Ηλεκτρονική ταυτότητα πολιτών και επιλογές πολιτικής & υποδομών – η Ευρωπαϊκή εμπειρία

Ιούνιος 2010

ΠΑΡΑΤΗΡΗΤΗΡΙΟ
για την κοινωνία της πληροφορίας

«Ηλεκτρονική ταυτότητα πολιτών και επιλογές πολιτικής & υποδομών – η Ευρωπαϊκή εμπειρία»

Δρ Α. Κουντζέρης

Παρατηρητήριο για την Κοινωνία της Πληροφορίας

Σταδίου 33, 105 59, Αθήνα

Τηλ.: +302103313080, Fax: +302103313086

http://www.observatory.gr

Το «Παρατηρητήριο για την Κοινωνία της Πληροφορίας» εντάσσεται στο Ε.Π «Ψηφιακή Σύγκλιση» και συγχρηματοδοτείται σε ποσοστό 80% από το Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης και 20% από Εθνικούς Πόρους.

Ιούνιος 2010

Περιεχόμενα

1. Υφιστάμενη κατάσταση & προκλήσεις

Η διαχείριση ηλεκτρονικών ταυτοτήτων (eIDM) αποτελεί βασικό παράγοντα και προϋπόθεση για την ασφαλή και αποτελεσματική χρήση υπηρεσιών ηλεκτρονικών συναλλαγών από τους πολίτες. Μέσα σε ένα αξιόπιστο περιβάλλον ηλεκτρονικής ταυτοποίησης ενισχύεται η εμπιστοσύνη των πολιτών στις μεθόδους ηλεκτρονικής διακυβέρνησης και η πεποίθηση τους ότι διασφαλίζεται η προστασία των προσωπικών τους δεδομένων. Επιπλέον, οι δημόσιοι φορείς παροχής ηλεκτρονικών υπηρεσιών έχουν τη δυνατότητα να γνωρίζουν με σιγουριά την ταυτότητα των πολιτών με τους οποίους συναλλάσσονται, δηλαδή ότι αυτοί οι συγκεκριμένοι πολίτες έχουν τα δικαιώματα και τις παροχές που υποστηρίζουν ότι έχουν.

Την τελευταία πενταετία πολλές από τις χώρες μέλη της ΕΕ, σταδιακά έχουν υιοθετήσει συστήματα διαχείρισης ηλεκτρονικών ταυτοτήτων στο πλαίσιο του εκσυγχρονισμού των δημόσιων υπηρεσιών τους (π.χ. για φορολογικές υπηρεσίες, χορήγηση πιστοποιητικών και αδειών, κλπ) και οι υπόλοιπες σχεδιάζουν την εγκατάσταση λύσεων ηλεκτρονικής ταυτοποίησης πολιτών για το άμεσο μέλλον. Λειτουργούν ήδη συστήματα διαχείρισης ηλεκτρονικών ταυτοτήτων εθνικής, τοπικής και τομεακής εμβέλειας στο πλαίσιο της παροχής ηλεκτρονικών υπηρεσιών από φορείς της δημόσιας διοίκησης ενώ υφίστανται και εμπορικές εφαρμογές από τον ιδιωτικό τομέα. Το πλήθος δε των ηλεκτρονικών υπηρεσιών αναμένεται να αυξηθεί κατακόρυφα στο κοντινό μέλλον σαν αποτέλεσμα της αξιοποίησης των επενδύσεων στις υποδομές ευρυζωνικότητας που βρίσκονται σε εξέλιξη.

Στην Ελλάδα, ο «Καλλικράτης» θα αναδείξει μέσα στους επόμενους μήνες ως κυρίαρχη μορφή στη διοικητική μεταρρύθμιση τον ψηφιακό δήμο και αιχμή του δόρατος, την παροχή ηλεκτρονικών υπηρεσιών σε πολίτες (και επιχειρήσεις), με την αξιοποίηση της ηλεκτρονικής κάρτας για την ταυτοποίηση των πολιτών-δημοτών. Κάθε πολίτης θα έχει τη δική του ηλεκτρονική διοικητική κάρτα-ταυτότητα (την κάρτα πολίτη). Με την κάρτα αυτή πολίτες και διοίκηση θα περάσουν στην αυτόματη εξυπηρέτηση, όπως παραδείγματος χάριν για την έκδοση απλών πιστοποιητικών. Υπάρχει όμως και μια ακόμα διάσταση, αυτή της συμμετοχικής δημοκρατίας, με τη διευκόλυνση μέσω της κάρτας σε διαδικασίες ψηφοφορίας των πολιτών για μια σειρά από θέματα, π.χ. τοπικά δημοψηφίσματα. Επιπλέον, η Εθνική Διαδικτυακή Πύλη ΕΡΜΗΣ[1] ήδη λειτουργεί ως «υπηρεσία μιας στάσης» για την ψηφιακή επικοινωνία και εξυπηρέτηση των πολιτών και των επιχειρήσεων από τη Δημόσια Διοίκηση. Η Πύλη έχει σχεδιαστεί έτσι ώστε να αποτελέσει τη βάση ευρείας εφαρμογής μιας συνολικής λύσης ταυτοποίησης πολιτών, αυθεντικοποίησης των ηλεκτρονικών συναλλαγών, μετάδοσης πληροφοριών μεταξύ συστημάτων του δημοσίου τομέα και δημοσίευσης περιεχομένου σε ασφαλές περιβάλλον, στα πλαίσια της Ελληνικής Δημόσιας Διοίκησης και Ηλεκτρονικής Διακυβέρνησης (e-Government).

Η εφαρμογή και διαχείριση ηλεκτρονικών ταυτοτήτων συνεχίζει όμως να αποτελεί πρόκληση, δεδομένου ότι περιλαμβάνει *de facto* τη διαχείριση προσωπικών δεδομένων και επομένως ενέχει κινδύνους παραβίασης της ιδιωτικότητας (του προσωπικού απορρήτου) από την μη εξουσιοδοτημένη πρόσβαση, συλλογή και επεξεργασία προσωπικών ή και ευαίσθητων δεδομένων. Είναι λοιπόν πολύ σημαντικό κάθε λύση ηλεκτρονικής ταυτοποίησης να λαμβάνει πολύ σοβαρά υπόψη θέματα ιδιωτικότητας και να διασφαλίζει την ασφάλεια και προστασία των προσωπικών δεδομένων, πρωταρχικά γιατί αυτό αποτελεί βασικό ανθρώπινο δικαίωμα σύμφωνα με το Άρθρο 8 του Ευρωπαϊκού Συμφώνου Ανθρωπίνων Δικαιωμάτων (European Convention on Human Rights) αλλά και γιατί η Ευρωπαϊκή Οδηγία για την Προστασία των Προσωπικών Δεδομένων[2] προβλέπει συγκεκριμένους περιορισμούς για τη διαχείριση προσωπικών δεδομένων. Στο πλαίσιο αυτό, καθοριστικοί παράγοντες αποτελούν η σχετική ελευθερία των χωρών-μελών να προσδιορίσουν τις ειδικές συνθήκες κάτω από τις οποίες η διαχείριση προσωπικών δεδομένων είναι αποδεκτή και νόμιμη, τις εγγυήσεις που παρέχονται για την προστασία της ιδιωτικότητας, και τις συνθήκες κάτω από τις οποίες είναι επιτρεπτή η πρόσβαση σε προσωπικά δεδομένα. Όλα αυτά τα θέματα συνήθως

1 http://www.ermis.gov.gr/portal/page/portal/ermis/

2 Data Protection Directive (95/46/EC)

ρυθμίζονται σε επίπεδο χωρών-μελών μέσω της επίσημης νομοθεσίας (National Register Acts, Identity Card Acts, eGovernment Acts), με στόχο τη διασφάλιση της προστασίας των προσωπικών δεδομένων.

Παρόλα αυτά το θέμα της ηλεκτρονικής ταυτοποίησης οντοτήτων δεν είναι προς το παρόν συνολικά και επαρκώς θεσμοθετημένο σε Ευρωπαϊκό επίπεδο γιατί οι περισσότερες χώρες δεν έχουν ακόμα θεσμοθετήσει (προσδιορίσει νομικά) την έννοια της ηλεκτρονικής ταυτότητας σε εθνικό επίπεδο και γιατί το υφιστάμενο θεσμικό πλαίσιο (π.χ. η Ευρωπαϊκή Οδηγία για την Ηλεκτρονική Υπογραφή[3]) δεν καλύπτει όλα τα θέματα. Οι περισσότερες χώρες έχουν εξειδικεύσει την Οδηγία για την Ηλεκτρονική Υπογραφή με κανονισμούς που καθορίζουν θέματα υποδομής (π.χ. την υιοθέτηση ή όχι καρτών-ταυτοτήτων & επίσημων μητρώων) και θέματα πολιτικών αυθεντικοποίησης. Μόνον στην Αυστρία και πρόσφατα στη Φιλανδία[4] η έννοια της ηλεκτρονικής ταυτότητας είναι επαρκώς θεσμοθετημένη.

Αποτέλεσμα της διαφοροποίησης των προσεγγίσεων των χωρών-μελών της ΕΕ στην ερμηνεία της Ευρωπαϊκής Οδηγίας για την Προστασία Προσωπικών Δεδομένων και της θεσμικής ανεπάρκειας της Ευρωπαϊκής Οδηγίας για την Ηλεκτρονική Υπογραφή να προσδιορίσει την έννοια της ηλεκτρονικής ταυτότητας σε εθνικό επίπεδο, είναι η διασπορά και διαφοροποίηση των λύσεων διαχείρισης ηλεκτρονικών ταυτοτήτων πολιτών που υφίστανται ήδη στις χώρες-μέλη. Στο πλαίσιο αυτό, η παρούσα μελέτη αποσκοπεί στην παρουσίαση των τάσεων και καλών πρακτικών στην ανάπτυξη και λειτουργία λύσεων διαχείρισης ηλεκτρονικών ταυτοτήτων που προκύπτει από την ανάλυση των λύσεων σε επίπεδο χωρών μελών της ΕΕ, προκειμένου να αξιοποιηθεί η Ευρωπαϊκή εμπειρία στο πλαίσιο της επικείμενης υλοποίησης της ηλεκτρονικής κάρτας-ταυτότητας πολίτη στην Ελλάδα. Τα αποτελέσματα της μελέτης παρουσιάζονται στις παρακάτω ενότητες και συγκεκριμένα:

Στην ενότητα 2 εξετάζονται οι βασικές επιλογές που έχουν υιοθετηθεί από τις χώρες-μέλη της ΕΕ, όσον αφορά στη χρήση διακριτικών αυθεντικοποίησης (π.χ. ηλεκτρονικών καρτών-ταυτοτήτων) και στις πηγές δεδομένων που αξιοποιούνται για την ταυτοποίηση των πολιτών (έγκυρα μητρώα, μοναδικά αναγνωριστικά, χρήση βιομετρίας, κλπ).

