



Δημοκρίτειο Πανεπιστήμιο Θράκης

Πολυτεχνική Σχολή Ξάνθης

Τμήμα Ηλεκτρολόγων Μηχανικών και

Μηχανικών Υπολογιστών.

Μελέτη και ανάπτυξη λογισμικού Εθνικού μητρώου πολιτών

« Η κάρτα του πολίτη »



Εργαστήριο Προγραμματισμού και

Επεξεργασίας Πληροφοριών

Τομέας Λογισμικού και Ανάπτυξης

Εφαρμογών

Επιβλέπων αναπληρωτής

καθηγητής :

Καράκος Αλέξανδρος

Ηλεκτρολόγος Μηχανικός &

Μηχανικός υπολογιστών:

Δημήτριος Βεζέρης

Ο σχεδιασμός δεν είναι μόνο με τι μοιάζει κάτι ή ποια είναι η αίσθησή του.
Σχεδιασμός είναι το πώς λειτουργεί.
Steve Jobs (1955-2011)

Στο Θοδωρή, την Ιωάννα, τον Ηλία, το Στέλλιο και τη Χρύσα.
Στα νέα παιδιά της νέας Ευρώπης.

Περιεχόμενα

Εισαγωγή.....	9
Εισαγωγή : Τι πραγματεύεται το μεταπτυχιακό, αναφορές στην Ελληνική διαβούλευση, τί ισχύει στην EU & USA	10
Περίληψη κεφαλαίων διατριβής	12
Η Ελληνική διαβούλευση.	14
Η δική μας προσέγγιση (περίληψη) - Σχεδιασμός και υλοποίηση της eCC.....	16
Στις Ηνωμένες Πολιτείες της Αμερικής.	19
Στην Ευρώπη.....	20
Σε άλλες χώρες	29
Τα συνέδρια [1],[2],[3]	38
Το Ευρωπαϊκό θεσμικό πλαίσιο	38
1ο Κεφάλαιο : Η Ελληνική πραγματικότητα (μητρώα πολιτών)	41
1.1 Οι αριθμοί ταυτοποίησης και μητρώων που ισχύουν στην Ελλάδα σήμερα (ΑΜΚΑ,Αρ. Δημοτολογίου, ΑΦΜ, Αρ.Δελτίου ΤΑΥΤΟΤΗΤΑΣ, Διαβατήριο)	42
1.2 Δημοτολόγιο	42
1.3 Δήλωση γέννησης	42
1.4 Δελτίο αστυνομικής ταυτότητας.....	43
1.5 Δικαιολογητικά έκδοσης Δελτίου Ταυτότητας	44
1.6 Ποιές πληροφορίες περιλαμβάνει η ταυτότητα	44
1.7 Αριθμός μητρώου κοινωνικής ασφάλισης (ΑΜΚΑ)	45
1.8 Απόδοση Αριθμού Φορολογικού Μητρώου Α.Φ.Μ.....	47
1.9 Τι δικαιολογητικά χρειάζονται και από πού εκδίδονται;.....	47
1.10 Διαβατήριο	48
1.11 Συμπεράσματα	48
2ο Κεφάλαιο : Η δική μας πρόταση ίδρυσης e-μητρώου πολιτών	51
2.1 Τι είναι ο e-αριθμός ταυτοποίησης (e-ID).....	52
2.2 Η μεγάλη πρόκληση.....	52
2.3 Χτίζοντας ένα πρόγραμμα ηλεκτρονικής διακυβέρνησης	53
2.4 Το χρονοδιάγραμμα υλοποίησης.....	54
2.5 Μητρώο πολιτών (Ταυτοποίηση – Κοινωνική ασφάλεια – Φορολογία - Υγεία)....	55
2.6 Στοιχεία του δελτίου ΑΜΚΑ – Πως προκύπτει ο αριθμός.....	57
2.7 Συγχώνευση υπολοίπων μητρώων.	57
2.8 Η περίπτωση των τραπεζών.....	58
2.9 Δεύτερο πεδίο στις βάσεις δεδομένων ο αριθμός του πολίτη (σε εμάς ο ΑΜΚΑ)	59
2.10 Η αρχιτεκτονική του πληροφοριακού συστήματος.....	60

2.11 Υπηρεσία έκδοσης κάρτας.....	61
2.12 Κύκλος ζωής κάρτας παραμονής.....	63
2.13 Εθνικές eIDs από τη σκοπιά της HP – Χρωματική διαφοροποίηση.	65
3ο Κεφάλαιο : Φυσική σχεδίαση της κάρτας του πολίτη	71
3.1 Η εμφάνιση	72
3.2 Η δική μας πρόταση.....	73
4ο Κεφάλαιο : Ηλεκτρονική σχεδίαση της κάρτας του πολίτη	77
4.1 Ηλεκτρονική σχεδίαση της κάρτας του πολίτη.....	78
4.2 Το CHIP.....	79
4.3 Διασύνδεση κάρτας και συστημάτων	81
4.4 Το μοντέλο του συστήματος υποστήριξης και αρχιτεκτονικής της κάρτας[16]....	83
4.5 Πλατφόρμα πλαισίου διαλειτουργικότητας [16].	85
4.6 Συμπεράσματα – Εφαρμογή & Επιλογές	86
5ο Κεφάλαιο : Ανάπτυξη λογισμικού	89
5.1 Τα επίπεδα από το Server μέχρι τον τελικό χρήστη.....	90
5.2 Εργαλεία ανάπτυξης λογισμικού e-μητρώου	93
5.3 SQL Server Express 2008.	95
5.4 Visual Web Developer 2010 Express	96
5.5 Το λογισμικό	97
5.6 Οι εκτυπώσεις	102
5.7 Τα στατιστικά.....	103
5.8 Συμπεράσματα.....	106
6ο Κεφάλαιο : Θέματα ασφαλείας.....	109
6.1 Οι 10 αμετάθετοι νόμοι της ασφάλειας.	110
6.2 Θέματα ασφαλών online δημόσιων υπηρεσιών.....	110
6.3 Δικαιώματα του πολίτη - ENISA.....	111
6.4 ID ανοιχτού τύπου	113
6.5 Πιστοποιητικά και διαπιστευμένα πιστοποιητικά.	115
6.6 Παγκόσμιες συγκλίσεις και αποκλίσεις σε θέματα ταυτοποίησης και ιδιωτικότητας.....	117
6.7 Προσωπικά στοιχεία στο διαδίκτυο.	120
6.8 bit4id	120
6.9 Διασυνοριακή ασφάλεια μέσα στην Ευρωπαϊκή Ένωση [STORK].	122
6.10 Υπηρεσίες PKI.	125
6.11 Ασφαλείς συσκευές δημιουργίας υπογραφής.....	126
6.12 Ασφάλεια και έξυπνα τηλέφωνα.	128

6.11 Κλοπή ή απώλεια της κάρτας – Διασφάλιση ασφάλειας.	129
6.12 Αποδεδειγμένη ταυτοποίηση.	129
7ο Κεφάλαιο : Περαιτέρω χρήσεις της κάρτας του πολίτη	133
7.1 BankID – Το παράδειγμα της Σουηδίας.	134
7.2 Η χρήση στις τράπεζες γενικότερα.	137
7.3 Mobile BankID	139
7.4 Διασυνορικές προδιαγραφές SEPA	140
7.5 Πανευρωπαϊκές υπηρεσίες (Υγείας & Κοινωνικής μέριμνας)	142
7.6 Ασφάλεια φυσικών χώρων & εγκαταστάσεων	145
7.7 Κινητό PKI, eID και Σουηδική αστυνομία	147
7.8 Διατρίβη – Η αστυνομία Online	150
7.9 Αεροπορικές εταιρίες – Super market.....	155
7.10 Συμπεράσματα	156
8ο Κεφάλαιο : Συμπεράσματα.....	157
8.1 Διασυνοριακή κατωχέρωση εταιρίας.	158
8.2 Επιτυχείς eid & e-gon υπηρεσίες στο Βέλγιο.....	161
Αναφορές.....	167
Παράρτημα Α : Συμφωνία Σέγκεν	173
Παράρτημα Β : Βιομετρικός έλεγχος.....	177
Παράρτημα Γ: Hacking	183
Παράρτημα Δ : Η ιστορία ενός διαβατηρίου	187

Στην μελέτη αυτή πιστεύουμε στην ενοποίηση όλων των μητρώων που αφορούν πληροφορίες σχετικές με τον πολίτη και ενδιαφέρουν το Ελληνικό κρατικό σύστημα και την Ευρωπαϊκή ολοκλήρωση ευρύτερα. Είναι στοιχεία σχετικά με την ταυτότητα, την περιουσία, την ασφάλιση, τη δικαιοσύνη, την μόρφωση, τη φορολόγηση του πολίτη και εν γένει ότι αφορά στις δημόσιες υπηρεσίες και αγαθά. Είναι λοιπόν σαφές ότι ένα κράτος, μια πολιτεία, μια ομοσπονδία, η οποία αποτελείται από εκατομμύρια πολίτες, να πρέπει να έχει ένα ηλεκτρονικό μητρώο πολιτών, το οποίο να περιέχει όλες τις πληροφορίες εκείνες με τις οποίες θα μπορεί να εξυπηρετεί καλύτερα και ποιοτικότερα τα μέλη του. Από την άλλη να μπορεί να αξιοποιεί καλύτερα τα μέλη του και να ξέρει από τι πλαισιώνεται η ύπαρξή του. Φανταστείτε για παράδειγμα στην παρούσα φάση οικονομικής και όχι μόνο κρίσης που περνάει η Ελλάδα, να μπορούσαμε από ένα τέτοιο μητρώο να βρούμε τους καλύτερους Έλληνες που θα βοηθούσαν στην απαλλαγή της χώρας από την οικονομική φόρτιση που τη διέπει (2010-2011-2012). Φανταστείτε δηλαδή το μητρώο να απαντούσε στην ερώτηση «Ποιοι πολίτες έχουν δύο διδακτορικά στα οικονομικά, έχουν επιχείρηση με πάνω από 30εκ τζίρο και είναι εύποροι και νομοταγείς».... και το σύστημα απλά να έβγαζε το αποτέλεσμα αμέσως.

Στη παρούσα μελέτη προσπαθούμε να προσεγγίσουμε τον τρόπο και τα στοιχεία που θα έπρεπε να λάβουμε υπόψη μας ώστε να γίνει πράξη το μητρώο πολιτών. Να γίνει έργο η «κάρτα του πολίτη» η οποία υπάρχει σήμερα σε πρωτόγονες μορφές όπως η αστυνομική μας ταυτότητα (εν αντιθέσει με τις πιστωτικές κάρτες που ήδη χρησιμοποιούν ασφαλή και σύγχρονη τεχνολογία) και τις πλαστικές κάρτες με τον ΑΜΚΑ.

Δεν είναι μόνο όμως η ύπαρξη μιας κάρτας που θα λύσει το πρόβλημα της γραφειοκρατίας και των χαμηλής ποιότητας υπηρεσιών που λαμβάνει ο Έλληνας πολίτης από το κράτος. Είναι η ίδια η οργάνωση της διακυβέρνησης η οποία είναι κατακερματισμένη παντού με ασύμβατα συστήματα μεταξύ τους, σε όλους τους τομείς δημόσιας διοίκησης στη χώρα. Η δική μας σκέψη είναι η ενοποίηση μητρώων και συστημάτων της ηλεκτρονικής διακυβέρνησης όπου σε ένα μητρώο (σε υποδομή διακομιστών του υπουργείου εσωτερικών ΥΠΕΣ για παράδειγμα ή της γενικής γραμματείας πληροφοριακών συστημάτων ΓΓΠΣ) θα μπορεί η δικαιοσύνη, λόγω χάρη, να καταχωρεί τα ποινικά αδικήματα του πολίτη, η εφορία τους φόρους και την τακτοποίηση αυτών, τα πανεπιστήμια να καταχωρούν τα πιστοποιητικά επιμόρφωσης του πολίτη κλπ. Φανταστείτε για παράδειγμα αντί να «τρέχετε» στο ΙΚΑ για να πάρετε ασφαλιστική ενημερότητα για είσπραξη χρημάτων από το Δημόσιο (π.χ. μιας υποτροφίας), να μπορεί ο φορέας να βλέπει online αν χρωστάτε ή όχι χρήματα στο Δημόσιο και αντίστοιχα να γίνεται ή όχι η εκταμίευση της υποτροφίας ή αντί για προσκόμιση ποινικού μητρώου, το δημόσιο να μπορεί να δει online αν έχετε καταδικαστεί ώστε να μπορείτε να πάρετε μέρος σε Δημόσιους διαγωνισμούς ή όχι κλπ. Συνεπώς η κάρτα απλά ταυτοποιεί τον κάτοχο, ενώ οι υπηρεσίες είναι αυτές που κρύβονται πίσω από ένα ολοκληρωμένο σύστημα διαχείρισης των πολιτών.

Εμείς σε αυτή τη μελέτη προσπαθούμε να αγγίξουμε μια σειρά από θέματα, τα οποία μας βοηθούν να κατανοήσουμε πως θα μπορούσε να υλοποιηθεί ολόκληρο το σύστημα αυτό, της ηλεκτρονικής διακυβέρνησης, της κάρτας του πολίτη και της ασφάλειας στη χρήση και έκδοσή της. Παράλληλα υλοποιούμε λογισμικό βασισμένο σε SQL Server και με τη χρήση Web .net framework και C#, μιας διαδικτυακής εφαρμογής διαχείρισης του μητρώου πολιτών.

Εισαγωγή

Εισαγωγικά παρατίθενται όλα τα στοιχεία που πλαισιώνουν, μέχρι σήμερα, διαβουλεύσεις γύρω από το θέμα, σε εθνικό και σε Ευρωπαϊκό επίπεδο. Αναφέρονται στοιχεία εφαρμογής σε άλλες χώρες. Περιγράφεται περιληπτικά η δική μας προσέγγιση, βάση της Ελληνικής πραγματικότητας και εφαρμογής. Επιπλέον αναφέρονται στοιχεία ολοκλήρωσης της eCC (electronic Citizen Card) και των υπηρεσιών προπαρασκευής του έργου.

Εισαγωγή : Τι πραγματεύεται το μεταπτυχιακό, αναφορές στην Ελληνική διαβούλευση, τι ισχύει στην EU & USA

Στόχος του παρόντος κειμένου είναι να μελετήσει και να προτείνει το πλαίσιο εφαρμογής της ηλεκτρονικής κάρτας του πολίτη (electronic Citizen Card – eCC - eID), η οποία θα διέπεται από τους παράγοντες της λιτής και απλής λειτουργίας και χρήσης της. Πλέον των γενικών ορισμών για την κάρτα θα γίνει μία καθαρά Ελληνική προσέγγιση. Η μελέτη θα είναι εναρμονισμένη με τα Ελληνικά δεδομένα, θα είναι μία μελέτη εφαρμογής και θα θέτει τις προδιαγραφές ολοκλήρωσης, ανάπτυξης και χρήσης αυτής της κάρτας.

Η στρατηγική i2010 ήταν το πλαίσιο πολιτικής της (Ευρωπαϊκής Ένωσης) ΕΕ για την κοινωνία της πληροφορίας και μέσων μαζικής ενημέρωσης (2005-2009). Προώθησε τη θετική συνεισφορά των τεχνολογιών πληροφοριών και επικοινωνιών (ΤΠΕ) για το τι μπορούν να κάνουν για την οικονομία, την κοινωνία και την προσωπική ποιότητα ζωής.

Η Ευρωπαϊκή ένωση μέσω του προγράμματος i2010, είχε εισηγηθεί την ανάπτυξη κάρτας eCC, ήτοι την **European** Citizen Card, η οποία με κάποια μορφή θα είχε ολοκληρωθεί έως το 2010. Λόγω της οικονομικής κρίσης που έχει επέλθει, το συγκεκριμένο έργο αναστάλθηκε και αναμένετε μία σταδιακή εισχώρηση της τεχνολογίας και της εφαρμογής αυτής στα κράτη μέλη της Ευρωζώνης ξεχωριστά (δυστυχώς – άποψή μας είναι ότι έπρεπε να εφαρμοσθεί από την Ευρωζώνη στο σύνολό της με απόφαση της Ευρωπαϊκής Επιτροπής και υποχρεωτική εφαρμογή από τα κράτη - μέλη).

Στόχος της μεταπτυχιακής διατριβής, όπως αναφέραμε είναι να μελετήσει και να προτείνει το πλαίσιο εφαρμογής της ηλεκτρονικής κάρτας του πολίτη (electronic Citizen Card – eCC - eID), η οποία θα διέπεται από τους παράγοντες της λιτής και απλής λειτουργίας και χρήσης της. Πλέον των γενικών ορισμών για την κάρτα που γίνετε, στοιχειοθετείται μία καθαρά Ελληνική προσέγγιση. Η μελέτη είναι εναρμονισμένη με τα Ελληνικά δεδομένα, και είναι μία μελέτη εφαρμογής που θέτει τις προδιαγραφές ολοκλήρωσης, ανάπτυξης και χρήσης αυτής της κάρτας, στην Ελλάδα.

Σε διαβούλευση που πραγματοποιήθηκε σε Εθνικό επίπεδο, δυστυχώς αντιμετωπίστηκε με καχυποψία και θρησκευτικές προκαταλήψεις. Η οργάνωση του μητρώου πολιτών το οποίο διασπαρμένα υπάρχει και σήμερα (δημοτολόγιο, μητρώο φορολογούμενων, μητρώο δελτίων ταυτότητας, μητρώο κοινωνικής ασφάλισης κλπ) σε ένα ενοποιημένο περιβάλλον εξυπηρετεί σε μεγάλο βαθμό την ποιότητα ζωής του πολίτη, τον προστατεύει από την παρανομία και επιφέρει εξοικονόμηση πλούτου.

Ζούμε σε ένα κόσμο όπου η επικοινωνία από απόσταση είναι πλέον καθημερινή και η διαπροσωπική επαφή ολοένα και τείνει να φθίνει. Σε αυτήν την όλο και λιγότερη προσωπική επικοινωνία είναι αναγκαία η αίσθηση εμπιστοσύνης να τεθεί σε νέα βάση και αντίληψη.

Επιπλέον ζούμε σε μία κοινωνία η οποία είναι αλληλένδετη με την ταχύτητα και το χρόνο , περισσότερο από ποτέ άλλοτε.

Χρειαζόμαστε χρόνο για να κάνουμε κάτι καλά, χρόνο για εμπειρία, χρόνο για να σκεφτούμε.

Αυτές οι ανθρώπινες και κοινωνικές ανησυχίες πρέπει να διευθετηθούν , να συζητηθούν να βρεθούν βελτιώσεις. Σε αυτόν το πολύπλοκο κόσμο που ζούμε πρέπει να κάνουμε κάθε προσπάθεια να συνεχίσουμε να βελτιώνουμε τις ζωές των ανθρώπων,

- Κάνοντας τα πράγματα ευκολότερα μειώνοντας το τεχνολογικό στρες,
- Με την εξασφάλιση της ασφάλειας των προσωπικών δεδομένων και των συναλλαγών,
- Με την ανάπτυξη νέων εργαλείων και υπηρεσιών προσαρμοζόμενων στις νέες ανάγκες ενός ψηφιακού κόσμου.

Κάνοντας τα παραπάνω θα απελευθερώσουμε χρόνο στους ανθρώπους, βοηθώντας τους να συγχρονίσουν τον φυσικό τους ρυθμό με τον ρυθμό του έξω κόσμου, ώστε να ζήσουν μια πιο ευχάριστη ζωή. [4]

Όταν όλες οι υπηρεσίες θα παρέχονται ηλεκτρονικά θα είναι απόλυτα «φυσικό» για τους ανθρώπους και τους οργανισμούς, οι πολίτες, οι επιχειρήσεις και η Δημόσια διοίκηση να επικοινωνούν ηλεκτρονικά. [5]

Εισαγωγή

Εδώ παραθέτονται όλα τα στοιχεία που πλαισιώνουν, μέχρι σήμερα, διαβουλεύσεις γύρω από το θέμα, σε εθνικό και σε Ευρωπαϊκό επίπεδο. Αναφέρονται στοιχεία εφαρμογής σε άλλες χώρες. Περιγράφεται περιληπτικά η δική μας προσέγγιση, βάση της Ελληνικής πραγματικότητας και εφαρμογής. Επιπλέον αναφέρονται στοιχεία ολοκλήρωσης της eCC (electronic Citizen Card) και των υπηρεσιών προπαρασκευής του έργου.

1ο Κεφάλαιο

Αρχικά επιχειρείται η συγκέντρωση όλων των στοιχείων των Ελληνικών μητρώων, ώστε να διερευνηθούν οι δυνατότητες συγχώνευσης όλων των μητρώων σε ένα. Γίνετε σύγκριση μεταξύ των μητρώων και των δικαιολογητικών που απαιτούνται για κάθε εισαγωγή εγγραφής. Τελικά συμπεραίνετε η δυνατότητα συγχώνευσης καθώς και η αλληλεξάρτηση μεταξύ τους.

2ο Κεφάλαιο

Παρουσιάζεται η δική μας πρόταση ίδρυσης του e-μητρώου πολιτών. Ο τρόπος ολοκλήρωσης αλλά και μετάβασης στην νέα κατάσταση, σε εθνικό επίπεδο. Επιπλέον ορίζονται χρωματικές διαφορές σε σχέση με την ιδιότητα του πολίτη, όπως Έλληνας υπήκοος, Αλλοδαπός εργαζόμενος, Τουρίστας, Ενήλικας – Ανήλικος κλπ.

3ο Κεφάλαιο

Εδώ αναλύεται και παρουσιάζεται η πρότασή μας για τη φυσική σχεδίαση της κάρτας. Αναλύονται και αιτιολογούνται, το είδος και η ποσότητα των προσωπικών στοιχείων που θα εμφανίζονται πάνω σε αυτή. Ορίζονται τα ελάχιστα στοιχεία για την προσωπική ταυτοποίηση του κατόχου, ιδιαίτερα σε περιπτώσεις διακοπής ρεύματος και αστοχίας εξακρίβωσης μέσα από το πληροφοριακό σύστημα.

4ο Κεφάλαιο

Σχεδιασμός της ηλεκτρονικής κάρτας του πολίτη. Αναλύονται οι τεχνολογίες έξυπνων καρτών και RFID. Επιλέγεται η τεχνολογία χρήσης καθώς και αναλύονται τα αντίστοιχα επιχειρήματα αλλά και αδύνατα σημεία. Περιγράφεται η δομή, το είδος και η ποσότητα των δεδομένων που θα μπορεί να φέρει η κάρτα.

5ο Κεφάλαιο

Λογισμικό διαχείρισης. Στο συγκεκριμένο κεφάλαιο αιτιολογείται η χρήση συγκεκριμένων τεχνολογιών λογισμικού για την ανάπτυξη ενός τέτοιου μητρώου διαχείρισης πολιτών. Αναφέρονται όλες οι δυνατές πλατφόρμες ανάπτυξης και ολοκλήρωσης του έργου. Επιπλέον αναπτύσσεται demo λογισμικό για την εφαρμοσμένη δοκιμή της διατριβής.

6ο Κεφάλαιο

Στο κεφάλαιο αυτό αναλύονται θέματα ασφάλειας κατά την χρήση αλλά και την λειτουργία του συστήματος κάρτας – δικτύου. Αναφέρονται θέματα σε περιπτώσεις hacking, κλοπής ή απώλειας κλπ. Αναφέρονται όλα τα αδύνατα σημεία του θέματος και τρόποι αντιμετώπισης όπου είναι δυνατό.

7ο Κεφάλαιο

Χρήσεις και εφαρμογές πέρα από την κάρτα του πολίτη. Γίνετε προσέγγιση και αναλύονται τεχνικές όπου η κάρτα του πολίτη να αποτελέσει ένα πολύ-εργαλείο – πασπαρτού τόσο για άλλες δημόσιες υπηρεσίες όσο και για ιδιωτικές. Όσο αφορά στις ιδιωτικές, αναλύονται εφαρμογές από iBank μέχρι και προγράμματα δώρων από αεροπορικές εταιρίες.

Εφαρμογές – Δυσκολίες – Συμπεράσματα.

Τέλος, συνοψίζοντας όλα τα παραπάνω, απορρέουν τα ανάλογα συμπεράσματα, όσο αφορά θέματα υλοποίησης, εφαρμογής, χρήσης καθώς και των δυσκολιών που προκύπτουν.

Στην Ελλάδα το Δεκέμβριο του 2010 έλαβε χώρα η διαβούλευση για την κάρτα του πολίτη, επικεντρωμένη στα παρακάτω θέματα:

- Αξιοποίηση, επέκταση και ανάπτυξη νέων ηλεκτρονικών υπηρεσιών από τη Δημόσια Διοίκηση,
- Προστασία των προσωπικών δεδομένων και της ιδιωτικότητας των πολιτών,
- Προστασία ασφάλειας των συναλλαγών,
- Εισαγωγή και αξιοποίηση καινοτόμων ηλεκτρονικών υπηρεσιών από τον ιδιωτικό τομέα,
- Τεχνικές προτάσεις για το σχεδιασμό και υλοποίηση της κάρτας του πολίτη,
- Προτάσεις για την οργανωτική και επιχειρησιακή αρτιότητα του συνολικού εγχειρήματος.

Κατά την άποψή μου δεν έχει γίνει θετική και ολοκληρωμένη διαβούλευση λόγω:

- Μικρής πληροφόρησης σχετικά με το θέμα με αποτέλεσμα ενός μεγάλου κινήματος αντίδρασης ,
- Ανωριμότητα στην κατάσταση μηχανογράφησης του Δημοσίου,

Η κατ 'αρχήν δική μας προσέγγιση, διέπεται από την παραδοχή ότι η κάρτα θα χαρακτηρίζει με ένα και μοναδικό αριθμό, με το ίδιο μητρώο για τον πολίτη, για το δημότη, για το φοιτητή, τον αγρότη, το φορολογούμενο, τον ασφαλισμένο κλπ. Όλες αυτές οι ιδιότητες άπτονται πάνω στον πολίτη της Ευρωπαϊκής ένωσης, κάτοικο Ελλάδος, ο οποίος έχει ένα και μοναδικό αριθμό, για όλες του τις ιδιότητες.

Σκοπός και πλαίσιο – θέματα που προκύπτουν:

- Η κάρτα του πολίτη αποτελεί την ψηφιακή ταυτότητα, την φυσική ταυτοποίηση των στοιχείων και χρήσεων (π.χ. με την κάρτα αυτή δηλώνω ώρα προσέλευσης και αποχώρησης από την εργασία).
- Επιπλέον μπορεί να φέρει ψηφιακή υπογραφή.
- Μπορεί να παρέχονται υπηρεσίες από ιδιωτικές επιχειρήσεις.
- Υπάρχουν θέματα με το τι γίνεται σε περίπτωση απώλειας.
- Προσωρινή κάρτα πολίτη (π.χ. σε τουρίστες/ αλλοδαπούς εργαζόμενους, μετανάστες)
- Τι γίνεται σε διακοπή ρεύματος, - φυσική ταυτοποίηση με στοιχεία πάνω στην κάρτα,

- Υπηρεσίες μπορούν να ενεργοποιούνται προαιρετικά,
- Θέματα προσωπικών δεδομένων, ασφάλειας και θρησκείας,
- Block κάρτας για λάθος pin, προσοχή στην αλλαγή στοιχείων, διαβατήριο, ποιος έχει δικαίωμα στα στοιχεία κλπ

Θέματα που τέθηκαν στην διαβούλευση:

- Επιτήρηση και έλεγχος των λαών,
- Οι Χριστιανοί αναφέρουν πριν 2000 χρόνια για το 666 αλλά υπάρχει και το facebook για το φακέλωμα,
- Έξοδα εν μέσω οικονομικής κρίσης,
- Ασφάλεια δεδομένων,
- Να είναι προαιρετική,
- Χρήση εναλλακτική της ταυτότητας,
- Απώλεια,
- Όχι υποχρεωτική χρήση σε όλες τις υπηρεσίες,
- Διάλυση των ΚΕΠ,
- Διαφθορά υπαλλήλων,
- Προσωπικά δεδομένα,
- Τεχνολογία εξ' αποστάσεως (RFID πλίνθου και όχι bar code)
- Πρόσβαση φορέα, θα δίνετε πρόσβαση μέσω Pin
- Οι υπηρεσίες υπάρχουν και δεν αποδίδουν, γιατί θα αποδώσουν με την κάρτα,
- Αγοραπωλησίες,
- Ποια θα είναι τα πρότυπα έγγραφα για την κάρτα,
- Φόβοι για hackers (Chaos Computer Club, Αγγλία - Γερμανία),
- DNA, Ίριδα, Δακτυλοσκόπηση, Ιριδοσκόπηση για ταυτοποίηση,
- ΑΜΚΑ = e-ID (Θα μπορούσε γιατί περιέχει και την ημερομηνία γέννησης)
- Διάρκεια 100 ετών,
- Υπηρεσίες μέσω internet
- Φάρμακα μέσω κάρτας και ηλεκτρονική συνταγογράφηση,

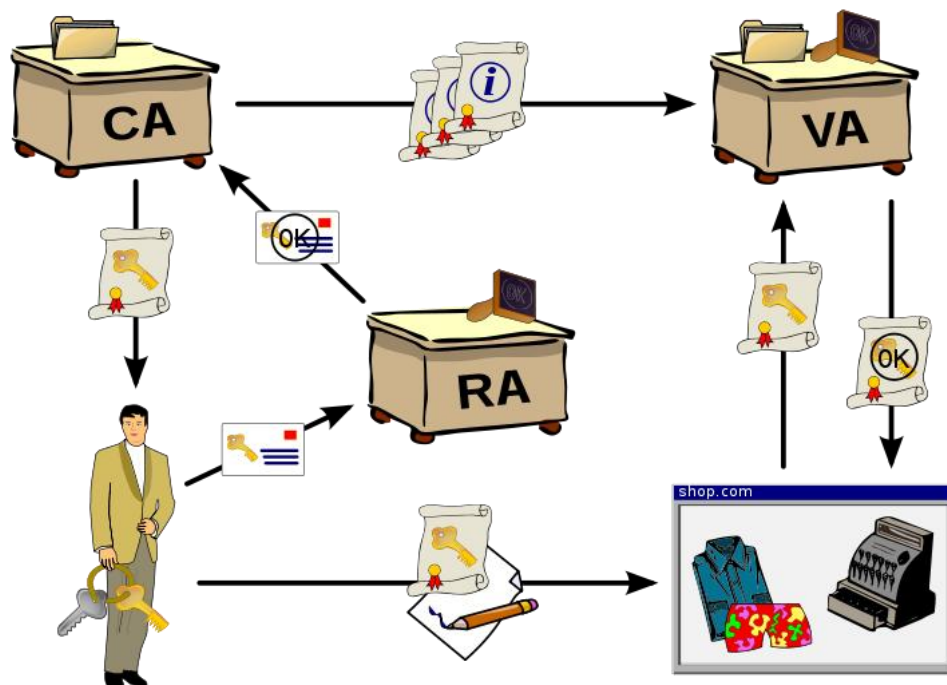
Θέματα για τα Τεχνικά χαρακτηριστικά

- Η κάρτα θα μπορούσε να έχει διαστάσεις όπως η κάρτα τράπεζας ανάληψης μετρητών. Θα φέρει πλινθίο, στοιχεία κατόχου και φωτογραφία.

- Θα μπορούσε να αποτελεί ψηφιακή υπογραφή, χωρίς barcode, με δημόσια και ιδιωτική χρήση.
- Θα μπορούσε να έχει δύο επίπεδα ασφάλειας, π.χ. Ονοματεπώνυμο και φωτογραφία, τα υπόλοιπα προς ταυτοποίηση (στο πλινθίο).
- Για να ξεκλειδώνει το view των περισσοτέρων δεδομένων θα θέλει pin.
- Η επαφή θα είναι και με επαφή και εξ' αποστάσεως. Η κάρτα θα είναι μόνο για ανάγνωση.

Η δική μας προσέγγιση (περίληψη) - Σχεδιασμός και υλοποίηση της eCC.

Χρειάζεται Εθνική υποδομή για Δημόσιο Κλειδί. Για την ολοκλήρωση του έργου μπορεί να χρησιμοποιηθεί το ΕΣΠΑ, ειδική μεταρρύθμιση – Ψηφιακή σύγκλιση. Το κλειδί αυτό θα μπορούσε να είναι πλέον ο ΑΜΚΑ σε όλα τα μητρώα για αρχή και να αποτελεί το μοναδικό αριθμό που μπορεί να δίνεται με τη γέννηση (η οποία ημερομηνία περιλαμβάνεται μέσα στον αριθμό). Μπορούν να εφαρμοστούν τεχνικές PKI (**Public Key Infrastructure (PKI)**) το οποίο περιέχει μεθόδους πιστοποίησης (http://en.wikipedia.org/wiki/Public_key_infrastructure).





Έτσι λοιπόν ο κάθε Έλληνας υπήκοος που σήμερα έχει την Ελληνική ταυτότητα, αλλά και κάτω των 18 θα έχει τη δική του eCC. Η κάθε eCC θα είναι μοναδική και θα φέρει τον ΑΜΚΑ για αριθμό ID του πολίτη (eID).

Εδώ θα εξετάσουμε (αναφέρουμε για πρώτη φορά) την ύπαρξη 4 ειδών “**χρωματικά**” καρτών, αναλόγως την προέλευση και την ιδιότητα του κατόχου. Η **μπλε** κάρτα θα συμβολίζει ότι ο κάτοχος είναι Έλληνας υπήκοος, ότι διαμένει και εργάζεται νόμιμα στην Ελλάδα ως Έλληνας πολίτης. Η κάρτα χρώματος **πορτοκαλί** θα συμβολίζει ότι ο κάτοχος είναι Έλληνας πολίτης κάτω των 18. Η **πράσινη** κάρτα θα συμβολίζει ότι ο κάτοχός της είναι αλλοδαπός, βρίσκεται νόμιμα στη χώρα και μπορεί να διαμένει και να εργάζεται ή να επιχειρεί νόμιμα στην Ελλάδα. Την ίδια κάρτα θα φέρουν και τα παιδιά του, τα οποία μετά την απόκτηση της Ελληνικής υπηκοότητας η κάρτα θα γίνεται μπλε ή πορτοκαλί. Τέλος θα υπάρχει και η **λευκή** κάρτα, η οποία θα είναι εθελοντική και θα συμβολίζει ότι ο κάτοχός της, έχει είναι εγγεγραμμένος στο μητρώο πολιτών που τηρεί η Ελλάδα και βρίσκεται νόμιμα σε

αυτήν. Αυτή την κάρτα θα μπορεί να φέρει οποιοσδήποτε τουρίστας – επισκέπτης εισέρχεται στην Ελλάδα, ο οποίος με τη χρήση αυτής θα μπορεί να απολαμβάνει τις σύγχρονες ψηφιακές υπηρεσίες του κράτους και των ιδιωτών καθώς και θα αποφεύγει οποιοδήποτε έλεγχο στοιχείων από τα σώματα ασφαλείας και τις αρχές.

Θα εξεταστεί η **συγχώνευση όλων των μητρώων** σε ένα, αυτό της eCC, όπου με αναφορά του eID της eCC, ο κάτοχος θα έχει πρόσβαση σε όλες της υπηρεσίες, όπως ΙΚΑ και εν γένει ασφαλιστικά ταμεία, Δήμους, Εκλογικά δικαιώματα, Αστυνομία, Εφορία, Δικαιοσύνη, Υγεία, Εκπαίδευση κλπ. Ο αριθμός ID της κάρτας του πολίτη θα είναι άμεσα και ΑΦΜ και ΑΜΚΑ, και μητρώο ΙΚΑ ή ΤΣΜΕΔΕ ή ΟΑΕΕ και Αριθμός ταυτότητας και Αριθμός δημοτολογίου καπ.

Θα δούμε ποια στοιχεία – τα ελάχιστα δυνατά θα φέρει η **φυσική** σχεδίαση της κάρτας του πολίτη, τα οποία σε οποιαδήποτε διακοπή ρεύματος θα μπορεί να **ταυτοποιεί** τον κάτοχο.

Θα εξετάσουμε την ηλεκτρονική **προδιαγραφή** της κάρτας, ώστε αυτή να φέρει **ψηφιακή υπογραφή** – ταυτοποίηση του κατόχου και να ανοίξει το δρόμο της ηλεκτρονικής εξυπηρέτησης του πολίτη.

Μετά τον καθορισμό των παραπάνω προδιαγραφών, θα προτείνουμε το **λογισμικό** και τις **τεχνολογίες**, οι οποίες θα μπορούσαν να υποστηρίξουν τη λειτουργία και την υλοποίηση ενός τέτοιου έργου, της eCC.

Τέλος θα τεθούν **επίπεδα ασφαλείας** για πρόσβαση αλλά και τροποποίηση των στοιχείων του πολίτη, για τις διάφορες υπηρεσίες, θα εξεταστεί η χρησιμότητα και η επέκταση των υπηρεσιών και στον ιδιωτικό τομέα καθώς και οι δυσκολίες που μπορεί να παρουσιαστούν στην εφαρμογή του έργου.

Πριν αρχίσουμε τη μελέτη και την ανάλυση των δεδομένων μας, ας ρίξουμε μια ματιά να δούμε τι γίνεται στη γειτονιά μας και σε άλλες χώρες του πλανήτη.

ΟΙ 10 ΧΩΡΕΣ ΤΗΣ Ε.Ε. ΜΕ ΗΛΕΚΤΡΟΝΙΚΕΣ ΤΑΥΤΟΤΗΤΕΣ		
Χώρα	Χρήση βιομετρικών δεδομένων	Φορείς έκδοσης και διαχείρισης της ταυτότητας
 Αυστρία	Όχι	Ιδιωτικοί, με κρατική άδεια
 Βέλγιο	Όχι	Δημόσιοι
 Γερμανία	Όχι	Δημόσιοι
 Εσθονία	Όχι	Δημόσιοι
 Ισπανία	Ναι	Δημόσιοι
 Ιταλία	Ναι	Δημόσιοι
 Λιθουανία	Ναι	Δημόσιοι
 Πορτογαλία	Ναι	Δημόσιοι
 Σουηδία	Όχι	Ιδιωτικοί με κρατική άδεια
 Φινλανδία	Όχι	Δημόσιοι

Σημ.: Η γερμανική ταυτότητα θα διατίθεται από την 1η/11/2010, ενώ Λουξεμβούργο και Τσεχία προτίθενται να προστεθούν στον κατάλογο των χωρών με ψηφιακές ταυτότητες το 2011 και το 2012 αντιστοίχως

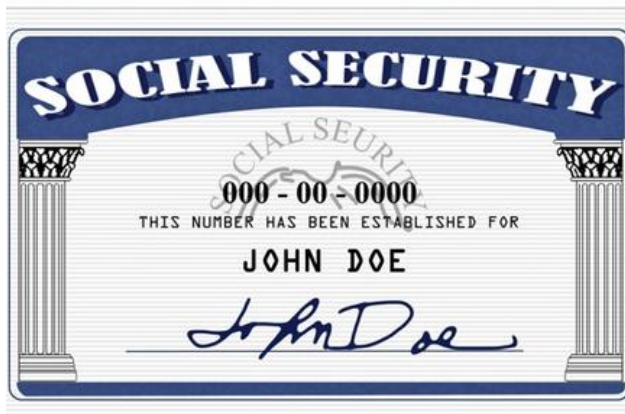
Στις Ηνωμένες Πολιτείες της Αμερικής.

Δεν υπάρχει πραγματική εθνική ταυτότητα στις Ηνωμένες Πολιτείες της Αμερικής, με την έννοια ότι δεν υπάρχει ομοσπονδιακή υπηρεσία με αρμοδιότητα σε εθνικό επίπεδο σε θέματα που συνδέονται άμεσα με τις κάρτες αυτές σε όλους τους Αμερικανούς πολίτες για την υποχρεωτική τακτική χρήση. Όλες οι νομοθετικές προσπάθειες απέτυχαν λόγω σθεναρής αντίστασης από φιλελεύθερες και συντηρητικές παρατάξεις όσο, αφορά την κατάργηση της τοπικής εθνικής (πολιτειακής) ταυτότητας.

Προς το παρόν, η μόνη εθνική ταυτότητα είναι η κάρτα διαβατηρίου που εκδίδεται σε πολίτες των ΗΠΑ μόνο από εθελοντική εφαρμογή. Παρά το γεγονός ότι η κύρια χρήση της είναι για ταξιδιωτικές υπηρεσίες οι Αμερικανοί την χρησιμοποιούν και σε άλλες υπηρεσίες ως ταυτότητα.

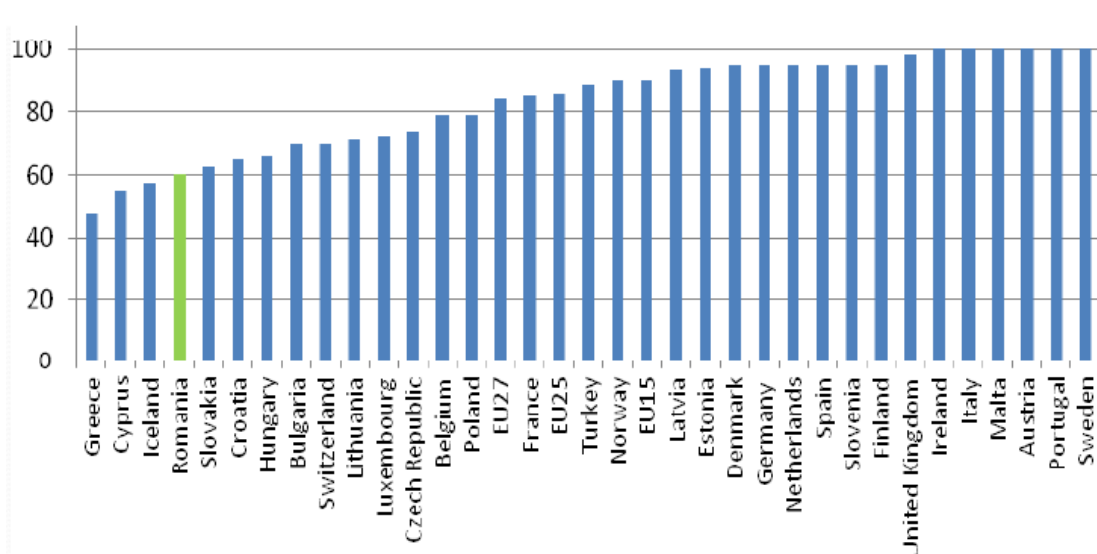


Μία άλλη κάρτα στις Ηνωμένες Πολιτείες της Αμερικής που πάει να γίνει η de facto κάρτα του πολίτη είναι η κάρτα εθνικής ασφάλειας (SSN)

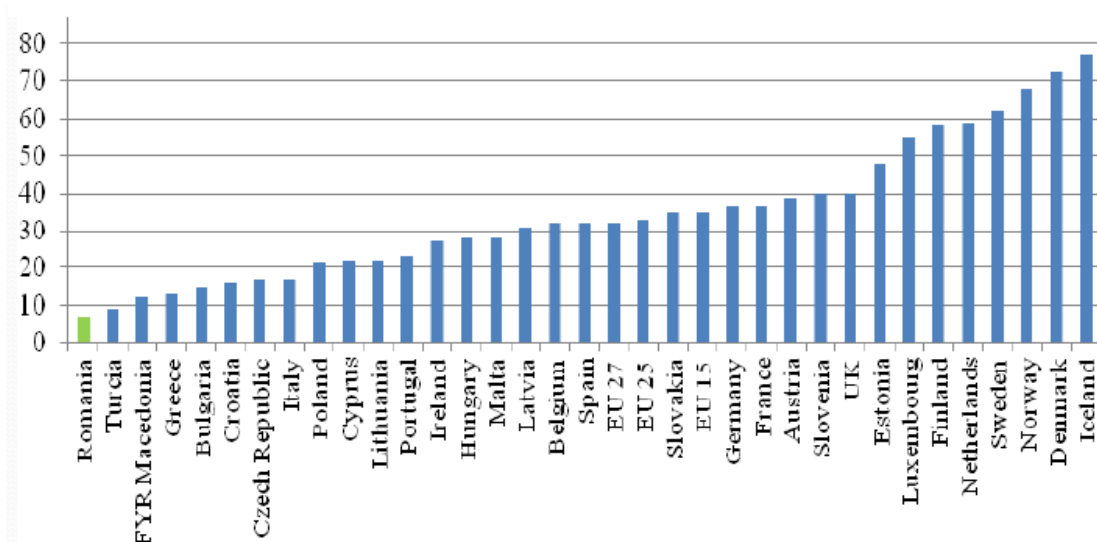


Στην Ευρώπη

Στην Ευρώπη οι υπηρεσίες ηλεκτρονικής διακυβέρνησης έχουν ολοκληρωθεί σε ποσοστά που εμφανίζονται στον παρακάτω πίνακα.[9]



Ενώ παρακάτω εμφανίζονται τα ποσοστά πληθυσμού που κάνουν χρήση των υπηρεσιών ηλεκτρονικής διακυβέρνησης.[9]



Η μπλε κάρτα.

Η Blue Card ή Blue European Labour Card, είναι εγκεκριμένη με την οδηγία (Council Directive 2009/50/EC). Η κάρτα αυτή εκδίδεται για υψηλά ειδικευμένους πολίτες εκτός Ευρωπαϊκής Ένωσης, οι οποίοι επιθυμούν νόμιμα να δουλέψουν σε κράτη μέλη αυτής.

Η κάρτα αυτή είχε προταθεί από τον πρόεδρο της επιτροπής Manuel Barosso και έγινε αποδεκτή από το Ευρωπαϊκό κοινοβούλιο αλλά έχει ακόμα αντιδράσεις στην εφαρμογή της.

Βουλγαρία

Στη Βουλγαρία ο κάθε υπήκοος άνω των 14^{ων} ετών υποχρεούται να αιτηθεί έκδοση ταυτότητας. Σε κάθε έλεγχο της αστυνομίας θ πρέπει να μπορεί να την υποδεικνύει.



Γαλλία

Στη Γαλλία η ταυτότητα υπάρχει από το Β' παγκόσμιο πόλεμο. Το 1955 όμως εισήχθη μία νέα εθελοντική κάρτα του πολίτη η carte nationale d'identité (CNI) για τους Γάλλους. Αυτή τη στιγμή διαβουλεύονται για νέα κάρτα με βιομετρικά στοιχεία αλλά και με προσκρούσεις στις υπηρεσίες ανθρωπίνων δικαιωμάτων. Πάντως σε έλεγχο από αρχές ο Γάλλος πολίτης μπορεί να αποδείξει την ταυτότητά του με οποιοδήποτε νομιμοποιητικό έγγραφο (δίπλωμα, πιστωτική, υγείας κλπ) και είναι στο χέρι της αρχής και του περιστατικού – ελέγχου για την αποδοχή της.



Γερμανία

Είναι υποχρεωτικό για όλους τους Γερμανούς πολίτες με ηλικία 16 ή άνω να διαθέτουν είτε Personalausweis (δελτίο ταυτότητας) ή το διαβατήριο, αλλά όχι για να το φέρουν μαζί τους. Αν και οι αστυνομικοί και μερικοί άλλοι αξιωματούχοι έχουν δικαίωμα να ζητήσουν να δουν ένα από τα έγγραφα αυτά, ο νόμος δεν αναφέρει ότι είναι κανείς υποχρεωμένος να υποβάλει το έγγραφο εκείνη τη στιγμή. Αλλά, όπως δεν είναι οι άδειες οδήγησης αποδεκτά νόμιμα έγγραφα ταυτοποίησης στη Γερμανία, μερικοί άνθρωποι επιλέγουν να μεταφέρουν την Personalausweis τους μαζί τους.

Ξεκινώντας το Νοέμβριο του 2010, τα γερμανικά δελτία ταυτότητας χορηγούνται στην ID-1 μορφή και μπορούν επίσης να περιλαμβάνουν μια ολοκληρωμένη ψηφιακή υπογραφή, εφόσον το επιθυμούν οι πολίτες. Μέχρι τον Οκτώβριο του 2010, η γερμανικές ταυτότητες εκδόθηκαν στο πρότυπο ISO / IEC 7810 ID-2 μορφή.



Στη Γερμανία η στρατηγική της ηλεκτρονικής κάρτας έχει τις παρακάτω μορφές [15]:



ePA: Ηλεκτρονική κάρτα του πολίτη

eGK: Ηλεκτρονική κάρτα υγείας

eLena : Κάρτα εργασίας

ELSTER: ηλεκτρονική δήλωση φόρου

Ρουμανία

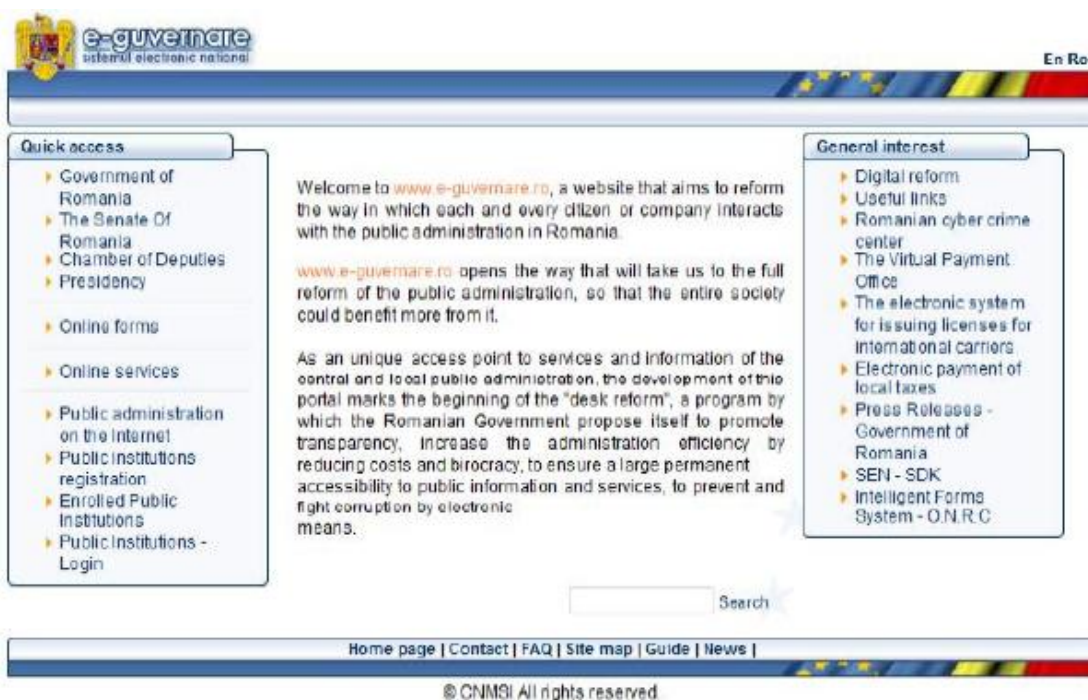
Εδώ πρέπει μετά τα 14 ο κάθε πολίτης να παραλάβει την κάρτα του (ταυτότητα), υποχρεωτικά και να την ανανεώνει κάθε 10 χρόνια. Με την κάρτα αυτή όμως μπορεί να ταξιδεύει μέσα στη χώρα αλλά και στις υπόλοιπες χώρες της Ευρωπαϊκής Ένωσης.



Από το 2014 όμως θα έχει ολοκληρωθεί νέα έργο για την έκδοση καρτών πολιτών στη Ρουμανία.

Το 2011 η Ρουμανία είναι στις 14 χώρες οι οποίες δηλώνουν έτοιμες για το αύριο. Αναγνωρίζει την σημαντικότητα και την πρόκληση της ευρυζωνικότητας. [9]

- 38% Σπίτια με πρόσβαση στο διαδίκτυο,
- 73% Επιχειρήσεις με πρόσβαση στο διαδίκτυο,
- 24% Σπίτια με ευρυζωνική πρόσβαση στο διαδίκτυο,
- 41% Επιχειρήσεις με ευρυζωνική πρόσβαση στο διαδίκτυο,
- 31% Πολίτες με τουλάχιστον μία πρόσβαση στο διαδίκτυο την εβδομάδα,
- 61% Πολίτες δεν έχουν κάνει χρήση internet.





Πορτογαλία

Στην Πορτογαλία έχει γίνει μία πολύ καλή πρακτική από το 2007, όπου όλοι οι πολίτες έχουν ηλ. Κάρτα. Υπάρχει το νομικό πλαίσιο, η πολιτικές διαπίστευσης και ασφάλειας, οι υποδομές ασφάλειας, αξιοπιστίας, διαθεσιμότητας, αυθεντικότητας και ακεραιότητας και έχουν δοθεί οι προσβάσεις. Το όραμα της Πορτογαλικής κυβέρνησης είναι να τοποθετεί πολίτες και επιχειρήσεις στο κέντρο μιας μοντέρνας και καινοτόμας δημόσιας διοίκησης [5],[8]

Στην Πορτογαλία σήμερα (Οκτώβριος του 2011), 6,2εκ πολίτες έχουν τη νέα κάρτα.



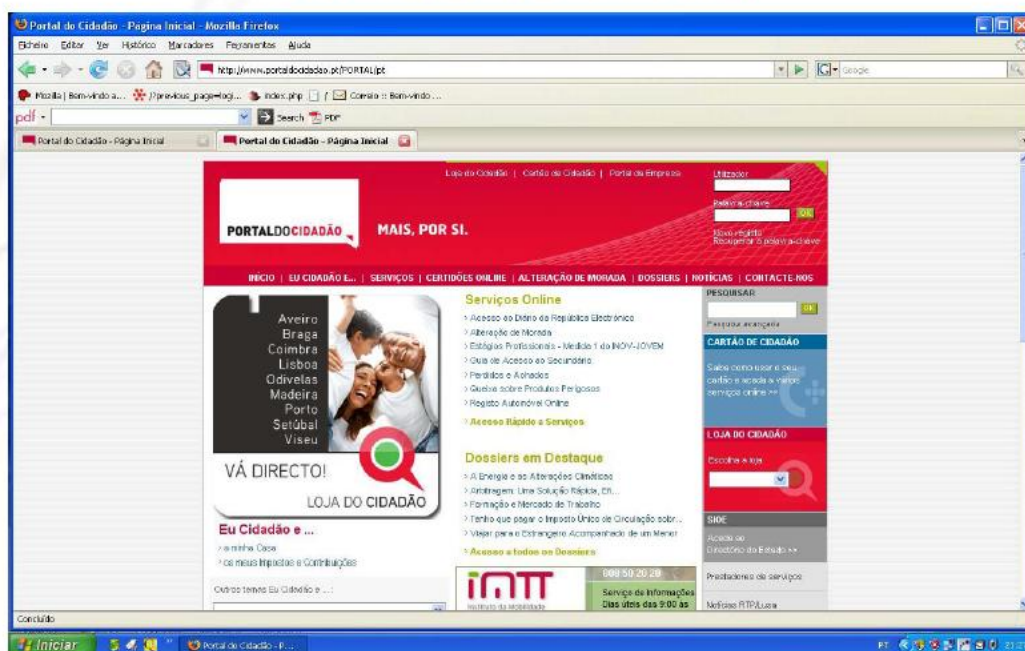
Επιπλέον οι πολίτες μέσω internet απολαμβάνουν κάποιες υπηρεσίες που έχουν μηχανογραφηθεί.

Government Web Portal



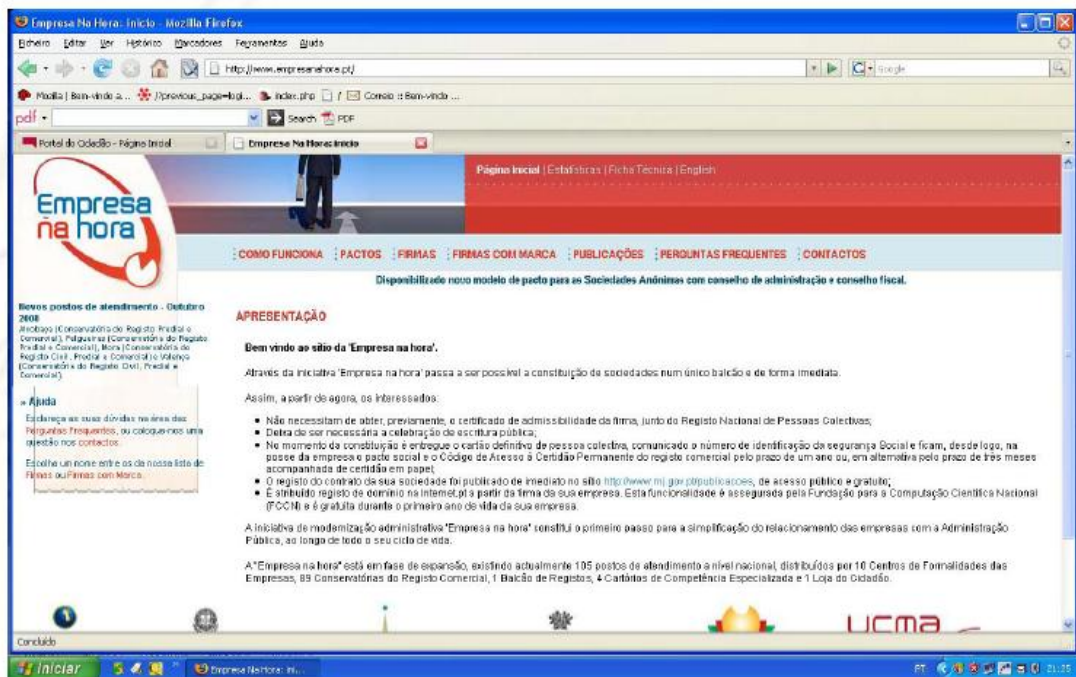
www.portugal.gov.pt

Citizen's Web Portal

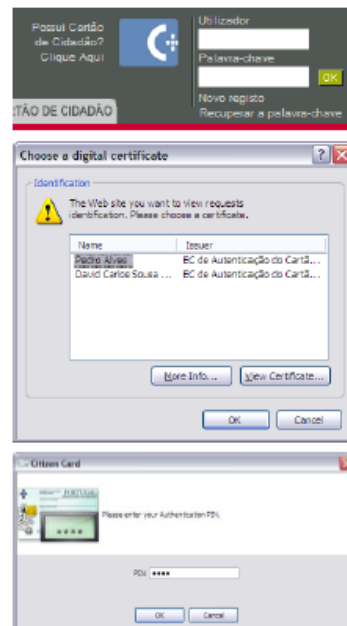
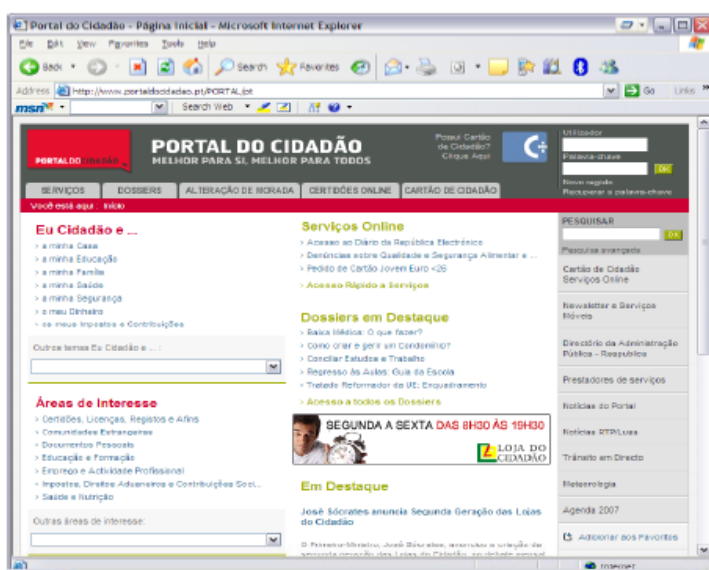


www.portaldocidadao.pt

Business Web Portal



www.empresanahora.pt



www.portaldocidadao.pt

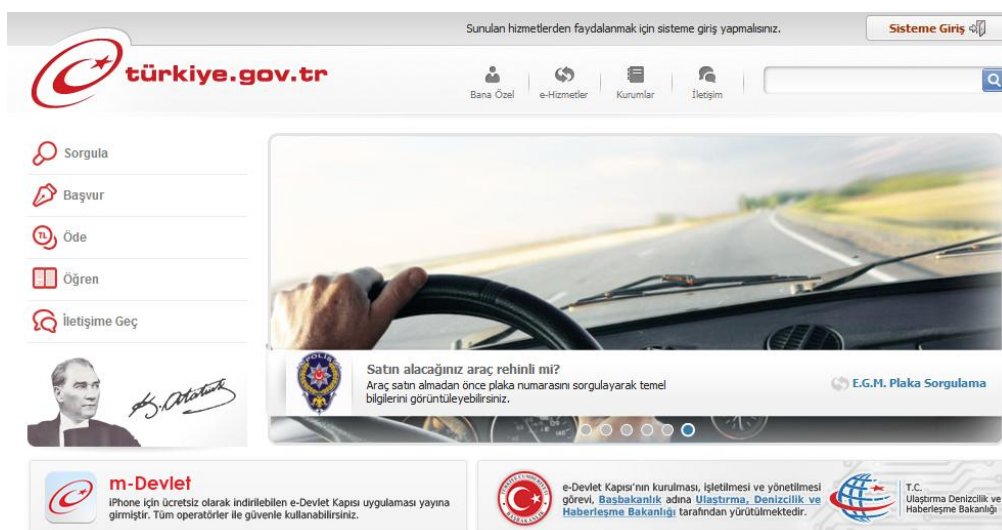


www.riac.azores.gov.pt

Σε άλλες χώρες

Τουρκία

Στην Τουρκία έχει δημιουργηθεί διαδικτυακή πύλη πολιτών με 10.200.000 χρήστες [32] όπου παρέχονται υπηρεσίες ηλεκτρονικής διακυβέρνησης με πάνω από 260 παρεχόμενες υπηρεσίες και πάνω από 38 δημόσιες υπηρεσίες μέλη.



 Türkiye Cumhuriyeti Vatandaş Kimlik Doğrulama Sistemi

Giriş Yapacağınız Adres www.turkiye.gov.tr
Giriş Yapacağınız Uygulama [e-Devlet Kapısı](#) 

Şifre İle Giriş

* T.C. Kimlik No  Sanal Klavye  Numaramı Gizle

* e-Devlet Şifresi  Sanal Klavye

 Güvenliğiniz için tarayıcınızın adres satırında <https://giris.turkiye.gov.tr> yazdığından ve tarayıcınızın güvenlik (kilit) simgesinin görüldüğünden emin olunuz. Eğer görünmüyorsa işleminize devam etmeyiniz.

  > Gizlilik ve Güvenlik
Her hakkı saklıdır © 2012

Καρτέλα σύνδεσης στις υπηρεσίες (login) [32]

Κτηματολόγιο [32]

Taşınmaz Detay Bilgileri

Bu hizmet TAKBİS'te T.C. Kimlik Numarası kayıtlı olan ve TAİ kapsamında sunulmaktadır. TAKBİS'e geçen tapu sicil müdürlükleri için geçerlidir.

