Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
στα Πληροφοριακά και Επικοινωνιακά Συστήματα

Τεχνολογίες Ιδιωτικότητας σε εφαρμογές Ηλεκτρονικής Διακυβέρνησης

Ελευθερία Καραγιώργου

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Μάιος 2015

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Τεχνολογίες Ιδιωτικότητας σε εφαρμογές Ηλεκτρονικής Διακυβέρνησης

Ελευθερία Καραγιώργου

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στα Πληροφοριακά Συστήματα

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Μάιος 2015

Περίληψη

Τα τελευταία χρόνια η αυξανόμενη χρήση του διαδικτύου έχει οδηγήσει τις ανεπτυγμένες χώρες στην αύξηση των παρεχόμενων υπηρεσιών Ηλεκτρονικής Διακυβέρνησης, οι οποίες στην πλειοψηφία τους, παρέχουν στους πολίτες ηλεκτρονικά μέσα, για την ταυτοποίησή τους, όπως την ηλεκτρονική ταυτότητα ή κάρτα πολίτη και τα ηλεκτρονικά διαβατήρια. Όμως η χρήση αυτών των ηλεκτρονικών μέσων εγείρει ανησυχίες για την ιδιωτικότητα και την προστασία των προσωπικών δεδομένων των ατόμων. Γι' αυτό το λόγο υπάρχει έντονη ερευνητική δραστηριότητα με στόχο την ανάπτυξη τεχνολογιών που ενισχύουν και προστατεύουν την ιδιωτικότητα και τα προσωπικά δεδομένα. Σε αυτήν την κατεύθυνση, η τεχνολογία των Πιστοποιητικών βάσει χαρακτηριστικών (Attribute Based Credentials-ABC) θεωρείται πολλά υποσχόμενη και μπορεί να προσφέρει σημαντική προστασία στην ιδιωτικότητα του ατόμου κατά τις ηλεκτρονικές του συναλλαγές με υπηρεσίες του Δημόσιου Τομέα.

Η παρούσα διατριβή μελετά υπηρεσίες ηλεκτρονικής διακυβέρνησης από τη σκοπιά της ιδιωτικότητας. Στο πλαίσιο αυτό, παρουσιάζονται οι τεχνολογικές προσεγγίσεις για τα ηλεκτρονικά διαβατήρια, τις ηλεκτρονικές ταυτότητες και τη χρήση της τεχνολογίας ABC, λαμβάνοντας υπόψη το υπάρχον νομικό πλαίσιο προστασίας προσωπικών δεδομένων που διέπει τα κράτη - μέλη της Ε.Ε. και ιδίως την Ελλάδα. Επιπλέον, δεδομένου ότι στην Ελλάδα δεν έχει ακόμα αναπτυχθεί η λεγόμενη ηλεκτρονική κάρτα πολίτη, πραγματοποιήθηκε έρευνα για την σημασία που δίνουν οι πολίτες στην έννοια της ιδιωτικότητας κατά την χρήση υπηρεσιών Ηλεκτρονικής Διακυβέρνησης, για το αν γνωρίζουν την τεχνολογία των Attribute - Based Credentials και κατά πόσο είναι έτοιμοι να την δεχτούνε στις καθημερινές τους συναλλαγές με υπηρεσίες του Δημόσιου Τομέα.

Summary

During the last years, the augmented use of Internet has lead the developed countries to the increase of the e-government services. Many of the provided services necessitate electronic means for the identification of citizens, such as the electronic identity or citizen card and the e-passports. Nevertheless, the use of such electronic means raises concerns about the privacy and the protection of personal data of individuals. Hence, ongoing research focuses on developing appropriate technological solutions for strengthening the protection of privacy and personal data. Towards this direction, the technology of Attribute based Credentials (ABC) is considered to be very promising and can offer significant protection to the individual's privacy during his electronic transactions with e-government services.

This thesis studies the identification and authentication techniques in e-government services, under the framework of the fundamental right of personal data protection. More precisely, e-passports, electronic identities and Attribute based Credentials technology are examined, with emphasis to the protection of individual's privacy, according to the existing legal framework in European Union (and especially in Greece). Benefits and drawbacks of each of the adopted solutions are analyzed, in terms of the privacy issues that arise. Moreover, since electronic identities in Greece are still in its infancy, a survey has been developed towards estimating whether citizens are appropriately aware of privacy risks in their use of e-government services, as well as to conclude whether privacy-friendly techniques such as Attribute based Credentials are being considered as acceptable solution or not.

Ευχαριστίες

Θα ήθελα να αποδώσω τις θερμές μου ευχαριστίες στον Επιβλέποντα καθηγητή μου κ. Λιμνιώτη Κωνσταντίνο για την καθοδήγηση που μου παρείχε και για την άψογη συνεργασία που είχαμε τόσο κατά την διάρκεια της εκπόνησης της μεταπτυχιακής μου διατριβής, όσο και στο μάθημα της Κρυπτογραφίας.

Δεν θα μπορούσα να μην ευχαριστήσω τον σύζυγό μου και την κόρη μου για την απεριόριστη αγάπη και κατανόηση που έδειξαν καθ' όλη την διάρκεια των σπουδών μου στο ΑΠΚΥ.

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Ένα από τα μεγάλα πλεονεκτήματα που παρέχει το Διαδίκτυο είναι η ανάπτυξη τεχνολογιών οι οποίες διευκολύνουν την ηλεκτρονική πρόσβαση οπουδήποτε και οποτεδήποτε. Οι ηγεσίες πολλών χωρών έχουν εκτιμήσει αυτό το φαινόμενο και πολλές από αυτές ήδη προσφέρουν υπηρεσίες ηλεκτρονικής διακυβέρνησης, στις οποίες οι πολίτες έχουν πρόσβαση ηλεκτρονική, χωρίς να χρειάζεται να συναλλαγούν με κάποιον υπάλληλο. Ωστόσο, η Ηλεκτρονική Διακυβέρνηση δεν σχετίζεται με την παροχή "παραδοσιακών" υπηρεσιών σε ηλεκτρονική μορφή. Η τεχνολογία είναι απλώς το εργαλείο.

Ο όρος "Ηλεκτρονική Διακυβέρνηση" (εφεξής Η.Δ.) προέρχεται από την μετάφραση των αντίστοιχων αγγλικών λέξεων "Electronic Government" ή αλλιώς "Digital Government". Παρόλα αυτά δεν πρέπει να

συγχέεται ο όρος "ηλεκτρονικός" ή αλλιώς "ψηφιακός" με την απλή εφαρμογή της πληροφορικής στη Δημόσια Διοίκηση.

Σήμερα η Η.Δ. έχει καταστεί απαραίτητο εργαλείο στην αναμόρφωση της Δημόσιας Διοίκησης, επαυξάνοντας τον βαθμό ικανοποίησης των πολιτών, όσον αφορά την ποιότητα των υπηρεσιών και δημιουργεί μια πιο ευέλικτη και διαφανή Δημόσια Διοίκηση. Η υλοποίησή της στηρίζεται στην ανάπτυξη στρατηγικού σχεδιασμού, ο οποίος θα πρέπει να προωθεί συγκεκριμένους στόχους. Σύμφωνα με την Ευρωπαϊκή Επιτροπή [01], οι σημαντικότεροι στόχοι είναι η επίτευξη της διαφάνειας, η καθολική παροχή υπηρεσιών και ο γενικότερος μετασχηματισμός του δημόσιου τομέα. Η επίτευξη των στόχων αυτών κρίνει και την αποτελεσματικότητα του κράτους, τόσο σε επίπεδο εσωτερικής διοίκησης και οργάνωσης, όσο και σε ότι αφορά την παροχή υπηρεσιών προς τον χρήστη.

Όσο, όμως, ο αριθμός των παρεχόμενων υπηρεσιών αυξάνεται, απαιτείται και υψηλότερο επίπεδο Ασφάλειας (security) των δεδομένων και Ιδιωτικότητας (privacy). Ο κίνδυνος για την ασφάλεια αυξάνει τόσο λόγω της κρισιμότητας των συστημάτων και των υπηρεσιών, όσο και λόγω των πληροφοριών που είναι αντικείμενα συλλογής και επεξεργασίας. Ειδικά το δεύτερο θέτει ζητήματα προστασίας προσωπικών δεδομένων, η οποία είναι στενά συνυφασμένη με την προάσπιση της ιδιωτικότητας: οι παρεχόμενες υπηρεσίες Η.Δ. θα πρέπει να μη θέτουν σε κίνδυνο τα προσωπικά δεδομένα των πολιτών (είτε αυτά είναι ευαίσθητα είτε όχι), όχι μόνο για να ενισχυθεί η εμπιστοσύνη των πολιτών ως προς αυτές τις υπηρεσίες αλλά και για τη συμμόρφωση με το σχετικό νομικό πλαίσιο.

1.1. Η έννοια της Ηλεκτρονικής Διακυβέρνησης

Σύμφωνα με τον ορισμό που δίνει η Ευρωπαϊκή Επιτροπή, *Ηλεκτρονική Διακυβέρνηση (E-Government) είναι η χρήση των Τεχνολογιών της Πληροφορικής και των Τηλεπικοινωνιών στη Δημόσια Διοίκηση, σε συνδυασμό με οργανωτικές αλλαγές και νέες δεξιότητες του προσωπικού, με σκοπό την βελτίωση της εξυπηρέτησης του κοινού, την ενδυνάμωση της δημοκρατίας και την υποστήριξη των δημόσιων πολιτικών.*[02]

Στην πράξη, Η.Δ. σημαίνει μια νέα πολιτισμική αντίληψη, έναν σαφή και ριζοσπαστικό μετασχηματισμό, κατά τον οποίο οι οργανισμοί της δημόσιας διοίκησης επιστρατεύουν τις δυνατότητες που τους παρέχει η ανάπτυξη της ηλεκτρονικής τεχνολογίας, ώστε να βελτιώσουν τη διαθεσιμότητα, την ποιότητα και τη διαφάνεια λειτουργίας των δημόσιων υπηρεσιών, όπως επίσης και να περικόψουν το κόστος τους. Αυτό έρχεται σε άμεση αντίθεση με τις συνήθεις ανακριβείς αντιλήψεις περί της Η.Δ. και συγκεκριμένα με το γεγονός ότι ο επιθετικός προσδιορισμός "ηλεκτρονική" υπονοεί απλά τη χρήση των υπολογιστικών συστημάτων και λογισμικού.

Σύμφωνα με την πρωτοβουλία της Επιτροπής, η Η.Δ. είναι:

1. *Ανοιχτή και διαφανής διαδικασία (transparent)*. Η Δημόσια Διοίκηση καθίσταται ικανή να ανταποκριθεί στις προσδοκίες των πολιτών και είναι υπόλογη και δεκτική ως προς την δημοκρατική συμμετοχή.

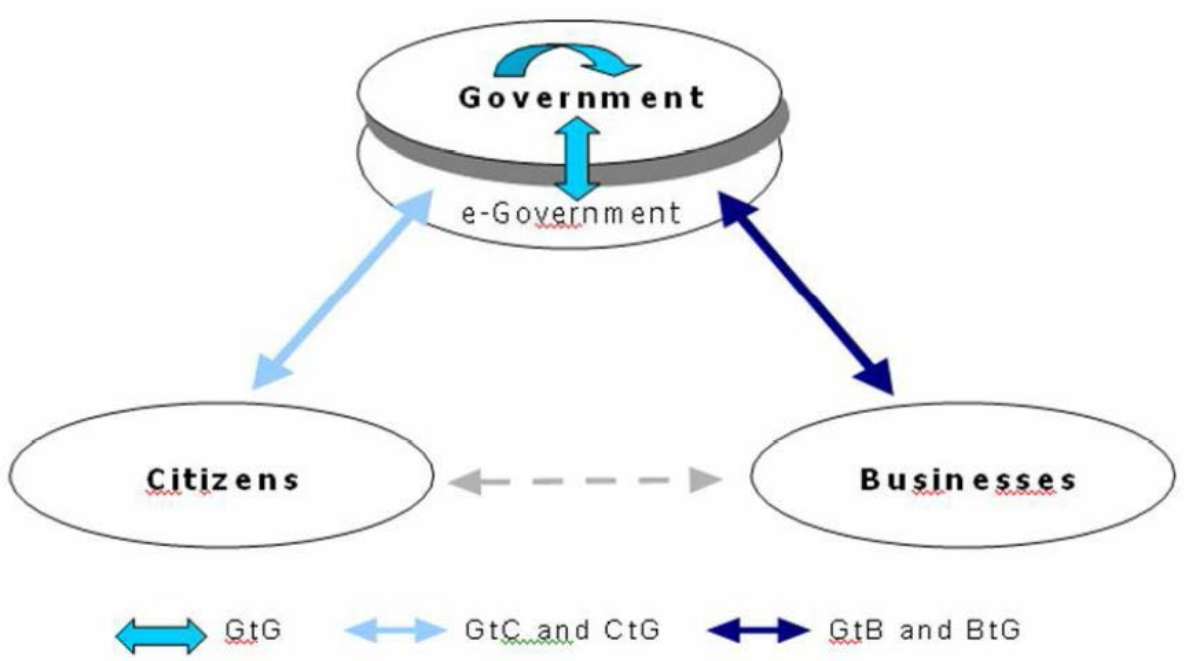
2. *Ανοιχτή σε όλους τους πολίτες (accessible, participatory, responsible, responsive)*. Η Δημόσια Διοίκηση με επίκεντρο τον χρήστη, θα πρέπει να παρέχει σε όλους ανεξαιρέτως εξατομικευμένες υπηρεσίες.

3. *Αποδοτική Δημόσια Διοίκηση (efficient & effective)*, η οποία λειτουργεί με γνώμονα την όσο γίνεται αποδοτικότερη χρήση των χρημάτων των φορολογούμενων, εξοικονομώντας χρόνο και κόστος.[03]

Ηλεκτρονική Διακυβέρνηση[04]

1.1.1. Μορφές Ηλεκτρονικής Διακυβέρνησης

Τα εμπλεκόμενα μέλη στην Η.Δ., τα οποία και καθορίζουν τις μορφές της, είναι οι πολίτες (Citizen), οι επιχειρήσεις (Business) και η ίδια η Δημόσια Διοίκηση με τους φορείς της (Government).



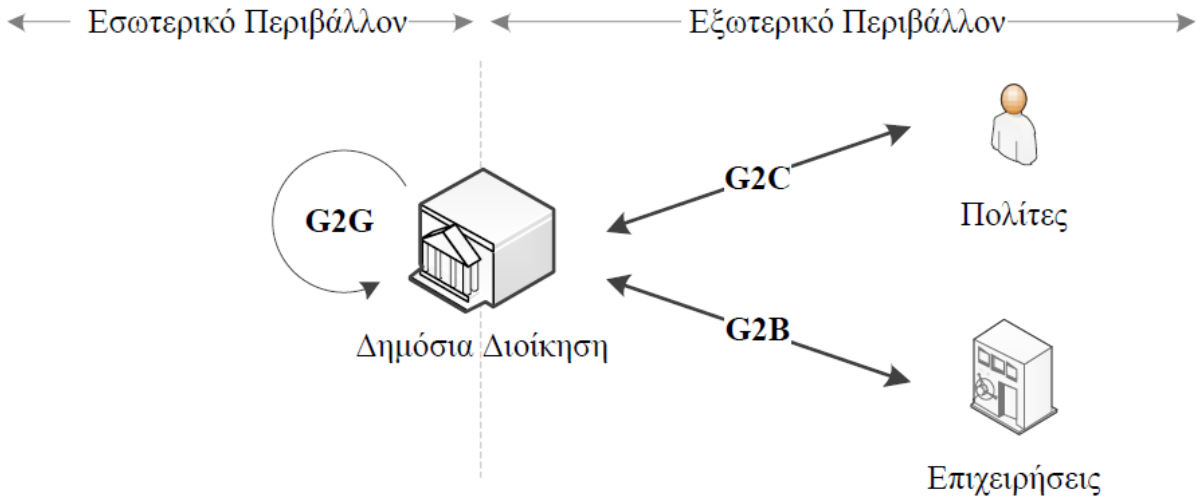
Μορφές Ηλεκτρονικής Διακυβέρνησης

Άρα, ανά ζεύγη, οι μορφές των συναλλαγών στην Η.Δ. μπορεί να είναι:

- *Δημόσιες υπηρεσίες προς Δημόσιες Υπηρεσίες (Government to Government, G2G*): Περιλαμβάνει την ηλεκτρονική ανταλλαγή πληροφοριών ανάμεσα στις διάφορες υπηρεσίες του Δημόσιου Τομέα.
- *Δημόσιες υπηρεσίες προς Επιχειρήσεις (Government to Business, G2B)*: Περιλαμβάνει την ηλεκτρονική ανταλλαγή πληροφοριών ανάμεσα σε υπηρεσίες του Δημόσιου Τομέα και σε επιχειρήσεις του Ιδιωτικού Τομέα, όπως την καταβολή προμήθειας στην αντίστοιχη Δημόσια Υπηρεσία.
- *Δημόσιες υπηρεσίες προς Πολίτες (Government to Citizen, G2C):* Περιλαμβάνει την συναλλαγή μεταξύ των πολιτών και των Δημόσιων Υπηρεσιών, όπως την ηλεκτρονική κατάθεση της φορολογικής δήλωσης στην υπηρεσία TAXISNET.

Οι μορφές του G2B και G2C χαρακτηρίζονται ως εξωτερικό περιβάλλον ηλεκτρονικής διακυβέρνησης *(external e-government),* ενώ η μορφή G2G χαρακτηρίζεται ως εσωτερικό περιβάλλον ηλεκτρονικής διακυβέρνησης *(internal e-government)*.[05]

Στο παρακάτω σχήμα φαίνεται αυτός ο διαχωρισμός:



Διαχωρισμός εσωτερικού και εξωτερικού περιβάλλοντος Η.Δ.

1.1.2. Πλεονεκτήματα Ηλεκτρονικής Διακυβέρνησης

Σύμφωνα με τον Szilard Molnar[03], με βάση την εμπειρία των ειδικών, η επιτυχία της Η.Δ. εξαρτάται από την τεχνολογία κατά ένα ποσοστό μόλις 20% , από την αναδόμηση των διαδικασιών από την πλευρά του παρόχου κατά 35% και κατά 40% από την διάθεση της διοίκησης.

Ωστόσο, δεν γίνεται να μην αναφερθούν τα πλεονεκτήματα της Η.Δ. τα οποία είναι:

- Η παροχή και η ποιότητα των πληροφοριών βελτιώνεται, αφού πλέον ψηφιοποιούνται και δεν απαιτείται η χειρόγραφη καταχώρηση των δεδομένων. Επιπλέον, παρέχεται διαλειτουργικότητα μεταξύ των βάσεων δεδομένων των διαφόρων δημόσιων υπηρεσιών και προσφέρεται καταμερισμός των πληροφοριών ώστε να αποφεύγεται ο κατ' επανάληψη εφοδιασμός με τα ίδια έγγραφα.

- Ο χρόνος διεκπεραίωσης μειώνεται λόγω αυτής της ψηφιοποίησης της πληροφορίας και των εγγράφων και τα ζητούμενα έγγραφα μπορούν να είναι πιο γρήγορα διαθέσιμα στους πολίτες.

- Ο διοικητικός φόρτος μειώνεται καθώς και ο φόρτος απασχόλησης των πολιτών, αφού στις περισσότερες περιπτώσεις το μόνο που χρειάζεται να κάνουν είναι να περιηγηθούν στην ηλεκτρονική φόρμα.

- Το κόστος μπορεί να μειωθεί, αν και δεν γίνεται εύκολα αντιληπτό. Τα κύρια οφέλη εξοικονόμησης κόστους μπορεί να μεταφράζονται σε λιγότερες ώρες εργασίας, μείωση εργατικού δυναμικού, χρήση ηλεκτρονικής επικοινωνίας - που είναι φθηνότερη από την παραδοσιακή μέθοδο.

- Γίνεται δυνατή η υλοποίηση υπηρεσιών υψηλότερου επιπέδου με δυνατότητα διαχείρισης εξατομικευμένων περιπτώσεων.

- Προώθηση της συμμετοχής των πολιτών στην διακυβέρνηση καθώς δίνεται η δυνατότητα συμμετοχής τους σε αντιπαραθέσεις (debates), σε συζητήσεις και σε ηλεκτρονικές ψηφοφορίες (Internet Voting).

- Μείωση της διαφθοράς και του πελατειακού καθεστώτος που χαρακτήριζε στο παρελθόν τις Δημόσιες Υπηρεσίες.

- Γεφύρωση του ψηφιακού χάσματος μέσω της εύκολης πρόσβασης στις Νέες Τεχνολογίες που προσφέρει η Ηλεκτρονική Διακυβέρνηση με υπηρεσίες της, όπως την Ηλεκτρονική Μάθηση (e-learning).

1.1.3. Διαλειτουργικότητα Ηλεκτρονικής Διακυβέρνησης

Διαλειτουργικότητα (interoperability) είναι η δυνατότητα ανταλλαγής και χρήσης της πληροφορίας με ενιαίο και αποτελεσματικό τρόπο από διαφορετικούς οργανισμούς και πληροφοριακά συστήματα της Δημόσιας Διοίκησης και αποτελεί βασικό χαρακτηριστικό και απαιτούμενο των υπηρεσιών Η.Δ.[06]

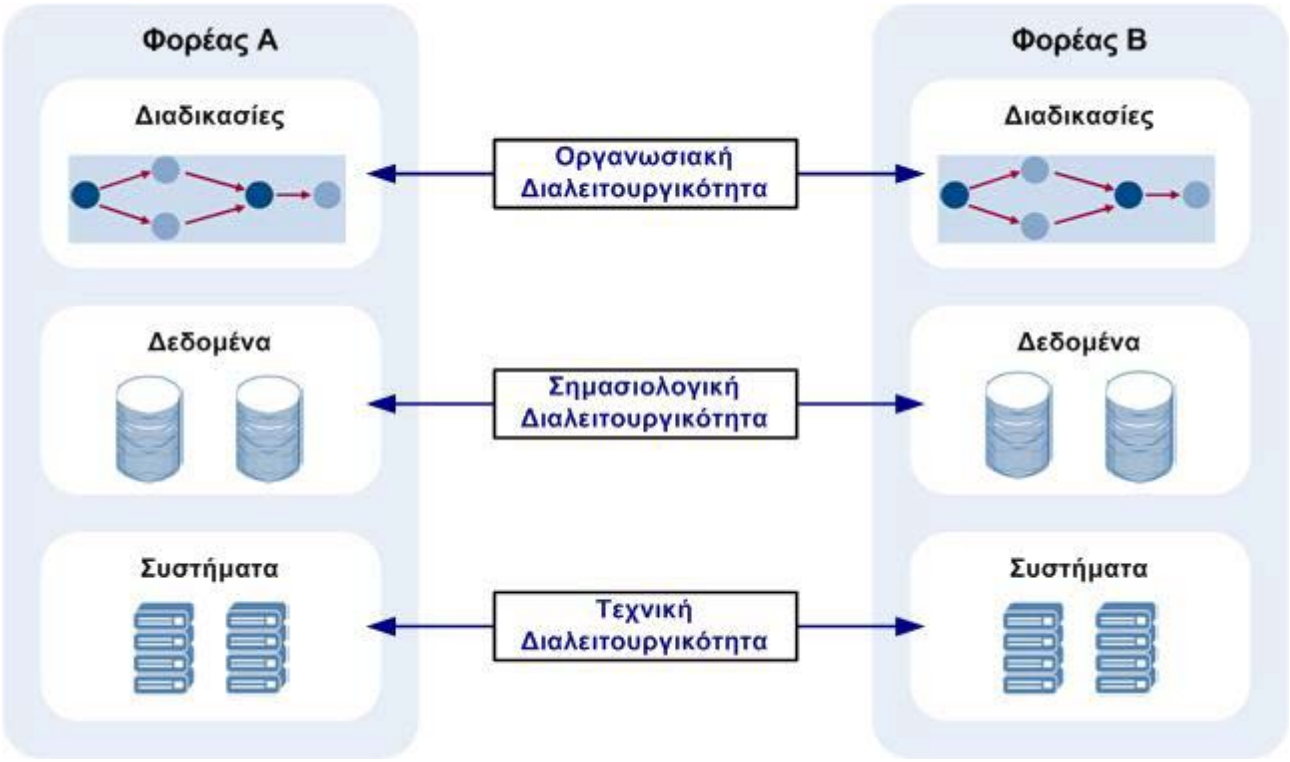
Ένας άλλος ορισμός που δίνεται από την ISO-IEC 2382-01, Information Technology Vocabulary Fundamental Terms [07], για την διαλειτουργικότητα, την περιγράφει ως "*η ικανότητα επικοινωνίας εκτέλεσης ή μεταφοράς δεδομένων μεταξύ διάφορων λειτουργικών μονάδων με έναν τρόπο ο οποίος απαιτεί λίγη ή καθόλου γνώση από τον χρήστη όσον αφορά τα μοναδικά χαρακτηριστικά αυτών των μονάδων*".

Οφέλη της Διαλειτουργικότητας:

1. Εξυπηρέτηση και ικανοποίηση διοικητικών πληροφοριακών αναγκών
2. Ανταλλαγή Δεδομένων
3. Συμμετοχή στη Διοίκηση

Η Διαλειτουργικότητα αναλύεται υπό τρία διαφορετικά πρίσματα:

- την *Οργανωσιακή Διαλειτουργικότητα,* η οποία αναφέρεται στον καθορισμό στόχων τη διαμόρφωση διαδικασιών και την επίτευξη συνεργασίας των φορέων που επιδιώκουν ανταλλαγή πληροφοριών. Επιπλέον, στοχεύει στην ικανοποίηση των χρηστών προσφέροντας υπηρεσίες αναγνωρίσιμες, προσβάσιμες και επικεντρωμένες στις ανάγκες του χρήστη.
- τη *Σημασιολογική Διαλειτουργικότητα*, η οποία διασφαλίζει την ακριβή σημασία των ανταλλασσόμενων πληροφοριών και επιτυγχάνεται ορίζοντας και υιοθετώντας κοινό λεξιλόγιο και ορισμούς σε όλα τα συστήματα και τις υπηρεσίες.
- την *Τεχνική Διαλειτουργικότητα*, η οποία ορίζεται ως η ικανότητα μεταφοράς και χρησιμοποίησης της πληροφορίας με ομοιογενή και αποτελεσματικό τρόπο μεταξύ των συστημάτων πληροφορικής των οργανισμών. Η Τεχνική Διαλειτουργικότητα αντιπροσωπεύει την διαλειτουργικότητα των υποδομών και του λογισμικού [08].



Διαστάσεις και Επίπεδα Διαλειτουργικότητας, Πηγή: http://blog.ots.gr/tag/%CE%B4%CE%B9%CE%B1%CE%BB%CE%B5%CE%B9%CF%84%CE%BF%CF%85%CF%81%CE%B3%CE%B9%CE%BA%CF%8C%CF%84%CE%B7%CF%84%CE%B1/#.VSZuaJMTSYw

Στην Ελλάδα, είναι σε ισχύ το *ΠΔΥΗΣ* (Πλαίσιο Διαλειτουργικότητας & Υπηρεσιών Ηλεκτρονικών Συναλλαγών) [09] το οποίο παρέχει τις τεχνικές προδιαγραφές που μπορούν να υιοθετηθούν στον Ελληνικό Δημόσιο Τομέα και να καλύψουν τις τοπικές ανάγκες.

Στην Ευρωπαϊκή Ένωση υπάρχει το *Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας (EIF-European Interoperability Framework*) [10] το οποίο είναι ένα σύνολο κατευθύνσεων εγγράφων και πρωτοβουλιών υπό την αιγίδα του προγράμματος IDABC (Interoperable Delivery of European e-Government Services to Public Administrations, Businesses and Citizens) και συμπληρώνει τα διάφορα Εθνικά Πλαίσια Διαλειτουργικότητας σε πανευρωπαϊκή διάσταση.

1.2. Η έννοια της Ιδιωτικότητας (Privacy)

Η Ιδιωτικότητα αποτελεί μία έννοια για την οποία δύσκολα μπορεί να δοθεί ένας ορισμός που να την καλύπτει απόλυτα: σύμφωνα και με τον Alan Westin, πρωτεργάτη του πεδίου, "*τα θέματα Ιδιωτικότητας είναι εκ θεμελίων ζητήματα αξιών, συμφερόντων και εξουσίας*", ενώ ο Fernando Volio Jimenez επισήμανε ότι "*με κάποια έννοια, όλα τα ανθρώπινα δικαιώματα είναι πτυχές του δικαιώματος στην Ιδιωτικότητα*" [11].

Άλλοι επιστήμονες υποστήριξαν ότι η ιδιωτικότητα είναι μια άκρως σημαντική ανθρώπινη αξία για την έκφραση της ηθικής και της κοινωνικής πλευράς του ανθρώπου, ενώ παρά τη δυσκολία στο να δοθεί ένας συγκεκριμένος ορισμός, οι ιδιότητές της μπορούν να συνοψιστούν στις εξής παρακάτω:

- Το δικαίωμα του ανθρώπου να μπορεί οποτεδήποτε να έχει πρόσβαση στις πληροφορίες που αφορούν το άτομό του.
- Το μέγεθος του ελέγχου που έχει το άτομο στις πληροφορίες που αφορούν το άτομό του.
- Το επίπεδο περιορισμού πρόσβασης στις ιδιωτικές πληροφορίες του ατόμου.

Συμπερασματικά, δεν μπορούμε να παραβλέψουμε την σπουδαιότητα και την σημαντικότητά της, αλλά και την ιδιαιτερότητά της. Άρα, θα πρέπει να την προστατέψουμε σε όλες τις μορφές της, είτε την παραδοσιακή, είτε την ψηφιακή, αφού θεωρείται πλέον θεμελιώδες δικαίωμα στη Χάρτα Θεμελιωδών Δικαιωμάτων.

1.2.1. Εμφάνιση και εξέλιξη της Ιδιωτικότητας

Ιστορικά, η ιδιωτικότητα έκανε για πρώτη φορά την εμφάνισή της πριν από περίπου 2.500 χρόνια στην αρχαία Ελλάδα, και πιο συγκεκριμένα στο βιβλίο του με τίτλο "Πολιτικά", ο αρχαίος φιλόσοφος Αριστοτέλης κάνει έναν ξεκάθαρο διαχωρισμό μεταξύ των δημοσίων θεμάτων του δήμου που απασχολούν όλους του πολίτες και των ιδιωτικών θεμάτων που απασχολούν τα άτομα σε σχέση με το σπίτι τους και την οικογένειά τους.

Στη συνέχεια, οι Ρωμαίοι εξέλιξαν την σημασία της ιδιωτικότητας ακόμα περισσότερο, διαχωρίζοντας την κοινωνική από την ιδιωτική ζωή του ρωμαίου πολίτη και για πρώτη φορά αναφέρονται ξεκάθαρα οι όροι "δημόσιος βίος" και "ιδιωτικός βίος". Λόγω της μεγάλης απήχησης που είχανε αυτοί οι όροι στην ρωμαϊκή κοινωνία, ο αυτοκράτορας Ιουστινιανός αποφάσισε να τις συμπεριλάβει στο ρωμαϊκό δίκαιο το 533 μ.Χ.

Στην σύγχρονη ιστορία, στα τέλη του 19ου αιώνα, ο όρος ιδιωτικότητα (privacy) έκανε την επανεμφάνισή του,-μετά από σιγή αιώνων- πρώτη φορά, στο αμερικάνικο δίκαιο, μετά από δημοσίευση των Warren και Brandeis το 1890 [12] για το δικαίωμα "*να μείνει κανείς μόνος του*" -λόγω των κινδύνων που εγκυμονούσε η νέα, τότε, τεχνολογία λήψης φωτογραφιών- ενώ στη συνέχεια εμφανίστηκε στο αγγλοσαξονικό δίκαιο. Ο όρος "ιδιωτικότητα", σύμφωνα με την αμερικάνικη νομολογία, είναι αποσυνδεδεμένος από την ιδιωτική ζωή, λειτουργώντας ως θεμέλιο επιμέρους δικαιωμάτων που, όμως, δεν συνδέονται αναγκαία με την στενή ιδιωτικότητα του πολίτη. Αντίθετα, με πολύ συγκεκριμένο τρόπο, χρησιμοποιείται αυτός ο όρος στις ευρωπαϊκές νομοθεσίες, όπου έχει επικρατήσει η απόλυτη ταύτισή του με το δικαίωμα στην ιδιωτική ζωή.

Χαρακτηριστικό της διαφοράς στην αντιμετώπιση της ιδιωτικότητας ανάμεσα στην Ευρώπη και στις Η.Π.Α., είναι οι δυσκολίες που συνάντησαν αρκετές αμερικάνικες επιχειρήσεις να δραστηριοποιηθούν στην Ευρώπη, με αποτέλεσμα να δημιουργηθεί, το

2000, ένας προαιρετικός κατάλογος αμερικάνικων επιχειρήσεων, γνωστός ως "Safe Harbor" (Ασφαλής Λιμένας), οι οποίες εναρμόνισαν τις λειτουργίες τους με βάση τις ρυθμίσεις του ευρωπαϊκού δικαίου σε θέματα ιδιωτικότητας. [13] Οι επιχειρήσεις αυτές οφείλουν να δηλώνουν εγγράφως και σε ετήσια βάση την συμμόρφωσή τους, ενώ το αμερικάνικο Υπουργείο Εμπορίου οφείλει να δημοσιοποιεί αυτόν τον κατάλογο.

1.2.2. Πληροφοριακή Ιδιωτικότητα

Ωστόσο, οι εξελίξεις στην πληροφορική τεχνολογία έχουν ως συνέπεια να μην υπάρχει όριο στην πληροφορία που μπορεί να καταχωριστεί, ενώ οι δυνατότητες εκμετάλλευσης της πληροφορίας μοιάζουν απεριόριστες. [14] Συνεπώς, παραμένει κρίσιμο το θέμα της προστασίας της ιδιωτικής ζωής και της προστασίας των προσωπικών δεδομένων.

Η τεχνολογική έκρηξη των τελευταίων δεκαετιών ανέδειξε την Ιδιωτικότητα μέσα στην Κοινωνία της Πληροφορίας, η οποία ονομάζεται *Πληροφοριακή Ιδιωτικότητα* (Informational Privacy), ή *Ιδιωτικότητα της Πληροφορίας* (Information Privacy) και η οποία περιλαμβάνει τη θέσπιση κανόνων που διέπουν τη συλλογή και την επεξεργασία δεδομένων προσωπικού χαρακτήρα, όπως κυβερνητικά δεδομένα, ιατρικά δεδομένα και οικονομικά δεδομένα. Αυτήν την πτυχή την αποκαλούμε και "Προστασία Προσωπικών Δεδομένων" [15].

1.2.3. Χαρακτηριστικά της Ιδιωτικότητας

Οι ακόλουθες ιδιότητες μπορούν να χρησιμοποιηθούν ως μέσα προάσπισης της ιδιωτικότητας [16]:

1. η *Ανωνυμία* (Anonymity) που σημαίνει ότι μία οντότητα δεν είναι αναγνωρίσιμη και εξασφαλίζεται η μη αποκάλυψη της ταυτότητας της κατά την πρόσβασή της στα δεδομένα.
2. η *Μη - Συνδεσιμότητα* (Unlinkability), η οποία εξασφαλίζει ότι η οντότητα μπορεί να αποκτήσει πρόσβαση σε διαφορετικά δεδομένα, χωρίς να είναι εφικτή η σύνδεση αυτών των γεγονότων από τρίτους.
3. η *Μη - Ανιχνευσιμότητα* (Undetectability), η οποία είναι η επιθυμητή ιδιότητα μιας οντότητας να αποκρύψει δεδομένα της, οπότε και αυτά να μην ανιχνεύονται από τρίτους.
4. η *Ψευδωνυμία* (Pseudonymity), η οποία αποτελεί την απόκρυψη του πραγματικού ονόματος μιας οντότητας, αντικαθιστώντας το με ένα άλλου τύπου προσδιοριστικό.
5. η *Διαχείριση Ταυτότητας* (Identity Management) που αναφέρεται στην διαχείριση μερικών ταυτοτήτων συγκεκριμένου προσώπου και η επιλογή της κατάλληλης ταυτότητας βασίζεται στην εκάστοτε κατάσταση στην οποία δρα το συγκεκριμένο πρόσωπο.

Η προστασία της Ιδιωτικότητας είναι ένα ζήτημα που πρέπει να επιλύεται με τεχνολογικά μέσα. Η υποστήριξη των Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας (Privacy Enhancing Technologies, PETs) είναι απαραίτητη για να ενισχυθεί η Ιδιωτικότητα και να υποβοηθηθεί η εφαρμογή των κανόνων Προστασίας Προσωπικών Δεδομένων σε συνδυασμό με την εφαρμογή της αντίστοιχης νομοθεσίας.