Στην ενότητα 3 εξετάζουμε τις επιλογές συστημάτων αυθεντικοποίησης στις χώρες-μέλη της ΕΕ. Στην ανάλυση περιλαμβάνονται συστήματα που βασίζονται σε Υποδομή Δημόσιου Κλειδιού (PKI) και συστήματα που βασίζονται στη χρήση συνθηματικών. Επιπλέον, εξετάζουμε τις πολιτικές αυθεντικοποίησης που έχουν υιοθετηθεί στις χώρες-μέλη της ΕΕ ως προς τα επίπεδα εμπιστοσύνης.

Στην ενότητα 4 εξετάζουμε βασικές επιλογές πολιτικής που επηρεάζουν την οργάνωση της υποδομής και τη δημιουργία εμπιστοσύνης στις λύσεις διαχείρισης ηλεκτρονικών ταυτοτήτων στις χώρες-μέλη της ΕΕ. Συγκεκριμένα εξετάζουμε τις τάσεις που επικρατούν σχετικά με τις επιμέρους τομεακές λύσεις και τις λύσεις μικρής εμβέλειας καθώς και το βαθμό ανάμιξης του ιδιωτικού τομέα.

Τέλος, στην ενότητα 5 παραθέτουμε διαπιστώσεις και συμπεράσματα σχετικά με τις κυρίαρχες τάσεις που προκύπτουν από την ανάλυση των λύσεων (eIDM σε επίπεδο χωρών-μελών της ΕΕ και στην ενότητα 6 εκτιμήσεις σχετικά με την προβλεπόμενη εξέλιξη βασικών παραμέτρων του πλαισίου που θα διαμορφωθεί για τη χρήση ηλεκτρονικών ταυτοτήτων για τους πολίτες μέσα στην δεκαετία που διανύουμε.

3 eSignature Directive (1999/93/EC)

4 New Act on Electronic Authentication and Signatures, September 2009

2. Υποδομές και επιλογές ταυτοποίησης

Στην παρούσα ενότητα παρουσιάζονται οι βασικές επιλογές των λύσεων διαχείρισης ηλεκτρονικών ταυτοτήτων που έχουν υιοθετηθεί από τις χώρες-μέλη της ΕΕ, όσον αφορά στη χρήση διακριτικών αυθεντικοποίησης (π.χ. ηλεκτρονικών καρτών-ταυτοτήτων) και στις πηγές δεδομένων που αξιοποιούνται για την ταυτοποίηση των πολιτών. Εξετάζεται η χρήση μοναδικών αναγνωριστικών και οι πρακτικές που ακολουθούνται σχετικά με τα υφιστάμενα επίσημα μητρώα (national registers). Επιπλέον εξετάζεται η χρήση βιομετρίας και η χρήση κινητών τηλεφώνων για την ταυτοποίηση των πολιτών Διαπιστώνεται ότι οι λύσεις που έχουν υιοθετηθεί διαφέρουν αν και η κυρίαρχη τάση αφορά στη χρήση ηλεκτρονικών καρτών και τομεακών αναγνωριστικών (η αξιοποίηση καθολικού μοναδικού αναγνωριστικού δεν αποτελεί κοινή πρακτική) και ότι η χρήση έγκυρων μητρώων τυγχάνει ολοένα αυξανόμενης αποδοχής από τις χώρες-μέλη της ΕΕ.

2.1 Διακριτικά αυθεντικοποίησης (identity tokens)

Όσον αφορά στις επιλογές διακριτικών αυθεντικοποίησης 10 από τις 27 χώρες-μέλη της ΕΕ έχουν υιοθετήσει ηλεκτρονικές κάρτες-ταυτότητες που έχουν εκδοθεί και διαχειρίζονται κυρίως από δημόσιους και σε ορισμένες περιπτώσεις από ιδιωτικούς φορείς. Σε 7 χώρες (Βέλγιο, Εσθονία, Φιλανδία, Ιταλία, Λιθουανία, Πορτογαλία και Ισπανία) οι ηλεκτρονικές κάρτες εκδίδονται και διαχειρίζονται από αμιγώς δημόσιους φορείς ενώ στις υπόλοιπες 3 χώρες (Αυστρία, Ολλανδία και Σουηδία) από ιδιωτικούς παρόχους υπηρεσιών πιστοποίησης (ΠΥΠ) που όμως έχουν εξουσιοδοτηθεί από το κράτος[5]. Ενδεικτικά, 25 εκατομμύρια έξυπνες κάρτες-ταυτότητες πολιτών κυκλοφορούν τώρα στο Βέλγιο, διασφαλίζοντας την ταυτοποίηση και τη χρήση άνω των 250 ηλεκτρονικών υπηρεσιών, δημόσιων και εμπορικών.

Επιπλέον, 12 χώρες-μέλη της ΕΕ που χρησιμοποιούν προς το παρόν χάρτινες-πλαστικοποιημένες ταυτότητες βρίσκονται στο στάδιο σχεδιασμού ή μετάβασης σε συστήματα ταυτοποίησης πολιτών που βασίζονται σε ηλεκτρονικές κάρτες-ταυτότητες. Υπάρχουν και 4 χώρες-μέλη που ιστορικά δεν έχουν υιοθετήσει ποτέ τη χρήση ταυτοτήτων (Δανία, Ιρλανδία, Λετονία και Βρετανία) όμως και αυτές, με εξαίρεση τη Δανία και πολύ πρόσφατα (Ιούνιος 2010) τη Βρετανία, σχεδιάζουν την υιοθέτηση κάποιου είδους ηλεκτρονικής κάρτας-ταυτότητας στο άμεσο μέλλον.

Συμπεραίνουμε ότι οι ηλεκτρονικές κάρτες-ταυτότητες αποτελούν την κυρίαρχη τάση όσον αφορά στα διακριτικά αυθεντικοποίησης και αναμένεται η ευρύτερη υιοθέτηση τους τα προσεχή χρόνια.

2.2 Χρήση μοναδικών αναγνωριστικών

Τα μοναδικά αναγνωριστικά είναι κώδικες (με χαρακτήρες ή/και αριθμούς) που εκχωρούνται και συσχετίζονται αποκλειστικά με μια οντότητα (π.χ. ένα πολίτη) και μέσω των οποίων ο πολίτης αναγνωρίζεται μοναδικά από διαφορετικές ηλεκτρονικές υπηρεσίες. Τέτοια αναγνωριστικά στην Ελλάδα είναι ό Αριθμός Δελτίου Ταυτότητας, ο ΑΦΜ για πρόσβαση σε φορολογικές υπηρεσίες, ο ΑΜΚΑ για πρόσβαση σε υπηρεσίες πρόνοιας και κοινωνικής ασφάλισης.

Όλες όμως οι χώρες-μέλη της ΕΕ έχουν υιοθετήσει κάποιου είδους μοναδικά αναγνωριστικά, το θεσμικό όπως πλαίσιο που διέπει τη νομιμότητα της χρήσης τους διαφέρει αισθητά από χώρα σε χώρα. Οι προσεγγίσεις αναφορικά με την ταυτοποίηση οντοτήτων σε περιβάλλοντα ηλεκτρονικής διακυβέρνησης στον ευρωπαϊκό χώρο είναι δυνατό να ενταχθούν σε δύο γενικές κατηγορίες με βάση την αξιοποίηση ενός καθολικού μοναδικού αναγνωριστικού για όλες τις υπηρεσίες ή εναλλακτικά διαφορετικών μοναδικών αναγνωριστικών ανά υπηρεσία ή πλαίσιο υπηρεσιών.

5 eID Interoperability for PEGS: Update of Country Profiles, IDABC, October 2009

Είναι προφανές ότι η χρήση ενός καθολικού μοναδικού αναγνωριστικού γενικής χρήσης (generic national ID number) για όλες τις ηλεκτρονικές υπηρεσίες διευκολύνει τη διαχείριση της ταυτοποίησης και αυθεντικοποίησης στις υπηρεσίες αυτές. Είναι όμως επίσης σαφές ότι τα μοναδικά αναγνωριστικά που χορηγούνται στους πολίτες αποτελούν προσωπικά τους δεδομένα (με την έννοια ότι μέσω αυτών καθίσταται ευχερής ο μονοσήμαντος προσδιορισμός της ταυτότητας ενός ατόμου) και επομένως δε μπορούν να γίνουν αντικείμενο επεξεργασίας και αποθήκευσης παρά μόνο κάτω από πολύ συγκεκριμένες συνθήκες σύμφωνα με το Άρθρο 7 της Οδηγίας για την Προστασία των Προσωπικών Δεδομένων. Οι περιορισμοί αυτοί συνήθως ερμηνεύονται από πολλές χώρες-μέλη με τρόπο ώστε τα μοναδικά αναγνωριστικά να μπορούν να χρησιμοποιηθούν μόνο μέσα σε συγκεκριμένο πλαίσιο υπηρεσιών και για τον σκοπό που εκχωρήθηκαν. Επιπλέον, ορισμένες χώρες-μέλη της ΕΕ θεωρούν ότι η χρήση των μοναδικών αναγνωριστικών που χορηγούνται από το δημόσιο πρέπει να περιορίζεται στο πλαίσιο των δημόσιων υπηρεσιών και να μην επεκτείνεται η χρήση τους σε εμπορικές υπηρεσίες και εφαρμογές του ιδιωτικού τομέα για λόγους προστασίας της ιδιωτικότητας. Κατά συνέπεια, η χρήση τέτοιων αναγνωριστικών για τη διασυνοριακή ταυτοποίηση πολιτών είναι νομικά πολύπλοκη υπόθεση.

Μοναδικά αναγνωριστικά καθολικής χρήσης περιλαμβάνονται συνήθως σε ψηφιακά πιστοποιητικά με θεσμική και τεχνική πρόβλεψη για προστασία από ανεξέλεγκτη χρήση. Παραδείγματα αποτελούν τα ψηφιακά πιστοποιητικά που περιλαμβάνονται στις ηλεκτρονικές κάρτες-ταυτότητες του Βελγίου και της Εσθονίας. Η πρακτική αυτή όμως υπονομεύει μέχρις ένα βαθμό το πλαίσιο προστασίας προσωπικών δεδομένων στις χώρες αυτές.

Ορισμένες χώρες-μέλη (η Φιλανδία, η Αυστρία και σύντομα η Τσεχία) χρησιμοποιούν μοναδικά αναγνωριστικά καθολικής χρήσης που βασίζονται σε μηχανισμούς και αλγορίθμους κρυπτογράφησης και τα οποία **δεν** περιλαμβάνουν σημασιολογικές πληροφορίες (semantic information) που θα μπορούσαν να οδηγήσουν στον προσδιορισμό της ταυτότητας του πολίτη σε περίπτωση αθέμιτης χρήσης. Και στις δύο αυτές περιπτώσεις πάρθηκαν επιπλέον μέτρα για την προστασία της ιδιωτικότητας. Το μεν Φιλανδικό αναγνωριστικό (FINUID number) δεν έχει άλλη χρήση πέρα από την ταυτοποίηση (μέσω της Φιλανδικής ηλεκτρονικής κάρτας-ταυτότητας) και επομένως η επεξεργασία του είναι ιδιαίτερα περιορισμένη. Στην περίπτωση της Αυστρίας, ο προσωπικός αριθμός αναγνώρισης (source PIN) δεν εμφανίζεται σε καμιά περίπτωση στους παρόχους των υπηρεσιών χωρίς να είναι κρυπτογραφημένος, κάνοντας έτσι την κακόβουλη χρήση του πρακτικά αδύνατη.

