|  |  |
| --- | --- |
| C:\A_PATRA_texts\PMS_2016\studentsMSC\MiaoulisDionysios\Latex diplwmatikh\University_of_Patras_(seal).png | **Σχολή Οργάνωσης και Διοίκησης Επιχειρήσεων****Τμήμα Διοίκησης Επιχειρήσεων** |

***Έξυπνες κάρτες και εφαρμογές τους στη διαχείριση Ηλεκτρονικής Ταυτότητας***

***(e-Identity) για τον πολίτη***



Μάθημα: Ηλεκτρονική Διακυβέρνηση

|  |
| --- |
| **Περιεχόμενα** |

|  |  |
| --- | --- |
| **Εισαγωγή…………………………………………………………………………………………………………** | **3** |
| **Ενότητα 1: Ηλεκτρονική Διακυβέρνηση…………………………………………………………** | **4** |
|  | 1.1 Ο όρος ηλεκτρονική διακυβέρνηση………………………………………….. | 4 |
|  | 1.2 Πλεονεκτήματα ηλεκτρονικής διακυβέρνησης…………………………. | 4 |
|  | 1.3 Μειονεκτήματα ηλεκτρονικής διακυβέρνησης…………………………. | 5 |
| **Ενότητα 2: Έξυπνες Κάρτες (Smart Cards)………………………………………………………** | **6** |
|  | 2.1 Εισαγωγή………………………………………………………………………………….. | 6 |
|  | 2.2 Τύποι έξυπνων καρτών……………………………………………………………… | 7 |
|  | 2.3 Μεταφορά δεδομένων………………………………………………………………. | 8 |
|  | 2.4 Multos……………………………………………………………………………………….. | 9 |
| **Ενότητα 3: Ηλεκτρονική Ταυτοποίηση (e-ID)………………………………………………….** | **10** |
|  | 3.1 Τι είναι η ηλεκτρονική ταυτοποίηση…………………………………………. | 10 |
|  | 3.2 Αρχιτεκτονική συστημάτων ηλεκτρονικής ταυτοποίησης………….. | 11 |
|  | 3.3 Πλεονεκτήματα ηλεκτρονικής ταυτοποίησης…………………………….. | 12 |
|  | 3.4 Μειονεκτήματα ηλεκτρονικής ταυτοποίησης…………………………….. | 13 |
| **Ενότητα 4: e-ID στην Ελλάδα…………………………………………………………………………..** | **15** |
|  | 4.1 Ηλεκτρονική διακυβέρνηση στην Ελλάδα………………………………….. | 15 |
|  | 4.2 Ηλεκτρονική ταυτοποίηση στην Ελλάδα……………………………………. | 16 |
|  | 4.3 Προτάσεις για επιτυχή εφαρμογή ηλεκτρονικής ταυτοποίησης…. | 18 |
| **Συμπεράσματα……………………………………………………………………………………………….** | **19** |
| **Βιβλιογραφία………………………………………………………………………………………………….** | **20** |

|  |
| --- |
| **Εισαγωγή** |

Τη σημερινή εποχή η αλματώδης εξέλιξη της τεχνολογίας προσφέρει διευκόλυνση στις ανθρώπινες δραστηριότητες, αυξάνοντας την αποτελεσματικότητα στην επικοινωνία, αλλά και την αποδοτικότητα στην εργασία. Η τελευταία δεκαετία ιδιαίτερα, χαρακτηρίζεται από καταιγισμό εφαρμογών Τεχνολογίας της Πληροφορίας. Το πρόβλημα της απόστασης έχει επιλυθεί, καθώς είναι δυνατή η άμεση επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου, τηλεδιασκέψεων και πολλών άλλων τρόπων, οι οποίοι καθιστούν δυνατές τόσο την επικοινωνία όσο και οποιουδήποτε είδους συναλλαγές, χωρίς να είναι απαραίτητη η φυσική παρουσία του ατόμου.

Οι σύγχρονες συνθήκες ζωής έχουν όλο και περισσότερες απαιτήσεις, γεγονός που αναγκάζει τους πολίτες να αναζητούν μεγαλύτερη ευκολία και ευελιξία στις συναλλαγές τους με τον δημόσιο τομέα. Συνεπώς, η Πολιτεία οφείλει να στραφεί στις νέες τεχνολογίες, ώστε να πραγματοποιούνται δραστηριότητες με μεγαλύτερη αποτελεσματικότητα, που θα ανταποκρίνονται στις απαιτήσεις του πολίτη και θα τον διευκολύνουν σε οποιεσδήποτε υποχρεώσεις του.

|  |
| --- |
| **Ενότητα 1: Ηλεκτρονική Διακυβέρνηση** |

* 1. **Ο όρος ηλεκτρονική διακυβέρνηση**

Γενικά, ο όρος ηλεκτρονική διακυβέρνηση (e-government) αφορά την εισαγωγή των τεχνολογιών της πληροφορικής και των υπολογιστών στη δημόσια διοίκηση. Κάθε εφαρμογή ηλεκτρονικής διακυβέρνησης αναγράφεται με το πρόθεμα «e-», για να δηλώσει τον ηλεκτρονικό τρόπο παραγωγής και διανομής των υπηρεσιών.

Μία μερίδα ανθρώπων υποστηρίζει, ότι η ηλεκτρονική διακυβέρνηση εστιάζει στην πρακτική αποδοτικότητα και στη μείωση του κόστους, όπως αυτές που μπορούν για παράδειγμα να προέλθουν από την ηλεκτρονική κατάθεση της φορολογικής δήλωσης και τον ηλεκτρονικό εφοδιασμό. Για κάποιους άλλους, εστιάζει στη δημοκρατική συμμετοχή και τείνει να ξεπεράσει την πολιτική αποστασιοποίηση.

