**Π**ΑΝΕΠΙΣΤΗΜΙΟ **Α**ΙΓΑΙΟΥ
**Τ**ΜΗΜΑ **Μ**ΗΧΑΝΙΚΩΝ **Π**ΛΗΡΟΦΟΡΙΑΚΩΝ **Κ**ΑΙ **Ε**ΠΙΚΟΙΝΩΝΙΑΚΩΝ **Σ**ΥΣΤΗΜΑΤΩΝ
**Π.Μ.Σ. Τ**ΕΧΝΟΛΟΓΙΕΣ & **Δ**ΙΟΙΚΗΣΗ **Π**ΛΗΡΟΦΟΡΙΑΚΩΝ **Σ**ΥΣΤΗΜΑΤΩΝ
**Κ**ΑΤΕΥΘΥΝΣΗ **Δ**ΙΟΙΚΗΣΗΣ **Π**ΛΗΡΟΦΟΡΙΑΚΩΝ **Σ**ΥΣΤΗΜΑΤΩΝ

# ΑΝΑΛΥΣΗ ΠΟΛΙΤΙΚΩΝ ΚΑΙ ΠΡΑΚΤΙΚΩΝ ΕΘΝΙΚΗΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΤΑΥΤΟΤΗΤΑΣ (eID) ΣΤΗΝ ΕΥΡΩΠΗ

**Σάββας Α. Λαζαρίδης**

Επιβλέπων: Ι. Χαραλαμπίδης, Επίκουρος Καθηγητής

Σάμος, Φεβρουάριος 2011

Η Διπλωματική Εργασία

παρουσιάστηκε ενώπιον

του Διδακτικού Προσωπικού του

Πανεπιστημίου Αιγαίου

---

Σε Μερική Εκπλήρωση

των Απαιτήσεων για το Δίπλωμα του

Μεταπτυχιακού Προγράμματος Σπουδών

Τεχνολογίες και Διοίκηση Πληροφοριακών και Επικοινωνιακών Συστημάτων

---

του

ΣΑΒΒΑ Α. ΛΑΖΑΡΙΔΗ

ΧΕΙΜΕΡΙΝΟ ΕΞΑΜΗΝΟ 2010

Η ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ ΔΙΔΑΣΚΟΝΤΩΝ ΕΓΚΡΙΝΕΙ
ΤΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
ΤΟΥ ΣΑΒΒΑ Α. ΛΑΖΑΡΙΔΗ

---

ΙΩΑΝΝΗΣ ΧΑΡΑΛΑΜΠΙΔΗΣ, Επίκουρος Καθηγητής, Επιβλέπων 08.02.2011
Τμήμα Μηχανικών Πληροφοριακών και
Επικοινωνιακών Συστημάτων

---

ΕΥΡΙΠΙΔΗΣ ΛΟΥΚΗΣ, Επίκουρος Καθηγητής, Μέλος
Τμήμα Μηχανικών Πληροφοριακών και
Επικοινωνιακών Συστημάτων

---

ΣΠΥΡΟΣ ΚΟΚΟΛΑΚΗΣ, Επίκουρος Καθηγητής, Μέλος
Τμήμα Μηχανικών Πληροφοριακών και
Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΧΕΙΜΕΡΙΝΟ ΕΞΑΜΗΝΟ 2010

# ΠΕΡΙΛΗΨΗ

Στον παράλληλο κόσμο τον οποίο διαμορφώνει το Ίντερνετ το θέμα της διαχείρισης ταυτότητας ψηφιοποιείται. Δημιουργείται η ανάγκη για την κάλυψη του ζητήματος της ηλεκτρονικής ταυτοποίησης των χρηστών οι οποίοι πρόκειται να χρησιμοποιήσουν τις υπηρεσίες που παρέχονται σε επίπεδο ηλεκτρονικής διακυβέρνησης, αλλά και σε άλλες εμπορικές συναλλαγές οι οποίες προσφέρονται από φορείς του ιδιωτικού τομέα. Για το λόγο αυτό το κάθε κράτος ανταποκρινόμενο στις ανάγκες των καιρών υλοποιεί μία πολιτική ή μία σειρά από πολιτικές και υιοθετεί πρακτικές προκειμένου να ρυθμίσει σε εθνικό επίπεδο το θέμα της διαχείρισης της ηλεκτρονικής ταυτοποίησης των πολιτών του.

Στον διαδικτυακό όμως αυτό περιβάλλον, δεν υφίστανται γεωγραφικοί περιορισμοί, για την παροχή τέτοιου είδους υπηρεσιών και έτσι πολύ σύντομα το θέμα της διαχείρισης των ηλεκτρονικών ταυτοτήτων παύει να αποτελεί ένα εθνικό ζήτημα. Για το λόγο αυτό κρίνεται κρίσιμο να αποτυπωθούν οι λύσεις διαχείρισης ηλεκτρονικών ταυτοτήτων οι οποίες υλοποιούνται σε εθνικό επίπεδο στο σύνολο των χωρών οι οποίες συνιστούν την ενιαία Ευρωπαϊκή αγορά. Στα πλαίσια της μελέτης αυτής, παρουσιάζονται συγκριτικά μέσα από μια ανάλυση στα επίπεδα των επιλογών ταυτοποίησης, σε νομικό επίπεδο, σε επίπεδο ασφάλειας αυθεντικοποίησης και τέλος σε επίπεδο χρησιμοποιούμενων τεχνολογιών και υποδομών οι εθνικές πολιτικές και πρακτικές οι οποίες εφαρμόζονται σε Ευρωπαϊκό επίπεδο από τα διάφορα κράτη.

Παρ' όλα αυτά επειδή ο χάρτης της ενιαίας Ευρωπαϊκής αγοράς, δεν θα μπορούσε να καθοριστεί μόνο μέσα από την ύπαρξη αυτόνομων και τεχνικά ή «πολιτικά» διαφοροποιημένων λύσεων, κρίσιμη κρίνεται η προσπάθεια «σύμπλευσης» των εθνικών λύσεων, σε μία ενιαία κατεύθυνση, ούτως ώστε αυτές να κατασταθούν διαλειτουργικές στην προσπάθεια επίτευξης μίας ενιαίας Ευρωπαϊκής αγοράς, ελεύθερα προσβάσιμης σε όλους τους Ευρωπαίους πολίτες. Η Ευρωπαϊκή Ένωση σε ρόλο συντονιστή, αναλαμβάνει τις απαραίτητες εκείνες πρωτοβουλίες, είτε υλοποιώντας είτε χρηματοδοτώντας μία σειρά από ενέργειες και έργα που ως σκοπό έχουν να καταγράψουν την υφιστάμενη κατάσταση και να άρουν τους περιορισμούς οι οποίοι υφίστανται εξ' αιτίας της διαφοροποίησης των εθνικών λύσεων διαχείρισης ταυτότητας.

Αναγκαία προϋπόθεση παραμένει όμως, πέρα από την άρση των υπαρχουσών περιορισμών, η εμπιστοσύνη των πολιτών και η υιοθέτηση του νέου τρόπου ταυτοποίησης. Σε αυτό το πλαίσιο βαρύνουσα σημασία φαίνεται να διαδραματίζει, ακόμη ίσως περισσότερο και από το θέμα του τεχνολογικού αναλφαβητισμού, η προστασία των προσωπικών δεδομένων των χρηστών.

ΣΑΒΒΑΣ Α. ΛΑΖΑΡΙΔΗΣ
Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων
ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

# ABSTRACT

In the parallel internet-based world, identity management is being digitalized. There is a growing need to cover the issue of electronic identification of users who are to use the services not only at an e-government level, but also in other commercial transactions offered by the private sector bodies. For this reason, each state, meeting the needs of modern times, implements a policy or a set of policies and adopts practices in order to regulate the issue of electronic identification management of its citizens at a national level.

However, in this internet-based world there are no geographic restrictions on the provision of such services, so soon eID is not considered a national issue any longer. For this reason it is crucial to find eID solutions that are implemented at a national level in all the countries which constitute one single European market. In this study, the national policies and practices implemented at European level by the various states are presented through a comparative analysis of levels of identification options, in terms of regulation, authentication security, and finally technology and infrastructure.

Nevertheless, the effort of 'aligning' of national solutions in a single direction is considered crucial, so that they become interoperable towards the achievement of a single European market, freely accessible to all European citizens. This is due to the fact that the chart of the single European market could not be determined only through the existence of autonomous and technically or 'politically' differentiated solutions. The European Union, acting as a coordinator, takes the necessary initiatives to document the current situation and to remove restrictions imposed by the diversity of national identity management solutions by either implementing or funding a series of actions and projects.

Yet, citizens' trust and the adoption of a new way of identification still remain a necessary condition in addition to the removal of existing restrictions. It is in this context that personal data protection of users seems to play an important role, maybe even more important than the issue of technological illiteracy.

SAVVAS A. LAZARIDIS
Department of Information and Communication Systems Engineering
UNIVERSITY OF THE AEGEAN

# ΕΥΧΑΡΙΣΤΙΕΣ – ΑΦΙΕΡΩΣΕΙΣ

*"Κάθε ταξίδι έχει τα δικά του μυστικά.*

*Τις περισσότερες φορές μόνο στο τέλος του ίσως μάθεις τους λόγους για τους οποίους έγινε.*

*Αντιλαμβάνεσαι την ουσία των γεγονότων που έζησες,*

*όταν η πραγματικότητα έχει σβήσει από μπροστά σου.*

*Και οι στιγμές μόνες τους οδηγημένες από τη μνήμη ξανάρχονται στο νου …"*

*Ένα μεγάλο ευχαριστώ στους καθηγητές μου οι οποίοι ήταν κοντά μου σε αυτή την προσπάθειά,*

*Ιδιαίτερα ευχαριστώ τη Ζωή μου, για την υπομονή της…*

# ΠΕΡΙΕΧΟΜΕΝΑ

# ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

# ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

# 1. ΕΙΣΑΓΩΓΗ

## 1.1 Ταυτοποίηση – Ορισμός Ηλεκτρονικής Ταυτότητας

Το θέμα της ταυτοποίησης δεν είναι ένα καινούργιο ζήτημα. Εμπειρία αιώνων είναι ήδη διαθέσιμη στο θέμα της ταυτοποίησης προσώπων, πρόσωπο με πρόσωπο. Αυτό που είναι καινούργιο στην Κοινωνία της Πληροφορίας είναι η ψηφιοποίηση της διαχείρισης ταυτότητας, τόσο μέσα στο Ίντερνετ, όσο και σε offline βάσεις δεδομένων. Η αυθεντικοποίηση του ατόμου σε αρκετά συστήματα, η σύνδεση του σε δίκτυα κινητών επικοινωνιών, καθώς επίσης και η διαδικασία του να παρέχει στοιχεία ταυτοποίησης προκειμένου να αποκτήσει πρόσβαση σε μία πλειάδα εφαρμογών, έχει γίνει κάτι το οποίο πραγματοποιείται από τον καθένα πολλές φορές μέσα στην καθημερινότητα του.

Η ουσιαστική αλλαγή πάνω στο θέμα της ταυτοποίησης είναι ότι με τις ψηφιακές τεχνολογίες τροποποιήθηκε σε πολύ μεγάλο βαθμό ο τρόπος που το θέμα της ταυτότητας διαχειρίζεται από τα άτομα, τις εταιρείες και τις κυβερνήσεις. Όλα αυτά την ώρα που στο κέντρο του θέματος της διαχείρισης της ψηφιακής ταυτότητας βρίσκεται μία κρίσιμη ερώτηση: «Πώς ξέρω ότι είσαι, αυτός που ισχυρίζεσαι ότι είσαι;». Μία πληθώρα από υπηρεσίες του δημόσιου και ιδιωτικού τομέα στην Ψηφιακή Οικονομία προσπαθούν να βρουν μία ουσιαστική, πειστική και αξιόπιστη απάντηση σε αυτή την ανάγκη για αυθεντικοποίηση[1].

Έτσι ο όρος ηλεκτρονική ταυτότητα αναφέρεται σε[1] «*οποιοδήποτε μέσο ή μέθοδο 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*»[2].

## *1.2 Η ανάγκη ύπαρξης ηλεκτρονικής ταυτοποίησης*

Προκειμένου οι πολίτες να καταφέρουν να πραγματοποιήσουν ηλεκτρονικές συναλλαγές, είτε με φορείς του δημόσιου τομέα είτε με φορείς του ιδιωτικού τομέα, απαιτείται η ύπαρξη ενός μηχανισμού ο οποίος θα είναι σε

[1] Ο ορισμός προέρχεται από το άρθρο 3 του Προσχεδίου Νόμου για την Ηλεκτρονική Διακυβέρνηση, το οποίο βρισκόταν στη φάση της δημόσιας διαβούλευσης έως τις 30/1/2011 και πιθανότατα θα υιοθετηθεί ως έχει από το ελληνικό κράτος. (Βλ. http://www.opengov.gr/ypes/wp-content/plugins/download-monitor/download.php?id=4 )

θέση να ταυτοποιεί τον κάθε συναλλασσόμενο πολίτη στο περιβάλλον της απρόσωπης επικοινωνίας του διαδικτύου, παρέχοντας τα εχέγγυα για την πραγματοποίηση της επιθυμητής κάθε φορά συναλλαγής.

Με τον τρόπο αυτό πείθεται πιο εύκολα ο πολίτης να ταυτοποιηθεί χρησιμοποιώντας στη συνέχεια υπηρεσίες οι οποίες άπτονται του πεδίου της ηλεκτρονικής διακυβέρνησης, νιώθοντας ότι πλέον τα προσωπικά του δεδομένα προστατεύονται και δεν είναι εκτεθειμένα στο μέτρο που αυτός το επιθυμεί.

Από την άλλη μεριά δίνεται η δυνατότητα στους δημόσιους φορείς οι οποίοι υλοποιούν τη συναλλαγή να γνωρίζουν μέσω της προηγούμενης ταυτοποίησης τον πολίτη ο οποίος συναλλάσσεται μαζί τους, εξαλείφοντας κατ' αυτό τον τρόπο το ενδεχόμενο να λάβει κάποιος συναλλασσόμενος παροχή ή να ασκήσει δικαίωμα που δεν το δικαιούται.

Όπως γίνεται ξεκάθαρο το θέμα της ταυτοποίησης ανάγεται σε ένα από τα σημαντικότερα θέματα τα οποία θα πρέπει να τύχουν ρύθμισης, προκειμένου να επιτευχθεί η απρόσκοπτη διάδοση των υπηρεσιών ηλεκτρονικής διακυβέρνησης και των ηλεκτρονικά παρεχόμενα υπηρεσιών γενικότερα.

## 1.3 Κατηγορίες λύσεων eIDM

Σε επίπεδο Ευρωπαϊκής Ένωσης λειτουργούν ήδη συστήματα ηλεκτρονικής ταυτοποίησης στα διάφορα κράτη μέλη, τα οποία ανάλογα με το εύρος χρήσης τους διακρίνονται σε:

- Συστήματα eIDM[2] εθνικής εμβέλειας
- Συστήματα eIDM τοπικής εμβέλειας, σε επίπεδο περιφερειών κ.τ.λ. και τέλος
- Συστήματα eIDM τα οποία τυγχάνουν εφαρμογή σε κάποιο συγκεκριμένο τομέα (όπως π.χ. για φορολογικά θέματα, θέματα υγείας κ.τ.λ.),

προκειμένου να γίνει εφικτή η παροχή ηλεκτρονικών υπηρεσιών από τους δημόσιους φορείς, ενώ σε κάποιες χώρες υφίστανται και εμπορικές εφαρμογές οι οποίες παρέχονται από εταιρείες του ιδιωτικού τομέα, αλλά αναγνωρίζονται από τον δημόσιο τομέα ως έγκυρες εφαρμογές ηλεκτρονικής ταυτοποίησης.

Η δραστηριότητα η οποία υπάρχει σε Ευρωπαϊκό επίπεδο πάνω στο θέμα των ηλεκτρονικών ταυτοτήτων βρίσκεται σε ιδιαίτερη διέγερση κατά την

[2] eIDM: Electronic Identification Management

τελευταία πενταετία. Στο διάστημα αυτό πολλές χώρες έχουνε υιοθετήσει συστήματα διαχείρισης ηλεκτρονικών ταυτοτήτων στα πλαίσια του εκσυγχρονισμού των υπηρεσιών τις οποίες ο δημόσιος τομέας του κάθε κράτους παρέχει προς τους πολίτες του (όπως ενδεικτικά αναφέρονται η παροχή πιστοποιητικών, η διεκπεραίωση φορολογικών υποχρεώσεων κ.α.) [3]. Και στις υπόλοιπες όμως χώρες οι οποίες ακόμα δεν έχουν ενσωματώσει σχετικά συστήματα, σχεδιάζεται η εγκατάσταση αντίστοιχων συστημάτων στο εγγύς μέλλον.

## 1.4 Μεθοδολογία

Στην προσπάθεια να υπάρξει η όσο το δυνατόν πληρέστερη αποτύπωση της υφιστάμενης κατάστασης στο θέμα της διαχείρισης ηλεκτρονικών δελτίων ταυτότητας, η παρούσα μελέτη έπρεπε να τμηματοποιήσει το ενιαίο πλαίσιο το οποίο καθορίζει την πολιτική της κάθε χώρας στο ζήτημα αυτό.

Έτσι προσδιορίσθηκαν μία σειρά από τέσσερα επίπεδα στα οποία θα μπορούσε να διακριθεί το ζήτημα του eIDM της κάθε χώρας. Τα επίπεδα αυτά ποικίλουν από τις πολιτικές οι οποίες ακολουθούνται σε νομικά ζητήματα τα οποία παρουσιάζονται, έως τις τεχνικές λύσεις οι οποίες επιλέγονται κατά περίπτωση στα διάφορα κράτη. Αναλυτικότερα τα τέσσερα επίπεδα που διακρίθηκαν ήταν τα εξής:

A. **Επίπεδο Χρησιμοποιούμενων Υποδομών και Επιλογών Ταυτοποίησης.** Βασικό στοιχείο της κάθε χώρας αποτελεί η επιλογή των Υποδομών τις οποίες χρησιμοποίει προκειμένου να υλοποιήσει την πολιτική της στο ζήτημα των ηλεκτρονικών ταυτοτήτων. Η υιοθέτηση έξυπνων καρτών, συμβατικών δελτίων ταυτότητας ή άλλων τρόπων ταυτοποίησης των χρηστών, αποτελούν ένα καίριο ζήτημα πολιτικής απόφασης στην κάθε χώρα.

**B. Επίπεδο νομικών ρυθμιστικών διατάξεων.** Η ύπαρξη ενιαίου ρυθμιστικού πλαισίου σε Ευρωπαϊκό επίπεδο, το οποίο στη συνέχεια καλείται να υιοθετηθεί σε εθνικό επίπεδο, καθορίζει ανάλογα με τον τρόπο εφαρμογής την υιοθετούμενη πολιτική της κάθε χώρας στο ζήτημα του eIDM. Πολιτιστικές, κοινωνικές και πολιτικές ιδιαιτερότητες στην κάθε χώρα διαφοροποιούν αυτό το πλαίσιο και τις επιλογές οι οποίες λαμβάνονται στα πλαίσια της επιλεγόμενης πολιτικής. Η χρήση μοναδικών αναγνωριστικών σε συμφωνία και με τις συνταγματικές επιταγές του κάθε κράτους, η ισχύς των ψηφιακών τρόπων απόδειξης της ταυτότητας καθώς και η υποστήριξη τέτοιου είδους υποδομών

προκειμένου να πραγματοποιούνται και εμπορικές συναλλαγές εκτός του αυστηρού πλαισίου χρήσης για υπηρεσίες της ηλεκτρονικής διακυβέρνησης, χαρακτηρίζουν τις ακολουθούμενες πολιτικές στο ζήτημα του eIDM σε αυτό το επίπεδο.

C. **Επίπεδο Αυθεντικοποίησης των οντοτήτων.** Μηχανισμοί αυθεντικοποίησης σε ένα επίπεδο πιο κάτω από το νομικό επίπεδο, αναλαμβάνουν να υλοποιήσουν την πολιτική ως προς το eIDM στην κάθε χώρα. Οι επιλογές οι οποίες γίνονται στα συστήματα και τις πολιτικές αυθεντικοποίησης, με την υιοθέτηση συστημάτων PKI ή άλλων συστημάτων αυθεντικοποίησης, καθορίζουν κατά περίπτωση την εμπιστοσύνη και την αξιοπιστία με την οποία το κάθε κράτος περιβάλλει τη διαδικασία της ψηφιακής αυθεντικοποίησης.

D. **Επίπεδο Χρησιμοποιούμενων Τεχνολογιών.** Σε ένα τελευταίο επίπεδο, συγκεκριμένες τεχνολογίες και πρότυπα χρησιμοποιούνται προκειμένου να υλοποιηθούν οι διάφορες eIDM λύσεις για το κάθε κράτος. Ελάχιστα επίπεδα ασφάλειας κοινά καθοριζόμενα σε Ευρωπαϊκό επίπεδο, αλλά και επιπρόσθετες ανεξάρτητες κρατικές επιλογές καθορίζουν την πολιτική του κάθε κράτους σε αυτό το τελευταίο τεχνικό επίπεδο. [1]

Σε κάθε ένα από αυτά τα επίπεδα επιλέχθηκε και συγκρίθηκε μία πλειάδα χαρακτηριστικών γνωρισμάτων για την πολιτική την οποία ακολουθεί το κάθε κράτος μέλος. Συνοπτικά οι κύριες κατηγορίες γνωρισμάτων για κάθε επίπεδο παρουσιάζονται στον πίνακα που ακολουθεί:

| **Α. Χρησιμοποιούμενες Υποδομές και Επιλογές Ταυτοποίησης** | | |
|---|---|---|
| **Χαρακτηριστικό Γνώρισμα** | **Περιγραφή / Τιμές** | **Παρατηρήσεις** |
| **Μέσο Αποθήκευσης των δεδομένων ταυτοποίησης** | Εθνικό δελτίο eID. Υλοποιείται σε μορφή κάρτας, αλλά δύναται να λάβει και άλλες μορφές, όπως για παράδειγμα αποθήκευση σε κάποιο usb stick, ή ακόμη και μέσω κινητού τηλεφώνου. | Δεν αποτελεί όμως μοναδική λύση. Εναλλακτικές λύσεις, όπως παραδοσιακοί τρόποι ταυτοποίησης είναι ακόμα σε ισχύ σε αρκετές χώρες, ενώ δεν εκλείπουν και οι περιπτώσεις χωρών στην κουλτούρα των οποίων δεν υπάρχει η έννοια της ταυτοποίησης |
| **Υποχρεωτική κτήση δελτίου ταυτότητας** | Οι επιλογές ποικίλουν από χώρα σε χώρα. Η κατοχή είναι άλλοτε υποχρεωτική προκειμένου να προκύψει στα εν λόγω κράτη άμεση ωφέλεια σε κρατικό επίπεδο από την | Και η προαιρετική απόκτηση υιοθετεί την άποψη της «κέντρισης» του ενδιαφέροντος, προκειμένου επί της ουσίας σιγά σιγά να δημιουργηθεί στα |

| | | |
|---|---|---|
| | υιοθέτηση της νέας τεχνολογίας και άλλοτε προαιρετική. | κράτη η κρίσιμη μάζα για την χρήση της εν λόγω τεχνολογίας. |
| **Κατηγορίες Χρηστών** | Το σύνολο ή υποσύνολα του γενικού πληθυσμού κάθε κράτους (τα οποία συγκεντρώνουν συγκεκριμένα χαρακτηριστικά) , όπου όμως και πάλι ενδιαφέρον παρουσιάζουν στοιχεία στα οποία κάποιος θεωρείται ικανός για δικαιοπραξία (ακόμη ίσως και υπό το πρίσμα μίας αγοραπωλησίας) και καθορίζουν την προμήθεια ή όχι από αυτόν ενός δελτίου eID | Υπάρχουν και περιπτώσεις όπου κάτοχοι τέτοιου είδους δελτίων eID μπορεί να είναι είτε αλλοδαποί, υπό την έννοια της μόνιμης διαμονής στη χώρα, αλλά και αλλοδαποί υπό την έννοια του πολίτη ο οποίος προέρχεται από άλλη χώρα και συναλλάσσεται σε κάποια τρίτη χώρα πέραν της δικής του |
| **Κατάσταση Χρήσης** | Τα δελτία eID δεν αποτελούν ενιαία αποδεκτή τεχνολογία. Γι' αυτό οι καταστάσεις υιοθέτησης ποικίλουν από ήδη υιοθετημένα σε υπό σχεδιασμό, ή ίσως ακόμη και σε τεχνολογία η οποία ίσως δεν εξετάζεται καθόλου από κάποια κράτη. | |
| **Βιομετρικά Δεδομένα** | Η χρήση βιομετρίας μπορεί να αποτελεί την πιο προηγμένη επιλογή της πρόσωπο με πρόσωπο ταυτοποίησης, εν τούτοις δεν υιοθετείται από το σύνολο των χωρών. | Ζητήματα τα οποία άπτονται της αρχής της «αναλογικότητας» αποτρέπουν ορισμένα κράτη από το να υιοθετήσουν την εν λόγω μέθοδο ταυτοποίησης. Επιπλέον μπορεί να διαφοροποιούνται ακόμη και τα δεδομένα τα οποία χρησιμοποιούνται σε κάθε λύση. |
| **Έτος εισαγωγής** | Η χρονολογία εισαγωγής σαφέστατα αποτελεί ένα στοιχείο ανάδειξης της ευελιξίας στην υιοθέτηση αντιστοίχων τεχνολογιών από το κάθε κράτος μέλος. | Από το 1999 οπότε και η πρώτη Ευρωπαϊκή χώρα εισήγαγε το πρώτο δελτίο eID έως και σήμερα αρκετές από τις χώρες έχουνε υιοθετήσεις κάποιου είδους δελτίο eID |
| **Β. Ρυθμιστικό Πλαίσιο** | | |
| **Χαρακτηριστικό Γνώρισμα** | **Περιγραφή / Τιμές** | **Παρατηρήσεις** |
| **Χρήση μοναδικού κωδικού** | Η χρήση ενός μοναδικού αναγνωριστικού για τον προσδιορισμό ενός ατόμου και η ταύτιση του με ένα αλφαριθμητικό, αποτελεί μία πολιτική επιλογή στρατηγικής σημασίας για κάθε κράτος. | Ως μέθοδος δεν υιοθετείται από όλα τα κράτη, αν και στην πράξη αποτελεί τον πιο ασφαλή τρόπο μοναδικής ταυτοποίησης ενός πολίτη. |
| **Τομεακά διακριτικά** | Κάθε κράτος διαθέτει έναν αριθμό από έγκυρα τομεακά διακριτικά ταυτοποίησης (βλ. ΑΦΜ, και ΑΜΚΑ για την ελληνική πραγματικότητα) | Γενικά πρόκειται για μία κατηγορία διακριτικών η οποία σχετίζεται με το είδος των παρεχόμενων υπηρεσιών (βλ. υπηρεσίες κοινωνικής ασφάλισης, |

| | | |
|---|---|---|
| | | υπηρεσίες φορολογικών θεμάτων κ.τ.λ.) |
| **Υποστήριξη επιπλέον υπηρεσιών (π.χ. πωλήσεις, αγορές αγαθών)** | Η δυνατότητα πρόσβασης φορέων του ιδιωτικού τομέα στα δεδομένα ταυτοποίησης αποτελεί μία πολιτική επιλογή η οποία δεν υιοθετείται από όλα τα κράτη. | Η εξωστρέφεια των υπαρχουσών υποδομών με την συμπερίληψη στη δυνατότητα χρήσης και φορέων του ιδιωτικού τομέα, εκδηλώνει έως ένα σημείο, το βαθμό διαλειτουργικότητας των λύσεων eIDM. |
| **Έκδοση από ιδιωτικό τομέα** | Η έκδοση των δελτίων eID παύει να αποτελεί προνόμιο μόνο των κρατικών αρχών, μετά από εξουσιοδότηση η οποία παρέχεται κατά περίπτωση σε φορείς του ιδιωτικού τομέα. | Η διείσδυση φορέων του ιδιωτικού τομέα στον πυρήνα της ιδιωτικότητας του ατόμου, μέσω των προσωπικών του δεδομένων για ταυτοποίηση, αποτελεί μία πρακτική μη κοινά αποδεκτή από τα διάφορα κράτη μέλη. |
| **Προστασία προσωπικών δεδομένων** | Το νομικό πλαίσιο, και οι κατ' εξουσιοδότηση του αποφάσεις καθορίζουν τα δεδομένα τα οποία θα χρησιμοποιηθούν για τους σκοπούς ταυτοποίησης καθώς και το βαθμό προστασίας τους | Έκπληξη προκαλεί το γεγονός ότι στις περισσότερες Ευρωπαϊκές χώρες, δεν έχει ακόμα οριστεί η έννοια της ηλεκτρονικής ταυτότητας. |
| **Έγκυρα μητρώα** | Τα μητρώα τα οποία χρησιμοποιεί το κάθε κράτος ως πρωτεύοντα κλειδιά για το σύνολο του πληθυσμού, ή για κατηγορίες πληθυσμού με συγκεκριμένα γνωρίσματα και τα οποία χρησιμοποιούνται για τις ανάγκες ταυτοποίησης των χρηστών, υποκείμενα στην αρχή της «επικαιροποίησης» των δεδομένων που περιέχουν. | Παράδειγμα αποτελούν οι αριθμοί μητρώου οι οποίοι χορηγούνται για χρήση από τις υπηρεσίες κοινωνικής ασφάλισης κ.λπ. |
| **Συναίνεση του πολίτη** | Η συναίνεση του πολίτη για την διατήρηση των προσωπικών του στοιχείων προκειμένου να συγκροτηθούν έγκυρα μητρώα αποτελεί άλλη μία κρίσιμη παράμετρο η οποία καθορίζεται από την εθνική νομοθεσία του κάθε κράτους. | Προαιρετική, Υποχρεωτική ή μη αναγκαία οι λύσεις διαφοροποιούνται σε κάθε κράτος. |
| **C. Επιλογές Αυθεντικοποίησης** | | |
| **Χαρακτηριστικό Γνώρισμα** | **Περιγραφή / Τιμές** | **Παρατηρήσεις** |
| **Συστήματα Δημοσίου Κλειδιού** | Τα συστήματα PKI αποτελούν την πιο διαδεδομένη μέθοδο αυθεντικοποίησης. Εξετάζονται οι προϋποθέσεις κάτω από τις οποίες λειτουργούν σε κάθε κράτος και οι αρχές οι οποίες είναι υπεύθυνες για την | Υφίστανται διαφοροποιήσεις από κράτος σε κράτος ως προς την επιλογή του φορέα διατήρησης των έγκυρων μητρώων ο οποίος μπορεί να διίσταται από κάποια δημόσια αρχή έως κάποιο φορέα του |

| | | |
|---|---|---|
| | λειτουργία των συστημάτων αυτών. | ιδιωτικού τομέα |
| **Άλλοι τρόποι αυθεντικοποίησης** | Συστήματα βασισμένα στη χρήση συνθηματικών, αποτελούν μία άλλη ευρέως υιοθετημένη εναλλακτική πρακτική αυθεντικοποίησης η οποία εφαρμόζεται στα διάφορα κράτη. Διακρίνονται Συστήματα single factor, multifactor με password list, με password based PIN calculator, ή μέσω κινητού τηλεφώνου. | Οι πολιτικές δύναται να διαφέρουν σε αρκετά σημεία, από τον φορέα έκδοσης των διαπιστευτηρίων εισόδου στις εφαρμογές έως την πλήρη διαχείριση τους από φορείς του δημόσιου ή εναλλακτικά του ιδιωτικού τομέα |
| **Πολιτικές αυθεντικοποίησης** | Συγκρίνονται οι πολιτικές αυθεντικοποίησης του κάθε κράτους και τα επίπεδα εμπιστοσύνης τα οποία καθορίζονται στο κάθε κράτος. Διαφοροποιήσεις από επίσημα υιοθετημένες πολιτικές, έως τελείως άτυπες προσεγγίσεις είναι ευδιάκριτες μεταξύ των κρατών μελών. | |
| **Επίπεδα εμπιστοσύνης** | Ο καθορισμός επιπέδων ασφάλειας κατά την αυθεντικοποίηση διαφέρει σημαντικά από κράτος σε κράτος με τον καθορισμό από 2 έως 5 επιπέδων στα διάφορα κράτη που μελετήθηκαν. | Τα επίπεδα ασφάλειας συγκρίνονται και με βάση το ενιαίο Ευρωπαϊκό πιλοτικό πρόγραμμα STORK, προκειμένου να τυποποιηθούν τα επίπεδα στη βάση μίας ενιαίας κωδικοποίησης. Διακρίνονται επίπεδα από 1 έως και 4 με βάση την κωδικοποίηση του προγράμματος STORK. |

## D. Χρησιμοποιούμενες Τεχνολογίες

| Χαρακτηριστικό Γνώρισμα | Περιγραφή / Τιμές | Παρατηρήσεις |
|---|---|---|
| **Πρότυπα smart cards που υποστηρίζονται** | Τα πρότυπα τα οποία χρησιμοποιούνται διαφέρουν από τα ελάχιστα δυνατά πρότυπα τα οποία επιβάλλονται από την Ευρωπαϊκή Ένωση και τους κανονισμούς του ICAO. | Αποδεκτά πρότυπα προς τα οποία πρέπει να συμμορφώνονται οι λύσεις ως προς τις κάρτες αποτελούν τα ISO 7816, ISO 24727 και ISO 14443 για όσες χώρες εκδίδουν δελτία σύμφωνα με τις προδιαγραφές για την κάρτα του πολίτη. |
| **Μέσο ενσωμάτωσης διακριτικών ταυτοποίησης** | Αναλύονται τεχνολογικές υποδομές οι οποίες υποστηρίζουν τις υλοποιήσεις των κρατών σε έξυπνες κάρτες, RFID chips και κάρτες SIM κινητών τηλεφώνων. | |
| **Κατασκευαστές υλικών** | Διάφορες εταιρείες – προμηθευτές οι οποίες αναλύονται κατά κράτος | |

| | | |
|---|---|---|
| **Τύπος/Μικροελεγκτής** | Συγκριτική παρουσίαση των λύσεων συμμορφούμενες ως προς πιστοποιήσεις EAL4+, EAL5+ κ.τ.λ. | |
| **Χρησιμοποιούμενα πρότυπα προστασίας** | Στο θέμα της ασφάλειας αποδεκτά πρότυπα ασφάλειας αποτελούν τα ISO 9796, 9797, 9798, ISO 10116, ISO 10118, ISO 15408 | |
| **Πολλαπλή Χρηστικότητα** | Τα κατά περίπτωση χρησιμοποιούμενα applets σε ορισμένα κράτη εξυπηρετούν την χρηστικότητα των λύσεων eID σε πολλούς τομείς δραστηριότητας. | |
| **Φορέας παροχής λύσεων ταυτοποίησης κινητής τηλεφωνίας** | Εταιρείες κινητής τηλεφωνίας ανά κράτος οι οποίες υλοποιούν λύσεις eID. | Προσδιορίζεται και ο τρόπος με τον οποίο παρέχεται η υπηρεσία ταυτοποίησης σε κάθε ξεχωριστή λύση. |

**Πίνακας 1: Κριτήρια αξιολόγησης εθνικών πολιτικών eIDM ανά επίπεδο τμηματοποίησης**

## 1.5 Ανάλυση Περιεχομένων κεφαλαίων

Η παρούσα μελέτη αποσκοπεί στην παρουσίαση των τάσεων και πρακτικών στην ανάπτυξη και λειτουργία των λύσεων ηλεκτρονικής ταυτοποίησης, όπως αυτές προκύπτουν από την ανάλυση των λύσεων σε επίπεδο χωρών στην Ευρώπη, αλλά και σε επίπεδο ευρύτερου ενιαίου σχεδιασμού στην Ευρωπαϊκή Ένωση.

Οι χώρες των οποίων οι εθνικές πολιτικές θα αναλυθούν, είναι οι 27 χώρες Κράτη Μέλη της Ευρωπαϊκής Ένωσης, οι 3 χώρες μέλη της ΕΕΑ[3] (Νορβηγία, Ισλανδία και Λιχτενστάιν)[4] και οι 2 υποψήφιες προς ένταξη χώρες στην Ευρωπαϊκή Ένωση (Τουρκία και Κροατία).

Τα αποτελέσματα της μελέτης παρουσιάζονται στις παρακάτω ενότητες και συγκεκριμένα:

Στο **2ο Κεφάλαιο**, εξετάζονται οι βασικές επιλογές που έχουν υιοθετηθεί από τις Ευρωπαϊκές χώρες-μέλη, στο θέμα της χρήσης διακριτικών αυθεντικοποίησης όπως ηλεκτρονικές κάρτες ταυτοποίησης, soft διακριτικά ταυτοποίησης, καθώς και μία σειρά από άλλες πρόσφατα υλοποιημένες μεθόδους ταυτοποίησης όπως τα βιομετρικά δεδομένα.

Στο **3ο Κεφάλαιο** συγκεντρώνεται και αναλύεται το βασικό σύνολο της Ευρωπαϊκής Νομοθεσίας, το οποίο σε μεγάλο βαθμό καθορίζει το ρου στο θέμα

[3] EEA: European Economic Area

[4] Για τις οποίες χώρες αυτές, αν και δεν έχουνε ενσωματωθεί στην Ε.Ε., προβλέπεται η συμμετοχή τους στην εσωτερική αγορά της Ευρωπαικής Ένωσης. Βλ. http://eeas.europa.eu/eea/

της υλοποίησης και της διαχείρισης των ηλεκτρονικών ταυτοτήτων στην Ευρώπη.

Στο **4ο Κεφάλαιο** αναλύονται οι πολιτικές οι οποίες συναντώνται στις υπό μελέτη χώρες ως προς το θέμα βασικών στρατηγικών ζητημάτων, τα οποία εν πολλοίς χαρακτηρίζουν την εξωστρέφεια των εθνικών συστημάτων eID και τις τάσεις διαλειτουργικότητάς τους, όπως οι φορείς διαχείρισης των συστημάτων, η ανάμιξη του ιδιωτικού τομέα και η χρήση έγκυρων μητρώων ως πηγή δεδομένων ταυτοποίησης.

Στην **5ο Κεφάλαιο** εξετάζονται οι επιλογές των συστημάτων αυθεντικοποίησης στις υπό μελέτη χώρες. Στην ανάλυση περιλαμβάνονται συστήματα που βασίζονται σε Υποδομή Δημόσιου Κλειδιού (PKI) και συστήματα που βασίζονται στη χρήση συνθηματικών. Επιπλέον, εξετάζονται οι πολιτικές αυθεντικοποίησης που έχουν υιοθετηθεί στις διάφορες χώρες ως προς τα επίπεδα εμπιστοσύνης.

Στο **6ο Κεφάλαιο** η ανάλυση και η συγκριτική επισκόπηση περιστρέφεται γύρω από τις χρησιμοποιούμενες τεχνολογίες και τις υποδομές οι οποίες χρησιμοποιούνται από τα κράτη προκειμένου να θωρακίσουν τα δημόσια πιστοποιητικά τα οποία εκδίδουν για τους σκοπούς της ταυτοποίησης και τα οποία απαιτούνται προκειμένου να επιτύχουν την ακεραιότητα των δεδομένων που περιέχονται στα δημόσια έγγραφα, την μείωση της πιθανότητας κλοπής των δεδομένων και της αποποίησης εκ μέρους των πολιτών που αυθεντικοποιούνται.

Στο **7ο Κεφάλαιο** παρουσιάζεται το βασικό Ευρωπαϊκό πλάνο στο θέμα της διαχείρισης των eID, το eIDM Roadmap, καθώς και μία σειρά από Ευρωπαϊκά έργα τα οποία περιστρέφονται γύρω από το θέμα των ηλεκτρονικών ταυτοτήτων και είτε βρίσκονται σε εξέλιξη, είτε πρόκειται να υλοποιηθούν στο άμεσο μέλλον.

Στο **8ο Κεφάλαιο** αναλύεται το παράδειγμα της πρόσφατα υλοποιημένης λύσης του Γερμανικού δελτίου eID, το οποίο αποτελεί αυτή την στιγμή την πλέον σύγχρονη από την άποψη των ενσωματωμένων μηχανισμών ασφάλειας εθνική λύση, και η οποία αναμένεται να αποτελέσει οδηγό για την υλοποίηση της Κάρτας του Πολίτη στην Ελλάδα.

Στο **9ο Κεφάλαιο** παρουσιάζονται μία σειρά από μελλοντικές προκλήσεις τις οποίες αντιμετωπίζουν τα συστήματα διαχείρισης ταυτοτήτων, τόσο σε εθνικό επίπεδο, όσο και σε επίπεδο διαλειτουργικότητας σε σχέση με τις αντίστοιχες λύσεις των άλλων χωρών.

Τέλος στο **10ο Κεφάλαιο** περιλαμβάνονται κάποια συνολικά συμπεράσματα.

# 2. ΥΠΟΔΟΜΕΣ ΚΑΙ ΕΠΙΛΟΓΕΣ ΤΑΥΤΟΠΟΙΗΣΗΣ

Σε αυτό το κεφάλαιο θα παρουσιαστούν οι βασικές δυνατότητες – επιλογές που υπάρχουν στο θέμα των μεθόδων ταυτοποίησης και οι οποίες επιλέγονται κατά περίπτωση από τα διάφορα κράτη μέλη της Ευρωπαϊκής Ένωσης.

Η ανάλυση που θα ακολουθήσει αφορά :

Στα **διακριτικά αυθεντικοποίησης**, τα μέσα δηλαδή τα οποία χρησιμοποιούνται για την επίτευξη της ταυτοποίησης (όπως π.χ. η χρήση κάρτας ηλεκτρονικής ταυτοποίησης), καθώς επίσης εξετάζεται η χρήση μοναδικών αναγνωριστικών και οι πρακτικές που ακολουθούν τα διάφορα κράτη σε σχέση με τα διάφορα εθνικά μητρώα[5] .

Επιπρόσθετα εξετάζεται η δυνατότητα ταυτοποίησης των πολιτών με τη χρήση κινητών τηλεφώνων ή ακόμη και βιομετρικών δεδομένων.

## 2.1 Διακριτικά Ταυτοποίησης

### 2.1.1 Παραδοσιακά έντυπα δελτία ταυτοποίησης

Στην ενότητα αυτή παρέχεται μία σύνοψη των παραδοσιακών (έντυπων) δελτίων ταυτοποίησης, τα οποία δεν συμπεριλαμβάνουν ηλεκτρονική λειτουργικότητα (όπως για παράδειγμα μία ταυτότητα η οποία παρέχεται σε έντυπη μορφή, χωρίς καμία επιπλέον λειτουργικότητα έξυπνης κάρτας η οποία θα μπορούσε να την καταστήσει κατάλληλη για ηλεκτρονική ταυτοποίηση/αυθεντικοποίηση σε εφαρμογές της ηλεκτρονικής διακυβέρνησης) οι οποίες χρησιμοποιούνται στις υπό μελέτη χώρες[4].

Ειδικότερα περιλαμβάνονται:

- ✓ Κάθε εθνικό δελτίο ταυτότητας το οποίο έχει εκδοθεί από κυβερνητικό φορέα και βρίσκεται σε λειτουργική φάση. Εάν το δελτίο έχει αντικατασταθεί, ή πρόκειται να αντικατασταθεί από κάποια ηλεκτρονική ταυτότητα, αυτό περιγράφεται στην στήλη με την ένδειξη “ΚΑΤΑΣΤΑΣΗ”.

[5] National registers

- ✓ Άλλες έντυπες κάρτες οι οποίες δεν αποτελούν κύρια ταυτότητα και οι οποίες δεν περιέχουν κάποιο τσιπ ή ηλεκτρονικό εξάρτημα, αλλά οι οποίες παρ' όλα αυτά χρησιμοποιούνται για ηλεκτρονική αυθεντικοποίηση. Ειδικότερα σε αυτή την κατηγορία ανήκουν έντυπες κάρτες οι οποίες περιλαμβάνουν κωδικούς οι οποίοι είναι τυπωμένοι επ' αυτών και οι οποίοι χρησιμοποιούνται για τους σκοπούς της αυθεντικοποίησης δύο παραγόντων (password lists).[6]

Ο κύριος σκοπός του πίνακα που ακολουθεί είναι να προσδιορίσει το ποιες χώρες εκδίδουν έντυπα δελτία ταυτοποίησης (και θα μπορούσαν συνεπώς να είναι λιγότερο δεκτικές κοινωνικά ή πολιτικά προκειμένου να εισάγουν κάρτες ηλεκτρονικής ταυτοποίησης ως διακριτικά αυθεντικοποίησης, αν δεν το κάνουν ήδη), όπως επίσης και να προσδιορίσει σε ποιο βαθμό αυτά τα έντυπα διακριτικά ταυτοποίησης χρησιμοποιούνται ως εργαλεία ταυτοποίησης σε εφαρμογές της ηλεκτρονικής διακυβέρνησης.

| Χώρα | Περιγραφή | Ομάδα Χρηστών | Προαιρετική/ Υποχρεωτική | Κατάσταση |
|---|---|---|---|---|
| **Βέλγιο** | Εθνικό δελτίο ID | Βέλγοι άνω των 12 ετών & αλλοδαποί οι οποίοι διαμένουν μόνιμα στο Βέλγιο | Υποχρεωτική | Η έκδοση τους σταμάτησε από το 2008, οπότε και ξεκίνησαν να εκδίδονται στη θέση της αντίστοιχα δελτία eID[7]. Για τους αλλοδαπούς η προαιρετική έκδοση ξεκίνησε από τον Ιούλιο του 2008. [8] |
| | Ομοσπονδιακό αναγνωριστικό<br><br>(όχι δελτίο ID) | Αφορά τα ίδια ως άνω άτομα (δικαιούχους κάρτας ID) καθώς και τους δικαιούχους κάρτας SIS[9] | Προαιρετικό | Καταργείται σταδιακά υπέρ του δελτίου eID (ομοίως όπως και παραπάνω) |

[6] Τέτοιου είδους κάρτες κωδικών είναι δυνατόν να εκδίδονται και από φορείς οι οποίοι ανήκουν στον ιδιωτικό τομέα, όπως για παράδειγμα οι τράπεζες για την επίτευξη εισόδου στα συστήματα ηλεκτρονικής τραπεζικής που διαθέτουν.

[7] Δράση που ολοκληρώνεται στα πλαίσια του έργου BelPIC: Belgian Personal Identity Card Project. Παρόμοια δελτία ταυτότητας υπάρχουν και για τους αλλοδαπούς που διαμένουν στη χώρα, τα οποία θα αντικατασταθούν από ισοδύναμα δελτία eID από τον Ιούλιο του 2008.

[8] Belgium – the national eID Card, A true e-Government building block, Gemalto p.3

[9] Κάρτες Υγείας των Βέλγων Πολιτών

| | | | | |
|---|---|---|---|---|
| **Βουλγαρία** | Εθνικό δελτίο ID | Βούλγαροι πολίτες οι οποίοι έχουν ηλικία μεγαλύτερη των 14 ετών | Υποχρεωτικό | Επιχειρησιακή Λειτουργία. Δεν σχεδιάζεται ακόμα η χρήση δελτίων eID. Ταυτότητα τύπου TD1[10] [5] από τις 29/3/2010. |
| | Δελτίο BULLSTAT[11] | Εταιρείες, μη κερδοσκοπικοί οργανισμοί, δημόσιοι φορείς, άλλες νομικές οντότητες, υποκαταστήματα ξένων εταιρειών, και αυτοαπασχολούμενοι | Υποχρεωτικό | Οι χρήστες μπορούν να επιλέξουν να λάβουν ηλεκτρονικό ή έντυπο δελτίο BULLSTAT. |
| **Γαλλία** | Εθνικά δελτία ID | Γάλλοι πολίτες πάνω από την ηλικία των 16 (οι αλλοδαποί λαμβάνουν άδεια παραμονής επί ειδικού δελτίου) | Προαιρετικό | Σχεδιάζεται να αντικατασταθεί από ένα δελτίο eID, το οποίο υλοποιείται αυτή την περίοδο. |
| **Γερμανία** | Δελτίο Ταυτότητας (Personalausweis) | Γερμανοί πολίτες πάνω από την ηλικία των 16 | Υποχρεωτικό | Τύπου ID2[6]. Αντικαθίσταται από δελτίο eID από την 1η Νοεμβρίου του 2010[7] |
| **Ελλάδα** | Εθνικό δελτίο ID | Έλληνες πολίτες πάνω από την ηλικία των 12 | Υποχρεωτικό | Θα αντικατασταθεί σταδιακά από δελτία eID (Κάρτα του Πολίτη) σε χρόνο που δεν έχει προσδιορισθεί, εκτιμάται όμως εντός του 2011. Ο σχεδιασμός της κάρτας βρίσκεται ένα στάδιο μετά τη δημόσια διαβούλευση.[12] |
| | Δελτία Ταυτότητας Αστυνομικών | Εν ενεργεία αστυνομικοί | Υποχρεωτικό | Δελτίο Ταυτότητας με format TD1 τα οποία αντικατέστησαν μέσα |

[10] TD1: Travel Document 1. Κωδικοποίηση του ICAO για τα ταξιδιωτικά έγγραφα με διαστάσεις (85,6x53,98mm). Διαθέτουν Μηχαναγνώσιμη Ζώνη (MRZ).

[11] Bullstat: Δελτίο το οποίο εκδίδεται και στο οποίο υπάρχει ένας μοναδικός αριθμός ο οποίος αντιστοιχεί τον κάτοχό του με την αντίστοιχη εγγραφή στις οικονομικές υπηρεσίες της Βουλγαρίας, από όπου μέσω του οποίου στη συνέχεια μπορεί να του γίνεται ο ανάλογος οικονομικός έλεγχος

[12] Δημόσια Διαβούλευση για τη μέγιστη αξιοποίηση της κάρτας του πολίτη. Ολοκληρώθηκε την 12/10/2010 Βλ. http://www.opengov.gr/ypes/?p=863

| | | | | |
|---|---|---|---|---|
| | | | | στο 2010 τα παλαιού τύπου υπηρεσιακά δελτία ταυτότητας |
| **Ηνωμένο Βασίλειο** | Εθνικό Δελτίο ID | Όλα τα άτομα πάνω από την ηλικία των 16 οι οποίοι είναι ή επιθυμούν να διαμείνουν μόνιμα στην Αγγλία | Προαιρετικό | Για τους πολίτες του Η.Β. η πρόβλεψη είναι ότι τα πρώτα νέα δελτία ταυτότητας θα εκδοθούν το 2012[8] |
| **Ισλανδία** | Εθνικά δελτία ID | Κάθε πολίτης ο οποίος είναι καταγεγραμμένος στο μητρώο πληθυσμού και έχει ηλικία άνω των 14 ετών | Υποχρεωτικό | Περιλαμβάνει το SSN[13] το οποίο αποτελεί την βάση για την διαχείριση των ταυτοτήτων στην Ισλανδία |
| **Ιταλία** | Εθνικό δελτίο ID | Ιταλοί πάνω από την ηλικία των 15 ετών, καθώς και οι αλλοδαποί οι οποίοι διαμένουν μόνιμα στην Ιταλία | Προαιρετικό | Σταδιακά αντικαθίσταται από το δελτίο eID σε μία βάση επαρχεία προς επαρχεία μετά την 8/11/2007[14] |
| **Ισπανία** | Εθνικό δελτίο ID ("Documento Nacional de Identidad", "DNI") | Ισπανοί πολίτες πάνω από την ηλικία των 14 | Υποχρεωτικό | Αντικαθίστανται από δελτία eID από το Μάρτιο του 2006.[15] |
| **Κροατία** | Εθνικό δελτίο ID | Κροάτες με ηλικία πάνω από 14 | Υποχρεωτικό | Αντικαθίσταται σταδιακά από την 1/1/2009 από το αντίστοιχο δελτίο eID |
| **Κύπρος** | Εθνικό δελτίο ID | Κύπριοι και φυσικά πρόσωπα με μόνιμη διαμονή στη Κύπρο | Υποχρεωτικό | Οι έξυπνες κάρτες[16] θεωρούνταν μη νομικά αποδεκτές, αλλά από τον Μάρτιο του 2008 ξεκίνησαν οι διαδικασίες προκειμένου να εισαχθούν eIDs για ηλεκτρονικά |

[13] SSN: Social Security Number

[14] Βλ. http://www.servizidemografici.interno.it/sitoCNSD/pagina.do?metodo=homeSettore&servizio=navigazione&codiceFunzione=PR&codiceSettore=CI

[15] Βλ. Cuepro Nacional de Policia. http://www.dnielectronico.es/

[16] Τον Μάρτιο του 2008, η Κυπριακή Κυβέρνηση ξεκίνησε τις διαδικασίες προκειμένου να εισάγει ηλεκτρονικά δελτία ταυτοποίησης/αυθεντικοποίησης (eID, smart cards) για δημόσιες υπηρεσίες, προκειμένου να εξασφαλιστεί η απρόσκοπτη πρόσβαση σε υπηρεσίες του δημόσιου τομέα πέραν των συνόρων

| | | | | |
|---|---|---|---|---|
| | | | | παρεχόμενες δημόσιες υπηρεσίες[9].[17] |
| **Λιθουανία** | Εθνικό δελτίο ID | Λιθουανοί πολίτες πάνω από την ηλικία των 16 | Υποχρεωτικό | Αντικαθίστανται από το Λιθουανικό δελτίο eID, από την 1/1/2009[18] |
| **Λιχτενστάιν** | Εθνικό δελτίο ID | Πολίτες του Λιχτενστάιν | Προαιρετικό | Αντικαθίσταται από το νέο δελτίο eID από τις 23 Ιουνίου 2009. |
| **Λουξεμβούργο** | Εθνικό δελτίο ID | Πολίτες του Λουξεμβούργου πάνω από την ηλικία των 15 | Υποχρεωτικό | Ένα δελτίο eID το οποίο πρόκειται να εκδοθεί στα πλαίσια του κράτους αναμένεται να αντικαταστήσει σταδιακά το παλιό δελτίο ταυτότητα από το2011. |
| **Μάλτα** | Εθνικό δελτίο ID | Μαλτέζοι πολίτες πάνω από την ηλικία των 14 | Υποχρεωτικό | Σχεδιάζεται να αντικατασταθεί από δελτίο eID, διαδικασία η οποία είναι προγραμματισμένη να ξεκινήσει τον Σεπτέμβριο του 2011[10] |
| **Ολλανδία** | Εθνικό δελτίο ID | Ολλανδοί πολίτες πάνω από την ηλικία των 14 | Προαιρετικό[19] | Σχέδια σχετικά με την αντικατάσταση των δελτίων με μία κάρτα eID βρίσκονται σε φάση αναθεώρησης |
| **Πολωνία** | Εθνικό δελτίο ID | Πολωνοί πολίτες πάνω από την ηλικία των 18, ή πάνω από την ηλικία των 15 εφ' όσον εργάζονται ή είναι νομικά ανεξάρτητοι | Υποχρεωτικό | Σχεδιάζεται να εισαχθεί ένα δελτίο eID το 2011 |
| **Πορτογαλία** | Εθνικό δελτίο ID | Πορτογάλοι πολίτες πάνω από την ηλικία των 6 [20] | Υποχρεωτικό | Σταδιακά αντικαθίσταται από δελτίο eID από το |

[17] Τα σχέδια αυτά παραμένουν σε αυτή την φάση στην διαδικασία της προέγκρισης από το Υπουργείο Εσωτερικών της Κύπρου.
[18] Βλ. http://www.dokumentai.lt/en/pic.php#atk%202009
[19] Οι πολίτες θα πρέπει να μεταφέρουν ένα έγγραφο αποδεικτικό της ταυτότητάς τους, αλλά αυτό μπορεί για παράδειγμα να είναι κάποιο διαβατήριο ή ίσως κάποια άδεια οδήγησης

| | | | | |
|---|---|---|---|---|
| | | | | Φεβρουάριου 2007 |
| **Ρουμανία** | Εθνικό δελτίο ID (Carte de identitate) | Πολίτες πάνω από την ηλικία των 14 | Υποχρεωτικό | Σχεδιάζεται να αντικατασταθεί από ένα δελτίο eID από το 2011[11] |
| **Σλοβακία** | Εθνικό δελτίο ID | Πολίτες πάνω από την ηλικία των 15 | Υποχρεωτικό | Σχεδιάζεται να αντικατασταθεί από ένα δελτίο eID μετά το 2012 [21] |
| **Σλοβενία** | Εθνικό δελτίο ID | Πολίτες πάνω από την ηλικία των 18 (ή και νεότεροι εφόσον οι γονείς συναινούν προς τούτο | Προαιρετικό | Σχεδιάζεται να αντικατασταθεί από ένα δελτίο eID[22] |
| **Τσέχικη Δημοκρατία** | Εθνικό δελτίο ID | Τσέχοι πολίτες και φυσικά πρόσωπα με μόνιμη διαμονή στην Τσεχία | Υποχρεωτικό | Από το 2010 αναμενόταν να ξεκινήσει η αντικατάσταση τους από νέα δελτία ID μέσω του νόμου Act on ID Cards, η προτεινόμενη όμως πλέον νέα ημερομηνία εισαγωγής ανάγεται στη 1/1/2012. Μία νέα πλαστική κάρτα θα αντικαταστήσει την κλασσική ταυτότητα. Το δελτίο αυτό θα εκδοθεί σε δύο εκδόσεις, ένα πλαστικό δελτίο χωρίς τσιπ και ένα σε έξυπνη κάρτα. [12] |
| **Ουγγαρία** | Εθνικά δελτία ID | Κάθε πολίτης ο οποίος | Προαιρετικό | Θα αντικατασταθεί από |

[20] Καλύπτονται και Βραζιλιάνοι πολίτες από τη συνθήκη του Porto Seguro

[21] Αυτή την περίοδο πραγματοποιούνται αναλύσεις στην Σλοβακία και η τελική απόφαση θα καθορίσει τις ακριβείς προδιαγραφές των ταυτοτήτων, οι οποίες δεν αναμένεται να εκδοθούν πριν από την συμπλήρωση 2 ετών. Οπότε η αρχή έκδοσης eID στην Σλοβακία προσδιορίζεται για το 2012.

