

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή στα Πληροφοριακά και Επικοινωνιακά Συστήματα



**Ανάλυση Πολιτικών Ηλεκτρονικής Ταυτοποίησης
(e-Identification) σε Περιβάλλοντα Ηλεκτρονικής
Διακυβέρνησης στην Ευρώπη : Τεχνικά και Νομικά Θέματα**

Ευτυχία Σαμαρτζοπάνου

Επιβλέπων Καθηγητής
Στέφανος Γκρίτζαλης

Ανοικτό Πανεπιστήμιο Κύπρου
Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Ιούνιος 2014

Ανάλυση Πολιτικών Ηλεκτρονικής Ταυτοποίησης (e-Identification) σε Περιβάλλοντα Ηλεκτρονικής Διακυβέρνησης στην Ευρώπη: Τεχνικά και Νομικά Θέματα

Ευτυχία Σαμαρτζοπάνου

**Επιβλέπων Καθηγητής
Στέφανος Γκρίτζαλης**

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

μεταπτυχιακού τίτλου σπουδών στα
Πληροφοριακά Συστήματα

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του
Ανοικτού Πανεπιστημίου Κύπρου

Περίληψη

Στο σύγχρονο κόσμο του Διαδικτύου σημαντικό ζήτημα αποτελεί το θέμα της ηλεκτρονικής ταυτοποίησης και διαχείρισης ηλεκτρονικής ταυτότητας πολιτών, για την υποστήριξη υπηρεσιών ηλεκτρονικής διακυβέρνησης. Σημαντικό ζήτημα αποτελεί η ύπαρξη ενός μοναδικού χαρακτηριστικού βάσει του οποίου ο πολίτης θα μπορεί να προσπελάσει πλήθος υπηρεσιών αρχικά σε ένα κράτος και κατ'

Ιούνιος 2014

επέκταση στα κράτη της Ευρωπαϊκής Ένωσης. Αυτό το μοναδικό χαρακτηριστικό αξιοποιείται στο πλαίσιο ηλεκτρονικής ταυτότητας (electronic IDentification -eID).

Τα κράτη-μέλη της Ευρωπαϊκής Ένωσης αναπτύσσουν και υλοποιούν πολιτικές ρύθμισης σχετικών θεμάτων. Στο πλαίσιο αυτό, στην παρούσα διπλωματική εργασία θα μελετηθούν τεχνολογικά και νομικά θέματα που σχετίζονται με υποδομές ηλεκτρονικής ταυτοποίησης, συστήματα και πολιτικές αυθεντικοποίησης σε περιβάλλοντα Ηλεκτρονικής Διακυβέρνησης. Παρόλο που τα κράτη-μέλη της Ευρωπαϊκής Ένωσης διατηρούν μηχανισμούς ηλεκτρονικής αυθεντικοποίησης σε εθνικό επίπεδο, πλέον δίνεται ιδιαίτερη έμφαση στην προσπάθεια σύγκλισης ενός τρόπου διασυνοριακής ταυτοποίησης. Σημαντική παράμετρο που λαμβάνεται υπόψη αποτελεί η Ιδιωτικότητα κατά την Online Αυθεντικοποίηση.

Ξεχωριστή έμφαση θα δοθεί στο πλάνο της Ηλεκτρονικής Διακυβέρνησης για την Ελληνική πραγματικότητα, στα χαρακτηριστικά των υπηρεσιών Ηλεκτρονικής Διακυβέρνησης, στο θεσμικό και τεχνικό πλαίσιο, την Κάρτα Πολίτη και τα μέτρα προστασίας της πληροφορίας.

Επιπλέον, στο παράρτημα της παρούσας εργασίας παρουσιάζονται έργα που έχουν υλοποιηθεί σχετικά με την ενίσχυση της ιδιωτικότητας των συστημάτων διαχείρισης ταυτότητας, την παροχή διαλειτουργικότητας σε πανευρωπαϊκές υπηρεσίες ηλεκτρονικής διακυβέρνησης, στις δημόσιες υπηρεσίες, στις επιχειρήσεις και στους πολίτες. Όλα τα έργα προσανατολίζονται στην εναρμόνιση των κρατών-μελών σε ασφαλή ηλεκτρονικά συστήματα ταυτοποίησης των πολιτών παρέχοντας υψηλές υπηρεσίες σε ευρωπαϊκό πλαίσιο. Επιπρόσθετα περιλαμβάνεται αγγλοελληνικό λεξικό με τα τεχνικά χαρακτηριστικά των εγγράφων ηλεκτρονικής ταυτοποίησης.

Summary

In the modern world of communication and in particular the World Wide Web (or more commonly known as the internet) the issue of electronic identification has become of paramount importance for ordinary users in support, particularly/' of services pertaining to electronic governance. The existence of a singular characteristic or a unique attribute applicable to each individual, enabling him to access a plethora of services initially in one state and eventually in all the states of the European Union appears to be a major issue.

This unique attribute is commonly known as the electronic identification (eID).

The member states of the European Union are currently developing and putting into practice certain regulations pertaining to this matter. In this context therefore, this thesis will explore the technological and legal issues which are related to the infrastructure of electronic identification, the systems required as well as authentication policies in environments of electronic governance. Notwithstanding the fact that the member states of the European Union currently/ maintain numerous mechanisms of electronic identification at a national level, there appears to be an attempt to shift towards a uniform cross border identification system. Of major consideration in this regard, is the online privacy of an individual on authentication.

A separate and a special emphasis will be placed upon the electronic governance plan in so far as Greece is concerned with particular emphasis on the characteristics of electronic governance including the institutional and technical framework thereof, the individual card of each citizen and the measures for the protection of information.

In the various sections of the present thesis, there are numerous references to studies relating to the strengthening and improvement of the individual privacy of identity in such management systems, the availability at a pan - European level of a system of interoperability for electronic governance access to public agencies, businesses as well as individuals. All the efforts are geared to the harmonization by the member states towards a system where safe electronic identification is the order of the day, providing citizens of the various member states with high quality services across the European Union. In addition thereto, provision has been made for the inclusion of an English-Greek dictionary with the technical characteristics of electronic identification documents.

Ευχαριστίες

Στη ζωή μου δεν θέτω πολλούς στόχους. Αλλά ότι με γοήτευσε ήταν πολύ ψηλά και αρκετά δύσκολο να το κατακτήσω. Ως μάνα, εργαζόμενη, φοιτήτρια και περισσότερο παιδί, με σκληρή προσπάθεια κατάφερα τον πολυπόθητο στόχο του μεταπτυχιακού τίτλου σπουδών στην Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων.

Χαίρομαι που εκπλήρωσα ένα όνειρό μου. Χαίρομαι που ολοκλήρωσα αυτό το πολύ αντιφατικό ταξίδι. Έτσι, για να μπορώ πια να πάρω την ταχεία και να πάω για άλλες πολιτείες...

Απρόσμενα στηρίγματα στην εξ αποστάσεως διδασκαλία ήταν συμφοιτητές και συμφοιτήτριες που γνώρισα μέσα από τις θεματικές μου ενότητες και πλέον φίλοι και φίλες μου. Πίσω από την ηλεκτρονική τάξη βρέθηκε η Στέλλα, η Λία, ο Σπύρος, η Κλεοπάτρα, ο Θοδωρής, ο Βαγγέλης, ο Κώστας και η Μαρία.

Ιούνιος 2014

Σε όλη μου την προσπάθεια ήταν δίπλα μου η οικογένεια μου, με αποκορύφωμα το "γνωστό στίχο από τα χείλη ενός γιου μου : «Θέλω να ζήσω ελεύθερος, δίχως ταυτότητα πια!». Αλλά, ήταν δίπλα μου. Με το δικό τους μοναδικό τρόπο.

Βαθιές ευχαριστίες στον καθοδηγητή καθηγητή μου, κύριο Στέφανο Γκρίτζαλη.

Ευχαριστώ για την υπομονή και την υποστήριξη,

Ευτυχία Σαμαρτζοπάνου

Ιούνιος 2014

Περιεχόμενα

1	Εισαγωγή	1
1.1	Ταυτότητα του πολίτη.....	1
1.2	Ηλεκτρονική Ταυτοποίηση.....	3
1.3	Δομή της εργασίας.....	4
2	Πολιτικές Ταυτοποίησης Πολιτών	6
2.1	Φυσική Ταυτοποίηση.....	7
2.2	Ηλεκτρονική Ταυτοποίηση.....	14
2.2.1	Ηλεκτρονικές Κάρτες - Ταυτότητες.....	14
2.2.2	Μοναδικά Αναγνωριστικά.....	36
3	Ευρωπαϊκές Οδηγίες	43
3.1	Προστασία προσωπικών δεδομένων (95/46/EK).....	44
3.2	Ηλεκτρονικές υπογραφές (1999/93/EK).....	46
3.2.1	Προηγμένη Ηλεκτρονική Υπογραφή.....	47
3.2.2	Ψηφιακά Πιστοποιητικά.....	48
3.3	Προστασία της Ιδιωτικής ζωής στις ηλεκτρονικές υπηρεσίες (2002/58/EK)..	49
3.4	Διατήρηση δεδομένων θέσης και κίνησης (2006/24/EK).....	50
3.5	Παροχή Υπηρεσιών στην εσωτερική αγορά (2006/123/EK).....	52
3.6	Κανονισμός eIDAS (Electronic Identification and Signature).....	53
4	Ηλεκτρονική Διακυβέρνηση	55
4.1	Πλαίσιο Ηλεκτρονικής Διακυβέρνησης.....	56
4.1.1	Περί Ηλεκτρονικής Διακυβέρνησης.....	56
4.1.2	Ανάγκες Ηλεκτρονικής Διακυβέρνησης.....	57
4.1.3	Μέσα Ηλεκτρονικής Διακυβέρνησης.....	58
4.1.4	Επίπεδα Αξιολόγησης Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης.....	58
4.2	Ιδιωτικότητα και Ηλεκτρονική Διακυβέρνηση.....	60
4.3	Διαλειτουργικότητα Ηλεκτρονικής Διακυβέρνησης.....	62
4.4	Η Ηλεκτρονική Διακυβέρνηση στην Ευρώπη.....	64
4.4.1	Στρατηγικές Ταυτοποίησης σε περιβάλλοντα ΗΔ.....	64
4.4.2	Πολιτικές Ταυτοποίησης σε περιβάλλοντα ΗΔ.....	65
4.4.3	Πύλες Ηλεκτρονικής Διακυβέρνησης.....	66

4.4.4	Ευρωπαϊκή Εξέλιξη Ηλεκτρονικής Διακυβέρνησης.....	68
5	Πολιτικές Αυθεντικοποίησης Πολιτών	72
5.1	Αυθεντικοποίηση.....	73
5.2	Ασφάλεια Αυθεντικοποίησης.....	74
5.2.1	Επίπεδο Εμπιστοσύνης.....	75
5.2.2	Επίπεδο Αυθεντικοποίησης.....	76
5.2.3	Επίπεδο Εγγραφής	78
5.3	Διακριτικά Αυθεντικοποίησης.....	79
5.4	Υποδομή Δημοσίου Κλειδιού.....	83
5.4.1	Συνιστώσες Υποδομής Δημοσίου Κλειδιού.....	84
5.4.2	Ευρωπαϊκές υλοποιήσεις.....	85
6	Η Ελληνική Ηλεκτρονική Πραγματικότητα.....	89
6.1	Θεσμικό πλαίσιο.....	90
6.2	Τεχνικά θέματα.....	94
6.3	Κάρτα Πολίτη.....	95
6.3.1	Δομή Κάρτας Πολίτη.....	96
6.3.2	Κύκλος Ζωής.....	97
6.3.3	Προστασία της πληροφορίας	98
6.3.4	Προϋποθέσεις - Υποχρεώσεις Ηλεκτρονικού Παρόχου	101
6.4	Εξέλιξη Ηλεκτρονικής Διακυβέρνησης.....	102
7	Επίλογος.....	104
7.1	Αποτίμηση της μελέτης.....	105
7.2	Ευρωπαϊκό όραμα	106
	Βιβλιογραφία.....	109
	Παράρτημα Α: Ευρωπαϊκά Έργα	
A.1	Ενιαίος Χάρτης στην Ευρώπη	A-1
A.2	FIDIS	A-3
A.3	PRIME.....	A-3
A.4	IDADC	A-3
A.5	CROMBIES	A-4

A.6	SPOCS.....	A-4
A.7	PEPPOL.....	A-4
A.8	OpenPEPPOL.....	A-5
A.9	STORK.....	A-5
A.10	TABULA RASA.....	A-7
A.11	E-SENS.....	A-7

Παράρτημα Β: Τεχνικά Χαρακτηριστικά Εγγράφων Ταυτότητας και Ταξιδιού

B.1	Επιγραμμικό Δημόσιο Μητρώο Γνήσιων Εγγράφων Ταυτότητας και Ταξιδιού	B-1
-----	---------------------------------------------------------------------	-----

Κατάλογος Πινάκων

Πίνακας 2.1:	Κράτη - μέλη Ευρωπαϊκής Ένωσης ανά έτος ένταξης και κατά αλφαβητική σειρά.....	6
Πίνακας 2.2:	Φυσική Ταυτοποίηση πολιτών στην Ευρωπαϊκή Ένωση	8
Πίνακας 2.3:	Τεχνικά χαρακτηριστικά ηλεκτρονικών καρτών - ταυτοτήτων.....	31
Πίνακας 2.4:	Μοναδικά αναγνωριστικά πολιτών στην Ευρωπαϊκή Ένωση	37
Πίνακας 4.1:	Επίπεδα αξιολόγησης υπηρεσιών Ηλεκτρονικής Διακυβέρνησης.....	59
Πίνακας 4.2:	Ηλεκτρονικές Πύλες κρατών μελών Ευρωπαϊκής Ένωσης κατά αλφαβητική σειρά.....	66
Πίνακας 4.3:	Κατάταξη 10 καλύτερων ευρωπαϊκών χωρών βάσει του δείκτη ανάπτυξης e-gov	70
Πίνακας 5.1:	Χαρακτηριστικά επιπέδων εμπιστοσύνης Ελληνικού Πλαισίου Αυθεντικοποίησης	75
Πίνακας 5.2:	Απαιτήσεις Ασφαλείας Επιπέδων Αυθεντικοποίησης	77
Πίνακας 5.3:	Απαιτήσεις Πολιτών και Υπηρεσιών ανά Επίπεδο Εγγραφής.....	78
Πίνακας 5.4:	Διακριτικά Αυθεντικοποίησης Χρηστών.....	80
Πίνακας 5.5:	Υποστήριξη Αυθεντικοποίησης Υποδομής Δημοσίου Κλειδιού στην ΕΕ.....	85
Πίνακας Β.1:	Αγγλο-ελληνικό λεξικό χαρακτηριστικών ασφαλείας ταξιδιωτικών εγγράφων.....	B-2

Κεφάλαιο 1

Εισαγωγή

Για κάθε άνθρωπο, ως μοναδική οντότητα, καταγράφεται η ανάγκη δήλωσης της ύπαρξης του για την ένταξή του στην ομαλή λειτουργία της πολιτείας. Συνήθως κατά την γέννηση ενός ανθρώπου ακολουθούνται οι προβλεπόμενες διαδικασίες, ανά κράτος, ώστε να καταχωρείται η ύπαρξη της οντότητας. Συνεπώς, από την γέννηση ενός ανθρώπου τίθεται το θέμα καταγραφής του σε ένα σύστημα. Με την πάροδο των χρόνων και καθώς ο άνθρωπος μεγαλώνει, εμπλέκεται σε διαδικασίες όπου πρέπει να πιστοποιήσει την ταυτότητά του. Συνήθως αυτό συμβαίνει με την προσκόμιση ενός εγγράφου. Πλέον, ζούμε στην εποχή του Διαδικτύου. Και εδώ τα πράγματα αλλάζουν. Και οι άνθρωποι πια πρέπει να πιστοποιήσουν την ταυτότητά τους σε ένα ηλεκτρονικό σύστημα. Με αυτόν τον τρόπο ο άνθρωπος οδηγείται στην εποχή της Ηλεκτρονικής Διακυβέρνησης.

1.1 Ταυτότητα του πολίτη

Για την ανάδειξη της σημασίας της ταυτοποίησης των πολιτών χρειάζεται να γυρίσουμε το ρολόι μας πίσω αρκετούς αιώνες. Στην Αρχαία Αθήνα, παρόλο που στην Εκκλησία του Δήμου συμμετείχαν μόνο οι άνδρες άνω των 18 ετών οργανώθηκε η δημοκρατική κοινότητα όπου οι

πολίτες μπορούσαν να λένε τη γνώμη τους ελεύθερα, να αναγνωρίζουν καλύτερα τους εαυτούς τους, να εκλέγονται και να αποφασίζουν [64].

Πρόσθετα, στις θεατρικές παραστάσεις και συγκεκριμένα στα Διονύσια απαιτούνταν ο καθορισμός ταυτότητας του Αθηναίου πολίτη, ενώ ο Αριστοτέλης καθόρισε στα Πολιτικά τον ορισμό του αρχαίου Έλληνα πολίτη κάνοντας αναφορά στα χαρακτηριστικά του πολίτη. Το κύριο χαρακτηριστικό ήταν το όνομα του πολίτη. Αυτό όμως δεν ήταν αρκετό. Όπως αναφέρει ο Όμηρος χρειάστηκε ένα πρόσθετο διακριτικό όνομα, το σύγχρονο επώνυμο και δίδονταν συνήθως το πατρωνυμικό επίθετο [03]. Προσφιλή για όλους ήταν τα ονόματα του Αχιλλεύς Πηλείδη (από τον πατέρα του Πηλέα), του Οδυσσέα Λαερτιάδη και του Αγαμέμνονα Ατρείδη. Σε άλλες περιπτώσεις προστίθεται και η καταγωγή του ατόμου, ώστε να προσδοθεί μεγαλύτερη ακρίβεια, ως προπομπός της ανάγκης μοναδικότητας της ταυτότητας. Παράδειγμα αποτελεί η ονομασία του Θουκυδίδη Ολόρου Αλιμούσιου.

Αργότερα, περί τον 16^ο έως 18 αιώνα, στον δυτικό κόσμο υπήρξε μια μετάβαση από τα έως τότε βασίλεια στα έθνη κράτη. Σύντομα χάθηκε η εθνική ταυτότητα και η ιδιότητα του πολίτη και η απουσία της διάκρισης παραμένει μέχρι την Γαλλική επανάσταση. Οι Γάλλοι πολιτικοί και συγγραφείς της ρομαντικής περιόδου γίνονται υπέρμαχοι μιας συλλογικής ταυτότητας που κατέληξε να είναι η ιδιότητα του πολίτη. Στην συνέχεια, ο Άγγλος οικονομολόγος Alfred Marshall συνδέει την ιδιότητα του πολίτη με τον πολιτισμένο βίο και πλέον η εθνική ταυτότητα συνδέεται με την κοινωνική τάξη.

Στην Αρχαία Ελλάδα υπήρχαν οι πόλεις-κράτη. Σήμερα, στην Ευρωπαϊκή Ένωση υπάρχουν τα κράτη-μέλη. Παραλληλίζοντας το τότε με το σήμερα διαπιστώνεται η ανάγκη απόδοσης της ταυτότητας των πολιτών με ένα τρόπο αποδεκτό από την Ευρωπαϊκή Ένωση. Πλέον όμως οι πολίτες των κρατών ταξιδεύουν, μετοικούν σε άλλες χώρες και πρέπει να ταυτοποιούνται στην Ευρωπαϊκή Ένωση με τρόπο που να διευκολύνει τον τρόπο ζωής τους και όχι να τον δυσχεραίνει. Παρόλο που ανά κράτος υπάρχουν έντυπα μέσα και μηχανισμοί διαχείρισης ταυτοποίησης για τους πολίτες, οδηγούμαστε στην ηλεκτρονική ταυτότητα προσδοκώντας να δοθεί μια διασυνοριακή ταυτότητα στους πολίτες για την διευκόλυνση τους σε οποιαδήποτε ηλεκτρονική συναλλαγή.

1.2 Ηλεκτρονική Ταυτοποίηση

Θέτοντας τον ορισμό της Ηλεκτρονικής ταυτοποίησης (electronic Identification, συνοπτικά αναφερόμενη ως «eID») αναφερόμαστε στην διαδικασία βάσει την οποίας καθορίζεται με σαφήνεια η ταυτότητα μιας οντότητας κατά την χρήση ηλεκτρονικών μέσων. Μείζον ζήτημα δεν αποτελεί η ταυτοποίηση από ένα μόνο σύστημα σε μια καθορισμένη γεωγραφική περιοχή, αλλά η παροχή της διαδικασίας από πολλά κράτη μέλη της Ευρωπαϊκής Ένωσης.

Ζητούμενο λοιπόν είναι η ύπαρξη και η υποστήριξη μηχανισμών από τα Ευρωπαϊκά κράτη-μέλη, προκειμένου να απλοποιηθούν οι ηλεκτρονικές συναλλαγές των πολιτών με τον βέλτιστο ασφαλή τρόπο. Στην Ευρώπη, υπάρχουν πολλά κράτη μέλη που χρησιμοποιούν τεχνολογικές λύσεις (π.χ. έξυπνες κάρτες, κινητά τηλέφωνα) για να παρέχουν υπηρεσίες στους πολίτες τους. Ορισμένα κράτη μέλη συνδυάζουν την ηλεκτρονική ταυτότητα «e-ID» με τη λειτουργία του δελτίου ταυτότητας που χρησιμοποιείται και ως ταξιδιωτικό έγγραφο, όπως προδιαγράφεται από τους κανονισμούς του ICAO. Σε άλλα κράτη ορισμένοι υπάλληλοι έχουν μια κάρτα πολίτη για την πρόσβαση σε δημόσιες υπηρεσίες σε απευθείας σύνδεση, άλλοι εργάζονται με φορητές συσκευές, ή με συνδυασμό καρτών και τηλεφώνου.

Η ηλεκτρονική αναγνώριση αποτελεί μια λύση για την διακρατική αναγνώριση των πολιτών. Ωστόσο, εάν δεν ληφθούν κατάλληλα μέτρα ασφαλείας για την υποστήριξη του μηχανισμού ασφαλείας, τα στοιχεία των πολιτών μπορούν να προσχωρήσουν σε μη εξουσιοδοτημένες οντότητες. Οικοδομώντας την έννοια της ηλεκτρονικής ταυτότητας πρέπει να αναφερθεί η αξία της διασφάλισης της ιδιωτικότητας και της ασφαλείας των δεδομένων των πολιτών από την Ηλεκτρονική διακυβέρνηση. Θωρακίζοντας την ασφάλεια των προσωπικών δεδομένων των πολιτών, με την κατάλληλη τεχνολογία παρέχεται η διασφάλιση ότι τα δεδομένα τους υποβάλλονται σε θεραπεία με πλήρη σεβασμό της ισχύουσας νομοθεσίας περί προστασίας δεδομένων [108].

Όπως αναφέρεται στην στρατηγική «Ευρώπη 2020»[92], η ηλεκτρονική ταυτότητα μπορεί να εγγυηθεί την αδιαμφισβήτητη ταυτοποίηση ενός προσώπου και να καταστήσει δυνατή την παροχή υπηρεσίας στο πρόσωπο που πραγματικά το δικαιούται. Επισημαίνεται όμως η έλλειψη κοινής νομικής βάσης για τα κράτη μέλη, με αποτέλεσμα να μην μπορεί να καταστεί δυνατή η αναγνώριση και αποδοχή των ηλεκτρονικών ταυτοτήτων που εκδίδονται σε άλλα κράτη μέλη. Η ανεπαρκής διασυνοριακή διαλειτουργικότητα των εθνικών ηλεκτρονικών ταυτοτήτων (κενά στην τεχνική και οργανωτική διαλειτουργικότητα) εμποδίζει τους πολίτες και τις επιχειρήσεις να ωφεληθούν πλήρως από την ψηφιακή ενιαία αγορά.

1.3 Δομή της Εργασίας

Στην εισαγωγή έγινε μια σύντομη αναφορά στην έννοια της ταυτοποίησης των πολιτών καταδεικνύοντας την σπουδαιότητά της, μιας και οι βάσεις της τέθηκαν από την αρχαιότητα. Δεδομένου ότι σήμερα πια ζούμε στην ηλεκτρονική εποχή, οι πολίτες έχουν ανάγκη την διασυνοριακή τους ταυτοποίηση και

οδηγούμαστε στην ηλεκτρονική ταυτότητα και στην υιοθέτηση περιβαλλόντων Ηλεκτρονικής Διακυβέρνησης.

Στα κεφάλαια που ακολουθούν εξετάζονται οι παράμετροι του τίτλου της διατριβής. Οραματιζόμενη μια ροζέτα όπου στο κέντρο της βρίσκεται η έννοια της ταυτοποίησης απεικονίζονται οκτώ φύλλα. Τα έξι φύλλα αποτυπώνονται σε αντίστοιχα κεφάλαια όπου περιγράφονται οι πολιτικές ταυτοποίησης, οι οδηγίες της Ευρωπαϊκής Ένωσης, η Ηλεκτρονική Διακυβέρνηση, οι πολιτικές αυθεντικοποίησης, η Ελληνική πραγματικότητα και τα συμπεράσματα της μελέτης. Τα δύο τελευταία φύλλα αφορούν τα δύο παραρτήματα της μελέτης, όπου στο πρώτο αναφέρονται ευρωπαϊκά έργα και στο δεύτερο περιλαμβάνεται ένα αγγλοελληνικό λεξικό τεχνικών χαρακτηριστικών των εγγράφων ηλεκτρονικής ταυτοποίησης.

Στο κεφάλαιο 2 αναφέρονται τα μέσα ταυτοποίησης που διατηρούν τα είκοσι οκτώ (28) κράτη μέλη της Ευρωπαϊκής Ένωσης [105]. Κάθε κράτος μέλος διατηρεί τα δικά του μέσα ταυτοποίησης. Πέρα από τα παραδοσιακά μέσα ταυτοποίησης (τις συνηθισμένες χάρτινες ταυτότητες), έχουν σχεδιαστεί ή αναπτυχθεί ηλεκτρονικές ταυτότητες (έξυπνες κάρτες ή ηλεκτρονικά μέσα με βιομετρικά στοιχεία) για την υιοθέτηση του πλαισίου της Ηλεκτρονικής Διακυβέρνησης.

Στο κεφάλαιο 3 παρατίθενται οι Οδηγίες της Ευρωπαϊκής Ένωσης για την προστασία των προσωπικών δεδομένων, την διατήρηση δεδομένων, την προστασία των δικαιωμάτων και την παροχή υπηρεσιών. Αναφορικά με την προστασία των προσωπικών δεδομένων αναλύονται οι ψηφιακές υπογραφές, τα ψηφιακά πιστοποιητικά και οι προηγμένες ηλεκτρονικές υπογραφές.

Στο κεφάλαιο 4 αναλύεται η έννοια της Ηλεκτρονικής Διακυβέρνησης. Γίνεται αναφορά στα χαρακτηριστικά της και στους κύριους άξονες που πρέπει να ακολουθούν τα κράτη μέλη προκειμένου να επιτύχουν ένα επιτυχημένο σύστημα Ηλεκτρονικής Διακυβέρνησης. Ιδιαίτερη σημασία δίδεται στις παραμέτρους της Ιδιωτικότητας και της Διαλειτουργικότητας και τις σχέσεις τους με τα περιβάλλοντα Ηλεκτρονικής Διακυβέρνησης. Τέλος, παρατίθενται κάποιες προσεγγίσεις σχετικά με τα ευρωπαϊκά συστήματα Ηλεκτρονικής Διακυβέρνησης.

Στο κεφάλαιο 5 εξετάζονται οι πολιτικές Αυθεντικοποίησης. Αναλύεται η έννοια της αυθεντικοποίησης και παρουσιάζονται οι υπάρχουσες ευρωπαϊκές πολιτικές υποδομής δημοσίου κλειδιού και οι πολιτικές αναγνωριστικών. Σε ξεχωριστή παράγραφο του κεφαλαίου γίνεται αναφορά στην ασφάλεια των πολιτικών αυθεντικοποίησης, ενώ παρατίθενται πολιτικές αυθεντικοποίησης των κρατών μελών και ορισμένες υλοποιήσεις συστημάτων αυθεντικοποίησης.

Στο κεφάλαιο 6 παρουσιάζεται το πλαίσιο για την ηλεκτρονική ταυτοποίηση στην ελληνική πραγματικότητα και Διακυβέρνηση. Συγκεκριμένα, παρατίθεται το υφιστάμενο θεσμικό πλαίσιο καλύπτοντας τεχνικά και νομικά θέματα, γίνεται παρουσίαση της Κάρτας Πολίτη και των εμπλεκόμενων φορέων για την υλοποίησή της και οι δράσεις της Ομάδας Ηλεκτρονικής Διακυβέρνησης.

Το κεφάλαιο 7 αποτελεί τον επίλογο της μελέτης Ανάλυσης Πολιτικών Ηλεκτρονικής Ταυτοποίησης σε Περιβάλλοντα Ηλεκτρονικής Διακυβέρνησης στην Ευρώπη, όπου καταγράφονται τα συμπεράσματα της μελέτης και αναφέρεται το ευρωπαϊκό όραμα για το μέλλον των πολιτικών ηλεκτρονικής ταυτοποίησης.

Το παράρτημα απαρτίζεται από δύο τμήματα. Στο πρώτο τμήμα της μελέτης αναφέρονται περιληπτικά διάφορα έργα που έχουν υλοποιηθεί σχετικά με την ενίσχυση της ιδιωτικότητας των συστημάτων διαχείρισης ταυτότητας, την παροχή διαλειτουργικότητας σε πανευρωπαϊκές υπηρεσίες ηλεκτρονικής διακυβέρνησης, στις δημόσιες υπηρεσίες, στις επιχειρήσεις και στους πολίτες. Όλα τα έργα προσανατολίζονται στην εναρμόνιση των κρατών μελών σε ασφαλή ηλεκτρονικά συστήματα ταυτοποίησης των πολιτών παρέχοντας υψηλές υπηρεσίες σε ευρωπαϊκό πλαίσιο. Το δεύτερο τμήμα περιλαμβάνει ένα αγγλοελληνικό λεξικό με τα τεχνικά χαρακτηριστικά των εγγράφων ταυτοποίησης (συμπεριλαμβανομένων και των ηλεκτρονικών καρτών) και των ευρωπαϊκών ταξιδιωτικών εγγράφων από το Συμβούλιο της Ευρωπαϊκής Ένωσης.

Κεφάλαιο 2

Πολιτικές Ταυτοποίησης Πολιτών

Στο παρόν κεφάλαιο αναφέρονται τα μέσα ταυτοποίησης που διατηρούν τα κράτη μέλη της Ευρωπαϊκής Ένωσης [105]. Πριν την παρουσίαση των ευρημάτων, ακολουθεί ο πίνακας 2.1 όπου αναφέρονται τα 28 κράτη μέλη της Ευρωπαϊκής Ένωσης ανά χρονολογία ένταξης τους στην Ευρωπαϊκή Ένωση.

Έτος Ένταξης	Κράτος Μέλος
1952	Βέλγιο, Γαλλία, Γερμανία, Ιταλία, Λουξεμβούργο, Ολλανδία
1973	Δανία, Ηνωμένο Βασίλειο, Ιρλανδία
1981	Ελλάδα
1986	Ισπανία, Πορτογαλία

1995	Αυστρία, Σουηδία, Φινλανδία
2004	Εσθονία, Κύπρος, Λετονία, Λιθουανία, Μάλτα, Ουγγαρία, Πολωνία, Σλοβακία, Σλοβενία, Τσεχία
2007	Βουλγαρία, Ρουμανία
2013	Κροατία

Πίνακας 2.1: Κράτη - μέλη Ευρωπαϊκής Ένωσης ανά έτος ένταξης και κατά αλφαβητική σειρά.

Στις επόμενες ενότητες παρατίθενται πίνακες με τα εξεταζόμενα στοιχεία των κρατών μελών, οι οποίοι ακολουθούν αλφαβητική ταξινόμηση των κρατών (για λόγους ευκολότερης αναζήτησης στα στοιχεία του πίνακα).

2.1 Φυσική Ταυτοποίηση

Στο κεφάλαιο 1 αναφέρθηκε η σημασία της ταυτοποίησης των ανθρώπων. Στην παρούσα ενότητα θα αναφερθούν τα μέσα με τα οποία πραγματοποιείται η φυσική ταυτοποίηση των πολιτών στα κράτη μέλη της Ευρωπαϊκής Ένωσης, τα οποία ακολουθούν τις προδιαγραφές του πρότυπου που έθεσε η Ευρωπαϊκή Ένωση το 2006.

Στα φυσικά μέσα περιλαμβάνονται οι προσωπικοί αριθμοί ταυτοποίησης, τα δελτία ταυτοποίησης των πολιτών, τα διαβατήρια, τα πιστοποιητικά που εκδίδουν οι αρμόδιες υπηρεσίες κάθε χώρας και οι κάρτες που περιλαμβάνουν στοιχεία αναγνώρισης των πολιτών χωρίς την παρουσία πλινθίου (chip). Συνήθως τα κράτη εκδίδουν φυσικά μέσα ταυτοποίησης σε πολίτες άνω των 12 ετών. Ως επί το πλείστον, η ταυτοποίηση των παιδιών πραγματοποιείται με το πιστοποιητικό γέννησης.

Για την καλύτερη κατανόηση των αποτελεσμάτων της μελέτης, τα ευρήματα παρουσιάζονται σε μορφή πίνακα. Ο πίνακας 2.2 περιλαμβάνει ανά κράτος τα φυσικά μέσα με τα οποία πραγματοποιείται η ταυτοποίηση των πολιτών στα κράτη μέλη της Ευρωπαϊκής Ένωσης. Στις στήλες του πίνακα περιλαμβάνεται το μέσο ταυτοποίησης και μια περιγραφή του μέσου ταυτοποίησης. Τα κράτη διατάσσονται στις γραμμές του πίνακα σε αλφαβητική σειρά.

Σημειώνεται ότι τα εθνικά δελτία ταυτότητας που συμπεριλαμβάνουν την πληροφορία της ιθαγένειας των πολιτών αποτελούν και επίσημα ταξιδιωτικά έγγραφα [134].

Κράτος Μέλος	Φυσικά Μέσα Ταυτοποίησης Πολιτών	
	Μέσο	Περιγραφή
Αυστρία	Πιστοποιητικό Γέννησης, γάμου και θανάτου	Τα μέσα αυτά είναι αποσπάσματα από το Ληξιαρχείο και περιλαμβάνουν το όνομα της οικογένειας, το όνομα του προσώπου, την ημερομηνία και τον τόπο γέννησης, το φύλο και τα στοιχεία των γονέων και την θρησκευτική κοινότητα. Οι κάρτες ταυτοποίησης στην Αυστρία κατατάσσονται στα ηλεκτρονικά μέσα [130].
Βέλγιο	Κάρτα ταυτότητας Πιστοποιητικά ταυτοποίησης, γέννησης, γάμου και θανάτου	Η κάρτα ταυτότητας (carte d'identrtte / identiteitskaart / Personalausweis) χορηγείται σε παιδιά ηλικίας 12 ετών, ενώ είναι υποχρεωτική από την ολοκλήρωση των 15 ετών. Το πιστοποιητικό ταυτοποίησης αφορά παιδιά ηλικίας έως 12 ετών [139]. Τα πιστοποιητικά αυτά παρέχονται ηλεκτρονικά μέσω του συστήματος IRISBOX [59].
Βουλγαρία	Κάρτα / Ταυτότητα (ID)	Η κάρτα χορηγείται υποχρεωτικά σε πολίτες ηλικίας 14 ετών και άνω. Η κάρτα περιλαμβάνει τα στοιχεία του προσώπου και το 10ψηφιο αριθμό αναγνώρισης της κάρτας (Ε^ΗΗΘΗ γρα>ΚflаНСКН НОМӨР). Τα έξι πρώτα ψηφία αναφέρονται στην ημερομηνία γέννησης του πολίτη, τα επόμενα τρία στην περιοχή γέννησης, την σειράγέννησης και το φύλο. Το τελευταίο ψηφίο αποτελεί ψηφίο ελέγχου εγκυρότητας της ταυτότητας [59].
Γαλλία	Εθνική ταυτότητα (CNIS)	Η εθνική ταυτότητα αποτελεί προαιρετικό έγγραφο με διάρκεια ισχύος τα 15 έτη από την ημερομηνία έκδοσής του. [148]. Για κάθε πολίτη αναγράφεται το ονοματεπώνυμό του,
	Διαβατήριο (Passport)	μια φωτογραφία και η διεύθυνση κατοικίας του. Το δακτυλικό αποτύπωμα του πολίτη είναι μόνο σε έντυπη μορφή.
Γερμανία	Δελτίο αστυνομικής ταυτότητας Διαβατήριο Πιστοποιητικό γέννησης	Το δελτίο ταυτότητας ((Personalausweis) αποτελεί υποχρεωτικό έγγραφο και απευθύνεται σε πολίτες άνω των 16 ετών, αλλά πλέον υιοθετεί ηλεκτρονικό χαρακτήρα [59]. Το πιστοποιητικό γέννησης αποδεικνύει την ταυτότητα του παιδιού.
Δανία	Δελτίο ταυτότητας Διαβατήριο	Δεν είναι υποχρεωτική η κτήση δελτίου ταυτότητας. Παρόλα αυτά, στο δελτίο ταυτότητας και το διαβατήριο αναγράφεται ο

		προσωπικός αριθμός ταυτοποίησης (Det Centrale Personregister), μέσω του οποίου οι πολίτες χαρακτηρίζονται μοναδικά [51].
Ελλάδα	Δελτίο αστυνομικής ταυτότητας Ληξιαρχική πράξη γέννησης	Το δελτίο αστυνομικής ταυτότητας είναι υποχρεωτικό σε πολίτες άνω των 12 ετών με δεκαπενταετή διάρκεια ισχύος [160]. Από το 2000 αναγράφονται με λατινικούς χαρακτήρες το ονοματεπώνυμο και το πατρώνυμο του πολίτη και επιτρέπουν την μετακίνηση των πολιτών εντός ΕΕ. Η ληξιαρχική πράξη γέννησης είναι το πρώτο υποχρεωτικό έγγραφο που αποδεικνύει την γέννηση και καταγραφή ενός παιδιού.
Εσθονία		Δεν υπάρχει δελτίο ταυτότητας, αλλά οι πολίτες χαρακτηρίζονται μοναδικά από τον Προσωπικό αριθμό ταυτοποίησης isikukood (IK).
Ηνωμένο Βασίλειο	Διαβατήριο, δίπλωμα οδήγησης	Η Βρετανική κυβέρνηση αποφάσισε το 2011 να καταργήσει το σύστημα εθνικής ταυτοποίησης των πολιτών [167]. Η ταυτοποίηση πραγματοποιείται από τα διαβατήρια και τις άδειες οδήγησης των πολιτών.
Ιρλανδία		Η Δημοκρατία της Ιρλανδίας δεν έχει επίσημο έγγραφο ταυτότητας. Ο προσωπικός αριθμός δημόσιας υγείας είναι το μοναδικό αναγνωριστικό των Ιρλανδών πολιτών (Personal Public Service Number - PPS No).
Ισπανία	Δελτίο ταυτότητας	Το δελτίο ταυτότητας (Documento Nacional de Identidad) εκδίδεται για ισπανούς πολίτες, αλλά και αλλοδαπούς κατοίκους και αποτελεί υποχρεωτικό έγγραφο με την συμπλήρωση των 14 ετών. Η ταυτότητα χαρακτηρίζεται από ένα μοναδικό 8ψήφιο αριθμό (Documento Nacional de Identidad - DNI) που είναι κοινός για φορολογικούς, νομικούς σκοπούς, αλλά και την κοινωνική ασφάλιση. Το δελτίο ταυτότητας περιλαμβάνει το ονοματεπώνυμο του πολίτη, ημερομηνία γέννησης, την υπογραφή του πολίτη, στοιχεία διαμονής, την ημερομηνία έκδοσης και λήξης και την εκδούσα αρχή.
Ιταλία	Δελτίο ταυτότητας	Το δελτίο ταυτότητας (Carta d'identita) δεν θεωρείται υποχρεωτικό έγγραφο. Αποτελείται από τέσσερα φύλλα και περιλαμβάνει τα προσωπικά στοιχεία του πολίτη (ονοματεπώνυμο,

		πατρώνυμο), ημερομηνία γέννησης, οικογενειακή κατάσταση, χρώμα ματιών, ύψος, στοιχεία διαμονής, την εκδούσα αρχή και την ημερομηνία έκδοσης.
Κροατία	Δελτίο ταυτότητας	Η εθνική ταυτότητα χορηγείται υποχρεωτικά στους πολίτες άνω των 16 ετών, ενώ είναι υποχρεωτική η επίδειξή της σε κάθε έλεγχο (με κίνδυνο επιβολής προστίμου).
Κύπρος	Δελτίο πολιτικής ταυτότητας	Το δελτίο υποχρεωτικής ταυτότητας χορηγείται υποχρεωτικά στους πολίτες άνω των 12 ετών.
Λετονία	Δελτίο ταυτότητας Διαβατήριο	Το δελτίο ταυτότητας χορηγείται υποχρεωτικά στους πολίτες άνω των 15 ετών. Το διαβατήριο και η ταυτότητα αποδεικνύουν εξίσου την ταυτότητα του πολίτη στις συναλλαγές με το δημόσιο τομέα. Κάθε πολίτης διατηρεί ένα προσωπικό κωδικό (Personas kods) [175]
Λιθουανία	Δελτίο ταυτότητας	Το δελτίο ταυτότητας χορηγείται υποχρεωτικά στους πολίτες άνω των 16 ετών, με 10ετή διάρκεια ισχύος, ενώ για πολίτες κάτω των 16 ετών η διάρκεια ισχύος ορίζεται στα 5 έτη [178]. Κάθε πολίτης διατηρεί ένα προσωπικό κωδικό (Asmens kodas).
Λουξεμβούργο	Δελτίο ταυτότητας	Το δελτίο ταυτότητας χορηγείται υποχρεωτικά στους πολίτες άνω των 15 ετών, με 10ετή διάρκεια ισχύος [182]. Οι πολίτες διατηρούν ένα μοναδικό αριθμό, τον εθνικό αριθμό μητρώου NIF (Numero ^identification national), που αναγράφεται στο βιβλιάριο κοινωνικών ασφαλίσεων.
Μάλτα	Δελτίο ταυτότητας	Το δελτίο ταυτότητας είναι υποχρεωτικό για πολίτες άνω των 14 ετών. Το δελτίο συμπεριλαμβάνει τον αριθμό προσωπικού εγγράφου ταυτότητας (Kartatal-Identita).
Ολλανδία	Δελτίο ταυτότητας Διαβατήριο Δίπλωμα οδήγησης	Το δελτίο ταυτότητας χορηγείται υποχρεωτικά στους πολίτες άνω των 14 ετών. Το διαβατήριο και το δίπλωμα οδήγησης αποδεικνύουν εξίσου την ταυτότητα του πολίτη στις συναλλαγές με το δημόσιο τομέα.
Ουγγαρία	Δελτίο ταυτότητας	Το δελτίο ταυτότητας (zemelyazonosito igazolvany) είναι υποχρεωτικό για τους πολίτες άνω των 14 ετών, αλλά μπορεί να εκδοθεί από την ημερομηνία γέννησης του Ούγγρου πολίτη. Κάθε πολίτης διατηρεί ένα προσωπικό αριθμό μητρώου (Szemelyi azonosito szam)

Πολωνία	Δελτίο ταυτότητας	<p>Το δελτίο ταυτότητας (Dowod osobisty) χορηγείται εθελοντικά στους πολίτες άνω των 18 ετών.</p> <p>Ωστόσο όλοι οι πολίτες διατηρούν υποχρεωτικά ένα μοναδικό αριθμό (PESEL, Powszechny Elektroniczny System Ewidencji Ludnosci) που αναφέρει την ημερομηνία γέννησης, το φύλο και έναν αριθμό ισοτιμίας.</p>
Πορτογαλία	Δελτίο ταυτότητας	<p>Το δελτίο ταυτότητας (Bilhete de identidade) είναι υποχρεωτικό από την ηλικία των 6 ετών.</p>
Ρουμανία	Δελτίο ταυτότητας	<p>Το δελτίο ταυτότητας (carte de identitate) χορηγείται υποχρεωτικά στην ηλικία των 14 ετών με δεκαετή ισχύ διάρκειας. Οι πολίτες διατηρούν υποχρεωτικά τον προσωπικό αριθμό μητρώου CNP (Cod Numeric Personal)</p> <p>Για τους πολίτες που δεν δικαιούνται Δελτίο ταυτότητας είναι διαθέσιμη η Προσωρινή ID με μονοετή διάρκεια.</p>
Σλοβακία	Δελτίο ταυτότητας	<p>Το δελτίο ταυτότητας (Občiansky preukaz) χορηγείται υποχρεωτικά στην ηλικία των 15 ετών.</p>
Σλοβενία	Δελτίο ταυτότητας Potni list (διαβατήριο)	<p>Το δελτίο ταυτότητας (Osebna izkaznica) χορηγείται υποχρεωτικά στην ηλικία των 18 ετών, αλλά μπορεί να εκδοθεί σε μικρότερη ηλικία. Η διάρκεια ισχύος του δελτίου διαφοροποιείται ανάλογα με την ηλικία του κατόχου σε 5 ή</p>

		10 έτη.
Σουηδία	Δελτίο ταυτότητας	Το δελτίο ταυτότητας δεν είναι υποχρεωτικό, αλλά δύναται να εκδοθεί από την ηλικία των 13 ετών. Για τις συναλλαγές των πολιτών απαιτείται έκδοση μοναδικού προσωπικού κωδικού (Personnummer) από την Φορολογική υπηρεσία.
Τσεχία	Δελτίο ταυτότητας	Το δελτίο ταυτότητας (OObcansky prukaz) εκδίδεται υποχρεωτικά σε ηλικία 15 ετών και αναγνωρίζεται ως ταξιδιωτικό έγγραφο στην Ευρωπαϊκή Ένωση.
Φινλανδία	Κάρτα ταυτότητας Διαβατήριο	Η κάρτα ταυτότητας (henkilokortti/identitetskort) και το διαβατήριο είναι προαιρετικά.

Πίνακας 2.2: Φυσική Ταυτοποίηση πολιτών στην Ευρωπαϊκή Ένωση [59]

Όλα τα κράτη μέλη έχουν επίσημες πηγές καταγραφής των στοιχείων των πολιτών, είτε είναι δημοτολόγια, ληξιαρχεία, φορολογικές υπηρεσίες και λοιπές δημόσιες υπηρεσίες. Μάλιστα σε πολλά κράτη, έχει αποδοθεί σε κάθε πολίτη ένας προσωπικός αριθμός ταυτοποίησης.

Η Αυστρία, η Εσθονία, το Ηνωμένο Βασίλειο και η Ιρλανδία δεν διατηρούν φυσικά μέσα ταυτοποίησης, αλλά διατηρούν μοναδικούς προσωπικούς αριθμούς ταυτοποίησης. Οι προσωπικοί αριθμοί ταυτοποίησης αποδίδονται κυρίως για φορολογικούς σκοπούς. Από τα 28 κράτη μέλη της Ευρωπαϊκής Ένωσης, δώδεκα εξ αυτών (Βέλγιο, Δανία, Εσθονία, Ισπανία, Φινλανδία, Κροατία, Λιθουανία, Λετονία, Μάλτα, Ολλανδία, Ρουμανία, Τσεχία) αναγράφουν τους προσωπικούς αριθμούς ταυτοποίησης στα μέσα ταυτοποίησης. Ο πίνακας 2.2 περιλαμβάνει τα ευρήματα των φυσικών μέσων ταυτοποίησης των πολιτών της Ευρωπαϊκής Ένωσης.

Αναφορικά με τις έντυπες ταυτότητες, από τα 28 κράτη μέλη της Ευρωπαϊκής Ένωσης, τα 18 κράτη διατηρούν υποχρεωτική την έκδοση ταυτοτήτων, ενώ 6 από αυτά την καθιστούν εθελοντική. Τα υπόλοιπα 4 κράτη (Αυστρία, Εσθονία, Ηνωμένο Βασίλειο, Ιρλανδία) δεν διαθέτουν ταυτότητες. Όμως, σε όλα τα κράτη υπάρχουν άλλου είδους παραστατικά, όπως πιστοποιητικά γέννησης, διαβατήρια, δίπλωμα οδήγησης που ταυτοποιούν ένα πρόσωπο.

Συμπερασματικά, τα κράτη διαθέτουν μηχανισμούς φυσικής ταυτοποίησης των πολιτών με την αναγραφή των προσωπικών στοιχείων τους, των στοιχείων κατοικίας, της ημερομηνίας έκδοσης, της εκδούσας αρχής, καθώς και της διάρκειας ισχύος του μέσου ταυτοποίησης.

2.2 Ηλεκτρονική Ταυτοποίηση

Στην παράγραφο 1.2 δόθηκε μια πτυχή του ορισμού της ηλεκτρονικής ταυτοποίησης. Σύμφωνα με τον ορισμό της Ευρωπαϊκής Επιτροπής «η ηλεκτρονική ταυτοποίηση είναι η διαδικασία της εξόρυξης της ταυτότητας ενός πολίτη με την χρήση ηλεκτρονικών μέσων» [41]. Η πρόοδος στο ζήτημα ηλεκτρονικής ταυτοποίησης είναι ιδιαίτερα σημαντική. Κατανοώντας τα οφέλη της ψηφιακής πραγματικότητας του Διαδικτύου σε συνδυασμό με την διαρκή αναζήτηση παραμέτρων που θα ενδυναμώνουν την ασφάλεια των συστημάτων eID, τα κράτη μέλη της Ευρωπαϊκής Ένωσης υιοθετούν το θεσμό της ηλεκτρονικής αναγνώρισης των πολιτών και μελετούν τις τεχνολογίες προκειμένου να επιτευχθεί ορθή αναγνώριση και ταυτοποίηση των πολιτών από κυβερνητικούς και μη οργανισμούς, ώστε να χορηγηθεί η πρόσβαση στις ψηφιακές τους υπηρεσίες.