Το θεσμικό πλαίσιο σε τουλάχιστον δύο χώρες (Γερμανία και Ουγγαρία) απαγορεύει την ταυτοποίηση πολιτών μέσω καθολικών μοναδικών αναγνωριστικών γενικής χρήσης, λόγω περιορισμών του απορρέουν από το Σύνταγμα των χωρών αυτών. Αυτό όμως δε σημαίνει αναγκαστικά ότι απαγορεύεται τελείως η χρήση μοναδικών αναγνωριστικών, αλλά ότι η χρήση των μοναδικών αναγνωριστικών πρέπει να περιορίζεται στο συγκεκριμένο πλαίσιο και για τον σκοπό που εκχωρήθηκαν, δηλαδή στο πλαίσιο των συγκεκριμένων υπηρεσιών στις οποίες αφορά.

Η Πορτογαλία αντιμετώπισε πρόσφατα το θέμα επιλογής και τρόπου χρήσης μοναδικών αναγνωριστικών στο πλαίσιο της εθνικής ηλεκτρονικής κάρτας-ταυτότητας. Στην περίπτωση αυτή ακολουθήθηκε η αντίθετη λογική από αυτή της Φιλανδίας. Η Πορτογαλική ηλεκτρονική κάρτα-ταυτότητα δεν περιλαμβάνει κάποιο νέο καθολικό αναγνωριστικό παρά μόνο τα 4 ήδη υφιστάμενα

τομεακά αναγνωριστικά, δηλαδή τον αριθμό ταυτότητας και τα αναγνωριστικά για φορολογικές υπηρεσίες, για υπηρεσίες πρόνοιας και κοινωνικής ασφάλισης και για υπηρεσίες υγείας.

Οι ίδιες επιφυλάξεις σχετικά με την προστασία της ιδιωτικότητας ισχύουν και για τα συστήματα ταυτοποίησης που βασίζονται στη χρήση συνθηματικών (username/authentication systems) δεδομένου ότι τα συνθηματικά αποτελούν de facto μοναδικά αναγνωριστικά τα όποια επιπροσθέτως δε διασφαλίζουν την ασφάλεια και την προστασία της ιδιωτικότητας και επομένως δεν είναι κατάλληλα για υπηρεσίες ηλεκτρονικής διακυβέρνησης επιπέδου 3 και άνω.

Οι παραπάνω εναλλακτικές προσεγγίσεις για την προστασία της ιδιωτικότητας των πολιτών και οι περιορισμοί στη χρήση μοναδικών αναγνωριστικών που απορρέουν από την Οδηγία 1995/46/ΕC πρέπει να ληφθούν υπόψη στο σχεδιασμό της Ελληνικής λύσης ταυτοποίησης πολιτών. Παρότι όλες οι λύσεις που έχουν υιοθετηθεί από τις χώρες-μέλη της ΕΕ περιέχουν μοναδικά αναγνωριστικά, οι επιλογές τους διαφέρουν σημαντικά ως προς τη χρήση υφιστάμενων ή νέων καθολικών προστατευμένων αναγνωριστικών, μη-προστατευμένων αναγνωριστικών, αναγνωριστικών που μπορούν να χρησιμοποιηθούν μόνο μέσα στο συγκεκριμένο πλαίσιο και για τον σκοπό που εκχωρήθηκαν και αναγνωριστικών που ελέγχονται από τον ιδιωτικό τομέα. Όπως όμως γίνεται αντιληπτό, η αξιοποίηση ενός καθολικού μοναδικού αναγνωριστικού για ταυτοποίηση πολιτών στα μέλη κράτη της Ευρωπαϊκής Ένωσης δεν αποτελεί κοινή πρακτική.

2.3 Χρήση έγκυρων μητρώων και συναίνεση του πολίτη

Εκτός από τα διακριτικά αυθεντικοποίησης και τα αναγνωριστικά, μια τρίτη πηγή άντλησης δεδομένων για την ταυτοποίηση πολιτών αποτελούν τα υφιστάμενα επίσημα μητρώα πολιτών τα οποία οι δημόσιες υπηρεσίες δημιουργούν και στη συνέχεια διαχειρίζονται. Τα μητρώα αυτά συνήθως προκύπτουν από τις συναλλαγές του πολίτη με τις δημόσιες υπηρεσίες και έτσι περιλαμβάνουν προσωπικά στοιχεία τα οποία διαφοροποιούνται ανάλογα με την περίπτωση που εξυπηρετούν. Προκειμένου όμως να διασφαλιστεί η εγκυρότητα και η ποιότητα των προσωπικών στοιχείων είναι απαραίτητο να υφίσταται μια & μοναδική έγκυρη πηγή άντλησης κάθε ενός από τα επιμέρους στοιχεία (δεδομένα επαλήθευσης) που συνδέονται με την πιστοποίηση της ταυτότητας μιας οντότητας. Αυτή η προσέγγιση αποτελεί την **αρχή έγκυρης πηγής** - the authentic source principle – και συνεπάγεται ότι τα επιμέρους στοιχεία για την ταυτοποίηση μιας οντότητας που υφίστανται στα έγκυρα μητρώα μπορούν να επαναχρησιμοποιηθούν από κάθε σύννομο φορέα, έτσι ώστε να μην επιβαρύνεται ο πολίτης με την επαναληπτική παροχή των ιδίων στοιχείων κάθε φορά χρησιμοποιεί τις δημόσιες υπηρεσίες.

Στον αντίποδα βρίσκεται η πολιτοκεντρική (citizen centric) προσέγγιση η οποία απαιτεί την **ρητή συγκατάθεση του πολίτη** (user consent, όπως εννοείται από το άρθρο 7(α) της Ευρωπαϊκής Οδηγίας για την Προστασία των Προσωπικών δεδομένων), δίνοντας του τη δυνατότητα να επιλέγει ποια και πόσα από τα προσωπικά του δεδομένα είναι διατεθειμένος να καταθέσει ο ίδιος προκειμένου να ταυτοποιηθεί, κάθε φορά χρησιμοποιεί τις δημόσιες υπηρεσίες. Η συγκατάθεση πρέπει να είναι ελεύθερη, ρητή και ειδική δήλωση βουλήσεως, που εκφράζεται με τρόπο σαφή, και εν πλήρη επίγνωση, και με την οποία το υποκείμενο των δεδομένων, αφού προηγουμένως ενημερωθεί, δέχεται να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν[6].

Όλες οι χώρες-μέλη της ΕΕ διαθέτουν δημοτολόγια και άλλα μητρώα με δεδομένα ταυτοποίησης των πολιτών (π.χ. στην Ελλάδα το μητρώο του TAXIS στη ΓΓΠΣ του Υπουργείου Οικονομικών), στα οποία όλοι οι πολίτες εγγράφονται με τη γέννηση τους ή κατόπιν νομικών η διοικητικών συναλλαγών με τις αρμόδιες διοικητικές αρχές, οι οποίες είναι επιφορτισμένες να διασφαλίζουν την ακρίβεια και ακεραιότητα των στοιχείων αυτών. Το Άρθρο 6(d) της Οδηγίας για την Προστασία των Προσωπικών Δεδομένων απαιτεί από τους διαχειριστές των μητρώων (δηλαδή από τις ίδιες τις διοικητικές αρχές) να διασφαλίζουν την ακρίβεια και ακεραιότητα των προσωπικών δεδομένων που συντηρούν. Επιπλέον, η απαίτηση αυτή αποτελεί υποχρέωση των διοικητικών αρχών στο πλαίσιο της «καλής διακυβέρνησης». Η εγκυρότητα όμως των μητρώων αυτών δεν είναι αυτονόητη, δεδομένου ότι

6 Πλαίσιο Ψηφιακής Αυθεντικοποίησης, ΥΠΕΣ, Αύγουστος 2007

περιέχουν διαπιστωμένα λάθη και παραλήψεις σε αρκετές χώρες-μέλη της ΕΕ περιλαμβανομένης της Πολωνία, της Τσεχίας αλλά και της Ελλάδας. Σ' όλες αυτές τις περιπτώσεις έχουν ήδη αναληφθεί διορθωτικές πρωτοβουλίες.

Σύμφωνα με τα στοιχεία του 2009[7], η αρχή έγκυρης πηγής και η χρήση έγκυρων μητρώων τυγχάνει ολοένα αυξανόμενης αποδοχής από τις χώρες-μέλη της ΕΕ, παρόλο που η θεσμική κατοχύρωση της αφορά μόνο σε 6 χώρες (Βέλγιο, Φιλανδία, Εσθονία, Γαλλία, Ιρλανδία, Λιθουανία). Άλλες 8 χώρες κάνουν ήδη χρήση έγκυρων μητρώων ανεπίσημα όμως, χωρίς να την έχουν θεσμοθετήσει (Βρετανία, Λουξεμβούργο, Ολλανδία, Πολωνία, Πορτογαλία, Σλοβενία, Ισπανία και Σουηδία), ενώ 2 χώρες αναφέρουν άμεσα σχέδια (Βουλγαρία και Μάλτα) για χρήση έγκυρων μητρώων στο πλαίσιο της ταυτοποίησης πολιτών.

Από την άλλη μεριά, η πολιτοκεντρική προσέγγιση και η ρητή συγκατάθεση του πολίτη (user consent) είναι σαφώς προτιμητέα όσον αφορά στην προστασία των προσωπικών δεδομένων και εν' τέλει στη συμμόρφωση στο πνεύμα και το γράμμα της Οδηγίας για την Προστασία των Προσωπικών Δεδομένων. Επισημαίνουμε όμως ότι για τους σκοπούς της ηλεκτρονικής διακυβέρνησης οι χώρες μέλη της ΕΕ που ήδη υιοθετούν ή έχουν την τάση να υιοθετήσουν την αρχή της έγκυρης πηγής, δημιουργούν ένα ειδικό θεσμικό πλαίσιο (National Register Acts, Identity Card Acts, eGovernment Acts) όσον αφορά στη διαχείριση των προσωπικών δεδομένων, το οποίο προβλέπει την επεξεργασία των πληροφοριών αυτών χωρίς να είναι απαραίτητη η ρητή συναίνεση του χρήστη.

2.4 Χρήση βιομετρίας για ταυτοποίηση πολιτών

Μόνον πέντε από τις χώρες-μέλη της ΕΕ κάνουν χρήση βιομετρίας στο πλαίσιο της ταυτοποίησης πολιτών (Ιταλία, Λιθουανία, Ολλανδία, Πορτογαλία και Ισπανία) με βάση τα δακτυλικά αποτυπώματα. Όλες οι υπόλοιπες χώρες δεν χρησιμοποιούν και δεν σχεδιάζουν να κάνουν χρήση βιομετρικής ταυτοποίησης για υπηρεσίες ηλεκτρονικής διακυβέρνησης.