[22] Το 2008 το υφιστάμενο νομοθετικό πλαίσιο τροποποιήθηκε προκειμένου να εισαχθεί ένα δελτίο eID το οποίο θα επιτρέπει την ενσωμάτωση σε μία ενιαία κάρτα του δελτίου ταυτότητας, αναγνωρισμένων πιστοποιητικών καθώς επίσης και ενός δελτίου ιατρικής ασφάλισης. Παρ' όλα αυτά αν και οι διατάξεις ψηφίστηκαν, εν τούτοις το έργο ανεστάλη και αυτό είχε ως αποτέλεσμα ότι αν τελικά κάποια στιγμή προκριθεί προς υλοποίησης, οι διατάξεις αυτές θα πρέπει να αλλάξουν εκ νέου, δεδομένου του ότι το project για το θέμα της κάρτας για την ασφάλεια υγείας προχωράει ανεξάρτητα από αυτό της ταυτότητας.

| | | | | |
|---|---|---|---|---|
| | | είναι καταγεγραμμένος στο μητρώο πληθυσμού και έχει ηλικία άνω των 14 ετών | | ένα δελτίο ηλεκτρονικής ταυτότητας στο εγγύς μέλλον (χωρίς να προσδιορίζεται το πότε) |
| | Προσωπική ταυτοποίηση & πιστοποιητικό διεύθυνσης | Κάθε πολίτης ο οποίος είναι καταγεγραμμένος στο μητρώο πληθυσμού και έχει ηλικία άνω των 14 ετών | Προαιρετικό | Περιέχει τον προσωπικό αριθμό ταυτοποίησης |
| **Τουρκία** | Εθνικά Δελτία ID | Τούρκοι πολίτες | Υποχρεωτικό | Αντικαθίστανται από δελτία eID από το 2007 |
| **Φινλανδία** | Έντυπο δελτίο του Συλλόγου Φινλανδικών Τραπεζών (TUPAS[23]) | Πελάτες τραπεζικής | Προαιρετικό | Στην παρούσα φάση χρησιμοποιείται πιο συχνά από ότι τα δελτία eID |

**Πίνακας 2: Έντυπα διακριτικά αυθεντικοποίησης στα Ευρωπαϊκά Κράτη**

Στον παραπάνω πίνακα δεν περιλαμβάνονται χώρες όπως η Αυστρία και η Εσθονία όπου τα δελτία eID έχουνε αντικαταστήσει πλήρως τα έντυπα δελτία ID που χρησιμοποιούνταν τα προηγούμενα χρόνια.

Ο παραπάνω πίνακας δείχνει ότι:

- ✓ Σε σύνολο 32 χωρών, οι 25 έχουνε κάποιο έντυπο διακριτικό το οποίο χρησιμοποιείται για την ταυτοποίηση των χρηστών, σε 17 από τις οποίες η προμήθειά του διακριτικού αυτού είναι υποχρεωτική ενώ σε 8 από τις οποίες η κατοχή τους είναι προαιρετική

- ✓ Από το σύνολο των χωρών οι οποίες έχουνε κάποιο έντυπο δελτίο ταυτότητας, οι 22 έχουνε αποφασίσει να εισάγουνε κάποιου τύπου ηλεκτρονικό δελτίο ταυτότητας στη θέση του προϋπάρχοντος έντυπου. Οι 11 από αυτές εκδίδουν ήδη δελτία eID για τους πολίτες των χωρών τους (Βέλγιο, Γερμανία, Ισλανδία, Ισπανία, Ιταλία, Κροατία, Λιχτενστάιν, Λιθουανία, Πορτογαλία, Τουρκία και Φινλανδία). 8 χώρες πρόκειται να το πράξουν μέσα στα επόμενα 2 χρόνια (Ελλάδα, Ηνωμένο Βασίλειο, Λουξεμβούργο, Μάλτα, Πολωνία, Ρουμανία, Σλοβακία και Τσεχία). Σε 3 από τις χώρες βρίσκονται στη φάση του σχεδιασμού (Γαλλία, Κύπρος και Σλοβενία). Τέλος η εισαγωγή κάποιου δελτίου eID βρίσκεται σε φάση

[23] TUPAS: Πρόκειται για μία μέθοδο αυθεντικοποίησης που δημιουργήθηκε για την Φινλανδική Ομοσπονδία Οικονομικών Υπηρεσιών και χρησιμοποιείται από όλες τις κύριες Φινλανδικές τράπεζες συμπεριλαμβανομένων των Aktia, Osuuspankki, Nordea, Sampo, και Tapiola

αναθεώρησης επί του παρόντος στην Ολλανδία, αλλά χωρίς ακόμα να υπάρχουν διαθέσιμα συγκεκριμένα σχέδια.

- ✓ Τέλος σε 2 από τις 32 χώρες, κάποια άλλη κάρτα πέραν της ταυτότητας, φαίνεται να μπορεί να διαδραματίσει τον ίδιο ρόλο μέσω της οποίας μπορείς επίσης να καταστεί εφικτή και η on-line αυθεντικοποίηση. Στις χώρες αυτές (Βέλγιο και Φινλανδία) το ρόλο αυτό διαδραματίζουν οι ήδη υπάρχουσες έξυπνες κάρτες. Επιπρόσθετα στην Φινλανδία η αποδοχή του κόσμου για τα παλιού τύπου έντυπα δελτία φαίνεται να υπερβαίνει αυτή των έξυπνων καρτών.

### 2.1.2 Ηλεκτρονικά δελτία ταυτοποίησης

Όπως ήδη διαπιστώθηκε από την προηγούμενη ενότητα, πολλές είναι οι χώρες οι οποίες πραγματοποίησαν στροφή προς τις ηλεκτρονικές ταυτότητες. Στην ενότητα αυτή δίνεται θα πραγματοποιηθεί μία πιο κοντινή προσέγγιση στα δελτία ηλεκτρονικής ταυτοποίησης (όπως για παράδειγμα έξυπνες κάρτες, οι οποίες περιέχουνε κάποιο τσιπ ή κάποιο άλλο ηλεκτρονικό εξάρτημα, όπως RFID, το οποίο να μπορεί να χρησιμοποιηθεί στα πλαίσια της ηλεκτρονικής αυθεντικοποίησης) τα οποία να έχουν εκδοθεί ή των οποίων η χρήση να εξετάζεται στις υπό μελέτη χώρες.

Θα πρέπει να σημειωθεί ότι κάποιες χώρες οι οποίες έχουνε παρουσιαστεί στην προηγούμενη ενότητα, μπορεί να μην παρουσιάζονται στην παρούσα ενότητα (επειδή ίσως δεν έχουνε ακόμη κάποιο σχέδιο σχετικά με τις ηλεκτρονικές ταυτότητες), καθώς επίσης και αντίθετα κάποια χώρα μπορεί να περιλαμβάνεται στην παρούσα ενότητα, αλλά να μην είχε αναφερθεί στην προηγούμενη (όπως οι περιπτώσεις της Αυστρίας και της Εσθονίας για τις οποίες έχει ήδη γίνει αναφορά στην προηγούμενη ενότητα).

Επιπρόσθετα θα πρέπει να σημειωθεί ότι ο παρακάτω πίνακας χρησιμοποιεί μία ευρεία έννοια του όρου "δελτίο eID". Έτσι κάτω υπό τον όρο αυτό περιλαμβάνεται κάθε δελτίο eID το οποίο έχει εκδοθεί από τη δημόσια διοίκηση, μίας χώρας, αλλά και ακόμη περιπτώσεις όπου τα δελτία eID έχουνε εκδοθεί από κάποιο ιδιωτικό CSP[24] ο οποίος έχει λάβει κάποια συγκεκριμένη κυβερνητική εντολή-εξουσιοδότηση προς τούτο (όπως για παράδειγμα στο Λουξεμβούργο και το Λιχτενστάιν), ή όπου οι έξυπνες κάρτες μπορούν να ενεργοποιηθούν και να χρησιμοποιηθούν σε εφαρμογές της ηλεκτρονικής διακυβέρνησης κατόπιν κάποιας απόφασης ορισμένου δημόσιου φορέα (όπως για παράδειγμα η Αυστριακή Bürgerkarte η οποία μπορεί να εκδοθεί από

[24] CSP: Certification Service Provider. Πάροχος Υπηρεσιών Πιστοποίησης

εταιρείες του ιδιωτικού τομέα, αλλά πρέπει να ενεργοποιηθεί ως Bürgerkarte με απόφαση της Αυστριακής SourcePIN authority, η οποία είναι τμήμα της Αυστριακής αρχής προστασίας δεδομένων).

Τέλος θα πρέπει να σημειωθεί ότι σε ένα αριθμό περιπτώσεων (όπως στην Ουγγαρία και την Ιταλία), η λύση η οποία παρουσιάζεται δεν είναι μία εξειδικευμένη έξυπνη κάρτα, αλλά μία σειρά από πρότυπα τα οποία μπορούν να χρησιμοποιηθούν προκειμένου να δημιουργηθούν συμβατές κάρτες. Στην περίπτωση της Αυστρίας , η λύση δεν χρειάζεται να είναι ούτε καν κάρτα αυτή καθ' αυτή (παρ' όλο που για τις ανάγκες του ακόλουθου πίνακα θεωρούνται ως λύσεις μόνο οι έξυπνες κάρτες που χρησιμοποιούνται).

Οι ακόλουθες χώρες αναφέρουν ότι εκδίδουν δελτία ηλεκτρονικής ταυτοποίησης (eID), ή σχεδιάζουν να πράξουν κάτι τέτοιο στο κοντινό μέλλον.

| Χώρα | Περιγραφή | Ομάδα Χρηστών | Προαιρετικό/ Υποχρεωτικό | Κατάσταση |
|---|---|---|---|---|
| **Αυστρία** | Κάρτα του πολίτη (Bürgerkarte) – σημειώνεται ότι η κάρτα του πολίτη μπορεί να πάρει και άλλες μορφές εκτός από έξυπνη κάρτα, αποτελώντας κατά βάση μία έννοια[25] η οποία δεν αντικατοπτρίζεται σε συγκεκριμένη τεχνολογική υποδομή | Φυσικά πρόσωπα που είναι εγγεγραμμένα στην Αυστρία και έχουν ηλικία > 18 | Προαιρετικό | Επιχειρησιακά Λειτουργικό από το 2003.[26] Το σύστημα βασίζεται σε πιστοποιητικά υπογραφής σε συνδυασμό με τη χρήση μοναδικών αναγνωριστικών[13] |
| **Βέλγιο** | Εθνικό δελτίο eID (BELPIC) | Βέλγοι πολίτες πάνω από την ηλικία των 12, καθώς και οι αλλοδαποί οι οποίοι διαμένουν μόνιμα στο Βέλγιο | Υποχρεωτικό | Σε επιχειρησιακή λειτουργία από το 2008. |
| **Γαλλία** | Εθνικό δελτίο eID (INES[27]) | Γάλλοι πολίτες (χωρίς όριο ηλικίας) | Υπό εξέταση | Στάδιο σχεδιασμού |

[25] Ουσιαστικά το Αυστριακό πλαίσιο αναφέρεται σε μία σειρά από κανόνες οι οποίοι υλοποιούμενοι με το συγκεκριμένο τρόπο σε οποιαδήποτε τεχνολογική υποδομή, μπορούν να έχουν το ίδιο έννομο αποτέλεσμα

[26] Η Αυστρία είναι η δεύτερη χώρα η οποία εισήγαγε ένα πλήρως λειτουργικό σύστημα διαχείρισης ηλεκτρονικών ταυτοτήτων, μόλις από το 2003, ακολουθώντας το παράδειγμα της Φινλανδίας η οποία ήταν η πρώτη Ευρωπαική χώρα η οποία είχε εισάγει ένα αντίστοιχο σύστημα eID από το 1999.

[27] INES: Identité Nationale Electronique *Sécurisée. Ασφαλές Ηλεκτρονικό δελτίο Ταυτότητας*

| | | | | |
|---|---|---|---|---|
| **Γερμανία** | Ηλεκτρονικό δελτίο ταυτότητας eID (Personalausweis) | Γερμανοί πολίτες πάνω από την ηλικία των 16 | Υποχρεωτικό[28] | Επιχειρησιακή Λειτουργία από την 1/11/2010 |
| **Ελλάδα** | Εθνικό δελτίο eID (Κάρτα του Πολίτη) | Δεν έχει καθοριστεί | Υποχρεωτικό | Σχεδιάζεται να τεθεί σε λειτουργία εντός του 2011. Έχει ολοκληρωθεί η φάση της δημόσιας διαβούλευσης |
| **Εσθονία** | Εθνικό δελτίο eID | Εσθονοί πολίτες, και ξένοι οι οποίοι διαμένουν μόνιμα στην Εσθονία | Υποχρεωτικό πάνω από την ηλικία των 15, προαιρετικό κάτω των 15 | Επιχειρησιακή Λειτουργία |
| **Ηνωμένο Βασίλειο** | Εθνικό δελτίο eID | Πολίτες του Ηνωμένου Βασιλείου και αλλοεθνείς οι οποίοι παραμένουν μόνιμα στο Ηνωμένο Βασίλειο για περισσότερο από 3 μήνες | Εθελοντικά, αλλά υπό αναθεώρηση προκειμένου να γίνει υποχρεωτικό στο μέλλον | Υλοποιημένο. Αλλά η εφαρμογή του αναβλήθηκε για το 2012 |
| **Ιρλανδία** | Κάρτα δημοσίων υπηρεσιών | Θα αποφασιστεί. Πιθανόν φυσικά πρόσωπα υποκείμενα στις Ιρλανδικές υπηρεσίες υγείας και στις κοινωνικές υπηρεσίες | Θα αποφασιστεί | Η κάρτα έχει ολοκληρώσει την φάση του σχεδιασμού. Η Ιρλανδία είναι μία χώρα όπου παραδοσιακά δεν υπάρχει ταυτοποίηση μέσω ταυτοτήτων και έτσι η εισαγωγή των eID καθυστερεί, με ένα αναθεωρημένο πλάνο να κάνει λόγο για εισαγωγή τους μέσα στο 2011. |
| **Ισλανδία** | Εθνικά δελτία eID τα οποία εκδίδονται από ιδιωτικούς CSPs | Φυσικά πρόσωπα τα οποία έχουνε ένα SSN στην Ισλανδία | Προαιρετικό | Επιχειρησιακή Λειτουργία από το 2007 |
| **Ισπανία** | Εθνικό δελτίο eID ("DNI electrónico" ή "DNI-e") | Ισπανοί πολίτες πάνω από την ηλικία των 14, καθώς και αλλοδαποί των | Υποχρεωτικό | Επιχειρησιακή Λειτουργία από το 2006. Εκτιμήσεις για το 2009 κάνανε λόγο για έκδοση 14.000.000 καρτών. |

[28] Η υποχρέωση αυτή δεν υφίσταται αν ο πολίτης έχει στην κατοχή του κάποιο άλλο αντίστοιχο δημόσιο έγγραφο όπως είναι το διαβατήριο.

| | | | | |
|---|---|---|---|---|
| | | οποίων έχει εγκριθεί η παραμονή στην Ισπανία | | |
| **Ιταλία** | Εθνικό δελτίο eID (carta d'identità elettronica – CIE) | Ιταλοί πολίτες και αλλοδαποί οι οποίοι έχουνε λάβει άδεια παραμονής στην Ιταλία από την ηλικία των 15 και πάνω | Προαιρετικό | Επιχειρησιακή Λειτουργία από το 2007. |
| | Εθνική κάρτα υπηρεσιών (National Service Card – CNS). Σημειώνεται ότι αυτό είναι μία προδιαγραφή για έξυπνες κάρτες, με κύριο στόχο να διασφαλίσει τη διαλειτουργικότητα, χωρίς να λαμβάνει απαραίτητα μόνο τη μορφή μιας κάρτας[29] | Εξαρτάται από την υλοποίηση, η οποία κυρίως αποφασίζεται σε επίπεδο επαρχίας | Εξαρτάται από την υλοποίηση, η οποία κυρίως αποφασίζεται σε επίπεδο επαρχίας | Έχει αναπτυχθεί. Επινοήθηκε κυρίως ως μία προσωρινή λύση έως ότου το CIE να είναι καθολικά διαθέσιμο. |
| **Κροατία** | Εθνικό δελτίο eID | Πολίτες πάνω από την ηλικία των 14 | Υποχρεωτικό | Σε επιχειρησιακή λειτουργία από το 2009, ένα χρόνο νωρίτερα από το προβλεπόμενο. |
| | FINA eID card | Όλες οι επιχειρήσεις και τα φυσικά πρόσωπα | Προαιρετικό | Σε επιχειρησιακή λειτουργία. Εκδίδεται από τον Κροατικό Χρηματοπιστωτικό Οργανισμό. Περιέχει δύο πιστοποιητικά: Για ταυτοποίηση και αυθεντικοποίηση |
| **Λετονία** | Εθνικό δελτίο eID | Πολίτες οι οποίοι έχουν ηλικία μεγαλύτερη των 15 | Υποχρεωτικό | Η επιχειρησιακή λειτουργία των δελτίων eID σχεδιαζόταν για το 1ο 6μηνο του 2010[30]. Δεν εντοπίστηκαν αναφορές της θέσης σε λειτουργία του εν λόγω συστήματος |
| **Λιθουανία** | Εθνικό δελτίο eID | Λιθουανοί | Υποχρεωτικό | Σε επιχειρησιακή λειτουργία από |

[29] Τα κύρια παραδείγματα του NSCs είναι το έργο SISS (Κάρτα Υγείας της επαρχίας Lombardy, όπου εκδόθηκαν περισσότερα από 9 εκατομμύρια κάρτες) και το NSC που εκδόθηκε στην επαρχεία Friuli Venezia Giulia

[30] Σχεδιάστηκε για το 2ο μισό του έτους 2008, αλλά στο τέλος του 2008, κάτω από ένα κυβερνητικό σχέδιο δράσης η Γραμματεία Ειδικών Υποθέσεων του Υπουργείου Υποθέσεων Ηλεκτρονικής Διακυβέρνησης εξουσιοδοτήθηκε να επανασχεδιάσει το προηγούμενο πλαίσιο που αφορούσε τα δελτία eID

| | | | | |
|---|---|---|---|---|
| | | πολίτες πάνω από 16 | | 1/1/2009 |
| **Λιχτενστάιν** | Εθνικό δελτίο eID | Πολίτες του Λιχτενστάιν | Προαιρετικό | Σε επιχειρησιακή λειτουργία από τις 23/6/2009 |
| **Λουξεμβούργο** | Έξυπνες κάρτες του ιδιωτικού τομέα ( Κάρτες της LuxTrust[31]) | Όλα τα φυσικά και νομικά πρόσωπα | Προαιρετικό | Βρίσκεται σε επιχειρησιακή λειτουργία, ενώ σχεδιάζεται και η θέση σε λειτουργία ενός δελτίο eID, μέσα στο 2011. |
| **Μάλτα** | Εθνικό δελτίο eID | Μαλτέζοι πολίτες πάνω από την ηλικία των 14 | Υποχρεωτικό | Αναμένεται να τεθεί σε κυκλοφορία και επιχειρησιακή λειτουργία από τον Σεπτέμβριο του 2011. |
| **Νορβηγία** | Εθνικό δελτίο eID | Φυσικά πρόσωπα που είναι εγγεγραμμένα στην Νορβηγία | Προαιρετικό | Βρίσκεται στο στάδιο του σχεδιασμού. Στην παρούσα φάση οριστικοποιούνται οι νομοθετικές ρυθμίσεις και οι τεχνικές προδιαγραφές και εκτιμάται ότι θα τεθεί σε λειτουργία εντός του 2011. |
| **Ολλανδία** | Εθνικό δελτίο eID (ENIK) | Ολλανδοί πολίτες | Προαιρετικό (οι πολίτες πρέπει να μεταφέρουν ένα αποδεικτικό της ταυτότητάς τους έγγραφο, όπως διαβατήριο ή δίπλωμα οδήγησης | Υπό αναθεώρηση[32] πιστοποίησης. Τα PKI Overheid πιστοποιητικά[33] αποτελούν αναγνωρισμένα πιστοποιητικά τα οποία μπορούν να χρησιμοποιηθούν για εφαρμογές ηλεκτρονικής διακυβέρνησης. Στην παρούσα φάση είναι επιχειρησιακοί τέσσερεις (ιδιωτικοί) PKI Overheid πάροχοι πιστοποιητικών |
| | Πιστοποιητικά PKI Overheid[34] τα οποία αποτελούν έμπιστη υποδομή για τους CSPs, η οποία ικανοποιεί αρκετές | Χωρίς περιορισμούς | Προαιρετικό | Επιχειρησιακή Λειτουργία |

[31] Βλ. https://www.luxtrust.lu/?setLocale=EN

[32] Τα σχέδια το Ολλανδικό δελτίο eID καθυστέρησαν όταν κατά τη διάρκεια του διαγωνισμού για μία λύση eID ολοκληρώθηκε επιτυχώς πριν από την εκδίκαση μίας σχετικής υπόθεσης σε ένα Ολλανδικό δικαστήριο, κάτι το οποίο σήμαινε ότι ο διαγωνισμός θα έπρεπε να ξεκινήσει από την αρχή με νέους όρους. Από τότε έχουνε ξεκινήσει εκ νέου οι συζητήσεις σχετικά με τα οφέλη μίας λύσης ηλεκτρονικών ταυτοτήτων, και ειδικότερα σχετικά με το κατά πόσο μία εκτεταμένη και περισσότερο συστηματική χρήση του ήδη υπάρχοντος DigiD-scheme δεν αποτελεί ίσως μία πιο προτιμητέα επιλογή.

[33] Βλ. http://www.quovadisglobal.nl/en-GB/Beheer/Documenten.aspx

[34] http://www.pkioverheid.nl

| | | | | |
|---|---|---|---|---|
| | απαιτήσεις ποιότητας | | | |
| **Ουγγαρία** | Εθνικό δελτίο eID (HUNEID). Σημειώνεται το HUNEID αποτελεί πρότυπο για έξυπνες κάρτες και μπορεί να έχει οποιασδήποτε μορφής υλοποίηση (εθνικά δελτία ID, κάρτα υγείας, κάρτα επαγγελματιών υγείας, κ.τ.λ.) | Φυσικά πρόσωπα τα οποία είναι εγγεγραμμένα στην Ουγγαρία | Εξαρτάται από την υλοποίηση | Στάδιο σχεδιασμού |
| **Πολωνία** | Εθνικό δελτίο eID (pl.ID) σχεδιάζεται χωρίς να έχει ακόμα αναπτυχθεί | Πολωνοί πολίτες πάνω από την ηλικία των 18, ή πάνω από την ηλικία των 15 εάν εργάζονται ή είναι νομικά ανεξάρτητοι | Υποχρεωτικό | Βρίσκεται στο στάδιο του σχεδιασμού. Το 2011 εκτιμάται πως θα τεθεί σε επιχειρησιακή λειτουργία |
| **Πορτογαλία** | Εθνικό δελτίο eID (Cartão do Cidadão) | Πορτογάλοι πολίτες πάνω από την ηλικία των 6[35] | Υποχρεωτικό | Επιχειρησιακή λειτουργία από το 2007. |
| **Ρουμανία** | Εθνικό δελτίο eID | Ρουμάνοι πολίτες πάνω από την ηλικία των 15 | Υποχρεωτικό | Βρίσκεται στο στάδιο του σχεδιασμού, ενώ αναμένεται ότι θα αναπτυχθεί το 2011 (η αρχική ημερομηνία ήταν για το 2009). |
| **Σλοβακία** | Εθνικό δελτίο eID | Σλοβάκοι πολίτες πάνω από την ηλικία των 15 | Προαιρετικό (οι πολίτες θα επιτρέπεται να επιλέξουν ανάμεσα σε ένα μη ηλεκτρονικό δελτίο ID | Βρίσκεται στο στάδιο του σχεδιασμού, ενώ αναμένεται να τεθεί σε επιχειρησιακή λειτουργία μέσα σε χρονικό διάστημα δύο χρόνων, το οποίο εκτιμάται περίπου για το 2012 |
| **Σλοβενία** | Εθνικό δελτίο eID | Σλοβένοι πολίτες πάνω από την ηλικία των 15 | Υποχρεωτικό | Στάδιο σχεδιασμού. Το έργο παραμένει σε αυτό το στάδιο από το 2008. |

[35] Επίσης καλύπτονται και Βραζιλιάνοι πολίτες λόγω της συνθήκης του Porto Seguro

| | | | | |
|---|---|---|---|---|
| **Σουηδία** | Ηλεκτρονικό δελτίο eID | Το εθνικό Σουηδικό δελτίο ταυτότητας μπορεί αποκτηθεί από οποιονδήποτε έχει δικαίωμα να εκδώσει διαβατήριο | Προαιρετικό | Σε επιχειρησιακή λειτουργία από τον Αύγουστο του 2009. Εκδίδεται από τις τοπικές αστυνομικές αρχές |
| **Τουρκία** | Εθνικό δελτίο eID | Τούρκοι πολίτες | Δεν προσδιορίζεται | Σε επιχειρησιακή λειτουργία από το 2007 |
| **Τσεχία** | Εθνικό δελτίο eID | Τσέχοι πολίτες | Προαιρετικό – θα υπάρξουν τόσο κάρτες με ηλεκτρονική λειτουργικότητα, όσο και άλλες χωρίς τέτοια. Ο πολίτης θα μπορεί να αποφασίσει το ποια από τις 2 επιθυμεί να εκδοθεί γι' αυτόν | Φάση σχεδιασμού. Εκτιμάται ότι θα γίνει επιχειρησιακά λειτουργικό από το 2012. |
| **Φινλανδία** | Εθνικά δελτία eID (FINEID) | Φιλανδοί πολίτες και αλλοεθνείς οι οποίοι είναι καταγεγραμμένοι στην Φινλανδία | Προαιρετικό | Σε Επιχειρησιακή λειτουργία από το 1999, με διαφορετική τότε μορφή. Η Φινλανδία είναι η πρώτη χώρα στην Ευρώπη η οποία χρησιμοποίησε δελτία eID. |

**Πίνακας 3: Ηλεκτρονικά δελτία ταυτοποίησης στα Ευρωπαϊκά Κράτη**

Έτσι συνδέοντας τους δύο παραπάνω πίνακες (αυτόν με τα έντυπα δελτία ταυτότητας χωρίς ηλεκτρονική λειτουργικότητα και αυτόν για τις ηλεκτρονικές ταυτότητες) μεταξύ τους, η κατάσταση ως προς την πολιτική των διαφόρων χωρών στο θέμα των δελτίων ταυτότητας είναι η εξής:

| Χώρα | Απλό Έντυπο ID | Υποχρεωτικό | Κατάσταση | eID | Κατάσταση | Υποχρεωτικό |
|---|---|---|---|---|---|---|
| **Αυστρία** | ΟΧΙ | | Άλλο διακριτικό ταυτοποίησης | ΝΑΙ | Επιχειρησιακή Λειτουργία από το 2003 | ΟΧΙ |
| **Βέλγιο** | ΝΑΙ | ΝΑΙ | Αντικαθίσταται από το 2008 με eID | ΝΑΙ | Επιχειρησιακή Λειτουργία από το 2008 | ΝΑΙ |
| **Βουλγαρία** | ΝΑΙ | ΝΑΙ | Επιχειρησιακή Λειτουργία | ΟΧΙ | ---------- | ------ |
| **Γαλλία** | ΝΑΙ | ΟΧΙ | Επιχειρησιακή Λειτουργία | ΟΧΙ | Υπό ανάπτυξη | ------ |
| **Γερμανία** | ΝΑΙ | ΝΑΙ | Αντικαθίσταται από το 2010 με eID | ΝΑΙ | Επιχειρησιακή Λειτουργία από 1/11/2010 | ΝΑΙ |
| **Δανία** | ΟΧΙ | | Παραδοσιακά δεν διαθέτει δελτίο ID | ΟΧΙ | ------ | ------ |
| **Ελλάδα** | ΝΑΙ | ΝΑΙ | Επιχειρησιακή Λειτουργία | ΟΧΙ | Σχεδιάζεται από το 2010 | ------ |
| **Εσθονία** | ΟΧΙ | | Άλλο διακριτικό ταυτοποίησης | ΝΑΙ | Επιχειρησιακή Λειτουργία | ΝΑΙ |
| **Ηνωμένο Βασίλειο** | ΝΑΙ | ΟΧΙ | Επιχειρησιακή Λειτουργία | ΟΧΙ | Σχεδιάζεται για εισαγωγή από το 2012 | ΟΧΙ |
| **Ιρλανδία** | ΟΧΙ | | | ΟΧΙ | Σχεδιάζεται για εισαγωγή το 2011 | ------ |
| **Ισλανδία** | ΝΑΙ | ΝΑΙ | Επιχειρησιακή Λειτουργία | ΝΑΙ | Επιχειρησιακή Λειτουργία από το 2007 | ΟΧΙ |
| **Ισπανία** | ΝΑΙ | ΝΑΙ | Αντικαθίσταται από το 2006 με eID | ΝΑΙ | Επιχειρησιακή Λειτουργία από το 2006 | ΝΑΙ |
| **Ιταλία** | ΝΑΙ | ΟΧΙ | Αντικαθίσταται από το 2007 με eID | ΝΑΙ | Επιχειρησιακή Λειτουργία από το 2007 | ΟΧΙ |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Κροατία** | ΝΑΙ | ΝΑΙ | Αντικαθίσταται από το 2009 με eID | ΝΑΙ | Επιχειρησιακή Λειτουργία από το 2009 | ΝΑΙ |
| **Κύπρος** | ΝΑΙ | ΝΑΙ | Επιχειρησιακή Λειτουργία | ΟΧΙ | Σχεδιάζεται από το 2008 | ------ |
| **Λετονία** | | | | ΟΧΙ | Σχεδιάζεται από το 2008 | ΝΑΙ |
| **Λιθουανία** | ΝΑΙ | ΝΑΙ | Αντικαθίσταται από το 2009 με eID | ΝΑΙ | Επιχειρησιακή Λειτουργία από 1/1/2009 | ΝΑΙ |
| **Λιχτενστάιν** | ΝΑΙ | ΟΧΙ | Επιχειρησιακή Λειτουργία | ΝΑΙ | Επιχειρησιακή Λειτουργία από 23/6/2009 | ΟΧΙ |
| **Λουξεμβούργο** | ΝΑΙ | ΝΑΙ | Επιχειρησιακή Λειτουργία | ΟΧΙ | Σχεδιάζεται για εισαγωγή από το 2011 | ------ |
| **Μάλτα** | ΝΑΙ | ΝΑΙ | Επιχειρησιακή Λειτουργία | ΟΧΙ | Σχεδιάζεται για εισαγωγή από 09/2011 | ΝΑΙ |
| **Νορβηγία** | | | | ΟΧΙ | Σχεδιάζεται για εισαγωγή το 2011 | ΟΧΙ |
| **Ολλανδία** | ΝΑΙ | ΟΧΙ | Επιχειρησιακή Λειτουργία | ΟΧΙ | Φάση συζητήσεων | ΟΧΙ |
| **Ουγγαρία** | ΝΑΙ | ΟΧΙ | Επιχειρησιακή Λειτουργία | ΟΧΙ | ---------- | ------ |
| **Πολωνία** | ΝΑΙ | ΝΑΙ | Επιχειρησιακή Λειτουργία | ΟΧΙ | Σχεδιάζεται για εισαγωγή το 2011 | ------ |
| **Πορτογαλία** | ΝΑΙ | ΝΑΙ | Αντικαθίσταται από το 2007 με eID | ΝΑΙ | Επιχειρησιακή Λειτουργία από το 2007 | ΝΑΙ |
| **Ρουμανία** | ΝΑΙ | ΝΑΙ | Επιχειρησιακή Λειτουργία | ΟΧΙ | Σχεδιάζεται για εισαγωγή το 2011 | ΝΑΙ |
| **Σλοβακία** | ΝΑΙ | ΝΑΙ | Επιχειρησιακή Λειτουργία | ΟΧΙ | Σχεδιάζεται για εισαγωγή το 2012 | ΟΧΙ |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Σλοβενία** | ΝΑΙ | ΌΧΙ | Επιχειρησιακή Λειτουργία | ΌΧΙ | Σχεδιάζεται από το 2008 | ΝΑΙ |
| **Σουηδία** | | | | ΝΑΙ | Επιχειρησιακή Λειτουργία από τον 08/2009 | ΌΧΙ |
| **Τουρκία** | ΝΑΙ | ΝΑΙ | Αντικαθίσταται από το 2007 με eID | ΝΑΙ | Επιχειρησιακή Λειτουργία από το 2007 | |
| **Τσεχία** | ΝΑΙ | ΝΑΙ | Επιχειρησιακή Λειτουργία | ΌΧΙ | Σχεδιάζεται για εισαγωγή από 1/1/2012 | ΝΑΙ |
| **Φινλανδία** | ΌΧΙ | | Άλλο διακριτικό ταυτοποίησης | ΝΑΙ | Επιχειρησιακή Λειτουργία από το 1999 | ΌΧΙ |

**Πίνακας 4: Συγκριτική παρουσίαση έντυπων και ηλεκτρονικών δελτίων eID στα Ευρωπαϊκά Κράτη**

Με βάση αυτό τον πίνακα, εξάγονται τα ακόλουθα συμπεράσματα:

- Από τις 32 χώρες, οι 28 εκδίδουν δελτία ταυτότητας (87,5%), συμπεριλαμβανομένων και των 5 χωρών οι οποίες εκδίδουν δελτία eID μέσω ιδιωτικών CSPs κατόπιν προηγηθείσας εξουσιοδότησης του δημόσιου τομέα των χωρών τους, (Αυστρία, Ισλανδία, Λιχτενστάιν, Ολλανδία και Σουηδία). Από αυτές τις 28:
    - 3 χώρες (Βουλγαρία, Ουγγαρία και Ολλανδία) ενώ χρησιμοποιούν έντυπα δελτία ID, δεν έχουν συγκεκριμένα σχέδια για ανάπτυξη εθνικών δελτίων eID. Στην περίπτωση μάλιστα της Ολλανδίας υπάρχουν σχέδια για ένα δελτίο eID (με την ονομασία eNIK) τα οποία βρισκόταν σε προχωρημένο επίπεδο, αλλά αναθεωρούνται συνεχώς καθυστερώντας συστηματικά την υλοποίηση του έργου[36].
    - 11 χώρες ενώ χρησιμοποιούν έντυπα δελτία ID, έχουνε άλλες λιγότερο και άλλες περισσότερο άμεσα σχέδια για την υλοποίηση δελτίων eID στο μέλλον: Γαλλία, Ελλάδα, Ηνωμένο Βασίλειο, Κύπρος, Λουξεμβούργο, Μάλτα, Πολωνία, Ρουμανία, Σλοβακία, Σλοβενία και Τσεχία .

[36] Για ένα διάστημα αυτό συνέβαινε προκειμένου να ανευρεθούν ενδιαφερόμενοι ιδιώτες προκειμένου να συμμετάσχουν στο έργο της έκδοσης των νέων Ολλανδικών ταυτοτήτων. Συνολικά πάντως η μη υλοποίηση του έργου, φαίνεται πως συστηματικά τρενάρεται εξ' αιτίας έλλειψης ανάλογης πολιτικής βούλησης.

- 15 χώρες έχουνε αναπτύξει δελτία eID, οι οποίες τμηματοποιούνται περαιτέρω στο γκρουπ των πέντε χωρών οι οποίες εκδίδουν eID σε συνδυασμό με ιδιωτικούς φορείς κατόπιν σχετικής κρατικής εξουσιοδότησης (Αυστρία, Ισλανδία, Λιχτενστάιν, Ολλανδία και Σουηδία) και σε αυτό των το γκρουπ των υπολοίπων 10 οι οποίες εκδίδουν τις αντίστοιχες κάρτες μέσω δημόσιων φορέων (Βέλγιο, Γερμανία, Εσθονία, Ισπανία, Ιταλία, Κροατία, Λιθουανία, Πορτογαλία, Τουρκία και Φιλανδία).

- Υπάρχουν ακόμη 4 χώρες οι οποίες δεν εκδίδουν δελτία ταυτότητας: Δανία, Ιρλανδία, Λετονία και Νορβηγία. Όπως σημειώθηκε παραπάνω ωστόσο, σχεδιάζουν να εκδώσουν δελτία eID σε κάποια μορφή, όλες εκτός από τη Δανία. Στη Λετονία, εκτιμάται ότι θα υιοθετήσουν τον τρόπο έκδοσης εξ' ολοκλήρου μέσω του κράτους, ενώ στην Νορβηγία και την Ιρλανδία οι έξυπνες κάρτες οι οποίες εκδίδονται από τον ιδιωτικό τομέα μετά από σχετική κρατική εξουσιοδότηση θα είναι το μοντέλο που θα ισχύσει. Η Δανία παραδοσιακά επιλέγει ένα συνδυασμό δελτίου κοινωνικής ασφάλισης (sygesikringbevis), διπλωμάτων οδήγησης και διαβατηρίων ή καρτών τραπέζης, χωρίς να διαθέτει κάποιο είδους δελτίου ταυτοποίησης αποκλειστικά και μόνο για τη χρήση αυτή. Σε επίπεδο ηλεκτρονικής λειτουργικότητας η λειτουργία αυθεντικοποίησης παρέχεται από την λύση OCES[37].

Από όλα αυτά είναι ξεκάθαρο ότι τα δελτία ταυτότητας αποτελούν μία κυρίαρχη λύση ταυτοποίησης στις υπό μελέτη χώρες, με παρουσία στο 87,5% των χωρών, και με μόνη τη Δανία να μην εξετάζει το θέμα της εισαγωγής οποιασδήποτε αντίστοιχης λύσης στο εγγύς μέλλον. Γίνεται ξεκάθαρο ότι, αν και δεν συμπεριλαμβάνεται σε όλα τα κράτη μέλη, τα δελτία eID θα γίνουν ολοένα και πιο κοινά τα επόμενα χρόνια, εξ' αιτίας της ευκολία την οποία προσφέρουν για στα πλαίσια ηλεκτρονικών υπηρεσιών τόσο σε εθνικό όσο και σε διασυνοριακό επίπεδο.

Ενδιαφέρον ακόμη είναι να αναφερθεί ο δυνατός ρόλος που διαδραματίζει ο ιδιωτικός τομέας στην έκδοση δελτίων eID. Ενώ τα έντυπα δελτία ταυτοτήτων εκδιδόταν πάντοτε κατ' αποκλειστικότητα από δημόσιους φορείς, αυτό δεν αποτελεί πλέον παράδειγμα και για την περίπτωση των eIDs. Πλέον σε πέντε από τις χώρες τα eIDs εκδίδονται από ιδιωτικούς φορείς, όπου παράλληλα υπάρχει επίβλεψη και έλεγχος της έκδοσης ταυτοτήτων από το δημόσιο τομέα. Στις χώρες αυτές τίθεται ένα θέμα το οποίο άπτεται του γεγονότος του κατά

[37] Το OCES αναφέρεται σε αναγνωρισμένες ψηφιακές υπογραφές. Πρόκειται για πιστοποιητικά τα οποία διατίθενται σε soft μορφή, όχι δηλαδή σε συγκεκριμένη hardware υποδομή όπως μία κάρτα.

πόσο δελτία ταυτότητας τα οποία εκδίδονται από ιδιωτικούς φορείς, μπορούν να θεωρούνται «εθνικά δελτία ταυτότητας».

Εν τούτοις η παράμετρος αυτή παρακάμπτεται και θεωρείται ότι όλες αυτές οι χώρες όπου εκδίδονται δελτία eID κάτω από τον έλεγχο του δημόσιου τομέα, αποτελούν λύσεις οι οποίες μπορούνε να γίνουν αποδεκτές στην ηλεκτρονική διακυβέρνηση, σε περιπτώσεις όπου υπάρχει η ανάγκη για μεγαλύτερα επίπεδα ασφάλειας.

### 2.1.3 Soft διακριτικά ταυτοποίησης

Τα διακριτικά ταυτοποίησης δεν περιορίζονται όμως μόνο στο να συμπεριλαμβάνονται μέσα σε έξυπνες κάρτες. Άλλα διακριτικά συμπεριλαμβανομένων των πιστοποιητικών PKI σε soft μορφή ή τα οποία αποθηκεύονται σε κάποιο άλλο (όχι απαραίτητα σε κάρτα) υλικό φορέα, όπως κάποιο USB stick είναι επίσης διαθέσιμα σε αρκετές χώρες. Οι λύσεις αυτές προσφέρουν το όφελος της μεγαλύτερης ευελιξίας (δεν απαιτείται η συνεχής παρουσίας card reader ή ακόμη και της ίδιας της κάρτας).

Θα πρέπει να σημειωθεί ότι ο πίνακας περιλαμβάνει μόνο λύσεις οι οποίες έχουνε ήδη αναπτυχθεί στην παρούσα φάση από τα υπό εξέταση κράτη, και όχι λύσεις οι οποίες σχεδιάζονται ή αναθεωρούνται προκειμένου να εισαχθούν για χρήση στο μέλλον (σε αντίθεση με τον ανωτέρω πίνακα των ηλεκτρονικών ταυτοτήτων, όπου συμπεριλαμβανόταν αντίστοιχες λύσεις).

Οι ακόλουθες χώρες αναφέρουν ότι εκδίδουν soft διακριτικά τα οποία χρησιμοποιούνται για ταυτοποίηση και αυθεντικοποίηση:

| Χώρα | Περιγραφή | Ομάδα Χρηστών | Υποχρεωτικό/ Προαιρετικό | Κατάσταση |
|---|---|---|---|---|
| **Αυστρία** | Κάρτα του πολίτη (Bürgerkarte), η οποία είναι ένα πλαίσιο και μπορεί να πάρει διάφορες μορφές διαφορετικές από ότι μία έξυπνη κάρτα | Φυσικά πρόσωπα που είναι καταγεγραμμένα στην Αυστρία | Προαιρετικό | Βρίσκεται σε επιχειρησιακή λειτουργία. Σημειώνεται ότι το σύστημα συνδυάζει πιστοποιητικά υπογραφής με μοναδικά αναγνωριστικά |
| **Βέλγιο** | Soft Αναγνωρισμένα πιστοποιητικά | Φυσικά και νομικά πρόσωπα | Προαιρετικό | Βρίσκεται σε επιχειρησιακή λειτουργία, αλλά σε ένα |

| | | | | |
|---|---|---|---|---|
| | ιδιωτικού τομέα | | | περιορισμένο πλήθος εφαρμογών |
| **Δανία** | Soft πιστοποιητικά υπογραφής OCES | Φυσικά πρόσωπα τα οποία είναι εγγεγραμμένα στη Δανία[38] | Προαιρετικό | Βρίσκεται σε επιχειρησιακή λειτουργία. Σημειώνεται ότι το σύστημα βασίζεται σε πιστοποιητικά υπογραφής σε συνδυασμό με μοναδικά εθνικά αναγνωριστικά-αριθμός ταυτότητας |
| **Εσθονία** | Υπολογιστές τραπεζικών PIN | Πελάτες τραπεζών | Προαιρετικό | Βρίσκεται σε επιχειρησιακή λειτουργία σε ευρύ μάλιστα επίπεδο. Η δημόσια πολιτική που ακολουθείται τάσσεται υπέρ των δελτίων eID για μελλοντική χρήση |
| | Mobile PKI/ Mobile-eID | Πελάτες των σχετικών εταιρειών κινητής τηλεφωνίας | Προαιρετικό | Βρίσκεται σε επιχειρησιακή λειτουργία (ακολουθεί ανάλυση στην υποενότητα για ταυτοποίηση μέσω κινητών που ακολουθεί) |
| **Ηνωμένο Βασίλειο** | Soft πιστοποιητικά υπογραφής από αναγνωρισμένους CSPs | Φυσικά και νομικά πρόσωπα | Προαιρετικό | Βρίσκεται σε επιχειρησιακή λειτουργία. |
| **Ισπανία** | Ο δημόσιος και ιδιωτικός τομέας εκδίδουν αναγνωρισμένα πιστοποιητικά υπογραφής (είτε soft είτε σε έξυπνες κάρτες) | Φυσικά και νομικά πρόσωπα | Προαιρετικό | Βρίσκεται σε επιχειρησιακή λειτουργία. |
| **Λιθουανία** | Ο ιδιωτικός τομέας εκδίδει αναγνωρισμένα πιστοποιητικά υπογραφής (είτε σε έξυπνες κάρτες είτε όχι) και τραπεζικούς υπολογιστές PIN | Φυσικά και νομικά πρόσωπα | Προαιρετικό | Βρίσκεται σε επιχειρησιακή λειτουργία. |
| **Λουξεμβούργο** | Το LuxTrust Signing Stick (USB stick με δύο ψηφιακά | Όλα τα φυσικά και νομικά πρόσωπα | Προαιρετικό | Βρίσκεται σε επιχειρησιακή λειτουργία. |

[38] Πρόσωπα τα οποία κατέχουν έναν Δανέζικο κεντρικό αριθμό ταυτοποίησης

| | | | | |
|---|---|---|---|---|
| | πιστοποιητικά) | | | |
| **Πολωνία** | Ο ιδιωτικός τομέας εκδίδει αναγνωρισμένα πιστοποιητικά υπογραφής (είτε σε έξυπνες κάρτες είτε όχι) | Φυσικά πρόσωπα (τα οποία χρησιμοποιούν το PESEL[39] ή το NIP[40] αριθμό για ταυτοποίηση) | Προαιρετικό | Βρίσκεται σε επιχειρησιακή λειτουργία. |
| **Σλοβακία** | Ο ιδιωτικός τομέας εκδίδει εγκεκριμένα πιστοποιητικά υπογραφής (είτε σε έξυπνες κάρτες είτε σε κάποιο άλλο SSCD[41]) | Φυσικά πρόσωπα | Προαιρετικό | Βρίσκεται σε επιχειρησιακή λειτουργία. |
| **Σλοβενία** | Ο δημόσιος και ιδιωτικός τομέας εκδίδουν αναγνωρισμένα πιστοποιητικά υπογραφής (είτε soft είτε σε έξυπνες κάρτες) | Φυσικά και νομικά πρόσωπα | Προαιρετικό | Βρίσκεται σε επιχειρησιακή λειτουργία. |
| **Σουηδία** | Soft πιστοποιητικά εκδίδονται από αναγνωρισμένους συνεργάτες του ιδιωτικού τομέα (σήμερα κυρίως τράπεζες). Έτοιμη είναι να ξεκινήσει και η έκδοση σε κινητά τηλέφωνα μέσω αντιστοίχων SIM καρτών | Σουηδοί πολίτες καθώς και αλλοδαποί οι οποίοι έχουν εισαχθεί στο μητρώο πολιτών. Χρησιμοποιεί τον προσωπικό αριθμό ταυτότητας για μοναδική ταυτοποίηση | Προαιρετικό | Βρίσκεται σε επιχειρησιακή λειτουργία. |
| **Τουρκία** | Αναγνωρισμένα πιστοποιητικά υπογραφής τα οποία εκδίδονται από | Φυσικά πρόσωπα | Προαιρετικό | Βρίσκεται σε επιχειρησιακή λειτουργία. |

[39] PESEL: (Powszechny Elektroniczny System Ewidencji Ludności), ουσιαστικά πρόκειται για το μοναδικό αριθμό ταυτοποίησης ο οποίος χρησιμοποιείται στην Πολωνία.
[40] NIP: (Numeru Identyfikacji Podatkowej). Ο Αριθμός Φορολογικού Μητρώου.
[41] SSCD: Secure Signature-Creation Device

| | | | | |
|---|---|---|---|---|
| | διαπιστευμένους CSPs | | | |

**Πίνακας 5: Soft χρησιμοποιούμενα διακριτικά ταυτοποίησης**

Ο παραπάνω πίνακας επιτρέπει να εξαχθούν κάποια ενδιαφέροντα συμπεράσματα:

- Σε 13 από τις 32 χώρες (40%) παρατηρήθηκε η χρήση soft διακριτικών ταυτοποίησης. Αυτό αποτελεί ένα ποσοστό μικρότερο από ότι ίσως αναμενόταν, δεδομένου του ότι τέτοιες λύσεις μπορούν να συμπεριλάβουν τη χρήση υπογραφής και χαρακτηρίζονται από την ευκολία χρήσης τους.

- Όλες οι λύσεις είναι καθαρά εθελοντικές ως προς τη χρήση τους. Αυτό το γεγονός δεν προκαλεί ιδιαίτερη έκπληξη, δεδομένου του ότι η χρήση τους απαιτεί κάποιο βαθμό δεξιοτήτων, ή τουλάχιστον την προθυμία να τις χρησιμοποιήσουν, κάτι το οποίο αποτρέπει την υποχρεωτική έκδοσή τους (σε αντίθεση με ένα δελτίο eID, το οποίο είναι κατανοήσιμο και χρήσιμο και σε κάποιο πλαίσιο πέραν του ηλεκτρονικού, στην βάση του κειμένου το οποίο είναι τυπωμένο επί της κάρτας-δελτίου της ταυτότητας).

- Όλες αυτές οι λύσεις προσφέρονται από εταιρείες του ιδιωτικού τομέα, μολονότι σε μία περίπτωση (το Δανέζικο OCES) αυτή προσφέρεται στη βάση μίας συμφωνίας με την κυβέρνηση.

- Τέλος σε 9 από τις 13 λύσεις δεν βασίζονται σε στοιχεία όπως η μόνιμη κατοικία στη χώρα, η εγγραφή σε μητρώα ή η εγκατάσταση σε μία ορισμένη χώρα, οπότε εκ τούτου παραμένουν τουλάχιστον στην θεωρία ανοικτές για χρήση από πολίτες άλλων χωρών.

### 2.1.4 Τομεακά/εξειδικευμένων εφαρμογών διακριτικά eIDM

Στα πλαίσια αυτής της ενότητας παρουσιάζονται όλα τα ηλεκτρονικά μέσα ελέγχου ταυτότητας, τα οποία χρησιμοποιούνται για την ταυτοποίηση σε εξειδικευμένες εφαρμογές ή σε συγκεκριμένους τομείς κρατικής δραστηριότητας στο κάθε κράτος.

Ένας σημαντικός αριθμός χωρών αναφέρει την ύπαρξη τέτοιων διακριτικών ως ένα σημαντικό τμήμα των εθνικών πολιτικών τους στο θέμα του eIDM.

Οι ακόλουθες χώρες βρέθηκαν να εκδίδουν τομεακά/εξειδικευμένων εφαρμογών διακριτικά eIDM:

| Χώρα | Περιγραφή | Ομάδα Χρηστών | Προαιρετικό/ Υποχρεωτικό | Κατάσταση |
|---|---|---|---|---|
| **Αυστρία** | Ένα πλήθος από παραλλαγές της κάρτας του πολίτη (Bürgerkarte) συμπεριλαμβανομένης της κάρτας Υγειονομικής ασφάλισης | Φυσικά πρόσωπα που είναι καταχωρημένα στην Αυστρία | Προαιρετικό | Σε επιχειρησιακή λειτουργία. Σημειώνεται ότι το σύστημα βασίζεται σε πιστοποιητικά υπογραφής σε συνδυασμό με μοναδικά αναγνωριστικά |
| **Βέλγιο** | Δελτίο SIS[42] | Φυσικά πρόσωπα υποκείμενα στη Βελγική κοινωνική ασφάλιση | Υποχρεωτικό | Σε επιχειρησιακή λειτουργία. |
| **Γαλλία** | Κάρτα Vitale | Οποιοσδήποτε δικαιούχος κοινωνικής ασφάλισης μεγαλύτερος των 16 | Υποχρεωτικό (αλλά η χρήση του είναι προαιρετική, καθώς έντυπα βασισμένα στο χαρτί είναι ακόμη διαθέσιμες) | Σε επιχειρησιακή λειτουργία. |
| **Γερμανία** | Ηλεκτρονικό Δελτίο Υγείας (elektronische Gesundheitskarte) | Φυσικά πρόσωπα υποκείμενα στη Γερμανική κοινωνική ασφάλιση | Υποχρεωτικό | Πιλοτικό στάδιο |
| **Δανία** | Κάρτα κοινωνικής ασφάλισης (sygesikringbevis) | Φυσικά πρόσωπα υποκείμενα στην Δανέζικη κοινωνική ασφάλιση | Υποχρεωτικό | Σε επιχειρησιακή λειτουργία. |
| **Ιταλία** | Εθνική κάρτα Υπηρεσιών (CNS). Δεν είναι κάρτα[43] | Εξαρτάται από την υλοποίηση | Εξαρτάται από την υλοποίηση | Σε επιχειρησιακή λειτουργία |
| **Κροατία** | CIHI δελτίο ιατρικής ασφάλισης – 'isprava 2' | Φυσικά πρόσωπα υποκείμενα στην Κροατική κοινωνική ασφάλιση | Υποχρεωτικό | Σε επιχειρησιακή λειτουργία |
| **Ουγγαρία** | Ηλεκτρονική κάρτα Υγείας | Δεν έχει προσδιορισθεί | Δεν έχει προσδιορισθεί | Βρίσκεται στο στάδιο του σχεδιασμού |

[42] Κάρτα Κοινωνικής Ασφάλισης

[43] Τα κύρια παραδείγματα του CNS είναι το SISS project ( κάρτα Υγείας της επαρχίας Lombardy, με περισσότερες από 9 εκατομμύρια κάρτες να έχουν εκδοθεί) και το NSC της επαρχίας Friuli Venezia Giulia

| | | | | |
|---|---|---|---|---|
| **Πολωνία** | Ηλεκτρονική κάρτα για υγειονομική ασφάλεια EKUZ | Φυσικά πρόσωπα (ασθενείς) στο τμήμα Silesian Voivodeship του εθνικού ταμείου Υγείας | Υποχρεωτικό | Σε επιχειρησιακή λειτουργία |
| **Ρουμανία** | Εθνική κάρτα Ιατρικής Ασφάλισης (NHI card) | Φυσικά πρόσωπα τα οποία περιλαμβάνονται στο σύστημα κοινωνικής υγείας της Ρουμανίας | Υποχρεωτικό | Στάδιο σχεδιασμού. |
| **Σλοβενία** | Δελτία Υγειονομικής Ασφάλισης | Όλος ο πληθυσμός | Υποχρεωτικό | Σε επιχειρησιακή λειτουργία |

**Πίνακας 6: Τομεακά Διακριτικά & Διακριτικά Εξειδικευμένων Εφαρμογών για τους σκοπούς της ταυτοποίησης**

Από τις 11 λύσεις που αναφέρθηκαν, μόλις 7 από αυτές έχουνε ήδη αναπτυχθεί στην παρούσα φάση, δηλαδή ένα ποσοστό 22% επί του συνόλου των 32 χωρών. Αυτό το περιορισμένο ποσοστό είναι πιθανόν ενδεικτικό του γεγονότος ότι τα τομεακά/ εξειδικευμένων εφαρμογών διακριτικά δεν θεωρούνται γενικά βασικό μέρος μίας κυβερνητικής eIDM στρατηγικής.

Η κύρια περίπτωση σχετίζεται με την κοινωνική ασφάλιση και τις λύσεις eHealth, οι οποίες συναντώνται σε 6 από τις 7 αναπτυχθείσες λύσεις, με εναπομείνασα περίπτωση να παραμένει αυτή της Αυστριακής Κάρτας του Πολίτη (Bürgerkarte) η οποία έχει ένα πλήθος παραλλαγών συμπεριλαμβανομένης και μίας κάρτας ασφάλειας υγείας.

### 2.1.5 Αναγνωριστικά eID εξειδικευμένων ομάδων χρηστών

Σε κάθε χώρα όμως, δεν υφίστανται μόνο συστήματα τα οποία να χρησιμοποιούνται σε καθολικό επίπεδο. Έτσι επιμέρους υποσυστήματα σε κάθε χώρα, ενδέχεται να εξυπηρετούν τους σκοπούς της ταυτοποίησης των κατά περίπτωση χρηστών, το οποίο ως υποσύνολο μπορεί να μην ταυτίζεται με την έννοια του γενικού πληθυσμού. Αντίθετα πρόκειται για εξειδικευμένες ομάδες χρηστών, όπως δημόσιοι υπάλληλοι, αλλοδαποί κ.τ.λ..

Σε κάθε περίπτωση τα κράτη αναφέρουν λύσεις ή μία σειρά από λύσεις οι οποίες ικανοποιούν τον προαναφερόμενο σκοπό και αποτελούν μέρος της eIDM πολιτικής τους.