İl	KAYSERİ	Ac
İlçe	KOCASINAN	Pa
Mahalle/Köy	ERKİLET	Cl
Nitelik	ADSA	Ca
Yüzölçümü (m2)	317	

 Yukarıdaki haritaya tıklayarak taşınmazınızı harita üzerinde

Taşınmaz Detay Bilgileri

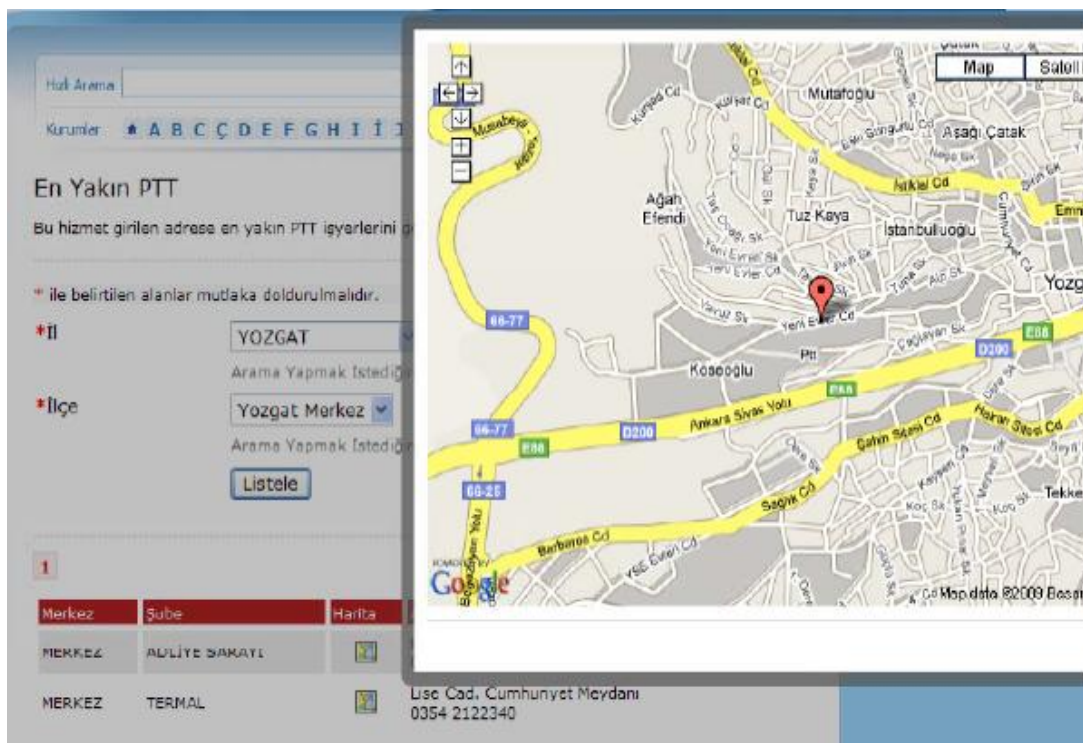
[← Taşınmaz Listesine Dön](#)

 Map Satellite

Imagery ©2011 DigitalGlobe, GeoEye - Terms of Map

TAMAM X

Ακίνητα [32]



Προσωπικά στοιχεία [32]



Benim Sayfam

Başbakanlık İletişim Merkezi Başvurularım

Bu hizmet ile Benim'e internet üzerinden yaptığınız başvurularınızı cevaplandırabilirsiniz. Başvuru tarihi ve sayısını seçiniz.

Tarih: 10.12.2000 :: Sayı: 224477

Günlük Hava Durumu

ANKARA
Yağmurlu
En Düşük Sıcaklık: 4°C
En Yüksek Sıcaklık: 8°C

İSTANBUL
Sağanak Yağışlı
En Düşük Sıcaklık: 5°C
En Yüksek Sıcaklık: 10°C

SGK Bilgilerim

Son Yatırılan Prim Tarihi Dönem/Ay	Kasım 2009
İlk Çalışmaya Başlama Tarihi	01/02/2001
Son Yatırılan Prim Tutarı	4504,5
Toplam Prim Ödeme Lun Sayısı	1583
Toplam Prim Ödeme Prim Tutarı	177443,8

Detaylı bilgilerinizi görmek için tıklayınız

Trafik Ceza Puanım

Toplam ceza puanınız	30
----------------------	----

Detaylı bilgi almak için tıklayınız

Kamu Personeli e-Bordro

 Teknik bir sorun olmuştur. Tekrar deneyiniz.

Görüntülenme:

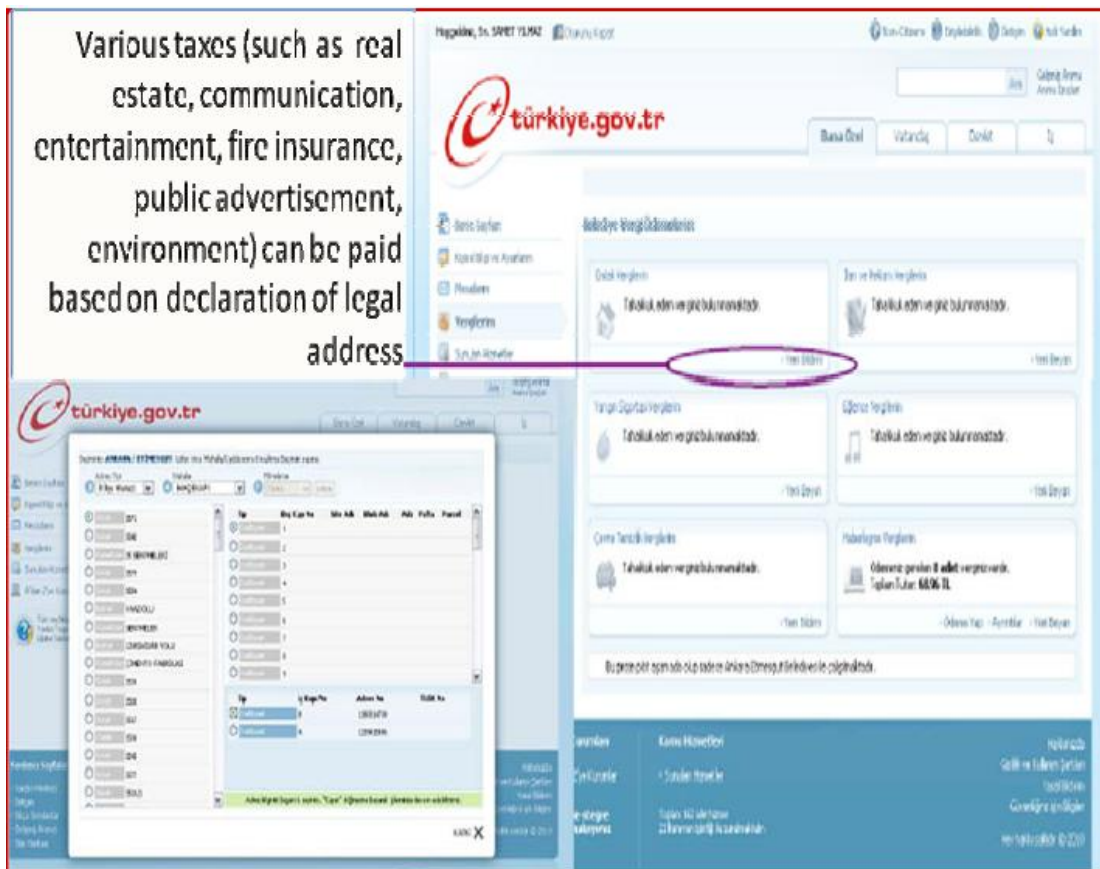
TCMB Döviz Kurları

USD	1.4522 / 1.4593
EUR	2.0904 / 2.1005

Son Güncelleme: 15.01.2010

Detaylı döviz kurları için tıklayınız

Πληρωμές φόρων [32]



Η νέα ταυτότητα στην Τουρκία θα είναι όπως εμφανίζεται στην παρακάτω εικόνα:



Kiva

Η Λαϊκή Δημοκρατία της Κίνας απαιτεί ο κάθε πολίτης άνω των 16 ετών να διαθέτει δελτίο ταυτότητας. Η κάρτα είναι το μόνο αποδεκτό νομικό έγγραφο για να αποκτήσουν οι πολίτες άδεια παραμονής, απασχόλησης, να ανοίξουν τραπεζικούς

λογαριασμούς, να λάβουν διαβατήριο, δίπλωμα οδήγησης, αίτηση για την τριτοβάθμια εκπαίδευση και τεχνικές σχολές, καθώς και για σημεία ελέγχου της ασφάλειας στις εγχώριες τερματικές ζώνες κυκλοφορίας και σταθμούς όπως των κινεζικών αερολιμένων.



Μαλαισία

Στη Μαλαισία, η MyKad, ή κυβερνητική κάρτα πολλαπλών χρήσεων, (GMPC) είναι η επίσημη υποχρεωτική έκδοση δελτίου ταυτότητας. Θεωρείται ως η πρώτη έξυπνη κάρτα ταυτότητας του κόσμου. Επίσημα ξεκίνησε στις 5 Σεπτεμβρίου 2001 και ενσωματώνει ένα μικροτσίπ, το οποίο περιέχει μερικά στοιχεία των δεδομένων του πολίτη συμπεριλαμβανομένων των βιομετρικών δεδομένων. Από το 2006, η MyKad έχει οκτώ τρέχουσες και σχεδιασμένες αρκετές άλλες εφαρμογές οι οποίες σχετίζονται κυρίως με την απόδειξη της ταυτότητας ή του ηλεκτρονικού χρήματος. Από το Μάρτιο του 2003, μια παραλλαγή της έκδοσης για νεογέννητα μωρά εισήχθη, που είναι γνωστή ως MyKid.

Η Μαλαισία είχε σύστημα Ταυτότητας σε ισχύ από τη δεκαετία του '50. Πριν από την έναρξη της MyKad, της Μαλαισίας η ταυτότητα ονομαζόταν Kad Penggalan Μαλαισία. Οι πολίτες άνω των 12 ετών υποχρεούνται να κάνουν αίτηση για την έκδοση δελτίου ταυτότητας, και οφείλουν να ανανεώνουν την κάρτα στην ηλικία των 18 ετών.



Μπαχρεΐν

Το Μπαχρεΐν έχει αναπτύξει μία σειρά από ηλεκτρονικές υπηρεσίες, στις οποίες έχει πρόσβαση ο πολίτης από το 2004, όπου ανακοινώθηκε επίσημα την έναρξη της ηλεκτρονικής διακυβέρνησης.

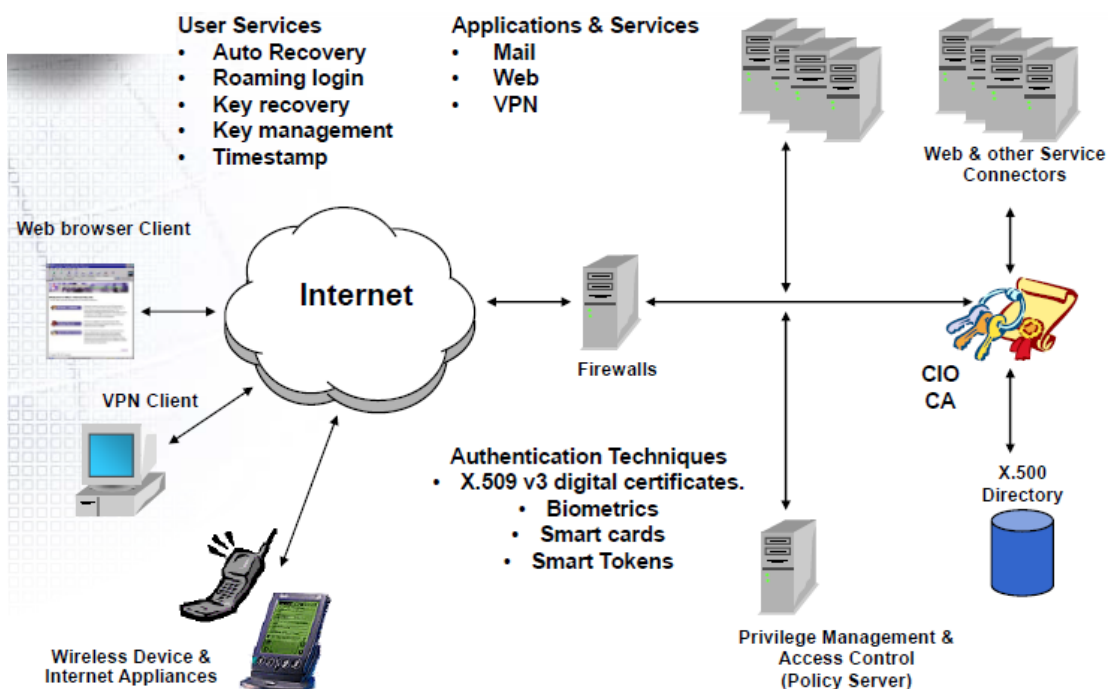
Ως μέρος ενός μεγαλύτερου έργου, το Μπαχρεΐν αποφάσισε την υιοθέτηση της eID κάρτας. Το έργο ήταν να εκδοθεί ένα πολυχρηστικό εργαλείο το οποίο θα αντικαθιστούσε την παλιά ταυτότητα [37]. Ο οργανισμός κεντρικών πληροφοριών, χρεώθηκε να ολοκληρώσει το έργο.



Η κάρτα ισχύει για πέντε χρόνια και πρέπει να ανανεώνεται. Στην κάρτα περιλαμβάνονται ο αριθμός ταυτότητας, ενσωματωμένα δακτυλικά αποτυπώματα, φωτογραφία και υπογραφή κατόχου, άδεια οδήγησης, εντοπιότητα, δεδομένα υγείας.



Στο Μπαχρεϊν ήδη χρησιμοποιούν την κάρτα και για υπηρεσίες μέσω διαδικτύου και PKI εφαρμογές.



Ινδία

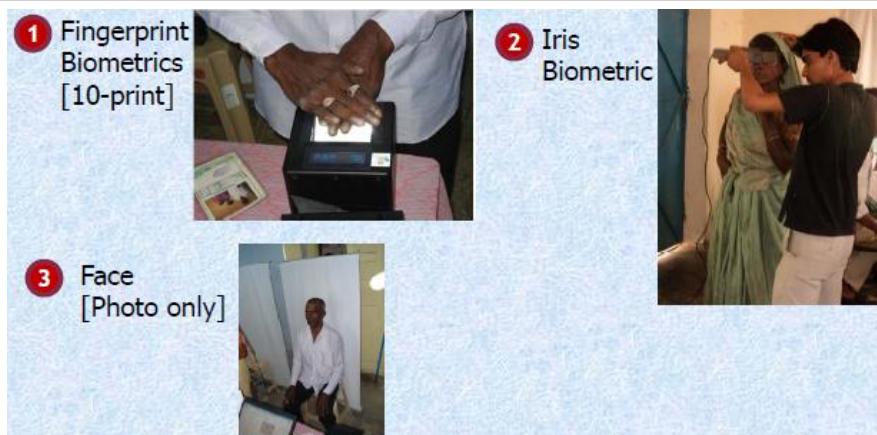
Στην Ινδία θα έχουν τακτοποιήσει [38], 1,2δισ πολίτες, οι οποίοι θα χρησιμοποιούν eID βιομετρικές κάρτες έως το 2016. Αυτό είναι το μεγαλύτερο πρόγραμμα τέτοιου τύπου στον κόσμο. Το πρόγραμμα αυτό θα κοστίσει περίπου 33δισ\$. Με αυτόν τον τρόπο ελπίζουν σε δικαιότερες πολιτικές εκλογές, καταπολέμηση τρομοκρατίας, διακοπή παράνομης λαθρομετανάστευσης κλπ

Στην Ινδία 320 εκ άνθρωποι δεν έχουν ταυτότητα και δεν μπορούν να αποδείξουν ποιοι είναι [38]. Το AADHAAR είναι ένα πρόγραμμα της Ινδικής κυβέρνησης για να ολοκληρωθεί το έργο με την ηλεκτρονική ταυτότητα. Στην παρακάτω εικόνα φαίνονται οι προεκτάσεις του προγράμματος AADHAAR.

Program / Entity	Better Reach & Targeting	Reduced Leakages / fraud	Reduced Cost of Service Delivery	Widen Tax Base	Greater efficiencies & effectiveness
Employment - MNREGA, SGSY, IAY, KVIC, PMEGP	✓	✓	✓		✓
Education - SSA, Right to Education	✓	✓	✓		✓
Food & Nutrition - PDS, Food Security, Mid Day Meals, ICDS	✓	✓	✓		✓
Inclusion & Soc Sec - JSY, Dev ofPTGs, IGNOAPS	✓	✓	✓		✓
Healthcare - RSBY, Janshri BY, Aam Aadmi BY	✓	✓			✓
Financial Services incl Insurance	✓	✓		✓	✓
Property Transactions		✓		✓	✓
Voter ID	✓	✓			✓
PAN Card		✓		✓	✓

Οι υπηρεσίες που συλλέγονται είναι:

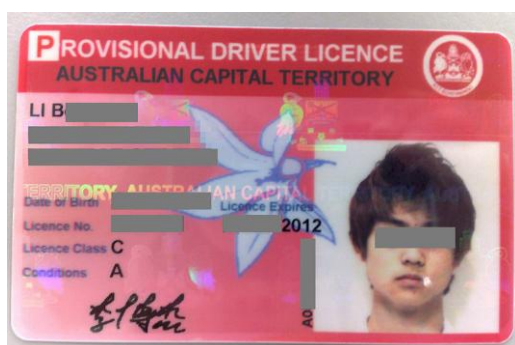
- Όνομα , διεύθυνση , φύλλο, ημερομηνία γέννησης,
- Φωτογραφία και πιστοποιητικό μόνιμης κατοικίας,
- Δακτυλικά αποτυπώματα,
- Ίριδα,



Αυστραλία

Η ταυτότητα συνήθως απαιτείται για την αγορά αλκοόλ και του καπνού, και για να εισέλθουν οι πολίτες πάνω των 18 στα νυχτερινά κέντρα. Σε γενικές γραμμές, η κύρια μορφή αναγνώρισης που χρησιμοποιούνται είναι η αυστραλιανή άδεια οδήγησης. Ωστόσο, ορισμένα κράτη, όπως η Victoria επιτρέπουν την επιλογή για τα άτομα να αγοράσουν μία προαιρετική "απόδειξη της ηλικίας" keycard.

Υπήρξαν δύο προτάσεις για την εισαγωγή δελτίων ταυτότητας για τους φόρους και την κοινωνική ασφάλεια, και μία για την πρόσβαση στην Αυστραλία: **Η Κάρτα Αυστραλία** το 1985 από την κυβέρνηση του Εργατικού Hawke και η **Υγεία και Κοινωνική Κάρτα** για τις Υπηρεσίες Πρόσβασης το 2006 από τον Χάουαρντ της φιλελεύθερης κυβέρνησης. Παρά το γεγονός ότι η κάρτα δε θα ήταν μια επίσημη υποχρεωτική ταυτότητα, και οι δύο επικρίθηκαν ότι οδηγούν σε de facto δελτία ταυτότητας. Τελικά, οι δύο προτάσεις απέτυχαν. Επί του παρόντος, οι άδειες οδήγησης, που εκδίδονται από τα κράτη και τις πολιτείες, είναι το πιο ευρέως χρησιμοποιούμενο έγγραφο ταυτότητας.



Τα συνέδρια [1],[2],[3]

Μέχρι σήμερα έχουν πραγματοποιηθεί τρία ακαδημαϊκά συνέδρια με θέμα το national eID & ePassport, ένα στη Λισαβόνα το 2009, στην Αθήνα το 2010 και στην Κωνσταντινούπολη το 2011. Στα συνέδρια αυτά έχουν λάβει μέρους ακαδημαϊκοί, σπουδαστές καθώς και επιστήμονες από εταιρίες. Έχουν τεθεί και αναλυθεί θέματα, σχεδιασμού, χρήσεων στο Δημόσιο και ιδιωτικό τομέα, τεχνολογιών υλοποίησης, θέματα ασφάλειας και ιδιωτικότητας.

Επιπλέον για το μέλλον της Ευρώπης και των Ευρωπαίων πολιτών, έχει ήδη τεθεί σε όλα τα κράτη, όπως έχουμε προαναφέρει, το θέμα κάρτας του Ευρωπαίου πολίτη, European Citizen Card, το μέλλον του eID στην Ευρώπη.

Για αυτήν την εργασία έχουν μελετηθεί όλα τα δοκίμια και οι μελέτες των τριών παραπάνω συνεδρίων και έχουν αντληθεί θέματα και απόψεις μερικές των οποίων υιοθετούνται σε αυτήν την εργασία και μελέτη. [1], [2], [3]

Το Ευρωπαϊκό Θεσμικό πλαίσιο

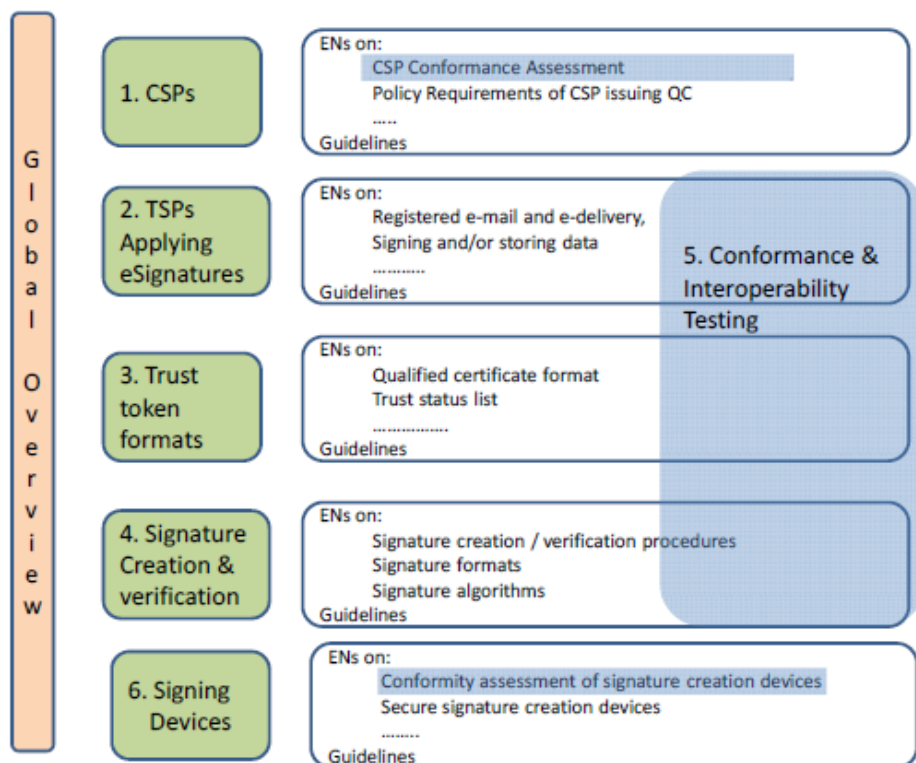
Με την οδηγία 1999/93/EC δημιουργήθηκε το νομικό πλαίσιο[33] το οποίο μεταξύ άλλων ορίζει και υιοθετεί:

- Χωρίς διακριτική μεταχείριση η ηλεκτρονική υπογραφή,
- Ισοδυναμία ηλεκτρονικής και χειρόγραφης υπογραφής,
- Βασικές έννοιες απλής, προηγμένης και ειδικής υπογραφής, πάροχοι πιστοποιητικών κλπ
- Βασικές αρχές: εποπτείας, ελεύθερης πρόσβασης στην αγορά, ...
- Δημιουργήθηκαν περίπου 30 CEN & ETSI πρότυπα.

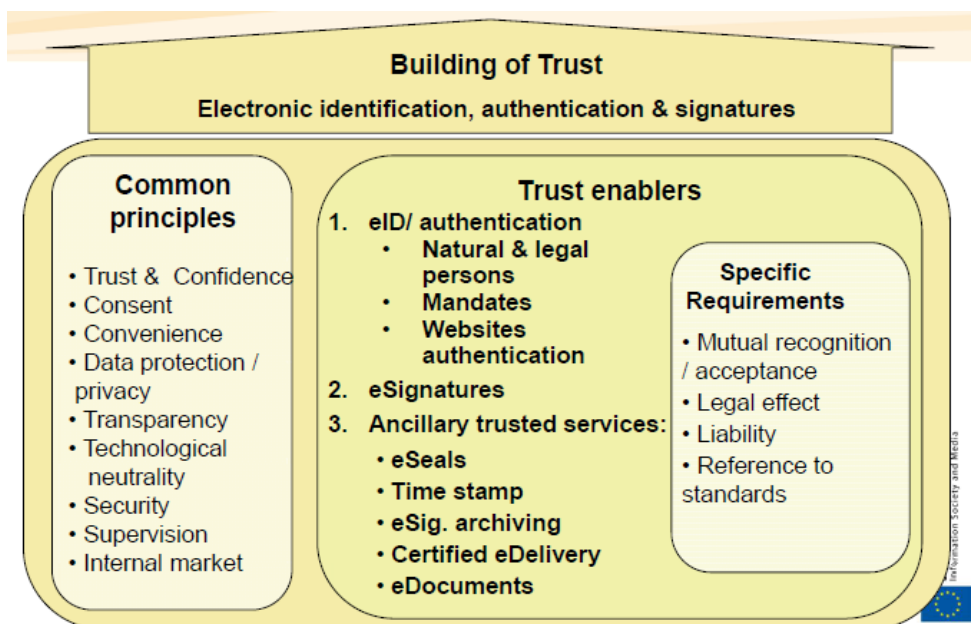
Τα αποτελέσματα από τη δράση βελτίωσης του πλαισίου ηλεκτρονικής υπογραφής στην Ευρώπη, αναφέρονται παρακάτω:

- Δημιουργήθηκε EU λίστα εμπιστοσύνης επιλεγμένων παρόχων πιστοποιητικών (2009-2010, [decision 2010/425/EU](#)),
- Υπάρχει η οδηγία υπηρεσιών ([Services Directive decision 2011/130/EU, 2011](#)) για το :
 - ο Χειρισμό των ETSI διαμορφώσεων υπογραφών ([CAAdES, XAdES, PAdES](#)),
 - ο Υποδομή επικύρωσης υπογραφών,

- Πρότυπα εξορθολογισμού ηλεκτρονικών υπογραφών (**mandate m460** to CEN and ETSI, [2011-2014](#)) [34]

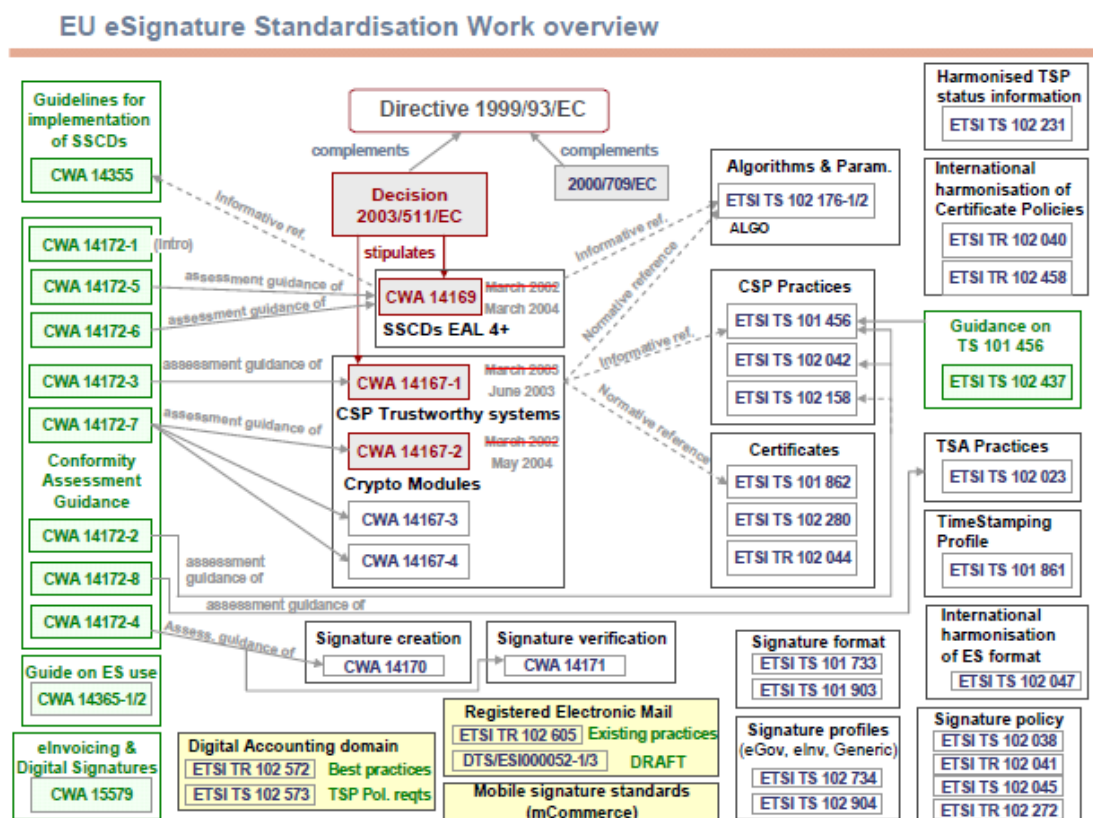


Ο στόχος των Ευρωπαϊκών οδηγιών είναι «να ενισχύσει την εμπιστοσύνη στις online συναλλαγές». Ανάμεσα σε διαχειριστές συστημάτων, ανάμεσα σε επιχειρήσεις και πολίτες, με εύκολη χρήση για όλους και χαμηλό κόστος, μέσα και έξω από τα σύνορα της Ευρωπαϊκής ένωσης απαιτείτε ασφαλή διαδραστικότητα.



Συνεπώς λοιπόν, όλοι μας στην Ευρώπη θέλουμε, με την ενίσχυση της εμπιστοσύνης

στο διαδίκτυο, να υπάρχει ένα πανευρωπαϊκό πλαίσιο, για ηλεκτρονική ταυτοποίηση, επικύρωση και υπογραφή. Να αναγνωρίζεται μεταξύ χωρών της Ευρωπαϊκής ένωσης, διαλειτουργικότητα και χρήση της ηλεκτρονικής υπογραφής, διασυννοιακές υπηρεσίες εμπιστοσύνης με χρονοσφραγίδες, υπογραφή αρχειοθέτησης, ηλεκτρονικές σφραγίδες καταχώρησης εγγράφων, ηλεκτρονικά έγγραφα[34]



Μέχρι εδώ λοιπόν έχουμε ορίσει τι θέλουμε να υλοποιήσουμε, έχουμε αναφέρει τα έργα των γειτονικών και όχι μόνο κρατών και έχουμε δει το Ευρωπαϊκό θεσμικό πλαίσιο μες στο οποίο μπορούμε να κινηθούμε, ώστε να υλοποιήσουμε την κάρτα του πολίτη. Στο επόμενο κεφάλαιο κάνουμε μία διείσδυση στην Ελληνική πραγματικότητα.

1ο Κεφάλαιο : Η Ελληνική πραγματικότητα (μητρώα πολιτών)

Εδώ επιχειρείται η συγκέντρωση όλων των στοιχείων των Ελληνικών μητρώων, ώστε να διερευνηθούν οι δυνατότητες συγχώνευσης όλων των μητρώων σε ένα. Γίνετε σύγκριση μεταξύ των μητρώων και των δικαιολογητικών που απαιτούνται για κάθε εισαγωγή εγγραφής. Τελικά συμπεραίνετε η δυνατότητα συγχώνευσης καθώς και η αλληλεξάρτηση μεταξύ τους.

1.1 Οι αριθμοί ταυτοποίησης και μητρώων που ισχύουν στην Ελλάδα σήμερα (ΑΜΚΑ, Αρ. Δημοτολογίου, ΑΦΜ, Αρ. Δελτίου ΤΑΥΤΟΤΗΤΑΣ, Διαβατήριο)

Σήμερα στην Ελλάδα, ο πρώτο αριθμός ταυτοποίησης που δίνεται σε Έλληνα πολίτη, είναι ο αριθμός δημοτολογίου. Ο αριθμός αυτός καθώς και η οικογενειακή κατάσταση, είναι στοιχεία που συνοδεύουν τον Έλληνα πολίτη, σε όλη τη διάρκεια της ζωής του.

Το δεύτερο στοιχείο που συνήθως ακολουθεί, με την ενηλικίωση του πολίτη, είναι ο αριθμός ταυτότητας. Ο πολίτης αποκτάει στα 16 του αστυνομική ταυτότητα που φέρει πάνω ένα μοναδικό αλφαριθμητικό.

Με την ταυτότητα και την εγγραφή στο δημοτολόγιο πλέον ο πολίτης μπορεί να εκδώσει ΑΦΜ (αριθμό φορολογικού μητρώου), ΑΜΚΑ (αριθμό μητρώου κοινωνικής ασφάλισης), Διαβατήριο.

Η δική μας προσέγγιση σε αυτό το κεφάλαιο είναι να μελετήσουμε πως γίνεται η έκδοση των παραπάνω αριθμών και πως θα μπορούσε αυτό να ολοκληρωθεί σε ένα αριθμό μητρώου της κάρτας του πολίτη, όπου εδώ θα υιοθετηθεί ο ΑΜΚΑ.

1.2 Δημοτολόγιο

Στο δημοτολόγιο γίνονται όλες οι αρχικές εγγραφές από γεννήσεως ενός πολίτη. Γίνεται δήλωση της γέννησης, οπότε και επισημοποιείτε η ύπαρξη ληξιαρχικής πράξης γέννησης. Εδώ ο πολίτης (δημότης) έχει πλέον μερίδα και εγγράφεται μέσα στην οικογενειακή μερίδα.

1.3 Δήλωση γέννησης

Αν πρόκειται για το 1ο παιδί χρειάζεται:

1. **Ιατρικό Πιστοποιητικό γέννησης** (κλινικής ή νοσοκομείου)
2. Αστυνομικές ταυτότητες των γονέων
3. Πράξη προσδιορισμού επωνύμου τέκνων, που ήδη υπάρχει από την τέλεση του γάμου των γονέων
4. Πιστοποιητικό οικογενειακής κατάστασης ή Ληξιαρχική Πράξη Γάμου

Αν πρόκειται για το 2ο παιδί και επόμενα:

1. Ιατρικό Πιστοποιητικό γέννησης (κλινικής ή νοσοκομείου)
2. Αστυνομικές ταυτότητες των γονέων

3. Πιστοποιητικό οικογενειακής κατάστασης

Οι αλλοδαποί, χρειάζεται να προσκομίσουν διαβατήρια, μεταφρασμένα πιστοποιητικά ή μεταφρασμένο πιστοποιητικό γάμου.

Προθεσμία Δήλωσης: Εντός 10 ημερών από τον τοκετό

Υπόχρεοι για τη δήλωση: Ο **πατέρας**, ο **γιατρός**, η **μαία**, η **μητέρα** και κάθε **τρίτος** που αποδεδειγμένα παραστάθηκε στον τοκετό

Στο σημείο λοιπόν αυτό καταλαβαίνουμε ότι, για να δηλώσουμε την ύπαρξη ενός ανθρώπου, ουσιαστικά για να καταχωρήσουμε στο σύστημα έναν πολίτη, χρειαζόμαστε ένα γονέα, τη μαία, το γιατρό και τον τοκετό (ιατρικό πιστοποιητικό). Συνεπώς οι παραπάνω μαρτυρίες αποτελούν ικανή και αναγκαία συνθήκη για την ύπαρξη. Εδώ λοιπόν, με την καταχώρηση του γεγονότος και των στοιχείων θα μπορούσε να δημιουργηθεί το δημόσιο κλειδί, ο ΑΜΚΑ, όπου θα είχε την ημερομηνία γέννησης και τον αύξων αριθμό πολίτη, δηλαδή π.χ. 0511201110000004, όπου αυτός ο αριθμός δηλώνει ότι ο πολίτης υπ'αριθμού 10.000.004 γεννήθηκε την 05/11/2011 και είναι ο πολίτης με αριθμό 0511201110000004.

1.4 Δελτίο αστυνομικής ταυτότητας

Το Δελτίο Αστυνομικής Ταυτότητας (συχνά αποκαλούμενο και Δελτίο Ταυτότητας, Αστυνομική Ταυτότητα ή απλά Ταυτότητα) είναι επίσημο έγγραφο του Ελληνικού Κράτους.

Πρόκειται για έγγραφο υποχρεωτικό για όλους του πολίτες του Κράτους άνω των 12 ετών, που εκδίδεται από την Ελληνική Αστυνομία. Οι πολίτες είναι υποχρεωμένοι να το φέρουν πάντοτε μαζί τους και να το επιδεικνύουν όταν ζητείται από τις Αστυνομικές Αρχές, διαφορετικά είναι πιθανή η μεταφορά τους στο πλησιέστερο Αστυνομικό Τμήμα για εξακρίβωση στοιχείων. Το Ελληνικό διαβατήριο θεωρείται έγγραφο ταυτοποίησης ισοδύναμο με την αστυνομική ταυτότητα.

Καθώς η Ελλάδα είναι χώρα-μέλος της Συμφωνίας Σένγκεν, το δελτίο αστυνομικής ταυτότητας αποτελεί έγκυρο ταξιδιωτικό έγγραφο μεταξύ των χωρών της Συμφωνίας. Το ονοματεπώνυμο αναγράφεται και με λατινικούς χαρακτήρες από το 2000, ενώ τα παλιά δελτία ταυτότητας είναι ισοδύναμα με τα νέα και οι χώρες-μέλη του Συμφώνου Σένγκεν είναι υποχρεωμένες να τα αναγνωρίζουν ως έγκυρα ταξιδιωτικά έγγραφα. Εξάλλου, το δελτίο αστυνομικής ταυτότητας χρησιμοποιείται για την ταυτοποίηση

προσώπου των πολιτών στις εκλογικές διαδικασίες (τοπικές/περιφερειακές, εθνικές/βουλευτικές και Ευρωπαϊκού Κοινοβουλίου).

1.5 Δικαιολογητικά έκδοσης Δελτίου Ταυτότητας

Για την **έκδοση Δελτίου Ταυτότητας** υποβάλλονται αυτοπροσώπως από τον ενδιαφερόμενο, στην αρμόδια αστυνομική αρχή, τα ακόλουθα δικαιολογητικά:

1. Τέσσερις πρόσφατες ασπρόμαυρες φωτογραφίες (για ταυτότητα), διαστάσεων 0,036*0,036 cm.

2. Αίτηση που θα προμηθευθείτε από το Αστυνομικό Τμήμα

3. Βεβαίωση Νοσηλευτικού Ιδρύματος ή Υγειονομικού Εργαστηρίου για την ομάδα Αίματος και το RHESUS (εφόσον επιθυμείτε την αναγραφή του στο δελτίο σας.)

4. Ταξιδιωτικό ή άλλο έγγραφο ημεδαπής ή αλλοδαπής Αρχής, από το οποίο να προκύπτει προηγούμενη εγγραφή των στοιχείων «ΕΠΩΝΥΜΟ, ΟΝΟΜΑ και ΟΝΟΜΑ ΠΑΤΕΡΑ» των ενδιαφερόμενων, με λατινικούς χαρακτήρες (εφόσον επιθυμείτε αναγραφή των ανωτέρω στοιχείων διαφορετική του προτύπου ΕΛΟΤ 743, υποβάλλοντας παράλληλα και σχετική υπεύθυνη δήλωση)

5. Για την πρώτη έκδοση του δελτίου ταυτότητας, απαιτείται επίσης η βεβαίωση των στοιχείων του αιτούντος από έναν μάρτυρα. Σε περίπτωση που είστε ανήλικος/η, την βεβαίωση των στοιχείων μπορεί να κάνει ο γονέας ή εκείνος που έχει την επιμέλεια ή επιτροπεία του.

**** Η Αρχή έκδοσης του δελτίου ταυτότητας υποχρεωτικά αναζητά αυτεπάγγελτα το πιστοποιητικό γέννησης του Δήμου ή της Κοινότητας του αιτούντος, και η αποστολή του γίνεται από την Αρχή που το εκδίδει, με τηλεομοιοτυπία ή ηλεκτρονική αλληλογραφία. Το πιστοποιητικό αυτό θα πρέπει να έχει εκδοθεί το αργότερο τρεις μήνες πριν την υποβολή του.**

1.6 Ποιές πληροφορίες περιλαμβάνει η ταυτότητα

Στην μπροστινή όψη περιλαμβάνει την υπογραφή του κατόχου, τυποποιημένη ασπρόμαυρη φωτογραφία, ομάδα και ρέζους αίματος (προαιρετικά) και τα στοιχεία

του δελτίου ταυτότητας (αριθμός, τόπος και ημερομηνία έκδοσης, αρχή έκδοσης). Στην πίσω όψη περιλαμβάνονται το επώνυμο, όνομα και όνομα πατέρα του κατόχου με ελληνικούς και λατινικούς χαρακτήρες, καθώς και το ονοματεπώνυμο της μητέρας, η ημερομηνία και ο τόπος γέννησης, το ύψος, ο Δήμος στον οποίο είναι εγγεγραμμένος ο κάτοχος και ο αριθμός δημοτολογίου, καθώς και η αρχή έκδοσης του δελτίου ταυτότητας.



ΣΤΟΙΧΕΙΑ ΤΑΥΤΟΤΗΤΑΣ

ΕΠΩΝΥΜΟ
SURNAME

ΟΝΟΜΑ
GIVEN NAMES

ΟΝΟΜΑ ΠΑΤΕΡΑ
FATHER'S NAME

ΕΠΩΝΥΜΟ ΠΑΤΕΡΑ
ONOMATOPATROS

ΟΝΟΜΑ ΜΗΤΕΡΑΣ
ONOMATIMATROS

ΗΜΕΡΟΜΗΝΙΑ ΓΕΝΝΗΣΗΣ (DATE OF BIRTH)
ΤΟΠΟΣ ΓΕΝΝΗΣΗΣ

ΥΨΟΣ (HEIGHT)
ΔΗΜΟΣ Α.Δ.

ΑΡΧΗ ΕΚΔΟΣΗΣ ΔΕΛΤΙΟΥ ΤΑΥΤΟΤΗΤΑΣ
Ο ΣΥΝΤΑΞΑΣ ΤΟ Α.Τ.

(ΥΠΟΓΡΑΦΗ - ΣΦΡΑΓΙΔΑ)

1.7 Αριθμός μητρώου κοινωνικής ασφάλισης (ΑΜΚΑ)

Εδώ δίνουμε τον ορισμό και τις χρήσεις του ΑΜΚΑ όπως δηλώνονται και ορίζονται από της Ελληνική Δημοκρατία και το θεσμικό πλαίσιο.

Ο ΑΜΚΑ (Αριθμός Μητρώου Κοινωνικής Ασφάλισης) είναι ουσιαστικά η ταυτότητα **εργασίας** και **ασφάλισης** κάθε εργαζόμενου, συνταξιούχου και προστατευόμενου μέλους της οικογένειάς τους στη χώρα μας. Με τον ΑΜΚΑ μπορείτε να προχωρήσετε σε **έναρξη απασχόλησης** και **ασφάλισης**, να καταβάλετε τις **ασφαλιστικές** σας **εισφορές**, να εκδώσετε ή να ανανεώσετε το **βιβλιάριο ασθένειας**, να πάρετε τη **σύνταξη** σας ή τις οποιεσδήποτε **παροχές, επιδόματα** και **βοηθήματα** και όλα αυτά με πολύ λιγότερες καθυστερήσεις και γραφειοκρατικές διαδικασίες.

Απαραίτητα δικαιολογητικά έκδοσης ανά κατηγορία είναι τα εξής:

1. Για Έλληνες Υπηκόους

- Το **Δελτίο Αστυνομικής Ταυτότητας** ή Δελτίο Ελληνικής Στρατιωτικής Ταυτότητας.
- Για ανήλικα άτομα που δεν έχουν συμπληρώσει το 12ο έτος της ηλικίας τους και δεν έχουν αστυνομική ταυτότητα, απαιτείται η προσκόμιση **πιστοποιητικού οικογενειακής κατάστασης** από το γονέα ή το νόμιμο εκπρόσωπό του.

2. Για Ξένους Υπηκόους:

- Το **Δελτίο Ταυτότητας ομογενούς** ή **δελτίο ταυτότητας** (αντίστοιχο της ελληνικής αστυνομικής) ή **διαβατήριο**
- **πιστοποιητικό οικογενειακής κατάστασης**, επίσημα μεταφρασμένο στα ελληνικά, όταν δεν υπάρχει δελτίο ταυτότητας ή διαβατήριο ή τα έγγραφα αυτά δεν περιέχουν τα ζητούμενα για την απογραφή στοιχεία
- Για ανήλικα άτομα που γεννήθηκαν στην Ελλάδα απαιτείται η **ληξιαρχική πράξη γέννησης**.

Διαδικασία μεταβολής ή επικαιροποίησης στοιχείων: Είναι δυνατή η **μεταβολή** και η **επικαιροποίηση** των στοιχείων όσων έχουν ήδη ΑΜΚΑ (όπως **όνομα, τηλέφωνο, δ/νση, ασφαλιστικός φορέας** κ.λπ.), μέσω των **ΚΕΠ** ή των γραφείων ΑΜΚΑ, με **πρωτοβουλία** του **ενδιαφερομένου**.

1.8 Απόδοση Αριθμού Φορολογικού Μητρώου Α.Φ.Μ.

Ο **ΑΦΜ** είναι ένας **μοναδικός αριθμός** που αποδίδεται σε κάθε **συναλλασσόμενο** και τον **«ταυτοποιεί»** μοναδικά με βάση τα **ατομικά** του στοιχεία. Υποχρέωση να αποκτήσουν ΑΦΜ έχουν τα ημεδαπά ή αλλοδαπά φυσικά πρόσωπα που :

- Είναι ή πρόκειται να γίνουν επιτηδευματίες.
- Μισθωτοί πριν τη πρόσληψή τους.
- Είναι υπόχρεοι σε υποβολή δήλωσης Φορολογίας Εισοδήματος.
- Αποκτούν περιουσιακά στοιχεία που προσδιορίζουν τεκμήριο (όπως Ε.Ι.Χ., μοτοσυκλέτα >50cc, σκάφος αναψυχής, αεροπλάνο, ελικόπτερο κλπ, καθώς και απόκτηση άδειας οδήγησης αυτών).
- Ζητούν Αποδεικτικό Φορολογικής Ενημερότητας, Πιστοποιητικά ή Βεβαιώσεις από την ΔΟΥ.
- Πρέπει να υποβάλλουν δηλώσεις Κεφαλαίου (λόγω απόκτησης περιουσιακών στοιχείων κλπ).
- Είναι μέλη, εταίροι ή σχετιζόμενοι με επιχειρήσεις (Ο.Ε, Ε.Ε., ΕΠΕ, Α.Ε. κλπ).
- Είναι εκπρόσωποι φορολογουμένων και διενεργούν πράξεις φορολογικού ενδιαφέροντος αντ' αυτών (κηδεμόνας σχολάζουσας κληρονομιάς, εκκαθαριστής, φορολογικός αντιπρόσωπος, αντίκλητος κλπ).

Δικαίωμα να αποκτήσουν **ΑΦΜ** έχουν όλα τα φυσικά πρόσωπα, **ημεδαπά** ή **αλλοδαπά**, που **κατοικούν** στην **Ελλάδα**.

Αρμόδια ΔΟΥ για την Απόδοση Αριθμού Φορολογικού Μητρώου σε μη Επιτηδευματία είναι η ΔΟΥ στη χωρική αρμοδιότητα της οποίας βρίσκεται η κατοικία του. Προκειμένου όμως να διευκολυνθεί η συναλλαγή του, μπορεί να αποδοθεί **ΑΦΜ** στον **ενδιαφερόμενο** από άλλη ΔΟΥ και ταυτόχρονα να διευθετηθεί υπηρεσιακά η **«ηλεκτρονική»** (on-line) μεταγραφή του στην αρμόδια ΔΟΥ.

1.9 Τι δικαιολογητικά χρειάζονται και από πού εκδίδονται;

Απαραίτητο δικαιολογητικό για την **απόδοση ΑΦΜ** είναι η επίδειξη του **αστυνομικού δελτίου ταυτότητας** (είτε κατά περίπτωση της ταυτότητας Σωμάτων Ασφαλείας για φορολογουμένους που υπηρετούν σ'αυτά) προκειμένου για **Έλληνες πολίτες** ή του **διαβατηρίου** για τους **αλλοδαπούς**. Για την περίπτωση που ο ενδιαφερόμενος στερείται ταυτότητας (π.χ. ανήλικος), τότε προσκομίζεται **πιστοποιητικό γέννησης**.

1.10 Διαβατήριο

Το **διαβατήριο** είναι ταξιδιωτικό έγγραφο, που εκδίδεται από κρατική αρχή και χρησιμεύει για τη μετάβαση του κατόχου του σε χώρες του εξωτερικού και ως αποδεικτικό στοιχείο ταυτότητας και ιθαγένειας του κατόχου.

Υπάρχουν πολλοί διαφορετικοί τύποι διαβατηρίων, ανάμεσά τους το απλό διαβατήριο, το υπηρεσιακό διαβατήριο και το διπλωματικό διαβατήριο.

Πολλές χώρες εκδίδουν πλέον βιομετρικά διαβατήρια, που περιέχουν μικροτσιπ με ψηφιακή φωτογραφία του κατόχου ή/και δακτυλικά αποτυπώματα. Στην Ελλάδα, βιομετρικά διαβατήρια εκδίδονται ήδη από το 2006 με ψηφιακή φωτογραφία, από τα τέλη του Ιουνίου 2009 δε, περιέχουν και δακτυλικό αποτύπωμα του κατόχου.

Σήμερα, για να ταξιδέψει ένας πολίτης της [Ευρωπαϊκής Ένωσης](#) σε άλλη χώρα της Ε.Ε. αρκεί η αστυνομική ταυτότητα και δεν απαιτείται η έκδοση και κατοχή διαβατηρίου.

1.11 Συμπεράσματα

Φαίνεται λοιπόν ότι στην Ελλάδα τηρούνται ουσιαστικά τέσσερα βασικά μητρώα πολιτών. Αυτά είναι το μητρώο του Δήμου, το μητρώο της αστυνομίας ταυτοποίησης στοιχείων, το μητρώο ασφάλισης και το φορολογικό μητρώο. Μεγαλύτερο ενδιαφέρον και νεότερο μητρώο είναι αυτό της κοινωνικής ασφάλισης το οποίο περιέχει στον μοναδικό αριθμό – κλειδί την ημερομηνία γέννησης. Όπως είδαμε και παραπάνω στις Ηνωμένες Πολιτείες της Αμερικής, η κάρτα που ντε φάκτο έχει παραμείνει ως ταυτότητα είναι αυτή την κοινωνικής ασφάλισης. Προτείνουμε λοιπόν την χρήση αυτού του αριθμού, χωρίς καμία αλλαγή στο μητρώο κοινωνικής ασφάλισης. Αυτό σημαίνει ότι τα μητρώα που θα πρέπει να τροποποιηθούν είναι τα υπόλοιπα τρία ήτοι : Δήμου – Αστυνομίας – Εφορίας.

Η συγχώνευση των μητρώων μπορεί να γίνει, ξεκινώντας από την αστυνομία, με αμοιβαία ανταλλαγή της παλιά ταυτότητας με νέα, η οποία θα φέρει πλέον τον ΑΜΚΑ και θα αποτελεί την νέα e-ID ή eCC. Εκεί, εκ του μηδενός θα δημιουργηθεί αύξων αριθμός πολίτη, όπου μια γεννήτρια αριθμών παράγει σε σειρά τους αριθμούς ταυτοτήτων.

Μετά την απόκτηση των eCC από τους πολίτες, μέσα σε μικρό χρονικό διάστημα, τόσο μητρώα επιχειρήσεων όσο και δημόσια μητρώα, στα πεδία που

καταχωρούσαν τον αριθμό αστυνομικής ταυτότητας πλέον θα μεταβάλλουν αυτό στον ΑΜΚΑ ή καλύτερα στο νέο αριθμό πολίτη ο οποίος θα ταυτίζεται με τον ΑΜΚΑ. Ας δούμε όμως περισσότερες λεπτομέρειες στο επόμενο κεφάλαιο.

2ο Κεφάλαιο : Η δική μας πρόταση ίδρυσης e-μητρώου πολιτών

Σε αυτό το κεφάλαιο παρουσιάζεται η δική μας πρόταση ίδρυσης του e-μητρώου πολιτών. Ο τρόπος ολοκλήρωσης αλλά και μετάβασης στην νέα κατάσταση, σε εθνικό επίπεδο, αναλύεται εδώ. Επιπλέον ορίζονται χρωματικές διαφορές σε σχέση με την ιδιότητα του πολίτη, όπως Έλληνας υπήκοος, Αλλοδαπός εργαζόμενος, Τουρίστας, Ενήλικας – Ανήλικος κλπ.

Η δική μας πρόταση ίδρυσης e-μητρώου πολιτών – συγχώνευση όλων των υπολοίπων, e-ID = eCC. Αναφορά σε δημόσια και ιδιωτικά μητρώα πολιτών – πελατών (προσωπικά δεδομένα – bar κλπ). Η μπλε – η πορτοκαλί – η πράσινη και η λευκή κάρτα.

2.1 Τι είναι ο e-αριθμός ταυτοποίησης (e-ID).

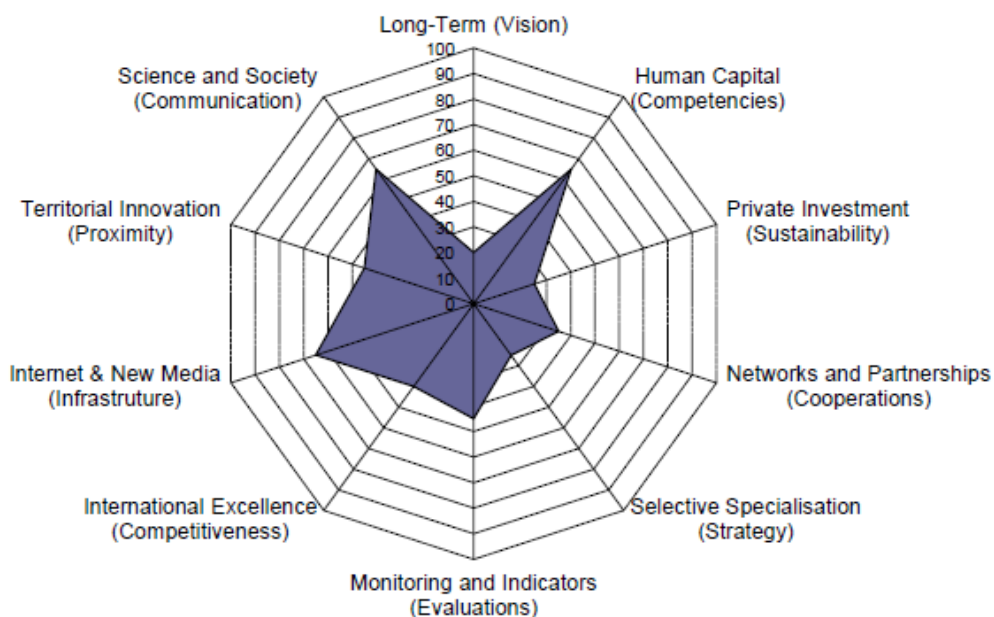
Η e-ταυτοποίηση είναι ο τρόπος που οι πολίτες, οι επιχειρήσεις, οι οργανισμοί και οι δημόσιες υπηρεσίες, ταυτοποιούνται μεταξύ τους, μέσω ψηφιακών υποδομών και άλλων ηλεκτρονικών δικτύων επικοινωνίας . [5]

2.2 Η μεγάλη πρόκληση.

Στη σημερινή δεινή θέση που βρίσκεται η Ελλάδα μας, το μόνο ισχυρό και δυστυχώς αναξιοποίητο στοιχείο που μπορεί να φέρει συνθήκες διεθνούς αριστείας, είναι οι νέοι ικανότατοι επιστήμονες των Ελληνικών Πανεπιστημιακών μας Ιδρυμάτων.

Αυτοί οι επιστήμονες μπορούν να δείξουν την Ελλάδα που διαπρέπει, φτάνει να τους δοθούν τα κατάλληλα μέσα και εργαλεία για να αναπτύξουν τις ικανότητές τους.

Παρακάτω εμφανίζονται οι 10 τάσεις – προκλήσεις για τη διακυβέρνηση και την πολιτική για τη διεθνή ασφάλεια. [7]



- Όραμα (Μακροπρόθεσμα)
- Ικανότητες (Ανθρώπινο κεφάλαιο)
- Αειφορία – βιωσιμότητα (Ιδιωτικές επενδύσεις),
- Συνεργασίες (Δίκτυα και συνεργάτες),
- Στρατηγική (Επιλεκτική εξειδίκευση),
- Αξιολογήσεις (Παρακολούθηση και δείκτες),

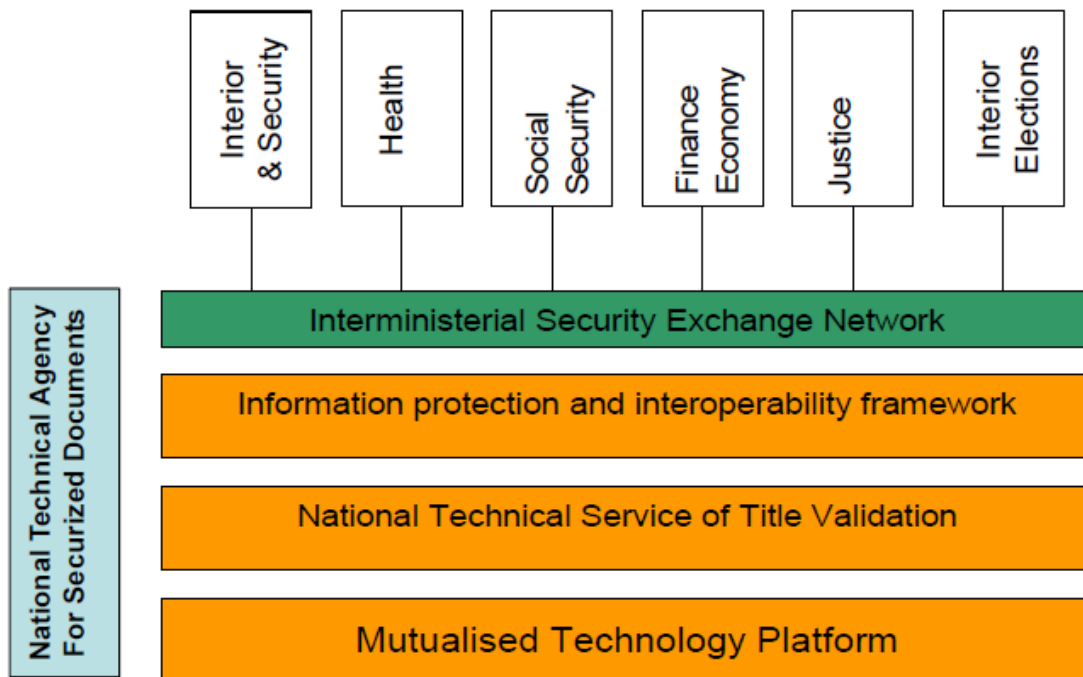
- Ανταγωνιστικότητα (Διεθνής αριστεία),
- Υποδομή (Διαδίκτυα και νέα μέσα),
- Εγγύτητα (Καινοτομία περιοχής),
- Επικοινωνία (Επιστήμη και κοινωνία).

2.3 Χτίζοντας ένα πρόγραμμα ηλεκτρονικής διακυβέρνησης

Τα βασικά θέματα [22] ενός πολιτοκεντρικού προγράμματος ηλεκτρονικής διακυβέρνησης, αφορούν:

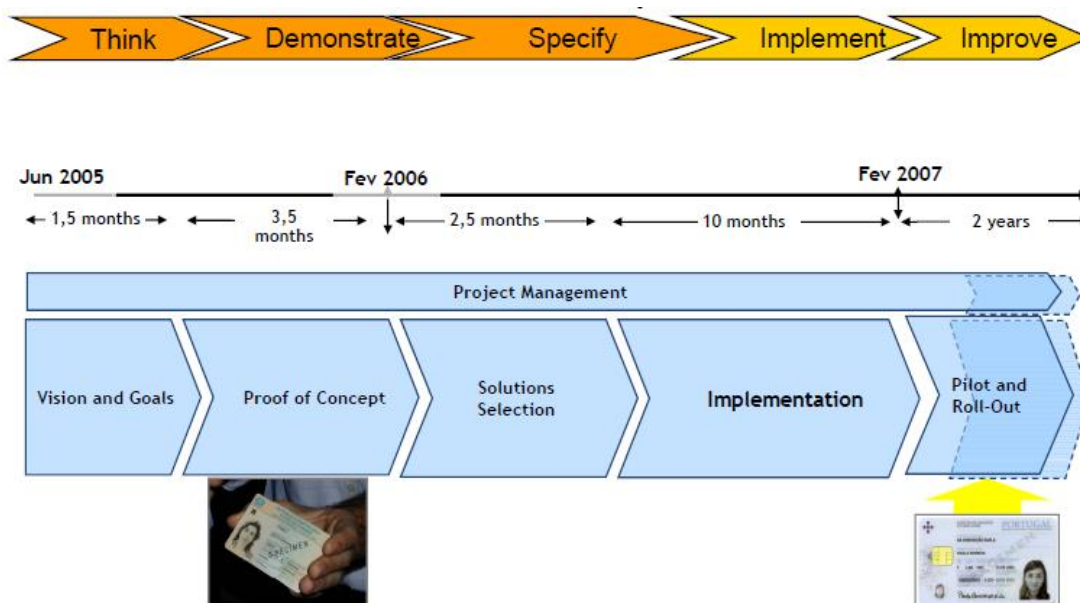
- Αξιόπιστα και ασφαλή αναγνωριστικά θα επιτρέχουν την εξάπλωση της χρήσης λόγω εμπιστοσύνης,
- Οι ποιότητα των πηγών σε θέματα πολιτών,
- Ο κεντρικός ρόλος του μητρώου,
- Το θέμα της εθνικής εμπιστοσύνης σε τρίτα μέρη,
- Το ζήτημα ασφάλειας των δεδομένων και της προσωπικής ζωής,
- Τα αρχιτεκτονικά μοντέλα για την ταυτότητα και την διαλειτουργικότητα των ηλεκτρονικών υπηρεσιών,
- Η πρόκληση της πολιτιστικής αποδοχής,
- Οι συνεργασίες για την ταχύτερη διανομή και εγκατάσταση.

Λαμβάνοντας υπόψη τα παραπάνω και δίνοντας τα επίπεδα αρχιτεκτονικής ενός μοντέλου ηλεκτρονικής διακυβέρνησης, όπου μέσω της ηλεκτρονικής κάρτας θα υπάρχει πρόσβαση σε υπηρεσίες του κράτους (ασφάλιση, υγεία, δικαιοσύνη κλπ) έχουμε το παρακάτω διαστρωματικό διάγραμμα:



2.4 Το χρονοδιάγραμμα υλοποίησης

Αν και παρακάτω προτείνουμε τον τρόπο, όπου θα μπορούσε να υλοποιηθεί το έργο στην Ελληνική περίπτωση, ενδεικτικά θα αναφέρουμε την εφαρμογή που είχε στην Πορτογαλία[16].



Όπως φαίνεται στην παραπάνω εικόνα, η χρονοσειρά και η ακολουθία συντελείται γενικά από τα βήματα της σκέψης, της παρουσίασης, της εξειδίκευσης, της

ολοκλήρωσης και της βελτίωσης. Ειδικά αν το κοινό που απευθύνεσαι είναι όλοι οι πολίτες, όλα τα παραπάνω βήματα είναι αναγκαία, ώστε να ωριμάσει η ιδέα και να γίνει αποδεκτή μια τέτοια κάρτα. Αυτός είναι και ο λόγος όπου η υλοποίηση της κάρτας πήρε δύο χρόνια και δόθηκαν άλλα δύο για τη βελτίωσή της.

