρία είναι άμεση απειλή για τη χρήση του κινητού, ωστόσο η διάρκεια μπαταρίας των σύγχρονων κινητών τηλεφώνων αλλά και η ύπαρξη φορητών μπαταριών (powerbanks) ελαττώνουν δραματικά τις περιπτώσεις όπου κάποιος πολίτης μπορεί να ξεμείνει χωρίς κινητό, και άρα χωρίς ταυτότητα. Αντίστοιχη απειλή μπορεί να είναι η παροχή Ίντερνετ, που θα πρέπει να είναι αδιάλειπτη για να πετύχουν σωστά οι κρυπτογραφημένες ανταλλαγές μηνυμάτων μεταξύ των εξυπηρετητών (Servers) για να πετύχει άρα η χρήση ταυτότητας. Αυτή η ανάγκη καλύπτεται από τα δεδομένα κινητής τηλεφωνίας σχεδόν σε όλους τους εξωτερικούς χώρους, ενώ στο εσωτερικό των κτηρίων, όπου σπανίζει και πάλι η απουσία σήματος, υπάρχει συνήθως τοπικό, ασύρματο δίκτυο (WiFi). Το γεγονός, ακόμη, ότι απαιτείται smartphone και όχι απλό κινητό, πρέπει να λαμβάνεται υπόψιν από τους χρήστες, αν και γενικότερα η πλειονότητα των χρηστών έχει, γι’ αυτό και η περίοδος προσαρμογής στη χρήση smartphones είναι μετριασμένη.

Στη συνέχεια θα πρέπει να εξετάσουμε τα περιεχόμενα που θα περιέχει η εφαρμογή αυτή ως το φυσικό μέσο της Ηλεκτρονικής Ταυτότητας Πολίτη. Τα στοιχεία

αυτά, πέραν των απαραίτητων κλειδιών για την αυθεντικοποίησή των χρηστών, είναι, για παράδειγμα: Ονοματεπώνυμο, Αριθμός Δελτίου Ταυτότητας (Α.Δ.Τ.), Αριθμός Φορολογικού Μητρώου (Α.Φ.Μ.), Αριθμός Μητρώου Κοινωνικής Ασφάλισης (Α.Μ.Κ.Α.), Φωτογραφία κατόχου. Ακόμη, θα πρέπει να συμπεριληφθούν και κάποια στοιχεία επικοινωνίας όπως τηλέφωνα, διεύθυνση και email. Κατά το πέρασμα του χρόνου, καθώς οι πολίτες ανήκουν σε διαφορετικές κατηγορίες και αλληλεπιδρούν με διαφορετικές υπηρεσίες, θα προστίθενται και άλλα ταυτοποιητικά στοιχεία του κάθε πολίτη. Έτσι, ο κάθε πολίτης θα αρκεί να χρησιμοποιήσει τα βασικά του credentials και να ταυτοποιηθεί με αυτά συν το βιομετρικό χαρακτηριστικό που θα έχει εισάγει (δαχτυλικό αποτύπωμα), ώστε ανάλογα την υπηρεσία που θα θέλει να χρησιμοποιήσει, να «ξεκλειδωθεί» προς αυτήν μόνο το κατάλληλο χαρακτηριστικό/αναγνωριστικό (attribute) του χρήστη.

Έχοντας καταλήξει, λοιπόν, πως θα αναπτυχθεί εφαρμογή (app) που θα διαδραματίσει το ρόλο της ταυτότητας του πολίτη, χρήσιμο θα ήταν να δώσουμε κάποια τεχνικά χαρακτηριστικά της συσκευής που χρησιμοποιήσουμε για τις ανάγκες των δοκιμών μας (demos). Όπως θα δούμε, η συσκευή είναι αρκετά ισχυρή και υποστηρίζει το βιομετρικό χαρακτηριστικό που θέλουμε να χρησιμοποιήσουμε, δηλαδή το δακτυλικό αποτύπωμα.

Η συσκευή που θα χρησιμοποιηθεί θα είναι μία συσκευή Samsung Galaxy S6 (2015) με κωδικό μοντέλου G920F. Στον πίνακα που ακολουθεί δίνουμε βασικά χαρακτηριστικά της συσκευής, σε επίπεδο υλικών (hardware) και λογισμικού (software).

Πίνακας 2. Samsung Galaxy S6 specifications [21]

Chipset	Exynos 7420 Octa
CPU	Octa-core (4x2.1 GHz Cortex-A57 & 4x1.5 GHz Cortex-A53)
GPU	Mali-T760MP8
RAM	3 GB
ROM	32 GB
Screen	Super AMOLED capacitive touchscreen, 16M colors, 5.1 inches, 1440 x 2560 pixels, 16:9 ratio (~577 ppi density)
Camera	Main: 16 MP, f/1.9, 28mm (wide) Front: 5 MP, f/1.9, 22mm (wide)
Sensors	Fingerprint (front-mounted), accelerometer, gyro, proximity, compass, barometer, heart rate, SpO2
OS	Android Nougat 7.0

Στη συνέχεια θα εμβαθύνουμε περισσότερο στις υπο-οντότητες οι οποίες όταν συντεθούν κάτω από μία ενιαία εφαρμογή θα αποτελέσουν την Ηλεκτρονική Ταυτότητα Πολίτη και θα αναφέρουμε παραπάνω τεχνικά χαρακτηριστικά και λεπτομέρειες.

Εφαρμογή χρήστη (Mobile App): Αυτή η εφαρμογή είναι η βάση πάνω στην οποία θα χτιστεί η Ηλεκτρονική Ταυτότητα υπό τη μορφή εφαρμογής. Αυτή θα

αποτελέσει το σημείο αναφοράς και τον «ενορχηστρωτή» όλων των άλλων οντοτήτων που θα χρησιμοποιηθούν, καθώς η κάθε μία είναι επιφορτισμένη με μία συγκεκριμένη λειτουργία. Έτσι, είναι απαραίτητη η ένωση και η επικοινωνία τους (integration), ώστε όλες μαζί να βοηθούν στην ταυτοποίηση του χρήστη και στην αποκάλυψη μόνον των ζητούμενων χαρακτηριστικών του (attribute-based eID) όταν θα προσπαθεί να συνδεθεί στην Κεντρική Διαδικτυακή Πύλη. Πιο συγκεκριμένα, η εφαρμογή αυτή θα διαθέτει μία οθόνη που θα προτρέπει το χρήστη να τοποθετήσει το δάχτυλό του στον σχετικό αισθητήρα ανάγνωσης αποτυπωμάτων, προκειμένου να γίνει η ταυτοποίησή του και να ξεκλειδωθούν τα κρυπτογραφημένα κλειδιά του FIDO πρωτοκόλλου, που θα εφαρμόσουμε και θα αναλυθεί και παρακάτω. Τα κλειδιά αυτά θα είναι αποθηκευμένα στο Ασφαλές Αποθετήριο Κρυπτογραφημένων Δεδομένων, που παρέχεται από το λογισμικό Android, στο Android Hardware Credential Storage με χρήση του Android Gatekeeper. Ακόμη, για το δαχτυλικό αποτύπωμα θα γίνει χρήση των κατάλληλων Application Program Interfaces (APIs) που παρέχει το Android για την επικοινωνία με το υλικό του αναγνώστη αποτυπωμάτων (δηλαδή με τον driver του), καθώς και του Fingerprint HAL που θα διασφαλίσει την προστασία του αποτυπώματος. Να σημειωθεί στο σημείο αυτό πως τα πρωτόκολλα-frameworks και λογισμικά που αναφέρουμε πως θα χρησιμοποιηθούν (FIDO, Android Gatekeeper, Fingerprint HAL) θα αναλυθούν στη συνέχεια του κεφαλαίου.

- **FIDO UAF Client**: Στην εφαρμογή που περιγράψαμε παραπάνω, μία από τις διαδικασίες που θα τρέχουν παρασκηνιακά, όταν θα γίνονται οι αιτήσεις ταυτοποίησης ενός χρήστη είναι και η ανταλλαγή μηνυμάτων του πρωτοκόλλου FIDO. Για τη διαδικασία αυτή επιφορτισμένος είναι ο FIDO client που θα ενσωματώσουμε στην εφαρμογή μας, ώστε να επικοινωνεί με τον FIDO UAF Server, που θα ανήκει στην οντότητα του Διαχειριστή Ταυτότητας που θα αναλυθεί στην συνέχεια του παρόντος κεφαλαίου, μέσω αυστηρά ορισμένων μηνυμάτων από το πρωτόκολλο FIDO.
- **FIDO UAF Authenticator**: Αυτή είναι μία ακόμα οντότητα που σχετίζεται με το πρωτόκολλο FIDO και με την οποία επικοινωνεί ο FIDO UAF Client. Με αυτόν, ανταλλάσσει επίσης κρυπτογραφημένα μηνύματα και για την συγκεκριμένη επικοινωνία γίνεται χρήση του FIDO ASM API (FIDO Authenticator-Specific Module API). Ο authenticator που αναφέρουμε είναι υπεύθυνος για την ασφαλή αποθήκευση στο προαναφερθέν «Ασφαλές Αποθετήριο Κρυπτογραφημένων Δεδομένων» αλλά και για τη χρήση των ιδιωτικών κλειδιών που απαιτούνται κατά τη διαδικασία αυθεντικοποίησης.
- **Irma**: Η υπο-οντότητα αυτή που θα συμπεριληφθεί στην εφαρμογή της Ηλεκτρονικής Ταυτότητας είναι υπεύθυνη για τη διαχείριση των διαπιστευτηρίων που είναι αποθηκευμένα στο ασφαλές αποθετήριο της κινητής συσκευής. Σύμφωνα με αυτό, ανάλογα την υπηρεσία στην οποία θέλει να συνδεθεί ο χρήστης/πολίτης αποκαλύπτονται μόνο τα ζητούμενα από αυτή χαρακτηριστικά στοιχεία του και δε δίνεται όλη την πληροφορία που φέρει η Ηλεκτρονική Ταυτότητα, διαφυλάσσοντας έτσι την ιδιωτικότητά του. Όπως

έχουμε ήδη τονίσει, τα διαπιστευτήρια του χρήστη βασίζονται σε χαρακτηριστικά του ίδιου (attribute-based) και αποθηκεύονται μόνο στο αποθετήριο της συσκευής και όχι κάπου αλλού, ώστε να υπάρχουν άλλοι κίνδυνοι διαρροών προσωπικών στοιχείων.

- **Mobile Federated Login**: Αρχικό βήμα για όλα τα παραπάνω είναι η διαδικασία εισόδου (login) που θα εμφανίζεται κατά την εκκίνηση της εφαρμογής. Στο πρωτόκολλο του OpenID Connect θα βασιστεί η εφαρμογή μας, ώστε να μπορέσει να διαλειτουργήσει επιτυχώς με τους servers που απαιτούνται για τις διαδικασίες ταυτοποίησης και αυθεντικοποίησης που έχουμε αναφέρει. Θα πρέπει δηλαδή να επικοινωνήσει με τον βασικό Πάροχο Ταυτότητας (Identity Provider) που είναι το Keycloak, στο οποίο ενσωματώνεται και ο πάροχος OpenId Connect και OAuth 2.0. Αυτά θα συναποτελέσουν τον Android Client που θα διαχειρίζεται αιτήσεις και απαντήσεις (requests και responses) για τα πρωτόκολλα που αναφέραμε, ακολουθώντας αυστηρά τις προδιαγραφές που έχουν τεθεί.

4.1.2 Κρυπτογραφικοί Μηχανισμοί

Καθώς όπως αναφέραμε ο βασικός όγκος των πληροφοριών του χρήστη εμπεριέχεται στην Ηλεκτρονική του Ταυτότητα, δηλαδή στην κινητή του συσκευή, πρέπει να εξετάσουμε τις δυνατότητες κρυπτογραφικών μηχανισμών που παρέχονται από το λογισμικό Android, που είναι αυτό το οποίο τρέχει στην κινητή αυτή συσκευή.

Το Android χρησιμοποιεί την έννοια των κρυπτογραφικών κλειδιών που βασίζονται σε έλεγχο ταυτότητας χρήστη και απαιτεί τα ακόλουθα στοιχεία:

- **Κρυπτογραφική αποθήκευση κλειδιών και πάροχος υπηρεσιών (Cryptographic key storage and service provider)**: Αποθηκεύει κρυπτογραφικά κλειδιά και παρέχει τυπικές ρουτίνες κρυπτογράφησης πάνω από αυτά τα πλήκτρα. Το Android υποστηρίζει ένα Keystore και το Keymaster που υποστηρίζονται από υλικό για υπηρεσίες κρυπτογράφησης, συμπεριλαμβανομένης κρυπτογραφίας που υποστηρίζεται από το υλικό για αποθήκευση των κλειδιών που μπορεί να περιλαμβάνει ένα Trusted Execution Environment (TEE) ή Secure Element (SE), όπως το Strongbox [22].
- **Πιστοποιητικά χρήστη (User authenticators)**: Με τη βοήθεια αυτών, γίνεται επιβεβαίωση για την παρουσία του χρήστη και / ή για επιτυχή έλεγχο ταυτότητας. Το Android υποστηρίζει το Gatekeeper για έλεγχο ταυτότητας με κωδικό PIN / μοτίβο / κωδικό πρόσβασης και δακτυλικό αποτύπωμα για έλεγχο ταυτότητας δακτυλικού αποτυπώματος. Οι συσκευές που κυκλοφορούν με Android 9 και νεότερες εκδόσεις μπορούν να χρησιμοποιήσουν το BiometricPrompt ως ενιαίο σημείο ολοκλήρωσης για τα δακτυλικά αποτυπώματα και τα πρόσθετα βιομετρικά στοιχεία. Αυτά τα στοιχεία κοινοποιούν την κατάσταση επαλήθευσης ταυτότητας με την υπηρεσία αποθήκευσης κλειδιών μέσω ενός πιστοποιημένου καναλιού [22].

Στο σημείο αυτό ας δούμε αναλυτικότερα το Android Gatekeeper αλλά και το Fingerprint HAL που όπως αναφέραμε παραπάνω κατέχουν πολύ σημαντική θέση στην υλοποίησή μας.

- **Android Gatekeeper**: Το υποσύστημα Gatekeeper εκτελεί έλεγχο ταυτότητας συσκευών / κωδικού πρόσβασης σε ένα περιβάλλον αξιόπιστης εκτέλεσης (Trusted Execution Environment - TEE). Ο Gatekeeper κάνει εγγραφή και επαλήθευση στους κωδικούς πρόσβασης μέσω ενός HMAC (Hash-based Message Authentication Code) με μυστικό κλειδί που υποστηρίζεται από υλικό. Επιπλέον, ο Gatekeeper ρυθμίζει τις συνεχείς αποτυχημένες προσπάθειες επαλήθευσης και πρέπει να αρνηθεί την εξυπηρέτηση αιτήσεων με βάση ένα συγκεκριμένο χρονικό όριο και έναν δεδομένο αριθμό διαδοχικών αποτυχημένων προσπαθειών. Όταν οι χρήστες επαληθεύουν τους κωδικούς πρόσβασής τους, ο Gatekeeper χρησιμοποιεί το διαμοιραζόμενο κλειδί από το TEE για να υπογράψει μια βεβαίωση ελέγχου ταυτότητας για να στείλει στο Keystore. Δηλαδή, μια βεβαίωση από το Gatekeeper ενημερώνει το Keystore ότι μπορούν να απελευθερωθούν για χρήση από εφαρμογές τα κλειδιά που έχουν δεσμευτεί για έλεγχο ταυτότητας (για παράδειγμα, τα κλειδιά που έχουν δημιουργήσει οι εφαρμογές) [23].
- **Fingerprint HAL**: Σε συσκευές με αισθητήρα δακτυλικών αποτυπωμάτων, οι χρήστες μπορούν να εγγράψουν ένα ή περισσότερα δακτυλικά αποτυπώματα και να χρησιμοποιήσουν αυτά τα δακτυλικά αποτυπώματα για να ξεκλειδώσουν τη συσκευή και να εκτελέσουν άλλες εργασίες. Το Android χρησιμοποιεί το Fingerprint Hardware Abstraction Layer (HAL) για να συνδεθεί αφενός με μια συγκεκριμένη βιβλιοθήκη του προμηθευτή και αφετέρου με το ίδιο το υλικό του αναγνώστη δακτυλικών αποτυπωμάτων.

Παρακάτω αποσαφηνίζουμε περισσότερο τη διαδικασία ταιριάσματος δακτυλικού αποτυπώματος του χρήστη, που είναι καθοριστική για την ταυτοποίησή του, στο επίπεδο του λειτουργικού Android.

Ο αισθητήρας δακτυλικών αποτυπωμάτων μιας συσκευής είναι γενικά αδρανής. Ωστόσο, απαντώντας σε μια κλήση προς τη λειτουργία ελέγχου ταυτότητας ή εγγραφής, ο αισθητήρας δακτυλικών αποτυπωμάτων «ακούει» για μια αφή (η οθόνη μπορεί επίσης να ξυπνήσει όταν ένας χρήστης αγγίξει τον αισθητήρα δακτυλικών αποτυπωμάτων). Η ροή διαδικασιών υψηλού επιπέδου (high level flow procedure) της αντιστοίχισης δακτυλικών αποτυπωμάτων περιλαμβάνει τα ακόλουθα βήματα:

1. Ο χρήστης τοποθετεί ένα δάχτυλο στον αισθητήρα δακτυλικών αποτυπωμάτων.
2. Η συγκεκριμένη βιβλιοθήκη προμηθευτή καθορίζει εάν υπάρχει αντιστοιχία δακτυλικών αποτυπωμάτων στο τρέχον σύνολο των πρότυπων δακτυλικών αποτυπωμάτων που έχουν εγγραφεί.
3. Τα αποτελέσματα μίας επιτυχημένης αντιστοίχισης μεταβιβάζονται στο Fingerprint HAL επίπεδο, το οποίο ειδοποιεί τον fingerprintd (the fingerprint

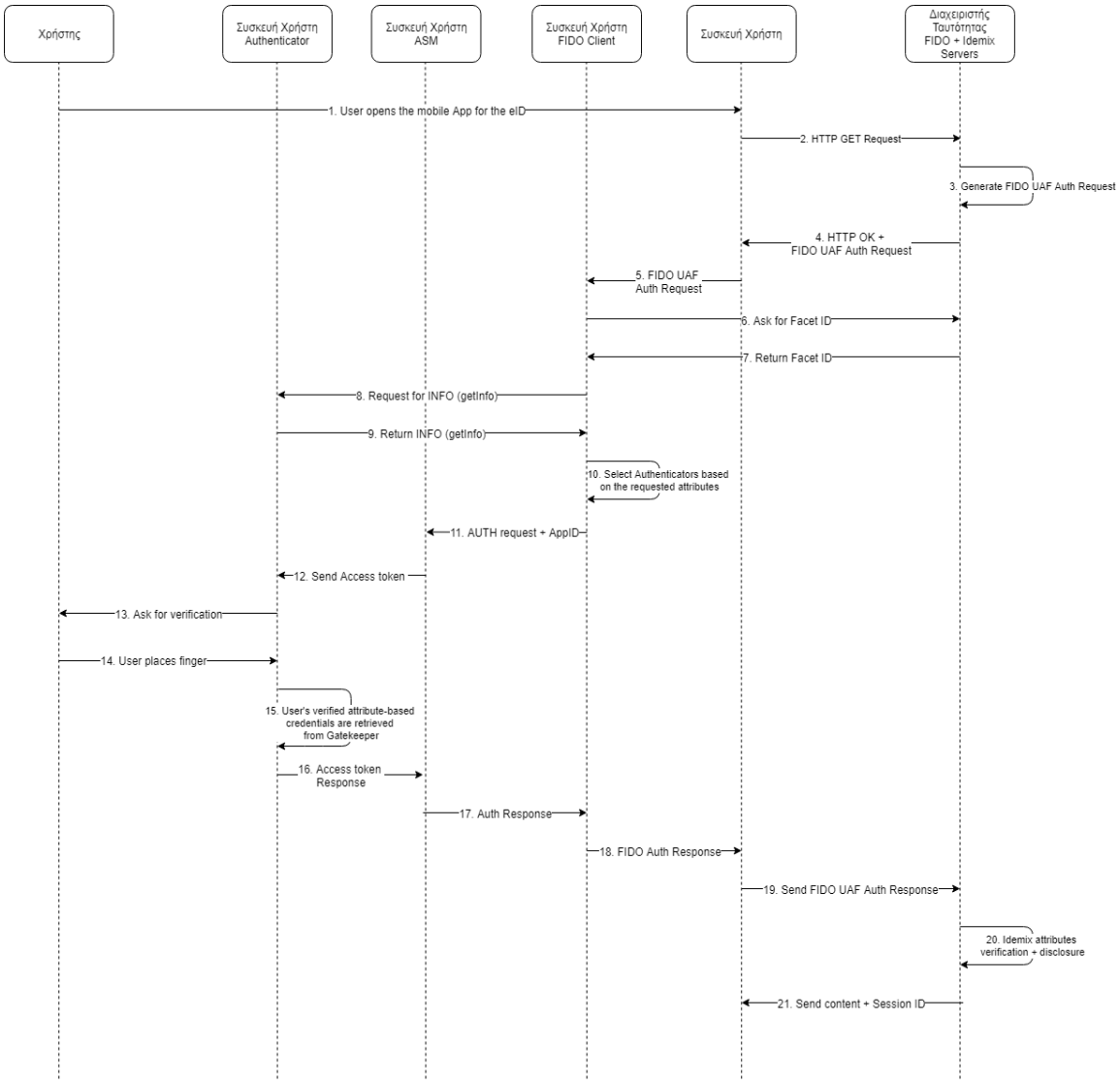
deamon – ο δαίμονας δακτυλικών αποτυπωμάτων) για την πετυχημένη ή μη αυθεντικοποίηση ταυτότητας με δακτυλικό αποτύπωμα.

