ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Μελέτη Ασφαλούς Εφαρμογής της Κάρτας Πολίτη στην Ελλάδα

18 Οκτωβρίου 2011

Αυτή η σελίδα έχει αφεθεί σκοπίμως κενή.

Η Μεταπτυχιακή Διπλωματική Εργασία παρουσιάστηκε ενώπιον του Διδακτικού Προσωπικού του Πανεπιστημίου Πειραιά

Σε Μερική Εκπλήρωση των Απαιτήσεων για το Δίπλωμα του Μεταπτυχιακού Προγράμματος Σπουδών

«Διδακτική της Τεχνολογίας και Ψηφιακών Συστημάτων»

Κατεύθυνση Δικτυοκεντρικών Συστημάτων

της

ΓΕΩΡΓΙΑΣ Ν. ΤΕΡΖΗ

2011

Η ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ ΔΙΔΑΣΚΟΝΤΩΝ ΕΓΚΡΙΝΕΙ

ΤΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΤΗΣ ΓΕΩΡΓΙΑΣ Ν. ΤΕΡΖΗ

ΚΩΝΣΤΑΝΤΙΝΟΣ ΛΑΜΠΡΙΝΟΥΔΑΚΗΣ, Επιβλέπων,
Επίκουρος Καθηγητής,

Τμήμα Ψηφιακών Συστημάτων

ΣΩΚΡΑΤΗΣ ΚΑΤΣΙΚΑΣ, Καθηγητής,

Τμήμα Ψηφιακών Συστημάτων

ΜΑΡΙΝΟΣ ΘΕΜΙΣΤΟΚΛΕΟΥΣ, Καθηγητής,

Τμήμα Ψηφιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

2011

Αυτή η σελίδα έχει αφεθεί σκοπίμως κενή.

ΠΕΡΙΛΗΨΗ

Μελέτη Ασφαλούς Εφαρμογής της Κάρτας Πολίτη στην Ελλάδα

Στο σύγχρονο περιβάλλον, όπως διαμορφώνεται από τις συνθήκες της παγκοσμιοποίησης και την ψηφιακή εποχή η ανάγκη για ασφαλείς και αξιόπιστες μεθόδους ταυτοποίησης και αυθεντικοποίησης των πολιτών εντός και εκτός συνόρων αποκτά νέα διάσταση. Η Ηλεκτρονική Διακυβέρνηση δεν αποτελεί μόνο επιλογή και ανάγκη, αλλά και μια πραγματικότητα. Η Κάρτα Πολίτη (ΚΠ) αποτελεί τη σύγχρονη μέθοδο για τον τρόπο προσδιορισμού του κατόχου (ταυτοποίηση) και την επιβεβαίωση ότι ο ισχυρισμός του κατόχου είναι πράγματι αληθής (αυθεντικοποίηση). Η ενσωμάτωση της τεχνολογίας των έξυπνων καρτών αποτελεί την ιδανική επιλογή για την ΚΠ, καθώς μέσω του μικροεπεξεργαστή που περιέχει, παρέχει σημαντικές δυνατότητες ευελιξίας και ασφάλειας. Σημαντικός είναι ο ρόλος των προτύπων και των προδιαγραφών προκειμένου να διασφαλίζεται το ελάχιστο απαιτούμενο επίπεδο ασφάλειας και διαλειτουργικότητας στις εφαρμογές ΚΠ. Η Ευρωπαϊκή ΚΠ (ECC) είναι μια σημαντική προσπάθεια για τη δημιουργία ενός ενιαίου πλαισίου συμμόρφωσης στις απαιτήσεις ασφάλειας και παροχής διασυνοριακών υπηρεσιών στους Ευρωπαίους πολίτες, εξασφαλίζοντας παράλληλα σχετική ευελιξία επιλογών στα κράτη μέλη.

Όπως έχει ήδη αναδειχθεί από προηγούμενες μελέτες και στην παρούσα κατέστη σαφές ότι τα ζητήματα ασφάλειας και ιδιωτικότητας είναι τα πιο κρίσιμα για την επιτυχή εφαρμογή μιας Εθνικής λύσης ΚΠ. Επομένως, είναι απαραίτητη η προσοχή μας στην επιλογή των μηχανισμών ασφαλείας και τεχνικών ιδιωτικότητας που θα ανταποκρίνονται με τον πιο αποδοτικό τρόπο στις απαιτήσεις ασφάλειας και στις απειλές που έχουμε αναγνωρίσει. Παράλληλα όμως, είναι απολύτως κρίσιμη η εναρμόνιση της τεχνικής λύσης με το ισχύον εθνικό και κοινοτικό θεσμικό πλαίσιο, καθώς η εφαρμογή της όποιας τεχνικής επιλογής εντάσσεται σε ένα θεσμικό και επιχειρησιακό περιβάλλον, στις ανάγκες του οποίου πρέπει να ανταποκρίνεται. Ωστόσο, οι απειλές για την ΚΠ εξελίσσονται παράλληλα με την εξέλιξη της τεχνολογίας των ΚΠ και των τεχνικών ασφάλειας και ιδιωτικότητας, γεγονός που τις κάνει πάντα ανταγωνιστικές απέναντι στην ασφαλή εφαρμογή της ΚΠ. Συνεπώς, ιδανική λύση αποτελεί μια διαρκή ισορροπία ανάμεσα στις απειλές που πρέπει να αντιμετωπισθούν και εκείνες που είτε είναι λιγότερο πιθανές, είτε λιγότερα κρίσιμες, έπειτα από την αξιολόγηση της βαρύτητάς του.

Αν και τα θέματα ασφάλειας και διαλειτουργικότητας είναι σε μεγάλο βαθμό ανοιχτά, η μελέτη της Ευρωπαϊκής και διεθνούς εμπειρίες αποτελεί πολύ σημαντικό εργαλείο για την αποφυγή πιθανών κινδύνων και την αντιμετώπιση προβλημάτων. Ενώ, πολύ σημαντική εργασία γίνεται ήδη σε ευρωπαϊκό επίπεδο για την εξασφάλιση της ιδιωτικότητας και διαλειτουργικότητας μεταξύ των επιμέρους συστημάτων ΚΠ σε εθνικό και ευρωπαϊκό επίπεδο, έχοντας να επιδείξει σύγχρονες και καινοτόμες λύσεις για τη βέλτιστη εφαρμογή ΚΠ.

Σε αυτό το πλαίσιο, προτείνεται η βέλτιστη, κατά την άποψή μας σχεδιαστική επιλογή για την εφαρμογή της ΚΠ στην Ελλάδα λαμβάνοντας υπόψη της λειτουργικές, επιχειρησιακές, τεχνικές απαιτήσεις και απαιτήσεις ασφάλειας, αλλά και τις ιδιαιτερότητες της Ελληνικής περίπτωσης και την εναρμόνιση της λύσης με την Εθνική κουλτούρα των Ελλήνων Πολιτών. Είναι απόλυτη η πεποίθησή μας, ότι προκειμένου για την επιτυχία του εγχειρήματος πρέπει να αναδειχθούν οι ανάγκες της Ελληνικής κοινωνίας με τις οποίες να εναρμονίζεται η σχεδιαστική λύση.

Ο ορισμός, με σαφήνεια και πληρότητα, των κανόνων που επιθυμούμε να διέπουν τη λειτουργία και διαχείριση της ΚΠ, μπορούν να συμβάλλουν σημαντικά στη δημιουργία ενός ασφαλούς και προστατευμένου περιβάλλοντος εφαρμογής της Ελληνικής ΚΠ. Σε κάθε περίπτωση, πάντως, η σχεδιαστική επιλογή της ΚΠ για την Ελλάδα πρέπει να ανταποκρίνεται στην ανάγκη στάθμισης του δημόσιου και ιδιωτικού συμφέροντος, δημιουργώντας προϋποθέσεις για ασφαλείς συναλλαγές του πολίτη μέσω της χρήσης της ΚΠ και της ταυτόχρονης προστασίας των προσωπικών ή μη δεδομένων του από τη μη εξουσιοδοτημένη χρήση και πρόσβαση. Η εμπιστοσύνη του πολίτη στην ΚΠ και τις εφαρμογές αυτής είναι καταλυτική τόσο ως προϋπόθεση για την υιοθέτησή της, όσο και υπό το πρίσμα της περαιτέρω ανάπτυξή της.

ABSTRACT

Security Assessment of the Greek Electronic Citizen Card

In today's environment, as it is shaped by the conditions of globalization and the digital age, there is a new need for safe and reliable methods for identification and authentication of citizens within and across national borders. E-Governance is not only a choice and necessity, but also a reality. The Citizen Card (CC) is the modern method of identifying the owner (identification) and to confirming that the card holder's identity is indeed true (authentication). Integrating smart cards' technology is the perfect choice for the CC, because through the containing chip they provide significant flexibility and security. The role of standards and specifications is very important for ensuring that the minimum required level of security and interoperability in CC applications will be met. The European CC (ECC) is a major attempt of creating a single set of compliance requirements for security and border services to European citizens, while simultaneously providing some flexibility options to Member States.

As previous studies have already demonstrated, this study will also confirm that issues of security and privacy are the most critical for the successful implementation of a national CC solution. It is therefore essential that our attention during the selection of security mechanisms and privacy techniques must respond in the most efficient way to safety requirements and threats that have been recognized as important. At the same time, it is absolutely critical to harmonize the technical solution with the current national and EU institutional framework, having in mind that the appliance of any technical choice will be part of an institutional and operational environment, with which it needs to be compliant. However, threats to the CC evolve as CC security and privacy technologies evolve, making them always competing regarding the safe implementation of CC's. Therefore, the best solution is a constant balance between the threats to be addressed and those that are either less likely or less critical, after assessing their importance.

Although security and interoperability issues are widely open, the study of European and international experience is a very important tool in order to troubleshoot and address potential risks. At the same time, significant work is already been done at a European level in order to ensure that privacy and interoperability between individual CC systems is met at national and European level, boasting modern and innovative solutions for the optimal implementation of CC's.

In this context, we propose the best –as seen from our view- design solution for the implementation of the CC in Greece, taking into account the functional, operational, technical and safety requirements, but also the particularities of the Greek case and the harmonization of the solution with the National culture of Greek society. It is our belief that

in order for the project to be successful we should identify the needs of the Greek society with which to line the design solution.

The clear and specific definition of the rules we want to govern the operation and management of the CC, can contribute significantly into creating a safe and secure environment for the Greek CC. In any event, the design choice for the CC in Greece should address the need to balance between the public and private interests, by creating conditions for safe trade for citizens through the use of CC and simultaneous protect personal or general data from unauthorized use and access. The citizen's trust in the CC and its applications is a catalyst both as a precondition for its adoption, as well as its further development.

ΕΥΧΑΡΙΣΤΙΕΣ

«Να αγαπάς την ευθύνη. Να λες: Εγώ μονάχος μου έχω χρέος να σώσω τη γης.
Άμα δε σωθεί εγώ θα φταίω.»,

Ασκητική, Νίκος Καζαντζάκης

Ειλικρινείς ευχαριστίες οφείλω στον επιβλέποντα της διπλωματικής μου, Κώστα Λαμπρινουδάκη, Επίκουρο Καθηγητή του Τμήματος Ψηφιακών Συστημάτων, για τη βοήθεια, την υπομονή και τη στήριξη που μου παρείχε καθ' όλη τη διάρκεια εκπόνησης της παρούσας διπλωματικής εργασίας, αλλά και για τη γνώση που έχει μοιραστεί μαζί μου καθ' όλη τη διάρκεια των σπουδών μου.

Ιδιαίτερες ευχαριστίες οφείλω στους δύο σημαντικούς μου Δασκάλους, Καθ. Σωκράτη Κάτσικα και Καθ. Στέφανο Γκρίτζαλη, για την αγάπη και την εμπιστοσύνη που μου δείχνουν, όλα αυτά τα χρόνια και για τη δύναμη που δίνουν για να προχωρήσω στα επόμενά μου βήματα, ελπίζοντας να μην διαψεύσω τις προσδοκίες τους.

Επίσης, ευχαριστώ πολύ τους δύο πολύτιμους συνεργάτες και φίλους μου πια, τον Δρ. Πέτρο Λάλο για την τεράστια υπομονή, τη διαρκή του παρουσία και την υποστήριξη της προσπάθειάς μου, με χρήσιμες συμβουλές και διορθώσεις, καθώς και το Δρ. Βασίλη Τσούμα για τις σημαντικές του παρεμβάσεις, αλλά και για τα μαθήματα που μου δίνει.

Ευχαριστώ ακόμη τις φίλες μου και τους συνεργάτες μου για την υπομονή τους όλο αυτό το διάστημα.

Για το τέλος, φυλάω την αγάπη και ένα μεγάλο ευχαριστώ για την οικογένειά μου, στην οποία οφείλω ό,τι είμαι μέχρι σήμερα, και η οποία είναι πάντα δίπλα μου, με τη στήριξη των επιλογών μου και την απόλυτη εμπιστοσύνη, σε καθετί που κάνω. Στον πατέρα μου, Νίκο, που πάντα προσπαθώ να κάνω περήφανο, στη μητέρα μου, Βάσω, που μου δίνει τόσο απλόχερα την αγάπη της και στον αγαπημένο μου αδελφό, Γιάννη-Κωστή που είμαι σίγουρη ότι σύντομα θα με κάνει πολύ υπερήφανη.

Τίποτα δεν είναι δεδομένο. Μα πρέπει να μπορείς να πεις:
Ακόμη κι αν ξεκινήσω από την αρχή, πάλι θα τα καταφέρω.

Γιούλη Τερζή,

Οκτώβριος 2011

Αυτή η σελίδα έχει αφεθεί σκοπίμως κενή.

ΠΕΡΙΕΧΟΜΕΝΑ

Πίνακας περιεχομένων

ΕΥΡΕΤΗΡΙΟ ΕΙΚΟΝΩΝ ΚΑΙ ΣΧΗΜΑΤΩΝ

ΕΥΡΕΤΗΡΙΟ ΠΙΝΑΚΩΝ

Αυτή η σελίδα έχει αφεθεί σκοπίμως κενή

1. ΕΙΣΑΓΩΓΗ

1.1. Ταυτοποίηση και Αυθεντικοποίηση

Αναγκαία συνθήκη για την ομαλή λειτουργία μιας οργανωμένης κοινωνίας αποτέλεσε από πολύ παλιά η ταυτοποίηση των πολιτών με τρόπο τέτοιο ώστε να γίνεται καλύτερος επιμερισμός των δραστηριοτήτων, να επιτυγχάνεται η καλύτερη οργάνωση του κοινωνικού συνόλου και να παρέχεται η δυνατότητα αλληλεπίδρασης με τις δημόσιες αρχές, ακόμα κι αν αυτές ήταν σε πρώιμο στάδιο.

Προσωπική ταυτότητα και προσωπική ταυτοποίηση διαφέρουν εννοιολογικά, καθώς η προσωπική ταυτοποίηση αφορά στη μεθοδολογία ακριβούς προσδιορισμού των στοιχείων της ατομικότητας που συναποτελούν την προσωπική ταυτότητα του ατόμου (το αντικείμενο προσδιορισμού της ταυτότητας του ατόμου).

Συναφής, είναι και η έννοια της αυθεντικοποίησης, η οποία αφορά στη διαδικασία αναγνώρισης και επιβεβαίωσης της ορθότητας της ταυτότητας του πολίτη ή κάποιων χαρακτηριστικών της. Η επαλήθευση αυτή βασίζεται στα διαπιστευτήρια, δηλαδή στα αναγνωριστικά, που το πρόσωπο έχει στην κατοχή του.

Η ανάγκη έγκυρης ταυτοποίησης ενός προσώπου γίνεται ακόμη πιο επιτακτική στην εποχή της παγκοσμιοποίησης, αλλά πολύ δε περισσότερο στη νέα Ψηφιακή Εποχή. Σήμερα περισσότερο από ποτέ, η αναγνώριση του ατόμου γίνεται δυσκολότερη αλλά και πιο αναγκαία. Όταν επιπλέον στον ψηφιακό κόσμο ο χρήστης-πολίτης ταυτοποιείται και αυθεντικοποιείται καθημερινά, το ζήτημα της διαχείρισης της ηλεκτρονικής ταυτοποίησης είναι πια επιβεβλημένο.

Η ταυτοποίηση στον ψηφιακό κόσμο δεν διαφέρει ιδιαίτερα από την ταυτοποίηση στο φυσικό κόσμο. Ωστόσο, είναι σίγουρα περισσότερο πολύπλοκη διαδικασία, κυρίως καθώς δεν μπορεί να συνοδευτεί από τη φυσική παρουσία του προσώπου, αλλά καθώς και ο τρόπος διαχείρισης της έννοιας της ταυτοποίησης από τους πολίτες/χρήστες για τις ανάγκες του ψηφιακού περιβάλλοντος είναι διαφορετικός. Έτσι, κατ' αναλογία με την ταυτοποίηση στο φυσικό κόσμο και στο ψηφιακό περιβάλλον απαιτείται αρχικά

- 1ο επίπεδο: σύνδεση (κατ' αναλογία με τη φυσική παρουσία)
- 2ο επίπεδο: αυθεντικοποίηση, χρήση υπηρεσιών, είσοδος στον ψηφιακό κόσμο και σε κάποιες περιπτώσεις μη αποποίηση

Τα σύγχρονα ερωτήματα ταυτοποίησης ακολουθούν κατ' αναλογία με την ταυτοποίηση στον φυσικό κόσμο την εξής λογικής ακολουθία.

1. Ποιος είσαι;

2. Πως αποδεικνύεται;
3. Είσαι πράγματι αυτός που ισχυρίζεσαι;

Στο τελευταίο ερώτημα η απάντηση εφόσον δεν συνοδεύεται με την φυσική παρουσία γίνεται, όπως είναι αντιληπτό, δυσκολότερη. Οδηγούμαστε λοιπόν άμεσα στο ερώτημα αν η ταυτοποίηση στον ηλεκτρονικό κόσμο είναι πραγματικά εφικτή.

Μπορεί άραγε να δοθεί ασφαλής , αξιόπιστη και πειστική απάντηση σε αυτά τα ερωτήματα χωρίς την ύπαρξη της ηλεκτρονικής υπογραφής; Έτσι το θέμα της ηλεκτρονικής ταυτοποίησης είναι άρρηκτα συνδεδεμένο με τις ηλεκτρονικές υπογραφές. [1]

Ηλεκτρονική Ταυτότητα: «οποιοδήποτε μέσο ή μέθοδος που χρησιμοποιεί ο χρήστης των υπηρεσιών ηλεκτρονικής διακυβέρνησης για τη δήλωση και αναγνώριση της ταυτότητάς του σχετικά με την πρόσβαση σε μια ηλεκτρονική υπηρεσία.» [33]

1.2. Ηλεκτρονική Ταυτοποίηση

Είναι όμως άραγε τόσο σημαντική η «ηλεκτρονική ταυτοποίηση»;

Στην περίπτωση της ηλεκτρονικής ταυτότητας του πολίτη, η έννοια της προσωπικής ταυτοποίησης παίρνει λίγο διαφορετική διάσταση και αφορά στη μεθοδολογία αυτή αφορά την συσχέτιση δεδομένων με ένα ορισμένο πρόσωπο. Έτσι, η ταυτοποίηση του κατόχου ηλεκτρονικής ταυτότητας του πολίτη απαντά στο ερώτημα «ποιος είναι ο κάτοχος» ενώ η αυθεντικοποίηση απαντά στο «αν ο κάτοχος της ταυτότητας είναι πράγματι αυτός που ισχυρίζεται ότι είναι».

Είναι σαφές ότι το κυριότερο εμπόδιο για την περαιτέρω ανάπτυξη του ηλεκτρονικού εμπορίου, των ηλεκτρονικών συναλλαγών και των υπηρεσιών ηλεκτρονικής διακυβέρνησης είναι η έλλειψη εμπιστοσύνης των πολιτών, του κράτους και των επιχειρήσεων σχετικά με το πόσο ασφαλείς είναι τέτοιου είδους συναλλαγές. [3]

Σήμερα περισσότερο από ποτέ, σε έναν ψηφιακό κόσμο που δε γνωρίζει σύνορα είναι επιτακτική η ανάγκη για διεθνή ταυτοποίηση. Οι δυσκολίες στην επαλήθευση ταυτότητας και υπογραφής σε συνδυασμό με το χαμηλό επίπεδο εμπιστοσύνης των πολιτών και των επιχειρήσεων κατά τις συναλλαγές τους σε απευθείας ηλεκτρονική σύνδεση συνιστούν ανασταλτικό παράγοντα για την ανάπτυξη της διαδικτυακής οικονομίας, σύμφωνα με τις περισσότερες μελέτες [3][4]. Η παροχή ασφαλών, αξιόπιστων και εύχρηστων διαδικτυακών υπηρεσιών είναι ζωτικής σημασίας για μια ισχυρή και υγιή ενιαία ευρωπαϊκή ψηφιακή αγορά. Για τη συμμετοχή σε μια ηλεκτρονική συναλλαγή απαιτείται ένας μηχανισμός που θα εγγυάται την ταυτοποίηση των δύο μερών της συναλλαγής, την πραγματοποίηση της επιθυμητής και από τα δύο μέρη συναλλαγής, καθώς και τη μη αποποίηση της συναλλαγής. Ωστόσο, μέχρι σήμερα, όσο έντονες και σημαντικές κι αν είναι οι προσπάθειες για τη δημιουργία ασφαλών και αξιόπιστων μηχανισμών ταυτοποίησης, αυθεντικοποίησης και μη αποποίησης, τόσο η εμπιστοσύνη στις ηλεκτρονικές συναλλαγές, όσο και η αναγνώριση της

ανάγκης ηλεκτρονικής ταυτοποίησης που μπορεί να εγγυηθεί τη συναλλαγή και να εδραιώσει την εμπιστοσύνη δεν είναι αυτονόητα ζητήματα.

Η Ευρωπαϊκή Επιτροπή, μάλιστα, θέτει ψηλά στην ατζέντα το θέμα των ηλεκτρονικών υπογραφών, της ηλεκτρονικής ταυτοποίησης και επαλήθευσης της ταυτότητας με στόχο την ανάπτυξη της ενιαίας ευρωπαϊκής ψηφιακής αγοράς, αλλά και το θέμα της ασφάλειας [46]. Επιπλέον, πρόσφατα, στο Ψηφιακό Θεματολόγιο 2020 για την Ευρώπη ανακοινώθηκε ανασκόπηση της οδηγίας για τις ηλεκτρονικές υπογραφές [41], καθώς και σχετική πρωτοβουλία για την αμοιβαία αναγνώριση της ηλεκτρονικής ταυτοποίησης και της ηλεκτρονικής επαλήθευσης ταυτότητας [2].

Και αυτό γιατί πρέπει να απαντήσουμε ουσιαστικά σε ένα πρόβλημα με δύο θεμελιωδώς αντικρουόμενες πτυχές. Όσο προσπαθούμε να αυξήσουμε την ασφάλεια μιας συναλλαγής, τόσο μεγαλύτερη είναι η παραβίαση της ιδιωτικότητας του συναλλασσόμενου, καθώς απαιτούνται περισσότερες πληροφορίες για τη επίτευξη της αυξημένης ασφάλειας.

Είναι άραγε εφικτό να δώσουμε ταυτόχρονα λύση και στα δύο αυτά αντικρουόμενα προβλήματα; Δηλαδή, να πετύχουμε όσο το δυνατόν ασφαλέστερες συναλλαγές, με όσο το δυνατόν λιγότερες απαιτούμενες πληροφορίες από τον πολίτη;

Η απάντηση ίσως μπορεί να δοθεί από την ηλεκτρονική ταυτοποίηση και την ΚΠ.

Έτσι, η σημαντικότερη συμβολή της ηλεκτρονικής ταυτοποίησης μπορεί να είναι η εγκαθίδρυση της εμπιστοσύνης μεταξύ των δύο συναλλασσόμενων μερών: του πολίτη συναλλασσόμενου(φυσικό ή νομικό πρόσωπο) και του κράτους ή της επιχείρησης που αποτελεί το άλλο μέρος της συναλλαγής.

Η ηλεκτρονική υπογραφή και η ηλεκτρονική ταυτοποίηση (eID) και επαλήθευση ταυτότητας μπορούν να αποτελέσουν σημαντικά εργαλεία ώστε όλοι οι συμμετέχοντες σε μια συναλλαγή να μπορούν να βασίζονται σε ασφαλείς, αξιόπιστες και εύχρηστες διαδικτυακές υπηρεσίες.

Σε αυτήν την κατεύθυνση, η Ευρώπη αναγνωρίζοντας την ανάγκη για την προώθηση του ηλεκτρονικού εμπορίου, του ηλεκτρονικού επιχειρείν, τη διευκόλυνση της διαδικτυακής διεξαγωγής διοικητικών διαδικασιών στην ενιαία αγορά και κατανοώντας την ανάγκη ύπαρξης ενιαίας αντιμετώπισης για όλα τα κράτη μέλη, επανεξετάζει τα θέματα των ηλεκτρονικών υπογραφών αλλά και ανοίγει το θέμα της αμοιβαίας αναγνώρισης της ηλεκτρονικής ταυτοποίησης και της επαλήθευσης ταυτότητας [48]. Τόσο η ΕΕ, όσο και κάθε κράτος-μέλος ξεχωριστά οφείλουν να απαντήσουν στα παραπάνω ζητήματα αλλά και να ενισχύσουν την ανάπτυξη τόσο του ηλεκτρονικού εμπορίου και της ηλεκτρονικής τραπεζικής, όσο και την ανάπτυξη της ηλεκτρονικής διακυβέρνησης προς όφελος των πολιτών και των επιχειρήσεων. Η ανεπαρκής αντιμετώπιση των ζητημάτων ασφαλείας θα δημιουργήσει αθωράκιστες υπηρεσίες και απροστάτευτους πολίτες (φυσικά ή νομικά πρόσωπα).

Κατά συνέπεια, η διαχείριση ηλεκτρονικών ταυτοτήτων (eIDM) αποτελεί βασικό παράγοντα και προϋπόθεση για την ασφαλή και αποτελεσματική χρήση υπηρεσιών ηλεκτρονικών

συναλλαγών από τους πολίτες. Όπως εξάλλου είναι προφανές, σε ένα αξιόπιστο περιβάλλον ηλεκτρονικής ταυτοποίησης ενισχύεται τόσο η εμπιστοσύνη των πολιτών στη χρήση υπηρεσιών ηλεκτρονικής διακυβέρνησης, όσο και η πεποίθηση τους ότι διασφαλίζεται η προστασία των προσωπικών τους δεδομένων κατά τη χρήση των υπηρεσιών αυτών. Από την πλευρά του κράτους δε, οι δημόσιοι φορείς παροχής ηλεκτρονικών υπηρεσιών έχουν τη δυνατότητα να ταυτοποιούν τους πολίτες με τους οποίους συναλλάσσονται, δηλαδή ότι αυτοί οι συγκεκριμένοι πολίτες έχουν τα δικαιώματα και τα δεδομένα που υποστηρίζουν ότι έχουν, όπως αποδεικνύεται κι από μελέτη του Παρατηρητηρίου για την ΚτΠ [3].

Όσο όμως σημαντική κι αν είναι η ανάγκη για ηλεκτρονική ταυτοποίηση σε ένα ενιαίο ψηφιακό διεθνές περιβάλλον, εξίσου σημαντικά είναι τα ζητήματα ασφάλειας και ιδιωτικότητας που εγείρονται [5]. Με δεδομένη τη διαχείριση προσωπικών δεδομένων από εφαρμογές ηλεκτρονικής ταυτοποίησης, οι κίνδυνοι παραβίασης της ιδιωτικότητας από τη μη εξουσιοδοτημένη πρόσβαση, συλλογή και επεξεργασία προσωπικών ή και ευαίσθητων δεδομένων είναι εμφανείς. Είναι λοιπόν πολύ σημαντικό τα θέματα ασφάλειας, ιδιωτικότητας και προστασίας προσωπικών δεδομένων, να αντιμετωπίζονται με την απαιτούμενη σοβαρότητα και προσοχή.

Δεδομένου ότι, δεν έχει προσδιοριστεί επαρκώς η έννοια της ηλεκτρονικής ταυτότητας και εφόσον η οδηγία περί ηλεκτρονικών υπογραφών δεν καταφέρνει να καλύψει συνολικά το ζήτημα, το θέμα της ηλεκτρονικής ταυτοποίησης οντοτήτων δεν είναι και επαρκώς θεσμοθετημένο σε Ευρωπαϊκό επίπεδο και σε εθνικό επίπεδο των κρατών μελών. Εντούτοις, ζητήματα ασφάλειας και προστασίας προσωπικών δεδομένων έχουν τύχει ιδιαίτερης προσοχής από τον Ευρωπαίο νομοθέτη. Μάλιστα, πέραν των οδηγιών (βλ. Ευρωπαϊκή Οδηγία για την Προστασία των Προσωπικών Δεδομένων [44], σύμφωνα με το Ευρωπαϊκό Σύμφωνο Ανθρωπίνων Δικαιωμάτων (European Convention on Human Rights) [8] προβλέπονται συγκεκριμένοι περιορισμοί όσον αφορά στη διαχείριση προσωπικών δεδομένων στο άρθρο 8. Ειδικότερα θέματα που καθορίζουν τις ειδικές συνθήκες κάτω από τις οποίες η διαχείριση προσωπικών δεδομένων είναι αποδεκτή και νόμιμη, τις εγγυήσεις που παρέχονται για την προστασία της ιδιωτικότητας, και τις συνθήκες κάτω από τις οποίες είναι επιτρεπτή η πρόσβαση σε προσωπικά δεδομένα ορίζονται σε εθνικό επίπεδο από την εθνική νομοθεσία (National Register Acts, Identity Card Acts, eGovernment Acts) [9].

Όσο τα διλήμματα για ηλεκτρονική ταυτοποίηση πληθαίνουν τόσο μπορούν να απλοποιηθούν αν τα ανάγουμε στα ερωτήματα κλασικής ταυτοποίησης. Μήπως, αν δεν υπάρχει ανάγκη για ηλεκτρονική ταυτοποίηση, δεν υπάρχει ούτε η ανάγκη για φυσική ταυτοποίηση; Θα μπορούσαμε να φανταστούμε έναν κόσμο όπου η αναγνώριση του ατόμου δεν ήταν απαραίτητη; Θα μπορούσαμε στην περίπτωση αυτή να μιλάμε για οργανωμένες κοινωνίες, τουλάχιστον όπως τις γνωρίσαμε μέχρι σήμερα;

1.3. Το Σύγχρονο Περιβάλλον

Η λειτουργία της Διοίκησης δεν περιορίζεται πλέον στην άσκηση δημόσιας εξουσίας, αντίθετα η συναλλακτική δραστηριότητα αποτελεί σήμερα ένα από τα βασικότερα πεδία της διάδρασης μεταξύ κράτος και πολίτη. Η τεχνολογική εξέλιξη αλλά και οι απαιτήσεις για ποιοτική παροχή υπηρεσιών επέφεραν σημαντικές αλλαγές, καθιστώντας την ηλεκτρονικής διακυβέρνηση πραγματικότητα και τις ηλεκτρονικές συναλλαγές καθόλα νόμιμες και ενδεδειγμένες.

Ωστόσο, η έλλειψη φυσικής παρουσίας που να αποδεικνύει τα δεδομένα του πολίτη αποτελεί το κρίσιμο ζήτημα της ηλεκτρονικής συναλλαγής, καθώς απαιτείται επαυξημένη πλήρωση εγγυήσεων ασφάλειας, προκειμένου να είναι εφικτή η επαλήθευση της ταυτότητας του ατόμου που προβαίνει στην συναλλαγή. Διάφορες τεχνολογικές λύσεις, όπως μοναδικά αναγνωριστικά, ψηφιακά πιστοποιητικά, μέθοδοι κρυπτογράφησης, καθώς και οι ψηφιακές υπογραφές, που να επιφέρουν τις ίδιες έννομες συνέπειες με τις «πραγματικές» συναλλαγές.

Η Κάρτα Πολίτη, στο εξής ΚΠ, αποτελεί ένα πρόσφορο μέσο για την πραγματοποίηση τέτοιων συναλλαγών, καθώς έχει τη δυνατότητα να χρησιμοποιείται όχι μόνο ως αποδεικτικό της ταυτότητας του κατόχου αλλά και ως μέσο: α) αυθεντικοποίησής του για χρήση ηλεκτρονικών υπηρεσιών και β) ψηφιακής υπογραφής εγγράφων.

Την τελευταία πενταετία πολλές από τις χώρες μέλη της ΕΕ, σταδιακά έχουν υιοθετήσει ή σχεδιάζουν συστήματα διαχείρισης ηλεκτρονικών ταυτοτήτων, εθνικής ή τοπικής εμβέλειας, στο πλαίσιο της ηλεκτρονικής διακυβέρνησης και του εκσυγχρονισμού της συναλλαγής του πολίτη με τη Δημόσια Διοίκηση. Ενώ, παράλληλα, το πλήθος των ηλεκτρονικών υπηρεσιών που απαιτούν πιο επαρκείς λύσεις για την αυθεντικοποίηση του χρήστη αναμένεται να αυξηθεί κατακόρυφα στο άμεσο μέλλον, ιδιαίτερα με την ανάπτυξη των ευρυζωνικών υποδομών.

Είναι επομένως απαραίτητη προϋπόθεση η ανάπτυξη ασφαλών και αποτελεσματικών συστημάτων διαχείρισης ηλεκτρονικών ταυτοτήτων (electronic Identity Management System – eIDM) με γνώμονα την ποιοτικότερη παροχή υπηρεσιών αλλά και τον ίδιο τον πολίτη. Εξάλλου, η εμπιστοσύνη του χρήστη για τις ηλεκτρονικές συναλλαγές βασίζεται αναμφισβήτητα στην αξιοπιστία των ίδιων των συστημάτων ηλεκτρονικής διακυβέρνησης που μπορεί να περιορίσει την ανησυχία του πολίτη για την προστασία των δεδομένων του, προσωπικών ή μη.

Οι βασικοί παράγοντες για την υποστήριξη μιας εθνικής ηλεκτρονικής ταυτότητας είναι:

- η ανάγκη ανάπτυξης ηλεκτρονικών υπηρεσιών,
- η κοινή καταπολέμηση της απάτης ταυτότητας,
- η ανάπτυξη εθνικών και πανευρωπαϊκών μέτρων κατά της τρομοκρατίας,
- η δόμηση μιας Ευρωπαϊκής ταυτότητας

- και η εμφάνιση νέων 'διευρωπαϊκών' υπηρεσιών προκειμένου να μειωθούν οι δαπάνες.

Εκτός όμως από τους προαναφερθέντες παράγοντες, υπάρχουν επίσης διάφοροι νομοθετικοί, όπως η οδηγία 2005/60/ΕΚ [43] για το ξέπλυμα μαύρου χρήματος, η οποία απαιτεί τη χρήση ισχυρότερων μηχανισμών προσδιορισμού ταυτότητας από τους χρηματοδοτικούς οργανισμούς και η οδηγία 1999/93/ΕΚ [41] για τις ηλεκτρονικές υπογραφές, οι οποίες αξιοποιούνται για την επικύρωση οντοτήτων.

Το ενδιαφέρον ως προς τη χρήση της ηλεκτρονικής ταυτότητας παρουσιάζεται εξαιτίας της δυνατότητας χρησιμοποίησής της ως εγγράφου ταυτότητας, ως ταξιδιωτικού εγγράφου και ως μέσου παροχής ηλεκτρονικών υπηρεσιών. Έτσι μια ηλεκτρονική ταυτότητα περιλαμβάνει εξής βασικές λειτουργίες:

- ταυτοποίηση,
- αυθεντικοποίηση
- και ψηφιακή υπογραφή.

Οι τρείς αυτές λειτουργίες μπορούν δυνητικά να αξιοποιηθούν από ένα πλήθος διαφορετικών τεχνολογιών και εφαρμογών. Υπάρχει, όμως, και μια σημαντική ανάγκη για διαλειτουργικότητα μεταξύ των Εθνικών συστημάτων, προκειμένου να επιτρέπεται η χρήση της από Ευρωπαίους πολίτες παντού στην Ευρώπη. Για το λόγο αυτό, η διαλειτουργικότητα των ηλεκτρονικών υπηρεσιών πρέπει να βασιστεί σε ένα γενικό πλαίσιο με συγκεκριμένες προδιαγραφές, στο οποίο θα συμφωνούν όλα τα κράτη μέλη και το οποίο θα προστατεύει την ελευθερία των πολιτών και των προσωπικών τους δεδομένων. Επιπλέον, θα καλύπτει τις νομικές, οργανωτικές και λειτουργικές πτυχές, καθώς επίσης και την εμπιστοσύνη, την ασφάλεια και το τεχνικό πλαίσιο.

Το δελτίο ταυτότητας σύμφωνα με τον κλασσικό ορισμό της χρησιμεύει ως ένα «μοναδικό» έγγραφο για τον οπτικό προσδιορισμό της ταυτότητας του ιδιοκτήτη της [7]. Η ηλεκτρονική ταυτότητα, ως έξυπνη κάρτα με ενσωματωμένο τσιπ, έρχεται να καλύψει τις προαναφερόμενες απαιτήσεις σχετικά με την προστασία της ιδιωτικότητας, την υπεύθυνη και αποδεδειγμένη επικύρωση, την προστασία από την πλαστογράφηση, την διαλειτουργικότητα και την ενσωμάτωση ψηφιακών υπογραφών. Στις έξυπνες κάρτες προσδιορισμού ταυτότητας, σε αντίθεση με τις κάρτες SIM και τις τραπεζικές κάρτες με πλήρως ψηφιακά χαρακτηριστικά λειτουργίας, όλα τα χαρακτηριστικά γνωρίσματα ολόκληρης της κάρτας ταυτότητας είναι εξίσου σημαντικά, καθώς αξιοποιούνται και για τον οπτικό προσδιορισμό του φέροντος την ταυτότητα.

Η ευρωπαϊκή ΚΠ αποτελεί ένα ανοικτό πλαίσιο προδιαγραφών, το οποίο επιτρέπει στις κυβερνήσεις να επιλέξουν από τις προτεινόμενες συστάσεις εκείνες που μπορούν να ενσωματωθούν με τον πιο βέλτιστο τρόπο στη διαδικασία ταυτοποίησης που ακολουθούν. Για παράδειγμα, καθορίζονται οι επαφικές και οι ανεπαφικές διασυνδέσεις έξυπνων καρτών, βιομετρικά ή/και PIN για επικύρωση και προδιαγράφεται το πλήρες πλαίσιο για

μια ηλεκτρονική υπογραφή, καθώς επίσης και ένα σύνολο ηλεκτρονικών υπηρεσιών που μπορούν να υλοποιηθούν μέσα από τη χρήση της ΚΠ.

Στη σημερινή πραγματικότητα, όπου ολοένα και περισσότερες Ευρωπαϊκές χώρες υλοποιούν τέτοιες εθνικές ηλεκτρονικές κάρτες, και καθώς αναμένεται και η Ελλάδα σύντομα να διαθέτει μια αντίστοιχη υποδομή, ένα αρκετά ενδιαφέρον πεδίο μελέτης αποτελεί ο τρόπος εφαρμογής της ΚΠ στην ιδιαίτερη περίπτωση της χώρας μας, λαμβάνοντας υπόψη πιθανές ιδιαιτερότητες, αλλά και την υφιστάμενη κατάσταση στα ζητήματα της διαχείρισης ταυτοτήτων και της αυθεντικοποίησης, όπως και τις υπάρχουσες υποδομές ταυτοποίησης και ηλεκτρονικών υπηρεσιών.

Η παρούσα μελέτη φιλοδοξεί να καταγράψει την υφιστάμενη κατάσταση, να διακρίνει τα ιδιαίτερα χαρακτηριστικά που θα επηρεάσουν την επιτυχή υιοθέτησή της και κυρίως να προτείνει ρεαλιστικές επιλογές για την εφαρμογή της ΚΠ στην Ελλάδα, εστιάζοντας στους εξής διακριτούς τομείς:

- Στις σύγχρονες τάσεις και τη διεθνή πρακτική,
- Στις τεχνικές ιδιατερότητες που προκύπτουν από τις υφιστάμενες ΤΠΕ υποδομές
- Στις επιχειρησιακές ιδιαιτερότητες της χώρας,
- Στην πληρότητα και τα κενά του νομικού και κανονιστικού πλαισίου σε εθνικό και κοινοτικό επίπεδο,
- Στους μηχανισμούς ασφάλειας (φυσικής κάρτας και τσιπ) και της χρήσης των ηλεκτρονικών υπογραφών,

Ο στόχος της μελέτης είναι η δημιουργία ενός οδικού χάρτη για την ανάπτυξη μιας εύχρηστης, ασφαλούς και διαλειτουργικής κάρτας για τον Έλληνα πολίτη , η οποία θα σέβεται και θα προστατεύει τα προσωπικά δεδομένα και την ιδιωτικότητα του και θα τον καθιστά ασφαλή σε ένα παγκοσμιοποιημένο ηλεκτρονικό περιβάλλον.

1.4. Ηλεκτρονική Ταυτοποίηση και ΚΠ

Με τον όρο κάρτα ηλεκτρονικής ταυτότητας του πολίτη ορίζουμε την κάρτα, η οποία βασίζεται σε ηλεκτρονικές υποδομές για την ταυτοποίηση του νομίμου κατόχου της και την απόδοση σε αυτόν της ιδιότητας του πολίτη [3]. Η ηλεκτρονική αυτή ταυτότητα εμπεριέχει κρατικές εγγραφές - δηλ. εγγραφές που έχουν γίνει από επίσημη δημόσια αρχή - που αφορούν προσωπικά δεδομένα του πολίτη, με σκοπό την σύνδεσή τους με το συγκεκριμένο πρόσωπο κατά τρόπο αξιόπιστο και μοναδικό.

Επομένως, το κρίσιμο χαρακτηριστικό μιας τέτοιας κάρτας δεν είναι η δυνατότητα χρήσης σε συγκεκριμένες συναλλαγές - όπως συμβαίνει για τις ηλεκτρονικές ταυτότητες εν γένει - αλλά η αποδεικτική ισχύς της ως επίσημου αναγνωριστικού του κατόχου ως πολίτη. Με

άλλα λόγια, πρόκειται για την ηλεκτρονική κάρτα που παρέχεται υπό συγκεκριμένες διαδικασίες και προϋποθέσεις από αρμόδια δημόσια αρχή και συνιστά την βάση πάνω στην οποία «χτίζονται» οι επιμέρους έννομες σχέσεις κράτους - πολίτη, είτε υπό την μορφή παροχής υπηρεσιών και κτήσης δικαιωμάτων είτε υπό την μορφή τήρησης υποχρεώσεων και επιβολής κυρώσεων σε περίπτωση παράβασής τους.

Η ταυτοποίηση και αυθεντικοποίηση του πολίτη - χρήστη υπηρεσιών ηλεκτρονικής διακυβέρνησης αποτελούν εγγενές στοιχείο της ηλεκτρονικής επικοινωνίας του με το Δημόσιο, η δε ηλεκτρονική ταυτότητα αποσκοπεί στην ποιοτική ενίσχυση αυτής ακριβώς της επικοινωνίας κράτους - πολίτη. Συνεπώς, πριν αναφερθούμε στο θεσμικό πλαίσιο που ρυθμίζει την έκδοση και κατοχή του Ελληνικού αστυνομικού δελτίου ταυτότητας αλλά και στη δυνατότητα εισαγωγής ηλεκτρονικής ταυτότητας στην Ελλάδα, κρίνεται απαραίτητο να προβούμε σε μια σύντομη επισκόπηση των βασικών σημείων σχετικά με την ηλεκτρονική επικοινωνία κράτους - πολίτη υπό το ισχύον θεσμικό πλαίσιο.

Συνοπτικά, η εφαρμογή της ΚΠ μπορεί να εξασφαλίσει :

α) εμπιστευτικότητα ως προς την χρήση και διαχείριση των δεδομένων που απαιτούνται για την πραγματοποίηση των συναλλαγών

β) ακεραιότητα δεδομένων

γ) αξιόπιστες μεθόδους αυθεντικοποίησης ώστε να διασφαλίζεται ότι το άτομο είναι πράγματι αυτό που ισχυρίζεται ή προκύπτει ότι είναι και

δ) νομική δεσμευτικότητα συναλλαγής ανάλογη με αυτήν που συνεπάγεται μια διαπροσωπική συναλλαγή, υπό την έννοια της μη αποποίησης.

1.5. Ερευνητικά Ερωτήματα

Τα ερευνητικά ερωτήματα που θέτει και επιχειρεί να απαντήσει η παρούσα μελέτη αφορούν την ιδιαίτερη περίπτωση της εφαρμογής της ΚΠ στην Ελλάδα με βάση τις Ευρωπαϊκές προδιαγραφές ,και με ιδιαίτερη εστίαση στα θέματα ασφάλειας και ιδιωτικότητας που προκύπτουν, όπως είναι:

- Το Νομικό πλαίσιο
- Τα τεχνικά χαρακτηριστικά με βάση την υπάρχουσα υποδομή
- Τα λειτουργικά χαρακτηριστικά με βάση τις ιδιαίτερες ανάγκες της Ελλάδας

Ειδικότερα, ως προς το νομικό πλαίσιο θα επιχειρηθεί μια πλήρη καταγραφή του εθνικού και κοινοτικού ρυθμιστικού πλαισίου, μια αξιολόγηση της πληρότητάς του και μια ανάδειξη των κενών της νομοθεσίας, τόσο στο ευρύτερο θέμα της διαχείρισης ταυτοτήτων και της ηλεκτρονικής ταυτοποίησης, όσο και ειδικότερα στο ζήτημα της εφαρμογής της ΚΠ στην

Ελλάδα. Επίσης θα αναλυθούν οι νομικές προσεγγίσεις που μπορεί να επιλύσουν πιθανά προβλήματα στις μεθόδους ηλεκτρονικής ταυτοποίησης του πολίτη.

Σχετικά με τα τεχνικά χαρακτηριστικά και τη χρησιμοποιούμενη τεχνολογία, η μελέτη προσπαθεί αφενός να αναδείξει τη βέλτιστη τεχνολογικά λύση για την ηλεκτρονική ταυτοποίηση και διαχείριση ηλεκτρονικών ταυτοτήτων στην χώρα, να εντοπίσει και να προτείνει λύσεις για τη διαλειτουργικότητα της κάρτας σε ένα ευρωπαϊκό και διεθνές περιβάλλον και αφετέρου να αξιοποιήσει τη διεθνή σύγχρονη πρακτική. Τέλος, η εφαρμογή της ΚΠ στην Ελλάδα, αποτελεί ένα ιδιαίτερα φιλόδοξο έργο κυρίως ως προς τις λειτουργικές απαιτήσεις και το επιχειρησιακό μοντέλο. Στην Ελλάδα ζητήματα που είναι πιθανά λυμένα σε άλλες χώρες βρίσκονται σε πρώιμο στάδιο. Η Δημόσια Διοίκηση παρουσιάζει αρκετά μεγάλη πολυπλοκότητα και η γραφειοκρατία στην Ελλάδα είναι σχεδόν ο αποκλειστικός τρόπος περιγραφής της συναλλαγής του πολίτη με το δημόσιο. Μάλιστα, ακόμη και ο τρόπος οργάνωσης των υπηρεσιών του δημοσίου και των διαδικασιών του ακολουθούν ιδιαίτερα πολύπλοκα μοντέλα. Επιπλέον η ηλεκτρονική διακυβέρνηση, η προσφορά και η εξοικείωση με τη χρήση ηλεκτρονικών υπηρεσιών δεν είναι δεδομένη, καθώς ακόμη και αυτονόητες υπηρεσίες δεν παρέχονται ηλεκτρονικά, αλλά και ο πολίτης δεν έχει εντάξει στην καθημερινότητά του ακόμη τον ηλεκτρονικό τρόπο συναλλαγών.

Τέλος, αξίζει να σημειωθεί ότι στην περίπτωση της Ελλάδας, ζητήματα ηθικής, συμπεριφοράς και ευαισθησίας του λαού μας (π.χ. θρησκευτικές αντιλήψεις) μπορούν να αποτελέσουν κάποια από τα σημαντικότερα εμπόδια κατά την εφαρμογή της ΚΠ και σημαντικούς κινδύνους για την επιτυχή υιοθέτησή της από το σύνολο των πολιτών και μπορούν ακόμη να οδηγήσουν σε πλήρη απαξίωση της προσπάθειας.

1.6. Ανασκόπηση Κεφαλαίων

Η μελέτη δομείται κατά κεφάλαια ως εξής:

1. Στο Κεφάλαιο 1 εισάγεται η έννοια της ηλεκτρονικής ταυτοποίησης και η προσέγγιση στο ζήτημα της εφαρμογής της ΚΠ στα πλαίσια της ανάγκης για ταυτοποίηση στο σύγχρονο φυσικό και ψηφιακό διεθνές περιβάλλον.
2. Στο Κεφάλαιο 2 γίνεται αναφορά στις έξυπνες κάρτες, στα τεχνικά χαρακτηριστικά τους και στις χρήσεις και τα πλεονεκτήματα τους στην εφαρμογή της ΚΠ, ενώ καταγράφονται και οι προϋποθέσεις για ασφαλή ταυτοποίηση. Γίνεται αναφορά στις προδιαγραφές του ICAO αλλά και στο πρότυπο CEN 15480, στις τεχνικές λεπτομέρειες από το σχεδιασμό έως την υλοποίηση και αναφέρονται νέες τεχνικές εξελίξεις, όπως η ενσωμάτωση και διαχείριση βιομετρικών χαρακτηριστικών, ή η τεχνολογία RFID.
3. Στο Κεφάλαιο 3 καταγράφεται το σύνολο της εθνικής και κοινοτικής νομοθεσίας που είναι απαραίτητη για την κατανόηση και επεξεργασία των ζητημάτων που σχετίζονται άμεσα ή έμμεσα με την εφαρμογή της ΚΠ στην Ελλάδα και γίνεται μια

προσπάθεια για νομικές προσεγγίσεις και προτάσεις που θα επίλυαν διαχειριστικά και νομοτεχνικά ανακύπτοντα προβλήματα.

4. Στο Κεφάλαιο 4 περιγράφεται η Ευρωπαϊκή εικόνα σχετικά με την ηλεκτρονική ταυτοποίηση και η Ευρωπαϊκή προσέγγιση για την Ευρωπαϊκή ΚΠ. Παρέχονται λεπτομέρειες για το επιχειρησιακό μοντέλο, τις προδιαγραφές, τις λειτουργίες που εξυπηρετεί, τις χρήσεις και τα δεδομένα που περιέχει σε κάθε χώρα Κράτος-Μέλος της ΕΕ. Αξιολογείται η επιμέρους εφαρμογή των ηλεκτρονικών ταυτοτήτων και παρουσιάζονται τα συγκριτικά αποτελέσματα.
5. Στο Κεφάλαιο 5 επιχειρείται η κάλυψη των απαιτήσεων ασφάλειας κατά την εφαρμογή της ΚΠ, και η αντιμετώπιση ζητημάτων προστασίας προσωπικών δεδομένων και διασφάλισης της ιδιωτικότητας των πολιτών. Επιπλέον, θα περιγραφούν και θα συγκριθούν οι τεχνικές ασφάλειας και ιδιωτικότητας που μπορούν να χρησιμοποιηθούν για την αυθεντικοποίηση, εμπιστευτικότητα, ακεραιότητα και τη μη αποποίηση, την ταυτοποίηση και διαχείριση ταυτοτήτων, τις ψηφιακές υπογραφές και τελικά για τη διασφάλιση ενός ασφαλούς περιβάλλοντος για τον πολίτη-κάτοχο της ΚΠ.
6. Στο Κεφάλαιο 6 εξετάζεται η εφαρμογή της ΚΠ στην Ελλάδα, τα σενάρια υλοποίησης και συγκρίνονται τα σενάρια μεταξύ τους. Αναλύονται, ακόμη, τα δεδομένα που η ΚΠ πρέπει να περιέχει ανάλογα με τα σενάρια εφαρμογής, τις λειτουργίες που θα επιτελεί και τις χρήσεις της ΚΠ, καθώς επίσης το επιχειρησιακό μοντέλο εφαρμογής της, τον κύκλο ζωής, τις δομές που θα την υποστηρίξουν και τις αλλαγές που θα φέρει η υλοποίησή της. Τέλος αντιπαραβάλλεται η συμμόρφωσή της με διεθνή πρότυπα.
7. Στο Κεφάλαιο 7, τέλος, έπειτα από την προσπάθεια της μελέτης για μια όσο το δυνατόν πληρέστερη προσέγγιση για την ασφαλή και βέλτιστη εφαρμογή της ΚΠ στην Ελλάδα, συγκεντρώνονται τα κυριότερα συμπεράσματα που προκύπτουν από την ανάλυση των επιμέρους ενοτήτων, καθώς επίσης τα συμπεράσματα σχετικά με τις προτεινόμενες λύσεις/σενάρια για την εφαρμογή της κάρτας λαμβάνοντας υπόψη τα ιδιαίτερα χαρακτηριστικά. Στο κεφάλαιο αυτό, θα επισημανθούν κίνδυνοι που πιθανόν να προκύψουν από την υιοθέτησή της και απειλές που μπορεί να οδηγήσουν σε μη επιτυχημένη εφαρμογή της και θα αναδειχθούν ζητήματα για μελλοντική έρευνα.

2. ΤΕΧΝΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΑΙ ΠΡΟΔΙΑΓΡΑΦΕΣ

2.1. Η χρήση τεχνολογίας της Έξυπνης Κάρτας ως ΚΠ

Η ανάγκη για ασφάλεια και μυστικότητα αυξάνεται καθώς οι ηλεκτρονικές μορφές προσδιορισμού αντικαθιστούν τις φυσικές μορφές «πρόσωπο με πρόσωπο» και αυτές που βασίζονται σε έντυπα. Η εμφάνιση του Διαδικτύου και η επέκταση του εταιρικού δικτύου για να συμπεριλάβει την πρόσβαση από πελάτες και προμηθευτές εκτός «αναχωμάτων ασφάλειας» (firewalls) έχουν επιταχύνει την απαίτηση για λύσεις βασισμένες στην τεχνολογία κρυπτογράφησης δημόσιου κλειδιού.

Η σύγχρονη εκδοχή της ΚΠ θα είναι μια έξυπνη κάρτα (τεχνολογίας smart card), που θα έρθει να αντικαταστήσει τις παλαιού τύπου ελληνικές αστυνομικές ταυτότητες. Τα στοιχεία που θα περιλαμβάνει η ΚΠ, -όπως θα παρουσιασθούν αναλυτικά και στο Κεφάλαιο 6- τόσο εκτυπωμένα στην επιφάνειά της όσο και στο εσωτερικό της, δυνητικά θα είναι:

- Στοιχεία ΚΠ
- Προσωπικά στοιχεία πολίτη
- Ο αριθμός φορολογικού μητρώου (ΑΦΜ)
- Ο αριθμός μητρώου κοινωνικής ασφάλισης (ΑΜΚΑ)
- Ο αριθμός αστυνομικής ταυτότητας (ΑΔΤ)
- Ο αριθμός δημοτολογίου και Δήμος

Η ΚΠ θα συνοδεύεται από σειριακό αριθμό και κωδικό ασφαλείας που θα επιτρέπουν στους πολίτες την πρόσβαση σε διαδικτυακές υπηρεσίες όπως για παράδειγμα ηλεκτρονικού φορολογικού φακέλου, ηλεκτρονικού ιατρικού φακέλου, ηλεκτρονικού διαβατηρίου κ.α., ενώ ο στόχος είναι σταδιακά να γίνει εργαλείο πρόσβασης και σε άλλα μητρώα και υπηρεσίες με την πλήρη αξιοποίηση της ψηφιακής υπογραφής του κατόχου που σχεδιάζεται να συμπεριληφθεί σαν τεχνολογικό μέτρο ασφάλειας.

Για να γίνει περισσότερο κατανοητό του τι ακριβώς θα διασφαλίσει η ενσωμάτωση τεχνολογίας της έξυπνης κάρτας στην ΚΠ, θα πρέπει να γίνει μια αναλυτική περιγραφή των τεχνικών και λειτουργικών χαρακτηριστικών της χρήσης της, έτσι ώστε να γίνει αντιληπτό το γιατί είναι μια ιδανική λύση γι’ αυτό το σκοπό.

Ιστορικά οι πρόγονοι των έξυπνων καρτών θεωρούνται οι κάρτες του οργανισμού Diners Club που πρωτοεμφανίστηκαν την δεκαετία του 1950 [10]. Η αρχική τους εμφάνιση είχε το μέγεθος επαγγελματικής κάρτας (business card) με τυπωμένο το όνομα του κατόχου στην εμπρόσθια πλευρά. Η επίδειξη της και μόνο ήταν αρκετή, για να παρέχεται πίστωση στον κάτοχό της . Αρκετά χρόνια μετά, η κάρτα άρχισε να εκτυπώνεται με ανάγλυφη εκτύπωση

των στοιχείων του κατόχου ενώ το αμέσως επόμενο βήμα ήταν η παρουσία στο πίσω μέρος της μιας μαγνητικής λωρίδας (magnetic stripe), η οποία επέτρεπε τη μηχανική αποτύπωση των στοιχείων του κατόχου. Η συγκεκριμένη υλοποίηση κατάφερε να ενεργοποιήσει αλλά και να επιταχύνει την ηλεκτρονική επεξεργασία των συναλλαγών. Αυτό που όμως δεν κατάφερε να λύσει ήταν το πρόβλημα της απάτης, αφού οποιοσδήποτε κάτοχος εκτυπωτή καρτών (Embosser) ή με άλλον κατάλληλο εξοπλισμό, μπορούσε να δημιουργήσει πλαστές κάρτες .

Εικόνα 1-Έξυπνη κάρτα και Κάρτα μαγνητικής ταινίας

Η έξυπνη κάρτα ήρθε ως το επιστέγασμα της ταυτόχρονης βελτίωσης των πλαστικών καρτών και των microchip. Το 1969 παρουσιάστηκε στη Γαλλία μία κάρτα η οποία έφερε ενσωματωμένο κύκλωμα (chip). Παράλληλη ανάπτυξη των συγκεκριμένων καρτών παρουσιάστηκε στη Γερμανία (1967), στην Ιαπωνία (1970) και στις Η.Π.Α. (1972).

Δώδεκα χρόνια μετά και πιο συγκεκριμένα στο διάστημα 1982-84 η Ένωση Τραπεζικών Καρτών της Γαλλίας «έτρεξε» το πρώτο πιλοτικό πρόγραμμα έξυπνων καρτών και στην συνέχεια συνεργάστηκε με τις εταιρείες Bull, Philips και Schlumberger κάνοντας δοκιμές στις Γαλλικές πόλεις Blois, Caen και Lyon. Οι δοκιμές παρουσίασαν τεράστια επιτυχία και μέσα από αυτή την συνεργασία προέκυψε μία βελτίωση που αφορούσε την ενσωμάτωση της μαγνητικής λωρίδας, με σκοπό να διατηρηθεί η συμβατότητα με τα τότε υπάρχοντα συστήματα. Οι συγκεκριμένες πιλοτικές δοκιμές έδωσαν το έναυσμα στις Γαλλικές τράπεζες να εισάγουν τη χρήση των έξυπνων καρτών στις λειτουργίες τους και να τις προωθήσουν στο ευρύ κοινό. Παράλληλα, στο χώρο του marketing ξεκίνησε μία μεγάλη διαφημιστική εκστρατεία, μέσω της οποίας καθιερώθηκε ο όρος «έξυπνη κάρτα» (smart card).

2.2. Συγκριτικά πλεονεκτήματα της αξιοποίησης της τεχνολογίας των έξυπνων καρτών

Τα πλεονεκτήματα των έξυπνων καρτών σε σχέση με τις κάρτες μαγνητικής ταινίας είναι πάρα πολλά, και τείνουν να αποτελέσουν τη κυρίαρχη τάση για ανεπτυγμένες, απλές ή και πιο σύνθετες εφαρμογές σε ποικίλους τομείς.

Οι έξυπνες κάρτες μπορούν να παρέχουν ταυτοποίηση, επικύρωση, αποθήκευση δεδομένων και λειτουργία εφαρμογών, ωστόσο, το κύριο γνώρισμα των έξυπνων καρτών

είναι η ικανότητα να αποθηκεύουν και να επεξεργάζονται πληροφορίες με ασφαλή τρόπο. Έχουν ένα μοναδικό σύνολο ιδιοτήτων που τις καθιστά ιδιαίτερα πολύτιμες, οι κυριότερες από τις οποίες είναι η υψηλή ασφάλεια και η προστασία των δεδομένων που παρέχουν, η φορητότητα και η ευκολία χρήσης, η ανθεκτικότητα, η ικανότητα αποθήκευσης στοιχείων και εφαρμογών (για τα κρυπτογραφικά κλειδιά και άλλα στοιχεία) και το περιβάλλον προγραμματισμού.

Τα οφέλη των έξυπνων καρτών σχετίζονται άμεσα με τον όγκο των πληροφοριών και των εφαρμογών που είναι προγραμματισμένες για χρήση σε μια κάρτα. Μια απλή επαφική/ ανεπαφική έξυπνη κάρτα (αναλυτική περιγραφή των οποίων ακολουθεί παρακάτω) μπορεί να παρέχει δυνατότητα πρόσβασης σε πολλές τραπεζικές υπηρεσίες, προγράμματα φορολογικών συναλλαγών, πιστοποιητικά ταυτοποίησης κ.α., αλλά και να καλύπτει χρήσεις όπως, άδεια οδήγησης, κάρτα δημόσιων συγκοινωνιών. Επιπλέον, τα αποθηκευμένα στοιχεία σε μια κάρτα θα μπορούσαν να περιέχουν τον ιατρικό φάκελο του πολίτη και άλλες ιατρικές πληροφορίες που είναι κρίσιμες σε περίπτωση έκτακτης ανάγκης.

Μηχανισμοί ελέγχου πρόσβασης ενσωματώνονται στις έξυπνες κάρτες για να αυξήσουν την ασφάλεια όλων των υπηρεσιών. Παραδείγματος χάριν, στην περίπτωση των ανεπαφικών καρτών, είναι εφικτό να μπορεί να επιτρέψει μια συναλλαγή μόνο αν η κάρτα βρίσκεται εντός εμβέλειας μιας άλλης συσκευής. Αυτό μπορεί να αυξήσει σημαντικά την ασφάλεια της έξυπνης κάρτας αυξάνοντας με τη σειρά του την ανάπτυξη και χρήση δημόσιων υπηρεσιών. Έτσι μπορεί να δημιουργηθούν οικονομίες κλίμακας μέσω της μείωσης της γραφειοκρατίας και της πολυπλοκότητας των διαδικασιών.

Αν προσπαθούσαμε να συγκρίνουμε τις δύο προαναφερθείσες μορφές πλαστικών καρτών, θα παρατηρήσουμε σημαντικές διαφορές σε διάφορους τομείς τους οποίους και θα αναλύσουμε :

- *Στην αποθήκευση δεδομένων:* Οι περιορισμένες δυνατότητες αποθήκευσης πληροφοριών σε κάρτες μαγνητικής ταινίας (ως 140 byte πληροφορίας) την οδηγούν σε μειονεκτική θέση σε σχέση με τις έξυπνες κάρτες που παρουσιάζουν χωρητικότητα με δυνατότητα αποθήκευσης ως και 80 φορές περισσότερων ηλεκτρονικών δεδομένων (από 1Kbyte ως 32Kbytes πληροφορίας).
- *Στην ασφάλεια:* Η αλλοίωση ή και αναπαραγωγή καρτών μαγνητικής ταινίας από μη έγκυρους χρήστες με τον κατάλληλο εξοπλισμό αποτελεί εύκολη υπόθεση σε σχέση με τις έξυπνες κάρτες που παρέχουν αυξημένη ασφάλεια δεδομένων και συναλλαγών μέσω κρυπτογράφησης.
- Στ*ην αντοχή / διάρκεια:* Οι κάρτες μαγνητικής ταινίας είναι πολύ ευαίσθητες σε απομαγνητισμούς που μπορεί να οφείλονται στην χρήση ή σε εξωτερικά μαγνητικά πεδία. Αντίθετα, οι έξυπνες κάρτες είναι πολύ ανθεκτικές με αντοχή σε αλλεπάλληλες εισαγωγές μηχανημάτων υποδοχής καρτών που ξεπερνά τις 100.000 φορές και με μεγάλη διάρκεια ζωής.

- *Στην χρήση:* Η κάρτα μαγνητικής ταινίας γίνεται με σχεδιασμό μίας εφαρμογής (single application) που περιορίζεται σε απλά και επαναλαμβανόμενα καθήκοντα, ενώ αντίθετα οι έξυπνες κάρτες υποστηρίζουν πολλαπλές εφαρμογές (multiple applications).

- *Στην ευελιξία:* τα δεδομένα μίας κάρτας μαγνητικής ταινίας είναι μόνο αναγνώσιμα και οποιαδήποτε αλλαγή απαιτεί επανέκδοση κάρτας, ενώ σε μία έξυπνες κάρτες διαδικασίες ανάγνωσης, εγγραφής και ανανέωσης δεδομένων γίνονται εύκολα και γρήγορα.

- *Στη συνδεσιμότητα:* Χρήση καρτών μαγνητικής ταινίας μπορεί να γίνει μόνο μέσα από online σύνδεση με κάποια κεντρική βάση δεδομένων και ύπαρξη μισθωμένης γραμμής. Το συγκεκριμένο κόστος είναι δυστυχώς ένα επιπλέον κόστος επιβάρυνσης που δεν υπάρχει στην περίπτωση των έξυπνων καρτών, οι οποίες μπορούν να εκτελούν offline συναλλαγές με τρόπο ασφαλή και γρήγορο και τα στοιχεία των οποίων θα περάσουνε στο κεντρικό σύστημα συναλλαγών του εκδότη της κάρτας (Authentication Host) σε δεδομένη χρονική στιγμή, ανεξάρτητη της στιγμής της συναλλαγής.

Το κόστος κατασκευής έξυπνων καρτών είναι μεγαλύτερο από το αντίστοιχο των καρτών μαγνητικής ταινίας. Όμως λόγω της ανθεκτικότητάς τους, της δυνατότητας υποστήριξης πολλαπλών εφαρμογών, της μείωσης της απάτης αλλά και της μείωσης του κόστους τηλεφωνική σύνδεσης, οι έξυπνες κάρτες είναι τελικά πιο αποδοτικές ως προς το κόστος. Παρόλα αυτά η χρήση των έξυπνων καρτών αντί των καρτών μαγνητικής ταινίας δεν έχει την ίδια απήχηση παγκοσμίως. Έτσι το συγκεκριμένο προϊόν παρουσιάζεται εμπορικά επιτυχημένο σε αγορές όπως της Ευρώπης, της Ασίας και της Αφρικής. Υπάρχουν όμως αγορές στις οποίες δεν έχουν καταφέρει ακόμα να καθιερωθούν και να αποκτήσουν το ειδικό βάρος ως κοινού μέσου συναλλαγών και εφαρμογών.

Χαρακτηριστικό παράδειγμα αποτελεί η αγορά της Αμερικής στην οποία η τεχνολογία των έξυπνων καρτών είναι ακόμα σε πρώιμο στάδιο Βασικός λόγος αποτελεί το υψηλό κόστος των έξυπνων καρτών σε σχέση με τις κάρτες μαγνητικής ταινίας αλλά και η αναγκαιότητα ειδικών συσκευών ανάγνωσης καρτών (card readers). Πρόκειται για μία υψηλή επένδυση για την οποία τα Αμερικανικά οικονομικά ιδρύματα αντιδρούν αιτιολογώντας πως ήδη έχουν επενδύσει στα συστήματα μαγνητικής ταινίας.

Ο χρόνος και το κόστος πάντοτε αποτελούσαν στην τεχνολογία ανασταλτικούς παράγοντες για τολμηρές επενδύσεις. Βασικός όμως ανασταλτικός παράγοντας στην προηγούμενη περίπτωση αποτέλεσε η δομή διεξαγωγής οικονομικών και πληροφοριακών συναλλαγών η οποία έχει εξελιχθεί διαφορετικά από ότι στην Ευρώπη. Πιο συγκεκριμένα η Ευρώπη κατάφερε να αναπτύξει την τεχνολογία των έξυπνων καρτών με την λογική ενός αποδοτικού, ως προς το κόστος, τρόπου διεξαγωγής συναλλαγών οι οποίες αποσυνδέθηκαν από τις online διαδικασίες πιστοποίησης που στην Ευρώπη συνεπάγονται μεγάλο τηλεπικοινωνιακό κόστος. Αντίθετα στην Αμερική το τηλεπικοινωνιακό κόστος είναι χαμηλό με αποτέλεσμα να αποδυναμωθεί ένας πολύ βασικός παράγοντας εισαγωγής των έξυπνων καρτών.

2.3. Τα χαρακτηριστικά των Έξυπνων Καρτών

2.3.1. Περιγραφή της Έξυπνης Κάρτας

Οι έξυπνες κάρτες αποτελούν μια διαδεδομένη τεχνολογία εφαρμογής της αυθεντικοποίησης που βασίζεται σε κάτι που ο χρήστης κατέχει. Η αξιοποίηση της τεχνολογίας των έξυπνων καρτών παρουσιάζει ολοένα και μεγαλύτερη δυναμική και έχουν πλέον ευρύτατες εφαρμογές αφού χρησιμοποιούνται σήμερα πλέον στις τραπεζικές συναλλαγές, στις εφαρμογές ΚΠ (eID), στις τηλεπικοινωνίες, στις ηλεκτρονικές συσκευές κοκ. Αυτό, κατά κύριο λόγο, οφείλεται στην πρόοδο των τεχνολογιών κατασκευής ολοκληρωμένων κυκλωμάτων, στην αποτελεσματικότητα των δραστηριοτήτων προτυποποίησης και στην αύξηση των περιστατικών απάτης σε συγκεκριμένους τομείς εφαρμογών. Οι έξυπνες κάρτες αναπτύχθηκαν μέσα από την εξέλιξη των ολοκληρωμένων κυκλωμάτων και σε αντίθεση με τις μαγνητικές κάρτες (μερικά bytes επαναχρησιμοποίησης μνήμης και κάποιους στατικούς μηχανισμούς ασφάλειας για την προστασία της κάρτας), διαθέτουν μικροεπεξεργαστή μέσω του οποίου επιτυγχάνουν ένα υψηλό επίπεδο ασφαλείας για τα δεδομένα που αποθηκεύουν και επεξεργάζονται και υποστηρίζουν την ασφαλή ενημέρωση/επικαιροποίηση ή επαναλαμβανόμενη εγγραφή δεδομένων στην κάρτα, οποτεδήποτε μετά την έκδοσή της.

Εικόνα 2- Έξυπνη κάρτα ως Ευρωπαϊκή ΚΠ

Εάν προσπαθούσε κανείς να δώσει μία σύντομη ερμηνεία για το τι ακριβώς είναι μία έξυπνη κάρτα θα μπορούσε να την περιγράψει ως ένα chip περιβεβλημένο με πλαστικό και μάλιστα στο μέγεθος μιας κάρτας. Λειτουργικά, θα λέγαμε ότι είναι ένας μικροϋπολογιστής με δυνατότητες ευελιξίας, εύκολης και ταχύτατης μεταφοράς των δεδομένων, διασφάλισης αυτών, καθώς και προστασίας όλων των προσωπικών δεδομένων. Και τελικά, ένας προσωπικός ηλεκτρονικός υπολογιστής, με δυνατότητα να χωρά στο πορτοφόλι ή την τσέπη του κατόχου του.

Οι έξυπνες κάρτες είναι ουσιαστικά μικροσκοπικοί υπολογιστές, που έχουν το μέγεθος και τη φόρμα μιας πιστωτικής κάρτας, πάνω στην οποία είναι ενσωματωμένο ένα ολοκληρωμένο κύκλωμα (chip), στην εμπρόσθια αριστερή πλευρά.

Εικόνα 3-Έξυπνη κάρτα με ενσωματωμένο ολοκληρωμένο κύκλωμα (Chip)

Το ολοκληρωμένο κύκλωμα περιέχει τις επαφές εισόδου-εξόδου και μπορεί να περιέχει μόνο μνήμη ή και μικροεπεξεργαστή. Το ολοκληρωμένο κύκλωμα μπορεί να παρέχει μια ασφαλή δομή πολλαπλών επιπέδων και να επιτρέπει ιεραρχημένη πρόσβαση, καθιστώντας δύσκολη την πρόσβαση στα στοιχεία και την παραποίηση αυτών, να υπολογίζει κρυπτογραφικές συναρτήσεις (cryptographic functions) και να αντιλαμβάνεται άμεσα προσπάθειες πρόσβασης, οι οποίες δεν είναι έγκυρες όπως για παράδειγμα το κλείδωμα της κάρτας SIM σε περίπτωση εισαγωγής λανθασμένου PIN περισσότερες από τρεις -συνήθως- φορές.

Η έξυπνη κάρτα ενσωματώνει ένα μικροεπεξεργαστή, ο οποίος βρίσκεται κάτω από μια επαφή από χρυσό, προσαρμοσμένο στη μια πλευρά της. Οι έξυπνες κάρτες ή κάρτες με μικροεπεξεργαστή διαθέτουν CPU (συνήθως 16 bytes) που υποστηρίζει μικρή ομάδα εντολών (εξασφαλίζοντας μικρό μέγεθος), απαραίτητων για την επικοινωνία με τον αναγνώστη καρτών/υπολογιστή και την κρυπτογράφηση των περιεχόμενων δεδομένων, μνήμη ROM (μέχρι 346 Kbytes) για την αποθήκευση του λειτουργικού συστήματος, μνήμη RAM (μέχρι 8 Kbytes) για γρήγορη εκτέλεση εντολών και μνήμη EE PROM (μέχρι 256 Kbytes) για την αποθήκευση δεδομένων και εφαρμογών. Πρόκειται ουσιαστικά για ολοκληρωμένους μικρούς ηλεκτρονικούς υπολογιστές, οι οποίοι στερούνται μόνο συσκευών εισόδου/εξόδου. Η τροφοδοσία της κάρτας εξασφαλίζεται από τον αναγνώστη έξυπνης κάρτας (smart card reader), στον οποίο εισάγεται η κάρτα προκειμένου να επικοινωνήσει με κάποιο κεντρικό υπολογιστή, όπου υπάρχουν τα στοιχεία του χρήστη ώστε να εξασφαλιστεί η πρόσβαση σε δεδομένα. Ο μικροεπεξεργαστής της κάρτας και ο υπολογιστής, με τον οποίο συνδέεται, επικοινωνούν πριν ο μικροεπεξεργαστής επιτρέψει την πρόσβαση στα δεδομένα που περιέχονται στη μνήμη της κάρτας. Με τον τρόπο αυτό ενισχύεται η ασφάλεια των δεδομένων σε αντίθεση κι έτσι ο χρήστης διασφαλίζεται, αν η κάρτα του βρεθεί σε διαφορετικά από τα δικά του χέρια.

Μια έξυπνη κάρτα μπορεί:

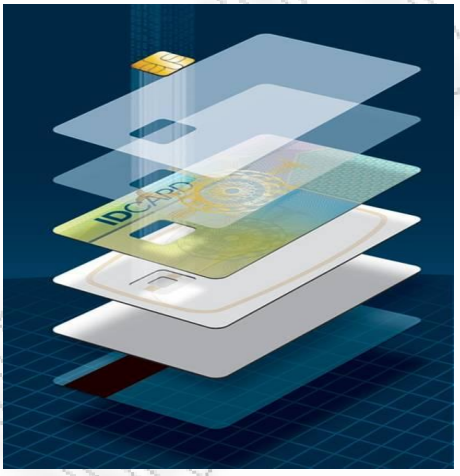
- Να συμμετέχει σε μια αυτοματοποιημένη ηλεκτρονική συναλλαγή,

- Να χρησιμοποιείται για να προσθέσει ασφάλεια στην συναλλαγή,
- Να καταστήσει πρακτικά αδύνατη οποιαδήποτε απόπειρα παραποίησης ή αντιγραφής της
- Να αποθηκεύσει στοιχεία με ασφάλεια,
- Να φιλοξενήσει/τρέξει μια σειρά αλγορίθμων και λειτουργιών ασφάλειας και

Να αντικατασταθεί άμεσα σε περίπτωση απώλειας χωρίς να μπορεί να χρησιμοποιηθεί από τρίτους.

2.3.2. Τα κατασκευαστικά χαρακτηριστικών της «έξυπνης» Κάρτας

Η κάρτα κατασκευάζεται από πλαστικό, συνήθως πολυβινυλικό χλωρίδιο, αλλά είτε και πολυανθρακικού ή στυρένιο ακρυλονιτριλιακού βουταδιενίου (acrylonitrile butadiene styrene).



Εικόνα 4-Στρώσεις κατασκευής της έξυπνης κάρτας

Τα φυσικά χαρακτηριστικά της προσδιορίζονται από διεθνή πρότυπα. Παραδείγματος χάριν, το μέγεθος μιας κάρτας καθορίζεται από το διεθνή οργανισμό για την τυποποίηση (International Organization for Standardization, ISO) με το πρότυπο ISO 7810. Το ISO 7816 και τα μεταγενέστερα πρότυπα καλύπτουν παραμέτρους κατασκευής, φυσικά και ηλεκτρονικά χαρακτηριστικά, θέση των σημείων επαφής, πρωτόκολλα επικοινωνίας, χώρο αποθήκευσης στοιχείων και άλλα. Το σχεδιάγραμμα και ο μορφότυπος των στοιχείων, εντούτοις, μπορούν να ποικίλουν από προμηθευτή σε προμηθευτή.

Εκτός από τα κατασκευαστικά και φυσικά πρότυπα, ένας αυξανόμενος αριθμός προτύπων αφορά και τις εφαρμογές. Οι προμηθευτές πιστωτικών καρτών και κινητής τηλεφωνίας, οι τράπεζες των Ηνωμένων Πολιτειών και της Ευρώπης, οι πιστωτικές και χρεωστικές αντιπροσωπείες είναι παραδείγματα των οργανώσεων που προσαρμόζουν εφαρμογές και διαδικασίες έξυπνων καρτών που συνδέονται αποκλειστικά στις υπηρεσίες που προσφέρουν και τις επιχειρήσεις με τις οποίες συνεργάζονται/συναλλάσσονται. Οι δύο

μεγαλύτεροι προμηθευτές λειτουργικών συστημάτων για έξυπνες κάρτες είναι η MAOSCO (μια βιομηχανική κοινοπραξία) και η Microsoft.

2.3.3. Συσκευές «ανάγνωσης» έξυπνων καρτών

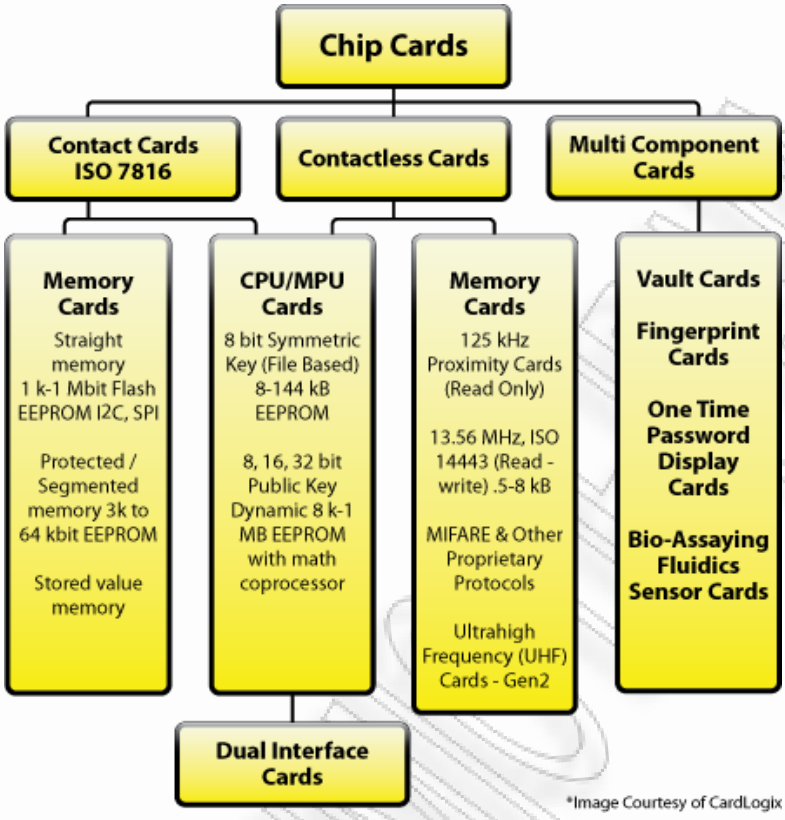
Τερματικές συσκευές που διαθέτουν συσκευές επικοινωνίας με την κάρτα όπως πληκτρολόγιο, εκτυπωτή, οθόνη, modem κλπ. (EFT/POS, κινητά τηλέφωνα, καρτοτηλέφωνα, αυτόματοι πωλητές, αποκωδικοποιητές, ATM, κλπ) και αναγνώστες-εγγραφείς έξυπνων καρτών που δε φέρουν εξοπλισμό, αλλά συνδέονται με τερματικές συσκευές που δε διαθέτουν αναγνώστη έξυπνων καρτών, όπως οι Η/Υ και τα info kiosks.

Οι περισσότερες κάρτες με chip κατασκευάζονται από πολλαπλές επιστρώσεις από διαφορετικά υλικά, τα οποία όταν έρθουν σε επαφή προσδίδουν στην κάρτα συγκεκριμένα χαρακτηριστικά και χρόνο ζωής. Η τυπική κάρτα σήμερα κατασκευάζεται από PVC, Polyester ή Polycarbonate. Οι επιστρώσεις της κάρτας τυπώνονται πρώτα και συμπιέζονται σε πρέσα. Στη συνέχεια ακολουθεί το κόψιμο το οποίο ακολουθείται από την ενσωμάτωση του chip και την εισαγωγή δεδομένων στην κάρτα. Στο σύνολο, υπάρχουν μέχρι και 30 βήματα για την κατασκευή μιας έξυπνης κάρτας. Τα συνολικά μέρη συμπεριλαμβανομένου και του λογισμικού και των πλαστικών μπορεί να φτάσουν και τα 12 διακριτά μέρη – όλα αυτά υπάρχουν ενοποιημένα σε ένα ενωμένο πακέτο, το οποίο εμφανίζεται στον τελικό χρήστη ως μια απλή κάρτα.

2.3.4. Είδη καρτών

Οι έξυπνες κάρτες διακρίνονται:

1. Από τον τρόπο που η κάρτα «διαβάζεται» και «γράφεται».
2. Από τον τύπο του chip που ενσωματώνεται μέσα στην κάρτα και τις δυνατότητές του. Υπάρχει μια μεγάλη γκάμα από δυνατότητες οι οποίες μπορούν να επιλεγούν κατά τον σχεδιασμό.



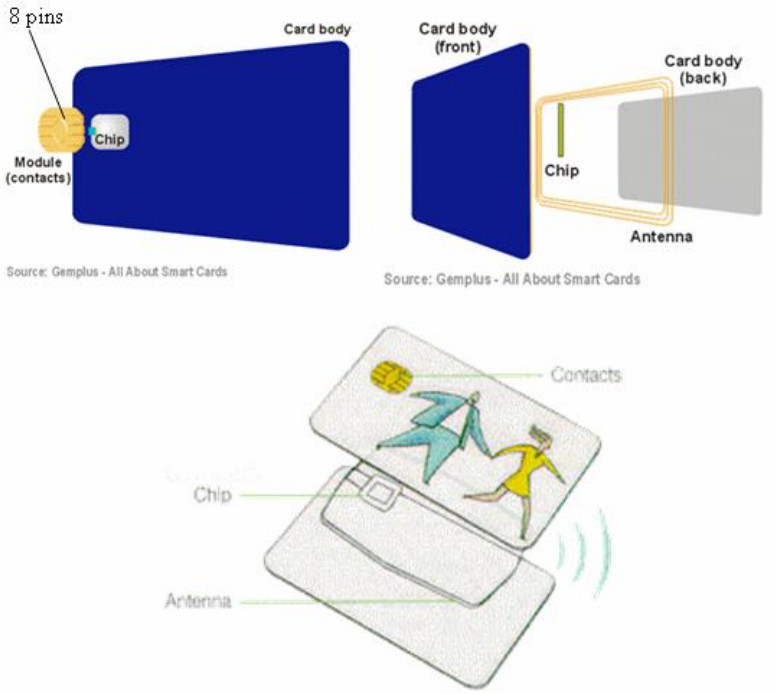
Εικόνα 5- Κατηγορίες έξυπνων καρτών (Πηγή http://www.cardlogix.com)

2.3.4.1. *Επαφικές ή μη-επαφικές έξυπνες κάρτες (Contact or Contactless)*

Με βάση τον τρόπο επικοινωνίας τους με το εξωτερικό περιβάλλον διακρίνουμε τις κάρτες σε:

- έξυπνες κάρτες με επαφές (contact cards)
- Ανεπαφικές ή ασύρματες έξυπνες κάρτες (contactless cards)
- Υβριδικές κάρτες ή συνδυασμένες κάρτες (Hybrid or Combination Cards)

Διατάξεις των παραπάνω ειδών καρτών μπορούμε να δούμε στο σχήμα που ακολουθεί.



Εικόνα 6-Έξυπνες Κάρτες(Αριστερά contact, δεξιά contactless κάρτα, κάτω combination)

2.3.4.1.1. Επαφικές έξυπνες κάρτες (Contact cards)

Οι έξυπνες κάρτες με επαφές (contact cards) έχουν ένα χρυσό καλυμμένο υλικό διαμέτρου εκατοστόμετρου με 8 επαφές. Αυτές οι επαφές συνδέονται με ένα καλώδιο και στη συνέχεια σε ένα μικροτσίπ κάτω από το υλικό. Το μικροτσίπ μπορεί να είναι ένα τσιπ μνήμης ή ένα τσιπ μικροεπεξεργασίας που περιέχει τη μνήμη και μια CPU. Επικοινωνούν με τις ηλεκτρικές επαφές και πρέπει να εισαχθούν σε μια συσκευή ανάγνωσης προκειμένου να διαβασθούν ή να εισαχθούν δεδομένα.

Μία τέτοια κάρτα δε μπορεί να λειτουργήσει αυτόνομα. Δηλαδή, είναι απαραίτητη η επικοινωνία της με άλλες συσκευές για την ανταλλαγή δεδομένων εισόδου και εξόδου αλλά και για την παροχή ενέργειας. Οι συσκευές που «συνδέονται» με τις κάρτες λέγονται CAD (Card Acceptance Device) και μπορεί να είναι είτε card reader μέσω ενός υπολογιστή είτε ένα τερματικό το οποίο λειτουργεί αυτόνομα. Ανάλογα με τη συναλλαγής στην οποία σκοπεύουμε να χρησιμοποιήσουμε μια κάρτα μπορούμε να επιλέξουμε έναν από τους παρακάτω τύπους.

2.3.4.1.2. Ανεπαφικές έξυπνες κάρτες (Contactless cards)

Οι ανεπαφικές ή ασύρματες έξυπνες κάρτες (contactless cards) έχουν ένα ενσωματωμένο τσιπ μικροεπεξεργασίας και χρησιμοποιούν τους proximity couplers για να πάρουν τις πληροφορίες από το τσιπ της κάρτας. Στην περίπτωση μιας ανεπαφικής κάρτας η επικοινωνία γίνεται ασύρματα, χωρίς φυσική επαφή, με ηλεκτρομαγνητικά πεδία. Οι κάρτες αυτές δεν διαθέτουν pins , αλλά έχουν ενσωματωμένο ραδιοπομποδέκτη και κεραία γύρω από την περιφέρεια της κάρτας και ενεργοποιείται όταν η κάρτα ακτινοβολείται σε μια συγκεκριμένη απόσταση από το συζευκτήρα και επομένως επιτρέπουν απομακρυσμένη

επικοινωνία. Η αμφίδρομη μετάδοση κωδικοποιείται και μπορεί να κρυπτογραφηθεί με τη χρησιμοποίηση ενός συνδυασμού ενός αλγορίθμου που ενσωματώνει ο κατασκευαστής του τσιπ από την κατασκευή του, την τυχαία παραγωγή αριθμών συνόδου και το πιστοποιητικό του κατόχου της κάρτας, το μυστικό κλειδί, ή προσωπικό αριθμό αναγνώρισης (personal identification number, PIN).

Ο σχεδιασμός της σύνδεσης μπορεί να προάγει χωριστές και ιδιαίτερες συνδέσεις με πολλαπλάσιες κάρτες εάν είναι μέσα στην ακτίνα/εύρος του αναγνώστη. Η ενέργεια μπορεί να παρέχεται με μια μικρή μπαταρία είτε μέσω της κεραίας. Επειδή οι ανεπαφικές κάρτες δεν απαιτούν φυσική επαφή με έναν αναγνώστη, το εύρος της επικοινωνίας μπορεί να εκτείνεται αρκετά, αλλά γενικά περιορίζεται από τα πρότυπα. Ενδεικτικά, η μέγιστη απόσταση που απαιτεί η κεραία για την επικοινωνία είναι περίπου δέκα μέτρα, ενώ πριν από πέντε χρόνια ήταν περίπου εξήντα εκατοστά. Πρόκειται για κάρτες πολύ πιο δαπανηρές από τις κάρτες με επαφή και είναι καταλληλότερες για τις εφαρμογές πρόσβασης και προσπέλασης. Οι χρήσεις τους αναφέρονται αναλυτικά σε ξεχωριστή ενότητα στη συνέχεια του παρόντος κεφαλαίου.

2.3.4.1.3. Υβριδικές έξυπνες κάρτες (Combination cards)

Τέλος, οι Υβριδικές κάρτες ή συνδυασμένες κάρτες (Hybrid or Combination Cards) είναι συνδυασμός των δύο παραπάνω κατηγοριών αφού ενσωματώνουν και τους δύο παραπάνω τρόπους μετάδοσης κι επομένως μπορούν κατά περίπτωση να επικοινωνήσουν με τις συσκευές ανάγνωσης είτε με ενσύρματο τρόπο (φυσική επαφή), είτε ασύρματα, με ραδιοσυχνότητα.

2.3.5. Κάρτες Μνήμης, Μικροεπεξεργαστών και Κάρτες Πολλαπλών Εφαρμογών

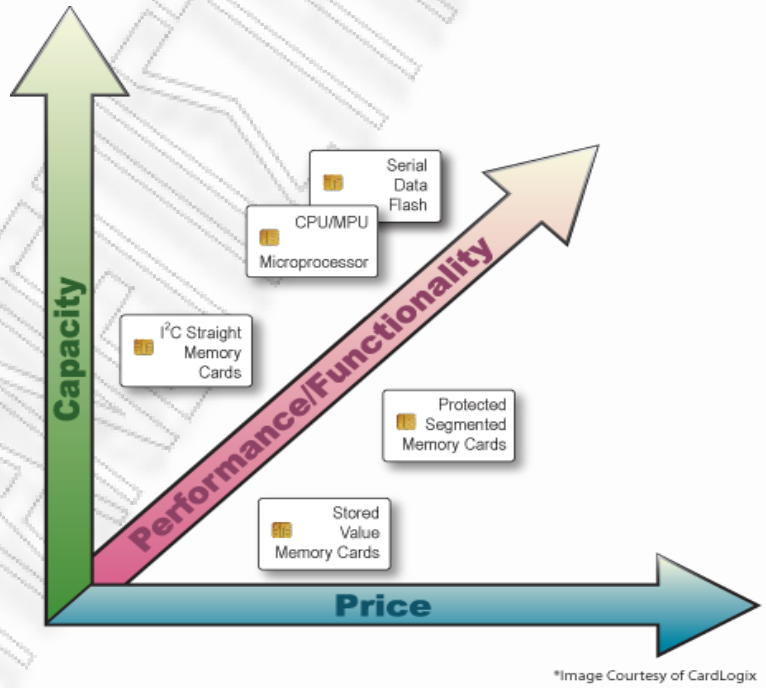
Με το κριτήριο ικανότητας επεξεργασίας, διακρίνονται τρεις κατηγορίες έξυπνων καρτών:

- **Κάρτες Μνήμης**: Οι κάρτες μνήμης δεν μπορούν να διαχειριστούν αρχεία και δεν έχουν καμία ισχύ επεξεργασίας για τη διαχείριση των δεδομένων. Όλες οι κάρτες μνήμης επικοινωνούν με τους αναγνώστες μέσα από σύγχρονα πρωτόκολλα. Σε όλες τις κάρτες μνήμης διαβάζονται και γράφονται σε μια σταθερή διεύθυνση μνήμης στην κάρτα. Υπάρχουν τρεις πρωτογενείς τύποι καρτών μνήμης: Straight, Protected, & Stored Value:
    - **Straight Κάρτες Μνήμης**: Θεωρούνται καταχρηστικά έξυπνες κάρτες καθώς περιέχουν μόνο τα τμήματα αποθήκευσης μη επανεγγράψιμης μνήμης και μπορούν να αντιμετωπισθούν ως μικρές δισκέτες με προαιρετική ασφάλεια και δεν έχουν δυνατότητα επεξεργασίας δεδομένων. Αυτές οι κάρτες απλά αποθηκεύουν δεδομένα και δεν έχουν κάποια επεξεργαστική δυνατότητα. Αυτό σιγά σιγά αλλάζει καθώς μεγάλες ποσότητες αυτού του είδους καρτών χρησιμοποιούνται και στην GSM αγορά, όπου και τέτοιου είδους

χαρακτηριστικά είναι ευπρόσδεκτα. Αυτού του είδους οι κάρτες δεν μπορούν να ταυτοποιηθούν από τον αναγνώστη όποτε και το σύστημα host θα πρέπει να ενημερωθεί για τον τύπο των καρτών με μη αυτοματοποιημένο τρόπο. Οι κάρτες αυτές αντιγράφονται εύκολα και δεν μπορούν να εντοπιστούν από on-card identifiers.

- **Protected / Segmented Κάρτες Μνήμης**: Αυτές οι κάρτες έχουν ενσωματωμένη λογική για έλεγχο πρόσβασης της μνήμης τους. Πολλές φορές αναφέρονται και ως intelligent Memory cards, και μπορούν να ρυθμιστούν ώστε να προστατεύσουν μέρος μόνο ή το σύνολο της μνήμης τους. Μερικές από αυτές μπορούν να εμποδίσουν την εγγραφή ή το διάβασμα με τη χρήση ενός κλειδιού ή ενός password. Οι κάρτες αυτές δεν αντιγράφονται εύκολα και μπορούν να εντοπιστούν από on-card identifiers.

- **Stored Value Κάρτες Μνήμης**: Αυτές οι κάρτες έχουν σχεδιαστεί με αποκλειστικό στόχο την αποθήκευση πληροφορίας ή token. Οι περισσότερες κάρτες αυτού του είδους ενσωματώνουν μέτρα ασφάλειας κατά την κατασκευή τους. Τέτοια μέτρα μπορεί να είναι password keys και logic τα οποία είναι hard-coded στο chip από τον κατασκευαστή. Υπάρχει ελάχιστη μνήμη διαθέσιμη για άλλη χρήση. Για απλές εφαρμογές όπως τηλεφωνικές κάρτες, το chip έχει 60 ή 12 memory cells, για κάθε μονάδα τηλεφώνου. Η κάρτα μνήμης αδειάζει κάθε φορά που μια τηλεφωνική μονάδα χρησιμοποιείται.



Εικόνα 7-Ισοζύγιο πλεονεκτημάτων – μειονεκτημάτων ειδών μνήμης έξυπνων καρτών (Πηγή http://www.cardlogix.com)

- **Έξυπνες κάρτες ή κάρτες μικροεπεξεργαστών (smart cards, IC cards, microprocessor cards)**: Οι έξυπνες κάρτες ή κάρτες μικροεπεξεργαστών περιέχουν τα επανεγγράψιμα τμήματα μνήμης, δηλαδή μπορεί να προστεθεί, διαγραφεί και επεξεργαστεί η πληροφορία που περιλαμβάνεται. Ο επεξεργαστής τους πέρα από την αποθήκευση και την ασφάλιση πληροφοριών μπορεί να λαμβάνει αποφάσεις που ορίζονται στις προδιαγραφές του έργου για το οποίο θα χρησιμοποιηθούν.

- **Έξυπνες κάρτες πολλαπλών εφαρμογών (multi-application smart cards)**: Οι έξυπνες κάρτες νέας γενιάς έχουν ανοιχτά λειτουργικά συστήματα (Java, MULTOS) και μπορούν να εκτελούν περισσότερες από μία εφαρμογές, αλλά παρέχουν και τη δυνατότητα στο χρήση να επεξεργάζεται τις εγκατεστημένες εφαρμογές, να διαγράφει ή/και να προσθέτει άλλες.

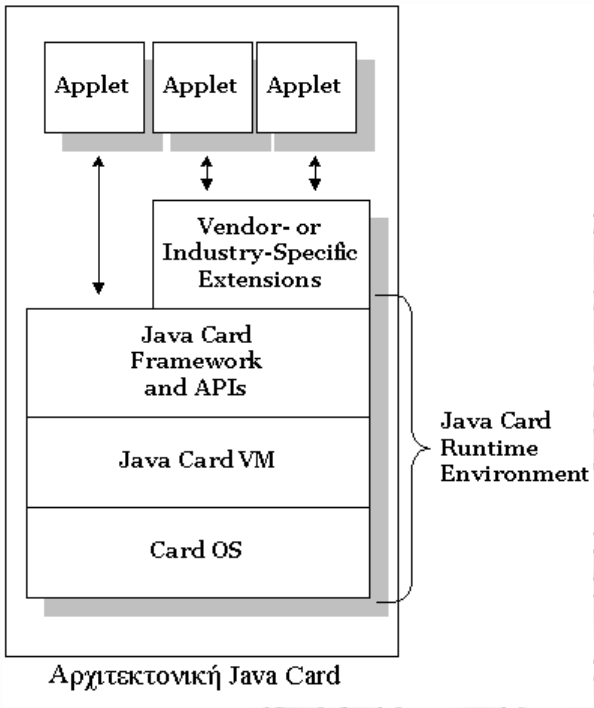
2.3.6. Τεχνολογία Java Card

Αρχικά, το λογισμικό των έξυπνων καρτών ήταν γραμμένο ειδικά για το συγκεκριμένο μικροεπεξεργαστή της κάθε κάρτας. Αυτό σημαίνει ότι είναι πολύ δύσκολη η συνεργασία εφαρμογών που προορίζονται για διαφορετικές κάρτες. Μια λύση στο πρόβλημα αυτό, αποτελεί η τεχνολογία που μας προσφέρει η sun για την ανάπτυξη εφαρμογών με το υποσύνολο της γλώσσας java, την java card. Αυτή χρησιμοποιείται και για τον προγραμματισμό smart buttons αλλά και USB tokens. Τα προγράμματα τα οποία είναι ικανά να φορτωθούν σε μια java card είναι όλα java card applets. Τα applets αυτά επικοινωνούν με το Java Card Runtime Environment (JCRE). Υποστηρίζεται επίσης η δυνατότητα ανάπτυξης ενός ενδιάμεσου επιπέδου το οποίο θα παρεμβάλλεται στην επικοινωνία των appletse το JCRE και λέγεται Vendor- or Industry-Specific Extensions.

Το JCRE αποτελείται από:

- Java Card Framework and APIs: Περιλαμβάνει τις κλάσεις και τα πακέτα που είναι απαραίτητα για τον προγραμματισμό μιας java card. Είναι το πιο «υψηλό» επιπέδου και έρχεται σε επικοινωνία με τα applets πριν από όλα. Τέλος, στέλνει τις εντολές στο Java Card Virtual Machine.

- Java Card Virtual Machine: Ορίζει ένα υποσύνολο της γλώσσας Java, τη Java Card, και της Java Virtual Machine, τη Java Card Virtual Machine. Χωρίζεται σε δύο μέρη εκ των οποίων το ένα βρίσκεται εκτός κάρτας, java card converter, και το άλλο εντός. Το δεύτερο περιλαμβάνει τον Java Card Inerpreter ο οποίος εκτελεί εντολές Java Card Bytecode, ελέγχει τη δέσμευση μνήμης και τη δημιουργία αντικειμένων, παίζει κύριο ρόλο για την ασφάλεια κατά το χρόνο εκτέλεσης.



Εικόνα 8-Αρχιτεκτονική JavaCard

Ο Java Card Converter βρίσκεται εκτός κάρτας και η κύρια λειτουργία του είναι η μετατροπή των αρχείων που θέλουμε να φορτώσουμε στην κάρτα, παράδειγμα μια εφαρμογή, σε μορφή τέτοια ώστε να επιτρέπεται η φόρτωση και η εκτέλεση της. Με άλλα λόγια μετατρέπει τα αρχεία .class, τα οποία παράγονται από τον πηγαίο κώδικα (source code) μέσω ενός Java compiler, σε ένα αρχείο CAP. Κατά τη διαδικασία της μετατροπής, ο Java Card Converter εκτελεί κάποιες ενέργειες τις οποίες Java Virtual Machine εκτελεί κατά τη φόρτωση κλάσεων (class loading):

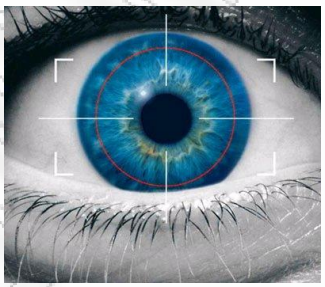
- Πιστοποιεί ότι οι java κλάσεις είναι σωστά σχηματισμένες.
- Ελέγχει για τυχών παραβιάσεις της Java Card.
- Αρχικοποιεί τις static μεταβλητές.
- Αναλύει συμβολικές αναφορές σε κλάσεις, μεθόδους και πεδία σε μια συμπαγή μορφή την οποία η κάρτα μπορεί να διαχειριστεί πιο αποτελεσματικά.
- Βελτιστοποιεί τον bytecode μέσω της εκμετάλλευσης πληροφοριών που λαμβάνονται κατά τη φόρτωση των κλάσεων και κατά τη διάρκεια της σύνδεσης (linking time).
- Εκχωρεί μνήμη και δημιουργεί δομές δεδομένων της Virtual Machine για την αναπαράσταση κλάσεων.
- Card OS: Το λειτουργικό σύστημα της κάρτας το οποίο υλοποιεί τις βασικές της λειτουργίες όπως έχει αναλυθεί πιο πάνω.

