ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΔΙΔΑΚΤΙΚΗΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

- Διπλωματική Εργασία -

ΔΙΑΧΕΙΡΙΣΗ ΤΑΥΤΟΤΗΤΑΣ

ΣΙΜΑΡΟΥ ΦΩΤΕΙΝΗ, Α.Μ. Ε/01148

Πειραιάς, 10/10/2011

Περιεχόμενα

Λίστα Πινάκων

Ευχαριστίες

Η παρούσα Διπλωματική Εργασία εκπονήθηκε στο πλαίσιο των σπουδών μου στο Προπτυχιακό Πρόγραμμα Σπουδών του Τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς.

Θα ήθελα να ευχαριστήσω ιδιαίτερα των επιβλέπων καθηγητή μου, Κάτσικα Σωκράτη του Τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς για τη συμβολή του στην ολοκλήρωση αυτής της εργασίας, για τη διαρκή υποστήριξη και τις πολύτιμες συμβουλές που μου προσέφερε για την συγγραφή της παρούσας εργασίας.

1. Εισαγωγή

1.1 Ποιο Θέμα Διαπραγματεύεται η Εργασία

Η κοινωνία των πληροφοριών καθημερινά παρέχει οφέλη στα άτομα, τις επιχειρήσεις και τις οργανώσεις. Η αυξανόμενη διείσδυση των νέων τεχνολογιών στις καθημερινές πρακτικές των ανθρώπων οδηγεί στον επαναπροσδιορισμό θεμελιωδών εννοιών οι οποίες οφείλουν να προσαρμοστούν στα δεδομένα και στις ιδιαιτερότητες του ψηφιακού περιβάλλοντος.

Η διαχείριση ταυτότητας αποτελεί ένα ζήτημα που αν και αποτελεί διαδικασία ρουτίνας στην καθημερινή ζωή, η μεταφορά των αντίστοιχων πρακτικών στο διαδίκτυο δημιουργεί μια επιπρόσθετη πολυπλοκότητα. Η ανάγκη διαχείρισης ταυτότητας ανέκυψε αφενός λόγω της ενσωμάτωσης του ηλεκτρονικού επιχειρείν στις αγοραστικές συνήθειες των καταναλωτών και αφετέρου λόγω τις σταδιακής διασύνδεσης των πληροφοριακών συστημάτων μεταξύ συνεργαζόμενων επιχειρήσεων.

Ο συνδυασμός αυτών των δύο τάσεων που αφορά στην συμπεριφορά του ατόμου ως εργαζόμενος και ως καταναλωτής ανέδειξε την διαχείριση ταυτότητας σε θέμα μείζονος σημασίας. Παράλληλα, η τάση ανασχεδιασμού των λειτουργιών του Δημοσίου Τομέα με επίκεντρο τον πολίτη όπως αυτή εκδηλώθηκε μέσα από την Ηλεκτρονική Διακυβέρνηση δημιούργησε την επιπλέον ανάγκη διαχείρισης ταυτότητας και στις συναλλαγές με το Δημόσιο.

Αναφορικα στον τομέα του η-επιχειρίν, κάθε επιχείρηση που προσφέρει συναλλαγές στο διαδίκτυο συλλέγει στοιχεία ταυτότητας των πελατών (συνήθως ονοματεπώνυμο, διεύθυνση και άλλα δεδομένα) προκειμένου να αποδώσει κωδικό χρήστη και συνθηματικό τα οποία επιτρέπουν την πρόσβαση στις διαδικασίες πληρωμής. Από την άλλη πλευρά, ο πελάτης είναι υποχρεωμένος να διαχειρίζεται ένα διαρκώς αυξανόμενο αριθμό κωδικών χρήστη και συνθηματικών, κάνοντας δύσχρηστη τη χρήση αυτού του είδους των συναλλαγών. Κατ'επεκταση αναιρείται το ασφαλές περιβάλλον, καθώς τα συστήματα γίνονται εκ των πραγμάτων ευάλωτα και απειλείται η ασφάλεια των ίδιων των συναλλαγών (Pato & Rouault, 2003).

Η δεύτερη παράμετρος που ανέδειξε τη σημασία της διαχείρισης ταυτότητας είναι η ολοκλήρωση εταιρικών συστημάτων. Η ανάγκη για συγκέντρωση και

ολοκληρωμένη διαχείριση της πληροφορίας καθώς και η επίδραση διαφόρων τάσεων του μάνατζμεντ .

Επίσης η αναδιάρθρωση επιχειρηματικών διαδικασιών (BPR) οδήγησε στην αναμόρφωση των πληροφοριακών συστημάτων ώστε να εξυπηρετούν δέσμες επιχειρήσεων. Κάτι τέτοιο γίνεται εφικτό με την κατάλληλη επιλογή και χρήση προγραμμάτων από μέλη των ενδιαφερόμενων επιχειρήσεων οι οποίοι θα έχουν το ρόλο των χρηστών των αντίστοιχων προγραμμάτων. Έτσι, προτείνονται προγράμματα διαχειριζόμενα από το χρήστη όσον αφορά την διαχείριση των ταυτοτήτων.

Σε αυτά τα προγράμματα τοποθετούνται οι ανάλογοι χρηστές και τα τεχνολογικά μέσα που θα χρησιμοποιηθούν. Στο σύστημα εξετάζεται το πλήρες φάσμα αναγκών των χρηστών σε σχέση με το νόμο μυστικότητας. Παράλληλα απαιτείται αλληλεπίδραση μεταξύ των χρηστών για να αναπτυχθούν κατάλληλες στρατηγικές και να επιτευχθούν τα επιθυμητά αποτελέσματα.

Το ζήτημα διαχείρισης ταυτότητας καθώς και το σύνολο των θεμάτων που ανέκυψαν κατά την ανάπτυξη και εφαρμογή λύσεων στον ιδιωτικό τομέα είτε στα πλαίσια εταιρικών συστημάτων είτε στο λιανεμπόριο, μεταφέρθηκε και στον δημόσιο τομέα.

Η ηλεκτρονική διακυβέρνηση ως όραμα τοποθετεί τον πολίτη στο επίκεντρο σημαντικού αριθμού δημοσίων υπηρεσιών σε συνδυασμό με την συνολική προσπάθεια δημιουργίας ενός αποδοτικού δημοσίου τομέα αναπτύσσοντας πληθώρα συστημάτων τα οποία πλέον απαιτούν μια συγκροτημένη στρατηγική διαχείρισης ταυτότητας.

Οι δημόσιες υπηρεσίες πάντα υπήρξαν οι βασικοί φορείς που απέδιδαν, διαχειρίζονταν και πιστοποιούσαν την ταυτότητα των πολιτών. Για το λόγο αυτό η διαχείριση ταυτότητας στις Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης μπορεί να γίνει αντιληπτή ως η διαχείριση των δεδομένων προσωπικού χαρακτήρα που αυθεντικοποιούν ένα άτομο. Επομένως η διαχείριση ταυτότητας δεν αφορά απλά την αυθεντικοποίηση ενός πολίτη στις συναλλαγές του, αλλά την δημιουργία και διαχείριση μιας όλο και πιο λεπτομερούς εικόνας του ατόμου με πληθώρα ευαίσθητων πληροφοριών.

1.2 Μεθοδολογία Υλοποίησης της Εργασίας

Στόχος της παρούσας μελέτης είναι να αναλύσει τα ζητήματα που προκύπτουν από την προσέγγιση της διαχείρισης ταυτότητας στον δημόσιο τομέα, αναγνωρίζοντας επίσης τις ιδιαιτερότητές αυτής άλλα και τις κοινωνικές της επιρροές. Αξίζει να σημειώσουμε πως τέτοιες επιρροές είναι δυνατό να προσδιορίζουν τον βαθμό ανάπτυξης των υπηρεσιών ηλεκτρονικής διακυβέρνησης στον ελληνικό Δημόσιο Τομέα και να καθορίσουν την αποδοχή των προτεινόμενων τεχνολογικών λύσεων από τους πολίτες.

Για το λόγο αυτό, στην παρούσα μελέτη εξετάζονται:

- Η έννοια της διαχείρισης ταυτότητας όπως αυτή τείνει να επικρατήσει στις πρακτικές του Δημοσίου Τομέα, δίνοντας ιδιαίτερη έμφαση στα οφέλη αυτής.

- Το σύνολο των πληροφοριακών συστημάτων που έχουν αναπτυχθεί στην Ελλάδα με στόχο την καταγραφή των διαδικασιών διαχείρισης ταυτότητας που περιλαμβάνουν. Παρουσιάζεται αναφορικά και η κατάσταση σε ορισμένες αναπτυγμένες τεχνολογικά χώρες στον τομέα αυτό.

- Οι υπάρχουσες τεχνολογίες διαχείρισης ταυτότητας Με την πάροδο του χρόνου νέες τεχνολογίες διαχείρισης ταυτότητας κάνουν την εμφάνισή τους προκειμένου να καλύψουν τις ανάγκες που ανακύπτουν από τη πάροδο του χρόνου στα πλαίσια της ηλεκτρονικής Διακυβέρνησης.

Η εξέταση των ανωτέρω θεμάτων θα οδηγήσει σε μια ολοκληρωμένη αποτίμηση της διαχείρισης ταυτότητας στις υπηρεσίες ηλεκτρονικής διακυβέρνησης.

2. Περί Διαχείρισης Ταυτότητας

2.1 Εισαγωγή

Η ταυτότητα ως έννοια έχει εκτενέστερα εξεταστεί στις κοινωνικές επιστήμες. Έρευνες έχουν αναλύσει τις διάφορες εκφάνσεις της στα πλαίσια μιας ευρύτερης διαδικασίας που εκτείνεται από την διαμόρφωση της ατομικής ταυτότητας του ατόμου μέχρι την ένταξη του στην κοινωνία και σε ευρύτερα μορφώματα όπως το κράτος.

Η διαδικασία προσδιορισμού της ατομικής ταυτότητας, οι πληροφορίες που συνδέονται με αυτήν και η χρήση τους στις διάφορες εκφάνσεις της κοινωνικής και επαγγελματικής ζωής του ατόμου έχουν διαμορφώσει ένα σύνολο αντιλήψεων και προσδοκιών για την ανθρώπινη συμπεριφορά, τόσο σε ατομικό όσο και σε συλλογικό επίπεδο.

Η ανάπτυξη του διαδικτύου επέτρεψε την σταδιακή μεταφορά πολλών ανθρώπινων δραστηριοτήτων (π.χ. αγοραπωλησίες, ενημέρωση, ψυχαγωγία) σε ένα νέο περιβάλλον.

Στην παρούσα ενότητα εξετάζουμε τις νέες διαστάσεις που έχει προσδώσει το ψηφιακό περιβάλλον στην έννοια της ταυτότητας.

2.2 Η Έννοια της Ταυτότητας

Η ταυτότητα κάθε ατόμου συνίσταται στην φυσική του παρουσία και στην πληροφοριακή του ταυτότητα (informational identity), που απαρτίζεται από το σύνολο των πληροφοριών που συλλέγονται από διάφορες κρατικές και μη υπηρεσίες (Stalder, 2000). Κυρίαρχη σημασία τόσο στο φυσικό αλλά κυρίως στο ψηφιακό περιβάλλον έχουν οι πληροφορίες που προσδιορίζουν μοναδικά το άτομο.

Η πληροφοριακή ταυτότητα αποτελείται από μια σειρά δεδομένων όπως όνομα, ηλικία, τόπος γέννησης, επάγγελμα. Κάποια από τα δεδομένα αυτά λειτουργούν ως *φορείς ταυτοποίησης* (identifier) καθώς προσδιορίζουν την ταυτότητα του ατόμου χωρίς την παροχή όλων των πληροφοριών που την απαρτίζουν (Pato, 2003).

Στοιχεία όπως ο Αριθμός Ταυτότητας, ο Αριθμός Φορολογικού Μητρώου ή και το Αριθμό Μητρώου Ασφάλισης θεωρούνται *φορείς αυθεντικοποίησης* (authenticators) καθώς επιτρέπουν την πιστοποίηση της ταυτότητας του ατόμου.

Κατ' αναλογία με το φυσικό κόσμο, κάθε άνθρωπος πρέπει να έχει το δικαίωμα παρόμοιας συμπεριφοράς και στο διαδίκτυο. Στα πλαίσια αυτά, η έννοια της "ψηφιακής ταυτότητας" ταυτίζεται με την προσπάθεια δημιουργίας, οργάνωσης, αυτοματοποίησης και ολοκλήρωσης όλων των χαρακτηριστικών της ανθρώπινης συμπεριφοράς στον ψηφιακό κόσμο και της σύνδεσης τους με υπάρχουσες φυσικές ταυτότητες

2.3 Η Έννοια της Διαχείρισης Ταυτότητας

Η ταυτότητα ενός ανθρώπου, αποτελείται από δεδομένα τα οποία προσδιορίζουν το άτομο, και κατά συνέπεια διαφορετικοί συνδυασμοί αυτών είναι σε θέση να το ταυτοποιήσουν μοναδικά. Δεδομένης της πληθώρας πληροφοριών που συνδέονται με την ταυτότητα ενός ατόμου και τον τρόπο που ορίζεται αυτή, ανάλογα με το πλαίσιο χρήσης, είναι απαραίτητη η δημιουργία ενός συστήματος που θα επιτρέπει την διαχείριση των πληροφοριών αυτών στον ψηφιακό χώρο (Buell & Sandhu, 2003).

Τα βασικά στοιχεία μιας ψηφιακής ταυτότητας είναι:

(1) στοιχεία αυθεντικοποίησης-ταυτοποίησης,

(2) δικαιώματα πρόσβασης (εξουσιοδοτήσεις) και

(3) προσωπικά δεδομένα [MTE-02].

