ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
Τμήμα Μηχανικών Σχεδίασης Προϊόντων & Συστημάτων

ΘΕΜΑ ΕΡΓΑΣΙΑΣ:

«ΝΟΜΙΚΑ ΖΗΤΗΜΑΤΑ ΠΟΥ ΕΓΕΙΡΕΙ Η ΧΡΗΣΗ ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΕΘΟΔΩΝ ΨΗΦΟΦΟΡΙΑΣ ΣΤΙΣ ΠΟΛΙΤΙΚΕΣ ΕΚΛΟΓΕΣ».

ΕΚΠΟΝΗΘΗΚΕ ΑΠΟ ΤΟΝ

ΚΟΝΤΑΚΗ ΠΕΤΡΟ

ΠΕΡΙΕΧΟΜΕΝΑ

1. Πρόλογος

Η ενεργός ενσωμάτωση των Τεχνολογιών της Πληροφορίας και των Επικοινωνιών σε όλες τις διαστάσεις της καθημερινής μας ζωής αλλάζει ουσιωδώς την υφή των βασικών δομών και δημιουργεί μία νέα μορφή κοινωνικής, πολιτικής και οικονομικής πραγματικότητας, αποκαλούμενη ως «Κοινωνία της Πληροφορίας» . Βαθμιαία γεννάται μία νέα «Ηλεκτρονική Δημόσια Διοίκηση» (e-Government), η οποία βασίζεται όλο και περισσότερο στη χρήση των τεχνολογιών αυτών, τόσο για την υλοποίηση των εσωτερικών λειτουργιών της όσο και για την επικοινωνία και συναλλαγή της με τους πολίτες και τις επιχειρήσεις. Έτσι, νέα λειτουργικά μοντέλα όπως η «Ηλεκτρονική Διακυβέρνηση» (e-Governance) χαρακτηρίζονται από υψηλότερη αποτελεσματικότητα όσο αφορά την αντιμετώπιση κοινωνικών προβλημάτων και την κάλυψη των αναγκών των πολιτών.

Η «Ηλεκτρονική Διακυβέρνηση» είναι ένα διεπιστημονικό αντικείμενο πολλών επιμέρους γνωστικών περιοχών, εκ των οποίων μία είναι η Ηλεκτρονική Ψηφοφορία (e-Vote) εκλογών, η οποία αφορά το σύνολο των πολιτών με απώτερο σκοπό να περιοριστεί το «ψηφιακό χάσμα».

Η ηλεκτρονική ψηφοφορία εκλογών έχει ήδη εφαρμοστεί παγκοσμίως και αποσκοπεί να γίνει το κύριο εργαλείο για πανεπιστημιακές, δημοτικές, συνδικαλιστικές, εθνικές, ακόμη και ευρωπαϊκές εκλογές. Χρησιμοποιείται από αρκετές χώρες για τη διενέργεια τόσο των εθνικών και δημοτικών εκλογών όσο και για δημοψιφίσματα και διαδικασίες απογραφής (e-census). Συγκεκριμένα, στη Βραζιλία πρωτοεμφανίστηκε η ηλεκτρονική ψηφοφορία στις δημοτικές εκλογές του 1996 και στην Ινδία υλοποιήθηκε τον Απρίλιο του 2004, αφού το 2003 είχε προηγηθεί ένα πιλοτικό σύστημα. Στο Βέλγιο εφαρμόσθηκε το 1999 ενώ είχε ψηφιστεί νόμος το 1994, στην Ιταλία το Φεβρουάριο του 2004 ανακοινώθηκε η πραγματοποίηση πειραματικού προγράμματος για το Ευρωπαϊκό Κοινοβούλιο. Στην Αγγλία τριάντα τοπικές κυβερνήσεις δοκίμασαν πολλές διαφορετικές εφαρμογές ψηφοφορίας και καταμέτρησης ψήφων, καθώς επίσης στη Γαλλία συνεχίζουν να λαμβάνουν χώρα πειραματικά σχέδια από το 1994 χωρίς την ύπαρξη αυξημένου ενδιαφέροντος για την υιοθέτηση της ηλεκτρονικής ψηφοφορίας, όπως το ίδιο συμβαίνει και σε χώρες όπως Ισπανία και Ιαπωνία.[1]

Τα οφέλη ενός τέτοιου προγράμματος είναι τόσο οικονομικά όσο και κοινωνικά, ενώ το σύστημα αποσκοπεί σε μία τεχνικά άρτια και νομικά συμβατή εφαρμογή, η οποία θα λειτουργήσει συμπληρωματικά, αρκεί βέβαια να ληφθούν πολύ σοβαρά υπόψιν, από τις αρμόδιες αρχές, οι απειλές και οι κίνδυνοι που μπορεί να προκληθούν με αποτέλεσμα τραγικές κοινωνικές, τεχνολογικές αλλά και νομικές επιπτώσεις.

Σκοπός της παρούσης εργασίας είναι η παρουσίαση των μεθόδων ηλεκτρονικής ψηφοφορίας, των τεχνολογικών και νομικών προβλημάτων και των μορφών επιθέσεων και απειλών της, προτείνοντας συγκεκριμένες προδιαγραφές που πρέπει να πληροί ένα τέτοιο σύστημα ώστε να λειτουργεί άρτια και με ασφάλεια τόσο για την διεκπεραίωση των εκλογικών διαδικασιών όσο και για τον ίδιο ψηφοφόρο-πολίτη. Τέλος, αναλύονται οι προδιαγραφές από διεθνείς οργανισμούς πιστοποίησης και πως αυτές συνδέονται με τις προτάσεις που τίθενται στην ενότητα 5.

2. Μέθοδοι ηλεκτρονικής ψηφοφορίας

Η ηλεκτρονική ψηφοφορία (e-voting) επιτρέπει την ψήφο από απόσταση με τη χρήση ηλεκτρονικών μεθόδων. Απλοποιείται έτσι και διευκολύνεται η συμμετοχή των πολιτών στις εκλογικές διαδικασίες δημιουργώντας προσδοκίες για αυξημένη συμμετοχή σε αυτές. Ο παραπάνω όρος συμπεριλαμβάνει μια μεγάλη κλίμακα επιμέρους μορφών και διαδικασιών που αφορούν στην οργάνωση και διεξαγωγή μιας εκλογικής διαδικασίας. [2]

Μία βασική μορφή της ηλεκτρονικής ψηφοφορίας είναι η χρήση ηλεκτρονικών μηχανημάτων για την απλοποίηση της διαδικασίας καταμέτρησης ψήφων. Τα μηχανήματα αυτά τοποθετούνται κυρίως εντός του εκλογικού κέντρου ή σε ειδικά διαμορφωμένους χώρους που βρίσκονται σε κεντρικά σημεία των εκλογικών περιφερειών. Τα πλέον διαδεδομένα συστήματα ηλεκτρονικής καταμέτρησης ψήφων είναι τα συστήματα δίατρησης καρτών (punch card systems) και τα συστήματα οπτικής σάρωσης (optical scanning systems).

Πέραν των μηχανημάτων ηλεκτρονικής καταμέτρησης ψήφων υπάρχουν και τα μηχανήματα *ηλεκτρονικής ψηφοφορίας*, γνωστά και ως μηχανήματα αυτόματης εγγραφής (Direct Recording Electronic machines-DREs). Ο εκλογέας χρησιμοποιώντας απευθείας την οθόνη του μηχανήματος ενεργοποιεί τη ψήφο του μειώνοντας σημαντικά το χρόνο και το κόστος τόσο της διαδικασίας ψηφοφορίας (όπως μεταφορά σε εκλογικά κέντρα) όσο και της καταμέτρησης των ψήφων, ενώ αυξάνει τη συμμετοχή από άτομα με αναπηρίες.