Αυτή η ροή προϋποθέτει ότι ένα δακτυλικό αποτύπωμα έχει ήδη εγγραφεί στη συσκευή, δηλαδή η συγκεκριμένη βιβλιοθήκη προμηθευτή έχει εγγράψει ένα πρότυπο για το δακτυλικό αποτύπωμα [24].

4.1.3 Περιγραφή Κλάσεων και Αλληλεπιδράσεων - Λειτουργίες και Υποστηριζόμενες Υπηρεσίες eID

Μεταξύ των οντοτήτων και των κλάσεων που έχουν αναφερθεί, προφανώς, υπάρχει συνεχής και προστατευμένη αλληλεπίδραση ώστε να λειτουργεί σωστά και με ασφάλεια η Ηλεκτρονική Ταυτότητα Πολίτη. Άρα, οι διεργασίες που συμβάλλουν στην ανταλλαγή μηνυμάτων μεταξύ αυτών έχει μία συγκεκριμένη ακολουθία.

Αρχικά, ο χρήστης, όταν του ζητηθεί να ταυτοποιηθεί (από την ΚΔΠ), ανοίγει την εφαρμογή eID στο κινητό του. Η συσκευή του χρήστη στέλνει ένα HTTP GET Request προς τον FIDO Server της οντότητας «Διαχειριστής Ταυτότητας». Σε εκείνη επιστρέφεται ένα HTTP OK, καθώς και το FIDO UAF AUTH Request από τη μεριά του server προς τον χρήστη, ζητώντας τα attributes του χρήστη που πρέπει να ταυτοποιηθούν για τη χρήση της συγκεκριμένης υπηρεσίας (που ζητήθηκε σε προηγούμενο στάδιο στην ΚΔΠ). Αυτό το AUTH Request φτάνει στην συσκευή χρήστη, δηλαδή στην εφαρμογή του eID και στη συνέχεια αυτό το χειρίζεται η υπο-οντότητα FIDO Client που αναφέραμε ότι είναι μέρος της Ηλεκτρονικής Ταυτότητας. Αφού αναλυθεί, κατασκευάζεται και στέλνεται το Request προς τον FIDO Authenticator (επίσης μέρος της εφαρμογής στο κινητό), ο οποίος με τη σειρά του απαντάει τους διαθέσιμους authenticators ανάλογα με την πολιτική/επίπεδο ασφάλειας που έχει τεθεί, στην προκειμένη περίπτωση το δαχτυλικό αποτύπωμα. Ζητείται από το χρήστη, έπειτα, να ταυτοποιηθεί, ο οποίος με τη σειρά του τοποθετεί στον αναγνώστη αποτυπωμάτων το δάχτυλο του και επιβεβαιώνει την ταυτότητά του. Έτσι, ξεκλειδώνεται το σύνολο από τα ζητούμενα attributes με τη βοήθεια του Gatekeeper. Αυτό κωδικοποιείται και δημιουργείται έτσι το Access Token του χρήστη, το οποίο ενσωματώνεται στο AUTH Response που προωθείται στον FIDO Client, και αυτός με τη σειρά του δημιουργεί και αποστέλλει το FIDO UAF AUTH Response, με «υπογεγραμμένα» από το χρήστη τα δεδομένα για τα οποία ζητήθηκε η ταυτοποίηση, προς την εφαρμογή στη συσκευή χρήστη. Το συγκεκριμένο Response αντικείμενο προωθείται στον FIDO Server που εμπεριέχεται στον Διαχειριστή Ταυτότητας. Εκεί, με χρήση του Irma Server που αποτελεί επίσης υπο-οντότητα του Διαχειριστή Ταυτότητας, γίνεται η πιστοποίηση των χαρακτηριστικών (attribute-based) που ζητήθηκαν. Πλέον, έχοντας αυτά πιστοποιηθεί, προωθούνται στην οντότητα που τα ζήτησε, δηλαδή στην Κεντρική Διαδικτυακή Πύλη, και ο χρήστης εισάγεται στην υπηρεσία που ζήτησε.



Εικόνα 3. Διαδικασία ταυτοποίησης χρήστη με FIDO UAF-Idemix

4.2 Κεντρική Διαδικτυακή Πύλη (ΚΔΠ)

4.2.1 Το Γραφικό Περιβάλλον της ΚΔΠ και οι λειτουργίες της

Η Κεντρική Διαδικτυακή Πύλη (ΚΔΠ) αποτελεί ένα από τα σημαντικότερα κομμάτια του συστήματός μας, καθώς αποτελεί την πρώτη διεπαφή του χρήστη με το σύστημα. Αφενός θα πρέπει να είναι όμορφη από αισθητικής άποψης, αφετέρου θα πρέπει να επιτελεί τους σκοπούς της άμεσα, γρήγορα, σωστά και με σαφήνεια. Είναι πολύ σημαντικό ακόμα να δίνονται στους χρήστες οι απαραίτητες πληροφορίες εγγραφής, εισόδου και όποιας άλλης λειτουργίας θα μπορεί να κάνει δια μέσου της πύλης.

Οι δύο βασικοί πυλώνες της, δηλαδή το να είναι αισθητικά ωραία αλλά συνάμα και λειτουργική, δε πρέπει να συγχέονται, παρότι στο Γραφικό Περιβάλλον Χρήστη (Graphical User Interface - GUI) μία λειτουργία αναπαρίσταται από ένα απλό κουμπί ή ένα σύμβολο που πατώντας το εκτελείται η επιθυμητή ενέργεια. Παρακάτω ακολουθεί

η περιγραφή της Κεντρικής Διαδικτυακής Πύλης και κατ' επέκταση της αρχικής σελίδας του συστήματος.

Μόλις ο χρήστης συνδεθεί στην πύλη, αυτή είναι η πρώτη οθόνη που του παρουσιάζεται. Στα αριστερά, υπάρχει ένα κεντρικό μενού κάτω από τον τίτλο «Κρατικές Υπηρεσίες». Αυτό αναλύεται σε 3 σελίδες:

- **Αρχική**: Όπου αντιστοιχεί στην εικόνα παραπάνω όπου εμφανίζονται τα γενικά μενού καθώς και οι διαθέσιμες κρατικές υπηρεσίες που παρέχονται ηλεκτρονικά στους πολίτες. Αυτές συγκεντρώνονται κάτω από την «ομπρέλα» της ΚΔΠ, δίνοντας ένα συνολικό σημείο διεπαφής με τους χρήστες.
- **Πληροφορίες**: Εδώ, παρέχεται στους χρήστες πληροφόρηση σχετική με χρήση της Κεντρικής Διαδικτυακής Πύλης και τις λειτουργίες της.
- **Επικοινωνία**: Στην καρτέλα αυτή παρέχονται πληροφορίες για το φυσικό σημείο ύπαρξης της υπηρεσίας, όπου παρέχει την απαραίτητη υποστήριξη στους πολίτες σε ζητήματα και προβλήματα που ανακύπτουν, καθώς και για την πρώτη εγγραφή τους όπου απαιτείται η φυσική τους παρουσία μαζί με τα απαραίτητα δικαιολογητικά.

Πιο κεντρικά και κάτω από τον τίτλο «Κεντρική Διαδικτυακή Πύλη» βλέπουμε μία λίστα από κατηγορίες όπως «Όλες», «Υγεία», «Εκπαίδευση», «Οικονομία» και άλλες. Αυτή, μας βοηθάει να ομαδοποιήσουμε τις κρατικές υπηρεσίες ανάλογα με τις ανάγκες μας και άρα να βρούμε πιο γρήγορα αυτή που αναζητούμε.

Τέλος, κάτω από τις καρτέλες που προσφέρουν ομαδοποίηση, εμφανίζονται σε μορφή πλακιδίων οι υπηρεσίες που παρέχονται ηλεκτρονικά. Σε κάθε ένα πλακίδιο, υπάρχει για λόγους ευκολίας αναγνώρισης της κάθε υπηρεσίας το σήμα/σύμβολό της, το οποίο κατά το πάτημά του ανακατευθύνει τους πολίτες στην ζητούμενη υπηρεσία, αν ο πολίτης έχει περάσει από το στάδιο της ταυτοποίησης. Για να συνδεθεί ο χρήστης, πατώντας στην υπηρεσία που τον ενδιαφέρει, πρώτα θα ανακατευθυνθεί στη σελίδα σύνδεσης, όπου θα καταχωρήσει τους προσωπικούς του κωδικούς και μετά θα του ζητηθεί να επιβεβαιώσει την ταυτότητά του με χρήση της ηλεκτρονικής του ταυτότητας (Ταυτοποίηση 2 παραγόντων – 2 factor Authentication). Κατά την ανταλλαγή των κωδικών, εφαρμόζεται Single Sign-On (SSO) πολιτική μέσα από τη χρήση του πλαισίου Keycloak, που ενισχύει την ασφάλεια εισόδου των χρηστών. Στο σημείο αυτό, θα γίνει η αποκάλυψη μόνον των χαρακτηριστικών που απαιτούνται για την είσοδό του στην συγκεκριμένη υπηρεσία, πετυχαίνοντας έτσι και την attribute-based φύση του συστήματος, όπως υποδεικνύεται από την ανάγκη για προστασία της ιδιωτικότητας των πολιτών.

4.2.2 Περιγραφή Κλάσεων και Αλληλεπιδράσεων

Η παραπάνω περιγραφή της Κεντρικής Διαδικτυακής Πύλης σε ό,τι αφορά το γραφικό της περιβάλλον και τις λειτουργίες που επιτελεί, παρέχεται μέσα από μία εφαρμογή Web. Δηλαδή η ΚΔΠ είναι μία online εφαρμογή, που γίνεται hosted τοπικά

σε έναν server (Tomcat) και σε αυτή ο χρήστης αιτείται πρόσβαση σε οποιαδήποτε κρατική υπηρεσία eGovernment θέλει.

Απαραίτητο συστατικό της ΚΔΠ είναι η εφαρμογή του Federated login, που θα υλοποιηθεί μέσω του πρωτοκόλλου OpenID Connect που ήδη αναφέραμε. Το πλαίσιο (framework) Keycloak παρέχει και αυτήν την δυνατότητα, άρα θα μπορεί η σελίδα της πύλης να επικοινωνεί με το Keycloak για να διασφαλίσει το Single Sign-On στο login page της. Όταν γίνουν όλες οι σωστές ρυθμίσεις (configuration) σχετικά με τις IP διευθύνσεις και τις πόρτες που θα «ακούει» κάθε server, θα μπορεί η πύλη να επικοινωνεί με τον Keycloak server (wildfly). Έτσι, θα μπορεί να λαμβάνει έγκυρα διαπιστευτήρια από τον Διαχειριστή Ταυτότητας μετά από κατάλληλο έλεγχο που αυτός θα κάνει και άρα θα μπορεί να θεωρηθεί αξιόπιστη οντότητα στα πλαίσια της αλυσίδας "Federated login" του Keycloak. Σε πιο τεχνικό επίπεδο, παρέχονται Java Adapters για OpenID Connect και Client Authentication, άρα και σε ό, τι αφορά τον κώδικα μπορεί να γίνει η επικοινωνία και το integration των συστημάτων εύκολα.

4.2.3 Βάση Δεδομένων της ΚΔΠ

Αναπόσπαστο κομμάτι και της ΚΔΠ είναι το προσωρινό αποθετήριο στοιχείων του χρήστη. Αυτό αποτελεί μία βάση δεδομένων στην οποία έχουν αποθηκευτεί προσωρινά στοιχεία που αφορούν ένα χρήστη που ζητάει πρόσβαση σε κάποια παρεχόμενη υπηρεσία Ηλεκτρονικής Διακυβέρνησης από την ΚΔΠ. Κατά την παρούσα μελέτη και σύμφωνα με την υλοποίηση που τη συνοδεύει, το framework Keycloak παρέχει και αυτή τη δυνατότητα. Έχει δηλαδή ενσωματωμένη βάση δεδομένων, την οποία χρησιμοποιούμε καλύπτοντας ταυτόχρονα και την ανάγκη για ασφάλεια των δεδομένων των χρηστών, αφού αυτά τα διαχειρίζεται εσωτερικά ο ίδιος ο Keycloak Server.

4.3 Εξυπηρετητής Διαχείρισης Ταυτότητας

4.3.1 Λειτουργίες του server – Αρχιτεκτονική

Η συγκεκριμένη οντότητα αποτελεί την καρδιά του συστήματος που υλοποιούμε, καθώς σε αυτή βασίζεται η κεντρική διαχείριση των ηλεκτρονικών ταυτοτήτων των πολιτών. Όπως γίνεται αντιληπτό, πρόκειται για μία σύνθετη οντότητα που συνδυάζει σε μία ενιαία οντότητα την server-side μεριά των πρωτοκόλλων που αναφέραμε παραπάνω ως clients.

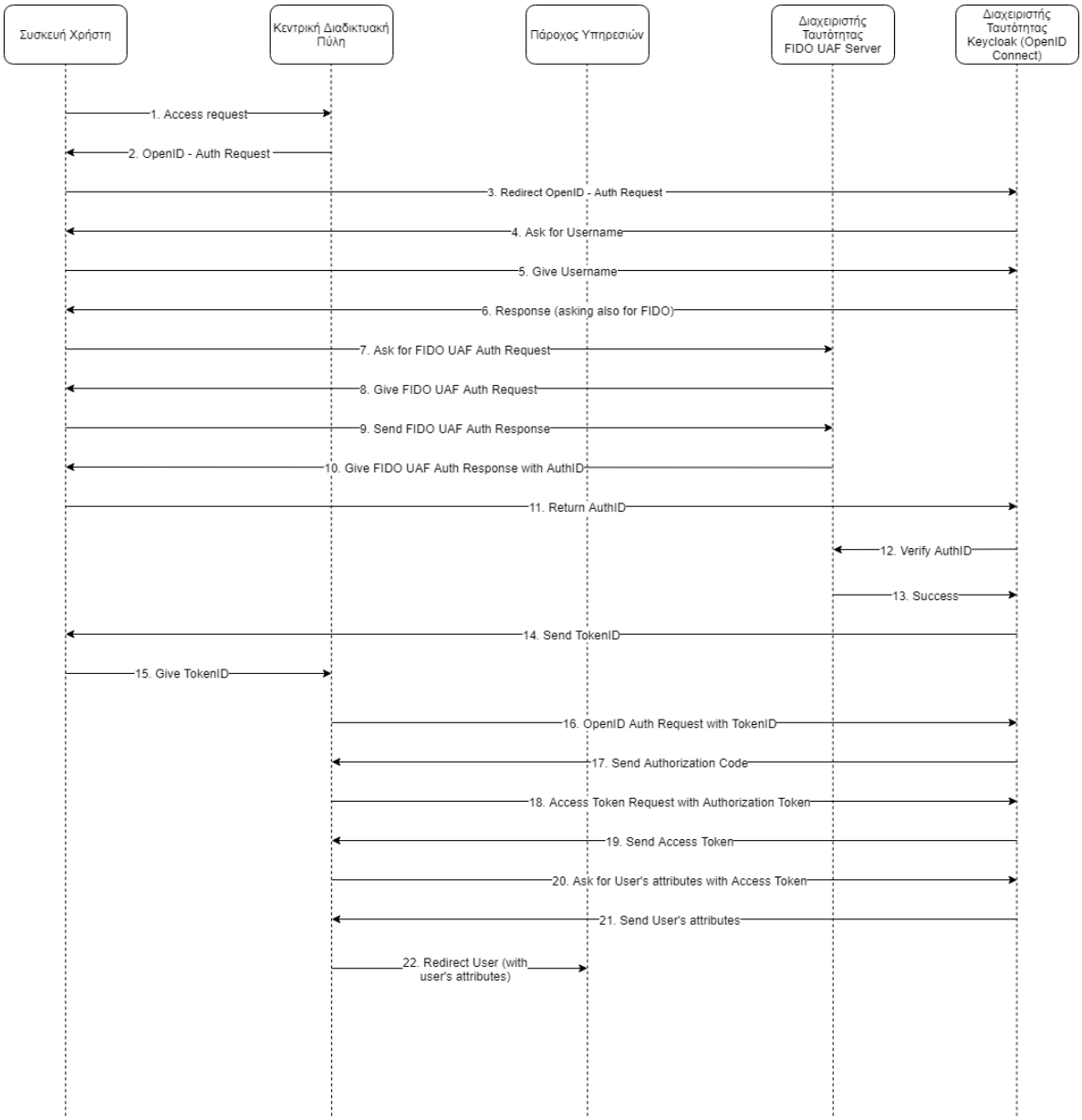
Πιο συγκεκριμένα, ο Διαχειριστής Ταυτότητας στηρίζεται στους server που είναι επιφορτισμένοι να διαχειρίζονται τις αιτήσεις από τους αντίστοιχους clients. Έτσι, για να μπορεί να επιτευχθεί η ταυτοποίηση των χρηστών με δαχτυλικό αποτύπωμα, όπως αναφέραμε, χρησιμοποιείται το πρωτόκολλο FIDO, άρα είναι απαραίτητος ο FIDO Server. Αυτός εμπεριέχεται στο Διαχειριστή Ταυτότητας και συμβάλλει καταλυτικά στη διαδικασία ταυτοποίησης. Είναι η μία πλευρά ανταλλαγής των FIDO UAF μηνυμάτων, όπου ακολουθείται μία συγκεκριμένη διαδικασία που καταλήγει στην αίτηση προς τον

χρήστη να εφαρμόσει το δαχτυλικό του αποτύπωμα στον αναγνώστη. Έπειτα, μετά από εσωτερικές κλήσεις προς το Fingerprint HAL, επιβεβαιώνεται το αποτύπωμα και σε επόμενο στάδιο, με αναζήτηση στο Ασφαλές Αποθετήριο που παρέχει το Android, ταυτοποιείται ο χρήστης. Όπως αναφέραμε, μετά από αυτό το στάδιο πρέπει να γίνει η αποκάλυψη των attributes του χρήστη που ζητήθηκαν. Για το στάδιο αυτό, απαραίτητη είναι η παρουσία του Irma server σαν υπο-οντότητα του Διαχειριστή Ταυτότητας. Πρέπει να σημειώσουμε, ακόμη, ότι ο Irma Server θα κατέχει και θέση Identity Provider (Παρόχου Ταυτότητας). Στον server αυτό, λοιπόν, γίνεται η διαχείριση των διαπιστευτηρίων που βασίζονται στις ιδιότητες του χρήστη. Για την επιτυχημένη υλοποίηση, τέλος, είναι απαραίτητο το login στην Κεντρική Διαδικτυακή Πύλη να γίνεται με εφαρμογή του Single Sign-On. Το απαραίτητο SSO μπορεί να μας το παρέχει ο Keycloak Server, ο οποίος στο παρόν σύστημα θα κατέχει και ρόλο Identity Broker, δηλαδή Μεσολαβητή Ταυτότητας.