1.2.4. Απαιτήσεις Ιδιωτικότητας

Για την μετατροπή της Ιδιωτικότητας από μία γενική έννοια σε τεχνική απαίτηση ορίσθηκαν οι εξής επιμέρους απαιτήσεις της Ιδιωτικότητας:

- *Αυθεντικοποίηση*: η διαδικασία διά της οποίας επιβεβαιώνεται η ταυτότητα ενός χρήστη. Σε ιδιωτικά και δημόσια δίκτυα, η αυθεντικοποίηση υλοποιείται, συνήθως, με την χρήση κωδικών πρόσβασης.
- *Εξουσιοδότηση*: η διαδικασία μέσω της οποίας ένας χρήστης αποκτά δικαιώματα σε μία ηλεκτρονική υπηρεσία. Σε ένα πληροφοριακό σύστημα όπου υπάρχουν πολλοί χρήστες, ο διαχειριστής του συστήματος φροντίζει να εξουσιοδοτεί τον καθένα με τα αντίστοιχα δικαιώματα, ανάλογα με τον ρόλο και τις υποχρεώσεις στο σύστημα.
- *Αναγνώριση*: η διαδικασία ελέγχου αν τα δεδομένα που ζητούνται απαιτούν αυθεντικοποίηση και στη συνέχεια εξουσιοδότηση ή όχι. Επίσης, η διαδικασία αναγνώρισης φροντίζει να μην επιτραπεί σε κανέναν μη εξουσιοδοτημένο χρήστη η πρόσβαση σε αυτά τα δεδομένα, προφυλάσσοντας έτσι την ιδιωτικότητα των κατόχων τους.
- *Προστασία Δεδομένων*: η συμμόρφωση με το υφιστάμενο νομικό πλαίσιο, δηλαδή, όσον αφορά τα κράτη- μέλη της Ευρωπαϊκής Ένωσης, με την Ευρωπαϊκή Οδηγία 95/46/ΕΚ (όπως αυτήν έχει ενσωματωθεί στα κράτη- μέλη) που αφορά την επεξεργασία των προσωπικών δεδομένων και την ελεύθερη διακίνησή τους.
- *Ανωνυμία*: σύμφωνα με την Fischer-Hubner [17] η διαδικασία με την οποία "*ένας χρήστης μπορεί να χρησιμοποιήσει μία διαδικασία ή να επικοινωνήσει μέσω διαδικτύου χωρίς να αποκαλύψει την ταυτότητά του*".
- *Ψευδωνυμία*: σύμφωνα με την Fischer-Hubner [17] "*η απαίτηση που διασφαλίζει την απόκρυψη της ταυτότητας ενός χρήστη όταν αυτός ενεργεί στα πλαίσια μιας επικοινωνίας χρησιμοποιώντας ένα ή*

περισσότερα ψευδώνυμα. Η ψευδωνυμία υλοποιείται όταν δεν μπορεί να υλοποιηθεί η ανωνυμία".

- *Μη-συνδεσιμότητα*: η διαδικασία η οποία εξασφαλίζει ότι ο χρήστης μπορεί να αποκτήσει πρόσβαση σε δεδομένα χωρίς να είναι εφικτή η σύνδεση αυτών των γεγονότων από τρίτους.
- *Μη-Ανιχνευσιμότητα*: η διαδικασία κατά την οποία είναι επιθυμία του χρήστη να αποκρύψει δεδομένα του, οπότε και αυτά να μην ανιχνεύονται από τρίτους.

1.2.5. Πολιτική Ιδιωτικότητας (Privacy Policy)

Πολλοί ιστότοποι αναγράφουν στην αρχική τους σελίδα την πολιτική ιδιωτικότητας που ακολουθούν, η οποία αποτελεί ένα είδος υπόσχεσης της επιχείρησης ότι θα επεξεργαστεί τα δεδομένα των χρηστών του ιστοτόπου της με συγκεκριμένο τρόπο. Η πολιτική ιδιωτικότητας αποτελεί ένα μέσο προστασίας της ιδιωτικότητας των χρηστών, διότι τούς παρέχεται ενημέρωση για το ποια προσωπικά δεδομένα τους θα επεξεργαστούν και με ποιον τρόπο (που και πώς θα χρησιμοποιηθούν και αν θα δοθούν σε τρίτους ή όχι).

Παρά τις προσπάθειες ανάπτυξης εμπιστοσύνης των εταιρειών με τους χρήστες τους, οι πολιτικές ιδιωτικότητας παρουσιάζουν κάποια μειονεκτήματα [18]:

1. Ο χρήστης διαβάζει την πολιτική ιδιωτικότητας που διέπει τον ιστότοπο της συγκεκριμένης εταιρίας και αποφασίζει, εφόσον συμφωνεί, να επιτρέψει την χρήση των προσωπικών του δεδομένων από την εταιρία.
2. Η πολιτική ιδιωτικότητας μπορεί να αλλάξει ανά πάσα στιγμή, οπότε πρέπει να υπάρχει κάποιος μηχανισμός από τη μεριά της εταιρίας για ενημέρωση των χρηστών, μιας και η προστασία των προσωπικών τους δεδομένων δεν είναι πλέον δεδομένη με τον τρόπο που γνωρίζανε.

3. Σε περίπτωση μη τήρησης της πολιτικής ιδιωτικότητας από την εταιρία, δεν υπάρχει τρόπος ο χρήστης να ενημερωθεί γι' αυτό, παρά μόνο αν το εντοπίσει μόνος του, πράγμα πολύ δύσκολο. Άρα, η τήρηση της πολιτικής ιδιωτικότητας βασίζεται στην εμπιστοσύνη και στην αξιοπιστία που εμπνέει η ίδια η εταιρία στους χρήστες της.

Σε κάθε περίπτωση, τέλος, πρέπει να να επισημανθεί ότι πολλοί χρήστες δεν διαβάζουν την πολιτική ιδιωτικότητας: συνεπώς, πέραν της ουσιαστικής υποχρέωσης των υπευθύνων επεξεργασίας να διαχειρίζονται σωστά τα προσωπικά δεδομένα των χρηστών τους (δηλ. με απόλυτο σεβασμό στο τρέχον νομικό πλαίσιο), είναι κρίσιμο να γνωρίζουν και οι χρήστες τα σχετικά δικαιώματά τους (συμπεριλαμβανομένου του προαναφερθέντος δικαιώματος την ενημέρωση).

1.2.6. Απειλές κατά της Ιδιωτικότητας

Όπως ήδη έχουμε αναφέρει, η ραγδαία τεχνολογική ανάπτυξη και χρήση ηλεκτρονικών υπηρεσιών δημιουργεί προβληματισμούς σε σχέση με την ασφάλεια της ιδιωτικότητας και των προσωπικών δεδομένων. Οι πιο συνηθισμένες απειλές της πληροφοριακής ιδιωτικότητας σε περιβάλλον Η.Δ. είναι:

- η απώλεια της εμπιστευτικότητας (loss of confidentiality), η οποία προκύπτει από εισβολή σε ηλεκτρονικούς φακέλους προσωπικών δεδομένων -σύμφωνα με το άρθρο 10 του νόμου 2472/1997[1] "*Η επεξεργασία προσωπικών δεδομένων είναι απόρρητη, ενώ για την διεξαγωγή της επεξεργασίας ο υπεύθυνος επεξεργασίας οφείλει να επιλέγει πρόσωπα με αντίστοιχα επαγγελματικά προσόντα που παρέχουν επαρκείς εγγυήσεις από πλευράς τεχνικών γνώσεων και προσωπικής ακεραιότητας για την τήρηση του απορρήτου*"
- ολοένα και περισσότερες απειλές κατά αυτής, όπως: η κλοπή ταυτότητας (identity theft) για εκτέλεση ηλεκτρονικών συναλλαγών

[1] Ο ν.2472/1997 ενσωματώνει, στην ελληνική έννομη τάξη, την Οδηγία 95/46/ΕΚ – βλ. και Κεφ. 5

Όμως, όσο εξελίσσεται η τεχνολογία για την προστασία της Ιδιωτικότητας και των προσωπικών δεδομένων, τόσο εμφανίζονται καινούρια είδη επιθέσεων:

1. *Επίθεση ανάλυσης κίνησης*: Παρακολουθεί την κίνηση των δεδομένων, χωρίς, όμως, να παραβιάζει την ιδιωτικότητα.
2. *Παραβίαση απορρήτου*: Προκαλεί την έλλειψη εμπιστοσύνης, η οποία είναι ύψιστου βαθμού σε συναλλαγές Η.Δ. .Θεωρείται δεδομένο το απόρρητο των προσωπικών δεδομένων στις συναλλαγές με τον Δημόσιο Τομέα. Ο πάροχος πρέπει να είναι έμπιστος.
3. *Ανάλυση προφίλ χρήστη*: Οι διαδικτυακές «συνήθειες» του χρήστη μπορεί να παρακολουθούνται (π.χ. είδος σελίδων που επισκέπτεται, συχνότητα επισκέψεων κτλ.), γεγονός που μπορεί να οδηγήσει κάποιον τρίτο, που συλλέγει αυτήν την πληροφορία, στη δημιουργία προφίλ του χρήστη. Ένα μέσο να επιτευχθεί αυτό είναι μέσω χρήσης των λεγόμενων cookies: Τα cookies είναι μικρά αρχεία δεδομένων τα οποία αποθηκεύονται στους υπολογιστές των χρηστών και παρέχουν πληροφορίες για τους ιστότοπους που επισκέπτονται. Τα cookies μπορούν να χρησιμοποιηθούν για να παραβιάσουν την ανωνυμία από τους χρήστες ή αντίθετα, να την ενισχύσουν, επιτρέποντας την παροχή προστασίας προς τον χρήστη.
4. *Επίθεση "man-in-the-middle"*: όταν ο επιτιθέμενος θέτει τον εαυτό του ανάμεσα στον υπολογιστή του χρήστη και τον πάροχο υπηρεσιών Η.Δ. με σκοπό την παρακολούθηση και την κλοπή προσωπικών δεδομένων.
5. *Επίθεση πλαστοπροσωπείας*: Όταν ο εισβολέας δημιουργεί ένα προφίλ για τον χρήστη, υποδυόμενος εκείνον.

Συνεπώς, παρά την αυξημένη δημοφιλία και ανάπτυξη των υπηρεσιών Η.Δ., εξακολουθούν να υφίστανται απειλές στο κομμάτι της ασφάλειας και της ιδιωτικότητας. Γενικά, οι χρήστες είναι σκεπτικοί και δύσπιστοι απέναντι στις παρεχόμενες υπηρεσίες, θεωρώντας ότι θέτουν σε κίνδυνο τα προσωπικά τους δεδομένα, οπότε αυτήν η αντιμετώπιση αποτελεί το μεγαλύτερο εμπόδιο στην χρήση και στην υιοθέτηση αυτών των υπηρεσιών. Τα περιβάλλοντα Η.Δ. έχουν γίνει πιθανοί στόχοι των κυβερνοεισβολέων (cyber attackers). Η εισβολή σ' αυτά τα περιβάλλοντα

θα μπορούσε να πλήξει τις παρεχόμενες υπηρεσίες, αν δεν είναι καλά προστατευμένες: το πρόβλημα αυτό μπορεί να αντιμετωπιστεί με ανάπτυξη τεχνολογιών κρυπτογραφίας όπως θα αναπτύξουμε σε επόμενο κεφάλαιο.

1.3. Ηλεκτρονικά Διαβατήρια (e-passports)

Ένα από τα βασικά χαρακτηριστικά του 21ου αιώνα είναι η ραγδαία τεχνολογική εξέλιξη σε διάφορους τομείς, όπως στην βιομετρία. Η Βιομετρία είναι η τεχνολογία που χρησιμοποιεί μία αυτοματοποιημένη μέθοδο για την αναγνώριση ενός ανθρώπου βάσει κάποιων χαρακτηριστικών της φυσιολογίας του, όπως το πρόσωπο, την ίριδα του ματιού ή το δακτυλικό του αποτύπωμα. Μέχρι το 2001, η Βιομετρία χρησιμοποιούνταν κυρίως σε στρατιωτικό και κυβερνητικό επίπεδο. Σε εμπορικό επίπεδο, χρησιμοποιούνταν μία παρόμοια τεχνολογία η RFID (**R**adio **F**requency **Id**entification) σε υπηρεσίες μεταφοράς και πληρωμών σε τράπεζες. Μετά το τρομοκρατικό χτύπημα της 11/9 στις Η.Π.Α., οι δύο τεχνολογίες συγχωνεύτηκαν σε μία για πρώτη φορά στα διαβατήρια, τα οποία λέγονται, από τότε, ηλεκτρονικά (e-passports). Αυτήν η τεχνολογία έδωσε τη λύση στα κράτη για την αντιμετώπιση προβλημάτων που σχετίζονται με την ασφάλεια και την αναγνώριση των πολιτών, καθώς και τον εντοπισμό και την αναγνώριση αυτών που κατέχουν και χρησιμοποιούν πλαστά έγγραφα.

Η τεχνολογία RFID χρησιμοποιήθηκε για πρώτη φορά στα διαβατήρια το 1998 από τις αρχές της Μαλαισίας και στην οποία καταχωρούσαν και το ιστορικό ταξιδιών του ιδιοκτήτη του. Ωστόσο, μέχρι το 2002, αυτά τα διαβατήρια δεν ικανοποιούσαν βασικές απαιτήσεις ασφάλειας, αφού οι πληροφορίες των κατόχων τους δεν ήταν κρυπτογραφημένες. Το μόνο μέτρο ασφάλειας που περιείχαν ήταν η χρήση ψηφιακής υπογραφής σε όλα τα δεδομένα του.

Αργότερα, το 2004, ο Διεθνής Οργανισμός Πολιτικής Αεροπορίας (International Civil Aviation Organization-ICAO) ο οποίος ρυθμίζει τις διεθνείς αερομεταφορές και αποτελεί τμήμα των Ηνωμένων Εθνών (Ο.Η.Ε.), δημοσίευσε έναν οδηγό σχεδιασμού και τα κριτήρια για τα κράτη που επιθυμούν να υλοποιήσουν e-passports με χρήση RFID, το ISO 7501-1:2005. Αυτό έγινε στην προσπάθεια προτυποποίησης του ηλεκτρονικού διαβατηρίου, ώστε να είναι πιο ασφαλές. Τις αρχές του ICAO υιοθέτησαν πρώτες οι Η.Π.Α. οι οποίες και εξέδωσαν το 2005 το δικό τους ηλεκτρονικό διαβατήριο.

1.4. Ηλεκτρονικές Ταυτότητες (eID's)

Η διαχείριση ηλεκτρονικών ταυτοτήτων αποτελεί βασικό παράγοντα και προϋπόθεση για την ασφαλή και αποτελεσματική χρήση υπηρεσιών ηλεκτρονικών συναλλαγών από τους πολίτες. Μέσα σ' ένα αξιόπιστο περιβάλλον ηλεκτρονικής ταυτοποίησης ενισχύεται η εμπιστοσύνη των πολιτών στις υπηρεσίες Η.Δ. και η πεποίθησή τους ότι διασφαλίζεται η προστασία των προσωπικών τους δεδομένων. Επιπλέον, οι δημόσιοι φορείς έχουν την δυνατότητα να γνωρίζουν την ταυτότητα των πολιτών με τους οποίους συναλλάσσονται, δηλαδή ότι αυτοί οι συγκεκριμένοι πολίτες έχουν τα δικαιώματα και τις παροχές που υποστηρίζουν ότι έχουν.

Η ηλεκτρονική ταυτοποίηση αποτελεί την λογική εξέλιξη της φυσικής ταυτότητας, και σύμφωνα με την Ευρωπαϊκή Επιτροπή "*η ηλεκτρονική ταυτοποίηση είναι η διαδικασία εξόρυξης της ταυτότητας ενός πολίτη με τη χρήση ηλεκτρονικών μέσων".*

Τα περισσότερα κράτη - μέλη της Ε.Ε. έχουν υλοποιήσει την ηλεκτρονική ταυτότητα ή αλλιώς κάρτα πολίτη δίνοντας, έτσι, την δυνατότητα στους πολίτες τους να πραγματοποιούν ηλεκτρονικές συναλλαγές με τις Δημόσιες Υπηρεσίες και τους Φορείς. Η Ελλάδα και η Κύπρος είναι χώρες που ακόμα δεν έχουν υιοθετήσει κάρτα πολίτη,-

εξαίρεση αποτελούν κάποιες πιλοτικές περιπτώσεις που απευθύνονται σε συγκεκριμένες ομάδες προσώπων και για περιορισμένο εύρος εφαρμογών.

1.5. Πιστοποιητικά βάσει χαρακτηριστικών

Οι ολοένα αυξανόμενες ανάγκες της δικτυακής κοινωνίας μας απαιτούν με τη σειρά τους όλο και πιο ασφαλή συστήματα ταυτοποίησης. Όσον αφορά την αυθεντικοποίηση, ο χρήστης πρέπει να πείσει τον πάροχο ότι κατέχει ένα σύνολο χαρακτηριστικών και ο πάροχος, με τη σειρά του, να επιβεβαιώσει ότι αυτό είναι αληθές. Η τεχνολογία των Πιστοποιητικών Βάσει Χαρακτηριστικών (Attribute - Based Credentials) είναι σχεδιασμένη για να είναι πιο φιλική σε σχέση με άλλες μεθόδους ταυτοποίησης και αυθεντικοποίησης, οι οποίες πάσχουν από διαβίβαση πληροφοριών, περισσότερων από όσο πραγματικά χρειάζεται. Αποτελούν, αναμφίβολα, μία πολλά υποσχόμενη τεχνολογία στον τομέα της διασφάλισης της ιδιωτικότητας.

Με τον όρο "*πιστοποιητικά*" εννοούμε τα μέσα- χαρακτηριστικά που χρησιμοποιούνται για να αποδειχθεί η εγκυρότητα των στοιχείων ενός ατόμου και να πιστοποιηθεί η ταυτότητά του.

Μερικά από τα χαρακτηριστικά, όπως ο αριθμός ταυτότητας, ταυτοποιούν το άτομο. Όμως, κάποια άλλα, όπως το φύλο, δεν προσδιορίζουν μοναδικά ένα πρόσωπο, αλλά έχουν την ίδια τιμή και για άλλους ανθρώπους.

Γνωρίζουμε ότι η ηλεκτρονική ταυτοποίηση πραγματοποιείται είτε με χρήση ηλεκτρονικών ταυτοτήτων, είτε με ηλεκτρονικά διακριτικά ελέγχου ταυτότητας (authentication tokens) είτε με χρήση τεχνολογίας RFID, είτε με κρυπτογραφικά πιστοποιητικά (cryptographic certificates). Ωστόσο, όλα τα παραπάνω δεν προσφέρουν πλήρη ασφάλεια της ιδιωτικότητας και κάποιος κακόβουλος θα μπορούσε να αποκαλύψει την ταυτότητα του ατόμου. Επίσης, σε πολλές περιπτώσεις μπορεί να

αποκαλυφθούν περισσότερες πληροφορίες από όσες χρειάζονται για το άτομο με αποτέλεσμα την ζημίωση της ιδιωτικότητας του.

Σε αντίθεση με τις παραπάνω εφαρμογές, τα πιστοποιητικά που βασίζονται στα χαρακτηριστικά, αποτελούν κρυπτογραφικές λύσεις που επιτρέπουν στον κάτοχό τους να αποκαλύψει μόνο τις πληροφορίες που του ζητούνται, χωρίς να αποκαλυφθούν τα πλήρη στοιχεία του. Ένα τέτοιο παράδειγμα αποτελούν τα κρυπτογραφικά πιστοποιητικά, ενώ οι δύο πιο αντιπροσωπευτικές τεχνολογίες που βασίζονται σε αυτά είναι η U-Prove της Microsoft και η Idemix της IBM. Τα τελευταία χρόνια, το ευρωπαϊκό έργο ABC4Trust είχε σκοπό να ενσωματώσει τις δύο παραπάνω τεχνολογίες σε μία ενοποιημένη αρχιτεκτονική, ενώ και το ακαδημαϊκό έργο IRMA επικεντρώνεται στην αποτελεσματικότητα της χρήσης αυτών των πιστοποιητικών.

1.6. Δομή της εργασίας

Αντικείμενο της παρούσας εργασίας αποτελεί η μελέτη υπηρεσιών Ηλεκτρονικής Διακυβέρνησης από την σκοπιά της ιδιωτικότητας και των προσωπικών δεδομένων. Όπως ήδη αναφέρθηκε, οι υπηρεσίες αυτές, παρά τα πλεονεκτήματά τους, ενδεχομένως οδηγήσουν σε επεξεργασίες μη σύμφωνες με την προστασία προσωπικών δεδομένων, εφόσον ο σεβασμός προς την ιδιωτικότητα δεν αποτελέσει βασική σχεδιαστική παράμετρο κατά την ανάπτυξή τους. Ειδικότερα, ως προς το ζήτημα της ηλεκτρονικής ταυτότητας, δεν υπάρχει κοινή προσέγγιση στα διάφορα κράτη, γεγονός που καταδεικνύει την σύνθετη δομή του προβλήματος. Δεδομένου ότι στον ελληνικό χώρο πολλές συναφείς υπηρεσίες είναι υπό διαμόρφωση, η εργασία εστιάζει στην μελέτη των τεχνολογιών εκείνων που είναι φιλικές προς την ιδιωτικότητα. Πιο συγκεκριμένα:

Το πρώτο κεφάλαιο είναι εισαγωγικό και στο οποίο γίνεται ανάλυση των σημαντικότερων εννοιών της εργασίας, δηλαδή της ηλεκτρονικής

διακυβέρνησης, της ιδιωτικότητας, των ηλεκτρονικών διαβατηρίων, των ηλεκτρονικών ταυτοτήτων και της τεχνολογίας των διαπιστευτηρίων με βάση τα χαρακτηριστικά.

Στο δεύτερο κεφάλαιο αναπτύσσονται τα ηλεκτρονικά διαβατήρια που αποτελούν μία ευρέως διαδεδομένη προσέγγιση διεθνώς για την αποτελεσματική αναγνώριση των ταξιδιωτών, καθώς επίσης και οι τεχνολογίες που τα διέπουν.

Στο τρίτο κεφάλαιο αναπτύσσεται η ευρύτερη έννοια των ηλεκτρονικών ταυτοτήτων και η χρήση τους από τα κράτη - μέλη της Ε.Ε.

Στο τέταρτο κεφάλαιο αναπτύσσεται μία πολλά υποσχόμενη τεχνολογία ως προς την ιδιωτικότητα, η τεχνολογία των πιστοποιητικών βάσει χαρακτηριστικών (ABC), αναδεικνύοντας τα βασικά της πλεονεκτήματα αλλά και τις τρέχουσες εφαρμογές της.

Στο πέμπτο κεφάλαιο αναπτύσσεται το νομικό πλαίσιο που διέπει την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων, τόσο στην Ευρωπαϊκή Ένωση, όσο και στην Ελλάδα.

Στο έκτο κεφάλαιο αναπτύσσονται ζητήματα ασφάλειας και προστασίας της ιδιωτικότητας σε περιβάλλον Η.Δ.

Στο έβδομο κεφάλαιο αναλύεται η δυνατότητα ενσωμάτωσης των τεχνολογιών που αναλύσαμε στις χώρες της Ευρωπαϊκής Ένωσης και στην Ελλάδα.

Στο όγδοο κεφάλαιο αναλύεται το ερωτηματολόγιο που υλοποιήθηκε για την ιδιωτικότητα και την χρήση της τεχνολογίας ABC στις ηλεκτρονικές υπηρεσίες του Δημόσιου Τομέα.

Τέλος, τα τελικά συμπεράσματα της εργασίας αποτυπώνονται στο ένατο κεφάλαιο.

Κεφάλαιο 2

Ηλεκτρονικά Διαβατήρια (e-passports)

2.1. Εισαγωγή

Ένας μεγάλος αριθμός διαβατηρίων που χρησιμοποιούνται σήμερα παγκοσμίως είναι ηλεκτρονικού τύπου και αναμένεται ως το 2017, αυτός ο τύπος να κατέχει το 53% των διαβατηρίων [19]. Οι απαιτήσεις για τον νέο αυτόν τύπο διαβατηρίων καθορίζονται από τις Η.Π.Α. και τον ICAO, οι οποίες πρέπει να ικανοποιούν ένα υψηλό επίπεδο ασφάλειας και ιδιωτικότητας των κατόχων τους.

Το σύμβολο των βιομετρικών διαβατηρίων

2.1.1. Σκοπός και χαρακτηριστικά των ηλεκτρονικών διαβατηρίων

Η ραγδαία τεχνολογική εξέλιξη δεν επέφερε μόνο καινοτομία, αλλά έπαιξε ρόλο και στο να βρεθούν νέοι τρόποι εξαπάτησης, παραβίασης και υποκλοπής δεδομένων. Έτσι, σκοπός των ηλεκτρονικών διαβατηρίων είναι:

- ❖ να εμποδίσουν την παράνομη είσοδο ταξιδιωτών σε μία χώρα.
- ❖ να περιορίσουν τη χρήση πλαστών ταξιδιωτικών εγγράφων αναγνώρισης των ατόμων.
- ❖ να αυξηθούν τα επίπεδα ασφάλειας μιας χώρας με καλύτερο έλεγχο των συνόρων της και των αεροδρομίων της.
- ❖ να ενισχυθεί η διαδικασία ελέγχου στα σύνορα και στα αεροδρόμια.
- ❖ να διασφαλιστεί η ακεραιότητα και η αυθεντικότητα των εγγράφων.

Το απλό διαβατήριο περιέχει σημαντικές προσωπικές πληροφορίες του κατόχου του, όπως

- φωτογραφία,
- ονοματεπώνυμο,
- ημερομηνία και τόπος γέννησης,
- εθνικότητα,
- ημερομηνία έκδοσης,
- ημερομηνία λήξης,
- υπηρεσία έκδοσής του
- αριθμός διαβατηρίου

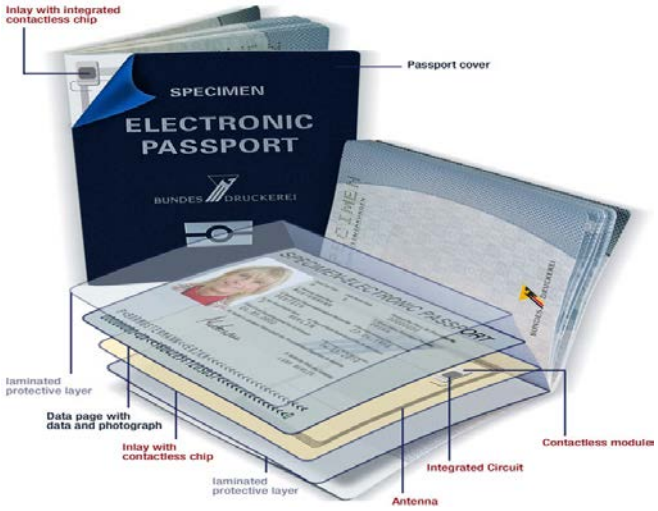
Τα ηλεκτρονικά διαβατήρια, εκτός των παραπάνω, περιέχουν και ένα ηλεκτρονικό τσιπ που βασίζεται στην τεχνολογία RFID, το οποίο περιέχει βιομετρικές μετρήσεις του κατόχου του και χρησιμοποιεί κρυπτογραφικές τεχνικές που αυξάνουν την ασφάλειά του.

Συνοπτικά, τα ηλεκτρονικά διαβατήρια βασίζονται σ' έναν συνδυασμό τεχνικών για να αναπαραχθούν:

1. *Βιομετρία*, δηλαδή την ανάλυση βιολογικών στοιχείων με τη χρήση στατιστικών και μαθηματικών μεθόδων
1. *Τεχνολογία RFID*, η οποία βασίζεται σε ταυτοποίηση του κατόχου μέσω ραδιοσυχνοτήτων και η οποία δίνει τη δυνατότητα ασύρματης επικοινωνίας με τα τερματικά ανάγνωσης ηλεκτρονικών διαβατηρίων
2. *Κρυπτογραφικές τεχνικές* και συγκεκριμένα την Υποδομή Δημόσιου Κλειδιού (PKI-Public Key Infrastructure)

Έτσι, τα επιπλέον χαρακτηριστικά του e-passport σε σχέση με το απλό διαβατήριο είναι:

- ψηφιακή φωτογραφία
- τύπος διαβατηρίου
- ψηφιακή υπογραφή, για την αποτροπή αλλαγής των στοιχείων



Το ηλεκτρονικό διαβατήριο με την ετικέτα RFID, το chip και την κεραία
Πηγή: Jeng and Chen (2009)

2.1.2. Κατηγορίες και εξέλιξη των ηλεκτρονικών διαβατηρίων

Το πρώτο επίσημο ηλεκτρονικό διαβατήριο που πληρούσε τις προϋποθέσεις του ICAO εκδόθηκε το 2005 από τις Η.Π.Α. και ανήκει στην κατηγορία της **πρώτης γενιάς ηλεκτρονικών διαβατηρίων**. Αυτά τα διαβατήρια χρησιμοποιούσαν τον μηχανισμό *BAC (Basic Access Control)*, ο

οποίος βασιζόταν στην συμμετρική κρυπτογράφηση και χρησιμοποιούνταν για την αποτροπή κλοπής και υποκλοπής και προστάτευε τα δεδομένα του chip, όπως τα βιομετρικά. Αυτός ο μηχανισμός προτείνεται ακόμη από τον ICAO ως απαραίτητος για την προστασία της ιδιωτικότητας των δεδομένων.

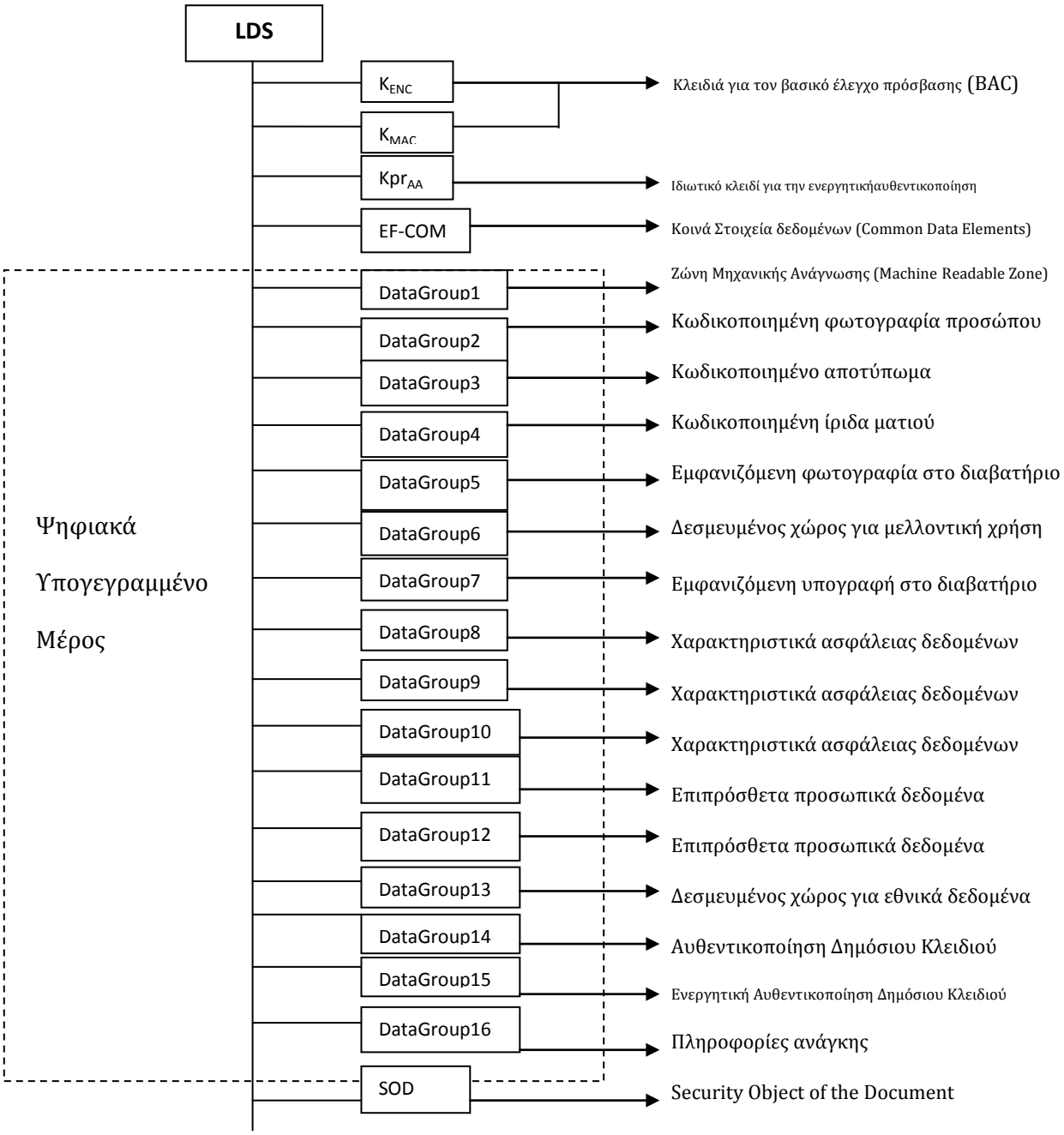
Το 2006, η Ευρωπαϊκή Ένωση πρότεινε στα κράτη-μέλη της να συμπεριλάβουν επιπλέον βιομετρικές πληροφορίες στα ηλεκτρονικά τους διαβατήρια, και πιο συγκεκριμένα, το ψηφιακό αποτύπωμα. Έτσι, στα μέσα του 2009, εμφανίστηκε η **δεύτερη γενιά ηλεκτρονικών διαβατηρίων**.

Για να προστατευθούν αυτά τα επιπρόσθετα δεδομένα, ήταν απαραίτητος ένας νέος μηχανισμός ασφάλειας: ο *EAC (Extended Access Control) version 1.11*, ο οποίος περιορίζει την πρόσβαση στα πολύ ευαίσθητα βιομετρικά δεδομένα, όπως το αποτύπωμα και την ίριδα στις εξουσιοδοτημένες αρχές μόνο, και προσθέτει λειτουργικότητα για την επιβεβαίωση της αυθεντικότητας του chip και της συσκευής ανάγνωσης (terminal authentication). ενώ κάνει χρήση ενός ισχυρού ασύμμετρου κρυπταλγόριθμου που βασίστηκε στην Ελλειπτική Καμπύλη Diffie-Hellman. Έτσι οδηγηθήκαμε στην **τρίτη γενιά ηλεκτρονικών διαβατηρίων.**

Αν και ο EAC προστατεύει τα δεδομένα, η αύξηση της παραβατικότητας μέσω της εξέλιξης της τεχνολογίας οδήγησε στην εισαγωγή ενός νέου μηχανισμού ασφάλειας, του *SAC (Supplemental Access Control)*. Το πρωτεύον πλεονέκτημα αυτού είναι ότι το επίπεδο ασφάλειας που είναι ανεξάρτητο του κωδικού για την αυθεντικοποίηση και παράγει τα κλειδιά για την ασφαλή μετάδοση. Χάρη στον SAC τα δεδομένα είναι καλά προστατευμένα, τόσο κατά την αποθήκευση, όσο και κατά την μετάδοσή τους στην συσκευή ανάγνωσης. Η εμπιστευτικότητα των δεδομένων ενισχύεται και η υποκλοπή καθίσταται αδύνατη. Ο SAC προτείνεται από τον ICAO με το τέλος του 2014, ενώ και η Ευρωπαϊκή Ένωση τον προτείνει στα κράτη-μέλη της να τον υιοθετήσουν κατά το ίδιο διάστημα. Οπότε, το 2015, οδηγούμαστε στην **τέταρτη γενιά ηλεκτρονικών διαβατηρίων.** [19]

2.2. Λογική Δομή Δεδομένων

Ο ICAO εξέδωσε μία τυποποιημένη λογική δομή των δεδομένων για την αποθήκευσή τους, η οποία είναι ίδια και για τις τέσσερις γενιές e-passports. Ο λόγος είναι να υπάρχει παγκόσμια διαλειτουργικότητα και για τις ετικέτες των e-passports και για τους αναγνώστες τους, και η οποία να διατηρηθεί για όλα τα κράτη που εκδίδουν τα νέου τύπου διαβατήρια. [20]



Δομή Δεδομένων των e-passports

Σύμφωνα με το παραπάνω σχήμα, σε κάθε βιομετρικό διαβατήριο υπάρχει μία λογική δομή δεδομένων (LDS-Logical Data Structure έκδοση 1.7) για την αποθήκευση των δεδομένων στο τσιπ. Αυτά τα δεδομένα κατηγοριοποιούνται σε 16 ομάδες δεδομένων (DataGroup1 έως DataGroup16 στο ανωτέρω Σχήμα), δίπλα από τις οποίες αναγράφεται και το είδος της πληροφορίας που περιέχει και οι οποίες είναι προστατευμένες και γράφονται μόνο όταν είναι να εκδοθεί το διαβατήριο από την αρμόδια αρχή. Εκτός από αυτά τα δεδομένα είναι, επίσης, αποθηκευμένα και τα κλειδιά για τον έλεγχο και την αυθεντικοποίηση σε ξεχωριστό τμήμα της μνήμης. Επιπλέον, ο κατακερματισμός (hash) όλων αυτών των δεδομένων είναι αποθηκευμένος στο Τεκμηριωμένο Αντικείμενο Ασφάλειας (Security Object of the Document-S.O.D.) και όλα είναι ψηφιακά υπογεγραμμένα από την Εκδίδουσα Αρχή (DS) της κάθε χώρας (βλ. και Ενότητα 2.5, όπου περιγράφεται η δομή των ψηφιακών πιστοποιητικών και η έννοια των ψηφιακών υπογραφών). Το τερματικό πρέπει να έχει το ψηφιακό πιστοποιητικό της εκδίδουσας αρχής, το πιστοποιητικό της Κρατικής Αρχής Πιστοποίησης(CSCA) που πιστοποιεί την ψηφιακή υπογραφή και την λίστα ανάκλησης πιστοποιητικών. Έτσι, αφού εξάγει όλα τα δεδομένα, υπολογίζει την κατακερματισμένη τιμή τους (hash) και την συγκρίνει με το Τεκμηριωμένο Αντικείμενο Ασφάλειας (SOD) – εάν ταυτίζονται, τότε το διαβατήριο είναι έγκυρο.