2.4. Χρήση Βιομετρικών Στοιχείων

2.4.1. Βιομετρικά στοιχεία ενσωματωμένα στην Κάρτα του Έλληνα Πολίτη

Μια από τις καινοτομίες της ηλεκτρονικής ταυτότητας του πολίτη έγκειται στην δυνατότητα χρήσης βιομετρικών του δεδομένων ως μοναδικών αναγνωριστικών χαρακτηριστικών. Η ενίσχυση της προσπάθειας για ασφαλή ταυτοποίηση συνίσταται στην εφαρμογή μεθόδων βιομετρίας - όπως αναγνώριση της ίριδας του οφθαλμού ή δακτυλικού αποτυπώματος - κατά τις οποίες χρησιμοποιούνται στοιχεία που συνδέονται άμεσα με την φυσική υπόσταση του χρήστη, παρέχοντας έτσι εχέγγυα μοναδικότητας και αξιοπιστίας. Η ποιοτική διαφοροποίηση που συνεπάγεται η χρήση βιομετρικών μεθόδων συνίσταται στο ότι η ταυτοποίηση ή αυθεντικοποίηση του ατόμου δεν βασίζεται σε κάτι που έχει ή σε κάτι που γνωρίζει, αλλά σε κάτι που είναι.

Ήδη, αρκετές χώρες υιοθέτησαν ή πρόκειται να υιοθετήσουν βιομετρικά στοιχεία στην ηλεκτρονική τους ταυτότητα. Σε ευρωπαϊκό επίπεδο, στα πλαίσια της καταπολέμησης της τρομοκρατίας σε παγκόσμιο επίπεδο με παράλληλο σεβασμό των ανθρωπίνων δικαιωμάτων, σύμφωνα με τον Κανονισμό ΕΚ 2252/2004 [26] θεσπίστηκε η χρήση βιομετρικών μεθόδων στο ευρωπαϊκό διαβατήριο, για τις εθνικές ταυτότητες. Στη στρατηγική αυτή εκτιμάται ότι οι βελτιώσεις στις χρησιμοποιούμενες τεχνολογίες καταχώρησης και ανταλλαγής δεδομένων, καθώς και η συμπερίληψη βιομετρικών πληροφοριών σε ταξιδιωτικά έγγραφα και έγγραφα ταυτότητας, μπορεί να συμβάλει στην αποτελεσματικότητα των συνοριακών ελέγχων και στην επίτευξη μεγαλύτερης ασφάλειας για τους πολίτες.



Εικόνα 9-Βιομετρικό στοιχείο ίριδας

Ο ICAO [65], λαμβάνοντας υπόψη του τη νομοθεσία σχετικά με τα προσωπικά δεδομένα διεθνώς, στις σχετικές του συστάσεις (έγγραφο ICAO 9303 P3V2 [87]) για τα MRTDs, επιλέγει ως υποχρεωτικό διαλειτουργικό βιομετρικό τα χαρακτηριστικά του προσώπου με τη μορφή της φωτογραφίας, και καθορίζει άλλα βιομετρικά, όπως τα δακτυλικά αποτυπώματα ή την ίριδα του ματιού, ως προαιρετικά, καθώς τα δακτυλικά αποτυπώματα ή η αναγνώριση της ίριδας θεωρούνται ως μια μεγαλύτερη «εισβολή» έναντι της ιδιωτικότητας και απαιτούν μια περισσότερο χρονοβόρα συλλογή τόσο κατά την αρχικοποίηση/εξατομίκευση της κάρτας όσο και μετέπειτα στα διάφορα σημεία ελέγχου.

Εικόνα 10-Έξυπνη κάρτα με βιομετρικά χαρακτηριστικά ίριδας και δακτυλικού αποτυπώματος

Η χρήση βιομετρικών στοιχείων γίνεται μέσω αυτοματοποιημένων μεθόδων ταυτοποίησης ή αυθεντικοποίησης, οι οποίες βασίζονται σε μοναδικά χαρακτηριστικά της φυσιολογίας ή της συμπεριφοράς του φυσικού προσώπου. Οι δύο βασικές κατηγορίες τεχνικών βιομετρίας είναι : α) τεχνικές που βασίζονται στην φυσιολογία και καταμετρούν τα βιολογικά και, άρα, σταθερά, χαρακτηριστικά του ατόμου όπως αναγνώριση δακτυλικών αποτυπωμάτων, ίριδας οφθαλμού, προσώπου ή σχήματος χεριών, αναγνώριση φωνής, ανάλυση τύπου DNA και β) τεχνικές βασιζόμενες στην συμπεριφορά του ατόμου με τις οποίες καταμετρώνται δυναμικά, και άρα μεταβλητά, στοιχεία όπως ανάλυση τρόπου βαδίσματος, εξακρίβωση χειρόγραφης υπογραφής κ.λπ. Για την ΚΠ επιλέγονται σταθερά βιομετρικά, κυρίως δακτυλικά αποτυπώματα, αναγνώριση προσώπου και ίριδας οφθαλμού.

Υπό την προϋπόθεση ότι πληρούνται οι απαιτήσεις για ασφαλή και αξιόπιστη ταυτοποίηση και αυθεντικοποίηση του κατόχου μέσω της χρήσης των κατάλληλων χαρακτηριστικών, η ηλεκτρονική ταυτότητα του πολίτη διαθέτει όλες τις απαιτούμενες ιδιότητες ενός «καλού αναγνωριστικού», αφού πληροί τα εξής κριτήρια :

1. *καθολικότητα εφαρμογής και εύρους*, δεδομένου ότι αποτελεί αναγνωριστικό με εφαρμογή σε όλους τους πολίτες - ή νόμιμους κατοίκους - του κράτους έκδοσης

2. *μοναδικότητα ανά άτομο*, αφού βασίζει την ταυτοποίηση /αυθεντικοποίηση σε στοιχεία που προσδιορίζουν κατά τρόπο μοναδικό τον νόμιμο κάτοχό της

3. *μονιμότητα-διάρκεια*, το βιομετρικό στοιχείο μένει αμετάβλητο για μεγάλη χρονική περίοδο, ή για πάντα

4. *αποκλειστικότητα - μοναδικότητα χρήσης*, αφού αποτελεί επαρκή και ακριβή τρόπο ταυτοποίησης του ατόμου, χωρίς να χρειάζεται η χρήση και άλλου αναγνωριστικού μέσου

5. *αξιοπιστία*, ακριβώς γιατί τα δεδομένα που καταγράφει ή/και ενσωματώνει συνδέονται με το άτομο κατά τρόπο αναπόσπαστο και αναλλοίωτο από την πάροδο του χρόνου (με αυτό το κριτήριο αναφερόμαστε κυρίως στην χρήση βιομετρικών δεδομένων)

Εκτός από τα υποχρεωτικά ποιοτικά χαρακτηριστικά, κρίσιμο είναι τα βιομετρικά χαρακτηριστικά που επιλέγονται να πληρούν και μια σειρά από πρόσθετες απαιτήσεις ποιότητας (υψηλή και ακριβή απόδοση κατά την βιομετρική μέτρηση, μη δυνατότητα καταστρατήγησης αξιόπιστης χρήσης του και αποδοχή από το υποκείμενο). Επιπλέον, σχετικά με τη διαδικασία εκτίμησης του βιομετρικού χαρακτηριστικού είναι σημαντικό να λαμβάνονται υπόψη παράγοντες που αφορούν στο μέγεθος του πληθυσμού προς εγγραφή, στη χρήση του (ταυτοποίηση ή αυθεντικοποίηση), στο περιβάλλον εφαρμογής του κ.α..

Η ενσωμάτωση των βιομετρικών χαρακτηριστικών γίνεται με τη διαδικασία εγγραφής και επαλήθευσης. Ειδικότερα, για την εγγραφή χρησιμοποιείται κατάλληλος αισθητήρας με τον οποίο εξάγονται ειδικά χαρακτηριστικά για κάθε χρήστη, ώστε να δημιουργηθεί μια διαρθρωμένη σμίκρυνση της βιομετρικής του εικόνας (template) . Η βιομετρική μέτρηση, και όχι το ίδιο το βιομετρικό δεδομένο, είναι το στοιχείο που τελικώς αποθηκεύεται σε ψηφιακή μορφή, αφού η απευθείας καταγραφή του ανεπεξέργαστου βιομετρικού αποφεύγεται για λόγους προστασίας των προσωπικών δεδομένων του κατόχου. Κατά την επαλήθευση, ο κάτοχος δίνει νέο βιομετρικό δείγμα που επίσης μετατρέπεται σε εικόνα, ώστε να συγκριθεί με το αποθηκευμένο και να πιστοποιηθεί, μέσω ειδικής διαδικασίας, ότι και τα δύο ανήκουν στο ίδιο άτομο. Η επαλήθευση διαφέρει, ανάλογα με τον σκοπό χρήσης της βιομετρικής μεθόδου (ταυτοποίηση ή αυθεντικοποίηση). Στην ταυτοποίηση, το νέο δείγμα συγκρίνεται με το σύνολο των σχεδιότυπων που έχουν αποθηκευθεί σε σχετική κεντρική βάση δεδομένων, ώστε να πιστοποιηθεί ο κάτοχος (one-to-many identification). Αντίθετα, στην περίπτωση της αυθεντικοποίησης, το δείγμα συγκρίνεται μόνο με το σχεδιότυπο που βρίσκεται αποθηκευμένο (όχι απαραίτητα σε κεντρική βάση) και σχετίζεται με τον κάτοχο της ηλεκτρονικής ταυτότητας (one-to-one authentication).

Η βιομετρική ταυτοποίηση αν και αποτελεί μηχανισμό που θα μπορούσε να καταπολεμήσει περισσότερο αποτελεσματικά προβλήματα αυθεντικοποίησης και περιπτώσεις πλαστοπροσωπίας και πλαστογραφίας (όπως για παράδειγμα την πλαστογραφία «σχετικής ομοιότητας», η οποία αφορά σε συλλογή γνήσιων εγγράφων πιστοποίησης π.χ. eIDs, διαβατήρια, ώστε να βρεθεί κάποιο που σχεδόν να ταιριάζει με το αυθεντικό) αλλά εγείρει σημαντικές ανησυχίες για την παραβίαση της ιδιωτικότητας των πολιτών. Εντούτοις, η χρήση των βιομετρικών χαρακτηριστικών προωθείται πολιτικά ,διεθνώς, στα πλαίσιο της καταπολέμησης της τρομοκρατίας.

Που βρίσκεται όμως το όριο στη χρήση τέτοιων τεχνολογιών; Και ποιες είναι οι συνέπειες που μπορούν να προκύψουν από την πιθανή διαρροή των βιομετρικών των πολιτών και η συσχέτισή τους με το υποκείμενο, ή η μη εξουσιοδοτημένη αναπαραγωγή τους και η μη εξουσιοδοτημένη χρήση τους; Και σε αυτήν την περίπτωση πόσο μεγαλύτεροι μπορεί να είναι οι κίνδυνοι για τον πολίτη (π.χ. πως μπορεί κάποιος να αποδείξει την αθωότητά του για ένα έγκλημα που δεν διέπραξε, αν βρεθούν δικά του βιομετρικά ίχνη); Η χρήση μονόδρομων συναρτήσεων μπορεί να δώσει λύσεις. Ωστόσο, αφενός προϋποθέτει τη χρήση templates (που χρησιμοποιούνται ως μονόδρομες συναρτήσεις) για την επαλήθευση του αποθηκευμένου στο τσιπ template με το βιομετρικό χαρακτηριστικό που θα παραχθεί κατά τη διαδικασία ελέγχου (κάτι το οποίο προς το παρόν δεν προβλέπεται από το θεσμικό πλαίσιο και δεν εφαρμόζεται) και αφετέρου δεν επιλύει το ζήτημα της καταστρατήγησης της ιδιωτικότητας του πολίτη από τις κρατικές υπηρεσίες και της συλλογής βιομετρικών του δεδομένων σε κεντρικές βάσεις δεδομένων.

Συνοψίζοντας, τα συμπεράσματα που προκύπτουν από την ανάλυση της χρήσης των βιομετρικών στοιχείων ως μοναδικών αναγνωριστικών για την ηλεκτρονική ταυτότητα είναι σαφείς οι αυξημένες εγγυήσεις αξιοπιστίας που προκύπτουν, καθώς είναι ιδιαίτερα δύσκολο να αποκρύψει κάποιος την ταυτότητά του ή να χρησιμοποιήσει στοιχεία ενός τρίτου (identity theft). Εντούτοις, η εκτεταμένη χρήση τέτοιων μεθόδων γεννά έντονους προβληματισμούς για τους κινδύνους από αθέμιτη, καταχρηστική ή αυθαίρετη χρήση αυτού του τόσο ισχυρού εργαλείου.

2.5. Η τεχνολογία Radio Frequency Identification στην κάρτα του Πολίτη

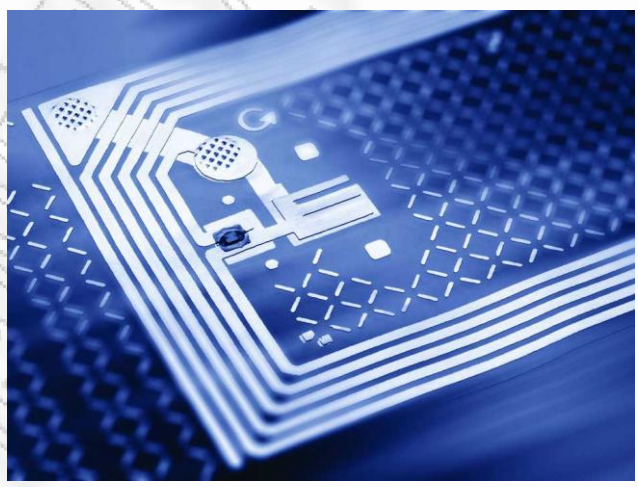
Μια RFID ΚΠ είναι υβριδική (hybrid card), ανήκει δηλαδή στη κατηγορία έξυπνων καρτών (smart cards) πού έχουν ενσωματωμένα δύο microchips. Ένα ανεπαφικό τσιπ μνήμης (contactless memory chip) και ένα επαφικό με επεξεργαστή (contact processor chip).

Εικόνα 11- Η RFID έξυπνη κάρτα ως ΚΠ (πάνω δεξιά το ασύρματο microchip, αριστερά το microchip επαφής)

Η τεχνολογία Radio Frequency Identification (RFID) είναι μία μέθοδος αυτόματου εντοπισμού και αναγνώρισης αντικειμένων, που βασίζεται στην αποθήκευση και στην ασύρματη ανάκτηση, από μακριά, δεδομένων, τα οποία αποθηκεύονται σε ειδικές μικροσκοπικές συσκευές που ονομάζονται ετικέτες RFID (RFID tags), ή αναμεταδότες (transponders).

Εικόνα 12-Το σύμβολο των βιομετρικών εγγράφων εμφανιζόμενο υποχρεωτικά στο εξωτερικό περίβλημα

Ένα σύστημα RFID αποτελείται από τα εξής μέρη: Την ετικέτα (tag), η οποία αποτελείται από το τσιπ και την κεραία, τον αναγνώστη (RFID reader) με κεραία, τους servers και άλλες διατάξεις, καθώς και το λογισμικό της εφαρμογής. Σκοπός του συστήματος είναι να διευκολύνει την μετάδοση δεδομένων, ασύρματα από την ετικέτα RFID, σε έναν αναγνώστη RFID και στην συνέχεια να επιτρέψει την επεξεργασία αυτών για τις ανάγκες της συγκεκριμένης εφαρμογής. Η ετικέτα RFID είναι μία συσκευή που μπορεί να συνδεθεί με η να ενσωματωθεί σε ένα προϊόν, ένα ζώο, η ένα άτομο με σκοπό τον εντοπισμό του, με την χρήση ραδιοκυμάτων. Οι ετικέτες RFID αποτελούνται από τουλάχιστον δύο μέρη. Το ένα είναι ένα ολοκληρωμένο κύκλωμα για την αποθήκευση και την επεξεργασία των πληροφοριών, την διαμόρφωση και την αποδιαμόρφωση ενός σήματος ραδιοσυχνότητας (RF) και ίσως άλλες εξειδικευμένες λειτουργίες. Το δεύτερο μέρος είναι μία κεραία που αποτελείται από επίπεδες σπείρες κατασκευασμένες από χαλκό η αλουμίνιο και χρησιμοποιείται για την λήψη και την εκπομπή του σήματος.



Εικόνα 13-Ολοκληρωμένο κύκλωμα

Η ετικέτα RFID διαβάζεται ακόμη και από πολλά μέτρα μακριά, αυτόματα με ειδική συσκευή, η οποία ονομάζεται αναγνώστης (RFID reader), και δεν είναι απαραίτητο να είναι στην γραμμή θέας του αναγνώστη (reader).

2.5.1. Ετικέτες RFID

Υπάρχουν τρεις γενικές κατηγορίες ετικετών RFID: παθητικές (passive), ημιπαθητικές (semi-passive) και ενεργές (active). Οι παθητικές ετικέτες RFID δεν έχουν εσωτερική πηγή ενέργειας, δηλ. μπαταρία. Αυτό σημαίνει ότι η κεραία τους είναι κατά τέτοιο τρόπο σχεδιασμένη, ώστε να παίρνει ενέργεια από το σήμα που λαμβάνει και απαντά στέλνοντας σήμα το οποίο λαμβάνεται από τον αναγνώστη (RFID reader).

Οι ημιπαθητικές ετικέτες είναι όμοιες με τις ενεργές. δηλαδή έχουν δική τους πηγή ενέργειας, αλλά η μπαταρία τους χρησιμοποιείται μόνο για να τροφοδοτεί με ενέργεια το μικροτσίπ και όχι για να εκπέμπει σήματα. Τα ραδιοκύματα αντανακλώνται πίσω και λαμβάνονται από τον αναγνώστη, όπως συμβαίνει με τις παθητικές ετικέτες. Σε αντίθεση με τις παθητικές ετικέτες, οι ενεργές έχουν δική τους πηγή ενέργειας, η οποία χρησιμοποιείται για να τροφοδοτεί το ολοκληρωμένο κύκλωμα και να εκπέμπει το σήμα στον αναγνώστη (reader).

Πολλές ενεργές ετικέτες έχουν δραστική εμβέλεια περίπου 100 μέτρων και η διάρκεια ζωής της μπαταρίας τους είναι περίπου 10 χρόνια.

2.5.2. Εφαρμογές της τεχνολογίας RFID

Η τεχνολογία RFID έχει πολλές χρήσιμες εφαρμογές, σημαντικότερες από τις οποίες είναι:

- *Πληρωμή διοδίων:* Μία από τις πιο διαδεδομένες χρήσεις της τεχνολογίας RFID είναι η πληρωμή διοδίων στις εθνικές οδούς. Στην Ελλάδα εφαρμόζεται το σύστημα «e-Pass» για την πληρωμή διοδίων στην Αττική Οδό και το σύστημα «ΤΕΟ-Pass» για την πληρωμή διοδίων σε όλες τις εθνικές οδούς της χώρας.

- *Διαβατήρια:* Microchip RFID ενσωματώνονται στα νέου τύπου διαβατήρια, τα λεγόμενα βιομετρικά διαβατήρια η e-passports, τα οποία περιλαμβάνουν προσωπικά δεδομένα του κατόχου τους, όπως ονοματεπώνυμο, εθνικότητα, φύλο, ημερομηνία γέννησης, ύψος, χρώμα μαλλιών, κεφαλής και ματιών, τον αριθμό του διαβατηρίου, ημερομηνία έκδοσης, ημερομηνία λήξης, καθώς επίσης και μία ψηφιακή φωτογραφία. Τα διαβατήρια αυτά έχουν αρχίσει να εκδίδονται από πολλές χώρες. Ο ICAO (International Civil Aviation Organization) [65] είναι ο διεθνής οργανισμός ο οποίος έχει συντάξει τις διεθνείς προδιαγραφές για τα βιομετρικά διαβατήρια.

- *Πιστωτικές κάρτες:* Αρκετές πιστωτικές κάρτες περιέχουν ήδη RFID.

- *Βιβλιοθήκες:* Μεταξύ των πολλών εφαρμογών της τεχνολογίας RFID είναι η χρησιμοποίησή της στις βιβλιοθήκες. Η τεχνολογία αυτή έχει αρχίσει σταδιακά να αντικαθιστά τα παραδοσιακά barcodes σε αντικείμενα που διατίθενται στις βιβλιοθήκες (βιβλία, CD, DVD κ.λπ.). Σε κάθε ετικέτα RFID η οποία επικολλάται σε ένα βιβλίο, CD η DVD, περιέχονται πληροφορίες όπως: ο τίτλος, ο συγγραφέας, χρόνος κυκλοφορίας κ.λπ.

- *Διαχείριση προϊόντων (product tracking):* Ετικέτες RFID χρησιμοποιούνται για την διαχείριση των εμπορευμάτων σε καταστήματα λιανικής πώλησης, στην διαχείριση εμπορευματοκιβωτίων και παλετών (containers & pallet tracking), καθώς και για την διαχείριση αποσκευών και εμπορευμάτων στα αεροδρόμια.

- *Έλεγχος πρόσβασης σε κτίρια:* Ειδικές κάρτες, εφοδιασμένες με microchip RFID, χρησιμοποιούνται στα σύγχρονα συστήματα ελέγχου πρόσβασης σε κτίρια. Τις κάρτες αυτές αρκεί να τις πλησιάσει ο κάτοχός τους σε απόσταση λίγων εκατοστών, σε ειδικούς σταθερούς αναγνώστες, για να γίνει η ταυτοποίηση του κατόχου τους.

- *Διαχείριση και έλεγχος οχημάτων:* Στις νήσους Βερμούδες, γίνεται καταγραφή μέσω συστήματος RFID των περίπου 47.000 οχημάτων που κυκλοφορούν στο νησί με σκοπό την καταγραφή της οδικής συμπεριφοράς των οδηγών και κυρίως τον αποτελεσματικότερο τρόπο για την είσπραξη των προστίμων από τροχαίες παραβάσεις. Σύμφωνα με το πρόγραμμα αυτό που έχει αρχίσει να εφαρμόζεται, σε κάθε αυτοκίνητο, στο νησί, έχει τοποθετηθεί μία ετικέτα RFID, η οποία θα επικοινωνεί με μία βάση δεδομένων στην Τροχαία, και θα είναι αναγνώσιμη από φορητούς και σταθερούς αναγνώστες των αστυνομικών Αρχών.

- *Αυτοκινητοβιομηχανία:* Τα κλειδιά των αυτοκινήτων Toyota , Lexus, Ford και άλλων εταιρειών, από το 2004, είναι τεχνολογίας RFID. Ο οδηγός μπορεί να ανοίξει την πόρτα του αυτοκινήτου από απόσταση 1 μέτρου περίπου.

- *Εφαρμογή λύσεων RFID στην βιομηχανία:* Οι γραμμές παραγωγής στις μεγάλες βιομηχανίες είναι απέραντες και πολυσύνθετες εγκαταστάσεις. Αυτός είναι ο λόγος για τον οποίο πολλοί βιομήχανοι προστρέχουν στην τεχνολογία RFID για να τους βοηθήσει στην απλοποίηση των λειτουργιών της βιομηχανίας τους, στην μείωση του κόστους και στην βελτίωση της ποιότητας των παραγόμενων προϊόντων. Το προσωπικό μιας γραμμής παραγωγής σε μία βιομηχανία μπορεί να χρησιμοποιήσει αναγνώστες RFID για να ελέγχει την ολοκλήρωση των διαφόρων φάσεων παραγωγής.

- *Διαχείριση και καταγραφή ζώων:* Η Καναδική Υπηρεσία Εντοπισμού Βοοειδών είναι η πρώτη στον κόσμο η οποία εφάρμοσε την τεχνολογία RFID για την καταγραφή και παρακολούθηση των κοπαδιών βοοειδών. Γι' αυτόν τον σκοπό γίνεται εμφύτευση στο δέρμα των ζώων ειδικών microchip RFID. Στην Ελλάδα ξεκίνησε το 2003 η σήμανση και καταγραφή όλων των ιδιόκτητων σκύλων .Όλοι οι ιδιοκτήτες σκύλων υποχρεούνται να σημαίνουν τον σκύλο τους σύμφωνα με τον Ν. 3170/2003 και την Υπουργική Απόφαση 280241. Αρμόδιος φορέας για την τήρηση της ηλεκτρονικής βάσης δεδομένων των στοιχείων των σκύλων είναι ο Πανελλήνιος Κτηνιατρικός Σύλλογος. Ο τρόπος σήμανσης των ζώων είναι η μέθοδος της ηλεκτρονικής ταυτοποίησης με την τεχνολογία RFID και συνίσταται στην εμφύτευση ειδικού microchip RFID κάτω από το δέρμα του σκύλου. Βασίζεται στα πρότυπα ISO 11784 και 11785, όπως καθορίζεται από τον Κανονισμό 998/2003 του Ευρωπαϊκού Κοινοβουλίου. Κάθε microchip φέρει ένα μοναδικό αριθμό που αντιστοιχεί στο ζώο

που σημαίνεται, αποτελείται από 16 στοιχεία και αντιστοιχεί στα στοιχεία που αναγράφονται στο Πιστοποιητικό Ηλεκτρονικής Ταυτοποίησης.

- *Εμφύτευση microchip τεχνολογίας RFID σε ανθρώπους:* Τα εμφυτεύσιμα microchips RFID τα οποία σχεδιάσθηκαν για τα ζώα έχουν αρχίσει να εμφυτεύονται και στους ανθρώπους. Η Υπηρεσία Τροφίμων & Φαρμάκων των ΗΠΑ (Food & Drug Administration) ενέκρινε, τον Οκτώβριο 2004, την εμφύτευση microchip σε ανθρώπους, έπειτα από αίτημα της εταιρείας VeriChip, η οποία ειδικεύεται στην κατασκευή εμφιτεύσιμων microchip. Τα microchips αυτά, που έχουν μήκος 11mm και μέγεθος κόκκου ρυζιού, εμφυτεύονται με ειδική σύριγγα στον λιπώδη ιστό στο χέρι του ανθρώπου. Επιχειρήσεις σε όλο τον κόσμο έχουν αρχίσει να εμφυτεύουν, εθελοντικά, microchip σε ανθρώπους. Μερικά παραδείγματα:
    - Εμφύτευση microchip στους θαμώνες νυκτερινών κέντρων στην Βαρκελώνη, και στο Ρότερνταμ για τον έλεγχο της τιμολόγησης και της πληρωμής του λογαριασμού.
    - Το 2004, ο γενικός εισαγγελέας του Μεξικού εισηγήθηκε την εμφύτευση microchip στους 180 υπαλλήλους του γραφείου του για να ελέγχεται η πρόσβασή τους στον χώρο φύλαξης εμπιστευτικών εγγράφων του αρχείου της Εισαγγελίας.
- Παρακολούθηση κρατουμένων σε φυλακές: Σε μερικές φυλακές των ΗΠΑ, καθιερώθηκε οι κρατούμενοι να φορούν στο χέρι τους ένα βραχιόλι τεχνολογίας RFID, το οποίο χρησιμοποιείται για την συνεχή παρακολούθηση και τον εντοπισμό τους σε πραγματικό χρόνο.

2.5.3. Απειλές από την τεχνολογία RFID

Σημαντικότερη απειλή είναι το γεγονός ότι οι πληροφορίες που βρίσκονται στα microchips RFID που είναι ενσωματωμένα στα βιομετρικά διαβατήρια (όπως θα δούμε παρακάτω) και τις νέου τύπου πιστωτικές κάρτες, μπορούν να υποκλαπούν πολύ εύκολα με ηλεκτρονικές διατάξεις, για την κατασκευή των οποίων υπάρχει πληθώρα πληροφοριών στο Διαδίκτυο. Επίσης, με παρόμοιες διατάξεις μπορεί να γίνει και κλωνοποίηση microchip RFID, όπως π.χ. αυτό που βρίσκεται στα ηλεκτρονικά κλειδιά αυτοκινήτων.

Άλλη απειλή είναι ο παράνομος εντοπισμός των ετικετών RFID, οι οποίες είναι ενσωματωμένες σε διάφορα προϊόντα όπως τρόφιμα, ρούχα, παπούτσια, προσωπικά είδη κ.λπ. Λύση στο πρόβλημα υπάρχει με την εφαρμογή της κρυπτογραφίας στο κανάλι επικοινωνίας των ετικετών RFID με τους αναγνώστες RFID. Η εφαρμογή όμως αυτή αυξάνει πολύ το κόστος παραγωγής των ετικετών.

2.5.3.1. Προβλήματα με την ασφάλεια

Σε όλες τις χώρες της Ε.Ε., αλλά και σε άλλες χώρες του κόσμου, έγινε υποχρεωτική η έκδοση βιομετρικών διαβατηρίων με σκοπό την αντιμετώπιση της τρομοκρατίας. Δημοσιογράφος της Guardian σε συνεργασία ειδικού στην ασφάλεια υπολογιστών και στην τεχνολογία RFID- κατάφερε σχετικά εύκολα να σπάσει τον κώδικα ασφαλείας του microchip

που είναι ενσωματωμένο στα βρετανικά βιομετρικά διαβατήρια, με αποτέλεσμα να υποκλέψει τα προσωπικά δεδομένα του κατόχου του (Guardian, 17-11-2006 [103]).

Σύμφωνα με ανταπόκριση του αμερικανικού τηλεοπτικού καναλιού (ABC News, 18-4-2007), με μια συσκευή αξίας 20 μόλις δολαρίων που μπορεί οποιοσδήποτε να αγοράσει από το διαδικτυακό ηλεκτρονικό κατάστημα e-bay, είναι δυνατή η υποκλοπή των πληροφοριών που είναι αποθηκευμένες στα βιομετρικά διαβατήρια και σε πιστωτικές κάρτες νέου τύπου, τεχνολογίας RFID [104].

Ένας απλός, αλλά περιορισμένος, τρόπος προστασίας των βιομετρικών διαβατηρίων και των πιστωτικών καρτών τεχνολογίας RFID είναι η φύλαξή τους σε ειδικά πορτοφόλια τα οποία περιέχουν κλωβό Faraday [104]. Το πρόβλημα όμως παραμένει την στιγμή που το διαβατήριο ή η κάρτα είναι έξω από το πορτοφόλι για να διαβαστεί από τον αναγνώστη.

Με τα προσωπικά δεδομένα τα οποία μπορούν να υποκλαπούν από ένα βιομετρικό διαβατήριο η μία πιστωτική κάρτα τεχνολογίας RFID είναι δυνατόν να διαπραχθεί το αδίκημα της πλαστοπροσωπίας (identity theft) («Πεμπτουσία», τεύχος 15, Νοέμβριος 2004).

2.5.3.2. Κίνημα αντιδράσεων

Στις ΗΠΑ, αμέσως μετά την έγκριση από την Υπηρεσία Τροφίμων & Φαρμάκων (Food & Drug Administration – FDA) χρησιμοποίησης της τεχνολογίας RFID για την εμφύτευση microchip σε ανθρώπους, υπήρξαν αντιδράσεις που είχαν ως αποτέλεσμα την δημιουργία κινήματος κατά αυτής της απόφασης. Ιδρυτές του κινήματος αυτού είναι οι Αμερικανίδες δικηγόροι, Katherine Albrecht και Liz McIntyre.

Η Katherine Albrecht και η Liz McIntyre ίδρυσαν στις ΗΠΑ το 1999 την CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering), μία εθνική οργάνωση καταναλωτών με σκοπό την προστασία τους από τις δυσμενείς επιπτώσεις της τεχνολογίας RFID. Επίσης είναι αυτές οι οποίες καθιέρωσαν για τις ετικέτες RFID τον όρο «Spy Chip» (τσιπ κατάσκοπος), ο οποίος πλέον χρησιμοποιείται από όλους τους πολέμιους της τεχνολογίας RFID. Σύμφωνα με την Katherine Albrecht: «Η παραβίαση της ιδωτικότητάς μας θα είναι αδύνατο να αποφευχθεί».

2.5.3.3. Απειλές για την ιδιωτικότητα

Ο μεγαλύτερος φόβος όλων όσοι αντιδρούν στην εμφύτευση microchip σε ανθρώπους είναι το γεγονός ότι κάποια στιγμή, αυταρχικές κυβερνήσεις ίσως κάνουν υποχρεωτικές τις εμφυτεύσεις αυτές με στόχο την συνεχή παρακολούθηση των πολιτών.

Αναλυτές της τεχνολογίας RFID δηλώνουν ότι δεν είναι μακριά η εποχή που η τεχνολογία RFID θα εφαρμοσθεί παγκοσμίως σε όλα τα προϊόντα που υπάρχουν στον κόσμο με την εφαρμογή του συστήματος EPC – Electronic Product Code (Ηλεκτρονικός Κωδικός Προϊόντος), το οποίο θα αντικαταστήσει το σύστημα UPC – Universal Product Code (Παγκόσμιος Κωδικός Προϊόντος) δηλαδή το σύστημα barcode. Με το σύστημα EPC το κάθε προϊόν θα έχει τον δικό του κωδικό αριθμό (unique ID code). Απώτερος σκοπός υλοποίησης των εφαρμογών της τεχνολογίας RFID είναι να δημιουργηθεί ένα παγκόσμιο

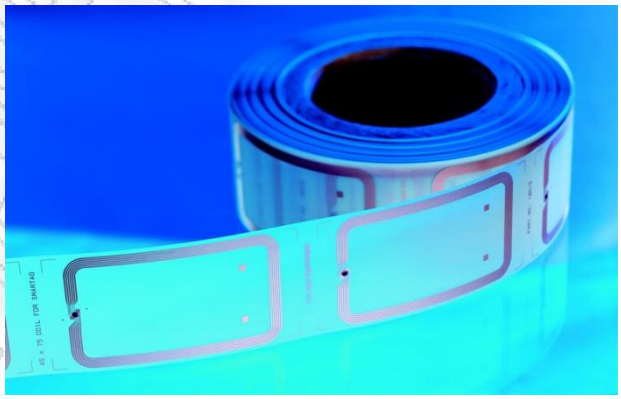
δίκτυο, στο οποίο θα είναι συνδεδεμένα όλα τα προϊόντα που κυκλοφορούν στις αγορές όλου του κόσμου. Οι καταναλωτές είναι πολύ επιφυλακτικοί την στιγμή που γνωρίζουν ότι οι πιστωτικές τους κάρτες μπορούν να «διαβαστούν» από συσκευές ανάγνωσης (RFID readers) χρησιμοποιούμενες από μη εξουσιοδοτημένα άτομα η και από κακοποιούς.

Είναι σαφές πάντως, ότι η ανάπτυξη της τεχνολογίας RFID δεν πρέπει να γίνει ανεξέλεγκτα, χωρίς νομικούς περιορισμούς και χωρίς βαθιά και αναλυτική μελέτη των επιπτώσεών της στα προσωπικά δεδομένα των πολιτών. Σε αντίθετη περίπτωση, είναι πιθανό καταστάσεις και σκηνές από το μυθιστόρημα του George Orwell «1984» να δούμε να πραγματοποιούνται στο άμεσο μέλλον.

2.5.3.4. Μέτρα προστασίας

Αν και υφίστανται οι παραπάνω φόβοι, υπάρχουν πολλά που μπορεί να γίνουν και να αποτρέψουν περιπτώσεις παραβίασης της ιδιωτικότητας:

- Στα καταστήματα θα πρέπει να υπάρχουν ευανάγνωστες επιγραφές, για ενημέρωση των καταναλωτών, στις οποίες θα αναγράφεται ποιά προϊόντα φέρουν ετικέτες RFID.
- Οι ετικέτες RFID οι οποίες είναι ενσωματωμένες στα διάφορα προϊόντα θα πρέπει να είναι αναγνώσιμες μόνο από αναγνώστες οι οποίοι λειτουργούν επίσημα στο κατάστημα για λόγους ασφαλείας η/και τιμολόγησης και για κανέναν άλλο λόγο.
- Στο ταμείο, αμέσως μετά την πληρωμή του προϊόντος, θα πρέπει να απενεργοποιείται αυτόματα η ετικέτα RFID.
- Θα πρέπει να απαγορεύεται αυστηρά η παρακολούθηση των πολιτών μέσω της τεχνολογίας RFID είτε άμεσα είτε έμμεσα μέσω διαφόρων προϊόντων και καταναλωτικών αγαθών.
- Να εφαρμοσθεί η λύση της κρυπτογραφίας για προσωπικά δεδομένα που μεταβιβάζονται με ραδιοσυχνότητες.



Εικόνα 14-Ετικέτες RFID

2.5.4. Κανονισμοί λειτουργίας και τυποποίηση RFID

Δεν υπάρχει διεθνής οργανισμός ο οποίος συντονίζει τα πρότυπα λειτουργίας των συσκευών RFID. Κάθε χώρα έχει τους δικούς της κανόνες λειτουργίας. Στην Ευρώπη η λειτουργία των συσκευών RFID ρυθμίζεται με τις συστάσεις EN 300 220, EN 302 208 και ERO 70 03 (http://en.wikipedia.org/wiki/Radio-frequency_identification). Τα σημαντικότερα πρότυπα σχετικά με την τεχνολογία RFID είναι:

- ISO 11784 και 11785: Αφορούν την ρύθμιση λειτουργίας των ραδιοσυχνοτήτων στην περίπτωση εμφύτευσης ετικετών RFID σε ζώα.
- ISO 14443: Το πρότυπο αυτό ρυθμίζει την λειτουργία του συστήματος RFID με το οποίο είναι εφοδιασμένα τα βιομετρικά διαβατήρια.

ISO 18000: Το πρότυπο της σειράς 18000 καλύπτει τις περισσότερες ζώνες συχνοτήτων που χρησιμοποιούν τα συστήματα RFID.

Ενώ υπάρχουν χρήσιμες εφαρμογές της τεχνολογίας RFID, κάποιες δυνατότητές της μπορούν να αποτελέσουν απειλή για την ιδιωτικότητα και τις ελευθερίες των πολιτών. Για το λόγο αυτό είμαστε κριτικοί και απολύτως επιφυλακτικοί για τη χρήση της τεχνολογίας RFID στην εφαρμογή της ΚΠ.

Υπάρχουν πολλά που πρέπει να γίνουν ακόμη όσον αφορά τα θέματα ασφάλειας που έχουν προκύψει στις διάφορες εφαρμογές της τεχνολογίας RFID και κυρίως σε ό,τι αφορά τα βιομετρικά διαβατήρια και τις πιστωτικές κάρτες. Εξάλλου, πρέπει να παρατηρήσουμε ότι δεν δίνει ιδιαίτερη προστιθέμενη αξία για τη χρήση μιας ΚΠ.

Οι Αρχές Προστασίας Προσωπικών Δεδομένων των διαφόρων χωρών θα πρέπει να μελετήσουν καλά τις επιπτώσεις από την χρήση της τεχνολογίας RFID και να δημιουργήσουν ένα πλαίσιο αρχών που θα έχει σαν γνώμονα την προστασία της ιδιωτικότητας, των προσωπικών δεδομένων και των πολιτικών ελευθεριών και το οποίο θα ρυθμίζει τις εφαρμογές της τεχνολογίας αυτής και θα συμβάλλει παράλληλα στην περαιτέρω ανάπτυξή της.

2.6. Πρότυπα της Έξυπνης Κάρτας

Σημαντική προϋπόθεση για την παγκόσμια διείσδυση των έξυπνων καρτών στην καθημερινότητά μας ήταν η δημιουργία εθνικών και διεθνών προτύπων. Κατά κύριο λόγο, η έξυπνη κάρτα διέπεται από τα πρότυπα, τις φυσικές ιδιότητες, τα χαρακτηριστικά επικοινωνίας, και τα αναγνωριστικά εφαρμογών του ενσωματωμένου τσιπ και των δεδομένων του.

Η διαλειτουργικότητα των καρτών ανοικτού συστήματος πρέπει να εφαρμόζεται στο επίπεδο της κάρτας, στα τερματικά πρόσβασης της κάρτας (αναγνώστες), στα δίκτυα και στους εκδότες καρτών.

Η αυξανόμενη χρήση των έξυπνων καρτών και η διείσδυση τους σε διάφορες εφαρμογές και επιχειρηματικά μοντέλα, έχει οδηγήσει στον ορισμό ανοικτών προτύπων που εγγυώνται τη διαλειτουργικότητα των σχετικών προϊόντων σε όλα τα επίπεδα, εντείνοντας την ανταγωνιστικότητα και τη συμβατότητα μεταξύ διαφορετικών κατασκευαστών.

Στο πλαίσιο αυτό, για τη διασφάλιση της διαλειτουργικότητας και της συμβατότητας των έξυπνων καρτών σε ένα διεθνές και πολυμορφικό περιβάλλον έχει καθιερωθεί από τον ένα σύνολο προτύπων (σειρές ISO/IEC 7816 , μέρος 1-14 και ISO/IEC 14443 για τις ανεπαφικές κάρτες, αλλά και ISO/IEC 15693 και ISO/IEC 7501), που προέρχονται κυρίως από πρότυπα ταυτοτήτων και απαριθμούν διεπαφή φυσικού, ηλεκτρικού, μηχανικού, και προγραμματισμού εφαρμογής.

Το ISO 7816 είναι ένα πολυμερές διεθνές πρότυπο για τις κάρτες ολοκληρωμένων κυκλωμάτων (κοινώς γνωστές ως έξυπνες κάρτες) που χρησιμοποιούν τις ηλεκτρικές επαφές της κάρτας, καθώς και για τις κάρτες που επικοινωνούν με τους αναγνώστες και τους τερματικούς σταθμούς χωρίς επαφές, όπως για παράδειγμα με τεχνολογία ραδιοσυχνοτήτων (RF / Contactless) και αποτελείται από 14 επιμέρους τμήματα. Τα 7816 μέρη 1, 2 και 3 αφορούν μόνο επαφικές έξυπνες κάρτες και προσδιορίζουν διάφορα χαρακτηριστικά των καρτών και των διεπαφών τους, συμπεριλαμβανομένων και των διαστάσεών τους, των ηλεκτρικών διεπαφών και των πρωτοκόλλων επικοινωνίας. Ενώ, τα μέρη 4, 5, 6, 8, 9, 11, 13 και 15 είναι αφορούν στο σύνολο των έξυπνων καρτών και καθορίζουν τη λογική δομή (αρχεία και στοιχεία μνήμης), τις εντολές εφαρμογών για βασικές χρήσεις, για διαχείριση εφαρμογών, για βιομετρικές επαληθεύσεις και για κρυπτογραφικές υπηρεσίες.

Ακολουθεί μια απαρίθμηση των προτύπων που εμπλέκονται στις προδιαγραφές των έξυπνων καρτών καθώς και αναλυτικότερες περιγραφές σε συγκεκριμένες προδιαγραφές ειδικού ενδιαφέροντος:

- ISO/IEC 14443
- ISO/IEC 15693
- ISO/IEC 7501 International Civil Aviation Organization (ICAO)
- Federal Information Processing Standards (FIPS)
- FIPS 140 (1-3)
- FIPS 201
- Europay, MasterCard, and Visa (EMV)
- PC/SC
- Comité Européen de Normalisation (CEN) and European Telecommunications Standards Institute (ETSI)

- The Health Insurance Portability and Accountability Act (HIPAA)
- IC Communications Standards
- Global System for Mobile Communication (GSM)
- OpenCardT Framework
- GlobalPlatform (GP)
- Common Criteria (CC)
- ANSI-INCITS 358-2002 (Biometric Standards)
- ANSI-INCITS 398 (Biometric Standards)
- ANSI-INCITS (Biometric Standards)
- ANSI-INCITS 377-2004 (Biometric Standards)
- ANSI-INCITS 378-2004 (Biometric Standards)
- ANSI-INCITS 379-2004 (Biometric Standards)
- ANSI-INCITS 381-2004 (Biometric Standards)
- ANSI-INCITS 385-2004 (Biometric Standards)
- ANSI-INCITS 395-2005 (Biometric Standards)
- ANSI-INCITS 396-2004(Biometric Standards)ISO/IEC 19794 (Biometric Standards)

2.6.1. Το Πρότυπο CEN 15480

Η Ευρωπαϊκή Επιτροπή Προτυποποίησης εργάζεται πάνω σε μια σειρά προτύπων CEN 15480 που αφορούν την Ευρωπαϊκή ΚΠ (European Citizen Card, ECC), ώστε να αρθούν τα εθνικά και ευρωπαϊκά εμπόδια και να εξασφαλισθούν οι απαιτήσεις παροχής ασφάλειας και διασυνοριακών υπηρεσιών στους Ευρωπαίους πολίτες. Το CEN 15480 αποτελεί περισσότερο ένα σύνολο εργαλείων που παρέχει ευελιξία επιλογών ως προς τα ζητήματα ταυτοποίησης και αυθεντικοποίησης ενώ παράλληλα, ορίζει ό,τι αφορά στις διεπαφές, τα προφίλ χρήσης, τη λογική δομή των δεδομένων και τους μηχανισμούς ασφάλειας και προστασίας της ιδιωτικότητας ώστε να προάγει τη διαλειτουργικότητα.

Το CEN/TS 15480 "Identification card systems — European Citizen Card" αποτελείται από τα ακόλουθα μέρη:

1. *Μέρος 1*: περιγράφονται τα φυσικά και ηλεκτρικά χαρακτηριστικά της ECC, ο μορφότυπος, τα πρωτόκολλα μεταφοράς για την επικοινωνία κάρτας — τερματικού

κλπ χωρίς να ορίζεται κάτι πέρα από τα ήδη υπάρχοντα πρότυπα όπως ISO7810, ISO7816, ISO14443 και τις ICAO συστάσεις για eMRTD τύπου ID-1.

2. Το *Μέρος 2*: ορίζει τις υπηρεσίες της ECC κάρτας που είναι υποχρεωτικές καθώς και άλλες ως προαιρετικές επεκτάσεις. Προσδιορίζει τη λογική δομή των δεδομένων της κάρτας και την αρχιτεκτονική του συστήματος αρχείων. Επιπλέον, ορίζει ένα κοινό σετ εντολών για την ECC ώστε να εξασφαλίζεται η διαλειτουργικότητα. Γίνεται μια διαφοροποίηση μεταξύ βασικών και εκτεταμένων υπηρεσιών ηλεκτρονικών καρτών. Στις αναφερόμενες ως εκτεταμένες υπηρεσίες υιοθετούνται οι μηχανισμοί ασφάλειας του ICAO και BSI [89] [86]. Οι ηλεκτρονικές υπηρεσίες για την ταυτοποίηση, αυθεντικοποίηση και τη δημιουργία υπογραφών (IAS services) βασίζονται κυρίως σε κρυπτογραφικές λειτουργίες δημοσίου κλειδιού και στον αλγόριθμο RSA. Ανάλογα με τον τύπο διεπαφής προσαρμόζονται και οι παραπάνω υπηρεσίες. Για παράδειγμα στο ανεπαφικό τσιπ ορίζονται επιπλέον μηχανισμοί για την προστασία της επικοινωνίας. Για λόγους διαλειτουργικότητας οι IAS υπηρεσίες είναι σε συμφωνία με τα πρότυπα [94] και [95]. Καθώς η ECC δύναται να υλοποιεί διαφορετικές πρωταρχικές εφαρμογές (πχ ID κάρτα ή κάρτα υγείας) έχουν αναπτυχθεί διαφορετικά προφίλ τα οποία ορίζονται στο ECC πρότυπο στο Μέρος 4.

3. Το *Μέρος 3*: περιγραφή του μοντέλου διαλειτουργικότητας για την υποστήριξη μιας συμβατής εφαρμογής σε Η/Υ ώστε να λειτουργεί αρμονικά με τις διαφορετικές υλοποιήσεις της ECC κάρτας. Πρόκειται για την περιγραφή ενός γενικού middleware που θα επιτρέπει την ασφαλή χρήση της ECC σε online συναλλαγές. Η middleware αρχιτεκτονική βασίζεται στο ISO/IEC 24727 με κάποια επιπρόσθετα στοιχεία. Το middleware ανεξάρτητα της EEC υλοποίησης και ανεξάρτητα του τύπου δι*επαφής του* τσιπ, είναι σε θέση να ανιχνεύσει τις δυνατότητες/υπηρεσίες της ECC κάρτας και να τις διαχειριστεί.

4. Στο *Μέρος 4*: Συστάσεις για διάφορα οργανωσιακά θέματα όπως είναι η έκδοση της κάρτας, η διαδικασία εγγραφής του πολίτη για κάρτα κα. Επιπλέον παρουσιάζονται ως σημείο αναφοράς, διάφορα προφίλ εφαρμογών που έχουν ήδη αναπτυχθεί, ενώ επιπλέον προφίλ θα προστίθενται από την ομάδα εργασίας ακόμη και μετά την δημοσίευσή του CEN/TS 15480-4.

5. *Μέρος 0*: «General Framework of the ECC Standard» είναι μη-τεχνικό και εξηγεί το ECC πλαίσιο ιδίως σε σχέση με τα υπόλοιπα μέρη του προτύπου και ενδεχόμενα και με τα υπόλοιπα ISOs. Αναμένεται να συμπεριλάβει λεπτομέρειες για τα χαρακτηριστικά προστασίας της ιδιωτικότητας που αφορούν το πρότυπο καθώς και μια πρακτική υλοποίηση του προτύπου.

Καθένα από *αυτά τα* προφίλ περιέχουν μία ή περισσότερες εφαρμογές που χρησιμοποιούν διεπαφές και πρωτόκολλα μεταφοράς που περιγράφονται στα μέρη 1 και 2 των προδιαγραφών. Για παράδειγμα το Προφίλ 1 είναι η κάρτα ID που χρησιμεύει ως έγγραφο ταυτότητας. Για κάθε προφίλ που ορίζεται με αυτό τον τρόπο παρέχεται το αντίστοιχο ξεχωριστό αναγνωριστικό του (OID) ώστε να δύναται να χρησιμοποιηθεί ως αναφορά για λόγους διαλειτουργικότητας, π.χ. να διευκολυνθεί η ανακάλυψη της κάρτας ή/και οι

δυνατότητες της εφαρμογής. Σε κάθε άλλη περίπτωση το middleware διενεργεί αυτόματο εντοπισμό των υπηρεσιών στην κάρτα (Global Profile) [22].

2.6.1.1. Αρχιτεκτονική CEN15480-3 και Card- Verifiable Certificates

Με αυτή την αρχιτεκτονική που ο Πάροχος Υπηρεσιών χρησιμοποιώντας «Card-Verifiable Certificates, CVCs» (σύμφωνα με το πρότυπο ISO 7816-8), αποδεικνύει στο τσιπ της ECC τα δικαιώματα πρόσβασης που του έχουν εκχωρηθεί από την αντίστοιχη έμπιστη αρχή, προκειμένου να πραγματοποιηθούν οι σχετικοί μηχανισμοί αυθεντικοποίησης και ελέγχου πρόσβασης στα δεδομένα του τσιπ.

Τα CVC πιστοποιητικά χρησιμεύουν και στη μεταφορά δημόσιων κλειδιών. Ένα CVC πιστοποιητικό είναι υπογεγραμμένο με το ιδιωτικό κλειδί της έμπιστης αρχής CA. Το αντίστοιχο δημόσιο CA κλειδί, τηρείται στην ECC και έτσι η κάρτα δύναται να ελέγξει την αυθεντικότητα του πιστοποιητικού που προσκομίζεται από τον πάροχο. Έτσι μπορεί να «εμπιστευθεί» το δημόσιο κλειδί του παρόχου που του παραδόθηκε και να το αποθηκεύσει εσωτερικά στην ECC μνήμη.

2.6.1.2. Προφίλ

- **Προφίλ eID**: Η εφαρμογή αυτή υλοποιεί τις υπηρεσίες ηλεκτρονικών καρτών ταυτότητας και των σχετικών δομών δεδομένων. Τα στοιχεία του κατόχου της κάρτας (που αντιστοιχούν στα δεδομένα των συμβατικών εγγράφων ταυτότητας) αποθηκεύονται σε ξεχωριστές ομάδες δεδομένων. Το προφίλ περιέχει υποχρεωτικά μία μοναδική ανεπαφική διεπαφή σύμφωνα με το ISO/IEC 14443 η οποία πρέπει να είναι σε θέση να υποστηρίξει:
    - MRTD εφαρμογή σε συμμόρφωση με τις προδιαγραφές του ICAO, συγκρίσιμη με το e-passport, με υποχρεωτική εφαρμογή μηχανισμών Passive Authentication, BAC, EAC με Chip & Terminal Authentication και Secure Messaging.
    - Εφαρμογή ψηφιακών υπογραφών σύμφωνα με το πρότυπο EN 14890 [94] [95], που περιέχει την υπηρεσία υπογραφών εντός της κάρτας με δυνατότητα εγκατάσταση πιστοποιητικών ή κλειδιών κατά την έκδοση ή την προσωποποίηση της κάρτας (personalization).
- **Προφίλ eID (IAS)**: Η βασική του διαφορά είναι ότι έχει υιοθετήσει τεχνικές επιλογές της ECC και επιτρέπει πλήρη διαλειτουργικότητα μεταξύ διαφορετικών κατασκευαστώ. Η αρχιτεκτονική του μπορεί να αναβαθμιστεί για να ενσωματώσει νέες λειτουργίες ή τεχνικές ασφάλειας. Υλοποιεί την προηγούμενη έκδοση του μηχανισμού EAC και ανεπαφική ή υβριδική διεπαφή. Το προφίλ αυτό IAS-ECC επελέγη πρόσφατα από τη Γαλλία για την υλοποίηση της Εθνικής της ΚΠ η οποία θα είναι συμβατή με την ECC, για τη δυνατότητά του να αξιοποιήσει τις υφιστάμενες υποδομές και υπηρεσίες (PKI υποδομή, ηλεκτρονική κάρτα υγείας, ePassport) [11], [22].

2.6.1.3. Σύστημα Αρχείων και Αναγνωριστικό του Τσιπ

Το σύστημα αρχείων καθορίζεται από το πρότυπο ISO/IEC 7816-4, αφού αναφερόμαστε ουσιαστικά σε υποδομή έξυπνης κάρτας και ορίζει τους τύπους MF (Master File, προαιρετικό), DF (Dedicated Files) και EF (ElementaryFiles). Το personalization της ECC κάρτας λαμβάνει χώρα στο υποχρεωτικό αρχείο EF.DIR που βρίσκεται ακριβώς κάτω της ρίζας (με αναγνωριστικό '2F00' και σύντομο αναγνωριστικό "30"). Επίσης στο EF.DIR περιλαμβάνεται λίστα των εφαρμογών που περιέχει η κάρτα δηλ. λίστα των ADF (Application Dedicated Files).

Οι βασικοί μηχανισμοί της ECC είναι το πρωτόκολλο αμοιβαίας αυθεντικοποίησης τσιπ-αναγνώστη με χρήση συμμετρικής ή ασύμμετρης κρυπτογραφίας. Για το λόγο αυτό η ECC ενσωματώνει ένα μοναδικό αναγνωριστικό τον αριθμό PAN (Primary Account Number). Ο PAN αποθηκεύεται στο αρχείο EF.SN κάτω από τη ρίζα. Τα λιγότερο σημαντικά ψηφία του αριθμού αυτού (8 Bytes) αποτελούν το σειριακό αριθμό του τσιπ SN.ICC που χρησιμοποιείται στα πρωτόκολλα αυθεντικοποίησης ως αναγνωριστικό του τσιπ.

Κατά το CEN, η αυθεντικοποίηση πρέπει να είναι αμοιβαία και να περιλαμβάνει δύο μηχανισμούς, σύμφωνα με την παρακάτω διαδικασία:

- Το ICC επιβεβαιώνει τον εξωτερικό κόσμο και αντίστροφα ο εξωτερικός κόσμος επιβεβαιώνει το ICC,
- Τα δύο μέρη που επικοινωνούν ανταλλάσουν ή συμφωνούν σε πληροφορίες, που θα επιτρέψουν τη μετέπειτα εγκαθίδρυση κοινών κλειδιών συνόδου (με βάση τα κλειδιά συνόδου, μπορεί να θωρακιστούν οι μετέπειτα επικοινωνίες με Secure Messaging).

Όσον αφορά τους μηχανισμούς αυθεντικοποίησης της συσκευής γίνεται παραπομπή στο πρότυπο EN 14890-1. Για λόγους απόδοσης (ταχύτητας) τα κλειδιά του Secure Messaging είναι συμμετρικά. Τέλος, στο ECC πρότυπο ορίζεται ως υποχρεωτική η υποστήριξη της συμμετρικής αυθεντικοποίησης.

2.7. Σύνοψη Κεφαλαίου

Στο κεφάλαιο αυτό παρουσιάσθηκαν οι σημαντικότερες τεχνολογίες που εφαρμόζονται σε λύσεις ηλεκτρονικής ταυτοποίησης. Στην κατεύθυνση αυτή αναλύσαμε αρκετά επαρκώς τις την τεχνολογία των έξυπνων καρτών, τα χαρακτηριστικά τα είδη, τα οφέλη και τις αδυναμίες αυτών, καθώς η ΚΠ είναι στην πραγματικότητα μια έξυπνη κάρτα. Επιπλέον, εξετάσθηκε η εισαγωγή βιομετρικών χαρακτηριστικών σε εφαρμογές ΚΠ, προκειμένου να διαπιστωθεί η σκοπιμότητα, αλλά και η αναγκαιότητα εισαγωγής τους στην προτεινόμενη Ελληνική ΚΠ. Από την ανάλυση αυτή, δεν φάνηκε να προκύπτουν ιδιαίτερα σημαντικοί λόγοι που θα έκαναν επιτακτική τη χρήση τους, αλλά περισσότεροι κίνδυνοι και αναδυόμενες απειλές από την ενσωμάτωσής τους στην ΚΠ. Επίσης, για λόγους πληρότητας, αναφέρθηκε η τεχνολογία RFID, για την οποία ωστόσο η κατεύθυνση ήταν ξεκάθαρη ως προς την μη εφαρμογή της σε εφαρμογές εθνικής ΚΠ. Τέλος, παρουσιάσθηκαν τα πρότυπα,

με τα οποία οφείλουν να συμμορφώνονται οι έξυπνες κάρτες και οι ΚΠ, προκειμένου να διασφαλίζουν κοινές προδιαγραφές μεταξύ των επιμέρους λύσεων και ελάχιστες προϋποθέσεις για διαλειτουργικότητα, ασφάλεια και χρηστικότητα. Στο πλαίσιο αυτό, έγινε ιδιαίτερη αναφορά στο πρότυπο CEN 15480, που προδιαγράφει την Ευρωπαϊκή ΚΠ και το οποίο θα είναι ιδιαίτερα χρήσιμο για τις προδιαγραφές της Ελληνικής ΚΠ.

3. ΝΟΜΙΚΟ ΚΑΙ ΚΑΝΟΝΙΣΤΙΚΟ ΠΛΑΙΣΙΟ

Στο κεφάλαιο αυτό περιλαμβάνεται μία επισκόπηση της βασικής Ευρωπαϊκής και Εθνικής Νομοθεσίας, όπως αυτή ισχύει σήμερα καθορίζοντας το νομικό πλαίσιο της ηλεκτρονικής διακυβέρνησης και ηλεκτρονικής αυθεντικοποίησης. Επιπλέον, γίνεται μια προσπάθεια ανάλυσης του κανονιστικού πλαισίου και ερμηνείας αυτού υπό το πρίσμα της εφαρμογής της ΚΠ τόσο στην Εθνική και Κοινοτική Νομοθεσία, όσο και στη Δημόσια Διοίκηση, καθώς και επεξεργασίας των κατευθύνσεων που έχουν ακολουθήσει τα κράτη μέλη της Ευρωπαϊκής Ένωσης.

Σχετικά με το θεσμικό πλαίσιο ταυτοποίησης των πολιτών, η Ευρωπαϊκή Νομοθεσία υιοθετεί στους Κανονισμούς που αφορούν διαβατήρια/ταξιδιωτικά έγγραφα [26], [27] και άδειες διαμονής για υπηκόους τρίτων χωρών [24], [25] σύμφωνα με τις συστάσεις του ICAO [65].

Εξαιτίας της παγκόσμιας φύσης των ηλεκτρονικών επικοινωνιών, είναι αναγκαίος ο συντονισμός των εθνικών κανονιστικών μέτρων σε ευρωπαϊκό επίπεδο, στον άξονα δημιουργίας ενός ενιαίου ευρωπαϊκού κανονιστικού πλαισίου, ώστε να αποφευχθεί η κατάτμηση της εσωτερικής αγοράς. Ωστόσο, τα κράτη-μέλη φαίνεται να έχουν σημαντικά διαφορετικές προσεγγίσεις σχετικά με τη διαχείριση των ηλεκτρονικών ταυτοτήτων, οι οποίες ποικίλουν από την ολοκληρωτική αποδεικτική ικανότητα των ηλεκτρονικών υπογραφών, τη χρήση εξειδικευμένων υποδομών αυθεντικοποίησης PKI, την αξιοποίηση των συστημάτων PKI μέσω κινητών τηλεφώνων, συστήματα αυθεντικοποίησης δύο παραγόντων, και απλά συστήματα αυθεντικοποίησης (όνομα χρήστη/κωδικός πρόσβασης).

Κεντρικό ζήτημα σε όλα τα ερωτήματα περί αυθεντικοποίησης, είτε σε εθνικό είτε σε διασυνοριακό επίπεδο αποτελεί η ασφάλεια και ιδιωτικότητα των πολιτών. Έτσι, η κατεύθυνση που φαίνεται να υπάρχει είναι προς την εξασφάλιση σαφών όρων και προϋποθέσεων σχετικά με την επεξεργασία και προσπελασιμότητα των προσωπικών δεδομένων, με τρόπο τέτοιο που να περιορίζονται όσο το δυνατόν περισσότερο οι κίνδυνοι που απορρέουν από την αυξημένη πρόσβαση σε προσωπικά δεδομένα, μέσω των συστημάτων αυθεντικοποίησης.

Για κάθε ένα από τα νομοθετικά κείμενα που σχετίζονται άμεσα ή έμμεσα με την εφαρμογή της ΚΠ στην Ελλάδα, θα εξεταστούν οι βασικές αρχές, καθώς και η εφαρμοσιμότητά τους σε θέματα διαχείρισης ηλεκτρονικών ταυτοτήτων.

3.1. Ηλεκτρονική Διακυβέρνηση

ΝΟΜΟΣ ΥΠ' ΑΡΙΘ. 3979/2011 (ΦΕΚ Α' 138) Για την ηλεκτρονική διακυβέρνηση και λοιπές διατάξεις [33]

Ο νόμος για την ηλεκτρονική διακυβέρνηση αποτελεί το θεσμικό πλαίσιο με το οποίο θα οργανωθεί και θα απλοποιηθεί η σχέση της δημόσιας διοίκησης με τους πολίτες και τις επιχειρήσεις χρησιμοποιώντας τις τεχνολογίες πληροφορικής και επικοινωνιών (ΤΠΕ). Στην κατεύθυνση αυτή, ο νόμος προδιαγράφει τις προϋποθέσεις για την υλοποίηση ενός πλαισίου για την παροχή ηλεκτρονικών υπηρεσιών με εμπλεκόμενους τους φορείς της Δημόσιας Διοίκησης, τους Πολίτες και τις Επιχειρήσεις.

Με γνώμονα την εξυπηρέτηση και διευκόλυνση των πολιτών (φυσικό ή νομικό πρόσωπο) μέσα από τη χρήση ηλεκτρονικών υπηρεσιών και υπό την προϋπόθεση της απλούστευσης των διαδικασιών που θα επιφέρει δραστική μείωση των διοικητικών επιβαρύνσεων που υφίστανται πολίτες και επιχειρήσεις κατά τις συναλλαγές τους με φορείς του δημόσιου τομέα και των γραφειοκρατικών φαινομένων, αλλά και την εδραίωση σχέσεων εμπιστοσύνης ανάμεσα σε πολίτες, επιχειρήσεις και φορείς του δημόσιου τομέα, ο νόμος στοχεύει σε ποιοτικότερες, ασφαλέστερες, ταχύτερες και πιο ευέλικτες υπηρεσίες. Εισάγεται πλήθος καινοτομιών, όπως:

α) έκδοση ηλεκτρονικών διοικητικών πράξεων με παράλληλη κατοχύρωση των προϋποθέσεων για τη νομική και αποδεικτική ισχύ των ηλεκτρονικών εγγράφων,

β) αυτεπάγγελτη ή κατ' αίτηση αναζήτηση εγγράφων που τηρούνται σε οποιοδήποτε φορέα του δημόσιου τομέα, απαλλάσσοντας τον πολίτη ή τις επιχειρήσεις από την επιβάρυνση για επικύρωση αντιγράφων για κάθε συναλλαγή τους με τη Διοίκηση,

γ) καθιέρωση της δυνατότητας ηλεκτρονικών συναλλαγών, συμπεριλαμβανομένων και των ηλεκτρονικών οικονομικών συναλλαγών και πληρωμών με φορείς του δημόσιου τομέα.

Στο πλαίσιο, αυτό, ιδιαίτερη έμφαση μέσα από τις διατάξεις του νόμου δίδεται:

- Στην ηλεκτρονική επικοινωνία και ανταλλαγή δεδομένων μεταξύ φυσικών/νομικών προσώπων και των δημόσιων φορέων, τόσο με τη διάσταση της ενδοδιοικητικής επικοινωνίας, διακίνησης εγγράφων και διεκπεραίωσης διοικητικών πράξεων, όσο και με της παραγωγής ηλεκτρονικών διοικητικών πράξεων και εγγράφων. Στο πλαίσιο αυτό, δημιουργείται το θεσμικό πλαίσιο για την παροχή ηλεκτρονικών υπηρεσιών από τη δημόσια διοίκηση και την ηλεκτρονική διακίνηση εγγράφων, το ηλεκτρονικό πρωτόκολλο μέσω του οποίου ο πολίτης θα μπορεί να παρακολουθεί διαδικτυακά την πορεία της υπόθεσης, να υποβάλει ηλεκτρονικά αιτήσεις, δηλώσεις, δικαιολογητικών, να διεκπεραιώνει υποθέσεις ηλεκτρονικά και να επικοινωνεί αντίστοιχα με τους φορείς του Δημοσίου. Η σημασία πέραν της θεσμοθέτησης των υπηρεσιών ηλεκτρονικής διακυβέρνησης έρχεται μέσω της πρόβλεψης για τη νομική και αποδεικτική ισχύ ηλεκτρονικών εγγράφων.
- Στη δημόσια πληροφορία του δημόσιου τομέα και στον τρόπο που αυτή πρέπει να γίνεται αντικείμενο επεξεργασίας προκειμένου να είναι χρήσιμη και αξιοποιήσιμη για να διευκολύνει πολίτες και επιχειρήσεις και σε θέματα ανοικτής πρόσβασης σε δημόσια δεδομένα. «Οι φορείς του δημόσιου τομέα μεριμνούν για την εγκυρότητα, νομιμότητα, ακεραιότητα, ακρίβεια και επικαιροποίηση των πληροφοριών στις οποίες τα συναλλασσόμενα με τον φορέα φυσικά πρόσωπα ή Ν.Π.Ι.Δ. έχουν

πρόσβαση με χρήση ΤΠΕ.» σύμφωνα με το άρθρο 4 του νόμου. Επιπλέον, σύμφωνα με το άρθρο 5, οι δικτυακοί τόποι όλων των φορέων του δημοσίου τομέα αποτελούν πλέον οργανικό τμήμα της δομής του φορέα που οφείλει να ενημερώνεται καθημερινά. Στη συνέχεια στο άρθρο 7 ορίζονται οι πληροφοριακές υποχρεώσεις των φορέων του δημόσιου τομέα. Εισάγεται μάλιστα, η υποχρέωση των φορέων να διατηρούν μητρώα στα οποία καταγράφουν το σύνολο των υποδομών τους και ηλεκτρονικά αρχεία. Με τον τρόπο αυτό, επιτυγχάνεται για τον πολίτη πρόσβαση σε οργανωμένη και δομημένη πληροφορία μέσω των δικτυακών τόπων, ενώ θεσμοθετείται ακόμη κι η δυνατότητα ηλεκτρονικής εγγραφής για πρόσβαση σε υπηρεσίες που παρέχονται από φορείς του δημόσιου τομέα και βεβαίως, η ελεύθερη διάθεση δημόσιων δεδομένων.

- Σε θέματα όπως οι ηλεκτρονικές πληρωμές (Πλαίσιο για τις Ηλεκτρονικές Πληρωμές) και η αυτεπάγγελτη αναζήτηση αρχείων και εγγράφων κ.α..
- Σε ζητήματα προστασίας προσωπικών δεδομένων και προστασίας της ιδιωτικότητας του πολίτη.

Ενδιαφέροντες ορισμοί στα πλαίσια του νόμου για την ηλεκτρονική διακυβέρνηση είναι οι ακόλουθοι:

- Επιβεβαίωση ταυτότητας (αυθεντικοποίηση): η διαδικασία πιστοποίησης και επιβεβαίωσης της ταυτότητας των φυσικών και νομικών προσώπων, τα οποία είναι χρήστες υπηρεσιών ηλεκτρονικής διακυβέρνησης και επικοινωνούν – συναλλάσσονται με φορείς του δημόσιου τομέα με χρήση ΤΠΕ, που βασίζεται στα διαπιστευτήρια που κατέχουν και με την οποία αναγνωρίζεται και επιβεβαιώνεται η ορθότητα της ταυτότητας ενός προσώπου.
- Ηλεκτρονική υπογραφή: δεδομένα σε ηλεκτρονική μορφή, τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με αυτά και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας.
- Πιστοποιητικό: ηλεκτρονική βεβαίωση, η οποία συνδέει δεδομένα επαλήθευσης υπογραφής με ένα άτομο και επιβεβαιώνει την ταυτότητά του.
- Προηγμένη ηλεκτρονική υπογραφή: ηλεκτρονική υπογραφή, που πληροί τους εξής όρους:
  i. συνδέεται μονοσήμαντα με τον υπογράφοντα,
  ii. είναι ικανή να καθορίσει ειδικά και αποκλειστικά την ταυτότητα του υπογράφοντος,
  iii. δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο και
  iv. συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο τέτοιο ώστε να μπορεί να εντοπισθεί οποιαδήποτε μεταγενέστερη αλλοίωση των εν λόγω δεδομένων.

- Ταυτοποίηση: οποιαδήποτε μέθοδος που χρησιμοποιεί το πρόσωπο που είναι χρήστης υπηρεσιών ηλεκτρονικής διακυβέρνησης για τη δήλωση και αναγνώριση

της ταυτότητάς του αναφορικά με την πρόσβαση σε μια ηλεκτρονική υπηρεσία και η οποία βασίζεται στο αναγνωριστικό που κατέχει.

3.2.1. Δικαιώματα φυσικών και νομικών προσώπων για ηλεκτρονικές συναλλαγές

Ο νόμος αναγνωρίζει το δικαίωμα φυσικών και Νομικών Προσώπων Ιδιωτικού Δικαίου (πολιτών και επιχειρήσεων) να συναλλάσσονται ηλεκτρονικά με φορείς του δημόσιου τομέα και τα δικαιώματα περί ασφάλειας και ιδιωτικότητας.

Ιδιαίτερα αναφορικά με την προστασία των δεδομένων προσωπικού χαρακτήρα δίνεται ιδιαίτερη μέριμνα, όπως παρουσιάζεται στο άρθρο 7 του νόμου, με διατάξεις και ρυθμίσεις που θα μπορούσαν να χαρακτηρισθούν καινοτόμες σε ευρωπαϊκό ακόμη επίπεδο. Στην κατεύθυνση αυτή, εισάγεται η αξιολόγηση των επιπτώσεων (privacy impact assessment) και κινδύνων που σχετίζονται με την ιδιωτικότητα και την προστασία δεδομένων προσωπικού χαρακτήρα κατά τον σχεδιασμό, διαμόρφωση και προμήθεια πληροφοριακών συστημάτων και υπηρεσιών ηλεκτρονικής διακυβέρνησης, με ταυτόχρονη μέριμνα για την όσο το δυνατών ελάχιστη επεξεργασία προσωπικών δεδομένων, λαμβάνοντας υπόψη τη – συνταγματική και νομοθετική – επιταγή για προστασία προσωπικών δεδομένων (privacy by design).

Ειδικότερα δε, αναφορικά με τα δικαιώματα των προσώπων σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς ηλεκτρονικής διακυβέρνησης, όπως ορίζεται στο άρθρο 8, τα πρόσωπα μπορούν να επιλέξουν την επαναχρησιμοποίηση των προσωπικών δεδομένων που έχουν ήδη γνωστοποιήσει σε φορείς του δημόσιου τομέα για μελλοντικές, ηλεκτρονικές ή μη, συναλλαγές με αυτούς, υπό την προϋπόθεση της ενημερωμένης συγκατάθεσής τους(Informed consent). Η περαιτέρω χρήση δεδομένων προσωπικού χαρακτήρα για στατιστικούς λόγους ή για τη βελτίωση των παρεχόμενων υπηρεσιών είναι ωστόσο εφικτή είτε επί τη βάση της ανωνυμοποίησης, είτε, εφόσον τα δεδομένα δεν ανωνυμοποιούνται, επί τη βάση της έγγραφης συγκατάθεσης των φυσικών προσώπων ή των νομίμων εκπροσώπων τους.

Ο νόμος όμως προχωράει και σε διοικητικές ρυθμίσεις για την εξασφάλιση της συμμόρφωσης των φορέων του δημόσιου τομέα στις επιταγές της προστασίας προσωπικών δεδομένων μέσω του άρθρου 36, όπου προβλέπεται ο ορισμός εσωτερικού υπεύθυνου προστασίας δεδομένων προσωπικού χαρακτήρα, με καθήκον τη μέριμνα για τη λήψη όλων των αναγκαίων τεχνικών και οργανωτικών μέτρων για την τήρηση των αρχών και των υποχρεώσεων που περιγράφονται στον νόμο για την ηλεκτρονική διακυβέρνηση και στον Ν.2472/97, στην αντίστοιχη Γενική Διεύθυνση Ηλεκτρονικής Διακυβέρνησης σε κάθε Υπουργείου. Μέχρι τη σύσταση των Γενικών Διευθύνσεων, ο εκπρόσωπος αυτός θα συμμετέχει στην ομάδας διοίκησης έργου(ΟΔΕ). Με την θέσπιση του εσωτερικού υπεύθυνου προστασίας δεδομένων προσωπικού χαρακτήρα εισάγεται η αρχή της λογοδοσίας (accountability) που συγκαταλέγεται στις βασικές επιλογές του υπό αναθεώρηση κοινοτικού πλαισίου για την προστασία προσωπικών δεδομένων.

Σχετικά με τα δικαιώματα πρόσβασης στην πληροφορία του δημόσιου τομέα και ηλεκτρονικής επικοινωνίας, ο νόμος αντιμετωπίζει τον δικτυακό τόπο των φορέων ως οργανικό τμήμα της λειτουργίας της Δημόσιας Διοίκησης μέσω του οποίου οι φορείς οφείλουν να παρέχουν χρήσιμη πληροφορία προς τους πολίτες και τις επιχειρήσεις. Στα πλαίσια του νόμου δίνεται ιδιαίτερη σημασία στην ελεύθερη και χωρίς περιορισμούς πρόσβαση στους δικτυακούς τόπους και ελεύθερη χρήση των παρεχόμενων πληροφοριών, στη δυνατότητα επικοινωνίας με τον φορέα(υποβολή ερωτημάτων, ηλεκτρονική διεύθυνση επικοινωνία), στη σχετική νομοθεσία που διέπει τη λειτουργία τους καθιστώντας προσιτή την πρόσβαση σε αυτή αλλά και σε κάθε άλλη πληροφορία που διευκολύνει την άσκηση δικαιωμάτων και υποχρεώσεων, στη διευκόλυνση πολιτών και επιχειρήσεων. Για την ακρίβεια, την ορθότητα και την πληρότητα της πληροφορίας, οι φορείς εγγυώνται την εγκυρότητα και νομιμότητα και μεριμνούν για την ποιότητα και επικαιροποίηση των πληροφοριών που διαθέτουν ώστε να γνωρίζει ο πολίτης με βεβαιότητα την εγκυρότητα της πληροφορίας που λαμβάνει.

3.2.2. Ηλεκτρονικές διοικητικές πράξεις και Ηλεκτρονικά δημόσια έγγραφα

Ο νόμος εισάγει κι οργανώνει το πλαίσιο για την έκδοση διοικητικών πράξεων, τη σύνταξη, επεξεργασία και τήρηση εγγράφων και τη διακίνηση, διαβίβαση, κοινοποίηση και ανακοίνωση αυτών μεταξύ φορέων του δημόσιου τομέα ή μεταξύ αυτών και των φυσικών προσώπων και Ν.Π.Ι.Δ. με χρήση ΤΠΕ (άρθρο 12). Επιπλέον, εισάγεται η υποχρέωση τήρησης ηλεκτρονικών αρχείων για κάθε φορέα του δημόσιου τομέα (άρθρο 15) και της δημιουργίας και επικύρωσης επιμέρους αρχείων για την ταχύτερη διεκπεραίωση της εκάστοτε διαδικασίας ή υπόθεσης και τη βέλτιστη λειτουργία των φορέων. Στα πλαίσια της καλύτερης εξυπηρέτησης του πολίτη και του περιορισμού της γραφειοκρατίας ορίζεται επίσης η ισχύς ενός αντιγράφου χωρίς να απαιτείται επικύρωσή του, εφόσον το έγγραφο έχει παραχθεί από φορέα του δημόσιου τομέα και τηρείται από αυτόν ή άλλον φορέα και είναι δυνατή η επιβεβαίωση της ακρίβειας και ισχύος τους με χρήση ΤΠΕ.

Τα φυσικά πρόσωπα και Ν.Π.Ι.Δ. δια των νομίμων εκπροσώπων τους, δύναται να συναλλάσσονται ηλεκτρονικά με τους φορείς του δημόσιου τομέα αξιοποιώντας τις υπηρεσίες ηλεκτρονικής διακυβέρνησης (ηλεκτρονική υποβολή αιτήσεων, βεβαιώσεων, δικαιολογητικών, προσφορών και λοιπών νομιμοποιητικών εγγράφων, εφόσον πληρούνται οι κατά περίπτωση προϋποθέσεις που αφορούν στην παροχή των αναγνωριστικών και διαπιστευτηρίων, της ταυτοποίησης και της επιβεβαίωσης της ταυτότητας (αυθεντικοποίησης) και της πολιτικής ασφάλειας του εκάστοτε φορέα (άρθρο 23). Μάλιστα, στις περιπτώσεις που σχετικά έγγραφα τηρούνται ήδη σε ηλεκτρονικό ή μη αρχείο φορέα του δημοσίου, ο νόμος προβλέπει την αυτεπάγγελτη αναζήτησή τους από τον τον φορέα στον οποίο απευθύνονται. Ο πολίτης μπορεί να αιτηθεί την αναζήτηση αυτών των εγγράφων βεβαιώνοντας με υπεύθυνη δήλωση την ακρίβεια των στοιχείων που περιλαμβάνονται σε αυτά.

Σχετικά με τις ηλεκτρονικές πληρωμές, προβλέπεται η δυνατότητα ανεξάρτητα από την ιδιότητα του συναλλασσομένου (δικαιούχος ή οφειλέτης) και εξασφαλίζεται ότι υπό τις

προϋποθέσεις ταυτοποίησης και επιβεβαίωσης της ταυτότητάς του (αυθεντικοποίησης) η διεκπεραίωση μπορεί να γίνεται απευθείας από τον ίδιο και με εναλλακτικούς τρόπους (ΚΕΠ, Ενιαία Κέντρα Εξυπηρέτησης, ΕΛΤΑ), για τη διευκόλυνση των συναλλαγών.

Η σημαντικότερη όμως διάταξη που προκύπτει σχετικά με την αντιμετώπιση των ηλεκτρονικών εγγράφων αφορά στο κύρος και την αποδεικτική ισχύ των ηλεκτρονικά παραγόμενων και διακινούμενων εγγράφων. Εξασφαλίζεται δηλαδή η εξίσωση της νομικής και αποδεικτικής ισχύος των ηλεκτρονικών εγγράφων που φέρουν προηγμένη ψηφιακή υπογραφή εξουσιοδοτημένου οργάνου που βασίζεται σε αναγνωρισμένο πιστοποιητικό με εκείνα που φέρουν ιδιόχειρη υπογραφή και σφραγίδα (άρθρο 13). Επιπλέον μέσω της χρονοσήμανσης που θα φέρουν τα ηλεκτρονικά έγγραφα θα μπορεί να επιβεβαιώνεται η προέλευσή τους.

Η ηλεκτρονική επικοινωνία μεταξύ φορέων του δημόσιου τομέα και φυσικών προσώπων ή Ν.Π.Ι.Δ., με την επιφύλαξη ειδικών ρυθμίσεων που καθιστούν υποχρεωτική τη χρήση ΤΠΕ για την επικοινωνία και τη συναλλαγή με φορέα του δημόσιου τομέα, πραγματοποιείται ύστερα από σχετικό αίτημα των εν λόγω προσώπων ή μετά από την παροχή ρητής συγκατάθεσή τους. (Άρθρο 21). Τόσο η ίδια αίτηση ή παροχή συγκατάθεσης όσο και η τυχόν ανάκλησή τους μπορούν να διαβιβαστούν και με ηλεκτρονικό τρόπο, υπό την προϋπόθεση ότι τηρούνται οι ρυθμίσεις για την ταυτοποίηση και επιβεβαίωση της ταυτότητας (αυθεντικοποίηση) ώστε να είναι προκύπτει με ασφάλεια η ταυτότητα του υποβάλλοντος την αίτηση, συγκατάθεση ή ανάκληση. Σημειώνεται επίσης ότι οι φορείς του δημόσιου τομέα επικοινωνούν και συναλλάσσονται με φυσικά πρόσωπα και Ν.Π.Ι.Δ. και παρέχουν υπηρεσίες ηλεκτρονικής διακυβέρνησης τηρώντας τις προϋποθέσεις και τους όρους ασφάλειας που περιέχονται στο Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης (άρθρο 27 ν. 3731/2008) ή στην πολιτική ασφάλειας του εκάστοτε φορέα του δημόσιου τομέα.

Για την πληρότητα της ανάλυσης της θεσμοθέτησης της ηλεκτρονικής επικοινωνίας με τη δημόσια διοίκηση είναι σημαντικό να αναφέρουμε τη συνταγματική κατοχύρωσή της το 2001, αλλά και άλλες νομοθετικές ρυθμίσεις που ρυθμίζουν την διακίνηση εγγράφων με ηλεκτρονικά μέσα, την κατοχύρωση της για διοικητικούς σκοπούς ηλεκτρονικής επικοινωνίας, τις ηλεκτρονικές διοικητικές συναλλαγές, όπως επίσης και την ενσωμάτωση κοινοτικών οδηγιών. Ειδικότερα, το Π.Δ. 150/2001 [34] ενσωμάτωσε την Οδηγία 1999/93/ΕΚ "Σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές" [41] και σύμφωνα με το οποίο κατοχυρώνεται η νομική ισχύς της προηγμένης ηλεκτρονικής υπογραφής , θεσπίζοντας έτσι έναν καθόλα νόμιμο και ισότιμο με τον παραδοσιακό τρόπο νομικής δέσμευσης των μερών που συναλλάσσονται ηλεκτρονικά.

Στην κατεύθυνση λοιπόν ορισμού ενός ολοκληρωμένου θεσμικού πλαισίου για την επικοινωνία με τους φορείς του δημοσίου με ηλεκτρονικά μέσα, εκτός των πρόσφατων διατάξεων του νόμου περί ηλεκτρονικής διακυβέρνησης, διακρίνουμε τις ακόλουθες ρυθμιστικές πράξεις:

- Άρθρο 5Α Συντάγματος: Κατοχυρώνεται συνταγματικά το δικαίωμα συμμετοχής στην κοινωνία της πληροφορίας. Το δικαίωμα βρίσκει ουσιαστικό αντίκρισμα στην

επικοινωνία κράτους-πολίτη και στην ηλεκτρονική επικοινωνία με τη δημόσια διοίκηση, στην πρόσβαση σε δημόσια πληροφορία και σε υπηρεσίες ηλεκτρονικής διακυβέρνησης.

- Άρθρο 9Α Συντάγματος: Κατοχυρώνεται συνταγματικά η προστασία του ατόμου από συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων και η ιδιωτικότητα του υποκειμένου των πληροφοριών, σταθμίζοντας το δικαίωμα συμμετοχής σε μια κοινωνία με απεριόριστες δυνατότητες πρόσβασης στην πληροφορία.
- Άρθρο 14, Ν.2672/1998(«Διακίνηση Εγγράφων με ηλεκτρονικά μέσα»): Δυνατότητα ηλεκτρονικής επικοινωνίας με τους φορείς του δημόσιο, μέσω τηλεομοιοτυπίας και ηλεκτρονικού ταχυδρομείου.
- Π.Δ.342/2002: Ρυθμίζει τη διακίνηση εγγράφων μέσω ηλεκτρονικού ταχυδρομείου μεταξύ των δημοσίων υπηρεσιών, Ν.Π.Δ.Δ και Ο.Τ.Α. ή μεταξύ αυτών και των φυσικών ή νομικών προσώπων ιδιωτικού δικαίου και ενώσεων φυσικών προσώπων σε ορισμένες περιπτώσεις με υποχρεωτική ψηφιακή υπογραφή (π.χ. αποφάσεις, πιστοποιητικά κ.λπ.) και σε άλλες χωρίς ψηφιακή υπογραφή (εγκύκλιοι, οδηγίες κ.λπ). Καθορισμός των προϋποθέσεων ηλεκτρονικής επικοινωνίας για διοικητικούς σκοπούς, θεσπίζοντας την υποχρεωτική ψηφιακή υπογραφή διοικητικών εγγράφων που αποστέλλονται μέσω e-mail και παράγουν έννομες συνέπειες ως εκτελεστές διοικητικές πράξεις .
- Άρθρο 8, Ν.3242/2004: Θεσμοθέτηση της δυνατότητας διεκπεραίωσης διοικητικών συναλλαγών από την αρμόδια για την έκδοση της τελικής πράξης υπηρεσία με την χρήση ηλεκτρονικών μέσων.
- Άρθρο 20, Ν. 3448/2006, όπως ισχύει σήμερα μετά τις τροποποιήσεις του άρθρου 25 του Ν. 3536/2007:, Ορισμός της Υπηρεσία Ανάπτυξης Πληροφορικής (ΥΑΠ) του ΥΠΔΜΗΔ ως Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (Πρωτεύουσα Αρχή Πιστοποίησης).
- Εγκύκλιος ΥΑΠ/Φ.60/10/21711-5-2007 [36] της ΥΑΠ: Ορισμός της διαδικασία έκδοσης αναγνωρισμένου πιστοποιητικού.
- Με βάση το θεσμικό πλαίσιο ψηφιακής υπογραφής, την δημιουργία και λειτουργία υποδομής δημόσιου κλειδιού (PKI) μέσα από το έργο «ΣΥΖΕΥΞΙΣ» και τον Κανονισμό Πιστοποίησης ρυθμίστηκαν οι προϋποθέσεις παροχής υπηρεσιών πιστοποίησης στον δημόσιο τομέα, σύμφωνα με τις οποίες δίδεται η δυνατότητα στα στελέχη του Δημοσίου, με την χρήση «έξυπνων καρτών» που τους διατίθενται, να υπογράφουν ψηφιακά τις μεταξύ τους ηλεκτρονικές επικοινωνίες και συναλλαγές .

Η κατεύθυνση του νόμου είναι προς τη θεσμοθέτηση του δικαιώματος του πολίτη στην ηλεκτρονική επικοινωνία με τη Δημόσια Διοίκηση και στην ηλεκτρονική διεκπεραίωση των συναλλαγών, όπως και η υποχρέωση του κράτους για ηλεκτρονική προσφορά των υπηρεσιών του. Ο νόμος προσπαθεί να καθορίσει ένα πλαίσιο που θα λειτουργήσει συμπληρωματικά και παράλληλα με την ΚΠ. Δημιουργεί έτσι το πλαίσιο μέσα στο οποίο θα λειτουργήσει και προσπαθεί να προετοιμάσει το έδαφος, ώστε να υπάρχουν δομές

που θα την υποστηρίξουν και υπηρεσίες που μπορούν να προσφερθούν με την εφαρμογή της. Με τον τρόπο αυτό, η ΚΠ καθίσταται χρήσιμη για τον πολίτη, ως προς τις συναλλαγές του με το Δημόσιο. Επιπλέον, είναι σημαντική η αναφορά του νόμου στις προηγμένες ηλεκτρονικές υπογραφές.

3.3. Οδηγία για τις υπηρεσίες (2006/123/ΕΚ)

Η Οδηγία για τις Υπηρεσίες, της 12ης Δεκεμβρίου 2006, στοχεύει στην εναρμόνιση της εσωτερικής αγοράς στην παροχή υπηρεσιών, με σκοπό κυρίως να διευκολύνει την ελεύθερη κυκλοφορία των υπηρεσιών και εγκατάστασης των παρόχων των υπηρεσιών, εντός ΕΕ, αυξάνοντας τον ανταγωνισμό για ποιοτικότερες και φθηνότερες υπηρεσίες.

Τα σημαντικότερα σημεία της οδηγίας που πρέπει να κρατήσουμε υπό το πρίσμα της επιρροής της στην εφαρμογή της ΚΠ εντοπίζονται κυρίως στο άρθρο 8 της Οδηγίας περί ηλεκτρονικής διεκπεραίωσης διαδικασιών και τα οποία παρουσιάζονται ακολούθως.

- Δημιουργείται η υποχρέωση στα Κράτη-Μέλη να εξασφαλίζουν την από απόσταση και με χρήση ηλεκτρονικών μέσων διεκπεραίωση διαδικασιών για την πρόσβαση σε δραστηριότητες παροχής υπηρεσιών και την άσκηση αυτών.
- Ουσιαστικά, τα Κράτη-Μέλη οφείλουν να δημιουργήσουν ένα ηλεκτρονικό one-stop-shop , μέσω του οποίου θα ικανοποιούνται όλες οι απαιτήσεις, σχετικά με την πρόσβαση ή την άσκηση των υπηρεσιών των παρόχων σε κάθε κράτος.
- Η Επιτροπή θεσπίζει, σύμφωνα με τη διαδικασία του άρθρου 40 παράγραφος 2, τους όρους εφαρμογής της παραγράφου 1 του παρόντος άρθρου, με στόχο τη διευκόλυνση της διαλειτουργικότητας των πληροφοριακών συστημάτων και της χρησιμοποίησης των διαδικασιών τους μεταξύ των κρατών μελών, λαμβάνοντας υπόψη τα κοινά πρότυπα που εκπονούνται σε κοινοτικό επίπεδο.

Είναι σαφής η ανάγκη ύπαρξης διαλειτουργικών μηχανισμών αυθεντικοποίησης, προκειμένου να ικανοποιηθούν οι διατάξεις του άρθρου 8, για τις απομακρυσμένες συναλλαγές.

Το ερώτημα που πρέπει να κρατήσουμε είναι αν είναι αρκετή η διάταξη αυτή για την επίλυση του ζητήματος εφαρμογής ενιαίου αξιόπιστου διαλειτουργικού συστήματος ηλεκτρονικής ταυτοποίησης σε επίπεδο Ευρωπαϊκής Ένωσης, στην περίπτωση που κάποιο κράτος μέλος δεν επιθυμεί να το εφαρμόσει.

3.4. Ηλεκτρονικές Υπογραφές

Το θεσμικό πλαίσιο για την κατοχύρωση και των καθορισμό χρήσης και ισχύος των ηλεκτρονικών υπογραφών συμπυκνώνεται στις εξής παρεμβάσεις:

- Η Οδηγία 1999/93/ΕΚ [41] εξεδόθη από το Ευρωπαϊκό Συμβούλιο και το Ευρωπαϊκό Κοινοβούλιο στην προσπάθεια για την αξιοπιστία των ηλεκτρονικών συναλλαγών μεταξύ κρατών ή μεταξύ συναλλασσομένων μερών. Η οδηγία συνιστά μια ενιαία νομοθετική βάση, κοινή για όλες τις χώρες της Ευρωπαϊκής Ένωσης, περί της νομικής αναγνώρισης των ηλεκτρονικών υπογραφών, της αναγνώρισης των ψηφιακών πιστοποιητικών και της παροχής υπηρεσιών πιστοποίησης. Επιπλέον, θέτει τα ελάχιστα απαιτούμενα επίπεδα ασφάλειας, ενώ παράλληλα φροντίζει να διασφαλίσει την ελεύθερη διακίνηση των σχετικών προϊόντων και υπηρεσιών στην ενιαία αγορά.
- Η ΕΚ/709/2000, απόφαση της Επιτροπής, της 6ης Νοεμβρίου 2000, για τα ελάχιστα κριτήρια που πρέπει να λαμβάνουν υπόψη τα κράτη-μέλη, όταν ορίζουν φορείς σύμφωνα με το άρθρο 3 παράγραφος 4 της οδηγίας 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές [41].
- Το ΠΔ 150/2001 [34] αποτελεί την εθνική εναρμόνιση στη σχετική Ευρωπαϊκή Οδηγία [41] σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές.

Σε διεθνές επίπεδο συναντάμε δυο κύριες νομικές προσεγγίσεις, αναφορικά με την ανάλυση του θεσμικού πλαισίου για τις ηλεκτρονικές υπογραφές [41]. Σύμφωνα με τη μινιμαλιστική προσέγγιση, «κάθε αξιόπιστη τεχνολογική μέθοδος απόδειξης της προέλευσης και της αυθεντικότητας των ψηφιακών δεδομένων πρέπει να γίνεται νομικώς αποδεκτή» [21]. Όπως είναι προφανές, η μινιμαλιστική προσέγγιση αφήνει την αγορά να αποφασίσει για θέματα ασφάλειας και αξιοπιστίας. Αντιθέτως, στην αναλυτική προσέγγιση, «μόνο συγκεκριμένες τεχνολογικές μέθοδοι, οι οποίες ικανοποιούν συγκεκριμένα κριτήρια ασφάλειας και αξιοπιστίας, αναγνωρίζονται άμεσα ως νομικά ισότιμες με τις ιδιόχειρες υπογραφές». Η Ευρωπαϊκή Ένωση ακολούθησε μια μικτή προσέγγιση δύο επιπέδων, η οποία συνδυάζει και τις προαναφερόμενες κατευθύνσεις (μινιμαλιστική και αναλυτική), καταλήγοντας στην Οδηγία 1999/93/ΕΚ [41]. Στην οδηγία λοιπόν εφαρμόζεται η «προσέγγιση των δύο βαθμίδων» κάνοντας διάκριση ανάμεσα σε μια «ηλεκτρονική υπογραφή» και σε μια «προηγμένη ηλεκτρονική υπογραφή» (ή ψηφιακή υπογραφή).

3.4.1. Οδηγία 1999/93/ΕΚ

Στην οδηγία διαχωρίζονται οι τύποι των ηλεκτρονικών υπογραφών, οι ισχύοντες όροι για ορισμένους παρόχους υπηρεσιών πιστοποίησης, τα στοιχεία που περιλαμβάνει ένα αναγνωρισμένο πιστοποιητικό ηλεκτρονικής υπογραφής, συστάσεις για την ασφαλή επαλήθευση της υπογραφής, καθώς επίσης και τις απαιτήσεις για ασφαλείς διατάξεις δημιουργίας υπογραφής. Στην κατεύθυνση αυτή, οι κυριότεροι στόχοι της οδηγίας αφορούν στη δημιουργία ενός ενιαίου πλαισίου για τη νομική αναγνώριση των ηλεκτρονικών υπογραφών στο ευρωπαϊκό και εθνικό δίκαιο, την ενιαία ψηφιακή αγορά και την εξασφάλιση της τεχνολογικής ουδετερότητας.

Ωστόσο, το πλαίσιο της οδηγίας παρέμεινε τουλάχιστον ασαφές ως προς το ζήτημα της εφαρμογής της στην αυθεντικοποίηση οντοτήτων.

Η μια προσέγγιση θέλει τον οδηγία να στοχεύει στη δημιουργία ενός ενιαίου πλαισίου κανόνων για τον προσδιορισμό της ηλεκτρονικής υπογραφής, ως το ψηφιακό ισοδύναμο της χειρόγραφης υπογραφής. Σε αυτήν την ερμηνεία υπερέχει το στοιχείο της σύνδεσης του παραδοσιακού νομικού πλαισίου με τα τεχνικά ζητήματα της διαδικασίας υπογραφής. Εντούτοις, το έννομο αποτέλεσμα μίας υπογραφής ως μηχανισμού αυθεντικοποίησης οντοτήτων δεν έχει εφαρμογή το άρθρο 5, συνεπώς η συσχέτιση της οδηγίας με τη χρήση συστημάτων PKI για την αυθεντικοποίηση οντοτήτων είναι περιορισμένη.

Στον αντίποδα, η άλλη προσέγγιση θέλει την οδηγία να ρυθμίζει τη χρήση ψηφιακών υπογραφών ως μία τεχνολογία εν γένει, που η εφαρμογή της καλύπτει σχεδόν κάθε πιθανή χρήση ενός συστήματος PKI. Η ερμηνεία αυτή ενισχύεται από το γεγονός ότι η Οδηγία ορίζει την έννοια του «παρόχου υπηρεσιών πιστοποίησης» γενικά ως τον «φορέα ή φυσικό ή νομικό πρόσωπο που εκδίδει πιστοποιητικά ή παρέχει άλλες υπηρεσίες, συναφείς με τις ηλεκτρονικές υπογραφές», δηλαδή αρκεί μία «σχέση» με τις ηλεκτρονικές υπογραφές, ανεξάρτητα από την πραγματική εφαρμογή [41].

Επιχειρώντας μια ανάλυση των ορισμών που χρησιμοποιούνται στην οδηγία, μπορούμε να εντοπίσουμε σημαντικά ευρήματα σχετικά με την κατεύθυνση που προσπαθεί να δώσει ο νομοθέτης σε ζητήματα ταυτοποίησης και αυθεντικοποίησης, τα οποία θα φανούν, μάλλον, χρήσιμα στη μελέτη της εφαρμογής συστημάτων ηλεκτρονικής ταυτοποίησης και της ΚΠ.

Η οδηγία κάνει διάκριση ανάμεσα στις ηλεκτρονικές υπογραφές και τις προηγμένες ηλεκτρονικές υπογραφές. Έτσι, σύμφωνα με τους ορισμούς της οδηγίας μια ηλεκτρονική υπογραφή είναι «δεδομένα σε ηλεκτρονική μορφή, τα οποία επισυνάπτονται ή σχετίζονται λογικά με άλλα ηλεκτρονικά δεδομένα και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας (αυθεντικοποίηση)». Παρατηρούμε ότι για τις ηλεκτρονικές υπογραφές υιοθετήθηκε ένας ιδιαίτερα ευρύς ορισμός, όχι επαρκής, για ουσιαστικές νομικές εγγυήσεις και νομικές συνέπειες, σε αντίθεση με τον ορισμό που χρησιμοποιείται για τις προηγμένες ηλεκτρονικές υπογραφές και τα αναγνωρισμένα πιστοποιητικά.

Ως προς τις έννομες συνέπειες των ηλεκτρονικών υπογραφών η πάγια θέση του κοινοτικού νομοθέτη αφήνει το ζήτημα της ρύθμισης των ηλεκτρονικών εγγράφων που δεν διαθέτουν προηγμένη ηλεκτρονική υπογραφή στον νομοθέτη των κρατών μελών αλλά και στην κρίση του δικαστή με βάση τα γενικότερα συναλλακτικά ήθη, την καλή πίστη αλλά και τις γενικότερες επιταγές του ουσιαστικού και δικονομικού δικαίου. Παρόλα αυτά, προβλέπεται ότι η νομική ισχύς μιας ηλεκτρονικής υπογραφής (οποιασδήποτε μορφής ηλεκτρονική υπογραφή) και η αποδοχή της ως αποδεικτικού μέσου σε νομικές διαδικασίες δεν απορρίπτεται μόνο λόγω του γεγονότος ότι είναι σε ηλεκτρονική μορφή (δε βασίζεται σε αναγνωρισμένο πιστοποιητικό ή αναγνωσμένο πιστοποιητικό που εκδόθηκε από διαπιστευμένο φορέα παροχής υπηρεσιών πιστοποίησης ή δεν έχει δημιουργηθεί από ασφαλή διάταξη δημιουργίας υπογραφής). Σε αυτήν την προσέγγιση άλλωστε, υπακούουν και διατάξεις σχετικών οδηγιών, όπως της Οδηγίας 2002/31/ΕΚ για το ηλεκτρονικό εμπόριο, όπου στο άρθρο 9 ορίζεται η υποχρέωση των κρατών-μελών να μεριμνούν ώστε το νομικό τους σύστημα να επιτρέπει την σύναψη συμβάσεων με ηλεκτρονικά μέσα χωρίς να θέτει ως προϋπόθεση ότι τα έγγραφα αυτά οφείλουν να είναι ηλεκτρονικά υπογεγραμμένα.

Μια προηγμένη ηλεκτρονική υπογραφή (ψηφιακή υπογραφή) πρέπει να συνδέεται μονοσήμαντα με τον υπογράφοντα και να μπορεί να τον ταυτοποιήσει, να έχει δημιουργηθεί με τέτοια μέσα που ο υπογράφων μπορεί να διατηρήσει, υπό τον αποκλειστικό του έλεγχο, και να συνδέεται με τα δεδομένα στα οποία αναφέρεται με τρόπο τέτοιο, ώστε να μπορεί να εντοπισθεί οποιαδήποτε προκληθείσα αλλοίωση των δεδομένων. [εισαγωγή παραπομπής ορισμού]

Η ισοδυναμία με μια χειρόγραφη υπογραφή προβλέπεται σαφώς για την προηγμένη ηλεκτρονική υπογραφή, καθώς ο νομοθέτης ορίζει ότι ικανοποιούν τις νομικές απαιτήσεις υπογραφής σε σχέση με δεδομένα ηλεκτρονικής μορφής με τον ίδιο τρόπο που μια χειρόγραφη υπογραφή ικανοποιεί τις απαιτήσεις αυτές σε σχέση με δεδομένα επί χάρτου και γίνονται δεκτές ως αποδεικτικό στοιχείο σε νομικές διαδικασίες.

Τέλος, η οδηγία ορίζει τη «διάταξη (συσκευή) δημιουργίας υπογραφής», ως «διαμορφωμένο υλικό ή λογισμικό που χρησιμοποιείται για την εφαρμογή των δεδομένων δημιουργίας της υπογραφής». Μια τέτοια συσκευή θα μπορούσε να είναι μια έξυπνη κάρτα. Η έννοια του υποκειμένου της υπογραφής συνδέεται άμεσα με τη συσκευή παραγωγής της, αφού ως «υπογράφων» ορίζεται το «φυσικό ή νομικό πρόσωπο που κατέχει μια διάταξη (συσκευή) δημιουργίας υπογραφής και ενεργεί είτε για λογαριασμό του είτε εξ ονόματος φυσικού ή νομικού προσώπου ή οντότητας που εκπροσωπεί». Είναι επίσης σαφές, ότι στη διαμόρφωση των ορισμών ελήφθη υπόψη ο τρόπος λειτουργίας και η χρήση των PKI συστημάτων. Κατ' αντιστοιχία λοιπόν, για την οδηγία το ιδιωτικό κλειδί είναι τα δεδομένα δημιουργίας υπογραφής, τα οποία ορίζονται ως «μονοσήμαντα δεδομένα, όπως κώδικες ή ιδιωτικά κλειδιά κρυπτογραφίας που χρησιμοποιούνται από τον υπογράφοντα για τη δημιουργία ηλεκτρονικής υπογραφής». Το δημόσιο κλειδί, δηλαδή, τα δεδομένα επαλήθευσης υπογραφής σύμφωνα με την οδηγία είναι «δεδομένα, όπως κώδικες ή δημόσια κρυπτογραφικά κλειδιά, τα οποία χρησιμοποιούνται με σκοπό την επαλήθευση μιας ηλεκτρονικής υπογραφής» [41].