Στον πίνακα που ακολουθεί καταγράφονται οι χώρες στις οποίες υφίστανται τέτοιου είδους διακριτικά.

| Χώρα | Περιγραφή | Ομάδα Χρηστών | Προαιρετικό/ Υποχρεωτικό | Κατάσταση |
|---|---|---|---|---|
| **Αυστρία** | Κάρτα δημοσίων υπαλλήλων (η οποία αποτελεί μία μορφή της κάρτας του πολίτη (Bürgerkarte) | Δημόσιοι Υπάλληλοι | Προαιρετικό | Σε επιχειρησιακή λειτουργία. Σημειώνεται ότι το σύστημα βασίζεται σε πιστοποιητικά υπογραφής σε συνδυασμό με μοναδικούς προσδιοριστές ταυτοποίησης |
| **Βέλγιο** | Δελτίο eID αλλοδαπών | Αλλοεθνείς οι οποίοι δεν είναι επιλέξιμοι για ένα εθνικό δελτίο eID | Υποχρεωτικό | Σε επιχειρησιακή λειτουργία (βρισκόταν σε πιλοτικό στάδιο) |
| | Παιδικό-ID (δελτίο eID) | Παιδιά κάτω των 12 | Προαιρετικό | Σε επιχειρησιακή λειτουργία (βρισκόταν σε πιλοτικό στάδιο) |
| **Γαλλία** | Κάρτες επαγγελματιών Υγειονομικής Περίθαλψης CPS[44] | Επαγγελματίες Υγειονομικής Περίθαλψης | Υποχρεωτικό (ακόμη είναι διαθέσιμα τα προηγούμενης γενιάς έντυπα δελτία) | Σε επιχειρησιακή λειτουργία. (Μία νέα γενιά από δελτία CPS πρόκειται να παρουσιασθεί στο εγγύς μέλλον)[45] |
| **Γερμανία** | Κάρτες Επαγγελματιών Υγειονομικής Περίθαλψης | Επαγγελματίες Υγειονομικής Περίθαλψης | Δεν έχει προσδιορισθεί ακόμα | Στάδιο σχεδιασμού |
| **Ελλάδα** | Έξυπνη κάρτα του Σύζευξης[46] | Δημόσιοι Υπάλληλοι | Υποχρεωτικό | Στάδιο εφαρμογής |
| | Έξυπνη κάρτα του Police On Line[47] | Αστυνομικοί | Υποχρεωτικό | Σε επιχειρησιακή λειτουργία |
| **Ισπανία** | eID αλλοδαπών ("NIE electronico" ή NIE-e") | Αλλοδαποί που τους έχει επιτραπεί να διαμένουν νόμιμα στην Ισπανία | Προαιρετικό | Στάδιο σχεδιασμού |
| **Ιταλία** | Δελτίο eID των δημοσίων υπαλλήλων ή | Δημόσιοι Υπάλληλοι | Υποχρεωτικό | Σε επιχειρησιακή λειτουργία |

[44] CPS: Carte professionelle de la Santé

[45] Θα προστεθεί μία ασύρματη δυνατότητα ανάγνωσης και τελικά έπειτα από τις απαραίτητες αλλαγές, θα είναι σύμφωνη με τις απαιτήσεις για την Ευρωπαϊκή κάρτα για τους επαγγελματίες υγείας όπως προβλέπεται στην Οδηγία EC 2005/46 της 7ης Δεκεμβρίου 2005 σχετικά με την αναγνώριση των επαγγελματικών κατηγοριοποιήσεων.

[46] Το Εθνικό Δίκτυο Δημόσιας Διοίκησης. Βλ. http://www.syzefxis.gov.gr

[47] Police On Line: Το Ολοκληρωμένο Πληροφοριακό Σύστημα της Ελληνικής Αστυνομίας. Βλ. http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1871&Itemid=400&langEN

| | | | | |
|---|---|---|---|---|
| | αλλιώς "AT-E model" [48] | | | |
| | Ηλεκτρονική Άδεια διαμονής PSE[49] | Πολίτες κρατών μελών μη μέλη της ΕΕ, που τους έχει επιτραπεί να διαμένουν στην Ιταλία | Υποχρεωτικό | Σε επιχειρησιακή λειτουργία |
| **Λιθουανία** | Δελτία eID των δημοσίων Υπαλλήλων | Δημόσιοι Υπάλληλοι | Προαιρετικό | Σε επιχειρησιακή λειτουργία |
| **Ολλανδία** | UZI-card[50] | Επαγγελματίες υπηρεσιών υγειονομικής περίθαλψης | Προαιρετικό | Σε επιχειρησιακή λειτουργία |
| **Ουγγαρία** | Μαθητική κάρτα | Μαθητές σε δημόσια σχολεία (συμπεριλαμβανομένης και της ανώτατης εκπαίδευσης) | Υποχρεωτικό | Σε επιχειρησιακή λειτουργία |
| | Κάρτες Επαγγελματιών Υγειονομικής Περίθαλψης | Επαγγελματίες Υγειονομικής Περίθαλψης | Δεν έχει προσδιορισθεί ακόμα | Βρίσκεται σε Πιλοτικό στάδιο |
| **Πορτογαλία** | Soft αναγνωρισμένα πιστοποιητικά υπογραφής για εξειδικευμένα επαγγέλματα | Δικηγόροι και συμβολαιογράφοι | Προαιρετικό | Σε επιχειρησιακή λειτουργία |
| **Σλοβενία** | PKI πιστοποιητικά τα οποία εκδίδονται από το Υπουργείο Δημόσιας Διοίκησης | Εξαρτάται από τον τύπο του πιστοποιητικού, μία κατηγορία είναι οι δημόσιοι υπάλληλοι | Προαιρετικό | Σε επιχειρησιακή λειτουργία |
| | Επαγγελματίες Υγειονομικής Περίθαλψης | Όλοι οι επαγγελματίες Υγειονομικής Περίθαλψης | Υποχρεωτικό | Σε επιχειρησιακή λειτουργία |
| | PKI πιστοποιητικά για συγκεκριμένες | Εξαρτάται από τον τύπο του πιστοποιητικού: | Προαιρετικό | Σε επιχειρησιακή λειτουργία |

[48] Αλλιώς "Carta Multiservizi del Dipendente" δηλαδή η Multiservice (Public) Employee Card
[49] PSE: Permesso di Soggiorno Elettronico
[50] Βλ. http://www.uziregister.nl/Images/UZI-folder_per_pagina_engels_tcm19-12644.pdf

| | | | | |
|---|---|---|---|---|
| | επαγγελματικές ομάδες | δικηγόροι, συμβολαιογράφοι | | |
| **Τουρκία** | Soft πιστοποιητικά αυθεντικοποίησης για δικηγόρους | Δικηγόροι | Προαιρετικό | Σε επιχειρησιακή λειτουργία |
| **Φινλανδία** | Κάρτες επαγγελματιών Υγειονομικής περίθαλψης (Valvira) | Επαγγελματίες Υγειονομικής Περίθαλψης | Υποχρεωτικό | Πιλοτικό στάδιο |

**Πίνακας 7: Αναγνωριστικά eID εξειδικευμένων ομάδων χρηστών**

Σε ένα σύνολο 14 από τις 32 χώρες (44%) παρατηρείται η ύπαρξη εξειδικευμένων διακριτικών eID για συγκεκριμένες ομάδες χρηστών, η πλειονότητα από τις οποίες (αναφέρθηκε σε 6 χώρες) σχετίζονται με τους επαγγελματίες Υγειονομικής Περίθαλψης. Ωστόσο μόνο 3 από αυτές τις χώρες βρίσκονται στην παρούσα φάση στη διαδικασία έκδοσης αυτών των καρτών (Γαλλία, Ολλανδία και Σλοβενία), με τις άλλες τρείς να παραμένουν ακόμα και τώρα σε πιλοτικό στάδιο. Άλλες σημαντικές περιπτώσεις αποτελούν οι κάρτες για τους δημόσιους υπαλλήλους (Αυστρία, Ιταλία, Λιθουανία και Σλοβενία), τα δελτία eID για αλλοδαπούς (Βέλγιο, Ιταλία και Ισπανία) και τέλος οι κάρτες για χρήση από δικηγόρους (Πορτογαλία, Ισπανία και Τουρκία).

Το σχετικά χαμηλό ποσοστό χωρών οι οποίες χρησιμοποιούν τέτοια διακριτικά ταυτοποίησης για συγκεκριμένες ομάδες χρηστών οφείλεται πιθανότατα στο γεγονός ότι η χρήση τέτοιου είδους λύσεων, που περιορίζονται σε συγκεκριμένες ομάδες και διαδικασίες, αντιβαίνει της λογικής των ενιαία εφαρμοζόμενων λύσεων σε επίπεδο κράτους κατ' αρχήν και σε ένα διασυνοριακό μοντέλο στη συνέχεια.

### 2.1.6 Συμπεράσματα σε σχέση με τα διακριτικά ταυτοποίησης

Τα δελτία ταυτότητας αποτελούν το κύριο διακριτικό ταυτοποίησης το οποίο προωθείται στο σύνολο σχεδόν των υπό μελέτη χωρών. Τα συστήματα PKI αποτελούν μία επιλογή για τα δελτία eID των οποίων η δημοφιλία φαίνεται να αυξάνεται συνεχώς. Δεν συνιστούν όμως τη μόνη λύση, καθώς διακριτικά ταυτοποίησης τα οποία δεν έχουνε τη μορφή κάρτας (κατά κύριο λόγο πιστοποιητικά PKI) αποτελούν μία συχνή επίσης επιλογή.

Ένας ακόμη σημαντικός παράγοντας, είναι οι συνέργειες δημόσιου-ιδιωτικού τομέα οι οποίες παρατηρούνται και είναι ένας σημαντικός παράγοντας στις περισσότερες υλοποιήσεις αυθεντικοποίησης οι οποίες

βασίζονται σε PKI, όπως μπορεί εύκολα να γίνει αντιληπτό από το μεγάλο πλήθος των λύσεων αυθεντικοποίησης τα οποία εκδίδονται από ιδιωτικούς CSPs.

Σε κάποιες ακόμα χώρες, παρατηρήθηκε ότι χρησιμοποιούνται λύσεις για συγκεκριμένους τομείς ή για εξειδικευμένες ομάδες χρηστών όπως ηλεκτρονικές κάρτες κοινωνικής ασφάλισης ή PKI πιστοποιητικά που εκδίδονται για εξειδικευμένες ομάδες χρηστών όπως δημόσιοι υπάλληλοι, συμβολαιογράφοι ή δικηγόροι.

Ωστόσο η υιοθέτηση τέτοιων λύσεων φαίνεται να είναι περιορισμένη, τουλάχιστον προς το παρόν.

## 2.2 Χρήση Βιομετρίας για ταυτοποίηση

Η χρήση βιομετρικών στοιχείων[51] στα διαβατήρια και τα ταξιδιωτικά έγγραφα λήφθηκε υπ' όψη από την Ευρωπαϊκή Ένωση μετά την επίθεση της 11ης Σεπτεμβρίου 2001, οπότε και τέθηκε στα Ευρωπαϊκά Κράτη το θέμα της βελτίωσης των επιπέδων ασφάλειας των δεδομένων που χρησιμοποιούν στα ταξιδιωτικά τους έγγραφα[14]. Έτσι εκδόθηκε σχετική Σύσταση από το Ευρωπαϊκό Συμβούλιο[52] [15] ρυθμιστικά προς το ανωτέρω θέμα.

Η Ευρωπαϊκή Επιτροπή με την απόφαση που εξέδωσε την 28η Ιουνίου 2006[16] καθόρισε τις τεχνικές προδιαγραφές σχετικά με τα πρότυπα ασφάλειας και των βιομετρικών δεδομένων που ενσωματώνονται στα διαβατήρια και τα ταξιδιωτικά έγγραφα που εκδίδονται από τις Ευρωπαϊκές χώρες, υλοποιώντας το σχετικό Κανονισμό[15].

Στο παράρτημα της ανωτέρω απόφασης ορίζονται τα εξής στοιχεία:

1) Κύριο βιομετρικό δεδομένο ορίζεται το πρόσωπο (η εικόνα του προσώπου).

2) Δευτερεύον βιομετρικό δεδομένο ορίζονται τα δακτυλικά αποτυπώματα

3) Το μέσο αποθήκευσης (για τα βιομετρικά δεδομένα ορίζεται ότι αυτά θα πρέπει να αποθηκεύονται σε «ανεπαφικό πλινθίο»[53]).

4) Θέματα ασφάλειας δεδομένων και ακεραιότητας των δεδομένων

5) Αξιολόγηση της Συμμόρφωσης ως προς τον εκδοθέν κανονισμό [15]

[51] Τα βιομετρικά χαρακτηριστικά είναι μοναδικά, μετρήσιμα, φυσικά γνωρίσματα που χρησιμοποιούνται προκειμένου αναγνωριστεί η ταυτότητα ενός ατόμου. Τέτοια γνωρίσματα είναι μεταξύ των άλλων το πρόσωπο και τα δακτυλικά αποτυπώματα.

[52] Με τον κανονισμό αυτό εναρμονίστηκαν τα Ευρωπαϊκά Ταξιδιωτικά Έγγραφα με τις απαιτήσεις του εντύπου του ICAO 9303

[53] Ο όρος αναφέρεται στην αντίστοιχη αγγλική ορολογία contactless chip

Στο άρθρο 2 της Σύστασης αναφέρεται ότι:

> *"Τα διαβατήρια και τα ταξιδιωτικά έγγραφα[54] περιλαμβάνουν μέσο αποθήκευσης το οποίο περιέχει εικόνα του προσώπου. Τα κράτη μέλη προβλέπουν επίσης την ενσωμάτωση δακτυλικών αποτυπωμάτων υπό μορφή που εξασφαλίζει τη διαλειτουργικότητα. Τα δεδομένα ενσωματώνονται κατά τρόπο ασφαλή και το μέσο αποθήκευσης διαθέτει επαρκή χωρητικότητα και ικανότητα προκειμένου να διασφαλίζεται η ακεραιότητα, η αυθεντικότητα και η εμπιστευτικότητα των δεδομένων".*

Έτσι στον πίνακα που ακολουθεί παρουσιάζεται η κατάσταση που επικρατεί στην Ευρώπη μεταξύ των χωρών οι οποίες έχουνε ήδη εισάγει ή οι οποίες σχεδιάζουν να εισάγουν στη λειτουργικότητα των ηλεκτρονικών ταυτοτήτων τους τη χρήση βιομετρίας, στα πλαίσια εφαρμογής της Σύστασης.

Η ταυτοποίηση του ατόμου με τη χρήση των βιομετρικών δεδομένων πραγματοποιείται ως εξής: Η αναγνώριση προσώπου σχετίζεται με τα χαρακτηριστικά γνωρίσματα του προσώπου. Π.χ. τις αποστάσεις μεταξύ των ματιών, μύτης, στόματος και αυτιών. Οι μετρήσεις κωδικοποιούνται ψηφιακά και αυτό μπορεί έπειτα να χρησιμοποιηθεί για λόγους σύγκρισης και επαλήθευσης[17][55]. Πάντως η χρήση της βιομετρίας προκειμένου να ταυτοποιηθούν οι πολίτες αποτελεί μία μέθοδο η οποία δεν φαίνεται να προκρίνεται μεταξύ των διαθέσιμων επιλογών ανάμεσα στα κράτη – μέλη.

| Χώρα | Κατάσταση | Περιγραφή |
|---|---|---|
| **Γαλλία** | Σχεδιάζεται η χρήση τους | Τα μελλοντικά δελτία eID στην παρούσα φάση σχεδιάζονται με τη δυνατότητα να περιέχουν βιομετρικά στοιχεία (εικόνα προσώπου και δύο αποτυπώματα) τα οποία επίσης θα αποθηκεύονται σε μία κεντρική βάση δεδομένων. Σημειώνεται ότι τα αποτυπώματα έχουνε ήδη ληφθεί όταν ο πολίτης αιτούνταν έντυπο δελτίο ID, αλλά τα δεδομένα προς το παρόν δεν επεξεργάζονται περαιτέρω. |
| **Γερμανία** | Χρησιμοποιούνται | Τα νέα δελτία eID τα οποία εκδίδονται στη Γερμανία από την 1/11/2010, περιλαμβάνουν βιομετρικά δεδομένα και πιο συγκεκριμένα την εικόνα του προσώπου του πολίτη το οποίο περιλαμβάνεται υποχρεωτικά και τα δακτυλικά του αποτυπώματα η συμπερίληψη των οποίων είναι θέμα επιλογής του πολίτη. Την αρμοδιότητα για τη διαχείριση και διατήρηση των στοιχείων την έχουν οι κεντρικές Υπηρεσίες έκδοσης ταυτοτήτων της χώρας. |
| **Εσθονία** | Σχεδιάζεται η χρήση τους | Η ένταξη βιομετρικής υποστήριξης σχεδιάζεται για τα δελτία eID επόμενης γενιάς (2011+). Το πότε τα βιομετρικά δεδομένα θα ενσωματωθούν στις Εσθονικές κάρτες του πολίτη δεν έχει ακόμα αποφασισθεί |

[54] Στον όρο ταξιδιωτικά έγγραφα περιλαμβάνονται και οι ηλεκτρονικές ταυτότητες, στο μέτρο που αυτές χρησιμοποιούνται για σκοπούς ταυτοποίησης και επίτευξη της ελεύθερης μετακίνησης των πολιτών εντός και εκτός των συνόρων μίας χώρας.

[55] Βλ. http://www.passport.gov.gr/npc-periexomeno/npc-periexomeno/viometrika-xaraktiristika-diavatiriou.html

| | | |
|---|---|---|
| **Ηνωμένο Βασίλειο** | Σχεδιάζεται η χρήση τους | Το μελλοντικό δελτίο eID σχεδιάζεται να περιέχει την εικόνα του προσώπου του πολίτη και τα δακτυλικά αποτυπώματα του. Τα στοιχεία αυτά διαχειρίζονται από την υπηρεσία Identity & Passport Service του Υπουργείου Εσωτερικών. |
| **Ισπανία** | Χρησιμοποιούνται | Το εθνικό δελτίο eID χρησιμοποιεί περιέχει την εικόνα του προσώπου και τα δακτυλικά αποτυπώματα του ατόμου |
| **Ιταλία** | Χρησιμοποιούνται | Βιομετρικά δεδομένα με τη μορφή δακτυλικών αποτυπωμάτων και εικόνας του προσώπου χρησιμοποιούνται στο δελτίο eID (CIE), ενώ επίσης δακτυλικά αποτυπώματα μπορούν να χρησιμοποιηθούν στην ηλεκτρονική κάρτα διαμονής (PSE) και στην κάρτα των δημοσίων υπαλλήλων (CMD). |
| **Λιθουανία** | Χρησιμοποιούνται | Βιομετρικά δελτία ταυτοποίησης με εικόνα του προσώπου και δακτυλικά αποτυπώματα του πολίτη περιλαμβάνονται από τις 2 Ιανουαρίου 2009 |
| **Πορτογαλία** | Χρησιμοποιούνται | Βιομετρικά δεδομένα: εικόνα προσώπου και δακτυλικά αποτυπώματα περιλαμβάνονται στο νέο δελτίο eID. Τα δεδομένα διατηρούνται από το Υπουργείο Δικαιοσύνης της Πορτογαλίας |
| **Σουηδία** | Χρησιμοποιούνται | Βιομετρικά δελτία ταυτοποίησης με εικόνα του προσώπου και δακτυλικά αποτυπώματα του πολίτη περιλαμβάνονται από τον Αύγουστο του 2009 |
| **Τουρκία** | Σχεδιάζεται η χρήση τους | Τα δακτυλικά αποτυπώματα σχεδιάζεται να περιέχονται σε μία μελλοντική ηλεκτρονική κάρτα υγείας |

**Πίνακας 8: Βιομετρικά Δεδομένα για σκοπούς ταυτοποίησης**

Όπως προκύπτει από τον παραπάνω πίνακα:

- Μόλις 6 από το σύνολο των 32 χωρών της ΕΕ (22%) έχουν εισάγει τη βιομετρία, μέσω της χρήσης δακτυλικών αποτυπωμάτων προκειμένου να ταυτοποιήσουν τους πολίτες των κρατών τους (Γερμανία, Ισπανία , Ιταλία, Λιθουανία, Πορτογαλία και Σουηδία).

- Στις υπόλοιπες τέσσερεις χώρες οι οποίες εμφανίζονται στο πίνακα σχεδιάζεται να εισάγουν τη χρήση βιομετρίας στα συστήματα ταυτοποίησης τα οποία χρησιμοποιούν (Γαλλία, Εσθονία, Τουρκία και Ηνωμένο Βασίλειο).

Για το σύνολο των υπολοίπων χωρών της ΕΕ δεν υπάρχουν αναφορές οι οποίες να υποδηλώνουν ότι οι χώρες αυτές σκοπεύουν να εισάγουν τη βιομετρία προκειμένου να ταυτοποιούν τους πολίτες των κρατών τους ούτως ώστε να χρησιμοποιήσουν υπηρεσίες στα πλαίσια της ηλεκτρονικής διακυβέρνησης.

## 2.3 Η χρήση κινητών τηλεφώνων για ταυτοποίηση πολιτών

Ένας άλλος τρόπος ο οποίος μπορεί να χρησιμοποιηθεί προκειμένου να ταυτοποιηθεί ένα πολίτης, είναι μέσω του κινητού τηλεφώνου που αυτός διαθέτει.

Τα πλεονεκτήματα της μεθόδου είναι προφανή, καθώς με όρους 2011 ο καθένας πλέον διατηρεί μαζί του ένα κινητό τηλέφωνο το οποίο έως τώρα εξυπηρετούσε απλά και μόνο ορισμένες τηλεπικοινωνιακές του ανάγκες. Οπότε θα χαρακτηριζόταν τουλάχιστον «βολικό» για κάποιον να μπορεί αντί να χρειάζεται να μεταφέρει διαφορετικές κάρτες οι οποίες θα απαιτούνται προκειμένου να ταυτοποιηθεί σε κάθε δοθείσα περίπτωση, να μπορεί να πράττει κάτι τέτοιο απλά και μόνο μέσω του κινητού του τηλεφώνου. Για την ακρίβεια μέσω των δυνατοτήτων τις οποίες προσφέρει η κάρτα SIM την οποία τα κινητά τηλέφωνα όλων περιέχουν.

Όπως προκύπτει ορισμένες από τις χώρες υιοθετούν τον τρόπο αυτό ταυτοποίησης ως έγκυρο, κάτω από την διασφάλιση ορισμένων κάθε φορά προϋποθέσεων. Στην ενότητα αυτή περιλαμβάνονται οι χώρες στις οποίες η χρήση κινητού τηλεφώνου προκειμένου να επιτευχθεί η διαχείριση της ταυτοποίησης των πολιτών βρίσκεται στο στάδιο της επιχειρησιακής λειτουργίας ή του σχεδιασμού.

Η μελέτη η οποία πραγματοποιείται πάνω στη χρήση κινητών τηλεφώνων είναι ιδιαίτερης σημασίας, ειδικά αν αναλογιστούμε ότι η χρήση κινητών τηλεφώνων στα πλαίσια συμφωνιών για roaming τείνει να είναι ολοένα και πιο αυξανόμενη και ως εκ τούτου αποτελεί μία υποδομή η οποία συνοδεύει τον πολίτη στις μετακινήσεις του εκτός της χώρας του. Το κινητό θα μπορούσε να χρησιμοποιηθεί ούτως ώστε ο πολίτης να ταυτοποιείται από μία τρίτη χώρα στα πλαίσια της διασυνοριακής χρήσης των ηλεκτρονικών ταυτοτήτων, καθώς εξ' αιτίας της διαλειτουργικότητας των δικτύων κινητής τηλεφωνίας αυτός το φέρει σχεδόν πάντα μαζί του.

| Χώρα | Κατάσταση | Περιγραφή / Κατάσταση |
|---|---|---|
| **Αυστρία** | Χρησιμοποιείται | Από το 4$^{o}$ τρίμηνο του 2009, η ταυτοποίηση που βασίζεται στη χρήση κινητών τηλεφώνων είναι δυνατή σε αρκετές εφαρμογές της ηλεκτρονικής διακυβέρνησης (για παράδειγμα για τη δήλωση φόρου εισοδήματος), κάτι το οποίο καθίσταται εφικτό με τη χρήση αναγνωρισμένων πιστοποιητικών στα οποία ένα τμήμα hardware security (HSM) της κάρτας SIM η οποία διαχειρίζεται από το διαχειριστή λειτουργεί ως ένα SSCD που αποθηκεύει τα κλειδιά κρυπτογραφίας, καθιστώντας τη λύση ως μία εφαρμογή του γενικού |

| | | |
|---|---|---|
| | | πλαισίου της Αυστριακής κάρτας του πολίτη |
| **Εσθονία** | Χρησιμοποιείται | Σύστημα PKI κινητών που ονομάζεται "Mobile ID" εισήχθηκε από τον Μάιο του 2007 από το μεγαλύτερο φορέα εκμετάλλευσης επικοινωνιών κινητής τηλεφωνίας EMT. Αν και η εξάπλωση του Mobile ID δεν πραγματοποιήθηκε γρήγορα, η ικανοποίηση των χρηστών ήταν μεγάλη. Η γενική πολιτική που ακολουθήθηκε ήταν να γίνουν αποδεκτά το δελτίο eID και το Mobile-ID στο ίδιο επίπεδο εμπιστοσύνης. |
| **Λιθουανία** | Χρησιμοποιείται | Δύο κύριοι φορείς εκμετάλλευσης κινητής τηλεφωνίας η "Omnitel" και η "Bite Lietuva" παρέχουν επίσης μία υπηρεσία βασισμένη στη χρήση αναγνωρισμένων ψηφιακών ηλεκτρονικών υπογραφών μέσω κινητής τηλεφωνίας στο κοινό. |
| **Νορβηγία** | Χρησιμοποιείται | Είναι δυνατή η ταυτοποίηση μέσω κινητού τηλεφώνου ως μέρος των συστημάτων Buypass και BankID. |
| **Ολλανδία** | Χρησιμοποιείται | Υποστηρίζεται ως τμήμα του συστήματος ταυτοποίησης DigiID (2$^{ο}$ επίπεδο του εν λόγω συστήματος), χρησιμοποιώντας SMS. Ένας ιδιωτικός πάροχος αυθεντικοποίησης (Diginotar) ανακοινώθηκε ότι θα αρχίσει επίσης να παρέχει ταυτοποίηση μέσω κινητής τηλεφωνίας το οποίο θα ονομάζεται EazyID[56] |
| **Πολωνία** | Χρησιμοποιείται | Στο τέλος του 2008 η εταιρεία MobiTrust[57] ενεργοποίησε υπηρεσίες για αναγνωρισμένες ηλεκτρονικές υπογραφές μέσω κινητών τηλεφώνων. |
| **Σλοβενία** | Χρησιμοποιείται | Υπογραφές μέσω κινητών προσφέρονται από τον φορέα παροχής τηλεπικοινωνιακών υπηρεσιών MOBITEL. Η υπηρεσία παρουσιάσθηκε πρόσφατα και ως εκ τούτου η διάδοσή της παραμένει μικρή. |
| **Τουρκία** | Χρησιμοποιείται | Από τον Μάιο του 2009 δύο υποδομές ηλεκτρονικής υπογραφής μέσω κινητών τηλεφώνων έχουν ολοκληρωθεί και οι χρήστες μπορούν να δημιουργήσουν νομικά δεσμευτικές ηλεκτρονικές υπογραφές χρησιμοποιώντας τις κάρτες SIM τους. |

**Πίνακας 9: Ταυτοποίηση μέσω κινητών τηλεφώνων**

Σε 8 από τα κράτη μέλη της ΕΕ υπάρχουν εφαρμογές οι οποίες υποστηρίζουν την αυθεντικοποίηση των χρηστών μέσω των κινητών τηλεφώνων που αυτοί χρησιμοποιούν. Οι χώρες αυτές είναι η Αυστρία, η Εσθονία, η Λιθουανία, η Νορβηγία, η Ολλανδία, η Πολωνία και η Σλοβενία και η Τουρκία.

Ωστόσο είναι ενδιαφέρον να σημειωθεί ότι μόνο δύο από αυτές, η Ολλανδία και η Νορβηγία παρουσιάζονται ξεκάθαρα ως λύσεις πολυπαραγοντικής αυθεντικοποίησης, καθώς στις υπόλοιπες έξι παρουσιάζονται κατ' αρχήν ως λύσεις οι οποίες χρησιμοποιούνται προκειμένου να υλοποιηθεί η ηλεκτρονική υπογραφή.

[56] http://www.diginotar.nl/Producten/Themas/EazyIDMobile/tabid/1217/Default.aspx
[57] http://www.mobitrust.pl

Στην πρώτη περίπτωση το κινητό τηλέφωνο χρησιμοποιείται απλά για την υποστήριξη της αυθεντικοποίησης δύο παραγόντων, μέσω ενός SMS το οποίο παρέχει ένα περιορισμένης χρονικής ισχύος κωδικό το οποίο επιτρέπει στον τελικό χρήστη να συνδεθεί σε μία εξειδικευμένη υπηρεσία.

Η δεύτερη προσέγγιση όπως είναι για παράδειγμα στην Εσθονία και τη Λιθουανία απαιτεί την ύπαρξη μίας κάρτας SIM η οποία είναι PKI-enabled, γεγονός το οποίο επιτρέπει στην κάρτα SIM να λειτουργεί ως μία γεννήτρια παραγωγής υπογραφών.

Το πλαίσιο των υπηρεσιών στις χώρες αυτές για τις οποίες παρέχεται αυτή η δυνατότητα αυθεντικοποίησης είναι περιορισμένης έκτασης και ακόμη παρακολουθείται σε πειραματικό στάδιο. Οι υπόλοιπες χώρες της ΕΕ δεν διαπιστώθηκε ότι σκοπεύουν να χρησιμοποιήσουν τέτοιες λύσεις στο άμεσο μέλλον.

# 3. ΤΟ ΕΥΡΩΠΑΪΚΟ ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ

Στο κεφάλαιο αυτό περιλαμβάνεται μία επισκόπηση της βασικής Ευρωπαϊκής Νομοθεσίας, όπως αυτή ισχύει σήμερα καθορίζοντας το νομικό πλαίσιο της ηλεκτρονικής αυθεντικοποίησης και τις πολιτικές των Ευρωπαϊκών κρατών ως προς τις λύσεις ηλεκτρονικής ταυτοποίησης που μπορούν να υλοποιήσουν.

Τα διάφορα κράτη-μέλη έχουνε πολύ διαφορετικές προσεγγίσεις σχετικά με τη διαχείριση των ηλεκτρονικών ταυτοτήτων, οι οποίες ποικίλουν από την ολοκληρωτική αποδεικτική ικανότητα των ηλεκτρονικών υπογραφών, τη χρήση εξειδικευμένων υποδομών αυθεντικοποίησηςPKI, την αξιοποίηση των συστημάτων PKI μέσω κινητών τηλεφώνων, συστήματα αυθεντικοποίησης δύο παραγόντων, και απλά συστήματα όνομα χρήστη/κωδικός πρόσβασης.

Πρώτα απ' όλα θα εξετασθεί το εφαρμοστέο Ευρωπαϊκό νομικό πλαίσιο, το οποίο συμπεριλαμβάνει την Οδηγία για της ηλεκτρονικές Υπογραφές[18], την Οδηγία για την Προστασία των Προσωπικών Δεδομένων[19], και την Οδηγία για τις παρεχόμενες Υπηρεσίες[20]. Σε κάθε περίπτωση, θα εξετασθούν οι βασικές αρχές από αυτά τα πλαίσια, και το κατά πόσο έχουνε εφαρμοστεί στα διάφορα κράτη μέλη.

Επίσης θα εξετασθούν τα εθνικά ρυθμιστικά πλαίσια αυτά καθ' αυτά, επικεντρώνοντας σε υψηλότερου επιπέδου επιλογές πολιτικής, όσον αφορά το βαθμό του συγκεντρωτισμού/αποκεντρωτισμού της διαχείρισης των ηλεκτρονικών ταυτοτήτων στις υπό μελέτη χώρες, και όσον αφορά σε θέματα αρμοδιοτήτων διαχείρισης των εν λόγω συστημάτων.

Σημαντικής αποδοχής σε σύνταξη με το εν λόγω ζήτημα είναι η αντίληψη ότι η τάση που διαμορφώνεται προκειμένου να επιτευχθεί η διασυνοριακή αυθεντικοποίηση, θα μπορούσε να συνεπάγεται μία αυξημένη πρόσβαση σε προσωπικά δεδομένα, το οποίο θα μπορούσε να απειλήσει την ιδιωτικότητα των πολιτών εάν δεν ληφθούν επαρκή μέτρα σχετικά με το ποιος έχει το δικαίωμα να προσπελάσει και να επεξεργαστεί τέτοιου είδους δεδομένα.

Τα κύρια Ευρωπαϊκά νομικά κείμενα τα οποία εξετάζονται όσον αφορά το θέμα της διαχείρισης των ηλεκτρονικών ταυτοτήτων είναι τα εξής:

- Η Οδηγία για τις ηλεκτρονικές υπογραφές[18], ως η κύρια πηγή του κανονιστικού πλαισίου στον τομέα των υπηρεσιών πιστοποίησης. Αυτό το κείμενο είναι σημαντικό, καθώς τα συστήματα PKI γίνονται ολοένα

και περισσότερο μία βασική λύση διαχείρισης ταυτότητας και η λειτουργία τους ρυθμίζεται εν πολλοίς μέσω αυτής της Οδηγίας.

- Η Οδηγία για την Ιδιωτικότητα[19], ως η κύρια πηγή του κανονιστικού πλαισίου στο θέμα της επεξεργασίας προσωπικών δεδομένων, συμπεριλαμβανομένων των μοναδικών αναγνωριστικών ταυτοποίησης. Αυτή η Οδηγία είναι σημαντική, καθώς τα θέματα ιδιωτικότητας αναφέρονται συχνά ως ένας από τους κύριους περιορισμούς στην υλοποίηση ενός πλαισίου διαλειτουργικότητας.

- Η Οδηγία για τις Υπηρεσίες[20] στο τμήμα που απαιτεί από τα Κράτη Μέλη να παρέχουν ένα ενιαίο σημείο επαφής όπου οι φορείς από χώρες του εξωτερικού οι οποίοι που φιλοδοξούν να παρέχουν υπηρεσίες σε τρίτες χώρες, πέραν της δικής τους, να μπορούν να συναντήσουν ηλεκτρονικά στην τρίτη χώρα όπου απευθύνονται τις οποιεσδήποτε απαιτήσεις σχετίζονται με την πρόσβαση και άσκηση οποιασδήποτε δραστηριότητας σχετιζόμενη με κάποια υπηρεσία η οποία καλύπτεται από την Οδηγία. Αυτό συνεπάγεται μία defacto υποχρέωση να προβλεφθεί ένα μηχανισμός αυθεντικοποίησης ο οποίος θα είναι προσβάσιμος από το εξωτερικό. Ο ρόλος των ηλεκτρονικών υπογραφών σε αυτή τη διαδικασία είναι ιδιαίτερα σημαντικός, και θα εξεταστεί με μεγαλύτερη λεπτομέρεια παρακάτω.

Για κάθε ένα από αυτά τα κείμενα, στις παρακάτω ενότητες θα εξεταστούν οι βασικές αρχές και η εφαρμοσιμότητα τους σε θέματα διαχείρισης ηλεκτρονικών ταυτοτήτων.

## 3.1 Οδηγία για τις Ηλεκτρονικές Υπογραφές (1999/93/ΕΚ)

### 3.1.1 Πεδίο Εφαρμογής της Οδηγίας

*(PKI, υπογραφές και αυθεντικοποίηση οντοτήτων)*

Το ακριβές πεδίο εφαρμογής της Οδηγίας για τις ηλεκτρονικές υπογραφές, συμπεριλαμβανομένης της εν δυνάμει εφαρμογής της στην αυθεντικοποίηση οντοτήτων, αποτελεί ένα πεδίο συνεχούς αντιπαράθεσης. Το κύριο πρόβλημα που δημιουργείται περιστρέφεται γύρω από την ερμηνεία της έννοιας “υπογραφή”. Όσο η Οδηγία ορίζει την ηλεκτρονική υπογραφή ως «δεδομένα σε ηλεκτρονική μορφή τα οποία επισυνάπτονται ή σχετίζονται λογικά με άλλα ηλεκτρονικά δεδομένα και τα οποία χρησιμεύουν ως μέθοδος

αυθεντικοποίησης» αυτό δεν επιλύει την κύρια σύγκρουση μεταξύ των δύο αντιμαχόμενων απόψεων.

- Μία πρώτη άποψη θεωρεί ότι ο κύριος στόχος της Οδηγίας στο συγκεκριμένο θέμα[58], ήταν να δημιουργήσει ένα σύνολο από κανόνες προκειμένου να αξιολογηθεί η αξία των ηλεκτρονικών υπογραφών ως το ψηφιακό ισοδύναμο μίας χειρόγραφης υπογραφής, και να προσδιορίσει πότε η εφαρμοζόμενη τεχνολογική λύση οδηγεί πράγματι σε ένα νομικό ισοδύναμο (δηλαδή σε μία ερμηνεία η οποία επιτυγχάνει μία ισχυρή σύνδεση μεταξύ του παραδοσιακού νομικού πλαισίου και την τεχνική διαδικασία υπογραφής). Σύμφωνα με αυτή την ερμηνεία, ο αντίκτυπος της Οδηγίας στην διαδικασία της χρησιμοποίησης της τεχνολογίας PKI, ως ένα σύστημα για την αυθεντικοποίηση οντοτήτων είναι περιορισμένος, εξ' αιτίας του γεγονότος ότι το έννομο αποτέλεσμα μίας υπογραφής ως ενός μηχανισμού για την αυθεντικοποίηση οντοτήτων είναι εντελώς απροσδιόριστο στην Οδηγία, καθώς δεν έχει εφαρμογή το άρθρο 5.
- Μία δεύτερη άποψη θεωρεί ότι η Οδηγία στο σύνολό της, ρυθμίζει τη χρήση ψηφιακών υπογραφών ως μία τεχνολογία εν γένει, και ότι 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»[59] 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.

Είναι ξεκάθαρο ότι ο όρος «Οδηγία για τις Ηλεκτρονικές Υπογραφές» είναι αρκετά παραπλανητικός, ή τουλάχιστον ασαφής ως προς το ακριβές περιεχόμενο του. Στις ενότητες που ακολουθούν θα εξετασθεί εάν και κατά πόσο η Οδηγία έχει εφαρμογή στην διαχείριση ταυτότητας.

### 3.1.2 Εφαρμογή στο ζήτημα της διαχείρισης ταυτότητας

Το βασικό ερώτημα σε σχέση με την εφαρμογή της Οδηγίας είναι το αν ή όχι οι υπηρεσίες αυθεντικοποίησης οντοτήτων (συμπεριλαμβανομένων ιδίως εκείνες που βασίζονται σε μεθόδους PKI) καλύπτονται από την Οδηγία, και αν ναι, ποιο θα είναι το αποτέλεσμα.

[58] Άρθρο 5 της Οδηγίας 1999/93/ΕΚ
[59] CSP: Certification Service Provider

Προκειμένου να προσδιορισθεί η αξία της Οδηγίας για τους σκοπούς της διαχείρισης ταυτότητας, η διάταξη κλειδί είναι η ρήτρα που αφορά στις έννομες συνέπειες μίας ηλεκτρονικής υπογραφής (άρθρο 5).

Όσον αφορά στη νομική αξία της ηλεκτρονικής υπογραφής, η Οδηγία καθιερώνει ένα κλιμακωτό σύστημα:

*"Άρθρο 5 – Έννομες συνέπειες των ηλεκτρονικών υπογραφών*

> *"1. Τα κράτη μέλη διασφαλίζουν ότι οι προηγμένες ηλεκτρονικές υπογραφές που βασίζονται σε αναγνωρισμένο πιστοποιητικό και οι οποίες δημιουργούνται από ασφαλή διάταξη δημιουργίας υπογραφής:*
>
> *(α) ικανοποιούν τις νομικές απαιτήσεις υπογραφής σε σχέση με τα δεδομένα σε ηλεκτρονική μορφή κατά τον ίδιο τρόπο που μια ιδιόχειρη υπογραφή ικανοποιεί τις απαιτήσεις αυτές σε σχέση με τα δεδομένα που καταχωρούνται επί χάρτου, και*
>
> *(β) γίνονται δεκτές ως αποδεικτικό στοιχείο σε νομικές διαδικασίες*
>
> *2) Τα κράτη μέλη διασφαλίζουν ότι δεν απορρίπτεται η νομική ισχύς και το παραδεκτό μιας ηλεκτρονικής υπογραφής ως αποδεικτικού στοιχείου σε νομικές διαδικασίες μόνο λόγω του γεγονότος ότι:*
>
> - *είναι υπό μορφή ηλεκτρονικών δεδομένων, ή*
> - *δεν βασίζεται σε αναγνωρισμένο πιστοποιητικό, ή*
> - *δεν βασίζεται σε αναγνωρισμένο πιστοποιητικό που εξεδόθη από διαπιστευμένο πάροχο υπηρεσιών πιστοποίησης, ή*
> - *δεν δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής."*

Σύμφωνα με αυτό το άρθρο, η λεγόμενη αναγνωρισμένη υπογραφή (άρθρο 5§1) θεωρείται ισοδύναμη με την χειρόγραφή υπογραφή, ενώ και άλλοι τύποι ηλεκτρονικών υπογραφών (άρθρο 5§2) θα πρέπει να γίνονται αποδεκτοί ίσως σε μικρότερο βαθμό και δεν θα πρέπει να απορρίπτονται εξ' αιτίας του ηλεκτρονικού τους χαρακτήρα.

Όπως προαναφέρθηκε, η πρώτη παράγραφος δεν έχει πραγματικό νόημα για τους σκοπούς της αυθεντικοποίησης οντοτήτων καθώς μία ιδιόχειρη υπογραφή ποτέ δεν θεωρήθηκε ως κατάλληλος τρόπος για την απόδειξη της ταυτότητας μίας οντότητας. Ως εκ τούτου, η νομική ισοδυναμία με μία ιδιόχειρης υπογραφής δεν ασχολείται με την έννομη συνέπεια της διαδικασίας ταυτοποίησης. Ομοίως, η δεύτερη παράγραφος εισάγει απλά την αρχή της μη διάκρισης, και επομένως η μόνη νομική ισχύ για τα συστήματα αυθεντικοποίησης που βασίζονται σε PKI είναι ότι το σύστημα δεν θα πρέπει να θεωρηθεί νομικά αναποτελεσματικό. Με λίγα λόγια, το άρθρο 5 δεν περιέχει διατάξεις που να αναφέρουν ότι θα πρέπει να εκχωρηθεί σε μία ηλεκτρονική

υπογραφή ή αντίστοιχη κάποια συγκεκριμένη αξία γνησιότητας για την αυθεντικοποίηση οντοτήτων.

Είναι συνεπώς σημαντικό να γνωρίζουμε ότι το νομικό πλαίσιο για τις ηλεκτρονικές υπογραφές δεν επιλύει το κρίσιμο ερώτημα της αυθεντικοποίησης, δηλαδή το πώς ξέρω ότι το άτομο με το οποίο επικοινωνώ είναι αυτό που ισχυρίζεται ότι είναι. Αυτό αποτελεί ένα ζήτημα το οποίο δεν επιλύεται από την Οδηγία, η οποία προϋποθέτει την προηγούμενη επίλυση του ζητήματος της ταυτοποίησης, χωρίς να παρέχει προς τούτο συγκεκριμένες οδηγίες.

Αυτό καθίσταται σαφές και στον ορισμό της προηγμένης ηλεκτρονικής υπογραφής (άρθρο 2§2) όπου απλώς διευκρινίζεται ότι η υπογραφή θα πρέπει να είναι «ικανή να ταυτοποιεί τον υπογράφοντα», χωρίς να προσδιορίζεται ο τρόπος με τον οποίο κάτι τέτοιο θα μπορούσε να επιτευχθεί, ενώ και στον ορισμό ενός πιστοποιητικού απλώς αναφέρεται ότι θα πρέπει να «επιβεβαιώνει την ταυτότητα αυτού του ατόμου».

Πράγματι, ακόμη και όταν αναφέρεται σε εγκεκριμένες υπογραφές, το Παράρτημα ΙΙ της Οδηγίας αποφεύγει ρητά αυτό το ζήτημα και αφήνει την ερμηνεία του στην διακριτική ευχέρεια των κρατών μελών:

> *«ΠΑΡΑΡΤΗΜΑ ΙΙ – Όροι ισχύοντες για παρόχους υπηρεσιών πιστοποίησης που εκδίδουν αναγνωρισμένα πιστοποιητικά*
>
> *Οι πάροχοι υπηρεσιών πιστοποίησης πρέπει:*
>
> *[…]*
>
> *(δ) να προβαίνουν, με κατάλληλα μέσα και σύμφωνα με το εθνικό δίκαιο, σε επαλήθευση, της ταυτότητας και ενδεχομένως, τυχόν ειδικών χαρακτηριστικών του ατόμου στο όνομα του οποίου έχει εκδοθεί αναγνωρισμένο πιστοποιητικό*
>
> *[…]».*

Αυτό δεν αποκλείει συστήματα PKI από το να αποτελέσουν μία απολύτως κατάλληλη τεχνική λύση για τη διαχείριση των eID.

Ωστόσο είναι σημαντικό να σημειωθεί ότι η Οδηγία αυτή καθ' αυτή δεν θίγει το έννομο αποτέλεσμα της αυθεντικοποίησης του ατόμου. Δεν καθορίζει το πότε μία οντότητα έχει αναγνωριστεί μονοσήμαντα, ούτε το ποια είναι η νομική συνέπεια ενός πιστοποιητικού αυθεντικοποίησης. Με λίγα λόγια, το ζήτημα της αυθεντικοποίησης οντοτήτων δεν ρυθμίζεται επί του παρόντος σε Ευρωπαϊκό επίπεδο!

Για το λόγο αυτό, καθώς επίσης και προκειμένου να αξιοποιηθούν τα συμπεράσματα των έργων τα οποία αυτή τη στιγμή βρίσκονται σε εξέλιξη, η Ευρωπαϊκή Ένωση έχει εντάξει στις προτεραιότητες για τα έτη 2011 έως και 2015 την δράση 35 η οποία υπάγεται στο σχέδιο δράσεων 4.2 για την ηλεκτρονική διακυβέρνηση και η οποία αναφέρεται στην αναθεώρηση της Οδηγίας για τις Ηλεκτρονικές Υπογραφές[21].

## 3.2 Οδηγία για την προστασία προσωπικών δεδομένων (95/46/ΕΚ)

Το κύριο αντικείμενο της Οδηγίας 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»[60].

Κατά συνέπεια, δεν προκαλεί έκπληξη ότι η διαχείριση των ηλεκτρονικών ταυτοτήτων – η οποία εξ' ορισμού περιστρέφεται γύρω από τη διαχείριση των προσωπικών δεδομένων για ταυτοποίηση – επηρεάζεται σε μεγάλο βαθμό από τις αρχές της Οδηγίας.

Αυτές οι βασικές αρχές συνοψίζονται στο άρθρο 6 της Οδηγίας, και περιλαμβάνουν τις απαιτήσεις που τα προσωπικά δεδομένα θα πρέπει να έχουν και πιο συγκεκριμένα ότι:

*Α) να υφίστανται σύννομη και θεμιτή επεξεργασία*

*Β) να συλλέγονται για καθορισμένους, σαφείς και νόμιμους σκοπούς και η μεταγενέστερη επεξεργασία τους να συμβιβάζεται με τους σκοπούς αυτούς. Η μεταγενέστερη επεξεργασία για ιστορικούς, στατιστικούς ή επιστημονικούς σκοπούς δεν θεωρείται ασυμβίβαστη εφόσον τα κράτη μέλη προβλέπουν κατάλληλες εγγυήσεις*

*Γ) να συλλέγονται να είναι κατάλληλα, συναφή προς το θέμα και όχι υπερβολικά σε σχέση με τους σκοπούς για τους οποίους συλλέγονται και υφίστανται επεξεργασία*

*Δ) να είναι ακριβή και, εφόσον χρειάζεται να ενημερώνονται – πρέπει να λαμβάνονται όλα τα εύλογα μέτρα ώστε δεδομένα ανακριβή ή ελλιπή σε σχέση με τους σκοπούς για τους οποίους έχουν συλλεγεί ή υφίστανται κατόπιν επεξεργασία, να διαγράφονται ή να διορθώνονται και τέλος*

[60] Άρθρο 1§1 της Οδηγίας 95/46/ΕΚ

*Ε) να διατηρούνται με μορφή που επιτρέπει τον προσδιορισμό της ταυτότητας των προσώπων στα οποία αναφέρονται μόνο κατά τη διάρκεια περιόδου που δεν υπερβαίνει την απαιτούμενη για την επίτευξη των σκοπών για τους οποίους έχουν συλλεγεί ή για τους οποίους αργότερα υφίστανται επεξεργασία. Τα κράτη μέλη προβλέπουν κατάλληλες εγγυήσεις για τα δεδομένα προσωπικού χαρακτήρα που διατηρούνται πέραν της περιόδου αυτής για σκοπούς ιστορικούς, στατιστικούς ή επιστημονικούς.*

Για τους σκοπούς της διαχείρισης ταυτοτήτων σε ένα πλαίσιο ηλεκτρονικής διακυβέρνησης, ένα βασικό μέλημα αποτελεί η σχετική ελευθερία των Κρατών Μελών να καθορίζουν, πότε η επεξεργασία προσωπικών δεδομένων είναι επιτρεπτή και εντός των ορίων της αρχής τη αναλογικότητας, τι είδους εγγυήσεις θα πρέπει να δοθούν στα πλαίσια της προστασίας της ιδιωτικής ζωής (και υπό ποιους όρους). Δεδομένου του ότι αυτές είναι βασικές επιλογές πολιτικής, οι οποίες καθιερώθηκαν μέσω της επίσημης νομολογίας (όπως Εθνικοί Νόμοι, Νόμοι για τα Δελτία Ταυτότητας, Νόμοι για την Ηλεκτρονική Διακυβέρνηση και ούτω καθ' εξής).

Από την οπτική της διασυνοριακής διαλειτουργικότητας, τα άρθρα 6(Β) έως 6(Δ) παρουσιάζουν ιδιαίτερο ενδιαφέρον, καθώς καθορίζουν σε υψηλό επίπεδο τις προϋποθέσεις για τη νόμιμη διασυνοριακή αυθεντικοποίηση με τη χρήση πηγών του δημόσιου τομέα.

- Το άρθρο 6(Β) καθιερώνει την βασική αρχή ότι τα προσωπικά δεδομένα θα πρέπει να συλλέγονται για καθορισμένους, σαφείς και νόμιμους σκοπούς οι οποίοι θα πρέπει να παραμένουν ως έχουν και μετά τη συλλογή. Αυτή η αρχή είναι σημαντική σε ένα πλαίσιο ηλεκτρονικής διακυβέρνησης, 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. Ως γενική αρχή η ερμηνεία της υπόκειται σε εξέλιξη και σε προσαρμογή σε τοπικές παραμέτρους, ωστόσο είναι σαφές ότι η χρήση πηγών ταυτοποίησης σε ένα διασυνοριακό πλαίσιο θα πρέπει ως ένας γενικός κανόνας, να είναι δυνατή μόνο με τη συγκατάθεση του υποκειμένου των δεδομένων, δηλαδή θα πρέπει να είναι «πολιτικοκεντρική». Οποιαδήποτε άλλη λύση ενέχει τον κίνδυνο της παραβίασης αυτής της πρώτης βασικής αρχής.

- Το άρθρο 6(Γ) διατυπώνει την αρχή της αναλογικότητας, αναφέροντας ότι τα προσωπικά δεδομένα θα πρέπει να είναι κατάλληλα, συναφή και απολύτως αναγκαία για την επίτευξη του επιδιωκόμενου σκοπού. Στην περίπτωση της αυθεντικοποίησης, αυτό θα σημαίνει ότι δεν θα πρέπει να απαιτείται να διατηρούνται για το υποκείμενο των δεδομένων,

περισσότερα προσωπικά δεδομένα από τα απολύτως αναγκαία για την επίτευξη του σκοπού της εφαρμογής. Για τις περισσότερες εφαρμογές, αυτό θα σήμαινε ένα σύνολο δεδομένων το οποίο θα επέτρεπε στο υποκείμενο των δεδομένων να ταυτοποιηθεί μοναδικά. Ωστόσο για κάποιες εφαρμογές οι απαιτήσεις αυθεντικοποίησης ικανοποιούνται επαρκώς με την καθιέρωση κάποιων χαρακτηριστικών γνωρισμάτων για το υποκείμενο των δεδομένων (όπως για παράδειγμα να απαιτείται το άτομο να είναι ενήλικο, ή ίσως να απαιτείται το άτομο να είναι πολίτης κάποιας χώρας), και κατά τον τρόπο αυτό δεν απαιτείται από κάθε μεμονωμένο άτομο να ταυτοποιηθεί ως προς κάθε στοιχείο του. Η αυθεντικοποίηση δηλαδή θα πρέπει να υπαγορεύεται από πληροφοριακές ανάγκες οι οποίες έχουνε υφίστανται για το άτομο, και όχι από την πιθανότητα που ίσως προκύψουν τέτοιες ανάγκες.

- Το άρθρο 6(δ) απαιτεί οι υπεύθυνοι επεξεργασίας δεδομένων να ελέγχουν την ακρίβεια των προσωπικών δεδομένων που διαχειρίζονται. Η αρχή αυτή είναι μία σημαντική αρχή, ειδικά για τα δεδομένα τα οποία διαχειρίζονται οι δημόσιοι φορείς, τα οποία συνήθως τα επικαλούνται ως προς την ακρίβειά τους τόσο δημόσιοι όσο και ιδιωτικοί φορείς. Το άρθρο αυτό απαιτεί από τις κυβερνήσεις να διασφαλίσουν ότι οι πληροφοριακοί πόροι τους οποίους διαθέτουν υπό τον έλεγχό τους, είναι ακριβής και ενημερωμένοι. Από διασυνοριακή οπτική, αυτό σημαίνει ότι οι οντότητες πέραν των συνόρων της χώρας τους, προκειμένου να μπορούν να ταυτοποιηθούν θα πρέπει η ταυτοποίση να βασίζεται σε πληροφορίες οι οποίες παρέχονται μέσω ενός συστήματος διαχείρισης ηλεκτρονικών ταυτοτήτων, το οποίο εξασφαλίζει τις υφιστάμενες κάθε φορά νομικές εγγυήσεις.

Οι αρχές αυτές, είναι επίσης στενά συνδεδεμένες με την αρχή της αυθεντικής πηγής η οποία βρίσκει αυξημένη αποδοχή στις υπό μελέτη χώρες. Η αρχή συνεπάγεται ότι για κάθε δεδομένο χαρακτηριστικό (τμήμα δεδομένων ταυτοποίησης), μία και μόνο μία πηγή μπορεί να θεωρηθεί ότι είναι αυθεντική για τη διασταύρωση αυτού του στοιχείου. Η πληροφορία αυτή θα πρέπει να επαναχρησιμοποιηθεί από όλα τα μέρη που έχουν ορισμένο έννομο συμφέρον, έτσι ώστε να ελαχιστοποιηθεί η ενόχληση του χρήστη (με το να μην απαιτείται από αυτόν να παρέχει την ίδια απαραίτητη πληροφορία ξανά και ξανά, και να διαβεβαιώνει ότι υπάρχει μόνο ένα σημείο στο οποίο η οποιαδήποτε τροποποιούμενη πληροφορία θα πρέπει να διορθώνεται (ενεργοποιώντας έτσι την αρχή της «ακρίβειας» της Οδηγίας).

Εκτός από αυτές τις βασικές αρχές, το άρθρο 7 της Οδηγίας περιγράφει τις συνθήκες κατά τις οποίες τα προσωπικά δεδομένα μπορεί να τύχουν επεξεργασίας, συμπεριλαμβανομένων και των:

*"α) όταν το πρόσωπο στο οποίο αναφέρονται τα δεδομένα έχει δώσει τη ρητή συγκατάθεσή του ή*

*β) 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*

*γ) όταν είναι απαραίτητη για την τήρηση εκ του νόμου υποχρεώσεως του υπευθύνου της επεξεργασίας ή*

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

*ε) 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*

*στ) 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."*

Έχοντας κατά νου την προαναφερθείσα αρχή η οποία έχει ως επίκεντρο τον χρήστη, η χρήση των δεδομένων ταυτοποίησης είναι προφανώς προτιμότερο να πραγματοποιείται κατόπιν της συναίνεσης του πολίτη. Ωστόσο θα πρέπει να σημειωθεί ότι για τους σκοπούς της ηλεκτρονικής διακυβέρνησης δημιουργείται συχνά ένα ξεχωριστό νομικό πλαίσιο ως προς τη διαχείριση των ηλεκτρονικών πηγών προσωπικών δεδομένων, συνήθως με τη μορφή Εθνικού Νόμου περί μητρώων, Νόμου σχετικά με τις ταυτότητες, Νόμου σχετικά με την ηλεκτρονική διακυβέρνηση, και ούτω καθεξής, οι οποίοι χρησιμεύουν για τη νομική κατοχύρωση της επεξεργασίας προσωπικών δεδομένων ακόμη και χωρίς την ρητή συγκατάθεση του υποκειμένου των δεδομένων.

## 3.3 Οδηγία για τις Υπηρεσίες (2006/123/ΕΚ)

Τέλος, η Οδηγία για τις Υπηρεσίες, της 12ης Δεκεμβρίου 2006[61], εισάγει ένα νομικό πλαίσιο με στόχο να επέλθει η εναρμόνιση της εσωτερικής αγοράς, στο θέμα της παροχής υπηρεσιών, τόσο σε σχέση με το θέμα της ελευθερίας εγκατάστασης των παρόχων των υπηρεσιών όσο και στο θέμα της ελεύθερης κυκλοφορίας των υπηρεσιών[62].Αυτό θα διευκολύνει την παροχή και χρήση

[61] Η οποία θα έπρεπε να έχει μεταφερθεί στις εθνικές νομοθεσίες και να έχει εφαρμοστεί από τα κράτη μέλη έως την 28η Δεκεμβρίου 2009, σύμφωνα με το άρθρο 44 της Οδηγίας

[62] Άρθρο 1 της Οδηγίας των Υπηρεσιών, Επίσημη Εφημερίδα L 376 της 27.12.2006

υπηρεσιών οι οποίες παρέχονται σε διασυνοριακό επίπεδο στην Ευρωπαϊκή Ένωση αυξάνοντας έτσι το διασυνοριακό ανταγωνισμό στις αγορές υπηρεσιών, προκαλώντας μείωση στις τιμές των παρεχόμενων υπηρεσιών και βελτίωση της ποιότητας και των επιλογών των τελικών καταναλωτών.