Στην Ελλάδα μόνο ένα πολύ μικρό ποσοστό επενδύσεων αφορά τη βελτίωση των υπηρεσιών, που προσφέρονται στον πολίτη. Αντίθετα, σε άλλες χώρες δίνεται ιδιαίτερη έμφαση από τις δημόσιες υπηρεσίες για την εξυπηρέτηση του πολίτη, ο οποίος αποκτά μία πολύ θετική εικόνα για αυτές. Ο λόγος αυτής της διαφοράς αφορά τα μειονεκτήματα, που έχει η μηχανογραφική οργάνωση του ελληνικού δημόσιου τομέα.

* 1. **Πλεονεκτήματα ηλεκτρονικής διακυβέρνησης**

Μία προσπάθεια ηλεκτρονικής διακυβέρνησης σίγουρα παρουσιάζει αρκετές δυσκολίες, όμως μπορεί να προσφέρει σημαντικά πλεονεκτήματα.

Το πιο σημαντικό πλεονέκτημα είναι η εξοικονόμηση πόρων, καθώς μειώνει σε μεγάλο βαθμό το κόστος λειτουργίας των δημόσιων υπηρεσιών. Οι συναλλαγές γίνονται πλέον ηλεκτρονικά, περιορίζοντας έτσι, το κόστος προμήθειας χαρτιού, εκτύπωσης εντύπων, ταχυδρομικής αποστολής εγγράφων και εξόδων προσωπικού.

Δεύτερο και εξίσου σημαντικό πλεονέκτημα, το οποίο αφορά τη διευκόλυνση του πολίτη, είναι η καλύτερη εξυπηρέτησή του, καθώς μειώνεται η γραφειοκρατία, δεν είναι αναγκασμένος να περιμένει σε πολύωρες ουρές και μπορεί να κάνει χρήση των καλύτερων αυτών υπηρεσιών οποιαδήποτε στιγμή της ημέρας.

Το τρίτο πλεονέκτημα έχει να κάνει με την ενίσχυση της δημοκρατίας. Η χώρα χαρακτηρίζεται από ένα κλίμα αδιαφορίας και απαξίωσης για τα πολιτικά δρώμενα, γεγονός, που εύκολα γίνεται αντιληπτό από το μεγάλο ποσοστό αποχής από την εκλογική διαδικασία. Η ηλεκτρονική διακυβέρνηση έρχεται, για να δημιουργήσει μία πιο προσιτή κυβέρνηση με δυνατότητες ενημέρωσης και συμμετοχής του πολίτη μέσω ηλεκτρονικών μέσων για λήψεις περισσότερο δημοκρατικών αποφάσεων.

Τέλος, είναι σημαντικό για τις δημόσιες υπηρεσίες να δημιουργούν μία καλή εικόνα απέναντι στους πολίτες, αυτή της σύγχρονης δημόσιας διοίκησης, με μηδαμινή γραφειοκρατία και υψηλά αποδοτικές δομές.

* 1. **Μειονεκτήματα ηλεκτρονικής διακυβέρνησης**

Η πρόοδος, που έχει ήδη επιφέρει η ηλεκτρονική διακυβέρνηση είναι πολύ μεγάλη και με την πάροδο του χρόνου αναμένεται ακόμα μεγαλύτερη. Οι δυνατότητες συλλογής, αποθήκευσης και επεξεργασίας της πληροφορίας είναι πλέον ιδιαίτερα αυξημένες, γεγονός που θέτει σε κίνδυνο την ιδιωτική ζωή των πολιτών. Η μετάδοση προσωπικών δεδομένων μέσω ίντερνετ, η αποθήκευση σε δημόσια υπολογιστικά συστήματα και η υψηλή πιθανότητα υποκλοπής δυσκολεύουν τις προσπάθειες προστασίας και σεβασμού της ιδιωτικής ζωής.

Για την αντιμετώπιση τέτοιων απειλών, που μπορεί να ξεκινούν από μικρής σημαντικότητας μέχρι ιδιαίτερα υψηλής, κρίνονται απαραίτητοι μηχανισμοί ασφαλείας, οι οποίοι θα μπορούν να εγγυηθούν την αυθεντικότητα της ταυτότητας των συναλλασσόμενων, την ακεραιότητα και την εμπιστευτικότητα του περιεχομένου κάθε συναλλαγής. Όλα τα παραπάνω καλύπτονται με μία σειρά τεχνολογιών, όπως είναι οι έξυπνες κάρτες (smart cards).

Όταν ένας πολίτης πραγματοποιεί συναλλαγές με το κράτος καλείται να κατέχει και να επιδείξει μία ταυτότητα. Είναι σαφές, ότι σε ένα σύστημα ηλεκτρονικής διακυβέρνησης οι συναλλαγές θα υλοποιούνται με ηλεκτρονικές ταυτότητες σε μορφή έξυπνων καρτών, δηλαδή καρτών με ενσωματωμένο μικροεπεξεργαστή.

|  |
| --- |
| **Ενότητα 2: Έξυπνες Κάρτες (Smart Cards)** |

**2.1 Εισαγωγή**

Οι έξυπνες κάρτες είναι πλαστικές κάρτες, έχουν μέγεθος αντίστοιχο με τις πιστωτικές και διαθέτουν ενσωματωμένο μικροεπεξεργαστή. Σκοπός τους είναι η υλοποίηση ευαίσθητων, από άποψη ασφάλειας, κρυπτογραφικών λειτουργιών στο προστατευόμενο εσωτερικό τους περιβάλλον. Αυτό σημαίνει, ότι η πληροφορία δεν αποθηκεύεται σε υπολογιστή, σε μέρος δηλαδή, όπου η πιθανότητα υποκλοπής των δεδομένων είναι σαφώς μεγαλύτερη.