3.4.1.1. Αναγνωρισμένα Πιστοποιητικά

Συνεχίζοντας την ανάλυση των ορισμών της οδηγίας, ως πιστοποιητικό (certificate) ορίζεται η «ηλεκτρονική βεβαίωση που συνδέει δεδομένα επαλήθευσης υπογραφής με ένα πρόσωπο και επιβεβαιώνει την ταυτότητά του» [41] και ως αναγνωρισμένο πιστοποιητικό, «το πιστοποιητικό που ανταποκρίνεται στις απαιτήσεις του παραρτήματος I της οδηγίας και το οποίο εκδίδεται από φορέα παροχής υπηρεσιών πιστοποίησης, ο οποίος πληροί τις οριζόμενες στο παράρτημα II απαιτήσεις» [41].

Τα αναγνωρισμένα πιστοποιητικά πρέπει να περιλαμβάνουν:

- Ένδειξη ότι το πιστοποιητικό εκδίδεται ως αναγνωρισμένο πιστοποιητικά, ένδειξη της έναρξης και τέλος της περιόδου ισχύος του πιστοποιητικού και τον κωδικό ταυτοποίησης του πιστοποιητικού.

- Τα στοιχεία αναγνώρισης του παρόχου υπηρεσιών πιστοποίησης, την προηγμένη ηλεκτρονική υπογραφή του παρόχου υπηρεσιών πιστοποίησης που το εκδίδει και το κράτος-μέλος στο οποίο είναι εγκατεστημένο.
- Το όνομα του υπογράφοντος ή ψευδώνυμο.
- Πρόβλεψη ειδικού χαρακτηριστικού του υπογράφοντος, που θα περιληφθεί εφόσον είναι σημαντικό σε σχέση με τον σκοπό για τον οποίο προορίζεται το πιστοποιητικό.
- Δεδομένα επαλήθευσης υπογραφής που αντιστοιχούν σε δεδομένα δημιουργίας υπογραφής υπό τον έλεγχο του υπογράφοντος.
- Ενδεχόμενους περιορισμούς του πεδίου χρήσης του πιστοποιητικού, και

3.4.1.2. Πάροχοι Υπηρεσιών Πιστοποίησης (ΠΥΠ)

Ως φορέας παροχής υπηρεσιών πιστοποίησης (certificate service provider) ορίζεται «ο φορέας ή το φυσικό ή νομικό πρόσωπο που εκδίδει πιστοποιητικά ή παρέχει άλλες υπηρεσίες συναφείς με ηλεκτρονικές υπογραφές» [41] κατ' αντιστοιχία με την Αρχή Πιστοποίησης. Τα πιστοποιητικά που εκδίδει ένας φορέας παροχής υπηρεσιών πιστοποίησης μπορούν να θεωρηθούν αναγνωρισμένα (qualified), εφόσον ικανοποιούν τις απαιτήσεις του παραρτήματος I της οδηγίας 99/93/ΕΚ» [41]. και ο φορέας που τα εκδίδει πρέπει να συμμορφώνεται με τους όρους του Παραρτήματος II της εν λόγω Οδηγίας, ως εξής:

- Να λειτουργεί με επαρκή ασφάλεια και να λαμβάνει κατάλληλα μέτρα για να επαληθεύσει την ταυτότητα αυτών για τους οποίους εκδίδει πιστοποιητικά .
- Να τηρεί κατάλληλα αρχεία και να μην αποθηκεύει τα δεδομένα δημιουργίας υπογραφών (ιδιωτικά κλειδιά).
- Να αποδεικνύει αξιοπιστία κατά την παροχή υπηρεσιών πιστοποίησης, να απασχολεί έμπειρο και εξειδικευμένο προσωπικό, να διαθέτει επαρκείς οικονομικούς πόρους και να χρησιμοποιεί αξιόπιστα πληροφοριακά συστήματα, λαμβάνοντας επιπλέον μέτρα ώστε να εμποδίσει πλαστογραφήσεις και να διατηρήσει την εμπιστευτικότητα των κλειδιών υπογραφής.
- Να ενημερώνει με ανθεκτικά μέσα επικοινωνίας (Δήλωση πρακτικής και Όροι χρήσης των πιστοποιητικών) τους συνδρομητές, παρέχοντας τις κατάλληλες πληροφορίες σχετικά με τους όρους και τις προϋποθέσεις, υπό τις οποίες εκδίδονται τα πιστοποιητικά.
- Να προβαίνει σε άμεση ανάκληση των πιστοποιητικών όταν συντρέχει λόγος. Και να παρέχουν δημοσίευση, σε 24ωρη βάση, της Λίστας Ανακληθέντων Πιστοποιητικών προς ενημέρωση κάθε τρίτου.
- Να διασφαλίζει ότι η ημερομηνία έκδοσης ή ανάκλησης του πιστοποιητικού προσδιορίζεται επακριβώς.

- Να επαληθεύει την ταυτότητα των πιστοποιούμενων υποκειμένων και να διατηρεί τα σχετικά αποδεικτικά στοιχεία για κατάλληλη χρονική περίοδο (30 χρόνια για την Ελλάδα), για χρήση σε δικαστική ή εξώδικη επίλυση διαφορών.
- Να αποθηκεύει τα πιστοποιητικά σε επαληθεύσιμη μορφή.

Σχετικά με την αδειοδότηση και διαπίστευση των φορέων παροχής υπηρεσιών πιστοποίησης, ο κοινοτικός νομοθέτης παίρνει σαφή θέση υπέρ των σχημάτων εθελοντικής πιστοποίησης. Η οδηγία απαγορεύει ρητά την υποχρεωτική λήψη άδειας για την παροχή υπηρεσιών πιστοποίησης επιθυμώντας να διευκολύνει την ελεύθερη ανάπτυξη των αντίστοιχων υπηρεσιών και του ανταγωνισμού, με δυνατότητα θέσπισης όμως ειδικών μηχανισμών εθελοντικής διαπίστευσης, με τη μορφή ειδικών οργανισμών ή σωμάτων, για την εξασφάλιση βελτιωμένου επιπέδου παροχής υπηρεσιών πιστοποίησης. Οι φορείς παροχής υπηρεσιών διαπίστευσης μπορούν να λαμβάνουν, έπειτα από αίτησή τους, διαπίστευση στην οποία ορίζονται τα δικαιώματα και οι υποχρεώσεις που διέπουν την παροχή υπηρεσιών πιστοποίησης. Κάθε κράτος μέλος εξασφαλίζει την καθιέρωση κατάλληλου συστήματος που καθιστά δυνατή την επιτήρηση των εγκατεστημένων στο έδαφός του παρόχων υπηρεσιών πιστοποίησης, οι οποίοι εκδίδουν για το κοινό αναγνωρισμένα πιστοποιητικά.

Για την ορθότητα και ακρίβεια των πληροφοριών που περιέχονται σε ένα αναγνωρισμένο πιστοποιητικό, καθώς και την ακρίβεια των πινάκων ανάκλησης πιστοποιητικών (CRLs) με γνώμονα την αξιοπιστία των πληροφοριών που πιστοποιούνται και την προστασία των συναλλασσομένων, η οδηγία προβλέπει την ευθύνη των παρόχων υπηρεσιών πιστοποίησης για πιθανές ζημίες που θα προκληθούν σε βάρος οποιουδήποτε προσώπου ή φορέα από τη χρήση των αναγνωρισμένων πιστοποιητικών που εκδίδουν, αλλά και την πιθανή παράλειψη της καταγραφής της ανάκλησης του πιστοποιητικού. Ο πάροχος υπηρεσιών πιστοποίησης, που εκδίδει αναγνωρισμένο πιστοποιητικό ή εγγυάται για την ακρίβεια πιστοποιητικού, ευθύνεται έναντι οποιουδήποτε φορέα ή φυσικού ή νομικού προσώπου για τη ζημιά που προκλήθηκε σε βάρος του επειδή το πρόσωπο αυτό εύλογα βασίσθηκε στο πιστοποιητικό, όσον αφορά:

- Την ακρίβεια, κατά τη στιγμή έκδοσης του, όλων των πληροφοριών που περιέχονται στο αναγνωρισμένο πιστοποιητικό, καθώς και την ύπαρξη όλων των στοιχείων που απαιτούνται για την έκδοση του.
- Τη διαβεβαίωση ότι ο υπογράφων που ταυτοποιείται στο αναγνωρισμένο πιστοποιητικό ήταν κάτοχος, κατά τη στιγμή έκδοσης του πιστοποιητικού, των δεδομένων δημιουργίας υπογραφής (ιδιωτικό κλειδί) που αντιστοιχούν στα δεδομένα επαλήθευσης υπογραφής (δημόσιο κλειδί) που αναφέρονται στο πιστοποιητικό.
- Τη διαβεβαίωση ότι τα δεδομένα δημιουργίας της υπογραφής και τα δεδομένα επαλήθευσης της υπογραφής μπορούν να χρησιμοποιηθούν συμπληρωματικά, εφόσον προέρχονται από πάροχο υπηρεσιών πιστοποίησης.

Εκτός όμως της ευθύνης, αναγνωρίζεται και το δικαίωμα του ΠΥΠ να περιορίζει συμβατικά την παραπάνω ευθύνη που μπορεί να προκύψει από κακή από τη χρήση των

πιστοποιητικών που εκδίδει, με την εισαγωγή περιορισμών χρήσης (π.χ. επιτρεπόμενο ύψος των συναλλαγών) του πιστοποιητικού που εκδίδει. Επίσης, ο ΠΥΠ απαλλάσσεται από κάθε ευθύνη του αν αποδείξει ότι δεν έπραξε αμελώς. Ο γενικός κανόνας, πάντως, είναι ότι τα κράτη-μέλη μπορεί μεν να θέσουν πιο αυστηρούς όρους ως προς τον περιορισμό της ευθύνης, δεν μπορούν όμως να καθορίσουν μικρότερη έκταση ευθύνης για τους εν λόγω φορείς.

Επιπλέον, στην οδηγία εισάγεται το ζήτημα της διασυνοριακής αναγνώρισης των πιστοποιητικών που εκδίδονται από φορείς παροχής υπηρεσιών πιστοποίησης. Οι όροι οι οποίοι ισχύουν για την αναγνώριση πιστοποιητικών από τρίτες χώρες είναι αυστηροί, γεγονός που συνεπάγεται ότι οι χώρες που δεν έχουν αντίστοιχη νομοθεσία θα πρέπει είτε να συνεργαστούν με ευρωπαίους ΠΥΠ ή να έρθουν σε συμφωνία με την ΕΕ αναφορικά με τα τεχνικά και διαδικαστικά πρότυπα που χρησιμοποιούν για την πιστοποίηση. Ειδικότερα, προβλέπεται ότι τα αναγνωρισμένα πιστοποιητικά που έχουν εκδοθεί από φορέα παροχής υπηρεσιών πιστοποίησης εγκατεστημένο σε τρίτη χώρα θεωρούνται νομικώς ισοδύναμα με τα αντίστοιχα που εκδίδονται από φορέα παροχής υπηρεσιών πιστοποίησης εγκατεστημένο σε χώρα της Κοινότητας, εφόσον ισχύει ένας από τους παρακάτω όρους:

i. Ο φορέας παροχής υπηρεσιών πιστοποίησης ικανοποιεί τις απαιτήσεις που περιλαμβάνονται στην οδηγία και έχει λάβει διαπίστευση από μηχανισμό διαπίστευσης εγκατεστημένο σε χώρα-μέλος.
ii. Κάποιος φορέας παροχής υπηρεσιών πιστοποίησης, εγκατεστημένος στην Κοινότητα και ο οποίος πληροί τις απαιτήσεις της οδηγίας, εγγυάται για το πιστοποιητικό.
iii. Το πιστοποιητικό του φορέα αναγνωρίζεται βάσει διμερούς ή πολυμερούς συμφωνίας μεταξύ της Κοινότητας και τρίτων χωρών ή διεθνών οργανισμών.

Ο φορέας παροχής υπηρεσιών πιστοποίησης κατά την έκδοση πιστοποιητικού, δύναται να συγκεντρώνει δεδομένα προσωπικού χαρακτήρα μόνο από το απευθείας ενδιαφερόμενο πρόσωπο ή κατόπιν ρητής συγκατάθεσης του και μόνο στο βαθμό που είναι απαραίτητο για την έκδοση και διατήρηση του πιστοποιητικού. Η συλλογή ή επεξεργασία δεδομένων προσωπικού χαρακτήρα για άλλους σκοπούς απαγορεύεται, χωρίς τη συγκατάθεση του ενδιαφερόμενου προσώπου. (Άρθρο 8, παράγραφοι 2 και 3). Ο σεβασμός και η αναγνώριση, εξάλλου, του δικαιώματος της προστασίας δεδομένων και της ιδιωτικής ζωής του ατόμου είναι προϋπόθεση για την ενδυνάμωση, εδραίωση και αύξηση της εμπιστοσύνης των χρηστών στις ηλεκτρονικές επικοινωνίες και στις υπηρεσίες ηλεκτρονικής διακυβέρνησης και σε αυτήν την κατεύθυνση διακρίνεται η συμβατότητα της λειτουργίας των ΠΥΠ με τη σχετική νομοθεσία για τα προσωπικά δεδομένα και την ιδιωτικότητα.

Σε σχέση με τις απαιτήσεις προστασίας προσωπικών δεδομένων, ιδιαίτερη βαρύτητα πρέπει να δοθεί στη διασπορά πληροφοριών (πληροφορίες πιστοποιητικών και πληροφορίες ανάκλησης) καθώς και στους κανονισμούς σύννομης πρόσβασης σε δεδομένα διαθέσιμα σε ΠΥΠ. Οι Αρχές Προστασίας Δεδομένων συνίσταται να παρέχουν διευκολύνσεις στις δημόσιες αρχές να παρακολουθούν την πολιτική προστασίας της ιδιωτικότητας των ΠΥΠ. Επιπλέον, οι υποχρεώσεις και απαιτήσεις που καθορίζουν τις

απαραίτητες δεσμεύσεις, να καταγράφονται σε ειδικές πράξεις προστασίας δεδομένων, που θα συμπεριλαμβάνονται σε συμβόλαια μεταξύ του δημόσιου τομέα και των ΠΥΠ. Τέλος, πριν την υπογραφή συμβολαίου με ΠΥΠ, πρέπει να επαληθεύεται ο σεβασμός και εφαρμογή των κανονισμών προστασίας προσωπικών δεδομένων (όπως προβλέπεται στο άρθρο 17 της Κοινοτικής Οδηγίας Προστασίας Δεδομένων 95/46).

3.4.1.3. Απαιτήσεις ασφάλειας της υπογραφής

Προκειμένου για τη δημιουργία αναγνωρισμένης ηλεκτρονικής υπογραφής απαραίτητη είναι η χρήση ασφαλούς διάταξης δημιουργίας υπογραφής (Secure Signature Device Creation-SSCD) όπως προσδιορίζεται στην οδηγία (Παράρτημα III Οδηγίας). Η διάταξη ασφαλούς δημιουργίας υπογραφής, μέσω της χρήσης ενδεδειγμένων τεχνικών και διαδικαστικών μέσων, πρέπει να διασφαλίζει τουλάχιστον ότι τα δεδομένα δημιουργίας υπογραφής (ιδιωτικό κλειδί) που χρησιμοποιούνται για την παραγωγή υπογραφών:

- Απαντούν κατ'ουσίαν μόνο μια φορά και το απόρρητο είναι διασφαλισμένο. Αναλυτικότερα, αυτό σημαίνει ότι τα σχετικά κρυπτογραφικά κλειδιά πρέπει να δημιουργούνται με αλγόριθμους δημιουργίας τυχαίων κωδικών, είτε απευθείας μέσα στη συσκευή του χρήστη, είτε από συσκευές του ΠΥΠ που μεταφέρουν τα ιδιωτικά κλειδιά σε προσωπικές συσκευές του χρήστη για τον οποίο προορίζονται, χωρίς να τα εκθέτουν ή να διατηρούν αντίγραφα τους.
- Δεν είναι εφικτό, με σχετική εύλογη βεβαιότητα, να αντληθούν από άλλη πηγή (απαγορεύεται η διατήρηση αντιγράφου του ιδιωτικού κλειδιού) και η υπογραφή προστατεύεται από πλαστογραφία μέσω της χρήσης σύγχρονων τεχνολογιών (ασύμμετρη κρυπτογράφηση).
- Δύναται να προστατεύονται αποτελεσματικά από τον νόμιμο υπογράφοντα κατά της χρησιμοποίησής τους από τρίτους (π.χ. χρήση μυστικού κωδικού αναγνώρισης PIN).
- Τα προς υπογραφή δεδομένα δεν πρέπει να μεταβληθούν από τις ασφαλείς διατάξεις δημιουργίας υπογραφής και είναι δυνατό να εμφανίζονται στον υπογράφοντα πριν από τη διαδικασία υπογραφής.

Παράλληλα, κατά τη διαδικασία επαλήθευσης της υπογραφής θα πρέπει να διασφαλίζεται, με εύλογη βεβαιότητα, ότι:

- Τα δεδομένα που χρησιμοποιούνται προς επαλήθευση της υπογραφής αντιστοιχούν στα δεδομένα που εμφανίζονται στον επαληθεύοντα και η γνησιότητα και η εγκυρότητα του πιστοποιητικού που απαιτείται κατά τη στιγμή της επαλήθευσης της υπογραφής έχουν ελεγχθεί με αξιοπιστία.
- Η υπογραφή επαληθεύεται με αξιοπιστία και το αποτέλεσμα της επαλήθευσης και η ταυτότητα του υπογράφοντος εμφανίζονται με τον ορθό τρόπο.
- Ο επαληθεύων μπορεί να ορίσει με βεβαιότητα τα περιεχόμενα των δεδομένων που υπογράφονται.
- Η χρησιμοποίηση ψευδωνύμου δηλώνεται εμφανώς.

- Μπορούν να εντοπιστούν τροποποιήσεις απτόμενες της ασφάλειας.

3.4.2. Προεδρικό Διάταγμα 150/2001

Το Προεδρικό Διάταγμα 150/2001 (ΦΕΚ 125 Α'/25-6-2001) με τίτλο «Προσαρμογή στην Οδηγία 1999/93/ΕΚ [41] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές» ενσωματώνει στην ελληνική νομοθεσία την οδηγία 99/93/ΕΚ. Στο μεγαλύτερο μέρος του αποτελεί πιστή μεταφορά των αντίστοιχων αναφορών και προβλέψεων της Οδηγίας και αποδέχεται την ισοδύναμη νομική ισχύ των προηγμένων ηλεκτρονικών υπογραφών, με τις ιδιόχειρες υπογραφές. Οι ισχύοντες όροι για τα αναγνωρισμένα πιστοποιητικά, τους παρόχους υπηρεσιών πιστοποίησης που τα εκδίδουν, τις απαιτήσεις για ασφαλείς διατάξεις δημιουργίας υπογραφής και τις συστάσεις για την ασφαλή επαλήθευση της υπογραφής έχουν αντιγραφεί πιστά από τα παραρτήματα της οδηγίας. Το ίδιο συμβαίνει και με την προστασία δεδομένων, όπου όμως παρατηρούνται και πρόσθετοι κανόνες για τους παρόχους, όπως η υποχρέωσή τους να αναφέρουν σε ετήσια βάση στην ΕΕΤΤ τα μέτρα που λαμβάνουν για την προστασία αρχειοθετημένων, αποθηκευμένων πληροφοριών.

Ενδιαφέρον παρουσιάζει ο ορισμός για τις προηγμένες ηλεκτρονικές υπογραφές. Ο νομοθέτης ορίζει ότι, η ηλεκτρονική υπογραφή που επέχει θέση ιδιόχειρης, τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο, είναι μόνο η προηγμένη ηλεκτρονική υπογραφή που δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής και βασίζεται σε αναγνωρισμένο πιστοποιητικό που εκδίδεται από Πάροχο Υπηρεσιών Πιστοποίησης, ο οποίος πληροί τις προϋποθέσεις που περιγράφονται στην οδηγία. Η προσέγγιση του νομοθέτη, ουσιαστικά, κατοχυρώνει με πιο επαρκή τρόπο την ηλεκτρονική υπογραφή ως νομικό ισοδύναμο της ιδιόχειρης εφόσον τηρούνται συγκεκριμένες προϋποθέσεις - προηγμένη ηλεκτρονική υπογραφή που δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής και βασίζεται σε αναγνωρισμένο πιστοποιητικό (άρθρ. 3 § 1, Π.Δ. 150/2001 [34])- , καθώς της προσδίδει ιδιότητες που χαρακτηρίζουν την ιδιόχειρη υπογραφή. Πιο συγκεκριμένα, ως προηγμένη ηλεκτρονική υπογραφή (ή ψηφιακή υπογραφή) ορίζεται η «ηλεκτρονική υπογραφή που πληροί τους εξής όρους: α) συνδέεται μονοσήμαντα μα τον υπογράφοντα, β) είναι ικανή να καθορίσει ειδικά και αποκλειστικά τη ταυτότητα του υπογράφοντος, γ) δημιουργείται με μέσα, τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό έλεγχό του και δ) συνδέεται με τα δεδομένα, στα οποία αναφέρεται κατά τρόπο, ώστε να μπορεί να εντοπισθεί οποιαδήποτε μεταγενέστερη αλλοίωση των εν λόγω δεδομένων». Ωστόσο, η απλή ηλεκτρονική υπογραφή -παρότι δεν μπορεί να εξισωθεί με την ιδιόχειρη υπογραφή- δεν χάνει τη νομική της ισχύ μόνο εξ αιτίας του γεγονότος ότι δεν είναι προηγμένη και είναι δυνατό να αρκεί ως αποδεικτικό στοιχείο για την εγκυρότητα συμβάσεων, για τις οποίες δεν προβλέπεται έγγραφος τύπος καθώς ορίζεται ότι η κατάρτιση συμβάσεων με ηλεκτρονικά μέσα είναι δυνατή με τη χρήση της απλής ηλεκτρονικής υπογραφής, όταν από το νόμο δεν προβλέπεται έγγραφος τύπος για την κατάρτισης μιας ορισμένης σύμβασης (Άρθρα 3 § 2 και 8 § 1 του Π.Δ. 150/2001 [34]). Επομένως, το ηλεκτρονικό έγγραφο στο οποίο περιέχεται η ηλεκτρονική υπογραφή και το οποίο προσάγεται ως αποδεικτικό μέσο, εκτιμάται ελεύθερα από το δικαστήριο και δεν απορρίπτεται ως απαράδεκτο εξαιτίας της μη πλήρωσης των προϋποθέσεων προηγμένης

ηλεκτρονικής υπογραφής. Κρίνεται, έτσι, αναγκαίο, να συμφωνούν αμοιβαία τα μέρη στις επιμέρους εμπορικές συναλλαγές ότι τα ηλεκτρονικά διαβιβαζόμενα έγγραφα τους θα αποτελούν πλήρη απόδειξη ως ιδιωτικά έγγραφα ακόμη και αν δεν περιλαμβάνουν ηλεκτρονική υπογραφή. Με τον τρόπο αυτό, όπως προκύπτει από την Οδηγία, τα ηλεκτρονικά κείμενα που ανταλλάσσουν μεταξύ τους οι συναλλασσόμενοι, όπως για παράδειγμα τα email ανάγονται δυνητικά σε παραδεκτό αποδεικτικό μέσο που απορρέει από την σχετική συμφωνία των μερών.

Στο άρθρο 2 του Π.Δ. ορίζεται ακόμη το αναγνωρισμένο πιστοποιητικό ως η ηλεκτρονική βεβαίωση που εκδίδεται από κάποιον πάροχο υπηρεσιών πιστοποίησης και η οποία συνδέει μονοσήμαντα τα δεδομένα επαλήθευσης μιας υπογραφής (δημόσιο κλειδί) με ένα συγκεκριμένο φυσικό πρόσωπο, τηρώντας κάποιους βασικούς όρους (Παραρτήματα I & IV του Π.Δ. 150/2001) [34]. Ο φορέας παροχής υπηρεσιών πιστοποίησης είναι υπεύθυνος για την ακρίβεια του πιστοποιητικού (άρθρο 3 § 1 Π.Δ. 150/2001), το οποίο εκδίδεται υπό τους όρους του Παραρτήματος I κι έχει ως σκοπό να συμβάλλει στη διαπίστωση της γνησιότητας της προηγμένης ηλεκτρονικής υπογραφής. Τα φυσικά ή νομικά πρόσωπα (φορείς παροχής υπηρεσιών πιστοποίησης) που εκδίδουν πιστοποιητικά ή παρέχουν άλλες υπηρεσίες συναφείς με τις ηλεκτρονικές υπογραφές οφείλουν να πληρούν ορισμένους όρους οι οποίοι περιγράφονται στο Παράρτημα II του Π.Δ..

Σύμφωνα με το άρθρο 4 του Π.Δ. 150/2001 [34], για την Ελλάδα, ορίζεται η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων(ΕΕΤΤ) ως αρμόδια αρχή για τον ορισμό και την εποπτεία ιδιωτικών ή δημόσιων φορέων για τη διαπίστευση των Παρόχων Πιστοποίησης, για τον έλεγχο και την εποπτεία των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης ηλεκτρονικής υπογραφής, καθώς και για τη διαπίστωση της συμμόρφωσης προς τις ασφαλείς διατάξεις δημιουργίας υπογραφής, ως συνέπεια συμμόρφωσης με την υποχρέωση της οδηγίας περί σύστασης φορέων επιτήρησης.

Ως προς την ευθύνη των Παρόχων Υπηρεσιών Πιστοποίησης διακρίνεται η ευθύνη τους ανάλογα με το αν εκδίδουν αναγνωρισμένα ή μη αναγνωρισμένα πιστοποιητικά. Η ευθύνη των ΠΥΠ για τα μη αναγνωρισμένα πιστοποιητικά κρίνεται με τις γενικές διατάξεις περί ευθύνης. Σε αντιστοιχία με τις διατάξεις της Κοινοτικής Οδηγίας, αν ο ΠΥΠ εκδίδει αναγνωρισμένα πιστοποιητικά τεκμαίρεται η ευθύνη του σε περίπτωση ζημιογόνου γεγονότος που αφορά:

- στην ακρίβεια και πληρότητα του πιστοποιητικού,
- στην ταυτότητα του υπογράφοντος, στην ηλεκτρονική υπογραφή του οποίου αναφέρεται το πιστοποιητικό
- στη δυνατότητα συμπληρωματικής χρήσης των δεδομένων δημιουργίας και επαλήθευσης της ηλεκτρονικής υπογραφής και
- στην μη έγκαιρη καταγραφή της ανάκληση ενός πιστοποιητικού.

Στα πλαίσια της ευθύνης του παρόχου, έστω και ελαφριά αμέλεια αρκεί για την γένεση της ευθύνης και επομένως η μόνη περίπτωση απαλλαγής είναι να αποδειχθεί ότι ο πάροχος ενήργησε επιμελώς. Επιπλέον, ιδιαίτερη σημασία έχει το γεγονός ότι το βάρος απόδειξης αντιστρέφεται προς όφελος κάθε φορέα που εύλογα βασίζεται στο πιστοποιητικό,

ανεξάρτητα από το αν τον συνδέει συμβατικός δεσμός με τον πάροχο. Ο βαθμός υπαιτιότητας είναι σημαντικός για τον καθορισμό του ύψους της αποζημίωσης, το οποίο όμως, υπόκειται σε περιορισμούς, ανάλογα με τα όρια που έχει ρητώς θέσει ο ΠΥΠ ως προς τη χρήση των πιστοποιητικών του. Εντούτοις, δεν είναι σαφώς ορισμένο το ζήτημα του πιθανού περιορισμού της συνολικής ευθύνης από πλευράς του παρόχου, παρέχοντάς του τη δυνατότητα ορισμού ενός ανώτατου ορίου ευθύνης που θα προστάτευε τον πάροχο από το πλήθος των ζημιών που θα μπορούσε να προκαλέσει ένα εσφαλμένο πιστοποιητικό. Για το αστικό δίκαιο, μάλιστα, συνήθως τέτοιοι όροι κρίνονται άκυροι ως καταχρηστικοί.

3.4.5. Συμπληρωματικές Διατάξεις

Η ΕΕΤΤ με την υπ' αριθμόν 248/71 Απόφασή της «Κανονισμός Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής» (ΦΕΚ 603/Β'/16-5-2002) ρυθμίζει ζητήματα των αναγνωρισμένων πιστοποιητικών και καθορίζει το θεσμικό πλαίσιο για την εποπτεία και τον έλεγχο των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης. Στα πλαίσια αυτά, τηρεί τον Κατάλογο Εμπίστευσης εποπτευόμενων/διαπιστευομένων παρόχων υπηρεσιών πιστοποίησης (Trusted Service Provider List, TSL) της Ελλάδας παρέχοντας πληροφορίες σχετικά με την κατάσταση εποπτείας/διαπίστευσης των υπηρεσιών πιστοποίησης από τους παρόχους υπηρεσιών πιστοποίησης (CSP) οι οποίοι εποπτεύονται/διαπιστεύονται από την ΕΕΤΤ ως προς τη συμμόρφωση με τις σχετικές διατάξεις της οδηγίας [41]. Ο Κατάλογος Εμπίστευσης περιλαμβάνει τους ΠΥΠ που είναι εγγεγραμμένοι στο μητρώο της ΕΕΤΤ ως πάροχοι που εκδίδουν αναγνωρισμένα πιστοποιητικά ηλεκτρονικής υπογραφής κατά δήλωσή τους.

1. Αρχή Πιστοποίησης Ελληνικού Δημοσίου που ανήκει στο Υπουργείο Εσωτερικών, Υπηρεσία Ανάπτυξης Πληροφορικής (http://pki.syzefxis.gov.gr)
2. Adacom Qualified Certificate Services CA (http://www.adacom.com/repository)
3. ASYK Qualified Certificates CA της Χρηματιστήριο Αθηνών ΑΕ (http://www.ase.gr/repository)

Η Αρχή Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ) ορίστηκε ως Πρωτεύουσα Αρχή Πιστοποίησης με σχετικό κόμβο τον syzefxis.gov.gr όπως ορίζεται στη σχετική απόφαση [40]. Με την ΚΥΑ ΥΑΠ/Φ.60/38/232 [99] κυρώθηκε ο Κανονισμός Πιστοποίησης της ΑΠΕΔ, ενώ με την ΥΑ ΥΑΠ/Φ.60/7/135 [98] καθορίστηκαν οι οργανικές μονάδες για την παροχή υπηρεσιών πιστοποίησης (ΥΑΠ, ΚτΠ ΑΕ, ΚΕΠ).

Σύμφωνα με την Εγκύκλιο της ΥΑΠ [36] η PKI Υποδομή βασίζεται σε μια ιεραρχικά κατανεμημένη δομή αρμοδιοτήτων, ως εξής :

1. Αρχή Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ): Ως «Πρωτεύουσα Αρχή Πιστοποίησης» (ΠΑΠ) ορίστηκε, σύμφωνα με το άρθρο 20 του Ν. 3448/2006 (ΦΕΚ 57/Α715-3-2006), έτσι όπως τροποποιήθηκε από το άρθρο 25 του Ν. 3536/2007 (ΦΕΚ 42/Α723-2-2007), η Υπηρεσία Ανάπτυξης Πληροφορικής (ΥΑΠ) της Γενικής Γραμματείας Δημόσιας Διοίκησης & Ηλεκτρονικής Διακυβέρνησης του ΥΠ.ΕΣ.Δ.Δ.Α..

2. Υποκείμενη Αρχή Πιστοποίησης (ΥπΑΠ) του Υπουργείου Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης ορίζεται το Τμήμα Επεξεργασίας και Διαρκούς Απογραφής της Διεύθυνσης Προγραμματισμού και Εφαρμογών της Υπηρεσίας Ανάπτυξης Πληροφορικής της Γενικής Γραμματείας Δημόσιας Διοίκησης και Ηλεκτρονικής Διακυβέρνησης του ΥΠ.ΕΣ.Δ.Δ.Α..

3. Αρχή Εγγραφής (ΑΕ) του ΥΠ.ΕΣ.Δ.Δ.Α., ορίζεται ο Τομέας Υλοποίησης και Παραγωγικής Λειτουργίας Έργων και Συστημάτων της «Κοινωνίας της Πληροφορίας ΑΕ - ΚτΠ Α.Ε.».

4. Εντεταλμένα Γραφεία, ορίζονται τα Κέντρα Εξυπηρέτησης Πολιτών (ΚΕΠ), σε ολόκληρη τη χώρα.

Επιπλέον, με τον Ν.3979/2011 περί Ηλεκτρονικής Διακυβέρνησης [33] ορίζονται επιπλέον ζητήματα για τις ηλεκτρονικές υπογραφές και πιστοποιητικά. Ειδικότερα, στο άρθρο 13 (Κύρος και αποδεικτική ισχύς ηλεκτρονικών εγγράφων), άρθρο 14 (Αντίγραφα), άρθρο 22(Διακίνηση εγγράφων μεταξύ φορέων του δημοσίου τομέα και φυσικών προσώπων ή Ν.Π.Ι.Δ.) και άρθρο 31(Εγγραφή σε υπηρεσίες ηλεκτρονικής διακυβέρνησης).

Οι ηλεκτρονικές υπογραφές αποτελούν το πιο σημαντικό θεσμικό βήμα στο θέμα της ΚΠ. Ωστόσο, είναι σημαντικό να σημειωθεί ότι η Οδηγία αυτή καθ' αυτή ούτε θίγει το έννομο αποτέλεσμα της αυθεντικοποίησης του ατόμου, ούτε καθορίζει το πότε μία οντότητα έχει αναγνωριστεί μονοσήμαντα, ούτε το ποια είναι η νομική συνέπεια ενός πιστοποιητικού αυθεντικοποίησης. Εξάλλου ούτε η ιδιόχειρη υπογραφή μπορεί να ταυτοποιήσει το υποκείμενο. Η υπογραφή δρα συμπληρωματικά καθώς είναι «ικανή να ταυτοποιεί τον υπογράφοντα» (άρθρο 2§2) και το αναγνωρισμένο πιστοποιητικό πρέπει να «επιβεβαιώνει την ταυτότητα αυτού του ατόμου».

Παρόλα αυτά, η Οδηγία ανοίγει το ζήτημα και θα λέγαμε ότι προκρίνει τα συστήματα PKI ως κατάλληλη τεχνική λύση για τη διαχείριση των eID. Σε κάθε περίπτωση, το θεσμικό βήμα είναι μεγάλο ακόμη κι αν δεν έχει άμεση εφαρμογή στις υπηρεσίες αυθεντικοποίησης οντοτήτων (συμπεριλαμβανομένων ιδίως εκείνων που βασίζονται σε μεθόδους PKI) και κατ' επέκταση στην ηλεκτρονική ταυτοποίηση και στην ΚΠ.

3.5. ΔΙΑΣΦΑΛΙΣΗ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΤΟΥ ΑΤΟΜΟΥ

Το θεσμικό πλαίσιο που ρυθμίζει και θωρακίζει την ιδιωτικότητα συνοψίζεται στα εξής:

1. Ν.2472/1997 «περί προστασίας του ατόμου έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα»,
2. Ν. 2774/1999 «περί προστασίας των δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα», ο οποίος αντικαταστάθηκε από τον Ν. 3471/2006 ως

3. Εναρμόνιση με την Οδηγία 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών [42],
4. Οδηγία 1995/46/ΕΚ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη διακίνηση των δεδομένων αυτών [44], και το
5. Άρθρο 8 της Ευρωπαϊκής Σύμβασης για τα Ανθρώπινα Δικαιώματα του Ανθρώπου. Η αντιγραφή, χρήση, αποκάλυψη ή υποκλοπή προσωπικών δεδομένων, που τηρούνται σε αρχεία ή μεταδίδονται μέσω δικτύων, είναι εφικτό να επιφέρει την επιβολή των κυρώσεων των άρθρων 370Α , 370Β και 370Γ ΠΚ.

«Προσωπικά δεδομένα: κάθε πληροφορία που αναφέρεται σε ένα φυσικό πρόσωπο, του οποίου ή ταυτότητα είναι γνωστή ή μπορεί να προσδιοριστεί άμεσα ή έμμεσα ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσοτέρων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική.» (Οδηγία 95/46, άρθρο 2Α [44]).

Κατά συνέπεια, είναι απολύτως προφανές ότι στο θέμα της ηλεκτρονικής ταυτοποίησης η οδηγία για τα προσωπικά δεδομένα έχει μεγάλη σημασία καθώς, η διαχείριση ηλεκτρονικών ταυτοτήτων εξ' ορισμού περιστρέφεται γύρω από τη διαχείριση των προσωπικών δεδομένων για ταυτοποίηση. Για παράδειγμα, δεδομένα που χρησιμοποιούνται για τον προσδιορισμό της ταυτότητας του προσώπου είναι το όνομα, αριθμός της κοινωνικής ασφάλισης, αριθμός του δελτίου ταυτότητας, αριθμός πελάτη, κωδικοί αναγνώρισης ή πρόσβασης του προσώπου, PIN κ.α. Επιπλέον, οι προσωπικές πληροφορίες που μπορεί να αφορούν τις σχέσεις ενός προσώπου προς πρόσωπα ή τις σχέσεις του προς πράγματα: περιουσιακή κατάσταση, επαγγελματική και οικονομική δραστηριότητα, οικογενειακή κατάσταση, τις προσωπικές δραστηριότητες και σχέσεις (συνήθειες του ελεύθερου χρόνου, συμμετοχή και δραστηριοποίηση σε ενώσεις, καταναλωτική συμπεριφορά), καθώς και τις σχέσεις και καταστάσεις ιδιωτικού και δημοσίου δικαίου (ιδιοκτησία, συμβατικές σχέσεις, διοικητικές άδειες κλπ.) [21].

Για την Ελλάδα, η Αρχή Προστασίας Προσωπικών Δεδομένων (ΑΠΔΠΧ) ως ανεξάρτητη αρχή κατοχυρωμένη στο Σύνταγμα (άρθρα 9Α και 101Α) έχει έναν πολυσχιδή θεσμικό ρόλο και ευρείες αρμοδιότητες μέσα στο παραπάνω πλαίσιο. Η ΑΠΔΠΧ ιδρύθηκε με το νόμο 2472/1997, ο οποίος ενσωματώνει στο ελληνικό δίκαιο την Ευρωπαϊκή Οδηγία 95/46/ΕΚ, 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 58/2002.

Αποστολή της Αρχής αποτελεί η προστασία των δικαιωμάτων της προσωπικότητας και της ιδιωτικής ζωής του ατόμου στην Ελλάδα, σύμφωνα με τις διατάξεις των Ν. 2472/1997 και 3471/2006. 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.ο.κ). Επίσης, 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. [102]

3.5.1. Οδηγία για την προστασία προσωπικών δεδομένων (95/46/ΕΚ)

Το κύριο αντικείμενο της Οδηγίας [44] για την προστασία των προσωπικών δεδομένων είναι όπως αναφέρεται «η προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων, και ιδίως της ιδιωτικής του ζωής σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα» . Η κύρια επιλογή που διατρέχει τις ρυθμίσεις της Οδηγίας είναι ο περιορισμός της επεξεργασίας προσωπικών δεδομένων στο ελάχιστο δυνατό.

Στο άρθρο 6 της Οδηγίας καθορίζονται οι ποιοτικές προδιαγραφές δεδομένων επεξεργασίας. Οι βασικές αρχές για τη διαχείριση και επεξεργασία των προσωπικών δεδομένων συνοψίζονται στα ακόλουθα:

- Τα δεδομένα μπορούν να υφίστανται σύννομη και θεμιτή επεξεργασία.
- Η συλλογή των δεδομένων πρέπει να συνδέεται με την εξυπηρέτηση σαφών και νόμιμων σκοπών και η πιθανή μεταγενέστερη επεξεργασία τους να συμβιβάζεται με τους σκοπούς αυτούς. Σε διασυνοριακό επίπεδο, μπορούμε να πούμε ότι η αρχή αυτή ακολουθεί μια «πολιτικοκεντρική» προσέγγιση, καθώς απαγορεύει στις κυβερνήσεις να χρησιμοποιούν μητρώα ή άλλες πηγές ταυτοποίησης οι οποίες έχουν δημιουργηθεί για τους σκοπούς της δημόσιας διοίκησης, για άλλους σκοπούς, χωρίς περαιτέρω σαφή και νόμιμη νομιμοποιητική βάση και χωρίς την προηγούμενη εξασφάλιση της ρητής συγκατάθεσης του υποκειμένου των δεδομένων.
- Τα δεδομένα πρέπει να είναι κατάλληλα, συναφή και απολύτως αναγκαία για την επίτευξη του επιδιωκόμενου σκοπού («Αρχή της αναλογικότητας» ως προς την επεξεργασία και την έκτασή της). Στην περίπτωση της αυθεντικοποίησης, η αρχή της αναλογικότητας μεταφράζεται στη μη διατήρηση περισσότερων προσωπικών δεδομένων από εκείνα που είναι απολύτως αναγκαία, για την ταυτοποίηση του υποκειμένου των δεδομένων και την επίτευξη του σκοπού της εφαρμογής. Η αυθεντικοποίηση, ωστόσο, πρέπει να υπαγορεύεται από πληροφοριακές ανάγκες οι οποίες έχουν υφίστανται για το άτομο, και όχι από την πιθανότητα να προκύψουν τέτοιες ανάγκες.
- Τα δεδομένα πρέπει να είναι ορθά, ακριβή και επικαιροποιημένα («Αρχή της ακρίβειας»). Δεδομένα ανακριβή ή ελλιπή σε σχέση με τους σκοπούς για τους

οποίους έχουν συλλέγει πρέπει να διαγράφονται ή να επικαιροποιούνται. Σύμφωνα λοιπόν με τη συγκεκριμένη αρχή, οι υπεύθυνοι επεξεργασίας δεδομένων οφείλουν να ελέγχουν την ακρίβεια των προσωπικών δεδομένων που διαχειρίζονται. Η σημασία της αρχής αυτής αφορά στην εγκυρότητα των στοιχείων που ο πολίτης, οι επιχειρήσεις και οι δημόσιοι φορείς χρησιμοποιούν για τις μεταξύ τους συναλλαγές και επικαλούνται στις πράξεις τους καθώς και στις νομικές εγγυήσεις που προκύπτουν από τη χρήση τέτοιων δεδομένων. Έτσι, , από διασυνοριακή οπτική, ταυτοποίηση των οντοτήτων πρέπει να βασίζεται σε πληροφορίες που παρέχονται μέσω συστημάτων που διασφαλίζουν τις υφιστάμενες, για κάθε περίπτωση, νομικές εγγυήσεις.

- Η επεξεργασία πρέπει να περιορίζεται στο χρονικό διάστημα που είναι αναγκαίο για την εκπλήρωση του σκοπού της επεξεργασίας. Επιπλέον, τα δεδομένα πρέπει 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 συλλέγει ή για τους οποίους αργότερα υφίστανται επεξεργασία. Τα κράτη μέλη προβλέπουν κατάλληλες εγγυήσεις για τα δεδομένα προσωπικού χαρακτήρα που διατηρούνται πέραν της περιόδου αυτής για σκοπούς ιστορικούς, στατιστικούς ή επιστημονικούς.

- Για κάθε δεδομένο, μία και μόνο μία πηγή μπορεί να θεωρηθεί ότι είναι αυθεντική για τη διασταύρωση αυτού του στοιχείου («Αρχή της αυθεντικής πηγής»). Η πληροφορία αυτή θα πρέπει να επαναχρησιμοποιηθεί από όλα τα μέρη που έχουν ορισμένο έννομο συμφέρον, έτσι ώστε να ελαχιστοποιηθεί η ενόχληση του χρήστη και να συντηρείται μόνο ένα σημείο επικαιροποίησης της πληροφορίας.

Ειδικότερα στο άρθρο 6, στις παραγράφους β έως δ, από πλευράς διασυνοριακής διαλειτουργικότητας, οι αναφορές έχουν ιδιαίτερο ενδιαφέρον, καθώς καθορίζονται σε υψηλό επίπεδο οι προϋποθέσεις για τη νόμιμη διασυνοριακή αυθεντικοποίηση με τη χρήση πηγών της δημόσιας διοίκησης.

Στη συνέχεια, το άρθρο 7 της Οδηγίας περιγράφει τις συνθήκες κατά τις οποίες είναι αποδεκτή η αυτοματοποιημένη ή από αρχείο χρήση των προσωπικών δεδομένων, με τρόπο τέτοιο που να εξασφαλίζεται η γνώση του κατόχου σχετικά με το ποιος και για ποιο σκοπό κατέχει τις προσωπικές πληροφορίες του και που/πως σκοπεύει να τις χρησιμοποιήσει. Έτσι, εξασφαλίζεται η αρχή της διαφάνειας έναντι του υποκειμένου των δεδομένων και η διαφάνεια της επεξεργασίας.

Πιο συγκεκριμένα, τα προσωπικά δεδομένα μπορεί να τύχουν επεξεργασίας:

- όταν ενημερωθεί το άτομο για την ταυτότητα αυτού που πρόκειται να χρησιμοποιήσει τα δεδομένα, καθώς και για το σκοπό της χρήσης τους («Αρχή του σκοπού»),

- όταν το πρόσωπο στο οποίο αναφέρονται τα δεδομένα έχει δώσει τη ρητή συγκατάθεσή του ή υπάρχει άλλος νόμιμος λόγος για την επιτρεπόμενη χρήση (π.χ. η ενάσκηση της ελευθερίας της έκφρασης) ή

- όταν είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το ενδιαφερόμενο πρόσωπο είναι συμβαλλόμενο μέρος ή για την εκτέλεση προσυμβατικών μέτρων ληφθέντων αιτήσει του ή

- όταν είναι απαραίτητη για την τήρηση εκ του νόμου υποχρεώσεως του υπευθύνου της επεξεργασίας ή

- όταν είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του προσώπου στο οποίο αναφέρονται τα δεδομένα ή

- όταν είναι απαραίτητη για την εκπλήρωση έργου δημοσίου συμφέροντος ή εμπίπτοντος στην άσκηση δημοσίας εξουσίας που έχει ανατεθεί στον υπεύθυνο της επεξεργασίας ή στον τρίτο στον οποίο ανακοινώνονται τα δεδομένα ή

- όταν είναι απαραίτητη για την επίτευξη του εννόμου συμφέροντος που επιδιώκει ο υπεύθυνος της 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 δυνάμει του άρθρου 1 παράγραφος 1 της Οδηγίας και

- όταν τα δεδομένα είναι σχετικά με το σκοπό της χρήσης, ακριβή, επικαιροποιημένα και όχι περισσότερα από όσα είναι αναγκαίο για το σκοπό της χρήσης.

3.5.2. Απόρρητο Επικοινωνιών

Το θεσμικό πλαίσιο για το απόρρητο των επικοινωνιών διαμορφώνεται από τα ακόλουθα:

1. Άρθρο 19 παρ. 1 του Συντάγματος: «Το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο είναι απόλυτα απαραβίαστο. Νόμος ορίζει τις εγγυήσεις υπό τις οποίες η δικαστική αρχή δε δεσμεύεται από το απόρρητο για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.»

2. Ν.2225/1994 περί «Προστασίας της ελευθερίας της ανταπόκρισης και επικοινωνίας και άλλες διατάξεις».

3. Ν.3115/2003

4. Ν.3471/2006

5. Π.Δ. 47/2005

Το απόρρητο αφορά όλες τις μορφές επικοινωνίας υπό την έννοια της μυστικότητας και απαγορεύει κάθε ενέργεια των δημοσίων αρχών προς λήψη γνώσης ή κοινοποίηση σε τρίτους του περιεχομένου/στοιχείων επικοινωνίας και κάθε πολίτη. Σημαντική δε προσθήκη στην ερμηνεία αυτή, είναι η επέκταση στις περιστάσεις στις οποίες διενεργείται η επικοινωνία, αλλά και δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς διαβίβασης μιας επικοινωνίας ή της χρέωσής της («εξωτερικά στοιχεία» και «δεδομένα κίνησης και θέσης» της επικοινωνίας, Ν.3471/06, ενσωμάτωση της Οδηγίας 2002/58/ΕΚ).

Αναφερόμενοι στην έννοια του όρου "επικοινωνία" περιλαμβάνεται προφανώς και η ανταλλαγή δεδομένων μεταξύ του IC της κάρτας και του αναγνώστη, όπως ακριβώς συμβαίνει και με την πλοήγηση στο διαδίκτυο ή την αποστολή e-mail όπου πραγματοποιείται διαφανώς ανταλλαγή πληροφοριών ανάμεσα σε χρήστη — πάροχο — εξυπηρετητή κλπ..

Για την Ελλάδα η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών είναι η συνταγματικά κατοχυρωμένη Αρχή (άρθρο 1 του νόμου 3115/2003, κατά την παράγραφο 2 του άρθρου 19 του Συντάγματος), που είναι αρμόδια για την προστασία του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο καθώς και την ασφάλεια των δικτύων και πληροφοριών. Στην έννοια της προστασίας του απορρήτου των επικοινωνιών περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου, που προβλέπονται από τον νόμο.

Καθίσταται σαφές, ότι η προστασία των προσωπικών δεδομένων αποτελεί, ίσως, το πιο κρίσιμο ζήτημα στην εφαρμογή της ΚΠ. Το θεσμικό πλαίσιο είναι επαρκές προκειμένου να εξασφαλίζεται η διαχείριση και επεξεργασία των δεδομένων, υπό την ικανοποίηση των αρχών της αναλογικότητας και διαφάνειας με σεβασμό στην ιδιωτικότητα του πολίτη.

Σχετικά με το απόρρητο, το πιο ουσιαστικό συμπέρασμα είναι η στάθμιση του ιδιωτικού και δημόσιου συμφέροντος. Οποιαδήποτε λύση αξιολογηθεί για την εφαρμογή της ΚΠ στην Ελλάδα οφείλει να υπακούει σε αυτό το πλαίσιο.

Εντούτοις, στο θεσμικό πλαίσιο του απορρήτου παρατηρείται νομικό κενό, καθώς η στάθμιση του δικαιώματος της ιδιωτικότητας απέναντι στο δημόσιο συμφέρον, σε περιπτώσεις εγκλημάτων ή ενδεχόμενων εγκλημάτων δεν έχει διακριτά όρια και επομένως δεν αποτελεί εύκολη υπόθεση.

Στην πράξη, η εξιχνίαση εγκλημάτων (για παράδειγμα παιδική πορνογραφία), πιθανά προϋποθέτει άρση απορρήτου για ένα σύνολο πολιτών (για παράδειγμα έλεγχος ενός συνόλου από IPs), που πιθανά δεν έχει καμία απολύτως σχέση με την υπόθεση που μας αφορά, ωστόσο προκειμένου να διαπιστωθεί η πράξη είναι απαραίτητη από τις αστυνομικές αρχές ο έλεγχος του. Από την άλλη πλευρά, οι αρχές προστασίας προσωπικών δεδομένων οφείλουν να παρεμποδίζουν τέτοιου εύρους εκτεταμένες έρευνες, οι οποίες παραβιάζουν κατάφορα το δικαίωμα του πολίτη στην ιδιωτικότητα.

Ποιος μπορεί σε αυτή την περίπτωση να «σταθμίσει» το όριο ιδιωτικού και δημόσιου συμφέροντος;

3.6. Θεσμικό Πλαίσιο Ελληνικών Ταυτοτήτων

Το θεσμικό πλαίσιο της ταυτότητας του πολίτη στην Ελλάδα συνοψίζεται στις εξής νομοθετικές παρεμβάσεις:

1. Κώδικας Διοικητικής Διαδικασίας ΚΔΔσίας/ν. 2690/99
2. Ν.Δ. 127 της 17/18.2.1969- (Α` 29), «Περί αποδεικτικής ισχύος των Αστυνομικών Ταυτοτήτων»
3. Ν.3345/2005 (ΦΕΚ Α 138/16.6.2005).
4. Ν.1599 /1986 (ΦΕΚ-Α 75/11-6-1986) Σχέσεις κράτους-πολίτη, καθιέρωση νέου τύπου δελτίου ταυτότητας και άλλες διατάξεις
5. ΥΑ 3021/19/53/2005 ΦΕΚ Β' 1440/18.10.2005 για τον καθορισμού του Δελτίου ταυτότητας (ΥΑ 3021/19/53–ζ΄ 2009, ΦΕΚ Β΄ 1440/2009 Τροποποίηση της υπ' αριθμ. ΚΥΑ 3021/19/53 από 14.10.2005 κοινής υπουργικής απόφασης των Υπουργών Οικονομίας και Οικονομικών και Δημόσιας Τάξης όπου καθορίζονται «Τύπος, δικαιολογητικά, αρμόδιες υπηρεσίες και διαδικασία έκδοσης δελτίων ταυτότητας Ελλήνων πολιτών»). Οι τροποποιήσεις της παρούσας έχουν ήδη ενσωματωθεί στην 3021/19/53/2005 Υ.Α.
6. ΥΑ 21385/11246

Στην χώρα μας, η έντυπη ταυτότητα είναι υποχρεωτική για όλους τους Έλληνες πολίτες άνω των 12 ετών σύμφωνα με το άρθρο 1, παράγραφος 1 του Ν. 127/1969, όπως αντικαταστάθηκε από την παράγραφο 3 του άρθρου 13 του Ν.3345/2005 (ΦΕΚ Α 138/16.6.2005) που ορίζει ως εξής αυτή την υποχρέωση: «Έλληνες πολίτες που κατοικούν ή διαμένουν προσωρινά στην Ελλάδα και έχουν συμπληρώσει το 12ο έτος της ηλικίας τους υποχρεούνται να εφοδιασθούν με δελτίο αστυνομικής ταυτότητας, το οποίο εκδίδεται ατελώς, κατά τις διατάξεις του παρόντος νομοθετικού διατάγματος. Κατ' εξαίρεση οι στρατιωτικοί των Ενόπλων Δυνάμεων και του Λιμενικού Σώματος, το αστυνομικό προσωπικό, οι συνοριακοί φύλακες, οι ειδικοί φρουροί, καθώς και το πυροσβεστικό προσωπικό του Πυροσβεστικού Σώματος που τελούν στην ενέργεια ή σε πολεμική ή μόνιμη διαθεσιμότητα εφοδιάζονται μόνο με ειδικά δελτία ταυτότητας που χορηγούνται από την Υπηρεσία τους.».

Σύμφωνα με το άρθρο 3 παρ.3 και 4 του Κώδικα Διοικητικής Διαδικασίας , αποτελεί νόμιμο αποδεικτικό μέσο των στοιχείων της ταυτότητας του ατόμου κατά τις συναλλαγές του με το Δημόσιο ενώ, όπως και στις άλλες ευρωπαϊκές χώρες που εξετάσαμε, μπορεί να χρησιμοποιηθεί και ως επίσημο ταξιδιωτικό έγγραφο εντός της Ε.Ε. Η χρονική ισχύς της ταυτότητας είναι 15 έτη από την έκδοσή της, ωστόσο δεν προβλέπεται ημερομηνία λήξης, το οποίο συνεπάγεται ότι στην πράξη, η ανανέωσή της δε συνηθίζεται. Για αλλοδαπούς που μένουν μόνιμα στην χώρα δεν προβλέπεται έκδοση τέτοιας ταυτότητας αλλά έντυπης κάρτας παραμονής, σύμφωνα με τη νόμιμη διαδικασία απόκτησης «νόμιμης διαμονής (Ν..3386/2005) .

3.6.1. Στοιχεία και Διαδικασία Έκδοσης ΑΔΤ

Το βασικό νομοθετικό πλαίσιο που διέπει τις προϋποθέσεις και την διαδικασία έκδοσης ταυτότητας στη χώρα μας είναι το Ν.Δ. 217/1969 και η υπουργική απόφαση υπ'αριθμ.3021/19/53 «Τύπος, δικαιολογητικά, αρμόδιες υπηρεσίες και διαδικασία έκδοσης δελτίων ταυτότητας Ελλήνων πολιτών» (ΦΕΚ Β' 1440/18-10-2005).

Χαρακτηριστική είναι επίσης και η πορεία των δεδομένων που περιλαμβάνει η Ελληνική Αστυνομική Ταυτότητα. Αρχικά, ο Νόμος 1599/1986 (ΦΕΙΚ Α 75) καθόριζε την υποχρέωση έκδοσης δελτίου από το 12ο έτος, ότι τα δελτία θα εκδίδονται από τις Νομαρχίες, προέβλεπε την προαιρετική αναγραφή του θρησκεύματος του κατόχου και επίσης καθιέρωνε τον ισόβιο 13ψήφιο ενιαίο κωδικό ΕΚΑΜ, ο οποίος θα ενοποιούσε τα υπόλοιπα μητρώα (καθώς θα περιελάμβανε τον ειδικό εκλογικό αριθμό, του διαβατηρίου, της ταυτότητας, τον ΑΜΚΑ, τον ΑΦΜ και του διπλώματος οδήγησης). Ο ΕΚΑΜ στην ουσία δεν εφαρμόστηκε ποτέ, καθώς συνέχισαν να εκδίδονται παλαιού τύπου δελτία βάσει του Ν.Δ. 127/1969, ενώ ο ΕΚΑΜ στη συνέχεια καταργήθηκε από το Ν. 1988/1991 (ΦΕΚ Α 189), ο οποίος επίσης επανέφερε την υποχρεωτική αναγραφή του θρησκεύματος και θέσπισε την προαιρετική αναγραφή (ΔΙΟΣ) Δωρητής Ιστών και Οργάνων Σώματος. Συνολικά, ο Ν. 1599/1986 δέχτηκε μεγάλο αριθμό τροποποιήσεων από τους Ν. 1832/1989, Ν. 1839/1989, Ν. 1988/1991, Ν. 2479/1997, Ν. 2521/1997, Ν. 2690/1999, Ν. 2990/2002, Ν. 3242/2004, Υ.Α. 3021/19/53/2005 και πρόσφατη τροποποίηση της ΦΕΚ Β' 1253/25.6.2009.

Με την Υπουργική Απόφαση 21385/11246 καθορίζεται ο τύπος και οι προδιαγραφές του δελτίου της Ελληνικής Αστυνομικής Ταυτότητας που χρησιμοποιούμε σήμερα (ΦΕΙΚ 421/Β/02.07.1992). Στο ΦΕΙΚ αυτό καθορίζονται οι τεχνικές εκτύπωσης κ.λπ. που αφορούν τη φυσική ασφάλεια του εγγράφου. Χαρακτηριστικό είναι ότι στο άρθρο 1 προβλέπει ότι το έντυπο θα φέρει ειδική λευκή λωρίδα πλάτους 16 χιλιοστών στο κάτω μέρος της πρόσθιας όψης, προοριζόμενη να χρησιμοποιηθεί για μηχανική οπτική αναγνώριση, κάτι που, ωστόσο, δεν εφαρμόστηκε.

Σήμερα, ο τύπος του Δελτίου Ταυτότητας έχει μεταβληθεί και ισχύει αυτός που καθορίζεται στην Υπουργική Απόφαση [ΥΑ3021/2005] (ΦΕΚ Β' 1440/18.10.2005). Φυσικά στα πλαίσια της διασφάλισης της ιδιωτικότητας, η αναγραφή του θρησκεύματος έχει καταργηθεί. Για την έκδοση υποβάλλεται αυτοπροσώπως στην αρμόδια αστυνομική αρχή ειδική αίτηση, τα στοιχεία της οποίας αντλούνται από πιστοποιητικό του δήμου ή της κοινότητας, στο δημοτολόγιο του οποίου είναι εγγεγραμμένος ο αιτών. Ενώ μέχρι πρότινος επρόκειτο για πρωτότυπο πιστοποιητικό που παρουσίαζε ο ενδιαφερόμενος, με την τροποποίηση του ΦΕΚ Β' 1253/25.6.2009 αναζητείται πλέον από την αρχή έκδοσης του δελτίου αυτεπάγγελτα από τον οικείο δήμο ή κοινότητα.

Σύμφωνα με την ισχύουσα νομοθεσία, τα δεδομένα που αναγράφονται στην ταυτότητα είναι: επώνυμο, όνομα, όνομα πατέρα, επώνυμο πατέρα, όνομα μητέρας, επώνυμο μητέρας, ημερομηνία γέννησης, τόπος γέννησης, ύψος, δήμος ή κοινότητα δημοτολογίου, αριθμός οικογενειακής μερίδας, ιθαγένεια και, εθελοντικά, ομάδα αίματος του κατόχου . Ως προς τα πρόσθετα δεδομένα που δεν αναγράφονται πλέον, τεκμαίρεται ότι η σχετική πρόβλεψη έχει σιωπηρώς καταργηθεί. Από αυτά, το επώνυμο, το όνομα και το όνομα πατέρα αναγράφονται και με λατινικούς χαρακτήρες με μεταγραφή, κατά το πρότυπο ΕΛΟΤ

743 (αντίστοιχο του διεθνούς ISO 843:1997). Παρέκκλιση από το πρότυπο μπορεί να υπάρξει μόνο με αίτημα του ενδιαφερομένου και τότε τα στοιχεία αναγράφονται όπως σε προηγούμενο ταξιδιωτικό ή άλλο έγγραφο ημεδαπής ή αλλοδαπής αρχής. Τα στοιχεία ταυτότητας του αιτούντος βεβαιώνονται από ένα μάρτυρα. Ο αρμόδιος υπάλληλος της αστυνομικής αρχής έκδοσης ερευνά στο κεντρικό αρχείο ταυτοτήτων που τηρείται από τη Διεύθυνση Κρατικής Ασφάλειας του Αρχηγείου Ελληνικής Αστυνομίας για τυχόν ύπαρξη προηγούμενου δελτίου ταυτότητος στο όνομα του ενδιαφερομένου.

Ο προσδιορισμός των δεδομένων που αναγράφονται στα δελτία ταυτότητας αποτέλεσε νομικό αλλά και κοινωνικό ζήτημα στις αρχές της προηγούμενης δεκαετίας. Αφορμή στάθηκε η απόφαση 510/17/2000 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, με την οποία κρίθηκε μη συνάδουσα με την αρχή του σκοπού και της αναγκαιότητας και προσφορότητας των μέσων η συλλογή και επεξεργασία δεδομένων που αναγράφονταν έως τότε και αφορούσαν : όνομα και επώνυμο συζύγου, γένος, επάγγελμα, διεύθυνση κατοικίας, υπηκοότητα, θρήσκευμα και συλλογή δακτυλικού αποτυπώματος. Η απόφαση προέβη σε μια εύστοχη στάθμιση σκοπού - μέσων, θεωρώντας πολλά από τα έως τότε στοιχεία ταυτότητας μη αναγκαία , κάνοντας, μάλιστα μνεία και σε πρακτική που συμβάλει σε κοινωνικό διαχωρισμό (profiling).

Εφαρμογή βρίσκει και ο Ν.2472/1997 περί προστασίας δεδομένων προσωπικού χαρακτήρα, αφού τέτοια δεδομένα συλλέγονται και αναγράφονται στα δελτία ταυτότητας του Έλληνα πολίτη .

Είναι φανερό ότι ο νομοθέτης προσπάθησε να σταθμίσει την εξυπηρέτηση του σκοπού ταυτοποίησης και αυθεντικοποίησης του πολίτη με την νομοθεσία και νομολογία περί προστασίας προσωπικών δεδομένων. Το αποτέλεσμα κρίνεται κατά βάση ικανοποιητικό και δεν μπορούμε παρά να αναγνωρίσουμε ότι η συζήτηση σχετικά με τα προσωπικά δεδομένα στο δελτίο ταυτότητας αποτέλεσε σταθμό για την εξοικείωση του Έλληνα πολίτη με το πλαίσιο προστασίας προσωπικών δεδομένων, προσδίδοντας έντονο κοινωνικό ενδιαφέρον σε ζητήματα νομικής προστασίας που δύσκολα θα κέντριζαν την προσοχή της κοινής γνώμης.

3.6.2. Αντικατάσταση ΑΔΤ

Ακύρωση του δελτίου ταυτότητας ή Αντικατάσταση μπορεί να γίνει όταν:

3. επέλθει μεταβολή οποιουδήποτε στοιχείου της ταυτότητας του κατόχου, όπως ορίζεται στο άρθρο 6 ν.δ. 127/1969,
4. λόγω μη αναγραφής στο δελτίο ταυτότητας της ιθαγένειας του κατόχου ή λόγω μη αναγραφής των στοιχείων του κατόχου με λατινικούς χαρακτήρες,
5. λόγω φθοράς,
6. λόγω παρέλευσης του χρόνου ισχύος του (τροποποίηση με το ΦΕΚ Β' 1253/25.6.2009, προηγούμενα ήταν δεκαετίας από την έκδοσή του),
7. λόγω απώλειας ή κλοπής.

Για την αντικατάσταση δελτίου ταυτότητας υποβάλλονται τα δικαιολογητικά και ακολουθείται η διαδικασία που προβλέπεται για την αρχική έκδοση, ενώ επιπλέον

υποβάλλεται το παλαιό δελτίο ταυτότητας, με εξαίρεση τις περιπτώσεις κλοπής ή απώλειας. Σε περίπτωση απώλειας ή κλοπής δελτίου ταυτότητας, ο δικαιούχος αυτού οφείλει να υποβάλει αμέσως υπεύθυνη δήλωση στην αστυνομική ή προξενική αρχή του τόπου διαμονής ή κατοικίας του της περιφέρειας στην οποία έλαβε χώρα η απώλεια ή η κλοπή και να παράσχει κάθε πληροφορία που να αποδεικνύει το βάσιμο των ισχυρισμών του.

Τα έντυπα δελτίου ταυτότητας και αιτήσεων αποτελούν υλικό του Ελληνικού Δημοσίου. Ο υπάλληλος που παραλαμβάνει και διαχειρίζεται τα έντυπα αυτά καθίσταται υπόλογος για τη χρήση τους σύμφωνα με τις ισχύουσες διατάξεις. Για κάθε απώλεια ή φθορά σε έντυπο δελτίου ταυτότητας υποβάλλεται λεπτομερής αναφορά στη Δ.Κ.Α./Α.Ε.Α. Από την κατά τόπο αρμόδια Διεύθυνση Ασφαλείας ή Αστυνομική Διεύθυνση ενεργείται ένορκη διοικητική εξέταση (Ε.Δ.Ε.), σύμφωνα με τις ισχύουσες διατάξεις και επιβάλλονται κυρώσεις κατά παντός υπαιτίου. Επιπλέον, από τις οικείες διαχειρίσεις καταλογίζεται σε βάρος των υπαιτίων η αξία των εντύπων. Τα έντυπα δελτίων ταυτότητας που υπέστησαν φθορά καταστρέφονται από τριμελή επιτροπή βαθμοφόρων, εκ των οποίων ο ένας τουλάχιστον είναι αξιωματικός, που συγκροτείται από την αρχή έκδοσης μετά το πέρας της Ε.Δ.Ε. και τον καταλογισμό της αξίας του. Η επιτροπή αυτή συντάσσει σχετικό πρακτικό εις τριπλούν, από τα οποία ένα παραμένει στο αρχείο της αρχής έκδοσης, ένα υποβάλλεται στην οικεία Διαχείριση Υλικού και ένα στην κατά τόπο αρμόδια Διεύθυνση Ασφαλείας ή Υποδιεύθυνση ή Τμήμα Ασφαλείας της έδρας της Αστυνομικής Διεύθυνσης. Τα έντυπα των δελτίων ταυτότητας που από την εκτύπωσή τους δεν πληρούν τις προϋποθέσεις για περαιτέρω χρήση υποβάλλονται με σχετική αναφορά στην Δ.Κ.Α./Α.Ε.Α. Οι παραπάνω διαδικασίες αποτελούν μια ένδειξη για τα μέτρα ασφάλειας που θα πρέπει να τηρούνται και στην περίπτωση της ΚΠ.

3.6.3. Χρήση της ταυτότητας ως ταξιδιωτικού εγγράφου

Η ισχύουσα νομοθεσία για την χρησιμοποίηση της ταυτότητας ως ταξιδιωτικό έγγραφο συνοψίζεται στις ακόλουθες νομοθετικές πράξεις:

1. Π.Δ. 308/1991 επικαλούμενο τις οδηγίες 68/360/ΕΟΚ και 73/148/ΕΟΚ, ορίζει στο άρθρο 1 ότι «Το Διάταγμα αυτό εκδίδεται με σκοπό την προσαρμογή της ισχύουσας Ελληνικής νομοθεσίας στο Κοινοτικό Δίκαιο όσον αφορά τη διακίνηση των Ελλήνων πολιτών στα Κράτη- Μέλη της Ε.Ο.Κ.» και στην παράγραφο 1 του άρθρου 2 ό τι «Οι Έλληνες πολίτες, κατά τη διακίνησή τους σε Κράτη - Μέλη των Ευρωπαϊκών Κοινοτήτων μπορούν να χρησιμοποιούν ως ταξιδιωτικό έγγραφο είτε το εν ισχύ δελτίο ταυτότητάς τους είτε εν ισχύ διαβατήριο». (ολομέλεια του ΣτΕ 2281/2001)
2. ΕΚ 562/2006 Συνθήκη Schengen (Schengen Borders Code) σύμφωνα με τις διατάξεις της οποίας δεν διενεργείται συνοριακός έλεγχος προσώπων κατά τη διέλευση των εσωτερικών συνόρων μεταξύ κρατών μελών της Ευρωπαϊκής Ένωσης (άρθρα 1, 20 και 21).
3. ΕΚ 2252/2004 [26] σχετικά με την καθιέρωση προτύπων για τα χαρακτηριστικά ασφαλείας και τη χρήση βιομετρικών στοιχείων στα διαβατήρια και τα ταξιδιωτικά

έγγραφα των κρατών μελών, λαμβάνοντας υπόψη τις προδιαγραφές του Οργανισμού Διεθνούς Πολιτικής Αεροπορίας ICAO (International Civil Aviation Organization) [65] και ιδίως εκείνες που ορίζονται στο έγγραφο Doc 9303 [87] [88] σχετικά με τα αναγνώσιμα από μηχάνημα ταξιδιωτικά έγγραφα, θέσπισε εγγυήσεις ως προς την τήρηση των ελάχιστων προτύπων ασφαλείας που πρέπει να πληρούν τα διαβατήρια και τα ταξιδιωτικά έγγραφα των κρατών μελών.

4. ΕΚ 444/2009 [27] επικαιροποίηση του ΕΚ 2252/2004 με θέσπιση εξειδικευμένων ρυθμίσεων περί εφαρμογής βιομετρικών στοιχείων στα διαβατήρια και τα ταξιδιωτικά έγγραφα των κρατών μελών. Η λήψη δακτυλικών αποτυπωμάτων ως βιομετρικών στοιχείων στα διαβατήρια και τα ταξιδιωτικά έγγραφα των Κρατών Μελών καθίσταται υποχρεωτική από τον Ιούνιου του 2012.

Η χρήση της αστυνομικής ταυτότητας ως ταξιδιωτικού εγγράφου εντός κρατών μελών της Ε.Ε. εξασφαλίζεται μέσω της συμμετοχής της Ελλάδας στη Συνθήκη Schengen (Schengen Borders Code), κανονισμός 562/2006, αν και η κατάργηση του ελέγχου των εσωτερικών συνόρων δεν θίγει την άσκηση αστυνομικών αρμοδιοτήτων, υπό την προϋπόθεση ότι η άσκηση των αρμοδιοτήτων αυτών δεν έχει αποτέλεσμα ισοδύναμο με συνοριακούς ελέγχους και, συνεπώς, εφόσον υπάρξουν ενδείξεις κινδύνου για τη δημόσια ασφάλεια ή δειγματοληπτικά οι αρχές ασφαλείας διενεργούν αστυνομικό έλεγχο. Λόγω της πρόβλεψης στη Συνθήκη για μη ισοδύναμο αποτέλεσμα μεταξύ των αστυνομικών ελέγχων που δύνανται να πραγματοποιούνται και των συνοριακών ελέγχων που καταργούνται στο εσωτερικό της επικράτειας, κατά τη διενέργεια αστυνομικού ελέγχου στους έχοντες ιθαγένεια Κράτους Μέλους αρκεί η χρήση αστυνομικής ταυτότητας και δεν απαιτείται η χρήση διαβατηρίου ή ταξιδιωτικού εγγράφου.

Επιπλέον, σύμφωνα με τις διατάξεις του ΕΚ 2252/2004 [26], τα ταξιδιωτικά έγραφα πρέπει να έχουν συγκεκριμένα χαρακτηριστικά ασφαλείας και να φέρουν μεταξύ άλλων περιοχή μηχανικής ανάγνωσης (MRZ) και τσιπ (chip) με ψηφιοποιημένη τη φωτογραφία προσώπου του κατόχου. Συνεπώς, σύμφωνα με την εφαρμοστέα Κοινοτική νομοθεσία, μετά την πάροδο της προθεσμίας, εκδοθείσες ΑΤ, που δεν πληρούν τις προβλεπόμενες απαιτήσεις ασφαλείας και τις προδιαγραφές του ICAO [65], δεν επιτρέπεται να χρησιμοποιούνται ως ταξιδιωτικά έγγραφα. Παρόλα αυτά, για τα έγγραφα ταυτότητας που εκδίδουν τα κράτη μέλη για τους πολίτες τους δεν απαιτείται προσαρμογή (άρθρο 1 παρ.3).

Αντίστοιχα, θα μπορούσε να χρησιμοποιηθεί και η ΚΠ για ταυτοποίηση εντός των εσωτερικών συνόρων κρατών μελών της Συνθήκης Schengen, όπου και δεν ασκείται συνοριακός έλεγχος των προσώπων. Σε αυτήν την περίπτωση, δεν είναι απαραίτητη η εξασφάλιση των χαρακτηριστικών ασφαλείας των ταξιδιωτικών εγγράφων και δεν είναι επιβεβλημένη η χρήση δακτυλικών αποτυπωμάτων. Για την χρήση της εκτός Schengen, πρέπει να συμμορφώνεται με τη σχετική Κοινοτική νομοθεσία και να φέρει χαρακτηριστικά και προδιαγραφές ασφαλείας κατά ICAO [65].

3.7. Πιστοποιητικό γέννησης

Το πιστοποιητικό γέννησης εκδίδεται από τον Δήμο, όπου είναι εγγεγραμμένος ο πολίτης (άρθρο 86 παρ. 1 ζ΄ και 106 παρ. 1 ζ΄ ΔΚΚ/ν. 3463/2006). Το πιστοποιητικό αυτό μπορεί να ζητηθεί και τηλεφωνικώς στο 1502 (άρθρο 22 παρ. 1 β΄ ν. 2539/1997 και ΥΑ ΔΙΣΚΠΟ/Φ.29/2145 ΦΕΚ Β' 58/30.1.1998).

Πρέπει να σημειωθεί ότι η βεβαίωση στοιχείων, αν αυτά δεν είναι δυνατό να προκύψουν με άλλο τρόπο, όπως για παράδειγμα από το Ληξιαρχείο, είναι δυνατό να επιτευχθεί δικαστικώς, με τη διαδικασία της εκούσιας δικαιοδοσίας (άρθρο 782). Η εκούσια δικαιοδοσία αποτελεί ένδικη προστασία χωρίς την ύπαρξη προϋφιστάμενης διαφορά. Μοιάζει πιο πολύ με διοικητική παρά με δικαστική διαδικασία, αφού δεν υπάρχει αντιδικία. Η «αίτηση βεβαίωσης στοιχείων» αποτελεί τρόπο πιστοποίησης γεγονότων που αφορούν την προσωπική κατάσταση φυσικού προσώπου, δηλ. τη γέννηση, ονοματοδοσία, γάμο, θάνατο κλπ. Η αίτηση υποβάλλεται οποτεδήποτε, δηλ. χωρίς χρονικό περιορισμό, από οποιοδήποτε πρόσωπο έχει έννομο συμφέρον (ή και τον Εισαγγελέα), όταν πρόκειται να ασκηθεί κάποιο δικαίωμα (π.χ. συνταξιοδότηση) ή υπάρχει ανάγκη για βεβαιότητα και ακρίβεια της σχετικής ληξιαρχικής πράξης ως προς την προσωπική κατάσταση του ατόμου. Αρμόδιο δικαστήριο είναι το Μονομελές Πρωτοδικείο. Η απόφαση, ως προς το γεγονός που βεβαιώνει, είναι δεσμευτική.

3.8. Απόδοση Α.Φ.Μ.

Το άρθρο 31 του Ν. 2515/1997 (Α` 54) προβλέπει την υποχρεωτική χορήγηση Αριθμού Φορολογικού Μητρώου σε όλα τα φυσικά και νομικά πρόσωπα καθώς και στις ενώσεις προσώπων που έχουν την κατοικία τους ή την επαγγελματική τους εγκατάσταση στην Ελλάδα ή διενεργούν σε αυτήν πράξεις φορολογικού ενδιαφέροντος. Το ίδιο άρθρο εξουσιοδοτεί τον Υπουργό Οικονομικών να καθορίσει με απόφασή του την διαδικασία χορήγησης του ΑΦΜ, την αρμόδια δημοσία οικονομική υπηρεσία και κάθε αναγκαία σχετική λεπτομέρεια (ΣτΕ 2560/2004). Η απόδοση Αριθμού Φορολογικού Μητρώου(ΑΦΜ) ρυθμίζεται από την Υ.Α. 1027411/842/ΔΜ/26.2.1998 (ΦΕΚ Β΄-193) και χορηγείται υποχρεωτικά (άρθρο 2) σε μια σειρά από κατηγορίες προσώπων.

Ο ΑΦΜ είναι ένας ευρέως χρησιμοποιούμενος μοναδικός αριθμός που αποδίδεται σε κάθε συναλλασσόμενο και τον ταυτοποιεί μοναδικά με βάση τα ατομικά του στοιχεία. Δικαίωμα να αποκτήσουν ΑΦΜ έχουν όλα τα φυσικά πρόσωπα, ημεδαπά ή αλλοδαπά, που κατοικούν στην Ελλάδα. Ο ΑΦΜ αποτελεί βασική προϋπόθεση για μια σειρά οικονομικών συναλλαγών, ωστόσο προϋποθέτει τουλάχιστον την ενηλικίωσή του και επίσης δεδομένου ότι δίνει πρόσβαση σε ένα πλήθος συναλλαγών μπορεί να χρησιμοποιηθεί κακόβουλα.

Υποχρέωση να αποκτήσουν ΑΦΜ έχουν τα ημεδαπά ή αλλοδαπά φυσικά πρόσωπα που είναι ή πρόκειται να γίνουν επιτηδευματίες, μισθωτοί πριν τη πρόσληψή τους, είναι υπόχρεοι σε υποβολή δήλωσης Φορολογίας Εισοδήματος, αποκτούν περιουσιακά στοιχεία που προσδιορίζουν τεκμήριο, ζητούν Αποδεικτικό Φορολογικής Ενημερότητας, Πιστοποιητικά ή Βεβαιώσεις από την ΔΟΥ, πρέπει να υποβάλλουν δηλώσεις Κεφαλαίου

(λόγω απόκτησης περιουσιακών στοιχείων κλπ), είναι μέλη, εταίροι ή σχετιζόμενοι με επιχειρήσεις (Ο.Ε, Ε.Ε., ΕΠΕ, Α.Ε. κλπ), είναι εκπρόσωποι φορολογουμένων και διενεργούν πράξεις φορολογικού ενδιαφέροντος αντ' αυτών.

Για την απόδοση ΑΦΜ υποβάλλεται στην αρμόδια ΔΥΟ το έντυπο «Απόδοσης ΑΦΜ/Μεταβολής ατομικών στοιχείων» όπου δηλώνονται:

α) τα προσωπικά στοιχεία του υπόχρεου, δηλαδή, όνομα, επώνυμο, πατρώνυμο, μητρώνυμο, ημερομηνία και τόπος γέννησης, β) στοιχεία ταυτότητας, γ) υπηκοότητα, επάγγελμα και οικογενειακή κατάσταση, δ) διεύθυνση κατοικίας και αλληλογραφίας.

Με τη δήλωση απόδοσης ΑΦΜ υποβάλλεται από τον υπόχρεο και το έντυπο «Δήλωση Σχέσεων Φορολογουμένου», όπου σύμφωνα με το άρθρο 3 παρ. 1 του Κώδικα Διοικητικής Διαδικασίας (ΚΔΔσίας/ν. 2690/99) «αίτηση του ενδιαφερόμενου, για την έκδοση διοικητικής πράξης, απαιτείται όταν το προβλέπουν οι σχετικές διατάξεις».

3.9. Θεσμικό Πλαίσιο Ελληνικών Διαβατηρίων

Το θεσμικό πλαίσιο για την έκδοση διαβατηρίου στην Ελλάδα συνοψίζεται στις εξής νομοθετικές παρεμβάσεις:

1. Ν. 3103/2003 (ΦΕΚ Α'/23/29.1.2003)
2. Υ.Α. 3021/2005 και η πρόσφατη τροποποίησή της Υ.Α. 3021/2010 που καθορίζει τα δικαιολογητικά και τη διαδικασία έκδοσης

Στην ΥΑ 3021 καθορίζεται ότι για την έκδοση διαβατηρίου υποβάλλονται αυτοπροσώπως από τον ενδιαφερόμενο τα δικαιολογητικά στην αστυνομική διεύθυνση ή διεύθυνση αστυνομίας του τόπου κατοικίας του ή στο αστυνομικό τμήμα του τόπου κατοικίας του, εφόσον πρόκειται για κάτοικο νησιού, όπου δεν εδρεύουν οι προαναφερόμενες υπηρεσίες.

Ως «βασικό» δικαιολογητικό υποβάλλεται φωτοαντίγραφο των δύο όψεων του δελτίου ταυτότητας του ενδιαφερομένου. Προκειμένου για ανήλικο κάτω των 12 ετών υποβάλλεται πιστοποιητικό εγγραφής στα δημοτολόγια.

Σύμφωνα με την πρόσφατη τροποποίηση της [ΥΑ3021/2010], για την έκδοση Ελληνικών Διαβατηρίων ισχύουν πλέον τα κάτωθι άρθρα:

- Άρθρο 1, παράγραφος 4: «Η υπηρεσία παραλαβής των δικαιολογητικών λαμβάνει και κρυπτογραφεί δακτυλικά αποτυπώματα των δεικτών και των δύο χειρών του αιτούντος εκτός αν πρόκειται για ανήλικο κάτω των δώδεκα (12) ετών. Σε περίπτωση μόνιμης ή προσωρινής αδυναμίας λήψης δακτυλικού αποτυπώματος δείκτη λαμβάνεται κατά σειρά αποτύπωμα του αντίχειρα ή του μέσου ή του παράμεσου του ιδίου χεριού, ενώ στην περίπτωση μονόχειρα λαμβάνεται αποτύπωμα και δεύτερου δακτύλου από το υπάρχον χέρι, με την ίδια ως άνω σειρά. Η μόνιμη ή προσωρινή αδυναμία λήψης δακτυλικών αποτυπωμάτων

αποδεικνύεται με ιατρικό πιστοποιητικό, το οποίο φέρει την υπογραφή ιατρού αντίστοιχης ειδικότητας με την πάθηση που βεβαιώνεται.»

- Άρθρο 1, παράγραφος 5: «... Η κεντρική υπηρεσία έκδοσης διαβατηρίων, μετά την παραλαβή των δικαιολογητικών, εκδίδει, εφόσον συντρέχουν οι νόμιμες προϋποθέσεις, το διαβατήριο και το διαβιβάζει ταχυδρομικά με επιχείρηση παροχής υπηρεσιών ταχυδρομείου με την οποία έχει συμβληθεί το Αρχηγείο Ελληνικής Αστυνομίας στην οικεία αστυνομική υπηρεσία ή μέσω της αρμόδιας Υπηρεσίας του Υπουργείου Εξωτερικών στην οικεία Προξενική Αρχή όπου υποβλήθηκαν τα δικαιολογητικά, απ' όπου παραλαμβάνεται από τον ίδιο τον ενδιαφερόμενο ή από τα πρόσωπα που προβλέπονται στην παρ. 3 του άρθρου 1 ή από νόμιμα εξουσιοδοτημένο προς τούτο πρόσωπο. Μαζί με το διαβατήριο επιστρέφονται και τα σχετικά δικαιολογητικά, τα οποία τηρούνται στο αρχείο των υπηρεσιών παραλαβής για διάστημα έξι (6) ετών από την υποβολή τους. Δεν επιστρέφεται στις υπηρεσίες παραλαβής η κρυπτογραφημένη σελίδα με τα στοιχεία του κατόχου και τα δακτυλικά του αποτυπώματα, η οποία καταστρέφεται από τη Διεύθυνση Διαβατηρίων/Α.Ε.Α., αμέσως μετά την επεξεργασία τους. Διαβατήριο το οποίο δεν παραλαμβάνεται κατά τα ανωτέρω μέσα σε έξι (6) μήνες από την έκδοσή του επιστρέφεται στην κεντρική υπηρεσία και ακυρώνεται».
- Άρθρο 2: «Στο διαβατήριο περιλαμβάνονται επίσης η υπογραφή του κατόχου, εφόσον αυτός είναι άνω των δώδεκα (12) ετών, καθώς και ενσωματωμένο μέσο αποθήκευσης στο οποίο περιέχονται η φωτογραφία του κατόχου, τα στοιχεία που αναγράφονται στη μηχανικώς αναγνώσιμη ζώνη του διαβατηρίου και τα δακτυλικά αποτυπώματα, υπό μορφή που εξασφαλίζεται η διαλειτουργικότητα.»

Κατ' εξαίρεση, όταν για ενδιαφερόμενο συντρέχουν ιδιαίτερα σοβαροί λόγοι υγείας, που καθιστούν αδύνατη ή δυσχεραίνουν ουσιωδώς τη μετακίνησή του και αποδεικνύονται με ιατρικό πιστοποιητικό κρατικού νοσοκομείου, για την παραλαβή των δικαιολογητικών μεταβαίνει στον ενδιαφερόμενο υπάλληλος της Υπηρεσίας. Οι Έλληνες πολίτες που διαμένουν στο εξωτερικό μπορούν να υποβάλλουν τα δικαιολογητικά σε 151 Προξενικές Αρχές ανά την υφήλιο.

Επιπλέον, στη Διεύθυνση Διαβατηρίων λειτουργεί το 5ο Τμήμα Επείγουσας Έκδοσης και μεριμνά ώστε για ειδικές περιπτώσεις, η έκδοση του διαβατηρίου να πραγματοποιείται σε μία μόνο ημέρα. Αυτό συμβαίνει όταν συντρέχουν οι εξής λόγοι: Σοβαροί λόγοι υγείας που επιβάλλουν νοσηλεία στο εξωτερικό (ασθενής και συνοδός), θάνατος συγγενή εξ' αίματος ή εξ' αγχιστείας μέχρι δευτέρου βαθμού, τραυματισμός ή εξαφάνιση συγγενή δευτέρου βαθμού, καταστροφή περιουσίας του ενδιαφερομένου που βρίσκεται στο εξωτερικό.

3.10. Ενσωμάτωση Βιομετρικών Χαρακτηριστικών

Η Κοινοτική Νομοθεσία με τον ΕΚ 2252/2004 [26] και την τροποποίησή του (ΕΚ 444/2009 [27]), υποδεικνύει ότι στα διαβατήρια και ταξιδιωτικά έγγραφα που εκδίδουν τα κράτη-μέλη, πρέπει στο μέσο αποθήκευσης να περιέχονται η εικόνα προσώπου και δύο επίπεδα

δακτυλικά αποτυπώματα, υπό μορφή που να εξασφαλίζει διαλειτουργικότητα. Ορίζεται ακόμη ότι τα δεδομένα πρέπει να ενσωματώνονται με ασφαλή τρόπο και ότι το μέσο αποθήκευσης πρέπει να διαθέτει επαρκή χωρητικότητα και ικανότητα, προκειμένου να διασφαλίζεται η ακεραιότητα, η αυθεντικότητα και η εμπιστευτικότητα των δεδομένων. Η διαλειτουργικότητα εξασφαλίζεται με την αποθήκευσή τους με τη μορφή εικόνας. Διευκρινίζεται πάλι ότι αυτό δεν ισχύει επίσης για τα έγγραφα ταυτότητας που εκδίδουν τα κράτη-μέλη για τους υπηκόους τους (Άρθρο 1, Παρ 3 του ΕΚ 2252/2004 [26]).

Με τον ΕΚ 444/2009 θεσπίζονται πρόσθετες τεχνικές προδιαγραφές για τα διαβατήρια και ταξιδιωτικά έγγραφα, σύμφωνα με τα διεθνή πρότυπα, συμπεριλαμβανομένων ιδίως των συστάσεων του ICAO [65] [86] [87] [88]. Ειδικότερα ο ICAO, τονίζει ότι το μέσο αποθήκευσης των βιομετρικών πληροφοριών, εκτός των προδιαγραφών για την ασφάλειά του, οφείλει να περιλαμβάνει και μέτρα πρόληψης ενάντια στην μη εξουσιοδοτημένη πρόσβαση. Στον ίδιο κανονισμό διευκρινίζεται ότι η συλλογή και αποθήκευση βιομετρικών στοιχείων στο μέσο αποθήκευσης των διαβατηρίων και των ταξιδιωτικών εγγράφων γίνεται για τους σκοπούς της έκδοσής τους, με την επιφύλαξη οποιασδήποτε άλλης χρήσης ή αποθήκευσης των δεδομένων αυτών σύμφωνα με την εθνική νομοθεσία των κρατών μελών. Συνεπώς, το ζήτημα της δημιουργίας, διατήρησης και διαχείρισης βάσεων δεδομένων για την αποθήκευση των προαναφερόμενων δεδομένων υπάγεται αποκλειστικά στην εθνική νομοθεσία, παρέχοντας σχετική ελευθερία στα κράτη μέλη.

Η εθνική προσαρμογή στην οδηγία (ΥΑ 3021/2010), ορίζει ότι για την έκδοση Ελληνικών Διαβατηρίων λαμβάνονται και κρυπτογραφούνται δακτυλικά αποτυπώματα των δεικτών και των δύο χειρών του αιτούντος, εκτός αν πρόκειται για ανήλικο μικρότερο των δώδεκα ετών. Τα δικαιολογητικά που προσκομίζονται, διαβιβάζονται στην κεντρική υπηρεσία έκδοσης διαβατηρίων. Η κρυπτογραφημένη σελίδα με τα στοιχεία του κατόχου και τα δακτυλικά του αποτυπώματα, πρέπει να καταστρέφεται από τη Διεύθυνση Διαβατηρίων/Α.Ε.Α., αμέσως μετά την επεξεργασία τους. Στο τσιπ του διαβατηρίου ενσωματώνεται η φωτογραφία του κατόχου, τα στοιχεία που αναγράφονται στην αναγνώσιμη ζώνη και τα δακτυλικά αποτυπώματα, με μορφή ώστε να εξασφαλίζεται η διαλειτουργικότητα. Ωστόσο, εντύπωση προκαλεί το ότι δεν αναφέρει ρητώς ότι τα βιομετρικά δεδομένα δεν αποθηκεύονται κεντρικά.

Τα ίδια ισχύουν για τις άδειες διαμονής υπηκόων τρίτων χωρών (ΕΚ 380/2008 [25]), όπου προβλέπεται ότι το σχετικό έγγραφο πρέπει επίσης να περιλαμβάνει ανεπαφικό τσιπ, στο οποίο να αποθηκεύονται η εικόνα του προσώπου και δύο εικόνες δακτυλικών αποτυπωμάτων του κατόχου.

Εξαιτίας όμως του ΕΚ 562/2006, που προβλέπει ότι δε διενεργείται συνοριακός έλεγχος προσώπων κατά τη διέλευση των εσωτερικών συνόρων μεταξύ των κρατών-μελών της ΕΕ, και υπηκόους χωρών που έχουν συνάψει σχετικές εν ισχύ συμφωνίες με την ΕΕ, δεν απαιτείται χρήση διαβατηρίου ή ταξιδιωτικού εγγράφου ισοδύναμων χαρακτηριστικών ασφαλείας με το διαβατήριο.

Είναι, κατά συνέπεια, παραπάνω από προφανής η διαπίστωση ότι δεν υπάρχει σαφής υποχρέωση για την αναγραφή και αποθήκευση στην ΚΠ των απαιτούμενων στοιχείων για

διαβατήρια ή ταξιδιωτικά έγγραφα αν χρησιμοποιηθεί για τη διέλευση των πολιτών εντός των εσωτερικών συνόρων της ζώνης Σένγκεν. Ωστόσο, η πρακτική αυτή μπορεί να στοιχίσει σημαντικά στη διαλειτουργικότητα, αλλά και στην μη εφαρμογή χαρακτηριστικών ασφαλείας και πιθανά σε μια λύση με σύντομη ημερομηνία λήξης.

Στην κατεύθυνση αυτή, ο Νομικός Σύμβουλος του Κράτους κ. Δασκαλαντωνάκη, επισημαίνει ότι αναφορικά με τους παραπάνω κοινοτικούς κανονισμούς τίθεται στη διακριτική ευχέρεια της Ελληνικής Πολιτείας η απόφαση να συμπεριλάβει ή μη στην Κάρτα του Πολίτη τα βιομετρικά στοιχεία, δεδομένου ότι προορίζεται να αντικαταστήσει την αστυνομική ταυτότητα. Το μόνο πρόβλημα που θα προκύψει αφορά τη διέλευση από κράτη μέλη της Ε.Ε. τα οποία δε δεσμεύονται από την Συνθήκη Σένγκεν και διατηρούν δικαίωμα άσκησης ελέγχων κατά τη διέλευση των συνόρων τους. Σε αυτή την περίπτωση, προκειμένου να χρησιμοποιηθεί η ΚΠ θα πρέπει να ενσωματώνει όλα τα δεδομένα και χαρακτηριστικά ασφάλειας που αφορούν τα διαβατήρια ή ισοδύναμα ταξιδιωτικά έγγραφα.

Παρότι έχει προβλεφθεί η καταστροφή των βιομετρικών δεδομένων και άλλων στοιχείων και δικαιολογητικών που προσκομίζονται για την έκδοση εγγράφων ταυτοποίησης και ταξιδιωτικών εγγράφων, αίσθηση προκαλεί η απουσία διάταξης για την απαγόρευση της αποθήκευσης των βιομετρικών και λοιπών δεδομένων σε κεντρικό σημείο.

Αν επιθυμούμε να υλοποιήσουμε μια ΚΠ που θα μπορεί να χρησιμοποιηθεί πλήρως και χωρίς περιορισμούς ως ταξιδιωτικό έγγραφο είναι απαραίτητη η συμμόρφωση με την κείμενη νομοθεσία και τους κανονισμούς των διεθνών οργανισμών.

3.11. Σύνοψη Κεφαλαίου

Για την εφαρμογή της ΚΠ ένα από τα κρισιμότερα θέματα αποτελεί η αξιολόγηση της επάρκειας του ισχύοντος θεσμικού πλαισίου, ώστε να διαπιστωθούν νομικά κενά και η δυνατότητα παρεμβάσεων που θα καταστίσουν την εφαρμογή της ΚΠ πιο αποτελεσματική και πιο λειτουργική. Με τη μελέτη του θεσμικού πλαισίου παρατηρήσαμε ήδη ότι προκύπτουν κάποια ζητήματα, ανοιχτά προς επίλυση και ερμηνεία.

Είναι όμως ήδη σαφές, ότι οποιαδήποτε επιλογή κι αν ακολουθήσουμε για την εφαρμογή της ΚΠ στην Ελλάδα οφείλει να υπακούει στην ανάγκη στάθμισης του ιδιωτικού και δημόσιου συμφέροντος.

Στο σημείο αυτό, θα προσπαθήσουμε να συγκεντρώσουμε και να ομαδοποιήσουμε τις διατάξεις του νομικού πλαισίου που βρίσκουν άμεση ή έμμεση εφαρμογή στην ΚΠ και στην συνέχεια θα επιχειρήσουμε δικές μας ερμηνείες και προσεγγίσεις.

Νομική υποχρέωση για έκδοση και κατοχή ταυτότητας από κάθε Έλληνα πολίτη άνω των 12 ετών.

Συλλογή και διαχείριση δεδομένων (προσωπικών ή μη), που περιέχονται στην ΚΠ. Η προστασία των προσωπικών δεδομένων αποτελεί έναν από τους κρισιμότερους παράγοντες στην εφαρμογή της ΚΠ. Η ΚΠ πρέπει να ακολουθεί τις αρχές νομιμότητας και της διαφάνειας, του σκοπού και της αναλογικότητας , αλλά και την υποχρέωση ακρίβειας και επικαιροποίησης των δεδομένων που τηρούνται για τους σκοπούς της ΚΠ (άρθρο 4 εδ. α', β΄ και γ', Ν.2472/1997). Στην πλήρωση των απαιτήσεων αυτών, η εφαρμογή της ΚΠ θα συναντήσει δυσκολίες στην περίπτωση ενσωμάτωσης βιομετρικών στοιχείων, εξαιτίας του μόνιμου χαρακτήρα τους.

Επεξεργασία δεδομένων χωρίς την συγκατάθεση του υποκειμένου. Ο νομοθέτης προβλέπει, εντούτοις, ρητά ότι είναι δυνατή η συλλογή και επεξεργασία δεδομένων του κατόχου μιας ΚΠ, και δίχως την συγκατάθεσή του, όταν αυτό είναι αναγκαίο για λόγους δημοσίου συμφέροντος (άρθρο 5, παρ.2.δ' Ν.2742/1997). Ειδικότερα, η εν λόγω διάταξη ορίζει ότι κατ' εξαίρεση, η επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται και χωρίς συγκατάθεση του υποκειμένου όταν «είναι αναγκαία για την εκτέλεση έργου δημοσίου συμφέροντος ή έργου που εμπίπτει στην άσκηση δημοσίας εξουσίας και εκτελείται από δημόσια αρχή ή έχει ανατεθεί από αυτή είτε στον υπεύθυνο επεξεργασίας είτε σε τρίτο, στον οποίο γνωστοποιούνται τα δεδομένα». Ερμηνεύοντας τη συγκεκριμένη διάταξη, διαπιστώνουμε ότι βρίσκει απόλυτη εφαρμογή στην υπό εξέταση περίπτωση της εφαρμογής της ΚΠ στην Ελλάδα, καθώς μπορεί να καλύψει τόσο το οργανικό μας κριτήριο - τη δυνατότητα επεξεργασίας δηλαδή από κάποια δημόσια αρχή-, όσο και το λειτουργικό, - άσκηση δημόσιας εξουσίας και λόγοι δημοσίου συμφέροντος-, δυνατότητα που μπορεί μάλιστα να μεταβιβασθεί/ανατεθεί σε τρίτο από την αρμόδια δημόσια αρχή. Παρόλα αυτά, αναφορικά με τη δυνατότητα ανάθεσης της συλλογής και επεξεργασίας προσωπικών δεδομένων σε τρίτο, αξίζει να τονισθεί ότι αυτή προϋποθέτει αυστηρούς κανόνες επιλογής και δέσμευσης του τρίτου και απαιτεί εγγυήσεις ιδιαίτερα αυξημένης προστασίας των δεδομένων, καθώς ο όγκος και η σημασία των δεδομένων αυτών στην υπό μελέτη περίπτωση σχετίζονται άμεσα με ατομικά δικαιώματα του πολίτη. Επομένως, είναι απολύτως απαραίτητη η εξασφάλιση αυστηρών κανόνων πρόσβασης σε τέτοια δεδομένα.

Από τη νομική αυτή διάταξη προκύπτει ότι είναι εφικτή η συλλογή των δεδομένων του πολίτη για τους σκοπούς της εφαρμογής και χρήσης της ΚΠ και μάλιστα για τους σκοπούς άσκησης της εξουσίας της Δημόσιας Διοίκησης, δεν απαιτείται επιπλέον συγκατάθεση του κατόχου της ΚΠ, για συλλογή, επεξεργασία και χρήση των δεδομένων του. Πάντως, για τις περιπτώσεις επεξεργασίας που εμπίπτουν στη συνθήκη της ρητής συγκατάθεσης του υποκειμένου των δεδομένων, αυτά αφορούν τα δεδομένα συναλλαγών και την περίπτωση επεξεργασίας δεδομένων από ιδιωτικό φορέα.

Διασύνδεση αρχείων. Η διάταξη του άρθρου 8 Ν.2742/1997 σχετικά με τους όρους και τις προϋποθέσεις διασύνδεσης αρχείων βρίσκει εφαρμογή και στην ενδεχόμενη χρήση της ΚΠ για την Ελλάδα. Ωστόσο, η διασύνδεση πιθανά να επιτραπεί έπειτα από τη γνωστοποίηση και κατόπιν έγκρισης από την ΑΠΔΠΧ και φυσικά υπό την προϋπόθεση ότι κανένα από τα αρχεία δεν περιλαμβάνει ευαίσθητα προσωπικά δεδομένα. Η παράγραφος 3 εξάλλου, είναι σαφής και ορίζει ότι «αν ένα τουλάχιστον από τα αρχεία που πρόκειται να διασυνδεθούν περιέχει ευαίσθητα δεδομένα ή εάν η διασύνδεση έχει ως συνέπεια την αποκάλυψη

ευαίσθητων δεδομένων ή, εάν για την πραγματοποίηση της διασύνδεσης, πρόκειται να γίνει χρήση ενιαίου κωδικού αριθμού, η διασύνδεση επιτρέπεται μόνο με άδεια της Αρχής (άδεια διασύνδεσης)». Έχει σημασία, πάντως, να τονίσουμε ότι η διάταξη αυτή, αφορά, στη χρήση ενιαίου κωδικού αριθμού και την επεξεργασία του ως μέσου (κλειδιού) για την επίτευξη των σκοπών της διασύνδεσης αρχείων, αλλά όχι και στην τήρηση σε αρχείο και πρόσβαση για τέτοιους αριθμούς. Συνεπώς, κατόπιν έγκρισης της Αρχής, είναι δυνατή η χρήση κωδικού αριθμού, ως αναγνωριστικό της ΚΠ, το οποίο μπορεί να σχετισθεί με επιμέρους μητρώα για τους σκοπούς της χρήσης και λειτουργίας της ΚΠ. Η έγκριση της Αρχής παρέχεται και χωρίς τη συγκατάθεση του υποκειμένου (αρθρ.5παρ.2περ.δ'), όπως αναλύθηκε και παραπάνω.

