Ηλεκτρονική Διαβούλευση (Φάση Ψηφοφορίας και Αποτελέσματα)

Μάραντος Νικόλαος

Υπ. Καθηγητής
Τριανταφύλλου Βασίλιος
Ασημακόπουλος Γεώργιος

Αντίρριο 2014

Πρόλογος

Σκοπός της πτυχιακής μας είναι η διερεύνηση των ηλεκτρονικών ψηφοφοριών τον τρόπο που μπορούν να διεξαχθούν, τα προβλήματα που υπάρχουν, τους περιορισμούς καθώς και τα πλεονεκτήματα και μειονεκτήματα που υπάρχουν σε αυτές.

Υπάρχει ένα μεγάλο πλήθος εφαρμογών που ενσωματώνονται στην έννοια της ηλεκτρονικής ψηφοφορίας. Η παρούσα πτυχιακή επικεντρώνεται στην ηλεκτρονική άσκηση του εκλογικού δικαιώματος, η οποία πραγματοποιείται μέσω της χρήσης είτε του Διαδικτύου (on line voting, παρέχοντας στους ψηφοφόρους τη δυνατότητα να προβούν στην κατάθεση μίας ασφαλούς και μυστικής ψήφου, με τη βοήθεια υπολογιστικών συστημάτων.

Στην πτυχιακή αυτή υλοποιήσαμε εφαρμογή κατάλληλη για την διεξαγωγή ηλεκτρονικών ψηφοφοριών. Η εφαρμογή ορίζει δύο κατηγορίες χρηστών. Τον διαχειριστή και τον απλό χρήστη. Ο διαχειριστής είναι αυτός που προκηρύσσει ψηφοφορίες, εγκρίνει και ορίζει νέους χρήστες, διαχειρίζεται τις ομάδες χρηστών κ.α. Ο απλός χρήστης συμμετέχει απλά σαν ψηφοφόρος και μπορεί να ψηφίσει μια μόνο φορά σε κάθε ψηφοφορία. Επίσης για την ταυτοπροσωπία χρησιμοποιούμε τις κινητές συσκευές των χρηστών (κινητό τηλέφωνο) όπου με την χρήση απλών SMS στέλνεται κωδικός που ο χρήστης τον καταχωρεί και δίνει στο σύστημα. Σε περίπτωση που ο χρήστης δεν έχει κινητό τότε ο χρήστης μπορεί να ψηφίσει σε εξουσιοδοτημένες υπηρεσίες όπου εκεί γίνεται αποστολή του κωδικού σε εξουσιοδοτημένο email.

Περιεχόμενα

Εισαγωγή

Σκοπός της πτυχιακής μας είναι η διερεύνηση των ηλεκτρονικών ψηφοφοριών τον τρόπο που μπορούν να διεξαχθούν, τα προβλήματα που υπάρχουν, τους περιορισμούς καθώς και τα πλεονεκτήματα και μειονεκτήματα που υπάρχουν σε αυτές.

Υπάρχει ένα μεγάλο πλήθος εφαρμογών που ενσωματώνονται στην έννοια της ηλεκτρονικής ψηφοφορίας. Η παρούσα πτυχιακή επικεντρώνεται στην ηλεκτρονική άσκηση του εκλογικού δικαιώματος, η οποία πραγματοποιείται μέσω της χρήσης είτε του Διαδικτύου (on line voting, παρέχοντας στους ψηφοφόρους τη δυνατότητα να προβούν στην κατάθεση μίας ασφαλούς και μυστικής ψήφου, με τη βοήθεια υπολογιστικών συστημάτων.

Στο σημείο αυτό έχουν γίνει αρκετές προσπάθειες. Στην μελέτη μας θα αναλύσουμε τις απαιτήσεις ενός τέτοιου συστήματος τόσο από υλικό όσο και από λογισμικό. Επίσης ελέγχουμε τον τρόπο διασύνδεσης των υπολογιστικών συστημάτων και τον τρόπο ταυτοποίησης των προσώπων.

Με βάση τα παραπάνω υλοποιήσαμε εφαρμογή κατάλληλη για την διεξαγωγή ηλεκτρονικών ψηφοφοριών. Η εφαρμογή ορίζει δύο κατηγορίες χρηστών. Τον διαχειριστή και τον απλό χρήστη. Ο διαχειριστής είναι αυτός που προκηρύσσει ψηφοφορίες, εγκρίνει και ορίζει νέους χρήστες, διαχειρίζεται τις ομάδες χρηστών κ.α. Ο απλός χρήστης συμμετέχει απλά σαν ψηφοφόρος και μπορεί να ψηφίσει μια μόνο φορά σε κάθε ψηφοφορία. Επίσης για την ταυτοπροσωπία χρησιμοποιούμε τις κινητές συσκευές των χρηστών (κινητό τηλέφωνο) όπου με την χρήση απλών SMS στέλνεται κωδικός που ο χρήστης τον καταχωρεί και δίνει στο σύστημα. Σε περίπτωση που ο χρήστης δεν έχει κινητό τότε ο χρήστης μπορεί να ψηφίσει σε εξουσιοδοτημένες υπηρεσίες όπου εκεί γίνεται αποστολή του κωδικού σε εξουσιοδοτημένο email.

Η πτυχιακή μας εργασία είναι διαρθρωμένη ως εξής:

Στο πρώτο κεφάλαιο ορίζουμε τις Ηλεκτρονικές Ψηφοφορίες και κάνουμε παράθεση, διακρίνουμε τα είδη που υπάρχουν στις ηλεκτρονικές ψηφοφορίες, παραθέτουμε τις θετικές και αρνητικές συνέπειες αυτών. Στην συνέχεια αναφερόμαστε στα επιμέρους ζητήματα που προκύπτουν από τις ψηφοφορίες μέσω internet. Τέλος ορίζονται οι απαιτήσεις που πρέπει να πληρούνται σε ένα τέτοιο πληροφοριακό σύστημα.

Επειδή η ψηφοφορίες απαιτούν διαφύλαξη των δεδομένων είναι αναγκαία η κρυπτογράφηση των δεδομένων που χρησιμοποιούμε. Έτσι στο κεφάλαιο 2 αναφερόμαστε

στην κρυπτογράφηση, ορίζουμε τις ανάγκες για κρυπτογράφηση και αναφερόμαστε σε βασικούς αλγόριθμους κρυπτογράφησης που χρησιμοποιούνται στην περίπτωση των ψηφοφοριών.

Στο κεφάλαιο 3 καθορίζουμε τις βασικές τεχνολογίες στο διαδίκτυο που χρησιμοποιούνται για τις ηλεκτρονικές ψηφοφορίες. Από αυτές χρησιμοποιούμε για την υλοποίηση της εφαρμογής μας το σύστημα βάσεων δεδομένων MYSQL και την γλώσσα PHP.

Στο κεφάλαιο 4 δείχνουμε την εφαρμογή μας. Αρχικά παρουσιάζουμε το σχήμα της βάσης δεδομένων που χρησιμοποιούμε για της ψηφοφορίες, στην συνέχεια εμφανίζουμε τα βασικά χαρακτηριστικά καθώς και τον τρόπο λειτουργία της.

Στο τέλος στα συμπεράσματα κάνουμε ένα συνολικό απολογισμό της εργασίας μας, και παρουσιάζουμε πιθανή επέκταση της εφαρμογής .

Στο παράρτημα παρουσιάζουμε τον κώδικα της εφαρμογής που χρησιμοποιήσαμε ανά αρχείο.

Κεφάλαιο 1 – Ηλεκτρονικές Ψηφοφορίες

1.2 Ορισμός της ηλεκτρονικής ψηφοφορίας

Με τον όρο ηλεκτρονική ψηφοφορία (electronic voting / e-voting), εννοούμε την άσκηση του εκλογικού δικαιώματος, με τη χρήση ηλεκτρονικών μεθόδων. Η εννοιολόγηση αυτή, σε μία πρώτη προσέγγιση είναι εξαιρετικά γενική, καθώς περιλαμβάνει μία μεγάλη κλίμακα επιμέρους θεμάτων και διαδικασιών που εμπίπτουν στο πεδίο της διεξαγωγής μιας εκλογικής διαδικασίας, τα οποία μπορεί να εκτείνονται από την αυτοματοποίηση στην καταμέτρηση των ψήφων έως την άσκηση του ηλεκτρονικού δικαιώματος με τη βοήθεια του τηλεφώνου.

Λόγω του μεγάλου εύρους των εφαρμογών που ενσωματώνονται στην έννοια της ηλεκτρονικής ψηφοφορίας, κρίθηκε αναγκαίο, η παρούσα μελέτη να επικεντρωθεί στην ηλεκτρονική άσκηση του εκλογικού δικαιώματος, η οποία πραγματοποιείται μέσω της χρήσης είτε του Διαδικτύου (on line voting) είτε άλλων δικτύων, παρέχοντας στους ψηφοφόρους τη δυνατότητα να προβούν στην κατάθεση μίας ασφαλούς και μυστικής ψήφου, με τη βοήθεια υπολογιστικών συστημάτων. Σύμφωνα με την ανωτέρω οριοθέτηση, επομένως, δυο είναι τα θεμελιώδη στοιχεία που συνθέτουν την ιδιαίτερη φύση της ηλεκτρονικής ψήφου και τη διαφοροποιούν σε μεγάλο βαθμό από τα υπάρχοντα συστήματα της εκλογικής διαδικασίας:

1) Η δυνατότητα άσκησης του εκλογικού δικαιώματος από απόσταση, χωρίς την αυτοπρόσωπη, επομένως, παρουσία του ψηφοφόρου στο εκλογικό τμήμα.

2) Η χρήση υπολογιστικού συστήματος και κατά συνέπεια αυτοματοποιημένων μεθόδων, για την οργάνωση και διεξαγωγή της όλης εκλογικής διαδικασίας.

Η ρίψη μίας ηλεκτρονικής ψήφου μέσω του διαδικτύου πρέπει να συνοδεύεται από επαρκείς εγγυήσεις ασφάλειας ότι η ταυτότητα του ψηφοφόρου δεν θα αποκαλυφθεί κατά τη διάρκεια της μεταφοράς και της επεξεργασίας της ψήφου, όπως επίσης και ότι το περιεχόμενο της δεν θα μεταβληθεί, λόγω μη αποτελεσματικής λειτουργίας του συστήματος ή εξαιτίας εκλογικής λαθροχειρίας. Με βάση τα παραπάνω, ηλεκτρονικό εκλογικό σύστημα ορίζεται το σύστημα εκείνο που είναι προορισμένο να εξυπηρετήσει τις ανάγκες διεξαγωγής μίας ηλεκτρονικής ψηφοφορίας.