(Με τον όρο, προσωπικά δεδομένα νοούνται οι οργανωμένες συλλογές πληροφοριών που αφορούν μια φυσική οντότητα και μπορούν να λάβουν τη μορφή περιγραμμάτων) [BER-00].

Ως ορισμός της Διαχείρισης Ταυτότητας αναφέρεται το σύνολο των διαδικασιών που επιτρέπουν την δημιουργία, διατήρηση και κατάργηση των πληροφοριών που ορίζουν μοναδικά κάθε χρήστη ενός συνόλου πληροφοριακών συστημάτων (Dyson, 2002).

Διαφορετικά, είναι η διαχείριση των διαφορετικών ταυτοτήτων για λογαριασμό ανθρώπων, συστημάτων και υπηρεσιών.

Αν και κατά την ανάπτυξη των πρώτων συστημάτων υπήρχαν διαφορετικές ερμηνείες για το ακριβές αντικείμενο της διαχείρισης ταυτότητας πλέον είναι σαφές, όπως φαίνεται και από τους ορισμούς στον πίνακα 1, ότι αφορά πρωτίστως στην διαχείριση των στοιχείων πιστοποίησης των χρηστών σε πληροφοριακά συστήματα.

Συγγραφέας	**Ορισμός**
Dyson (2002)	Τα συστήματα διαχείρισης ταυτότητας είναι μια σειρά από τεχνολογίες και δομές που έχουν ως στόχο την παγίωση της ταυτότητας ως μέσω αναγνώρισης των χρηστών συστημάτων μέσα και έξω από μια επιχείρηση, την διευκόλυνση στη διαχείρισή της και την παροχή διαδικασιών για την εξακρίβωσή της
Pato (2003)	Διαχείριση ταυτότητας είναι το σύνολο των διαδικασιών, εργαλείων και κοινωνικών συμβολαίων που προσδιορίζουν την δημιουργία, διατήρηση και κατάργηση της ψηφιακής ταυτότητας ατόμων για την ασφαλή πρόσβαση σ' ένα διευρυνόμενο σύνολο συστημάτων και εφαρμογών
Cpupedia	Διαχείριση ταυτότητας είναι ένα ολοκληρωμένο σύστημα από επιχειρηματικές διαδικασίες, πολιτικές και τεχνολογίες που βοηθούν τις επιχειρήσεις να διευκολύνουν και να ελέγχουν την πρόσβαση των χρηστών τους σε κρίσιμες online εφαρμογές και πόρους, ενώ παράλληλα προστατεύουν εμπιστευτικές προσωπικές και επιχειρησιακές πληροφορίες από μη εξουσιοδοτημένους χρήστες
DigitalWorld	Η διαχείριση ταυτότητας αναφέρεται στη χρήση τεχνολογιών με σκοπό τη διαχείριση πληροφορίας σχετικά με την ταυτοποίηση των χρηστών και τον έλεγχο πρόσβασης στους πόρους της επιχείρησης. Στόχος της διαχείρισης προσωπικών δεδομένων είναι η βελτίωση της παραγωγικότητας και της ασφάλειας παράλληλα με τη μείωση του κόστους διαχείρισης της ταυτοποίησης των χρηστών, των χαρακτηριστικών

Συγγραφέας	Ορισμός
	και των πιστοποιητικών τους
Wikipedia	Διαχείριση ταυτότητας είναι η διαχείριση του κύκλου ζωής της ταυτότητας οντοτήτων (ανθρώπων ή αντικειμένων) κατά τη διάρκεια του οποίου η ταυτότητα δημιουργείται με την καταχώρηση πληροφοριών, περιγράφεται από μία ή περισσότερες ιδιότητες και τελικά καταστρέφεται όταν δεν χρησιμεύει πλέον

Πίνακας 1: ***Ορισμοί Διαχείρισης Ταυτότητας***

Συμπερασματικά τα κύρια σημεία που εστιάζουν οι παραπάνω ορισμοί είναι: ο προσδιορισμός των επιχειρηματικών διαδικασιών που απαιτούν ταυτοποίηση των χρηστών, ο βαθμός ταυτοποίησης των χρηστών στο σύστημα δηλαδή στο πόσο ισχυρή είναι η ταυτότητα που δημιουργείται από το σύστημα, αν είναι ανθεκτική σε αντιγραφή ή κακή χρήση της, η διακριτική προσπέλαση των χρηστών σε διάφορες υπηρεσίες που προσφέρει το σύστημα, και η επιλογή εκείνων των εργαλείων που θα διαχειρίζονται αποτελεσματικά τις ταυτότητες των χρηστών και θα δημιουργούν ένα ασφαλές περιβάλλον χωρίς προβλήματα

2.4 Βασικά Ζητήματα στην Διαχείριση Ταυτότητας στο Πλαίσιο της Ηλεκτρονικής Διακυβέρνησης

Κάθε σύστημα διαχείρισης ταυτότητας στα πλαίσια της ηλεκτρονικής διακυβέρνησης οργανώνεται σε τρεις βασικές ενότητες. Η πρώτη αφορά στα τεχνικά ζητήματα που οφείλει να επιλύσει ώστε να θεωρηθεί επιτυχημένο. Η δεύτερη εστιάζει στα νομικά ζητήματα που ανακύπτουν και η τρίτη στον τρόπο που πρέπει να αναδιαρθρωθούν οι δημόσιες υπηρεσίες ώστε να μπορούν να διαχειριστούν αποτελεσματικά την ταυτοποίηση των δικαιούχων στο ψηφιακό περιβάλλον.

Από **τεχνολογική άποψη** τα βασικά ζητήματα είναι τα εξής:

- **Πληθώρα τεχνικών προτύπων και έλλειψη κοινά αποδεκτών τεχνολογικών λύσεων:** Η μέχρι τώρα εμπειρία σε συστήματα διαχείρισης ταυτότητας καταδεικνύει ως πρωτεύον ζήτημα την έλλειψη ομοιογένειας σε επίπεδο τεχνικών λύσεων. Η δημιουργία πληροφοριακών συστημάτων από

κάθε δημόσια υπηρεσία οδήγησε στην εμφάνιση πολλών λύσεων για το ίδιο πρόβλημα (Modinis, 2006).

Ομοίως και τα συστήματα διαχείρισης ταυτότητας χαρακτηρίζονται από ανομοιομορφία και διαφορετικές προσεγγίσεις μιας κοινής διαδικασίας. Πέραν των ιδιαιτεροτήτων κάθε οργανισμού που δικαιολογούν ένα βαθμό διαφορετικότητας στις υπάρχουσες λύσεις, η ανομοιογένεια οφείλεται κυρίως στον εμπειρικό χαρακτήρα των πρώτων συστημάτων και στην έλλειψη συντονισμένων δράσεων κατά τα πρώτα στάδια υλοποίησης λύσεων ηλεκτρονικής διακυβέρνησης. Το αποτέλεσμα είναι η συμβίωση συστημάτων που δυσχεραίνουν την καθολική εφαρμογή μιας κοινής λύσης. Παράλληλα, η ενσωμάτωση τους στις πρακτικές της κάθε υπηρεσίας καθιστούν δύσκολη την αντικατάστασή τους προς όφελος κοινών λύσεων.

- **Προσωρινός χαρακτήρας τεχνικών λύσεων:** Ένας περιορισμός των περισσοτέρων λύσεων διαχείρισης ταυτότητας, με βάση τα ανωτέρω, είναι ότι πληροφοριακά συστήματα που λειτουργούν αποτελεσματικά και τυγχάνουν ευρείας αποδοχής από τους χρήστες τους, δεν είναι δυνατόν να υποστούν σημαντικές μεταβολές προκειμένου να προσαρμοστούν σε λύσεις διαχείρισης ταυτότητας.

  Υπάρχουν δύο βασικές παράμετροι που πρέπει να λαμβάνονται υπόψη κατά τον σχεδιασμό και την υλοποίηση συστημάτων διαχείρισης ταυτότητας. Πρώτον, ότι το εύρος των επενδύσεων και η σημαντική οργανωσιακή προσπάθεια που απαιτείται για την υλοποίηση συστημάτων ηλεκτρονικής διακυβέρνησης αποτρέπει άμεσες και ριζικές αλλαγές στα υπάρχοντα συστήματα. Ακόμη θα πρέπει να προστεθεί το γεγονός ότι οι δημόσιες υπηρεσίες οφείλουν να παρέχουν τις υπηρεσίες τους αδιάλειπτα οπότε είναι αδύνατη η διακοπή λειτουργίας των συστημάτων για αναβαθμίσεις και ριζικές αλλαγές. Τέλος, το εύρος των συστημάτων του δημοσίου τομέα, που είναι σημαντικά μεγαλύτερο κάθε αντίστοιχου συστήματος στον ιδιωτικό, καθιστά ιδιαίτερα δύσκολη την μετάπτωση σε νέα συστήματα.

  Η δεύτερη παράμετρος που πρέπει να ληφθεί υπόψη είναι οι αλλαγές σε διεθνή πρότυπα, πρωτόκολλα επικοινωνίας και απαιτήσεις ασφάλειας που απαιτούν συχνές αναβαθμίσεις των συστημάτων προκειμένου να συμβαδίζουν με τις συνεχώς μεταβαλλόμενες απαιτήσεις. Ο δημόσιος τομέας δεν αποτελεί εξαίρεση σε αυτή την κατάσταση

- **Διαχείριση αδειών προσπέλασης:** Κάθε υπηρεσία ηλεκτρονικής διακυβέρνησης βασίζεται σε συστήματα διαχείρισης ταυτότητας προκειμένου να διαχειριστεί πληροφορίες σχετικά με τις παρεχόμενες άδειες προσπέλασης. Συχνά αφορούν όλους τους δικαιούχους των υπηρεσιών που μπορεί να είναι και εκατομμύρια στην περίπτωση πολιτών και επιχειρήσεων.

  Η ηλεκτρονική διακυβέρνηση ως πεδίο εφαρμογής συστημάτων διαχείρισης ταυτότητας είναι ιδιαίτερα απαιτητική καθώς ο όγκος της πληροφορίας είναι δύσκολο να διαχειριστεί ενώ η ανοχή στα λάθη είναι εξαιρετικά περιορισμένη. Λάθη στα συστήματα του δημοσίου τομέα δύσκολα γίνονται ανεχτά, σε σχέση με αντίστοιχες καταστάσεις του ιδιωτικού τομέα, καθώς η πληροφορίες που τηρούνται από τις δημόσιες υπηρεσίες θεωρούνται επίσημες και ως εκ τούτου εξ ορισμού ορθές. Η αποκατάσταση λαθών και ζημιών από κακόβουλη χρήση πληροφοριών είναι χρονοβόρα και προκαλεί αναξιοπιστία των δημοσίων υπηρεσιών.

- **Ελεύθερη επιλογή μεθόδων αυθεντικοποίησης:** Η δημιουργία των πρώτων συστημάτων ηλεκτρονικής διακυβέρνησης οδήγησε στην επικράτηση διαφορετικών τρόπων αυθεντικοποίησης. Αν και με αυτό τον τρόπο δημιουργούνται επιπλέον απαιτήσεις σε κάθε σύστημα διαχείρισης ταυτότητας είναι σαφές ότι η χρήση διαφορετικών τρόπων αυθεντικοποίησης ανταποκρίνεται ορθότερα στην πραγματικότητα και στις διαφορετικές ανάγκες της κάθε δημόσιας υπηρεσίας. Επιπλέον, εξατομικεύεται η σημασία κάθε υπηρεσίας με την χρήση μεθόδου αυθεντικοποίησης που θα αντιστοιχεί στο επίπεδο ασφάλειας που κρίνεται απαραίτητο. Βέβαια, η επικράτηση διαφορετικών μεθόδων αυθεντικοποίησης αυξάνει την πολυπλοκότητα μιας καθολικής λύσης διαχείρισης ταυτότητας. Εντούτοις ελαχιστοποιεί τις αλλαγές στα υπάρχοντα συστήματα και επιτρέπει την αυτόνομη και αποκεντρωμένη επιλογή λύσεων από κάθε δημόσια υπηρεσία ανάλογα με τις υπηρεσίες που προσφέρει.

Από **νομική άποψη** τα βασικά ζητήματα είναι τα εξής:

- **Χρήση μοναδικών φορέων ταυτοποίησης:** Από αυστηρά νομική άποψη είναι σαφές ότι η χρήση μοναδικών φορέων ταυτοποίησης διευκολύνει σημαντικά τον σχεδιασμό και την υλοποίηση συστημάτων διαχείρισης ταυτότητας. Η ταυτοποίηση οντοτήτων με μοναδικό τρόπο απλοποιεί σημαντικά διαδικασίες σε διάφορα στάδια ενώ επιτρέπει και την ανταλλαγή δεδομένων με εξαιρετικά αποτελεσματικό τρόπο. Εντούτοις, η χρήση μοναδικών διακριτικών δημιουργεί συχνά ανησυχίες για κακόβουλη χρήση

των πληροφοριών που συνδέονται με αυτά. Οι δημόσιες υπηρεσίες θα είναι πλέον σε θέση να συλλέγουν πληροφορίες για τους δικαιούχους που δεν θα σχετίζονται απαραίτητα με τις παρεχόμενες υπηρεσίες. Επιπλέον θα μπορούν να συγκεντρώνουν λεπτομερή στοιχεία και να συνθέτουν πλήρη εικόνα του κάθε ατόμου χωρίς να ζητούν την συγκατάθεσή του. Για το λόγο αυτό σε πολλές περιπτώσεις δεν επιτρέπεται η χρήση μοναδικών φορέων ταυτοποίησης προκειμένου να προστατευτεί η ιδιωτικότητα του ατόμου έστω και αν έτσι δυσχεραίνεται η τεχνολογική υποστήριξη των διοικητικών διαδικασιών.