2.2.1. Ασφαλής Πρόσβαση των Δεδομένων

Ο ICAO όρισε το 2004 τις προδιαγραφές για τα τρία κρυπτογραφικά πρωτόκολλα που διέπουν την ασφαλή πρόσβαση των δεδομένων των ηλεκτρονικών διαβατηρίων και από τότε η μόνη διαφοροποίηση που υπάρχει είναι σε σχέση με τον Βασικό Έλεγχο Πρόσβασης (BAC), ο οποίος αντικαταστάθηκε το 2008 με τον Εκτενή Έλεγχο Πρόσβασης (EAC) και ο οποίος περιέχει το πρωτόκολλο αυθεντικοποιημένης εγκατάστασης σύνδεσης με συνθηματικό (*PACE-Password-Authenticated Connection Establishment*), το οποίο και αποτέλεσε πρόταση της Γερμανικής

Ομοσπονδιακής Υπηρεσίας για την Ασφάλεια στην Πληροφορική με σκοπό της αύξηση της ασφάλειας μέσω ισχυρότερης αυθεντικοποίησης. Συνοπτικά, τα τρία αυτά πρωτόκολλα είναι:[21]

1. Η *παθητική αυθεντικοποίηση*, η οποία από την αρχή είναι και η πιο αναγκαία, χρησιμοποιείται για να επιβεβαιώσει την ακεραιότητα και την αυθεντικότητα των δεδομένων που βρίσκονται στη μνήμη του chip, μέσω ελέγχου της ψηφιακής υπογραφής τους. Όμως, αυθεντικοποιεί μόνο τα δεδομένα και όχι το chip, το οποίο αυθεντικοποιείται μέσω της ενεργητικής αυθεντικοποίησης.
2. Η *ενεργητική αυθεντικοποίηση* είναι προαιρετική και χρησιμοποιείται για την αυθεντικότητα του ίδιου του chip, το οποίο πρέπει να αποδείξει ότι έχει γνώση του ιδιωτικού κλειδιού που χρησιμοποιείται από το πρωτόκολλο ανταπόκρισης και κατά βάση προστατεύει από την ενδεχόμενη απειλή κλώνων.
3. Ο *Βασικός Έλεγχος Πρόσβασης* χρησιμοποιείται για να εμποδίσει την μη εξουσιοδοτημένη πρόσβαση στα δεδομένα του διαβατηρίου και για να εντοπίζει πιθανές επιθέσεις. Όταν το τερματικό προσπαθεί να αναγνώσει τα δεδομένα, δεσμεύει ένα πρωτόκολλο το οποίο απαιτεί από το τερματικό να γνωρίζει το ζευγάρι των κλειδιών που προέρχονται από την MRZ (Machine Readable Zone) των δεδομένων του διαβατηρίου. Μέσω αυτών των μυστικών κλειδιών αποκτιέται το κλειδί συνόδου για την ασφαλή αποστολή των δεδομένων το τερματικό.

   Επίσης, παράγει ένα κλειδί συνόδου το οποίο αποτρέπει τις επιθέσεις eavesdropping.

Όσον αφορά την αντικατάσταση του Βασικού Ελέγχου Πρόσβασης, με τον Εκτενή Έλεγχο Πρόσβασης που χρησιμοποιεί το πρωτόκολλο PACE, είχε παρατηρηθεί ότι τα κλειδιά που παρήγαγε είχανε χαμηλή εντροπία, (δηλαδή όχι καλά χαρακτηριστικά τυχαιότητας) όταν αυτά εξάγονταν από την MRZ (Machine Readable Zone) πληροφορία του e-passport. Η MRZ πληροφορία αποτελείται από:

- έναν σειριακό αριθμό 9 ψηφίων
- την ημερομηνία γέννησης (6 ψηφία)

- την ημερομηνία λήξης του διαβατηρίου (6 ψηφία)

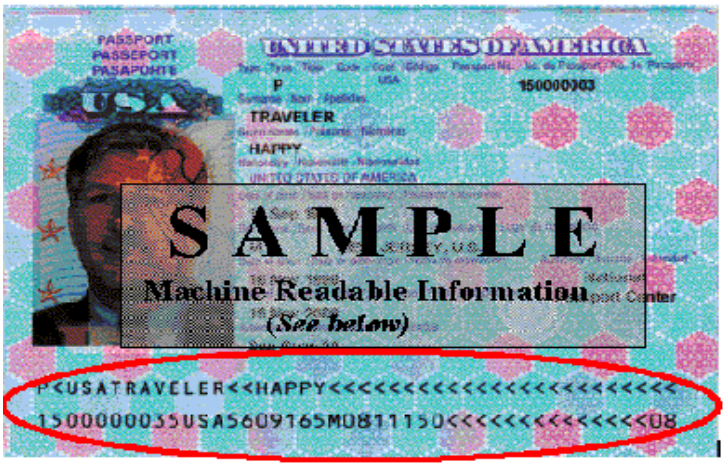
τα οποία είναι αποθηκευμένα στο πεδίο της μνήμης DataGroup1, όπως φαίνεται και στο Σχήμα της Λογικής Δομής των Δεδομένων.

Το τερματικό πρέπει να είναι σε οπτική επαφή με το ηλεκτρονικό διαβατήριο, ώστε να μπορέσει να διαβάσει τις παραπάνω πληροφορίες της MRZ.

Οι στόχοι ασφάλειας από την ICAO για τις προδιαγραφές κατασκευής των e-passports έχουν καθοριστεί ως εξής:

1. Εμπιστευτικότητα δεδομένων
2. Ακεραιότητα δεδομένων
3. Αυθεντικοποίηση προέλευσης δεδομένων
4. Αμοιβαία αυθεντικοποίηση
5. Ακεραιότητα κλειδιού
6. Μη απάρνηση δεδομένων

Όσον αφορά το πρωτόκολλο PACE προσφέρει πολύ μεγάλη ασφάλεια στα προσωπικά στοιχεία του διαβατηρίου, μιας και χρησιμοποιεί ένα κοινό μυστικό κλειδί το οποίο παράγει κλειδιά υψηλής εντροπίας. Αυτό οφείλεται σε μεγάλο βαθμό και στην χρήση της μεθόδου Diffie-Hellman [22] για την πραγματοποίηση της ανταλλαγής. Όσον αφορά τα βιομετρικά στοιχεία του διαβατηρίου, τα οποία είναι ευαίσθητα, προστατεύονται από τον μηχανισμό αυθεντικοποίησης του τερματικού, το οποίο θα δούμε παρακάτω.



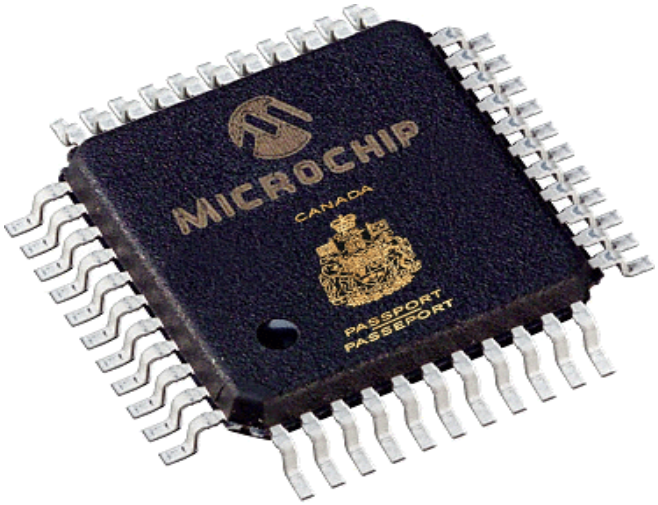
Ζώνη Μηχανικής Ανάγνωσης (MRZ) κυκλωμένη με κόκκινο μολύβι, η οποία βρίσκεται στην πρώτη σελίδα του e-passport, Πηγή: http://en.wikipedia.org/wiki/Machine-readable_passport

2.2.2 Τεχνολογία των chips

Το chip που βρίσκεται στο διαβατήριο νέου τύπου έχει διαστάσεις 0.15*0.15 χιλιοστά, ενώ το πάχος του είναι όσο ένα φύλλο χαρτί, δηλαδή 7.5 χιλιοστά. Εκπέμπει στην συχνότητα 13,56 MHz, ενώ ανήκει στην κατηγορία passive tag, δηλαδή δεν χρησιμοποιεί μπαταρία, οπότε και έχει απεριόριστη διάρκεια ζωής. Η μνήμη του είναι της τάξης των 32 με 72 Kbytes, ενώ εταιρείες που παράγουν τέτοιου είδους chips είναι η ολλανδική Philips, η γερμανική PolyC και η γαλλική ASK.

Στα e-passports τέταρτης γενιάς υπάρχει πρόβλεψη για αναβάθμιση της λογικής δομής των δεδομένων, από LDS version 1.7 σε LDS version 2.0, στην οποία θα μπορούν να προστεθούν επιπλέον βιομετρικές πληροφορίες, ενώ θα χωρούν δεδομένα της τάξεως των 500 Kbytes.

Όσον αφορά την ταχύτητα ανάγνωσης των δεδομένων του διαβατηρίου από τα τερματικά, στα e-passports τρίτης γενιάς που κυκλοφορούν τώρα, η ταχύτητα είναι περίπου στο 1.5 δευτερόλεπτα και αναμένεται να πέσει στο 0.8 δευτερόλεπτα με τα διαβατήρια τέταρτης γενιάς.



Το chip του Καναδέζικου e-passport, Πηγή:
http://www.rushpassport.com/blog/tag/epassport/

2.3. Βιομετρία

Βιομετρία είναι η επιστήμη η οποία περιλαμβάνει μετρήσεις μαθηματικές και στατιστικές που σχετίζονται με τα ανθρώπινα χαρακτηριστικά. Αυτά τα χαρακτηριστικά μπορεί να είναι είτε *σωματικά, φυσιολογικά, παθητικά*- όπως λέγονται-, και αφορούν ανθρώπινα χαρακτηριστικά που είναι σταθερά ή αμετάβλητα, όπως το δακτυλικό αποτύπωμα, το πρόσωπο, η γεωμετρία της παλάμης και η ίρις του ματιού, είτε *συμπεριφορικά, ενεργητικά*, όπως η χροιά της φωνής ή ο τρόπος πληκτρολόγησης στον υπολογιστή. Ωστόσο, οποιοδήποτε ανθρώπινο, σωματικό και συμπεριφορικό χαρακτηριστικό μπορεί να χρησιμοποιηθεί στην Βιομετρία, αρκεί να ικανοποιεί τις παρακάτω επιθυμητές απαιτήσεις:[23]

- *Καθολικότητα (Universality)*: κάθε άνθρωπος πρέπει να έχει αυτό το χαρακτηριστικό
- *Μοναδικότητα (Uniqueness)*: Δεν μπορεί δύο άνθρωποι να έχουν ακριβώς το ίδιο χαρακτηριστικό
- *Μονιμότητα (Permanence)*: Αυτό το χαρακτηριστικό πρέπει να παραμένει αμετάβλητο στο χρόνο

- *Δυνατότητα Συλλογής (Collectability)*: Αυτό το χαρακτηριστικό μπορεί να μετρηθεί ποσοτικά
- *Απόδοση (Performance)*: Οι απαιτήσεις που χρειάζονται για να επιτευχθεί με ακρίβεια μία δεκτή αναγνώριση
- *Δυνατότητα Αποδοχής (Acceptability)*: Δείχνει το βαθμό στον οποίο οι άνθρωποι μπορούν να δεχτούν τη χρήση του βιομετρικού συστήματος
- *Καταστρατήγηση (Circumvention)*: Δείχνει πόσο εύκολα μπορεί να ξεγελαστεί το σύστημα από δόλιες τεχνικές

Η Βιομετρία είναι μία πολλά υποσχόμενη επιστήμη η οποία μπορεί να έχει εφαρμογές σε πολλά επίπεδα, όμως η πιο δημοφιλής χρήση της είναι στα ηλεκτρονικά διαβατήρια, αφού μπορεί να προσφέρει ασφάλεια στα ταξιδιωτικά έγγραφα. Ο ICAO έχει ορίσει ως πρωτεύον βιομετρικό χαρακτηριστικό την *αναγνώριση προσώπου (face recognition*) και ως εφεδρικό και μη υποχρεωτικό χαρακτηριστικό την *αναγνώριση του δακτυλικού αποτυπώματος (fingerprint recognition)*.

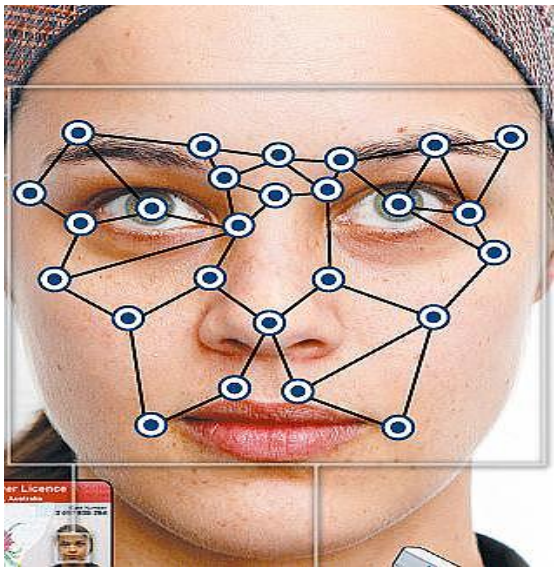
2.3.1. Αναγνώριση Προσώπου (Face Recognition)

Η αναγνώριση προσώπου αποτελεί το πιο ευρέως χρησιμοποιούμενο βιομετρικό χαρακτηριστικό. Διακρίνεται σε δύο τρόπους υλοποίησης:

Ο πρώτος τρόπος προκύπτει από την σύγκριση της φωτογραφίας του διαβατηρίου με τον ίδιο τον κάτοχό του, δηλαδή κρίνει οπτικά ο ελεγκτής αν το πρόσωπο της φωτογραφίας είναι το ίδιο με το άτομο που βρίσκεται μπροστά του. Αυτή η μέθοδος υλοποιείται στις περισσότερες χώρες του κόσμου και σε όλα τα κράτη-μέλη της Ε.Ε.

Ο δεύτερος τρόπος προκύπτει μέσω της φωτογραφίας (μορφής JPEG και μεγέθους 15 kbytes) και σχετίζεται με τα χαρακτηριστικά γνωρίσματα του προσώπου, όπως τις αποστάσεις μεταξύ των ματιών, της μύτης, του στόματος και των αυτιών. Οι μετρήσεις κωδικοποιούνται

ψηφιακά και αυτό μπορεί έπειτα να χρησιμοποιηθεί για λόγους σύγκρισης και επαλήθευσης της αποθηκευμένης εικόνας στην βάση δεδομένων με την φωτογραφία του. Δυσκολία προσδιορισμού παρουσιάζεται όταν η φωτογραφία έχει ληφθεί από μία δραστικά διαφορετική οπτική γωνία από την αποθηκευμένη εικόνα. Τίθεται, όμως, το ερώτημα κατά πόσο το πρόσωπο παρέχει επαρκή βάση για την αναγνώριση ενός μεγάλου αριθμού των ταυτοτήτων, δεδομένων των φυσικών μεταβολών που υφίσταται κατά τη διάρκεια της διαδικασίας γήρανσης ή των τεχνητών μεταβολών μέσω του μακιγιάζ ή της αλλαγής του χρώματος και του μήκους των μαλλιών.[24]



Αναγνώριση προσώπου μέσω μέτρησης αποστάσεων, σύγκρισης και επαλήθευσης αυτών, Πηγή: University of Toronto, Faculty of Applied Science & Engineering

2.3.2. Αναγνώριση Δακτυλικού Αποτυπώματος (Fingerprint Recognition)

Η αναγνώριση δακτυλικών αποτυπωμάτων συγκαταλέγεται μεταξύ των παλαιοτέρων βιομετρικών συστημάτων. Συστήματα αναγνώρισης δακτυλικών αποτυπωμάτων χρησιμοποιούνται πολύ συχνά, λόγω της ακρίβειάς τους για τον εντοπισμό ενός ατόμου, ενώ η μέθοδος σάρωσης

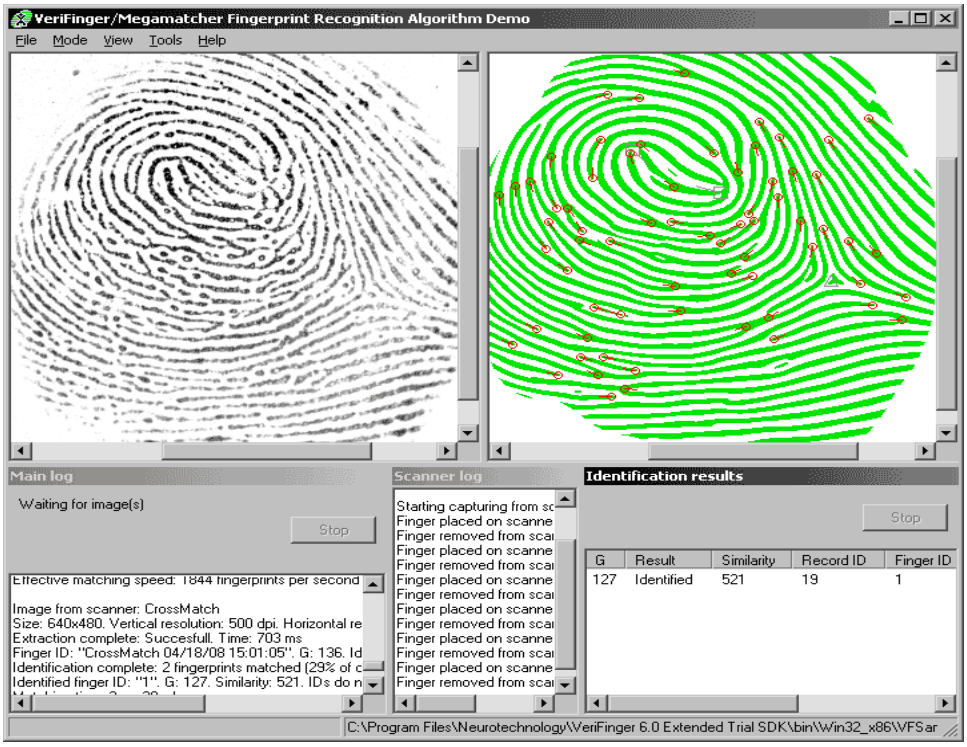
δακτυλικών αποτυπωμάτων είναι επίσης εξαιρετικά προσιτή. Ωστόσο, οι μέθοδοι αναγνώρισης δακτυλικών αποτυπωμάτων δεν είναι πάντα αλάνθαστοι. Γενετικοί παράγοντες, η γήρανση, το περιβάλλον ή επαγγελματικοί λόγοι (χειρωνακτική εργασία που προκαλεί μώλωπες ή κοψίματα) δύνανται να μεταλλάσσουν συνεχώς τα δακτυλικά αποτυπώματα.[24]

Η λήψη των δακτυλικών αποτυπωμάτων γίνεται με διαφόρων ειδών αισθητήρες (οπτικούς, θερμικούς, ηλεκτρομαγνητικούς) με στόχο την αποφυγή περιπτώσεων εξαπάτησης των συστημάτων μέσω παρουσίασης ψεύτικών ή κλεμμένων δακτυλικών αποτυπωμάτων. Η βάση δεδομένων περιέχει δακτυλικά αποτυπώματα αποθηκευμένα σε ψηφιακές φωτογραφίες με τις οποίες γίνεται η σύγκριση των ληφθέντων.

Σύγκριση μεταξύ face recognition-fingerprint recognition στην κλίμακα από 1 (χειρότερο) έως 5 (καλύτερο)

Τεχνολογία	Ακρίβεια	Βολικότητα	Κόστος	Μέγεθος
Face Recognition	2	3	4	3
Fingerprint Recognition	5	5	4	4

Πηγή: University of Toronto, Faculty of Applied Science & Engineering



Πρόγραμμα αναγνώρισης και ταυτοποίησης δακτυλικών αποτυπωμάτων, Πηγή: University of Toronto, Faculty of Applied Science & Engineering

2.4. Τεχνολογία RFID

Η Αναγνώριση/Ταυτοποίηση μέσω Ραδιοσυχνοτήτων (RFID) χρησιμοποιήθηκε για πρώτη φορά σε ηλεκτρονικά διαβατήρια το 1998 από τις Αρχές της Μαλαισίας, όμως μέχρι το 2002, τα συγκεκριμένα διαβατήρια απέτυχαν να ικανοποιούν τις βασικές απαιτήσεις ασφαλείας, μιας και οι πληροφορίες του κατόχου τους δεν ήταν κρυπτογραφημένες. Το μοναδικό μέτρο ασφαλείας που είχε υλοποιηθεί ήταν η ψηφιακή υπογραφή σε όλα τα δεδομένα του διαβατηρίου, η οποία αποτελείται από τέσσερα συστατικά:

- *την ετικέτα (tag)*, η οποία είναι μικρή ραδιοσυσκευή που επικολλάται στο διαβατήριο και η οποία αποτελείται από ένα κύκλωμα σιλικόνης, προσκολλημένο σε επίπεδη κεραία. Επίσης, διαθέτει μνήμη περιορισμένου μεγέθους για αποθήκευση του μοναδικού αναγνωριστικού

κωδικού EPC (Electronic Product Code) που αποτελεί μοναδική ταυτότητα για κάθε ετικέτα.

- *τον αναγνώστη (reader*), ο οποίος είναι μία συσκευή η οποία λαμβάνει δεδομένα από τις ετικέτες με ασύρματο τρόπο μέσω της κεραίας. Συγκεκριμένα λαμβάνει τον EPC κωδικό ο οποίος προωθείται στο back-end σύστημα ξενιστή.
- *back-end σύστημα ξενιστή (host computer system*) προκειμένου να τον επεξεργαστεί και να παράγει χρήσιμα δεδομένα, όπως να αναζητήσει σε μία βάση δεδομένων τις πληροφορίες που σχετίζονται με το συγκεκριμένο διαβατήριο.
- και *το ενδιάμεσο λογισμικό (middleware)* που περιλαμβάνει τις εφαρμογές του back-end, καθώς και *τα πρωτόκολλα επικοινωνίας.* [25]

Ασύρματος αναγνώστης RFID για e-passports

2.4.1. RFID ετικέτες

Οι RFID ετικέτες διακρίνονται σε *ενεργές (active)* και *παθητικές (passive)*, ενώ αυτές που χρησιμοποιούνται στα ηλεκτρονικά διαβατήρια είναι οι *παθητικές*.

Οι ενεργές ετικέτες τροφοδοτούνται από μπαταρία ή άλλη αυτόνομη πηγή ενέργειας, μπορούν να εκπέμψουν ένα σήμα στον αναγνώστη από μεγάλη απόσταση και λειτουργούν στις συχνότητες UHF και μικροκυμάτων.

Αντίθετα, οι παθητικές ετικέτες δεν περιέχουν κάποια πηγή ενέργειας, αλλά μπορούν να αξιοποιούν τα ραδιοκύματα που εκπέμπει ο αναγνώστης. Εκείνος εκπέμπει σε μια ραδιοσυχνότητα χαμηλής ενέργειας, και η ετικέτα λαμβάνει τα ραδιοκύματα αυτά μέσω της κεραίας της και τα μετατρέπει σε ενέργεια την οποία χρειάζεται για την λειτουργία της. Λόγω του τρόπου πρόσληψης της ενέργειας, οι παθητικές ετικέτες υφίστανται περιορισμούς στην απόσταση εκπομπής, τυπικά μέχρι τρία (3) μέτρα και στο μέγεθος της μνήμης που μπορούν να έχουν. Όμως το χαμηλό τους κόστος και η μεγάλη διάρκεια ζωής τους τις κάνει ελκυστικές για μεγάλο εύρος εφαρμογών, ενώ επιπρόσθετα μπορούν και λειτουργούν πέρα των UHF και των μικροκυματικών συχνοτήτων και στις LF και HF συχνότητες. [25]

2.4.2. Προτυποποίηση

Όσον αφορά την προτυποποίηση των RFID ετικετών, προκειμένου να επιτευχθεί η διαλειτουργικότητά τους μεταξύ των διαφόρων κατασκευαστών, έχουν συσταθεί φορείς προτυποποίησης. Στην Ευρώπη, τα τεχνικά χαρακτηριστικά, όπως οι χρησιμοποιούμενες ραδιοσυχνότητες και η ισχύς τους ρυθμίζονται από το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων ETSI (European Telecommunications Standards Institute), ενώ τα πρωτόκολλα επικοινωνίας προτείνονται από διάφορους φορείς και τους ίδιους τους κατασκευαστές. Οι δύο πιο σημαντικοί οργανισμοί προτυποποίησης είναι ο Διεθνής Οργανισμός Προτυποποίησης ISO και ο EPCglobal.

Η κωδικοποίηση των δεδομένων των RFID βασίζεται στο πρότυπο ISO 15962: Radio Frequency Identification for Item Management- Πρωτόκολλο Δεδομένων: κανόνες κωδικοποίησης Δεδομένων και συναρτήσεις λογικής μνήμης. Και το πρωτόκολλο επικοινωνίας βασίζεται στο πρότυπο ISO 15961: Radio Frequency Identification for Item Management- Πρωτόκολλο Δεδομένων: Διεπαφή εφαρμογής. Για τον μοναδικό αναγνωριστικό κωδικό (EPC), τα χαρακτηριστικά του ορίζονται

στο ανοικτό πρότυπο EPCglobal TDS Tag Data Standard, του οποίου η πιο πρόσφατη έκδοση είναι η Tag Data Standard v.1.6. [25]

2.4.3. Αλγόριθμοι Επικοινωνίας

Οι απλοί RFID αναγνώστες μπορούν να επικοινωνήσουν μόνο με μία ετικέτα κάθε στιγμή. Αν περισσότερες ετικέτες απαντήσουν στον αναγνώστη, τότε εκείνος δεν θα μπορέσει να διαβάσει καμία από αυτές τις ετικέτες, λόγω σύγκρουσης. Για να αντιμετωπιστεί αυτό το πρόβλημα έχουν προταθεί, κυρίως, δύο τεχνικές απομόνωσης, οι οποίες επιτρέπουν στον αναγνώστη να επικοινωνήσει διαδοχικά με όλες τις ετικέτες: ο αλγόριθμος διάσχισης δυαδικού δένδρου που συναντάται κυρίως στις UHF συχνότητες και μία παραλλαγή του αλγόριθμου Aloha που συναντάται κυρίως στις HF συχνότητες. [25]

Αλγόριθμος Διάσχισης Δυαδικού Δένδρου (Binary Tree-Walking)

Η Διάσχιση Δυαδικών Δένδρων επιτρέπει την αναγνώριση μεμονωμένων ετικετών χρησιμοποιώντας μία διαδικασία bit προς bit ερωτημάτων. Απαιτείται από τον αναγνώστη να μεταδώσει το πρόθεμα, δηλαδή τα αρχικά bits του μοναδικού αναγνωριστικού της ετικέτας που θέλει να διαβάσει. Το πλήθος των bits που πρέπει να μεταδώσει εξαρτάται από το πλήθος των συγκρούσεων που θα εντοπίσει. Για παράδειγμα, αν υπάρχουν δύο ετικέτες που διαφέρουν μόνο στα τρία τελευταία bits του αναγνωριστικού τους, τότε για να επιλέξει ο αναγνώστης τη μία από τις δύο, θα πρέπει να μεταδώσει όλα τα αρχικά bits μέχρι και το προτελευταίο. [25]

Αλγόριθμος Aloha

Αντίθετα με τον αλγόριθμο διάσχισης δυαδικού δένδρου, στον αλγόριθμο Aloha κάθε ετικέτα καθυστερεί κατά ένα τυχαίο χρονικό διάστημα σε σχέση με το σήμα του αναγνώστη, προτού απαντήσει σ' ένα ερώτημα. Αν συμβεί σύγκρουση, ο αναγνώστης ενημερώνει τις ετικέτες που βρίσκονται εντός της εμβέλειάς του και τις αναγκάζει να καθυστερήσουν για ένα ακόμη τυχαίο χρονικό διάστημα προτού απαντήσουν. Ο αναγνώστης δεν χρειάζεται να εκπέμψει κάποια σημαντική πληροφορία, καθώς το μόνο που μεταδίδεται από πλευράς αναγνώστη είναι εντολές. [25]

2.5. PKI-Υποδομή Δημόσιου Κλειδιού

Η *Υποδομή Δημόσιου Κλειδιού (PKI-Public Key Infrastructure*) είναι ένα σύνολο μηχανισμών ψηφιακής κρυπτογράφησης, το οποίο επιτρέπει την επικύρωση των δεδομένων ως προς την γνησιότητά τους και εμφανίζει οποιαδήποτε αλλαγή, προσθήκη ή διαγραφή στο chip των ηλεκτρονικών διαβατηρίων. Η PKI "κλειδώνει" τα δεδομένα, τα οποία έτσι προστατεύονται από οποιαδήποτε τροποποίηση, ενώ απαιτείται από την παθητική αυθεντικοποίηση, ώστε να διασφαλίζεται ο έλεγχος της ψηφιακής υπογραφής που πιστοποιεί την αυθεντικότητα των δεδομένων που περιέχονται στην LDS δομή του διαβατηρίου. Οι θεμελιώδεις μηχανισμοί του PKI είναι:

- ο έλεγχος αυθεντικότητας
- ο έλεγχος ακεραιότητας
- η διατήρηση εμπιστευτικότητας

Μέσω της Υποδομής Δημόσιου Κλειδιού, οι συνοριακές αρχές μπορούν να επιβεβαιώσουν ότι:

- το συγκεκριμένο διαβατήριο έχει εκδοθεί από εξουσιοδοτημένη αρχή.
- οι βιογραφικές και βιομετρικές πληροφορίες που βρίσκονται μέσα στο διαβατήριο δεν έχουν τροποποιηθεί.
- δεδομένης της ύπαρξης ενεργής αυθεντικοποίησης και /ή αυθεντικοποίησης του chip, οι πληροφορίες του διαβατηρίου δεν αποτελούν αντίγραφο, όπως κλώνος.
- αν το διαβατήριο έχει δηλωθεί απολεσθέν ή έχει ακυρωθεί, ο έλεγχος ταυτοποίησης μπορεί να επιβεβαιώσει αν το διαβατήριο παραμένει στην κατοχή του προσώπου για το οποίο έχει εκδοθεί.

Ως αποτέλεσμα, οι αρχές έκδοσης διαβατηρίων μπορούν να έχουν καλύτερο έλεγχο των διαβατηρίων που κυκλοφορούν και να αποσύρουν από την κυκλοφορία πλαστά έγγραφα. Η ταυτοποίηση των ηλεκτρονικών διαβατηρίων αποτελεί έναν πολύ σημαντικό παράγοντα για την βελτίωση της αεροπορικής ασφάλειας παγκοσμίως. [26]

Κάθε χώρα υλοποιεί τη δικιά της Υποδομή Δημόσιου Κλειδιού η οποία είναι αυτόνομη και αποκλειστικά υπεύθυνη για την έκδοση των διαβατηρίων των πολιτών της. Ωστόσο, κάθε χώρα οφείλει να ενημερώνεται για τα δημόσια κλειδιά και τις λίστες ανάκλησης όλων των άλλων χωρών και να ενημερώνει έγκαιρα τα τερματικά της για τον καλύτερο έλεγχο των διαβατηρίων.

Δημιουργώντας την Υποδομή Δημόσιου Κλειδιού μιας χώρας

Οι τομείς στους οποίους πρέπει να επικεντρωθεί η Υποδομή Δημόσιου Κλειδιού είναι:

1. η υιοθέτηση των σωστών αρχιτεκτονικών εμπιστοσύνης, η οποία αποτελείται από δύο επίπεδα: την βασική Αρχή Πιστοποίησης της χώρας και μία υποδεέστερη Αρχή Πιστοποίησης εγγράφων, η οποία υπογράφει τα δεδομένα του διαβατηρίου, όπως και το δημόσιο κλειδί (Κλειδί Ενεργής Αυθεντικοποίησης) που αποθηκεύεται σε

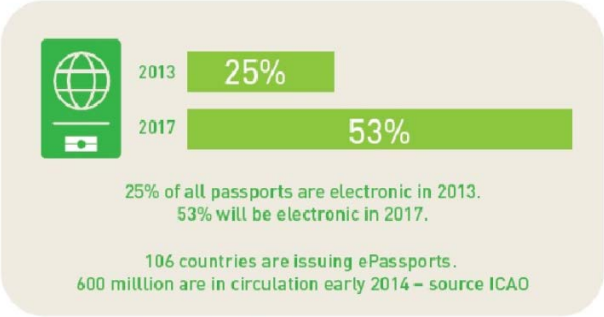
κάθε διαβατήριο και με αυτόν τον τρόπο παρέχεται ένα είδος πιστοποιητικού ταυτότητας για τον κάθε πολίτη.

2. η ύπαρξη νομικής υποδομής των παρόχων πιστοποίησης, όπως ότι η Αρχή Πιστοποίησης της χώρας να ακολουθεί τον Ευρωπαϊκό νόμο που διέπει όλες τις Αρχές που παρέχουν υψηλού επιπέδου ψηφιακές υπογραφές.
3. η διαχείριση κλειδιού και πιστοποιητικού. Ο ICAO τυποποιεί τον τρόπο διαχείρισης του κλειδιού και του πιστοποιητικού.
4. η διαλειτουργικότητα και η τεχνολογία που χρησιμοποιείται.

Ο κύκλος ζωής ενός κλειδιού που εκδίδεται από την βασική Αρχή Πιστοποίησης μίας χώρας δεν θα πρέπει να είναι μεγαλύτερος από:

- την διάρκεια της περιόδου κατά την οποία χρησιμοποιείται για την έκδοση διαβατηρίων
- την διάρκεια ζωής ενός διαβατηρίου, το οποίο έχει εκδοθεί με το συγκεκριμένο κλειδί.

Για να μεγιστοποιηθεί η ασφάλεια, ο ICAO προτείνει στις χώρες να αντικαθιστούν το κλειδί αυτό κάθε 3-5 χρόνια, ενώ οι λίστες ανάκλησης πρέπει να ενημερώνονται κάθε ενενήντα μέρες τουλάχιστον.