1.3 Διακρίσεις της ηλεκτρονικής ψηφοφορίας ανάλογα με το χώρο άσκησης του εκλογικού δικαιώματος

Η ηλεκτρονική ψηφοφορία είναι δυνατόν να πραγματοποιηθεί είτε στα παραδοσιακά εκλογικά τμήματα είτε, σε οποιοδήποτε άλλο χώρο από τον οποίο υπάρχει η δυνατότητα πρόσβασης στο διαδίκτυο. Σύμφωνα με τα παραπάνω, προκύπτει μια ουσιαστική διάκριση μεταξύ των μορφών που μπορεί να λάβει η ηλεκτρονική ψηφοφορία, η οποία συναρτάται με το χώρο από τον οποίο ο εκλογέας επιλέγει να ασκήσει το εκλογικό του δικαίωμα:

Α. Ηλεκτρονική ψηφοφορία εντός των εκλογικών τμημάτων (poll site e-voting): Στην περίπτωση αυτή, η ψηφοφορία γίνεται στα εκλογικά κέντρα, υπό την εποπτεία των αρμόδιων διοικητικών αρχών, οι οποίες έχουν την ευθύνη για τον έλεγχο της καλής λειτουργίας του υλικού και του λογισμικού του υπολογιστικού συστήματος, καθώς και την εποπτεία του περιβάλλοντος χώρου.

Με την ύπαρξη εποπτείας, διαφυλάσσεται ο μυστικός χαρακτήρας της διαδικασίας και αποτρέπονται φαινόμενα άσκησης πιέσεων επί των εκλογέων, όπως απειλές, εκφοβισμός, ή άσκηση βίας, προκειμένου να διαμορφώσουν την ψήφο τους κατά συγκεκριμένο τρόπο. Η εποπτεία των αρμόδια διοικητικών οργάνων καλείται να διασφαλίσει ότι οι πολίτες δεν θα συναντήσουν προσκόμματα κατά την άσκηση του εκλογικού τους δικαιώματος, ενώ ταυτόχρονα μειώνει τον κίνδυνο ύπαρξης φαινομένων πλαστοπροσωπίας.

Υποκατηγορία της άσκησης της ηλεκτρονικής ψηφοφορίας σε εποπτευόμενο από τις αρχές χώρο, αποτελεί η άσκηση του εκλογικού δικαιώματος σε κατάλληλα διαμορφωμένα περίπτερα (kiosk voting) ή θαλάμους, τα οποία είναι τοποθετημένα χώρους, όπου είναι ευχερής η προσέγγιση από το κοινό, όπως εμπορικά κέντρα, ταχυδρομεία, κ.ά. Και οι χώροι αυτοί θα επιτηρούνται από τους αρμόδιους υπαλλήλους.

Β. Ηλεκτρονική ψηφοφορία που πραγματοποιείται από απόσταση (remote e-voting): Η άσκηση του ηλεκτρονικού δικαιώματος γίνεται από οποιοδήποτε ιδιωτικό χώρο, όπου το μηχάνημα, μέσω του οποίου καταθέτει την ψήφο του ο εκλογέας, ελέγχεται από τον ίδιο ή κάποιον τρίτο. Ο χώρος αυτός μπορεί να είναι η οικία, ο επαγγελματικός χώρος του ψηφοφόρου, ή κάποιος δημόσιος χώρος, όπως τα "internet café". Το σύστημα αυτό ψηφοφορίας είναι προφανές ότι μεγιστοποιεί την ευκολία συμμετοχής στην ψηφοφορία.

Εγείρει, όμως, σημαντικές επιφυλάξεις για τις συνθήκες κάτω από τις οποίες ο ψηφοφόρος ασκεί το δικαίωμα του, καθώς και για το εάν οι δυνατότητες που παρέχει η σύγχρονη τεχνολογία, είναι σε θέση να διασφαλίσουν ότι το περιεχόμενο της ψήφου θα παραμείνει

μυστικό και αναλλοίωτο. Εν ολίγοις, η διάκριση μεταξύ της εποπτευόμενης και μη εποπτευόμενης ηλεκτρονικής ψήφου είναι ουσιαστική, διότι συνδέεται άμεσα με το επίπεδο ελέγχου που ασκούν στην όλη διαδικασία οι αρμόδιοι φορείς. Η απουσία εποπτείας είναι δυνατόν να επιτρέψει την παραβίαση της μυστικότητας και της ελευθερίας της ψήφου.

Η ηλεκτρονική ψηφοφορία από απόσταση με τη χρήση του διαδικτύου, αποτελεί επιμέρους κατηγορία των λεγόμενων RVEM (Remote Voting by Electronic Means) δηλαδή ψηφοφορία από απόσταση με τη χρήση ηλεκτρονικών μέσων: Άλλα τέτοια μέσα μπορεί να αποτελούν:

- Ψηφοφορία με τη χρήση τηλεφώνου. Αυτός ο τύπος του συστήματος μπορεί να λειτουργήσει είτε με τη χρήση των γραμμών της σταθερής τηλεφωνίας ή με τη χρήση κινητών τηλεφώνων.

- Η ψήφος με την αποστολή μηνυμάτων μέσω κινητού τηλεφώνου (SMS - Short Message Service),

- Χρήση της Ψηφιακής Διαδραστικής Τηλεόρασης (Interactive Digital Television). Η τεχνολογία αυτή αξιοποιεί τη δυνατότητα διάδρασης των νέων τύπων τηλεόρασης για να διευκολύνει τους ψηφοφόρους να καταθέσουν την ψήφο τους.

1.4 Άλλες μορφές άσκησης του εκλογικού δικαιώματος - Η εξέλιξη των εκλογικών συστημάτων

Η ηλεκτρονική ψηφοφορία από απόσταση αποτελεί ένα σταθμό σε μία μακραίωνη πορείας εξέλιξης του τρόπου με τον οποίο οι πολίτες συμμετέχουν στην άσκηση του εκλογικού δικαιώματος: Από την εποχή της ψηφοφορίας με την ανάταση του χεριού, ή την απόθεση φασολιών και δημητριακών σε ένα κουτί, μέχρι τη ρίψη του σφαιριδίου στη λευκή και τη μαύρη κάλπη, που είχαν οι υποψήφιοι στα μέσα του 18ου αιώνα, έχουν σίγουρα αλλάξει πολλά. Στη συνέχεια, γίνεται μία συνοπτική αναφορά στις διάφορες μορφές ασκήσεως του εκλογικού δικαιώματος, όπως αυτές εφαρμόζονται σήμερα:

- Παραδοσιακή μορφή ψηφοφορίας: Είναι η ψηφοφορία στα εκλογικά τμήματα με τη χρήση έντυπου ψηφοδελτίου. Εφαρμόζεται σε πολλά ευρωπαϊκά κράτη. Οι εγγεγραμμένοι στους εκλογικούς καταλόγους πολίτες, εισέρχονται στους ειδικά διαμορφωμένους χώρους και με τη μορφή του σταυρού ή της δεσμευμένης επιλογής (λίστα), επιλέγουν το κομματικό σχηματισμό της αρεσκείας τους. Όπως αναφέρθηκε ήδη, η μορφή αυτή ψηφοφορίας, παρέχει αρκετές εγγυήσεις για τη διασφάλιση του μυστικού χαρακτήρα της διαδικασίας.

- Επιστολική ψήφος: Ασκείται με την αποστολή στις αρμόδιες διοικητικές αρχές, μέσω ταχυδρομείου, του έντυπου ψηφοδελτίου που καταγράφει τη βούληση του εκλογέα. Η επιστολική ψήφος σε ορισμένα κράτη, απονέμεται σε ψηφοφόρους, οι οποίοι λόγω της συνδρομής συγκεκριμένων γεγονότων, αδυνατούν να προσέλθουν στα εκλογικά τμήματα, κατά την ημέρα διεξαγωγής των εκλογών και να ασκήσουν το εκλογικό τους δικαίωμα. Σήμερα η εκλογική νομοθεσία των περισσότερων κρατών επιτρέπει την άσκηση της επιστολικής ψήφου μετά από αίτηση του ψηφοφόρου (on demand), χωρίς να απαιτεί την επίκληση ιδιαίτερων λόγων. Τελευταία γίνεται λόγος για τη λεγόμενη καθολική επιστολική ψήφο (universal postal voting), όπου τα εκλογικά τμήματα θα καταργηθούν και η ψηφοφορία θα ασκείται αποκλειστικά μέσω ταχυδρομείου. Στην επιστολική ψήφο, οι ψήφοι μετρώνται μετά το πέρας της εκλογικής περιόδου, που ισχύει για τα συμβατικά εκλογικά τμήματα.

- Ηλεκτρονική ψηφοφορία (e-voting): Η έννοια της ηλεκτρονικής ψηφοφορίας, περιλαμβάνει μία μεγάλη κλίμακα από καινοτόμες εξελίξεις στον τρόπο οργάνωσης και διεξαγωγής των εκλογικών διαδικασιών. Τις αλλαγές αυτές προκάλεσε, μεταξύ άλλων, η ανάγκη για επιτάχυνση στον τρόπο με τον οποίο καταμετρούνταν τα ψηφοδέλτια, ο οποίος, ιδιαίτερα στα κράτη με μεγάλη δημογραφική συγκέντρωση, μπορούσε να αναστείλει για ημέρες την ανακοίνωση του εκλογικού αποτελέσματος, καθώς και η ανάγκη για μείωση του κόστους της εκλογικής διαδικασίας, μέσω της απασχόλησης οικονομικών και ανθρωπίνων πόρων. Οι αλλαγές αυτές αρχικά συνίστατο στην εισαγωγή ηλεκτρονικών μηχανημάτων, τα οποία στόχευαν στην απλοποίηση της διαδικασίας μέτρησης των ψήφων, την οποία αυτοματοποίησαν, και κατά συνέπεια στην επιτάχυνση στην ανακοίνωση των εκλογικών αποτελεσμάτων.

Μηχανήματα ηλεκτρονικής καταμέτρησης ψήφων

Τα μηχανήματα ηλεκτρονικής καταμέτρησης των ψήφων βρίσκονται εντός του εκλογικού κέντρου ή σε ειδικά διαμορφωμένους χώρους, που τοποθετούνται συνήθως σε κεντρικά σημεία των εκλογικών περιφερειών, για να διευκολύνουν την πρόσβαση των ψηφοφόρων. Συνολικά, τα συστήματα αυτά θεωρούνται ότι αυξάνουν την ταχύτητα και την ακρίβεια της μέτρησης.