4.3.2 Περιγραφή κλάσεων και αλληλεπιδράσεων

Όπως έγινε σαφές, τον Διαχειριστή Ταυτότητας συναποτελούν διάφορες υπο-οντότητες, δηλαδή servers των πρωτοκόλλων και των πλαισίων που χρησιμοποιούμε. Οι διαδικασίες, οι διεργασίες και οι ανταλλαγές των μηνυμάτων μεταξύ τους είναι αρκετά σύνθετες, γι’ αυτό και θα προσπαθήσουμε να τις αναλύσουμε με περιγραφές των αλληλεπιδράσεών τους σε υψηλό επίπεδο (high level).

Αρχικά, η συσκευή χρήστη ζητάει πρόσβαση στην ΚΔΠ, η οποία με τη σειρά της ζητάει Authentication request του πρωτοκόλλου OpenID Connect από το χρήστη. Ουσιαστικά το request αυτό γίνεται ανακατεύθυνση (redirect) προς τον Διαχειριστή Ταυτότητας, δηλαδή προς τον Keycloak server. Εκεί, εμφανίζεται η φόρμα όπου ζητούνται τα credentials του χρήστη και αφού αυτά εισαχθούν θα πρέπει ο χρήστης να ταυτοποιήσει την ταυτότητα του με χρήση του δαχτυλικού του αποτυπώματος. Για το λόγο αυτό, αποστέλλεται το FIDO UAF AUTH Request προς τη συσκευή (FIDO client), όπου μετά την αναγνώριση του αποτυπώματος, δίνεται ως απάντηση στον server το μήνυμα FIDO UAF AUTH Response. Ωστόσο, μέρος του Response προς την συσκευή χρήστη είναι το AuthID, το οποίο ανταλλάσσεται για πιστοποίηση με τον Διαχειριστή Ταυτότητας. Μετά την επιτυχή πιστοποίησή του, καταφέρνει πλέον η συσκευή χρήστη να αποκτήσει αξιόπιστο TokenID ως προς την υπο-οντότητα Keycloak του Διαχειριστή Ταυτότητας. Έτσι, η τελική αξιοποίηση αυτής της ασφαλούς πλέον σύνδεσης που επιτεύχθηκε με το TokenID είναι να ζητηθεί από το χρήστη η αποκάλυψη των attributes του. Αυτά είναι που απαιτεί η ΚΔΠ για τη σύνδεση στην ηλεκτρονική υπηρεσία που έχει επιλέξει ο χρήστης. Τέλος, η διαδικασία ολοκληρώνεται με την αποστολή από τον Irma server των στοιχείων αυτών και η ανακατεύθυνση του χρήστη στην υπηρεσία Ηλεκτρονικής Διακυβέρνησης που αιτήθηκε να χρησιμοποιήσει.



Εικόνα 4. Διαδικασία ταυτοποίησης χρήστη με Keycloak

4.3.3 Βάση Δεδομένων στον server

Ο server πάνω στον οποίο έχει στηθεί το Keycloak framework είναι ένας wildfly server και υποστηρίζεται κατευθείαν από το Keycloak η ύπαρξη βάσης δεδομένων, όπως έχουμε ήδη αναφέρει. Η συγκεκριμένη βάση είναι αναγκαία για τη διατήρηση των ιδιοτήτων των χρηστών που έχουν εγγραφεί στην υπηρεσία της Ηλεκτρονικής Ταυτότητας Πολίτη, μαζί με τα αναγνωριστικά τους και τα χαρακτηριστικά τους, ώστε να υποστηριχτεί αφενός το Single Sign-On, που ενισχύει την ασφάλεια εισόδου των χρηστών, και αφετέρου η attribute-based ταυτότητα, που διασφαλίζει την ιδιωτικότητα των χρηστών σε σχέση με την αποκάλυψη των στοιχείων τους στις διάφορες υπηρεσίες.

4.4 Τεχνολογίες που χρησιμοποιήθηκαν

4.4.1 Keycloak

Το Keycloak είναι μια λύση ανοιχτού κώδικα ταυτότητας και διαχείρισης πρόσβασης για σύγχρονες εφαρμογές και υπηρεσίες. Καθιστά αρκετά εύκολο να εξασφαλιστούν εφαρμογές και υπηρεσίες με ελάχιστο ή και καθόλου κώδικα.

Παρακάτω δίνεται μια σύντομη εισαγωγή στο Keycloak και σε μερικά από τα βασικά χαρακτηριστικά του που το ξεχωρίζουν ως μια αξιόλογη και συνολική λύση για την προστασία σύγχρονων εφαρμογών. Μέσα από την πληθώρα επιλογών που παρέχει το Keycloak σχετικά με τις ρυθμίσεις εγκατάστασής του, η χρήση του είναι γρήγορη και απλή.

- **Single Sign-On (SSO)**

Πριν δούμε ακριβώς την εφαρμογή του SSO μέσα από το Keycloak, χρήσιμο θα ήταν να δώσουμε έναν ορισμό του.

Το Single Sign-On (SSO) είναι μια διαδικασία ελέγχου ταυτότητας που επιτρέπει σε έναν χρήστη να έχει πρόσβαση σε πολλές εφαρμογές με το ίδιο σύνολο διαπιστευτηρίων σύνδεσης. Το SSO είναι μια κοινή διαδικασία στις επιχειρήσεις, όπου ένας πελάτης έχει πρόσβαση σε πολλούς πόρους συνδεδεμένους σε ένα τοπικό δίκτυο (LAN Network). Στα βασικά του πλεονεκτήματα είναι η εξάλειψη των αιτημάτων επανεγγραφής και έκδοσης πιστοποιητικών και άρα των γραφείων υποστήριξης, η βελτίωση της παραγωγικότητας, η βελτίωση της συμμόρφωσης μέσω μιας κεντρικής βάσης δεδομένων και η παροχή λεπτομερούς αναφοράς πρόσβασης των χρηστών.

Με το SSO, ένας χρήστης συνδέεται μία φορά και αποκτά πρόσβαση σε διαφορετικές εφαρμογές, χωρίς να χρειάζεται να ξαναμπεί σε διαπιστευτήρια σύνδεσης σε κάθε εφαρμογή. Ο έλεγχος ταυτότητας SSO διευκολύνει την απρόσκοπτη χρήση των πόρων του δικτύου. Οι μηχανισμοί SSO διαφέρουν ανάλογα με τον τύπο της εφαρμογής.

Το SSO δεν είναι κατάλληλο για συστήματα που απαιτούν εγγυημένη πρόσβαση, καθώς η απώλεια των διαπιστευτηρίων σύνδεσης καταλήγει σε άρνηση πρόσβασης σε όλα τα συστήματα. Στην ιδανική περίπτωση, το SSO χρησιμοποιείται με άλλες τεχνικές ελέγχου ταυτότητας, όπως οι έξυπνες κάρτες και κωδικοί πρόσβασης μιας χρήσης.

Σε ό,τι αφορά το Keycloak, οι χρήστες επαληθεύονται με αυτό και όχι με μεμονωμένες εφαρμογές. Αυτό σημαίνει ότι οι εφαρμογές δεν χρειάζεται να ασχολούνται με τις φόρμες σύνδεσης, τον έλεγχο ταυτότητας χρηστών και την αποθήκευση χρηστών. Μόλις συνδεθείτε στο Keycloak, οι χρήστες δεν χρειάζεται να συνδεθούν ξανά για πρόσβαση σε διαφορετική εφαρμογή. Αυτό ισχύει και για την αποσύνδεση. Το Keycloak παρέχει απλή έξοδο, πράγμα που σημαίνει ότι οι χρήστες πρέπει να αποσυνδέονται μόνο μία φορά για να αποσυνδεθούν από όλες τις εφαρμογές που χρησιμοποιούν το Keycloak.

- **Identity Brokering, Social Login & Standard protocols**

Η σύνδεση στα κοινωνικά δίκτυα είναι εύκολο να προστεθεί μέσω της κονσόλας διαχείρισης του Keycloak. Είναι απλώς θέμα επιλογής του κοινωνικού δικτύου που θέλει κανείς να προσθέσει. Δεν απαιτείται κωδικός ή αλλαγές στην αίτηση. Το Keycloak μπορεί επίσης να πιστοποιήσει τους χρήστες με υπάρχοντες παρόχους πρωτοκόλλων OpenID Connect ή SAML 2.0. Και πάλι, αυτό είναι απλώς θέμα ρύθμισης του παρόχου ταυτότητας μέσω της κονσόλας διαχείρισης.

Το Keycloak έχει ενσωματωμένη υποστήριξη για σύνδεση σε υπάρχοντες διακομιστές LDAP ή Active Directory. Μπορεί, επίσης, να εφαρμοστεί νέος πάροχος εάν υπάρχουν χρήστες σε άλλα σημεία αποθήκευσης, όπως μια σχεσιακή βάση δεδομένων. Εάν οι χρήστες επαληθευτούν στους σταθμούς εργασίας με το Kerberos (LDAP ή Active Directory), μπορούν επίσης να πιστοποιηθούν αυτόματα στο Keycloak χωρίς να χρειάζεται να δώσουν ξανά το όνομα χρήστη και τον κωδικό πρόσβασης (αφού συνδεθούν στον σταθμό εργασίας).

Σημαντικό και αναπόσπαστο κομμάτι του Keycloak αποτελεί και η Διαχείριση Ταυτότητας (Identity Management) που παρέχει, την οποία έχουμε ήδη αναφέρει και ορίσει. Χρησιμοποιείται για να αυθεντικοποιηθεί ένας χρήστης σε έναν τομέα (domain) ενός συστήματος, καθώς και να επιβεβαιωθούν τα δικαιώματά του, δηλαδή σε τι του επιτρέπεται και σε τι του απαγορεύεται η πρόσβαση. Για το λόγο αυτό, στη διαδικασία διαχείρισης ταυτότητας εμπεριέχονται αρκετές φάσεις όπως η αυθεντικοποίηση του χρήστη, το επίπεδο εξουσιοδότησης που έχει καθώς και οι ρόλοι που έχει ένας χρήστης στο εκάστοτε σύστημα, όπως για παράδειγμα η πρόσβαση σε ένα λογισμικό αλλά όχι σε όλα του τα επιμέρους συστατικά.

- **Keycloak Client Adapters**: Οι προσαρμογείς πελατών Keycloak (Keycloak Client Adapters) καθιστούν πραγματικά εύκολη την εξασφάλιση και προστασία εφαρμογών και υπηρεσιών. Υπάρχουν διαθέσιμοι adapters για διάφορες πλατφόρμες και γλώσσες προγραμματισμού. Το Keycloak βασίζεται σε πρότυπα πρωτόκολλα, ώστε να μπορεί να γίνει χρήση οποιασδήποτε βιβλιοθήκης πόρων OpenID Connect ή βιβλιοθήκης παρόχων υπηρεσιών SAML 2.0. Μπορεί, επίσης, να επιλεχθεί ένας διακομιστής μεσολάβησης (proxy server) για να ασφαλιστούν οι εφαρμογές, πράγμα που καταργεί την ανάγκη να τροποποίησης της εφαρμογής.
- **Keycloak Admin Console**: Όπως ήδη αναφέραμε, παρέχεται από το Keycloak διεπαφή (interface) με διαχειριστική κονσόλα. Μέσω της κονσόλας αυτής, οι διαχειριστές μπορούν να διαχειριστούν κεντρικά όλες τις πτυχές του διακομιστή Keycloak. Μπορούν να ενεργοποιήσουν και να απενεργοποιήσουν διάφορα χαρακτηριστικά, όπως μπορούν να διαμορφώσουν τη διαμεσολάβηση ταυτότητας (Identity Brokering) και την ομοσπονδία χρηστών (User Federation). Ακόμη, κάποιος με δικαιώματα διαχειριστή μπορεί να δημιουργεί και να διαχειρίζεται εφαρμογές και υπηρεσίες και να ορίζει λεπτομερείς πολιτικές εξουσιοδότησης. Στα δικαιώματα διαχειριστή, επίσης, είναι η διαχείριση των χρηστών, συμπεριλαμβανομένων των αδειών και των περιόδων σύνδεσης.

- **Account Management Console**: Πέραν της εξειδικευμένης κονσόλας για διαχειριστές, υπάρχει και η κονσόλα που παρέχει στους απλούς χρήστες τη διαχείριση του λογαριασμού τους. Μέσω της κονσόλας αυτής, λοιπόν, οι χρήστες μπορούν να διαχειρίζονται τους λογαριασμούς τους σε ό, τι αφορά την ενημέρωση του προφίλ τους, την αλλαγή κωδικών πρόσβασης και τη ρύθμιση ελέγχου ταυτότητας δύο παραγόντων (2-factor authentication). Οι χρήστες μπορούν επίσης να διαχειρίζονται τις περιόδους σύνδεσης καθώς και το ιστορικό προβολών του λογαριασμού τους. Εάν έχει ενεργοποιηθεί η κοινωνική σύνδεση (social login) ή η διαμεσολάβηση ταυτότητας (identity brokering), οι χρήστες μπορούν επίσης να συνδέσουν τους λογαριασμούς τους με πρόσθετους παρόχους, ώστε να τους επιτρέψουν να πιστοποιήσουν τον ίδιο λογαριασμό με διαφορετικούς παρόχους ταυτότητας.

4.4.2 FIDO Specification

Οι βασικές ιδέες που οδηγούν τις προσπάθειες της FIDO Alliance είναι: 1) η ευκολία χρήσης, 2) η προστασία της ιδιωτικής ζωής και της ασφάλειας, 3) η τυποποίηση. Ο πρωταρχικός στόχος είναι να επιτρέψει σε υπηρεσίες και ιστότοπους την απευθείας σύνδεση, είτε στο Διαδίκτυο είτε σε επιχειρήσεις που θέλουν να αξιοποιήσουν τις εγγενείς λειτουργίες ασφάλειας των υπολογιστικών συσκευών τους για ισχυρό έλεγχο ταυτότητας χρήστη. Ιδανικά, θέλουν ακόμη να μειώσουν τα προβλήματα που σχετίζονται με τη δημιουργία και την ανάμνηση πολλών διαπιστευτηρίων στο διαδίκτυο. Υπάρχουν δύο βασικά πρωτόκολλα που περιλαμβάνονται στην αρχιτεκτονική FIDO που καλύπτουν δύο βασικές επιλογές για την εμπειρία των χρηστών όταν ασχολούνται με υπηρεσίες Internet. Τα δύο πρωτόκολλα μοιράζονται μία κοινή βάση αλλά προσαρμόζονται σε συγκεκριμένες περιπτώσεις χρήσης.

- **Universal Authentication Framework (UAF) Protocol**: Το πρωτόκολλο UAF επιτρέπει στις online υπηρεσίες να προσφέρουν ασφάλεια χωρίς κωδικό πρόσβασης και χωρίς ασφάλεια πολλαπλών παραγόντων. Ο χρήστης καταχωρεί τη συσκευή του στην ηλεκτρονική υπηρεσία επιλέγοντας έναν τοπικό μηχανισμό επαλήθευσης, όπως το δάχτυλο, κοιτάζοντας την κάμερα, μιλώντας στο μικρόφωνο, εισάγοντας ένα PIN κλπ. Το πρωτόκολλο UAF επιτρέπει στην υπηρεσία να επιλέξει τους μηχανισμούς που θα παρουσιαστούν στο χρήστη. Μόλις καταχωριστεί, ο χρήστης επαναλαμβάνει απλώς την τοπική ενέργεια ελέγχου ταυτότητας όποτε χρειάζεται να πιστοποιηθεί στην υπηρεσία. Ο χρήστης δεν χρειάζεται πλέον να εισάγει τον κωδικό πρόσβασής του κατά τον έλεγχο ταυτότητας από τη συγκεκριμένη συσκευή. Το UAF επιτρέπει επίσης συνδυασμούς πολλαπλών μηχανισμών ελέγχου ταυτότητας, όπως δακτυλικό αποτύπωμα + PIN.

- **Universal 2nd Factor (U2F) Protocol**: Το πρωτόκολλο U2F επιτρέπει στις online υπηρεσίες να αυξήσουν την ασφάλεια της υπάρχουσας υποδομής κωδικών πρόσβασης προσθέτοντας έναν ισχυρό δεύτερο παράγοντα στην είσοδο χρήστη. Ο χρήστης συνδέεται με όνομα χρήστη και κωδικό πρόσβασης όπως και πριν. Η υπηρεσία μπορεί επίσης να ζητήσει από τον χρήστη να παρουσιάσει μια δεύτερη συσκευή παράγοντα ανά πάσα στιγμή που επιλέγει. Ο ισχυρός δεύτερος παράγοντας επιτρέπει στην υπηρεσία να απλοποιήσει τους κωδικούς πρόσβασής της (π.χ. 4ψήφιο PIN) χωρίς να θέτει σε κίνδυνο την ασφάλεια. Κατά τη διάρκεια της εγγραφής και του ελέγχου ταυτότητας, ο χρήστης παρουσιάζει τον δεύτερο παράγοντα απλά πατώντας ένα κουμπί σε μια συσκευή USB ή πατώντας το NFC (Near Field Communication). Ο χρήστης μπορεί να χρησιμοποιήσει τη συσκευή FIDO U2F σε όλες τις online υπηρεσίες που υποστηρίζουν το πρωτόκολλο, αξιοποιώντας την ενσωματωμένη υποστήριξη σε προγράμματα περιήγησης ιστού.
- **FIDO UAF High-Level Architecture**: Στη συνέχεια συνοψίζεται η αρχιτεκτονική του FIDO πρωτοκόλλου και δίνεται ο τρόπος με τον οποίο τα στοιχεία του σχετίζονται με τις τυπικές συσκευές χρηστών και τα Τρίτα Συμβαλλόμενα Μέρη (Relying Parties). Τα βασικά συστατικά στοιχεία για την αρχιτεκτονική του FIDO περιγράφονται παρακάτω.
- **FIDO UAF Client**: Ένας FIDO UAF client υλοποιεί την πλευρά του client των πρωτοκόλλων FIDO UAF και είναι υπεύθυνος για: α) την αλληλεπίδραση με συγκεκριμένους FIDO UAF Authenticators χρησιμοποιώντας το FIDO UAF Authenticator Abstraction Layer που παρέχεται μέσω του FIDO UAF Authenticator API, β) την αλληλεπίδραση με έναν χρήστη στη συσκευή (π.χ. μια εφαρμογή για κινητά, ένα πρόγραμμα περιήγησης) που χρησιμοποιεί διεπαφές ειδικά για το χρήστη, για επικοινωνία με τον FIDO UAF Server. Για παράδειγμα, ένα πρόσθετο πρόγραμμα περιήγησης συγκεκριμένο για το FIDO θα χρησιμοποιεί υπάρχουσες πρόσθετες επεκτάσεις (plugins) προγράμματος περιήγησης ή μια εφαρμογή για κινητά μπορεί να χρησιμοποιεί ένα SDK FIDO. Ο χρήστης είναι στη συνέχεια υπεύθυνος για την επικοινωνία των FIDO UAF μηνυμάτων σε ένα FIDO UAF διακομιστή (server) μέσα σε ένα περιβάλλον εμπιστοσύνης. Η αρχιτεκτονική FIDO UAF διασφαλίζει ότι το λογισμικό πελάτη FIDO μπορεί να εφαρμοστεί σε μια σειρά τύπων συστημάτων, λειτουργικών συστημάτων και προγραμμάτων περιήγησης στο Web. Παρόλο που το λογισμικό πελάτη FIDO είναι τυπικά για συγκεκριμένες πλατφόρμες, οι αλληλεπιδράσεις μεταξύ των στοιχείων πρέπει να εξασφαλίζουν συνεπή εμπειρία χρήστη από πλατφόρμα σε πλατφόρμα.
- **FIDO UAF Server**: Ένας FIDO UAF διακομιστής (server) υλοποιεί την πλευρά του διακομιστή των πρωτοκόλλων FIDO UAF και είναι υπεύθυνος για: α) την αλληλεπίδραση με τον διακομιστή ιστού του Relying Party για την επικοινωνία με μηνύματα πρωτοκόλλου FIDO UAF σε έναν FIDO UAF client μέσω μίας συσκευής χρήστη, β) την επαλήθευση των πιστοποιήσεων των FIDO UAF

Authenticators ώστε να διασφαλίζεται ότι έχουν καταχωρηθεί μόνο αξιόπιστοι για χρήση, γ) τη διαχείριση καταχωρημένων FIDO UAF Authenticators σε λογαριασμούς χρηστών του Relying Party, δ) την αξιολόγηση των απαντήσεων επιβεβαίωσης ταυτότητας χρήστη και επιβεβαίωσης συναλλαγής για τον προσδιορισμό της εγκυρότητάς τους. Ο FIDO UAF server έχει σχεδιαστεί ως server που μπορεί είτε να εγκατασταθεί επί τόπου από το εκάστοτε Relying Party που θέλει να τον χρησιμοποιήσει στα συστήματά του είτε ως εξωτερικός συνεργάτης σε τρίτο φορέα παροχής υπηρεσιών με δυνατότητα FIDO.