- **Αναντιστοιχία τεχνολογικών δυνατοτήτων και νομικών-ρυθμιστικών πλαισίων:** Η υλοποίηση μιας διοικητικής λειτουργίας είναι ως επί το πλείστον ένα αρκετά απλό ζήτημα από τεχνολογική άποψη. Η κατάσταση περιπλέκεται σημαντικά από τις νομικές διασφαλίσεις και τις θεσμοθετημένες πρακτικές που προσθέτουν επιπλέον βήματα στην κάθε διαδικασία και απαιτούν σχεδιαστικά πιο σύνθετες λύσεις από τα πληροφοριακά συστήματα.

  Για παράδειγμα, η εξουσιοδότηση ενός ατόμου να κάνει διοικητικές πράξεις για τρίτο, τεχνολογικά θα μπορούσε να λυθεί και με την απλή εκχώρηση του φορέα ταυτοποίησης του δικαιούχου. Η πράξη όμως για να είναι νομικά έγκυρη θα πρέπει να συνοδεύεται από έγγραφο που να πιστοποιεί την εξουσιοδότηση. Αν αυτό μεταφερθεί στην τεχνολογική λύση σημαίνει ότι το σύστημα θα πρέπει με κάποιο τρόπο να επιτρέπει εξουσιοδοτήσεις και να αναγνωρίζει επίσης το εύρος δικαιοδοσίας του κάθε εξουσιοδοτηθέντος ατόμου ώστε να κατοχυρώνονται νομικά όλα τα ενδιαφερόμενα μέρη.

- **Προστασία της ιδιωτικότητας:** Είναι σαφές ότι πρόκειται για ένα από τα πιο φλέγοντα ζητήματα στην διαχείριση ταυτότητας. Η βασική δυσκολία σχεδιασμού και υλοποίησης συστημάτων διαχείρισης ταυτότητας έγκειται ακριβώς στην προσπάθεια δημιουργίας αποτελεσματικών, από διοικητική άποψη, συστημάτων που παράλληλα θα διασφαλίζουν την ιδιωτικότητα των δικαιούχων. Η σημασία που αποδίδεται στην ιδιωτικότητα εστιάζει κυρίως στην διασφάλιση της εμπιστοσύνης που παραδοσιακά υπάρχει μεταξύ των δημοσίων υπηρεσιών και πολιτών/επιχειρήσεων.

Από **οργανωσιακή άποψη** τα βασικά ζητήματα είναι τα εξής:

- **Πληθώρα ψηφιακών ταυτοτήτων:** Ο αυξανόμενος όγκος των υπηρεσιών που προσφέρονται ηλεκτρονικά οδηγεί τους πολίτες στη απόκτηση πολλαπλών ψηφιακών ταυτοτήτων. Η κατάσταση αυτή οφείλεται αφενός

στον τρόπο υλοποίησης των πρώτων συστημάτων και στις πρακτικές που αυτά επέβαλαν στον τρόπο αυθεντικοποίησης των δικαιούχων και αφετέρου στην ανάγκη διασφάλισης της ιδιωτικότητας.

- **Αποτελεσματική διαχείριση εξουσιοδοτήσεων και πιστοποιητικών:** Ένα σημαντικό ζήτημα που απασχολεί και τη νομική διάσταση των συστημάτων διαχείρισης ταυτότητας είναι η διαχείριση των εξουσιοδοτήσεων και των πιστοποιητικών που εκχωρούνται στους δικαιούχους από τις δημόσιες υπηρεσίες για την πραγματοποίηση συναλλαγών. Δύσκολη παρουσιάζεται να είναι η εγκαθίδρυση εκείνων των διοικητικών διαδικασιών που θα διασφαλίζουν την ορθή τήρηση τους, την διασφάλιση των δεδομένων που συνδέονται με αυτά καθώς και την αποτελεσματική ανάκληση τους σε περίπτωση που κάποιος δικαιούχος εκπίπτει του δικαιώματος χρήσης τους. Επομένως, απαιτείται οι δημόσιες υπηρεσίες να έχουν σημαντική εμπειρία και εξοικείωση με τις νέες τεχνολογίες, διότι οφείλουν να καθιερώσουν εκείνες τις ενέργειες που απαιτούνται ώστε να διαχειριστούν αποτελεσματικά τις εξουσιοδοτήσεις και τα πιστοποιητικά των δικαιούχων. Απώτερος σκοπός είναι φυσικά η διαμόρφωση ενός ασφαλούς και αποτελεσματικού ψηφιακού περιβάλλοντος που θα δημιουργήσει συνθήκες εμπιστοσύνης οι οποίες τελικά θα προάγουν την υιοθέτηση των νέων υπηρεσιών ηλεκτρονικής διακυβέρνησης.

- **Κοινωνικές αντιλήψεις αναφορικά με τις παρεχόμενες λύσεις:** Βασικός παράγοντας αποδοχής των συστημάτων διαχείρισης ταυτότητας είναι οι αντιλήψεις που διαμορφώνει η κοινωνία αναφορικά με τις παρεχόμενες υπηρεσίες και το κόστος που συνεπάγεται η πιθανή εκχώρηση επιπλέον ελευθεριών στον κρατικό μηχανισμό. Σε πολλές χώρες, τα συστήματα διαχείρισης ταυτότητας δεν παρουσιάστηκαν στα πλαίσια ολοκληρωμένων προτάσεων για την διευκόλυνση των συναλλαγών των πολιτών με το δημόσιο. Η ορθή παρουσίαση αντίστοιχων συστημάτων, ώστε να ενισχυθεί η υιοθέτηση τους, θα ήταν στα πλαίσια οργανωμένων προσπαθειών αναβάθμισης της εμπειρίας των πολιτών/επιχειρήσεων στις συναλλαγές τους με το δημόσιο. Αντίθετα, τα συστήματα αυτά συχνά παρουσιάστηκαν αυτόνομα με αποτέλεσμα να θεωρηθούν από σημαντικό αριθμό χρηστών ως μια ακόμα προσπάθεια παρέμβασης του κράτους στην ιδιωτική ζωή των πολιτών.

Τα ζητήματα αυτά αποτελούν μια καταγραφή των θεμάτων που επηρεάζουν τον σχεδιασμό και την υλοποίηση συστημάτων διαχείρισης ταυτότητας. Είναι

προβλεπόμενο, οι προσπάθειες δημιουργίας συστημάτων διαχείρισης ταυτότητας από τις δημόσιες υπηρεσίες να επηρεαστούν από τεχνολογικές, οργανωσιακές και κυρίως πολιτικές εξελίξεις διεθνώς προκειμένου να είναι σε θέση να υποστηρίξουν και προσπάθειες διακρατικής διαχείρισης ταυτότητας.

2.5 Οφέλη από την Διαχείριση Ταυτότητας

Όπως αναφέρθηκε αναλυτικότερα παραπάνω η ταυτότητα ενός ατόμου όχι μόνο αποδεικνύει ότι είναι ποιο άτομο αναφέρει ότι είναι, αλλά προσδιορίζει επίσης τι μπορεί να κάνει και σε ποιους πόρους μπορεί να έχει πρόσβαση. Κυβερνήσεις και διοικητικοί τομείς είναι συχνά η πηγή εγγράφων που αφορούν την ταυτότητά κάποιου όπως πιστοποιητικά γέννησης, άδειες οδήγησης, φορολογικά μητρώα, πιστοποιητικά θανάτου και γάμων, και άλλα. Τα παραπάνω έγγραφα παρουσιάζονται σήμερα συχνά σε ηλεκτρονική μορφή.

Η διαχείριση της ταυτότητας σημαίνει τον έλεγχο των πληροφοριών σχετικά με τα αντίστοιχα στοιχεία της ταυτότητας του. Στο δημόσιο τομέα οι πληροφορίες αυτές είναι συνήθως επεξεργαζόμενες από διαφορετικούς μηχανισμούς αποφέροντας κάποια πλεονεκτήματα και τα οποία θα εξετάσουμε παρακάτω.

Σε έναν κυβερνητικό οργανισμό, ένα κατάλληλο σύστημα διαχείρισης ταυτότητας πρέπει να φέρει σημαντική οικονομία κόστους, λειτουργικές ικανότητες και αυξημένη ασφάλεια. Αυτά τα αποτελέσματα επιτυγχάνονται με:

- τη επιλογή ενός αποτελεσματικού προσωπικού,
- υποστήριξη από μια ποικιλία τεχνολογικών παρόχων, και
- τη χρήση αποτελεσματικών εφαρμογών με σίγουρο και ευέλικτο τρόπο.

Σημαντική προϋπόθεση είναι οι ταυτότητες του προσωπικού, στους οργανισμούς αυτούς, να μπορούν να ελεγχθούν εσωτερικά και να μπορούν να εισάγονται offline και online γρήγορα. Επιπρόσθετα, η ανάπτυξη μιας ενιαίας υποδομής περιορίζει την ευπάθεια του οργανισμού σε επιθέσεις ασφάλειας από τρέχοντες ή προηγούμενους υπαλλήλους και αναδόχους.

Αξίζει να εξετάσουμε τα πλεονεκτήματα αυτά στην «επικοινωνία» μεταξύ ποικίλων και αλληλένδετων οργανισμών. Παρακάτω συζητάμε συντόμως διαφορετικές περιπτώσεις.

2.5.1 Δημόσιο προς Δημόσιο

Πολλών ειδών πληροφορίες μπορούν να μοιραστούν μεταξύ κυβέρνησης και οργανωτικών θεσμών. Η διαλειτουργικότητα είναι απαραίτητη προϋπόθεση μεταξύ υπηρεσιών, οργανισμών ακόμα και μεταξύ εθνών. Πράγματι, η δυναμικά μεταβαλλόμενη φύση των εθνικών συνασπισμών επιβάλλει τους δυναμικούς Κύκλους Εμπιστοσύνης. Μία ορθή δομή επιτρέπει στα συστήματα να επικοινωνούν ενώ ταυτόχρονα να διατηρούν την αυτοδυναμία τους. Ο Κύκλος Εμπιστοσύνης παρέχει στους συνεργαζόμενους οργανισμούς το πλαίσιο ώστε να εξασφαλιστεί ότι αυτή η επικοινωνία είναι εγγυημένη.

Η ακαταμάχητη ανάγκη για ανταλλαγή ευαίσθητων πληροφοριών, μπορεί να ιδωθεί σε περιόδους καταστροφής. Ένα γεγονός, όπως ένας σεισμός ή μια κατολίσθηση, συμφιλιώνει και φέρνει κοντά αναρίθμητους οργανισμούς που πρέπει να μοιράσουν πληροφορίες μεταξύ υπηρεσιών και κυβερνήσεων, και συχνά γεφυρώνουν πολλαπλές χώρες. Όταν πληροφορίες σχετικά με άτομα, αντικατοπτριστούν σε πράξεις, είναι σημαντικό να διασφαλιστεί ότι τα άτομα είναι δεόντως πιστοποιημένα πριν από την ανταλλαγή τέτοιων ευαίσθητων πληροφοριών.

Το μοίρασμα κυβερνητικών πληροφοριών είναι απαραίτητο όχι μόνο σε περιόδους κρίσης: στην πραγματικότητα καταλαμβάνει όλες τις πτυχές της εξουσίας. Για παράδειγμα η δραστηριότητα της Ευρωπαϊκής Επιτροπής eEurope καλύπτει ένα εύρος πρωτοβουλιών που περιλαμβάνουν την ηλεκτρονική διακυβέρνηση (e-government), την ηλεκτρονική υγεία (e-health), την ηλεκτρονική μάθηση (e-learning) και την ηλεκτρονική επιχειρηματικότητα (e-business), όλα σχεδιασμένα να προάγουν την ανάπτυξη νέων και καλύτερων υπηρεσιών.

Παραδείγματα περιλαμβάνουν πρωτοβουλίες που σχετίζονται με τον τομέα της υγείας στην Ισπανία και την Φιλανδία, τη διοίκηση σχέσεων μεταξύ των διευθύνσεων και των εταιρειών στο Βέλγιο, την καταχώρηση δημοσίων φακέλων στην Ιταλία, την ηλεκτρονική ψήφο (e-voting) σε μερικά τοπικά συμβούλια στην Γαλλία, και ακόμα περισσότερα. Σε καθένα η ανάγκη για ανταλλαγή πληροφοριών απαιτεί ένα πλαίσιο μιας ομοσπονδιακής ταυτότητας διοίκησης για να επιτραπεί η ρέουσα κίνηση πληροφοριών και να διαφυλαχθεί η ασφάλεια και η ιδιωτική ζωή.

2.5.2 Δημόσιο προς Πολίτη

Πιθανόν σε κανένα άλλο τομέα της επικοινωνίας δεν είναι πιο σημαντική η ανάγκη για ασφαλή ανοικτή πρόσβαση όσο στην αλληλεπίδραση εξουσίας - πολίτη. Οι κυβερνήσεις ανά τον κόσμο ξεκινούν πρωτοβουλίες ηλεκτρονικής διακυβέρνησης (e-government) και ηλεκτρονικής πιστοποίησης (e-authentication), εκτεταμένη πρόσβαση και προγράμματα ηλεκτρονικής επικοινωνίας προκειμένου να φέρουν τα πλεονεκτήματα της τεχνολογίας στους πολίτες.

Στο δημόσιο τομέα, ποικίλα τμήματα και υπηρεσίες παρέχουν σε ιδιώτες και επιχειρήσεις πρόσβαση σε online υπηρεσίες μέσω πρωτοβουλιών της e-authentication. Για να αποφευχθεί οποιαδήποτε γενικευμένη διασύνδεση δημοσίων φακέλων που περιέχουν προσωπικές πληροφορίες, ο ιδανικός τρόπος προσέγγισης του θέματος πρέπει να διασφαλίζει ότι τα στοιχεία δεν ανατυπώνονται σε μια μοναδική κεντρική βάση δεδομένων.