Τα πλέον διαδεδομένα συστήματα ηλεκτρονικής καταμέτρησης των ψήφων είναι:

1) Συστήματα διάτρησης καρτών (punch card systems). Στα συστήματα αυτά, το ψηφοδέλτιο είναι μία ειδική ορθογώνια κάρτα, στην οποία ο εκλογέας, χρησιμοποιώντας ειδική διατρητική συσκευή, καταγράφει την επιλογή του. Οι κάρτες καταχωρούνται στη

συνέχεια σε μία ειδική μονάδα ανάγνωσης καρτών, η οποία καταγράφει την επιλογή των ψηφοφόρων. Με την ολοκλήρωση των εκλογών, η μονάδα αυτή υπολογίζει τα συνολικά αποτελέσματα, έχοντας προηγουμένως απορρίψει τα άκυρα ψηφοδέλτια. Είναι προφανές ότι τα παραπάνω συστήματα δεν διαφοροποίησαν ουσιαστικά τον τρόπο με τον οποίο ο ψηφοφόρος καταγράφει τις επιλογές του.

2) Συστήματα οπτικής σάρωσης (optical scanning systems). Στα συστήματα αυτά τα ονόματα των υποψηφίων είναι αναγραμμένα σε ένα έντυπο ψηφοδέλτιο, στο οποίο ο εκλογέας σημειώνει την επιλογή του με στυλό ή μολύβι. (σε μία συγκεκριμένη περιοχή). Κατόπιν η ειδική μονάδα (scanner), με μία φωτοευαίσθητη κεφαλή ανάγνωσης, αναγιγνώσκει το περιεχόμενο των ψηφοδελτίων και στη συνέχεια, όπως και στην προηγούμενη μέθοδο, καταγράφει τα συνολικά αποτελέσματα.

Μηχανήματα ηλεκτρονικής ψηφοφορίας

Είναι επίσης γνωστά με την ονομασία μηχανήματα άμεσης αυτόματης εγγραφής (Direct Recording Electronic machines – DREs). Τέτοιου είδους τεχνολογίες μπορεί να περιλαμβάνουν συστήματα με οθόνη αφής (touch screen systems) ή τεχνολογίες ηλεκτρονικών υπολογιστών (PC- based systems).

Με τα μηχανήματα αυτά ο εκλογέας δεν καταγράφει πλέον την επιλογή του, χρησιμοποιώντας ένα ξεχωριστό ψηφοδέλτιο, αλλά αντίθετα χρησιμοποιεί απευθείας την οθόνη του μηχανήματος, ενεργοποιώντας την ψήφο του με το άγγιγμα μίας συγκεκριμένης περιοχής. Οι ψήφοι αποθηκεύονται ηλεκτρονικά στη μνήμη του μηχανήματος και, μετά το πέρας της εκλογικής διαδικασίας, μεταφέρονται στο κεντρικό υπολογιστικό σύστημα είτε με τη μορφή φορητών μονάδων π.χ. δισκέτες, είτε μέσω δικτύου, όπου καταμετρώνται οι ψήφοι και πινακοποιούνται τα αποτελέσματα.

Με τη χρήση των μηχανημάτων αυτών, καταργείται η πιθανότητα διάπραξης λάθους κατά την άσκηση του δικαιώματος, καθώς είναι προγραμματισμένα να προβάλλουν ένα προειδοποιητικό μήνυμα στην περίπτωση που ο εκλογέας επιχειρήσει να ολοκληρώσει τη διαδικασία έχοντας ψηφίσει περισσότερους ή λιγότερους υποψηφίους από ότι επιτρέπεται. Επίσης, είναι δυνατόν να χρησιμοποιηθούν και από άτομα με ειδικές αναπηρίες (π.χ. ηχητικές εντολές, παροχή της μεθόδου μπραίγ σε περίπτωση ύπαρξης αναπηρίας στην όραση). Τέλος, μειώνουν σημαντικά το χρόνο και το κόστος της καταμέτρησης, εξαλείφοντας την πιθανότητα ανθρώπινου λάθους.

1.5 Θετικές και αρνητικές συνέπειες από την εισαγωγή της ηλεκτρονικής ψηφοφορίας

Θετικές συνέπειες

Η εισαγωγή της ηλεκτρονικής ψηφοφορίας στις διαδικασίες διενέργειας εκλογών σε τοπικό, εθνικό και ευρωπαϊκό επίπεδο, προσδοκάται να αναστραφεί η πορεία αποχωρισμού μίας σημαντικής μερίδας του εκλογικού σώματος από τα πολιτικές διαδικασίες. Η αύξηση της συμμετοχής των ψηφοφόρων στις διαδικασίες ανάδειξης των αιρετών αντιπροσώπων, είναι σημαντική στο πλαίσιο μίας δημοκρατικής κοινωνίας, γιατί μεγενθύνει τη νομιμοποίηση των πολιτικών αποφάσεων που θα κληθεί να λάβει η ηγεσία αυτή.

Η άνοδος του ποσοστού των ψηφοφόρων που θα κινητοποιηθεί για να ασκήσει τα εκλογικά του δικαιώματα, οφείλεται κυρίως:

1) Στην αύξηση της ευκολίας συμμετοχής των ψηφοφόρων (voters convenience), λόγω των εναλλακτικών λύσεων που προσφέρονται στον τρόπο άσκησης του εκλογικού δικαιώματος, όπως είναι η επέκταση της εκλογικής περιόδου. Η ηλεκτρονική ψήφος θα αποτελεί μία ικανοποιητική λύση για τη μείωση του κόπου, αλλά και του κόστους, που συνεπάγεται η υποχρέωση προσέλευσης στα εκλογικά τμήματα. Εκλογείς, οι οποίοι για διάφορους λόγους, όπως ασθένεια, απουσία στο εξωτερικό ή εγκατάσταση σε διαφορετική εκλογική περιφέρεια λόγω επαγγελματικών υποχρεώσεων, δεν είχαν τη δυνατότητα να προσέλθουν στα εκλογικά τμήματα, θα πάψουν πλέον να υφίστανται μια de facto αποστέρηση των πολιτικών δικαιωμάτων τους. Η ηλεκτρονική ψήφος εξάλλου θα αποδειχθεί ιδιαίτερα χρήσιμη για τους ψηφοφόρους με κινητικά προβλήματα ή άλλες σωματικές αναπηρίες.

2) Σημαντική ώθηση στην εκλογική συμμετοχή, εξάλλου, θεωρείται ότι θα επιφέρει η προσέλκυση που θα ασκήσει το διαδίκτυο καθ' αυτό ιδιαίτερα στους νεότερους σε ηλικία ψηφοφόρους, οι οποίοι αποτελούν και τη μερίδα εκείνη του πληθυσμού που παρουσιάζουν τη μεγαλύτερη εξοικείωση με τις νέες τεχνολογίες. Ο δυναμικός και καινοτόμος χαρακτήρας του όλου επιχειρήματος θα δώσει μια νέα πνοή σε μία παγιωμένη και ενδεχομένως ιδιαίτερα στατική, για την ενθουσιώδη φύση της νεαρής ηλικίας, εκλογική πρακτική.

Επιπλέον, λόγω του αυτοματοποιημένου χαρακτήρα του όλου εγχειρήματος, θα υπάρξει μείωση του μέσο-μακροπρόθεσμου κόστους των εκλογών και ταυτόχρονη βελτίωση της διοικητικής αποτελεσματικότητας. Η καταμέτρηση των ψήφων θα πραγματοποιείται

γρηγορότερα και με μεγαλύτερη ακρίβεια, μειώνοντας την πιθανότητα αμφισβητήσεως των εκλογικών αποτελεσμάτων και ανάγκης για επανάληψη της εκλογικής διαδικασίας.

Η προμήθεια βέβαια της τεχνολογικής υποδομής (υλικό, λογισμικό) αναπόφευκτα θα επιβαρύνει βραχυπρόθεσμα τον κρατικό προϋπολογισμό. Μακροπρόθεσμα, όμως, η υποδομή αυτή θα δίνει τη δυνατότητα διενέργειας πολλαπλών εκλογικών αναμετρήσεων, εξασφαλίζοντας σημαντική εξοικονόμηση πόρων τόσο οικονομικών (μείωση του κόστους έκδοσης των παραδοσιακών εντύπων ψηφοδελτίων) όσο και σε ανθρώπινο δυναμικό, καθώς η απλοποίηση, σε μεγάλο βαθμό, της διαδικασίας και η εναπόθεση των περισσοτέρων ενεργειών στη λειτουργική ικανότητα των μηχανημάτων, θα περιορίσει τις άνθρωποώρες που δαπανώνται υπό τις σημερινές συνθήκες, ιδιαίτερα κατά τη φάση προετοιμασίας των εκλογών.

Το εκλογικό αποτέλεσμα θα αναπαριστά με περισσότερη ακρίβεια την βούληση του εκλογικού σώματος, με την προϋπόθεση ότι ο σχεδιασμός των ηλεκτρονικών μηχανημάτων, θα προβλέπει τρόπους προειδοποίησης των ψηφοφόρων σε περίπτωση όπου εκ παραδρομής η ψήφος δεν ανταποκρίνεται στα κριτήρια εγκυρότητας που θέτει ο εκλογικός νόμος (π.χ. ψήφος με περισσότερες επιλογές από τις προβλεπόμενες).

Η ευκολία στην πρόσβαση που χαρακτηρίζει την ηλεκτρονική ψηφοφορία, αλλά και το ενδεχόμενο χρήσης της μεθόδου αυτής και σε άλλες διαδικασίες λήψης αποφάσεων (δημοψηφίσματα, λαϊκές πρωτοβουλίες, αιτήσεις ανάκλησης κ.ά.), θεωρείται από πολλούς ότι μπορεί να οδηγήσει σε μια νέα μορφή άμεσης δημοκρατίας, τη δημοκρατία του κυβερνοχώρου (cyber-democracy).

Οι πολίτες, αξιοποιώντας τις νέες πηγές πληροφόρησης και επικοινωνίας, θα ανακάμψουν από την πολιτική απάθεια, συμμετέχοντας σε δικτυακά fora και ανταλλάσσοντας απόψεις για σημαντικά ζητήματα της κοινωνικής και πολιτικής ζωής. Έτσι, η ηλεκτρονική ψηφοφορία δεν θα συμβάλλει μόνο σε μία ποσοτική αναβάθμιση του ποσοστού συμμετοχής των ψηφοφόρων, αλλά το κυριότερο σε μία ποιοτική βελτίωση της συμμετοχής αυτής (more votes, more informed voters).