Η τεχνολογία των έξυπνων καρτών παρουσιάζει ορισμένα πλεονεκτήματα, όπως το μικρό μέγεθος, και η ολοένα αυξανόμενη μνήμη και υπολογιστική ισχύς. Παρ’ όλα αυτά, ιδιαίτερα σημαντικό κρίνεται το μειονέκτημά τους, το οποίο είναι, ότι χρειάζεται συσκευή ανάγνωσης (smart card reader) στον υπολογιστή, που θα χρησιμοποιηθεί η κάρτα. Παρ’ όλο, που το κόστος των συσκευών αυτών έχει μειωθεί αρκετά, οι περισσότεροι υπολογιστές δεν διαθέτουν τέτοιες συσκευές.

Η Κοινωνία της Πληροφορίας βασίζεται σε μεγάλο βαθμό στις έξυπνες κάρτες, καθώς αποτελεί μία από τις κυριότερες λειτουργίες της. Ιδιαίτερη έμφαση, βέβαια, δίνει σε ένα συγκεκριμένο πεδίο εφαρμογής, που δεν είναι άλλο από τη δικτυακή ασφάλεια. Τα προβλήματα ασφάλειας κλονίζουν την εμπιστοσύνη των πολιτών για τα δίκτυα δεδομένων και τα πληροφοριακά συστήματα, με αποτέλεσμα να αρνούνται τη χρήση τους, και επομένως την ελλιπή αξιοποίηση των δυνατοτήτων τους προς όφελος των πολιτών.

Στο σημείο αυτό γίνεται λόγος για τις έξυπνες κάρτες, οι οποίες καθιστούν ασφαλέστερο τον έλεγχο αυθεντικότητας κατά την είσοδο σε ηλεκτρονικές υπηρεσίες. Η κάρτα έχει αποθηκευμένο ένα ψηφιακό πιστοποιητικό, το οποίο χρησιμοποιείται για τον έλεγχο αυθεντικότητας. Αντί για όνομα χρήστη και κωδικό ασφαλείας, ο χρήστης ακολουθεί μια διαδικασία πρόκλησης – απόκρισης (challenge – response). Ο έλεγχος αυθεντικότητας επιτυγχάνεται, αφού αποδεικνύεται η γνησιότητα του πιστοποιητικού και ότι ο χρήστης είναι ο γνήσιος χρήστης του πιστοποιητικού, αφού μόνο αυτός έχει πρόσβαση στο ιδιωτικό κλειδί (υπάρχει βέβαια πιθανότητα να έχει διαρρεύσει).

Συνεπώς, για να αποδεχθούν οι πολίτες τις έξυπνες κάρτες πρέπει να καταπολεμηθούν ορισμένα προβλήματα, όπως η προστασία των προσωπικών δεδομένων, που θα εμπεριέχουν, αλλά και η διάθεση συσκευών ανάγνωσής τους σε ηλεκτρονικές συσκευές καθημερινής χρήσης. Οι έξυπνες κάρτες μπορούν να προσφέρουν ασφαλή πρόσβαση σε υπηρεσίες για τους πολίτες και σε συνδυασμό με κατάλληλες πολιτικές χρήσης και σύγχρονη νομοθεσία, μπορούν να προστατεύσουν την ιδιωτική ζωή και να δημιουργήσουν ένα αίσθημα εμπιστοσύνης στους πολίτες προς αυτή τη νέα τεχνολογία. Με τον τρόπο αυτό, οι πολίτες θα μπορέσουν να τις αποδεχθούν και να τις εισάγουν στην καθημερινότητά τους.

**2.2 Τύποι έξυπνων καρτών**

Τα κριτήρια με βάση τα οποία διακρίνονται οι τύποι έξυπνων καρτών είναι το είδος της λογικής, που περιέχουν, ο τύπος των επαφών τους και το είδος και το πλήθος των εφαρμογών, που υποστηρίζουν. Έτσι, ταξινομούνται ως εξής:

* **Κάρτες μνήμης (Memory cards)**

Αποτελούν το πρώτο είδος έξυπνων καρτών και έχουν χρησιμοποιηθεί σε μεγάλες ποσότητες ως τηλεκάρτες. Τα δεδομένα, που αποτελούν και την αξία της κάρτας, είναι αποθηκευμένα σε μνήμη EEPROM και τα στοιχεία αναγνώρισης (όνομα κατασκευαστή, σειριακός αριθμός) σε μνήμη ROM. Όταν η αξία της κάρτας μηδενίζεται, η κάρτα δεν χρησιμοποιείται ξανά, λόγω ενός κυκλώματος ασφαλείας, που δεν επιτρέπει την επανεγγραφή. Οι κάρτες μνήμης έχουν χρήση ως τηλεφωνικές κάρτες, κάρτες ταυτότητας σε εφαρμογές με χαμηλό επίπεδο απαιτήσεων σε ασφάλεια, μέσο πληρωμής σε χώρους στάθμευσης, σταθμούς διοδίων κλπ.

* **Κάρτες μικροεπεξεργαστή (Microprocessor cards)**

Περιλαμβάνουν επεξεργαστή περιορισμένων δυνατοτήτων (8 ή 16 bit). Τη λειτουργία του υποστηρίζουν η μνήμη ROM (λειτουργικό σύστημα της κάρτας), η μνήμη EEPROM (εφαρμογές, που υποστηρίζει η κάρτα), η μνήμη RAM (περιοχή εργασίας του επεξεργαστή) και η μονάδα Εισόδου/Εξόδου (καταχωρητής 1 bit).