Η ηλεκτρονική ταυτοποίηση υποστηρίζεται από τα κράτη μέλη με την έκδοση ηλεκτρονικών ταυτοτήτων (συμπεριλαμβανομένων των έξυπνων καρτών). Τα κράτη εκμεταλλευόμενα τα στοιχεία των ήδη εγκατεστημένων συστημάτων (Δημοτολογία, Μητρώα Πληθυσμού) σε συνδυασμό με τις ηλεκτρονικές κάρτες, την χρήση μοναδικών διαπιστευτηρίων (αναγνωριστικό και συνθηματικό χρήστη) για την σύνδεση σε μία ή περισσότερες εφαρμογές και την χρήση των βιομετρικών στοιχείων των πολιτών επιτυγχάνουν την αναγνώριση των πολιτών. Στις ακόλουθες ενότητες πραγματοποιείται μια ανάλυση των συνιστωσών των ηλεκτρονικών καρτών - ταυτοτήτων και των επιμέρους στοιχείων που συμβάλουν στην ταυτοποίηση του πολίτη.

2.2.1 Ηλεκτρονικές Κάρτες - Ταυτότητες

Για την υλοποίηση της ηλεκτρονικής ταυτοποίησης, τα κράτη μέλη στράφηκαν στην έκδοση των εθνικών ηλεκτρονικών καρτών - ταυτοτήτων¹. Έτσι, για κάθε πολίτη συλλέγονται οι πληροφορίες που καθορίζουν την οντότητά του (όπως αναγράφονται στο φυσικό μέσο ταυτοποίησης) και ενσωματώνονται σε μια πλαστική κάρτα που περιλαμβάνει ένα πλινθίο. Το πλινθίο αποδίδει στην κάρτα την ηλεκτρονική της υπόσταση και μέσω αυτής ο πολίτης έχει την

¹ Στην ενότητα αυτή οι εθνικές ηλεκτρονικές κάρτες αναφέρονται ως ηλεκτρονικές κάρτες, είτε ως ηλεκτρονικές ταυτότητες.

δυνατότητα ταυτοποίησης σε πλήθος υπηρεσιών εντός της χώρας του, αλλά και σε άλλα κράτη μέλη.

Ο σχεδιασμός μιας ηλεκτρονικής κάρτας δεν αποτελεί μια αυθαίρετη υπόθεση. Το μέγεθος, το είδος διεπαφής (ανεπαφικό, επαφικό, συνδυασμός και των δύο), τα στοιχεία που περιλαμβάνει, η δυνατότητα πρόσβασης για ανάγνωση ή τροποποίηση των στοιχείων των πολιτών (ICAO, BAC, PACE, EAC) και η χρήση μοναδικού αναγνωριστικού πολίτη αποτελούν τεχνικά χαρακτηριστικά μιας ηλεκτρονικής κάρτας

που το καθένα υποδηλώνει ξεχωριστές λειτουργίες. Για παράδειγμα ένα ανεπαφικό πλινθίο προσφέρει δυνατότητα μνήμης, ταχύτητα και ανθεκτικότητα, άρα και μεγαλύτερο χρόνο ζωής. Επίσης, το πρωτόκολλο PACE προϋποθέτει ανεπαφικό πλινθίο και απαιτεί από τον χρήστη την πληκτρολόγηση κωδικού για την προσπέλαση των δεδομένων και αποστολή ειδοποίησης στον πολίτη για την προσπέλαση των δεδομένων του [121]. Τέλος, η πλειοψηφία των κρατών μελών περιλαμβάνει βιομετρικά δεδομένα στις ηλεκτρονικές κάρτες². Στα βιομετρικά δεδομένα συγκαταλέγονται η φωτογραφία του πολίτη και τα δακτυλικά του αποτυπώματα.

Η σπουδαιότητα που προσδίδει η Ευρωπαϊκή Επιτροπή στο θέμα των ηλεκτρονικών ταυτοτήτων είναι ιδιαίτερα υψηλή. Τον Αύγουστο του 2013, η Ευρωπαϊκή Επιτροπή ανακοίνωσε την χρηματοδότηση ύψους 13,7 εκατομμυρίων ευρώ για διασυνοριακές ψηφιακές υπηρεσίες, ώστε να διασυνδέονται οι ηλεκτρονικές ταυτότητες των πολιτών σε εθνικό, αλλά και ευρωπαϊκό επίπεδο [104].

Στην ενότητα αυτή μελετώνται δύο ζητήματα : η πρόοδος των κρατών μελών σχετικά με την έκδοση εθνικών ηλεκτρονικών καρτών - ταυτοτήτων και τα τεχνικά χαρακτηριστικά των ταυτοτήτων. Για κάθε κράτος παρατίθενται στοιχεία αναφορικά με την ηλεκτρονική ταυτοποίηση, ενώ στον πίνακα 2.3 παρουσιάζονται τα χαρακτηριστικά των ηλεκτρονικών καρτών. Η παράθεση των κρατών γίνεται ονομαστικά.

² Εκτός από τις εθνικές ηλεκτρονικές κάρτες, υπάρχει πλήθος έξυπνων καρτών που εξυπηρετούν συγκεκριμένες υπηρεσίες, συναντώνται ως «τομεακές κάρτες» και παρέχουν πρόσβαση σε εξειδικευμένες υπηρεσίες (π.χ. φορολογικές υπηρεσίες, κάρτα μεταφορών, κάρτα υγείας).

Αυστρία

Η ηλεκτρονική κάρτα της Αυστρίας -όπως και το σύνολο των ηλεκτρονικών καρτών των άλλων κρατών- περιλαμβάνει το ονοματεπώνυμο του πολίτη, ένα αριθμό, την ημερομηνία γέννησης, την υπογραφή του κατόχου, το φύλο, τον τόπο γέννησης, το χρώμα ματιών, το ύψος, την αρχή έκδοσης, την ημερομηνία έκδοσης και την ημερομηνία λήξης, καθώς και ένα πλινθίο [132].

Η Αυστρία υποστηρίζει τη διαλειτουργικότητα για συστήματα προερχόμενα από το Βέλγιο, την Εσθονία, την Φινλανδία και την Ιταλία χρησιμοποιώντας την τεχνολογία MOA (Module for Online Application). Η διαχείριση των πολιτών πραγματοποιείται από το Κεντρικό Μητρώο Κατοίκων, ενώ οι πολίτες εκτός Αυστρίας παρακολουθούνται από το Συμπληρωματικό μητρώο, χρησιμοποιώντας ως SourcePIN το μοναδικό αναγνωριστικό της χώρας προέλευσής τους.

Από τις 15 Ιουνίου 2009, στα αυστριακά διαβατήρια (Reisepass) συμπεριλήφθηκε πλινθίο [129, 135], ενώ τα δελτία ταυτότητας (Personalausweis) απευθύνονται σε πολίτες με αυστριακή ιθαγένεια. Η ισχύς τους διαφοροποιείται ανάλογα με την ηλικία. Στα παιδιά έως 2 ετών η διάρκεια είναι διετής, στα παιδιά ηλικιών 2-12 η διάρκεια είναι πενταετής, ενώ μετά το 12ο έτος η διάρκεια είναι δεκαετής. Στα παιδιά και τους ανήλικους κάτω των 14 ετών, η αίτηση πρέπει να υποβληθεί από τον γονέα ή κηδεμόνα του ανηλίκου.

Μελετώντας την Έκθεση των Ηνωμένων Εθνών για το 2012, η Αυστρία καταλαμβάνει την πρώτη θέση για την πρόοδο της ως προς την Ηλεκτρονική Διακυβέρνηση [46]. Το αυστριακό σύστημα ηλεκτρονικής ταυτοποίησης «Citizen Card» ξεκίνησε το 2003, ως μέρος ενός γενικότερου κυβερνητικού πλάνου που θα παρείχε πρόσβαση σε δημόσιες υπηρεσίες από τους πολίτες με την χρήση ενός μοναδικού κωδικού και εξελίχτηκε πολύ γρήγορα [131]. Μόλις το 2005, η Αυστρία κατάφερε να διακριθεί στην πρώτη πεντάδα των ευρωπαϊκών συστημάτων ηλεκτρονικής ταυτοποίησης και διακυβέρνησης.

Βέλγιο

Το Βέλγιο ήταν η πρώτη ευρωπαϊκή χώρα που εισήγαγε την ηλεκτρονική κάρτα. Από το 2001 έως το 2004 το σύστημα ήταν σε πειραματικό στάδιο, ενώ από το 2009 η ηλεκτρονική κάρτα πολίτη είναι υποχρεωτική. Η κάρτα αναγράφει το όνομα του κράτους και την σήμανση «κάρτα ταυτότητας» σε τέσσερις γλώσσες. Η κάρτα αναφέρει το ονοματεπώνυμο του πολίτη, τον τόπο και την ημερομηνία γέννησης, το φύλο, την εθνικότητα, τον αριθμό της κάρτας (12ψήφιος αριθμός), την ημερομηνία λήξης, την υπογραφή, την φωτογραφία, ένα ολόγραμμα, τον εθνικό αριθμό καταχώρησης μητρώου (NRNP), τον τόπο έκδοσης και τον εκδότη. Στο ενσωματωμένο πλινθίο είναι αποθηκευμένα τα στοιχεία της διαμονής του πολίτη και δύο ψηφιακά πιστοποιητικά: ένα για τον έλεγχο ταυτότητας και ένα για ψηφιακή υπογραφή.

Οι ηλεκτρονικές κάρτες εκδίδονται από την ηλικία των δώδεκα ετών και διακρίνονται σε τρεις κατηγορίες : την ηλεκτρονική κάρτα πολιτών άνω των 12 ετών με την ονομασία «eID», την ηλεκτρονική κάρτα παιδιών ηλικίας κάτω των 12 ετών με την ονομασία «Kids-ID» και την ηλεκτρονική κάρτα των μη Βέλγων κατοίκων με την ονομασία «foreigners-card». Οι ηλεκτρονικές κάρτες eID έχουν διάρκεια ισχύος τα πέντε έτη, ενώ οι ηλεκτρονικές κάρτες των παιδιών ισχύουν για τρία έτη.

Οι πληροφορίες της ηλεκτρονικής κάρτας είναι προσβάσιμες από ένα αναγνώστη καρτών. Για τις ηλεκτρονικές συναλλαγές απαιτείται η χρήση του ψηφιακού πιστοποιητικού, καθώς και του μοναδικού αναγνωριστικού PIN που κατέχει αποκλειστικά ο κάτοχος της κάρτας. Ωστόσο, ο πολίτης δύναται κατά

την διάρκεια της ηλεκτρονικής συναλλαγής του να ελέγξει σε ποιες από τις πληροφορίες του θα έχει πρόσβαση η κυβέρνηση. Οι ηλεκτρονικές ταυτότητες των παιδιών δεν περιέχουν ψηφιακό πιστοποιητικό για υπογραφή, αλλά αναγράφουν τα ονοματεπώνυμα των γονέων τους [138].

Σύμφωνα με την Έκθεση των Ηνωμένων Εθνών για το 2012, το Βέλγιο βρίσκεται στην τέταρτη θέση της παγκόσμιας κατάταξης σχετικά με την πρόοδο και την ανάπτυξη των κρατών που αφορά την Ηλεκτρονική Διακυβέρνηση [46].

Βουλγαρία

Στα πλαίσια του έργου «Βελτίωση των διοικητικών υπηρεσιών στους καταναλωτές μέσω της διεύρυνσης των κεντρικών συστημάτων της Ηλεκτρονικής Διακυβέρνησης» και του προγράμματος «Διοικητική Ικανότητα» που χρηματοδοτείται από την Ευρωπαϊκή Ένωση, η Βουλγαρία αναπτύσσει το σύστημα διαχείρισης ηλεκτρονικών ταυτοτήτων για τους Βούλγαρους πολίτες.

Η ηλεκτρονική ταυτότητα θα αποδίδεται κατόπιν αιτήματος σε Βούλγαρους πολίτες άνω των 14 ετών, είτε αλλοδαπούς μόνιμους κατοίκους. Περιλαμβάνει μια έξυπνη κάρτα και έναν αριθμητικό κωδικό PIN, ενώ η φιλοσοφία στρέφεται προς ένα ενιαίο σύστημα από το οποίο ο πολίτης θα έχει πρόσβαση σε υπηρεσίες υγείας, παιδείας, δικαιοσύνης και οικονομίας, ενώ θα τελεί χρέη ταξιδιωτικού εγγράφου βάσει της μηχαναγνώσιμης περιοχής της [142].

Γαλλία

Από το 2001 έχει ξεκινήσει ο σχεδιασμός της γαλλικής ηλεκτρονικής ταυτότητας. Στο άκουσμα της είδησης της ηλεκτρονικής ταυτοποίησης των πολιτών υπήρξαν μεγάλες αντιδράσεις από τους πολίτες για τα θέματα ασφαλείας προσωπικών δεδομένων που διέγειραν οι νέες κάρτες. Με την πρόταση του σχεδίου νόμου «για την προστασία της ταυτότητας» (a la protection de l'identite) οι Γάλλοι πολίτες δεν είναι υποχρεωμένοι να εκδίδουν την ηλεκτρονική κάρτα, η οποία σύμφωνα με την ονομασία της «Carte nationale d' identite securisee (CNIS)» αποτελεί την ασφαλή ηλεκτρονική ταυτότητα των πολιτών. Η ηλεκτρονική κάρτα δίνει την δυνατότητα ταξιδιωτικού εγγράφου και από την 1^η Ιανουαρίου 2014 η ισχύς της διευρύνθηκε από 10 σε 15 έτη.

Η ηλεκτρονική κάρτα χωρίζεται σε δύο τμήματα : το «regalien» και το «services». Το πρώτο τμήμα θεωρείται το κυρίαρχο τμήμα της ηλεκτρονικής κάρτας. Σε αυτό, ενσωματώνονται δύο βιομετρικά χαρακτηριστικά, καθώς και τα δεδομένα που περιλαμβάνει η κλασική ταυτότητα του πολίτη. Το δεύτερο τμήμα περιλαμβάνει το ψηφιακό πιστοποιητικό προκειμένου να πραγματοποιείται η πρόσβαση στις

ψηφιακές υπηρεσίες και η ταυτοποίηση του πολίτη. Η παρακολούθηση χρήσης δεδομένων πραγματοποιείται από την επιτροπή CNIL (Commission nationale de l'informatique et des libertés) και η πρόσβαση στα βιομετρικά δεδομένα γίνεται μετά από δικαστική απόφαση [146,147].

Γερμανία

Οι Γερμανοί πολίτες είναι προσανατολισμένοι στην ηλεκτρονική εποχή και ζουν με σύμμαχο της Ηλεκτρονική Διακυβέρνηση. Από τα τέλη του 2010, με την συμπλήρωση του 16ου έτους ηλικίας τους οι πολίτες είναι υποχρεωμένοι να αποκτήσουν την ηλεκτρονική ταυτότητα, ενώ η γέννηση των βρεφών καταγράφεται άμεσα από τους γονείς τους, το γιατρό και την μαία σε ειδική ηλεκτρονική εφαρμογή.

Κάθε ηλεκτρονική ταυτότητα περιλαμβάνει φωτογραφία του πολίτη, έναν 9ψήφιο αριθμό εγγράφου και έναν 6ψηφιο αριθμό πρόσβασης του ανέπαφου πλινθίου. Πρόσθετα περιλαμβάνεται το ονοματεπώνυμο του πολίτη, η ημερομηνία γέννησης, η εθνικότητα, ο τόπος γέννησης, η ημερομηνία λήξης, το χρώμα ματιών, το ύψος, η χρονολογία έκδοσης, η εκδούσα αρχή, η διεύθυνση κατοικίας και η μηχανικώς αναγνώσιμη ζώνη. Η κάρτα περιλαμβάνει χαρακτηριστικά υψηλής ασφάλειας : ολογράφημα της φωτογραφίας του πολίτη, τρισδιάστατη μορφή του γερμανικού συμβόλου και κινεεγράφημα [150,199].

Η γερμανική ηλεκτρονική ταυτότητα μπορεί να χρησιμοποιηθεί για ασφαλείς οικονομικές συναλλαγές στο Διαδίκτυο, για συναλλαγές σε συστήματα Ηλεκτρονικής Διακυβέρνησης και ως ταξιδιωτικό έγγραφο. Σύμφωνα με την μελέτη των Ηνωμένων Εθνών για το 2012, η Γερμανία καταλαμβάνει την 5^η θέση όσον αφορά την συμμετοχή των πολιτών στις ηλεκτρονικές υπηρεσίες.

Δανία

Στην ενότητα 2.1 αναφέρθηκε πως κάθε Δανός πολίτης που εγγράφεται στο σύστημα Δημόσιας Διοίκησης λαμβάνει ένα μοναδικό προσωπικό αριθμό. Στην Δανία δεν υπάρχει ηλεκτρονικό δελτίο ταυτότητας που να συμπεριλαμβάνει τα στοιχεία ταυτοποίησης ενός πολίτη. Ωστόσο με την χρήση του διαβατηρίου, είτε του διπλώματος οδήγησης και του προσωπικού αριθμού ταυτοποίησης (Det Centrale Personregister), οι πολίτες χρησιμοποιούν πολλά συστήματα ηλεκτρονικής ταυτοποίησης.

Χρησιμοποιώντας τον αριθμό CPR υλοποιήθηκε το διαλειτουργικό σύστημα NetID [61] για συναλλαγές σε τραπεζικά συστήματα, δημόσιες υπηρεσίες και ιδιωτικές επιχειρήσεις που υποστηρίζουν το συγκεκριμένο σύστημα. Κάθε Δανός πολίτης ηλικίας άνω των 15 ετών μπορεί να αιτηθεί ενός μοναδικού αναγνωριστικού ονόματος, ενός συνθηματικού και μιας κάρτας κωδικών. Στην ουσία η κάρτα κωδικών είναι μια κάρτα που παράγει μοναδικούς τυχαίους αριθμούς περιορισμένης χρονικής διάρκειας για την

πραγματοποίηση μιας ηλεκτρονικής συναλλαγής. Το NemID διαφυλάσσει την ασφάλεια των πληροφοριών του χρήστη μιας και ο πολίτης πρέπει να συνδυάσει κάτι που γνωρίζει (αναγνωριστικό και συνθηματικό) και κάτι που κατέχει (κάρτα κωδικών). Ένα παράδειγμα εφαρμογής που είναι προσβάσιμη μέσω του NemID είναι η Αρχή Φορολόγησης της Δανίας (SKAT) που παρέχει δύο μεθόδους ηλεκτρονικής υπογραφής για ιδιώτες πολίτες και επιχειρήσεις με συνθηματικά μιας χρήσης, είτε ψηφιακά πιστοποιητικά.

Ελλάδα

Στην Ελλάδα, η Κάρτα Πολίτη έχει σχεδιαστεί και προβλέπεται να είναι υποχρεωτική. Πρόκειται να περιλαμβάνει τα στοιχεία που αναγράφονται στο κλασικό δελτίο ταυτότητας, μοναδικά αναγνωριστικά και ένα πλινθίο. Απόσπασμα από την εξαγγελία αναφέρει ότι η κάρτα πολίτη *«θα φέρει πλινθίο, μέσω του οποίου θα προσφέρεται, για όποιον πολίτη το επιθυμεί, η δυνατότητα ψηφιακής ανθεντικοποίησης κατά τη χρήση ηλεκτρονικών υπηρεσιών στο δημόσιο και τον ιδιωτικό τομέα, καθώς και η δυνατότητα παραγωγής ψηφιακής υπογραφής εγγράφων»*.

Η Κάρτα δεν θα αποθηκεύει δεδομένα, αλλά θα αποτελείτο ψηφιακό διαβατήριο ώστε ο πολίτης να μπορεί να προσπελάσει τα δεδομένα του που τηρούνται σε διακριτά συστήματα στο Δημόσιο τομέα με τη ρητή έγκριση και συγκατάθεση του, χωρίς γραφειοκρατικές καθυστερήσεις.

Εσθονία

Η Εσθονία είναι μια χώρα που κατάφερε να στηρίξει επαρκώς την εθνική ηλεκτρονική ταυτοποίηση. Η εσθονική ταυτότητα καλύπτει την φυσική, αλλά και την ηλεκτρονική της υπόσταση και αποκαλείται Εθνική κάρτα. Στο μπροστινό μέρος της κάρτας περιλαμβάνονται το όνομα του πολίτη, η φωτογραφία, η υπογραφή, ο προσωπικός αριθμός ταυτότητας, η ημερομηνία γέννησης, το φύλο, η ιθαγένεια, ο αριθμός της κάρτας και η ημερομηνία λήξης της κάρτας. Η πίσω πλευρά της κάρτας αναφέρει τον τόπο γέννησης, την ημερομηνία έκδοσης της κάρτας και την άδεια παραμονής, εφόσον υπάρχουν. Η εθνική κάρτα περιλαμβάνει πλινθίο και χρησιμοποιεί κρυπτογράφηση δημοσίου κλειδιού μήκους 2048-bit.

Σύμφωνα με την έκθεση της ITIF για το 2011, αναφέρεται ότι «στην Εσθονία έχουν εκδοθεί περίπου 1,2 εκατομμύρια e-ID έξυπνες κάρτες, για πληθυσμό 1,3 εκατομμύρια πολίτες (άτομα ηλικίας δεκαπέντε ετών και άνω) και οι κάτοχοί τους έχουν χρησιμοποιήσει τις e-ID για να παράξουν 52 εκατομμύρια και να επικυρώσουν περισσότερες από 88 εκατομμύρια ηλεκτρονικές συναλλαγές» [04]. Ως αποτέλεσμα, η Εσθονία έχει καταφέρει τη δημιουργία μιας εθνικής κάρτας με την οποία οι πολίτες μπορούν να ταξιδεύουν εντός της ΕΕ, να ταυτοποιούνται σε συστήματα ηλεκτρονικής τραπεζικής, να υπογράφουν ψηφιακά τις συναλλαγές τους, να ψηφίζουν, καθώς και να συνταγογραφούν τα φάρμακά τους [166].

Ηνωμένο Βασίλειο

Σύμφωνα με τον νόμο «Identity Documents Act 2010» της 21^{ης} Ιανουαρίου 2010 [167], η κυβέρνηση ακύρωσε τις εθνικές ηλεκτρονικές κάρτες και έλαβε την απόφαση να καταστρέψει το Εθνικό Μητρώο Ταυτοτήτων με κύριο σκοπό την εξοικονόμηση 86 £ εκατομμυρίων λιρών εντός τετραετίας, καθώς και την αποφυγή δαπάνης 800£ εκατομμυρίων λιρών για τα επόμενα δέκα χρόνια.

Ωστόσο, για το έτος 2015 προβλέπεται η δημιουργία ενός ξεχωριστού συστήματος έκδοσης ταυτοτήτων για τους αλλοδαπούς του Ηνωμένου Βασιλείου που θα περιλαμβάνουν βιομετρικά στοιχεία. Ως αποτέλεσμα, οι άδειες παραμονής των αλλοδαπών θα είναι στην ουσία βιομετρικές άδειες παραμονής και θα ακολουθούν τις προσταγές της νομοθεσίας της Ευρωπαϊκής Ένωσης [44,45].

Ιρλανδία

Από το 2011 οι Ιρλανδοί πολίτες έχουν στην διάθεσή τους την Κάρτα Δημόσιων Υπηρεσιών. Πρόκειται για μια βιομετρική κάρτα, που περιλαμβάνει σε ηλεκτρονική μορφή το ονοματεπώνυμο του πολίτη, φωτογραφία, την ημερομηνία, τον τόπο γέννησης, το φύλο, την εθνικότητα, όλα τα προηγούμενα επώνυμα, και όλα τα προηγούμενα επώνυμα της μητέρας του, καθώς και την υπογραφή και τον μοναδικό προσωπικό κωδικό PPS [36]. Ο κύριος λόγος υιοθέτησης των υποχρεωτικών ηλεκτρονικών καρτών ήταν η καταπολέμηση της απάτης.

Ισπανία

Σύμφωνα με το βασιλικό διάταγμα 1553/2005, της 23ης Δεκεμβρίου, σχετικά με το ζήτημα της εθνικής ταυτότητας και πιστοποιητικών ηλεκτρονικής υπογραφής, «οι Ισπανοί πολίτες με την ολοκλήρωση των 14 ετών έχουν την υποχρέωση να εκδώσουν την ηλεκτρονική κάρτα DNIE (DNI electronico de Espana a fecha actual)». Η μορφή της κάρτας θυμίζει πιστωτική κάρτα και περιλαμβάνει πλινθίο με ψηφιακές πληροφορίες. Η διάρκεια ισχύος της κυμαίνεται ανάλογα με την ηλικία του κατόχου της. Έτσι, πολίτες ηλικίας μέχρι των 30 ετών υποχρεούνται να ανανεώνουν την κάρτα ανά 5 έτη, πολίτες ηλικίας μεταξύ των 30-70 ετών εκδίδουν την νέα κάρτα ανά δέκα έτη, ενώ η κάρτα καθίσταται μη ανανεώσιμη για τους πολίτες άνω των 70 ετών.

Η κάρτα περιλαμβάνει το ονοματεπώνυμο του πολίτη, το φύλο, την εθνικότητα, την ημερομηνία γέννησης, τον αύξοντα αριθμό της κάρτας (IDESP), την ημερομηνία έκδοσης, την ιδιόχειρη υπογραφή του κατόχου, τον μοναδικό αριθμό της κάρτας, ένα χαρακτήρα ελέγχου, τα πρώτα σύμφωνα του πρώτου ονόματος και του πρώτου επωνύμου, και μια ασπρόμαυρη φωτογραφία. Πρόσθετα, αναγράφονται τα στοιχεία γέννησης, τα στοιχεία κατοικίας, τα ονοματεπώνυμα των γονέων και η εκδούσα αρχή της κάρτας.

Στο ενσωματωμένο πλινθίο περιλαμβάνονται κρυπτογραφημένα το ψηφιακό πιστοποιητικό του πολίτη, αρχή έκδοσης πιστοποιητικού, βιομετρικά δεδομένα των δακτυλικών αποτυπωμάτων, ψηφιακή φωτογραφία του πολίτη και ψηφιοποιημένη εικόνα της ιδιόχειρης υπογραφής,

Τα στοιχεία της κάρτας μπορούν να αναγνωστούν είτε από δημόσιες υπηρεσίες, είτε από υπηρεσίες του ιδιωτικού τομέα, είτε από τα σημεία ενημέρωσης των καρτών. [170]

Ιταλία

Στην Ιταλία, η ηλεκτρονική κάρτα CIE (Carta d'Identita Elettronica) ενέχει προαιρετικό χαρακτήρα για τους πολίτες άνω των 15 ετών. Περιλαμβάνει πλινθίο με ενσωματωμένο ψηφιακό πιστοποιητικό X.509 για ψηφιακές υπογραφές. Πρόσθετα στοιχεία της ηλεκτρονικής κάρτας είναι το ονοματεπώνυμο του πολίτη, η ημερομηνία και ο τόπος γέννησης, το φύλο, ο αριθμός καταγραφής γέννησης, το ύψος, η ημερομηνία έκδοσης και λήξης της κάρτας, η ιθαγένεια, τα στοιχεία κατοικίας, ο αριθμός φορολογικού μητρώου, η υπογραφή, ο μοναδικός αριθμός αναγνώρισης της κάρτας, η φωτογραφία του κατόχου, το ολόγραμμα ασφαλείας και το πλινθίο [171]. Πέραν της ηλεκτρονικής κάρτας CIE, υφίσταται η προαιρετική κάρτα υπηρεσιών CIS, με την οποία πραγματοποιούνται οι λειτουργίες αυθεντικοποίησης και ψηφιακής υπογραφής.

Κροατία

Η Κροατία είναι το νεότερο μέλος της Ευρωπαϊκής Ένωσης. Με την ένταξή της τροποποιήθηκε η ταυτότητα των πολιτών, ώστε να εναρμονιστεί με το πλαίσιο των ευρωπαϊκών χωρών και να συμπεριληφθεί στα στοιχεία της κάρτας ένα πλινθίο, καθώς και ο προσωπικός αριθμός αναγνώρισης OIB (Osobni identifikacijski broj). Οι Κροάτες πολίτες οφείλουν να κατέχουν μια ηλεκτρονική κάρτα (Osobna iskaznica) με την συμπλήρωση των 16 ετών. Η ηλεκτρονική κάρτα αναγράφει τα στοιχεία που περιλαμβάνει το κλασικό δελτίο ταυτότητας : ονοματεπώνυμο, φύλο, αριθμό ταυτότητας, ιθαγένεια, υπογραφή, ημερομηνία γέννησης, ημερομηνία λήξης ισχύος, διεύθυνση κατοικίας, ημερομηνία έκδοσης και δεδομένα σε μαγνητική ταινία.

Κύπρος

Η κυπριακή ηλεκτρονική κάρτα πρόκειται να αντικαταστήσει την υφιστάμενη πολιτική κάρτα και βρίσκεται σε φάση σχεδιασμού. Σύμφωνα με την έκθεση για την «Ιεράρχηση των στόχων -μέτρων - δράσεων της Ψηφιακής Στρατηγικής Κύπρου» [173], στο Μέτρο 10 που αφορά την Ηλεκτρονική

Ταυτοποίηση και τις Ηλεκτρονικές υπογραφές, η δράση 10.3 περιλαμβάνει την ανάληψη από το Τμήμα Υπηρεσιών Πληροφορικής της Κυπριακής Δημοκρατίας της αρμοδιότητας παροχής υπηρεσιών πιστοποίησης προηγμένων ηλεκτρονικών υπηρεσιών και ενσωμάτωσής τους στην ηλεκτρονική ταυτότητα. Οι ταυτότητες θα περιλαμβάνουν βιομετρικά χαρακτηριστικά και θα εκδίδονται υποχρεωτικά όταν λήξει η ισχύς της πολιτικής ταυτότητας. Ωστόσο, οι Κύπριοι πολίτες μπορούν να εκδώσουν την ηλεκτρονική τους κάρτα πριν τη λήξη της [102,173].

Λετονία

Από τον Απρίλιο του 2012 οι Λετονοί πολίτες έχουν στην διάθεσή τους τις ηλεκτρονικές κάρτες για να μπορούν να αυθεντικοποιούνται ψηφιακά και να υπογράφουν τις ηλεκτρονικές τους συναλλαγές χρησιμοποιώντας ένα ψηφιακό πιστοποιητικό. Το συγκεκριμένο εγχείρημα είναι μέρος του σχεδίου «European eGovernment Action Plan 2011-2015» της ψηφιακής ατζέντας της Ευρώπης [15,106,107]. Οι ηλεκτρονικές κάρτες είναι υποχρεωτικές για τους πολίτες άνω των 18 ετών. Οι κάρτες αναγράφουν το ονοματεπώνυμο του πολίτη, ένα προσωπικό αριθμό, την ημερομηνία γέννησης, την ημερομηνία λήξης της κάρτας, φωτογραφία του κατόχου, το φύλο, το ανάστημα, την ημερομηνία έκδοσης της κάρτας, την αρχή έκδοσης και την υπογραφή του πολίτη. Πρόσθετα περιλαμβάνονται τα βιομετρικά χαρακτηριστικά (δακτυλικά αποτυπώματα και ψηφιακή εικόνα του προσώπου) σεπλινθίο[176].

Λιθουανία

Στην Λιθουανία, οι πολίτες υποχρεωτικά λαμβάνουν την ηλεκτρονική ταυτότητα με την συμπλήρωση των 16 ετών με 10ετή διάρκεια ισχύος. Εφόσον η κάρτα εκδοθεί σε μικρότερη ηλικία, η διάρκεια ισχύος της είναι 5 έτη. Η λιθουανική κάρτα περιλαμβάνει δεδομένα από το δημοτολόγιο, ανέπαφο πλινθίο, καθώς και πλινθίο επαφής με πιστοποιητικό για ταυτοποίηση και πιστοποιητικό για ψηφιακή υπογραφή [179].

Λουξεμβούργο

Στο Λουξεμβούργο, όλοι οι πολίτες ανεξαρτήτως ηλικίας λαμβάνουν υποχρεωτικά ηλεκτρονική ταυτότητα. Η ηλικία του πολίτη καθορίζει και την διάρκεια ισχύος της ηλεκτρονικής ταυτότητας. Στα παιδιά έως την ηλικία των 4 ετών οι κάρτες έχουν διετή διάρκεια, ενώ σε ηλικίες μεταξύ των 4 έως 14 ετών η διάρκεια ισχύος είναι πενταετής. Για ηλικία ανώτερη των 15 ετών η διάρκεια είναι δεκαετής [183]. Στην ηλεκτρονική κάρτα περιλαμβάνεται ο μοναδικός προσωπικός αριθμός κάθε πολίτη. Ο ίδιος αριθμός χρησιμοποιείται και στην κάρτα ασφάλισης [181].

Οι ηλεκτρονικές ταυτότητες βασίζονται στην υποδομή δημοσίου κλειδιού με χρήση πιστοποιητικών που προέρχονται από την LuxTrust, μια συνεργασία δημόσιου-ιδιωτικού τομέα.

Στις 19 Ιουνίου 2013 ψηφίστηκε ο νόμος για την «Αναγνώριση των Φυσικών Προσώπων», όπου στο άρθρο 3 της δεύτερης παραγράφου καθορίζεται ότι η βιομετρική αναγνώριση των φυσικών προσώπων σύμφωνα με τα βιολογικά και μορφολογικά χαρακτηριστικά τους θα μετατρέπεται σε ένα ψηφιακό αποτύπωμα [182]

Μάλτα

Στην Μάλτα, οι ηλεκτρονικές ταυτότητες (*Karta ta' l-Identita*) διαχειρίζονται από το Γραφείο Διαχείρισης Ταυτότητας (Identity Management Office - IDMO). Η ηλεκτρονική κάρτα περιλαμβάνει πλινθίο, δύο ψηφιακά πιστοποιητικά (για ταυτοποίηση και ψηφιακή υπογραφή) και εκδίδεται προαιρετικά από την συμπλήρωση των 14 ετών και υποχρεωτικά με την συμπλήρωση των 18 ετών. Εφόσον ένας πολίτης είναι άνω των 60 ετών τότε πρόσθετα με την ηλεκτρονική ταυτότητα πρέπει να λάβει και μια κάρτα (συνταξιοδότησης [184].

Η κάρτα περιλαμβάνει το ονοματεπώνυμο του πολίτη, μια φωτογραφία, την διεύθυνση κατοικίας την υπογραφή του πολίτη, την υπογραφή της εκδούσας αρχής την ημερομηνία γέννησης τον τόπο γέννησης τις ημερομηνίες έναρξης και λήξης ισχύος της κάρτας ένα σειριακό αριθμό, την εθνικότητα, το φύλο και την μηχανικώς αναγνώσιμη ζώνη.

Ολλανδία

Η ολλανδική ηλεκτρονική κάρτα eNIK (Elektronische Nederlandse Identiteitskaart) ακολουθεί την μορφή των καρτών των υπόλοιπων κρατών. Η κάρτα αναγράφει τα στοιχεία του έντυπου δελτίου ταυτοποίησης και περιλαμβάνει ένα πλινθίο. Στο πλινθίο υπάρχουν αποθηκευμένα τα στοιχεία του πολίτη (όπως αναγράφονται στην ηλεκτρονική κάρτα), καθώς και δύο δακτυλικά αποτυπώματα για τους πολίτες άνω των 12 ετών. Η χρονική ισχύς της κάρτας διαφοροποιείται από την ηλικία του κατόχου. Σε περίπτωση έκδοσης από έναν ανήλικο η κάρτα ισχύει για πέντε έτη, ενώ για ενήλικους πολίτες η διάρκεια ισχύος είναι δεκαετής [186].

Από τα αρχικά των λέξεων «Digita1 iDentity» σχηματίζεται η ονομασία «DigiD», η οποία αναφέρεται στο κύριο διακριτικό των Ολλανδών πολιτών που συνδέεται με την ηλεκτρονική κάρτα [185]. Το DigiD διασυνδέεται με το κεντρικό μητρώο (GBA), ελέγχει το συμπεριλαμβανόμενο χαρακτηριστικό Citizen Service Number και ταυτοποιεί τους πολίτες. Το DigiD διατηρεί τρία επίπεδα ασφαλείας : βασικό, μέσο και υψηλό. Το βασικό επίπεδο περιορίζεται στο συνθηματικό χρήστη και τον κωδικό, ενώ προσθέτοντας

την αποστολή μηνύματος στο κινητό τηλέφωνο το επίπεδο χαρακτηρίζεται μέσο. Το υψηλό επίπεδο περιλαμβάνει βιομετρικά στοιχεία, καθώς και την δυνατότητα ψηφιακής υπογραφής.

Τον Μάρτιο του 2011 το σύστημα DigiD βελτίωσε την ιδιωτικότητα της ηλεκτρονικής κάρτας με το σύστημα DigiD Machtigen. Μια καινοτομία που προστέθηκε ήταν η δυνατότητα εξουσιοδότησης τρίτου προσώπου για την υποβολή της φορολογικής δήλωσης στην αντίστοιχη αρχή (Belastingdienst) [185,187].

Ουγγαρία

Οι Ουγγρικές ηλεκτρονικές ταυτότητες εκδίδονται για πολίτες άνω των 14 ετών και έχουν υποχρεωτικό χαρακτήρα. Η ηλεκτρονική κάρτα αναγράφει το ονοματεπώνυμο του κατόχου, την ημερομηνία γέννησης, την εθνικότητα, το φύλο, την αρχή έκδοσης, την ημερομηνία λήξης ισχύος της ταυτότητας, μα μηχανικώς αναγνώσιμη ζώνη και απεικονίζει τον κάτοχο και την υπογραφή του [59].

Σύμφωνα με την μελέτη «Modinis Study on Identity Management in eGovernment», στην Ουγγαρία παρόλο που δεν υπάρχει κεντρική υποδομή ταυτοτήτων, υπάρχει ένα κοινό πλαίσιο που οροθετεί τις συστάσεις και τους κανονισμούς που άπτονται των ζητημάτων περί ταυτοτήτων. Στο πλαίσιο περιλαμβάνονται μηχανισμοί ταυτοποίησης, αυθεντικοποίησης, προηγμένων ηλεκτρονικών υπογραφών οι οποίοι αλληλεπιδρούν βάσει της κοινής διεπαφής HUNEID [86].

Πολωνία

Στην Πολωνία, οι ηλεκτρονικές ταυτότητες περιλαμβάνουν τα στοιχεία που αναγράφονται στο έντυπο δελτίο ταυτότητας (όνομα, επώνυμο, ημερομηνία και τόπος γέννησης, ονοματεπώνυμο γονέων), την ιθαγένεια, τον αριθμό κάρτας την ημερομηνία έκδοσης και λήξης ισχύος της κάρτας φωτογραφία του πολίτη, τον αριθμό PESEL, πληροφορίες για την υγεία, οικονομικές πληροφορίες, ψηφιακό πιστοποιητικό για ηλεκτρονική υπογραφή και ψηφιακό πιστοποιητικό για ταυτοποίηση. Τα στοιχεία διαμονής, το ύψος και το χρώμα ματιών αποτελούν μια ξεχωριστή ομάδα και η προσπέλαση τους γίνεται κατόπιν πληκτρολόγησης κωδικού PIN. Η ηλεκτρονική κάρτα είναι μια έξυπνη κάρτα με ανέπαφο πλινθίο. Η κάρτα είναι επιτακτική για τους πολίτες που συμπληρώνουν το 18^ο έτος ηλικίας, είτε συμπληρώνουν το 15^ο έτος αλλά εργάζονται [28 55,199].

Πορτογαλία

Κύριος σκοπός της Πορτογαλικής ηλεκτρονικής ταυτότητας ήταν να ενώσει πέντε βασικές διαφορετικές κάρτες σε μια : την ταυτότητα του πολίτη, την φορολογική κάρτα, την κάρτα ασφάλισης, την κάρτα

υπηρεσιών υγείας και την κάρτα ψηφοφορίας. Με την ηλεκτρονική ταυτότητα οι πολίτες θα έχουν πρόσβαση στις υπηρεσίες των υπουργείων Εσωτερικών, Οικονομικών, Υγείας και Δικαιοσύνης.

Γα κάθε πολίτη, η ηλεκτρονική του ταυτότητα περιλαμβάνει: πλινθίο, το φύλο, το ύψος την ιθαγένεια, μα μικρογραφία της ψηφιοποιημένης φωτογραφίας του κατόχου, τον αριθμό εγγράφου και τον αριθμό ταυτότητας, το επώνυμο, το όνομα, την ημερομηνία γέννησης, μα διαθλαστική εικόνα οπτικώς μεταβαλλόμενη (DOVID), τον φορολογικό αριθμό, τον αριθμό έκδοσης της κάρτας το ολόγραμμα του DOVID, τα ονοματεπώνυμα των γονέων, τον αριθμό κοινωνικής ασφάλισης, τον αριθμό υγείας, και μα μηχανικώς αναγνώσιμη ζώνη. Η κάρτα περιλαμβάνει δακτυλικά αποτυπώματα.

Η ηλεκτρονική κάρτα είναι υποχρεωτική μετά την συμπλήρωση των 6 ετών. Η πρώτη πιλοτική εφαρμογή ξεκίνησε το 2007. Μετά από τρία χρόνια εφαρμογής 2.5 εκατομμύρια πολίτες έλαβαν ηλεκτρονικές κάρτες- από την έκδοση ενός πιστοποιητικού γέννησης, μέχρι την αλλαγή διεύθυνσης κατοικίας, το ραντεβού στον παθολόγο και την πληρωμή φόρου [199].

Ρουμανία

Στην Ρουμανία η ηλεκτρονική κάρτα εκδίδεται υποχρεωτικά σε όλους τους πολίτες με την συμπλήρωση του 14^{ου} έτους ηλικίας τους. Η διάρκεια ισχύος εξαρτάται από την ηλικία του πολίτη κατά την έκδοση της ηλεκτρονικής κάρτας και χωρίζεται σε τέσσερις ομάδες:

S Τετραετής διάρκεια, σε πολίτες ηλικίας μεταξύ των 14 έως 17 ετών

S Επταετής διάρκεια, σε πολίτες ηλικίας μεταξύ των 18 έως 25 ετών

S Δεκαετής διάρκεια, σε πολίτες ηλικίας μεταξύ των 25 έως 54 ετών

■ *S* Απεριόριστη διάρκεια, σε πολίτες άνω των 55 ετών

Η ηλεκτρονική κάρτα περιλαμβάνει το ονοματεπώνυμο του πολίτη, την ιθαγένεια, την ημερομηνία γέννησης, την ημερομηνία λήξης ισχύος της κάρτας, τον αριθμό σειράς της κάρτας, τον αριθμό της κάρτας, φωτογραφία του κατόχου, το σύμβολο της Ρουμανίας, ανέπαφο πλίνθο, την ημερομηνία έκδοσης, την διεύθυνση κατοικίας, μα μηχανικώς αναγνώσιμη ζώνη και βιομετρικά δεδομένα (φωτογραφία πολίτη και δακτυλικά αποτυπώματα). Τέλος, συμπεριλαμβάνονται πιστοποιητικά για ηλεκτρονική υπογραφή και πιστοποιητικό αυθεντικοποίησης [06,18,189].

Σλοβακία

Στην Σλοβακία, η κατοχή ηλεκτρονικής ταυτότητας είναι υποχρεωτική για όλους τους πολίτες με την συμπλήρωση των 15 ετών [59]. Η ηλεκτρονική κάρτα της Datacard ακολουθεί το πρότυπο EAC και διατηρεί βιομετρικά δεδομένα, υποστηρίζει την υποδομή δημοσίου κλειδιού και περιλαμβάνει πιστοποιητικά ταυτοποίησης και ψηφιακής υπογραφής για την εύκολη και τάχιστα αυθεντικοποίηση των πολιτών [52].

Η ηλεκτρονική κάρτα περιλαμβάνει το ονοματεπώνυμο του πολίτη, το φύλο, τη διεύθυνση, την ημερομηνία γέννησης, ημερομηνία λήξης κάρτας, ανεπαφικό πλίνθο, καθώς και στοιχεία σχετικά με την ομάδα αίματος και την εκπαίδευση. Τα στοιχεία είναι αναγνώσιμα μόνο με τη συγκατάθεση των πολιτών και την πληκτρολόγηση του προσωπικού κωδικού ασφαλείας (από 6 έως 10 ψηφία) στον αναγνώστη καρτών [190].

Τον Δεκέμβριο του 2013 ανακοινώθηκε μια νέα eID κάρτα. Η νέα κάρτα θα μπορεί να χρησιμοποιηθεί και ως ασφαλής διάταξη δημιουργίας υπογραφής (Secure Signature Creation Device - SSCD), ώστε να αποθηκεύονται πιστοποιητικά και να δημιουργούνται πιστοποιημένες ηλεκτρονικές υπογραφές (Qualified Electronic Signature - QES).

Η ηλεκτρονική υπογραφή έχει ιδιαίτερη σημασία στον τομέα της τραπεζικής. Παρόλο που υπάρχει μηχανισμός, δυστυχώς οι Σλοβάκοι δεν αξιοποιούν την ηλεκτρονική υπογραφή. Σε αυτό συμβάλει και ο χαμηλός αριθμός των ψηφιακών υπηρεσιών που προσφέρονται από την κυβέρνηση της Σλοβακίας [200]. Η Σλοβακία πρέπει να αναπτύξει περισσότερες ψηφιακές υπηρεσίες, καθώς και προωθήσει την χρησιμότητα της ηλεκτρονικής ταυτότητας ώστε οι πολίτες να την αντιμετωπίζουν ως περιουσιακό αγαθό.

Σλοβενία

Στην Σλοβενία υπάρχει το Κεντρικό Μητρώο Πολιτών, όπου εγγράφονται όλοι οι πολίτες (συμπεριλαμβανομένων και των αλλοδαπών) και αναγνωρίζονται μοναδικά βάσει του προσωπικού αριθμού EMSO. Για την έκδοση της ηλεκτρονικής κάρτας οι πολίτες καταθέτουν το προσωπικό αριθμό τους στην Αρχή Πιστοποίησης SIGEN-CA και η Αρχή πιστοποιεί τον προσωπικό αριθμό προσθέτοντάς τον στο πιστοποιητικό του πολίτη.

Η Σλοβενία αποτελεί πρωτοπόρο στο θέμα των ηλεκτρονικών ταυτοτήτων. Η ηλεκτρονική κάρτα δεν είναι υποχρεωτική και περιλαμβάνει τα στοιχεία της κλασικής ταυτότητας (όνομα, επώνυμο, ημερομηνία γέννησης, ημερομηνία έκδοσης, υπογραφή, φωτογραφία, μοναδικό αριθμό αναγνώρισης), ένα

πιστοποιητικό (ζεύγος κλειδιού) για αυθεντικοποίηση και ένα πιστοποιητικό για υπογραφή και βιομετρικά δεδομένα. Το ψηφιακό πιστοποιητικό που είναι αποθηκευμένο στην έξυπνη κάρτα ισχύει για 5 χρόνια [94].

Σουηδία

Στην Σουηδία η ηλεκτρονική κάρτα (NIDEL) δεν είναι υποχρεωτική, έχει διάρκεια ισχύος 5 έτη από την ημερομηνία έκδοσής της και διατίθεται σε όλους τους πολίτες. Μάλιστα η εξοικείωση των πολιτών μέσω της υποδομής BankID (η κάρτα BankID υποστηρίζεται από πλήθος τραπεζών και ακολουθεί διαδικασία ταυτοποίησης) συνέβαλε θετικά στην χρήση των ηλεκτρονικών ταυτοτήτων [22].

Η ηλεκτρονική κάρτα περιλαμβάνει τον μοναδικό αριθμό πολίτη που προέρχεται από το Εθνικό Μητρώο. Στο μπροστινό τμήμα της υπάρχει ένα ανεπαφικό πλίνθο με την ψηφιακή αναπαράσταση των δεδομένων της έντυπης κάρτας ταυτοποίησης. Πα κάθε πολίτη αναγράφεται το ονοματεπώνυμό του, ο προσωπικός αριθμός του, η υπογραφή, το ύψος, η ημερομηνία γέννησης, η αρχή έκδοσης, η ημερομηνία έκδοσης και η ημερομηνία λήξης ισχύος της κάρτας και μια μηχανικώς αναγνώσιμη ζώνη. Το ανεπαφικό πλίνθο περιλαμβάνει την ψηφιακή απεικόνιση του πολίτη και ένα κλειδί εγκυρότητας των στοιχείων της κάρτας [192,193].

Η σουηδική πραγματικότητα είναι πολύπλοκη σε σχέση με τα υπόλοιπα Ευρωπαϊκά κράτη. Υπάρχουν πολλές διαφορετικές προσεγγίσεις τομεακών υπηρεσιών από ιδιωτικούς φορείς που παρέχουν και τις αντίστοιχες ηλεκτρονικές κάρτες και απουσιάζει ένα συγκεντρωτικό σύστημα eIDM. Παρά τα διαφορετικά συστήματα, η Σουηδική κοινωνία χρησιμοποιεί επαρκώς τις ηλεκτρονικές υπηρεσίες σε σύγκριση με τις υπόλοιπες Ευρωπαϊκές χώρες [194].