Χρήση των ηλεκτρονικών διαβατηρίων

Πηγή: Looking at the future of travel, The Fourth Generation of e-passport, June 2014,Gemalto

Κεφάλαιο 3

Ηλεκτρονικές Ταυτότητες

3.1. Τι είναι οι ηλεκτρονικές ταυτότητες (eID's)

Στο προηγούμενο κεφάλαιο μελετήθηκε μία ειδική περίπτωση εφαρμογής ηλεκτρονικής ταυτοποίησης και αυθεντικοποίησης, αυτή των ηλεκτρονικών διαβατηρίων. Στο παρόν κεφάλαιο θα εστιάσουμε γενικότερα στις τεχνολογίες ηλεκτρονικής ταυτότητας για αξιοποίηση υπηρεσιών Ηλεκτρονικής Διακυβέρνησης. Οι τεχνολογίες αυτές οδηγούν στη λεγόμενη ηλεκτρονική ταυτότητα, δηλαδή στο σύνολο των μέσων που χρησιμοποιεί ο χρήστης στο ψηφιακό κόσμο για να ταυτοποιείται, πέραν κάθε αμφιβολίας, από παρόχους υπηρεσιών Η.Δ. Η ηλεκτρονική ταυτότητα, αναπόφευκτα, εγείρει ζητήματα ιδιωτικότητας αφού ο κάτοχός της, για να αποδείξει το ποιος είναι, πρέπει να «αποκαλύψει»

κάποια προσωπικά του στοιχεία. Πριν μελετήσουμε τις τεχνολογικές δυνατότητες για ενίσχυση της ιδιωτικότητας, όπως η τεχνολογία ABC που μελετάται στο επόμενο κεφάλαιο, θα παρουσιάσουμε τον ορισμό και τις βασικές έννοιες των ηλεκτρονικών ταυτοτήτων και τον τρόπο και το εύρος χρήσης τους στα πλαίσια της Ηλεκτρονικής Διακυβέρνησης στην Ε.Ε.

Η *ηλεκτρονική ταυτότητα (e-Identity Card)* ή αλλιώς *Κάρτα Πολίτη* είναι μία κάρτα που εκδίδεται από την Πολιτεία και παρέχει έναν καθολικό μηχανισμό για τον έλεγχο ταυτότητας του χρήστη, την ταυτοποίηση και την αναγνώρισή του. Για την υλοποίησή της, συλλέγονται οι πληροφορίες από την φυσική ταυτότητα του κατόχου της και ενσωματώνονται σε μια πλαστική κάρτα που περιλαμβάνει ένα πλινθίο, το οποίο αποδίδει στην κάρτα την ηλεκτρονική της υπόσταση.

Οι ηλεκτρονικές ταυτότητες, στα περισσότερα κράτη - μέλη της Ε.Ε. εκδίδονται από τις Αρχές, ενώ σε κάποιες χώρες εκδίδονται από τον ιδιωτικό τομέα υπό την ευθύνη των Αρχών (π.χ. Αυστρία, Σουηδία).

Σύμφωνα με τους Fiat και Shamir [27], τα τρία βασικά στοιχεία που προστατεύουν οι ηλεκτρονικές κάρτες είναι:

1. Ταυτοποίηση
2. Αυθεντικοποίηση
3. Υπογραφή

Σε επίπεδο Ε.Ε., σκοπός των Αρχών, μέσω των ηλεκτρονικών καρτών, είναι:

- Να αντιμετωπίσουν και να ανακαλύψουν τις κοινές απάτες
- Να αντιμετωπίσουν την τρομοκρατία σε εθνικό και ευρωπαϊκό επίπεδο
- Να δημιουργήσουν ένα ενιαίο πλαίσιο ηλεκτρονικής αναγνώρισης των πολιτών εντός της Ευρωπαϊκής Ένωσης
- Να δημιουργήσουν νέες ενδοευρωπαϊκές υπηρεσίες για να μειώσουν το κόστος των υποδομών.

Όσον αφορά τους πολίτες, με την ανάπτυξη των υπηρεσιών Ηλεκτρονικής Διακυβέρνησης, έγινε απαραίτητη η δυνατότητα να μπορούν να ταυτοποιηθούν διαδικτυακά. Με αυτόν τον τρόπο, έχουν την πρόσβαση σε διαδικτυακές υπηρεσίες του Δημοσίου, μέσω των οποίων, αφού πιστοποιείται η ταυτότητά τους, μπορούν να κάνουν συναλλαγές με δημόσιες υπηρεσίες.

Με σκοπό να ταυτοποιηθεί για να κάνει χρήση υπηρεσιών Η.Δ., ένας χρήστης πρέπει να αποδείξει ότι έχει στην κατοχή του διαπιστευτήρια που συνδέουν την φυσική του ταυτότητα με τον συγκεκριμένο λογαριασμό. Αυτή η διαδικασία είναι η *αυθεντικοποίηση* του χρήστη.

Από την σκοπιά της τεχνολογίας, οι ηλεκτρονικές κάρτες διακρίνονται σε:

- αυτές που βασίζονται σε συστήματα κωδικών ή συνθηματικών (Password-Based)
- αυτές που βασίζονται σε Υποδομή Δημόσιου Κλειδιού
- αυτές που βασίζονται στην τεχνολογία ABC (αναλύονται στο επόμενο κεφάλαιο).

3.1.1. Ψηφιακά Πιστοποιητικά

Το *ψηφιακό πιστοποιητικό (digital certificate)* αποτελεί ένα είδος ταυτότητας και περιέχει στοιχεία του κατόχου του, καθώς και μία βεβαίωση κάποιας αρχής που πιστοποιεί την ακρίβειά τους.

Ένα ψηφιακό πιστοποιητικό αποτελείται από τρία βασικά στοιχεία:

1. Ένα δημόσιο κλειδί
2. Πληροφορίες του πιστοποιητικού
3. Ψηφιακή υπογραφή, της οποίας σκοπός είναι να επικυρώσει ότι τα στοιχεία που περιλαμβάνει πηγαίνουν μαζί με το δημόσιο κλειδί.

Έτσι, ένα πιστοποιητικό είναι στην ουσία ένα δημόσιο κλειδί μαζί με τα στοιχεία του κατόχου του και μια σφραγίδα έμπιστης οντότητας που επικυρώνει αυτήν την σύνδεση. Το πιο αντιπροσωπευτικό ψηφιακό πιστοποιητικό είναι το τύπου X.509.

Για την υλοποίηση αποτελεσματικών ηλεκτρονικών ταυτοτήτων χρησιμοποιούνται οι *Υποδομές Δημόσιου Κλειδιού (PKI),* οι οποίες υποστηρίζουν την ταυτοποίηση πιστοποιητικών, παρέχουν την δυνατότητα αποθήκευσής τους και την δυνατότητα παροχής υπηρεσιών και πρωτοκόλλων διαχείρισής τους. Αυτά τα πρωτόκολλα περιλαμβάνουν εκτός των άλλων και την δυνατότητα έκδοσης και ανάκλησης ενός πιστοποιητικού.

Το πιο σημαντικό στοιχείο της Υποδομής Δημόσιου Κλειδιού (βλ. και προηγούμενο κεφάλαιο) είναι η *Αρχή Πιστοποίησης (Certification Authority - CA).*

Μια Αρχή Πιστοποίησης δημιουργεί πιστοποιητικά και τα υπογράφει με το ιδιωτικό της κλειδί. Εξαιτίας του ρόλου της στην δημιουργία των πιστοποιητικών, η Αρχή Πιστοποίησης αποτελεί το βασικό συστατικό μιας PKI. Μπορούμε να επαληθεύσουμε την αυθεντικότητα ενός πιστοποιητικού χρησιμοποιώντας το δημόσιο κλειδί της Αρχής Πιστοποίησης για επαλήθευση.

Δεν μπορούμε να παραβλέψουμε την αδυναμία των ψηφιακών πιστοποιητικών δημόσιου κλειδιού, ότι είναι ανιχνεύσιμα και αυτό οφείλεται στο δημόσιο κλειδί και στην υπογραφή που περιλαμβάνονται σε αυτό. Πιο συγκεκριμένα, το δημόσιο κλειδί μπορεί να χρησιμοποιηθεί ως μοναδικό αναγνωριστικό για τον χρήστη και περιλαμβάνεται στην υπογραφή, η οποία, επίσης, μπορεί να επαληθευτεί.

3.2. Ηλεκτρονικές ταυτότητες και Ευρωπαϊκή Ένωση.

Οι περισσότερες ευρωπαϊκές χώρες ήδη αναπτύσσουν ή έχουν αναπτύξει ηλεκτρονικές ταυτότητες για εφαρμογές Ηλεκτρονικής Διακυβέρνησης. Όμως παρουσιάζεται μεγάλη ποικιλία εφαρμογών ηλεκτρονικών καρτών, από τις παραδοσιακές με χρήση συνδυασμού username-password, μέχρι τις περίπλοκες έξυπνες κάρτες (smart cards). Από τριάντα μία (31) ευρωπαϊκές χώρες, οι δεκαεπτά (17) υλοποιούν ηλεκτρονικές κάρτες που βασίζονται σε password-based συστήματα, είκοσι έξι (26) έχουν υλοποιήσει υποδομή Δημόσιου Κλειδιού και μία (η Γερμανία- την οποία θα δούμε παρακάτω) χρησιμοποιεί την τεχνολογία ABC. [28] Επίσης, δεκαεπτά (17) κράτη - μέλη της Ε.Ε. συμμετέχουν στο έργο STORK [29], το οποίο έχει αποδείξει ότι οι ηλεκτρονικές ταυτότητες μπορούν εύκολα να αναγνωριστούν σε άλλες χώρες. Σχεδόν όλα τα πεδία εφαρμογών των ηλεκτρονικών ταυτοτήτων στις χώρες της Ε.Ε. σχετίζονται με υπηρεσίες του Δημόσιου Τομέα, ενώ ο πιο αποτελεσματικός φορέας θεωρείται αυτός ο οποίος προσφέρει ένα είδος εισφοράς προς το Δημόσιο, όπως η είσπραξη φόρων. Άλλες εφαρμογές Η.Δ. περιλαμβάνουν: [30]

- Επιβεβαίωση ηλικίας
- Προσωπικά δεδομένα
- Ηλεκτρονική Ψηφοφορία (e-voting), το οποίο ήδη υλοποιείται στην Εσθονία
- Ασφαλές ηλεκτρονικό ταχυδρομείο, το οποίο ήδη στην Εσθονία κάθε πολίτης έχει στην κατοχή του εκτός από την κάρτα πολίτη.

Η Εσθονία θεωρείται, γενικότερα, ένα πολύ ενδιαφέρον παράδειγμα προς μίμηση σε σχέση με την ραγδαία ανάπτυξη υπηρεσιών Ηλεκτρονικής Διακυβέρνησης την τελευταία πενταετία.

Όσον αφορά την πρόοδο ως προς την Ηλεκτρονική Διακυβέρνηση, σύμφωνα με την έκθεση των Ηνωμένων Εθνών για το 2014 (E-

Government for the future we want), [31] αρκετά κράτη - μέλη της Ε.Ε. βρίσκονται στις πρώτες θέσεις στον πίνακα με την μεγαλύτερη πρόοδο και ανάπτυξη σε συστήματα ηλεκτρονικής ταυτοποίησης και διακυβέρνησης, όπως η Γαλλία, η Ολλανδία, η Φινλανδία.

Η πρώτη χώρα της Ε.Ε. που υιοθέτησε την χρήση της ηλεκτρονικής κάρτας πολίτη ήταν το 2001 -πιλοτικά μέχρι το 2009 όταν και έγινε υποχρεωτική η χρήση της- το Βέλγιο. Σύμφωνα με την έκθεση των Ηνωμένων Εθνών για το 2014 (E-Government for the future we want), [31] το Βέλγιο βρίσκεται στις πρώτες θέσεις της παγκόσμιας κατάταξης σε σχέση με την μεγαλύτερη πρόοδο και ανάπτυξη σε συστήματα ηλεκτρονικής διακυβέρνησης.

3.2.1. Η γερμανική ηλεκτρονική ταυτότητα

Από το 2010 η γερμανική ταυτότητα είναι ηλεκτρονική, ονομάζεται *"neuer Personalausweis" (nPa)*, εκδίδεται από τοπικά εξουσιοδοτημένα γραφεία, ενώ έχει ισχύ δέκα (10) χρόνια.

Η γερμανική ηλεκτρονική ταυτότητα μπορεί να χρησιμοποιηθεί για ασφαλείς οικονομικές συναλλαγές στο Διαδίκτυο, για συναλλαγές σε υπηρεσίες Ηλεκτρονικής Διακυβέρνησης και ως ταξιδιωτικό έγγραφο.

Η γερμανική ηλεκτρονική ταυτότητα περιέχει ένα τσίπ RFID παρόμοιο με αυτό των ηλεκτρονικών διαβατηρίων. Αυτό το τσιπ περιέχει τις πληροφορίες που αναγράφονται στην ταυτότητα, την φωτογραφία του κατόχου (είναι βιομετρική) και επιπλέον, αν ο χρήστης επιθυμεί, τα δακτυλικά του αποτυπώματα. Η γερμανική ηλεκτρονική ταυτότητα περιέχει τις παρακάτω πληροφορίες:

- Βιομετρική φωτογραφία
- Αριθμός ταυτότητας
- Κωδικός πρόσβασης του RFID τσιπ

- Επίθετο
- Όνομα
- Ημερομηνία Γέννησης
- Εθνικότητα
- Τόπος Γέννησης
- Ημερομηνία λήξης
- Υπογραφή κατόχου
- Χρώμα ματιών
- Ύψος
- Ημερομηνία έκδοσης
- Εκδούσα Αρχή
- Διεύθυνση κατοικίας
- Θρησκευτικό όνομα ή ψευδώνυμο
- Machine Readable Zone (MRZ)

Η γερμανική κάρτα πολίτη μαζί με την αυστριακή Bürgerkarte διακρίνονται για την ιδιωτικότητα που προσφέρουν στους πολίτες. Η γερμανική κάρτα πολίτη μεταφράζει την ιδιωτικότητα σε ένα σύνολο χαρακτηριστικών: Το πιο σημαντικό είναι ότι οι υπηρεσίες οφείλουν να αυθεντικοποιούνται στους πολίτες. Η δυνατότητα επιλογής συγκεκριμένων χαρακτηριστικών, ώστε να ελέγχει ο πολίτης την μετάδοση των δεδομένων του είναι , επίσης, πολύ σημαντική. Έτσι, οι πολίτες δίνουν την συγκατάθεσή τους σε κάθε πρόσβαση προσωπικών δεδομένων τους. Η online επιβεβαίωση υποστηρίζει χρήσεις όπως, την επιβεβαίωση ηλικίας, ενώ ταυτόχρονα δημοσιοποιεί ελάχιστες πληροφορίες. Τέλος, δίνεται η δυνατότητα μέσω της τεχνολογίας Privacy-ABC's - η οποία αναπτύσσεται στο επόμενο κεφάλαιο- για δημιουργία ψευδωνύμων, τα οποία είναι ασύνδετα μεταξύ τους. Αυτήν η τεχνολογία προσφέρει στην γερμανική κάρτα πολίτη τα εξής πλεονεκτήματα σε σχέση με κάρτες άλλων ευρωπαϊκών χωρών:

- Τα Privacy-ABC's δεν αφήνουν "ίχνη".
- Εμποδίζουν την κλοπή ταυτότητας

- Αντί για απόλυτη ανωνυμία, μπορούν να προσφέρουν, αν επιθυμείται, απεριόριστος αριθμός ψευδωνύμων τα οποία μπορούν να χρησιμοποιηθούν.

Έτσι, η τεχνολογία Privacy-ABC's προσφέρει σημαντικές δυνατότητες στους Γερμανούς πολίτες, μιας και αυξάνει τις λειτουργίες ιδιωτικότητας στην υπάρχουσα γερμανική ηλεκτρονική ταυτότητα. Με αυτόν τον τρόπο, οι Γερμανοί πολίτες έχουν την δυνατότητα να αποδείξουν χαρακτηριστικά της ταυτότητάς τους, ενώ ταυτόχρονα διατηρούν την ανωνυμία τους όταν αυτό απαιτείται. [32]

3.2.2. Η αυστριακή ηλεκτρονική ταυτότητα

Η Αυστρία είναι μία από τις πρώτες χώρες της Ε.Ε. που υλοποιήσανε την κάρτα πολίτη, το 2004, η οποία ονομάζεται *"Bürgerkarte"* και παρουσιάζει υψηλά επίπεδα χρήσης των υπηρεσιών Ηλεκτρονικής Διακυβέρνησης από τους πολίτες της. Η υλοποίηση της αυστριακής κάρτας βασίζεται σε Υποδομή Δημόσιου Κλειδιού, ενώ η αυθεντικοποίηση του κατόχου της κάρτας βασίζεται σε Password Based σύστημα. Επιπλέον, δεν είναι μια ταυτότητα ίδια για όλους τους πολίτες, όπως το διαβατήριο, αλλά αποτελεί μία ιδέα σχεδίασης ασφαλών ηλεκτρονικών δημόσιων υπηρεσιών. Επίσης, η αυστριακή ταυτότητα έχει την δυνατότητα να υλοποιηθεί σε διάφορες τεχνολογικές πλατφόρμες, όπως κινητά τηλέφωνα και USB sticks. [33]

Η Αυστρία υποστηρίζει την διαλειτουργικότητα για ηλεκτρονικές κάρτες προερχόμενες από Βέλγιο, Εσθονία, Φινλανδία και Ιταλία χρησιμοποιώντας την τεχνολογία MOA (Module for Online Application). Η διαχείριση των πολιτών πραγματοποιείται από το Κεντρικό Μητρώο Κατοίκων, ενώ η κάρτα έχει τα εξής χαρακτηριστικά:

- Πρόσβαση σε υπηρεσίες Ηλεκτρονικής Διακυβέρνησης

- Υποστήριξη μηχανισμού μοναδικών αναγνωριστικών (Source PIN)
- Ψηφιακό Πιστοποιητικό
- Αποθήκευση ελάχιστης πληροφορίας
- Ισχυρή κρυπτογράφηση μέσω MOA (Module for Online Application) για αναγνώριση, υπογραφή εξυπηρετητών, πιστοποίηση υπογραφής και ηλεκτρονική παράδοση.

Το πιο βασικό χαρακτηριστικό της αυστριακής κάρτας πολίτη είναι η *μη συνδεσιμότητα (unlinkability),* η οποία πηγάζει από ένα σύστημα που παράγει ασφαλή, συγκεκριμένου τομέα ψηφιακά πιστοποιητικά για διαφορετικές εφαρμογές ηλεκτρονικής διακυβέρνησης, το οποίο έχει προσελκύσει το ενδιαφέρον απ' όλη την Ευρώπη. Επίσης, η βάση της αυστριακής ηλεκτρονικής ταυτοποίησης είναι ένα πηγαίο PIN (Personal Identification Number) το οποίο είναι μυστικό και αποκλειστικού ελέγχου από τον πολίτη. [34]

Όσον αφορά την ιδιωτικότητα και την προστασία των δεδομένων που παρέχει η αυστριακή κάρτα πολίτη, θεωρείται η καλύτερη στην Ε.Ε. και για αυτό τον λόγο, τον Δεκέμβριο 2005, πήρε το βραβείο για την καλύτερη υλοποίηση ηλεκτρονικής ταυτότητας από την ισπανική Αρχή Προστασίας Δεδομένων. [33]

3.3. Ηλεκτρονικές ταυτότητες και Ιδιωτικότητα

Η ηλεκτρονική ταυτότητα λόγω των πληροφοριών που περιέχει για τον πολίτη, συνεπάγεται μια σειρά από απειλές κατά της ιδιωτικότητας, με την ανεπιθύμητη αποκάλυψη των προσωπικών πληροφοριών και την επακόλουθη κακή χρήση. [32]

Επιπλέον, είναι πολύ πιθανό να αυξηθούν οι μελλοντικοί κίνδυνοι, αν οι πολίτες χρησιμοποιούν τις ηλεκτρονικές τους ταυτότητες, όχι μόνο για υπηρεσίες ηλεκτρονικής διακυβέρνησης, αλλά και στο ηλεκτρονικό εμπόριο και σε τραπεζικές συναλλαγές. Ένα άλλο ζήτημα αποτελεί η

δυσπιστία που έχουν οι πολίτες ως προς το ποια προσωπικά τους δεδομένα υφίστανται επεξεργασία και από ποιους, γεγονός που τους αποθαρρύνει από την χρήση ενός τέτοιου συστήματος. Αυτό καθιστά την προστασία της ιδιωτικής ζωής απαραίτητη σε χώρες όπου η ταυτότητα είναι προαιρετική, αλλά ακόμη και όταν η κατοχή της είναι υποχρεωτική, οι κίνδυνοι για την ιδιωτικότητα θα επηρεάσουν τη χρήση της κάρτας και θα μειώσουν τη δημοτικότητά της, κάνοντας την επιβολή των όποιων υποχρεώσεων πιο δύσκολη. [35]

Μια ηλεκτρονική κάρτα περιλαμβάνει, σύμφωνα με την έρευνα που δημοσιεύτηκε από τον ENISA [35], τον έλεγχο για την αποκάλυψη πληροφοριών σε κακόβουλους χρήστες ή σε ανθρώπους που έχουν παράνομα στην κατοχή τους την κάρτα, με ακούσια ταυτοποίηση του κατόχου της κάρτας, μέσω της συνδεσιμότητας συμβάντων επαλήθευσης ταυτότητας, τη διαρροή των δεδομένων σε περιστασιακούς παρατηρητές και τη νόμιμη γνωστοποίηση του ιδιοκτήτη των δεδομένων με υψηλή διασφάλιση, λόγω της χρήσης της ψηφιακής υπογραφής ως διακριτικό ελέγχου ταυτότητας. Το βασικότερο πρόβλημα σε εθνικό επίπεδο αποτελεί η έλλειψη συντονισμού σε κάθε διασυνοριακή λειτουργία των ηλεκτρονικών καρτών ακόμα και σε τεχνικό επίπεδο, όπως χαρακτηριστικές προδιαγραφές της κάρτας μίας χώρας μπορεί να μην υπάρχουν σε κάρτα άλλης χώρας. Για παράδειγμα, η Αυστρία υποστηρίζει την διαλειτουργικότητα για ηλεκτρονικές κάρτες προερχόμενες μόνο από Βέλγιο, Εσθονία, Φινλανδία και Ιταλία χρησιμοποιώντας την τεχνολογία MOA (Module for Online Application).

Το πιο σημαντικό είναι η δημιουργία αναγκαίας εμπιστοσύνης στους χρήστες σε κάθε διασυνοριακό πρόγραμμα για να συμμετέχουν σε αυτό και πιο αδύναμα μέλη, έτσι ώστε όλες οι χώρες να προσφέρουν το ίδιο επίπεδο προστασίας και ασφάλειας.

Κεφάλαιο 4

Πιστοποιητικά βάσει Χαρακτηριστικών

Μέχρι τώρα, θεωρήσαμε ότι με τις ηλεκτρονικές ταυτότητες ο κάτοχός τους ταυτοποιείται πλήρως στις υπηρεσίες Η.Δ. τις οποίες αιτείται. Ωστόσο, για να το επιτύχει αυτό αποκαλύπτει κάποια προσωπικά του στοιχεία. Το κρίσιμο ερώτημα που ανακύπτει, από τη σκοπιά της ιδιωτικότητας, είναι το εξής: τα στοιχεία που αποκαλύπτει ο χρήστης είναι τα απολύτως απαραίτητα για να ταυτοποιηθεί ή μήπως αποκαλύπτει περισσότερα από ό,τι χρειάζεται[1]; Μάλιστα, υπάρχουν περιπτώσεις ηλεκτρονικών

[1] Η αρχή της ελαχιστοποίησης των δεδομένων αποτελεί άλλωστε νομική επιταγή για την προστασία των προσωπικών δεδομένων (βλ. και Κεφάλαιο 5)

υπηρεσιών όπου δεν χρειάζεται ούτε καν να ταυτοποιηθεί πλήρως ο χρήστης παρά μόνο να διασφαλιστεί ότι έχει κάποιο συγκεκριμένο γνώρισμα – π.χ. ότι είναι ενήλικος (άνω των 18).

Επ' αυτής της βάσης, αναπτύχθηκαν ειδικού τύπου ψηφιακά πιστοποιητικά για να αντιμετωπίσουν αυτό ακριβώς το ζήτημα. Τα πιστοποιητικά αυτά, που συνοδεύονται από τις αντίστοιχες τεχνολογίες, λέγονται πιστοποιητικά βάσει χαρακτηριστικών (Attribute Based Credentials – εφεξής ABC), και αποτελούν το αντικείμενο αυτού του κεφαλαίου.

4.1. Ιδιότητες και Πιστοποιητικά

Χαρακτηρίζουμε ως *Ιδιότητα ή χαρακτηριστικό (attribute)* μία πληροφορία ή μία κατάσταση που αφορά ένα άτομο. Παραδείγματα ιδιοτήτων αποτελούν τα παρακάτω:

- Είμαι μαθητής
- Είμαι άνω των 65 ετών
- Το φύλο μου είναι άρρεν/θήλυ
- Η διεύθυνσή μου είναι .....
- Η ημερομηνία γέννησής μου είναι .....
- Το ΑΜΚΑ μου είναι ....

Παρατηρούμε και από τα παραδείγματα ότι μερικές ιδιότητες, όπως το ΑΜΚΑ χαρακτηρίζουν μοναδικά ένα άτομο, ενώ άλλες ιδιότητες, όπως το φύλο, χαρακτηρίζουν και άλλους ανθρώπους. Ουσιαστικά, η ταυτότητα ενός ατόμου αποτελεί μία συλλογή ιδιοτήτων για το συγκεκριμένο άτομο. Πρακτικά, πολλές συναλλαγές βασίζονται σ' ένα ελάχιστο σύνολο ιδιοτήτων και πιο συγκεκριμένα σε αυτές που απαιτούνται για την ολοκλήρωση μιας συναλλαγής.

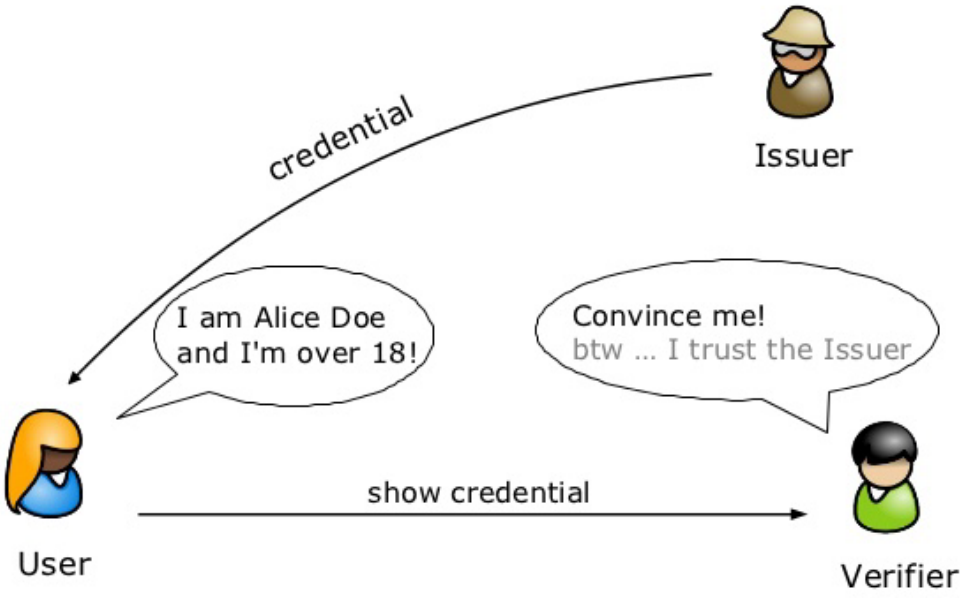
Υπάρχουν διάφορα κρυπτογραφικά συστήματα τα οποία χρησιμοποιούν ταυτότητες που βασίζονται σε ιδιότητες. Αυτά τα συστήματα διακρίνουν τις ιδιότητες από τα πιστοποιητικά.

Πιστοποιητικό είναι ένα σύνολο ιδιοτήτων που χαρακτηρίζει το άτομο. Παραδείγματα πιστοποιητικών αποτελούν τα παρακάτω:

- Ένα πιστοποιητικό διεύθυνσης που περιλαμβάνει την οδό, τον αριθμό, τον ταχυδρομικό κώδικα, την πόλη, την χώρα ως ιδιότητες.
- Ένα πιστοποιητικό ταυτότητας που περιλαμβάνει το όνομα, το γένος, την ημερομηνία γέννησης, τον ΑΜΚΑ ως ιδιότητες.

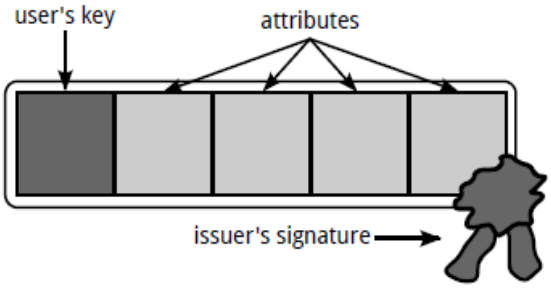
Τέτοιο κλασσικό παράδειγμα είναι η ταυτότητα ή το δίπλωμα οδήγησης. Μία πολύ σημαντική καινοτομία της τεχνολογίας ABC είναι ότι δεν βασίζεται στην ταυτότητα ή στο δίπλωμα οδήγησης, όπως αναφέρθηκε παραπάνω, αλλά σε συγκεκριμένα χαρακτηριστικά του ατόμου, τα οποία μπορεί να χαρακτηρίζουν και άλλους ανθρώπους. Για παράδειγμα, όταν το άτομο θέλει να αγοράσει ένα μπουκάλι με αλκοολούχο ποτό, θα πρέπει να επιδείξει στον πωλητή το χαρακτηριστικό ότι είναι άνω των 18 ετών. Αυτό το χαρακτηριστικό, στην συγκεκριμένη περίπτωση αποδεικνύεται από την ημερομηνία γέννησης η οποία αναγράφεται στην ταυτότητα. Όμως τον πωλητή δεν τον ενδιαφέρουν τα υπόλοιπα στοιχεία της ταυτότητας, παρά μόνο η ημερομηνία γέννησης ώστε να ελέγξει αν η συναλλαγή είναι νόμιμη ή όχι. Με άλλα λόγια, η τεχνολογία που είναι βασισμένη σε ABC αποσκοπεί στην αποκάλυψη, κάθε φορά, της απολύτως απαραίτητης πληροφορίας που χρειάζεται, προκειμένου να παρασχεθεί σε ένα χρήστη η υπηρεσία που αιτείται.

Τα πιστοποιητικά εκδίδονται και επιβεβαιώνονται, ενώ οι ιδιότητες αποδεικνύονται κατά τη διάρκεια της επιβεβαίωσης. Το πιστοποιητικό εκδίδεται από μία *Αρχή Έκδοσης (Issuer)* η οποία επιβεβαιώνει ότι οι ιδιότητες του πιστοποιητικού χαρακτηρίζουν τον κάτοχό του. Στη συνέχεια, εκείνος μπορεί να χρησιμοποιήσει το πιστοποιητικό για να αποδείξει ότι κατέχει συγκεκριμένες ιδιότητες-ικανότητες.



Αυθεντικοποίηση του χρήστη με χρήση πιστοποιητικών

Η Αρχή έκδοσης και ο χρήστης κατασκευάζουν μαζί ένα νέο πιστοποιητικό μέσω της ίδιας διαδικασίας. Πρώτα ο χρήστης αυθεντικοποιείται στην Αρχή έκδοσης, ενώ η Αρχή έκδοσης μόλις επιβεβαιώσει την αυθεντικοποίηση του χρήστη, συλλέγει ιδιότητες για τον χρήστη από έμπιστες πηγές. Στη συνέχεια, ο χρήστης και η Αρχή έκδοσης χρησιμοποιούν ένα κρυπτογραφικό πρωτόκολλο στο οποίο οι ιδιότητες συνδυάζονται σ' ένα πιστοποιητικό υπογεγραμμένο από την Αρχή έκδοσης. Το πιστοποιητικό αυτό περιλαμβάνει εκτός από τις ιδιότητες του χρήστη και το προσωπικό του κλειδί. Με αυτόν τον τρόπο, οι ιδιότητες του πιστοποιητικού επιβεβαιώνονται τόσο από την Αρχή έκδοσης μέσω της υπογραφής της, όσο και από τον χρήστη μέσω του προσωπικού κλειδιού. [36]



Αναπαράσταση Attribute - Based Credential

4.1.1. Επιλεκτική Γνωστοποίηση Ιδιοτήτων

Ένας χρήστης μπορεί να διαθέτει διάφορα πιστοποιητικά, και το καθένα να περιέχει συλλογή ιδιοτήτων. Όταν ο χρήστης αιτείται μιας υπηρεσίας από έναν πάροχο υπηρεσιών, πρέπει να αυθεντικοποιηθεί χρησιμοποιώντας ένα ή περισσότερα πιστοποιητικά. Κατά την διαδικασία επιβεβαίωσης ο χρήστης μπορεί να επιλέξει ποια πιστοποιητικά θα χρησιμοποιήσει. Επιπλέον, ο χρήστης αποφασίζει ποιες ιδιότητες του πιστοποιητικού θα αποκαλύψει. Με αυτόν τον τρόπο, η αυθεντικοποίηση γίνεται πιο ιδιωτική (αφού είναι στην ευχέρεια του χρήστη να επιλέξει ποια προσωπικά του δεδομένα θα διαβιβάσει/αποκαλύψει). Αυτή η διαδικασία επιβεβαίωσης ονομάζεται *επιλεκτική γνωστοποίηση (selective disclosure)* και περιλαμβάνει ένα πρωτόκολλο επιβεβαίωσης στο οποίο αποκαλύπτονται μόνο οι ιδιότητες του πιστοποιητικού που επέλεξε ο χρήστης, ενώ οι υπόλοιπες απλά υπάρχουν στο πιστοποιητικό χωρίς να φανερώνονται. Με αυτόν τον τρόπο αποδεικνύεται ότι το πιστοποιητικό ανήκει στον συγκεκριμένο χρήστη και ο πάροχος υπηρεσιών επιβεβαιώνει τις πληροφορίες που έχουν σταλεί, συμπεριλαμβανομένου και την υπογραφή της Αρχής έκδοσης.

4.1.2. Χρήση των Πιστοποιητικών βάσει χαρακτηριστικών

Ένα πιστοποιητικό ABC υπογράφεται από έναν εκδότη (issuer) με ειδική ηλεκτρονική υπογραφή (digital signature) για να παρέχει συγκεκριμένες ιδιότητες ιδιωτικότητας και ασφάλειας. Το πιστοποιητικό έχει δύο σημαντικά χαρακτηριστικά:

Πρώτον, η υπογραφή δεν μπορεί να πλαστογραφηθεί και εγγυάται την ακεραιότητα και την αυθεντικότητα των ιδιοτήτων. Αυτό σημαίνει ότι καμία μετατροπή δεν μπορεί να γίνει στις ιδιότητες μετά την έκδοση του πιστοποιητικού.

Δεύτερον, άμεση επιβεβαίωση του πιστοποιητικού πραγματοποιείται, χωρίς να περιλαμβάνονται οι εκδότες, και έτσι δεν μπορεί να συνδεθεί το πιστοποιητικό με τον χρήστη από τον εκδότη, ούτε οι διάφορες περιπτώσεις μπορούν να συνδεθούν με τον καθένα τους.

Τα πιστοποιητικά που βασίζονται στα χαρακτηριστικά χαρακτηρίζονται από την προαναφερθείσα ιδιότητα της *επιλεκτικής γνωστοποίησης* (*selective disclosure*) με την οποία ιδιότητες ενός ή περισσοτέρων πιστοποιητικών μπορούν να αποκαλυφθούν ανεξάρτητα από το καθένα. Ο χρήστης μπορεί να συλλέγει πιστοποιητικά από εκδότες και να τα βάζει σε μία έμπιστη συσκευή, τύπου έξυπνης κάρτας (smart card) με σκοπό να τα αποκαλύψει σε παρόχους υπηρεσιών για επιβεβαίωση και αυθεντικοποίηση ταυτοποιημένων σκοπών. Μετά από αυτήν την εξουσιοδότηση, μία υπηρεσία μπορεί να επιτραπεί ή να αρνηθεί από τον πάροχο ανάλογα με την ύπαρξη του πιστοποιητικού και την αξία των ιδιοτήτων του. Οι υπηρεσίες εξουσιοδότησης παίζουν σημαντικό ρόλο στην σχεδίαση των attribute - based credentials. Αυτές οι υπηρεσίες έχουν το δικαίωμα να:

1. καθορίζουν ποιοι εκδότες θα παρέχουν υπηρεσίες εξουσιοδότησης
2. καθορίζουν ποια πιστοποιητικά και ποιες ιδιότητες θα εκδίδει ο κάθε εκδότης
3. καθορίζουν ποιοι πάροχοι υπηρεσιών μπορούν να είναι μέλη των υπηρεσιών εξουσιοδότησης

4. καθορίζουν σε ποια πιστοποιητικά και σε ποιες ιδιότητες μπορεί ο κάθε πάροχος υπηρεσιών να έχει πρόσβαση
5. καθορίζουν ποιοι χρήστες εκδίδουν έξυπνη κάρτα.