Σαφώς λοιπόν και στην Ελλάδα, θα έπρεπε να ακολουθηθεί παρόμοια σειρά, κάτι το οποίο έπρεπε να είχε κατά τη γνώμη μου, προηγηθεί της διαβούλευσης. Ήτοι θα έπρεπε να είχαν τεθεί από την αρχή οι στόχοι και το όραμα χρήσης αυτής της κάρτας και να είχε υλοποιηθεί μία καμπάνια ενημέρωσης ως προς τα οφέλη χρήσης αυτής της νέας τεχνολογίας.

Το επόμενο στάδιο θα ήταν η απόδειξη της χρηστικότητας της κάρτας και η επιλογή της τελικής λύσης όσο αφορά στα τεχνικά χαρακτηριστικά αυτής. Ήτοι αυτό που κάνουμε εμείς στα επόμενα κεφάλαια. Τα τελευταία στάδια είναι η ολοκλήρωση και η εφαρμογή της νέας αυτής τεχνολογίας και κάρτας.

2.5 Μητρώο πολιτών (Ταυτοποίηση – Κοινωνική ασφάλεια – Φορολογία – Υγεία).

Όπως είδαμε στις προηγούμενες παραγράφους, η Ελλάδα διατηρεί μητρώα σε διαφορετικές υπηρεσίες και διαφορετικές οργανωτικές βαθμίδες της κυβερνητικής διαβάθμισης. Η πρόταση αυτής της μελέτης είναι η δημιουργία, υπό την αιγίδα του υπουργείου εσωτερικών, Εθνικού Μητρώου Πολιτών, στο οποίο θα έχει άμεση πρόσβαση η αστυνομία και τα δημοτολόγια της χώρας. Ουσιαστικά για κάθε παιδί που γεννιέται θα δημιουργείτε εγγραφή στο μητρώο πολιτών, από τις αστυνομικές αρχές, όπου στη συνέχεια θα γίνονται οι απαραίτητες διασυνδέσεις με οικογενειακές μερίδες από τη Δημοτική αρχή.

Αυτό σημαίνει ότι, με τη κατάθεση σε οποιοδήποτε αστυνομικό τμήμα της χώρας, της μαρτυρίας γέννησης παιδιού, της ιατρικής βεβαίωσης και της ταυτοποίησης των/του γονέων, θα δημιουργείτε εγγραφή στο μητρώο πολιτών του νέου πολίτη. Ο νέος αυτός πολίτης θα παίρνει έναν αριθμό, σύμφωνα με τον αλγόριθμο απόδοσης ΑΜΚΑ και πλέον θα πιστοποιείτε η ύπαρξη και ταυτοποίησή του μέσω του μητρώου αυτού.

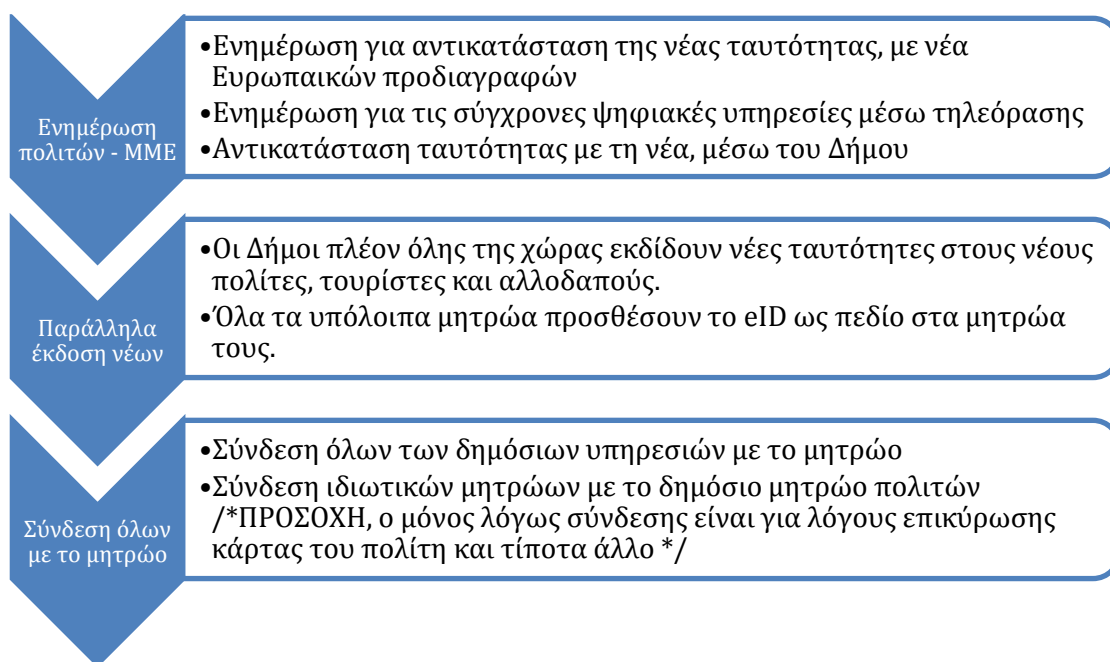
Στη συνέχεια όλες οι υπηρεσίες του κράτους θα μπορούν να συνδέουν δεδομένα και πληροφορίες για τον πολίτη αυτό, μέσω την πρόσβαση στο μητρώο, σε διάφορα επίπεδα ασφαλείας που θα δούμε σε επόμενο κεφάλαιο.

Όλοι οι πολίτες της χώρας, οι οποίοι φέρουν αστυνομική ταυτότητα, θα μπορούν να παραδίδουν αυτήν στην αστυνομική αρχή προς καταστροφή και να λαμβάνουν την νέα κάρτα του πολίτη η οποία θα φέρει το νέο ID.

Οι γονείς επίσης με το πιστοποιητικό γέννησης και οικογενειακής κατάστασης, θα μπορούν να λαμβάνουν την κάρτα των παιδιών τους.

Κατά συνέπεια μπορεί με την εφαρμογή του νέου μητρώου, εκτός της διανομής των νέων καρτών, να γίνει παράλληλα απογραφή και ταξινόμηση του πληθυσμού, όπου πλέον θα υπάρχει σε πραγματικό χρόνο ανά πάσα στιγμή.

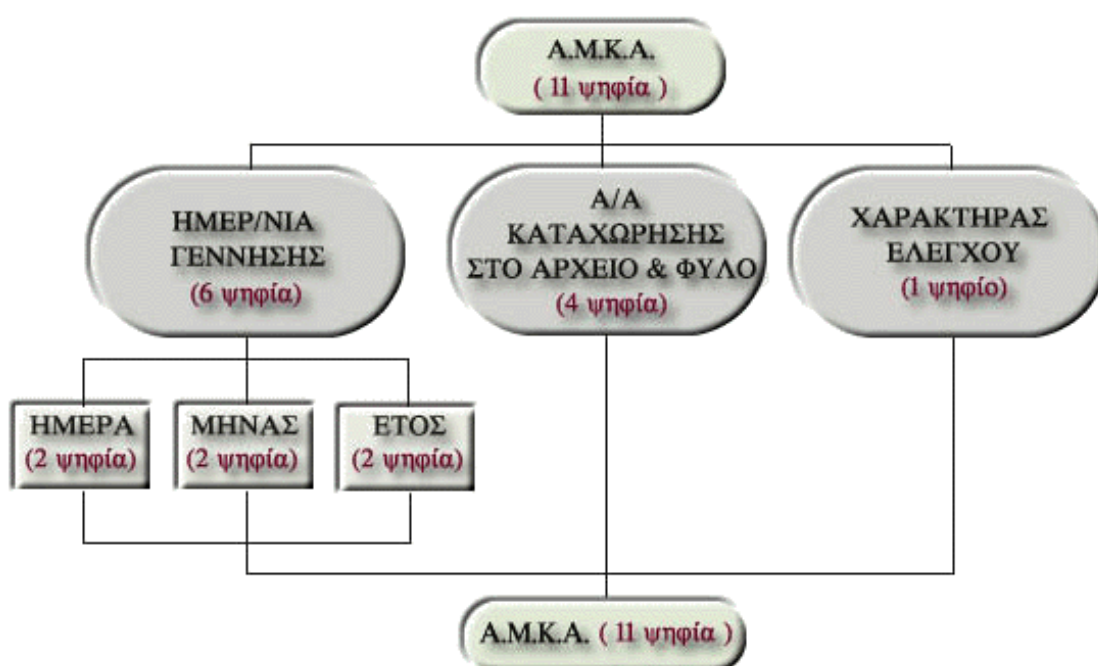
Συνεπώς τα βήματα μέχρι την ολοκλήρωση της μεταφοράς των πολιτών στο νέο μητρώο και την εφαρμογή του από εκεί και πέρα (ή και παράλληλα) είναι:



2.6 Στοιχεία του δελτίου ΑΜΚΑ – Πως προκύπτει ο αριθμός



/*Σημερινή κάρτα ΜΚΑ*/



Όπως βλέπουμε παραπάνω η κάρτα αυτή φέρει μόνο το Ονοματεπώνυμο, το Πατρώνυμο και τον αριθμό ΑΜΚΑ.

Ο παραπάνω αλγόριθμος ο οποίος χρησιμοποιείται για τη δημιουργία του δημόσιου κλειδιού – αριθμό ΜΚΑ, ο ίδιος μπορεί να χρησιμοποιηθεί για την δημιουργία του eID της eCC.

2.7 Συγχώνευση υπολοίπων μητρώων.

Με τη δημιουργία του μητρώου πολιτών, έχουμε κατάργηση – συγχώνευση του μητρώου που τηρεί η αστυνομία με τις εγγραφές των αστυνομικών δελτίων

ταυτότητας. Με την νέα εγγραφή στο μητρώο πολιτών, η αστυνομική αρχή έχει την ευθύνη να μεταφέρει όλες τις πληροφορίες που μέχρι τότε διατηρούσε στο μητρώο της, έτσι ώστε το νέο μητρώο πολιτών να κληρονομήσει όλες τις παρελθοντικές πληροφορίες της αστυνομίας.

Δημοτολόγιο – Μητρώο αρρένων κλπ. Οι Δημοτικές αρχές άμεσα θα έχουν πρόσβαση στο μητρώο πολιτών, αφού ο πολίτης όταν θα εγγράφεται θα εγγράφει ταυτόχρονα και τα ανήλικα παιδιά του. Κατά συνέπεια οι Δημοτικές αρχές θα ενημερώνουν σε βοηθητικούς πίνακες του μητρώου (δευτερευόντων πίνακες), όλα τα στοιχεία οικογενειακών μερίδων που θα διέπουν τον κάθε πολίτη. Κατά συνέπεια, πολίτη – πολίτη, θα ενημερώνεται το αρχείο πολιτών μέχρι να καταχωρηθεί ολόκληρος ο πληθυσμός της χώρας. Το αστυνομικό μητρώο αλλά και το δημοτικό μητρώο θα συνεχίσουν να υπάρχουν παράλληλα με μοναδικό λόγω ύπαρξης την άντληση και διασταύρωση πληροφοριών. Ουσιαστικά θα είναι ένα και το αυτό, αφού το μητρώο της αστυνομίας θα συγχωνευτεί με το δημοτικό.

Μητρώα ασφαλιστικών φορέων.

Δεν χρειάζεται να γίνει καμία παρέμβαση στα μητρώα ασφαλιστικών φορέων, διότι ο εθνικός αριθμός πολίτη θα είναι ο σημερινός ΑΜΚΑ. Αυτό όμως που θα χρειαστεί να γίνει είναι η διασύνδεση με το μητρώο πολιτών και η σταδιακή ή με γέφυρα ενημέρωση των δευτερευόντων πινάκων του μητρώου. Όπως αναφέραμε ο μόνος που θα μπορεί να επικυρώσει την ύπαρξη ενός αριθμού πολίτη θα είναι το Δημοτικό μητρώο.

2.8 Η περίπτωση των τραπεζών.

Οι ιδιωτικές εταιρίες έχουν την ίδια ευθύνη της ηλεκτρονικής εφαρμογής της ταυτοποίησης και των υπηρεσιών προς τους πελάτες τους που θα μπορούσαν να επωμιστούν όλο το βάρος της υλοποίησης του έργου. Η δημιουργία ενός καθολικού μητρώου πολιτών με συνεργασία όλων των εμπλεκόμενων φορέων, επιχειρήσεων και οργανισμών θα μπορούσε ίσως ταχύτερα και ασφαλέστερα να υλοποιηθεί το έργο αυτό.

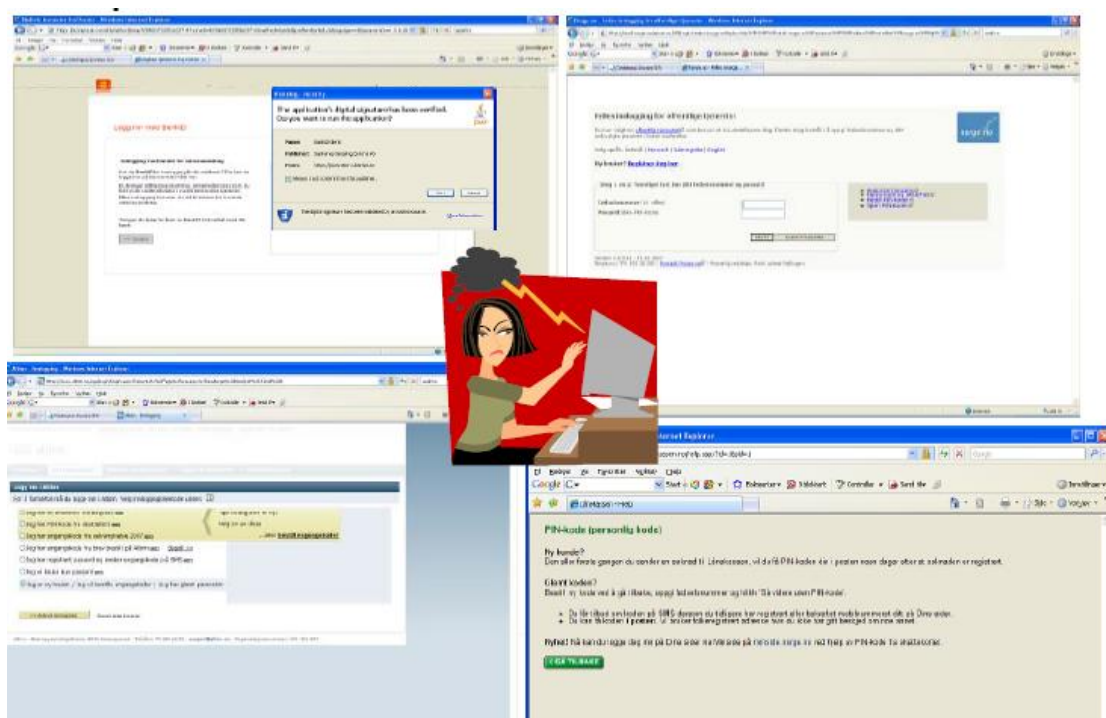
Ένα πετυχημένο παράδειγμα αποτελεί το BankID που εφαρμόζεται στη Σουηδία και έχει πάρει διαστάσεις ηλεκτρονικής διακυβέρνησης. [6],[31]

2.9 Δεύτερο πεδίο στις βάσεις δεδομένων ο αριθμός του πολίτη (σε εμάς ο ΑΜΚΑ)

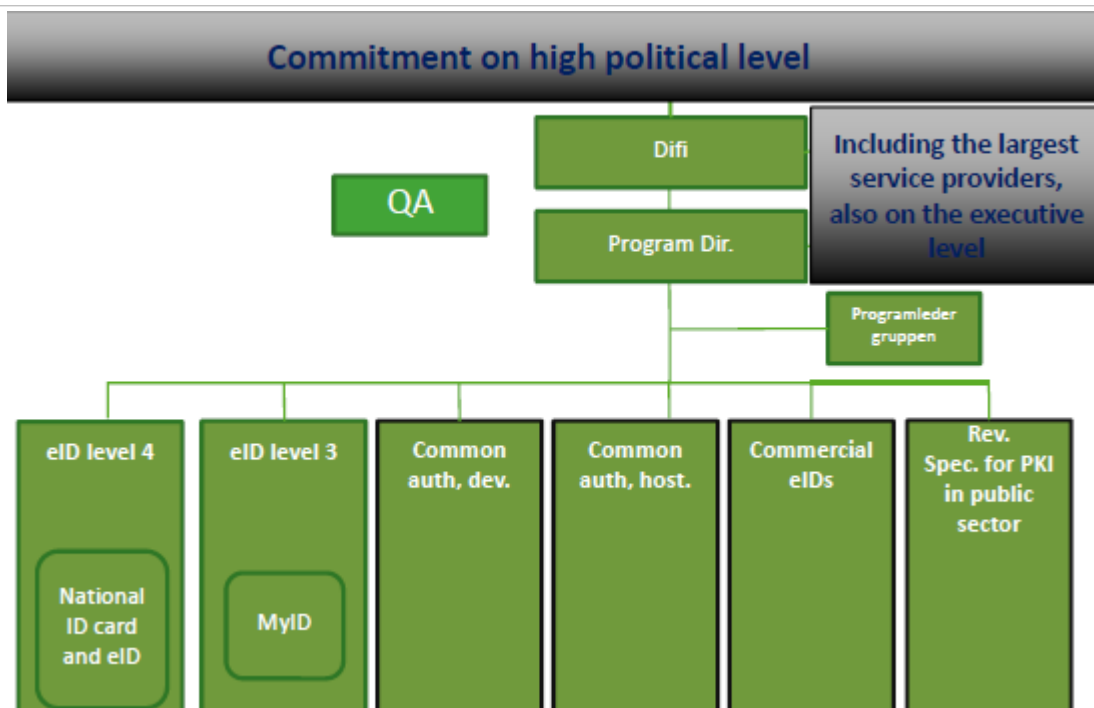
Ποιο είναι ουσιαστικά το πρόβλημα [17];

- Διαφορετικές υπηρεσίες – διαφορετικά ids
- Δεν είναι μόνο πρόβλημα του πολίτη αλλά και:
 - ο Πρόβλημα ανάπτυξης εφαρμογών και θεμάτων,
 - ο Πρόβλημα υποστήριξης και συντήρησης,
- Εάν η υπηρεσία ενσωματώνει άμεσα περισσότερων του ενός eIDs , σε κάθε νέα εφαρμογή ή αναβάθμιση θα πρέπει να γίνονται τεστ σε όλα τα ids.

Με διαφορετικές κάρτες ο χρήστης είναι αναγκασμένος να έχει διαφορετική εμπειρία σε κάθε περιβάλλον.



Για το λόγω αυτό θα πρέπει να προστεθεί σε κάθε βάση δεδομένων (δημοτολόγια, ληξιαρχεία, εφορίες κλπ) το πεδίο του αριθμού eID.



2.10 Η αρχιτεκτονική του πληροφοριακού συστήματος.

Το πληροφοριακό σύστημα θα πρέπει να υποστηρίζεται από συστήματα και διεργασίες. Το σύστημα θα πρέπει να εξάγει κάθε φορά ένα νέο αριθμό, μέσω του **PKI**. Το **μητρώο πολιτών** θα δημιουργεί την εγγραφή μέσω του PKI και το **σύστημα εξατομίκευσης της κάρτας** θα συνδέει αυτή με τον κάτοχό της.

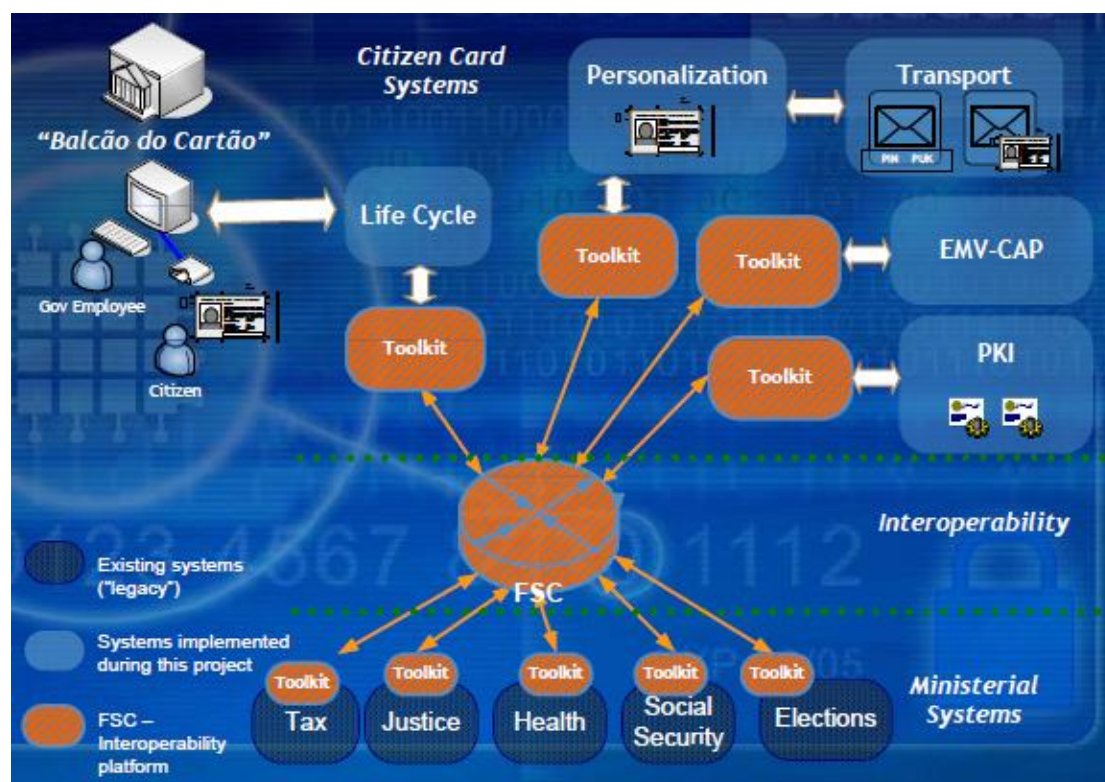
Πρακτικά το **μητρώο πολιτών** είναι υπεύθυνο να ορίζει τον κύκλο ζωής της κάρτας του πολίτη. Είναι υπεύθυνο για την έκδοση της κάρτας, να λαμβάνει αιτήσεις για την ανανέωση, την παράδοση της κάρτας – την αποστολή, την ακύρωση κάρτας, την ενεργοποίηση κλπ. Επιπλέον το σύστημα είναι υπεύθυνο για την έκδοση και προγραμματισμό της κάρτας, όπως το φυσικό – γραφιστικό σχεδιασμό, την αποτύπωση δεδομένων στην κάρτα και στο chip, ψηφιακά πιστοποιητικά, pin, ruks κλπ. Την έκδοση PKI που είναι υπεύθυνο για την επικύρωση και την διαχείριση των ψηφιακών πιστοποιητικών. Μέσα σε αυτό το σύστημα θα υπάρχουν και τα τομεακά δεδομένα του πολίτη, π.χ. κοινωνικής ασφάλισης, τμήματα εφορίας, υγείας κλπ.

Σύστημα εξατομίκευσης κάρτας. Το σύστημα αυτό είναι υπεύθυνο για την εξατομίκευση της κάρτας – Οπτικά χαρακτηριστικά του κατόχου στην κάρτα και στο chip. Το σύστημα αυτό επικοινωνεί με το μητρώο για να μπορεί να εξατομικεύσει βιομετρικά δεδομένα, κωδικούς, πιστοποιητικά από το PKI. Επιπλέον μέσω του

συστήματος αυτού, μπορούν να λειτουργούν άλλα υποσυστήματα, όπως της ενέργειας αποστολής της κάρτας προς τον κάτοχο, την αποστολή κωδικών και pins της κάρτας στη διεύθυνση του πολίτη κλπ.

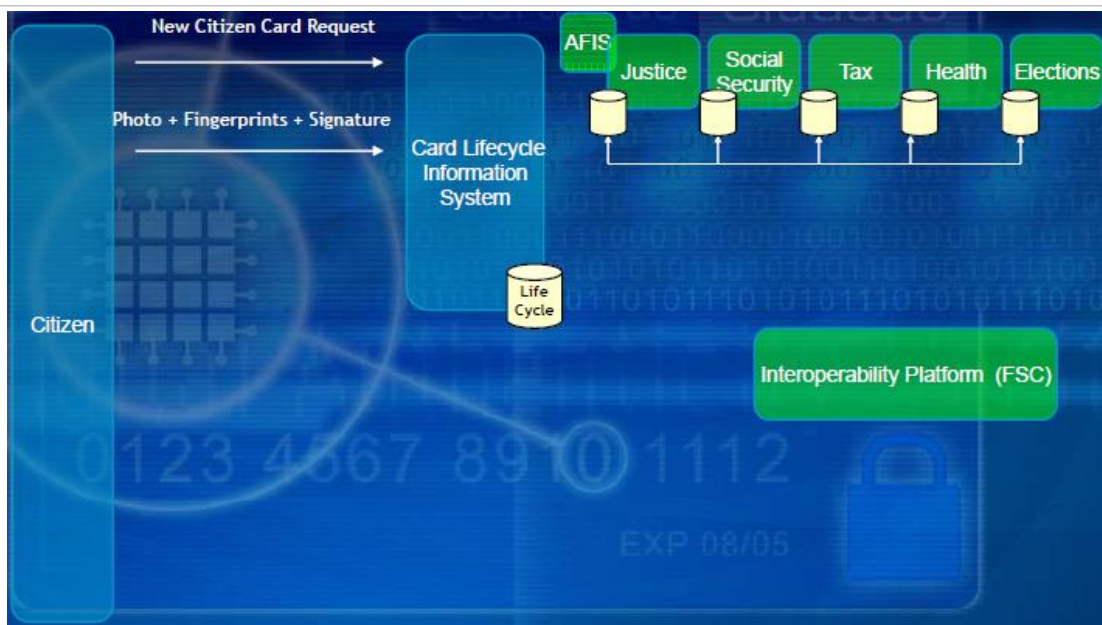
PKI: Το PKI (Public Key Infrastructure), λειτουργεί ως αρχή πιστοποίησης. Ως αρχή πιστοποίησης, είναι υπεύθυνη για την έκδοση ψηφιακών πιστοποιητικών, έκδοση υπηρεσίας σήμανσης χρονικής στιγμής, διαχείρισης όλου του PKI, κλπ.

Στο παρακάτω σχήμα φαίνεται το πλαίσιο παροχής υπηρεσιών από το μητρώο πολιτών, σε όλα τα επίπεδα [14]:

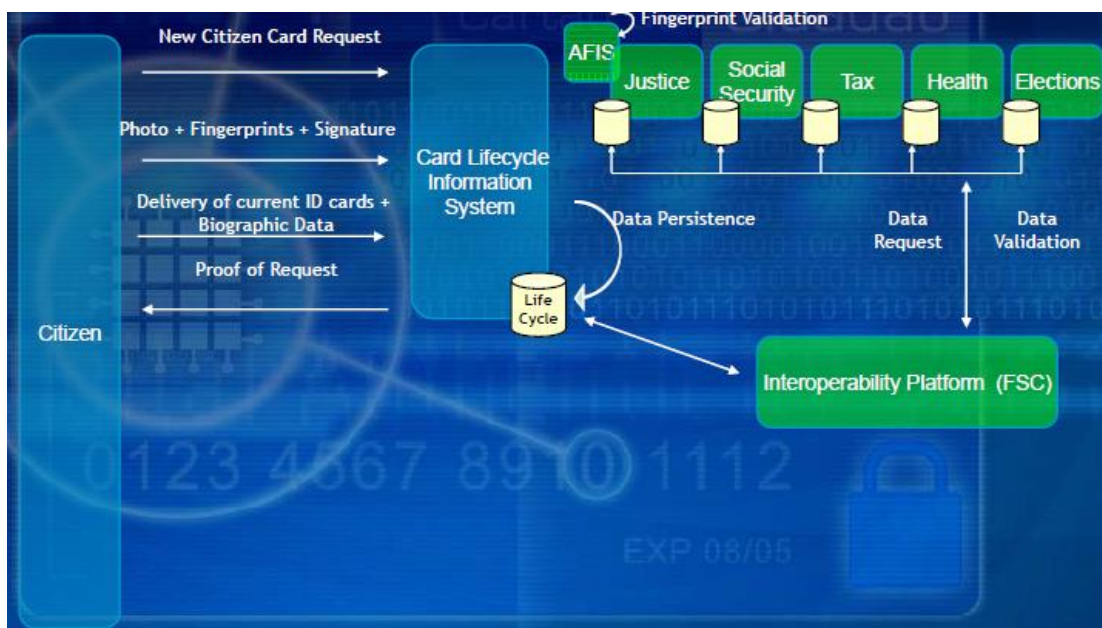


2.11 Υπηρεσία έκδοσης κάρτας.

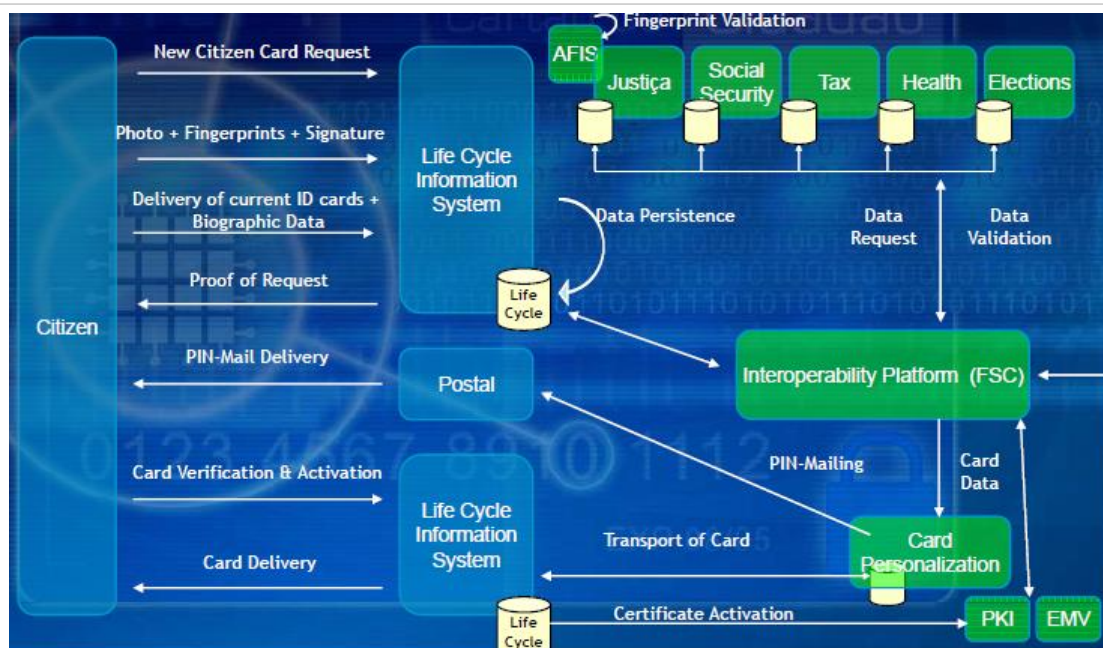
Σε επίπεδο όπου ο πολίτης αιτείται την έκδοση κάρτας (ή ο πληρεξούσιος ανάδοχος), τότε με τα στοιχεία της **φωτογραφίας**, των **δακτυλικών αποτυπωμάτων** και την **υπογραφή** (π.χ.) ολοκληρώνεται η αίτηση [14].



Το επόμενο βήμα είναι η αποστολή από τον πολίτη, των μέχρι σήμερα πιστοποιητικών και καρτών που κατέχει και τα βιογραφικά του δεδομένα, ως απόδειξη της πραγματικότητας του αιτήματος.



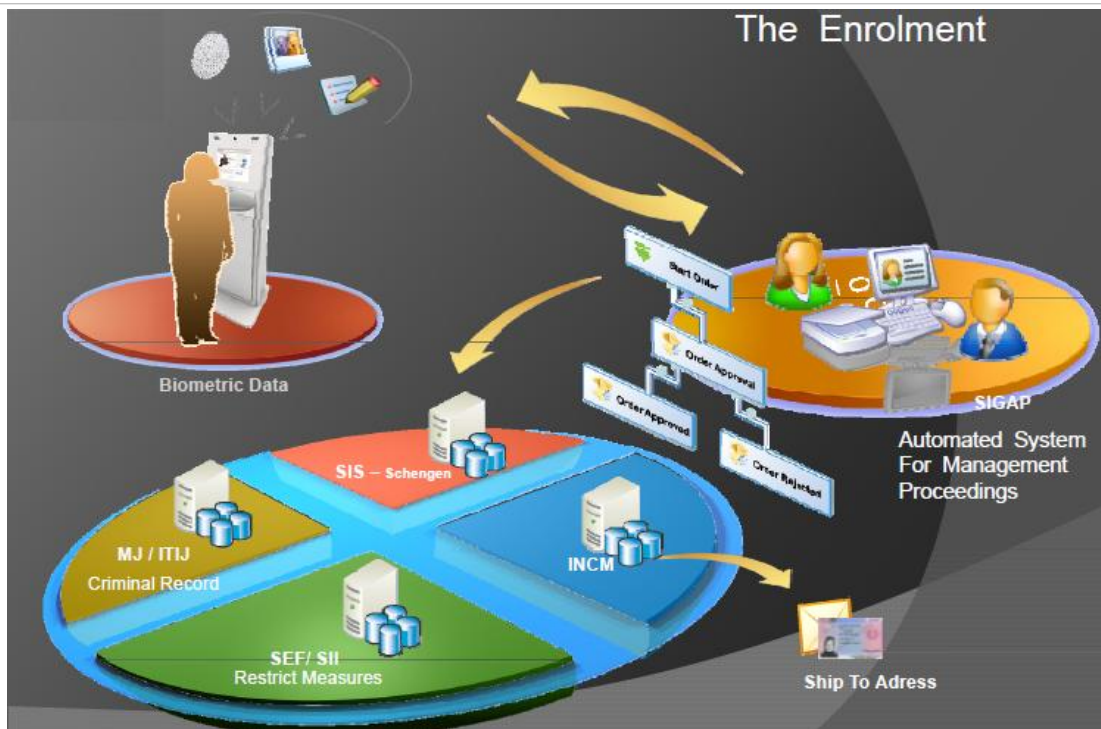
Τελικό στάδιο, όπου η πολίτης λαμβάνει την κάρτα και την ενεργοποιεί.



2.12 Κύκλος ζωής κάρτας παραμονής.

Όπως έχουμε αναφέρει στα πρώτα κεφάλαια, θα υπάρχει χρωματική διαφοροποίηση καρτών, για ανήλικες – ενήλικες και για τους ενήλικες η διαφοροποίηση Ευρωπαίων (Ελλήνων), Αλλοδαπών εργαζομένων στην Ευρώπη και Τουριστών. Η κάρτες εργαζομένων στην Ευρώπη και Τουριστών, από τρίτες χώρες αντιπροσωπεύουν την άδεια παραμονής στη χώρα. Ωστόσο λοιπόν, ως άδεια παραμονής θα έχει τα εξής χαρακτηριστικά:

- Θα εκδίδεται κάρτα για πολίτες τρίτων χωρών,
- Το έγγραφο θα είναι ασφαλές σύμφωνα με ICAO,
- Η ηλεκτρονική κάρτα θα φέρει chip το οποίο θα επιτρέπει την αποθήκευση βιογραφικών και βιομετρικών στοιχείων, όπως πρόσωπο, αποτύπωμα δακτυλικό κλπ,
- Διαμόρφωση ενιαίου τύπου όπως καθορίστηκε στον κανονισμό συμβουλίου 380/2008 και 1030/2002.



Το προξενείο της κάθε χώρας στην Ευρώπη θα είναι υπεύθυνο για την έκδοση άδειας παραμονής σε μία ή σε όλες τις χώρες της Ευρωπαϊκής Ένωσης ή της Visas. Αυτό θα είναι υπεύθυνο για να συγκεντρώσει τα στοιχεία που χρειάζονται για την έκδοση της άδειας παραμονής. Σάρωση εγγράφων, αποτυπώματα, χαρακτηριστικά βιομετρικά και βιογραφικά κλπ.

Οι στόχοι είναι [27]:

- Η ελαχιστοποίηση της φυσικής υποστήριξης (γραφειοκρατία) ώστε να αποφευχθούν οι καθυστερήσεις και οι φαύλοι κύκλοι,
- Να εναρμονιστεί η διαδικασία για όλους τους πολίτες,
- Η διευκόλυνση της ανταλλαγής πληροφοριών με άλλους οργανισμούς,
- Η προώθηση της αναγνώρισης συνεργατών και κίνητρα για τη χρήση νέων τεχνολογιών,
- Η βοήθεια στους πολίτες να παίρνουν πληροφορίες την ώρα που λαμβάνει χώρα η διαδικασία,
- Να δημιουργήσει συνθήκες αποθήκευσης βιομετρικών δεδομένων και να αύξηση την ασφάλεια των δεδομένων και στοιχείων των πολιτών.

2.13 Εθνικές eIDs από τη σκοπιά της HP – Χρωματική διαφοροποίηση.

Στην παράγραφο αυτή θα δούμε την τοποθέτηση της HP στην ολοκλήρωση των Εθνικών καρτών eIDs, που παρουσιάστηκε στην Αθήνα στο συνέδριο της 21/10/2010. Σύμφωνα λοιπόν με αυτή, σήμερα οι πολίτες έχουν πάνω από μία κάρτα. Το κίνητρο για την μία κάρτα του πολίτη εγγυάται στην ασφάλεια, βιομετρικά στοιχεία, ηλεκτρονικές υπηρεσίες, κόστος λειτουργίας. Είναι πάντως ευκαιρία λόγω του ότι τρέχουν 50 έργα σε 30 χώρες στο θέμα eID & eHealth. Η πρόκληση είναι ότι όταν υιοθετηθεί πλήρως από Γαλλία, Γερμανία και Αγγλία θα υπάρξει απαίτηση για εκατομμύρια κάρτες.

Το κίνητρο για προσωπικές κάρτες eID είναι:

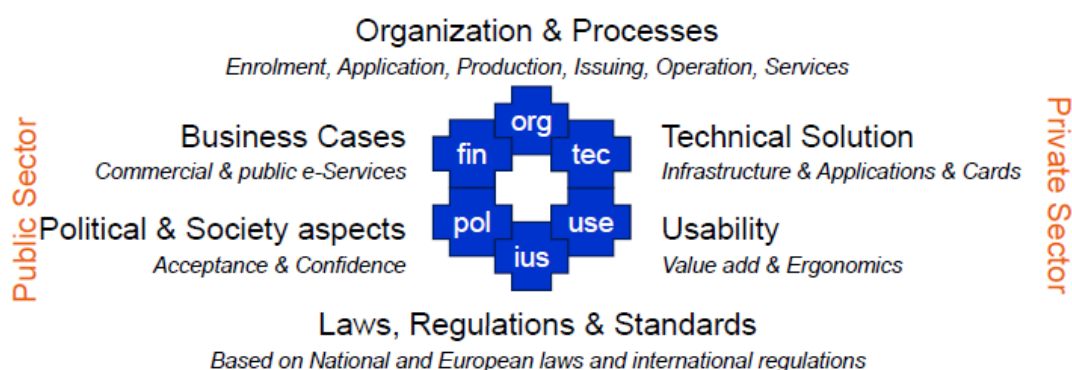
Από την πλευρά της κυβέρνησης:

- Ασφαλέστερα ταξίδια και καταπολέμηση απάτης,
- Συμμόρφωση με διεθνής κανονισμούς,
- Λιγότερες φορολογικές απάτες,
- (EU council regulation (EC) No 2252/2004, ICAO Doc 9303)

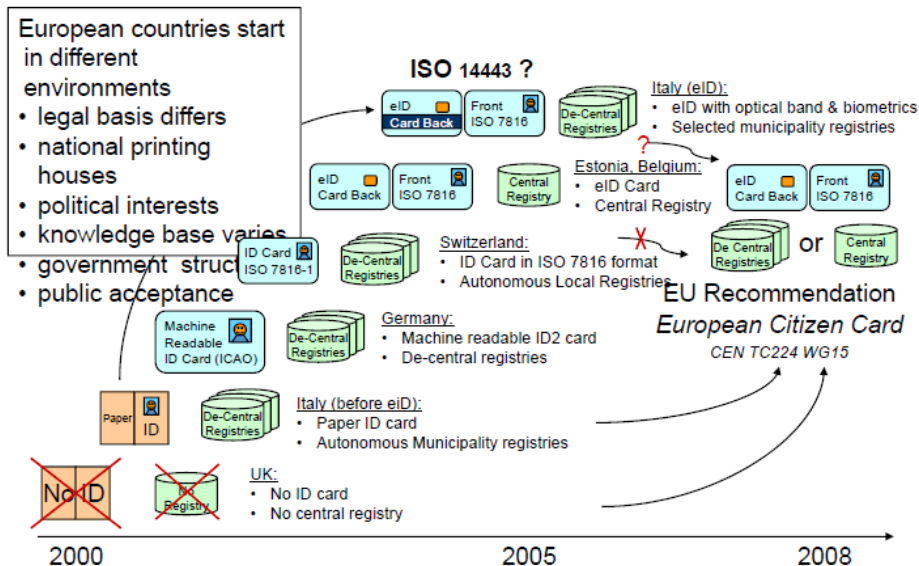
Από την πλευρά του πολίτη:

- Ταξίδια χωρίς θεώρηση visa
- Ασφαλές υπηρεσίες εμπορίου,
- Ασφαλές συναλλαγές ηλεκτρονικής διακυβέρνησης,
- Βελτίωση ποιότητας υπηρεσιών,
- Διευκόλυνση πολιτών και κινητικότητας,
- Ηλ. Υπογραφές (EU directive 1999/93/EC electronic signatures)

Η ολιστική προσέγγιση της HP είναι η παρακάτω:



Η εξέλιξη της διαλειτουργικότητας των eID καρτών στην Ευρώπη φαίνεται στην παρακάτω εικόνα.

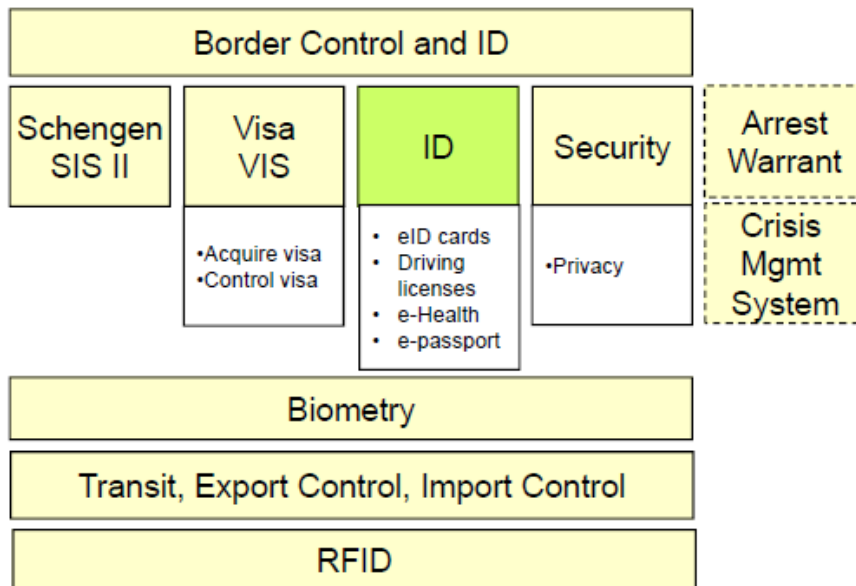


Προϋποθέσεις και παράγοντες επιτυχίας μεταξύ άλλων θεωρούνται:

- Το πολιτικό πλαίσιο πρέπει να είναι κατάλληλο,
 - ο Προώθηση ως δημόσια υπηρεσία,
 - ο Δημιουργία και παροχή υποδομής,
 - ο Δίκτυα υποδομής,
- Ανάπτυξη εμπιστοσύνης και αποδοχής από τους πολίτες και τους επιχειρηματίες,
 - ο Οι πολίτες είναι εξοικειωμένοι με τις κάρτες και τα pins,
 - ο Αποδεδειγμένη αξία και τα οφέλη της ιδιωτικής ζωής και εγγύηση της ασφάλειας,
- Η διεθνής εμπειρία , τα πρότυπα και η διαλειτουργικότητα,
 - ο eID υποχρεωτικά σε D,B,GR,E, επιλεκτικά σε A,SF,F,I,L,NL,S,...
 - ο Διασυνοριακή αναγνώριση και εγκυρότητα και κοινά στάνταρντ μέσα στην Ευρώπη,
- Χρηματοοικονομικά και επιχειρήσεις
 - ο Ποιος καλύπτει αρχικές επενδύσεις σε υποδομές,
 - ο Ποιές εργασίες πρέπει να γίνουν από την κυβέρνηση,
 - ο Τι είναι πρόθυμοι να πληρώσουν οι πολίτες.

Σήμερα η ηλεκτρονική κάρτα, το εμπόριο και οι διασυνοριακές σχέσεις, θα μπορούσαν να παραστούν στο παρακάτω διάγραμμα: [47]

Citizen



Σήμερα, η HP έχει υποστηρίξει τη διαχείριση της ταυτοποίησης των πολιτών ως παρακάτω:

Βουλγαρία τρέχουσα κάρτα εθνικής ταυτότητας, διαβατηρίου και των πιστοποιητικών οδηγών του συστήματος

Νέα Ζηλανδία βιομετρικό σύστημα έκδοσης διαβατηρίων και του ICAO συμβατό δημόσιου κλειδιού εφαρμογής υποδομών

Σλοβακία Κέντρο Εθνικής Εξατομίκευσης για τις άδειες οδήγησης και ταυτότητες, κάρτες ξένων κατοίκων και e-διαβατήρια

Ιταλία Εθνικό σύστημα Δελτίο Αστυνομικής Ταυτότητας, υποδομή και ασφάλεια, βιομετρικό σύστημα, ιταλική ePassport

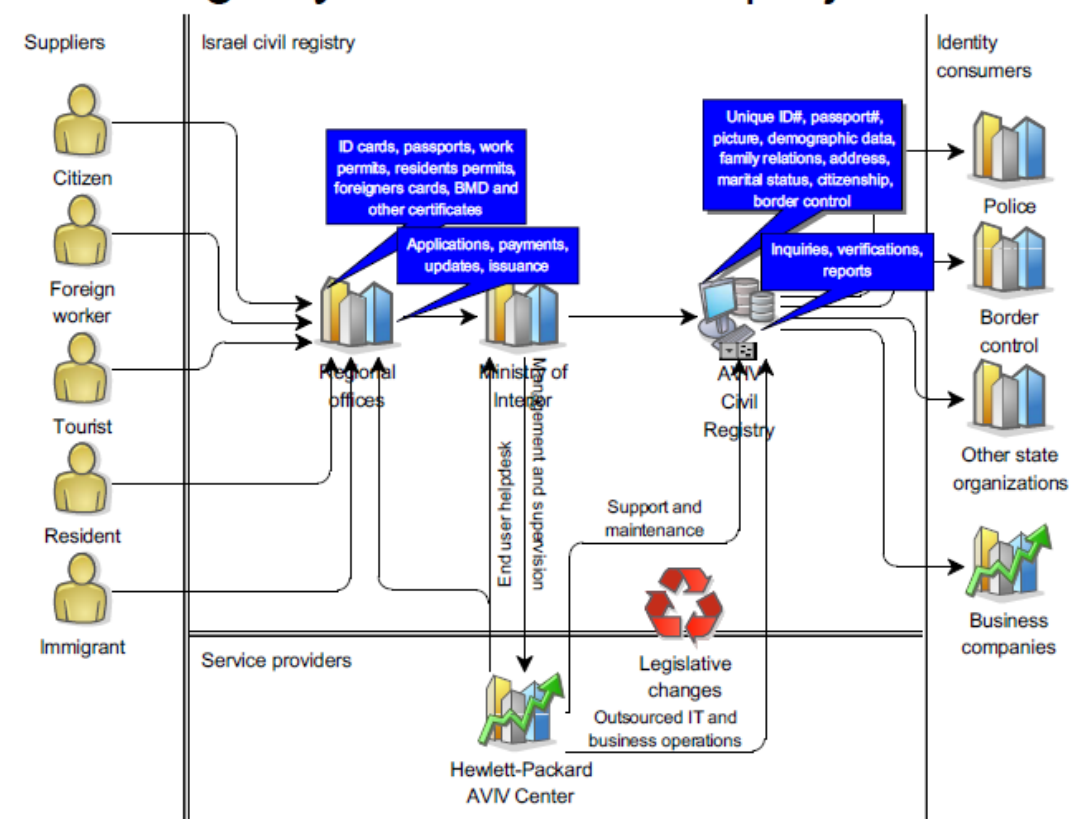
Πολωνία εθνικό δελτίο ταυτότητας, διαβατήριο και άδεια οδήγησης και πρόσφατα, επίσης έγγραφο κυκλοφορίας οχημάτων

Φλόριντα & Μέρυλαντ , άδεια οδηγού, Ίρις δελτία ταυτότητας Φυλακές, Ποινικό Σύστημα Κράτησης Ατλάντα, Αριζόνα Ποινικό Κρατήσεις,

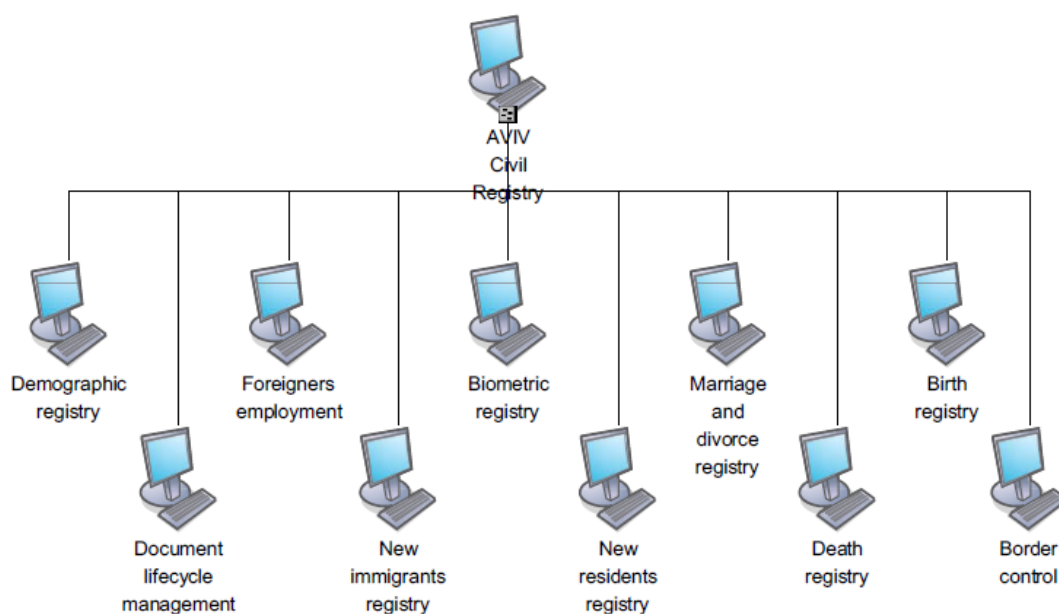
Χονγκ Κονγκ ασφαλή ηλεκτρονική πλατφόρμα παροχής για την ηλεκτρονική διακυβέρνηση και το σύστημα πιστοποίησής της βασίζονται στην ηλ-ταυτότητες

Ισραήλ Εθνικό Τμήμα Αρχείου Πληθυσμού διαβατήριο υποστήριξης, άδεια οδηγού, ταυτότητα ψηφοφόρου, γέννηση, γάμος και θάνατος πιστοποιητικό και άλλες ατζέντες

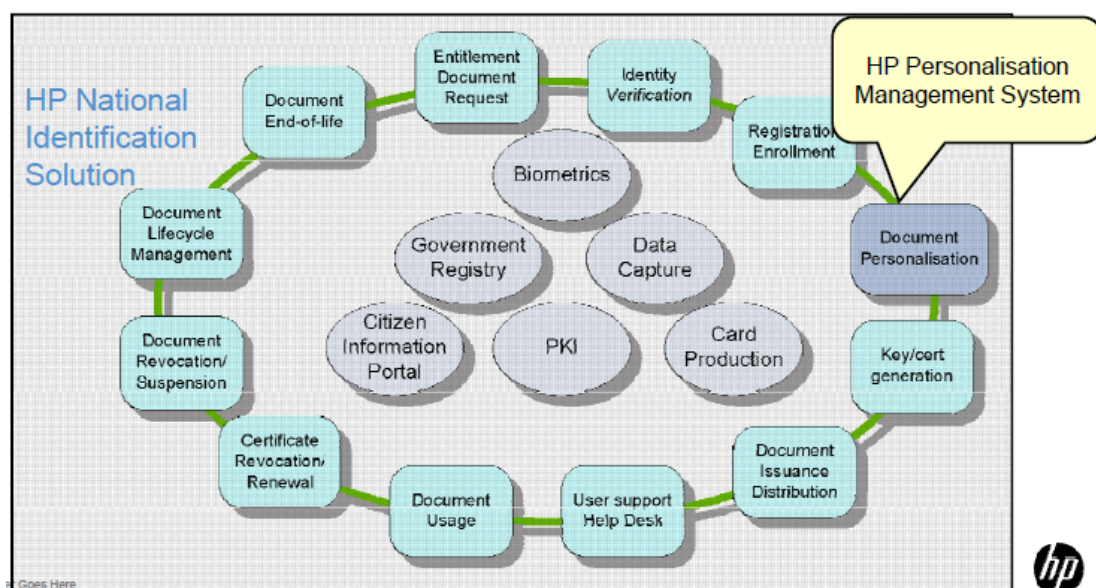
Civil registry in Israel - AVIV project



AVIV registry – high level structure



Στο παρακάτω διάγραμμα εμφανίζεται ο κύκλος ζωής της κάρτας του πολίτη σύμφωνα με τη HP.



Όπως βλέπουμε στην ολιστική ανάλυση της HP η αιτών της κάρτας μπορεί να είναι πολίτης, ξένος εργαζόμενος, τουρίστας, μετανάστης. Εμείς στην προσέγγισή μας θεωρούμε τέσσερις βασικές κατηγορίες.

Η **μπλε** κάρτα θα συμβολίζει ότι ο κάτοχος είναι Έλληνας υπήκοος, ότι διαμένει και εργάζεται νόμιμα στην Ελλάδα ως Έλληνας πολίτης. Η κάρτα αυτή θα προκύπτει από την συμπλήρωση των 18 ετών από Έλληνα υπήκοο ο οποίος θα παραδίδει την πορτοκαλί κάρτα και θα λαμβάνει τη μπλε. Όποιος φέρει μπλε κάρτα, εννοείτε ότι είναι εγγεγραμμένος στα μητρώα ασφάλισης, δικαιοσύνης, υγείας, εφορίας, παιδείας κλπ

Η κάρτα χρώματος **πορτοκαλί** θα συμβολίζει ότι ο κάτοχος είναι Έλληνας πολίτης κάτω των 18. Θα εκδίδεται με τη γέννηση του παιδιού και υπεύθυνος για την κατοχή της θα είναι ο γονιός, μέχρι να ενηλικιωθεί το παιδί.

Η **πράσινη** κάρτα θα συμβολίζει ότι ο κάτοχός της είναι αλλοδαπός, βρίσκεται νόμιμα στη χώρα και μπορεί να διαμένει και να εργάζεται ή να επιχειρεί νόμιμα στην Ελλάδα. Την ίδια κάρτα θα φέρουν και τα παιδιά του, τα οποία μετά την απόκτηση της Ελληνικής υπηκοότητας η κάρτα τους θα γίνεται μπλε ή πορτοκαλί, αναλόγως την ηλικία τους.

Τέλος θα υπάρχει και η **λευκή** κάρτα, η οποία θα είναι εθελοντική και θα συμβολίζει ότι ο κάτοχός της, έχει είναι εγγεγραμμένος στο μητρώο πολιτών που τηρεί η Ελλάδα και βρίσκεται νόμιμα σε αυτήν. Αυτή την κάρτα θα μπορεί να φέρει οποιοσδήποτε

τουρίστας – επισκέπτης εισέρχεται στην Ελλάδα, ο οποίος με τη χρήση αυτής θα μπορεί να απολαμβάνει τις σύγχρονες ψηφιακές υπηρεσίες του κράτους και των ιδιωτών καθώς και θα αποφεύγει οποιοδήποτε έλεγχο στοιχείων από τα σώματα ασφαλείας και τις αρχές.

Φυσικά όποιος θα φέρει κάρτα του πολίτη, θα γνωρίζει ότι μέσα στο chip θα είναι αποθηκευμένα βιομετρικά στοιχεία τα οποία θα μπορούν να ταυτοποιήσουν τον κάτοχο, όπως και η ανάγνωση περαιτέρω στοιχείων θα απαιτεί το pin από τον κάτοχο.

Στο παρακάτω κεφάλαιο θα προχωρήσουμε στην περιγραφή της φυσικής σχεδίασης της κάρτας του πολίτη.

3ο Κεφάλαιο : Φυσική σχεδίαση της κάρτας του πολίτη

Εδώ αναλύεται και παρουσιάζεται η πρότασή μας για τη φυσική σχεδίαση της κάρτας. Αναλύονται και αιτιολογούνται, το είδος και η ποσότητα των προσωπικών στοιχείων που θα εμφανίζονται πάνω σε αυτή. Ορίζονται τα ελάχιστα στοιχεία για την προσωπική ταυτοποίηση του κατόχου, ιδιαίτερα σε περιπτώσεις διακοπής ρεύματος και αστοχίας εξακρίβωσης μέσα από το πληροφοριακό σύστημα.

3.1 Η εμφάνιση

Η φυσική σχεδίαση της κάρτας του πολίτη, έγκειται στην σχεδίαση της εμφάνισης, η οποία θα προσδίδει τον πολιτισμό και την κουλτούρα της Ευρωπαϊκής ένωσης καθώς και λειτουργικά στο σχεδιασμό των απαραίτητων στοιχείων που θα πρέπει να απεικονίζονται σε αυτήν.

Συνεπώς λοιπόν θα πρέπει να επικεντρωθούμε στη χρήση και στις λειτουργίες που θα μπορούν να γίνουν με την κάρτα αυτή ώστε να καταλήξουμε στα απαραίτητα στοιχεία και κυκλώματα που θα την απαρτίζουν (που θα περιέχει).

Η κάρτα αυτή συγχωνεύει οπτική και ηλεκτρονική ταυτοποίηση [12], όπου οι απαιτήσεις για την κάρτα απορρέουν από τις συνθήκες, αποτελέσματα του παρακάτω πίνακα:

Ταυτοποίηση	
Οπτική αναγνώριση	Για τις δημόσιες υπηρεσίες και ιδιωτικές εταιρίες
Ηλεκτρονική ανάγνωση από συσκευές	
Επαλήθευση της γνησιότητας του εγγράφου	Πιστοποίηση μεταξύ κάρτας και τερματικής συσκευής – ανάγνωσης
Επαλήθευση της ταυτότητας του κατόχου της κάρτας	Π.χ. αποθήκευση/ σύγκριση δακτυλικών αποτυπωμάτων και/ή τα προσωπικά δεδομένα του κατόχου
Πιστοποίηση	
Online	Δημόσιες υπηρεσίες eBusiness (B2C,B2B,B2G)
Offline	Συσκευή πώλησης
Αντικατάσταση της ανασφαλούς πιστοποίησης με το όνομα και τον κωδικό με μοναδικό cardPIN	
Αμοιβαία πιστοποίηση μεταξύ παρόχου και χρήστη υπηρεσιών	
Ψηφιακή υπογραφή	
Προηγμένη (advanced) υπογραφή	Μοναδική είσοδος Κρυπτογράφηση Email υπογραφή
Εξειδικευμένη (διαβαθμισμένη) υπογραφή	e-τιμολόγια e-δήλωση φόρου κλπ

Σύμφωνα με την τυποποίηση της Ευρωπαϊκής Κάρτας του Πολίτη – ECC (15480-1/-4), η Ευρωπαϊκή κάρτα έχει την παρακάτω εμφάνιση:



Μέρος 4^ο : Προφίλ

Χωρίς να αποκλίνουμε από το Ευρωπαϊκό πρότυπο τυποποίησης, προτείνουμε για την Ελλάδα, την παρακάτω κάρτα (Στο σημείο αυτό να ευχαριστήσω τον Γεώργιο Κράλλη, Γραφίστα, ο οποίος με βοήθησε με το σχεδιασμό της κάρτας του πολίτη):



Η κάρτα φέρει πάνω της στοιχεία όπως φωτογραφία του κατόχου, διακριτικό χώρας έκδοσης, ονοματεπώνυμο, αριθμό, ομάδα αίματος, πόλη όπου προέρχεται ο κάτοχος (δημοτολόγιο), χώρα προέλευσης κατόχου και ημερομηνίες όπου είναι έγκυρη η κάρτα. Επιπλέον φέρει chip με όλα τα στοιχεία του κατόχου και τέλος φέρει την υπογραφή του. Στην πίσω όψη, υπάρχει το εθνόσημο του κράτους έκδοσης, διακριτικά δικτύου τραπεζών που αναγνωρίζει την κάρτα, ολόγραμμα οπτικής γνησιότητας και κωδικοί barcode. Στο chip θα αποθηκεύονται σε διάφορες διαβαθμίσεις ασφάλειας όλα τα βιομετρικά στοιχεία και φυσικά η ψηφιακή υπογραφή. Η ψηφιακή υπογραφή έχει την ίδια νομική εγκυρότητα με την ιδιόχειρη υπογραφή. Φανταστείτε ότι με την πιστοποίηση της κάρτας π.χ. από τον αναγνώστη καρτών, είναι σαν να υπογράφεται την αίτηση (κάποια αίτηση).

Το υλικό της κάρτα θα είναι πολυανθρακικό (πολυκαρβονικό) το οποίο έχει τις παρακάτω ιδιότητες [49]:

- Ιδανικό για την εξατομίκευση με λέιζερ,
- Κατασκευάζεται με προστατευτική επικάλυψη,
- Είναι δύσκολο να αντιγραφούν οι λεπτομέρειες,
- Είναι δύσκολη η αντιγραφή μέσω έγχρωμης εκτύπωσης,
- Είναι κατάλληλο για μεγάλη διάρκεια ζωής.



Αυτό το υλικό της κάρτας, αποτελεί συνθετικό υψηλής ασφάλειας. Είναι σταθερό και δεν έχει επιπτώσεις αλλοίωσης. Παρουσιάζει υψηλή αντοχή σε φθορά ανάγνωσης. Από την εκτύπωση έχουμε υψηλή αντίθεση ώστε να διακρίνεται εύκολα. Επιπλέον έχει υψηλή αντοχή σε υπεριώδη ακτινοβολία.

Η διαστρωματικές επιφάνειες τις κάρτας είναι οι παρακάτω:

1 ^ο επίπεδο : Πολυκαρβονική επικάλυψη	150 microns
2 ^ο επίπεδο : Πολυκαρβονική επικάλυψη Kinegrame	100 microns
3 ^ο επίπεδο : Πολυκαρβονικός πυρήνας	500 microns
4 ^ο επίπεδο : Πολυκαρβονική επικάλυψη	50 microns

Παρακάτω παραθέτουμε φωτογραφίες από όλες τις εκδόσεις των καρτών που έχουμε αναφέρει, ώστε να έχετε μια οπτική γνώση των προτεινόμενων σχεδίων.