Τσεχία

Η πλειοψηφία των κρατών διατηρούν μοναδικούς αριθμούς ταυτοποίησης σε κεντρικά ή περιφερειακά μητρώα. Από την 1^η Ιανουαρίου 2012 και η Τσεχία εξέδωσε ηλεκτρονικές ταυτότητες. Η ηλεκτρονική ταυτότητα έχει υποχρεωτικό χαρακτήρα για τους πολίτες άνω των 15 ετών και περιλαμβάνει τον μοναδικό αριθμό ταυτοποίησης του πολίτη που δίδεται κατά την γέννησή του. Οι πολίτες κάτω των 15 ετών αιτούνται εθελοντικά τις ηλεκτρονικές κάρτες και σε αυτή την περίπτωση η διάρκεια ισχύος της εκδιδόμενης κάρτας είναι πενταετής, ενώ σε πολίτες μεγαλύτερης ηλικίας η διάρκεια ισχύος καθορίζεται στα δέκα έτη [59].

Η ηλεκτρονική κάρτα υποστηρίζει μια πολυεπίπεδη αρχιτεκτονική, ενώ ενσωματώνεται η αρχιτεκτονική IAS ECC περιλαμβάνοντας πιστοποιητικά ταυτοποίησης και ψηφιακής υπογραφής για την αυθεντικοποίηση των πολιτών [195].

Η ηλεκτρονική κάρτα περιλαμβάνει το ονοματεπώνυμο του πολίτη, την ημερομηνία γέννησης, το φύλο, τον τόπο γέννησης, την ιθαγένεια, την ημερομηνία έκδοσης και την ημερομηνία λήξης, φωτογραφία του πολίτη, ακαδημαϊκό πτυχίο (αν ζητηθεί), οικογενειακή κατάσταση και την υπογραφή του. Επίσης, η κάρτα αναγράφει την διεύθυνση, τον προσωπικό αριθμό του πολίτη, την αρχή έκδοσης, ανεπαφικό πλίνθο και μια μηχανικώς αναγνώσιμη ζώνη. Τα στοιχεία είναι αναγνώσιμα μόνο με τη συγκατάθεση των πολιτών και την πληκτρολόγηση του προσωπικού κωδικού ασφαλείας (από 4 έως 10 ψηφία) στον αναγνώστη καρτών [195].

Φινλανδία

Οι ηλεκτρονικές ταυτότητες (FINEID) στην Φινλανδία είναι προαιρετικές, ισχύουν για πέντε έτη και είναι διαθέσιμες σε πολίτες άνω των 18 ετών. Η ταυτότητα συνδέεται με τον προσωπικό κωδικό του Μητρώου Καταγραφής Πληθυσμού, το οποίο αποτελεί την επίσημη Αρχή Πιστοποίησης της Φινλανδίας. Ο προσωπικός κωδικός διατηρείται στο πιστοποιητικό ταυτοποίησης του πολίτη. Εκτός από το συγκεκριμένο πιστοποιητικό, η ταυτότητα διαθέτει πιστοποιητικό για ψηφιακή υπογραφή. Και τα δύο πιστοποιητικά, συμπεριλαμβανομένων και βιομετρικών στοιχείων εμπεριέχονται σε ένα πλίνθο.

Η κάρτα αναγράφει το ονοματεπώνυμο του πολίτη, το φύλο, την ιθαγένεια και φωτογραφία του πολίτη, καθώς και ημερομηνίες γέννησης, έκδοσης και λήξης ισχύος της κάρτας. Στην δεύτερη όψη της κάρτας περιλαμβάνεται η αρχή έκδοσης της κάρτας και μια μηχανικώς αναγνώσιμη ζώνη.

Δυστυχώς η φινλανδική ηλεκτρονική ταυτότητα δεν είναι ιδιαίτερα δημοφιλής, γιατί οι Φινλανδοί πολίτες έχουν εξοικειωθεί περισσότερο από το πρότυπο TUPAS (με κωδικούς μιας χρήσης) που ακολουθείται στις τραπεζικές ψηφιακές υπηρεσίες.

Συγκεντρωτικά

Ο πίνακας 2.3 περιλαμβάνει ανά κράτος τα ηλεκτρονικά μέσα με τα οποία πραγματοποιείται η ταυτοποίηση των πολιτών στα κράτη μέλη της Ευρωπαϊκής Ένωσης. Στις στήλες του πίνακα περιλαμβάνεται η ονομασία του μέσου ταυτοποίησης, η αναφορά εάν το μέσο έχει υποχρεωτικό χαρακτήρα (ή όχι) και τα κύρια χαρακτηριστικά του μέσου ταυτοποίησης. Τα κράτη διατάσσονται στις

γραμμές του πίνακα σε αλφαβητική σειρά. Τα εθνικά δελτία ταυτότητας που συμπεριλαμβάνουν την πληροφορία της ιθαγένειας των πολιτών αποτελούν και επίσημα ταξιδιωτικά έγγραφα βάσει του ICAO.

Κράτος Μέλος	Χαρακτηριστικά Ηλεκτρονικών Μέσων Ταυτοποίησης	
	Ονομασία / Επιβολή μέσου	Χαρακτηριστικά
Αυστρία	Εθνική Ταυτότητα (Κάρτα Πολίτη) (Osterreichischer Personalausweis) Προαιρετική κτήση	<p>■ S Προσφέρει πρόσβαση σε υπηρεσίες Ηλεκτρονικής Διακυβέρνησης [27,28,149].</p> <p>■ S Υποστηρίζει το μηχανισμό μοναδικών αναγνωριστικών (Source PIN).</p> <p>■ S Εμπεριέχει ψηφιακό πιστοποιητικό.</p> <p>S Αποθηκεύει την ελάχιστη πληροφορία.</p> <p>S Παρέχει ισχυρή κρυπτογράφηση σε φυσικά πρόσωπα με χρήση του προτύπου MOA (Module for Online Applications) για αναγνώριση, υπογραφή εξυπηρετητών, πιστοποίηση υπογραφής, ηλεκτρονική παράδοση.</p>
Βέλγιο	eID, KIDS-ID, foreigners card Υποχρεωτική κτήση	<p>S Περιλαμβάνει ενσωματωμένο ηλεκτρονικό πλίνθο με δύο ψηφιακά πιστοποιητικά: ένα για συναλλαγές και ένα για υπογραφή.</p> <p>■ S Για τις κάρτες των παιδιών δεν υποστηρίζεται το ψηφιακό πιστοποιητικό για ψηφιακή υπογραφή.</p>
Βουλγαρία	Ηλεκτρονική κάρτα Προαιρετική κτήση	<p>S Περιλαμβάνει προστατευόμενο κωδικό PIN και συνθηματικό σε μια έξυπνη κάρτα,</p> <p>S Ψηφιακό πιστοποιητικό και ηλεκτρονική υπογραφή.</p>
Γαλλία	Ασφαλής	<p>■ S Ενσωματώνει δύο βιομετρικά στοιχεία του πολίτη και</p>
	Ηλεκτρονική ταυτότητα (INES) Προαιρετική κτήση	<p>την ψηφιακή αντιγραφή των δεδομένων της φυσικής κάρτας σε πλίνθο τεχνολογίας RFID με κρυπτογράφηση κλειδιού 2048 bits</p> <p>S Ενσωματώνει ψηφιακό πιστοποιητικό</p> <p>S Η παρακολούθηση χρήσης δεδομένων πραγματοποιείται από την επιτροπή CNIL (Commission nationale de l'informatique et des liberies)</p>
Γερμανία	Εθνική κάρτα ταυτοποίησης Υποχρεωτική	<p>S Περιλαμβάνει ανέπαφο πλίνθο</p> <p>S Βιομετρικά στοιχεία (δακτυλικά αποτυπώματα)</p> <p>S Ψηφιακό πιστοποιητικό για αυθεντικοποίηση (PACE)</p>
Δανία	Ηλεκτρονική Κάρτα (NemID)	<p>S Είναι μια ενιαία κάρτα (single sign on) για την Ηλεκτρονική διακυβέρνηση, πλήθος ηλεκτρονικών υπηρεσιών και την</p>

	Προαιρετική	υπογραφή ηλεκτρονικών συναλλαγών. S Προσφέρει έλεγχο ταυτότητας σε δύο επίπεδα.
Ελλάδα	Κάρτα Πολίτη Πιθανότατα Υποχρεωτική	S Θα περιλαμβάνει ενσωματωμένο ηλεκτρονικό πλίνθο με δύο ψηφιακά πιστοποιητικά: ένα για συναλλαγές και ένα για υπογραφή.
Εσθονία	Εθνική Ταυτότητα Υποχρεωτική	S Περιλαμβάνει πιστοποιητικό για την αναγνώριση και την ψηφιακή υπογραφή S Χρησιμοποιεί κρυπτογράφηση δημοσίου κλειδιού 2048-bit
Ηνωμένο Βασίλειο	-Εθνική Κάρτα Ταυτοποίησης	Ακυρώθηκε τον Ιανουάριο του 2010, βάσει του «Identity Documents Act 2010»
Ιρλανδία	Κάρτα Δημόσιων Υπηρεσιών Υποχρεωτική	■S Περιλαμβάνει πλίνθο, πιστοποιητικά για ταυτοποίηση και ψηφιακή υπογραφή, βιομετρικά δεδομένα και τον προσωπικό αριθμό δημόσιας υγείας (PPS No)
Ισπανία	Ηλεκτρονική κάρτα (DNI-e) Υποχρεωτική	■S Περιλαμβάνει πλίνθο, πιστοποιητικό αυθεντικοποίησης X509v3, ψηφιακή υπογραφή και βιομετρικά δεδομένα. S Υποστηρίζει υποδομή δημοσίου κλειδιού (RSA)
Ιταλία	1. Ηλεκτρονική κάρτα CIE Προαιρετική 2. Κάρτα Υπηρεσιών CNS Προαιρετική	1. i) Περιλαμβάνει πλίνθο με πιστοποιητικό X.509 για ψηφιακή υπογραφή. ίΠΠροαιρετική παρουσία βιομετρικών δεδομένων 2. Πα αυθεντικοποίηση και ψηφιακή υπογραφή
Κροατία	Ηλεκτρονική κάρτα Osobna iskaznica Υποχρεωτική	■S Περιλαμβάνει πλίνθο και τον προσωπικό αριθμό αναγνώρισης OIB (Osobni identifikacijski broj)
Κύπρος	Κυπριακή ταυτότητα Υποχρεωτική	S Περιλαμβάνει πλίνθο με βιομετρικά δεδομένα και ψηφιακό πιστοποιητικό για ταυτοποίηση. S Δυνατότητα ψηφιακής υπογραφής
Λετονία	Ηλεκτρονική κάρτα Υποχρεωτική	S Περιλαμβάνει πλίνθο με βιομετρικά δεδομένα και ψηφιακό πιστοποιητικό για ταυτοποίηση. S Δυνατότητα ψηφιακής υπογραφής
Λιθουανία	Προσωπική ταυτότητα (ID card) Υποχρεωτική	S Δεδομένα από το δημοτολόγιο S Βιομετρικά

		<p>δεδομένα S Ανέπαφο πλίνθο</p> <p>S Πλινθίο επαφής με πιστοποιητικό για ταυτοποίηση και πιστοποιητικό για ψηφιακή υπογραφή</p>
Λουξεμβούργο	<p>Ηλεκτρονική ταυτότητα</p> <p>Υποχρεωτική</p>	<p>S Βιομετρικά δεδομένα</p> <p>S Πλινθίο με πιστοποιητικό για ταυτοποίηση και πιστοποιητικό για ψηφιακή υπογραφή</p>
Μάλτα	<p>Ηλεκτρονική ταυτότητα</p> <p>Υποχρεωτική</p>	<p>S Πλινθίο με πληκτρολόγηση PIN</p> <p>S Πιστοποιητικό για ταυτοποίηση</p> <p>S Πιστοποιητικό για ψηφιακή υπογραφή</p>
Ολλανδία	<p>Ηλεκτρονική κάρτα eNIK Προαιρετική</p>	<p>S Περιλαμβάνει πλίνθο με βιομετρικά δεδομένα.</p> <p>S Δυνατότητα ψηφιακής υπογραφής</p> <p>S Ταυτοποίηση μέσω κινητής τηλεφωνίας</p>
Ουγγαρία	<p>Ηλεκτρονική ταυτότητα</p> <p>Υποχρεωτική</p>	<p>Μηχανισμοί ταυτοποίησης, αυθεντικοποίησης, προηγμένων ηλεκτρονικών υπογραφών υπό την διεπαφή HUNEID</p>
Πολωνία	<p>Ηλεκτρονική ταυτότητα (pl.ID)</p> <p>Υποχρεωτική</p>	<p>S Μοναδικός αριθμός PESEL</p> <p>S Ευαίσθητα δεδομένα με ελεγχόμενη πρόσβαση</p> <p>S Ανέπαφο πλίνθο</p>
		<p>■ S Πιστοποιητικά για ταυτοποίηση και πιστοποιητικό για ψηφιακή υπογραφή</p>
Πορτογαλία	<p>Κάρτα Πολίτη</p> <p>Υποχρεωτική</p>	<p>■ S Περιλαμβάνει πιστοποιητικά για την αναγνώριση και την ψηφιακή υπογραφή</p> <p>■ S Βιομετρικά στοιχεία (δακτυλικά αποτυπώματα)</p>
Ρουμανία	<p>Ηλεκτρονική κάρτα</p> <p>Υποχρεωτική</p>	<p>■ S Ανέπαφο πλίνθο</p> <p>■ S Περιλαμβάνει πιστοποιητικά για αυθεντικοποίηση και ψηφιακή υπογραφή</p> <p>■ S Βιομετρικά στοιχεία (δακτυλικά αποτυπώματα και</p>

		φωτογραφία κατόχου)
Σλοβακία	Ηλεκτρονική κάρτα Υποχρεωτική	■S Ανέπαφο πλίνθο ■S Περιλαμβάνει πιστοποιητικά για αυθεντικοποίηση και ψηφιακή υπογραφή
Σλοβενία	Ηλεκτρονική κάρτα Προαιρετική	S πιστοποιητικό (ζεύγος κλειδιού) για αυθεντικοποίηση ■S πιστοποιητικό για υπογραφή S βιομετρικά δεδομένα
Σουηδία	Ηλεκτρονική κάρτα NIDEL Προαιρετική	S βιομετρικά δεδομένα S προσωπικός αριθμός μητρώου

Φινλανδία	Ηλεκτρονική κάρτα FINEID Προαιρετική	S πιστοποιητικό για αυθεντικοποίηση S πιστοποιητικό για υπογραφή S βιομετρικά δεδομένα
-----------	--------------------------------------------	----------------------------------------------------------------------------------------------

Πίνακας 2.3: Τεχνικά χαρακτηριστικά ηλεκτρονικών καρτών - ταυτοτήτων [59,103]

Τσεχία	Ηλεκτρονική κάρτα Υποχρεωτική	S βιομετρικά δεδομένα S προσωπικός αριθμός μητρώου
--------	-------------------------------------	-------------------------------------------------------

Όπως προκύπτει από τον πίνακα 2.3, αλλά και από τα στοιχεία που δόθηκαν για κάθε ευρωπαϊκό κράτος, 24 από τα 28 κράτη μέλη της Ευρωπαϊκής Ένωσης υποχρεώνουν τους πολίτες να ταυτοποιούνται σε ένα ηλεκτρονικό σύστημα ταυτοποίησης και να υπογράφουν ψηφιακά τις συναλλαγές τους. Στις περισσότερες περιπτώσεις αναγράφονται τα μοναδικά αναγνωριστικά των πολιτών στις ηλεκτρονικές κάρτες και υποστηρίζεται κρυπτογραφημένη μετάδοση των δεδομένων.

2.2.2 Μοναδικά Αναγνωριστικά

Στην ενότητα 2.2.1 αναφέρθηκαν οι συνιστώσες μας ηλεκτρονικής κάρτας. Στις περισσότερες χώρες οι κάρτες αναφέρουν μοναδικά αναγνωριστικά που αποδίδονται στους πολίτες και προέρχονται από την καταγραφή των πολιτών σε κάποιο επίσημο μητρώο της χώρας. Επειδή τα μοναδικά αναγνωριστικά χαρακτηρίζουν μονοσήμαντα έναν πολίτη θεωρούνται ευαίσθητα προσωπικά δεδομένα.

Σε κάθε κράτος μπορεί να υπάρχουν διάφορα μοναδικά αναγνωριστικά, υπό την έννοια ότι μπορεί να υπάρχουν μοναδικοί αριθμοί που είναι αποδεκτοί από το σύνολο των ψηφιακών υπηρεσιών που παρέχονται στους πολίτες, καθώς και να υπάρχουν μοναδικά αναγνωριστικά ανά παρεχόμενη υπηρεσία. Για τον λόγο αυτό δεν είναι παράδοξο για ένα κράτος να διατηρεί περισσότερα του ενός μοναδικά αναγνωριστικά. Για παράδειγμα στην Ελλάδα υπάρχει ο Αριθμός Φορολογικού Μητρώου (ΑΦΜ), ο Αριθμός Αστυνομικού Δελτίου Ταυτότητας (ΑΔΤ) και ο Αριθμός Μητρώου Κοινωνικής Ασφάλισης (ΑΜΚΑ). Και οι τρεις αριθμοί χαρακτηρίζουν μοναδικά έναν πολίτη. Οι ΑΦΜ και ΑΜΚΑ αξιοποιούνται απολύτως ισοδύναμα σε επιμέρους διαλειτουργούντα περιβάλλοντα στη δημόσια διοίκηση (π.χ. σε όλες τις βάσεις δεδομένων, ανά πολίτη, φαίνεται ότι σταδιακά θα περιλαμβάνονται δύο πεδία και ΑΦΜ και ΑΜΚΑ).

Στην ενότητα αυτή, παρουσιάζονται σε μορφή πίνακα τα μοναδικά αναγνωριστικά των πολιτών ανά κράτος.

Κράτος Μέλος	Μοναδικά Αναγνωριστικά Πολιτών		
	Κωδικοποίηση	Ονομασία	Χαρακτηριστικά
Αυστρία	28 bytes base64	ssPIN(BW)	Ο προσωπικός αριθμός CCR Id κρυπτογραφείται και παράγεται ο SourcePin. Το SourcePin κωδικοποιείται με βάση την επιθυμητή υπηρεσία BW και παράγεται το ssPIN(BW).
Βέλγιο	11 ψηφία	National Number	Τα έξι πρώτα ψηφία αναφέρονται στην ημερομηνία γέννησης του πολίτη, τα επόμενα τρία στο φύλο και τα δύο τελευταία χρησιμοποιούνται για την εγκυρότητα του αριθμού. Ο περιττός αριθμός αναφέρεται σε άνδρα, ειδάλλως σε γυναίκα.
Βουλγαρία	10 ψηφία	E,O,HHΘH gra>KflaHCKH HOMθp	Τα έξι πρώτα ψηφία αναφέρονται στην ημερομηνία γέννησης του πολίτη, τα επόμενα τρία στην περιοχή γέννησης, την

			σειράγέννησης και το φύλο. Το τελευταίο ψηφίο αποτελεί ψηφίο ελέγχου εγκυρότητας της ταυτότητας [142].
Γαλλία	15 ψηφία	INSEE	syymmllloookkk cc, όπου το s αναφέρεται στο φύλο (1 : άνδρας, 2 : γυναίκα), τα yymm σηματοδοτούν το χρόνο και το μήνα γέννησης, το 11 είναι ο αριθμός διαμερίσματος προέλευσης, το
			ooo είναι ο αριθμός κοινότητας του διαμερίσματος, το kkk είναι ο αύξον αριθμός (για άτομα που γεννήθηκαν την ίδια ημέρα), τα cc είναι χαρακτήρες εγκυρότητας.
Δανία	10 ψηφία	Det Centrale Personregister	Τα έξι πρώτα ψηφία αναφέρονται στην ημερομηνία γέννησης του πολίτη και τα επόμενα τέσσερα είναι ένας σειριακός αριθμός.
Ελλάδα	7-8 ψηφία 9 ψηφία 11 ψηφία	ΑΔΤ ΑΦΜ ΑΜΚΑ	ΑΔΤ: 2 χαρακτήρες και 6 ψηφία ΑΦΜ : 8 ψηφία συν 1 ψηφίο ελέγχου ΑΜΚΑ: 6 ψηφία για την ημερομηνία γέννησης, 5 ψηφία αύξοντα αριθμού
Εσθονία	11 ψηφία	isikukood	GYMMDDSSSC, όπου το G αναφέρεται στο φύλο και τον αιώνα γέννησης, τα YMMDD υποδηλώνουν την ημερομηνία γέννησης, SSS είναι ένας σειριακός αριθμός και το C είναι ψηφίο ελέγχου.
Ηνωμένο Βασίλειο	10 ψηφία	National Health Service number	NNN-NNN-NNNN, όπου το τελευταίο ψηφίο είναι ψηφίο ελέγχου
Ιρλανδία	9 ψηφία	Personal Public Service Number (PPS No)	1234567TA, όπου τα 7 ψηφία είναι τυχαία, το όγδοο είναι ένας χαρακτήρας ελέγχου και το ένατο είναι ένας χαρακτήρας βάρους του 9.
Ισπανία	10 ψηφία	Documento Nacional de Identidad(DNI)	00000000-A, όπου τα 8 πρώτα είναι ψηφία και ο τελευταίος χαρακτήρας είναι χαρακτήρας ελέγχου
Ιταλία	16 ψηφία	Codice fiscale	SSSNNNYMDDZZZZX, όπου SSS είναι τα τρία πρώτα σύμφωνα της οικογένειας, NNN

			το πρώτο, τρίτο και τέταρτο σύμφωνα του ονόματος, ΥΥ τα 2 τελευταία ψηφία του έτους γέννησης, Μ το γράμμα του μήνα γέννησης, DD η ημέρα γέννησης, ZZZZ ο κωδικός του δήμου γέννησης, X ένα ψηφίο ισοτιμίας
Κροατία	11 ψηφία	Osobni identifikacijski broj	10 τυχαία ψηφία και το τελευταίο αποτελεί ψηφίο ελέγχου
Λετονία	11 ψηφία	Personas kods	DDMMYY-XNNNC, όπου τα πρώτα 6 ψηφία αφορούν την ημερομηνία γέννησης, το X στον αιώνα γέννησης, το NNN στον σειριακό αριθμό γέννησης και το C αποτελεί ψηφίο ελέγχου
Λιθουανία	11 ψηφία	Asmens kodas	GYMMDDNNNC, όπου το G υποδηλώνει το φύλο και τον αιώνα γέννησης, τα YMMDD την ημερομηνία γέννησης, NNN τον σειριακό αριθμό γέννησης και το C αποτελεί ψηφίο ελέγχου
Ολλανδία	8 ή 9 ψηφία	Burgerservicenummer (BSN)	8 ή 9 τυχαία ψηφία
Ουγγαρία	11 ψηφία	Szemelyi azonosító szám	GYMMDDXXXC, όπου το G υποδεικνύει το φύλο, το YMMDD στην ημερομηνία γέννησης, το XXX σε ένα σειριακό αριθμό και το C σε ένα χαρακτήρα ελέγχου
Πολωνία	11 ψηφία	Powszechny Elektroniczny System Ewidencji Ludności (PESEL)	YMMDDZZZXQ όπου YMMDD η ημερομηνία γέννησης, ZZZ ο αύξων αριθμός γέννησης και το C αποτελεί χαρακτήρα ελέγχου
Ρουμανία		Cod Numeric Personal CNP	GYMMDDCCNNNC, όπου το G υποδηλώνει το φύλο και τον αιώνα γέννησης, τα DDMMYY αφορούν την ημερομηνία

			γέννησης, τα CC ο κωδικός χώρας, το NNN στον σειριακό αριθμό γέννησης και το C αποτελεί ψηφίο ελέγχου
Σλοβακία	10 ψηφία	rodne Cislo (RC)	YYXXDD/SSSC, όπου τα έξι πρώτα ψηφία αναφέρονται στο έτος, μήνα, ημέρα γέννησης, τα ψηφία SSS αναφέρονται στο αύξον αριθμό και το ψηφίο C αποτελεί χαρακτήρα ελέγχου
Σλοβενία	13 ψηφία	Enotna maticna stevilka obcana (EMSO)	DDMMYYRRSSSX, όπου τα έξι πρώτα ψηφία αναφέρονται στο έτος, μήνα, ημέρα γέννησης, τα ψηφία RR αναφέρονται στη ζώνη γέννησης, το SSS αναφέρονται στο αύξον αριθμό γέννησης και το ψηφίο C αποτελεί χαρακτήρα ελέγχου
Σουηδία	10 ψηφία	personnummer	YYMMDD-NNGC, όπου τα έξι πρώτα ψηφία αναφέρονται στο έτος, μήνα, ημέρα γέννησης, τα ψηφία NNG αναφέρονται στο αύξον αριθμό και το

			ψηφίο C αναφέρεται στο φύλο
Τσεχία	10 ψηφία	rodne Cislo (RC)	YYXXDD/SSSC, όπου τα έξι πρώτα ψηφία αναφέρονται στο έτος, μήνα, ημέρα γέννησης, τα ψηφία SSS αναφέρονται στο αύξον αριθμό και το ψηφίο C αποτελεί χαρακτήρα ελέγχου
Φινλανδία	11 ψηφία	Henkilotunnus	DDMMYYCZZZQ όπου τα έξι πρώτα ψηφία αναφέρονται στο έτος, μήνα, ημέρα γέννησης, το ψηφίο C σηματοδοτεί τον αιώνα (+,-,A), τα περιττά ψηφία ZZZ αναφέρονται στον αύξοντα αριθμό ανδρών, ενώ τα άρτια ψηφία ZZZ αναφέρονται στον αύξον αριθμό γυναικών (επιτρεπτές τιμές: 002-899) και το ψηφίο C αποτελεί χαρακτήρα ελέγχου

Πίνακας 2.4: Μοναδικά αναγνωριστικά πολιτών στην Ευρωπαϊκή Ένωση [39]

Όπως προκύπτει από τον παραπάνω πίνακα 23 από τα 28 κράτη μέλη διατηρούν μοναδικά αναγνωριστικά ταυτοποίησης. Σε 18 από τα 28 κράτη το αναγνωριστικό ταυτοποίησης έχει ως τμήμα του την ημερομηνία γέννησης και ένα ψηφίο ελέγχου, σε 16 κράτη αναφέρεται ο αύξον αριθμός αρίθμησης των πολιτών που γεννήθηκαν την ίδια ημέρα, σε 9 κράτη αναφέρεται το φύλο. Σε 5 κράτη το μοναδικό αναγνωριστικό είναι ψευδοτυχαίο.

Στις περισσότερες περιπτώσεις το μήκος του αναγνωριστικού είναι 10ψηφιο και 11ψηφιο. Μια γενική παρατήρηση είναι ότι στο μοναδικό αναγνωριστικό κρύβονται προσωπικές πληροφορίες του πολίτη (ημερομηνία γέννησης και φύλο). Όπως αναφέρθηκε στην προηγούμενη παράγραφο, οι προσωπικοί κωδικοί περιλαμβάνονται στις ηλεκτρονικές ταυτότητες. Συνεπώς, μελετώντας τα στοιχεία των μοναδικών αναγνωριστικών απορρέει το συμπέρασμα ότι κάποιες πληροφορίες που είναι προφανείς στις ηλεκτρονικές κάρτες εμπεριέχονται στα μοναδικά χαρακτηριστικά ενδεχομένως να μην απαιτείται να αναγράφονται εκ νέου στις ηλεκτρονικές ταυτότητες.

Κεφάλαιο 3

Ευρωπαϊκές Οδηγίες

Στο δεύτερο κεφάλαιο της μελέτης παρουσιάστηκαν αναλυτικά τα στοιχεία που περιλαμβάνονται στα φυσικά και ηλεκτρονικά μέσα ταυτοποίησης. Ορισμένες από τις πληροφορίες που περιλαμβάνονται στο σύνολο των μέσων ενέχουν ιδιαίτερη σημασία, δεν πρέπει να είναι προσπελάσιμες από τον οποιονδήποτε και είναι γνωστές ως «ευαίσθητα προσωπικά δεδομένα». Συνεπώς η διαχείριση των δεδομένων ταυτοποίησης των πολιτών παραπέμπει στην ανάγκη της ενίσχυσης της ασφάλειας των πληροφοριών με τεχνικά και νομικά μέσα.

Στο παρόν κεφάλαιο παρατίθεται το νομικό πλαίσιο της Ευρωπαϊκής Ένωσης (οδηγίες) για την προστασία των προσωπικών δεδομένων, την διατήρηση δεδομένων, την προστασία των δικαιωμάτων και την παροχή υπηρεσιών. Αναφορικά με την προστασία των προσωπικών δεδομένων αναλύονται οι ψηφιακές υπογραφές, τα ψηφιακά πιστοποιητικά και οι προηγμένες ηλεκτρονικές υπογραφές. Οι οδηγίες παρατίθενται ανά ημερομηνία έκδοσης.

3.1 Προστασία προσωπικών δεδομένων (95/46/EK)

Η οδηγία 95/46/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 αφορά την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία των δεδομένων αυτών. Η οδηγία αυτή είναι άρρηκτα συνδεδεμένη με το ζήτημα διαχείρισης των ηλεκτρονικών ταυτοτήτων.

Στον ορισμό των «δεδομένων προσωπικού χαρακτήρα» του άρθρου 2 της οδηγίας αναφέρεται: *«κάθε πληροφορία που αναφέρεται σε φυσικό πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί»* και στην ίδια παράγραφο προστίθεται : *«ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσοτέρων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόσταση του από φυσική, βιολογική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική άποψη»*. Συσχετίζοντας τα μοναδικά αναγνωριστικά, καθώς και τα στοιχεία που αναγράφονται και περιλαμβάνονται στις ηλεκτρονικές ταυτότητες, η οδηγία αυτή θεωρείται η πρώτη οδηγία που πρέπει να λαμβάνεται υπόψη στο ζήτημα των ηλεκτρονικών ταυτοτήτων.

Το πρώτο σημαντικό ζήτημα που θέτει η Οδηγία είναι η *«επεξεργασία δεδομένων προσωπικού χαρακτήρα»*. Αντιπαραβάλλοντας την ανάλυση των μέσων ταυτοποίησης, διαπιστώνεται ότι τα δεδομένα προσωπικού χαρακτήρα είναι καταγεγραμμένα είτε στο κλασικό δελτίο ταυτοποίησης, είτε στην ηλεκτρονική ταυτότητα. Ωστόσο, με την παρουσία του πλινθίου στην ηλεκτρονική ταυτότητα πλέον δίνεται η δυνατότητα επεξεργασίας των προσωπικών δεδομένων, αφού τα δεδομένα είναι καταγεγραμμένα σε ένα ηλεκτρονικό μέσο. Στο σημείο αυτό πρέπει να δοθεί έμφαση στον *«υπεύθυνο της επεξεργασίας»* των πληροφοριών του πολίτη, στον *«εκτελών την επεξεργασία»*, καθώς και στις *«τρίτες»* οντότητες. Το άρθρο 2 θεωρείται ιδιαίτερα σημαντικό γιατί ορίζει τους εμπλεκόμενους με τα δεδομένα, άρα και με το ζήτημα διαχείρισης των ταυτοτήτων.

Στο άρθρο 6 τίθενται οι αρχές που πρέπει να τηρούνται ως προς την ποιότητα των δεδομένων. Τα κράτη μέλη προβλέπουν τα δεδομένα να *«υφίστανται σύννομη και θεμιτή επεξεργασία, να συλλέγονται για καθορισμένους σαφείς και νόμιμους σκοπούς και η μεταγενέστερη επεξεργασία τους να συμβιβάζεται με τους σκοπούς αυτούς να είναι κατάλληλα, συναφή προς το θέμα και όχι υπερβολικά σε σχέση με τους σκοπούς για τους οποίους συλλέγονται και υφίστανται επεξεργασία να είναι ακριβή και εφόσον χρειάζεται να ενημερώνονται 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»*.

Αρχή της αναλογικότητας

Τα δεδομένα προς επεξεργασία πρέπει να συλλέγονται με νόμιμους και καθορισμένους τρόπους και ο αρμόδιος πρέπει να είναι ρητά καθορισμένος από κάθε κράτος. Πρόσθετα, τα δεδομένα προς συλλογή πρέπει να είναι ακριβή ως προς το θέμα για το οποίο συλλέγονται, να διατηρούνται για καθορισμένο χρονικό διάστημα, να μην υπάρχει υπερβολή ως προς τον όγκο της συλλεγόμενης πληροφορίας και να χρησιμοποιούνται αποκλειστικά για τον σκοπό για τον οποίο συλλέχτηκαν.

Αρχή του περιορισμού και του σκοπού χρήσης

Ιδιαίτερη προσοχή πρέπει να δίδεται στο μέσο που αποθηκεύονται, καθώς πολλές φορές δεδομένα που συγκεντρώθηκαν για καθορισμένο σκοπό καταλήγουν να αποτελούν δείγμα δεδομένων για περαιτέρω μελέτες.

Αρχή της διαφάνειας και της συμμετοχής του ατόμου

Στο άρθρο 11 γίνεται ρητή η υποχρέωση γνωστοποίησης της ταυτότητας του υπεύθυνου επεξεργασίας στο πρόσωπο στο οποίο αναφέρονται τα δεδομένα, του σκοπού και των αποδεκτών των προσωπικών τους δεδομένων, ώστε να υπάρχει διαφάνεια, ενώ στο άρθρο 14 αναφέρεται το δικαίωμα αντίταξης των δεδομένων.

Αρχή της ευθύνης

Στο άρθρο 17 αναφέρονται οι ενέργειες που πρέπει να πράξει, καθώς και τα κατάλληλα μέτρα που οφείλει να λάβει ο υπεύθυνος της επεξεργασίας, προκειμένου να διασφαλιστεί η ασφάλεια της επεξεργασίας και να καταλογιστούν οι αντίστοιχες ευθύνες.

Συμπερασματικά

Η οδηγία 95/46/EK αποτέλεσε την πρώτη οδηγία που σχετίζεται με το ζήτημα των ταυτοτήτων διότι και στις ταυτότητες περιλαμβάνονται προσωπικά δεδομένα. Το νομικό πλαίσιο καθορίζει ρητά τους ρόλους των εμπλεκόμενων οντοτήτων, επισημαίνει την ανάγκη της διαφάνειας και ασφάλειας της επεξεργασίας της πληροφορίας, η οποία πρέπει να είναι η ελάχιστη δυνατή.

3.2 Ηλεκτρονικές Υπογραφές (1999/93/EK)

Η οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13^{ης} Δεκεμβρίου 1999 αφορά τις ηλεκτρονικές υπογραφές, τις υπηρεσίες πιστοποίησης και τις προϋποθέσεις που θα εφαρμόζονται, προκειμένου να ενισχυθεί η εμπιστοσύνη των πολιτών της Ευρωπαϊκής Ένωσης στις νέες τεχνολογίες, στη γενικότερη αποδοχή τους και στην προαγωγή της διαλειτουργικότητας [97].

Στο άρθρο 2 της οδηγίας ορίζονται οι βασικές συνιστώσες της οδηγίας. Ακολουθούν οι ορισμοί της «ηλεκτρονικής υπογραφής», της «προηγμένης ηλεκτρονικής υπογραφής» και του «υπογράφοντα»:

S «ηλεκτρονική υπογραφή»: δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε, ή λογικά συσχετιζόμενα με, άλλα ηλεκτρονικά δεδομένα και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας

S «προηγμένη ηλεκτρονική υπογραφή»: ηλεκτρονική υπογραφή που ανταποκρίνεται στις εξής απαιτήσεις:

α) συνδέεται μονοσήμαντα με τον υπογράφοντα β) είναι

ικανή να ταυτοποιήσει τον υπογράφοντα

γ) δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο, και

δ) συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο ώστε να μπορεί να εντοπιστεί οποιαδήποτε επακόλουθη αλλοίωση των εν λόγω δεδομένων.

•S «υπογράφων»: φυσικό ή νομικό πρόσωπο που κατέχει διάταξη δημιουργίας υπογραφής και ενεργεί είτε για λογαριασμό του είτε εξ ονόματος φυσικού ή νομικού προσώπου ή φορέα που αντιπροσωπεύει

3.2.1. Προηγμένη Ηλεκτρονική Υπογραφή

Η ηλεκτρονική υπογραφή είναι στην ουσία η προσπάθεια μεταφοράς των στοιχείων της ιδιόχειρης υπογραφής στον ψηφιακό κόσμο. Εδώ και πολλούς αιώνες, η χρήση της φυσικής ή χειρόγραφης υπογραφής έχει σκοπό να επισημοποιήσει και να καταστήσει ισχυρή μια συμφώνηση μεταξύ δύο μερών, δεσμεύοντας τα ως προς την τήρηση των συμφωνηθέντων. Συνήθως προστίθεται πάνω σε ένα έγγραφο και έχει ως μορφή της το ονοματεπώνυμο του υπογράφοντος, είτε οποιαδήποτε σύμβολα προσδιορίζουν

την ταυτότητα του υπογράφοντος. Πρόσθετα δηλώνει ή επιβεβαιώνει την πρόθεση του υπογράφοντος να υπογράψει το έγγραφο και την έγκριση και υιοθέτηση των περιεχομένων του εγγράφου [100].

Μια εκδοχή ηλεκτρονικής υπογραφής μπορεί να συμπεριλάβει την χειρόγραφη υπογραφή ενός προσώπου που έχει σαρωθεί και έχει επισυναφθεί σε ένα κείμενο. Ωστόσο, μια ηλεκτρονική υπογραφή για να είναι ισοδύναμη με μια ιδιόχειρη υπογραφή αρκεί να:

- *S* εξασφαλίζει την γνησιότητα του υπογραφόμενου εγγράφου, καθώς και τις απαιτήσεις της ακεραιότητας, της εμπιστευτικότητας και της μη αποποίησης της ευθύνης του υπογράφοντα.
- *S* βασίζεται σε αναγνωρισμένο πιστοποιητικό που έχει εκδοθεί από εξουσιοδοτημένο παροχέα υπηρεσιών πιστοποίησης. *S* δημιουργείται από ασφαλή διάταξη δημιουργίας ψηφιακής υπογραφής.

Η οδηγία 99/93/EK διευκρινίζει ότι : *«Οι προηγμένες ηλεκτρονικές υπογραφές ικανοποιούν τις νομικές απαιτήσεις υπογραφής σε σχέση με δεδομένα ηλεκτρονικής μορφής με τον ίδιο τρόπο που μια χειρόγραφη υπογραφή ικανοποιεί τις απαιτήσεις αυτές σε σχέση με δεδομένα επί χάρτου και γίνονται δεκτές ως αποδεικτικό στοιχείο σε νομικές διαδικασίες».*

Στην πράξη μια ηλεκτρονική υπογραφή για να είναι ισοδύναμη με την ιδιόχειρη υπογραφή πρέπει να εμπίπτει στον ορισμό της προηγμένης ηλεκτρονικής υπογραφής και όχι στην αναφορά της ηλεκτρονικής υπογραφής.

Σημείο υπό περαιτέρω συζήτηση αποτελεί η αναφορά της μονοσήμαντης σύνδεσης της υπογραφής με τον υπογράφοντα. Η οδηγία απλά αναφέρει την προϋπόθεση, αλλά δεν υποδεικνύει τρόπο επίλυσης, κάτι που γενικότερα υφίσταται στις οδηγίες.

3.2.2. Ψηφιακά Πιστοποιητικά

Εκτός από την ψηφιακή υπογραφή, βασική παράμετρος των ηλεκτρονικών ταυτοτήτων αποτελεί το ψηφιακό πιστοποιητικό. Σύμφωνα με την οδηγία, ένα πιστοποιητικό προσδιορίζεται ως η *«ηλεκτρονική βεβαίωση, η οποία συνδέει δεδομένα επαλήθευσης υπογραφής με ένα άτομο που επιβεβαιώνει την ταυτότητά του»*, ενώ ένα αναγνωρισμένο πιστοποιητικό πρέπει να περιλαμβάνει:

«ένδειξη ότι αφορά αναγνωρισμένο πιστοποιητικό, τα στοιχεία αναγνώρισης του παρόχου υπηρεσιών πιστοποίησης και το κράτος στο οποίο είναι εγκατεστημένο, το όνομα του υπογράφοντος ή ψευδώνυμο που αναγνωρίζεται ως ψευδώνυμο, μια πρόβλεψη ειδικού χαρακτηριστικού του υπογράφοντος που θα περιληφθεί εφόσον είναι σημαντικό σε σχέση με τον σκοπό για τον οποίο προορίζεται το πιστοποιητικό, δεδομένα επαλήθευσης υπογραφής που αντιστοιχούν σε δεδομένα δημιουργίας υπογραφής υπό τον έλεγχο

του υπογράφοντος, μια ένδειξη της έναρξης και τέλος της περιόδου ισχύος του πιστοποιητικού, τον κωδικό ταυτοποίησης του πιστοποιητικού, την προηγμένη ηλεκτρονική υπογραφή του παρόχου υπηρεσιών πιστοποίησης που το εκδίδει, πιθανούς περιορισμούς του πεδίου χρήσης του πιστοποιητικού, και ενδεχομένως, όρια στο ύψος των συναλλαγών για τις οποίες το πιστοποιητικό μπορεί να χρησιμοποιηθεί».

Το ψηφιακό πιστοποιητικό εκδίδεται από κάποιο πάροχο υπηρεσιών πιστοποίησης, ο οποίος έχει την ευθύνη βεβαίωσης των δεδομένων του πιστοποιητικού που εξέδωσε. Η Κοινότητα αναγνωρίζει Παρόχους εντός και εκτός των ορίων της, αρκεί να πληρούν τις προϋποθέσεις της οδηγίας, να έχουν διαπιστευτεί από έναν εθελοντικό μηχανισμό πιστοποίησης και να υπερασπίζονται τις αρχές της αναλογικότητας, της νομιμότητας, του σκοπού, της ακρίβειας των δεδομένων και του καθορισμού της χρονικής διάρκειας της επεξεργασίας τους.

Μελετώντας το κείμενο της οδηγίας είναι εμφανής η περιγραφή των συμμετεχουσών οντοτήτων μας υποδομής δημοσίου κλειδιού χωρίς αυτή να αναφέρεται ρητά.

Συμπέρασμα

Η οδηγία για τις ηλεκτρονικές υπογραφές (οδηγία 1999/93/EK), έχει τεθεί σε ισχύ για πάνω από 14 χρόνια. Η οδηγία έχει κενά, όπως απροσδιόριστες υποχρεώσεις για την εθνική εποπτεία των παρόχων υπηρεσιών, οι οποίες συγκρατούν τις διασυννοριακές ηλεκτρονικές υπογραφές, και δεν καλύπτουν πολλές νέες τεχνολογίες [114]. Δεδομένης της ζήτησης για μεγαλύτερη εμπιστοσύνη στα ηλεκτρονικά υπηρεσίες, τα ζητήματα αυτά αντιμετωπίζονται καλύτερα από μια εξέλιξη για περισσότερο ολοκληρωμένη νομοθεσία.

3.3 Προστασία της Ιδιωτικής ζωής στις ηλεκτρονικές υπηρεσίες (2002/58/EK)

Η οδηγία 2002/58/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 διασφαλίζει τη προστασία των θεμελιωδών δικαιωμάτων των πολιτών των κρατών μελών της Ευρωπαϊκής Ένωσης κατά την επεξεργασία των δεδομένων προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες).

Η οδηγία αυτή προσαρμόζει και αντικαθιστά την οδηγία 97/66/EK, ώστε να παρέχεται το ίδιο επίπεδο προστασίας της ιδιωτικότητας των χρηστών ηλεκτρονικών υπηρεσιών ανεξαρτήτως των

χρησιμοποιούμενων τεχνολογιών [100], δρα συμπληρωματικά με την οδηγία 95/46/EK και στην ουσία μετατρέπει τις αρχές της οδηγίας 95/46/EK σε κανόνες.

Πρόσθετα με τους ορισμούς της παραγράφου 3.1, στο άρθρο 2 της οδηγίας σημειώνονται οι εξής ορισμοί:

- S «χρήστης» : κάθε φυσικό πρόσωπο που χρησιμοποιεί διαθέσιμη στο κοινό υπηρεσία ηλεκτρονικών επικοινωνιών, για προσωπικούς ή επαγγελματικούς σκοπούς χωρίς να είναι απαραίτητα συνδρομητής της εν λόγω υπηρεσίας
- S «δεδομένα κίνησης», τα δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μιας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσης της
- S «δεδομένα θέσης», τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μιας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών
- S «επικοινωνία», κάθε πληροφορία που ανταλλάσσεται ή διαβιβάζεται μεταξύ ενός πεπερασμένου αριθμού μερών, μέσω μιας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών.

Σύμφωνα με την οδηγία, η εγκατάσταση λογισμικού παρακολούθησης των αναγνωριστικών στοιχείων των χρηστών για την ανίχνευση των δραστηριοτήτων του (π.χ. cookies) παραβιάζει την ιδιωτική ζωή του χρήστη. Ωστόσο, σε ελάχιστες περιπτώσεις και μόνο όταν εξυπηρετούνται θεμιτοί σκοποί (λχ. διευκόλυνση παροχής υπηρεσιών), μπορούν να χρησιμοποιούνται cookies, υπό την προϋπόθεση ότι οι χρήστες είναι ενήμεροι (σύμφωνα με την οδηγία 95/46/EK) για τις πληροφορίες που αποθηκεύονται στον τερματικό τους εξοπλισμό.

Τα κράτη μέλη οφείλουν να ρυθμίσουν σε εθνικό επίπεδο το κατάλληλο νομικό πλαίσιο για τη διασφάλιση του απόρρητου επικοινωνιών μέσω του δημοσίου δικτύου επικοινωνιών. Στην Οδηγία συστήνεται προς τους παρόχους υπηρεσιών των κρατών μελών να υποστηρίξουν την αρχή της ελάχιστης πληροφορίας, τα θέματα διαχείρισης των ταυτοτήτων των χρηστών και την δυνατότητα απόκρυψης της ταυτότητάς του ατελώς.

Τα δεδομένα κίνησης και θέσης πρέπει να απαλείφονται, να καθίστανται ανώνυμα ή να διατίθενται για επεξεργασία για διαφημιστικούς σκοπούς μόνο με τη συγκατάθεση του χρήστη. Η ανωνυμία δεδομένων και η ρητή συγκατάθεση αποτελούν κεντρικές έννοιες στην επεξεργασία δεδομένων κίνησης, καθώς και των δεδομένων θέσης. Η συγκατάθεση δεν μπορεί να θεωρείται τελεσίδικη, καθώς ο χρήστης θα πρέπει να μπορεί να αρνηθεί την προσωρινή επεξεργασία των δεδομένων του.

3.4 Διατήρηση δεδομένων θέσης και κίνησης (2006/24/EK)

Η οδηγία 2006/24/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15^{ης} Μαρτίου 2006 στοχεύει στην εναρμόνιση των κρατών μελών σε μια κοινή πορεία για το ζήτημα της διατήρησης των δεδομένων των υπηρεσιών ηλεκτρονικής επικοινωνίας από τους παρόχους υπηρεσιών, ώστε να είναι διαθέσιμα σε περίπτωση δίωξης σοβαρών ποινικών αδικημάτων. Η παρούσα οδηγία τροποποιεί την οδηγία 2002/58/EK της παραγράφου 3.3 [101].

Στο άρθρο 2 της οδηγίας ορίζονται οι βασικές συνιστώσες της οδηγίας:

- S «δεδομένα» : τα δεδομένα κίνησης και θέσης και τα συναφή δεδομένα που είναι αναγκαία για την αναγνώριση του συνδρομητή ή χρήστη
- S «χρήστης» : κάθε νομική οντότητα ή φυσικό πρόσωπο που χρησιμοποιεί διαθέσιμη στο κοινό υπηρεσία ηλεκτρονικών υπηρεσιών, για ιδιωτικούς ή εμπορικούς σκοπούς χωρίς να είναι απαραίτητα συνδρομητής της εν λόγω υπηρεσίας
- S «τηλεφωνική υπηρεσία»: κλήσεις, συμπληρωματικές υπηρεσίες, υπηρεσίες μηνυμάτων και πολυμέσων
- S «κωδικός ταυτότητας χρήστη» : ο μοναδικός αναγνωριστικός κωδικός που αποδίδεται σε κάθε πρόσωπο όταν καθίσταται συνδρομητής ή εγγράφεται σε κάποια υπηρεσία πρόσβασης στο Διαδίκτυο ή επικοινωνίας μέσω του Διαδικτύου
- S «κωδικός ταυτότητας κυψέλης» : η ταυτότητα του κυψελωτού κυττάρου από το οποίο ξεκινά ή στο οποίο καταλήγει η συγκεκριμένη κλήση κινητής τηλεφωνίας

Τα δεδομένα που διατηρούνται, είτε υποβάλλονται σε επεξεργασία πρέπει να γνωστοποιούνται στις εθνικές αρχές μόνο σε ειδικές περιπτώσεις σύμφωνα με την εθνική νομοθεσία. Τα κράτη μέλη οφείλουν να διατηρούν δεδομένα που είναι απαραίτητα για τον προσδιορισμό:

- S της πηγής και του προορισμού επικοινωνίας, είτε η επικοινωνία είναι τηλεφωνική είτε αφορά σε επικοινωνία Διαδικτύου

■Στης υπηρεσίας ηλεκτρονικού ταχυδρομείου

■Στης ημερομηνίας, ώρας και διάρκειας επικοινωνίας

■Στου είδους της επικοινωνίας

■Στου εξοπλισμού επικοινωνίας των χρηστών

Σ της θέσης του εξοπλισμού κινητής επικοινωνίας

Σημαντικό στοιχείο της Οδηγίας είναι η διατήρηση των δεδομένων για περιορισμένο χρονικό διάστημα. Συγκεκριμένα, όταν η διατήρηση των δεδομένων αφορά παρόχους επικοινωνιών Διαδικτύου, τότε οι πάροχοι οφείλουν να διατηρούν δεδομένα των υπηρεσιών τους ή του δικτύου τους. Στην παρούσα οδηγία υφίσταται και το δικαίωμα αποζημίωσης των χρηστών από οποιαδήποτε παράνομη επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Συμπέρασμα

Οι νομικές και τεχνικές διαφοροποιήσεις μεταξύ των εθνικών διατάξεων ώστε να διαπιστωθούν και διωχθούν ποινικά αδικήματα είναι τα βασικά εμπόδια που αντιμετωπίζουν οι πάροχοι υπηρεσιών κατά την διατήρηση των δεδομένων θέσης και κίνησης. Προφανώς, το κλειδί και στην υπό μελέτη οδηγία είναι η τήρηση των αρχών αναλογικότητας και η υποστήριξη των ρητών και νόμιμων σκοπών κατά την διατήρηση αυτών των δεδομένων.