Αρνητικές συνέπειες

Οι επιδράσεις της ηλεκτρονικής ψηφοφορίας στην αναδιοργάνωση της εκλογικής διαδικασίας και στην αύξηση της ευκολίας των ψηφοφόρων, αναμφισβήτητα αποτελούν σημαντικά στοιχεία στην επιχειρηματολογία των θιασωτών αυτής της μεθόδου. Εντούτοις, εξίσου ισχυρός είναι και ο αντίλογος όσων υποστηρίζουν ότι η ψηφιοποίηση της εκλογικής

διαδικασίας κρύβει πολλούς κινδύνους για τις κατακτήσεις που έχουν πραγματοποιηθεί στο χώρο των πολιτικών δικαιωμάτων και οι οποίες ως ένα βαθμό αποτελούν θεσμικό κεκτημένο.

Ειδικότερα, υποστηρίζουν ότι η εισαγωγή της ηλεκτρονικής ψηφοφορίας δεν είναι σε θέση, με την υπάρχουσα υποδομή της πληροφοριακής τεχνολογίας να διασφαλίσει τις προϋποθέσεις ασφάλειας, που είναι απαραίτητο να παρέχει ένα αξιόπιστο εκλογικό σύστημα. Η ασφάλεια, σε γενικές γραμμές, μπορεί να αφορά:

- Την ακεραιότητα της ψήφου, την εγγύηση, δηλαδή, ότι το περιεχόμενο της δεν θα μεταβληθεί στο στάδιο που μεσολαβεί από την άσκηση του εκλογικού δικαιώματος του ψηφοφόρου μέχρι την καταμέτρηση της ψήφου από το κεντρικό υπολογιστικό σύστημα. Η μη εξουσιοδοτημένη πρόσβαση στα εκλογικά δεδομένα και η απόπειρα πρόκλησης δυσλειτουργιών στην εξέλιξη της διαδικασίας, λόγω του συγκεντρωτικού τρόπου με τον οποίο λειτουργούν τέτοιου είδους συστήματα, είναι δυνατόν να οδηγήσει σε αυτοματοποιημένη λαθροχειρία μεγάλης κλίμακας.

- Τη μυστικότητα της ψήφου. Η δυνατότητα των εκλογέων να ρίξουν την ψήφο τους, χωρίς την υποχρέωση να προσέλθουν στα εκλογικά τμήματα επιβάλλει, εκ των πραγμάτων, τη θέσπιση αυστηρότερων προϋποθέσεων για την ανάγκη εξακρίβωσης της ταυτότητας του ψηφοφόρου. Οι προϋποθέσεις αυτές πιθανά θα συνίσταται στη χορήγηση ψηφιακών υπογραφών ή κωδικών πρόσβασης, ανάλογα με τις συγκεκριμένες προδιαγραφές με τις οποίες έχει σχεδιαστεί το κάθε ηλεκτρονικό σύστημα.

Παρά την ικανότητα που παρουσιάζουν οι συγκεκριμένες μέθοδοι να προστατεύσουν το περιεχόμενο της ψήφου των εκλογέων, αλλά και να αποστρέψουν τον κίνδυνο αποκάλυψης της ταυτότητας του ψηφοφόρου, εντούτοις αμφισβητείται ευρέως η αποτελεσματικότητα τους σε εφαρμογές μεγάλης κλίμακας και ιδιαίτερης συνθετότητας, όπως είναι η ηλεκτρονική ψηφοφορία.

Παράλληλα, παρά την εντυπωσιακή διάδοση, τα τελευταία χρόνια, της χρήσης των μέσων πληροφοριακής τεχνολογίας και ιδιαίτερα του διαδικτύου, εξακολουθεί να υπάρχει διαφοροποιημένη πρόσβαση στις νέες τεχνολογίες μεταξύ των κοινωνικών ομάδων. Συνεπώς, η εισαγωγή της ηλεκτρονικής ψηφοφορίας ενδεχομένως να ευνοήσει τους ψηφοφόρους εκείνους που έχουν εξοικειωθεί με τις νέες τεχνολογίες και να οδηγήσει στον αποκλεισμό των υπολοίπων από τις διαδικασίες λήψης αποφάσεων.

Η ψηφιοποίηση μίας διαδικασίας, η οποία αποτελεί τον κορυφαίο θεσμό της δημοκρατίας, χάριν ικανοποίησης ατομικιστικών επιδιώξεων (ευκολία συμμετοχής) υποβιβάζει την άσκηση ενός θεμελιώδους πολιτικού δικαιώματος στο επίπεδο των ηλεκτρονικών συναλλαγών στις οποίες προβαίνει καθημερινά ο πολίτης.

Οι εκλογές αποσκοπούν στο να ενδυναμώσουν την ιδιότητα του πολίτη, υπενθυμίζοντας την σημασία του να θέτει κανείς το ευρύτερο δημόσιο συμφέρον πάνω από τις στενές του ατομικές επιδιώξεις. Η δημοκρατική συμμετοχή πάντα θα συνεπάγεται ένα μικρό ποσοστό αναστάτωσης για τον πολίτη, όπως άλλωστε συμβαίνει με τις περισσότερες σημαντικές δραστηριότητες στη ζωή. Η αντιμετώπιση της ηλεκτρονικής ψηφοφορίας ως μια επέκταση των εφαρμογών του διαδικτύου παραγνωρίζει βασικές αρχές του συνταγματικού βίου και υπονομεύει την ίδια αρχή της λαϊκής κυριαρχίας.

Πεδίο εφαρμογής της ηλεκτρονικής ψηφοφορίας

Εκτός από την εφικτότητα εφαρμογής της ηλεκτρονικής ψηφοφορίας, η ηλεκτρονική ψηφοφορία μπορεί να χρησιμοποιηθεί και σε πλήθος άλλων διαδικασιών λήψης αποφάσεων, με δεσμευτικό ή μη χαρακτήρα. Τέτοιες διαδικασίες μπορεί να είναι:

1) Δημοψηφίσματα και αιτήσεις ανάκλησης: Οι διαδικασίες αυτές, όπως και οι εθνικές εκλογές, διενεργούνται από τις εθνικές αρχές κάθε κράτους και έχουν δεσμευτικό χαρακτήρα. Υπάγονται σε ειδικές νομοθετικές ρυθμίσεις και, δεδομένου ότι τα αποτελέσματα τους είναι αποφασιστικής σημασίας για τη ζωή των πολιτών, η χρήση της ηλεκτρονικής ψηφοφορίας οφείλει πρωτίστως να υπακούει στη δημοκρατική νομιμότητα και να διασφαλίζει τη διαφάνεια της διαδικασίας.

2) Εσωτερικές εκλογές (και άλλες διαδικασίες με παρόμοιο περιεχόμενο): Ανάλογα με το εάν έχουν δημόσιο ή ιδιωτικό χαρακτήρα μπορεί να υπάγονται σε συγκεκριμένες ρυθμίσεις του νόμου και να έχουν δεσμευτικό ή μη χαρακτήρα.

3) Ψηφοφορίες συμβουλευτικού χαρακτήρα (advisory polls): Διενεργούνται συνήθως από εθνικές ή τοπικές αρχές και έχουν ως στόχο να ενθαρρύνουν την ανάμιξη των πολιτών στη διαδικασία λήψης αποφάσεων, μέσω της εισαγωγής διαδικασιών διαβούλευσης. Για το λόγο αυτό θα πρέπει να συμμορφώνονται με τις επιταγές του νόμου.

4) Ψηφοφορίες στο διαδίκτυο: Τέτοιου είδους διαδικασίες πραγματοποιούνται συχνά στο διαδίκτυο, είτε από ιδιώτες είτε από οργανώσεις και δεν έχουν δεσμευτικό χαρακτήρα. Τα αποτελέσματα αυτών των σφυγμομετρήσεων δεν μπορούν πάντα να θεωρούνται

αξιόπιστα, διότι δεν καταγράφεται συνήθως το προφίλ αυτών που συμμετέχουν, ούτε το πόσες φορές ψηφίζουν.

1.7 Επιμέρους ζητήματα ηλεκτρονικής ψηφοφορίας με χρήση διαδικτύου

Τα θέματα που αναλύθηκαν προηγουμένως, αποτελούν θεμελιώδεις απαιτήσεις για τη διενέργεια γενικών, ελεύθερων, ισότιμων, ευθέων και δημοκρατικών εκλογών. Στη συνέχεια θα αναλύσουμε κάποιες απαιτήσεις ασφαλείας, που σχετίζονται, κυρίως, με θέματα ασφαλείας υπολογιστικών συστημάτων, έχουν, όμως, άμεση σχέση με μία εκλογική διαδικασία που βασίζεται σε υπολογιστές και τεχνολογίες δικτύου και κατ' επέκταση αφορούν εξ' ολοκλήρου τη διαδικασία μιας ηλεκτρονικής ψηφοφορίας.

Απαιτήσεις σε υλικό

Αρχικά πολύ σημαντικό ζήτημα είναι η επιλογή και συντήρηση κατάλληλου υλικού εξοπλισμού (hardware). Στην υπάρχουσα εκλογική διαδικασία το κυριότερο, αν όχι το μοναδικό υλικό, που χρησιμοποιείται είναι οι κάλπες και τα παραβάν. Όπως είναι προφανές δεν έχει νόημα να αναφέρουμε αυτό το θέμα ως απαίτηση ασφαλείας της συμβατικής εκλογικής διαδικασίας. Στην ηλεκτρονική ψηφοφορία, όμως, το θέμα του υλικού εξοπλισμού είναι πολύ σημαντικό. Ο τρόπος λειτουργίας του, καθώς και η ποιότητα των τμημάτων που το αποτελούν, πρέπει να είναι όσο το δυνατόν καλύτερης ποιότητας. Οι κίνδυνοι που μπορεί να προκύψουν από ελλιπές ή ελαττωματικό υλικό δεν προκύπτουν μόνο από ηθελημένη και κακόβουλη τροποποίηση του, αλλά και από ακούσια βλάβη. Όσον αφορά την κακόβουλη τροποποίηση του υλικού εξοπλισμού πρέπει να υπάρχουν εντατικοί έλεγχοι και κατά την κατασκευή του, αλλά και κατά το χρονικό διάστημα που θα ακολουθήσει μέχρι να χρησιμοποιηθούν. Πιθανή προσπάθεια τροποποίησης των μηχανημάτων, που χρησιμοποιούνται σε μια εκλογική διαδικασία, θα πρέπει να οδηγεί είτε σε αποτυχία της προσπάθειας είτε σε καταστροφή του μηχανήματος, έτσι ώστε ένα μηχάνημα που λειτουργεί να είναι σίγουρο πως δεν έχει υποστεί τροποποίηση. Όσον αφορά τυχόν βλάβη κατά τη διάρκεια της εκλογικής διαδικασίας, πρέπει να υπάρχει ειδικευμένο και εξουσιοδοτημένο προσωπικό σε κάθε εκλογικό κέντρο, ώστε να μπορεί άμεσα να επιδιορθώνει το πρόβλημα και να αποκαθιστά την ορθή λειτουργία του υλικού. Μέχρι τώρα έχουν γίνει διάφορες προτάσεις για ειδικά μηχανήματα που μπορούν να χρησιμοποιηθούν για μια εκλογική διαδικασία με επικρατέστερα μέχρι στιγμής τα DREs. Να αναφέρουμε πως μέσα στις ανάγκες για κατάλληλο υλικό μπορεί να αναφερθεί τυχόν χρήση έξυπνων καρτών (smart cards) για αυθεντικοποίηση των χρηστών.