- **FIDO UAF Authenticator**: Ένας FIDO UAF Authenticator (Επαληθευτής) είναι μια ασφαλής οντότητα, συνδεδεμένη ή τοποθετημένη μέσα σε συσκευές χρήστη FIDO, που μπορούν να δημιουργήσουν το βασικό υλικό (κλειδί) που σχετίζεται με ένα Relying Party. Το κλειδί αυτό μπορεί στη συνέχεια να χρησιμοποιηθεί για συμμετοχή σε ισχυρά πρωτόκολλα ελέγχου ταυτότητας FIDO UAF. Για παράδειγμα, ο FIDO UAF Authenticator μπορεί να δώσει απάντηση σε μια κρυπτογραφική πρόκληση χρησιμοποιώντας το βασικό υλικό (κλειδί) και έτσι θα επαληθεύσει τον εαυτό του στο Relying Party. Προκειμένου να επιτευχθεί ο στόχος της απλοποίησης της ενοποίησης των αξιόπιστων δυνατοτήτων επαλήθευσης ενός χρήστη, ένας FIDO UAF Authenticator θα μπορεί να πιστοποιεί τον συγκεκριμένο τύπο (π.χ. βιομετρικά) και τις δυνατότητές του (π.χ. υποστηριζόμενους αλγόριθμους κρυπτογράφησης) καθώς και την προέλευσή του. Αυτό παρέχει σε ένα Relying Party την εμπιστοσύνη ότι ο χρήστης που πιστοποιείται είναι ο χρήστης που είχε αρχικά καταχωρηθεί στον ιστότοπο.

- **Σενάρια Χρήσης FIDO UAF and Μηνύματα Ροής Πρωτοκόλλο**υ
  - **Authenticator Registration**: Δεδομένης της αρχιτεκτονικής FIDO UAF, ένα Relying Party είναι σε θέση να ανιχνεύσει με διαφάνεια πότε ένας χρήστης αρχίζει να αλληλεπιδρά με αυτό ενώ κατέχει έναν αρχικοποιημένο FIDO UAF Authenticator. Σε αυτήν την αρχική φάση εισαγωγής, ο ιστότοπος θα προτρέψει τον χρήστη σχετικά με οποιονδήποτε ανιχνευμένο FIDO UAF Authenticator (δηλαδή κάποιον διαθέσιμο), δίνοντας επιλογές στον χρήστη σχετικά με την εγγραφή του στον ιστότοπο ή όχι.
  - **Authentication**: Μετά την εγγραφή, ο FIDO UAF Authenticator θα χρησιμοποιηθεί στη συνέχεια κάθε φορά που ο χρήστης επαληθεύεται με τον ιστότοπο (και ο Authenticator είναι παρών). Ο ιστότοπος μπορεί να εφαρμόσει διάφορες εναλλακτικές στρατηγικές για εκείνες τις περιπτώσεις που αυτός δεν υπάρχει. Αυτά μπορεί να κυμαίνονται από το να επιτρέπεται η συμβατική σύνδεση με μειωμένα δικαιώματα έως και το να μην επιτρέπεται η σύνδεση. Αυτό το συνολικό σενάριο θα ποικίλει ελαφρώς ανάλογα με τον τύπο του FIDO UAF Authenticator που χρησιμοποιείται. Ορισμένοι έλεγχοι ταυτότητας ενδέχεται να κάνουν

δειγματοληψία βιομετρικών δεδομένων, όπως εικόνα προσώπου, δακτυλικό αποτύπωμα ή φωνητικό δείγμα. Άλλοι θα απαιτήσουν μια καταχώριση κωδικού PIN ή τοπικού κωδικού πρόσβασης για τον έλεγχο ταυτότητας. Ακόμα άλλοι μπορεί απλώς να απαιτούν ο χρήστης να φέρει/κατέχει έναν επαληθευτή σε υλική μορφή. Λάβετε υπόψη ότι επιτρέπεται σε έναν FIDO client να αλληλεπιδρά με εξωτερικές υπηρεσίες ως μέρος της πιστοποίησης του χρήστη προς τον έλεγχο ταυτότητας, αρκεί να τηρούνται οι Αρχές Προστασίας Προσωπικών Δεδομένων FIDO.

- **Transaction Confirmation**: Υπάρχουν διάφορες καινοτόμες περιπτώσεις χρήσης, δεδομένου ότι τα διάφορα Relying Parties που χρησιμοποιούν FIDO UAF και αλληλεπιδρούν με τελικούς χρήστες χρησιμοποιούν τους επαληθευτές FIDO UAF. Η σύνδεση στο διαδίκτυο και η αυθεντικοποίηση είναι σχετικά απλά παραδείγματα. Μια κάπως πιο προηγμένη περίπτωση χρήσης είναι η ασφαλής επεξεργασία συναλλαγών. Φανταστείτε μια κατάσταση στην οποία ένα Τρίτο μέρος (Relying Party) επιθυμεί ο τελικός χρήστης να επιβεβαιώσει μια συναλλαγή (π.χ. οικονομική λειτουργία, προνομιακή λειτουργία κ.λπ.) έτσι ώστε να μπορεί να εντοπιστεί τυχόν παραβίαση ενός μηνύματος συναλλαγής κατά τη διαδρομή του προς την τελική συσκευή απεικόνισης και πίσω. Η αρχιτεκτονική FIDO έχει την έννοια της "ασφαλούς συναλλαγής" η οποία παρέχει αυτή τη δυνατότητα. Βασικά, εάν ένας FIDO UAF Authenticator έχει δυνατότητα εμφάνισης επιβεβαίωσης συναλλαγής, η αρχιτεκτονική FIDO UAF διασφαλίζει ότι το σύστημα υποστηρίζει τη λειτουργία What You See Is What You Sign (WYSIWYS), δηλαδή «αυτό που βλέπεις είναι αυτό που υπογράφεις». Μια σειρά διαφορετικών περιπτώσεων χρήσης μπορεί να προκύψει από αυτήν την ικανότητα, που σχετίζονται κυρίως με την εξουσιοδότηση συναλλαγών όπως η αποστολή χρημάτων, η πραγματοποίηση ειδικής προνομιακής δράσης, η επιβεβαίωση ηλεκτρονικού ταχυδρομείου / διεύθυνσης κ.λπ.
- **Authenticator Deregistration**: Υπάρχουν κάποιες καταστάσεις στις οποίες ένα συμβαλλόμενο μέρος μπορεί να χρειαστεί να καταργήσει τα διαπιστευτήρια UAF που σχετίζονται με ένα συγκεκριμένο λογαριασμό χρήστη στο FIDO Authenticator. Για παράδειγμα, αν πρέπει ο λογαριασμός του χρήστη να ακυρωθεί ή διαγραφεί, επειδή ο χρήστης FIDO Authenticator χάθηκε ή κλάπηκε κλπ. Σε αυτές τις περιπτώσεις, το Relying Party μπορεί να ζητήσει από τον FIDO Authenticator να διαγράψει τα κλειδιά ελέγχου ταυτότητας που δεσμεύονται στο λογαριασμό χρήστη.

4.4.3 IRMA

Το IRMA αποτελεί μια μοναδική πλατφόρμα ταυτότητας φιλική προς το ιδιωτικό απόρρητο. Κατά τον έλεγχο της ταυτότητας, ο χρήστης αποκαλύπτει μόνο σχετικές ιδιότητες (χαρακτηριστικά) του εαυτού του, χρησιμοποιώντας μια εφαρμογή IRMA στο κινητό του τηλέφωνο – για παράδειγμα εάν ο χρήστης είναι μεγαλύτερος από την ηλικία των 16. Επιπρόσθετα, με την εφαρμογή αυτή δίνεται η δυνατότητα υπογραφής ψηφιακών μηνυμάτων. Με αυτόν τον τρόπο μπορεί ο χρήστης να υπογράψει το όνομα και τη διεύθυνσή του ή την ιατρική του εγγραφή, αν είναι γιατρός ή απλά με τη διεύθυνση ηλεκτρονικού ταχυδρομείου, αν δεν επιθυμεί να αποκαλύψει κάποιο άλλο στοιχείο.

Βασικός στόχος της εφαρμογής είναι η υλοποίηση του συστήματος βάσει χαρακτηριστικών Idemix. Προκειμένου οι χρήστες να είναι σε θέση να διαχειριστούν τα χαρακτηριστικά τους πρέπει να διαθέτουν έναν πελάτη (client) IRMA. Αυτή την περίοδο, υπάρχουν δύο υλοποιήσεις πελατών IRMA. Μια έκδοση έξυπνης κάρτας που δεν διατηρείται πλέον και μια πολύ νεότερη και ευέλικτη εφαρμογή για συσκευές Android και iOS.

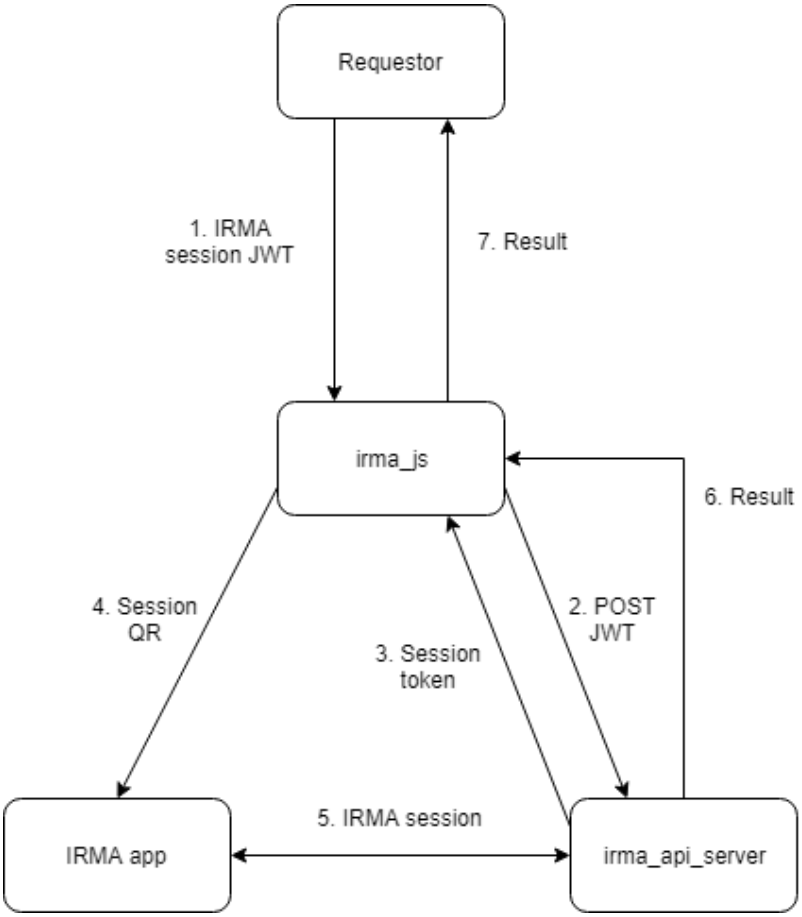
- **Επαλήθευση και έκδοση διαπιστευτηρίων**

Για την πραγματοποίηση, επαλήθευση ή/και έκδοση διαπιστευτηρίων, χρησιμοποιούνται δύο βασικές οντότητες για την υλοποίηση του framework:

- **IRMA API Server**: Ο διακομιστής API χειρίζεται όλες τις κρυπτογραφικές λεπτομέρειες για την έκδοση και επαλήθευση χαρακτηριστικών για λογαριασμό της υπηρεσίας ή του παρόχου ταυτότητας. Από τη μία διαχειρίζεται τα tokens που ανταλλάσσονται και από την άλλη επιτρέπει την αλληλεπίδραση των εξουσιοδοτημένων παρόχων υπηρεσιών με τους παρόχους ταυτότητας. Αποτελεί, λοιπόν, ένα RESTful (Representational station transfer) API JSON που βασίζεται στα JSON Web Tokens (JWTs) για την ταυτοποίηση.
- **IRMA Javascript client**: Το Irma_js αποτελεί τον πελάτη Javascript του RESTful API JSON που προσφέρεται από τον διακομιστή IRMA API, ο οποίος πραγματοποιεί την πραγματική την επαλήθευση και την έκδοση. Αυτό το πρόγραμμα συνδέει ουσιαστικά τη λογική της ιστοσελίδας με τη διαδικασία επαλήθευση/έκδοση, καθιστώντας πολύ εύκολη την ανάπτυξη της τεχνολογίας IRMA στους ιστοτόπους.

- **Ροή περιόδου λειτουργίας IRMA (IRMA session flow)**

Το παρακάτω διάγραμμα παρουσιάζει τη ροή δεδομένων μεταξύ των στοιχείων του λογισμικού IRMA σε μια τυπική συνεδρία IRMA.



Εικόνα 5. Ροή δεδομένων σε μία συνεδρία IRMA

Επεξήγηση των βημάτων:

1. Ο αιτών (δηλαδή ο πάροχος υπηρεσιών ή ταυτότητας που επιθυμεί να επαληθεύσει ή να εκδώσει ιδιότητες) παρέχει ένα JWT που περιέχει ένα αίτημα περιόδου σύνδεσης IRMA, μαζί με τις ανταποκρίσεις επιτυχίας και αποτυχίας στο irma_js.
2. Το irma_js στέλνει ένα POST το JWT στο διακομιστή API.
3. Ο διακομιστής API αποστέλλει το session token στο irma_js.
4. Το irma_js μετατρέπει το αναγνωριστικό σύνδεσης μαζί με τη διεύθυνση URL στον εξυπηρετητή API σε ένα QR code το οποίο ανιχνεύει την εφαρμογή IRMA.
5. Η εφαρμογή IRMA επικοινωνεί με το διακομιστή API και πραγματοποιεί την συνεδρία IRMA.
6. Ο διακομιστής API ενημερώνει το irma_js για το αποτέλεσμα (στην περίπτωση μιας επιτυχημένης συνεδρίας γνωστοποίησης, αυτό περιλαμβάνει ένα JWT που περιέχει τα αποκαλυπτόμενα χαρακτηριστικά).
7. Το irma_js ενημερώνει τον αιτούντα μέσω των ανταποκρίσεων που παρέχονται στο βήμα 1, συμπεριλαμβανομένων των γνωρισμάτων που αποκαλύπτονται στις συνεδρίες επαλήθευσης.

Κεφάλαιο 5

Ανάπτυξη Συστήματος

5.1 Υλοποίηση

Κατά την υλοποίηση του συστήματος, παρατηρήθηκαν έντονα προβλήματα που αφορούσαν την ενσωμάτωση του πυρήνα της εφαρμογής του FIDO με το framework του IRMA. Η εφαρμογή του IRMA για Android συσκευές είναι υπό συνεχή αναδιαμόρφωση και δε δίνεται εύκολα να υιοθετηθεί από εφαρμογές αντίστοιχου ύφους. Αποφασίστηκε, λοιπόν, να υλοποιηθούν δύο βασικά σενάρια που διαχωρίζουν και συγκρίνουν παράλληλα τις επιμέρους εφαρμογές προκειμένου να καταλήξουμε στο ιδανικό πρότυπο που θα αποτελεί την ηλεκτρονική ταυτότητα πολίτη.

Το πρώτο μέρος της υλοποίησης συνδυάζει την ασφαλή αυθεντικοποίηση χρήστη του SSO μηχανισμού του Keycloak μαζί με το framework του FIDO. Όπως έχει αναφερθεί σε προηγούμενο κεφάλαιο, ο χρήστης χρησιμοποιεί το Federated Identity που του παρέχεται από το Keycloak κάνοντας σύνδεση στην ΚΔΠ. Άμεσα ενημερώνεται η συσκευή του που περιέχει την ηλεκτρονική του ταυτότητα πως ο συγκεκριμένος χρήστης αιτείται να συνδεθεί στη πύλη και ξεκινάει η διαδικασία της αυθεντικοποίησης. Μετά την επιλογή της υπηρεσίας που θα χρησιμοποιηθεί, ενημερωτικό μήνυμα εμφανίζεται στην ΚΔΠ προκειμένου ο χρήστης να ταυτοποιηθεί μέσω του FIDO. Η επιτυχημένη ταυτοποίηση του χρήστη στον server του FIDO επικοινωνείται στην ΚΔΠ η οποία ανακατευθύνει τον χρήστη στην κατάλληλη σελίδα που του επιτρέπει ο λογαριασμός που διατηρεί.

Το δεύτερο μέρος της υλοποίησης αφορά στην αυθεντικοποίηση χρήστη με επίγνωση της ιδιωτικότητας και των χαρακτηριστικών του. Κυρίαρχο μέρος της συγκεκριμένης υλοποίησης αποτελεί το πρωτόκολλο επικοινωνίας IRMA και οι ιδιότητες του εκάστοτε χρήστη. Δηλαδή, ο πολίτης εισέρχεται στην ΚΔΠ και επιλέγει την υπηρεσία που επιθυμεί να χρησιμοποιήσει. Εμφανίζεται, τότε, κατάλληλο QR code που απαιτεί ανάγνωση από την εφαρμογή android του IRMA πρωτοκόλλου. Με την ανάγνωση του QR code από τη συσκευή του χρήστη (ηλεκτρονική ταυτότητα) ξεκινάει η επικοινωνία για την επιβεβαίωση των ιδιοτήτων του. Ο χρηστής ερωτάται αν επιτρέπεται να γνωστοποιηθούν στην υπηρεσία συγκεκριμένα χαρακτηριστικά του και εφόσον ληφθεί θετική απάντηση μέσω της εφαρμογής, ανακατευθύνεται από την ΚΔΠ στην κατάλληλη σελίδα της υπηρεσίας που επιθυμεί να συνδεθεί.

5.1.1 Ασφαλής Αυθεντικοποίηση Χρήστη

Οι τρεις βασικές οντότητες του πρώτου σεναρίου υλοποίησης που χρησιμοποιήθηκαν είναι οι εξής:

- **Ηλεκτρονική Ταυτότητα Πολίτη**

Η ηλεκτρονική ταυτότητα πολίτη που υλοποιήθηκε αποτελείται από μία εφαρμογή για συσκευές android και περιέχει δύο βασικές υπο-οντότητες. Η πρώτη αφορά τη SSO λειτουργία που παρέχεται μέσω του framework του OpenID του Keycloak ενώ η δεύτερη το πρωτόκολλο ταυτοποίησης και αυθεντικοποίησης του FIDO. Όπως έχει αναφερθεί στην σχεδίαση του συστήματος, η αρχή της ροής περιόδου λειτουργίας πραγματοποιείται από την ΣΧ με αίτημα για την απόκτηση session ID από την ΚΔΠ. Η ΚΔΠ στέλνει το κατάλληλο OpenID-Auth Request ώστε να ενημερωθεί ο ΔΤ (στη προκειμένη περίπτωση ο Keycloak server) για το ποια συσκευή πρόκειται να επιτρέψει την ταυτοποίηση. Η εφαρμογή περιέχει το όνομα χρήστη αποθηκευμένο ώστε να χρησιμοποιηθεί σε οποιοδήποτε αίτημα για ταυτοποίηση από την ΚΔΠ. Συνεπώς, τα αιτήματα ταυτοποίησης για το ΔΤ στέλνονται από την εφαρμογή μέσω του Keycloak client που υπάρχει εγκαταστημένος. Όταν η ταυτοποίηση επιτευχθεί αποστέλνεται στη συσκευή το access token από τον διακομιστή αυθεντικοποίησης (Keycloak server).