Έτσι, η πλευρά που λειτουργεί ως υπηρεσία εξουσιοδότησης έχει την μεγαλύτερη επιρροή στην εμπιστοσύνη, στην λειτουργία και στους σκοπούς του attribute - based credentials συστήματος.[37]

4.2. Τεχνολογία Πιστοποιητικών βάσει χαρακτηριστικών

Όπως ήδη είδαμε στην παράγραφο 1.4., τα κλασικά διαπιστευτήρια δεν προστατεύουν την ιδιωτικότητα. Τα κλασικά κρυπτογραφικά πιστοποιητικά παρόλο που προσφέρουν επαρκή ασφάλεια για αρκετούς σκοπούς, δεν καλύπτουν τις ανάγκες της ιδιωτικότητας γιατί συνδέονται με ένα υπαρκτό πρόσωπο. Η αποκάλυψη περισσότερων πληροφοριών από τις απαραίτητες όχι μόνο ζημιώνει την ιδιωτικότητα των χρηστών αλλά αυξάνει και το ρίσκο κακής χρήσης των πληροφοριών του, όπως κλοπή ταυτότητας, όταν οι πληροφορίες πέσουν σε λάθος χέρια.

Σε αντίθεση με τα παραπάνω, τα ABC επιτρέπουν στον κάτοχο να αποκαλύψει μόνο την ελάχιστη πληροφορία που απαιτείται από την εφαρμογή, χωρίς να αποκαλύπτουν μια πλήρη ταυτότητα. Έτσι αυτά τα πιστοποιητικά διευκολύνουν την υλοποίηση μιας αξιόπιστης ψηφιακής κοινωνίας που ταυτόχρονα προστατεύει την ιδιωτικότητα.

Τα ABC's εκδίδονται όπως τα κρυπτογραφικά πιστοποιητικά χρησιμοποιώντας ένα ψηφιακό κλειδί υπογραφής. Ένα πιστοποιητικό βασισμένο σε χαρακτηριστικά επιτρέπει στον κάτοχό του να το μετατρέψει σ' ένα νέο πιστοποιητικό που περιέχει μόνο ένα υποσύνολο των χαρακτηριστικών που περιέχονται στο αρχικό πιστοποιητικό. Αυτά τα πιστοποιητικά μπορούν να επαληθευτούν όπως τα κοινά

κρυπτογραφικά πιστοποιητικά- χρησιμοποιώντας το δημόσιο κλειδί επαλήθευσης του εκδότη- και προσφέρουν την ίδια ασφάλεια.

Οι τεχνολογίες ABC, που συχνά ονομάζονται ανώνυμα συστήματα πιστοποιητικών επιτρέπουν σ' έναν πάροχο υπηρεσιών ταυτότητας να εκδώσει ένα πιστοποιητικό σ' έναν χρήστη. Αυτό το πιστοποιητικό περιέχει χαρακτηριστικά του χρήστη όπως την διεύθυνση ή την ημερομηνία γέννησης, αλλά και τα δικαιώματά του ή ρόλους του ως χαρακτηριστικά. Χρησιμοποιώντας το πιστοποιητικό, ο χρήστης μπορεί να αποδείξει σε τρίτους ότι έχει στην κατοχή του ένα πιστοποιητικό που περιέχει ένα συγκεκριμένο χαρακτηριστικό ή ρόλο χωρίς να αποκαλύπτει άλλες πληροφορίες που είναι αποθηκευμένες στο πιστοποιητικό.

Για παράδειγμα, ο χρήστης μπορεί να χρησιμοποιήσει ένα ανώνυμο ID πιστοποιητικό που έχει εκδοθεί από την κυβέρνηση για να αποδείξει ότι είναι ενήλικας, δηλαδή ότι το πιστοποιητικό περιέχει μία ημερομηνία γέννησης που δείχνει ότι είναι άνω των 18 ετών.

Έτσι, τα *ανώνυμα πιστοποιητικά (anonymous credentials)* υπόσχονται να είναι ο ακρογωνιαίος λίθος για την προστασία της ιδιωτικότητας του χρήστη σ' ένα ηλεκτρονικό περιβάλλον.

Σύμφωνα και με τα παραπάνω, έχουν αναπτυχθεί διάφορες τεχνολογίες οι οποίες εστιάζουν στην χρήση της κρυπτογραφίας και διευκολύνουν την εφαρμογή των πιστοποιητικών.

Παρακάτω παρουσιάζονται οι τεχνολογίες που κάνουν χρήση των ABC με στόχο την επίτευξη ασφάλειας και ιδιωτικότητας.

Τυχαιοποιημένα Πιστοποιητικά (Randomisable Certificates)

Τα διαπιστευτήρια που βασίζονται σε τυχαιοποιημένα Πιστοποιητικά χρησιμοποιούν ειδικές κρυπτογραφικές τεχνικές, όπως την ελλειπτική καμπύλη, που διευκολύνουν την τυχαιοποίηση του Πιστοποιητικού χρησιμοποιώντας έννοιες όπως η *τυφλή υπογραφή (blind signature)* η οποία αποτελεί ένα διαδραστικό πρωτόκολλο ανάμεσα στον

χρήστη και τον εκδότη του πιστοποιητικού., η οποία καταλήγει σε έγκυρη υπογραφή στον χρήστη χωρίς ο αποστολέας να γνωρίζει το περιεχόμενο του μηνύματος. Οι τυφλές υπογραφές χρησιμοποιούνται για την έκδοση πιστοποιητικών βάσει χαρακτηριστικών. Ο χρήστης δεν αποκαλύπτει στον εκδότη του πιστοποιητικού το μυστικό κλειδί, αλλά επιπρόσθετα λαμβάνει μία έγκυρα πιστοποιημένη υπογραφή από τον εκδότη η οποία περιλαμβάνει το μυστικό κλειδί και τις ιδιότητες του πιστοποιητικού. Πρέπει να σημειωθεί ότι η απειλή να ιχνηλατηθεί η υπογραφή υπάρχει, όταν αυτήν δεν έχει τυχαιοποιηθεί πριν την επιβεβαίωση. [38]

Κατά τα άλλα, το πλεονέκτημα αυτής της προσέγγισης είναι ότι η χρήση των πιστοποιητικών είναι μη ανιχνεύσιμη.

Μονής Όψης Πιστοποιητικά (Single-show Credentials)

Αυτού του είδους τα πιστοποιητικά χρησιμοποιούνται σε συνδυασμό με ένα πρωτόκολλο *τυφλής υπογραφής (blind signature)* ως ψευδώνυμα. Πιο συγκεκριμένα, ο χρήστης προσθέτει την τυφλή υπογραφή στο πιστοποιητικό του και με αυτόν τον τρόπο το κρύβει από την Αρχή έκδοσης. Έτσι, δεν μπορεί να συσχετισθεί το εκδοθέν πιστοποιητικό με την διαδικασία έκδοσης. Ονομάζονται μονής όψης αυτά τα πιστοποιητικά, αφού δεν παρέχουν την ιδιότητα της πολλαπλής όψεως μη συνδεσιμότητας και δεν μπορούν να συνδεθούν όταν χρησιμοποιούνται περισσότερες από μία φορές. Η πολλαπλής όψης μη συνδεσιμότητα μπορεί να υλοποιηθεί μέσω έκδοσης πολλαπλών πιστοποιητικών για το ίδιο σύνολο ιδιοτήτων και τα οποία μπορούν να επιβεβαιωθούν αργότερα, ανεξάρτητα το ένα από το άλλο.

Αυτά τα διαπιστευτήρια χρησιμοποιούνται κυρίως στην τεχνολογία U-Prove της Microsoft. [36]

Πολλαπλής Όψης Πιστοποιητικά (Multi-show Credentials)

Η χρήση πρωτοκόλλων μηδενικής γνώσης (zero-knowledge) επιτρέπει στον χρήστη να αποδείξει την ιδιοκτησία του πιστοποιητικού, χωρίς να αποκαλύψει το ίδιο το πιστοποιητικό. Αυτό επιτυγχάνει πολλαπλής όψης μη συνδεσιμότητα, καθώς αυτός που επιβεβαιώνει δεν βλέπει το πιστοποιητικό. Βασικό μειονέκτημα αυτής της τεχνολογίας αποτελεί η απαίτηση ενός χρονικού διαστήματος κάποιων δευτερολέπτων για τον έλεγχο του πιστοποιητικού, κάτι το οποίο μειώνει την πρακτική εφαρμογή αυτής της υλοποίησης.

Αυτά τα πιστοποιητικά χρησιμοποιήθηκαν στην τεχνολογία Identity Mixer της IBM. [36]

Μοιραζόμενα Κλειδιά (Shared Keys)

Οι παραπάνω τεχνολογίες παρέχουν Ιδιωτικότητα βάσει Σχεδιασμού (privacy by design) και μπορούν να υλοποιηθούν σε έξυπνες κάρτες (smart cards).

Υπάρχει, όμως, και η προσέγγιση που χρησιμοποιείται στην γερμανική κάρτα πολίτη, όπου ένας περιορισμένος τύπος ανώνυμων ιδιοτήτων επιτυγχάνεται, τροποποιώντας το ηλεκτρονικό πρωτόκολλο ταυτότητας που βασίζεται στην ελλειπτική καμπύλη, μοιραζόμενου τα ιδιωτικά κλειδιά ανάμεσα σε σύνολα καρτών. Οι υπογεγραμμένες ιδιότητες είναι εν μέρει ανώνυμες, λόγω του ότι ο διαμοιρασμός των κλειδιών υπογραφής μεταξύ των συνόλων των καρτών εμποδίζει τη σύνδεση μιας υπογραφής με μία μόνο κάρτα. [36]

4.2.1. I Reveal My Attributes

Οι δύο πιο σημαντικές τεχνολογίες που χρησιμοποιούν την προσέγγιση των Attribute - Based Credentials είναι η U-Prove της Microsoft και η Idemix της IBM. Η Idemix είναι τεχνολογία βασιζόμενη στα χαρακτηριστικά που έχει αναπτυχθεί από το ερευνητικό τμήμα της IBM στη Ζυρίχη και περιλαμβάνει ισχυρή αυθεντικοποίηση και ιδιωτικότητα ταυτόχρονα. Βασίζεται στον αλγόριθμο RSA.

Το έργο *IRMA* (*I Reveal My Attributes*) είναι πιλοτικό και βασίζεται στην ανάπτυξη μίας πλατφόρμας που υποστηρίζει τα πιστοποιητικά βασιζόμενα στα χαρακτηριστικά σε μία ηλεκτρονική κάρτα και αποτελεί υλοποίηση, εν μέρει, της Idemix. Προς το παρόν, το IRMA χρησιμοποιεί μόνο την τεχνολογία Idemix, ενώ θα μπορούσε ή και στο μέλλον να χρησιμοποιήσει και την τεχνολογία U-Prove. Το έργο αυτό έχει σκοπό να δείξει την εφαρμοσιμότητα των Attribute - Based Credentials στην πράξη σε έξυπνες κάρτες και ήδη υλοποιείται μέσω της επιλεκτικής γνωστοποίησης (selective disclosure) χρησιμοποιώντας πρωτόκολλα μηδενικής γνώσης.

Η βασική ιδέα πίσω από την κάρτα IRMA είναι ότι η πληροφορία που αποθηκεύεται στην κάρτα μπορεί να διαβαστεί ψηφιακά από την κάρτα μόνο όταν ο κάτοχός της δίνει συγκεκριμένη αδειοδότηση για το ποια χαρακτηριστικά μπορούν να διαβαστούν (όπως όνομα, ηλικία κ.α.).

Συγκεκριμένα, στο Πανεπιστήμιο Radboud οι φοιτητές χρησιμοποιούν την κάρτα IRMA πειραματικά, με την οποία μπορούν να αγοράσουν καφέ σε χαμηλότερη τιμή από το κυλικείο του Πανεπιστημίου καθώς και να χρησιμοποιήσουν δωρεάν, με χρήση της κάρτας, τους εκτυπωτές του Πανεπιστημίου. Τα τερματικά επιβεβαίωσης της κάρτας IRMA είναι tablets που τρέχουν σε android λειτουργικό σύστημα και έχουν εγκατασταθεί στο κυλικείο του Πανεπιστημίου. Αυτά τα τερματικά ελέγχουν την κάρτα αν ανήκει στο συγκεκριμένο φοιτητή του Πανεπιστημίου, ώστε να μην πληρώσει τον καφέ του. Αυτό το project είναι μικρής κλίμακας που όμως, θα μπορούσε να επεκταθεί στις

ηλεκτρονικές κάρτες πολίτη. Πάνω στην κάρτα υπάρχει μία φωτογραφία του κατόχου κι ένας σειριακός αριθμός. Για να επιτευχθεί μεγαλύτερη ιδιωτικότητα, το IRMA επιτρέπει στον κάτοχό του να φανερώσει ένα ή περισσότερα attributes ενός πιστοποιητικού και επίσης, ένας αριθμός PIN που μπορεί να συσχετισθεί με ένα attribute το οποίο θεωρείται ευαίσθητο δεδομένο, όπως το ΑΜΚΑ. Όμως το μεγαλύτερο πλεονέκτημα της κάρτας IRMA είναι η ιδιωτικότητα που προσφέρει. [39]

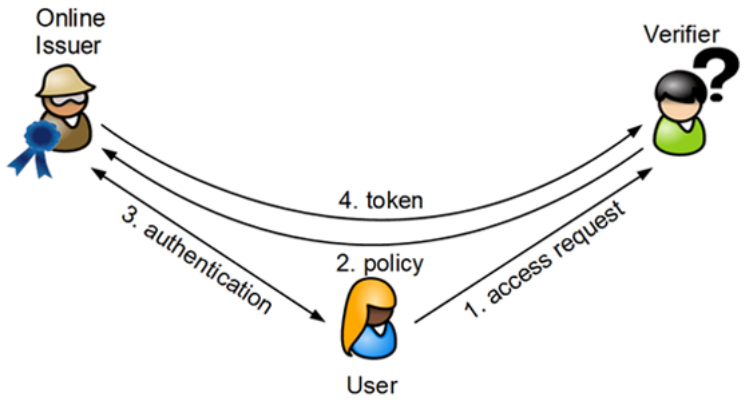
Κάρτα IRMA στην οποία φαίνεται η φωτογραφία του κατόχου της και ο σειριακός αριθμός, Πηγή: Brinda Badarinath Hampiholi, University of Twente, Master Thesis "Secure & Privacy - preserving eID systems with Attribute-Based Credentials"

4.2.2. Οι τεχνολογίες Idemix και U-Prove

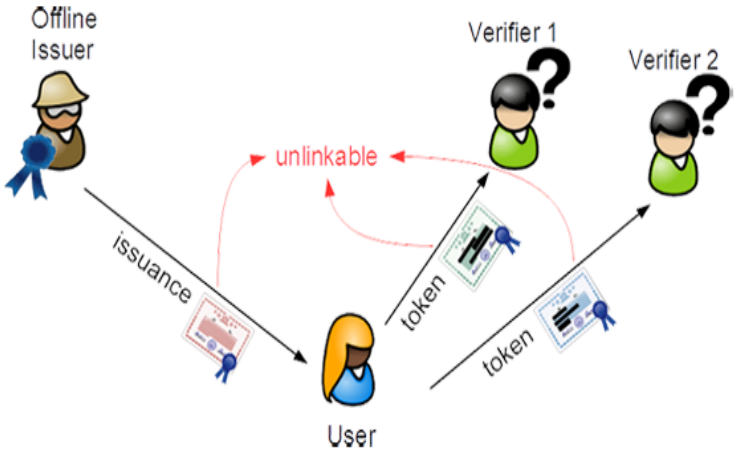
Idemix

Όπως αναφέρθηκε και στην παράγραφο 3.2.1., η τεχνολογία *Idemix (Identity Mixer)* είναι ένα ανώνυμο σύστημα πιστοποιητικών, μια οικογένεια πρωτοκόλλων, που αναπτύχθηκε από την IBM Research στη Ζυρίχη, βασίζεται σε κρυπτογράφηση με RSA αλγόριθμο και παρέχει ισχυρή αυθεντικοποίηση και ιδιωτικότητα στους χρήστες της. Οι ίδιοι μπορούν να προμηθευτούν από τον εκδότη, ένα πιστοποιητικό που περιέχει όλες τις πληροφορίες που ο εκδότης μπορεί να πιστοποιήσει για

τους ίδιους. Όταν αργότερα ένας χρήστης θελήσει να αποδείξει σε έναν πάροχο υπηρεσιών έναν ισχυρισμό του για τον ίδιο, θα χρησιμοποιήσει την συγκεκριμένη τεχνολογία για να μετασχηματίσει με ασφάλεια το εκδοθέν πιστοποιητικό. Εκείνο περιέχει ένα υποσύνολο μόνο των πιστοποιημένων πληροφοριών που ο χρήστης είναι πρόθυμος να αποκαλύψει. Ο χρήστης έχει την δυνατότητα να μετασχηματίσει όσες φορές επιθυμεί τα πιστοποιητικά χωρίς αυτά να μπορούν να συνδεθούν μεταξύ τους. [40]



Τεχνολογία Idemix της IBM, Πηγή:
http://www.zurich.ibm.com/idemix/whatitdoes.html



Μη συνδεσιμότητα των διαπιστευτηρίων μέσω τεχνολογίας Idemix, Πηγή:
http://www.zurich.ibm.com/idemix/whatitdoes.html

U-Prove

Η τεχνολογία *U-Prove* της Microsoft είναι μια προηγμένη τεχνολογία κρυπτογράφησης, μια προδιαγραφή του πυρήνα λειτουργικότητας ενός ευρύτερου συνόλου πρωτοκόλλων, που και αυτήν διασφαλίζει την αυθεντικοποίηση και την ιδιωτικότητα του χρήστη ταυτόχρονα. Η λειτουργία της είναι παρόμοια με αυτήν των πιστοποιητικών Υποδομής Δημόσιου Κλειδιού, τα οποία μπορούν να κωδικοποιήσουν ιδιότητες (attributes) πολλών τύπων, με δύο ,όμως, διαφορές:

- Η έκδοση και παρουσίαση του δείγματος (token) είναι ασύνδετη εξαιτίας του δημόσιου κλειδιού και της υπογραφής που έχει κωδικοποιηθεί στο δείγμα.
- Οι χρήστες μπορούν να συμπεριλάβουν πληροφορίες σε σχέση με τις ιδιότητες που έχουν κωδικοποιηθεί στο δείγμα. Δηλαδή ένας χρήστης μπορεί να επιλέξει το υποσύνολο των κρυπτογραφημένων ιδιοτήτων που θα περιλαμβάνονται και θα αποτελούν απόδειξη ότι το όνομά του δεν περιλαμβάνεται σε κάποια "μαύρη λίστα", για παράδειγμα. [41]

Δεδομένου ότι αυτές οι δύο τεχνολογίες υποστηρίζονται από κορυφαίες εταιρίες τεχνολογίας, υπάρχει η πεποίθηση ότι μπορούν να συμβάλλουν στη δημιουργία διαδικασίας τυποποίησης στον τομέα των ABC. Είναι, όμως απαραίτητο, διαφορετικές ABC τεχνολογίες να μπορούν να συνυπάρχουν ή να εναλλάσσονται σε σενάρια που αφορούν ίδιους χρήστες και τεχνολογίες. Κάτι που προς το παρόν δεν υφίσταται.

4.3. Το περιβάλλον των Attribute - Based Credentials

Στα Πιστοποιητικά βάσει χαρακτηριστικών λόγω των ψευδωνύμων και των πιστοποιημένων χαρακτηριστικών που περιλαμβάνουν την χρήση ενός ιδιωτικού κλειδιού άγνωστο στον εκδότη, και λόγω της ασύμμετρης

κρυπτογράφησης, ο πάροχος ταυτότητας δεν είναι σε θέση να επισκιάσει την ταυτότητα του χρήστη. Τα πιστοποιητικά βασιζόμενα σε ιδιότητες δεν είναι πάντα συμβατά με τα συστήματα που μπορούν να χρησιμοποιούν, όπως SAML, OPENID, X.509, ωστόσο το σημαντικό που προσφέρουν είναι ένα υπερσύνολο λειτουργικότητας και ασφάλειας, προστασία της ιδιωτικής ζωής και δυνατότητα επεκτασιμότητας των χαρακτηριστικών αυτών των συστημάτων.

4.4. Το έργο ABC4Trust

Παρά τις αξιόλογες προσπάθειες κατανόησης των Attribute Based Credentials τεχνολογιών ακόμα δεν υπάρχει ένα κοινά συμφωνημένο σύνολο για τις λειτουργίες, τα χαρακτηριστικά, τα πρωτόκολλα και τις μετρήσεις για τη σύγκρισή τους κι έτσι είναι δύσκολο να τις κρίνουμε. Το χάσμα μεταξύ των τεχνικών κρυπτογράφησης και των πρωτοκόλλων αυτών των τεχνολογιών, καθώς και η έλλειψη προτύπων για την ανάπτυξή τους δυσκολεύουν τη χρήση τους σε περιβάλλοντα Ηλεκτρονικής Διακυβέρνησης, αλλά και γενικότερα σε διαδικτυακές εφαρμογές.

Μία αξιόλογη προσπάθεια προσέγγισης της ελάχιστης αποκάλυψης πληροφοριών για τον χρήστη είναι το ερευνητικό έργο ABC4Trust. Στόχος του είναι η κατανόηση εις βάθος των ABC τεχνολογιών, η αποδοτική και αποτελεσματική ανάπτυξή τους στην πράξη, και η ενοποίησή τους σε διάφορους τομείς. Για το σκοπό αυτό το έργο:

- ορίζει μία κοινή, ενοποιημένη αρχιτεκτονική για τα συστήματα ABC και επιτρέπει σε διάφορες υλοποιήσεις αυτών των τεχνολογιών να συνυπάρχουν, να εναλλάσσονται και να ενοποιούνται
- ορίζει κριτήρια για την σύγκριση των ιδιοτήτων αυτών των πραγματοποιήσεων σε διάφορες τεχνολογίες

- παρέχει υλοποιήσεις αναφοράς για καθεμία από αυτές τις συνιστώσες. [42]

Οι προδιαγραφές αρχιτεκτονικής και πρωτοκόλλου που προτείνονται από το έργο, ανοίγουν το δρόμο για την καθιέρωση προτύπων που επιτρέπουν την εναλλαξιμότητα και την ενοποίηση των ABC τεχνολογιών.

Η συνεισφορά του έργου έγκειται στην ενοποιημένη αρχιτεκτονική για την συνένωση και την ανταλλαγή διαφορετικών ABC τεχνολογιών ώστε:

- οι χρήστες να μπορούν να αποκτήσουν πιστοποιήσεις για πολλές ABC τεχνολογίες
- οι πάροχοι να είναι σε θέση να υιοθετούν οποιαδήποτε από τις ABC τεχνολογίες, ανάλογα με τις ανάγκες τους. [42]

Επιπλέον, η αρχιτεκτονική του έργου έχει σχεδιαστεί για να αποσυντεθούν μελλοντικές εφαρμογές των ABC τεχνολογιών και να καθορίσουν την αφηρημένη λειτουργικότητα αυτών των στοιχείων με τέτοιο τρόπο ώστε να είναι ανεξάρτητες από τους αλγόριθμους κρυπτογράφησης. Το πρόγραμμα στοχεύει όχι μόνο στην ενοποίηση των ABC τεχνολογιών, αλλά και στην συνύπαρξη αυτών στην ίδια πλατφόρμα. Αυτό με τη σειρά του συνεπάγεται ότι διαφορετικά συστήματα πρέπει να είναι σε θέση να μοιραστούν κοινά στοιχεία. Έτσι, οι ενιαίες μορφές δεδομένων και τα πρωτόκολλα μπορούν να επιτρέψουν όχι μόνο τη συνύπαρξη στον ίδιο κόμβο του δικτύου, αλλά και την πιθανή ενοποίηση σε διαφορετικούς κόμβους του δικτύου.

Το έργο είχε διάρκεια 52 μήνες, από τον Νοέμβριο του 2010 ως τον Φεβρουάριο του 2015, ενώ μεγάλο μέρος της χρηματοδότησής του προέρχεται από την Ευρωπαϊκή Ένωση.

4.4.1.Εφαρμογές του έργου

Το έργο περιλαμβάνει δύο πιλοτικές εφαρμογές:

1. Η μία πιλοτική εφαρμογή πραγματοποιείται σε σχολείο δευτεροβάθμιας εκπαίδευσης της Σουηδίας, στο δήμο Söderhamn και περιλαμβάνει πρόσβαση στην κοινότητα του σχολείου με χρήση ψευδωνύμων και παροχή κοινωνικής δικτύωσης για τους μαθητές του σχολείου, και πιο συγκεκριμένα με χρήση *Privacy Enhancing Attribute-Based Credentials (Privacy-ABC's)*. Συγκεκριμένα, οι μαθητές μπορούν να ζητούν συμβουλές και να κάνουν πολύ προσωπικές ερωτήσεις χωρίς κατ' ανάγκη να αποκαλύπτουν την ταυτότητά τους. Αυτή η εφαρμογή έχει σκοπό την αντιμετώπιση των ειδικών προκλήσεων που προκύπτουν από το γεγονός ότι οι χρήστες του διαδικτύου είναι όλο και μικρότερης ηλικίας και μερικές φορές ανήλικοι. Στη Σουηδία, τα σχολεία χρησιμοποιούν το Διαδίκτυο κυρίως για την επικοινωνία ανάμεσα σε μαθητές, γονείς και εκπαιδευτικούς μέσω διαφορετικών πυλών και σε ιδιωτικές κοινότητες.

   Μία μεγάλη απειλή για την ιδιωτικότητα των μαθητών αποτελεί η μη εξουσιοδοτημένη πρόσβαση σε σημαντικές προσωπικές πληροφορίες, όπως οι βαθμοί, τα αποτελέσματα διαγωνισμάτων, αλλά και άλλες πληροφορίες που είναι διαθέσιμες μέσω της πύλης του σχολείου. Οι εφαρμογές της κοινωνικής δικτύωσης και των συμβουλών ιατρικής και ψυχολογικής φύσης επωφελούνται από το έργο, καθώς επιτρέπει τον συνδυασμό ισχυρής αυθεντικοποίησης και προστασίας της ιδιωτικότητας μέσω των ABC.

   Από τη μία μεριά, οι μαθητές μπορούν να επιβεβαιώνουν την ταυτότητά τους για να έχουν πρόσβαση σε "δωμάτια συνομιλιών" (chat rooms) και από την άλλη μεριά, μπορούν να παραμένουν ανώνυμοι όταν ερωτώνται προσωπικές και ευαίσθητες πληροφορίες από το προσωπικό του σχολείου, ενώ παράλληλα το προσωπικό του σχολείου διασφαλίζει ότι επικοινωνεί με εξουσιοδοτημένους μαθητές. Αυτή η μορφή εφαρμογής βοηθά στο να συγκεντρωθούν πληροφορίες για την

χρηστικότητα της ABC τεχνολογίας κάτω από δύσκολες και ευαίσθητες συνθήκες χρήσης, μιας και οι χρήστες της είναι παιδιά. [43]

2. Η δεύτερη πιλοτική εφαρμογή, ξεκίνησε τον Σεπτέμβριο του 2012, πραγματοποιείται στην Ελλάδα, στο Πανεπιστήμιο Πατρών και περιλαμβάνει δημοσκόπηση και πιο συγκεκριμένα, ανώνυμη συλλογή ανατροφοδότησης από εξουσιοδοτημένους φοιτητές σχετικά με τα μαθήματα που παρακολούθησαν κι τους καθηγητές τους. Σε αυτήν την περίπτωση εκδόθηκαν διαπιστευτήρια και συγκεκριμένα *Privacy-Enhanced Attribute-Based Credentials (Privacy-ABC's)* σε φοιτητές που πιστοποιούν μια σειρά από γεγονότα, επιτρέποντάς τους να παρέχουν ανώνυμα ανατροφοδότηση. Για να είναι τα αποτελέσματα της δημοσκόπησης ορθά και αξιόπιστα θα πρέπει να διατηρείται η ιδιωτικότητα των φοιτητών που συμμετέχουν.

   Η αξιολόγηση μαθημάτων έχει γίνει συνήθη πρακτική στα περισσότερα πανεπιστήμια των ανεπτυγμένων χωρών. Παρόλα αυτά, πραγματοποιούνται όχι ψηφιακά, για να προστατευτεί η ιδιωτικότητα των φοιτητών. Εάν διεξάγονταν ψηφιακά, οι υπολογιστές θα έπρεπε να λειτουργούν κάτω από το πρίσμα ενός ουδέτερου, αξιόπιστου οργανισμού, ανεξάρτητου από το πανεπιστήμιο που κάνει την αξιολόγηση, διαφορετικά οι φοιτητές θα έπρεπε να είχαν "τυφλή" εμπιστοσύνη στις πρακτικές προστασίας της ιδιωτικότητας που εφαρμόζει το κάθε πανεπιστήμιο.

   Οι ABC τεχνολογίες δίνουν τη δυνατότητα σε κάθε πανεπιστήμιο να εκδίδει τα δικά του ηλεκτρονικά δελτία ταυτότητας τα οποία να περιέχουν λίστες με τα μαθήματα που δηλώνει ο κάθε φοιτητής. Στη συνέχεια, το πανεπιστήμιο μπορεί να έχει το δικό του σύστημα ανατροφοδότησης χωρίς να χρειάζεται ν' αποκτήσει την εμπιστοσύνη των φοιτητών του, γιατί οι ABC τεχνολογίες, χρησιμοποιούμενες στα δελτία φοιτητικής ταυτότητας μπορούν και αποκόπτουν όλους τους συνδέσμους ανάμεσα στην εισερχόμενη ηλεκτρονική ανατροφοδότηση και την ταυτότητα του φοιτητή που την υποβάλλει, εξασφαλίζοντας παράλληλα πως η ανατροφοδότηση προέρχεται από διαπιστευμένους φοιτητές. [43]

4.4.2.Αποτελέσματα των εφαρμογών του έργου

Το ABC4Trust θα συγκεντρώσει την εμπειρία από τις δύο παραπάνω πιλοτικές εφαρμογές του ώστε να γίνει προσπάθεια υλοποίησής του σε περιβάλλοντα παραγωγής. Από αυτές τις δύο πιλοτικές εφαρμογές του μπορεί να ελεγχθεί η χρήση και η απόδοση των πιστοποιητικών με τις δύο παραπάνω διαφορετικές ομάδες χρηστών, που έχουν διαφορετικές δεξιότητες και διαφορετικές ανάγκες.

Επιπλέον, η κατεύθυνση της ανταλλαγής πληροφοριών διαφέρει σε σχέση με τίνος η ιδιωτικότητα προστατεύεται, όπως επίσης και η δομή της ανταλλαγής πληροφοριών. Λαμβάνοντας υπόψη την συλλογή κριτηρίων και την σχεδίαση και υλοποίηση της απαραίτητης υποδομής, η αξιολόγηση των παραπάνω πιλοτικών εφαρμογών παρέχει μια σαφή απόδειξη για την δυνατότητα εφαρμογής τόσο της ιδέας των ενοποιημένων πιστοποιητικών όσο και για την σχετική αρχιτεκτονική, παρέχοντας ανατροφοδότηση για βελτιώσεις. [44]

4.4.3. ABC4Trust και Ηλεκτρονικές Ταυτότητες

Το έργο ABC4Trust θεωρεί τις ηλεκτρονικές ταυτότητες ως βέλτιστη περίπτωση χρήσης για την ευρεία ανάπτυξη των τεχνολογιών Attrribute - Based Credentials που προστατεύουν την ιδιωτική ζωή, και πιο συγκεκριμένα τις τεχνολογίες Privacy-ABC's.

Η έννοια της ελαχιστοποίησης των προσωπικών δεδομένων είναι στενά συνυφασμένη με την αρχή της αναλογικότητας, η οποία είναι θεμελιώδης αρχή για τη νόμιμη επεξεργασία προσωπικών δεδομένων. Προφανώς, με βάση τα ανωτέρω, ένας τρόπος για να ενεργοποιηθεί και να επιβληθεί η ελαχιστοποίηση των δεδομένων με τεχνικά μέσα αποτελεί η έννοια της επιλεκτικής αποκάλυψης χαρακτηριστικών (selective disclosure), όπως είδαμε και στο έργο IRMA. Η λύση της ηλεκτρονικής

ταυτότητας βασίζεται στα χαρακτηριστικά για ένα άτομο με την αντίστοιχη ιδιότητα. Τα e-token της ταυτότητας ή τα πιστοποιητικά δεν επιτρέπουν την αποκάλυψη μόνο ενός επιλεγμένου χαρακτηριστικού χωρίς να ακυρωθεί η υπογραφή του εκδότη.

Οι πρώτες εμπειρίες από τις δύο παραπάνω πιλοτικές εφαρμογές δείχνουν ότι η λειτουργία των ABC's με ασφαλείς έξυπνες κάρτες μπορεί να αποτελεί απαραίτητη προϋπόθεση για πολλά κράτη μέλη της Ε.Ε. να ενσωματώσουν την τεχνολογία αυτή στην εθνική ηλεκτρονική ταυτότητά τους.

Κεφάλαιο 5

Προστασία Προσωπικών Δεδομένων: Νομικό Πλαίσιο

5.1 Νομικό Πλαίσιο

5.1.1. Ευρωπαϊκό Νομοθετικό Πλαίσιο

Η ραγδαία ανάπτυξη της τεχνολογίας κατέστησε επιτακτική την ανάγκη για την εφαρμογή μιας νομικής ρύθμισης, ορισμένης από την Ευρωπαϊκή Ένωση για όλα τα κράτη - μέλη της. Έτσι, το 1995, ως αποτέλεσμα των προσπαθειών να συντονιστούν όλα τα κράτη - μέλη υπό ένα κοινό νομικό καθεστώς ήταν η δημιουργία μίας ρύθμισης, σύμφωνα με την οποία, κάθε κράτος - μέλος πρέπει να θεσπίσει συγκεκριμένες νομικές διατάξεις και να δημιουργήσει μία αρμόδια υπηρεσία.

Ευρωπαϊκή Οδηγία 95/46/ΕΚ

Η νομική ρύθμιση, σύμφωνα με την οποία κάθε κράτος - μέλος πρέπει να θεσπίσει συγκεκριμένες νομικές διατάξεις, είναι η *Ευρωπαϊκή Οδηγία 95/46/ΕΚ,* η οποία δίνει την κατευθυντήρια γραμμή σε όλα τα κράτη- μέλη της Ε.Ε. για θέματα που έχουν σχέση με την Προστασία Δεδομένων Προσωπικού Χαρακτήρα και αποτελεί το πιο επιδραστικό νομοθετικό κείμενο παγκοσμίως σε σχέση με την Προστασία Προσωπικών Δεδομένων. Όλα τα κράτη - μέλη αναγκάστηκαν μέσα σε τρία χρόνια να αναπροσαρμόσουν τις αντίστοιχες εθνικές νομοθεσίες με βάση την Οδηγία 95/46/ΕΚ.

Βασικός σκοπός αυτής της Οδηγίας είναι η προστασία της Ιδιωτικότητας σαν θεμελιώδες δικαίωμα του ανθρώπου, αναφορικά προς την συλλογή, την επεξεργασία, αποθήκευση και μετάδοση δεδομένων προσωπικού χαρακτήρα. Επιπλέον, όπως προαναφέρθηκε έχει ως στόχο την εφαρμογή κοινού νομοθετικού πλαισίου σε όλα τα κράτη-μέλη της Ευρωπαϊκής Ένωσης σε σχέση με την προστασία και την διακίνηση δεδομένων προσωπικού χαρακτήρα.

Δεδομένα Προσωπικού Χαρακτήρα είναι, σύμφωνα με την Οδηγία 95/46/ΕΚ, κάθε πληροφορία που αναφέρεται στο πρόσωπο ενός ατόμου, όπως το όνομα, το επάγγελμα, η οικογενειακή κατάσταση, η ηλικία.[45]

Ευαίσθητα Δεδομένα είναι, κατά την ίδια Οδηγία, τα δεδομένα που αφορούν τη φυλετική ή εθνική προέλευση, τα πολιτικά φρονήματα, τις θρησκευτικές πεποιθήσεις, την υγεία, την ερωτική ζωή, τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και τα δεδομένα που είναι σχετικά με ποινικές διώξεις ή καταδίκες. [45] Με άλλα λόγια, ως ευαίσθητα χαρακτηρίζονται τα προσωπικά δεδομένα που κρίθηκε ότι εμπίπτουν στο σκληρό πυρήνα της ιδιωτικότητας και χρήζουν ακόμα μεγαλύτερης προστασίας.