Στο επόμενο κεφάλαιο αναπτύσσουμε την ηλεκτρονική σχεδίαση της κάρτας με το chip που θα ενσωματώνει.

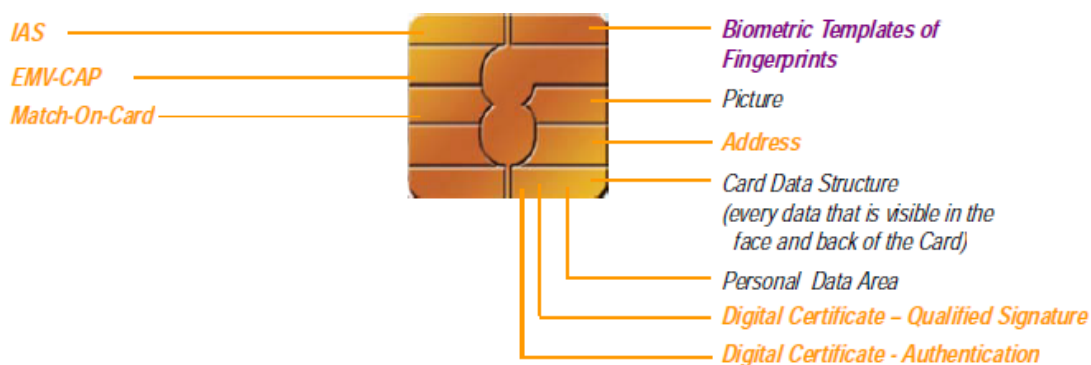
4ο Κεφάλαιο : Ηλεκτρονική σχεδίαση της κάρτας του πολίτη

Σχεδιασμός της ηλεκτρονικής κάρτας του πολίτη. Αναλύονται οι τεχνολογίες έξυπνων καρτών και RFID. Επιλέγεται η τεχνολογία χρήσης καθώς και αναλύονται τα συστήματα υποστήριξης. Περιγράφεται η δομή , το είδος και η ποσότητα των δεδομένων που θα μπορεί να φέρει η κάρτα.

4.2 Το CHIP

Οι κύριες εφαρμογές που θα φιλοξενούνται στο chip της κάρτας θα είναι:

- **IAS** – εφαρμογή υπεύθυνη για τη διαχείριση της αυθεντικότητας της κάρτας, την ηλεκτρονική υπογραφή και την πρόσβαση στα δεδομένα της κάρτας,
- **ENV-CAP** – εφαρμογή η οποία θα παρέχει στιγμιαίο κωδικό ασφαλείας για εναλλακτικό κανάλι αυθεντικοποίησης (π.χ. τηλεφωνία),
- **Match-on-Card** – εφαρμογή η οποία επαληθεύει βιομετρικά δεδομένα και τα δακτυλικά αποτυπώματα (μέσα στο chip)

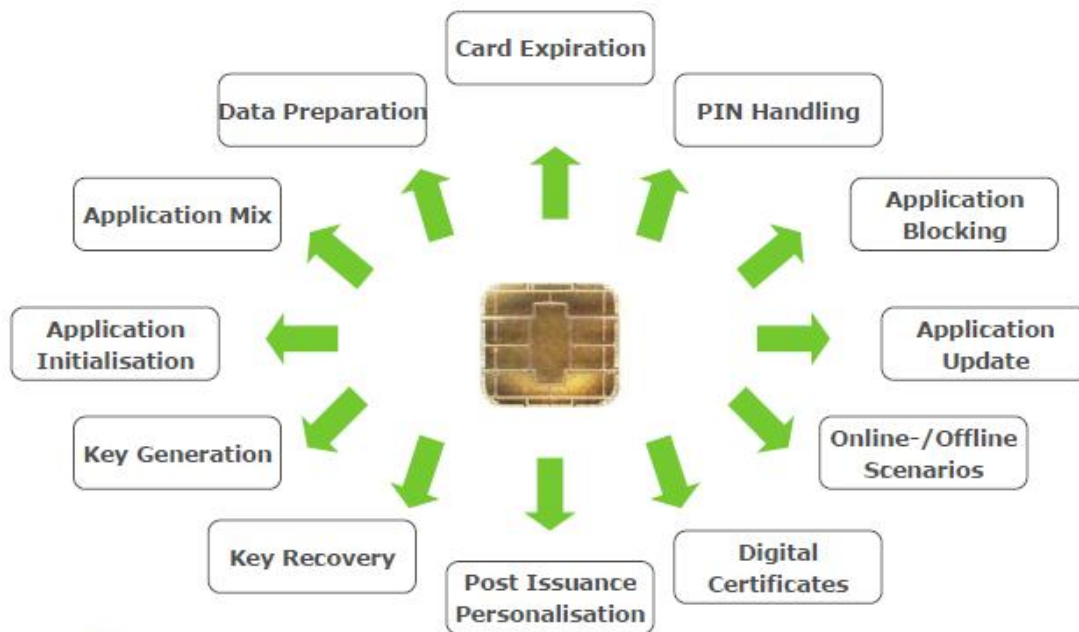


Στην παραπάνω εικόνα, με πορτοκαλί χρώμα εμφανίζονται οι εφαρμογές οι οποίες προστατεύονται μέσω pin.

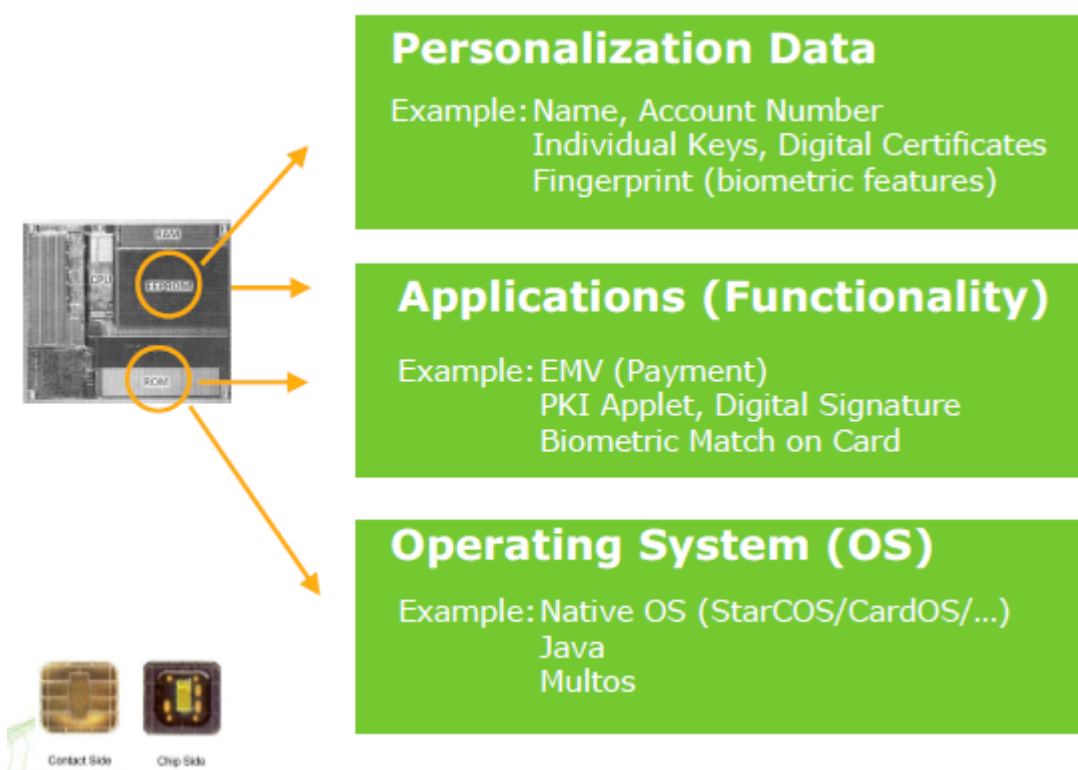
Με μαύρο χρώμα οι εφαρμογές που έχουν προσπέλαση από όλους.

Με μωβ τα δεδομένα – εφαρμογές που δεν είναι διαθέσιμα. [16]

Μία τέτοια κάρτα έχει πολλές πτυχές και υποστηρίζει πολλές εφαρμογές [42] και φυσικά πολλά στοιχεία.



Όπως φαίνεται και παραπάνω, ένα chip φέρει πολλαπλά αντικείμενα δεδομένων τα οποία χρήζουν διαχείρισης. Μπορεί να φέρει προσωπικά δεδομένα (όνομα, κλειδιά, αριθμό λογαριασμού, αποτύπωμα), εφαρμογές και λειτουργίες (EMV, payment, PKI Applet, Βιομετρικό στοιχείο επαλήθευσης πάνω στην κάρτα), λειτουργικό σύστημα (CardOS, Java, Multos).



4.3 Διασύνδεση κάρτας και συστημάτων

Η Ευρωπαϊκή κάρτα του πολίτη, όπως έχουμε αναφέρει [44] ορίζεται με το στάνταρ ECC (15480-1/-4). Περιέχει τέσσερα βασικά μέρη, το μέρος 1 το οποίο περιέχει φυσικά, ηλεκτρικά χαρακτηριστικά και χαρακτηριστικά μεταφοράς, το μέρος 2 που περιέχει λογικές δομές δεδομένων, μέρος 3 που περιέχει διαλειτουργικότητα της κάρτας με τη χρήση διασύνδεσης μέσω εφαρμογής και το μέρος 4 που περιέχει προφίλ.

Στην Γερμανία η eID είναι ένα ηλεκτρονικό chip το οποίο αποτελεί το λειτουργικό σύστημα και λειτουργεί σε τρεις διαφορετικές εφαρμογές: ePassport, eID και QeS. Η κάρτα λειτουργεί σε κατάσταση από απόσταση (contactless). Οι εντεταμένοι μηχανισμοί ασφάλειας είναι το PACE αντί του BAC (basic access control), EAC 2.0 πριν την πιστοποίηση του chip κλπ

Οι τεχνολογίες που χρησιμοποιούνται για τη διασύνδεση είναι [44]:

A) Ανέπαφη, B) Υβριδική κάρτα με δύο chips και Γ) Διπλής διασύνδεσης με ένα chip.

A – Ανέπαφη

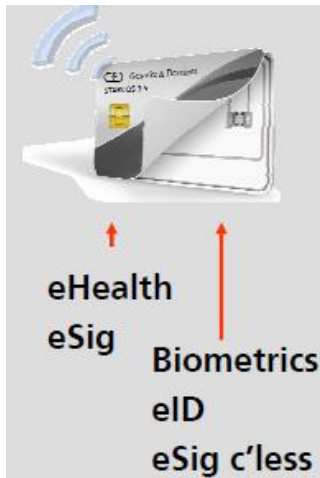
Η ανέπαφη διασύνδεση έχει λιγότερη επίδραση του περιβάλλοντος για τους αναγνώστες, υψηλότερη ανθεκτικότητα των καρτών, επαναχρησιμοποίηση των υφιστάμενων ηλεκτρονικών διαβατηρίων και της υποδομής κάρτας μεταναστών, υψηλούς ρυθμούς δεδομένων και τελευταία λέξη της τεχνολογίας.



B – Υβριδική τεχνολογία

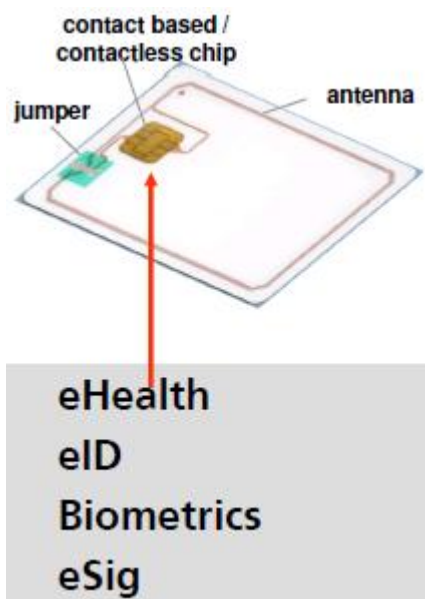
Η υβριδική τεχνολογία έχει το πλεονέκτημα ότι υπάρχει φυσικός διαχωρισμός των chips λειτουργίας. Αυτό είναι σημαντικό για την ασφάλεια. Ευέλικτο στο να χρησιμοποιηθεί ανέπαφη αλλά και εξ' επαφής υποδομή τεχνολογίας. Υπάρχει μακροπρόθεσμη και υψηλής παραγωγής υποστήριξη. Κανένας περιορισμός σε μοναδικούς προμηθευτές. Υψηλή ευελιξία λόγω των δύο chip και γρηγορότερη

δείσδυση στην αγορά. Λίγο υψηλότερο κόστος λόγω δύο chip αλλά φθηνότερα λειτουργικά.



Γ – Τεχνολογία διπλής διασύνδεσης

Ενώ το πλεονέκτημα είναι ότι απαιτείτε μόνο ένα chip, τα μειονεκτήματα είναι η κλασική τεχνολογία, η μικρή διάρκεια ζωής της κάρτας η οποία ενδέχεται να είναι και κάρτα οδήγησης.



Συνεπώς όλα τα συστήματα είναι συμβατά με τα Ευρωπαϊκά στάνταρντ. Το ανέπαφο εργαλείο είναι παρόμοιο με το ECC προφίλ. Το στοιχείο επαφής στην υβριδική ή στην ανεξάρτητη κάρτα με το μικρό επεξεργαστή CC EAL 4+ είναι πιστοποιημένο για εφαρμογές ηλεκτρονικής υγείας (EHIC, ψηφιακή υπογραφή), όπως στην Αυστρία, Γερμανία και στην Ελβετία.

4.4 Το μοντέλο του συστήματος υποστήριξης και αρχιτεκτονικής της κάρτας[16].

Όπως έχουμε αναφέρει, η κάρτα πρέπει να υποστηρίζεται από τα παρακάτω συστήματα:

Το σύστημα κύκλου ζωής της κάρτας, το οποίο είναι υπεύθυνο για την καταχώρηση και την ανανέωση καρτών, την ανάκληση κάρτας, την πιστοποίηση κλπ. Το σύστημα αυτό θα υποστηρίζει διάφορες συσκευές – εξοπλισμό βιομετρικών δεδομένων. Θα μπορεί να υποστηρίζει μηχανήματα διαφόρων κατασκευαστών και διαφορετικών τύπων. Θα αναπτυχθεί και θα βασίζεται στο Web, θα επιτρέπει online και Offline εργασίες ενώ θα υπάρχει 24/7 γραφείο υποστήριξης.

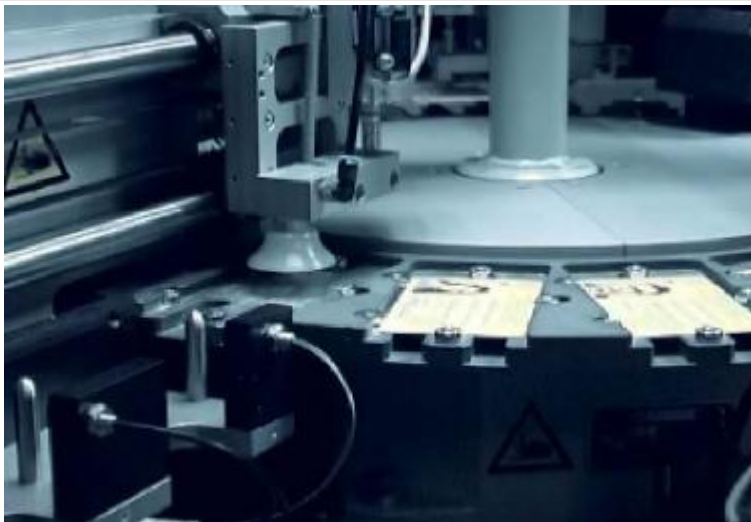
Το σύστημα εξατομίκευσης της κάρτας, το οποίο είναι υπεύθυνο για την φυσική εξατομίκευση της κάρτας, την παραλαβή της κάρτας από τον κάτοχο, την παραλαβή pin & puk κλπ. Η φυσική εξατομίκευση έχει να κάνει με τα δεδομένα, τις εφαρμογές εγγραφής δεδομένων στο chip. Αλληλεπιδρά με το πλαίσιο κύκλου ζωής της κάρτας για τη συλλογή:

- Από το σύστημα πληροφοριών κύκλου ζωής, δεδομένα που αφορούν την εξατομίκευση της κάρτας και αποθήκευσης στο chip,
- Από το EMV-CAP σύστημα, παραμέτρους για την εφαρμογή κωδικού μιας χρήσης, σε κάθε κάρτα,
- Από το PKI, πιστοποιητικά προς αποθήκευση στο chip,

Επιπλέον είναι υπεύθυνο να επικοινωνεί με το σύστημα παράδοσης, το οποίο ορίζεται ως:

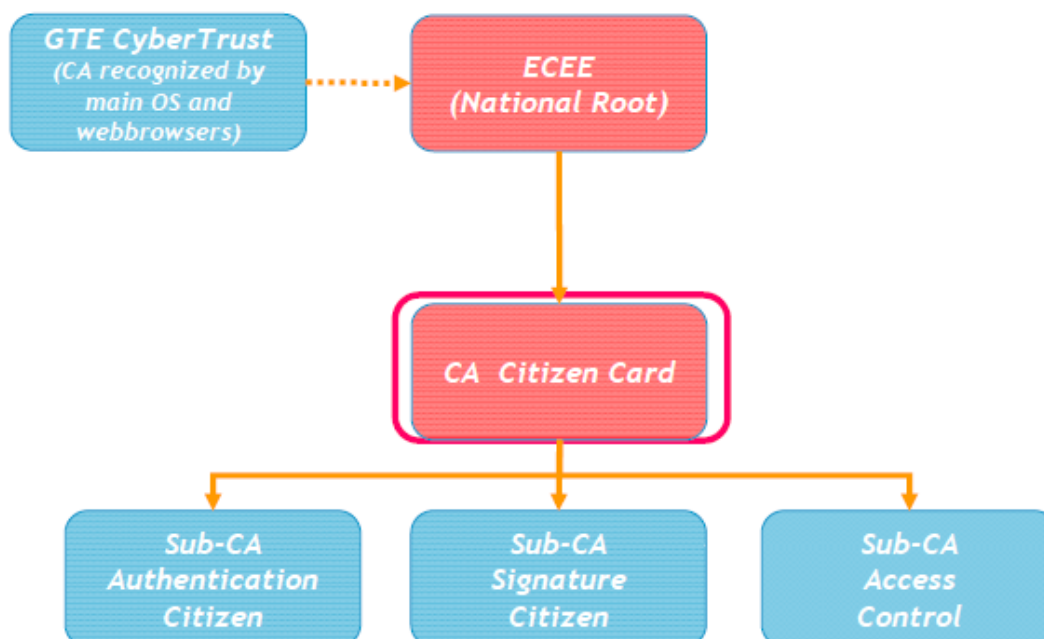
- Παράδοση κάρτας,
- Παράδοση επιστολών με PIN στις διευθύνσεις των αποδεκτών.

Επιπλέον το σύστημα αυτό θα είναι το γενικός αρμόδιο για τον έλεγχο παραγωγής και ποιότητας των καρτών.

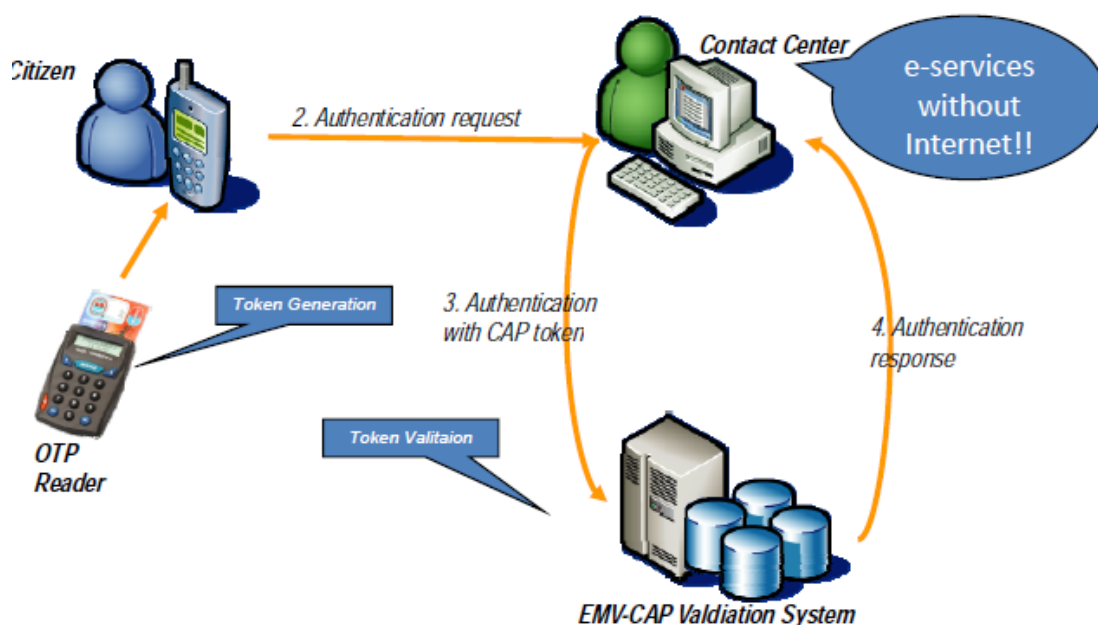


Το **PKI**, το οποίο είναι υπεύθυνο για την ψηφιακή πιστοποίηση.

Η αρχή πιστοποίησης, αποτελείται από υποδιεργασίες – υποφορείς , οι οποίοι φαίνονται στο παρακάτω διάγραμμα:



EMV-CAP σύστημα επικύρωσης, υπεύθυνο για την κεντρική επικύρωση της ταυτότητας του πολίτη, με συγκεκριμένα στοιχεία που έχουν δημιουργηθεί στο chip της κάρτας με την εφαρμογή EMV-CAP. Το σύστημα αυτό επικυρώνει μία CAP συναλλαγή (μία ακολουθία από ψηφία), τα οποία δημιουργούνται από την EMV-CAP εφαρμογή στην κάρτα.

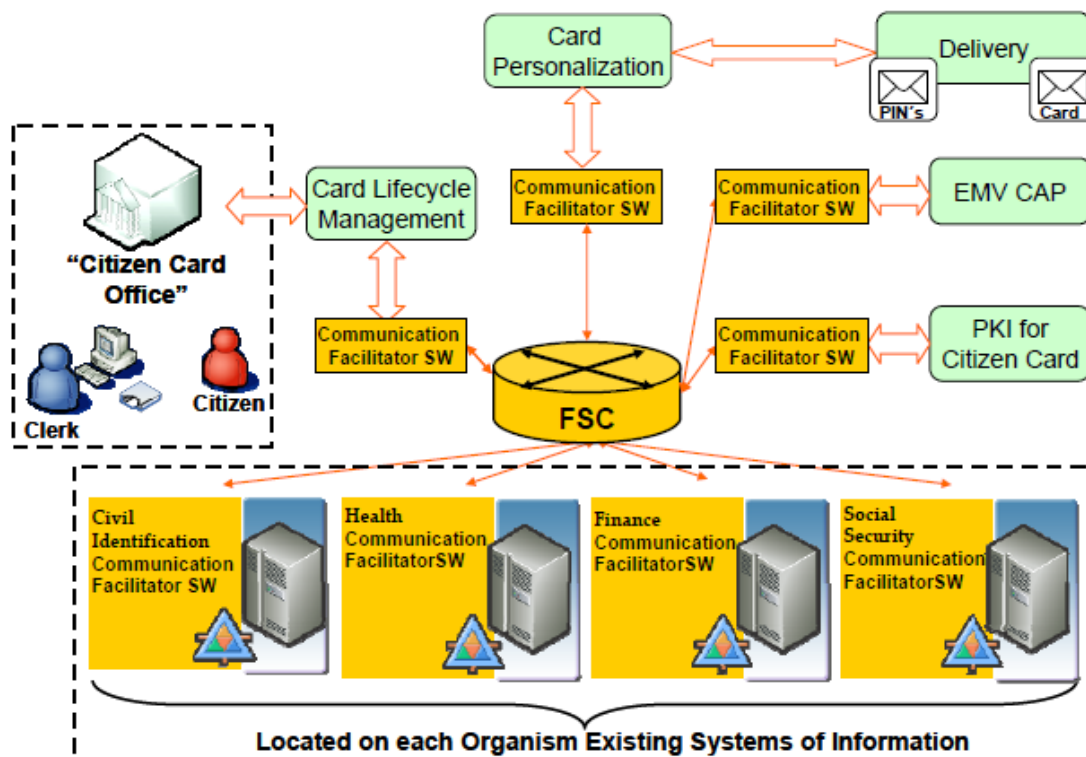


Συστήματα δημόσιων φορέων, τα οποία αποτελούν υπάρχοντα και νέα συστήματα δημόσιων οργανισμών, τα οποία περιέχουν δεδομένα των πολιτών.

4.5 Πλατφόρμα πλαισίου διαλειτουργικότητας [16].

Το σύστημα πλαισίου διαλειτουργικότητας, είναι υπεύθυνο για :

- **Τεχνική, συντακτική και σημασιολογική** ολοκλήρωση των συστημάτων δημόσιας διοίκησης,
- **Ομοσπονδία ταυτοποίησης**, διασφαλίζοντας ότι κάθε οργανισμός διατηρεί μόνο τα τομεακά στοιχεία του πολίτη και επιτρέπει τις διυπουργικές διεργασίες,
- **Ηλεκτρονικό έλεγχο ταυτότητας και εξουσιοδότησης του πολίτη**,
- **Συντονισμό διεργασιών**,
- **Ασφάλεια και επιθεώρηση**.



4.6 Συμπεράσματα – Εφαρμογή & Επιλογές

Συνεπώς λοιπόν η δική μας επιλογή είναι η κατασκευή **υβριδικής κάρτας** με chip επαφής αλλά και chip ανέπαφης λειτουργίας, όπου προσφέρεται η μεγαλύτερη ασφάλεια. Η κάρτα αυτή θα υποστηρίζεται από όλα τα παραπάνω συστήματα ώστε να διασφαλίζεται μέχρι την παράδοση στον κάτοχο και πλέον για τη χρήση της ίδιας της κάρτας η ασφάλεια. Αυτό θα φέρει την εμπιστοσύνη στον πολίτη για τη χρήση της.

Υιοθετούμε λοιπόν όλο το σύστημα κύκλου ζωής της κάρτας, το σύστημα εξατομίκευσης, PKI, EMV-CAP, και φυσικά όλο το πλαίσιο διαλειτουργικότητας της κάρτας.

Ειδικότερα στο chip έχουμε:

- Πιστοποιητικό ταυτότητας και συναφή κλειδιά,
- Πιστοποιητικό υπογραφής και συναφή κλειδιά,
- Πιστοποιητικό του εκδότη της αρχής πιστοποίησης,
- Δεδομένα υπαγωγής του πολίτη,
- Εικόνα της φωτογραφίας,
- Εικόνα την χειρόγραφης υπογραφής,
- Πρότυπο δακτυλικού αποτυπώματος,
- Εφαρμογή ταυτοποίησης πάνω στην κάρτα.

CC EAL 5+

CC EAL 4+

CWA 14890

Αλλαγές χρωματισμών

Ανέπαφο chip
ανιχνεύσιμο μόνο
με υπέρυθρο φως

Κρυπτογραφημένο
chip
με ψηφιακή υπογραφή
με κρυπτ. δεδομένα
με βιομετρικά στοιχεία

Φωτογραφία με
βιομετρικά στοιχεία
όπως στο
διαβατήριο

Εκτύπωση σε
επίπεδο background
της Ακρόπολης για
ασφάλεια

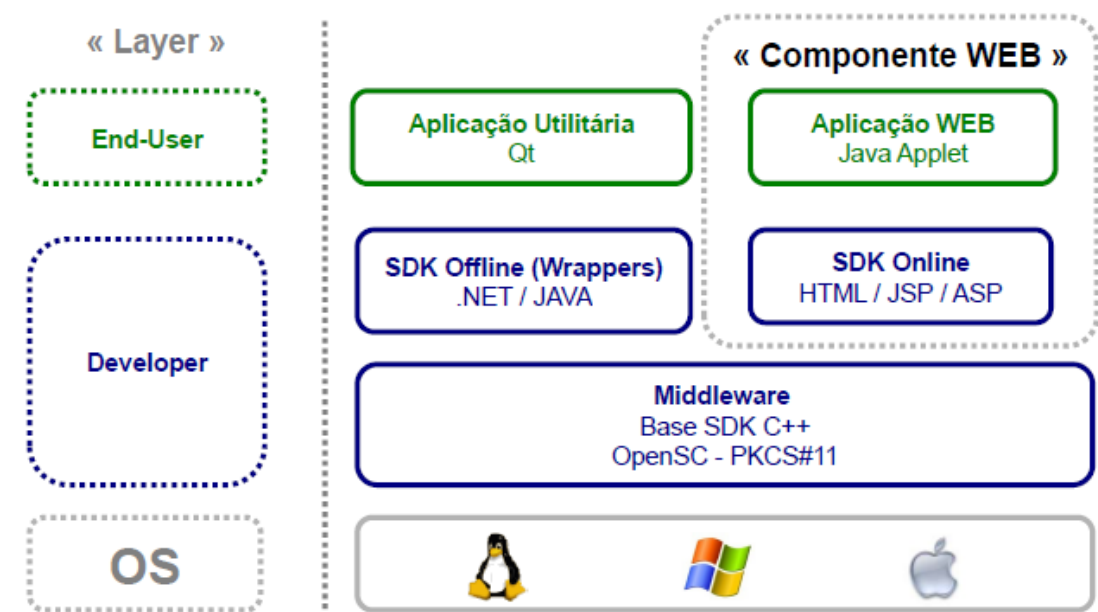
Ολόγραμμα
ασφαλείας με
επικόλληση 100μ

5ο Κεφάλαιο : Ανάπτυξη λογισμικού

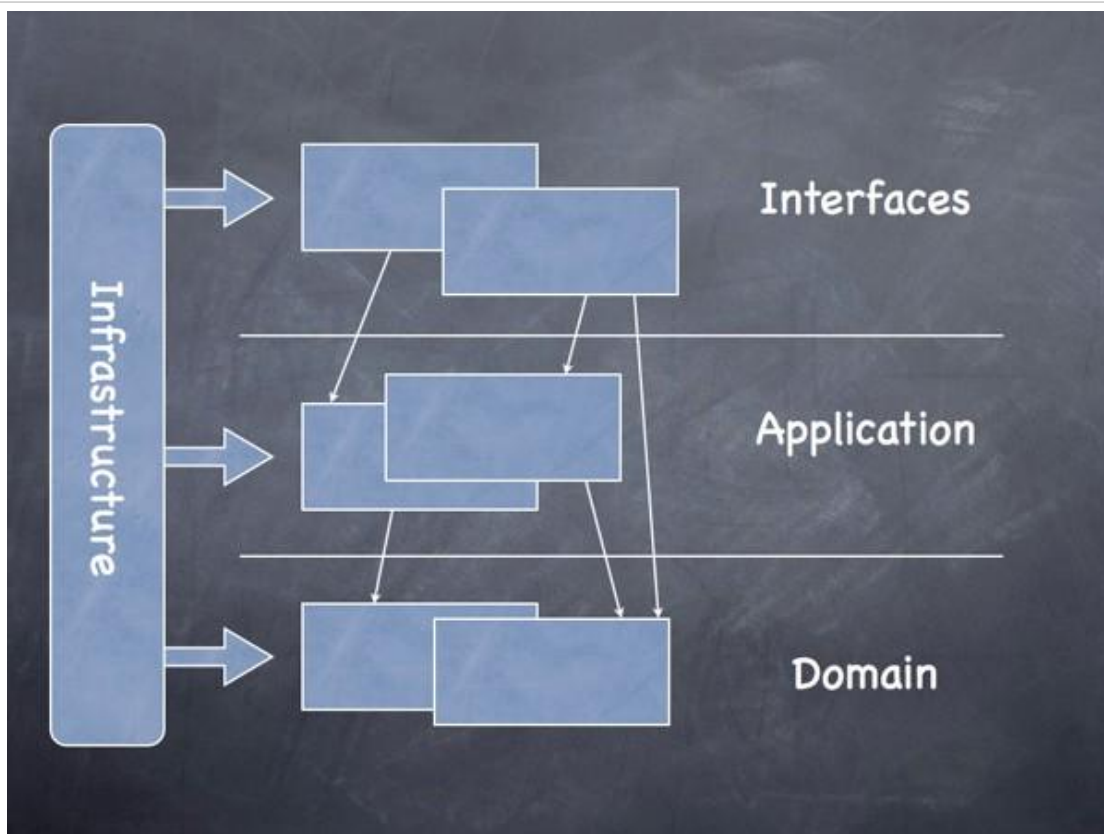
Λογισμικό διαχείρισης. Στο συγκεκριμένο κεφάλαιο αιτιολογείται η χρήση συγκεκριμένων τεχνολογιών λογισμικού για την ανάπτυξη ενός τέτοιου μητρώου διαχείρισης πολιτών. Αναφέρονται όλες οι δυνατές πλατφόρμες ανάπτυξης και ολοκλήρωσης του έργου. Επιπλέον αναπτύσσεται demo λογισμικό για την εφαρμοσμένη δοκιμή της διατριβής.

5.1 Τα επίπεδα από το Server μέχρι τον τελικό χρήστη.

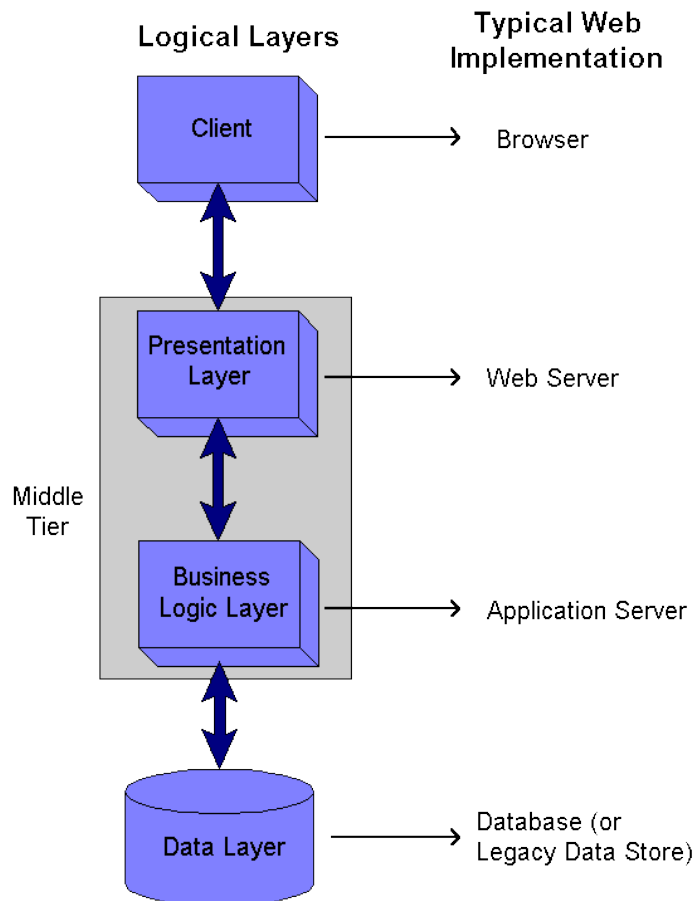
Τα επίπεδα μεταξύ των servers και του τελικού χρήστη, όπως φαίνεται και στο παρακάτω σχεδιάγραμμα, είναι δύο. Το ένα είναι το βασικό πηγαίο kit ανάπτυξης της C++ και το δεύτερο είναι τεχνολογίες .net και java για εφαρμογές και html, jsp, asp για σελίδες. Εδώ θα καταλήξουμε ακολουθώντας το συλλογισμό που θα αναφέρουμε στις επόμενες παραγράφους.



Στην παρούσα εφαρμογή βέβαια, κάτι το οποίο δεν λαμβάνουμε εμείς υπόψη, είναι ότι σε κρατικό επίπεδο, θα μπορούσε να ελέγχεται το domain που συνδέεται για τις προσφερόμενες υπηρεσίες. Δηλαδή η κάρτα για παράδειγμα, σε περίπτωση αίτησης αλλαγής προσωπικών δεδομένων, θα μπορούσε να δίνει πρόσβαση μόνο στο κρατικό domain όπως το gov.gr και σε κανένα άλλο. Σε άλλα domains θα μπορούσε η κατάσταση να είναι read mode μόνο. Εκτός από την κάρτα θα μπορούσε για μεγαλύτερη ασφάλεια να ελέγχεται το domain και από τις ίδιες τις εφαρμογές. Αυτό θα είχε ως συνέπεια οι εφαρμογές να μην αλληλεπιδρούν με την κάρτα όταν η αίτηση (request) γίνεται από μη αναγνωρίσιμο domain.

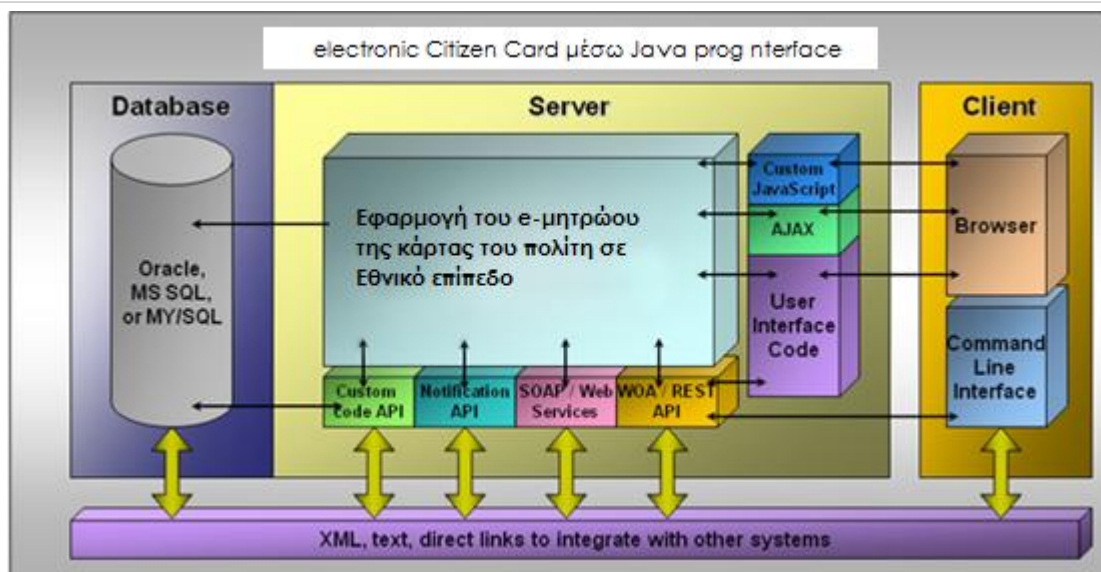


Αφήνοντας το επίπεδο της ασφάλειας με τη χρήση και του domain, μπορούμε τώρα να δούμε όλα τα προγραμματιστικά επίπεδα, που πρέπει να λάβουμε υπόψη για την υλοποίηση της εφαρμογής. Επειδή όλα στηρίζονται στην ανάπτυξη μητρώου πολιτών, χρειαζόμαστε μία ασφαλής και σταθερή βάση δεδομένων η οποία να μπορεί να ανταπεξέλθει σε εφαρμογή διαδικτύου. Οι πρώτες σχεσιακές βάσεις δεδομένων σε server mode που μας έρχονται στο μυαλό είναι η Oracle, η Microsoft SQL και η MySQL. Η MySQL αποκλείεται για λόγους αξιοπιστίας σε σχέση με την Microsoft SQL και την Oracle. Οποιαδήποτε από τις προηγούμενες δύο θα μπορούσαν να υποστηρίξουν την ανάπτυξη της εφαρμογής της κάρτας του πολίτη και της ηλεκτρονικής διακυβέρνησης. Η επιλογή της βάσης είναι κάτι το οποίο θα εξαρτηθεί και από την ευκολία γεφύρωσης των ήδη υπάρχοντων μητρώων στην Ελλάδα, κάτι το οποίο δεν είμαστε σε θέση να το γνωρίζουμε όπως η ΓΓΠΣ. Εμείς για χάριν ευκολίας ανάπτυξης του μητρώου επιλέξαμε την Microsoft SQL την οποία και εγκαταστήσαμε, με το δωρεάν λογισμικό Ms SQL Express 2008.



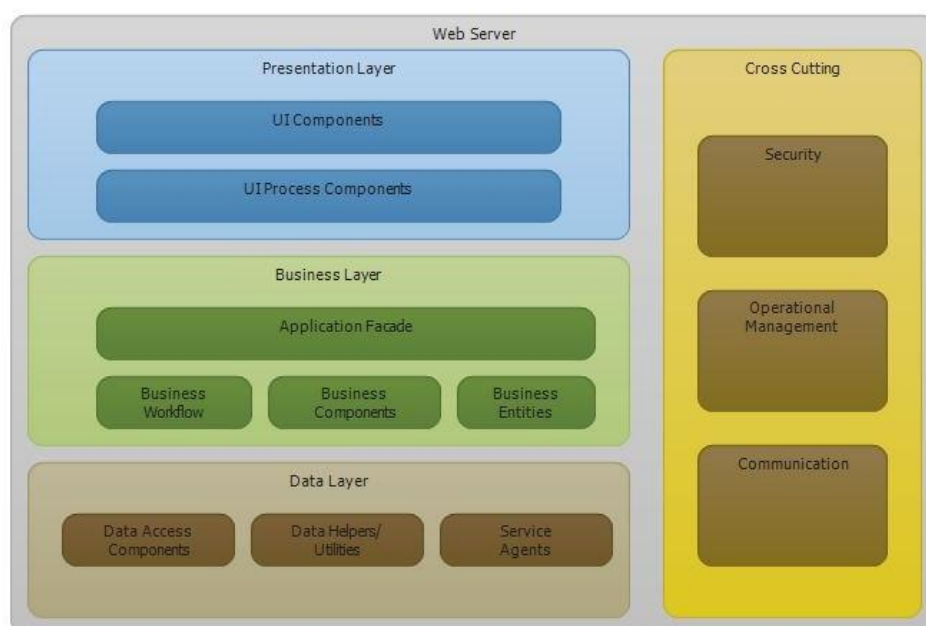
Το επόμενο επίπεδο είναι ο application server όπου εδώ θα μπορούσαμε να επιλέξουμε μεταξύ Java & .net. Η java θα ήταν η καλύτερη επιλογή, λόγω του ότι είναι cross platform, τα στάνταρντ τα έχουν υιοθετήσει όλοι οι οίκοι λογισμικού διαδικτύου και έχει εφαρμογές σε όλους τους υπολογιστές, κινητά, λειτουργικά συστήματα κλπ. Εμείς όμως για λόγους καθαρά γνώσεων προγραμματισμού επιλέξαμε το .net framework της Microsoft λόγω σχετικής γνώσης και περιβάλλοντος Visual Studio C# για την ανάπτυξη της εφαρμογής. Σε κάθε όμως άλλη περίπτωση θα συνιστούσαμε ανεπιφύλακτα Java (jre & jdk) και Java γλώσσα προγραμματισμού για την υλοποίηση της εφαρμογής στο διαδίκτυο.

Σε αυτή την περίπτωση η ανάπτυξη εφαρμογής της κάρτας του πολίτη θα ακολουθούσε τα επίπεδα του παρακάτω διαγράμματος:



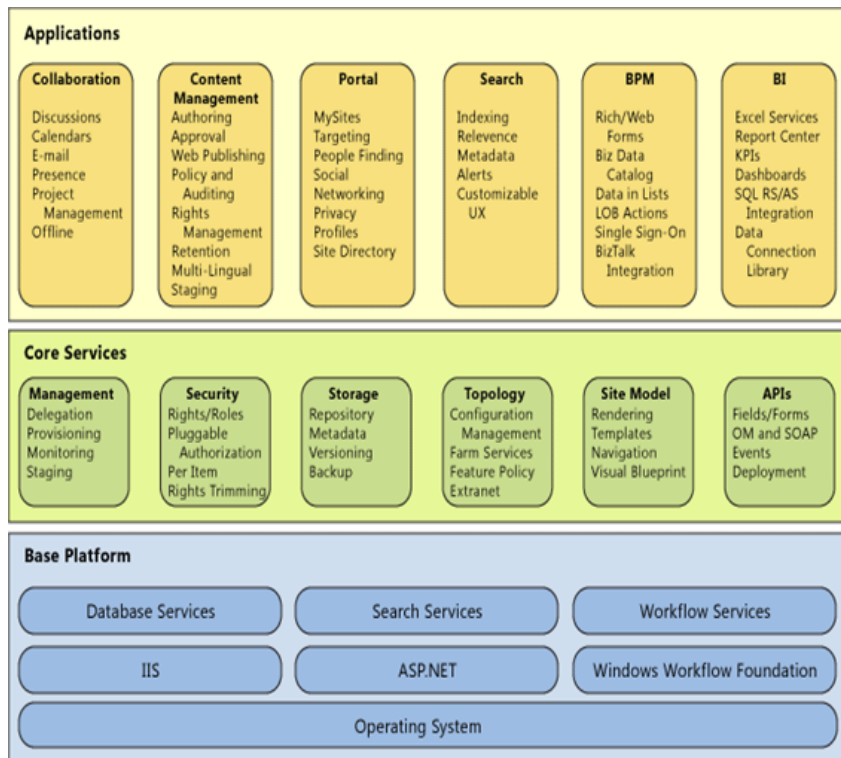
5.2 Εργαλεία ανάπτυξης λογισμικού e-μητρώου

Στην παρούσα εφαρμογή, αναπτύξαμε το μητρώο πολιτών σε Microsoft SQL Database 2008. Το λογισμικό αναπτύχθηκε σε Visual C#, μέσω του Visual Studio 2010 express και τεχνολογία .net framework 3.5. Το σύστημα σήμερα φιλοξενείται σε ένα Windows Server 2003 στη διεύθυνση <http://eid.vezeris.gr/>. Για να το δείτε καλύτερα χρησιμοποιείτε Internet Explorer 8 ή Internet Explorer 9 με συμβατότητα. Τα επίπεδα μιας τέτοιας τεχνολογίας εμφανίζονται στο παρακάτω διάγραμμα της Microsoft.

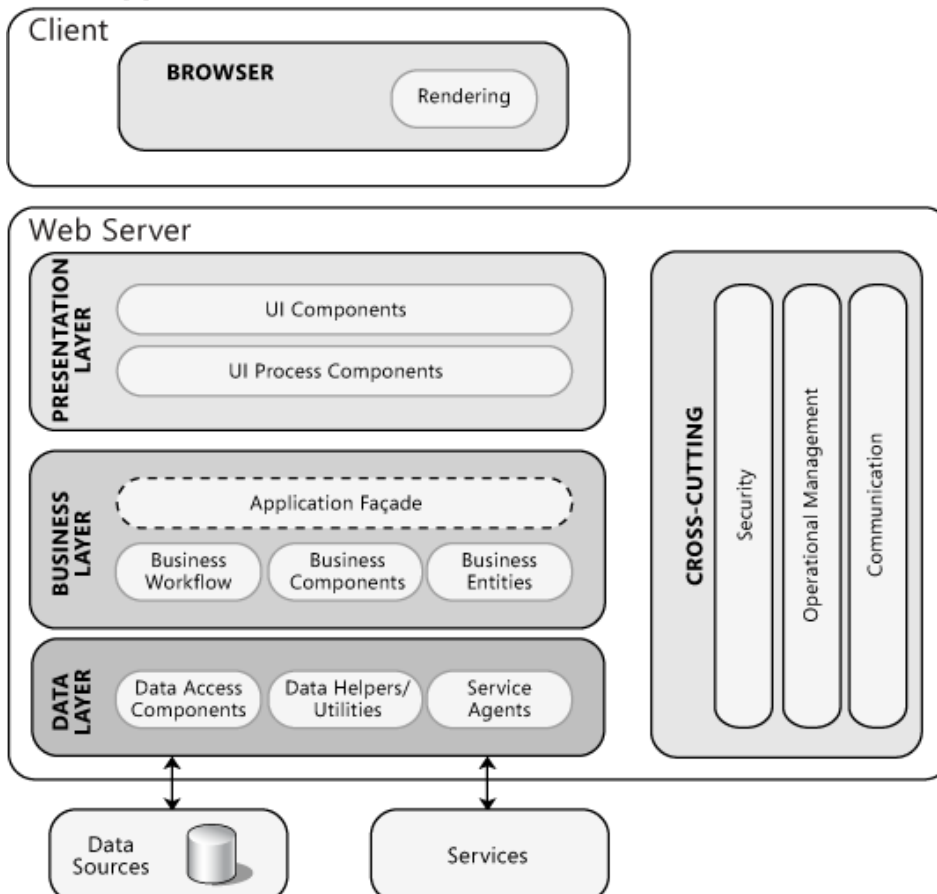


Source: Microsoft Application Architecture Guide, 2nd Edition.
Refer to "Chapter 21: Designing Web Applications" for more information.
URL: <http://msdn.microsoft.com/en-us/library/ee658099.aspx>

Ασφάλεια εφαρμογών σε περιβάλλον .net

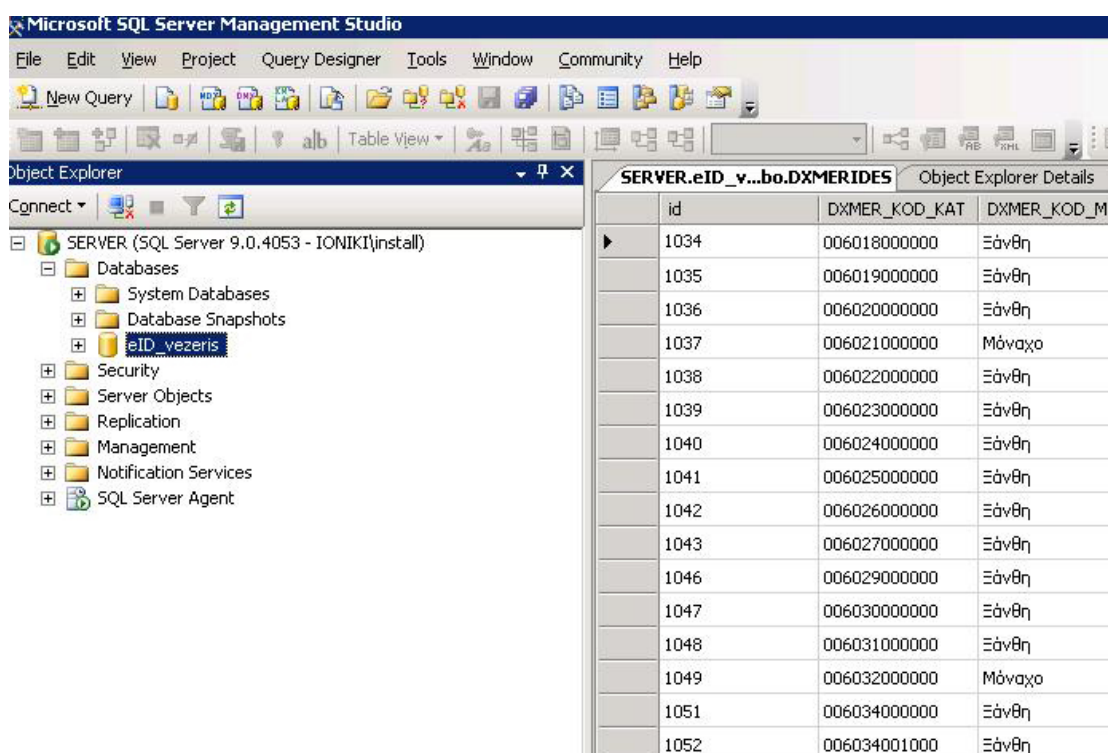


Web Application



5.3 SQL Server Express 2008.

Χρησιμοποιήθηκε δωρεάν λογισμικό της Microsoft και συγκεκριμένα ο SQL Server Express 2008, ο οποίος έχει την ίδια μηχανή για τη βάση δεδομένων με τον κανονικό SQL Server, με μόνο περιορισμό τα 10Gb ανά βάση δεδομένων αποθηκευτικό χώρο. Εμάς μας κάλυπτε πλήρως η έκδοση αυτή όπου επίσης συνεργάζεται με το Visual Studio Express Edition Web Development (και τη C#). Υποστηρίζει τεχνολογία ASP .net και οι ρυθμίσεις όλες καταχωρούνται στο web.config στο root directory του site της εφαρμογής.

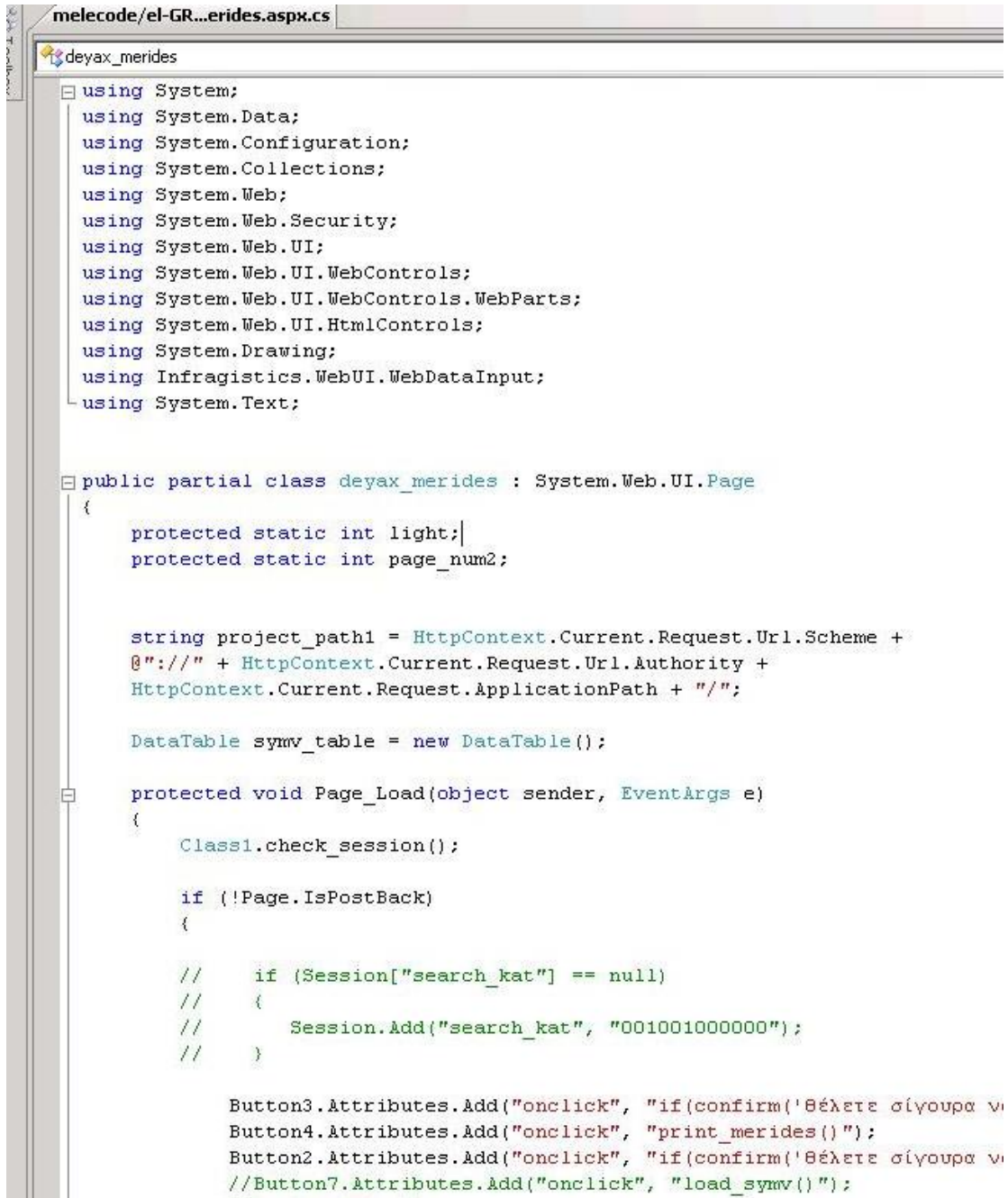


The screenshot shows the Microsoft SQL Server Management Studio interface. The Object Explorer on the left displays the server structure for 'SERVER (SQL Server 9.0.4053 - IONIKI\install)', including Databases, Security, Server Objects, Replication, Management, Notification Services, and SQL Server Agent. The 'eID_vezeris' database is selected. The main window shows a table view for 'SERVER.eID_v...bo.DXMERIDES' with the following data:

id	DXMER_KOD_KAT	DXMER_KOD_M.
1034	006018000000	Ξάνθη
1035	006019000000	Ξάνθη
1036	006020000000	Ξάνθη
1037	006021000000	Μόναχο
1038	006022000000	Ξάνθη
1039	006023000000	Ξάνθη
1040	006024000000	Ξάνθη
1041	006025000000	Ξάνθη
1042	006026000000	Ξάνθη
1043	006027000000	Ξάνθη
1046	006029000000	Ξάνθη
1047	006030000000	Ξάνθη
1048	006031000000	Ξάνθη
1049	006032000000	Μόναχο
1051	006034000000	Ξάνθη
1052	006034001000	Ξάνθη

5.4 Visual Web Developer 2010 Express

Χρησιμοποιήθηκε δωρεάν λογισμικό της Microsoft και συγκεκριμένα το Visual Web Developer Express 2010, το οποίο ενσωματώνει υποστήριξη ASP .net & C#. Επίσης για τις εκτυπώσεις χρησιμοποιήθηκε το Crystal Reports for Visual Studio το οποίο ενσωματώνεται στο περιβάλλον.



```
melecode/el-GR...erides.aspx.cs
de yax_merides

using System;
using System.Data;
using System.Configuration;
using System.Collections;
using System.Web;
using System.Web.Security;
using System.Web.UI;
using System.Web.UI.WebControls;
using System.Web.UI.WebControls.WebParts;
using System.Web.UI.HtmlControls;
using System.Drawing;
using Infragistics.WebUI.WebDataInput;
using System.Text;

public partial class de yax_merides : System.Web.UI.Page
{
    protected static int light;
    protected static int page_num2;

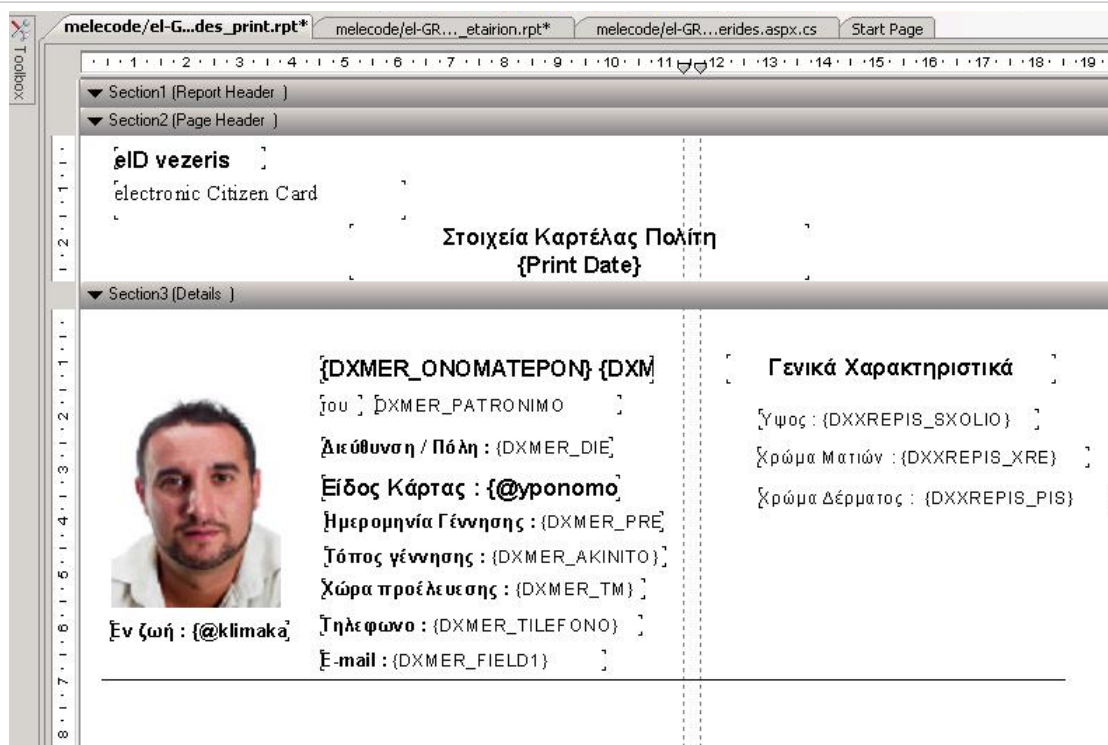
    string project_path1 = HttpContext.Current.Request.Url.Scheme +
@":///" + HttpContext.Current.Request.Url.Authority +
HttpContext.Current.Request.ApplicationPath + "/";

    DataTable symv_table = new DataTable();

    protected void Page_Load(object sender, EventArgs e)
    {
        Class1.check_session();

        if (!Page.IsPostBack)
        {
            // if (Session["search_kat"] == null)
            // {
            //     Session.Add("search_kat", "001001000000");
            // }

            Button3.Attributes.Add("onclick", "if(confirm('Θέλετε σίγουρα να...')){print_merides()}");
            Button4.Attributes.Add("onclick", "print_merides()");
            Button2.Attributes.Add("onclick", "if(confirm('Θέλετε σίγουρα να...')){load_symv()}");
            //Button7.Attributes.Add("onclick", "load_symv()");
        }
    }
}
```



melecode/el-G...des_print.rpt* melecode/el-GR..._etairion.rpt* melecode/el-GR...erides.aspx.cs Start Page

Section1 (Report Header)

Section2 (Page Header)

elD vezeris
electronic Citizen Card

Στοιχεία Καρτέλας Πολίτη
{Print Date}

Section3 (Details)

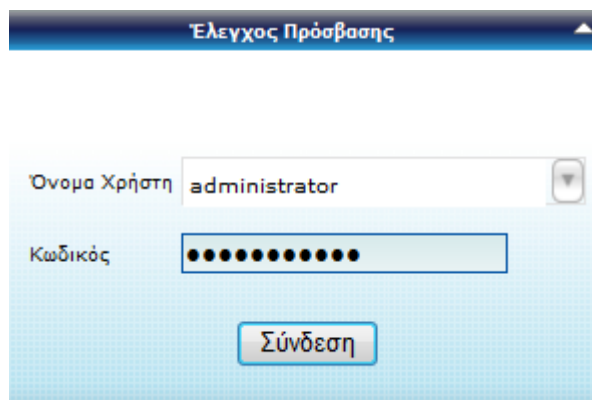
{DXMER_ONOMATEPON} {DXM
του {DXMER_PATRONIMO }
Διεύθυνση / Πόλη : {DXMER_DIE
Είδος Κάρτας : {@gyronomo
Ημερομηνία Γέννησης : {DXMER_PRE
Τόπος γέννησης : {DXMER_AKINITO}
Χώρα προέλευσης : {DXMER_TM}
Εν ζωή : {@klimaka
Τηλεφωνο : {DXMER_TILEFONO}
E-mail : {DXMER_FIELD1}

Γενικά Χαρακτηριστικά

Υψος : {DXXREPIS_SXOLIO}
Χρώμα Ματιών : {DXXREPIS_XRE}
Χρώμα Δέρματος : {DXXREPIS_PIS}

5.5 Το λογισμικό

Το λογισμικό, λόγω του ότι χρησιμοποιεί controls της Microsoft μπορεί να δοκιμαστεί σε Internet Explorer 8 ή 9 με επιλογή συμβατότητας. Στην πρώτη οθόνη εμφανίζεται η κάρτα σύνδεσης στο σύστημα όπου θεωρούμε ότι στο μητρώο μόνο εξουσιοδοτημένοι χρήστες μπορούν να συνδεθούν. Το λογισμικό κατασκευάστηκε ώστε να δείξει τις δυνατότητες και τα οφέλη που μπορεί να αποκομίσει το κράτος και οι πολίτες με τη χρήση και τη λειτουργία του. Θα παραθέσουμε εδώ εικόνες με τις δυνατότητες του προγράμματος ώστε ο αναγνώστης – μελετητής να πάρει μια ιδέα για τις ικανότητες αλλά και δυνατότητες ενός τέτοιου ηλεκτρονικού μητρώου.