Οι μεμονωμένες κυβερνητικές αρχές μπορούν να δρουν σαν παροχείς στους πολίτες εγκαθιστώντας Κύκλους Εμπιστοσύνης και προσφέροντας ένα εύρος ολοκληρωμένων εξατομικευμένων εφαρμογών μεταξύ διαφορετικών κυβερνητικών υπηρεσιών και τομέων. Παραδείγματα είναι: η ηλεκτρονική κατάθεση φορολογικής δήλωσης, η αποζημίωση για ιατρικά έξοδα, η ταξινόμηση αυτοκινήτου, το ηλεκτρονικό διαβατήριο και οι ανανεώσεις οδηγών. Επίσης, με ισχυρή εύχρηστη επικύρωση, οι κυβερνήσεις μπορούν να διασφαλίσουν ότι τα πλεονεκτήματα προορίζονται προς τους εξουσιοδοτημένους αποδέκτες. Ένα τέτοιο σχέδιο μπορεί γρήγορα να οδηγήσει τη μείωση του κόστους και την αυξημένη ασφάλεια.

Παράλληλα οι πολίτες παρουσιάζουν μια συνεχώς αυξανόμενη απαίτηση για όλο και πιο εξελιγμένες υπηρεσίες. Οι ίδιοι είναι συνηθισμένοι σε γρήγορες χρονικές αποκρίσεις και σε υψηλότερη ποιότητα προϊόντων και υπηρεσιών από τον ιδιωτικό τομέα. Αναμένουν λοιπόν την ίδια επίδοση από τις δημόσιες αρχές. Δυσνόητες διαδικασίες, μεγάλες ουρές, το να πρέπει να ξαναεισαχθεί κάποια πληροφορία που έχει ήδη παρθεί από τη διοίκηση, και προσεγγίσεις του τύπου «ένα είδος ταιριάζει σε όλα» είναι πρακτικές που όλο και περισσότερο κριτικάρονται.

Τελικά οι πολίτες περιμένουν οι αρχές να γίνουν υπόλογοι για τη διαχείριση των χρημάτων που πληρώνουν μέσω των φόρων. Επίσης απαιτούν περισσότερη διαφάνεια στη λήψη αποφάσεων και δημοκρατική ανάμιξη σε όλες τις φάσεις της ανάπτυξης της πολιτικής στρατηγικής.

Το Σχέδιο Δράσης eEurope 2005 ενσωματώνει τέτοιες πρωτοβουλίες στοχεύοντας στον εκσυγχρονισμό των δημόσιων υπηρεσιών και δίνοντας στον καθένα την δυνατότητα να συμμετέχει στην παγκόσμια κοινωνία της πληροφορίας. Ένας τομέας ενδιαφέροντος είναι η υγεία. Τα τελευταία χρόνια έχει γίνει μεγάλη πρόοδος για να χτιστούν ενιαία περιφερειακά δίκτυα επικοινωνίας για την υγεία, τυποποιημένες ηλεκτρονικές εγγραφές που αφορούν στον τομέα της υγείας και άλλα παρόμοια. Νέες πρωτοβουλίες θα ενεργοποιήσουν ραγδαία αντίδραση εναντίον απειλών για την υγεία, ενώ θα προστατευτεί η πληροφορία από μη εξουσιοδοτημένη πρόσβαση.

2.5.3 Δημόσιο προς Επιχείρηση

Οι επιχειρήσεις περιμένουν μεγαλύτερη ηλεκτρονική αλληλεπίδραση με την κυβέρνηση. Αυτό είναι αλήθεια για τις μικρού και μεσαίου μεγέθους επιχειρήσεις: έχοντας περιορισμένες πηγές για να συνεργαστούν με της κυβερνητικές υπηρεσίες. Είναι έτσι πρόθυμες να βρουν βολικές διαδικασίες για τις δραστηριότητες τους όπως είναι οι δηλώσεις του ΦΠΑ ή οι καταχωρήσεις εταιρειών. Είναι απαραίτητη μία ενωμένη αρχιτεκτονική η όποια θα εξασφαλίζει μια ασφαλή αλληλεπίδραση με ξεχωριστές λειτουργίες ή υπηρεσίες, ενώ θα αφήνει σε κάθε χρήστη τον έλεγχο των στοιχείων του.

Η ηλεκτρονική πιστοποίηση (e-Authentication) ελαχιστοποιεί το βάρος στις επιχειρήσεις, τους ιδιώτες και την κυβέρνηση όταν αποκτούν on-line υπηρεσίες με το να τους παρέχουν μία ασφαλή υποδομή για on-line συναλλαγές, μειώνοντας την ανάγκη για ξεχωριστές διαδικασίες εξακρίβωσης της ταυτότητας και των ηλεκτρονικών υπογραφών.

Όταν η επιχείρηση συνεργάζεται με την κυβέρνηση, οι αντικρουόμενες απαιτήσεις της ιδιωτικότητας και της διαλειτουργικότητας πρέπει να κρατηθούν σε μια λεπτή ισορροπία. Ένα ενδιαφέρον παράδειγμα μπορεί να ιδωθεί σήμερα στο Ιαπωνικό EduMart, μέρος του προγράμματος e-Japan Policy Priority και καθοδηγούμενο από τα Στρατηγικά Επιτελεία για την Προώθηση της Ανεπτυγμένου Δικτύου της Κοινωνίας Πληροφορίας και Τηλεπικοινωνιών (IT Strategic Headquarters). Σε μια προσπάθεια να δώσουν πλούσιο εκπαιδευτικό υλικό σε μαθητές σε περισσότερα από 40.000 σχολεία, οι Strategic Headquarters ίδρυσαν μία ανοικτή διεπιφάνεια (interface) και έχτισαν ένα δίκτυο διανομής εκπαιδευτικού περιεχομένου το οποίο θα οδηγήσει σε ένα σύστημα στο οποίο τόσο τα δημόσια ιδρύματα όσο και οι ιδιωτικές επιχειρήσεις μπορούν να συνδέονται και να συμμετάσχουν ελεύθερα.

Εκ φύσεως, το αίτημα για ασφαλή ιδιωτικοποίηση έπρεπε να ισορροπήσει με την ανάγκη να υπάρχει ευθύτητα. Καθώς οι χρήστες είναι μαθητές, προσωπικές πληροφορίες τους, το ιστορικό τους, πρέπει να προστατεύονται. Ωστόσο ένα συγκεκριμένο επίπεδο προσωπικών πληροφοριών πρέπει να μοιράζονται έτσι ώστε να εξάγονται σχετικά, επιδιωκόμενα στοιχεία. Το EduMart είναι ικανό να εξασφαλίσει διαλειτουργικότητα και ευθύτητα για το αποτέλεσμα, της προσωπικές πληροφορίες και τη διαχείριση των πνευματικών δικαιωμάτων. Όλα τα παραπάνω είχαν σαν αποτέλεσμα να αξιολογηθεί ως το πρώτο παγκόσμιας εμβέλειας σύστημα ηλεκτρονικής μάθησης (e-learning) βασισμένο στις προδιαγραφές του Liberty Alliance.

Επιπρόσθετα παραδείγματα μπορούν να ιδωθούν από τα κυβερνητικώς ελεγχόμενα προγράμματα για την υγεία που πρέπει να επικοινωνούν με της προμηθευτές και της ασθενείς, μέχρι της κυβερνητικές συμφωνίες με ξένους προμηθευτές, τη βασική χορήγηση αδειών για επιχειρήσεις και τη φορολογία. Η ταχύτητα, η εξάλειψη χρόνων, η ακρίβεια και το φιλικό περιβάλλον προς το χρήστη είναι τα προφανή αποτελέσματα τέτοιων πρωτοβουλιών.

3. Η Διαχείριση Ταυτότητας στην Ελλάδα

3.1 Εισαγωγή

Στην ενότητα αυτή εξετάζεται εκτενώς η κατάσταση στην Ελλάδα αναφορικά με τα θέματα διαχείρισης ταυτότητας στην ηλεκτρονική διακυβέρνηση. Συγκεκριμένα, εξετάζεται η ετοιμότητα της χώρας σε τεχνολογικό επίπεδο με την καταγραφή και παρουσίαση των υπηρεσιών ηλεκτρονικής διακυβέρνησης που προσφέρονται στους πολίτες και τις επιχειρήσεις της χώρας.

3.2 Τεχνολογική Υποδομή της Χώρας

Παρατηρώντας τα ζητήματα που αφορούν στη διαχείριση ταυτότητας σε κρατικό επίπεδο είναι προφανές ότι γίνονται προσπάθειες ακολουθώντας αυστηρή προτυποποίηση και ομοιογένεια αλλά και κατάλληλο διαμορφωμένο σχεδιασμό των πληροφοριακών συστημάτων της με βάση τις ανάγκες της.

Στα συστήματα αυτά πρωτεύοντα ρόλο έχουν οι πολίτες, οι επιχειρήσεις και επιλεγμένοι δημόσιοι φορείς που είναι και οι χρήστες αυτών των προγραμμάτων. Κύριος στόχος είναι η δημιουργία μιας κοινής βάσης που θα εξομαλύνει την συνεργασία μεταξύ συστημάτων συνδράμοντας στην ανάπτυξη υπηρεσιών οι οποίες, με τη σειρά τους, θα διευκολύνουν τον πολίτη στις συναλλαγές του με το Δημόσιο. Στην παρούσα ενότητα παρουσιάζονται οι δράσεις του κρατικού μηχανισμού για τον παραπάνω στόχο.

3.2.1 Το Πρόγραμμα Σύζευξις

Η βασική δράση της ελληνικής δημόσιας διοίκησης για την δημιουργία μιας κοινής βάσης επί της οποίας θα δομηθούν οι υπηρεσίες ηλεκτρονικής διακυβέρνησης έγκειται στο έργο «ΣΥΖΕΥΞΙΣ» που υλοποιείται από το Υπουργείο Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης.

Πρόκειται για τον σχεδιασμό και υλοποίηση μιας σύγχρονης επικοινωνιακής υποδομής που προϋποθέτει, και ταυτόχρονα επιβάλει, μια ευρύτερη και διαφοροποιημένη λειτουργική στη Δημόσια Διοίκηση. Συντελεί έτσι στη συνεχή και αποτελεσματική ροή της πληροφορίας μεταξύ των Δημοσίων Υπηρεσιών.

Η άρτια εξυπηρέτηση του πολίτη είναι γενικά ο κύριος άξονας του έργου. Ειδικότερα ορίζονται και οι επιμέρους στόχοι:

- μείωση του κόστους της επικοινωνίας (περίπου 50%) μεταξύ των φορέων του Δημοσίου με ταυτόχρονη αύξηση της ταχύτητας και ασφάλειας διακίνησης των πληροφοριών
- αποτελεσματική εκμετάλλευση των πληροφοριακών συστημάτων των φορέων του Δημοσίου μέσω της λειτουργικής διασύνδεσης των συστημάτων, και των εναλλακτικών πηγών πληροφοριών
- αποφυγή επικαλύψεων – επαναλήψεων σε βάσεις δεδομένων και δικτυακές εγκαταστάσεις
- δημιουργία προϋποθέσεων συμβατότητας στις δικτυακές εγκαταστάσεις των φορέων του Δημοσίου.
- βελτίωση της εξυπηρέτησης του πολίτη, ιδιαίτερα στις περιπτώσεις που απαιτούν εμπλοκή περισσοτέρων του ενός φορέων, με τελικό στόχο την παροχή onestop-shop υπηρεσιών ή «μίας στάσης» όπως θα μπορούσαμε να ονομάσουμε τη μορφή των υπηρεσιών αυτών.

Το έργο υποστηρίζει την Κεντρική και Περιφερειακή Διοίκηση, καθώς και την Νομαρχιακή και Τοπική Αυτοδιοίκηση, παρέχοντας προηγμένες τηλεματικής υπηρεσίες.

Αν και πρόκειται για μια τεχνολογική υποδομή η οποία παρέχει κυρίως υπηρεσίες τηλεφωνίας, δεδομένων και video στους συνδεδεμένους φορείς, είναι σαφές ότι ο κρατικός μηχανισμός αποβλέπει σε ευρύτερα οφέλη στην δημόσια διοίκηση. Μια από της άμεσες θετικές επιδράσεις του δικτύου αυτού είναι η εισαγωγή του Διαδικτύου στην Δημόσια Διοίκηση. Οι δημόσιοι υπάλληλοι αποδεχόμενοι της νέες προκλήσεις, εξοικειώνονται με ταχείς ρυθμούς με τα νέα τεχνολογικά δεδομένα ώστε αφενός να βελτιώσουν της συνθήκες εργασίας τους, και αφετέρου να παρέχουν καλύτερη ποιότητα υπηρεσιών στους πολίτες.

Παράλληλα, η παρεχόμενη τεχνολογική υποδομή επιτρέπει την δικτύωση μεταξύ των διαφόρων υπηρεσιών. Έτσι, εκτός των οικονομιών κλίμακας, δημιουργείται και μια νέα αντίληψη για τον τρόπο λειτουργίας και συνεργασίας μεταξύ των δημοσίων υπηρεσιών. Η χρήση της βασίζεται κυρίως στην ανταλλαγή πληροφοριών μεταξύ των δημοσίων υπαλλήλων και στην δημιουργία κλίματος εμπιστοσύνης και συνεργασίας στοχεύοντας και πάλι στην καλύτερη εξυπηρέτηση του πολίτη.