Ενδεικτικά, στο άρθρο 6 της Οδηγίας τίθενται οι αρχές που πρέπει να τηρούνται ως προς την ποιότητα των δεδομένων. Το Ευρωπαϊκό Κοινοβούλιο προβλέπει τα δεδομένα να *"α. υφίστανται σύννομη και θεμιτή επεξεργασία, β. να συλλέγονται για καθορισμένους σαφείς και νόμιμους*

σκοπούς και η μεταγενέστερη επεξεργασία τους να συμβιβάζεται με τους σκοπούς αυτούς , γ. να είναι κατάλληλα, συναφή προς το θέμα και όχι υπερβολικά σε σχέση με τους σκοπούς για τους οποίους συλλέγονται και υφίστανται επεξεργασία, δ. να είναι ακριβή και εφόσον χρειάζεται να ενημερώνονται, ε. να διατηρούνται με μορφή που επιτρέπει τον προσδιορισμό της ταυτότητας των προσώπων στα οποία αναφέρονται μόνο κατά τη διάρκεια περιόδου που δεν υπερβαίνει την απαιτούμενη για την επίτευξη των σκοπών για τους οποίους έχουν συλλεγεί ή για τους οποίους αργότερα υφίστανται επεξεργασία...".[45]

Από την παραπάνω διάταξη προκύπτει, μεταξύ άλλων, και η αρχή της ελαχιστοποίησης των δεδομένων (βλ. και προηγούμενο κεφάλαιο, όπου η ελαχιστοποίηση των δεδομένων τίθεται ως βασικός σχεδιαστικός στόχος των τεχνολογιών ABC) ως θεμελιώδη αρχή για τη νομιμότητα κάθε επεξεργασίας προσωπικών δεδομένων.

Συνεχίζοντας, στο άρθρο 7 της Οδηγίας αναφέρονται οι βασικές αρχές της νόμιμης επεξεργασίας δεδομένων, σύμφωνα με τις οποίες *"...η επεξεργασία δεδομένων προσωπικού χαρακτήρα μπορεί να γίνει μόνο αν α. το πρόσωπο στο οποίο αναφέρονται έχει δώσει τη ρητή συγκατάθεσή του ή β. είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το ενδιαφερόμενο πρόσωπο είναι συμβαλλόμενο μέρος ή για την εκτέλεση προσυμβατικών μέτρων ληφθέντων αιτήσει του ή γ. είναι απαραίτητη για την τήρηση εκ του νόμου υποχρεώσεως του υπευθύνου της επεξεργασίας ή δ. είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του προσώπου στο οποίο αναφέρονται τα δεδομένα ή ε. είναι απαραίτητη για την εκπλήρωση έργου δημοσίου συμφέροντος ή εμπίπτοντος στην άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο της επεξεργασίας ή στον τρίτο τον οποίο ανακοινώνονται τα δεδομένα ή στ. είναι απαραίτητη για την επίτευξη του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας ή ο τρίτος ή οι τρίτοι στους οποίους ανακοινώνονται τα δεδομένα, υπό τον όρο ότι δεν προέχει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του προσώπου στο οποίο αναφέρονται τα δεδομένα που χρήζουν προστασίας ..."* [45]

Τέλος, στο άρθρο 14 αναφέρεται το δικαίωμα της αντίρρησης του προσώπου στο οποίο αναφέρονται τα δεδομένα, ενώ στο άρθρο 16 αναφέρεται το απόρρητο της επεξεργασίας των δεδομένων και στο άρθρο 17 η ασφάλεια της επεξεργασίας των δεδομένων.

Στην Ελλάδα, η Οδηγία 95/46/ΕΚ έχει ενσωματωθεί στην εθνική έννομη τάξη με το ν. 2472/1997 [46] , ενώ στην Κύπρο με το ν. 138(I)/(2001). [47]

Θα πρέπει να σημειωθεί ότι η Ε.Ε. σχεδιάζει νέο Κανονισμό [48] προς αντικατάσταση της Οδηγίας 95/46/ΕΚ με στόχο την περαιτέρω ενίσχυση της προστασίας των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Ο νέος Κανονισμός, ο οποίος θα έχει απευθείας ισχύ σε όλα τα Κράτη-Μέλη, εισάγει νέες υποχρεώσεις και απαιτήσεις προς ενίσχυση της προστασίας προσωπικών δεδομένων, γεγονός που καταδεικνύει τη σπουδαιότητα που πρέπει να αποδίδεται στην ιδιωτικότητα. Ιδιαίτερες απαιτήσεις θα θέσει ο νέος Κανονισμός για κρίσιμες επεξεργασίες (στις οποίες φαίνεται, κατ' αρχάς, ότι εμπίπτουν επεξεργασίες στο πλαίσιο υπηρεσιών ηλεκτρονικής διακυβέρνησης). Ειδικότερα, σύμφωνα με το άρθρο 33 του νέου Κανονισμού "*αν οι πράξεις επεξεργασίας ενέχουν συγκεκριμένους κινδύνους για τα δικαιώματα και τις ελευθερίες των προσώπων στα οποία αναφέρονται τα δεδομένα, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία διενεργεί εκτίμηση των επιπτώσεων των προβλεπόμενων πράξεων επεξεργασίας σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα*".

Το ερώτημα λοιπόν που τίθεται είναι το πότε μία επεξεργασία προσωπικών δεδομένων ενέχει ιδιαίτερους κινδύνους. Στο σχέδιο του Κανονισμού γίνεται μία προσπάθεια περιγραφής αυτών: ειδικότερα, σύμφωνα με το άρθρο 33 αυτού, η επεξεργασία ενέχει κινδύνους κατά:

- την συστηματική αξιολόγηση προσωπικών πτυχών ενός προσώπου με στόχο π.χ. την ανάλυση της οικονομικής του κατάστασης, των προσωπικών του προτιμήσεων, της αξιοπιστίας ή της συμπεριφοράς του, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία και βάσει

της οποίας λαμβάνονται μέτρα τα οποία παράγουν σημαντικές έννομες συνέπειες.

- την επεξεργασία ευαίσθητων δεδομένων, αν τα δεδομένα υποβάλλονται σε επεξεργασία για τη λήψη μέτρων ή αποφάσεων σε μεγάλη κλίμακα.
- την χρήση συστημάτων αρχειοθέτησης μεγάλης κλίμακας, τα οποία περιέχουν δεδομένα για παιδιά, γενετικά ή βιομετρικά δεδομένα. [49]

Όμως, δεν παρατηρείται μόνο η ραγδαία ανάπτυξη της τεχνολογίας, αλλά και η ραγδαία ανάπτυξη στις τηλεπικοινωνίες.

Το 2007, η Ελλάδα κέρδισε μία πρωτιά, που δεν έγινε ευρέως γνωστή: Στην *"Διεθνή κατάταξη Ιδιωτικότητας για το 2007"* - η οποία καταρτίζεται κάθε χρόνο από την αμερικάνικη Electronic Privacy Information Center και την αγγλική Privacy International- η Ελλάδα ήταν πρώτη στην προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων ανάμεσα στις 27 χώρες της Ε.Ε. και σε επιπλέον 20 χώρες. [50]

Ανεξάρτητες αρχές προστασίας προσωπικών δεδομένων

Η Ευρωπαϊκή Οδηγία 95/46/ΕΚ, που έχει ενσωματωθεί σε όλα τα Κράτη-Μέλη, ορίζει τη θέσπιση ανεξάρτητης Αρχής που θα εποπτεύει και επιβλέπει τις διατάξεις του νόμου για την προστασία προσωπικών δεδομένων – και, συνεπώς, και τον τρόπο με τον οποίο μία Δημόσια Υπηρεσία χρησιμοποιεί και επεξεργάζεται προσωπικά δεδομένα πολιτών.

Στην *Κύπρο*, η επεξεργασία προσωπικών δεδομένων ελέγχεται από το Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ο οποίος διορίζεται για θητεία τεσσάρων ετών και αυτή τη στιγμή είναι ο κ. Γιάννος Δανιηλίδης.

Στην *Ελλάδα*, αντίστοιχα, υπάρχει η Ανεξάρτητη Αρχή Προστασίας Προσωπικών Δεδομένων (Data Protection Authority, DPA), η οποία

ιδρύθηκε με το νόμο 2472/1997, ενώ είναι και συνταγματικά κατοχυρωμένη. Πρόεδρος της Αρχής είναι ο κ. Πέτρος Χριστόφορος.

Ευρωπαϊκή Οδηγία 2002/58/ΕΚ

Η νομική ρύθμιση σύμφωνα με την οποία προστατεύονται τα δεδομένα προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες είναι η Οδηγία 2002/58/ΕΚ. Αυτήν η Οδηγία προέκυψε από εξειδίκευση της Οδηγίας 95/46/ΕΚ στον τομέα των τηλεπικοινωνιών, ο οποίος είχε ραγδαία ανάπτυξη τα τελευταία χρόνια.

Σύμφωνα με την παρούσα οδηγία οι πάροχοι υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλουν να διασφαλίζουν το απόρρητο των τηλεπικοινωνιών, να προστατεύουν τα δεδομένα και να άρουν αυτήν την προστασία μόνο όταν πρόκειται για διενέργεια ερευνών ποινικού χαρακτήρα ή για τη διαφύλαξη της εθνικής ασφάλειας. Επιπλέον, στην συγκεκριμένη οδηγία γίνεται ανάλυση για την απαγόρευση των αυτόκλητων ηλεκτρονικών μηνυμάτων, το καθεστώς προηγούμενης συγκατάθεσης του χρήστη, και την εγκατάσταση cookies. [51]

5.1.2. Ελληνικό Νομοθετικό Πλαίσιο

Όπως είδαμε στην προηγούμενη παράγραφο, η Ευρωπαϊκή Οδηγία 95/46/ΕΚ ενσωματώθηκε στην ελληνική νομοθεσία μέσω του νόμου 2472/1997, με σκοπό την προστασία του ατόμου από την επεξεργασία των δεδομένων του προσωπικού του χαρακτήρα, ενώ η προστασία των προσωπικών δεδομένων καλύπτεται από τον Νόμο 3471/2006.

Νόμος 2472/1997

Ο Νόμος 2472/1997 καλύπτει το πεδίο της Προστασίας Προσωπικών Δεδομένων, ενώ αποτελείται από έξι κεφάλαια και είκοσι έξι άρθρα, τα οποία περιληπτικά είναι:

- Κεφάλαιο Α' - Γενικές Διατάξεις που περιλαμβάνει τρία άρθρα σε σχέση με τους ορισμούς και το πεδίο εφαρμογής του νόμου
- Κεφάλαιο Β' - Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα που περιλαμβάνει δέκα άρθρα σε σχέση με τον τρόπο συλλογής και επεξεργασίας δεδομένων προσωπικού χαρακτήρα, με την ποιότητά τους και τον διαμοιρασμό τους
- Κεφάλαιο Γ' - Δικαιώματα του Υποκειμένου των Δεδομένων που περιλαμβάνει τέσσερα άρθρα σε σχέση με τα δικαιώματα του ατόμου πάνω στα δεδομένα του προσωπικού του χαρακτήρα
- Κεφάλαιο Δ' - Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα που περιλαμβάνει έξι άρθρα σε σχέση με την σύσταση της Ανεξάρτητης Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
- Κεφάλαιο Ε' - Κυρώσεις που περιλαμβάνει τρία άρθρα σε σχέση με τις ποινές που επιβάλλει η Αρχή στους υπεύθυνους επεξεργασίας για τυχόν παραβάσεις τους.
- Κεφάλαιο ΣΤ' - Τελικές-Μεταβατικές Διατάξεις που περιλαμβάνει τρία άρθρα σε σχέση με τις απαραίτητες μεταβατικές διατάξεις για την εφαρμογή του συγκεκριμένου νόμου. [52]

Νόμος 3471/2006

Η Ευρωπαϊκή Οδηγία 2002/58/ΕΚ ενσωματώθηκε στην Ελληνική Νομοθεσία με τον Νόμο 3471/2006 που έχει ως στόχο την προστασία των δικαιωμάτων του ατόμου και της ιδιωτικής του ζωής και την θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα

και τη διασφάλιση του απόρρητου των ηλεκτρονικών επικοινωνιών.

Επιπλέον, ο συγκεκριμένος νόμος αποτελεί συμπλήρωση και εξειδίκευση αυτών που λείπουν από τον Ν. 2472/1997, αλλά σε θέματα για τα οποία δεν υπάρχει ειδική ρύθμιση, υπάρχει μέριμνα για εφαρμογή του Νόμου 2472/1997. [53]

Σε περίπτωση παραβίασης προσωπικών δεδομένων, ο πάροχος ηλεκτρονικών επικοινωνιών οφείλει να γνωστοποιήσει άμεσα την παραβίαση στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και στην Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών. Επιπλέον, ο πάροχος οφείλει να διατηρεί αρχείο παραβιάσεων όπου περιλαμβάνεται η περιγραφή των περιστατικών.

Ένα στοιχείο που πρέπει να επισημανθεί είναι ότι η σχετική νομοθεσία επικεντρώνεται κυρίως στην προστασία προσωπικών δεδομένων και όχι στην προστασία της ιδιωτικότητας των ατόμων με την ευρύτερη έννοια. Είναι γεγονός ότι αυτήν η προσέγγιση είναι πιο ρεαλιστική, εν αντιθέσει με την προστασία της ιδιωτικότητας που είναι έννοια πιο αφηρημένη. Από την άλλη πλευρά, το νομικό πλαίσιο προστασίας προσωπικών δεδομένων καλύπτει κάθε επεξεργασία προσωπικών δεδομένων, είτε αυτά χαρακτηρίζονται ως «ιδιωτικά» είτε όχι, οπότε και – υπό αυτήν την έννοια – είναι κάτι ευρύτερο από την προστασία της ιδιωτικότητας.

5.2. Θεμελιώδεις αρχές για την προστασία προσωπικών Δεδομένων

Η Οδηγία 95/46/ΕΚ θέτει κάποιες θεμελιώδεις αρχές για τη νόμιμη επεξεργασία προσωπικών δεδομένων, οι οποίες είναι:

Αρχή Προσδιορισμού του Σκοπού (purpose specification principle)

Τα δεδομένα πρέπει να συλλέγονται με νόμιμους και καθορισμένους τρόπους για σαφείς και νόμιμους σκοπούς και να υφίστανται επεξεργασία μόνο στ πλαίσια των σκοπών αυτών.

Αρχή της Αναλογικότητας

Τα δεδομένα πρέπει να είναι ακριβή ως προς το σκοπό που συλλέγονται, να διατηρούνται για καθορισμένο χρονικό διάστημα και να μην είναι περισσότερα σε όγκο από όσα χρειάζονται.

Αρχή του Περιορισμού Συλλογής (collection limitation principle)

Τα δεδομένα που συλλέγονται χρησιμοποιούνται αποκλειστικά για τον σκοπό που συλλέχθηκαν και με την συναίνεση του χρήστη.

Αρχή της διαφάνειας και της συμμετοχής του ατόμου (openess and individual participation principle)

Στο άρθρο 11 της Οδηγίας 95/46/ΕΚ αναφέρεται η υποχρεωτική γνωστοποίηση της ταυτότητας του υπεύθυνου επεξεργασίας των δεδομένων στο άτομο στο οποία αναφέρονται αυτά τα δεδομένα, ώστε να υπάρχει διαφάνεια. Στο άρθρο 14 της ίδιας Οδηγίας αναφέρεται το δικαίωμα του ατόμου στην αντίρρηση των δεδομένων που αναφέρονται στο ίδιο.[45]

Αρχή της Ευθύνης (accountability principle)

Στο άρθρο 17 της Οδηγίας 95/46/ΕΚ αναφέρεται η ασφάλεια της επεξεργασίας των δεδομένων μέσω της ευθύνης που έχει ο υπεύθυνος της επεξεργασίας τους απέναντι στους πολίτες λαμβάνοντας τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την διαφύλαξη των δεδομένων και η δυνατότητα να του καταλογιστούν ευθύνες σε περίπτωση μη τήρησης αυτών των μέτρων.[45]

Αρχή της επεξεργασίας (security safeguards principle)

Τα δεδομένα που συλλέχθηκαν πρέπει να προστατεύονται με χρήση κατάλληλων μηχανισμών ενάντια σε καταστροφή, τροποποίηση, κακόβουλη χρήση, μη εξουσιοδοτημένη χρήση.

Αυτονόητο είναι ότι οι παραπάνω αρχές θα πρέπει να τηρούνται σε κάθε επεξεργασία προσωπικών δεδομένων στο πλαίσιο υπηρεσιών ηλεκτρονικής διακυβέρνησης.

5.3. Ελληνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Η ελληνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) είναι συνταγματικά κατοχυρωμένη ανεξάρτητη Αρχή, η οποία ιδρύθηκε με το νόμο 2472/1997, ο οποίος ενσωματώνει στο ελληνικό δίκαιο την Ευρωπαϊκή Οδηγία 95/46/ΕΚ. Η Οδηγία αυτή θέτει κανόνες για την προστασία των προσωπικών δεδομένων σε όλες τις χώρες της Ευρωπαϊκής Ένωσης.

Επίσης, όσον αφορά την προστασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, η ΑΠΔΠΧ εφαρμόζει τον νόμο 3471/2006 που αντίστοιχα ενσωματώνει στο εθνικό δίκαιο την Ευρωπαϊκή Οδηγία 2002/58/ΕΚ.

Πρωταρχικός σκοπός της Αρχής είναι η προστασία του πολίτη από την παράνομη επεξεργασία των προσωπικών του δεδομένων αλλά και η συνδρομή προς αυτόν σε κάθε περίπτωση που διαπιστώνεται παραβίαση των σχετικών δικαιωμάτων του σε κάθε επιχειρησιακό τομέα

(χρηματοπιστωτικά, υγεία, ασφάλιση, εκπαίδευση, δημόσια διοίκηση, μεταφορές, ΜΜΕ, κ.α.).

Επιπλέον, σκοπός της Αρχής είναι η υποστήριξη και καθοδήγηση των υπεύθυνων επεξεργασίας στην εκπλήρωση των υποχρεώσεων τους απέναντι στο νόμο, λαμβάνοντας υπόψη τις νέες ανάγκες υπηρεσιών της ελληνικής κοινωνίας, καθώς και την διείσδυση των σύγχρονων ψηφιακών επικοινωνιών και δικτύων. Ως εκ τούτου, η Αρχή στρέφει ιδιαίτερα την προσοχή της μεταξύ άλλων στην παρατήρηση και αντιμετώπιση ζητημάτων που προκύπτουν με την εξέλιξη των νέων τεχνολογιών και εφαρμογών.

Επίσης, η Αρχή συμμετέχει σε διεθνείς ομάδες εργασίας και σε Εθνικές Επιτροπές, όπως:[54]

- Κοινή Αρχή Ελέγχου Σένγκεν
- Κοινή Εποπτική Αρχή Ελέγχου Ευρωπόλ
- Ομάδα του άρθρου 29 της Οδηγίας 95/46/ΕΚ
- Ομάδα εργασίας της Ε.Ε. για την καταπολέμηση της αζήτητης ηλεκτρονικής επικοινωνίας
- Διεθνή ομάδα εργασίας του Βερολίνου για την προστασία των προσωπικών δεδομένων στις τηλεπικοινωνίες
- Εθνική Επιτροπή για τα Δικαιώματα του Ανθρώπου
- Ομάδα εργασίας για την Διαχείριση Καταγγελιών
- Αξιολόγηση Σένγκεν
- Εαρινή Σύνοδο Επιτροπών Ευρωπαϊκών Αρχών Προστασίας Δεδομένων
- Διεθνή Σύνοδο των Αρχών και των Επιτροπών Προστασίας Δεδομένων
- Working Party on Policy and Justice
- Εθνικό Συμβούλιο Ηλεκτρονικώς Επιχειρείν
- Επιτροπή Παρακολούθησης Ε.Π. Κοινωνία της Πληροφορίας

Η ελληνική Αρχή έχει εκδώσει Αποφάσεις και Γνωμοδοτήσεις σχετικά με υπηρεσίες ηλεκτρονικής διακυβέρνησης (βλ. ενδεικτικά Αποφάσεις 121/2014, 139/2014 για διαδικτυακές εφαρμογές του

Υπουργείου Παιδείας, αλλά και τη Γνωμοδότηση 1/2010 για το πρόγραμμα ΔΙΑΥΓΕΙΑ).

Κεφάλαιο 6

Ζητήματα Ασφάλειας και προστασίας της Ιδιωτικότητας σε περιβάλλον Η.Δ.

6.1 Εισαγωγή

Τα Πληροφοριακά Συστήματα Ηλεκτρονικής Διακυβέρνησης που παρέχουν υπηρεσίες θα πρέπει να διασφαλίζουν:

- *διαθεσιμότητα*
- *εμπιστευτικότητα*
- *ιδιωτικότητα*
- *ακεραιότητα*

Όσον αφορά την *διαθεσιμότητα*, πιθανά προβλήματα στην λειτουργία του Πληροφοριακού Συστήματος μπορούν να οδηγήσουν σε μεγάλης κλίμακας αναστάτωση ή και διακοπή (παύση) υπηρεσιών: αυτό , δυστυχώς, είναι αλήθεια λόγω της μεγάλης συνδεσιμότητας των πολιτών με το Διαδίκτυο.

Επιπλέον, για την σωστή λειτουργία της Η.Δ. απαιτείται συλλογή εμπιστευτικών δεδομένων. Οπότε, αυτά τα πληροφοριακά συστήματα θα πρέπει να εγγυώνται την παροχή ενός υψηλού επιπέδου *εμπιστευτικότητας* των δεδομένων που επεξεργάζονται. Πρέπει να παρέχουν όχι μόνο εμπιστοσύνη κατά την συλλογή των δεδομένων, αλλά και αποδείξεις ότι υπάρχουν δικλείδες ασφαλείας, ώστε αυτά τα δεδομένα να μην πέσουν σε λάθος χέρια.

Επίσης, υπάρχει η πιθανότητα συνδυασμού συλλεχθέντων δεδομένων μέσω των υπηρεσιών Η.Δ. από κακόβουλους χρήστες, η οποία μπορεί να δημιουργήσει τις προϋποθέσεις για παρείσφρηση στην *ιδιωτικότητα* του ατόμου μέσω εξαγωγής συμπερασμάτων για το άτομο τα οποία, φυσιολογικά, δεν θα έπρεπε να εξαχθούν.

Τέλος, επειδή τα δεδομένα είναι πολύ σημαντικά για την σωστή λειτουργία αυτών των υπηρεσιών, θα πρέπει να λαμβάνεται σοβαρά υπόψη η *ακεραιότητά* τους, δηλαδή η μη παραποίησή τους.

6.2. Ζητήματα Προστασίας της Ιδιωτικότητας σε περιβάλλον Η.Δ.

Όσον αφορά το μείζον ζήτημα της Ιδιωτικότητας, υπάρχουν τρία σημεία τα οποία θα πρέπει να ληφθούν υπόψη για τη σωστή λειτουργία των υπηρεσιών Η.Δ.

1. Έχει παρατηρηθεί αύξηση των συναλλαγών των πολιτών μέσω αυτών των ηλεκτρονικών υπηρεσιών, κάτι το οποίο δημιουργεί προβληματισμό σε σχέση με την ιδιωτικότητα των προσωπικών πληροφοριών που απαιτούνται για την διεκπεραίωση αυτών των συναλλαγών.
2. Παρατηρείται αύξηση στην χρήση έξυπνων καρτών (smart cards) και άλλων συναφών συσκευών μεταφοράς πληροφοριών. Αυτές οι συσκευές έχουν εμφυτευμένες προσωπικές πληροφορίες οι οποίες καθίστανται ευάλωτες σε σχέση με την ιδιωτικότητά τους.
3. Τέλος, η τρομοκρατική επίθεση της 11ης Σεπτεμβρίου 2001 στις Η.Π.Α. έχει προκαλέσει την αύξηση της παρακολούθησης των πολιτών, οι οποίοι ζητούνται -κατά κάποιον τρόπο- να εγκαταλείψουν ή να «χαλαρώσουν» το δικαίωμα στην Ιδιωτικότητά τους, ώστε να παρέχεται μεγαλύτερη ασφάλεια.

Αυτοί οι παραπάνω λόγοι θέτουν την Ιδιωτικότητα των προσωπικών δεδομένων εξαιρετικά σημαντική για την προστασία της Δημόσιας Διοίκησης. Πιστεύεται ότι, στο μέλλον, η ανησυχία των πολιτών για τον τρόπο με τον οποίο συλλέγονται, αποθηκεύονται, επεξεργάζονται και μεταδίδονται τα προσωπικά τους δεδομένα, θα αποτελεί ένα σημαντικό εμπόδιο στην σωστή λειτουργία των υπηρεσιών Η.Δ. Όσο περισσότερα προσωπικά δεδομένα βρίσκονται στην βάση δεδομένων της Η.Δ., τόσο μεγαλύτερο ρίσκο δημιουργείται για την προσβολή τους από τρίτους ή στην περίπτωση που ο Δημόσιος τομέας χρησιμοποιεί τα δεδομένα για αμφίβολους σκοπούς.

Στις υπηρεσίες Η.Δ. όπου είναι απλά πληροφοριακού χαρακτήρα, δεν τίθεται καταρχήν θέμα Ιδιωτικότητας , αφού ο χρήστης δεν παρέχει πληροφορίες στην υπηρεσία.

Ωστόσο, στις υπηρεσίες όπου προσφέρεται πλήρης ηλεκτρονική διεκπεραίωση, οι πολίτες-χρήστες πρέπει να παρέχουν ευαίσθητα προσωπικά δεδομένα που εγείρουν θέμα ιδιωτικότητας.

6.2.1. Αντιμετώπιση ζητημάτων προστασίας της Ιδιωτικότητας

Η ομάδα Αποτίμησης των Εφαρμογών της Επιστήμης και της Τεχνολογίας του Ευρωπαϊκού Κοινοβουλίου (STOA) ανέπτυξε το έργο "Security of eGovernment Systems" το οποίο έχει στόχο στο να βοηθήσει στη δημιουργία πολιτικών ασφάλειας και ιδιωτικότητας στα περιβάλλοντα Η.Δ. στα πλαίσια της Ευρωπαϊκής Ένωσης. Μέσα από αυτό το έργο, προτείνονται οι παρακάτω τρόποι για αύξηση της προστασίας της Ιδιωτικότητας σε συστήματα Η.Δ.:[55]

- Η επιβολή μεγαλύτερων προστίμων στις υπηρεσίες και στους οργανισμούς που δεν συμμορφώνονται με τα μέτρα και τους κανονισμούς.
- Τα δικαιώματα των πολιτών ενδυναμώνονται με την αύξηση των απαιτήσεων για διαφάνεια στην επεξεργασία των δεδομένων και περιλαμβάνουν και νέα δικαιώματα όπως "το δικαίωμα στη λήθη" και το δικαίωμα της "μεταφοράς δεδομένων".
- Ο προσχέδιος κανονισμός στοχεύει στην απευθείας εφαρμογή της Ευρωπαϊκής Νομοθεσίας σε όλα τα κράτη - μέλη της Ε.Ε. και αντικατάσταση των εθνικών νόμων.
- Επιβολή της ιδιωτικότητας ως σχεδιαστική παράμετρο κατά την ανάπτυξη κάθε νέας τεχνολογίας / υπηρεσίας (Privacy by Design base). Η αρχή της ιδιωτικότητας-ήδη-κατά-το-σχεδιασμό προβλέπεται στον *Κανονισμό COM(2012) 11 Final του Ευρωπαϊκού Κοινοβουλίου* [48] ως "Προστασία Δεδομένων βάση σχεδιασμού" (Data Protection by Design) και η οποία θα αυξήσει το κίνητρο προς τους Δημόσιους φορείς να χρησιμοποιήσουν την συγκεκριμένη τεχνική στην σχεδίαση των υπηρεσιών τους.

6.2.2. Privacy by Design

Η αρχή *Privacy by Design (Ιδιωτικότητα-ήδη-κατά-τον-σχεδιασμό*) είναι η ενσωμάτωση των αρχών προστασίας της ιδιωτικότητας από τη φάση, ακόμη, του σχεδιασμού ενός πληροφοριακού συστήματος με σκοπό την προστασία των δεδομένων και της ιδιωτικότητας των χρηστών.

Σύμφωνα με την κα Cavoukian Ann, Επίτροπο Πληροφοριών και Εμπιστευτικότητας του Οντάριο στον Καναδά, αυτός ο τρόπος προστασίας της Ιδιωτικότητας έχει επτά θεμελιώδεις αρχές: [56]

1. *Προφυλακτική όχι Διορθωτική*: Η προσέγγιση της Privacy by Design είναι να προλαμβάνει τα γεγονότα πριν αυτά συμβούν, δηλαδή δεν περιμένει να υλοποιηθούν οι κίνδυνοι της προστασίας της ιδιωτικής ζωής.
2. *Η προστασία της ιδιωτικής ζωής ως προεπιλεγμένη ρύθμιση:* Διασφαλίζει ότι τα προσωπικά δεδομένα προστατεύονται αυτομάτως σε κάθε σύστημα πληροφοριακό.
3. *Η προστασία της Ιδιωτικής ζωής είναι χαραγμένη στη σχεδίαση*: Δηλαδή είναι αναπόσπαστο μέρος του πληροφοριακού συστήματος χωρίς να μειώνει τη λειτουργικότητα.
4. *Πλήρης λειτουργικότητα: Θετικό Άθροισμα, όχι Μηδενικό:* Αποφεύγει εσφαλμένες διχοτομήσεις, όπως η προστασία της ιδιωτικότητας έναντι της ασφάλειας, αποδεικνύοντας ότι και οι δύο μπορούν να συνυπάρχουν.
5. *Πλήρης Ασφάλεια: Προστασία για όλη τη ζωή*: Αφού χαραχθεί στο σύστημα, πριν συγκεντρωθεί το πρώτο στοιχείο δεδομένων, επεκτείνεται σε όλον τον κύκλο ζωής των δεδομένων, διασφαλίζοντας ότι όλα τα δεδομένα διατηρούνται με ασφάλεια και μετά, καταστρέφονται με ασφάλεια, στο τέλος της διαδικασίας.
6. *Ορατότητα και Διαφάνεια*: Διασφαλίζει ότι οποιαδήποτε και αν είναι η τεχνολογία ή η πρακτική, λειτουργεί σύμφωνα με τις δηλωμένες υποσχέσεις και τους στόχους, ενώ επιπλέον, τα συστατικά μέρη και οι λειτουργίες παραμένουν ορατά και διαφανή.

7. *Σεβασμός για την Ιδιωτική Ζωή του χρήστη*: Μέσω ισχυρών προεπιλογών προστασίας της ιδιωτικής ζωής.

Η κα. Μήτρου Λίλιαν προσθέτει [57] ότι *"η τεχνολογική προστασία της ιδιωτικότητας δεν συντίθεται απλώς από τις επιταγές για υιοθέτηση της ως σχεδιαστικής παραμέτρου, αλλά περιλαμβάνει και την αξιολόγηση κινδύνων και των επιπτώσεων στην ιδιωτικότητα καθώς και την υιοθέτηση της προστασίας ως εξ ορισμού επιλογή (privacy by default)".*

Σύμφωνα και με την Ευρωπαία Επίτροπο σε θέματα Δικαιοσύνης, Reding Viviane [58] *"...μπορούμε μόνο να φανταστούμε πώς η τεχνολογία θα αλλάξει τις ζωές μας αύριο. Δεν γνωρίζουμε ακόμα τις λεπτομέρειες. Αυτός είναι ο λόγος που το κανονιστικό περιβάλλον πρέπει να είναι προστατευμένο από το μέλλον, να είναι τεχνολογικά ουδέτερο. Αυτός είναι και ο λόγο που η Privacy by Design πρέπει να είναι απαραίτητη...."*

Για την υιοθέτηση της Privacy by Design απαιτείται η ανάπτυξη μιας βάσης γνώσης, η οποία θα περιλαμβάνει αρχιτεκτονικές, σχεδιαστικά πρότυπα, τεχνικές ανωνυμίας και ψευδωνυμίας με σκοπό να ορίζουν τι θα περιέχει η PbD. Επιστημονικά έργα της Ευρωπαϊκής Ένωσης, όπως το PRIME, το PRIMELIFE και το ABC4TRUST παρέχουν τη βάση για την ανάπτυξη αυτής της γνωσιολογικής πλατφόρμας, η οποία, όμως, θα πρέπει να είναι υπό την εποπτεία ενός ανεξάρτητου Ευρωπαϊκού οργανισμού.[55]

6.2.3. Τεχνολογίες Ενίσχυσης και Προστασίας της Ιδιωτικότητας

Το Διαδίκτυο δεν σχεδιάστηκε για να προστατεύει την Ιδιωτικότητα των χρηστών, οπότε έπρεπε να βρεθούν λύσεις για την αντιμετώπιση επιθέσεων κακόβουλων χρηστών που είχανε σκοπό την αποκάλυψη και υποκλοπή πληροφοριών. Η κρυπτογράφηση δεν παρέχει μία ολοκληρωμένη προστασία από τους κακόβουλους χρήστες ή από επιθέσεις

ανάλυσης κίνησης, οπότε αναπτύχθηκαν οι Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας (Privacy Enhanced Technologies, PETs) για να ενισχύσουν την προστασία της Ιδιωτικότητας στα Πληροφοριακά Συστήματα, τα οποία υποστηρίζουν υπηρεσίες Η.Δ. και όχι μόνο.

Συγκεκριμένος ορισμός δεν υπάρχει για αυτές τις τεχνολογίες, αλλά μπορούμε να τις αντιληφθούμε ως "*ένα ολοκληρωμένο σύστημα ψηφιακών μέτρων που προστατεύουν την Ιδιωτικότητα εξαλείφοντας ή περιορίζοντας τη μη αναγκαία αποκάλυψη, συλλογή, τήρηση, διαμοιρασμό των προσωπικών δεδομένων, συχνά με την παροχή εργαλείων για την ενίσχυση του ελέγχου του χρήστη πάνω στα προσωπικά του στοιχεία, και χωρίς να μειώνεται η λειτουργικότητα του πληροφοριακού συστήματος*". [57]

Χαρακτηριστικά των PETs αποτελούν:

- η παροχή δυνατότητας ελέγχου των χρηστών ως προς τον βαθμό κοινοποίησης και μετάδοσης των προσωπικών τους δεδομένων.
- ο περιορισμός της αποκάλυψης προσωπικών δεδομένων των χρηστών κατά τη χρήση του Διαδικτύου.
- η συμμόρφωση με τις αρχές της Ιδιωτικότητας και της αντίστοιχης νομοθεσίας.

Οι βασικές *ιδιότητες* που πρέπει να έχουν οι PETs για να είναι χρήσιμες και αποτελεσματικές, σύμφωνα με τον Goldeberg (2007) [59], είναι:

- *ευχρηστία* (usability): οι χρήστες να μπορούν να χρησιμοποιήσουν ένα PET εργαλείο και να θέλουν να το χρησιμοποιήσουν, ασχέτως κόστους και δυσκολιών.
- *αποτελεσματικότητα* (efficiency): τα εργαλεία PETs να υλοποιούν το σκοπό για τον οποίο δημιουργήθηκαν.
- *ευρωστία* (robustness): το εργαλείο PET να παρέχει την μεγαλύτερη δυνατή προστασία.

Εκτός, όμως, από τις παραπάνω ιδιότητες, οι PETs θα πρέπει να ικανοποιούν και να διαθέτουν και τα βασικά χαρακτηριστικά της Ιδιωτικότητας, τα οποία αναφέρθηκαν στην παράγραφο 1.3.1. και είναι:

1. *η Ανωνυμία*
2. *η Μη - Συνδεσιμότητα*
3. *η Μη - Ανιχνευσιμότητα*
4. *η Ψευδωνυμία*
5. *και η Διαχείριση Ταυτότητας*

6.2.4. Κατηγοριοποίηση Τεχνολογιών PET's

Οι τεχνολογίες ενίσχυσης της ιδιωτικότητας (PET's) μπορούν να ταξινομηθούν ενδεικτικά στις εξής:

- *ταξινόμηση FIDIS* (Future of Identity in the Information Society), η οποία χρησιμοποιείται στο Ευρωπαϊκό πρόγραμμα για το Μέλλον της Ταυτότητας στην Κοινωνία της Πληροφορίας. Αποτελείται από εργαλεία διαφάνειας (transparency tools) και αδιαφάνειας (opacity tools), τύπου MixMaster και Tor. Στην παρούσα διπλωματική, επειδή ασχολούμαστε με υπηρεσίες Ηλεκτρονικής Διακυβέρνησης, δεν θα μπορούσαμε να ασχοληθούμε με τα εργαλεία αδιαφάνειας, μιας και πρέπει να αυθεντικοποιούμαστε όταν συναλλασσόμαστε με τον Δημόσιο Τομέα. Με τα εργαλεία διαφάνειας δίνεται η δυνατότητα στον χρήστη να δει τι προσωπικά δεδομένα υφίστανται επεξεργασία, με ποιον τρόπο και ποιος τα επεξεργάζεται. Τέτοια παραδείγματα αποτελούν τα αρχεία log, οι ελεγκτικοί παράγοντες και οι έλεγχοι ιδιωτικότητας (privacy audits). [60]
- *ταξινόμηση METAgroup* η οποία περιλαμβάνει εργαλεία για την προστασία και την διαχείριση της ιδιωτικότητας, όπως ενημερωτικά εργαλεία και εργαλεία διαχείρισης τα οποία προσφέρονται ως add-on's σε σουίτες διαχείρισης του πληροφοριακού συστήματος. Επιπλέον παρέχει εργαλεία για ψευδωνυμία, προϊόντα και υπηρεσίες ανωνυμίες,

εργαλεία κρυπτογράφησης, φίλτρα, track erasers, τα οποία, όμως, δεν μπορούν να έχουν σχέση με την χρήση υπηρεσιών Ηλεκτρονικής Διακυβέρνησης κατά την οποία οφείλει ο κάθε χρήστης να αυθεντικοποιείται.