### 3.3.1 Εφαρμογή στο θέμα της διαχείρισης ταυτοτήτων

Αν και δεν έχει ρητή σχέση σχετικά με την ηλεκτρονική διακυβέρνηση ή την διαχείριση ταυτότητας στο σύνολό της, η Οδηγία παρέχει μία ειδικότερη διάταξη η οποία θα έχει άμεσο αντίκτυπο στην κατάσταση των συστημάτων διαχείρισης ηλεκτρονικής ταυτότητας σε πολλές χώρες. Ειδικότερα στο άρθρο 8 της Οδηγίας ορίζεται ότι:

> *Άρθρο 8 - Ηλεκτρονική διεκπεραίωση διαδικασιών:*
>
> *1. Τα κράτη μέλη εξασφαλίζουν ότι όλες οι διαδικασίες και οι διατυπώσεις για την πρόσβαση σε δραστηριότητες παροχής υπηρεσιών και για την άσκησή τους μπορούν να διεκπεραιωθούν εύκολα από απόσταση και με ηλεκτρονικά μέσα μέσω του οικείου ενιαίου κέντρου εξυπηρέτησης και στις αρμόδιες αρχές.*
>
> *2. Η παράγραφος 1 δεν αφορά τις επιθεωρήσεις του τόπου παροχής της υπηρεσίας ή του εξοπλισμού που χρησιμοποιείται από τον πάροχο ή την υλική εξέταση των ικανοτήτων ή της προσωπικής ακεραιότητας του παρόχου ή του αρμόδιου προσωπικού του.*
>
> *3. 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 συστημάτων πληροφοριών και τη χρήση διαδικασιών με ηλεκτρονικά μέσα μεταξύ των κρατών μελών, λαμβάνοντας υπόψη τα κοινά πρότυπα που εκπονούνται σε κοινοτικό επίπεδο.*

Η πρώτη παράγραφος αυτού του άρθρου απαιτεί από τα Κράτη-Μέλη να δημιουργήσουν ουσιαστικά ένα on-line one-stop-shop[63], όπου οι πάροχοι των υπηρεσιών θα μπορούν να βρούνε ένα χώρο όπου ικανοποιούνται όλες οι απαιτήσεις οι οποίες καλύπτονται από την Οδηγία, σχετικά με την πρόσβαση ή την άσκηση των υπηρεσιών τους στην κάθε χώρα. Ένα από τα πιο κρίσιμα ζητήματα στην υλοποίηση τέτοιου είδους συστημάτων είναι η ηλεκτρονική ταυτοποίηση των χρηστών.

Θα πρέπει να σημειωθεί ότι αυτή η παράγραφος δεν επιβάλλει στα Κράτη Μέλη να εφαρμόσουν ένα εξειδικευμένο σύστημα διαχείρισης ηλεκτρονικών ταυτοτήτων το οποίο να είναι διαλειτουργικό με οποιοδήποτε μη εθνικό σύστημα. Θα ήταν εξίσου πιθανό να εφαρμόσουν ένα αυστηρά εθνικό σύστημα

[63] a point of single contact - PSC

ελέγχου αυθεντικοποίησης χαμηλότερου επιπέδου το οποίο να επιτρέπει σε μη εθνικές οντότητες να ικανοποιήσουν τις ανάγκες τους ηλεκτρονικά από απόσταση.

Θεωρητικά, η πιο ιδανική λύση θα ήταν να εφαρμοστεί ένα διαλειτουργικό σύστημα eIDM το οποίο θα επέτρεπε στις μη εθνικές οντότητες, με ένα αποδεκτό βαθμό βεβαιότητας να αυθεντικοποιούνται χρησιμοποιώντας τα δικά τους εθνικά eIDM συστήματα. Ωστόσο, στην περίπτωση αυτή συνεχίζει να υπάρχει η εγγενής αδυναμία που απαιτεί ένα αξιόπιστο μη εθνικό σύστημα να είναι διαλειτουργικό, το οποίο μπορεί να μην υπάρχει σε ορισμένες χώρες.

Είναι σαφές ότι η Οδηγία προβλέπει την δημιουργία διαλειτουργικών μηχανισμών (τόσο όσον αφορά στο θέμα της αυθεντικοποίησης όσο και στο θέμα της ανταλλαγής εγγράφων) ως ένα βασικό μοχλό για την τήρηση των διατάξεων του άρθρου 8. Αυτό καταμαρτυρείται από την τρίτη παράγραφο του άρθρου, η οποία παρέχει στην Ευρωπαϊκή Επιτροπή την εξουσία να «υιοθετεί λεπτομερείς κανόνες για την εφαρμογή της παραγράφου 1 του άρθρου, με στόχο την διευκόλυνση της διαλειτουργικότητας των πληροφοριακών συστημάτων και της χρησιμοποίησης των διαδικασιών τους».

Το ζήτημα της διαχείρισης ταυτότητας ελέγχθηκε μέσω του Ευρωπαϊκού έργου CROBIES το οποίο ως έργο τιτλοφορείται ως πρόγραμμα για τις «ελάχιστες απαιτήσεις για ένα αναγνωρισμένο πιστοποιητικό το οποίο θα υποστηρίζει τις αναγνωρισμένες ηλεκτρονικές υπογραφές»[22]. Όπως αναφέρεται και στον τίτλο, το έργο αυτό εστιάζεται κυρίως στη βελτίωση της διαλειτουργικότητας των ηλεκτρονικών υπογραφών που βασίζονται σε αναγνωρισμένα πιστοποιητικά και όχι στον έλεγχο αυθεντικοποίησης μίας οντότητας ως τέτοια, ωστόσο ενδέχεται να έχει επίσης μία σημαντική επίδραση σε θέματα διαχείρισης ταυτότητας.

# 4. ΕΘΝΙΚΑ ΡΥΘΜΙΣΤΙΚΑ ΠΛΑΙΣΙΑ ΚΑΙ ΠΡΟΣΕΓΓΙΣΕΙΣ

Τα εθνικά ρυθμιστικά πλαίσια (National Register Acts, Identity Card Acts, eGovernment Acts) τα οποία διαμορφώνονται προκειμένου να καθιερωθούν οι ηλεκτρονικές ταυτότητες σε κάθε κράτος μέλος αλλά και προκειμένου να μπορούν αυτές να διαχειρίζονται από τους αρμόδιους φορείς επηρεάζονται από κάποιους βασικούς παράγοντες. Οι παράγοντες αυτοί αποτελούν το πλαίσιο εντός του οποίου πραγματοποιείται η νομική θωράκιση και διαμορφώνεται από τα ελάχιστα προσωπικά δεδομένα τα οποία είναι απαραίτητα προκειμένου να καταστεί εφικτή η ταυτοποίηση του πολίτη κάθε φορά που αυτός χρησιμοποιεί μία υπηρεσία του δημόσιου τομέα και αφετέρου από τον τρόπο με τον οποίο διασφαλίζεται η εμπιστοσύνη στην ακρίβεια αυτής της πληροφορίας.

Η προσέγγιση η οποία εφαρμόζεται κατά περίπτωση στα διάφορα κράτη μέλη προκειμένου να εγκαθιδρυθεί αυτός ο ασφαλής δίαυλος εμπιστοσύνης μεταξύ των διαφόρων φορέων που εμπλέκονται στη διαδικασία ταυτοποίησης διαφέρει. Στην διαδικασία αυτή υπάρχει από τη μία πλευρά ο πάροχος υπηρεσιών πιστοποίησης (identity provider) και από την άλλη οι πάροχοι υπηρεσιών προς τον πολίτη (relying third parties). Όσες όμως και αν είναι οι διαφορές στις διάφορες προσεγγίσεις εν τούτοις υπάρχουν και κάποια κοινά στοιχεία τα οποία αναφέρονται στις ενότητες που ακολουθούν.

## *4.1 Αποκέντρωση και εσωτερική εναρμόνιση λύσεων και συστημάτων eIDM*

Η προσέγγιση η οποία έχει επιλεγεί σε όλες τις χώρες δεν περιλαμβάνει κάποιο κεντρικό σύστημα το οποίο να διαχειρίζεται μοναδικά τις ηλεκτρονικές ταυτότητες της εκάστοτε χώρας. Η βασική υλοποίηση των περισσοτέρων χωρών περιλαμβάνει την ύπαρξη περισσοτέρων του ενός συστημάτων (περιορισμένου πάντως πλήθους συστημάτων) τα οποία θα είναι επιφορτισμένα με αυτό το ρόλο. Αυτό το περιβάλλον όμως το οποίο διαμορφώνεται με την χρησιμοποίηση αυτών των νέων συστημάτων που εγκαθίστανται, δεν αναιρεί τη θέση και τον ρόλο τον οποίο διαδραματίζουν άλλα μικρότερης εμβέλειας συστήματα τα οποία συνεχίζουν να υπάρχουν παράλληλα, συνήθως υποβοηθώντας στην παροχή κάποιας συγκεκριμένης κατηγορίας υπηρεσιών (π.χ. υπηρεσίες φορολογίας) ή στα πλαίσια κάποιας εφαρμογής (όπως για παράδειγμα την αίτηση κάποιου πιστοποιητικού).

Οι Ευρωπαϊκές χώρες ως προς το θέμα της διαχείρισης των ηλεκτρονικών ταυτοτήτων για την πραγματοποίηση ηλεκτρονικών συναλλαγών

των πολιτών με την δημόσια διοίκηση, βρίσκονται στην παρούσα φάση ακόμα στο στάδιο της εσωτερικής εναρμόνισης (internal consolidation), κάτι το οποίο υποδηλώνει ότι οι διαδικασίες δεν έχουνε ωριμάσει πλήρως.

Η τάση η οποία φαίνεται πως επικρατεί, είναι η σταδιακή κατάργηση των τομεακών λύσεων και των λύσεων μικρής εμβέλειας και η αντικατάσταση τους από πιο ευρύτερου πεδίου εφαρμογής λύσεις, μέσω των αντιστοίχων συστημάτων ταυτοποίησης, οι οποίες θα έχουνε μεγαλύτερο λόγο απόδοσης σε σχέση με την πραγματοποιούμενη κάθε φορά επένδυση, από ότι η υποστήριξη αντιστοίχων κάθε φορά υλοποιήσεων οι οποίες θα υφίστανται προκειμένου να υποστηρίζεται η παροχή συγκεκριμένων κάθε φορά υπηρεσιών.

Αυτή η τάση όμως δεν τυγχάνει καθολικής εφαρμογής. Οι κεντρικές λύσεις διαχείρισης ηλεκτρονικών ταυτοτήτων φαίνεται πως δεν έχουνε εφαρμογή σε δύο περιπτώσεις όπως φαίνεται στη συνέχεια οι οποίες εξαιρούνται του γενικού κανόνα-υφιστάμενης τάσης-:

- Η περίπτωση της καθιέρωσης εξειδικευμένων λύσεων για συγκεκριμένες κατηγορίες χρηστών. Η εξαίρεση αυτή αναφέρεται σε πολιτικές αποφάσεις οι οποίες λαμβάνονται σε κάποιες περιπτώσεις και βάσει τον οποίων μπορεί να θεωρείται ότι η ύπαρξη τοπικών και εξειδικευμένων λύσεων μπορεί να εξυπηρετεί πιο ολοκληρωμένα και με πιο κατάλληλο τρόπο τις υπάρχουσες ανάγκες. Ένα ενδεικτικό παράδειγμα αποτελεί η Γαλλική Carte Vitale[64] και η Ιταλική CNS[65] οι οποίες έχουνε δημιουργηθεί ως ηλεκτρονικές κάρτες-ταυτότητες και αφορούν σε συγκεκριμένες περιφέρειες με διοικητική αυτονομία. Ακόμη ενδέχεται να εκδοθούν διακριτικά αυθεντικοποίησης κατάλληλα για την αυθεντικοποίηση συγκεκριμένων ομάδων χρηστών εξ' αιτίας της ιδιότητας ή του ρόλου τους όπως για παράδειγμα η κάρτα CMD για τα στελέχη της δημόσιας διοίκησης στην Ιταλία και τα ψηφιακά πιστοποιητικά αυθεντικοποίησης για τους δικηγόρους και τους συμβολαιογράφους στην Πορτογαλία[23]. Στις περιπτώσεις που προαναφέρθηκαν όπου προκρίνεται μία πιο συγκεκριμένη επιλογή, η επιλογή αυτή της εξειδικευμένης λύσης για ορισμένους χρήστες τεκμηριώνεται από πλεονεκτήματα τα οποία κατά περίπτωση προκύπτουν από την επιλογή αυτή.

- Σε μία δεύτερη εξαίρεση που παρατηρείται έχουμε την ανάπτυξη εξειδικευμένων λύσεων ηλεκτρονικών ταυτοτήτων όταν πρόκειται να πραγματοποιηθεί επεξεργασία ευαίσθητων προσωπικών δεδομένων[66]. Σε

[64] French Carte Vitale, βλ. σχετικά http://www.french-property.com/guides/france/public-services/health/health-card/

[65] Τα αρχικά CNS αναφέρονται στην Italian Carta Nazionale dei Servizi (CNS), βλ. σχετικά http://www.opensc-project.org/opensc/wiki/ItalianCNS

[66] Ως ευαίσθητα δεδομένα ορίζονται με βάση το άρθρο 2 του Ν.2472/97 (περί προστασίας προσωπικών δεδομένων) τα δεδομένα που αφορούν τη φυλετική ή εθνική προέλευση, τα πολιτικά

αυτή την κατηγορία ανήκουν λύσεις οι οποίες αναπτύσσονται και λειτουργούν στον τομέα της υγείας, της κοινωνικής ασφάλισης καθώς επίσης και για επαγγελματίες ειδικά του ιατρικού και φαρμακευτικού κλάδου.

Ορισμένα Ευρωπαϊκά κράτη (όπως η Αυστρία, η Ουγγαρία και η Ιταλία) έχουνε επιλέξει να δημιουργήσουν μία ενιαία υποδομή ηλεκτρονικών ταυτοτήτων βασισμένη σε συγκεκριμένες αρχιτεκτονικές και πρότυπα. Στις περιπτώσεις αυτές η συνολική λύση διαχείρισης ηλεκτρονικών ταυτοτήτων προσδιορίζεται από την ικανοποίηση μίας σειράς προδιαγραφών και απαιτήσεων, με αποτέλεσμα οι επιμέρους λύσεις να μπορούν να υλοποιηθούν με διαφορετικούς τρόπους ανάλογα με τις ανάγκες. Στην περίπτωση της Αυστρίας η ηλεκτρονική κάρτα του πολίτη, δεδομένου του ότι οι επιμέρους λύσεις μπορούν να αναπτυχθούν στη βάση της οποιασδήποτε διαθέσιμης τεχνολογίας, συμπεριλαμβανομένης και της ταυτοποίησης μέσω των καρτών κινητής τηλεφωνίας του χρήστη[24]. Με τον τρόπο αυτό οι Αυστριακοί πολίτες δεν είναι υποχρεωμένοι να κατέχουν πλαστική έξυπνη κάρτα «παραδοσιακού» τύπου. Κατ' αντιστοιχία αλλά σε πιο περιορισμένο πλαίσιο, η Ουγγαρία διαθέτει την HUNEID[25] [67] και η Ιταλία την CMD/ATA-E[26].

## *4.2 Ανάμιξη του ιδιωτικού τομέα*

Από το σύνολο των χωρών της ΕΕ κρίνεται απαραίτητη η ανάμιξη του ιδιωτικού τομέα στο πλαίσιο της διαχείρισης των ηλεκτρονικών ταυτοτήτων. Οι λόγοι για τους οποίους συμβαίνει κάτι τέτοιο είναι διάφοροι και θα αναπτυχθούν στη συνέχεια.

Οι περισσότερες από τις χώρες της ΕΕ αναγνωρίζουν τη μεγάλη σημασία που έχει η υιοθέτηση των λύσεων διαχείρισης ηλεκτρονικών ταυτοτήτων και από τις επιχειρήσεις του ιδιωτικού τομέα. Είναι κοινά αποδεκτό μεταξύ των κρατών μελών ότι το να προκριθεί μία λύση η οποία θα αφορά στην ενσωμάτωση ενός συστήματος αποκλειστικά για υπηρεσίες του δημόσιου τομέα δεν θα αποτελούσε κάτι το ξεχωριστό για τους πολίτες. Αυτό προκύπτει αν

---

φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε ένωση, σωματείο και συνδικαλιστική οργάνωση, την υγεία, την κοινωνική πρόνοια και τη ερωτική ζωή, καθώς και τα σχετικά με ποινικές διώξεις ή καταδίκες

[67] HUNEID – Αρχικά για το Hungarian eID project. Οι απαιτήσεις του και τα υποστηριζόμενα πρότυπα δημοσιεύτηκαν τον Ιούλιο του 2005, ενώ αναπροσαρμόστηκαν στις αρχές του 2008, προσαρμοζόμενα σύμφωνα με τις απαιτήσεις της Ευρωπαϊκής κάρτας του Πολίτη.

ληφθεί υπόψη η συχνότητα των συναλλαγών των πολιτών με τη δημόσια διοίκηση, η οποία κρίνεται ότι δεν είναι ιδιαιτέρως μεγάλη.

Υπάρχουν όμως κάποιες κατηγορίες χρηστών-πολιτών οι οποίοι έχουνε πολύ μεγαλύτερη συχνότητα συναλλαγής με το δημόσιο τομέα, όπως ενδεικτικά αναφέρονται οι δικηγόροι, οι συμβολαιογράφοι, οι επαγγελματίες του φαρμακευτικού κλάδου κ.τ.λ. Για τις ομάδες προκρίνονται λύσεις συστημάτων οι οποίες αφορούν αποκλειστικά στο δημόσιο τομέα.

Ένα πολύ χαρακτηριστικό παράδειγμα χώρας όπου αναδεικνύεται η ανάμιξη του ιδιωτικού τομέα στη διαχείριση ηλεκτρονικών ταυτοτήτων είναι η Σουηδία. Στη Σουηδία ο δημόσιος τομέας εκμεταλλεύθηκε την ήδη εγκατεστημένη και επιτυχώς λειτουργούσα υποδομή δημοσίου κλειδιού που ήταν διαθέσιμη στους πελάτες των ιδιωτικών τραπεζών, κάτι το οποίο είχε σαν αποτέλεσμα η συχνότητα χρήσης ηλεκτρονικών ταυτοτήτων για υπηρεσίες ηλεκτρονικής διακυβέρνησης από τους πολίτες να είναι μεγαλύτερη στην Σουηδία από ότι σε οποιαδήποτε άλλη χώρα της Ευρώπης[27].

Με την ανάμιξη όμως του ιδιωτικού τομέα στον τομέα της διαχείρισης των ηλεκτρονικών ταυτοτήτων, ανακύπτουν άμεσα ορισμένα θέματα. Πιο συγκεκριμένα τίθεται ένα μείζον θέμα το οποίο σχετίζεται με την προστασία των προσωπικών δεδομένων των πολιτών. Με την ανάμιξη του ιδιωτικού τομέα στις λειτουργίες διαχείρισης των ηλεκτρονικών ταυτοτήτων τα προσωπικά δεδομένα τα οποία συλλέγονται και χρησιμοποιούνται, επαναχρησιμοποιούνται και επεξεργάζονται έξω από το συγκεκριμένο πλαίσιο για το οποίο είχανε συλλεγεί και για το οποίο είχε δοθεί η συγκατάθεση του χρήστη. Αυτό αυτομάτως έρχεται σε αντίθεση με την κείμενη νομοθεσία περί προστασία προσωπικών δεδομένων[68].

Ένα ακόμη θέμα τα οποίο τίθεται σχετίζεται με το πλήθος των προσωπικών δεδομένων τα οποία συλλέγονται και χρησιμοποιούνται προκειμένου να παρασχεθεί μία υπηρεσία. Υφίσταται γενικά ο κίνδυνος να χρησιμοποιηθούν περισσότερα προσωπικά δεδομένα των χρηστών από αυτά τα οποία είναι στην πραγματικότητα απαραίτητα προκειμένου να παρασχεθεί η κάθε διαθέσιμη υπηρεσία. Η διαδικασία όμως αυτή είναι αντίθετη απέναντι στην αρχή της αναλογικότητας[69] η οποία προβλέπει ότι τα δεδομένα τα οποία συλλέγονται θα πρέπει να είναι τα απολύτως αναγκαία για την εκπλήρωση του σκοπού που επιδιώκεται. Το πιο δύσκολο μάλιστα σε αυτή την περίπτωση είναι το γεγονός ότι είναι σχεδόν ανέφικτο να ελεγχθεί στην πράξη η τήρηση του εν λόγω περιορισμού.

[68] Άρθρο 6§1 περίπτωση β' της Οδηγίας 95/46/ΕΚ
[69] Άρθρο 6§1 περίπτωση γ' της Οδηγίας 95/46/ΕΚ

Συνοψίζοντας τις τάσεις οι οποίες υπάρχουν σε Ευρωπαϊκό επίπεδο ως προς την ανάμιξη του ιδιωτικού τομέα στη διαχείριση των ηλεκτρονικών ταυτοτήτων, διακρίνονται δύο κύριες. Πιο συγκεκριμένα:

- Η περίπτωση όπου όλο το σύστημα και οι λειτουργίες διαχείρισής των ηλεκτρονικών ταυτοτήτων ελέγχονται από τον ιδιωτικό τομέα, αλλά αξιοποιούνται και από υπηρεσίες και εφαρμογές του δημόσιου τομέα (eGovernment). Παραδείγματα αποτελούν τα συστήματα αυθεντικοποίησης τα οποία ελέγχονται από εταιρείες του ιδιωτικού τομέα και χρησιμοποιούνται και για συναλλαγές με δημόσιες υπηρεσίες όπως συμβαίνει στην Εσθονία, στη Σουηδία και στην Λιθουανία. Ακόμη στην ίδια κατηγορία ανήκουν ιδιωτικοί πάροχοι πιστοποίησης (ΠΥΠ) οι οποίοι εκδίδουν ψηφιακά πιστοποιητικά τα οποία μπορούν να χρησιμοποιηθούν και για συναλλαγές με το δημόσιο τομέα όπως στο παράδειγμα της Αυστρίας και του Λουξεμβούργου.

- Στη δεύτερη εναλλακτική το σύστημα και οι λειτουργίες διαχείρισης των ηλεκτρονικών ταυτοτήτων ελέγχονται από το δημόσιο τομέα, αλλά χρησιμοποιείται και από υπηρεσίες και εφαρμογές του ιδιωτικού τομέα. Η επιλογή αυτή προκρίνεται κυρίως στις χώρες όπου τις ηλεκτρονικές κάρτες-ταυτότητες τις εκδίδει από δημόσιους φορείς. Την εναλλακτική αυτή τάση την ακολουθούν επίσης αρκετές χώρες με πιο πρόσφατη αυτή της Γερμανίας η οποία ανακοίνωσε ότι από τον Νοέμβριο του 2010, θα εκδώσει μία ηλεκτρονική κάρτα-ταυτότητα η οποία θα μπορεί να χρησιμοποιηθεί τόσο για την πραγματοποίηση συναλλαγών με δημόσιες υπηρεσίες, όσο επίσης και για συναλλαγές με υπηρεσίες του ιδιωτικού τομέα[28].

## 4.3 Κίνδυνοι Ιδιωτικότητας και ανάγκη ταυτοποίησης

Η έννοια της αυθεντικοποίησης με μία ευρύτερη έννοια, θα μπορούσε να οριστεί και ως «η επιβεβαίωση της αναφερόμενης ταυτότητας μίας οντότητας, ή ενός συνόλου παρατηρούμενων χαρακτηριστικών γνωρισμάτων». Επομένως θα πρέπει να γίνει μία διάκριση, μεταξύ των δύο περιπτώσεων:

- Στην πρώτη περίπτωση, η εφαρμογή αυθεντικοποιεί την οντότητα προκειμένου να πιστοποιήσει το κατά πόσον αυτός ή αυτή συγκεντρώνει ορισμένα απαιτούμενα χαρακτηριστικά, όπως
    - Το να είναι ενήλικος/η,
    - Να είναι κάτοικος ορισμένης περιοχής,
    - Το να είναι μία εταιρεία περιορισμένης ευθύνης

Σε αυτές τις περιπτώσεις, δεν είναι αναγκαίο για μία εφαρμογή να γνωρίζει το ποια ακριβώς είναι η κάθε ξεχωριστή οντότητα που τη χρησιμοποιεί. Η εφαρμογή καθορίζει την «κατάσταση» της οντότητας με βάση τα απαιτούμενα χαρακτηριστικά γνωρίσματα και όχι την ταυτότητά της.

- Στην δεύτερη περίπτωση, η εφαρμογή χρειάζεται να αυθεντικοποιήσει την οντότητα εξακριβώνοντας την ακριβή ταυτότητά της, δηλαδή η διαδικασία αυθεντικοποίησης στην περίπτωση αυτή σχετίζεται άμεσα με την ακριβή ταυτοποίηση του ατόμου. Οπότε στη φάση της αυθεντικοποίησης, η εφαρμογή χρειάζεται να διαθέτει αρκετή πληροφορία προκειμένου να επιλέξει μία συγκεκριμένη οντότητα, από ένα σύνολο διαθέσιμων υποψήφιων οντοτήτων (π.χ. ένα συγκεκριμένο άνθρωπο από το σύνολο του γενικού πληθυσμού, ή μία μεμονωμένη επιχείρηση από το σύνολο των νομικών προσώπων).

Έτσι ο έλεγχος μπορεί κάποιες φορές να γίνει:

- Με απλή διαπίστωση κάποιου ποιοτικού χαρακτηριστικού (1ος τρόπος) ή
- Με τον ακριβή προσδιορισμό της ακριβής ταυτότητας μίας οντότητας (2ος τρόπος).

Και στις δύο περιπτώσεις, ο τελικός στόχος θα εξυπηρετούνταν προφανώς με την σύγκριση ορισμένων χαρακτηριστικών από το σύνολο των χαρακτηριστικών τα οποία αναφέρονται σε μία οντότητα.

Η κατάλληλη χρήση του πρώτου συστήματος αποκλείει συχνά[70] τη δυνατότητα εφαρμογής της Οδηγίας για τα προσωπικά δεδομένα (ή την αντίστοιχη μεταφορά της στην εκάστοτε εθνική νομοθεσία), γιατί η πραγματοποιούμενη επεξεργασία των δεδομένων δεν θα επιτρέπει σε ένα συγκεκριμένο υποκείμενο των δεδομένων να ταυτοποιηθεί, κάτι το οποίο αποτελεί προϋπόθεση για την εφαρμογή της Οδηγίας.

[70] Δεν μπορεί να μην ληφθεί υπόψη η περίπτωση όπου η αυθεντικοποίηση ενός ποιοτικού χαρακτηριστικού καταδεικνύει με μοναδικό τρόπο για μία συγκεκριμένη οντότητα. Για παράδειγμα ένα σύστημα διαχείρισης ταυτοτήτων το οποίο απλά επιβεβαιώνει ότι κάποιος είναι ενήλικας και διαμένει σε μία συγκεκριμένη οδό, θα ταυτοποιεί μοναδικά το άτομο στην σπάνια περίπτωση όπου μόνο ένας ενήλικος διαμένει στη συγκεκριμένη οδό. Το παράδειγμα αρκεί προκειμένου να δείξει ότι οποιοδήποτε σύστημα αυθεντικοποίησης το οποίο επιβεβαιώνει μόνο ορισμένα ποιοτικά χαρακτηριστικά, μπορεί να καταλήξει τελικά ένα σύστημα ταυτοποίησης εάν ελεγχθεί ένα κατάλληλο σύνολο ποιοτικών στοιχείων. Για παράδειγμα, κατά τη δοκιμή ενός συστήματος επιδοτήσεων σε μία συγκεκριμένη περιφέρεια όπου μία εταιρεία περιορισμένης ευθύνης καταχωρήθηκε στην κοινότητα Χ μετά την 31 Δεκεμβρίου 2010, μπορεί κάλλιστα να οδηγήσει σε ταυτοποίηση της συγκεκριμένης εταιρείας.

Ωστόσο στην πράξη, οι Ευρωπαϊκές Χώρες χρησιμοποιούν το δεύτερο σύστημα, που προβλέπει ότι για μία υπό αυθεντικοποίηση οντότητα θα πρέπει να παρουσιάζονται και να επιβεβαιώνονται ένα σύνολο από χαρακτηριστικά γνωρίσματα τα οποία είναι αρκετά, ανάλογα με την κάθε υπηρεσία, προκειμένου να είναι ικανή να καθορίσει την ακριβή ταυτότητα της υπό αυθεντικοποίησης οντότητας. Για την όσο το δυνατόν πιο εύκολη επίτευξη του σκοπού της ταυτοποίησης στην περίπτωση αυτή, ορισμένες χώρες χρησιμοποιούν μοναδικά αναγνωριστικά (unique identifiers) με τη χρήση των οποίων μπορεί πολύ εύκολα να ταυτοποιηθεί μονοσήμαντα, έναντι της αναζήτησης του καταλληλότερου σε άλλη περίπτωση συνδυασμού στοιχείων, η επιθυμητή οντότητα.

Το μοναδικό γνώρισμα είναι ένα γνώρισμα ή ένα σύνολο γνωρισμάτων μίας οντότητας τα οποία μπορούν να προσδιορίσουν μοναδικά την οντότητα μέσα σε ένα συγκεκριμένο πλαίσιο». Ο όρος αυτός συχνά παρεξηγείται ως προς το ότι ερμηνεύεται ότι θα πρέπει να ταυτίζεται με ένα συγκεκριμένο αριθμό (όπως ένα εθνικό αριθμό μητρώου, τον αριθμό ΑΦΜ, κ.τ.λ.). Οι αριθμοί αυτοί αποτελούν την πιο κοινή μορφή των μοναδικών αναγνωριστικών, ωστόσο θα πρέπει να γίνει κατανοητό και πως κάθε ικανό μοναδικό σύνολο χαρακτηριστικών γνωρισμάτων το οποίο σχετίζεται με την οντότητα μπορεί να εξυπηρετήσει ακριβώς τον ίδιο σκοπό θα πρέπει να θεωρείται ισάξιο.

Στην πράξη, τα συστήματα ταυτοποίησης έχουν την τάση να επιτρέπουν την χρήση συγκεκριμένων μοναδικών αριθμών αναγνώρισης ως μοναδικά αναγνωριστικά στοιχεία, παρά τη χρήση συνδυασμού πληροφορίας, καθώς οι αριθμοί αυτοί μπορούν να προσφέρουν μεγαλύτερες εγγυήσεις επίτευξης του μονοσήμαντου προσδιορισμού της οντότητας. Είτε έτσι είτε αλλιώς, η πληροφορία η οποία επεξεργάζεται συνιστά προσωπικό δεδομένο από τη στιγμή που αναφέρεται σε φυσικά πρόσωπα.

Ωστόσο η χρήση κάθε μοναδικού αναγνωριστικού παρουσιάζει την πιθανότητα της κατάχρησης, δεδομένου του ότι κάθε μέρος το οποίο μπορεί να έχει πρόσβαση μπορεί ενδεχόμενα να το χρησιμοποιήσει προκειμένου να συνδέσει υπάρχουσα πληροφορία με μία συγκεκριμένη οντότητα, εάν η πληροφορία αυτή περιλαμβάνει το μοναδικό αναγνωριστικό , δίνοντας έτσι τη δυνατότητα να συνδυαστούν πολλά μικρότερα τμήματα πληροφορίας σε ένα μεγαλύτερου περιεχομένου τμήμα πληροφορίας. Αυτό μπορεί πρακτικά να αποτελέσει ένα κίνδυνο όταν ένα μοναδικό αναγνωριστικό γίνει υπερβολικά δημοφιλές, και τείνει να αποτελεί ένα καθιερωμένο αναγνωριστικό τόσο σε εφαρμογές του δημόσιου τομέα όσο και σε εφαρμογές του ιδιωτικού τομέα. Σε αυτές τις περιπτώσεις, ένα πλήθος χωρών θεωρεί ότι ο κίνδυνος διαρροών δεδομένων (στις περιπτώσεις όπου υπάρχει διάσπαρτη τυχαία πληροφορία στο δημόσιο τομέα) καθίσταται σημαντικά υπολογίσιμος, καθώς φορείς του

ιδιωτικού τομέα μπορούν να λάβουν την πληροφορία αυτή και να την συνδυάσουν με άλλη πληροφορία την οποία διαθέτουν και την έχουνε αποκτήσει με νόμιμο τρόπο.

Αντιλαμβανόμενες αυτό τον κίνδυνο, πολλές κυβερνήσεις έχουνε λάβει ενεργά μέτρα (πέραν της εφαρμογής της γενικής νομοθεσίας τους για την προστασία των προσωπικών δεδομένων) προκειμένου ορισμένα ή το σύνολο των μοναδικών αναγνωριστικών τα οποία χρησιμοποιούνται στα πλαίσια της λειτουργίας των υπηρεσιών τους, να υπόκεινται σε επιπρόσθετους μηχανισμούς προστασίας, καθορίζοντας τα αποδεκτά κατά περίπτωση επίπεδα ασφάλειας για κάθε κατηγορία δεδομένων που διακινείται.

## 4.4 Χρήση μοναδικών αναγνωριστικών

Με τον όρο μοναδικά αναγνωριστικά εννοούμε τους κώδικες (αποτελούμενους από χαρακτήρες ή/και αριθμούς) οι οποίοι σχετίζονται υπό τη μορφή πρωτεύοντος κλειδιού στην εγγραφή κάθε διαφορετικής οντότητας (όπως για παράδειγμα ενός πολίτη) και οι οποίοι μπορούν να προσδιορίσουν τον πολίτη μοναδικά την ώρα που κάνει χρήση κάποιων ηλεκτρονικών υπηρεσιών τις οποίες επιθυμεί να χρησιμοποιήσει. Αντίστοιχοι αυτών των κωδικών για την Ελλάδα αποτελούν για κάθε πολίτη ο ΑΜΚΑ για τις υπηρεσίες πρόνοιας και ασφάλισης και ο ΑΦΜ για τις υπηρεσίες οι οποίες σχετίζονται με τις φορολογικές και οικονομικές υποθέσεις του πολίτη ευρύτερα.

Σε όλες τις χώρες της Ευρωπαϊκής Ένωσης προκειμένου να καταστεί δυνατό το «γκρουπάρισμα» των κωδικών οι οποίοι συνοδεύουν μία οντότητα, έχουνε καθιερωθεί ενιαίοι κωδικοί αριθμοί αναφοράς. Παρ' όλα αυτά το πλαίσιο το οποίο διέπει την ύπαρξη τους καθώς και ο τρόπος που μπορούν κατά περίπτωση να εφαρμοστούν στα διάφορα κράτη μέλη διαφέρει σημαντικά.

Οι δύο διαφορετικές προσεγγίσεις οι οποίες υπάρχουν είναι :

**Α)** ***με βάση τη χρήση ενός ενιαίου μοναδικού αναγνωριστικού κωδικού για όλες τις υπηρεσίες (generic national ID number)*** και

***Β) με τη χρήση διαφορετικών μοναδικών αναγνωριστικών ανά υπηρεσία ή κατηγορία υπηρεσιών***.

Στην περίπτωση των ενιαίων μοναδικών αναγνωριστικών, αυτό που επιτυχαίνεται είναι η εύκολη ταυτοποίηση του πολίτη από το σύνολο των υπηρεσιών οι οποίες παρέχουν ηλεκτρονικά τις υπηρεσίες τους, κάτι το οποίο γίνεται μέσω της ταυτοποίησης των στοιχείων του ατόμου μέσω του μοναδικού αναγνωριστικού κωδικού και διασταύρωσης των στοιχείων από τις εμπλεκόμενες υπηρεσίες.

Γίνεται όμως σαφές ότι με την έννοια ότι ένας κωδικός όπως ο προαναφερόμενος καταλήγει να προσδιορίζει μονοσήμαντα κάθε διαφορετικό άτομο, τότε αποτελεί με έναν τελείως συγκεκριμένο τρόπο προσωπικό δεδομένο του ατόμου. Ως εκ τούτου απορρέει ότι αυτά θα πρέπει να τύχουν αντικείμενο επεξεργασίας και αποθήκευσης κάτω από πολύ συγκεκριμένες προϋποθέσεις, σύμφωνα με την Οδηγία για την Προστασία των Προσωπικών Δεδομένων.[71]

Προκειμένου να περιέλθουν οι εθνικές νομοθεσίες εντός των τεθέντων περιορισμών της ως άνω διάταξης ορίζουν στις νομοθεσίες τους, τόσο το πλαίσιο των υπηρεσιών για τις οποίες μπορεί να χρησιμοποιηθεί ο ενιαίος προσδιοριστικός αριθμός, όσο επίσης ορίζουν ότι αυτά θα χρησιμοποιηθούν στα πλαίσια του σκοπού για τον οποίο εκχωρήθηκαν. Από την άλλη σε ορισμένα κράτη-μέλη τίθεται ένα αυστηρό πλαίσιο εντός του οποίου δύναται να χρησιμοποιούνται οι ενιαίοι προσδιοριστικοί αριθμοί και το οποίο περιλαμβάνει κατ' αποκλειστικότητα τις υπηρεσίες του δημόσιου τομέα, αποκλείοντας την με οποιονδήποτε τρόπο χρησιμοποίηση του εν λόγω κωδικού για εμπορική χρήση. Ο περιορισμός αυτός αποτελεί και ένα εν δυνάμει πολύ σημαντικό εμπόδιο στην προσπάθεια που καταβάλλεται σε Ευρωπαϊκό επίπεδο να χρησιμοποιηθούν οι ενιαίοι αυτοί κωδικοί και σε διασυνοριακές συναλλαγές όπου θα απαιτηθεί να ταυτοποιούνται οι πολίτες, καθιστώντας με τον τρόπο αυτό την εν λόγω διαδικασία νομικά πολύπλοκη υπόθεση.

Μοναδικά αναγνωριστικά καθολικής χρήσης χρησιμοποιούνται σε συνήθως σε πιστοποιητικά με θεσμική και τεχνική πρόβλεψη για προστασία από ανέλεγκτη χρήση. Παραδείγματα χωρών οι οποίες διαθέτουν τέτοιου είδους ψηφιακά πιστοποιητικά είναι το Βέλγιο και η Εσθονία οι οποίες τα έχουνε ενσωματώσει στις ηλεκτρονικές ταυτότητες τις οποίες έχουν εισάγει προς χρήση. Παρ' όλα αυτά αν και στη γραμμή της νομιμότητας με βάση την Οδηγία για την προστασία των προσωπικών δεδομένων, η τακτική αυτή κρίνεται πως ίσως και να υπονομεύει την προστασία των προσωπικών δεδομένων στις χώρες αυτές ειδικά απέναντι στο ενδεχόμενο αποκάλυψης και συσχέτισης των μοναδικών αυτών αναγνωριστικών με την φυσική ταυτότητα του χρήστη ως προϊόν κακόβουλης χρήσης.

Παραλλαγή της παραπάνω εκδοχής αποτελεί η τακτική χωρών να διαθέτουν μοναδικά αναγνωριστικά καθολικής χρήσης στις ηλεκτρονικές τους

[71] Άρθρο 7 της Οδηγίας 95/46/ΕΚ

ταυτότητες, χωρίς όμως αυτά να περιλαμβάνουν σημασιολογικές πληροφορίες (semantic information) οι οποίες θα μπορούσαν να οδηγήσουν στην αποκάλυψη της φυσικής ταυτότητας του πολίτη στο ενδεχόμενο κακόβουλης χρήσης. Στην κατηγορία αυτή ανήκουν η Φινλανδία, η Αυστρία και σύντομα και η Τσεχία.

Και στις δύο παραπάνω περιπτώσεις κρίθηκε πως θα έπρεπε να ληφθούν επιπλέον μέτρα ασφάλειας προκειμένου να εξασφαλιστεί η ιδιωτικότητα των χρηστών. Συγκεκριμένα στην Φινλανδική ταυτότητα το αναγνωριστικό (FINUID number) δεν έχει άλλη χρήση πέρα από την ταυτοποίηση του χρήστη διαμέσου της χρήσης της ηλεκτρονικής του ταυτότητας και ως εκ τούτου η δυνατότητα επεξεργασίας του είναι πολύ περιορισμένη. Τέλος στην Αυστριακή ταυτότητα ο προσωπικός αριθμός αναγνώρισης (source PIN) εμφανίζεται στου πάροχους των διαφόρων υπηρεσιών μόνο κρυπτογραφημένος, κάνοντας ως εκ τούτου την προσπάθεια κακόβουλης χρήσης του πρακτικά αδύνατη.

Το θεσμικό πλαίσιο όπως αυτό καθορίζεται ως προς τις βασικές του αρχές από το Σύνταγμα κάθε χώρας, απαγορεύει στην περίπτωση τουλάχιστον δύο χωρών (Γερμανία και Ουγγαρία) την καθιέρωση καθολικού μοναδικού αναγνωριστικού για την ταυτοποίηση των πολιτών[1]. Αυτός ο περιορισμός παρακάμπτεται όμως καθώς μπορεί ναι μεν το Σύνταγμα να μην επιτρέπει καθολικά μοναδικά αναγνωριστικά, αλλά από την άλλη δεν απαγορεύει όμως και τον περιορισμό ενός πολύ μεγάλου υποσυνόλου από το συνολικό πλήθος των διαθέσιμων υπηρεσιών οι οποίες ρητά θα αναφέρονται εντός των κείμενων διατάξεων στις οποίες το εν λόγω αναγνωριστικό θα έχει αποκλειστική χρήση και δυνατότητα επεξεργασίας των προσωπικών δεδομένων των χρηστών που προσδιορίζονται μέσω αυτού.

Μία χώρα η οποία πρόσφατα κλήθηκε να αποφασίσει στο εσωτερικό της για την καθιέρωση ή μη κάποιου καθολικού αναγνωριστικού ήταν η Πορτογαλία. Στην Πορτογαλία σε αντίθεση με το παράδειγμα της Φινλανδίας, δεν καθιερώθηκε ένα ενιαίο αναγνωριστικό, αλλά επελέγη να συσχετισθούν στην ίδια κάρτα όλα εκείνα τα μοναδικά τομεακά αλφαριθμητικά τα οποία προσδιορίζουν ένα πολίτη στο ενιαίο δελτίο της ηλεκτρονικής του ταυτότητας. Τα μοναδικά αυτά τομεακά αναγνωριστικά του κάθε πολίτη στην Πορτογαλία είναι ο αριθμός της ταυτότητας, το αναγνωριστικό για τις φορολογικές υπηρεσίες, το αναγνωριστικό για τις υπηρεσίες πρόνοιας και κοινωνικής ασφάλειας και τέλος το αναγνωριστικό για τις υπηρεσίες υγείας.

Οι ίδιες επιφυλάξεις υφίστανται και για την επιλογή η οποία προβλέπει τη χρήση συνθηματικών για την πραγματοποίηση της ταυτοποίησης των πολιτών (username / authentication systems), καθώς η χρήση συγκεκριμένου συνθηματικού πρόσβασης από κάθε πολίτη, μπορεί να τον προσδιορίσει κατά μοναδικό τρόπο, ενώ ακόμη η εν λόγω μέθοδος ταυτοποίησης δεν αποτελεί μέθοδο η οποία να διασφαλίζει την ασφάλεια και την προστασία της

ιδιωτικότητας και επομένως δεν είναι κατάλληλα για υπηρεσίες ηλεκτρονικής διακυβέρνησης επιπέδου 3 και πάνω[3].

Οι προσεγγίσεις που αναλύθηκαν παραπάνω αποτελούν τις εναλλακτικές οι οποίες εφαρμόζονται στις διάφορες χώρες με σκοπό την προστασία της ιδιωτικότητας των πολιτών στα όρια του πλαισίου που καθορίζει η Οδηγία 1995/46/ΕC σχετικά με τη χρήση μοναδικών αναγνωριστικών. Όμως οι κατά περίπτωση ερμηνείες και επιλογές οι οποίες έχουνε γίνει στα πλαίσια των κρατών μελών της ΕΕ διαφέρουν πολύ ως προς τη χρησιμοποίηση μοναδικών αναγνωριστικών τα οποία σε άλλες περιπτώσεις εισάγονται προς εξυπηρέτηση του εν λόγω σκοπού της ταυτοποίησης ενώ σε άλλες χώρες χρησιμοποιούνται αναγνωριστικά τα οποία ήδη υφίστανται από πριν. Από την άλλη αναφέρθηκαν περιπτώσεις αναγνωριστικών τα οποία μπορούν να χρησιμοποιηθούν μόνο μέσα στο συγκεκριμένο πλαίσιο και για το σκοπό που εκχωρήθηκαν και αναγνωριστικών που ελέγχονται από τον ιδιωτικό τομέα. Έτσι γίνεται εύκολα αντιληπτό ότι η πρακτική της χρησιμοποίησης ενός καθολικού μοναδικού αναγνωριστικού για την ταυτοποίηση των πολιτών στα κράτη μέλη της ΕΕ, δεν αποτελεί κοινή πρακτική.

## 4.5 Χρήση έγκυρων μητρώων και συναίνεση του πολίτη

Ένας άλλος τρόπος ο οποίος μπορεί να χρησιμοποιηθεί προκειμένου να καταστεί εφικτή η ταυτοποίηση των πολιτών, χωρίς την ύπαρξη μοναδικού αναγνωριστικού, είναι μέσω της χρήσης επίσημων μητρώων τα οποία διαθέτουνε στοιχεία για κάθε πολίτη. Τα μητρώα αυτά δημιουργούνται και στη συνέχεια διαχειρίζονται από δημόσιες υπηρεσίες οι οποίες τα αναπτύσσουν προκειμένου να έχουνε κάποιο αλφαριθμητικό ως κωδικό αριθμό αναφοράς για κάθε συναλλασσόμενο πολίτη. Όπως προαναφέρθηκε τα μητρώα σε κάποιες περιπτώσεις προκύπτουν με βάση τις συναλλαγές τις οποίες πραγματοποιεί ο κάθε διοικούμενος και έτσι μπορούν να διαθέτουν μία πλειάδα στοιχείων ανάλογα με το είδος της συναλλαγής το οποίο είχε με την υπηρεσία ο διοικούμενος και το σκοπό που εξυπηρετούν.

Αυτό το οποίο ενδιαφέρει όμως σε αυτή την περίπτωση είναι η ύπαρξη ενός «μέτρου» το οποίο θα καθορίζει εάν τα προσωπικά δεδομένα τα οποία υπάρχουν για κάθε διοικούμενο είναι τέτοια ως προς την «ποιότητα» και την «εγκυρότητα» τους ώστε να μπορούν να χρησιμοποιηθούν για να μπορεί να προσδιοριστεί μονοσήμαντα ο κάθε διοικούμενος.

Τα στοιχεία αυτά θα πρέπει να παρέχονται από μία αρχή η οποία θα μπορεί να επαληθεύει με μοναδικό και έγκυρο τρόπο τα στοιχεία τα οποία διαθέτει για τον κάθε πολίτη, προσέγγιση η οποία είναι γνωστή ως αρχή της

έγκυρης πηγής[72] και το οποίο συνεπάγεται ότι επιμέρους προσωπικά δεδομένα τα οποία υφίστανται και είναι ήδη καταγεγραμμένα για τον πολίτη σε ένα έγκυρο μητρώο, θα μπορούν να χρησιμοποιηθούν αυτόματα από κάθε άλλη υπηρεσία η οποία θα χρειαστεί να τα χρησιμοποιήσει, χωρίς να μπαίνει κάθε φορά ο πολίτης στη διαδικασία του να τα προσκομίζει εκ νέου σε κάθε δημόσια υπηρεσία η οποία τα απαιτεί προκειμένου να ολοκληρώσει μία διοικητική διαδικασία.

Στον αντίποδα αυτής τη προσέγγισης βρίσκεται η πολιτοκεντρική (**citizen centric**) βάσει τη οποίας απαιτείται η ρητή συγκατάθεση του πολίτη (user consent)[73] σχετικά με το ποια και πόσα από τα προσωπικά του δεδομένα επιθυμεί ο ίδιος να χρησιμοποιούνται προκειμένου να ταυτοποιηθεί κάθε φορά που χρησιμοποιεί κάποια δημόσια υπηρεσία. Η συγκατάθεσή του θα πρέπει να είναι ελεύθερη, ρητή και ειδική δήλωση βούλησης, η οποία να εκφράζεται με σαφή τρόπο, για την οποία το άτομο θα πρέπει να έχει πλήρη επίγνωση και με την οποία το άτομο ως υποκείμενο και φορέας των προσωπικών δεδομένων, αφού προηγουμένως ενημερωθεί, δέχεται να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν[29].

Όλα τα κράτη μέλη διαθέτουν τέτοια έγκυρα δημόσια μητρώα, τα οποία στην πιο απλή μορφή τους μπορεί να είναι τα δημοτολόγια της κάθε περιοχής ή και όχι μόνο. Στην Ελλάδα ένα τέτοιου είδους έγκυρο μητρώο είναι το μητρώο το οποίο διατηρεί η Γενική Γραμματεία Πληροφορικών Συστημάτων του Υπουργείου Οικονομικών στα πλαίσια λειτουργίας του Ο.Π.Σ. TAXIS. Στα μητρώα αυτά οι πολίτες εγγράφονται είτε με την γέννηση τους ή όταν έρθουν σε κάποια ηλικία, είτε σε κάποια άλλη περίπτωση όταν θα χρειαστεί να συναλλαγούν με τις υπηρεσίες αυτές. Οι υπηρεσίες αυτές άμα τη δημιουργία των μητρώων αυτών είναι επιπλέον υποχρεωμένες, μέσω των διαχειριστών τους, βάσει της κείμενης νομοθεσίας να φροντίζουν για την εγκυρότητα των στοιχείων τα οποία περιλαμβάνονται μέσα στα μητρώα τους[74].

Όσο όμως και αν προκύπτει σχετική υποχρέωση για επικαιροποίηση των περιεχόμενων στοιχείων στα εν λόγω μητρώα, αυτή δεν θα πρέπει να θεωρείται καθόλου δεδομένο ότι υφίσταται κιόλας.

Στα μητρώα αυτά υπάρχουν διαπιστωμένα λάθη και παραλήψεις σε αρκετά κράτη μέλη ανάμεσα στα οποία η Ελλάδα, η Τσεχία και η Πολωνία[3]. Προκειμένου να καταστεί δυνατή η χρησιμοποίηση των μητρώων αυτών ως **«έγκυρων» πηγών** αναφοράς καταβάλλονται όλες οι δυνατές προσπάθειες ούτως ώστε τα οποιαδήποτε υπάρχοντα προβλήματα επικαιροποίησης των στοιχείων να πάψουν να υφίστανται.

[72] Authentication source principle
[73] Βλ. σχετικά Άρθρο 7(α) της Οδηγίας 95/46/ΕΚ
[74] Άρθρο 6(δ) της Οδηγίας 95/46/ΕΚ

Η αρχή έγκυρης πηγής και η αρχή των έγκυρων μητρώων τυγχάνει όλο και μεγαλύτερης αποδοχής μεταξύ των κρατών μελών της ΕΕ[26]. Η ανωτέρω αρχή είναι θεσμικά κατοχυρωμένη σε μόλις 6 χώρες (Βέλγιο, Φινλανδία, Εσθονία, Γαλλία, Ιρλανδία και Λιθουανία). Σε άλλες 8 χώρες πραγματοποιούν χρήση τέτοιων έγκυρων μητρώων άτυπα χωρίς ακόμη να την έχουν θεσμοθετήσει (Βρετανία, Λουξεμβούργο, Ολλανδία, Πορτογαλία, Σλοβενία, Ισπανία και Σουηδία), ενώ 2 χώρες αναφέρουν ότι σκοπεύουν να χρησιμοποιήσουν έγκυρα μητρώα προκειμένου να ταυτοποιούν τους πολίτες τους (Βουλγαρία και Μάλτα).

Από την άλλη η «πολιτοκεντρική» προσέγγιση όπως έχει ήδη αναπτυχθεί η οποία απαιτεί την ρητή συγκατάθεση του πολίτη, μοιάζει να είναι σαφώς προτιμητέα σύμφωνα με το πνεύμα της Οδηγίας ως προς την προστασία των προσωπικών δεδομένων των χρηστών. Στα πλαίσια όμως της καθιέρωσης της ηλεκτρονικής διακυβέρνησης στο σύνολο των χωρών της ΕΕ, όσες χώρες υιοθετούν την αρχή της έγκυρης πηγής, φροντίζουν να καθιερώνουν τον αντίστοιχο θεσμικό πλαίσιο στα πλαίσια του οποίου θα είναι δυνατή η χρήση των έγκυρων μητρώων και της επακόλουθης επεξεργασίας των προσωπικών τους δεδομένων χωρίς την συναίνεση του χρήστη.[75]

[75] Δράσεις οι οποίες τυποποιούνται κάτω από τους όρους: National Register Acts, Identity Cards Acts, eGovernment Acts)

# 5. ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΠΟΛΙΤΙΚΕΣ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ

Προκειμένου να μπορέσει να ταυτοποιηθεί ένας πολίτης, θα πρέπει προηγουμένως να έχει αυθεντικοποιηθεί με κάποιο τρόπο μέσω κάποιου συστήματος αυθεντικοποίησης.

Οι δύο εναλλακτικές οι οποίες μπορούνε να χρησιμοποιηθούνε περιλαμβάνουνε την αυθεντικοποίηση μέσω κάποιας υποδομής δημοσίου κλειδιού (PKI), ενώ ένας άλλος τρόπος είναι μέσω συστημάτων τα οποία χρησιμοποιούνε συνθηματικά.

Επιπλέον ανάλογα με την μέθοδο αυθεντικοποίησης που χρησιμοποιείται το κάθε κράτος καθορίζει ένα επίπεδο εμπιστοσύνης ως προς το υποσύνολο των ηλεκτρονικών υπηρεσιών του τις οποίες είναι διατεθειμένο να προσφέρει στους πολίτες του με βάση τον δεδομένο τρόπο αυθεντικοποίησης[76].

## *5.1 Συστήματα Δημοσίου Κλειδιού (PKI)*

Η αυθεντικοποίηση οντοτήτων (φυσικών και νομικών προσώπων) αποτελεί την πιο διαδεδομένη μέθοδο αυθεντικοποίησης στην Ευρώπη. Συνολικά οι 29 από τις 32 χώρες έχουν υιοθετήσει τέτοια συστήματα αυθεντικοποίησης βασισμένα σε υποδομές δημοσίου κλειδιού (PKI).

Στην ενότητα αυτή θα αναλυθεί το ποιες χώρες έχουνε αναπτύξει κάποιας μορφής ενός PKI συστήματος προκειμένου να αυθεντικοποιήσουνε διάφορες ομάδες οντοτήτων ως βασικό μέρος των πολιτικών τους στο θέμα της διαχείρισης ηλεκτρονικών ταυτοτήτων.

Έχει γίνει μία διάκριση μεταξύ των συστημάτων PKI που ελέγχονται από το δημόσιο τομέα και αυτών όπου έχουμε συνέργειες του δημόσιου με φορείς του ιδιωτικού τομέα. Η διάκριση έγκειται στην κατανομή της λειτουργίας της αρχής του έγκυρου μητρώου η οποία επαληθεύει την ταυτότητα της οντότητας που αιτείται το διακριτικό PKI. Θα πρέπει να σημειωθεί ότι είναι απολύτως πιθανό (και στην πράξη πολύ σύνηθες ως πρακτική) ένα σύστημα το οποίο κατηγοριοποιείται ως «ελεγχόμενο από το δημόσιο τομέα» στους πίνακες που ακολουθούν, αλλά παρ' όλα αυτά η αρχή αυθεντικοποίησης στο σύστημα αυτό να είναι μία οντότητα του ιδιωτικού τομέα.

[76] Το ελληνικό κείμενο όπου ρυθμίζεται το αντίστοιχο ζήτημα, είναι το Ελληνικό Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης και Πρότυπα Διαλειτουργικότητας ή άλλως «Πλαίσιο Ψηφιακής Αυθεντικοποίησης», έκδοση 2.00, Μάιος 2008, όπου στη σελίδα 28 περιγράφονται τα επίπεδα εμπιστοσύνης των διαφόρων υπηρεσιών.

Προκειμένου να προσδιορισθεί το πεδίο εφαρμογής του κάθε συστήματος, καταγράφεται επίσης στους πίνακες το κατά πόσο ή όχι τα PKI συστήματα είναι προσπελάσιμα και από φορείς του ιδιωτικού τομέα, όπως για παράδειγμα εάν το hardware ή middleware έχει σχεδιασθεί έχοντας κατά νου την χρήση από φορείς του ιδιωτικού τομέα, ή κατά πόσο το PKI σύστημα σχεδιάστηκε για χρήση μόνο από μία ή περισσότερες εξειδικευμένες εφαρμογές ηλεκτρονικής διακυβέρνησης.