Η ηλεκτρονική ψηφοφορία είναι ένας νέος τρόπος ψηφοφορίας και ο λόγος για τον οποίο έχουν αναπτυχθεί ποικίλες μορφές της ανάλογα με το κοινωνικό, οικονομικό και πολιτισμικό πλαίσιο στο οποίο αυτή εφαρμόζεται. Δύο βασικοί τύποι της είναι:

i. Ηλεκτρονική ψηφοφορία σε *Εκλογικά Σημεία (Polling Place E-Voting)*
   Η ψηφοφορία λαμβάνει χώρα σε εκλογικά κέντρα υπό την εποπτεία των αρμόδιων διοικητικών αρχών, οι οποίες έχουν την ευθύνη για τον έλεγχο της καλής λειτουργίας του υλικού και λογισμικού του υπολογιστικού συστήματος και την εποπτεία του περιβάλλοντος χώρου, αλλά όχι του χώρου όπου πραγματοποιείται η εκλογική διαδικασία, όπως μικρά κιόσκια ψηφοφορίας.

ii. Ηλεκτρονική ψηφοφορία μέσω *Διαδικτύου (Internet Voting)*
   Εντάσσεται στην από απόσταση ψηφοφορία (Remote e-Voting) και αναφέρεται στην διαδικασία αποστολής ψήφου από οποιονδήποτε ιδιωτικό χώρο συνδεδεμένο στο ίντερνετ. Τα κυριότερα μέσα και μηχανήματα που χρησιμοποιούνται στην περίπτωση αυτή είναι η κινητή τηλεφωνία (αποστολή μηνυμάτων – SMS ή online αποστολή από ηλεκτρονικό ιστότοπο), η ψηφιακή διαδραστική τηλεόραση (Interactive digital Television), εφαρμογή την οποία παρέχουν οι νέοι τύποι τηλεόρασης, καθώς και οι προσωπικοί υπολογιστές, οι οποίοι αποτελούν το πιο σύνηθες ευρέως μέσο της υποβολής ηλεκτρονικής ψήφου συνδεδεμένο στο internet.

iii. Θάλαμοι ψηφοφορίας (Kiosk Voting)

Στο γενικό ηλεκτρονικό πλαίσιο, οι θάλαμοι ψηφοφορίας σημαίνουν τη χρήση μηχανών ψηφοφορίας σε εκλογικούς σταθμούς ή σε άλλες ελεγχόμενες τοποθεσίες. Οι ψηφοφόροι αποτυπώνουν την επιλογή τους ηλεκτρονικά αντί των χάρτινων ψηφοδελτίων. Οι ψήφοι καταμετρούνται σε ατομικές μηχανές και τέλος μεταφέρονται στο κεντρικό σύστημα. Ένα ψηφοδέλτιο μπορεί να εκτυπώνεται και να παραμένει στο κουτί ψηφοδελτίων σαν επιπρόσθετη απόδειξη. [3]

Στο σημείο αυτό χρειάζεται να διευκρινιστεί ότι τα στάδια, στα οποία βασίζονται οι προαναφερθείσες μέθοδοι ηλεκτρονικής ψηφοφορίας, είναι κοινά. Συγκεκριμένα, προηγείται η *Εγγραφή (Registration)*, η υποβολή δηλαδή στοιχείων που αποδεικνύουν ότι το συγκεκριμένο άτομο έχει δικαίωμα ψήφου, και μετέπειτα την καταχώρησή του στους εκλογικούς καταλόγους. *Η Επικύρωση (Identification)* βάσει της οποίας γίνεται η ταυτοποίηση του ψηφοφόρου, ζήτημα το οποίο θίγει τη νομική πολυπλοκότητα του συστήματος όπως αναλύεται παρακάτω (ενότητα 3.2). Έπεται η *Υποβολή ψήφου (Ballot Casting)* στην οποία οι ψηφοφόροι υποβάλλουν τη ψήφο τους και τέλος, η *Καταμέτρηση ψήφων (Tallying).* Σημαντικό είναι τα δύο τελευταία στάδια, Υποβολή και Καταμέτρηση ψήφων, να έπονται από την αρχή μυστικότητας δηλαδή το απόρρητο της επιλογής του κάθε ψηφοφόρου.

3. Ανάλυση τεχνικών και νομικών προβλημάτων

Η ενεργός ενσωμάτωση των Τεχνολογιών της Πληροφορίας και των Επικοινωνιών σε όλες τις διαστάσεις της καθημερινής μας ζωής αλλάζει ουσιωδώς την υφή βασικών δομών και δημιουργεί μια νέα μορφή κοινωνικής, πολιτικής και οικονομικής πραγματικότητας, αποκαλούμενη «Κοινωνία της Πληροφορίας» (Information Society).

Τα συστημικά μοντέλα που προκύπτουν από την υιοθέτηση της τεχνολογίας χαρακτηρίζονται από υψηλότερη αποτελεσματικότητα όσο αφορά την αντιμετώπιση των κοινωνικών προβλημάτων και την κάλυψη των αναγκών των πολιτών. Δεν παύει, όμως, να υποβόσκουν κίνδυνοι, οι οποίοι αφορούν τόσο τεχνικά αλλά και νομικά ζητήματα που επιτάσσουν ιδιαίτερη προσοχή προκειμένου να αποφευχθεί η κατάρρευση του συστήματος Ηλεκτρονικής Δημοκρατίας και η ολοκληρωτική έλλειψη εμπιστοσύνης των πολιτών. Παρακάτω ακολουθεί ανάλυση των περισσότερο σημαντικών προβλημάτων που εγείρει η ηλεκτρονική ψηφοφορία εκλογών, καθώς και τρόποι αντιμετώπισής τους από τους αρμόδιους φορείς (ανάλυση στην ενότητα 5).

3.1 Τεχνικά προβλήματα

- ✓ ***Ασφάλεια προσωπικών δεδομένων***

  Μεγάλες ποσότητες προσωπικών δεδομένων που χρησιμοποιούνται από τους ψηφοφόρους για να επικυρώσουν τους εαυτούς τους στη φάση της καταχώρησης μπορούν να αποκαλυφθούν. Πληροφορίες μπορούν να χρησιμοποιηθούν για να συνδεθούν οι ψηφοφόροι με τις ψήφους και να υπονομευθεί η ανωνυμία.

- ✓ ***Αντοχή μηχανογραφικού συστήματος στο αυξημένο φόρτο εργασίας την ημέρα των εκλογών.***

  Ένα ενδεχόμενο κύμα ψηφοφόρων, είτε τις πρώτες ώρες της ψηφοφορίας, πολλοί είναι αυτοί που θέλουν να είναι οι πρώτοι που ψηφίζουν online, είτε λίγο πριν κλείσουν οι ηλεκτρονικές κάλπες καθιστά εξαιρετικά πιθανή την κατάρρευση του συστήματος και πρέπει να έχουν προβλεφθεί εκ των προτέρων σχετικά μέτρα αντιμετώπισης.