6.3. Ζητήματα προστασίας της ιδιωτικότητας στα ηλεκτρονικά διαβατήρια (e-passports)

Τα δεδομένα τα οποία περιλαμβάνονται στα e-passports και τα οποία αποθηκεύονται στο RFID chip, αποτελούν πληροφορίες που σχετίζονται με ένα αναγνωρισμένο ή αναγνωρίσιμο φυσικό πρόσωπο, όπως ο κάτοχος του διαβατηρίου και συνεπώς, θεωρούνται προσωπικά του δεδομένα, σύμφωνα και με την Ευρωπαϊκή Οδηγία 95/46/ΕΚ. Αυτό σημαίνει ότι η Ευρωπαϊκή Νομοθεσία για την προστασία των δεδομένων εφαρμόζεται στα ηλεκτρονικά διαβατήρια και οι νόμοι για την προστασία των δεδομένων θα πρέπει να είναι σεβαστοί.

Όταν το διαβατήριο ελέγχεται από το εξουσιοδοτημένο προσωπικό, η επεξεργασία των αποθηκευμένων δεδομένων πρέπει να γίνεται νόμιμα και μόνο από το εξουσιοδοτημένο προσωπικό, σύμφωνα με την Ευρωπαϊκή Οδηγία 95/46/ΕΚ. Σε περίπτωση μη εξουσιοδοτημένης ανάγνωσης των δεδομένων, όπως δημιουργίας κλώνου (skimming) ή υποκλοπής (eavesdropping), ο κάτοχος των δεδομένων δεν γνωρίζει ότι τα δεδομένα του συλλέγονται παράνομα. Από τη στιγμή που ο κάτοχος δεν συναινεί σε κάτι το οποίο δεν γνωρίζει, η επεξεργασία των δεδομένων είναι παράνομη.

Ο κάτοχος του διαβατηρίου πρέπει να είναι ενήμερος για τα δεδομένα που περιλαμβάνονται σε αυτό και για τους τρόπους με τους οποίους μπορεί να έχει πρόσβαση, να διορθώσει, να σβήσει λανθασμένα δεδομένα που είναι αποθηκευμένα. Επιπλέον, προσωπικά δεδομένα πρέπει να επεξεργάζονται δίκαια και νόμιμα, σύμφωνα και με την Ευρωπαϊκή

Οδηγία 95/46/ΕΚ. Τα δεδομένα συλλέγονται για συγκεκριμένους και νόμιμους σκοπούς και μπορούν να υποστούν περαιτέρω επεξεργασία με τρόπο συμβατό σύμφωνα με αυτές τις αρχές.

Όσον αφορά τους ελέγχους που πραγματοποιούνται από τις Αρχές χωρών εκτός Ευρωπαϊκής Ένωσης, η χρήση του RFID chip ως αποθηκευτικού μέσου στο διαβατήριο δημιουργεί σημαντική ανησυχία σε σχέση με την ιδιωτικότητα του ατόμου. Όταν προσωπικά δεδομένα υπόκεινται σε επεξεργασία σε τρίτες χώρες, αυτές θα πρέπει να διασφαλίζουν ένα επαρκές επίπεδο προστασίας, σύμφωνα και με την Νομοθεσία της Ε.Ε., αλλά και με τις διεθνείς συμφωνίες για τις διαδικασίες που πρέπει να ακολουθούνται.

6.3.1. Βιομετρικές μέθοδοι και Προστασία της Ιδιωτικότητας

Τα βιομετρικά συστήματα εγείρουν σοβαρές ανησυχίες κυρίως στον τομέα της ιδιωτικής ζωής και της προστασίας δεδομένων. Δεδομένου ότι οι βιομετρικές τεχνολογίες δεν μπορούν να εξασφαλίσουν απόλυτη ακρίβεια, υπάρχει πάντα έμμεσος κίνδυνος από εσφαλμένες ταυτοποιήσεις. Σοβαρές ζημιές για τον κάτοχο του διαβατηρίου μπορεί να προκαλέσει η υποκλοπή του με την χρήση παραποιημένων ή κλεμμένων βιομετρικών πηγών.

Όμως, δεν μπορούμε να παραβλέψουμε ότι στο μέλλον, λόγω της ευρείας χρήσης των βιομετρικών δεδομένων, ο χρήστης δεν θα χρειάζεται να καταχωρεί τον μυστικό κωδικό του (password) για να αποκτήσει πρόσβαση σε κάποια διαδικτυακή υπηρεσία, όπως γίνεται σήμερα. Αντίθετα, θα πιστοποιεί την ταυτότητά του μέσω ευρείας χρήσης δακτυλικών αποτυπωμάτων, τοποθετώντας, π.χ. στον υπολογιστή μία συσκευή ή αφήνοντας το έξυπνο κινητό του ή την ταμπλέτα του να αναγνωρίσουν το δακτυλικό του αποτύπωμα, τη φωνή ή την ίριδα του ματιού του. Τα δακτυλικά αποτυπώματα του χρήστη ή το μοναδικό αναγνωριστικό οποιασδήποτε USB συσκευής δεν θα στέλνονται πουθενά

στο Διαδίκτυο, αλλά θα ελέγχονται τοπικά. Το μόνο που θα μεταφέρεται θα είναι τα κλειδιά κρυπτογραφήσεως που δεν μπορούν να αποκρυπτογραφηθούν, για να κλαπεί η ταυτότητα του χρήστη.

Σε σχέση με την χρήση βιομετρικών μεθόδων, η ελληνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) έχει αποφανθεί ότι, ιδίως ορισμένες από αυτές, θίγουν κατάφωρα την ανθρώπινη αξιοπρέπεια και την προσωπικότητα του υποκειμένου των δεδομένων (βλ. ενδεικτικά Αποφάσεις 127/2012, 17/2014, καθώς και τη Γνωμοδότηση 3/2014).

Τίθεται το ζήτημα αν η εφαρμογή βιομετρικών μεθόδων συνιστά προσβολή των ατομικών δικαιωμάτων, μιας και κάποιος μπορεί να διερωτάται αν τα δεδομένα αποθηκεύονται σε μία κεντρική βάση δεδομένων και αν ναι, ποιος είναι ο διαχειριστής των προσωπικών δεδομένων, από τον οποίο το άτομο μπορεί να αξιώσει την εφαρμογή των δικαιωμάτων του.

Η απόφαση ΔΕΕ Michael Schwarz κατά κρατιδίου Bochum (C-291/2012)

Στην εν λόγω υπόθεση, ο Michael Schwarz αιτήθηκε από το κρατίδιο του Bochum της Γερμανίας την χορήγηση διαβατηρίου, αρνούμενος όμως, να υποστεί την υποχρεωτική λήψη των ψηφιακών δακτυλικών του αποτυπωμάτων. Κατόπιν της απόρριψης του αιτήματός του από το κρατίδιο του Bochum, ο Schwarz προσέφυγε ενώπιον του αιτούντος διοικητικού δικαστηρίου Gelsenkirchen ζητώντας του να διατάξει το εν λόγω κρατίδιο να του χορηγήσει διαβατήριο χωρίς την λήψη των ψηφιακών δακτυλικών του αποτυπωμάτων. Ενώπιον του δικαστηρίου αυτού, ο Schwarz αμφισβήτησε το κύρος του κανονισμού 2252/2004, με τον οποίο επιβάλλεται η υποχρέωση λήψεως των ψηφιακών δακτυλικών αποτυπωμάτων των αιτούντων την έκδοση διαβατηρίου. Ο Schwarz υποστήριξε ότι ο κανονισμός αυτός δεν στηρίζεται σε κατάλληλη νομική βάση και πάσχει από διαδικαστική πλημμέλεια.

Το διοικητικό δικαστήριο Gelsenkirchen αποφάσισε να αναστείλει την ενώπιων του διαδικασία και να υποβάλει στο Δικαστήριο της Ευρωπαϊκής Ένωσης (Δ.Ε.Ε.) προδικαστικό ερώτημα αναφορικά με την εγκυρότητα του άρθρου 1, παράγραφος 2, του Κανονισμού 2252/2004. Πιο συγκεκριμένα, το γερμανικό διοικητικό δικαστήριο Gelsenkirchen με το προδικαστικό του ερώτημα ζήτησε από το Δ.Ε.Ε. να εξετάσει:

- την καταλληλότητα της νομικής βάσης του Κανονισμού
- την πιθανή ύπαρξη πλημμέλειας κατά τη διαδικασία εκδόσεώς του
- και την ενδεχόμενη προσβολή των θεμελιωδών δικαιωμάτων σεβασμού της ιδιωτικής ζωής και προστασίας των προσωπικών δεδομένων.

Μετά από την απόρριψη των δύο πρώτων λόγων ακυρότητας, έμφαση δόθηκε στην ενδεχόμενη προσβολή της ιδιωτικής ζωής και των προσωπικών δεδομένων. Το Δικαστήριο δέχτηκε ότι η, εκ μέρους των αρμοδίων εθνικών αρχών, λήψη και αποθήκευση ψηφιακών δακτυλικών αποτυπωμάτων συνιστά επεξεργασία δεδομένων προσωπικού χαρακτήρα και επέμβαση στο δικαίωμα ιδιωτικότητας και προστασίας προσωπικών δεδομένων.

Σύμφωνα με το παραπάνω περιστατικό, διαπιστώνουμε μία υποχώρηση του δικαιώματος της ιδιωτικότητας προς χάριν της δημόσιας ασφάλειας, κάτι το οποίο χρήζει αυστηρής νομοθετικής αντιμετώπισης.

Ένας από τους μεγάλους κινδύνους των βιομετρικών συστημάτων είναι ότι εισβάλλουν στην ιδιωτικότητα των ατόμων. Ο μεγαλύτερος φόβος που εκφράζεται είναι η δημιουργία βάσης βιομετρικών δεδομένων υπό κεντρική διαχείριση και η χρήση των δεδομένων για άλλους πλην από τους κατά το νόμο προβλεπόμενους σκοπούς. [24]

6.4. Ζητήματα προστασίας της ιδιωτικότητας κατά την χρήση της τεχνολογίας ABC

Η αλήθεια είναι ότι οι επιπτώσεις της τεχνολογίας δεν μπορούν εύκολα να προβλεφτούν μέχρι την πλήρη ανάπτυξη της τεχνολογίας. Ωστόσο, από την στιγμή που εδραιωθεί μία τεχνολογία, δύσκολα αλλάζει. Η τεχνολογία των Attribute - Based Credentials θα πρέπει να αντιμετωπίζεται ως ένα κοινωνικό-τεχνολογικό σύστημα το οποίο απαιτεί την συνύπαρξη του ανθρώπου και των υπολογιστών.

Η συγκεκριμένη τεχνολογία ελαχιστοποιεί την διαρροή προσωπικών δεδομένων και πρέπει να θεωρείται τεχνολογία που προσφέρει προστασία δεδομένων βάσει σχεδιασμού *(data protection by design)* και όχι εξ ορισμού *(data protection by default)*, επειδή αρκετοί παράγοντες είτε δεν έχουν καλυφθεί επαρκώς σε σχέση με την ασφάλεια, είτε εξαρτώνται από τον σχεδιαστή της συγκεκριμένης τεχνολογίας.

Σε σχέση με την ιδιωτικότητα, ένας ανασταλτικός παράγοντας, ο οποίος και εμποδίζει την ανάπτυξη των ABC τεχνολογιών, είναι η κοινή πρακτική των νομικών και των δικηγόρων για συλλογή δεδομένων με σκοπό την άσκηση αστικής αγωγής ή ποινικής δίωξης. Η ανάπτυξη εργαλείων ABC τεχνολογιών παρεμποδίζεται από τέτοιες νομικές πρακτικές. Η εκτίμηση ότι οι ABC τεχνολογίες μπορούν να επιλύσουν πρακτικά και νομικά ζητήματα που έχουν σχέση με την ιδιωτικότητα των ατόμων αποτελεί προσδοκία που προσδοκάται στο μέλλον να συμβεί.

Κεφάλαιο 7

Ανοιχτά Ζητήματα κατά την υιοθέτηση ηλεκτρονικών ταυτοτήτων στην Ε.Ε.

7.1. Προβληματισμοί και καταγραφή λύσεων στα e-passports

Οι κίνδυνοι που υπάρχουν για τα e-passports οφείλονται σε δύο παράγοντες:

- την εγγύτητα επικοινωνίας (RFID) του διαβατηρίου με άλλα συστήματα
- και την ύπαρξη βιομετρικών δεδομένων μέσα στο διαβατήριο

Για την αποτροπή και μείωση των πιθανοτήτων να κλαπούν τα δεδομένα από το ηλεκτρονικό διαβατήριο, κυκλοφορούν στην αγορά προστατευτικά καλύμματα για διαβατήρια, τα οποία είναι, συνήθως, κατασκευασμένα από αλουμίνιο και σκοπό έχουν την προστασία του διαβατηρίου από ενδεχόμενη λαθραία ανάγνωση της ετικέτας RFID, όπου είναι αποθηκευμένα τα προσωπικά δεδομένα του κατόχου του. Τα συγκεκριμένα καλύμματα μπορεί να δείχνουν όμορφα και να διατηρούν το διαβατήριο σε άψογη κατάσταση, αλλά τελικά ο πραγματικός λόγος είναι η προστασία των δεδομένων. Πιο απλή και προσιτή οικονομικά λύση είναι να τυλίξουμε το διαβατήριο με αλουμινόχαρτο, το οποίο λειτουργεί κατά τον ίδιο τρόπο.

Υπάρχουν αναφορές ότι έχουν συμβεί *παθητικές υποκλοπές (passive eavesdropping)* κατά τη διάρκεια επικοινωνίας του διαβατηρίου με τον νόμιμο αναγνώστη, καθώς και *ενεργητικές υποκλοπές (active eavesdropping)* κατά τις οποίες ο υποκλοπέας ξεκινά την επικοινωνία με το διαβατήριο. Οι περιπτώσεις αυτές συνέβησαν σε απόσταση, μεταξύ του διαβατηρίου και του υποκλοπέα, μικρότερης των δέκα μέτρων.

Τα e-passports των Η.Π.Α. καλύπτονται από ένα μεταλλικό κάλυμμα το οποίο προστατεύει από υποκλοπή, μπλοκάροντας τις ραδιοσυχνότητες, όταν είναι κλειστά. Έτσι, μόνο όταν είναι ανοικτό το διαβατήριο, οι ραδιοσυχνότητες του νόμιμου αναγνώστη μπορούν να διαβάσουν τα δεδομένα της ετικέτας RFID του διαβατηρίου.

Επίσης, κυκλοφορεί στην αγορά μία κάρτα, η οποία έχει μία ετικέτα RFID, και η οποία προσφέρει ενεργητική RFID προστασία από ανεπιθύμητα RFID σήματα, τα οποία προσπαθούν να επικοινωνήσουν με το διαβατήριό μας.

Τέλος, ίσως, μία πρόταση για την καλύτερη προστασία της ιδιωτικότητας και των προσωπικών δεδομένων στα ηλεκτρονικά διαβατήρια θα ήταν να ελεγχτεί η δυνατότητα μετατροπής των ασύρματων μηχανισμών ελέγχου των e-passports σε ενσύρματους.

7.2. Ενσωμάτωση των e-passports στην Ευρωπαϊκή Ένωση

Σύμφωνα με το άρθρο 1 του Ευρωπαϊκού Κανονισμού 2252/2004 [61] "*διαβατήρια και ταξιδιωτικά έγγραφα θα περιλαμβάνουν έναν μέσο αποθηκευτικό χώρο ο οποίος θα περιέχει την φωτογραφία προσώπου. Τα κράτη μέλη θα συμπεριλάβουν, επίσης, τα δακτυλικά αποτυπώματα σε διαλειτουργική μορφή στα e-passports. Τα δεδομένα θα ασφαλιστούν και ο αποθηκευτικός χώρος θα έχει επαρκές μέγεθος και την δυνατότητα να εγγυηθεί την ακεραιότητα, την αυθεντικότητα και την εμπιστευτικότητα των δεδομένων*".

Οι προδιαγραφές που καθορίζονται από τον παραπάνω Ευρωπαϊκό Κανονισμό δεσμεύουν όλα τα κράτη μέλη της Ε.Ε. με την συνθήκη Σένγκεν -εκτός από την Ιρλανδία και τη Μεγάλη Βρετανία, και περιλαμβάνει την Ισλανδία, την Νορβηγία και την Ελβετία-. Αυτές οι χώρες ήταν υποχρεωμένες να ενσωματώσουν στο διαβατήριο ψηφιακή φωτογραφία του κατόχου του μέχρι τον Αύγουστο του 2006 και δακτυλικά αποτυπώματα μέχρι τον Ιούνιο του 2009.

Ενδεικτικά, τα σύγχρονα βρετανικά διαβατήρια περιλαμβάνουν μόνο ψηφιακή φωτογραφία και όχι δακτυλικά αποτυπώματα, ενώ τα γερμανικά διαβατήρια, μετά το Νοέμβριο του 2007, περιέχουν δύο δακτυλικά αποτυπώματα, ένα από κάθε χέρι και την ψηφιακή φωτογραφία. Τα ολλανδικά διαβατήρια περιέχουν, επίσης, δύο δακτυλικά αποτυπώματα και είναι το μόνο κράτος μέλος της Ε.Ε. το οποίο σχεδιάζει να αποθηκεύσει κεντρικά σε βάση δεδομένων αυτά τα αποτυπώματα.

7.3. Ενσωμάτωση των e-passports στην Ελλάδα

Στην Ελλάδα, το ηλεκτρονικό διαβατήριο εισήχθη στις 26 Αυγούστου 2006, περιέχει 32 σελίδες και έχει ισχύ πέντε (5) χρόνια για τους ενήλικες, και δύο (2) χρόνια για τα παιδιά κάτω των 14 ετών. Εκδίδεται από την Διεύθυνση Διαβατηρίων/ Αρχηγείο Ελληνικής Αστυνομίας, και ενώ μέχρι τον Ιούνιο 2009 περιείχε μόνο δακτυλικό αποτύπωμα, στην συνέχεια προστέθηκε και η ψηφιακή φωτογραφία του κατόχου του. [62]

Το εξώφυλλο του ελληνικού e-passport,

Πηγή: en.wikipedia.org/wiki/Greek_passport

Το ελληνικό ηλεκτρονικό διαβατήριο περιέχει τα εξής στοιχεία του κατόχου του:

- Τύπος διαβατηρίου
- Αριθμός διαβατηρίου
- Χώρα (ΕΛΛ)
- Επίθετο (με ελληνικούς και λατινικούς χαρακτήρες)
- Όνομα (με ελληνικούς και λατινικούς χαρακτήρες)
- Εθνικότητα (Ελληνική)
- Ημερομηνία Γέννησης
- Τόπος Γέννησης (με ελληνικούς και λατινικούς χαρακτήρες)

- Φύλο (M/F)
- Ημερομηνία Έκδοσης
- Ημερομηνία Λήξης
- Γραφείο Έκδοσης (με ελληνικούς και λατινικούς χαρακτήρες)

7.4. Ενσωμάτωση της ηλεκτρονικής ταυτότητας στην Ευρωπαϊκή Ένωση

Τα τελευταία χρόνια, τα περισσότερα κράτη - μέλη της Ε.Ε. έχουν σταδιακά υιοθετήσει συστήματα διαχείρισης ηλεκτρονικών ταυτοτήτων στο πλαίσιο εκσυγχρονισμού των δημόσιων υπηρεσιών τους, ενώ οι περισσότερες υποστηρίζουν την Υποδομή Δημόσιου Κλειδιού στις ηλεκτρονικές τους ταυτότητες.

Επόμενος στόχος είναι η διασύνδεση των εθνικών ηλεκτρονικών ταυτοτήτων , κάτι που μέχρι τώρα ισχύει σε λίγες χώρες. Η σπουδαιότητα που δίνει η Ευρωπαϊκή Επιτροπή στο θέμα αυτό είναι ιδιαίτερα υψηλή. Τον Αύγουστο 2013, η Ευρωπαϊκή Επιτροπή ανακοίνωσε την χρηματοδότηση ύψους 13,7 εκατ. ευρώ για διασυνοριακές ψηφιακές υπηρεσίες, ώστε να συνδέονται οι ηλεκτρονικές ταυτότητες των πολιτών σε εθνικό αλλά και σε ευρωπαϊκό επίπεδο. [63]

7.5. Ενσωμάτωση της ηλεκτρονικής ταυτότητας στην Ελλάδα

Στην Ελλάδα, με βάση πληροφορίες που αναφέρονται στην Wikipedia, χωρίς να είναι σαφείς οι πηγές αυτών [64], η ηλεκτρονική

ταυτότητα που ακόμα δεν έχει θεσπιστεί, προβλέπεται να είναι υποχρεωτική για τους πολίτες. Η ελληνική ηλεκτρονική ταυτότητα δεν θα αποθηκεύει δεδομένα, θα βασίζεται τεχνολογικά στην Υποδομή Δημόσιου Κλειδιού, και θα αποτελεί ένα ψηφιακό διαβατήριο ώστε ο κάθε πολίτης να μπορεί να προσπελάσει δεδομένα του που είναι αποθηκευμένα σε υπηρεσίες του Δημοσίου, χωρίς την ύπαρξη της γραφειοκρατίας.

Η ελληνική κάρτα πολίτη θα περιλαμβάνει, τόσο εκτυπωμένα στην επιφάνειά της, όσο και εντός της, τα στοιχεία της αστυνομικής ταυτότητας του κατόχου της και επιπλέον:

- αριθμός δημοτολογίου και δήμος
- αριθμός φορολογικού μητρώου
- αριθμός μητρώου κοινωνικής ασφάλισης
- αριθμός δελτίου ταυτότητας [64]

Επιπλέον, θα συνοδεύεται από σειριακό αριθμό και κωδικό πρόσβασης που θα επιτρέπουν τον κάτοχό τους σε δικτυακές υπηρεσίες του Δημόσιου Τομέα. Πιθανώς μελλοντικά να υπάρξει και δυνατότητα ενσωμάτωσης της ψηφιακής υπογραφής του κατόχου της.

Όπως προαναφέρθηκε, η Ελλάδα δεν έχει ακόμη προχωρήσει στη θέσπιση και υλοποίηση κάρτας πολίτη. Ωστόσο, φαίνεται ότι μάλλον είναι απλά ζήτημα χρόνου: σε σχέδιο νόμου που τέθηκε σε διαβούλευση το Μάρτιο του 2015 (http://www.opengov.gr/ypes/?p=2575), στο αρ. 16 αυτού αναφέρονται, μεταξύ άλλων, τα εξής: «α) *Μια πιλοτική εφαρμογή της «κάρτας πολίτη» που θα περιλαμβάνει ένα ή περισσότερα αναγνωριστικά που σχετίζονται με τα βασικά μητρώα που περιγράφονται στην παράγραφο 1 του άρθρου 32 του Ν. 3979/2011, όπως τροποποιήθηκε και ισχύει, μπορεί να εφαρμοστεί και ως μέσο ταυτοποίησης των δικαιούχων και χορήγησης της επιδότησης σίτισης (…), ή για ανάλογες επιδοτήσεις, με έλεγχο των εισοδηματικών κριτηρίων βάσει των τηρουμένων ηλεκτρονικών αρχείων από το Υπουργείο Οικονομικών και Εργασίας και Κοινωνικής Αλληλεγγύης. Για την δημιουργία του αρχείου που θα χρησιμοποιηθεί για κάθε περίπτωση χορήγησης της επιδότησης, υπεύθυνος Επεξεργασίας είναι το Υπουργείο Εργασίας και Κοινωνικής*

Αλληλεγγύης. Για το σκοπό αυτό, χρησιμοποιούνται οι βάσεις δεδομένων που τηρούνται από το ΤΑΧΙS και το ΗΔΙΚΑ για την διακρίβωση του εισοδήματος και της οικογενειακής κατάστασης. Η διάρκεια τήρησης των στοιχείων ορίζεται διετής από την ημερομηνία συλλογής τους.» Συνεπώς, είναι η πρώτη φορά που η έννοια της κάρτας πολίτη εμφανίζεται σε σχέδιο νόμου – έστω και αν πρόκειται για πιλοτική εφαρμογή, η οποία θα απευθύνεται σε πολύ συγκεκριμένη κατηγορία προσώπων και για έναν ειδικό σκοπό. Αξίζει ωστόσο να αναφερθεί ότι, βάσει δημοσιευμάτων κατά τη χρονική περίοδο που γράφονται αυτές οι γραμμές, η εν λόγω διάταξη τελικά θα αποσυρθεί από το συγκεκριμένο σχέδιο νόμου. Μάλιστα, στην Ανοιχτή Διαβούλευση για το εν λόγω σχέδιο νόμου, το συγκεκριμένο άρθρο συγκέντρωσε τα περισσότερα σχόλια πολιτών, στην πλειοψηφία τους δε αρνητικά – γεγονός που καταδεικνύει επίσης το «σκεπτικισμό» που έχουν οι πολίτες για το εν λόγω ζήτημα (βλ. και Κεφάλαιο 8).

Κεφάλαιο 8

Ερωτηματολόγιο για την Ιδιωτικότητα και την τεχνολογία ABC

8.1. Εισαγωγή

Εισαγωγή

Σ' αυτό το κεφάλαιο θα προβούμε σε ανάλυση της έρευνας που κάναμε για την έννοια της ιδιωτικότητας στις υπηρεσίες Ηλεκτρονικής Διακυβέρνησης και για το αν οι πολίτες γνωρίζουν την τεχνολογία των Attribute - Based Credentials και κατά πόσο είναι έτοιμοι να την δεχτούνε στις καθημερινές τους συναλλαγές με υπηρεσίες του Δημόσιου Τομέα.

Σκοπός της έρευνας

Σκοπός του συγκεκριμένου ερωτηματολογίου είναι να μελετηθεί πιθανή ανησυχία των χρηστών των υπηρεσιών Ηλεκτρονικής Διακυβέρνησης σε σχέση με την προστασία της ιδιωτικότητάς τους και σε δεύτερη φάση κατά πόσο γνωρίζουν την ύπαρξη της τεχνολογίας των ABC και αν ναι, πόσο δεκτικοί είναι στην χρήση της στις υπηρεσίες ηλεκτρονικής διακυβέρνησης.

Διατύπωση ερευνητικών υποθέσεων

Υπόθεση0: Η χρήση υπηρεσιών Ηλεκτρονικής Διακυβέρνησης προκαλεί ανασφάλεια στους χρήστες για την προστασία της ιδιωτικότητάς τους

Υπόθεση1: Οι χρήστες υπηρεσιών Ηλεκτρονικής Διακυβέρνησης έχουν εμπιστοσύνη σε αυτές για την προστασία της ιδιωτικότητάς τους.

Είδος έρευνας

Η έρευνα που προσφέρει το συγκεκριμένο ερωτηματολόγιο είναι *ποσοτική*, μιας και αποσκοπεί στην ακριβή περιγραφή των μεγεθών - μεταβλητών και βασίζεται στην συλλογή των στοιχείων μέσω της συλλογής δομημένων ερωτηματολογίων.

Το χρονικό διάστημα που απαιτήθηκε για την συμπλήρωση του ερωτηματολογίου ήταν 24/02/2015 με 27/02/2015. Η μέθοδος που επιλέχτηκε για την συμπλήρωση του ερωτηματολογίου ήταν διαδικτυακά μέσω ηλεκτρονικού ταχυδρομείου (email). Αυτή η μέθοδος συμπλήρωσης ερωτηματολογίων προσφέρει το πλεονέκτημα της γρήγορης συλλογής, είναι ανέξοδη, ενώ όσον αφορά το μέγεθος του ερωτηματολογίου ήταν μέτριο, ώστε να μην προκαλέσει δυσφορία στη συμπλήρωσή του, ενώ οι ερωτήσεις ήταν σαφείς.

Δομή ερωτηματολογίου

Το ερωτηματολόγιο αποτελείται από 11 ερωτήσεις οι οποίες χρειάστηκαν περίπου τρία (3) λεπτά για την συμπλήρωσή τους.

Οι θεματικές ενότητες που περιλαμβάνει είναι οι εξής:

1. *Δημογραφικά στοιχεία*: οι δύο (2) πρώτες ερωτήσεις αφορούν καταγραφή δημογραφικών στοιχείων, το φύλο και το εύρος ηλικίας στο οποίο ανήκει ο ερωτώμενος.
2. *Ιδωτικότητα και Προσωπικά Δεδομένα στις υπηρεσίες Ηλεκτρονικής Διακυβέρνησης*: οι ερωτήσεις 3-7 αφορούν το μέγεθος ανησυχίας και ενδιαφέροντος των χρηστών για την προστασία της ιδιωτικότητάς τους και των προσωπικών τους δεδομένων κατά τις συναλλαγές τους με φορείς του Δημόσιου Τομέα.
3. *Γνώση τεχνολογίας ABC*: οι ερωτήσεις 8 έως 11 αφορούν την γνώση των ερωτώμενων της τεχνολογίας Attribute - Based Credentials και αν ενδιαφέρονται να ενσωματωθεί στις υπηρεσίες Ηλεκτρονικής Διακυβέρνησης.

Ορισμός Πληθυσμού και Μεγέθους Δείγματος

Ο πληθυσμός είναι το σύνολο των ερωτώμενων που συμμετείχαν στη συμπλήρωση του ερωτηματολογίου και αποτελείται από δεκαοκτώ (18) άτομα, τα οποία είναι εξοικειωμένα με τις διαδικτυακές εφαρμογές και την τεχνολογία γενικότερα. Οπότε και το δείγμα μας αποτελείται από αυτά τα δεκαοκτώ άτομα.

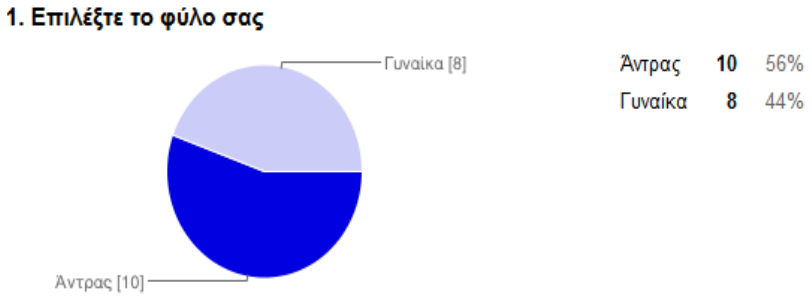
8.2. Παρουσίαση και Ανάλυση αποτελεσμάτων

Το ερωτηματολόγιο συντάχθηκε σε Google Form, η οποία και στάλθηκε στους ερωτώμενους, οπότε και η ανάλυση των ερωτηματολογίων πραγματοποιήθηκε από το έτοιμο εργαλείο που παρέχει η Google Form μέσω της "Σύνοψης Απαντήσεων" στο μενού "Απαντήσεις", ενώ τα γραφήματα είναι σε μορφή "πίτας".

8.2.1. Δημογραφικά στοιχεία

Φύλο

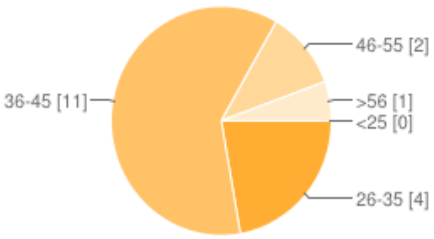
Η πρώτη ερώτηση εξετάζει το φύλο. Το ερωτηματολόγιο συμπληρώθηκε συνολικά από 18 άτομα, από τα οποία οι δέκα (10) ήταν άντρες (56%) και οι οκτώ (8) γυναίκες (44%).



Ηλικία

Η δεύτερη ερώτηση εξετάζει την ηλικία. Παρατηρούμε ότι στο δείγμα μας, η πλειοψηφία των ερωτώμενων (11) ανήκει στο ηλικιακό εύρος των 36-45 ετών με ποσοστό 61%.

2. Επιλέξτε την ηλικία σας



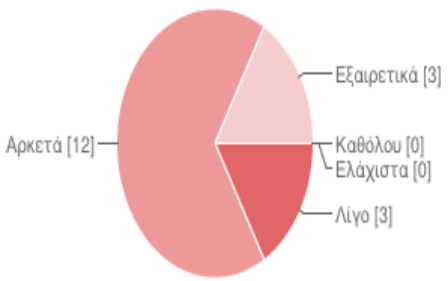
<25	0	0%
26-35	4	22%
36-45	11	61%
46-55	2	11%
>56	1	6%

8.2.2. Ιδωτικότητα και Προσωπικά Δεδομένα στις υπηρεσίες Ηλεκτρονικής Διακυβέρνησης

Αίσθηση ασφάλειας των προσωπικών δεδομένων

Στην τρίτη ερώτηση οι ερωτώμενοι έπρεπε να απαντήσουν αν αισθάνονται ασφαλείς όταν οι ιστότοποι που επισκέπτονται τούς ζητάνε προσωπικά δεδομένα. Έτσι, η πλειοψηφία (12) με ποσοστό 67% απάντησε θετικά, ενώ δεν υπήρξε καμία αρνητική απάντηση σε αυτήν την ερώτηση.

3. Πόσο ασφαλείς αισθάνεστε όταν επισκέπτεστε ιστοτόπους όπου ζητούνται προσωπικά δεδομένα;



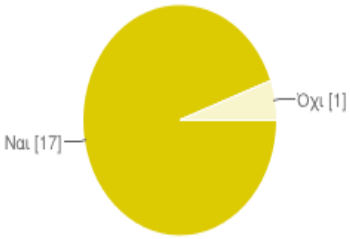
Καθόλου	0	0%
Ελάχιστα	0	0%
Λίγο	3	17%
Αρκετά	12	67%
Εξαιρετικά	3	17%

Χρήση υπηρεσιών Ηλεκτρονικής Διακυβέρνησης

Στην τέταρτη ερώτηση οι ερωτώμενοι απαντούν αν κάνουν χρήση υπηρεσιών ηλεκτρονικής διακυβέρνησης. Εφόσον οι πλειοψηφία των

ερωτώμενων (9/10) είναι εξοικειωμένοι ψηφιακά, ανάλογο ήταν και το ποσοστό τους (94%).

4. Κάνετε χρήση υπηρεσιών Ηλεκτρονικής Διακυβέρνησης;

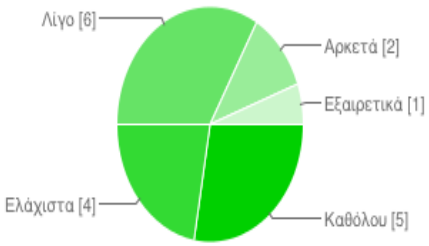


Ναι	17	94%
Όχι	1	6%

Ιδιωτικότητα και χρήση υπηρεσιών Ηλεκτρονικής Διακυβέρνησης

Οι απαντήσεις στην πέμπτη ερώτηση δείχνουν ότι οι ερωτώμενοι έχουν μικρή ανησυχία για την παραβίαση της ιδιωτικότητας και δείχνουν ότι είτε δεν τους απασχολεί, είτε θεωρούν ότι η χρήση υπηρεσιών του Δημόσιου Τομέα δεν αποτελεί απειλή για την ιδιωτικότητά τους. Έτσι, το 33% ανησυχεί λίγο, το 28% δεν ανησυχεί καθόλου, το 22% ανησυχεί ελάχιστα και μόλις το 17% έχει κάποιο βαθμό ανησυχίας για την ιδιωτικότητα των δεδομένων του.

5. Ανησυχείτε για την Ιδιωτικότητά σας όταν κάνετε χρήση υπηρεσιών Ηλεκτρονικής Διακυβέρνησης;



Καθόλου	5	28%
Ελάχιστα	4	22%
Λίγο	6	33%
Αρκετά	2	11%
Εξαιρετικά	1	6%

Στην συγκεκριμένη ερώτηση ανήκουν και οι δύο ερευνητικές υποθέσεις που διατυπώθηκαν στην παράγραφο 8.1. και θα τις ελέγξουμε χρησιμοποιώντας τον συντελεστή συσχέτισης x^2 *(chi-square)*.