2.5 Η χρήση κινητών τηλεφώνων για ταυτοποίηση πολιτών

Η χρήση κινητών τηλεφώνων για ταυτοποίηση πολιτών στο πλαίσιο παροχής δημόσιων ηλεκτρονικών υπηρεσιών βρίσκεται ακόμα σε πειραματικό στάδιο. Παρόλο που 6 χώρες-μέλη διαθέτουν λύσεις αυθεντικοποίησης που βασίζονται σε κινητά τηλέφωνα (Austria, Estonia, Lithuania, the Netherlands, Poland, Slovenia) οι υπόλοιπες δεν προγραμματίζουν ακόμα να υιοθετήσουν τέτοιες λύσεις στο άμεσο μέλλον.

7 eID Interoperability for PEGS: Update of Country Profiles, IDABC, October 2009

3. Συστήματα και πολιτικές αυθεντικοποίησης

Στην παρούσα ενότητα εξετάζουμε τη χρήση συστημάτων αυθεντικοποίησης στις χώρες-μέλη της ΕΕ. Στην ανάλυση περιλαμβάνονται συστήματα που βασίζονται σε Υποδομή Δημόσιου Κλειδιού (PKI) και συστήματα που βασίζονται στη χρήση συνθηματικών. Επιπλέον, εξετάζουμε τις πολιτικές αυθεντικοποίησης που έχουν υιοθετηθεί στις χώρες-μέλη της ΕΕ ως προς τα επίπεδα εμπιστοσύνης.

3.1 Συστήματα Δημόσιου Κλειδιού (PKI)

Οι περισσότερες χώρες της ΕΕ (24 από 27) έχουν υιοθετήσει συστήματα αυθεντικοποίησης οντοτήτων (φυσικών και νομικών προσώπων) που βασίζονται σε Υποδομή Δημόσιου Κλειδιού (PKI). Για τις μισές περίπου από τις χώρες αυτές η διαχείριση των σχετικών λειτουργιών και υπηρεσιών αποτελεί αποκλειστική αρμοδιότητα δημοσίων φορέων σε κεντρικό ή τοπικό επίπεδο, ενώ κάποιες έχουν εκχωρήσει συγκεκριμένες αρμοδιότητες και υπηρεσίες διαχείρισης σε μικτά σχήματα και κοινοπραξίες δημόσιου-ιδιωτικού τομέα (public/private partnerships), βλ. ΠΑΡΑΡΤΗΜΑ.

Στις χώρες που έχουν υιοθετήσει συστήματα PKI περιλαμβάνονται οι 7 χώρες (Βέλγιο, Εσθονία, Φιλανδία, Ιταλία, Λιθουανία, Πορτογαλία και Ισπανία) που έχουν εκδώσει ηλεκτρονικές κάρτες-ταυτότητες τις οποίες διαχειρίζονται αποκλειστικά δημόσιοι φορείς και οι 3 χώρες (Αυστρία, Ολλανδία και Σουηδία) που έχουν εκδώσει ηλεκτρονικές κάρτες-ταυτότητες που διαχειρίζονται από ιδιωτικούς παρόχους υπηρεσιών πιστοποίησης (ΠΥΠ) που όμως έχουν εξουσιοδοτηθεί από το κράτος. Στις περισσότερες περιπτώσεις οι ηλεκτρονικές κάρτες-ταυτότητες περιέχουν ψηφιακά πιστοποιητικά για αυθεντικοποίηση αλλά και για ηλεκτρονική υπογραφή. Η Αυστριακή κάρτα αποτελεί εξαίρεση δεδομένου ότι περιλαμβάνει μόνο ένα ψηφιακό πιστοποιητικό για ηλεκτρονική υπογραφή το οποίο όμως χρησιμοποιείται και για αυθεντικοποίηση.

Μια από τις αιτίες στις οποίες οφείλεται η κυριαρχία των συστημάτων PKI είναι ότι ενώ η Ευρωπαϊκή Οδηγία για την Ηλεκτρονική Υπογραφή δεν αφορά συγκεκριμένα στην ταυτοποίηση-αυθεντικοποίηση, η Οδηγία ερμηνεύεται στο πλαίσιο αυτό από τις χώρες-μέλη της ΕΕ και επομένως συνήθως υιοθετείται η τεχνολογία PKI για ψηφιακές υπογραφές που καλύπτει τις ανάγκες που προκύπτουν από την εφαρμογή της Οδηγίας σε εθνικό επίπεδο. Έτσι το εργαλείο για ψηφιακές υπογραφές γίνεται de facto εργαλείο για αυθεντικοποίηση, αν και αυτό δεν προκύπτει νομικά.

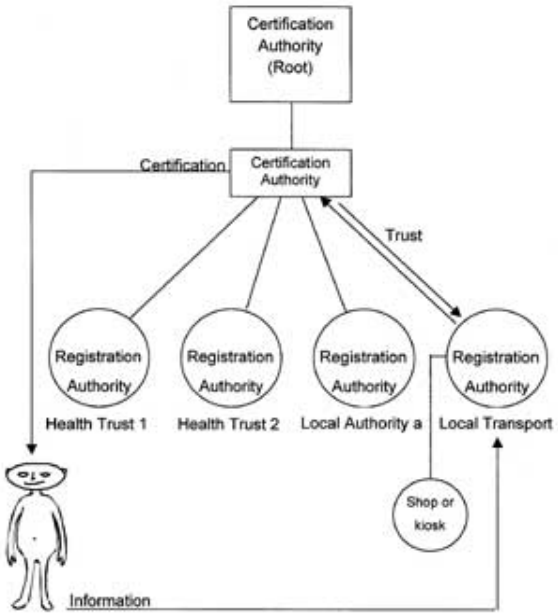
3.2 Χρήση συνθηματικών (username/password)

Η τάση για υιοθέτηση συστημάτων αυθεντικοποίησης που βασίζονται στη χρήση συνθηματικών εξακολουθεί να είναι επίσης ισχυρή στις χώρες-μέλη της ΕΕ (περιλαμβανομένης και της χρήσης συνθηματικών μιας χρήσης, two factor authentication και time specific password calculators). Συνολικά, 19 χώρες χρησιμοποιούν συστήματα αυθεντικοποίησης που βασίζονται στη χρήση συνθηματικών. Οι περισσότερες χώρες (15) χρησιμοποιούν απλά συστήματα με χρήση συνθηματικών single factor; οι υπόλοιπες 4 (Βέλγιο, Εσθονία, Φιλανδία, Λιθουανία) χρησιμοποιούν συστήματα multifactor (password lists & password calculators).

3.3 Πολιτικές αυθεντικοποίησης και επίπεδα εμπιστοσύνης

Όπως γίνεται φανερό από τα παραπάνω οι περισσότερες χώρες έχουν υιοθετήσει παράλληλα συστήματα αυθεντικοποίησης που βασίζονται σε Υποδομή Δημόσιου Κλειδιού (PKI) -με διακριτικά χαλαρής (soft tokens) ή σκληρής αποθήκευσης (κάρτες)- και συστήματα που βασίζονται στη χρήση συνθηματικών (single factor, multifactor). Το επίπεδο ασφάλειας και προστασίας των προσωπικών δεδομένων που παρέχουν τα συστήματα αυτά διαφέρει από χώρα σε χώρα και από σύστημα σε σύστημα, με τα συστήματα PKI να προσφέρουν μεγαλύτερη ασφάλεια.

Για να καθορίσουν το βαθμό αξιοπιστίας των συστημάτων αυτών, ορισμένες χώρες έχουν υιοθετήσει πολιτικές αυθεντικοποίησης που προσδιορίζουν συγκεκριμένα επίπεδα εμπιστοσύνης, λαμβάνονται υπόψη την ασφάλεια των δεδομένων, δηλαδή το βαθμό κρισιμότητας και τις επιπτώσεις που μπορεί να προκύψουν λόγω της παράνομης και αθέμιτης χρήσης των δεδομένων αυτών. Αυτό είναι σημαντικό στοιχείο μιας εθνικής στρατηγικής διαχείρισης ηλεκτρονικών ταυτοτήτων, δεδομένου ότι δίνει τη δυνατότητα στους δημοσίους φορείς παροχής ηλεκτρονικών υπηρεσιών να προσδιορίζουν πολλαπλά επίπεδα εμπιστοσύνης ανάλογα με την κρισιμότητα των συναλλαγών τους (κίνδυνοι και επιπτώσεις) και να απαιτούν αντιστοίχως συγκεκριμένα επίπεδα ασφάλειας τα οποία ενδεχομένως αντιστοιχούν σε διαφορετικά συστήματα αυθεντικοποίησης. Τέτοιες πολιτικές αυθεντικοποίησης είναι πολύ χρήσιμες για τον εξορθολογισμό μιας εθνικής πολιτικής για τη διαχείριση ηλεκτρονικών ταυτοτήτων ακριβώς γιατί παρέχει στους δημόσιους φορείς ένα αντικειμενικό πρότυπο σύμφωνα με το οποίο μπορούν να προσδιορίσουν το επιθυμητό επίπεδο ασφάλεια και εμπιστοσύνης των συναλλαγών τους και άρα να επιλέξουν το κατάλληλο σύστημα αυθεντικοποίησης.



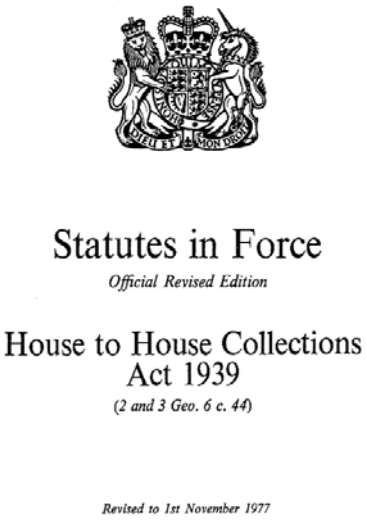
Οι πολιτικές αυθεντικοποίησης είναι επίσης πολύ χρήσιμες και στο πλαίσιο διασυνοριακής λειτουργικότητας των Ευρωπαϊκών λύσεων διαχείρισης ηλεκτρονικών ταυτοτήτων, γιατί επιτρέπουν στις διαφορετικές εφαρμογές και υπηρεσίες που λειτουργούν σε εθνικό επίπεδο να απαιτούν συγκεκριμένα επίπεδα εμπιστοσύνης αντί για συγκεκριμένες τεχνικές λύσεις για τη διασφάλιση της αξιοπιστίας τους. Η προσέγγιση αυτή έχει ήδη υιοθετηθεί στο πλαίσιο του συγχρηματοδοτούμενου από την Ευρωπαϊκή Ένωση μεγάλου πιλοτικού έργου (LSP) για την ασφαλή διασυνοριακή ταυτοποίηση πολιτών STORK[8], σκοπός του οποίου είναι να εφαρμόσει ένα ευρωπαϊκό διαλειτουργικό σύστημα αναγνώρισης και πιστοποίησης των ηλεκτρονικών ταυτοτήτων, το οποίο θα επιτρέπει στις επιχειρήσεις, στους πολίτες και στους δημόσιους υπαλλήλους να χρησιμοποιούν τις εθνικές ηλεκτρονικές τους ταυτότητες σε οποιοδήποτε Κράτος-Μέλος της Ε.Ε. Παράλληλα θα παράσχει διασυνοριακές υπηρεσίες αναγνώρισης ηλεκτρονικών ταυτοτήτων στον τομέα της ηλεκτρονικής διακυβέρνησης και θα προτείνει μεθόδους για την ανάπτυξη τέτοιου είδους υπηρεσιών από τα κράτη-μέλη.