3.5 Παροχή Υπηρεσιών στην εσωτερική αγορά (2006/123/EK)

Η οδηγία 2006/123/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12^{ης} Δεκεμβρίου 2006 θεσπίζει τις γενικές διατάξεις που διευκολύνουν την άσκηση της ελευθερίας εγκατάστασης των παρόχων υπηρεσιών και την ελεύθερη κυκλοφορία των υπηρεσιών κάθε κράτους μέλους, διατηρώντας ταυτόχρονα υψηλό ποιοτικό επίπεδο υπηρεσιών [98].

Στο άρθρο 4 της οδηγίας ορίζονται οι βασικές συνιστώσες της οδηγίας,

- S «υπηρεσία» : κάθε μη μισθωτή οικονομική δραστηριότητα, που παρέχεται κατά κανόνα έναντι αμοιβής,
- S «πάροχος υπηρεσιών» : κάθε φυσικό πρόσωπο που έχει την ιθαγένεια κράτους μέλους ή κάθε νομικό πρόσωπο, κατά το άρθρο 48 της συνθήκης εγκατεστημένο σε κράτος μέλος τα οποία προσφέρουν ή παρέχουν μια υπηρεσία-
- S ως «αποδέκτης» : κάθε φυσικό πρόσωπο που έχει την ιθαγένεια κράτους μέλους ή που επωφελείται από δικαιώματα που του παρέχονται από κοινοτικές πράξεις ή κάθε νομικό πρόσωπο, κατά το άρθρο 48 της συνθήκης εγκατεστημένο σε κράτος μέλος τα οποία χρησιμοποιούν ή επιθυμούν να χρησιμοποιήσουν μια υπηρεσία για επαγγελματικούς ή άλλους σκοπούς

Η οδηγία αυτή καθορίζει τους κανόνες που πρέπει να διέπουν την ελεύθερη κυκλοφορία των υπηρεσιών στην εσωτερική αγορά της Ευρωπαϊκής Ένωσης. Με την έννοια της εσωτερικής αγοράς καθορίζονται ως σύνορα της αγοράς τα ευρωπαϊκά σύνορα και προάγεται η διαλειτουργικότητα. Συνεπώς με την προάσπιση της διαλειτουργικότητας των υπηρεσιών, υποστηρίζεται ρητά η ενιαία αγορά των υπηρεσιών με την ταυτόχρονη διαφύλαξη των δικαιωμάτων των πολιτών ως καταναλωτών και η υιοθέτηση ενός δυναμικού και επιλεκτικού πλαισίου προσανατολισμένο στα χαρακτηριστικά της εκάστοτε υπηρεσίας.

Οι πάροχοι υπηρεσιών θα πρέπει να υποστηρίζονται διασυνοριακά και να μπορούν να εγκαθίστανται σε ένα κράτος μέλος, ώστε να προσδιορίζεται ο τόπος εγκατάστασης. Ωστόσο, θα πρέπει να απλουστευτούν οι διοικητικές διαδικασίες με διαδικασίες ηλεκτρονικής διεκπεραίωσης προς όφελος των παρόχων, των αποδεκτών και των αρμόδιων αρχών.

Εφόσον θα πρέπει να υποστηριχτούν οι διαδικασίες ηλεκτρονικής διεκπεραίωσης, οι πολίτες πρέπει να ταυτοποιούνται ηλεκτρονικά. Ως αποτέλεσμα, ένα ενιαίο σύστημα διαχείρισης ταυτοτήτων αποτελεί την βέλτιστη πρακτική, γεγονός που καταγράφεται στο άρθρο 8 της Οδηγίας : «τα κράτη μέλη εξασφαλίζουν ότι όλες οι διαδικασίες και οι διατυπώσεις για την πρόσβαση σε δραστηριότητες παροχής υπηρεσιών και για την άσκηση τους μπορούν να διεκπεραιωθούν εύκολα από απόσταση και με ηλεκτρονικά μέσα μέσω του οικείου ενιαίου κέντρου εξυπηρέτησης και στις αρμόδιες αρχές».

3.6 Κανονισμός eIDAS (Electronic Identification and Signature)

Τον Ιούνιο του 2012 η Ευρωπαϊκή Επιτροπή ενέκρινε μια πρόταση κανονισμού που αφορούσε την ηλεκτρονική ταυτοποίηση και την εμπιστοσύνη για τις ηλεκτρονικές συναλλαγές με τις υπηρεσίες στην εσωτερική αγορά. Τον Μάιο του 2014 πρόκειται να κυκλοφορήσει επίσημα η συναινετική θέση μεταξύ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της Ευρωπαϊκής Ένωσης [19,101].

Το νέο πλαίσιο θα αντικαταστήσει την οδηγία 1999/93/EK και θα εκσυγχρονίσει τους υφιστάμενους κανόνες σε σχέση με τις ηλεκτρονικές υπογραφές. Ως αποτέλεσμα θα υπάρξει το πολυπόθητο νομικό πλαίσιο για την υποστήριξη της πανευρωπαϊκής αναγνώρισης των ηλεκτρονικών ταυτοτήτων που χρησιμοποιούνται από τα κράτη μέλη (π.χ. βελγική eID), καθώς και θα υποστηριχτούν υπηρεσίες ηλεκτρονικής επικύρωσης (electronic seals) χρονοσήμανσης (time stamping) και ηλεκτρονικής συστημένης επιστολής (electronic registered delivery).

Στις 28 Φεβρουαρίου 2014, κατά την υπογραφή του σχεδίου κανονισμού για την ηλεκτρονική ταυτοποίηση και εμπιστοσύνη για τις ηλεκτρονικές συναλλαγές υπηρεσιών η Αντιπρόεδρος της Ευρωπαϊκής Επιτροπής Neelie Kroes στο χαιρετισμό που απηύθυνε ανέφερε : *«Η έγκριση του παρόντος κανονισμού σχετικά με την ηλεκτρονική ταυτότητα είναι ένα θεμελιώδες βήμα προς την ολοκλήρωση της ενιαίας ψηφιακής αγοράς. Η συμφωνία αυτή αποτελεί την ώθηση για την εμπιστοσύνη και την διευκόλυνση των διασυνοριακών και διατομεακών ηλεκτρονικών συναλλαγών. Θα ήθελα να ευχαριστήσω το Ευρωπαϊκό Κοινοβούλιο, την εισηγήτρια της ITRE, Marita Ulvskog και την εισηγήτρια της IMCO Marielle Gallo και τους αφανείς εισηγητές από την Ελλάδα, την Λιθουανία, την Ιρλανδία και την Κύπρο σχετικά με την εργασία τους για αυτό το αρχείο»* [101].

Ο κανονισμός πρόκειται να τεθεί σε ισχύ την 1η Ιουλίου του 2014 με άμεση εφαρμογή. Τα οφέλη από την εφαρμογή του προβλέπεται να γίνουν ορατά με την εφαρμογή του, καθώς σκοπός είναι η μείωση των κατακερματισμένων εθνικών νομικών συστημάτων και της γραφειοκρατίας των περιττών δαπανών. Το κλειδί στον κανονισμό -όπως βέβαια απορρέει και από προγενέστερες αναφορές στο παρόν κεφάλαιο- είναι η Διαλειτουργικότητα της ηλεκτρονικής ταυτότητας και των υπηρεσιών, ώστε να θωρακιστεί η νομιμότητα των εθνικών και διασυνοριακών συναλλαγών.

Η ονομασία του κανονισμού eIDAS στηρίχτηκε στις προασπιζόμενες αρχές ασφαλείας:

- /Διαφάνεια, λογοδοσία και Αξιοπιστία, καθιερώνοντας τις ελάχιστες υποχρεώσεις των Παροχών Υπηρεσιών Εμπιστοσύνης (Trust Services Providers - TSPs)
- /Αξιοπιστία των υπηρεσιών σε συνδυασμό με τις απαιτήσεις ασφαλείας των TSPs

S Τεχνολογική ανεξαρτησία

S Σύγκλιση με τους κανόνες της αγοράς και στήριξη της προτυποποίησης

Ως γενικό συμπέρασμα, οι πολίτες και οι επιχειρήσεις θα μπορούν να έχουν διασυνοριακή πρόσβαση σε δημόσιες υπηρεσίες σε άλλες χώρες της ΕΕ, με πλήρη σεβασμό της ιδιωτικής ζωής και των κανόνων προστασίας των δεδομένων και θα γίνουν οι απαραίτητες διαδικασίες ώστε να μην υπάρχουν εμπόδια για την εμπιστοσύνη στις ηλεκτρονικά παρεχόμενες διασυνοριακές υπηρεσίες.

Κεφάλαιο 4

Ηλεκτρονική Διακυβέρνηση

Κάποτε οι άνθρωποι στέκονταν στις ουρές των Δημόσιων Οικονομικών Υπηρεσιών, αναμένοντας να πληρώσουν οφειλές, είτε να τακτοποιήσουν διάφορα φορολογικά ζητήματα, αγανακτώντας από την ορθοστασία και χάνοντας τον πολύτιμο χρόνο τους. Τότε η ηλεκτρονική εξυπηρέτηση δεν υπήρχε, οπότε ήταν αναπόφευκτη η αναμονή. Κι όμως, δεν πέρασε πολλά χρόνια από το «τότε». Μέσα σε λίγα χρόνια τα πράγματα άλλαξαν. Το φαινόμενο των ουρών δεν εξαλείφθηκε, αλλά σίγουρα περιορίστηκε. Οι περισσότεροι πολίτες αξιοποίησαν την νέα πραγματικότητα. Και έτσι χρησιμοποίησαν την αντίστοιχη ηλεκτρονική φορολογική υπηρεσία πραγματοποιώντας, προϊόντος του χρόνου τις περισσότερες συναλλαγές τους ψηφιακά. Και η πορεία αυτή τα επόμενα χρόνια φαίνεται ότι θα συνεχιστεί.

Επιτηδευμένα η πρώτη παράγραφος του 4^{ου} κεφαλαίου αναφέρθηκε στις φορολογικές υπηρεσίες για να δοθεί έμφαση στην ταλαιπωρία του πολίτη. Καθημερινά οι πολίτες επισκέπτονται πλήθος δημόσιων υπηρεσιών για την διεκπεραίωση υποθέσεων οι οποίες χρήζουν αντίστοιχης ηλεκτρονικής υποστήριξης.

Στο κεφάλαιο αυτό μελετάται το πλαίσιο της Ηλεκτρονικής Διακυβέρνησης, με αναφορά στους στόχους των υπηρεσιών της, τα κύρια χαρακτηριστικά της, καθώς και τα επίπεδα ολοκλήρωσης υπηρεσιών που έχουν τεθεί. Σε ξεχωριστή ενότητα δίδεται έμφαση στην Διαλειτουργικότητα των ηλεκτρονικών υπηρεσιών. Η Διαλειτουργικότητα αποτελεί σημαντικό πυλώνα για τις ηλεκτρονικές υπηρεσίες, γεγονός που υποστηρίζεται από την Ευρωπαϊκή Ένωση στην οδηγία 2006/123/EK.

4.1 Πλαίσιο Ηλεκτρονικής Διακυβέρνησης

4.1.1 Περί Ηλεκτρονικής Διακυβέρνησης

Μια υπηρεσία Ηλεκτρονικής Διακυβέρνησης είναι μια συναλλαγή που για να ολοκληρωθεί απαιτεί τη συνύπαρξη τεσσάρων προϋποθέσεων:

1. να παρέχεται από έναν πάροχο,
2. να ρυθμίζεται από έναν ρυθμιστή
3. να πραγματοποιηθεί από έναν τελικό χρήστη, και
4. να έχει ένα τελικό παραδοτέο [68].

Η Ηλεκτρονική Διακυβέρνηση περιλαμβάνει όλους τους μηχανισμούς αξιοποίησης των τεχνολογιών πληροφορικής και επικοινωνιών στις δημόσιες υπηρεσίες με στόχο την εξυπηρέτηση των πολιτών με την Κυβέρνηση (Government to Citizen - G2C), την εξυπηρέτηση των επιχειρήσεων από την Κυβέρνηση (Government to Business - G2B) και την εξυπηρέτηση άλλων οργανισμών (Government to Government).

Η Ευρωπαϊκή Επιτροπή ορίζει την Ηλεκτρονική Διακυβέρνηση (ΗΔ) ως την *«χρήση των τεχνολογιών της πληροφορικής και των τηλεπικοινωνιών στη Δημόσια Διοίκηση, σε συνδυασμό με οργανωτικές αλλαγές και νέες δεξιότητες του προσωπικού, με σκοπό την βελτίωση της εξυπηρέτησης του κοινού, την ενδυνάμωση της δημοκρατίας και την υποστήριξη των δημόσιων πολιτικών»*.

4.1.2 Ανάγκες Ηλεκτρονικής Διακυβέρνησης

Οι κύριες ανάγκες που πρέπει να εξυπηρετούνται στην Ηλεκτρονική Διακυβέρνηση προκύπτουν από την μελέτη του ορισμού της προηγούμενης παραγράφου. Η κλασική Δημόσια Διοίκηση πρέπει να αλλάξει και να στραφεί στην Ψηφιακή Δημόσια Διοίκηση. Πολλές διαδικασίες χρήζουν περαιτέρω βελτίωσης,

εκσυγχρονισμού και αναδιοργάνωσης. Με σωστή καθοδήγηση, οι τεχνολογίες πληροφορικής και τηλεπικοινωνίας μπορούν να διεισδύσουν ριζικά και να επιταχύνουν τις διαδικασίες Δημόσιας Διοίκησης με στόχο μια Ανοιχτή, Διαλειτουργική και Συνεργατική Δημόσια Διοίκηση.

Πρώτη ανάγκη είναι η ταχύτητα και η ποιότητα εξυπηρέτησης του πολίτη. Η αξιοποίηση των Τεχνολογιών Πληροφορικής στις υπηρεσίες της Δημόσιας Διοίκησης συντελεί στην βελτίωση της εξυπηρέτησης κοινού. Με την διάθεση γρήγορων και αποτελεσματικών υπηρεσιών, ο πολίτης εξυπηρετείται ταχύτερα, χωρίς φυσική παρουσία, καθώς η εξυπηρέτηση πραγματοποιείται από οποιοδήποτε σημείο επί 24ωρου βάσεως. Πρόσθετα, η άμεση πρόσβαση στην ζητούμενη πληροφορία, δίχως την χρήση ενδιάμεσων σταδίων (one-stop-shop) και η συνεχής ενημέρωση της κατάστασης εξέλιξης της πορείας ενός αιτήματος υπηρεσίας, ενδυναμώνει το αίσθημα ικανοποίησης του πολίτη, εγκαθιστά ένα ισχυρό επίπεδο εμπιστοσύνης και συμβάλλει στην αύξηση της αξιοπιστίας των υπηρεσιών Ηλεκτρονικής Διακυβέρνησης [63].

Επόμενη σημαντική ανάγκη της Ηλεκτρονικής Διακυβέρνησης θεωρείται η βελτιστοποίηση των παρεχόμενων υπηρεσιών. Καθώς βελτιστοποιούνται οι υπηρεσίες, μειώνονται οι απαιτούμενες διοικητικές πράξεις και αντίστοιχα μειώνονται οι απαιτήσεις του εργατικού δυναμικού και το συνολικό κόστος των υπηρεσιών. Η επιτάχυνση των διοικητικών διαδικασιών συντελεί στην αύξηση της ανταγωνιστικότητας των επιχειρήσεων [107].

Σύμφωνα με την «Ψηφιακή πρόκληση της Ευρώπης, «η έξυπνη χρήση των ΤΠΕ από δημόσιους φορείς μπορεί να μειώσει το κόστος των δημόσιων διοικήσεων κατά 15-20%. Η ΕΕ πρέπει να κάνει πλήρη μετάβαση στις ηλεκτρονικές δημόσιες συμβάσεις έως το 2018, όπως απαιτείται από τις νέες οδηγίες περί δημοσίων συμβάσεων. Σύμφωνα με τις εκτιμήσεις η έγκριση της ηλεκτρονικής τιμολόγησης στις δημόσιες συμβάσεις σε ολόκληρη την ΕΕ θα μπορούσε να εξοικονομήσει 2,3 δις. Ευρώ» [191].

Η τρίτη ανάγκη των υπηρεσιών Ηλεκτρονικής Διακυβέρνησης αφορά την αξιοποίηση των πληροφοριών από τις Δημόσιες υπηρεσίες σε τοπικό και εθνικό επίπεδο, ώστε να καταστεί δυνατή η διασυνοριακή εξυπηρέτηση των πολιτών [68].

Τελευταία, αλλά ιδιαίτερη σημαντική είναι η ανάγκη καθορισμού ενός επιπέδου ασφάλειας των προσωπικών δεδομένων των πολιτών κατά τις ηλεκτρονικές συναλλαγές. Η υιοθέτηση τεχνολογιών για την ενίσχυση της Ιδιωτικότητας υπερασπίζεται την αυθεντικοποίηση, την ακεραιότητα, την εμπιστευτικότητα του περιεχομένου των συναλλαγών, καθώς και την μη-αποποίηση των συναλλαγών από πλευράς πολιτών.

4.1.3 Μέσα Ηλεκτρονικής Διακυβέρνησης

Στις προηγούμενες ενότητες του κεφαλαίου παρουσιάστηκαν οι ανάγκες που πρόκειται να προσπαθήσει να καλύψει η Ηλεκτρονική Διακυβέρνηση, καθώς επίσης και οι εμπλεκόμενοι που συμμετέχουν. Ωστόσο για να υπάρξει Ηλεκτρονική Διακυβέρνηση δεν αρκεί μόνο το όραμα και το κοινό στο οποίο θα απευθύνεται. Από τεχνικής πλευράς, είναι απαραίτητη η ύπαρξη μιας Υποδομής Πληροφορικής που θα υποστηρίξει το όλο εγχείρημα. Στην Υποδομή Πληροφορικής περιλαμβάνεται ο δικτυακός εξοπλισμός (συμπεριλαμβανομένων των ενσύρματων/ασύρματων συνδέσεων) μεταξύ των υπηρεσιών Ηλεκτρονικής Διακυβέρνησης, οι τεχνολογίες υποστήριξης της ασφάλειας των υπηρεσιών ΗΔ, οι εξυπηρετητές των εφαρμογών ΗΔ, οι εφαρμογές διαχείρισης του περιεχομένου και των συστημάτων ΗΔ, το υλικό και τα εργαλεία ανάπτυξης εφαρμογών [69].

4.1.4 Επίπεδα Αξιολόγησης Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης

Ένας πολίτης, είτε μια επιχείρηση μπορεί να αιτηθεί κάποια υπηρεσία από την Δημόσια Διοίκηση. Ωστόσο κάποιες υπηρεσίες μπορούν να περατωθούν ηλεκτρονικά, ενώ άλλες απαιτούν φυσική παρουσία στους αντίστοιχους φορείς. Σκοπός της Ηλεκτρονικής Διακυβέρνησης είναι να παρασχεθούν όσο το δυνατόν περισσότερες ηλεκτρονικές υπηρεσίες που θα επιφέρουν την ταχύτερη εξυπηρέτηση στους αιτούντες και τις άσκοπες μεταβάσεις τους στους αντίστοιχους φορείς. Πά να μπορέσει να καταστεί δυνατή η μέτρηση του βαθμού ανάπτυξης κάθε ηλεκτρονικής υπηρεσίας η Ευρωπαϊκή Ένωση καθόρισε πέντε επίπεδα αξιολόγησης, όπως επισημαίνονται στον πίνακα 4.1.

Επίπεδο	Επίπεδα Αξιολόγησης ΗΔ	Ποσοστό Ολοκλήρωσης	Στάδια ΗΔ
1	Πληροφοριακές Υπηρεσίες	20-39%	1. Δημοσιεύω
2	Επικοινωνιακές Υπηρεσίες	40-59%	
3	Διαδραστικές Υπηρεσίες	60-79%	2. Αλληλεπιδρώ
4	Συναλλακτικές Υπηρεσίες	80-99%	3. Συναλλάσσομαι
5	Προσωποποιημένες Υπηρεσίες	100%	

Πίνακας 4.1: Επίπεδα αξιολόγησης υπηρεσιών Ηλεκτρονικής Διακυβέρνησης

Στον πίνακα 4.1 παρουσιάζεται η συσχέτιση των σταδίων Ηλεκτρονικής Διακυβέρνησης με τα επίπεδα αξιολόγησης των υπηρεσιών ΗΔ. Κάθε επίπεδο σχετίζεται με ένα «ποσοστό ολοκλήρωσης». Παρόλο που δεν περιλαμβάνεται στα επίπεδα αξιολόγησης, υπάρχει ένα μηδενικό επίπεδο κατά το οποίο δεν υφίσταται «ηλεκτρονικός χαρακτήρας» για μια υπηρεσία και λαμβάνει το ποσοστό εύρους 0-19% [157].

Οι πληροφοριακές υπηρεσίες δεν απαιτούν αλληλεπίδραση του πολίτη και παρέχουν μόνο δημοσιεύσεις κατάλληλου υλικού για την διεκπεραίωση μιας υπηρεσίας. Οι επικοινωνιακές υπηρεσίες προσφέρουν έντυπα σε ηλεκτρονική μορφή, τα οποία μπορεί να αποθηκεύσει ο χρήστης και να τα αξιοποιήσει στις συναλλαγές με τον φορέα υπηρεσίας. Σε μια διαδραστική υπηρεσία ο πολίτης (G2C), είτε με επιχείρηση (G2B) μπορεί να υποβάλει ένα αίτημα εξυπηρέτησης ηλεκτρονικά και να λάβει μια απάντηση από την αντίστοιχη ηλεκτρονική υπηρεσία, ενώ μια συναλλακτική υπηρεσία υποκαθιστά πλήρως μια κλασική υπηρεσία [63, 82]. Ως προσωποποιημένες υπηρεσίες χαρακτηρίζονται οι υπηρεσίες όπου το κράτος παρέχει υπηρεσίες στον πολίτη δίχως δικό του προγενέστερο αίτημα.

4.2 Ιδιωτικότητα και Ηλεκτρονική Διακυβέρνηση

Η Ηλεκτρονική Διακυβέρνηση συνεπάγεται χρήση των υπηρεσιών που προσφέρονται στους χρήστες με την προϋπόθεση ανταλλαγής ορισμένων πληροφοριών. Η Ιδιωτικότητα αποτελεί μια παράμετρο που πρέπει να λαμβάνουν υπ' όψιν τους, αλλά και να την υπερασπίζονται τα συστήματα Ηλεκτρονικής Διακυβέρνησης. Στην ενότητα αυτή μελετάται η σαφής διάκριση της ιδιωτικότητας των δεδομένων και των υπηρεσιών στα περιβάλλοντα Ηλεκτρονικής Διακυβέρνησης και αναφέρονται τα στοιχεία που

πρέπει να τηρούν οι υπηρεσίες Ηλεκτρονικής Διακυβέρνησης προκειμένου να διασφαλίζεται η Ιδιωτικότητα των στοιχείων των πολιτών στις παρεχόμενες υπηρεσίες.

Ιδιωτικότητα

Η ιδιωτικότητα (privacy) αναφέρεται στο δικαίωμα ενός ατόμου να διαφυλάσσει στοιχεία της προσωπικής του ζωής και να διατηρεί έναν ιδιωτικό χώρο μακριά από προσπέλαση και παρεμβάσεις τρίτων. Η ιδιωτικότητα περιλαμβάνει τη δυνατότητα ενός ατόμου να ελέγχει το είδος της πληροφορίας που αποκαλύπτεται για αυτόν, αλλά και σε ποιόν αυτή αποκαλύπτεται. Επομένως, στην έννοια της ιδιωτικότητας περιλαμβάνεται τόσο το «ποια» πληροφορία, «πώς» και «σε ποιους» αποκαλύπτεται, όσο και η διατάραξη της προσωπικής ζωής του ατόμου από τρίτους.

Ένας παλιότερος ορισμός της Ιδιωτικότητας που δόθηκε από τον Alen Westin το 1967 ανέφερε πως η Ιδιωτικότητα αντικατοπτρίζει : «Το δικαίωμα του κάθε ανθρώπου ή ομάδας ατόμων ή οργανισμών, να καθορίζουν από μόνοι τους, πότε, πώς και σε ποιό βαθμό οι προσωπικές τους πληροφορίες θα γίνονται γνωστές σε τρίτους».

Μία από τις ιδιότητες της ηλεκτρονικής ταυτότητας είναι η αποθήκευση και επεξεργασία προσωπικών δεδομένων. Με την προσπέλαση των πολιτών σε υπηρεσίες Ηλεκτρονικής Διακυβέρνησης υπάρχει η περίπτωση καταγραφής των αιτημάτων του πολίτη. Ο εκτελών την επεξεργασία των δεδομένων του πολίτη ενδέχεται να σχηματίσει ικανοποιητική εικόνα για τον πολίτη, για τις συνήθειες του, καθώς και να προβλέψει στοιχεία από τη μελλοντική συμπεριφορά του. Υπό αυτές τις συνθήκες, θεμελιώδη ατομικά δικαιώματα και ελευθερίες εξανεμίζονται.

Ιδιωτικότητα δεδομένων

Από πλευράς ιδιωτικότητας, τα δεδομένα κατηγοριοποιούνται σε δημόσια, προσωπικά και ευαίσθητα προσωπικά δεδομένα. Για την υπεράσπιση της Ιδιωτικότητας των δεδομένων πρέπει να ακολουθηθούν οι απαιτήσεις της ασφάλειας. Συνεπώς για να διαφυλάσσεται η Ιδιωτικότητα πρέπει να προστατεύονται τα δεδομένα των πολιτών ως προς την:

■ **S** Εμπιστευτικότητα : τα δεδομένα να μην είναι διαθέσιμα σε μη εξουσιοδοτημένες οντότητες

■ **S** Ακεραιότητα : τα δεδομένα να μην επέρχονται αλλοιώσεις από μη εξουσιοδοτημένες οντότητες

■ **S** Διαθεσιμότητα : τα δεδομένα να είναι διαθέσιμα προς χρήση όταν ζητηθούν από μία εξουσιοδοτημένη οντότητα

■ **S Αυθεντικότητα:** η οντότητα να είναι πραγματικά αυτή που έχει ισχυριστεί ότι είναι

S Λογοδοσία - Απόδοση ευθύνης (Accountability) : η οντότητα να είναι υπεύθυνη για το πώς πράττει και ενεργεί

S Μη αποποίηση ευθύνης (Non-repudiation) : η οντότητα να μην μπορεί να αμφισβητήσει την συμμετοχή της σε ένα γεγονός ή μια ενέργεια [66]

Ιδιωτικότητα Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης

Η παρούσα υποπαράγραφος έχει άμεση σχέση με την ενότητα 4.1.4, όπου αναφέρονται τα επίπεδα ολοκλήρωσης των υπηρεσιών ηλεκτρονικής διακυβέρνησης. Σε μια υπηρεσία Ηλεκτρονικής Διακυβέρνησης, ανάλογα με την ιδιότητα του αιτούμενου (πολίτης, επιχείρηση), είτε ανάλογα με το θεματικό αντικείμενο υπηρεσίας παρέχονται και ανταλλάσσονται πολλές πληροφορίες.

Στις υπηρεσίες όπου προσφέρονται πληροφορίες διαδικασιών (και απαραίτητων δικαιολογητικών) δεν τίθεται θέμα Ιδιωτικότητας, αφού ο χρήστης δεν παρέχει οποιαδήποτε πληροφορία στην υπηρεσία.

Στις υπηρεσίες όπου παρέχεται η δυνατότητα ηλεκτρονικής αίτησης ο χρήστης πρέπει να παρέχει το όνομα και το συνθηματικό του προκειμένου να έχει πρόσβαση στην υπηρεσία. Σε αυτή την περίπτωση η υπηρεσία Ηλεκτρονικής Διακυβέρνησης συλλέγει ελάχιστα προσωπικά δεδομένα για τον χρήστη και δεν διακυβεύεται η ιδιωτικότητα του χρήστη.

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

Δεδομένου ότι η Ηλεκτρονική Διακυβέρνηση επηρεάζει άμεσα την Ιδιωτικότητα καθώς απαιτεί συλλογή και επεξεργασία δεδομένων των χρηστών, η Ευρωπαϊκή Επιτροπή έχει εκδώσει την οδηγία 2006/24/EK. Όπως περιγράφηκε στην αντίστοιχη ενότητα του Κεφαλαίου 3, τα δεδομένα των χρηστών πρέπει να είναι διαθέσιμα μόνο σε περίπτωση διάπραξης σοβαρών ποινικών αδικημάτων για την απονομή δικαιοσύνης και συστήνεται να θωρακίζονται με μηχανισμούς ασφαλείας.

Τεχνολογίες Ενίσχυσης Ιδιωτικότητας

Στις μέρες μας οι κυριότερες απειλές ιδιωτικότητας αφορούν επιθέσεις ιχνηλάτησης προς τα πίσω (backward -traceback attack), κακόβουλους συνεργούς (malicious collaborator), υποκλοπείς

(eavesdroppers), επιθέσεις κωδικοποίησης - όγκου μηνυμάτων (message coding -volume attack), επιθέσεις χρονισμού (timing attacks), επιθέσεις υπερχειλίσης (flooding attacks), επιθέσεις περιόδου σύνδεσης (connection periods attacks), cookies [78].

Κατά την σχεδίαση ψηφιακών υπηρεσιών διακυβέρνησης η ιδιωτικότητα πρέπει να αποτελεί σχεδιαστική παράμετρο και να ενισχύεται με τεχνολογικές μεθόδους. Καθώς οι υπηρεσίες ΗΔ θα δημοσιοποιούν την υποστήριξη ενός πλαισίου ενίσχυσης της Ιδιωτικότητας οι πολίτες θα αυξήσουν το επίπεδο εμπιστοσύνης τους προς τις παρεχόμενες ηλεκτρονικές υπηρεσίες.

4.3 Διαλειτουργικότητα Ηλεκτρονικής Διακυβέρνησης

Στα περιβάλλοντα Ηλεκτρονικής Διακυβέρνησης η διαλειτουργικότητα αποτελεί ένα πολύ ισχυρό πλεονέκτημα, γιατί είναι το χαρακτηριστικό εκείνο που δίνει την δύναμη σε διαφορετικά συστήματα να επικοινωνούν και να μοιράζονται την γνώση πληροφοριών. Σύμφωνα με τον ορισμό του Πλαισίου Ηλεκτρονικής Διακυβέρνησης του Υπουργείου Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης, με τον όρο *«διαλειτουργικότητα, εννοούμε την δυνατότητα που παρέχουν τα πληροφοριακά και τηλεπικοινωνιακά συστήματα καθώς επίσης και οι επιχειρηματικές διαδικασίες που υποστηρίζουν, να ανταλλάσσουν δεδομένα και να επιτρέπουν την κοινή χρήση πληροφορίας και γνώσης»* [153].

Η Διαλειτουργικότητα κατατάσσεται σε τρία επίπεδα:

S Οργανωσιακή Διαλειτουργικότητα : μελετώνται τα μοντέλα διαδικασιών για όλους τους εμπλεκόμενους

S Σημασιολογική Διαλειτουργικότητα : δημιουργούνται / συγκεντρώνονται μοντέλα

επαναχρησιμοποίησης ■ *S* Τεχνική Διαλειτουργικότητα : εκδίδονται περαιτέρω οδηγίες για τα επιμέρους πλαίσια

Η Ευρωπαϊκή Επιτροπή προάγει την Διαλειτουργικότητα και στην οδηγία 1999/93/ΕΚ, αλλά και στην οδηγία 2006/123/ΕΚ. Η διαλειτουργικότητα καλείται να επιλύσει προβλήματα που οφείλονται σε ασυμβατότητες και δυσκολίες κατά την εφαρμογή διαφορετικών πολιτικών ασφαλείας και πιστοποίησης, ρυθμίζει την εμπιστοσύνη μεταξύ των χρηστών καθορίζοντας διαφορετικά επίπεδα εμπιστοσύνης και υιοθετεί ένα μέσο μοντέλο αναφοράς για τις τεχνολογικές ασυμβατότητες.

Το 2002, στην Σύνοδο κορυφής της Σεβίλλης οι Ευρωπαίοι ηγέτες ενέκριναν το σχέδιο eEurope 2005, με σκοπό να εκδοθεί ένα συμφωνημένο πλαίσιο διαλειτουργικότητας για την παροχή πανευρωπαϊκών υπηρεσιών ηλεκτρονικής διακυβέρνησης στους πολίτες και τις επιχειρήσεις [168]. Το Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας για την Ηλεκτρονική Διακυβέρνηση (European Interoperability Framework - EIF) υποστηρίζει την στρατηγική της Ευρώπης. Στο EIF συμμετέχουν τρεις ομάδες οντοτήτων : οι ομάδες που πραγματοποιούν την ανάπτυξη και συντήρηση (κράτη μέλη, άλλοι εμπλεκόμενοι και η ομάδα διαχείρισης του έργου IDABC), η ομάδα πολιτικής στήριξης του πλαισίου (eEurope, IDABC) και η ομάδα στόχος (τα θεσμικά όργανα της Ευρωπαϊκής Ένωσης, οι διοικήσεις των κρατών μελών).

Το 2006 η Ευρωπαϊκή Επιτροπή έθεσε το στόχο της ασφαλούς διαλειτουργικής ελεγχόμενης πρόσβασης σε δημόσιες υπηρεσίες στο «Σχέδιο δράσης για τις ηλεκτρονικές διοικητικές υπηρεσίες στο πλαίσιο της πρωτοβουλίας i2010 : Επιτάχυνση της ηλεκτρονικής δημόσιας διοίκησης στην Ευρώπη προς όφελος όλων» [102]. Με το συγκεκριμένο έργο η Επιτροπή επεδίωξε την υποστήριξη μιας εθνικής κουλτούρας στις ηλεκτρονικές δημόσιες υπηρεσίες, ώστε να υποστηρίζεται η ενιαία αγορά και η συνεργασία των κρατών μελών στις ευρωπαϊκές προκλήσεις.

Σήμερα στην Ελλάδα, η διαλειτουργικότητα με βάση το ευρωπαϊκό σχέδιο δράσης 2011-2015 (ICT for Government and Public Services - Action plan 2011-2015) είναι σε πρώτη προτεραιότητα, διότι αποτελεί αναγκαία συνθήκη για την υλοποίηση διασυνοριακών Ηλεκτρονικών Υπηρεσιών σε Ευρωπαϊκό επίπεδο [167].

Συμπερασματικά

Η δυνατότητα ανταλλαγής πληροφοριών μεταξύ διαφορετικών πληροφοριακών συστημάτων επιλύει πολλά προβλήματα. Η ηλεκτρονική κάρτα που είναι ένα «χρήσιμο εισιτήριο» στο κόσμο της ηλεκτρονικής εποχής αποκτά την μέγιστη ισχύ όταν υποστηρίζεται η Διαλειτουργικότητα όταν δηλαδή μπορεί να αναγνωστεί με την συγκατάθεση του ιδιοκτήτη της από πολλά διαφορετικά συστήματα. Ένας πολίτης κουβαλώντας το «ίδιο εισιτήριο» μπορεί να «ταξιδεύει» σε πολλές υπηρεσίες. Όταν οι υπηρεσίες ανταλλάσσουν σε τοπικό, εθνικό, αλλά και ευρωπαϊκό επίπεδο, τότε το «χρήσιμο εισιτήριο» του πολίτη προάγεται σε «πολύτιμο».

4.4 Η Ηλεκτρονική Διακυβέρνηση στην Ευρώπη

4.4.1. Στρατηγικές Ταυτοποίησης σε περιβάλλοντα ΗΔ

Τα περισσότερα κράτη μέλη της Ευρωπαϊκής Ένωσης στρέφονται στην χάραξη στρατηγικών που θα ωφελήσουν το σύνολο των πολιτών, των επιχειρήσεων και τις ίδιες τις κυβερνήσεις. Οι κυβερνήσεις πρέπει να καθορίσουν στρατηγικές ισχυρής ηλεκτρονικής πιστοποίησης, να ενισχύσουν την ανάπτυξη νέων ψηφιακών υπηρεσιών σε δημόσιο και ιδιωτικό φορέα μειώνοντας το κόστος και αυξάνοντας την παραγωγικότητά τους. Σημαντικός παράγοντας για να υλοποιηθούν οι προαναφερθέντες στόχοι είναι η ενδυνάμωση της εμπιστοσύνης της ταυτότητας όλων των συμμετεχόντων [196].

Οι κυβερνήσεις είναι υπεύθυνες για την βελτίωση της διαχείρισης ψηφιακής ταυτότητας στην οικονομία του Διαδικτύου και υιοθετούν την ηλεκτρονική διακυβέρνηση. Ωστόσο, η υιοθέτηση της ηλεκτρονικής διακυβέρνησης και η χάραξη των στρατηγικών δεν είναι αρκετή. Πρέπει να διασφαλίζεται η ασφάλεια και η χρηστικότητα των υπηρεσιών, ώστε να οδηγούνται σε ισχυρές ταυτότητες, χωρίς όμως τον βομβαρδισμό πιστοποιητικών ανά χρήστη και υπηρεσία. Ως αποτέλεσμα, τα κράτη στρέφονται σταδιακά στην υποστήριξη ενιαίων λύσεων (τεχνολογιών sign on), όπου οι χρήστες του Διαδικτύου θα έχουν πρόσβαση στις ψηφιακές υπηρεσίες με τον ελάχιστο αριθμό διαπιστευτηρίων.

Αναφορικά με τις υφιστάμενες στρατηγικές ταυτοτήτων ακολουθείται μια εξελικτική προσέγγιση : το Μητρώο καταγραφής πληθυσμού κάθε χώρας αποτελεί τη βάση σχεδιασμού του συστήματος διαχείρισης ηλεκτρονικών ταυτοτήτων. Με τον τρόπο αυτό, δεν απορρίπτονται οι υφιστάμενες πρακτικές των ταυτοτήτων, αλλά προσαρμόζονται στις ψηφιακές διαδικασίες, σεβόμενες την πολιτισμική ταυτότητα και κουλτούρα του εκάστοτε κράτους.

Στην προσπάθεια θέσπισης κανόνων ορθών στρατηγικών προσεγγίσεων πρέπει να λαμβάνονται υπόψη:

- i. Η αναγνώριση των ιδιαιτεροτήτων κάθε χώρας
- ii. Η μετάπτωση των υφιστάμενων μη ηλεκτρονικών υπηρεσιών, παραδόσεων και διαδικασιών στις οποίες εμπλέκονται οι πολίτες σε ηλεκτρονικές
- iii. Η βελτιστοποίηση της χρηστικότητας των υπηρεσιών από τους υφιστάμενους χρήστες
- iv. Το χρονικό περιθώριο που απαιτείται για την υποστήριξη του συστήματος ηλεκτρονικών ταυτοτήτων εξαρτάται από τον βαθμό προϋπάρχουσας υποδομής πλαισίου ταυτοποίησης (υπάρχουν κράτη που δεν έχουν καμία υποδομή).

4.4.2. Πολιτικές Ταυτοποίησης σε περιβάλλοντα ΗΔ

Για την ανάπτυξη και υποστήριξη μιας εθνικής στρατηγικής για την διαχείριση ηλεκτρονικής ταυτότητας απαιτείται μεγάλο χρονικό διάστημα και η υλοποίησή του δεν θεωρείται απλή διαδικασία. Οι πολιτικές ταυτοποίησης των κρατών για την διαχείριση ηλεκτρονικής ταυτότητας διακρίνονται σε κεντρικές ή αποκεντρωμένες. Σε όσες χώρες παρατηρείται μικρή στρωματοποίηση της δημόσιας διοίκησης είναι πιο εύκολη η υποστήριξη μιας συγκεντρωτικής πολιτικής. Αντίθετα, όσες χώρες υποστηρίζουν αυτόνομες τοπικές διοικήσεις ακολουθούν αποκεντρωμένες πολιτικές. Ο διαχωρισμός οφείλεται στην εξελικτική προσέγγιση των στρατηγικών που σχετίζεται άμεσα με την κουλτούρα, την ιστορία και τον πολιτισμό των χωρών.

Οι πολιτικές ταυτοποίησης διαφοροποιούνται ανάλογα με τον τρόπο αντιμετώπισης των εθνικών προκλήσεων που σχετίζονται με την ασφάλεια, την διαλειτουργικότητα, την ιδιωτικότητα και την χρηστικότητα. Για παράδειγμα, εάν πρέπει να πραγματοποιηθεί μια συνταγογράφηση σε ένα αποκεντρωμένο σύστημα διαχείρισης ταυτοτήτων, αυτή προωθείται στο πλαίσιο της συμφωνίας των ομοσπονδιών και επιτυγχάνεται η μέγιστη ευελιξία. Στην περίπτωση κεντρικοποιημένης πολιτικής ακολουθείται μια λιγότερο ευέλικτη λύση λόγω των πολιτικών και τεχνικών επιλογών.

Κατά αντίστοιχο τρόπο λαμβάνονται αποφάσεις σχετικά με την Ιδιωτικότητα. Στις κεντρικές πολιτικές ταυτοποίησης υπάρχουν ζητήματα σχετικά με την ύπαρξη ενός κεντρικού μητρώου, μοναδικών χαρακτηριστικών και των εθνικών δελτίων ταυτότητας. Στις αποκεντρωμένες πολιτικές, τα μέτρα προστασίας της ιδιωτικής ζωής εξαρτώνται από τις συμφωνίες της εμπιστοσύνης μεταξύ των διαφόρων συμμετεχόντων στην ομοσπονδία, εμποδίζοντας την εφαρμογή μιας ενιαίας τεχνικής λύσης.

4.4.3. Πύλες Ηλεκτρονικής Διακυβέρνησης

Τα κράτη μέλη της Ευρωπαϊκής Ένωσης έχουν αναπτύξει πληροφοριακά συστήματα για τις υπηρεσίες Ηλεκτρονικής Διακυβέρνησης. Τα συστήματα, γνωστά και ως Πύλες (portals), είναι προσβάσιμα στους πολίτες μέσω ηλεκτρονικών σελίδων. Στον πίνακα 4.2 περιλαμβάνονται κυβερνητικές δικτυακές πύλες της Δημόσιας Διοίκησης για τα 28 κράτη μέλη της Ευρωπαϊκής Ένωσης.

A/α	Κράτος Μέλος	Ηλεκτρονική Πύλη
1	Αυστρία	https://www.he1p.gv.at/Porta1.Node/h1pd/pub1ic http://www.bundeskanz1eramt.at www.digitales.oesterreich.gv.at

2	Βέλγιο	http://www.be1gium.be/en
3	Βουλγαρία	http://www.esmis.government.bg/en
4	Γαλλία	http://www.service-public.fr/
5	Γερμανία	www.bund.de
6	Δανία	https://www.sundhed.dk/service/english/
7	Ελλάδα	http://www.ermis.gov.gr/porta1/page/porta1/ermis/
8	Εσθονία	https://www.eesti.ee/en
9	Ηνωμένο Βασίλειο	www.gov.uk
10	Ιρλανδία	http://www.basis.ie/home/home.jsp?pcategorv=10055&ec ategorv=10055&1anguage=EN http://www.gov.ie/
11	Ισπανία	http://www.060.es/060 Home/ServiciosLinea.html
12	Ιταλία	http://www.esteri.it/MAE/EN/ComeFarePer/servizi_egov_attivita.htm http://www.italia.gov.it/
13	Κροατία	http://www.vlada.hr/en/adresar_i_linkovi/javni_sektor
14	Κύπρος	http://www.cvprus.gov.cy/porta1/porta1.nsf/citizen_gr?OpenForm&access=0&SectionId=citizen&CategoryId=none&SectionId=home&print=0&lang=el
15	Λετονία	https://www.1atvija.lv/
Πίνακας 4.2: Ηλεκτρονικές Πύλες κρατών μελών Ευρωπαϊκής Ένωσης κατά αλφαβητική σειρά		
4.4.4 Ευρωπαϊκή Εξέλιξη Ηλεκτρονικής Διακυβέρνησης		

16	Λιθουανία	http://www.vrm.lt/1it/English
17	Λουξεμβούργο	http://www.guichet.public.lu/home/fr/index.html
18	Μάλτα	http://www.gov.mt/en/Pages/gov.mt%20homepage.aspx
19	Ολλανδία	http://www.overheid.nl/
20	Ουγγαρία	https://magvarorszag.hu/
21	Πολωνία	http://www.gov.pl/ http://epuap.gov.pl/wps/porta1/E2_ZdarzeniaZvciowe
22	Πορτογαλία	http://www.portaldocidadao.pt/PORTAL/pt
23	Ρουμανία	http://www.e-guvernare.ro/Default.aspx?LangID=4
24	Σλοβακία	http://www.government.gov.sk/
25	Σλοβενία	http://e-uprava.gov.si/e-uprava/
26	Σουηδία	http://www.edelegationen.se/
27	Τσεχία	http://porta1.gov.cz/porta1/obcan
28	Φινλανδία	http://www.suomi.fi/suomifi/english/index.html

Σε αυτήν την ενότητα περιλαμβάνονται κάποια στατιστικά στοιχεία για την ανάπτυξη της Ηλεκτρονικής Διακυβέρνησης, σύμφωνα με την έκθεση των Ηνωμένων Εθνών για το 2012.

Όπως πολύ εύστοχα αναφέρεται στην εισαγωγή της έκθεσης «η Ηλεκτρονική Διακυβέρνηση μπορεί να είναι μια κινητήρια δύναμη της ανάπτυξης για το λαό. Οι δημόσιες υπηρεσίες σχεδιάζονται για να ανταποκρίνονται στις ανάγκες των πολιτών, χωρίς κοινωνικούς αποκλεισμούς και οι κυβερνήσεις πλέον επικοινωνούν με τους πολίτες μέσω συμμετοχικών διαδικασιών παροχής υπηρεσιών»[46].

Σύμφωνα με το κατάλληλο θεσμικό πλαίσιο, τις στρατηγικές και τις πολιτικές δημιουργίας υποδομών στην ηλεκτρονική διακυβέρνηση τα κράτη μπορούν να επιτύχουν σημαντική ανάπτυξη. Όμως για να επιτευχθούν τα αποτελέσματα είναι απαραίτητη η επαρκής χρηματοδότηση. Ζώντας στην εποχή της κινητής τηλεφωνίας, του υπολογιστικού νέφους (cloud computing) οι πολίτες μπορούν με την κατάλληλη υποστήριξη να αυξήσουν την προσβασιμότητά τους στις υπηρεσίες Ηλεκτρονικής Διακυβέρνησης.

Σύμφωνα με την παγκόσμια κατάταξη 2012, από τα κράτη της Ευρωπαϊκής Ένωσης η Ολλανδία κατέχει την δεύτερη θέση (0,9125), το Ηνωμένο Βασίλειο την τρίτη θέση (0,8960), η Δανία την τέταρτη θέση (0,8889) και ακολουθούν η Γαλλία στην 7^η θέση, την Νορβηγία στην 8^η θέση και η Σουηδία στην 10^η θέση. Ως πρώτο συμπέρασμα λοιπόν η Ευρώπη είναι επικεφαλής στην κατάταξη για την ανάπτυξη Ηλεκτρονικής Διακυβέρνησης (ανεξαρτήτως του γεγονότος ότι η Νορβηγία δεν είναι μέλος της

Ευρωπαϊκής Ένωσης). Το γεγονός αυτό οφείλεται στο υψηλό επίπεδο εκπαίδευσης των πολιτών, καθώς και στις υποδομές τηλεφωνίας.

Η έρευνα διαπιστώνει ότι πολλά κράτη μέλη κινούνται από ένα αποκεντρωμένο μοντέλο προς σε ένα ολοκληρωμένο ενοποιημένο προκειμένου να αυξηθεί η αποδοτικότητα και η αποτελεσματικότητα των υπηρεσιών Ηλεκτρονικής Διακυβέρνησης. Το ενοποιημένο μοντέλο επιχειρεί την πρόσβαση των υπηρεσιών μέσα από μια ενιαία πύλη, από την οποία οι πολίτες θα αποκτούν πρόσβαση σε όλες τις κυβερνητικά παρεχόμενες υπηρεσίες, ανεξάρτητα από το ποια κυβερνητική εξουσία τις παρέχει. Όπως καταλήγει η έκθεση, η συγκέντρωση αυτή συντελεί σε ένα σύστημα διακυβέρνησης με διαφάνεια και ευελιξία.

Στον πίνακα 4.3 παρουσιάζεται η κατάταξη των δέκα καλύτερων ευρωπαϊκών χωρών σύμφωνα με τον δείκτη ανάπτυξης Ηλεκτρονικής διακυβέρνησης και οι αντίστοιχες βαθμολογήσεις των κρατών βάσει της έκθεσης που συντάχθηκε το 2010.