Για την ολοκλήρωση ταυτοποίησης του πρώτου σεναρίου, εκτός από την ταυτοποίηση στον OpenID server χρειάζεται και η αυθεντικοποίηση του FIDO server, ώστε να επιβεβαιωθούν τα βιομετρικά χαρακτηριστικά του χρήστη και συγκεκριμένα το δαχτυλικό του αποτύπωμα. Η εφαρμογή διαθέτει τον FIDO client που διαχειρίζεται την επικοινωνία με τον FIDO server μέσω καταλλήλων μηνυμάτων ταυτοποίησης. Ο FIDO client αποστέλλει αίτημα στον FIDO server ώστε να εκκινήσει την διαδικασία της ταυτοποίησης. Επαληθεύοντας το appID και το facetID της συσκευής, η ροή λειτουργίας συνεχίζεται με την επικοινωνία του FIDO UAF Authenticator με το HAL της συσκευής. Το FIDO UAF Authenticator περιέχεται στο core σύστημα της εφαρμογής και αφού λάβει την επιτυχημένη ή αποτυχημένη προσπάθεια του χρήστη για ταυτοποίηση του δαχτυλικού αποτυπώματός του, ενημερώνει αντιστοίχως τον FIDO client και ο client με τη σειρά του αποστέλλει κατάλληλο μήνυμα στο server. Παρακάτω παρουσιάζεται το Auth-Response που λαμβάνει ο FIDO server σε μορφή JSON:


```
[
    {
      "header": {
        "upv": {
          "major": 1,
          "minor": 0
        },
        "op": "Auth",
        "appID": "http://192.168.1.4:8081/fidouaf/v1/public/uaf/facets",
        "serverData":
"aUk0aGtMTWpUSDNpREtrV2JRcXJPTUxpVGVaUFBqUVFnemgxaFlDN2lSay5NVFUwT
```

VRJM09ERTVNREl4T1EuU2tSS2FFcEVSWGRLUlZwS1pEQkZkazlIT1dwaVZtUklaRlZrYjAwelZtRlJhMVpxVG1rMA"
},
"fcParams":
"eyJhcHBJRCI6Imh0dHA6Ly8xOTIuMTY4LjEuNDo4MDgxL2ZpZG91YWYvdjEvcHVibGljL3VhZi9mYWNldHMiLCJjaGFsbGVuZ2UiOiJKREpoSkRFd0pFWkpkMEV2T0c5amJWZEhkVWRvTTNWYVFrVmpOaTQiLCJmYWNldElEIjoiIn0",
"assertions": [
{
"assertionScheme": "UAFV1TLV",
"assertion": "Aj4lAQQ-1QALLgkARUJBMCMwMDAxDi4FAAAAAQIADy5AADc1YWYwMzkwNTkyNTIwODMwYjM4YmM0ZjAxOTFjMGRlMDkxMDU1NGMxYjdmYmRhZjgwZDVmMTExZDhhMDUzZTkKLiAA2951lZUpOiNDPpNw3_07hEmmvZf_AV6RmY4ijcTFs4EQLgAACS5HAFpXSmhlUzEwWlhOMExXdGxlUzFLUkVwb1NrUkZkMHBFYUhoUlZUVlhWSHBhVms1cWJGZGliVEF5V1c1S1JsWklSbkZPZVRRDS4EAAAAAQAGLkgAMEYCIQC_Gyvacng9oxyBjfkctEqtQ6bJSRzcMh0tOALahf1AtAIhAO18sNYTpKQZxLxpS1_CNr1H3M4ggS9kspLpXLBaHvNK",
"exts": null
}
]
}
]

Οι σημαντικότερες παράμετροι που χρειάζονται ανάλυση είναι το "op" που αναφέρεται στη διαδικασία αυθεντικοποίησης (Authentication), το "appID" το οποίο ταυτοποιεί στο server το facetID της εφαρμογής και το "assertion" που περιέχει κρυπτογραφημένα τις πληροφορίες της ταυτοποίησης.

Συνεπώς, η ηλεκτρονική ταυτότητα πολίτη αποτελείται από μία εφαρμογή με τρία βασικά στοιχεία υλοποιημένα: τον OpenID client, τον FIDO client και τον FIDO UAF Authenticator. Περιέχει προεγκατεστημένο το username που διαθέτει ο χρήστης και αποτελεί το μοναδικό αναγνωριστικό του σε ολόκληρο το σύστημα (Federated Identity) διότι αντικείμενο της συγκεκριμένης διπλωματικής εργασίας δεν αποτελεί η εγγραφή του χρήστη στην ΚΔΠ και στη χορήγηση των πιστοποιητικών του, που θα απαιτούνταν σε διαφορετική περίπτωση. Επιπρόσθετα, υπάρχει αποθηκευμένο στο ασφαλές αποθετήριο κρυπτογραφημένων δεδομένων το δαχτυλικό αποτύπωμα του χρήστη με το οποίο γίνεται η σύγκριση κατά την διαδικασία της ταυτοποίησης.

- **Κεντρική Διαδικτυακή Πύλη**

Η Κεντρική Διαδικτυακή Πύλη αποτελεί την αρχική σελίδα που επισκέπτεται ο χρήστης κατά την εισαγωγή του στην ιστοσελίδα και αποτελεί ένα maven project που σηκώνεται στη διεύθυνση localhost:8080. Περιέχει όλες τις υπηρεσίες που διαθέτει το σύστημα όπως ο Εθνικός Οργανισμός Παροχής Υπηρεσιών Υγείας (ΕΟΠΥΥ), το Εθνικό Μετσόβιο Πολυτεχνείο (ΕΜΠ), τη Γενική Γραμματεία Πληροφοριακών Συστημάτων (ΓΓΠΣ), όπως και κάποια σημεία επικοινωνίας (ηλεκτρονική διεύθυνση και τηλέφωνο). Κατά την υλοποίηση του πρώτου σεναρίου χρησιμοποιείται μόνο η

επιλογή του ΕΟΠΥΥ και η ανακατεύθυνση του χρήστη στις διαθέσιμες επιλογές της συγκεκριμένης υπηρεσίας.

Αφού ο χρήστης επιλέξει την υπηρεσία που επιθυμεί να ταυτοποιηθεί, ένα παράθυρο σύνδεσης με όνομα χρήστη και κωδικό πρόσβασης εμφανίζεται στο προσκήνιο. Ο κωδικός πρόσβασης συνδέεται μόνο με τα στοιχεία του ΔΤ που αποτελεί ο Keycloak server. Δεν συνδέεται με την χρήση του FIDO Framework. Έπειτα από τον server του Keycloak κατάλληλο μήνυμα στην εφαρμογή, ώστε να πραγματοποιηθεί η σχέση εμπιστοσύνης μεταξύ της εφαρμογής και του server.

Μετά από την ολοκληρωμένη ταυτοποίηση του χρήστη στο κινητό τόσο στον Keycloak server (λαμβάνοντας το κατάλληλο token) όσο και στον FIDO server τότε ο χρήστης μπορεί να πατήσει κατάλληλο κουμπί στην ΚΔΠ και να ανακατευθυνθεί στη υπηρεσία και τα περιεχόμενά της. Η υλοποίηση της εκάστοτε υπηρεσίας έχει πραγματοποιηθεί εμφωλευμένα στη ΚΔΠ (εμφωλευμένο περιεχόμενο σε γλώσσα html) διότι δίνεται δυνατότητα στο χρήστη να επιστρέψει άμεσα στην αρχική σελίδα της ΚΔΠ και να περιηγηθεί σε μια διαφορετική υπηρεσία.

- **Εξυπηρετητής Διαχείρισης Ταυτότητας**

Ο Εξυπηρετητής Διαχείρισης Ταυτότητας αποτελεί την σημαντικότερη οντότητα του συστήματος καθώς διαχειρίζεται τους δύο servers που είναι απαραίτητοι για την συνολική ταυτοποίηση του χρήστη στην υπηρεσία. Ο πρώτος server είναι ο Keycloak και συμβάλλει στην υλοποίηση του OpenID Framework, ενώ ο δεύτερος είναι του FIDO, που είναι υπεύθυνος για το UAF Authentication. Ο Keycloak server αποτελεί έναν wildfly server που σηκώνεται στη localhost:8180 (localhost:8180/auth είναι η διεύθυνση για τη διαχειριστική κονσόλα του Keycloak).

Μέσω της διαχειριστική κονσόλας του Keycloak δημιουργήθηκε ένα σχήμα Realm προκειμένου να τεθούν οι γενικές ρυθμίσεις του Διαχειριστή Ταυτότητας. Έπειτα δηλώθηκε ένας client (για το παράδειγμά μας ο ΕΟΠΥΥ) που αφορά την κάθε υπηρεσία ξεχωριστά η οποία πρόκειται να χρησιμοποιηθεί από το Federated Identity System και ένας ρόλος, αυτός των χρηστών του συστήματος. Στη βάση Users (Χρήστες) του Keycloak αποθηκεύτηκαν όλοι οι διαθέσιμοι χρήστες της ΚΔΠ, ενώ παράλληλα ρυθμίστηκαν οι διευθύνσεις και τα endpoints για την ταυτοποίηση των ιστοτόπων.

Ο server του Keycloak λαμβάνει σε πρώτη φάση το αίτημα όταν κάποιος χρήστης προσπαθήσει να συνδεθεί στην ΚΔΠ. Αφού επιβεβαιώσει την ύπαρξη του συγκεκριμένου χρήστη, αποστέλλει στην πύλη κατάλληλη απάντηση μαζί με το session ID το οποίο θα χρησιμοποιηθεί από την εφαρμογή του κινητού τηλεφώνου του χρήστη, επιτρέποντας την αναγνώριση της ασφαλούς σχέσης και επικοινωνίας ΚΔΠ-εφαρμογής. Αφού ο χρήστης ολοκληρώσει την ταυτοποίησή του στον FIDO server, νέο αίτημα αποστέλλεται από την ΚΔΠ προς τον Keycloak server για τον αν η ταυτοποίηση εκπληρώθηκε σωστά. Τότε, αυτός επικοινωνεί με τον FIDO server στέλνοντας αίτημα με παραμέτρους το όνομα του χρήστη και την κατάσταση της ταυτοποίησης, μαζί με το χρονικό σημείο της ταυτοποίησης. Αν η απάντηση είναι ταυτιστεί με αυτές τις παραμέτρους, επιστρέφει θετικό μήνυμα στην ΚΔΠ και ο χρήστης αυτόματα

ανακατευθύνεται στην υπηρεσία που έχει αιτηθεί. Το JSON response που ανταλλάσσουν οι δύο server μεταξύ τους είναι το εξής:


```
[
  {
    "AAID": "EBA0#0001",
    "KeyID":
"WldKaGVTMTBaWE4wTFd0bGVTMUtSRXBvU2tSRmQwcEVhSGhSVlRWWFZIcGFWaz
VxYkZkaWJUQXlXVzVLUmxaSVJuRk9lVFE",
    "username": "user1",
    "status": "SUCCESS",
    "auth_time": 1541278195
  }
]
```


Στην αντίθετη τροχιά, ο FIDO server λαμβάνει το πρώτο αίτημα μόλις ο χρήστης εκκινήσει την εφαρμογή του κινητού. Επαληθεύει την εγκυρότητά της, μαζί με το facetId της συσκευής που θα πρέπει να είναι αποθηκευμένο στη βάση του server. Ενημερώνει έπειτα τη συσκευή πως μπορεί να ξεκινήσει η διαδικασία ταυτοποίησης με το UAF Authenticator. Όταν η διαδικασία εισαγωγής του δαχτυλικού αποτυπώματος ολοκληρωθεί, ο FIDO client αποστέλλει κατάλληλο αίτημα με τα στοιχεία του χρήστη, της συσκευής και του αποτελέσματος της ταυτοποίησης και αυτά αποθηκεύονται στη βάση του FIDO server για τα επόμενα 5 λεπτά. Μέσα στο συγκεκριμένο χρονικό διάστημα, ο χρήστης πρέπει να πατήσει το κατάλληλο κουμπί στη ΚΔΠ ώστε ο Keycloak server να ρωτήσει για τον αν ο χρήστης με το συγκεκριμένο username ολοκλήρωσε την ταυτοποίηση του στην εφαρμογή. Στην περίπτωση που όλα έχουν ολοκληρωθεί σωστά ο FIDO server ενημερώνει τον Keycloak server και η ανακατεύθυνση πραγματοποιείται επιτυχώς. Διαφορετικά, ζητείται από τον χρήστη να ταυτοποιηθεί ξανά χρησιμοποιώντας την ηλεκτρονική του ταυτότητα (εφαρμογή κινητού).

5.1.2 Αυθεντικοποίηση Χρήστη με Επίγνωση της Ιδιωτικότητας

Σε αντίστοιχο πνεύμα, θα αναλυθούν οι τρεις οντότητες που υλοποιήθηκαν για την εκπόνηση της αυθεντικοποίησης χρήστη με επίγνωση της ιδιωτικότητας:

- **Ηλεκτρονική Ταυτότητα Πολίτη**

Η ηλεκτρονική ταυτότητα πολίτη στο δεύτερο σενάριο αποτελείται κυρίως από την εφαρμογή IRMA με έκδοση 5.3.2 (Οκτώβριος 2018) που έχει κατασκευαστεί από το Privacy by Design Foundation. Η εφαρμογή δίνει τη δυνατότητα στο χρήστη να αποκτά (issue attributes) και να αποκαλύπτει και επιβεβαιώνει (disclosure/verify attributes) χαρακτηριστικά που περιέχονται στο λογαριασμό της εφαρμογής κωδικοποιημένα. Προκειμένου να ταυτοποιηθεί ο χρήστης στην ΚΔΠ και εν συνεχεία στην υπηρεσία που θα επιλέξει, η αποκάλυψη χαρακτηριστικών αποτελεί την ενέργεια που πραγματοποιείται από την πλευρά της εφαρμογής.

Αρχικά, ο χρήστης του κινητού (πολίτης με συγκεκριμένα χαρακτηριστικά) χρειάζεται να αποκτήσει και να αποθηκεύσει τις ιδιότητες που απαιτούνται στις υπηρεσίες που επισκέπτεται. Για το δικό μας σενάριο, υλοποιήθηκαν δύο χρήστες (πολίτες) του Εθνικού Μετσόβιου Πολυτεχνείου. Ο πρώτος χρήστης είναι φοιτητής ενώ ο δεύτερος καθηγητής. Η απόκτηση των χαρακτηριστικών πραγματοποιήθηκε με χρήση του demo ιστότοπου που παρέχεται από Privacy by Design https://demo.irmacard.org/tomcat/irma_api_server/examples/issue-all.html. Αξιοποιήθηκε η κλάση χαρακτηριστικών irma-demo.RU.studentCard και πιο συγκριμένα τα πεδία studentID (7ψηφιος αριθμός μητρώου χρηστών ΕΜΠ) και level (ρόλος του χρήστη στο ΕΜΠ, φοιτητής ή καθηγητής). Οι υπόλοιπες κλάσεις αγνοήθηκαν καθώς δεν απαιτούνται για την εκτέλεση του σεναρίου.

Αφού συμπληρώθηκαν τα πεδία της κλάσης που θα χρησιμοποιηθεί, πατήσαμε το κουμπί “Issue credentials” το οποίο παρήγαγε το QR code που διαβάστηκε από δύο διαφορετικές συσκευές με την εφαρμογή IRMA (μία συσκευή για τον φοιτητή και μία για τον καθηγητή). Ο κάθε χρήστης αποδέχτηκε το αίτημα για απόκτηση χαρακτηριστικών και πλέον είναι σε θέση να τα διαθέτει για επιβεβαίωση στον πάροχο του ΕΜΠ κάθε φορά που αυτό απαιτείται.

Η υπηρεσία μετά την πρώτη επικοινωνία με τον server παράγει ένα QR code που διαβάζεται από την εφαρμογή. Το περιεχόμενο του κώδικα παρουσιάζεται παρακάτω σε μορφή JSON:

```
{
  "irmaqr": "disclosing",
  "u": "http://192.168.1.4:8088/api/v2/verification/sessionID",
  "v": "2.0",
  "vmax": "2.3"
}
```

Η πρώτη παράμετρος αφορά στη διαδικασία που αιτείται η υπηρεσία από τον χρήστη, στη συγκεκριμένη περίπτωση την αποκάλυψη χαρακτηριστικών (disclosing). Η παράμετρος “u” περιέχει το session token μαζί με το URL του server του IRMA. Αξίζει να αναφέρουμε πως σε κάθε αίτημα από την υπηρεσία για ταυτοποίηση η μεταβλητή “u” διαφοροποιείται καθώς παράγεται ένα καινούριο session ID. Τέλος, οι άλλες δύο παράμετροι αφορούν στο εύρος των εκδόσεων API που υποστηρίζει ο IRMA server.

Μετά την εγκαθίδρυση της επικοινωνίας εφαρμογής-server, ο τελευταίος ενημερώνει για τα χαρακτηριστικά που ζητάει η υπηρεσία να ταυτοποιηθούν και να αποκαλυφθούν. Στη συγκεκριμένη περίπτωση, ο server ζητάει να λάβει το περιεχόμενο των παραμέτρων irma-demo.RU.studentCard.studentID και irma-demo.RU.studentCard.level. Τότε, εμφανίζεται στην εφαρμογή κατάλληλο μήνυμα που αναφέρει τα χαρακτηριστικά προς αποκάλυψη και αν ο χρήστης αποδέχεται ή όχι την ενέργεια αυτή. Πατώντας είτε Αποδοχή (Accept) είτε Άρνηση (Refuse), αποστέλλεται από την εφαρμογή κατάλληλη απάντηση. Σε περίπτωση αποδοχής, αποστέλλεται μαζί με τη θετική απάντηση και το περιεχόμενο των παραμέτρων αυτών ώστε να γίνουν γνωστά στην υπηρεσία.

- **Κεντρική Διαδικτυακή Πύλη (ΚΔΠ)**

Η ΚΔΠ αποτελείται από ένα Dynamic Web Project σηκωμένο σε Tomcat server στη τοποθεσία localhost:8080. Το project της ΚΔΠ περιέχει html αρχεία καθώς και javascript που εκτελούν τις ενέργειες που απαιτούνται για την επικοινωνία της ΚΔΠ με την εφαρμογή και τον IRMA server. Το html αρχείο της ΚΔΠ απαρτίζεται από το κυρίως μέρος (body) αλλά και από το κομμάτι των χρωμάτων, των σχημάτων και των γραμματοσειρών (style).

Η αρχική σελίδα της ΚΔΠ απαρτίζεται από την κεφαλίδα συνοδευόμενη από κουμπιά των κατηγοριών των υπηρεσιών. Έπειτα από φωτογραφίες-κουμπιά των διαθέσιμων υπηρεσιών και στο κατώτερο της τμήμα περιέχονται γενικές πληροφορίες αλλά και μια φόρμα συμπλήρωσης στοιχείων επικοινωνίας με το Υπουργείο Εσωτερικών. Στο αριστερό μέρος βρίσκονται τρεις σελιδοδείκτες για την αμεσότερη πλοήγηση του χρήστη στην ιστοσελίδα.

Ο χρήστης πατώντας στην εικόνα του Πολυτεχνείου φορτώνεται η αρχική του σελίδα. Στο σενάριο της ταυτοποίησης το ΕΜΠ αποτελεί τον αιτών (requestor) στο framework του IRMA. Η ΚΔΠ μαζί με τη σελίδα του ΕΜΠ περιέχουν τον javascript client που επικοινωνούν αρχικά με το server προκειμένου να δοθεί το σήμα εκκίνησης και έπειτα με το κινητό παρουσιάζοντας το QR code session. Όπως αναφέρθηκε και προηγουμένως η ιστοσελίδα του πανεπιστημίου ζητάει να ταυτοποιηθεί ο χρήστης, αποκαλύπτοντας τον ρόλο που έχει εντός ιδρύματος καθώς και τον αριθμό μητρώου του. Για το σκοπό αυτό αποστέλλεται ένα JSON Web Token (JWT) με την εξής μορφή:

```
{
   "iss": "Service provider name",
   "kid": "service_provider_name",
   "sub": "verification_request",
   "iat": 1453377600,
   "sprequest": {
            "validity": 600,
            "timeout": 600,
            "request": {
                     "content": [
                     {
                     "label": "Type",
                     "attributes": ["irma-demo.RU.studentCard.level"]
                     },
                     {
                     "label": "ID",
                     "attributes": ["irma-demo.RU.studentCard.studentID"]
                     }
             ]
            }
  }
}
```

Από το παραπάνω JSON αξίζει να αναφερθεί το τμήμα που περιέχει το "sprequest" με τις μεταβλητές που ζητούνται για ταυτοποίηση. Εκτός αυτών, το "validity" αναφέρεται στο χρονικό διάστημα σε δευτερόλεπτα που παραμένει διαθέσιμο στο server το αποτέλεσμα της ταυτοποίησης, ενώ το "timeout" το μέγιστο χρονικό διάστημα εγκυρότητας του αιτήματος ταυτοποίησης. Το "iss" αναφέρεται στο όνομα του παρόχου υπηρεσιών και το "iat" ο χρόνος δημιουργίας του αιτήματος.