Στις 16 χώρες που έχουν συνειδητοποιήσει την ανάγκη για τη διαφοροποίηση των επιπέδων εμπιστοσύνης ανάλογα με τις ανάγκες ασφάλειας των συναλλαγών με διαφανή και συστηματικό τρόπο, εφαρμόζεται ήδη κάποια μορφή πολύ-επίπεδης πολιτικής αυθεντικοποίησης. Επισήμως όμως αναγνωρισμένες πολιτικές πολύ-επίπεδης αυθεντικοποίησης συναντώνται μόνο σε 4 χώρες-μέλη (Αυστρία, Δανία, Γαλλία και Βρετανία). Αξίζει να σημειώσουμε ότι όλες οι υφισταμένες πολιτικές αυθεντικοποίησης αφορούν εθνικές λύσης διαχείρισης ηλεκτρονικών ταυτοτήτων με εξαίρεση αυτή της Εσθονίας που προβλέπει κριτήρια διασυνοριακής αξιολόγησης ταυτοτήτων που έχουν εκδοθεί σε άλλες χώρες-μέλη της ΕΕ με βάση τα επίπεδα εμπιστοσύνης.

8 http://www.eid-stork.eu

4. Εθνικά ρυθμιστικά πλαίσια και προσεγγίσεις

Οι βασικοί παράγοντες που επηρεάζουν τα Εθνικά Ρυθμιστικά Πλαίσια (National Register Acts, Identity Card Acts, eGovernment Acts) που διαμορφώνονται στο πλαίσιο των λύσεων διαχείρισης ηλεκτρονικών ταυτοτήτων στην Ευρώπη είναι εφ' ενός ποια είναι τα ελάχιστα προσωπικά δεδομένα που είναι απαραίτητα προκειμένου να ταυτοποιηθεί ο πολίτης κάθε φορά χρησιμοποιεί τις δημόσιες υπηρεσίες και αφ' εταίρου πως διασφαλίζεται η εμπιστοσύνη στην ακρίβεια αυτής της πληροφορίας. Η προσέγγιση στα θέματα αυτά, ειδικά όσον αφορά στη δημιουργία εμπιστοσύνης μεταξύ των παρόχων υπηρεσιών πιστοποίησης (identity providers) και των παρόχων υπηρεσιών (δημόσιων ή ιδιωτικών) προς τον πολίτη (relying third parties), διαφέρει ριζικά από χώρα σε χώρα μέλος την ΕΕ, όπως έχουμε ήδη διαπιστώσει παραπάνω. Υπάρχουν όμως και κοινά στοιχεία στις εθνικές ρυθμιστικές προσεγγίσεις τα οποία παρουσιάζονται στις επόμενες ενότητες.


Statutes in Force

Official Revised Edition

House to House Collections Act 1939

(2 and 3 Geo. 6 c. 44)

Revised to 1st November 1977

4.1 Αποκέντρωση και εσωτερική εναρμόνιση λύσεων και συστημάτων eIDM

Ένα κοινό στοιχείο είναι ότι καμία από τις χώρες-μέλη της ΕΕ δεν βασίζεται αποκλειστικά σε ένα και μοναδικό κεντρικό σύστημα ή λύση διαχείρισης ηλεκτρονικών ταυτοτήτων. Οι περισσότερες χώρες έχουν επιλέξει ένα περιορισμένο αριθμό συστημάτων σαν την πρωταρχική τους λύση. Όμως, μικρότερης εμβέλειας συστήματα συνεχίζουν να συνυπάρχουν και να λειτουργούν παράλληλα, συνήθως στο πλαίσιο κάποιας συγκεκριμένης υπηρεσίας (π.χ. για φορολογικές υπηρεσίες) ή εφαρμογής (π.χ. αιτήσεις για πιστοποιητικά).

Είναι σημαντικό να επισημάνουμε ότι η διαχείριση ηλεκτρονικών ταυτοτήτων στην Ευρώπη, στο πλαίσιο ηλεκτρονικών συναλλαγών των πολιτών με τη δημόσια διοίκηση (eGovernment), δεν έχει ωριμάσει πλήρως και βρίσκεται ακόμα στο στάδιο της εσωτερικής εναρμόνισης (internal consolidation) στις περισσότερες από τις χώρες μέλη. Η τάση είναι η σταδιακή κατάργηση των τομεακών λύσεων και των λύσεων μικρής εμβέλειας και η αντικατάσταση τους από ένα περιορισμένο αριθμό συστημάτων ταυτοποίησης, έτσι ώστε να μεγιστοποιείται η απόδοση της επένδυσης. Υπάρχουν όμως δύο εξαιρέσεις σ' αυτή την τάση για εσωτερική εναρμόνιση και για κεντρικές λύσεις διαχείρισης ηλεκτρονικών ταυτοτήτων.

- Η πρώτη εξαίρεση οφείλεται συνήθως σε πολιτικές αποφάσεις για την καθιέρωση αποκεντρωμένων λύσεων, έτσι ώστε οι τοπικές και εξειδικευμένες λύσεις και τα συστήματα να έχουν τη δυνατότητα να καλύπτουν πλήρως συγκεκριμένες ανάγκες (τοπικές ή ομάδων χρηστών) με τον κατάλληλο τρόπο. Παραδείγματα τέτοιων περιπτώσεων περιλαμβάνουν την αποκεντρωμένη έκδοση ηλεκτρονικών καρτών-ταυτοτήτων που αφορούν σε συγκεκριμένες περιφέρειες με διοικητική αυτονομία (π.χ. η Γαλλική Carte Vitale και η Ιταλική CNS), η έκδοση διακριτικών αυθεντικοποίησης κατάλληλων για συγκεκριμένες ομάδες χρηστών εξαιτίας της ιδιότητας τους ή του ρόλου τους (π.χ. η κάρτα CMD για τα στελέχη της δημόσιας διοίκησης στην Ιταλία και τα ψηφιακά πιστοποιητικά αυθεντικοποίησης για τους δικηγόρους και τους συμβολαιογράφους στην Πορτογαλία). Στις περιπτώσεις αυτές η επιλογή για την υιοθέτηση εξειδικευμένων λύσεων για συγκεκριμένες ομάδες χρηστών τεκμηριώνεται με συγκεκριμένα πλεονεκτήματα που απορρέουν από την επιλογή αυτή.
- Η δεύτερη εξαίρεση αφορά στην υιοθέτηση εξειδικευμένων λύσεων διαχείρισης ηλεκτρονικών ταυτοτήτων για την επεξεργασία ευαίσθητων δεδομένων. Μεταξύ άλλων, τέτοια δεδομένα είναι

όσα έχουν μία σαφή και στενή σχέση με την υγεία (παρελθούσα, παρούσα και μέλλουσα κατάσταση) αλλά και δεδομένα που σχετίζονται με τη λήψη παροχών κοινωνικής πρόνοιας. Παραδείγματα τέτοιων εξειδικευμένων λύσεων αποτελούν η χρήση ηλεκτρονικών καρτών υγείας και κοινωνικής ασφάλισης και ηλεκτρονικών καρτών επαγγελματιών του ιατροφαρμακευτικού κλάδου. Δεδομένου ότι η ίδια η Ευρωπαϊκή και Ελληνική νομοθεσία εμπεριέχει ειδικές ρυθμίσεις για την προστασία των ευαίσθητων δεδομένων, δεν αποτελεί έκπληξη η διαφοροποίηση αυτών των συστημάτων από τις πρωταρχικές λύσεις eIDM σε πολλές από τις χώρες-μέλη της ΕΕ.

Είναι ενδιαφέρον στο σημείο αυτό να επισημάνουμε ότι ορισμένες χώρες-μέλη της ΕΕ (όπως η Αυστρία, η Ουγγαρία και η Ιταλία) έχουν επιλέξει να δημιουργήσουν μια ενιαία υποδομή ηλεκτρονικών καρτών-ταυτοτήτων που βασίζεται σε συγκεκριμένες αρχιτεκτονικές και πρότυπα. Στις περιπτώσεις αυτές η συνολική λύση διαχείρισης ηλεκτρονικών ταυτοτήτων προσδιορίζεται από την ικανοποίηση μιας σειράς προδιαγραφών και απαιτήσεων, με αποτέλεσμα οι επιμέρους λύσεις να μπορούν να υλοποιηθούν με διαφορετικούς τρόπους ανάλογα με τις ανάγκες. Η Αυστριακή ηλεκτρονική κάρτα του πολίτη είναι ένα πολύ καλό παράδειγμα αυτής της προσέγγισης, δεδομένου ότι οι επιμέρους λύσεις να μπορούν να υλοποιηθούν με διαφορετικές τεχνολογίες, περιλαμβανομένης της υποστήριξης για ταυτοποίηση μέσω καρτών κινητών τηλεφώνων. Έτσι ο περιορισμός για χρήση παραδοσιακών έξυπνων καρτών δεν υφίσταται για τους Αυστριακούς πολίτες. Παρόμοιες αλλά λιγότερο ριζοσπαστικές προσεγγίσεις έχουν ακολουθήσει η Ουγγαρία (κάρτα HUNEID) και η Ιταλία (κάρτα CMD/ATA-E).

4.2 Ανάμιξη του ιδιωτικού τομέα

Μια άλλη κοινή προσέγγιση που παρατηρείται αφορά στην ανάμιξη του ιδιωτικού τομέα στο πλαίσιο της διαχείρισης ηλεκτρονικών ταυτοτήτων στις χώρες-μέλη της ΕΕ, η οποία θεωρείται απαραίτητη για πολλούς λόγους. Οι περισσότερες από τις χώρες αυτές αναγνωρίζουν την καίρια σημασία της υιοθέτησης των λύσεων διαχείρισης ηλεκτρονικών ταυτοτήτων και από τις επιχειρήσεις του ιδιωτικού τομέα. Η άποψη που κυριαρχεί είναι ότι το επιχειρηματικό μοντέλο για μια λύση που αφορά αποκλειστικά στο δημόσιο τομέα είναι ιδιαίτερα περιοριστικό για να είναι ελκυστικό για τους πολίτες, δεδομένου ότι η συχνότητα των συναλλαγών των πολιτών με τη δημόσια διοίκηση με ταυτοποίηση είναι σχετικά χαμηλή. Αυτό βέβαια δεν ισχύει για τις περιπτώσεις ομάδων χρηστών όπως οι δικηγόροι, οι λογιστές, οι συμβολαιογράφοι και οι επαγγελματίες του ιατροφαρμακευτικού κλάδου, οι οποίοι λόγω της ιδιότητας τους έχουν συχνές δοσοληψίες με τη δημόσια διοίκηση. Για τις ομάδες αυτές προκρίνονται λύσεις που αφορούν αποκλειστικά στο δημόσιο τομέα.