Αρχή του σκοπού, της αναλογικότητας και της νόμιμης επεξεργασίας. Είναι απαραίτητο να διευκρινίσουμε ότι η υπαγωγή στην προαναφερόμενη διάταξη δεν πρέπει σε καμία περίπτωση να ερμηνευτεί ως απαλλαγή της υποχρέωσης για τήρηση των αρχών νόμιμης επεξεργασίας, σκοπού και αναλογικότητας (άρθρο 8παρ.4 Ν.2742/1997). Αντιθέτως, η νομοθεσία ορίζει ρητά την αναγκαιότητα στάθμισης μέσου – σκοπού. Αυτό σημαίνει, ότι προκειμένου να είναι επιτρεπτή και σύννομη η διασύνδεση αρχείων, πρέπει να αποδεικνύεται προηγουμένως η αναγκαιότητά της και να περιγράφεται με ακρίβεια ο σκοπός της. Στην κατεύθυνση αυτή, η όποια έγκριση αφορά αποκλειστικά και μόνο το λόγο για τον οποίο αιτήθηκε η διασύνδεση, το είδος των δεδομένων, καθώς και το χρονικό διάστημα για το οποίο η διασύνδεση απαιτείται, ακολουθώντας την αρχή της αναλογικότητας, που ορίζει ότι η επεξεργασία δεν πρέπει να υπερβαίνει τον απαραίτητο χρόνο για την εκπλήρωση του σκοπού της. Στην περίπτωση πάντως της ΚΠ, η εξυπηρέτηση σκοπών δημοσίου συμφέροντος ή άσκησης δημόσιας εξουσίας, δίνει τη δυνατότητα για ελαστικό ορισμό της χρονικής περιόδου, καθώς πρακτικά αυτή είναι μάλλον μη υπολογίσιμη και πιθανά έκτακτη. Συμπεραίνουμε, σε κάθε περίπτωση, ότι είναι δυνατή η διασύνδεση των επιμέρους μητρώων των φορέων για τους σκοπούς της εφαρμογής της ΚΠ, εφόσον πληρούνται οι παραπάνω προϋποθέσεις. Επειδή όμως το σύννομο, πιθανώς να μην είναι και επιθυμητό, μένει, να καταλήξουμε σχετικά με το αν αυτή είναι η ιδανική επιλογή για την εξασφάλιση της προστασίας των δεδομένων και της διασφάλισης της ιδιωτικότητας των πολιτών.

Ποια όμως είναι η κατάσταση στη χώρα μας;

Στην Ελλάδα, δεν προβλέπεται η χρήση ενιαίου μοναδικού αναγνωριστικού αριθμού για τις συναλλαγές του πολίτη με το κράτος, αλλά επιμέρους τομεακά αναγνωριστικά, ανά φορέα ή/και υπηρεσία. Η υφιστάμενη κατάσταση είναι μάλιστα συνταγματική επιλογή, ακολουθώντας τις αρχές τους Συντάγματος, περί αξίας του ανθρώπου (άρθρο 2παρ.1Σ) και το δικαίωμα προστασίας των δεδομένων του (άρθρο 9Α Σ), γεγονός που καθιστά την καθολική διασύνδεση αρχείων μη σύννομη. Κάτι τέτοιο σημαίνει ότι η εισαγωγή ενιαίου μοναδικού αναγνωριστικού αριθμού ως χαρακτηριστικού της ΚΠ, είναι μη επιθυμητή επιλογή, καθώς αυτή θα σήμαινε κατάργηση των τομεακών αναγνωριστικών και καθιστά δυνατή την αδιάκριτη και καθολική διασύνδεση αρχείων.

Στο ίδιο ακριβώς πλαίσιο, η Ελλάδα, σε αντίθεση με άλλες ευρωπαϊκές χώρες, δε διαθέτει Εθνικό Μητρώο για την τήρηση και καταχώρηση των δεδομένων των Ελλήνων πολιτών, αλλά επιμέρους μητρώα. Τέτοια μητρώα τηρούνται στις Δημόσιες υπηρεσίες που παρέχουν κεντρικές υπηρεσίες προς τους πολίτες και στις τοπικές αρχές, όπως οι Δήμοι που τηρούν για τους δημότες τους αρχεία και εκδίδουν πιστοποιητικά (π.χ. γεννήσεως), απαραίτητα για την έκδοση αστυνομικής ταυτότητας.

Συνεπώς, καταλήγουμε ότι η ΚΠ πρέπει να εφαρμοσθεί χωρίς δομικές αλλαγές στο νομικό και λειτουργικό πλαίσιο της Ελλάδας, καθώς η χρήση των τομεακών αναγνωριστικών και της τήρησης των επιμέρους μητρώων, που θα διασυνδέονται, κατά περίπτωση, με το μητρώο της ΚΠ, είναι μια ρεαλιστική επιλογή.

Όμως, το σημαντικότερο, ίσως, εμπόδιο που πρέπει να ξεπεράσει η ΚΠ, είναι τα όρια της χρήσης της σημερινής αστυνομικής ταυτότητας και της ιδιόχειρης υπογραφής. Μέχρι σήμερα, η ταυτότητα μπορούσε να ταυτοποιήσει τον πολίτη, σε συνδυασμό με τη φυσική του παρουσία για τις περιπτώσεις φυσικού ελέγχου. Επιπλέον, η ιδιόχειρη υπογραφή, μπορούσε να επιβεβαιώσει την αυθεντικότητα και την εγκυρότητα μιας πράξης. Τις δύο αυτές ανάγκες, πρέπει να καλύψει και η ΚΠ, χωρίς να είναι απαραίτητη η φυσική παρουσία του κατόχου της. Επομένως, ο πολίτης με τη χρήση της ΚΠ, τόσο στον πραγματικό, όσο και στον ψηφιακό κόσμο, πρέπει να μπορεί να ταυτοποιείται και να αυθεντικοποιείται μοναδικά, με αποτελεσματικό και ασφαλή τρόπο.

Σε σύνδεση με τα παραπάνω, ένα επιπλέον ζήτημα ασφάλειας και αυθεντικότητας, είναι η διαβίβαση αιτημάτων και πιστοποιητικών/εγγράφων με ηλεκτρονικά μέσα, χωρίς να απαιτείται απαραίτητα η χρήση προηγμένων ηλεκτρονικών υπογραφών. Ήταν όμως μέχρι σήμερα απαραίτητη άλλη πράξη επιβεβαίωσης της αυθεντικότητας του εγγράφου, έπειτα από την προσκόμιση ενός πρωτότυπου πιστοποιητικού σε κάποια δημόσια αρχή, από τον πολίτη; Η απάντηση είναι προφανώς όχι, εντούτοις, για εμάς το ζήτημα της εφαρμογής της ΚΠ στην Ελλάδα εκτιμάται ότι πρέπει να παρέχει περισσότερες εγγυήσεις. Προκειμένου να ξεπερασθεί το εμπόδιο της απουσίας της φυσικής παρουσίας του συναλλασσόμενου, επιπρόσθετοι μηχανισμοί και εγγυήσεις ασφάλειας πρέπει να ικανοποιούνται., καθώς και οι κίνδυνοι και οι απειλές από την ενδεχόμενη κακή ή/και μη εξουσιοδοτημένη χρήση της ΚΠ είναι αναμφισβήτητα μεγαλύτεροι και περισσότεροι.

Τέλος, πρέπει να επισημάνουμε ότι η υλοποίηση της Ελληνικής ΚΠ, υπό την χρήση της και ως ταξιδιωτικού εγγράφου, αλλά και υπό την εφαρμογή της σε ένα ευρύτερο Ευρωπαϊκό περιβάλλον, πρέπει να πληρούνται οι προϋποθέσεις που προκύπτουν από την κοινοτική νομοθεσία, τις προδιαγραφές και τα πρότυπα των διεθνών οργανισμών, καθώς επίσης και οι απαιτήσεις διαλειτουργικότητας.

4. ΕΥΡΩΠΑΙΚΗ ΚΑΡΤΑ ΠΟΛΙΤΗ ΚΑΙ ΔΙΑΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑ

Το σύγχρονο διασυνοριακό περιβάλλον υπαγορεύει την ανάγκη για συστήματα ταυτοποίησης και αυθεντικοποίησης σε διεθνές επίπεδο, τόσο στο φυσικό, όσο και στον ψηφιακό κόσμο. Για το λόγο αυτό, έχει γίνει αρκετή δουλειά σε διεθνές και ευρωπαϊκό επίπεδο, τόσο για την καθιέρωση προτύπων και προδιαγραφών για την εξασφάλιση ενός ασφαλούς, ευέλικτου και διαλειτουργικού περιβάλλοντος εφαρμογής της ΚΠ, όσο και στην ανασκόπηση της εφαρμογής λύσεων που σχετίζονται με την ηλεκτρονική ταυτοποίηση και τα συστήματα διαχείρισης ηλεκτρονικής ταυτότητας, προς αναζήτηση των βέλτιστων πρακτικών και προς αποφυγή αποτυχημένων μοντέλων εφαρμογής.

Ως εκ τούτου διαπιστώνουμε ότι, προκειμένου να διαμορφωθεί ολοκληρωμένη εικόνα για την ΚΠ, είναι καθοριστικής σημασίας η ανασκόπηση της ευρωπαϊκής εμπειρίας, ως προς τα πρότυπα, τις προδιαγραφές, τις υλοποιήσεις και τις πρακτικές που ακολούθησαν.

Παράλληλα όμως, στα πλαίσια της Ευρωπαϊκής ολοκλήρωσης, είναι σημαντική τόσο η εξασφάλιση της διαλειτουργικότητας μεταξύ των εθνικών συστημάτων ηλεκτρονικής ταυτοποίησης των κρατών μελών, όσο και η εφαρμογή ασφαλών, αξιόπιστων λύσεων με σεβασμό στην προστασία των προσωπικών δεδομένων και την ασφάλεια των πολιτών. Προς αυτήν ακριβώς την κατεύθυνση, η Ευρωπαϊκή Ένωση, οι Διεθνείς Οργανισμοί, αλλά και οι Κυβερνήσεις, Πανεπιστημιακά Ιδρύματα, επιχειρήσεις και άλλοι φορείς έχουν προχωρήσει στον καθορισμό προτύπων, στην εξαγωγή μελετών, στην υλοποίηση πιλοτικών προγραμμάτων και ερευνητικών έργων. Έτσι, ο δρόμος για μια ποιοτική, ασφαλή, εύχρηστη και διαλειτουργική Ευρωπαϊκή ΚΠ περνάει μέσα από τη μελέτη της εμπειρίας που προκύπτει από τις υφιστάμενες επιλογές και λύσεις που έχουν εφαρμοστεί, καθώς και μέσω της αξιολόγησης των αποτελεσμάτων που αναδύονται από την εφαρμογή τους στα κράτη μέλη. Αντίστοιχα, η καλή γνώση της υφιστάμενης τεχνολογικής και επιχειρησιακής κατάστασης, αλλά και των πιθανών αποτυχιών, λαθών και μη επιτυχημένων μοντέλων εφαρμογής είναι απολύτως χρήσιμη και αναγκαία, στην αναζήτηση της βέλτιστης, τεχνολογικά και επιχειρησιακά, σχεδιαστικής επιλογής για την εφαρμογή της ΚΠ στην Ελλάδα, πάντα υπό το πρίσμα της δημιουργίας μιας ασφαλούς και αποτελεσματικής υποδομής για την Εθνική ΚΠ με σεβασμό της ιδωτικότητας του πολίτη.

Στην πρώτη ενότητα του κεφαλαίου θα παρουσιάσουμε την εικόνα των κρατών μελών της Ευρωπαϊκής Ένωσης σχετικά με τις λύσεις περί ηλεκτρονικής ταυτοποίησης που προσφέρουν. Στο πλαίσιο αυτό, σημαντικά σημεία αποτελούν το ευρύτερο πλαίσιο ταυτοποίησης των πολιτών που ισχύει για κάθε χώρα, η τεχνολογική λύση που υλοποιούν, οι τεχνικές ασφάλειας που χρησιμοποιούν, η διάρκεια ζωής της κάρτας, το επιχειρησιακό μοντέλο που εφαρμόζουν, η χρήση των αναγνωριστικών(μοναδικά/ τομεακά αναγνωριστικά), τα δεδομένα που χρησιμοποιούν και αποθηκεύουν, καθώς και η συμμόρφωσή τους με τις συστάσεις του ICAO [65], της Ευρωπαϊκής Κάρτας Πολίτη (ECC) και τα διεθνή πρωτόκολλα και πρότυπα.

Επιπλέον, θα περιγραφούν και τα κρισιμότερα σημεία των λύσεων που θεωρούμε περισσότερο επιτυχημένες, σε μια προσπάθεια να αναδείξουμε τις «απαιτήσεις» για την εφαρμογή της δικής μας ΚΠ.

Στην επόμενη ενότητα, με έμφαση στην εξασφάλιση της διαλειτουργικότητας μεταξύ των επιμέρους εθνικών λύσεων για την ηλεκτρονική ταυτοποίηση, γίνεται παρουσίαση των σημαντικότερων ευρωπαϊκών μελετών και έργων για τα θέματα που σχετίζονται άμεσα ή έμμεσα με την ΚΠ, από τις ηλεκτρονικές υπογραφές, τη διαχείριση των προσωπικών δεδομένων και την ανάπτυξη μιας ενιαίας ψηφιακής αγοράς, μέχρι τη διαχείριση ηλεκτρονικών ταυτοτήτων και την ηλεκτρονική ταυτοποίηση.

Τέλος, στην ίδια ενότητα, θα αναφερθούν σημαντικές κατά τη γνώμη μας σύγχρονες τεχνολογίες που μπορούν να προσδώσουν επιπλέον ασφάλεια στη χρήση της ΚΠ και να εξασφαλίσουν με αποδοτικότερο τρόπο την ιδιωτικότητα και την ανωνυμία του πολίτη.

4.1. Ανασκόπηση της Ευρωπαϊκής Πρακτικής

Η παρουσίαση της ενότητας θα γίνει κατά κύριο λόγο με τη χρήση συγκριτικών πινάκων για την καλύτερη απεικόνιση και αξιολόγηση των επιλογών και πρακτικών των Ευρωπαϊκών χωρών γύρω από το ζήτημα της εθνικής ηλεκτρονικής ταυτότητας και την ευκολότερη διεξαγωγή συμπερασμάτων.

Το πρώτο υπό εξέταση ερώτημα είναι το πλαίσιο εθνικής ταυτοποίησης που ισχύει σε κάθε χώρα και η πιθανή σύγκλισή του με την εφαρμογή της ηλεκτρονικής ταυτότητας. Στον παρακάτω πίνακα εξετάζεται αν υπάρχει κάποιο έγγραφο εθνικής ταυτοποίησης για τα κράτη μέλη της ΕΕ κι αν αυτό είναι υποχρεωτικό και παράλληλα, αν έχουν ήδη υλοποιηθεί ή σχεδιάζονται λύσεις ηλεκτρονικής ταυτότητας.

Όπως θα διαπιστώσουμε, με μια γρήγορη ματιά στον πίνακα, για τις περισσότερες χώρες υπάρχει επίσημο εθνικό σύστημα ταυτοποίησης και σε μεγάλο ποσοστό, αυτό είναι υποχρεωτικό. Αναφορικά, τώρα, με την εμπειρία στην ηλεκτρονική ταυτότητα, οι περισσότερες Κυβερνήσεις έχουν ήδη εφαρμόσει σχετικές λύσεις, και από όσες ακόμη δεν εφαρμόζουν σύστημα ηλεκτρονικής ταυτοποίησης, η συντριπτική πλειοψηφία ήδη το σχεδιάζει.

Κράτος Μέλος ΕΕ	Δελτίο Ταυτότητας	Υποχρεωτικό	eID Κάρτα	Σχεδιασμός eID
Αυστρία	ΝΑΙ	ΟΧΙ	ΝΑΙ (Bürgerkarte)	-
Βέλγιο	ΝΑΙ	ΝΑΙ	ΝΑΙ (BELPIC)	-
Βουλγαρία	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΟΧΙ
Γαλλία	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ (INES)
Γερμανία	ΝΑΙ	ΝΑΙ	ΝΑΙ (Personalausweis)	ΝΑΙ
Δανία	ΟΧΙ	ΟΧΙ	ΟΧΙ	ΟΧΙ
Ελλάδα	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΝΑΙ
Εσθονία	ΝΑΙ	ΝΑΙ	ΝΑΙ	-

Ηνωμένο Βασίλειο	ΜΕΡΙΚΩΣ	ΟΧΙ	ΚΑΤΑΡΓΗΘΗΚΕ	-
Ιρλανδία	ΟΧΙ Proof of age card(μετά τα 18)	ΟΧΙ	ΟΧΙ	ΟΧΙ
Ισλανδία	ΝΑΙ	ΝΑΙ	ΝΑΙ	-
Ισπανία	ΝΑΙ	ΝΑΙ	ΝΑΙ	-
Ιταλία	ΝΑΙ	ΟΧΙ	ΝΑΙ	-
Κύπρος	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΟΧΙ
Λετονία	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΝΑΙ
Λιθουανία	ΝΑΙ	ΝΑΙ	ΝΑΙ	-
Λιχτενστάιν	ΝΑΙ	ΟΧΙ	ΝΑΙ	-
Λουξεμβούργο	ΝΑΙ	ΝΑΙ	ΝΑΙ (LuxTrust smart card, Δεν υπάρχει ακόμη διαμορφωμένο πλαίσιο)	-
Μάλτα	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΝΑΙ
Νορβηγία	ΝΑΙ	ΟΧΙ	ΟΧΙ	ΟΧΙ
Ολλανδία	ΝΑΙ	ΝΑΙ	ΝΑΙ	-
Ουγγαρία	ΝΑΙ	ΟΧΙ	ΟΧΙ	ΝΑΙ
Πολωνία	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΝΑΙ
Πορτογαλία	ΝΑΙ	ΝΑΙ	ΝΑΙ	-
Ρουμανία	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΝΑΙ
Σλοβακία	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΝΑΙ
Σλοβενία	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΝΑΙ
Τσέχικη Δημοκρατία	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΟΧΙ
Σουηδία	ΝΑΙ	ΟΧΙ	ΝΑΙ	-
Φινλανδία	ΝΑΙ	ΟΧΙ	ΝΑΙ	-
ΣΥΝΟΛΟ	25	20	15	10

Πίνακας 1- Εθνικά Συστήματα Ταυτότητας και ΚΠ

Σχετικά με την περίπτωση του Ηνωμένου Βασιλείου πρέπει να σημειώσουμε ότι η ΚΠ χρησιμοποιείτο, ωστόσο από στις αρχές του 2011, αυτή καταργήθηκε.

Στον επόμενο πίνακα, θα παρουσιάσουμε τις τεχνολογικές λύσεις που εφαρμόζουν οι χώρες που έχουν ήδη υιοθετήσει την ΚΠ.

	Διεπαφή Τσιπ	Διάρκεια Ζωής	ICAO	BAC	EAC
Αυστρία	ΕΠΑΦΙΚΟ	10			
Βέλγιο	ΕΠΑΦΙΚΟ	5			
Γερμανία	ΑΝΕΠΑΦΙΚΟ	10	ΝΑΙ	ΟΧΙ	PACE
Εσθονία	ΕΠΑΦΙΚΟ	10	ΝΑΙ		
Ισλανδία	ΕΠΑΦΙΚΟ	10	ΝΑΙ		
Ισπανία	ΕΠΑΦΙΚΟ	10			
Ιταλία	ΕΠΑΦΙΚΟ	10			
Λιθουανία	ΥΒΡΙΔΙΚΟ	10	ΝΑΙ	ΝΑΙ	ΝΑΙ
Λιχτενστάιν	ΕΠΑΦΙΚΟ	10	ΟΧΙ		
Λουξεμβούργο	ΕΠΑΦΙΚΟ	10			
Ολλανδία	ΑΝΕΠΑΦΙΚΟ	5	ΝΑΙ	PACE	ΝΑΙ

Πορτογαλία	ΕΠΑΦΙΚΟ	5			
Σουηδία	ΥΒΡΙΔΙΚΟ	5	ΝΑΙ	ΝΑΙ	ΟΧΙ
Φινλανδία	ΕΠΑΦΙΚΟ	5			
ECC	ΕΠΑΦΙΚΟ/ ΑΝΕΠΑΦΙΚΟ/ ΥΒΡΙΔΙΚΟ	10	ΠΡΟΑΙΡΕΤΙΚΑ	ΠΡΟΑΙΡΕΤΙΚΑ	ΠΡΟΑΙΡΕΤΙΚΑ
ICAO/EU	ΑΝΕΠΑΦΙΚΟ	5	ΝΑΙ	ΠΡΟΑΙΡΕΤΙΚΑ	ΠΡΟΑΙΡΕΤΙΚΑ

Πίνακας 2- Εφαρμοζόμενες τεχνολογικές επίλογές

Επεξεργαζόμενοι τα στοιχεία του παραπάνω πίνακα καταλήγουμε στο συμπέρασμα ότι παρά τις συστάσεις του ICAO για τη χρήση ανεπαφικού τσιπ οι περισσότερες ευρωπαϊκές χώρες που χρησιμοποιούν ήδη συστήματα ηλεκτρονικών ταυτοτήτων, δεν έχουν υιοθετήσει την ανεπαφική διεπαφή του τσιπ. Επιπλέον , για τις κάρτες με ανεπαφικό τσιπ επιβάλλεται η χρήση πρωτοκόλλων BAC, PACE και EAC. Η διάρκεια ζωής των καρτών ανεξάρτητα από τη διεπαφή του τσιπ κυμαίνεται μεταξύ των 5 και 10 ετών.

	Ψηφιακή Αυθεντικοποίηση	Ψηφιακή Υπογραφή	Αλλαγή Δεδομένων	Εγγραφή Πρόσθετων Δεδομένων
Αυστρία	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ
Βέλγιο	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ
Γερμανία	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ
Εσθονία	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΟΧΙ
Ισλανδία	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΟΧΙ
Ισπανία	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ
Ιταλία	ΝΑΙ	ΝΑΙ	ΟΧΙ	ΝΑΙ
Λιθουανία	ΟΧΙ	ΟΧΙ	ΟΧΙ	ΟΧΙ
Λιχτενστάιν	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΟΧΙ
Λουξεμβούργο	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ
Ολλανδία	ΟΧΙ	ΟΧΙ	ΟΧΙ	ΟΧΙ
Πορτογαλία	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ
Σουηδία	ΝΑΙ	ΝΑΙ	ΟΧΙ	ct ΝΑΙ cl ΟΧΙ
Φινλανδία	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ
ECC	ΝΑΙ	ΝΑΙ	ΠΡΟΑΙΡΕΤΙΚΑ	ΠΡΟΑΙΡΕΤΙΚΑ
ICAO/EU	ΟΧΙ	ΟΧΙ	ΟΧΙ	ΟΧΙ

Πίνακας 3- Επιλογές λειτουργικότητας της ΚΠ

Όσον αφορά στη λειτουργικότητα των εθνικών καρτών του πολίτη περιλαμβάνει στο σύνολο των λύσεων την ψηφιακή αυθεντικοποίηση, καθώς επίσης ενσωματώνει και τη δυνατότητα ψηφιακής υπογραφής. Ειδικότερα, για την Εσθονία, η χρήση της ψηφιακής υπογραφής είναι υποχρεωτική και συγκεκριμένα για την Αυστρία και απαιτείται για την ενεργοποίηση της κάρτας.

Το επόμενο στοιχείο του πίνακα σχετίζεται με τη δυνατότητα αλλαγής δεδομένων και εγγραφής πρόσθετων δεδομένων στην κάρτα του πολίτη μετά την έκδοση της κάρτας και την αντιστοίχισή της με τον πολίτη-κάτοχο. Τα χαρακτηριστικά αυτά είναι απολύτως κρίσιμος σχεδιαστικός παράγοντας για την υλοποίηση της ΚΠ. Οι δυνατότητες τροποποίησης και εγγραφής νέων δεδομένων στην κάρτα σχετίζονται άμεσα με θέματα ασφάλειας και ιδιωτικότητας και επιπλέον επηρεάζουν τη χρήση της κάρτας από επιμέρους ηλεκτρονικές εφαρμογές.

Τα δεδομένα που παρουσιάζονται στην τέταρτη στήλη του παραπάνω πίνακα, αφορούν σε προσωπικά δεδομένα του κατόχου της κάρτας, τα μοναδικά αναγνωριστικά του χρήστη και στοιχεία επικοινωνίας και διεύθυνσης, ενώ στην τελευταία στήλη αναφερόμαστε σε δευτερεύοντα δεδομένα του πολίτη που σχετίζονται κυρίως με τις εφαρμογές που χρησιμοποιεί, όπως για παράδειγμα η φορολογική ενημερότητα.

Στον επόμενο πίνακα θα προσπαθήσουμε να συγκεντρώσουμε τις τεχνικές που χρησιμοποιούνται για τον έλεγχο πρόσβασης, προκειμένου να διασφαλίσουμε την εξουσιοδοτημένη μόνο πρόσβαση στα δεδομένα και τις δυνατότητες της κάρτας. Στο πλαίσιο αυτό, παρατηρούμε ότι η απλή τεχνική της εισαγωγής του από τον χρήστη PIN, προκειμένου να εξασφαλίσει πρόσβαση σε δεδομένα και εφαρμογές είναι διαδεδομένη σε όλες τις επιμέρους εθνικές λύσεις.

Επίσης, η συμμετρική κρυπτογραφία και η χρήση μυστικών κλειδιών θα μπορούσε να είναι αποδεκτή μέθοδος, όπως αναλύσαμε και σε προηγούμενη ενότητα [15][16]. Ωστόσο, όπως θα δούμε, δεν τυγχάνει ιδιαίτερης αναγνώρισης στις, υπό μελέτη, ευρωπαϊκές λύσεις. Αυτό από ότι φαίνεται συμβαίνει, πιθανότατα, εξαιτίας δυσκολίας διαχείρισης των κλειδιών, κυρίως, ως προς την ασφαλή ανταλλαγή τους μεταξύ των οντοτήτων κατά τη διάρκεια των συναλλαγών, στις οποίες συμμετέχει η ΚΠ.

Αντίθετα, η χρήση πιστοποιητικών για τον έλεγχο πρόσβασης αποτελεί την ενδεδειγμένη λύση σύμφωνα και με τον ICAO, παρότι δεν έχει γίνει ακόμη αποδεκτή.

Όλες οι λύσεις που έχουν εφαρμοστεί στα κράτη μέλη της ΕΕ δεν απαιτούν κρυπτογράφηση των δεδομένων κατά την αποθήκευσή τους στην κάρτα, παρά μόνο κατά την μετάδοσή τους.

	PIN	Συμμετρική Κρυπτογραφία	Πιστοποιητό
Αυστρία	ΝΑΙ	ΟΧΙ	ΟΧΙ
Βέλγιο	ΝΑΙ	ΟΧΙ	ΝΑΙ
Γερμανία	ΝΑΙ	ΟΧΙ	ΝΑΙ
Εσθονία	ΝΑΙ	ΝΑΙ	ΟΧΙ
Ισλανδία	ΝΑΙ	ΟΧΙ	ΝΑΙ
Ισπανία	ΝΑΙ	ΝΑΙ	ΟΧΙ
Ιταλία	ΝΑΙ	ΟΧΙ	ΟΧΙ
Λιθουανία	ΟΧΙ	ΝΑΙ	ΟΧΙ
Λιχτενστάιν	ΝΑΙ	ΟΧΙ	ΝΑΙ
Λουξεμβούργο	ΝΑΙ	ΟΧΙ	ΝΑΙ
Ολλανδία	ΟΧΙ	ΟΧΙ	ΟΧΙ
Πορτογαλία	ΝΑΙ	ΟΧΙ	ΝΑΙ
Σουηδία	Ct ΝΑΙ Cl ΟΧΙ	ΟΧΙ	ΟΧΙ
Φινλανδία	ΝΑΙ	ΝΑΙ	ΟΧΙ
ECC	ΠΡΟΑΙΡΕΤΙΚΑ	ΠΡΟΑΙΡΕΤΙΚΑ	ΠΡΟΑΙΡΕΤΙΚΑ
ICAO/EU	ΟΧΙ	ΟΧΙ	ΝΑΙ

Πίνακας 4- Μηχανισμοί Ελέγχου Πρόσβασης

Στη συνέχεια θα αντιμετωπίσουμε το ερώτημα της χρήσης ή μη μοναδικών αναγνωριστικών, ανά πολίτη, της πρόσβασης σε αυτό και την αντίστοιχη διείσδυση των τομεακών/πολλαπλών αναγνωριστικών για τις υλοποιήσεις των επιμέρους εθνικών καρτών του Ευρωπαίου πολίτη. Είναι σαφές ότι η χρήση μοναδικών αναγνωριστικών δεν είναι η ασφαλέστερη επιλογή, υπό το πρίσμα της ασφάλειας και της προστασίας της ιδιωτικότητας του πολίτη. Στην περίπτωση αυτή, όλη η πληροφορία του πολίτη συνδέεται με αυτό το μοναδικό αναγνωριστικό και η αποκάλυψή του συνεπάγεται αποκάλυψη όλων των σχετιζόμενων πληροφοριών. Το μοναδικό αναγνωριστικό προσδιορίζει μοναδικά τον κάθε πολίτη (ένα προς ένα σχέση) και επομένως οι απαιτήσεις ασφαλείας μεγαλώνουν καθώς ο κίνδυνος από την αποκάλυψη και την κακή χρήση του μπορεί να έχουν σημαντικές συνέπειες για τον πολίτη, εκτός από την παραβίαση των προσωπικών του δεδομένων και των δικαιωμάτων του για ιδιωτικότητα και ανωνυμία. Παρόλα αυτά, τα μοναδικά αναγνωριστικά μπορεί να αποτελέσουν ευέλικτη, εύχρηστη και απλή λύση για τις κυβερνήσεις κι έτσι ίσως μπορεί να εξηγηθεί η εντυπωσιακή διείσδυσή του στις υφιστάμενες υποδομές. Πρέπει να γίνει κατανοητό ότι αυτή η λύση απαιτεί αυξημένη προστασία του αναγνωριστικού και των συστημάτων από απειλές ασφάλειας και ιδιωτικότητας.

Στις περισσότερες χώρες που εφαρμόζεται η επιλογή της χρήσης του μοναδικού αναγνωριστικού, αυτό συνήθως, αποδίδεται κατά τη γέννηση του πολίτη και παραμένει ίδιο για όλη του τη ζωή.

	Μοναδικό Αναγνωριστικό	Πρόσβαση στο Μοναδικό Αναγνωριστικό	Τομεακά Αναγνωριστικά	Πρόσβαση στα Τομεακά Αναγνωριστικά
Αυστρία	ΟΧΙ	-	ΝΑΙ	ΜΕ ΣΥΓΚΑΤΑΘΕΣΗ
Βέλγιο	ΝΑΙ	ΟΠΟΙΟΣΔΗΠΟΤΕ	ΟΧΙ	-
Γερμανία	ΟΧΙ	-	ΝΑΙ	ΚΑΤΟΧΟΣ ΚΡΑΤΙΚΕΣ ΥΠΗΡΕΣΙΕΣ
Εσθονία	ΝΑΙ	ΟΠΟΙΟΣΔΗΠΟΤΕ	ΟΧΙ	-
Ισλανδία	ΝΑΙ	ΟΠΟΙΟΣΔΗΠΟΤΕ	ΝΑΙ	ΚΑΤΟΧΟΣ ΚΡΑΤΙΚΕΣ ΥΠΗΡΕΣΙΕΣ
Ισπανία	ΝΑΙ	ΜΕ ΣΥΓΚΑΤΑΘΕΣΗ	ΟΧΙ	-
Ιταλία	ΝΑΙ	ΜΕ ΣΥΓΚΑΤΑΘΕΣΗ	ΟΧΙ	-
Λιθουανία	ΟΧΙ	ΜΕ ΣΥΓΚΑΤΑΘΕΣΗ	ΟΧΙ	ΚΑΤΟΧΟΣ ΚΡΑΤΙΚΕΣ ΥΠΗΡΕΣΙΕΣ
Λιχτενστάιν	ΝΑΙ	ΜΕ ΣΥΓΚΑΤΑΘΕΣΗ	ΟΧΙ	-
Λουξεμβούργο	ΟΧΙ	ΟΠΟΙΟΣΔΗΠΟΤΕ	ΟΧΙ	-
Ολλανδία	ΟΧΙ	ΟΠΟΙΟΣΔΗΠΟΤΕ	ΟΧΙ	-
Πορτογαλία	ΝΑΙ	ΟΠΟΙΟΣΔΗΠΟΤΕ	ΟΧΙ	-
Σουηδία	Ct ΝΑΙ Cl ΟΧΙ	ΟΠΟΙΟΣΔΗΠΟΤΕ/ -	ΟΧΙ	-
Φινλανδία	ΝΑΙ	ΟΠΟΙΟΣΔΗΠΟΤΕ	ΟΧΙ	-
ECC	-	-	-	-
ICAO/EU	ΟΧΙ	-	-	-

Πίνακας 5- Χρήση Αναγνωριστικών

Δεδομένου ότι δεν υπάρχει η ενδεδειγμένη λύση από τους οργανισμούς, παρά την επισήμανση για μη χρήση μοναδικού αναγνωριστικού από τον ICAO, τα περισσότερα κράτη μέλη εφαρμόζουν τη λύση των μοναδικών αναγνωριστικών, στα οποία είναι δυνατή η πρόσβαση από τον οποιονδήποτε, εκτός από την Ιταλία και Ισπανία, στις οποίες η πρόσβαση στο μοναδικό αναγνωριστικό γίνεται μόνο έπειτα από τη ρητή συγκατάθεση του πολίτη. Στον αντίποδα, η Αυστρία και η Γερμανία χρησιμοποιούν πολλαπλά ή τομεακά αναγνωριστικά, ανά φορέα και υπηρεσία.

Στο τέλος της συγκριτικής ανασκόπησης θα εξετάσουμε τις δυνατότητες πρόσβασης στα προσωπικά δεδομένα (στοιχεία ταυτότητας, βιομετρικά χαρακτηριστικά και φωτογραφία).

	Προσωπικά Στοιχεία	Φωτογραφία	Δακτυλικό Αποτύπωμα
Αυστρία	ΟΠΟΙΟΣΔΗΠΟΤΕ	-	-
Βέλγιο	ΟΠΟΙΟΣΔΗΠΟΤΕ	ΟΠΟΙΟΣΔΗΠΟΤΕ	-
Γερμανία	ΜΕ ΣΥΓΚΑΤΑΘΕΣΗ	ΥΠΗΡΕΣΙΕΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΔΙΑΣΥΝΟΡΙΑΚΟΣ ΕΛΕΓΧΟΣ	ΠΡΟΑΙΡΕΤΙΚΗ ΧΡΗΣΗ/ ΠΡΟΣΒΑΣΗ ΜΟΝΟ ΑΠΟ ΥΠΗΡΕΣΙΕΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΔΙΑΣΥΝΟΡΙΑΚΟΥ ΕΛΕΓΧΟΥ
Εσθονία	ΟΠΟΙΟΣΔΗΠΟΤΕ	ΟΠΟΙΟΣΔΗΠΟΤΕ	-
Ισλανδία	ΟΠΟΙΟΣΔΗΠΟΤΕ	ΟΠΟΙΟΣΔΗΠΟΤΕ	-
Ισπανία	ΜΕ ΣΥΓΚΑΤΑΘΕΣΗ	ΜΕ ΣΥΓΚΑΤΑΘΕΣΗ	-
Ιταλία	ΜΕ ΣΥΓΚΑΤΑΘΕΣΗ	ΜΕ ΣΥΓΚΑΤΑΘΕΣΗ	ΠΡΟΑΙΡΕΤΙΚΗ ΧΡΗΣΗ/ ΔΙΑΣΥΝΟΡΙΑΚΟΣ ΕΛΕΓΧΟΣ
Λιθουανία	ΟΠΟΙΟΣΔΗΠΟΤΕ	ΟΠΟΙΟΣΔΗΠΟΤΕ	-
Λιχτενστάιν	ΜΕ ΣΥΓΚΑΤΑΘΕΣΗ	ΜΕ ΣΥΓΚΑΤΑΘΕΣΗ	ΠΡΟΑΙΡΕΤΙΚΗ ΧΡΗΣΗ
Λουξεμβούργο	ΜΕ ΣΥΓΚΑΤΑΘΕΣΗ	ΜΕ ΣΥΓΚΑΤΑΘΕΣΗ	ΥΠΟΧΡΕΩΤΙΚΗ ΧΡΗΣΗ/ ΔΙΑΣΥΝΟΡΙΑΚΟΣ ΕΛΕΓΧΟΣ
Ολλανδία	ΟΠΟΙΟΣΔΗΠΟΤΕ	ΟΠΟΙΟΣΔΗΠΟΤΕ	ΥΠΟΧΡΕΩΤΙΚΗ ΧΡΗΣΗ/ ΔΙΑΣΥΝΟΡΙΑΚΟΣ ΕΛΕΓΧΟΣ
Πορτογαλία	ΟΠΟΙΟΣΔΗΠΟΤΕ	ΟΠΟΙΟΣΔΗΠΟΤΕ	ΥΠΟΧΡΕΩΤΙΚΗ ΧΡΗΣΗ/ ΔΙΑΣΥΝΟΡΙΑΚΟΣ ΕΛΕΓΧΟΣ
Σουηδία	ΟΠΟΙΟΣΔΗΠΟΤΕ	ΟΠΟΙΟΣΔΗΠΟΤΕ	-
Φινλανδία	ΟΠΟΙΟΣΔΗΠΟΤΕ	-	-
ECC	-	-	ΠΡΟΑΙΡΕΤΙΚΗ ΑΠΟΘΗΚΕΥΣΗ
ICAO/EU	ΔΙΑΣΥΝΟΡΙΑΚΟΣ ΕΛΕΓΧΟΣ	ΔΙΑΣΥΝΟΡΙΑΚΟΣ ΕΛΕΓΧΟΣ	ΔΙΑΣΥΝΟΡΙΑΚΟΣ ΕΛΕΓΧΟΣ

Πίνακας 6- Προσωπικά δεδομένα και Πρόσβαση

4.2. Ευρωπαϊκά Παραδείγματα Εφαρμογής Εθνικών ΚΠ

4.2.1. Μελέτη Περίπτωσης Αυστρίας

Η βασική καινοτομία για την Αυστρία και την Αυστριακή ΚΠ (Burgerkarte) είναι ότι υπάρχουν περισσότεροι του ενός τύποι κάρτας που μπορούν να χρησιμοποιηθούν, αρκεί να είναι σε θέση να αποθηκεύουν δεδομένα και να ενσωματώνουν λειτουργίες ψηφιακής υπογραφής. Η Burgerkarte είναι μια έξυπνη κάρτα που ενσωματώνει δυνατότητες ψηφιακής υπογραφής και ψηφιακών πιστοποιητικών και χρησιμοποιείται προκειμένου να προσδώσει ασφάλεια, για τις ηλεκτρονικές συναλλαγές του πολίτη με το κράτος. Τα ψηφιακά πιστοποιητικά εκδίδονται από το φορέα παροχής υπηρεσιών πιστοποίησης για την αξιοπιστία των ηλεκτρονικών συναλλαγών (a.trust).

Μάλιστα, από το 2005 υπάρχει, επιπλέον, η δυνατότητα ενσωμάτωσης των λειτουργικών της ΚΠ της Αυστρίας, στις τραπεζικές κάρτες (Maestro). Μέσω αυτής, της επιλογής, της ενσωμάτωσης δηλαδή της τεχνολογίας της ψηφιακής υπογραφής σε μια τραπεζική κάρτα, που πρώτη η Αυστριακή Κυβέρνηση υιοθέτησε, αναμένεται εξασφάλιση οικονομίας

κλίμακας. Στην Αυστριακή ΚΠ παρέχεται, επίσης, λειτουργικότητα μέσω συσκευών κινητής τηλεφωνίας ('light' Citizen Card) για τη διεκπεραίωση ηλεκτρονικών συναλλαγών.

Η λειτουργία της κάρτας απαιτεί την χρήση Η/Υ, συνδεδεμένου στο διαδίκτυο και ενός αναγνώστη καρτών (Card Reader), προκειμένου να καταστήσει δυνατή και ασφαλή την πρόσβαση σε πληθώρα ηλεκτρονικών υπηρεσιών της Δημόσιας Διοίκησης. Η χρήση της ΚΠ για την υπογραφή εγγράφων, συναλλαγών και διοικητικών πράξεων, μέσω της ψηφιακής υπογραφής, θεωρείται για την Αυστρία, νομικά ισοδύναμη με την ιδιόχειρη υπογραφή του πολίτη.

4.2.2. Μελέτη Περίπτωσης Βελγίου

Όλοι οι Βέλγοι πολίτες ηλικίας 12 και άνω γίνονται κάτοχοι μιας ηλεκτρονικής ΚΠ. Μετά την ηλικία των 15 είναι υποχρεωτικό να την φέρουν πάντοτε επάνω τους εκτός και αν βρίσκονται εντός 200 μέτρων από την οικία τους. Οι ξένοι υπήκοοι πρέπει να μπορούν ανά πάσα στιγμή να μπορούν να αποδεικνύουν με επίσημα έγγραφα το ποιοι είναι, είτε με το διαβατήριό τους είτε με κάποιο επίσημο έγγραφο που έχει εκδοθεί από άλλη Χώρα – μέλος της Ε.Ε. Οι κάτοχοι κάρτας που είναι Βέλγοι πολίτες μπορούν να χρησιμοποιούν την κάρτα τους για διεθνή ταξίδια μέσα στην Ευρωπαϊκή Ένωση και σε κάποιες άλλες Χώρες όπως FYROM, Κροατία, Σερβία και Αλβανία ισοδύναμα με ένα διαβατήριο.

Χρήση εντός Βελγίου

Παρότι είναι υποχρεωτικό να την φέρουν επάνω τους, οι Βέλγοι δεν είναι υποχρεωμένοι να επιδεικνύουν την κάρτα τους εκτός και αν:

- Τους ζητηθεί από ορισμένες κυβερνητικές υπηρεσίες
- Τους ζητηθεί από την Αστυνομία
- Τους ζητηθεί από εξουσιοδοτημένο προσωπικό των λεωφορείων και τραίνων

Φυσικά χαρακτηριστικά

Όλα τα πεδία στη κάρτα είναι δίγλωσσα (Αγγλικά σε συνδυασμό με την επιλογή του κατόχου μεταξύ Γαλλικών, Ολλανδικών ή Γερμανικών) και οι όροι Belgium και "Identity Card" αναγράφονται και στις τέσσερις γλώσσες.

Η μορφή είναι παρόμοια με αυτή των πιστωτικών καρτών, και περιέχει ένα 3-γραμμο κώδικα σε γλώσσα μηχανής στο πίσω μέρος που ξεκινά με τα αρχικά IDBEL. Η κάρτα περιέχει τις παρακάτω πληροφορίες:

- Φωτογραφία του κατόχου της κάρτας
- Όνομα του κατόχου (Επώνυμο και όνομα/τα (2) και τα αρχικά των επιπλέον ονομάτων)

- Ημερομηνία και τόπο γέννησης
- Φύλο
- Εθνικότητα: Belg (Belgian)
- ID νούμερο κάρτας, 12 ψηφία με τη μορφή xxx-xxxxxxx-yy. Το νούμερο ελέγχου yy είναι το υπόλοιπο της διαίρεσης του xxxxxxxxxx με το 97.
- Περίοδο ισχύος (τυπικά 5 χρόνια)
- Υπογραφή
- Αναγνωριστικό νούμερο του Εθνικού Μητρώου (σε κάθε πολίτη χορηγείται ένα μοναδιαίο αναγνωριστικό νούμερο για διαχειριστικούς λόγους). Το νούμερο αυτό αποτελείται από 11 ψηφία με τη μορφή yy.mm.dd-xxx.xx όπου yy.mm.dd είναι η ημερομηνία γέννησης του κατόχου.
- Τόπος έκδοσης
- Οικογενειακή κατάσταση (προαιρετικά)

Πριν από το 2005 η κάρτα δεν περιείχε chip, και η διεύθυνση του κατόχου αναγράφονταν πάνω της με φυσικό τρόπο. Πλέον αυτό γίνεται ηλεκτρονικά εντός του chip.

Η κάρτα μπορεί να χρησιμοποιείται ως επίσημο ταξιδιωτικό έγγραφο μέσα στην Ε.Ε. Για τις περισσότερες Χώρες εκτός Ε.Ε. οι Βέλγοι πρέπει να φέρουν μαζί τους διαβατήριο.

4.3. Διαλειτουργικότητα στην ΕΕ και Ευρωπαϊκά Έργα

Στο σημερινό περιβάλλον παγκοσμιοποίησης τίθεται ολοένα και πιο επιτακτική η ανάγκη για τα φυσικά και νομικά πρόσωπα μιας χώρας να χρησιμοποιούν τα ηλεκτρονικά τους διαπιστευτήρια υπό το νομικό καθεστώς της χώρας τους για να αποκτούν πρόσβαση σε δημόσιες υπηρεσίες που παρέχονται από τη χώρα τους, αλλά κι από τρίτες χώρες. Οι υπηρεσίες αυτές συνήθως παρέχονται με βάση διαφορετικά διαπιστευτήρια και διέπονται από διαφορετικό νομικό καθεστώς.

Παρά τις προσπάθειες που γίνονται τα τελευταία χρόνια τόσο σε τεχνολογικό, όσο και σε επιχειρησιακό επίπεδο, στην Ευρώπη, εντούτοις, δεν έχει εξασφαλισθεί ακόμη ικανό επίπεδο ωριμότητας στα κράτη μέλη, αναφορικά με τα ζητήματα της διαχείριση ηλεκτρονικών ταυτοτήτων και υπηρεσιών ηλεκτρονικής διακυβέρνησης. Στην κατεύθυνση αυτή, έχει αναγνωριστεί η ανάγκη ανάμιξης του ιδιωτικού τομέα, τόσο για την καλύτερη δυνατή υιοθέτηση τέτοιων λύσεων, όσο και για την συμβολή του στην ανάπτυξη τέτοιων λύσεων. Σήμερα, ένας αριθμός από ερευνητικά έργα που τρέχουν σε επίπεδο Ευρωπαϊκής Ένωσης προσπαθούν να δώσουν λύση στο πρόβλημα της αυθεντικοποίησης του συναλλασσόμενου, μέσω της χρήσης συστημάτων διαχείρισης ταυτότητας που εξασφαλίζουν διαλειτουργικότητα μεταξύ των δημόσιων οργανισμών των διαφόρων Ευρωπαϊκών κρατών μελών.

Το σημαντικότερο σημείο αναγνώρισης όμως, εντός ΕΕ είναι ότι τα ζητήματα ιδιωτικότητας και προστασίας των προσωπικών δεδομένων πρέπει να είναι πολύ ψηλά στην ατζέντα εφαρμογής της ευρωπαϊκής ΚΠ και αναγκαία προϋπόθεση για την δημιουργία σχέσεων εμπιστοσύνης μεταξύ των πολιτών-χρηστών των υπηρεσιών ηλεκτρονικής ταυτοποίησης που θα οδηγήσει στην περαιτέρω ανάπτυξη των υπηρεσιών ηλεκτρονικής διακυβέρνησης και ηλεκτρονικών συναλλαγών.

Εικόνα 15-Ηλεκτρονικές υπηρεσίες και αλληλεπίδραση

Η Ευρώπη το τελευταίο διάστημα έχει προχωρήσει σε μια σειρά συντονισμένων δράσεων προκειμένου να αξιολογήσει και να υιοθετήσει λύσεις που αφορούν στα ζητήματα διαλειτουργικότητας που προκύπτουν από την εφαρμογή της ΚΠ και των συστημάτων

διαχείρισης ηλεκτρονικών ταυτοτήτων. Ένα σύνολο πιλοτικών προγραμμάτων έχει ήδη ολοκληρωθεί και ένα άλλο είναι σε εξέλιξη. Στην κατεύθυνση αυτή, πολύ σημαντική είναι και η συνεισφορά του ιδιωτικού τομέα, ο οποίος προκειμένου να εξυπηρετήσει τις κυβερνητικές δράσεις έχει προχωρήσει στην ανάπτυξη σημαντικών λύσεων και συμμετέχει ενεργά στην εύρεση νέων μέσω ερευνητικών έργων που συμμετέχει.

Άλλωστε, σύμφωνα με τον *Windley (2005), η διαλειτουργικότητα είναι η πιο σημαντική πρόκληση που πρέπει να απαντηθεί για την ανάπτυξη των υποδομών διαχείρισης ταυτότητας.*

Παρακάτω επιχειρείται μια συνοπτική παρουσίαση των σημαντικότερων ευρωπαϊκών έργων που σχετίζονται άμεσα ή έμμεσα με την εφαρμογή της ΚΠ.

«**Modinis eIDM Study**»

Από τις πρώτες μελέτες που πραγματοποιήθηκαν αναφορικά με τη χρήση, τις επιρροές και τις επιπτώσεις συστημάτων διαχείρισης ταυτότητας. [69]

«**TLS-Federation**»

Έργο το οποίο επικεντρώθηκε στην αξιοποίηση προτύπων και τεχνολογιών με γνώμονα την εξασφάλιση ενός ασφαλούς περιβάλλοντος για τον πολίτη, απέναντι σε απειλές και κινδύνους κακής χρήσης των δεδομένων που τον ταυτοποιούν [70]. Το έργο αυτό προσπάθησε να μοντελοποιήσει ένα ενιαίο κανονιστικό και διαλειτουργικό περιβάλλον εφαρμογής συστημάτων διαχείρισης ταυτότητας σε ευρωπαϊκό επίπεδο.

«**GUIDE (Creating a European Identity Management Architecture for eGovernment)**»

Το έργο αυτό, επίσης, στόχευε στην ανάπτυξη ενός διαλειτουργικού μοντέλου διαχείρισης των ευρωπαϊκών ταυτοτήτων, ώστε να επιτρέψει την αξιοπιστία των εγγράφων και τεχνικών ταυτοποίησης και αυθεντικοποίησης μεταξύ των κρατών μελών της ΕΕ και την εγκαθίδρυση σχέσεων εμπιστοσύνης μεταξύ τους [71]. Αυτό πολύ απλά σημαίνει, ότι το ένα κράτος μέλος πρέπει να εμπιστεύεται την ταυτότητα που έχει εκδοθεί από άλλο κράτος μέλος και να την αντιμετωπίζει ισοδύναμα με αυτές που το ίδιο εκδίδει Για το σκοπό αυτό, προέβλεπε επιχειρησιακές(ανάμεσα σε παρόχους υπηρεσιών και φορέων παροχής υπηρεσιών πιστοποίησης) και διακρατικές συμφωνίες που θα διασφαλίζουν τις επιμέρους σχέσεις εμπιστοσύνης, στο πλαίσιο ενός ομοσπονδιακού συστήματος διαχείρισης ταυτότητας για όλη την Ευρωπαϊκή Ένωση.

«CROBIES (Cross-Border Interoperability of eSignatures)»

Μελέτη την οποία εκπόνησε η Ευρωπαϊκή Επιτροπή για τη χρήση και την ισχύ των ηλεκτρονικών υπογραφών εκτός των εθνικών συνόρων του κάθε Ευρωπαϊκού κράτους μεταξύ του 2008 και 2010. Στόχος ήταν να προταθούν λύσεις για την άρση των περιορισμών στη διασυνοριακή διαλειτουργικότητα των ηλεκτρονικών υπογραφών και των προηγμένων ηλεκτρονικών υπογραφών, οι οποίες βασίζονται σε αναγνωρισμένα πιστοποιητικά [74]. Το CROBIES πρότεινε επίσης βελτιώσεις σε νομικό και τεχνικό επίπεδο,

όσο και σε επίπεδο εμπιστοσύνης ως προς το θέμα των ηλεκτρονικών υπογραφών. Σημαντική είναι η πρότασή του για υποχρεωτική εφαρμογή ενός εναρμονισμένου σειριακού αριθμού στο πεδίο περιγραφής του πιστοποιητικού. [73]

«FIDIS (Future of Identity in the Information Society)»

Το έργο υλοποιήθηκε μεταξύ 2004 και 2009 στα πλαίσια του EU FP6 Network of Excellence [72], και εστίασε σε διάφορες πτυχές της ψηφιακής ταυτότητας και της ιδιωτικότητας και συμμετείχαν πανεπιστήμια και ιδιωτικές εταιρείες. Το έργο είχε σημαντική συνεισφορά στο θέμα στο θέμα της «μερικής ταυτοποίησης» (personae) [75].

Το σχέδιο FIDIS παρουσιάζει το πρωτότυπο iManager, το οποίο είναι η διαχείριση ταυτότητας για εν μέρει ταυτότητες. Η κάθε μερική ταυτότητα περιέχει ένα υποσύνολο πληροφορίες του χρήστη που είναι εφαρμόσιμες στις πληροφορίες που χρειάζονται για τον τρέχοντα ρόλο του χρήστη, όπως μια ταυτότητα που περιέχει τον αριθμό πιστωτικής κάρτας και διευθύνσεις ηλεκτρονικού ταχυδρομείου, όταν ο χρήστης συναλλάσσεται σε πραγματικό χρόνο.

Ο όρος «μερική ταυτοποίηση» αναφέρεται στη δυνατότητα που δίνεται από μεμονωμένα στοιχεία, τα οποία υπάρχουν διαθέσιμα για ένα άτομο στο διαδίκτυο και τα οποία δεν είναι ικανά να ταυτοποιήσουν το άτομο, να συλλεχθούν, με ένα κατάλληλο τρόπο να συσχετισθούν με τρόπο τέτοιο που να προσδιορίζουν το υποκείμενο.[75]

Οι περιοχές ενδιαφέροντος του FIDIS περιελάμβαναν νέες μορφές για τα δελτία ταυτότητας, χρήση χαρακτηριστικών γνωρισμάτων ταυτοποίησης σε πληροφοριακά συστήματα, τεχνολογίες για την ταυτοποίηση των πολιτών και καταγραφή των ιδιαιτεροτήτων των χωρών, εξασφάλιση διαλειτουργικότητας των εθνικών eIDs και των συστημάτων διαχείρισης ταυτοτήτων, προσδιορισμός απειλών, δημιουργία πλαισίου που να εξασφαλίζει την ιδιωτικότητα και ανάλυση του νομικό-κοινωνικού περιεχομένου των ταυτοτήτων, τεχνικά χαρακτηριστικά και περαιτέρω ανάπτυξη τεχνολογιών και προτύπων καθώς και ζητήματα φορητότητας.

Σε συνδυασμό με το έργο PRIME που αναφέρεται αμέσως παρακάτω, παρήγαγαν πρωτότυπα συστήματα διαχείρισης ταυτότητας που επιτρέπουν στους χρήστες εναλλαγή ταυτοτήτων (ρόλων).

«PRIME»

Ερευνητικό έργο επίσης στα πλαίσια του EU FP6, που ξεκίνησε τον Ιούνιο του 2004, με στόχο να αναπτύξει ένα λειτουργικό πρωτότυπο σύστημα διαχείρισης ταυτοτήτων το οποίο θα έδινε βάση στην προστασία της ιδιωτικότητας, και συμπεριελάμβανε δραστηριότητα με σκοπό τη διαμόρφωση των τεχνολογιών ενίσχυσης της ιδιωτικότητας (Privacy Enhancing Technologies, PET) και της ενδεχόμενης συμβολής τους στην εμπιστοσύνη [76]. Στα πλαίσια του έργου εφαρμόστηκαν απαιτητικά και δύσκολα σενάρια, που κατέστησαν δυνατή την αποδοχή του από την αγορά.

Το σχέδιο PRIME παρουσιάζει το πρωτότυπο σύστημα IDM. Το σύστημα IDM βελτιώνει την ιδιωτικότητα επιτρέποντας στο χρήστη να παραμείνει ανώνυμος, ακόμη και κατά τη διάρκεια μιας συναλλαγής, εξασφαλίζοντας παράλληλα την αξιοπιστία του, εξαιτίας της ύπαρξης της έμπιστο τρίτης οντότητας που μπορεί να πιστοποιήσει τον χρήστη..

Η δουλειά που έγινε με το PRIME συνεχίζεται τώρα από το «**PRIMELife»**, το οποίο συνιστά τη συνέχεια του έργου PRIME και χρηματοδοτήθηκε από το FP7 (ξεκίνησε το 2009), με σκοπό να ενισχύσει την ανωνυμία του ατόμου, κατά τη συμμετοχή του σε ηλεκτρονικές συναλλαγές, παρά τη χρήση δεδομένων που σχετίζονται άμεσα τον χρήστη και τον προσδιορίζουν και να προχωρήσει ακόμη περισσότερο σε ζητήματα διαλειτουργικότητας. [77]

«**IDABC (Interoperable Delivery of European eGovernment Services)**»

Ευρωπαϊκό πρόγραμμα που ολοκληρώθηκε το 2009 με στόχο την υποστήριξη της διαλειτουργικότητας κατά την ηλεκτρονική επικοινωνία μεταξύ των Εθνικών Διοικήσεων της ΕΕ [78]. Το συνολικό πρόγραμμα είχε να κάνει με την χρήση των τεχνολογιών πληροφορικής και επικοινωνιών (ΤΠΕ) προκειμένου για τη δημιουργία και ανάπτυξη διασυνοριακά παρεχόμενων ηλεκτρονικών υπηρεσιών που θα βελτίωναν την αποτελεσματικότητα και τη συνεργασία μεταξύ των Ευρωπαϊκών δημόσιων διοικήσεων και υπό τη σκέψη της ανάπτυξη μιας ενιαίας ψηφιακής αγοράς.

Στα πλαίσια αυτού του προγράμματος, υλοποιήθηκε το υποέργο **«eID Interoperability for PEGS»** [79] το οποίο ξεκίνησε το 2005 και ολοκληρώθηκε το 2009, συνεχίζοντας να παραδίδει παραδοτέα έως και τον Φεβρουάριο του 2010. Η κεντρική ιδέα του προγράμματος αφορούσε στην αξιολόγηση της σκοπιμότητας δημιουργίας μιας ενιαίας ευρωπαϊκής Αρχής Πιστοποίησης (European IDABC Bridge/Gateway CA - EBGCA) με σκοπό τη διασφάλιση της διαλειτουργικότητας μεταξύ των επιμέρους εθνικών συστημάτων και την εξασφάλιση της αμοιβαίας εμπιστοσύνης, η οποία θα προέρχεται από την ενιαία και αμοιβαία αναγνωρισμένη Αρχή Πιστοποίησης, καθώς και στην εγκαθίδρυση σχέσεων εμπιστοσύνης μεταξύ των εθνικών Αρχών Πιστοποίησης των κρατών μελών με ή χωρίς την ύπαρξη της ενιαίας Αρχής Πιστοποίησης. Στα πλαίσια του προγράμματος, προτάθηκε ακόμη η διατήρηση του Καταλόγου των Έμπιστων/Πιστοποιημένων Παρόχων Υπηρεσιών Πιστοποίησης (Trusted Service Provider List, TSL) από τις εθνικές Αρχές Πιστοποίησης.

«**ISA (Interoperability Solutions for European Public Administrations)**»

Είναι το πρόγραμμα που ήρθε να διαδεχθεί το IDABC. Το πρόγραμμα αυτό είναι σε εξέλιξη, ξεκίνησε το 2010 και αναμένεται να ολοκληρωθεί το 2015. [80]

«BRITE»

Χρηματοδοτούμενο από την ΕΕ έργο που περιλαμβάνει μία κοινοπραξία οργανισμών, όπως δημόσιοι φορείς, επιμελητήρια, πανεπιστήμια και εταιρείες εντός ΕΕ. Το BRITE θα αναπτύξει μία ενιαία πλατφόρμα πληροφοριών, επικοινωνιών και τεχνολογίας βασισμένη

σε ένα διαλειτουργικό μοντέλο ροής δεδομένων υλοποιώντας ένα τρόπο λειτουργίας ο οποίος θα επιτρέπει στα μητρώα να αλληλεπιδρούν σε ολόκληρη την πλατφόρμα και να ανταλλάσουν δεδομένα και πληροφορίες [81]. Στα πλαίσια του BRITE ένα από τα σημαντικότερα θέματα είναι η ψηφιακή υπογραφή των εγγράφων που θα εξασφαλίσει την αμοιβαία αναγνώριση και εγκυρότητα τους. Κρίσιμα σημεία στα πλαίσια του έργου είναι το νομικό πλαίσιο (αφομοίωση του Ευρωπαϊκού Εταιρικού Δικαίου και των Κοινοτικών Οδηγιών και Εθνικής Νομοθεσίας, σχετικών με την προστασία προσωπικών δεδομένων και τήρηση μητρώων) και η προστασία της ιδιωτικότητας. [http://www.briteproject.eu/]

«**PEPPOL (Pan-European Public Procurement Online)**» [68]

Λειτουργεί στα πλαίσια του προγράμματος της Ευρωπαϊκής Επιτροπής για την Ανταγωνιστικότητα και την Καινοτομία, και στα πλαίσια του υποστηρικτικού προγράμματος για ICT Policy (2008-2011), με στόχο την εφαρμογή κοινών προτύπων για την πραγματοποίηση ηλεκτρονικών δημόσιων προμηθειών σε ένα ευρύ Ευρωπαϊκό επίπεδο. Τα υπάρχοντα εθνικά συστήματα για δημόσιες ηλεκτρονικές προμήθειες θα συνδεθούν έτσι ώστε όλοι οι συμμετέχοντες να μπορούν να απολαύσουν τα πλήρη οφέλη μίας ενιαίας Ευρωπαϊκής αγοράς, επιτρέποντας σε οποιονδήποτε προμηθευτή να συμμετέχει σε οποιαδήποτε Ευρωπαϊκή δημόσια προκήρυξη [68]. Για την επίτευξη του σκοπού αυτού, κομβικό σημείο αποτελεί υλοποίηση ενός διαλειτουργικού σε επίπεδο ΕΕ μοντέλου για τις ψηφιακές υπογραφές. Το πρόγραμμα βασίζεται στην ιδέα λειτουργίας της ψηφιακής υπογραφής επεκτεινόμενη εκτός των εθνικών συνόρων ενός κράτους μέλους, ώστε στην πράξη μία οντότητα του δημόσιου τομέα να μπορεί να επικυρώνει πιστοποιητικά που εκδόθηκαν σε άλλο κράτος μέλος, επιτρέποντας τη διασυνοριακή ηλεκτρονική προσφορά υπηρεσιών. Για τη διαχείριση του μοντέλου δημιουργούνται επιμέρους PEPPOL Access Points στις ευρωπαϊκές κυβερνήσεις και την ΕΕ. Η πλατφόρμα VeriSign Managed Public Key Infrastructure, της εταιρίας Symantec VeriSign έρχεται να προτείνει λύση στο θέμα της δημιουργίας μιας κοινής υποδομής για την ασφαλή ανταλλαγή δεδομένων μεταξύ των PEPPOL Access Points. [68]

«**SPOCS (Simple Procedures Online for Cross- border Services)**»

Είναι ένα πιλοτικό ευρωπαϊκό έργο μεγάλης κλίμακας που βρίσκεται σε εξέλιξη από το 2009 και αναμένεται να ολοκληρωθεί το 2012. Το έργο αυτό, έχει να κάνει με τη χρήση των διαλειτουργικών ηλεκτρονικών υπηρεσιών ταυτοποίησης, από τις ευρωπαϊκές μικρομεσαίες επιχειρήσεις, με τρόπο ασφαλή και αποδοτικό, με στόχο την ανάπτυξη της ανταγωνιστικότητας [82]. Στους στόχους του προγράμματος εντάσσεται, μεταξύ άλλων οι ανάπτυξη συμπληρωματικών τεχνικών λύσεων για τη βελτίωση της χρήσης των μεθόδων ηλεκτρονικής ταυτοποίησης και διακίνησης ηλεκτρονικών εγγράφων σε διασυνοριακό επίπεδο. Στο πιλοτικό αυτό πρόγραμμα, συμμετέχει και η Ελλάδα.

«STORK (Secure idenTity acrOss boRders linKed)»

Το STORK (Secure idenTity acrOss boRders [67]) αποτελεί το πιο μεγαλόπνοο σύγχρονο έργο (2008-2011) της ένωσης, τα αποτελέσματα του οποίου ανακοινώθηκαν το 2011 και είναι απολύτως σημαντικά για τη διαχείριση ηλεκτρονικών ταυτοτήτων (eIDM), παρέχοντας

αποτελεσματική, αποδοτική, επεκτάσιμη και βιώσιμη λύση. Εξαιτίας της συμβολής του, κέρδισε, μάλιστα, το βραβείο της καλύτερης πρακτικής του Ευρωπαϊκού Δημόσιου Τομέα μέσω Συνεργατικής Διακυβέρνησης.

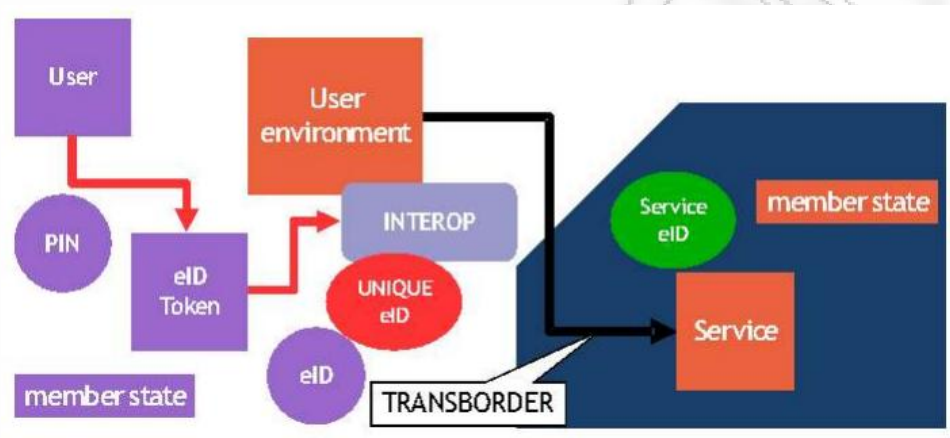
Το STORK είναι ένα ευρείας κλίμακας πιλοτικό έργο το οποίο εκτελείται από μία κοινοπραξία από Ευρωπαϊκές Δημόσιες Διοικήσεις και ιδιωτικούς συνεργάτες και χρηματοδοτείται από την Ευρωπαϊκή Ένωση σε ποσοστό 50%. Πιο συγκεκριμένα, τα εμπλεκόμενα μέρη του έργου ήταν, α)Κράτη μέλη της ΕΕ και ειδικότερα οι αντίστοιχοι φορείς της δημόσιας διοίκησης, μέλη του Member State Reference Group και G2G υπηρεσίες της Ευρωπαϊκής Επιτροπής , επιχειρήσεις που δραστηριοποιούνται στις eID λύσεις και συνεργάζονται μέσω του STORK Industry Group και άλλα σχετικά ευρωπαϊκά eID έργα, με αποτέλεσμα να είναι ένα ευρέως αποδεκτό έργο, τόσο από τις επιμέρους διοικήσεις, όσο και από τον ιδιωτικό τομέα.

Ο στόχος του προγράμματος είναι να καθιερωθεί μια ευρωπαϊκή πλατφόρμα διαλειτουργικότητας eID (ηλεκτρονικής ταυτότητας) που θα επιτρέψει στους πολίτες να καθιερώσουν νέες ηλεκτρονικές σχέσεις πέρα από τα σύνορα, με την παρουσίαση και μόνο του εθνικού eID [67]. Στα πλαίσια των δράσεων του έργου, εντάσσεται η ανάπτυξη κοινού πλαισίου και προδιαγραφών για την αμοιβαία και ασφαλή διασυνοριακή αναγνώριση και αυθεντικοποίηση μέσω των εθνικών ηλεκτρονικών ταυτοτήτων και την απλοποίηση της διαλειτουργικότητας των εθνικών eID συστημάτων. Το πρόγραμμα επίσης, φιλτράρει και αξιολογεί ένα σύνολο ασφαλών και εύχρηστων λύσεων eID για τους πολίτες και τη δημόσια διοίκηση των κρατών μελών, αλληλεπιδρώντας με άλλα ευρωπαϊκά προγράμματα, προκειμένου για τη μεγιστοποίηση της χρησιμότητας των υπηρεσιών ηλεκτρονικής ταυτοποίησης και των επιδράσεών της. Η λύση διαλειτουργικότητας του STORK για την εφαρμογής της ΚΠ και των ηλεκτρονικών ταυτοτήτων ευρύτερα στηρίζεται στην κατανεμημένη αρχιτεκτονική που στοχεύει ουσιαστικά στην ολοκλήρωση των ηλεκτρονικά παρεχόμενων ευρωπαϊκών υπηρεσιών, λαμβάνοντας υπόψη τις τρέχουσες προδιαγραφές και τις εθνικές υποδομές των ευρωπαϊκών χωρών. Το πρώτο βήμα, στην πορεία προς την ολοκλήρωση είναι η απλοποίηση των διοικητικών διαδικασιών, και η ασφαλής πρόσβαση στις επιμέρους ευρωπαϊκές δημόσιες υπηρεσίες, σε πραγματικό χρόνο. Η κυριότερη συμβολή του είναι η λύση στα ζητήματα πιστοποίησης της ταυτότητας του πολίτη/χρήστη σε πραγματικό περιβάλλον, από ιδιώτες και επιχειρήσεις για την ασφαλή διεκπεραίωση συναλλαγών.

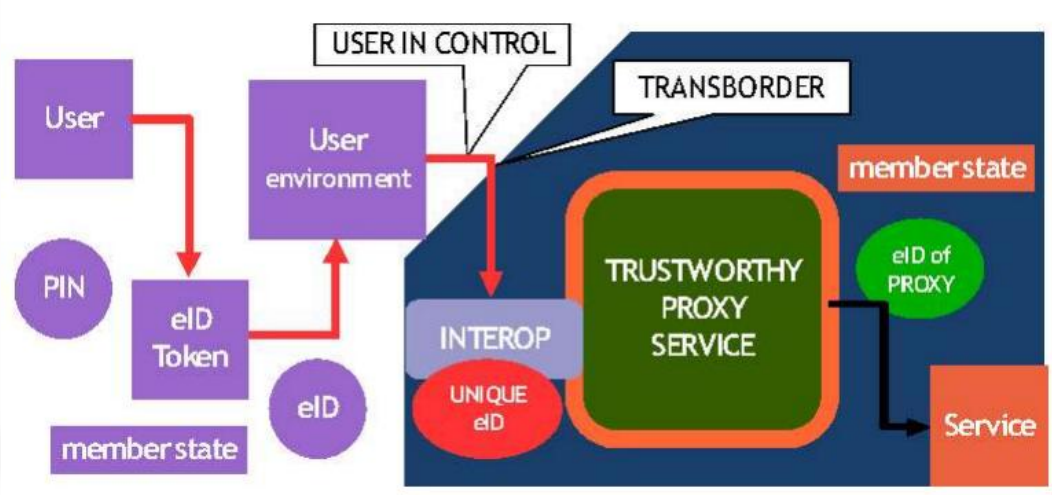
Στην πραγματικότητα, οι επιμέρους φορείς παροχής υπηρεσιών θα συνδεθούν με την πλατφόρμα STORK ώστε να παρέχουν διασυνοριακά τις υπηρεσίες τους με ασφαλή και αξιόπιστο τρόπο. Η προσέγγιση του προγράμματος είναι πολιτικοκεντρική, δηλαδή, έχει ως επίκεντρο τη διευκόλυνση και την προστασία του Ευρωπαίου πολίτη σε ένα διασυνοριακό περιβάλλον διακίνησης και συναλλαγών. Η κεντρική ιδέα, είναι να οδηγηθούμε σε μια πλατφόρμα που θα παρέχει υπηρεσίες χωρίς την απαίτηση της φυσικής παρουσίας, αλλά με την εισαγωγή των απαραίτητων κάθε φορά στοιχείων ή τη χρήση των εθνικών eID καρτών. Η πλατφόρμα STORK θα ικανοποιεί τις απαιτήσεις για εμπιστοσύνη, ασφάλεια και

ιδιωτικότητα, παρέχοντας εγγυήσεις για την ταυτοποίηση και αυθεντικοποίηση του πολίτη και ο πολίτης θα μπορεί μέσω της πλατφόρμας να έχει πρόσβαση σε πληθώρα υπηρεσιών που διευκολύνουν την καθημερινότητά του, όπως έναρξη επιχείρησης, φορολογική ενημερότητα κ.α.. Ο πολίτης θα είναι σε θέσει να ελέγχει τον τρόπο διαχείρισης και επεξεργασίας των προσωπικών του δεδομένων και μόνο με τη ρητή συγκατάθεσή του θα αποστέλλονται τα απαραίτητα για συναλλαγή στοιχεία στον φορέα παροχής υπηρεσιών [67].

Στα παρακάτω σχήματα παρουσιάζονται οι δύο προσεγγίσεις για την επίτευξης της διαλειτουργικότητας μεταξύ των υπηρεσιών των κρατών μελών. [66]



Εικόνα 16-Middleware approach



Εικόνα 17- Proxy approach

«Action Plan 2011-2015»

Η Ευρωπαϊκή Ένωση για το διάστημα 2011-2015 έχει καταρτίσει ένα πλάνο δράσεων προκειμένου να καταστεί δυνατή την ασφάλεια και τη διαλειτουργικότητα των συστημάτων

των κρατών μελών. Στο πλαίσιο αυτό, στην ανάπτυξη ανοιχτών προδιαγραφών, ως μέσο για την προώθηση της διαλειτουργικότητας και την ανάπτυξη καινοτόμων υπηρεσιών ηλεκτρονικής διακυβέρνησης [49].

Πιο συγκεκριμένα στις προτεραιότητες για τα έτη 2011 έως και 2015, αναφέρεται ότι στο σχέδιο δράσεων του άξονα 4.2 για την ηλεκτρονική διακυβέρνηση υπάρχουν τρεις δράσεις, οι οποίες άπτονται άμεσα στο ζήτημα της εφαρμογής της ΚΠ.

Ειδικότερα:

- Δράση 35: Αναθεώρηση της Οδηγίας για τις Ηλεκτρονικές Υπογραφές για τη διασυνοριακή αναγνώριση και διαλειτουργικότητα των συστημάτων ασφαλούς ηλεκτρονικής αυθεντικοποίησης
- Δράση 36: Εξασφάλιση αμοιβαίας αναγνώρισης της ηλεκτρονικής ταυτοποίησης και αυθεντικοποίησης
- Δράση 37: Ανάπτυξη και εφαρμογή λύσεων ηλεκτρονικής ταυτοποίησης

4.4. «Digital Agenda 2020»

Το Ευρωπαϊκό Ψηφιακό Θεματολόγιο είναι μια από τις επτά βασικές πρωτοβουλίες της Στρατηγικής «Ευρώπη 2020» και στοχεύει στο να αναδείξει και να προωθήσει τον ρόλο των Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) στην προετοιμασία της ευρωπαϊκής οικονομίας για τις προκλήσεις της επόμενης δεκαετίας. Είναι αποτέλεσμα ευρείας διαβούλευσης και συγκεκριμένα βασίζεται στα βασικά σημεία της Έκθεσης για την Ψηφιακή Ανταγωνιστικότητα 2009 [47], στα αποτελέσματα της δημόσιας διαβούλευσης που πραγματοποίησε το 2009 η Επιτροπή σε σχέση με τις μελλοντικές προτεραιότητες των ΤΠΕ, στα Συμπεράσματα του Συμβουλίου Τηλεπικοινωνιών του Δεκεμβρίου 2009, στα αποτελέσματα της διαβούλευσης για τη διαμόρφωση της στρατηγικής «Ευρώπη 2020», στη συνεισφορά της Σύμπραξης Εταιρειών ΤΠΕ στην Ευρωπαϊκή Ψηφιακή Στρατηγική της Ισπανικής Προεδρίας, στην πρωτοβουλία του Ευρωπαϊκού Κοινοβουλίου για «Μια νέα Ψηφιακή Ατζέντα για την Ευρώπη: 2015.eu» [50].

Οι βασικοί τομείς δράσης του (που έπονται των πολιτικών i2010 - European Information Society for growth and employment (2005-2010) και του eEurope Action Plan (2000-2005)) περιλαμβάνουν:

1. Ενιαία ψηφιακή αγορά: Στόχος είναι η άρση των εμποδίων στις διαδικτυακές υπηρεσίες πέραν των εθνικών συνόρων. Δίνεται έμφαση στην ενίσχυση του περιεχομένου που σχετίζεται με μουσική (music download business), στην κοινή υποδομή ηλεκτρονικού εμπορίου προϊόντων και υπηρεσιών καθώς και στην προστασία των ευρωπαίων καταναλωτών, αναζητώντας τις πλέον συμφέρουσες προσφορές από οποιαδήποτε χώρα της ΕΕ.

2. Διασφάλιση της διαλειτουργικότητας: Η ΕΕ πρέπει να διασφαλίσει ότι νέες συσκευές, εφαρμογές, βάσεις δεδομένων και υπηρεσίες μπορούν να διαλειτουργούν. Το Ψηφιακό Θεματολόγιο αναγνωρίζει τις πρότυπες διαδικασίες και τη διαλειτουργικότητα ως κλειδιά για την ανάπτυξη καινοτόμων προϊόντων και υπηρεσιών.

3. Ευρυζωνικότητα υψηλών ταχυτήτων (High speed broadband): Πρόσβαση στο διαδίκτυο υψηλών και υπέρ-υψηλών ταχυτήτων - ως γέφυρα για το μέλλον της Ευρώπης. Ως το 2020 όλοι οι Ευρωπαίοι πολίτες θα πρέπει να έχουν πρόσβαση στο διαδίκτυο με ταχύτητες τουλάχιστον 30 Mbps, ενώ πάνω από τα μισά ευρωπαϊκά νοικοκυριά θα πρέπει να διαθέτουν συνδέσεις 100 Mbps.

4. Ασφάλεια και εμπιστοσύνη: Βασική προϋπόθεση για την ανάπτυξη των υπηρεσιών διαδικτύου. Η ΕΕ ασχολείται με την κατάρτιση μια λογικής αντιμετώπισης στο θέμα της κυβερνο-ασφάλειας, δεδομένων των πρόσφατων επιθέσεων στις υποδομές των ΗΠΑ και της ΕΕ, καθώς και με τους περιορισμούς στην πρόσβαση στα κοινωνικά δίκτυα από παιδιά μικρότερα των 13 ετών. Επίσης εξετάζει το κανονιστικό πλαίσιο για πολιτικές ρύθμισης του διαδικτύου κυρίως μέσω της προστασίας των προσωπικών δεδομένων, της διασφάλισης της ιδιωτικότητας και της αντιμετώπισης των επιθέσεων στον κυβερνοχώρο.

5. Έρευνα και Καινοτομία: Περιλαμβάνει δράσεις για την αύξηση των επενδύσεων στην έρευνα και την ανάπτυξη νέων ιδεών και προϊόντων, τον συντονισμό των πόρων, την εξασφάλιση εύκολου και γρήγορου (light and fast) τρόπου πρόσβασης στην έρευνα και την ανάπτυξη νέας γενιάς υπηρεσιών διαδικτύου.

6. Άρση του χάσματος στη δυνατότητα χρήσης του διαδικτύου: Η ΕΕ δίνει ιδιαίτερη έμφαση στην ενίσχυση των ψηφιακών δεξιοτήτων των Ευρωπαίων πολιτών, (ανεξαρτήτως ηλικίας, προέλευσης, τόπου κατοικίας ή οικονομικής κατάστασης) και στη γεφύρωση του «ψηφιακού χάσματος», ώστε να μπορούν όλοι να συμμετέχουν ισότιμα στην ψηφιακή κοινωνία της γνώσης.

7. ΤΠΕ για την αντιμετώπιση κοινωνικών προκλήσεων: Αξιοποίηση των ΤΠΕ για την αντιμετώπιση των μεγάλων κοινωνικών προκλήσεων, όπως η κλιματική αλλαγή, η μείωση της ενεργειακής κατανάλωσης, η γήρανση του πληθυσμού και η υποστήριξη των ατόμων με αναπηρίες.

8. Διεθνής διάσταση

Στο Digital Agenda Assembly που πραγματοποιήθηκε στις Βρυξέλλες 16-17/06/2011, και στο οποίο συμμετείχαν 1500 εκπρόσωποι φορέων (παραγωγικοί φορείς, βιομηχανία, ερευνητική κοινότητα και Μη Κυβερνητικές Οργανώσεις, εκπρόσωποι κυβερνήσεων των κρατών μελών, και άλλα θεσμικά όργανα της ΕΕ) σε παράλληλα workshops, αξιολογήθηκε η πρόοδος ως προς την επίτευξη των στόχων και των δράσεων του Ψηφιακού Θεματολογίου, τον προσδιορισμό των μελλοντικών προκλήσεων, καθώς και την ενεργοποίηση των ενδιαφερομένων μερών. Ειδικότερα, στο θέμα της εφαρμογής της ΚΠ, τα

συμπεράσματα δύο κυρίως εκ των workshops: α)Ηλεκτρονική ταυτοποίηση και ηλεκτρονικές υπογραφές (“What next for e-Identity and e-Signatures?”) και β) Η εμπιστοσύνη ως βάση για την ενιαία ψηφιακή ευρωπαϊκή αγορά (“Building confidence for the digital single market”), ήταν απολύτως σημαντικά και πρόσφορα για την καλύτερη δυνατή προσέγγιση του θέματος της ηλεκτρονικών ταυτοτήτων, καθώς προσπάθησαν να αντιμετωπίσουν τις ανησυχίες και τις ανάγκες των ενδιαφερομένων μερών και να αναπτύξουν πιθανές επιλογές πολιτικής.

Οι παρουσιάσεις, το πρόγραμμα και τα συμπεράσματα είναι διαθέσιμα: στον ιστότοπο του της Ευρωπαϊκής Επιτροπής για το Ψηφιακό Θεματολόγιο [51].

Η ηλεκτρονική ταυτοποίηση και οι ηλεκτρονικές υπογραφές από κοινού μπορούν να ενισχύσουν το αίσθημα ασφάλειας, καθώς και να εγκαθιδρύσουν περιβάλλον εμπιστοσύνης και αξιοπιστίας σε έναν εικονικό κόσμο γεμάτο νέες προκλήσεις. Ωστόσο, βελτιώσεις στην εφαρμογή τους είναι απαραίτητες προς την κατεύθυνση αυτή.

Η ενότητα ξεκίνησε με μια επίδειξη για το πώς η ηλεκτρονική ταυτοποίηση και οι ηλεκτρονικές υπογραφές μπορούν να λειτουργήσουν σε ένα διασυνοριακό περιβάλλον, φέρνοντας σε επαφή τρία σχετικά έργα Ηλεκτρονικής Διακυβέρνησης (STORK, PEPPOL και SPOCS).

Σύμφωνα με το workshop, τρεις είναι οι κύριες παράμετροι για την ασφαλή και εναρμονισμένη χρήση των eIDs:

1. Οικονομικός παράγοντας: Με την πεποίθηση ότι το αγοραστικό ενδιαφέρον δε γνωρίζει σύνορα και σε συνδυασμό με την ανάπτυξη του ηλεκτρονικού εμπορίου, η ανάγκη για ασφαλή και αξιόπιστο μηχανισμό αμοιβαίας αναγνώρισης των συναλλασσομένων μερών είναι επιβεβλημένη. Επιπλέον, είναι σημαντική η συνεισφορά των λύσεων αυτών στην εξοικονόμηση κόστους και στη δημιουργία οικονομιών κλίμακας.

2. Εξασφάλιση της εμπιστοσύνης: Η εγκαθίδρυση σχέσεων εμπιστοσύνης μπορεί να προκύψει από την ασφαλή εγγραφή και αυθεντικοποίηση του πολίτη/πελάτη των υπηρεσιών, την αύξηση της ποιότητας των CRM δεδομένων και τον αποκλεισμό της μη εξουσιοδοτημένης πρόσβασης σε αυτά. Η κατεύθυνση που προτάθηκε αφορούσε σε «καθαρά», έγκυρα, μοναδικά δεδομένα για κάθε πολίτη. Αν αυτή είναι η βέλτιστη επιλογή θα προσπαθήσουμε, να το απαντήσουμε παρακάτω.

3. Ανάπτυξη υπηρεσιών και υποστηρικτικών δράσεων: Για την επίτευξη μεγαλύτερης διείσδυσης των eID λύσεων απαιτείται η ανάπτυξη και παροχή ηλεκτρονικών υπηρεσιών προς όφελος του πολίτη. Σημαντική είναι η παροχή απλοποιημένων λύσεων, που μπορεί να τονώσει ακόμη περισσότερο το αγοραστικό ενδιαφέρον. Στο πλαίσιο αυτό, η ενημέρωση και «καθοδήγηση» των εμπλεκομένων (πάροχοι υπηρεσιών, επιχειρήσεις) είναι καταλυτική για την επιτυχία του εγχειρήματος. Η ανάπτυξη αυτή, βέβαια, πρέπει να γίνει υπό ένα πλαίσιο διαλειτουργικότητας που θα αξιοποιεί τις υφιστάμενες υποδομές και τα ευρήματα των πιλοτικών

προγραμμάτων (π.χ. STORK 19 χώρες). Ένα ενιαίο σύστημα ταυτοποίησης σε επίπεδο Ευρωπαϊκής Ένωσης είναι μια πολύ βάσιμη σκέψη προς αυτή την κατεύθυνση. Έτσι θα οδηγηθούμε σταδιακά σε νέα επιχειρησιακά μοντέλα, για τα οποία η χρήση των ψηφιακών υπογραφών επαναπροσδιορίζεται διακριτά από τις εφαρμογές ΚΠ.

Αν και η επίδειξη για τη μελλοντική χρήση των ηλεκτρονικών υπογραφών και της ηλεκτρονικής ταυτότητας σ' ένα διασυνοριακό πλαίσιο ήταν πολλά υποσχόμενη, εντοπίστηκαν τα παρακάτω «ανοιχτά» ζητήματα :

- Η αξιοποίηση των ηλεκτρονικών υπογραφών και της ηλεκτρονικής ταυτότητας και η ευαισθητοποίηση γύρω από τη χρήση αυτών των τεχνολογιών είναι ανησυχητικά χαμηλή.

- Το κανονιστικό πλαίσιο είναι υπερβολικά περίπλοκο και ασαφές για τις ηλεκτρονικές υπογραφές, ενώ για την ηλεκτρονική ταυτοποίηση είναι μάλλον ανύπαρκτο, αν και απολύτως αναγκαίο, πόσο μάλλον υπό το πρίσμα της ανάγκης για διασυνοριακή αναγνώριση των πολιτών-χρηστών.

- Χρειάζεται βελτίωση η χρησιμοποιούμενη τεχνολογία για σκοπούς ταυτοποίησης, ενώ παράλληλα η ανάπτυξη προτύπων και η συνεργασία μεταξύ των κρατών-μελών είναι αναμφισβήτητης σημασίας.

- Νέες προκλήσεις, όπως το cloud πρέπει να αντιμετωπιστούν.

- Ζητήματα που αφορούν στην προστασία των προσωπικών δεδομένων και της ιδιωτικότητας είναι απολύτως κρίσιμα και πρέπει να αντιμετωπισθούν κυρίως υπό τη σκοπιά του πλεονεκτήματος ώστε να μπορούν να συμβάλλουν στην προώθηση της ηλεκτρονικής ταυτότητας καθώς και της χρήσης των ηλεκτρονικών υπογραφών και όχι να αποτελούν ανασταλτικό παράγοντα για την εφαρμογή τους.

- Ταυτοποίηση μη φυσικών προσώπων.

Τα κριτήρια, για την μέτρηση των αποτελεσμάτων προόδου, ταυτίζονται με τις λειτουργικές απαιτήσεις της ΚΠ. Ωστόσο, το πιο κρίσιμο είναι να βρεθεί η κρίσιμη μάζα για την εφαρμογή της ΚΠ, να δοθεί η απαιτούμενη βαρύτητα για τα ζητήματα ασφάλειας, αξιοπιστίας, εμπιστευτικότητας και ιδιωτικότητας και τέλος, να αναδειχθεί η χρηστικότητα και η χρησιμότητα της εφαρμογής ΚΠ στην καθημερινότητα του πολίτη.

Πρέπει επιπλέον να αναφέρουμε ότι ιδιαίτερη μνεία έγινε για τη χρήση της ηλεκτρονικής ταυτοποίησης και των ψηφιακών υπογραφών στον ιατρικό τομέα. Αναφέρθηκε το θέμα των ευαίσθητων δεδομένων και η πολυπλοκότητα στη διαχείριση του ιατρικού φακέλου. Εντούτοις, όπως συνειδητά δεν αναφέραμε το EPSO προηγουμένως, στην αναφορά των σημαντικότερων έργων που έχουν γίνει σε επίπεδο ΕΕ, δεν θα αναφέρουμε ούτε σε αυτό το σημείο, αναλυτικά συμπεράσματα. Ο λόγος είναι διττός και αφορά αφενός στην πολυπλοκότητα του ζητήματος χρήσης των ιατρικών δεδομένων του πολίτη-ασθενή και αφετέρου στην προσέγγισή μας ότι στην εφαρμογή μιας εθνικής λύσης ΚΠ, για

ταυτοποίηση και αυθεντικοποίηση, δεν πρέπει να δοθεί και η διάσταση της διαχείρισης του ιατρικού φακέλου του ασθενή. Εκτιμούμε ότι ο ιατρικός φάκελος και η διαχείριση του θέματος της ταυτοποίησης του ασθενή είναι ένα μεγάλο θέμα από μόνο του και πρέπει να εντοπισθεί απομονωμένα από άλλες εφαρμογές της ΚΠ.

Στο workshop για την εμπιστοσύνη και την αξιοπιστία στις ηλεκτρονικές συναλλαγές, οι συμμετέχοντες από τους ιδιωτικούς φορείς του κλάδου παρείχαν δεδομένα και στατιστικά στοιχεία τα οποία δεν είχαν δημοσιευτεί στο παρελθόν, έτσι ώστε να υπάρξει ουσιαστική συζήτηση και ποιοτικότερο αποτέλεσμα.

Η συμμετοχή σε online δραστηριότητες προϋποθέτει εμπιστοσύνη και η αξιοπιστία. Η έλλειψη εμπιστοσύνης των καταναλωτών εξακολουθεί να αποτελεί μεγάλο εμπόδιο για το ηλεκτρονικό εμπόριο στην Ευρώπη, ιδίως για τις διασυνοριακές συναλλαγές. Για το λόγο αυτό, τα όποια μέτρα πρέπει να στοχεύουν στην αύξηση της αξιοπιστίας και της εμπιστοσύνης για την ενδυνάμωση των ηλεκτρονικών συναλλαγών και τη μείωση του κατακερματισμού της αγοράς , δημιουργώντας ταυτόχρονα συνθήκες ανταγωνισμού.

Τέσσερα είναι τα κύρια ερωτήματα που τέθηκαν:

- Ποια είναι τα κυριότερα ζητήματα για το θέμα της εμπιστοσύνης σήμερα;
- Ποιες είναι οι κύριες δράσεις που θα μπορούσαν να ληφθούν άμεσα για την αντιμετώπιση των ζητημάτων εμπιστοσύνης ειδικά στις διασυνοριακές συναλλαγές;
- Ποιες είναι οι υπάρχουσες τεχνολογίες για τη στήριξη των καταναλωτών και την εγκαθίδρυση της εμπιστοσύνης σε ένα διασυνοριακό ηλεκτρονικό περιβάλλον;
- Ποιοι είναι οι διαθέσιμοι μηχανισμοί εξασφάλισης της εμπιστοσύνης σήμερα, που μπορούν να συμβάλουν στην ευαισθητοποίηση των καταναλωτών και των επιχειρήσεων;

Το αποτέλεσμα του workshop ήταν σαφές: υπάρχει ανάγκη για περαιτέρω διερεύνηση των επιλογών που θα βοηθήσουν στην εγκαθίδρυση σχέσεων εμπιστοσύνης στις διασυνοριακές συναλλαγές, χωρίς ωστόσο να προκύψει σαφής κατεύθυνση για τα υφιστάμενα ή νέα σχήματα εμπιστοσύνης.

Η δημιουργία ενός μοντέλου πιστοποίησης -σε εθελοντική βάση ή υποστηριζόμενο από κοινοτική ρύθμιση που να καθορίζει ελάχιστα κριτήρια- βασιζόμενο στα υφιστάμενα εθνικά μοντέλα πιστοποίησης έλαβε ευρεία αποδοχή. Ένα τέτοιο σχήμα εμπιστοσύνης θα μπορούσε να είναι ένα νέο εργαλείο που θα παρέχει πειστήρια στον πελάτη ότι ο πάροχος υπηρεσιών συμμορφώνεται με τους κανόνες, ανεξάρτητα από το κράτος μέλος στο οποίο ανήκει. Η εμπλοκή της ΕΕ για μία από κοινού ρύθμιση των σχημάτων εμπιστοσύνης θεωρήθηκε καταλυτική. Εντούτοις, στο συγκεκριμένο workshop ήταν έντονο το κλίμα του προβληματισμού για τα περιθώρια της εγκαθίδρυσης και διατήρησης της εμπιστοσύνης των online και offline συναλλαγών.

Πρέπει να αποφύγουμε, μήπως, τη χρήση ψηφιακής υπογραφής στις εφαρμογές ΚΠ; Η απάντηση είναι όχι, απλώς προτείνεται να τη χρησιμοποιήσουμε στο τελευταίο βήμα μιας συναλλαγής.

Για την βέλτιστη διαχείριση των εφαρμογών ΚΠ είναι απαραίτητη η εναρμόνιση των νομικών, επιχειρησιακών και τεχνικών παραμέτρων. Αυτές οι παράμετροι είναι εκείνες που θα προσδιορίσουν και θα κατευθύνουν τη σχεδιαστική επιλογή για μια λύση ΚΠ.

4.5. Λύσεις για Ασφάλεια και Διαλειτουργικότητα με άλλα Συστήματα ΚΠ

Συνοψίζοντας τη γνώση από την ανάλυση της Ευρωπαϊκής πρακτικής, αλλά και των μελετών και λύσεων που έχουν ανακύψει από τα αποτελέσματα των ευρωπαϊκών προγραμμάτων, που ασχολήθηκαν με το θέμα της ηλεκτρονικής ταυτοποίησης και των συστημάτων ηλεκτρονικής ταυτότητας, θα επιχειρήσουμε να δώσουμε το στίγμα της δικής μας προσέγγισης για την Ελληνική ΚΠ και ταυτόχρονα να εντοπίσουμε σημαντικές σύγχρονες και καινοτόμες λύσεις που μπορούν να αξιοποιηθούν στα πλαίσια της σχεδιαστικής επιλογής.

Πρώτα από όλα, όμως, πρέπει να εντοπίσουμε το πρόβλημα, στο οποίο πρέπει να δώσουμε λύση.

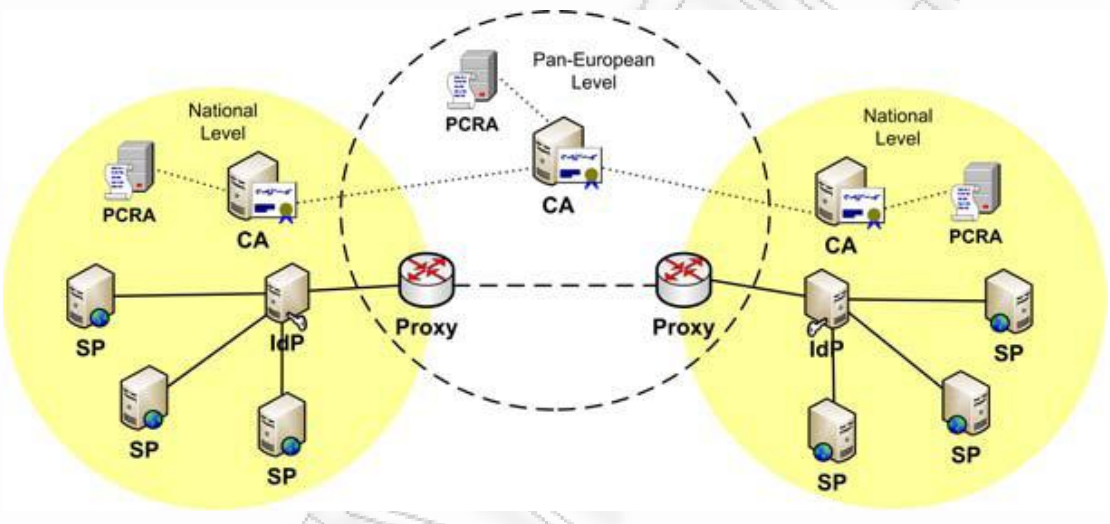
Ένας Ευρωπαίος πολίτης μπορεί να ταξιδέψει ανά την Ευρώπη κάνοντας χρήση της εθνικής του ΚΠ, ως ταξιδιωτικό έγγραφο για να αποδείξει την ταυτότητά του, δεν έχει όμως την ίδια δυνατότητα στον ψηφιακό κόσμο. Πως μπορεί, δηλαδή, ένας Ευρωπαίος πολίτης να αποκτήσει πρόσβαση σε ηλεκτρονικές υπηρεσίες που παρέχονται από άλλο κράτος μέλος, και πως το εθνικό σύστημα του επιθυμητού κράτους μέλους θα μπορούσε να διαχειρισθεί και να επιβεβαιώσει τα στοιχεία ενός μη εθνικού «εγγράφου».

Με λίγα λόγια, η εκάστοτε ΚΠ δεν μπορεί να αναγνωρισθεί από τα επιμέρους εθνικά συστήματα διαχείρισης ταυτοτήτων, αν αυτά δεν είναι συμβατά μεταξύ τους και άρα δεν μπορεί να αποτελέσει εργαλείο για την αυθεντικοποίηση του χρήστη στις ηλεκτρονικές του συναλλαγές, σε πανευρωπαϊκό επίπεδο, μέχρι να λυθούν τα προβλήματα συμβατότητας μεταξύ των επιμέρους συστημάτων.

Γενικά εξαιτίας της πολυμορφίας αυτών των συστημάτων, πρέπει να διασυνδέονται με τρόπο τέτοιο που η ταυτότητα του χρήστη για ένα σύστημα, να μπορεί να γίνεται αποδεκτή κι από άλλο. Αυτό αποτελεί ένα τυπικό πρόβλημα διαλειτουργικότητας, για συστήματα που βρίσκονται και εντός συνόρων μιας χώρας.

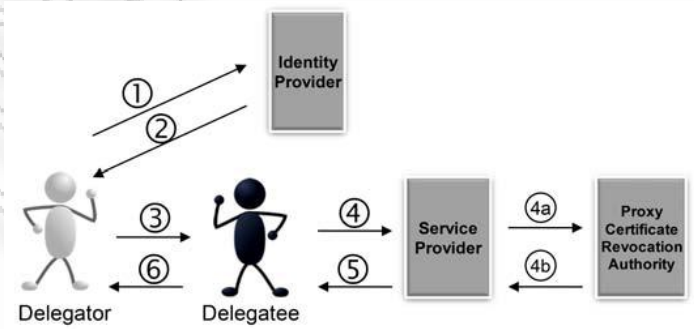
Οι Sergio Sánchez García και Ana Gómez Oliva από το Πολυτεχνείο της Μαδρίτης [18] προτείνουν μια σύγχρονη ενδιαφέρουσα λύση για την εξασφάλιση διαλειτουργικότητας σε πανευρωπαϊκό επίπεδο, η οποία βασίζεται στην εγκαθίδρυση σχέσεων εμπιστοσύνης.

Η κεντρική ιδέα είναι να δημιουργηθούν κύκλοι εμπιστοσύνης, τόσο σε εθνικό επίπεδο μεταξύ των επιμέρους τοπικών συστημάτων, όσο και σε ευρωπαϊκό μεταξύ των επιμέρους εθνικών συστημάτων, που θα συνδέουν τις αρχές ταυτοποίησης (Identity Providers, για τους σκοπούς της ενότητας) και τους παρόχους υπηρεσιών (Service Providers) που βρίσκονται στο ίδιο επίπεδο. Στο σχήμα αυτό, είναι απαραίτητη η αντιστοίχιση των επιμέρους στοιχείων αυθεντικοποίησης (token mapping), με κοινά στοιχεία αυθεντικοποίησης που θα εγγυώνται τη διαλειτουργικότητα των υπηρεσιών, μέσω της χρήσης ψηφιακών πιστοποιητικών X.509. Με τον τρόπο αυτό, ουσιαστικά, επιτυγχάνουμε την τη σύνδεση των επιμέρους εθνικών αρχών πιστοποίησης με μια κεντρική Αρχή Πιστοποίησης. Η κεντρική Αρχή Πιστοποίησης θα παρέχει τις κατάλληλες εγγυήσεις για τα πιστοποιητικά που εκδίδουν οι εθνικές αρχές και επομένως το ζήτημα της χρήσης ενός πιστοποιητικού σε άλλη χώρα φαίνεται να επιλύεται.



Εικόνα 18-Προτεινόμενη αρχιτεκτονική διαλειτουργικότητας

Η σημαντικότερη καινοτομία που εισάγουν είναι ένα μοντέλο αρχιτεκτονικής που να μπορεί να υποστηρίξει τη δυναμική εξουσιοδότηση ενός χρήστη από τον κάτοχο της ταυτότητας με τη χρήση των SAML δηλώσεων (attribute assertions) των X.509 πιστοποιητικών. Τα σχετικά πιστοποιητικά που χρησιμοποιούνται ονομάζονται X.509 Proxy πιστοποιητικά.



Εικόνα 19- Διαδικασία εξουσιοδότησης

Η βασική διαφορά των X.509 Proxy έγκειται στον τρόπο έκδοσής τους. Τα πιστοποιητικά αυτά δεν εκδίδονται από κάποια Αρχή Πιστοποίησης, όπως τα υπόλοιπα ψηφιακά πιστοποιητικά, αλλά από οποιαδήποτε οντότητα-κάτοχο πιστοποιητικού. Η ιδέα είναι ότι η εμπιστοσύνη που παρέχεται στο πιστοποιητικό του πολίτη, διαχέεται και στην εξουσιοδότηση-δηλαδή στο X.509 Proxy πιστοποιητικό - του πολίτη σε τρίτο, καθιστώντας τον πολίτη, μια ευέλικτη αρχή πιστοποίησης. Προκειμένου, ωστόσο, να διασφαλισθεί το ασφαλές και ακέραιο της διαδικασίας, τα πιστοποιητικά αυτά εμπλουτίζονται με SAML δηλώσεις, οι οποίες εμπεριέχουν πληροφορίες ασφάλειας που αφορούν στην εξουσιοδότηση και στον εξουσιοδοτούμενο. Τέτοιες δηλώσεις ασφάλειας μπορεί να είναι το διάστημα ισχύος της αυθεντικοποίησης, οι μέθοδοι αυθεντικοποίησης, οι ισχυρισμοί ελέγχου πρόσβασης συγκεκριμένων πόρων κ.α.. Έτσι, ο κάτοχος ενός πιστοποιητικού μπορεί να εκδώσει απευθείας ένα Proxy πιστοποιητικό για την οντότητα στην οποία επιθυμεί να παρέχει εξουσιοδότηση, με ασφαλή και έγκυρο τρόπο. Παρόλα αυτά, η πιο σημαντική αδυναμία της διαδικασίας εξουσιοδότησης αφορά στον τρόπο χρήσης της εξουσιοδότησης από τον εξουσιοδοτούμενο. Στην πραγματικότητα, είναι σε θέση να χρησιμοποιήσει το πιστοποιητικό καταχρηστικά, για περισσότερο χρονικό διάστημα από όσο του επιτρέπεται και πιθανά για άλλους λόγους και διαφορετικές συναλλαγές, χωρίς τη γνώση και συγκατάθεση του υποκειμένου, δημιουργώντας δυνητικά μεγάλα προβλήματα τόσο στο υποκείμενο, όσο και προς το τρίτο συμβαλλόμενο μέρος (το υποκείμενο καθώς είναι θύμα μη εξουσιοδοτημένης χρήσης και ο συναλλασσόμενος γιατί συναινεί σε μια πράξη χωρίς την πραγματική συγκατάθεση του άλλου μέρους της συναλλαγής).