- ✓ ***Κακόβουλα προγράμματα "malware"***

  Υπάρχει πάντα ο κίνδυνος εισχώρησης ενός κακόβουλου προγράμματος στον server πριν ή κατά τη διάρκεια των εκλογών, μέσω ηλεκτρονικού ταχυδρομείου ή εξωτερικού συνδέσμου επικοινωνίας. Επιπλέον, ο τεράστιος αριθμός Ηλεκτρονικών Υπολογιστών (Η/Υ) που επικοινωνούν με το σύστημα μπορεί να αυξήσει τη πιθανότητα κινδύνου ενός κακόβουλου προγράμματος. Αυτό μπορεί να προκαλέσει ζημιά στο server και πιθανότατα να πολλαπλασιαστεί και σε άλλους Η/Υ. Η κυβέρνηση πρέπει να είναι προετοιμασμένη για οποιαδήποτε ζημιά. Εάν, για παράδειγμα ένα πρόγραμμα τύπου "Δούρειος Ίππος" εγκατασταθεί στο σύστημα, η εμπιστευτικότητα και η ακεραιότητα των ψήφων επηρεάζεται αρνητικά και μπορεί να ακυρωθεί η διαδικασία. Είναι πιθανό για έναν εισβολέα να εγκαταστήσει κακόβουλο πρόγραμμα που να παραμένει ανενεργό μέχρι τη στιγμή της εκλογής. Ένα πρόγραμμα όπως ο "Δούρειος Ίππος" είναι ικανό να μεταβιβάσει πληροφορίες σε τρίτους για τον τρόπο με τον οποίο ένα άτομο ψήφισε ή ακόμα και να αλλάξει τη ψήφο του. Άλλου τύπου κακόβουλα προγράμματα είναι τα λεγόμενα «Σκουλήκια» (worms) που αναπαράγουν τον εαυτό τους εσωτερικά σε έναν υπολογιστή ή ακόμα και σε άλλους μέσω δικτύου. Τα προγράμματα αυτά εκμεταλλεύονται λάθη του συστήματος και μετά από κάποιο χρονικό διάστημα το κατακλύζουν ώστε να μην μπορεί να λειτουργήσει.

- ✓ ***Πρόβλημα υπηρεσίας***

  Με τη συνεχή και ταυτόχρονη χρήση του συστήματος ίσως δημιουργηθεί πρόβλημα και η εφαρμογή παραμείνει προσωρινά μη διαθέσιμη. Μια κακόβουλη επίθεση ή μια μαζική ακούσια κακή χρήση μπορεί να καταστήσει το σύστημα μη διαθέσιμο, είτε προσωρινά, είτε κατά τη διάρκεια της εκλογής.

- ✓ ***Επιθέσεις στο Domain Name System (DNS)***

  Υπάρχει πάντα η πιθανότητα ένας επιτιθέμενος να αλλάξει μια εγγραφή στο DNS. Αυτό θα επέτρεπε στον κάτοχο του ψεύτικου site να υπονομεύσει τη ψηφοφορία του επαναπροσανατολιζόμενου ψηφοφόρου. Το ίδιο αποτέλεσμα μπορεί να επιτευχθεί από τον επιτιθέμενο αν εγκαταστήσει ένα πρόγραμμα που θα λέει στον browser να χρησιμοποιεί μια ιστοσελίδα, ουσιαστικά κάνοντας μια, όπως αποκαλείται, επίθεση πλαστοπροσωπείας (man in the middle). [4]

3.2 Νομικά προβλήματα

Η ασφάλεια Προσωπικών και Ευαίσθητων Δεδομένων είναι ο όρος που χρησιμοποιείται για τα δεδομένα προσωπικού χαρακτήρα σύμφωνα με τους ορισμούς της οδηγίας 95/46/ΕΚ και αναφέρεται σε οποιεσδήποτε πληροφορίες αφορούν ένα προσδιορισμένο ή προσδιορίσιμο φυσικό πρόσωπο. [5] Ένα πρόσωπο, δηλαδή, το οποίο μπορεί να προσδιοριστεί σε σχέση με τον αριθμό ταυτοποίησής του ή στοιχεία που αφορούν τη φυσική, φυσιολογική, διανοητική, οικονομική, πολιτιστική ή κοινωνική ταυτότητά του.

Οι πιο σημαντικές σχετικές νομοθετικές παρεμβάσεις στην Ελλάδα αναφέρονται: α)Ν.2472/97 *«για την προστασία του ατόμου έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα»* και γίνεται υπό την εποπτεία της Αρχής Προστασίας Προσωπικών Δεδομένων και β) ΠΔ 150/2001 για τη χρήση των *«Ψηφιακών Υπογραφών» (Digital Signatures).* [6]

Όσον αφορά τα ζητήματα που εγείρει η ηλεκτρονική ψηφοφορία στις εκλογές και βάσει του ισχύοντος ελληνικού Συντάγματος (άρθρο 51 παρ. 3-5) τίθενται οι έξης νομοθετικές αρχές [7]:

<u>Καθολικότητα</u>
Πρόκειται για την ενσυνείδητη εκ μέρους της Πολιτείας ελαχιστοποίηση των προσόντων που απαιτούνται ώστε να μπορεί ένα πρόσωπο να συμμετάσχει ως ψηφοφόρος σε εκλογές. Η καθολικότητα είναι ένα από τα ζητήματα που θίγει η ηλεκτρονική ψηφοφορία καθώς απαιτεί ειδικές γνώσεις και δεξιότητες από τα άτομα που πρόκειται να ψηφίσουν ηλεκτρονικά. Έτσι προκύπτει το λεγόμενο «ψηφιακό χάσμα», δηλαδή τον διαχωρισμό μεταξύ των καταρτισμένων σε γνώση ατόμων της τεχνολογίας που απαιτεί η εν λόγω ψηφοφορία από τα μη καταρτισμένα άτομα, το οποίο σε πρώτο τουλάχιστον στάδιο της εφαρμογής θα επιτείνει την διάκριση αυτών.

<u>Αμεσότητα</u>
Είναι η μη παρεμβολή ενδιάμεσης βούλησης ή οργάνου ανάμεσα στην έκφραση της επιλογής του ψηφοφόρου και στην αποτύπωσή της στο εκλογικό αποτέλεσμα.
Η αμεσότητα προσκρούει τόσο τη δυνατότητα των χειριστών του συστήματος να αλλοιώσουν το περιεχόμενο της δοθείσας ψήφου όσο και ατόμων που δεν έχουν πρόσβαση στο σύστημα να επηρεάσουν τα αποτελέσματα της ψηφοφορίας. Είναι γεγονός ότι παρά την υψηλή προστασία δεδομένων που επικαλούνται κάποιοι ηλεκτρονικοί φορείς τα δεδομένα, και στην προκειμένη περίπτωση οι ψήφοι, δεν παραμένουν αδιάβλητοι καθότι υπάρχουν οι λεγόμενοι «υποκλοπείς» οι οποίοι μέσω των προηγμένων τεχνολογικών γνώσεων έχουν τη δυνατότητα να αλλοιώσουν τα αποτελέσματα των εκλογών προς όφελος κάποιου κόμματος. Έτσι, θίγεται η αρχή της ακεραιότητας, της εξασφάλισης δηλαδή ότι τα στοιχεία δεν μπορούν να μεταβληθούν ή να διαγραφούν από αναρμόδια άτομα.