Απαιτήσεις σε λογισμικό

Εξίσου σημαντικό ζήτημα είναι και η ανάπτυξη και ο έλεγχος του λογισμικού που χρησιμοποιείται. Τα σημαντικότερα θέματα που φαίνεται να σχετίζονται με το λογισμικό έχουν να κάνουν με τους κρυπτογραφικούς αλγόριθμους και με τη διαφάνεια του κώδικα. Η κρυπτογραφία είναι, ίσως, το σημαντικότερο εργαλείο για την εξασφάλιση της ακεραιότητας και της εμπιστευτικότητας των ψήφων, αλλά και των μηχανισμών αυθεντικοποίησης των ψηφοφόρων.

Η διαφάνεια του κώδικα είναι, επίσης, πολύ σημαντικό θέμα. Αρχικά, ο κώδικας πρέπει να είναι όσο το δυνατόν πιο απλός και ευκολονόητος, χωρίς βέβαια αυτό να σημαίνει υποβάθμιση της ασφάλειας. Όσο πιο απλός είναι ο κώδικας, τόσο πιο ευκολονόητος θα είναι και τόσο πιο εύκολος θα είναι ο έλεγχός του. Το να είναι ευκολονόητος ο κώδικας είναι βασικό στοιχείο για τη διαφάνεια του. Αυτό δεν σημαίνει βέβαια πως πρέπει οποιοσδήποτε, χωρίς κατάλληλο υπόβαθρο γνώσεων, να μπορεί να τον καταλάβει, αλλά δεν πρέπει ο κώδικας να είναι κατανοητός μόνο στην προγραμματιστική ομάδα που το δημιούργησε, όσο έμπιστη και κοινής αποδοχής και να είναι. Επίσης, ένας απλός και καλά δομημένος κώδικας μπορεί να οδηγήσει στην εύκολη και έγκαιρη ανίχνευση κάποιας προσθήκης μη-εξουσιοδοτημένων τμημάτων (δούρειοι ίπποι, ιοί, κ.λπ.).

Απαιτήσεις διασύνδεσης υπολογιστικών συστημάτων

Ένα ακόμα πολύ σημαντικό ζήτημα, που μπορεί να θέσει σε κίνδυνο μία ηλεκτρονική ψηφοφορία είναι το θέμα τις διασύνδεσης των διαφόρων υπολογιστικών συστημάτων που μετέχουν στην διαδικασία. Όσο μεγαλύτερη είναι η χρήση δικτυακής τεχνολογίας, τόσο περισσότεροι είναι και οι κίνδυνοι που δημιουργούνται. Το κατά πόσο η διαδικασία της ηλεκτρονικής ψηφοφορίας θα προϋποθέτει χρήση δικτύου είναι κάτι που θα εξαρτηθεί από την ακριβή δομή της. Γεγονός είναι, πάντως, πως όσο μεγαλύτερη χρήση δικτυακών επικοινωνιών γίνεται, η διαδικασία γίνεται πιο λειτουργική, αλλά παράλληλα αυξάνονται και οι πιθανότητες για παραβίαση της ασφάλειάς της. Διάφορες προτάσεις που έχουν γίνει ανά διαστήματα προσεγγίζουν το ζήτημα με διαφορετικούς τρόπους.

Το ότι σε κάθε εκλογικό κέντρο θα υπάρχουν ειδικά μηχανήματα που θα ψηφίζουν οι πολίτες δεν σημαίνει αυτόματα πως αυτά θα πρέπει να επικοινωνούν μεταξύ τους μέσω δικτύου. Η συγκέντρωση των αποτελεσμάτων θα μπορούσε να γίνει με την χρήση CDs, η ακόμα και με τη χρήση διαφόρων μορφών κινητής μνήμης. Με αυτόν τον τρόπο η διαδικασία γίνεται πολύ πιο χρονοβόρα και το θέμα της ασφάλειας μετατίθεται στη φερεγγυότητα των ανθρώπων και των διαδικασιών μεταφοράς.

Κεφάλαιο 2- Κρυπτογράφηση

2.1 Ορισμός και ανάγκες Κρυπτογραφίας

Στις μέρες μας οι επιθέσεις εναντίον δικτύων και υπολογιστικών συστημάτων έχουν πάρει μεγάλη έκταση και προκαλούν πολλά προβλήματα σε οργανισμούς , εταιρείες και χρήστες.

Ειδικά στο θέμα της ψηφοφορίας η παραβίαση των συστημάτων αυτών αποτελεί στόχο αφού για τους συμμετέχοντες στην ψηφοφορία υπάρχει έντονο συμφέρον από κάθε μεριά η πιθανή αλλαγή των αποτελεσμάτων.

Συνήθως στόχος ενός κακόβουλου είναι η υποκλοπή απόρρητων δεδομένων και η χρήση τους προς όφελός του. Η προστασία και η ασφάλεια της ευαίσθητης αυτής πληροφορίας , που διατηρείται και αποστέλλεται σε ένα δίκτυο κρίνεται επιτακτική.

Η διασφάλιση της ακεραιότητας της πληροφορίας απαιτεί την χρήση μαθηματικών τεχνικών οι οποίες παρέχονται μέσω της επιστήμης της Κρυπτογραφίας. Η επιστήμη αυτή παρέχει την δυνατότητα ασφαλούς αποθήκευσης ευαίσθητης πληροφορίας , καθώς επίσης και αποστολής αυτής μέσω μη ασφαλών δικτύων , εξασφαλίζοντας την ανάγνωσή της μόνο από τον εξουσιοδοτούμενο παραλήπτη. Θα πρέπει να τονισθεί ότι η Κρυπτογραφία δεν αποτελεί το μόνο εργαλείο που εξασφαλίζει την ασφάλεια της πληροφορίας , παρά μόνο αποτελεί ένα σύνολο συνεχώς εξελισσόμενων αλγορίθμων.

Οι κυριότεροι στόχοι της Κρυπτογραφίας είναι οι εξής:

1. Η *Μυστικότητα της Πληροφορίας* (Confidentiality) εξασφαλίζει ότι το περιεχόμενο της πληροφορίας είναι διαθέσιμο μόνο στον νόμιμο κάτοχο αυτής και μυστικό σε κάθε άλλο εκτός αυτού. Για την επίτευξη του στόχου αυτού μπορούν να χρησιμοποιηθούν είτε φυσικά μέσα είτε μαθηματικοί αλγόριθμοι οι οποίοι καθιστούν τα δεδομένα μη αναγνώσιμα.
2. Η *Ακεραιότητα της Πληροφορίας* (Integrity) αναφέρεται στη αλλοίωση των δεδομένων. Για να διακρίνει κάποιος την αλλοίωση της πληροφορίας θα πρέπει να διαθέτει μέσα ώστε να μπορεί να εξετάσει την αποκοπή , αντικατάσταση ή εισαγωγή δεδομένων.
3. Η *Πιστοποίηση της Προέλευσης και Αυθεντικότητας της Πληροφορίας* (Authentication) έχει δύο διαστάσεις. Η πρώτη αναφέρεται στα άκρα της επικοινωνίας (entity authentication) : οι δύο οντότητες που επικοινωνούν θα πρέπει να αναγνωρίζει η μία την άλλη. Σαν δεύτερη προυπόθεση ορίζεται η αναγνώριση της προέλευσης της πληροφορίας (data origin authentication).

Είναι αναγκαίο να πιστοποιείται η προέλευση των δεδομένων , το περιεχόμενό τους , ο χρόνος καθώς η ημερομηνία αποστολής τους.

4. Η *Απαγόρευση Άρνησης της Αποστολής της Πληροφορίας* (Non-repudiation) από μία οντότητα είναι απολύτως σημαντική για ένα ασφαλές δίκτυο. Σαν παράδειγμα μπορούμε να αναφέρουμε την περίπτωση μιας οντότητας η οποία εξουσιοδοτεί μια άλλη οντότητα στο να έχει πρόσβαση σε μία πληροφορία και στην συνέχεια να υποστηρίξει πως ουδέποτε είχε παραχωρήσει τέτοια δικαιοδοσία. Στην περίπτωση αυτή κρίνεται αναγκαία η ύπαρξη μιας απολύτως εμπιστευόμενης τρίτης οντότητας (trusted third party) ώστε να δοθεί μία λύση.

Έτσι πρωταρχικός στόχος της Κρυπτογραφίας είναι να συνδυάσει επιτυχώς τα ανωτέρω θεμελιώδη αιτήματα σε επίπεδο θεωρίας αλλά κυρίως σε πρακτικό επίπεδο.

2.2 Message-Digest algorithm 5(MD5)

Στην κρυπτογραφία το Message-Digest algorithm 5 (MD5) χρησιμοποιείται ευρέως , κυρίως η επισφαλής κρυπτογραφική συνάρτηση κατακερματισμού, με τιμή κατακερματισμού 128 bits. Το MD5 χρησιμοποιείται σε διάφορες εφαρμογές ασφαλείας και κυρίως χρησιμοποιείται για τον έλεγχο της ακεραιότητας των αρχείων. Ένας MD5 κατακερματισμός τυπικά εκφράζεται σαν ένα 32 ψηφίων δεκαεξαδικός αριθμός. Το MD5 σχεδιάστηκε το 1991 από τον Ron Rivest για να αντικαταστήσει την προηγούμενη συνάρτηση κατακερματισμού MD4. Το 1996 ένα μειονέκτημα στο σχεδιασμό του MD5 οδήγησε τους σχεδιαστές στην εύρεση ενός πιο αποδοτικού και αξιόπιστου αλγορίθμου τον SHA-1.