Ακόμα όμως κι αν το πρόβλημα των εξουσιοδοτήσεων είναι υπαρκτό, δεν έχουμε δώσει σαφή απάντηση στο ζήτημα της ευθύνης της εγκυρότητας στο επίπεδο της διαλειτουργικότητας των συστημάτων αυτών. Το ρίσκο σε αυτές τις περιπτώσεις πέφτει στο μέρος της συναλλαγής που αποτελεί τον αποδέκτη της ΚΠ και ενός ψηφιακού πιστοποιητικού. Κατά τη χρήση λοιπόν της ΚΠ, ο κάτοχος μιας Εθνικής eID που συμμετέχει σε μια συναλλαγή σε άλλο κράτος μέλος, εξασφαλίζει ότι η κάρτα του είναι έγκυρη και τα πιστοποιητικά της σε ισχύ. Αυτό σημαίνει, ότι η υπηρεσία του άλλου κράτους μέλους εφόσον αποδεχτεί τη συναλλαγή και την διαπίστευση μέσω του Εθνικού eID, αναλαμβάνει το ρίσκο της συναλλαγής. Προκειμένου κάτι τέτοιο να είναι εφικτό, απαιτείται αρχικά η διασύνδεση των επιμέρους Εθνικών Αρχών Πιστοποίησης με μια Κεντρική Ευρωπαϊκή Αρχή Πιστοποίησης. Επιπλέον, ωστόσο, προϋποθέτει έλεγχο και αποδοχή των μεθόδων αυθεντικοποίησης και ελέγχου και του θεσμικού πλαισίου της κάθε χώρας.

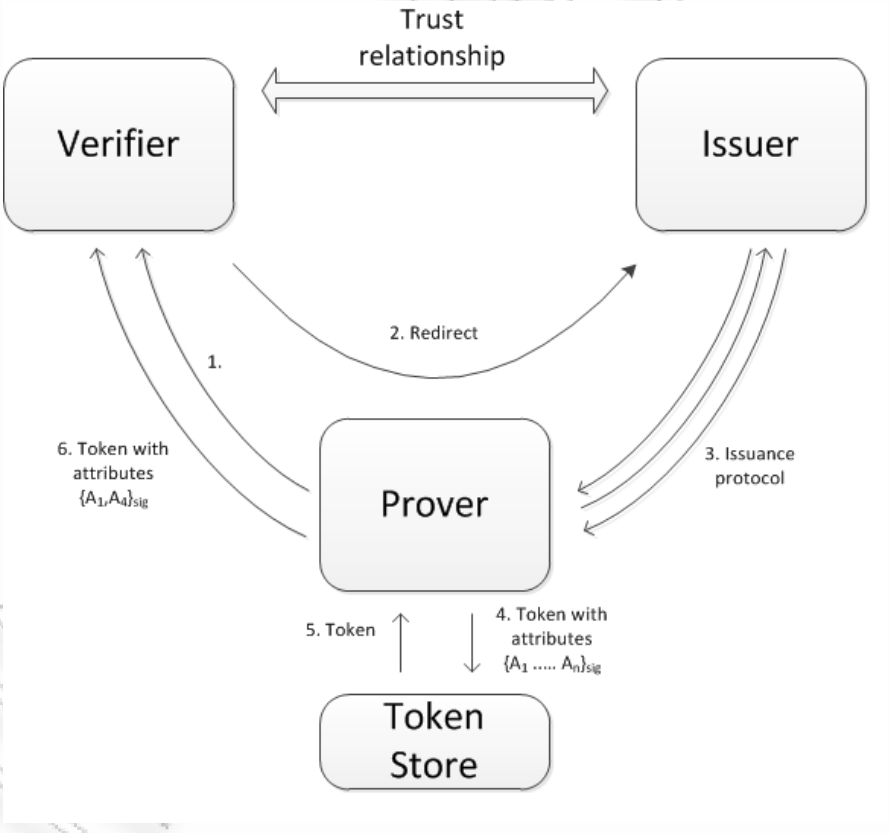
Επιπρόσθετα, στην περίπτωση των ψηφιακών υπογραφών, πέραν της προφανής διασύνδεσης των Αρχών Πιστοποίησης, το πρόβλημα είναι ακόμη εδώ, καθώς η νομικές εγγυήσεις και συνέπειες τις ψηφιακής υπογραφής μπορούν να προκαλέσουν σοβαρούς κινδύνους. Σε κάθε περίπτωση το βάρος πέφτει στον αποδέκτη μιας υπογραφής, που πρέπει να λάβει υπόψη την εγκυρότητά της, ώστε να αποδεχτεί και να προχωρήσει μια συναλλαγή. Στην πραγματικότητα, την ίδια στιγμή, αυτό το μέρος αξιολογεί ταυτόχρονα το ρίσκο υιοθέτησης της ψηφιακής υπογραφής που καθορίζεται από τη νομική περίπτωση, την ασφάλεια των κρυπτογραφικών αλγορίθμων που χρησιμοποιήθηκαν, τη συγκεκριμένη νομική ευθύνη που προκύπτει και την αξιοπιστία της Αρχής Πιστοποίησης από την οποία προέρχονται οι εγγυήσεις της υπογραφής.

«U-Prove»

«Η πρωτοποριακή U- Prove τεχνολογία κρυπτογράφησης μπορεί να χρησιμοποιηθεί για να ικανοποιήσει φαινομενικά αντικρουόμενες απαιτήσεις ασφάλειας και προστασίας της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες και τα συστήματα συναλλαγών.» [56]

Η ιστορία του U-Prove ξεκινά από τον Δρ. Stefan Brands [54] [55], ο οποίος προσπαθώντας να δώσει αποτελεσματική λύση στα προβλήματα ιδιωτικότητας που προκύπτουν από τις ηλεκτρονικές συναλλαγές καθιστώντας ικανή την χρήση και διακίνηση ακριβώς των αναγκαίων για τη συναλλαγή προσωπικών δεδομένων με ασφάλεια μέσω του U-Prove και ίδρυσε την Credentica, η οποία αγοράστηκε από την Microsoft το Μάρτιο του 2008.

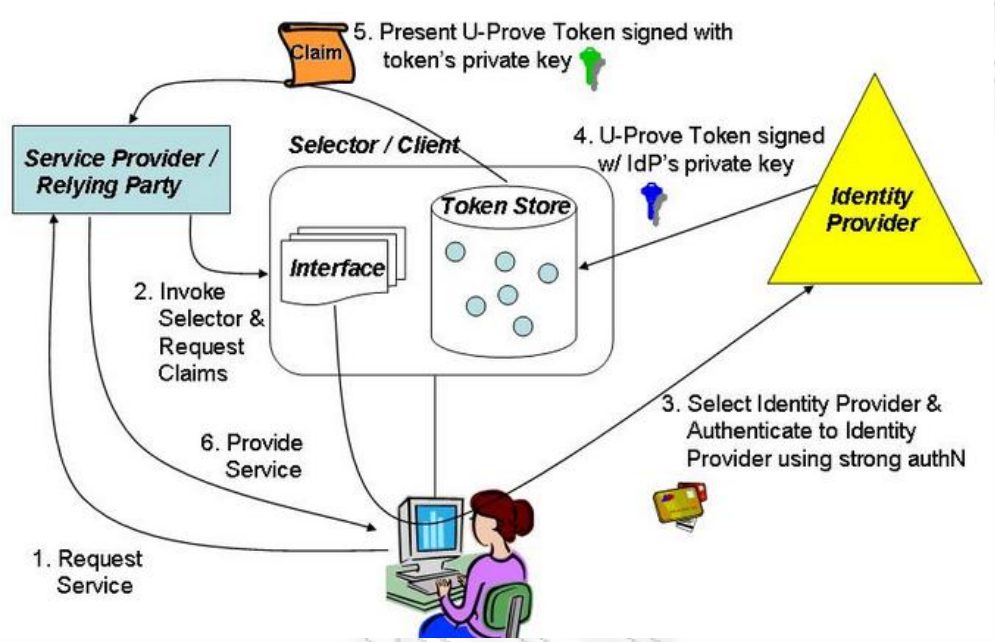
Το U-Prove επιτρέπει την δημιουργία secure ID tokens (ασφαλών ψηφιακών τεκμηρίων αυθεντικοποίησης), ως τμήματα δεδομένων που ενσωματώνουν ακριβώς την απαραίτητη πληροφορία που απαιτείται για μια συναλλαγή, με κρυπτογραφική προστασία ώστε να διασφαλισθεί ότι τα δεδομένα αυτά δεν μπορούν να πλαστογραφηθούν, να επαναχρησιμοποιηθούν, να σχετισθούν με τον ιδιοκτήτη τους ή να συνδεθούν με άλλα τεκμήρια αυθεντικοποίησης του ίδιου χρήστη.



Εικόνα 20-Χρήση secure ID tokens

Βασίζεται στις κρυπτογραφικές μεθόδους, ωστόσο, προσθέτει τη δυνατότητα απόκρυψης στοιχείων. Ουσιαστικά, προχωράει ένα βήμα παραπέρα τις δυνατότητες των PKI συστημάτων, εξασφαλίζοντας εκτός από την αντιστοίχηση ενός προσώπου με την

κρυπτογραφημένη πληροφορία που διακινεί, προκειμένου να πραγματοποιεί ασφαλείς συναλλαγές, χωρίς να προσβάλλεται η ιδιωτικότητά του και την αποκάλυψη της ελάχιστης δυνατής πληροφορίας του κατόχου για την πραγματοποίηση της αυθεντικοποίησης. Το U-Prove επιτρέπει στον χρήστη να διατηρεί, κατά περίπτωση, την ανωνυμία του, εισάγοντας επίσης και τη χρήση ψευδωνύμων.



Εικόνα 21-Συναλλαγή με U-Prove token

Η τελευταία έκδοση του U-Prove που προσφέρεται από τη Microsoft (CTP Release 2) περιλαμβάνει, επιπλέον, ένα σύνολο καινοτομιών, όπως την αποθήκευση των U-Prove tokens απευθείας στη συσκευή του χρήστη για μεγαλύτερη ευελιξία, εξασφάλιση διπλής προστασίας της πληροφορίας του χρήση που εμπεριέχεται στα ID tokens μέσω της χρήσης έξυπνων καρτών και τη χρήση τεχνολογιών cloud.

Ωστόσο, παρά τις αντικειμενικά πρωτοποριακές δυνατότητες που προσφέρει για την ασφάλεια και ιδιωτικότητα του χρήστη και την προστασία των συναλλαγών, η λύση αυτή δεν έχει τύχει ακόμη υιοθέτησης από τις Κυβερνήσεις και τους ιδιωτικούς φορείς.

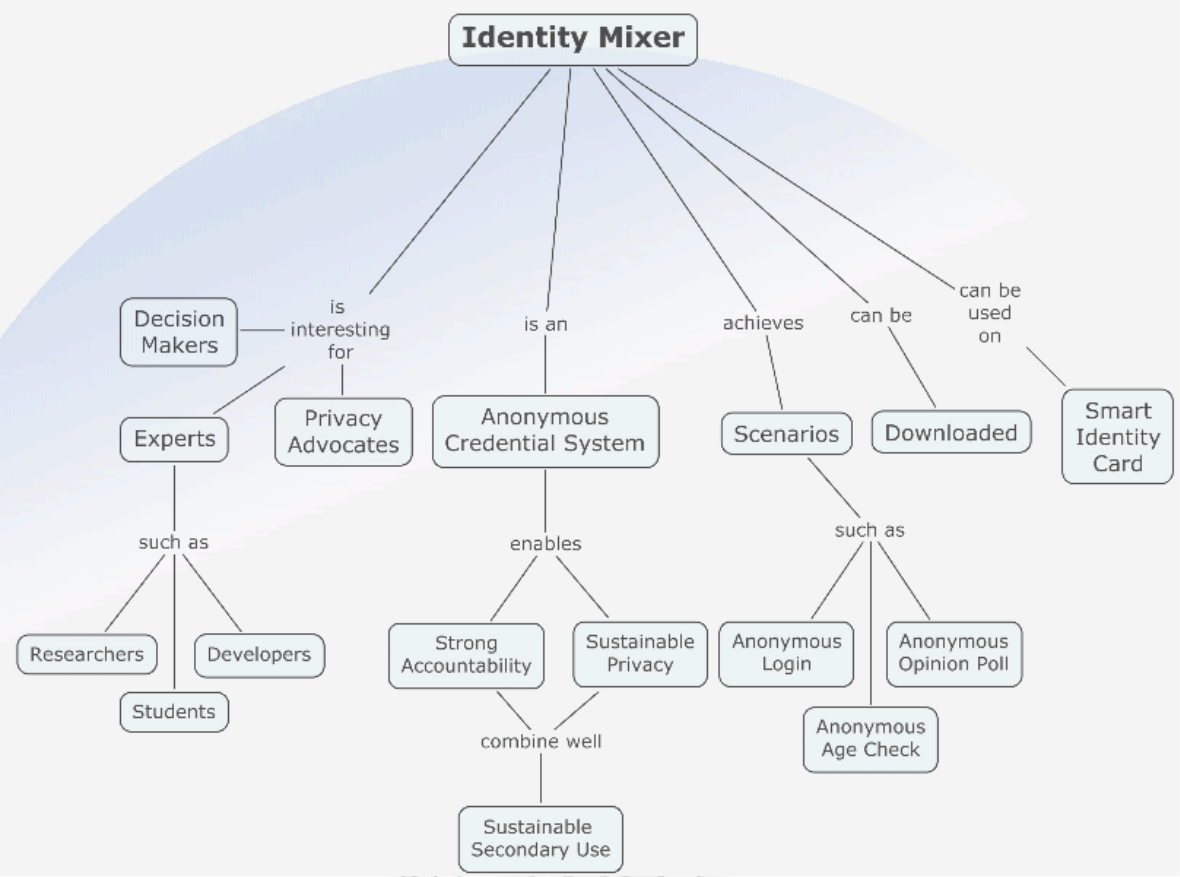
Πάντως, πρόσφατα, υιοθετήθηκε η λύση του U-Prove χρησιμοποιήθηκε στην υλοποίηση του Γερμανικού eID, από το Πανεπιστήμιο του Fraunhofer σε συνεργασία με τη Microsoft [17].

«IDEMIX (Identity Mixer IBM)»

Το IDEMIX ή Identity Mixer της είναι ένα σύστημα που αναπτύχθηκε από την IBM Research – της Ζυρίχης [58], βασισμένο στην ιδέα των «ανώνυμων credentials», που δίνει συγχρόνως τη δυνατότητα για ισχυρή αυθεντικοποίηση και ιδιωτικότητα στο ψηφιακό περιβάλλον.

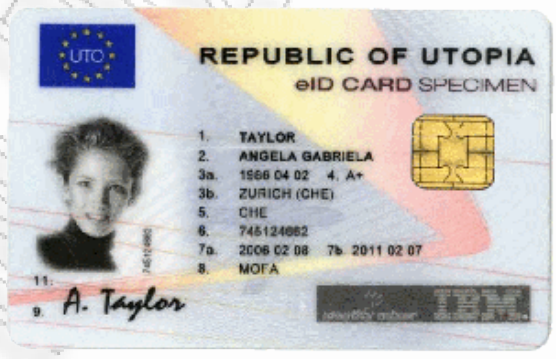
Τα «ανώνυμα credentials» λειτουργούν ουσιαστικά με τρόπο τέτοιο που να γίνεται εφικτή η πιστοποίηση του χρήστη, αποκαλύπτοντας επιλεκτικά μόνο δεδομένα αναγκαία για την αυθεντικοποίησή του, καλύπτοντας τα ίχνη των στοιχείων του χρήστη που αποκαλύπτονται κατά τις ηλεκτρονικές συναλλαγές. Έτσι, θα μπορούσαμε να πούμε ότι το λογισμικό IDEMIX της IBM εξαλείφει το ίχνος του συναλλασσόμενου με τη χρησιμοποίηση των τεχνητών στοιχείων ταυτότητας, γνωστών ως ψευδώνυμα, με στόχο την εξασφάλιση της ανωνυμίας του χρήστη σε συναλλαγές πραγματικού χρόνου [57].

Η διαδικασία του IDEMIX ουσιαστικά αφορά στην έκδοση πιστοποιητικού για την αυθεντικοποίηση του χρήστη, ώστε να μπορέσει να χρησιμοποιήσει μια υπηρεσία. Εκδίδεται για τον χρήστη ένα πιστοποιητικό, το οποίο περιλαμβάνει όλες τις πληροφορίες που τον πιστοποιούν, από μια έμπιστη τρίτη οντότητα, με χρήση του κατάλληλου λογισμικού. Για να μπορέσει ο χρήστης να χρησιμοποιήσει μια υπηρεσία, πρέπει να αυθεντικοποιηθεί από τον πάροχο της υπηρεσίας, χωρίς ωστόσο να απαιτείται η αποκάλυψη των πληροφοριών του, αλλά μόνο το παράγωγο της μετατροπής του πιστοποιητικού του από το IDEMIX. Το παράγωγο αυτό περιλαμβάνει μόνο ένα υποσύνολο των πληροφοριών του χρήστη. Με τη χρησιμοποίηση περίπλοκων κρυπτογραφικών αλγορίθμων, το IDEMIX πρακτικά δρα ως μεσάζων έτσι ώστε η πραγματική ταυτότητα του χρήστη να μην εκτίθεται ποτέ στον πάροχο της εκάστοτε επιθυμητής υπηρεσίας. Ο χρήστης μπορεί να εφαρμόσει τη διαδικασία αυτή, όσες φορές επιθυμεί, δίχως τα παράγωγα των πιστοποιητικών του να μπορούν να σχετισθούν μεταξύ τους και την επόμενη φορά που χρησιμοποιεί την υπηρεσία ή επικοινωνεί με τον πάροχο, ένα νέο κρυπτογραφημένο πιστοποιητικό μπορεί να χρησιμοποιηθεί [57].



Εικόνα 22-Περιγραφή Identity Mixer [57]

Το κύριο πρόβλημα που προσπαθεί να αντιμετωπίσει το IDEMIX σχετίζεται με τη διασπορά των προσωπικών δεδομένων του πολίτη, προκειμένου να έχει τη δυνατότητα χρήσης ηλεκτρονικών υπηρεσιών και εφαρμογών.



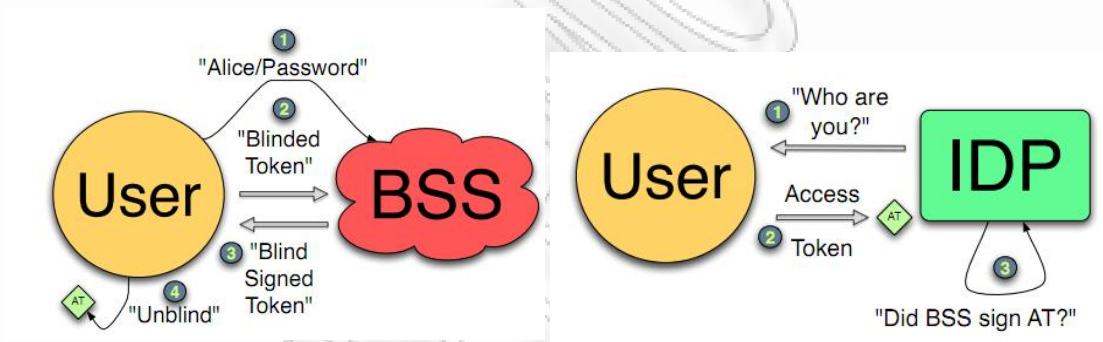
Εικόνα 23- eID με χρήση IDEMIX

Έχει εφαρμοστεί ήδη σε έξυπνη κάρτα (τύπου NXP JCOP 41 v2.2, mask 36 με 1536-bit Strong RSA keys μέγεθος κλειδιού, το οποίο μπορεί να επεκταθεί μέχρι τα 1984 bits) κερδίζοντας το βραβείο καινοτομίας στη Γερμανία το 2009, καθιστώντας ένα χρήστης ικανό να αποδείξει ότι είναι ο πραγματικός κάτοχος της κάρτας ή ότι έχει ορισμένες ιδιότητες, διατηρώντας παράλληλα την εμπιστευτικότητα των προσωπικών του δεδομένων και τη μη συσχέτιση του κατόχου της κάρτας με τις συναλλαγές που εκείνη χρησιμοποιείται.

[http://idemix.wordpress.com/smart-identity-card/] Τα επιπλέον χαρακτηριστικά που προσδίδει η ενσωμάτωση ενός αυτόνομου credential συστήματος στην έξυπνη κάρτα είναι η πρόσθετη ασφάλεια από μη αξιόπιστα τερματικά και η μεγαλύτερη ταχύτητα.

«PseudoID»

Το PseudoID είναι ένα μονόδρομο, συνεπές, μη σχετιζόμενο με το υποκείμενο σύστημα ελέγχου πρόσβασης [59], οποίο αυξάνει την ιδιωτικότητα στα συστήματα ομοσπονδιακής διαχείρισης ταυτότητας και είναι συμβατό με το OpenID (ένα δημοφιλές σύστημα ομοσπονδιακής διαχείρισης ταυτότητας) [59]. Το PseudoID έχει ως σκοπό να προστατεύσει τους χρήστες από την κοινοποίηση των ιδιωτικών στοιχείων σύνδεσης. Βασίζεται στην λογική της «τυφλής υπογραφής» που αναπτύχθηκε από τον David Chaum[35, η οποία στην πραγματικότητα είναι μια μορφή ψηφιακής υπογραφής στην οποία το περιεχόμενο ενός μηνύματος είναι μη ορατό προτού να υπογραφεί (blind signature) [83]. Η λειτουργία της τυφλής υπογραφής και η χρήση της σε έναν πάροχο πιστοποίησης παρουσιάζονται στα παρακάτω σχήματα.



Εικόνα 24 -Η λειτουργία του PseudoID [59]

Στην κατεύθυνση αυτή γίνεται ακόμη ερευνητική εργασίας και είναι σαφές, ότι η συγκεκριμένη τεχνολογία έχει ανοιχτά ζητήματα ασφάλειας.

Το συμπέρασμα που απορρέει από την προηγούμενη μελέτη είναι ότι χωρίς ένα ενιαίο Ευρωπαϊκό πλαίσιο, με σαφείς κανόνες, προδιαγραφές και εγγυήσεις, η επίτευξη διαλειτουργικότητας σε Ευρωπαϊκό επίπεδο δεν θα ήταν εφικτή, καθώς θα έθετε σε σοβαρό κίνδυνο τις θεμελιώδεις σχέσεις εμπιστοσύνης μέσω των Αρχών Πιστοποίησης.

4.6. Σύνοψη Κεφαλαίου

Στο Κεφάλαιο αυτό ο στόχος ήταν μέσα από τη μελέτη και ανάλυση της διεθνούς πρακτικής και την αξιολόγηση εφαρμοστέων λύσεων, να αντλήσουμε συμπεράσματα που θα

εξασφαλίσουν την αναγκαία γνώση ώστε να καταλήξουμε στην καλύτερη δυνατή επιλογή για την εφαρμογή της ΚΠ στην Ελλάδα.

Έτσι, στην πρώτη ενότητα του κεφαλαίου παρουσιάσαμε μια συγκριτική ανάλυση των Ευρωπαϊκών λύσεων για τις εφαρμογές ΚΠ, τόσο ως προς την τεχνολογία που χρησιμοποιούν, όσο και ως προς τις τεχνικές ασφάλειας που εφαρμόζουν και στις χρήσεις των ΚΠ.

Στη συνέχεια, ακολούθησε μια συνοπτική περιγραφή κάποιων Ευρωπαϊκών λύσεων ΚΠ, η επιλογή των οποίων έγινε με το κριτήριο της «αντιστοιχίας» με την Ελληνική περίπτωση.

Η μελέτη της δουλείας που έχει γίνει σε επίπεδο Ευρωπαϊκής Ένωσης είναι απολύτως σημαντική, καθώς τα αποτελέσματα και τα συμπεράσματα αυτών των δράσεων έχουν επηρεάσει σημαντικά, αν όχι καθοδηγήσει, τον τρόπο χρήσης και εφαρμογής των συστημάτων ΚΠ στην Ευρώπη. Από τα ευρωπαϊκά αυτά έργα, μάλιστα, έχει προκύψει ένα σύνολο προδιαγραφών, αλλά και τα πρότυπα με τα οποία οφείλουν να συμμορφώνονται οι επιμέρους εφαρμογές ΚΠ. Ιδιαίτερη αξία, έχει και η παρουσίαση των συμπερασμάτων του Ευρωπαϊκού Θεματολογίου για την Ευρώπη 2020, στην επίσημη συνεδρίαση του Ιουνίου, καθώς είναι η πιο σύγχρονη προσπάθεια σε ευρωπαϊκό επίπεδο, η οποία θέτει και τους επόμενους στόχους.

Η ασφάλεια και ιδιωτικότητα είναι σε κάθε περίπτωση από τα πιο κρίσιμα ζητήματα στην ατζέντα. Η αναζήτηση νέων λύσεων για τη διασφάλιση του μέγιστου δυνατού βαθμού ασφάλειας των συστημάτων αυθεντικοποίησης και ηλεκτρονικής ταυτοποίησης είναι θεμέλιος λίθος για την εξασφάλιση της αξιοπιστίας των συστημάτων αυτών. Η δημιουργία ενός Ευρωπαϊκού σχήματος εμπιστοσύνης, το οποίο θα συμβάλλει στην εγκαθίδρυση σχέσεων εμπιστοσύνης εντός και εκτός συνόρων, είναι η νέα πρόκληση για την Ευρώπη.

Η διασφάλιση της διαλειτουργικότητας σε ένα ενιαίο Ευρωπαϊκό περιβάλλον είναι απαραίτητη προϋπόθεση για τη μετάβαση στην ενιαία ψηφιακή αγορά. Σε αυτό ακριβώς το πλαίσιο, σύγχρονες λύσεις εξασφάλισης της διασυνοριακής διαλειτουργικότητας μεταξύ συστημάτων διαχείρισης ηλεκτρονικών ταυτοτήτων είναι ιδιαίτερα σημαντικές, ώστε να μας οδηγήσουν σε ένα σύγχρονο και επίκαιρο μοντέλο εφαρμογής για την Ελληνική ΚΠ.

5. ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΤΗΣ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΚΑΡΤΑΣ ΠΟΛΙΤΗ

Η ασφάλεια της πληροφορίας αποτελεί σημαντικό ζήτημα για την ηλεκτρονική κοινωνία ιδιαίτερα στην εποχή της πλήρους ανάπτυξης του διαδικτύου. Ωστόσο, ένα πλήθος ζητημάτων ασφάλειας εξαιτίας των εγγενών αδυναμιών του διαδικτύου εγείρονται. Συνεπώς, προκύπτει η ανάγκη για δημιουργία ασφαλών συστημάτων που βασίζονται στην αυθεντικοποίηση των χρηστών και στην κρυπτογραφία.

Τα συστήματα ταυτοποίησης είναι σχεδόν συνυφασμένα με την ανάγκη λειτουργίας τους μέσα σε ένα ασφαλές περιβάλλον. Για το λόγο αυτό, περισσότερη βαρύτητα δίνεται στα ζητήματα που αφορούν στην ασφάλεια, είτε υπό την έκφανση της ιδιωτικότητας και της διασφάλισης της προστασίας των προσωπικών δεδομένων του πολίτη που αλληλεπιδρά μέσω των συστημάτων ηλεκτρονικής ταυτοποίησης και που χρησιμοποιεί την ΚΠ, είτε υπό την έννοια της ασφάλειας των ίδιων συστημάτων με σκοπό την εξασφάλιση της αυθεντικότητας, της ακεραιότητας, της εμπιστοσύνης και της μη αποποίησης για τις συναλλαγές που σχετίζονται και διεκπεραιώνονται μέσω της ΚΠ. Αυτό μας οδηγεί στο συμπέρασμα ότι η επιτυχής εφαρμογή τέτοιων συστημάτων και ειδικότερα της ΚΠ για τη χώρα μας περνάει πρώτα από την εξασφάλιση των προϋποθέσεων και απαιτήσεων περί ασφάλειας.

Εξαιτίας μάλιστα της ανάγκης για διασυνοριακή ηλεκτρονική ταυτοποίηση και χρήση ηλεκτρονικών ταυτοτήτων και διαλειτουργικότητα των δεδομένων, διαδικασιών και συστημάτων ηλεκτρονικής ταυτοποίησης, γίνεται επιτακτική αλλά και περισσότερο πολύπλοκη η απαίτηση για ασφάλεια σε ένα διεθνές περιβάλλον. Πρέπει, λοιπόν, να εντοπισθούν τεχνολογικές λύσεις μέσω των οποίων να επιτυγχάνεται η ασφάλεια και η ιδιωτικότητα των αποθηκευμένων δεδομένων και να παρέχονται τα εχέγγυα στον κάτοχο της κάρτας, στη χώρα έκδοσής της και γενικότερα σε όποιον είναι κατάλληλα εξουσιοδοτημένος για την ανάγνωση των δεδομένων, ότι τα δεδομένα δεν έχουν υποστεί μη εξουσιοδοτημένες τροποποιήσεις από τη στιγμή που κατεγράφησαν από την αρμόδια αρχή έκδοσης έως την ανάγνωσή τους.

Στην κατεύθυνση αυτή, ο Διεθνής Οργανισμός ICAO, η Ευρωπαϊκή Επιτροπή Προτυποποίησης CEN και η Γερμανική υπηρεσία ασφάλειας πληροφοριών BSI έχουν αναπτύξει προδιαγραφές για τη χρήση κρυπτογραφικών τεχνικών που κατά κύριο λόγο εμπλέκουν τη χρήση υποδομής δημοσίου κλειδιού (PKI), πρωτόκολλα αυθεντικοποίησης και εγκαθίδρυσης κοινού μυστικού κλειδιού, μηχανισμούς ελέγχου πρόσβασης στα αποθηκευμένα δεδομένα κλπ. με γνώμονα τη διασφάλιση όσο το δυνατών μεγαλύτερων επιπέδων ασφάλειας.

Στο κεφάλαιο αυτό επιχειρείται μια συνοπτική και περιεκτική παρουσίαση της τεχνολογικής υποδομής που υποστηρίζει τα συστήματα διαχείρισης ταυτότητας στην ηλεκτρονική διακυβέρνηση, γνώση που είναι χρήσιμη για την εφαρμογή της ΚΠ και στην Ελλάδα. Θα προσπαθήσουμε να δούμε πως απαντά η τεχνολογία στις τέσσερις απαιτήσεις για την

ασφάλεια, *αυθεντικότητα, ακεραιότητα, εμπιστευτικότητα* και *μη αποποίηση*. Στόχος μας είναι η παρουσίαση εκείνων των εννοιών και επιτυχημένων τεχνολογικών λύσεων που χρησιμοποιούνται ήδη από τα περισσότερα συστήματα διαχείρισης ταυτότητας.

Η κριτική μας ματιά είναι απαραίτητη, καθώς όπως έχουμε ήδη αναλύσει σε προηγούμενες ενότητες, τα συστήματα ηλεκτρονικής ταυτοποίησης εντάσσονται σε ένα ιδιαίτερα ρευστό περιβάλλον, καθώς εξαρτώνται από ένα πλήθος μη τεχνολογικών παραμέτρων, γεγονός που σημαίνει συνήθως δύο πράγματα: α)η βέλτιστη τεχνικά λύση πιθανά δεν αποτελεί απαραιτήτως και τη βέλτιστη λύση, συνολικά, για το εγχείρημα της ηλεκτρονικής ταυτοποίησης και β)η όποια τεχνική λύση πρέπει να είναι και πρακτικά εφαρμόσιμη, καθώς άλλοι παράγοντες, όπως κοινωνικοπολιτικές συνθήκες, ήθη, διοικητικές δομές, αντιστάσεις μπορούν να αποτελέσουν ανασταλτικούς παράγοντες για την ομαλή και επιτυχή υιοθέτηση της λύσης. Επομένως, συμπεραίνουμε ότι η λήψη αποφάσεων για τις τεχνολογικές επιλογές στην Εφαρμογή της ΚΠ στην Ελλάδα, αλλά πολύ δε περισσότερο και η υλοποίηση της όποιας λύσης , πρέπει να γίνεται πάντα υπό το πρίσμα της ανάλυσης όλων των παραμέτρων που επηρεάζουν άμεσα ή έμμεσα και επιδρούν στο περιβάλλον εφαρμογής της λύσης.

Για το λόγο αυτό, οι διεθνείς οργανισμοί επισημαίνουν ως υποχρεωτικές κάποιες τεχνολογικές λύσεις και ως προαιρετικές κάποιες άλλες, παρέχοντας σχετική ελευθερία στα κράτη που εφαρμόζουν συστήματα ηλεκτρονικής ταυτοποίησης και διαχείρισης ηλεκτρονικών ταυτοτήτων να επιλέγουν λύσεις που ταιριάζουν περισσότερο στο επιχειρησιακό τους μοντέλο και στο εσωτερικό τους περιβάλλον, χωρίς ωστόσο να αίρεται η προϋπόθεση για διαλειτουργικότητα μεταξύ των συστημάτων αυτών. Έτσι, πέρα την επισήμανση για υποχρεωτική εφαρμογής μηχανισμών ασφάλειας σε συστήματα ταυτοποίησης, το κάθε κράτος είναι σε θέση να κάνει και τις δικές του επιλογές σε ένα σύνολο από επιμέρους ζητήματα που σχετίζονται με την ασφάλεια (αυθεντικοποίηση, ελέγχου πρόσβασης, αυτοματοποιημένης διέλευσης συνόρων κλπ) επιλέγοντας ποιους από τους προτεινόμενους επιπρόσθετους προαιρετικούς μηχανισμούς πρόκειται να εφαρμόσει.

5.1. Ιδιωτικότητα, Προσωπικά Δεδομένα και Ανωνυμία

Προκειμένου να κατανοήσουμε την κρισιμότητα των απαιτήσεων ασφάλειας και να μπορέσουμε να αντιμετωπίσουμε αποτελεσματικότερα τους κινδύνους, πρέπει πρώτα να κατανοήσουμε ποια αγαθά καλούμαστε να προστατεύσουμε, πόσο σημαντικά είναι για τον πολίτη και το σεβασμό των δικαιωμάτων του, καθώς επίσης και τους κίνδυνους που μπορεί να προκύψουν.

Στην κατεύθυνση αυτή σημαντικές έννοιες είναι η ιδιωτικότητα, η ανωνυμία και τα προσωπικά δεδομένα.

Ιδιωτικότητα θα μπορούσαμε να πούμε ότι είναι το δικαίωμα του πολίτη να επιλέγει ποιες πληροφορίες του είναι κοινοποιήσιμες, σε ποιον, πότε και με ποιος τρόπους. Τα

προηγούμενα χρόνια έχει γίνει προσπάθεια για την ακριβή απόδοση του ορισμού της έννοιας της ιδιωτικότητας.

Σημαντικότεροι ορισμοί είναι:

- «Το δικαίωμα του κάθε ανθρώπου ή ομάδας ατόμων ή οργανισμών, να καθορίζουν από μόνοι τους, πότε, πώς και σε ποιό βαθμό οι προσωπικές τους πληροφορίες θα γίνονται γνωστές σε τρίτους.» (Alen Westin, 1967 [60])
- «Το δικαίωμα του να είναι κανείς μόνος του.» (Warren & Brandeis, 1890 [60])
- Οι τρεις διαστάσεις της ιδιωτικότητας σύμφωνα με τον Rosenberg (1992) [60]:
    - Χωρική Ιδιωτικότητα (territorial privacy): Προστασία του στενού φυσικού χώρου που περιβάλει ένα άτομο (π.χ. χώρος εργασίας).
    - Ιδιωτικότητα του ατόμου (privacy of the person): Προστασία του ατόμου από αναίτιες παρεμβάσεις τρίτων σε αυτό (π.χ. φυσική έρευνα χωρίς δικαιολογία, έλεγχο για κατοχή φαρμάκων, ανήθικη και παράνομη έρευνα για την απόκτηση προσωπικών πληροφοριών κλπ.).
    - Ιδιωτικότητα της πληροφορίας (informational privacy): Το δικαίωμα του κάθε ατόμου να ελέγχει αν και με ποιο τρόπο τα προσωπικά του δεδομένα συλλέγονται, αποθηκεύονται επεξεργάζονται και διαμοιράζονται σε τρίτους.

Στο πλαίσιο αυτό πρέπει να ορίσουμε και τα προσωπικά δεδομένα. Μάλλον, ο πιο περιεκτικός ορισμός είναι η θεώρηση των προσωπικών δεδομένων (personal data) ως κάθε πληροφορία που προσδιορίζει την προσωπικότητα ενός ατόμου. (Fischer-Hubner, 2001) [60]. Αντίστοιχα, η προστασία προσωπικών δεδομένων (data protection), αφορά στην προστασία των προσωπικών δεδομένων με σκοπό τη διαφύλαξη της ιδιωτικότητας και αποτελεί μέρος της γενικής έννοιας της ιδιωτικότητας [60].

Ανωνυμία, αντίστοιχα, είναι το δικαίωμα των χρηστών που διασφαλίζει περιβάλλον στο οποίο η ταυτότητα του χρήστη παραμένει κρυφή. Η αποκάλυψη πληροφοριών από τις οποίες μπορεί να προσδιοριστεί η ταυτότητα ενός προσώπου (π.χ. επάγγελμα, διεύθυνση, χαρακτηριστικά, οικογενειακή κατάσταση, παλαιότερο ή παράλληλο ψευδώνυμο, θρησκευτικές ή πολιτικές πεποιθήσεις, σεξουαλικός προσανατολισμός, καταγωγή κλπ) αποτελεί παραβίαση της επιλογής του για ανωνυμία. Δεν επεκτείνεται, εντούτοις, εκτός νομίμων ορίων. Η χρήση της για την αποποίηση ευθύνης για παράνομες πράξεις είναι καταχρηστική.

5.2. Απειλές Ιδιωτικότητας

Ως χαρακτηριστικό που μπορεί να προσβάλει την ιδιωτικότητα του πολίτη νοείται εκείνο το χαρακτηριστικό που περιλαμβάνεται στην ΚΠ, η γνωστοποίηση του οποίου μπορεί να οδηγήσει σε αποκάλυψη των στοιχείων του κατόχου της κάρτας και σε συσχέτιση αυτού με τα δεδομένα και τις κινήσεις της κάρτας.

Τα στοιχεία της ΚΠ που προσδίδουν προστασία της ιδιωτικότητας οφείλουν να εξασφαλίζουν τον έλεγχο του κατόχου της κάρτας σχετικά με τα δεδομένα που γνωστοποιούνται, όποτε το επιθυμεί (επιλέγοντας μια συναλλαγή) και σε ποιον αυτά αποκαλύπτονται.

Προκειμένου να διασφαλίσουμε επαρκώς τα κρίσιμα σημεία για την ιδιωτικότητα, πρέπει πρώτα να εντοπίσουμε τις απειλές που μπορεί να τα προσβάλουν. Υπό αυτό το πλαίσιο, οι κίνδυνοι δεν πρέπει να αντιμετωπίζονται ως επιμέρους απειλές ως προς τις ευπάθειες των συστημάτων, αλλά και υπό το πρίσμα της πιθανότητας εμφάνισής τους. Η περιγραφή αυτή εμπεριέχει τον έλεγχο για την αποκάλυψη πληροφοριών σε περιπτώσεις μη εξουσιοδοτημένης πρόσβασης, ακούσια ταυτοποίηση του κατόχου της κάρτας, την καταγραφή του ιστορικού των συναλλαγών ταυτοποίησης και τη διασύνδεση με τον κάτοχο της κάρτας, τη διαρροή δεδομένων σε περιστασιακούς παρατηρητές και τα έννομα αποκάλυψη του ιδιοκτήτη των δεδομένων με υπερβολικά υψηλούς διασφάλισης συνδέονται με αυτό, τη χρήση της ψηφιακής υπογραφής ως διακριτικό ταυτότητας.

Υπάρχει μια μεγάλη ποικιλία από χαρακτηριστικά προστασίας της ιδιωτικής ζωής: από απλούς μηχανισμούς ελέγχου πρόσβασης PIN μέχρι εξελιγμένα πιστοποιητικά -με βάση μηχανισμούς ελέγχου πρόσβασης ή τομεακά μοναδικά αναγνωριστικά.

Αγαθό: Τα αγαθά αποτελούν το στόχο των απειλών. Στην ΚΠ τα σημαντικά αγαθά είναι συνήθως τα προσωπικά δεδομένα του πολίτη και η διασφάλιση της ανωνυμίας και ιδιωτικότητάς του. Η αποκάλυψη ή παραβίαση αυτών θέτει σε κίνδυνο και περαιτέρω στοιχεία του πολίτη όπως πληροφορίες για οικονομικά και περιουσιακά στοιχεία και οικονομικές συναλλαγές, ιατρικά δεδομένα, αγοραστικό ενδιαφέρον κ.α., τα οποία μπορεί να οδηγήσουν σε αποκάλυψη της προσωπικής του ζωής, αλλά ακόμη και σε απάτη εις βάρος του θίγοντας άμεσα άλλα αγαθά του, όπως η φυσική ιδιοκτησία, οικονομικά αγαθά και η φήμη του πολίτη. Σε κάθε περίπτωση η διασφάλιση των αγαθών είναι ζωτικής σημασίας υπό το πλαίσιο του σεβασμού του δικαιώματος του πολίτη στην ιδιωτικότητα. Οι ευπάθειες του συστήματος που οδηγούν σε έκθεση των προσωπικών πληροφοριών οδηγούν ταυτόχρονα σε απειλές της ιδιωτικότητας.

5.2.1. Απειλές

Κίνδυνος ιδιωτικότητας: κάθε ευπάθεια η οποία εκθέτει τα δεδομένα της κάρτας δημιουργεί κίνδυνο απέναντι στην προστασία προσωπικών δεδομένων.

Παρακάτω θα προσπαθήσουμε να παρουσιάσουμε τις πιο σημαντικές επιπτώσεις εξαιτίας των ευπαθειών ενός συστήματος -τους σημαντικότερους κινδύνους για τα προσωπικά στοιχεία του υποκειμένου των δεδομένων της ΚΠ [53]:

1. Παραποίηση περιεχομένου: Η παραποίηση του περιεχομένου μέσω της μη εξουσιοδοτημένης εγγραφής στο σύστημα αρχείων της κάρτας. Ένα τροποποιημένο UID θα μπορούσε, για παράδειγμα, να γίνει αποδεκτό ως αυθεντικό, αν δεν υπάρχουν τα κατάλληλα και επαρκή μέτρα ασφάλειας σε ισχύ, που να εξασφαλίζουν την ακεραιότητα

και αυθεντικότητα των δεδομένων. Για παράδειγμα, ένα αλλοιωμένο μοναδικό αναγνωριστικό μπορεί να γίνει αποδεκτό από τον πάροχο υπηρεσίας οδηγώντας σε μη επιθυμητές και πιθανά αρνητικές συνέπειες για τον κάτοχο της κάρτας, όπως πλαστοπροσωπία, άρνηση εξυπηρέτησης κλπ.

2. Υποκλοπή: Η παρακολούθηση της επικοινωνίας κάρτας-αναγνώστη από τρίτο και η αποκάλυψη των δεδομένων. Αυτή η απειλή είναι ιδιαίτερα σημαντική κυρίως στις ανεπαφικές κάρτες. Μπορεί πάντως να γίνει επικίνδυνη και στην περίπτωση επαφικού τσιπ αν, για παράδειγμα, δεν είναι θωρακισμένη η καλωδίωση του αναγνώστη, κατ' αναλογία, με την εγκατάσταση κακόβουλου λογισμικού στον ηλεκτρονικό υπολογιστή του χρήστη που δρα εν αγνοία του και χωρίς φυσικά τη συγκατάθεσή του.

3. Man-in-the-middle: Η διαφορά με την προηγούμενη απειλή είναι ότι ο «υποκλοπέας» δρα μεταξύ της κάρτας και του εξυπηρετητή /middleware, υποκλέπτοντας και παραποιώντας την επικοινωνία και με τις δύο πλευρές, καταφέρνοντας να εξαπατήσει και τα δύο συνδιαλεγόμενα μέρη.

4. Υπογραφή ψευδούς ή τροποποιημένου εγγράφου: Στην περίπτωση αυτή ο χρήστης δεν βλέπει το πραγματικό περιεχόμενο του εγγράφου και υπογράφει ένα διαφορετικό ανεπιθύμητο έγγραφο. Με τον τρόπο αυτό, ο πολίτης μπορεί να αποτελέσει θύμα απάτης ή ψευδούς συναλλαγής. Επιπλέον, πιθανότατα συμβαίνει παραποίηση των στοιχείων του χρήστη, χωρίς τη δυνατότητα διόρθωσης και ενέχει τον κίνδυνο τα δεδομένα αυτά να παρουσιασθούν σε τρίτους, χωρίς την συγκατάθεση του κατόχου, αλλά και χωρίς τη δυνατότητα ανάκλησης της ισχύος τους.

5. Αυθεντικοποίηση του χρήστη σε ψευδή εξυπηρετητή: Με τη σύνδεση του χρήστη στον εξυπηρετητή εξασφαλίζεται η πρόσβαση στις πληροφορίες του χρήστη και μάλιστα, όχι μόνο κατά τη διάρκεια της σύνδεσης από μη πραγματικά εξουσιοδοτημένη οντότητα.

6. Παραχώρηση της κάρτας σε τρίτο: Σε ορισμένες περιπτώσεις, η κάρτα μπορεί συνειδητά να εκχωρηθεί σε άλλο πρόσωπο, εξασφαλίζοντας μάλιστα τη νόμιμη χρήση αυτής. Ωστόσο, δεν είναι ενδεδειγμένη πρακτική και μπορεί να τεθούν σε κίνδυνο οι πληροφορίες του κατόχου, αλλά και ο ίδιος εξαιτίας πιθανής κακής χρήσης της κάρτας του από τον εξουσιοδοτούντα.

7. Απώλειας ή κλοπής της κάρτας: Αν η κάρτα δεν διαθέτει μηχανισμούς εύκολης και επαρκούς απόδειξης κατοχής ή/και μηχανισμούς ελέγχου πρόσβασης, τότε τα προσωπικά δεδομένα τίθενται σε άμεσο κίνδυνο, καθώς γίνεται αρκετά πιθανή μη εξουσιοδοτημένη χρήση της κάρτας από τρίτο.

8. Φυσικές επιθέσεις: Επεμβάσεις στα φυσικά μέρη της κάρτας για την παρακολούθηση της ροής των δεδομένων. Συνήθως στοχεύουν στην κλοπή ιδιωτικών κλειδιών, ώστε να έχουν πρόσβαση στα απόρρητα δεδομένα.

9. Side-Channel επιθέσεις: Χρησιμοποιούν πληροφορίες της κάρτας που μέσω των side channels, ώστε να αποκτήσουν πρόσβαση στα δεδομένα που περιέχονται στην κάρτα. Αυτές οι πρόσθετες πληροφορίες θα μπορούσε να είναι κατανάλωση ενέργειας,

ακτινοβολία, χρονισμός σημάτων και αποκρίσεων της κάρτας κ.α.. Για την πραγματοποίηση τέτοιων επιθέσεων χρησιμοποιούνται μέθοδοι που μπορούν να παρακάμπτουν τους υλοποιημένους κρυπτογραφικούς μηχανισμούς ασφάλειας, χωρίς να αφήνουν ίχνη και χωρίς να απαιτούν ακριβό εξοπλισμό, όπως η Διαφορική Ανάλυση Ισχύος (Differential Power Analysis), που πραγματοποιεί επαναλαμβανόμενη στατιστική ανάλυση πολλαπλών μετρήσεων κατανάλωσης ισχύος έως ότου εξάγει το συνολικό κλειδί και η Simple Power Analysis.

10. Κρυπτογραφικές επιθέσεις: Στις περιπτώσεις αυτές έχουμε απευθείας επίθεση στους κρυπτογραφικούς αλγορίθμους, με στόχο την εμπιστευτικότητα των μεταδιδόμενων πληροφοριών (π.χ. μεταξύ κάρτας και αναγνώστη).

11. Επιθέσεις skimming: Ο εισβολέας ανοίγει μια μη εξουσιοδοτημένη σύνδεση με την κάρτα και επιτυγχάνει πρόσβαση στα δεδομένα. Η απειλή αυτή είναι υπαρκτή μόνο στις περιπτώσεις ανεπαφικών καρτών, αν και η μέγιστη απόσταση από την οποία η κάρτα μπορεί να διαβαστεί γενικά είναι σχετικά μικρή (για τις συμβατές με ISO14443 κάρτες είναι περίπου στα 25cm). Πειράματα πάντως έχουν δείξει πως υπάρχουν τεχνικές (π.χ. ειδικοί ενισχυτές κεραιών) που μπορούν να αυξήσουν σημαντικά αυτήν την απόσταση από τα λίγα εκατοστά, σε μερικές δεκάδες μέτρα, εκπέμποντας με μεγαλύτερη ισχύ [61].

12. Ιχνηλασιμότητα διαδρομής: Ο εισβολέας δημιουργεί προφίλ για τον κάτοχο της κάρτας και για τις κινήσεις που αυτός πραγματοποιεί, παρακολουθώντας την επικοινωνία της κάρτας του χρήστη με τους αναγνώστες που χρησιμοποιεί. Αυτή η απειλή δεν είναι πάντα εκτός νομίμων ορίων. Υπάρχουν περιπτώσεις που η δημιουργία προφίλ γίνεται με αποδεκτό τρόπο και μπορεί να αποτελέσει ιδιαίτερα χρήσιμο εργαλείο (π.χ. εισαγωγή των χρήση smart cards για πληρωμή εισιτηρίου σε μέσα μαζικής μεταφοράς). Σε αυτήν την κατεύθυνση, καθοριστικό ρόλο για τη διασφάλιση της ιδιωτικότητας έχει η χρήση(αποκλειστική χρήση ανά πάροχο υπηρεσίας/υπηρεσία, συνδεσιμότητα με άλλα αναγνωριστικά ή/και δεδομένα) και ο σχεδιασμός (χρήση σημασιολογίας, τεχνική και ρυθμιστική προστασία) των μοναδικών αναγνωριστικών για πρόσβαση στις υπηρεσίες. Ειδικότερα, για να γίνει αντιληπτή η προηγούμενη αναφορά, αν για το σχεδιασμό τους έχει χρησιμοποιηθεί σημασιολογία (semantics), τότε με τη γνωστοποίηση του αναγνωριστικού, εύκολα αποκαλύπτονται άλλα προσωπικά δεδομένα του πολίτη που σχετίζονται λογικά με το αναγνωριστικό.

13. Δημιουργία προφίλ συμπεριφοράς: Σε συνέχεια της προηγούμενης, είναι πολύ συχνή απειλή και μάλιστα αποτελεί πηγή πλουτισμού για όσους ασχολούνται με το profiling. Η ιδέα είναι ότι δημιουργείται το προφίλ του χρήστη, χωρίς τη συγκατάθεσή του, βασισμένο στις συνήθειές του, τις επιλογές, τις συναλλαγές που πραγματοποιεί, τις καταναλωτικές του συνήθειες, τα μέρη που επισκέπτεται κλπ.

14. Υπογεγραμμένα ψηφιακά πιστοποιητικά: Μπορεί να συμβεί όταν στην κάρτα είναι αποθηκευμένο δημόσιο ψηφιακό πιστοποιητικό, το οποίο περιέχει προσωπικά δεδομένα του χρήστη και επιπλέον είναι υπογεγραμμένο από τον εκδότη της κάρτας. Το ερώτημα εδώ είναι αν ο πάροχος των υπηρεσιών έχει τη δυνατότητα πρόσβασης σε περισσότερη πληροφορία από αυτή που του επιτρέπεται να έχει. Στη περίπτωση που μια συναλλαγή

απαιτεί απλώς κάποια δεδομένα χωρίς να απαιτεί να είναι και ψηφιακά υπογεγραμμένα, η προσκόμιση ψηφιακά υπογεγραμμένου πιστοποιητικού αποτελεί δυνητική παραβίαση ιδιωτικότητας, καθώς τα δεδομένα παρουσιάζονται με υψηλότερο επίπεδο ασφάλειας από αυτό που απαιτείται για την πράξη της συναλλαγής. Ένα περιττό επίπεδο διασφάλισης έναντι απειλών και παραβιάσεων, εκεί που πραγματικά δεν χρειάζεται, μπορεί να οδηγήσει σε αυξημένη πρόσβαση στον πάροχο μια υπηρεσίας κατά τη συναλλαγή με αυτόν και κατά συνέπεια σε κίνδυνο κατάχρησης των δεδομένων και μελλοντικής χρήσης τους με τρίτη οντότητα, χωρίς την εξουσιοδότηση του κατόχου.

5.2.2. Αντιμετώπιση των απειλών στην ΚΠ

Τα παραδείγματα των ευρωπαϊκών eID, που έχουν ήδη υλοποιηθεί υιοθετούν διαφορετικά χαρακτηριστικά για την προστασία της ιδιωτικότητας. Σε αυτό το σημείο επιχειρείται μια χαρτογράφηση των μέτρων που χρησιμοποιούνται για την αντιμετώπιση των απειλών που αναφέρθηκαν στην προηγούμενη ενότητα και σκοπεύουν στη διασφάλιση της προστασίας κατά τη χρήση της ΚΠ.

Παρακάτω περιγράφονται σε γενικές γραμμές, οι τεχνικές για την αντιμετώπιση των προαναφερθέντων κινδύνων:

1. Κρυπτογραφημένα σύνολα δεδομένων: Τα στοιχεία της κάρτας είναι κρυπτογραφημένα με ένα ιδιωτικό κλειδί. Κάθε αναγνώστης μπορεί να διαβάσει τη γραμμή των δεδομένων, αλλά απαιτείται το ιδιωτικό κλειδί για την πρόσβαση στην πληροφορία που περιλαμβάνεται. Εκτός από τον έλεγχο πρόσβασης στην πληροφορία, ο οποίος μάλλον εξασφαλίζεται προηγούμενα με άλλες μεθόδους, το πρόσθετο χαρακτηριστικό ασφάλειας που προσδίδεται μέσω αυτής της τεχνικής είναι η δυνατότητα η πληροφορία να διατηρήσει τον εμπιστευτικό χαρακτήρα όταν διαβιβάζεται στα τρίτα μέρη εφόσον τα ιδιωτικά κλειδιά δεν έχουν μεταδοθεί. Αυτή η τεχνική δεν φαίνεται να χρησιμοποιείται σε καμιά περίπτωση εφαρμογής eID κάρτας από τα κράτη μέλη της ΕΕ.

2. Μηχανισμοί ελέγχου πρόσβασης: Η κάρτα φέρει τα δεδομένα ως απλό κείμενο και έπειτα από την επιτυχημένη αυθεντικοποίηση του χρήστη, ο Πάροχος υπηρεσιών μπορεί να έχει πρόσβαση σε αυτά. Συνήθως, χρησιμοποιούνται μηχανισμοί ελέγχου πρόσβασης PIN ή ιδιωτικών κλειδιών. Αμοιβαία αυθεντικοποίηση έχουμε όταν πραγματοποιείται ταυτόχρονα η αυθεντικοποίηση της κάρτας σε μια υπηρεσία και η αυθεντικοποίηση του αναγνώστη στην κάρτα ή στον κάτοχό της.

3. Χρήση μοναδικών αναγνωριστικών (UIDs): Τα μοναδικά αναγνωριστικά είναι αλφαριθμητικά/κωδικοί που επιτρέπουν στις εφαρμογές τη διάκριση μεταξύ των πολιτών και τη μοναδική ταυτοποίησή τους. Τα μοναδικά αναγνωριστικά, αν χρησιμοποιηθούν σωστά, μπορούν να βοηθήσουν σημαντικά και στην προστασία των δεδομένων, εκτός από την ευκολία χρήσης που προσφέρουν, καθώς δεν απαιτούν τη χρήση άλλων δεδομένων για την πραγματοποίηση μιας συναλλαγής. Ωστόσο, πρέπει να αποφεύγεται η συσχέτισή τους άλλες συναλλαγές ή δεδομένα, όπου δεν απαιτείται, προκειμένου να αποφευχθούν προφανείς κίνδυνοι για την ιδιωτικότητα. Μοναδικό αναγνωριστικό για μια κάρτα μπορεί

να είναι οποιοδήποτε στατικό δεδομένο της κάρτας, όπως για παράδειγμα, ένα δημόσιο κλειδί, αρκεί να πληροί την προϋπόθεση να είναι μοναδικό.

4. Χρήση τομεακών μοναδικών αναγνωριστικών (Domain/sector-specific UID or sector-specific personal identifiers): Η χρήση διαφορετικών αναγνωριστικών ανάλογα με την υπηρεσία για την οποία χρησιμοποιούνται (π.χ. ΑΦΜ για τη ΓΓΠΣ, ΑΔΤ για την αστυνομία κλπ) και τα πεδία εφαρμογής μπορεί να αποτρέψει/αποφύγει τη δημιουργία βάσεων δεδομένων με σχετιζόμενα δεδομένα. Σε συγκεκριμένους τομείς αναγνωριστικά μπορούν να προέρχονται από (μυστικά) αναγνωριστικά που παράγονται και διαχειρίζονται από έναν αξιόπιστο κεντρικό εκδότη (π.χ. ΓΓΠΣ, ΕΛΑΣ, ΗΔΙΚΑ).

5. Επιλεκτικής γνωστοποίησης: Μια κοινώς αποδεκτή και σημαντική αρχή της προστασίας της ιδιωτικής ζωής είναι ότι πρέπει να γνωστοποιείται το ελάχιστο απαιτούμενο σύνολο δεδομένων και ακριβώς για τους προδιαγεγραμμένους σκοπούς (Οδηγία για την προστασία προσωπικών δεδομένων, άρθρο 7 [44]). Αν απαιτείται, για παράδειγμα, μόνο το ονοματεπώνυμο του κατόχου για την ολοκλήρωση μιας συναλλαγής, τότε η κάρτα δεν πρέπει να παρέχει πρόσβαση σε άλλα στοιχεία, όπως τα στοιχεία επικοινωνίας του κατόχου.

6. Λειτουργία ύστερα από επιβεβαίωση: Αποτελεί μια απλή περίπτωση της επιλεκτικής γνωστοποίησης. Στην περίπτωση αυτή, προκειμένου να γίνει η αποκάλυψη της πραγματικής τιμής ενός πεδίου πρέπει πρώτα να απαντηθεί μια ερώτηση τύπου ναι/όχι και να ικανοποιηθεί το ερώτημα. Μια πλήρης υλοποίηση θα απαιτούσε την εφαρμογή μιας μηχανής ερωτημάτων εντός της κάρτας, μέσω της οποίας θα εκτελείτο μια σειρά ερωτημάτων πριν από κάθε συναλλαγή, ώστε να αποφεύγεται η συγκέντρωση στοιχείων. Ωστόσο, στην πραγματικότητα, οι περιπτώσεις όπου το ερώτημα δεν μπορεί να συνδυαστεί με ακρίβεια με κάποια από τα υπάρχοντα πεδία δεν είναι σχετικά πιθανές για τις περισσότερες εφαρμογές καρτών eID. Παρόλα αυτά, είναι ιδιαίτερα σημαντική η χρήση της μεθόδου αυτής για την επιστροφή μόνο των επιλεγμένων-επιθυμητών πεδίων κατά τη διάρκεια μιας συναλλαγής (π.χ. επιστροφή της τιμής «ενήλικας» ή η τοποθέτηση της ηλικίας του συναλλασσόμενου εντός ενός εύρους τιμών για την πραγματοποίηση μιας συναλλαγής).

7. Βιομετρικά πρότυπα: Ένα βιομετρικό πρότυπο είναι ένα σύνολο δεδομένων που προέρχονται από βιομετρική πληροφορία (π.χ. μια ψηφιακή εικόνα του δακτυλικού αποτυπώματος), μέσω του οποίου καθίσταται δυνατή η σύγκριση με «ζωντανά» βιομετρικά δεδομένα (σύγκριση της ψηφιακής εικόνας του δακτυλικού αποτυπώματος με το δακτυλικό αποτύπωμα). Η χρήση βιομετρικών προτύπων θα μπορούσε, υπό προϋποθέσεις να θεωρηθεί ότι κινείται στην κατεύθυνση της προστασίας της ιδιωτικής ζωής, καθώς τα βιομετρικά δεδομένα δεν αποθηκεύονται ως πληροφορίες στην κάρτα κι έτσι περιορίζεται η πληροφορία που είναι αποθηκευμένη στην κάρτα του πολίτη, αλλά και διασφαλίζεται ότι πράγματι ο πολίτης πραγματοποιεί και συναινεί για τη συναλλαγή.

8. Ασφαλής επικοινωνία μεταξύ της κάρτας, το middleware και τον εξυπηρετητή: Τα στοιχεία της κάρτας είναι ευάλωτα σε υποκλοπή και αντιγραφή από την πρώτη επικοινωνία με τον εξυπηρετητή και γνωστοποίησή τους. Για το λόγο αυτό, απαιτείται η

κρυπτογράφηση των δεδομένων που αποθηκεύονται στην κάρτα για την επικοινωνία μεταξύ των τριών αυτών οντοτήτων(κάρτα, middleware, server).

5.3. Τεχνικές ενίσχυσης της ιδιωτικότητας

Ορισμένες σημαντικές τεχνικές ενίσχυσης της ιδιωτικότητας (Privacy Enhancing Technology, PET) έχουν ήδη χρησιμοποιηθεί σε πολλές χώρες σε συστήματα ηλεκτρονικής ταυτοποίησης, Από τη μελέτη της σχετικής βιβλιογραφίας και την ανάλυση της διεθνούς-ευρωπαϊκής πρακτικής στο θέμα της διασφάλισης της ιδιωτικότητας στα συστήματα διαχείρισης ηλεκτρονικών ταυτοτήτων καταλήγουμε στις πιο κρίσιμες και χρήσιμες τεχνικές για περαιτέρω μελέτη και επεξεργασία και δυνητικά για εφαρμογή τους στην περίπτωση της εφαρμογής της ΚΠ στην Ελλάδα.

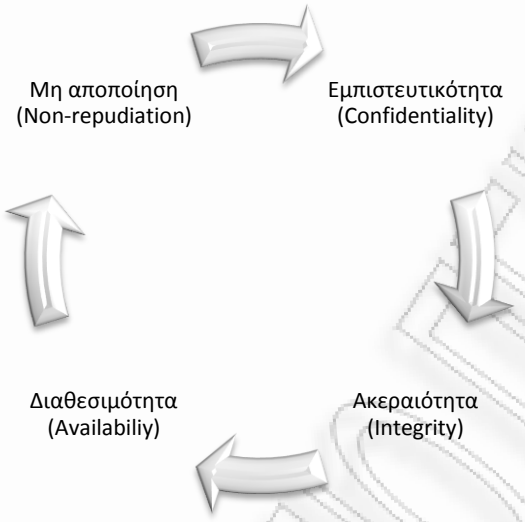
1. BAC (Basic Access Control): Χρησιμοποιείται κυρίως για την αποφυγή του skimming και, σε μικρότερο βαθμό, των πιθανών υποκλοπών, όπως ορίζεται στις προδιαγραφές του ICAO [65] για τα ηλεκτρονικά ταξιδιωτικά έγγραφα (machine-readable travel documents).
2. EAC ((European) Extended Access Control): Έρχεται να αντιμετωπίσει μικρές αδυναμίες της BAC και να αποτρέψει την μη εξουσιοδοτημένη πρόσβαση στην πληροφορία των δακτυλικών αποτυπωμάτων που είναι αποθηκευμένη στα ευρωπαϊκά διαβατήρια, όπως εντοπίστηκαν από τη Γερμανική υπηρεσία για την ασφάλεια των πληροφοριών (German Federal Office for Information Security). Ο μηχανισμός αυτό προτείνεται να ενταχθεί (Modular EAC) στο ευρωπαϊκό πρότυπο για την ΚΠ [63] [64].
3. PACE: Η PACE, όπως και άλλα παρόμοια πρωτόκολλα, μερικά εκ των οποίων έχουν υιοθετηθεί από το ευρωπαϊκό πρότυπο για την ΚΠ (ECC), αναπτύχθηκε για τη γερμανική eID κάρτα. Αντικαθιστά την BAC και συμπληρώνει την EAC, ώστε να καταστήσει δυνατή την αυθεντικοποίηση σε απομακρυσμένους διακομιστές μέσω του διαδικτύου.

Τυχαία παραγόμενα μοναδικά αναγνωριστικά (Random UIDs): Χρησιμοποιούνται για την εγκατάσταση ανεπαφικών καναλιών επικοινωνίας [65] [87] [88]. Τα τομεακά αναγνωριστικά περιλαμβάνονται ήδη στις προδιαγραφές της Αυστριακής και Γερμανικής ΚΠ.

5.3.1. Κρυπτογραφία

Στις κύριες επιθέσεις που εμφανίζονται στις υπηρεσίες διαδικτύου η απάντηση έρχεται μέσω της κρυπτογραφίας, η οποία αντιμετωπίζει θέματα υποκλοπών (Eavesdropping), δηλαδή θέματα εμπιστευτικότητας της πληροφορίας που μεταφέρεται μέσα σε ένα κανάλι

επικοινωνίας, των ψηφιακών υπογραφών, που εξαλείφουν περιπτώσεις παραποίησης (Tampering) της μεταφερόμενης πληροφορίας και των ψηφιακών πιστοποιητικών που αντιμετωπίζουν περιπτώσεις προσποίησης (spoofing) και πλαστοπροσωπίας (impersonation).



Εικόνα 25-Απαιτήσεις Ασφάλειας

Προκειμένου να θωρακίσουμε τα δεδομένα που διακινούνται μέσω των συναλλαγών και να εξασφαλίσουμε την ασφάλεια των συναλλασσομένων πρέπει να εδραιώσουμε προϋποθέσεις ασφάλειας. Αυτή η παραδοχή μας οδηγεί στην προστασίας της:

- εμπιστευτικότητας, ότι, δηλαδή, η πληροφορία που μεταδίδεται πρέπει να είναι προσβάσιμη μόνο από τα εξουσιοδοτημένα μέλη (data confidentiality). Η πληροφορία πρέπει να μη μπορεί να γίνει κατανοητή από οποιοδήποτε τρίτο.
- ακεραιότητας, ότι, δηλαδή, η πληροφορία μεταφέρεται ακέραια, χωρίς λάθη ή τροποποιήσεις (data integrity). Πρέπει να είναι σε θέση ο παραλήπτης να ελέγχει αν το μήνυμα δεν έχει τροποποιηθεί κατά τη μεταφορά, ώστε να μην μπορεί κάποιος τρίτος να αντικαταστήσει το μήνυμα με ένα ψεύτικο το οποίο να φαίνεται αληθινό.
- διαθεσιμότητας (availability), ότι η πληροφορία είναι συνεχώς διαθέσιμη
- μη αποποίησης (non-repudiation), ότι ένας χρήστης δεν μπορεί να αρνηθεί τη συμμετοχή του σε μια συναλλαγή που έκανε,

αλλά και να υλοποιήσουμε μηχανισμούς για την

- ταυτοποίηση και αυθεντικοποίηση (identification and authentication), τον έλεγχο δηλαδή της γνησιότητας της ταυτότητας του συναλλασσόμενου. Πρέπει να είναι σε θέση ο δέκτης να εξακριβώνει αν το μήνυμα ανήκει πράγματι στον αποστολέα ή ότι ο αποστολέας είναι αυτός που ισχυρίζεται ότι είναι.
- έλεγχο πρόσβασης, δηλαδή τον έλεγχο προσπέλασης και τις αναγκαίες εξουσιοδοτήσεις (access control and authorizations).

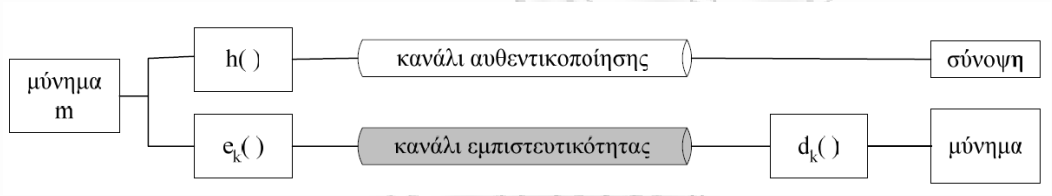
Αυτές οι έννοιες είναι ζωτικής σημασίας για την κοινωνική αλληλεπίδραση με την χρήση υπολογιστών, και είναι ανάλογες με τις διαπροσωπικές αλληλεπιδράσεις.

Σε αυτήν την κατεύθυνση τα σημαντικότερα εργαλεία, δηλαδή οι μέθοδοι και τεχνικές προστασίας είναι η κρυπτογράφηση, είτε για την αυθεντικοποίηση των χρηστών, είτε για την μεταφορά δεδομένων, οι μηχανισμοί ελέγχου πρόσβασης (Συνθηματικά και Ψηφιακές υπογραφές) και τα ασφαλή δικτυακά πρωτόκολλα.

5.3.1.1. Αυθεντικοποίηση και Εμπιστευτικότητα (με χρήση Hash και MAC)

Με την χρήση hash συναρτήσεων και MAC κωδικών επιτυγχάνεται αυθεντικοποίηση και εμπιστευτικότητα των μηνυμάτων.

Στην πράξη για να πετύχουμε αυθεντικοποίηση και εμπιστευτικότητα χρειαζόμαστε μια κρυπτογραφική μονόδρομη hash, ώστε να δημιουργήσουμε ένα κανάλι αυθεντικοποίησης και έναν κρυπταλγόριθμο, που δημιουργεί ένα κανάλι εμπιστευτικότητας μεταξύ των δύο μερών, όπως φαίνεται στο παρακάτω σχήμα. [101]



Εικόνα 26- Αυθεντικοποίηση και εμπιστευτικότητα

Ανάλογα με σειρά της εφαρμογής των δύο αυτών στοιχείων στο μήνυμα, έχουμε τις ακόλουθες περιπτώσεις:

- *Αυθεντικοποίηση απλού κειμένου ή εσωτερικός έλεγχος σφαλμάτων*: Η αυθεντικοποίηση πραγματοποιείται στο απλό κείμενο. Για να γίνει ο έλεγχος αυθεντικοποίησης πρέπει να αποκρυπτογραφηθεί η σύνοψη και το απλό κείμενο. Το κανάλι εμπιστευτικότητας περικλείει το κανάλι αυθεντικοποίησης.
- *Αυθεντικοποίηση κρυπτοκειμένου*: Η εμπιστευτικότητα προσφέρεται μόνο στο μήνυμα και όχι και στη σύνοψή του, εφόσον παράγεται η σύνοψη του κρυπτοκειμένου. Ο έλεγχος αυθεντικοποίησης πραγματοποιείται στο λαμβανόμενο κρυπτοκείμενο. Το κανάλι εμπιστευτικότητας περικλείεται στο κανάλι αυθεντικοποίησης.

Στην περίπτωση των μονόδρομων hash συναρτήσεων, σε ένα μήνυμα του οποίου η αυθεντικοποίηση προστατεύεται με μια συνάρτηση MAC, ακόμη κι αν ο επιτιθέμενος γνωρίζει το απλό κείμενο και την αντίστοιχη σύνοψη, πρέπει επιπλέον να ανακαλύψει το κλειδί της MAC. Επομένως, η ασφάλεια της αυθεντικοποίησης εξαρτάται από το μήκος του κλειδιού. Δεδομένου ότι, η μόνη επίθεση στο MAC είναι η εξαντλητική αναζήτηση στο κλειδί, τότε αποδεικνύεται [εισαγωγή παραπομπής] ότι η προσπάθεια που απαιτείται από

κάποιον προκειμένου να ανακαλύψει το κλειδί είναι ίση ή μεγαλύτερη με την προσπάθεια που θα έκανε για να ανακαλύψει το ίδιο (σε μέγεθος) κλειδί, σε ένα κρυπτοσύστημα.

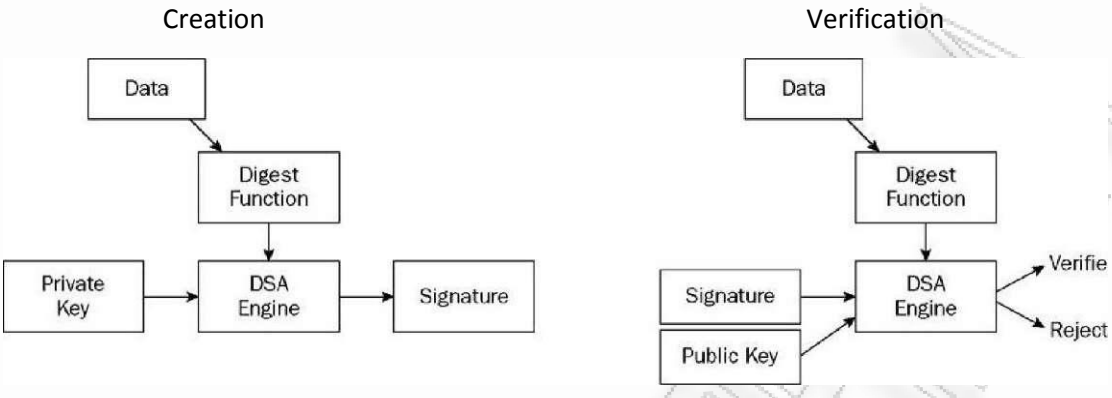
5.3.2. Ψηφιακές Υπογραφές

Ως ψηφιακή υπογραφή ορίζεται η κρυπτογράφηση δεδομένων με το ιδιωτικό κλειδί ενός χρήστη. Η διαδικασία η οποία ορίζεται από τη δημιουργία σύνοψης ενός μηνύματος και την κρυπτογράφηση αυτής με το ιδιωτικό κλειδί του αποστολέα, αποτελεί την ψηφιακή υπογραφή του μηνύματος. [101] Αυτό έχει ως αποτέλεσμα τα δεδομένα αυτά να είναι ταυτοποιημένα, γιατί ο μόνος τρόπος για να τα διαβάσει κανείς είναι αποκρυπτογραφώντας τα, με το δημόσιο κλειδί του χρήστη. Η αποκρυπτογράφηση με οποιοδήποτε άλλο κλειδί δεν θα αποκαλύψει τα αρχικά δεδομένα, αλλά θα έχει ως αποτέλεσμα θόρυβο. Με αυτή λοιπόν τη διαδικασία έχουμε και αυθεντικοποίηση του μηνύματος και non-repudiation.

Στην πράξη η ψηφιακή υπογραφή εφαρμόζεται στη σύνοψη, αφενός για την αποφυγή της επίθεσης «αποκοπής και επικόλλησης» (cut-and-paste attack) που μπορεί να πραγματοποιηθεί σε πολλά ασύμμετρα κρυπτοσυστήματα [101] και αφετέρου για λόγους οικονομίας χρόνου και πόρων.

Αν θεωρήσουμε ότι ο ασύμμετρος κρυπταλγόριθμος εφαρμόζεται χωριστά σε τμήματα του μηνύματος, τότε ο αποστολέας πρέπει να υπογράψει ψηφιακά ένα μήνυμα τόσες φορές, όσα είναι και τα τμήματα του μηνύματος. Το φυσικό ανάλογο είναι οι υπογραφές που μπαίνουν διαδοχικά στις σελίδες ενός συμβολαίου. Ωστόσο, η αδυναμία της πρακτικής αυτής είναι εντονότερη στον ψηφιακό κόσμο. Αν και θεωρητικά θα μπορούσε ο παραλήπτης μπορεί να συνθέσει το αρχικό μήνυμα, συνθέτοντας τα επιμέρους τμήματά του, στην περίπτωση των ηλεκτρονικών μηνυμάτων τα τμήματα είναι πολύ μικρότερα. Για το λόγο αυτό, η πρακτική υπογραφής της σύνοψης, δηλαδή της τιμής hash ενός μηνύματος, είναι η πλέον ενδεδειγμένη και αποδοτική λύση. Στη συνέχεια, το μήνυμα και η ψηφιακή υπογραφή αποστέλλονται στον παραλήπτη.

Από πλευράς απαιτήσεων ασφάλειας, η κρυπτογραφική μονόδρομη hash συνάρτηση που θα χρησιμοποιηθεί για την παραγωγή της , προς υπογραφή, σύνοψης πρέπει να έχει ασθενή ανθεκτικότητα σε συγκρούσεις, εφόσον απαιτείται να είναι υπολογιστικά αδύνατο για τον παραλήπτη ενός μηνύματος να μπορεί να παράγει αντίγραφο, το οποίο να αντιστοιχίζεται στη σύνοψη του αρχικού ψηφιακά υπογεγραμμένου μηνύματος. Επιπλέον, σε άλλη περίπτωση η μη αποποίηση της ευθύνης από τον αποστολέα θα ήταν αρκετά δύσκολη, αν χρησιμοποιείτο συνάρτηση hash δίχως προστασία από συγκρούσεις. Έτσι, ο υπογράφων, θα μπορούσε να βρει ένα διαφορετικό από το αυθεντικό υπογεγραμμένο μήνυμα, για το οποίο η τιμή σύνοψης να συμπίπτει με την τιμή του αρχικού μηνύματος (hash(M)=hash(M'), για M αυθεντικό και M' άλλο μήνυμα) και να ισχυριστεί ότι υπέγραψε ένα άλλο μήνυμα, αντί του πραγματικού.



Εικόνα 27-Δημιουργία και Επιβεβαίωση Ψηφιακής Υπογραφής

Η ψηφιακή υπογραφή πρέπει να εφαρμόζεται στη σύνοψη του απλού κειμένου, δεδομένου ότι πρέπει ο υπογράφων, αφενός, να έχει ακριβή γνώση του αρχείου που υπογράφει και αφετέρου, πρέπει να υπογράφει το «πρωτότυπο» αρχείο, το οποίο ισοδυναμεί με τη σύνοψη του απλό κειμένου, καθότι ένα κρυπτοκείμενο μπορεί να αντιστοιχεί τόσες φορές σε ένα απλό μήνυμα, όσα είναι και τα κλειδιά («ψηφιακό καρμπόν»).

Η Ψηφιακή Υπογραφή συνοδεύει ένα αρχείο και αποτελείται από δεδομένα συνημμένα ή συσχετισμένα με ένα ηλεκτρονικό αρχείο, τα οποία χρησιμεύουν στην επαλήθευση της αυθεντικότητας του.

Με τον τρόπο αυτό, μια ψηφιακή υπογραφή, επικυρώνει το κείμενο που υπογράφει και επαληθεύει την προέλευση του και αποτελεί αποδεικτικό στοιχείο για τον παραλήπτη.

Η ψηφιακή υπογραφή είναι μονοσήμαντα συνδεδεμένη με τον υπογράφοντα, παρέχει δυνατότητα αναγνώρισής του και δημιουργείται με μέσα που βρίσκονται υπό τον αποκλειστικό του έλεγχο. Για την ψηφιακή υπογραφή ισχύει, επίσης, ότι είναι μονοσήμαντα συνδεδεμένη με το κείμενο που συνοδεύει, με τρόπο τέτοιο που να εξασφαλίζεται η ακεραιότητά του. Επιπλέον, διασφαλίζεται ότι η ίδια υπογραφή δεν μπορεί να δημιουργηθεί από άλλη οντότητα ή/και να μεταφερθεί σε άλλο κείμενο. Τέλος, με τη χρήση των ψηφιακών υπογραφών, ικανοποιείται η απαίτηση για μη αποποίηση, καθώς ο υπογράφων δε δύναται να αρνηθεί ότι δημιούργησε μια υπογραφή.

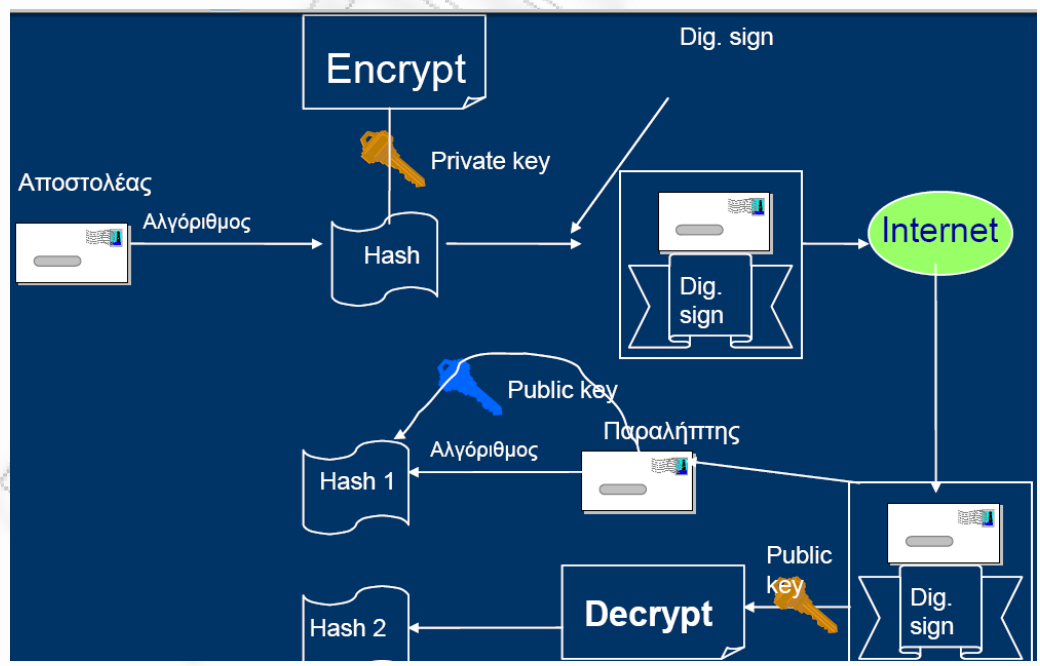
Ένα έγκυρο ψηφιακά υπογεγραμμένο έγγραφο αποτελείται από τα εξής στοιχεία [101]:

- Το κύριο έγγραφο, το οποίο μπορεί να είναι οποιασδήποτε γνωστής ηλεκτρονικής μορφής (.doc, .xl, .pdf, .jpeg, .tif, .bmp κλπ).
- Την συνημμένη ψηφιακή υπογραφή του, δηλαδή την κρυπτογράφηση, με το ιδιωτικό κλειδί του υπογράφοντα, μιας σύνοψης του κύριου εγγράφου που παράγεται από ειδικό αλγόριθμο κατακερματισμού (hashing).

- Τη χρονοσήμανση της υπογραφής, που αποδίδεται αξιόπιστα από τρίτο πάροχο υπηρεσιών χρονοσήμανσης που κρυπτογραφεί με το ιδιωτικό του κλειδί τον συνδυασμό της ψηφιακής υπογραφή και της ακριβής ώρας (timestamp).
- Το πιστοποιητικό του δημοσίου κλειδιού του υπογράφοντα ή άλλα πιστοποιητικά.

Η διαδικασία υπογραφής ενός μηνύματος συνοπτικά μπορεί να περιγραφεί μέσα από τα ακόλουθα βήματα:

1. Ο αποστολέας παράγει μια σειρά χαρακτήρων σταθερού μήκους (message digest), που προκύπτει από την εφαρμογή συνάρτησης hash στο αρχικό μήνυμα. Το message digest είναι ένα ψηφιακό αποτύπωμα ενός μηνύματος (πρόκειται ουσιαστικά για μια συνάρτηση hash) και χρησιμοποιείται για την πιστοποίηση της ακεραιότητας ενός μηνύματος μέσω της ψηφιακής υπογραφής.
2. Η message digest κρυπτογραφείται με το ιδιωτικό κλειδί του αποστολέα και παράγει την ψηφιακή υπογραφή του αρχείου.
3. Η ψηφιακή υπογραφή επισυνάπτεται στο μήνυμα και αποστέλλεται στον παραλήπτη.
4. Ο παραλήπτης με χρήση hash συνάρτησης παράγει ένα άλλο message digest.
5. Έπειτα, χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα αποκρυπτογραφεί την ψηφιακή υπογραφή και παράγει το αρχικό message digest.
6. Αν τα δύο message digest που προέκυψαν, τότε συμπεραίνουμε ότι το μήνυμα είναι ακέραιο και δεν έχει αλλοιωθεί.



Εικόνα 28-Χρήση Ψηφιακής Υπογραφής

Για τη λειτουργία της ψηφιακής υπογραφής προϋποθέτουμε την ασφάλεια του χρησιμοποιούμενου αλγορίθμου κρυπτογράφησης και την ασφάλεια των συναρτήσεων

σύνοψης. Επιπλέον, για την χρήση των ψηφιακών υπογραφών βασιζόμαστε στην αντιστοίχηση δημόσιων κλειδιών στις οντότητες που συμμετέχουν στο σχήμα της ψηφιακής υπογραφής. Παρόλα αυτά, δεν έχουμε απαντήσει στο πρόβλημα δήλωσης του δημόσιου κλειδιού από άλλη οντότητα, πέραν του αυθεντικού κατόχου. Με τον τρόπο αυτό, κάποιος μπορεί να υπογράψει με το ιδιωτικό του κλειδί ένα έγγραφο, να δηλώσει ως δικό του δημόσιο κλειδί το κλειδί κάποιου άλλου (θύμα απάτης) και έτσι να τον εξαπατήσει και να πραγματοποιεί συναλλαγές με τρίτους, εξαπατώντας κι εκείνους συγχρόνως. Προφανώς, το σενάριο αυτό προϋποθέτει την εμπιστοσύνη των τρίτων στη δήλωση του πρώτου. Εντούτοις, η εμπιστοσύνη στον τρόπο με τον οποίο γίνεται η αντιστοίχηση κλειδιού-ταυτότητας είναι απολύτως σημαντική για την επιτυχή και ασφαλή εφαρμογή των ψηφιακών υπογραφών. Η κρυπτογραφία δημόσιου κλειδιού λύνει το ένα μέρος του προβλήματος, εκείνο της διανομής κλειδιών αλλά όχι και το πρόβλημα της αντιστοίχησης των κλειδιών. Η μόνη πιθανή λύση που διαφαίνεται ως προς αυτή την κατεύθυνση είναι η ύπαρξη μιας Έμπιστης τρίτης οντότητας.

5.3.3. Ψηφιακά Πιστοποιητικά

Τα ψηφιακά πιστοποιητικά(digital certificates) θα λέγαμε ότι είναι ένας τρόπος διανομής και αντιστοίχησης των δημόσιων κλειδιών, καθώς είναι ηλεκτρονικά έγγραφα, με συγκεκριμένη μορφή που σχετίζουν μια οντότητα με ένα δημόσιο κλειδί. Η πιο διαδεδομένη δομή τους είναι η X.509 v3 που αποτελεί την πιο πρόσφατη έκδοση του πρότυπου X.509. Με μια άλλη απόπειρα ορισμού των ψηφιακών πιστοποιητικών θα μπορούσαμε να πούμε ότι αποτελούν μια ψηφιακά υπογεγραμμένη δομή δεδομένων, η οποία αντιστοιχίζει μία ή περισσότερες ιδιότητες μιας φυσικής οντότητας στο δημόσιο κλειδί που της ανήκει [101].

Τα ψηφιακά πιστοποιητικά έρχονται να δώσουν απάντηση στα προβλήματα διανομής των κλειδιών και της αντιστοίχησής τους με οντότητες.

Ένα ψηφιακό πιστοποιητικό περιλαμβάνει πληροφορία για τα ακόλουθα πεδία δεδομένων:

1. Αναγνωριστικά πιστοποιητικού: Τύπος - Πρότυπο, Έκδοση, Μοναδικός Σειριακός αριθμός(serial number), Αλγόριθμος υπογραφής
2. Περίοδος Ισχύος: Από – Έως
3. Πληροφορίες Εκδότη(Αρχή Έκδοσης Πιστοποιητικών -Certification Authority): Διακριτικό όνομα, Σημείο πρόσβασης, Αναγνωριστικό κλειδιού
4. Υποκείμενο: Πλήρες Διακριτικό Όνομα του κατόχου του πιστοποιητικού
5. Δημόσιο κλειδί που αντιστοιχεί στο υποκείμενο
6. Επεκτάσεις: Επιτρεπόμενες χρήσεις, Σημείο διανομής πληροφοριών κατάστασης, άλλα εξειδικευμένα ανά εφαρμογή πεδία
7. Κρίσιμες επεκτάσεις: Όπως οι προηγούμενες, αλλά χαρακτηρισμένες ως απαράβατες.
8. Υπογραφή Εκδότη σε όλη τη δομή (Αρχή Πιστοποίησης - Authority)
9. Σύνοψη πιστοποιητικού ως κλειδί αναφοράς

Το πιστοποιητικό είναι υπογεγραμμένο από μία αναγνωρισμένη έμπιστη τρίτη οντότητα που δρα ως Πάροχος Υπηρεσιών Πιστοποίησης – ΠΥΠ (Trusted Third Party –TTP & Certification Services Provider – CSP). Η Έμπιστης Τρίτης Οντότητας, ο ΠΥΠ είναι ίσως και η σημαντικότερη «προσφορά» των πιστοποιητικών αυτών στην εγκαθίδρυση σχέσεων εμπιστοσύνης στην πραγματοποίηση ψηφιακών συναλλαγών. Ενώ, η Αρχή Έκδοσης Πιστοποιητικών (Certification Authority) είναι η αρχή που χρησιμοποιείται για την έκδοση ψηφιακών πιστοποιητικών και την ψηφιακή τους υπογραφή, προκειμένου να διασφαλίσει την αυθεντικότητα του πιστοποιητικού. Επιπλέον, ιδιαίτερη αξία έχει το γεγονός ότι υπακούουν σε ιεραρχικό σχήμα και ότι περιέχουν στοιχεία, η εγκυρότητα των οποίων επιβεβαιώνεται από τρίτο εγγυητή, για χρήση σε διάφορες εφαρμογές (αυθεντικοποίηση και έλεγχος πρόσβασης). Τέλος, τα ψηφιακά πιστοποιητικά δεν προϋποθέτουν συναλλαγές πραγματικού χρόνου και μπορούν να χρησιμοποιηθούν σε δεύτερο χρόνο.

Ένα ψηφιακό πιστοποιητικό χρησιμοποιείται για να διασφαλίσει με τεχνικά και νομικά μέσα ότι ένα δημόσιο κλειδί ανήκει σε μία και μόνο μία οντότητα, η οποία αποτελεί τον νόμιμο κάτοχο του αντίστοιχου ιδιωτικού κλειδιού, μέσω της Έμπιστης Τρίτης Οντότητας (Trusted Third Party). Με τον τρόπο αυτό σημαίνει ότι βεβαιώνεται ταυτόχρονα και η ακεραιότητα του δημόσιου κλειδιού.

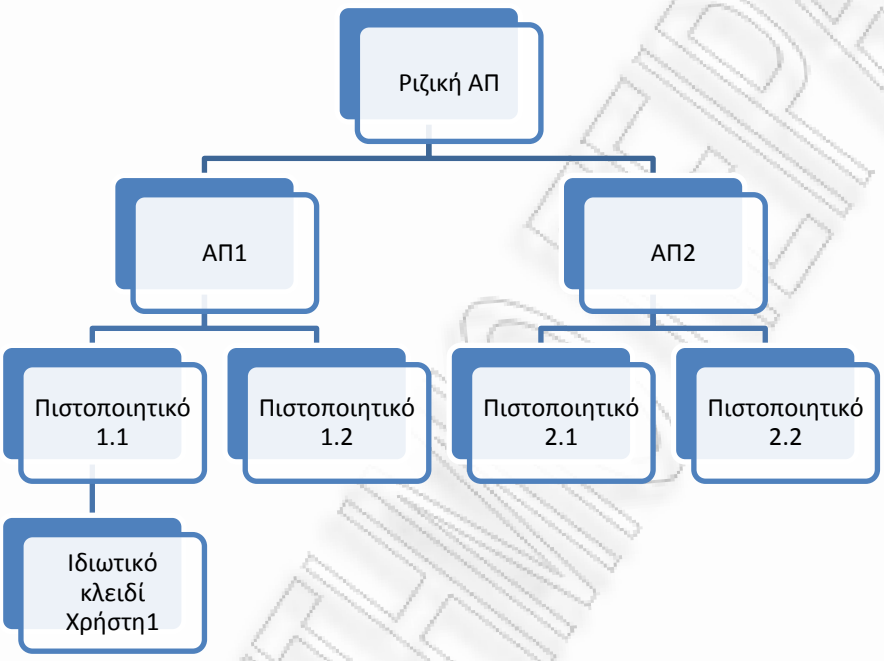
Έτσι, μέσω των αναγνωρισμένων πιστοποιητικών (Qualified Certificates – QC) είναι εφικτός ο μονοσήμαντος προσδιορισμός ταυτότητας του Παρόχου και του Υποκειμένου, ο προσδιορισμός της προσδοκώμενης χρήσης, των δεδομένων που μπορούν να χρησιμοποιηθούν για την επαλήθευση της υπογραφής (Signature Verification Data) που αντιστοιχεί στο υποκείμενο και των δεδομένων που προσδιορίζουν το ίδιο το πιστοποιητικό, όπως η περίοδος ισχύος, ο κωδικός αναγνώρισης του πιστοποιητικού. Επιπλέον, περιλαμβάνονται πιθανοί περιορισμοί στη χρήση και οι ευθύνες του Παρόχου, η ψηφιακή υπογραφή του και πιθανές επεκτάσεις του, κατά περίπτωση εφαρμογής.

Ο τρόπος χρήσης και ανταλλαγής των ψηφιακών πιστοποιητικών και η ιεραρχία πιστοποίησης ορίζεται με ακρίβεια στο πρότυπο X.509. Η διαχείρισή τους γίνεται μέσω των εξυπηρετητών πιστοποιητικών (Certificate Servers), που συνήθως ενεργούν και ως πάροχοι υπηρεσιών πιστοποίησης, παίζοντας το ρόλο της Αρχής Πιστοποίησης.

Κατηγορίες Ψηφιακών Πιστοποιητικών

1. Προσωπικό πιστοποιητικό ή Πιστοποιητικό Ταυτότητας (Personal or Identity certificate): Το υποκείμενο είναι φυσικό πρόσωπο.
2. Πιστοποιητικό Συσκευής ή Εξυπηρέτη (Server or Device certificate): Για παράδειγμα δρομολογητές ή web server.
3. Πιστοποιητικό Ρόλου (Role-based certificate): Το υποκείμενο δεν είναι φυσικό πρόσωπο και ο κάτοχος του ιδιωτικού κλειδιού μπορεί να αλλάζει.
4. Πιστοποιητικό Οργανισμού (Organisational certificate): Για παράδειγμα το Microsoft Corp για την υπογραφή λογισμικού.
5. Πιστοποιητικό Ιδιοτήτων (Attribute certificate): Αποδίδει ρόλους και δικαιώματα σε μια φυσική οντότητα, χωρίς κλειδί.

6. Ομαδικό Πιστοποιητικό (Group certificate): Ταυτοποιεί μία ομάδα και επιβεβαιώνει τη συμμετοχή οντοτήτων σε αυτή.
7. Πιστοποιητικό Αντιπροσώπου ή Προσωρινό (Proxy certificate): Παράγεται από το ίδιο το υποκείμενο με μικρή διάρκεια ισχύος (π.χ. μηχανισμοί single-sign-on)



Εικόνα 29-Ιεραρχία Ψηφιακών Πιστοποιητικών

Τα ψηφιακά πιστοποιητικά υπακούουν σε ιεραρχικό σχήμα, όπως φαίνεται παραπάνω. Στην κορυφή της ιεραρχίας βρίσκεται η Ριζική Αρχή Πιστοποίησης, τα πιστοποιητικά τα οποία εκδίδει είναι επίσης στην κορυφή της εμπιστοσύνης. Η ίδια κατέχει αυτο-υπογραφόμενο πιστοποιητικό. Στο επόμενο ιεραρχικά επίπεδο από τη Ριζική Αρχή Πιστοποίησης, βρίσκονται οι επιμέρους ενδιάμεσες Αρχές Πιστοποίησης. Οι ενδιάμεσες ΑΠ εκδίδουν πιστοποιητικά τα οποία χρησιμοποιούνται για να πιστοποιήσουν την ακεραιότητα στις συναλλαγές που συμμετέχουν. Είναι σαφές ότι εφόσον χρησιμοποιώ την ΑΠ για την έκδοση ενός πιστοποιητικού που μπορεί να χρησιμοποιηθεί για συναλλαγές με τρίτους και την εμπιστεύομαι για την πιστοποίηση της συναλλαγής μου, την εμπιστεύομαι παράλληλα, για τα πιστοποιητικά που εκδίδει σε τρίτους και άρα για την πιστοποίηση της συναλλαγής με τρίτο. Το ίδιο συμβαίνει για τις ΑΠ που βρίσκονται ιεραρχικά στο ίδιο επίπεδο. Έτσι, στο επόμενο επίπεδο βρίσκεται το κάθε πιστοποιητικό που εκδίδεται προς χρήση για συναλλαγές με τρίτα μέρη από τις ενδιάμεσες ΑΠ και στο τελευταίο επίπεδο, το προσωπικό πιστοποιητικό του χρήστη, το οποίο ουσιαστικά αποτελεί το ιδιωτικό του κλειδί, και το οποίο αφενός «κληρονομεί» τη σχέση εμπιστοσύνης και αφετέρου είναι ισοδύναμο με τα ιδιωτικά κλειδιά που προκύπτουν με αντίστοιχη διαδικασία.

Οι κυριότεροι τύποι ψηφιακών πιστοποιητικών καταγράφονται ακολούθως:

- Client SSL Certificates: Για την αναγνώριση των χρηστών σε εξυπηρετητές μέσω SSL (client authentication)
- Server SSL Certificates: Για την αναγνώριση των εξυπηρετητών μέσω SSL (server authentication)
- S/MIME Certificates: Για κρυπτογράφηση και υπογραφή του ηλεκτρονικού ταχυδρομείου
- Object-signing Certificates: Για την αναγνώριση υπογεγραμμένου κώδικα Java, Javascript κ.α.
- CA Certificates: Για την αναγνώριση των CAs
    - ✓ Root: το υποκείμενο του πιστοποιητικού, υπογράφει ψηφιακά το πιστοποιητικό. Εκδίδει Intermediate πιστοποιητικά.
    - ✓ Intermediate: μπορεί να εκδώσει κάθε τύπο πιστοποιητικού όπως και Intermediate πιστοποιητικά.

Για τη δημιουργία και χρήση ψηφιακών πιστοποιητικών ακολουθείται μια σειρά από πρότυπα, τα οποία καλούνται να προσδώσουν επιπλέον χαρακτηριστικά ασφάλειας και διαλειτουργικότητας, τόσο κατά τη δημιουργία και υλοποίηση των πιστοποιητικών, όσο και για τη χρήση τους και τις λειτουργίες που επιτελούν. Έτσι, τα σημαντικότερα πρότυπα, σύμφωνα με τους διεθνείς οργανισμούς, είναι τα εξής:

- Μορφοποίηση
    - ✓ X.509 (ITU)
    - ✓ SPKI – SDSI - PKIX (IETF)
    - ✓ PGP
    - ✓ PKCS#6 (RSA)
- Αίτηση
    - ✓ PKCS#10 (RSA)
    - ✓ RFC-2511 (IETF)
- Διανομή
    - ✓ PKCS#7 & PKCS#12 (RSA)
- Πληροφορίες κατάστασης
    - ✓ RFC-2560: OCSP (IETF)
    - ✓ TR 102-030 (ETSI)

Η έκδοση αναγνωρισμένων πιστοποιητικών γίνεται συνήθως από τις αρχές πιστοποίησης. Έτσι, ένας πάροχος υπηρεσιών πιστοποίησης αποτελεί έναν πολύ σημαντικό κρίκο στην αλυσίδα της ασφάλειας των ψηφιακών πιστοποιητικών και για το λόγο αυτό πρέπει να πληροί ένα σύνολο από ιδιαίτερα αυστηρές προϋποθέσεις και απαιτήσεις ασφαλείας. Το σημαντικό στοιχείο που εξασφαλίζεται μέσω των ψηφιακών πιστοποιητικών είναι η εμπιστοσύνη, κατά συνέπεια, η εμπιστοσύνη στον ΠΥΠ είναι τόσο επιτακτική, όσο και αυτονόητη για την επιτυχία της λύσης. Ο πάροχος, συνεπώς, πρέπει να επιδεικνύει την απαιτούμενη αξιοπιστία και να εξασφαλίζει ασφαλής μηχανισμούς για την έκδοση, δημοσίευση και ανάκληση πιστοποιητικών. Ο πάροχος πρέπει να ακολουθεί διαδικασία που διασφαλίζει την αδιαμφισβήτητη επαλήθευση της ταυτότητας της πιστοποιούμενης οντότητας. Προκειμένου, να διατηρήσει την αξιοπιστία του, οφείλει να χρησιμοποιεί

αξιόπιστα Πληροφοριακά Συστήματα και να απασχολεί κατάλληλα εκπαιδευμένο επιστημονικό προσωπικού και να διασφαλίζει την οικονομική του ικανότητα του (εξασφάλιση απαραίτητων οικονομικών, υλικών και ανθρώπινων πόρων για την ομαλή λειτουργία του) και να πληροί τις απαιτήσεις για φυσική ασφάλεια. Επιπλέον, υποχρεούται να ακολουθεί πρακτικές όπως η τήρηση ημερολογίου πράξεων (audit log), η δημοσίευση πολιτικών, πρακτικών και συνθηκών με τις οποίες συμμορφώνεται και να σέβεται τους κανόνες που αφορούν στην προστασία των δεδομένων δημιουργίας υπογραφής του ΠΥΠ (signature creation data). Ιδανικά, ο πάροχος θα πρέπει να είναι σε θέση να πραγματοποιεί και να διενεργεί ασφαλή εκτίμηση κινδύνων (Risk Analysis). Τέλος, ο ΠΥΠ μπορεί να είναι πιστοποιημένος κατά ISO 9000, ISO 9001. Το πιο σημαντικό ζήτημα που προκύπτει από τη λειτουργία του παρόχου αφορά στη διαχείριση ενός μεγάλου όγκου διασυνδεόμενων προσωπικών δεδομένων. Αυτό εγείρει σημαντικές ανησυχίες σχετικά με την ασφάλεια των προσωπικών δεδομένων και σε αυτόν τον προβληματισμό δρα ενισχυτικά και η πιθανά μακροχρόνια αποθήκευση δεδομένων για την επαλήθευση υπογραφών.