<u>Εμπιστευτικότητα</u>
Είναι η εξασφάλιση μη γνωστοποίησης του περιεχομένου της ψήφου σε άλλο πρόσωπο εκτός του ψηφίζοντος. Η αρχή της εμπιστευτικότητας κινδυνεύει με δύο τουλάχιστον τρόπους: λόγω της πιθανής ύπαρξης άλλου προσώπου που να βλέπει, ακόμα και να

επηρεάζει, την ψήφο τη στιγμή που αυτή δίδεται από τον ψηφοφόρο και λόγω της πιθανής αντιστοίχησης της δοθείσας ψήφου με συγκεκριμένο ψηφοφόρο από χειριστή του συστήματος. Το πρώτο πρόβλημα μπορεί να λυθεί μόνο με αποκλεισμό της δυνατότητας να ψηφίζει κανείς σε οποιονδήποτε χώρο, αλλά τη διεξαγωγή της ψηφοφορίας μόνο σε ειδικά εξοπλισμένα δημόσια «καταστήματα», κάτι που αμέσως εξαλείφει σε μεγάλο βαθμό το πλεονέκτημα της απόλυτης προσβασιμότητας και της απλούστευσης της διαδικασίας. Το δεύτερο μπορεί να αντιμετωπισθεί με τεχνικούς τρόπους, όμως όπως έχει προαναφερθεί η εξασφάλιση δεν θα είναι ποτέ απόλυτη και το κοινωνικό σώμα δύσκολα θα πεισθεί ότι θα είναι ικανοποιητική.

Ταυτόχρονη διεξαγωγή

Η νομική αυτή αρχή που θίγεται σημαίνει ότι η έκφραση της ατομικής εκλογικής προτίμησης διατυπώνεται χωρίς να υπάρχει δυνατότητα γνώσης άλλων αποτελεσμάτων στην ίδια. Πιο συγκεκριμένα, το ταυτόχρονο εκ των πραγμάτων παραβιάζεται εάν η καταμέτρηση των ηλεκτρονικών ψήφων γίνει σε ύστερο από της «κλασικής» ψηφοφορίας χρόνο, ενώ υπάρχει πάντα και ο κίνδυνος ο χειριστής του συστήματος να ψηφίσει γνωρίζοντας τα αποτελέσματα της εκάστοτε κάλπης που επιβλέπει.

Ταυτοποίηση (Αυθεντικότητα ή Επικύρωση)

Πρόκειται για τη διασφάλιση ότι αυτός που ψηφίζει είναι πράγματι αυτός που λέει ότι είναι, ότι δικαιούται να ψηφίσει και ότι ψηφίζει μόνο μία φορά σε κάθε εκλογή. Η ψηφοφορία είναι πράξη ατομική, τόσο από ψυχική άποψη (εδώ τίθεται το ζήτημα του επηρεασμού), όσο και από φυσική καθότι το ελληνικό, τουλάχιστον, σύστημα δικαίου δεν δέχεται την ψήφο δια αντιπροσώπου. Η δυνατότητα συντέλεσης της ηλεκτρονικής ψηφοφορίας σε ιδιωτικούς και πάντως «μη ελέγξιμους» χώρους εγείρει από αυτή την άποψη προβληματισμό, θεωρείται, ωστόσο, από καθαρά τεχνική άποψη, ότι αυτή η σειρά των ζητημάτων είναι τα πιο εύκολα επιλύσιμα.

Υπευθυνότητα

Όταν οι ενέργειες ενός προσώπου-χρήστη, ειδικά οι τροποποιήσεις που εκτελεί στα στοιχεία που αποθηκεύονται, μπορούν να εντοπιστούν ή και να επισημανθούν (auditing files) κάτι που ορίζει το πρόσωπο αυτό πλήρως υπεύθυνο.

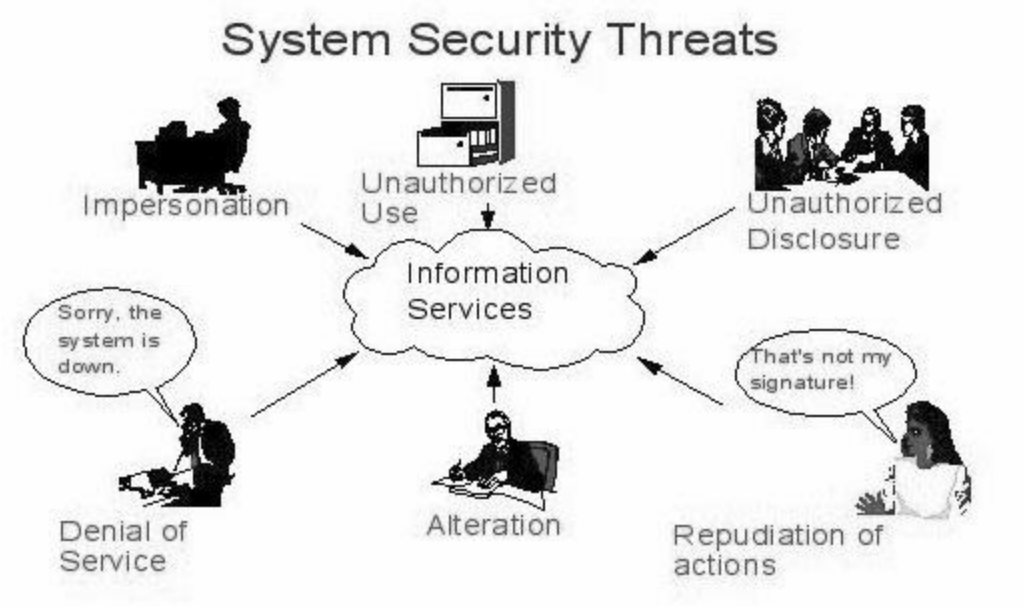
Το Σύνταγμα έχει χρέος να προσαρμόζεται στην πραγματικότητα και όχι η πραγματικότητα να διαμορφώνεται βάσει των ισχυουσών νομικών αρχών, ακόμα και αν αυτές διαθέτουν συνταγματικό κύρος, ανεξαρτήτως των τεχνικών λεπτομερειών του συστήματος που θα επιλεγεί και τους ακριβείς όρους υπό τους οποίους θα διεξαχθεί η ψηφοφορία.

Επιπλέον, χρειάζεται να τονισθεί η διαφορετικότητα των νομοθετικών κανόνων ψηφοφορίας που διέπει κάθε χώρα, γεγονός που επιβάλλει την προσαρμοστικότητα του συστήματος e-Vote (Ηλεκτρονική Ψηφοφορία). Για να εφαρμοστεί η ηλεκτρονική ψηφοφορία σε εθνικές ή δημοτικές εκλογές θα πρέπει είτε να το επιτρέπει η νομοθεσία του κράτους ή να θεσπιστεί το κατάλληλο νομοθετικό πλαίσιο.

4. Μέθοδοι Επιθέσεων και Απειλές στα Συστήματα Ηλεκτρονικής Ψηφοφορίας

Λόγω της ραγδαίας ανάπτυξης των τεχνολογιών υπολογιστών και των εξελίξεων στην κρυπτογραφία παρουσιάζεται η ηλεκτρονική ψηφοφορία ως εφαρμόσιμη εναλλακτική από τη μια, από την άλλη όμως οι υψηλές απαιτήσεις ασφαλείας εξακολουθούν να την καθιστούν ένα από τα μεγαλύτερα προβλήματα προς επίλυση, κάτι που απαιτεί τη συνεργασία ειδικών σε διάφορους τομείς, όπως λογισμικό, κρυπτογραφία, πολιτική, νομικές, οικονομικές και πολιτικές επιστήμες [8] [9].