### 5.1.1. Εγκατεστημένα PKI συστήματα που ελέγχονται αποκλειστικά από Δημόσιους Φορείς

| Χώρα | Περιγραφή | Εκδούσα Αρχή | Προσβάσιμο στον ιδιωτικό τομέα |
|---|---|---|---|
| **Βέλγιο** | Πιστοποιητικό αυθεντικοποίησης στο δελτίο eID | Παρέχεται μέσω των Δημοτικών και Κοινοτικών Αρχών | Ναι, μέσω ελεύθερα διακινούμενου λογισμικού |
| **Γαλλία** | Πιστοποιητικό αυθεντικοποίησης στην κάρτα Daily Life | Τοπική Αυτοδιοίκηση | Όχι |
| **Ελλάδα** | Δίκτυο «ΣΥΖΕΥΞΙΣ» για τους δημοσίους υπαλλήλους χρησιμοποιώντας πιστοποιητικό υπογραφής, υλοποιημένο σε έξυπνες κάρτες | Το αρμόδιο Υπουργείο, ανάλογα με το δημόσιο υπάλληλο | Όχι |
| | Δίκτυο του «Police On Line» για την αστυνομία, χρησιμοποιώντας πιστοποιητικό υπογραφής, υλοποιημένο με έξυπνες κάρτες | Υπουργείο Προστασίας του Πολίτη | Όχι |
| **Εσθονία** | Πιστοποιητικό αυθεντικοποίησης στο δελτίο eID | Επιτροπή Ιθαγένειας και Μετανάστευσης (CMB)[77] | Ναι |
| **Ισλανδία** | Soft Πιστοποιητικά Αυθεντικοποίησης | Ορισμένες διοικήσεις φορέων, όπως η Εφορία και η Δ/νση Τελωνείων. Στο μέλλον, τα δελτία τα οποία θα εκδίδονται από τις τράπεζες θα περιλαμβάνουν πιστοποιητικά τόσο υπογραφής όσο και αυθεντικοποίησης | Ναι |

[77] CMB : Citizenship and Migration Board

| | | | |
|---|---|---|---|
| **Ισπανία** | Πιστοποιητικό αυθεντικοποίησης στην στο εθνικό eID | Τεχνικό Γραφείο έκδοσης δελτίων ταυτότητας[78] | Ναι (μερικές τράπεζες) |
| **Ιταλία** | Ψηφιακό / Αναγνωρισμένο πιστοποιητικό στο δελτίο eID | Μέσω των Δήμων | Ναι |
| | Ψηφιακό / Αναγνωρισμένο πιστοποιητικό στην κάρτα CNS | Εξαρτάται από την τοπική αρχή που έχει αναλάβει την έκδοση της κάρτας | Όχι |
| | Ψηφιακό / Αναγνωρισμένο πιστοποιητικό στην κάρτα CMD[79] | Την αρμόδια κρατική υπηρεσία (ανάλογα με την κάρτα: π.χ. Υπουργείο Άμυνας) | Όχι |
| **Κροατία** | Πιστοποιητικό αυθεντικοποίησης σε smart card της FINA[80] | Μέσω της υπηρεσίας Οικονομικών της Κροατίας | Ναι |
| | Πιστοποιητικό αυθεντικοποίησης στην κάρτα υγείας CIHI[81] | Κροατικό Ινστιτούτο Υγείας και Ασφάλισης | Όχι |
| **Λετονία** | Ψηφιακά / Αναγνωρισμένα πιστοποιητικά σε έξυπνες κάρτες του ιδιωτικού τομέα | Από τις τοπικές εφορίες – Απαιτείται διαβατήριο για να γίνει η αίτηση | Ναι |
| **Λιθουανία** | Πιστοποιητικό αυθεντικοποίησης στο δελτίο eID | Μέσω κοινοτήτων | Ναι |
| | Πιστοποιητικό αυθεντικοποίησης στο δελτίο eID των δημοσίων υπαλλήλων | Την αρμόδια κρατική υπηρεσία (ανάλογα με την κάρτα) | Ναι |
| **Λιχτενστάιν** | Πιστοποιητικό Αυθεντικοποίησης σε δελτία eID | Μέσω κοινοτήτων | Ναι |
| **Μάλτα** | Μη αναγνωρισμένα πιστοποιητικά ψηφιακής υπογραφής | Η κυβέρνηση της Μάλτας[82] | Ναι |
| **Ουγγαρία** | Κάρτες εκπαίδευσης που εμπεριέχουν πιστοποιητικά υπογραφής (μόνο για καθηγητές και διοικητικό προσωπικό και όχι για μαθητές) | Υπουργείο Παιδείας | Όχι |
| **Πορτογαλία** | Πιστοποιητικό αυθεντικοποίησης στο δελτίο eID | INCM[83] | Ναι |
| **Σλοβενία** | Αναγνωρισμένο πιστοποιητικό ψηφιακής υπογραφής που περιλαμβάνει ένα μοναδικό αναγνωριστικό συνδεδεμένο σε μια βάση | Αρχή Πιστοποίησης του Υπουργείου Δημόσιας Διοίκησης | Ναι |

[78] Officina Técnica del DNI electrónico
[79] Κάρτα δημοσίων υπαλλήλων
[80] FINA (Financijska agencija) eID card
[81] CIHI : Croatian Institute for Health Insurance
[82] http://repository.ca.gov.mt
[83] INCM : Imprensa Nacional Casa de Moeda (Εθνικό Νομισματοκοπείο της Πορτογαλίας), βλ. http://www.incm.pt/site/home.html

| | | | |
|---|---|---|---|
| | δεδομένων | | |
| **Τουρκία** | Soft πιστοποιητικά αυθεντικοποίησης | Υπουργείο Δικαιοσύνης | Όχι |
| **Φινλανδία** | Πιστοποιητικό αυθεντικοποίησης στο ηλεκτρονικό δελτίο eID[84] | Μέσω τοπικών αστυνομικών αρχών | Ναι |

**Πίνακας 10: PKI συστήματα ελεγχόμενα αποκλειστικά από Δημόσιους Φορείς**

### 5.1.2. Εγκατεστημένα PKI συστήματα που ελέγχονται από συμπράξεις δημόσιου-ιδιωτικού τομέα

| Χώρα | Περιγραφή | Εκδούσα Αρχή | Προσβάσιμο στον Ιδιωτικό τομέα |
|---|---|---|---|
| **Αυστρία** | Αναγνωρισμένο πιστοποιητικό υπογραφής στην Κάρτα του Πολίτη | Εξαρτάται από την υλοποίηση της κάρτας του πολίτη | Ναι. Η Κάρτα του Πολίτη μπορεί επίσης να εκδοθεί από συνεργάτες που ανήκουν στον ιδιωτικό τομέα. |
| **Βέλγιο** | Πιστοποιητικά υπογραφής, αναγνωρισμένα και μη αναγνωρισμένα | Αναγνωρισμένοι πάροχοι υπηρεσιών πιστοποίησης, CSPs (όλοι Βελγικοί) | Ναι |
| **Βουλγαρία** | Ψηφιακή υπογραφή μέσω αναγνωρισμένων soft πιστοποιητικών | Καταχωρημένοι CSPs στην Επιτροπή Επικοινωνιών της Βουλγαρίας | Ναι |
| **Γαλλία** | Πιστοποιητικό Αυθεντικοποίησης στην Κάρτα Υγείας[85] | Ασφαλιστικοί Φορείς του κλάδου Υγείας. | Ναι |
| **Δανία** | Προηγμένη ψηφιακή υπογραφή OCES (soft πιστοποιητικό, το οποίο μπορεί να συμπεριληφθεί σε κάποια hardware υποδομή στο μέλλον) | Η TDC[86], ένας αναγνωρισμένος ιδιωτικός CSP. Το πιστοποιητικό εμπεριέχει ένα μοναδικό αναγνωριστικό το οποίο συνδέεται με τον εθνικό αριθμό μητρώου[87] στην περίπτωση των φυσικών προσώπων, αλλά ο αριθμός CPR δεν αποκομίζεται χωρίς έννομη εντολή | Ναι |
| **Εσθονία** | Mobile-PKI/ Mobile-ID | Σύστημα PKI που βασίζεται σε κινητά τηλέφωνα | Ναι |
| **Ηνωμένο Βασίλειο** | Αναγνωρισμένα soft πιστοποιητικά υπογραφής | Εμπορικό Επιμελητήριο Βρετανίας και Equifax[88] | Ναι |
| **Ισλανδία** | Πιστοποιητικά Αυθεντικοποίησης κάτω | Στην παρούσα φάση μόνο | Ναι |

[84] Finland eID (FINEID)
[85] Carte Vitale
[86] http://tdc.com/
[87] CPR: Det Centrale Personregiste – Κεντρικό Μητρώο Πολιτών Δανίας
[88] http://www.equifax.co.uk/

| | | | |
|---|---|---|---|
| | από μία κοινή Ισλανδική ιεραρχία ρίζας[89] | ένας CSP έχει εξουσιοδοτηθεί να εκδίδει πιστοποιητικά[90] | |
| **Ισπανία** | Αναγνωρισμένα πιστοποιητικά υπογραφής, είτε soft είτε σε έξυπνες κάρτες – χρήση μοναδικού αριθμού αναγνώρισης | Διαπιστευμένοι και αναγνωρισμένοι CSPs | Ναι |
| **Λιχτενστάιν** | Πιστοποιητικά που εκδίδονται από την A-Trust[91] για χρήση στα πλαίσια της δημόσιας διοίκησης | Ο Αυστριακός CSP A-SIT | Ναι |
| **Λιθουανία** | Αναγνωρισμένα πιστοποιητικά υπογραφής, είτε soft είτε σε έξυπνες κάρτες | Τρεις αναγνωρισμένοι CSPs είναι προς το παρόν διαθέσιμοι στην Λιθουανία | Ναι |
| | Mobile-PKI/Mobile-ID | Σύστημα PKI που βασίζεται σε κινητά τηλέφωνα | Ναι |
| **Νορβηγία** | Πιστοποιητικά Αυθεντικοποίησης και υπογραφής (αναγνωρισμένα και μη αναγνωρισμένα) εκδίδονται από ιδιωτικούς CSPs. Μπορούν να αποθηκευτούν σε smart cards ή στην πλευρά του server | Ένας αριθμός συνεργατών του ιδιωτικού τομέα, συμπεριλαμβανομένων αρκετών τραπεζών[92] | Ναι |
| **Ολλανδία** | Ψηφιακά Πιστοποιητικά[93] | Ένας αριθμός ιδιωτικών CSPs | Ναι |
| **Πολωνία** | Αναγνωρισμένα πιστοποιητικά υπογραφής, είτε soft είτε σε έξυπνες κάρτες | Τρεις αναγνωρισμένες Αρχές Πιστοποίησης: η Certum[94], η Sigillum[95] και η Szafir[96] | Ναι |
| **Πορτογαλία** | Αναγνωρισμένα soft πιστοποιητικά υπογραφής για δικηγόρους, νομικούς συμβούλους ή συμβολαιογράφους | Ο Δικηγορικός Σύλλογος[97], ο Σύνδεσμος Νομικών Συμβούλων[98] και ο Σύνδεσμος Συμβολαιογράφων[99] | Ναι |
| **Ρουμανία** | Αναγνωρισμένα και μη αναγνωρισμένα soft πιστοποιητικά υπογραφής | Ιδιωτικοί CSPs[100] | Ναι |
| **Σλοβακία** | Αναγνωρισμένα soft πιστοποιητικά υπογραφής | Διαπιστευμένοι CSPs του ιδιωτικού τομέα | Ναι |
| **Σλοβενία** | Αναγνωρισμένο πιστοποιητικό υπογραφής, το οποίο συνήθως εμπεριέχει ένα επίσημο αναγνωριστικό (όπως ο αριθμός φορολογικού μητρώου) | Τρεις διαπιστευμένοι CSPs του ιδιωτικού τομέα | Ναι |
| **Σουηδία** | Προηγμένα πιστοποιητικά, είτε soft είτε | Πιστοποιητικά εκδίδονται | Ναι |

[89] Islandsrot, Υπάρχει δηλαδή ένα πιστοποιητικό δημοσίου κλειδιού διαθέσιμο το οποίο ονομάζεται root certificate και μπορεί να χρησιμοποιηθεί προκειμένου να ταυτοποιηθεί η Root Certificate Authority, η οποία έχει πιστοποιήσει τον CSP βλ. http://www.islandsrot.is

[90] Auokenni hf

[91] A-Trust: Αυστριακή Εταιρεία η οποία ιδρύθηκε από Αυστριακές τράπεζες, με σκοπό να εξασφαλίσει την ασφάλεια του ηλεκτρονικού εμπορίου στην Αυστρία παρέχοντας ασφαλείς ηλεκτρονικές υπογραφές και ασφαλείς ηλεκτρονικές συναλλαγές

[92] Κυρίως η εταιρεία Buypass (http://www.buypass.no/) και μέλη του γκρουπ BankID

[93] http://www.pkioverheid.nl/

[94] http://www.certum.pl

[95] http://www.sigillum.pl.com.pl

[96] http://www.kir.com.pl

[97] Ordem dos Advocados

[98] Câmara dos Solicitadores

[99] Ordem dos Notários

[100] Οι Trans sped, Certsign, Digisign και Internet DomReg

| | | | |
|---|---|---|---|
| | hard. Δύο ξεχωριστά πιστοποιητικά σε κάθε διακριτικό, ένα για αυθεντικοποίηση και ένα για υπογραφή. | από συνεργάτες του ιδιωτικού τομέα[101]. Το Δελτίο Ταυτότητας εκδίδεται από την Αστυνομία (έχει αναπτυχθεί, αλλά δεν είναι πλήρως λειτουργικό για ηλεκτρονική χρήση) | |
| **Τουρκία** | Αναγνωρισμένα πιστοποιητικά υπογραφής σε έξυπνες κάρτες | Τέσσερεις διαπιστευμένοι CSPs | Ναι |
| | Mobile-PKI/ Mobile-ID | PKI σύστημα βασισμένο σε κινητά τηλέφωνα από την Turkcell | Ναι |
| **Τσεχία** | Ψηφιακή υπογραφή μέσω αναγνωρισμένων πιστοποιητικών (είτε soft (το πιο σύνηθες) είτε κατ' εξαίρεση με έξυπνες κάρτες) | Αναγνωρισμένοι CSPs. Το πιστοποιητικό περιλαμβάνει τον αριθμό μητρώου του ασφαλιστικού φορέα, ο οποίος χρησιμοποιείται για λόγους αυθεντικοποίησης | Ναι |
| | Υπογραφή που χρησιμοποιεί αναγνωρισμένα πιστοποιητικά (είτε soft (το πιο σύνηθες) είτε κατ' εξαίρεση με έξυπνες κάρτες) | Αναγνωρισμένοι CSPs. Η ψηφιακή υπογραφή χρησιμοποιείται σε ηλεκτρονικά έγγραφα που περιέχουν και άλλα σημαντικά στοιχεία αναγνώρισης, όπως ο ΑΔΤ, τα οποία έπειτα χρησιμοποιούνται για λόγους πιστοποίησης | Ναι |

**Πίνακας 11: PKI συστήματα που ελέγχονται από συμπράξεις δημόσιου-ιδιωτικού τομέα**

### 5.1.3 – Συμπεράσματα για συστήματα αυθεντικοποίησης βασισμένα σε PKI

Με βάση τους παραπάνω πίνακες, μπορούν να εξαχθούν τα ακόλουθα συμπεράσματα:

Στις μισές περίπου από το σύνολο των παραπάνω χωρών που διαθέτουν υποδομές δημοσίου κλειδιού, τη διαχείριση των σχετικών λειτουργιών και υπηρεσιών την ασκούν με αποκλειστικό τρόπο δημόσιοι φορείς σε κεντρικό ή τοπικό επίπεδο, ενώ κάποιες από τις υπόλοιπες παρέχουν τις εν λόγω υπηρεσίες από σχήματα τα οποία έχουνε καταρτίσει με συμπράξεις δημοσίου και ιδιωτικού τομέα, ή μόνο του ιδιωτικού τομέα (public/private partnerships), μέσω της παράλληλης εκχώρησης συγκεκριμένων αρμοδιοτήτων.

Ανάμεσα στις χώρες οι οποίες έχουνε υιοθετήσεις τέτοιου τύπου PKI συστήματα είναι το Βέλγιο, η Εσθονία, η Φινλανδία, η Ιταλία, η Λιθουανία και η Ισπανία. Στις χώρες αυτές όπως έχει ήδη αναφερθεί έχουνε εκδοθεί ηλεκτρονικές κάρτες-

[101] Μία κοινοπραξία από 8 τράπεζες οι οποίες συνθέτουν το BankID, η τράπεζα Nordea, η εταιρία τηλεπικοινωνιών Telia Sonera και η εταιρία πληροφορικής Steria

ταυτότητες στις οποίες την ευθύνη αυθεντικοποίησης έχουν αποκλειστικά δημόσιοι φορείς. Σε άλλες τρεις χώρες (Αυστρία, Ολλανδία και Σουηδία) η διαχείριση των συστημάτων αυθεντικοποίησης πραγματοποιείται από ιδιωτικούς παρόχους υπηρεσιών πιστοποίησης (ΠΥΠ), κατόπιν σχετικής εξουσιοδότησης των εν λόγω κρατών μελών.

Στις περισσότερες περιπτώσεις μέσα στην ίδια ηλεκτρονική κάρτα-ταυτότητα συνυπάρχουν δύο ψηφιακά πιστοποιητικά από τα οποία το ένα χρησιμεύει για την αυθεντικοποίηση ενώ το άλλο για την ηλεκτρονική υπογραφή από το χρήστη. Αυτή την τακτική δεν την ακολουθεί όμως η Αυστρία όπου το ένα και μοναδικό ψηφιακό πιστοποιητικό το οποίο υπάρχει στην ηλεκτρονική ταυτότητα χρησιμεύει για ηλεκτρονική υπογραφή, αλλά είναι και εκείνο βάσει του οποίου αυθεντικοποιείται ο χρήστης.

## 5.2 Χρήση συνθηματικών (username/password)

Η άλλη εναλλακτική πολιτική αυθεντικοποίησης, αναφέρεται στην υιοθέτηση συστημάτων αυθεντικοποίησης μέσω συνθηματικών. Και αυτή η εναλλακτική τυγχάνει ευρείας αποδοχής μεταξύ των κρατών.

Στον πίνακα που ακολουθεί παρουσιάζονται τα συστήματα αυτού του είδους τα οποία βρίσκονται σε χρήση σε Ευρωπαϊκές χώρες. Σε κάθε περίπτωση αναφέρεται το είδος του login password τα οποία κατηγοριοποιούνται ως εξής:

- ✓ Single Factor με χρήση username/password
- ✓ Multifactor με χρήση password list
- ✓ Multifactor με χρήση Password based PIN calculator
- ✓ Multifactor με χρήση mobile phone

Ακόμη διακρίνεται το ποιος εκδίδει τα ζεύγη των διαπιστευτηρίων[102], και/ή το διακριτικό, και το κατά πόσο ή όχι το σύστημα είναι προσβάσιμο σε φορείς του ιδιωτικού τομέα. Το τελευταίο βέβαια είναι πολύ πιο σπάνιο, και αφορά κυρίως στην περίπτωση όπου το σύστημα ελέγχεται εξ' ολοκλήρου από οντότητες του ιδιωτικού τομέα.

Οι ακόλουθες χώρες έχουνε αναπτύξει κάποια μορφή συστήματος login/password προκειμένου να αυθεντικοποιούν ομάδες οντοτήτων, ως ένα βασικό μέρος της eIDM πολιτικής τους. Περιγράφονται μόνο συστήματα τα οποία είναι λειτουργικά και όχι συστήματα τα οποία βρίσκονται σε στάδιο σχεδιασμού.

[102] credentials

| Χώρα | Περιγραφή | Οντότητα που εκδίδει το username/password ή το διακριτικό παραγωγής κωδικών | Προσβάσιμο στον ιδιωτικό τομέα; |
|---|---|---|---|
| **Βέλγιο** | Multifactor – password list (ομοσπονδιακό διακριτικό: με τη χρήση username, password και τυχαίου αλφαριθμητικού από διακριτικό σε έντυπη μορφή | Βελγική Ομοσπονδιακή Κυβέρνηση μέσω του ομοσπονδιακού διαδικτυακού portal | Όχι |
| **Ελλάδα** | Single factor (username/password) στο σύστημα TAXISnet, βασίζεται σε on-line ταυτοποίηση με τη χρήση του Α.Φ.Μ. και των βασικών στοιχείων ταυτότητας του ατόμου (Επώνυμο, Όνομα, και Πατρώνυμο). Απαιτείται πρότερη ταυτοποίηση στις κατά τόπους Δ.Ο.Υ. από την 6/12/2010[103] | Κατά τόπους Δ.Ο.Υ. | Όχι |
| | Single factor (username/password) E-KEP platform, βασισμένη στην on-line ταυτοποίηση[104] | Κέντρο Εξυπηρέτησης Πολιτών. Η πρόσβαση είναι δυνατή και σε αλλοδαπούς από τη στιγμή που εισαγωγή αριθμού ID δεν είναι υποχρεωτική | Όχι |
| **Εσθονία** | Multifactor – password list, χρησιμοποιούνται username, password και τυχαίο αλφαριθμητικό από ένα διακριτικό σε έντυπη μορφή | Τράπεζες της Εσθονίας | Ναι (διαχειρίζεται από τις τράπεζες). Στην παρούσα φάση χρησιμοποιείται πιο συχνά από ότι τα εθνικά δελτία eID |
| | Multifactor – password based PIN calculator | Τράπεζες της Εσθονίας | Ναι (διαχειρίζεται από τις τράπεζες). Στην παρούσα φάση χρησιμοποιείται πιο συχνά από ότι τα εθνικά δελτία eID |

[103] Βλ. http://www.gsis.gr/taxisnet/help.html
[104] Διαδικτυακή Πύλη ΕΡΜΗΣ. Βλ. http://www.ermis.gov.gr/portal/page/portal/ermis/

| | | | |
|---|---|---|---|
| **Ηνωμένο Βασίλειο** | Single factor (username/password) μέσω της αντίστοιχης Κυβερνητικής Πύλης | Η Κυβερνητική Πύλη | Όχι |
| **Ισλανδία** | Single factor (username/password) το οποίο χρησιμοποιείται σε αρκετές εφαρμογές | Εξαρτάται από τον ιδιοκτήτη της εφαρμογής | Όχι |
| **Ιρλανδία** | Single factor (username/password)[105] για φορολογικά θέματα, βασισμένο σε ηλεκτρονική καταχώρηση χρησιμοποιώντας τον αριθμό PPS[106] | Ο Broker για τις δημόσιες Υπηρεσίες | Όχι |
| **Κροατία** | Single factor συστήματα (username/password) σε ένα πλήθος από μικρότερες εφαρμογές | Εξαρτάται από την εφαρμογή | Όχι |
| **Κύπρος** | Single factor (username/password) – TAXISnet, βασισμένο σε πρότερη ταυτοποίηση σε κάποιο τοπικό γραφείο της εφορίας | Τμήμα Εσωτερικών Προσόδων | Όχι |
| **Λετονία** | Multifactor – password list στο σύστημα ηλεκτρονικών προμηθειών, χρησιμοποιεί username, password και τυχαίο αλφαριθμητικό από ένα διακριτικό σε έντυπη μορφή | Άγνωστο | Όχι |
| | Single factor (username/password) – στα πλαίσια του συστήματος EDS[107], βασισμένο σε μία ηλεκτρονική υπογραφή για την λήψη των αιτούμενων credentials | Κρατική Υπηρεσία Εσόδων. Απαιτείται η ύπαρξη διαβατηρίου προκειμένου να πραγματοποιηθεί η αίτηση | Όχι |
| **Λιθουανία** | Multifactor – password list, χρησιμοποιώντας (username, password και τυχαία αλφαριθμητικά από ένα διακριτικό σε έντυπη μορφή) | Οι 9 εμπορικές τράπεζες της Λιθουανίας | Ναι (διαχειρίζεται από τις τράπεζες) |
| **Λουξεμβούργο** | Single factor συστήματα (username/password), οι διαδικασίες εξαρτώνται από τις εφαρμογές | Χρησιμοποιείται σε μία πληθώρα εφαρμογών. Εξαρτάται από τον εκδότη της εφαρμογής | Όχι |
| **Μάλτα** | Multifactor – password list με τη χρήση username, password και ενός PIN-code | Τοπικά αυτοδιοικητικά γραφεία. Εκδίδονται μετά τον έλεγχο της ταυτότητας του ατόμου | Όχι |
| | Single factor συστήματα (username/password), οι διαδικασίες εξαρτώνται από την εφαρμογή | Χρησιμοποιούνται σε μία πληθώρα εφαρμογών, με | Όχι |

[105] Reach Services portal, βλ. https://www.reachservices.ie/reachPortal/appmanager/portal/default
[106] Personal Public Service Number. Βλ. http://www.citizensinformation.ie/en/social_welfare/irish_social_welfare_system/personal_public_service_number.html
[107] Electronic Declaration System

| | | | |
|---|---|---|---|
| | | διάφορους εκδότες ανάλογα με την εφαρμογή | |
| **Νορβηγία** | Single factor (username/password) και Multifactor σε μία ποικιλία συστημάτων, μερικές φορές single factor, άλλες two-factor, συμπεριλαμβανομένης της ταυτοποίησης μέσω SMS. Το MyID[108] (MinID) αποτελεί το πιο σημαντικό παράδειγμα, το οποίο βασίζεται σε PIN code κάρτα. | Εξαρτάται από τον πάροχο της εφαρμογής. Σημειώνεται ότι ορισμένα από αυτά τα συστήματα περιλαμβάνουν επίσης λειτουργικότητα ηλεκτρονικής εφαρμογής βασισμένης σε PKI για υψηλότερα επίπεδα ασφάλειας | Όχι |
| **Ουγγαρία** | Single factor (username/password) – Πύλη Χρηστών, βασίζεται στην προηγούμενη προσωπική ταυτοποίηση του ατόμου ή στην ταυτοποίηση μέσω ενός ηλεκτρονικά υπογεγραμμένου[109] εγγράφου[30] | Περιφερειακά γραφεία εγγράφων. Ο αιτούμενος πρέπει να προσκομίσει έγγραφο ταυτοποίησης, διαβατήριο ή άδεια οδήγησης. Ως εκ τούτου είναι διαθέσιμο και σε αλλοδαπούς (κατόχους διαβατηρίων) | Όχι |
| **Ολλανδία** | Single factor (username/password) DigiD 1ου επιπέδου. Απαιτεί την ύπαρξη ενός αριθμού κοινωνικής ασφάλισης | GBO[110] και οι Ολλανδικές εφορίες | Όχι |
| | Multifactor – mobile phone – DigiD με τη χρήση κινητού τηλεφώνου για αυθεντικοποίηση δύο παραγόντων | GBO και οι Ολλανδικές εφορίες | Όχι |
| **Πορτογαλία** | Single factor (username/password) – για την Πύλη του Πολίτη[111] | UMIC[112]. Σημειώνεται ότι το σύστημα μπορεί να χρησιμοποιηθεί από αλλοδαπούς (δεν απαιτεί πληροφορίες οι οποίες να είναι μόνο για τους Πορτογάλους πολίτες), αλλά οι εφαρμογές είναι | Όχι |

[108] Βλ. http://minid.difi.no/minid/minid.php?lang=en

[109] Χρησιμοποιώντας ένα εεξελιγμένο πιστοποιητικό υπογραφής. Τα μητρώα τα οποία χρησιμοποιούν προηγμένες υπογραφές (παρά την φυσική παρουσία του ατόμου) αντιπροσωπεύουν 68 από ένα σύνολο 520.000 περιπτώσεων, ποσοστό δηλαδή περίπου 0,01%

[110] Gemeenschappeliijke Beheerorganisatie

[111] Portal do Cidadao. Βλ. http://www.portaldocidadao.pt/PORTAL/pt

[112] Knowledge Society Agency. Βλ. http://www.english.umic.pt/

| | | | |
|---|---|---|---|
| | | προσαρμοσμένες στις τοπικές ανάγκες | |
| | Single factor (username/password) σε μία ποικιλία ασφαλών συστημάτων κοινωνικών/φορολογικών, ενώ απαιτείται η ύπαρξη ενός κατάλληλου διακριτικού (όπως για παράδειγμα ο Α.Φ.Μ.) | Εξαρτάται από την αρχή που το διαχειρίζεται (για παράδειγμα η εφορία) | Όχι |
| **Ρουμανία** | Single factor (username/password) σε μία ποικιλία εφαρμογών | Εξαρτάται από την αρχή που το διαχειρίζεται | Όχι |
| **Σλοβακία** | Single factor (username/password) – Κεντρικό Portal της Δημόσιας Διοίκησης | Κεντρικό Portal της Δημόσιας Διοίκησης | Όχι |
| **Σλοβενία** | Single factor (username/password) το οποίο χρησιμοποιείται σε αρκετές εφαρμογές | Εξαρτάται από τον ιδιοκτήτη της εφαρμογής | Όχι |
| **Τουρκία** | Single factor (username/password) σε πολλές εφαρμογές | Εξαρτάται από την εφαρμογή | Όχι |
| **Τσεχία** | Single factor σύστημα (username/password) όπου τα credentials εκδίδονται μετά από την υπογραφή μίας αίτησης με αναγνωρισμένο πιστοποιητικό | Εξαρτάται από την εφαρμογή[113] | Όχι |
| **Φινλανδία** | Multifactor – password list, με τη χρήση username, password και τυχαίου αλφαριθμητικού από κάποιο έγγραφο διακριτικό | Φινλανδικές τράπεζες οι οποίες ανήκουν σε μία συγκεκριμένη ένωση[114] | Ναι (διαχειρίζεται από τις τράπεζες). Στην παρούσα φάση χρησιμοποιείται περισσότερο από ότι τα εθνικά δελτία eID. Χρησιμοποιεί τον εθνικό αριθμό κοινωνικής ασφάλισης ως διακριτικό. |

**Πίνακας 12: Χρησιμοποιούμενα συστήματα Username/password**

Από το σύνολο των χωρών της Ευρώπης, οι 22 χρησιμοποιούν τέτοια συστήματα αυθεντικοποίησης βασισμένα στη χρήση συνθηματικών. Από αυτές

[113] Ενδεικτικά παραδείγματα αποτελούν οι εφαρμογές που υφίστανται στον φορέα Κοινωνικής Ασφάλισης της Τσεχίας, το Υπουργείο Γεωργίας κ.τ.λ.
[114] Finnish Bankers Association authentication service

στις περισσότερες χρησιμοποιείται η τακτική των συνθηματικών single factor[115] (στις 19 χώρες), ενώ σε 4 από τις χώρες της ΕΕ (Βέλγιο, Εσθονία, Φινλανδία, Λιθουανία) χρησιμοποιούνται συστήματα αυθεντικοποίησης συνθηματικών multifactor (password lists[116] & password calculators).

Η ασφάλεια των χρησιμοποιούμενων συστημάτων όμως μπορεί να διαφέρει σε πολύ μεγάλο βαθμό. Ενώ ορισμένα συστήματα username/password δεν έχουν κάποιο συγκεκριμένο ενσωματωμένο μηχανισμό ασφάλειας κατά την διάρκεια της εγγραφής, τα περισσότερα από τα παραπάνω συστήματα προϋποθέτουν από τον χρήστη είτε:

Α) να παρέχει ένα συγκεκριμένο διακριτικό αυθεντικοποίησης κατά την διάρκεια της εγγραφής (παράδειγμα αποτελεί το TAXISnet στην Ελλάδα, όπου απαιτείται η χρήση του αντίστοιχου έγκυρου ΑΦΜ), είτε

Β) να παρουσιαστεί προσωπικά προκειμένου να λάβει τα διακριτικά πρόσβασης ή κάποιο άλλο αλφαριθμητικό ενεργοποίησης (παράδειγμα το TAXISnet στην Κύπρο ή ακόμη και το TAXISnet νέας γενιάς στην Ελλάδα μετά την 6/12/2010), ή τέλος

Γ) επιτρέπουν τα συνθηματικά να παραληφθούν μετά από μία αίτηση η οποία πρέπει να υποβληθεί μέσω της χρήσης ενός συστήματος ηλεκτρονικών υπογραφών βασισμένο σε PKI (όπως η Πύλη του Πολίτη στην Ουγγαρία).

Έτσι ενώ η χρήση ενός απλού συστήματος με username/password είναι εγγενώς λιγότερο ασφαλής από ένα σύστημα το οποίο επίσης απαιτεί ένα hardware διακριτικό, οι διαδικασίες εγγραφής σε αυτά είναι στις περισσότερες των περιπτώσεων ασφαλείς ενάντια στην μη εξουσιοδοτημένη χρήση.

Όσον αφορά στη συμμετοχή του ιδιωτικού τομέα, τα συστήματα login λογικά αναμένεται ότι δεν θα είναι προσβάσιμα σε φορείς του ιδιωτικού τομέα (εκτός και αν το σύστημα από μόνο του ελέγχεται από ένα φορέα του ιδιωτικού τομέα), καθώς τέτοια συστήματα αναπόφευκτα απαιτούν πρόσβαση σε μία βάση δεδομένων από όπου θα παρασχεθούν εξειδικευμένα δεδομένα ταυτοποίησης. Ο παραπάνω πίνακας επιβεβαιώνει αυτή την εκτίμηση καθώς μόνο 3 από τα 28 συστήματα (11%) μπορούν να χρησιμοποιηθούν από τον ιδιωτικό τομέα και όλα αυτά είναι συστήματα τραπεζών, όπου ο όρος «ιδιωτικός τομέας» στην περίπτωση αυτή αναφέρεται απλά στην ίδια την τράπεζα η οποία έχει τον έλεγχο της εφαρμογής.

[115] Κλασσικό σύστημα username/password

[116] Λίστα με κωδικούς, από όπου κάθε ένας μπορεί να αντιστοιχεί σε μία κατηγορία υπηρεσιών ή σε μία συγκεκριμένη υπηρεσία

## 5.3 Πολιτικές αυθεντικοποίησης και επίπεδα εμπιστοσύνης

Όπως γίνεται εύκολα αντιληπτό είναι άλλο το επίπεδο εμπιστοσύνης το οποίο μπορεί να παρέχει στα προσωπικά δεδομένα των χρηστών ένα σύστημα βασισμένο στην αυθεντικοποίηση μέσω συστημάτων PKI και άλλο το επίπεδο εμπιστοσύνης ενός συστήματος βασισμένου σε συνθηματικά. Τα πιο πολλά από τα κράτη μέλη της ΕΕ έχουνε υιοθετήσει παράλληλα συστήματα και των δύο κατηγοριών, PKI με διακριτικά soft αποθήκευσης (soft tokens[117]) ή αποθήκευσης σε σκληρό μέσο (κάρτες) και από την άλλη συστήματα τα οποία βασίζονται στη χρήση συνθηματικών (single factor, multifactor). Μεταξύ αυτών των συστημάτων, αυτά τα οποία βασίζονται στην υποδομή δημοσίου κλειδιού είναι και αυτά τα οποία προσφέρουν και τη μεγαλύτερη ασφάλεια.

Προκειμένου να καθοριστεί το επίπεδο ασφάλειας που το κάθε ένα από αυτά τα συστήματα προσφέρει και ως εκ τούτου το σε ποιες κατηγορίες υπηρεσιών μπορεί να χρησιμοποιηθεί, τα διάφορα κράτη-μέλη έχουνε υιοθετήσει πολιτικές αυθεντικοποίησης, οι οποίες καθορίζουν διάφορα επίπεδα εμπιστοσύνης. Τα επίπεδα εμπιστοσύνης αποτελούν διαβαθμίσεις της προστασίας για τα προσωπικά δεδομένα των χρηστών από τη μία, αλλά και των παρεχόμενων υπηρεσιών από την άλλη, όπου λαμβάνονται υπόψη οι επιπτώσεις που ενδέχεται να υπάρξουν από την κακόβουλη και αθέμιτη χρήση των δεδομένων των χρηστών με βάση την κάθε δεδομένη ηλεκτρονικά παρεχόμενη υπηρεσία.

Τα επίπεδα ασφάλειας που το κάθε κράτος-μέλος θα καθορίσει, αποτελεί κρατική υπόθεση του κάθε κράτους. Τα επίπεδα ασφάλειας αποτελούν μία κεντρική στρατηγική επιλογή του κάθε κράτους ως προς το θέμα της διαχείρισης των ηλεκτρονικών οντοτήτων, καθώς δίνουνε τη δυνατότητα στον κάθε δημόσιο φορέα ο οποίος παρέχει ηλεκτρονικές υπηρεσίες, να σταθμίσει το επίπεδο των κινδύνων και επακόλουθων επιπτώσεων οι οποίες συνοδεύουν την κάθε ηλεκτρονικά παρεχόμενη υπηρεσία. Απόρροια αυτής της στάθμισης αποτελεί ο καθορισμός επιτρεπτών επιπέδων ασφάλειας για τα προσωπικά δεδομένα, η αντιστοίχιση των οποίων υποδηλώνει και τους επιτρεπτούς τρόπους αυθεντικοποίησης και πιστοποίησης των χρηστών.

Επειδή δεν θα ήταν πρακτικά εφικτό στα πλαίσια της παρούσας μελέτης να παρουσιαστούν τα επίπεδα ασφάλειας ανά κατηγορία δεδομένων που χρησιμοποιεί το κάθε κράτος, επελέγη η λύση της παρουσίασης του αντίστοιχου ελληνικού πλαισίου, όπως αυτό προκύπτει από το Ελληνικό Πλαίσιο Ψηφιακής Αυθεντικοποίησης, με τις περιγραφές που αυτό περιλαμβάνει για την κάθε

[117] Δεν απαιτείται hardware υποδομή

κατηγορία δεδομένων που ενδέχεται να χρησιμοποιηθούν ή να διακινηθούν κατά τη διάρκεια της παροχής μίας ηλεκτρονικά παρεχόμενης υπηρεσίας[29].

| **Επίπεδο Αυθεντικοποίησης 0 (ΕΑ0)** | | | |
|---|---|---|---|
| **Περιγραφή Καλυπτόμενων Υπηρεσιών** | **Απαιτήσεις ασφάλειας** | **Συσχετισμός με επίπεδο εμπιστοσύνης** | **Προτεινόμενος μηχανισμός αυθεντικοποίησης** |
| Σε αυτό το επίπεδο δεν απαιτείται αυθεντικοποίηση του χρήστη καθώς οποιαδήποτε οντότητα είναι δυνατόν να έχει πρόσβαση στις πληροφορίες που θεωρούνται δημόσιες. Συνήθως, τέτοιου τύπου υπηρεσίες είναι όσες παρέχουν πληροφοριακό υλικό | Σε αυτό το επίπεδο αυθεντικοποίησης θα πρέπει να διασφαλίζονται, κατ' ελάχιστον, τα ακόλουθα:<br><br>Α)Ακεραιότητα του παρεχόμενου πληροφοριακού υλικού<br><br>Β)Αυθεντικότητα υπηρεσίας | Το επίπεδο αυθεντικοποίησης 0 σχετίζεται με το επίπεδο εμπιστοσύνης 0, καθώς δεν απαιτείται η επιβεβαίωση της ορθότητας της ηλεκτρονικής ταυτότητας του χρήστη. | Δεν απαιτείται μηχανισμός αυθεντικοποίησης. |
| **Επίπεδο Αυθεντικοποίησης 1 (ΕΑ1)** | | | |
| **Περιγραφή Καλυπτόμενων Υπηρεσιών** | **Απαιτήσεις ασφάλειας** | **Συσχετισμός με επίπεδο εμπιστοσύνης** | **Προτεινόμενος μηχανισμός αυθεντικοποίησης** |
| Σε αυτό το επίπεδο αυθεντικοποίησης απαιτείται μικρή έως μέτρια βεβαιότητα για την ορθότητα της ηλεκτρονικής ταυτότητας μιας οντότητας, καθώς αφορούν υπηρεσίες στις οποίες δικαίωμα πρόσβασης έχουν μόνον εξουσιοδοτημένες οντότητες. Τέτοιου είδους υπηρεσίες θεωρούνται αυτές που υποστηρίζουν τη δυνατότητα παροχής αιτήσεων στους χρήστες για περαιτέρω (off-line) επεξεργασία και την πραγματοποίηση της συναλλαγής με το φορέα σε φυσικό επίπεδο. | Σε αυτό το επίπεδο αυθεντικοποίησης θα πρέπει να διασφαλίζονται, κατ' ελάχιστον, τα ακόλουθα:<br><br>Α) Εμπιστευτικότητα των δεδομένων ταυτοποίησης (αναγνωριστικά) του χρήστη (τήρηση κανόνων προστασίας προσωπικών δεδομένων) ο διαπιστευτηρίων του χρήστη<br><br>Β) Ακεραιότητα των ο δεδομένων ταυτοποίησης (αναγνωριστικά) του | Το επίπεδο αυθεντικοποίησης 1 σχετίζεται με τα επίπεδα εμπιστοσύνης 1 και 2, καθώς απαιτείται έως και μέτρια βεβαιότητα για την ορθότητα της ηλεκτρονικής ταυτότητας του χρήστη. | Οι μηχανισμοί αυθεντικοποίησης που προτείνονται για το συγκεκριμένο επίπεδο συμπεριλαμβάνουν: συνθηματικά και συνθηματικά μιας χρήσης |

| | | | |
|---|---|---|---|
| | χρήστη<br>ο διαπιστευτηρίων του χρήστη<br>ο δεδομένων που λαμβάνονται από την ηλεκτρονική υπηρεσία<br><br>Γ) Αυθεντικότητα υπηρεσίας | | |
| **Επίπεδο Αυθεντικοποίησης 2 (ΕΑ2)** | | | |
| **Περιγραφή Καλυπτόμενων Υπηρεσιών** | **Απαιτήσεις ασφάλειας** | **Συσχετισμός με επίπεδο εμπιστοσύνης** | **Προτεινόμενος μηχανισμός αυθεντικοποίησης** |
| Σε αυτό το επίπεδο αυθεντικοποίησης απαιτείται υψηλή βεβαιότητα για την ορθότητα της ηλεκτρονικής ταυτότητας μιας οντότητας, καθώς είναι εξαιρετικά κρίσιμο να εξασφαλιστεί ότι μόνο εξουσιοδοτημένα πρόσωπα έχουν τη δυνατότητα πρόσβασης στις προσφερόμενες υπηρεσίες. Εδώ εντάσσονται οι ηλεκτρονικές υπηρεσίες που επεξεργάζονται ευαίσθητα προσωπικά δεδομένα ή υποστηρίζουν τη διενέργεια οικονομικών συναλλαγών. | Στο ΕΑ2 θα πρέπει να διασφαλίζονται κατ' ελάχιστον τα ακόλουθα:<br><br>Α)Εμπιστευτικότητα των<br>ο δεδομένων ταυτοποίησης (αναγνωριστικά) του χρήστη (ιδιωτικότητα)<br>ο διαπιστευτηρίων του χρήστη<br>ο δεδομένων που αποστέλλονται από το χρήστη στην ηλεκτρονική υπηρεσία<br>ο δεδομένων που ο χρήστης λαμβάνει από την ηλεκτρονική υπηρεσία<br><br>Β)Ακεραιότητα των<br>ο δεδομένων ταυτοποίησης (αναγνωριστικά) του χρήστη<br>ο διαπιστευτηρίων του χρήστη<br>ο δεδομένων που αποστέλλονται από το χρήστη στην ηλεκτρονική υπηρεσία<br>ο δεδομένων που ο χρήστης λαμβάνει από την ηλεκτρονική υπηρεσία<br><br>Γ)Αυθεντικότητα υπηρεσίας | Το επίπεδο αυθεντικοποίησης 2 σχετίζεται με το επίπεδο εμπιστοσύνης 3 καθώς απαιτείται υψηλή βεβαιότητα για την ορθότητα της ηλεκτρονικής ταυτότητας του χρήστη. | Ο μηχανισμός αυθεντικοποίησης που προτείνεται για το συγκεκριμένο επίπεδο αξιοποιεί ψηφιακά πιστοποιητικά (digital certificates) που θα εκδίδονται από την κατάλληλη Υποδομή Δημόσιου Κλειδιού (PKI) και την Αρχή Χρονοσήμανσης (Time Stamping Authority - TSA), υπό την αίρεση βεβαίως ότι η TSA επιτελεί και έργο CA. Επιπρόσθετα προτείνεται η αξιοποίηση διακριτικών χαλαρής ή σκληρής αποθήκευσης. Ο διαχωρισμός αυτός πραγματοποιείται δεδομένου ότι θεωρείται ότι δεν προάγει την ευρεία διάδοση υπηρεσιών ηλεκτρονικής διακυβέρνησης η απαίτηση όλοι οι πολίτες να προμηθευτούν άμεσα αναγνώστες έξυπνων καρτών για να δύνανται να έχουν πρόσβαση στις ηλεκτρονικές υπηρεσίες υψηλού επιπέδου εμπιστοσύνης. Ουσιαστικά στόχος είναι να μη δημιουργηθούν έμμεσα προϋποθέσεις αποκλεισμού της συντριπτικής πλειονότητας των πολιτών από τις παρεχόμενες και υπό ανάπτυξη ηλεκτρονικές υπηρεσίες. Παράλληλα βεβαίως τονίζεται η ανάγκη προσεχτικής μελέτης όσων προβλέπει το Π.Δ. 150/2001 σε σχέση με τις «ψηφιακές υπογραφές» και τις ενδεχόμενες απαιτήσεις μη αποποίησης στο πλαίσιο μιας ηλεκτρονικής υπηρεσίας, κυρίως όσον αφορά τα διακριτικά χαλαρής αποθήκευσης. Σε κάθε περίπτωση, αποκλειστικά υπεύθυνος για την τελική επιλογή του τύπου διακριτικών αποθήκευσης είναι πάντοτε ο φορέας |

| | | | |
|---|---|---|---|
| | Δ)Μη αποποίηση<br>ο αποστολής δεδομένων<br>ο λήψης δεδομένων<br><br>Ε)Υπηρεσίες εποπτείας (auditing)<br><br>ΣΤ)Χρονοσήμανση των ενεργειών | | παροχής της ηλεκτρονικής υπηρεσίας. Όποια επιλογή και αν τελικά υιοθετηθεί, τα διακριτικά αποθήκευσης θα πρέπει να προστατεύονται από τους αντίστοιχους προσωπικούς κωδικούς του χρήστη. |

**Πίνακας 13: Επίπεδα Αυθεντικοποίησης Ελληνικού Πλαισίου Ψηφιακής Αυθεντικοποίησης**

Τα ανωτέρω μάλιστα επίπεδα Αυθεντικοποίησης όπως αυτά περιλαμβάνονται στο ελληνικό Πλαίσιο Ψηφιακής Αυθεντικοποίησης δεν είναι απλά συμβουλευτικού χαρακτήρα προς τους φορείς οι οποίες πρόκειται να παράσχουν αντίστοιχες υπηρεσίες, αλλά η πολιτεία έχει φροντίσει να δώσει ένα δεσμευτικό χαρακτήρα ως προς την υποχρέωση τήρησής τους μέσα από σχετικό νόμο επικύρωσης του[31].

Οι πολιτικές αυτές αυθεντικοποίησης είναι πολύ κρίσιμες για το κάθε κράτος μέλος, καθώς παρέχουν στους δημόσιους οργανισμούς της κάθε χώρας το περιθώριο να καθορίσουν το επίπεδο ασφάλειας και εμπιστοσύνης το οποίο απαιτούν για κάθε υπηρεσία την οποία παρέχουν και ως εκ τούτου να επιλέξουν με βάσει το αντίστοιχο επίπεδο ασφάλειας και τον αντίστοιχο τρόπο αυθεντικοποίησης ο οποίος θα απαιτείται για τους χρήστες της κάθε υπηρεσίας.

Στη συνέχεια περιγράφεται εάν κάθε μία από τις χώρες έχει επίσημα ή ανεπίσημα υιοθετήσει μία πολιτική αυθεντικοποίησης προκειμένου να αξιολογήσει την ασφάλεια/αξιοπιστία των συστημάτων eIDM που διαθέτει, και το τι μορφή παίρνει σε κάθε περίπτωση αυτή η πολιτική. Μία πολιτική θεωρείται ότι έχει και «επίσημα υιοθετημένη» εφόσον έχει υπάρξει συγκεκριμένη απόφαση της κυβέρνησης με την οποία να την αποδέχεται και να χρησιμοποιείται στην πράξη, ενώ όπου μία πολιτική αναφέρεται ως «ανεπισήμως υιοθετημένη» πρόκειται για μία πολιτική στην οποία γίνεται αναφορά περιστασιακά από το κράτος μέλος και χωρίς καμία επίσημη κυβερνητική στήριξη ή συστηματικές επιπτώσεις στην πράξη.

| Χώρα | Κατάσταση (Επίσημα υιοθετημένη/ ανεπίσημα υιοθετημένη/ Δεν υφίσταται) | Αριθμός Επιπέδων | Περιγραφή / Χαρακτηριστικά (αναγνωρισμένο επίπεδο πιστοποίησης STORK)[118][32] |
|---|---|---|---|
| **Αυστρία** | Επίσημα υιοθετημένη | 2 | Ο Αυστριακός νόμος για την ηλεκτρονική διακυβέρνηση[119] δίνει έμφαση στην έννοια της κάρτας του πολίτη και βασίζεται στις αναγνωρισμένες υπογραφές ως το μοναδικό επίπεδο ασφάλειας. Αυτό το μόνο επίπεδο (η κάρτα του πολίτη) είναι το μόνο ρητά αναγνωρισμένο επίπεδο. Δηλαδή τα επίπεδα:<br>Επίπεδο 0: Χωρίς αυθεντικοποίηση (STORK QAA[120] Level: ∅) και<br>Επίπεδο 1: Με αυθεντικοποίηση (STORK QAA Level: 4) |
| **Βέλγιο** | Ανεπισήμως υιοθετημένη | 5 | Η ομοσπονδιακή δημόσια υπηρεσία για τις ΤΠΕ[121] αναγνωρίζει ότι υπάρχουν πέντε επίπεδα αυθεντικοποίησης για τα φυσικά πρόσωπα:<br>Επίπεδο 0: Χωρίς αυθεντικοποίηση (STORK QAA Level: ∅)<br>Επίπεδο 1: Αυθεντικοποίηση με χρήση username και password που αποτελεί επιλογή του χρήστη (STORK QAA Level: 1)<br>Επίπεδο 2: Αυθεντικοποίηση με χρήση username και password που αποτελεί επιλογή του χρήστη και επιπλέον έναν τυχαίο ισχυρό κωδικό από ένα έντυπο διακριτικό ταυτοποίησης. (STORK QAA Level: 2)<br>Επίπεδο 3: Αυθεντικοποίηση με τη χρήση πιστοποιητικού αυθεντικοποίησης της eID με τη χρήση PIN (STORK QAA Level: 3)<br>Επίπεδο 4: Αυθεντικοποίηση με τη χρήση πιστοποιητικού αυθεντικοποίησης της eID και επιπλέον χρήση της ψηφιακής υπογραφής μέσω του πιστοποιητικού υπογραφής του eID (STORK QAA Level: 4) |
| **Βουλγαρία** | Δεν υφίσταται | - | Δεν έχει εφαρμογή |
| **Γαλλία** | Επίσημα υιοθετημένη | 4 | Έχει υιοθετηθεί επίσημα ένα σύστημα τριών επιπέδων μέσω του πλαισίου αναφοράς[33] Γενικής Ασφάλειας[122], τα |

[118] Για κάθε χώρα στην περίπτωση που αυτή συμμετέχει στο πρόγραμμα STORK(για το πρόγραμμα βλ. στις αναφορές που προηγήθηκαν, ή στο Κεφάλαιο «Ευρωπαϊκά Έργα»), παρέχεται η πληροφορία, σχετικά με το ποια είναι τα αντίστοιχα κοινά αποδεκτά επίπεδα ασφάλειας, κατά το STORK, το οποίο μπορεί να προσφέρει το σύστημα το οποίο έχει υιοθετήσει ανά επίπεδο προστασίας η κάθε χώρα. Το STORK αναγνωρίζει τέσσερα δυνατά επίπεδα ασφάλειας, τα οποία στην κλίμακα 1-4, και τα οποία προσδιορίζονται ανάλογα με την βλάβη η οποία μπορεί να επέλθει για το άτομο, η οποία και προσδιορίζει το κατά περίπτωση επίπεδο.