Ο κύκλος ζωής των κλειδιών είναι ιδιαίτερα σημαντικός για λόγους ασφάλειάς τους. Ο κύκλος ζωής ενός κλειδιού είναι ανάλογος με το μήκος του κλειδιού, επομένως χρειάζεται ένα αρκούντος μεγάλο κλειδί για ένα σχετικά μεγάλο κύκλο ζωής. Ωστόσο, όσο μεγαλύτερος είναι ο χρόνος ζωής ενός κλειδιού, τόσο αυξάνονται οι πιθανότητες κακού χειρισμού του. Για την ακρίβεια, όσο περισσότερο εκτίθεται ένα κλειδί, τόσο αυξάνουν οι πιθανότητες εφαρμογής μεθόδων κρυπτανάλυσης σε αυτό. Κατ' αντίστοιχα, όσο περισσότερη πληροφορία κρυπτογραφείται με ένα κλειδί τόσο αυξάνονται οι πιθανότητες κρυπτανάλυσής του. Για τους παραπάνω λόγους, είναι απαραίτητο να υπάρχει ένας μηχανισμός ανανέωσης κλειδιών και κατά συνέπεια και των σχετικών πιστοποιητικών.

Η ανάκληση των πιστοποιητικών μπορεί να γίνει για λόγους απώλειας , κλοπής, ή διαρροής του ιδιωτικού κλειδιού του χρήστη, αλλαγής στοιχείων ή ρόλου του κατόχου του πιστοποιητικού και σε περιπτώσεις αλλαγής ή παύσης λειτουργίας ενός ΠΥΠ. Για λόγους συνέχειας και συνέπειας απαιτείται η δημοσίευση των πληροφοριών κατάστασης των πιστοποιητικών (Certificate Status Information – CSI), η οποία πραγματοποιείται μέσω της κατάρτισης της Λίστας Ανάκλησης Πιστοποιητικών (CLS), του πρωτοκόλλου OCSP (Online Certification Status Protocol , RFC-2560), του μηχανισμού delta-CRL: περιοδική καταχώρηση ανακληθέντων πιστοποιητικών και της πρόσβασης σε online βάσεις δεδομένων με http, ftp ή ldap URLs.

5.3.4. Συστήματα Δημόσιου Κλειδιού (PKI)

Στο επίκεντρο των τεχνολογιών που υποστηρίζουν τα συστήματα διαχείρισης ταυτότητας βρίσκονται οι ψηφιακές υπογραφές που υποστηρίζονται από την υποδομή δημοσίου κλειδιού. Η υποδομή δημοσίου κλειδιού αποτελεί διεθνώς τη βασική τεχνολογική λύση.

Τα ζητήματα που προκύπτουν από τη χρήση συστημάτων PKI στις υποδομές διαχείρισης ηλεκτρονικής ταυτοποίησης αντιμετωπίζονται από δύο πλευρές.

- Τεχνολογική σκοπιά: Βασικό ζητούμενο αποτελεί η αποτελεσματική και έγκυρη διαχείριση των πληροφοριών που αποτελούν την πληροφοριακή ταυτότητα του ατόμου.
- Κοινωνική σκοπιά: Ανησυχία εξαιτίας των μοναδικών φορέων ταυτοποίησης που χρησιμοποιούνται προκειμένου να ταυτοποιηθούν έγκυρα οι χρήστες.

Η Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure - PKI) ενσωματώνει ψηφιακά πιστοποιητικά, κρυπτογραφία δημόσιου κλειδιού και αρχές πιστοποίησης σε ένα ασφαλές αρχιτεκτονικό σχήμα, που επιτρέπει την πιστοποίηση της ταυτότητας και την ορθή απόδοση και διαχείριση πιστοποιητικών κάθε φυσικού προσώπου που εμπλέκεται σε μια ηλεκτρονική συναλλαγή, προστατεύοντας συγχρόνως την ασφάλεια της συναλλαγής. Μια τυπική υλοποίηση PKI περιλαμβάνει την παροχή ψηφιακών πιστοποιητικών σε χρήστες, εξυπηρετητές (servers) και λογισμικό χρηστών. Παράλληλα, προσφέρει σειρά εργαλείων για τη διαχείριση, ανανέωση και ανάκληση των πιστοποιητικών.[13]

Τα PKIs συστήματα μπορούν να διασφαλίσουν και τα τέσσερα χαρακτηριστικά της έννοιας της ασφάλειας, την *ακεραιότητα*, την *εμπιστευτικότητα*, την *αυθεντικοποίηση* και τη *μη αποποίηση*.

Η διάδοση της υποδομής δημοσίου κλειδιού στο ηλεκτρονικό εμπόριο έχει οδηγήσει στην δημιουργία προϊόντων από πολλές εταιρίες (RSA, Verisign, GTE CyberTrust, Xcert, Netscape). Το ενδιαφέρον αυτό δημιουργεί παράλληλα, ένα πρόσφορα έδαφος για την υιοθέτηση ανάλογων τεχνολογιών και από τις δημόσιες υπηρεσίες σε θέματα ηλεκτρονικής διακυβέρνησης.

Τα PKIs αντιμετωπίζονται ως υποστηρικτικές μέθοδοι για τη διαχείριση ταυτοτήτων και τα ταξιδιωτικά έγγραφα, σύμφωνα με τον ICAO [65]. Το ζήτημα που, ωστόσο, δεν φαίνεται να επιλύεται, μέσω των PKI υποδομών, είναι εκείνο της διαλειτουργικότητας, παρά το γεγονός ότι προβλέπονται σχετικές διαδικασίες όπως η αμοιβαίας αναγνώρισης και διαπιστοποίησης (cross-certification) για τα διεθνώς «μετακινούμενα» πιστοποιητικά. Αυτό πιθανότατα οφείλεται στην απουσία μιας κεντρικής ευρωπαϊκή Αρχής Πιστοποίησης (Root-CA). Δεδομένου, ότι το ζήτημα της διαλειτουργικότητας είναι πολύ σημαντικό για την περαιτέρω ανάπτυξη και χρήση της ευρωπαϊκής ΚΠ, πολλά έργα τρέχουν ήδη προς αυτή την κατεύθυνση.

5.3.4.1. Αρχιτεκτονική PKI

Η βασική αρχιτεκτονική για χρήση κρυπτογραφίας δημοσίου κλειδιού είναι η υποδομή δημοσίου κλειδιού (PKI-Public Key Infrastructure) που βασίζεται σε ζεύγη κλειδιών και ψηφιακά πιστοποιητικά. Στην κρυπτογραφία δημοσίου κλειδιού, τόσο το δημόσιο όσο και το ιδιωτικό κλειδί δημιουργούνται ταυτόχρονα, από την Αρχή Πιστοποίησης, με την χρήση του ίδιου αλγόριθμου. Το ιδιωτικό κλειδί δίνεται μόνο στον αιτούντα ενώ το δημόσιο κλειδί είναι διαθέσιμο (ως τμήμα του ψηφιακού πιστοποιητικού) σ' ένα κατάλογο στον οποίο έχουν πρόσβαση όλοι οι δικαιούχοι. Αντίθετα, το ιδιωτικό κλειδί δεν κοινοποιείται ποτέ ούτε αποστέλλεται μέσω διαδικτύου.

Τα PKIs διαχειρίζονται δημόσια κλειδιά πιστοποιητικών και διασφαλίζουν την ασφάλεια των πληροφοριών παρέχοντας έναν τρόπο οργάνωσης της φυσικής υποδομής, των εφαρμογών, της διαχείρισης και των διαδικασιών που υποστηρίζουν. Οι χρήστες, ωστόσο, δεν χρειάζεται να καταλαβαίνουν τον τρόπο που γίνεται η διαχείριση των κλειδιών και των πιστοποιητικών προκειμένου να χρησιμοποιήσουν τις υπηρεσίες του PKI, σύμφωνα με την αρχή της διαφάνειας (transparency). Η υποδομή αυτή αποτελεί συνήθη επιλογή για πληθώρα λογισμικού και εφαρμογών που βασίζουν τη λειτουργία τους σε κάποιο είδος PKI. Ειδικότερα, δε στην περίπτωση της ηλεκτρονικής ταυτοποίησης και των έξυπνων καρτών αποτελούν την πλέον ενδεδειγμένη πρακτική.

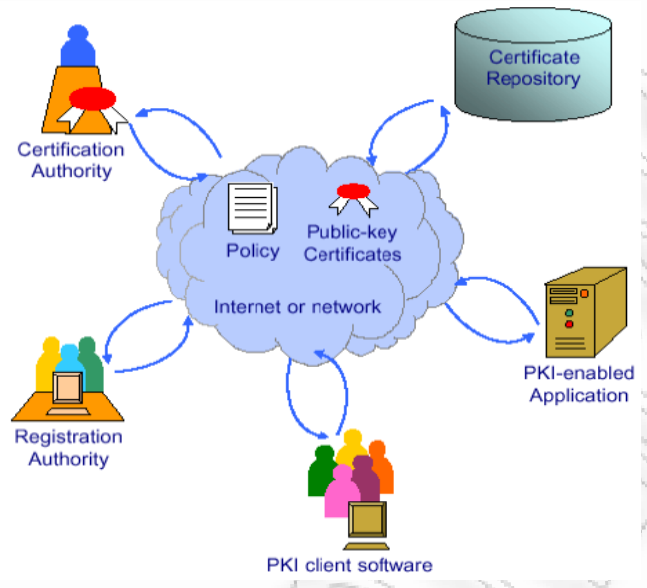
Η πιο σημαντική έννοια που εισάγεται με την υποδομή δημόσιου κλειδιού είναι η έννοια της τρίτης οντότητας. Οι υπηρεσίες Έμπιστης οντότητας σε PKI συστήματα χρησιμοποιούνται για την αποθήκευση κλειδιού, τη χρονολόγηση, την αρχειοθέτηση εγγράφων και ως ενδιάμεση οντότητα, ενώ οι υπηρεσίες επίλυσης διαφορών προσδίδουν ακόμη περισσότερη εμπιστοσύνη.

5.3.4.2. Οντότητες και λειτουργίες PKI

Οι βασικές οντότητες που αλληλεπιδρούν μεταξύ τους στα συστήματα PKI (σύμφωνα με το PKIX Working Group της IETF [84]) είναι :

- Αρχή Πιστοποίησης (Certification Authority), η οποία εκδίδει και πιστοποιεί ψηφιακά πιστοποιητικά. Τα ψηφιακά πιστοποιητικά που εκδίδονται από την αρχή περιλαμβάνουν το δημόσιο κλειδί ή πληροφορίες για το δημόσιο κλειδί.
- Αρχή Εγγραφής (Registration Authority), η οποία χρησιμεύει για την επιβεβαίωση της αρχής έκδοσης πιστοποιητικών προτού εκδοθεί ένα ψηφιακό πιστοποιητικό.
- Σύστημα διαχείρισης πιστοποιητικών που περιλαμβάνει την αποθήκη πιστοποιητικών και λιστών ανάκλησης πιστοποιητικών (Repository/Certificate Revocation Lists) και υπηρεσίες καταλόγου (directory services) όπου διατηρούνται τα πιστοποιητικά (μαζί με τα δημόσια κλειδιά)
- Πελάτες (Clients)

Στην παρακάτω εικόνα μπορούμε να δούμε και την αλληλεπίδραση των οντοτήτων μεταξύ τους.



Εικόνα 30- Αλληλεπίδραση οντοτήτων

Στο σημείο αυτό όμως γίνεται και μια προσπάθεια περιγραφής όλων των συστατικών μερών που παίζουν ρόλο στις διαδικασίες των PKI.

Αρχή Πιστοποίησης (Certification Authority): Χρησιμοποιείται για τη διαχείριση ψηφιακών πιστοποιητικών. Μια αρχή πιστοποίησης αποτελείται από πρόσωπα, διαδικασίες και εργαλεία που συνδέουν χρήστες με δημόσια κλειδιά, για τη δημιουργία ψηφιακών πιστοποιητικών. Η Αρχή αποτελεί εκείνον τον φορέα που προσδίδει εμπιστοσύνη στα PKI συστήματα. Συνεπώς, όταν οι χρήστες εμπιστεύονται μια αρχή πιστοποίησης εμπιστεύονται, παράλληλα, και τα πιστοποιητικά που εκείνη εκδίδει και διαχειρίζεται (Third Party Trust). Η ακεραιότητα ενός πιστοποιητικού μπορεί να καθοριστεί από την επιβεβαίωση της υπογραφής της αρχής πιστοποίησης και επομένως δεν απαιτούνται επιπρόσθετοι μηχανισμοί ασφάλειας. Το γεγονός αυτό σημαίνει ότι μπορούν να διανέμονται δημόσια (μέσα από συστήματα καταλόγου που επιτρέπουν την πρόσβαση σε όλους)

Αρχή Καταχώρησης (Registration Authority): Η αρχή αυτή πιστοποίει την ταυτότητα όσων ζητούν πιστοποιητικό. Αποτελεί τη διεπαφή μεταξύ του χρήστη και της αρχής πιστοποίησης. Η ποιότητα της διαδικασίας ταυτοποίησης καθορίζει και το επίπεδο εμπιστοσύνης του παρεχόμενου πιστοποιητικού.

Πολιτική ασφάλειας (Security Policy): Περιλαμβάνει οδηγίες για τη διαχείριση των κλειδιών και των σημαντικών πληροφοριών.

Αρχές Ασφάλειας Πληροφοριών (Certificate Practice Statement): Περιλαμβάνει όλες τις λειτουργικές διαδικασίες προκειμένου να εφαρμοστεί η ασφάλεια της λειτουργίας των

αρχών πιστοποίησης στην πράξη (δηλαδή, δημιουργία και ανάκληση πιστοποιητικών και δημιουργία, κατοχύρωση, επιβεβαίωση, αποθήκευση και διανομή των κλειδιών).

Σύστημα διανομής πιστοποιητικών (Directory Services): Χρησιμοποιείται για την αποθήκευση πιστοποιητικών που εκδίδει η αρχή πιστοποίησης. Οι υποδομές δημόσιου κλειδιού αποθηκεύουν τα πιστοποιητικά που εκδίδουν σε αποθήκες πιστοποιητικών (certificate repositories), ώστε να μπορούν να ανακτούνται από τις εφαρμογές των χρηστών. Η πιο συχνά χρησιμοποιούμενη τεχνολογία για την αποθήκευση πιστοποιητικών είναι τα συστήματα καταλόγου (Directory Systems) που είναι συμβατά με το πρωτόκολλο LDAP (Lightweight Directory Access Protocol), καθώς είναι κατανεμημένα, μπορούν να υποστηρίξουν μεγάλο αριθμό εγγραφών και να ανταποκριθούν αποτελεσματικά σε ερωτήματα αναζήτησης πιστοποιητικών.

Οι υποδομές δημόσιου κλειδιού αποτελούνται δηλαδή από :

- Πιστοποιητικά (Certificates)
- Υποκείμενα ή Εγγραφόμενους (Subjects or Subscribers)
- Βασιζόμενες οντότητες (Relying Parties - RP)
- Δηλώσεις Πρακτικών Πιστοποίησης (Certification Practice Statements - CPS)
- Πολιτικές Πιστοποιητικών (Certificate Policies - CP)
- Αποθηκευτικούς μηχανισμούς και Υπηρεσίες Καταλόγου (Repositories & Directories)
- Μηχανισμούς Διαλειτουργικότητας (Interoperability mechanisms)
- Δεδομένα Δημιουργίας Υπογραφής (Signature-creation data)
- Συσκευές Δημιουργίας Υπογραφής (Signature-creation device)
- Δεδομένα Επαλήθευσης Υπογραφής (Signature-verification data)

5.3.4.3. Διαδικασίες PKI

Οι βασικές λειτουργίες ενός συστήματος PKI είναι η έκδοση νέου πιστοποιητικού για ένα δημόσιο κλειδί (καταγραφή δημοσίου κλειδιού - Key Registration), η ακύρωση ενός εκδοθέντος πιστοποιητικού(Certificate Revocation), η απόκτηση δημοσίου κλειδιού της άλλης οντότητας, είτε αυτή είναι χρήστης, είτε υπηρεσία (Key Selection) και η εκτίμηση εμπιστοσύνης (Trust Evaluation) με βάση την οποία αποφασίζεται αν ένα πιστοποιητικό είναι έγκυρο και σε ποιες υπηρεσίες επιτρέπει πρόσβαση.

Στο πλαίσιο αυτό, οι κύριες υπηρεσίες που παρέχονται μέσα από τέτοιες υποδομές περιγράφονται ακολούθως:

1. Δημιουργία κλειδιού (Generation): Αφορά στη δημιουργία ενός ζεύγους ιδιωτικού/δημόσιου κλειδιού.
2. Καταχώρηση κλειδιού (Registration): Είναι η κατοχύρωση της σχέσης μεταξύ του κλειδιού και της οντότητας στην οποία αντιστοιχεί (ψηφιακό πιστοποιητικό).
3. Διανομή κλειδιού (Distribution) στον χρήστη.
4. Επιβεβαίωση της εγκυρότητας του κλειδιού (Verification).

5. Ανάκληση κλειδιού (Revocation), όταν ένα κλειδί δεν είναι έγκυρο ή έχει κλαπεί. Ένα PKI πρέπει να παρέχει ένα σύστημα ανάκλησης των πιστοποιητικών, ώστε να μπορούν οι εφαρμογές να ελέγχουν την κατάσταση των πιστοποιητικών κάθε φορά πριν να τα χρησιμοποιήσουν. Η αρχή πιστοποίησης οφείλει να δημοσιεύει τις πληροφορίες για την κατάσταση κάθε πιστοποιητικού του συστήματος σε τακτά χρονικά διαστήματα και η πράξη της ανάκλησης αποθηκεύεται στις αντίστοιχες λίστες ανάκλησης (Certificate Revocation Lists) για λόγους συνέπειας και ασφάλειας και δημοσιεύεται μέσω του συστήματος καταλόγου. Για τις λίστες ανάκλησης πρέπει να ισχύει α) να είναι ανά πάσα στιγμή επικαιροποιημένες, αυθεντικές, ακέραιες και διαθέσιμες, β) να παρέχουν τη δυνατότητα πολλαπλών προσπελάσεων σε εγγραφές που βρίσκονται σε διαφορετικές βάσεις δεδομένων.
6. Επαναφορά κλειδιού (Recovery): Δημιουργούνται μέσω της επαναφοράς αντίγραφα κλειδιών σε περιπτώσεις απώλειας ή αδυναμίας χρήσης τους (αν ξεχάσει τον κωδικό πρόσβασης). Τα μόνα κλειδιά που χρειάζονται επαναφορά είναι τα κλειδιά κρυπτογράφησης. Αντίθετα, τα κλειδιά που χρησιμοποιούνται για ψηφιακές υπογραφές δεν πρέπει να επαναφέρονται γιατί τότε δεν ικανοποιείται μια βασική απαίτηση από ένα PKI, περί μη αποποίησης.

5.3.4.4. Πιστοποίηση μέσω PKI

Η δημιουργία κλειδιού είναι ουσιαστικά η διαδικασία ανάθεσης ενός ζεύγους δημόσιου/ιδιωτικού κλειδιού σε μία οντότητα. Ο έλεγχος για την μοναδικότητα του κλειδιού πραγματοποιείται με τη βοήθεια της βάσης δημόσιων κλειδιών, της Αρχής Πιστοποίησης. Μια αρχή πιστοποίησης δέχεται αιτήσεις πιστοποίησης από πολλές αρχές καταχώρησης.

Η Αρχή Καταχώρησης ουσιαστικά μεταβιβάζει το αίτημα του χρήστη για έκδοση πιστοποιητικού στην Αρχή Πιστοποίησης έχοντας προηγουμένως συλλέξει όλες τις απαιτούμενες πληροφορίες από τον χρήστη, ανάλογα με τη διαδικασία που χρησιμοποιεί (online αίτηση μέσω ηλεκτρονικής φόρμας, αίτηση με αποστολή συνοδευτικού υλικού, αίτηση με φυσική παρουσία). Οι καταχωρημένες πληροφορίες μεταφέρονται στην Αρχή Πιστοποίησης μέσω ασφαλών μηνυμάτων και ο χρήστης κατοχυρώνει ένα δημόσιο κλειδί. Μετά την δημιουργία του, το δημόσιο τμήμα του κλειδιού αποστέλλεται στην Αρχή Πιστοποίησης προκειμένου να επιβεβαιωθεί η μοναδικότητά του, ότι δηλαδή το συγκεκριμένο δημόσιο κλειδί δεν έχει καταχωρηθεί από άλλο χρήστη και να ενσωματωθεί σε πιστοποιητικό και έτσι να πιστοποιηθεί η εγκυρότητα αυτού και η συσχέτισή του με τα στοιχεία της οντότητας που υπάρχουν στο πιστοποιητικό. Το πιστοποιητικό εκδίδεται με ορισμένη ισχύ, μοναδικό αριθμό και συγκεκριμένη κατάσταση.

Η εναλλακτική περίπτωση της παραπάνω διαδικασίας είναι η παραγωγή των κλειδιών από την Αρχή Πιστοποίησης, η οποία, συγχρόνως, αναλαμβάνει συχνά και το ρόλο της διαφύλαξης των κλειδιών (key escrow) για νομικούς, πρακτικούς ή επιχειρηματικούς λόγους [13].

Μέσω της διαδικασίας πιστοποίησης, ο κάθε χρήστης διαθέτει ένα ιδιωτικό και ένα δημόσιο κλειδί. Το ιδιωτικό κλειδί είναι μυστικό καθώς διασφαλίζει την απόδειξη της ταυτότητας του αποστολέα και την πλήρη ακεραιότητα της πληροφορίας που μεταφέρεται. Η γνωστοποίηση του σε τρίτο καθίσταται απαγορευτική, ακόμη κι αν πρόκειται για την Αρχή Πιστοποίησης κι ακόμη και στην περίπτωση που ζητηθεί κάτι τέτοιο από το χρήστη. Για το λόγο αυτό, σημειώνεται η ανάγκη προστασίας του με μεθόδους προσωπικών κωδικών πρόσβασης (PIN - Personal Identification Number).

Αντίθετα, το δημόσιο κλειδί ενός χρήστη είναι διαθέσιμο στην αποκρυπτογραφημένη (απλή) μορφή του, σε οποιονδήποτε άλλη οντότητα. Το δημόσιο κλειδί χρησιμοποιείται συνήθως:

- Για την επιβεβαίωση ή εξακρίβωση ότι ένα ψηφιακά υπογεγραμμένο μήνυμα έχει δημιουργηθεί μετά από την χρήση του αντίστοιχου ιδιωτικού κλειδιού. Αυτή η επιβεβαίωση σημαίνει ότι σίγουρα μόνο ο κάτοχος του ιδιωτικού κλειδιού έχει υπογράψει το συγκεκριμένο μήνυμα.
- Δίνει την δυνατότητα σε οποιονδήποτε θελήσει να στείλει κάποιο κρυπτογραφημένο μήνυμα στον κάτοχο του αντίστοιχου δημόσιου κλειδιού που έχει στην κυριότητά του ο αποστολέας.

Οι χρήστες εξάγουν πληροφορίες για τα πιστοποιητικά από καταλόγους, με την βοήθεια πρακτόρων (agents). Οι κατάλογοι είναι απαραίτητοι για την επαλήθευση της εγκυρότητας ενός πιστοποιητικού. Ένα καταχωρημένο πιστοποιητικό δεν είναι απαραίτητα και έγκυρο.

5.3.4.5. Third party trust

Αναφέρεται στην περίπτωση όπου δύο οντότητες εμπιστεύονται απόλυτα η μια την άλλη, χωρίς να έχουν προηγουμένη συναλλαγή μεταξύ τους. Σε αυτή την περίπτωση, υπάρχει εμπιστοσύνη γιατί μοιράζονται κοινή σχέση με μια τρίτη πλευρά (Αρχή Πιστοποίησης), που εμπιστεύονται και οι δύο και η οποία πιστοποιεί την ταυτότητά τους.

Οι Αρχές Πιστοποίησης συνδέονται μεταξύ τους σε σχέσεις-αρχιτεκτονικές εμπιστοσύνης, οι κατηγορίες των οποίων παρουσιάζονται παρακάτω:

- Ομοπάτρια (single parent)
- Διμερής (web-of-trust)
- Ιεραρχική (hierarchy): Όλα τα πιστοποιητικά που ανήκουν σε ένα έμπιστο πιστοποιητικό, θεωρούνται επίσης έμπιστα. Το πιστοποιητικό που βρίσκεται στην κορυφή της ιεραρχίας (πιστοποιητικό ρίζας) είναι «αυτό-υπογραφόμενο» (self-signed). Αποτελεί έναν πρακτικό μηχανισμό για τη διανομή του κλειδιού, ωστόσο δεν είναι ασφαλής, καθώς ενέχουν τον κίνδυνο ασφάλειας όλης της δομής από μια μη ασφαλή κορυφή και δεν χρησιμοποιείται σε διεθνές επίπεδο.
    - Απόλυτα ιεραρχική
    - Ιεραρχία με χρήση αντίστροφων πιστοποιητικών
    - Μοντέλο προσανατολισμένου γράφου

- Δια-πιστοποίηση (cross-certification): Η διαδικασία ανταλλαγής πληροφοριών μεταξύ δύο αρχών πιστοποίησης, ώστε να μπορεί η μία να εμπιστεύεται τα κλειδιά που παράγονται από την άλλη και αντιστρόφως. Η διαπιστοποίηση αποτελεί μια εκτεταμένη μορφή third party trust, όπου όλοι οι χρήστες που ανήκουν στην μία αρχή εμπιστεύονται όλους τους χρήστες της άλλης. Η διαδικασία αυτή, προϋποθέτει ότι κάθε μια από τις εμπλεκόμενες Αρχές Πιστοποίησης πρέπει να εγκρίνει την πολιτική ασφάλειας που ακολουθεί η άλλη και δημιουργούν μεταξύ τους σχέση εμπιστοσύνης (αμφίδρομη ή μονόδρομη) υπογράφοντας η μία το πιστοποιητικό της άλλης. Συνεπάγεται λοιπόν ταυτόχρονα, και η εμπιστοσύνη μιας οντότητας στο πιστοποιητικό μιας άλλης, εφόσον εκδίδεται από Αρχή Πιστοποίησης που εμπιστεύεται η αρχική οντότητα. Έτσι, η Αρχή Πιστοποίησης γίνεται το σημείο εμπιστοσύνης (trust anchor) και οτιδήποτε συνδέεται μέσω έμπιστης διαδρομής μαζί της, είναι επίσης έμπιστο.
- Έμπιστου μεσολαβητή (Trusted broker ή Bridge CA): Όλες οι Αρχές Πιστοποίησης διαπιστοποιούνται με μία κεντρική Αρχή Πιστοποίησης (Bridge CA) σε σχήμα αστεριού. Μία οντότητα που εμπιστεύεται τον έμπιστο μεσολαβητή (σημείο εμπιστοσύνης) εμπιστεύεται και όλες τις Αρχές Πιστοποίησης που εκείνος υποδεικνύει.
- Δάσος ή Μικτή (Forest ή Mixed)

Η εμπιστοσύνη σε ένα πιστοποιητικό βασίζεται στην ψηφιακή υπογραφή της εκδούσας Αρχής Πιστοποίησης αλλά και στο πόσο έμπιστη είναι η ίδια η αρχή έκδοσης. Για να υπάρχει εμπιστοσύνη μεταξύ δυο μερών, πρέπει να μπορούν να αποκτήσουν και να επιβεβαιώσουν ο ένας το πιστοποιητικό του άλλου. Η διαδικασία συνήθως έχει ως εξής:

1. Το ένα μέρος λαμβάνει το δημόσιο κλειδί της αρχής πιστοποίησης που πιστοποιεί το άλλο μέρος.
2. Στην περίπτωση που πιστοποιούνται από διαφορετικές αρχές πιστοποίησης, τότε πρέπει να πιστοποιηθούν με βάση την ιεραρχία αυτών, εκτός αν υπάρχει αμοιβαία πιστοποίηση.
3. Κάθε συναλλασσόμενο μέρος λαμβάνει το πιστοποιητικό του άλλου και ελέγχει την εγκυρότητα του με βάση το δημόσιο κλειδί της εκδούσας αρχής.
4. Τέλος, ελέγχεται η εγκυρότητα των πιστοποιητικών και εφόσον αυτά είναι έγκυρα, τα δημόσια κλειδιά τους μπορούν να χρησιμοποιηθούν για ασφαλή μετάδοση πληροφοριών.

5.3.5. Τεχνικές κατά ICAO και BSI

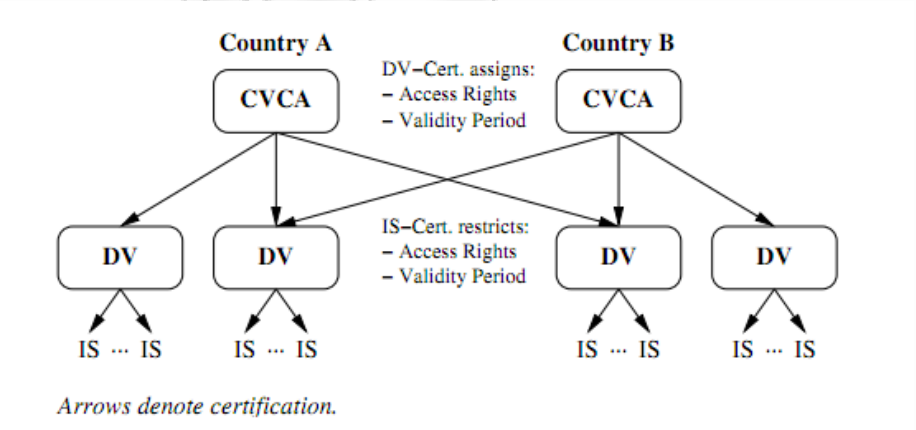
Όσον αφορά τη χρήση της PKI στα ταξιδιωτικά έγγραφα (MRTD) κατά τον ICAO η τεχνολογία αυτή είναι απλά ένας επιπλέον τρόπος και όχι ο μοναδικός διαθέσιμος για τον προσδιορισμό της αυθεντικότητας ενός MRTD σε έναν συνοριακό έλεγχο.

Όπως περιγράφεται στο έγγραφο 9303 P3V2 [88], του ICAO, οι εμπλεκόμενες PKI οντότητες είναι:

- Η Εθνική Αρχή Πιστοποίησης του κάθε κράτους (Country Signing Certification Authority, CSCA) η οποία εκδίδει το αυθυπόγραφο πιστοποιητικό (Country Signing Certification Authority Certificates, CCSCA) για τη διανομή του δημοσίου κλειδιού της. Το πιστοποιητικό αυτό θα πρέπει να είναι εγκατεστημένο σε όλα τα συστήματα επιθεώρησης (Inspection Systems, IS) καθώς το σχετικό δημόσιο κλειδί χρησιμοποιείται για την επιβεβαίωση αυθεντικότητας του πιστοποιητικού της υφιστάμενης οντότητας. Το αντίστοιχο ιδιωτικό κλειδί είναι υψίστης κρισιμότητας για την ασφάλεια της αρχιτεκτονικής και πρέπει να φυλάσσεται σε ασφαλές περιβάλλον.
- Οι αρχές έκδοσης της κάρτας που έχουν δικαίωμα υπογραφής των αποθηκευμένων δεδομένων (Document Signer, DS). Το σχετικό τους πιστοποιητικό (Document Signer Certificates, Cds) που εκδίδεται από την Αρχή είναι αποθηκευμένο στο σύστημα επιθεώρησης και περιλαμβάνει το δημόσιο κλειδί, που χρησιμοποιείται για την επιβεβαίωση της αυθεντικότητας.

Το κάθε Κράτος οφείλει να εγκαθιστά, με δική του ευθύνη, ασφαλείς υποδομές για την παραγωγή κλειδιών και πιστοποιητικών. Οι υποδομές αυτές θα πρέπει να πληρούν όλες τις σύγχρονες καλές πρακτικές ασφάλειας, όσον αφορά την προστασία φυσικής ή απομακρυσμένης πρόσβασης από μη εξουσιοδοτημένα άτομα μέσω κατάλληλου κτιριακού σχεδιασμού, υιοθέτηση μηχανισμών και διαδικασιών ασφάλειας, εγκατάσταση υλικού ασφάλειας καθώς και τήρηση όσων ορίζει το Νομικό Πλαίσιο αναφορικά με τη παροχή υπηρεσιών πιστοποίησης (Οδηγία 1999/93/ΕΚ «Παράρτημα ΙΙ» [41]).

Τα Κράτη που εξετάζουν σε συνοριακούς ελέγχους τα MRTD θα πρέπει να λαμβάνουν σε τακτική βάση ενημερωμένη λίστα από το ICAO PKD προκειμένου να λειτουργούν αποτελεσματικά τα επιμέρους συστήματα επιθεώρησης.



Εικόνα 31-Σχήμα πιστοποίησης

Στην προσέγγιση του γερμανικού BSI στην τεχνική αναφορά του [86], η βασική διαφορά εντοπίζεται στο ρόλο του PKI που δεν περιορίζεται στην υπογραφή των MRTDs αλλά και στην επιβεβαίωση των πιστοποιητικών που φέρουν τα συστήματα επιθεώρησης. Αυτή η προσέγγιση ακολουθείται και στο Ευρωπαϊκό πρότυπο [94] για την υποστήριξη έξυπνων καρτών που χρησιμοποιούνται ως ασφαλείς διατάξεις παραγωγής ψηφιακών υπογραφών.

Στην προσέγγιση αυτή εισάγεται ένας νέος τύπος πιστοποιητικού που καλείται Terminal Certificate. Το πιστοποιητικό αυτό ενσωματώνει το δημόσιο κλειδί του συστήματος επιθεώρησης (Terminal) και τα δικαιώματα πρόσβασής του. Ένα MRTD θα εξετάζει αυτό το πιστοποιητικό για να αποφανθεί ότι το σύστημα επιθεώρησης είναι αυθεντικό και ότι έχει πράγματι τα σχετικά δικαιώματα πρόσβασης σε ορισμένα δεδομένα του MRTD.

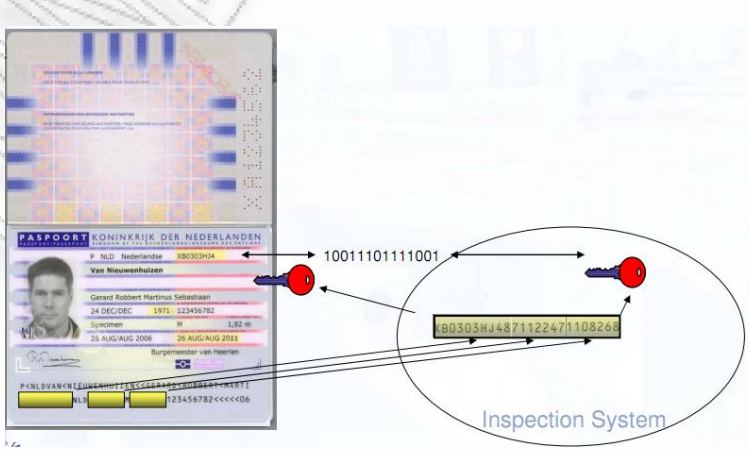
Στη ρίζα της ιεραρχίας εξακολουθεί να είναι η Εθνική Αρχή Πιστοποίησης του κάθε κράτους η οποία εκτός του ότι εκδίδει πιστοποιητικά για τις αρχές έκδοσης της κάρτας (Document Signers) καθορίζει και τα δικαιώματα πρόσβασης των σχετικών αρχών (Document Verifiers) στα δεδομένα των εθνικών MRTDs. Στο επόμενο επίπεδο βρίσκονται οι Document Verifiers, οργανωτικές μονάδες που έχουν υπό την εποπτεία τους μια ομάδα από συστήματα επιθεώρησης. Η πρόσβαση σε προσωπικά δεδομένα που είναι αποθηκευμένα σε ένα MRTD μιας άλλης χώρας, επιτυγχάνεται μέσω των Terminal Certificates.

5.3.5.1. Basic Access Control (BAC)

Ο Βασικός μηχανισμός Ελέγχου Πρόσβασης (Basic Access Control, BAC) που ανέπτυξε ο ICAO αποτελεί την κύρια διαδικασία αμοιβαίας αυθεντικοποίησης κι έρχεται να επιλύσει θέματα ασφάλειας και ιδιωτικότητας.

Ο BAC δημιουργεί κρυπτογραφικά κλειδιά (Document Basic Access Keys) για την εμπιστευτικότητα και την ακεραιότητα (KENC και KMAC αντίστοιχα), τα οποία είναι απαραίτητα για την πρόσβαση στα δημόσια δεδομένα του τσιπ και εξασφαλίζουν την ασφαλή επικοινωνία μεταξύ MRTD και του συστήματος επιθεώρησης. Για να δημιουργηθούν αυτά τα κλειδιά είναι απαραίτητη η ανάγνωση οπτικά του MRZ από τη φυσική κάρτα. Ως εκ τούτου, ο μηχανισμός BAC βασίζεται στη μυστικότητα της MRZ ζώνης. Αυτό σημαίνει ότι πρέπει να προφυλάσσεται η MRZ ζώνη από μη εξουσιοδοτημένη πρόσβαση.

Ο BAC αποσκοπεί, επιπλέον, στην εγκαθίδρυση νέων μυστικών κλειδιών συνόδου (ISO/IEC 11770-2, μηχανισμός 6 [96]), τα οποία χρησιμεύσουν για μελλοντικές ασφαλείς επικοινωνίες (secure messaging - προστασία εμπιστευτικότητας και ακεραιότητας) μεταξύ ICC(Integrated Circuit Card) και IFD (Interface Device) για την εν λόγω σύνοδο.



Εικόνα 32-Χρήση του BAC

Αναφορικά με το ζήτημα της ασφαλούς μετάδοσης, ο BAC ενσωματώνει χαρακτηριστικά Secure Messaging, προκειμένου να εξασφαλίσει την ακεραιότητα, αυθεντικότητα και εμπιστευτικότητα όλων των μηνυμάτων (εντολών και αποκρίσεων) που διακινούνται μεταξύ αναγνώστη και κάρτας.

Παρότι ο BAC μηχανισμός είναι εύκολος στην υλοποίηση υπάρχει μια σημαντική ευπάθεια ασφάλειας αναφορικά με τα συμμετρικά βασικά κλειδιά πρόσβασης (KENC και KMAC) που χρησιμοποιούνται για την αμοιβαία αυθεντικοποίηση και την ασφαλή μετάδοση των επικοινωνιών μεταξύ κάρτας και αναγνώστη. Τα εν λόγω κλειδιά που προκύπτουν κρυπτογραφικά αδύναμα και κατά συνέπεια, μπορεί δυνητικά να παραβιαστεί ο αλγόριθμος μέσω του οποίου δημιουργήθηκε το κλειδί, χρησιμοποιώντας κάποιες σχετικά απλές εκτιμήσεις (εκτιμώντας την ηλικία του κατόχου, καθώς ενδέχεται να έχει οπτική επαφή με τον κάτοχο, αναλύοντας του σειριακού αριθμού – διακριτικά χώρας, εκδούσας αρχής- του MRTD, σχέση ημερομηνίας λήξης και αριθμού σειράς στην περίπτωση της μονοτονικής αύξησης του αριθμού σειράς). Έτσι, είναι επιρρεπής σε επιθέσεις Brute-Force, όπου μετά την καταγραφή της κρυπτογραφημένη σύνοδο και τον υπολογισμό των κλειδιών βασικής πρόσβασης μπορούν να υπολογισθούν τα κλειδιά συνόδου και επομένως να αποκρυπτογραφηθεί η αποθηκευμένη συνεδρία. Για να ενισχυθεί η ασφάλεια του BAC θα μπορούσε να χρησιμοποιηθεί ένα προαιρετικό πεδίο δεδομένων για την συμπερίληψη ενός τυχαίου αριθμού με ψηφίο ελέγχου.

Ένα αντίμετρο που εφαρμόζεται είναι η επιβράδυνση της εκτέλεσης της BAC διαδικασίας ώστε να επιμηκύνεται ο χρόνος που ο επιτιθέμενος πρέπει να μείνει σε επαφή με το εν λόγω MRTD τσιπ. Αυτό περιορίζει τις skimming επιθέσεις αλλά όχι και τις επιθέσεις υποκλοπής όπου τα δεδομένα αναλύονται offline σε δεύτερο χρόνο.

5.3.5.2. Extended Access Control (EAC)

Το πρωτόκολλο εκτεταμένου ελέγχου πρόσβασης (Extended Access Control, EAC) χρησιμοποιείται για την αμοιβαία αυθεντικοποίηση των δύο μερών (ICC και σύστημα επιθεώρησης). Στόχος του πρωτοκόλλου είναι να εγκαθιδρύσει, ασφαλώς, μυστικά κλειδιά συνόδου, μέσω των οποίων, τα δύο μέρη να «θωρακίσουν» τις μελλοντικές τους επικοινωνίες.

Το πρωτόκολλο ανταλλαγής κλειδιού EAC περιλαμβάνει δύο φάσεις:

1. Εκτέλεση πρωτοκόλλου πρόκλησης-απόκρισης (Terminal Authentication), για τον περιορισμό της πρόσβασης στα δεδομένα του τσιπ της κάρτας μόνο σε εξουσιοδοτημένα τερματικά.
2. Εκτέλεση πρωτοκόλλου ανταλλαγής κλειδιού (Chip Authentication) όπου τα δύο συμβαλλόμενα μέρη με βάση τον Diffie-Hellman μηχανισμό συμφωνούν σε ένα μυστικό κλειδί που παράγεται από το εφήμερο κλειδί του τερματικού και το στατικό πιστοποιημένο κλειδί του τσιπ της κάρτας. Επιπλέον το τσιπ αυθεντικοποιείται ως γνήσιο και τέλος η διαδικασία ολοκληρώνεται επιβάλλοντας

ισχυρή κρυπτογράφηση και προστασία της ακεραιότητας των δεδομένων που διαβιβάζονται στις επικοινωνίες (Secure Messaging).

Σχηματικά η διαδικασία παρουσιάζεται στο ακόλουθο σχήμα [93]:

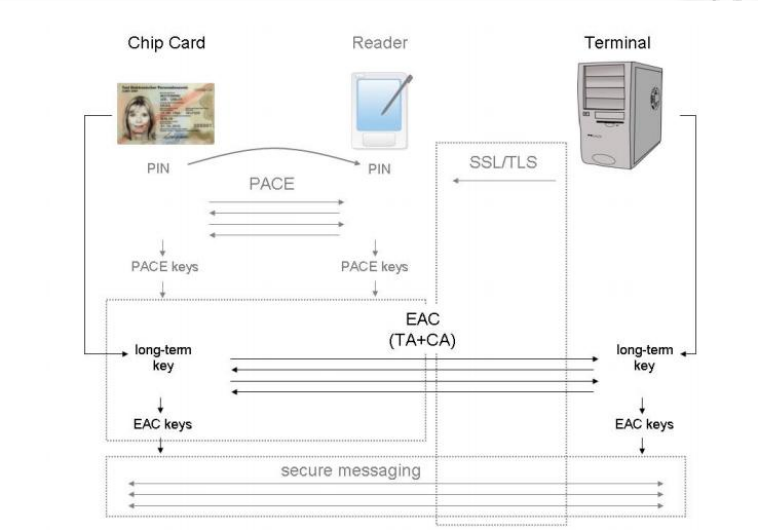


Fig. 1. EAC Protocol for Machine Readable Travel Documents

Εικόνα 33-Εφαρμογή EAC σε MRTD

Ένα άλλο υπο-πρωτόκολλο που προτείνει ο BSI είναι το PACE (για αντικατάσταση του BAC) το οποίο εκτελείται πριν από τα υπόλοιπα και χρησιμοποιείται για την ασφαλή εγκαθίδρυση μυστικού κλειδιού μεταξύ του τσιπ της κάρτας και του αναγνώστη. Στην περίπτωση που το τερματικό είναι ξεχωριστή απομακρυσμένη συσκευή, θα πρέπει επίσης να προστατεύεται η επικοινωνία με τον αναγνώστη με SSL/TLS, πριν ξεκινήσουν οι διαδικασίες του EAC.

Στην EAC εφαρμόζονται μοντέλα ασφαλείας που αφορούν στην αυθεντικοποιημένη εγκαθίδρυση κλειδιού (Authenticated Key Exchange) [93]. Τα μοντέλα αυτά παρέχουν ισχυρές εγγυήσεις ότι τα κλειδιά που παράγονται παραμένουν ασφαλή ακόμη και υπό τη παρουσία ενεργών επιθέσεων και υπό την εκτέλεση πολλαπλών συναλλαγών. Κατά συνέπεια, η EAC είναι ασφαλής υπό την προϋπόθεση ότι οι θεμελιώδεις κρυπτογραφικές λειτουργίες της είναι επίσης ασφαλείς (αλγόριθμοι υπογραφής, MAC αλγόριθμοι, συναρτήσεις σύνοψης κλπ).

5.3.5.3. Password Authenticated Connection Establishment (PACE)

Ο μηχανισμός Password Authenticated Connection Establishment ή PACE που προτείνει ο BSI μπορεί να χρησιμοποιηθεί ως αυτόνομο πρωτόκολλο για την αντικατάσταση του BAC, καθώς είναι περισσότερο ασφαλές [92]. Μάλιστα, ο ICAO αναγνωρίζοντας τα προβλήματα του BAC, ορίζει τον PACE μηχανισμό ως συμπληρωματικό του BAC και ξεκινά την προώθησή του ως πρότυπο, στην σχετική τεχνική αναφορά του [91].

Συγκεκριμένα επιτρέπει στο MRTD τσιπ να επιβεβαιώσει ότι το τερματικό είναι εξουσιοδοτημένο για πρόσβαση στα λιγότερο ευαίσθητα αποθηκευμένα δεδομένα στο τσιπ. Επίσης εγκαθιδρύει ασφαλή μετάδοση Secure Messaging μεταξύ MRTD και τερματικού με χρήση ισχυρών κλειδιών συνόδου. Σε αντίθεση με τον BAC που τα παραγόμενα κλειδιά έχουν σχετικά χαμηλή εντροπία λόγω της σχέσης τους με τα MRZ δεδομένα, στον PACE η εντροπία των κωδικών (passwords) που χρησιμοποιούνται για την αυθεντικοποίηση του συστήματος επιθεώρησης έχει αρκετά μικρότερη επιρροή στα παραγόμενα κλειδιά. Αυτό έχει ως συνέπεια ο PACE να παράγει ισχυρά κλειδιά ακόμη και με χρήση μικρής εντροπίας password (σύντομα passwords πχ 6 μόνο ψηφίων). Το πλεονέκτημα είναι ότι πλέον αυτά τα passwords μπορούν εύκολα να εισάγονται χειροκίνητα.

Ο PACE υποστηρίζει 4 διαφορετικούς τύπους κωδικών:

- Card Access Number (CAN): μικρός κωδικός που είτε είναι τυπωμένος στην κάρτα είτε εμφανίζεται δυναμικά με διάφορες τεχνολογίες (π.χ. OLED) και χρησιμοποιείται για πρόσβαση στις εφαρμογές του MRTD τσιπ.
- Personal Identification Number (PIN): σύντομος κωδικός τον οποίο γνωρίζει μόνο ο νόμιμος κάτοχος της κάρτας και χρησιμοποιείται για τον έλεγχο πρόσβασης στις εφαρμογές της κάρτας.
- PIN Unblock Key (PUK): μυστικός κωδικός μεγάλου μήκους γνωστός μόνο στον νόμιμο κάτοχο της κάρτας και χρησιμοποιείται για την απεμπλοκή του PIN.
- Κωδικός MRZ: μυστικό κλειδί που παράγεται από την MRZ ζώνη.

Το πρωτόκολλο PACE είναι στην ουσία ένα αυθεντικοποιημένο με μυστικό κλειδί Κπ (που προκύπτει από τον κωδικό π που γνωρίζουν τα συμβεβλημένα μέρη) πρωτόκολλο συμφωνίας κλειδιού Diffie-Hellman. Η αυθεντικοποίηση των δύο μερών βασίζεται στον μυστικό κωδικό π.

5.3.5.4. Chip Authentication (CA)

Ο μηχανισμός αυθεντικοποίησης του τσιπ (Chip Authentication, CA) που προτείνει ο BSI μπορεί να χρησιμοποιηθεί ως αυτόνομο πρωτόκολλο για την αντικατάσταση του Active Authentication του ICAO. Ο ρόλος του είναι ακριβώς ο ίδιος με του AA, δηλαδή εξασφαλίζει σε ένα μεγάλο βαθμό ότι η κάρτα είναι αυθεντική. Επιπλέον, παράγει ισχυρά κρυπτογραφικά κλειδιά συνόδου και εξαλείφει τα ζητήματα ιδιωτικότητας που προέκυπταν από τον μηχανισμό Active Authentication αναφορικά με την υπογραφή ψευδοτυχαία παραγόμενων προκλήσεων και την ανίχνευση των κατόχων καρτών.

Ο CA μηχανισμός είναι στην ουσία ένα πρωτόκολλο συμφωνίας κλειδιού Diffie-Hellman εφήμερου και στατικού κλειδιού. Η αυθεντικοποίηση είναι μονομερής μόνο για τη μεριά του MRTD τσιπ που διατηρεί ένα στατικό ζεύγος κρυπτογραφικών κλειδιών. Το πρωτόκολλο επίσης προσφέρει παραγωγή κλειδιών συνόδου για υποστήριξη Secure Messaging. Ο CA μηχανισμός έπεται των μηχανισμών PACE ή BAC που σημαίνει ότι ήδη έχουν δημιουργηθεί κλειδιά συνόδου και ήδη όλα τα μηνύματα που ανταλλάσσονται στον Chip Authentication είναι προστατευμένα με Secure Messaging. Με την επιτυχής ολοκλήρωση του CA

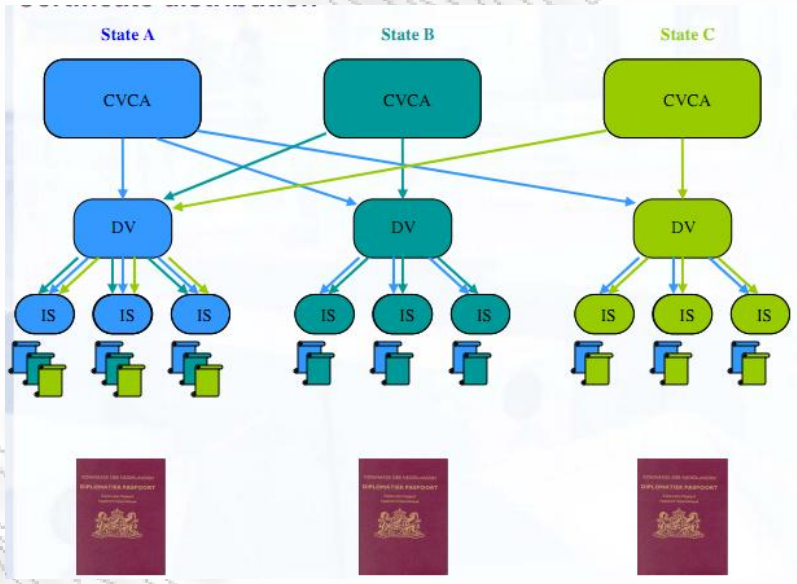
μηχανισμού όπου παράγονται νέα κλειδιά συνόδου, το Secure Messaging επανεκκινείται και πλέον χρησιμοποιεί αυτά τα νέα κλειδιά.

5.3.5.5. Terminal Authentication (TA)

Ο μηχανισμός αυθεντικοποίησης του συστήματος επιθεώρησης (Terminal Authentication, TA) επιτρέπει στο MRTD τσιπ να επιβεβαιώσει ότι το εν λόγω τερματικό που αιτείται πρόσβαση είναι αυθεντικό και ότι όντως έχει κατάλληλα δικαιώματα πρόσβασης στα ευαίσθητα δεδομένα του τσιπ. Όλα τα μηνύματα που ανταλλάσσονται στον TA προστατεύονται με Secure Messaging καθώς έχει ήδη προηγηθεί η δημιουργία κλειδιών συνόδου με τους μηχανισμούς PACE ή Chip Authentication.

Η αυθεντικοποίηση στον TA είναι μονομερής, μόνο για τη μεριά του τερματικού, το οποίο διατηρεί ένα στατικό ζεύγος κρυπτογραφικών κλειδιών.

Ο Terminal Authentication αποτελεί το πρώτο στάδιο και ακολουθεί έπειτα το Chip Authentication πρωτόκολλο. Η σύνοψη του εφήμερου δημόσιου κλειδιού του τερματικού παρέχεται από το TA πρωτόκολλο ενώ το ίδιο το εφήμερο κλειδί παρέχεται αργότερα από το CA πρωτόκολλο και πραγματοποιείται η επιβεβαίωση. Κατά αυτόν τον τρόπο τα 2 πρωτόκολλα αλληλοσυμπληρώνονται.



Εικόνα 34-Αυθεντικοποίηση με TA

Αδυναμίες του TA

Το πρόβλημα μπορεί να προκύψει όταν ένα τερματικό κλαπεί όπου πρακτικά τα δικαιώματα πρόσβασής του παραμένουν ακόμη και μετά τη λήξη της περιόδου ισχύος του πιστοποιητικού του δεδομένου ότι δεν ενημερώνει τα MRTDs για την πραγματική ημερομηνία και ώρα. Δεδομένου βέβαια ότι ο κάτοχος της κάρτας κάποια στιγμή θα

αναγκαστεί να την παραδώσει σε ένα έγκυρο τερματικό κάποια στιγμή θα ενημερωθεί ως προς την σωστή ημερομηνία. Αυτό ευνοεί όσους χρησιμοποιούν συχνά την κάρτα τους ενώ παραμένουν περισσότερο ευάλωτοι αυτοί που χρησιμοποιούν την κάρτα τους περιστασιακά [97].

Σύμφωνα με τα όσα αναφέρθηκαν για τους τύπους τερματικών κατά τον BSI, τα τερματικά που έχουν πρόσβαση στα βιομετρικά δεδομένα είναι μόνο όσα αυθεντικοποιούνται ως Σύστημα Επιθεώρησης (Inspection system, IS). Αυτό σημαίνει ότι άλλου είδους εφαρμογές πέρα από αυτή της διασυνοριακής επιθεώρησης δεν θα έχουν πρόσβαση σε τέτοια δεδομένα κάτι που περιορίζει τις προσφερόμενες υπηρεσίες της κάρτας. Θεωρητικά για να έχει κάποιος πρόσβαση στα βιομετρικά θα πρέπει να αιτηθεί για IS πιστοποιητικό ή DV πιστοποιητικό από τη χώρα έκδοσης της κάρτας. Στην πράξη λόγω της «ρηχής» PKI ιεραρχίας η τεράστια επιβάρυνση της DV οντότητας για την έκδοση πιστοποιητικών για κάθε τερματικό που σχετίζεται με μια νέα εφαρμογή θα είναι απαγορευτική. Για παράδειγμα για υπηρεσίες από το σπίτι με τη χρήση της κάρτας θα απαιτείται τερματικό για κάθε Η/Υ. Δυστυχώς δεν μπορούν να αυξηθούν τα επίπεδα ιεραρχίας της «ρηχής» PKI υποδομής καθώς κάτι τέτοιο θα είχε ως αποτέλεσμα μεγαλύτερες καθυστερήσεις απόκρισης από το τσιπ της κάρτας καθώς αυξάνεται το πλήθος των πιστοποιητικών που ως μέρος της αλυσίδας οφείλει να επιβεβαιώσει.

Ως μια λύση στο παραπάνω πρόβλημα οι συγγραφείς του [97] προτείνουν την on-line αυθεντικοποίηση τερματικού δεδομένου ότι ακόμα και τα φορητά συστήματα επιθεώρησης μπορούν να συνδέονται στο δίκτυο οπουδήποτε μέσω GPRS των συστημάτων κινητής τηλεφωνίας. Σύμφωνα με το σκεπτικό, υπάρχει μια αρχή για κάθε χώρα (back office) που αποθηκεύει για κάθε αρχή δικαιοδοσίας μιας εφαρμογής (που επιθυμεί να αναγνωρίζει), τα δικαιώματα πρόσβασης για τη συγκεκριμένη εφαρμογή. Επιπλέον η αρχή αυτή αποθηκεύει τα δημόσια κλειδιά των τερματικών που έχουν ανακληθεί. Το πρώτο στάδιο της διαδικασίας της on-line αυθεντικοποίησης είναι όμοιο με του Terminal Authentication μηχανισμού. Αφού λοιπόν το τερματικό αποστείλει το πιστοποιητικό της αρχής δικαιοδοσίας της εφαρμογής και αυθεντικοποιηθεί στο τσιπ ακολούθως σε δεύτερη φάση το τσιπ εγκαθιδρύει ένα αυθεντικοποιημένο κανάλι με το back office του κράτους έκδοσης χρησιμοποιώντας σχετικό πιστοποιητικό της χώρας που εμπεριέχεται στο τσιπ κατά τη διαδικασία προσωποποίησης του χρήστη (personalization). Μέσω του καναλιού αυτού το τσιπ προωθεί το πιστοποιητικό της αρχής δικαιοδοσίας της εφαρμογής που έλαβε από το τερματικό. Η αρχή της χώρας στο back office αναλαμβάνει να επιβεβαιώσει το πιστοποιητικό αυτό της εφαρμογής να ανακτήσει τα σχετικά δικαιώματα πρόσβασης και τέλος να τα αποστείλει στο τσιπ της κάρτας.

5.3.5.6. Restricted Identification (RI)

Ο μηχανισμός περιορισμένης αναγνώρισης (Restricted Identification, RI) μπορεί να χρησιμοποιηθεί αφού έχουν προηγηθεί επιτυχώς οι Chip και Terminal Authentication. Πρόκειται για έναν μηχανισμό ο οποίος εξυπηρετεί την μοναδική αναγνώριση του MRTD μέσα σε έναν συγκεκριμένο τομέα και χρησιμοποιείται για την επαναγνώριση των MRTDs

μέσα στα όρια ενός τομέα (ομάδα τερματικών τα οποία βρίσκονται υπό την ευθύνη ενός συγκεκριμένου οργανισμού ή φορέα δηλαδή πιστοποιούνται από έναν συγκεκριμένο Document Verifier σύμφωνα με τα όσα περιγράφηκαν για την PKI δομή) αλλά και την τυχών ανάκλησή τους.

Ένας τομέας (Terminal Sector) ορίζεται για κάθε τερματικό μέσα στο σχετικό Terminal Certificate που εκδίδεται. Αρμόδιος για την εκχώρηση τομέων είναι ο Document Verifier. Για κάθε Terminal Sector αντιστοιχεί ένα δημόσιο κλειδί του τομέα (PKSector). Το κλειδί αυτό μπορεί να σχηματίζεται με ένα μυστικό ιδιωτικό κλειδί τομέα, οπότε τότε είναι υπολογιστικά αδύνατη η συσχέτιση αναγνωριστικών με άλλους τομείς και συνεπώς η «παρακολούθηση κίνησης» (tracing) των MRTDs. Ενδέχεται όμως το δημόσιο κλειδί τομέα να σχηματίζεται ως ζεύγος κλειδιών ώστε το ιδιωτικό μέρος να χρησιμοποιείται για την ανάκληση MRTDs ανά τομέα. Ανάλογα με τον τρόπο δημιουργίας των τομέων μια έμπιστη τρίτη οντότητα ενδέχεται να είναι σε θέση να συσχετίσει τα αναγνωριστικά μεταξύ των τομέων.

Με τον RI το ίδιο το MRTD τσιπ δημιουργεί το μοναδικό αναγνωριστικό του (I c 10 r) για τον συγκεκριμένο τομέα όπως παρουσιάζεται στο Σχήμα 31. Τα αναγνωριστικά αυτά δημιουργούνται με hash επί ενός συγκεκριμένου μοναδικού μυστικού κλειδιού αναγνώρισης (SKID) που κατέχει το τσιπ εκ των προτέρων (κατά τη φάση εγγραφής του/(pre)-personalization) και σε σχέση με το δημόσιο κλειδί του εκάστοτε τομέα (PKSector). Το ιδιωτικό κλειδί αναγνώρισης SKID αποθηκεύεται στο τσιπ ενώ το δημόσιο μέρος του σε βάση δεδομένων όπου μαζί με υπόλοιπα δεδομένα προσδιορίζεται ο κάτοχος του MRTD.

5.3.6. Privacy-Enhanced PKI tokens

Υλοποιούνται σε προϊόντα όπως το U-Prove της Microsoft και το Idemix της IBM και παρέχουν κρυπτογραφικές τεχνικές που μπορούν να:

- Αποφύγουν τη συνδεσιμότητα μεταξύ των αναγνωριστικών που εμφανίζονται σε διάφορες υπηρεσίες ακόμη κι αν οι πάροχοι των υπηρεσιών και η Αρχή Πιστοποίησης στη συνέχεια μοιράζονται τα δεδομένα (collude). Με την τεχνική αυτή είναι δυνατή η εξασφάλιση της ανωνυμίας του χρήστη σε κάθε πάροχο υπηρεσιών μέσω της χρήσης διαφορετικών ψευδωνύμων. Έτσι είναι εφικτή η επιβεβαίωση των ισχυρισμών του κατά τη χρήση της ΚΠ σε συναλλαγές, χωρίς όμως μπορούν να συνδέονται και να αποκαλύπτονται περιττές πληροφορίες που πιθανά προκύπτουν μέσω της συσχέτισης με άλλες συναλλαγές, καθώς απαγορεύεται η αποκάλυψη των ψευδονύμων που χρησιμοποιούνται στις επιμέρους συναλλαγές.
- Παρέχουν, πιο εκτεταμένα, τις λειτουργίες επιλεκτικής αποκάλυψης.
- Ενισχύουν τα limited show πρωτόκολλα (π.χ. για e-cash και τραπεζικές συναλλαγές), όπου ο χρήστης μπορεί να προσπαθήσει να αποδείξει τον ισχυρισμό του για ορθή χρήση της συναλλαγής μόνο έναν μικρό περιορισμένο αριθμό φορών.
- Παρέχουν δυνατότητα για διεθνή ανάκληση των πιστοποιητικών που κατέχονται από ένα χρήστη, διατηρώντας παράλληλα τη μη διασύνδεσή τους (unlinkability).

Στην ανάλυση αυτή, βέβαια, γίνεται η λογική υπόθεση ότι ούτε η εκδούσα αρχή, ούτε ο ελεγκτής μπορεί να προσθέσει αυθαίρετες καταχωρήσεις στο CRL, γιατί αυτό θα τους επέτρεπε να εφαρμόσουν brute-force επιθέσεις με συνδυασμούς από προσωρινά ανακληθέντα πιστοποιητικά. συνδυασμούς των πιστοποιητικών και στη συνέχεια προσπαθεί να ελέγξει τους άλλους. Οφείλουμε, πάντως, να αναγνωρίσουμε ότι είναι σχετικά ασφαλής η υπόθεσή μας, δεδομένου ότι τα περισσότερα CRL ελέγχονται από αρκετά αυστηρές διαδικασίες που θα καθιστούσαν αδύνατη αυτήν την επίθεση.

Ως εκ τούτου, παρότι ακόμη δεν έχουν υιοθετηθεί και αξιοποιηθεί σε ικανοποιητικό βαθμό, εντούτοις, οι privacy-enhanced PKI τεχνολογίες έχουν σημαντικές δυνατότητες για την ενίσχυση της ιδιωτικότητας στις υφιστάμενες eID εφαρμογές.

5.4. Σύνοψη Κεφαλαίου

Στο κεφάλαιο αυτό επιχειρήσαμε μια συνοπτική παρουσίαση των τεχνολογιών που έχουν αναπτυχθεί για την εξασφάλιση της ασφάλειας και της ιδιωτικότητας κατά τη χρήση εργαλείων ηλεκτρονικής ταυτοποίησης, όπως η Ελληνική ΚΠ. Οι απειλές ιδιωτικότητας και ασφάλειας, είναι εκείνες που προσδιορίζουν τα σημεία προσοχής και αδυναμιών και τους κινδύνους που μπορούν να προκύψουν και τελικά είναι εκείνες που μας οδηγούν στην εφαρμογή τεχνικών ασφάλειας και ιδιωτικότητας. Με τον τρόπο αυτό, προέκυψε ένα σύνολο απαιτήσεων ασφάλειας και ένα ακόμη σύνολο τεχνολογικών λύσεων που μπορούν να εφαρμοσθούν για να αντιμετωπίσουν αυτές τις απειλές. Ωστόσο, πάντοτε κάποιες απειλές θα παραμένουν, παρά τις λύσεις που εφαρμόζουμε και στο σημείο αυτό απαιτείται η αξιολόγηση της βαρύτητας των απειλών σύμφωνα με τα τις ιδιαιτερότητες τις κάθε περίπτωσης και των επιπτώσεων αυτών στην εφαρμοζόμενη λύση και πολύ δε περισσότερο η στάθμιση των παραγόντων αυτών για την όσο το δυνατόν ασφαλέστερη λύση.

Το κεφάλαιο αυτό ορίζει το πλαίσιο ασφάλειας που πρέπει να πληροί μια ΚΠ, τόσο ως προς το επίπεδο των απειλών ασφάλειας και ιδιωτικότητας, όσο και ως προς το επίπεδο των απαιτήσεων και τεχνικών ασφάλειας και ιδιώτικοτητας που πρέπει να εφαρμόζονται, ώστε στο επόμενο κεφάλαιο, που αποτελεί τη μελέτη εφαρμογής της Ελληνικής ΚΠ, όπου εκεί πλέον συγκεκριμένα θα εντοπίσουμε τις απειλές και τα προβλήματα και θα προσπαθήσουμε να δώσουμε τη βέλτιστη σχεδιαστική επιλογή, υπό το πρίσμα της στάθμισης των επιμέρους παραγόντων ασφάλειας και λειτουργικότητας.

6. ΕΦΑΡΜΟΓΗ ΤΗΣ ΚΑΡΤΑΣ ΠΟΛΙΤΗ

Προκειμένου να καταλήξουμε στην κατάλληλη επιλογή για την εφαρμογή της ΚΠ στην Ελλάδα, πρέπει πρώτα να ορίσουμε ευκρινώς τις απαιτήσεις στις οποίες πρέπει να ανταποκρίνεται η ΚΠ. Οι απαιτήσεις αυτές μπορούν να διακριθούν σε δύο βασικές κατηγορίες, τις λειτουργικές και τις τεχνικές απαιτήσεις. Οι λειτουργικές απαιτήσεις αφορούν στη χρήση της ΚΠ και στις λειτουργίες που θέλουμε να υποστηρίζει. Οι τεχνικές απαιτήσεις αφορούν στην ασφάλεια και διαλειτουργικότητα και τη συμμόρφωση με τα διεθνή πρότυπα και προδιαγραφές.

Αξίζει να σημειώσουμε στο σημείο αυτό, ότι η παρουσίαση των προηγούμενων κεφαλαίων ουσιαστικά αποσκοπούσε στην ανάδειξη των κρίσιμων ζητημάτων, ώστε να οδηγηθούμε στην όσο το δυνατόν καλύτερη και αποδοτικότερη σχεδιαστική επιλογή. Για το λόγο αυτό, είναι καλό να μελετήσουμε το συγκεκριμένο κεφάλαιο, ανασύροντας την πληροφορία που καταγράφηκε προηγουμένως και τα ανοιχτά ζητήματα που προέκυψαν από τη μελέτη της βιβλιογραφίας.

Η υφιστάμενη κατάσταση στην Ελλάδα έχει να επιδείξει κυρίως την Κυβερνητική Πύλη «Ερμής» και το Ελληνικό Πλαίσιο Διαλειτουργικότητας (e-Gif) στον τομέα της ηλεκτρονικής διακυβέρνησης στην Ελλάδα και την εφαρμογή της Ελληνικής ΚΠ. Οι δύο αυτές υποδομές/δράσεις βασίζονται ακριβώς στην αξιοποίηση της διεθνούς πρακτικής που καταδεικνύει δύο βασικούς τρόπους επίτευξης διαλειτουργικότητας μεταξύ των συστημάτων της Δημόσιας Διοίκησης, ο ένας αφορά στη δημιουργία κεντρικών κυβερνητικών πυλών που θα παρέχουν στους πολίτες, συγκεντρωμένες όλες τις απαραίτητες πληροφορίες και υπηρεσίες της Δημόσιας Διοίκησης και ο άλλος, ορίζει την κατάρτιση Πλαισίων Διαλειτουργικότητας που θέτουν τις προδιαγραφές για την επίτευξη της διαλειτουργικότητας και μιας ολοκληρωμένης ηλεκτρονικής διακυβέρνησης (E-Government Interoperability Framework – Ελληνικό Πλαίσιο Διαλειτουργικότητας Ηλεκτρονικής Διακυβέρνησης - ΕΠΔΗΔ).

Η ΚΠ για την Ελλάδα θα αποτελέσει τον τρόπο φυσικής και ψηφιακής ταυτοποίησης του πολίτη, τόσο εντός όσο και εκτός συνόρων.

Ειδικότερα οι κύριες απαιτήσεις για την σχεδιαστική λύση αποκρυσταλλώνονται στα ακόλουθα:

1. Αντικατάσταση του Αστυνομικού Δελτίου Ταυτότητας
2. Χρήση ως ταξιδιωτικό έγγραφο
3. Χρήση για υπηρεσίες ηλεκτρονικής διακυβέρνησης
4. Χρήση για ψηφιακή αυθεντικοποίηση
5. Δυνατότητα ψηφιακής υπογραφής

6. Προστασία της ιδιωτικότητας του κατόχου
7. Ασφάλεια στις συναλλαγές
8. Αξιοποίηση υφιστάμενων υποδομών και εξασφάλιση διαλειτουργικότητας με υφιστάμενες εφαρμογές και διαδικασίες
9. Συμμόρφωση με διεθνή πρότυπα
10. Διαλειτουργικότητα με Ευρωπαϊκά συστήματα
11. Εναρμόνιση της λειτουργικότητας της ΚΠ με την κουλτούρα της Ελληνικής κοινωνίας

6.1. Λειτουργικές Απαιτήσεις και Απαιτήσεις Ασφάλειας

6.1.1. Αντικατάσταση του Αστυνομικού Δελτίου Ταυτότητας

Ο πολίτης πρέπει να μπορεί να χρησιμοποιήσει την ΚΠ, όπως ακριβώς χρησιμοποιεί την έντυπη αστυνομική του ταυτότητα. Έτσι, η ΚΠ θα αποτελεί το δημόσιο εκείνο έγγραφο που ταυτοποιεί και προσδιορίζει τον πολίτη στις συναλλαγές που απαιτούν φυσική παρουσία και φυσικό έλεγχο. Θα χρησιμοποιείται, επίσης, ως αποδεικτικό στοιχείο ταυτότητας από υπηρεσίες ασφαλείας και ελέγχου (π.χ. ΕΛ.ΑΣ.).

Κατά συνέπεια, η ΚΠ θα πρέπει να είναι ικανή να προσδιορίζει τον κάτοχό της κατά την επίδειξή της. Ως εκ τούτου, πρέπει να περιέχει ένα σύνολο πεδίων που θα αναγράφεται στο εξωτερικό τμήμα της κάρτας και θα περιλαμβάνει πληροφορία που προσδιορίζει τον πολίτη, η οποία μέχρι σήμερα ήταν γνωστή ως στοιχεία ταυτότητας. Επιπλέον, θα πρέπει να περιλαμβάνει μεθόδους που να καθιστούν εφικτή την φυσική αναγνώριση του πολίτη. Στα ΑΔΤ μέχρι σήμερα, για το λόγο αυτό χρησιμοποιείτο η φωτογραφία του πολίτη και η υπογραφή του στην εμπρόσθια όψη της αστυνομικής ταυτότητας και στην πίσω όψη τα επιπλέον στοιχεία ταυτότητας, όπως Ονοματεπώνυμο, όνομα πατρός, μητρός, ημερομηνία και τόπο γέννησης, αριθμό δημοτολογίου κ.α..

Αυτό είναι το πρώτο στοιχείο που πρέπει να κρατήσουμε αναφορικά με τα δεδομένα που είναι απαραίτητα στην ελληνική ΚΠ.

Το κύριο εύρημα από την ανάλυση αυτή είναι ότι απαιτείται κατ' ελάχιστο, η φωτογραφία του κατόχου και το ονοματεπώνυμό του.

6.1.2. Χρήση ως ταξιδιωτικό έγγραφο

Μια άλλη χρήση της ΚΠ αφορά στη χρήση της ως ταξιδιωτικού εγγράφου. Για την εξασφάλιση της συγκεκριμένης δυνατότητας οι επιλογές είναι δύο.

Η πρώτη επιλογή αναφέρεται στη χρήση της εντός ορίων της συνθήκης Schengen ή τρίτων χωρών με τις οποίες έχουν συναφθεί σχετικές συμφωνίες για τη διακίνηση πολιτών. Στην

περίπτωση αυτή, η χρήση της, όπως και τα δεδομένα που περιέχει, συμπίπτει με τη χρήση ως τυπικό δελτίο ταυτότητας.

Η δεύτερη επιλογή ταυτίζεται περισσότερο με τη χρήση του διαβατηρίου. Σε αυτήν την περίπτωση, όπως είναι προφανές, οι λειτουργίες και οι προδιαγραφές των διαβατηρίων πρέπει επίσης να ενσωματωθούν στην ΚΠ.

Η σημαντικότερη διαφορά ανάμεσα στις δύο επιλογές είναι η ενσωμάτωση ή όχι βιομετρικών χαρακτηριστικών, ως αναγνωριστικά της ΚΠ.

Ανεξάρτητα από την επιλογή στην οποία θα καταλήξουμε, η ΚΠ πρέπει να μπορεί να χρησιμοποιηθεί ως μέσο φυσικής ταυτοποίησης στα σημεία διασυνοριακού ελέγχου. Η ΚΠ πρέπει να δίνει τη δυνατότητα στα σημεία διασυνοριακού ελέγχου (αεροδρόμια, λιμάνια κλπ) και στις αρχές ασφαλείας (αστυνομικές αρχές) να ελέγχουν την εγγυρότητα της ΚΠ, να ταυτοποιούν και να πιστοποιούν με βεβαιότητα τον πραγματικό κάτοχο και να διαπιστώνουν την ισχύ της ΚΠ μέσω της ημερομηνίας λήξης, το ονοματεπώνυμο και την ημερομηνία γέννησης του κατόχου. Εξαιτίας, της διασυνοριακής χρήσης της ΚΠ, αυτή πρέπει επίσης να περιλαμβάνει την υπηκοότητα του κατόχου της καθώς και τον κωδικό της χώρας έκδοσης.

Για την επαλήθευση και πιστοποίηση των παραπάνω χαρακτηριστικών πρέπει επιπλέον να εξασφαλίζεται και η συμβατότητα με τις μηχανές αυτόματης ανάγνωσης ταξιδιωτικών εγγράφων (MRTD), όπως ορίζεται σύμφωνα με τα πρότυπα και τις προδιαγραφές του ICAO και να εξασφαλίζεται δυνατότητα πρόσβασης σε αυτές.

6.1.3. Χρήση για ηλεκτρονικές συναλλαγές και Ψηφιακή αυθεντικοποίηση

Παράλληλα με την ανάπτυξη των υπηρεσιών ηλεκτρονικής διακυβέρνησης και την προσφορά στον πολίτη ενός πλήθους δημόσιων υπηρεσιών ηλεκτρονικά, η ανάγκη για αυθεντικοποίση του πολίτη στο νέο ψηφιακό περιβάλλον είναι επιβεβλημένη. Στην κατεύθυνση αυτή η ΚΠ πρέπει να μπορεί να εξασφαλίσει στον κάτοχό της πρόσβαση στις ηλεκτρονικές υπηρεσίες της Δημόσιας Διοίκησης. Η απομακρυσμένη πρόσβαση στις υπηρεσίες μέσω της ΚΠ πρέπει να είναι εφικτή είτε διαδικτυακά από τον χώρο του πολίτη, είτε μέσα από εξουσιοδοτημένα σημεία δημόσιας πρόσβασης (π.χ. ΚΕΠ) προς διευκόλυνση των πολιτών που δεν είναι εξοικειωμένοι με τη χρήση των ΤΠΕ, αλλά έχουν δικαίωμα να απολαμβάνουν τέτοιες υπηρεσίες.

Για τη χρήση και πρόσβαση στα δεδομένα που περιέχονται στην ΚΠ πρέπει να εξασφαλίζεται η ρητή συγκατάθεση του πολίτη και για το λόγο αυτό προτείνεται η απόδοση με την έκδοση της ΚΠ ενός ζεύγους συνθηματικών πρόσβασης (PIN και PUK), ως προσωπικοί αριθμοί ασφαλείας.

Εξαιτίας της χρήσης της ΚΠ σε υπηρεσίες διαδικτύου τα δεδομένα που πρέπει να τηρούνται στην ΚΠ πρέπει να είναι τα απολύτως αναγκαία για τους σκοπούς της εξυπηρέτησης του πολίτη και της ασφαλούς διεκπεραίωσης των συναλλαγών του και ταυτόχρονα, να μην δημιουργούν συσχετίσεις με άλλα προσωπικά στοιχεία του πολίτη. Κατά συνέπεια, τα

επιμέρους συστήματα των εφαρμογών που χρησιμοποιεί ο πολίτης πρέπει να έχουν πρόσβαση αποκλειστικά και μόνο στα δεδομένα εκείνα που απαιτούνται για τη χρήση της εκάστοτε υπηρεσίας και διεκπεραίωση της εκάστοτε συναλλαγής και όχι στο σύνολο της αποθηκευμένης στην κάρτα πληροφορίας. Μάλιστα, για την καλύτερη διασφάλιση αυτής της προϋπόθεσης προτείνεται η επιπλέον συγκατάθεση και ερώτηση του πολίτη για την πρόσβαση της εφαρμογής στο συγκεκριμένο τμήμα των δεδομένων που απαιτείται για τη συναλλαγή. Πιο συγκεκριμένα, αν η ΚΠ χρησιμοποιηθεί για την έκδοση της φορολογικής ενημερότητας του πολίτη, ο πολίτης αρχικά θα εισάγει τον προσωπικό του αριθμό, PIN προκειμένου να αποκτήσει πρόσβαση στην εφαρμογή και να ζητήσει την υπηρεσία που επιθυμεί (έκδοση φορολογικής ενημερότητας) και στη συνέχεια η εφαρμογή προκειμένου να προχωρήσει στην ολοκλήρωση του αιτήματος, πρέπει να γνωρίζει την απαιτούμενη πληροφορία (π.χ. ΑΦΜ) της ΚΠ, για την οποία ο πολίτης επιτρέπει την πρόσβαση της εφαρμογής. Έτσι, στο παράδειγμα που χρησιμοποιήσαμε το taxis θα είχε πρόσβαση μόνο στο ΑΦΜ του πολίτη για την έκδοση της φορολογικής του ενημερότητας.

Στα πλαίσια της ηλεκτρονικής διακυβέρνησης, επιπλέον, προτείνεται η δυνατότητα χρήσης της ψηφιακής υπογραφής και των ψηφιακών πιστοποιητικών. Ο πολίτης στην περίπτωση που επιθυμεί να χρησιμοποιήσει αυτή τη δυνατότητα, πρέπει να μπορεί να υπογράφει ηλεκτρονικά έγγραφα μέσω της ΚΠ. Εξάλλου, η ΚΠ ως έξυπνη κάρτα είναι απολύτως κατάλληλη για χρήση σε υποδομή δημοσίου κλειδιού προσφέροντας τις απαιτούμενες προδιαγραφές για την δημιουργία και χρήση προηγμένης ηλεκτρονικής υπογραφής. Η ΚΠ μπορεί να αποθηκεύσει με ασφάλεια τα ψηφιακά πιστοποιητικά και τα ιδιωτικά κλειδιά προστατεύοντας τα από την δυνατότητα εξαγωγής τους.

Ως προς την αξιοποίηση της δυνατότητας της ψηφιακής υπογραφής, δεδομένου ότι, αυτή έχει ισοδύναμη νομική ισχύ με την χειρόγραφη, όπως προέκυψε κατά τη μελέτη και ανάλυση του θεσμικού πλαισίου, η ασφαλής χρήση της πρέπει να αντιμετωπισθεί με ιδιαίτερη προσοχή. Για το λόγο αυτό, προτείνεται η χρήση διακριτού αριθμού PIN για την χρήση της ψηφιακής υπογραφής.

Η ΚΠ εισιτήριο για τον ψηφιακό κόσμο.

Η ΚΠ μπορεί να λειτουργήσει ως μοναδική προϋπόθεση για τις ηλεκτρονικές συναλλαγές με τον δημόσιο τομέα, απαλλάσσοντας και τα δύο μέρη από διοικητικά βάρη και περιττή γραφειοκρατία.

Συνοψίζοντας τα παραπάνω, η ΚΠ πρέπει να περιέχει την ελάχιστη δυνατή πληροφορία και να εξασφαλίζει την εξουσιοδοτημένη πρόσβαση αποκλειστικά και μόνο στο τμήμα της πληροφορίας που απαιτείται για μια συγκεκριμένη συναλλαγή.

Η υιοθέτηση της ΚΠ αποτελεί βασική συνιστώσα στην προοπτική ηλεκτρονικής διακυβέρνησης και στην ανάπτυξη και καθιέρωση των υπηρεσιών ηλεκτρονικής διακυβέρνησης.

Οι ηλεκτρονικές υπογραφές επιπλέον μπορούν να διευκολύνουν περαιτέρω τις δυνατότητες της ηλεκτρονικής διακυβέρνησης, εντούτοις, πρέπει να αντιμετωπίζονται με ιδιαίτερη προσοχή.

6.1.4. Διασφάλιση της ιδιωτικότητας και ασφάλειας του πολίτη

Όπως αναφέραμε και προηγουμένως η έκδοση και προσωποποίηση της ΚΠ θα συνοδεύεται παράλληλα από την έκδοση του προσωπικού αριθμού ασφαλείας (PIN - PUK). Με τη χρήση του PIN θα επιβεβαιώνεται σε πρώτο επίπεδο ότι ο χρήστης είναι ο πραγματικός κάτοχος της ΚΠ, κατά τη διάρκεια μιας συναλλαγής. Η διαδικασία αυθεντικοποίησης του χρήστη θα περιλαμβάνει την εισαγωγή της ΚΠ στην πιστοποιημένη συσκευή ανάγνωσης και έπειτα θα απαιτείται η εισαγωγή ενός έγκυρου PIN. Η ανάγνωση της ΚΠ θα γίνεται μόνο από πιστοποιημένες ασφαλείς συσκευές ανάγνωσης (αναγνώστες), οι οποίες θα βρίσκονται σε δημόσιες υπηρεσίες και σημεία εξυπηρέτησης (π.χ. ΚΕΠ), ή από το χώρο του χρήστη εφόσον αυτός έχει προμηθευτεί πιστοποιημένο αναγνώστη. Με την εισαγωγή του PIN εξασφαλίζεται ρητά και η συγκατάθεση του χρήστη για πρόσβαση στην πληροφορία της ΚΠ, προκειμένου να κάνει χρήση κάποιας υπηρεσίας.

Γιατί όμως η χρήση της ΚΠ κάνει πιο ασφαλή τον πολίτη σχετικά με τη χρήση των προσωπικών του δεδομένων, κατά την συμμετοχή του σε ηλεκτρονικές συναλλαγές;

Η απάντηση είναι σχετικά απλή. Ωστόσο, προϋποθέτει και από τον χρήστη την ορθή και κατάλληλη χρήση της ΚΠ, αλλά και την κατανόηση της αξίας των προσωπικών του δεδομένων.

Ο χρήστης μέσω της ΚΠ θα έχει τον πλήρη έλεγχο για τα στοιχεία που θα χρησιμοποιηθούν από την εφαρμογή. Αφενός πρέπει πρώτα να χρησιμοποιήσει την κάρτα του και να εισάγει το σχετικό PIN για την υπηρεσία που επιθυμεί και μέσω του δικτυακού τόπου που εμπιστεύεται. Γεγονός που διασφαλίζει τη ρητή συγκατάθεσή του για την πρόσβαση στην ΚΠ και δεν περιορίζεται σε απλή επίδειξη της ταυτότητάς του ή κάποιων δικαιολογητικών ή την απλή χρήση συνθηματικών για τον ψηφιακό κόσμο. Απαιτεί θα λέγαμε και τα δύο, άρα κάνει πιο δύσκολη τη μη εξουσιοδοτημένη πρόσβαση.

Αφετέρου, ο πολίτης έχει πλήρη και απόλυτο έλεγχο των προσωπικών του δεδομένων, καθώς η ΚΠ θα περιέχει την ελάχιστη δυνατή πληροφορία, αλλά και θα πρέπει να εξασφαλίζει πρόσβαση σε ακόμη μικρότερο τμήμα αυτής. Δηλαδή, δεν θα επιτρέπεται η πρόσβαση στην πληροφορία της ΚΠ, χωρίς τη ρητή συγκατάθεση του πολίτη, αλλά παράλληλα, δεν θα επιτρέπεται πρόσβαση σε μεγαλύτερο τμήμα της πληροφορίας από εκείνο που απαιτείται για την χρήση ή ολοκλήρωση κάποιας συναλλαγής. Αν κάτι τέτοιο είναι απαραίτητο, ο χρήστης πρέπει να ερωτάται ρητώς και να επιτρέπεται επιπλέον πρόσβαση μόνο έπειτα από τη ρητώς εκπεφρασμένη συμφωνία του. Στην προηγούμενη ενότητα αναδείξαμε σχετικά το παράδειγμα της φορολογικής ενημερότητας και της χρήσης του ΑΦΜ.

Επιπλέον, είναι σαφές ότι δεν θα απαιτείται από τον πολίτη κανένα άλλο δεδομένο ή πληροφορία για την αυθεντικοποίησή του, προκειμένου να κάνει χρήση μιας συναλλαγής, παρά μόνο η ίδια η ΚΠ.

Ωστόσο, η χρήση της ΚΠ δημιουργεί προϋποθέσεις ασφάλειας και στο άλλο μέρος της συναλλαγής. Μέσω της χρήσης της ΚΠ, επομένως, ο πάροχος της ηλεκτρονικής υπηρεσίας που επιθυμεί να χρησιμοποιήσει ο χρήστης, θα είναι βέβαιος για την αυθεντικότητα του χρήστη και την αυθεντικότητα της συναλλαγής, καθώς η ΚΠ πιστοποιεί επαρκώς την ταυτότητα του συναλλασσόμενου.

Όπως είναι κατανοητό, η ΚΠ πρέπει να υπακούει στα διεθνή πρότυπα και τις Ευρωπαϊκές προδιαγραφές για την ασφάλεια.

Με βάση τα παραπάνω, κατανοούμε ότι απαιτείται μια χρυσή τομή για την πληροφορία που πρέπει να περιέχεται στην ΚΠ. Η σχεδιαστική λύση πρέπει να ισορροπεί ανάμεσα στην διασφάλιση της ιδιωτικότητας του πολίτη με χρήση της όσο το δυνατόν ελάχιστης πληροφορίας και στη διασφάλιση της ασφάλειας των συναλλαγών, καθώς για την ολοκλήρωση του απαιτείται, πάντως, κάποια πληροφορία.

Η εμπιστοσύνη του πολίτη στην ΚΠ και στα συστήματα που τη χρησιμοποιούν είναι καταλυτική για την επιτυχία του εγχειρήματος.

Η πιστοποίηση των ΚΠ και των αναγνωστών τους, και οι πολιτικές ασφάλειας για την ανάπτυξη και συντήρηση των συστημάτων είναι κρίσιμα ζητήματα για την επιλογή της βέλτιστης σχεδιαστικής επιλογής.

6.1.5. Διαλειτουργικότητα και Εναρμόνιση

Η επιλεγόμενη λύση ΚΠ πρέπει να πληροί τις προϋποθέσεις διαλειτουργικότητας με κατασκευαστές καρτών, αναγνωστών, συστημάτων παροχής ηλεκτρονικών υπηρεσιών, καθώς και να εξασφαλίζει τη διαλειτουργικότητα της λύσης με τις υφιστάμενες υποδομές.

Σε ένα άλλο επίπεδο, πρέπει ακόμη να σημειωθεί, ότι η διασφάλιση της διαλειτουργικότητας της ΚΠ είναι απολύτως κρίσιμη και αναγκαία προκειμένου να εξασφαλίσει πιθανά δυνατότητες της ΚΠ για χρήση σε ένα ευρωπαϊκό ψηφιακό περιβάλλον, που δεν μπορούμε, ίσως, να αναγνωρίσουμε ευκρινώς σήμερα. Εξάλλου, όπως αναλύσαμε και στη δεύτερη ενότητα του 4ου Κεφαλαίου, η ΕΕ έχει ήδη υλοποιήσει ένα σύνολο έργων (με σημαντικότερο το STORK) για τη διαλειτουργικότητα των εθνικών ΚΠ με συστήματα ΚΠ άλλων χωρών έχοντα εκπεφρασμένη τη βούλησή της για ενιαία ευρωπαϊκή ηλεκτρονική ταυτότητα. Πολλά σχετικά έργα είναι ακόμη εν εξελίξει. Στην κατεύθυνση αυτή, η ΚΠ πρέπει να μπορεί να χρησιμοποιηθεί εκτός εθνικών συνόρων, δυνητικά και από ευρωπαϊκές ηλεκτρονικές υπηρεσίες, πέραν της χρήσης της ως ταξιδιωτικό έγγραφο, που περιγράψαμε προηγουμένως.

Σε κάθε περίπτωση η ΚΠ πρέπει να συμμορφώνεται με τα διεθνή πρότυπα διαλειτουργικότητας.

Εντούτοις, πρέπει να αναγνωρίσουμε ότι δεδομένου ότι τα πρότυπα και η νομοθεσία δεν επιβάλλουν τη διαλειτουργικότητα, δεν είμαστε πολύ κοντά στην εξασφάλιση μιας ενιαίας ΚΠ για όλες τις χώρες σε επίπεδο ΕΕ.

6.1.6. Εναρμόνιση με εθνική κουλτούρα

Η εναρμόνιση με την εθνική κουλτούρα και η αντίληψη του κόσμου είναι ίσως οι πιο σημαντικοί παράγοντες για την επιτυχημένη εφαρμογή της ΚΠ στην Ελλάδα. Η κάθε σχεδιαστική επιλογή πρέπει να λαμβάνει σοβαρά υπόψη τα κεντρικά σημεία στην αντίληψη του Έλληνα πολίτη, καθώς και να αναγνώσει και αντιμετωπίσει τα στοιχεία που του προκαλούν ανησυχία. Η αντίσταση των πολιτών στην εφαρμογή της ΚΠ, καθώς και οι πιθανές αντιδράσεις μπορεί να γίνουν κρίσιμοι ανασταλτικοί παράγοντες και μπορούν να επηρεάσουν σημαντικά την επιτυχία του εγχειρήματος.

Είναι ενδεικτικό, ότι σύμφωνα με τη διαβούλευση που πραγματοποιήθηκε το προηγούμενο διάστημα τα περισσότερα σχόλια ήταν αρνητικά. Ειδικότερα, από τα 1400 περίπου σχόλια της διαβούλευσης, το 60% των σχολίων αποδοκίμαζαν το ενδεχόμενο της εφαρμογής της ΚΠ. Τα πιο συχνά σημεία ανησυχίας σχετίζονταν με την παραβίαση προσωπικών δεδομένων και τους φόβους των πολιτών για το ενδεχόμενο «ηλεκτρονικό φακέλωμα» και τη δυσπιστία των πολιτών απέναντι στη συσσώρευση της πληροφορίας σε κεντρικό και τον τρόπο διαχείρισής της ακόμη και από το κράτος. Η ελλιπής ενημέρωση από την πολιτεία σχετικά με την χρήση και λειτουργία της ΚΠ είχαν σημαντική επίδραση στη διαμόρφωση του αρνητικού κλίματος. Το αποτέλεσμα της διαβούλευσης αξιολογούσε την υλοποίηση της ΚΠ ως μη απαραίτητη και αναποτελεσματική.

Εξάλλου, η ανησυχία της ελληνικής κοινής γνώμης για ζητήματα που αφορούν στην προστασία προσωπικών δεδομένων και την διασφάλιση της ιδιωτικότητας του πολίτη.

Επιπλέον, λόγοι θρησκευτικής συνείδησης είναι αρκετά σημαντικοί για τη διαμόρφωση της κοινής γνώμης και η σχέση Κράτους-Εκκλησίας ενισχύει ακόμη περισσότερο το διαβούλευσης για την ΚΠ υπήρξε έντονη ανησυχία για τον αριθμό «666», Αυτό με τεχνικούς όρους μεταφράζεται σε μη χρήση των προτύπων UPC-A (11+1), EAN13 (12+1 ψηφία) και της Luhn formula, αλλά και του γραμμωτού κώδικα(barcode).

Επομένως, η χρήση συγκεκριμένων τεχνολογικών μεθόδων μπορούν να επηρεάσουν πολύ σημαντικά τη διείσδυση της ΚΠ στην κοινωνία. Εκτιμούμε, ωστόσο, ότι κάποιες τεχνολογικές λύσεις δεν απαιτείται να υλοποιηθούν στην Ελληνική ΚΠ, καθώς παρότι μπορεί να μην συμμεριζόμαστε την ανησυχία και τις αιτιάσεις των πολιτών, ο κίνδυνος αντίδρασης από την εφαρμογής τους θα είναι μεγαλύτερος από τον πιθανό κίνδυνο της μη εφαρμογής τους. Εξάλλου, τα πρότυπα αυτά δεν αποτελούν τεχνολογικό μονόδρομο για την υλοποίηση της ΚΠ. Τουναντίον, θα μπορούσαμε να χρησιμοποιήσουμε για την παραγωγή του αριθμού εντύπου της ΚΠ, 9ψηφιο αλφαριθμητικό με αξιοποίηση του mod10 731731 του ICAO για την παραγωγή του τελευταίου ψηφίου.

Επιπλέον, το μοναδικό αναγνωριστικό ως στοιχείο της ΚΠ που μπορεί να προσδιορίζει μονοσήμαντα τον πολίτη είναι σχεδόν απαγορευτικό για την αντίληψη της ελληνικής κοινωνίας. Με δυσκολία ακόμη θα μπορούσε να γίνει αποδεκτή η χρήση βιομετρικών χαρακτηριστικών.

Είναι σαφές ότι η ελληνική κοινωνία είναι ιδιαίτερα ευαίσθητη με την έννοια της ελευθερίας και το δικαίωμα της ιδιωτικότητας. Για το λόγο αυτό, η προτεινόμενη σχεδιαστική λύση πρέπει να προσμετρήσει τις ανησυχίες για την καταστρατήγηση θεμελιωδών δικαιωμάτων των πολιτών, καθώς επίσης και τους κινδύνους που μπορούν οι αντιλήψεις αυτές να αποτελέσουν για την εφαρμογή της ΚΠ στην Ελλάδα.

Η υποχρεωτική εφαρμογή της ΚΠ δεν θα οδηγήσει απαραίτητα σε επιτυχή υιοθέτησή της από την κοινωνία, που μπορεί σταδιακά να την απαξιώσει. Επομένως, είναι επιθυμητό, τόσο επικοινωνιακά, όσο και ουσιαστικά, τέτοιες ανησυχίες να καμφθούν.

Η βέλτιστη λύση είναι εκείνη που λαμβάνει υπόψη τις κοινωνικές ανάγκες.

6.2. Περιγραφή της ΚΠ

Αποκρυσταλλώνοντας τα συμπεράσματα από τις απαιτήσεις που πρέπει να πληροί η ΚΠ μπορούμε να καταλήξουμε στο σύνολο των χαρακτηριστικών, τα οποία η ΚΠ πρέπει να περιλαμβάνει.

Η ΚΠ για την Ελλάδα θα αποτελέσει τον τρόπο φυσικής και ψηφιακής ταυτοποίησης και αυθεντικοποίησης του πολίτη, τόσο εντός όσο και εκτός συνόρων. Επομένως, πρέπει να συμμορφώνεται με το πρότυπο CEN/TS 15480 ECC, Part 1&2, για την Ευρωπαϊκή ΚΠ (ECC) και με τους κοινοτικούς κανονισμούς ΕΚ 2252/2004 [26] και 444/2009 [27], εφόσον αποτελεί ταξιδιωτικό έγγραφο, καθώς και την προδιαγραφή ICAO Doc 9303 [87] [88] για τα ταξιδιωτικά έγγραφα.

Λαμβάνοντας, επιπλέον, υπόψη τη χρήση της ΚΠ ως εργαλείο ψηφιακής αυθεντικοποίησης και πρόσβασης σε υπηρεσίες ηλεκτρονικής διακυβέρνησης, καθώς και τις λειτουργίες ψηφιακής υπογραφής εγγράφων προκύπτει ένα σύνολο υποχρεώσεων για τα χαρακτηριστικά που πρέπει να φέρει η ΚΠ.

Σταθμίζοντας, κατά συνέπεια, τη λειτουργικότητα της ΚΠ, την επίδραση της χρήσης ή μη κάποιων δεδομένων για την ικανοποίηση των απαιτήσεων, και το δικαίωμα του πολίτη στην ιδιωτικότητα και στην ασφάλεια κατά τη χρήση της ΚΠ, οδηγούμαστε στην κατάλληλη επιλογή για τα δεδομένα που πρέπει να συμπεριληφθούν στην Ελληνική ΚΠ.

6.2.1. Δεδομένα της ΚΠ

Σε συνδυασμό λοιπόν με τις απαιτήσεις που αναλύσαμε στην προηγούμενη ενότητα προτείνεται.

Στην εμπρόσθια όψη της κάρτας σύμφωνα με τα διεθνή πρότυπα, αλλά και προσπαθώντας να καλύψουμε την απαίτηση για φυσική ταυτοποίηση θα περιλαμβάνεται

1. Εθνόσημο
2. Ελληνική Δημοκρατία –Υπουργείο Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης, ως ο φορέας έκδοσης της ΚΠ
3. Φωτογραφία κατόχου
4. Ιδιόχειρη υπογραφή
5. Προσωπικά Δεδομένα Κατόχου

Στο πίσω μέρος της ΚΠ θα αναγράφεται μόνο η ημερομηνία έκδοσης της ΚΠ (η εκδούσα αρχή δεν φαίνεται να είναι απαραίτητη πληροφορία). Το πίσω μέρος θα φέρει, επίσης, μια περιοχή αυτόματης ανάγνωσης (MRZ), η οποία θα εμπεριέχει και τα παραπάνω δεδομένα.

Στο τσιπ μπορούν προαιρετικά να εγγράφονται δεδομένα κυρίως για περιπτώσεις έκτακτης ανάγκης, προς ειδοποίηση (π.χ. ανήλικοι, ηλικιωμένοι, Α.Μ.Ε.Α., άτομα με σοβαρές παθήσεις).

Ως Προσωπικά Δεδομένα Κατόχου για την ΚΠ θα ορίσουμε το σύνολο των δεδομένων που προτείνονται από τον ICAO να αναγράφονται κατ' ελάχιστον στην ΚΠ και είναι τα εξής:

1. Κωδικός & Τύπος Εγγράφου
2. Κωδικός Χώρας Έκδοσης
3. Ιθαγένεια
4. Αριθμός Εντύπου της ΚΠ
5. Επώνυμο
6. Όνομα
7. Ημερομηνία Γέννησης
8. Φύλλο
9. Ημερομηνία Λήξης Ισχύος της ΚΠ
10. Φωτογραφία
11. Ιδιόχειρη Υπογραφή

Τα δεδομένα πρέπει να αναγράφονται και στην Αγγλική, όπως και στο παραδοσιακό έντυπο ΑΔΤ, για διευκόλυνση της χρήσης της εκτός Ελλάδας. Δεδομένα που αναγράφονται στην ΑΔΤ, όπως ύψος, πατρώνυμο, τόπος γέννηση, ομάδα αίματος κλπ, δεν απαιτούνται.

Τα τρία πρώτα πεδία (Κωδικός & Τύπος Εγγράφου, Κωδικός Χώρας Έκδοσης και Ιθαγένεια) θα ακολουθούν την κωδικοποίηση του ICAO, όπως ήδη χρησιμοποιούνται στα ελληνικά διαβατήρια.

Ο Αριθμός Εντύπου της ΚΠ θα είναι ένας αλφαριθμητικός τυχαία παραγόμενος αριθμός και η χρήση του θα είναι αντίστοιχη με τον σημερινό αριθμό ΑΔΤ. Ο αριθμός αυτός δεν αποτελεί μοναδικό αναγνωριστικό της ΚΠ. Σε περίπτωση επανέκδοσης της ΚΠ, για οποιοδήποτε λόγο, παράγεται νέος αριθμός εντύπου, καθώς ακολουθεί τη λογική του εγγράφου.

Η διάρκεια ζωής της ΚΠ προτείνεται να είναι στα 10 έτη και επομένως η Ημερομηνία Λήξης Ισχύος θα προκύπτει στα δέκα χρόνια από την ημερομηνία έκδοσης.

Η φωτογραφία και η ιδιόχειρη υπογραφή θα λαμβάνονται κατά την προσκόμιση των δικαιολογητικών για την έκδοση της ΚΠ, από τον πολίτη.

Πέραν όμως, των προαναφερόμενων δεδομένων, η ΚΠ πρέπει να περιλαμβάνει και ένα σύνολο δεδομένων που να την κάνει χρήσιμη για τις συναλλαγές του πολίτη και τη χρήση των υπηρεσιών ηλεκτρονικής διακυβέρνησης. Τα δεδομένα αυτά θα αποθηκεύονται ηλεκτρονικά και θα χρησιμοποιούνται όταν και όπου απαιτείται, έπειτα από τη συγκατάθεση του πολίτη.

Τα μη αναγραφόμενα δεδομένα προκύπτουν από την ανάγνωση της υφιστάμενης κατάστασης για τις συναλλαγές του πολίτη με τη Δημόσια Διοίκηση και την ανάλυση του θεσμικού πλαισίου, όπως παρουσιάζεται στο Κεφάλαιο 3, υπό το πρίσμα της διευκόλυνσης της χρήσης της ΚΠ, ως εργαλείο πρόσβασης και αυθεντικοποίησης για τις ηλεκτρονικές συναλλαγές. Τα δεδομένα αυτά αποτελούν αναγνωριστικά του πολίτη.