Ο server του IRMA απαντάει σύμφωνα με το JSON που αναφέρθηκε στην προηγούμενη ενότητα το οποίο κωδικοποιείται σε QR code αφού ο χρήστης πατήσει το κατάλληλο κουμπί. Το QR code δημιουργείται σε ένα στοιχείο του html που λέγεται καμβάς (canvas) και παράγεται από τη βιβλιοθήκη javascript με όνομα "qrcode".

Μετά την ταυτοποίηση του χρήστη, εμφανίζεται στη σελίδα του ΕΜΠ κουμπί που εξαρτάται από τον ρόλο που έχει ο χρήστης ο οποίος προσπαθεί να ταυτοποιηθεί. Αν είναι φοιτητής, ανακατευθύνεται σε σελίδα με τις υπηρεσίες που προσδιορίζονται αποκλειστικά για εκείνον. Σε αντίστοιχη περίπτωση, ο καθηγητής πλοηγείται σε σελίδα που απευθύνεται στο διδακτικό προσωπικό του ιδρύματος. Το αποτέλεσμα που λαμβάνει ο javascript client είναι κρυπτογραφημένο με τον αλγόριθμο RS256.

- **Εξυπηρετητής Διαχείρισης Ταυτότητας**

Ο εξυπηρετητής διαχείρισης ταυτότητας αποτελείται στο σχήμα ταυτοποίησης από τον server του IRMA, ο οποίος σηκώνεται στη διεύθυνση localhost:8088. Η υλοποίησή του διευκολύνεται από τη χρήση του docker (πλατφόρμας διαχείρισης εφαρμογών διαδικτύου). Επιπρόσθετα, όταν εκκινείται ο server δίνεται και το δημόσιο κλειδί (public key), ώστε να δημιουργηθεί σχέση εμπιστοσύνης με τον αιτούντα πάροχο υπηρεσιών.

Όταν η υπηρεσία ζητήσει την αποκάλυψη συγκεκριμένων χαρακτηριστικών ο server επικυρώνει την εγκυρότητα του αιτήματος, επιστρέφοντας το κατάλληλο session ID στον javascript client για να δημιουργήσει το QR code. Έπειτα, η εφαρμογή επικοινωνεί απευθείας με τον server ώστε να επιβεβαιώσει την ταυτότητα του χρήστη με τις κατάλληλες τιμές. Η κρυπτογραφημένη απάντηση του server με το αποτέλεσμα της ταυτοποίησης παρουσιάζεται παρακάτω με τη μορφή JSON:


```
{
  "exp": 1448636691,
  "sub": "disclosure_result",
  "attributes": {
    "irma-demo.RU.studentCard.level": "Student",
    "irma-demo.RU.studentCard.studentID": "s1234567",
  },
  "iat": 1448636631,
  "status": "VALID"
}
```

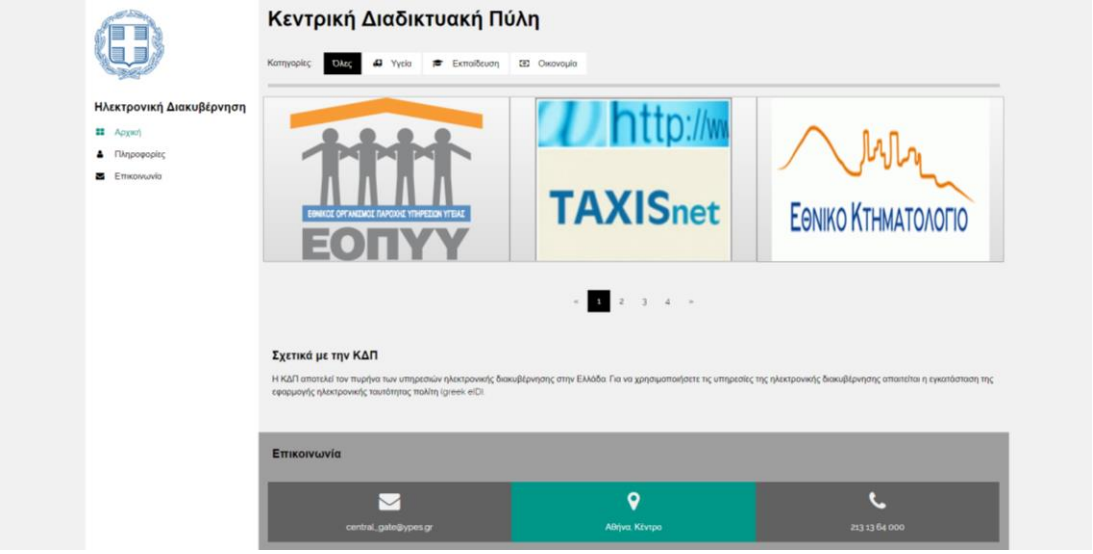

Δύο παράμετροι αποτελούν τον πυρήνα της απάντησης. Η πρώτη είναι τα χαρακτηριστικά και οι τιμές τους ("attributes") και η δεύτερη η κατάσταση της

απάντησης (“status”). Η παράμετρος “iat” προσδιορίστηκε προηγουμένως, ενώ το “exp” αναφέρεται στο χρόνο εκπνοής της απάντησης του αιτήματος ταυτοποίησης.

5.2 Παραδείγματα χρήσης – Εκτέλεση πιλοτικών σεναρίων

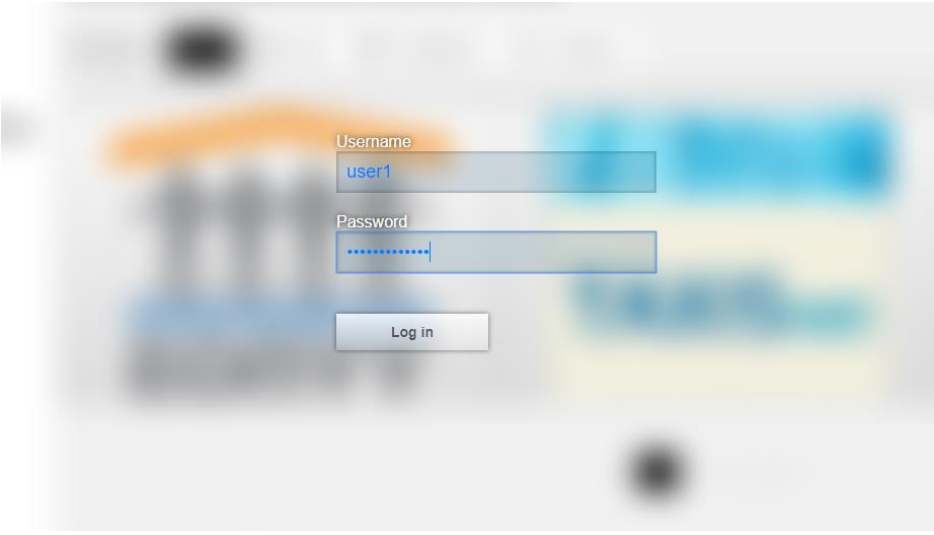
Σενάριο 1ο

Πλοήγηση στην Κεντρική Διαδικτυακή Πύλη:



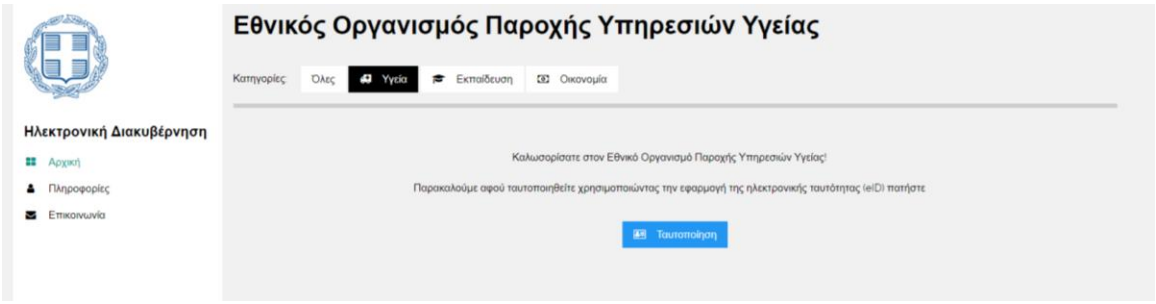
Εικόνα 6. Κεντρική Διαδικτυακή Πύλη

Επιλογή στην υπηρεσία του ΕΟΠΥΥ και εμφάνιση φόρμας ονόματος χρήστη – κωδικού πρόσβασης:



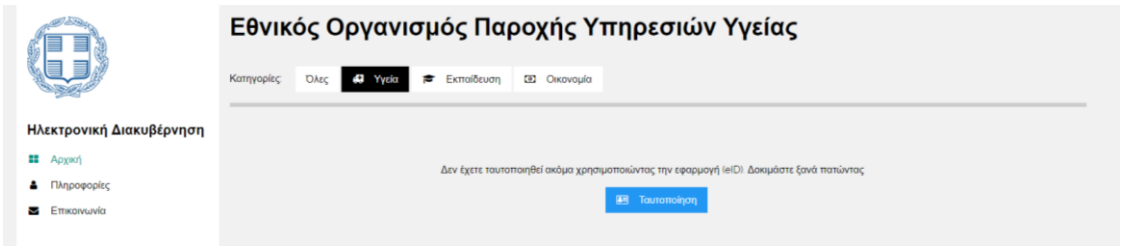
Εικόνα 7. Φόρμα συμπλήρωσης όνομα χρήστη και κωδικού πρόσβασης

Είσοδος στην κεντρική σελίδα του ΕΟΠΥΥ (πριν από την ταυτοποίηση με τη χρήση της ηλεκτρονικής ταυτότητας):



Εικόνα 8. Αρχική σελίδα ΕΟΠΥΥ

Σε περίπτωση αποτυχημένης προσπάθειας ταυτοποίησης με το FIDO ή σε περίπτωση που ο χρήστης πατήσει το κουμπί «Ταυτοποίηση» χωρίς να έχει ταυτοποιηθεί μέσω της εφαρμογής.



Εικόνα 9. Μήνυμα λάθους στη σελίδα του ΕΟΠΥΥ

Εκκίνηση της εφαρμογής Ηλεκτρονικής Ταυτότητας Πολίτη:

Εικόνα 10. Αρχική σελίδα εφαρμογής eID

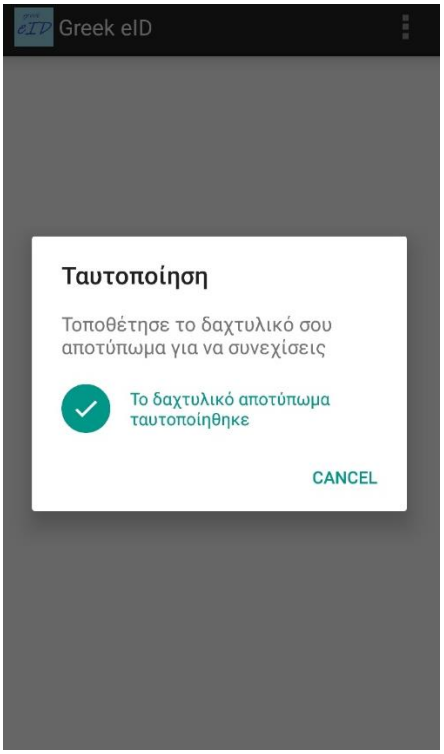
Είσοδος στην ταυτότητα πολίτη:

Εικόνα 11. Εικόνα μετάβασης στην κεντρική σελίδα της εφαρμογής

Εμφάνιση της ταυτότητας πολίτη και επιλογή του κουμπιού ταυτοποίηση:

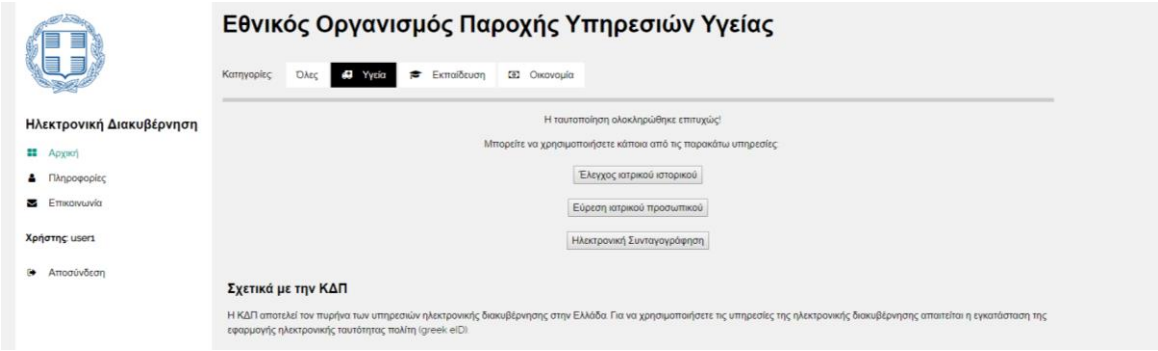
Εικόνα 12. Κεντρική σελίδα της εφαρμογής eID

Τοποθέτηση δαχτύλου στον αναγνώστη δαχτυλικών αποτυπωμάτων και έλεγχος αυτού:



Εικόνα 13. Παράθυρο ταυτοποίησης δαχτυλικού αποτυπώματος

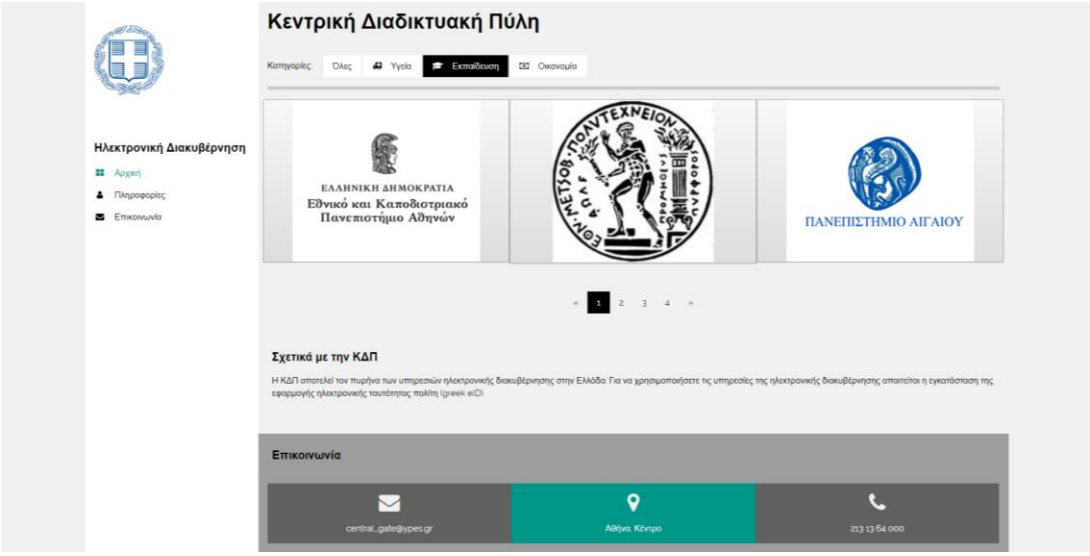
Επιστροφή στην υπηρεσία του ΕΟΠΥΥ και πάτημα του κουμπιού «Ταυτοποίηση» και εμφάνιση των διαθέσιμων υπηρεσιών που μπορεί να επιλέξει ο χρήστης μετά την επιτυχημένη ταυτοποίησή του:



Εικόνα 14. Κεντρική σελίδα ΕΟΠΥΥ ταυτοποιημένου χρήστη

Σενάριο 2.a (ταυτοποίηση φοιτητή)

Πλοήγηση στην Κεντρική Διαδικτυακή Πύλη (Εικόνα 6. Κεντρική Διαδικτυακή Πύλη) και επιλογή της ενότητας εκπαίδευσης:

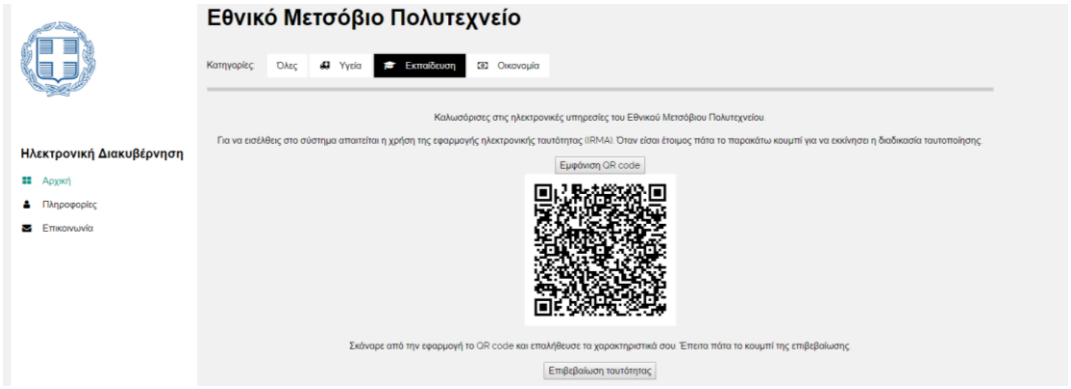


Εικόνα 15. Υπηρεσίες Εκπαίδευσης

Είσοδος στην κεντρική σελίδα του Εθνικού Μετσόβιου Πολυτεχνείου:

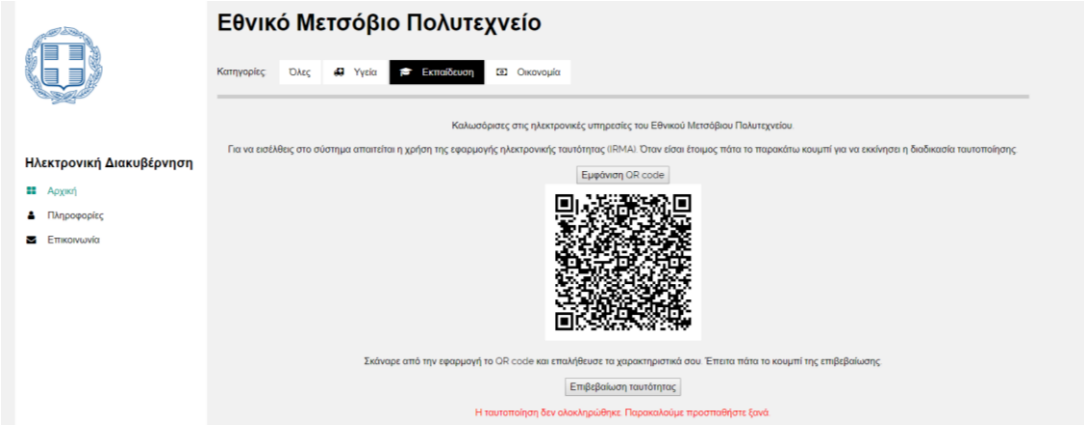
Εικόνα 16. Κεντρική σελίδα ΕΜΠ

Πάτημα του πλήκτρου «Εμφάνιση QR code»:



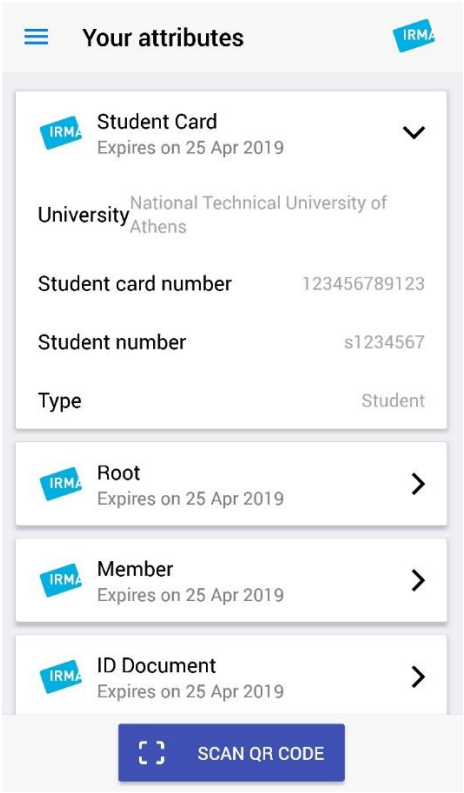
Εικόνα 17. Εμφάνιση QR code στη σελίδα του ΕΜΠ