Τα απομακρυσμένα ηλεκτρονικά συστήματα ψηφοφορίας καταργούν τα γεωγραφικά εμπόδια και τα παραδοσιακά συστήματα εκλογών. Το σύστημα ψηφοφορίας δεν είναι πλέον περιορισμένο στον τοπικό σταθμό ψηφοφορίας, Είναι προσβάσιμο παγκοσμίως, αυξάνοντας δραματικά το πιθανό αριθμό επιθέσεων. Από την ίδια τη φύση της, η διαδικασία της εκλογής είναι ένας ελκυστικός στόχος για κακόβουλες ενέργειες καθώς οι κακόβουλοι χρήστες ποικίλουν από ερασιτέχνες μέχρι βιομηχανικούς κατασκόπους ακόμη και Κυβερνήσεις.



Εικόνα 1: Απειλές συστημάτων Ηλεκτρονικής Ψηφοφορίας [10]

Οι πηγές επιθέσεων χωρίζονται σε εσωτερικές και σε εξωτερικές. Συγκεκριμένα [11]:

i) Εσωτερικές

Οι ***νόμιμοι χρήστες*** των απομακρυσμένων ηλεκτρονικών συστημάτων ψηφοφορίας ίσως επιδιώξουν την κακή χρήση ή ζημιά στο εκλογικό σύστημα και με τις ανάλογες τεχνικές τους ικανότητες να υπονομεύσουν το σύστημα. Στην περίπτωση όμως που η επίθεση επικεντρώνεται σε αυτούς υπόκεινται και στις αντίστοιχες νομικές κυρώσεις.

Οι ***διαχειριστές*** του συστήματος ηλεκτρονικής ψηφοφορίας μπορούν να συγκεντρώσουν πληροφορίες ιδιοτελώς από κυβερνητικούς υπαλλήλους, υπαλλήλους οργανισμών αλλά και εξωτερικούς υπαλλήλους όσον αφορά τα δικαιώματα προσβασιμότητας. Κίνητρο των

διαχειριστών υπηρεσιών της διαδικασίας αυτής θεωρείται το οικονομικό κέρδος είτε για προσωπικό όφελος είτε για πολιτικούς σκοπούς. Οι αναφερθέντες υπόκεινται εξίσου εύκολα σε κυρώσεις αν η επίθεση επικεντρώνεται σε αυτούς.

Οι ***υπόλοιποι*** κάτοχοι μυστικών πληροφοριών που έχουν πρόσβαση στο απομακρυσμένο σύστημα ηλεκτρονικής πληροφορίας, όπως κυβερνητικοί υπάλληλοι, αλλά δεν συσχετίζονται με τη φροντίδα των εκλογικών υπηρεσιών είναι πιθανόν να καθοδηγήσουν εσωτερικές επιθέσεις.

ii) Εξωτερικές

Οι αποκαλούμενοι ***"Hackers"***, οι εγκληματικοί οργανισμοί, οι ομάδες διαμαρτυρίας ή οι ακτιβιστές αποτελούν ομάδες ανθρώπων που αντιλαμβάνονται ως πρόκληση την επίθεση στο κυβερνητικό σύστημα μέσω της ηλεκτρονικής ψηφοφορίας. Σκοπός της κακόβουλης ενέργειας αυτής είναι ο προσωπικός φθόνος, η έντονη επιθυμία τους να διαμαρτυρηθούν στην κυβέρνηση, η εκμετάλλευση των εκλογικών πληροφοριών, η τροποποίηση των ηλεκτρονικών ψήφων και γενικότερα η φθορά του εκλογικού συστήματος.

Εξωτερική πηγή επίθεσης θεωρείται επίσης και η ***ομάδα ερευνητών ή δημοσιογράφων*** καθότι ενδιαφέρονται να υπονομεύσουν το σύστημα απομακρυσμένης ηλεκτρονικής ψηφοφορίας εκλογών ώστε σκόπιμα να αποδείξουν ότι πίσω από την καινοτομία αυτή κρύβονται προβλήματα ασφάλειας.

Επιπλέον, οι ***τρομοκρατικές οργανώσεις*** ενδιαφέρονται για τη συλλογή προσωπικών πληροφοριών μέσω της απομακρυσμένης παρακολούθησης των αποτελεσμάτων της ψηφοφορίας. Σκοπός τους είναι γνωρίζοντας τις εκλογικές προθέσεις να μπορούν να επηρεάσουν το αποτέλεσμα ή ακόμα και να διακόψουν τη διαδικασία.

5. Προτάσεις για προδιαγραφές που πρέπει να πληροί η ηλεκτρονική ψηφοφορία

Η εγγενής αδυναμία του Internet, καθότι πρόκειται για ένα πλήρως «ανοικτό» δίκτυο, ευρέως προσβάσιμο και εκ φύσεως «μη ασφαλές», αποτέλεσε βασικό ανασταλτικό παράγοντα για την εξάπλωση τόσο των ηλεκτρονικών συναλλαγών με τη Δημόσια Διοίκηση [12] όσο και των διαδικασιών Ηλεκτρονικής Ψηφοφορίας που προκύπτουν από την αποκαλούμενη «Ηλεκτρονική Διακυβέρνηση». Συνεπώς είναι απαραίτητη η χρήση των κατάλληλων τεχνολογιών για την ικανοποίηση των τεσσάρων βασικών απαιτήσεων, οι οποίες αναλύονται παρακάτω, και για την επίτευξη ασφαλών ηλεκτρονικών συναλλαγών μέσω Διαδικτύου. Οι τεχνολογίες αυτές όπως είναι η *κρυπτογραφία, η Ψηφιακή Υπογραφή, τα Ψηφιακά Πιστοποιητικά και οι Έξυπνες Κάρτες* παρουσιάζονται αναλυτικά στις υποενότητες *5.1, 5.2, 5.3 και 5.4* αντίστοιχα.

Οι τέσσερις βασικές λοιπόν απαιτήσεις ασφάλειας που εξασφαλίζουν την εγκυρότητα της ηλεκτρονικής ψηφοφορίας των εκλογών είναι:

a) Εμπιστευτικότητα (Confidentiality)
Ο αποδέκτης είναι ο μόνος που πρέπει να μπορεί να διαβάσει το μήνυμα που του αποστέλλει ο αποστολέας και κανένας άλλος. Εάν η απαίτηση αυτή δεν ικανοποιείται, τότε δημιουργείται ο κίνδυνος διαρροής των προσωπικών δεδομένων και τα προβλήματα που έπονται είναι αλυσιδωτά.

b) Ακεραιότητα (Integrity)
Το μήνυμα που αποστέλλει ο αποστολέας πρέπει να ταυτίζεται πλήρως με το μήνυμα που λαμβάνει ο αποδέκτης και να μην είναι δυνατόν να γίνουν αλλαγές, σκόπιμες ή μη, στο μήνυμα αυτό από κανέναν. Εάν η απαίτηση αυτή δεν ικανοποιείται, τότε δημιουργείται ο κίνδυνος οι ενέργειες του αποδέκτη να διαφέρουν από τα αντίστοιχα αιτήματα του αποστολέα, καθώς επίσης και να επιβληθούν άδικα κυρώσεις από τον αποδέκτη στον αποστολέα για «αναληθείς δηλώσεις», με τελικό αποτέλεσμα διενέξεις, δικαστικούς αγώνες και άλλα.

c) Αυθεντικότητα (Authentication)
Ο αποδέκτης ενός μηνύματος πρέπει να είναι σίγουρος ότι ο αποστολέας του είναι πράγματι ο αναγραφόμενος, και όχι κάποιος που τον «υποδύεται» ηλεκτρονικά. Εάν η απαίτηση αυτή δεν ικανοποιείται, τότε δημιουργείται κίνδυνος να μην είμαστε σίγουροι με ποιον συναλλασσόμαστε ηλεκτρονικά, με όλες τις αρνητικές συνέπειες που προκύπτουν από αυτήν την αβεβαιότητα.

d) Μη αποποίηση (Non-Repudiation)
Πρέπει ο ψηφοφόρος να μην μπορεί να αρνηθεί ότι απέστειλε τη συγκεκριμένη ψήφο ηλεκτρονικά, καθώς επίσης και ο παραλήπτης να μην μπορεί να αρνηθεί ότι την παρέλαβε.