* **Κάρτες υποδομής δημόσιου κλειδιού (PKI cards)**

Είναι κάρτες μικροεπεξεργαστή, που περιλαμβάνουν συνεπεξεργαστή για τις κρυπτογραφικές λειτουργίες. Τέτοιες λειτουργίες είναι η δημιουργία ζεύγους RSA κλειδιών, η δημιουργία και επαλήθευση ψηφιακών υπογραφών, η κρυπτογράφηση και η αποκρυπτογράφηση.

* **Κάρτες χωρίς επαφές (Contactless cards)**

Χαρακτηριστικό τους είναι ο τρόπος με τον οποίο επικοινωνεί η κάρτα με τη συσκευή ανάγνωσης, αλλά και το πώς τροφοδοτείται η κάρτα, δηλαδή μέσω ραδιοσυχνοτήτων (δεν έχουν ηλεκτρικές επαφές), που εκπέμπει μία ενσωματωμένη κεραία. Προτιμώνται σε περιπτώσεις μεγάλου αριθμού συναλλαγών σε σύντομο χρονικό διάστημα (πχ χρέωση δημόσιων συγκοινωνιακών μέσων).

* **Υβριδικές κάρτες (Hybrid cards)**

Όπως δηλώνει και η ονομασία τους, συνδυάζουν δύο διαφορετικές τεχνολογίες καρτών. Όταν γίνεται λόγος για κάρτες μικροεπεξεργαστή, οι υβριδικές περιέχουν δύο ολοκληρωμένα κυκλώματα: το ένα συνδέεται σε ηλεκτρικές επαφές και το άλλο σε κεραία και η κάρτα αυτή ονομάζεται διπλής διεπαφής (dual interface card). Άλλου είδους υβριδικές κάρτες είναι αυτές, που έχουν μικροεπεξεργαστή με μαγνητική ταινία, με bar code κλπ.

* **Οπτικές έξυπνες κάρτες (Optical smart cards)**

Διαθέτουν στην επιφάνειά τους μια οπτική περιοχή για εγγραφή (αποθηκεύουν μερικά megabyte) και ανάγνωση δεδομένων. Έχουν αρκετά μεγάλη χωρητικότητα σε σχέση με τους άλλους τύπους καρτών και γι’ αυτό χρησιμοποιούνται για αποθήκευση ιατρικών δεδομένων. Παρ’ όλα αυτά, σημαντικά μειονεκτήματα είναι το κόστος και το ότι δεν υπάρχει η δυνατότητα επανεγγραφής στην οπτική περιοχή.

* **Κάρτες πολλαπλών εφαρμογών (Multi-application smart cards)**

Μπορούν να υποστηρίξουν παραπάνω από μία εφαρμογές. Στη μνήμη EEPROM αποθηκεύονται όλες οι εφαρμογές, που μπορεί να έχει ο χρήστης. Δηλαδή, ηλεκτρονικό πορτοφόλι και άλλα συστήματα πληρωμών, τραπεζικές εφαρμογές, ηλεκτρονική ταυτότητα, δίπλωμα οδήγησης, διαβατήριο, κάρτα υπηρεσιών υγείας, κάρτα κοινωνικής ασφάλισης κλπ.

**2.3 Μεταφορά δεδομένων**

Η επικοινωνία μεταξύ συσκευής ανάγνωσης και έξυπνης κάρτας είναι μονόδρομη, λόγω της μίας επαφής, που χρησιμοποιείται. Αυτό σημαίνει, ότι χρησιμοποιούν εναλλάξ τη γραμμή εισόδου/εξόδου για την αποστολή δεδομένων. Πρώτη κάνει αίτηση η συσκευή ανάγνωσης και ύστερα απαντά η κάρτα στις αιτήσεις. Είναι, δηλαδή, σχέση αφέντη – σκλάβου (master – slave), με αφέντη τη συσκευή ανάγνωσης.

**2.4 Multos**

Η κοινοπραξία Multos δημιουργήθηκε με στόχο τον ορισμό ενός προτύπου για έξυπνες κάρτες πολλαπλών εφαρμογών, η οποία εκπληρώνει τους παρακάτω όρους και πετυχαίνει τα υψηλότερα επίπεδα ασφάλειας:

* Μόνο ο εκδότης της κάρτας μπορεί να προσθαφαιρέσει εφαρμογές για την καλή λειτουργία της.
* Η μεταφορά εφαρμογών μπορεί να γίνεται μέσω δημόσιων και μη προστατευόμενων δικτύων χωρίς να μειώνεται η ασφάλειά της.
* Υποστηρίζονται πολλοί προμηθευτές εφαρμογών χωρίς να είναι απαραίτητη η γνωστοποίηση μυστικών κλειδιών ή του κώδικα των εφαρμογών μεταξύ προμηθευτών εφαρμογών και εκδοτών καρτών.

Το αποτέλεσμα της κοινοπραξίας ήταν η δημιουργία του Multos, του πρώτου ανοιχτού, υψηλής ασφάλειας λειτουργικού συστήματος για έξυπνες κάρτες πολλαπλών εφαρμογών.

|  |
| --- |
| **Ενότητα 3: Ηλεκτρονική Ταυτοποίηση (e-ID)** |

**3.1 Τι είναι η ηλεκτρονική ταυτοποίηση**

Η ηλεκτρονική ταυτοποίηση είναι η ηλεκτρονική λύση για την ταυτοποίηση των πολιτών, με σκοπό την υποστήριξη χρήσης υπηρεσιών ηλεκτρονικής διακυβέρνησης. Ένας τρόπος ηλεκτρονικής ταυτοποίησης είναι η ηλεκτρονική ταυτότητα, με τη χρήση της οποίας, τα άτομα αποδεικνύουν, ότι είναι τα πρόσωπα, που ισχυρίζονται, και στη συνέχεια μπορούν να αποκτήσουν πρόσβαση σε σχετικές ηλεκτρονικές υπηρεσίες.