Το «ΣΥΖΕΥΞΙΣ» είναι ιδιαίτερα σημαντική προσπάθεια ειδικά για χώρες, όπως η Ελλάδα, που τώρα δημιουργούν της προϋποθέσεις εκείνες για την είσοδο τους στον ψηφιακό κόσμο. Ακολουθώντας έτσι τις διεθνείς τάσεις, η Δημόσια Διοίκηση προχωρεί και στην δημιουργία συγκεκριμένων οδηγιών για το πώς θα δομούνται στο εξής οι υπηρεσίες ηλεκτρονικής διακυβέρνησης.

3.2.2 Το Ελληνικό e-Gif και η Κυβερνητική Πύλη Ερμής

Η πληθώρα πληροφοριακών συστημάτων που αναπτύχθηκαν στα αρχικά στάδια της ηλεκτρονικής διακυβέρνησης, τόσο στην Ελλάδα όσο και στο εξωτερικό, σε συνδυασμό με την έλλειψη συντονισμού μεταξύ των αρμόδιων φορέων σημείωσαν ιδιαίτερες ελλείψεις που εμπόδισαν τη σωστή λειτουργία τους.

Πρόκειται ουσιαστικά για την αδυναμία μεταφοράς και χρήσης της πληροφορίας με ένα ομοιογενές και αποτελεσματικό τρόπο μεταξύ διαφόρων οργανισμών σε επίπεδο συστημάτων πληροφορικής. Αυτή η αδυναμία οδηγεί σε χρονοβόρες διαδικασίες ανταλλαγής πληροφοριών μεταξύ των δημοσίων υπηρεσιών ακυρώνοντας τα οφέλη της ηλεκτρονικής διακυβέρνησης. Η ανάπτυξη συστημάτων που δεν επικοινωνούν μεταξύ τους δεν εξαλείφει της γραφειοκρατικές διαδικασίες απλά της καθιστά δυσδιάκριτες στους πολίτες.

Η διεθνής πρακτική έχει παραθέσει δύο βασικούς τρόπους επίτευξης διαλειτουργικότητας μεταξύ των πληροφοριακών συστημάτων της Δημόσιας Διοίκησης. Ο πρώτος αφορά στην δημιουργία κεντρικών κυβερνητικών πυλών που θα παρέχουν συγκεντρωμένες τις απαραίτητες πληροφορίες στους δικαιούχους (πολίτες/επιχειρήσεις). Ο δεύτερος στην κατάρτιση Πλαισίων Διαλειτουργικότητας που θέτουν τεχνικά τις προδιαγραφές συνοχής των συστημάτων πληροφορικής του δημοσίου τομέα, ορίζοντας της βασικές προαπαιτήσεις για μία ολοκληρωμένη και ηλεκτρονική κυβέρνηση.

Η ελληνική δημόσια διοίκηση, αν και δεν αντιμετώπισε άμεσα το πρόβλημα αδυναμίας επικοινωνίας μεταξύ των πληροφοριακών της συστημάτων δεδομένου του περιορισμένου αριθμού αυτών σε χρήση, ακολουθώντας τη διεθνή εμπειρία προχωρά στην δημιουργία κεντρικής δικτυακής πύλης για την ηλεκτρονική διακυβέρνηση και καθιστά κατάλληλο πλαίσιο διαλειτουργικότητας.

Η Κυβερνητική Πύλη «Ερμής» παρέχει ολοκληρωμένη ενημέρωση στους πολίτες και στις επιχειρήσεις σχετικά με τις συναλλαγές τους με την Δημόσια Διοίκηση (φυσικές ή ηλεκτρονικές), καθώς επίσης και επιλεγμένες υπηρεσίες Ηλεκτρονικών

Συναλλαγών. Από επιχειρησιακής άποψης, το έργο κινείται σε τρεις βασικούς άξονες που αφορούν:

- Στην ολοκληρωμένη συλλογή και οργάνωση της απαιτούμενης πληροφορίας από το σύνολο της Δημόσιας Διοίκησης. Την διάθεσή αυτής στο Διαδίκτυο με σκοπό την αξιόπιστη ενημέρωση των πολιτών και των επιχειρήσεων όσον αφορά στις συναλλαγές τους και την αλληλεπίδρασή τους με τον κρατικό μηχανισμό.

- Στην ανάπτυξη των απαραίτητων υποδομών για την πλήρη υποστήριξη της Διαλειτουργικότητας μεταξύ των πληροφοριακών συστημάτων της Δημόσιας Διοίκησης και στην ανάπτυξη εφαρμογών για την παροχή υπηρεσιών Ηλεκτρονικών Συναλλαγών.

- Στην παροχή μηχανισμών πρόσβασης και Ψηφιακής Αυθεντικοποίησης των πολιτών και των επιχειρήσεων σε υπηρεσίες Ηλεκτρονικών Συναλλαγών της Δημόσιας Διοίκησης, λειτουργώντας σε ένα πλαίσιο ασφαλές από όλα τα επίπεδα.

Το Ελληνικό Πλαίσιο Διαλειτουργικότητας Ηλεκτρονικής Διακυβέρνησης (ΕΠΔΗΔ) παρέχει οδηγίες και καθορισμένες πολιτικές για:

- Τη μορφή πληροφοριών για ανταλλαγή (μορφή πληροφορίας και δεδομένων)
- Τον τρόπο ανταλλαγής πληροφοριών (επικοινωνία /πρωτόκολλα)
- Τον τρόπο πρόσβασης πληροφοριών (ασφάλεια / έλεγχος πρόσβασης)
- Τον τρόπο αναζήτησης πληροφοριών (υπηρεσίες καταλόγου)

Στόχος είναι να διασφαλιστεί η διαλειτουργικότητα μεταξύ όλων των Ελληνικών δημοσίων οργανισμών (Υπουργεία, Νομαρχίες, Δήμοι, Περιφέρειες), ιδιωτικών επιχειρήσεων, του πολίτη, καθώς και μεταξύ Ελλάδος και συστημάτων άλλων χωρών (EU, USA, Asia, κλπ.) η οποία θα καλύπτει όλους της τομείς της Οικονομίας.

3.3 Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης στην Ελλάδα

Στην ενότητα αυτή παρουσιάζονται συνοπτικά τα βασικότερα Ολοκληρωμένα Πληροφοριακά Συστήματα (ΟΠΣ) που βρίσκονται σε ισχύ στα πλαίσια της Δημόσιας Διοίκησης στην Ελλάδα. Πρόκειται για Πληροφοριακά Συστήματα που αλληλεπιδρούν δυναμικά με τους χρήστες τους (πολίτες, επιχειρήσεις, δημόσιοι φορείς) και είναι τα παρακάτω:

- Πληροφοριακό Σύστημα Ιδρύματος Κοινωνικής Ασφάλισης (ΙΚΑ & ΙΚΑnet)
- Πληροφοριακό Σύστημα Τελωνείων (ICIS & ICISnet)
- Πληροφοριακό Σύστημα Εφορίας (TAXIS & TAXISnet)
- Πληροφοριακό Σύστημα Κέντρων Εξυπηρέτησης Πολιτών (Κ.Ε.Π.)

3.3.1 Πληροφοριακό Σύστημα Ιδρύματος Κοινωνικής Ασφάλισης

Το Ίδρυμα Κοινωνικών Ασφαλίσεων, ο μεγαλύτερος ασφαλιστικός φορέας στην Ελλάδα, στο πλαίσιο του εκσυγχρονισμού της λειτουργίας του, υλοποίησε και χρησιμοποιεί ένα Ολοκληρωμένο Πληροφοριακό Σύστημα (Ο.Π.Σ.), με στόχο να καλύψει με ηλεκτρονικά αυτοματοποιημένο τρόπο το σύνολο των συναλλαγών και εργασιών των Μονάδων Ασφάλισής του. Πρόκειται για ένα ενιαίο και κεντροποιημένο σύστημα, που χρησιμοποιείται επιτυχώς και αποσκοπεί στη διεύρυνση των παρεχομένων υπηρεσιών ηλεκτρονικής διακυβέρνησης που προσφέρονται της πολίτες επί 24ώρου βάσης και 7ήμερης βάσης.

Το σύστημα παρέχει online πληροφόρηση σε ασφαλισμένους και εργοδότες, επιτρέπει ηλεκτρονικές συναλλαγές με το Ίδρυμα και παρέχει υπηρεσίες χορήγησης ασφαλιστικής ενημερότητας. Οι υπηρεσίες πληροφόρησης αφορούν σε οργανωτικά και λειτουργικά θέματα του ΙΚΑ, ενημερώσεις για Ασφάλιση, Παροχές, Συντάξεις, υποχρεώσεις εργοδοτών (π.χ. ημερομηνίες υποβολής Αναλυτικής Περιοδικής Δήλωσης.), ασφαλιστική ενημερότητα, ενημέρωση για συνεργαζόμενες τράπεζες για την καταβολή ασφαλιστικών εισφορών, παροχή εντύπων και πληροφοριακό υλικό για την Υγεία και το Ίδρυμα.

Το σύστημα επιτρέπει στους εργοδότες του να υποβάλουν ηλεκτρονικά την Αναλυτική Περιοδική Δήλωσής της (Α.Π.Δ.), εξυπηρετεί προμηθευτές του ΙΚΑ και λοιπούς φορείς του Δημοσίου. Επιπλέον διαθέτει μηχανισμό αυτόματου υπολογισμού του ποσού σύνταξης για τους ασφαλισμένους.

Με την υποβολή του Α.Π.Δ. καταχωρούνται στο σύστημα βασικά δεδομένα των εργοδοτών: Α.Φ.Μ., εισόδημα, εισπράξεις εταιρείας, ονοματεπώνυμα υπαλλήλων, μισθοί, εισφορές και επιδοτήσεις. Η ασφάλεια των ευαίσθητων αυτών πληροφοριών επιτυγχάνεται με την αυθεντικοποίηση τόσο των χρηστών της ιστοσελίδας του ΙΚΑ όσο και των υπαλλήλων του Ιδρύματος.

Δεδομένα Ο.Π.Σ.Ι.Κ.Α.	
ΑΦΜ	ΗΜΕΡΟΜΙΣΘΙΟ
ΕΙΣΟΔΗΜΑ	ΑΠΟΔΟΧΕΣ
ΕΙΣΠΡΑΞΕΙΣ ΕΤΑΙΡΕΙΑΣ	ΕΙΣΦΟΡΕΣ ΕΡΓΟΔΟΤΗ
ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΥΠΑΛΛΗΛΟΥ	ΕΙΣΦΟΡΕΣ ΕΡΓΑΖΟΜΕΝΟΥ
ΔΙΕΥΘΥΝΣΗ ΕΠΙΧΕΙΡΗΣΗΣ	ΕΠΙΔΟΤΗΣΕΙΣ
ΟΝΟΜΑ ΜΗΤΡΟΣ	ΟΝΟΜΑ ΠΑΤΡΟΣ

Πίνακας 2: **Δεδομένα Ο.Π.Σ.Ι.Κ.Α.**

3.3.2 Πληροφοριακό Σύστημα Τελωνείων

Το Ολοκληρωμένο Πληροφοριακό Σύστημα των Ελληνικών Τελωνείων (Ο.Π.Σ.Τ.) σχεδιάστηκε και λειτουργεί βάση του νομικού (Κοινοτικού και Εθνικού) πλαισίου για τα τελωνεία, με σκοπό:

- τη βελτίωση των υπηρεσιών με τους συναλλασσόμενους,
- την προστασία της δημόσιας υγείας,
- την ενημέρωση της Πολιτικής και Υπηρεσιακής Ηγεσίας με δεδομένα και
- την γενική εναρμόνιση και απλούστευση των εκτελούμενων τελωνειακών εργασιών.

Το σύστημα καλύπτει μηχανογραφικά τις τελωνειακές διατυπώσεις και διαδικασίες που εκτελούνται καθημερινά στα τελωνεία. Με τη χρήση του επιτυγχάνεται μείωση των λαθρεμποριών, των τελωνειακών παραβάσεων της δασμοφοροδιαφυγής, καθώς και του χρόνου αποδέσμευσης των εμπορευμάτων στην κατανάλωση,

εξαγωγή και εισαγωγή. Επιπλέον παρέχει στατιστικά στοιχεία για Εθνική χρήση και για την Ευρωπαϊκή Ένωση.

Το Ο.Π.Σ.Τ. αποτελείται από εννέα υποσυστήματα που διασυνδέονται αυτόματα μεταξύ τους:

1. *Υποσύστημα Διαχείρισης Εμπορευμάτων* (δηλωτικών). Με το υποσύστημα αυτό παρακολουθείται η διαχείριση των εμπορευμάτων που εισάγονται από το εξωτερικό και αποθηκεύονται σε δημόσιους ή ιδιωτικούς χώρους. Γίνεται μηχανογραφική τήρηση της λογιστικής παρακολούθησης της αποθήκης προσωρινής εναπόθεσης και διασύνδεση με άλλα υποσυστήματα του Ο.Π.Σ.Τ. για αυτόματη ενημέρωση του υποσυστήματος.

2. *Υποσύστημα Διαμετακόμισης* (TIR, ATA). Πραγματοποιείται μηχανογραφική κάλυψη της διακίνησης των εμπορευμάτων τρίτων χωρών μεταξύ δύο σημείων της χώρας. Μέσω του υποσυστήματος αυτού ανταλλάσσονται μηνύματα έγκαιρης προειδοποίησης από το τελωνείο αναχώρησης τους για το τελωνείο προορισμού για επικείμενη άφιξη συγκεκριμένης κίνησης εμπορευμάτων.

3. *Υποσύστημα Εισαγωγών – Εξαγωγών*. Καλύπτονται μηχανογραφικά οι τελωνειακές διατυπώσεις που τηρούνται στο τελωνείο, οι οποίες σχετίζονται με τα εισαγόμενα και εξαγόμενα εμπορεύματα από της τρίτες χώρες. Με το υποσύστημα αυτό συλλέγονται στοιχεία για της τελωνειακές εισπράξεις εσόδων και στατιστικά στοιχεία.