Κατάταξη	Κράτος Μέλος	Δείκτης Ανάπτυξης eGov		Παγκόσμια Κατάταξη βάσει Δείκτη Ανάπτυξης	
		2012	2010	2012	2010
1	Ολλανδία	0.9125	0.8097	2	5
2	Ηνωμένο Βασίλειο	0.8960	0.8147	3	4
3	Δανία	0.8889	0.7872	4	7
4	Γαλλία	0.8635	0.7510	6	10
5	Σουηδία	0.8599	0.7474	7	12
6	Νορβηγία	0.8593	0.8020	8	6
7	Φινλανδία	0.8505	0.6967	9	19
8	Λιχτενστάιν	0.8264	0.6694	14	23
9	Ελβετία	0.8134	0.7136	15	18
10	Γερμανία	0.8079	0.7309	17	16
Μέσος όρος περιοχής		0.7188	0.6227		
Παγκόσμιος μέσος όρος		0.4882	0.4406		

Πίνακας 4.3: Κατάταξη 10 καλύτερων ευρωπαϊκών χωρών βάσει του δείκτη ανάπτυξης e-gov

Οι περισσότερες χώρες της Ευρωπαϊκής Ένωσης (ΕΕ) ακολουθούν την προσέγγιση των ξεχωριστών πυλών για την παροχή των υπηρεσιών τους. Σε αρκετές ευρωπαϊκές χώρες, οι υπηρεσίες ηλεκτρονικής διακυβέρνησης επικεντρώνονται σε ένα σημείο πρόσβασης για την παροχή 20 βασικών ηλεκτρονικών υπηρεσιών που είναι απαραίτητες για τους πολίτες τους.

Σύμφωνα με μια άλλη κατάταξη για τους αναδυόμενους ηγέτες Ηλεκτρονικής διακυβέρνησης για την Ευρώπη, οι υψηλότεροι δείκτες τους επιτυγχάνονται από τις χώρες της Αυστρίας (0.7840), Ισλανδίας (0.7835), Ισπανίας (0.7770) και του Βελγίου (0.7718).

Κεφάλαιο 5

Πολιτικές Αυθεντικοποίησης

Πολιτών

Στο κεφάλαιο 2 αναφέρθηκαν τα μέσα ταυτοποίησης που διατηρούν στα είκοσι οκτώ (28) κράτη μέλη της Ευρωπαϊκής Ένωσης. Στο κεφάλαιο 3 έγινε μια παράθεση των οδηγιών που αφορούν στοιχεία που αφορούν την ταυτοποίηση των πολιτών, καθώς και τις υπηρεσίες που παρέχονται, ενώ στο κεφάλαιο 4 αναλύθηκαν τα χαρακτηριστικά της Ηλεκτρονικής Διακυβέρνησης.

Στο κεφάλαιο 5 αναλύεται η έννοια της Αυθεντικοποίησης, η σύνδεσή της με τα προαναφερόμενα και παρατίθενται σχόλια για τις υπάρχουσες ευρωπαϊκές πολιτικές, είτε διακριτικών αυθεντικοποίησης, είτε αναγνωριστικών υποδομής δημοσίου κλειδιού. Σε ξεχωριστή παράγραφο του κεφαλαίου γίνεται αναφορά στην ασφάλεια των πολιτικών αυθεντικοποίησης.

5.1 Αυθεντικοποίηση

Σύμφωνα με τον πρότυπο ISO 27000:2009, η Αυθεντικοποίηση ορίζεται ως η «παροχή διασφάλισης ότι το χαρακτηριστικό που ισχυρίζεται ότι διαθέτει μία οντότητα, είναι ορθό» [66]. Ένας δεύτερος ορισμός για την Αυθεντικοποίηση, σύμφωνα με τον N. 3979/2011 αναφέρει ότι: ««Επιβεβαίωση ταυτότητας (Αυθεντικοποίηση) καλείται η διαδικασία πιστοποίησης και επιβεβαίωσης της ταυτότητας των φυσικών και νομικών προσώπων, τα οποία είναι χρήστες υπηρεσιών ηλεκτρονικής διακυβέρνησης και επικοινωνούν - συναλλάσσονται με φορείς του δημόσιου τομέα με χρήση ΤΠΕ, που βασίζεται στα διαπιστευτήρια που κατέχουν και με την οποία αναγνωρίζεται και επιβεβαιώνεται η ορθότητα της ταυτότητας ενός προσώπου».

Στο σημείο αυτό πρέπει να αναφερθεί η σχέση ταυτοποίησης και αυθεντικοποίησης. Στην ενότητα 2.2.2 αναφέρθηκαν τα μοναδικά χαρακτηριστικά των πολιτών. Με την αυθεντικοποίηση επιτυγχάνεται η επαλήθευση της ταυτότητας (π.χ. μοναδικού αναγνωριστικού) από το σύστημα διαχείρισης ηλεκτρονικών υπηρεσιών, δηλαδή επιβεβαιώνεται ότι ο πολίτης είναι πραγματικά αυτός που ισχυρίζεται ότι είναι. Η αυθεντικοποίηση έχει διττή σημασία : χρειάζεται για να μπορεί τελικά ένας πολίτης να προσπελάσει τις υπηρεσίες ηλεκτρονικής διακυβέρνησης, αλλά και να καταγραφεί ότι η υπηρεσία παρασχέθηκε στον πολίτη.

Η αυθεντικοποίηση ενός χρήστη μπορεί να επιτευχθεί είτε με:

- S Κάτι που γνωρίζει (πχ. ένα συνθηματικό)
- S Κάτι που κατέχει (πχ. ψηφιακό πιστοποιητικό)
- S Κάτι που τον χαρακτηρίζει με βάση μονοσήμαντα βιομετρικά χαρακτηριστικά του (πχ. δακτυλικά αποτυπώματα, ίριδα ματιού)
- S Είτε με συνδυασμό των προηγούμενων τριών στοιχείων [73]

Στην μελέτη «Mapping security services to authentication levels, Reflecting on STORK QAA 1eve1s» του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών (εφεξής ENISA) [10] αναφέρεται πολύ εύστοχα ότι, παρόλο που τα μέλη της Ευρωπαϊκής Ένωσης υποστηρίζουν τα συστήματα ηλεκτρονικής ταυτοποίησης με την δημιουργία ετερογενών συστημάτων και παρά την προτυποποίηση της βιομηχανίας έξυπνων καρτών (βάσει του προτύπου CEN EN/TS 15480 [14] για μια πανευρωπαϊκή κάρτα) από την Ευρωπαϊκή Επιτροπή Προτυποποίησης (European

Committee for Standardization) για λόγους ορθότερης αντίληψης συνίσταται πριν την παρουσίαση των μηχανισμών αυθεντικοποίησης να γίνει αναφορά των επιπέδων αυθεντικοποίησης που πρέπει να υποστηρίζονται από κάθε υπηρεσία ηλεκτρονικής διακυβέρνησης. Στην συνέχεια θα αναφερθούν οι

πολιτικές αυθεντικοποίησης που χρησιμοποιούνται, δηλαδή η πολιτική χρήσης διακριτικών και υποδομή δημοσίου κλειδιού.

5.2 Ασφάλεια Αυθεντικοποίησης

Η ασφάλεια της αυθεντικοποίησης ενός πολίτη προϋποθέτει την ενημέρωση του πολίτη για τις πληροφορίες που παρέχει σε μια υπηρεσία προκειμένου να αυθεντικοποιηθεί (επίπεδο εγγραφής), καθώς επίσης και το επίπεδο εμπιστοσύνης που εντάσσεται η παρεχόμενη υπηρεσία. Στην ενότητα αυτή περιλαμβάνονται τα επίπεδα εγγραφής, τα επίπεδα εμπιστοσύνης, καθώς και τα επίπεδα διασφάλισης αυθεντικοποίησης (STORK Quality Assurance Authentication -QAA) βάσει του έργου STORK. Τα επίπεδα αυθεντικοποίησης καθορίζονται σύμφωνα με τα επίπεδα εμπιστοσύνης των υπηρεσιών. Υψηλό επίπεδο εμπιστοσύνης συνεπάγεται απαίτηση περισσότερων εγγυήσεων ταυτοποίησης από πλευράς παρόχου υπηρεσιών μεγαλύτερη εμπιστοσύνη στην δηλούμενη ταυτότητα του πολίτη, προκειμένου να συμμετάσχουν σε μια συναλλαγή.

Ένα άλλο σημαντικό ζήτημα που λαμβάνεται υπόψη στα επίπεδα αυθεντικοποίησης είναι οι απαιτήσεις ασφαλείας που πρέπει να υποστηρίζονται κατά την πρόσβαση σε ηλεκτρονικές υπηρεσίες. Μάλιστα, στην έκθεση για τα «θέματα ασφαλείας της διασυνοριακής αυθεντικοποίησης» του ENISA [178] αναλύονται διεξοδικά οι βασικές αρχές ασφαλείας κατά ISO 27002 (Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα, Μη αποποίηση ευθύνης) και γίνεται μια κατηγοριοποίηση των απαιτήσεων προστασίας για την διασυνοριακή αυθεντικοποίηση.

Το κύριο στοιχείο της μελέτης έγκειται στο γεγονός της διεξοδικής εξέτασης όλων των αρχών ασφαλείας για τα προσωπικά δεδομένα των πολιτών (Personal data), για τα δεδομένα εφαρμογής (Application data), για το «token» του πολίτη (το Token περιλαμβάνει προσωπικά δεδομένα, αλλά και δεδομένα εφαρμογής), την Αρχή πιστοποίησης (ID authority), τον διαχειριστή συστήματος (System operator), τον παροχέα της υπηρεσίας (User service provider), τον διασυνοριακό προσαρμογέα (Cross-border adapter), τον προσαρμογέα Token (Token adapter) και την διεπαφή χρήστη (User interface).

Στην έκθεση για την αντιστοίχιση των υπηρεσιών σε επίπεδα αυθεντικοποίησης του έργου STORK [173] αναφέρεται ότι «Κάθε μεμονωμένο μέτρο ασφαλείας υψηλής ποιότητας έχει μικρή χρησιμότητα, εκτός αν περιβάλλεται από εξίσου αποτελεσματικά μέτρα». Τα μέτρα πρέπει να λαμβάνουν υπ' όψιν τους όλα τα αλληλεπιδρώντα στοιχεία (υπηρεσίες, πολίτες) ώστε η διασφάλιση της αξίας ενός μέτρου να μην μειώνει την αξία του άλλου.

Για την αυθεντικοποίηση ενός πολίτη προαπαιτείται ο καθορισμός του επιπέδου εμπιστοσύνης για την ηλεκτρονική υπηρεσία στην οποία θα αυθεντικοποιηθεί. Οι φορείς υπηρεσιών πρέπει να καθορίσουν τις πληροφορίες που απαιτούν από τους πολίτες και να τις εντάξουν σε μια κατηγορία, το λεγόμενο επίπεδο εμπιστοσύνης. Ακολουθούν οι ορισμοί των επιπέδων εμπιστοσύνης, αυθεντικοποίησης και εγγραφής που καθορίζονται σύμφωνα με το Ελληνικό Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης και Ψηφιακής Αυθεντικοποίησης [154].

5.2.1 Επίπεδο εμπιστοσύνης

Ως επίπεδο εμπιστοσύνης καθορίζεται ο «*Βαθμός βεβαιότητας στην αξιοπιστία, εντιμότητα, αξία ή ικανότητα κάποιας οντότητας*». Στον πίνακα 5.1 περιλαμβάνονται τα επίπεδα εμπιστοσύνης με τα χαρακτηριστικά τους.

Κωδικός Επιπέδου Εμπιστοσύνης	Χαρακτηριστικά Επιπέδου Εμπιστοσύνης
EEM0	<ul style="list-style-type: none"> ■ S Αξιοποίηση δημόσιων προσπελάσιμων πληροφοριών, αρκεί η υπηρεσία να είναι διαθέσιμη ■ S Δεν απαιτείται προγενέστερη ανταλλαγή πληροφοριών ■ S Δεν προκύπτουν επιπτώσεις για τους πολίτες
EEM1	<p>S Ανταλλαγή πληροφοριών μικρής κρίσιμότητας (ονοματεπώνυμο, ηλεκτρονική διεύθυνση)</p> <p>S Απαιτείται μικρός βαθμός βεβαιότητας για την</p>

	ηλεκτρονική οντότητα του πολίτη ■S Επιπτώσεις δευτερεύουσας σημασίας για τους πολίτες ■S Συστήνονται μέτρα προστασίας πολιτών
EEM2	S Ανταλλαγή μη ευαίσθητων δεδομένων (ημερομηνία γέννησης, οικογενειακή κατάσταση, φύλο) ■S Απαιτείται μέτριος βαθμός βεβαιότητας για την ηλεκτρονική οντότητα του πολίτη (καθορισμός εξουσιοδότησης) ■S Επιθέσεις προβολής στοιχείων σε μη εξουσιοδοτημένα πρόσωπα
EEM3	S Ανταλλαγή ευαίσθητων δεδομένων (ποινικό μητρώο), ή οικονομικών δεδομένων ■S Απαιτείται υψηλός βαθμός εμπιστοσύνης για την ηλεκτρονική οντότητα του πολίτη ■S Σοβαρές επιπτώσεις στους πολίτες

Πίνακας 5.1: Χαρακτηριστικά επιπέδων εμπιστοσύνης Ελληνικού Πλαισίου Αυθεντικοποίησης

5.2.2 Επίπεδο αυθεντικοποίησης

Ως επίπεδο αυθεντικοποίησης καθορίζεται η «Ένταξη σε συγκεκριμένου τύπου διαπιστευτήρια για την τεκμηρίωση της εγκυρότητας της ταυτότητας μιας οντότητας». Στον πίνακα 5.2 αποτυπώνονται οι απαιτήσεις ασφάλειας που πρέπει να πληρούνται για τα τρία επίπεδα αυθεντικοποίησης, σε σχέση με τα επίπεδα εμπιστοσύνης. Όπως προαναφέρθηκε, για την πρόσβαση σε υπηρεσία υψηλού επιπέδου εμπιστοσύνης απαιτείται ισχυρότερος μηχανισμός αυθεντικοποίησης [158].

Κωδικός Επιπέδου Αυθεντικοποίησης	Επίπεδο EEM	Απαιτήσεις Ασφάλειας Επιπέδου Αυθεντικοποίησης
ΕΑ0	EEM0	<p>S Ακεραιότητα παρεχόμενων πληροφοριών</p> <p>S Αυθεντικότητα Υπηρεσίας</p> <p>■S Δεν απαιτούνται μηχανισμοί αυθεντικοποίησης</p>
ΕΑ1	EEM1 EEM2	<p>■S Εμπιστευτικότητα των αναγνωριστικών και διαπιστευτηρίων χρήστη</p> <p>■S Ακεραιότητα αναγνωριστικών, διαπιστευτηρίων χρήστη</p> <p>S Ακεραιότητα δεδομένων λήψης</p> <p>S Αυθεντικότητα Υπηρεσίας</p>
ΕΑ2	EEM3	<p>■S Εμπιστευτικότητα των αναγνωριστικών και διαπιστευτηρίων χρήστη, των δεδομένων αποστολής και λήψης</p> <p>■S Ακεραιότητα αναγνωριστικών, διαπιστευτηρίων χρήστη, των δεδομένων αποστολής και λήψης</p> <p>S Ακεραιότητα δεδομένων λήψης</p> <p>S Μη αποποίηση αποστολής και λήψης δεδομένων</p> <p>S Καταγραφή και Χρονοσήμανση</p>

Πίνακας 5.2: Απαιτήσεις Ασφαλείας Επιπέδων Αυθεντικοποίησης

Οι πολιτικές αυθεντικοποίησης που προτείνονται για τις υπηρεσίες που εντάσσονται στο επίπεδο εμπιστοσύνης 1 είναι τα συνθηματικά και τα συνθηματικά μιας χρήσης.

Η πολιτική αυθεντικοποίησης που προτείνεται για τις υπηρεσίες που εντάσσονται στο επίπεδο αυθεντικοποίησης 2 είναι τα ψηφιακά πιστοποιητικά.

5.2.3 Επίπεδο εγγραφής

Ως επίπεδο εγγραφής καθορίζεται η «ένταξη σε συγκεκριμένο σύνολο διαδικασιών που ακολουθούνται για τη συλλογή των απαιτούμενων στοιχείων και την πιστοποίηση της ορθότητας».

Βασικός πυλώνας για τον καθορισμό των επιπέδων εγγραφής είναι το επίπεδο εμπιστοσύνης που

Κωδικός Επιπέδου Εγγραφής	Επίπεδο ΕΑ	Απαιτήσεις Ασφάλειας Πολίτη	Απαιτήσεις Ασφάλειας Υπηρεσίας Εγγραφής
ΕΕ0	ΕΑ0		
ΕΕ1	ΕΑ1	·/Εμπιστευτικότητα & Ακεραιότητα δεδομένων αποστολής και διαπιστευτηρίων χρήστη S Μη αποποίηση αποστολής - λήψης δεδομένων	■S Εμπιστευτικότητα και δεδομένων αποστολής Ακεραιότητα δεδομένων αποστολής
ΕΕ2	ΕΑ1	S Όμοια με ΕΕ1 S Μη αποποίηση συμμετοχής	Όμοια με ΕΕ1
ΕΕ3	ΕΑ2	S Όμοια με ΕΕ2	Όμοια με ΕΕ1

Πίνακας 5.3: Απαιτήσεις Πολιτών και Υπηρεσιών ανά Επίπεδο Εγγραφής [154,158]

εντάσσεται η κάθε υπηρεσία, ώστε ο πολίτης να προβεί σε εγγραφή.

Στον πίνακα 5.3 αναφέρονται τα επίπεδα εγγραφής, η αντιστοίχιση τους με τα επίπεδα αυθεντικοποίησης και οι απαιτήσεις ασφαλείας των πολιτών και της υπηρεσίας εγγραφής. Όμοια με τα προηγούμενα, ισχύει ο κανόνας ότι στοχεύοντας σε υπηρεσίες υψηλών επιπέδων εμπιστοσύνης απαιτείται μεγαλύτερο επίπεδο εγγραφής. Για την εγγραφή σε ένα επίπεδο εγγραφής πρέπει να ακολουθούνται οι διαδικασίες που ορίζει το επίπεδο αυθεντικοποίησης.

Παρατηρώντας τον πίνακα 5.3, στο επίπεδο εγγραφής 2, καθώς και στο επίπεδο εγγραφής 3 επαναλαμβάνονται οι απαιτήσεις ασφαλείας του επιπέδου 1. Στην πράξη παρουσιάζονται διαφοροποιήσεις ως προς τα επίπεδα εγγραφής 2 και 3 στο γεγονός της αυθεντικοποίησης του χρήστη. Κατά το επίπεδο εγγραφής 2 ο πολίτης ταυτοποιείται αυτοπροσώπως σε υπάλληλο της υπηρεσίας εγγραφής ώστε να παραλάβει το διακριτικό αυθεντικοποίησης, ενώ στο επίπεδο εγγραφής 3 ακολουθείται η ίδια διαδικασία ταυτοποίησης αλλά ο προσωπικός αριθμός αποστέλλεται ταχυδρομικά στον πολίτη [158].

5.3 Διακριτικά Αυθεντικοποίησης

Για την επαλήθευση της ψηφιακής ταυτότητας ενός χρήστη χρησιμοποιούνται διάφορα διακριτικά αυθεντικοποίησης σύμφωνα με το επίπεδο αυθεντικοποίησης της υπηρεσίας. Όπως αναφέρθηκε στην ενότητα 5.1, η αυθεντικοποίηση ενός χρήστη μπορεί να πραγματοποιηθεί είτε με κάποιο χαρακτηριστικό ιδιοκτησίας, είτε με κάποιο χαρακτηριστικό γνώσης, είτε με κάποιο βιομετρικό χαρακτηριστικό. Ανάλογα με τον αριθμό χαρακτηριστικών που αξιοποιούνται χαρακτηρίζονται ως μονοδιάστατα ή πολυδιάστατα και η πολυπλοκότητα των χαρακτηριστικών εξαρτάται από το επίπεδο εμπιστοσύνης της υπηρεσίας [158]. Για παράδειγμα, όταν ένας χρήστης χρησιμοποιεί δύο χαρακτηριστικά τότε συναντάται ο όρος two-factor [62].

Το κύριο διακριτικό αυθεντικοποίησης με το οποίο αυθεντικοποιούνται οι χρήστες και στο οποίο στηρίζεται πληθώρα διακριτικών είναι το συνθηματικό. Το συνθηματικό (password) αποτελεί μια τεχνική αυθεντικοποίησης και αναφέρεται στην εμπιστευτική συμβολοσειρά που χρησιμοποιείται για τον έλεγχο της αυθεντικότητας του χρήστη. Η χρήση των συνθηματικών είναι απαραίτητη για να προβληθεί ένα «εμπόδιο» σε οποιοδήποτε κακόβουλο χρήστη προσπαθήσει να υποκλέψει τις πληροφορίες ενός οργανισμού [157]. Συνήθως τα συνθηματικά απαντώνται σε υπηρεσίες με χαμηλό επίπεδο εμπιστοσύνης. Τα συνθηματικά ανάλογα με την διάρκεια ζωής τους και την χρήση τους συναντώνται με διάφορες ονόμασες. Τα συνήθη συνθηματικά μπορούν να χρησιμοποιούνται από τους χρήστες για ακαθόριστη χρονική διάρκεια, εκτός και αν επιβάλλεται αλλαγή τους βάσει πολιτικής χρόνου ωρίμανσης συνθηματικού από την αντίστοιχη υπηρεσία που χρησιμοποιείται. Μια άλλη μορφή συνθηματικών είναι

τα λεγόμενα συνθηματικά μιας χρήσης, που παράγονται τυχαία από ειδικές συσκευές και ισχύουν για μία και μόνη χρήση. Οι συσκευές αυτές είναι ιδιαίτερα διαδεδομένες στα τραπεζικά συστήματα για ηλεκτρονικές οικονομικές συναλλαγές.

Στον πίνακα 5.4 αναφέρονται τα υφιστάμενα διακριτικά αυθεντικοποίησης και η κατηγοριοποίηση τους. Στον πίνακα περιλαμβάνονται τα διακριτικά που υφίστανται ανεξαρτήτως αν αυτή την στιγμή υποστηρίζεται το σύνολο τους από τα συστήματα ηλεκτρονικής ταυτοποίησης. Τα τελευταία χρόνια η αγορά έχει κατακλυστεί με έξυπνα τηλέφωνα, γεγονός που καθοδηγεί τα συστήματα αυθεντικοποίησης προς τα εκεί. Στις περισσότερες περιπτώσεις τα διακριτικά αυθεντικοποίησης συνδυάζουν δύο χαρακτηριστικά, γεγονός που υποδηλώνει υψηλότερο επίπεδο εμπιστοσύνης.

Διακριτικό Αυθεντικοποίησης	Χαράκτη ρι στικό	Χαράκτη ριστικό! Διακριτικού
Συνθηματικό	Γνώσης	Μια εμπιστευτική συμβολοσειρά
PIN (Personal identification number)	Γνώσης	Προσωπικός αριθμός για συναλλαγές σε ATM τραπεζών
Pattern	Γνώσης	Μια ακολουθία κελιών για συσκευές Android.
Συνθηματικό μιας χρήσης (One-time pads)	Γνώσης	Μια τυχαία ακολουθία που παράγεται από ειδικές συσκευές και ισχύει για μία και μόνη χρήση
Συνθηματικά οθόνης (disconnected tokens)	Ιδιοκτησίας	Συσκευές LCD που παράγουν αριθμούς μιας χρήσης για την αυθεντικοποίηση σε ηλεκτρονικές συναλλαγές. Ο αριθμός παράγεται είτε με την χρήση ενός κουμπιού
		(sequence-based), είτε με το πέρας ενός καθορισμένου χρονικού διαστήματος (time-based).
Connected tokens	Ιδιοκτησίας Γνώσης	Συσκευές με λειτουργία αντίστοιχη των disconnected tokens με την διαφορά ότι διατηρούν μια θύρα υποδοχής για σύνδεση και χρησιμοποιείται ένα μυστικό κλειδί.
Μαγνητικές κάρτες	Ιδιοκτησίας Βιομετρικό	Κάρτα που αναγνωρίζει το αποτύπωμα του χρήστη και παράγει ένα δυναμικό ψηφιακό αναγνωριστικό.

Έξυπνες κάρτες	Ιδιοκτησίας (Βιομετρικό)	<p>S Επαφική έξυπνη κάρτα S Ανέπαφη κάρτα με ενσωμάτωση RFID</p> <p>■S Και οι δυο υποστηρίζουν πιστοποιητικό X.509</p>
Ασύρματα	Ιδιοκτησίας	<p>S Βασισμένα σε RFID S Βασισμένα σε Bluetooth</p> <p>■S Βασισμένα σε ανέπαφες έξυπνες κάρτες</p>
USB tokens	Ιδιοκτησίας Γνώσης	Χρησιμοποιείται πρωτόκολλο ερώτησης / απόκρισης (challenge/response)
Audio Port tokens	Ιδιοκτησίας	Συσκευές micro usb, mini usb, iDock (ενσωματώνει ψηφιακά πιστοποιητικά).
Διακριτικά χαλαρής αποθήκευσης (Soft	Ιδιοκτησίας	Χρήση μυστικού κλειδιού που περιλαμβάνει

tokens)	Γνώσης	πιστοποιητικό SSL
SMS one time password	Ιδιοκτησίας Γνώσης	Χρήση ενός PIN μέσω μηνύματος κινητής τηλεφωνίας
Smartphone Push	Ιδιοκτησίας Γνώσης	Χρήση μηχανισμού πρόκλησης/απάντησης τεχνολογιών Android APNs iPhone και Android C2DM/GCM
Additional phone token	Ιδιοκτησίας Γνώσης	Το κινητό τηλέφωνο περιλαμβάνει το διακριτικό ασφαλείας (Java ME client.), αλλά έχει και το ρόλο Επεξεργαστή
Υπογραφή μέσω κινητού (mobile signature)	Ιδιοκτησίας Γνώσης	Δημιουργία υπογραφής στη κάρτα SIM με τη χρήση μυστικού κλειδιού
Εφαρμογές μέσω κινητού (mobile applications)	Ιδιοκτησίας Γνώσης	Χρήση κρυπτογραφικών μηχανισμών

Πίνακας 5.4: Διακριτικά Αυθεντικοποίησης Χρηστών

Σύμφωνα με την έκθεση «Ηλεκτρονική Ταυτότητα πολιτών και επιλογές πολιτικής και υποδομών - Ευρωπαϊκή εμπειρία» του Παρατηρητηρίου της Κοινωνίας της Πληροφορίας για το 2010 [75], τα κράτη μέλη της Ευρωπαϊκής Ένωσης χρησιμοποιούν συστήματα αυθεντικοποίησης που στηρίζονται σε πολιτικές χρήσης συνθηματικών μιας χρήσης, two-factor [58] και συνθηματικά οθόνης «time based». Οι 15 χώρες σε σύνολο 19 κρατών μελών χρησιμοποιούν μονοδιάστατα συστήματα, ενώ το Βέλγιο, η Εσθονία, η Λιθουανία και η Φινλανδία χρησιμοποιούν πολυδιάστατα συστήματα.

5.4 Υποδομή Δημοσίου Κλειδιού

Μια ισχυρή πολιτική αυθεντικοποίησης είναι η χρήση συστημάτων που βασίζονται στην Υποδομή Δημοσίου Κλειδιού (Public Key Infrastructure - PKI). Μελετώντας το κείμενο της οδηγίας 1999/93/EK είναι εμφανής η περιγραφή των συμμετεχουσών οντοτήτων μιας υποδομής δημοσίου κλειδιού χωρίς αυτή να αναφέρεται ρητά. Στην ενότητα αυτή περιγράφονται συνοπτικά τα χαρακτηριστικά και οι

εμπλεκόμενοι μιας Υποδομής Δημοσίου Κλειδιού. Ανατρέχοντας στα στοιχεία που αναφέρθηκαν στο 2^ο κεφάλαιο της μελέτης και ιδιαίτερα στους πίνακες που περιλαμβάνουν την υποστήριξη των ψηφιακών πιστοποιητικών στις ηλεκτρονικές ταυτότητες, είναι κατανοητή η εφαρμογή της υποδομής δημοσίου κλειδιού στο ζήτημα των ηλεκτρονικών ταυτοτήτων και η άμεση σχέση τους με την Ηλεκτρονική Διακυβέρνηση.

Η αυθεντικοποίηση με την υποστήριξη της υποδομής δημοσίου κλειδιού αποτελεί μια από τις κυριότερες διαθέσιμες τεχνολογίες ασφάλειας. Με την αξιοποίηση του εργαλείου ασφαλείας της Κρυπτογραφίας προκύπτουν δύο σημαντικές εφαρμογές : η κρυπτογράφηση και οι ψηφιακές υπογραφές. Η κρυπτογράφηση εξασφαλίζει την εμπιστευτικότητα των διακινούμενων πληροφοριών, ενώ οι ψηφιακές υπογραφές επικύρωση τον αποστολέα των δεδομένων (προέλευση δεδομένων) και επιβεβαιώνουν την μη-παραποίηση τους. Με την ενσωμάτωση υποδομών δημοσίου κλειδιού και την έκδοση των πιστοποιητικών ταυτότητας και χαρακτηριστικών από Έμπιστες Τρίτες Οντότητες εγγυάται η αυθεντικοποίηση του αποστολέα.

Η Υποδομή Δημοσίου Κλειδιού είναι ένα σύνολο που περιλαμβάνει οντότητες, υλικό, λογισμικό, τεχνολογίες κρυπτογράφησης, διαδικασίες και υπηρεσίες προκειμένου να επιτευχθεί η διαχείριση των πιστοποιητικών δημοσίου κλειδιού για την διασφάλιση της εμπιστευτικότητας, της αυθεντικοποίησης και της μη-αποποίησης των συμμετεχόντων μιας επικοινωνίας. Συστατικά μέρη μιας υποδομής είναι η Αρχή Πιστοποίησης (Certification Authority), το Αποθετήριο Πιστοποιητικών (Certificate Repository), η Αρχή Εγγραφής (Registration Authority), το λογισμικό εξυπηρετούμενου (PKI client software) και η εφαρμογή πιστοποίησης (PKI enabled Application). Βασικό ρόλο στην υποδομή δημοσίου κλειδιού διαδραματίζει ο χρήστης πιστοποιητικού.

5.4.1 Συνιστώσες Υποδομής Δημοσίου Κλειδιού Χρήστης

Πιστοποιητικού

Ένας χρήστης πιστοποιητικού μπορεί να είναι είτε ένα φυσικό, είτε ένα νομικό πρόσωπο (ιδιωτικού ή δημοσίου δικαίου) που έχει αιτηθεί, πιστοποιηθεί και λάβει ένα ψηφιακό πιστοποιητικό από μια Αρχή Πιστοποίησης. Κατά την αίτηση ενός ψηφιακού πιστοποιητικού ο χρήστης είναι υποχρεωμένος να υποβάλει αληθή στοιχεία και κατά την χρήση του να τηρεί τους κανόνες ορθής χρήσης.

Τα ψηφιακά πιστοποιητικά (digital certificates) αξιοποιούνται για λόγους αυθεντικοποίησης και περιλαμβάνουν πληροφορίες για τον κάτοχο τους, καθώς και τεχνικά στοιχεία του πιστοποιητικού. Συγκεκριμένα περιλαμβάνονται η έκδοση του προτύπου X.509, ο αριθμός σειράς, ο αλγόριθμος

υπογραφής, το διακριτικό όνομα του εκδότη, η χρονική διάρκεια ισχύος πιστοποιητικού (ημερομηνία έναρξης ισχύος, ημερομηνία λήξης ισχύος), το δημόσιο κλειδί του χρήστη και η υπογραφή του εκδότη του πιστοποιητικού.

Ο χρήστης πιστοποιητικού μπορεί να το χρησιμοποιήσει σε υπηρεσίες Ηλεκτρονικής Διακυβέρνησης είτε για ψηφιακή υπογραφή ηλεκτρονικών μηνυμάτων και εγγράφων, είτε για κρυπτογράφηση ηλεκτρονικών μηνυμάτων ή εγγράφων [67].

Αρχή Πιστοποίησης

Η Αρχή Πιστοποίησης αποτελεί μια αρχή που την εμπιστεύονται ένας ή περισσότεροι χρήστες πιστοποιητικών προκειμένου να λάβουν ή να πιστοποιήσουν ένα πιστοποιητικό δημοσίου κλειδιού και να συμμετάσχουν σε υπηρεσίες Ηλεκτρονικής Διακυβέρνησης.

Η Αρχή πιστοποίησης μπορεί να δημιουργεί, να αποθηκεύει και να ανακτά τα απαραίτητα κλειδιά, να διανέμει ψηφιακά πιστοποιητικά και να προβαίνει σε ανάκλησή τους όταν απαιτείται και να δημοσιεύει την Λίστα Ανάκλησης Πιστοποιητικών (Certificate Revocation List). Η Αρχή πιστοποίησης επιλύει το πρόβλημα διαχείρισης και διανομής των δημοσίων κλειδιών στην ασύμμετρη κρυπτογραφία.

Μια Αρχή Πιστοποίησης που διαχειρίζεται και δημιουργεί ζεύγη ιδιωτικών / δημοσίων κλειδιών (πέραν της διαχείρισης ψηφιακών πιστοποιητικών), παρέχει υπηρεσίες χρονοσήμανσης και πιστοποιεί άλλες αρχές πιστοποίησης μέσω ενδιάμεσων μονοπατιών εμπιστοσύνης είναι γνωστή και ως Έμπιστη Τρίτη Οντότητα και δρα ως Πάροχος Υπηρεσιών Εμπιστοσύνης [80].

Αρχή Εγγραφής

Η Αρχή Εγγραφής είναι ο ενδιάμεσος διαμεσολαβητής μεταξύ ενός χρήστη μιας υπηρεσίας (είτε φυσικού, είτε νομικού προσώπου) και της υπηρεσίας Πιστοποίησης. Ο χρήστης μιας υπηρεσίας ελέγχεται από την Αρχή Εγγραφής και αφού πιστοποιηθεί η ακρίβεια των στοιχείων του, τότε η Αρχή Εγγραφής προωθεί τα στοιχεία του χρήστη στην Αρχή ώστε να εκδοθεί το ψηφιακό πιστοποιητικό.

5.4.2 Ευρωπαϊκές Υλοποιήσεις

Πολλά ευρωπαϊκά κράτη έχουν υλοποιήσει συστήματα αυθεντικοποίησης που βασίζονται στην Υποδομή δημοσίου κλειδιού. Σύμφωνα με την μελέτη του Παρατηρητηρίου για την Κοινωνία της Πληροφορίας [75], αλλά και τα στοιχεία της παρούσας εργασίας (παράγραφος 2.2) η πλειοψηφία των κρατών μελών έχει

συμπεριλάβει στις ηλεκτρονικές κάρτες τα ψηφιακά πιστοποιητικά για την ταυτοποίηση και ψηφιακή υπογραφή των πολιτών τους.

Η υιοθέτηση των συστημάτων αυθεντικοποίησης ελέγχονται είτε αποκλειστικά από Δημόσιους φορείς, είτε από συμπράξεις δημόσιου και ιδιωτικού τομέα. Στον πίνακα 5.5 παρουσιάζονται τα αποτελέσματα της καταγραφής ύπαρξης συστημάτων αυθεντικοποίησης Υποδομής δημοσίου κλειδιού ανά κράτος και σημειώνεται εάν η υλοποίηση ελέγχεται από Δημόσιους φορείς ή κοινοπραξίες δημόσιου - ιδιωτικού τομέα.

Κράτος Μέλος	Υποδομές Δημοσίου Κλειδιού που ελέγχονται από:	
	Δημόσιο Τομέα	Σύμπραξη
Αυστρία		Ψηφιακό πιστοποιητικό
Βέλγιο	Ψηφιακό πιστοποιητικό	Ψηφιακή υπογραφή
Βουλγαρία		Ψηφιακή υπογραφή
Γαλλία	Ψηφιακό πιστοποιητικό	Ψηφιακό πιστοποιητικό
Γερμανία	Ψηφιακό πιστοποιητικό	
Δανία		Ψηφιακή υπογραφή
Ελλάδα	Ψηφιακή υπογραφή	
Εσθονία	Ψηφιακό πιστοποιητικό	Σύστημα βασισμένο σε Κινητή τεχνολογία
Ηνωμένο Βασίλειο		Ψηφιακή υπογραφή
Ιρλανδία	Ψηφιακό πιστοποιητικό ψηφιακή υπογραφή	
Ισπανία	Ψηφιακό πιστοποιητικό	
Ιταλία	Ψηφιακό πιστοποιητικό ψηφιακή υπογραφή	
Κροατία		
Κύπρος	Ψηφιακό πιστοποιητικό Ψηφιακή υπογραφή	
Λετονία	Ψηφιακό πιστοποιητικό Ψηφιακή υπογραφή	
Λιθουανία	Ψηφιακό πιστοποιητικό Ψηφιακή υπογραφή	
Λουξεμβούργο	Ψηφιακό πιστοποιητικό	

	Ψηφιακή υπογραφή	
Μάλτα	Ψηφιακό πιστοποιητικό Ψηφιακή υπογραφή	
Ολλανδία		Ψηφιακά Πιστοποιητικά
Ουγγαρία	Ψηφιακά Πιστοποιητικά	
Πολωνία		Ψηφιακά Πιστοποιητικά
Πορτογαλία	Ψηφιακά Πιστοποιητικά	Ψηφιακή Υπογραφή
Ρουμανία		Ψηφιακή Υπογραφή
Σλοβακία		Ψηφιακά Πιστοποιητικά
Σλοβενία	Ψηφιακό Πιστοποιητικό	Ψηφιακή Υπογραφή
Σουηδία		Ψηφιακά Πιστοποιητικά
Τσεχία		Ψηφιακό Πιστοποιητικό Ψηφιακή Υπογραφή
Φινλανδία	Ψηφιακό Πιστοποιητικό	

Πίνακας 5.5: Υποστήριξη Αυθεντικοποίησης Υποδομής Δημοσίου Κλειδιού στην

Από τα στοιχεία του πίνακα 5.5 διαπιστώνεται ότι στα 27 από τα 28 κράτη της Ευρωπαϊκής Ένωσης παρουσιάζονται λύσεις αυθεντικοποίησης. Από τα στοιχεία προκύπτει ότι 17 από τα 28 κράτη της Ευρωπαϊκής Ένωσης περιλαμβάνουν υλοποιήσεις που ελέγχονται από τον δημόσιο τομέα, ενώ 15 κράτη μέλη υποστηρίζουν συστήματα από συμπράξεις δημοσίου - ιδιωτικού τομέα. Στο Βέλγιο, την Γαλλία, την Εσθονία, την Πορτογαλία και την Σλοβενία υπάρχουν ψηφιακά πιστοποιητικά και για τις δύο κατηγορίες. Η μόνη περίπτωση που δεν αναφέρεται παρουσία ψηφιακού πιστοποιητικού είναι η περίπτωση της Κροατίας. Η συγκεκριμένη χώρα είναι η τελευταία χώρα που προσχώρησε στην Ευρωπαϊκή Ένωση και με την ένταξή της το 2013 ανασχεδίασε την ταυτότητα σε ηλεκτρονική κάρτα συμπεριλαμβάνοντας το

πλινθίο, χωρίς ωστόσο να αναφέρεται ύπαρξη ψηφιακού πιστοποιητικού, είτε υποστήριξη ψηφιακής υπογραφής. Συνήθως όπου υπάρχει παρουσία ψηφιακού πιστοποιητικού για την ταυτοποίηση υπάρχει και η παρουσία της ψηφιακής υπογραφής.

Κεφάλαιο 6

Η Ελληνική Ηλεκτρονική Πραγματικότητα

"Καθένας έχει δικαίωμα συμμετοχής στην Κοινωνία της Πληροφορίας. Η διευκόλυνση της πρόσβασης στις πληροφορίες που διακινούνται ηλεκτρονικά, καθώς και της παραγωγής ανταλλαγής και διάδοσης τους αποτελεί υποχρέωση του Κράτους τηρούμενων πάντα των εγγυήσεων των άρθρων 9, 9Α και 19."

Το παρόν κεφάλαιο ξεκινά με το άρθρο 5Α του Ελληνικού Συντάγματος, σε μια προσπάθεια να επιδειχθεί η σημαντική αξία της ίσης συμμετοχής των πολιτών με διαφανή τρόπο στις πληροφορίες που διανέμονται ηλεκτρονικά, καθώς επίσης και η υπευθυνότητα με την οποία αντιμετωπίζει το ίδιο το Κράτος τις παρεχόμενες υπηρεσίες προς τον πολίτη. Στο «πώς» θα έχει πρόσβαση ο πολίτης συντελεί η Κάρτα Πολίτη.

Η σχέση της Ελλάδας με την Ηλεκτρονική Διακυβέρνηση ξεκίνησε το 1999, όταν και διαμορφώθηκε η πρώτη εθνική στρατηγική ώστε να παρέχονται τυποποιημένες υπηρεσίες πληροφόρησης και συναλλαγών μέσα από την τεχνολογία του Διαδικτύου. Σήμερα, το Υπουργείο Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης έχει τον πρωτεύοντα

ρόλο για τον συντονισμό των ενεργειών που απαιτούνται προκειμένου να οργανωθεί η Δημόσια Διοίκηση με αποδοτικότητα και διαφάνεια και να παρέχονται ταχύτερες ηλεκτρονικές υπηρεσίες στους πολίτες με απλότητα και ποιότητα.

Στο παρόν κεφάλαιο παρουσιάζεται το πλαίσιο για την ηλεκτρονική ταυτοποίηση στην ελληνική πραγματικότητα και Διακυβέρνηση. Συγκεκριμένα, παρατίθεται το υφιστάμενο θεσμικό πλαίσιο καλύπτοντας νομικά και τεχνικά θέματα, γίνεται παρουσίαση της Κάρτας Πολίτη και των εμπλεκόμενων φορέων για την υλοποίηση της και γίνεται μια παρουσίαση των δράσεων της Ομάδας Ηλεκτρονικής Διακυβέρνησης.

6.1 Θεσμικό πλαίσιο

Στην εισαγωγή του κεφαλαίου αναφέρθηκε το άρθρο 5Α του Συντάγματος. Ωστόσο στο άρθρο 5Α γίνεται αναφορά του άρθρου 9Α όπου επισημαίνεται η ανάγκη προστασίας της Ιδιωτικότητας των πολιτών : *«Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει.»*. Με το άρθρο 9Α θεσπίζεται ότι όλοι (καθένας) πρέπει να προστατεύονται από την ηλεκτρονική επεξεργασία των δεδομένων τους και το δικαίωμα αυτό υπερασπίζεται από ανεξάρτητη αρχή.

Νόμος 2472/97 (Προστασία ατόμων από επεξεργασία δεδομένων προσωπικού χαρακτήρα)

Ο Νόμος 2472/97 ενσωμάτωσε την Οδηγία 95/46/ΕΚ στην ελληνική πραγματικότητα, προκειμένου να θεσπιστεί η προστασία των ατόμων και να καθοριστούν οι όροι και οι προϋποθέσεις για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και κυρίως η ιδιωτική ζωή. Στο νομικό κείμενο γίνεται διάκριση των δεδομένων προσωπικού χαρακτήρα, των δεδομένων στατιστικής φύσης και των ευαίσθητων δεδομένων, καθορίζεται η έννοια της Επεξεργασίας δεδομένων και του υπεύθυνου και εκτελών της επεξεργασίας. Πα το υποκείμενο των δεδομένων αναφέρονται τα δικαιώματα ενημέρωσης, πρόσβασης και αντίρρησης, ενώ ορίζεται ως επίσημη Αρχή η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Ο νόμος αυτός αποτελεί την ασπίδα για την οργάνωση του ελέγχου προστασίας των προσωπικών δεδομένων και την διασφάλιση της εφαρμογής του νομοθετικού πλαισίου.

Νόμος 2774/99 (Δεδομένα προσωπικού χαρακτήρα στις τηλεπικοινωνίες)

Ο Νόμος 2774/99 ενσωμάτωσε την Οδηγία 97/66/ΕΚ προκειμένου να θεσπιστεί η προστασία των θεμελιωδών δικαιωμάτων των ατόμων και ιδίως της ιδιωτικής ζωής και η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα. Βάσει του νόμου

2774/99 ορίζονται οι κύριοι εμπλεκόμενοι του πεδίου εφαρμογής του νόμου, δηλαδή οι συνδρομητές, οι χρήστες, το δημόσιο τηλεπικοινωνιακό δίκτυο και οι τηλεπικοινωνιακές υπηρεσίες.

Ο νόμος καθορίζει την προστασία του απορρήτου των επικοινωνιών, την επεξεργασία δεδομένων μόνο κατόπιν της συγκατάθεσης του χρήστη, την υπεράσπιση των αρχών του ελαχίστου και του σκοπού και την δυνατότητα ανώνυμης και ψευδώνυμης χρήσης υπηρεσιών. Τα δεδομένα κίνησης που διατηρούνται από τον παροχέα υπηρεσιών οφείλουν να διατηρούνται για καθορισμένο χρονικό διάστημα ή να καθίστανται ανώνυμα κατά την ολοκλήρωση της επεξεργασίας. Τα φυσικά πρόσωπα διατηρούν το δικαίωμα μη συμπερίληψης στους τηλεφωνικούς καταλόγους, είτε σε περίπτωση συμπερίληψης την επιλεγμένη παρουσίαση στοιχείων τους. Στο άρθρο 10 ορίζεται η υποχρέωση λήψης των κατάλληλων μηχανισμών ασφάλειας από πλευράς παροχέα υπηρεσιών προκειμένου να προστατευτούν οι χρήστες, καθώς και η ενημέρωση σε περιπτώσεις αποτροπής κινδύνων ασφαλείας.

ΠΔ150/2001 (Ψηφιακές υπογραφές)

Το Προεδρικό Διάταγμα 150/2001 (ΦΕΚ 125/Α/25 Ιουνίου 2001) αφορά την προσαρμογή της Οδηγίας 1999/93/ΕΚ σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές στην ελληνική κοινωνία. Στο προεδρικό διάταγμα ορίζονται τα θέματα που αφορούν τις ψηφιακές υπογραφές, τις έννομες συνέπειες των ηλεκτρονικών υπογραφών και τις προϋποθέσεις χρήσης προηγμένης ηλεκτρονικής υπογραφής ως τρόπο ισότιμης ιδίως χειρής υπογραφής.

ΠΔ 342/2002 (Διακίνηση εγγράφων)

Το Προεδρικό Διάταγμα 342/2002 (ΦΕΚ 284/Α/22 Νοεμβρίου 2002) αφορά την Διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο μεταξύ των δημοσίων υπηρεσιών, Ν.Π.Δ.Δ. και Ο.Τ.Α. ή μεταξύ αυτών και των φυσικών ή νομικών προσώπων ιδιωτικού δικαίου και ενώσεων φυσικών προσώπων. Στο διάταγμα αναφέρεται η διακίνηση των εγγράφων με ηλεκτρονικό ταχυδρομείο με υποχρεωτική ψηφιακή υπογραφή και ορίζονται οι έννομες συνέπειες των ηλεκτρονικών εγγράφων.

Νόμος 3861/2010 (Δι@γεια)

Ο Νόμος 3861/2010 ρυθμίζει την Διαφάνεια στο Δημόσιο τομέα προβλέποντας την υποχρεωτική ανάρτηση των νόμων, πράξεων νομοθετικού περιεχομένου, προεδρικών διαταγμάτων κανονιστικού χαρακτήρα, ερμηνευτικών εγκυκλίων, γνωμοδοτήσεων, δωρεών, ατομικών πράξεων και προϋπολογισμών στο Διαδίκτυο. Τα αναρτώντα στοιχεία υπερασπίζονται των περιορισμών για τα ευαίσθητα προσωπικά δεδομένα.

Νόμος 3979/2011 (Ηλεκτρονική Διακυβέρνηση)

Ο Νόμος 3979/2011 αποτελεί το θεσμικό πλαίσιο με τις προϋποθέσεις για την παροχή ηλεκτρονικών υπηρεσιών της Δημόσιας Διοίκησης σε πολίτες και επιχειρήσεις. Ο νόμος αναγνωρίζει τα δικαιώματα φυσικών και νομικών προσώπων για ηλεκτρονικές συναλλαγές, λαμβάνει μέριμνα για την προστασία των δεδομένων προσωπικού χαρακτήρα και παρέχει από τους δικτυακούς τόπους των φορέων κάθε χρήσιμη πληροφορία για την εξυπηρέτησή τους [195]. Στο άρθρο 3 ορίζονται σημαντικές παράμετροι: τα αναγνωριστικά των χρηστών, η Αρχή Εγγραφής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης, η Αρχή Πιστοποίησης, το πλαίσιο της Ασφάλειας Πληροφοριακών Συστημάτων, η Ασφάλεια Τεχνολογιών Πληροφορικής και Επικοινωνιών, τα Δεδομένα προσωπικού χαρακτήρα, τα Διαπιστευτήρια, η Εγγραφή, η Επιβεβαίωση Ταυτότητας, η Ηλεκτρονική διαχείριση εγγράφων, η Ηλεκτρονική υπογραφή, το Πιστοποιητικό, η Πολιτική Ασφαλείας, η Προηγμένη Ηλεκτρονική Υπογραφή, η Ταυτοποίηση, οι υπηρεσίες Ηλεκτρονικής Διακυβέρνησης, οι υπηρεσίες χρονοσήμανσης.

Στόχος του πλαισίου είναι η παροχή απλουστευμένων ηλεκτρονικών υπηρεσιών για τις συναλλαγές του Δημόσιου τομέα, ώστε να μειωθεί η γραφειοκρατία και να περιοριστεί δραστικά ο χρόνος εξυπηρέτησης των πολιτών/επιχειρήσεων. Η πλήρης εναρμόνιση με τις νέες τεχνολογίες θα αποφέρει ταχύτητα στις διοικητικές διαδικασίες, αξιοποίηση του εργατικού δυναμικού και μείωση του κόστους της Δημόσιας Διοίκησης.