2.2 Ανάλυση του αλγορίθμου MD5

Το MD5 επεξεργάζεται ένα μεταβλητού μήκους μήνυμα σε μία σταθερού μήκους έξοδο μήκους 128 bits. Το μήνυμα εισόδου κόβεται σε μεγάλα blocks των 512 bits (δεκαέξι block των 32 bits little endian ακέραιοι), το μήνυμα συμπληρώνεται έτσι ώστε το μήκος του να διαιρείται από το 512 (κ*512 – 64, όπου κ ακέραιος). Για τη συμπλήρωση αρχικά τοποθετούμε ένα bit 1 στο τέλος του μηνύματος. Αυτό ακολουθείται από όσα μηδενικά χρειάζονται έτσι ώστε το μέγεθος του μηνύματος να γίνει 64 bits λιγότερα από ένα πολλαπλάσιο του 512. Τα υπόλοιπα bits γεμίζονται με ένα 64 bit ακέραιο που αναπαριστά το μήκος του αληθινού μηνύματος σε bits.

Ο κύριος αλγόριθμος MD5 λειτουργεί πάνω σε σύνολο 128 bits, το οποίο χωρίζεται σε 4 λέξεις των 32 bits η κάθε μία που ονομάζονται A, B, C και D. Αυτές αρχικοποιούνται σε μία συγκεκριμένη σταθερά.. Ο κύριος αλγόριθμος ενεργεί πάνω σε κάθε ένα από τα block

μηνυμάτων των 512 bits με τη σειρά. Κάθε block μορφοποιεί το σύνολο. Η διαδικασία της επεξεργασίας ενός block μηνύματος αποτελείται από τέσσερα όμοια στάδια, που ονομάζονται γύροι. Κάθε γύρος αποτελείται από 16 όμοιες λειτουργίες που βασίζονται σε μία μη γραμμική συνάρτηση F. Υπάρχουν τέσσερεις πιθανές συναρτήσεις F και σε κάθε γύρο χρησιμοποιείται διαφορετική. Οι συναρτήσεις είναι :

2.3 Τρωτά σημεία MD5

Επειδή το MD5 κάνει μόνο ένα πέρασμα στα δεδομένα, εάν δύο προθέματα με το ίδιο κατακερματισμό μπορούν να κατασκευαστούν ,τότε ένα κοινό επίθεμα μπορεί να προστεθεί και στα δύο για να γίνει η σύγκρουση πιο εύλογη.

Επειδή αυτές οι τεχνικές εύρεσης σύγκρουσης επιτρέπουν την προηγούμενη κατάσταση κατακερματισμού να προσδιορίζεται αυθαίρετα, μία σύγκρουση μπορεί να υπάρξει σε κάθε επιθυμητό πρόθεμα, για κάθε δοσμένη ακολουθία από χαρακτήρες X (δύο συγκρουόμενα αρχεία μπορούν να προσδιοριστούν ότι και τα δύο ξεκινούν με X.)

Όλο αυτό που απαιτείται για τη δημιουργία δύο συγκρουόμενων αρχείων ,είναι ένα αρχείο πρότυπο, με ένα 128 byte block δεδομένων στοιχισμένο σε ένα 64 byte όριο, το οποίο μπορεί να αλλάξει ελεύθερα από τον αλγόριθμο εύρεσης συγκρούσεων.

Πρόσφατα διάφορες εργασίες έχουν δημιουργήσει τα MD5 « rainbow tables», τα οποία είναι εύκολα online προσπελάσιμα και μπορεί να χρησιμοποιήσουν για να μετατρέψουν πολλούς MD5 κατακερματισμούς σε ακολουθίες που συγκρούονται με την αρχική είσοδο (μήνυμα). Χρησιμοποιείται συνήθως για το σπάσιμο συνθηματικών (password cracking.).

Η χρήση του MD5 στα URLs κάποιων ιστοσελίδων δείχνει ότι το Google μπορεί επίσης να λειτουργήσει σαν εργαλείο για την αντίστροφη αναζήτηση των MD5 κατακερματισμών.

2.4 Χρήση υλικού στην κρυπτογραφία

Οι ολοένα και αυξανόμενες απαιτήσεις για ταχύτητα μεταφοράς δεδομένων που επιβάλλονται από τις τεχνολογικά προηγμένες συσκευές και τα υψηλής ταχύτητας δίκτυα τηλεπικοινωνιών(κινητά τηλέφωνα, ISDN δίκτυα,Bluetooth πρωτόκολλα κ.λπ.) σε συνδυασμό με την πάγια, πλέον απαίτηση για ασφαλή μετάδοση των δεδομένων αυτών γρήγορα φανέρωσαν την επιτακτική ανάγκη να εξεταστεί η αποδοτικότητα υλοποίηση σε ολοκληρωμένα κυκλώματα VLSI όλων των δημοφιλών σχημάτων κρυπτογράφησης

δημοσίου και κρυφού κλειδιού. Ένα πλέον γενικά αποδεκτό κριτήριο αποδοτικότητας ενός κρυπταλγόριθμου είναι η ταχύτητα υλοποίησης σε λογισμικό και οι μικρές απαιτήσεις αποθήκευσης βοηθητικών δεδομένων, είναι η ευκολία υλοποίησης του σε υλικό καθώς και η αποδοτικότητα αυτών των υλοποιήσεων. Πλέον η υλοποίηση κρυπταλγόριθμων σε υλικό είναι μία επιθυμητή και σε ορισμένες περιπτώσεις επιτακτική αντιμετώπιση συγκεκριμένων κρυπτογραφικών εφαρμογών.

Όμως το μειονέκτημα των υλοποιήσεων αυτών δεν είναι άλλο παρά η έλλειψη ευκολίας αλλαγής παραμέτρων του κρυπταλγόριθμου, πράγμα εξαιρετικά εύκολο σε υλοποιήσεις σε λογισμικό. Από την άλλη μεριά, αυτό που μετατρέπει αυτή την έλλειψη αυτής της ευκολίας σε ενδιαφέρον πρόβλημα είναι ότι υπάρχουν κρίσιμες καταστάσεις, ιδιαίτερα στο χώρο των στρατιωτικών εφαρμογών, όπου είναι επιτακτική ανάγκη αλλαγής του αλγορίθμου που βρίσκεται και εκτελείται στο υλικό. Κάτι τέτοιο θα ήταν αναγκαίο, για παράδειγμα, σε καταστάσεις όπου το υλικό βρίσκεται μέσα σε μία απομακρυσμένη και δύσκολα προσπελάσιμη συσκευή και υπάρχουν υποψίες ή και στοιχεία ακόμη που συνηγορούν στο ότι η συσκευή βρίσκεται υπό προσπάθειες κρυπτανάλυσης από αντίπαλες δυνάμεις. Τότε η αλλαγή του κρυπταλγόριθμου που βρίσκεται στο υλικό ουσιαστικά θα δυσκολέψει ή και θα αποτρέψει, ακόμα, τις προσπάθειες αυτές επεκτείνοντας ακόμη περισσότερο το χρόνο ασφαλούς λειτουργίας της συσκευής που περιέχει το υλικό. Εναλλακτικά θα μπορούσαμε να ανανεώναμε, περιοδικά, τον κρυπταλγόριθμο ανάλογα με τις εκτιμήσεις μας σε σχέση με την ασφάλεια του και έτσι να έχουμε ένα προληπτικά ασφαλές (proactively secure) κρυπτοσύστημα, ικανό να αντιστέκεται σε επιχειρούμενες προσπάθειες κρυπτανάλυσης. Πώς είναι όμως δυνατό να αλλάξει κανείς το υλικό στο οποίο έχει «χαραχτεί» ο κρυπταλγόριθμος και να τον αντικαταστήσει με κάποιον άλλο; Ενώ το να αλλάξει κανείς το λογισμικό, θα ήταν το πιο εύκολο πράγμα : απλώς διαγράφεται το πιο παλιό λογισμικό από τη μνήμη και φορτώνεται το νέο(κρυπταλγόριθμος) .Η τεχνολογία και πάλι έρχεται να δώσει τη λύση με τις Επαναπρογραμματιζόμενες Αρχιτεκτονικές Υλικού(Reconfigurable Hardware Architectures). Αυτές οι αρχιτεκτονικές δεν είναι παρά ειδικά ολοκληρωμένα κυκλώματα που έχουν ενσωματωμένη επαναπρογραμματιζόμενη λογική, η οποία μπορεί να αλλάζει δυναμικά κάθε φορά που αυτό απαιτείται από την εφαρμογή μας, αλλάζοντας τη συμπεριφορά της εφαρμογής μας καθώς και την εικόνα που δίνει προς τα έξω. Κάθε φορά, για παράδειγμα, που υποψιάζεται κάποιος ότι η συσκευή που περιέχει αυτά τα κυκλώματα κρυπταναλύεται, μπορεί να «φορτώσει » στα κυκλώματα αυτά μία ειδική ακολουθία από bits που επαναπρογραμματίζει το υλικό και υλοποιεί τον κρυπταλγόριθμο, με αποτέλεσμα αυτός να παρουσιάζει μια εντελώς διαφορετική συμπεριφορά, μπερδεύοντας τους κρυπταναλυτές.

Κεφάλαιο 3. Τεχνολογίες διαδικτύου

3.1 Τεχνολογίες διαδικτύου στην Ηλεκτρονική Ψηφοφορία

Στην ψηφοφορία μέσω internet η ψήφος υποβάλλεται μέσω Internet και τα συστήματα-πελάτες βρίσκονται υπό χαλαρή ή μηδαμινή επίβλεψη (στο σπίτι, στον χώρο εργασίας, σε βιβλιοθήκες, σχολεία, πανεπιστήμια). Η Εγγραφή μπορεί να γίνει με φυσικές (π.χ. σε εκλογικά γραφεία) ή με ηλεκτρονικές διαδικασίες (π.χ. ψηφιακή υπογραφή, μέθοδοι βιομετρικής). Τα στάδια της Επικύρωσης, της Υποβολής και της Καταμέτρησης γίνονται μόνο ηλεκτρονικά.