4. *Υποσύστημα Διαχείρισης Προϊόντων με Ειδικό Φόρο Κατανάλωσης*. Παρακολουθούνται οι τελωνειακές διαδικασίες για ενδοκοινοτική διακίνηση, αποθήκευση και θέση των προϊόντων που επιβαρύνονται με Ε.Φ.Κ. (πετρελαιοειδή προϊόντα, αλκοόλη, αλκοολούχα ποτά και βιομηχανοποιημένος καπνός). Επίσης παρακολουθούνται κοινοτικά οχήματα που μεταφέρονται, αποστέλλονται και τίθενται σε ανάλωση στο εσωτερικό της χώρας, καταβάλλοντας το ανάλογο τέλος ταξινόμησης.

5. *Υποσύστημα Διαχείρισης Ειδικών Πληροφοριών και Υποθέσεων*. Το υποσύστημα αυτό καλύπτει τη λειτουργία από την καταχώρηση των πληροφοριών μέχρι την τελεσιδικία των υποθέσεων για παραβάσεις. Επιπλέον, περιλαμβάνει την πληροφόρηση του χρήστη για το στάδιο στο οποίο βρίσκεται συγκεκριμένη υπόθεση και δίνει στοιχεία αποτελεσμάτων

ελέγχου στο υποσύστημα Ανάλυσης Κινδύνων για τη δημιουργία των κριτηρίων ελέγχου και επικινδυνότητας.

6. *Υποσύστημα Διαχείρισης Δασμολογίου και Νομοθεσίας* (TARIC). Γίνεται μηχανογραφική κάλυψη της πληροφορίας ανά κωδικό εμπορεύματος για της εισαγωγικούς δασμούς, της περιορισμούς εισαγωγής/εξαγωγής, τα μέτρα εμπορικής πολιτικής u960 που επιβάλλει η Ευρωπαϊκή Ένωση, καθώς και της απαγορεύσεις και της περιορισμούς. Περιλαμβάνει της βάση δεδομένων της εθνικής τελωνειακής νομοθεσίας.

7. *Υποσύστημα Διαχείρισης Φυσικών και Ανθρώπινων Πόρων*. Καλύπτει τη διαχείριση των στοιχείων που αφορούν στο προσωπικό των τελωνείων. Η τελωνειακή υπηρεσία διαχειρίζεται τους φυσικούς πόρους (μεταφορικά μέσα, υλικό, εξοπλισμό κ.λπ.). Ακόμη, το υποσύστημα διαχειρίζεται τις δαπάνες για την πραγματοποίηση των μετακινήσεων των υπαλλήλων εντός και εκτός χώρας και υπολογίζει αυτόματα τα ΔΕΤΕ (Δικαιώματα Εκτέλεσης Τελωνειακών Εργασιών) για την πληρωμή των υπαλλήλων.

8. *Υποσύστημα Διαχείρισης Αξιών εμπορευμάτων*. Το υποσύστημα αυτό δε λειτουργεί παραγωγικά σήμερα. Αν λειτουργήσει θα έχει τη δυνατότητα να ενημερώνεται σε κεντρικό επίπεδο για της ενδεικτικές τιμές επιλεγμένων (ευαίσθητων σε παράβαση) εμπορευμάτων, ώστε να μπορεί να επαληθεύει η υπηρεσία εάν η δηλούμενη στα παραστατικά αξία είναι αποδεκτή.

Υποσύστημα Λήψης Αποφάσεων και Ανάλυση Κινδύνων (DSS). Το υποσύστημα αυτό, μετά από εκτιμήσεις ορισμένων παραμέτρων που καθορίζουν την επικινδυνότητα των εμπορευμάτων που εισάγονται στη χώρα, αποδίδει το βαθμό και κατατάσσει το εμπόρευμα κατά περίπτωση σε μία από τις τρεις κατηγορίες επικινδυνότητας. Βάσει της κατάταξης τους, προγραμματίζεται στη συνέχεια και η μορφή του ελέγχου που θα διεξαχθεί σε αυτό.

Δεδομένα Ο.Π.Σ.Τ.	
ΑΦΜ ΥΠΟΧΡΕΟΥ ΚΑΤΑΘΕΣΗΣ	ΑΡΙΘΜΟΣ ΔΙΑΒΑΤΗΡΙΟΥ Ή ΤΑΥΤΟΤΗΤΑΣ ΥΠΟΧΡΕΟΥ ΔΗΛΩΣΗΣ
ΚΩΔΙΚΟΣ ΤΕΛΩΝΕΙΟΥ ΥΠΟΒΟΛΗΣ	ΕΙΣΦΟΡΕΣ ΕΡΓΟΔΟΤΗ
ΠΕΡΙΦΕΡΕΙΑ & ΑΡΙΘΜΟΣ ΠΤΥΧΙΟΥ ΤΕΛΩΝΙΣΤΗ	ΚΩΔΙΚΑΣ ΧΩΡΑΣ ΠΡΟΟΡΙΣΜΟΥ

Δεδομένα Ο.Π.Σ.Τ.	
ΑΦΜ ΑΝΤΙΠΡΟΣΩΠΟΥ	ΕΠΩΝΥΜΟ Ή ΕΠΩΝΥΜΙΑ ΤΟΥ ΑΠΟΣΤΟΛΕΑ/ΥΠΟΧΡΕΟΥ
ΤΥΠΟΣ ΜΗΝΥΜΑΤΟΣ	ΟΝΟΜΑ ΠΑΤΡΟΣ
ΠΑΤΡΩΝΥΜΟ ΥΠΟΧΡΕΟΥ ΔΗΛΩΣΗΣ	ΟΝΟΜΑ ΜΗΤΡΟΣ
ΗΜΕΡΟΜΗΝΙΑ ΓΕΝΝΗΣΗΣ	

Πίνακας 3: **Δεδομένα Ο.Π.Σ.Τ.**

3.3.3 Πληροφοριακό Σύστημα Εφορίας

Το πληροφοριακό σύστημα TAXIS αποτελεί τη μηχανογραφική απεικόνιση όλων των φορολογικών διαδικασιών του κράτους και λειτουργεί από το 1998. Είναι το μεγαλύτερο έργο πληροφορικής στην Ελλάδα. Υλοποιήθηκε από τη Γενική Γραμματεία Πληροφοριακών Συστημάτων (Γ.Γ.Π.Σ.) στα πλαίσια του Επιχειρησιακού Προγράμματος «Κλεισθένης» του Β' Κ.Π.Σ., ενώ η προσαρμογή των εφαρμογών στο ευρώ υλοποιήθηκε στα πλαίσια του Επιχειρησιακού Προγράμματος «Κοινωνία της Πληροφορίας» του Γ' Κ.Π.Σ.

Το σύστημα αυτό στοχεύει:

- στον εκσυγχρονισμό και τη βελτίωση της αποτελεσματικότητας των υπηρεσιών του Υπουργείου Οικονομίας και Οικονομικών,
- την πάταξη της φοροδιαφυγής και
- τη βέλτιστη εξυπηρέτηση των πολιτών.

Μετά την ανάπτυξη του Πληροφοριακού Συστήματος TAXIS και τη δημιουργία των αναγκαίων ηλεκτρονικών υποδομών (Βάσεις Δεδομένων), αναπτύχθηκαν εναλλακτικοί τρόποι εξυπηρέτησης των πολιτών μέσω ηλεκτρονικών συναλλαγών στο Internet (TAXISnet).

Το TAXIS είναι υλοποιημένο σε κεντρικό (Γ.Γ.Π.Σ.) και περιφερειακό επίπεδο (Δ.Ο.Υ.). Στις κεντρικές υποδομές της Γ.Γ.Π.Σ. φιλοξενείται η κεντρική βάση του TAXIS, ενώ κάθε Δ.Ο.Υ. διαθέτει δικό της εξυπηρετητή με περιφερειακή βάση δεδομένων, η οποία περιλαμβάνει τα δεδομένα αρμοδιότητάς της.

Το Ο.Π.Σ. των TAXIS υποστηρίζει τις λειτουργίες της Εφορίας και διατηρεί στοιχεία που σχετίζονται με τους φορολογούμενους και τους φόρους. Τα προσωπικά δεδομένα της φορολογούμενου αφορούν σε στοιχεία που δηλώνει ο ίδιος στο τμήμα μητρώου για να του αποδοθεί ο Α.Φ.Μ. Το TAXIS χρησιμοποιεί ως κύριο κλειδί τον Α.Φ.Μ. γιατί είναι μοναδικό, σε αντίθεση με τον αριθμό ταυτότητας που μπορεί να αλλάξει σε περίπτωση απώλειάς ή κλοπής της.

Δεδομένα Ο.Π.Σ.Ε.	
ΑΦΜ	ΥΠΗΚΟΟΤΗΤΑ
ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΦΟΡΟΛΟΓΟΥΜΕΝΟΥ	ΔΙΕΥΘΥΝΣΗ ΚΑΤΟΙΚΙΑΣ
ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΠΑΤΡΟΣ	ΔΙΕΥΘΥΝΣΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ
ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΜΗΤΡΟΣ	*ΣΤΟΙΧΕΙΑ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ ΕΠΙΧΕΙΡΗΣΗΣ*
ΗΜΕΡΟΜΗΝΙΑ ΓΕΝΝΗΣΗΣ	*ΕΙΔΟΣ ΛΟΓΙΣΤΙΚΩΝ ΒΙΒΛΙΩΝ*
ΑΡΙΘΜΟΣ ΤΕΚΝΩΝ	*ΔΙΕΥΘΥΝΣΗ ΕΠΙΧΕΙΡΗΣΗΣ*
ΑΡΙΘΜΟΣ ΤΑΥΤΟΤΗΤΑΣ	

Πίνακας 4: **Δεδομένα Ο.Π.Σ.Ε.**

3.3.4 Πληροφοριακό Σύστημα Κέντρων Εξυπηρέτησης Πελατών

Τα Κέντρα Εξυπηρέτησης Πολιτών (ΚΕΠ) δημιουργήθηκαν στο πλαίσιο των Επιχειρησιακών Προγραμμάτων «Κοινωνία της Πληροφορίας», «Πολιτεία» και «ΑΣΤΕΡΙΑΣ» και υπάγονται στην δράση του Υπουργείου Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης (ΥΠΕΣΔΔΑ).

Οι θεσμικές καινοτομίες που προάγουν τα ΚΕΠ βασίστηκαν στην ανάγκη για ποιοτική αναβάθμιση της εξυπηρέτησης πολιτών και επιχειρήσεων και για τη βελτίωση της παραγωγικότητας της δημόσιας διοίκησης και επιπρόσθετα για την τοπική και περιφερειακή ανάπτυξη του κράτους.

Πιο συγκεκριμένα αναβαθμίστηκε ο εξοπλισμός και η παραγωγική λειτουργία διαφόρων φορέων Τοπικής Αυτοδιοίκησης καθώς επίσης βελτιώθηκε η οργάνωση, και παρατηρήθηκε σημαντική ανανέωση και εμπλουτισμός της υπάρχουσας

δημόσιας πληροφορίας σε ψηφιακή μορφή, ώστε να επιτρέπεται η περαιτέρω ταξινόμησή της σε δικτυωμένες και υποστηριζόμενες βάσεις.

4. Συστήματα - Τεχνολογίες Διαχείρισης Ταυτότητας

4.1 Εισαγωγή

Με την πάροδο του χρόνου νέες τεχνολογίες διαχείρισης ταυτότητας κάνουν την εμφάνισή τους, στοχεύοντας στη μεγιστοποίηση της ασφάλειας και ταυτόχρονα στη διατήρηση της ανωνυμίας των χρηστών.

4.2 Βασικά Στοιχεία ενός Συστήματος Διαχείρισης Ταυτότητας

Τα συστήματα διαχείρισης ταυτότητας απαρτίζονται από μια σειρά υπηρεσιών και επιμέρους συστημάτων τα οποία έχουν ως στόχο τη διαχείριση αλλά ακόμα και κατάργησης των δεδομένων που συγκροτούν την ταυτότητα των χρηστών.

Ένα σύστημα διαχείρισης ταυτότητας διαρθρώνεται σε τρία επίπεδα. Κάθε ένα από αυτά αποσκοπεί στην ρύθμιση εκείνων των στοιχείων που σχετίζονται με τους κανόνες δημιουργίας και διαχείρισης των δεδομένων, και την πρόσβαση στο σύστημα των κατόχων αυτών. Τα επίπεδα αυτά είναι:

i. **Βάση** (foundation): πρόκειται για το επίπεδο που ρυθμίζει τους κανόνες πρόσβασης στα δεδομένα που τηρούνται στο σύστημα.

ii. **Κύκλος ζωής** (lifecycle): εδώ ρυθμίζονται όλα εκείνα στοιχεία που αφορούν στην έκδοση ηλεκτρονικών ταυτοτήτων καθώς και στην διαχείριση των δεδομένων που τις απαρτίζουν.

iii. **Πρόσβαση & χρήση** (consumable): στο επίπεδο αυτό ορίζεται ο τρόπος πρόσβασης στο σύστημα και προσπέλασης των δεδομένων.

Σε κάθε ένα από αυτά τα επίπεδα διάφορα τμήματα του συστήματος ταυτότητας αλληλεπιδρούν με στόχο την συλλογή και αποτελεσματική διαχείριση των δεδομένων που θα επιτρέψει την απρόσκοπτη χρήση των υπηρεσιών του από τον τελικό χρήστη.