Έλεγχος Πρόσβασης

Όνομα Χρήστη administrator

Κωδικός

Σύνδεση

Η γενική φιλοσοφία του προγράμματος είναι ότι όλα στρέφονται γύρω από τον πολίτη (πολιτοκεντρικό σύστημα ανάπτυξης της βάσης δεδομένων). Αυτό σημαίνει ότι το ζητούμενο κάθε φορά είναι ο ορισμός του ΑΜΚΑ (eID) πάνω στον οποίο θα στρέφονται όλες οι λειτουργίες. Ο χρήστης λοιπόν του συστήματος θέλει να βρει τον ζητούμενο πολίτη ώστε να εφαρμόσει τις λειτουργίες που θέλει εγγραφής / ανάγνωσης. Στη συγκεκριμένη περίπτωση αναζητούμε κάποιον Παπαδόπουλο.....

Βρέθηκαν 18 Πολίτες (Εν ζωή: 15 Όχι εν ζωή: 3)

Κωδικός Πολίτη	Πόλη	Ονοματεπώνυμο	Διεύθυνση	Ον. Πατρός
001008011000	Ξάνθη	ΠΑΠΑΔΟΠΟΥΛΟΣ	ΒΑΣ.ΣΟΦΙΑΣ 5	ΒΑΣΙΛΕΙΟΣ
001035000000	Ξάνθη	ΠΑΠΑΔΟΠΟΥΛΟΣ	ΒΑΣ.ΣΟΦΙΑΣ 8	ΗΛΙΑΣ
001063000000	Ξάνθη	ΠΑΠΑΔΟΠΟΥΛΟΣ	ΒΑΣ.ΣΟΦΙΑΣ 8	ΙΩΑΝΝΗΣ
001070000000	Ξάνθη	ΠΑΠΑΔΟΠΟΥΛΟΣ	ΒΑΣ.ΣΟΦΙΑΣ	ΣΠΥΡΟΣ
001151000000	Ξάνθη	ΠΑΠΑΔΟΠΟΥΛΟΥ	ΠΕΡΑ ΑΜΠΕΛΙΑ	ΕΛΕΥΘΕΡΙΑ
003058002000	Ξάνθη	ΠΑΠΑΔΟΠΟΥΛΟΣ	ΠΛΑΤΑΙΩΝ 56	ΑΛΕΞΑΝΔΡΟΣ
003084000000	Ξάνθη	ΠΑΠΑΔΟΠΟΥΛΟΣ	ΚΑΤΣΩΝΗ 14	ΙΩΑΝΝΗΣ
003096000000	Ξάνθη	ΠΑΠΑΔΗΜΗΤΡΙΟΥ	ΚΑΤΣΩΝΗ 22	ΑΝΑΣΤΑΣΙΟΣ
003112000000	Ξάνθη	ΠΑΠΑΔΟΠΟΥΛΟΣ	ΚΑΤΣΩΝΗ 54-A	ΑΝΤΩΝΙΟΣ
003113000000	Ξάνθη	ΠΑΠΑΔΟΠΟΥΛΟΣ	ΚΑΤΣΩΝΗ 56	ΓΕΩΡΓΙΟΣ
003117000000	Ξάνθη	ΠΑΠΑΔΟΠΟΥΛΟΣ	ΚΑΤΣΩΝΗ ΤΕΡΜΑ	ΑΛΕΞΑΝΔΡΟΣ

Με την επιλογή του πολίτη, εισερχόμαστε σε όλες τις εγγραφές που αφορούν αυτόν τον πολίτη και είναι καταχωρημένες στο μητρώο. Αυτές τις χωρίζουμε σε βασικές οι οποίες υπάρχουν και στο chip της κάρτας αλλά και σε δευτερεύουσες που αφορούν τις εγγραφές δευτερευόντων μητρώων από τα βασικά στοιχεία. Αυτό σημαίνει, σε ότι αφορά στα βασικά στοιχεία του πολίτη (βιομετρικά χαρακτηριστικά, διευθύνσεις κατοικίας, ηλικία, φωτογραφία, αποτυπώματα κλπ), ότι αυτά κρατούνται και αποθηκεύονται στον βασικό πίνακα του e-μητρώου.

Εύρεση	Μητρώο	Χαρακτηριστικά	Φορολογία	Ασφάλιση	Υγεία
Νέα εγγραφή Αποθήκευση Αλλαγών Εκτύπωση Διαγραφή Εγγραφή: 61 απο 999 συνολικά (Ενεργές: 844 Ανενεργές: 155) << Πρώτη Εγγραφή < Προηγ. Εγγραφή Επόμενη Εγγραφή > Τελευταία Εγγραφή :					
Αριθμός Πολίτη (Πρώην ΑΜΚΑ)		001/035/000/000			
Εν ζωή		ΝΑΙ			
Φύλο		Άρρεν			
Είδος κάρτας		Πορτοκαλί			
Επώνυμο		ΠΑΠΑΔΟΠΟΥΛΟΣ			
Όνομα		ΗΛΙΑΣ			
Πατρώνυμο		ΒΑΣΙΛΕΙΟΣ			
Διεύθυνση		ΒΑΣ. ΣΟΦΙΑΣ 8			
Πόλη		Ξάνθη			
Τηλέφωνο		2540802039			
Ημερομηνία Γέννησης		11/7/2003			
Τόπος γέννησης		Ξάνθη			
Χώρα προέλευσης		Ελλάδα			
E-mail		ant@cosmos4u.com			

Οι βοηθητικοί πίνακες του μητρώου πολιτών, είναι πλέον η φορολογία, η ασφάλιση, η υγεία, η δικαιοσύνη καπ.

Στον κεντρικό πίνακα , όπως βλέπεται στην παραπάνω εικόνα, υπάρχουν αποθηκευμένα τα βασικά στοιχεία του πολίτη, στοιχεία τα οποία βρίσκονται και πάνω στη φυσική κάρτα. Αυτά τα στοιχεία, ή ακόμα καλύτερα η επικύρωση της ύπαρξης της εγγραφής εν ζωή, αποδεικνύει και την εγκυρότητα της κάρτας του πολίτη. Στην καρτέλα των χαρακτηριστικών, όπου εκεί μπορεί να έχει π.χ. πρόσβαση μόνο η αστυνομία, υπάρχουν τα κάτωθι στοιχεία:

Φωτογραφία	Ύψος	Χρώμα Ματιών	Χρώμα δέρματος
	1.63	Μπλε	Σκουρόχρωμο

Από τη στιγμή που έχουμε το βασικό πίνακα του μητρώου, μπορούμε να «κρεμάσουμε» οποιοδήποτε δευτερέων πίνακα θέλουμε να διατηρήσουμε στην ηλεκτρονική διακυβέρνηση. Ένα σημαντικότατος τομέας είναι η φορολογία εισοδήματος. Στο e-μητρώο θα μπορούσαμε να διατηρούμε όλα τα οικονομικά στοιχεία του πολίτη, ήτοι δηλωθέντα εισοδήματα και φόροι που έχουν ή όχι ταχτοποιηθεί, κινητή και ακίνητη περιουσία, συμμετοχή σε εταιρίες καπ. Ένα δείγμα όλων αυτών εμφανίζεται παρακάτω:

Έτος εισοδήματος	Ημερομηνία Πληρωμής	Εισόδημα	Καθαρό	Φόρος	Τακτοποιημένος
2010	05-07-2011	20000	5000	4.166,67	NAI ▾
2009	07-07-2010	18000	5000	4.166,67	NAI ▾
2008	10-07-2009	16000	4000	3.333,33	NAI ▾
2007	06-07-2008	15000	3000	2.500,00	NAI ▾
2006	05-07-2007	14000	2000	1.666,67	NAI ▾
2005	06-07-2006	11000	1000	833,33	NAI ▾

Βλέπουμε στην παραπάνω εικόνα, τα φορολογικά στοιχεία του πολίτη, μέσω των οποίων απορρέουν οι εκκρεμότητες προς το κράτος ή όχι. Μόνο με τις παραπάνω εγγραφές φαίνεται ότι ο πολίτης είναι φορολογικά ενήμερος και έτσι σε καμία υπηρεσία δε θα χρειαζόταν να προσκομίσει φορολογική ενημερότητα.

Είδος	Ημερομηνία Αγοράς	Αξία αγοράς	Κυβισμός	Ισχύς	Ανάλυση
Αυτοκίνητο	2008	14000	1400	35	Ανάλυση
Μηχανάκι	2007	2000	125	2	Ανάλυση

Η κινητή περιουσία του πολίτη ήτοι άμεση εικόνα των φορολογητέων ίππων και του τέλους κυκλοφορίας.

Περιγραφή Ακινήτου	Ημερομηνία Αγοράς	Αξία Αγοράς	Εμβαδό	Διαγραφή
Εξ. Μονοκατοικία	2007	150000	82	Διαγραφή
Διαμέρισμα	2006	120000	90	Διαγραφή

Δηλώσεις ακίνητης περιουσίας.

Πλέον των παραπάνω θα μπορούσαμε να δούμε και από πού προέρχονται τα εισοδήματα του πολίτη, π.χ. η συμμετοχή του σε εταιρίες κλπ. Από αυτές τις εικόνες

καταλαβαίνουμε ότι το κράτος έχει πλήρη γνώση (και εικόνα) της κατάστασης του πολίτη, της οικονομικής επιφάνειας, των δραστηριοτήτων του κλπ.

Επωνυμία εταιρίας	Αριθμός Μητρώου Εταιρίας	Είδος Δραστηριότητας	Ημερομηνία Συμμετοχής	Ποσοστό Συμμετοχής
ΤΣΙΠΚΙΔΗΣ	031000000	ΕΜΠΟΡΙΚΗ	20-04-2007	56

Ομοίως με τη συμμετοχή του πολίτη σε εταιρία, μπορούμε να πληροφορηθούμε για την συνολική του ασφάλιση.

Ημερομηνία Εγγραφής	Ημερομηνία Διαγραφής	Έτη Ασφάλισης	Μέρες Ασφάλισης	Αριθμός Ενσήμων	Ασφαλιστικός Τομέας	Επωνυμία Εταιρίας
27-11-1971	21-07-2010	39	14116	21646	ΙΚΑ	Εταιρία Α.Ε.

Αντιλαμβάνεστε λοιπόν ότι ο υπολογισμός της σύνταξης ή η διασταύρωση πληροφοριών και έλεγχος των εταιριών (εισφοροδιαφυγές κλπ) θα μπορούν να αποτελούν παρελθόν ή να διεκπεραιώνονται ταχύτερα οι τυχόν καταγγελίες. Από τη στιγμή που θα κτιστεί η σχέση εμπιστοσύνης πολίτη – κράτους όλο αυτό το σύστημα θα λειτουργεί προληπτικά. Διότι ο έλεγχος σε τέτοιο βαθμό θα απομάκρυνε πράξης απάτης.

Θα μπορούσαμε εδώ να ολοκληρώσουμε πολλούς τέτοιους πίνακες με σχετικές με τον πολίτη πληροφορίες όπως οι ποινικές διώξεις – ποινικό μητρώο του πολίτη, σπουδές και πτυχία καπ αλλά δεν είναι αντικείμενο του παρόντος η πλήρη δημιουργία ενός πλήρους προγράμματος e-μητρώου. Ενδεικτικά έχουμε κατασκευάσει μερικούς πίνακες και έχουμε συμπληρώσει στοιχεία για να δείξουμε τις δυνατότητες και τη χρησιμότητα. Όπως είναι συμπληρωμένος ο παρακάτω πίνακας ο οποίος περιέχει στοιχεία ιατρικού ιστορικού του πολίτη.

Ημερομηνία	Ιατρείο	Ονοματεπώνυμο Ιατρού	Είδος Περιήλαψης	Αποτέλεσμα
05-07-2011	Ιατρ. Πανου	ΣΟΥΛΕΙΜΑΝ ΜΕΧΜΕΤ	Σπάσιμο	Επιτυχής
07-07-2010	Αχέπα	ΣΑΛΙΑΡΑ ΜΑΡΙΑ	Εγχείριση Αμυγδαλές	Επιτυχής
10-07-2009	Γεν. Νοσ. Ξάνθης	ΚΕΧΑΓΙΑΣ ΒΑΣΙΛΕΙΟΣ	Κάταγμα	Επιτυχής
06-07-2008	Αχέπα	ΚΟΤΤΑ ΔΙΑΜΑΝΤΩ	Γενική Εξέταση	Επιτυχής
05-07-2007	Αχέπα	ΑΣΤΡΙΔΟΥ ΑΝΔΡΟΜΑΧΗ	Εξέταση Αίματος	Επιτυχής
06-07-2006	Αχέπα	ΚΑΔΗΡ ΟΓΛΟΥ	Εξέταση ίριδας	Επιτυχής

5.6 Οι εκτυπώσεις

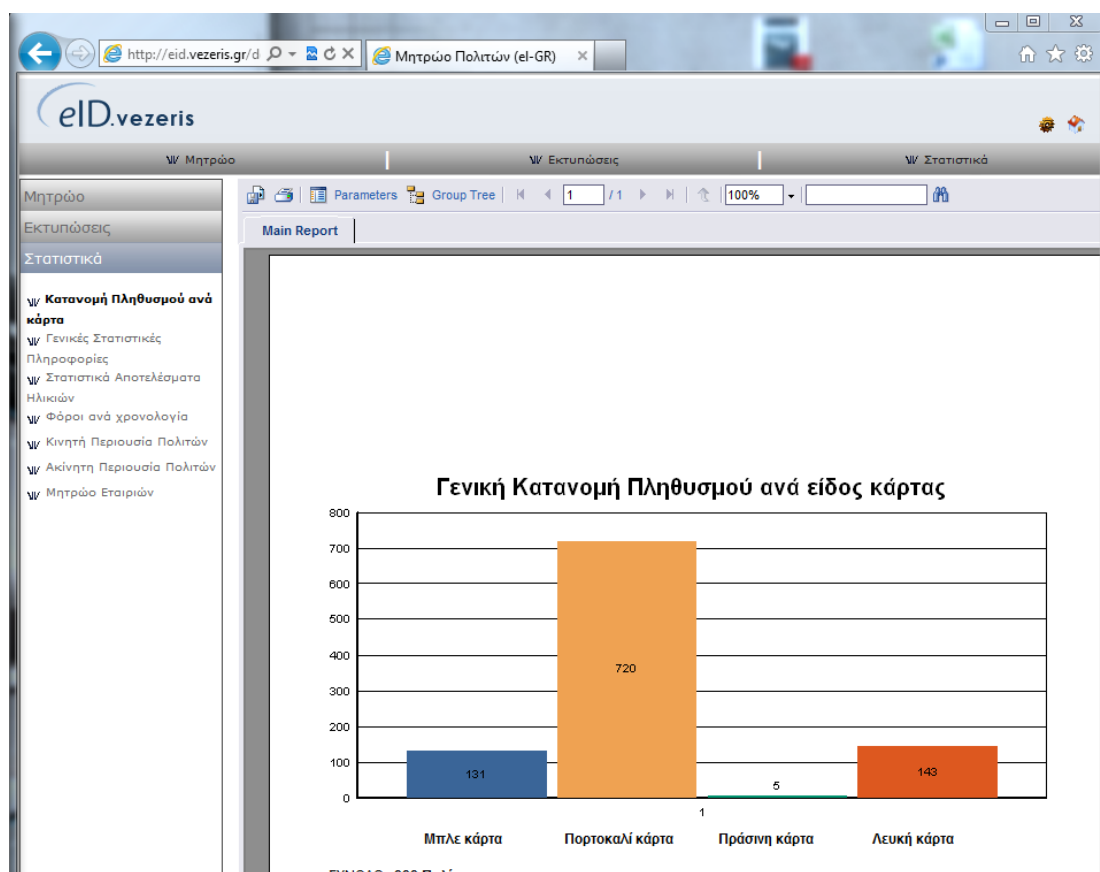
Από τη στιγμή που όλα αυτά τα δεδομένα θα υπάρχουν μέσα σε αυτό το πανίσχυρο μητρώο πολιτών, αντιλαμβάνεστε ότι υπάρχουν τεράστιες δυνατότητες άντλησης στοιχείων και φυσικά με την επίδραση φίλτρων μπορούμε να πάρουμε πολύ συγκεκριμένα αποτελέσματα. Παρακάτω φαίνεται η εικόνα του Γενικού Μητρώου πολιτών και αριστερά στο μενού διάφορες έτοιμες εκτυπώσεις.

A/A	Αριθμός Πολίτη (Πρώην ΑΜΚΑ)	Εν ζωή	Είδος κάρτας	Επώνυμο	Όνομα	Πατρώνυμο	Διεύθυνση	Τ
1	001001000000	ΝΑΙ	Λευκή	ΜΟΥΣΤΑΦΑ	ΟΓΛΟΥ	ΧΡΥΣΤΟΣ	ΒΑΣΙΟΦΙΑΣ 1	Μόν
2	001002000000	ΝΑΙ	Λευκή	ΝΤΟΣΗΣ	ΙΩΑΝΝΗΣ	ΒΑΣΙΛΕΙΟΣ	ΒΑΣΙΟΦΙΑΣ 1	Μόν
3	001003000000	ΝΑΙ	Λευκή	ΣΤΕΡΓΙΟΥ	ΑΙΚΑΤΕΡΙΝΗ	ΒΑΣΙΛΕΙΟΣ	ΒΑΣΙΟΦΙΑΣ 1	Μόν
4	001004000000	ΝΑΙ	Λευκή	Χ'ΣΑΒΒΑ	ΑΦΡΟΔΙΤΗ	ΕΠΑΜΕΙΝΩΝΔΑΣ	ΒΑΣΙΟΦΙΑΣ 1	Μόν
5	001005000000	ΝΑΙ	Πορτοκαλί	ΙΩΑΝΝΙΔΗΣ	ΟΔΥΣΣΕΥΣ	ΟΔΥΣΣΕΥΣ	ΒΑΣΙΟΦΙΑΣ 3	Εάν
6	001006000000	ΝΑΙ	Πορτοκαλί	ΔΗΜΗΤΡΙΑΔΗΣ	ΓΕΩΡΓΙΟΣ	ΕΠΑΜΕΙΝΩΝΔΑΣ	ΒΑΣΙΟΦΙΑΣ 3	Εάν
7	001007000000	ΝΑΙ	Μπλε	ΚΑΛΕΝΤΕΡΙΔΗΣ	ΛΑΖΑΡΟΣ	ΒΑΣΙΛΕΙΟΣ	ΒΑΣΙΟΦΙΑΣ 4	Εάν
8	001007010000	ΝΑΙ	Λευκή	ΚΑΛΕΝΤΕΡΙΔΗΣ	ΧΡΗΣΤΟΣ	ΚΩΣΤΑΣ	ΒΑΣΙΟΦΙΑΣ 4	Μόν
9	001008001000	ΝΑΙ	Πορτοκαλί	ΖΟΥΡΝΑΤΖΗΣ	ΓΡΗΓΟΡΙΟΣ	ΕΠΑΜΕΙΝΩΝΔΑΣ	ΒΑΣΙΟΦΙΑΣ 5	Εάν
10	001008002000	ΝΑΙ	Πορτοκαλί	ΚΟΤΑΣ	ΧΡΗΣΤΟΣ	ΕΠΑΜΕΙΝΩΝΔΑΣ	ΒΑΣΙΟΦΙΑΣ 5	Εάν
11	001008003000	ΝΑΙ	Πορτοκαλί	ΚΑΡΑΤΣΑΝΗΣ	ΝΙΚΟΛΑΟΣ	ΕΠΑΜΕΙΝΩΝΔΑΣ	ΒΑΣΙΟΦΙΑΣ 5	Εάν
12	001008004000	ΝΑΙ	Πορτοκαλί	ΜΑΧΑΙΡΙΔΗΣ	ΓΡΗΓΟΡΙΟΣ	ΓΡΗΓΟΡΙΟΣ	ΒΑΣΙΟΦΙΑΣ 5	Εάν
13	001008005000	ΝΑΙ	Λευκή	ΔΗΜΟΓΛΟΥ	ΕΛΕΥΘΕΡΙΟΣ	ΕΠΑΜΕΙΝΩΝΔΑΣ	ΒΑΣΙΟΦΙΑΣ 5	Μόν
14	001008006000	ΝΑΙ	Πορτοκαλί	ΑΡΣΕΝΑΚΗ	ΟΥΡΑΝΙΑ	ΔΗΜΗΤΡΙΟΣ	ΒΑΣΙΟΦΙΑΣ 5	Εάν
15	001008007000	ΝΑΙ	Λευκή	ΓΕΩΡΓΙΟΥ	ΣΙΜΕΛΑ	ΔΗΜΗΤΡΙΟΣ	ΒΑΣΙΟΦΙΑΣ 5	Μόν
16	001008008000	ΝΑΙ	Πορτοκαλί	ΧΡΙΣΤΟΦΟΡΙΔΗΣ	ΛΕΩΝΙΔΑΣ	ΒΑΣΙΛΕΙΟΣ	ΒΑΣΙΟΦΙΑΣ 5	Εάν
17	001008009000	ΝΑΙ	Λευκή	ΖΟΥΡΝΑΤΖΙΔΗΣ	ΑΝΤΩΝΙΟΣ	ΔΗΜΗΤΡΙΟΣ	ΒΑΣΙΟΦΙΑΣ 5	Μόν
18	001008010000	ΝΑΙ	Μπλε	ΚΑΡΑΤΣΑΝΗΣ	ΕΥΑΓΓΕΛΟΣ	ΕΠΑΜΕΙΝΩΝΔΑΣ	ΒΑΣΙΟΦΙΑΣ 5	Εάν
19	001008011000	ΝΑΙ	Πορτοκαλί	ΠΑΠΑΔΟΠΟΥΛΟΣ	ΒΑΣΙΛΕΙΟΣ	ΔΗΜΗΤΡΙΟΣ	ΒΑΣΙΟΦΙΑΣ 5	Εάν
20	001008012000	ΝΑΙ	Μπλε	ΖΟΥΡΝΑΤΖΙΔΗΣ	ΑΝΤΩΝΙΟΣ	ΒΑΣΙΛΕΙΟΣ	ΒΑΣΙΟΦΙΑΣ 5	Εάν
21	001008013000	ΝΑΙ	Λευκή	ΓΚΟΥΝΤΑΚΟΣ	ΓΕΩΡΓΙΟΣ	ΒΑΣΙΛΕΙΟΣ	ΒΑΣΙΟΦΙΑΣ 5-A	Μόν
22	001008014000	ΝΑΙ	Λευκή	ΠΑΣΒΑΝΤΗΣ	ΚΩΝ/ΝΟΣ	ΔΗΜΗΤΡΙΟΣ	ΒΑΣΙΟΦΙΑΣ 5-A	Μόν
23	001008015000	ΝΑΙ	Λευκή	Χ'ΚΛΕΑΡΧΟΥ	ΝΙΚΟΛΑΟΣ	ΔΗΜΗΤΡΙΟΣ	ΒΑΣΙΟΦΙΑΣ 5	Μόν
24	001008016000	ΝΑΙ	Πράσινη	ΠΑΝΕΡΗΣ	ΛΕΩΝΙΔΑΣ	ΙΩΑΝΝΗΣ	ΒΑΣΙΟΦΙΑΣ 5-A	Καλι
25	001008017000	ΝΑΙ	Πράσινη	ΚΑΡΑΤΣΑΝΗΣ	ΕΥΑΓΓΕΛΟΣ	ΕΥΑΓΓΕΛΟΣ	ΒΑΣΙΟΦΙΑΣ 5	Καλι
26	001008018000	ΝΑΙ	Πράσινη	ΔΙΑΜΑΝΤΗΣ	ΒΑΣΙΛΕΙΟΣ	ΕΠΑΜΕΙΝΩΝΔΑΣ	ΒΑΣΙΟΦΙΑΣ 5	Καλι

Οι εκτυπώσεις δημιουργήθηκαν με τις δυνατότητες του Crystal reports για Visual Studio.

5.7 Τα στατιστικά

Τα στατιστικά είναι ένα από τα στοιχεία μεγάλης αξίας (προστιθέμενης) στην πληροφόρηση του κράτους και στην εικόνα των πολιτών του. Ουσιαστικά στοιχεία που αναδεικνύουν την εικόνα του ίδιου του κράτους. Μέχρι σήμερα η Ελλάδα δεν έχει γνώση στατιστικών σε πραγματικό χρόνο, αν αναλογιστούμε ότι πριν λίγο διάστημα δεν γνώριζε τον αριθμό των υπαλλήλων που είχε. Μέσω του e-μητρώου πολιτών ,μπορεί σε πραγματικό χρόνο να έχει όσα στοιχεία θέλει με όποιον τρόπο μπορεί να τεθεί sql ερώτημα στην βάση δεδομένων. Παρακάτω παραθέτω μερικά στατιστικά στοιχεία, τυχαίου πλήθους εγγραφών και είδους εγγραφών, διότι τα δεδομένα πέρασαν τυχαία χωρίς επεξεργασία (έτσι και αλλιώς είναι τυχαία, ψεύτικα και για τις ανάγκες τις μελέτης όλα τα στοιχεία που παρουσιάζονται από το πρόγραμμα). Ας δούμε λοιπόν τις δυνατότητες ενός τέτοιου μητρώου:



Το Μητρώο Αποτελείται από:

Συνολικές Εγγραφές : 999 Πολίτες

Εν Ζωή : 999 Πολίτες - Θανόντες : 0 Πολίτες

Μπλε κάρτα	131 Πολίτες	Άντρες	727 Πολίτες
Πορτοκαλί κάρτα	720 Πολίτες	Γυναίκες	272 Πολίτες
Πράσινη κάρτα	5 Πολίτες	Ανοιχτόχρωμοι	536 Πολίτες
Λευκή κάρτα	143 Πολίτες	Σκουρόχρωμοι	463 Πολίτες
Ύψος > 1.70		873 Πολίτες	
Ύψος <= 1.70		126 Πολίτες	

Στατιστικά Αποτελέσματα Ηλικιών

Έως 18 χρονών

Άντρες	523 Πολίτες
Γυναίκες	197 Πολίτες

Από 18 έως 40 χρονών

Άντρες	86 Πολίτες
Γυναίκες	33 Πολίτες

Από 40 έως 65 χρονών

Άντρες	118 Πολίτες
Γυναίκες	42 Πολίτες

ΣΥΝΟΛΟ ΠΟΛΙΤΩΝ : 999

Φόροι ανά χρονολογία

Το έτος	2005	εισέπραξε το κράτος	111.250,00	Ευρώ από φόρους
Το έτος	2006	εισέπραξε το κράτος	222.500,00	Ευρώ από φόρους
Το έτος	2007	εισέπραξε το κράτος	333.750,00	Ευρώ από φόρους
Το έτος	2008	εισέπραξε το κράτος	445.000,00	Ευρώ από φόρους
Το έτος	2009	εισέπραξε το κράτος	556.250,00	Ευρώ από φόρους
Το έτος	2010	εισέπραξε το κράτος	556.250,00	Ευρώ από φόρους

ΣΥΝΟΛΟ ΦΟΡΩΝ :	2.225.000,00	Ευρώ
----------------	---------------------	------

Κινητή περιουσία πολιτών

Το έτος	2007	αγοράστηκαν	94	Μηχανάκι
Το έτος	2008	αγοράστηκαν	100	Αυτοκίνητο
Το έτος	2009	αγοράστηκαν	31	Μηχανάκι
Το έτος	2010	αγοράστηκαν	20	Αυτοκίνητο
Το έτος	2011	αγοράστηκαν	11	Αυτοκίνητο

ΣΥΝΟΛΟ:	256
---------	------------

Ακίνητη περιουσία πολιτών

Το	2006	αγοράστηκαν	131	Διαμέρισμα
Το	2007	αγοράστηκαν	120	Εξ. Μονοκατοικία
Το	2008	αγοράστηκαν	5	Διαμέρισμα

ΣΥΝΟΛΟ:	256
---------	------------

The screenshot shows a web browser window with the URL <http://eid.vezeris.gr/d>. The page title is "Μητρώο Πολιτών (el-GR)". The application interface includes a sidebar with navigation options: "Μητρώο", "Εκτυπώσεις", "Στατιστικά", "Κατανομή Πληθυσμού ανά κάρτα", "Γενικές Στατιστικές", "Πληροφορίες", "Στατιστικά Αποτελέσματα", "Ηλικιών", "Φόροι ανά χρονολογία", "Κινητή Περιουσία Πολιτών", "Ακίνητη Περιουσία Πολιτών", and "Μητρώο Εταιριών". The main content area displays a table with three columns: "Επωνυμία εταιρίας", "Αριθμός Μητρώου", and "Δραστηριότητα".

Επωνυμία εταιρίας	Αριθμός Μητρώου	Δραστηριότητα
ΑΒΕΡΟΠΟΥΛΟΥ	038000000	ΕΜΠΟΡΙΚΗ
ΑΛΗ ΟΓΛΟΥ	025024000	ΜΕΤΑΠΟΙΗΣΗ
ΑΜΑΝΑΤΙΔΗΣ	008007000	ΜΕΤΑΠΟΙΗΣΗ
ΑΜΕΤ ΟΓΛΟΥ	111111111	ΜΕΤΑΠΟΙΗΣΗ
ΑΝΑΓΙΑΝΝΗΣ	008001000	ΕΜΠΟΡΙΚΗ
ΑΝΑΣΤΑΣΙΑΔΗΣ	019000000	ΜΕΤΑΠΟΙΗΣΗ
ΑΝΤΩΝΟΥΔΗΣ	071012000	ΕΜΠΟΡΙΚΗ
ΑΡΑΜΠΑΤΖΗ	097009016	ΜΕΤΑΠΟΙΗΣΗ
Β.ΑΡΙΦΟΓΛΟΥ-Π.ΧΟΥΜΑΙΔΗΣ Ο.Ε.	011090000	ΜΕΤΑΠΟΙΗΣΗ
ΒΑΓΚΑΝΟΒΑ	073000008	ΠΑΡΟΧΗ ΥΠΗΡΕΣΙΩΝ
ΒΑΣΙΛΕΙΟΥ	012002000	ΕΜΠΟΡΙΚΗ
ΒΛΑΣΣΟΠΟΥΛΟΥ	020003000	ΜΕΤΑΠΟΙΗΣΗ
ΒΡΑΝΙΑΣ	105002000	ΜΕΤΑΠΟΙΗΣΗ
ΓΑΛΗΝΟΣ	111111111	ΜΕΤΑΠΟΙΗΣΗ
ΓΙΑΚΙΝΤΖΑΚΗΣ	018004000	ΠΑΡΟΧΗ ΥΠΗΡΕΣΙΩΝ
ΓΚΑΙΝΤΑΤΖΗ	109000000	ΕΜΠΟΡΙΚΗ
ΓΚΑΜΠΡΑ	006011000	ΜΕΤΑΠΟΙΗΣΗ
ΓΚΟΥΡΛΙΑΣ	144010000	ΜΕΤΑΠΟΙΗΣΗ
ΓΟΥΝΑΡΗΣ	193000000	ΜΕΤΑΠΟΙΗΣΗ
ΓΡΗΓΟΡΙΑΔΗΣ	046050009	ΠΑΡΟΧΗ ΥΠΗΡΕΣΙΩΝ
ΔΑΛΑΚΟΥΡΑΣ	066010000	ΠΑΡΟΧΗ ΥΠΗΡΕΣΙΩΝ
ΔΑΜΙΓΟΥ	020000000	ΕΜΠΟΡΙΚΗ
ΔΑΤΣΙΟΣ	182002000	ΕΜΠΟΡΙΚΗ
ΔΕΡΜΙΤΖΑΚΗΣ	117002000	ΜΕΤΑΠΟΙΗΣΗ
ΔΙΑΜΑΝΤΑΚΗ	044000017	ΕΜΠΟΡΙΚΗ
ΕΔΕΜ Ε.Π.Ε	002001000	ΕΜΠΟΡΙΚΗ
ΕΥΑΓΟΡΟΥ	102063000	ΕΜΠΟΡΙΚΗ
ΕΦΡΑΙΜΙΔΗΣ	091116000	ΜΕΤΑΠΟΙΗΣΗ
ΖΑΦΕΙΡΙΑΔΗΣ	122000000	ΜΕΤΑΠΟΙΗΣΗ
ΖΟΡΠΙΔΗΣ	105056000	ΜΕΤΑΠΟΙΗΣΗ
ΗΛΙΑΔΟΥ	136110000	ΕΜΠΟΡΙΚΗ
ΙΜΠΡΑΗΜ	032008000	ΠΑΡΟΧΗ ΥΠΗΡΕΣΙΩΝ
ΙΣΛΑΜ	111111111	ΠΑΡΟΧΗ ΥΠΗΡΕΣΙΩΝ
ΚΑΠΗΣΙΖΟΓΛΟΥ	117003000	ΕΜΠΟΡΙΚΗ
ΚΑΡΑΓΙΑΝΝΙΔΟΥ	066003000	ΕΜΠΟΡΙΚΗ
ΚΑΡΥΜΠΙΔΗΣ	622000000	ΜΕΤΑΠΟΙΗΣΗ

5.8 Συμπεράσματα

Είναι πασιφανές το κέρδος και η χρηστικότητα ενός τέτοιου μητρώου τόσο για το κράτος όσο και για τους πολίτες οι οποίοι θα απαλλαχτούν από τη λογική της γραφειοκρατίας και των αλληπάλληλων γραφείων εξυπηρέτησης. Επειδή το κράτος παρέχει υπηρεσίες, οι περισσότερες μπορούν να διεκπεραιώνονται ψηφιακά μέσω internet σε τάχιστο χρόνο. Τα οφέλη για το κράτος και τους πολίτες του είναι:

- Α) Ταχύτερη ανάπτυξη,
- Β) Μικρό λειτουργικό κόστος για το κράτος – λιγότερους μη παραγωγικούς υπαλλήλους,
- Γ) Μεγαλύτερος έλεγχος – καταπολέμηση της ανομίας και της απάτης,
- Δ) Αύξηση της ανταγωνιστικότητας
- Ε) Καπ.

Το μόνο θολό σημείο είναι η προστασία των προσωπικών δεδομένων ντου πολίτη και η προσεκτική και ασφαλής χρήση του e-μητρώου πολιτών και καθώς η διαχείριση και τα δικαιώματα πρόσβασης.

Όσο αφορά στο λογισμικό ολοκλήρωσης , αν και το αναπτύξαμε λόγω γνώσεων σε C# και .net framework θα προτείναμε την ανάπτυξη του σε cross platform τεχνολογίες όπως html 5 και java.

Σε αυτό το σημείο θα ήθελα να ευχαριστήσω τον Θανάση Μπατσακίδη για την πολύτιμη βοήθειά του στην ολοκλήρωση του προγραμματισμού του λογισμικού που παρουσιάζουμε εδώ ως παράδειγμα e-μητρώου πολιτών.

6ο Κεφάλαιο : Θέματα ασφαλείας

Στο κεφάλαιο αυτό αναλύονται θέματα ασφάλειας κατά την χρήση αλλά και την λειτουργία του συστήματος κάρτας – δικτύου. Αναφέρονται θέματα σε περιπτώσεις hacking, κλοπής ή απώλειας κλπ. Αναφέρονται όλα τα αδύνατα σημεία του θέματος και τρόποι αντιμετώπισης όπου είναι δυνατό.

Επίπεδα ασφάλειας πρόσβασης και τροποποίησης των στοιχείων του πολίτη – ταυτοποίηση. Περιπτώσεις κλοπής – απώλειας.

6.1 Οι 10 αμετάθετοι νόμοι της ασφάλειας.

1. Εάν ένας κακός τύπος μπορεί να σας πείσει να τρέξετε το πρόγραμμά του στον υπολογιστή σας, δεν είναι πλέον ο υπολογιστής σας.
2. Εάν ένας κακός τύπος μπορεί να αλλάξει το λειτουργικό σύστημα στον υπολογιστή σας, δεν είναι πλέον ο υπολογιστής σας.
3. Εάν ένας κακός τύπος έχει απεριόριστη πρόσβαση στον υπολογιστή σας, δεν είναι πλέον ο υπολογιστής σας.
4. Αν επιτρέψετε σε έναν κακό να ανεβάσετε τα προγράμματά του στην ιστοσελίδα σας, δεν είναι πλέον η ιστοσελίδα σας.
5. Οι απλοί κωδικοί πρόσβασης καταστρέφουν την ισχυρή ασφάλεια.
6. Ένας υπολογιστής είναι τόσο ασφαλές όσο ο διαχειριστής είναι αξιόπιστος.
7. Κρυπτογραφημένα δεδομένα είναι τόσο ασφαλές όσο το κλειδί αποκρυπτογράφησης.
8. Ένα μη ενημερωμένο πρόγραμμα ανίχνευσης ιών είναι μόνο οριακά καλύτερο από το να μην υπάρχει.
9. Η απόλυτη ανωνυμία δεν είναι πρακτική, ούτε στην πραγματική ζωή ούτε στο διαδίκτυο.
10. Η τεχνολογία δεν αποτελεί πανάκεια.[46]

Στα προηγούμενα κεφάλαια αναφέραμε το PKI και θέματα στην φυσική και ηλεκτρονική υλοποίηση της κάρτας του πολίτη, όπου προσφέρουν ή προλαμβάνουν θέματα ασφάλειας στην παραγωγή και στη χρήση της κάρτας του πολίτη. Εδώ θα επικεντρωθούμε σε διάφορα επίπεδα ασφαλείας που απασχολούν το όλο θέμα και παρουσιάζουν ενδιαφέρον.

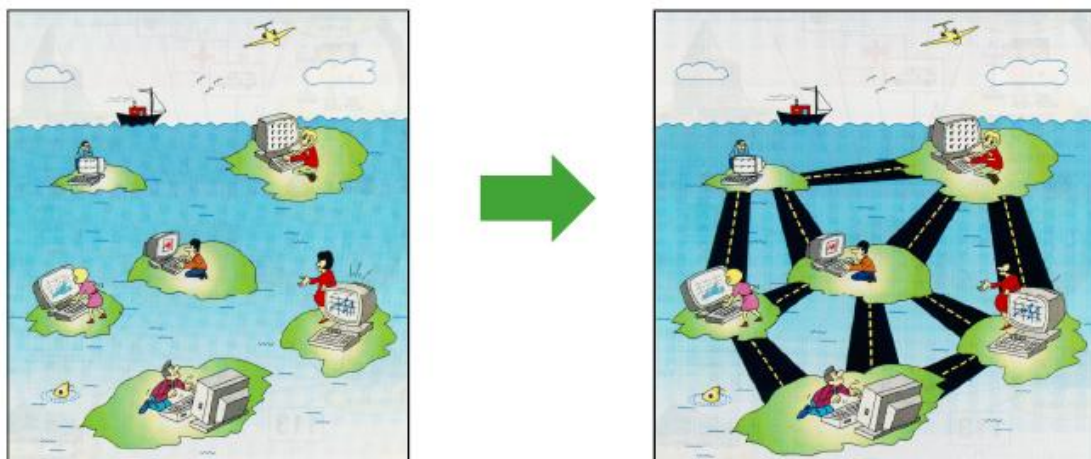
6.2 Θέματα ασφαλών online δημόσιων υπηρεσιών.

Η πρόκληση για την ασφάλεια είναι πάρα πολύ μεγάλη. Από την μία αφενός έχουμε την ασφάλεια του πολίτη η οποία θα πρέπει να εγγυάται το δημόσιο και οι υπηρεσίες, κάνοντας χρήση της κάρτας αυτής και των δεδομένων της και αφετέρου οι την ασφάλεια των συναλλαγών και των συστημάτων γενικότερα.

Θέματα τα οποία απασχολούν την ασφάλεια, αναφέροντάς τα ενδεικτικά είναι [17]:

- Αυξανόμενος αριθμός δημόσιων υπηρεσιών στο διαδίκτυο,
- Σωστές πληροφορίες πρέπει να παραδίδονται στο σωστό πρόσωπο,
- Διάφορες υπηρεσίες – διαφορετικές λύσεις,
- Μεταρρυθμίσεις στο δημόσιο τομέα με έργα ΤΠΕ μέσω κοινής υποδομής και ανάπτυξης αρχών – πρωτοτύπων,
- Πρέπει να διατηρηθεί η υψηλή εμπιστοσύνη στο δημόσιο τομέα μεταξύ του πληθυσμού.
- Οι νόμοι και οι κανονισμοί μπορούν να υποστηρίξουν της ασφάλεια των πληροφοριών.

Οι προκλήσεις είναι μεγάλες και η χρηστή διαχείριση θα πρέπει να προωθεί την μετατροπή από διαφορετικές λύσεις σε μία ενοποιημένη υποδομή.



6.3 Δικαιώματα του πολίτη - ENISA

Το ENISA - European Network and Information Security Agency (2004) αποτελεί τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια των Δικτύων και Πληροφοριών. Τα συστήματα επικοινωνίας και πληροφοριών είναι σημαντικοί παράγοντες στην εξέλιξη της οικονομίας και κοινωνίας. Τα ασφαλή δίκτυα καθίστανται με τον καιρό τόσο απαραίτητα για τη λειτουργία της Ψηφιακής Οικονομίας όσο ο ηλεκτρισμός και το νερό.

Για αυτό το λόγο, η ασφάλεια των συστημάτων δικτύων και των πληροφοριών παίζει σημαντικό ρόλο για την κοινωνία. Αυτό πηγάζει από την πολυπλοκότητα των

πληροφοριακών συστημάτων, τα ατυχήματα, τα λάθη και τις επιθέσεις στις φυσικές υποδομές που παρέχουν κρίσιμες υπηρεσίες στους πολίτες της Ευρωπαϊκής Ένωσης.

Ο ENISA δημιουργήθηκε για να ενδυναμώσει τη δυνατότητα της Ευρωπαϊκής Ένωσης, των Κρατών μελών της Ε.Ε. και της επαγγελματικής κοινότητας να αποφεύγει, να διευθύνει και να ανταποκρίνεται σε προβλήματα που αφορούν την ασφάλεια των δικτύων και πληροφοριών.

Προκειμένου να πετύχει το στόχο του, ο ENISA αποτελεί ένα κέντρο εμπειρογνωμοσύνης σε θέματα Ασφάλειας των Δικτύων και Πληροφοριών και προωθεί τη συνεργασία ανάμεσα στο δημόσιο και ιδιωτικό τομέα.

Τα δικαιώματα του πολίτη εξαρτώνται από την γεωγραφική του τοποθεσία. Τα δικαιώματα των Ευρωπαίων πολιτών ορίζονται αποτελεσματικά από οδηγίες και εθνικούς κανονισμούς [21]. Ένα παράδειγμα είναι το δικαίωμα να διατηρούν ορισμένα δεδομένα ιδιωτικά, το οποίο καθορίζεται από το άρθρο 8 της σύμβασης για τα Δικαιώματα του Ανθρώπου και καλύπτονται από την Οδηγία για την Ευρωπαϊκή Προστασία Προσωπικών Δεδομένων. Σε πιο αναλυτικό επίπεδο, τα δικαιώματα στον ηλεκτρονικό κόσμο, καθορίζονται από συμβατικές ρυθμίσεις.

Επιπρόσθετα εκτός του δικαιώματος της ιδιωτικότητας, οι Ευρωπαίοι πολίτες έχουν το δικαίωμα της ορθότητας των δεδομένων (διορθωτικά). Ειδικότερα ο Ευρωπαίος πολίτης μπορεί να απαιτήσει την επιμέλεια για την ενημέρωση και την ορθότητα των στοιχείων του. Αυτό βέβαια προϋποθέτει τη συστημική παρακολούθηση της επικαιρότητας των στοιχείων. Στην πράξη η επικαιροποίηση των στοιχείων δεν είναι εύκολη διεργασία.

Το πρόβλημα της ερμηνείας[21] εντοπίζεται όταν το eID χρησιμοποιείτε σε περιβάλλοντα εκτός Ε.Ε. π.χ. υπάρχει η ίδια κάλυψη ασφάλειας δεδομένων στις Η.Π.Α. όπως στην Ε.Ε.; Ή ακόμα ότι το συμβατικό πλαίσιο είναι σύμφωνο με ένα συγκεκριμένο εθνικό δίκαιο, ποιο από τα δύο ισχύει στην Ευρώπη; (στην πράξη βέβαια).

Όπως τα δικαιώματα και οι υποχρεώσεις του πολίτη ορίζονται από οδηγίες και εθνικούς νόμους. Παρομοίως συμβάσεις προσδιορίζουν τις υποχρεώσεις του

κατόχου eID. Π.χ. να διατηρεί προστατευτικά το pin, να μην διατηρεί ανάρμοστα τα διαπιστευτήρια, να είναι ενήμερος για τους περιορισμούς της χρήσης της ηλεκτρονικής ταυτότητας κ.α.π.

Οι πολίτες για να επωφεληθούν πλήρως από τους μηχανισμούς ισχυρής ασφάλειας, θα πρέπει να ασφαλίσουν και οι ίδιοι τα υπάρχοντά τους και το περιβάλλον τους. Το πιο βασικό καθήκον ενός πολίτη του ηλεκτρονικού κόσμου, είναι να δώσει έμφαση στο να αντιληφθεί πλήρως τα εργαλεία τα οποία χρησιμοποιεί. Από την άλλη εξορισμού τα ισχυρότερα περιβάλλοντα είναι λιγότερο επιρρεπή σε προσβολή (επίθεση) από τα υπόλοιπα.

6.4 ID ανοιχτού τύπου

Το ID ανοιχτού τύπου έχει πολλές ευκολίες και αποκεντρωμένο σύστημα επαλήθευσης [11]. Η δυσκολία εφαρμογής είναι στο σημείο που δεν υπάρχει εγγυημένος φορέας διασφάλισης της ασφάλειας του χρήστη. Παρόλα αυτά θεωρώ ότι πρέπει να αναφερθεί στην παρούσα εργασία, λόγω του ότι πολλές εφαρμογές και υπηρεσίες ήδη παρέχονται με ασφάλεια από ότι έχουν αποδείξει οι πρακτικές και εφαρμογές μέχρι σήμερα.

Το OPEN ID διαθέτει τα παρακάτω χαρακτηριστικά:

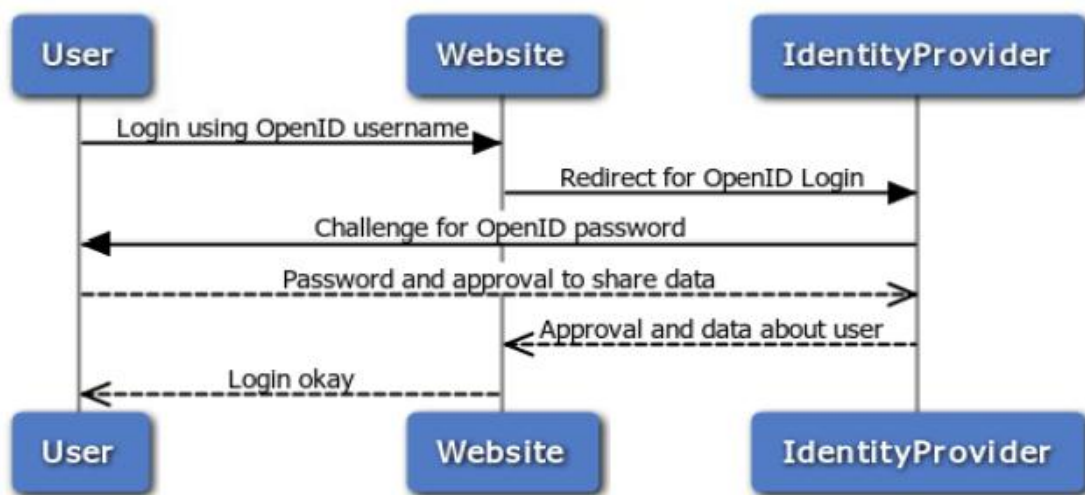
- Απλό login σε πολλά web sites με το ίδιο όνομα χρήστη,
- Απλή διαδικασία πρόσβασης και σύνδεσης,
- Ευκολία χρήσης,
- Ανοικτό στάνταρ
- Αποκεντρωμένη πιστοποίηση ταυτότητας,
- Χωρίς χρέωση.

Παρόμοια τέτοια μητρώα έχουμε δει στο Microsoft Passport Network (Microsoft,MSN,etc) και Google Account Network (Gmail,Gtalk,etc). Μέχρι το 2015 [11] αναμένεται οι χρήστες να έχουν φτάσει τα 5δισεκατομμύρια με 15 εκατομμύρια web sites να το υποστηρίζουν.

Με το open ID οι χρήστες, με έναν λογαριασμό έχουν πρόσβαση σε πολλαπλά sites, χωρίς να πρέπει να θυμούνται διαφορετικά, με εύκολη πρόσβαση στις υπηρεσίες.

Από την άλλη, η διαχείριση του open ID δίνει ευκολία στους προγραμματιστές να διαχειριστούν χαρακτηριστικά και τεχνολογίες στα sites, αφαιρεί την πολυπλοκότητα και φέρνει ευκολία σε εργαλεία και δίνει πρόσβαση σε εκατομμύρια χρήστες.

Στο παρακάτω σχήμα φαίνεται η διαδραστικότητα – διεργασίες πρόσβασης στις υπηρεσίες.



Πάροχοι τέτοιων υπηρεσιών είναι μεταξύ άλλων, μεγάλες εταιρίες υπηρεσιών internet, όπως παρακάτω:



6.5 Πιστοποιητικά και διαπιστευμένα πιστοποιητικά.

Μετά λοιπόν από τα παραπάνω, θα πρέπει να υπάρχει τρόπος να διασφαλιστεί η ασφάλεια των πολιτών και η απόκτηση της εμπιστοσύνης, ώστε να χρησιμοποιηθεί η κάρτα του πολίτη για όλες τις υπηρεσίες. Ένα από τα σημαντικότερα εργαλεία είναι τα πιστοποιητικά από τις αρχές πιστοποίησης.

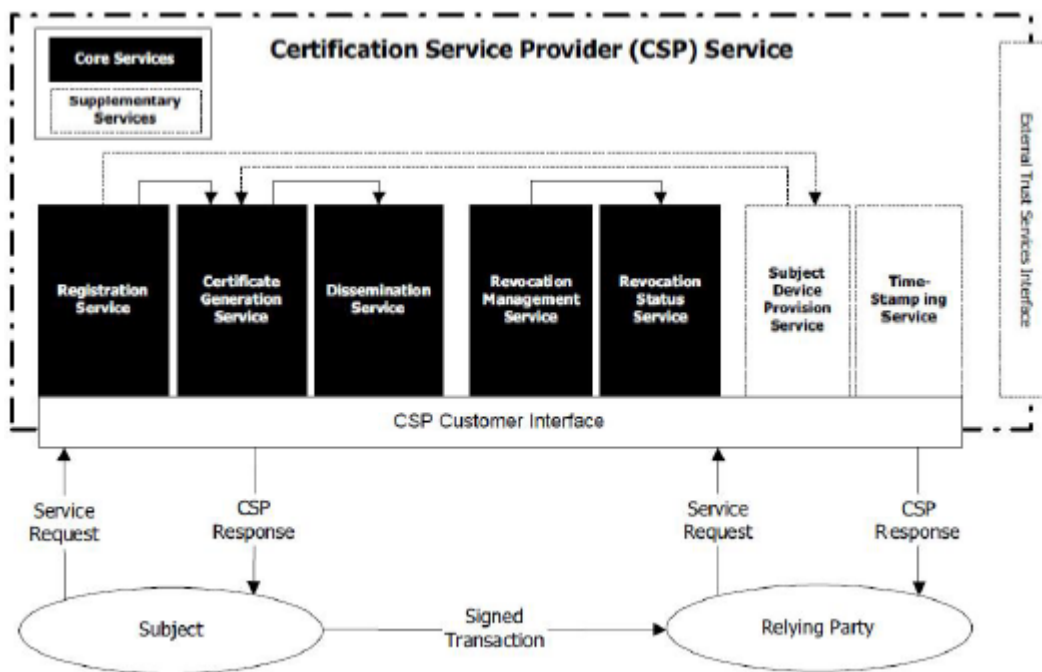
Υπάρχουν ψηφιακά πιστοποιητικά, διαπιστευμένα πιστοποιητικά, παροχή πιστοποιητικών υπηρεσιών, διαπίστευσης. Ένα θέμα που προκύπτει είναι ο φορέας διαπίστευσης των πιστοποιητικών της κάρτας του πολίτη.

Τι είναι το πιστοποιητικό : Είναι μία δομή δεδομένων σε ηλεκτρονική μορφή, η οποία παρέχει συσχέτιση μεταξύ μιας οντότητας με το δημόσιο κλειδί της, [13] όπου:

- Το πιστοποιητικό είναι απλώς μια πιστοποίηση όπως η ταυτότητα,
- Η συσχέτιση αυτή είναι εγγυημένη από την CA (αρχή πιστοποίησης) μία υπογραφή , όπου εμπιστεύονται και τα δύο μέρη,
- Η αρχή εγγυάται ότι ένα δημόσιο κλειδί ανήκει σε μία ειδική οντότητα. Δεν εγγυάται, σε καμία περίπτωση, την καταλληλότητα της οντότητας και την ορθή χρήση του πιστοποιητικού.

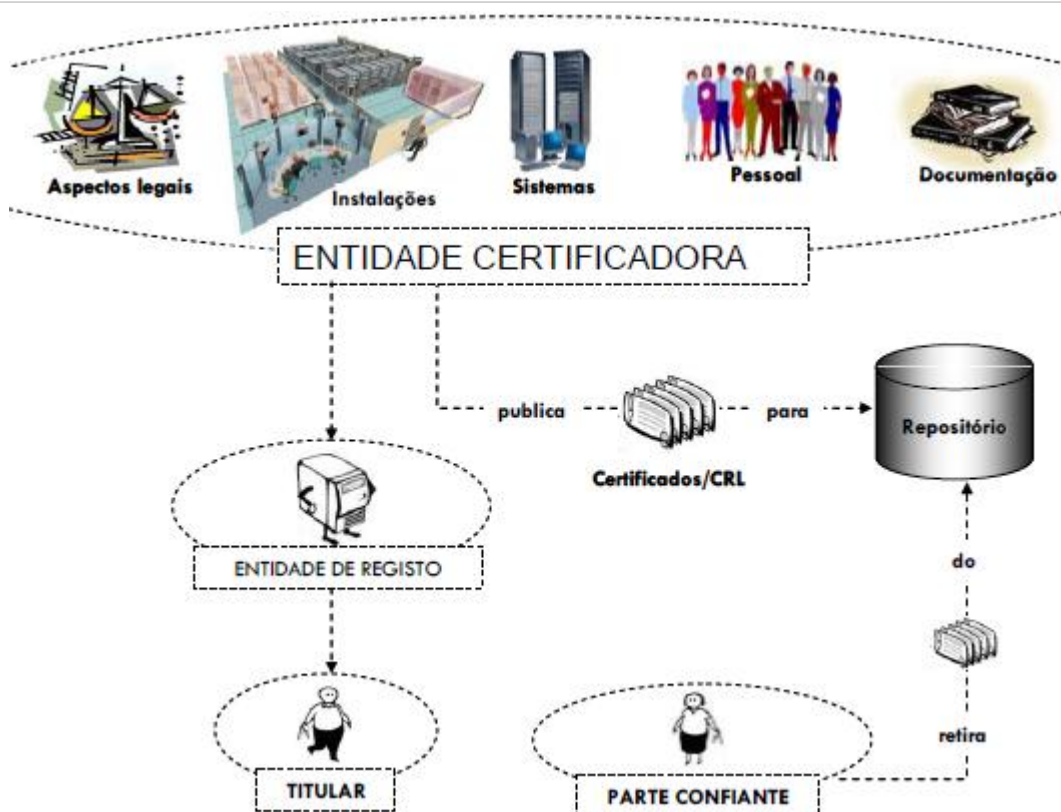
Τα αναγνωρισμένα πιστοποιητικά, σε σχέση με τα απλά πιστοποιητικά, υπερτερούν στο ότι ο φορέας έκδοσης ενός αναγνωρισμένου πιστοποιητικού, έχει διασφαλίσει τα αναφερόμενα στο άρθρο 29 της Decree n.209-D/99. Αυτό σημαίνει ότι το πιστοποιητικό ικανοποιεί τις απαιτήσεις του άρθρου 24 της Decree n.209-D/99.

Ο πάροχος ενός πιστοποιητικού, διέπεται ουσιαστικά από το κάτωθι σχεδιάγραμμα υπηρεσιών, για την υπηρεσία πιστοποίησης (Source:CWA 14167-1):



ενώ παρακάτω φαίνεται η υπηρεσία από την πλευρά της διαπίστευσης.

Ο φορέας διαπίστευσης ουσιαστικά πιστοποιεί του φορείς πιστοποίησης. Αυτό σημαίνει ότι το κάθε κράτος μπορεί να έχει τον φορέα διαπίστευσης, όπως στην Ελλάδα έχουμε το ΕΣΥΔ, στη Γερμανία το DAR κλπ, οι οποίοι φορείς πιστοποιούν φορείς πιστοποίησης όπως τον ΕΛΟΤ, τον TÜV , την Eurocert, Lloyd's κλπ. Η αποτελεσματικότητα έγκειται στους ελέγχους του ΕΣΥΔ απέναντι στους φορείς πιστοποίησης. Οι φορείς πιστοποίησης εννοείτε ότι μπορούν να είναι ιδιωτικού τομέα.



6.6 Παγκόσμιες συγκλίσεις και αποκλίσεις σε θέματα ταυτοποίησης και ιδιωτικότητας.

«Το να κρατάς το μυστικό σου είναι σοφό. Το να περιμένεις όμως από τους άλλους να το κρατήσουν είναι τρέλα» -Samuel Johnson [20].

Οι παγκόσμιες κοινές αρχές περί ιδιωτικότητας , συνοψίζονται στο ότι είναι δικαίωμα του ατόμου να:

- Γνωρίζει ποιες πληροφορίες συλλέγονται, πώς χρησιμοποιούνται και σε ποιόν δίνονται,
- Έχει την επιλογή να μην συλλέγονται οι πληροφορίες του και να μην χρησιμοποιούνται,
- Γνωρίζει σε ποιον δόθηκαν οι πληροφορίες, πότε μοιράστηκαν και να γνωρίζει αν προστατεύονται ακόμα,
- Είναι ικανός να δει τις πληροφορίες που έχουν συλλεχτεί,
- Έχει ένα μέσο για να λάβει ικανοποίηση σε περίπτωση παραβίασης των αρχών.

Από την άλλη ένας οργανισμός είναι υπεύθυνος να:

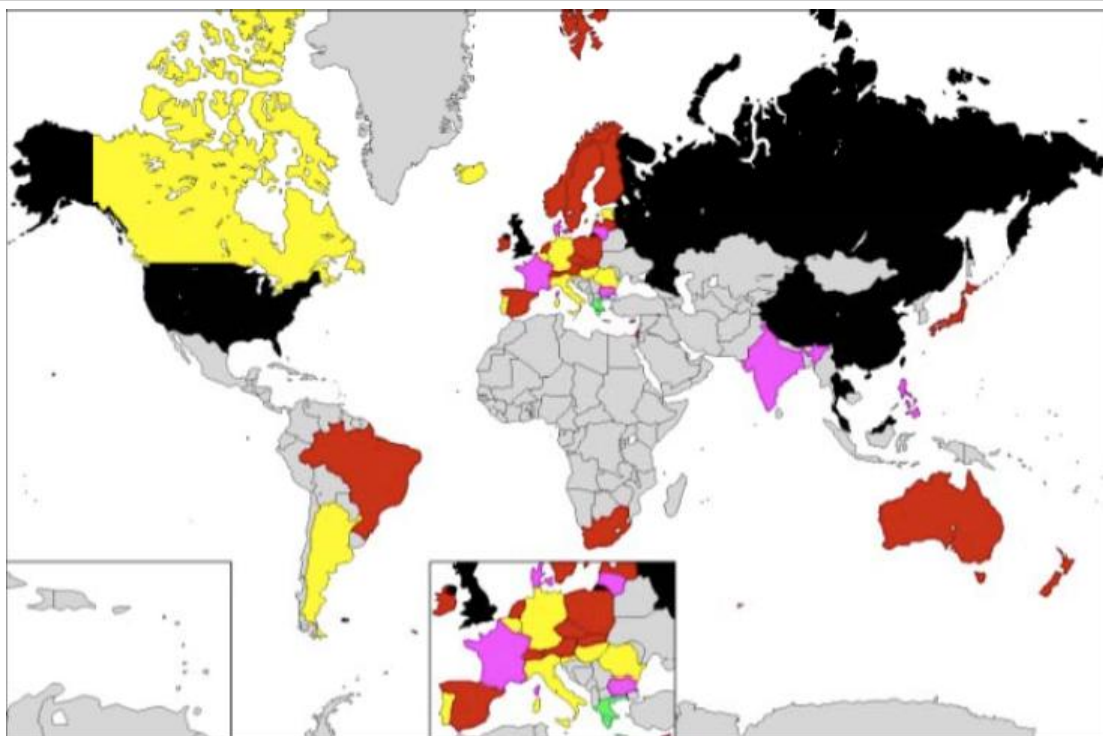
- Διατηρεί ασφαλείς τις πληροφορίες,
- Διατηρεί ακριβείς τις πληροφορίες και να μην τις χρησιμοποιεί εκτός αν εγκριθεί.

Το παγκόσμιο θεσμικό πλαίσιο που ορίζει τα παραπάνω κ.α.π. είναι:

- European Union Data Protection Directive (DPD) Union Directive 95/46/EC Effective Oct 1998
- GLBA - The Gramm-Leach-Bliley Act (The Financial Services Modernization Act of 1999)
- Canadian Personal Information Protection and Electronic Documents Act (C6)including Model Code for the Protection of Personal Information
- HIPAA - Health Information Portability and Accountability Act of 1996 - Effective 2001 – Privacy 2003 - Security
- COPPA - Children's Online Privacy Protection Act - Federal Trade Commission 16 CFR Part 312
- OPPA – Financial Privacy Act – California Privacy Laws,Effective July 2004

Παρακάτω παρατίθεται παγκόσμιος χάρτης των κοινωνιών επιτήρησης (<http://www.privacyinternational.org>).