Η χρήση προηγμένης ψηφιακής υπογραφής που βασίζεται σε αναγνωρισμένο πιστοποιητικό πιστοποιεί τα ηλεκτρονικά έγγραφα, υποστηρίζεται το Ηλεκτρονικό Πρωτόκολλο στο σύνολο των φορέων και καθιερώνεται η ηλεκτρονική επικοινωνία μεταξύ των φορέων και των εξυπηρετούμενων (πολιτών / επιχειρήσεων) με τις διασφαλίσεις αυθεντικοποίησης των συμμετεχουσών οντοτήτων. Από το πλαίσιο προάγεται η διαρκής βελτίωση των παρεχόμενων υπηρεσιών και η διαλειτουργικότητα.

Νόμος 4013/2011 (Δημόσιες Συμβάσεις)

Ο νόμος συστήνει μια Ανεξάρτητη Αρχή Δημοσίων Συμβάσεων και το Κεντρικό Ηλεκτρονικό Μητρώο Δημοσίων Συμβάσεων «*με σκοπό την ανάπτυξη και προαγωγή της εθνικής στρατηγικής, πολιτικής και δράσης στον τομέα των δημοσίων συμβάσεων, τη διασφάλιση της διαφάνειας αποτελεσματικότητας συνοχής και εναρμόνισης των συμβάσεων προς το εθνικό και ευρωπαϊκό δίκαιο*» [196]. Στον νόμο καθορίζονται οι αρμοδιότητες της Αρχής και συστήνεται στο Υπουργείο Ανάπτυξης, Ανταγωνιστικότητας και Ναυτιλίας το Κεντρικό Ηλεκτρονικό Μητρώο Δημοσίων Συμβάσεων ώστε να συλλέγονται, επεξεργάζονται και δημοσιεύονται τα στοιχεία προκειμένου να δύναται η ηλεκτρονική καταχώριση των αιτημάτων των φορέων δημοσίου τομέα, καθώς και των υπογεγραμμένων συμβάσεων.

ΥΑΠ/Φ.60/76/984 (Υποδομή Δημοσίου Κλειδιού)

Σύμφωνα με την Υπουργική Απόφαση Φ.60/76/984 (ΦΕΚ 1162/Β/10 Απρ 2012) [197], ορίστηκε η Υποδομή Δημοσίου Κλειδιού με συνισταμένες:

Σ ως Αρχή Πιστοποίησης του Ελληνικού Δημοσίου (Πρωτεύουσα Αρχή Πιστοποίησης) :
την Υπηρεσία Ανάπτυξης Πληροφορικής (ΥΑΠ) του Υπουργείου Διοικητικής
Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης. *Σ* ως Υποκείμενη Αρχή Πιστοποίησης»
(ΥπΑΠ) : το Τμήμα Επεξεργασίας και Διαρκούς
Απογραφής της Διεύθυνσης Προγραμματισμού και Εφαρμογών της ΥΑΠ
του Υπουργείου Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης. *Σ* ως «Αρχή
Εγγραφής» : τον Τομέα Υλοποίησης και Παραγωγικής Λειτουργίας Έργων και
Συστημάτων της «Κοινωνίας της Πληροφορίας ΑΕ», το Τεχνικό Επιμελητήριο Ελλάδος
και ο Δικηγορικός Σύλλογος Αθηνών. *Σ* ως «Εντεταλμένα Γραφεία» (ΕΓ) της ΑΠΕΔ : τα Κέντρα
Εξυπηρέτησης Πολιτών (ΚΕΠ), τα
κατά τόπους περιφερειακά τμήματα του Τ.Ε.Ε. και ο Δ.Σ.Α Υποστήριξης της ΥΑΠ

Για την ταυτοποίηση του τελικού χρήστη, οι Έλληνες πολίτες προσκομίζουν το δελτίο αστυνομικής ταυτότητας ή το βιβλιάριο υγείας, ενώ οι αλλοδαποί πολίτες προσκομίζουν την ταυτότητα, το διαβατήριο ή άλλο επίσημο έγγραφο ταυτοποίησης. Τα νομικά πρόσωπα ταυτοποιούνται με τις οριζόμενες διατάξεις της έδρας τους.

6.2 Τεχνικά Θέματα

Μετά από την μελέτη των ευρωπαϊκών οδηγιών, καθώς και την θεσμική προσπάθεια της Ελληνικής κυβέρνησης προκύπτουν ορισμένα θέματα που πρέπει να λαμβάνονται υπόψη προκειμένου να διασφαλιστεί η τεχνική προσέγγιση της ηλεκτρονικής ταυτοποίησης των πολιτών και η ασφάλεια των προσωπικών δεδομένων τους.

Αρχικά, πρέπει να υπάρχει ένα σύστημα διαχείρισης των ηλεκτρονικών ταυτοτήτων, το οποίο να συντονίζει όλες τις εργασίες έκδοσης, επεξεργασίας και ακύρωσης των ταυτοτήτων, χωρίς προβλήματα. Σύμφωνα με τα παραπάνω στοιχεία, υπάρχει ανάμιξη του ιδιωτικού τομέα στο πλαίσιο διαχείρισης των ηλεκτρονικών ταυτοτήτων με αποτέλεσμα τα δεδομένα των πολιτών να βρίσκονται στην ευχέρεια ιδιωτικών εταιριών. Παρά το γεγονός ότι υπάρχει σαφής περιγραφή στο νομικό πλαίσιο για το χρονικό διάστημα που πρέπει να αποθηκεύονται τα δεδομένα των χρηστών και τις απατήσεις συγκατάθεσης είναι

πιθανόν να υπάρχει επαναχρησιμοποίηση σε διαφορετικά πλαίσια για τα οποία έχουν συλλεχθεί. Ως αποτέλεσμα, η διαχείριση του συστήματος ηλεκτρονικής ταυτοποίησης εγείρει κινδύνους διαρροής των προσωπικών δεδομένων των χρηστών.

Δεύτερο σημαντικό θέμα είναι η υλοποίηση στρατηγικών αυθεντικοποίησης με διπλό χαρακτήρα. Θα πρέπει να γίνεται αυθεντικοποίηση από πλευράς χρηστών, αλλά και από πλευράς υπηρεσιών. Όπως αναφέρθηκε στην ενότητα της Ασφάλειας Αυθεντικοποίησης, αναπτύχθηκαν τα επίπεδα εμπιστοσύνης των υπηρεσιών που αναφέρουν την σχέση εμπιστοσύνης υπηρεσίας και των πολιτών.

Ένα άλλο ζήτημα είναι ο τρόπος επιβεβαίωσης της ταυτότητας ενός χρήστη. Στην επίλυση αυτού του ζητήματος συντελεί η Υποδομή Δημοσίου Κλειδιού, η οποία επιτρέπει την επιβεβαίωση της ταυτότητας ενός χρήστη από μια Έμπιστη Τρίτη Οντότητα (Trusted Third Party). Σε ένα περιβάλλον PKI, ένας χρήστης μπορεί να χρησιμοποιεί την ηλεκτρονική του κάρτα (όπου είναι αποθηκευμένο το ιδιωτικό κλειδί του) και να συναλλάσσεται με υπηρεσίες, απαντώντας στις κρυπτογραφικές προκλήσεις της εκάστοτε υπηρεσίας.

Ένα πρόσθετο στοιχείο που ενσωματώνεται στην ηλεκτρονική ταυτότητα είναι η βιομετρική αναγνώριση των πολιτών. Στο παράρτημα Β της μελέτης αναφέρονται τα χαρακτηριστικά της κάρτας ταυτοποίησης και στον κωδικό 181 περιλαμβάνονται τα βιομετρικά αναγνωριστικά στοιχεία που συντελούν στην μοναδική αναγνώριση των χρηστών. Πρόσθετα, οι κάρτες ταυτοποίησης πρέπει να δημιουργούνται με διαδικασίες και την απαραίτητη τεχνολογία ώστε να μην είναι εύκολη η αντιγραφή της.

6.3 Κάρτα Πολίτη

Στη Ελλάδα, το δελτίο αστυνομικής ταυτότητας αποτελεί το υποχρεωτικό μέσο ταυτοποίησης για όλους τους Έλληνες πολίτες άνω των 12 ετών με διάρκεια ισχύος τα 15 έτη. Στην ελληνική νομοθεσία αναφέρεται ότι η αστυνομική ταυτότητα είναι το νόμιμο αποδεικτικό στοιχείο για ένα πολίτη προκειμένου να προβεί σε οποιαδήποτε συναλλαγή που απαιτεί ταυτοποίηση. Πρόσθετα, επειδή η χώρα μας συμμετέχει στη Συνθήκη Schengen, ένας πολίτης μπορεί να κινηθεί στα κράτη-μέλη της Ευρωπαϊκής Ένωσης με χρήση της αστυνομικής ταυτότητας.

Η ηλεκτρονική μορφή της φυσικής ταυτοποίησης του πολίτη θα διεξάγεται με τη Κάρτα Πολίτη. Στο Επιχειρησιακό Πρόγραμμα «Διοικητική Μεταρρύθμιση 2007-2013» με τίτλο «Ανάπτυξη Οδικού Χάρτη για την εισαγωγή της κάρτας Πολίτη» εκπονήθηκε μελέτη που μπορεί να αποτελέσει το βασικό Οδικό Χάρτη για την εισαγωγή της Κάρτας Πολίτη (ΚΠ). Η Κάρτα Πολίτη θα επιτρέπει ταυτοποίηση, δυνατότητα μετακίνησης στο εξωτερικό, αλλά κυρίως στον ψηφιακό κόσμο.

Αρχικός στόχος θα είναι η εξυπηρέτηση των πολιτών μέσω της ψηφιακής αυθεντικοποίησης τους σε ηλεκτρονικές υπηρεσίες που παρέχονται από τη δημόσια διοίκηση, και η επέκτασή σε ιδιωτικές πρωτοβουλίες [121]. Δεύτερος στόχος θα είναι η υποστήριξη όλων των κανονισμών που θέτει ο Διεθνής Οργανισμός Πολιτικής Αεροπορίας (International Civil Aviation Organization - ICAO), ώστε η Κάρτα Πολίτη να αποτελεί και επίσημο ταξιδιωτικό έγγραφο για τους πολίτες που θέλουν να ταξιδέψουν εντός των κρατών που συνυπογράφουν την συνθήκη Schengen.

Με την Κάρτα Πολίτη ο πολίτης δεν θα χρειάζεται να γίνεται αχθοφόρος δικαιολογητικών για κάθε συναλλαγή με την Δημόσια Διοίκηση, αλλά δεν θα απαιτείται και από τις αντίστοιχες υπηρεσίες να απασχολούν υπαλλήλους για την κατ' επανάληψη χορήγηση πιστοποιητικών για κάθε πολίτη. Σε κάθε περίπτωση, θα μειώνονται τα λειτουργικά κόστη της Δημόσιας Διοίκησης που πλέον μπορεί να χαρακτηριστεί και ως «οικολογική» Δημόσια Διοίκηση, καθώς και φαινόμενα διαφθοράς που παρουσιάζονται κατά τις διαζώσης συναλλαγές των πολιτών με δημόσιους υπαλλήλους.

Τέλος, από πλευράς χρονικών καθυστερήσεων για την ολοκλήρωση μιας συναλλαγής δεν θα τίθεται θέμα, μιας και η ψηφιακή υπογραφή συντελεί στην παράκαμψη της υποχρεωτικής παρουσίας (και πιθανής αναμονής) του πολίτη για την έκδοση οποιουδήποτε δικαιολογητικού.

6.3.1 Δομή Κάρτας Πολίτη

Στον ψηφιακό κόσμο, η Κάρτα Πολίτη θα αποτελέσει το διαβατήριο για την ταχύτατη πρόσβαση των πολιτών στις ηλεκτρονικές υπηρεσίες της Δημόσιας Διοίκησης. Η κάρτα πολίτη θα φέρει μια διεπαφή ανεπαφικού πλινθίου, μέσα από το οποίο όσοι πολίτες επιθυμούν θα μπορούν να επιβεβαιώσουν την ταυτότητά τους, αλλά και να υπογράψουν ψηφιακά τα αιτήματά τους. Τα στοιχεία της Κάρτας Πολίτη διαχωρίζονται σε δύο ομάδες : στην ομάδα Α που περιλαμβάνει τα αναγνωριστικά στοιχεία του πολίτη και στην ομάδα Β που περιλαμβάνει πρόσθετα στοιχεία για τις υπηρεσίες Ηλεκτρονικής Διακυβέρνησης.

Τα δεδομένα της ομάδας Α, που αποτελούν τα αναγνωστικά στοιχεία της Κάρτας πολίτη περιλαμβάνουν:

S το εθνόσημο,

S την αναγραφή «Ελληνική Δημοκρατία - Υπουργείο Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης»

S Κωδικός & Τύπος Εγγράφου

S Κωδικός Χώρας Έκδοσης

S Ιθαγένεια

S Αριθμός Εντύπου της ΚΠ

■S Επώνυμο

S Όνομα

S Ημερομηνία Γέννησης

S Ημερομηνία Λήξης Ισχύος της ΚΠ

S Φωτογραφία

S Υπογραφή

Τα δεδομένα της ομάδας Β που με την συγκατάθεση του πολίτη μπορούν να διατηρούνται στα επιμέρους πληροφοριακά συστήματα των υπηρεσιών Δημόσιας Διοίκησης, αφορούν το ΑΦΜ, ΑΜΚΑ, ΑΔΤ, Αριθμό Δημοτολογίου, το Δήμο και την διεύθυνση επικοινωνίας. Οι αριθμοί ΑΦΜ και ΑΜΚΑ είναι σταθερά αναγνωριστικά των πολιτών, ενώ ο Αριθμός Δημοτολογίου και ο Δήμος αποτελούν μεταβλητά στοιχεία. Τα στοιχεία αυτά *δεν διατηρούνται στην Κάρτα Πολίτη*, αλλά σε περίπτωση εγγραφής του πολίτη σε μια υπηρεσία, τότε πραγματοποιείται η σύνδεση των δύο ομάδων δεδομένων.

6.3.2 Κύκλος Ζωής

Η χρήση της Κάρτας Πολίτη προϋποθέτει τρεις εμπλεκόμενους : τον ιδιοκτήτη της, το σύστημα Αυθεντικοποίησης και τον πάροχο της υπηρεσίας που επιθυμεί ο πολίτης. Στις προηγούμενες παραγράφους αναφέρθηκαν οι ανάγκες της κάρτας πολίτη, τα χαρακτηριστικά της δομής της και στοιχεία που προστατεύουν τα δεδομένα της. Όλα αυτά βέβαια αναπαριστούν μέρη της «ζωής» της κάρτας.

Στην προσπάθεια μας επιγραμματικής καταγραφής των φάσεων ζωής μας κάρτας, τα βήματα που ακολουθεί η κάρτα είναι τα εξής:

S Αρχική έκδοση της ΚΠ ανάλογα με την κατηγορία πολιτών (ενήλικες, ανήλικοι)

S Χρήση (προσθήκη δυνατότητας ψηφιακής υπογραφής, αλλαγή στοιχείων επικοινωνίας)

S Ανάκληση (λόγω κλοπής, βλάβης, λήξης)

S Επανεκδοση μετά από ανάκληση

■S Οριστική ανάκληση (σε περίπτωση θανάτου)

Πίσω από το σύστημα αυθεντικοποίησης της Κάρτας Πολίτη πρέπει να βρίσκεται μια αρμόδια αρχή, η οποία θα φέρει την ευθύνη και θα συντονίζει την έκδοση της ΚΠ και τους εμπλεκόμενους του συστήματος. Η αρμόδια εκδούσα αρχή θα πρέπει να παραλαμβάνει τα αιτήματα έκδοσης ΚΠ των πολιτών με τα αντίστοιχα δικαιολογητικά, να επεξεργάζεται τα στοιχεία και να εκδίδει τις κάρτες. Πρόσθετα, η εκδούσα αρχή παραλαμβάνει αιτήματα ένταξης παρόχων ηλεκτρονικής υπηρεσίας και μεριμνά αντίστοιχα. Η εκδούσα αρχή υποχρεούται να φυλάξει με ύψιστη ασφάλεια όλα τα έγγραφα αιτήματα και δικαιολογητικά, είτε να προβεί σε καταστροφή τους. Σε κάθε περίπτωση είναι τόσο λεπτό το ζήτημα των προσωπικών δεδομένων και για αυτό απαιτείται η δέουσα προσοχή και πρόβλεψη ώστε να είναι η ασφαλής τήρηση μητρώων Καρτών πολίτη, ηλεκτρονικών παρόχων, ρόλων και δικαιωμάτων πρόσβασης.

6.3.3 Προστασία της πληροφορίας

Η έννοια «Προστασία της πληροφορίας» στην Κάρτα Πολίτη αναφέρεται στην προστασία της ταυτότητας και της ιδιωτικότητας του πολίτη.

Τι γνωρίζει ο πολίτης πριν

Η Κάρτα Πολίτη θα ακολουθεί την αρχή του ελαχίστου και δεν θα περιλαμβάνει ευαίσθητα προσωπικά δεδομένα. Μάλιστα τα δεδομένα που θα αναγράφονται θα είναι εκ των προτέρων γνωστά και ο πολίτης θα έχει δώσει την συγκατάθεσή του. Πρόσθετα, στην κάρτα δεν θα μπορούν να προστεθούν στοιχεία από μη εξουσιοδοτημένες οντότητες, ούτε θα μπορούν να διαβαστούν τα στοιχεία εφόσον δεν υπάρξει η συγκατάθεση του πολίτη. Κάθε τροποποίηση των στοιχείων της ομάδας Β θα μπορεί να πραγματοποιηθεί μόνο σε εξουσιοδοτημένα κέντρα εξυπηρέτησης.

Ασφάλεια και Προστασία Συναλλαγών

Για την ασφάλεια των συναλλαγών των πολιτών, όταν πραγματοποιείται μια συναλλαγή τότε θα ελέγχεται εάν ισχύει η κάρτα πολίτη και εάν η υπηρεσία έχει το δικαίωμα πρόσβασης στα δεδομένα του πολίτη βάσει του επιπέδου υπηρεσίας που προσφέρει. Μέσω της Διαδικτυακής Πύλης της Δημόσιας

Διοίκησης ΕΡΜΗΣ [159], οι χρήστες της θα έχουν πρόσβαση στα δεδομένα που τους αφορούν και τηρούνται στα μητρώα της Δημόσιας Διοίκησης, καθώς και στους παρόχους υπηρεσιών που έχουν πρόσβαση στα δεδομένα τους [121].

Ιδιωτικότητα

Για την προστασία της ιδιωτικότητας των προσωπικών δεδομένων των πολιτών, οι πολίτες θα μπορούν να ενημερωθούν κατόπιν αιτήματος τους για τα συστήματα που προσπέλασαν τα δεδομένα τους. Επιπρόσθετα, για την προστασία της ιδιωτικότητας των συναλλαγών του πολίτη και την μη συνδεσιμότητα τους, υπάρχει πιθανότητα να παράγεται από το πλινθίο διαφορετικό αναγνωριστικό για κάθε πάροχο υπηρεσίας ή να χρησιμοποιείται η λειτουργία του ψευδωνύμου.

Πλαστοπροσωπία

Η κάρτα πολίτη θα διαθέτει υψηλού επιπέδου χαρακτηριστικά ασφάλειας, σύμφωνα με διεθνώς αναγνωρισμένα πρότυπα, για την αποφυγή πλαστοπροσωπίας. Συγκεκριμένα, για την κατασκευή της κάρτας θα χρησιμοποιείται πολυανθρακικό, θα λαμβάνει μέγεθος πιστωτικής κάρτας και θα ακολουθεί το πρότυπο ISO/IEC 7810. Θα περιλαμβάνεται σχέδιο ασφαλείας με έχει δύο ειδικά χρώματα και μικροσκοπική γραφή και θα καλύπτει μέρος της φωτογραφίας του κατόχου και ειδικά στοιχεία εκτύπωσης και μεταβλητά οπτικά στοιχεία, όπως αναφέρονται στο ευρωπαϊκό πρότυπο CEN/TS 15480 Part 1[14].

Ακεραιότητα

Για την προστασία της ακεραιότητας των δεδομένων χρησιμοποιείται το ψηφιακό πιστοποιητικό X.509, κατά το οποίο ακολουθείται η διαδικασία ελέγχου της ακεραιότητας Passive Authentication. Σχετικά με την διασφάλιση της ακεραιότητας των δεδομένων, στην μελέτη «Ανάπτυξη Οδικού Χάρτη για την Εισαγωγή της Κάρτας πολίτη» αναφέρεται:

Κορυφή της ιεραρχίας των Αρχών Έκδοσης (Certification Authority, CA) ψηφιακών πιστοποιητικών για τη χώρα μας αποτελεί η «Πρωτεύουσα Αρχή Πιστοποίησης» (N.3448/2006) (Country Signing Certification Authority, CSCA). Η «Πρωτεύουσα Αρχή Πιστοποίησης» (CSCA) εκδίδει και αυτοϋπογράφει τα πιστοποιητικά της χώρας (Country Signing Certification Authority Certificates, CCSCA) τα οποία περιλαμβάνουν το ιδιωτικό (privet key, KPRCSCA) και το δημόσιο κλειδί (Public Key, KPUCSCA). Το δημόσιο κλειδί (KPUCSCA) εισάγεται στο πλινθίο της ΚΠ σε αρχικό στάδιο της παραγωγής της μαζί με την εκτύπωση του εθνόσημου, ενώ με το ιδιωτικό κλειδί (KPRCSCA) υπογράφεται το πιστοποιητικό της Αρχής Έκδοσης της Κάρτας Πολίτη (Document Signer Certificates/ CDS). Το πιστοποιητικό της Αρχής Έκδοσης της Κάρτας Πολίτη (CDS' περιλαμβάνει/ αντίστοιχα/ το ιδιωτικό (KPRDS) και το δημόσιο κλειδί (KPUDS).

Στη συνέχεια/ από τα δεδομένα της «Ομάδας Α» που εγγράφονται στο πλινθίο κατά τη φάση της προσωποποίησης της Κάρτας Πολίτη/ μέσω ειδικής μονόδρομης συνάρτησης -αλγόριθμο κατακερματισμού - (one way hash - SHA-x)/ δημιουργείται μια σύνοψη. Το χαρακτηριστικό του αλγορίθμου αυτού είναι ότι αφενός από τη σύνοψη που παράγει είναι αδύνατο να αναπαραχθεί το αρχικό περιεχόμενο και αφετέρου πως είναι πρακτικά αδύνατο από δύο διαφορετικά σύνολα δεδομένων να παραχθούν δύο ίδιες συνόψεις. Η παραχθείσα σύνοψη υπογράφεται με το ιδιωτικό κλειδί (KPRDS) της Αρχής Έκδοσης της Κάρτας Πολίτη και αποθηκεύεται ως αντικείμενο ασφαλείας (Document Security Object DSO) σε ειδικό χώρο στο πλινθίο της ΚΠ. Στη φάση αυτή αποθηκεύεται στο πλινθίο και το αντίστοιχο δημόσιο κλειδί (KPU DS) της Αρχής Έκδοσης της Κάρτας Πολίτη και με τον τρόπο αυτό ολοκληρώνεται η προσωποποίηση της ΚΠ.

Κατά την ανάγνωση του περιεχόμενου του πλινθίου της ΚΠ εφαρμόζεται στα δεδομένα η ίδια μονόδρομη συνάρτηση (SHA-x) που χρησιμοποιήθηκε κατά την προσωποποίηση της ΚΠ και η σύνοψη που παράγεται συγκρίνεται με το αντικείμενο ασφαλείας (DSO) του πλινθίου αφού πρώτα το περιεχόμενό του αποκωδικοποιηθεί κάνοντας χρήση του δημόσιου κλειδιού (KPU DS) της Αρχής Έκδοσης της Κάρτας Πολίτη. Αν κατά τη σύγκριση η παραγόμενη σύνοψη ταυτίζεται με το αποκωδικοποιημένο περιεχόμενο του αντικειμένου ασφαλείας (DSO)/ τότε βεβαιώνεται η ακεραιότητα των δεδομένων του πλινθίου της ΚΠ. Η ανωτέρω διαδικασία ελέγχου της ακεραιότητας καλείται *Passive Authentication (PA)* και αποτελεί τον πυρήνα όλων των διαδικασιών πρόσβασης στα δεδομένα της Κάρτας Πολίτη [121].

Το πλινθίο προτείνεται να ακολουθεί το πρωτόκολλο BAC, το οποίο κλειδώνει το πλινθίο και δεν παρέχει πρόσβαση στα δεδομένα του, είτε το πρωτόκολλο PACE που προϋποθέτει ύπαρξη μυστικού κωδικού PIN(και PUK) και χρήση της μεθόδου Chip Authentication (CA), με σκοπό την προστασία από κλωνοποίηση. Εφόσον ακολουθηθούν τα προαναφερθέντα πρωτόκολλα, τότε απαιτείται η αποθήκευση στο πλινθίο ενός νέου ζεύγους κλειδιών που θα πραγματοποιεί τις διαδικασίες πρόκλησης/απάντησης.

Τέλος, σε περίπτωση κλοπής της κάρτας πολίτη υπάρχει η δυνατότητα άμεσης ανάκλησης και ενημέρωσης των συστημάτων και των υπηρεσιών προκειμένου να μην υπάρχει πρόσβαση σε δεδομένα/υπηρεσίες από μη νόμιμους κατόχους.

6.3.4 Προϋποθέσεις - Υποχρεώσεις Ηλεκτρονικού Παρόχου

Ο πάροχος ηλεκτρονικής υπηρεσίας είναι ο τρίτος εμπλεκόμενος κατά την χρήση μιας κάρτας πολίτη από τον ιδιοκτήτη της. Πα να είναι σε θέση ένας πάροχος ηλεκτρονικής υπηρεσίας να προσπελαύνει τα στοιχεία των καρτών πολίτη πρέπει να αυθεντικοποιηθεί και ο ίδιος στο σύστημα αυθεντικοποίησης της Κάρτας Πολίτη, αφού έχει παραθέσει τις κατάλληλες εξηγήσεις και διασφαλίσεις για την ορθή χρήση των προσωπικών δεδομένων του πολίτη που πρόκειται να περιέλθουν στη διάθεσή του.

Τα στάδια που ακολουθεί ένας Πάροχος είναι τα εξής:

1. Ο πάροχος αιτείται την συμμετοχή του στο σύστημα αυθεντικοποίησης με τον σκοπό ένταξής του, το είδος της παρεχόμενης υπηρεσίας και τα δεδομένα πολιτών που απαιτούνται για την

παροχή υπηρεσίας. Η αίτηση κοινοποιείται και στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

2. Το σύστημα αυθεντικοποίησης Κάρτας Πολίτη καταγράφει τον ρόλο και τον πάροχο σε αντίστοιχο μητρώο και ενημερώνει την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Στην συνέχεια χορηγεί τον αντίστοιχο ρόλο πρόσβασης των δεδομένων στον πάροχο και παρέχει το κατάλληλο ψηφιακό πιστοποιητικό.
3. Ο πάροχος εγκαθιστά το κατάλληλο ενδιάμεσο λογισμικό «επικοινωνίας» (middleware) στον εξυπηρέτη του, ώστε να μπορούν να αυθεντικοποιηθούν οι χρήστες και να είναι εφικτές οι απαραίτητες ενημερώσεις του παρόχου από πλευράς συστήματος αυθεντικοποίησης Κάρτας Πολίτη.
4. Σε περίπτωση τροποποίησης ή παροχής νέων υπηρεσιών ο πάροχος πρέπει να ενημερώσει εκ νέου το μητρώο και να ακολουθηθούν τα βήματα 1-3.

6.4 Εξέλιξη Ηλεκτρονικής Διακυβέρνησης

Παρόλο που το ηλεκτρονικό διαβατήριο της Κάρτας Πολίτη δεν είναι ακόμη διαθέσιμο στους πολίτες (διατίθεται σε υπαλλήλους του Υπουργείου Δημοσίας Τάξης και Προστασίας του Πολίτη), υπάρχει πλήθος ηλεκτρονικών υπηρεσιών. Οι παρεχόμενες ηλεκτρονικές υπηρεσίες χρησιμοποιούν ως μέθοδο αυθεντικοποίησης την χρήση ονομάτων χρηστών και συνθηματικών. Δυστυχώς, η πολιτική συνθηματικών δεν προσδίδει την μέγιστη ασφάλεια [158].

Τον Μάρτιο του 2012 εκδόθηκε από το Υπουργείο Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης το Πλαίσιο Ψηφιακής Αυθεντικοποίησης (εφεξής ΠΨΑ), ένα κείμενο που αναλύει την κατηγοριοποίηση των δεδομένων που επεξεργάζονται οι ηλεκτρονικές υπηρεσίες, τον καθορισμό των επιπέδων εμπιστοσύνης, την σύνδεση των επιπέδων εμπιστοσύνης με τις κατάλληλες διαδικασίες εγγραφής και πολιτικές αυθεντικοποίησης. Το πλαίσιο απευθύνεται στο κοινό που χρησιμοποιεί υπηρεσίες ηλεκτρονικής διακυβέρνησης, αλλά και στους φορείς της Δημόσιας Διοίκησης. Στόχος της κατανόησης του περιεχομένου του Πλαισίου και της υιοθέτησης των πρακτικών του είναι η βελτίωση της ασφάλειας των ηλεκτρονικών συναλλαγών [154].

Λίγο νωρίτερα όμως, τον Οκτώβριο του 2009 είχε συσταθεί Ομάδα Ηλεκτρονικής Διακυβέρνησης στο γραφείο του Πρωθυπουργού, με στόχο την ανάπτυξη δράσεων και εφαρμογών για τον καλύτερο συντονισμό της Δημόσιας Διοίκησης, την μείωση δαπανών με την κινητοποίηση των διαθέσιμων πόρων

και την γενική συνεισφορά στο συντονισμό κεντρικών δράσεων σε θέματα Τεχνολογιών Πληροφορικής και Επικοινωνιών.

Οι δράσεις που αναπτύχθηκαν είναι ιδιαίτερα σημαντικές και συμβάλουν στην καθημερινή βελτίωση της Δημόσιας Διοίκησης. Στις δράσεις αξιοποιούνται οι υπάρχουσες υποδομές και ανθρώπινο δυναμικό του Δημοσίου Τομέα και εξυπηρετούν θέματα δαπανών, εσόδων, διαφάνειας και συμμετοχής, θεσμικών παρεμβάσεων, μεταφοράς τεχνογνωσίας, παρακολούθησης κυβερνητικού έργου και υποδομών. Το πρόγραμμα Δι@ύγεια, το επιχειρησιακό σχέδιο εφαρμογής του Νόμου 3979/2011, η απογραφή των μισθοδοτούμενων του δημοσίου τομέα, το πρόγραμμα «ΑΓΟΡΑ», ο σχεδιασμός, η υλοποίηση, η επιχειρησιακή υποστήριξη της δράσης για την Ανοικτή Διακυβέρνηση, η διάθεση ανοικτών δεδομένων της Δημόσιας Διοίκησης, η δικτύωση και συνεργασία των στελεχών του δημοσίου είναι ορισμένες από τις σημαντικές δράσεις της Ομάδας ΗΔ [158].

Τον Μάο του 2013 εκδόθηκαν τα αποτελέσματα της έρευνας για την «Εξέλιξη των 20 βασικών ηλεκτρονικών υπηρεσιών στην Δημόσια Διοίκηση» από την Κοινωνία της Πληροφορίας. Στην έρευνα αποτυπώνεται η εξέλιξη για 12 υπηρεσίες προς τους πολίτες και 8 υπηρεσίες προς τις επιχειρήσεις. Οι υπηρεσίες αυτές αξιολογούνται σε ευρωπαϊκό επίπεδο βάσει κοινής μεθοδολογίας ώστε να μπορεί να υπάρχει μια σύγκριση μεταξύ των κρατών. Συγκεκριμένα καταγράφεται ο βαθμός αξιολόγησης μας ηλεκτρονικής υπηρεσίας σε σχέση με το επίπεδο παροχής υπηρεσιών. Από τα αποτελέσματα της έκθεσης διαπιστώνεται ότι 7 από τις 20 βασικές υπηρεσίες Ηλεκτρονικής Διακυβέρνησης πέτυχαν το ανώτατο επίπεδο. Δυστυχώς όμως η επίδοση της χώρας σχετικά με το ποσοστό παροχής ολοκληρωμένων υπηρεσιών σε πολίτες και επιχειρήσεις εντός της Ευρωπαϊκής Ένωσης ήταν χαμηλή με αποτέλεσμα η χώρα μας να κατατάσσεται στην τελευταία θέση [122]. Στα αρνητικά αποτελέσματα περιλαμβάνεται και η υστέρηση της Ελλάδας στο 72% των δεικτών του Ευρωπαϊκού ψηφιακού θεματολογίου. Είναι χαρακτηριστικό το γεγονός ότι ποσοστό 41,9%ο δεν έχει χρησιμοποιήσει ποτέ το Διαδίκτυο.

Συμπέρασμα

Παρά τις προσπάθειες για στροφή προς τις ηλεκτρονικές υπηρεσίες χρειάζεται πολύς δρόμος για να είναι διαθέσιμα τα απαιτούμενα συστήματα και ακολούθως να πειστούν οι πολίτες ώστε να χρησιμοποιούν το πλήθος των παρεχόμενων ηλεκτρονικών υπηρεσιών. Στην παρούσα φάση η Ελλάδα κινείται στην Στρατηγική για την Ηλεκτρονική Διακυβέρνηση 2014 - 2020 με όραμα για εφαρμογή των αρχών της Διαλειτουργικότητας, συμμόρφωσης των ηλεκτρονικών υπηρεσιών, ενοποίησης, εξοικονόμησης πόρων και μοναδικής καταχώρησης δεδομένων, βιωσιμότητας, διαφάνειας, ανάκτησης εμπιστοσύνης, προσβασιμότητας, ασφάλειας, ιδιωτικότητας και φυσικά της απαραίτητης συμμετοχής των πολιτών. Απομένει να αποτιμήσουμε το αποτέλεσμα του συνολικού εγχειρήματος.

Κεφάλαιο 7

Επίλογος

Η μελέτη αυτή ήταν ένα γρήγορο ηλεκτρονικό ταξίδι με ένα ψηφιακό διαβατήριο, την ηλεκτρονική κάρτα. Ξεκίνησε με την αναφορά της ανάγκης των ανθρώπων να ταυτοποιούνται από τα αρχαία χρόνια, έδωσε μια περιγραφή των εντύπων ταυτοποίησης και πέρασε στην ανάλυση των επιλογών ταυτοποίησης πολιτών από τα ευρωπαϊκά κράτη και στους τρόπους μοναδικής αναγνώρισής τους.

Στην συνέχεια, αναφέρθηκαν οι ευρωπαϊκές οδηγίες που εκδόθηκαν από την Ευρωπαϊκή Ένωση προκειμένου να επιστήσουν την προσοχή και την ανάγκη σύγκλισης στην ανάπτυξη ενός ψηφιακού τρόπου συναλλαγών από τα κράτη μέλη και αναλύθηκε η Ηλεκτρονική Διακυβέρνηση όπου δόθηκε έμφαση στις δύο μεγάλες ιδιαιτερότητες : της Διαλειτουργικότητας και της Ιδιωτικότητας. Στην πορεία της μελέτης αναπτύχθηκαν οι πολιτικές αυθεντικοποίησης των πολιτών και τα δεδομένα της Ελληνικής πραγματικότητας.

Στις επόμενες ενότητες δίνονται τα συμπεράσματα της μελέτης και μια νότα για το όραμα της Ευρώπης στο ζήτημα της ηλεκτρονικής ταυτοποίησης και Διακυβέρνησης. Ως τελευταία γεύση, σκεφτόμενη την Ευρωπαϊκή Ένωση ως τον Πύργο της Βαβέλ, η απαίτηση είναι η ύπαρξη κοινής γλώσσας. Στην δική μας περίπτωση, μιας διαλειτουργικής λύσης για την ταυτοποίηση των Ευρωπαίων πολιτών στις συναλλαγές τους με την Ηλεκτρονική Διακυβέρνηση στα κράτη-μέλη.

7.1 Αποτίμηση μελέτης

Από τη μελέτη της έρευνας διαπιστώνεται ότι όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης διαθέτουν μηχανισμούς φυσικής ταυτοποίησης των πολιτών, όπου αναγράφονται τα προσωπικά στοιχεία των πολιτών. Με την αλματώδη τεχνολογική εξέλιξη, τα κράτη μέλη προσάρμοσαν τα φυσικά μέσα ταυτοποίησης σε μια ηλεκτρονική μορφή, ώστε να μπορούν οι πολίτες να ταυτοποιούνται ψηφιακά.

Η ηλεκτρονική ταυτότητα, με την μορφή μιας έξυπνης κάρτας αποτέλεσε το ψηφιακό διαβατήριο των πολιτών προκειμένου να απλοποιηθούν οι συναλλαγές τους με την Δημόσια Διοίκηση. Στην Ευρωπαϊκή Ένωση, 24 από τα 28 κράτη μέλη υποχρεώνουν τους πολίτες να ταυτοποιούνται σε ένα ηλεκτρονικό σύστημα ταυτοποίησης και να υπογράφουν ψηφιακά τις συναλλαγές τους, ενώ τα 23 από τα 28 κράτη μέλη διατηρούν μοναδικά αναγνωριστικά ταυτοποίησης.

Παρόλο που παρατηρείται πολυμορφία στις υλοποιήσεις των καρτών των κρατών της Ευρώπης, όπως προκύπτει από τον πίνακα 2.3 η πλειοψηφία των χωρών παρέχει ψηφιακή αυθεντικοποίηση και δυνατότητα ψηφιακής υπογραφής. Η διάρκεια ισχύος της ηλεκτρονικής κάρτας και το είδος της διεπαφής του χρησιμοποιούμενου πλινθίου εξαρτάται από την πολιτική που ακολουθείται.

Αντίστοιχη πολυμορφία παρουσιάζεται και την περίπτωση χρήσης μοναδικών αναγνωριστικών, εκτός της περίπτωσης της Γερμανίας η οποία δεν έχει μοναδικό αναγνωριστικό για τον πολίτη και χρησιμοποιεί τομεακά αναγνωριστικά.

Στις περισσότερες περιπτώσεις οι κάρτες περιλαμβάνουν βιομετρικά στοιχεία των πολιτών, αλλά διαφορετικής μορφής για κάθε κράτος. Στις περιπτώσεις που τηρούνται δακτυλικά αποτυπώματα, αυτό γίνεται με την συγκατάθεση του πολίτη.

Η διαλειτουργικότητα μεταξύ των συστημάτων και υπηρεσιών βρίσκεται σε νηπιακό επίπεδο. Πέραν της περίπτωσης υποστήριξης της διαλειτουργικότητας κατά τη χρήση της ηλεκτρονικής ταυτότητας ως ταξιδιωτικό έγγραφο (όπως καθορίζει ο ICAO), η Αυστρία αποτελεί το παράδειγμα - υπόδειγμα. Στην Αυστρία, υποστηρίζεται η διαλειτουργικότητα για συστήματα προερχόμενα από το Βέλγιο, την Εσθονία, την Φινλανδία και την Ιταλία χρησιμοποιώντας την τεχνολογία MOA (Module for Online Application), όπου το ρόλο του Διαχειριστή αναλαμβάνει το

Κεντρικό Μητρώο Κατοίκων, ενώ οι μη-Αυστριακοί παρακολουθούνται από το Συμπληρωματικό μητρώο, χρησιμοποιώντας ως SourcePIN το μοναδικό αναγνωριστικό της χώρας προέλευσής τους.

Για το ζήτημα τήρησης μητρώων ταυτοτήτων η κουλτούρα της διαφορετικότητας των Ευρωπαίων είναι ευδιάκριτη. Οι Γερμανοί πολίτες είναι αντίθετοι στην ύπαρξη ενός κεντρικού μητρώου ταυτοτήτων, ενώ οι Φιλανδοί τηρούν και επικαιροποιούν τα στοιχεία τους που είναι αποθηκευμένα στο κεντρικό μητρώο πολιτών.

Ένα άλλο σημείο που χρήζει βελτίωσης είναι η χρήση συστημάτων αυθεντικοποίησης. Τα κράτη μέλη έχουν συστήματα που στηρίζονται σε πολιτικές χρήσης συνθηματικών μιας χρήσης, two-factor και συνθηματικά οθόνης «time based». Οι 15 χώρες σε σύνολο 19 κρατών μελών χρησιμοποιούν μονοδιάστατα συστήματα, ενώ το Βέλγιο, η Εσθονία, η Λιθουανία και η Φινλανδία χρησιμοποιούν πολυδιάστατα συστήματα. Ζώντας στην εποχή της κινητής τηλεφωνίας και του υπολογιστικού νέφους (cloud computing) θα πρέπει οι πολίτες να μπορούν να στραφούν σε ενισχυμένα διακριτικά, τουλάχιστον δύο παραγόντων.

Σχετικά με την ανάμιξη του ιδιωτικού τομέα στο πλαίσιο διαχείρισης των ηλεκτρονικών ταυτοτήτων, σε 15 από τα 28 κράτη υπάρχει ανάμιξη του ιδιωτικού τομέα. Ως αποτέλεσμα τα δεδομένα των πολιτών είναι στην διάθεση ιδιωτικών εταιριών, γεγονός που εγκυμονεί κινδύνους διαρροής των προσωπικών δεδομένων των χρηστών.

Η έρευνα διαπιστώνει ότι πολλά κράτη μέλη κινούνται από ένα αποκεντρωμένο μοντέλο προς σε ένα ολοκληρωμένο ενοποιημένο προκειμένου να αυξηθεί η αποδοτικότητα και η αποτελεσματικότητα των υπηρεσιών Ηλεκτρονικής Διακυβέρνησης. Επιθυμητή είναι η πρόσβαση στις ηλεκτρονικές υπηρεσίες μέσα από μια ενιαία πύλη, ανεξάρτητα από το ποια κυβερνητική εξουσία τις παρέχει. Η συγκέντρωση αυτή συντελεί σε ένα σύστημα διακυβέρνησης με διαφάνεια και ευελιξία.

7.2 Ευρωπαϊκό όραμα

Η Πολιτεία προσφέρει την δυνατότητα ηλεκτρονικών υπηρεσιών, με στόχο την ταχύτατη διεκπεραίωση των συναλλαγών τους με την Δημόσια Διοίκηση και την βέλτιστη εξυπηρέτηση χωρίς την φυσική τους παρουσία στους αντίστοιχους φορείς.

Ακολουθώντας τις συστάσεις της Ευρωπαϊκής Ένωσης, οι ηλεκτρονικές υπηρεσίες δεν αρκεί να προσφέρονται εντός των συνόρων των κρατών, αλλά εντός των συνόρων της κοινότητας των μελών, γεγονός που δεν ακολουθείται. Αλλαγή πλεύσης λοιπόν προς την Διαλειτουργικότητα, με την οποία αξιοποιούνται οι πληροφορίες από τις Δημόσιες υπηρεσίες σε τοπικό και εθνικό επίπεδο με στόχο την διασυνοριακή εξυπηρέτηση των πολιτών.

Παράλληλα, η χρήση των υπηρεσιών Ηλεκτρονικής Διακυβέρνησης συνεπάγεται ανταλλαγή πληροφοριών από πλευράς των πολιτών, οι οποίες εξαρτώνται από το είδος της παρεχόμενης υπηρεσίας, οπότε ελλοχεύουν κίνδυνοι για την Ιδιωτικότητα των πολιτών. Για το λόγο αυτό είναι αναγκαία η ύπαρξη πρόσθετων μηχανισμών που θα ενισχύουν την Ιδιωτικότητα των στοιχείων των πολιτών στις παρεχόμενες υπηρεσίες.

Η Ευρωπαϊκή Επιτροπή έχει θεσπίσει οδηγίες που στην συνέχεια τα κράτη μέλη εναρμόνισαν στο εθνικό θεσμικό πλαίσιο. Πλέον, το θεσμικό πλαίσιο της Ευρωπαϊκής Ένωσης συμπληρώνεται με την πρόσφατη ψήφιση του κανονισμού eIDAS, προκειμένου να θεμελιωθεί περαιτέρω η ολοκλήρωση της εσωτερικής αγοράς και να οικοδομηθεί μια γερή βάση εμπιστοσύνης στις ηλεκτρονικές συναλλαγές των πολιτών. Οι αρχές της διαφάνειας, της λογοδοσίας και της αξιοπιστίας ως ελάχιστες υποχρεώσεις των Παρόχων Υπηρεσιών Εμπιστοσύνης, η τεχνολογική ανεξαρτησία των υπηρεσιών και η σύγκλιση με τους κανόνες της αγοράς, καθώς και η ενημέρωση του πολίτη με την εξέλιξη της πορείας των αιτημάτων του σε μια ηλεκτρονική συναλλαγή οδηγούν σε ένα μεγαλύτερο ποσοστό εμπιστοσύνης από πλευράς του.

Η βελτιστοποίηση του θεσμικού πλαισίου, η χάραξη νέων στρατηγικών από πλευράς των κρατών με στήριξη της διαλειτουργικότητας, η υλοποίηση πλήθους έργων από τα κράτη μέλη της Ευρωπαϊκής Ένωσης με την εμπλοκή επιχειρήσεων και ακαδημαϊκών ιδρυμάτων υπερασπιζόμενα την διαφύλαξη της Ιδιωτικότητας, καθώς και η σταθερή προσπάθεια της Ελληνικής Κυβέρνησης να ακολουθεί ανοδική πορεία για την ανάπτυξη ασφαλών ηλεκτρονικών υπηρεσιών, θα συμβάλουν στην πολυπόθητη ανάπτυξη της εσωτερικής αγοράς της Ευρωπαϊκής Ένωσης.

Και όπως εύστοχα σημειώνει η Μελέτη των Ηνωμένων Εθνών για την Ηλεκτρονική Διακυβέρνηση, για επιτευχθούν τα παραπάνω οφέλη απαιτείται επαρκής χρηματοδότηση, αλλά τα Ευρωπαϊκά κράτη έχουν αντίληψη και το πράττουν. Το πιο σημαντικό στοιχείο όμως είναι η συμμετοχή και η εμπιστοσύνη του πολίτη στην ηλεκτρονικές υπηρεσίες. Ζώντας πια στην εποχή της κινητής τηλεφωνίας και του υπολογιστικού νέφους όλα εναρμονίζονται με τις υπηρεσίες ΗΔ. Απαιτείται όμως και η κατάλληλη υποστήριξη προς τους πολίτες για να αυξήσουν την προσβασιμότητα τους στις συστήματα eIDM.

Τελικά, σήμερα, ο βαθμός αξιοποίησης των υπηρεσιών Ηλεκτρονικής Διακυβέρνησης βαίνει αυξανόμενος, το σταθερό όραμα περιλαμβάνει την αυξανόμενη συμμετοχή των πολιτών σε χρήσιμες, φιλικές και αποτελεσματικές υπηρεσίες.