Καλό παράδειγμα ανάμιξης του ιδιωτικού τομέα στη διαχείρισης ηλεκτρονικών ταυτοτήτων αποτελεί η Σουηδία, όπου ο δημόσιος τομέας εκμεταλλεύτηκε μια ήδη εγκατεστημένη και επιτυχώς λειτουργούσα υποδομή δημόσιου κλειδιού που ήταν διαθέσιμη στους πελάτες των ιδιωτικών τραπεζών με αποτέλεσμα η συχνότητα χρήσης ηλεκτρονικών ταυτοτήτων για υπηρεσίες ηλεκτρονικής διακυβέρνησης από τους πολίτες να είμαι μεγαλύτερη στη Σουηδία από οπουδήποτε αλλού στην Ευρώπη[9].

Προκύπτουν όμως κάποια θέματα από την ανάμιξη του ιδιωτικού τομέα στη διαχείριση ηλεκτρονικών ταυτοτήτων, τα οποία σχετίζονται με την προστασία των προσωπικών δεδομένων των πολιτών. Ένα βασικό πρόβλημα που προκύπτει αναγκαστικά από την ανάμιξη του ιδιωτικού τομέα στις λειτουργίες διαχείρισης ηλεκτρονικών ταυτοτήτων αφορά στην επαναχρησιμοποίηση και επεξεργασία προσωπικών δεδομένων έξω από το συγκεκριμένο πλαίσιο

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

συναλλαγών για το οποίο έχει δοθεί η συγκατάθεση, πράγμα το οποίο δε συνάδει με τις προβλέψεις της Ευρωπαϊκής νομοθεσίας για την Προστασία Προσωπικών Δεδομένων. Επιπλέον, υπάρχει ο κίνδυνος να συλλέγονται και να επεξεργάζονται περισσότερα από τα ελάχιστα απαιτούμενα προσωπικά δεδομένα για την παροχή συγκεκριμένης υπηρεσίας ή κατηγορίας υπηρεσιών, δεδομένου ότι η νομοθεσία προβλέπει ότι θα πρέπει να συλλέγονται εκείνα και μόνο όσα είναι αναγκαία και κατάλληλα για την εκπλήρωση του σκοπού αυτού (υπό στενή έννοια αναλογικότητα των δεδομένων). Η δε εφαρμογή του περιορισμού αυτού είναι πολύ δύσκολο να ελεγχθεί πρακτικά.

Συνολικά, όσον αφορά στην ανάμιξη του ιδιωτικού τομέα στη διαχείριση ηλεκτρονικών ταυτοτήτων στις χώρες-μέλη της ΕΕ, ξεχωρίζουν δύο βασικές περιπτώσεις:

- Το σύστημα και οι λειτουργίες διαχείρισης ηλεκτρονικών ταυτοτήτων να ελέγχονται από τον ιδιωτικό τομέα, αλλά να αξιοποιούνται και από υπηρεσίες και εφαρμογές του δημόσιου τομέα (eGovernment). Παραδείγματα αποτελούν τα συστήματα αυθεντικοποίησης που ελέγχονται από ιδιωτικές τράπεζες τα οποία χρησιμοποιούνται και για συναλλαγές με δημόσιες υπηρεσίες σε χώρες όπως η Εσθονία, η Λιθουανία και η Σουηδία και οι ιδιωτικοί πάροχοι υπηρεσιών πιστοποίησης (ΠΥΠ) που εκδίδουν ψηφιακά πιστοποιητικά τα οποία μπορούν να χρησιμοποιηθούν και για συναλλαγές με δημόσιες υπηρεσίες σε χώρες όπως η Αυστρία και το Λουξεμβούργο.
- Το σύστημα και οι λειτουργίες διαχείρισης ηλεκτρονικών ταυτοτήτων ελέγχεται από το δημόσιο τομέα, αλλά αξιοποιείται και από υπηρεσίες και εφαρμογές του ιδιωτικού τομέα. Αυτό συμβαίνει συνήθως στις χώρες όπου κυριαρχούν οι ηλεκτρονικές κάρτες-ταυτότητες που εκδίδονται από δημόσιους φορείς. Το πιο πρόσφατο παράδειγμα αποτελεί η Γερμανία όπου ανακοινώθηκε ότι από το Νοέμβριο του 2010 πρόκειται να εκδοθεί ηλεκτρονική κάρτα-ταυτότητα για τους πολίτες που θα υποστηρίζει και ηλεκτρονική υπογραφή και θα χρησιμοποιείται για συναλλαγές με δημόσιες αλλά και ιδιωτικές υπηρεσίες. Σημειώνεται ότι η συγκεκριμένη κάρτα θα υποστηρίζεται και από αυτόματες μηχανές πώλησης τσιγάρων προκειμένου να επιβεβαιώνεται η ηλικία του αγοραστή!

Μια ενδιαφέρουσα προσέγγιση αφορά συγκεκριμένα στον έλεγχο των διαδικασιών εγγραφής και έκδοσης των διακριτικών αυθεντικοποίησης στα εγκατεστημένα συστήματα PKI, που γίνεται είτε αποκλειστικά από δημόσιους φορείς ή από κοινοπραξίες δημόσιου-ιδιωτικού τομέα, όπως φαίνεται στο ΠΑΡΑΡΤΗΜΑ.

- Σε 13 χώρες χρησιμοποιούνται 17 συστήματα PKI όπου η διαδικασίας εγγραφής και έκδοσης των διακριτικών αυθεντικοποίησης γίνεται αποκλειστικά από δημόσιους φορείς. Από τα 17 αυτά συστήματα, τα 12 χρησιμοποιούνται στο πλαίσιο παροχής ηλεκτρονικών υπηρεσιών **και** από τον ιδιωτικό τομέα.
- Σε 15 χώρες χρησιμοποιούνται συστήματα PKI όπου η διαδικασίας εγγραφής και έκδοσης των διακριτικών αυθεντικοποίησης γίνεται από μικτούς φορείς, δηλαδή από κοινοπραξίες δημόσιου-ιδιωτικού τομέα. Προφανώς όλα αυτά τα συστήματα χρησιμοποιούνται και στο πλαίσιο παροχής ηλεκτρονικών υπηρεσιών από τον ιδιωτικό τομέα.

Από τα παραπάνω στοιχεία είναι φανερό ότι ο βαθμός και ο τρόπος ανάμιξης του ιδιωτικού τομέα στις εθνικές λύσεις διαχείρισης ηλεκτρονικών ταυτοτήτων και η υιοθέτηση των λύσεων αυτών και από τις επιχειρήσεις του ιδιωτικού τομέα αποτελούν κομβικά σημεία στο σχεδιασμό τέτοιων λύσεων από της χώρες-μέλη της ΕΕ.

5. Συμπεράσματα και κυρίαρχες τάσεις

Στην παρούσα ενότητα παραθέτουμε συνοπτικά διαπιστώσεις και συμπεράσματα που προκύπτουν από την ανάλυση των πρακτικών που έχουν υιοθετηθεί από τις 27 χώρες-μέλη της ΕΕ. Πέρα από θέματα νομιμότητας και σεβασμού των ανθρωπίνων δικαιωμάτων, είναι σαφές ότι η διασφάλιση της προστασίας των προσωπικών δεδομένων και η ελαχιστοποίηση των πιθανοτήτων παραβίασης τους αποτελεί παράγοντα που επηρεάζει άμεσα τη αποδοχή και το επίπεδο υιοθέτησης και χρήσης αυτών των ηλεκτρονικών υπηρεσιών.

Είναι σημαντικό να επισημάνουμε στο σημείο αυτό ότι:

- Η διαχείριση ηλεκτρονικών ταυτοτήτων στην Ευρώπη, στο πλαίσιο ηλεκτρονικών συναλλαγών των πολιτών με τη δημόσια διοίκηση (eGovernment), δεν έχει ωριμάσει πλήρως και βρίσκεται ακόμα στο στάδιο της εσωτερικής εναρμόνισης στις περισσότερες από τις χώρες μέλη.
- Η επιτυχής αντιμετώπιση των θεμάτων ιδιωτικότητας και προστασίας των προσωπικών δεδομένων πολιτών στο πλαίσιο της υλοποίησης και υιοθέτησης λύσεων ηλεκτρονικής ταυτοποίησης είναι εκ των ων ουκ άνευ προϋπόθεση για την δημιουργία κλίματος εμπιστοσύνης τους πολίτες-χρήστες των υπηρεσιών.
- Ο τρόπος ανάμιξης του ιδιωτικού τομέα στις εθνικές λύσεις διαχείρισης ηλεκτρονικών ταυτοτήτων και η υιοθέτησης των λύσεων αυτών και από τις επιχειρήσεις του ιδιωτικού τομέα αποτελούν κομβικά σημεία στο σχεδιασμό τέτοιων λύσεων από της χώρες-μέλη της ΕΕ.

Όσον αφορά στις κυρίαρχες τάσεις, διαπιστώνεται ότι αν και οι λύσεις που έχουν υιοθετηθεί από τις χώρες-μέλη της ΕΕ διαφέρουν ριζικά, αναδεικνύονται οι εξής τάσεις:

Η σταδιακή κατάργηση των τομεακών λύσεων και των λύσεων μικρής εμβέλειας και η αντικατάσταση τους από ένα περιορισμένο αριθμό πρωταρχικών συστημάτων ταυτοποίησης, έτσι ώστε να μεγιστοποιείται η απόδοση της επένδυσης. Υπάρχουν όμως δύο εξαιρέσεις σ' αυτή την τάση που αφορούν σε τοπικές ή εξειδικευμένες λύσεις που καλύπτουν συγκεκριμένες ανάγκες τοπικές ή ομάδων χρηστών εξαιτίας της ιδιότητας τους ή του ρόλου τους (π.χ. λογιστές, συμβολαιογράφοι) και για την επεξεργασία ευαίσθητων δεδομένων (π.χ. ιατρικών δεδομένων).

Οι περισσότερες χώρες έχουν υιοθετήσει παράλληλα συστήματα αυθεντικοποίησης που βασίζονται σε Υποδομή Δημόσιου Κλειδιού (περίπου το 90% των χωρών), με διακριτικά χαλαρής (soft tokens) ή σκληρής αποθήκευσης (κάρτες), *και συστήματα που βασίζονται στη χρήση συνθηματικών* (περίπου το 70% των χωρών) με συνθηματικά single factor, multifactor. Το επίπεδο ασφάλειας και προστασίας των προσωπικών δεδομένων που παρέχουν τα συστήματα αυτά διαφέρει από χώρα σε χώρα και από σύστημα σε σύστημα, με τα συστήματα PKI να προσφέρουν μεγαλύτερη ασφάλεια.

Η κυρίαρχη τάση αφορά στη χρήση ηλεκτρονικών καρτών και τομεακών αναγνωριστικών, η δε αρχή της έγκυρης πηγής και η χρήση έγκυρων μητρώων τυγχάνει ολοένα αυξανόμενης αποδοχής από τις χώρες-μέλη της ΕΕ.