Σε περίπτωση που ο χρήστης πατήσει «Επιβεβαίωση ταυτότητας» πριν ολοκληρωθεί η ταυτοποίηση ή η ταυτοποίηση αποτύχει:



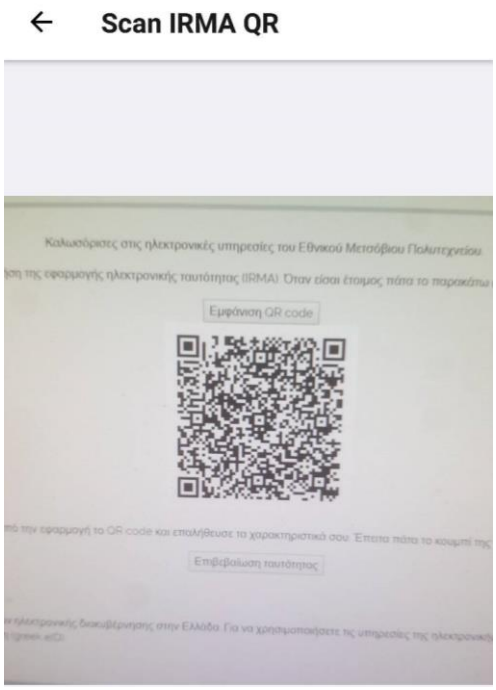
Εικόνα 18. Μήνυμα λάθους στη σελίδα του ΕΜΠ

Εκκίνηση της εφαρμογής IRMA:



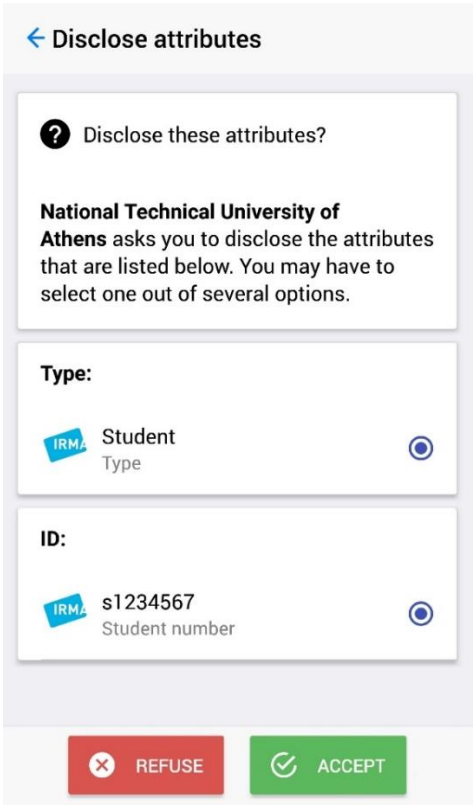
Εικόνα 19. Αρχική σελίδα εφαρμογής IRMA - Στοιχεία φοιτητή

Επιλογή «SCAN QR CODE» για να εκκινήσει η ανάγνωση του QR code:



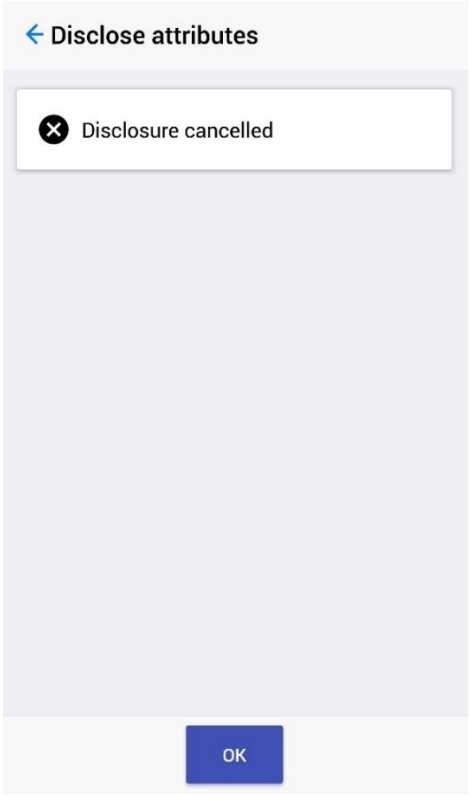
Εικόνα 20. Σάρωση QR code

Αναγνώριση του αιτήματος ταυτοποίησης καθώς και των χαρακτηριστικών που ζητούνται από την υπηρεσία:



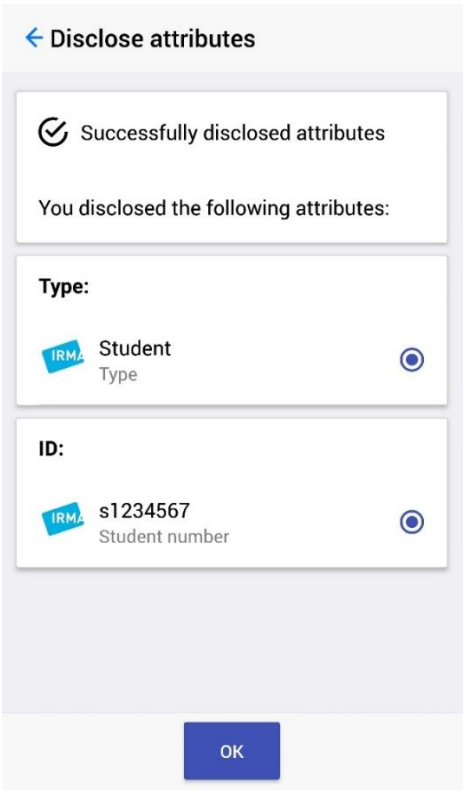
Εικόνα 21. Αίτημα αποκάλυψης χαρακτηριστικών φοιτητή

Άρνηση παραχώρησης των χαρακτηριστικών της ηλεκτρονικής ταυτότητας:



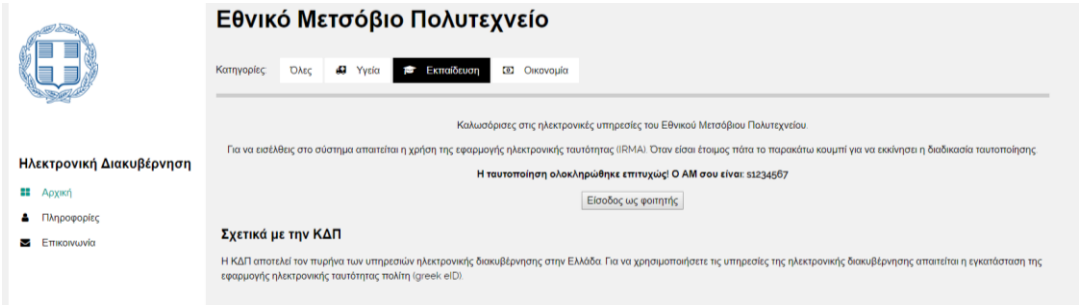
Εικόνα 22. Άρνηση αποκάλυψης χαρακτηριστικών

Επιβεβαίωση παραχώρησης των χαρακτηριστικών της ηλεκτρονικής ταυτότητας:



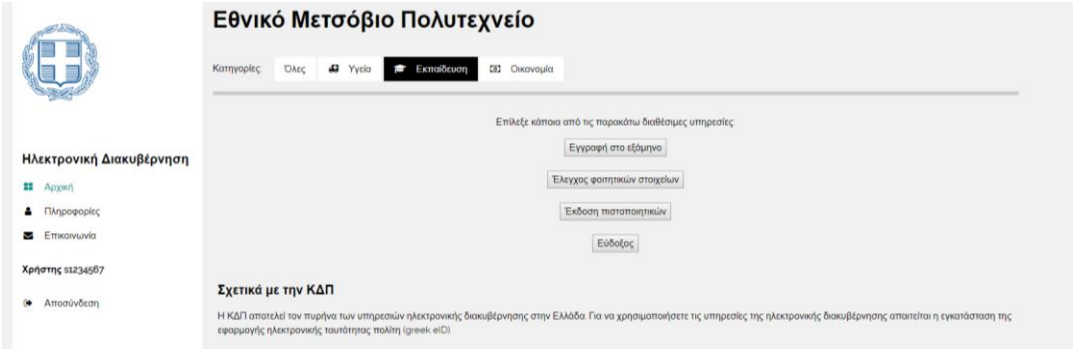
Εικόνα 23. Επιτυχημένη αποκάλυψη χαρακτηριστικών φοιτητή

Επιστροφή στη σελίδα του Πολυτεχνείου και επιλογή του κουμπιού «Επιβεβαίωση ταυτότητας»:



Εικόνα 24. Επιτυχημένη ταυτοποίηση φοιτητή

Επιλογή «Είσοδος ως φοιτητής» και εμφάνιση των διάφορων υπηρεσιών του ΕΜΠ για φοιτητές:



Εικόνα 25. Κεντρική σελίδα ΕΜΠ για υπηρεσίες φοιτητών

Σενάριο 2.b (ταυτοποίηση καθηγητή)

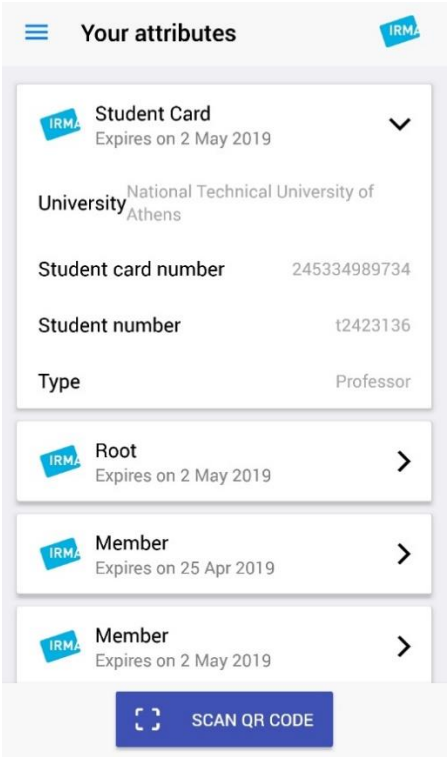
Πλοήγηση στην Κεντρική Διαδικτυακή Πύλη (Εικόνα 6. Κεντρική Διαδικτυακή Πύλη) και επιλογή της ενότητας εκπαίδευσης (Εικόνα 15. Υπηρεσίες Εκπαίδευσης).

Είσοδος στην κεντρική σελίδα του Εθνικού Μετσόβιου Πολυτεχνείου (Εικόνα 16. Κεντρική σελίδα ΕΜΠ).

Πάτημα του πλήκτρου «Εμφάνιση QR code» (Εικόνα 17. Εμφάνιση QR code στη σελίδα του ΕΜΠ).

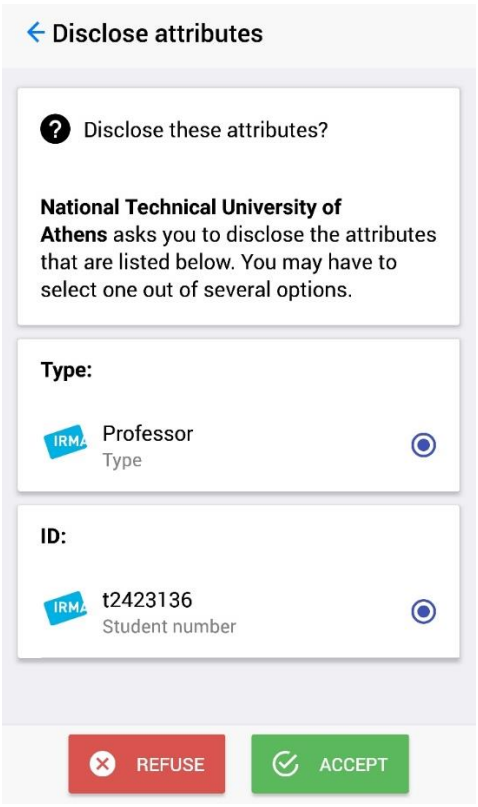
Σε περίπτωση που ο χρήστης πατήσει «Επιβεβαίωση ταυτότητας» πριν ολοκληρωθεί η ταυτοποίηση ή η ταυτοποίηση αποτύχει (Εικόνα 18. Μήνυμα λάθους στη σελίδα του ΕΜΠ).

Εκκίνηση της εφαρμογής IRMA:



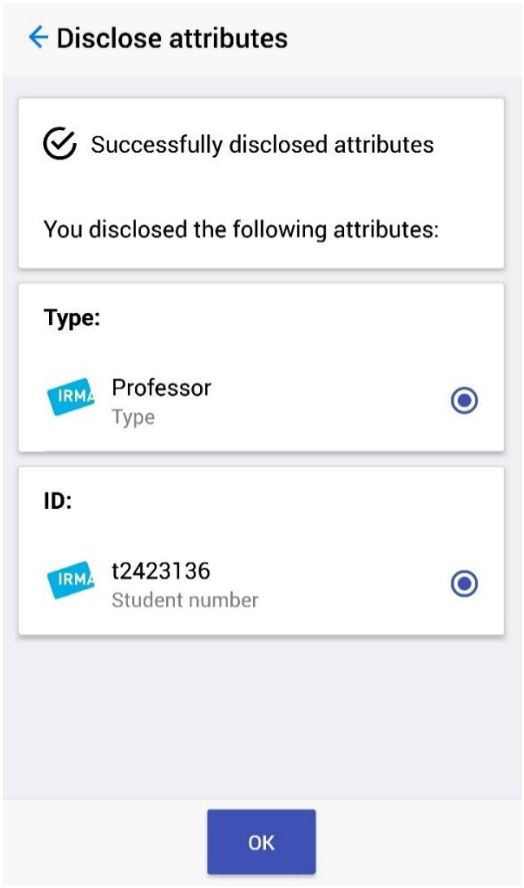
Εικόνα 26. Αρχική σελίδα εφαρμογής IRMA - Στοιχεία καθηγητή

Επιλογή «SCAN QR CODE» για να εκκινήσει η ανάγνωση του QR code (Εικόνα 20. Σάρωση QR code) και αναγνώριση του αιτήματος ταυτοποίησης καθώς και των χαρακτηριστικών που ζητούνται από την υπηρεσία:



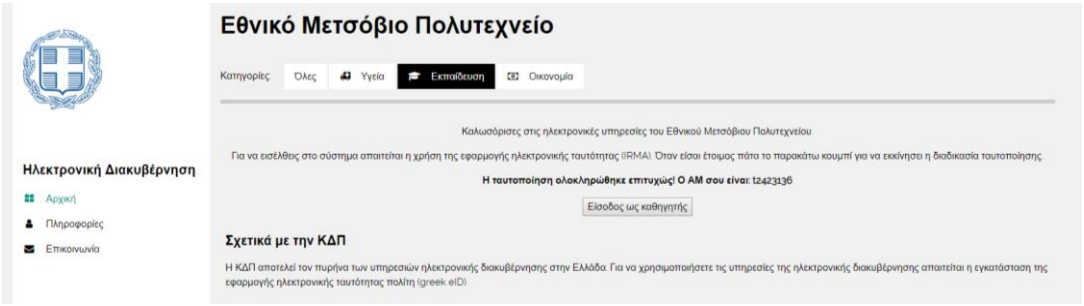
Εικόνα 27. Αίτημα αποκάλυψης χαρακτηριστικών καθηγητή

Άρνηση παραχώρησης των χαρακτηριστικών της ηλεκτρονικής ταυτότητας (Εικόνα 22. Άρνηση αποκάλυψης χαρακτηριστικών) και επιβεβαίωση παραχώρησης των χαρακτηριστικών της ηλεκτρονικής ταυτότητας:



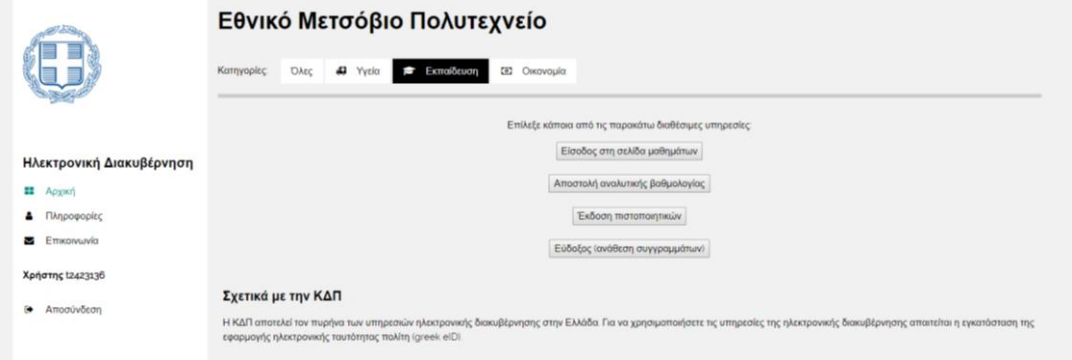
Εικόνα 28. Επιτυχημένη αποκάλυψη χαρακτηριστικών καθηγητή

Επιστροφή στη σελίδα του Πολυτεχνείου και επιλογή του κουμπιού «Επιβεβαίωση ταυτότητας»:



Εικόνα 29. Επιτυχημένη ταυτοποίηση καθηγητή

Επιλογή «Είσοδος ως καθηγητής» και εμφάνιση των διάφορων υπηρεσιών του ΕΜΠ για το διδακτικό προσωπικό:



Εικόνα 30. Κεντρική σελίδα ΕΜΠ με υπηρεσίες διδακτικού προσωπικού

5.3 Σύγκριση υλοποιήσεων

Μετά την υλοποίηση και εκτέλεση των δύο σεναρίων, κρίνεται απαραίτητο να μελετηθούν τα πλεονεκτήματα και τα μειονεκτήματα της κάθε περίπτωσης ξεχωριστά προκειμένου να αξιολογηθεί ο βαθμός επίτευξης του ιδανικού μοντέλου ηλεκτρονικής ταυτότητας πολίτη.

Κατά την εκτέλεση του πρώτου σεναρίου με τα frameworks των Keycloak και FIDO, γίνεται αντιληπτό πως η ασφάλεια αποτελεί το μεγαλύτερο προτέρημα. Ο χρήστης καλείται να ταυτοποιηθεί όχι μόνο εισάγοντας το όνομα χρήστη και τον κωδικό πρόσβασής του στην ΚΔΠ αλλά επαληθεύοντας και την φυσική του παρουσία με τη χρήση του δαχτυλικού αποτυπώματος. Επιπροσθέτως, οι πληροφορίες των χρηστών που ανταλλάσσονται μεταξύ των οντοτήτων του συστήματος είναι κρυπτογραφημένες προς αποφυγή αλλοιώσεων ή παραβιάσεων, ενώ το μόνο κοινό χαρακτηριστικό που υπάρχει στο σύστημα για την ταυτότητα ενός πολίτη είναι το όνομα χρήστη του.

Σε αντίστοιχο πλαίσιο ασφάλειας εντάσσεται και το δεύτερο σενάριο υλοποίησης με το framework του IRMA. Η επικοινωνία των συστημάτων είναι πλήρως κρυπτογραφημένη και τα μηνύματα που στέλνονται δεν εμπεριέχουν προσωπικές πληροφορίες του χρήστη. Εν αντιθέσει με την πρώτη υλοποίηση, το IRMA δίνει μεγάλη βαρύτητα και στην ιδιωτικότητα του πολίτη. Δηλαδή, κατά την είσοδο και ταυτοποίηση ενός χρήστη σε μια υπηρεσία, τα μοναδικά χαρακτηριστικά που αποκαλύπτονται και αποστέλλονται είναι εκείνα που η ίδια η υπηρεσία απαιτεί χωρίς να έχει πρόσβαση στα υπόλοιπα στοιχεία του πολίτη.

Ένα απλό παράδειγμα της καθημερινότητας μπορεί να αναδείξει την σημασία της ιδιωτικότητας που παρέχεται από το IRMA μέσω της ηλεκτρονικής ταυτότητας. Ένας 17χρονος μαθητής επιθυμεί να παρακολουθήσει μια ταινία στον τοπικό κινηματογράφο με την ένδειξη «άνω των 16 ετών». Κατά την έκδοση των εισιτηρίων τού ζητείται η αστυνομική ταυτότητα. Παραχωρώντας την αστυνομική ταυτότητα, ο μαθητής αποκαλύπτει και άλλα προσωπικά του στοιχεία που δεν χρειαζόντουσαν να αποκαλυφθούν κατά την επικαιροποίηση της ηλικίας του όπως το ονοματεπώνυμό του, ο τόπος καταγωγής του ή ακόμα και η ομάδα αίματός του. Συνεπώς, η ίδια ταυτοποίηση με την χρήση της ηλεκτρονικής ταυτότητας η οποία εμπεριέχει το πρωτόκολλο του IRMA θα γινόταν αποκαλύπτοντας το περιεχόμενο μόλις μιας παραμέτρου (ηλικία άνω

των 16 ετών – ναι ή όχι) χωρίς να δημοσιευτεί καν η πλήρης ημερομηνία γεννήσεως του πολίτη.