Βιβλιογραφία

[01] Arduini Davide, Zanfei Antonello, Denni Mario, Giungato Gerolamo, «The eGovernment Services Delivery of the Italian Municipalities, Springer Link

- [02] Bj ones Ronny, Krontiris Ioannis, Paillier Pascal, Rannenber Kai, «Integrating Anonymous Credentials with eID for Privacy respecting online Authentication», Digital Agenda, 2012, <http://ec.europa.eu/digital-agenda/futurium/en/content/integrating-anonymous-credentials-eids-privacy-respecting-online-authenticatim>
- [03] Cartledge Paul, «Θεατρικά Έργα με βάθος: το θέατρο ως διαδικασία στην ζωή των πολιτών της αρχαίας Ελλάδας», http://www.cup.gr/Downloads/PDF/tragedy_ch01.pdf
- [04] Castro Daniel, "Explaining International Leadership: Electronic Identification Systems", The Information Technology & Innovation Foundation (ITIF), September 2011, <http://www.itif.org/files/2011-e-id-report.pdf>
- [05] DuraCi Vladimir, Balogh Tomas, Sevcfk Michal, Kiefer Peter, «2014: the year of the Slovakian eID», SILICON TRUST, 13 November 2013, <http://silicontrustwordpress.com/2014/03/31/2014-the-year-of-the-slovakian-eid/>
- [06] Costin N. Hariton, Ciocoiu Iulian, Barbu Tudor, Rotariu Cristian, «Through Biometric Card in Romania: Person Identification by Face, Fingerprint and Voice Recognition», World Academy of Science, Engineering and Technology, International Journal of Computer, Information Science and Engineering, Vol:2 No:5,2008 <http://wasetorg/publications/8832/through-biometric-card-in-romania-person-identification-by-face-fingerprint-and-voice-recognitio>
- [07] Drogkaris P., Gritzalis S, Lambrinouidakis C., "Employing Privacy Policies and Preferences in Modern e-Government Environments", Special Issue on "Security and Privacy of E-Government Applications and Services" of the International Journal of Electronic Governance, 2013, Inderscience Publishers
- [08] Drogkaris P., Gritzalis S, Lambrinouidakis C., "An Hierarchical Multitier Approach for Privacy Policies in e-Government Environments", the International Journal of Electronic Governance, (Under Review), Inderscience Publishers
- [09] EDRI, «E1ectronic identities al1 over the EU?», 23 May 2012, <https://edri.org/edri-gram/edrigramnumber10-10/>
- [10] ENISA «Mapping security services to authentication levels, Reflecting on STORK QAA 1evels», <https://www.eid-stork.eu/dmdocuments/pub1ic/mapping.pdf>

- [11] ENISA, «Security Issues in Cross Border E1ectronic Authentication»,
http://www.enisa.europa.eu/act/it/eid/xborderauth/at_download/fullReport
- [12] E-SENS, <http://www.esens.eu/home/>
- [13] Espinosa Garcia, Javier, Hernandez Encinas Luis, Queiruga Dios, Arace1i, "The new Spanish e1ectronic identity card: DNI-e". International Conference on Information Technologies (InfoTech-2007).
 vo11: Techno1ogica1 Aspects of the e-Governance and Data Protection. ISBN 978-954-9518-41-2.14
 May 2011.
- [14] European Committee of Standardization, «Identification card systems - European Citizen Card - Part
 1: Physica1, e1ectrica1 and transport proto1 characteristics (CEN/TS 15480 ECC)», 18 June 2012
- [15] European Interoperability Framework for Pan-European eGovernment
 Services, <http://www.e-gif.gov.gr/porta1/pls/porta1/docs/1/210659.PDF>
- [16] FIDIS, <http://www.fidis.net/about/>
- [17] Fritsch Lothar, «FutureID - Shaping the future of e1ectronic identity»,
<http://www.nr.no/nb/projects/fu1tjreid-shaping-fu1tjre-elec^onic-iden1:it>. 04 January 2013
- [18] Georges Jean-Noe1, «Nationa1 ID Cards and E1ectronic Identity Documents: Route to
 Success», Frost & SuHivan, 15 March 2011,
http://www.s1ideshare.net/FrostandSullivan/nationa1-id-car_ds-and-e1ectronic-identiry-documentsroute-to-success
- [19] Graux Hans, «E1ectronic Identification and Trust Services (eIDAS) Regu1ation Nears
 Comp1etion», Time.1ex, 31 March 2014
- [20] Gronlund A., «Electronic identity management in Sweden: governance of a market approach»,
 Springer Link, July 2010, Volume 3, Issue 1, pp 195-211, 9 March 2010
- [21] Gus Hosein, Edgar A. Whitey, Global Challenges for Identity Policies, Basingstoke Palgrave
 Macmillan 2010
- [22] IDABC European eGovernment Services, «eID Interoperability for PEGS: Update of Country
 Profiles study Slovenian country profile», August
 2009, <http://ec.europa.eu/idabc/servlets/Docdf6b.pdf?id=32292>

- [23] IDABC, <http://ec.europa.eu/idabc/servlets/Doc60efpdf?id=32115>
- [24] International Standards Organization, ISO/IEC 27000:2009, «Information Technology -Security Techniques - Information security management systems - Overview and vocabulary», http://www.iso.org/iso/catalogue_detail?csnumber=41933
- [25] International Standards Organization, ISO/IEC 7810:2003, «Identification cards - Physical characteristics», 03 March 2010, [http://www.iso.org/iso/catalogue/catalogue tc/catalogue detailhtm?csnumber=3143 2](http://www.iso.org/iso/catalogue/catalogue%20tc/catalogue_detail.htm?csnumber=31432)
- [26] Leuven K.U., eGovernment Unit, «Modinis Study on Identity Management in eGovernment», DG Information Society and Media European Commission, 6 June 2006 [https://www.cosic.esatku1euven.be/modinis-idm/twiki/pub/Main/ProjectDocs/modinis.D3.5 Identity Management Initiative Report 1 IIR1.pdf](https://www.cosic.esatku1euven.be/modinis-idm/twiki/pub/Main/ProjectDocs/modinis.D3.5%20Identity%20Management%20Initiative%20Report%201%20IIR1.pdf)
- [27] Lyon David, "Surveillance as Social Sorting, Privacy, risk, and digital discrimination", Routledge London and New York
- [28] Martin Zack, «Poland's eID programs bodes well for smart card industry», SecureIDNews, <http://secureidnews.com/news-item/polands-eid-programs-bodes-wdl-for-smart-card-industry/>
- [29] MODINIS, Nationa1 profile for eGovernIDM initiatives in the Czech Repub1ic, 2005-2014, Modinis-IDM consortium, <https://www.cosic.esatku1euven.be/modinis-idm/twiki/bin/view.cgi/Main/CzechProfile>
- [30] Morrison Peter, "The Comp1icated Rise of the e1ectronic identity card in Europe", myeurop.info, 06/04/2012, <http://en.myeurop.info/2012/04/06/comp1icated-rise-e1ectronic-identity-card-europe-5145>
- [31] OECD (2011), «Nationa1 Strategies and Po1icies for Digita1 Identity Management in OECD Countries", OECD Digita1 Economy Papers, No. 177, OECD Publishing **Error! Hyperlink reference not valid.**
- [32] OpenPeppo1, <http://www.peppo1.eu/about%20peppo1/about-openpeppo1-1>

- [33] Persona1 Identification Documents Law, J Straume, 5 June 2002
- [34] Prime And Identity Management in Europe, <https://www.prime-project.eu/>
- [35] Securenet, «Best So1utions for Biometrics and eID»,
http://www.p1anetbiometrics.com/creo_files/upload/artic1e-fiTes/secunet_best_so1utions_for_biometrics_and_eid.pdf
- [36] Sheahan Fionnah , «New ID cards to be used in we1fare fraud c1ampdown»,
<http://www.independentie/irish-news/new-id-cards-to-be-used-in-we1fare-fraud-c1ampdown-29209183.html> Independentie, 20 Apri12013
- [37] Smith Anthony, London Schoo1 of Economics, "Set in the Si1ver Sea: English Nationa1 Identity and European Integration", Centre for the Study of Democratic Government, 13 May 2005, http://oxpo.po1itics.ox.ac.uk/materials/nationa1_identity/Smith_Paper.pdf
- [38] SPOCS, http://www.eu-spocs.eu/indexphp?option=com_content&view=artic1e&id=1&Itemid=42
- [39] SSEIDC, «Bui1ding a Thematic Network for European ID» <http://www.eid-ssedic.eu/>
- [40] STORK, «Πιλοτικό 1: Διασυνοριακή αυθεντικοποίηση για ηλεκτρονικές υπηρεσίες», https://www.eid-stork.eu/pilots/pilot1_GR_more.htm
- [41] STORK, https://www.eid-stork.eu/pilots/faq_GR.htm
- [42] STORK 2.0, https://www.eid-stork2.eu/index.php?option=com_content&view=article&id=27:electronic-identity-card-available-from-april-2012-in-latvia&catid=3:latest-news&Itemid=38
- [43] Sevcik Michal, Hewlett-Packard,« Can eID card make life easier and more secure?», 9 November 2010, <http://www.itapa.sk/data/att/599.pdf>
- [44] Travis Alan, «ID cards scheme to be scrapped within 100 days»

<http://www.theguardian.com/politics/2010/may/27/theresa-may-scrapping-id-cards>, Theguardian,
27 May 2010

[45] Travis Alan, «European citizens in Britain will be charged for ID cards»,

<http://www.theguardian.com/politics/2013/feb/25/eu-citizens-britain-id-cards>, Theguardian, 25
February 2013

[46] United Nations E-Government Survey 2012, United Nations Department of Economic and Social

Affairs, <http://www.un.org/en/development/desa/publications/connecting-governments-to-citizens.html>

[47] Teemu Rissanen, «Electronic identity in Finland: ID cards vs. bank IDs», SpringerLink July 2010,

Volume 3, Issue 1, pp 175-194,

http://download.springer.com/static/pdf/853/art%253A10.1007%252Fs12394-010-0049-8.pdf?auth66=1398125446_6f9d7e7721019bed786adfbde2ec8d79&ext=.pdf

[48] UL Transaction Security's Data Security, «Electronic Identities in Europe

White», <http://www.ul-ts.com/downloads/whitepapers/finish/6-whitepapers/114-electronic-identities-in-europe>

[49] Vashisht Deepti, «The magic of Sweden's personal ID number», The Local, 04 April

2014, <http://www.thelocal.se/20140404/the-personnummer-waved-a-magic-wand-over-my-life-in-swedert>

[50] VejaČka Martin, «Utilization of Electronic Signature in Slovak Banks», Department of applied

mathematics and business informatics Faculty of Economics, Technical university of Kosice, 25-29
March 2013, <http://www.ictic.sk/archive/7vid-l&aid=3&kid=50201-96&q=fl>

[51] Vipinwest, "Schengen Area, Europe and Latvia, Legal and

Regulation", <http://yipinwest.com/residence-permit/>

[52] Vrankulj Adam, «Infineon to supply security controllers for Slovakian eID

cards», [BiometricUpdate.com](http://www.biometricupdate.com), 24 January 2014,

<http://www.biometricupdate.com/201401/infineon-to-supply-security-contrdlers-for-slovakian-eid-cards>

[53] Wikipedia, «Βαθμός Διαλειτουργικότητας»,

[http://en.wikipedia.org/wiki/European Interoperability Framework](http://en.wikipedia.org/wiki/European_Interoperability_Framework)

[54] Wikipedia, <http://en.wikipedia.org/wiki/EUCARK>

[55] Wikipedia, «Electronic Identity Card»,

[http://en.wikipedia.org/wiki/Electronic identity card](http://en.wikipedia.org/wiki/Electronic_identity_card)

[56] Wikipedia, «Identity document», [[http://en.wikipedia.org/wiki/Identity document](http://en.wikipedia.org/wiki/Identity_document)

[57] Wikipedia, «List of identity card policies»,

[http://en.wikipedia.org/wiki/List of identity card policies by country](http://en.wikipedia.org/wiki/List_of_identity_card_policies_by_country)

[58] Wikipedia, «Multi - Factor Authentication^ [http://en.wikipedia.org/wiki/Multi-factor authentication](http://en.wikipedia.org/wiki/Multi-factor_authentication)

[59] Wikipedia, «National Identity Cards in the European Union»,

[http://en.wikipedia.org/wiki/National identity cards in the European Union](http://en.wikipedia.org/wiki/National_identity_cards_in_the_European_Union)

[60] Wikipedia, «National Identification Numbers»,

[http://en.wikipedia.org/wiki/National identification number#Netherlands](http://en.wikipedia.org/wiki/National_identification_number#Netherlands)

[61] Wikipedia, ^Personal Identification numbers,

[http://en.wikipedia.org/wiki/Personal identification number %28Denmark%29](http://en.wikipedia.org/wiki/Personal_identification_number_%28Denmark%29)

[62] Wikipedia, «Strong Authentication», [http://en.wikipedia.org/wiki/Strong authentication](http://en.wikipedia.org/wiki/Strong_authentication)

[63] Αγρότης Κώστας, «Ηλεκτρονική Διακυβέρνηση στην Τοπική Αυτοδιοίκηση», Τμήμα Υπηρεσιών Πληροφορικής, Κύπρος, Μάιος 2011

[64] Αντωνάκου Αικατερίνη, «Η διαμόρφωση της πολιτικής κουλτούρας στην Ελλάδα: Ο τύπος του Έλληνα πολίτη», Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών, 2008 [http://www.dlinika.org.nz/file.php/3/Antonakou Katerina 0 typos toy Ellina politi.pdf](http://www.dlinika.org.nz/file.php/3/Antonakou_Katerina_0_typos_toy_Ellina_politi.pdf)

[65] Γκρίτζαλης Σ., Λαμπρινουδάκης Κ., Κάτσικας Σ., Μήτρου Λ., «Προστασία της ιδιωτικότητας και τεχνολογίες πληροφορικής και επικοινωνιών», Εκδόσεις Παπασωτηρίου

- [66] Γκρίτζαλης Στέφανος, «Εισαγωγικά Θέματα και Εννοιολογική θεμελίωση κατά ISO 27000:2009», Σημειώσεις Ασφάλειας Πληροφοριακών και Επικοινωνιακών Συστημάτων, Πανεπιστήμιο Αιγαίου, Σεπτέμβριος 2013
- [67] Γκρίτζαλης Στέφανος, Σημειώσεις «Εισαγωγή στην Κρυπτογραφία και Υποδομή Δημοσίων κλειδιών», Ανοικτό Πανεπιστήμιο Κύπρου, Μάιος 2013
- [68] Γκρίτζαλης Στέφανος, «Ασφάλεια και Προστασία της Ιδιωτικότητας σε Περιβάλλοντα Ηλεκτρονικής Διακυβέρνησης», Ανοικτό Πανεπιστήμιο Κύπρου, Μάιος 2013
- [69] Δρογκάρης Προκόπιος, «Ασφάλεια και Προστασία της Ιδιωτικότητας σε Πληροφοριακά Συστήματα Ηλεκτρονικής Διακυβέρνησης», Πανεπιστήμιο Αιγαίου, Σάμος, 2013
- [70] Ζούλοβιτς Μ., Σαμαρτζή Β., «Εγγραφή σε υπηρεσίες Ηλεκτρονικής Διακυβέρνησης, Έννοια & πρακτική υπό το καθεστώς του ν.3979/2011», Δίκαιο Πληροφορικής, www.ethemis.gr
- [71] Ζούλοβιτς Μ., Φύλλα Α., «Ηλεκτρονική Διακυβέρνηση: Βήματα για διαλειτουργικότητα και ασφάλεια», it Professional security, Τεύχος 13, Νοέμβριος-Δεκέμβριος 2013, <http://www.itsecuritypro.gr/contents/article.php?id=80&cattid=6>
- [72] Καλλονιάτης Χρήστος, Σημειώσεις «Απαιτήσεις Ασφάλειας και Ιδιωτικότητας», Σημειώσεις Καλλονιάτη Χρήστου, Πανεπιστήμιο Αιγαίου, [http://www.ct.aegean.gr/people/vkavak1i/MIS/slides/Security & Privacy kal1oniatis.pdf](http://www.ct.aegean.gr/people/vkavak1i/MIS/slides/Security%20&%20Privacy%20kal1oniatis.pdf)
- [73] Καλλονιάτης Χρήστος, Σημειώσεις «Ταυτοποίηση και Αυθεντικοποίηση», Ασφάλεια Δεδομένων στην Κοινωνία της Πληροφορίας, Πανεπιστήμιο Αιγαίου
- [74] Καμπουράκη Ντίνα, «Ταυτοποίηση και Αυθεντικοποίηση», Σημειώσεις, Πανεπιστήμιο Αιγαίου, <http://www.icsd.aegean.gr/website/files/proptyxiako/185755266.pdf>
- [75] Κουντζέρης Α., «Ηλεκτρονική ταυτότητα πολιτών και επιλογές πολιτικής & υποδομών -η Ευρωπαϊκή εμπειρία», Παρατηρητήριο για την Κοινωνία της Πληροφορίας, Ιούνιος 2010, <http://www.observatory.gr/files/meletes/eID%20Status%20&%20Citizen%20benefits%20Er> **ror! Hyperlink reference not valid.**
- [76] Κιοσσέ Ελισάβετ, «Η πορεία της Ηλεκτρονικής Διακυβέρνησης στις χώρες της Ε.Ε. και την Ελλάδα - Οι επιδόσεις των χωρών», Πανεπιστήμιο Μακεδονίας, Θεσσαλονίκη, 2011

- [77] Λαζαρίδης Σ., «Ανάλυση πολιτικών και πρακτικών εθνικής ηλεκτρονικής ταυτότητας eID στην Ευρώπη», Πανεπιστήμιο Αιγαίου, Φεβρουάριος 2011
- [78] Λαμπρινουδάκης Κ., Μήτρου Ε., Γκρίτζαλης Σ., Κάτσικας Κ. (Επιμέλεια Έκδοσης), «Προστασία της Ιδιωτικότητας στις Τεχνολογίες της Πληροφορικής και των Επικοινωνιών: Τεχνικά και Νομικά Θέματα», Εκδόσεις Παπασωτηρίου, Αθήνα, 2009
- [79] Λαμπρινουδάκης Κώστας, «Πλαίσιο Ψηφιακής Αυθεντικοποίησης», Τεχνολογίες Ενίσχυσης Ιδιωτικότητας, Πανεπιστήμιο Πειραιώς
- [80] Λιμνιώτης Κωνσταντίνος, «Ψηφιακά Πιστοποιητικά - Ψηφιακές Υπογραφές», Σημειώσεις Κρυπτογραφίας, Ανοιχτό Πανεπιστήμιο Κύπρου, Νοέμβριος 2013
- [81] Μήτρου Λίλιαν, Σημειώσεις «Νομικά Ζητήματα Ηλεκτρονικών Συναλλαγών -Ηλεκτρονικές Υπογραφές», Πανεπιστήμιο Αιγαίου, Θερινό Εξάμηνο 2011
- [82] Σαρρή Κατερίνα, «Ηλεκτρονική Διακυβέρνηση : Μια ευκαιρία για καλύτερη διακυβέρνηση με επίκεντρο τον πολίτη - Η Ελληνική περίπτωση», Εθνική Σχολή Δημόσιας Διοίκησης, Κ' Εκπαιδευτική Σειρά, Αθήνα, 2010
- [83] Σπηλιωτόπουλος Αθανάσιος, «Η στρατηγική της Λισσαβώνας: Διαδικασία και λόγοι υιοθέτησης, παρουσίαση - ανάλυση, απολογισμός της προόδου και επαναθεώρηση της Στρατηγικής της Λισσαβώνας για την περίοδο 2000-2005», Πανεπιστήμιο Πειραιώς, Αθήνα, 2006 <http://digilib.lib.unipi.gr/dspace/bitstream/unipi/1377/1/Spiliotopoulos.pdf>
- [84] Σφάγγος Αλέξανδρος, «Έξυπνες κάρτες σε Εφαρμογές Ηλεκτρονικής Διακυβέρνησης», Εθνικό Μετσόβιο Πολυτεχνείο, Αθήνα, Ιούλιος 2005
- [85] Εθνικό Κέντρο Τεκμηρίωσης, Ηλεκτρονική Διακυβέρνηση, Πηγές στο Διαδίκτυο, Εθνικοί Κόμβοι, <http://www.ekt.gr/content/display?prnbr=5196>
- [86] Ευρωπαϊκή Επιτροπή, «Αριθμοί Μοναδικής Ταυτοποίησης (ΑΦΤ), οι ΑΦΜ ανά θέμα: Δομή και Περιγραφή του ΑΦΤ», 26 Ιουνίου 2013, http://ec.europa.eu/taxation_customs/tin/pdf/el/TIN-subjects-sheet-2-structure-and-specificities_el.pdf
- [87] Ευρωπαϊκή Επιτροπή, «Άρθρο για την χρήση οδοντιατρικής ηλεκτρονικής ταυτότητας eZAA», <http://www.epractice.eu/en/news/5419681>

- [88] Ευρωπαϊκή Επιτροπή, «Δώδεκα δράσεις για την τόνωση της ανάπτυξης και την ενίσχυση της εμπιστοσύνης», <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0206:FIN:en:PDF>
- [89] Ευρωπαϊκή Επιτροπή, «Εμβληματικές Πρωτοβουλίες Ευρώπη 2020», http://ec.europa.eu/europe2020/europe-2020-in-a-nutshd1/flagship-initiatives/index_el.htm
- [90] Ευρωπαϊκή Επιτροπή, Έγγραφα υπηκόων χωρών Ευρωπαϊκής Ένωσης, http://europa.eu/youreurope/citizens/travel/entry-exit/eu-citizen/index_el.htm
- [91] Ευρωπαϊκή Επιτροπή - Συμβούλιο Ευρωπαϊκής Ένωσης, «Ενοποιημένη απόδοση της Συνθήκης για την Ευρωπαϊκή Ένωση και της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης καθώς και του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης», 12 Νοεμβρίου 2012, <http://register.consilium.europa.eu/doc/srv?!=EL&f=ST%206655%202008%20REV%207>
- [92] Ευρωπαϊκή Επιτροπή, «Ευρωπαϊκή στρατηγική 2020», http://europa.eu/abc/euslides/index_el.htm
- [93] Ευρωπαϊκή Επιτροπή - IP/08/824 «Ηλεκτρονικές ταυτότητες: εύκολη πρόσβαση στις δημόσιες υπηρεσίες ανά την ΕΕ», 30 May 2008, http://europa.eu/rapid/press-release_IP-08-824_el.htm
- [94] Ευρωπαϊκή Επιτροπή, «Η ψηφιακή πρόκληση της Ευρώπης», 24-25 Οκτωβρίου 2013, http://ec.europa.eu/europe2020/pdf/20131010_el.pdf
- [95] Ευρωπαϊκή Επιτροπή, Οδηγία για την Διατήρηση των δεδομένων (2006/24/EK), 15 Μαρτίου 2006
- [96] Ευρωπαϊκή Επιτροπή, Οδηγία για την Ηλεκτρονική Ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στο εσωτερικό εμπόριο, Ευρωπαϊκή Ένωση, Ιούνιος 2012, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:EN:PDF>
- [97] Ευρωπαϊκή Επιτροπή, «Οδηγία 1999/93/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 1999, σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές»
- [98] Ευρωπαϊκή Επιτροπή, «Οδηγία για τις υπηρεσίες στην εσωτερική αγορά», 12 Δεκεμβρίου 2006

- [99] Ευρωπαϊκή Επιτροπή, Οδηγία του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, σχετικά με την ηλεκτρονική ταυτοποίηση και την εμπιστοσύνη για τις ηλεκτρονικές συναλλαγές με τις υπηρεσίες στην εσωτερική αγορά, 26 Μαρτίου 2014, <http://certifiedsignature.eu/files/2014/04/eIDAS-Regulation-Amendments-Consolidated-Text.pdf>
- [100] Ευρωπαϊκή Επιτροπή, Οδηγία για την Προστασία Ιδιωτικής Ζωής στις Ηλεκτρονικές Επικοινωνίες (2002/58/EK), 12 Ιουλίου 2002
- [101] Ευρωπαϊκό Κοινοβούλιο, «Πρόταση για την Ηλεκτρονική Ταυτοποίηση και τις Υπηρεσίες Εμπιστοσύνης στις Ηλεκτρονικές συναλλαγές στην εσωτερική αγορά», Βρυξέλλες, 04 Ιουνίου 2012, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:en:PDF>
- [102] Ευρωπαϊκή Επιτροπή, «Σχέδιο δράσης για τις ηλεκτρονικές διοικητικές υπηρεσίες στο πλαίσιο της πρωτοβουλίας i2010: Επιτάχυνση της ηλεκτρονικής δημόσιας διοίκησης στην Ευρώπη προς όφελος όλων», Βρυξέλλες, 25 Απριλίου 2006
- [103] Ευρωπαϊκή Επιτροπή, «Τι απαιτείται για να υποστηρίξετε μια Ευρωπαϊκή Πρωτοβουλία Πολιτών», <http://ec.europa.eu/citizens-initiative/files/requirements-el.pdf>
- [104] Ευρωπαϊκή Επιτροπή, «Χρηματοδότηση ύψους 13,7 εκατομμυρίων ευρώ για διασυνοριακές ψηφιακές δημόσιες υπηρεσίες ανακοίνωσε η Ευρωπαϊκή Επιτροπή», 14 Αυγούστου 2013, http://europa.eu/rapid/press-release_IP-13-778_el.htm
- [105] Ευρωπαϊκή Επιτροπή, «Χώρες Ευρωπαϊκής Ένωσης», europa.eu/about-eu/countries/index_el.htm
- [106] Ευρωπαϊκή Επιτροπή, Ψηφιακό Θεματολόγιο (Digital Agenda) για την Ευρώπη, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=com:2010:0245:fin:en:pdf>
- [107] Ευρωπαϊκή Επιτροπή, «Ψηφιακό θεματολόγιο για την Ευρώπη : βασικές πρωτοβουλίες», MEMO/10/200, 19 May 2010, [http://europa.eu/rapid/press-release MEMO-10-200_el.htm](http://europa.eu/rapid/press-release_MEMO-10-200_el.htm)
- [108] Ευρωπαϊκή Επιτροπή, Ψηφιακό Θεματολόγιο, «Ψηφιακή Ατζέντα για την Ευρώπη», <https://ec.europa.eu/digital-agenda/node/50812>

- [109] Ευρωπαϊκή Επιτροπή, Ψηφιακό Θεματολόγιο «CROBIES : Study on Cross - Border Interoperability of eSignatures 2010», 20 Σεπτεμβρίου 2012, <http://ec.europa.eu/digital-agenda/en/news/crobies-study-cross-border-interoperability-esignatures-2010>
- [110] Ευρωπαϊκή Επιτροπή, [http://europa.eu/rapid/press-release MEMO-12-403 en.htm](http://europa.eu/rapid/press-release_MEMO-12-403_en.htm)
- [111] Ευρωπαϊκή Επιτροπή, «DG Information Society and Media European Commission», 6 June 2006, [http://ec.europa.eu/taxation_customs/tin/pdf/en/TIN-country sheet HU en.pdf](http://ec.europa.eu/taxation_customs/tin/pdf/en/TIN-country_sheet_HU_en.pdf)
- [112] Ευρωπαϊκή Επιτροπή, «eID Interoperability for PEGS: Update of Country Profiles study The Netherlands country profile, July 2009», European Communities, 2009, <http://ec.europa.eu/idabc/servlets/Doc9c1a.pdf?id=32286>
- [113] Ευρωπαϊκή Επιτροπή, «EU-funded project to take biometric security systems to the next level», MEMO/13/924, 22 October 2013, <http://europa.eu/rapid/press-release MEMO-13-924 en.htm>
- [114] Ευρωπαϊκή Επιτροπή, Commission MEMO/12/403, «Electronic identification, signatures and trust services: Questions and Answers», Europa.eu, 4 June 2012, <http://europa.eu/rapid/press-release MEMO-12-403 en.htm>
- [115] Ευρωπαϊκή Επιτροπή, Certified Electronic Signature, «eIDAS - Electronic Identification and Signature (Electronic Trust Services) final draft», <http://certifiedsignature.eu/2014/03/01/eidas-electronic-identification-and-signature-electronic-trust-services-final-draft/>
- [116] Ευρωπαϊκή Επιτροπή, «Feasibility Study on a Electronic Identification, Authentication and Signature Policy (IAS)», 19 September 2013, <http://ec.europa.eu/digital-agenda/en/news/feasibility-study-electronic-identification-policy-ias-0>
- [117] Ευρωπαϊκή Επιτροπή, «Manchester Ministerial Declaration 2005», ePractice.eu, 24 November 2005, <http://www.epractice.eu/en/library/281737>
- [118] Ευρωπαϊκή Επιτροπή, «SK: eID cards to be issued from December 2012», 24 February 2012, <http://www.epractice.eu/en/news/5338346>
- [119] Ευρωπαϊκή Επιτροπή, TABULA RASA Project, "EU-funded project to take biometric security systems to the next level" <http://europa.eu/rapid/press-release MEMO-13-924 en.htm>

- [120] Ευρωπαϊκή Επιτροπή, «The Government Office for Science London», 2013, http://ec.europa.eu/digital-agenda/futurium/sites_/futurium/files/futurium/library/The%20Government%20Office%20for%20Science%20London%20-%202013%20-%20Foresight%20Future%20Identities.%20Changing%20identities%20in%20the%20UK%20the%20next%2010%20years.pdf
- [121] Ινστιτούτο Πληροφοριακών Συστημάτων και Προσομοίωσης - Ι.Π.ΣΥ.Π. / Ε.Κ. «Αθηνά», «Ανάπτυξη Οδικού Χάρτη για την εισαγωγή της Κάρτας Πολίτη», 04 Απριλίου 2011
- [122] Κοινωνία της Πληροφορίας, «Εξέλιξη των 20 βασικών υπηρεσιών Ηλεκτρονικής Διακυβέρνησης στην Ελλάδα», Παρατηρητήριο για την Κοινωνική Μεταρρύθμιση, Μάιος 2013
- [123] Μελέτη σκοπιμότητας σχετικά με την ηλεκτρονική ταυτοποίηση, έλεγχος γνησιότητας και Πολιτική Υπογραφής (IAS), <http://www.iasproject.eu/>
- [124] Οργανισμός Πνευματικής Ιδιοκτησίας, «Προσβολή στο Διαδίκτυο», <http://www.opi.gr/index.php/2013-10-03-12-23-43/2013-10-29-08-47-46>
- [125] Παρατηρητήριο για την Ψηφιακή Ελλάδα, <http://www.observatory.gr/Page/default.asp?La=1&ID=1544>
- [126] Παρατηρητήριο για την Ψηφιακή Ελλάδα, «Αναζήτηση Βέλτιστων Πρακτικών» <http://www.observatory.gr/Page/default.asp?La=2&ID=1288&recid=2257>
- [127] Συμβούλιο Ευρωπαϊκής Ένωσης, <http://prado.consilium.europa.eu/EN/7926/docHome.html#docelement1secfeature13>
- [128] Συμβούλιο Ευρωπαϊκής Ένωσης, PRADO, <http://prado.consilium.europa.eu/el/5020/docHome.html>
- [129] Συμβούλιο της Ευρώπης, Dictionary_PRADO, Council of the European Union, Public Registry of Authenticity and Travel Documents Online, <http://prado.consilium.europa.eu/EN/dictionary.html>
- [130] Αυστρία, «Ηλεκτρονική Κάρτα», <http://www.austriacard.at/ac.jsp>
- [131] Αυστρία, A-SIT, «eID in Austria, The Citizen Card», http://www.a-sitat/pdfs/rp_eid_in_austria.pdf

- [132] Αυστρία, Ηλεκτρονική κάρτα
http://www.austriacard.at/download/AC_GOVERNMENT.PDF
- [133] Αυστριακή Ηλεκτρονική Κάρτα, «Access public services online with your Mobile Phone Signature or Citizen Card», <http://www.buergerkarte.at/en/>
- [134] Αυστρία, «Πύλη Ηλεκτρονικής Διακυβέρνησης»,
<https://www.help.gv.at/Portal.Node/hlpd/public/content/99/Seite.990006.html>
- [135] Αυστρία, «eSignature and eID in Austria»,
[http://www.egov2012.gov.cy/mof/DITS/conference/Europeone.nsf/Al/E7916860932FB_B22C2257_ACB004BAEBE/\\$file/SESSION1_No2_KUSTOR.pdf](http://www.egov2012.gov.cy/mof/DITS/conference/Europeone.nsf/Al/E7916860932FB_B22C2257_ACB004BAEBE/$file/SESSION1_No2_KUSTOR.pdf)
- [136] Βέλγιο, <http://eid.belgium.be/>
- [137] Βέλγιο, «Βελγική πύλη ηλεκτρονικής διακυβέρνησης», <http://sma-help.fedict.belgium.be/rn>
- [138] Βέλγιο, Ηλεκτρονική Διακυβέρνηση, <https://irisbox.irisnet.be/>
- [139] Βέλγιο, «Ηλεκτρονικές Ταυτότητες στο Βέλγιο»
http://www.gemalto.com/brochures/download/gov_belgium_id.pdf
- [140] Βέλγιο, «Πιστοποιητικά ταυτότητας στο Βέλγιο» <http://www.brussels.irisnet.be/living-in-brussels/administrative-documents#birth-death-marriage-divorce-certifcate>
- [141] Βέλγιο, eGov profile,
<https://iamapps.belgium.be/sma/generalinfo?language=en®istratton=true>
- [142] Βουλγαρία, <http://psc.egov.bg/en/psc-electronic-identtficatin>
- [143] Βουλγαρία, <http://psc.egov.bg/en/psc-electronic-signature>
- [144] Βουλγαρία, <http://eid.egov.bg/>

- [145] Βουλγαρία, Ηλεκτρονική Κάρτα Βουλγαρίας,
Wikipedia, http://bg.wikipedia.org/wiki/^HHHa_KapTa
- [146] Γαλλία, Ηλεκτρονική Διακυβέρνηση, <http://www.cnil.fr/>
- [147]
Γαλλία, <http://www.zdnet.fr/actualites/la-future-carte-d-identite-electronique-ne-sera-pas-obligatoire-39294159.htm>
- [148] Γαλλία, Εθνική ταυτότητα Γαλλίας, Wikipedia
[http://en.wikipedia.org/wiki/National identity card \(France\)](http://en.wikipedia.org/wiki/National_identity_card_(France))
- [149] Γερμανία, «Άρθρο για την χρήση ηλεκτρονικών ταυτοτήτων από το Γερμανικό Ταμείο Υγειονομικής Περιθαλψης», 22 September 2013, <http://www.epractice.eu/en/news/5419799>
- [150] Γερμανία, «Γερμανική Ηλεκτρονική Κάρτα»,
Wikipedia [http://en.wikipedia.org/wiki/German identity card](http://en.wikipedia.org/wiki/German_identity_card)
- [151] Γερμανία, Ηλεκτρονική Διακυβέρνηση,
<http://www.berlinforalthefamily.com/8/post/2013/10/how-birth-registration-in-germany-works.html>
- [152] Γερμανία, «Συστήματα Ηλεκτρονικής Διακυβέρνησης»,
http://www.personalausweisportal.de/EN/Citizens/Electronic-Identification/Electronic-Identification/node.html;jsessionid=FDAA188B3B066BB30F13F609DB8DAE75.2_cid334
- [153] Ελλάδα, Διαλειτουργικότητα, <http://interoperability-definition.info/e>
- [154] Ελλάδα, «Ελληνικό Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης και Πρότυπα Διαλειτουργικότητας», <http://www.e-gif.gov.gr/portal/page/portal/egif/>
- [155] Ελλάδα, «Ελληνική προσέγγιση Νόμος 3979/2011: για την Ηλεκτρονική Διακυβέρνηση», http://www.egovp1an.gr/7page_id=14-
- [156] Ελλάδα, Εφημερίδα της Κυβέρνησης, «Νόμος 4013/2011/Τεύχος Α'/ΦΕΚ 204 : Σύσταση Ενιαίας Αρχής Δημοσίων Συμβάσεων και Κεντρικού Ηλεκτρονικού Μητρώου Δημοσίων Συμβάσεων», 15 Σεπτεμβρίου 2011

- [157] Ελλάδα, Ελληνικό Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης και Ψηφιακής Αυθεντικοποίησης, Μάρτιος
2012, <http://www.e-gif.gov.gr/porta1/p1s/porta1/docs/840023.PDF>
- [158] Ελλάδα, Ομάδα Ηλεκτρονικής Διακυβέρνησης & Τεχνολογιών Πληροφορικής & Επικοινωνιών, «Παρουσίαση Δράσεων Ομάδας Ηλεκτρονικής Διακυβέρνησης», Απρίλιος
2012, <http://egovict.blogspotgr/>
- [159] Ελλάδα, Πύλη της Δημόσιας Διοίκησης ΕΡΜΗΣ, <http://www.ermis.gov.gr>
- [160] Ελλάδα, Υπουργείο Δημόσιας Τάξης και Προστασίας Πολίτη
http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=139&Itemid=132&lang=
- [161] Ελλάδα, Υπουργείο Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης,
«Χαρακτηριστικά Διαλειτουργικότητας», 22 Αυγούστου
2011, <http://www.yap.gov.gr/index.php/e-gif-menu/e-gif-pdyhs-menu/32-egif-interoperability.html>
- [162] Ελλάδα, Υπουργείο Διοικητικής Μεταρρύθμισης & Ηλεκτρονικής Διακυβέρνησης,
«Οργανωτικές Μονάδες της ΑΠΕΔ», 16 Ιουνίου 2012,
<http://www.yap.gov.gr/index.php/aped/ypiresies-ypodomis-dimosiou-k1eidiou/146-pki-aped-diar8rosi-mixanismou.html>
- [163] Ελλάδα, Υπουργείο Διοικητικής Μεταρρύθμισης & Ηλεκτρονικής Διακυβέρνησης, «Ο νόμος για την Ηλεκτρονική Διακυβέρνηση», 16 Ιουνίου 2011, http://www.egovp1an.gr/?page_id=14
- [164] Ελλάδα, Υπουργείο
Εσωτερικών, http://www.3y5es.gr/UserFiles/f0ff9297-f516-40ff-a70e-eca84e2ec9b9/KanonEK211_2011.pdf
- [165] Ελλάδα, Υπουργείο Συγκοινωνιών και Έργων, Τμήμα Ηλεκτρονικών Επικοινωνιών, «Ιεράρχηση Στόχων - Μέτρων - Δράσεων της Ψηφιακής Στρατηγικής της Κύπρου», Οκτώβριος 2013,
[http://www.mcw.gov.cy/MCW/DEC/Digital Cyprus/ictnsf/F9B9F1BBC76ABE9DC2257A6F0038427B/\\$file/%CE%88%CE%B3%CE%B3%CF%81%CE%B1%CF%86%CE%BF%20%CE%A0%CF%81%CE%BF%CF%84%CE%B5%CF%81%CE%B1%CE%B9%CE%BF%CF%80%CE%BF%CE%AF%CE%B7%CF%83%CE%B7%20%CE%A3%CF%84%CF%8C](http://www.mcw.gov.cy/MCW/DEC/Digital%20Cyprus/ictnsf/F9B9F1BBC76ABE9DC2257A6F0038427B/$file/%CE%88%CE%B3%CE%B3%CF%81%CE%B1%CF%86%CE%BF%20%CE%A0%CF%81%CE%BF%CF%84%CE%B5%CF%81%CE%B1%CE%B9%CE%BF%CF%80%CE%BF%CE%AF%CE%B7%CF%83%CE%B7%20%CE%A3%CF%84%CF%8C)

[%CF%87%CF%89%CE%BD.pdf](#)

[166] Εσθονία, <http://e-estonia.com/component/electronic-id-card/>

[167] Ηνωμένο

Βασίλειο, <https://www.gov.uk/identity-cards-and-new-identity-and-passport-service-suppliers#overview>

[168] Ιρλανδία, Κάρτα Δημόσιου Τομέα

http://www.citizensinformation.ie/en/social_welfare/irish_social_welfare_system/public_services/card.html

[169] Ιρλανδία, «New biometric ID card aims to prevent welfare fraud»,

<http://www.breakingnews.ie/ireland/new-biometric-id-card-aims-to-prevent-welfare-fraud-523238.html>, breakingnews.ie, 05 October 2011

[170] Ισπανία, Ηλεκτρονική Κάρτα Ισπανίας, Wikipedia

http://es.wikipedia.org/wiki/DNI_electr%C3%B3nico_en_Espa%C3%B1a

[171] Ιταλία, «Ηλεκτρονική κάρτα Ιταλίας», Wikipedia,

http://en.wikipedia.org/wiki/Italian_electronic_identity_card

[172] Ιταλία, <http://owni.eu/2011/07/28/e-government-in-italy-a-race-against-time/>

[173] Κυπριακή Δημοκρατία, «Διαδικτυακή Πύλη της Κυπριακής Δημοκρατίας»,

http://www.cyprus.gov.cy/portal/portal.nsf/citizen_____gr?OpenForm&access=0&SectionId=citizen&CategoryId=none&SelectionId=home&print=0&lang=en

[174] <http://dazzlepod.com/cable/10VIENNA58/>

[175]

Λετονία. <https://www.latvija.lv/en/PPK/Tiesibu-aizsardziba/Apliecibas-izzinas-par-personu-pase/p329/ProcesaApraksts>

[176] Λετονία, <https://www.eparaksts.lv/en/eid-card/eid-users/>

- [177] Λετονία, International Students, Immigration procedure, Riga Stradins University, <http://www.rsu.lv/eng/international-students/practical-information/immigration-procedure>
- [178] Λιθουανία, «Έγγραφα ταυτοποίησης»,
[\[https://www.dokumentai.lt/viewpage.php?page_id=77\]](https://www.dokumentai.lt/viewpage.php?page_id=77)
- [179] Λιθουανία, «Ηλεκτρονική κάρτα», http://en.wikipedia.org/wiki/Lithuanian_identity_card
- [180] Λιθουανία, «Χαρακτηριστικά ηλεκτρονικής κάρτας», https://www.dokumentai.lt/viewpage.php?page_id=78
- [181] Λουξεμβούργο, «Εθνική Κάρτα», 29 Οκτωβρίου 2012,
<http://www.guichet.public.lu/citoyens/fr/citoyennete/papiers-identite/carte-identite/carte-identite-lux-adulte/index.html>
- [182] Λουξεμβούργο, Ευρωπαϊκή Ένωση,
http://ec.europa.eu/eurostat/ramon/nat_methods/SBS/SBS_Meth_LU.pdf
- [183] Λουξεμβούργο, Recueil de legislation, Journal Officiel du Grand-Duché de Luxembourg, «Identification des personnes physiques» 25 juin 2013 <http://www.legilux.public.lu/leg/a/archives/2013/0107/a107.pdf>
- [184] Μάλτα, «Γραφείο Διαχείρισης Ταυτότητας», <https://mhas.gov.mt/en/MHAS-Departments/Land%20Public%20Registry/Pages/ID-MO.as^>
- [185] Ολλανδία, <https://www.digid.nl/en/about-digid/>
- [186] Ολλανδία, Ηλεκτρονική Διακυβέρνηση,
http://www.ocg.at/ak/edemocracy/wiki2/en/doku.php?id=projects:netherlands:e-government_and_e-voting_in_the_netherlands
- [187] Ολλανδία, «The Netherlands Digital signatures in the Netherlands» <https://www.tractis.com/contracts/727438240/compare/23/22>

- [188] Πολωνία, «Polish e-ID Card Project Re-launched, Frost and Sullivan Comments», <http://findbiometrics.com/polish-e-id-card-project-re-launched-frost-038-sullivan-comments/>
- [189] Ρουμανία, Ministry of Administration and Interior, «Electronic Identity Card (e-ID Card) Project», http://www.riserid.eu/fileadmin/user_upload/Datei/5_konferenz/S5_13_Electronic_ID_Card_Romania_Balasa.pdf
- [190] Σλοβακία, PRO Security Zone, «Equipment Installed In Slovakia For Citizen e-ID System», 11 September, 2012
http://www.prosecurityzone.com/News_Detail_Equipment_installed_in_slovakia_for_citizen_e-id_system_19314.asp#axzz2zjtJE5Sw
- [191] Σλοβενία, «Slovenian General Certification Authority», <http://www.sigen-ca.si/eng/eng-predstavitev-SIGEN-CA.php>
- [192] Σουηδία, <http://www.BankID.com/>
- [193] Σουηδία, «National Identity Card (Sweden)», Wikipedia, [http://en.wikipedia.org/wiki/National_identity_card_\(Sweden\)](http://en.wikipedia.org/wiki/National_identity_card_(Sweden))
- [194] Σουηδία, «Swedish ePassport and eID Programs», http://www.gemalto.com/brochures/download/gov_sweden_e-pass.pdf
- [195] Τσεχία, Gemalto, «The Czech Republic's National eID card»
http://www.gemalto.com/brochures/download/gov_cs_czech_eID_cardpdf
- [196] Φινλανδία, Population Register Centre, «Electronic Identity and Certificates» <http://www.vrk.fi/default.aspx?id=21>
- [197] «Ενσωμάτωση Διαπιστευτηρίων Ανωνυμίας eIDs για (Μη Αυθεντικοποίηση προσανατολισμένη στο σεβασμό της Ιδιωτικότητας)»
- [198] «Statewatch Briefing ID Cards in the EU: Current state of play», <http://www.statewatch.org/analyses/no-107-national-ID-cards-questionnaire.pdf>
- [199] Z-Squared Technology, «Biometric Identification Solutions», 02 October 2012 <http://www.zsquaretech.com/biometric-identification-solutions/>

[200] <http://www.datacard.com/downloads/ViewDownload.dyn?elementId=repositories/download1/xm1/Slovakia Case Study Enhanced Security Gov IDs.xml&repositoryName=downloads&index=5>

Παράρτημα Α

Ευρωπαϊκά Έργα

Στο παράρτημα Α της μελέτης αναφέρονται περιληπτικά διάφορα έργα που έχουν υλοποιηθεί, σχετικά με την ενίσχυση της ιδιωτικότητας των συστημάτων διαχείρισης ταυτότητας, την παροχή διαλειτουργικότητας σε πανευρωπαϊκές υπηρεσίες ηλεκτρονικής διακυβέρνησης, στις δημόσιες υπηρεσίες, στις επιχειρήσεις και στους πολίτες. Όλα τα έργα προσανατολίζονται στην εναρμόνιση των κρατών μελών σε ασφαλή ηλεκτρονικά συστήματα ταυτοποίησης των πολιτών παρέχοντας υψηλές υπηρεσίες σε ευρωπαϊκό πλαίσιο.

A.1 Ενιαίος Χάρτης στην Ευρώπη

Η ιστορία για την πορεία προς ένα ενιαίο ευρωπαϊκό πλαίσιο που θα ενισχύσει την απασχόληση, την οικονομική δραστηριότητα, την έρευνα, την καινοτομία και την επιχειρηματικότητα ξεκινά το 2000 στην Λισσαβόνα, όπου οι ηγέτες της Ευρωπαϊκής Ένωσης συμφώνησαν σε ένα νέο στρατηγικό στόχο που στόχευε:

■ *S Σε μία δυναμική και ανταγωνιστική Οικονομία βασισμένη στην γνώση*

■S Στον εκσυγχρονισμό του ευρωπαϊκού κοινωνικού μοντέλου με επένδυση στον άνθρωπο και στην οικοδόμηση ενός ενεργού κράτους πρόνοιας

■S Στην ενσωμάτωση των στόχων της αειφόρου ανάπτυξης [83]

Η στρατηγική της Λισσαβόνας αναθεωρήθηκε το 2005 και έθεσε νέο στόχο για μια Ευρώπη περισσότερο ανταγωνιστική και ευέλικτη με έμφαση στους τομείς της οικονομίας και της απασχόλησης για την τρέχουσα δεκαετία.

Στις 25 Απριλίου 2006 εγκρίθηκε ένα σχέδιο δράσης για την ηλεκτρονική διακυβέρνηση, όπου η Επιτροπή δεσμεύτηκε ότι θα συνεχίσει τις προσπάθειές της σε συνεργασία με τα κράτη μέλη για την ανάπτυξη πολιτικών ασφαλούς πρόσβασης σε υπηρεσίες σε όλη την ΕΕ και την διευκόλυνση των πολιτών την αμοιβαία αναγνώριση των εθνικών ηλεκτρονικών ταυτοτήτων από την Δημόσια Διοίκηση. Οι πρώτες αρχές για το σχεδιασμό του χάρτη αφορούσαν:

■S Ασφαλή συστήματα

■S Ικανά (διαλειτουργικά) συστήματα ταυτοποίησης των χρηστών εντός των συνόρων της Ευρωπαϊκής Ένωσης

■S Τα κράτη οφείλουν να εκδίδουν τα μέσα αυθεντικοποίησης των πολιτών

■S Τα κράτη οφείλουν να εξασφαλίζουν την ορθή επικοινωνία των συστημάτων αυθεντικοποίησης των πολιτών

S Τα κράτη οφείλουν να ακολουθούν τις αρχές της επικουρικότητας

Τα έργα και οι δράσεις για την υλοποίηση του χάρτη αφορούσαν τη βελτίωση της διασυνοριακής χρηστικότητας των διακριτικών ταυτοποίησης (με πρωτοβουλίες τυποποίησης και διαλειτουργικότητας) και των πηγών ταυτοποίησης (μηχανισμών ανταλλαγής πληροφοριών ταυτοποίησης, πρόσβαση στις πηγές από τον τελικό χρήστη).

A.2 FIDIS

Το έργο FIDIS (Future of Identity in the Information Society) ξεκίνησε το 2004 και ολοκληρώθηκε το 2009. Υλοποιήθηκε από ένα δίκτυο 24 συμμετεχόντων (Ευρωπαϊκών ακαδημαϊκών ιδρυμάτων και

επιχειρήσεων) σε 13 ευρωπαϊκά κράτη με σκοπό την μελέτη και την αναγνώριση των πολιτών, των διαφορετικών χαρακτηριστικών της ταυτότητας, της ιδιωτικότητας και της ασφάλειας προκειμένου να δοθούν διαφορετικές απόψεις για την καλύτερη σχεδίαση συστημάτων διαχείρισης ταυτοτήτων. Το έργο FIDIS δομήθηκε σε επτά ερευνητικές δραστηριότητες : τον προσδιορισμό της ταυτότητας της ταυτότητας, την ιδιωτικότητα και το κοινωνικο-νομικό περιεχόμενο της ταυτότητας, τη μελέτη του προφίλ, τον καθορισμό ταυτότητας υψηλής τεχνολογίας, τη διαλειτουργικότητα των συστημάτων ταυτοποίησης, την εγκληματικότητα και την φορητότητα της ταυτοποίησης [16].

A.3 PRIME

Το έργο PRIME (Privacy and Identity Management for Europe) ξεκίνησε το 2004 με στόχο να αναπτύξει ένα λειτουργικό πρωτότυπο για ένα σύστημα διαχείρισης ταυτοτήτων που θα ενίσχυε την Ιδιωτικότητα, μας και όλες οι συναλλαγές των ανθρώπων επέβαλαν την ανταλλαγή δεδομένων προσωπικού χαρακτήρα. Το έργο PRIME εστιάζει σε λύσεις για την προστασία της ιδιωτικής ζωής, την ενίσχυση της διαχείρισης ταυτότητας χρηστών και την ασφαλή αλληλεπίδραση στα ηλεκτρονικά συστήματα με σεβασμό στα προσωπικά τους δεδομένα [34].

A.4 IDADC

Το πρόγραμμα IDABC (Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens) στόχευε στην παροχή διαλειτουργικών ευρωπαϊκών υπηρεσιών ηλεκτρονικής διακυβέρνησης στις δημόσιες διοικήσεις, τις επιχειρήσεις και τους πολίτες [112]. Χρησιμοποιώντας τα οφέλη των Τεχνολογιών Πληροφοριών και Επικοινωνίας, το IDABC ενθάρρυνε τις διασυνοριακές υπηρεσίες του δημόσιου τομέα προς τους πολίτες και τις επιχειρήσεις πανευρωπαϊκά για να βελτιωθεί η αποτελεσματικότητα και η συνεργασία μεταξύ των δημόσιων υπηρεσιών των ευρωπαϊκών κρατών. Πα να καταστούν δυνατοί οι στόχοι του προγράμματος IDABC εκπονήθηκαν μελέτες, συστάσεις και λύσεις για την επικοινωνία των κρατών.