5.1 Κρυπτογραφία

Όταν εξετάζουμε συστήματα ασφαλείας ηλεκτρονικής ψηφοφορίας αναφερόμαστε σε πρωτόκολλα και λογισμικά που σχετίζονται με κρυπτογραφικούς αλγορίθμους και με τη διαφάνεια του κώδικα αυτών προκειμένου να προστατευθεί κατά το μέγιστο δυνατό η

διαδικασία υποβολής ηλεκτρονικής ψήφου δίχως την προσβολή των νομικών δικαιωμάτων του ψηφοφόρου.

Η ευρύτερα χρησιμοποιούμενες σήμερα τεχνολογίες για την ικανοποίηση των παραπάνω τεσσάρων βασικών απαιτήσεων ασφαλείας βασίζονται στην κρυπτογράφηση των ηλεκτρονικά ανταλλασσόμενων μηνυμάτων. Ως Κρυπτογράφηση (Encryption) ορίζεται *«ο μετασχηματισμός του αρχικού μηνύματος από τον αποστολέα ώστε αυτό να λάβει μια "ακατανόητη" μορφή (κρυπτομήνυμα) για οποιονδήποτε τρίτο».* [13] Στην περίπτωσή μας το αρχικό μήνυμα, βάσει ορισμού, αναφέρεται στην ηλεκτρονική ψήφο ενώ, ο αποστολέας στον ψηφοφόρο. Έτσι το κρυπτομήνυμα μεταδίδεται μέσω του καναλιού επικοινωνίας, όπως είναι το Internet, προς τον αποδέκτη, αυτός με την σειρά του παραλαμβάνει το κρυπτομήνυμα και πραγματοποιεί την Αποκρυπτογράφησή του, η οποία ορίζεται ως ο μετασχηματισμός του κρυπτομηνύματος στην αρχική και κατανοητή μορφή της ψήφου. Η κρυπτογράφηση χωρίζεται σε δύο κατηγορίες, τη Συμμετρική (ή Κρυπτογραφία Ιδιωτικού Κλειδιού) και την Ασύμμετρη (ή Κρυπτογραφία Δημόσιου Κλειδιού), η διαδικασία των οποίων δεν θα αναλυθεί στην παρούσα εργασία.

5.2 Ψηφιακή Υπογραφή

Πέραν της εξασφάλισης της εμπιστευτικότητας καθώς και της αυθεντικότητας του ψηφοφόρου μέσω της κρυπτογράφησης, εξίσου σημαντική απαίτηση ασφάλειας είναι και η εξασφάλιση της ακεραιότητας της ηλεκτρονικής ψηφοφορίας. Το μήνυμα, δηλαδή που αποστέλλει ο ψηφοφόρος των εκλογών πρέπει να ταυτίζεται με απόλυτη ακρίβεια με το μήνυμα (ψήφος) που θα λάβει ο αποδέκτης. Υπάρχουν διάφορες μέθοδοι με τις οποίες ελέγχεται εάν το περιεχόμενο ενός ηλεκτρονικού μηνύματος έχει αλλάξει σκόπιμα ή μη κατά τη μετάδοση από τον αποστολέα στον παραλήπτη. Σχεδόν όλες βασίζονται στον υπολογισμό μιας ή περισσότερων Τιμών Ελέγχου Ακεραιότητας (Integrity Check Values), οι οποίες είναι συναρτήσεις του μηνύματος και από τους δύο εμπλεκόμενους της μετάδοσης της πληροφορίας.

Προκειμένου λοιπόν, να εξασφαλιστεί ταυτόχρονα τόσο η αρχή της ακεραιότητας όσο και της αυθεντικότητας του ψηφοφόρου είθισται να χρησιμοποιούνται οι «Συναρτήσεις Σύνοψης» σε συνδυασμό με την ασύμμετρη κρυπτογραφία. Έτσι, αφού υπολογιστεί ή σύνοψη του αρχικού μηνύματος, κρυπτογραφείται με το Ιδιωτικό Κλειδί του ψηφοφόρου και το αποτέλεσμα ονομάζεται «Ψηφιακή Υπογραφή» (Digital Signature).

«Η Ψηφιακή Υπογραφή (Digital Signature) ορίζεται ως η σύνοψη ενός μηνύματος κρυπτογραφημένη με το Ιδιωτικό Κλειδί του αποστολέα του.»

Από τον ορισμό καθίσταται σαφές ότι μία ψηφιακή υπογραφή αφορά ένα συγκεκριμένο μήνυμα γραμμένο από ένα συγκεκριμένο χρήστη, χαρακτηρίζει δηλαδή μονοσήμαντα ένα ζεύγος μηνύματος-χρήστη και όχι μόνο έναν συγκεκριμένο χρήστη-άτομο, όπως συμβαίνει με τη «φυσική υπογραφή».

Έτσι, προκύπτει από τα παραπάνω ότι η χρήση της ψηφιακής υπογραφής εξασφαλίζει την ακεραιότητα, την αυθεντικότητα, την εμπιστευτικότητα του ψηφοφόρου πολίτη αλλά και τη μη αποποίηση των ηλεκτρονικών "μηνυμάτων", αφού δεν είναι δυνατόν να αμφισβητηθούν ούτε το "μήνυμα" αλλά ούτε και ο αποστολέας του. Η ψηφιακή υπογραφή,

υπό τις προϋποθέσεις που αναφέρονται στη σχετική νομοθεσία [14] είναι νομικά δεσμευτική όσο και η φυσική.

Η Ευρωπαϊκή οδηγία EC/93/99 για τις ηλεκτρονικές υπογραφές έχει ήδη υιοθετηθεί από όλα τα κράτη-μέλη, ενώ στην Ελλάδα υιοθετήθηκε με το Π.Δ. 150/2001. [17].Η ΕΕΤΤ με την απόφαση 248/71 (ΦΕΚ 603/Β'16-2-2002) ρυθμίζει τη διαπίστευση των παροχών υπηρεσιών πιστοποίησης και την έκδοση "αναγνωρισμένων πιστοποιητικών".