Η ηλεκτρονική ταυτότητα ορίζεται ως η ψηφιακή αναπαράσταση πεπερασμένου αριθμού πληροφοριών για ένα πολίτη ή οργανισμό. Μπορεί να περιλαμβάνει τα χαρακτηριστικά ενός ατόμου, όπως όνομα και επώνυμο, προσωπικό αναγνωριστικό αριθμό (PIN), αριθμό διαβατηρίου, βιομετρικά δεδομένα, πληροφορίες σχετικά με τις δραστηριότητές του στο διαδίκτυο (αναζητήσεις, συναλλαγές κλπ).

Η ηλεκτρονική ταυτοποίηση αποτελείται από τρία στάδια. Αρχικά ο χρήστης παρουσιάζει μία ταυτοποίηση, μετά αυτή επαληθεύεται και τέλος, αν η επαλήθευση είναι επιτυχής, επιτρέπεται η πρόσβαση στο περιεχόμενο της υπηρεσίας, που επιθυμεί ο χρήστης (εικόνα 1).

 Ταυτοποίηση Επαλήθευση Εξουσιοδότηση

***Εικόνα 1: Στάδια ηλεκτρονικής ταυτοποίησης***

Ο ρόλος της ηλεκτρονικής ταυτότητας, λοιπόν, είναι να αποτελέσει το μέσο για την ταυτοποίηση των πολιτών στο περιβάλλον της ηλεκτρονικής διακυβέρνησης. Στόχος είναι η αντικατάσταση της απλής ταυτότητας με ηλεκτρονική, η οποία θα μπορεί να χρησιμοποιηθεί σε όλους τους τομείς, και στον φυσικό κόσμο, αλλά και σε ηλεκτρονικές υπηρεσίες. Σκοπός είναι να χρησιμοποιείται σε πληθώρα εφαρμογών (πχ και ως διαβατήριο) χωρίς να είναι απαραίτητη η κατοχή κάποιου άλλου μέσου, αλλά και να ενισχύσει την εμπιστοσύνη των πολιτών με την παροχή δυνατοτήτων προστασίας δεδομένων υψηλού επιπέδου.

Μέχρι και σήμερα, λοιπόν, η δημιουργία ηλεκτρονικής ταυτότητας πραγματοποιείται με έξυπνες κάρτες. Η ηλεκτρονική ταυτότητα είναι μία έξυπνη κάρτα, που περιέχει δύο τουλάχιστον ιδιωτικά κλειδιά (για ψηφιακές υπογραφές και για κρυπτογράφηση δεδομένων) και τα αντίστοιχα πιστοποιητικά δημόσιου κλειδιού.



***Εικόνα 2: Ηλεκτρονική ταυτότητα (e-ID) στο Βέλγιο***

**3.2 Αρχιτεκτονική συστημάτων ηλεκτρονικής ταυτοποίησης**

Κατά τη διαδικασία εξυπηρέτησης του πολίτη σε κάποια ηλεκτρονική υπηρεσία συμμετέχουν ο χρήστης, δηλαδή το άτομο, που επιθυμεί να χρησιμοποιήσει την ηλεκτρονική υπηρεσία, ο πάροχος υπηρεσιών, δηλαδή ο φορέας, που προσφέρει την αντίστοιχη υπηρεσία και ο πάροχος ταυτότητας, δηλαδή ο φορέας, που επιβεβαιώνει την ταυτότητα του χρήστη στον πάροχο υπηρεσιών.

Για να είναι επιτυχημένη η αρχιτεκτονική των συστημάτων ηλεκτρονικής ταυτοποίησης, θα πρέπει να ικανοποιούνται δύο σχέσεις εμπιστοσύνης:

* μεταξύ χρήστη και παρόχου ταυτότητας, καθώς ο πάροχος ταυτότητας γνωρίζει και διαχειρίζεται τις πληροφορίες ταυτότητας του χρήστη και επαληθεύει την ταυτότητά του.
* μεταξύ παρόχου ταυτότητας και παρόχου υπηρεσιών, καθώς ο πάροχος υπηρεσιών καλείται να εμπιστευθεί τις απαντήσεις του παρόχου ταυτότητας, ώστε να επιτρέψει στον χρήστη την πρόσβαση στις υπηρεσίες του.

Πρακτικά, το σύστημα αυτό προϋποθέτει μία βάση δεδομένων, που εμπεριέχει όλες τις πληροφορίες του χρήστη. Σε αυτή πρέπει αρχικά να εγγραφεί ο χρήστης και μετά να κάνει χρήση των ηλεκτρονικών υπηρεσιών. Σε κάθε αίτηση του χρήστη πρέπει να γίνει ηλεκτρονική ταυτοποίηση. Ο πάροχος υπηρεσιών απευθύνεται στον πάροχο ταυτότητας, ο οποίος με τη σειρά του ανατρέχει στην κεντρική βάση δεδομένων. Αφού επεξεργαστεί τις απαιτούμενες πληροφορίες και αναγνωρίσει τον χρήστη, απαντά θετικά στον πάροχο υπηρεσιών, ώστε να επιτρέψει πρόσβαση στο χρήστη.



***Εικόνα 3: Αρχιτεκτονική συστημάτων ηλεκτρονικής ταυτοποίησης***

**3.3 Πλεονεκτήματα ηλεκτρονικής ταυτοποίησης**

Η τεχνολογία της ηλεκτρονικής ταυτοποίησης παρέχει ουσιαστικά οποιεσδήποτε πληροφορίες στο διαδίκτυο. Ο κάτοχος ηλεκτρονικής ταυτότητας έχει τη δυνατότητα, δηλαδή, να κάνει χρήση πολλών υπηρεσιών μετά από την επαλήθευση της ταυτότητάς του.