	Consistently upholds human rights standards
	Significant protections and safeguards
	Adequate safeguards against abuse
	Some safeguards but weakened protections
	Systemic failure to uphold safeguards
	Extensive surveillance societies
	Endemic surveillance societies



Το δημόσιο συμφέρον, οι αξιώσεις για λόγους ασφαλείας επιβολής του νόμου, η καταπολέμηση κατά της τρομοκρατίας και της παράνομης μετανάστευσης, της διοικητικής αποτελεσματικότητας και της απάτης πρόνοιας έχουν καταστήσει το θεμελιώδες δικαίωμα της ιδιωτικής ζωής εύθραυστο και εκτεθειμένο.

Οι τεχνολογικές εξελίξεις, τα τεχνολογικά πρότυπα, η διαλειτουργικότητα μεταξύ των πληροφοριών, τα συστήματα και η παγκοσμιοποίηση των πληροφοριών θέτουν εξαιρετική πίεση για τις λίγες υπόλοιπες ασφάλειες προστασίας της ιδιωτικής ζωής.

Η δημιουργία σε όλη την κοινωνία της "τέλειας" ταυτότητας με τα δακτυλικά αποτυπώματα και σάρωση της ίριδας ως βιομετρικών στοιχείων, η σύνδεση των συστημάτων πληροφορικής του δημόσιου τομέα, η ανάπτυξη σε πραγματικό χρόνο της παρακολούθησης και του ελέγχου σε όλο το φάσμα των επικοινωνιών, η ανάπτυξη σε πραγματικό χρόνο του εντοπισμού της γεωγραφικής θέσης του οχήματος και τον εντοπισμό του κινητού τηλεφώνου, οι εθνικές βάσεις δεδομένων DNA καθώς και η δημιουργία παγκόσμιων συμφωνιών ανταλλαγής πληροφοριών οδηγούν στην εξάλειψη της ανωνυμίας στον κυβερνοχώρο.

Όλα αυτά τα παραπάνω πρεσβεύουν την ανάγκη για απόλυτη διασφάλιση των προσωπικών δεδομένων και διαχείριση – εγγύηση της ασφάλειας του πολίτη.

6.7 Προσωπικά στοιχεία στο διαδίκτυο.

«Η σωστή μόχλευση της Google, έχει περισσότερες δυνατότητες εισβολής από οποιοδήποτε εργαλείο hacking» [20] – Hacker Adrian Lamo.

Πληκτρολογώντας τη φράση "Επιλέξτε μια βάση δεδομένων για να δείτε (select a database to view)" στο Google απέδωσε περίπου 200 συνδέσεις, σχεδόν το σύνολο των οποίων οδήγησε σε βάσεις δεδομένων του FileMaker, οι οποίες είναι προσβάσιμες ηλεκτρονικά.

Ένα από τα αποτελέσματα αναζήτησης τόνισε σε μια σελίδα που εξυπηρετείται από ένα πανεπιστήμιο College of Medicine, το οποίο συνδέεται με μια βάση δεδομένων των 5.500 εγγραφών από τα αρχεία των ασθενών νευροχειρουργικής του Ιατρικού Κολεγίου . Υπάρχουν εγγραφές ρεκόρ που περιλαμβάνονται διευθύνσεις, αριθμοί τηλεφώνου και λεπτομερείς από ασθένειες και θεραπείες.

6.8 bit4id

Στο συνέδριο της Λισαβόνας τον Οκτώβριο του 2009, η εταιρία bit4id, παρουσίασε τρεις λύσεις ασφάλειας σε κάρτες και ηλεκτρονικές συναλλαγές μέσω τηλεφώνου κλπ. Λόγω του ότι είναι πέρα του συγγράμματος αυτού οι εμπορικές λύσεις, παρόλα αυτά παραθέτουμε προτάσεις της εταιρίας ενδεικτικά με εικόνες:

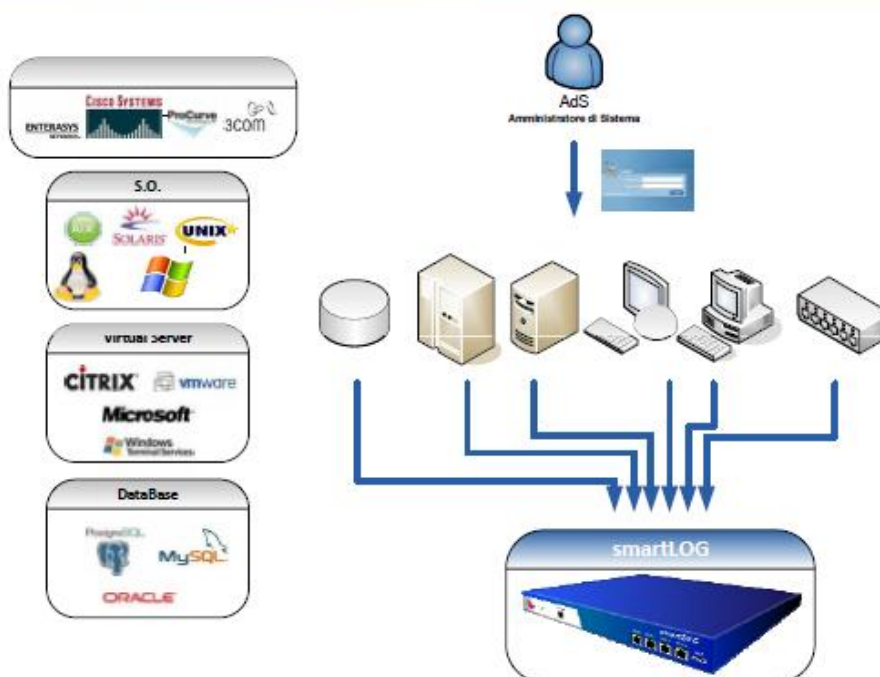
smartSEC: Plug & play security

- ❖ Hardware based
- ❖ ZERO Installation cost/effort
- ❖ No virus vulnerability



- ❖ Plug'nplay security
- ❖ Multi-token support
- ❖ Native National eID support

Functional Architecture

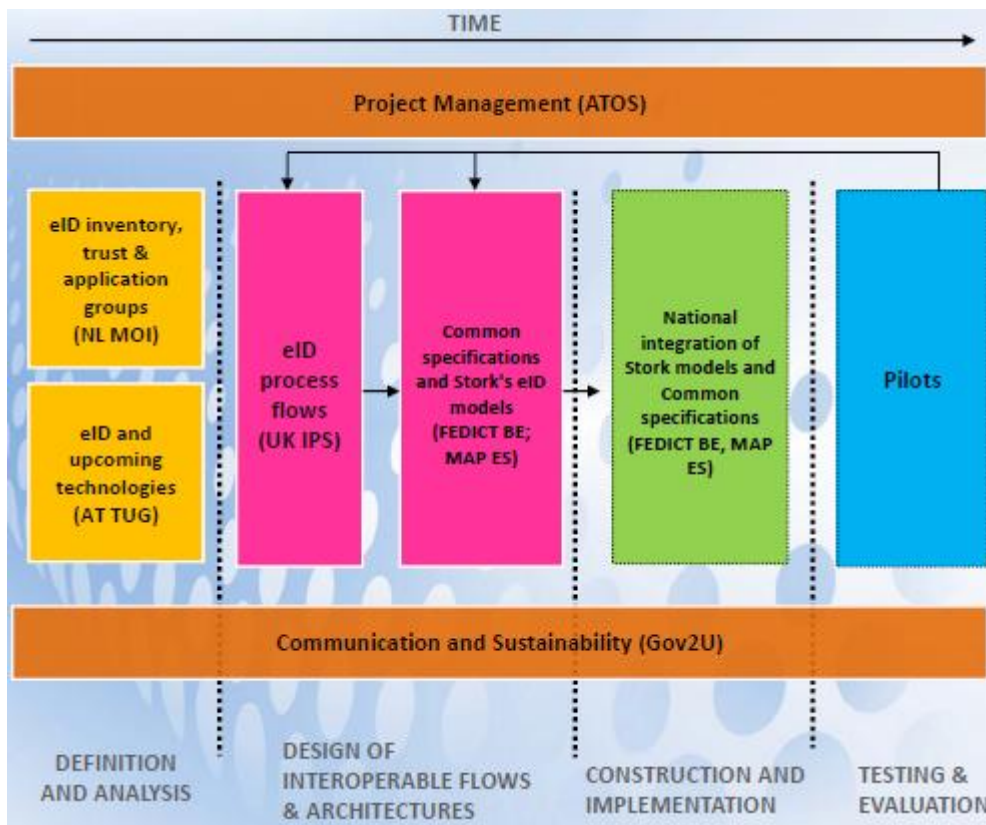


6.9 Διασυννοριακή ασφάλεια μέσα στην Ευρωπαϊκή Ένωση [STORK].

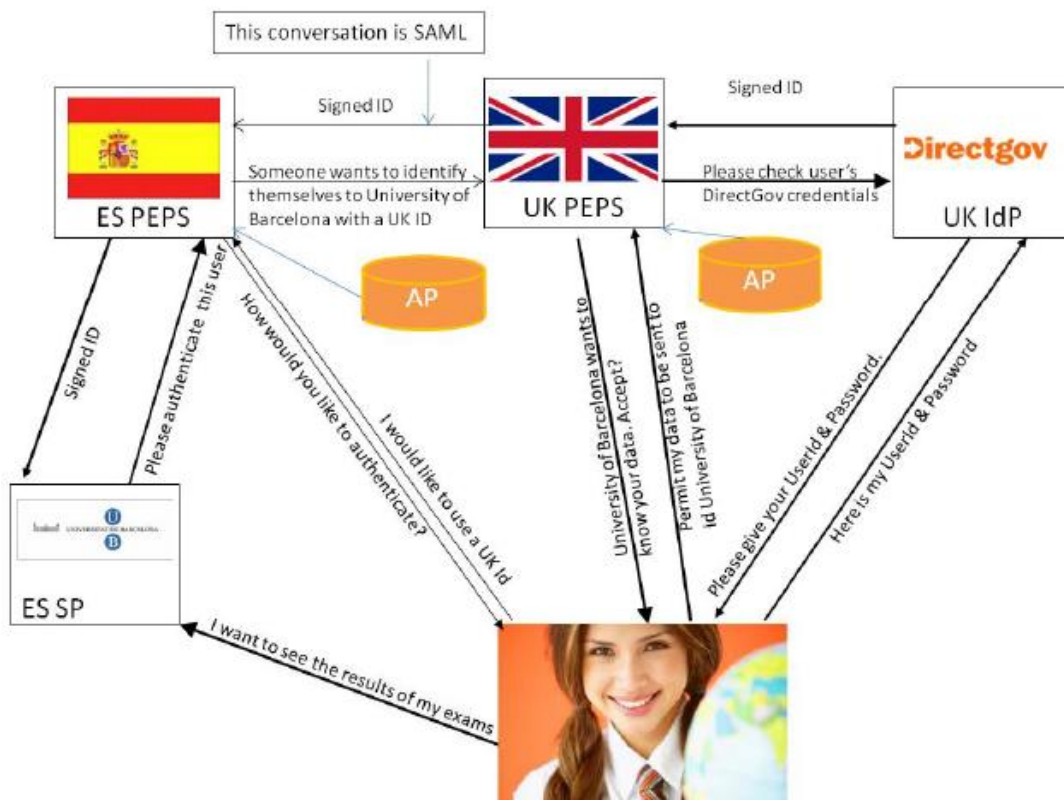
Η εταιρία STORK [25],[29], έχει αναπτύξει ένα σχεδιασμό, προς υλοποίηση ασφαλών συναλλαγών με ηλεκτρονικές ταυτότητες, μεταξύ χωρών που συμμετέχουν. Οι φάσεις ολοκλήρωσης του έργου, περιέχουν τέσσερις βασικούς σκοπούς. Ο πρώτος σκοπός είναι ο ορισμός και η ανάλυση του έργου και των στόχων, ο δεύτερος είναι ο σχεδιασμός διαλειτουργικών ροών και αρχιτεκτονικής, ο τρίτος είναι η κατασκευή και η ολοκλήρωση του έργου και ο τέταρτος οι δοκιμές.

Φυσικά για να μπορεί να ξεκινήσει η υλοποίηση ακόμα και του πρώτου βήματος, θα πρέπει οι χώρες που συμμετέχουν να έχουν ήδη μία εθνική υποδομή για eID πύλες, παρόχους πιστοποιήσεων κλπ

Η γλώσσα που κτίστηκε για την πιστοποίηση και θεώρηση ασφαλούς δεδομένων μεταξύ ζωνών (χωρών, domains κλπ) είναι SAML (Security Assertion Markup Language), ένα στάνταρντ ανοικτού τύπου, βασισμένο στην XML. Αυτή η γλώσσα μπορεί να χρησιμοποιηθεί μεταξύ κρατών για πιστοποίηση των Ευρωπαϊκών eIDs , όπως φαίνεται στα παρακάτω διαγράμματα.



Στην παραπάνω εικόνα φαίνονται οι φάσεις και οι σκοποί για κάθε φάση του έργου.



Στην παραπάνω εικόνα, με χρήση της SAML, φαίνεται ένα παράδειγμα διασυνοριακής συναλλαγής.

Η STORK από το 2009 [25], προσπαθεί να πειραματιστεί και να εφαρμόσει έναν αριθμό έργων, πιλοτικά ώστε να εξάγει πολύτιμα συμπεράσματα. Μερικά από αυτά θα τα αναφέρουμε εδώ, δείχνοντας και τις δυνατότητες της εφαρμογής της eID.

Διασυνοριακή πιστοποίηση.

Στη διασυνοριακή πιστοποίηση αυτό που προέχει είναι η διασύνδεση υπάρχοντων εθνικών πυλών (διαδικτυακών) και υπηρεσιών στην Ευρωπαϊκή Ένωση. Όπου εδώ θα πρέπει να δοκιμαστεί το πλαίσιο εμπιστοσύνης. Να δοκιμαστεί ότι η ολοκλήρωση των διαφόρων συνδέσεων είναι ασφαλής. Έτσι θα μπορούσε να κατασκευαστεί μία Ευρωπαϊκή πύλη, ως οδηγός για ηλεκτρονικές υπηρεσίες και ασφαλές πύλες στην Ευρωπαϊκή Ένωση.

Ασφαλέστερες συνομιλίες μεταξύ πολιτών με τη χρήση των eIDs.

Σε αυτό το έργο ο σκοπός είναι να δημιουργηθεί μία ασφαλής πλατφόρμα για ασφαλέστερο online περιβάλλον, όπου οι άνθρωποι μπορούν να επικοινωνούν χρησιμοποιώντας τις eIDs. Σε αυτό το σύστημα θα μπορούσαμε να φανταστούμε, ότι τα chat – rooms (δωμάτια συνομιλίας), θα έπαιρναν πιστοποίηση ασφάλειας ώστε να γνωρίζει ο πολίτης ότι είναι πιστοποιημένα και ασφαλή. Ιδιαίτερα και αυστηρότερα δωμάτια συνομιλίας για παιδιά και εφήβους.

eID – Φοιτητές – Μαθητές.

Ο σκοπός του έργου είναι η διακίνηση φοιτητών – μαθητών σε όλη την Ευρώπη. Εδώ τα πανεπιστήμια θα πρέπει να προβλέψουν, μέσα σε ένα περιβάλλον ασφαλούς αναγνώρισης των eIDs, να μπορούν να δέχονται φοιτητές – μαθητές άλλων εφάμιλλων χωρών της Ευρωπαϊκής Ένωσης. Ο ρόλος των πανεπιστημίων ολοκληρώνεται στην παροχή αυτής της υπηρεσίας και στην παροχή των χαρακτηριστικών εκπαίδευσης. Οι φοιτητές έχουν πρόσβαση στις πανεπιστημιακές υπηρεσίες, τις οποίες το πανεπιστήμιο πιστοποιεί ότι παρέχει, στο πανεπιστήμιο που έστειλε τον φοιτητή.

eID – Ηλεκτρονική παράδοση

Ο σκοπός αυτού του έργου είναι η διασυνοριακή ηλεκτρονική παράδοση με βάση την υπάρχουσα εγχώρια υποδομή. Το πεδίο εφαρμογής είναι ο ορισμός πλαισίου που θα διέπει τις ηλεκτρονικές παραδόσεις. Επικεντρώνεται σε θέματα που σχετίζονται με την ταυτότητα και εστιάζει στους μηχανισμούς που ορίζουν οντότητες που εμπλέκονται σε όλες τις φάσεις την ηλεκτρονικής παράδοσης.

Αλλαγή διεύθυνσης σε πολίτες της Ευρωπαϊκής Ένωσης.

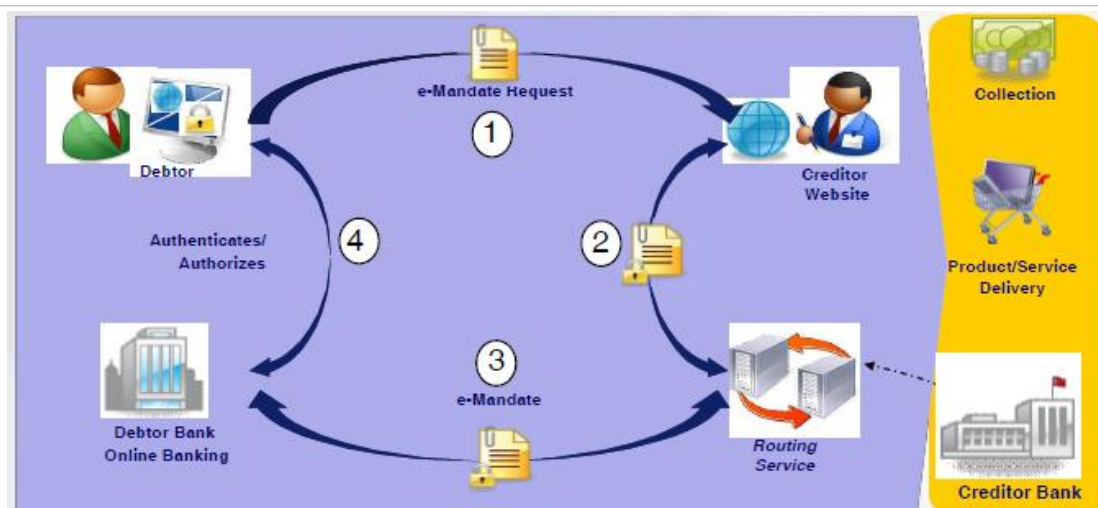
Το συγκεκριμένο έργο απαιτεί τη διασύνδεση όλων των εγχώριων συστημάτων μεταξύ τους, αυτών που είναι μέλη της Ευρωπαϊκής Ένωσης. Η αλλαγή διεύθυνσης θα πρέπει να επισημοποιείται μέσα από το εγχώριο σύστημα και όταν θα αναγνώσουν τα υπόλοιπα συστήματα πληροφορίες σχετικά με τον πολίτη θα ενημερώνονται για τη νέα διεύθυνση.

6.10 Υπηρεσίες PKI.

Είναι αυτονόητο ότι οι υπηρεσίες θα παρέχονται από παντού, η πιστοποίηση θα γίνεται στον πυρήνα και η καταχώρηση – κατοχύρωση στην είσοδο!. Το θέμα πιστοποίησης της ταυτότητας δεν περιέχει μόνο θέματα λογισμικού και υπολογιστών [28],[30]. Περιέχει θέματα όπως εξειδικευμένου ανθρώπινου δυναμικού, εγκαταστάσεων, διαδικασιών, τεχνικών ασφαμάτων και υποστήριξης, εγγράφων, κανόνων, ελέγχων, γνώσεων και εμπειρίας. Όπως η καταχώρηση εμπεριέχει θέματα συλλογής δεδομένων, επικύρωσης, εγγραφής, αναστολής – ανάκλησης της κάρτας, παράδοσης, υποστήριξης.

Υπό του PKI θα πρέπει με ασφάλεια οι υπηρεσίες να υπάρχουν από παντού. Να υπάρχουν online, να εξυπηρετούνται αιτήματα, να δίνονται καταστάσεις σε πραγματικό χρόνο και άμεσα, να υπάρχει ανταπόκριση σε υπογραφή έτσι ώστε να υπάρχει αυξημένη αίσθηση ασφάλειας. Οι παραπάνω υπηρεσίες προαπαιτούν την ύπαρξη μιας αρχής πιστοποίησης **χρονοσφραγίδας**. Ίσως το σημαντικότερο όλων είναι η απόδειξη της ύπαρξης δεδομένων πληροφοριών σε αποδεδειγμένη χρονική στιγμή. Αποδεδειγμένη στιγμή με ακρίβεια χρόνου. Κατά συνέπεια αυτό θα φέρει και αύξηση της νομικής αξίας των ψηφιακών υπογραφών.

Λαμβάνοντας υπόψη της εξειδίκευση των υπηρεσιών PKI τότε μπορούμε να διανοηθούμε την ύπαρξη παρόχων ταυτότητας. Αυτοί μπορούν να χρησιμοποιηθούν από τρίτους συμβαλλόμενους, για εγκρίσεις, διαβεβαιώσεις ταυτότητας κατόχων & για ευκολίες στους κατόχους. Έτσι μπορούν να υπάρξουν κατάλογοι, μηχανές αναζήτησης σε ευρετήρια, κίτρινες σελίδες και βάσης δεδομένων με προσπέλαση από του παρόχους ταυτότητας.



6.11 Ασφαλείς συσκευές δημιουργίας υπογραφής.

Η οδηγία της E.E. για τις ηλεκτρονικές υπογραφές περιέχει απαιτήσεις για ασφαλείς συσκευές δημιουργίας υπογραφής (SSCD), στο παράρτημα III. Στην πράξη μια ασφαλής συσκευή μπορεί να είναι μια έξυπνη κάρτα, ένα usb , μια κάρτα SIM η οποία είναι σε θέση να παράγει ψηφιακές υπογραφές, ήτοι κρυπτογραφημένα checksums.

Για να δημιουργηθεί μία ειδική ηλεκτρονική υπογραφή πρέπει να συμμορφώνεται με το παράρτημα III. (CWA 14169 : 2004 Secure Signature Creation devices "EAL 4+"). Τα βασικά χαρακτηριστικά μιας ασφαλούς συσκευής σύμφωνα με το CWA 14169 είναι:

- Να περιέχει ένα ιδιωτικό κλειδί που χρησιμοποιείτε για την ψηφιακή υπογραφή,
- Δεν πρέπει να περιέχει οποιοδήποτε πιστοποιητικό,
- **Η ψηφιακή υπογραφή προστατεύεται από pin,**
- Οι υπογραφές θα δημιουργούνται από ασφαλές κανάλι,
 - ο Δεν μπορεί να παραχθεί υπογραφή off-line,
 - ο Όλες οι εντολές και η εντολή pin, θα πρέπει να μεταφέρονται online μέσω διακομιστή,
 - ο Ο online διακομιστής, χρειάζεται να χρησιμοποιεί HSM ώστε να μπορεί να υπολογίζει ένα κλειδί ώστε να δημιουργεί ένα ασφαλές κανάλι,
 - ο Το HSM, περιέχει κεντρικά μυστικά για την δημιουργία SSCDs. Κάθε SSCD έχει εξοπλιστεί με ένα HSM.

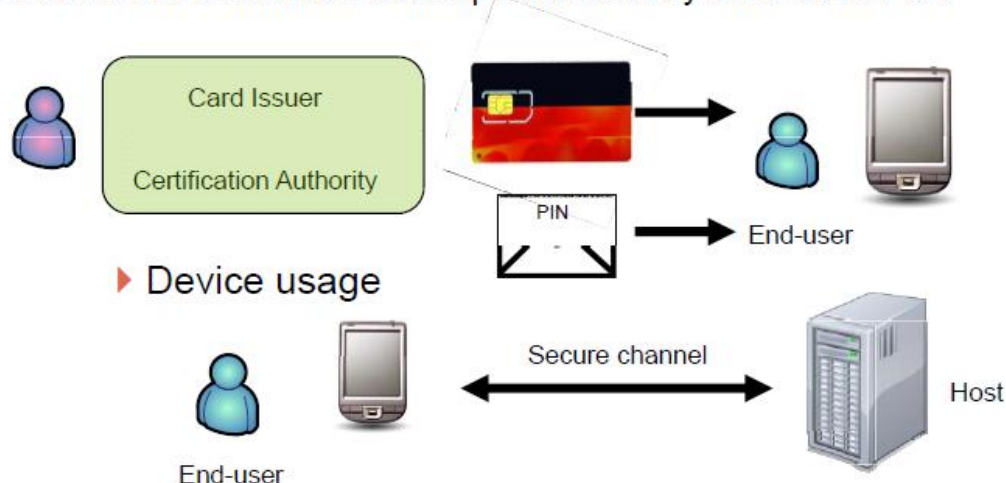
Για να ξεπεράσουμε τους περιορισμούς και να επιτρέπονται:

- **Υπογραφή σε offline κατάσταση,**

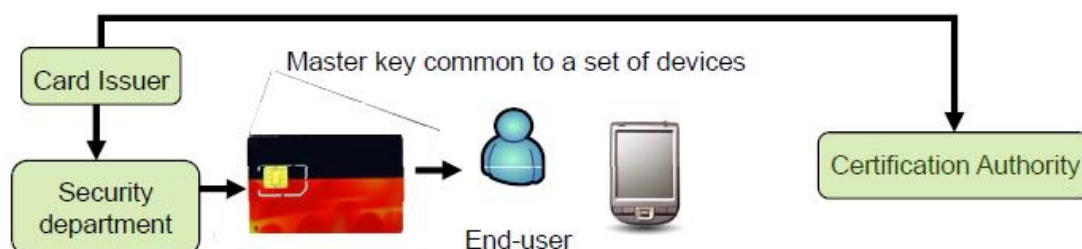
- Να υπάρχουν παραπάνω από ένα ιδιωτικά κλειδιά,
- Να αποθηκεύονται αντίστοιχα πιστοποιητικά στην SSCD,
- Να διαγράφονται και να αποθηκεύονται ιδιωτικά κλειδιά και πιστοποιητικά,
- Να παραδίδεται μία SSCD στον τελικό χρήστη χωρίς κανένα ιδιωτικό κλειδί και πιστοποιητικό μέσα του,

υπάρχουν δύο βασικά σχέδια προτεραιότητας, βάση του κατά πόσο η SSCD, μπορεί α) να δημιουργήσει ένα ζεύγος κλειδών και να εξάγει το δημόσιο κλειδί ή β) να εισάγει το ιδιωτικό κλειδί. Από εκεί και πλέον μπορούμε με πρόσθετα σχέδια να επιτρέψουμε την υποστήριξη και πρόσθετων λειτουργιών[45]. Η συσκευή με την δημιουργία κλειδιού, θα μπορούσε να έχει εφαρμογή πιστοποιήσεων. Μία συσκευή με εισαγωγή κλειδιού δεν μπορεί να έχει εφαρμογή πιστοποιήσεων.

► **Device & PIN distribution: device personalized by Card Issuer / CA**



Αυτό λοιπόν που θα μπορούσε να γίνει είναι, ο εκδότης της κάρτας να επικοινωνεί με την αρχή πιστοποίησης, ώστε να πιστοποιεί τις συσκευές. Ο τελικός χρήστης παίρνει μία συσκευή (σαν έπιπλο) και επιλέγει pin.

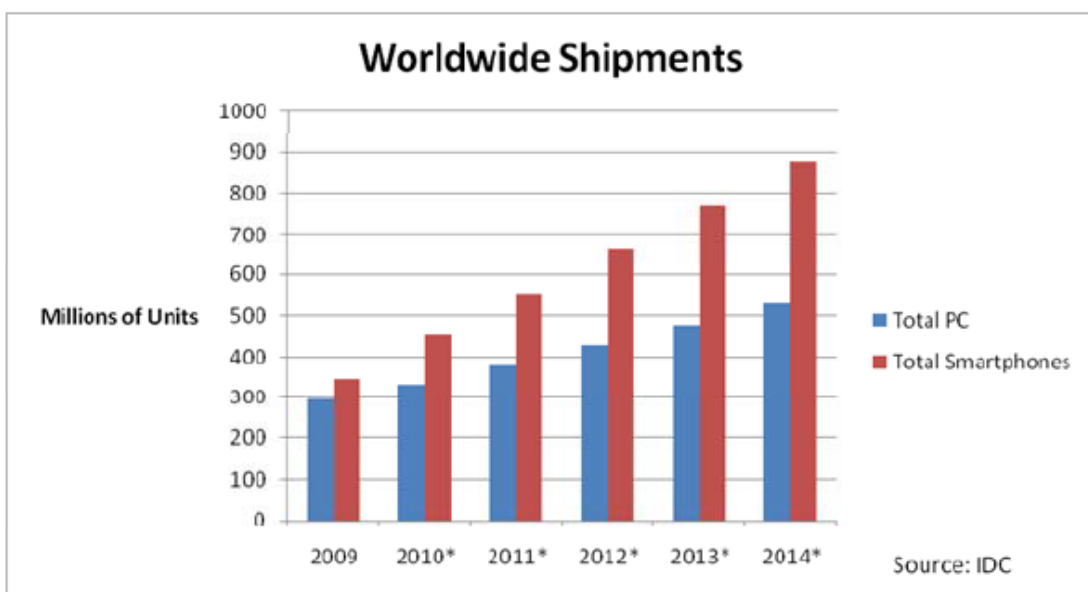


Στη συνέχεια ο χρήστης συνδέεται στην αρχή πιστοποίησης και χρησιμοποιώντας https, η συσκευή δημιουργεί ένα ζευγάρι κλειδών και εξάγει το δημόσιο κλειδί στην

αρχή πιστοποίησης. Ο τελικός χρήστης καταχωρεί τα στοιχεία του και λαμβάνει τον αριθμό καταχώρησής του. Τέλος λαμβάνει από την αρχή το πιστοποιητικό.

6.12 Ασφάλεια και έξυπνα τηλέφωνα.

Στα κινητά η αναγκαιότητα της ασφάλειας είναι δεδομένη, λαμβάνοντας υπόψη ότι πλέον τα έξυπνα κινητά είναι ένας υπολογιστής, πολύ μικρά για να τα χάσεις και ευρείας εξάπλωσης[46].



Και φυσικά λόγω του ότι πλέον η τεχνολογία κλείνει το μάτι στην ταυτοποίηση του πολίτη μέσω κινητού τηλεφώνου, είναι ένα θέμα που θα μας απασχολήσει πάρα πολύ σύντομα. Ας αναλογιστούμε ότι υπάρχουν πάνω από 4.000.000 μολύνσεις στους υπολογιστές, με ρυθμό αύξησης 280% στα Windows, ενώ στα έξυπνα κινητά 106 οικογένειες των 514 παραλλαγών (http://www.securelist.com/en/analysis/204792080/Mobile_Malware_Evolution_An_Overview_Part_3), με μεγάλη αύξηση και σε διαφορετικά λειτουργικά συστήματα.

Λαμβάνοντας υπόψη λοιπόν του 10 αμετάθετους κανόνες ασφάλειας στα κινητά τηλέφωνα θα πρέπει να έχουμε κατά νου :

- Να υπάρχει πάντα ένας δυνατός κωδικός πρόσβασης,
- Η ασφάλεια ενός κινητού μπορεί να επηρεάζει την ασφάλεια πολλών ανθρώπων. Υπάρχουν επιχειρήσεις που τρέχουν διαδικασίες μέσα από κινητά. Ασφαλές κινητό = ασφαλής διαχειριστής.

- Παρακάμπτοντας ενσωματωμένους ελέγχους του λειτουργικού, ενδέχεται να υπονομευτεί η επιχειρησιακή ακεραιότητα και να παρέχει πρόσβαση σε τοπικά δεδομένα,
- Προσοχή στις εφαρμογές,
- Το antivirus δεν είναι του μπαμπά σου,
- Καλύτερα να σπάσουν το κινητό παρά να σπάσουν τα δεδομένα του,
- Τα κρυπτογραφημένα δεδομένα είναι τόσο ασφαλή όσο το κλειδί αποκρυπτογράφησης (δεν πρέπει να αποθηκεύεται τίποτα στο κινητό)
- Πάντα θα υπάρχουν σφάλματα, πάντα θα υπάρχουν άνθρωποι.

6.11 Κλοπή ή απώλεια της κάρτας – Διασφάλιση ασφάλειας.

Κάτι που μπορεί ανά πάσα στιγμή να συμβεί είναι η απώλεια, για οποιοδήποτε λόγω της κάρτας. Αυτό είναι πάρα πολύ επικίνδυνο αν αφορά πρόσβαση σε υπηρεσίες όπως αγορές – πιστωτικής κάρτας υπηρεσίες ή ακόμα ότι η κάρτα θα περιλαμβάνει την απόδειξη της φυσικής παρουσίας του κατόχου (?) της.

Αυτή η ατυχής συγκυρία μπορεί να αντιμετωπιστεί με τους εξής παρακάτω τρόπους.

A. Ταυτοποίηση κατόχου από την ίδια / στην ίδια την κάρτα.

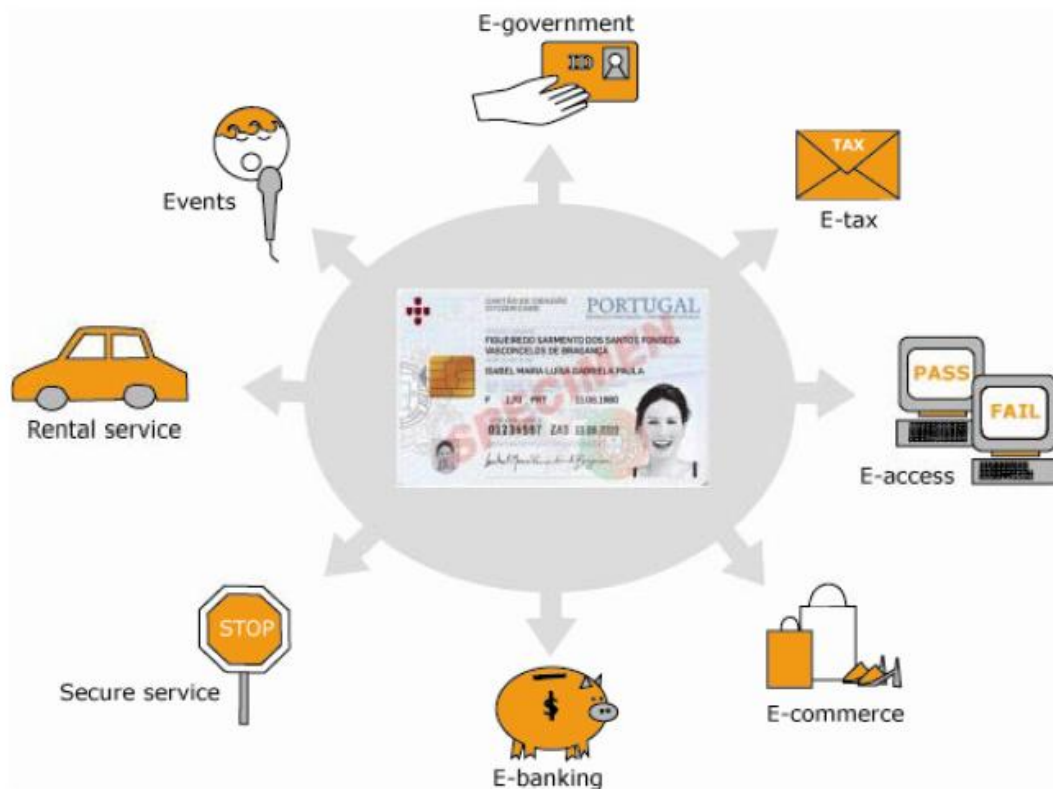
Σε υπηρεσίες που θα πρέπει να διασφαλίζεται η ταυτότητα του κατόχου, για την παροχή της, θα απαιτείτε η διαδικασία match on card, δηλαδή η ταυτοποίηση του κατόχου από/στην την ίδια την κάρτα. Ο τρόπος αυτός ο οποίος αναλύεται στην επόμενη παράγραφο με τίτλο «αποδεδειγμένη ταυτοποίηση», περιλαμβάνει την ταυτοποίηση στην ίδια την κάρτα του δακτυλικού αποτυπώματος του κατόχου. Πριν την παροχή της υπηρεσίας από τρίτους, ο κάτοχος ακουμπάει το δακτυλικό αποτύπωμα στην κάρτα, η οποία κατά την χρήση της επικυρώνει την ταυτότητα του κατόχου της, ότι είναι ο ίδιος ο πολίτης.

B. Δήλωση απώλειας και απενεργοποίηση της κάρτας.

Όπως ακριβώς συμβαίνει η απενεργοποίηση κάρτας από την τράπεζα λόγω απώλειας, με δήλωση από τον κάτοχό της, ο χρήστης θα μπορεί τηλεφωνικά, αποδεικνύοντας ότι είναι ο κάτοχος, να ακυρώνει την κάρτα και να επανεκδίδει νέα άμεσα από την ίδια υπηρεσία ή να απενεργοποιεί την κάρτα του μέσω διαδικτύου με pin και puk.

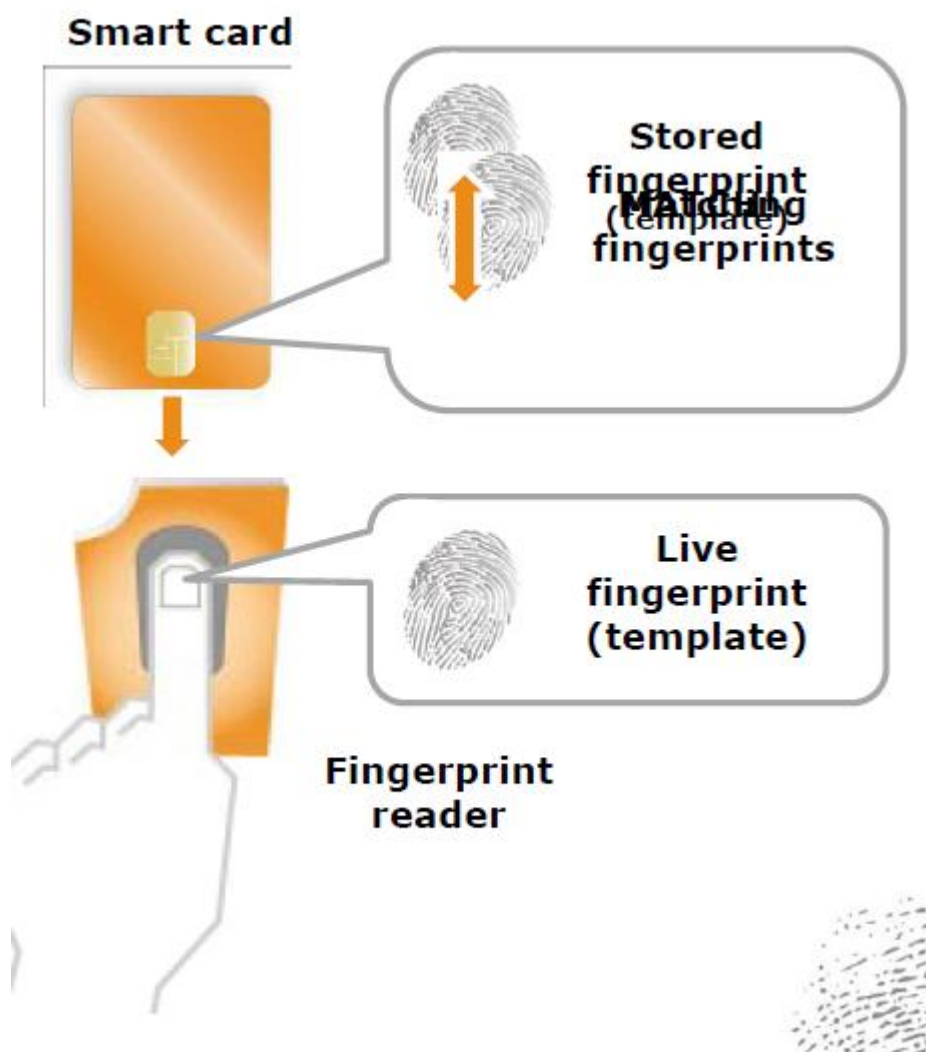
6.12 Αποδεδειγμένη ταυτοποίηση.

Η ηλεκτρονική κάρτα μπορεί να επιβεβαιώνει με τη χρήση της, τη φυσική παρουσία του κατόχου, σε διάφορες περιστάσεις και μάλιστα να τείνει αυξητικά να διευρύνει τη χρήση της.



Περίπτωση 1: Επαλήθευση κατόχου.

Η κάρτα θα μπορούσε να αυτοαναγνωρίζει την αυθεντικότητα του κατόχου του. Για παράδειγμα θα μπορούσε να επαληθεύει το δακτυλικό αποτύπωμα του κατόχου.



Περίπτωση 2: Κυβερνητικό ID.

Το υπουργείο εξωτερικών των ΗΠΑ χρησιμοποιεί την ταύτιση κατόχου μέσω της κάρτας για τους εργαζόμενους σε αυτό.

Στην Ταϊλάνδη, στο υπουργείο εσωτερικών, γίνεται χρήση της κάρτας για τη σύνδεση του χρήστη στον υπολογιστή.

Περίπτωση 3: Χρόνος και παρουσία.

Χρήση βιομετρικών στοιχείων για την πιστοποίηση της φυσικής παρουσίας του κατόχου εκθέτει τα προσωπικά δεδομένα. Η ταυτοποίηση στην κάρτα δεν εκθέτει προσωπικά δεδομένα.

Περίπτωση 4: Τράπεζες και χρηματοοικονομικά.

Οι εργαζόμενοι στην τράπεζα θα μπορούν να συνδέονται στον υπολογιστή τους μέσω της κάρτας , όπως και η πρόσβαση θα γίνεται μέσω της κάρτας. Επιπλέον η τεχνολογία αυτή μπορεί να χρησιμοποιηθεί για την επαλήθευση των συμμετεχόντων σε μία συναλλαγή.

Περίπτωση 5: Ταξίδια και μεταφορές.

Αεροπορικές μεταφορές, εισιτήρια και έκδοση εισιτηρίων, έλεγχος επιβάτη, έλεγχος σε αεροδρόμια.

Περίπτωση 6: Φαρμακεία και υγεία.

Η ενημέρωση ασθενών θα γίνεται μόνο με πιστοποίηση, ώστε να προστατεύεται η προσωπική ζωή. Εάν μέσω της κάρτας διασφαλιστεί η προσωπική παρουσία του ασθενούς μειώνονται οι απάτες.

Περίπτωση 7: Κινητοί έλεγχοι.

Έλεγχος αστυνομίας, κατανομή επιδοτήσεων σε απομακρυσμένες περιοχές, παρουσία προσωπικού έκτακτης ανάγκης είναι μερικά κρίσιμα θέματα που μπορεί να διασφαλίσει την ορθή λειτουργία τους η ταυτοποίηση του κατόχου από την κάρτα.

7ο Κεφάλαιο : Περαιτέρω χρήσεις της κάρτας του πολίτη

Χρήσεις και εφαρμογές πέρα από την κάρτα του πολίτη. Γίνετε προσέγγιση και αναλύονται τεχνικές όπου η κάρτα του πολίτη να αποτελέσει ένα πολύ-εργαλείο – πασπαρτού τόσο για άλλες δημόσιες υπηρεσίες όσο και για ιδιωτικές. Όσο αφορά στις ιδιωτικές, αναλύονται εφαρμογές από iBank μέχρι και προγράμματα δώρων από αεροπορικές εταιρίες.

Δημόσιες και ιδιωτικές υπηρεσίες στην κάρτα του πολίτη – ταυτοποίηση στοιχείων (Δίπλωμα, Aegean, Τράπεζες, Super Market....)

7.1 BankID – Το παράδειγμα της Σουηδίας.

Το BankID είναι μία εθνική λύση ηλεκτρονικής ταυτοποίησης και σήμανσης η οποία παρέχεται από τις Σουηδικές τράπεζες. Μπορεί να χρησιμοποιηθεί από το δημόσιο, ιδιωτικές επιχειρήσεις και τράπεζες. [6],[31]

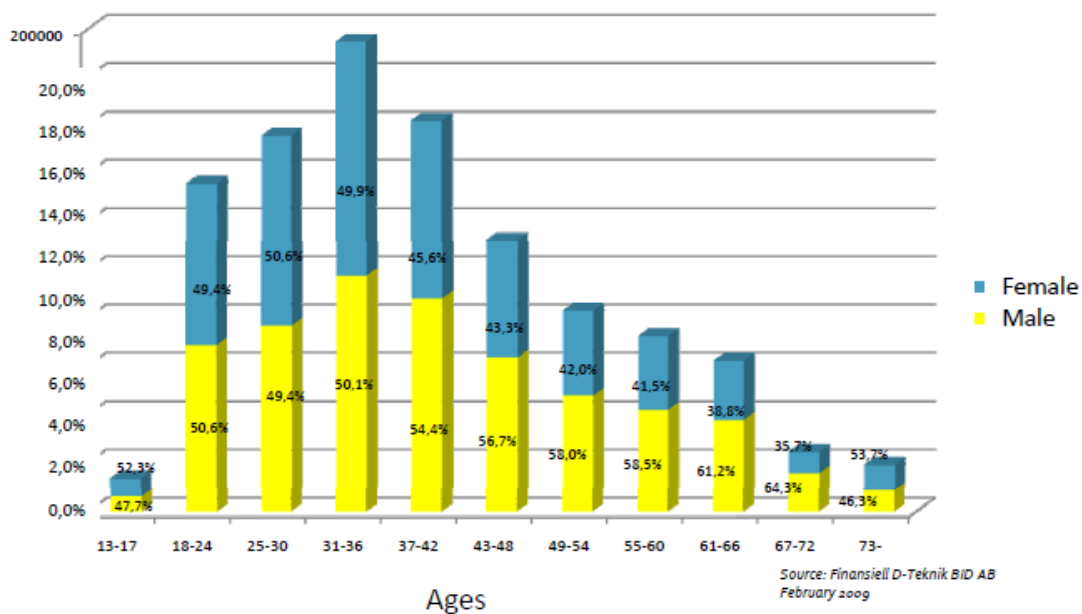
Το BankID είναι μία IT υποδομή η οποία περιέχει διεργασίες και επιχειρηματικό μοντέλο. Έχει αναπτυχθεί ώστε να ικανοποιεί τόσο τις απαιτήσεις της ηλεκτρονικής διακυβέρνησης όσο και την ασφάλεια της τραπεζικής μέσω διαδικτύου. Οι περισσότερες τράπεζες στη Σουηδία έχουν συνδεθεί με την υποδομή για το BankID εδώ και έξι χρόνια.

Κάθε πολίτης δέχεται ένα μοναδικό εθνικό αριθμό ID. Οι τράπεζες χορηγούν BankIDs στους πελάτες τους. Η τράπεζα εγγυάται την ταυτοποίηση του BankID χρήστη (την ύπαρξη). Βέβαια δεν πρέπει να αγνοούμε ότι το 60% των Σουηδών είναι χρήστες διαδικτυακής τραπεζικής.

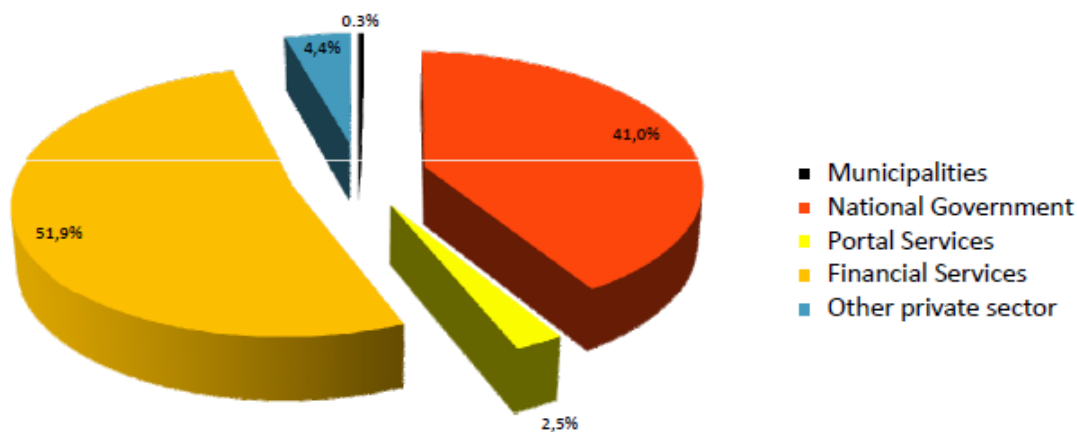
Σύμφωνα με την [6] αναφορά,

- 10 τράπεζες χρησιμοποιούν το BankID
- 2.000.000 μοναδικοί χρήστες
- Περισσότεροι από 5.000.000 πελάτες μπορούν να δεχθούν ένα BankID θέμα,
- Περισσότερες από 500 διαφορετικές web-υπηρεσίες μπορούν να χρησιμοποιηθούν με το BankID,
- 5.000.000 χρήσεις το μήνα,
- Είναι αποδεκτή από το δημόσιο και τις εταιρίες,

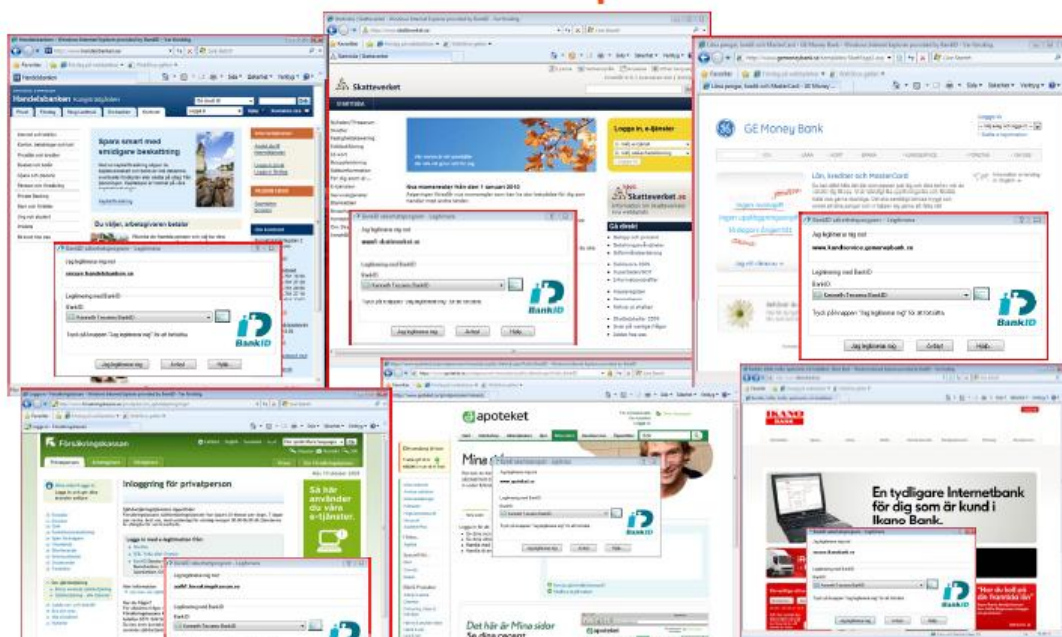
Στο παρακάτω γράφημα φαίνεται το ποσοστό πληθυσμού που χρησιμοποιεί το BankID ανά ηλικία.



Στο παρακάτω γράφημα φαίνονται οι συναλλαγές ανά επιχειρηματικό τομέα.



Σε όποιο web site και αν προσπαθήσει να έχει πρόσβαση ο πολίτης, έχει την ίδια εμπειρία, όπως δείχνει η παρακάτω εικόνα.

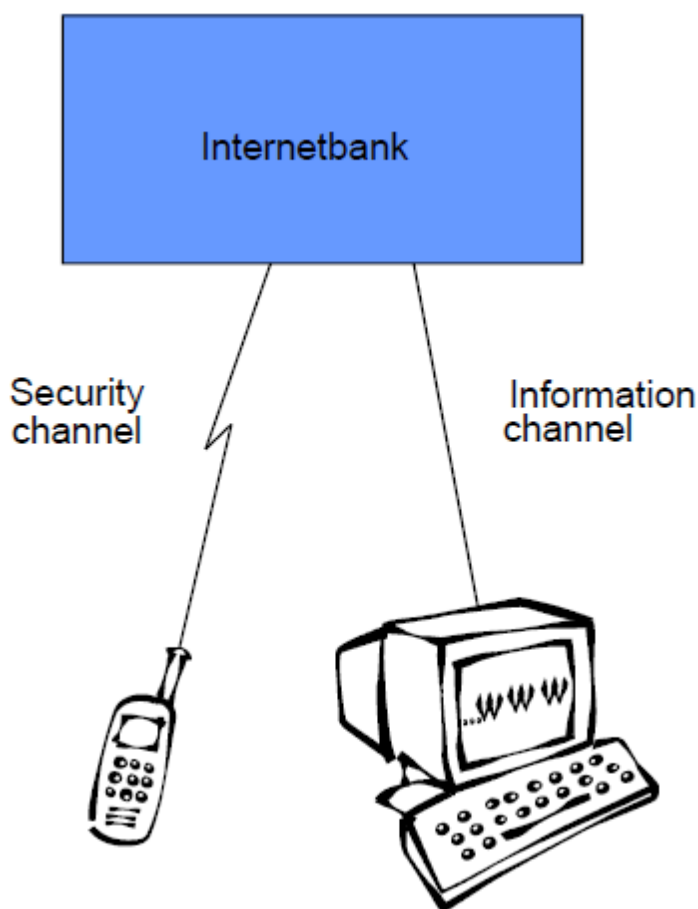


Οι υπηρεσίες που παρέχονται μέσω του BankID είναι:

- Πλήρες διαδικτυακή τραπεζική,
- Επιχειρηματικές αμοιβές υψηλής αξίας,
- Άμεση online πίστωση,
- Υπηρεσίες δήλωσης φόρου,
- Εκτύπωση πιστοποιητικού γέννησης,
- Υπηρεσίες λογιστικής φόρων,
- Εφαρμογές για μείωση φόρων,
- Καταχώρηση νέας μόνιμης ή προσωρινής διεύθυνσης,
- Αίτηση φροντίδας παιδιού,
- Αίτηση σύνταξης,
- Πληροφορίες σύνταξης και σχεδιασμός,
- Αίτηση πιστοποιητικού κατοικίας,
- Καταχώρηση επιχειρήσεων,
- Διευθέτηση βοηθού μελέτης δευτεροβάθμιας εκπαίδευσης,
- Χειρισμός ραντεβού με γιατρό,
- Συνταγογράφηση για φαρμακείο,
- Ανανέωση ιατρικής συνταγής,
- Ανανέωση πιστοποιητικού ασθένειας,
- Απόσπασμα από το μητρώο ασθενών,
- Ιατρικές συμβουλές από νοσηλευτές και ψυχολόγους – ψυχίατρους,

- Δημοτικές υπηρεσίες (Οικογενειακό κέντρο φροντίδας, Προσχολικό, Σχολικό, Φροντίδα ηλικιωμένων)
- Καπ

Η τεχνολογία στηρίζεται στο PKI, με λογισμικό επικύρωσης από έξι (6), οίκους. Επίσης γίνεται χρήση μέσω κινητού, με WPKI με ιδιωτικό κλειδί στην SIM-card. Σχεδόν όλοι οι ενήλικοι έχουν πλέον κινητό το οποίο φέρουν παντού και συνέχεια. Η χρήση του ιδιωτικού κλειδιού γίνεται μέσω της SIM με ένα διαφορετικό κωδικό (password).



7.2 Η χρήση στις τράπεζες γενικότερα.

Σε μία σύγκριση μεταξύ των eID καρτών έναντι των τραπεζικών πιστωτικών καρτών, έχουμε τις παρακάτω διαπιστώσεις [18]:

Electronic ID cards

- Γίνονται όλο και πιο δημοφιλής και ευρείας εξάπλωσης,
- Υποστηρίζουν συναλλαγές με ενεργοποιημένη την απομακρυσμένη πιστοποίηση ασφάλειας ,
- Περιέχουν ευαίσθητα προσωπικά δεδομένα,
- Έχουν έλλειψη διασυννοριακής λειτουργικότητας
- Έχουν έλλειψη ευρείας υποδομής.

Το τραπεζικό σύστημα συναλλαγών έχει αναπτύξει EMV για χρεωστικές και πιστωτικές κάρτες πληρωμών

- Οι οποίες έχουν ευρέως εξαπλωθεί από ότι οι κάρτες του πολίτη,
- Υποστηρίζουν συναλλαγές με ενεργοποιημένη την απομακρυσμένη πιστοποίηση ασφάλειας (EMV-CAP),
- Είναι διαλειτουργικές,
- Υποστηρίζονται από μεγάλες επενδύσεις, από τράπεζες, παραγωγούς, εμπόρους κλπ

Ευκαιρίες

Πιθανή χρήση της Εθνικής κάρτας του πολίτη για τραπεζικές συναλλαγές ή συναλλαγές πληρωμών:

- Οικιακή τραπεζική
- Απομακρυσμένες πληρωμές μέσω διαδικτύου,
- Online καταχωρήσεις για άνοιγμα λογαριασμών ή εγγραφές σε νέες υπηρεσίες πληρωμών, κλπ

ή το αντίστροφο.

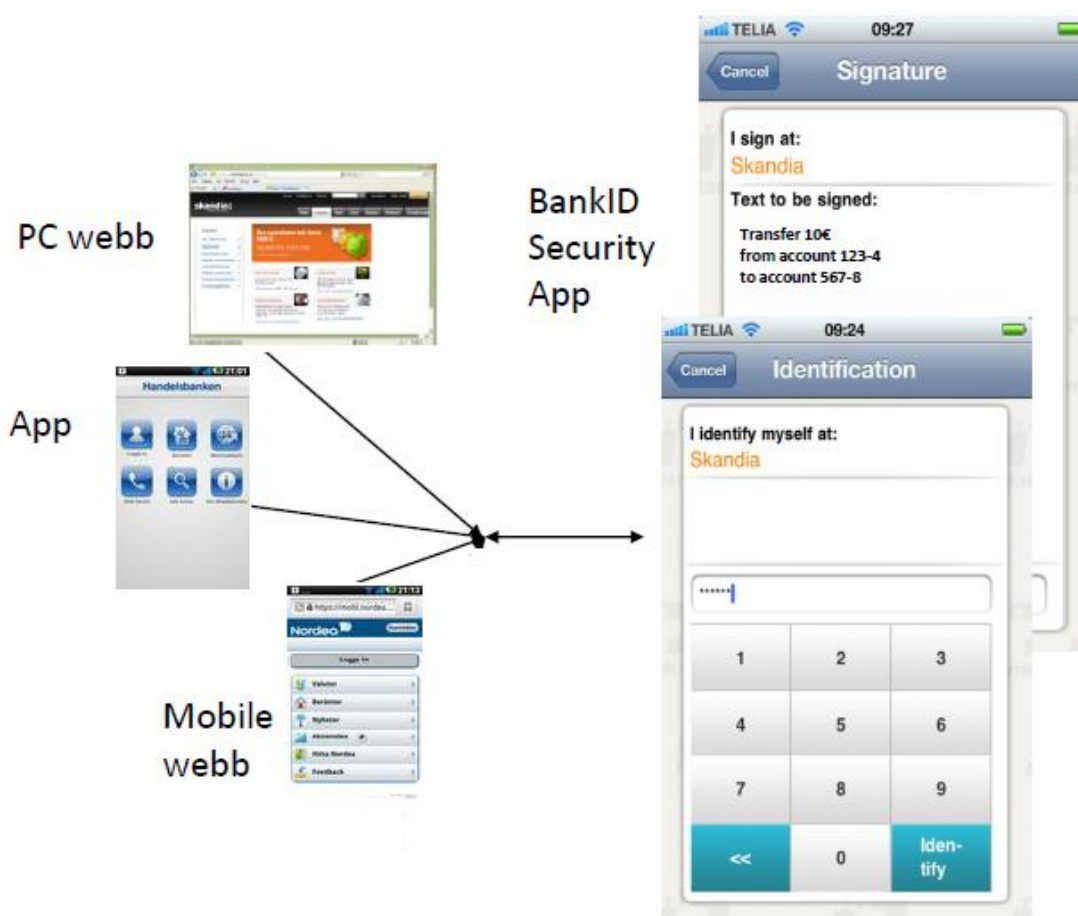
Πιθανή χρήση των EMV καρτών για μη τραπεζικές συναλλαγές:

- Πιστοποίηση για υπηρεσίες ηλεκτρονικής διακυβέρνησης,
- Πιστοποίηση για διαδικτυακές υπηρεσίες,
- Ηλεκτρονική τιμολόγηση,
- ...

7.3 Mobile BankID

Η επέκταση των όσων αναφέραμε παραπάνω είναι οι υπηρεσίες όλες να ολοκληρώνονται μέσω κινητού τηλεφώνου. Με login, pin και φυσικά υπό την προστασία του mobile PKI [35]. Θα μπορούσε να υποστηρίζεται από όλες τις πλατφόρμες, όπως iOS, Android, Windows, Java ME, Blackberry κλπ. Να είναι 90%(?) διαθέσιμο (μόνο θέμα δικτύων xG) κλπ. Σε περίπτωση κλοπής όπως και στην κάρτα θα χρειάζεται επιβεβαίωση pin.

Επιπλέον θα μπορούσαν οι εταιρίες που θέλουν να κάνουν χρήση του eID μέσω mobile PKI, να κατασκευάσουν ειδικές εφαρμογές (client - server) με πρόσβαση στις υπηρεσίες τους, παρά να έχουν μη ασφαλή web sites.