Βέβαια το πρωτόκολλο του IRMA δεν αρκεί όπως μελετήθηκε και παραπάνω για την ολοκληρωμένη υλοποίηση της ηλεκτρονικής ταυτότητας. Σε περίπτωση απώλειας της συσκευής οποιοσδήποτε χρήστης θα είναι σε θέση να παραχωρήσει τα χαρακτηριστικά και τις ιδιότητες σε όποια υπηρεσία είναι εγγεγραμμένη η εφαρμογή. Ο χρήστης προστατεύεται πλήρως όταν η προσωπική του ταυτότητα, επικυρώνεται και από τη φυσική του παρουσία, μέσω του δαχτυλικού αποτυπώματος. Το FIDO αποτελεί μια ανερχόμενη αρχιτεκτονική ταυτοποίησης συσκευών παρέχοντας άμεση προσβασιμότητα και ασφάλεια.

Το πρώτο σενάριο προσδίδει μία ακόμη σημαντική παράμετρο. Το χαρακτηριστικό του SSO που προσφέρεται μέσω του framework του Keycloak αποτελεί τον πυρήνα των Federated Identity Management (Ομαδοποιημένη Διαχείριση Ταυτοτήτων). Ο πολίτης είναι σε θέση να συνδεθεί και να χρησιμοποιήσει την εκάστοτε υπηρεσία με μόλις ένα κοινό όνομα χρήστη και την εφαρμογή της ηλεκτρονικής ταυτότητας. Δεν χρειάζεται διαφορετικά ονόματα χρήστη, αλλά το σημαντικότερο: ο τρόπος ταυτοποίησης είναι ο ίδιος σε όλες τις υπηρεσίες ανεξαρτήτου τομέα.

Συνεπώς η ιδανική σχεδίαση και υλοποίηση της ηλεκτρονικής ταυτότητας, καθιστά απαραίτητη τη χρήση και των τριών προαναφερθέντων μηχανισμών ταυτοποίησης: Keycloak (Open ID – SSO Technology), FIDO (UAF Authentication), IRMA (Idemix). Είναι εξάλλου απαραίτητο να αναφερθεί ότι οι παραπάνω τεχνολογίες – μέσω της υλοποίησης και των δύο σεναρίων - προσδίδουν εκτός από την ασφάλεια και την ιδιωτικότητα και τις υπόλοιπες γενικές αρχές και στρατηγικές τοποθετήσεις που έχει θεσπίσει η Ευρωπαϊκή Επιτροπή όπως:

- Διαλειτουργικότητα: Όλες οι διαθέσιμες υπηρεσίες συνεργάζονται με τα πληροφοριακά συστήματα που παρέχει η ΚΔΠ.
- Συμμόρφωση στους κανόνες: Αυστηρές προδιαγραφές που ακολουθούν του δεσμευτικούς κανόνες της Ηλεκτρονικής Διακυβέρνησης.
- Ενοποίηση: Η πρόσβαση στις πληροφορίες όλων των υπηρεσιών γίνεται μέσω της ΚΔΠ.
- Εξοικονόμηση: Επιφέρει εξοικονόμηση πόρων, χρόνου και κόστους τόσο στη Δημόσια Διοίκηση όσο και στους πολίτες και τις επιχειρήσεις.
- Διαφάνεια: Οι πολίτες είναι σε θέση ανά πάση στιγμή να διαχειρίζονται τις πληροφορίες που καταγράφονται στις δημόσιες υπηρεσίες.
- Προσβασιμότητα: Δίνεται η δυνατότητα χρήσης της ηλεκτρονικής διακυβέρνησης από όλους τους πολίτης, ακόμα και στους ψηφιακά αναλφάβητους ή στα άτομα με ειδικές ανάγκες.
- Συμμετοχή πολιτών: Οι πολίτες μπορούν να συμμετέχουν ενεργά στη λήψη κυβερνητικών αποφάσεων αλλά και στο σχεδιασμό και την αξιολόγηση των υπηρεσιών δημόσιας διοίκησης.

Κεφάλαιο 6

Συμπεράσματα και Μελλοντικές Επεκτάσεις

Στο παρόν κεφάλαιο θα γίνει μία σύνοψη της παρούσας διπλωματικής εργασίας της οποίας αντικείμενο, όπως έχει ήδη αναφερθεί, είναι η υλοποίηση της Ηλεκτρονικής Ταυτότητας Πολίτη (eID). Θα γίνει μια αναφορά σχετικά με την υφιστάμενη κατάσταση σε θεωρητικό αλλά και πρακτικό επίπεδο, καθώς και μία παρουσίαση των συμπερασμάτων που προέκυψαν σε ό,τι αφορά τη χρήση της αλλά και τις δυνατότητες που υπάρχουν για μελλοντικές της επεκτάσεις.

Αρχικά, πραγματοποιήθηκε μία έρευνα σχετικά με το πλαίσιο της Ηλεκτρονικής Διακυβέρνησης και τη θέση της Ηλεκτρονικής Ταυτότητας σε αυτό και παρουσιάστηκε μία σύνοψη από τα αποτελέσματά της. Μελετήθηκε το εύρος εφαρμογής και χρήσης τους, τόσο σε ευρωπαϊκό επίπεδο όσο και σε ελληνικό, καθώς και τα πλαίσια διαλειτουργικότητας που εφαρμόζονται. Στη συνέχεια, δόθηκε μία περιγραφή του προβλήματος θέτοντας αυστηρούς κανόνες ασφάλειας, σύμφωνα με τα όσα μελετήθηκαν, και τηρώντας τα διεθνή πρότυπα. Από την επακόλουθη ανάλυση των απαιτήσεων του συστήματος και λαμβάνοντας υπόψη όλες τις παραμέτρους ασφάλειας και προστασίας της ιδιωτικότητας, σχεδιάστηκε με προσοχή η αρχιτεκτονική του συστήματος μέσα στο οποίο θα γίνεται η χρήση της Ηλεκτρονικής Ταυτότητας Πολίτη. Ακριβώς λόγω του γεγονότος ότι η εφαρμογή που αναπτύχθηκε θα χρησιμοποιείται από τους πολίτες, δόθηκε μεγάλη έμφαση στην αλληλεπίδραση με τους χρήστες, φροντίζοντας για την ευκολία, ευχρηστία και φιλικότητα προς τους αυτούς με γνώμονα πάντα την ασφάλειά τους.

Στην πορεία, έγινε μία ανάλυση των βασικών οντοτήτων του συστήματος, δηλαδή της ίδιας της Ηλεκτρονικής Ταυτότητας Πολίτη, της Κεντρικής Διαδικτυακής Πύλης και του Διαχειριστή Ταυτότητας. Αυτές οι οντότητες χρησιμοποιούν συγκεκριμένα frameworks και εφαρμόζουν αυστηρούς κανόνες (specifications) κατά την υλοποίησή τους και ακριβώς για να πετύχει η επικοινωνία τους μέσα από αυστηρά κανάλια και κωδικοποιημένα μηνύματα, τα frameworks και οι κανόνες διαλειτουργούν μεταξύ τους. Αφού έγιναν ξεκάθαρες οι οντότητες αυτές και οι λειτουργίες που κάθε μία θα επιτελεί, σχεδιάστηκαν όλες μαζί ως ενιαίο σύστημα και καθορίστηκε το βασικό σενάριο χρήσης. Σύμφωνα με αυτό, ο εκάστοτε πολίτης θα εισέρχεται στην Κεντρική Διαδικτυακή Πύλη, θα επιλέγει την υπηρεσία που επιθυμεί και στη συνέχεια θα ταυτοποιείται με χρήση του δαχτυλικού του αποτυπώματος, εγκρίνοντας ταυτόχρονα την αποκάλυψη μόνον όσων χαρακτηριστικών του είναι απαραίτητα για να εισέλθει στην υπηρεσία και να ανακατευθυνθεί ανάλογα με τις ιδιότητες που έχει.

Υλοποιήθηκαν στην πράξη δύο σενάρια χρήσης της Ηλεκτρονικής Ταυτότητας και του συστήματος στο οποίο αυτή θα χρησιμοποιείται. Στην πρώτη περίπτωση έγινε συνδυασμός των τεχνολογιών Single Sign-On και UAF Authentication με χρήση των αντίστοιχων πρωτοκόλλων που τα εφαρμόζουν, δίνοντας ιδιαίτερη έμφαση στην ασφάλεια του χρήστη. Στη δεύτερη περίπτωση, εφαρμόστηκε η τεχνολογία Idemix μέσα από το κατάλληλο πλαίσιο, σύμφωνα με την οποία ο χρήστης είναι αυτός που επιλέγει ποια από τα χαρακτηριστικά και προσωπικά του στοιχεία που εμπεριέχει η ηλεκτρονική του ταυτότητα θα αποκαλυφθούν σε μία υπηρεσία όταν αυτή τα ζητήσει.

Όπως διαπιστώθηκε και κατά την εκτέλεση των δύο σεναρίων χρήσης, η σαφής διαφοροποίησή τους είναι τα σημεία στα οποία εστιάζει η κάθε υλοποίηση. Αφενός στο πρώτο σενάριο έχουμε απόλυτα διασφαλισμένη την αυθεντικοποίηση του χρήστη, αφού για να ταυτοποιηθεί χρειάζεται το δαχτυλικό του αποτύπωμα (security-aware), ενώ στο δεύτερο σενάριο γίνεται φιλτράρισμα και επιλεκτική αποκάλυψη στοιχείων, διασφαλίζοντας την ιδιωτικότητα του εκάστοτε πολίτη (privacy-aware).

Είναι αδιαμφισβήτητο ότι και τα δύο σενάρια επιβεβαιώνουν στην πράξη την εφαρμογή των απαραίτητων συστατικών μίας επιτυχημένης ανάπτυξης μίας Ηλεκτρονικής Ταυτότητας Πολίτη. Προφανώς, ένα τέτοιο εγχείρημα δε θα μπορούσε να υπάρξει και να γίνει αποδεκτό από κυβερνήσεις και κυρίως πολίτες που νοιάζονται για την ασφάλεια των δεδομένων τους, των ιδιαίτερων χαρακτηριστικών τους και γενικά της ταυτότητάς τους. Ωστόσο, όπως ήδη σημειώθηκε, η υπάρχουσα υλοποίηση χωρίζεται σε δύο υπο-συστήματα, κάνοντας σαφή τα σημεία που υπερτερεί και υστερεί το καθένα. Το Single Sign-On, που παρέχεται μέσα από την εφαρμογή του OpenID Connect πρωτοκόλλου του πρώτου σεναρίου, διασφαλίζει το Federated login (Ομοσπονδιακή είσοδο), δηλαδή την είσοδο ενός χρήστη σε όλα τα συστήματα της Ηλεκτρονική Ταυτότητας με τους ίδιους προσωπικούς κωδικούς, δηλαδή με την ίδια ταυτότητα. Η επιλεκτική αποκάλυψη των χαρακτηριστικών του χρήστη στην εκάστοτε υπηρεσία, πάντα μετά από έγκριση του χρήστη, που παρουσιάζεται στο δεύτερο σενάριο εφαρμόζει το attributed-based IRMA πρωτόκολλο.

Όπως φαίνεται, τα δύο αυτά σενάρια έχουν ξεχωριστά πλεονεκτήματα το καθένα και καθώς το πρωτόκολλο του IRMA χρησιμοποιείται όλο και περισσότερο από σύγχρονες εφαρμογές, πρέπει να μελετηθούν οι μελλοντικές επεκτάσεις της παρούσας υλοποίησης. Με βάση και τον αρχικό σχεδιασμό, μία συνένωση και ενοποίηση των δύο διαφορετικών σεναρίων φαντάζει ως η ιδανική μελλοντική επέκταση στην υπάρχουσα υλοποίηση. Πρέπει, δηλαδή, να χρησιμοποιηθεί το IRMA σε συνδυασμό με το Keycloak και το FIDO που εφαρμόζονται στην πρώτη περίπτωση. Έτσι, θα έχουμε διασφαλίσει αφενός την πραγματική παρουσία του ίδιου του κατόχου της Ηλεκτρονικής Ταυτότητας, αφού θα πρέπει να ταυτοποιηθεί με το δαχτυλικό του αποτύπωμα, και αφετέρου την αποκάλυψη μόνο όσων στοιχείων του πολίτη χρειάζεται μία υπηρεσία της Ηλεκτρονικής Διακυβέρνησης και πάντα με την συγκατάθεσή του.

Μία, ακόμη, μελλοντική επέκταση ώστε να παρέχεται μία πιο ολοκληρωμένη υπηρεσία στο χρήστη είναι η δυνατότητα εγγραφής. Με την τωρινή υλοποίηση, ο πολίτης πρέπει να κάνει κάποιες γραφειοκρατικές διαδικασίες και να παρουσιαστεί

αυτοπροσώπως, ώστε να πιστοποιηθεί και να αποκτήσει η συσκευή του τα κατάλληλα πιστοποιητικά για να μπορεί να επιτύχει η επικοινωνία της με τον κάθε server του συστήματος, όταν ξεκινήσει να χρησιμοποιεί την Ηλεκτρονική Ταυτότητα. Αν υλοποιηθεί, θα υπάρχει αντίστοιχο κουμπί εγγραφής και θα ακολουθείται μία διαδικασία ηλεκτρονικής κατάθεσης/αποστολής δικαιολογητικών, καθώς και μία διαδικασία έκδοσης μοναδικών κωδικών όπου αφού εγκριθούν, θα δημιουργείται η ταυτότητα του πολίτη.

Τέλος, σημαντική προσθήκη για το μέλλον στη λειτουργικότητα που περιγράφηκε είναι η δυνατότητα υποστήριξης Ηλεκτρονικών Συναλλαγών. Έτσι, με την ύψιστη ασφάλεια που θα παρέχει η Ηλεκτρονική Ταυτότητα σχετικά με την απόδειξη της αυθεντικοποίησης ενός πολίτη, αλλά και με την δυνατότητα επιλογής των προσωπικών στοιχείων που θα εκτεθούν σε μία συναλλαγή, οι συναλλαγές θα περάσουν σε μία νέα εποχή. Η ασφάλεια, η εχεμύθεια, η διακριτικότητα και η μυστικότητα των συναλλαγών, συνάμα με τη διαφάνεια στις δοσοληψίες και στους συναλλασσόμενους θα συμβάλλουν στην καταπολέμηση της φοροδιαφυγής και άλλων οικονομικών απατών, καθώς θα δώσουν και ώθηση σε πολλούς τομείς του εμπορίου.

Καταλήγοντας, στην παρούσα διπλωματική εργασία παρουσιάστηκε μία αρχική έκδοση της Ηλεκτρονικής Ταυτότητας Πολίτη (eID), βγήκαν σημαντικά συμπεράσματα για τα εργαλεία που μπορούν να χρησιμοποιηθούν και προτάθηκαν μελλοντικές υλοποιήσεις και προσθήκες. Στη σύγχρονη εποχή και δεδομένων των ραγδαίων ρυθμών ανάπτυξης της τεχνολογίας, είναι απαραίτητη η υλοποίηση και η εφαρμογή ενός τέτοιου συστήματος που θα διευκολύνει τους πολίτες στις καθημερινές τους συναλλαγές με το δημόσιο τομέα, κρατώντας πάντα σε προτεραιότητα την τήρηση των υψηλότερων προδιαγραφών ασφάλειας του μοναδικού ταυτοποιητικού στοιχείου των πολιτών, της Ηλεκτρονικής τους Ταυτότητας.

Βιβλιογραφία

[1] EUR-lex, Ευρωπαϊκή Επιτροπή, "Ανακοίνωση της Επιτροπής προς το Συμβούλιο, το Ευρωπαϊκό Κοινοβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών - Ο ρόλος της ηλεκτρονικής διακυβέρνησης για το μέλλον της Ευρώπης", Σεπτέμβριος 2003, [Online]. Available at: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX%3A52003DC0567

[2] Α. Κουμιώτης (2010), "Η Ηλεκτρονική Διακυβέρνηση στην Ελλάδα"

[3] IDABC, Ευρωπαϊκή Επιτροπή, "European Commission > IDABC > The programme", [Online]. Available at: http://ec.europa.eu/idabc/en/chapter/3.html

[4] K. De Vriendt (2009), "Interoperability Solution for European Public Administrations, A Commission-driven EU programme (2010-2015)"

[5] EUR-lex, Ευρωπαϊκή Επιτροπή, "Έκτακτο Ευρωπαϊκό Συμβούλιο της Λισσαβόνας: προς την Ευρώπη της καινοτομίας και της γνώσης", Μάρτιος 2000, [Online]. Available at: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=LEGISSUM%3Ac10241

[6] EUR-lex, Ευρωπαϊκή Επιτροπή, "eEurope 2002", Μάρτιος 2001, [Online]. Available at: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=LEGISSUM%3Al24226a

[7] EUR-lex, Ευρωπαϊκή Επιτροπή, "eEurope 2005", Μάιος 2002, [Online]. Available at: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=LEGISSUM:l24226

[8] EUR-lex, Ευρωπαϊκή Επιτροπή, "i2010: η κοινωνία της πληροφορίας και τα μέσα ενημέρωσης στην υπηρεσία της ανάπτυξης και της απασχόλησης", Ιούνιος 2005, [Online]. Available at: https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=LEGISSUM:c11328&from=EN

[9] EUPAN, Ευρωπαϊκή Επιτροπή, "EU e-Government Action Plan 2011-2015", Απρίλιος 2013, [Online]. Available at: http://www.eupan.eu/files/repository/20130327174505_EU-e-Government_Action_Plan_2011-2015.ppt

[10] EUR-lex, Ευρωπαϊκή Επιτροπή, "Σχέδιο δράσης της ΕΕ για την ηλεκτρονική διακυβέρνηση 2016-2020", Απρίλιος 2016, [Online]. Available at: https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52016DC0179&from=EN

[11] INSPIRE, Ευρωπαϊκή Επιτροπή, "About INSPIRE", [Online]. Available at: https://inspire.ec.europa.eu/about-inspire/563

[12] Δ. Σπινέλλης, Ν. Βασιλάκης, Ν. Πουλούδη, Ν. Τσούμα, ΔιαΝΕΟσις, Οργανισμός Έρευνας & Ανάλυσης (2018), "Ηλεκτρονική Διακυβέρνηση στην Ελλάδα – Επιτυχίες, Προβλήματα και ο Δρόμος Προς τον Ψηφιακό Μετασχηματισμό"

[13] Ν. Πετροπούλου (2015), "Η Ηλεκτρονική Διακυβέρνηση στην Ελλάδα και την Ευρώπη"

[14] Ευρωπαϊκή Επιτροπή (2017), "Ευρωπαϊκό πλαίσιο διαλειτουργικότητας – Στρατηγική εφαρμογή"

[15] R. Baldoni (2009), "Federated Identity Management Systems in e-Government: the Case of Italy", Electronic Government, An International Journal

[16] Κ. Λαμπρόπουλος (2011), "Σχεδιασμός και υλοποίηση συστήματος διαχείρισης και ενοποίησης διαφορετικών ταυτοτήτων χρηστών σε δίκτυα νέας γενιάς", Διδακτορική Διατριβή

[17] Ε. Πόπη (2015), Η Διαχείριση των προσωπικών δεδομένων στην εποχή του διαδικτύου

[18] R. McKenzie, M. Crompton, C. Wallis (2008), “Use Cases for Identity Management in E-Government”, published by the IEEE Computer Society.
[19] General Data Protection Regulation – GDPR, [Online], Availiable at: https://gdpr-info.eu/
[20] Michael West, “Computer and Information Security Handbook”, part I: “Overview of System and Network Security: A Comprehensive Introduction”
[21] Samsung Galaxy S6 specifications, [Online], Availiable at: https://www.gsmarena.com/samsung_galaxy_s6-6849.php
[22] Android Authentication, [Online], Availiable at: https://source.android.com/security/authentication
[23] Android Gatekeeper, [Online], Availiable at: https://source.android.com/security/authentication/gatekeeper
[24] Android Fingerprint HAL, [Online], Availiable at: https://source.android.com/security/authentication/fingerprint-hal