5.3 Ψηφιακά Πιστοποιητικά

Μία ακόμα τεχνολογία που εξασφαλίζει τις νομικές απαιτήσεις, ώστε η διαδικασία ψηφοφορίας δια των ηλεκτρονικών μέσων να είναι πιο ασφαλής, είναι τα «Ψηφιακά Πιστοποιητικά» (Digital Certificates). Τα ψηφιακά πιστοποιητικά εκδίδονται από εξειδικευμένους Φορείς Παροχής Υπηρεσιών Πιστοποίησης (Certification Services Providers – CSPs), και αποσκοπούν στην αντιστοίχηση των "Δημοσίων Κλειδιών" [15] με κάποια συγκεκριμένη οντότητα – φυσικό πρόσωπο. Χαρακτηρίζεται από τα αναγνωριστικά στοιχεία του πιστοποιητικού (τύπος-πρότυπο, έκδοση, σειριακός αριθμός, αλγόριθμος υπογραφής), την περίοδο ισχύος (από-έως), τις πληροφορίες εκδότη (διακριτικό όνομα, σημείο πρόσβασης και αναγνωριστικό κλειδιού), την υπογραφή εκδότη σε όλη τη δομή και τη σύνοψη πιστοποιητικού ως κλειδί αναφοράς.

Το ψηφιακό πιστοποιητικό έχει τη μορφή ηλεκτρονικού αρχείου, το οποίο περιλαμβάνει τα στοιχεία της οντότητας – κατόχου (subject) του και τα στοιχεία παροχής υπηρεσιών πιστοποίησης που έχει εκδώσει το ψηφιακό αυτό πιστοποιητικό (εκδότης – user). Περιλαμβάνει επίσης, την αντίστοιχη ψηφιακή υπογραφή, δηλαδή την κρυπτογράφηση της σύνοψης του περιεχόμενου του ψηφιακού πιστοποιητικού, ώστε να εξασφαλίζεται η αυθεντικότητα του εκδότη και η αυθεντικότητα και ακεραιότητα του περιεχομένου του.

5.4 Έξυπνες Κάρτες

Οι Κοινωνία Πληροφορίας συνεχώς εισάγει ζητήματα ασφαλείας και προστασίας των προσωπικών δεδομένων, καθιστώντας απαραίτητη τη χρήση τεχνολογικά προηγμένων και ασφαλών εφαρμογών έξυπνων καρτών. Οι έξυπνες κάρτες, που παρέχουν τη δυνατότητα συνδυασμού πολλαπλών εφαρμογών και αποτελούν αντικείμενο μελέτης και ανάπτυξης σε παγκόσμιο επίπεδο, εξυπηρετούν σκοπούς ηλεκτρονικής ταυτοποίησης.

Τα συστήματα αναγνώρισης έξυπνων καρτών ενσωματώνουν προηγμένες τεχνολογίες, όπως βιομετρικά δεδομένα (κρυπτογραφημένα δακτυλικά αποτυπώματα, στοιχεία ίριδας), ψηφιακή υπογραφή και processor chip, που επιτρέπει πρόσθετους ελέγχους σε βάση δεδομένων. Οι πιο διαδεδομένες εφαρμογές είναι οι κυβερνητικές ταυτότητες (για υπηρεσίες ηλεκτρονικής διακυβέρνησης), οι στρατιωτικές ταυτότητες (για εξακρίβωση ταυτότητας, παραχώρηση φυσικών και λογικών δικαιωμάτων πρόσβασης, διαχείριση μισθολογίου, έλεγχο αγορών κ.λ.π.) και οι άδειες οδήγησης (για αποτελεσματική διαχείριση παραβάσεων, έλεγχο των συνηθειών οδήγησης, επίβλεψη παραβατών, αύξηση του ρυθμού είσπραξης προστίμων). [16]

6. Ανάλυση προδιαγραφών από διεθνείς οργανισμούς πιστοποίησης

Η χρήση υπολογιστικών συστημάτων, ηλεκτρονικών αρχείων και δικτύων μεταφοράς δεδομένων αποτελεί πλέον απαραίτητο εργαλείο για την εύρυθμη λειτουργία της διαδικασίας ηλεκτρονικής ψήφου που τείνει να εφαρμοστεί ευρέως σε χώρες παγκοσμίως. Ωστόσο, η απροβλημάτιστη λειτουργία των ηλεκτρονικών συστημάτων και η ασφάλεια της πληροφορίας καθημερινά απειλείται από απρόβλεπτες βλάβες του εξοπλισμού, εξωτερικές κακόβουλες επιθέσεις, ιούς και άλλα βλαβερά λογισμικά ή ακόμα και από την αδυναμία του προσωπικού να αξιοποιήσει πλήρως τις τεχνολογικές δυνατότητες των συστημάτων.

Το ***ISO/IEC 27001:2005*** είναι μια διεθνής προδιαγραφή Διαχείρισης Ασφάλειας Πληροφοριών που έχει εκδοθεί από τον οργανισμό ISO (International Organization for Standardization) και αποτελεί μια συλλογή κοινώς αποδεκτών καλών πρακτικών για την προστασία των ηλεκτρονικών δεδομένων. Στόχος του προτύπου είναι η διαφύλαξη της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών, αρχές που έχουν αναλυθεί σε προηγούμενες ενότητες, μέσω της χρήση ενός συνόλου μέτρων ελέγχου. Το ISO 27001:2005 καλείται να προστατεύσει τη διαδικασία από κινδύνους και απειλές που μπορούν να δυσχεράνουν ή να σταματήσουν τη λειτουργία της και θα της επιτρέψει να αξιοποιήσει πλήρως τις δυνατότητες των πληροφοριακών της συστημάτων και να αποτρέψει περιστατικά απώλειας, καταστροφής ή διαρροής δεδομένων. Διακρίνεται από χαρακτηριστικά ταχείας αποκατάστασης λειτουργίας του συστήματος σε περίπτωση καταστροφής και απόλυτη συμμόρφωση με την Ελληνική και Κοινοτική νομοθεσία. [17]

Η *«Ψηφιακή Υπογραφή»* ορίζεται από τον οργανισμό πιστοποίησης ISO με το διεθνές πρότυπο ***ISO/IEC 9796***, στο οποίο περιέχεται η διεργασία υπογραφής και η διεργασία επαλήθευσης, χρησιμοποιώντας μια συνάρτηση κατακερματισμού και ένα ασύμμετρο κρυπτογραφικό σύστημα. [18] Το συγκεκριμένο διεθνές πρότυπο επαληθεύει την ακεραιότητα, αυθεντικότητα και τη μη αποποίηση αποστολής των ηλεκτρονικών συστημάτων ψηφοφορίας που τυχόν εφαρμόζονται σε περιπτώσεις εκλογών. Παρεμφερή πρότυπα που έχουν οριστεί από διαφόρους οργανισμούς πιστοποίησης είναι: TS 101-903(ETSI), CWA-14171 (CEN), ISO 9798 (ISO), ISO FDIS 14888 (ISO), ISO WD 15945 (ISO), RFC 3275 (IETF), IEEE P1363 (IEEE) κλπ. [19]

Τα πεδία ενός *«Ψηφιακού Πιστοποιητικού»* ορίζονται από το πρότυπο ***ISO/ITU-TX.509***. Το πρότυπο αυτό καλύπτει την νομοθετική αρχή της ταυτοποίησης ή αναγνώρισης της ταυτότητας του ψηφοφόρου. Παρεμφερή πρότυπα πιστοποίησης είναι: PKCS#6 (RSA), RFC-2511 (IETF), TR 102-030 (ETSI), RFC-2560: OCSP (IETF) κλπ.

Οι «Έξυπνες Κάρτες» ορίζονται από πιστοποιητικά πρότυπα όπως ISO/IEC 7816, ISO7810, CWA-14355 & CWA-14169 (CEN), ISO 10373-1, ISO 10202 και PKCS #11 & PKCS #15 (RSA).