[119] Austrian eGovernment Act

[120] QAA: Quality Assurance of Authentication

[121] FedICT

| | | | |
|---|---|---|---|
| | | | οποία διακρίνονται σε: μεσαίο (αναφέρεται ως '*') (STORK QAA Level: 3), δυνατό/στάνταρ ('**') (STORK QAA Level: 4) και ενισχυμένο ('***') (STORK QAA Level: 4). Το επίπεδο ασφάλειας το οποίο απαιτείται για κάθε υπηρεσία που προσφέρεται ορίζεται από τη δημόσια αρχή που παρέχει την υπηρεσία, αυτή η αρχή (αρχή της σταδιακής ασφάλειας) είναι επίσης επίσημα αποδεκτή από την CNIL[123]. |
| **Γερμανία** | Δεν υφίσταται | 4 | Επίσημα δεν υφίστανται επίπεδα ασφάλειας αυθεντικοποίησης. Παρ' όλα αυτά άτυπα διακρίνονται 4 επίπεδα: χωρίς αυθεντικοποίηση(STORK QAA Level: 1), αυθεντικοποίηση με username και password(STORK QAA Level: 2), αυθεντικοποίηση με hardware διακριτικό και PIN (STORK QAA Level: 3)και τέλος με τη χρήση αναγνωρισμένου hardware διακριτικού και ενός card reader (STORK QAA Level: 4) |
| **Δανία** | Επισήμως υιοθετημένη | 4 | Δημιουργήθηκε μία πολιτική και επικυρώθηκε ως δημόσια σύσταση το 2005, βασισμένη στο US Government E-Authentication Guidance for Federal Agencies[124]. Καθιερώνει και περιγράφει τέσσερα επίπεδα αξιοπιστίας ταυτοτήτων: απλά εμπιστευτικό, ορισμένως εμπιστευτικό, υψηλό και πολύ υψηλό |
| **Ελλάδα** | Επίσημα Υιοθετημένη | 3 | Υφίσταται ένα επίσημο σύστημα τριών επιπέδων: ένα στο οποίο δεν υπάρχει κανενός είδους αυθεντικοποίηση, ένα δεύτερο το πρώτο βασίζεται σε σύστημα username/password, και το τρίτο το οποίο βασίζεται στη χρήση αναγνωρισμένων πιστοποιητικών. |
| **Εσθονία** | Ανεπίσημα Υιοθετημένο | 2 | Δεν υπάρχει προς το παρόν κάποιο σύστημα, ωστόσο τρέχει ένα έργο από τα τέλη του 2009, το οποίο θα αναπτύξει τις μεθόδους εκτίμησης και τα κριτήρια για την αξιολόγηση διαφορετικών (ξένων) eIDs. Πιθανότατα θα αναπτυχθεί ένα σύστημα αυθεντικοποίησης, το οποίο θα καλύπτει τόσο τις εγχώριες όσο και τις ξένες eIDs. Προς το παρόν το Εσθονικό σύστημα καθορίζει δύο επίπεδα προστασίας: Ένα με απλά μέσα όπως ταυτοποίηση μέσω τραπεζικών συστημάτων (STORK QAA Level: 2,3,4) και ένα με ταυτοποίηση πιστοποιητικού PKI το οποίο περιέχεται στο mobile-ID ή στο εθνικό δελτίο ID (STORK QAA Level: 4). |
| **Ηνωμένο Βασίλειο** | Επίσημα υιοθετημένη | 4 | Το Στρατηγικό σχέδιο δράσης της κυβέρνησης του Η.Β. διακρίνει έναν αριθμό μέσων αυθεντικοποίησης βασισμένο στους κινδύνους που απειλούνται κατά |

[122] Référentiel Général de Sécurité
[123] National Data Protection Authority
[124] Η πολιτική των Ηνωμένων Πολιτειών όπως αναφέρεται στην Οδηγία για την Ηλεκτρονική Αυθεντικοποίηση προς τις Ομοσπονδιακές Υπηρεσίες, αναφέρεται στο μνημόνιο M-04-04 του Γραφείου Προϋπολογισμού και Διοίκησης, της 16ης Δεκεμβρίου 2003

| | | | |
|---|---|---|---|
| | | | περίπτωση[34], αλλά χωρίς να εφαρμόζει μία αυστηρή ιεραρχία μεταξύ αυτών. Σε ένα πολύ υψηλό επίπεδο διακρίνονται 4 επίπεδα ασφάλειας. |
| **Ισλανδία** | Δεν υφίσταται | 4 | Δεν έχει εφαρμογή καθώς χρησιμοποιούνται για την ταυτοποίηση μία πληθώρα συστημάτων τα οποία απλά αν γίνει προσπάθεια να κατηγοριοποιηθούν, διακρίνονται 4 κατηγορίες μα αντίστοιχα (STORK QAA Level: 1 έως 4) |
| **Ισπανία** | Ανεπίσημα υιοθετημένη | 3 | Προκύπτει ένα άτυπο σύστημα τριών επιπέδων: username/password με (STORK QAA Level: 1 και 2), αυθεντικοποίηση δύο παραγόντων με χρήση τυχαίου κωδικού(STORK QAA Level: 3), και αυθεντικοποίηση με πιστοποιητικό με (STORK QAA Level: 4). |
| **Ιρλανδία** | Δεν υφίσταται | | Δεν έχει εφαρμογή |
| **Ιταλία** | Ανεπίσημα υιοθετημένο | 2 | Εξ' ορισμού χρησιμοποιείται ένα σύστημα δύο επιπέδων, όπου οι εφαρμογές χαμηλότερης ασφάλειας χρησιμοποιούν συστήματα username/password(STORK QAA Level: 2), και τα υψηλότερου επιπέδου συστήματα χρησιμοποιούν μία ή περισσότερες λύσεις βασισμένες σε smart cards (STORK QAA Level: 4) |
| **Κροατία** | Δεν υφίσταται | - | Υφίσταται μία νομική απαίτηση[125] η οποία απαιτεί την χρήση των πιστοποιητικών FINA στην ανάπτυξη εφαρμογών ηλεκτρονικής διακυβέρνησης οι οποίες χρησιμοποιούν ηλεκτρονικές υπογραφές. Ωστόσο αυτό σχετίζεται άμεσα με την έννοια των υπογραφών και όχι της ταυτοποίησης αυτής καθ' αυτής |
| **Κύπρος** | Δεν υφίσταται | - | Δεν έχει εφαρμογή |
| **Λετονία** | Δεν υφίσταται | - | Δεν έχει εφαρμογή |
| **Λιθουανία** | Δεν υφίσταται | - | Δεν έχει εφαρμογή |
| **Λιχτενστάιν** | Δεν υφίσταται | - | Δεν έχει εφαρμογή |
| **Λουξεμβούργο** | Δεν υφίσταται | 3 | Ανεπίσημα υπολογίζονται τρία επίπεδα ασφάλειας με (STORK QAA Level: ∅) για το 1$^{ο}$ και (STORK QAA Level: 4) για τα υπόλοιπα 2. |
| **Μάλτα** | Ανεπίσημα υιοθετημένο | 3 | Τα σχέδια για την αυθεντικοποίηση στη Μάλτα περιγράφονται γύρω από ένα σύστημα τριών επιπέδων (ως προς την πρόσβαση του κοινού): 1$^{ο}$ επίπεδο: περιορισμένη αυθεντικοποίηση (login, password και PIN), 2$^{ο}$ επίπεδο: εμπιστευτική αυθεντικοποίηση (ψηφιακό πιστοποιητικό), 3$^{ο}$ επίπεδο: μέγιστη αυθεντικοποίηση (αναγνωρισμένο ψηφιακό πιστοποιητικό). Ωστόσο, έχει αναπτυχθεί μόνο το 1$^{ο}$ επίπεδο. |

[125] Regulation on the scope of operations, content and responsible authority for operations of electronic signature certification for state administration bodies

| | | | |
|---|---|---|---|
| **Νορβηγία** | Επίσημα υιοθετημένη | 4 | Έχει υιοθετηθεί μία αρκετά λεπτομερής άτυπη πολιτική[126]. Περιγράφεται ένα σύστημα ασφάλειας τεσσάρων επιπέδων, έχοντας κατά νου απαιτήσεις καταχώρισης, πολιτικές διαχείρισης και τους πιθανούς κινδύνους. |
| **Ολλανδία** | Ανεπίσημα υιοθετημένη | 4 | Συνάγεται ένα σύστημα τριών επιπέδων πάνω στο σχήμα DigiD, το πρώτο βασίζεται στο σύστημα username/password του DigID(STORK QAA Level: 2), το δεύτερο βασίζεται στο σύστημα ελέγχου αυθεντικοποίησης δύο παραγόντων με αποστολή μηνύματος μέσω κινητού τηλεφώνου(STORK QAA Level: 3) και το τρίο θα χρησιμοποιεί το μελλοντικό δελτίο eID ENIK ως μία συσκευή PKI(STORK QAA Level: 4). Ωστόσο, είναι ασαφές κατά πόσο το τρίτο επίπεδο θα αναπτυχθεί τελικά στο μέλλον |
| **Πολωνία** | Ανεπίσημα υιοθετημένη | 3 | Το Υπουργικό Συμβούλιο ενέκρινε (στις 26 Μαΐου 2009) το σχέδιο που εκπονήθηκε από το Υπουργείο Εσωτερικών και Δημόσιας Διοίκησης, το οποίο προτείνει μία νέα μέθοδο διαχείρισης αυθεντικοποίησης πελατών – το επονομαζόμενο έμπιστο προφίλ ePUAP[127], μία λύση με κωδικό προκειμένου εισέλθει στην ηλεκτρονική πλατφόρμα της δημόσιας διοίκησης (e-PUAP[128]. Το προφίλ αυτό θα περιλαμβάνει κατ' ελάχιστο: όνομα και επίθετο, PESEL[129], login name, διεύθυνση e-mail. Ως το υψηλότερο επίπεδο μπορούν να θεωρηθούν οι αναγνωρισμένες υπογραφές, με τις λύσεις με κωδικούς να παίζουν ένα δεύτερο ρόλο. |
| **Πορτογαλία** | Δεν υφίσταται | 3 | Το πιο σημαντικό σύστημα στην Πορτογαλία βασίζεται στην Κάρτα του Πολίτη η οποία μπορεί να καλύψει υπηρεσίες επιπέδου ασφάλειας (STORK QAA Level: 4). Παράλληλα υπάρχει ένα σύστημα το «Justice» το οποίο προσδιορίζεται ως (STORK QAA Level: ∅) και τέλος ένα επίπεδο με χρήση username/password και επιπλέον κάποιο τομεακό χαρακτηριστικό το οποίο χαρακτηρίζεται ως επιπέδου (STORK QAA Level: 2) |
| **Ρουμανία** | Ανεπίσημα υιοθετημένη | 2 | Στην ιστοσελίδα της ηλεκτρονικής διακυβέρνησης[130] αναφέρονται δύο τρόποι αυθεντικοποίησης: Ως υψηλότερο επίπεδο θεωρούνται οι αναγνωρισμένες υπογραφές, με τις λύσεις με κωδικό να καταλαμβάνουν ένα δεύτερο ρόλο |

[126] Μέσω του εγγράφου πολιτικής "Strategy on eID and signature in the Public Sector"
[127] zaufany profil
[128] Trusted ePUAP profile – το σύνολο των πληροφοριών που ταυτοποιούν και περιγράφουν μία οντότητα ή ένα άτομο το οποίο διαθέτει έναν λογαριασμό ePUAP, επιβεβαιώνεται με έναν αξιόπιστο τρόπο από μία εξουσιοδοτημένη οντότητα της δημόσιας διοίκησης
[129] Polish Powszechny Elektroniczny System Ewidencji Ludności
[130] Βλ. σχετικά http://www.e-guvernare.ro/Default.aspx?LangID=4

| | | | |
|---|---|---|---|
| **Σλοβακία** | Ανεπίσημα υιοθετημένη | 3 | Δεν υπάρχει επίσημο σύστημα, άλλα μπορεί να συναχθεί ένα ανεπίσημο τριών επιπέδων σύστημα (username/password, αναγνωρισμένη υπογραφή με προσωπική ταυτοποίηση και ψηφιακή υπογραφή με χρήση μοναδικού αναγνωριστικού στο πιστοποιητικό |
| **Σλοβενία** | Ανεπίσημα υιοθετημένη | 4 | Έχει υιοθετηθεί ένα άτυπο σύστημα τριών επιπέδων (άμεση εισαγωγή προσωπικών δεδομένων, username/password και αναγνωρισμένα πιστοποιητικά) με αντίστοιχες STORK διαβαθμίσεις (STORK QAA Level: 1,3 και 4). Το 4$^{ο}$ επίπεδο περιλαμβάνει υπηρεσίες οι οποίες προσφέρονται με δημόσια διακινούμενα δεδομένα |
| **Σουηδία** | Επίσημα υιοθετημένο | 2 | Η λύση της Σουηδίας βασίζεται σε προηγμένα πιστοποιητικά (soft και σε hardware) τα οποία χρησιμοποιούμενα μπορούν να μας δώσουνε συνολικά δύο κλάσεις επιπέδων ασφάλειας: στο πρώτο απαιτείται soft eID με (STORK QAA Level: 4), ενώ στο δεύτερο απαιτείται hard eID με (STORK QAA Level: 4) |
| **Τσεχία** | Δεν υφίσταται | - | Δεν έχει εφαρμογή |
| **Ουγγαρία** | Ανεπίσημα υιοθετημένο | 4 | Έχει αναφερθεί ένα σύστημα τεσσάρων επιπέδων, αλλά δεν υπάρχουν επίσημες συνέπειες ως προς αυτό |
| **Σουηδία** | Δεν υφίσταται | - | Υψηλή προτυποποίηση (μέσω των τραπεζικά εκδιδόμενων eIDs) καθιστά τις πολυεπίπεδες πολιτικές μη αναγκαίες. |
| **Τουρκία** | Ανεπίσημα υιοθετημένη | 3 | Το έργο «Πύλη για την Ηλεκτρονική Διακυβέρνηση» προϋποθέτει την ύπαρξη ενός συστήματος τριών επιπέδων: login βασισμένο σε ένα μοναδικό αριθμό ID, αυθεντικοποίηση δύο παραγόντων με τη χρήση τυχαίων αλφαριθμητικών, και πιστοποιητικά αυθεντικοποίησης |
| **Φινλανδία** | Ανεπίσημα υιοθετημένη | 4 | Υπάρχει ένα σύστημα τεσσάρων επιπέδων, αλλά δεν έχει υιοθετηθεί επίσημα από τους ιδιοκτήτες των εφαρμογών |

**Πίνακας 14: Ευρωπαϊκές πολιτικές αυθεντικοποίησης και διακρινόμενα επίπεδα ασφάλειας**

Έτσι οι πολιτικές αυθεντικοποίησης είναι πολύ χρήσιμες σε επίπεδο διαλειτουργικότητας των Ευρωπαϊκών λύσεων διαχείρισης ηλεκτρονικών ταυτοτήτων. Ο λόγος είναι ότι επειδή το κάθε κράτος μέλος καθορίζει τα δικά του επίπεδα ασφάλειας, τότε αν μία υπηρεσία που παρέχεται από κάποιο τρίτο κράτος-μέλος μπορεί να παρασχεθεί και σε άλλα κράτη μέλη, ο φορέας της υπηρεσίας μπορεί δεδομένου του επιπέδου εμπιστοσύνης που απαιτεί για την εν λόγω υπηρεσία να απαιτήσει την υποστήριξη του αντίστοιχου επιπέδου αυθεντικοποίησης από το κράτος μέλος στο οποίο επεκτείνει την παροχή της εν λόγω υπηρεσίας, αντί να απαιτεί για την παροχή της συγκεκριμένες τεχνικές λύσεις.

Παρατηρούμε ότι η διαφοροποίηση των επιπέδων ασφάλειας έχει ήδη πραγματοποιηθεί σε 24 Ευρωπαϊκές χώρες, ανάλογα με τις ανάγκες ασφάλειας

των πραγματοποιούμενων συναλλαγών. Στις χώρες αυτές εφαρμόζεται κάποια μορφή διαβάθμισης σε επίπεδα των πολιτικών αυθεντικοποίησης.

Πέρα όμως από την άτυπη καθιέρωση κλιμακούμενων διαβαθμίσεων των επιπέδων πολιτικών αυθεντικοποίησης, υπάρχουν και 7 χώρες (Αυστρία, Γαλλία, Δανία, Ελλάδα, Ηνωμένο Βασίλειο, Νορβηγία και Σουηδία) όπου έχουν καθιερωθεί και υφίστανται επίσημα αυτά τα επίπεδα διαβάθμισης των πολιτικών ασφάλειας.

Σε όλες όμως τις περιπτώσεις τα επίπεδα πολιτικών ασφάλειας τα οποία εφαρμόζονται έχουν ένα καθαρά εθνικό χαρακτήρα. Η κάθε χώρα προχωράει στην καθιέρωση αποδεκτών επιπέδων ασφάλειας τα οποία πρέπει να διασφαλίζονται κατά περίπτωση. Αυτή η τακτική όμως δεν δίνει λύση στο πρόβλημα της διασυνοριακής παροχής υπηρεσιών μεταξύ των διαφόρων κρατών μελών. Προς αυτή την κατεύθυνση κατατείνει η τακτική την οποία προς το παρόν εφαρμόζει μόνο η Εσθονία, η οποία πέραν της καθιέρωσης των επιπέδων ασφάλειας αυθεντικοποίησης τα οποία καθιερώνει για εσωτερική χρήση, προβαίνει και στην ανάπτυξη μίας σειράς κριτηρίων διασυνοριακής αξιολόγησης ταυτοτήτων που έχουν εκδοθεί σε άλλες χώρες-μέλη της ΕΕ με βάση τα δικά της επίπεδα εμπιστοσύνης.

# 6. ΑΝΑΛΥΣΗ ΤΕΧΝΟΛΟΓΙΩΝ / ΥΠΟΔΟΜΩΝ

Στο Κεφάλαιο αυτό περιγράφεται για κάθε μία από τις χώρες, το είδος των τεχνολογικών υποδομών που χρησιμοποιεί στα συστήματά της. Η αξία της προσέγγισης δεν έγκειται τόσο στην αποτύπωση των τεχνολογικών υποδομών που αυτές χρησιμοποιούν, όσο στη μετέπειτα αξιοποίηση τους προκειμένου να συγκριθεί το κατά πόσο οι λύσεις αυτές είναι σύμφωνες με τις κοινές προδιαγραφές χρήσης και ασφάλειας οι οποίες τίθενται από τα μεγάλα Ευρωπαϊκά Έργα τα οποία βρίσκονται σε εξέλιξη.

Επιπλέον οι τεχνολογίες που η κάθε χώρα χρησιμοποιεί είναι πολύ σημαντικές από την σκοπιά της διασφάλισης της ιδιωτικότητας και το επίπεδο προστασίας που η κάθε χώρα επιθυμεί να παράσχει για τους πολίτες της χώρας της και το σύνολο των προσωπικών δεδομένων που περιλαμβάνονται μέσα σε αυτά τα δελτία.

## 6.1 Συχνά χρησιμοποιούμενα διακριτικά

Στην ενότητα αυτή περιγράφεται το ποια διακριτικά (αν υπάρχουν) διανέμονται στις οντότητες του κάθε κράτους. Αυτά τα διακριτικά περιλαμβάνουν κάθε hardware υποδομή εντός της οποίας μπορούν να παρέχονται τα credentials του πολίτη, όπως για παράδειγμα οι πληροφορίες οι οποίες πιστοποιούν την ακεραιότητα των χαρακτηριστικών της ταυτοποίησης. Εκτός από τα δελτία ταυτότητας, άλλα αντίστοιχα παραδείγματα μπορεί να αποτελεί και οποιαδήποτε φορητή συσκευή, αν και πιο κρίσιμο και ενδιαφέρον κρίθηκε να αναφερθούν οι υποδομές οι οποίες υφίστανται για κινητά τηλέφωνα στα οποία μπορεί να περιέχονται πιστοποιητικά PKI.

## *6.2 Συστήματα με κάρτες*

Στα πλαίσια αυτής της ενότητας θα παρουσιασθούν τα διακριτικά τα οποία βασίζονται σε hardware υλοποιήσεις και χρησιμοποιούνται στις διάφορες Ευρωπαϊκές Χώρες. Για αυτά τα διακριτικά αναφέρεται ο πραγματικός κατασκευαστής τους, ο τύπος της χρησιμοποιούμενης συσκευής ή μία λίστα από κοινά αποδεκτά πρότυπα τα οποία χρησιμοποιούνται. Ο τύπος της περιγραφής εξαρτάται από την υπό μελέτη κάθε φορά χώρα, καθώς κάποιες από τις χώρες προβαίνουν σε λεπτομερή περιγραφή των διακριτικών, ενώ κάποιες άλλες απλά

αρκούνται στο να προσδιορίσουν ότι τα διακριτικά αυτά θα πρέπει να είναι σύμφωνα με τα στάνταρ που κάθε φορά τίθενται για τα διακριτικά των ηλεκτρονικών ταυτοτήτων.

Το αποτέλεσμα της επισκόπησης συγκρινόμενο σε ένα άλλο επίπεδο, θα μπορούσε να χρησιμοποιηθεί προκειμένου να εξαχθεί το συμπέρασμα του κατά πόσο οι υλοποιήσεις αυτές είναι επιδεκτές διαλειτουργικής χρήσης στα πλαίσια του ενιαίου περιβάλλοντος που διαμορφώνεται στην Ευρώπη γύρω από το θέμα της διαχείρισης των ηλεκτρονικών ταυτοτήτων.

Κατά την εξέταση των υποδομών για τα eID από την πλευρά του τελικού χρήση (πολίτη) το πιο κρίσιμο σημείο προκειμένου να επιτευχθεί η διαλειτουργικότητα, είναι η χρησιμοποιούμενη μέθοδος η οποία υποστηρίζεται από την συσκευή ελέγχου αυθεντικοποίησης που αυτός χρησιμοποιεί. Στις περισσότερες περιπτώσεις η συσκευή αυθεντικοποίησης και η διαδικασία αυθεντικοποίησης είναι το μόνο πράγμα που ο πολίτης αντιλαμβάνεται από ένα σύστημα διαχείρισης eID. Όταν ο πολίτης χρησιμοποιεί τη συσκευή αυθεντικοποίησής του μέσα στη χώρα του, αυτή η πρόκληση συνήθως δεν υφίσταται, αλλά όταν η χρήση αρχίσει να αποκτά στοιχεία φορητότητας (περιβάλλον κινητών τηλεφώνων) και ο πολίτης αρχίζει να κινείται και να δρα ως επισκέπτης σε διαφορετικά κάθε φορά Κράτη της Ευρωπαϊκής Ένωσης, τίθενται ερωτήσεις γύρω από τα credentials και την διαλειτουργικότητα των ενδιάμεσων υποδομών[131] τα οποία σε εκείνη την περίπτωση αποκτούν μία πιο σημαντική αξία.

Στον πίνακα που ακολουθεί αναφέρονται για κάθε κράτος:

- Τη στήλη με το **«Όνομα»** της χώρας
- Τη στήλη **«Κατασκευαστής»** όπου παρατίθενται όλοι οι εθνικά αποδεκτοί προμηθευτές των διακριτικών. Σε ορισμένες χώρες δεν έχει επιλεχθεί συγκεκριμένος πάροχος, οπότε στις περιπτώσεις αυτές παρέχονται στοιχεία μόνο σχετικά με τα χρησιμοποιούμενα στάνταρ.
- Η στήλη **«Type/Microcontroller/Επίπεδο Προστασίας των Δεδομένων»** όπου περιγράφεται με περισσότερη λεπτομέρεια ο τύπος συσκευής που έχει επιλεγεί και η μέθοδος η οποία χρησιμοποιείται προκειμένου να διασφαλιστούν τα προσωπικά δεδομένα των πολιτών που περιέχονται στις κάρτες, αλλά και επίσης και η ακεραιότητα τους. Σε κάποιες από τις υπό μελέτη χώρες, δεν έχει γίνει επιλογή κατασκευαστή, οπότε σε αυτές τις περιπτώσεις στην αντίστοιχη στήλη θα περιλαμβάνονται πληροφορίες σχετικά με τα χρησιμοποιούμενα στάνταρ.
- Η στήλη **«Πολλαπλή Χρηστικότητα»** περιγράφει τις περιπτώσεις όπου στις υπό μελέτη χώρες έχει επιλεγεί κάποιο διακριτικό σε hardware το

[131] Middleware interoperability

οποίο μπορεί να χρησιμοποιηθεί σε διάφορες εφαρμογές (όπως τη χορήγηση πιστοποιητικών, φορολογική χρήση, θέματα υγείας, κ.τ.λ.). Εάν χρησιμοποιείται διακριτικό πολλαπλής χρηστικότητας, τότε περιγράφεται και η τεχνολογία που υποστηρίζει τη λειτουργία του.

| Χώρα | Κατασκευαστής | Type/ Microcontroller/ Επίπεδο προστασίας των Δεδομένων | Πολλαπλή Χρηστικότητα |
|---|---|---|---|
| **Αυστρία** | Δεν έχει καθοριστεί. Μπορούν να χρησιμοποιηθούν όλες οι αναγνωρισμένες έξυπνες κάρτες ανεξαρτήτου κατασκευαστή | Κοινά κριτήρια πιστοποιητικών για το ChipOS στο EAL4+[132] και EAL5+ για την chip platform | Δεν υπάρχει πολλαπλή χρήση. Ανάλογα με τον εκδότη, υποστηρίζονται άλλες εφαρμογές για την κάρτα ιατρικής ασφάλισης μέσω των αντίστοιχων πιστοποιητικών υγείας, ή από την άλλη παρέχονται λειτουργικότητες για ATM και άλλες οικονομικές δραστηριότητες για όσους χρησιμοποιούν τις κάρτες των τραπεζών |
| **Βέλγιο** | Gemalto[133] | Contact chip: Cryptoflex JavaCard32K/ Infineon SLE66CX322P και έναν πρόσθετο επεξεργαστή crypto (για υπολογισμούς RSA και DES)<br><br>Πιστοποιητικά X.509 | Ναι, το Java Applet χειρίζεται όλη την επικοινωνία με τον έξω κόσμο. Το δελτίο eID έχει επίσης την δυνατότητα να περιέχει προγράμματα τα οποία μπορούν να τρέξουν εντός του chip processor της κάρτας |
| **Βουλγαρία** | Μη διαθέσιμο | Μη διαθέσιμο | Μη διαθέσιμο |
| **Γαλλία** | Δεν έχει καθοριστεί. Βρίσκεται σε χρήση μία αυθεντικοποίηση τριών επιπέδων, (Middle, Strong και Strengthened)[134] [135] | Δεν διευκρινίζονται. Εκδίδονται συνολικά τρεις διαφορετικές smart cards.<br><br>**Vitale Card 2:**<br><br>32Kb Eeprom memory, crypto-processor, πιστοποιημένα κοινά | Δεν έχει καθοριστεί |

[132] EAL: Evaluation Assurance Level
[133] http://www.gemalto.com/index.html
[134] Middle: Κρυπτογραφικό τμήμα το οποίο συμμορφώνεται με τις απαιτήσεις του προτύπου CP
Strong: Κρυπτογραφικό τμήμα πιστοποιημένο στο επίπεδο CC EAL2+
Strengthened: Κρυπτογραφικό τμήμα πιστοποιημένο στο επίπεδο CC EAL4+
[135] Τα στάνταρ των χρησιμοποιούμενων έξυπνων καρτών είναι ISO 7816, ISO 7816-15 και PKCS#15 για πιστοποιητικά X509 V3

| | | | |
|---|---|---|---|
| | | κριτήρια EAL4+ (PPSSCD, PP9911) και το πρότυπο ISO7816 και EMV.<br><br>**Η κάρτα επαγγελματιών υγείας:**<br><br>Το επίπεδο ασφάλειας είναι EAL4+. Η κάρτα αυτή περιέχει έναν μικροεπεξεργαστή και έναν επεξεργαστή κρυπτογραφίας. (ISO 14443A ή ISO 14443B στα 13,56MHz.)<br><br>**Το μελλοντικό Εθνικό δελτίο eID:**<br><br>Το μελλοντικό δελτίο eID θα υιοθετήσει το πρότυπο των πιστωτικών καρτών. Θα βασίζεται σε ECC στάνταρ. (Ο Τύπος και ο Μικροεπεξεργαστής δεν έχουνε ακόμα καθοριστεί, αλλά θα είναι επιπέδου strengthened). | |
| **Γερμανία** | Το νέου τύπου δελτίο eID κατασκευάζεται από την Ολλανδική NXP[136] | Ολοκληρωμένο RFID contactless chip. Ακολουθείται το πρότυπο ISO 14443 και η μέθοδος προστασίας είναι EAC & PACE | Ναι. Και για σκοπούς συναλλαγής με επιχειρήσεις |
| **Δανία** | Οι ψηφιακές υπογραφές OCES είναι software-based ψηφιακές υπογραφές. Το πιστοποιητικό μπορεί να αποθηκευτεί ως διακριτικό soft ή hard | Άγνωστο | Άγνωστο |
| **Ελλάδα** | Χρησιμοποιούνται ευρέως γνωστά στάνταρ.<br><br>Οι έξυπνες κάρτες είναι SysGillo CryptoSmartCard από την InCard ST Microelectronics | Κριτήρια αναγνωρισμένα για EAL4+. Κοινά χρησιμοποιούμενα πρότυπα όπως τα ISO/IEC 15408-3, ISO 17799, ETSI TS 101 456, ITSEC-E3 FIPS 140-1 | Όχι |
| **Εσθονία** | TRUB Baltic SA[137] | Contact chip: Micardo COS με ένα | Δεν έχει οριστεί. |

[136] http://www.nxp.com/

[137] http://www.trueb.ee/index.php?lang=eng . Πρόκειται για τη νέα γενιά ηλεκτρονικών ταυτοτήτων της Εσθονίας οι οποίες ξεκίνησαν να παρασκευάζονται από τις 31/03/2010, ύστερα από την

| | | | |
|---|---|---|---|
| | | crypto-processor[35] | Υλοποιημένη σε Java platform |
| **Ηνωμένο Βασίλειο** | Μη διαθέσιμο | RF Contactless chip με μνήμη 68Kb. Η Μέθοδος προστασίας που χρησιμοποιείται είναι BAC και EAC | Μη διαθέσιμο |
| **Ισλανδία** | Διαφορετικοί κατασκευαστές. Χρησιμοποιούνται διαφορετικές τραπεζικές κάρτες[138].<br><br>Άλλες κάρτες[139] είναι διαθέσιμες σε όλους όσους είτε δεν μπορούν να αποκτήσουν τραπεζικές κάρτες ή για κάποιο άλλο λόγο θέλουν ειδικές κάρτες, όπως για παράδειγμα κάρτες εργαζομένων σε εταιρείες.<br><br>Και οι 2 χρησιμοποιούν (ISO-7816 – PKCS#15) | Μη διαθέσιμο | Μη διαθέσιμο |
| **Ισπανία** | Ακολουθεί τα ακόλουθα στάνταρ: ETSI TS 102 042, ETSI TS 101 456, ETSI TS 101 862, CWA 14167, CWA 14172, CWA 14.890. Οι κάρτες αυτές χρησιμοποιούνται για το εθνικό δελτίο eID και το Royal Mint το οποίο ακολουθεί τα πρότυπα PKCS#11, CSP και API PC/SC | Το δελτίο eID χρησιμοποιεί contact chip ICs, με ISO 7816-3 για συμβατή πρόσβαση και μία EEPROM 64Kb για δεδομένα.<br><br>Πιστοποιημένο CC EAL4+ πιστοποιητικό ως έξυπνη κάρτα και μία συσκευή Δημιουργίας Ασφαλούς Υπογραφής.<br><br>Χρησιμοποιεί EAC | Μία κάρτα πολλαπλής χρήσης που χρησιμοποιείται υποστηρίζει τα χρησιμοποιούμενα Java Applet και Active eSignature σε επίπεδο middleware. |
| **Ιταλία** | Υπάρχουν αρκετοί προμηθευτές καρτών οι οποίοι μπορούν να παρέχουν κάρτες. Στην παρούσα φάση χρησιμοποιούνται οι Siemens, Incard και Oberthur | Η Siemens και η Incard παρέχουν το λειτουργικό σύστημα, ενώ η Oberthur παρέχει την Java card. Σε όλες τις περιπτώσεις το λειτουργικό σύστημα συμμορφώνεται με τις απαιτήσεις του CNS και έτσι είναι διαλειτουργικό. Διαθέτει μνήμη 64Kb. Smartcard integrated circuit and an optics stripe band. Cryptographic coprocessor (ISO | |

εξάντληση των προηγούμενων αποθεμάτων της εταιρείας ORGA η οποία παρείχε τα δελτία eID 1ης γενιάς τα οποία χορηγούσε η Εσθονία.

[138] Οι eIDs στα δελτία των τραπεζών θα αποτελέσουν το κύριο διακριτικό eID στην Ισλανδία στο εγγύς μέλλον. Επίσης σχεδιάζεται το Εθνικό Μητρώο προκειμένου να μπορούν να εκδίδονται Κάρτες του Πολίτη με πιστοποιητικά, αλλά δεν έχει αποφασιστεί τίποτα σχετικά με αυτό.

[139] Αυτά τα πιστοποιητικά εκδίδονται κάτω από το ίδιο ενδιάμεσο πιστοποιητικό όπως το πιστοποιητικό στις κάρτες των τραπεζών και πληρούν τις ίδιες απαιτήσεις

| | | | |
|---|---|---|---|
| | | 7816-3, 7816-4, 7816-8) που υποστηρίζει RSA με ελάχιστο μήκος κλειδιού 1024bits.<br><br>Συμμορφώνεται με τα πρότυπα: ISO/IEC 7816-1, 7816-2 e ISO/ID-001.<br><br>Cryptographic chip PIN to open data. Πιστοποιητικά X509v.3 από την CNSD CA | |
| **Ιρλανδία** | Μη διαθέσιμο | Μη διαθέσιμο | Μη διαθέσιμο |
| **Κροατία** | Μη διαθέσιμο | Μη διαθέσιμο | Μη διαθέσιμο |
| **Κύπρος** | Μη διαθέσιμο | Μη διαθέσιμο | Μη διαθέσιμο |
| **Λετονία** | Ένας πάροχος έξυπνων καρτών ο οποίος ακόμα δεν έχει αποφασιστεί. Contact ICs (ISO 7816) με δομή[140] PKCS#15 | 64Kb EEPROM | Δεν έχει καθοριστεί |
| **Λιθουανία** | Πρέπει να είναι σύμφωνα με το CC EAL4+ . Τα CA private keys διατηρούνται σε συσκευές συμβατές με PKCS#11, FIPS140-1 επιπέδου προστασίας 1ου έως και 3ου (με την υποστήριξη της nCipher και της Chrysalis)[141] | Contact Chip 72Kb memory. Επίσης Contactless Chip 80Kb memory (για βιομετρικό σύστημα ICAO)<br><br>Χρησιμοποιείται EAC για την προστασία των δεδομένων | Δεν έχει καθοριστεί |
| **Λιχτενστάιν** | Μη διαθέσιμο[142] | Encrypted Keys (PKI) | Μη διαθέσιμο |
| **Λουξεμβούργο** | Μη διαθέσιμο | Μη διαθέσιμο | Μη διαθέσιμο |
| **Μάλτα** | Μη διαθέσιμο | Μη διαθέσιμο | Μη διαθέσιμο |
| **Νορβηγία** | Μη διαθέσιμο | Υπάρχει η εκτίμηση για συμπερίληψη ενός contactless chip προκειμένου να εισαχθούν στο δελτίο eID και βιομετρικά δεδομένα | Μη διαθέσιμο |
| **Ολλανδία** | Μη διαθέσιμο | Μη διαθέσιμο | Μη διαθέσιμο |
| **Ουγγαρία** | Μη διαθέσιμο | Μη διαθέσιμο | Μη διαθέσιμο |

[140] Τα ηλεκτρονικά δελτία eID που είναι διαθέσιμα από τις 12/1/2010 διαθέτουν τα ανωτέρω χαρακτηριστικά τα οποία όμως είχανε καθοριστεί σε ένα πρόγραμμα σχεδιασμού των ηλεκτρονικών ταυτοτήτων το οποίο είχε προηγηθεί

[141] Οι τεχνικές προδιαγραφές των πιστοποιητικών εκδίδονται από την UAB "Skaitmeninio sertifikavimo centras"

[142] Οι προδιαγραφές του hardware θα βασίζονται στις συστάσεις που έχουνε γίνει από την A-trust

| | | | |
|---|---|---|---|
| **Πολωνία** | Δεν υπάρχουν συγκεκριμένες λεπτομέρειες. Υπάρχουν στοιχεία μόνο για το σχεδιαζόμενο pl.ID | Μη διαθέσιμο | Θα είναι μία eID κάρτα πολλών εφαρμογών συμμορφούμενη με τις απαιτήσεις των Ευρωπαϊκών στάνταρ (κυρίως με το EN 15480 Identification card Systems – European Citizen Card). |
| **Πορτογαλία** | Η e-card είναι μία Cryptoflex JavaCard της Gemalto στα 64Kb | Είναι εξοπλισμένη με ένα microcontroller (Infineon SLE66CX322P) και έναν πρόσθετο crypto επεξεργαστή (για RSA και DES υπολογισμούς)<br><br>Είναι EAL5 certified | Ένα Java Applet υλοποιεί το CAP[143] |
| **Ρουμανία** | Μη διαθέσιμο | Μη διαθέσιμο | Μη διαθέσιμο |
| **Σλοβακία** | Μη διαθέσιμο[144] | Μη διαθέσιμο | Μη διαθέσιμο |
| **Σλοβενία**[145] | Gemplus PKCS#15 (HIC Card)<br>ActivIdentity smartcard (SIGOVCA) | Κάρτα HIC:<br><br>Samsung S3CC91C chip (καθαρό τσιπ επαφής με διεπαφή 7816 και 72Kb EEPROM διαθέσιμη για την αποθήκευση δεδομένων) με Java Card λειτουργικό σύστημα το οποίο παρέχεται από την Gemalto (αξιολογημένο EAL4+) | Μη διαθέσιμο |
| **Σουηδία** | **eID:** Δεν προσδιορίζεται<br><br>**Nordea:** Setec TAG AB (PKCS#15 profile), με το λειτουργικό σύστημα SetC0S στην έκδοση 4.4.1.[146]<br><br>**Steria:** Εκδίδονται κάρτες με λειτουργικό σύστημα της Setec το SetCOS (διάφορων εκδόσεων) και | Contactless RF chip για βιομετρικά δεδομένα και συμμόρφωση με τον ICAO, 32Kb. Contact Chip για e-services 32Kb<br><br>**Nordea:** Δεν έχει καθοριστεί.<br><br>Χρησιμοποιεί το πρότυπο ISO 7816<br><br>**Steria:** Δεν έχει καθοριστεί. | Δεν έχει καθοριστεί |

[143] CAP: Chip Authentication Program

[144] Ως προς τα μελλοντικά σχέδια, όταν θα υπάρχει ένα κεντρικό eIDM σύστημα, ο μηχανισμός αυθεντικοποίησης θα βασίζεται σε υποδομή PKI και το ιδιωτικό κλειδί θα περιλαμβάνεται στην έξυπνη κάρτα με contact ICs (στο πρότυπο ISO 7816) ή με διπλή διεπαφή ICs (ένα τσιπ και δύο διεπαφές – contact ISO 7816 και contactless ISO 14443).

[145] Έχουν καθοριστεί προδιαγραφές μόνο για μία έξυπνη κάρτα η οποία θα χρησιμοποιείται για υγειονομική περίθαλψη, οι Αρχές Πιστοποίησης της ηλεκτρονικής διακυβέρνησης μπορούν να εκδώσουν πολλούς τύπους έξυπνων καρτών.

[146] Οι τραπεζικές κάρτες της Nordea (Xpon Card με λειτουργικό σύστημα Proton Prisma EMV) μπορούν επίσης να χρησιμοποιηθούν ως ο φορέας για μία ηλεκτρονική ταυτότητα

| | | | |
|---|---|---|---|
| | Cryptoflex από την Axalto.<br><br>**BankID:** Oberthur (Siemens CardOS 4.3b), Gemalto (SetCOS 4.4.1) και Gemalto (Jacacard με applet eid2048). Όλες οι κάρτες έχουνε ένα PKCS#15 προφίλ | Χρησιμοποιεί το πρότυπο ISO 7816.<br><br>**BankID:** Δεν έχει καθοριστεί. Χρησιμοποιεί το πρότυπο ISO 7816.<br><br>**TeliaSonera:** Δεν έχει καθοριστεί | |
| **Τουρκία** | Μη διαθέσιμο[147] | Μη διαθέσιμο | Μη διαθέσιμο |
| **Τσεχία** | OKSystem. Υπάρχουν δύο δελτία ID (ένα με smart card και ένα πλαστικό χωρίς όμως chip) | Contact Chip: 128KB+ EEPROM, Πλατφόρμα βασισμένη σε Java Card 2.2.2 | Όχι |
| **Φινλανδία** | **FINEID (Κάρτα του πολίτη):**<br><br>Gemalto. Το προφίλ του FINEID συμμορφώνεται με το ISO/IEC 7816-15[148]<br><br>**Organization card:**<br><br>Εκδίδεται σε φυσικά πρόσωπα με επαγγελματική χρήση από την Oberthur Card Systems Finland[149]<br><br>Το JavaCard Applet παράγεται από την Charismathics Gmbh[150] και ακολουθεί τις ίδιες προδιαγραφές με το Applet command interface όπως το FINEID applet | **FINEID:** SetCos 5.1.1B/72Kb (64Kb stated) μνήμη EEPROM, όπου μόνο ένα μικρό τμήμα διατίθεται για συμπληρωματικά πιστοποιητικά ή data objects. Μεγάλο μέρος της μνήμης παραμένει σε αχρησία<br><br>**Organization card:**<br><br>Oberthur Cosmopolic 5.4 RSA 64 JavaCard platform, η οποία είναι αναγνωρισμένη για SSCD. | Ναι, Κάρτα Java Open Platform. Οι προδιαγραφές του FINEID δεν επιτρέπουν τη χρήση του σε άλλες πρόσθετες εφαρμογές |

**Πίνακας 15: Παρουσίαση τεχνολογικών υποδομών στα χρησιμοποιούμενα δελτία eID**

[147] Το σχετικό project για την προμήθεια όλων των Τούρκων πολιτών με eID υπολογίζεται για το 2013, και το μόνο που έχει καθοριστεί είναι ο προμηθευτής των υποδομών σε επίπεδο middleware. Βλ. (http://www.teridian.com/assets/001/5079.pdf)

[148] Εξ' αιτίας της μειωμένης χρήσης των Φινλανδικών Καρτών του Πολίτη αλλάζει η στρατηγική τους γύρω από το FINEID. Το τρέχον σύστημα πιστοποιητικών το οποίο βασίζεται σε smart cards θα αλλάξει. Δεν έχει επιλέγει νέος φορέας διατήρησης του πιστοποιητικού, αλλά οι συζητήσεις που διεξάγονται υποδεικνύουν την χρήση συσκευών τύπου USB memory.

[149] http://www.oberthur.com/content/179/identity

[150] http://www.charismathics.com/

## 6.3 Διακριτικά ταυτοποίησης Κινητών

Στην ενότητα αυτή θα αναλυθούν το ποια διακριτικά ταυτοποίησης μέσω κινητών τηλεφώνων χρησιμοποιούνται σε εφαρμογές ηλεκτρονικής διακυβέρνησης στις χώρες της Ευρώπης. Τα συστήματα αυτά περιλαμβάνουν μεθόδους πρόσβασης βασισμένες σε πιστοποιητικά και συστήματα one-time SMS message. Το κύριο προσδιοριστικό στοιχείο αυτής της κατηγορίας διακριτικών είναι ότι είναι αποδεκτά ως μέθοδοι αυθεντικοποίησης μέσα στις χώρες όπου χρησιμοποιούνται.

Στον πίνακα που ακολουθεί παρουσιάζονται οι λύσεις οι οποίες έχουνε υιοθετηθεί από τα διάφορα κράτη. Η έννοια της αυθεντικοποίησης μέσω συσκευών κινητής τηλεφωνίας είναι μία πολύ σημαντική έννοια, καθώς δεν απαιτείται επιπρόσθετο λογισμικό ή υλική υποδομή για την περίπτωση που ο πολίτης μετακινείται από σημείο σε σημείο.

Η φύση της φορητής συσκευής αυθεντικοποίησης παρουσιάζει τα πλεονεκτήματα ότι μέσω τη φορητής συσκευής μπορεί να καλυφθούν όλες οι προκλήσεις οι οποίες παρουσιάζονται ως προς το θέμα της αυθεντικοποίησης για ένα πολίτη ο οποίος καλείται να χρησιμοποιήσει την εν λόγω τεχνολογία, δηλαδή σε αυτή την περίπτωση έχουμε μία συσκευή η οποία μπορεί να μεταφέρει ως φορέας τα δεδομένα τα οποία χρειάζονται για την επίτευξη της ταυτοποίησης, ενώ ταυτόχρονα μπορεί να λειτουργήσει ως αναγνώστης των στοιχείων ταυτοποίησης, αλλά και ως μία ενδιάμεση συσκευή για τη διαβίβαση της απαραίτητης πληροφορίας.

Στον πίνακα που ακολουθεί περιλαμβάνονται:

- Το όνομα της χώρας
- Η στήλη **«Περιγραφή»** παρέχει το όνομα και κάποιες πληροφορίες σχετικά με το σύστημα που χρησιμοποιείται από την κάθε χώρα
- Η στήλη **«Ομάδα Χρηστών»** αναλύει τις λίστες των χρηστών οι οποίοι έχουν πρόσβαση στην εφαρμογή της πραγματικής λύσης
- Η στήλη **«Λεπτομέρειες/Χρήση Αυθεντικοποίησης»** παρέχει λεπτομερείς πληροφορίες σχετικά με τη χρήση των διακριτικών ταυτοποίησης μέσω των κινητών.

| Χώρα | Περιγραφή | Ομάδες Χρηστών | Λεπτομέρειες/ Χρήση Αυθεντικοποίησης |
|---|---|---|---|
| **Αυστρία** | Υπογραφές κινητών οι οποίες παρέχονται από όλους τους παρόχους τηλεπικοινωνιών | Κάθε συνδρομητής κινητής τηλεφωνίας | Από το 4$^{ο}$ τετράμηνο του 2009 η ταυτοποίηση μέσω κινητού τηλεφώνου είναι πλέον δυνατή σε αρκετές εφαρμογές ηλεκτρονικής διακυβέρνησης (όπως για παράδειγμα για τη δήλωση φόρου εισοδήματος), με τη χρήση αναγνωρισμένων πιστοποιητικών στα οποία ένα HSM[151] λειτουργεί ως ένα SSCD αποθηκεύοντας τα κλειδιά κρυπτογράφησης, καθιστώντας τη λύση μία εφαρμογή του πλαισίου της Αυστριακής Κάρτας του Πολίτη η οποία παράγει αναγνωρισμένες υπογραφές |
| **Εσθονία** | Mobile-ID | Εισήχθηκε στην Εσθονική αγορά τον Μάιο του 2007 από τον πάροχο τηλεπικοινωνιών EMT[152], ενώ από το δεύτερο μισό του 2009 δύο ακόμα πάροχοι κινητών επικοινωνιών, η Elisa και η Tele2, άρχισαν να παρέχουν Mobile-ID. | Προκειμένου να λάβει ο χρήστης το Mobile-ID, χρειάζεται να αντικαταστήσει την SIM κάρτα του με την κατάλληλη κάρτα η οποία υποστηρίζει δυνατότητα PKI. Παρόλο που η διαδικασία εγγραφής πραγματοποιείται από τον τηλεπικοινωνιακό φορέα, δεν θεωρείται αρκετά αξιόπιστο. Ως εκ τούτου ο χρήστης πρέπει να «ενεργοποιήσει» το Mobile-ID του με το δελτίο ταυτότητας του στο κατάλληλο web περιβάλλον[153]. Με αυτό τον τρόπο η έκδοση του Mobile-ID συνδέεται με την ασφάλεια και την ποιότητα του αντίστοιχου δελτίο ID που χρησιμοποιήθηκε για την ενεργοποίηση. |
| **Λιθουανία** | Mobile-ID | Δύο Λιθουανικοί πάροχοι κινητής τηλεφωνίας η “Bite Lietuva” και η “Omnitel” παρέχουν ηλεκτρονική ταυτοποίηση μέσω κινητών τηλεφώνων. Οι πελάτες των τραπεζών μπορούν να χρησιμοποιήσουν επίσης την λύση. | Οι πελάτες αυτών των παρόχων μπορούν να παραγγείλουν ηλεκτρονικές υπογραφές, υπογράφοντας την σχετική αίτηση για την υπηρεσία ηλεκτρονικής υπογραφής. Μετά από αυτό εκδίδεται στον πελάτη μία ειδική κάρτα SIM με εγκατεστημένη δυνατότητα κρυπτογράφησης και δύο ψηφιακά πιστοποιητικά: ένα πιστοποιητικό για τη σύνδεση και ένα πιστοποιητικό για την υπογραφή. Το πιστοποιητικό ηλεκτρονικής υπογραφής συμμορφώνεται με τις απαιτήσεις που θα πρέπει να έχει ένα αναγνωρισμένο πιστοποιητικό. |
| **Νορβηγία** | BankID[154] | Πρόκειται για μία υπηρεσία η οποία είναι διαθέσιμη σε πελάτες οι οποίοι | Το κλειδί αποθηκεύεται στην κάρτα SIM. Προκειμένου να συνδεθεί ένας χρήστης εισάγει |

[151] HSM: Hardware security module
[152] https://www.emt.ee/
[153] https://digidoc.sk.ee/?authType=mobile&c=EE
[154] https://www.bankid.no/

| | | | |
|---|---|---|---|
| | Buypass Mobile-ID | έχουν την Telenor ως πάροχο κινητής τηλεφωνίας.[155]<br><br>Η λύση δεν έχει συνδεθεί με ένα συγκεκριμένο πάροχο κινητής. Μπορούν επίσης να χρησιμοποιηθούν κάρτες SIM από το εξωτερικό. Η Norsk Tipping και οι χρήστες της μέσω διαδικτύου, ήταν οι πρώτοι χρήστες αυτής της εφαρμογής | τον αριθμό του κινητού τηλεφώνου και την ημερομηνία γέννησής του, και εμφανίζεται ένας κωδικός στην ιστοσελίδα και στο κινητό τηλέφωνο, οι οποίοι θα πρέπει να αντιστοιχούν ο ένας στον άλλο.<br><br>Δεν έχει καθοριστεί. Δουλεύει σε όλα τα κινητά τηλέφωνα τα οποία υποστηρίζουν Java. |
| **Ολλανδία** | DigiD / SMS[156] | Εγγεγραμμένοι χρήστες στο σύστημα DigiD | Μεσαίο επίπεδο αυθεντικοποίησης για χρήση στα συστήματα ηλεκτρονικής διακυβέρνησης. Ο κωδικός SMS μίας χρήσης αποστέλλεται στο κινητό τηλέφωνο του χρήστη |
| **Ουγγαρία** | Λύση SMS OTP[157] | Η ταυτοποίηση OTP είναι αρκετά κοινή μεταξύ των Ουγγρικών τραπεζών και το κράτος θεωρεί επίσης το SMS OTP ως μία λύση ταυτοποίησης | One-Time-Password logon σε τραπεζικές υπηρεσίες. Ο κωδικός στέλνεται στο χρήστη μέσω ενός μηνύματος SMS το οποίο από εκεί και έπειτα χρησιμοποιείται προκειμένου να εισέλθει στην εφαρμογή. |
| **Σλοβενία** | Αναγνωρισμένα πιστοποιητικά της Mobitel WPKI[158] | Η Mobitel παρέχει σε όλους τους ενδιαφερόμενους CSPs τη δυνατότητα να ολοκληρώσουν τα συστήματά τους με την λύση της και ήδη υπάρχουν CSPs οι οποίοι εκδίδουν πιστοποιητικά κινητών, αλλά αρκετοί άλλοι αντί να υποστηρίξουν τη λύση αναβαθμίζουν τα δικά τους συστήματα ούτως ώστε να είναι ικανοί να εκδίδουν και αυτοί τέτοιου είδους πιστοποιητικά | Τα κλειδιά για τα πιστοποιητικά του κινητού αποθηκεύονται σε μία κάρτα SIM την οποία φέρει το κινητό τηλέφωνο. |
| **Σουηδία** | BankID – σε συνεργασία με την Telia και την Telenor[159] | Πελάτες της Telenor και της Telia | eIDs οι οποίες είναι ολοκληρωμένες σε κάρτες SIM στο κινητό τηλέφωνο του χρήστη. Η χρήση αυτών των λύσεων κινητής ακόμα βρίσκεται στην φάση του καθορισμού των προδιαγραφών. |

**Πίνακας 16: Παρουσίαση χρησιμοποιούμενων τεχνολογιών eID μέσω κινητών τηλεφώνων**

[155] http://www.telenor.com/en/news-and-media/press-releases/2006/telenor-and-the-banking-industry-launch-bankid-for-mobile-phones
[156] http://www.digid.nl/english/
[157] OTP: One Time Password
[158] WPKI: Wireless PKI
[159] Πάροχοι υπηρεσιών κινητής τηλεφωνίας της Σουηδίας

Βασιζόμενοι στις εθνικές υποδομές με βάση τους ανωτέρω πίνακες, μπορούν να προκύψουν τα εξής συμπεράσματα:

- Από το σύνολο των 32 χωρών, οι 18 έχουνε συγκεκριμένες προδιαγραφές στο θέμα των διακριτικών ταυτοποίησης που είναι αποθηκευμένα σε κάποια hardware συσκευή.
- Από τις υπόλοιπες 14 χώρες, οι 2 έχουνε πραγματοποιήσει κάποιο σχεδιασμό καθορίζοντας τις προδιαγραφές για τις υλοποιήσεις των εν λόγω διακριτικών τους, ενώ τέλος
- Σε 13 από τις χώρες δεν υπάρχουν προδιαγραφές ή σχεδιασμός σε προχωρημένο επίπεδο σχετικά με την χρήση διακριτικών ταυτοποίησης που είναι αποθηκευμένα σε κάποια hardware συσκευή.
    - Γίνεται μνεία ότι αυτές οι χώρες διαθέτουν ενδεχόμενα κάποια σχέδια με πιο αναλυτικές προδιαγραφές, για τα οποία όμως δεν κατέστη δυνατόν να εντοπιστούν πηγές ή απλά δεν τα διαθέτουν σε κοινή χρήση.

- Από το σύνολο των 32 χωρών, οι 9 έχουνε κάποιο είδος αποδεκτού διακριτικού εκτός από τις κάρτες eID προκειμένου να ικανοποιούν τις ανάγκες της ταυτοποίησης των πολιτών στη χώρα τους.
    - 5 από αυτές τις χώρες χρησιμοποιούν κεντρικά παρεχόμενα συστήματα username/password.[160]
    - 7 από αυτές τις χώρες χρησιμοποιούν διακριτικά κινητών τηλεφώνων

[160] Συμπεριλαμβανομένης της λύσης των Government based paper tokens που χρησιμοποιεί η κυβέρνηση του Βελγίου. Πρόκειται για μία μικρή έντυπη κάρτα η οποία διαθέτει 24 κωδικούς και όπου η αυθεντικοποίηση είναι δύο παραγόντων: Ο χρήστης εισάγει το username και το password του και κατόπιν τούτου το σύστημα του ζητάει κάποιον συγκεκριμένο από τους 24 κωδικούς οι αναγράφονται στην κάρτα η οποία του έχει χορηγηθεί.

# 7. ΕΥΡΩΠΑΙΚΑ ΕΡΓΑ

## 7.1 Εισαγωγή

Όπως έγινε αντιληπτό από τα προηγούμενα κεφάλαια, στο θέμα των ηλεκτρονικών ταυτοτήτων επικρατεί ένας πλουραλισμός λύσεων και υλοποιήσεων ανάλογα με την πολιτική του κάθε κράτους. Αυτό μπορεί να είναι ενδιαφέρον, όσο ίσως και θεμιτό στα πλαίσια που το κάθε κράτος υλοποιεί συστήματα eIDM τα οποία είναι προσαρμοσμένα στις δικές του ανάγκες. Πέρα όμως από αυτό το πολύ θετικό στο θέμα των αυτόνομων λύσεων eIDM, υφίστανται και μία σειρά άλλων παραγόντων οι οποίοι ανάγουν σε εξίσου αρνητική την ανεξάρτητη αυτή ανάπτυξη συστημάτων.

Η Ευρωπαϊκή Ένωση αποτελεί ένα ενιαίο χωρικά γεωγραφικό χώρο ο οποίος καθορίστηκε μέσα από τη συνθήκη Σέγκεν και ο οποίος επιτρέπει την ελεύθερη μετακίνηση των πολιτών από χώρα σε χώρα. Σε αυτό το ενιαίο έδαφος οι πολίτες τείνουν όλο και περισσότερο να μετακινούνται με αποτέλεσμα να εξέρχονται των γεωγραφικών ορίων των χωρών τους. Μία άλλη όμως παράμετρος «ταξιδεύει» ακόμα πιο γρήγορα και συχνά από τους πολίτες. Πρόκειται για το εμπόριο για το οποίο η τάση είναι να πραγματοποιείται σε ολοένα και πιο διευρυμένα γεωγραφικά όρια ειδικά στη σημερινή εποχή και στα πλαίσια της επέκτασης του μέσω του e-commerce.

Απέναντι σε αυτές τις δύο πολύ σημαντικές προκλήσεις, υπάρχει μία σειρά από βασικές παραμέτρους οι οποίες πρέπει να υλοποιηθούν προκειμένου να επιτευχθούν οι σκοποί της ελεύθερης μετακίνησης των πολιτών και της διασυνοριακής παροχής υπηρεσιών και προϊόντων στα πλαίσια μίας ενιαίας αγοράς. Μία από αυτές είναι και η ταυτοποίηση των χρηστών, η οποία αν μεταφραστεί σε σημερινούς όρους, συνεπάγεται την ύπαρξη διαλειτουργικών συστημάτων διαχείρισης ηλεκτρονικών ταυτοτήτων τα οποία θα ταυτοποιούν τον χρήστη-πολίτη μίας χώρας σε όποια άλλη χώρα και αν βρίσκεται.

Προκειμένου να επέλθει όμως αυτή η διαλειτουργικότητα, ο φορέας ο οποίος συντονίζει τις διάφορες χώρες προκειμένου να επιτευχθεί αυτός ο σκοπός είναι η Ευρωπαϊκή Ένωση. Έτσι προγραμματίζονται μία σειρά από δράσεις, άλλες περισσότερο θεωρητικές και άλλες περισσότερο πρακτικές, σε επίπεδο εφαρμογών και ανάπτυξης ενιαίων πλατφόρμων υλοποίησης, προσπαθεί να εξυπηρετήσει την ενιαία πολιτική και τις επιδιώξεις που καθορίζει στα πλαίσια της σε κάθε περίοδο.

Στο θέμα των ηλεκτρονικών ταυτοτήτων υλοποιούνται μία σειρά από έργα τα οποία θα αναλυθούν στα πλαίσια του παρόντος κεφαλαίου και όλα

αυτά υλοποιούνται στη βάση μίας ενιαίας στρατηγικής, η οποία καθορίζεται περίπου κάθε 5 χρόνια και η οποία θα παρουσιαστεί επίσης.

## 7.2 eIDM Roadmap: Ο Χάρτης προς ένα Πανευρωπαϊκό πλαίσιο στο eIDM έως το 2010

### 7.2.1 Η ανάγκη δημιουργίας ενός ενιαίου χάρτη

Η στρατηγική του eIDM Roadmap[36] είναι βαθιά ριζωμένη στην στρατηγική της Λισαβόνας, την στρατηγική i2010, και το σχέδιο δράσης στην ηλεκτρονική διακυβέρνηση i2010[37], το οποίο υιοθετήθηκε το 2006. Ειδικά στο τελευταίο έγγραφο, η διαθεσιμότητα των λύσεων eIDM αναγνωρίστηκε ως βασικό στοιχείο το οποίο θα πρέπει να ικανοποιηθεί προκειμένου να επιτευχθούν οι στόχοι της στρατηγικής της Λισαβόνας, και του σχεδίου δράσης που απαιτούσε να παρθούν ορισμένες πρωτοβουλίες προκειμένου να επιτευχθεί ο στόχος αυτός. Ο πρώτος από αυτούς, προγραμματίστηκε για το 2006, και ήταν η δημιουργία ενός χάρτη ο οποίος θα έθετε μετρήσιμους στόχους και ορόσημα, ώστε να επιτευχθεί ένα Ευρωπαϊκό πλαίσιο στον τομέα του eIDM έως το 2010 βασισμένο στη διαλειτουργικότητα και την αμοιβαία αναγνώριση των εθνικών eIDM.

Ο κύριος σκοπός αυτού του χάρτη, ήταν ως εκ τούτου να ορίσει τα βήματα που έπρεπε να γίνουν προκειμένου να επιτευχθεί η Ευρωπαϊκή φιλοδοξία της επίτευξης της διαλειτουργικότητας μεταξύ των εθνικών λύσεων eID (άλλοτε βασισμένων σε smart cards, άλλοτε σε soft πιστοποιητικά, username/password συστήματα, κ.τ.λ.), ιδιαίτερα για τους σκοπούς της επίτευξης πρόσβασης σε εφαρμογές της ηλεκτρονικής διακυβέρνησης. Ήδη είχε σχεδιαστεί ένα αρχικό υψηλού επιπέδου χρονοδιάγραμμα στα eIDM στο έγγραφο Signposts[38] το οποίο προσδιορίζει ένα αριθμό κρίσιμων προς επίτευξη στοιχείων, συμπεριλαμβανομένης της ανάγκης να οριστεί ένα μοντέλο αυθεντικοποίησης και τα επίπεδα ασφάλειας, η αμοιβαία αναγνώριση των εθνικών eIDs, και η υλοποίηση ενός ομοσπονδιακού μοντέλου eIDM.

Ωστόσο το χρονοδιάγραμμα που παρουσιάστηκε στο Signposts ήταν προσωρινό, καθώς τα δομικά στοιχεία που περιελάμβανε δεν θεωρούνταν πλήρη και κατανοητά. Για το λόγο αυτό, το σχέδιο δράσης για την ηλεκτρονική διακυβέρνηση απαίτησε να καταρτισθεί ένα πιο λεπτομερής κατευθυντήριος χάρτης.

Εκείνη την εποχή, κάτω από την ομπρέλα του προγράμματος MODINIS[161] ορισμένες πρωτοβουλίες οι οποίες σχετιζόταν με το eIDM βρισκόταν ήδη στην αρχή του να εξετάσουν θέματα διαλειτουργικότητας μεταξύ των υφιστάμενων λύσεων εθνικών ταυτοτήτων και να παράσχουν συστάσεις και στρατηγικές για βελτίωση.