A.5 CROBIES

Η μελέτη CROBIES (Cross Border Interoperability of eSignatures) ξεκίνησε τον Αύγουστο του 2008 και ολοκληρώθηκε τον Ιούνιο του 2010. Τα αρχικά CROBIES παραπέμπουν στο στόχο της μελέτης που αφορά την άρση των εμποδίων για την διασυνοριακή διαλειτουργικότητα των ηλεκτρονικών υπογραφών που βασίζονται σε αναγνωρισμένο πιστοποιητικό.

Το CROBIES είχε ως πυρήνα την οδηγία 1999/93/EK για την υποστήριξη του σχεδίου δράσης της Ευρωπαϊκής Ένωσης για την ηλεκτρονική υπογραφή και την ηλεκτρονική ταυτοποίηση. Στην μελέτη γίνεται ανάλυση απαιτήσεων των ηλεκτρονικών υπογραφών ώστε να μπορεί να καταστεί δυνατή η διαλειτουργικότητα [109].

A.6 SPOCS

Το έργο SPOCS (Simple Procedures Online for Crossborder Services) ξεκίνησε το Μάο του 2009. Πρόκειται για ένα έργο που στοχεύει στην απρόσκοπτη και αδιάλειπτη λειτουργία των ηλεκτρονικών διαδικασιών, ώστε να προσφέρεται η διαλειτουργικότητα στα υφιστάμενα συστήματα. Ο στόχος του SPOCS είναι να δημιουργήσει «σημεία δεύτερης γενιάς» προκειμένου να εξυπηρετηθούν οι πολίτες μέσα από ένα υψηλό επίπεδο ηλεκτρονικών διαδικασιών διασυνοριακά.

Σύμφωνα με την οδηγία 2006/123/EK ορίζεται ένα σημείο ενιαίας εξυπηρέτησης για κάθε κράτος μέλος, από το οποίο οι επιχειρήσεις και οι πολίτες θα μπορούν να λάβουν σαφείς και αναλυτικές πληροφορίες και διοικητικές διαδικασίες που επιθυμούν. Αυτό επιτυγχάνεται με τις ηλεκτρονικές πύλες, όπως αναφέρθηκε στην παράγραφο 4.3.3. Στο έργο SPOCS συμμετείχαν η Αυστρία, Γαλλία, Γερμανία, Ελλάδα, Ηνωμένο Βασίλειο, Ιταλία, Λιθουανία, Λουξεμβούργο, Μάλτα, Νορβηγία, Ολλανδία, Πολωνία, Πορτογαλία, Ρουμανία, Σλοβενία, Σουηδία [38].

A.7 PEPPOL

Ο στόχος του έργου PEPPOL (Pan European Public Procurement Online) ήταν να δημιουργήσει μια πανευρωπαϊκή λύση που θα διευκολύνει την διαλειτουργικότητα στις υφιστάμενες εθνικές λύσεις, υπό το πρίσμα της διακήρυξης του Manchester τον Νοέμβρη του 2005 [32]. Παρά το γεγονός ότι οι κυβερνήσεις αποτελούν τους μεγαλύτερους αγοραστές της Ευρωπαϊκής Ένωσης δεν χρησιμοποιούσαν ορθά τις τεχνολογικές ευκαιρίες για να σας διαχειριστούν ηλεκτρονικά τις δημόσιες συμβάσεις. Το έργο PEPPOL είχε τη φιλοδοξία να επιτύχει την επικοινωνία μεταξύ εταιρειών και κυβερνητικών οργάνων για όλες τις διαδικασίες προμηθειών. Το τελικό αποτέλεσμα του PEPPOL ήταν ένα διεπιχειρησιακό περιβάλλον που στηρίζει τα εθνικά συστήματα και τις υποδομές.

A.8 OpenPEPPOL

Απόγονος του PEPPOL είναι το Association OpenPeppol [32]. Η σύσταση μας «συνεργασίας» (Association) με ονομασία OpenPEPPOL, ξεκίνησε την 1 Σεπτεμβρίου 2012 για να συνεχίσει την επιτυχή ολοκλήρωση του έργου PEPPOL. Σύμφωνα με το Βελγικό δίκαιο, το OpenPEPPOL International είναι ένας μη - κερδοσκοπικός οργανισμός με μέλη του δημόσιου και του ιδιωτικού τομέα. Η συνεργασία έχει την πλήρη ευθύνη για την ανάπτυξη και τη συντήρηση των προδιαγραφών PEPPOL, τα δομικά στοιχεία και τις υπηρεσίες του και την εφαρμογή σε ολόκληρη την Ευρώπη, με σκοπό την συμμετοχή των ευρωπαϊκών επιχειρήσεων στις διαδικασίες προμηθειών του δημόσιου τομέα, την αύξηση των δυνατοτήτων για την αύξηση του ανταγωνισμού της παροχής της λεγόμενης «value for money» αξίας για τα χρήματα των φορολογουμένων.

Η συνεργασία OpenPEPPOL παρέχει στους εμπλεκόμενους ευρέως αποδεκτά τεχνολογικά πρότυπα και διασφαλίζει την βιωσιμότητα και την προώθηση της ευρείας χρήσης των προδιαγραφών PEPPOL στις ηλεκτρονικές υπηρεσίες διακυβέρνησης.

A.9 STORK

Το έργο STORK αποτελεί ένα έργο μεγάλης κλίμακας που στοχεύει στην ανταγωνιστικότητα και την καινοτομία στην Ευρωπαϊκή Ένωση. Η ονομασία του προέρχεται από τα κεφαλαία γράμματα της περιγραφής «Secure Identity Across Borders Linked» και αφορά την ασφαλή και διασυνοριακή ταυτοποίηση των πολιτών για την πρόσβαση σε υπηρεσίες του δημόσιου τομέα. Το STORK βασίζεται σε μια κατανομημένη αρχιτεκτονική για την ηλεκτρονική ταυτοποίηση των πολιτών της Ευρωπαϊκής Ένωσης με στοιχεία από τις ήδη υπάρχουσες εφαρμογές των κρατών. Οι πολίτες μπορούν να πραγματοποιήσουν ηλεκτρονικές συναλλαγές πέρα από τα σύνορα της χώρας τους.

Στην αρχική υλοποίηση του έργου συμμετείχαν οι εξής χώρες : Αυστρία, Βέλγιο, Γερμανία, Εσθονία, Ισπανία, Ισλανδία, Ιταλία, Λουξεμβούργο, Πορτογαλία, Σουηδία και Σλοβενία. Ως παρατηρητές είχαν καθοριστεί οι χώρες της Γαλλία, της Ολλανδίας και του Ηνωμένου Βασιλείου. Τον Ιανουάριο του 2010 τα σύνορα του STORK «διευρύνθηκαν» στις χώρες της Ελλάδας, της Σλοβακίας και της Φινλανδίας.

Το STORK αποτελεί ένα ασφαλές περιβάλλον, με εύκολη υλοποίηση ώστε να μπορεί να χρησιμοποιηθεί από κάθε χρήστη. Διασφαλίζει την ασφαλή πρόσβαση των πολιτών σε ηλεκτρονικές υπηρεσίες, ενώ οι πολίτες διατηρούν τον έλεγχο των διαμοιραζόμενων δεδομένων στις συνεδρίες.

Στο STORK υπάρχουν δύο μοντέλα υλοποίησης : το απευθείας μοντέλο (Middleware Model -MW) και το Πανευρωπαϊκό μοντέλο πληρεξούσιων υπηρεσιών (Pan-European Proxy Services model - PEPS).

Σύμφωνα με το μοντέλο MW ο πολίτης επικοινωνεί απευθείας με τον παροχέα υπηρεσιών. Στο μοντέλο PEPS υπάρχει η φιλοσοφία του μεσάζοντα. Η πιστοποίηση της ταυτότητας του πολίτη πραγματοποιείται από την χώρα που εξέδωσε την ηλεκτρονική κάρτα.

Βασικά προγράμματα του STORK είναι τα ακόλουθα:

S «Διασυνοριακή Αυθεντικοποίηση για Ηλεκτρονικές Υπηρεσίες», με συμμετοχή των χωρών της Αυστρίας, του Βελγίου, της Εσθονίας, της Ελλάδας, της Γερμανίας, της Ισλανδίας, της Πορτογαλίας, της Φιλανδίας, της Λιθουανίας και της Γαλλίας

S «Ασφαλής συνομιλία (chat)», με συμμετοχή των χωρών της Αυστρίας και της Ισλανδίας

S «Ανταλλαγή φοιτητών», με συμμετοχή των χωρών της Αυστρίας, της Εσθονίας, του Λουξεμβούργου, της Σλοβενίας και της Φινλανδίας

■ *S* «Διασυνοριακή πιστοποιημένη ηλεκτρονική επικοινωνία»

S «Αλλαγή Διεύθυνσης», με συμμετοχή των χωρών της Εσθονίας, της Ισπανίας, της Πορτογαλίας, της Σλοβενίας, της Σουηδίας και της Φιλανδίας

S «Υπηρεσίες της Ευρωπαϊκής Επιτροπής» με συμμετοχή των χωρών της Αυστρίας, του Βελγίου, της Γερμανίας, της Εσθονίας, της Ισλανδίας, της Ισπανίας, της Ιταλίας, της Πορτογαλίας, της Σλοβενίας και της Διεύθυνσης Πληροφορικής της ΕΕ

Γα κάθε συνεδρία στο περιβάλλον STORK καταγράφονται η ημερομηνία και ώρα της συνεδρίας και ένα κρυπτογράφημα των προσωπικών δεδομένων του πολίτη [40,41,42].

A.10 TABULA RASA

Το έργο Tabula Rasa έχει στόχο τον προσδιορισμό ασφαλών βιομετρικών συστημάτων. Στο έργο ενεπλάκησαν 12 διαφορετικές οργανώσεις από επτά χώρες, που εργάστηκαν για μια τριετή περίοδο στην έρευνα τρωτών σημείων στα βιομετρικά συστήματα. Στόχος του έργου ήταν η ανάπτυξη αντιμέτρων για την δημιουργία ασφαλέστερων βιομετρικών συστημάτων [119]. Άξια αναφοράς είναι η πρόσκληση-πρόκληση που έκαναν οι ερευνητές κατά την διάρκεια της έρευνας όπου προσκλήθηκαν ερευνητές από όλο τον κόσμο για να αναπτύξουν σχέδια επίθεσης προς τα βιομετρικά συστήματα.

Αποτέλεσμα του έργου ήταν η καταγραφή επιθέσεων απόκρυψης ταυτότητας (spoofing), η αξιολόγηση των ευπαθειών των βιομετρικών συστημάτων και η ανάπτυξη αντιμέτρων.

Τα αποτελέσματα του έργου συνέβαλαν στην ανάπτυξη του TABULA RASA Consortium, όπου συμμετέχουν 12 μέλη από ερευνητικά ιδρύματα και εταιρείες. Με την τεχνογνωσία που παρήχθη εξακολουθούν να εργάζονται τα μέλη για να δώσουν ασφαλείς λύσεις στην αγορά. Υπεύθυνος του TABULA RASA Consortium είναι το Ινστιτούτο Ερευνών IDAP, ενώ συμμετέχουν το Πανεπιστήμιο του Southampton (Ηνωμένο Βασίλειο), το Πανεπιστήμιο του Κάλιαρι (Ιταλία), το Πανεπιστήμιο του Oulu (Φινλανδία), το Πανεπιστήμιο Universidad Autonoma de Madrid (Ισπανία), EURECOM (Γαλλία), ένα ερευνητικό κέντρο μηχανικής και τηλεπικοινωνιών, το Morpho (Γαλλία), καθώς και η εταιρεία Starlab Barcelona που αποτελεί τον παγκόσμιο ηγέτη στα συστήματα βιομετρικής (Ισπανία), η Κινεζική Ακαδημία Επιστημών (Κίνα), η εταιρεία KeyLemon (Ελβετία), μια εταιρεία που παρέχει ασφαλείς λύσεις πρόσβασης που βασίζονται στο πρόσωπο και την αναγνώριση ήχου, BIOMETRY (Ελβετία), μια εταιρεία που παρέχει ταυτόχρονη χρήση βιομετρικών στοιχείων με τυχαία απάντηση πρόκληση και το Κέντρο για την Επιστήμη, την Κοινωνία και την Ιθαγένεια (Ιταλία).

A.11 ESENS

Το έργο e-SENS (Electronic Simple European Networked Services) ενσαρκώνει την ιδέα της ανάπτυξης ευρωπαϊκής ψηφιακής αγοράς μέσω καινοτόμων λύσεων ΤΠΕ. Το έργο πρόκειται να βελτιώσει και να επεκτείνει τις τεχνικές λύσεις για την προώθηση της διασυνοριακής

Ηλεκτρονικής Διακυβέρνησης σε θέματα υγείας, δικαιοσύνης, διαχείρισης συμβάσεων και οργάνωσης των επιχειρήσεων.

Το έργο στοχεύει στην εύκολη πρόσβαση σε ηλεκτρονικές δημόσιες υπηρεσίες, την διασφάλιση της διαλειτουργικότητας μεταξύ των διαφορετικών εθνικών συστημάτων και την ανάπτυξη επαναχρησιμοποιήσιμων λύσεων για ηλεκτρονικές υπηρεσίες στην δημόσια διοίκηση.

Στο έργο συμμετέχουν η Αυστρία, η Γαλλία, η Γερμανία, η Δανία, η Ελλάδα, η Εσθονία, η Ιρλανδία, η Ισπανία, η Ιταλία, το Λουξεμβούργο, η Νορβηγία, η Ολλανδία, η Πολωνία, η Ρουμανία, η Σλοβακία, η Σλοβενία, η Σουηδία, η Τσεχία και τα OpenPEPPOL και ETSI [12].

Παράρτημα Β

Τεχνικά Χαρακτηριστικά Εγγράφων Ταυτότητας και Ταξιδιού

Β.1 Επιγραμμικό Δημόσιο Μητρώο Γνήσιων Εγγράφων Ταυτότητας και Ταξιδιού

Το Επιγραμμικό δημόσιο μητρώο γνήσιων εγγράφων ταυτότητας και ταξιδιού του Συμβουλίου της Ευρωπαϊκής Ένωσης (Public Register of Authentic Identity and travel Documents Online -PRADO) αποτελεί ένα ιστότοπο όπου παρέχονται με πληροφορίες σχετικά με τα ευρωπαϊκά γνήσια έγγραφα ταυτότητας και ταξιδιού [127]. Ο ιστότοπος εμπλουτίζεται ώστε να περιλαμβάνει πληροφορίες σχετικά με την εγκυρότητα των εγγράφων αυτών, νομικές και τεχνικές πτυχές τους.

Στην ενότητα αυτή αξιοποιήθηκαν τα στοιχεία του ιστότοπου για να παρατεθεί ένα αγγλοελληνικό λεξικό με στοιχεία που αφορούν χαρακτηριστικά, τεχνικές και πληροφορίες σχετικά με τα ταξιδιωτικά και τα έγγραφα. Οι ηλεκτρονικές ταυτότητες - κάρτες περιλαμβάνονται στην Κατηγορία Εγγράφου «Β. Δελτίο Ταυτότητας». Το λεξικό αυτό είναι βασικό εργαλείο καθώς σημειώνει την αντιστοιχία των αριθμών αναφορών, την αγγλική απόδοση των χαρακτηριστικών και την επεξήγησή τους.

Πα κάθε χαρακτηριστικό ασφαλείας περιλαμβάνονται οι κατηγοριοποιήσεις (αντιστοιχίσεις) για τις τεχνικές επικόλλησης, επικύρωσης και δεσίματος, τα βιομετρικά χαρακτηριστικά, την μορφή του εξώφυλλου, την τεχνολογία αποθήκευσης των δεδομένων, την μέθοδο στερέωσης, το μορφότυπο εικόνας, την εκδούσα αρχή, τις γλώσσες, το νομικό καθεστώς, το φωτισμό, το χρώμα, το υλικό, την θέση αρίθμησης, το είδος OVD, την τεχνική ενσωμάτωσης της φωτογραφίας, την τεχνική εκτύπωσης, τα χαρακτηριστικά ασφαλείας της τεχνικής εκτύπωσης, το είδος στοιχείου ασφαλείας, την χρονική μονάδα διάρκειας και την θέση του υδατόσημου.

		Dictionary en	Λεξικό el
Glossary reference numbers	en	Additional Safeguard	Πρόσθετο χαρακτηριστικό ασφαλείας
	1	transparent window	διαφανές παράθυρο
	en	Application Technique	Τεχνική επικόλλησης
057	1	cold-applied	επικόλληση εν ψυχρώ
056	2	heat-applied	επικόλληση εν θερμώ
	5	other	άλλη
	en	Authentication	Επικύρωση
083	1	ink stamp	σφραγίδα μελάνης
084	2	embossing stamp	ανάγλυφη σφραγίδα
083	3	ink and / or embossing stamp	σφραγίδα μελάνης ή/και ανάγλυφη
122	4	background lines continue across the image	οι γραμμές του δαπέδου διασχίζουν και τη φωτογραφία
073	5	embossing stamp and eyelet	ανάγλυφη σφραγίδα και κρίκος
	6	none	καμία
	7	other	άλλη
042	8	scrambled (encrypted) image	κρυπτογραφημένη εικόνα (scrambled image)
148	9	rip cuts	εντομές
Glossary reference numbers	en	Additional Safeguard	Πρόσθετο χαρακτηριστικό ασφαλείας
005	en	Binding Technique	Τεχνική δεσίματος
059	1	stitched in the spine	ραχιοραφή
059	2	saddle stitching with thread	σαμαροραφή με νήμα
059	3	saddle stitching with staples	σαμαροραφή με συνδετήρες

175	4	side stitching with thread	πλαγιοραφή με νήμα
005	5	side stitching with staples	πλαγιοραφή με συνδετήρες
014	6	adhesive binding	κολλητή βιβλιοδεσία
005	7	binding using wire	δέσιμο με σύρμα
005	8	binding using plastic	δέσιμο με πλαστικό
005	9	other	άλλη
181	en	Biometric Identifier	Βιομετρικά αναγνωριστικά στοιχεία
181	1	facial image	εικόνα προσώπου
181	2	fingerprint	δακτυλικό αποτύπωμα
181	3	iris image	εικόνα ίριδας
181	4	hand geometry	μορφολογία χεριού
181	5	other	άλλο
	en	Construction of the Cover	Εξώφυλλο - Υλική μορφή
	1	hard cover	σκληρό εξώφυλλο
	2	flexible	εύκαμπτο
	3	other	άλλο
140	en	Cover Embossing	Ανάγλυφα εντυπώματα εξωφύλλου
140	1	hot foil stamping	εντύπωμα με θερμοτυπία
	en	Data Expansion Technology	Τεχνολογία αποθήκευσης δεδομένων
152	1	microchip - contact	μικροκύκλωμα με επαφή
153	2	microchip - contactless	μικροκύκλωμα χωρίς επαφή
119	3	magnetic strip	μαγνητική ταινία
004	4	barcode	γραμμικός κώδικας
004	5	2D barcode	δισδιάστατος γραμμικός κώδικας
118	6	optical stripe	οπτική λωρίδα
	7	other	άλλη
Glossary reference numbers	en	Additional Safeguard	Πρόσθετο χαρακτηριστικό ασφαλείας
	en	Document Category	Κατηγορία εγγράφου
128	A	National passport (all types of passport)	Εθνικό διαβατήριο (κάθε είδους)
128	B	Identity card	Δελτίο ταυτότητας
128	C	Visa	Θεώρηση
083	D	Stamp	Σφραγίδα
128	E	Entry paper	Έγγραφο εσόδου
128	F	Driving licence	Άδεια οδήγησης
128	G	Vehicle licence / log book	Άδεια κυκλοφορίας / ημερολόγιο οχήματος
128	H	Residence permit	Άδεια παραμονής
128	I	Seaman's book	Ναυτικό φυλλάδιο
128	J	Travel document issued to non-nationals	Ταξιδιωτικό έγγραφο χορηγούμενο σε αλλοδαπούς
128	X	Other document	Άλλου είδους έγγραφο

	en	Document Element Description	Χαρακτηρισμός μέρους του εγγράφου
	DOC	Document (valid for all physical document elements, including cover)	Έγγραφο (ισχύει για ολόκληρο το έγγραφο, περιλαμβανομένου του εξωφύλλου)
	DEC	Document except cover	Έγγραφο, εξαιρουμένου του εξωφύλλου
	COV	Cover (generic information about the cover)	Εξώφυλλο (γενικές πληροφορίες για το εξώφυλλο)
	CFO	Cover - front, outside	Εξώφυλλο - εμπρόσθια εξωτερική
	CFI	Cover - front, inside	Εξώφυλλο - εμπρόσθια εσωτερική σελίδα
	CBO	Cover - back, outside	Εξώφυλλο - οπίσθια εξωτερική όψη
	CBI	Cover - back, inside	Εξώφυλλο - οπίσθια εσωτερική σελίδα
	REC	Recto - identity	Εμπρόσθια όψη - με προσδιορισμό ταυτότητας
	VER	Verso	Οπίσθια όψη
	ICR	Integrated biodata card - recto (identity)	Ενσωματωμένη κάρτα στοιχείων κατόχου - εμπρόσθια όψη (με προσδιορισμό ταυτότητας)
	ICV	Integrated card - verso	Ενσωματωμένη κάρτα - οπίσθια
	ELE	Document element (if no other qualifier is applicable)	Μέρος του εγγράφου (εφόσον δεν ταιριάζει κάποιος άλλος χαρακτηρισμός)
	BIO	Biodata page	Σελίδα στοιχείων κατόχου
	INP	Inner page(s)	Εσωτερική/ές σελίδα/ες
Glossary reference numbers	en	Additional Safeguard	Πρόσθετο χαρακτηριστικό ασφαλείας
	en	Document Type	Είδος εγγράφου
128	O	Ordinary	Κοινό
128	S	Service / Official	Υπηρεσιακό / Αξιωματούχος
128	D	Diplomatic	Διπλωματικό
128	P	Emergency / Provisional	Έκτακτης ανάγκης / Προσωρινό
083	E	Entry Stamp	Σφραγίδα εισόδου
083	X	Exit Stamp	Σφραγίδα εξόδου
	en	Fixing Method	Μέθοδος στερέωσης
076	1	glued	κολλη μένη
	2	-	-
130	3	photo patch	photo patch (αυτοκόλλητη)
073	4	eyelets (rivets)	κρίκοι
131	5	perforation	διάτρηση
130	6	other	άλλη
	en	Form of the Stamp	Σχήμα σφραγίδας
083	1	small round (< 15 mm)	στρογγυλό μικρού μεγέθους (< 15 mm)
083	2	medium round (15-25 mm)	στρογγυλό μεσαίου μεγέθους (15-25 mm)
083	3	large round (> 25 mm)	στρογγυλό μεγάλου μεγέθους (> 25 mm)
083	4	oval	ωοειδές
083	5	square	τετράγωνο

083	6	open text	ανοικτό κείμενο
083	7	row stamp with a line around	πολύστιχη σφραγίδα με περίγραμμα
083	8	row stamp without a line around	πολύστιχη σφραγίδα χωρίς περίγραμμα
084	9	embossing stamp	ανάγλυφη σφραγίδα
083	10	other	άλλο
	en	Image Format	Μορφότυπος εικόνας
	PNG	PNG	PNG
	JPG	JPEG	JPEG
	en	Issuing Authority	Εκδούσα αρχή
	1	Police Authority	Αστυνομία
	2	Border Control	Αρχή ελέγχου συνόρων
	3	Customs	Τελωνείο
	4	Emigration and/or Immigration Authority	Υπηρεσία μετανάστευσης
	5	Diplomatic Authority (e.g. embassy)	Διπλωματική αρχή (π.χ. πρεσβεία)
	6	Local Government	Τοπική / περιφερειακή αρχή
	7	other	άλλη
	en	Language	Γλώσσα
	BG	bg - Bulgarian	bg - βουλγαρική
	CS	cs - Czech	cs - τσεχική
	DA	da - Danish	da - δανική
	DE	de - German	de - γερμανική
	EL	el - Greek	el - ελληνική
	EN	en - English	en - αγγλική
	ES	es - Spanish	es - ισπανική
	ET	et - Estonian	et - εσθονική
	FI	fi - Finnish	fi - φινλανδική
	FR	fr - French	fr - γαλλική
	HU	hu - Hungarian	hu - ουγγρική
	IT	it - Italian	it - ιταλική
	LT	lt - Lithuanian	lt - λιθουανική
	LV	lv - Latvian	lv - λετονική
	NL	nl - Dutch	nl - ολλανδική
	MT	mt - Maltese	mt - μαλτέζικη
	PL	pl - Polish	pl - πολωνική
	XT	pt - Portuguese	pt - πορτογαλική
	RO	ro - Romanian	ro - ρουμανική
	SL	sl - Slovenian	sl - σλοβενική
	SK	sk - Slovak	sk - σλοβακική
	SV	sv - Swedish	sv - σουηδική
	IE	ie - Irish	ie - ιρλανδική

en	Legal Status	Νομικό καθεστώς
00	free text	ελεύθερο κείμενο
01-CC	Document issued to nationals of <CC>	Έγγραφο που χορηγείται σε υπηκόους της χώρας <CC>
02	Document issued to stateless persons	Έγγραφο που χορηγείται σε ανιθαγενείς
03-CC	Travel document issued to nationals of <CC>	Ταξιδιωτικό έγγραφο που χορηγείται σε υπηκόους της χώρας <CC>
04-CC	Travel document issued to persons who are not nationals of <CC>	Ταξιδιωτικό έγγραφο που χορηγείται σε μη υπηκόους της χώρας <CC>
05	Travel document issued to Danish nationals from Greenland	Ταξιδιωτικό έγγραφο που χορηγείται σε Δανούς υπηκόους από τη Γροιλανδία
06	Travel document issued to Danish nationals from the Faroe Islands	Ταξιδιωτικό έγγραφο που χορηγείται σε Δανούς υπηκόους από τις Φερόες Νήσους
07-CC	Travel document issued to nationals of <CC>, with diplomatic immunity	Ταξιδιωτικό έγγραφο που χορηγείται σε υπηκόους της χώρας <CC> με διπλωματική ασυλία.
08	Travel document issued to foreign nationals	Ταξιδιωτικό έγγραφο που χορηγείται σε αλλοδαπούς
09-CC	Travel document issued to foreign nationals, resident in: <CC>	Ταξιδιωτικό έγγραφο που χορηγείται σε αλλοδαπούς που διαμένουν στο/στη <CC>
10	Travel document issued to third-country nationals	Ταξιδιωτικό έγγραφο που χορηγείται σε υπηκόους τρίτων χωρών
11	Travel document issued to foreign nationals or stateless persons	Ταξιδιωτικό έγγραφο που χορηγείται σε αλλοδαπούς ή ανιθαγενείς
12	Travel document which establishes the holder's identity but does not confer Portuguese nationality nor the right to protection abroad by the Portuguese authorities.	Ταξιδιωτικό έγγραφο το οποίο προσδιορίζει την ταυτότητα του κατόχου του αλλά δεν παρέχει πορτογαλική υπηκοότητα ούτε το δικαίωμα προστασίας στο εξωτερικό από τις πορτογαλικές αρχές.
13-CC	Document establishing identity issued to nationals of: <CC>	Έγγραφο το οποίο προσδιορίζει την ταυτότητα και χορηγείται σε υπηκόους του/της <CC>
14-CC	Document establishing identity issued to nationals of, or to foreign nationals legally resident in: <CC>	Έγγραφο το οποίο προσδιορίζει την ταυτότητα και χορηγείται σε υπηκόους του/της <CC> ή σε αλλοδαπούς που διαμένουν νομίμως εκεί.
15-CC	Document establishing identity and nationality and granting authori zati on to res i de i n: <CC>.	Έγγραφο το οποίο προσδιορίζει την ταυτότητα και την υπηκοότητα και παρέχει άδεια παραμονής στο/στην <CC>
16	Document establi shi ng i dentity i ssued to resi dent foreign nati onals	Έγγραφο το οποίο προσδιορίζει την ταυτότητα και χορηγείται σε αλλοδαπούς κατοίκους
17-CC	Authori zati on to enter the territory of: <CC>	Άδεια εισόδου στην επικράτεια του/της <CC>
18-CC	Authori zati on to enter the territory of: <CC> - for a li mited peri od	Άδεια εισόδου στην επικράτεια του/της <CC> για περιορισμένο χρονικό διάστημα
19-CC	Document i ssued to persons havi ng refugee status i n: <CC>	Έγγραφο που χορηγείται σε άτομα με καθεστώς πρόσφυγα στο/στη <CC>
20-CC	Res idence document i ssued to European	Έγγραφο διαμονής που χορηγείται σε

		Union citizens and to citizens of Iceland, Liechtenstein, Norway and Switzerland residing in: <CC>	πολίτες της Ισλανδίας, του Λιχτενστάιν, της Νορβηγίας και της Ελβετίας οι οποίοι διαμένουν νομίμως στη χώρα: <CC>
	21-CC	Residence document issued to European Union citizens residing in: <CC>	Έγγραφο διαμονής που χορηγείται σε πολίτες της Ευρωπαϊκής Ένωσης οι οποίοι διαμένουν νομίμως στη χώρα: <CC>
	22	Authorization for entry to and stay in the Schengen Agreement area	Άδεια εισόδου και παραμονής στο χώρο εφαρμογής της Συμφωνίας Σένγκεν
	23	Document issued to stateless persons and foreign nationals with the right to remain in: <CC>	Έγγραφο το οποίο χορηγείται σε ανιθαγενείς και αλλοδαπούς με δικαίωμα παραμονής στο/στη <CC>
	24-CC	Document issued by: <CC> -pursuant to Article 28 of the Convention of 28 September 1954.	Έγγραφο το οποίο έχει εκδοθεί από το/τη <CC> δυνάμει του άρθρου 28 της Σύμβασης της 28ης Σεπτεμβρίου 1954
	25	Document establishing the holder's identity but not conferring Portuguese nationality. Confers a general status of equal rights and obligations on Brazilian nationals vis-a-vis Portuguese nationals.	Έγγραφο το οποίο προσδιορίζει την ταυτότητα του κατόχου του αλλά δεν παρέχει την πορτογαλική υπηκοότητα. Παρέχει ένα γενικό καθεστώς ίσων δικαιωμάτων και υποχρεώσεων στους υπηκόους της Βραζιλίας έναντι των υπηκόων της Πορτογαλίας
	26	Confirmation of Right of Abode in the United Kingdom	Επιβεβαίωση του δικαιώματος εγκατάστασης στο Ηνωμένο Βασίλειο
	27	Confirmation of indefinite leave to remain in the United Kingdom given by the Home Office Immigration and Nationality Directorate (IND).	Επιβεβαίωση της άδειας παραμονής επί αόριστον στο Ηνωμένο Βασίλειο η οποία χορηγείται από την Υπηρεσία Μετανάστευσης και Ημεδαπών (IND) του Υπουργείου Εσωτερικών (Home Office).
	28-CC	Driving licence issued to persons legally resident in: <CC>. Document establishes the holder's identity within the territory of that country but is not evidence of the holder's nationality.	Άδεια οδήγησης χορηγούμενη σε άτομα που διαμένουν νομίμως στη χώρα: <CC>. Το έγγραφο αυτό πιστοποιεί μεν την ταυτότητα του κατόχου στο έδαφος της εν λόγω χώρας, δεν αποτελεί όμως απόδειξη της εθνικότητάς του.
	29	Residence card for a family member of a European Union citizen; evidence for a third-country national who is a family member of a citizen of the EU, or of Iceland, Norway or Liechtenstein, of the right to move and reside freely within the territory of the Member States.	Άδεια παραμονής για μέλος της οικογένειας πολίτη της Ευρωπαϊκής Ένωσης· αποδεικνύει το δικαίωμα ελεύθερης κυκλοφορίας και διαμονής στο έδαφος των κρατών μελών υπηκόου τρίτης χώρας που έχει την ιδιότητα μέλους της οικογένειας πολίτη της ΕΕ ή της Ισλανδίας/Νορβηγίας/Λιχτενστάιν.
	30CC	Residence permit granting authorization to third country nationals to reside in: <CC> and to move within the Schengen Agreement Area.	Άδεια παραμονής η οποία παρέχει σε υπηκόους τρίτων χωρών δικαίωμα παραμονής στο/στη <CC> καθώς και δικαίωμα διακίνησης στο Χώρο εφαρμογής της Συμφωνίας Σένγκεν
	31CC	Residence permit for third country nationals with long-term EC residence status issued by: <CC>	Άδεια παραμονής επί μακρόν διαμένοντος ΕΚ για υπηκόους τρίτων χωρών που έχει εκδοθεί από το/τη <CC>
	32CC	Document for applicants for international protection issued by: <CC>	Έγγραφο για αιτούντες διεθνή προστασία που έχει εκδοθεί από το/τη <CC>
	33CC	Document for beneficiaries of subsidiary protection issued by: <CC>	Έγγραφο για δικαιούχους επικουρικής προστασίας που έχει εκδοθεί από το/τη <CC>
	34CC	Document for asylum seekers issued by:	Έγγραφο για αιτούντες άσυλο που έχει

		<CC>	εκδοθεί από το/τη <CC>
	35CC	Document confirming that an initial residence permit application has been submitted in: <CC>	Έγγραφο που αποδεικνύει ότι έχει υποβληθεί μια πρώτη αίτηση άδειας παραμονής στο/στη <CC>
	36CC	Document confirming that an application for an extension of a residence permit has been submitted in: <CC>	Έγγραφο που αποδεικνύει ότι έχει υποβληθεί αίτηση για παράταση άδειας παραμονής στο/στη <CC>
	37CC	Document establishing identity issued to diplomats and consular officials and to members of international organizations accredited in: <CC>.	Έγγραφο το οποίο προσδιορίζει την ταυτότητα και χορηγείται σε διπλωματικούς και προξενικούς υπαλλήλους καθώς και σε μέλη διεθνών οργανισμών διαπιστευμένων στο/στη <CC>
	38CC	Document establishing identity issued to administrative and technical staff of foreign representations accredited in: <CC>.	Έγγραφο το οποίο προσδιορίζει την ταυτότητα και χορηγείται στο διοικητικό και τεχνικό προσωπικό ξένων διπλωματικών και προξενικών αρχών διαπιστευμένων στο/στη <CC>
	39CC	Document establishing identity issued to service and private staff of foreign representations accredited in: <CC>.	Έγγραφο το οποίο προσδιορίζει την ταυτότητα και χορηγείται σε προσωπικό υπηρεσίας και ιδιωτικό προσωπικό ξένων διπλωματικών και προξενικών αρχών διαπιστευμένων στο/στη <CC>

	50	Proof of entry into the Schengen area at an external border	Αποδεικτικό εισόδου στο χώρο του Σένγκεν διαμέσου εξωτερικών συνόρων
	51CC	Proof of entry into the territory of: <CC> at an external border	Αποδεικτικό εισόδου διαμέσου εξωτερικών συνόρων στο έδαφος της εξής χώρας: <CC>
	52	Proof of departure from the Schengen area at an external border	Αποδεικτικό εξόδου από το χώρο του Σένγκεν διαμέσου εξωτερικών συνόρων
	53CC	Proof of departure from the territory of: <CC> at an external border	Αποδεικτικό εξόδου διαμέσου εξωτερικών συνόρων από το έδαφος της εξής χώρας: <CC>

Glossary reference numbers	en	Additional Safeguard	Πρόσθετο χαρακτηριστικό ασφαλείας
	en	Light Source	Φωτισμός
	NOR	NORMAL	ΚΑΝΟΝΙΚΟΣ
103	UV	ULTRAVIOLET	ΥΠΕΡΙΩΔΕΙΣ ΑΚΤΙΝΕΣ
173	TRA	TRANSMITTED	ΕΚΤΩΝ ΟΠΙΣΘΕΝ
049	IR	INFRARED	ΥΠΕΡΥΘΡΕΣ ΑΚΤΙΝΕΣ
156	OBL	OBLIQUE	ΛΟΞΟΣ
126	COA	CO-AXIAL	ΟΜΟΑΞΟΝΙΚΟΣ
	OTH	other	άλλος
	en	Main colours	Χρώματα
	1	white	λευκό
	2	grey	γκρίζο
	3	red	κόκκινο
	4	magenta (purple)	magenta (πορφυρό)

	5	yellow	κίτρινο
	6	green	πράσινο
	7	cyan (blue-green)	cyan (κυανοπράσινο)
	8	blue	μπλε
	9	violet	ιώδες (μωβ)
	10	brown	καφέ
	11	black	μαύρο
	12	burgundy	μπορντώ
	13	multi-coloured	πολύχρωμο
	14	other	άλλο
	15	gold	χρυσό
	16	silver	αργυρό
	17	orange	πορτοκαλί
	18	-	
	19	pink	ροζ
	20	beige	μπεζ
	en	Material	Υλικό
166	1	plastic	πλαστικό
	5	leather	δέρμα
	6	linen	πανί
087	8	paper	χαρτί
	13	other	άλλο
	en	Nationality	Εθνικότητα
Glossary reference numbers	en	Additional Safeguard	Πρόσθετο χαρακτηριστικό ασφαλείας
070	en	Numbering Position	Θέση αρίθμησης
	1	bottom right-hand corner	κάτω δεξιά
	2	bottom left-hand corner	κάτω αριστερά
	3	top right-hand corner	πάνω δεξιά
	4	top left-hand corner	πάνω αριστερά
101	5	perforated on all pages	διάτρητη σε όλες τις σελίδες
	6	bottom	κάτω μέρος σελίδας
	7	top	πάνω μέρος σελίδας
	8	bottom - centred	κάτω, στη μέση
	9	top - centred	πάνω, στη μέση
	10	top-right and bottom-left	πάνω δεξιά και κάτω αριστερά
	11	other	άλλη
	12	bottom outer corner	κάτω εξωτερική γωνία
	13	top outer corner	πάνω εξωτερική γωνία
	14	bottom inner corner	κάτω εσωτερική γωνία
	15	top inner corner	πάνω εσωτερική γωνία
011	en	OVD Type	Είδος OVD
039	1	hologram	ολογράφημα

054	2	Ki negram®	Ki negram® (κινεγράφημα)
079	3	P ixelgram®	P ixelgram® (εικονοστοιχειογράφημα)
176	4	Identi gram®	Identi gram® (ταυτογράφημα)
158	5	vari able laser i mage	μεταβαλλόμενη εικόνα λέιζερ
143	6	i ri descent lam i nate	ιριδίζουσα προστατευτική μεμβράνη
177	7	Movigram®	Movigram®
178	8	Stereogram®	Stereogram® (στερεόγραμμα)
	9	none	ουδέν
011	10	other	άλλο
055	11	retroref ective lam i nate	αντανακλαστική μεμβράνη
115	12	Alphagram®	Alphagram®
115	13	Exelgram®	Exelgram®
	en	Overall Construction	Υλική μορφή
119	CAR	card	κάρτα
058	BOO	multi ple booklet	πολλαπλό βιβλιάριο
058	SBO	s i ngle booklet	απλό βιβλιάριο
	FOL	folded	πολύπτυχο
	PAP	paper	χαρτί
	STI	sti cker	αυτοκόλλητο
083	STA	stamp	σφραγίδα

OTH other άλλη

Glossary reference numbers	en	Additional Safeguard	Πρόσθετο χαρακτηριστικό ασφαλείας
	en	Photo Type	Είδος φωτογραφίας
	1	black & wh i te	ασπρόμαυρη
	2	colour	έγχρωμη
	3	black & wh ite or colour	ασπρόμαυρη ή έγχρωμη
168	4	secondary (ghost) image - black & wh ite	δευτερογενής (φασματική) φωτογραφία, ασπρόμαυρη
168	5	secondary (ghost) image -monochrome	δευτερογενής (φασματική) φωτογραφία, μονόχρωμη
168	6	secondary (ghost) image - colour	δευτερογενής (φασματική) φωτογραφία, έγχρωμη
168	7	secondary (ghost) image	δευτερογενής (φασματική) φωτογραφία
107	8	secondary i mage - laser perforated	δευτερογενής φωτογραφία από διάτρηση με λέιζερ
168	9	secondary (ghost) image - UV	δευτερογενής (φασματική) φωτογραφία, αντιδρά σε υπεριώδεις ακτίνες
168	10	secondary (ghost) image - black & wh ite or colour	δευτερογενής (φασματική) φωτογραφία, ασπρόμαυρη ή έγχρωμη
122	en	Photo Integration Technique	Τεχνική ενσωμάτωσης της φωτογραφίας
046	1	laser pri nted (electro-photograph ic)	εκτύπωση με λέιζερ (ηλεκτροφωτογραφική)
047	2	i nkjetpri nted	εκτύπωση με ψεκασμό μελάνης
089	3	dye subl imati on	εξάχνωση χρωστικής
030	4	laser engraved	εγχάραξη με λέιζερ
161	5	photograph ic	φωτογραφική
122	6	other	άλλη
048	7	thermo transfer pri nted	εκτύπωση με θερμομεταφορά
107	8	laser perforated	διάτρηση με λέιζερ
179	9	holographi c	ολογραφία
	en	Printing Technique	Τεχνική εκτύπωσης
157	1	offset pri nti ng	όφσετ
097	2	letterpress pri nti ng	υψιτυπία (κλασική τυπογραφία)
002	3	i ntagli o pri nti ng	βαθυτυπία (χαλκοχαρακτική)
085	4	screen pri nti ng	μεταξοτυπία
155	5	needle pri nti ng	ακιδοτυπία
147	6	laser perforati on	διάτρηση με λέιζερ
030	7	laser engravi ng	εγχάραξη με λέιζερ
047	8	i nkjetpri nti ng	ψεκασμός μελάνης

046	9	laser print/copy	εκτύπωση / αντιγραφή με λέιζερ
089	10	thermal dye sublimation	θερμική εξάχνωση χρώματος

048	11	thermal transfer printing	θερμομεταφορά
161	12	photographic process	φωτογραφική μέθοδος
140	13	hot foil stamping	θερμοτυπία
125	14	bronze process	επιχάλκωση
139	15	gravure printing	περιστροφική βαθυτυπία
	16	handwritten	χειρόγραφη
029	17	relief embossing	ανάγλυφη εκτύπωση
101	18	needle perforation	διάτρηση με βελόνες
	19	other	άλλη
	en	Printing Technique-Security Element	Χαρακτ. ασφαλείας της τεχνικής εκτύπωσης
	1	standard	συνήθης
028	2	guilloches / fine line patterns	γραμμοκοσμήματα / λεπτόγραμμα μοτίβα
045	3	rainbow colouring	εκτύπωση ίριδος
092	4	OVI (optically variable ink)	οπτικώς μεταβλητή μελάνη (OVI)
069	5	see-through register	αμφιπλεύρως αλληλοσυμπληρούμενη παράσταση
067	6	miniprint	μινιεκτύπωση
068	7	microprint	μικροεκτύπωση
154	8	nanoprint	νανοεκτύπωση
129	9	endless text	ατέρμον κείμενο
043	10	latent image	λανθάνουσα εικόνα
120	11	anti-scan/anti-copy pattern	σχέδιο προστασίας από ηλεκτρονική σάρωση/ φωτοτυπία
042	12	scrambled (encrypted) image	κρυπτογραφημένη εικόνα (scrambled image)
052	13	iridescent ink	ιριδίζουσα μελάνη
142	14	iridescent, photochromic ink	ιριδίζουσα μελάνη φωτοχρωματική
141	15	iridescent, fluorescent ink	ιριδίζουσα μελάνη φθορίζουσα
124	16	bleeding ink	διδυτική μελάνη (bleeding ink)
066	17	metameric colours	μεταμερή χρώματα
151	18	metallic pigment	μεταλλική χρωστική
172	19	tinting effect	εφέ κλίσης
121	20	anti-Stokes ink	μελάνη που φθορίζει σε υψηλότερη συχνότητα
170	21	schablon (stencil) multiple colouring process	μέθοδος πολυχρωμίας με στένσιλ
112	22	collation mark	σημάδι ταξινόμησης
112	23	collation mark with page number (floating numbering)	σημάδι ταξινόμησης με αριθμό σελίδας (κλιμακωτή σελιδαρίθμηση)
093	24	fugitive / soluble ink	ευδιάλυτη μελάνη (fugitive ink)
094	25	thermochromic ink	θερμοχρωματική / θερμοευαίσθητη μελάνη
Glossary reference numbers	en	Additional Safeguard	Πρόσθετο χαρακτηριστικό ασφαλείας
	en	Print Mode	Τρόπος εκτύπωσης
086	PRT	pre-printed text	προεκτυπωμένο κείμενο
026	PRB	background / security printing	δάπεδο / εκτύπωση ασφαλείας
	OTH	other	άλλο
169	SNB	serial number	αύξων αριθμός
123	BIO	biographical / other personalization text	στοιχεία κατόχου ή άλλο εξατομικευτικό κείμενο

	en	Security Type	Είδος στοιχείου ασφαλείας
087	SUB	Substrate	Υπόστρωμα
181	BIO	Biometric	Βιομετρικά στοιχεία
103	UVF	UV feature	Αντίδραση σε υπεριώδεις ακτίνες
025	LAM	Laminated	Προστατευτική μεμβράνη
	ADS	Additional safeguard	Πρόσθετο χαρακτηριστικό ασφαλείας
011	OVF	Optically variable feature	Οπτικώς μεταβλητό στοιχείο
123	PER	Biographical data	Στοιχεία κατόχου
	PHO	Image of the holder	Εικόνα κατόχου
070	NUM	Numbering	Αρίθμηση
	PRT	Printing technique	Τεχνική εκτύπωσης
005	BIN	Binding	Δέσιμο
061	WAT	Watermark	Υδατόσημο
	OTH	Other	Άλλο
	en	Single / Double Pages	Απλές/διπλές σελίδες
180	SNG	single	απλές
180	DBL	double	διπλές
087	en	Substrate Material	Υλικό υποστρώματος
087	1	paper	χαρτί
088	2	photographic paper	φωτογραφικό χαρτί
166	3	PVC /polyvinylchloride)	PVC /πολυβινυλοχλωρίδιο)
159	4	PC /polycarbonate)	PC /πολυανθρακικό πολυμερές)
166	5	plastic	πλαστικό
	6	other	άλλο
087	7	cotton fibre paper	χαρτί από ίνες βαμβακιού
	en	Validity Period Time Measure	Χρονική μονάδα διάρκειας ισχύος
	Y	year(s)	έτος/έτη
	M	month(s)	μήνας/μήνες
	W	week(s)	εβδομάδα/εβδομάδες
	D	day(s)	ημέρα/ημέρες
103	en	UV Feature Type	Είδος αντίδρασης σε UV
087	1	substrate contains optical brightener	το υπόστρωμα περιέχει οπτικό λευκαντικό
133	2	fluorescent ink	φθορίζουσα μελάνη
137	3	fluorescent stitching thread	φθορίζον συρραπτικό νήμα
132	4	fluorescent fibres	φθορίζουσες ίνες
134	5	fluorescent planchettes	φθορίζοντα δισκία
024	6	fluorescent overprint	φθορίζουσα επιτύπωση
136	7	fluorescent serial number	φθορίζων αύξων αριθμός
168	8	image of the holder	εικόνα κατόχου
027	9	phosphorescent ink	φωσφορίζουσα μελάνη
160	10	photochromic ink	φωτοχρωμική μελάνη
103	11	other	άλλο
135	12	fluorescent security thread	φθορίζον νήμα ασφαλείας
087	13	substrate without optical brightener	υπόστρωμα χωρίς οπτικό λευκαντικό
111	14	hilites (fluorescent pigments in the	φθορίζοντα σωματίδια στο χαρτί (hilites

		paper)	ites)
	en	Validity Period	Διάρκεια ισχύος
	L	li mited / restri cted	περιορισμένη
	V	vari able	μεταβλητή
	I	i ndefi nite	επ' άοριστον
	S	s i ngle journey	ένα μόνο ταξίδι
061	en	Watermark Position	Θέση υδατοσήμου
061	1	random	τυχαία
061	2	pos iti oned	συγκεκριμένη
061	3	pos iti oned - centred	συγκεκριμένη - στο κέντρο
061	4	pos iti oned - top of page	συγκεκριμένη - κορυφή σελίδας
061	5	pos iti oned - upper portion of page	συγκεκριμένη - πάνω μέρος σελίδας
061	6	repeated	επαναλαμβανόμενο
061	7	other	άλλη
061	en	Watermark Type	Είδος υδατοσήμου
064	1	s i ngle tone	μονοτονικό
174	2	duotone	διτονικό
063	3	multitone	πολυτονικό
061	4	other	άλλο

Glossary reference numbers	en	Additional Safeguard	Πρόσθετο χαρακτηριστικό ασφαλείας
	en	Yes - no - not known	ναί - όχι - άγνωστο
	Y	yes	ναί
	N	no	όχι
	Not Known	not known	άγνωστο
	en	Type of Fraud	Είδος πλαστογραφίας
167	FOR	FORGERY	ΠΑΡΑΠΟΙΗΜΕΝΟ
127	COU	COUNTERFEIT	ΕΞ ΟΛΟΚΛΗΡΟΥ ΠΛΑΣΤΟ
163	FAN	PSEUDO DOCUMENT: Fantasy document	ΨΕΥΔΟΕΓΓΡΑΦΟ : Φανταστικό έγγραφο
164	CAM	PSEUDO DOCUMENT: Camouf age document	ΨΕΥΔΟΕΓΓΡΑΦΟ : [Εγγραφο παραλλαγής
165	PSE	OTHER PSEUDO DOCUMENT	ΑΛΛΟ ΨΕΥΔΟΕΓΓΡΑΦΟ
(162)		PSEUDO DOCUMENT	ΨΕΥΔΟΕΓΓΡΑΦΟ

Πίνακας Β.1: Αγγλο-ελληνικό λεξικό χαρακτηριστικών ασφαλείας ταξιδιωτικών εγγράφων [128,129]