7. Επίλογος

Η Ηλεκτρονική Δημοκρατία έχει ως στόχο την καλλιέργεια της κοινωνίας των πολιτών και την παροχή αναβαθμισμένων δυνατοτήτων συμμετοχής στις πολιτικές διαδικασίες, ώστε να ελαχιστοποιηθεί στο ελάχιστο το «ψηφιακό χάσμα» υπερασπίζοντας τα νόμιμα δικαιώματα κάθε ψηφοφόρου πολίτη. Απώτερος στόχος της είναι η επαναφορά του πολίτη μέσα στις πολιτικές διαδικασίες, το αίσθημα ασφάλειας των διαδικασιών και η μείωση της αμφισβήτησής του απέναντι στους πολιτικούς εκπροσώπους.

Είναι πολύ σημαντικό να τεθούν ρεαλιστικοί στόχοι προκειμένου να επιτευχθεί ο σκοπός της Ηλεκτρονικής Διακυβέρνησης. Για να γίνει κάτι τέτοιο θα πρέπει να πειστεί η πολιτεία για την αξιοπιστία, το αδιάβλητο και την αποτελεσματικότητα της Ηλεκτρονικής Ψηφοφορίας.

Η κοινωνία οφείλει να κατοχυρώσει τα δικαιώματα του πολίτη προκειμένου να υλοποιηθεί η ηλεκτρονική διαδικασία Δημοτικών ή και Ευρωπαϊκών εκλογών, και αυτό θα επιτευχθεί με την κάλυψη των προδιαγραφών που πρέπει να πληρούν οι ηλεκτρονικές μηχανές, όπως έχει αναλυθεί στην εν λόγω εργασία, κατά το δυνατόν μέγιστο. Έτσι, εστιάζοντας στα τεχνικά και νομικά προβλήματα που προκύπτουν από το eVote, καθώς και τις μεθόδους επιθέσεων και απειλών ενός τέτοιου συστήματος και συγκριτικά με τα πρότυπα που έχουν ήδη θεσπιστεί από οργανισμούς πιστοποίησης, η Ηλεκτρονική Δημοκρατία μπορεί πλέον να λάβει χώρα βελτιστοποιώντας τις διαδικασίες ψηφοφορίας και ικανοποιώντας τις ανάγκες των πολιτών κάθε κράτους. Πλέον, γίνεται λόγος για ένα τεχνικά άρτιο και νομικά συμβατό σύστημα που θα λειτουργήσει συμπληρωματικά του «κλασικού» τρόπου ψηφοφορίας, ενσωματώνοντας έτσι την ψηφοφορία στην «Κοινωνία της Πληροφορίας» που συνεχίζει να αναπτύσσεται με ραγδαίους ρυθμούς.

Βιβλιογραφία

[1] *Χ. Κωστόπουλος, (Επίβλεψη Δ. Χριστοδουλάκης), «Οι Ηλεκτρονικές Ψηφοφορίες ως εργαλεία λήψης αποφάσεων σε συστήματα Ηλεκτρονικής Διακυβέρνησης», Μεταπτυχιακή εργασία, Πάτρα,2007*

[2] Γκρτίτζαλης Δ., «Ασφάλεια Πληροφοριακών Συστημάτων», Εκδόσεις ΕΠΥ, 1991.

[3] Ι. Αποστολάκης, Ε. Λουκής, Ι. Χάλαρης, «Ηλεκτρονική Δημόσια Διοίκηση – Οργάνωση, τεχνολογία και Εφαρμογές»,σελ. 164-166, εκδ. Παπαζήση, Αθήνα, 2008

[4] Ι. Αποστολάκης, Ε. Λουκής, Ι. Χάλαρης, «Ηλεκτρονική Δημόσια Διοίκηση – Οργάνωση, τεχνολογία και Εφαρμογές», σελ. 52-55, εκδ. Παπαζήση, Αθήνα, 2008

[5] Χ. Κωστόπουλος, (*Επίβλεψη Δ. Χριστοδουλάκης*), «Οι Ηλεκτρονικές Ψηφοφορίας ως Εργαλεία Λήψης Αποφάσεων σε Συστήματα Ηλεκτρονικής Διακυβέρνησης», Μεταπτυχιακή εργασία, Πανεπιστήμιο Πατρών, 2007.

[6] Ι. Αποστολάκης, Ε. Λουκής, Ι. Χάλαρης, «Ηλεκτρονική Δημόσια Διοίκηση – Οργάνωση, τεχνολογία και Εφαρμογές», σελ. 191- 192, εκδ. Παπαζήση, Αθήνα, 2008.

[7] Ομάδα συγγραφέων (1995), «Ασφάλεια Πληροφοριών: Τεχνικά, Νομικά και Κοινωνικά Θέματα», Εκδόσεις ΕΠΥ

[8] Orhan Cetinkaya, Deniz Cetinkaya, "Towards Secure E-Elections in Turkey: Requirements and Principles", Second International Conference on Availability, Reliability and Security (ARES'07) © 2007, IEEE

[9] Peter G. Neumann, "The problems and potentials of voting systems", COMMUNICATIONS OF THE ACM October 2004/Vol. 47, No. 10

[10]*Ι. Αποστολάκης, Ε. Λουκής, Ι. Χάλαρης, «Ηλεκτρονική Δημόσια Διοίκηση – Οργάνωση, τεχνολογία και Εφαρμογές», σελ. 52, εκδ. Παπαζήση, Αθήνα, 2008*

[11] Ελ. Βενιζέλου, Μαθήματα Συνταγματικού Δικαίου, σελ. 353-364εκδ. Παρατηρητής, Θεσσαλονίκη, 1996.

[12] Χ. Κωστόπουλος, (Επίβλεψη Δ. Χριστοδουλάκης), «Οι Ηλεκτρονικές Ψηφοφορίες ως εργαλεία λήψης αποφάσεων σε συστήματα Ηλεκτρονικής Διακυβέρνησης», Μεταπτυχιακή εργασία, Πάτρα,2007

[13] Συμβούλιο της Ευρωπαϊκής Ένωσης, Επιτροπή των Ευρωπαϊκών Κοινοτήτων, «eEurope 2002, Κοινωνία των Πληροφοριών για όλους», Σχέδιο Δράσης για το Ευρωπαϊκό Συμβούλιο της Feira (19-20/6/2000), 2000

[14] Γκρίτζαλης Στ., Κάτσικας Σ. Και Γκρίτζαλης Δ., «Ασφάλεια Δικτύων και Υπολογιστών», Εκδόσεις Παπασωτηρίου, Αθήνα, 2003.

[15]Ευρωπαϊκή Επιτροπή, Οδηγία 99/93/ΕΚ, «Το Κοινοτικό Πλαίσιο για τις Ηλεκτρονικές Υπογραφές», 1999.

[16] http://www.lykos.gr/LykosGroup/docrep/docs/Solutions/Application_Management/smart_cards/DSRender_html?dr_page_number=3

[17] http://www.priority.com.gr/el/iso27001.html

[18] Ζορκάδης Β., «Προστασία και Ασφάλεια Συστημάτων Υπολογιστών», Ελληνικό Ανοικτό Πανεπιστήμιο, Πάτρα, 2002

[19]Ξενάκης Χ., «Υποδομή Δημοσίων Κλειδιών», Πανεπιστήμιο Πειραιά.