Ενώ οι ειδικές ανάγκες του σχεδίου δράσης για την ηλεκτρονική διακυβέρνηση δεν συμπεριλαμβανόταν ρητά στις μελέτες που πραγματοποιούνται στα πλαίσια του MODINIS, οι όροι αναφοράς θεωρήθηκαν πολύ ευρείς, και η ομάδα μελέτης κλήθηκε προκειμένου να προετοιμάσει ένα σχέδιο ενός κατευθυντήριου χάρτη. Έτσι στα πλαίσια του MODINIS ολοκληρώθηκε ο κατευθυντήριος χάρτης σε συνεργασία με την ομάδα μελέτης του SecurEgov[162] τον Δεκέμβριο του 2006. Το έγγραφο αυτό το οποίο δεν έχει τροποποιηθεί από τότε, υπέβαλλε συμπληρωματικά στοιχεία τα οποία θα έπρεπε να υλοποιηθούν, χρονικά ορόσημα και δράσεις οι οποίες χρειαζόταν να αναληφθούν προκειμένου να υλοποιηθούν οι φιλοδοξίες του σχεδίου δράσης.

### 7.2.2 Η παρούσα κατάσταση και βασικά χαρακτηριστικά

Το eID Roadmap, δημοσιεύτηκε στην ιστοσελίδα του DG INFSO[163] και αποτελείται από τρία βασικά μέρη:

- Μία εισαγωγή όπου σχολιάζονται οι στόχοι του Ευρωπαϊκού eIDM,
- Ένας κατευθυντήριος χάρτης όπου ορίζονται δομικά στοιχεία, ορόσημα κ.τ.λ. και
- Ένα παράρτημα όπου σχολιάζονται κάθε ένα από τα δομικά στοιχεία και εξηγείται η σημασία τους.

Αρχικά υπενθυμίζεται το ιστορικό των πολιτικών του κατευθυντήριου χάρτη, ενώ έπειτα ορίζονται οι βασικές αρχές οι οποίες θα πρέπει να τηρούνται από κάθε πρόταση η οποία έχει ως στόχο να βελτιώσει την διαλειτουργικότητα του eIDM σε Πανευρωπαϊκό επίπεδο προκειμένου να ορίσει τους περιορισμούς οι οποίοι θα πρέπει να τηρηθούν από τον κατευθυντήριο χάρτη. Κεντρική ανάμεσα τους είναι η αρχή της επικουρικότητας, το οποίο σημαίνει ότι τα κράτη

[161] Πολυετές πρόγραμμα το οποίο σχεδιάστηκε για την παρακολούθηση του σχεδίου δράσης eEurope 2005, τη διάδοση καλών πρακτικών και την βελτίωση της ασφάλειας των δικτύων και των επικοινωνιών (MODINIS), συστάθηκε μέσω της Απόφασης No 2256/2003/EC του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 17ης Νοεμβρίου 2003 που υιοθέτησε το MODINIS, βλ. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:02003D2256-20051227%20:EN:NOT και για μία συνολική επισκόπηση των δραστηριοτήτων του MODINIS, βλ. http://ec.europa.eu/information_society/eeurope/i2010/archive/modinis/index_en.htm

[162] SecurEgov: Security at the heart of eGovernment

[163] Βλ. http://ec.europa.eu/information_society/activities/egovernment/policy/key_enablers/eid/index_en.htm

μέλη θα πρέπει να διατηρήσουν την αυτονομία και την ευθύνη να επιδιώκουν τους δικούς τους στόχους για το eIDM χρησιμοποιώντας τα μέσα τα οποία θεωρούν κατάλληλα. Παρά την αρχή αυτή, η υιοθέτηση της Δήλωσης των Υπουργών στο Manchester υποδηλώνει ότι ορισμένες ελάχιστες απαιτήσεις θα πρέπει να θεσπιστούν και να ακολουθούνται από όλα τα εμπλεκόμενα μέρη. Ο τελικός στόχος είναι να δημιουργηθεί ένα διαλειτουργικό πλαίσιο το οποίο θα είναι αρκετά ελκυστικό για τους τελικούς χρήστες (και κυρίως από τους πολίτες) να εξασφαλίζει ότι θα το αγκαλιάσουν, παρά επειδή θα είναι ίσως αναγκασμένοι να το πράξουν.

Στον κατευθυντήριο χάρτη ορίζονται οι ακόλουθες αρχές σχεδιασμού ως κρίσιμοι για την ανάπτυξη ενός τέτοιου πλαισίου:

1. Οι εκτιμήσεις χρησιμοποίησης θα πρέπει να είναι ο πιο σοβαρός περιορισμός όταν δημιουργείται ένα πανευρωπαϊκό πλαίσιο για το eIDM. Αυτό σημαίνει ότι το σύστημα θα πρέπει να είναι ασφαλές, να υλοποιεί τις αναγκαίες προϋποθέσεις για την διασφάλιση της ιδιωτικότητας των χρηστών και η χρήση του να επιτρέπει το συντονισμό του με τοπικές προτεραιότητες και ευαισθησίες.

2. Κάθε κράτος μέλος θα πρέπει να είναι ικανό να ταυτοποιεί τους χρήστες του εντός των συνόρων του, εάν επιθυμεί να τους επιτρέψει να έχουν πρόσβαση σε υπηρεσίες eIDM στο εξωτερικό. Για το σκοπό αυτό, η συνεπής χρήση κατάλληλων αναγνωριστικών είναι απαραίτητη προκειμένου να επιτρέχει την ακριβή ταυτοποίηση και αυθεντικοποίηση της εκάστοτε οντότητας και να επιτρέψει την ανταλλαγή πληροφορίας μεταξύ των διοικήσεων στο βαθμό που κάτι τέτοιο απαιτείται για τους σκοπούς της ταυτοποίησης. Οι θεμελιώδεις απαιτήσεις για ένα σύστημα το οποίο ρυθμίζει τις ανάγκες των φυσικών προσώπων θα πρέπει επίσης να είναι επεκτάσιμο και για χρήση από νομικά πρόσωπα.

3. Κάθε κράτος μέλος θα πρέπει να εκδίδει για κάθε πολίτη όλα εκείνα τα μέσα να ταυτοποιεί και να αυθεντικοποιεί τον εαυτό του ηλεκτρονικά, εάν επιθυμεί να τους επιτρέπεται η πρόσβαση και οι ωφέλειες τις οποίες μπορεί να επωφεληθεί με την χρήση υπηρεσιών eIDM εκτός των συνόρων της χώρας του. Ένας χρήστης έχει την δυνατότητα να δράσει αυτόνομα και να κάνει χρήση των προσφερόμενων υπηρεσιών.

4. Κάθε Κράτος Μέλος θα πρέπει να παρέχει τα μέσα για τη διαχείριση των αρμοδιοτήτων επικοινωνίας και ταυτοποίησης για τους χρήστες που ταυτοποιούνται εντός των συνόρων του, εφόσον οι εν λόγω λειτουργίες

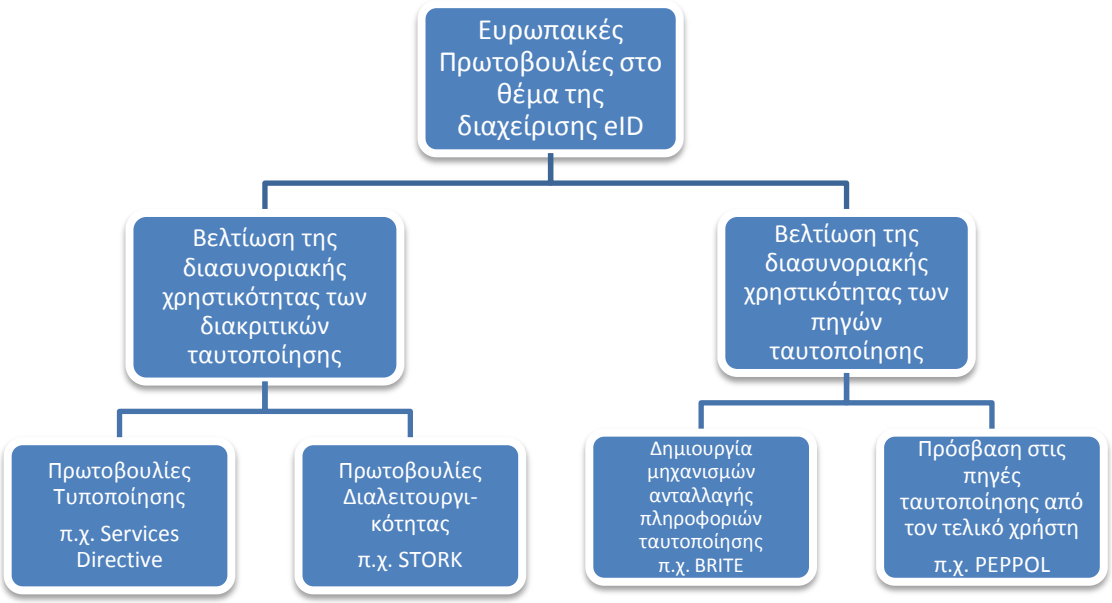
δεν υπόκεινται σε διαδικασία προηγούμενης έγκρισης από κάποιο άλλο Κράτος Μέλος.

5. Κάθε Κράτος Μέλος θα πρέπει να υποστηρίζει μηχανισμούς online ταυτοποίησης, διαχείρισης αρμοδιοτήτων και εντολών, αν επιθυμεί να παράσχει υπηρεσίες eIDM.

6. Θα πρέπει να καθιερώνεται η συναίνεση σε πολύ υψηλό επίπεδο μεταξύ των κρατών μελών σχετικά με την ορολογία στο eIDM προκειμένου να εξασφαλίζεται η εννοιολογική και σημασιολογική διαλειτουργικότητα. Προκειμένου να επιβεβαιωθεί αυτή η συναίνεση μπορεί να χρησιμοποιείται η κατά περίπτωση απαιτούμενη κατάλληλη πολιτική ή ενδεχόμενα ακόμη και τα κατάλληλα νομικά μέτρα.

Οι παραπάνω αρχές οι οποίες τίθενται σε επίπεδο σχεδιασμού δίνουν ιδιαίτερη έμφαση στις συνέπειες από την εφαρμογή της αρχής της επικουρικότητας. Πιο συγκεκριμένα αναφέρεται ότι οι ευρύτερες Ευρωπαϊκές πρωτοβουλίες που λαμβάνονται δεν θα πρέπει να απαγορεύουν στα κράτη μέλη να αναπτύξουν λύσεις οι οποίες θα είναι καλά προσαρμοσμένες στις δικές τους ιδιαίτερες ανάγκες, ενώ τα κράτη μέλη θα πρέπει να διατηρούν τον έλεγχο των τοπικών υποδομών eIDM, συμπεριλαμβανομένων της επιλογής και της χρήσης των στοιχείων ταυτοποίησης, των χαρακτηριστικών γνωρισμάτων τους και των εντολών των συστημάτων τους. Η κύρια υποχρέωση που επιβλήθηκε στα κράτη μέλη, είναι το καθήκον τους να διασφαλίσουν ότι αυτές οι υποδομές είναι λειτουργικές: θα πρέπει να είναι ικανά να ταυτοποιούν μοναδικά και/ή να αυθεντικοποιούν τους πολίτες και της επιχειρήσεις οι οποίοι βρίσκονται εντός των συνόρων τους, χρησιμοποιώντας ηλεκτρονικά μέσα, και να καθορίζουν τις εξουσιοδοτήσεις τους ή τις εντολές στις περιπτώσεις που κάτι τέτοιο απαιτείται. Γίνεται έτσι σαφές ότι οι αρχές που τίθενται δίνουν μία σαφή κατεύθυνση προς ένα ομόσπονδο σύστημα ενιαίας χρήσης.

Προκειμένου να συντονίσει τις ενέργειες αυτές η Ευρωπαϊκή Ένωση στην προσπάθεια υλοποίησης αυτού του χάρτη, εκπόνησε μία σειρά από έργα και δράσεις τα οποία κατηγοριοποιούνται ως εξής:




**Σχήμα 1: Προσεγγίσεις για την βελτίωση των eIDM πρακτικών στην Ευρώπη[39]**

Στις ενότητες που ακολουθούν θα παρουσιαστούν τα κυριότερα έργα και δράσεις οι οποίες υλοποιούνται, κάποιες από τις οποίες απεικονίζονται και στην παραπάνω σχηματική αναπαράσταση. Η σειρά που θα ακολουθηθεί είναι η χρονολογική, καθώς κάποια από τα έργα λαμβάνουν ως input τα παραδοτέα των έργων που προηγήθηκαν.

## 7.3 FIDIS

Το έργο FIDIS[164] ή αλλιώς «Το Μέλλον των ταυτοτήτων στην Κοινωνία της Πληροφορίας»[165] είναι ένα μεγάλο έργο το οποίο υλοποιήθηκε από το 2004 έως τον Μάρτιο του 2009 στα πλαίσια του EU FP6 Network of Excellence[166], και εστιάστηκε σε διάφορες πτυχές της ψηφιακής ταυτότητας και της ιδιωτικότητας. Οι συνεργάτες στα πλαίσια του έργου ήταν πανεπιστήμια και εταιρείες οι οποίοι εργάζονταν στις περιοχές οι οποίες σχετίζονταν με την ψηφιακή ταυτότητα. Οι περιοχές ενδιαφέροντος του FIDIS περιελάμβαναν νέες μορφές για τα δελτία ταυτότητας, χρήση χαρακτηριστικών γνωρισμάτων ταυτοποίησης σε πληροφοριακά συστήματα, τεχνολογίες οι οποίες χρησιμοποιούνταν για την ταυτοποίηση των πολιτών και συνόψεις των βασικών χαρακτηριστικών στις διάφορες χώρες.

Οι δραστηριότητες καλύπτουν:

[164] FIDIS: Future od Identity in the Information Society
[165] http://www.fidis.net
[166] http://cordis.europa.eu/fp6/instr_noe.htm

- «ταυτότητα της ταυτότητας» (ορισμοί όρων κλειδιών στον υπό μελέτη τομέα,
- Προφίλ χωρών και συστημάτων
- Διαλειτουργικότητα των IDs και των συστημάτων διαχείρισης ταυτοτήτων.
- Επιπτώσεις της εγκληματικότητα στα συστήματα Ταυτοποίησης
- Πλαίσιο ιδιωτικότητα και νομικό-κοινωνικό περιεχόμενο των ταυτοτήτων
- ID υψηλής τεχνολογίας
- Φορητότητα και Ταυτότητα

Το FIDIS έχει παράσχει ένα πλήθος δημοσιεύσεων στην διαφοροποιούμενη «φύση» της ταυτότητας προς την ψηφιοποίηση της και δημοσιεύσεις σχετικά με προβλέψεις επί ενδεχόμενων σεναρίων για το μέλλον της ταυτότητας. Αυτό συμπεριλαμβάνει σημαντικό έργο στο θέμα της «μερικής ταυτοποίησης» ή αλλιώς personae[167][40]. Το FIDIS ξεκίνησε το 2004, και ενώ τεχνικά έχει ολοκληρωθεί από το 2008, συνέχισε να παραδίδει παραδοτέα έως και το 2ο εξάμηνο του 2009.

## 7.4 PRIME

Το PRIME είναι ένα έργο στα πλαίσια του EU FP6, που ξεκίνησε τον Ιούνιο του 2004[168]. Το PRIME είχε ως 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 PETs[169] και της ενδεχόμενης συμβολής τους σε μία κοινωνία της πληροφορία βασισμένη στην εμπιστοσύνη. Προκειμένου να προωθήσει την αποδοχή από την αγορά, οι καινοτόμες λύσεις για τη διαχείριση ταυτοτήτων οι οποίες προτεινόταν, ελέγχθηκαν σε δύσκολα πραγματικά σενάρια, όπως για παράδειγμα οι Επικοινωνίες μέσω Διαδικτύου, οι Διαδικασίες τις οποίες υλοποιούν οι πελάτες των Αεροπορικών Εταιρειών, Υπηρεσίες οι οποίες βασίζονται στη γεωγραφική θέση όπου βρίσκεται το άτομο, και συνεργατικό e-learning.

[167] Ο όρος μερική ταυτοποίηση αναφέρεται στη δυνατότητα που δίνεται από μεμονωμένα στοιχεία, τα οποία υπάρχουν διαθέσιμα για ένα άτομο στο Internet και τα οποία δεν είναι ικανά να ταυτοποιήσουν το άτομο, να συλλεχθούν, με ένα κατάλληλο τρόπο να αλληλοσυσχετισθούν και έτσι τελικά να φτάσει η πληροφορία αυτή η πρώην «κατακερματισμένη» πληροφορία να είναι πολύ πιο ποιοτική για κάθε άτομο, προσδιορίζοντας το.
[168] https://www.prime-project.eu/
[169] PETs: Privacy Enhancing Technologies

Το PRIME ήταν πρώτιστα ένα ερευνητικό έργο. Η δραστηριότητα του πάνω στο θέμα της ανάπτυξης του πρωτοτύπου ήταν ένα μέσο για την επικύρωση των νέων επιστημονικών και ερευνητικών αποτελεσμάτων του. Η δουλειά που έγινε με το PRIME συνεχίζεται τώρα από το PRIMELife, το οποίο συνιστά τη συνέχεια του έργου PRIME.

## 7.5 PRIMELife

Ο διάδοχος του PRIME, το PRIMElife[170] είναι ένα έργο το οποίο χρηματοδοτείται από το FP7 και ασχολείται με την έρευνα του πυρήνα της ιδιωτικότητας και των θεμάτων εμπιστοσύνης. Στόχος του προγράμματος είναι να διευκολύνει την ανωνυμία σε δεδομένα τα οποία διατηρούνται για όλη τη διάρκεια της ζωής του ατόμου, χωρίς να δίνεται η εντύπωση ότι πραγματοποιούνται για την επίτευξη της διατήρησής τους συμβιβασμοί σε επίπεδο λειτουργιών του συστήματος. Προκειμένου να επιτευχθεί αυτό, το PRIMELife θα επικεντρώσει σε περιοχές των διεπαφών του ανθρώπου με τους υπολογιστές , διαμορφώσιμες γλώσσες πολιτικής, ομοσπονδιακές υπηρεσίες μέσω web, υποδομές και κρυπτογραφία η οποία θα ενισχύει την ιδιωτικότητα. Οι κοινότητες ανοιχτού κώδικα και οι φορείς προτυποποίησης θα παροτρυνθούν να υιοθετήσουν τις τεχνολογίες αυτές οι οποίες προστατεύουν την ιδιωτική ζωή. Το έργο ξεκίνησε το 2009 και βρίσκεται ακόμα στα πρώτα του στάδια, αλλά παραμένοντας ταυτόχρονα πολύ χρήσιμο πάνω στο θέμα της διαλειτουργικότητας στον τομέα των eIDs.

## 7.6 IDABC: eID interoperability for PEGS

Τα αρχικά IDABC[171] είναι τα αρχικά της φράσης «Διαλειτουργική Παροχή Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης στην Ευρώπη», προς δημόσιες διοικήσεις, Επιχειρήσεις και Πολίτες[172]. Το IDABC χρησιμοποίησε τις δυνατότητες που προσφέρθηκαν από τις ΤΠΕ προκειμένου να ενθαρρύνει την παροχή διασυνοριακά παρεχόμενων υπηρεσιών σε επιχειρήσεις και πολίτες σε Ευρωπαϊκό επίπεδο, να αυξήσει την αποτελεσματικότητα και τη συνεργασία μεταξύ των Ευρωπαϊκών δημόσιων διοικήσεων και να συμβάλλει στο να καταστεί η Ευρώπη ένα ελκυστικό μέρος για να ζεις, να εργάζεσαι και να επενδύεις.

[170] http://www.primelife.eu/
[171] IDABC: Interoperable Delivery of European eGovernment Services
[172] Βλ. http://ec.europa.eu/idabc/

Στα πλαίσια αυτού του οράματος, υλοποιήθηκε το υποέργο eID Interoperability for PEGS[173] το οποίο ξεκίνησε το 2005 και ολοκληρώθηκε το 2009, συνεχίζοντας να παραδίδει παραδοτέα έως και τον Φεβρουάριο του 2010.[174] Ο σκοπός του προγράμματος ήταν να ασχοληθεί με τα ηλεκτρονικά δελτία ταυτότητας ή άλλες λύσεις διαχείρισης ταυτότητας τις οποίες είχανε αναπτύξει τα προηγούμενα χρόνια τα διάφορα κράτη μέλη. Αυτά τα συστήματα ταυτοποίησης θα έπρεπε να είναι ικανά να ταυτοποιούν και ηλεκτρονικά τον κάθε χρήστη, έτσι ώστε να μπορεί αυτός να γίνει αποδέκτης από εκεί και έπειτα των ευεργετημάτων και των λοιπών υπηρεσιών οι οποίες προσφερόταν γι' αυτόν σε εθνικό επίπεδο μέσω των υπηρεσιών ηλεκτρονικής διακυβέρνησης με τη χρήση ψηφιακών πιστοποιητικών. Από εκεί και έπειτα θα έπρεπε να κριθεί το κατά πόσο οι λύσεις αυτές θα μπορούσαν να υποστηρίξουν τη διαλειτουργική ανταλλαγή υπηρεσιών και πληροφοριών μεταξύ των διαφόρων δημόσιων διοικήσεων των διαφόρων κρατών μελών.

## 7.7 BRITE

Το έργο BRITE[175] είναι ένα έργο το οποίο χρηματοδοτείται από την Ευρωπαϊκή Ένωση και περιλαμβάνει μία κοινοπραξία οργανισμών, συμπεριλαμβανομένων Μητρώων Επιχειρήσεων εντός της Ευρώπης, εμπορικά επιμελητήρια, πανεπιστήμια και εταιρείες. Φτιάχτηκε προκειμένου να αναπτυχθεί ένα διαλειτουργικό μοντέλο ροής εργασιών το οποίο θα επέτρεπε στα Μητρώα Επιχειρήσεων να ανταλλάσουν δεδομένα και πληροφορίες σε όλη την Ευρωπαϊκή Ένωση. Το BRITE θα αναπτύξει μία ενιαία πλατφόρμα πληροφοριών, επικοινωνιών και τεχνολογίας βασισμένη στο μοντέλο ροής δεδομένων και θα υλοποιήσει ένα τρόπο λειτουργίας ο οποίος θα επιτρέπει στα Μητρώα Επιχειρήσεων να αλληλεπιδρούν σε ολόκληρη την πλατφόρμα.

Το μοντέλο του BRITE, η πλατφόρμα και τα μέσα που αυτό προσφέρει θα επεκτείνουν τη διαλειτουργικότητα μεταξύ των Μητρώων Επιχειρήσεων, των επιχειρήσεων, και άλλων δημόσιων υπηρεσιών και θα βοηθήσουν τα Μητρώα Επιχειρήσεων να εξελιχθούν αφομοιώνοντας το Ευρωπαϊκό Εταιρικό Δίκαιο.

Στα πλαίσια του BRITE ένα από τα σημαντικότερα θέματα θα είναι η ψηφιακή υπογραφή των εγγράφων η οποία θα καθορίζει και την αμοιβαία αναγνώριση και την ισχύ αυτών, στην προσπάθεια των εταιρειών να αναζητήσουν και να αξιοποιήσουν δημόσια προσβάσιμα στοιχεία από τα

[173] PEGS: Pan European Government Services
[174] http://ec.europa.eu/idabc/en/document/6484.html
[175] Βλ. http://www.briteproject.eu/ (Στοιχεία μόνο στα Γερμανικά)

μητρώα των διαφόρων χωρών προκειμένου να υλοποιήσουν στη συνέχεια τις εμπορικές συναλλαγές τους.

## 7.8 CROBIES

Το CROBIES[176] είναι μία μελέτη την οποία εκπόνησε η Ευρωπαϊκή Επιτροπή με τίτλο «Μελέτη στη Διασυνοριακή Διαλειτουργικότητα των Ηλεκτρονικών Υπογραφών». Το αντικείμενο αυτής της μελέτης, όπως περιγραφικά αναφέρεται και από τον τίτλο ήταν η μελέτη των ηλεκτρονικών υπογραφών όταν αυτές τίθενται σε ένα πλαίσιο εκτός των εθνικών συνόρων του κάθε Ευρωπαϊκού κράτους.[177] Στόχος του ήταν να προτείνει λύσεις προκειμένου να αρθούν οι περιορισμοί στη διασυνοριακή διαλειτουργικότητα των ηλεκτρονικών υπογραφών και των προηγμένων ηλεκτρονικών υπογραφών οι οποίες βασίζονται σε αναγνωρισμένα πιστοποιητικά.

Το CROBIES βασίστηκε και έλαβε υπόψη του τις σχετικές διατάξεις της Οδηγίας 1999/93/ΕΚ καθώς και τις εθνικές εφαρμογές της, όπως επίσης και τις διαδικασίες προτυποποίησης οι οποίες πραγματοποιήθηκαν με βάση την εν λόγω Οδηγία.

Το CROBIES πρότεινε επίσης βελτιώσεις σε νομικό και τεχνικό επίπεδο, όσο και σε επίπεδο εμπιστοσύνης ως προς το θέμα των ηλεκτρονικών υπογραφών.

Η Ευρωπαϊκή επιτροπή ξεκίνησε τη μελέτη του CROBIES υποστηρικτικά προς το Σχέδιο Δράσης των ηλεκτρονικών υπογραφών και της ηλεκτρονικής ταυτοποίησης. Η μελέτη ξεκίνησε τον Αύγουστο του 2008 και ολοκληρώθηκε τον Ιούνιο του 2010.[178]

Οι σχετικές προσπάθειες στα πλαίσια του CROBIES με μία συνιστώσα του το eIDM δεν σχετίζονται κατά κύριο λόγο σε ζητήματα τα οποία αφορούν κατά κύριο λόγο στη διαχείριση ταυτότητας, όπως εφαρμόζεται με τον υπογράφοντα, αλλά με το περιεχόμενο και τη δομή της εγκεκριμένων πιστοποιητικών υπογραφής στο σύνολό τους. Ως εκ τούτου, το έργο CROBIES αποσκοπεί στην θέσπιση μίας καλύτερης και πιο εναρμονισμένης υλοποίησης του προτύπου TS 102 280 (X.509 V.3 Πιστοποιητικό Προφίλ για Πιστοποιητικά τα οποία

[176] CROBIES: Cross-Border Interoperability of eSignatures

[177] Βλ. http://ec.europa.eu/information_society/policy/esignature/crobies_study/index_en.htm

[178] Μία από τις σημαντικότερες συνεισφορές του ήταν η συμμετοχή του στον καθορισμό των όρων της εντολής M460 η οποία εκδόθηκε από την Ευρωπαϊκή Επιτροπή και αναφέρεται στις ηλεκτρονικές υπογραφές, η οποία απευθύνεται προς τους Ευρωπαϊκούς Οργανισμούς Προτυποποίησης ηλεκτρονικών υπογραφών.

εκδίδονται από φυσικά πρόσωπα[179]). Μία από τις αναμενόμενες κύριες επιπτώσεις θα είναι η υποχρεωτική χρήση ενός εναρμονισμένου serial Number στο πεδίο Θέμα του πιστοποιητικού, το οποίο θα εξασφαλίζει ότι τουλάχιστον μία πηγή είναι διαθέσιμη προκειμένου να καταστεί εφικτή η ταυτοποίηση του υπογράφοντος. Θα πρέπει να έχουμε κατά νου ωστόσο, ότι το έργο αυτό αναμένεται να επηρεάσει άμεσα τα εγκεκριμένα πιστοποιητικά και ότι το serial Number ως τέτοιο ίσως δεν θα μπορεί να είναι άμεσα χρησιμοποιήσιμος πόρος σε κάθε δεδομένη εφαρμογή ηλεκτρονικών υπογραφών. Έτσι, από την οπτική αυτή, η συμβολή του έργου CROBIES είναι πολύ σημαντική προκειμένου να τακτοποιηθούν σημασιολογικά θέματα τα οποία σχετίζονται με την ταυτότητα και την ικανότητα των υπογραφόντων προς ενέργεια.

## 7.9 PEPPOL

Το PEPPOL[180] (2008-2011), έχει ως στόχο την εφαρμογή κοινών προτύπων τα οποία θα επιτρέψουν την πραγματοποίηση ηλεκτρονικών δημόσιων προμηθειών σε ένα ευρύ Ευρωπαϊκό επίπεδο.[181] 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. Το PEPPOL λειτουργεί στα πλαίσια του προγράμματος της Ευρωπαϊκής Επιτροπής για την Ανταγωνιστικότητα και την Καινοτομία, και στα πλαίσια του υποστηρικτικού προγράμματος για ICT Policy.

Το ευρύτερο όραμα του PEPPOL είναι οποιαδήποτε εταιρεία στην Ευρώπη να μπορεί να επικοινωνεί ηλεκτρονικά με οποιοδήποτε Ευρωπαϊκό κυβερνητικό φορέα για την προ-ανάθεση της σύμβασης και μετά την ανάθεση για τις υπόλοιπες ενέργειες της προμήθειας. Το PEPPOL θα επιτρέπει σε οποιοδήποτε προμηθευτή μέσα στην Ευρωπαϊκή Ένωση να ανταποκρίνεται σε οποιαδήποτε Ευρωπαϊκή δημόσια προσφορά για την πραγματοποίηση κάποιας προμήθειας το οποίο συνεπάγεται τη χρησιμοποίηση των υφιστάμενων εθνικών υποδομών τους.

### 7.9.1 Ψηφιακές Υπογραφές

Για την επίτευξη του σκοπού αυτού, μία από τις έννοιες η οποία θα πρέπει να λυθεί, να υλοποιηθεί και να λειτουργεί με ένα ενιαίο διαλειτουργικό τρόπο είναι αυτή της ηλεκτρονικής υπογραφής.

[179] Βλ. σχετικά http://www.etsi.org/WebSite/Technologies/ElectronicSignature.aspx
[180] PEPPOL: Pan-European Public Procurement Online
[181] http://www.peppol.eu/

Ήδη βρίσκονται σε χρήση ηλεκτρονικές υπογραφές οι οποίες βασίζονται σε ηλεκτρονικά πιστοποιητικά τα οποία ταυτοποιούν εταιρείες ή ακόμη και μεμονωμένα άτομα. Επιτρέπουν την ασφαλή ταυτοποίηση του αποστολέα ενός εγγράφου και διασφαλίζουν ότι ένα έγγραφο δεν έχει τροποποιηθεί. Το PEPPOL αποσκοπεί να δημιουργήσει διαλειτουργικότητα μεταξύ των διαφορετικών εθνικών σχημάτων, έτσι ώστε στην πράξη μία οντότητα του δημόσιου τομέα να μπορεί να επικυρώνει πιστοποιητικά τα οποία εκδόθηκαν σε κάποιο άλλο κράτος μέλος, επιτρέποντας την ηλεκτρονική προσφορά υπηρεσιών πέρα από τα σύνορα.

PEPPOL & eSignatures

Οι εργασίες υλοποίησης του έργου PEPPOL στα πλαίσια του WP1[182], διακρίνονται σε 4 φάσεις. Στην παρούσα φάση οι δύο ενεργές φάσεις είναι η 3 και η 4.

Οι φάσεις υλοποιούνται ως εξής:

- 1η φάση: Proof of concept (03/2009 – 09/2009)
- 2η φάση: Beta test (10/2009 – 01/2010)
- 3η φάση: System scale up (11/2009 – 04/2010)
- 4η φάση: Roll out phase/pilot (04/2010 – 10/2011)

## 7.10 STORK

### 7.10.1 Σύνοψη

Το STORK[183] (2008-2011)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%. Αποτελεί το σημαντικότερο έργο στον τομέα των eIDM το οποίο βρίσκεται αυτή την περίοδο σε εξέλιξη. Σκοπεύει να υλοποιήσει ένα ευρείας έκτασης Ευρωπαϊκό διαλειτουργικό σύστημα για την αναγνώριση eIDs και αυθεντικοποίηση, το οποίο θα επιτρέψει στις επιχειρήσεις, στους πολίτες και στους κρατικούς λειτουργούς να χρησιμοποιούν τις εθνικές ηλεκτρονικές τους ταυτότητες σε οποιοδήποτε Κράτος Μέλος. Επίσης στα πλαίσια του ελέγχονται οι υπηρεσίες ταυτοποίησης στην ηλεκτρονική διακυβέρνηση σε διασυνοριακό επίπεδο και προκύπτει το πώς στην πράξη πλέον θα πρέπει να εισάγονται

[182] WP1: Work Package 1 – αναφέρεται στο θέμα των eSignatures
[183] http://www.eid-stork.eu/

αντίστοιχες υπηρεσίες, και να παρέχεται η εμπειρία σχετικά με τα οφέλη και τις προκλήσεις που θα μπορούσε να φέρει ένα ευρείας έκτασης Ευρωπαϊκό διαλειτουργικό σύστημα για αναγνώριση eIDs.

### 7.10.2 Στόχοι

Η λύση διαλειτουργικότητας του STORK για τις ηλεκτρονικές ταυτότητες βασίζεται σε μία κατανεμημένη αρχιτεκτονική η οποία θα ανοίξει τον δρόμο προς την πλήρη ολοκλήρωση στις Ευρωπαϊκές ηλεκτρονικά παρεχόμενες υπηρεσίες, λαμβάνοντας υπόψη τις τρέχουσες προδιαγραφές και υποδομές των Ευρωπαϊκών χωρών. Ο στόχος είναι να απλοποιηθούν οι διοικητικές διαδικασίες με το να παρέχεται ασφαλής on line πρόσβαση στις δημόσιες υπηρεσίες κατά μήκος της Ευρωπαϊκής Ένωσης. Η λύση που παρέχεται πρόκειται να είναι ιδιαίτερης βαρύτητας, διαφανής, ασφαλής στη χρήση και επεκτάσιμη, και θα πρέπει να υλοποιηθεί κατά τέτοιο τρόπο ώστε να είναι βιώσιμη μετά το πέρας του προγράμματος.

### 7.10.3 Δράσεις

Στα πλαίσια των δράσεων του έργου περιλαμβάνονται τα εξής:

- Να αναπτύξει κοινούς κανόνες και προδιαγραφές προς την κατεύθυνση της επίτευξης αμοιβαίας αναγνώρισης των eIDs πέρα από τα εθνικά σύνορα των χωρών
- Να ελέγξει, σε πραγματικό περιβάλλον, ασφαλής και εύκολες να χρησιμοποιηθούν λύσεις eID για τους πολίτες και τις επιχειρήσεις
- Να αλληλεπιδράσει με άλλα προγράμματα της Ευρωπαϊκής Ένωσης προκειμένου να μεγιστοποιηθεί η χρησιμότητα των υπηρεσιών ηλεκτρονικής ταυτοποίησης

### 7.10.4 Αποτελέσματα

Το STORK παίρνει πολλές εφαρμογές και τις φιλτράρει σε ένα σύνολο από αρχιτεκτονικές δυνατότητες, οι οποίες απλοποιούν τη διαλειτουργικότητα των συστημάτων ID των κρατών μελών. Το πιλοτικό ρεαλιστικό πρόγραμμα το οποίο υλοποιείται στα πλαίσια του STORK και στο οποίο θα συμμετέχουν και πάροχοι υπηρεσιών ταυτοποίησης του ιδιωτικού τομέα, αναμένεται να τεθεί σε επιχειρησιακή χρήση το 2011 τελευταία χρονιά του προγράμματος STORK.

### 7.10.5 Εμπλεκόμενοι Φορείς

Οι βασικοί εμπλεκόμενοι φορείς του έργου είναι:

α) Εταιρείες του ιδιωτικού τομέα οι οποίες δραστηριοποιούνται πάνω στα eID οι οποίες συνεργάζονται μέσω του STORK Industry Group

β) Άλλες Ευρωπαϊκές Δημόσιες Διοικήσεις, οι οποίες είναι μέλη του Member State Reference Group

γ) Άλλα μεγάλης κλίμακας Ευρωπαϊκά έργα στο θέμα των eID και

δ) Υπηρεσίες A2A[184] της Ευρωπαϊκής Επιτροπής όπως η ECAS[185].

Ως εκ τούτου το STORK δεν έχει ανταγωνιστές, καθώς πρόκειται για ένα έργο το οποίο χειρίζεται από τον δημόσιο τομέα. Παρ' όλα αυτά οι εμπορικές λύσεις στον τομέα των eID θα μπορούσαν να επισκιάσουν κάπως τις προσπάθειες των δημόσιων διοικήσεων, εάν η συνταύτιση δεν θα επιτευχθεί με επιτυχία[1].

## 7.11 Δράσεις στο πεδίο eIDM 2011-2015

Προκειμένου να καταστεί δυνατή η ασφαλής και αποτελεσματική ηλεκτρονική συνεργασία μεταξύ των κρατών μελών της Ευρωπαϊκής Ένωσης, πρέπει να πληρούνται μία σειρά από προϋποθέσεις. Σε αυτό το πλαίσιο οι δράσεις που προγραμματίζονται για την επόμενη πενταετία, περιλαμβάνουν την ανάπτυξη, εγκατάσταση και τη διαλειτουργικότητα των υποδομών ΤΠΕ. Μεγάλη προσοχή δίνεται επίσης στο θέμα των οφελών από την ύπαρξη ανοιχτών προδιαγραφών, ως μέσο για την προώθηση της διαλειτουργικότητας, προκειμένου να βελτιωθούν οι υφιστάμενες και να αναπτυχθούν νέες υπηρεσίες, καθώς επίσης και στην καινοτομία των υπηρεσιών της ηλεκτρονικής διακυβέρνησης μέσω της έρευνας και της ανάπτυξης, καθώς επίσης και σε πιλοτικά προγράμματα και άλλα σχέδια υλοποίησης[21].

Πιο συγκεκριμένα στις προτεραιότητες για τα έτη 2011 έως και 2015, αναφέρεται ότι στο σχέδιο δράσεων 4.2 για την ηλεκτρονική διακυβέρνηση υπάρχουν τρεις δράσεις οι οποίες άπτονται άμεσα του θέματος των ηλεκτρονικών ταυτοτήτων. Πιο αναλυτικά :

[184] A2A: Administration to Administration
[185] ECAS: European Commission Authentication Service

- Δράση 35 : Αναθεώρηση της Οδηγίας για τις Ηλεκτρονικές Υπογραφές για τη διασυνοριακή αναγνώρισης και διαλειτουργικότητα των συστημάτων ασφαλούς ηλεκτρονικής αυθεντικοποίησης[186]

- Δράση 36: Απόφαση για να εξασφαλιστεί η αμοιβαία αναγνώριση της ηλεκτρονικής ταυτοποίησης και της ηλεκτρονικής αυθεντικοποίησης[187]

- Δράση 37: Ανάπτυξη και εφαρμογή λύσεων ηλεκτρονικής ταυτοποίησης[188]

[186] Η υλοποίηση της δράσης αυτής τοποθετείται για το 2011.

[187] Η Επιτροπή θα προτείνει μία Απόφαση του Συμβουλίου και του Ευρωπαϊκού Κοινοβουλίου προκειμένου να εξασφαλίσει την αμοιβαία αναγνώριση των ηλεκτρονικών ταυτοτήτων και της ηλεκτρονικής αυθεντικοποίησης σε ολόκληρη την Ευρωπαϊκή Ένωση, στη βάση των on-line υπηρεσιών αυθεντικοποίησης οι οποίες προσφέρονται σε όλα τα Κράτη Μέλη (οι οποίες μπορούν να χρησιμοποιούν τα πλέον κατάλληλα επίσημα έγγραφα ταυτοποίησης – τα οποία θα έχουνε εκδοθεί είτε από φορείς του δημόσιου, είτε του ιδιωτικού τομέα. Η υλοποίηση της δράσης αυτής έχει προγραμματιστεί για το έτος 2012.

[188] Τα Κράτη Μέλη θα πρέπει να αναπτύξουν και να εφαρμόσουν τις κατάλληλες λύσεις ηλεκτρονικής ταυτοποίησης, βασισμένα στα αποτελέσματα του προγράμματος STORK και άλλων έργων σχετιζόμενων με τις ηλεκτρονικές ταυτότητες. Η υλοποίηση της δράσης αυτής έχει προγραμματιστεί για το χρονικό διάστημα από το 2012 έως και το 2014.

# 8. ΤΟ ΓΕΡΜΑΝΙΚΟ ΠΑΡΑΔΕΙΓΜΑ … ΠΙΛΟΤΟΣ ΓΙΑ ΤΗΝ ΕΛΛΗΝΙΚΗ ΠΡΑΓΜΑΤΙΚΟΤΗΤΑ (;)

## 8.1 Εισαγωγή

Το παράδειγμα της Γερμανίας, αποτελεί ένα παράδειγμα εθνικής λύσης eIDM το οποίο επιλέχθηκε προκειμένου να παρουσιασθεί σε εκτενέστερο βαθμό, εξ' αιτίας της συνάφειας την οποία εμφανίζει με το αντίστοιχο ελληνικό δελτίο eID (κάρτα του πολίτη), το οποίο αυτή τη στιγμή βρίσκεται στην φάση της δημόσιας διαβούλευσης.

Η Ελλάδα υλοποιώντας τη σχετική υποδομή της από το 2010 και έπειτα, είχε το περιθώριο να επιλέξει μεταξύ των διαφόρων εναλλακτικών προσεγγίσεων στο θέμα του eIDM των διαφόρων Ευρωπαϊκών κρατών μελών, σταθμίζοντας τα οφέλη και τις παραμέτρους που η κάθε μία από τις διάφορες λύσεις παρουσιάζει.

Μία από τις 3 εναλλακτικές λύσεις-προσεγγίσεις οι οποίες εξετάζονται, λαμβάνει υπ' όψη της το σενάριο της Γερμανικής υλοποίησης για τα δελτία eID, με πολύ σημαντικές πιθανότητες τελικής επιλογής για υλοποίηση. Το νέο αυτό δελτίο εισήχθηκε στο στάδιο της επιχειρησιακής λειτουργίας από την 1η Νοεμβρίου 2010.

## 8.2 Χρήσεις του eID δελτίου

Το Γερμανικό eID δελτίο ενσωματώνει περισσότερη λειτουργικότητα από ότι το προϋπάρχον συμβατικό δελτίο ID.Οι χρήσεις του συνοψίζονται στα εξής:

**Internet ID:** Τα δεδομένα του δελτίου ID τα οποία στο προηγούμενο δελτίο ήταν οπτικά αναγνώσιμα επάνω στο ID δελτίο, αποθηκεύονται πλέον στο ID chip, επιτρέποντας στους χρήστες να ταυτοποιούν τους εαυτούς τους online όταν συναλλάσσονται με κυβερνητικές αρχές, όπως επίσης και με παρόχους εμπορικών υπηρεσιών του ιδιωτικού τομέα, όπως για παράδειγμα όταν πραγματοποιούν αγορές on-line ή όταν συναλλάσσονται με τράπεζες επίσης online. Σε ένα διευρυμένο δηλαδή πλαίσιο λειτουργίας το νέο δελτίο eID, δεν αποτελεί μία υποδομή η οποία να αξιοποιείται μόνο για σκοπούς ηλεκτρονικής διακυβέρνησης, αλλά αξιοποιείται επίσης και για χρήση σε εμπορικές δραστηριότητες.

Την ίδια ώρα, οι κάτοχοι των καρτών μέσω των μηχανισμών ασφάλειας οι οποίοι έχουνε ενσωματωθεί στο eID δελτίο, γνωρίζουν ότι σε όποια περίπτωση κάποιος αιτείται των δεδομένων τους, θα έχει προηγουμένως εξουσιοδοτηθεί προκειμένου να πραγματοποιήσει κάτι τέτοιο.
Αυτό καθιστά το νέο δελτίο, πιο οικονομικό και πιο ασφαλές στο άνοιγμα και στη σύνδεση με τους λογαριασμούς του χρήστη, όπως επίσης και στην διαδικασία επιβεβαίωσης πληροφοριών σχετικές με τη διεύθυνση και την ηλικία του χρήστη.
Παρέχει επιπλέον προστασία ενάντια στην πλαστοπροσωπία, και νέους, φιλικούς προς τον χρήστη τρόπους προκειμένου να προστατευτούν οι νέοι, όπως για παράδειγμα με το να αποτρέπει ανήλικους κατόχους eIDs από το να αγοράζουν τσιγάρα από αυτόματα σημεία πώλησης, μέσω της ηλεκτρονικής ταυτοποίησής τους.

**Ηλεκτρονική Υπογραφή:** Στους κατόχους δελτίων eID δίνεται η δυνατότητα να «φορτώσουν» μία αναγνωρισμένη ηλεκτρονική υπογραφή στο δελτίο ID τους την οποία θα μπορούν να χρησιμοποιούν σε εφαρμογές ηλεκτρονικής διακυβέρνησης και ηλεκτρονικού επιχειρείν.

**Ασφαλές ταξιδιωτικό έγγραφο:** Προκειμένου να διασφαλιστεί ότι τα εθνικά δελτία ID συνεχίζουν να αποτελούν ασφαλή ταξιδιωτικά έγγραφα, το εθνικό δελτίο e-ID, όπως το ηλεκτρονικό διαβατήριο, διαθέτει βιομετρικά δεδομένα ταυτοποίησης αποθηκευμένα στο τσιπ το οποίο πληροί τις απαιτήσεις για τους επίσημους ελέγχους ταυτότητας – και τα οποία θα χρησιμοποιούνται μόνο γι' το σκοπό αυτό. Όλα τα δελτία eID διαθέτουν μία ψηφιακή φωτογραφία, και οι κάτοχοι μπορούν επίσης να επιλέξουν να συμπεριλάβουν στο τσιπ προαιρετικά δύο ψηφιακά δακτυλικά αποτυπώματα[41]. Και τα δύο αναγνωριστικά ταυτότητας συνιστούν ένα αποτελεσματικό τρόπο προκειμένου να αυξηθεί η ασφάλεια των ελέγχων ταυτότητας και είναι ιδιαίτερα χρήσιμα στην καταπολέμηση της κακόβουλης χρήσης εγγράφων ταυτοποίησης από πρόσωπα τα οποία μοιάζουν εμφανισιακά με τον κάτοχο του δελτίου ή προσαρμόζουν την εμφάνισή τους με σκοπό να πράξουν κάτι τέτοιο.[189]

**Πορεία των εργασιών υλοποίησης του eID δελτίου:** Το γενικό πλαίσιο υλοποίησης για την εισαγωγή των ηλεκτρονικών δελτίων ταυτότητας, εκδόθηκε το 2008 και συζητήθηκε με τους εκπροσώπους των καταναλωτικών οργανώσεων, της αρχής προστασίας δεδομένων, της επιχειρηματικής και

[189] Βλ. https://www.bsi.bund.de/cln_165/ContentBSI/EN/Topics/ElectrIDDocuments/eIDcard/eIDcard_Start.html

ερευνητικής κοινότητας σε κοινά workshops και εκδηλώσεις πληροφόρησης οι οποίες οργανώθηκαν.

Το Ομοσπονδιακή Υπουργικό Συμβούλιο ενέκρινε το σχέδιο νόμου για τις ταυτότητες και την ηλεκτρονική απόδειξη της Ταυτότητας[190] της 23 Ιουλίου 2008. Τελικά ο νόμος ψηφίσθηκε από τη Βουλή στις 18 Δεκεμβρίου 2008 και εγκρίθηκε από την κάτω Βουλή του κοινοβουλίου την 23 Φεβρουαρίου 2009. Σε συνέχεια αυτών ακολούθησε δημοσίευση του σχετικού νόμου, ενώ οριστικοποιήθηκαν και οι τεχνικές προδιαγραφές των eID δελτίων[191].

Από την 1η Νοεμβρίου 2010 τα δελτία eID αποτελούν μία πραγματικότητα για το Γερμανικό κράτος, και η σχετική διαδικασία έκδοσης τέθηκε επίσημα σε επιχειρησιακή λειτουργία.

## 8.3 Ποια δεδομένα καταγράφονται στην κάρτα

Όταν υποβάλλεται μία αίτηση για την χορήγηση ενός δελτίου eID, καταγράφονται τα εξής δεδομένα για κάθε πολίτη:

Επίθετο, Όνομα, Επίπεδο Διδακτικής Επάρκειας (διδακτικών γνώσεων π.χ. κάτοχος PhD, MSc κ.τ.λ.), Ημερομηνία και Τόπος γέννησης, Φωτογραφία, Υπογραφή, Ύψος, Χρώμα Ματιών, Διεύθυνση, Εθνικότητα, Σειριακός Αριθμός και Θρησκευτικό Όνομα.

Το σύνολο των εν λόγω στοιχείων υφίστανται και στο δελτίο eID.

Στο πίσω μέρος του δελτίου, βρίσκεται μία ζώνη μηχαναγνώσιμου κώδικα τριών γραμμών (MRZ), η οποία μπορεί να διαβαστεί με σύστημα OCR[192].

Στο RF chip περιλαμβάνονται όλα τα στοιχεία της μηχαναγνώσιμης ζώνης, όλα τα τυπωμένα στοιχεία συμπεριλαμβανομένου του ύψους, του χρώματος των ματιών και της υπογραφής, καθώς και τα δακτυλικά αποτυπώματα αν κάτι τέτοιο αποτελεί επιθυμία του πολίτη.

[190] The draft Act on Identity Cards and Electronic Proof of Identity and to Amend Further Provisions
[191] Η αρχή η οποία οριστικοποίησε τις τεχνικές προδιαγραφές είναι το Federal Office of Information Security (BSI).
[192] OCR: Optical Character Recognition

## 8.4 Προστασία από μη εξουσιοδοτημένη πρόσβαση

Τα προσωπικά δεδομένα των πολιτών τα οποία περιλαμβάνονται στο eID δελτίο του καθενός, προστατεύονται από την μη εξουσιοδοτημένη χρήση ως εξής:

Δεν υφίσταται κεντρικοποιημένη βάση αποθήκευσης των δεδομένων που αποθηκεύονται στο ηλεκτρονικό δελτίο ταυτότητας. Στα μητρώα ταυτοτήτων αποθηκεύονται μόνο τα δεδομένα τα οποία αποθηκευόταν από τις αρχές έκδοσης ταυτοτήτων όπως και πριν από την εισαγωγή των ηλεκτρονικών δελτίων ταυτότητας (δηλαδή τα προσωπικά δεδομένα και η εικόνα του προσώπου). Τα δακτυλικά αποτυπώματα – εάν το επιθυμεί ο κάτοχος της κάρτας –αποθηκεύονται μόνο στο RF chip και προσωρινά κατά τη διάρκεια της διαδικασίας κατασκευής της κάρτας. Τα δακτυλικά αποτυπώματα τα οποία απαιτούνται για την καταχώρηση και κατασκευή του δελτίου ID διαγράφονται μετά από την παραγωγή του. Αυτό απαιτείται από την §26[193] του Γερμανικού Νόμου για το Εθνικό Δελτίο Ταυτότητας[194]. Τέλος κρίσιμο είναι να αναφερθεί από πλευράς πολιτικής που εφαρμόστηκε, ότι επιλέγηκε η «πολιτοκεντρική» προσέγγιση δίνοντας το δικαίωμα στους χρήστες να καθορίζουν με τη συναίνεσή τους το σε ποιες εφαρμογές και ποια από τα δεδομένα τους θα μπορούν κάθε φορά να διαθέτουν.

Για την προστασία των δεδομένων των πολιτών τα οποία βρίσκονται αποθηκευμένα στο δελτίο eID, υφίσταται μία σειρά μηχανισμών ψηφιακής ασφάλειας οι οποίοι εξασφαλίζουν ότι τα δεδομένα στο ηλεκτρονικό δελτίο ID μπορούν να διαβαστούν μόνο από εξουσιοδοτημένα προς τούτο πρόσωπα. Επίσης εξασφαλίζεται, ότι αυτά τα εξουσιοδοτημένα πρόσωπα, έχουν πρόσβαση μόνο στα δεδομένα τα οποία τους αφορούν.

Οι μηχανισμοί ασφαλείας στο δελτίο eID έχουνε τους ακόλουθους αντικειμενικούς σκοπούς:

- **Προστασία δεδομένων:** Πρώτα απ' όλα θα πρέπει να εξασφαλιστεί η προστασία των προσωπικών δεδομένων του κατόχου της κάρτας έναντι μη εξουσιοδοτημένης χρήσης.
- **Αυθεντικότητα & Προστασία έναντι της πλαστογραφίας:** Κατά δεύτερον, θα πρέπει να εξασφαλιστεί ότι το δελτίο eID έχει εκδοθεί από ένα κυβερνητικό ίδρυμα και ότι μπορεί να ανιχνευθεί μία πιθανή παραποίηση του περιεχομένου του δελτίου.

[193] Βλ. http://bundesrecht.juris.de/pauswg/index.html
[194] Personalausweisgesetz

### 8.4.1 Επίπεδα μηχανισμού ασφάλειας

Τα δεδομένα που υπάρχουν στο RF chip ασφαλίζονται μέσω ενός μηχανισμού ασφάλειας τριών επιπέδων:

- Μέσω ψηφιακής υπογραφής η οποία πιστοποιεί αφενός ότι τα κωδικοποιημένα στοιχεία είναι γνήσια και αφετέρου την χώρα που έχει εκδώσει το eID δελτίο. Το πιστοποιητικό αυτό αποθηκεύεται και αυτό εντός του eID δελτίου και είναι το επονομαζόμενο **"document signer certificate"**, από όπου μπορεί να προκύψει η γνησιότητα των περιεχόμενων δεδομένων.
- Προστασία ενάντια οποιασδήποτε μη εξουσιοδοτημένης ανάγνωσης ("skimming") μέσω των μηχανισμών ελέγχου εκτεταμένης πρόσβασης (EAC), ένα ασφαλές πρωτόκολλο πρόσβασης και του μηχανισμού ελέγχου PACE οι οποίοι αναλύονται στη συνέχεια.
- Τα δεδομένα κλειδώνονται κάνοντας χρήση Υποδομής Δημοσίου Κλειδιού (PKI), το οποίο παρέχει προστασία κατά οποιασδήποτε τροποποίησης κωδικοποιημένων δεδομένων. Το PKI είναι η τεχνολογία ψηφιακής κρυπτογράφησης, η οποία επιτρέπει την επικύρωση των δεδομένων ως προς την γνησιότητα τους και εμφανίζει οποιαδήποτε αλλαγή - προσθήκη ή διαγραφή στο chip του δελτίου eID.

Στη συνέχεια ακολουθεί μία παρουσίαση των πρωτοκόλλων και άλλων μέτρων ασφάλειας, τα οποία χρησιμοποιούνται προκειμένου να υποστηριχτούν οι πτυχές ασφάλειας που προαναφέρθηκαν. Προκειμένου να καταστεί δυνατή η σύγκριση αναφέρεται και ο μηχανισμός BAC, ο οποίος αποτελεί το ελάχιστο στάνταρ ασφάλειας το οποίο έχει καθιερωθεί για την προστασία των στοιχείων τα βρίσκονται αποθηκευμένα στα ηλεκτρονικά Travel Documents της Ευρωπαϊκής Ένωσης.

| Συντομογραφία | Τίτλος | Πεδίο Εφαρμογής |
|---|---|---|
| **BAC**[195] | Basic Access Control | Ο Βασικός Έλεγχος Πρόσβασης προστατεύει το RF chip |

[195] Basic Access Control: Πρόκειται για ένα μηχανισμό, ο οποίος μπορεί να εξασφαλίσει ότι μόνο εξουσιοδοτημένα μέρη μπορούν ασύρματα να διαβάσουν προσωπικά δεδομένα από ένα έγγραφο το οποίο φέρει ένα RFID chip. Χρησιμοποιεί δεδομένα όπως ο αριθμός του διαβατηρίου, η ημερομηνία γέννησης και η ημερομηνία λήξης προκειμένου να δημιουργηθεί ένα κλειδί συνόδου. Αυτό το κλειδί μπορεί στη συνέχεια να χρησιμοποιηθεί προκειμένου να κρυπτογραφηθεί η επικοινωνία μεταξύ του chip του διαβατηρίου και της συσκευής ανάγνωσης. Έτσι μόνο όποιος έχει πρόσβαση σε αυτές τις πληροφορίες προκειμένου να δημιουργήσει το «κλειδί» μπορεί να εγκαθιδρύσει ένα ασφαλές κανάλι επικοινωνίας μεταξύ του τσιπ του διαβατηρίου και της συσκευής ανάγνωσης. Το κείμενο και οι παράμετροι οι οποίες απαιτούνται για την δημιουργία του κλειδιού, πραγματοποιούνται μέσω ενός OCR συστήματος το οποίο μπορεί να διαβάσει συγκεκριμένα δεδομένα από το δελτίο eID, μέσω της MRZ ζώνης την οποία ήδη διαθέτει πάνω του. Ο μηχανισμός παραμένει στην απλή του μορφή πολύ λίγο ασφαλής, μιας και οι πιθανοί συνδυασμοί των αριθμών διαβατηρίων που έχουνε εκδοθεί, καθώς επίσης και των ημερομηνιών γέννησης των ατόμων τα οποία συνήθως ταξιδεύουν, μπορεί να τον κάνει πολύ ευάλωτο σε επιθέσεις τύπου Brute-force. Στη βασική του μορφή, η επικοινωνία

| | | |
|---|---|---|
| | | ενάντια στο skimming[196]. Με BAC προστατεύονται πολλά ταξιδιωτικά έγγραφα. Ακόμη και η Γερμανία χρησιμοποιεί τον εν λόγω μηχανισμό προστασίας στα διαβατήρια τα οποία εκδίδει. |
| **PACE** | Password Authenticated Connection Establishment | Έλεγχος Πρόσβασης, προστατεύει το RF chip ενάντια στο skimming. Αποτελεί και τον τρόπο προστασίας ο οποίος έχει ενσωματωθεί στα Γερμανικά eID δελτία. |
| **EAC** | Extended Access Control[197] | Ο έλεγχος εκτεταμένης πρόσβασης, αποτελείται από διάφορα πρωτόκολλα. Όπως ορίζεται στην Ευρωπαϊκή Ένωση διακρίνεται στο "Chip Authentication" και στο "Terminal Authentication". |
| | CA: Chip Authentication | Δημιουργείται ένας ασφαλής δίαυλος επικοινωνίας (ισχυρότερος από αυτόν που δημιουργείται με τον BAC) και εντοπίζει τα "κλωνοποιημένα" RF chips. Η CA ανήκει στο πρωτόκολλο EAC |
| | TA: Terminal Authentication | Αυθεντικοποίηση της συσκευής ανάγνωσης για πρόσβαση σε ευαίσθητα προσωπικά δεδομένα τα οποία βρίσκονται στο RF chip. Η TA ανήκει στο πρωτόκολλο EAC |
| **PA** | Passive Authentication | Επαληθεύεται η αυθεντικότητα και η ακεραιότητα(μη παραποίηση) των δεδομένων τα οποία βρίσκονται στο RF chip |
| **PKI** | Public Key Infrastructure | Ιεραρχία των ψηφιακών πιστοποιητικών |
| | CSCA: Country Signing Certification Authority | Ιεραρχία των ψηφιακών πιστοποιητικών τα οποία χρησιμοποιούνται για την υπογραφή δεδομένων στα eID |
| | CVCA: Country Verifying Certification Authority | Ιεραρχία των ψηφιακών πιστοποιητικών σχετικά με τα δικαιώματα ανάγνωσης των eID |

**Πίνακας 17: Μηχανισμοί Ασφάλειας Γερμανικού Δελτίου eID**

### 8.4.2 PACE

Το PACE[198] είναι ο μηχανισμός ο οποίος χρησιμοποιείται προκειμένου να εξασφαλίσει ότι το RFID chip στο δελτίο eID δεν μπορεί να αναγνωστεί από απόσταση και ότι τα δεδομένα που ανταλλάσσονται με τη συσκευή ανάγνωσης μεταδίδονται κρυπτογραφημένα. Το PACE αποτελεί το μηχανισμό ο οποίος έχει επιλεγεί στο θέμα αυτό για την υλοποίηση του γερμανικού eID δελτίου, έναντι του BAC.