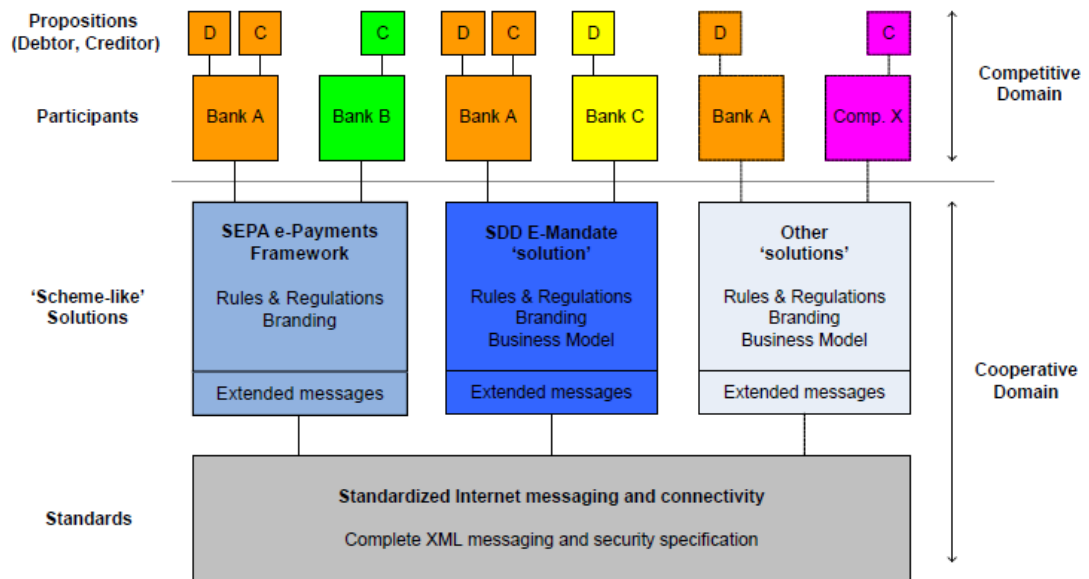


7.4 Διασυννοριακές προδιαγραφές SEPA

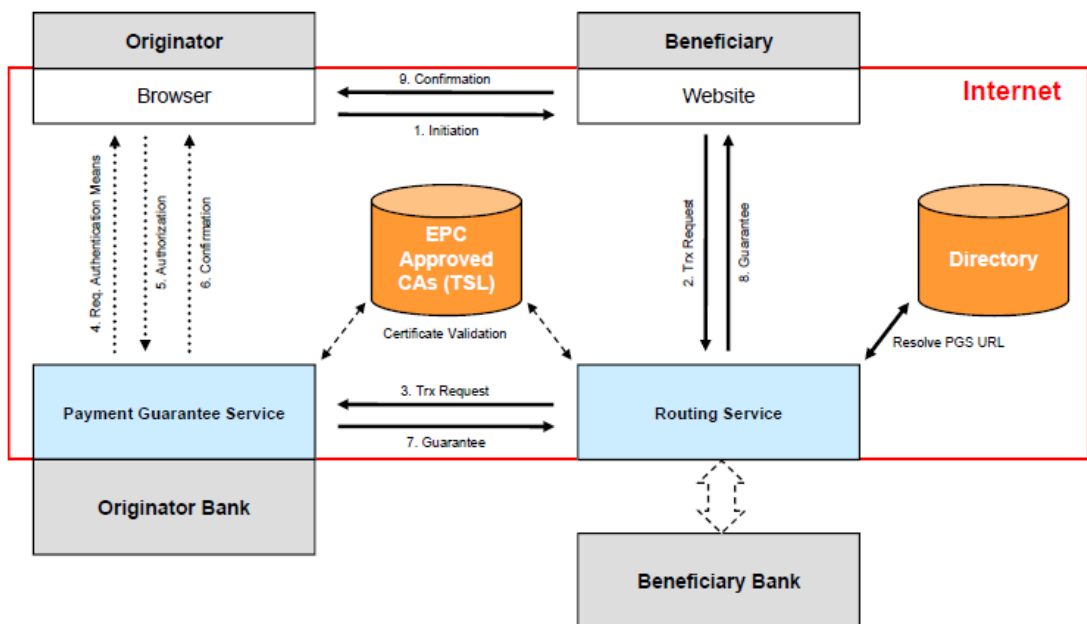
Η χρήση του διαδικτύου για τραπεζικές πληρωμές – συναλλαγές είναι μια βασική δραστηριότητα των Ευρωπαϊκών τραπεζών. Η χρήση των online τραπεζικών συναλλαγών, απαιτούν όπως έχουμε αναφέρει την ασφαλή εξακρίβωση της γνησιότητας των πελατών. Το Ευρωπαϊκό συμβούλιο πληρωμών, εργάζεται για την κατασκευή ενός πυρήνα τυποποιημένων λύσεων ηλεκτρονικών πληρωμών [26] (SEPA, Single Euro Payment Area).

Μία διεργασία ηλεκτρονικής εντολής (e-Mandate) έχει τα εξής χαρακτηριστικά:

- Η ηλεκτρονική εντολή είναι στοιχείο του SEPA. Η ηλεκτρονική εντολή δίνει τη δυνατότητα σε πιστωτές και χρεώστες να εκτελούν εντολές σε πλήρως ηλεκτρονικό περιβάλλον,
- Η διαδικασία συλλογής ηλεκτρονικών εντολών είναι όμοια με τις διεργασίες του πυρήνα,
- Το σύνολο δεδομένων των εντολών και τα μηνύματα ISO 20022 XML συνυπάρχουν στο ίδιο σχήμα,
- Επιτρέπει την πλήρη αποφυγή γραφειοκρατίας,



Το μοντέλο ηλεκτρονικής λειτουργίας κτίστηκε πάνω από το πλαίσιο πληρωμών SEPA και εισαγάγει νέους συμβαλλόμενους ήτοι τις αρχές αρχειοθέτησης και πιστοποίησης.



7.5 Πανευρωπαϊκές υπηρεσίες (Υγείας & Κοινωνικής μέριμνας)

Σύμφωνα με την Ευρωπαϊκή επιτροπή, η δαπάνη για την υγειονομική περίθαλψη στην Ευρώπη, που παρέχεται σε ασθενείς, εκτός του κράτους μέλους στο οποίο είναι ασφαλισμένοι, αντιπροσωπεύουν περίπου :

- Το 1% της συνολικής δημόσιας δαπάνης,
- Περίπου 10δισ€ ετησίως,
- Το 3%-4% των Ευρωπαίων (15εκ άνθρωποι) [36]

Σύμφωνα με την οδηγία 2011/24/EU του Ευρωπαϊκού κοινοβουλίου και της Ευρωπαϊκής επιτροπής, της 9/3/2011, άρθρο 14 για την εφαρμογή των δικαιωμάτων των ασθενών, στη διασυνοριακή υγειονομική περίθαλψη, η Ένωση υποστηρίζει και διευκολύνει τη συνεργασία και την ανταλλαγή πληροφοριών μεταξύ των κρατών μελών που εργάζονται μέσα σε ένα εθελοντικό δίκτυο που συνδέει τις εθνικές αρχές που είναι αρμόδιες για την ηλεκτρονική υγεία που ορίζονται από τα κράτη μέλη.

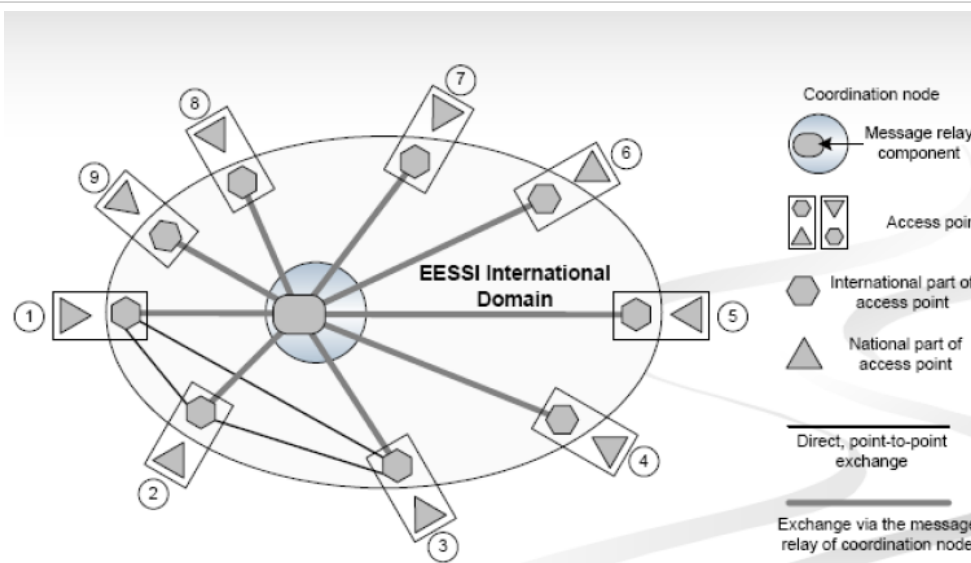
Οι στόχοι του δικτύου e-Health θα είναι:

- (Α) εργασίες για την επίτευξη βιώσιμων οικονομικών και κοινωνικών παροχών των ευρωπαϊκών συστημάτων ηλ-υγείας και των υπηρεσιών και διαλειτουργικών εφαρμογών, με σκοπό την επίτευξη ενός υψηλού επιπέδου εμπιστοσύνης και ασφάλειας, την ενίσχυση της συνέχειας της περίθαλψης και την εξασφάλιση της πρόσβασης σε ασφαλή και υψηλής ποιότητας υγειονομική περίθαλψη? ...
- (Β) Τα κράτη μέλη υποστηρίζουν την ανάπτυξη κοινής ταυτότητας και τα μέτρα ελέγχου ταυτότητας για τη διευκόλυνση της μεταφοράς των δεδομένων στη διασυνοριακή υγειονομική περίθαλψη.

Σύμφωνα με τον EU/EEE 883/04 κανονισμό, ο οποίος εφαρμόζεται από 1/5/2010, οι διασυνοριακές ηλεκτρονικές υπηρεσίες υγείας, διέπονται από τις παρακάτω οδηγίες:

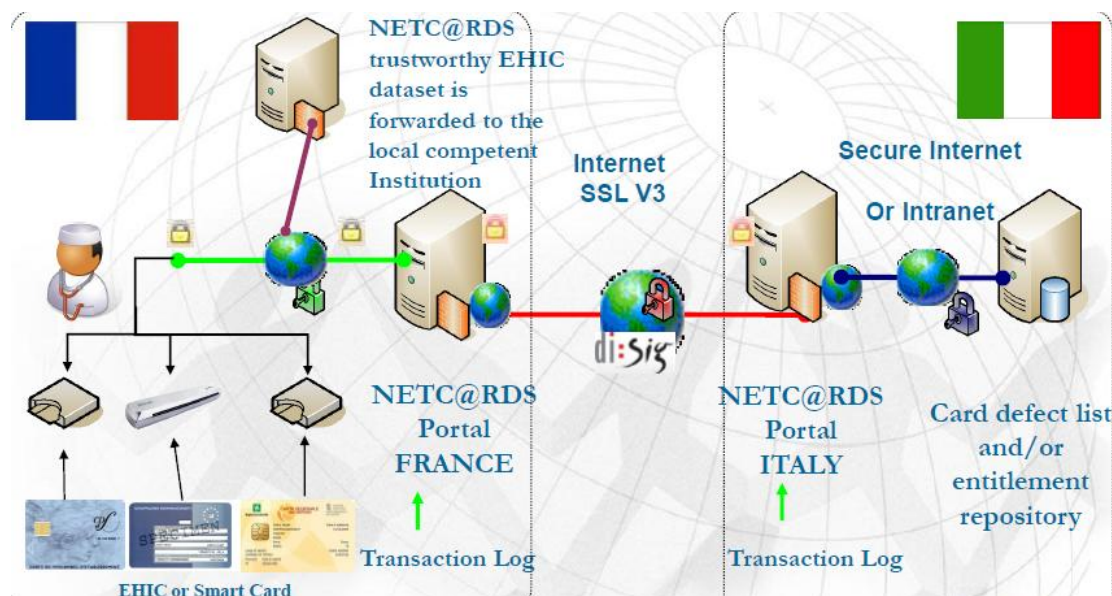
A) Όλα τα έντυπα αιτήσεων, δηλώσεων, που ανταλλάσσονται μεταξύ διοικήσεων αντικαθίστανται από SED (Structured Electronic Documents).

B) Όλα τα SEDs θα ανταλλάσσονται μέσω ασφαλών μηνυμάτων μέσω του TESTA/EESSI (Electronic Exchange of Social Information). Το EESSI βασίζεται σε ασύγχρονα συστήματα μηνυμάτων μεταξύ κοινωνικών οργανισμών.



Στις 1/6/2004 η Ευρωπαϊκή ασφάλιση υγείας, υιοθέτησε την EHIC (European Health Insurance Card). Όποιος δεν έχει μαζί του την EHIC, ένα προσωρινό πιστοποιητικό αντικατάστασης μπορεί να παραδοθεί στον αρμόδιο φορέα.

Παράδειγμα όπου ένας Ιταλός ασθενής λαμβάνει υπηρεσίες υγείας στη Γαλλία:





<http://www.netcards-project.com/hca/gmaps/home.php>

NETC@RDS Healthcare Abroad

Choose Home country & Language:  Ελλάδα (Ελληνικά)

Καλωσήρθατε στο NETC@RDS. Εδώ μπορείτε να βρείτε μια λίστα των Παρόχων Υγειονομικής Περίθαλψης στην Ευρώπη, όπου μπορείτε να χρησιμοποιήσετε την Ευρωπαϊκή Κάρτα Ασφάλισης Ασθένειας σας (ΕΚΑΑ) ως ηλεκτρονικό αποδεικτικό στοιχείο του δικαιώματός σας για υπηρεσίες ιατρικής περίθαλψης στο εξωτερικό.

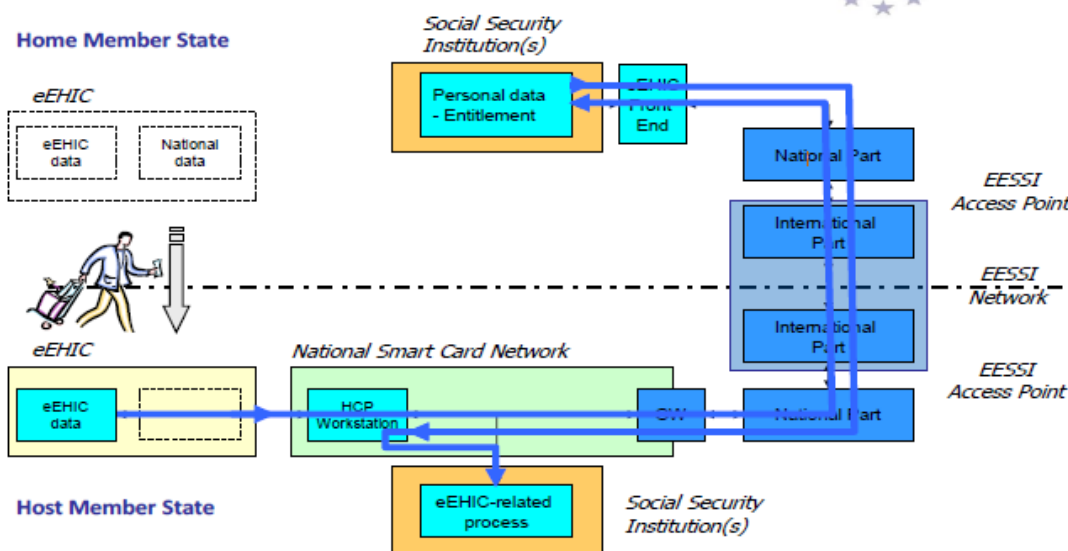
Παρακαλώ επιλέξτε την τοποθεσία σας για να δείτε ποιά σημεία εξυπηρέτησης NETC@RDS υπάρχουν στην περιοχή:

 Αυστρία	 Γαλλία	 Γερμανία
 Ελλάδα	 Ιταλία	 Λίχτενσταϊν
 Ολλανδία	 Νορβηγία	 Ουγγαρία
 Πολωνία	 Ρουμανία	 Σλοβακία
 Σλοβενία	 Τσεχία	 Φινλανδία

Για περισσότερες πληροφορίες σχετικά με το NETC@RDS, παρακαλώ επισκεφτείτε το <http://www.netcards.eu>

Με τη χρήση της ηλεκτρονικής υγείας, μπορούμε να μειώσουμε διοικητικές δαπάνες με τη μείωση χρήσης χαρτιού, ελαχιστοποιούνται οι διαδικασίες πιστοποίησης της προέλευσης του ασθενή, περιορίζει τις απάτες, ενισχύει τις αξιόπιστες πληρωμές, σε βάθος χρόνου θα εξοικονομήσει 200εκ € [36].

Verification of entitlement at the point of care

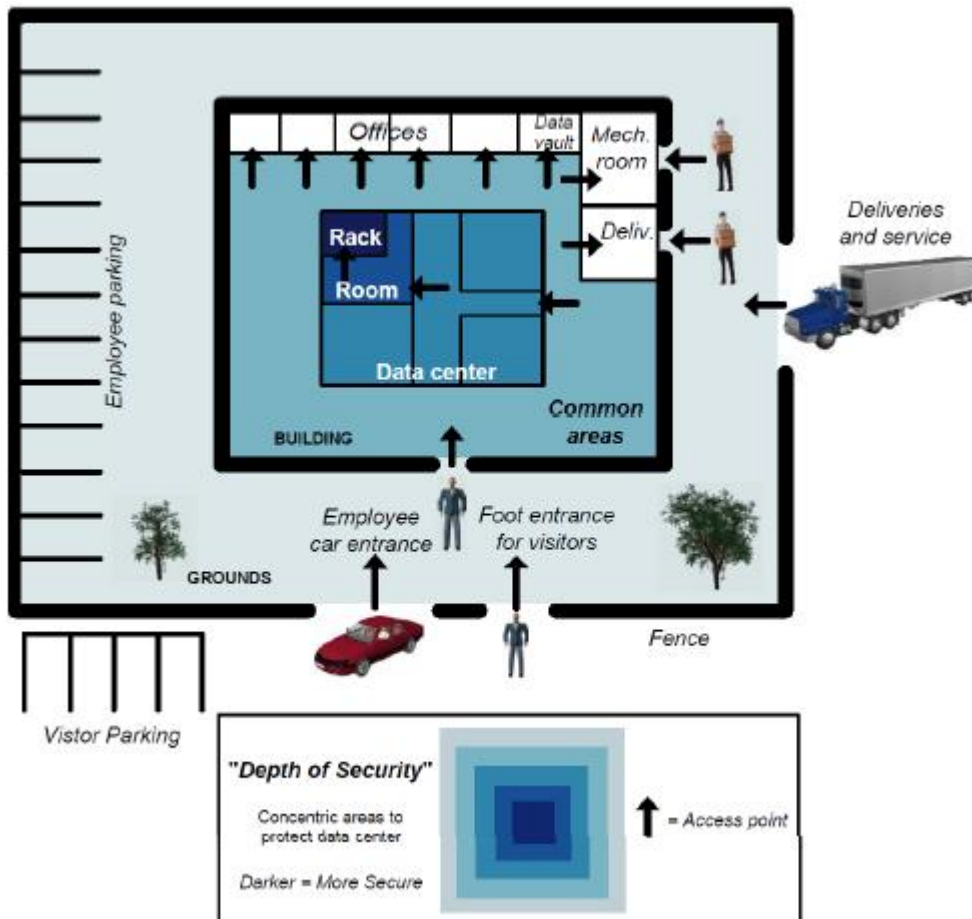


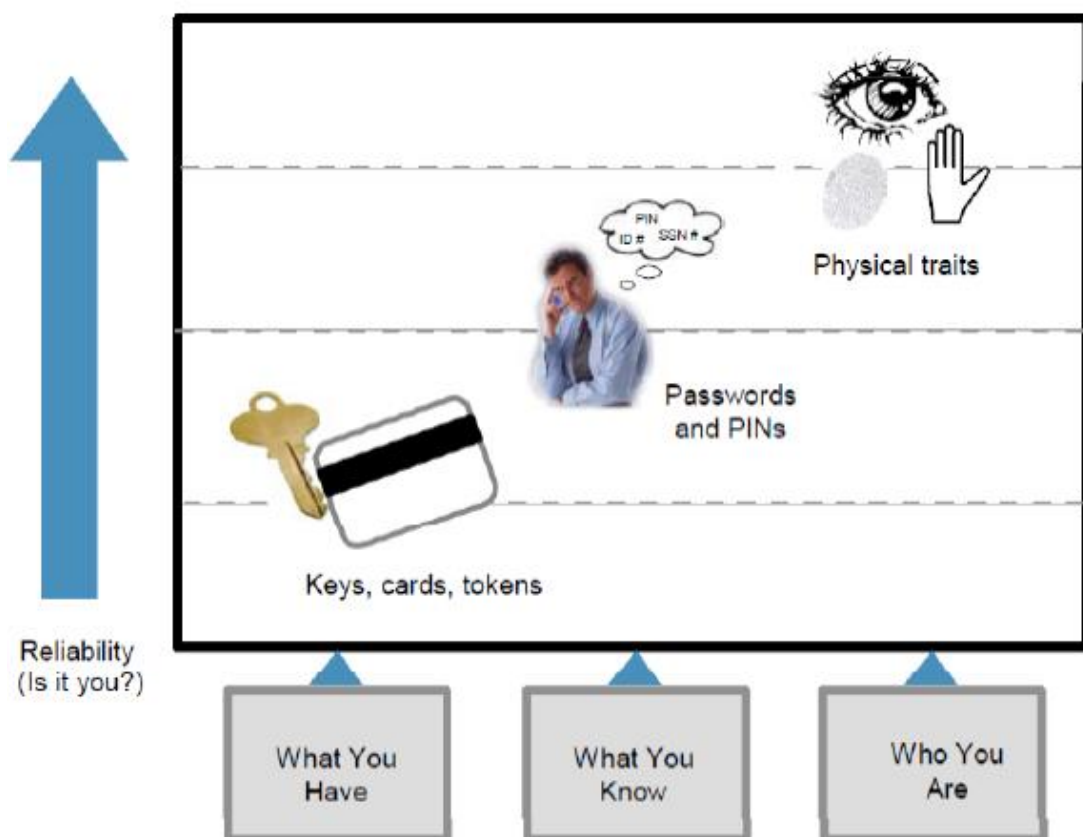
7.6 Ασφάλεια φυσικών χώρων & εγκαταστάσεων

Μία εφαρμογή της κάρτας του πολίτη καθώς θα αναπτύσσετε η χρήση της παντού, είναι η εφαρμογή της στην πρόσβαση χώρων τόσο του ιδιωτικού όσο και του δημόσιου τομέα. Υπάρχουν και σήμερα εφαρμογές με κάρτες για την πρόσβαση σε φυσικούς χώρους, οι οποίες μπορούν να αντικαταστήσουν αυτές με την κάρτα του πολίτη. Μια τέτοια τύπου ελεγχόμενη πρόσβαση, διέπεται από τα παρακάτω κριτήρια πρόσβασης[39]:

- Προσωπική ταυτότητα (ορισμένα άτομα έχουν πρόσβαση σε χώρους σύμφωνα με τη θέση εργασίας)
- Λόγος για να είσαι εκεί (ένας τεχνίτης μπορεί να έχει πρόσβαση μόνο στα μηχανουργεία),
- Οι τεχνικοί δικτύου πρέπει να έχουν πρόσβαση σε χώρους με racks και δίκτυα υποδομών,

- Πληροφορίες (Πρόσβαση σε ευαίσθητες περιοχές, όπου υπάρχουν δεδομένα της εταιρίας, μπορεί να έχουν μόνο δυο – τρεις άνθρωποι).





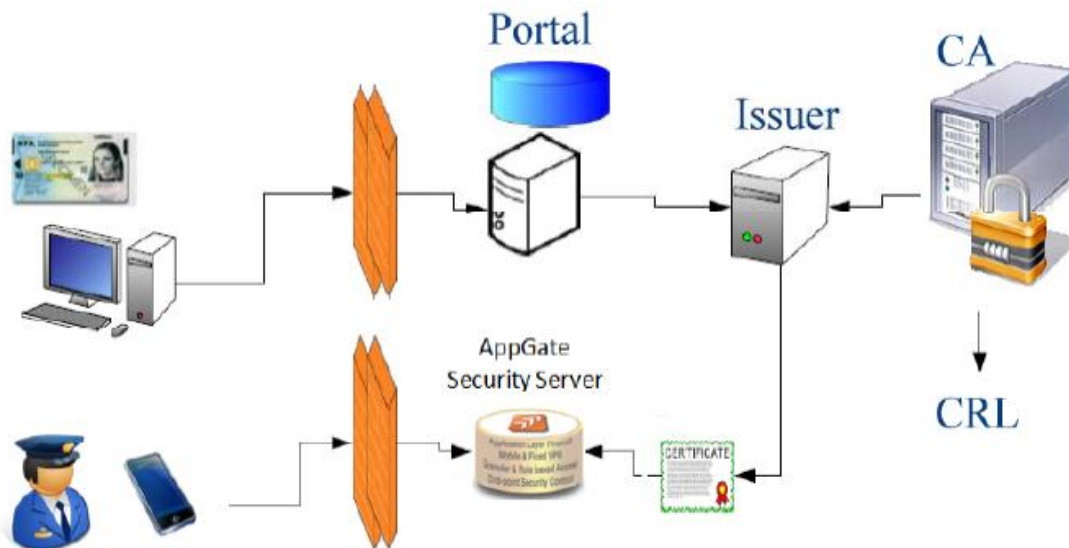
Έτσι λοιπόν για την εφαρμογή των παραπάνω και τη χρήση της κάρτας του πολίτη για πρόσβαση σε φυσικούς χώρους , έχουμε:

- Χρήση ηλεκτρονικής κάρτας του πολίτη,
- Χρήση κωδικών,
- Χρήση Pin,
- Πρόσβαση μέσω υπολογιστών,
- Αναγνώριση πρόσβασης μέσω κάρτας ή σάρωσης βιομετρικών στοιχείων,
- Αναγνώριση μέσω φωνής
- Κλπ

7.7 Κινητό PKI, eID και Σουηδική αστυνομία

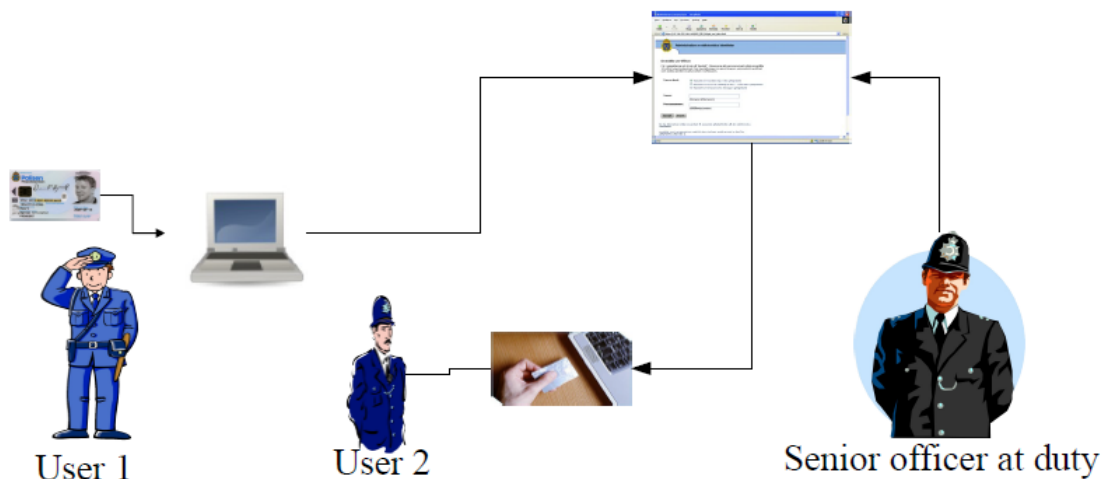
Το AppGate είναι μία εφαρμογή που εγκαθίσταται στον τομέα της άμυνας και σε δύσκολες συνθήκες λειτουργίας. Η Σουηδική αστυνομία χρειάζεται ασφαλή πρόσβαση σε προστατευμένα δεδομένα. Θέλει κρυπτογραφημένες επικοινωνίες και έλεγχο πρόσβασης. Θέλει λεπτομερέστατο αρχείο καταγραφής δραστηριοτήτων. Επιπλέον πρέπει η πρόσβαση να μπορεί να γίνεται με διάφορες συσκευές. Μία

απλή μέθοδος για την εξακρίβωση στοιχείων παρουσιάζεται στο παρακάτω διάγραμμα[41].



Η Σουηδική αστυνομία έχει 25.000 χρήστες [43], 400 γραφεία με 5-1000 χρήστες / γραφείο. Ο στόχος από τη μεριά της αστυνομίας είναι να μπορούν να είναι μετρήσιμες οι δραστηριότητες των πολιτών. Η λύση που εφαρμόζουν είναι να εκδίδουν έξυπνες κάρτες με τον εξής τρόπο:

- A) Ο χρήστης 1 αιτείται μία κάρτα από τον χρήστη 2,
- B) Ο χρήστης 2 βάζει μία νέα κάρτα στον αναγνώστη καρτών,
- Γ) Ο προϊστάμενος γραφείου εγκρίνει την αίτηση,
- Δ) Ο χρήστης 2 εκδίδει την κάρτα,
- Ε) Όλα είναι καταγεγραμμένα.



Τα ωφέλει από την χρήση της παραπάνω διαδικασίας αλλά και όλου του εγχειρήματος είναι:

- Για τους χρήστες
 - ο Μία κάρτα ένα pin,
 - ο Λειτουργίες για κάρτες
 - ο Μία διαδικασία για όλες τις λειτουργίες
 - ο Έκδοση από τοπικά γραφεία
- Για τους οργανισμούς
 - ο Μεγαλύτερη απόδοση
 - ο Χαμηλότερο κόστος
 - ο Καλύτερος έλεγχος
 - ο Βελτίωση της ασφάλειας

Από την άλλη το PKI σήμερα έχει φτάσει σε σημείο όπου είναι εύκολο να το επεκτείνεις (λειτουργικά), έχει πολλές αρχές θεώρησης πιστοποιητικού για διακομιστές, VPN, υπογραφές, ePassports, κρυπτογραφήσεις κλπ. [43]. Ωστόσο στο μέλλον αυτό που πρέπει να επιτευχθεί είναι η προσωπική διαχείριση της κάρτας από το χρήστη, η προσωπική συγκέντρωση πιστοποιητικών, υπηρεσίες αλλαγής κωδικών, ηλεκτρονικές υπογραφές και διακίνηση ηλεκτρονικών εγγράφων.

7.8 Διατριβή – Η αστυνομία Online

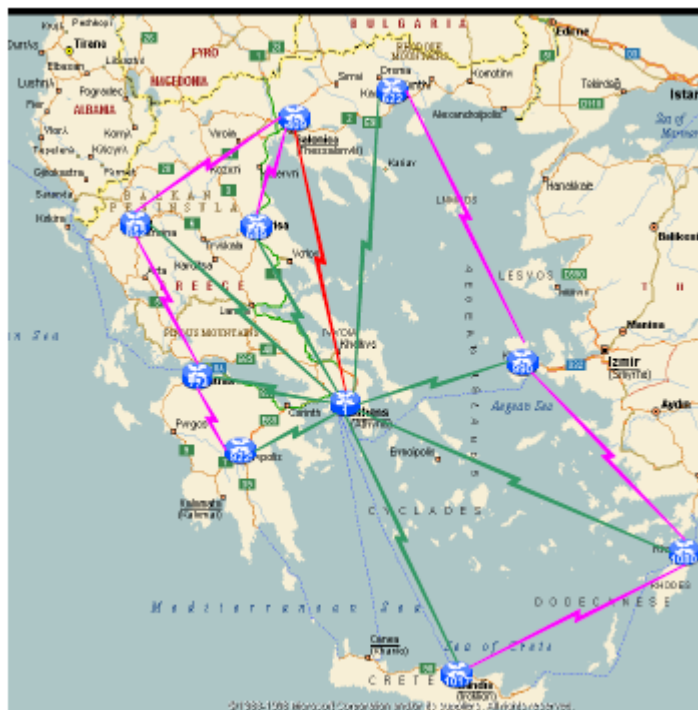
Η αστυνομία online είναι ένα project της εταιρίας Byte Computer S.A., που παρουσιάστηκε από το Νίκο Βεζεριανό στην Κωνσταντινούπολη τον Οκτώβριο του 2011 [48].

Το έργο αυτό περιέχει στοιχεία όπως:

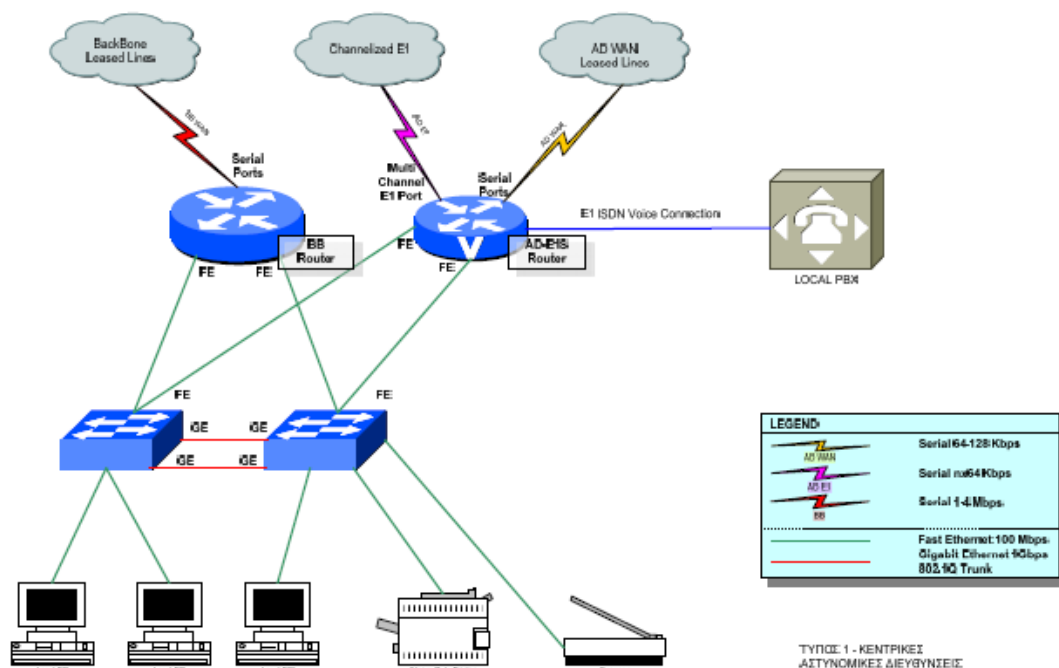
- Πανελλήνιο δίκτυο (δεδομένων και IP φωνής), με 1500 τερματικά σημεία,
- Κέντρο δεδομένων, SAN, NMS, διαχείριση ID,
- Web Based applications,
- 5.000 σταθμοί εργασίας, πάνω από 1500 εκτυπωτές (φαξ και σαρωτές), 6.000 αναγνώστες/προγραμματιστές καρτών,
- Κόστος 23m €,
- Χρόνος εκτέλεσης 24 μήνες.

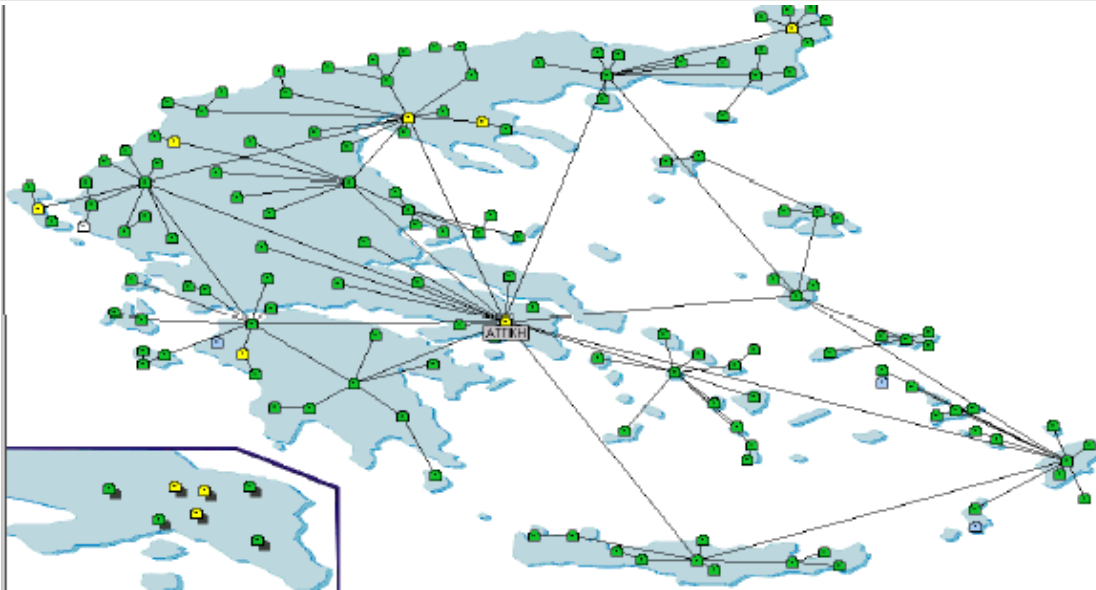
Στο έργο αυτό έχουμε πρόσβαση από οποιοδήποτε σημείο σε οποιαδήποτε εφαρμογή στα κεντρικά γραφεία μέσω του πανελληνίου δικτύου. Έχουμε κεντροποιημένα συστήματα και αποθηκευτικούς χώρους 10TBs. Οι web apps (PolDoc, Asset, Card...) είναι σύγχρονες. Τα δικαιώματα πρόσβασης και η ασφάλεια διέπεται μέσα από κάρτες. Εκδίδονται ψηφιακά πιστοποιητικά αναλόγως της θέσης και το ρόλο του κάθε υπαλλήλου. Κεντρική διαχείριση και κατάλογος χρηστών. Αποστολή μηνυμάτων και εγγράφων από κάθε θέση προς κάθε θέση. Επιπλέον υπάρχει IP τηλεφωνία μέσω του πανελληνίου δικτύου.

Στις παρακάτω εικόνες απεικονίζεται το δίκτυο (ραχοκοκαλιά), ο εξοπλισμός των κεντρικών αστυνομικών διευθύνσεων και ολόκληρο το δίκτυο.



Ραχοκοκαλιά



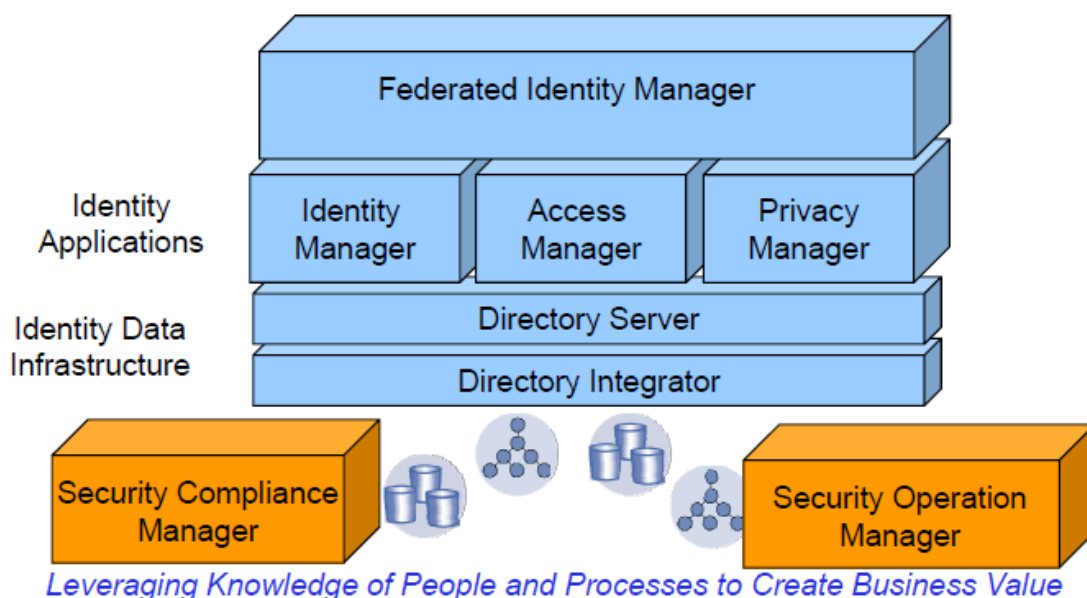


Πάνω από 1500 σημεία.

Για να μπορέσει να υλοποιηθεί όλο αυτό το σύστημα και να λειτουργήσει με ηλεκτρονικές κάρτες και ασφάλεια, χρησιμοποιήθηκε ο παρακάτω εξοπλισμός[48]:

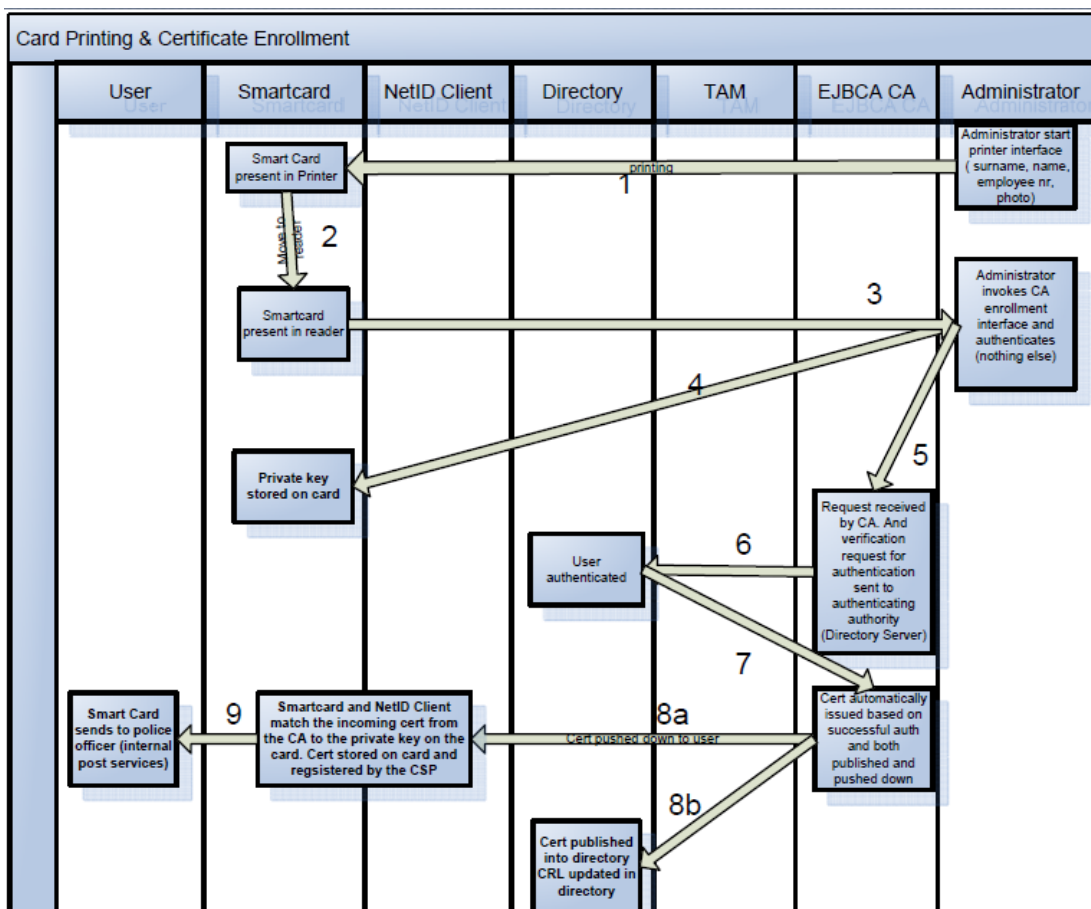
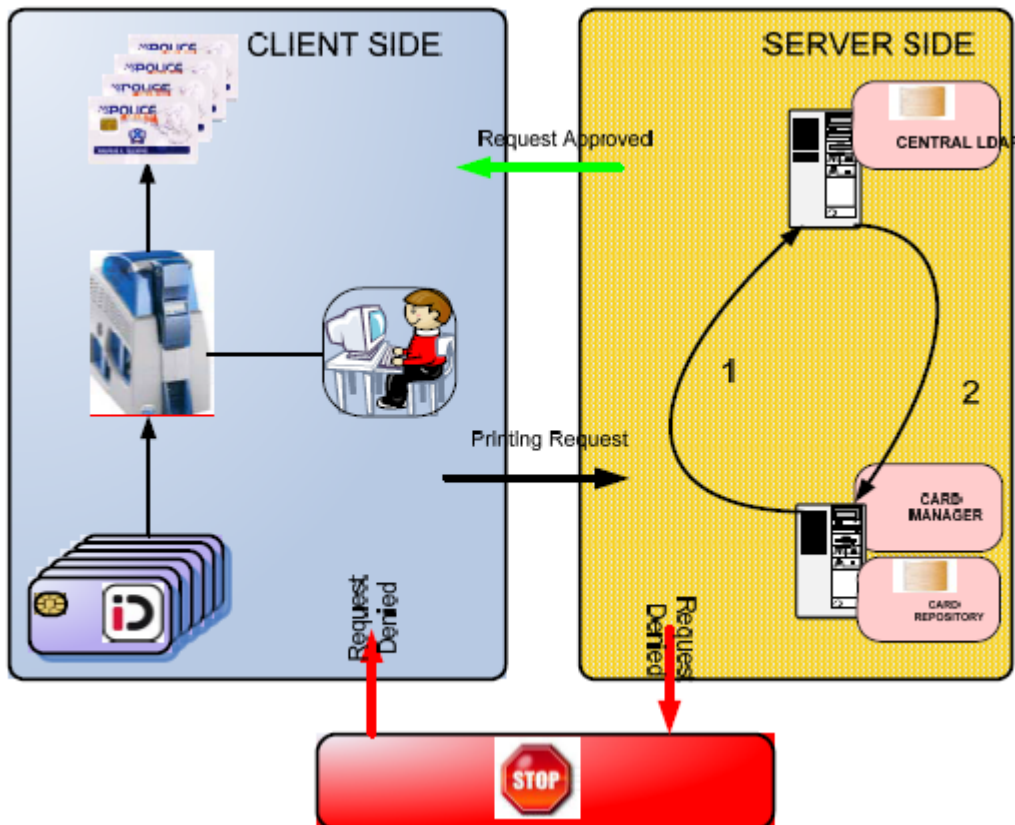
- Cisco, Firewalls, IDS etc
- Samba
- Tivoli
 - Tivoli Identity Manager, TIM
 - Tivoli Access Manager, TAM
 - Tivoli Configuration Manager, TCM
 - Tivoli Directory Integrator, IBM Directory Server
 - Tivoli Agents
- Smart Cards
- **Certification Authority, PrimeKey EJBCA (RSA KEON)**
- **Card Management System, BYTE**
- **PC access client, NetID (RSA)**

Οι βάση ανάπτυξης του domain των χρηστών και του active directory (όπως θα λέγαμε σε Microsoft windows domain controllers), φαίνεται στο παρακάτω διάγραμμα :

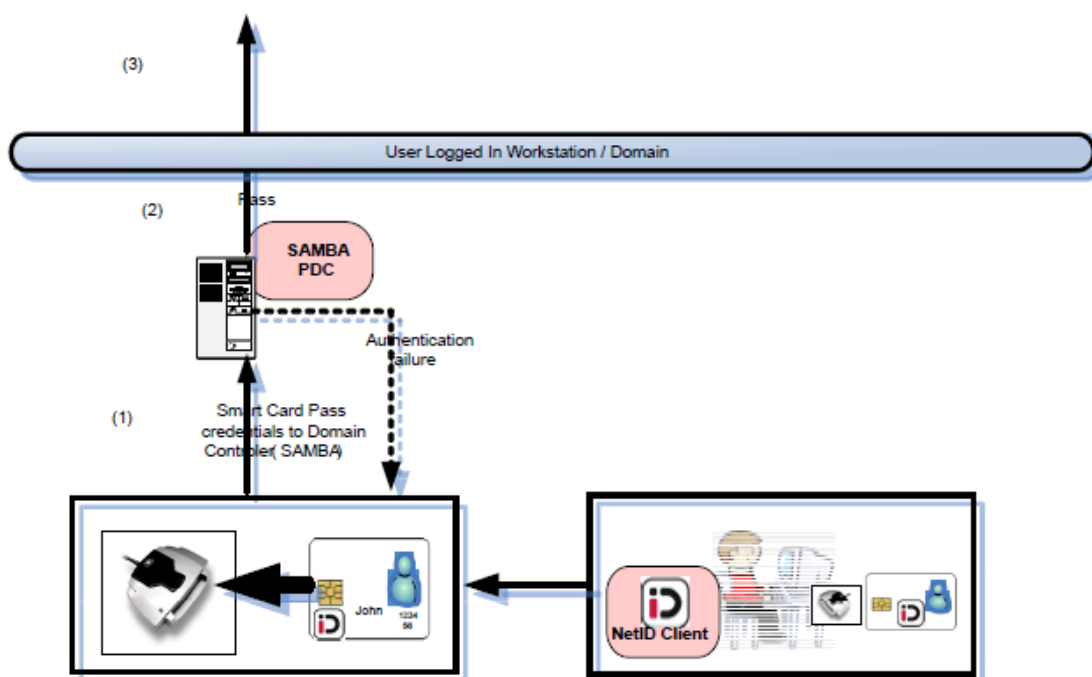


Το σύστημα διαχείρισης καρτών είναι ένα από τα πιο κρίσιμα σημεία. Οι επιλογές που έχει ο διαχειριστής είναι, εκτύπωση καρτών, δημιουργία πιστοποιητικού, ανάκληση πιστοποιητικού, αναστολή πιστοποιητικού, αποκατάσταση πιστοποιητικού, ακύρωση κάρτας, αποδεικτικά pin/puk. Επιπλέον ο διαχειριστής μπορεί να ορίζει χειριστές και να επιβλέπει το active directory.

Στο παρακάτω διάγραμμα φαίνεται η διαδικασία έκδοση και πιστοποίησης της κάρτας οργάνου της αστυνομίας.



Από τη στιγμή που εκδίδεται η κάρτα και τα πιστοποιητικά της και προγραμματίζεται το chip, ο χρήστης πλέον της ενεργοποίησης από τον διαχειριστή έχει πρόσβαση στο σύστημα. Η πρόσβαση γίνεται μέσω ενός αναγνώστη καρτών. Τα στοιχεία πιστοποιούνται από τον SAMBA Domain Controller και ορίζεται το πλαίσιο εργασίας του χρήστη στο σύστημα.

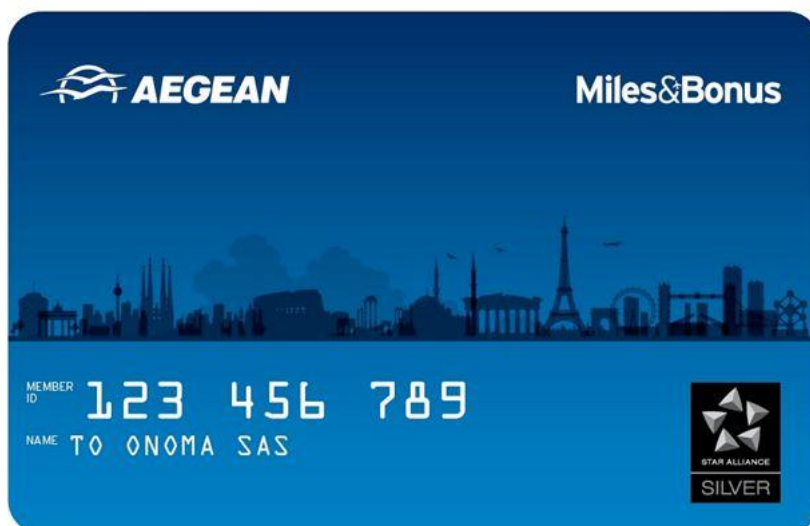


Από εκεί και πέρα υπάρχουν πολλές web εφαρμογές μέσα από την πύλη της Ελληνικής αστυνομίας, όπου μπορεί να κάνει χρήση ο χρήστης. Σε διαβαθμισμένες ενέργειες το λογισμικό μπορεί να ζητάει pin αφού πλέον ο συγκεκριμένος χρήστης έχει δικαίωμα πρόσβασης.

7.9 Αεροπορικές εταιρίες – Super market

Όπως βλέπουμε η χρήση της κάρτας του πολίτη μπορεί να έχει χρήση στην καθημερινότητά μας ακόμα και στο χώρο εργασίας μας, όποιος και αν είναι αυτός. Μπορεί όμως η κάρτα του πολίτη να χρησιμοποιηθεί για καθημερινά πιο απλά πράγματα όπως στα ψώνια στο Super market μέχρι και στα bonus & miles που δίνουν αεροπορικές εταιρίες. Η μόνη διαδικασία που θα επιτρέπεται να γίνεται μεταξύ της ιδιωτικής εταιρίας και του πολίτη, θα είναι η επικύρωση της αυθεντικότητας της κάρτας και την εγγραφής στο μητρώο πολιτών και από εκεί και πλέον όλα τα υπόλοιπα στοιχεία που θα θέλει να κρατάει ο ιδιωτικός φορέας είναι στη δική του

κρίση και στην κρίση του πελάτη αν θα τα διαθέσει. Για παράδειγμα, σε ένα super market ή σε μια αεροπορική εταιρία, θα μπορεί να ζητάτε να αναγνωστεί η κάρτα. Η διαδικασία θα στέλνει ένα validation code στην εταιρία ότι η κάρτα είναι έγκυρη και το eID της κάρτας. Σε αυτό το σημείο (όπως δηλαδή ο αρ. ταυτότητας) η εταιρία θα μπορεί να κρατάει δικό της μητρώο με στοιχεία για τον πελάτη της. Μπορεί να κρατάει μίλια για μπόνους, αγορές για εκπώσεις κλπ.



7.10 Συμπεράσματα

Μπορεί με μεγάλη ασφάλεια να αντικατασταθεί οποιαδήποτε κάρτα έχουμε μέχρι σήμερα (κάρτες), με μόνο την κάρτα του πολίτη. Όταν θα γίνει αυτό και με γνώμονα ότι οι ιδιωτικές εταιρίες θα συνεχίσουν την έρευνα πάνω σε υπηρεσίες λόγω κάρτας, η κάρτα του πολίτη θα γίνει η πιο διαδεδομένη και τεχνολογικά state of the art κάρτα που θα έχει υπάρξει ποτέ.

8ο Κεφάλαιο : Συμπεράσματα

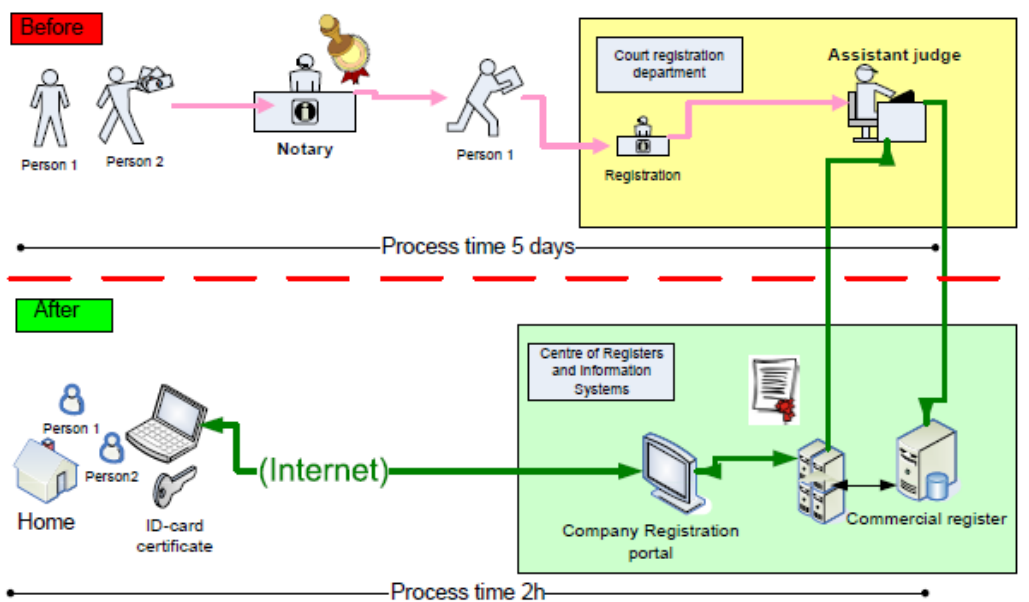
Τέλος, συνοψίζοντας όλα τα παραπάνω, απορρέουν τα ανάλογα συμπεράσματα , όσο αφορά θέματα υλοποίησης, εφαρμογής, χρήσης καθώς και των δυσκολιών που προκύπτουν.

Εφαρμογές – Δυσκολίες – Συμπεράσματα.

Μέχρι εδώ λοιπόν έχουμε δει πάρα πολλές εφαρμογές της κάρτας του πολίτη, τόσο στην ηλεκτρονική διακυβέρνηση όσο και στον ιδιωτικό τομέα. Κλείνοντας αυτή τη μεταπτυχιακή μελέτη, της κάρτας του πολίτη, θα αναφέρω δύο παραγράφους που δείχνουν και αποτελούν συμπέρασμα για τις δυνατότητες και την εφαρμογή της χρήσης της κάρτας του πολίτη στην καθημερινότητά μας και στην Ευρωπαϊκή κουλτούρα των συμπολιτών μας.

8.1 Διασυννοριακή κατοχύρωση εταιρίας.

Φανταστείτε την ίδρυση νέας εταιρίας μέσα σε 12 λεπτά [23]. Αυτό μπορεί να επιτευχθεί με τη χρήση της κάρτας και μίας πύλης κατοχύρωσης και καταχώρησης εταιριών. Από τη μία θέλουμε e-ID με ψηφιακή υπογραφή και χρήση PKI και από την άλλη θέλουμε πρόσβαση στο διαδίκτυο, αναγνώστη καρτών και pin κωδικούς. Με τη χρήση αυτών των τεχνολογιών μπορούμε να ιδρύουμε μέσα σε λίγο χρόνο εταιρίες.



Στο παραπάνω διάγραμμα φαίνεται ότι η σημερινή διαδικασία προϋποθέτει την συνεύρεση των εταίρων, την υπογραφή καταστατικού, την κατοχύρωση της εταιρίας και την θεώρηση από το πρωτοδικείο ή το τμήμα εμπορίου, με φυσική παρουσία των προσώπων ή/και του νόμιμου εκπροσώπου (χρόνος ίδρυσης 5 μέρες).

Σήμερα θα μπορούσε μέσω διαδικτύου να ιδρύεται εταιρία μέσα σε 2 ώρες, από το σπίτι (Όπως στην Εσθονία) [22] (<http://www.rik.ee/>).



e-äriregister
RIK Centre of Registers and Information Systems

COMPANY REGISTRATION PORTAL

Opening page Petitions for entries regarding alteration Petitions for an initial entry Filing of annual reports Submission of the means of communication

1 Preparation of the entry petition Confirmation of the entry petition Payment of the state fee Sending the entry petition

Trader:

Business name: [Enter the name](#)

Business name

Address: [Enter the address](#)

Address:

Capital: [Enter the capital](#)

Share capital Foreign currency

Persons in the entry: [Enter the persons in the entry](#)

Function	Code / Date of birth	Name / business name	Place of residence / seat	Contribution
----------	----------------------	----------------------	---------------------------	--------------

Normal regulation of the right of representation:

The member of the management board:	The member of the management board represents the private limited company alone unless noted otherwise in the commercial register.
Procurator:	The procurator represents the private limited company in all legal acts related to economic activities alone unless noted otherwise in the commercial register. The procurator may transfer or encumber an immovable if this right is noted in the commercial register.

Specifications of the right of representation: [Enter the conditions of the right of representation](#)

Type	Contents
------	----------

§ Legal form:

Name
Private limited company

Financial year: [Enter the financial year period](#)

Start of a financial year End of a financial year

Articles of association: [Enter the articles of association](#)

Date of approval	Date of alteration	Explanation	PDF document
------------------	--------------------	-------------	--------------

Persons outside the entry: [Enter the persons outside the entry](#)

Function	Code / Date of birth	Name / business name	Place of residence / seat
----------	----------------------	----------------------	---------------------------

Founders: [Please enter the capital](#)

Code / Date of birth	Name / business name	Place of residence / seat	Contribution
----------------------	----------------------	---------------------------	--------------

Means of communication: [Enter the means of communication](#)

Type	Contents
------	----------

Planned principal activity: [Enter the planned principal activity](#)

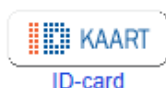
EMTAK Area of activity

Additional documents to be submitted with the entry petition: [Add a document](#)

ID	Type	Name	Size
----	------	------	------

Μέχρι σήμερα στο Portal αυτό, γίνονται δεκτές ηλεκτρονικές κάρτες από διάφορες χώρες, όπως φαίνεται παρακάτω αλλά και στην επίσημη ιστοσελίδα:

Authenticate with ID-card or Mobile-ID:



Enter by foreign ID-card or Mobile-ID:



Finnish ID-card



Portuguese ID-card

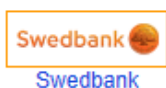


Belgian ID-card



Lithuanian Mobile-ID

Authenticate through an internet bank:



Swedbank



SEB bank



Krediidipank

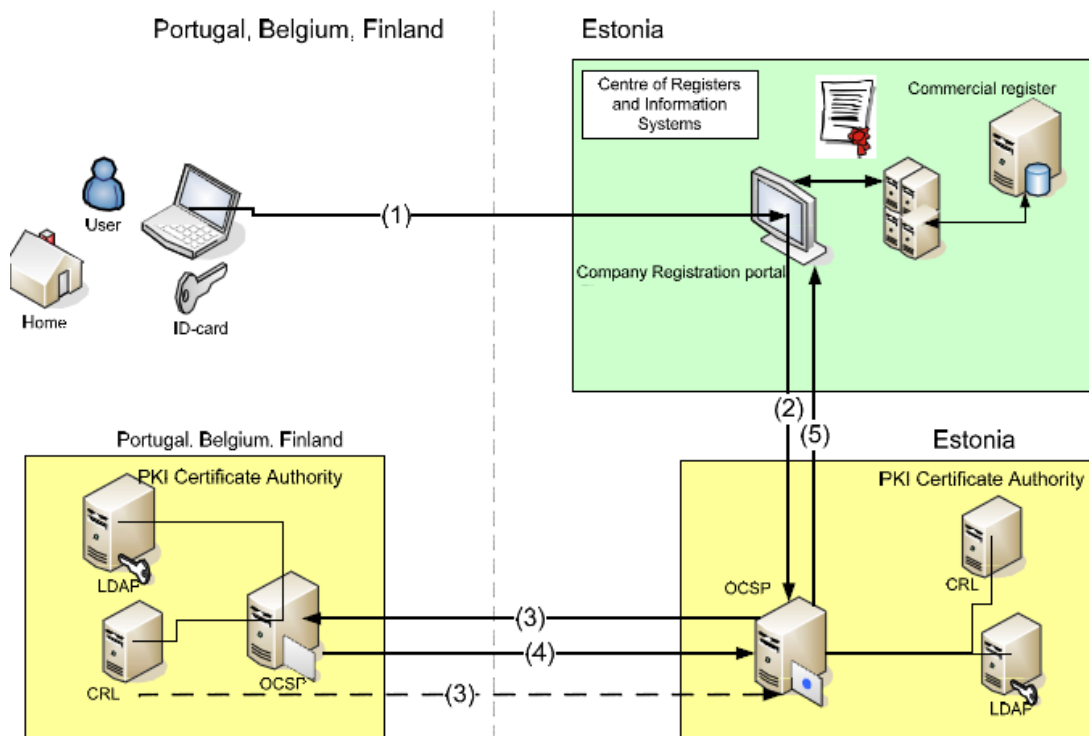


Sampo bank



Nordea bank

Ο τρόπος πιστοποίησης καρτών γίνεται μέσω διαδικτύου, μέσω της αρχής PKI πιστοποίησης, όπως εμφανίζεται παρακάτω:





Belgium ID-card Portuguese ID-card Finnish ID-card Lithuanian Mobile-ID

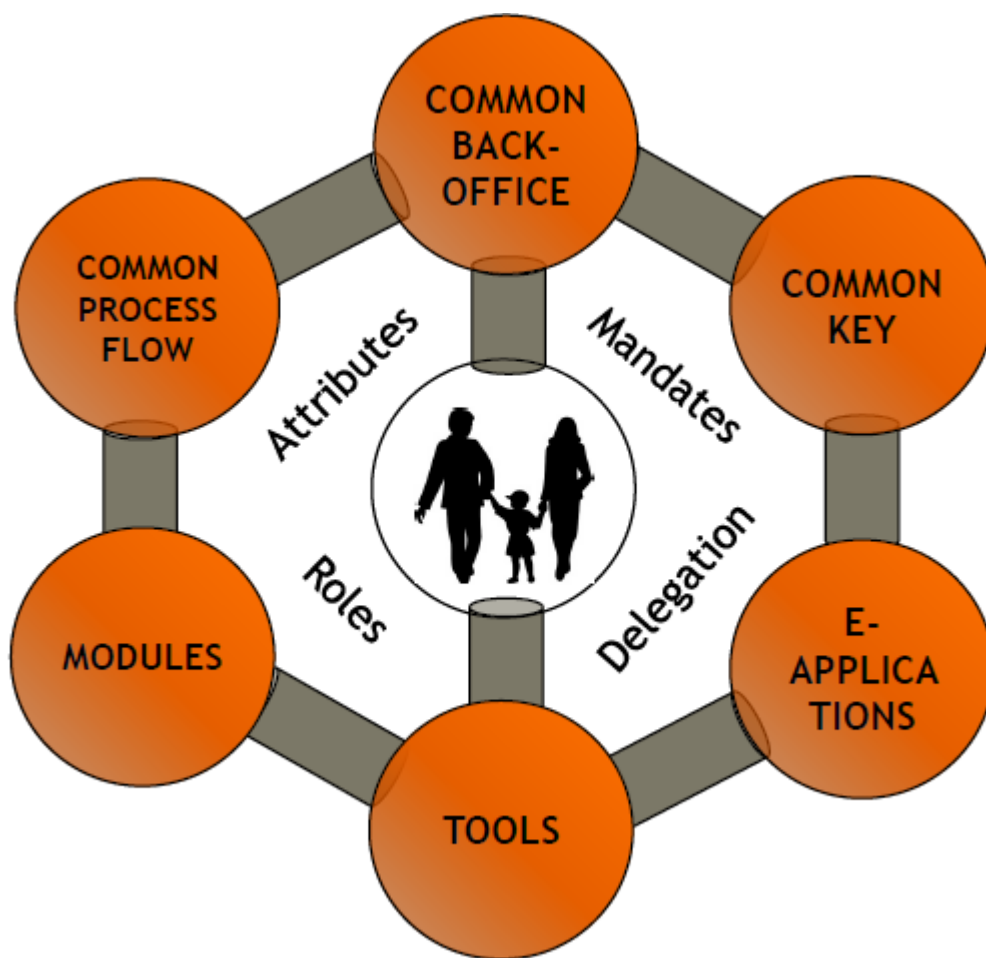


Από νομικής πλευράς θα πρέπει να αναλυθεί και να καθοριστεί το θεσμικό πλαίσιο. Θα πρέπει να οριστεί η διαδικασία αξιολόγησης της ψηφιακής πιστοποίησης και της ασφαλούς συλλογής και αποθήκευσης πληροφοριών.