- Οι ηλεκτρονικές κάρτες-ταυτότητες αποτελούν την κυρίαρχη τάση και αναμένεται η ευρύτερη υιοθέτηση τους τα προσεχή χρόνια. Περίπου το 80% των χωρών μελών της ΕΕ είτε έχουν ήδη υιοθετήσει είτε βρίσκονται στο στάδιο σχεδιασμού ή μετάβασης σε συστήματα που βασίζονται σε ηλεκτρονικές κάρτες-ταυτότητες. Στις περισσότερες περιπτώσεις οι κάρτες περιέχουν ψηφιακά πιστοποιητικά για αυθεντικοποίηση αλλά και για ηλεκτρονική υπογραφή.
- Όλες οι χώρες-μέλη της ΕΕ έχουν υιοθετήσει λύσεις που περιέχουν μοναδικά αναγνωριστικά, το θεσμικό όπως πλαίσιο που διέπει τη νομιμότητα της χρήσης τους διαφέρει αισθητά από χώρα σε χώρα. Οι επιλογές διαφέρουν ως προς τη χρήση υφιστάμενων ή νέων, καθολικών προστατευμένων και μη-προστατευμένων αναγνωριστικών, αναγνωριστικών που μπορούν να χρησιμοποιηθούν μόνο μέσα στο συγκεκριμένο τομέα και για τον σκοπό που εκχωρήθηκαν, και αναγνωριστικών που ελέγχονται από τον ιδιωτικό τομέα. Είναι όμως σαφές ότι η αξιοποίηση ενός

καθολικού μοναδικού αναγνωριστικού για ταυτοποίηση πολιτών στα μέλη κράτη της ΕΕ δεν αποτελεί κοινή πρακτική.

- Περίπου το 50% των χωρών μελών της ΕΕ (14 χώρες) κάνουν ήδη χρήση έγκυρων μητρώων, παρόλο που η θεσμική τους κατοχύρωση προβλέπεται μόνο από 6 χώρες. Η προσέγγιση που απαιτεί τη ρητή συγκατάθεση του πολίτη (user consent) και είναι σαφώς προτιμητέα όσον αφορά στη συμμόρφωση με την Οδηγία για την Προστασία των Προσωπικών Δεδομένων. Επισημαίνουμε ότι χώρες μέλη της ΕΕ που έχουν ήδη υιοθετήσει την αρχή της έγκυρης πηγής, έχουν δημιουργήσει ένα ειδικό θεσμικό πλαίσιο, το οποίο προβλέπει την επεξεργασία των πληροφοριών αυτών χωρίς να είναι απαραίτητη η ρητή συναίνεση του χρήστη.

Μόνον το 20% (5 χώρες) από τις χώρες-μέλη της ΕΕ κάνουν χρήση βιομετρίας στο πλαίσιο της ηλεκτρονικής ταυτοποίησης πολιτών με βάση τα δακτυλικά αποτυπώματα, η δε χρήση κινητών τηλεφώνων για ταυτοποίηση πολιτών στο πλαίσιο παροχής δημόσιων ηλεκτρονικών υπηρεσιών βρίσκεται ακόμα σε πειραματικό στάδιο.

Περίπου το 50% των χωρών μελών της ΕΕ (16 χώρες) εφαρμόζουν ήδη κάποια μορφή πολύ-επίπεδης πολιτικής αυθεντικοποίησης, έχοντας συνειδητοποιήσει την ανάγκη για τη διαφοροποίηση των επιπέδων εμπιστοσύνης ανάλογα με τις ανάγκες ασφάλειας των συναλλαγών με διαφανή και συστηματικό τρόπο. Επισήμως όμως αναγνωρισμένες πολιτικές πολύ-επίπεδης αυθεντικοποίησης συναντώνται μόνο σε 4 χώρες-μέλη.

Η ανάμιξη του ιδιωτικού τομέα στο πλαίσιο της διαχείρισης ηλεκτρονικών ταυτοτήτων στις χώρες-μέλη της ΕΕ θεωρείται απαραίτητη. Οι περισσότερες από τις χώρες αναγνωρίζουν την καίρια σημασία της υιοθέτησης των λύσεων διαχείρισης ηλεκτρονικών ταυτοτήτων και από τις επιχειρήσεις / παρόχους υπηρεσιών του ιδιωτικού τομέα καθώς επίσης και της ανάμιξης του ιδιωτικού τομέα στις λειτουργίες διαχείρισης ηλεκτρονικών ταυτοτήτων. Παραμένει όμως ο προβληματισμός που αφορά στην επαναχρησιμοποίηση και επεξεργασία προσωπικών δεδομένων έξω από το συγκεκριμένο πλαίσιο συναλλαγών για το οποίο έχει δοθεί η συγκατάθεση.

Η μελέτη και τα σχετικά στοιχεία είναι διαθέσιμα στη διεύθυνση www.observatory.gr.

6. Εκτιμήσεις για τη μελλοντική εξέλιξη

Στην παρούσα ενότητα παραθέτουμε συνοπτικά ορισμένες παρατηρήσεις σχετικά με την προβλεπόμενη εξέλιξη βασικών παραμέτρων του πλαισίου που θα διαμορφωθεί για τη χρήση ηλεκτρονικών ταυτοτήτων για τους πολίτες μέσα στην δεκαετία που διανύουμε.

6.1 Η έννοια της ταυτότητας – ομαδικής και ατομικής

Η έννοια της ατομικής ταυτότητας είναι καθοριστική για την κοινωνική συμπεριφορά ανθρώπων και ομάδων δεδομένου ότι μέσω αυτής είναι δυνατή η σύνδεση των ατομικών ενεργειών και επιλογών του κάθε ένα από εμάς (επιλογών που αφορούν στο παρελθόν και το παρόν) με τις επιπτώσεις που έχουν αυτές στο μέλλον. Το ίδιο ισχύει και στο διαδίκτυο, όπου είναι φανερό ότι η ηλεκτρονική ταυτότητα αποτελεί το πιο σημαντικό άυλο στοιχείο της κοινωνίας της πληροφορίας. Στο πλαίσιο αυτό το διαδίκτυο θέτει ήδη μεγάλες προκλήσεις και ενδεχομένως δημιουργεί κινδύνους, γιατί καθιστά την έννοια της ατομικής ηλεκτρονικής πια ταυτότητας περισσότερο κατακερματισμένη, αποσπασματική και με περιορισμένη χρονική διάρκεια, ενώ δημιουργεί ανασφάλεια στους πολίτες λόγω της μικρότερης προστασίας της ιδιωτικότητας που παρέχει. Επιπλέον έχει διαπιστωθεί ότι η έννοια της διαδικτυακής ταυτότητας χαλαρώνει τους κοινωνικούς κανόνες και περιορισμούς που βοηθούν στο να ευθυγραμμίζονται τα ατομικά με τα ομαδικά ή συλλογικά συμφέροντα.

Για το μέλλον, προκύπτουν ερωτήματα σχετικά με τα επίπεδα ιδωτικότητας και αυτονομίας που θα μπορούν να εξασφαλίσουν οι πολίτες κατά τη χρήση ηλεκτρονικών υπηρεσιών που απαιτούν ταυτοποίηση, σχετικά με την εγκυρότητα συλλογικών διαδικτυακών δράσεων και ενεργειών (π.χ. δράσεων επηρεασμού και διαμόρφωσης διοικητικών και πολιτικών αποφάσεων), και σχετικά με τον τρόπο δημιουργίας διαδικτυακών ομάδων (π.χ. σχετικά με τις διαδικασίες εγγραφής και αποχώρησης από αυτές).

6.2 Η έννοια της ιδιωτικότητας και μέσα προστασίας της

Κάποιας μορφής προστασία της ιδιωτικότητας και των προσωπικών δεδομένων θα υπάρχει στο τέλος της δεκαετίας που διανύουμε, η οποία θα προωθείται είτε από τη δημόσια διοίκηση (με την εξέλιξη των υφιστάμενων σχετικών θεσμικών πλαισίων), είτε από τις επιχειρήσεις (μέσω της αυτορύθμισης ή/και της προστασίας της ιδιωτικότητας με κόστος – at a premium - για τον πολίτη), είτε από τους ίδιους τους πολίτες (μέσω της πίεσης της κοινωνίας των πολιτών στις διαδικασίες λήψης αποφάσεων). Η μελλοντική προσέγγιση θα καθοδηγείται κυρίως από οικονομικά κριτήρια, δηλαδή αναμένεται να τείνει περισσότερο προς την ανάληψη κινδύνου παρά προς την εφαρμογή περιορισμών που μπορεί μεν να διασφαλίζουν την προστασία των προσωπικών δεδομένων, κάνουν όμως τις λύσεις περισσότερο πολύπλοκες και ακριβές. Θα ισχύουν οι γενικές αρχές προστασίας της ιδιωτικότητας, οι οποίες όμως θα περιλαμβάνουν ισχυροποιημένη την έννοια της προσωπικής ευθύνης (personal liability) και μηχανισμούς επιβολής κυρώσεων (redress instruments). Αναμένεται επίσης ότι οι τεχνολογικές λύσεις (ειδικά όσον αφορά στην ασφάλεια) που θα υιοθετηθούν θα παίξουν μεγάλο ρόλο στην ενίσχυση της προστασίας των προσωπικών δεδομένων. Οι πολίτες θα έχουν σχεδόν απόλυτο έλεγχο (μέσω θεσμικά προδιαγεγραμμένων εργαλείων) που θα περιλαμβάνει το δικαίωμα ανάκλησης και ενδεχομένως την αποκλειστική διαχείριση και επιμέλεια των προσωπικών δεδομένων τους.

6.3 Η σημασία της δημιουργίας εμπιστοσύνης

Η δημιουργία εμπιστοσύνης είναι καθοριστική για την ευρεία αποδοχή και αξιοπιστία των συστημάτων διαχείρισης ηλεκτρονικών ταυτοτήτων και αφορά σε όλες τις εμπλεκόμενες οντότητες (πολίτες, δημόσια διοίκηση, παρόχους ηλεκτρονικών υπηρεσιών, ιδιωτικούς φορείς υποστήριξης λειτουργιών eIDM). Σύμφωνα με τις υφιστάμενες τάσεις, δεν φαίνεται ότι ο δημόσιος τομές θα είναι ο τελικός κυρίαρχος του παιγνιδιού με την έννοια του ελέγχου των υποδομών και των λειτουργιών ταυτοποίησης και αυθεντικοποίησης. Η ίδια η αποκεντρωμένη και άναρχη δομή του διαδικτύου (end-to-end principle) βρίσκεται σε αντιπαράθεση με την επιβολή ισχυρών ιεραρχικών «εκ-των-άνω» προσεγγίσεων και κανόνων και επομένως προβλέπεται μια πιο ισότιμη σχέση συνεργασίας μεταξύ

των εμπλεκομένων οντοτήτων. Καθοριστικό ρόλο στη δημιουργία εμπιστοσύνης θα έχει η διαφάνεια των διαδικασιών που θα διαφυλάσσονται από αξιόπιστα θεσμικά πλαίσια και οι τεχνολογικές λύσεις, που θα διαμορφωθούν εν μέσω αντιμαχόμενων προσεγγίσεων για ανοικτά ή κλειστά δίκτυα, στα οποία όμως η συμμετοχή του ιδιωτικού τομέα θα είναι αναπόφευκτη.