---

υλοποιείται ως εξής: Όταν το chip βρεθεί πάνω στη συσκευή ανάγνωσης, διαβιβάζει ένα τυχαίο αριθμό στη μηχανή ανάγνωσης. Η συσκευή ανάγνωσης κρυπτογραφεί αυτό τον αριθμό χρησιμοποιώντας το κλειδί πρόσβασης και στη συνέχεια το διαβιβάζει πίσω στο RF chip. Το RF chip ελέγχει αν ο τυχαίο αριθμός, έχει κρυπτογραφηθεί με το σωστό κλειδί πρόσβασης. Εάν κάτι τέτοιο όντως συμβαίνει, το RF chip επιτρέπει στην συσκευή να αποκτήσει πρόσβαση στα δεδομένα που περιέχει, όπως για παράδειγμα την εικόνα του προσώπου, το όνομα, την ημερομηνία γέννησης, κ.λπ.

[196] Πρόκειται για τον τύπο επίθεσης ο οποίος υλοποιείται μέσω της προσπάθειας ανάγνωσης περιεχομένων από απόσταση με μη εξουσιοδοτημένο τρόπο.

[197] Υπάρχουν πολλές διαφορετικές υλοποιήσεις του μηχανισμού, οι οποίοι επιτρέπουν στο EAC να εφαρμοστεί παράλληλα με το BAC το οποίο είναι υποχρεωτικό στην Ευρωπαϊκή Ένωση.

[198] Password Authenticated Connection Establishment

Το ποιος κωδικός μπορεί να χρησιμοποιηθεί από το PACE εξαρτάται από το ψηφιακό πιστοποιητικό της συσκευής ανάγνωσης. Συνήθως αυτό είναι ο εξαψήφιος «Προσωπικός Αριθμός Ταυτοποίησης» PIN[199], ο οποίος είναι γνωστός μόνο στον κάτοχο του δελτίου ταυτότητας και εισάγεται από αυτόν.

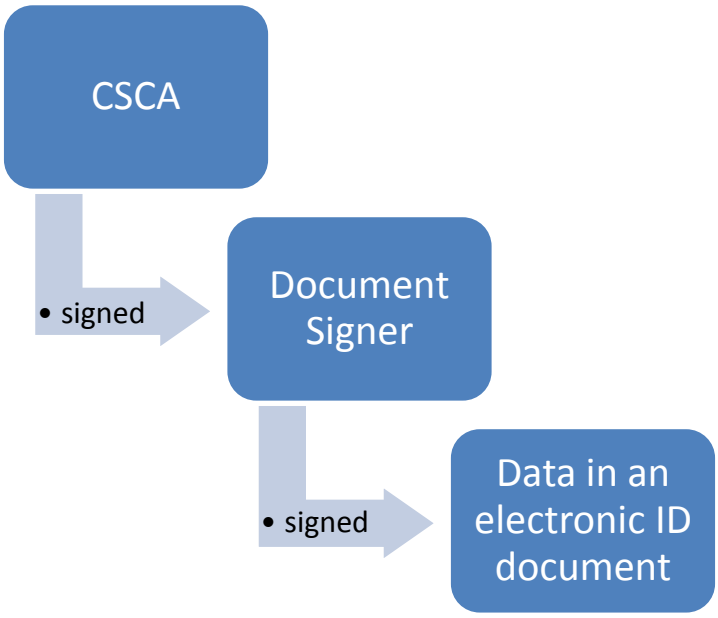
Για συσκευές ανάγνωσης με ψηφιακά πιστοποιητικά χρήση σε επίσημα σημεία όπου απαιτείται αυθεντικοποίηση, όπως είναι ο διαβατηριακός έλεγχος στα σύνορα, αρκούνε ακόμη και η μηχαναγνώσιμη ζώνη (MRZ) η οποία είναι τυπωμένη στο πίσω μέρος του δελτίου eID ή το εξαψήφιο «Card Access Number» (CAN) το οποίο είναι τυπωμένο στην μπροστινή πλευρά της ταυτότητας.

Ο μηχανισμός PACE είναι ένα πρωτόκολλο τύπου Diffie-Hellman, το οποίο παρέχει ασφαλή επικοινωνία μέσω προσυμφωνημένου κλειδιού μεταξύ του RFID chip και του τερματικού βάσης[42]. Το PACE έχει το πλεονέκτημα ότι το μήκος του κωδικού, δεν έχει επίπτωση στο επίπεδο ασφάλειας της κρυπτογράφησης. Αυτό σημαίνει ότι ακόμη και με το μικρό σε μέγεθος – σε αντίθεση με το MRZ – PIN ή CAN τα δεδομένα τα οποία περιέχονται στο RF chip του eID δελτίου είναι προστατευμένα σε πολύ μεγάλο βαθμό και κατά τη διάρκεια της μετάδοσης.

### 8.4.3 Passive Authentication

Τα δεδομένα τα οποία αποθηκεύονται στο RF chip είναι ψηφιακά υπογεγραμμένα κατά τη διάρκεια της διαδικασίας παραγωγής του eID δελτίου. Για το σκοπό αυτό, χρησιμοποιείται το επονομαζόμενο “document signer certificate”, το οποίο είναι με τη σειρά του υπογεγραμμένο με το CSCA (Country Signer Certificate Authority) πιστοποιητικό της εκδούσας χώρας και το οποίο είναι διαθέσιμο μόνο στον εκδότη στον οποίο επίσημα έχει ανατεθεί η έκδοση των εν λόγω δελτίων της χώρας. Το πιστοποιητικό αυτό αποτελεί τη ρίζα του CSCA-PKI (Country Signer Certificate Authority Public Key Infrastructure), και από εκεί και έπειτα προκύπτει μία ιεραρχία για τα πιστοποιητικά προκειμένου να αποδειχθεί η αυθεντικότητα των δεδομένων τα οποία περιέχονται στο eID δελτίο[43].

[199] Personal Identification Number




**Σχήμα 2: Ιεραρχία Πιστοποιητικών στη Γερμανική Signer Certificate Authority PKI υποδομή για eID**

Κατά την διάρκεια της ανάγνωσης ενός δελτίου eID η υπογραφή που έχουν τα δεδομένα που βρίσκονται αποθηκευμένα στο RF chip ελέγχονται και οδηγούνται πίσω στο CSCA πιστοποιητικό χρησιμοποιώντας την Παθητική Αυθεντικοποίηση. Με τον τρόπο αυτό μπορεί να προσδιορισθεί, εάν ο επίσημος εκδότης των δελτίων eID έχει αποθηκεύσει τα δεδομένα στο δελτίο eID μέσα στο RF chip, και αν τα δεδομένα είναι αυθεντικά.

### 8.4.4 EAC

Το EAC αποτελεί ένα εξειδικευμένο μηχανισμό ο οποίος επιτρέπει την ανάγνωση των δεδομένων μόνο σε εξουσιοδοτημένα συστήματα ελέγχου (συστήματα τα οποία χρησιμοποιούνται προκειμένου να διαβάσουν δελτία eID) τα οποία διαβάζουν ευαίσθητα βιομετρικά δεδομένα όπως τα δακτυλικά αποτυπώματα από τα eIDs. Το EAC χρησιμοποιούνταν σε συνδυασμό με το μηχανισμό BAC, κάτι το οποίο πλέον έχει τροποποιηθεί, και ως εκ τούτου τα βιομετρικά δεδομένα όπως τα δακτυλικά αποτυπώματα τα οποία δεν είναι εύκολο να προκύψουν με κάποιο άλλο τρόπο, εκτός από την μη εξουσιοδοτημένη πρόσβαση, κρυπτογραφούνται με συνδυασμό EAC και PACE[43].

Ο έλεγχος εκτεταμένης πρόσβασης, αποτελείται από διάφορα πρωτόκολλα. Όπως ορίζεται στην Ευρωπαϊκή Ένωση διακρίνεται στο “Chip Authentication” και στο “Terminal Authentication”.

#### 8.4.4.1 Chip Authentication

Με το **Chip Authentication** δημιουργείται ένας ασφαλής δίαυλος επικοινωνίας (ισχυρότερος από αυτόν που δημιουργείται με τον BAC) και εντοπίζει τα "κλωνοποιημένα" RF chips.

Ένα ειδικό ζεύγος κλειδιών αποθηκεύεται σε κάθε RF chip του δελτίου ταυτότητας, προκειμένου να υποστηριχθεί αυτό το πρωτόκολλο. Αυτό το ζεύγος αποτελείται από ένα δημόσιο και ένα ιδιωτικό κλειδί. Το ιδιωτικό κλειδί αποθηκεύεται σε μία συγκεκριμένη περιοχή του RF chip, από την οποία δεν μπορεί να αναγνωστεί. Το ιδιωτικό μάλιστα αυτό κλειδί δεν είναι δυνατόν να αντιγραφεί ακόμη και αν κλωνοποιηθεί ολόκληρο το τσιπ (αντιγραφή).

Κατά της διάρκεια του Chip authentication, το δημόσιο κλειδί στέλνεται στον αναγνώστη μαζί με ένα τυχαίο αριθμό. Ο αναγνώστης επίσης παράγει ένα ιδιωτικό ζεύγος κλειδιών, το οποίο αποτελείται από ένα δημόσιο και ένα ιδιωτικό κλειδί, για κάθε διαδικασία ανάγνωσης. Το δημόσιο κλειδί του το διαβιβάζει στο RF chip. Τώρα και το RF chip και ο αναγνώστης μπορούν να υπολογίσουν το ίδιο μυστικό κλειδί με το δικό τους ιδιωτικό κλειδί, το δημόσιο κλειδί του άλλου και τον τυχαίο αριθμό. Το μυστικό αυτό εξασφαλίζει την ισχυρή κρυπτογράφηση κατά τη διάρκεια της υπόλοιπης επικοινωνίας μεταξύ του RF chip και του αναγνώστη.

Με τη βοήθεια του διαμοιραζόμενου μυστικού κλειδιού, ο αναγνώστης μπορεί τώρα να ελέγξει το κατά πόσο το τσιπ έχει το σωστό ιδιωτικό κλειδί ή όχι. Ένα κλωνοποιημένο τσιπ μπορεί να μην έχει το αυθεντικό ιδιωτικό κλειδί. Εάν χρησιμοποιεί ένα διαφορετικό ιδιωτικό κλειδί, ο διαμοιραζόμενος κωδικός θα είναι λανθασμένος. Εάν δημιουργηθεί ένα καινούργιο ζεύγος κλειδιών για το κλωνοποιημένο RF chip, αυτό θα μπορούσε να ανιχνευθεί κατά τη διάρκεια της Παθητικής Αυθεντικοποίησης (PA), επειδή το δημόσιο κλειδί είναι προστατευμένο από πραγματοποιούμενες αλλαγές επ' αυτού μέσω ψηφιακής υπογραφής.

#### 8.4.4.2 Terminal Authentication

Με το **Terminal Authentication** πραγματοποιείται αυθεντικοποίηση της συσκευής ανάγνωσης για πρόσβαση σε ευαίσθητα προσωπικά δεδομένα τα οποία βρίσκονται στο RF chip και τα οποία δεν θα πρέπει να είναι προσβάσιμα σε μη εξουσιοδοτημένα άτομα.

Τα ευαίσθητα προσωπικά δεδομένα μπορούν να διαβαστούν μόνο όταν το πρωτόκολλο Terminal Authentication, εκτελείται επιτυχώς στη μεριά του αναγνώστη.

Το RF chip του ID δελτίου είναι σχεδιασμένο έτσι ώστε να επιτρέπει ορισμένα από τα δεδομένα που περιέχει να διαβάζονται μόνο όταν ο αναγνώστης μπορεί να αποδείξει ένα ρητό δικαίωμα ανάγνωσης ακριβώς για αυτά τα δεδομένα (όπως για παράδειγμα την ημερομηνία γέννησης). Προκειμένου να επιτραπεί στο RF chip να επαληθεύσει αυτή την άδεια, το CVCA[200] πιστοποιητικό αποθηκεύεται σε αυτό. Το πιστοποιητικό αυτό αποτελεί την ρίζα του CV PKI[201], μία ιεραρχία από εξουσιοδοτημένα πιστοποιητικά για την ανάγνωση ευαίσθητων δεδομένων στα έγγραφα ID.

Κατά τη διάρκεια του Terminal Authentication, ο αναγνώστης διαβιβάζει τα δικαιώματα πρόσβασής του στο RF chip στη μορφή ενός terminal certificate[202]. Επιπρόσθετα ο αναγνώστης διαβιβάζει επίσης το CVCA πιστοποιητικό και όλα τα πιστοποιητικά τα οποία βρίσκονται μεταξύ αυτών των δύο πιστοποιητικών στην ιεραρχία των πιστοποιητικών. Τα πιστοποιητικά είναι έγκυρα σε όλες τις περιπτώσεις για περιορισμένη χρονική περίοδο και τα οποία μπορούν ελεύθερα να ανακαλούνται σε περίπτωση που κάτι τέτοιο κριθεί αναγκαίο. Προκειμένου να τα προμηθευτούν οι ενδιαφερόμενοι πάροχοι υπηρεσιών (χωρίς αυτό να περιορίζεται σε υπηρεσίες eGovernment) και προκειμένου να καταστεί εφικτή η διαβίβαση των επιθυμητών δεδομένων, αιτείται εξουσιοδότηση πρόσβασης στα απαιτούμενα δεδομένα, διενεργείται επαλήθευση των στοιχείων, σχετικά με το ποια δεδομένα όντως χρειάζεται ο πάροχος των υπηρεσιών για τον σκοπό που τα ζητάει από το δελτίο ID και το αν είναι αξιόπιστος. Με τον τρόπο αυτό το RF chip μπορεί να επαληθεύσει την αυθεντικότητα και την ακεραιότητα του terminal certificate. Προκειμένου να υπάρξει θετική επιβεβαίωση, όλα τα πιστοποιητικά τα οποία ακολουθούν στην ιεραρχία θα πρέπει να είναι υπογεγραμμένα με το μυστικό κλειδί του προκατόχου τους, ξεκινώντας με το CVCA πιστοποιητικό. Αυτό λογίζεται ως αξιόπιστο από το RF chip, από τη στιγμή που το κλειδί επιπρόσθετα έχει αποθηκευτεί στο RF chip κατά τη διάρκεια της παραγωγής του.

### 8.4.5 Επικουρικοί μηχανισμοί προστασίας δεδομένων

Μέσω των νέων δελτίων eID, διατίθεται μία **λειτουργία ψευδωνύμου**, η οποία δίνει την δυνατότητα κάποιο άτομο να εγγράφεται σε κάποια υπηρεσία και να αναγνωρίζεται από εκεί και έπειτα, από τον ίδιο πάροχο υπηρεσιών, χωρίς να απαιτείται από τον πάροχο της υπηρεσίας να απαιτεί να λάβει γνώση των ακριβών προσωπικών δεδομένων του χρήστη, κάθε φορά που αυτός χρησιμοποιεί την υπηρεσία (όπως για παράδειγμα μέσα σε ένα internet forum).

[200] Country Verifier Certification Authority certificate, όπως αναφέρθηκε και παραπάνω στο σχετικό πίνακα με τα μέσα προστασίας των Γερμανικών eID
[201] Country Verifier Public Key Infrastructure
[202] Πιστοποιητικό το οποίο διατίθεται και χαρακτηρίζει την εκάστοτε συσκευή ανάγνωσης

Η λειτουργία αυτή είναι εξειδικευμένη όσον αφορά το συνδυασμό δελτίου eID και υπηρεσίας. Δηλαδή αν ένα άτομο εγγράφεται σε δύο υπηρεσίες χρησιμοποιώντας τη λειτουργικότητα του ψευδωνύμου, δεν μπορεί να καθοριστεί αν στην πραγματικότητα πρόκειται για το ίδιο πρόσωπο στο οποίο εφαρμόζεται το ψευδώνυμο και στις δύο υπηρεσίες. Αποκλείεται δηλαδή η δυνατότητα αλληλοσυσχέτισης του ατόμου μεταξύ των διαφορετικών εφαρμογών που χρησιμοποιεί.

Στην **περίπτωση που χαθεί το eID** δελτίο, είναι δυνατόν να κλειδώσει η εφαρμογή του eID, χρησιμοποιώντας ένα προσωπικό κωδικό. Επιπρόσθετα η εφαρμογή eID στο δελτίο eID μπορεί να απενεργοποιηθεί από την αρχή η οποία εξέδωσε το δελτίο, εάν κάτι είναι επιθυμητό.

Τέλος εάν το **PIN εισαχθεί λανθασμένα** πάρα πολλές φορές, πρέπει να απενεργοποιηθεί χρησιμοποιώντας το PUK[203], αντίστοιχο προς τον τρόπο λειτουργίας του PIN ενός κινητού τηλεφώνου.

## 8.5 Ότι κλειδώνει … ξεκλειδώνει …

### 8.5.1 Το περιστατικό ασφάλειας

Τα μέλη της ομάδας έργου για την ανάπτυξη του δελτίου eID προέβησαν στον εξοπλισμό του με μία πλειάδα μηχανισμών ασφαλείας προκειμένου να το θωρακίσουν έναντι των υφιστάμενων κινδύνων από ενδεχόμενες επιθέσεις ασφάλειας.

Παρ' όλα αυτά πριν ακόμα να τεθεί σε επιχειρησιακή λειτουργία το δελτίο eID της Γερμανίας, μόλις τον Σεπτέμβριο του 2010, δέχτηκε το πρώτο πλήγμα αξιοπιστίας του από μία ομάδα Γερμανών hackers[204]. Για την ακρίβεια οι ίδιοι οι hackers δήλωσαν ότι η επίθεση δεν πραγματοποιήθηκε στους μηχανισμούς ασφαλείας της κάρτας οι οποίοι κρίθηκαν και από αυτούς ως ιδιαιτέρως επαρκείς.

Η επίθεση εκδηλώθηκε ως εκ τούτου στον πιο αδύναμο κρίκο της διαδικασίας χρήσης ενός δελτίου eID, ο οποίος είναι ο τελικός χρήστης - κάτοχος του δελτίου.

Μέσω ενός μη προστατευμένου από άποψη λογισμικού προστασίας υπολογιστή στο οποίο βρισκόταν εγκατεστημένος ένας αναγνώστης καρτών για

[203] PIN Unlocking Key
[204] Η εν λόγω ομάδα hackers είναι μία κολεκτίβα Γερμανών hackers με την επωνυμία Chaos Computer Club. Βλ. και http://www.ccc.de/en/

τα νέα δελτία ταυτότητας, εγκατέστησαν ένα spyware το οποίο μέσω της λειτουργικότητας key logging που διέθετε σύντομα υπέκλεψε τον προσωπικό μυστικό αριθμό PIN του κατόχου της κάρτας. Από εκεί και έπειτα τα δεδομένα του κατόχου της κάρτας ήταν άμεσα διαθέσιμα, καθώς μπορούσαν να διαβιβασθούν χωρίς την βούληση του ιδιοκτήτη τους σε κάποιον τρίτο και από εκεί να αντιγραφούν αποκαλυπτόμενα στο σύνολο τους, όπως περιλαμβάνονται μέσα στην κάρτα. Επιπλέον με τον προσωπικό αριθμό PIN διαθέσιμο και την κάρτα επάνω στον αναγνώστη, θα μπορούσαν να πραγματοποιηθούν δοσοληψίες εν αγνοία του χρήση από τους hackers προσποιούμενοι ότι είναι αυτός.

### 8.5.2 Ένα ακριβό λάθος

Η κυβέρνηση της Γερμανίας έχει ήδη ξοδέψει 24 εκατομμύρια ευρώ, για την προμήθεια περίπου ενός εκατομμυρίου αναγνωστών κάρτας βασικής τεχνολογίας, όπως αυτός ο οποίος χρησιμοποιήθηκε από τους hackers. Οι ειδικοί συστήνουν ότι θα πρέπει να χρησιμοποιηθούν υψηλής ποιότητας αναγνώστες, οι οποίοι διαθέτουν το δικό τους ενσωματωμένο πληκτρολόγιο για την εισαγωγή του PIN, και οι οποίοι θα καθιστούσαν πρακτικά ανέφικτη την εκμετάλλευση του εν λόγω σημείου ευπάθειας, προκειμένου να αποτραπούν και άλλα πιθανά κρούσματα πλαστοπροσωπίας στο μέλλον από hackers[44].

### 8.5.3 Η επίσημη δήλωση

Ο Manuel Bach, υπεύθυνος του έργου για λογαριασμό του BSI καλούμενος να σχολιάσει το συμβάν, συμφώνησε ότι ο τελικός χρήστης αποτελεί τον πιο αδύναμο κρίκο της αλυσίδας, αλλά αντιτάχθηκε λέγοντας ότι οι υπολογιστές οι οποίοι είναι έκθετοι σε Trojan horses είναι έκθετοι και σε οποιοδήποτε κίνδυνο μπορεί να απειλεί την ασφάλειά τους, ανεξάρτητα της χρήσης ή μη ενός δελτίου eID. Ο Bach δήλωσε χαρακτηριστικά ότι «Αποτελεί ευθύνη του κάθε χρήστη να ασφαλίσει το σύστημά του. Εάν κάποιος προβεί σε αυτές τις ενέργειες θωράκισης, τότε θα είναι ασφαλής ακόμα και με ένα απλό card reader. Σε κάθε περίπτωση ο τρόπος αυτός αυθεντικοποίησης είναι πιο ασφαλής από μία «ταλαντευόμενη» γραμμή με μελάνι πάνω σε ένα κομμάτι χαρτί»[7].

# 9. ΜΕΛΛΟΝΤΙΚΕΣ ΠΡΟΚΛΗΣΕΙΣ ΣΤΑ ΣΥΣΤΗΜΑΤΑ eIDM

## 9.1 Προβλήματα Διαλειτουργικότητας

Όποια και αν είναι όμως τα διάφορα συστήματα ταυτοποίησης τα οποία αναπτύσσονται, παρατηρείται ότι αυτά έχουνε εφαρμογή στην καλύτερη περίπτωση σε εθνικό επίπεδο στα πλαίσια του κάθε κράτους μέλους. Έτσι μία σειρά από μηχανισμούς αυθεντικοποίησης οι οποίοι αναπτύσσονται επί σειρά ετών σε επίπεδο Ευρωπαϊκής Ένωσης, δυστυχώς δεν μπορούν να τύχουν εφαρμογής σε διασυνοριακό επίπεδο, με άμεσο αποτέλεσμα τον περιορισμό των παρεχόμενων υπηρεσιών του κάθε κράτους μέλους σε εθνικό και μόνο επίπεδο.

Προκειμένου να παρακαμφθεί αυτός ο σκόπελος, έχει προσδιορισθεί σε επίπεδο Ευρωπαϊκής Ένωσης ένα πλαίσιο[36] για τη διαχείριση των ηλεκτρονικών ταυτοτήτων το οποίο αποτελεί την ασφαλιστική δικλείδα που καθορίζει τις προϋποθέσεις για την επίτευξη «αμοιβαίας» εμπιστοσύνης μεταξύ των συναλλασσομένων μερών σε επίπεδο Ευρωπαϊκής Ένωσης.

## 9.2 Κίνδυνοι Παραβίασης Ιδιωτικότητας

Σε αυτό το ψηφιακό περιβάλλον και παρά τη σχετική πρόοδος η οποία παρουσιάζεται, κανένας δεν μπορεί να παραβλέψει τον κίνδυνο ο οποίος υφίσταται από την ενδεχόμενη κακόβουλη χρήση των προσωπικών δεδομένων των χρηστών τα οποία χρησιμοποιούνται προκειμένου αυτοί να ταυτοποιηθούν.

Δεδομένου του ότι οι ηλεκτρονικές ταυτότητες αποτελούν από μόνες τους ένα φορέα προσωπικών δεδομένων των διοικούμενων, καταλήγει να αποτελεί πρόκληση η επίτευξη του μέγιστου δυνατού επιπέδου ασφάλειας, ούτως ώστε να μην υπάρχει ο κίνδυνος παραβίασης της ιδιωτικότητας[45], από την μη εξουσιοδοτημένη πρόσβαση, συλλογή και επεξεργασία προσωπικών ή και ευαίσθητων δεδομένων των πολιτών.

Με την Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών έγινε μία προσπάθεια ώστε τα κράτη μέλη της Ευρωπαϊκής Ένωσης να προσδιορίσουν τις περιπτώσεις κάτω από τις οποίες η διαχείριση των προσωπικών δεδομένων είναι εφικτή και

νόμιμη, ορίζοντας έτσι τα κατά περίπτωση αποδεκτά επίπεδα εξασφάλισης της ασφάλειας και της ιδιωτικότητας των πολιτών.

Η ενσωμάτωση της σχετικής Οδηγίας στις εθνικές νομοθεσίες των κρατών μελών, σε συνδυασμό με τον καθορισμό των σχετικών ορίων ρυθμίζονται μέσω επίσημων νομοθετημάτων όπως National Register Acts, Identity Card Acts & eGoverment Acts κ.τ.λ..

## 9.3 Έλλειψη σαφούς νομικού πλαισίου για τις ηλεκτρονικές ταυτότητες

Παρ' όλες τις νομοθετικές πρωτοβουλίες οι οποίες όπως προαναφέρθηκε έχουν ήδη ληφθεί και λαμβάνονται σε επίπεδο κρατών μελών, εντούτοις το θέμα της ηλεκτρονικής ταυτοποίησης οντοτήτων δεν έχει ακόμα θεσμοθετηθεί επαρκώς σε όλες τις Ευρωπαϊκές χώρες, καθώς δεν έχει οριστεί στο σύνολο των χωρών η έννοια της ηλεκτρονικής ταυτότητας, αλλά και ακόμη η σχετική Οδηγία η οποία ρυθμίζει σε κεντρικό επίπεδο το εν λόγω θέμα[18] δεν προβλέπει διατάξεις για το σύνολο των θεμάτων που ανακύπτουν από την λειτουργική αξιοποίηση των ηλεκτρονικών ταυτοτήτων. Αυτός είναι και ο λόγος που η εν λόγω Οδηγία κρίνεται ότι πρέπει να τύχει αναθεώρησης στα πλαίσια του Πλαισίου Δράσης 2011-2015 για την ηλεκτρονική διακυβέρνηση της Ευρωπαϊκής Ένωσης[21].

Η εμπειρία στα διάφορα κράτη μέλη καταδεικνύει ότι οι περισσότερες χώρες στην προσπάθεια τους να ενσωματώσουν στην κείμενη νομοθεσία τους την παραπάνω Οδηγία για τις ηλεκτρονικές υπογραφές, προέβησαν στην καθιέρωση κανονισμών οι οποίοι εξειδικεύουν την οδηγία σε διάφορα θέματα υποδομής (όπως π.χ. την καθιέρωση ή όχι καρτών-ταυτοτήτων & επισήμων μητρώων) και σε θέματα πολιτικών αυθεντικοποίησης. Ενδεικτικό του κενού που υπάρχει, είναι το γεγονός ότι η έννοια της ηλεκτρονικής ταυτότητας ορίζεται επαρκώς μόνο στην εθνική νομοθεσία της Αυστρίας και πρόσφατα και της Φινλανδίας[205].

Αποτέλεσμα αυτής της διαφορετικής κατά περίπτωση εξειδίκευσης της Οδηγίας για τις ηλεκτρονικές υπογραφές στις εθνικές νομοθεσίες, καθώς επίσης και της θεσμικής ανεπάρκειάς της να προσδιορίσει την έννοια της ηλεκτρονικής ταυτότητας αποτελεί η υιοθέτηση διαφορετικών λύσεων διαχείρισης των ηλεκτρονικών ταυτοτήτων πολιτών τα οποία ήδη υφίστανται στα κράτη μέλη, τα οποία επιπλέον δεν είναι και διαλειτουργικά μεταξύ τους σε επίπεδο Ευρωπαϊκής Ένωσης.

[205] New Act on Electronic Authentication and Signatures, September 2009

# 10. ΣΥΜΠΕΡΑΣΜΑΤΑ

Με βάση την ανάλυση που πραγματοποιήθηκε στα προηγούμενα κεφάλαια εξάγεται μία σειρά συμπερασμάτων για κάθε επίπεδο τμηματοποίησης των διάφορων εθνικών πολιτικών eIDM.

Στις ενότητες που ακολουθούν παρουσιάζονται τα συμπεράσματα στα εξής επίπεδα:

- ✓ Ηλεκτρονικής Διακυβέρνησης
- ✓ Νομικό Επίπεδο
- ✓ Τεχνολογικό Επίπεδο
- ✓ Επίπεδο Υποδομών
- ✓ Επίπεδο Εκμετάλλευσης & Παρεχόμενων Υπηρεσιών

## 10.1 Ηλεκτρονική Διακυβέρνηση

Η ανάπτυξη της αγοράς στα eID καθυστερεί εξ' αιτίας ορισμένων περιορισμών οι οποίοι σχετίζονται με το θέμα των εθνικών πολιτικών.

Κατά πρώτον υφίσταται έλλειψη κατάλληλων προτύπων διαλειτουργικότητας στα eID, κάτι το οποίο σημαίνει ότι τα προσωπικά δεδομένα τα οποία χρησιμοποιούνται για ταυτοποίηση και οι ηλεκτρονικές ταυτότητες, δεν μπορούν τεχνικά να κατασταθούν χρησιμοποιήσιμα σε διασυνοριακό επίπεδο. Ακόμη και αν αυτά τα πρότυπα υπήρχαν, θα ήταν αμφίβολο το κατά πόσο θα χρησιμοποιούνταν άμεσα σε διασυνοριακό επίπεδο.

Επίσης, καθώς οι στόχοι ως προς το θέμα της χρηστικότητας των eID ποικίλουν μεταξύ των διαφόρων Ευρωπαϊκών κρατών, η ανάπτυξη της αγοράς δεν μπορεί να πραγματοποιηθεί ομοιόμορφα, με αποτέλεσμα κάτι τέτοιο να είναι εμφανές στις πολιτικές και τις πρακτικές τις οποίες εφαρμόζουν τα διάφορα κράτη μέλη με εμφανώς αντικρουόμενους στόχους.

Ως εκ τούτου απαιτείται μία συντονισμένη πανευρωπαϊκή προσέγγιση στην ανάπτυξη ενός ομοιογενούς ως προς τους στόχους και τις επιδιώξεις του περιβάλλοντος eID προκειμένου να:

- Αυξηθεί η χρήση κοινών προτύπων: Θα πρέπει να αυξηθεί η δέσμευση ως προς τις χρησιμοποιούμενες τεχνολογίες, αλλά και ως προς τις προσεγγίσεις, ως προς τις εφαρμογές αλλά και τις ακολουθούμενες πολιτικές για υιοθέτηση των eID από τις κυβερνήσεις προκειμένου να

προωθηθεί η διαλειτουργικότητα σε διασυνοριακό επίπεδο και επομένως για εμπορικές επενδύσεις και ουσιαστική στήριξη των eIDs.

- Εναρμόνιση των στόχων: Θα πρέπει να πραγματοποιηθεί προσπάθεια ούτως ώστε να επιτευχθούν κοινοί στόχοι για τις ηλεκτρονικές ταυτότητες έτσι ώστε τα συστήματα που παραδίδονται να μην βρίσκονται σε ουσιαστική σύγκρουση μεταξύ τους. Για την ακρίβεια, η εθνική ασφάλεια δεν θα πρέπει να επικαλείται ως η βασική κινητήρια δύναμη, αλλά να αντιμετωπίζεται ως δευτερεύον, μετρήσιμο όφελος. Στηριζόμενοι κυρίως στην εθνική ασφάλεια δημιουργείται θεμελιώδης σύγκρουση μεταξύ των συστημάτων τα οποία κατασκευάζονται έχοντας στο επίκεντρο τους τον πολίτη και άρα είναι φύσει πιο εξωστρεφή και σε αυτά τα οποία έχουν στο επίκεντρο τους την εθνική ασφάλεια.

## 10.2 Νομικό επίπεδο

Κατά πρώτον υφίστανται σημαντικές ανισότητες στις ρυθμιστικές προσεγγίσεις για τις ηλεκτρονικές ταυτότητες σε ολόκληρη την Ευρώπη. Διαφορετικές χώρες, υιοθετούν διαφορετικές αρχές και μεθόδους προσπαθώντας να ρυθμίσουν το περιβάλλον των ηλεκτρονικών ταυτοτήτων τους, διαμορφώνοντας διαφορετικά πεδία και περιορισμούς σε κάθε χώρα, για την ανάπτυξη και λειτουργία δραστηριοτήτων και ηλεκτρονικών συναλλαγών βασισμένων στις ηλεκτρονικές ταυτότητες από τους διάφορους παρόχους οι οποίοι δραστηριοποιούνται τόσο εντός, όσο και εκτός των συνόρων της κάθε χώρας.

Κατά δεύτερο, λόγω της έλλειψης στην παρούσα φάση μίας κεντρικής αρχής για τα θέματα τα οποία σχετίζονται με τα eIDs, δεν υπάρχει κοινή προσέγγιση σε θέματα όπως η διασυνοριακή χρήση των ταυτοτήτων, γεγονός το οποίο εμποδίζει μία πιο ευρεία υιοθέτηση των υπηρεσιών των ηλεκτρονικών ταυτοτήτων.

Κατά τρίτον, επειδή υπάρχει η τάση προς την «ιδιοκτησία» του κάθε εθνικού σχήματος εξ' αιτίας των κείμενων νομοθεσιών, παρά προς την κατεύθυνση της υιοθέτησης διαλειτουργικών εθνικών σχημάτων eID, δεν υπάρχει κοινά αποδεκτή κατανόηση σχετικά με το πώς θα πρέπει τα εθνικά σχήματα να αλληλεπιδρούν μεταξύ τους. Αυτό περιορίζει επίσης τις πιθανότητες να χρησιμοποιηθούν εθνικές ταυτότητες πέραν των εθνικών συνόρων.

Κατά τέταρτον, υφίστανται σημαντικές διαφορές μεταξύ των προτύπων των eIDs στην Ευρώπη, κάτι το οποίο συνεπάγεται ότι ακόμη και από τεχνολογική άποψη, οι διάφορες λύσεις eID μπορεί και σε πολλές περιπτώσεις δεν είναι συμβατές μεταξύ τους.

Προκειμένου να επιτευχθεί η διαλειτουργικότητα στα eIDs, οι ρυθμιστικοί φορείς θα πρέπει να παράσχουν ένα «πεδίο ίσων όρων» μεταξύ των συμμετεχουσών χωρών, και ιδίως να προετοιμάσουν:

- Κανονιστική Ισοτιμία: Να επιδιώξουν δηλαδή τη μεγαλύτερη ισότητα στον ρόλο, τη λειτουργία και τις αρμοδιότητες των Επιτρόπων για την Προστασία των Προσωπικών Δεδομένων (ή ισοδύναμων αρχών) προκειμένου να εποπτεύουν την ενδυνάμωση του ρόλου των eIDs.
- Κεντρική Καθοδήγηση και Ρύθμιση: Να δημιουργηθεί μία κεντρική ευρωπαϊκή αρχή για την διαχείριση της διαλειτουργικότητας, προκειμένου να επιλύσει τις υπάρχουσες διαφορές και να ενδυναμώσει τις αποφάσεις ευθύνης μεταξύ των εθνικών συστημάτων ταυτοποίησης.
- Διαλειτουργικά κυβερνητικά eID: Τα Ευρωπαϊκά κράτη θα πρέπει να δώσουν μεγαλύτερη προτεραιότητα στην διαλειτουργικότητα των credentials τα οποία εκδίδουν, κάτι το οποίο σε μία ευρεία κλίμακα δεν θα πρέπει να περιορίζεται στα Ευρωπαϊκά όρια.
- Τυποποίηση: Θα πρέπει να πραγματοποιηθούν εργασίες με αρμόδιους φορείς τυποποίησης προκειμένου να προωθηθεί η εναρμόνιση των τεχνολογιών των eIDs και οι προσεγγίσεις των υποδομών για τα eID.

## 10.3 Τεχνολογικό επίπεδο

Στο τεχνολογικό επίπεδο αυτό που χρειάζεται είναι πρώτα απ' όλα καλύτερα διακριτικά ταυτοποίησης για τους τελικούς χρήστες τα οποία θα μπορούν να είναι διαχειρίσιμα σε πολλαπλά λειτουργικά περιβάλλοντα και σενάρια χρήσης. Επί του παρόντος, οι υπάρχουσες τεχνολογίες δεν είναι αρκετά ευέλικτες προκειμένου να υποστηρίξουν την ποικιλία των αναδυόμενων υπηρεσιών eID οι οποίες μπορεί να χρειαστούν ιδιαίτερες λειτουργικότητες απαιτήσεις.

Κατά δεύτερον, προκειμένου να αυξηθεί η φορητότητα των διακριτικών, το ιδανικό για τους πολίτες θα ήταν να μπορούν να είναι ικανοί να αποθηκεύουν τα προσωπικά δεδομένα ταυτοποίησής τους σε συσκευές διαφορετικές από μία smart card, όπως κινητά τηλέφωνα.

Τέλος φαίνεται πως υφίσταται μία ανάγκη για φορητές τεχνολογίες βιομετρικών δεδομένων προκειμένου να καταπολεμηθεί ο αυξημένος κίνδυνος της απάτης η οποία βασίζεται σε θέματα σχετιζόμενα με τις ηλεκτρονικές ταυτότητες.

Παρ' όλο που δεν υπάρχει κάποια συγκεκριμένη ανάγκη για κυβερνητική παρέμβαση προκειμένου να αναπτυχθούν νέες τεχνολογίες eID, και οι πολίτες δεν παροτρύνονται προκειμένου να χρησιμοποιούν περισσότερο τα βιομετρικά

δεδομένα στην παρούσα φάση, αρκετές τεχνολογίες θα πρέπει να ενθαρρυνθούν προκειμένου να προωθηθεί η ανάπτυξη των eIDs, συμπεριλαμβανομένων των:

- Ενισχυμένα διακριτικά: Η παροχή διακριτικών ταυτοποίησης τα οποία να μπορούν να ενοποιήσουν πολλαπλά διακριτικά και λειτουργικότητες, ή να ενσωματώσουν card reader/PIN τεχνολογίες προκειμένου να προωθηθεί η χρήση δυναμικών κωδικών πρόσβασης και αυθεντικοποίησης δύο παραγόντων.
- Φορητότητα πιστοποιητικών: Να επιτρέπεται η φορητότητα των πιστοποιητικών έτσι ώστε αυτά να μην συμπεριλαμβάνονται μόνο μέσα σε μία smart card, αλλά και σε οποιοδήποτε ασφαλές διακριτικό της επιλογής του χρήστη.
- Ανάπτυξη των βιομετρικών: Η ενίσχυση των τεχνολογιών βιομετρίας οι οποίες είναι φορητές και οικονομικές θα ενθαρρύνουν την ευρεία αποδοχή της αυθεντικοποίησης τριών παραγόντων όπου χρειάζεται και θα βοηθήσουν να αντιμετωπιστούν προβλήματα phishing και επιθέσεις πλαστοπροσωπίας.

## 10.4 Επίπεδο Υποδομών

Οι κυβερνήσεις μπορούν να παράσχουν κίνητρα ανάπτυξης των eIDs με το να ενσωματώσουν λειτουργικότητες και την υποστήριξη στοιχείων τα οποία θεωρούνται πολύ επικίνδυνα ή δαπανηρά προκειμένου να υλοποιηθούν από τον ιδιωτικό τομέα (όπως στην αρχική εγγραφή των χρηστών), εμποδίζοντας έτσι τον κατακερματισμό των εθνικών λύσεων ταυτοποίησης. Αυτό θα προσφέρει επίσης έναν εύκολο τρόπο στους πολίτες προκειμένου να αρχίσουν να χρησιμοποιούν τις νέες υπηρεσίες οι οποίες βασίζονται στις ηλεκτρονικές ταυτότητες σε μία πλειάδα περιπτώσεων. Σε αυτό το πλαίσιο, υπάρχει μία ανάγκη να ενσωματωθούν οι τεχνολογίες των eIDs μέσα σε άλλα προϊόντα και υπηρεσίες προκειμένου να δημιουργηθεί μία «κρίσιμη μάζα» από υποδομές οι οποίες θα βασίζονται στην δυνατότητα επίτευξης μεγαλύτερης βάσης χρήσης για μία πλειάδα υπηρεσιών οι οποίες θα βασίζονται στα eIDs.

Επιπλέον, η παροχή και υποστήριξη τεχνολογιών διάχυσης πέραν των διεπαφών έξυπνων καρτών θα μπορούσαν να διευκολύνουν την φορητή πρόσβαση στα πιστοποιητικά των eIDs σε όλες τις πλατφόρμες και τοποθεσίες, εξασφαλίζονται την αυξημένη πρόσβαση στα διακριτικά.

Υπάρχει επίσης η ανάγκη για μεγαλύτερη χρήση τεχνολογιών βασισμένων σε ομόσπονδες βάσεις δεδομένων προκειμένου να βελτιωθεί η διαλειτουργικότητα, καθώς πολλές εξελίξεις στις eIDs τείνουν να είναι περιορισμένης έκτασης σε κάθε χώρα ή σε μεμονωμένους τομείς ή εφαρμογές.

Η επίτευξη μίας διαλειτουργικής υποδομής eID η οποία στη συνέχεια θα προωθεί τις ηλεκτρονικές ταυτότητες σε επίπεδο ηλεκτρονικά παρεχόμενων υπηρεσιών (του δημοσίου και του ιδιωτικού τομέα), μπορεί να επιτευχθεί μέσω των:

- Εγγραφή χρηστών: Η εγγραφή των χρηστών θα πρέπει να είναι κεντρικοποιημένη ή να πραγματοποιείται σε συνεργασία με εταιρείες του ιδιωτικού τομέα, κάτι το οποίο θα εξασφάλιζε την αξιοπιστία των eID credentials.
- Ενσωμάτωση eID: Οι κυβερνήσεις των διαφόρων χωρών θα πρέπει να είναι σε θέση να επιταχύνουν την ανάπτυξη των eID παρέχοντας κίνητρα στους βασικούς προμηθευτές προκειμένου να ενσωματώσουν προτυποποιημένους μηχανισμούς eID μέσα στα προϊόντα τους.
- Προώθηση των καθολικών αναγνωριστικών: η μεγαλύτερη χρήση συστημάτων ταυτοποίησης τα οποία χρησιμοποιούν καθολικά αναγνωριστικά ακόμη και για χρήση από τον ιδιωτικό τομέα, θα έπρεπε να ενθαρρύνεται για χρήση από τις κυβερνήσεις των κρατών, εάν βέβαια θα είχε υπάρξει η από πριν διαβεβαίωση των δημόσιων αρχών του κάθε κράτους ότι θα ήταν πρόθυμες να χρησιμοποιήσουν αξιόπιστα καθολικά αναγνωριστικά.

## 10.5 Επίπεδο Εκμετάλλευσης & Υπηρεσιών

Τα πραγματικά συστήματα eID που διαχειρίζονται από το δημόσιο τομέα είναι μη ελαστικά και δεν επιτρέπουν εύκολα την εξέλιξή τους, προκειμένου να προωθηθούν προς τα έξω εκτός του μοντέλου με βάση το οποίο λειτουργούν στην παρούσα φάση. Από την άλλη, υπάρχει μία απαίτηση για πρόσβαση σε συστήματα eID από την βιομηχανία μέσω ανοιχτών προτύπων, καθώς και για μεγαλύτερη συνεργασία μεταξύ των ενδιαφερόμενων μερών του δημόσιου και του ιδιωτικού τομέα. Από την άποψη αυτών των απαιτήσεων και δεδομένης της στρατηγικής θέσης των κυβερνήσεων να επηρεάζουν την ανάπτυξη των eID, ένας μεγαλύτερος βαθμός συνεργασίας μεταξύ της βιομηχανίας και των κυβερνητικών φορέων θα αποτελούσε μία θετική εξέλιξη.

Μία τέτοια συνεργασία θα μπορούσε να οδηγήσει σε:

- Καινοτόμες προσεγγίσεις: Οι δημόσιοι φορείς του κάθε κράτους, θα πρέπει να ξεκινήσουν να ενσωματώνουν την καινοτομία στα μοντέλα των eIDs, χρησιμοποιώντας self-asserted credentials και μοντέλα VPI[206].
- Open Interfaces: Τα κυβερνητικά σχήματα eID, θα πρέπει να παρέχουν ελεύθερη πρόσβαση στον ιδιωτικό τομέα προκειμένου αυτός να

[206] Volunteered Personal Information

χρησιμοποιεί τα δημόσια συστήματα (με ή χωρίς την απαίτηση για την κτήση σχετικής άδειας), και υποστήριξη αυτής της χρήσης, ενθαρρύνοντας μία σειρά από Αρχές Πιστοποίησης να αναπτυχθούν γύρω από κυβερνητικά συστήματα.

- Συμπράξεις δημόσιου-ιδιωτικού τομέα: Οι κυβερνήσεις θα πρέπει να εργαστούν με εμπορικούς εταίρους προκειμένου να εξασφαλίσουν ότι οι στόχοι για την ανάπτυξη συστημάτων eID είναι ρεαλιστικοί, ότι οι ανάγκες των ενδιαφερόμενων μελών αναθεωρούνται σε όλη την διάρκεια της ανάπτυξης και ότι το κόστος του εκάστοτε προγράμματος είναι ανάλογο με την αξία των παραδοτέων.

# ΒΙΒΛΙΟΓΡΑΦΙΑ


[1]. The State of the Electronic Identity Market: Technologies, Infrastructure, Services and Policies, Toby Stevens et.al., JRC Reports, EUR 24567 EN – 2010

[2]. http://www.opengov.gr/ypes/?p=984 - Δικτυακός Τόπος Διαβουλεύσεων. Δημόσια Διαβούλευση του Ελληνικού Κράτους για το Σχέδιο Νόμου για την Ηλεκτρονική Διακυβέρνηση

[3]. Ηλεκτρονική ταυτότητα πολιτών και επιλογές πολιτικής και υποδομών, Δρ Α. Κουντζέρης, Παρατηρητήριο της Κοινωνίας της Πληροφορίας, Ιούνιος 2010

[4]. Note 9949/10 Council of The European Union: State of play concerning the electronic identity cards in the EU Member States, 2010

[5]. http://www2.icao.int/en/MRTD/Pages/Doc9393.aspx - ICAO, Document 9303, σχετικά με τα Machine Readable Travel Documents

[6]. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=31432 - Κωδικοποίηση σύμφωνα με το ISOIEC 7810:2003 για τα φυσικά χαρακτηριστικά των καρτών ταυτοποίησης.

[7]. New digital German ID cards arrive on November 1, Stuart Tiffen, Deutsche Welle, 28/10/2010. Βλ. Βλ. http://www.dw-world.de/dw/article/0,,6140545,00.html

[8]. "Next –generation super ID card on the cards for 2012", Nick Heath, 17/03/2010, Βλ. http://www.silicon.com/technology/security/2010/03/17/exclusive-next-generation-super-id-card-on-the-cards-for-2012-39745599/

[9]. "eGovernment Factsheet – Cyprus – National Infrastructure", Last Updated April 2010, βλ. http://www.epractice.eu/en/document/288192

[10]. EU will not fund ID cards renewal, Ivan Camilleri, Brussels, 6/12/2010. Βλ. http://www.timesofmalta.com/articles/view/20101206/local/eu-will-not-fund-id-cards-renewal

[11]. Romanian Government Wants to Issue Electronic ID Cards, EDRi-gram - Number 8.16, 25/08/2010 . Βλ. http://www.edri.org/edrigram/number8.16/electronic-id-romania-proposal

[12]. Chech national e-ID cards, Basic Infromation, Ministerstvo Vnitra Ceske Republiky, 23/10/2008. Βλ. http://www.ants.interieur.gouv.fr/evenements/IMG/File/Czech%20national%20e-ID%20card2.pdf

[13]. AT: First electronic ID cards issued in Austria, 24/2/2003. Βλ. http://www.epractice.eu/en/news/284155

[14]. Integration of biometric features in passports and travel documents. European Comission. Βλ. http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l14154_en.htm

[15]. Κανονισμός (ΕΚ) αριθ. 2252/2004 του Συμβουλίου της 13.12.2004 σχετικά με την καθιέρωση προτύπων για τα χαρακτηριστικά ασφαλείας και τη χρήση βιομετρικών στοιχείων στα διαβατήρια και τα ταξιδιωτικά έγγραφα των κρατών μελών της Ε.Ε.

[16]. C(2006) 2909 final – Δεν δημοσιεύτηκε στην Επίσημη Εφημερίδα – Τεχνικές προδιαγραφές σχετικά με τα πρότυπα ασφάλειας και των βιομετρικών δεδομένων που ενσωματώνονται στα διαβατήρια και τα ταξιδιωτικά έγγραφα που εκδίδονται από τις Ευρωπαϊκές χώρες, σε υλοποίηση της Οδηγίας (ΕC) 2252/2004.

[17]. COM(2004)0116 – C5-0101/2004 – Ψήφισμα νομοθετικού περιεχομένου του Ευρωπαϊκού Κοινοβουλίου σχετικά με την πρόταση για την έκδοση κανονισμού του Συμβουλίου σχετικά με την καθιέρωση προτύπων για τα χαρακτηριστικά ασφαλείας και τη χρήση βιομετρικών στοιχείων στα διαβατήρια των πολιτών της ΕΕ

[18]. Οδηγία 1999/93/ΕC του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 1999 σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές, βλ. σχετικά http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EL:HTML

[19]. Οδηγία 95/46/ΕC του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24 Οκτωβρίου 1995 σχετικά με την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα και σχετικά με την ελεύθερη διακίνηση τέτοιων δεδομένων, βλ. σχετικά http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EL:NOT

[20]. Οδηγία 2006/123/ΕCτου Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12 Δεκεμβρίου 2006 σχετικά με τις υπηρεσίες στην εσωτερική αγορά. Βλ. σχετικά http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0123:EL:NOT

[21]. European Commission – Information Society - ICT for Government and Public Services: Action Plan 2011-2015, Pre-conditions for Developing eGovernment, 15/12/2010 βλ. σχετικά http://ec.europa.eu/information_society/activities/egovernment/action_plan_2011_2015/priorities_objectives/developing_egovernment/index_en.htm

[22]. Μελέτη για τη Διασυνοριακή Διαλειτουργικότητα των ηλεκτρονικών υπογραφών (Cross Border Interoperability of eSignatures [CROBIES]), βλ. σχετικά http://ec.europa.eu/information_society/policy/esignature

[23]. Study on Mutual Recognition of eSignatures: update of Country Profile, Portuguese country profile, July 2009

[24]. eGovernment Factsheet – Austria – History. Last Edited Date 08 Ιουλίου 2010. Βλ. http://www.epractice.eu/en/document/288168

[25]. eGovernment Factsheets – eGovernment in Hungary, April 2010, edition 13.0, p.29

[26]. Study on eID Interoperability for PEGS – Update of Country Profiles – Analysis and Assessment report, October 2009, p.120

[27]. Government eID Projects Need Private Sector Initiative And Support For Broader Success, A Look At Europe's Experience With PKI-Enabled National ID Cards, Gardner Research April 7, 2008

[28]. Overview of IT Projects: The electronic ID card, German Bundesministerium des Innern, Division IT4, Biometrics, Travel and ID Documents Registration, July 2009, p.2. Βλ. https://www.eid-stork.eu/dmdocuments/public/090715_Overview_electronic_ID_card.pdf

[29]. Πλαίσιο Ψηφιακής Αυθεντικοποίησης, Υπουργείο Εσωτερικών, Έκδοση 2.00, Μάιος 2008

[30]. European Commission Directorate General For Informatics: eID Interoperability for PEGS: Multilevel authentication mechanism (WP4). Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms, Βρυξέλες Σεπτέμβριος 2007, p.67

[31]. Ν.3731/2008, περί αναδιοργάνωσης της δημοτικής αστυνομίας και ρυθμίσεις λοιπών θεμάτων αρμοδιότητας Υπουργείου Εσωτερικών. ΦΕΚ Α 263/2008

[32]. STORK: D2.1 – Framework Mapping of Technical/Organisational Issues to a Quality Scheme, 13/10/2008

[33]. Διάταγμα n. 2007-284 της 2 Μαρτίου 2007 σχετικά με το γενικό πλαίσιο αναφοράς για τη διαλειτουργικότητα [relative au referential general d' interopérabilité], J.O. n. 53 pf 3 March 2007, σελίδα 4060. Με βάση την έκδοση 1.00 του RGS διαθέσιμο στο site: http://references.modernisation.gouv.fr/rgs-securite

[34]. Registration and Authentication – eGovernment Strategy Framework Policy and Guidelines Version 3.0, Βλ. http://interim.cabinetoffice.gov.uk/govtalk/policydocuments/security/security_framework/registration_and_authentication_.aspx

[35]. Estonia launches new generation e-ID cards by Trub, Smart Insights, 15/04/2010. Βλ. http://www.smartinsights.net/?2010/04/15/298-estonia-launches-new-generation-e-id-cards-by-trub

[36]. A Roadmap for a pan-European eIDM Framework by 2010, 15/01/2007, European Commission, Information Society and Media Directorate-General, eGovernment Unit. Βλ. http://ec.europa.eu/information_society/activities/egovernment/docs/pdf/eidm_roadmap_paper.pdf

[37]. The i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All, Communication from the Commission, 25 Απριλίου 2006, βλ. http://ec.europa.eu/transparency/archival_policy/docs/moreq/action_plan_i2010_en.pdf

[38]. Signposts toward eGovernment 2010, European Commission, Information Society and Media, Directorate General, November 2005. Βλ. http://ec.europa.eu/information_society/activities/ict_psp/documents/signposts2005.pdf

[39]. ENISA Report on the state of pan-European eID initiatives, Hans Graux & Jos Dumortier, 29/01/2009, p.6

[40]. FIDIS Deliverable 3.12: Federated Identity Management – what's in it for the citizen/customer?, WP3,FIDIS, 10 June 2009, p.12

[41]. The electronic ID card, Bundesministerium des Innern (Ομοσπονδιακό Υπουργείο Εσωτερικών). Βλ. http://www.bmi.bund.de/EN/Themen/Sicherheit/PaesseAusweise/ePersonalausweis/ePersonalausweis_node.html

[42]. Advanced Security Mechanisms for Machine Readable Travel Documents, Technical Guideline TR-03110, Bundesamt für Sicherheit in der Informationstechnik, Version 2.05, 14/10/2010

[43]. Security mechanisms in electronic ID documents: Country Signer Certificate Authority (CSCA), Federal Office for Information Security. Βλ. https://www.bsi.bund.de/ContentBSI/EN/Topics/ElectrIDDocuments/SecurityMechanisms/PKI/CSCA/securitymechanismsCSCA.html

[44]. New German ID card easily hacked by ordinary computer nerds, Sara Harman, Deutsche Welle, 23/09/2010. Βλ. http://www.dw-world.de/dw/article/0,,6039502,00.html

[45]. Electronic Identity Management Infrastructure for trust worthy services, ELSA, INFSO H2 – January 2010, p.6

Επιπλέον μία πλειάδα ιστοσελίδων, ανά κράτος (φορείς έκδοσης ταυτοτήτων, εταιρείες κινητών επικοινωνιών, ιστοσελίδες ηλεκτρονικής διακυβέρνησης και άλλες σελίδες περιέχουσες άλλο πληροφοριακό υλικό).

Ιδιαίτερα τέλος χρησιμοποιήθηκαν μία σειρά παραδοτέων έργων με στοιχεία για κάθε χώρα τα οποία δεν μνημονεύονται ρητώς, από τα παραδοτέα των έργων STORK και IDABC, από όπου αντλήθηκε πολύτιμο πληροφοριακό υλικό.

Σχετικοί σύνδεσμοι προσπέλασης των εν λόγω πηγών είναι οι εξής:

IDABC: Interoperability for Pan European Government Services Deliverables (http://ec.europa.eu/idabc/en/document/6484.html)

STORK Project Deliverables (https://www.eid-stork.eu/index.php?option=com_processes&act=list_documents&s=1&Itemid=60&id=312)