Υπόθεση0: Η χρήση υπηρεσιών Ηλεκτρονικής Διακυβέρνησης προκαλεί ανασφάλεια στους χρήστες για την προστασία της ιδιωτικότητάς τους

Υπόθεση1: Οι χρήστες υπηρεσιών Ηλεκτρονικής Διακυβέρνησης έχουν εμπιστοσύνη σε αυτές για την προστασία της ιδιωτικότητάς τους.

Βαθμός εμπιστοσύνης σε σχέση με την ιδιωτικότητα στις e-government	**Γυναίκες - Παρατηρούμενη συχνότητα f_0**	**Άνδρες Παρατηρούμενη συχνότητα f_0**	**Σύνολο σειράς**
Καθόλου	0	5	5
Ελάχιστα	1	3	4
Λίγο	5	1	6
Αρκετά	1	1	2
Εξαιρετικά	1	0	1
Σύνολο στήλης	8	10	18

Οι βαθμοί ελευθερίας d_f υπολογίζονται από τον τύπο: $(r-1)(c-1)=4$

Ο τύπος της chi-square είναι: $x^2=sum(f_0-f_e)^2/f_e= 11,79$

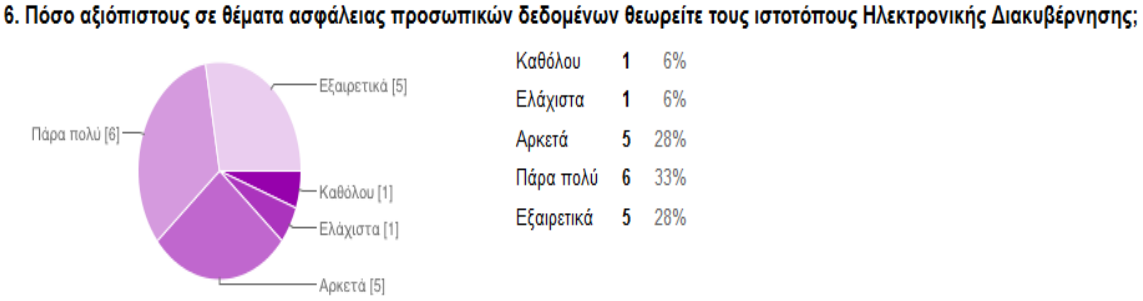
Για επίπεδο σημαντικότητας $\alpha=0,10$, $x^2=7,779<11,79$

Για επίπεδο σημαντικότητας $\alpha=0,05$, $x^2=9,488<11,79$

Άρα, παρατηρούμε ότι και με την χρήση του συντελεστή συσχέτισης chi-square, η συσχέτιση μεταξύ εμπιστοσύνης σε σχέση με την ιδιωτικότητα και υπηρεσιών ηλεκτρονικής διακυβέρνησης είναι θετικά ισχυρή και άρα απορρίπτουμε την Υπόθεση0.

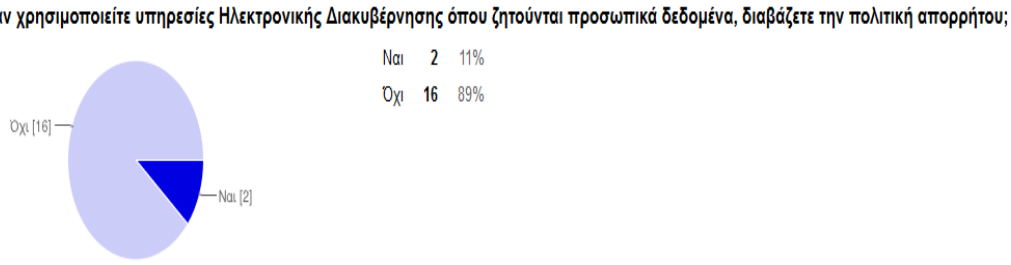
Αξιοπιστία ιστοτόπων Ηλεκτρονικής Διακυβέρνησης σε σχέση με την ασφάλεια των προσωπικών δεδομένων

Στην έκτη ερώτηση οι πλειοψηφία των ερωτώμενων θεωρεί αξιόπιστους τους ιστότοπους ηλεκτρονικής διακυβέρνησης σε ποσοστό συνολικά 89%.



Πολιτική απορρήτου (Privacy Policy)

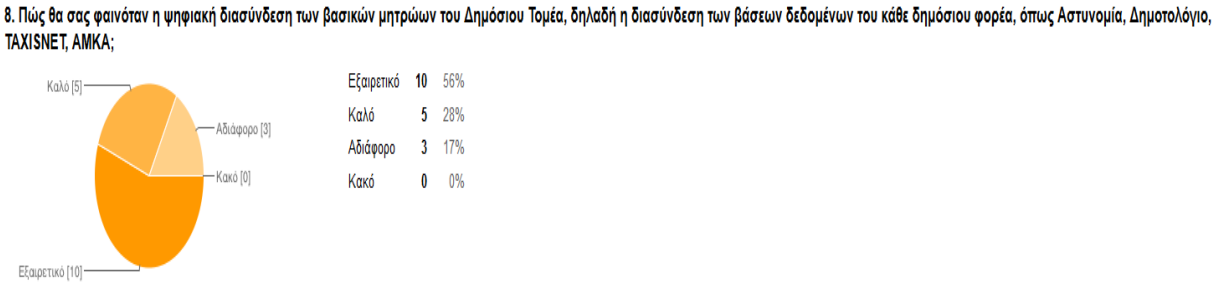
Σε σχέση με την πολιτική απορρήτου που υπάρχει συνήθως με μικρά γράμματα στους ιστοτόπους, στην έβδομη ερώτηση, η πλειοψηφία των ερωτώμενων απάντησε ότι δεν την διαβάζει σε ποσοστό 89%.



8.2.3. Γνώση τεχνολογίας ABC (Attribute - Based Credentials)

Διασύνδεση βάσεων δεδομένων του Δημόσιου Τομέα

Στην όγδοη ερώτηση, η πλειοψηφία των ερωτώμενων απάντησε θετικά με ποσοστό συνολικά 84% στην διασύνδεση των βάσεων δεδομένων δημόσιων φορέων, όπως της Αστυνομίας, των Δημοτολογίων, του TAXISNET και του ΑΜΚΑ.



Πιστοποιητικά που βασίζονται στα χαρακτηριστικά (ABC)

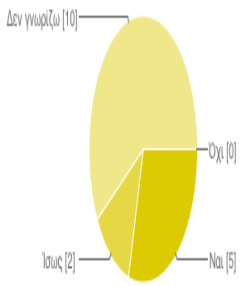
Στην ένατη ερώτηση, όπως ήταν αναμενόμενο, οι περισσότεροι ερωτώμενοι δεν γνώριζαν την τεχνολογία ABC σε ποσοστό 61%.

ABC και ιδιωτικότητα υπηρεσιών Ηλεκτρονικής Διακυβέρνησης

Η δέκατη ερώτηση ζητά την γνώμη των ερωτώμενων σε σχέση με το αν θεωρούν ότι η τεχνολογία ABC παρέχει ιδιωτικότητα στην χρήση των υπηρεσιών Ηλεκτρονικής Διακυβέρνησης. Η πλειοψηφία των ερωτώμενων

δεν το γνωρίζει, ακόμα και αν γνωρίζει για την τεχνολογία ABC, σε ποσοστό 56%.

10. Αν απαντήσατε θετικά στην προηγούμενη ερώτηση, θεωρείτε ότι η χρήση των Πιστοποιητικών είναι ασφαλής και παρέχει ιδιωτικότητα στην χρήση υπηρεσιών Ηλεκτρονικής Διακυβέρνησης;

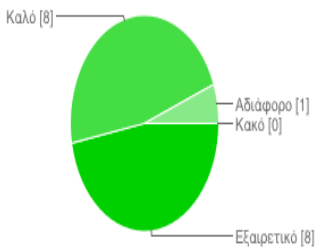


Ναι	5	27.8%
Ίσως	2	11.1%
Δεν γνωρίζω	10	55.6%
Όχι	0	0%

Χρήση όλων των υπηρεσιών Ηλεκτρονικής Διακυβέρνησης με ένα μόνο αναγνωριστικό

Στην τελευταία ενδέκατη ερώτηση, οι ερωτώμενοι πρέπει να δώσουν την γνώμη τους για την χρήση ενός και μόνο αναγνωριστικού για τις συναλλαγές τους με τις υπηρεσίες του Δημοσίου. Η πλειοψηφία, συνολικά το 88%, θεωρεί πολύ καλή την ιδέα αυτή.

11. Πώς θα σας φαινόταν η χρήση ενός και μόνο αναγνωριστικού (π.χ. ΑΜΚΑ) σε όλες τις συναλλαγές σας με τις υπηρεσίες του Δημοσίου;



Εξαιρετικό	8	44%
Καλό	8	44%
Αδιάφορο	1	6%
Κακό	0	0%

8.3. Συμπεράσματα έρευνας

Από τα αποτελέσματα της έρευνας συνάγεται ένα βασικό συμπέρασμα σε σχέση με το πώς οι πολίτες αντιλαμβάνονται την ιδιωτικότητα και την προστασία των προσωπικών τους δεδομένων όταν διενεργούν συναλλαγές με υπηρεσίες του Δημόσιου Τομέα. Αν και σχεδόν όλοι οι ερωτώμενοι έχουν μεγάλη εξοικείωση με τις ηλεκτρονικές συναλλαγές- αυτό φαίνεται και από τις απαντήσεις τους-, εντούτοις δεν προβληματίζονται σε μεγάλο βαθμό για την προστασία της ιδιωτικότητάς τους και των προσωπικών τους δεδομένων, ίσως επειδή θεωρούν δεδομένη την ασφάλεια και την ιδιωτικότητα των ηλεκτρονικών υπηρεσιών που παρέχουν οι δημόσιοι φορείς. Όσον αφορά την πολιτική απορρήτου, η πλειοψηφία των ερωτώμενων δεν την διαβάζει, γεγονός που μπορεί να οφείλεται στις ίδιες τις ηλεκτρονικές υπηρεσίες του Δημόσιου Τομέα που δεν εκφράζουν εμφανώς και κατανοητώς την πολιτική απορρήτου τους, αλλά και στους ίδιους τους χρήστες οι οποίοι μπορεί να μην έχουν επαρκείς γνώσεις για τους κινδύνους που κρύβονται.

Ένα δεύτερο συμπέρασμα της έρευνάς μας είναι ότι παρά το γεγονός ότι η πλειοψηφία των ερωτώμενων δεν γνωρίζει την τεχνολογία των Attribute - Based Credentials, εντούτοις καταλαβαίνει από το ύφος των σχετικών ερωτήσεων ότι η χρήση της συγκεκριμένης τεχνολογίας είναι προς όφελος των χρηστών των ηλεκτρονικών υπηρεσιών του Δημόσιου Τομέα και άρα απαντά θετικά. Άρα, παρατηρείται ότι το έδαφος είναι προσοδοφόρο για την ανάπτυξη και εξάπλωση της τεχνολογίας ABC, γεγονός που φαίνεται και από τις απαντήσεις στο ερωτηματολόγιο, οι οποίες είναι θετικές, και από το ευρωπαϊκό έργο ABC4Trust και από την χρήση της στην γερμανική κάρτα πολίτη. Δεν πρέπει, όμως, να παραλείψουμε την άγνοια των ερωτώμενων για την τεχνολογία ABC και την ευκολία με την οποία απάντησαν υπέρ της, πράγμα που μπορεί να συνέβη λόγω αυτής της άγνοιας. Όποτε, διατηρούμε επιφύλαξη για την δεκτικότητα των χρηστών σε σχέση με τα ABC πιστοποιητικά.

Συμπεραίνουμε, λοιπόν, ότι το να είσαι ψηφιακός χρήστης απαιτεί εκπαίδευση και ανάληψη ρίσκων, ενώ οι ηλεκτρονικές υπηρεσίες του Δημόσιου Τομέα οφείλουν να παρέχουν ασφάλεια και ιδιωτικότητα στους χρήστες τους, ώστε να κερδίσουν την εμπιστοσύνη τους, αλλά και να συμβαδίζουν με τις ραγδαίες τεχνολογικές εξελίξεις.

8.4. Το Ερωτηματολόγιο

Ιδιωτικότητα και Χρήση Attribute-Based Credentials

Ερωτηματολόγιο σε σχέση με την Ιδιωτικότητα και την χρήση των Attribute-Based Credentials (Πιστοποιητικά βάσει Χαρακτηριστικών) σε περιβάλλοντα Ηλεκτρονικής Διακυβέρνησης.
Τα στοιχεία είναι εμπιστευτικά και θα χρησιμοποιηθούν μόνο για τον σκοπό της έρευνας.

1. Επιλέξτε το φύλο σας

- Άντρας
- Γυναίκα

2. Επιλέξτε την ηλικία σας

- <25
- 26-35
- 36-45
- 46-55
- >56

3. Πόσο ασφαλείς αισθάνεστε όταν επισκέπτεστε ιστοτόπους όπου ζητούνται προσωπικά δεδομένα;

- Καθόλου
- Ελάχιστα
- Λίγο
- Αρκετά
- Εξαιρετικά

4. Κάνετε χρήση υπηρεσιών Ηλεκτρονικής Διακυβέρνησης;

- Ναι
- Όχι

5. Ανησυχείτε για την Ιδιωτικότητά σας όταν κάνετε χρήση υπηρεσιών Ηλεκτρονικής Διακυβέρνησης;

- Καθόλου
- Ελάχιστα
- Λίγο
- Αρκετά
- Εξαιρετικά

6. Πόσο αξιόπιστους σε θέματα ασφάλειας προσωπικών δεδομένων θεωρείτε τους ιστοτόπους Ηλεκτρονικής Διακυβέρνησης;

- Καθόλου
- Ελάχιστα
- Αρκετά
- Πάρα πολύ
- Εξαιρετικά

7. Όταν χρησιμοποιείτε υπηρεσίες Ηλεκτρονικής Διακυβέρνησης όπου ζητούνται προσωπικά δεδομένα, διαβάζετε την πολιτική απορρήτου;

- Ναι
- Όχι

8. Πώς θα σας φαινόταν η ψηφιακή διασύνδεση των βασικών μητρώων του Δημόσιου Τομέα, δηλαδή η διασύνδεση των βάσεων δεδομένων του κάθε δημόσιου φορέα, όπως Αστυνομία, Δημοτολόγιο, TAXISNET, ΑΜΚΑ;

- Εξαιρετικό
- Καλό
- Αδιάφορο
- Κακό

9. Γνωρίζετε τι είναι τα Πιστοποιητικά που βασίζονται στα Χαρακτηριστικά (ABC);

- Ναι
- Όχι

10. Αν απαντήσατε θετικά στην προηγούμενη ερώτηση, θεωρείτε ότι η χρήση των Πιστοποιητικών είναι ασφαλής και παρέχει ιδιωτικότητα στην χρήση υπηρεσιών Ηλεκτρονικής Διακυβέρνησης;

- Ναι
- Ίσως
- Δεν γνωρίζω
- Όχι

11. Πώς θα σας φαινόταν η χρήση ενός και μόνο αναγνωριστικού (π.χ. ΑΜΚΑ) σε όλες τις συναλλαγές σας με τις υπηρεσίες του Δημοσίου;

- Εξαιρετικό
- Καλό
- Αδιάφορο
- Κακό

Υποβολή

100%: Τα καταφέρατε.

Κεφάλαιο 9

Συμπεράσματα-Επίλογος

Στην παρούσα διατριβή μελετήθηκαν οι υπηρεσίες ηλεκτρονικής διακυβέρνησης από τη σκοπιά της ιδιωτικότητας. Έμφαση δόθηκε στις τεχνικές ηλεκτρονικής ταυτοποίησης και στις εφαρμογές τους, αναδεικνύοντας τα ζητήματα ασφάλειας και προστασίας προσωπικών δεδομένων που ανακύπτουν, καθώς και ποιες τεχνολογικές προσεγγίσεις υπάρχουν για την αντιμετώπισή τους. Πέρα από το γεγονός ότι οι ηλεκτρονικές συναλλαγές των πολιτών με τον Δημόσιο Τομέα δεν μπορούν να υφίστανται και να εξελιχθούν αν δεν ικανοποιείται το αίσθημα της ιδιωτικότητας του κάθε πολίτη, η ιδιωτικότητα και προστασία προσωπικών δεδομένων αποτελούν θεμελιώδη δικαιώματα των πολιτών και αντίστοιχες υποχρεώσεις της Πολιτείας, όπως αυτές ρυθμίζονται μέσα από ένα στέρεο και σαφές νομικό πλαίσιο.

Στο πλαίσιο της διατριβής αναπτύχθηκαν, αρχικά, τα ηλεκτρονικά διαβατήρια (e-passports) και οι τεχνολογίες που τα διέπουν. Πέραν των

τεχνολογικών προσεγγίσεων, έμφαση δόθηκε και σε αυτή καθ' αυτή τη χρήση των βιομετρικών τεχνολογιών που περιλαμβάνονται σε αυτά - όπως κατά τη λήψη δακτυλικών αποτυπωμάτων – οι οποίες εγείρουν ερωτήματα ως προς την ιδιωτικότητα. Προς επικύρωση αυτού, έγινε ειδική αναφορά σε πραγματικό σενάριο, όπου ο πολίτης και κάτοχος του διαβατηρίου δεν συμφώνησε στη λήψη των αποτυπωμάτων του, τα οποία θεωρούνται προσωπικά δεδομένα - βλέπε απόφαση ΔΕΕ Michael Schwarz κατά κρατιδίου Bochum (C-291/2012), η οποία παρουσιάστηκε στο κεφάλαιο 6.

Ένα αρκετά επίκαιρο θέμα για την Ελλάδα αποτελεί η ηλεκτρονική ταυτότητα, η οποία, ήδη, χρησιμοποιείται στις περισσότερες χώρες της Ευρωπαϊκής Ένωσης και σύμφωνα με δημοσιεύματα, θα υιοθετηθεί στους επόμενους μήνες και από την Ελλάδα. Όπως και με τα ηλεκτρονικά διαβατήρια, έτσι και με τις ηλεκτρονικές ταυτότητες, ερευνάται το νομικό πλαίσιο που θα τις διέπει με σκοπό την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων.

Στη συνέχεια παρουσιάστηκε η τεχνολογία των Πιστοποιητικών βάσει Χαρακτηριστικών (ABC), η οποία μπορεί να προσφέρει πολύ μεγάλη προστασία της ιδιωτικότητας και των προσωπικών δεδομένων στις ηλεκτρονικές ταυτότητες, και η οποία ακόμα δεν έχει υιοθετηθεί παρά μόνο από την Γερμανία. Η τεχνολογία αυτή δείχνει να είναι από τις πλέον φιλικές προς την ιδιωτικότητα. Υπάρχουν, όμως, κάποιοι προβληματισμοί και για αυτήν την τεχνολογία, όπως: [65]

Παρά τα πολλαπλά οφέλη στην προστασία της ιδιωτικότητας και των προσωπικών δεδομένων, η τεχνολογία ABC αποτελεί ένα αρκετά περίπλοκο κρυπτοσύστημα, το οποίο αντιμετωπίζει τεχνικά και όχι μόνο προβλήματα στην υλοποίησή του, τα οποία απαιτούν διερεύνηση και επίλυση ώστε η τεχνολογία αυτή να μπορέσει να εφαρμοστεί πιο μαζικά.

Ένας σοβαρός ανασταλτικός παράγοντας ενσωμάτωσης της τεχνολογίας αυτής στις ηλεκτρονικές ταυτότητες και στις έξυπνες κάρτες είναι η απουσία ενιαίου ευρωπαϊκού νομοθετικού πλαισίου σε σχέση με την υλοποίησή της και την προστασία της ιδιωτικότητας και των

προσωπικών δεδομένων. Μέχρι τώρα, όπως είδαμε και παραπάνω, μόνο η Γερμανία την έχει υιοθετήσει, όμως αναμένουμε τα επόμενα χρόνια να την ενσωματώσουν και άλλα κράτη-μέλη της Ε.Ε..

Ωστόσο, όταν ο Δημόσιος Τομέας αναπτύσσει πολιτικές προστασίας της Ιδιωτικότητας, θα πρέπει να λαμβάνονται υπόψη τα ιδιαίτερα πολιτισμικά και δημογραφικά χαρακτηριστικά του συνόλου των πολιτών από τους οποίους συλλέγονται οι προσωπικές πληροφορίες, επειδή η ιδιωτικότητα εξαρτάται σε μεγάλο βαθμό από αυτά τα χαρακτηριστικά του κάθε λαού.

Επιπλέον, ένας άλλος προβληματισμός που παρατηρείται στην υλοποίηση της τεχνολογίας ABC είναι η δυσκολία συνεργασίας της με ήδη υπάρχουσες τεχνολογίες αυθεντικοποίησης. Ένα τέτοιο παράδειγμα αποτελούν οι έξυπνες κάρτες (smart cards) και πάνω σε αυτόν τον προβληματισμό εργάζονται οι εμπλεκόμενοι στο έργο IRMA.

Ένας ακόμα προβληματισμός ο οποίος δεν έχει επιλυθεί ακόμα, είναι η δυνατότητα κατάργησης μη έγκυρων ή ληγμένων πιστοποιητικών χρηστών. Θα πρέπει να δίνεται η δυνατότητα σε μία αρχή κατάργησης να καταργεί ή να ανακαλεί πιστοποιητικά τα οποία έχουν κλαπεί ή χαθεί. Όταν ένα πιστοποιητικό ανακαλείται δεν θα μπορεί πλέον να χρησιμοποιηθεί για αυθεντικοποίηση, και θα πρέπει ο χρήστης να το γνωρίζει αυτό εξαρχής. Γι αυτό το λόγο, ο πάροχος υπηρεσιών θα πρέπει να ενημερώνει συχνά την λίστα κατάργησης/ ανάκλησης πιστοποιητικών που διαθέτει.

Όσον αφορά την υιοθέτησή της, δεν θα πρέπει να παραβλέψουμε ότι λόγω της πολυπλοκότητας της τεχνολογίας αυτής και της έλλειψης ευρωπαϊκού νομοθετικού πλαισίου, πολλές χώρες δυσκολεύονται να την ενσωματώσουν στην υπάρχουσα τεχνολογία τους.

Η έρευνα που πραγματοποιήθηκε μέσω συμπλήρωσης ερωτηματολογίων και η οποία παρουσιάζεται και αναλύεται στο όγδοο κεφάλαιο, ολοκλήρωσε αυτήν την πολύμηνη μελέτη, ενώ εστίασε στο κατά πόσο οι ψηφιακά εγγράμματοι πολίτες είναι δεκτικοί σε νέες τεχνολογίες,

οι οποίες διευκολύνουν την καθημερινότητά τους και τις συναλλαγές τους με τις Δημόσιες Υπηρεσίες.

Το συμπέρασμα που μπορούμε να βγάλουμε από αυτήν την μελέτη είναι ότι η ιδιωτικότητα θα συνεχίσει να αποτελεί σημαντικό θέμα για το μέλλον των ηλεκτρονικών συναλλαγών με τον Δημόσιο Τομέα, οπότε θα πρέπει να προστατευτεί, ώστε ο πολίτης να θέλει να πραγματοποιεί και να εμπιστεύεται τις ηλεκτρονικές συναλλαγές με τις Δημόσιες Υπηρεσίες. Απαιτείται κατάλληλη υποστήριξη -νομική και μη- προς τους πολίτες για να γίνουν πιο δεκτικοί απέναντι σε αυτές.

Βιβλιογραφία

[01] Σχέδιο δράσης i2010 για την ηλεκτρονική διακυβέρνηση, Ανακτήθηκε από http://europa.eu/legislation_summaries/information_society/strategies/l24226j_el.htm

[02] Torres L., Pina V., Royo S.(2005) E-Government and the transformation of public administrations in EU countries, Emerald, Vol.25, No5

[03] Molnár S., Η ηλεκτρονική διακυβέρνηση στην Ευρωπαϊκή Ένωση

[04] Daniel V., Huntgeburth J., (2014), Foundations of Digital Government,Springer Berlin Heidelberg, ISBN 978-3-642-38511-7

[05] Δρογκάρης Π., (2013),"Ασφάλεια και Προστασία της Ιδιωτικότητας σε Πληροφοριακά Συστήματα Ηλεκτρονικής Διακυβέρνησης, Πανεπιστήμιο Αιγαίου, Σάμος

[06] Η Διαλειτουργικότητα στο Δημόσιο Τομέα - Σημειώσεις Γεωργίας Προκοπιάδου, Ιόνιο Πανεπιστήμιο, Ανακτήθηκε από www.ionio.gr/~papatheodor/lessons/psi-nteroperability.ppt

[07] ISO/IEC 2382-1:1993, Information Technology Vocabulary Fundamental Terms, Ανακτήθηκε από www.iso.org/obp/ui/#iso:std:iso-iec:2382:-1:ed-3:v1:en

[08] Πλαίσιο Διαλειτουργικότητας & Υπηρεσιών Ηλεκτρονικών Συναλλαγών - Κοινωνία της Πληροφορίας Α.Ε., Ανακτήθηκε από www.e-gif.gov.gr/portal/pls/portal/docs/211041.pdf

[09] Παράρτημα ΙΙ: Κανόνες και πρότυπα για την διαλειτουργικότητα σε οργανωτικό, σημασιολογικό και τεχνολογικό επίπεδο, για την ανταλλαγή δεδομένων μεταξύ πληροφοριακών συστημάτων των φορέων του δημόσιου τομέα, Ανακτήθηκε από http://www.e-gif.gov.gr/portal/page/portal/egif/

[10] Ψηφιακό Θεματολόγιο: το σχέδιο δράσης για την ηλε-διακυβέρνηση θα διευκολύνει την πρόσβαση στις δημόσιες υπηρεσίες σε όλη την Ε.Ε., Ανακτήθηκε από

http://europa.eu/rapid/press-release_IP-10-1718_el.htm

[11] Τι είναι η ιδιωτικότητα , Ανακτήθηκε από http://antiauthor.wordpress.com/2011/08/06/τι-είναι-η-ιδιωτικότητα

[12] Warren S.D., Brandeis L.D. (1890), "The Right to Privacy (the omplicit made explicit)", Harvard Law Review, 4/1890, σελ. 193-220

[13] Perkins E., Markel M.(2004), "Multinational Data-Privacy Laws: An Introduction for IT Managers", IEEE Transactions on Professional Communication, Vol.47, No.2

[14] Public Administration and Information Technology, Christopher Reddick, Jones & Bartlett Learning, 2011, WEB-ISBN-13:978-1-4496-5264-7

[15] Μορφές ιδιωτικότητας, Ανακτήθηκε από http://antiauthor.wordpress.com/2011/08/17/μορφές-ιδιωτικότητας

[16] Pfitzmann A., Hansen M.,(2010) "A terminology for talking about Privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity and Identity Management", v0.34, 10 August 2010, Ανακτήθηκε από http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf

[17] Fischer-Hübner S., Duquenoy P., Zuccato A., Martucci L., (2008) "The Future of Identity in the Information Society", Springer

[18] Pollach I., (2007),"What's wrong with online privacy policies?", Communications of ACM, September/Vol.50, No.9

[19] Gemalto, (June 2014), Looking at the Future of Travel, The Fourth Generation of e-passport

[20] Implementation of Inspection System for Biometric Passports based on ICAO Specifications, Technical Report (2009), Ecole Polytechnique Federale de Lausanne

[21] Belguechi R., Lacharme P., Rosenberger C., (2012), "Enhancing the Privacy of electronic passports", International Journal of Information Technology and Management (IJITM) Special Issue on: Advances and Trends in Biometrics

[22] Diffie W., Hellman M., "New directions in cryptography". IEEE Transactions on Information Theory, vol. 22, n. 6, pp. 644–654, 1976.

[23] Hatzinakos D., σημειώσεις του "Multimedia Communication Laboratory", Electrical and Computer Engineering, University of Toronto, Canada

[24] Παναγοπούλου-Κουτνατζή Φ., ΔiΜΕΕ 4/2013, "Βιομετρικές μέθοδοι και προστασία ιδιωτικότητας: Σκέψεις με αφορμή την απόφαση ΔΕΕ Michael Schwarz κατά κρατιδίου Bochum (C-291/2012)"

[25] Ρεκλείτης Ε., Ριζομυλιώτης Π., Γκρίτζαλης Σ., RFID: "Απειλές κατά της Ιδιωτικότητας και Μέτρα Προστασίας", κεφάλαιο στο συλλογικό τόμο «Προστασία της Ιδιωτικότητας στις Τεχνολογίες της Πληροφορικής και των Επικοινωνιών: Τεχνικά και Νομικά Θέματα», Λαμπρινουδάκης Κ., Μήτρου Ε., Γκρίτζαλης Σ., Κάτσικας Σ.(Επιμέλεια Έκδοσης), σελίδες 193-220, Εκδόσεις Παπασωτηρίου, Αθήνα 2010

[26] ICAO, Public Key Directory, Ανακτήθηκε από http://www.icao.int/security/mrtd/pages/ICAOPKD.aspx,ICAO Public Key Directory(PKD)

[27] Abdalla M., An J.H., Bellare M., Namprempre M. (2002), "From Identifications to Signatures via the Fiat-Shamir Transform: Minimizing Assumptions for Security and Forward-Security"

[28] Bour I., (2013), "Electronic Identities in Europe Overview of eID solutions connecting citizens to public authorities"

[29] STORK 2.0 Project, Ανακτήθηκε από https://www.eid-stork.eu/

[30] Arora S., Ganley M. (2008), "National e-ID Card Schemes: An Overview"

[31] United Nations E-Government Survey 2014 E-Government for the Future We Want

[32] Bjones R., Krontiris I., Paillier P., Rannnberg K., (2012), "Integrating Anonymous Credentials with eIDs for Privacy-respecting Online Authentication"

[33] Η αυστριακή κάρτα πολίτη, Ανακτήθηκε από http://www.fidis.net/resources/fidis-deliverables/hightechid/int-d36000/doc/31/

[34] eID case study: Austria, Ανακτήθηκε από http://ec.europa.eu/idabc/en/document/4486/5584.html

[35] ENISA, (2011), Report, "Managing Multiple Identities"

[36] Vullers P., (2014), "Efficient Implementations of Attribute-based Credentials on Smart Cards", Radboud University

[37] Koning M., Korenhof P., Alpar G., Hoepman J.-H. (2014), "The ABC of ABC: An Analysis of Attribute-Based Credentials in the Light of Data, Protection, Privacy and Identity", 10th International Conference "Internet, Law and Politics: a Decade of Transformations", Barcelona

[38] Gergely Alpar (2015), "Attribute-Based Identity Management Bridging the Cryptographic Design of ABCs with the real world", Radboud University

[39] Badarinath Hampiholi B., University of Twente, Master Thesis "Secure & Privacy - preserving eID systems with Attribute-Based Credentials"

[40] Identity Mixer, Ανακτήθηκε από http://www.zurich.ibm.com/idemix/whatitdoes.html

[41] U-Prove, Ανακτήθηκε από http://research.microsoft.com/en-us/projects/u-prove/

[42] About ABC4Trust, Ανακτήθηκε από https://abc4trust.eu/index.php/home/fact-sheet

[43] ABC4Trust, Pilots, Ανακτήθηκε από https://abc4trust.eu/index.php/home/pilots

[44] Deibler D., Engeler M., Krontiris I., Lehmann A., Liagkou V., Pyrgelis A., Schlehahn E., Stamatiou Y., Tesfay W., Zwingelberg H., D7.3 Evaluation of the Student Pilot, Deliverable, ABC4Trust (2014)

[45] Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, Ανακτήθηκε από [eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:31995L0046&from=en]

[46] Νόμος 2472/1997 "Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα με ενσωματωμένες τις τροποποιήσεις", Ανακτήθηκε από http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/NOMOTHESIA%20PROSOPIKA%20DEDOMENA/FILES/2472_97_JUNE2013.PDF

[47] Νόμος 138(I)/2001 "Περί επεξεργασίας δεδομένων προσωπικού χαρακτήρα (προστασία του ατόμου) της Κυπριακής Δημοκρατίας, Ανακτήθηκε από http://www.cylaw.org/nomoi/arith/2001_1_138.pdf

[48] Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, Ανακτήθηκε από http://www.digitalplan.gov.gr/resource-api/dipla/contentObject/Prostasia-Dedomenwn-COM-2012-11_el/content

[49] Αρχή Προστασίας Προσωπικών Δεδομένων, (2015) "Η σημασία της Εκτίμησης Επιπτώσεων στην Προστασία Προσωπικών Δεδομένων", Κ. Λιμνιώτης, Λ. Ρούσσος, Ανακτήθηκε από http://www.dpa.gr/portal/page?_pageid=33,227076&_dad=portal&_schema=PORTAL,

[50] Φραγκάκης, Ν., Δικηγόρος, (2/2008), "Τα όρια μεταξύ ελευθερίας και ασφάλειας, δημόσιου και ιδιωτικού",

Ανακτήθηκε από http://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=102,62,61,136,94,229,146,4

[51] Σύνοψη της νομοθεσίας της, Ανακτήθηκε από E.E.,http://europa.eu/legislation_summaries/information_society/legislative_framework/l24120_el.htm

[52] Αρχή Προστασίας Προσωπικών Δεδομένων, Ανακτήθηκε από http://www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL,

[53] Αρχή Προστασίας Προσωπικών Δεδομένων, Ανακτήθηκε από http://www.dpa.gr/portal/page?_pageid=33,123437&_dad=portal&_schema=PORTAL,

[54] Αρχή Προστασίας Προσωπικών Δεδομένων, Ανακτήθηκε από http://www.dpa.gr/,

[55] Security of eGovernment Systems - Final Report, (2013), ISBN:978-92-823-4618-1, Ανακτήθηκε από bookshop.europa.eu/el/security-of-egovernment-systems-pbBA0113378/

[56] Cavoukian A.,(2009), "Privacy by Design: Οι επτά θεμελιώδεις Αρχές", Ανακτήθηκε από www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-gree.pdf

[57] Μήτρου Λ.,(2013) "Privacy by Design: Η τεχνολογική διάσταση της προστασίας προσωπικών δεδομένων", Δίκαιο Μέσων Ενημέρωσης & Επικοινωνίας, Τεύχος 1/2013

[58] The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age, Viviane Reding, Munich, 2012, Ανακτήθηκε από europa.eu/rapid/press-release_SPEECH-12-26_el.htm

[59] Study on the economic benefits of privacy-enhancing technologies (PETs), Final Report, The European Commission DG Justice, Freedom and Security London Economics, 2010, Ανακτήθηκε από ec.europa.eu/justice/policies/privacy/docs/studies/final_repo

rt_pets16_07_10_en.pdf

[60] Future of Identity in the Information Society, Ανακτήθηκε από http://www.fidis.net/home/

[61] Κανονισμός (ΕΚ) αριθμ. 2252/2004 του συμβουλίου της 13ης Δεκεμβρίου 2004 σχετικά με την καθιέρωση προτύπων για τα χαρακτηριστικά ασφάλειας και τη χρήση βιομετρικών στοιχείων στα διαβατήρια και τα ταξιδιωτικά έγγραφα των κρατών μελών, Ανακτήθηκε από http://www.scribd.com/doc/97104345/%CE%9D%CE%95%CE%95%CE%A3-%CE%A4%CE%91%CE%A5%CE%A4%CE%9F%CE%A4%CE%97%CE%A4%CE%95%CE%A3-%CE%94%CE%99%CE%91%CE%92%CE%91%CE%A4%CE%97%CE%A1%CE%99%CE%91-%CE%9A%CE%91%CE%9D%CE%9F%CE%9D%CE%99%CE%A3%CE%9C%CE%9F%CE%A3-%CE%95%CE%9A-2252-2004#scribd

[62] Ελληνικό Διαβατήριο, Ανακτήθηκε από http://en.wikipedia.org/wiki/Greek_passport

[63] Ευρωπαϊκή Επιτροπή, "Χρηματοδότηση ύψους 13,7 εκατ. ευρώ για διασυνοριακές ψηφιακές υπηρεσίες ανακοίνωσε η Ευρωπαϊκή Επιτροπή", 14 Αυγούστου 2013, Ανακτήθηκε από http://europa.eu/rapid/press-release_IP-13-778_el.htm

[64] Τι είναι η κάρτα πολίτη, Ανακτήθηκε από http://el.wikipedia.org/wiki/Κάρτα_πολίτη

[65] Hazny J., Malina L., Martinasek Z., Tethal O., "Performance Evaluation of Primitives for Privacy-Enhancing Cryptography on Current Smart-cards and Smart-phones", Brno University of Technology