Επίσης, στην ηλεκτρονική ταυτοποίηση δεν είναι δυνατή η μη εξουσιοδοτημένη χρήση της ταυτότητας και των προσωπικών δεδομένων από άλλους χρήστες. Μέσω των μοναδικών διαπιστευτηρίων τους (συνήθως όνομα χρήστη και κωδικός πρόσβασης) οι πολίτες μπορούν να κάνουν χρήση μεγάλου φάσματος ηλεκτρονικών υπηρεσιών χωρίς να χρειάζεται πλέον να απομνημονεύουν πληροφορίες για τα διαπιστευτήριά τους.

Παράλληλα, οι κυβερνήσεις με τα συστήματα ηλεκτρονικής ταυτοποίησης επιτρέπουν στον πολίτη να υπογράφει ψηφιακά και να υποβάλλει έντυπα μέσω διαδικτύου στις δημόσιες υπηρεσίες χωρίς να είναι απαραίτητη η φυσική του παρουσία. Αυτό μειώνει τη γραφειοκρατία και οδηγεί στην ομοιόμορφη συγκέντρωση πληροφοριών. Η μειωμένη έως μηδαμινή γραφειοκρατία καθιστά τα συστήματα αυτά και φιλικά προς το περιβάλλον, καθώς έχουν σαν αποτέλεσμα περικοπές στη χρήση χαρτιού και μειωμένο κόστος χρόνου και ενέργειας για τη μεταφορά και τη χρήση του χαρτιού.

Τα εθνικά συστήματα ηλεκτρονικής ταυτοποίησης συμβάλλουν στην αντιμετώπιση κινδύνων για την ασφάλεια της ταυτότητας, όπως απάτη ταυτότητας ή κλοπή, αλλά και για την προστατευμένη χρήση ηλεκτρονικών εφαρμογών, όπως εφαρμογές υγειονομικής περίθαλψης, τραπεζικές υπηρεσίες κλπ. Παράλληλα, προσδίδουν στον πολίτη ευκολία και ευελιξία στις συναλλαγές του, αλλά και απόρρητο στα ευαίσθητα δεδομένα του.

Συνοπτικά, τα σημαντικότερα πλεονεκτήματα, που μπορεί να προσφέρει η ηλεκτρονική ταυτότητα είναι:

* ο αυτοπροσδιορισμός των πολιτών στο διαδίκτυο.
* η πρόσβαση σε δημόσια έγγραφα 24 ώρες το 24ωρο.
* η προστατευμένη ανταλλαγή πληροφοριών μέσα από ηλεκτρονικές υπηρεσίες.
* η εξοικονόμηση χρόνου, λόγω αυτόματης συμπλήρωσης ορισμένων πεδίων μετά την επαλήθευση της ταυτότητας, αλλά και λόγω της απουσίας ανάγκης για τη φυσική παρουσία του ατόμου στη δημόσια υπηρεσία.

**3.4 Μειονεκτήματα ηλεκτρονικής ταυτοποίησης**

Ένας όρος, που παίζει πολύ σημαντικό ρόλο στη ζωή των ανθρώπων, είναι η ιδιωτικότητα. Κάθε πολίτης θέλει να αισθάνεται ασφαλής και να μην είναι εκτεθειμένος σε οποιοδήποτε τομέα της ζωής του. Μια σύγχρονη άποψη του ορισμού δίνει ο Robert Ellis Smith, ορίζοντας την ιδιωτικότητα ως «την επιθυμία καθενός μας για ένα φυσικό χώρο στον οποίο είμαστε ελεύθεροι κάθε διακοπής, εισβολής, αμηχανίας ή υπευθυνότητας» καθώς και ως «την προσπάθεια να ελέγξουμε το χρόνο και τον τρόπο των κοινοποιήσεων προσωπικών πληροφοριών για τους εαυτούς μας».

Στα συστήματα ηλεκτρονικής ταυτοποίησης είναι μείζονος σημασίας η αποδοχή τους από τον πολίτη, ώστε να μην υπάρχει δυσκολία στην εφαρμογή τους. Η αποδοχή αυτή αφορά το κατά πόσο μπορεί να είναι πεπεισμένος ο χρήστης, ότι μπορεί να κάνει χρήση των ηλεκτρονικών υπηρεσιών χωρίς να παραβιάζεται η ιδιωτικότητά του. Για το λόγο αυτό, οι πολίτες έχουν τεχνολογικές απαιτήσεις, που αφορούν το υψηλό επίπεδο εμπιστοσύνης στη νέα αυτή τεχνολογία.

Δυστυχώς, πολύ συχνά παρατηρούνται στις μέρες μας πολλά περιστατικά εσφαλμένης διαχείρισης προσωπικών δεδομένων από εταιρείες, κρατικούς φορείς κλπ. Αυτός είναι ένας λόγος, για να αποτρέψει τους πολίτες από την αποδοχή της συγκεκριμένης τεχνολογίας.

Παράλληλα, όσο προχωρημένη και εξελιγμένη και να είναι μία τεχνολογία, δεν υπάρχει περίπτωση να μην έχει ορισμένα σφάλματα. Πιθανά, λοιπόν, κενά ασφάλειας στο σύστημα μπορούν να οδηγήσουν σε κλοπή ταυτότητας. Ένας κακόβουλος «κλέφτης» μπορεί να πραγματοποιήσει επιθέσεις στον τραπεζικό λογαριασμό του χρήστη, στα μηνύματα ηλεκτρονικού ταχυδρομείου του, στους κοινωνικούς λογαριασμούς του και σε πολλά ακόμη. Επιπρόσθετα, οι ηλεκτρονικές ταυτότητες είναι κατασκευασμένες με τέτοιο τρόπο, ώστε να έχουν πολλαπλές χρήσεις. Συνεπώς, η απώλειά τους απαιτεί μια πολυάριθμη σειρά από διορθωτικές ενέργειες.