Η βάση ενός συστήματος διαχείρισης ταυτότητας αποτελείται από τα εξής μέρη (Pato, 2003):

- *Πάροχος αυθεντικοποίησης* (authentication provider): είναι υπεύθυνος για την αρχική αυθεντικοποίηση ενός ατόμου που επιθυμεί να συνδεθεί με μια ταυτότητα. Ο πάροχος αυθεντικοποίησης παράγει έναν authenticator – ένα τεκμήριο που επιτρέπει στα άλλα τμήματα του συστήματος να γνωρίζουν ότι η αρχική αυθεντικοποίηση έχει πραγματοποιηθεί. Τεχνικές αρχικής αυθεντικοποίησης περιλαμβάνουν μηχανισμούς όπως η επαλήθευση συνθηματικών, επαλήθευση έξυπνων καρτών, σαρώσεις βιομετρικών δεδομένων κ.α. Κάθε ταυτότητα μπορεί να σχετίζεται με περισσότερους από έναν παρόχους αυθεντικοποίησης. Οι μηχανισμοί που χρησιμοποιούνται από τον κάθε πάροχο διαφέρουν ως προς την αποτελεσματικότητα και την ασφάλεια τους. Έτσι, ανάλογα με το πλαίσιο χρήσης ενός συστήματος διαχείρισης ταυτότητας είναι δυνατόν να απαιτούνται συγκεκριμένοι μηχανισμοί αυθεντικοποίησης.

- *Έλεγχος κανόνων* (policy control): Η πρόσβαση και χρήση των πληροφοριών που συνδέονται με την ταυτότητα ρυθμίζεται από μια σειρά κανόνων. Οι κανόνες αυτοί ορίζουν πώς διαχειρίζονται οι πληροφορίες που διατηρούνται στο σύστημα καθώς και υπό ποιες προϋποθέσεις είναι δυνατόν να εκχωρηθούν. Έλεγχοι αυτών των κανόνων μπορεί να προκαλέσουν τον έλεγχο συγκεκριμένων περιστατικών (events) του συστήματος. Επίσης είναι δυνατόν να ειδοποιηθεί ο κάτοχος της ταυτότητας σε περίπτωση προσπέλασης των δεδομένων του.

- *Έλεγχος* (auditing): Οι διαδικασίες ελέγχου αποτελούν ουσιαστικά ένα μηχανισμό για την καταγραφή της δημιουργίας, μεταβολής και χρήσης της πληροφορίας. Με τον τρόπο αυτό είναι δυνατός ο εντοπισμός περιπτώσεων παραβίασης των κανόνων του συστήματος.

Τα συστατικά του κύκλου ζωής είναι τα εξής:

- *Παροχή* (provisioning): πρόκειται για την αυτοματοποίηση όλων των διαδικασιών και των εργαλείων που επιτρέπουν τη διαχείριση του κύκλου ζωής μιας ταυτότητας. Τη δημιουργία του στοιχείου αναφοράς (identifier) για την ταυτότητα, τη διασύνδεση με τους παρόχους αυθεντικοποίησης, τον προσδιορισμό και τη μεταβολή των χαρακτηριστικών αλλά και των προνομίων, όπως και την κατάργηση της ταυτότητας. Σε συστήματα μεγάλης κλίμακας, αυτά τα εργαλεία επιτρέπουν στο χρήστη τη δημιουργία και τη διατήρησή της ταυτότητας του.

- *Διάρκεια* (longevity): τα εργαλεία αυτά επιτρέπουν την τήρηση αρχείου για την ταυτότητα, το οποίο περιλαμβάνει την μετεξέλιξη της ταυτότητας με την πάροδο του χρόνου.

Το επίπεδο πρόσβασης και χρήσης του συστήματος περιλαμβάνει τα ακόλουθα στοιχεία:

- *Εφ' άπαξ πρόσβαση* (single sign-on): με τον τρόπο αυτό η ταυτότητα του χρήστη πιστοποιείται μια φορά κατά την πρόσβαση του σε μια υπηρεσία του συστήματος ταυτότητας. Στην συνέχεια, μπορεί να έχει πρόσβαση σε όλες τις υπηρεσίες και τα συστήματα που έχουν διασυνδεθεί και απαρτίζουν το ευρύτερο περιβάλλον που διαχειρίζεται το σύστημα.

- *Εξατομίκευση* (personalization): τα εργαλεία αυτά επιτρέπουν πληροφορίες που αφορούν στις εφαρμογές που χρησιμοποιεί ο χρήστης καθώς και γενικές πληροφορίες διασύνδεσης σε μια συγκεκριμένη ταυτότητα. Παράλληλα παρέχουν στις επιχειρήσεις, που διαχειρίζονται το σύστημα, τη δυνατότητα να συγκεντρώνουν χρήσιμες πληροφορίες που μπορούν στη συνέχεια να χρησιμοποιήσουν για εμπορικούς σκοπούς.

- *Διακριτική προσπέλαση* (access management): τα στοιχεία αυτά του συστήματος επιτρέπουν πρόσβαση με βάση προνόμια και κανόνες που έχουν ήδη αποθηκευτεί.

4.3 Βασικά Στοιχεία Τεχνολογιών Υποστήριξης της Διαχείρισης Ταυτότητας

Στην παρούσα ενότητα γίνεται παρουσίαση των τεχνολογικών λύσεων που χρησιμοποιούνται στην πλειοψηφία των συστημάτων διαχείρισης ταυτότητας που υποστηρίζουν υπηρεσίες ηλεκτρονικής διακυβέρνησης. Οι τεχνολογίες που έχουν σχεδιαστεί για την παροχή ασφάλειας ακολουθούν κάποιους βασικούς κανονισμούς εφόσον καθίσταται αναγκαίο: να επιτυγχάνεται οικονομία δεδομένων, να συνεκτιμώνται οι διαφορετικές συγκρούσεις, τα συμφέροντα και οι απαιτήσεις των εμπλεκόμενων μελών της, όπως επίσης και να παραμένει εφικτή η αυτονομία αυτών.

4.3.1Υποδομή Δημόσιου Κλειδιού

Πρόκειται για την μέθοδο αυθεντικοποίησης που χρησιμοποιείται στο σύνολο των υπηρεσιών ηλεκτρονικής διακυβέρνησης. Η Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure - PKI) αποτελεί ένα συνδυασμό λογισμικού, τεχνολογιών κρυπτογραφίας και υπηρεσιών, ο οποίος πιστοποιεί την ταυτότητα κάθε φυσικού προσώπου που εμπλέκεται σε μια συναλλαγή στο Διαδίκτυο, και παράλληλα προστατεύει την ασφάλεια της συναλλαγής. Επιπρόσθετα, ενσωματώνει ψηφιακά πιστοποιητικά, κρυπτογραφία δημόσιου κλειδιού και αρχές πιστοποίησης σε ένα ασφαλές αρχιτεκτονικό σχήμα.

Στόχος είναι η διαμόρφωση εκείνων των προδιαγραφών που θα επιτρέπουν αφενός την πιστοποίηση των χρηστών και αφετέρου την ορθή απόδοση και διαχείριση πιστοποιητικών στους δικαιούχους. Μια τυπική υλοποίηση PKI περιλαμβάνει την παροχή ψηφιακών πιστοποιητικών σε χρήστες, εξυπηρετητές (servers) και λογισμικό χρηστών. Παράλληλα προσφέρει σειρά εργαλείων για τη διαχείριση, ανανέωση και ανάκληση των πιστοποιητικών.

Βασική του προϋπόθεση είναι η χρήση κρυπτογραφίας δημοσίου κλειδιού, που είναι και η πιο διαδεδομένη μέθοδος για την πιστοποίηση του αποστολέα ενός μηνύματος ή για την κρυπτογράφηση του. Διασφαλίζεται έτσι η εμπιστευτικότητα και η ακεραιότητα στο διαδίκτυο. Η αδυναμία της μεθόδου αυτής εμφανίζεται στο ότι αν το κλειδί αυτό αποκαλυφθεί είναι πλέον πολύ εύκολη η αποκρυπτογράφηση των μηνυμάτων, με αποτέλεσμα να απαιτείται εμπιστοσύνη μεταξύ των εμπλεκόμενων μελών.

Στην κρυπτογραφία δημοσίου κλειδιού, τόσο το δημόσιο όσο και το ιδιωτικό κλειδί δημιουργούνται ταυτόχρονα, από την Αρχή Πιστοποίησης, με την χρήση του ίδιου αλγόριθμου. Το ιδιωτικό κλειδί δίνεται μόνο στον αιτούντα ενώ το δημόσιο κλειδί είναι διαθέσιμο (ως τμήμα του ψηφιακού πιστοποιητικού) σ’ ένα κατάλογο στον οποίο έχουν πρόσβαση όλοι οι δικαιούχοι. Αντίθετα, το ιδιωτικό κλειδί δεν κοινοποιείται ποτέ ούτε αποστέλλεται μέσω διαδικτύου.

Η υποδομή δημοσίου κλειδιού περιλαμβάνει:

- Μια *Αρχή πιστοποίησης* (Certificate Authority) που εκδίδει και πιστοποιεί ψηφιακά πιστοποιητικά. Τα πιστοποιητικά αυτά περιλαμβάνουν το δημόσιο κλειδί ή πληροφορίες για το δημόσιο κλειδί.

- Μια *Αρχή Εγγραφής* (Registration Authority) όπου χρησιμεύει για την επιβεβαίωση της αρχής έκδοσης πιστοποιητικών πριν εκδοθεί ένα ψηφιακό πιστοποιητικό.

- Μια ή περισσότερες *Υπηρεσίες καταλόγου* (directory services) όπου διατηρούνται τα πιστοποιητικά (μαζί με τα δημόσια κλειδιά).

- Ένα *σύστημα διαχείρισης πιστοποιητικών.*

Πρακτικά οι λειτουργίες του PKI εφαρμόζονται από διαπιστευμένους ενδιάμεσους φορείς οι οποίοι παρέχουν επικοινωνιακές υπηρεσίες με στόχο την ενδυνάμωση της εμπιστοσύνης. Αυτοί οι φορείς από εδώ και στο εξής θα αναφέρονται ως οντότητες.

Η ανάθεση κλειδιού σε μία οντότητα είναι η διαδικασία εκείνη μέσω της οποίας ένα ζεύγος δημόσιου/ιδιωτικού κλειδιού συσχετίζεται με μία και μόνο οντότητα. Ο έλεγχος για την μοναδικότητα του κλειδιού πραγματοποιείται με τη χρήση της βάσης δημόσιων κλειδιών, της Αρχής Πιστοποίησης. Η οντότητα φέρει την ευθύνη της δημιουργίας του ζεύγους κλειδιών που θα χρησιμοποιήσει.

Μετά την δημιουργία, το δημόσιο τμήμα του κλειδιού αποστέλλεται στην Αρχή Πιστοποίησης για να ενσωματωθεί στο πιστοποιητικό και έτσι να πιστοποιηθεί η εγκυρότητα και η συσχέτισή του με τα στοιχεία της οντότητας. Το ιδιωτικό κλειδί δεν γνωστοποιείται στην Αρχή Πιστοποίησης ή σε οποιαδήποτε άλλον, σε καμία περίπτωση.

Η παραπάνω διαδικασία μπορεί να μεταβληθεί και η παραγωγή των κλειδιών να γίνει από την Αρχή Πιστοποίησης. Στην περίπτωση αυτή η αρχή πιστοποίησης αναλαμβάνει συχνά και το ρόλο της διαφύλαξης των κλειδιών (key escrow) για νομικούς, πρακτικούς ή επιχειρηματικούς λόγους.

Τα πιστοποιητικά αποθηκεύονται σε μια τοπική βάση δεδομένων και κατόπιν αποστέλλονται στον Εξυπηρετητή Καταλόγου προκειμένου να καταχωρηθούν στην εγγραφή της οντότητας την οποία πιστοποιούν.

Με τον τρόπο αυτό κάθε χρήστης διαθέτει ένα ιδιωτικό και ένα δημόσιο κλειδί Συγκεκριμένα το ιδιωτικό κλειδί χρησιμοποιείται για την ψηφιακή υπογραφή κειμένων ή μηνυμάτων ηλεκτρονικού ταχυδρομείου εξασφαλίζοντας με αυτό τον τρόπο την απόδειξη της ταυτότητας του αποστολέα και την πλήρη ακεραιότητα των προαναφερόμενων κειμένων ή μηνυμάτων, είναι μυστικό και πρέπει πάντα να

προστατεύεται από ένα προσωπικό κωδικό πρόσβασης (PIN - Personal Identification Number)

Το δημόσιο κλειδί ενός χρήστη είναι διαθέσιμο σε οποιονδήποτε άλλο χρήστη στην αποκρυπτογραφημένη μορφή του. Χρησιμοποιείται συνήθως με τους παρακάτω τρόπους :

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

Η διάδοση της υποδομής δημοσίου κλειδιού στο ηλεκτρονικό εμπόριο έχει οδηγήσει στην δημιουργία προϊόντων από πολλές εταιρίες όπως η RSA, η Verisign, η GTE CyberTrust, η Xcert και η Netscape που υποστηρίζουν τις διάφορες λειτουργίες της εν λόγω υποδομής. Παράλληλα, δημιουργούν και ένα πρόσφορα έδαφος για την υιοθέτηση ανάλογων τεχνολογιών από τις δημόσιες υπηρεσίες σε θέματα ηλεκτρονικής διακυβέρνησης.

4.3.2 Λειτουργικά Μοντέλα Διαχείρισης Ταυτότητας

4.3.2.1 Single Sign-On

Εξαιτίας της ανάγκης αυθεντικοποίησης των χρηστών σε πολλαπλά πληροφοριακά συστήματα, έγινε επιτακτική η διαχείριση των πολλών διαφορετικών διαπιστευτηρίων που μεταφέρει ο χρήστης, για να αποκτήσει πρόσβαση σε αυτά, γνωρίζοντας παράλληλα κάποια συγκεκριμένη μυστική συμβολοσειρά. Ένα τέτοιο παράδειγμα είναι το συνθηματικό πρόσβασης.