Η ψηφοφορία μέσω Internet απαιτεί ένα μεγαλύτερο επίπεδο ασφάλειας από αυτό που απαιτείται σε συνήθεις συναλλαγές ηλεκτρονικού εμπορίου. Ενώ η ταυτοποίηση των ψηφοφόρων και η εξασφάλιση της μοναδικότητας της ψήφου ανά ψηφοφόρο, μπορούν εν δυνάμει να αντιμετωπιστούν με τεχνικές που ήδη χρησιμοποιούνται σε εφαρμογές ηλεκτρονικών συστημάτων πληρωμών (π.χ. ψηφιακές υπογραφές - ψηφιακά πιστοποιητικά). Οι επιπλέον απαιτήσεις όπως μυστικότητα και ανωνυμία της ψήφου, οικουμενική επαληθευσιμότητα, καθώς και προστασία από καταναγκασμό, συνθέτουν ένα πολύπλοκο μοντέλο απαιτήσεων ασφάλειας το οποίο έως σήμερα δεν έχει αντιμετωπιστεί με μεθόδους που να είναι ασφαλείς και παράλληλα πρακτικές. Οι επικριτές των συστημάτων ηλεκτρονικής ψηφοφορίας μέσω Internet θεωρούν ότι οι υπάρχουσες τεχνολογίες δεν είναι ακόμα ώριμες να αντιμετωπίσουν τα προβλήματα ασφάλειας που προκύπτουν. Επίσης θεωρούν ότι η υιοθέτηση τους θα οδηγούσε στον κοινωνικό αποκλεισμό των λεγόμενων «ψηφιακά αναλφάβητων» πολιτών

Ένα σύστημα ηλεκτρονικής ψηφοφορίας που πρόκειται να χρησιμοποιηθεί σε εκλογές μεγάλης κλίμακας πρέπει να είναι:

- Δημοκρατικό (Democratic). Μόνο εξουσιοδοτημένοι ψηφοφόροι δικαιούνται να υποβάλλουν ψήφους, και κανείς ψηφοφόρος δε δικαιούται να υποβάλλει περισσότερες από μια ψήφους.

- Ακριβές (Accurate). Καμία ψήφος δεν είναι δυνατόν να αλλοιωθεί, να καταμετρηθεί περισσότερες από μια φορές, να διαγραφεί από τις Εκλογικές Αρχές ή άλλους εσωτερικούς / εξωτερικούς εχθρούς.

- Μυστικό (Secret). Καμία ψήφος δεν είναι δυνατόν να συνδεθεί με τον ψηφοφόρο που την υπέβαλλε, ενώ όλες οι ψήφοι παραμένουν μυστικές για όσο διάστημα διαρκεί η περίοδος υποβολής ψήφων.

- Προστατευμένο από Καταναγκασμό (Uncoercible). Κανένας χρήστης δεν έχει τη δυνατότητα να αποδείξει τη ψήφο του σε κάποιον τρίτο.

- Οικουμενικά Επαληθεύσιμο (Universally Verifiable). Κάθε εξωτερικός παρατηρητής μπορεί να πειστεί ότι το σύστημα είναι ακριβές και ότι το αποτέλεσμα του υπολογισμού των ψήφων της κάλπης αντανακλά τη βούληση των ψηφοφόρων που τις υπέβαλλαν.

- Ανθεκτικό (Robust). Όλες οι απαιτήσεις ασφάλειας ικανοποιούνται πλήρως, παρά τα όποια τυχαία σφάλματα ή τις κακόβουλες συμπεριφορές ορισμένων οντοτήτων (ψηφοφόροι, Αρχές, εσωτερικοί/εξωτερικοί εχθροί).

Πρέπει να τονίσουμε πως σε αρκετά δημοκρατικά καθεστώτα (π.χ. Αυστραλία, Ελλάδα, Βέλγιο), όπου η συμμετοχή των πολιτών στις εκλογές είναι υποχρεωτική από το νόμο, μια επιπλέον απαίτηση ασφάλειας είναι η εύρεση των ψηφοφόρων που δεν άσκησαν το εκλογικό τους δικαίωμα.

Επίσης κάθε σύστημα ηλεκτρονικής ψηφοφορίας πρέπει να είναι εύκολα υλοποιήσιμο, συμβατό με τις διάφορες τεχνολογίες και πλατφόρμες (λειτουργικά συστήματα, αρχιτεκτονικές, εργαλεία πλοήγησης στο Web κ.λ.π), λειτουργικό (Στις εκλογές του 2000 στην Florida των Η.Π.Α ένας μεγάλος αριθμός άκυρων ψήφων υποβλήθηκε λόγω ελλιπούς σχεδίασης των ψηφοδελτίων), και να απευθύνεται σε όλες τις κατηγορίες πληθυσμού ανεξαρτήτως ηλικίας, γλώσσας, φυσικών ικανοτήτων, μόρφωσης, εξοικείωσης με τις τεχνολογίες του Internet κ.λ.π..

Επίσης, το σύστημα πρέπει να υποστηρίζει μια ποικιλία από format ψήφων, συμπεριλαμβανομένων και των λεγόμενων «λευκών» ή άκυρων ψήφων. Το σύστημα θα πρέπει να παρουσιάζει χαμηλή υπολογιστική πολυπλοκότητα και η αποδοτικότητα του να μην επηρεάζεται δραστικά από το μέγεθος του εκλεκτορικού σώματος ή των υποψηφίων (scalability), ενώ οι υπηρεσίες ασφάλειας που προσφέρει θα πρέπει να είναι διαφανείς (transparent) στον χρήστη.

Επίσης θα πρέπει να έχει ληφθεί υπόψη ότι τα κίνητρα για μια επίθεση στην ασφάλεια ενός συστήματος ηλεκτρονικής ψηφοφορίας, ιδιαίτερα σε εθνικές εκλογές, είναι πολλά (πολιτικές επιδιώξεις, χρηματική αμοιβή, διεκδίκηση εξουσίας, εμπλοκή μυστικών υπηρεσιών, τρομοκρατικές οργανώσεις). Το είδος και η μορφή των επιθέσεων ποικίλουν. Στην ηλεκτρονική ψηφοφορία τα ηλεκτρονικά δεδομένα αντιγράφονται, αλλοιώνονται και καταστρέφονται πιο εύκολα από ότι οι φυσικές ψήφοι.

Επιπλέον, όλα τα ηλεκτρονικά συστήματα είναι ευάλωτα σε επιθέσεις από εσωτερικούς εχθρούς (insider attacks) καθώς και σε επιθέσεις Άρνησης Εξυπηρέτησης (Denial Of Service DOS). Τα σημερινά ηλεκτρονικά συστήματα ψηφοφορίας επίσης διαθέτουν ανεπαρκή στοιχεία ελέγχου (audit trail) και δεν παρέχουν οικουμενική επαληθευσιμότητα, με συνέπεια τα αποτελέσματα της ψηφοφορίας να τίθενται υπό αμφισβήτηση.

Επίσης από τη σκοπιά της ασφάλειας, οι εκλογές μέσω Internet είναι περισσότερο ευάλωτες σε επιθέσεις καταναγκασμού (coercion) όπου οι χρήστες αναγκάζονται ή συναλλάσσονται με κάποιον τρίτο για την υποβολή μιας προσυμφωνημένης ψήφου.

Επιπρόσθετα, σε ένα σύστημα εξ' αποστάσεως ψηφοφορίας οι ψηφοφόροι ενδεχομένως θα πρέπει να δημιουργήσουν οι ίδιοι ένα ασφαλές περιβάλλον στις υπολογιστικές τους μηχανές (συστήματα πελάτες), π.χ. προτού υποβάλλουν τη ψήφο τους. Οι έλεγχοι και η πιστοποίηση λογισμικού στα συστήματα ψηφοφορίας μέσω Internet παρουσιάζουν επίσης ιδιαίτερες δυσκολίες, καθώς τα συστατικά μέρη των συστημάτων αυτών είναι συνήθως διαφορετικής προέλευσης και έχουν μυστικό (κλειστό) κώδικα, όπως για παράδειγμα τα σύγχρονα λειτουργικά συστήματα Windows και τα προγράμματα πλοήγησης στο Web.

Παράλληλα, τα συστήματα ψηφοφορίας μέσω Internet είναι περισσότερο ευάλωτα, σε σχέση με τις υπόλοιπες κατηγορίες ηλεκτρονικής ψηφοφορίας, στα εξής σημεία:

- Στα συστήματα-πελάτες: Ιοί τύπου «σκουλήκια» (worms) ή «δούρειοι ίπποι» (trojan horses) μπορούν να αλλοιώσουν τη ψήφο, πολύ πριν αυτή κρυπτογραφηθεί ή αυθεντικοποιηθεί.

Επίσης, ο εισβολέας μπορεί εξ' αποστάσεως να εκμεταλλευτεί «τρύπες» ή λάθη στο σχεδιασμό του λειτουργικού συστήματος ή του προγράμματος πλοήγησης στο Web.

- Στο επίπεδο της επικοινωνίας: Οι κυριότερες επιθέσεις στο επίπεδο της επικοινωνίας είναι οι επιθέσεις πλαστοπροσωπίας (spoofing) DNS ονομάτων ή IP διευθύνσεων, και οι επιθέσεις ενδιάμεσης οντότητας (man in the middle). Η επικοινωνία μεταξύ πελάτη και εξυπηρετητή μπορεί επίσης να απειληθεί και από επιθέσεις τύπου TCP SYN/ACK στο επίπεδο δικτύου του μοντέλου TCP/IP, από επιθέσεις πλαστοπροσωπίας στο φυσικό επίπεδο του μοντέλου OSI (ARP spoofing) κ.λ.π. - Στα συστήματα-εξυπηρετητές: Οι επιθέσεις σε αυτό το επίπεδο είναι παρόμοιες με αυτές στα συστήματα-πελάτες.

Εδώ βέβαια οι επιθέσεις Άρνησης Εξυπηρέτησης (DOS), όπως IP fragmentation ή υπερχείλιση καταχωρητών (buffer overflow), έχουν μεγάλη επικινδυνότητα, αφού μπορούν να υπονομεύσουν ολόκληρη την εκλογική διαδικασία. Το πρόβλημα της συμφόρησης

(bottleneck) είναι παρόμοιο, ως προς τις συνέπειες του, με μια επίθεση Άρνησης Εξυπηρέτησης, με τη διαφορά ότι η συμφόρηση προκαλείται από υπερβολικά μεγάλο αριθμό ταυτόχρονων νομίμων αιτήσεων για σύνδεση με τον εξυπηρετητή, και όχι απαραίτητα από κακόβουλη επίθεση.