Κατά συνέπεια, προτείνονται:

1. Αριθμός Φορολογικού Μητρώου (ΑΦΜ) για χρήση υπηρεσιών που παρέχονται κυρίως από το Υπουργείο Οικονομικών, ή άλλων υπηρεσιών στις οποίες χρησιμοποιείτο έως σήμερα. Ο αριθμός ΑΦΜ αποτελεί μη μεταβλητό αριθμό που ταυτοποιεί μοναδικά τον πολίτη και χρησιμοποιείται, ευρέως, για ένα πλήθος οικονομικών κυρίως συναλλαγών, αλλά και ως αναγνωριστικό του πολίτη σε συστήματα άλλων υπηρεσιών.
2. Αριθμός Μητρώου Κοινωνικής Ασφάλισης (ΑΜΚΑ) για πρόσβαση στις υπηρεσίες ασφάλισης και υγείας. Ο ΑΜΚΑ είναι μη μεταβλητός αριθμός που προσδιορίζει μοναδικά τον πολίτη.
3. Αριθμός Δημοτολογίου και Κωδικός Δήμου στον οποίο είναι εγγεγραμμένος για χρήση των υπηρεσιών του Υπουργείο Εσωτερικών, ή άλλων υπηρεσιών στις οποίες χρησιμοποιείτο έως σήμερα. Τα στοιχεία αυτά είναι μεταβλητά και αλλάζουν πιθανώς έπειτα από αλλαγή της οικογενειακή κατάστασης του πολίτη και μεταδημότευσής του.

4. Αριθμός Δελτίου Ταυτότητας (ΑΔΤ), αποτελεί τον αριθμό του ΑΔΤ που παραδόθηκε κατά τη διαδικασία έκδοσης της ΚΠ. Ο ΑΔΤ θα χρησιμοποιηθεί για τη διασφάλιση της «προς τα πίσω συμβατότητας» με το μητρώο αστυνομικών ταυτοτήτων και προτείνεται να αντικατασταθεί σταδιακά από τον Αριθμό Εντύπου της ΚΠ.

5. Ψηφιακά Πιστοποιητικά (θα αναλυθεί στο σενάριο υλοποίησης)

Αν και ίσως θα ήταν αναμενόμενο να συμπεριλάβουμε και κάποια στοιχεία διεύθυνσης και επικοινωνίας του πολίτη στην κάρτα, ωστόσο, αυτό δεν κρίνεται απαραίτητο. Μάλιστα τα στοιχεία αυτά είναι πολύ συχνά μεταβαλλόμενα και δεν εκτιμάται ότι θα προσδώσουν κανένα σημαντικό όφελος από την ενσωμάτωσή τους. Σε περίπτωση που είναι αναγκαίο για τη διεκπεραίωση μιας συναλλαγής, τα στοιχεία διεύθυνσης μπορούν να ζητούνται από τον πολίτη κατά τη διάρκεια της συναλλαγής.

6.2.2. Κεντρικά Ερωτήματα Υλοποίησης

Ποιο σκοπό εξυπηρετεί η αποθήκευση αυτών των δεδομένων στην ΚΠ;

Για την Ελλάδα, τα μόνα αναγνωριστικά που σήμερα μπορούν να ταυτοποιήσουν μοναδικά τον πολίτη είναι ο ΑΦΜ και ο ΑΜΚΑ,. Στην περίπτωση των δελτίων ταυτότητας, ο ΑΔΤ ακολουθεί τη λογική του εγγράφου, δηλαδή σε περίπτωση επανέκδοσης της ταυτότητας του πολίτη εξαιτίας ανανέωσης, ακύρωσης, ανάκλησης, κλοπής ή απώλειας παράγεται νέος αριθμός για το δελτίο ταυτότητας, γεγονός που σημαίνει ότι για κάθε πολίτη αντιστοιχούν περισσότεροι του ενός αριθμοί ΑΔΤ.

Η αποθήκευση των τεσσάρων αναγνωριστικών του πολίτη στην ΚΠ είναι το στοιχείο που προσδίδει επιπλέον λειτουργικότητα και χρηστικότητα στην ΚΠ. Η κεντρική ιδέα είναι ότι η ΚΠ δεν θα πρέπει απλά να αντικαθιστά το δελτίο ταυτότητας και το διαβατήριο, ακόμη και προσδίδοντάς τους διαλειτουργικά χαρακτηριστικά, αλλά και να αποτελεί ένα χρήσιμο εργαλείο του πολίτη για τις συναλλαγές του με το κράτος.

Προκειμένου κάτι τέτοιο να γίνει εφικτό οι επιλογές είναι δύο. Είτε ο αριθμός εντύπου ή κάποιος άλλος αριθμός της ΚΠ πρέπει να αποτελέσει ένα μοναδικό αναγνωριστικό για τον πολίτη, που να σχετίζεται με τα αναγνωριστικά που χρησιμοποιούν οι επιμέρους υπηρεσίες/φορείς του Δημοσίου, είτε πρέπει να βρεθεί ένας τρόπος να αναγνωρισθούν και να αξιοποιηθούν τα υφιστάμενα αναγνωριστικά.

Αυτή είναι η επιλογή που προτείνουμε στη σχεδιαστική λύση της εφαρμογής της ΚΠ στην Ελλάδα.

Τα προαναφερόμενα τέσσερα αναγνωριστικά θεωρούμε ότι είναι εκείνα που χρησιμοποιούνται από το σύνολο των υπηρεσιών της Δημόσιας Διοίκησης και απαιτούνται για την ταυτοποίηση του χρήστη.

Με τη χρήση τους από την ΚΠ αποφεύγεται η δημιουργία ενός ενιαίου μοναδικού αναγνωριστικού που θα ταυτοποιεί μοναδικά τον πολίτη και θα σχετίζεται με όλα τα επιμέρους μητρώα των υπηρεσιών ηλεκτρονικής διακυβέρνησης. Με αποτέλεσμα να συγκεντρώνεται όλη η πληροφορία για τον πολίτη ουσιαστικά σε ένα σημείο, καθώς η

αποκάλυψη του αναγνωριστικού αυτού συνεπάγεται και ταυτόχρονη αποκάλυψη όλων των προσωπικών δεδομένων και των δεδομένων συναλλαγών του πολίτη.

Με ποιον τρόπο θα γίνεται η πρόσβαση σε αυτά;

Προκειμένου ο πολίτης να έχει πρόσβαση σε υπηρεσίες ηλεκτρονικής διακυβέρνησης, μέσω της χρήσης της ΚΠ, απαιτείται ο πολίτης να εγγραφεί στις αντίστοιχες ηλεκτρονικές υπηρεσίες (π.χ. taxisnet) που παρέχονται από επιμέρους αρμόδιες υπηρεσίες ή στην Κεντρική Διαδικτυακή Πύλη του Ελληνικού Δημοσίου (ΕΡΜΗΣ), που σχεδιάστηκε να παρέχει ηλεκτρονικά το σύνολο των υπηρεσιών του δημοσίου. Εντούτοις, αυτό δεν σημαίνει ότι ο πολίτης πρέπει επίσης να συναινέσει στη συσχέτιση των προσωπικών του δεδομένων που περιέχονται στην ΚΠ με τα επιμέρους δεδομένα που τηρούνται στα μητρώα των υπηρεσιών. Για την αντιστοίχιση αυτή απαιτείται επιπλέον ρητή συγκατάθεση του πολίτη.

Κατά τη διάρκεια μιας συναλλαγής, η ανάκτηση κάποιων δεδομένων της ΚΠ είναι απαραίτητη, ωστόσο πρέπει να εξασφαλίζεται ότι είναι το ελάχιστο δυνατό σύνολο πληροφοριών. Η πληροφορία που χρησιμοποιείται κοινοποιείται στον κάτοχο της ΚΠ και στον πάροχο της ηλεκτρονικής υπηρεσίας. Οι πληροφορίες αυτές είναι:

1. η ισχύς ή όχι της ΚΠ,
2. η δικαιοδοσία του παρόχου της ηλεκτρονικής υπηρεσίας για πρόσβαση στα δεδομένα της ΚΠ,
3. ποια δεδομένα είναι απαραίτητα για τη χρήση μιας υπηρεσίας

Σε κάθε περίπτωση, η ανάγνωση των προσωπικών δεδομένων και των αναγνωριστικών του πολίτη από συστήματα και υπηρεσίες κατά τη χρήση της ΚΠ μπορεί να εξασφαλίζεται αποκλειστικά και μόνο υπό την προϋπόθεση της ρητής συγκατάθεσης του χρήστη-πολίτη. Η συγκατάθεση εξασφαλίζεται με την καταχώριση του αριθμού PIN της ΚΠ σε ειδικό πληκτρολόγιο του αναγνώστη της κάρτας.

Η ανάγνωση της πληροφορίας με άλλο τρόπο από αυτόν που περιγράψαμε παραπάνω, πρέπει να είναι αδύνατη.

Σχετικά τώρα, με τα αποθηκευμένα αναγνωριστικά της ΚΠ πρέπει να επισημάνουμε ότι τα δεδομένα αυτά θα είναι αποθηκευμένα και δεν θα αναγράφονται σε εμφανές σημείο. Ο πολίτης χρησιμοποιώντας την ΚΠ για μια συναλλαγή δίνει ουσιαστικά την πρώτη συγκατάθεσή του για την πρόσβαση της συγκεκριμένης εφαρμογής στην πληροφορία της ΚΠ, προκειμένου η υπηρεσία να αναγνωρίσει τον χρήστη και η συναλλαγή του να ολοκληρωθεί. Σε περίπτωση, όμως, που η υπηρεσία που ζητήσει ο χρήστης απαιτεί περισσότερη πληροφορία, ο πολίτης θα πρέπει να ερωτάται αν θέλει να δώσει πρόσβαση σε κάποιο από τα τέσσερα αναγνωριστικά του. Έτσι, για παράδειγμα, η εφαρμογή θα ζητά πρόσβαση στον ΑΦΜ διευκρινίζοντας και τον σκοπό χρήσης της πληροφορίας και μόνο αν ο πολίτης την εξασφαλίσει θα έχει πρόσβαση για να διεκπεραιώσει τη συναλλαγή. Διαφορετικά, θα ενημερώνεται ο χρήστης ότι δεν μπορεί να διεκπεραιωθεί η συναλλαγή και τις εναλλακτικές υπηρεσίες που μπορεί να χρησιμοποιήσει.

Η ανάγνωση των στοιχείων ΑΦΜ, ΑΜΚΑ, ΑΔΤ και Αριθμού Δημοτολογίου θα γίνεται μόνο από εξουσιοδοτημένα συστήματα και εφαρμογές που δικαιοδοτούνται να έχουν πρόσβαση στα στοιχεία αυτά και εφόσον είναι απαραίτητη για την υπηρεσία που θα προσφέρουν. Για παράδειγμα, το σύστημα της ηλεκτρονικής συνταγογράφησης θα έχει πρόσβαση στον ΑΜΚΑ του πολίτη, ενώ αντίστοιχα το σύστημα TAXIS θα έχει πρόσβαση στον ΑΦΜ. [σύμφωνα και με τη μελέτη ΔΜ]

Ο πολίτης, κάνοντας χρήση των υπηρεσιών ηλεκτρονικής διακυβέρνησης και της Κεντρικής Πύλης (ΕΡΜΗΣ), μέσω της ΚΠ πρέπει να είναι σε θέση:

- Να ενημερώνεται για τα δεδομένα του που τηρούνται στα επιμέρους μητρώα της Δημόσιας Διοίκησης.
- Να γνωρίζει ποιοι πάροχοι πρέπει να έχουν πρόσβαση σε δεδομένα του και για ποιο σκοπό
- Να γνωρίζει την ιστορικότητα των συναλλαγών του, στην οποία θα περιλαμβάνονται τα συστήματα που προσπέλασαν τα δεδομένα του, την παρεχόμενη υπηρεσία για την οποία χρησιμοποιήθηκαν και τη χρονική στιγμή της συναλλαγής.

Οι παραπάνω λειτουργίες της ΚΠ εξασφαλίζουν το μέγιστο δυνατό επιπέδου ιδιωτικότητας και προστασίας των προσωπικών δεδομένων του πολίτη-κατόχου της ΚΠ.

Χρήση ή όχι μοναδικού αναγνωριστικού πολίτη;

Η χρήση ενός μοναδικού αναγνωριστικού σε ένα σύστημα διαχείρισης ταυτοτήτων μπορεί να μηδενίσει τα ζητήματα επικοινωνίας με υφιστάμενα συστήματα και εφαρμογές του δημόσιου και ιδιωτικού τομέα, αλλά και ζητήματα διαλειτουργικότητας με άλλα συστήματα εντός και εκτός χώρας. Αυτό μπορεί να το κάνει πολύ ελκυστική επιλογή. Παρόλα αυτά, αν θυμηθούμε τις απαιτήσεις που συγκεντρώσαμε κι αναλύσαμε προηγουμένως, θα διαπιστώσουμε ότι η εφαρμογή ενός ενιαίου μοναδικού αναγνωριστικού για τον πολίτη στην Ελληνική ΚΠ είναι μια επιλογή που θα συγκέντρωνε πληθώρα αρνητικών αντιδράσεων, γεγονός που πρέπει να μας οδηγήσει σε μια δεύτερη σκέψη της χρήσης του. Στην πραγματικότητα, η σημαντικότερη συμβολή του αφορά στην ενοποίηση των μητρώων που τηρούνται επιμέρους στους δημόσιους φορείς και στην ευχρηστία που θα προσέφερε στη διαχείριση των υπηρεσιών ηλεκτρονικής διακυβέρνησης, χωρίς πολύπλοκες παρεμβάσεις σε υφιστάμενα συστήματα. Εντούτοις, πρέπει να παρατηρήσουμε ότι κάτι τέτοιο πιθανόν να ήταν χρήσιμο, αν υπήρχε ήδη ένα αναπτυγμένο δίκτυο ηλεκτρονικών υπηρεσιών της Δημόσιας Διοίκησης κάτι που πρέπει να παραδεχτούμε ότι για την Ελληνική Δημόσια Διοίκηση δεν υφίσταται.

Εξάλλου, μελετώντας και τη διεθνή πρακτική παρατηρούμε ότι στην Αυστριακή ΚΠ, το μοναδικό αναγνωριστικό που είχε εισαχθεί, απαξιώθηκε στην πράξη και η αντίστοιχη ΚΠ λειτουργεί πλέον με τομεακά αναγνωριστικά. Σε περιπτώσεις όπως το Βέλγιο και η Φινλανδία, ένα προηγμένο πλαίσιο υπηρεσιών ηλεκτρονικής διακυβέρνησης προϋπήρχε

της εφαρμογής της ΚΠ και αντίστοιχα προϋπήρχε η χρήση μοναδικού αναγνωριστικού για να διευκολύνει τις σχέσεις του πολίτη με τη δημόσια διοίκηση.

Συνεπώς, η πλήρης αξιοποίηση της ΚΠ εκτιμούμαι ότι δεν προϋποθέτει την ύπαρξη ή δημιουργία και ενός μοναδικού αριθμού για τον πολίτη. Και επομένως αντιπροτείνεται η λύση των τομεακών αναγνωριστικών.

Ποιο θα είναι το αναγνωριστικό της ΚΠ;

Το αναγνωριστικό της ΚΠ θα είναι ο αριθμός εντύπου της ΚΠ που θα αναγράφεται και στην μπροστινή πλευρά της ΚΠ. Ο αριθμός εντύπου όπως σημειώσαμε και παραπάνω θα είναι ένας 9ψήφιος αλφαριθμητικός κωδικός, που προτείνεται να ακολουθεί το mod10 731731 του ICAO για την παραγωγή του τελευταίου ψηφίου, προκειμένου να αποφευχθούν οι πιθανές κοινωνικές αντιδράσεις. Ο αριθμός αυτός θα αποτελεί το αναγνωριστικό για την ΚΠ, το οποίο θα ακολουθεί τη λογική του εγγράφου και τον κύκλο ζωής της ΚΠ. Επομένως, ο αριθμός εντύπου θα αλλάζει μόνο στην περίπτωση επανέκδοσης της κάρτας για τον πολίτη. Θα μπορούσαμε να παραλληλίσουμε τον αριθμό εντύπου της ΚΠ με τον σημερινό ΑΔΤ, καθώς θα έχει ακριβώς την ίδια χρήση, πληρώντας αντίστοιχα χαρακτηριστικά. Έτσι, θα χρησιμοποιείται για τη φυσική ταυτοποίηση του πολίτη με την επίδειξη της ΚΠ, καθώς και κατά την ανάγνωση της ΚΠ (περιοχή MRZ) από τους καρταναγνώστες.

Αναγνωριστικό της ΚΠ και ηλεκτρονικές συναλλαγές

Προκειμένου να εξασφαλίσουμε μεγαλύτερη ασφάλεια κατά τη χρήση της ΚΠ, προτείνεται για τις συναλλαγές της ΚΠ να μην χρησιμοποιείται ως αναγνωριστικό, ο έντυπος αριθμός της ΚΠ. Με αυτόν τον τρόπο μπορούμε να αντιμετωπίσουμε το profiling, να αποφύγουμε τις συσχετίσεις με άλλα αναγνωριστικά και τις διασυνδέσεις της πληροφορίας που χρησιμοποιείται για τις συναλλαγές με διαφορετικούς παρόχους και τελικά να θωρακίσουμε την ιδιωτικότητα και να ενισχύσουμε το αίσθημα ασφάλειας των πολιτών. Κατά τη χρήση, λοιπόν, της ΚΠ σε μια ηλεκτρονική υπηρεσία, το τσιπ της ΚΠ μπορεί να παράγει ένα διαφορετικό αναγνωριστικό ανά συναλλαγή. Επειδή όμως, κάτι τέτοιο πιθανόν να επιβαρύνει, η ενδιάμεση λύση που φαίνεται να προκρίνεται είναι να παράγεται διαφορετικό αναγνωριστικό ανά πάροχο υπηρεσίας, ή ανά ομάδα παρόχων ηλεκτρονικών υπηρεσιών. Για την εξασφάλιση δε ακόμη μεγαλύτερης προστασίας, θα πρέπει να παρέχεται η δυνατότητα της χρήσης διαφορετικού ψευδωνύμου από τον χρήστη ανά ηλεκτρονική υπηρεσία, γεγονός που θα περιορίζει τη γνώση του παρόχου της εκάστοτε υπηρεσίας στα δεδομένα του πολίτη.

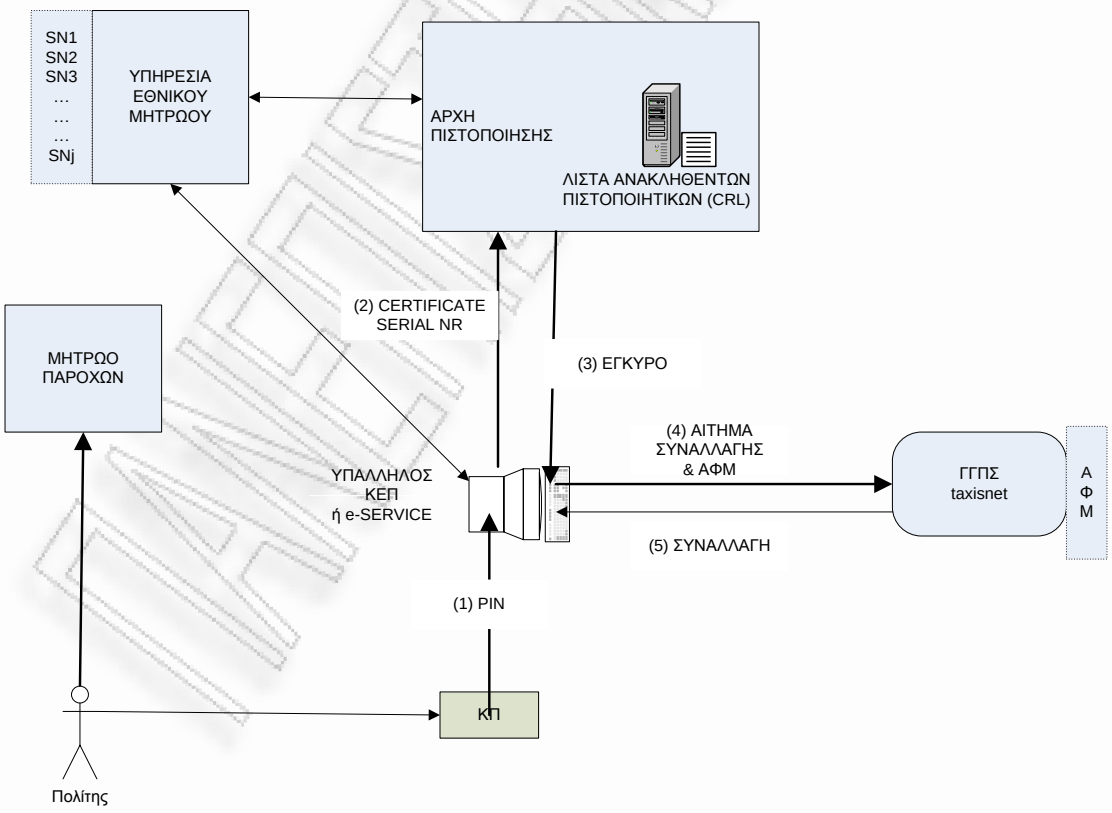
6.2.3. Σενάριο Υλοποίησης της ΚΠ

Στην ενότητα αυτή θα περιγράψουμε το βέλτιστο κατά την άποψή μας, σενάριο υλοποίησης της Ελληνικής ΚΠ. Στην πραγματικότητα, ήδη από την αρχή της παρούσας ενότητας περιγράφουμε την Ελληνική ΚΠ και τα δεδομένα που πρέπει να περιέχει, σε αυτό όμως, το σημείο θα δούμε πως μπορεί να χρησιμοποιηθεί αλληλεπιδρώντας με τους

υφιστάμενους παρόχους υπηρεσιών και ουσιαστικά θα μοντελοποιήσουμε τις απαντήσεις στα κρίσιμα ερωτήματα υλοποίησης που διατυπώθηκαν προηγουμένως.

Η Διεθνής πρακτική μας καταδυκνύει ότι η σύγχρονες λύσεις ηλεκτρονικής ταυτοποίησης οδηγούν στη χρήση πολλαπλών αναγνωριστικών. Εντούτοις, για να μπορέσουμε να εξασφαλίσουμε το μεγαλύτερο δυνατό βαθμό βεβαιότητας για την επιτυχή υιοθέτησή της ΚΠ από το σύνολο των πολιτών πρέπει να σταθμίσουμε την επίδραση της υλοποίησης στην ιδιαίτερη περίπτωση της Ελλάδας και να λάβουμε υπόψη τα ζητήματα διαλειτουργικότητας, την επίπτωση στην ιδιωτικότητα του πολίτη, καθώς και την ευκολία εφαρμογής της λύσης με βάση την υφιστάμενη κατάσταση και τις απαιτήσεις παρέμβασης σε υφιστάμενες δομές της δημόσιας διοίκησης, συστήματα και εφαρμογές.

Όπως έχει ήδη περιγραφεί και παραπάνω, για την εφαρμογή και πλήρη αξιοποίηση της ΚΠ δεν απαιτείται η δημιουργία ενός ενιαίου μοναδικού αναγνωριστικού ανά πολίτη-κάτοχο ΚΠ, αντιθέτως επιλέγεται η χρήση τομεακών αναγνωριστικών που θα αποθηκεύονται στο τσιπ της ΚΠ και θα διευκολύνουν τις συναλλαγές με τους επιμέρους παρόχους ηλεκτρονικών υπηρεσιών. Για το λόγο αυτό, καταλήξαμε ότι τα πρόσθετα στοιχεία στην ΚΠ θα είναι ο ΑΦΜ, ο ΑΜΚΑ, ο ΑΔΤ, Αριθμός Δημοτολογίου και ο Δήμος. Επιπλέον, θα αποθηκεύονται ψηφιακά πιστοποιητικά που θα την καθιστούν εκτός από λειτουργική και ασφαλή.



Εικόνα 35-Χρήση της ΚΠ για υπηρεσία της ΓΓΠΣ

Μέσω της χρήσης της ΚΠ, ο πολίτης μπορεί να αλληλεπιδρά με διαφορετικούς παρόχους ηλεκτρονικών υπηρεσιών με δύο τρόπους:

- Με την απευθείας χρήση ηλεκτρονικών υπηρεσιών
- Μέσω των υπηρεσιών της Δημόσιας Διοίκησης (π.χ. ΚΕΠ), οι οποίες θα προσφέρουν πρόσβαση στις ηλεκτρονικές υπηρεσίες των επιμέρους παρόχων υπηρεσιών.

Η διαδικασία που ακολουθείται θα είναι η ίδια, ανεξάρτητα με το αναγνωριστικό που θα ανασύρεται από την ΚΠ, για την παροχή μιας υπηρεσίας, ή το σύνολο των δεδομένων που απαιτούνται προκειμένου να διεκπεραιωθεί μια ηλεκτρονική συναλλαγή.

Κεντρικό ρόλο στην εγκαθίδρυση της εμπιστοσύνης στη διαδικασία αποτελεί η Αρχή Πιστοποίησης, η οποία αφενός πιστοποιεί τους παρόχους υπηρεσιών και αφετέρου διατηρεί τη Λίστα Ανακληθέντων ΚΠ, αλλά και επικοινωνεί με τις επιμέρους Λίστες Ανακληθέντων των επιμέρους μητρώων των παρόχων ηλεκτρονικών υπηρεσιών.

Επιπλέον, η Υπηρεσία Εθνικού Μητρώου ΚΠ αποτελεί την πιο σημαντική οντότητα στο σχήμα. Η υπηρεσία αυτή είναι αρμόδια για την τήρηση του Εθνικού Μητρώου ΚΠ, στο οποία θα περιλαμβάνονται τα serial numbers των ΚΠ και το ιστορικό των συναλλαγών με τα επιμέρους μητρώα και υπηρεσίες.

Εφόσον περιγράψαμε τις οντότητες που συμμετέχουν στη διαδικασία, μπορούμε να προχωρήσουμε στην περιγραφή των βημάτων που απαιτούνται για μια συναλλαγή με τη χρήση της ΚΠ.

Η διαδικασία περιλαμβάνει τα ακόλουθα βήματα:

1. Ο πολίτης εισάγει την ΚΠ στη συσκευή ανάγνωσης
2. Ο πολίτης εισάγει το PIN της ΚΠ, προκειμένου να πιστοποιήσει ότι είναι ο νόμιμος κάτοχός της
3. Ο αναγνώστης επικοινωνεί με την Αρχή Πιστοποίησης προκειμένου να διαπιστώσει την εγκυρότητα ή όχι της ΚΠ
4. Η Αρχή Πιστοποίησης επιβεβαιώνει την εγκυρότητα της ΚΠ. Εναλλακτικά, επιστρέφει απάντηση για μη έγκυρη ΚΠ και ο αναγνώστης ενημερώνει τον πολίτη για την αδυναμία διεκπεραίωσης της συναλλαγής και η διαδικασία ολοκληρώνεται.
5. Ο πολίτης αιτείται για μια συναλλαγή από τον αντίστοιχο πάροχο υπηρεσίας (π.χ. ΓΓΠΣ)
6. Ο πάροχος υπηρεσίας επιστρέφει ερώτημα σχετικά με το απαιτούμενο τομεακό αναγνωριστικό του πολίτη για την επιθυμητή συναλλαγή.
7. Ο πολίτης δίνει στον πάροχο ρητή συγκατάθεση για πρόσβαση σε ένα από τα τομεακά αναγνωριστικά που είναι αποθηκευμένα στο τσιπ της ΚΠ (π.χ. ΑΦΜ).

8. Ο πάροχος ελέγχει μέσω του μητρώου του αν το αναγνωριστικό είναι έγκυρο ή όχι. Σε περίπτωση άκυρου ή ανενεργού αναγνωριστικού επιστρέφει απάντηση για αδυναμία συναλλαγής και η διαδικασία ολοκληρώνεται.
9. Ο πάροχος εκτελεί τις απαραίτητες ενέργειες για τη διεκπεραίωση της συναλλαγής.
10. Ο πάροχος ολοκληρώνει τη συναλλαγή και επιστρέφει την απάντηση στον πολίτη.
11. Η Υπηρεσία Εθνικού Μητρώου ΚΠ καταγράφει τη συναλλαγή.
12. Ο πολίτης απολαμβάνει την υπηρεσία.

6.3. Επιχειρησιακό Μοντέλο Εφαρμογής της ΚΠ

Με τη λειτουργία του συστήματος της ΚΠ, δυο είναι οι βασικές ομάδες οντοτήτων που συμμετέχουν στη χρήση της: Οι κάτοχοι της ΚΠ και οι πάροχοι ηλεκτρονικών υπηρεσιών (η-πάροχοι). Αυτοί είναι που θα πρέπει να διευκολυνθούν ώστε να ενταχθούν στο σύστημα και να αξιοποιήσουν τις υποδομές και τις λειτουργίες της ΚΠ. Ακολούθως περιγράφονται οι καταστάσεις του κύκλου ζωής της ΚΠ που πρέπει να υποστηριχθούν, καθώς και βασικά σημεία της εξυπηρέτησης που απαιτείται για τον πολίτη και τον πάροχο.

6.3.1. Κύκλος ζωής της ΚΠ

Η ΚΠ μπορεί να μεταπέσει στις ακόλουθες καταστάσεις:

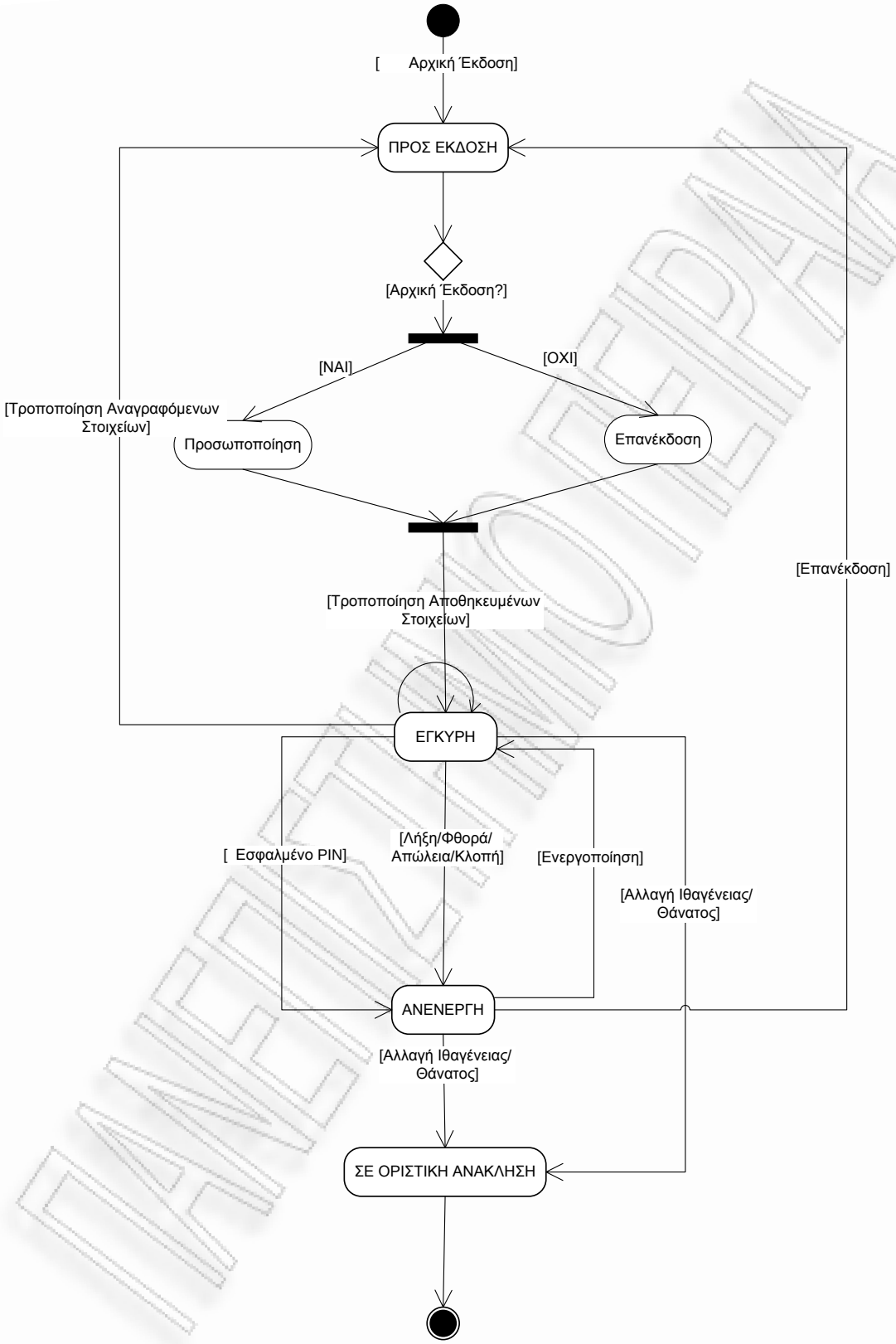
(1) Προς Έκδοση

(2) Έγκυρη

(3) Ανενεργή

(4) Σε Οριστική Ανάκληση

Στο παρακάτω σχήμα παρουσιάζεται ο τρόπος και οι συνθήκες μετάπτωσης της ΚΠ, από τη μία κατάσταση στην άλλη.



Εικόνα 36- Καταστάσεις ΚΠ

Στην κατάσταση (1) «Προς Έκδοση» η ΚΠ είναι λίγο πριν την αντιστοίχιση με τον πολίτη. Δεν είναι ενεργοποιημένη και δεν μπορεί να χρησιμοποιηθεί ως έγκυρη ΚΠ από τον πολίτη για

οποιαδήποτε συναλλαγή. Η αρχική έκδοση της ΚΠ αφορά τους κατόχους ΑΔΤ που προσέρχονται για αντικατάσταση της αστυνομικής τους ταυτότητας με την ΚΠ, τους πολίτες που κατέχουν Ελληνικό διαβατήριο και σε νέους πολίτες που δεν έχουν ακόμη δελτίο αστυνομικής ταυτότητας.

Κατά την κατάσταση αυτή, και πριν την μετάβαση στην λειτουργική της κατάσταση, γίνεται η προσωποποίηση του πολίτη με την κάρτα, προστίθενται οι απαραίτητες λειτουργίες στην ΚΠ, επιπλέον δυνατότητες (λειτουργίες ή/και εφαρμογές), αποδίδεται ο μυστικός αριθμός ασφαλείας (PIN-PUK) και αντιστοιχίζεται στον κάτοχό της. Η προσωποποίηση της ΚΠ είναι απαραίτητη μόνο κατά την πρώτη έκδοση της ΚΠ, σε περίπτωση επανέκδοσης δεν είναι απαραίτητη η διαδικασία.

Από την κατάσταση (1) «Προς Έκδοση» μπορεί να μεταβεί στην κατάσταση (2) «Έγκυρη», είτε έπειτα από την προσωποποίηση του χρήστη, κατά την αρχική έκδοση της ΚΠ, είτε έπειτα από επανέκδοση της ΚΠ, λόγω αλλαγής των αναγραφόμενων στοιχείων ή εξαιτίας της λήξης της ανάκλησής της.

Στην κατάσταση (2) «Έγκυρη», η ΚΠ βρίσκεται στην παραγωγική της λειτουργία. Ο κάτοχος ενεργοποιεί την ΚΠ, κατά την πρώτη χρήση της και η ΚΠ μπορεί πλέον να αξιοποιηθεί για οποιαδήποτε σχετική χρήση. Κατά την κατάσταση αυτή, μπορεί να γίνει τροποποίηση των αποθηκευμένων στοιχείων του πολίτη, ενεργοποίηση ή/και απενεργοποίηση λειτουργιών της κάρτας, προσθήκη νέων εφαρμογών (π.χ. ψηφιακή υπογραφή), χωρίς να αλλάζει κατάσταση η ΚΠ.

Από την «Έγκυρη» κατάσταση η ΚΠ μπορεί να μεταβεί α) σε «Ανενεργή» κατάσταση εξαιτίας λήξης ισχύος της κάρτας, απώλειας, κλοπής ή φθοράς και εξαιτίας μη έγκυρης εισαγωγής αριθμού PIN και β) «Σε Οριστική Ανάκληση» εξαιτίας αλλαγής ιθαγένειας γεγονός που καθιστά πλέον μη δικαιούχο τον μέχρι πρότινος κάτοχο της ΚΠ ή θανάτου του κατόχου της ΚΠ.

Στην κατάσταση (3) «Ανενεργή» η ΚΠ έχει απενεργοποιηθεί και δεν μπορεί να αξιοποιηθεί περαιτέρω.

Το αρχείο ανακληθέντων ΚΠ που πρέπει να τηρείται, πρέπει να είναι διαρκώς επικαιροποιημένο, ώστε να μην γίνεται εφικτή «κακή χρήση» της ΚΠ, είτε από τον ίδιο τον κάτοχό της (π.χ. απαγόρευση εξόδου από τη χώρα έπειτα από αξιόποινη πράξη), είτε από τρίτο πρόσωπο που την έχει πιθανά υπεξαιρέσει.

Από την κατάσταση αυτή η ΚΠ μπορεί να μεταβεί α)σε «Έγκυρη» κατάσταση σε περίπτωση που η άρση του λόγου ανάκλησής της δεν απαιτεί αλλαγή της κάρτας , β) «Προς Έκδοση», αν απαιτείται επανέκδοση της ΚΠ και γ) σε «Οριστική Ανάκληση».

Η υπό ανάκληση ΚΠ μπορεί να ενεργοποιηθεί εκ νέου, χωρίς αλλαγή εντύπου, στην περίπτωση που η ανάκλησή της έγινε εξαιτίας εισαγωγής λανθασμένου PIN και απαιτείται απλά επαναπρογραμματισμός της ΚΠ, είτε σε περιπτώσεις που έχει γίνει ανάκληση των λειτουργιών της ΚΠ (π.χ. από τις αρχές, ποινικό αδίκημα), στην περίπτωση αυτή ο κάτοχος έχει ακόμη στην πραγματικότητα την ΚΠ, ωστόσο, δεν μπορεί να τη χρησιμοποιήσει ως

ταξιδιωτικό έγγραφο, καθώς έχει ανακληθεί αυτή της η δυνατότητα, ούτε για χρήση ηλεκτρονικών υπηρεσιών. Θα μπορούσαμε να πούμε ότι η φυσική ταυτοποίηση από τις αρχές είναι δυνατή, εντούτοις, σε αυτήν την περίπτωση στο μητρώο των ΚΠ, η κατάστασή της είναι «Ανενεργή», γεγονός που σημαίνει ότι όλα τα επιμέρους μητρώα αναγνωρίζουν ως μη ενεργή την ΚΠ.

Στην κατάσταση (4) «Σε Οριστική Ανάκληση», η ΚΠ έχει ολοκληρώσει τον κύκλο ζωής της, είτε σε περίπτωση αλλαγής ιθαγένειας του πολίτη, είτε σε περίπτωση θανάτου. Στην πραγματικότητα η διαφοροποίηση από την προηγούμενη ανάκληση είναι ότι δεν υπάρχει δυνατότητα εκ νέου ενεργοποίησης ή επανέκδοσης της κάρτας με κάποιον τρόπο. Η κατάσταση αυτή αποτελεί την τελική κατάσταση της ΚΠ κι έπειτα από αυτή δεν μπορεί να μεταβεί σε άλλη κατάσταση.

Ο κύκλος ζωής της ΚΠ θα λέγαμε ότι μοιάζει αρκετά με τον κύκλο ζωής της έντυπης ΑΔΤ, αν και η αστυνομική ταυτότητα είναι πολύ πιο απλοποιημένη. Τα απαιτούμενα δικαιολογητικά και η ακριβής διαδικασία για τη μετάβαση της ΚΠ από την μία κατάσταση στην άλλη πρέπει να προσδιορισθεί μέσω του θεσμικού πλαισίου που θα έρθει να καλύψει την εφαρμογή της ΚΠ. Σε αυτήν την κατεύθυνση είτε θα απαιτηθούν νέες νομοθετικές παρεμβάσεις, είτε αν εκτιμηθεί ότι το υφιστάμενο θεσμικό πλαίσιο είναι επαρκές θα απαιτηθεί απλώς εξειδίκευση του θεσμικού πλαισίου.

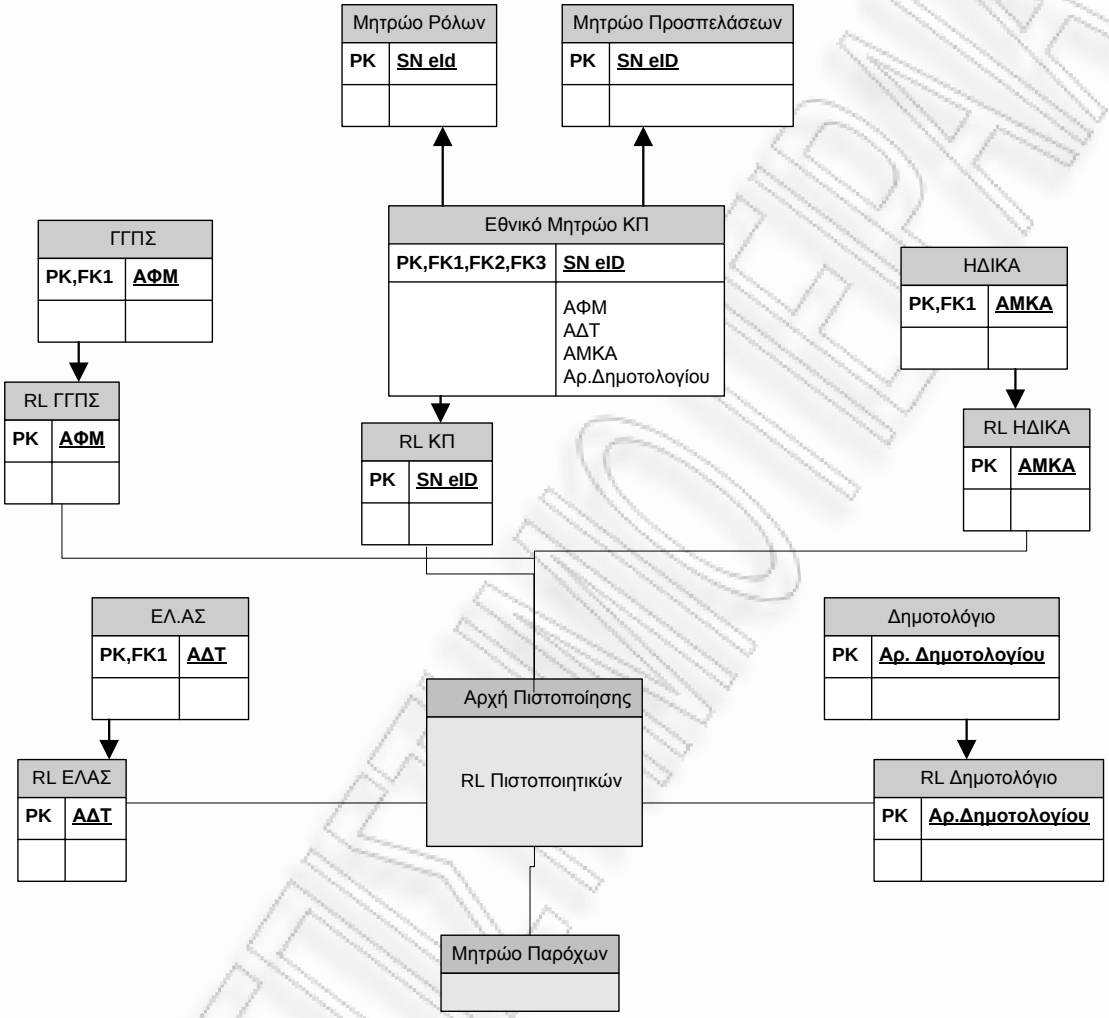
6.3.2. Τήρηση Μητρώων για την ΚΠ

Για την εφαρμογή της ΚΠ και την επιχειρησιακή της λειτουργία κρίσιμο ρόλο έχουν τα μητρώα που τηρούνται για την αποθήκευση και διαχείριση των δεδομένων που διακινούνται κατά τη χρήση της ΚΠ. Τα μητρώα που συνοδεύουν την ΚΠ είναι τα ακόλουθα:

1. Εθνικό Μητρώο ΚΠ
2. Μητρώο Προσπελάσεων
3. Μητρώο Ρόλων
4. Μητρώο Παρόχων
5. Επιμέρους Μητρώα Παρόχων Υπηρεσιών
6. Λίστες Ανάκλησης (Revocation Lists, RL)

Στο παρακάτω σχήμα μπορούμε να δούμε τον τρόπο διασύνδεσης των μητρώων. Θα παρατηρήσουμε ότι σκοπίμως τα επιμέρους μητρώα των παρόχων δεν διασυνδέονται με το Εθνικό Μητρώο ΚΠ, προκειμένου να μην υπάρχει η διασύνδεση των δεδομένων, την οποία θέλουμε να αποφύγουμε. Αυτό εξάλλου, όπως αναφέρουμε και προηγουμένως, αποτελεί αφενός σχεδιαστική μας επιλογή, αλλά αφετέρου και συνταγματική απαίτηση. Για κάθε μητρώο, υπάρχει η αντίστοιχη λίστα ανάκλησης, που όπως θα παρατηρήσουμε επικοινωνεί με την λίστα ανάκλησης της Αρχής Πιστοποίησης, προκειμένου να ελέγχεται η εγκυρότητα

των πιστοποιητικών. Είναι προφανές ότι η Αρχή Πιστοποίησης επίσης επικοινωνεί με τα επιμέρους μητρώα καθώς είναι εκείνη που παράγει και διαχειρίζεται τα πιστοποιητικά.



Εικόνα 37- Διασύνδεση Μητρώων

Το **Εθνικό Μητρώο ΚΠ** περιλαμβάνει τα στοιχεία της έκδοσης της ΚΠ (στοιχεία αίτησης, δικαιολογητικά απαιτούμενα για την έκδοση, στοιχεία της Υπηρεσίας έκδοσης, στοιχεία σχετικά με τον χειρισμό και τη διεκπεραίωση της έκδοσης της ΚΠ, όπως τα στοιχεία του αρμόδιου υπαλλήλου), τα δεδομένα της ΚΠ, τα στοιχεία που αναγράφονται στην έντυπη ΚΠ, τις παραμέτρους λειτουργίας του τσιπ, τα δημόσια κλειδιά που είναι αποθηκευμένα στην ΚΠ, τα ψηφιακά πιστοποιητικά και άλλες αποθηκευμένες πληροφορίες. Στο Μητρώο θα τηρούνται επίσης οι αλλαγές στην κατάσταση στην ΚΠ, οι εκδόσεις, οι ανακλήσεις και οι επανεκδόσεις των ΚΠ.

Προκειμένου να διασφαλισθεί η μέγιστη δυνατή εξασφάλιση της προστασίας της πληροφορίας που περιλαμβάνεται και διακινείται με την ΚΠ, είναι αναγκαία η ύπαρξη ενός **Μητρώου Προσπελάσεων**. Στην πραγματικότητα, το μητρώο αυτό θα προκύπτει ως παράγωγο του Μητρώου ΚΠ, και επιπλέον θα τηρεί στοιχεία συναλλαγών και

προσπελάσεων της ΚΠ. Ειδικότερα, από το Μητρώο ΚΠ, θα χρησιμοποιείται ο Αριθμός Εντύπου της ΚΠ, το αναγνωριστικό ανά συναλλαγή και τα στοιχεία της συναλλαγής. Τα στοιχεία της συναλλαγής, συγκεκριμένα, περιλαμβάνουν την υπηρεσία που χρησιμοποιήθηκε, τα στοιχεία του παρόχου της υπηρεσίας που προσπέλασε τα στοιχεία της ΚΠ, ο χρόνος εκτέλεσης της υπηρεσίας και τέλος τα δεδομένα που προσπελάσθηκαν και ο λόγος προσπέλασής τους από την υπηρεσία.

Σε ένα υποσύνολο του μητρώου, το οποίο θα αποτελεί με απλούς όρους το «ιστορικό της κάρτας» θα έχει πρόσβαση ο πολίτης-κάτοχος της ΚΠ για ανάγνωση των στοιχείων των συναλλαγών και της ΚΠ. Όπως και κάθε συναλλαγή στην κατάσταση της ΚΠ. Σε περίπτωση, μάλιστα, που η ΚΠ είναι ενεργή, δηλαδή σε κατάσταση «Έγκυρη», ο πολίτης θα μπορεί να ενεργοποιεί/απενεργοποιεί εφαρμογές και λειτουργίες της ΚΠ, εφόσον εντάσσονται στα λειτουργικά της όρια.

Το **Μητρώο Ρόλων** είναι το μητρώο που περιλαμβάνει τον ορισμό των ρόλων και των δικαιωμάτων πρόσβασης στα δεδομένα και τις λειτουργίες της ΚΠ. Η κυριότερη συμβολή του μητρώου αυτού είναι ο έλεγχος της πρόσβασης στην πληροφορία της ΚΠ. Το μητρώο αυτό, όπως είναι προφανές, πρέπει να είναι ανοιχτό και το περιεχόμενό του δημόσιο, προκειμένου να πληρούνται οι προϋποθέσεις ορθής και ασφαλούς λειτουργίας και εφαρμογής της ΚΠ. Η απόδοση ρόλων και δικαιωμάτων πρόσβασης στους εγγεγραμμένους παρόχους ηλεκτρονικών υπηρεσιών και συναλλαγών πρέπει να λαμβάνει υπόψη το θεσμικό πλαίσιο που διέπει τη λειτουργία τους.

Διακρίνονται οι ακόλουθοι βασικοί ρόλοι:

- Διαχειριστής: Ο διαχειριστής είναι ο ρόλος που μπορεί να έχει πλήρη πρόσβαση σε όλα τα επιμέρους στοιχεία των ΚΠ και μπορεί να αλλάζει και την κατάσταση της ΚΠ.

- Πλήρους Πρόσβασης: Ο ρόλος αυτός αποδίδεται στον ίδιο τον κάτοχο της ΚΠ, ο οποίος έχει δυνατότητα πλήρους πρόσβασης στα στοιχεία της ΚΠ. Ο ρόλος αυτός παρέχει δυνατότητα αλλαγής και στοιχείων της ΚΠ, για τα στοιχεία που είναι μεταβλητά εκτός βεβαίως της κατάστασης της ΚΠ. Επιπλέον, πλήρη πρόσβαση μπορούν να αποκτήσουν υπό προϋποθέσεις αρχές ασφάλειας και ελέγχου.

- Πρόσβαση Ασφάλειας και Ελέγχου : Ο ρόλος αυτός αφορά σε υπηρεσίας ασφάλειας και ελέγχου. Σχετικές τέτοιες υπηρεσίες είναι οι Αστυνομικές Αρχές της χώρας, οι Προξενικές Αρχές, και τα σημεία Διασυνοριακού Ελέγχου. Στην περίπτωση αυτή, επιτρέπεται η πρόσβαση σε εκείνο το σύνολο δεδομένων που αναγράφονται και στην εμπρόσθια όψη της ΚΠ και στο τσιπ, χωρίς να χρειάζεται η συγκατάθεση του πολίτη, μέσω της εισαγωγής του PIN.

- Παρόχου ηλεκτρονικών υπηρεσιών: Ο ρόλος αυτός θα έχει πρόσβαση αποκλειστικά και μόνο στα στοιχεία της ΚΠ, προσωπικά δεδομένα και αναγνωριστικά, που είναι απαραίτητα για την παροχή μιας ηλεκτρονικής υπηρεσίας και απολύτως για τον σκοπό της διεκπεραίωσης της υπηρεσίας. Ο ρόλος αυτός θα είναι διακριτός ανά

τομεακό αναγνωριστικό που χρησιμοποιείται για την εκάστοτε υπηρεσία (ΑΜΚΑ-ΗΔΙΚΑ, ΑΦΜ-ΓΓΠΣ, ΑΔΤ-ΕΛ.ΑΣ., Αρ. Δημοτολογίου-ΥΠΔΜΗΔ & ΟΤΑ).

- Για παράδειγμα, σε υπηρεσία ηλεκτρονικής συνταγογράφησης που παρέχεται από την ΗΔΙΚΑ, θα έχει αποδοθεί ο ρόλος «ηλεκτρονικής διακυβέρνησης - ΑΜΚΑ». Κατά τη χρήση της υπηρεσίας από τον πολίτη θα αξιώνονται προσωπικά στοιχεία του πολίτη, ο ΑΜΚΑ του, αλλά και ο ΑΜΚΑ του φαρμακοποιού. Ο πολίτης θα δηλώνει, μέσω της καταχώρισης του PIN, τη συγκατάθεσή του για τη χρήση από την υπηρεσία του ΑΜΚΑ και των προσωπικών του στοιχείων του, την επεξεργασία των δεδομένων και την παροχή της υπηρεσίας.

- Παρόχου ηλεκτρονικών συναλλαγών: Κατ' αντιστοιχία με τον Πάροχο ηλεκτρονικών υπηρεσιών, το μητρώο αυτό θα αφορά στις συναλλαγές ηλεκτρονικού εμπορίου. Στην περίπτωση αυτή, ο πάροχος ηλεκτρονικών συναλλαγών θα έχει πρόσβαση μόνο στην πληροφορία που αφορά στην ταυτοποίηση και αυθεντικοποίηση του πολίτη και την εγκυρότητα της ΚΠ για την Εκτέλεση μιας συναλλαγής.

Το **Μητρώο Παρόχων** είναι το μητρώο στο οποίο θα περιλαμβάνεται όλη η πληροφορία που αφορά στους παρόχους ηλεκτρονικών υπηρεσιών και συναλλαγών. Στο μητρώο αυτό θα εντάσσονται όσοι φορείς ή/και επιχειρήσεις μπορούν και επιθυμούν να παρέχουν ηλεκτρονικές υπηρεσίες μέσω της χρήσης της ΚΠ. Στο μητρώο αυτό θα καταγράφονται, επίσης, οι υπηρεσίες που παρέχονται από κάθε πάροχο, η περιγραφή των δεδομένων που απαιτούνται για την ολοκλήρωση κάθε υπηρεσίας, και ο σκοπός χρήσης των δεδομένων. Επιπλέον, θα καταχωρίζονται οι ρόλοι που αποδίδονται στον πάροχο από το Μητρώο Ρόλων και τα δεδομένα που δικαιοδοτείται να προσπελαύνει μέσω του ρόλου που του έχει αποδοθεί. Για κάθε πάροχο θα τηρούνται τα στοιχεία του φορέα, της επιχείρησης και του νόμιμου εκπροσώπου της, του υπεύθυνου για την ασφάλεια των υποδομών ΤΠΕ, του υπεύθυνου για τη διαχείριση προσωπικών δεδομένων (όπως ορίσθηκαν για τη δημιουργία των ΟΔΕ των εκάστοτε Υπουργείων και φορέων της Δημόσιας Διοίκησης) καθώς και στοιχεία των σχετικών αδειών λειτουργία της επιχείρησης. Με τη συμμετοχή του φορέα ή της επιχείρησης στο μητρώο αυτό, θα υπογράφονται τα σχετικά SLAs (Service Level Agreements), στα οποία θα ορίζονται οι όροι και οι προϋποθέσεις συμμετοχής στο μητρώο, παροχής ηλεκτρονικών υπηρεσιών μέσω της ΚΠ στον πολίτη και χρήσης δεδομένων, αλλά και οι όροι τήρησης και διαχείρισης των δεδομένων των παρόχων, από την υπηρεσία τήρησης του Μητρώου Παρόχων. Τα δεδομένα που τηρούνται στο Μητρώο Παρόχων και περιγράψαμε παραπάνω, πρέπει να σημειωθεί ότι είναι δημόσια δεδομένα, ελεύθερα προς επισκόπηση από τους πολίτες.

Τα **Επιμέρους Μητρώα Παρόχων Υπηρεσιών** είναι τα μητρώα που κρατούνται επιμέρους από τους φορείς της Δημόσιας Διοίκησης, ή από τις επιχειρήσεις ηλεκτρονικού εμπορίου σε περίπτωση που επεκταθεί η χρήση της ΚΠ και για συναλλαγές ηλεκτρονικού εμπορίου. Τα μητρώα αυτά θα επικοινωνούν με την ΚΠ, κάνοντας αποκλειστικά χρήση του αντίστοιχου αναγνωριστικού που είναι αποθηκευμένο στην ΚΠ (ΑΦΜ, ΑΜΚΑ, ΑΔΤ, Αρ. Δημοτολογίου). Όποια άλλη πληροφορία πιθανά απαιτείται για τη διεκπεραίωση της συναλλαγής βρίσκεται

ήδη στο εκάστοτε μητρώο. Τα μητρώα αυτά τηρούνται επιμέρους στους φορείς, πληρώντας τις προϋποθέσεις του θεσμικού πλαισίου.

Τέλος, θα πρέπει να επισημάνουμε, ότι με την εφαρμογή της ΚΠ στην Ελλάδα η κατεύθυνση για τη διαχείριση των επιμέρους μητρών των παρόχων υπηρεσιών (π.χ. ΓΓΠΣ, ΕΛ.ΑΣ, ΗΔΙΚΑ, Δημοτολόγιο) προκειμένου να συμμορφώνεται και με τον κανόνα περί μη τήρησης περισσότερων στοιχείων από των απαραίτητων για τις ανάγκες και τους σκοπούς της εκάστοτε υπηρεσίας θα πρέπει να στοχεύει στην εξάλειψη στοιχείων που κρατούνται σήμερα και πλέον δεν θα απαιτούνται είτε γιατί αυτά εμπεριέχονται στην ΚΠ ή στο Εθνικό Μητρώο της ΚΠ, είτε εφόσον δεν είναι απαραίτητα κατόπιν χρήσης της ΚΠ.

6.3.3. Διάθεση της ΚΠ

Η ΚΠ θα αφορά κάθε Έλληνα πολίτη που έχει συμπληρώσει το 12^{ο} έτος της ηλικίας του, ακολουθώντας τη λογική του ΑΔΤ και των Ελληνικών διαβατηρίων. Η χρήση της προτείνεται να είναι υποχρεωτική.

Με την έκδοση της ΚΠ και τη διαδικασία προσωποποίησης με τον κάτοχό της ένα σύνολο απαιτούμενων λειτουργιών θα ενσωματώνονται προκειμένου να καθίσταται χρήσιμη σε ηλεκτρονικές υπηρεσίες. Αυτή η λειτουργία, δεν θα προστίθεται στους ανήλικους κατόχους ΚΠ, οι οποίοι θα περιορίζονται σε χρήση μόνο των υπηρεσιών φυσικής ταυτοποίησης και διασυνοριακού ελέγχου.

Ωστόσο, οι ανήλικοι, ηλικιωμένοι και άλλες ειδικές κατηγορίες μπορούν να απολαμβάνουν εξειδικευμένες λειτουργικότητες που θα αφορούν σε υπηρεσίες άμεσης ειδοποίησης σε περιπτώσεις έκτακτης ανάγκης.

Επιπλέον, προτείνεται να περιλαμβάνονται επίσης και τα στοιχεία επικοινωνίας των γονέων και κηδεμόνων για λόγους ασφαλείας.

Η διάρκεια ισχύος της ΚΠ προτείνεται να είναι δέκα (10) έτη από την ημερομηνία έκδοσής της.

6.3.4. Διοικητική Δομή Υποστήριξης της ΚΠ

Η ΕΕΤΤ είναι αρμόδια για την εποπτεία και τον έλεγχο των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης και τηρεί τον Κατάλογο των διαπιστευμένων Παρόχων Υπηρεσιών Πιστοποίησης(CSP) της Ελλάδας.

Ο Κατάλογος των διαπιστευμένων Παρόχων Υπηρεσιών Πιστοποίησης (Trusted Service Provider List, TSL) θα περιλάμβανε όσους είναι εγγεγραμμένοι στο μητρώο της ΕΕΤΤ ως πάροχοι που εκδίδουν πιστοποιητικά και αναγνωρισμένα πιστοποιητικά ηλεκτρονικής υπογραφής, κατά δήλωσή τους. Ένας τέτοιος κατάλογος πρέπει επιπλέον να μπορεί να παρέχει πληροφορίες σχετικά με την κατάσταση εποπτείας/διαπίστευσης των υπηρεσιών πιστοποίησης από τους ΠΥΠ. Εντούτοις, για την Ελλάδα δεν υπάρχουν διαπιστευμένοι ΠΥΠ. Η ΕΕΤΤ, ωστόσο, ακολούθησε μια διαδικασία ελέγχου ειδικά για τους ΠΥΠ που παρέχουν

αναγνωρισμένα πιστοποιητικά (ΑΠΕΔ, Adacom, ASYK) σε συνεργασία με την εταιρεία Ernst & Young.

Οι ΠΥΠ που έχουν ελεγχθεί από την ΕΕΤΤ, εκτός από την ΑΠΕΔ, είναι η εταιρία Adacom Qualified Certificate Services CA και η ASYK Qualified Certificates CA του Χρηματιστήριο Αθηνών ΑΕ. Επιπλέον, η Adacom μέσω του λογισμικού της (Managed certification authority) υποστηρίζει την ΑΠΕΔ και την ΚτΠ ΑΕ, ως αρχή εγγραφής και παρέχε υπηρεσίες διαχείρισης σε άλλους ΠΥΠ.

Στο όλο σχήμα πολύ σημαντικό ρόλο διαδραματίζει η Εθνική Πύλη Δημόσιας Διοίκησης (ΥΔΚ ERMIS, https://pki.ermis.gov.gr/repository.html [100]).

Για το Ελληνικό Δημόσιο και το Υπουργείο Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης το ιεραρχικό σχήμα έχει ως εξής:

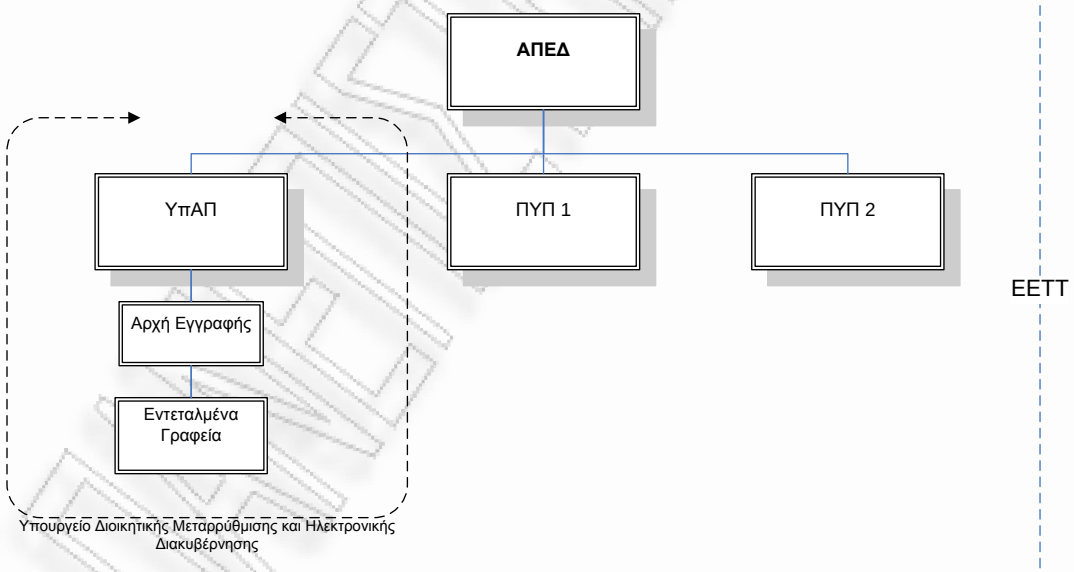
- Η Αρχή Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ) και ειδικότερα η Υπηρεσία Ανάπτυξης Πληροφορικής (ΥΑΠ) της Γενικής Γραμματείας Δημόσιας Διοίκησης & Ηλεκτρονικής Διακυβέρνησης του ΥΠΔΜΗΔ είναι η «Πρωτεύουσα Αρχή Πιστοποίησης» για την Ελλάδα. Η ΑΠΕΔ έχει προσαρμόσει την πολιτική πιστοποίησης στο πρότυπο Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (Πλαίσιο Πολιτικής Πιστοποιητικού Υποδομής Δημόσιου Κλειδιού και Κανονισμών Πιστοποίησης Χ.509 για το Διαδίκτυο), γνωστό και ως RFC 3647, της Ομάδας Δράσης για την Διαδικτυακή Μηχανική (Internet Engineering Task Force), φορέας ο οποίος είναι υπεύθυνος για τον καθορισμό προτύπων στο Διαδίκτυο, για να διευκολύνει την απεικόνιση της εφαρμοζόμενης πολιτικής πιστοποιητικού. Η ΑΠΕΔ είναι αρμόδια για την πιστοποίηση, τον καθορισμό των κατευθύνσεων και το συντονισμό των άλλων δημοσίων υπηρεσιών ή φορέων του δημόσιου τομέα (Υποκείμενες Αρχές Πιστοποίησης), οι οποίοι διαχειρίζονται ψηφιακά πιστοποιητικά και εγγράφονται στο μητρώο Παρόχων Υπηρεσιών Πιστοποίησης της ΕΕΤΤ, σύμφωνα με το άρθρο 10 του υπ' αριθ. 248/71/2002 Κανονισμού Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής (ΦΕΚ 603/Β'). Η ΑΠΕΔ η οποία ενεργεί ως Πρωτεύουσα Αρχή Πιστοποίησης (ΠΑΠ), πιστοποιεί τις Υποκείμενες Αρχές Πιστοποίησης με την έκδοση αντίστοιχων Πιστοποιητικών.
- Η Υποκείμενη Αρχή Πιστοποίησης (ΥπΑΠ) του ΥΠΔΜΗΔ είναι το Τμήμα Επεξεργασίας και Διαρκούς Απογραφής της Διεύθυνσης Προγραμματισμού και Εφαρμογών της Υπηρεσίας Ανάπτυξης Πληροφορικής της Γενικής Γραμματείας Δημόσιας Διοίκησης και Ηλεκτρονικής Διακυβέρνησης του ΥΠΔΜΗΔ. Στην ΥπΑΠ εντάσσονται οι φορείς του δημόσιου τομέα οι οποίοι παρέχουν υπηρεσίες πιστοποίησης σύμφωνα με το άρθρο 20 του Νόμου 3448/2006 (ΦΕΚ 57/Α') και ασκούν αρμοδιότητες για τη διεκπεραίωση των οποίων απαιτείται πιστοποίηση, αλλά και φορείς σύμφωνα με τις διατάξεις της παραγράφου 5 του άρθρου 20 του Νόμου 3448/2006 (ΦΕΚ 57/Α'). Οι ΥπΑΠ εφόσον πιστοποιηθούν από την ΑΠΕΔ, διαχειρίζονται τα πιστοποιητικά τελικών χρηστών σύμφωνα με τις πολιτικές πιστοποιητικών του παρόντος και είτε εκτελούν χρέη έκδοσης και καταχώρησης

πιστοποιητικών, είτε ορίζουν τις οργανικές μονάδες που θα ασκήσουν τις αρμοδιότητες των «Αρχών Εγγραφής» και των «Εντεταλμένων Γραφείων». Οι ΥπΑΠ, αναλαμβάνουν τη διαχείριση του κύκλου ζωής των ψηφιακών πιστοποιητικών (έκδοση, ανάκληση, ανανέωση, ανάκτηση κλπ.), ανάλογα με τη Δήλωση Πρακτικής τους. [99][100]

- Την Αρχή Εγγραφής (ΑΕ) του ΥΠΔΜΗΔ αποτελεί ο Τομέας Υλοποίησης και Παραγωγικής Λειτουργίας Έργων και Συστημάτων της «Κοινωνίας της Πληροφορίας ΑΕ - ΚτΠ Α.Ε.». Οι Αρχές Εγγραφής (ΑΕ) προκειμένου για τη χορήγηση των ψηφιακών Πιστοποιητικών, είναι αρμόδιες για τον έλεγχο των αιτημάτων, των εγγραφών και την επιβεβαίωση των στοιχείων της αιτούντος και είναι εκείνες που ελέγχουν και εισηγούνται την ανάκληση, ανάκτηση, ανανέωση και αναστολή των πιστοποιητικών..

- Ως Εντεταλμένα Γραφεία, ορίζονται τα Κέντρα Εξυπηρέτησης Πολιτών (ΚΕΠ), σε ολόκληρη τη χώρα. Σε κάθε Αρχή Εγγραφής μπορούν να αντιστοιχούν Εντεταλμένα Γραφεία για την επιβεβαίωση – επαλήθευση των στοιχείων ταυτότητας των Τελικών Χρηστών καθώς και την παραλαβή των αιτημάτων και υποστηριζόμενων λειτουργιών του κύκλου ζωής των πιστοποιητικών.

Άλλοι διαπιστευμένοι από την ΕΕΤΤ, ΠΥΠ για τη χώρα είναι η εταιρία Adacom Qualified Certificate Services CA και η ASYK Qualified Certificates CA του Χρηματιστήριο Αθηνών ΑΕ. Στο παρακάτω σχήμα μπορούμε να δούμε και την ιεραρχία των παραπάνω οντοτήτων.



Εικόνα 38-Ιεραρχία Σχήματος Εμπιστοσύνης

Ως Πάροχοι ηλεκτρονικών υπηρεσιών νοούνται όλοι οι φορείς του Ελληνικού Δημοσίου που παρέχουν ηλεκτρονικά υπηρεσίες, όπως ΓΓΠΣ, ΗΔΙΚΑ, ΕΛΑΣ, Δημοτολόγιο, ΟΠΕΚΕΠΕ. Πάροχοι ηλεκτρονικών υπηρεσιών είναι επίσης επιχειρήσεις που δραστηριοποιούνται

ηλεκτρονικά και θα μπορούσαν να παρέχουν υπηρεσίες προς τους πολίτες με τη χρήση της ΚΠ.

Οι πάροχοι υπηρεσιών επικοινωνούν με το παραπάνω σχήμα προκειμένου να αιτηθούν την έκδοση ψηφιακού πιστοποιητικού και να επιβεβαιώσουν την εγκυρότητα ενός άλλου. Με τον ίδιο τρόπο επικοινωνεί και ο πολίτης με τους ΠΥΠ (είτε με το σχήμα για το Ελληνικό Δημόσιο, όπως παρουσιάζεται στο αριστερό μέρος του σχήματος) για να αιτηθεί ψηφιακό πιστοποιητικό.

6.4. Τεχνικά Χαρακτηριστικά ΚΠ

Οι απαιτήσεις που αφορούν στα τεχνικά χαρακτηριστικά της ΚΠ, συνοψίζονται στα ακόλουθα:

α) τον καθορισμό του μορφότυπου και σώματος της ΚΠ με τη σχετική φυσική και λογική ασφάλεια,

β) τις ηλεκτρικές συνδέσεις της ΚΠ,

γ) εκτύπωση ασφάλειας και την προστασία ενάντια στην αντιγραφή,

δ) την εξατομίκευση της ΚΠ και εκτύπωση των στοιχείων ταυτοποίησης του πολίτη στην επιφάνεια της ΚΠ,

ε) τη φυσική προστασία και ασφάλεια της ΚΠ,

στ) τον ποιοτικό έλεγχο.

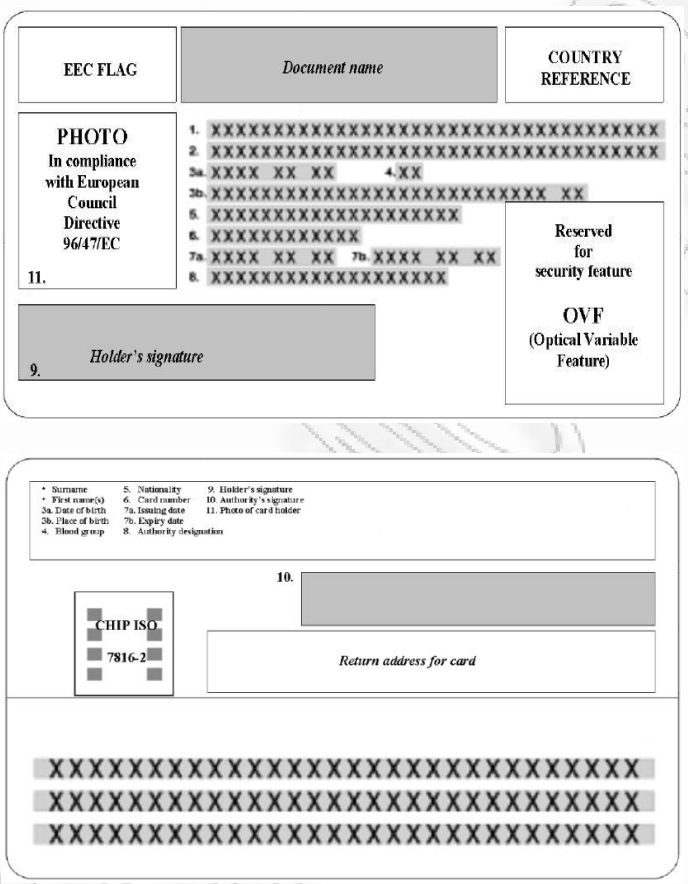
Ουσιαστικά, η εκτύπωση ασφαλείας, η προστασία ενάντια στην αντιγραφή, η εξατομίκευση και ο ποιοτικός έλεγχος θα μπορούσαν να θεωρηθούν ως οι κύριες φάσεις μέσα από τις οποίες περνά η παραγωγή της ΚΠ, προκειμένου να διασφαλισθεί η ασφάλεια της ΚΠ και των δεδομένων που περιέχει, καθώς επίσης και ότι κανένα χαρακτηριστικό γνώρισμα ή τεχνική ασφάλειας δεν παρεμποδίζει την αναγνωσιμότητα της κάρτας από τη συσκευή ανάγνωσης.

Παρακάτω με βάση τις τεχνικές και άλλες απαιτήσεις όπως έχουν προσδιορισθεί σε προηγούμενες ενότητες, καταγράφονται οι προτεινόμενες τεχνικές λύσεις για την εφαρμογή της ΚΠ στην Ελλάδα. Οι επιλογές αυτές βασίζονται στις προδιαγραφές των τεχνολογικών προτύπων που διέπουν την υλοποίηση μιας eID κάρτας. Το CEN/TS 15480 ECC, Part 1(Physical, electrical and transport protocols characteristics), Part 2(Logical data structures and card services), Part 3(ECC Interoperability using an application interface) και Part 4(Recommendations for ECC issuance, operation and use) που προέκυψε από την επιτροπή για την Ευρωπαϊκή ΚΠ (ECC-CEN TC224 WG15).

6.4.1. Μορφότυπος ΚΠ

Ο μορφότυπος ID-1 (ISO/IEC 7810) προτείνεται για την εφαρμογή της Ευρωπαϊκής ΚΠ (CEN 15480-1) και τον ίδιο μορφότυπο εκτιμούμε ότι πρέπει να ακολουθήσουμε στην υλοποίηση της Ελληνικής ΚΠ. Ο μορφότυπος ID-1 έχει διαστάσεις 85.60 X 53.98 mm και χρησιμοποιείται ευρέως στις eID κάρτες και στις τραπεζικές-πιστωτικές κάρτες, καθώς οι διαστάσεις του τον καθιστούν αρκετά βολικό και εύχρηστο.

Η Ελληνική ΚΠ θα πρέπει να ακολουθεί την μορφή που εμφανίζεται στο παρακάτω σχήμα.



Εικόνα 39-Μορφότυπος ΚΠ

6.4.2. Σώμα ΚΠ και Φυσική Προστασία

Για το φυσικό υλικό της κάρτας, έπειτα κι από την επιλογή του ID-1 μορφοτύπου, απαιτείται συμμόρφωση με το πρότυπο ISO/IEC 7810 ID1, αλλά και τα ISO/IEC 7813 και ISO/IEC 7816, Μέρος I.

Σύμφωνα με τις προδιαγραφές του ICAO (έγγραφο 9303 P3V1 [87]) για τα ταξιδιωτικά έγγραφα, η ΚΠ πρέπει να περιλαμβάνει χαρακτηριστικά ασφάλειας και τεχνικές προστασίας ενάντια στην μη εξουσιοδοτημένη αναπαραγωγή, αλλοίωση και παραποίηση. Έτσι, η υλοποίηση της ΚΠ πρέπει να μπορεί να αποκλείει την πλαστογράφηση, προσομοίωση, και τροποποίηση από μη εξουσιοδοτημένους χρήστες, θωρακίζοντάς την από φυσικές επιθέσεις.

Στην κατεύθυνση αυτή η ΚΠ πρέπει να περιλαμβάνει χαρακτηριστικά γνωρίσματα αναγνώσιμα από τον άνθρωπο χωρίς τη χρήση τεχνητών μέσων (επίπεδο επαλήθευσης 1), χαρακτηριστικά γνωρίσματα, η ανάγνωση των οποίων απαιτεί φορητό εξοπλισμό που μπορεί να χρησιμοποιηθεί από μη εκπαιδευμένους υπαλλήλους (επίπεδο επαλήθευσης 2), χαρακτηριστικά γνωρίσματα, η ανάγνωση των οποίων απαιτεί ειδικό εξοπλισμό (επίπεδο επαλήθευσης 3) και τέλος χαρακτηριστικό γνώρισμα γνωστό μόνο στην εκδούσα αρχή και τον κατασκευαστή, το οποίο εξασφαλίζει τη γνησιότητα της ΚΠ και την αντιμετώπιση της πλαστογράφησης (επίπεδο επαλήθευσης 4, forensic taggant).

Ειδικότερα η ΚΠ πρέπει να περιλαμβάνει τα ακόλουθα χαρακτηριστικά γνωρίσματα, τα οποία πρέπει να επισημάνουμε ότι δεν εξυπηρετούν σκοπούς αναβάθμισης της οπτικής παρουσίας της κάρτας, αλλά αύξησης του επιπέδου ασφάλειας:

- τσιπ
- ολόγραμμα
- αναγραφή προσωπικών δεδομένων με εκτύπωση και εγχάραξη με λέιζερ (κείμενο, φωτογραφία)
- πεδίο υπογραφής
- ανάγλυφη αποτύπωση
- αόρατα χαρακτηριστικά γνωρίσματα επικύρωσης (φθορίζοντα στοιχεία)
- εκτύπωση ασφάλειας

Το ευρωπαϊκό πρότυπο CEN/TS 15480 Part 1 καθορίζει το σύνολο αυτών των χαρακτηριστικών ασφαλείας.

Τα αναγραφόμενα προσωπικά δεδομένα της ΚΠ πρέπει να προστατεύονται από παραχάραξη ή παραποίηση και να περιλαμβάνουν χαρακτηριστικά ασφαλείας όπως μικροσκοπική γραφή, εκτύπωση και εγχάραξη με λέιζερ, χρήση μελάνης με υπεριώδη φθορισμό ορατή και αόρατη, ολογραφήματα σχετιζόμενα με στοιχεία κατόχου της κάρτας και μεταβλητά οπτικά στοιχεία (Optical Variable Feature, OVF).

Στο υπόβαθρο θα πρέπει να υπάρχει σχέδιο ασφαλείας, με περίπλοκες παραστάσεις σε δύο τουλάχιστον ειδικούς χρωματισμούς και να περιλαμβάνει μικροσκοπική γραφή, προορισμένο να ανθίσταται σε σάρωση ή αντιγραφή. Το σχέδιο δεν πρέπει να έχει χαρακτηριστικά ψηφιακών εκτυπώσεων, όπως τελείες (dots ή pixels). Το σχέδιο ασφάλειας του υποβάθρου και η φωτογραφία του κατόχου θα έχουν ένα επίπεδο αλληλοκάλυψης.

Για το υλικό που θα χρησιμοποιηθεί στην ΚΠ λαμβάνονται υπόψη οι οδηγίες του ICAO 9303 P3V1 [87] για ηλεκτρονικά και μηχανικά αναγνωρίσιμα ταξιδιωτικά έγγραφα και σχετικά με τις απαιτήσεις που πρέπει να πληρούν και αφορούν στην ανθεκτικότητα στην παραμόρφωση, στην τοξικότητα και την αντίσταση σε χημικές ουσίες, στο αποδεκτό εύρος

θερμοκρασιών και υγρασίας, την ανθεκτικότητα στην έκθεση στο φώς, καθώς επίσης και στη συμβατότητα με τα υπόλοιπα υλικά.

Για την κατασκευή της Ελληνικής ΚΠ προτείνεται η χρήση πολυανθρακικού (Polycarbonate PC) με βάση την αναλογία απόδοσης-κόστους. Το πολυανθρακικό είναι υλικό με μεγάλη διάρκεια ζωής, που φθάνει έως τα 10 έτη και προσφέρει ανθεκτικότητα σε συνθήκες καθημερινής χρήσης, όπως αυτές για τις οποίες προορίζεται η ΚΠ. Είναι άκαμπτο υλικό, με υψηλή αντίσταση σε καταστροφή από θερμότητα (-20°-100° C), κάμψη και τη UV ακτινοβολία, αλλά όχι ιδιαίτερα ανθεκτικό σε καυστικές ουσίες και ορισμένους διαλύτες.

	PVC	PC	PET	ABS
Heat Stability (warpage)	3	1	1	3
Flex Resistance	3	1	1	3
UV Resistance	3	2	1	3
Cost	1	3	2	1
Compatible with Contact Chip	1	1	1	1
Compatible with Contactless Chip	1	2	2	3
Delamination	2	1	1	2
Laser Engravability	3	1	2	3

1 = BEST
2 = BETTER
3 = GOOD

Εικόνα 40- Συγκριτικός πίνακας υλικών ΚΠ

6.4.2.1. Περιγραφή τσιπ

Σχετικά με το υλικό του τσιπ, γενική απαίτηση είναι η πιστοποίηση ασφάλειας σύμφωνα με τα Common Criteria ή τα πρότυπα FIPS. Για λόγους ασφάλειας, σχεδόν όλες οι πλατφόρμες για το τμήμα του προσδιορισμού είναι ακόμα βασισμένες στην EEPROM. Η απαραίτητη μνήμη θα εξαρτηθεί από το επιχειρησιακό μοντέλο και τις λειτουργικές ανάγκες.

Η συμμόρφωση της ΚΠ με τις συστάσεις του ICAO [65], δεδομένης της χρήση της ως ταξιδιωτικό έγγραφο, ορίζει την απαίτηση για ανεπαφικό τσιπ. Το ανεπαφικό τσιπ θα ακολουθεί τις προδιαγραφές του προτύπου ISO/IEC 14443 (proximity chip) και είναι ιδανικό για συνθήκες καθημερινής χρήσης, καθώς προστατεύεται από την τριβή και αποφεύγεται η φθορά και η οξείδωση που είναι δυνατή σε συχνή χρήση στα επαφικά πλινθία.

Η επιλογή του ανεπαφικού τσιπ αποτελεί ασφαλέστερη και μακροπρόθεσμα οικονομικότερη λύση, παρά του μεγαλύτερου κόστους των αναγνωστών των ανεπαφικών καρτών.

Παρόλα αυτά στην επιλογή αυτή, ιδιαίτερη προσοχή κατασκευαστικά πρέπει να δοθεί στην ποιότητα επαφής μεταξύ τσιπ και κεραίας, καθώς η σύνδεση τσιπ-κεραίας μπορεί να σπάσει αν η κόλληση είναι αδύναμη ή η κάρτα εκτεθεί σε υπερβολική κάμψη. Επίσης, κατά την κατασκευή της ΚΠ, είναι πολύ σημαντική η συγκόλληση των διαφορετικών στρωμάτων

της ΚΠ που εσωτερικά φιλοξενούν το τσιπ και την κεραία, ώστε να μην υπάρξει μελλοντικά διαχωρισμός τους.

Το ίδιο τσιπ είναι δυνατό να παρέχει στην κάρτα, τόσο επαφική, όσο και ανεπαφική διεπαφή, αλλά και είναι εφικτή και υβριδική λύση που θα περιλαμβάνει δύο πλινθία με διαφορετικές συνδέσεις. Ωστόσο κάτι τέτοιο δεν θεωρείται σκόπιμο για την Ελληνική ΚΠ δεδομένου ότι ανεβάζει κατακόρυφα το κόστος χωρίς να προσθέτει σε λειτουργικότητα για τις δικές μας απαιτήσεις και επομένως προτείνεται μία μόνο ανεπαφική διεπαφή.

6.4.3. Ασφάλεια ΚΠ και Προστασία της Ιδιωτικότητας

Κάποιες εκ των κύριων απαιτήσεων που καταγράψαμε στην πρώτη ενότητα του παρόντος κεφαλαίου είναι οι απαιτήσεις για ασφάλεια της ΚΠ, προστασίας της πληροφορίας που σχετίζεται με την ΚΠ και διασφάλισης της ιδιωτικότητας του κατόχου της ΚΠ. Στο πλαίσιο αυτό, όπως είναι κατανοητό οποιαδήποτε υποκλοπή ή/και παραχάραξη των δεδομένων της ΚΠ θα έχει ως συνέπεια να τεθούν σε κίνδυνο τα αγαθά και η φήμη του κατόχου. Για το λόγο αυτό η ΚΠ, πρέπει να προστατεύεται με φυσικά και ηλεκτρονικά μέσα, τόσο ως προς την αναγραφόμενη σε αυτήν πληροφορία, όσο και ως προς τα δεδομένα που είναι αποθηκευμένα στο τσιπ της κάρτας. Τα χαρακτηριστικά ασφαλείας που αφορούν στην φυσική προστασία περιγράφηκαν στην προηγούμενη ενότητα, όπου προτάθηκε το υλικό και το σώμα της ΚΠ.

Στην ενότητα αυτή, θα προτείνουμε τις μεθόδους εκείνες που θα προστατεύσουν την πληροφορία που είναι αποθηκευμένη στην ΚΠ, με γνώμονα την εξασφάλιση της ιδιωτικότητας του πολίτη και της προστασίας της ακεραιότητας και εμπιστευτικότητας των προσωπικών του δεδομένων.

Για την προστασία της πληροφορίας του τσιπ απαραίτητη είναι η χρήση ψηφιακών πιστοποιητικών X.509 (RFC 3280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", April 2002) και της συμμόρφωσης με τα ANSI X9.63 ISO/IEC 11770 [96] για την υποδομή δημόσιου κλειδιού (PKI). Επιπλέον, είναι επιβεβλημένη η συμμόρφωση με το CWA 14169(type 2 & 3) με σχήμα προστασίας (protection profile) EAL 4.

Όπως αναλύθηκε εκτενώς στο κεφάλαιο 5 της παρούσας εργασίας, η σημαντικότερη ωφέλεια της χρήση των ψηφιακών πιστοποιητικών είναι ο τρόπος διαχείρισης και διανομής των δημόσιων κλειδιών.

Στην Ελλάδα, σύμφωνα με τον Ν.3448/2006, ως «Πρωτεύουσα Αρχή Πιστοποίησης» ορίζεται η ΥΑΠ του ΥΠΔΜΗΔ, η οποία εκδίδει και αυτοϋπογράφει τα πιστοποιητικά της χώρας (CCSCA). Τα πιστοποιητικά αυτά περιλαμβάνουν το ιδιωτικό κλειδί, με το οποίο υπογράφεται το πιστοποιητικό της Αρχής Έκδοσης της ΚΠ και το δημόσιο κλειδί, το οποίο εισάγεται στο τσιπ της ΚΠ στο αρχικό στάδιο της παραγωγής της μαζί με την εκτύπωση του εθνόσημου.

Τα προσωπικά δεδομένα που αποθηκεύονται στο τσιπ κατά τη διαδικασία της προσωποποίησης της ΚΠ θα εγγράφονται με χρήση των συναρτήσεων σύνοψης και συγκεκριμένα αλγορίθμου SHA-1, που δημιουργεί μια σύνοψη των δεδομένων, ώστε αφενός να μην είναι δυνατή η παραγωγή του αρχικού περιεχομένου από τη σύνοψη και αφετέρου να μην είναι δυνατή η παραγωγή της ίδιας σύνοψης από διαφορετικά σύνολα δεδομένων. Η παραχθείσα σύνοψη, που αντιστοιχεί στα προσωπικά δεδομένα του πολίτη, υπογράφεται με το ιδιωτικό κλειδί της Αρχής Έκδοσης της ΚΠ και αποθηκεύεται στο τσιπ της ΚΠ, ως αντικείμενο ασφαλείας (Document Security Object), μαζί με το δημόσιο κλειδί της Αρχής Έκδοσης της ΚΠ.

Για την παραγωγή διαφορετικού αναγνωριστικού ανά πάροχο υπηρεσίας απαιτείται η εφαρμογή της μεθόδου Restricted Authentication (RA). Στην περίπτωση αυτή πρέπει να είναι επιπλέον ένα ψηφιακό πιστοποιητικό αποθηκευμένο στην ΚΠ, το δημόσιο κλειδί του οποίου θα αποθηκεύεται στο Μητρώο ΚΠ.

Για την ανάγνωση των προσωπικών δεδομένων της ΚΠ εφαρμόζεται πάλι η ίδια μονόδρομη συνάρτηση σύνοψης (SHA-1)και παράγεται μια νέα σύνοψη. Το αντικείμενο ασφαλείας που είναι αποθηκευμένο στο τσιπ της ΚΠ, αποκωδικοποιείται με τη χρήση του δημοσίου κλειδιού της Αρχής Έκδοσης της ΚΠ και το αποτέλεσμα συγκρίνεται με τη σύνοψη. Εάν συμπίπτουν τότε επιβεβαιώνεται η ακεραιότητα των δεδομένων (Passive Authentication).

Επιπλέον ασφάλεια και προστασία από τη μη εξουσιοδοτημένη πρόσβαση θα εξασφαλισθεί συμπληρωματικά με την εφαρμογή του BAC (Basic Access Control), ο οποίος «κλειδώνει» τα δεδομένα του τσιπ. Ο BAC χρησιμοποιείται, μάλιστα, από τις μηχανές ηλεκτρομηχανικής ανάγνωσης ταξιδιωτικών εγγράφων (e-MRTD), που είναι εγκατεστημένες στα σημεία του διασυνοριακού ελέγχου. Κατά την ανάγνωση της ΚΠ, θα γίνεται οπτική σάρωση της MRZ περιοχής και ένα ζεύγος κλειδιών θα δημιουργηθεί προκειμένου να αποκρυπτογραφήσει τα δεδομένα του τσιπ και να κρυπτογραφήσει την επικοινωνία με τον αναγνώστη. Με τη χρήση του BAC, αποτρέπεται η μη εξουσιοδοτημένη ανάγνωση των προσωπικών δεδομένων που αποθηκεύονται στο τσιπ (skimming), βεβαιώνεται η ακεραιότητα και συνέπεια των δεδομένων του τσιπ με τα δεδομένα που αναγράφονται στην ΚΠ και αποτρέπεται η υποκλοπή της επικοινωνίας ΚΠ-αναγνώστη (eavesdropping).

Καθώς όμως, ο BAC είναι σχετικά αδύναμος στην παραγωγή κλειδιών, τα οποία μετά από ένα σημείο μπορεί να γίνουν υπολογιστικά προβλέψιμα, προτείνεται η ενίσχυση με την εφαρμογή της PACE (Password Authentication Connection Establishment), με χρήση μοναδικού αριθμού ασφαλείας (PIN-PUK), ο οποίος θα διασφαλίζει τη ρητή συγκατάθεση του κατόχου της ΚΠ για οποιαδήποτε συναλλαγή.

Για την πρόσβαση, ωστόσο, στα δεδομένα του τσιπ απαιτούνται ασφαλείς αναγνώστες της ΚΠ, καθώς με την εισαγωγή και του PIN θα εξασφαλίζεται πλήρης πρόσβαση στα δεδομένα της ΚΠ. Επομένως, θα εφαρμοσθεί ο μηχανισμός Terminal Authentication (TA) για την αυθεντικοποίηση του συστήματος επιθεώρησης. Ο TA σε συνδυασμό με τον CA (Chip Authentication). Ο CA εξασφαλίζει την αυθεντικότητα της ΚΠ και προστατεύει από την κλωνοποίηση (cloning). Ο TA επιβάλει τον εφοδιασμό των αναγνωστών με ψηφιακά πιστοποιητικά που θα έχουν παραχθεί από την Αρχή Έκδοσης ΚΠ. Οι αναγνώστες αυτοί θα

εφαρμόζουν παράλληλα και το πρωτόκολλο Extended Access Control (EAC) του ICAO, ενώ η αυθεντικοποίησή τους (έμπιστοι αναγνώστες ή μη εμπιστοι) θα γίνεται με εφαρμογή του prEN 14890.

Για τις λειτουργίες των ψηφιακών υπογραφών θα χρησιμοποιηθούν τα πρότυπα prEN 14890 και ISO/IEC 9769-2. Προκειμένου, τέλος, να γίνει ασφαλής χρήση της δυνατότητας της ψηφιακής υπογραφής μέσω της ΚΠ, απαιτείται επιπλέον ένα ψηφιακό πιστοποιητικό και ζεύγος ιδιωτικού-δημόσιου κλειδιού, καθώς και επιπλέον αριθμός ασφαλείας PIN-PUK ειδικά για το σκοπό αυτό.

6.5. Σύνοψη Κεφαλαίου

Η καινοτομία της ηλεκτρονικής ταυτότητας του πολίτη έγκειται κυρίως στις μεθόδους ταυτοποίησης και αυθεντικοποίησης. Η ταυτοποίηση του κατόχου της ΚΠ απαντά επαρκώς στο ερώτημα «ποιος είναι ο κάτοχος» ενώ η αυθεντικοποίηση δίδει απάντηση για το «αν ο κάτοχος της ταυτότητας είναι πράγματι αυτός που ισχυρίζεται ότι είναι».

Υπό την προϋπόθεση ότι η ΚΠ ανταποκρίνεται στις βασικές απαιτήσεις ασφάλειας και προστασίας προσωπικών δεδομένων, συνιστά ένα εξαιρετικά αποδοτικό εργαλείο, τόσο για τον πολίτη, όσο και για τη Δημόσια Διοίκηση.

Η ΚΠ εκτός από έγγραφο ταυτοποίησης εντός και εκτός συνόρων θα αποτελέσει και εισιτήριο για τον ψηφιακό κόσμο, με σημαντική συμβολή στην καθιέρωση των υπηρεσιών ηλεκτρονικής διακυβέρνησης.

Η Ελληνική ΚΠ πρέπει να περιέχει την ελάχιστη δυνατή πληροφορία και να εξασφαλίζει την εξουσιοδοτημένη πρόσβαση αποκλειστικά και μόνο στο τμήμα της πληροφορίας που απαιτείται για μια συναλλαγή. Για το λόγο αυτό απαιτείται να βρεθεί η χρυσή τομή για την πληροφορία που πρέπει να περιέχεται στην ΚΠ, ισορροπώντας ανάμεσα στη ιδιωτικότητας του πολίτη (χρήση ελάχιστης-της απολύτως αναγκαίας- πληροφορίας) και στην ασφάλεια-αξιοπιστία των συναλλαγών. Η εμπιστοσύνη του πολίτη στην ΚΠ και στα συστήματα που τη χρησιμοποιούν είναι καταλυτική για την επιτυχία του εγχειρήματος. Επίσης, η πιστοποίηση των ΚΠ και των αναγνωστών τους, και οι πολιτικές ασφάλειας για την ανάπτυξη και συντήρηση των συστημάτων αποτέλεσαν σημαντικούς παράγοντες για την προτεινόμενη σχεδιαστική επιλογή. Έτσι, δόθηκε ιδιαίτερη βαρύτητα στο σχήμα πιστοποίησης και στην αναγκαιότητά του.

Κλείνοντας, είναι σημαντικό να διαπιστώσουμε ότι η εφαρμογή της ΚΠ στην Ελλάδα πρέπει να είναι εναρμονισμένη με την εθνική μας κουλτούρα, προκειμένου να τύχει υιοθέτησης και διείσδυσης. Εξάλλου, η ελληνική κοινωνία είναι ιδιαίτερα ευαίσθητη με το δικαίωμα της ιδιωτικότητας και έχει αυξημένες ανησυχίες για την καταστρατήγηση θεμελιωδών δικαιωμάτων των πολιτών. Η υποχρεωτική εφαρμογή της ΚΠ δεν θα οδηγήσει απαραίτητα σε επιτυχή υιοθέτησή της από την κοινωνία, που μπορεί σταδιακά να την απαξιώσει. Επομένως, είναι επιθυμητό, τόσο επικοινωνιακά, όσο και ουσιαστικά, τέτοιες ανησυχίες να

καμφθούν. Για το λόγο αυτό, για την προτεινόμενη σχεδιαστική λύση οι εθνικές ιδιαιτερότητες και η ελληνική κουλτούρα ελήφθησαν σοβαρά υπόψη. Εν κατακλείδι, πρέπει πάντα να γνωρίζουμε ότι η βέλτιστη λύση είναι εκείνη που αναγνωρίζει και σέβεται τις κοινωνικές ανάγκες, που έρχεται να υποστηρίξει.

7. ΣΥΜΠΕΡΑΣΜΑΤΑ

7.1. Συμπεράσματα από το Θεσμικό Πλαίσιο

Σχετικά με το νομικό και κανονιστικό πλαίσιο το κυριότερο σημείο που πρέπει να παρατηρήσουμε πριν τα επιμέρους ζητήματα που προκύπτουν από τη μελέτη των θεσμοθετημένων κειμένων, είναι η έλλειψη του θεσμικού πλαισίου για την ηλεκτρονική ταυτοποίηση και την ΚΠ. Στις περισσότερες χώρες δεν υπάρχει επαρκής θεσμική πρόβλεψη για την ΚΠ, καθώς κατά την ενσωμάτωση της οδηγίας για τις ηλεκτρονικές υπογραφές περιορίσθηκαν σε θέματα υποδομής και πολιτικών αυθεντικοποίησης. Αυτός είναι και ένας από τους σημαντικούς λόγους που κάνουν δύσκολη την επίτευξη διαλειτουργικότητας στα συστήματα ηλεκτρονικής ταυτοποίησης.

Οι ηλεκτρονικές υπογραφές αποτελούν αναμφισβήτητα το πιο σημαντικό θεσμικό βήμα στο θέμα της ΚΠ. Όπως όμως ήδη αναφέραμε, η Οδηγία δεν καθορίζει την μονοσήμαντη αναγνώριση μιας οντότητας, δε θίγει το έννομο αποτέλεσμα της αυθεντικοποίησης του και φυσικά δε διευκρινίζει τη νομική συνέπεια ενός πιστοποιητικού αυθεντικοποίησης. Έτσι η ψηφιακή υπογραφή απλώς περιορίζεται, όπως άλλωστε και η ιδιόχειρη, στο να μπορεί, υπό προϋποθέσεις και συμπληρωματικά, να ταυτοποιήσει το υποκείμενο/υπογράφοντα και το αναγνωρισμένο ψηφιακό πιστοποιητικό να μπορεί να επιβεβαιώνει την ταυτότητα αυτού του υποκειμένου. Σε κάθε περίπτωση όμως, η συμβολή της οδηγίας είναι μεγάλη , παρά την έμμεση μόνο εφαρμογή στις υπηρεσίες αυθεντικοποίησης οντοτήτων και στις εφαρμογές ΚΠ. Τεχνικά, πάντως, τα συστήματα PKI προκρίνονται εμμέσως μέσα από τις διατάξεις της οδηγίας, ως κατάλληλη τεχνική λύση για τη διαχείριση των eID.

Ο νόμος περί Ηλεκτρονικής Διακυβέρνησης στοχεύει στη θεσμοθέτηση του δικαιώματος του πολίτη στην ηλεκτρονική επικοινωνία με τη Δημόσια Διοίκηση και στην ηλεκτρονική διεκπεραίωση των συναλλαγών, όπως και η υποχρέωση του κράτους για ηλεκτρονική προσφορά των υπηρεσιών του, καθορίζοντας το πλαίσιο λειτουργίας της Ελληνικής ΚΠ και των υπηρεσιών που θα λειτουργούν συμπληρωματικά με την ΚΠ. Εξάλλου, η διείσδυση και η πλήρης υιοθέτηση της ΚΠ περνάει, σε μεγάλο βαθμό, μέσα από την χρησιμότητά της στις συναλλαγές του πολίτη με το κράτος. Έτσι, είναι σημαντικό να υπάρχουν δομές που θα την υποστηρίξουν και υπηρεσίες που μπορούν να προσφερθούν με την εφαρμογή της.

Επιπλέον, η Οδηγία για τις Υπηρεσίες προσπαθεί να καθορίσει το ευρωπαϊκό πλαίσιο μέσα στο οποίο παρέχονται διαλειτουργικές υπηρεσίες προς τον Ευρωπαίο πολίτη. Είναι όμως ανοιχτό θέμα η δυνατότητα εφαρμογής ενιαίου αξιόπιστου διαλειτουργικού συστήματος ηλεκτρονικής ταυτοποίησης σε επίπεδο Ευρωπαϊκής Ένωσης, μέσα από τις διατάξεις της Οδηγίας, καθώς παρέχεται ικανή ελευθερία στα κράτη μέλη, γεγονός που συνεπάγεται ότι αν ένα αν κάποιο κράτος μέλος δεν επιθυμεί να το εφαρμόσει διακυβεύεται επιτυχία του εγχειρήματος συνολικά .

Το θεσμικό πλαίσιο για την ιδιωτικότητα έχει κρίσιμο ρόλο στο θέμα της εφαρμογής της ΚΠ και δεδομένου ότι έχει αναγνωριστεί η σημασία του προκειμένου για την εγκαθίδρυση σχέσεων εμπιστοσύνης και την προστασία των προσωπικών δεδομένων, το θεσμικό

πλαίσιο κρίνεται επαρκές. Έμφαση δίνεται στη συλλογή, διαχείριση και επεξεργασία των δεδομένων, υπό την ικανοποίηση των αρχών της αναλογικότητας, του σκοπού, της διαφάνειας , της ακρίβειας και της αυθεντικής πηγής, με σεβασμό στην ιδιωτικότητα του πολίτη.

Παρόλα αυτά, σημαντική είναι η ανάγκη στάθμισης του ιδιωτικού και δημόσιου συμφέροντος, η οποία προβλέπεται στο θεσμικό πλαίσιο περί απορρήτου. Οποιαδήποτε λύση αξιολογηθεί για την εφαρμογή της ΚΠ στην Ελλάδα οφείλει να υπακούει σε αυτό το πλαίσιο.

Η επάρκεια όμως του θεσμικού πλαισίου δεν λύνει ζητήματα εμπιστοσύνης, ούτε και κάνει εύκολη τη διαχείριση θεμάτων προσωπικών ή μη δεδομένων, που περιλαμβάνονται στην ΚΠ, ή χρησιμοποιούνται για την υποστήριξή της.

Τέλος, πρέπει να τονίσουμε ότι αν επιθυμούμε να υλοποιήσουμε μια ασφαλή και διαλειτουργική ΚΠ που μπορεί να χρησιμοποιηθεί πλήρως και χωρίς περιορισμούς ως έγγραφο ταυτοποίησης και ως ταξιδιωτικό έγγραφο, πέρα από τη χρήση για ηλεκτρονικές υπηρεσίες είναι απαραίτητη η συμμόρφωση με την κείμενη νομοθεσία και τους κανονισμούς των διεθνών οργανισμών.