Χρησιμοποιώντας το συγκεκριμένο μοντέλο ο χρήστης απολαμβάνει πλεονεκτήματα όπως η ευκολία χρήσης και η ελαχιστοποίηση του κόστους της διαχείρισης, αφού ο αποκτά πολύ εύκολα πρόσβαση δηλώνοντας μόνο μια φορά το

όνομα του και τη μυστική συμβολοσειρά του. Από την άλλη πλευρά όμως αυτό το πρόγραμμα διαχείρισης απαιτεί χρήση εξειδικευμένου λογισμικού αλλά και αυξημένο κίνδυνο από επίβουλες οντότητες.

4.3.2.2. Συγχρονισμός Συνθηματικών

Το συγκεκριμένο μοντέλο βρίσκει απήχηση στους τομείς που χρησιμοποιούν συνθηματικά ως μέθοδο αυθεντικοποίησης και είναι οικονομικότερο εφόσον δεν απαιτεί εξειδικευμένο λογισμικό για τη χρήση του.

Ο βασικός χειρισμός αυτού του μοντέλου στηρίζεται στην επαναληπτική πληκτρολόγηση (συγχρονισμός) του μοναδικού συνθηματικού με σκοπό την πρόσβαση σε κάποιον συγκεκριμένο τομέα.

4.3.2.3 Συστήματα Ανώνυμων Πληρωμών & Τυφλές Ψηφιακές Υπογραφές

Βασικά στοιχεία στα συστήματα ανωνύμων πληρωμών είναι η κρυπτογραφία και οι τυφλές ψηφιακές υπογραφές. Η χρήση τους παρουσιάζει ορισμένες επιφυλάξεις από την πλευρά των χρηστών καθώς απαιτείται η δήλωση προσωπικών στοιχείων των ίδιων, όπως η διεύθυνση και το όνομα τους, και επιπρόσθετα η εφαρμογή τους γίνεται μέσα από μη πρότυπες τεχνολογίες.

Με τις τυφλές ψηφιακές υπογραφές ο χρήστης εξασφαλίζει την αυθεντικοποιήση των πληροφοριών χωρίς να γνωρίζει τον κάτοχο ή των αποστολέα αυτών. Συστήματα ανώνυμων πληρωμών είναι το Ecash και το Mondex.

4.3.2.4 Προστασία Ταυτότητας

Σκοπός της συγκεκριμένης τεχνολογίας είναι η προστασία των προσωπικών δεδομένων του κάθε χρήστη. Αυτό πραγματοποιείται με τη διαχείριση της πραγματικής ταυτότητας του, όπως επίσης και των διαφορετικών ψηφιακών ταυτοτήτων που χρησιμοποιεί κάθε χρήστης. Αφήνοντας του παράλληλα χώρο δράσης ως προς την πολυπλοκότητα των ταυτοτήτων του.

Ο προστάτης ταυτότητας τοποθετείται στο κέντρο του λειτουργικού συστήματος καθώς παρέχει τις λειτουργίες του ανάμεσα στους χρήστες ή τις εφαρμογές και στα προγράμματα, τα δεδομένα ή τις πληροφορίες για τις οποίες ζητά πρόσβαση ο χρήστης.

Σημαντικός ρόλος του προστάτη ταυτότητας είναι το ότι χωρίζει τα πεδία που μπορεί να ενεργήσει ο χρήστης χρησιμοποιώντας τις διάφορες ψηφιακές του ταυτότητες, και σε εκείνα που είναι απαραίτητη η εξακρίβωση της πραγματικής του ταυτότητας, προς αποφυγή μη επιθυμητών ή παράνομων ενεργειών του χρήστη.

Το σύστημα μετατρέπει την πραγματική ταυτότητα σε υποκείμενες ψευδοταυτότητες. Από τις τελευταίες δεν είναι δυνατή η αποκάλυψη της πραγματικής ταυτότητας εφόσον δεν περιέχονται εξακριβωμένα δεδομένα του χρήστη ώστε να συνδυαστούν ή και να αντιστοιχηθούν με τα πραγματικά προσωπικά του δεδομένα. Έτσι είναι αναγκαία η ύπαρξη τρίτων οντοτήτων υπηρεσιών που θα εξασφαλίζουν την αμοιβαία εμπιστοσύνη ως προς την αξιοπιστία της χρήσης του.

4.3.2.5 Re-Webbers και Onion Routing

Η τεχνολογία των re-webbers χρησιμοποιείται κυρίως από τα δίκτυα TAZ και Crowds και λειτουργεί με κατάλληλους εξυπηρετές υπηρεσιών παγκόσμιου ιστού. Κατά τη λειτουργία της τεχνολογίας αυτής δημοσιεύεται στο διαδίκτυο ένας «δείκτης» ο οποίος κατευθύνει το χρήστη στην διεύθυνση του επιθυμητού δικτυακού τόπου αλλά δεν δηλώνεται η συγκεκριμένη διεύθυνση σε αυτόν.

Επιπλέον οι παραπάνω δείκτες είναι κρυπτογραφημένοι για μεγαλύτερη ασφάλεια. Οι εξυπηρετητές που υποστηρίζουν αυτή τη διαδικασία ουσιαστικά δρομολογούν τα URL που εισάγει ο ενδιαφερόμενος χρήστης, με αποτελέσματα να μην γίνεται άμεση σύνδεση του με τον πραγματικό δικτυακό τόπο, αλλά έμμεση μέσω της παραπάνω λειτουργίας που περιγράψαμε.

Παρόμοια είναι η τεχνική των Onion Routing η οποία όμως είναι ανεξάρτητη και δρα σε επίπεδο δικτύου και με ακόλουθες κρυπτογραφήσεις των πληροφοριών χρησιμοποιώντας δημόσιο κλειδί. Κάτι τέτοιο την καθιστά ασφαλέστερη καθώς κάθε πακέτο πληροφοριών, που ανταλλάσσεται στη σύνδεση, περιέχει στοιχεία μόνο για τα γειτονικά βήματα που ακολουθούνται.

4.3.2.6 (OPS) & (P3P)

Το OPS-Open Profiling Standard είναι ένα μοντέλο που παρέχει στους χρήστες έλεγχο των προσωπικών τους στοιχείων και παράλληλα ασφαλή διαχείριση των πληροφοριών, που χρησιμοποιούν, από τους διαχειριστές των δικτυακών τόπων. Η λειτουργία του υποστηρίζεται από το P3P - Platform for Privacy Preferences.

Το P3P είναι ένα πρωτόκολλο το όποιο αυτοματοποιεί τη διαδικασία επεξεργασίας, αποθήκευσης και ελέγχου των προσωπικών δεδομένων από τους ίδιους τους χρήστες του διαδικτύου αλλά και από τους παρόχους των δικτυακών τόπων που χρησιμοποιεί ο χρήστης από τη δική τους πλευρά αντίστοιχα. Στην ουσία γίνονται αποδεκτά τα πλαίσια λειτουργίας ενός συστήματος ως προς την πολιτική προστασίας των δεδομένων που παρέχονται. Έτσι ο χρήστης είναι απόλυτα ενημερωμένος για τη συλλογή των στοιχείων του από τους παρόχους του δικτυακού τομέα που επισκέπτεται. Κάθε εφαρμογή που βασίζεται στο P3P περιέχει τη βεβαίωση αποδοχής του χρήστη.

Η χρήση του P3P εμπεριέχει πολλά μειονεκτήματα και αμφισβητήσεις εφόσον δεν παρέχει καμία βεβαιότητα αυθεντικοποίησης του συστήματος, το όποιο το χρησιμοποιεί, και κατά συνέπεια δεν εξασφαλίζεται ούτε η προστασία και η διακίνηση των δεδομένων από την πλευρά των παρόχων των δικτυακών τόπων.

Επιπρόσθετα, εξειδικευμένα λογισμικά που χρησιμοποιούνται για τον έλεγχο των δράσεων των cookies, δικτυοενδιάμεσοι, τα δίκτυα προστασίας και τα δίκτυα ιδιωτικότητας είναι επίσης κάποιες ευρέως χρησιμοποιούμενες τεχνολογίες διαχείρισης ταυτοτήτων στο διαδίκτυο.

5. Συμπεράσματα

Στην παρούσα μελέτη παρουσιάστηκε μια συστηματική προσέγγιση του θέματος της διαχείρισης ταυτότητας στα πλαίσια της ηλεκτρονικής διακυβέρνησης. Προς αυτή την κατεύθυνση, εξετάσθηκε η τεχνολογική ετοιμότητα της χώρας και οι παρεχόμενες τεχνολογικές λύσεις που καλούνται να υποστηρίξουν τα συστήματα διαχείρισης ταυτότητας αναλύοντας τη χρήση των τεχνολογιών διαχείρισης ταυτότητας.

Αν και οι τεχνολογικές λύσεις είναι σε θέση να δώσουν ικανοποιητικές απαντήσεις σε ένα σημαντικό αριθμό προβλημάτων που υφίστανται είναι σαφές ότι η ουσία της διαχείρισης ταυτότητας έγκειται στις τεχνολογίες που θα την υποστηρίξουν αλλά και στον τρόπο που θα οριστεί η ταυτότητα στις μέρες μας και στο είδος της σχέση που θα θελήσει να έχει η κοινωνία των πολιτών με τον κρατικό μηχανισμό.

Διαπιστώνεται ότι φλέγον ζήτημα παραμένει η ανάγκη διασύνδεσης και συνεργασίας μεταξύ των συστημάτων δηλαδή η διαλειτουργικότητα και κυρίως κατά πόσο η ομοιογένεια που επιβάλλει η τεχνολογία μπορεί να συμβαδίσει με την αποκέντρωση και αυτονομία που προωθούν οι περισσότερες δημόσιες διοικήσεις.

Η διαχείριση ταυτότητας εστιάζει στην ανεύρεση εκείνων των μοναδικών φορέων ταυτοποίησης που θα επιτρέπουν την ασφαλή ταυτοποίηση των δικαιούχων χωρίς παράλληλα να θεωρούνται ότι παραβιάζουν την προσωπικότητα και τις ελευθερίες του πολίτη αποδίδοντας πολλές αρμοδιότητες στο κράτος.

Οι κρατικές υπηρεσίες προτάσσουν ζητήματα ασφάλειας και προστασίας από ένα διαρκώς πιο απειλητικό διεθνές περιβάλλον ως επιχειρήματα για την ψηφιοποίηση και υιοθέτηση φορέων ταυτοποίησης των οποίων φυσικός φορέας μέχρι τώρα ήταν αποκλειστικά το ίδιο το άτομο (π.χ. βιομετρικά δεδομένα). Η κοινωνία είτε άμεσα είτε έμμεσα εστιάζει στον προσδιορισμό της πληροφοριακής ταυτότητας των πολιτών και στα περιθώρια ελεύθερης διαχείρισης των δεδομένων που έχουν οι ίδιοι στην κατοχή τους.

Στην Ελλάδα, η οποία συγκαταλέγεται σε εκείνες που έχασαν το πρώτο κύμα ανάπτυξης υπηρεσιών ηλεκτρονικής διακυβέρνησης και πλέον προχωρούν με βάση τις υπάρχουσες λύσεις και μια εγκαθιδρυμένη γνώση για τα ζητήματα του χώρου, το ζήτημα της διαχείρισης ταυτότητας δεν έχει ανακύψει στις ουσιαστικές του διαστάσεις.

Η επιτακτική ανάγκη της κοινωνίας να συμμετέχει στις νέες εξελίξεις στρέφει το ενδιαφέρον κάθε πλευράς σε τεχνολογικά ζητήματα. Σημασία πλέον έχει ο αριθμός νέων συστημάτων που υλοποιούνται καθώς και ο ρυθμός με τον οποίο η χώρα προσεγγίζει πιο ανεπτυγμένους εταίρους της.

Συμπερασματικά, η εξέλιξη των συστημάτων διαχείρισης ταυτότητας ευνοεί κυρίως την αντιμετώπιση τεχνολογικών προβλημάτων που προκύπτουν. Η διαφορά των ώριμων τεχνολογικά χωρών είναι ότι έχει αναπτυχθεί μια ευρύτερη συνείδηση ότι τα τεχνολογικά ζητήματα έχουν και ένα κοινωνικό-πολιτικό υπόβαθρο που πρέπει να λαμβάνεται υπόψη κατά την εξέταση πιθανών λύσεων.

Βιβλιογραφία - Αναφορές

- Ειδική Υπηρεσία Διαχείρισης Επιχειρησιακού Προγράμματος «Κοινωνία της Πληροφορίας» (2002). Ελληνικό πλαίσιο διαλειτουργικότητας ηλεκτρονικής διακυβέρνησης
- Candia, T. (2004). Benefits of Federated Identity to Government. Liberty Aliance Project.
- Dyson, E. (2002). Digital identity management. Release 1.0.
- E-business forum (2007). Διαχείριση Ταυτότητας στις Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης.
- Pato, J. & Rouault, J. (2003). Identity management: The drive to federation. Technical White Papers.
- Hansen, M. & Krasemann, H. (2005). Privacy and Identity Management for Europe – PRIME White Paper
- Stalder, F. (1998). Digital identities and smart cards.
- Stalder, F. (2000). Digital identities patterns in information flows. Budapest: Intermedia Departement, Academy of Fine Arts.
- Stalder, F. (2000). Informational identity: From analog to digital. Korunk
- Stalder, F. (2001). Digital Identities.
- Turkle, S. (1995). Life on the screen. Identity in the age of the internet.New York: Simon & Schuster.