8.2 Επιτυχείς eid & e-gov υπηρεσίες στο Βέλγιο

Το σύστημα διακυβέρνησης στο Βέλγιο είναι πολιτοκεντρικό. Σε ένα εθνικό website portal υπάρχει η διασύνδεση όλων των υπουργείων και των υπηρεσιών τους [40].





Στο Βέλγιο εφαρμόζεται μία παρόμοια λογική χρωματισμού καρτών, όπως αυτή που προτείνουμε και εμείς σε αυτή τη διατριβή. Η Λευκή κάρτα για πολίτες άνω των 12 ετών, πράσινη κάρτα για παιδιά κάτω των 12 ετών και ροζ κάρτα για ξένους μετανάστες.



► Belgian citizens >12 years old



► Children <12 years old



► Foreign residents

Οι κάρτες αυτές, διέπονται από πολλές υπηρεσίες όπως, υπηρεσίες υγείας, άδεια οδήγησης, κάρτα φοιτητή, οικιακή τραπεζική, απόδειξη μέλους, ηλεκτρονικό εμπόριο κλπ.



Vending machines

- No alcohol under 18 year...



Υπάρχει software Που εγκαθίστανται στον υπολογιστή σας, το οποίο μπορεί με ένα αναγνώστη καρτών να έχει πρόσβαση σε πολλές εφαρμογές.



1. Install the eID software



2. Connect the card reader to the computer



3. Consult your data

Υπάρχουν πληθώρα sites στο internet για το Βέλγιο, όπου κάνουν χρήση της ηλεκτρονικής κάρτας για την παροχή πολλαπλών υπηρεσιών τόσο στον ιδιωτικό

όσο και στο δημόσιο τομέα. Επιπλέον η κάρτα του πολίτη θα μπορούσε όπως και στο Βέλγιο να αντικαταστήσει μία σειρά από κάρτες (τράπεζας, οδήγησης, κάρτα μέλους ιδιωτικής επιχ. κλπ)

Θεωρώ ότι το παράδειγμα του Βελγίου είναι ένα πετυχημένο παράδειγμα εφαρμογής που θα μπορούσαμε να το δούμε και εμείς εδώ στην Ελλάδα.

Αναφορές.

Συνέδρια

[1] Lisbon 22-23 Οκτωβρίου 2009



22 - 23rd of October 2009,

Lisbon, Portugal

[2] Athens 21-22 Οκτωβρίου 2010



21 - 22nd of October 2010,

Athens, Greece

[3] Istanbul 24-25 Οκτωβρίου 2011



Ομιλίες

[4], Ομιλία του *José I. Toscano, Board Member, MULTICERT and INCM*, στο συνέδριο της Λισσαβόνας [1], 22/10/2009

[5], Ομιλία του *Alexandre Caldas - Director (CEGER - Centro de Gestão da Rede Informática do Governo)*, στο συνέδριο της Λισσαβόνας [1], 22/10/2009, CEGER, CENTRO DE GESTÃO DA REDE INFORMÁTICA DO GOVERNO, Management Center for the Electronic Government Network, Rua Almeida Brandão, 7, 1200-602 Lisboa, PORTUGAL, Telefone: +351 21 3923400, Fax: +351 21 3923499, E-mail: info@ceger.gov.pt, Homepage: <http://www.ceger.gov.pt>

[6], Ομιλία των *Gunnar Claesson (Bankgirocentralen BGC AB) and Kenneth Tessem (BankID)*, Εθνική υποδομή στη Σουηδία για την eID, στο συνέδριο της Λισσαβόνας [1], 22/10/2009

[7], Ομιλία του *Dr Alexandre Caldas - Director (CEGER - Centro de Gestão da Rede Informática do Governo)*, Κυβερνητικές πολιτικές στην ηλεκτρονική ταυτοποίηση και διεθνή ασφάλεια, στο συνέδριο της Αθήνας [2], 21/10/2010

[8], Ομιλία του *Mr. Gonçalo Caseiro, Vice Chairman, AMA Agência para a Modernização Administrativa – Portugal*, Ψηφιακή ταυτοποίηση στην Πορτογαλία, στο συνέδριο της Κωνσταντινούπολης [3], 24/10/2011

[9], Ομιλία του *Mr. Iosif Moldovan, Deputy Minister of IT and Communication - Romania*, Ψηφιακή ταυτοποίηση στην Ρουμανία, στο συνέδριο της Κωνσταντινούπολης [3], 25/10/2011

[10], Ομιλία του *Mr. Iosif Moldovan, Deputy Minister of IT and Communication - Rom*, *Mr. Jorge Silva, Vice-President of the Notary Association – Portugal*, Άυλες συμβάσεις – το νέο πρότυπο, στο συνέδριο της Κωνσταντινούπολης [3], 25/10/2011

[11], Ομιλία του *Mr. Mustafa Taylan Güvercin, Business Development Director, Türksat A.Ş. - Turkey*, Ανοικτού τύπου ID για ευκολότερη πρόσβαση στις δημόσιες υπηρεσίες, στο συνέδριο της Κωνσταντινούπολης [3], 25/10/2011

Δημοσιεύσεις

[12], Παρουσίαση μελέτης εφαρμογής της *G&D (Christian Zipfel)*, **From document to eidentity: current and next generation National Documents**, 22/10/2009, CHRISTIAN ZIPFEL, Leiter Vertrieb Europa / GUS, Head of Sales Europe / CIS, Government Solutions, Giesecke & Devrient GmbH, Prinzregentenstrasse 159 D-81677 Munich, Tel. +49 89 4119-2416, Fax +49 89 4119-9202, Mobile +49 171 562 1055, mailto: christian.zipfel@gd-de.com

[13], Παρουσίαση θεμάτων διαπίστευσης έκδοσης πιστοποιητικών, του *Gabinete Nacional de Segurança (Major Paulo Balsinhas)*, **Issuing qualified certificates - accreditation**, 22/10/2009.

[14], Το σύστημα κύκλου ζωής της κάρτας, του *ITIJ (José António Rodrigues)*, **Data capture and lifecycle infrastructure**, 22/10/2009.

[15], ecard στη Γερμανία, του *Utimaco Safeware AG (Andreas Philipp)*, **eCard in Germany. Status: Certification and the need for new protection profiles**, 22/10/2009.

[16], Εθνική Πορτογαλική eID, του *Agência de Modernização Administrativa (André Vasconcelos)*, **National eID in Portugal**, 22/10/2009.

[17], Εθνική Νορβηγική eID, *Difi (Mats Lillesund)*, **National eID in Norway**, 22/10/2009.

[18], Η προοπτική χρήσης της eID στις τράπεζες, *Chaired by Security4Biz (Marijke De Soete)*, **Usage of National eIDs cards - the perspective of the Banks**, 22/10/2009.

[20], Παγκόσμιες συγκλίσεις & αποκλίσεις, του *Bit4ID (Alessandro Scognamiglio)*, **World Convergence/Divergence**, 22/10/2009.

[21], Δικαιώματα και υποχρεώσεις του ηλεκτρονικά ταυτοποιημένου πολίτη, του *ENISA (Steve Purser)*, **Rights and duties of the e-authenticated Citizen in the e-World**, 22/10/2009.

[22], e-GOV 2.0, των *Gemalto SA (Eric Billiaert) YeMA Consultants (Youval Eched)*, **e-Gov 2.0: The keys to success - best practices and success factors**, 22/10/2009.

[23], Διασυνοριακή ψηφιακή υπογραφή στην καταχώρηση επιχειρήσεων, του *Estonian Centre of Registers and Information Systems (Ingmar Vali)*, **Cross border digital signature in company registration portal**, 22/10/2009.

[24], Ταυτοποίηση κατόχου, *Precise Biometrics*, **Match-on-card** – making the eID truly personal, 22/10/2009.

[25], Ασφάλεια, του *STORK (André Vasconcelos)*, **Match-on-card** – making the eID truly personal, 22/10/2009.

[26], SEPA, του *SIBS (Rui Patraquim)*, **Bank eID infrastructure: The new SEPA (Single Euro Payments Area) cross-border specifications**, 22/10/2009.

[27], Ηλεκτρονική άδεια παραμονής, της *Serviço de Estrangeiros e Fronteiras (Claudia Jorge)*, **e-TR – lifecycle**, 22/10/2009.

[28], Υπηρεσίες PKI, του *Multicert (Nuno Ponte)*, **PKI Services**, 24/10/2011.

[29], Ασφάλεια, του *Mr. Frank Leyman, FEDICT – Belgium*, **STORK - present and future in cross-border services and user authentication - legal issues**, 22/10/2009.

[30], Ηλεκτρονικές εντολές, του *Mr. Nuno Ponte, Multicert S.A. – Portugal*, **eMandates - The new SEPA Direct Debit Service**, 24/10/2011.

[31], Ασύρματο PKI & BankID, του *Mr Göran Zebühr, Swedbank, Sweden*, **Wireless PKI (BankID in mobile) - facilitator for new mobile services**, 21/10/2010.

[32], TURKSAT, του *Dr. Ahmet Kaplan, Türksat SA – Turkey*, **eGovernment Gateway**, 24/10/2011.

[33], Το Ευρωπαϊκό πλαίσιο, του *Moderator: Mr. Gérard Galler, Information Society & Media DG - European Commission*, **Pan European Framework for electronic**

identification, authentication, e-signature and ancillary trusted services - European Citizenship and Revision of the eSignature Directive, 24/10/2011.

[34], Νέες σκέψεις, του *Mr. Gérard Galler, Information Society & Media DG - European Commission*, **Challenges to Come...**, 24/10/2011.

[35], Mobile BankID, του *Mr. Kenneth Tessem, BankID – Sweden*, **The Next Generation of BankID in the Mobile in Sweden**, 24/10/2011.

[36], Υπηρεσίες υγείας και κοινωνίας, του *Mr. Noël Nader - GIE SESAM-Vitale – France*, **Smart and on-line Pan-European Services in the Health and Social Sector**, 24/10/2011.

[37], eID στο Bahrain, του *Mr Osama Khalid Erfaei Mohamed, Senior Computer Security Administrator, CIO Office, Kingdom of Bahrain* case: **Issuance of National eID Documents, CIO office**, 21/10/2010.

[38], Ινδία – έργο UIDAI, του *Mr Daniel Dingley, Suprema Inc*, **The Indian UIDAI project of enrolling 1.3 billion citizens and eID SmartCards**, 21/10/2010.

[39], Ασφάλεια πρόσβασης σε φυσικούς χώρους, του *Spiros Liolis, HP*, **Secure Physical Facilities**, 22/10/2010.

[40], Υπηρεσίες eID στο Βέλγιο, του *Frank LEYMAN, fedict*, **Successful eID and eGovernmental Service in Belgium**, 21/10/2010.

[41], Κινητό PKI και αστυνομία, του *Mr Tomas Olovsson, AppGate AB*, **MobilePKI at the Swedish Police**, 21/10/2010.

[42], Διαχείριση της κάρτας του πολίτη, του *Mr Bernhard Binz, akm Software, Germany*, **The Secret behind the issuance of Million Bank and HealthCare Cards and the usage of PKI applications**, 21/10/2010.

[43], eID στην Σουηδική αστυνομία, του *Mr Lars Bagnert, former Executive at the Swedish Police Board*, **Usage of eID cards at the Swedish Police**, 21/10/2010.

[44], Τεχνολογίες σύμφωνα με eCC, του *Mr Frank Bode, G&D*, **National eID and eHealth card technologies in compliance with the European Citizen Card**, 21/10/2010.

[45], Online πιστοποίηση, του *Mr Denis Pinkas, Bull, S.A.S.*, **New on-line certificate generation and renewal methods for secure signature creation devices (SSCDs)**, 21/10/2010.

[46], Ασφάλεια & έξυπνα κινητά, του *Mr Michael K. Brown, Research in Motion (RIM/Blackberry)*, **The Blackberry Case**, 21/10/2010.

[47], Εθνική eID λύση με την εμπειρία της HP, του *Spiros Liolis*, **National eID solutions with HP's universal experience**, 21/10/2010.

[48], Η Ελληνική Αστυνομία online, του *Mr Nikos Bezerianos, IT consultant*, **The Greek Police "On-Line Project"**, 21/10/2010.

[49], Ισπανική eID, του *Dr. Fernando de Pablo Martin, Director General para el Impulso de la Administración Electrónica, Ministerio de Política Territorial y Administración Pública (MPT) - Spain*, **Destination Spain: The Spanish eID Card**", 24/10/2011.

Παράρτημα Α : Συμφωνία Σένγκεν

Συμφωνία Σένγκεν ή **Συνθήκη Σένγκεν** καλείται η συμφωνία που υπεγράφη στις **14 Ιουνίου του 1985** στο Σένγκεν ανάμεσα σε πέντε κράτη μέλη (**Γερμανία, Βέλγιο, Γαλλία, Λουξεμβούργο και Κάτω Χώρες**) και είχε ως στόχο την προοδευτική κατάργηση των ελέγχων στα κοινά σύνορα την εγκατάσταση καθεστώτος ελεύθερης κυκλοφορίας για όλα τα πρόσωπα, υπηκόους των κρατών που υπέγραψαν τη Συμφωνία καθώς και **αστυνομική και δικαστική συνεργασία**. Η **Ιταλία** υπέγραψε τις συμφωνίες το **1990**, η **Ισπανία** και η **Πορτογαλία** το **1991**, η **Ελλάδα** το **1992**, η **Αυστρία** το **1995** και η **Φιλανδία**, η **Σουηδία** και η **Δανία** το **1996**. Η **Ιρλανδία** και το **Ηνωμένο Βασίλειο** συμμετέχουν μόνον εν μέρει στη Συμφωνία Σένγκεν εφόσον έχουν διατηρήσει ακόμη τους ελέγχους στα σύνορά τους. Η Σύμβαση Σένγκεν τέθηκε σε ισχύ το **1995** και ενσωματώθηκε στο πλαίσιο της **Ευρωπαϊκής Ένωσης** με οκτώ την έναρξη ισχύος της **συνθήκης του Άμστερνταμ** το Μάιο του **1999**. Έκτοτε, το κεκτημένο Σένγκεν (Schengen acquis) εφαρμόζεται και αναπτύσσεται περαιτέρω εντός του νομικού και θεσμικού πλαισίου της **Ευρωπαϊκής Ένωσης**.

Από τις **21 Δεκεμβρίου 2007**, η **Εσθονία**, η **Τσεχία**, η **Λιθουανία**, η **Ουγγαρία**, η **Λετονία**, η **Μάλτα**, η **Πολωνία**, η **Σλοβακία** και η **Σλοβενία** ανήκουν στον χώρο Σένγκεν. Οι έλεγχοι στα εσωτερικά χερσαία (στα χερσαία σύνορα συμπεριλαμβάνονται και τα αεροδρόμια) και θαλάσσια σύνορα μεταξύ αυτών των χωρών και των 15 σημερινών κρατών μελών αίρονται. Κατ' αυτό τον τρόπο θα υλοποιηθεί το ιδανικό της ελεύθερης κυκλοφορίας: η τελευταία διεύρυνση σημαίνει ότι τα ανατολικά σύνορα του χώρου Σένγκεν φθάνουν τα 4.278 χλμ. Ο χώρος Σένγκεν επεκτάθηκε στις **30 Μαρτίου του 2008** στα αεροδρόμια των οκτώ προαναφερθεισών χωρών της κεντρικής Ευρώπης και της **Μάλτας** με την κατάργηση των συνοριακών ελέγχων για τους επιβάτες που πραγματοποιούν πτήσεις στο εσωτερικό αυτής της ζώνης χωρίς σύνορα.

Στη Χώρα μας η Σύμβαση Εφαρμογής της Συνθήκης Σένγκεν, η Συνθήκη Σένγκεν και ορισμένα πρόσθετα Πρωτόκολλα κυρώθηκαν από το Κοινοβούλιο με το Νόμο 2514/1997.

Υπήκοοι Ευρωπαϊκής Ένωσης

Οι υπήκοοι της Ευρωπαϊκής Ένωσης έχουν το δικαίωμα να εισέλθουν σε οποιαδήποτε χώρα της ΕΕ χωρίς να προβούν σε οποιοδήποτε περαιτέρω έλεγχο, το μόνο που χρειάζεται είναι ένα διαβατήριο ή ταυτότητα κάποιου κράτους μέλους της ΕΕ, παρόλο που ένας Ευρωπαίος υπήκοος δεν χρειάζεται να δείχνει διαβατήριο για να εισέλθει σε κάποιο κράτος μέλος μερικά από τα κράτη μέλη Σένγκεν έχουν διατηρήσει το δικαίωμα, σύμφωνα με την εθνική τους νομοθεσία, να πραγματοποιούν ελέγχους ταυτότητας εντός της επικράτειάς τους στο πλαίσιο των αστυνομικών καθηκόντων.

Υπήκοοι τρίτων χωρών

Ένας πολίτης μιας χώρας εκτός ΕΕ και Συνθήκης Σένγκεν μπορεί να ταξιδέψει σε ένα κράτος μέλος για μια διάρκεια τριών μηνών (90 ημερών) με την προϋπόθεση ότι πληροί τους όρους Σένγκεν, δηλαδή, κάποιος πρέπει να έχει στην κατοχή του έγκυρο διαβατήριο, να έχει στην κατοχή του θεώρηση διαβατηρίου σύντομης διαμονής, να μπορεί να αποδείξει το σκοπό του ταξιδιού του, να έχει στην κατοχή του επαρκείς πόρους συντήρησης για την περίοδο παραμονής και για την επιστροφή και τελικώς πρέπει να μην είναι καταχωρημένος στο σύστημα πληροφοριών Σένγκεν για την άρνηση εισόδου και δεν πρέπει να θεωρείται επικίνδυνος για τη δημόσια πολιτική ή εθνική ασφάλεια όλων των κρατών Σένγκεν.

Μέλη της Συμφωνίας Σένγκεν

Η είσοδος των νέων μελών της Ε.Ε. στο χώρο του Σένγκεν θα γίνεται υπό δύο προϋποθέσεις:

3. Να πληρούν τα τεχνικά κριτήρια για τις ανταλλαγές πληροφοριών ασφάλειας μεταξύ των κρατών μελών.
4. Να είναι σε θέση να διασφαλίσουν τα εξωτερικά τους σύνορα.

Μέχρι στιγμής, το μοναδικό κράτος μέλος της Ευρωπαϊκής Ένωσης που δεν πληροί καμία από της προϋποθέσεις είναι η Κύπρος. Ενώ η Βουλγαρία και η Ρουμανία δεν πληρούν τα κριτήρια ασφαλείας.

Αυτή τη στιγμή υπάρχουν 25 μέλη της Συμφωνίας από τα οποία τα περισσότερα είναι μέλη της Ευρωπαϊκής Ένωσης, τα μέλη είναι η Αυστρία, το Βέλγιο, η Δανία, η Φινλανδία, η Γαλλία, η Γερμανία, η Ελβετία, η Ιταλία, η Ελλάδα, το Λουξεμβούργο, οι Κάτω Χώρες, η Πορτογαλία, η Ισπανία, η Σουηδία, η Νορβηγία η Ισλανδία, η Εσθονία, η Τσεχία, η Λιθουανία, η Ουγγαρία, η Λετονία, η Μάλτα, η Πολωνία, η

Σλοβακία και η **Σλοβενία**. Στα τέλη Φεβρουαρίου του 2008 το **Λιχτενστάιν** υπέγραψε την ένταξή του στη ζώνη ελεύθερης διακίνησης των 24 χωρών της ΕΕ (**Συνθήκη Σένγκεν**). Με βάση τη συμφωνία αυτή, το κρατίδιο υποχρεώθηκε να συνεργαστεί περισσότερο με τις χώρες της ΕΕ στις υποθέσεις φοροδιαφυγής.

Τα κράτη μέλη της ΕΕ που εξακολουθούν να είναι εκτός της ζώνης Σένγκεν είναι το **Ηνωμένο Βασίλειο** και η **Ιρλανδία**, που επέλεξαν να διατηρήσουν τους συνοριακούς ελέγχους με άλλα κράτη μέλη της ΕΕ, ωστόσο έχουν εξουσιοδοτηθεί να εφαρμόζουν μερικές από τις διατάξεις σχετικά με την **αστυνομική** και **δικαστική συνεργασία** σε ποινικές υποθέσεις. Επίσης η Ελβετία αποφάσισε να ενταχθεί στη ζώνη Σένγκεν. Η Ελβετία θα έχει το ίδιο καθεστώς συνδεδεμένης χώρας όπως η Νορβηγία και η Ισλανδία που επίσης δεν είναι μέλη της ΕΕ.

Όσον αφορά τα υποψήφια για προσχώρηση στην Ευρωπαϊκή Ένωση κράτη πρέπει να έχουν αποδεχθεί πλήρως το κεκτημένο Σένγκεν κατά την ένταξή τους.

Μετά την ένταξη των νέων 9 χωρών στην Συμφωνία στις **21 Δεκεμβρίου 2007** ο Πρόεδρος της Ευρωπαϊκής Επιτροπής, κ. José Manuel Barroso, δήλωσε:

Από σήμερα οι πολίτες θα μπορούν να ταξιδεύουν ανεμπόδιστα στις 24 χώρες του χώρου Σένγκεν- από την Πορτογαλία μέχρι την Πολωνία και από την Ελλάδα μέχρι την Φινλανδία-χωρίς ελέγχους στα εσωτερικά χερσαία και θαλάσσια σύνορα. Επιθυμώ να συγχαρώ τα εννέα νέα μέλη του Σένγκεν, την πορτογαλική προεδρία και όλα τα κράτη μέλη της Ένωσης για τις προσπάθειες που κατέβαλαν. Μαζί καταργήσαμε τους ελέγχους στα σύνορα—αυτά τα εμπόδια για την ειρήνη, την ελευθερία και την ενότητα στην Ευρώπη – δημιουργώντας παράλληλα τις προϋποθέσεις για μεγαλύτερη ασφάλεια.

Χαρακτηριστικά Σένγκεν

Το κύριο χαρακτηριστικό είναι η δημιουργία κοινού εξωτερικού συνόρου. Άλλα χαρακτηριστικά της Συμφωνίας Σένγκεν είναι:

1. Κοινοί κανόνες περί ασύλου
2. Το δικαίωμα της αστυνομίας να καταδιώξει άτομα και έξω από τα σύνορα της χώρας
3. Διαχωρισμός ανθρώπων στα αεροδρόμια σε «πτήσεις εντός Σένγκεν» και «πτήσεις εκτός Σένγκεν»
4. Κοινή λίστα χωρών των οποίων οι πολίτες χρειάζονται βίζα

5. Δημιουργία του συστήματος πληροφοριών Σένγκεν το οποίο επιτρέπει σε αστυνομικά τμήματα να μοιράζονται κοινό τμήμα αρχείων καταζητούμενων και ανεπιθύμητων ανθρώπων καθώς και κλεμμένων αντικειμένων
Κοινές προσπάθειες καταπολέμησης της διακίνησης ναρκωτικών



Δημόσια Ασφάλεια «Κεκτημένο Σένγκεν»

Το κεκτημένο Σένγκεν περιλαμβάνει μέτρα με τα οποία καταργείται ο έλεγχος στα εσωτερικά σύνορα των χωρών και ενισχύεται η ασφάλεια των εξωτερικών συνόρων της [Ευρωπαϊκής Ένωσης](#). Το σημαντικότερο από τα μέτρα αυτά είναι η απαίτηση τα κράτη μέλη που έχουν εξωτερικά σύνορα της [ΕΕ](#) να είναι υπεύθυνα για να εξασφαλίζουν την πραγματοποίηση σωστών ελέγχων και την αποτελεσματική επιτήρηση των εξωτερικών συνόρων της [ΕΕ](#). Συνεπώς, οι επιθεωρήσεις και οι έλεγχοι στα εξωτερικά σύνορα της [ΕΕ](#) είναι αρκετά αυστηροί για την παρεμπόδιση της λαθρομετανάστευσης, του λαθρεμπορίου ναρκωτικών και άλλων παράνομων δραστηριοτήτων.

Σε περίπτωση σοβαρού κινδύνου για τη δημόσια πολιτική ή τη δημόσια ασφάλεια εξουσιοδοτείται κάθε κράτος μέλος να αποκαταστήσει προσωρινά τους ελέγχους στα σύνορά του εντός της [Ευρωπαϊκής Κοινότητας](#).

Παράρτημα Β : Βιομετρικός έλεγχος

Τι κρύβουν τα νέα βιομετρικά διαβατήρια

Πόσο καλά προστατευμένα είναι τα προσωπικά μας δεδομένα που φωλιάζουν στο τσιπάκι των νέων διαβατηρίων; Μιλώντας στο «Βήμα» ο **ερευνητής Φαν Μπικ, ο οποίος «έσπασε» το σύστημα προστασίας τους**, τονίζει ότι χρειάζεται αναβάθμιση των συστημάτων ελέγχου. Παράλληλα, η κοινωνική συγκυρία επιβάλλει την άμεση εφαρμογή αυστηρότερων ελέγχων

ΔΗΜΟΣΙΕΥΣΗ: 30/11/2008, 07:10 ΕΦΗΜΕΡΙΔΑ ΤΟ ΒΗΜΑ SCIENCE



Το βιομετρικό διαβατήριο εκτίθεται στην υπεριώδη ακτινοβολία και αμέσως αποκαλύπτονται τα «κρυφά» σημεία τα οποία είναι αόρατα διά γυμνού οφθαλμού. Πέρα από αυτά όμως το e-Pass είναι εξοπλισμένο με σημεία-«φαντάσματα» για τον εντοπισμό των οποίων χρειάζονται ειδικοί αποκρυπτογράφοι

Τα νέα «αναβαθμισμένα» βιομετρικά διαβατήρια βρίσκονται προ των πυλών. Σύμφωνα με τον κανονισμό αριθ. 2252/2004 του Συμβουλίου της Ευρωπαϊκής Ένωσης, τόσο η χώρα μας όσο και τα υπόλοιπα κράτη-μέλη καλούνται από τις 28

Ιουνίου του 2009 να εφαρμόσουν την έκδοση των νέων διαβατηρίων, στα οποία θα συμπεριλαμβάνονται τα δακτυλικά αποτυπώματα του κατόχου. Τα ερωτήματα που προκύπτουν βέβαια από μια τέτοια εξέλιξη, η οποία αφορά την προσθήκη νέων ψηφιακών προσωπικών δεδομένων στα επίσημα αυτά έγγραφα, είναι άπειρα. Πέρα από την εξακρίβωση των στοιχείων του κατόχου, τα δακτυλικά αποτυπώματα θα χρησιμοποιούνται και για τον εντοπισμό υπόπτων; Θα φυλάσσονται όλα σε μια συγκεκριμένη τράπεζα δεδομένων, όπου θα πιστοποιείται η ασφάλειά τους; Υπάρχει άραγε η δυνατότητα να «σπάσει» κανείς τις, κατά τις αρχές, «αδιάτρητες» δικλίδες ασφαλείας πλαστογραφώντας τα διαβατήρια και κλέβοντας τα δακτυλικά αποτυπώματα του κατόχου; Αυτές και άλλες πολλές είναι οι απορίες που γεννιούνται στο μυαλό μας στο άκουσμα της νέας και τεχνολογικά προηγμένης εφαρμογής. Τι από όλα αυτά όμως ισχύει στην πραγματικότητα; **Τι περιέχει το τσιπάκι** Όπως είπε στο «Βήμα» αρμόδιος αξιωματικός της ΕΛ.ΑΣ., το μόνο που θα διαφοροποιεί τα νέα βιομετρικά διαβατήρια από τα υπάρχοντα είναι η προσθήκη των ψηφιακών δακτυλικών αποτυπωμάτων στο ειδικό μικροσίπ ταυτοποίησης μέσω ραδιοσυχνότητων RFID (Radio Frequency Identification), το οποίο με τη βοήθεια ραδιοκυμάτων επιτρέπει την ανάγνωση των στοιχείων που φέρει από απόσταση κάποιων εκατοστών. «Τα μοναδικά νέα στοιχεία που θα συμπεριληφθούν στο νέο διαβατήριο θα είναι τα δακτυλικά αποτυπώματα και συγκεκριμένα οι απλές αποτυπώσεις των δύο δεικτών του δεξιού και του αριστερού χεριού» εξηγεί. «Ηδη υπάρχει το τσιπάκι μέσα στο υπάρχον βιομετρικό διαβατήριο, όπου υπάρχουν οι φωτογραφίες και τα στοιχεία της προσωπικής του κατάστασης, τα οποία αναγράφονται και επάνω στη σελίδα του διαβατηρίου» προσθέτει ο ίδιος. Κάτι τέτοιο, όπως υποστηρίζει, βοηθά στο να εξακριβώνεται ότι το άτομο που φέρει το διαβατήριο είναι και ο νόμιμος κάτοχός του. Τι θα γίνει όμως με τα διαβατήρια που θα βρίσκονται ακόμη σε ισχύ; «Τα προηγούμενα διαβατήρια των οποίων η ημερομηνία λήξης δεν έχει επέλθει θα ισχύουν κανονικά, δεν καταργούνται. Όπως επίσης ισχύουν και τα διαβατήρια πριν από τις 26.8.2006, τότε που δεν διέθεταν ακόμη τσιπάκι» υπογραμμίζει ο αξιωματικός. **Πώς ξεκλειδώνουν τα στοιχεία** Βασικό ρόλο στη χρήση των νέων βιομετρικών διαβατηρίων παίζει το πρωτόκολλο Υποδομής Δημόσιου Κλειδιού (ΥΔΚ). Ένας συνδυασμός λογισμικού, τεχνολογιών κρυπτογράφησης και υπηρεσιών ο οποίος θα καθιστά δυνατή τη δημιουργία μιας ασφαλούς υποδομής διαδικτυακών επικοινωνιών. Με τον τρόπο αυτόν οι εξουσιοδοτημένοι χρήστες- που στην προκειμένη περίπτωση θα είναι τα κράτη-μέλη- θα μπορούν να «ξεκλειδώνουν» τα δεδομένα του εγγράφου καθιστώντας έτσι δυνατή

την επικύρωση των ψηφιακών στοιχείων ως προς τη γνησιότητά τους, ενώ παράλληλα θα εμφανίζει οποιαδήποτε τροποποίηση έχουν υποστεί. Για την ενεργοποίηση και την εφαρμογή του συγκεκριμένου συστήματος χρειάζονται ειδικοί κωδικοί, οι οποίοι για λόγους ασφαλείας αλλάζουν κατά διαστήματα. «Πρόκειται για ένα σύστημα υποδομής το οποίο μοιράζεται σε όλες τις χώρες που εκδίδουν τέτοια διαβατήρια. Εφαρμόζοντάς το στα ηλεκτρονικά συστήματα και στους ειδικούς ψηφιακούς “αναγνώστες” (readers) οι αρμόδιες αρχές θα είναι σε θέση να γνωρίζουν αν το συγκεκριμένο διαβατήριο που ελέγχουν έχει πραγματικά εκδοθεί στη χώρα που αναγράφεται σε αυτό και δεν είναι “μαϊμού”» περιγράφει ο αξιωματικός. «Δηλαδή, βάζοντας το κλειδί που εμείς μοιράζουμε στις άλλες χώρες, μπορεί ο αρμόδιος να βλέπει κατά πόσο το διαβατήριο που περνά ανήκει πράγματι στη χώρα που αναφέρει ή είναι πλαστογραφημένο». Ως προς τη χρήση των δακτυλικών αποτυπωμάτων των πολιτών η παράγραφος 3 του άρθρου 4 της συμβιβαστικής τροπολογίας, που αντικαθιστά τις τροπολογίες 14 και 26 του Ευρωπαϊκού Κανονισμού αριθ. 2252/2004, ξεκαθαρίζει: «Μετά την έκδοση των διαβατηρίων ή ταξιδιωτικών εγγράφων, τα βιομετρικά στοιχεία που έχουν συγκεντρωθεί για τον σκοπό αυτόν χρησιμοποιούνται αποκλειστικά για σκοπούς ελέγχου των συνόρων και μόνο για την εξακρίβωση: α) της γνησιότητας του εγγράφου και β) της ταυτότητας του κατόχου μέσω άμεσα διαθέσιμων συγκρίσιμων χαρακτηριστικών στις περιπτώσεις που είναι υποχρεωτική η επίδειξη διαβατηρίου ή άλλων ταξιδιωτικών εγγράφων σύμφωνα με τις διατάξεις του κανονισμού (ΕΚ) αριθ. 562/2006 (Κώδικας Συνόρων του Σένγκεν)». Ενώ τονίζει: «Τα βιομετρικά στοιχεία αποθηκεύονται αποκλειστικά στο μέσο αποθήκευσης και δεν τηρούνται σε βάση δεδομένων».

Σύμφωνα με πρόσφατη ομόφωνη απόφαση της Επιτροπής Ελευθεριών και Δικαιωμάτων των Πολιτών, τα παιδιά κάτω των 12 ετών θα εξαιρούνται από τη συγκεκριμένη διαδικασία καθώς τα δακτυλικά τους αποτυπώματα, ιδιαίτερα σε νεαρές ηλικίες, δεν αποτελούν αξιόπιστα τεκμήρια, καθ' ότι μπορεί να υποστούν αλλαγές. Παρ' όλα αυτά, στο πλαίσιο της καταπολέμησης της παράνομης διακίνησης και εμπορίας παιδιών (trafficking), όλα τα παιδιά κάτω των 14 ετών θα πρέπει να διαθέτουν προσωπικό διαβατήριο, το οποίο μάλιστα δεν μπορεί να έχει ισχύ άνω των τριών ετών. **Ταυτότητες και άδειες οδήγησης** Ανάμεσα στους άμεσους στόχους του ελληνικού κράτους είναι και η αντικατάσταση των σημερινών ταυτοτήτων και των αδειών οδήγησης από τη νέα γενιά των υπερσύγχρονων επίσημων εγγράφων που θα έχουν τη μορφή πιστωτικής κάρτας. Είναι άλλωστε γεγονός ότι η Ελλάδα συγκριτικά με άλλες χώρες (όπως π.χ. η Κύπρος), που εδώ και

αρκετά χρόνια απολαμβάνουν τα προνόμια των νέων αυτών τεχνολογιών σε ταυτότητες και άδειες οδήγησης, βρίσκεται αρκετά πίσω στον συγκεκριμένο τομέα. Από τις 19.1.2009 όμως αυτό αναμένεται να αλλάξει αρχικά με τις άδειες οδήγησης και στην πορεία (δεύτερο εξάμηνο του 2009) με τις ταυτότητες. «Οι νέες άδειες θα αρχίσουν να τυπώνονται περί το τέλος του πρώτου μήνα του νέου έτους» αναφέρει ο αξιωματικός της ΕΛ.ΑΣ. «Σε πρώτη φάση η αλλαγή θα πραγματοποιηθεί στις νέες άδειες για τους νέους οδηγούς και στις ανανεώσεις. Σε βάθος χρόνου θα γίνει σιγά σιγά και η αντικατάσταση των παλιών αδειών, ωστόσο μιλάμε για ένα χρονοδιάγραμμα το οποίο φτάνει περί τα 30 χρόνια». Γεγονός που διαφοροποιεί τη συγκεκριμένη διαδικασία από εκείνη των διαβατηρίων, όπου υπήρχε αυστηρός χρονικός περιορισμός. «Τα διαβατήρια είναι αποδεικτικό ταυτότητας, έγγραφο ασφαλείας, το οποίο παρέχει τη δυνατότητα ταξιδιού και παραμονής στο εξωτερικό, οπότε η ανάγκη της άμεσης αλλαγής είναι επιτακτικότερη» εξηγεί ο αρμόδιος.

Λείπουν τα μηχανήματα Το «κώλυμα» της τεχνολογίας των νέων διαβατηρίων, τουλάχιστον στο παρόν στάδιο, όπως μας ανέφερε ο ίδιος, εντοπίζεται στο γεγονός ότι πολλές χώρες δεν έχουν ακόμη εγκαταστήσει στους συνοριακούς σταθμούς τα απαιτούμενα συστήματα ανάγνωσης. «Πρόκειται για τους ειδικούς “readers” που επιτρέπουν την ανάγνωση και την εξακρίβωση των στοιχείων του διαβατηρίου και της ταυτότητας του κατόχου. Όταν όμως αυτοί λείπουν, τότε πραγματοποιείται μόνο μακροσκοπικός έλεγχος, δηλαδή το τι βλέπουμε μπροστά μας. Μόλις εγκατασταθούν τα μηχανήματα, η πιστοποίηση θα είναι ακόμη πιο εύκολη. Γιατί είναι συνδυασμός: εγώ βγάζω ένα αξιόπιστο ταξιδιωτικό έγγραφο με πολλά μέτρα ασφαλείας αλλά και ο άλλος που θα με δεχθεί θα πρέπει να έχει τους “αναγνώστες”, το κλειδί της χώρας προέλευσης, ώστε να μπορεί να πραγματοποιήσει την αντιπαραβολή» περιγράφει γλαφυρά. «Το διαβατήριο άλλωστε περιέχει συγκεκριμένα μέτρα ασφαλείας, όπως π.χ. ο βασικός έλεγχος πρόσβασης και η ενεργός πιστοποίηση, που προστατεύουν την κλωνοποίηση του εγγράφου ή την κλοπή των ψηφιακών δακτυλικών αποτυπωμάτων». Η ενσωμάτωση των δακτυλικών αποτυπωμάτων έχει ήδη εφαρμοστεί στα γερμανικά διαβατήρια. Μάλιστα η πρόωρη αυτή εφαρμογή ξεσήκωσε την έντονη αντίδραση του γερμανικού οργανισμού χάκερ Chaos Computer Club eV. (CCC), τα μέλη του οποίου έσπευσαν να χαρακτηρίσουν τους γερμανούς πολίτες «πειραματόζωα» που αποδέχθηκαν την εφαρμογή μιας «πρωτής», όπως υποστηρίζουν, τεχνολογίας. Προς ένδειξη διαμαρτυρίας τους, τον Μάρτιο του 2008 κατάφεραν να αποσπάσουν και να δημοσιεύσουν τα δακτυλικά αποτυπώματα του υπουργού Εσωτερικών της χώρας Βόλφγκανγκ Σόιμπλε. **Το**

πείραμα των «Times» Στις αρχές Αυγούστου η βρετανική εφημερίδα «The Times» προκειμένου να εξετάσει τα μέτρα ασφαλείας των νέων διαβατηρίων πραγματοποίησε ένα πρωτότυπο πείραμα: επιστρατεύοντας τον ολλανδό ερευνητή συστημάτων ασφαλείας του Πανεπιστημίου του Άμστερνταμ κ. Γερούν φαν Μπικ κατάφεραν να σπάσουν τους κωδικούς-«φρούριο» και να αλλάξουν βασικά στοιχεία όπως η φωτογραφία του κατόχου. Μάλιστα σε διαβατήριο που ανήκε σε ένα αγοράκι ο ειδικός κατάφερε να αφαιρέσει την ψηφιακή φωτογραφία του και στη θέση της να βάλει εκείνη του Οσάμα μπιν Λάντεν, ενώ σε ένα άλλο που ανήκε σε μια 36χρονη γυναίκα «ανέβασε» το πορτρέτο του Χίμπα Νταργκμέ , ενός παλαιστινίου βομβιστή αυτοκτονίας. Ο κ. Φαν Μπικ μίλησε αποκλειστικά στο «Βήμα» περιγράφοντας πώς ακριβώς έγινε η δοκιμή. «Για την ακρίβεια, από τον περασμένο Φεβρουάριο εργαζόμουν πάνω σε ένα λογισμικό που επιτρέπει την κλωνοποίηση των ePassports. Ο Ανταμ Λόρι, ένας βρετανός ειδικός στην τεχνολογία ταυτοποίησης μέσω ραδιοσυχνοτήτων (RFID), το γνώριζε αυτό και έτσι με ρώτησε αν ένας δημοσιογράφος βρετανικής εφημερίδας θα μπορούσε να επικοινωνήσει μαζί μου για να μάθει περισσότερα για τη δουλειά μου. Του απάντησα θετικά και έτσι κι έγινε. Ο δημοσιογράφος Στιβ Μπόγκαν με επισκέφθηκε τον Ιούλιο, όταν το μεγαλύτερο μέρος του λογισμικού μου ήταν έτοιμο» εξιστορεί ο 30χρονος άνδρας. «Ο Μπόγκαν είχε μαζί του δύο βρετανικά διαβατήρια για να τσεκάρει το σύστημα που έφεραν. Ήταν κάτι το οποίο δεν είχα επιχειρήσει προηγουμένως. Ως τότε είχα δοκιμάσει μόνο τα μικροσίπ των ολλανδικών διαβατηρίων. Για μένα ήταν η πρώτη φορά λοιπόν που θα προσπαθούσα να “σπάσω” ένα βρετανικό διαβατήριο» παραδέχεται ο κ. Φαν Μπικ.

Παράρτημα Γ: Hacking

«Σπάσιμο» -παιχνιδάκι

ΑΝΑΤΟΜΙΑ ΤΟΥ ΒΙΟΜΕΤΡΙΚΟΥ ΔΙΑΒΑΤΗΡΙΟΥ

Ασφάλεια και προστασία

Οι δικλίδες ασφαλείας για την πιστοποίηση της γνησιότητας του διαβατηρίου χωρίζονται σε τρία επίπεδα:

1. Το επίπεδο αναγνώρισης συγκεκριμένων «κρυμμένων» συμβόλων που είναι αόρατα διά γυμνού οφθαλμού.
2. Το επίπεδο αναγνώρισης με χρήση υπεριώδους ακτινοβολίας.
3. Το επίπεδο αναγνώρισης από εξειδικευμένους αποκρυπτογράφους.

Μηχανικώς αναγνώσιμη ζώνη

Συμπύσσει όλα τα στοιχεία του διαβατηρίου σε δύο γραμμές. Από τον ειδικό αλγόριθμο του Διεθνούς Οργανισμού Πολιτικής Αεροπορίας (ΔΟΠΑ) εξάγεται το κλειδί το οποίο αναγνωρίζει το μικροτσίπ που κρύβεται στο οπισθόφυλλο. Ωστόσο η ανταλλαγή δεδομένων προστατεύεται από το κρυπτογραφικό πρωτόκολλο της Υποδομής Δημόσιου Κλειδιού (ΥΔΚ).

Πώς λειτουργεί το σύστημα

Το πανίσχυρο μικροτσίπ το οποίο περιέχει όλα τα βιομετρικά δεδομένα του κατόχου εντοπίζεται στο οπισθόφυλλο του διαβατηρίου. Χάρη στην τεχνολογία RFID οι πληροφορίες διαβάζονται από τον αναγνώστη (reader) εξ αποστάσεως. Τα ραδιοκύματα που απαιτούνται για τη συγκεκριμένη διαδικασία έχουν ισχύ 13,56 MHz, με αποτέλεσμα να τροφοδοτούν παράλληλα το τσίπ με την απαιτούμενη λειτουργική ενέργεια. Η πρόσβαση στα στοιχεία που βρίσκονται αποθηκευμένα στο μικροτσίπ είναι εφικτή μόνο με τη βοήθεια ηλεκτρονικού «κλειδιού» που προκύπτει από την ανάγνωση της οπτικής ζώνης του διαβατηρίου. Στη συνέχεια πραγματοποιείται η κρυπτογραφημένη μετάδοση των βιομετρικών δεδομένων.

Η ανάγνωση των Διαβατηρίων

Επιτυγχάνεται σε δύο στάδια:

1. Το έγγραφο σκανάρεται. Κατά την αναγνώριση των γραφικών χαρακτήρων και των πληροφοριών που «κρύβονται» στην οπτική ζώνη, το σύστημα «υπολογίζει» ένα κλειδί το οποίο επιτρέπει τη συλλογή των πληροφοριών της μηχανικώς αναγνώσιμης ζώνης.



Οπισθόφυλλο διαβατηρίου Μικροκεραία

Το μικροτσίπ

Πρόκειται για ολοκληρωμένο μικροκύκλωμα όπου φορτώνονται και αποθηκεύονται όλα τα προσωπικά στοιχεία του κατόχου, όπως επίσης και σημαντικές πληροφορίες για την ανάγνωσή τους. Καταναλώνει περί τα 100 χιλιοβάτ, ενέργεια την οποία αντλεί από τη μικροκεραία που βρίσκεται κρυμμένη στο πλαίσιο του εσωτερικού φύλλου του οπισθόφυλλου, η οποία τροφοδοτείται από τα ραδιοκύματα που εκπέμπονται από τον αναγνώστη (reader) κατά την ανάγνωση του διαβατηρίου.



Φωτογραφία



Ψηφιακά δακτυλικά αποτυπώματα

Προσωπικά στοιχεία

(Hellas) Οπτικώς μεταβλητή μελάνη: Μελάνι «χαμαιλέων» το οποίο αλλάζει χρώμα όταν αλλάζει η γωνία παρατήρησης ή ο φωτισμός.

Φωτογραφία-φαντομάς: Μια δευτερογενής φωτογραφία η οποία είναι αόρατη και εμφανίζεται μόνο όταν το έγγραφο εκτεθεί σε υπεριώδη ακτινοβολία.

Φωτογραφία

Η έκφραση του κατόχου πρέπει να είναι ουδέτερη, με τα δύο μάτια κανονικά ανοικτά και το στόμα κλειστό. Ο φωτισμός τόσο στο πρόσωπο όσο και στο ανοιχτόχρωμο φόντο (λευκό ή ανοιχτό γκρι) της φωτογραφίας πρέπει να είναι ομοιόμορφος. Δεν πρέπει να υπάρχουν σκιές στο πρόσωπο ή στα μάτια λόγω των φρυδιών. Η ίριδα και η κόρη των ματιών πρέπει να είναι ευκρινώς ορατές. Αν το άτομο φοράει γυαλιά, τότε θα πρέπει να τα φοράει και στη συγκεκριμένη φωτογραφία, αλλά θα πρέπει να είναι καθαρά και διαφανή, ώστε να φαίνονται η ίριδα και η κόρη των ματιών, ενώ οποιαδήποτε άλλα καλύμματα του προσώπου θα πρέπει να αποβάλλονται.

2. Με τη βοήθεια των ραδιοκυμάτων τα στοιχεία που είναι αποθηκευμένα στο μικροτσίπ «διαβάζονται» και έτσι πραγματοποιείται η ταυτοποίηση των στοιχείων.

Όπως μας εξηγεί ο ίδιος, τα «εργαλεία» που απαιτούνται για το σπάσιμο των περιβόητων δικλίδων ασφαλείας είναι απλά και το κόστος τους είναι αρκετά χαμηλό. Ακόμη και η όλη διαδικασία υποστηρίζει ότι δεν χρειάζεται κάποια ιδιαίτερη εξειδίκευση στο αντικείμενο.

«Σε πρώτη φάση ο ενδιαφερόμενος θα πρέπει να αγοράσει έναν αναγνώστη RFID, κενά μικροτσίπ της ίδιας τεχνολογίας και να φορτώσει ένα ελεύθερο περιβάλλον προγραμματισμού. Στη συνέχεια θα πρέπει να φτιάξει ένα λογισμικό για τα κενά μικροτσίπ, τα οποία λειτουργούν όπως ακριβώς και τα πραγματικά μικροτσίπ των διαβατηρίων. Με τη βοήθεια του αναγνώστη μπορεί να διαβάσει τα δεδομένα που βρίσκονται αποθηκευμένα στο πραγματικό μικροτσίπ και να τα αντιγράψει στο κενό τσιπάκι. Έτσι επιτυγχάνεται η 100% αντιγραφή των δεδομένων» εξηγεί.

«Με τον τρόπο αυτόν μπορεί κάποιος να παρέμβει στα πραγματικά στοιχεία και να τα αλλάξει. Ωστόσο θα πρέπει να τα αντιγράψει στο κενό τσιπάκι και στη συνέχεια να εξετάσει κατά πόσο τα “πλαστά” μικροτσίπ περνούν με επιτυχία τα τεστ εξοπλισμού και εκείνο της αναφοράς εφαρμογής το οποίο ονομάζεται Golden Reader Tool (GRT) και έχει τη δυνατότητα να αναγνωρίζει λάθη και πλαστά στοιχεία, όπως π.χ. η γνησιότητα της υπογραφής. Επιπλέον ο ενδιαφερόμενος θα πρέπει να είναι σίγουρος ότι ο Διεθνής Οργανισμός Πολιτικής Αεροπορίας δεν έχει προχωρήσει σε αλλαγές του συστήματος» υπογραμμίζει ο ερευνητής.

Ο ολλανδός ειδικός κατάφερε ακόμη να δημιουργήσει επιπλέον λογισμικό το οποίο επιτρέπει στα «καλά φυλασσόμενα» πλαστά τσιπάκια, όπως τα χαρακτηρίζει ο ίδιος, να διαφεύγουν τον έλεγχο ενεργούς πιστοποίησης και να γίνονται δεκτά από το τεστ GRT.

«Ο μόνος τρόπος για να εντοπίσει κανείς τα πλαστά τσιπάκια είναι μέσω της εξακρίβωσης της γνησιότητας της πηγής της ηλεκτρονικής υπογραφής του διαβατηρίου. Και, σύμφωνα με τον Διεθνή Οργανισμό Πολιτικής Αεροπορίας, λίγες μόνο χώρες πραγματοποιούν τη συγκεκριμένη εξακρίβωση αυτόματα. Στις υπόλοιπες κάτι τέτοιο γίνεται είτε με τον συμβατικό “χειροκίνητο” τρόπο, αντιμετωπίζοντας έτσι αυξημένες πιθανότητες λάθους, είτε καθόλου» τονίζει.

Ποιες χώρες είναι όμως αυτές που διαθέτουν ήδη το ειδικό σύστημα (Public Key Directory PKD) για την εφαρμογή της Υποδομής Δημόσιου Κλειδιού; Σύμφωνα με επίσημα στοιχεία του ΔΟΠΑ, ως τον Μάιο του 2008 μόνο εννέα κράτη διέθεταν το συγκεκριμένο σύστημα ελέγχου και πιστοποίησης. «Αυτά είναι η Αυστραλία, ο Καναδάς, η Γερμανία, η Ιαπωνία, η Νέα Ζηλανδία, η Δημοκρατία της Κορέας, η Σιγκαπούρη, η Βρετανία και οι ΗΠΑ. Η Γαλλία αναμενόταν να ολοκληρώσει τις διαδικασίες συμμετοχής σύντομα, από όσο γνωρίζω» μας λέει ο κ. Φαν Μπικ.

Επηρεασμένοι από ταινίες επιστημονικής φαντασίας, οι περισσότεροι από εμάς τείνουμε να πιστεύουμε ότι η διαδικασία πλαστογράφησης αποτελεί πραγματικό εγχείρημα και απαιτεί πολύ εξειδικευμένες γνώσεις. «Ο καθένας που διαθέτει γνώσεις ηλεκτρονικού υπολογιστή μπορεί να το κάνει μέσα σε διάστημα λίγων μόλις λεπτών» ισχυρίζεται ο ερευνητής. Μάλιστα μέσα από την ιστοσελίδα του εξηγεί βήμα προς βήμα τη μέθοδο που χρησιμοποίησε ο ίδιος.

«Η ανάπτυξη και η διεξοδική εξέταση όλων των βημάτων μου πήρε περίπου δύο-τρεις εβδομάδες. Ωστόσο κατά τη χρονική περίοδο στην οποία πραγματοποιήθηκε το τεστ των “Times” με την απλή εφαρμογή των μη αυτοματοποιημένων βημάτων για τη δημιουργία ψευδών δεδομένων χρειάστηκα περίπου μία ώρα» περιγράφει.

«Δεν λέω ότι οι τρομοκράτες θα μπορούσαν άμεσα να προχωρήσουν σε κάτι τέτοιο. Ωστόσο πρόκειται για ανησυχίες γύρω από την ασφάλεια οι οποίες πρέπει να εκφράζονται πιο ανοιχτά» τονίζει ο ειδικός.

Απαιτείται αναβάθμιση

Ποιο σύστημα όμως θα μπορούσε να προσφέρει τη μεγαλύτερη ασφάλεια, προστατεύοντας επαρκώς τα ψηφιακά βιομετρικά δεδομένα; «Πιστεύω ότι κάτι τέτοιο δεν θα ήταν υπερβολικά δύσκολο. Παρ’ όλα αυτά, θα χρειαστεί να αντικατασταθούν τα υπάρχοντα μικροτσίπ, ειδικά των χωρών εκείνων που δεν φέρουν την ενεργό πιστοποίηση, όπως π.χ. η Βρετανία, οι ΗΠΑ, η Ιαπωνία και η Γερμανία, με νέα πιο ακριβά. Σημαντικότατο ρόλο όμως στη διασταύρωση και στην εξακρίβωση των αποθηκευμένων δεδομένων παίζει το ειδικό σύστημα ΥΔΚ και για τον λόγο αυτόν η εισαγωγή του στα συστήματα ελέγχου της κάθε χώρας είναι απαραίτητη» υποστηρίζει ο κ. Φαν Μπικ.

Ο αρμόδιος αξιωματικός της ΕΛ.ΑΣ. εμμένει στην ασφάλεια των νέων βιομετρικών διαβατηρίων, τα οποία, όπως λέει, αναμένεται να συμβάλουν στη μείωση της εγκληματικότητας. «Θα βοηθήσουν ιδιαίτερα στον περιορισμό της λαθρομετανάστευσης, της διακίνησης ναρκωτικών και όπλων και δεν αναφέρομαι σε αυτά που γίνονται στο Αιγαίο. Γιατί δυστυχώς δεν είναι μόνο αυτά. Αναφέρομαι φυσικά σε όλα αυτά που γίνονται με πλαστά διαβατήρια» δηλώνει.

Σε μια παγκόσμια κοινωνία όπου το ηλεκτρονικό έγκλημα βρίσκεται σε άνθηση θα

μπορέσουμε άραγε ποτέ να νιώσουμε απόλυτη ασφάλεια κλείνοντας τα ευαίσθητα προσωπικά μας δεδομένα σε ένα τσιπάκι το οποίο ενδεχομένως να γινόταν βορά στα αδηφάγα πλήκτρα των δεξιοτεχνών στους ηλεκτρονικούς υπολογιστές; Το σίγουρο είναι ότι το κύμα ψηφιακού εκσυγχρονισμού θα απλοποιήσει κατά πολύ την καθημερινότητά μας, απλοποιώντας τις μετακινήσεις μας σε ξένες χώρες και μεταμορφώνοντας άλλοτε χρονοβόρες διεργασίες σε αστραπιαίες διαδικασίες. Το θέμα είναι να υιοθετηθούν εις βάθος όλα τα απαιτούμενα μέτρα και συστήματα τα οποία πέρα από την ασφάλεια θα εγγυώνται τη σωστή λειτουργία του τεχνολογικά προηγμένου ενσωματωμένου συστήματος.

Παράρτημα Δ : Η ιστορία ενός διαβατηρίου

Οι πρώτες αναφορές για επίσημα έγγραφα γίνονται στην εβραϊκή Βίβλο και χρονολογούνται την εποχή της Περσικής Αυτοκρατορίας, γύρω στο 450 π.Χ. Τότε πιστεύεται ότι ζητήθηκε από τον Νεεμία, αξιωματούχο του βασιλιά Αρταξέρξη Α Δ , να ταξιδέψει στην Ιουδαία. Ο βασιλιάς έγραψε λοιπόν ένα γράμμα «προς τους κυβερνήτες πέρα από τον ποταμό» εξασφαλίζοντάς του έτσι ασφαλές πέρασμα από τα βασίλεια αυτά.

Ως προς την ετυμολογία της λέξης «passport» υπάρχουν δύο βασικές εκδοχές: η πρώτη υποστηρίζει ότι η λέξη προέρχεται από το «pass» (περνώ) και το «port» (λιμάνι). Η δεύτερη πάλι και πιο επικρατούσα, αναφερόμενη στα έγγραφα που χρησιμοποιούνταν από τους ταξιδιώτες κατά τον Μεσαίωνα, μεταφράζει το δεύτερο μέρος της σύνθετης λέξης ως πύλη από το λατινικό «porte», παραπέμποντας έτσι στην αναγκαιότητα ενός εγγράφου που να πιστοποιεί την ταυτότητα του ταξιδιώτη στα τείχη μιας πόλης για τη δυνατότητα εισόδου του σε αυτήν.

Η τελική μορφή της λέξης «διαβατήριο» στα ελληνικά πλάστηκε κατά τον 19ο αιώνα, όταν ο Αδαμάντιος Κοραΐς και οι Διδάσκαλοι του Γένους κήρυξαν το κίνημα καθαρμού της γλώσσας. Έτσι η ξενόφερτη λέξη «πασαπόρτι» από το passport μετατράπηκε στο σημερινό μας διαβατήριο.

Στα παλαιότερα διαβατήρια αναγράφονταν μόνο τα προσωπικά στοιχεία του κατόχου, ενώ στις αρχές του 20ού αιώνα- όταν πλέον η φωτογραφία εντάχθηκε στην καθημερινότητα προστέθηκε σε αυτά και μια μικρή φωτογραφία.

Στην Ευρώπη η επίσημη διαδικασία της πιστοποίησης των προσωπικών στοιχείων μέσω διαβατηρίων ξεκίνησε κατά τη διάρκεια του Α Δ Παγκοσμίου Πολέμου για λόγους ασφαλείας προκειμένου να περιορισθούν οι μετακινήσεις των κατασκόπων αλλά και να γίνεται ακόμη πιο ενδεδειγμένος έλεγχος στην ταυτότητα των πολιτών και των ιδιοτήτων τους. Μετά το τέλος του Πολέμου ο διασυνοριακός έλεγχος συνεχίστηκε.

Λίγα χρόνια αργότερα, έπειτα από μια σειρά συνεδριάσεων, η Κοινωνία των Εθνών

ανακοίνωσε νέες οδηγίες ως προς τη χρήση και τον έλεγχο των διαβατηρίων.

Αν και οι αξιωματούχοι των Ηνωμένων Εθνών το 1963 αποπειράθηκαν να θέσουν νέες οδηγίες, κάτι τέτοιο τελικώς δεν ευοδώθηκε.

Τελικώς η προτυποποίηση των διαβατηρίων εφαρμόστηκε το 1980 από τον Διεθνή Οργανισμό Πολιτικής Αεροπορίας (International Civil Aviation Organization- ICAO).

Τα πρώτα βιομετρικά στοιχεία

Η ανθρωπομετρία δημιουργήθηκε για πρώτη φορά από τον Γάλλο Αλφόνς Μπερτιγιόν το 1882. Ο ίδιος ξεκίνησε την καριέρα του ως απλός αρχειοθέτης της Αστυνομίας του Παρισιού, σύντομα όμως έκρινε ότι το σύστημα ταυτοποίησης των υπόπτων που εφαρμοζόταν ως τότε ήταν ανεπαρκές.

Έτσι αποφάσισε να φτιάξει ένα νέο πιο αξιόπιστο σύστημα αντιστοιχίας το οποίο βασιζόταν στη μέτρηση μερών του σώματος, όπως το μέγεθος της κεφαλής, του μήκους των άκρων και των γενικότερων διαστάσεων του σώματος. Στη συγκεκριμένη μέθοδο γινόταν ακόμη αναφορά στιγμάτων που εντοπίζονταν στο σώμα, όπως ουλές, τατουάζ κτλ., αλλά και συγκεκριμένων χαρακτηριστικών της προσωπικότητας του φυσικού προσώπου.

Σύντομα μάλιστα η ανθρωπομετρία, γνωστή και ως μπερτιγιονάζ (bertillonage), από το όνομα του επινοητή του, υιοθετήθηκε από τις βρετανικές και τις αμερικανικές αστυνομικές αρχές. Ωστόσο λίγα χρόνια αργότερα το σύστημα κρίθηκε αναξιόπιστο καθώς, πέρα από το γεγονός ότι οι μετρήσεις αλλοιώνονταν με την πάροδο του χρόνου, υπήρχε πιθανότητα διαφοράς ως προς τον τρόπο των μετρήσεων που πραγματοποιούνταν από διαφορετικά άτομα.

Δακτυλικά αποτυπώματα

Αν και τα δακτυλικά αποτυπώματα χρησιμοποιούνταν ήδη από την αρχαιότητα ως δείγμα υπογραφής, όπως μαρτυρούν αγγεία του αρχαίου ελληνικού, κινεζικού, αιγυπτιακού και ρωμαϊκού πολιτισμού, η επίσημη χρήση τους για την πιστοποίηση της ταυτότητας του κατόχου τους από την αστυνομία ξεκίνησε το 1892 από τον Χουάν Βούσειτις, αξιωματικό της αργεντίνικης αστυνομίας.

Ως τότε είχαν πραγματοποιηθεί αρκετές μελέτες οι οποίες υπογράμμιζαν την αξιοπιστία τους ως προσωπικά τεκμήρια καθώς δεν επιδέχονταν αλλοιώσεις. Έτσι για πρώτη φορά ο Βούσειτις κατάφερε να αποδείξει ότι η Φρανσίσκα Ροχάς, η οποία κατηγορούνταν για φόνο, ήταν πραγματικά ένοχη, όπως προέκυπτε από τα δακτυλικά αποτυπώματα από αίμα που είχε αφήσει στη σκηνή του εγκλήματος.