Ένα τελευταίο, λιγότερο σημαντικό από τα παραπάνω, μειονέκτημα, αλλά άξιο αναφοράς είναι, ότι η ανάπτυξη συστήματος ηλεκτρονικής ταυτοποίησης έχει πολύ μεγάλο κόστος. Πέρα από το κόστος ανάπτυξης, υπάρχουν και επιπλέον δαπάνες έκδοσης καρτών, οργανωτικών εξόδων και εγγραφής χρηστών.

|  |
| --- |
| **Ενότητα 4: e-ID στην Ελλάδα** |

**4.1 Ηλεκτρονική διακυβέρνηση στην Ελλάδα**

Ο Οργανισμός Ηνωμένων Εθνών (Ο.Η.Ε.) στην τελευταία δημοσιευθείσα έκθεσή του για το βαθμό ανάπτυξης της ηλεκτρονικής διακυβέρνησης σε κάθε χώρα κατέταξε την Ελλάδα στην 43η θέση με τιμή ίση με 0.6910 (οι τιμές κυμαίνονται από 0 έως 1) παγκοσμίως.

Στην εικόνα 4 παρατηρείται το επίπεδο ανάπτυξης της ηλεκτρονικής διακυβέρνησης για τα μέλη της Ευρωπαϊκής Ένωσης. Η Ελλάδα ξεπερνά μόλις τα 7 από τα 28.



***Εικόνα 4: Δείκτης ανάπτυξης ηλεκτρονικής διακυβέρνησης για τα κράτη της Ε.Ε.***

Σύμφωνα με αντίστοιχες εκθέσεις του Ο.Η.Ε. από το 2010 και μετά η χώρα έχει πτωτική πορεία στην παγκόσμια κατάταξη με χαμηλότερη θέση την τελευταία. Σε έρευνα της Ελληνικής Στατιστικής Αρχής (2016) διαπιστώθηκε, ότι οι πολίτες χρησιμοποιούν ηλεκτρονικές υπηρεσίες κυρίως για λήψη πληροφοριών και σε δεύτερη φάση για αποστολή αιτήσεων σε δημόσιες υπηρεσίες κλπ. Μάλιστα, είναι άξιο αναφοράς ότι το 2017 παρατηρήθηκε μείωση της χρήσης ηλεκτρονικής διακυβέρνησης στη χώρα.

**4.2 Ηλεκτρονική ταυτοποίηση στην Ελλάδα**

Σε αυτή τη φάση δεν υπάρχει κάποια κεντρική υποδομή ηλεκτρονικής ταυτοποίησης των Ελλήνων πολιτών κατά τη χρήση ηλεκτρονικών υπηρεσιών. Παρ’ όλα αυτά, έχουν γίνει κάποια βήματα προς αυτή την κατεύθυνση με την απόδοση του ΑΜΚΑ σε κάθε πολίτη της χώρας. Σε δεύτερο στάδιο το 2010 εφαρμόστηκε ηλεκτρονικό πρόγραμμα γενικής συνταγογράφησης φαρμάκων των ασφαλισμένων στη χώρα.

Η πύλη του Taxisnet μπορεί να θεωρηθεί ως κεντρική δομή ταυτοποίησης, καθώς σταδιακά όλοι οι ιστότοποι, που παρέχουν ηλεκτρονικές υπηρεσίες επιτρέπουν τη σύνδεση του χρήστη σε αυτούς μέσω των κωδικών του από το Taxisnet. Οι περισσότεροι Έλληνες πολίτες υποχρεούνται να καταθέσουν φορολογική δήλωση. Επομένως διαθέτουν αντίστοιχους κωδικούς σύνδεσης. Για την αρχική πιστοποίηση του χρήστη στο Taxisnet απαιτείται η εγγραφή του στον ιστότοπο του Taxisnet και μετά η επίσκεψη σε κάποια ΔΟΥ για ταυτοποίηση και λήψη σχετικού κλειδαρίθμου ταυτοποίησης. Τέλος, χρειάζεται να δηλώσει τον κλειδάριθμο στο Taxisnet για επαλήθευση της ταυτότητάς του.

Ένα σύστημα ηλεκτρονικής ταυτοποίησης πολιτών στο δημόσιο τομέα είναι η εθνική κυβερνητική πύλη της χώρας ΕΡΜΗΣ, η οποία παρέχει ελεύθερη πρόσβαση στους πολίτες για άντληση πληροφοριών για τη δημόσια διοίκηση χωρίς να χρειάζεται ταυτοποίηση. Η ταυτοποίηση είναι απαραίτητη για την υλοποίηση συναλλαγών. Η είσοδος στην πύλη ΕΡΜΗΣ πραγματοποιείται είτε με χρήση ονόματος χρήστη και κωδικού πρόσβασης, είτε με χρήση των κωδικών του Taxisnet, αφού ο χρήστης πραγματοποιήσει τις ενέργειες, που αναφέρθηκαν παραπάνω.

Στην εικόνα 5 φαίνονται οι δύο επιλογές του χρήστη στην κυβερνητική πύλη ΕΡΜΗΣ.

****

***Εικόνα 5: Επιλογές ταυτοποίησης χρήστη στο ΕΡΜΗΣ***

Αντίστοιχα, στον ιστότοπο του ΙΚΑ η ταυτοποίηση των χρηστών μπορεί να γίνει και πάλι με χρήση των κωδικών του Taxisnet ή με λήψη κλειδαρίθμου μετά από επίσκεψη σε υποκατάστημα του ΙΚΑ (εικόνα6).