7.2. Συμπεράσματα για τη χρήση τεχνολογιών

Η ανάγκη για ηλεκτρονική ταυτοποίηση σε ένα διασυνοριακό περιβάλλον, αλλά και στον ψηφιακό κόσμο οδήγησε σε έκρηξη τεχνολογικών εξελίξεων. Στην περίπτωση της ΚΠ, η χρήση των τεχνολογιών έξυπνης κάρτας είναι απαραίτητη.

Η σωστή κατασκευαστική επιλογή (υλικό κατασκευής και διεπαφή τσιπ) της ΚΠ είναι πολύ σημαντική, καθώς η ανθεκτικότητα και διάρκεια ζωής της κάρτας, η ταχύτητα ανταπόκρισης του τσιπ, η ευχρηστία, η διαθεσιμότητα της υποδομής για τους αναγνώστες κάρτας, η ασφάλεια στην χρήση της, ο έλεγχος πρόσβασης, η προστασία των αποθηκευμένων δεδομένων, το κόστος της λύσης, αλλά και ο συγχρονισμός με μελλοντικές διαφαινόμενες τεχνολογικές εξελίξεις (ανεπαφικό τσιπ, διπλή επαφή) είναι κρίσιμοι παράγοντες που επηρεάζονται και διαφέρουν ανάλογα με τη σχεδιαστική επιλογή. Έτσι, μια τεχνοοικονομική προσέγγιση που να λαμβάνει υπόψη τις ιδιαιτερότητες της χώρας (καιρικές συνθήκες, κλίμα, συνήθειες, κ.α.) είναι απαραίτητη προκειμένου για την επιτυχή εφαρμογή της ΚΠ στην Ελλάδα και από άποψη διείσδυσης, χρηστικότητας και ασφάλειας, αλλά και από άποψη κόστους.

Η χρήση των βιομετρικών στοιχείων ως μοναδικών αναγνωριστικών για την ηλεκτρονική ταυτότητα είναι αλήθεια ότι προσδίδουν αυξημένες εγγυήσεις αξιοπιστίας σε περιπτώσεις ταυτοποίησης, καθώς είναι ιδιαίτερα δύσκολο, μέσω τέτοιων μεθόδων, να αποκρύψει κάποιος την ταυτότητά του ή να χρησιμοποιήσει στοιχεία ενός τρίτου (identity theft).

Ωστόσο, από την μελέτη της εισαγωγής βιομετρικών χαρακτηριστικών σε εφαρμογές ΚΠ, ούτε από άποψη σκοπιμότητας, αλλά ούτε από άποψη εναρμόνισης με την Ελληνική κουλτούρα, προκύπτει αναγκαιότητα εισαγωγής βιομετρικών χαρακτηριστικών για την Ελληνική ΚΠ. Για την ακρίβεια, οι κίνδυνοι και το ρίσκο που φαίνεται να εμφανίζονται τόσο για τη διείσδυση της εφαρμογής της ΚΠ, όσο και από την κακή χρήση των τόσο ευαίσθητων βιομετρικών δεδομένων των πολιτών μάλλον κάνουν απαγορευτική την υιοθέτηση τέτοιων μεθόδων στην εφαρμογή της ΚΠ στην Ελλάδα. Πάντως για να μην υποτιμηθεί ο τρόπος της επιλογής, πρέπει να σημειώσουμε επιπλέον ότι δεν προκύπτουν ούτε ιδιαίτερα σημαντικοί λόγοι που θα μπορούσαν να κάνουν επιτακτική την ενσωμάτωσής τους στην ΚΠ. Εξάλλου, για την αυθεντικοποίηση και ταυτοποίηση του πολίτη αρκετές τεχνολογικές επιλογές μπορούν να προσθέσουν αξιοπιστία και εγγυήσεις στην αυθεντικοποίηση, χωρίς ταυτόχρονα να εκθέτουν ευαίσθητα δεδομένα του υποκειμένου στην μη ορθή και μη εξουσιοδοτημένη χρήση.

Κατ' αντιστοιχία και ίσως με πιο ισχυρά εμπόδια, αντιμετωπίσαμε και τη χρήση της τεχνολογίας RFID. Παρά τις χρήσιμες εφαρμογές που έχει να επιδείξει, οι κίνδυνοι και οι απειλές για την ιδιωτικότητα και τις ελευθερίες του πολίτη, ειδικότερα σε σχέση με τα ανοιχτά ζητήματα ασφάλειας της RFID τεχνολογίας (π.χ. προβλήματα στα βιομετρικά διαβατήρια και τις πιστωτικές κάρτες), μας κάνουν άκρως επιφυλακτικούς στην περίπτωση αξιοποίησής της στην Ελληνική ΚΠ.

Παρόλα αυτά, είναι σημαντικό για την κάθε τεχνολογική επιλογή να γνωρίζουμε εκτός από τις λύσεις που προσφέρει και τα προβλήματα που δημιουργεί. Αλλά ακόμη περισσότερο να μπορούμε να αναγνωρίσουμε τους σκοπούς που επιτελεί η χρήση νέων τεχνολογιών γενικότερα και τις εφαρμογές/χρήσεις που πρέπει και μπορεί να εξυπηρετήσει, καθώς, η εκτεταμένη ή κακή χρήση τέτοιων μεθόδων γεννά έντονους προβληματισμούς για τους κινδύνους από αθέμιτη, καταχρηστική ή αυθαίρετη χρήση αυτού του τόσο ισχυρού εργαλείου.

Οι Αρχές Προστασίας Προσωπικών Δεδομένων των διαφόρων χωρών θα πρέπει να δημιουργήσουν ένα πλαίσιο αρχών για την προστασία της ιδιωτικότητας, την προστασία των προσωπικών δεδομένων και τη διασφάλιση των πολιτικών ελευθεριών και δικαιωμάτων των πολιτών και το οποίο θα ρυθμίζει τις εφαρμογές κάθε νέας τεχνολογίας, μελετώντας τις επιπτώσεις από την χρήση της (π.χ. βιομετρικά χαρακτηριστικά και τεχνολογία RFID) και συμβάλλοντας, παράλληλα, στη βελτίωση και περαιτέρω ανάπτυξή της, αναδεικνύοντας τρωτά σημεία και αδυναμίες.

Η οριοθέτηση της κόκκινης γραμμής ιδιαίτερα εξαιτίας της απουσίας ενός ενιαίου και επαρκούς θεσμικού πλαισίου είναι απολύτως σημαντική, στην κατεύθυνση της στάθμισης της χρήσης μιας νέας τεχνολογικής επιλογής και του σεβασμού των δικαιωμάτων των πολιτών.

7.3. Συμπεράσματα για την ασφάλεια και διαλειτουργικότητα

Η ανάπτυξη και υιοθέτηση προτύπων είναι ένα από τα πιο σημαντικά ζητήματα για την επιτυχή εφαρμογή των λύσεων ΚΠ. Για την Ευρωπαϊκή Ένωση, η ανάπτυξη δράσεων για ενιαία αντιμετώπιση των θεμάτων ηλεκτρονικής ταυτοποίησης και την επίτευξη διαλειτουργικότητας μεταξύ των επιμέρους εθνικών λύσεων έχει ιδιαίτερη βαρύτητα.

Στην κατεύθυνση αυτή, η εξέταση της διεθνούς εμπειρίας είναι καταλυτική, καθώς έχει να επιδείξει ένα σύνολο προδιαγραφών και προτύπων με τα οποία οφείλουν να συμμορφώνονται οι εθνικές εφαρμογές ΚΠ.

Στην κορυφή των προτύπων που εφαρμόζονται στην ΚΠ βρίσκεται Ευρωπαϊκό πρότυπο CEN 15480 και οι συστάσεις του ICAO για τη λειτουργία και προστασία της ΚΠ. Ωστόσο, το πρότυπο διαφοροποιείται από τον ICAO, αναφορικά με το τι προτείνεται ως υποχρεωτικό και τι έχει καθαρά προαιρετικό χαρακτήρα. Εξάλλου, το πρότυπο CEN 15480 αποτελεί μια πιο γενικευμένη τεχνική αναφορά που επιτρέπει την εγκατάσταση επιπλέον εφαρμογών στην κάρτα και έχει ως στόχο να προάγει τη διαλειτουργικότητα, τουλάχιστον σε Ευρωπαϊκό επίπεδο. Πάντως, στην καθυστέρηση στην έκδοση του ενιαίου προτύπου οφείλονται σε μεγάλο βαθμό, τα διαφορετικά τεχνικά χαρακτηριστικά και λειτουργίες των ήδη εφαρμοζόμενων εθνικών λύσεων ΚΠ στα διάφορα κράτη μέλη είχαν ήδη υλοποιήσει eIDs.

Η διασφάλιση της διαλειτουργικότητας σε ένα ενιαίο Ευρωπαϊκό περιβάλλον είναι απαραίτητη προϋπόθεση για τη μετάβαση στην ενιαία ψηφιακή αγορά. Σε αυτό ακριβώς το πλαίσιο, σύγχρονες λύσεις εξασφάλισης της διασυνοριακής διαλειτουργικότητας μεταξύ συστημάτων διαχείρισης ηλεκτρονικών ταυτοτήτων είναι ιδιαίτερα σημαντικές, ώστε να μας οδηγήσουν σε ένα σύγχρονο και επίκαιρο μοντέλο εφαρμογής για την Ελληνική ΚΠ.

Η εξασφάλιση της αμοιβαίας εμπιστοσύνης μεταξύ των συναλλασσομένων μερών σε επίπεδο Ευρωπαϊκής Ένωσης είναι ένα εμπόδιο που πρέπει να ξεπερασθεί. Όπως και να έχει, το συμπέρασμα είναι ότι σε θέματα διαλειτουργικότητας πρέπει να γίνουν ακόμη πολλά.

Σε όλη την εργασία ένα κεντρικό σημείο προβληματισμού αφορούσε στα δικαιώματα του πολίτη και στην αναγκαιότητα στάθμισης δημοσίου συμφέροντος και προστασίας της προσωπικότητας του ατόμου.

Η ασφάλεια και η ιδιωτικότητα είναι ίσως τα πιο κρίσιμα ζητήματα στην ατζέντα. Η ανάγκη για αυξημένη ασφάλεια στα συστήματα αυθεντικοποίησης και ηλεκτρονικής ταυτοποίησης και αξιοπιστία των συστημάτων ΚΠ κάνει τη δημιουργία ενιαίου Ευρωπαϊκού σχήματος εμπιστοσύνης επιβεβλημένη. Η εγκαθίδρυση της εμπιστοσύνης τόσο σε εθνικό επίπεδο (κράτος, πολίτης, επιχειρήσεις), όσο και σε ευρωπαϊκό (κράτη-μέλη, πολίτης, επιχειρήσεις) είναι απολύτως απαραίτητη για τη δημιουργία ενός πραγματικά διασυνοριακού περιβάλλοντος για τον Ευρωπαίο πολίτη και ως εκ τούτου αποτελεί σημαντική πρόκληση για την Ευρώπη του 2020.

Παρά τα αδιαμφισβήτητα οφέλη που συνεπάγεται η χρήση της ΚΠ, δεν μπορούμε να παραγνωρίσουμε τις ευπάθειες και τους κινδύνους που απειλούν την αξιοπιστία του

εγχειρήματος. Η υποκλοπή της μετάδοσης δεδομένων, η παραποίηση των στοιχείων της ΚΠ, η ψηφιακή υπογραφή αλλοιωμένου/μη αυθεντικού εγγράφου, η αποκρυπτογράφηση των αλγορίθμων, οι επιθέσεις στην εμπιστευτικότητα των διακινούμενων πληροφοριών, ο εντοπισμός της τοποθεσίας του χρήστη κατά τη χρήση της ΚΠ (location tracking) είναι μερικές μόνο απειλές που μπορούν να θέσουν σε κίνδυνο την εφαρμογή της ΚΠ.

Για μια ασφαλή ΚΠ, οι μηχανισμοί ασφάλειας των δεδομένων που περιέχονται στην ΚΠ και προτείνονται από τον ICAO και τον BSI, μπορούν να εξασφαλίσουν τη μη διαρροή πληροφοριών από την ΚΠ χωρίς τη συγκατάθεση του κατόχου της (PACE), την εξασφάλιση πρόσβασης μόνο σε έμπιστες οντότητες μέσω της αυθεντικοποιήσης των τερματικών (Terminal Authentication), την απόδειξη γνησιότητας της ΚΠ στο τερματικό μέσω της αυθεντικοποιήσης του τσιπ της ΚΠ (Chip Authentication), την επιβεβαίωση της αυθεντικότητας των δεδομένων του τσιπ (Passive Authentication) και την εμπιστευτικότητα και ακεραιότητα στην επικοινωνία με τη χρήση κρυπτογραφικών μεθόδων (Secure Messaging).

Επιπλέον, η χρήση PKI tokens που υλοποιούνται στο U-Prove της Microsoft και το Idemix της IBM και παρέχουν κρυπτογραφικές τεχνικές που μπορούν να αποφύγουν τη συνδεσιμότητα μεταξύ των αναγνωριστικών που εμφανίζονται σε διάφορες υπηρεσίες ακόμη κι αν οι πάροχοι των υπηρεσιών και η Αρχή Πιστοποίησης μοιράζονται τα δεδομένα (collude) και να ενισχύσουν τον έλεγχο στη χρήση των δεδομένων της ΚΠ (limited show πρωτόκολλα). Ακόμη, παρέχουν λειτουργίες επιλεκτικής αποκάλυψης και δυνατότητες διεθνούς ανάκλησης των πιστοποιητικών του χρήστη διατηρώντας παράλληλα τη μη διασύνδεσή τους (unlinkability).

Διαδεδομένη μέθοδο αποτελεί η χρήση μοναδικών αναγνωριστικών αριθμών ή άλλων στοιχείων της ηλεκτρονικής ταυτότητας. Η χρήση τέτοιων αναγνωριστικών, είτε διαφοροποιώντας μοναδικά τον κάθε πολίτη (citizen specific UIDs) είτε την ίδια την κάρτα ηλεκτρονικής ταυτότητας (card specific UIDs) κατά τρόπο αξιόπιστο μπορεί να παρέχει εγγυήσεις υψηλής ασφάλειας αυθεντικοποίηση του κατόχου, εντούτοις δεν αποτελεί μοναδικό τρόπο εξασφάλισης αξιοπιστίας και ασφάλειας και θέτει σοβαρά ζητήματα ιδιωτικότητας, καθώς υπάρχει εξαιρετικά μεγάλη συγκέντρωση πληροφορίας σε ένα σημείο, γεγονός που προκαλεί επαυξημένους κινδύνους. Για το λόγο αυτό, δεν αποτελεί και σχεδιαστική επιλογή για την παρούσα μελέτη. Αντιθέτως, η χρήση τομεακών αναγνωριστικών (domain specific UIDs), προς ενίσχυση της προστασίας της ιδιωτικότητας του κατόχου της ΚΠ, ώστε να αποφεύγεται εκτεταμένη χρήση του μοναδικού αναγνωριστικού που ενέχει κινδύνους διαρροής .

Οι απειλές ιδιωτικότητας και ασφάλειας, είναι εκείνες που προσδιορίζουν τα σημεία προσοχής, τις αδυναμίες και ευπάθειες που διαμορφώνουν το σύνολο των απαιτήσεων ασφάλειας και των κατάλληλων τεχνολογικών λύσεων. Η υιοθέτηση του κατάλληλου, ανά περίπτωση, μηχανισμού ασφαλείας γίνεται κατόπιν στάθμισης των εννόμων συμφερόντων κράτους – πολίτη, κατ' εφαρμογή των αρχών της αναλογικότητας και σκοπού. Συνεπώς, όποια κι αν είναι η μέθοδος ταυτοποίησης και αυθεντικοποίησης που θα εφαρμοστεί, δε

δύναται να εσωκλείονται πληροφορίες πέραν των όσων είναι απολύτως αναγκαίες για τους σκοπούς της εφαρμογής.

Ωστόσο, η καταπολέμηση όλων των απειλών είναι μάλλον μη ρεαλιστική, αν όχι αδύνατη. Κάποιες απειλές θα είναι πάντα εκεί, γεγονός που καθιστά την αξιολόγηση της βαρύτητάς τους απαραίτητη για την καλύτερη δυνατή επιλογή της ασφαλέστερης σχεδιαστικής λύσης. Η αλήθεια είναι ότι παρά τη σημαντική πρόοδο, ο κίνδυνος από την κακόβουλη χρήση των προσωπικών ή μη δεδομένων της ΚΠ είναι ορατός και σε σημαντικό βαθμό, μη αντιμετωπίσιμος.

Τέλος, πρέπει να τονίσουμε ότι για την βέλτιστη διαχείριση των εφαρμογών ΚΠ είναι απαραίτητη η εναρμόνιση των νομικών, επιχειρησιακών και τεχνικών παραμέτρων. Αυτές οι παράμετροι είναι εκείνες που θα προσδιορίσουν και θα κατευθύνουν τη σχεδιαστική επιλογή για μια λύση ΚΠ σταθμίζοντας συγχρόνως τις ανάγκες και τους κινδύνους και το ιδιωτικό και δημόσιο συμφέρον.

7.4. Κρίσιμα ζητήματα

Στο σημείο αυτό, και έπειτα από την ανάλυση των συμπερασμάτων της παρούσας μελέτης, θα προσπαθήσουμε να συνοψίσουμε τα κρίσιμα στοιχεία για την επιτυχή εφαρμογή και υιοθέτηση της ΚΠ στην Ελλάδα. Τα σημεία αυτά θα αποτελέσουν

1. Εναρμόνιση νομικών επιχειρησιακών και τεχνικών παραμέτρων: Η οποιαδήποτε προτεινόμενη λύση πρέπει να λαμβάνει υπόψη τις νομικές, επιχειρησιακές και τεχνικές απαιτήσεις και να αντιμετωπίζει επαρκώς τα αντίστοιχα ζητήματα. Αυτή ακριβώς αποτέλεσε και τη δική μας προσέγγιση προκειμένου να οδηγηθούμε στην προτεινόμενη σχεδιαστική λύση. Για το λόγο αυτό, το 6^{ο} κεφάλαιο ξεκίνησε με τον ορισμό των απαιτήσεων που πρέπει να πληροί η Ελληνική ΚΠ.

2. Κρίσιμη μάζα: Τόσο για επικοινωνιακού, όσο και για ουσιαστικούς λόγους πρέπει να βρεθεί η κρίσιμη μάζα που θα υποστηρίξει την εφαρμογή της ΚΠ. Η κρίσιμη μάζα θα πρέπει να αναγνωρίζει και να συμμερίζεται την αναγκαιότητα εφαρμογής της ΚΠ. Για το λόγο αυτό πρέπει να είναι μερίδα του πληθυσμού που είναι εξοικειωμένη με τη χρήση των νέων τεχνολογιών, θα τη χρησιμοποιεί σε καθημερινό επίπεδο και θα διευκολυνθεί από τη χρήση της. Άρα, η επιλογή αυτή είναι πολύ σημαντική για την επιτυχία του εγχειρήματος. Με βάση τα παραπάνω, προτείνεται να είναι νέοι ηλικίας 25-40 και επαγγελματικές ομάδες (για παράδειγμα μηχανικοί, δικηγόροι) που θα επωφεληθούν στην καθημερινότητά τους από τη χρήση της ΚΠ.

3. Ασφάλεια: Σε όλη τη μελέτη έχει δοθεί ιδιαίτερη βαρύτητα στην ασφάλεια, την αξιοπιστία και την εμπιστευτικότητα που πρέπει να εξασφαλίζει η προτεινόμενη λύση ΚΠ. Η εμπιστοσύνη του πολίτη στην προτεινόμενη λύση είναι απολύτως αναγκαία, καθώς σε άλλη περίπτωση η ΚΠ δεν θα χρησιμοποιηθεί επαρκώς και θα

δημιουργήσει κινδύνους, που μπορούν να οδηγήσουν σε πλήρη αποτυχία του εγχειρήματος.

4. Χρησιμότητα/Χρηστικότητα: Όπως σημειώσαμε και προηγουμένως, η ανάπτυξη υπηρεσιών ηλεκτρονικής διακυβέρνησης που θα καθιστούν λειτουργική και χρήσιμη την ΚΠ είναι απαραίτητη. Ιδιαίτερη βαρύτητα πρέπει να δοθεί και στην ευχρηστία της ΚΠ.

5. Χρήση ψηφιακής υπογραφής: Πολύς λόγος έχει γίνει για τη χρήση της ψηφιακής υπογραφής στις εφαρμογές ΚΠ. Η λύση που φαίνεται να προκρίνεται, σε αυτό το σημείο είναι η χρησιμοποίησή της μόνο στο τελευταίο βήμα μιας συναλλαγής.

7.5. Ανοιχτά ζητήματα

Στο σημείο αυτό πρέπει να αναγνωρίσουμε ότι στο θέμα της υιοθέτησης της ΚΠ υπάρχουν ανοιχτά ζητήματα σε διεθνές επίπεδο, τα οποία χρήζουν άμεσης αντιμετώπισης, προκειμένου να καταστήσουν τις λύσεις ΚΠ περισσότερο λειτουργικές και ασφαλείς. Στην προσπάθεια να συνοψίσουμε τα ανοιχτά ζητήματα που θεωρούμε πιο σημαντικά και για τα οποία απαιτείται περαιτέρω μελέτη, εντοπίσαμε τα ακόλουθα:

1. Θεσμικό πλαίσιο: Είναι επιτακτική η ανάγκη για επαρκές θεσμικό πλαίσιο που να ορίζει ενιαία την ηλεκτρονική ταυτοποίηση και την ΚΠ, τη διασυνοριακή αναγνώριση, αλλά και την ανάγκη διαλειτουργικότητας μεταξύ των επιμέρους εθνικών συστημάτων ηλεκτρονικής ταυτοποίησης.

2. Εμπιστοσύνη-Ευρωπαϊκό Σχήμα Αρχών Πιστοποίησης: Σε αντιστοιχία με την ανάγκη κάλυψης των κενών του θεσμικού πλαισίου, η καθιέρωση ενιαίου Ευρωπαϊκού σχήματος εμπιστοσύνης (Ιεραρχία Αρχών Πιστοποίησης και Ενιαία Αρχή Πιστοποίησης) είναι απολύτως αναγκαία.

3. ΚΠ για νομικά πρόσωπα: Αν και ήδη υπάρχει πρόβλεψη για τη χρήση της ΚΠ όχι μόνο από φυσικά αλλά και από νομικά πρόσωπα, αυτή περιορίζεται στην απόδοση ρόλων. Ειδικότερα, δεν έχει λυθεί, τουλάχιστον επαρκώς, το ζήτημα της ανάκλησης της ΚΠ στις περιπτώσεις που το υποκείμενο (φυσικό πρόσωπο) που χρησιμοποιεί, μέσω του ρόλου του μια ΚΠ που αντιστοιχεί στο νομικό πρόσωπο που εκπροσωπεί, δεν έχει πλέον δικαίωμα χρήσης της ΚΠ εξαιτίας αλλαγής ρόλου.

4. Ιδιωτικός Τομέας και Τράπεζες : Είναι προφανές ότι για την πλήρη διείσδυση συστημάτων ηλεκτρονικής ταυτοποίησης, ο ιδιωτικός τομέας πρέπει να αποφασίσει και να επιδιώξει τη συμμετοχή του στο εγχείρημα. Επιπλέον , η εμπειρία του ιδιωτικού τομέα είναι άκρως απαραίτητη για την εφαρμογή της ΚΠ. Οι συμπράξεις δημόσιου-ιδιωτικού τομέα είναι πιθανά μια λύση που πρέπει να σκεφθούν σοβαρά τα κράτη-μέλη.

5. Κινητές συσκευές και cloud computing: Η καθολική χρήση των κινητών τηλεφώνων και η ανάγκη για φορητότητα πιστοποιητικών δημιουργούν σημαντικές

προϋποθέσεις για λύσεις ηλεκτρονικής ταυτοποίησης με εφαρμογή σε κινητά τηλέφωνα. Η χρήση της ΚΠ μέσω κινητών τηλεφώνων θα εξασφάλιζε σημαντική ευχρηστία, διαθεσιμότητα και ευκολία στη χρήση από τον κάτοχο/χρήστη κινητού τηλεφώνου. Τέλος, η τεχνολογία cloud computing που είναι ένα πολύ επίκαιρο επιστημονικά θέμα, μπορεί να προσδώσει χαρακτηριστικά ασφαλείας αλλά εγείρει και σημαντικά ερωτήματα, για τα οποία η μέχρι σήμερα τεχνολογικές λύσεις της ΚΠ δεν μπορούν να απαντήσουν ικανοποιητικά.

8. ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Παρατηρητήριο για την Ψηφιακή Ελλάδα, "Βέλτιστες Πρακτικές Χρήσης Τεχνολογιών Πληροφορικής και Επικοινωνιών στο Δημόσιο & Ιδιωτικό Τομέα", Μάιος 2007

[2] Παρατηρητήριο για την Ψηφιακή Ελλάδα, "Διαχείριση Ηλεκτρονικών Ταυτοτήτων στο πλαίσιο της χρήσης Υπηρεσιών Ηλεκτρονικών Συναλλαγών της Δημόσιας Διοίκησης", Απρίλιος 2007

[3] Παρατηρητήριο για την Ψηφιακή Ελλάδα, "Ηλεκτρονική ταυτότητα πολιτών και επιλογές πολιτικής & υποδομών – η Ευρωπαϊκή εμπειρία", Ιούνιος 2010

[4] Παρατηρητήριο για την Ψηφιακή Ελλάδα, "Η Χρήση των ΤΠΕ στον Ευρύτερο Δημόσιο και Ιδιωτικό Τομέα, Παραδοτέο 1: Αναφορά για την Υφιστάμενη Κατάσταση στην Ελλάδα – Συγκέντρωση Κειμένων Στρατηγικής και Σχετικών Μελετών", Οκτώβριος 2007

[5] Δημόσια διαβούλευση για την ηλεκτρονική υπογραφή και ταυτοποίηση, (http://ec.europa.eu/ellada/news/news/20110218electronikiypografi_el.htm), Φεβρούαριος 2011

[6] Forum Ηλεκτρονικής Διακυβέρνησης, (http://www.digitalgreece2020.gr/wp-content/uploads/group-documents/1/1290375833-eGOVForum_Interoperability_FinalReport.pdf), Α' Κύκλος Εργασιών, Νοέμβριος 2006

[7]http://el.wikipedia.org/wiki/%CE%94%CE%B5%CE%BB%CF%84%CE%AF%CE%BF_%CE%B1%CF%83%CF%84%CF%85%CE%BD%CE%BF%CE%BC%CE%B9%CE%BA%CE%AE%CF%82_%CF%84%CE%B1%CF%85%CF%84%CF%8C%CF%84%CE%B7%CF%84%CE%B1%CF%82_(%CE%95%CE%BB%CE%BB%CE%AC%CE%B4%CE%B1)

[8] European Convention on Human Rights (http://en.wikipedia.org/wiki/European_Convention_on_Human_Rights)

[9] E-Government_in_Europe (http://en.wikipedia.org/wiki/EGovernment_in_Europe)

[10] Company History , Diners Club, (https://www.dinersclubus.com/dce_content/aboutdinersclub/companyhistory), Official Web Site

[11] OPEN SC, e-ID IAS (http://www.opensc-project.org/opensc/wiki/IAS-ECC)

[12] e-Business Forum, «Ηλεκτρονικές Υπογραφές και Ηλεκτρονικά Πιστοποιητικά Ταυτοποίησης (Τεχνική & Νομική προσέγγιση), Αθήνα, Μάρτιος 2004

[13] e-Business Forum, «Διαχείριση Ταυτότητας στις Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης», Ια' Κύκλος Εργασιών, Ομάδα Εργασίας Ια5, Αθήνα, Ιούλιος 2007

[14] ΚτΠ Α.Ε. Ελληνικό Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης και Πρότυπα Διαλειτουργικότητας, «Πλαίσιο Ψηφιακής Αυθεντικοποίησης», Έκδοση 2.00, Μαίος 2008

[15] Stallings W., Network Security Essentials: Applications and Standards, Prentice Hall, 2000

[16] Stallings W., Cryptography and Network Security: Principles and Practice, 2nd edition, Prentice Hall, 1999

[17] End to End Trust Progress, (http://www.microsoft.com/mscorp/twc/endtoendtrust/vision/eid.aspx), MS Corporation, Φεβρουάριος 2011

[18] Sergio Sánchez García and Ana Gómez Oliva, "Solving Identity Management and Interoperability Problems at Pan-European Level", ON THE MOVE TO MEANINGFUL INTERNET SYSTEMS: OTM 2009 WORKSHOPS

[19] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, (http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ANNUALREPORTS/AR2009/DPA_ANNUAL_REPORT_2009.PDF), Ετήσια Έκθεση 2009

[20] Paulo S. L. M. Barreto, "Toward a secure public-key blockwise fragile authentication watermarking", IEE Proceedings - Vision, Image and Signal Processing, 2002

[21] Λίλιαν Μήτρου, "Κανονιστικό Πλαίσιο της Κοινωνίας της Πληροφορίας", πανεπιστήμιο Αιγαίου, 2011

[22] Eurosmart, The Voice of the Smart Security Industry, Position Paper, European Citizen Card: One Pillar of Interoperable eID Success,October 2008, available: http://www.eurosmart.com/images/doc/WorkingGroups/e-ID/Papers/ecc-position-paper-final.pdf

[23] Κανονισμός ΕΚ αριθ. 562/2006, «για τη θέσπιση του κοινοτικού κώδικα σχετικά με το καθεστώς διέλευσης προσώπων από τα σύνορα (κώδικας συνόρων του Σένγκεν)», 2006

[24] Κανονισμός ΕΚ αριθ. 1030/2002, «Καθιέρωση αδειών διαμονής ενιαίου τύπου για τους υπηκόους τρίτων χωρών», 2002

[25] Κανονισμός ΕΚ αριθ. 380/2008, «Τροποποίηση του κανονισμού (ΕΚ) αριθ. 1030/2002 για την καθιέρωση αδειών διαμονής ενιαίου τύπου για τους υπηκόους τρίτων χωρών», 2008

[26] Κανονισμός ΕΚ αριθ. 2252/2004, «Καθιέρωση προτύπων για τα χαρακτηριστικά ασφαλείας και τη χρήση βιομετρικών στοιχείων στα διαβατήρια και τα ταξιδιωτικά έγγραφα των κρατών μελών», 2004

[27] Κανονισμός ΕΚ αριθ. 444/2009, «Τροποποίηση του κανονισμού (ΕΚ) αριθ. 2252/2004 του Συμβουλίου σχετικά με την καθιέρωση προτύπων για τα χαρακτηριστικά ασφαλείας και

τη χρήση βιομετρικών στοιχείων στα διαβατήρια και τα ταξιδιωτικά έγγραφα των κρατών μελών», 2009

[28] Νόμος 2672/1998, «Διακίνηση εγγράφων με ηλεκτρονικά μέσα (τηλεομοιοτυπία-ηλεκτρονικό ταχυδρομείο)», ΦΕΚ 290 Α'/28.12.1998

[29] Νόμος 3230/2004, «Καθιέρωση συστήματος διοίκησης με στόχους, μέτρηση της αποδοτικότητας και άλλες διατάξεις», ΦΕΚ 44/11.2.2004

[30] Νόμος 3448/2006, «Παροχή υπηρεσιών πιστοποίησης. Αρχές Πιστοποίησης», ΦΕΚ 57Α΄/15.3.2006

[31] Νόμος 3471/2006, «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997», ΦΕΚ Α' 133/28.06.2006, διαθέσιμος: http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/NOMOTHESIA%20PROSOPIKA%20DEDOMENA/3471_2006.PDF

[32] Νόμος 3536/2007, «Αρμοδιότητες Υπηρεσίας Ανάπτυξης Πληροφορικής της Γενικής Γραμματείας Δημόσιας Διοίκησης και Ηλεκτρονικής Διακυβέρνησης», ΦΕΚ 42/Α'/23.2.2007

[33] Νόμος 3979/2011, «Για την Ηλεκτρονική Διακυβέρνηση και άλλες διατάξεις», 16 Ιουνίου 2011, ΦΕΚ Α' 138

[34] Προεδρικό Διάταγμα 150/2001, «Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές», ΦΕΚ Α' 125/25.6.2001

[35] Προεδρικό Διάταγμα 342/2002 (ΥΕΚ 284 Α΄/22-11-2002), Διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο μεταξύ των δημόσιων υπηρεσιών, ΝΠΔΔ και ΟΤΑ ή μεταξύ αυτών και των φυσικών ή νομικών προσώπων ιδιωτικού δικαίου και ενώσεων φυσικών προσώπων

[36] Εγκύκλιος Αριθ. Πρωτ. ΥΑΠ/Φ.60/10/217 της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) της Γ.Γ. Δημόσιας Διοίκησης & Η.Δ. του ΥΠ.ΕΣ.Δ.Δ.Α., «Εφαρμογή και χρήση ψηφιακής υπογραφής και κρυπτογράφησης στη Δημόσια Διοίκηση», Αθήνα 11 Μαΐου 2007

[37] Υπουργική Απόφαση Αριθ. 3021/19/53, «Τύπος, δικαιολογητικά, αρμόδιες υπηρεσίες και διαδικασία έκδοσης δελτίων ταυτότητας Ελλήνων πολιτών», ΦΕΚ Β' 440/18.10.2005

[38] Τροποποίηση διατάξεων της 3021/22/10/28−6−2005 ΥΑ «Δικαιολογητικά και διαδικασία έκδοσης, τύπος και περιεχόμενο ενδείξεων διαβατηρίου, χρονική ισχύς, αντικατάσταση, απώλεια και ακύρωση αυτών» (Β΄− 932), ΦΕΚ Β' 1298/17.8.2010

[39] Υπουργική Απόφαση 248/71, «Κανονισμός Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής», ΦΕΚ Β' 603/16.5.2002

[40] Υπουργική Απόφαση 2512/2006 «Κύρωση Κανονισμού Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου», ΦΕΚ Β' 1654/10.11.2006

[41] Κοινοτική Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 1999 σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές

[42] Κοινοτική Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών

[43] Κοινοτική Οδηγία 2005/60/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 26ης Οκτωβρίου 2005 σχετικά με την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες και τη χρηματοδότηση της τρομοκρατίας

[44] Κοινοτική Οδηγία 1995/46/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

[45] Κοινοτική Οδηγία 390/2009/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 23ης Απριλίου 2009 για την τροποποίηση της Κοινής Προξενικής Εγκυκλίου περί θεωρήσεων προς τις διπλωματικές και τις έμμισθες προξενικές αρχές όσον αφορά την εισαγωγή βιομετρικών στοιχείων καθώς και διατάξεων για την οργάνωση της παραλαβής και της εξέτασης των αιτήσεων θεώρησης

[46] Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, C 267, 85η σύνοδος ολομέλειας της 9ης και 10ης Ιουνίου 2010, 2010/C 267/01 Ψήφισμα της Επιτροπής των Περιφερειών με θέμα «Βελτίωση των μέσων εφαρμογής της στρατηγικής "ΕΕ 2020": Ολοκληρωμένες κατευθυντήριες γραμμές για τις οικονομικές πολιτικές και τις πολιτικές απασχόλησης των κρατών μελών και της Ένωσης» και 2010/C 267/02 Ψήφισμα της Επιτροπής των Περιφερειών με θέμα «Ισχυρότερη συμμετοχή των τοπικών και περιφερειακών αρχών στη στρατηγική "Ευρώπη 2020"», 1 Οκτωβρίου, 2010, (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:267:FULL:EL:PDF)

[47] COM(2009) 390 τελικό, Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, «Έκθεση για την ψηφιακή ανταγωνιστικότητα της Ευρώπης, Κύρια επιτεύγματα της στρατηγικής i2010 μεταξύ 2005-2009», Βρυξέλλες, 4.8.2009

[48] Ψηφιακό θεματολόγιο για την Ευρώπη βλ. IP/10/581, MEMO/10/199 και MEMO/10/200

[49] European Commission - Information Society - ICT for Government and Public Services: Action Plan 2011-2015, Pre-conditions for Developing eGovernment, 15/12/2010, http://ec.europa.eu/information society/activities/egovernment/action plan 2 011 2015/priorities objectives/developing egovernment/index en.htm

[50] «Μια νέα Ψηφιακή Ατζέντα για την Ευρώπη: 2015.eu», της 5ης Μαΐου 2010 και στη Διακήρυξη της Γρανάδας, που συμφωνήθηκε τον Απρίλιο του 2010.

[51] Συμπεράσματα Digital Agenda Assemply, Βρυξέλλες, 16-17 Ιουνίου 2011, http://ec.europa.eu/information_society/events/cf/daa11/item-display.cfm?id=5983, http://ec.europa.eu/information_society/events/cf/daa11/document.cfm?doc_id=18267, http://ec.europa.eu/information_society/events/cf/daa11/item-display.cfm?id=5998, http://ec.europa.eu/information_society/digital-agenda/daa/index_en.htm.

[52] Ψηφιακή Ελλάδα 2020, «Ψηφιακή Ατζέντα & Ελληνική πραγματικότητα: Προτάσεις στρατηγικής των Θεματικών Ομάδων», Αθήνα, Ιούνιος 2011

[53] ENISA Position Paper, "Privacy Features of European eID Card Specifications", Version 1.0.1, 2009

[54] Dr. Stefan Brands, MIT Press, "Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy", August 2000 , http://www.credentica.com/the_mit_pressbook.html

[55] Deep Dive into U-Prove Cryptographic Protocols, http://channel9.msdn.com/shows/Identity/Deep-Dive-into-U-Prove-Cryptographic-protocols

[56] Microsoft, Credentica, U-Prove SDK, http://www.credentica.com/u-prove_sdk.html, Microsoft U-Prove Ctp Release 2, Microsoft Corporation, February 2011, http://www.microsoft.com/mscorp/twc/endtoendtrust/vision/uprove.aspx

[57] IDEMIX, "What is Identity Mixer?", http://idemix.wordpress.com/

[58] Identity Mixer, Security Group, IBM Research Zurich, "Pseudonymity for E-Transactions", http://www.zurich.ibm.com/security/idemix/ , http://www.zurich.ibm.com/~pbi/identityMixer_gettingStarted/

[59] Arkajit Dey and Stephen Weis, «PseudoID: Enhancing Privacy for Federated Login», Massachusetts Institute of Technology, Cambridge, MA, USA 02139 and Google Inc., Mountain View, CA, USA 94043, http://static.googleusercontent.com/external_content/untrusted_dlcp/research.google.com/el//pubs/archive/36553.pdf

[60] Σημειώσεις Ασφάλεια Δεδομένων στην Κοινωνία της Πληροφορίας, Πανεπιστήμιο Αιγαίου, Καλλονιάτης Χρήστος, 2009, http://www.ct.aegean.gr/people/vkavakli/MIS/slides/Security_&_Privacy_kalloniatis.pdf

[61] Ari Juels, David Molnar, and David Wagner, «Security and privacy issues in e-passports», Cryptology ePrint Archive, Report 2005/095, 2005, http://eprint.iacr.org/

[62] Σημειώσεις Αυθεντικοποίηση Οντότητας, Ενότητα Έλεγχος Πρόσβασης & Επαλήθευση Ταυτότητας

[63] CEN: TC 224/WG 15 – European Citizen Card, Part 1-4, Technical Specification

[64] CEN: TC 224/WG 16 – Application Interface for Smart Cards Used as Secure Signature Creation Devices

[65] ICAO, Machine-readable travel documents, Doc 9303 and Technical Reports, http://mrtd.icao.int/

[66] Comite Reseau de Universite (www.cru.fr), "The ID/STORK EU project", http://www.terena.org/activities/tf-emc2/meetings/9/slides/eid-tfemc2-050907-v2.pdf

[67] STORK, Secure idenTity acrOss boRders linked, http://www.eid-stork.eu, https://www.eid-stork.eu/index.php?option=com_processes&act=list_documents&s=1&Itemid=60&id=312)

[68] PEPPOL, Pan-European Public Procurement Online, http://www.peppol.eu

[69] ModinisIDM, https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/WebHome

[70] Bruegger, B.P., Hohnlein, D., Schwenk, J., "TLS-Federation - a Secure and Relying-Party-Friendly Approach for Federated Identity Management", http://porvoo14.dvla.gov.uk/documents/tls_federation_final.pdf

[71] GUIDE, Creating a European Identity Management Architecture for eGovernment, http://istrg.som.surrey.ac.uk/projects/guide/overview.html

[72] CORDIS, http://cordis.europa.eu/fp6/instr noe.htm

[73] CROBIES: Cross-Border Interoperability of eSignatures, http://ec.europa.eu/information_society/policy/esignature/crobies_study/index_en.htm

[74]ETSI Word Class Standards, Electronic Signature, http://www.etsi.org/WebSite/Technologies/ElectronicSignature.aspx]

[75] FIDIS, Future od Identity in the Information Society, Deliverable 3.12: Federated Identity Management – What's in it for the citizen/customer?, WP3,FIDIS, 10 June 2009, p.12, http://www.fidis.net

[76] PRIME, https://www.prime-project.eu/

[77] PRIMELife, http://www.primelife.eu/

[78] IDABC (Interoperable Delivery of European eGovernment Services), http://ec.europa.eu/idabc/en/document/6484.html

[79] eID Interoperability for PEGS, http://ec.europa.eu/idabc/en/document/6484.html

[80] ISA (Interoperability Solutions for European Public Administrations), http://ec.europa.eu/isa/

[81] BRITE, http://www.briteproject.eu/

[82] SPOCS (Simple Procedures Online for Cross- border Services), http://www.eu-spocs.eu/

[83] Chaum, David, "Blind signatures for untraceable payments", 1983

[84] PKIX Working Group της IETF, X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol – OCSP, http://tools.ietf.org/pdf/draft-ietf-pkix-ocsp-07.pdf , http://datatracker.ietf.org/wg/pkix/charter/

[85] Federal Office for Information Security, "Security mechanisms in electronic ID documents: Country Signer Certificate Authority (CSCA)", https://www.bsi.bund.de/ContentBSI/EN/Topics/ElectrIDDocuments/SecurityMechanisms/PKI/CSCA/securitymechanismsCSCA.htmlBSI, https://www.bsi.bund.de/EN/Home/home_node.html)

[86] BSI TR-03110, "Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents", version 2.00, https://www.bsi.bund.de/cln_183/ContentBSI/EN/Publications/Techguidelines/TR03110/BSITR03110.html

[87] ICAO (International Civil Aviation Organisation), Doc 9303, Part 3 Machine Readable Official Travel Documents, Volume 1 MRtds with Machine Readable Data Stored in Optical Character Recognition Format, 3rd edition, 2008

[88] ICAO (International Civil Aviation Organisation), Doc 9303 Part 3 Machine Readable Official Travel Documents, Volume 2 Specifications for Electronically Enabled MRtds with Biometric Identification Capability, 3rd edition, 2008

[89] ICAO, Guide for Assessing Security of Handling and Issuance of Travel Documents. Version 3.4, January 2010.

[90] ICAO, Guidelines on e-MRTDs & Passenger Facilitation, ver 1.0, April 17, 2008

[91] ICAO, TAG-MRTD, Technical Report Supplemental Access Control, 2009, available: http://www.icao.int/icao/en/atb/meetings/2009/TAGmrtd19/Docs/TagMrtd19-wp04.pdf

[92] Jens Bender, Marc Fischlin, Dennis Kugler, "Security Analysis of the PACE Key-Agreement Protocol", 12th International Information Security Conference (ISC 2009), 2009

[93] Özgür Dagdelen and Marc Fischlin, "Security Analysis of the Extended Access Control Protocol for Machine Readable Travel Documents", ISC, Lecture Notes in Computer Science, Vol. 6531, 2010, http://www.minicrypt.cdc.informatik.tu-darmstadt.de/publications/dagdelen.eac.2010.pdf

[94] European Standard, EN 14890-1, "Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic services", Comité Européen de Normalisation (CEN), Dec 2009

[95] European Standard, EN 14890-2, "Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional services", Comité Européen de Normalisation (CEN), Dec 2009

[96] ISO/IEC 11770-2:2008 —Information technology – Security techniques - Key management- Part 2: Mechanisms using symmetric techniques

[97] Hoepman, J., Hubbers, E., Jacobs, B., Oostdijk, M., and Schreur, R.W., "Crossing Borders: Security and Privacy Issues of the European e-Passport", in Proceedings of IWSEC, 2006

[98] ΥΑ ΥΑΠ/Φ.60/7/135, «Καθορισμός Οργανικών Μονάδων για την παροχή υπηρεσιών πιστοποίησης, σύμφωνα με τις διατάξεις του άρθρου 20 ν. 3448/2006 (ΦΕΚ 57 Α)» ΦΕΚ 445/Β/02-04-2007

[99] Κοινή Υπουργική Απόφαση ΥΑΠ/Φ.60/38/232, «Κύρωση του Κανονισμού Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ).», ΦΕΚ 799/Β/09-06-2010

[100] Εθνική Πύλη Δημόσιας Διοίκησης, Υποδομή Δημοσίου Κλειδιού ermis, https://pki.ermis.gov.gr/repository.html

[101] Σημειώσεις Εισαγωγή στην Κρυπτογραφία, Ψηφιακά Πιστοποιητικά -Υποδομές Δημόσιου Κλειδιού –SSL, Αριστοτέλειο Πανεπιστήμιο,

[102] Ιστοσελίδα ΑΠΔΠΧ, http://www.dpa.gr/portal/page?_pageid=33,14970&_dad=portal&_schema=PORTAL

[103] Guardian, 17-11-2006, http://www.guardian.co.uk/idcards/story/0,,1950226,00.html

[104] DIFRwear, «What is the Problem with RFID/Near Field Communication Technology?» http://www.difrwear.com/

[105] Sergio Sanchez Garcia and Ana Gomez Oliva, —Improvements of pan-European IDM Architecture to Enable Identity Delegation Based on X.509 Proxy Certificates and SAMLE, P. Samarati et al. (Eds.): WISTP 2010, LNCS 6033, pp. 183–198, 2010

ΠΑΡΑΡΤΗΜΑ Ι

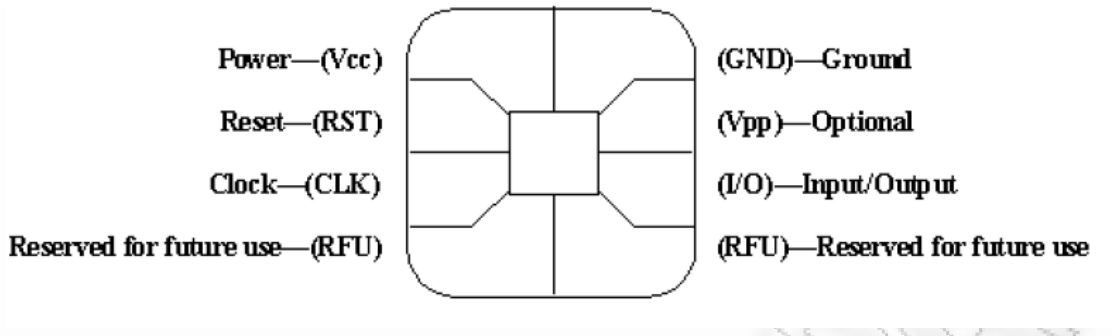
Τεχνικά χαρακτηριστικά των Έξυπνων Καρτών

Μια έξυπνη κάρτα διαθέτει κάποια σημεία επαφής με την CAD, στην επιφάνεια του πλαστικού υποστρώματος, μια κεντρική μονάδα επεξεργασίας, αρκετά είδη μνήμης και σε κάποιες περιπτώσεις ένα ειδικό επεξεργαστή για μαθηματικούς υπολογισμούς.

1.1. Σημεία Επαφής (Contact Pins)

Κάθε κάρτα έχει οκτώ σημεία επαφής με τα οποία συνδέεται στον αναγνώστη καρτών (card reader). Το κάθε ένα επιτελεί την παρακάτω λειτουργία:

- Vcc: Παροχή ενέργειας στο κύκλωμα με τιμές 3 ή 5 Volts
- RST: Χρησιμεύει για την αποστολή σήματος με σκοπό την επαναφορά αρχικών συνθηκών στο μικροεπεξεργαστή (warm reset). Ένας άλλος τρόπος reset είναι διακοπή παροχής ρεύματος και μετά ξανά παροχή, on off, ή η εξαγωγή της κάρτας και μετά ξανά εισαγωγή. Οι δύο τελευταίες περιπτώσεις λέγονται cold reset.
- CLK: Επειδή ο επεξεργαστείς δεν διαθέτουν εσωτερική γεννήτρια ρολογιού το CLK στέλνει το σήμα του εξωτερικού ρολογιού στο εσωτερικό ρολόι.
- GND: Γείωση
- Vpp: Αυτό το σημείο επαφής είναι προαιρετικό και δεν χρησιμοποιείται στις καινούργιες κάρτες. Σε κάποιες παλιές κάρτες ήταν απαραίτητο για τον προγραμματισμό της μνήμης EEPROM
- I/O: Από εδώ γίνεται η μεταφορά τόσο των δεδομένων όσο και των εντολών από και προς την κάρτα με μη ταυτόχρονο τρόπο (half-duplex). Δηλαδή είναι δυνατή η μετάδοση εντολών ή δεδομένων σε μία μόνο κατεύθυνση τη φορά.
- RFU: Προς το παρών δε χρησιμοποιούνται. Υπάρχουν για μελλοντική χρήση.



Εικόνα 41- Τα σημεία επαφής μιας contact smart card

1.2. Μονάδες Επεξεργασίας

Οι έξυπνες κάρτες στο παρελθόν διέθεταν 8-bit μικροελεγκτή (microcontroller) και χρησιμοποιούσαν συνήθως για ρεπερτόριο εντολών το Motorola 6805 ή το intel 8051. Τα τελευταία χρόνια εμφανίστηκε το μειωμένο ρεπερτόριο εντολών (RISC) και 16 ή 32 bit μικροελεγκτής. Ακόμα, οι κάρτες οι οποίες προορίζονται για χρήση σε εφαρμογές ασφάλειας είναι εφοδιασμένες με ένα ειδικό συνεπεξεργαστή (coprocessor) για πολύπλοκες αριθμητικές πράξεις που απαιτούνται από κρυπτογραφικούς αλγόριθμους όπως RSA.

Τα συνολικά συστατικά με τα οποία συνδυαστικά λειτουργεί η μονάδα επεξεργασίας είναι:

- Microprocessor Unit (MPU) : με σκοπό την εκτέλεση προγραμματισμένων οδηγιών ή εντολών. Η παλαιότερη έκδοση Micro controller 8-bit έχει αντικατασταθεί από νεότερο controller με επεξεργαστή 32-bit Reduced Instruction Set Computing - RISC, ο οποίος τρέχει μεταξύ 25 και 32 MHz.

- I/O Controller : με σκοπό την διαχείριση της ροής των δεδομένων μεταξύ του Card Acceptance Device (CAD) και του μικροεπεξεργαστή.

- Read Only Memory (ROM): Αποτελεί τον θεμελιώδη λίθο επί του οποίου δομείται το λειτουργικό σύστημα μιας chip κάρτας (Chip Operating System -COS) και το σημείο στο οποίο βρίσκονται οι μόνιμες οδηγίες για την λειτουργία του.

- Random Access Memory (RAM): Εχει την ίδια λογική με την μνήμη ενός απλού ηλεκτρονικού υπολογιστή, δηλαδή μνήμη ευμετάβλητη που χάνει οποιαδήποτε πληροφορία μετά την διακοπή παροχής ηλεκτρισμού στο chip.

- EEPROM (Electrically Erasable Programmable Read): Εχει δυνατότητα για εγγραφή, διαγραφή και ηλεκτρονική επανεγγραφή.

1.3. Τεχνικά Χαρακτηριστικά Μνήμης

Συνήθως σε μία έξυπνη κάρτα συναντάμε τρία είδη μνήμης ROM, EEPROM και RAM. Πιο ακριβή είναι η EEPROM και πιο φθηνή η ROM. Η RAM είναι αρκετά σπάνια. Παρακάτω παρουσιάζονται τα βασικά χαρακτηριστικά καθώς και η χρησιμότητα της κάθε μνήμης:

- ROM (Read only Memory): Χρησιμοποιείται για την αποθήκευση προγραμμάτων στην κάρτα. Δεν απαιτείται ενέργεια για τη διατήρηση των δεδομένων. Παρόλα αυτά δεν μπορούμε να ξαναγράψουμε κάτι στη μνήμη μετά την κατασκευή της κάρτας. Η ROM μιας έξυπνης κάρτας περιέχει ρουτίνες του λειτουργικού συστήματος, μόνιμα δεδομένα και της εφαρμογές του χρήστη.

- EEPROM (Electrical Erasable Programmable Read Only Memory): Όπως και η ROM έχει την ικανότητα να διατηρεί δεδομένα χωρίς να είναι απαραίτητη η παρουσία ενέργειας. Η διάφορα των δύο αυτών τύπων είναι ότι η EEPROM μπορεί να μεταβληθεί όσες φορές θέλουμε. Έτσι χρησιμοποιείται για την αποθήκευση δεδομένων όπως ο σκληρός δίσκος στον προσωπικό υπολογιστή. Οι εφαρμογές χρήστη μπορούν να γραφτούν στη μνήμη αυτή μετά την κατασκευή της κάρτας. Μία EEPROM σε smart card μπορεί να δεχτεί τουλάχιστον 100,000 κύκλους εγγραφής και να διατηρήσει τα δεδομένα για δέκα χρόνια. Η ταχύτητα ανάγνωσης της είναι περίπου τόσο όσο και της RAM, αρκετά γρήγορη, αλλά η ταχύτητα εγγραφής είναι 1,000 φορές πιο αργή από αυτή της RAM.

Τα τελευταία χρόνια έχουν εμφανιστεί και άλλες τεχνολογίες μνήμης όπως η flash. Αυτή προτιμάται για την αποθήκευση προγραμμάτων ή μεγάλων μπλοκ δεδομένων.

1.4. Λειτουργικά Συστήματα (Smart Card Operating System)

Το λειτουργικό σύστημα μιας έξυπνης κάρτας (COS–Chip Operating System) είναι ένα κομμάτι λογισμικού το οποίο επικοινωνεί με το hardware, τα κυκλώματα της κάρτας, παρέχοντας βασικές λειτουργίες όπως ασφαλή πρόσβαση στα δεδομένα, πιστοποίηση, κρυπτογράφηση. Χωρίς αυτό κάθε εφαρμογή θα έπρεπε να επικοινωνεί απευθείας με το υλικό με αποτέλεσμα η εγγραφή κώδικα για εφαρμογές κάρτας να απαιτούσαν προγραμματισμό πολύ χαμηλού επιπέδου. Διαφορετικά, θα μπορούσαμε να πούμε ότι το λειτουργικό σύστημα της έξυπνης κάρτας είναι μια ακολουθία οδηγιών, που ενσωματώνεται μόνιμα στη ROM της κάρτας και με βάση αυτήν την ερμηνεία προκύπτει η διάκριση των λειτουργικών συστημάτων του CHIP σε δύο οικογένειες:

α) COS γενικού σκοπού: γενικό πλαίσιο εντολών στο οποίο μια ποικιλία εντολών καλύπτει μεγάλο πλήθος εφαρμογών και

β) COS ειδικού σκοπού: εντολές που σχεδιάζονται για συγκεκριμένες εφαρμογές.

Επειδή το λειτουργικό σύστημα φορτώνεται στη μνήμη ROM μιας έξυπνης κάρτας, αυτό θα πρέπει οπωσδήποτε να μην έχει λάθη. Έτσι αν διαπιστωθεί κάποιο σημαντικό λάθος θα

πρέπει να αντικατασταθούν όλες οι κάρτες που έχουν εκδοθεί και η καταστροφή όλων των ICs σε αυτήν τη συγκεκριμένη σειρά παραγωγής. Για να αποφευχθεί αυτό πολλά λειτουργικά συστήματα επιτρέπουν τη χρησιμοποίηση επιπρόσθετων προγραμμάτων διόρθωσης λαθών (patches), έτσι ώστε τα μεγαλύτερα μέρη τους να μπορούν να φορτωθούν μέσα στην EEPROM, εάν πληρούνται οι απαραίτητες συνθήκες ασφαλείας. Παρόλα αυτά, τα λειτουργικά συστήματα των έξυπνων καρτών θα πρέπει να αναπτύσσονται και να ελέγχονται πιο προσεκτικά από ότι τα συμβατικά.

Τα λειτουργικά συστήματα πολλαπλών εφαρμογών υλοποιούνται σε ICs, οι οποίες παρέχουν ικανοποιητική ασφάλεια υλικού που εγγυάται ξεχωριστές περιοχές μνήμης, μπορούν μάλιστα να επιτρέψουν τη φόρτωση μιας καινούργιας εφαρμογής μετά την έκδοση της κάρτας. Αυτό υποστηρίζεται τόσο από το Java Card και το MULTOS όσο και από το Windows for Smart Cards, τα οποία είναι τα πιο σημαντικά λειτουργικά συστήματα έξυπνων καρτών. Υπάρχουν δύο κατηγορίες λειτουργικών συστημάτων:

- Καθορισμένης Δομής Αρχείων (Fixed File Structure): Αυτό το σύστημα μεταχειρίζεται την κάρτα σαν μια ασφαλή μονάδα υπολογισμού και αποθήκευσης δεδομένων. Τα αρχεία αλλά και τα δικαιώματα ορίζονται από τον εκδότη. Για αυτό το λόγο είναι ιδανικό για εφαρμογές που δεν προβλέπεται να χρειαστεί αλλαγή της λειτουργίας τους ή αναβάθμιση στο κοντινό μέλλον.

- Δυναμικό Σύστημα Εφαρμογών (Dynamic Application System): Αυτή η κατηγορία λειτουργικών επιτρέπει ανάπτυξη, τον έλεγχο εφαρμογών οι οποίες μπορούν να συνεργάζονται με ασφάλεια. Εδώ ανήκουν τα δύο πιο γνωστά λειτουργικά συστήματα για έξυπνες κάρτες, το MULTOS και το JAVA card. Υπάρχει σαφέστερος διαχωρισμός του λειτουργικού από τις εφαρμογές και έτσι είναι ευκολότερη η αναβάθμιση των εφαρμογών. Για παράδειγμα η αναβάθμιση της κάρτας SIM για κινητά GSM πραγματοποιείται κατεβάζοντας τη νέα έκδοση αλλάζοντας έτσι τις λειτουργίες της κάρτας δυναμικά.

Οι περισσότεροι κατασκευαστές έξυπνων καρτών προσφέρουν λειτουργικά συστήματα που εφαρμόζουν μερικές ή όλες τις τυποποιημένες εντολές. Αρχικά, υπήρχε αποκλειστικότητα για την ανάπτυξη εφαρμογής λειτουργικού συστήματος και τσιπ για κάθε υπηρεσία, γεγονός που οδηγούσε σε ακριβές και δύσκολες στην αλλαγή λύσεις. Ωστόσο, σήμερα , εμφανίζεται τάση ανάπτυξης ανοικτών λειτουργικών συστημάτων που στηρίζουν πολλαπλές εφαρμογές όπως, JavaCard OS, MultOS και πρόσφατα τα Windows (Διαβούλευση συστημάτων έξυπνων καρτών JCI, 2001).

ΠΑΡΑΡΤΗΜΑ ΙΙ

Κρυπτογραφία

1.1. Η Έννοια της Κρυπτογραφίας

Η κρυπτογραφία χρησιμοποιείται ως χρήσιμο εργαλείο για την ασφάλεια των πληροφοριών, δηλαδή την προστασία των δεδομένων ως προς την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητά τους. Με απλά λόγια, γίνεται απόκρυψη του αρχικού μηνύματος ούτως ώστε, μόνο ο σωστός παραλήπτης να μπορεί να το διαβάσει.

Στην κρυπτογράφηση μετατρέπεται το αρχικό κείμενο (plaintext) σε κρυπτογραφημένο (ciphertext). Η διαδικασία με την οποία αποκρύπτεται η ουσία του περιεχομένου του δηλαδή η πληροφορία που μεταφέρει σε ένα αρχικό μήνυμα (plaintext ή cleartext), ονομάζεται κρυπτογράφηση (encryption). Το plaintext μπορεί να αποτελεί είτε τη μεταφορά είτε την αποθήκευση δεδομένων. Το κρυπτογραφημένο μήνυμα είναι το ciphertext. Η μαθηματική σχέση που περιγράφει τη διαδικασία της κρυπτογράφησης είναι: $E(M) = C$, όπου M το αρχικό μήνυμα και C, το κρυπτογραφημένο.

Η αντίστροφη διαδικασία της κρυπτογράφησης είναι η αποκρυπτογράφηση, που μετατρέπει το κρυπτογραφημένο κείμενο (ciphertext) στην αρχική μορφή του (plaintext). Κατά τη διαδικασία αυτή, η συνάρτηση αποκρυπτογράφησης D επιδρά πάνω στο κρυπτογραφημένο για να παράγει το αρχικό μήνυμα M: $D(C) = M$

Ένας κρυπτογραφικός αλγόριθμος (cipher), είναι η μαθηματική συνάρτηση που χρησιμοποιείται για την κρυπτογράφηση και την αποκρυπτογράφηση [εισαγωγή παραπομπής ορισμού]. Στην κρυπτογραφία εντοπίζονται δύο σχετικές συναρτήσεις, μια για την κρυπτογράφηση και μια για την αποκρυπτογράφηση.

Ένας αλγόριθμος κρυπτογράφησης (Encryption) μετατρέπει τα δεδομένα σε μη αναγνώσιμη μορφή, με σκοπό τη διασφάλιση της εμπιστευτικότητας(confidentiality). Η κρυπτογράφηση προσφέρει το ψηφιακό ισοδύναμο ενός σφραγισμένου φακέλου. Ένας αλγόριθμος αποκρυπτογράφησης (Decryption), αντίστοιχα, αντιστρέφει τη διαδικασία της κρυπτογράφησης, μετατρέπει δηλαδή τα κρυπτογραφημένα δεδομένα στην αρχική τους μορφή.

Δεδομένου ότι η ουσία της κρυπτογράφησης και έπειτα της αποκρυπτογράφησης ενός μηνύματος είναι να ανακτηθεί το αρχικό plaintext, η ακόλουθη σχέση αποδεικνύει αυτό:

$D(E(M)) = M$.

Η σύγχρονη κρυπτογραφία, χρησιμοποιεί ένα κλειδί (key), δηλαδή μια συμβολοσειρά η οποία μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση ή/και αποκρυπτογράφηση, καθώς και για τη δημιουργία ή επαλήθευση ψηφιακής υπογραφής. Τα κρυπτογραφικά κλειδιά μπορεί να χρησιμοποιούνται από συμμετρικούς ή μη συμμετρικούς (δημόσιου κλειδιού) κρυπτογραφικούς αλγορίθμους. Αυτό το κλειδί μπορεί να είναι οποιοδήποτε από

ένα μεγάλο αριθμό τιμών. Η περιοχή των πιθανών τιμών του κλειδιού καλείται keyspace. Με την εισαγωγή του κλειδιού στις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης (αυτό σημαίνει ότι οι συναρτήσεις εξαρτώνται από το κλειδί – έστω δείκτης K), οι συναρτήσεις μεταβάλλονται ως εξής:

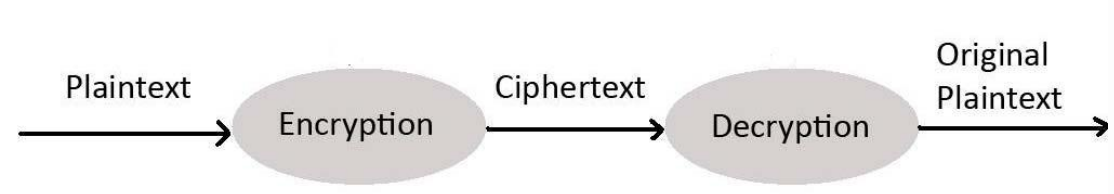
1. Εκ(M) = C
2. Dk(C) = M
3. Dk(Ek(M)) = M

1.2. Είδη Κρυπτογραφίας και Αλγόριθμοι που χρησιμοποιούνται

1. Συμμετρική (Ιδιωτικού κλειδιού): DES (Data Encryption Standard), Triple DES, RC2, Rivest, RC4, Rivest, RC5, Rivest, IDEA (International Data Encryption Algorithm), Lai, Massey
2. Μη Συμμετρική (Δημόσιου κλειδιού): RSA Rivest, Shamir, Adleman, Diffie-Hellman
3. Συναρτήσεις Σύνοψης (Hash Functions): SHA & SHA-1 Secure Hash Algorithm, MD2, MD4, MD5, Rivest

Η κρυπτογραφία μπορεί να εξασφαλίσει λύση σε μια σειρά προβλημάτων, όπως:

- Ασφαλή επικοινωνία
- Ταυτοποίηση και πιστοποίηση
- Κοινοποίηση μυστικής πληροφορίας
- Ηλεκτρονικά πιστοποιητικά
- Ασφαλή πρόσβαση σε υπολογιστικά συστήματα



Εικόνα 42- Κρυπτογράφηση και Αποκρυπτογράφηση

1.3. Βασικές έννοιες στην κρυπτογραφία:

1. Κλειδί (Key): ένας αριθμός που χρησιμοποιείται μαζί με τον αλγόριθμο.
2. Κρυπτογραφικός αλγόριθμος (cipher): αποτελείται από έναν αλγόριθμο κρυπτογράφησης και αποκρυπτογράφησης.
3. Αλγόριθμος Κρυπτογράφησης: Ένας αλγόριθμος Κρυπτογράφησης (Encryption) μετατρέπει τα δεδομένα σε μη αναγνώσιμη μορφή, με σκοπό την διασφάλιση της εμπιστευτικότητας των δεδομένων (confidentiality). Η κρυπτογράφηση προσφέρει το ψηφιακό ισοδύναμο ενός σφραγισμένου φακέλου.
4. Αλγόριθμος Αποκρυπτογράφησης: Ένας αλγόριθμος Αποκρυπτογράφησης (Decryption) αντιστρέφει την διαδικασία της κρυπτογράφησης, μετατρέπει τα κρυπτογραφημένα δεδομένα στην αρχική τους μορφή.
5. Κρυπτογραφικό κλειδί: Η σύγχρονη κρυπτογραφία, χρησιμοποιεί ένα κλειδί (key), δηλαδή μία συμβολοσειρά η οποία μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση ή/και αποκρυπτογράφηση, καθώς και για τη δημιουργία ή επαλήθευση ψηφιακής υπογραφής. Τα κρυπτογραφικά κλειδιά μπορεί να χρησιμοποιούνται από συμμετρικούς ή μη συμμετρικούς (δημόσιου κλειδιού) κρυπτογραφικούς αλγόριθμους.
6. Συμμετρική Κρυπτογράφηση: περιλαμβάνει τους κρυπτογραφικούς αλγόριθμους στους οποίους χρησιμοποιείται το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων. Στη συμμετρική κρυπτογράφηση το κλειδί κρυπτογράφησης/αποκρυπτογράφησης είναι εξ ορισμού μυστικό κλειδί, γνωστό μόνο στους εξουσιοδοτημένους κατόχους.
7. Μη Συμμετρική Κρυπτογράφηση ή Κρυπτογράφηση Δημοσίου Κλειδιού: περιλαμβάνει τους κρυπτογραφικούς αλγόριθμους στους οποίους χρησιμοποιείται ένα κλειδί για κρυπτογράφηση και ένα διαφορετικό κλειδί για την αποκρυπτογράφηση των δεδομένων. Τα κλειδιά αυτά αποτελούν ένα μαθηματικά συνδεδεμένο ζεύγος κλειδιών όπου η γνώση του ενός κλειδιού δεν οδηγεί στην αποκάλυψη του άλλου. Το κλειδί κρυπτογράφησης γνωστοποιείται (συνήθως μέσω ψηφιακού πιστοποιητικού) σε τρίτους και λέγεται δημόσιο κλειδί ενώ το κλειδί αποκρυπτογράφησης είναι γνωστό μόνο στον κάτοχό του και λέγεται ιδιωτικό ή μυστικό κλειδί. Η κρυπτογράφηση Δημοσίου Κλειδιού μπορεί να χρησιμοποιηθεί και για τη δημιουργία και επαλήθευση ψηφιακής υπογραφής.
8. Ψηφιακή Υπογραφή: μία συμβολοσειρά η οποία συνοδεύει ηλεκτρονικά δεδομένα

ή αρχεία και μπορεί να χρησιμοποιηθεί για την επαλήθευση της ακεραιότητάς τους, καθώς και για τον καταλογισμό ευθύνης (non repudiation). Για τη δημιουργία/επαλήθευση ψηφιακών υπογραφών χρησιμοποιείται κρυπτογράφηση δημόσιου κλειδιού. Το ιδιωτικό

κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το δημόσιο κλειδί για την επαλήθευση της υπογραφής.

1. Ψηφιακό Πιστοποιητικό: ένα ψηφιακό έγγραφο το οποίο χρησιμοποιείται στην κρυπτογραφία Δημόσιου Κλειδιού, για να πιστοποιήσει την αυθεντικότητα των

2. δημόσιων κλειδιών των χρηστών. Ένα ψηφιακό πιστοποιητικό περιλαμβάνει το δημόσιο κλειδί ενός χρήστη, το όνομα του κατόχου του, τους χρησιμοποιούμενους αλγόριθμους και διάφορες άλλες πληροφορίες σχετικά με τον κάτοχο του κλειδιού. Για να είναι έγκυρο ένα ψηφιακό πιστοποιητικό, είναι υπογεγραμμένο από κάποια Αρχή Πιστοποίησης και περιλαμβάνει μια ημερομηνία λήξης (ή Περίοδο Ισχύος).

3. Αρχή Πιστοποίησης: είναι μία οντότητα η οποία έχει το δικαίωμα να εκδίδει και να ανακαλεί ψηφιακά πιστοποιητικά. Μία Αρχή Πιστοποίησης θα πρέπει να κατέχει και η ίδια ένα ζεύγος κλειδιών για την υπογραφή των πιστοποιητικών που εκδίδει. Το δημόσιο κλειδί της Αρχής Πιστοποίησης θα πρέπει να είναι υπογεγραμμένο είτε από την ίδια την Αρχή Πιστοποίησης (αυτό-υπογεγραμμένο πιστοποιητικό) είτε από κάποια άλλη Αρχή Πιστοποίησης (π.χ. σε ένα ιεραρχικό σύστημα – Υποδομή Δημόσιου Κλειδιού).

4. Ασφάλεια του κρυπτογραφικού συστήματος: Η ασφάλεια ενός κρυπτογραφικού συστήματος δε βασίζεται στη μυστικότητα του αλγόριθμου αλλά στη μυστικότητα του κλειδιού (στους αλγόριθμους δημοσίου κλειδιού η ασφάλεια βασίζεται στη μυστικότητα του ιδιωτικού κλειδιού). Αν ένα μυστικό η ιδιωτικό κλειδί αποκαλυφθεί, τότε τα μηνύματα που είναι κρυπτογραφημένα με το κλειδί αυτό μπορούν να αποκρυπτογραφηθούν. Σε ένα σύστημα ψηφιακής υπογραφής, αν κάποιος τρίτος αποκτήσει (μη εξουσιοδοτημένη) πρόσβαση στο ιδιωτικό κλειδί μπορεί να υπογράψει ηλεκτρονικά δεδομένα, υποδυόμενος το νόμιμο κάτοχο του κλειδιού.

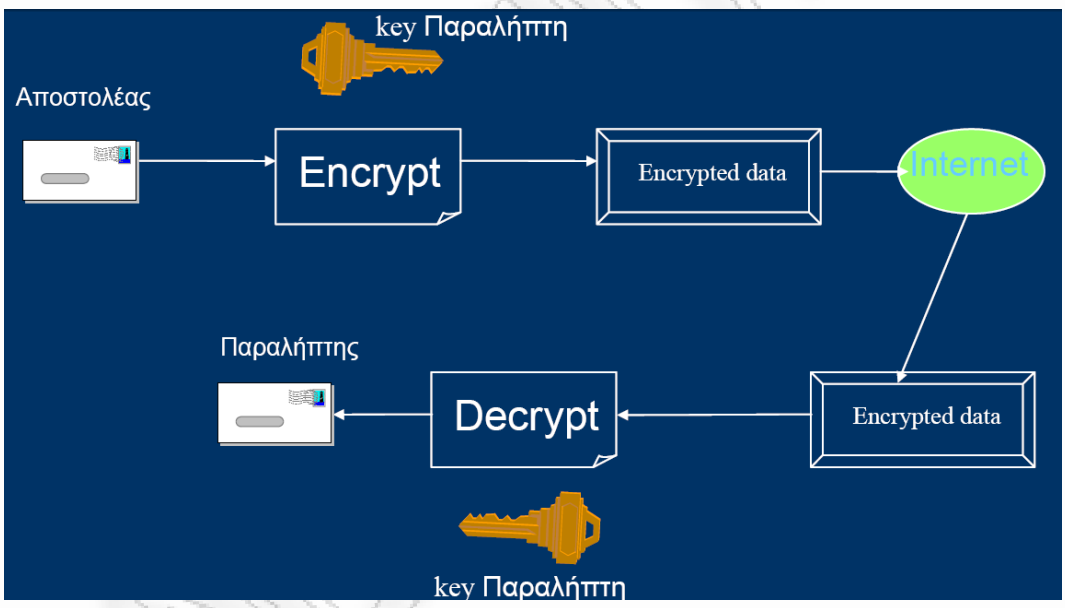
1.4. Συμμετρική Κρυπτογραφία

Η συμμετρική κρυπτογραφία symmetric cryptography) ή κλασική ή συμβατική κρυπτογραφία (conventional cryptography) ή κρυπτογραφία μυστικού κλειδιού (secret key cryptography), σύμφωνα με τη σχετική βιβλιογραφία αποτελείται ουσιαστικά από αλγόριθμους κρυπτογράφησης ενός μυστικού κλειδιού. Στη συμμετρική κρυπτογραφία, το ίδιο κλειδί χρησιμοποιείται, τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση των δεδομένων του μηνύματος κι επομένως τα συναλλασσόμενα μέρη πρέπει να συμφωνήσουν εκ των προτέρων για το κλειδί που θα χρησιμοποιηθεί.

Έτσι, οι κύριες συνιστώσες στη συμμετρική κρυπτογραφία είναι:

- Αρχικό κείμενο (plaintext): Τα αρχικά δεδομένα (μήνυμα) που εισάγονται στον αλγόριθμο κρυπτογράφησης.

- Αλγόριθμος κρυπτογράφησης (encryption algorithm): Ο μετασχηματισμός του αρχικού κειμένου για την κρυπτογράφηση ενός μηνύματος.
- Μυστικό κλειδί (secret key): Οι ακριβείς αντικαταστάσεις και τα αποτελέσματα των μετασχηματισμών που επιτελούνται από τον αλγόριθμο εξαρτώνται από αυτό το μυστικό κλειδί, το οποίο εισάγεται επίσης στον αλγόριθμο κρυπτογράφησης.
- Κρυπτογραφημένο μήνυμα ή κρυπτογράφημα (ciphertext): Το μετασχηματισμένο μήνυμα που παράγεται ως έξοδος από τον αλγόριθμο κρυπτογράφησης και το οποίο εξαρτάται τόσο από το αρχικό μήνυμα όσο και από το μυστικό κλειδί. Για ένα μήνυμα, διαφορετικά κλειδιά παράγουν διαφορετικά κρυπτογραφήματα.
- Αλγόριθμος αποκρυπτογράφησης (decryption algorithm): Η παραγωγή του αρχικού κειμένου από το κρυπτογράφημα και το μυστικό κλειδί που χρησιμοποιήθηκε στη διαδικασία της κρυπτογράφησης.



Εικόνα 43- Συμμετρική Κρυπτογραφία

Για την ασφαλή χρήση της συμμετρικής κρυπτογραφίας, απαιτείται η ύπαρξη ενός ισχυρού αλγορίθμου κρυπτογράφησης. Ειδικότερα, μάλιστα, ο αλγόριθμός που χρησιμοποιείται πρέπει να εξασφαλίζει ότι ο επιτιθέμενος πρέπει να είναι αδύνατο να κρυπταναλύσει το κρυπτογραφημένο μήνυμα ή να ανακαλύψει το κλειδί, ακόμη και αν κατέχει κάποια κρυπτογραφήματα μαζί με τα αντίστοιχα αρχικά μηνύματα. Επιπλέον, ιδιαίτερα σημαντική είναι η μεταφορά και αποθήκευση του μυστικού κλειδιού, ώστε να μην είναι εφικτή η χρήση του από μη εξουσιοδοτημένο χρήστη με σκοπό την αποκάλυψη της επικοινωνίας. Για το λόγο αυτό, είναι κρίσιμο τα δύο συναλλασσόμενα μέρη να παραλαμβάνουν τα αντίγραφα του μυστικού κλειδιού με ασφαλή τρόπο και να το φυλάσσουν σε ασφαλές

μέρος. Αν κάποιος γνωρίζει τον αλγόριθμο και ανακαλύψει το κλειδί, τότε όλη η επικοινωνία που χρησιμοποιεί αυτό το κλειδί είναι αναγνώσιμη, συνεπώς παραβιάζεται η εμπιστευτικότητα.

Κατά συνέπεια, το πιο ισχυρό σημείο αδυναμίας της συμμετρικής κρυπτογραφίας δεν είναι η μυστικότητα του αλγορίθμου, αλλά η μυστικότητα του κλειδιού. Εντούτοις, παρά τα ζητήματα μυστικότητας που μπορούν να προκύψουν από την ανταλλαγή του μυστικού κλειδιού και την αυθεντικοποίηση των συναλλασσόμενων μερών, η ταχύτητα και το χαμηλό κόστος αποτελούν σημαντικά πλεονεκτήματα της μεθόδου.

Ο κυριότερος συμμετρικός αλγόριθμός είναι ο DES (Data Encryption Standard), που ακολουθεί τη λογική κρυπτογράφησης τμημάτων (block ciphers), δηλαδή την επεξεργασία της εισόδου του αρχικού κειμένου σε σταθερού μεγέθους τμήματα, για την παραγωγή κρυπτογραφημάτων ίδιου μεγέθους για οποιοδήποτε τμήμα αρχικού κειμένου. Οι βασικοί αλγόριθμοι, που ακολουθούν τη λογική της κρυπτογράφησης τμημάτων, έχουν οδηγήσει στην ανάπτυξη του DES και του Triple DES (3DES). Άλλος σημαντικός συμμετρικός αλγόριθμος είναι ο AES (Advanced Encryption Standard) και άλλοι γνωστοί συμμετρικοί αλγόριθμοι είναι οι IDEA (International Data Encryption Algorithm), Blowfish, RC2, RC3, RC4 (ARCFOUR), RC5, RC6, SAFER και CAST-128.

1.5. Ασύμμετρη (Δημόσιου Κλειδιού) Κρυπτογραφία

Η κρυπτογράφηση δημοσίου κλειδιού (public-key encryption) εμφανίστηκε το 1976 από τους W.Diffie και M.Hellman και υπήρξε ένα εξόχως σημαντικό βήμα στην περαιτέρω διάδοση της κρυπτογραφίας. Οι αλγόριθμοι κρυπτογραφίας δημοσίου κλειδιού βασίζονται σε μαθηματικές συναρτήσεις και όχι σε απλές πράξεις με bit.

Σε αντίθεση με τη συμμετρική κρυπτογραφία, η ασύμμετρη κρυπτογραφία αντικαθιστά το κοινό μυστικό κλειδί με ένα ζεύγος κλειδιών που αποτελείται από το ιδιωτικό κλειδί (private key) και το δημόσιο κλειδί (public key). Τα δύο κλειδιά σχετίζονται μεταξύ τους με μονόδρομες συναρτήσεις (one-way functions) και η χρήση τους επιφέρει σημαντικές τροποποιήσεις σε θέματα που σχετίζονται με την εμπιστευτικότητα, την αυθεντικότητα και τη διανομή των κλειδιών.

Με την προϋπόθεση ότι όλοι οι συμμετέχοντες έχουν πρόσβαση στα δημόσια κλειδιά, τα ιδιωτικά κλειδιά παράγονται τοπικά για τον κάθε συναλλασσόμενο

Η διαδικασία έχει ως εξής, τα δεδομένα που κρυπτογραφούνται με το δημόσιο κλειδί (που χρησιμοποιείται για δημόσια χρήση) και αποκρυπτογραφούνται αποκλειστικά με το ιδιωτικό μυστικό κλειδί (που χρησιμοποίείται αποκλειστικά από τον κάτοχό του). Το δημόσιο κλειδί είναι διαθέσιμο στο κοινό, ενώ το ιδιωτικό κλειδί είναι γνωστό μόνο σε μία φυσική οντότητα. Να σημειωθεί επίσης ότι είναι υπολογιστικά αδύνατο να υπολογιστεί το κλειδί της αποκρυπτογράφηση από τη γνώση του κλειδιού κρυπτογράφησης και του αλγορίθμου που χρησιμοποιήθηκε.

Τα βήματα που ακολουθούνται είναι τα ακόλουθα:

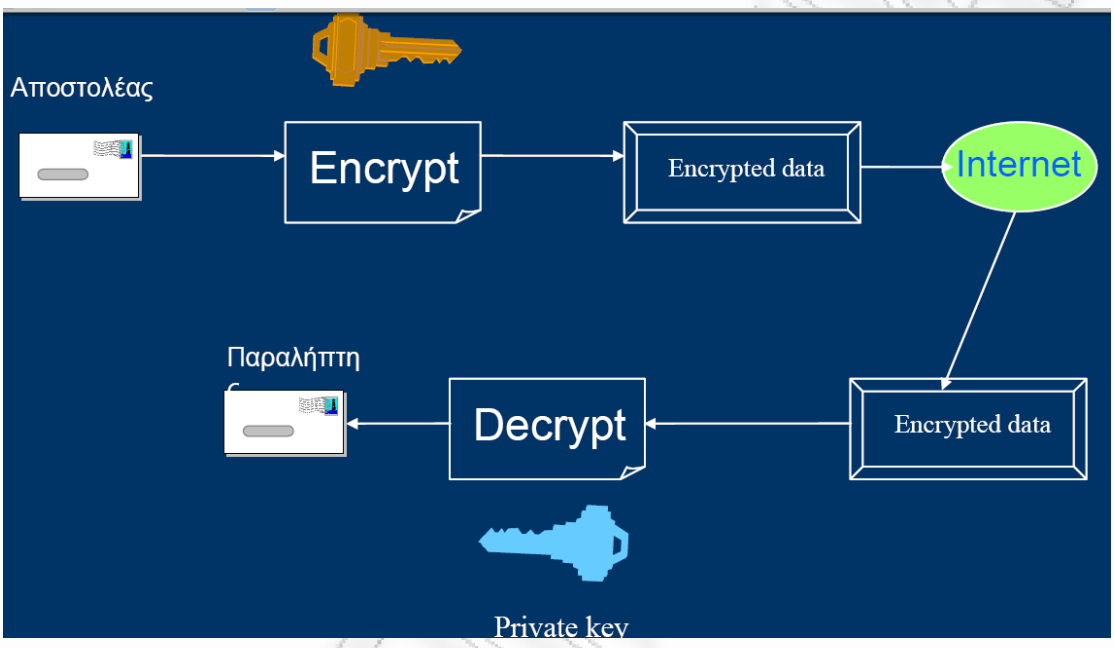
- Για κάθε χρήστη παράγεται ένα ζεύγος κλειδιών που χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση των μηνυμάτων.
- Κάθε χρήστης τοποθετεί το δημόσιο κλειδί σε μία βάση δεδομένων ενός φορέα ή σε κάποιο άλλο δημόσια προσβάσιμο αρχείο. Για λόγους λειτουργικότητας,

  απαιτείται κάθε χρήστης να είναι σε θέση να ανακτήσει εύκολα τα δημόσια κλειδιά άλλων.
- Ο χρήστης που επιθυμεί να αποστείλει ένα μήνυμα, κρυπτογραφεί το μήνυμά του με το δημόσιο κλειδί του παραλήπτη.
- Ο παραλήπτης λαμβάνει το κρυπτογραφημένο μήνυμα και το αποκρυπτογραφεί με το ιδιωτικό του κλειδί. Η αποκρυπτογράφηση μπορεί να γίνει μόνο με τη χρήση του ιδιωτικού κλειδιού, που σχετίζεται μοναδικά με το αντίστοιχο δημόσιο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση, και αποκλειστικά μόνο από τον επιθυμητό παραλήπτη.

Έτσι, κατ' αναλογία με τη συμμετρική κρυπτογραφία, οι κύριες συνιστώσες στην ασύμμετρη κρυπτογραφία είναι:

- Αρχικό κείμενο (plaintext): είναι το μη κρυπτογραφημένο μήνυμα που αποτελεί στοιχείο εισόδου στον αλγόριθμο κρυπτογράφησης.
- Αλγόριθμος κρυπτογράφησης (encryption algorithm): ο αλγόριθμος με τον οποίο πραγματοποιούνται οι διάφοροι μετασχηματισμοί στο αρχικό μήνυμα.
- Ζεύγος κλειδιών (key pair): Ζεύγος κλειδιών, όπου το δημόσιο κλειδί του παραλήπτη χρησιμοποιείται για την κρυπτογράφηση και το ιδιωτικό κλειδί του για την αποκρυπτογράφηση. Οι ακριβείς μετασχηματισμοί πραγματοποιούνται από τον αλγόριθμο κρυπτογράφησης/αποκρυπτογράφησης, εξαρτώμενοι από τις τιμές του δημοσίου και του ιδιωτικού κλειδιού που παρέχονται ως είσοδοι. Ένας χρήστης μπορεί να τροποποιήσει το ιδιωτικό του κλειδί και να ενημερώσει δημοσιεύοντας το αντίστοιχο νέο δημόσιο κλειδί του, έτσι ώστε να αντικατασταθεί το προηγούμενο μη ισχύον πλέον δημόσιο κλειδί.
- Δημόσιο κλειδί (public key): Το δημόσιο κλειδί είναι κοινοποιήσιμο και προορίζεται για δημόσια χρήση. Χρησιμοποιείται για την κρυπτογράφηση των μηνυμάτων.
- Ιδιωτικό κλειδί (private key): Το ιδιωτικό κλειδί χρησιμοποιείται αποκλειστικά και μόνο από τον κάτοχό του για την αποκρυπτογράφηση μηνυμάτων και πρέπει να παραμένει μυστικό.
- Κρυπτογραφημένο μήνυμα ή κρυπτογράφημα (ciphertext): Το μήνυμα που παράγεται από τον αλγόριθμο κρυπτογράφησης, ως έξοδος, και το οποίο εξαρτάται

- από το αρχικό μήνυμα και το δημόσιο κλειδί του παραλήπτη. Για ένα συγκεκριμένο μήνυμα από δύο διαφορετικά κλειδιά παράγονται από τη συνάρτηση κρυπτογράφησης δύο διαφορετικά κρυπτογραφημένα κείμενα.
- Αλγόριθμος αποκρυπτογράφησης (decryption algorithm): Με είσοδο το κρυπτογραφημένο μήνυμα και το ιδιωτικό κλειδί του παραλήπτη παράγεται το πρωτότυπο αρχικό μήνυμα.



Εικόνα 44- Ασύμμετρη Κρυπτογραφία

Γνωστοί αλγόριθμοι Δημόσιου Κλειδιού: RSA, Diffie-Hellman Key Exchange, ElGamal, Digital Signature Standard (DSS), , με κυριότερο τον RSA.

1.5.1. Πλεονεκτήματα:

1. Τα δημόσια κλειδιά δεν χρήζουν προστασίας, καθώς διανέμονται ελεύθερα με αποτέλεσμα την εύκολη σύσταση ασφαλών καναλιών επικοινωνίας μεταξύ δυο απομακρυσμένων χρηστών.
2. Τα ιδιωτικά κλειδιά δεν κοινοποιούνται ή διανέμονται σε τρίτους σε καμία περίπτωση.
    a. Για να σταλεί ένα εμπιστευτικό μήνυμα, χρησιμοποιείται το δημόσιο κλειδί του παραλήπτη. Μόνο το ιδιωτικό κλειδί που κατέχει ο παραλήπτης μπορεί να το αποκρυπτογραφήσει

b. Για να υπογραφεί ένα μήνυμα χρησιμοποιείται το ιδιωτικό κλειδί του αποστολέα. Οποιοσδήποτε τρίτος μπορεί να επαληθεύσει την υπογραφή με το δημόσιο κλειδί του αποστολέα

3. Ελαχιστοποίηση της διαδικασίας διαχείρισης κλειδιών, καθώς δεν απαιτείται κέντρο διανομής κλειδιών.
4. Μεγάλος κύκλος ζωής των κλειδιών.
5. Δίνουν τη δυνατότητα επαλήθευσης της ακεραιότητας δεδομένων.
6. Ψηφιακές Υπογραφές

Ωστόσο, παρά τη σημαντική της συμβολή σε όλα τα παραπάνω και παρά την πολλές φορές γενικευμένη αντίληψη ότι είναι πιο ασφαλής μέθοδος, ως ανθεκτικότερη σε κρυπταναλυκές επιθέσεις, από την συμμετρική κρυπτογράφηση, πρέπει να παραδεχτούμε ότι η ασύμμετρη κρυπτογραφία δεν έρχεται να επιλύσει ουσιαστικά τα ζητήματα ασφάλειας. Στην πραγματικότητα η ασφάλεια οποιουδήποτε συστήματος κρυπτογράφησης εξαρτάται από το μήκος κλειδιού και την υπολογιστική ισχύ που απαιτείται για την κρυπτανάλυση και επιτυχημένη αποκάλυψη του κρυπτογραφημένου μηνύματος.

Υπό αυτό το πρίσμα, επομένως, μπορούμε να εντοπίσουμε τα κυριότερα ζητήματα που μένουν «ανοιχτά» από την εφαρμογή της ασύμμετρη κρυπτογραφίας. Τα σημαντικότερα ερωτήματα που προκύπτουν αποτυπώνονται ως εξής:

- Πως επαληθεύεται η ταυτότητα του πραγματικού κατόχου ενός ζεύγους κλειδιών και πως εξασφαλίζεται η σύνδεση τους με τον κάτοχο, κατά τη διανομή τους;
- Πως διασφαλίζεται η ιδιωτικότητα και η ακεραιότητα των κλειδιών κατά τη δημιουργία τους;

Το σημαντικότερο συμπέρασμα που φαίνεται να προκύπτει είναι η ανάγκη ύπαρξης μίας Έμπιστης Τρίτης Οντότητας που διαχειρίζεται τα Ψηφιακά Πιστοποιητικά. [εισαγωγή παραπομπής]

1.6. ΣΥΝΑΡΤΗΣΕΙΣ ΣΥΝΟΨΗΣ - HASH

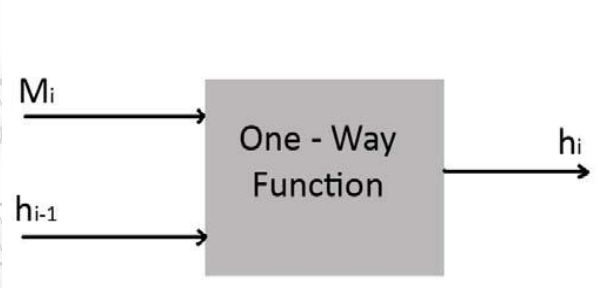
Η συμβολή των hash συναρτήσεων είναι μεγάλη στη σύγχρονη κρυπτογραφία, κυρίως εξαιτίας του γεγονότος ότι αποτελούν τους βασικούς μηχανισμούς για την υλοποίηση της ακεραιότητας και αυθεντικοποίησης των δεδομένων.

Οι συναρτήσεις Hash γνωστές και ως message digest, fingerprint, cryptographic checksum, MIC (Message Integrity Check), MDC(Message Detection Code), είναι στην πραγματικότητα, οι μονόδρομες Hash συναρτήσεις στηρίζονται στην ιδέα μιας συνάρτησης συμπίεσης.

Μια μονόδρομη συνάρτηση hash (one-way hash function) είναι μια συνάρτηση που δέχεται στην είσοδό της ένα αλφαριθμητικό μεταβλητού μήκους (pre-image) και επιστρέφει την έξοδο ένα αλφαριθμητικό σταθερού μήκους (σειρά από bits που αποτελεί την τιμή hash του μηνύματος), που ουσιαστικά αποτελεί τη μετατροπή των δεδομένων του αρχικού μηνύματος σε μονόδρομα δεδομένα. Το αποτέλεσμα της συνάρτησης ονομάζεται σύνοψη, ή ίχνος ή αποτύπωμα. Η συνάρτηση hash είναι μονόδρομη, γεγονός που σημαίνει ότι θεωρείται ανέφικτη η ανάκτηση του αρχικού κειμένου από τη σύνοψη που παρήγαγε. Η σύνοψη χαρακτηρίζει μοναδικά το αρχικό κείμενο, δηλαδή είναι πρακτικά ανέφικτο να βρεθούν δύο αρχικά κείμενα με την ίδια σύνοψη. Επιπλέον, το αποτελέσματα της μονόδρομης συνάρτησης hash είναι μια μεταβλητή hash με μικρότερο μήκος από το μήκος της μεταβλητής εισόδου.

Η μεταβλητή εισόδου (pre-image), πρέπει να περιέχει κάποια δυαδική αντιπροσώπευση του μήκους ολόκληρου του μηνύματος, γεγονός που ξεπερνά ζητήματα που μπορεί να προκύψουν από μηνύματα που πιθανόν έχουν διαφορετικά μήκη hashing για την ίδια μεταβλητή. Η τεχνική αυτή καλείται και ως MD-strengthening.

Στο παρακάτω σχήμα φαίνεται η λειτουργία μιας συνάρτησης hash. Οι είσοδοι (Mi, και hi-1) της συνάρτησης συμπίεσης είναι ένα block μηνύματος (Mi) και η έξοδος του προηγούμενου block από το κείμενο (hi-1), ενώ η έξοδος της συνάρτησης είναι το hash όλων των blocks (hi)μέχρι εκείνο το σημείο. Δηλαδή, το hash του block Mi θα ισούται με hi = f(Mi, hi-1). Αυτή η hash μεταβλητή, μαζί με το επόμενο block μήνυμα, γίνεται η επόμενη είσοδος της συνάρτησης συμπίεσης. Το Hash ολόκληρου του μηνύματος είναι το hash του τελευταίου block.



Εικόνα 45- Μονόδρομη Hash συνάρτηση

Μια κρυπτογραφική συνάρτηση hash, είναι μια μονοδρομη hash συνάρτηση με ιδιαίτερη προστασία από τις συγκρούσεις (collision resistant).

Μια κρυπτογραφική συνάρτηση hash πρέπει να πληροί τις ακόλουθες ιδιότητες:

1. Δοθέντος y, είναι υπολογιστικά αδύνατο να βρεθεί x τέτοιο ώστε h(x) = y

2. Δοθέντων x, h(x), είναι υπολογιστικά αδύνατο να βρεθεί x΄ τέτοιο ώστε h(x΄) = h(x)

3. Είναι υπολογιστικά αδύνατο να βρεθούν x1, x2 ∈ F*, τέτοια ώστε, h(x1) = h(x2)

Η τρίτη ιδιότητα περιλαμβάνει πρακτικά και τη δεύτερη, η οποία είναι πιο περιορισμένη και έτσι ονομάζεται ασθενής αντίσταση σε συγκρούσεις ενώ η τρίτη ιδιότητα ονομάζεται ισχυρή αντίσταση σε συγκρούσεις.

Σύμφωνα με τον παραπάνω ορισμό, οι συναρτήσεις που διατηρούν τις ιδιότητες (1) και (2), ονομάζονται μονόδρομες hash συναρτήσεις, ενώ οι συναρτήσεις που διατηρούν τις ιδιότητες (2) και (3) ονομάζονται ανθεκτικές σε συγκρούσεις hash συναρτήσεις (collision resistance hash functions), όπου σύγκρουση ονομάζουμε την περίπτωση όπου περισσότερα από ένα στοιχεία του πεδίου ορισμού της συνάρτησης αντιστοιχίζεται στο ίδιο στοιχείο του

συνόλου τιμών. Μια hash συνάρτηση είναι ανθεκτική σε συγκρούσεις, όταν δεν υπάρχει συστηματικός τρόπος, πέραν της εξαντλητικής αναζήτησης, να ανακαλύπτονται στοιχεία που να καταλήγουν στην ίδια σύνοψη. Εφόσον είναι υπολογιστικά αδύνατο να βρεθούν δύο οποιεσδήποτε τιμές οι οποίες έχουν την ίδια σύνοψη, τότε είναι ακόμη πιο δύσκολο να βρεθεί μια δεύτερη τιμή που να έχει την ίδια σύνοψη με μια δεδομένη τιμή.

Οι συναρτήσεις αυτές μπορούν να προσφέρουν αυθεντικοποίηση και ακεραιότητα των δεδομένων. και κατατάσσονται στις κατηγορίες των κωδικών αυθεντικοποίησης μηνυμάτων και των κωδικών ανίχνευσης τροποποίησης.

Αναφορικά με το αν είναι ασφαλής, πρέπει να σημειώσουμε ότι δεν υπάρχει μυστικότητα στον τρόπο λειτουργίας μιας συνάρτησης hash. Η ασφάλεια μιας μονόδρομης (one-way) συνάρτησης hash.της στηρίζεται στο γεγονός ότι είναι μονόδρομη, καθώς και στο μήκος (σε bit) του μηνύματος της εξόδου (output) . Επιπλέον, η έξοδος δεν εξαρτάται από την είσοδο (input) κατά εμφανή τρόπο. Μια απλή αλλαγή ενός bit στο μήνυμα εισόδου, αλλάζει, κατά μέσο όρο, τα μισά bit της τιμής hash.

Η βασική συνεισφορά στην ασφάλεια μέσω των hash συναρτήσεων προκύπτει από τις ακόλουθες διαπιστώσεις. Για μια συνάρτηση hash, ενώ είναι εξαιρετικά απλό να υπολογίσουμε την τιμή hash ενός μηνύματος, εντούτοις είναι υπολογιστικά αδύνατο να ανακτήσουμε το αρχικό μήνυμα δεδομένης της τιμής hash του. Υπολογιστικά αδύνατη είναι επίσης η πιθανότητα να υπάρξουν δύο αρχικά μηνύματα τα οποία μέσω της hash συνάρτησης να επιστρέφουν την ίδια τιμή.

Η ανάλυση της υπόθεσης της εξαντλητικής αναζήτησης είναι το κριτήριο που πρωτίστως πρέπει να λαμβάνεται υπόψη στην επιλογή μιας κρυπτογραφικής μονόδρομης hash και εμμέσως αποδεικνύει την κρυπτογραφική δύναμη μιας συνάρτησης. Κατά συνέπεια, μπορούμε να θεωρήσουμε ως ασφαλή μια κρυπτογραφική μονόδρομη συνάρτηση, αν μπορεί να αντισταθεί σε επίθεση τουλάχιστον ίση με την εξαντλητική αναζήτηση.

Παρά την προαναφερόμενη συμβολή της συνάρτησης σε ζητήματα ασφάλειας, ωστόσο, η θεωρητική έρευνα συνεχίζεται στην προσπάθεια απόδειξης ότι αν η συνάρτηση συμπίεσης είναι ασφαλής, συνεπάγεται ότι και η μέθοδος hashing είναι επίσης ασφαλής, χωρίς έως τώρα να έχει αποδειχθεί κάτι τέτοιο.

Γνωστοί αλγόριθμοι μονόδρομων συναρτήσεων hash είναι οι MD2, MD5, και οι SHA-1, BSHA (Secure Hash Algorithm) με μήκος σύνοψης 256 ή 512 bit, καθώς επίσης και οι RIPEMD-160 και Square-Mod (σύνηθες μήκος σύνοψης: 128-160 bits).

1.7. ΚΩΔΙΚΑΣ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ ΜΗΝΥΜΑΤΩΝ - MAC

«Ο κώδικας αυθεντικοποίησης μηνύματος (Message Authentication Code, MAC) είναι μια μονόδρομη κρυπτογραφική hash συνάρτηση με κλειδί, η οποία προσφέρει ασθενή αντίσταση σε συγκρούσεις:

• δοθέντων x, hk(x), είναι υπολογιστικά αδύνατο να βρεθεί x΄ τέτοιο ώστε hk(x΄) = hk(x).»

Η MAC είναι συνήθης τεχνική που χρησιμοποιείται για την αυθεντικοποίηση μηνυμάτων, κατά την οποία απαιτείται η χρήση ενός μυστικού κλειδιού, ώστε να παραχθεί ένα μικρό τμήμα δεδομένων το οποίο προσαρτάται στο μήνυμα. Έτσι, το MAC ενός μηνύματος υπολογίζεται ως συνάρτηση του αρχικού μηνύματος και του μυστικού κλειδιού, όπως περιγράφεται από την ακόλουθη σχέση, MAC(M) = f (K, M), όπου K το κλειδί και M το αρχικό μήνυμα. Η τεχνική δουλεύει όπως περιγράφεται ακολούθως. Ο αποστολέας στέλνει το μήνυμά του επισυνάπτοντας το MAC. Ο παραλήπτης, αντίστοιχα, πραγματοποιεί τον ίδιο υπολογισμό στο μήνυμα που έλαβε, χρησιμοποιώντας το ίδιο μυστικό κλειδί και παράγει ένα νέο MAC. Το MAC του αποστολέα, συγκρίνεται με το MAC του παραλήπτη και αν συμπίπτουν τότε έχει μεταφερθεί επιτυχώς το μήνυμα.

Εάν υποθέσουμε ότι το μυστικό κλειδί είναι γνωστό μόνο μεταξύ του αποστολέα και του παραλήπτη ενός μηνύματος και τα ότι μόνον ο παραλήπτης και ο αποστολέας γνωρίζουν το μυστικό κλειδί και εάν τα MAC που προέκυψαν συμπίπτουν, τότε συνάγουμε τα ακόλουθα:

- Το μήνυμα έχει μεταφερθεί ακέραιο στον παραλήπτη, καθώς σε άλλη περίπτωση τα δύο MAC δεν θα ήταν ίσα.
- Επαληθεύεται κατά την παραλαβή του μηνύματος και τη σύγκριση των MAC, ο αποστολέας του μηνύματος, καθώς κανείς, πλην του αποστολέα και του νόμιμα εξουσιοδοτημένου παραλήπτη, δε γνωρίζει το μυστικό κλειδί, ώστε να παράγει για το ίδιο μήνυμα, την ίδια MAC.
- Εάν το μήνυμα περιλαμβάνει αριθμό ακολουθίας, όπως αυτοί που χρησιμοποιούνται στα πρωτόκολλα X.25, HDLC και TCP, τότε ο παραλήπτης μπορεί να επιβεβαιώσει την ορθότητα της σωστής ακολουθίας, επειδή ο επιτιθέμενος δεν μπορεί να τροποποιήσει επιτυχώς έναν αριθμό ακολουθίας.