ΠΑΡΑΡΤΗΜΑ

1. Εγκατεστημένα PKI συστήματα που ελέγχονται αποκλειστικά από Δημόσιους Φορείς

Χώρα	Περιγραφή	Εκδοτική Αρχή	Προσβάσιμο στον Ιδιωτικό τομέα
Βέλγιο	Ψηφιακό Πιστοποιητικό στην ηλεκτρονική κάρτα - ταυτότητα	Μέσω των Δημοτικών και Κοινοτικών Αρχών	Ναι
Εσθονία	Ψηφιακό Πιστοποιητικό στην ηλεκτρονική κάρτα - ταυτότητα	Citizenship and Migration Board (CMB)	Ναι
Φινλανδία	Ψηφιακό Πιστοποιητικό στην ηλεκτρονική κάρτα - ταυτότητα FINEID	Μέσω τοπικών αστυνομικών αρχών	Ναι
Γαλλία	Ψηφιακό Πιστοποιητικό στην κάρτα Daily Life	Τοπική Αυτοδιοίκηση	Όχι
Ελλάδα	Δίκτυο "ΣΥΖΕΥΞΙΣ" για τους δημοσίους υπαλλήλους χρησιμοποιώντας πιστοποιητικό ψηφιακής υπογραφής, είτε σε έξυπνες κάρτες είτε σε διακριτικά χαλαρής αποθήκευσης	Το αρμόδιο Υπουργείο, ανάλογα με τον δημόσιο υπάλληλο	Όχι
Ουγγαρία	Κάρτες εκπαίδευσης που εμπεριέχουν πιστοποιητικά ψηφιακής υπογραφής (μόνο για καθηγητές και διοικητικό προσωπικό; όχι για μαθητές)	Υπουργείο Παιδείας	Όχι
Ιταλία	Ψηφιακό / Αναγνωρισμένο πιστοποιητικό στην κάρτα - ταυτότητα	Μέσω των Δημοτικών αρχών	Ναι
	Ψηφιακό / Αναγνωρισμένο πιστοποιητικό στην κάρτα CNS	Εξαρτάται από την τοπική αρχή που έχει αναλάβει την έκδοση της κάρτας	Όχι
	Ψηφιακό / Αναγνωρισμένο πιστοποιητικό στην κάρτα CMD (κάρτα δημοσίων υπαλλήλων)	Την αρμόδια κρατική υπηρεσία (ανάλογα με την κάρτα: πχ Υπουργείο Άμυνας)	Όχι
Λετονία	Ψηφιακά / Αναγνωρισμένα πιστοποιητικά σε έξυπνες κάρτες του ιδιωτικού τομέα	Από τις τοπικές ΔΟΥ (εφορία) - Απαιτείται διαβατήριο για να γίνει η αίτηση	Ναι
Λιθουανία	Ψηφιακό Πιστοποιητικό στην ηλεκτρονική κάρτα - ταυτότητα πολιτών	Μέσω των Κοινοτικών αρχών	Ναι
	Ψηφιακό Πιστοποιητικό στην κάρτα - ταυτότητα των δημοσίων υπαλλήλων	Την αρμόδια κρατική υπηρεσία (ανάλογα με την κάρτα)	Ναι
Μάλτα	Μη αναγνωρισμένα πιστοποιητικά ψηφιακής υπογραφής	Maltese government; see http://repository.ca.gov.mt	Ναι

Πορτογαλία	Ψηφιακό Πιστοποιητικό στην εθνική κάρτα - ταυτότητα	INCM (Νομισματοκοπείο Πορτογαλίας)	Ναι
Σλοβενία	Αναγνωρισμένο πιστοποιητικό ψηφιακής υπογραφής που περιλαμβάνει ένα μοναδικό σύστημα αναγνώρισης συνδεδεμένο σε μια βάση δεδομένων	Αρχή Πιστοποίησης του Υπουργείου Δημόσιας Διοίκησης	Ναι
Ισπανία	Ψηφιακό Πιστοποιητικό στην εθνική κάρτα - ταυτότητα (ή μελλοντική ηλεκτρονική κάρτα διαμονής)	Τεχνικό Γραφείο έκδοσης κάρτας - ταυτότητας *(Officina Técnica del DNI electrónico)*	Ναι *(μερικές τράπεζες)*

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

Χώρα	Περιγραφή	Εκδοτική Αρχή	Προσβάσιμο στον Ιδιωτικό τομέα
Αυστρία	Αναγνωρισμένο πιστοποιητικό ψηφιακής υπογραφής στην κάρτα πολίτη	Εξαρτάται από την έκδοση της κάρτας	Ναι. Μπορούν να εκδώσουν την κάρτα φορείς του ιδιωτικού τομέα
Βέλγιο	Αναγνωρισμένα και μη αναγνωρισμένα software πιστοποιητικά ψηφιακής υπογραφής	Αναγνωρισμένοι πάροχοι υπηρεσιών πιστοποίησης, CSPs	Ναι
Βουλγαρία	Ψηφιακή υπογραφή μέσω αναγνωρισμένων διακριτικών χαλαρής αποθήκευσης	CSPs καταχωρημένοι στο Σύστημα Επικοινωνιών της Βουλγαρίας - Regulation Commission	Ναι
Τσεχία	Ψηφιακή υπογραφή μέσω αναγνωρισμένων πιστοποιητικών (είτε με διακριτικά χαλαρής αποθήκευσης (το πιο σύνηθες) είτε κατ' εξαίρεση με έξυπνες κάρτες)	Γνωστά ως CSPs. Το πιστοποιητικό περιλαμβάνει τον αριθμό μητρώου του ασφαλιστικού φορέα, ο οποίος χρησιμοποιείται για λόγους πιστοποίησης	Ναι
	Ψηφιακή υπογραφή μέσω αναγνωρισμένων πιστοποιητικών (είτε με διακριτικά χαλαρής αποθήκευσης (το πιο σύνηθες) είτε κατ' εξαίρεση με έξυπνες κάρτες)	Γνωστά ως CSPs. Η ψηφιακή υπογραφή χρησιμοποιείται σε ηλεκτρονικά έγγραφα που περιέχουν και άλλα σημαντικά στοιχεία αναγνώρισης, όπως ο ΑΔΤ, τα οποία έπειτα χρησιμοποιούνται για λόγους πιστοποίησης	Ναι
Δανία	Εξειδικευμένη ψηφιακή υπογραφή OCES (διακριτικό χαλαρής αποθήκευσης; Στο μέλλον μπορεί και σε διακριτικό σκληρής αποθήκευσης)	TDC, ιδιωτικό αναγνωρισμένο CSP. Το πιστοποιητικό εμπεριέχει ένα σημαντικό στοιχείο αναγνώρισης το οποίο συνδέεται με τον αριθμό μητρώου (CPR number) για φυσικά πρόσωπα; αλλά ο αριθμός μητρώου δεν αποκομίζεται χωρίς έννομη εντολή.	Ναι
Εσθονία	Mobile-PKI/Mobile-ID	Σύστημα PKI που βασίζεται σε κινητά τηλέφωνα	Ναι
Γαλλία	Ψηφιακό Πιστοποιητικό στην Κάρτα Ζωής	Διαθέσιμα Ασφαλιστικών Φορέων Υγείας. Ο αριθμός αναγνώρισης είναι ο ADELI και/ή ο SIRET	Ναι

Λιθουανία	Αναγνωρισμένα πιστοποιητικά ψηφιακής υπογραφής, είτε σε διακριτικά χαλαρής αποθήκευσης είτε σε έξυπνες κάρτες	Τρία αναγνωρισμένα CSPs είναι προς το παρόν διαθέσιμα στην Λιθουανία	Ναι
	Mobile-PKI/Mobile-ID	Σύστημα PKI που βασίζεται σε κινητά τηλέφωνα	Ναι
Ολλανδία	Ψηφιακά Πιστοποιητικά (http://www.pkioverheid.nl/)	Ένας αριθμός ιδιωτικών CSPs	Ναι
Πολωνία	Αναγνωρισμένα πιστοποιητικά ψηφιακής υπογραφής, είτε σε διακριτικά χαλαρής αποθήκευσης είτε σε έξυπνες κάρτες	Τρεις αναγνωρισμένες Αρχές Πιστοποίησης: η Certum (www.certum.pl), η Sigillum (www.sigillum.pl.com.pl) και η Szafir (www.kir.com.pl)	Ναι
Πορτογαλία	Αναγνωρισμένα διακριτικά χαλαρής αποθήκευσης ψηφιακής υπογραφής για δικηγόρους, νομικούς συμβούλους ή συμβολαιογράφους	*Ordem dos Advocados* (Δικηγορικός Σύλλογος), *Câmara dos Solicitadores* (Σύνδεσμος Νομικών Συμβούλων) και *Ordem dos Notários* (Σύνδεσμος Συμβολαιογράφων)	Ναι
Ρουμανία	Αναγνωρισμένα και μη αναγνωρισμένα διακριτικά χαλαρής αποθήκευσης ψηφιακής υπογραφής	Ιδιωτικά CSPS Trans sped, Certsign, Digisign και Internet DomReg	Ναι
Σλοβακία	Αναγνωρισμένα διακριτικά χαλαρής αποθήκευσης ψηφιακής υπογραφής	Επικυρωμένα CSPs ιδιωτικού τομέα	Ναι
Σλοβενία	Αναγνωρισμένο πιστοποιητικό ψηφιακής υπογραφής; συνήθως εμπεριέχει ένα επίσημο στοιχείο αναγνώρισης (όπως ο αριθμός φορολογικού μητρώου)	Τρία επικυρωμένα CSPs ιδιωτικού τομέα	Ναι
Ισπανία	Αναγνωρισμένα πιστοποιητικά ψηφιακής υπογραφής, είτε σε διακριτικά χαλαρής αποθήκευσης είτε σε έξυπνες κάρτες – χρήση μοναδικού αριθμού αναγνωρισης.	Επικυρωμένα και αναγνωρισμένα CSPs	Ναι
Σουηδία	Εξειδικευμένα πιστοποιητικά, είτε σε διακριτικά χαλαρής αποθήκευσης είτε σε έξυπνες κάρτες. Δύο ξεχωριστά πιστοποιητικά, ένα για ταυτοποίηση και ένα για υπογραφή.	Πιστοποιητικά εκδίδονται από φορείς του ιδιωτικού τομέα (τραπεζικές συμφωνίες μεταξύ 8 τραπεζών συνθέτουν το BankID, η τράπεζα Nordea, η εταιρία τηλεπικοινωνιών Telia Sonera και η εταιρία πληροφορικής Steria). Το Δελτίο Αστυνομικής Ταυτότητας εκδίδεται από την Αστυνομική Αρχή (έχει αναπτυχθεί, αλλά δεν είναι πλήρως εγκεκριμένο για χρήση)	Ναι
Ηνωμένο Βασίλειο	Αναγνωρισμένα διακριτικά χαλαρής αποθήκευσης ψηφιακής υπογραφής	Εμπορικό Επιμελητήριο Βρετανίας και Equifax	Ναι