***Εικόνα 6: Τρόποι πιστοποίησης ασφαλισμένου στο ΙΚΑ***

**4.3 Προτάσεις για επιτυχή εφαρμογή ηλεκτρονικής ταυτοποίησης**

Είναι πολύ λογικό το γεγονός, ότι η τάση προς συστήματα ηλεκτρονικής ταυτοποίησης θα έχει αυξητική πορεία, αν υπάρχει δυνατότητα χρήσης των αντίστοιχων υπηρεσιών και μέσω κινητών τηλεφώνων εκτός των προσωπικών υπολογιστών. Μέχρι και σήμερα, παρατηρείται ότι οι περισσότεροι ιστότοποι στη χώρα μας παρουσιάζουν αδυναμία προσπέλασης μέσω κινητού τηλεφώνου. Μάλιστα, στην Ελλάδα η χρήση των κινητών συσκευών ολοένα και αυξάνεται. Θα ήταν ωφέλιμο, προκειμένου να επιτύχει η ηλεκτρονική διακυβέρνηση στη χώρα, να υπάρχει ευκολία στη χρήση των εφαρμοζόμενων μεθόδων ταυτοποίησης, να είναι δηλαδή οι ιστότοποι φιλικοί ως προς το χρήστη και μέσω κινητών τηλεφώνων, ώστε να αποδεχθεί τη χρήση τους.

Ένα ακόμη πολύ σοβαρό θέμα είναι, ότι υπάρχει ένα μεγάλο κομμάτι του πληθυσμού της Ελλάδας, που δεν κατέχει στοιχειώδεις γνώσεις χρήσης ηλεκτρονικών υπηρεσιών. Για να μπορέσει αυτό το σύστημα ηλεκτρονικής ταυτοποίησης να εφαρμοστεί στη χώρα, πρέπει να απαιτεί τις πολύ βασικές ψηφιακές δεξιότητες. Γι’ αυτό, θα πρέπει να αποφευχθούν απαιτήσεις τύπου εγκατάστασης επιπρόσθετων εφαρμογών ή ειδικών ρυθμίσεων στον υπολογιστή.

Τέλος, ίσως η σημαντικότερη πρόταση προς εφαρμογή είναι να υπάρχει στη διάθεση των πολιτών ηλεκτρονική ταυτότητα, η οποία θα έχει καθολική εφαρμογή (φυσική και ηλεκτρονική ταυτοποίηση). Η ταυτότητα αυτή θα πρέπει να εμπεριέχει: επίθετο, όνομα, ημερομηνία γέννησης, τόπο γέννησης, διεύθυνση, ημερομηνία λήξης, αναγνωριστικό κάρτας, ΑΜΚΑ και ΑΦΜ. Τα δύο τελευταία κρίνονται πολύ σημαντικά, ώστε να μπορεί ο πολίτης να διασυνδέεται εύκολα και άμεσα με ηλεκτρονικές υπηρεσίες υγειονομικής περίθαλψης, αλλά και φορολογικής ιδιότητας.

|  |
| --- |
| **Συμπεράσματα** |

Η δυνατότητα ηλεκτρονικής ταυτοποίησης αποτελεί σημαντικό προαπαιτούμενο για την ανάπτυξη της ηλεκτρονικής διακυβέρνησης. Σίγουρα συνεπάγεται πολλά οφέλη, αλλά και κινδύνους. Τοποθετώντας τα στη «ζυγαριά» τα οφέλη υπερτερούν. Οπότε αυτό, που μένει, είναι να πειστούν οι πολίτες, ότι πρόκειται για ένα άλμα προς την πρόοδο και να την αποδεχτούν.

Είναι πολλοί οι τομείς, που μπορεί να χρησιμοποιηθεί η ηλεκτρονική ταυτοποίηση, μερικοί από τους οποίους είναι:

* συμμετοχή σε ψηφοφορίες
* υπηρεσίες φορολόγησης
* άδειες οδήγησης
* κοινωνική ασφάλιση
* υγειονομική περίθαλψη
* εμπορικές συναλλαγές

Η ηλεκτρονική ταυτοποίηση αποτελεί έναν παράγοντα πρωταρχικής σημασίας για όλες σχεδόν τις εφαρμογές της ηλεκτρονικής διακυβέρνησης. Βέβαια, εξακολουθεί να αντιμετωπίζει ορισμένες προκλήσεις, που έχουν να κάνουν με την ασφάλεια, την προστασία προσωπικών δεδομένων και τη χρηστικότητα αντίστοιχων συστημάτων. Πολλά από αυτά τείνουν να καταπολεμηθούν και η τεχνολογία αυτή βρίσκεται σε ένα πολύ καλό στάδιο, σε συνδυασμό με την ευκολία και ευελιξία, που μπορεί να προσφέρει στον πολίτη.

Πιο γενικά, κάθε νέα εφαρμοζόμενη τεχνολογία χαρακτηρίζεται από πλεονεκτήματα και μειονεκτήματα. Είναι πολύ σημαντικό ο πολίτης να λειτουργεί, με σκοπό την πρόοδο και την εξέλιξη της χώρας, χωρίς αυτό να σημαίνει, ότι θα δέχεται οτιδήποτε καινούριο χωρίς αμφισβήτηση και επαρκή πληροφόρηση.

|  |
| --- |
| **Βιβλιογραφία** |

* Μπαχαριάδου Α., Φασιλάκη Ζ., Διπλωματική Εργασία: «Ηλεκτρονική Διακυβέρνηση και Εφαρμογές της Πληροφορικής στη Δημόσια Διοίκηση», ΤΕΙ Κρήτης
* Τεταγιώτης Μ., Διπλωματική Εργασία: «Κριτική επισκόπηση των τεχνολογιών ηλεκτρονικής ταυτοποίησης για συστήματα ηλεκτρονικής διακυβέρνησης», Πανεπιστήμιο Αιγαίου