Υπάρχουν αρκετές παράμετροι που πρέπει να ληφθούν σοβαρά υπ' όψιν ώστε να γίνει εφικτή η διεξαγωγή ηλεκτρονικών εκλογών μέσω Internet και αυτές είναι :

Πρωτόκολλα / Λογισμικό. Για να είναι ασφαλής η ηλεκτρονική ψηφοφορία, το σύστημα θα πρέπει να υλοποιεί ένα κρυπτογραφικό πρωτόκολλο. Για λόγους αξιοπιστίας επίσης, θεωρούμε πως το σύστημα θα πρέπει να υλοποιηθεί με ανοικτό λογισμικό (open source). Το σύστημα πρέπει επίσης να συνοδεύεται από τους κατάλληλους μηχανισμούς παρακολούθησης (monitoring) και επαλήθευσης (audit) της λειτουργίας του. Ανεξάρτητοι ηλεκτρονικοί ή φυσικοί μηχανισμοί επαλήθευσης ενδεχομένως να αυξήσουν την εμπιστοσύνη των πολιτών στο αποτέλεσμα των εκλογών.

Υποδομή Δημόσιου Κλειδιού. Οι εκλογές μέσω Internet θα γίνουν πλήρως ηλεκτρονικές (από το στάδιο της Εγγραφής έως και το στάδιο της Καταμέτρησης) μόνον όταν υιοθετηθεί και υλοποιηθεί μια ενιαία και ασφαλής Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure – PKI), όπου η ταυτοποίηση των ψηφοφόρων στο στάδιο της Εγγραφής και της Επικύρωσης θα γίνεται με τη χρήση ψηφιακών υπογραφών / ψηφιακών πιστοποιητικών, ενώ η ακεραιότητα και η εμπιστευτικότητα των επικοινωνιών θα υποστηρίζονται από κρυπτογραφικούς αλγόριθμους δημόσιου κλειδιού. Παράλληλα, τα προγράμματα πλοήγησης στο Web θα πρέπει να υποστηρίζουν κρυπτογράφηση και ψηφιακές υπογραφές στο επίπεδο Εφαρμογής του μοντέλου OSI. Επιπλέον, τεχνολογίες όπως SSL/TLS (Secure Socket Layer/Transport Layer Security) και SSH (Secure Shell) πρέπει να επανεκτιμηθούν και να αξιοποιηθούν για την αποτροπή των επιθέσεων πλαστοπροσωπίας και των επιθέσεων ενδιάμεσης οντότητας.

Ασφάλεια Πληροφοριακού Συστήματος. Συνίσταται η χρήση εφαρμογών όπως προγράμματα antivirus και εργαλεία firewalls στα συστήματα-πελάτες, καθώς και **Συστήματα Ελέγχου Εισβολής και firewalls στα συστήματα-εξυπηρετητές**. Παράλληλα επιβάλλεται η χρήση διαδικασιών πλεονασμού (redundancy), ανάκαμψης από επίθεση ή δυσλειτουργία στους εξυπηρετητές (π.χ. συστοιχίες δίσκων RAID, δυνατότητες hot swapping, τεχνικές clustering και load balancing για συστοιχίες εξυπηρετητών, αποθηκευτικές μονάδες DLT) στους εξυπηρετητές ή στο επίπεδο της επικοινωνίας (π.χ. ενσύρματα/ ασύρματα μέσα υψηλού ρυθμού διαμεταγωγής) καθώς και η υιοθέτηση

αυστηρών ελέγχων στην αξιοπιστία του λογισμικού και του υλικού που χρησιμοποιείται. Ένα συμπληρωματικό μέτρο για τη βελτίωση της διαθεσιμότητας του συστήματος θα ήταν και η παράταση της περιόδου υποβολής ηλεκτρονικών ψήφων, πλέον της μίας ημέρας (αρκεί βεβαίως οι ηλεκτρονικές ψήφοι να καταμετρούνται ταυτόχρονα με τις φυσικές, προκειμένου να διατηρηθεί η νομιμότητα των εκλογών).

Νομικά Θέματα. Πέρα από την ολοκλήρωση της θεσμοθέτησης για τη χρήση ηλεκτρονικών υπογραφών στις ηλεκτρονικές συναλλαγές, όπου ήδη έχουν γίνει σημαντικά βήματα, απαραίτητη προϋπόθεση αποτελεί και η ύπαρξη νομολογίας που θα κατοχυρώνει την μυστικότητα της ηλεκτρονικής ψήφου και θα προβλέπει επιθέσεις όπως καταναγκασμός του ψηφοφόρου, ηλεκτρονική εισβολή (hacking) και αλλοίωση εκλογικών συστημάτων ή προσωπικών ψήφων, επιθέσεις πλαστοπροσωπίας, επιθέσεις άρνησης εξυπηρέτησης κ.λ.π.

Σε κάθε περίπτωση, υπάρχει η ανάγκη για σχεδιασμό μιας αυστηρής πολιτικής ασφάλειας που θα προβλέπει διαδικασίες για την αντιμετώπιση απειλών και την ανάκαμψη από επιθέσεις. Το προσωπικό που εμπλέκεται στην ανάπτυξη, λειτουργία και διαχείριση συστημάτων ηλεκτρονικής ψηφοφορίας πρέπει να επιλέγεται προσεκτικά. Καταλήγοντας, θα λέγαμε ότι οι ψηφοφόροι πρέπει να εκπαιδευτούν και να ενημερωθούν για όλες τις πτυχές (σχεδιασμός και υλοποίηση) ενός συστήματος ηλεκτρονικής ψηφοφορίας.

3.2 Βάσεις Δεδομένων

Η αλματώδης ανάπτυξη της επιστήμης της πληροφορικής και των επικοινωνιών τα τελευταία χρόνια έχει καταστήσει την πληροφορία ως ένα από τα βασικότερα και πολυτιμότερα αγαθά. Είναι κοινός τόπος σήμερα η εκτίμηση ότι το αγαθό της πληροφορίας είναι επιθυμητό απ’ όλους τους εργαζόμενους αλλά και τους εκπαιδευόμενους, ώστε να είναι πιο αποδοτικοί, ανταγωνιστικοί αλλά και παραγωγικοί στην εργασία τους.

Τα συστήματα βάσεων δεδομένων τα χρησιμοποιούμε για να μπορούμε να αποθηκεύσουμε, να επεξεργαστούμε αλλά και να εκμεταλλευτούμε αποδοτικά αυτόν τον τεράστιο όγκο των πληροφοριών που αυξάνονται με αλματώδεις ρυθμούς καθημερινά.

Για να δοθεί μια λύση σ’ όλα τα παραπάνω προβλήματα, και με βάση το γεγονός ότι η χρήση των ηλεκτρονικών υπολογιστών και συνεπώς η ηλεκτρονική καταχώρηση και επεξεργασία δεδομένων αυξήθηκε κατακόρυφα ήδη από τη δεκαετία του ’70 στις μεγάλες επιχειρήσεις και άρα είχαμε πάρα πολλές εφαρμογές να επεξεργάζονται δεδομένα σε πάρα πολλά αρχεία ταυτόχρονα, προτάθηκε η συνένωση όλων των αρχείων μιας εφαρμογής. Εκτός, όμως, από τη συνένωση των αρχείων, απαιτείτο και μια σωστή οργάνωσή τους. Δημιουργήθηκαν έτσι οι Τράπεζες Πληροφοριών ή Βάσεις Δεδομένων (Data Bases).

Μια Βάση Δεδομένων (ΒΔ) είναι ένα σύνολο αρχείων με υψηλό βαθμό οργάνωσης τα οποία είναι συνδεδεμένα μεταξύ τους με λογικές σχέσεις, έτσι ώστε να μπορούν να χρησιμοποιούνται από πολλές εφαρμογές και από πολλούς χρήστες ταυτόχρονα. Υπάρχει ένα ειδικό λογισμικό το οποίο μεσολαβεί ανάμεσα στις αρχεία δεδομένων και τις εφαρμογές που χρησιμοποιούν οι χρήστες και αποκαλείται Σύστημα Διαχείρισης Βάσης Δεδομένων (ΣΔΒΔ) ή DBMS (Data Base Management System). Το ΣΔΒΔ είναι στην ουσία ένα σύνολο από προγράμματα και υπορουτίνες που έχουν να κάνουν με τον χειρισμό της βάσης δεδομένων, όσον αφορά τη δημιουργία, τροποποίηση, διαγραφή στοιχείων, με ελέγχους ασφαλείας κ.ά.

Οι χρήστες των εφαρμογών αντλούν τα στοιχεία που τους ενδιαφέρουν από τη βάση δεδομένων χωρίς να είναι σε θέση να γνωρίζουν με ποιο τρόπο είναι οργανωμένα τα δεδομένα σ' αυτήν. Το ΣΔΒΔ παίζει τον ρόλο του μεσάζοντα ανάμεσα στον χρήστη και τη βάση δεδομένων και μόνο μέσω του ΣΔΒΔ μπορεί ο χρήστης να αντλήσει πληροφορίες από τη βάση δεδομένων. Ένα ΣΔΒΔ μπορεί να είναι εγκατεστημένο σ' έναν μόνο υπολογιστή ή και σ' ένα δίκτυο υπολογιστών και μπορεί να χρησιμοποιείται από έναν χρήστη ή και από πολλούς χρήστες.

Ένα Σύστημα Βάσης Δεδομένων (ΣΒΔ) ή DBS (Data Base System) αποτελείται από το υλικό, το λογισμικό, τη βάση δεδομένων και τους χρήστες. Είναι δηλαδή ένα σύστημα με το οποίο μπορούμε να αποθηκεύσουμε και να αξιοποιήσουμε δεδομένα με τη βοήθεια ηλεκτρονικού υπολογιστή. Αναλυτικά :

- Το υλικό (hardware) αποτελείται όπως είναι γνωστό από τους ηλεκτρονικούς υπολογιστές, τα περιφερειακά, τους σκληρούς δίσκους, τις μαγνητικές ταινίες κ.ά., όπου είναι αποθηκευμένα τα αρχεία της βάσης δεδομένων αλλά και τα προγράμματα που χρησιμοποιούνται για την επεξεργασία τους.

- Το λογισμικό (software) είναι τα προγράμματα που χρησιμοποιούνται για την επεξεργασία των δεδομένων (στοιχείων) της βάσης δεδομένων.

- Η βάση δεδομένων (data base) αποτελείται από το σύνολο των αρχείων όπου είναι αποθηκευμένα τα δεδομένα του συστήματος. Τα στοιχεία αυτά μπορεί να βρίσκονται αποθηκευμένα σ' έναν φυσικό υπολογιστή αλλά και σε περισσότερους. Όμως, στον χρήστη δίνεται η εντύπωση ότι βρίσκονται συγκεντρωμένα στον ίδιο υπολογιστή. Τα δεδομένα των αρχείων αυτών είναι ενοποιημένα (data integration), δηλ. δεν υπάρχει πλεονασμός (άσκοπη επανάληψη) δεδομένων και μερισμένα (data sharing), δηλ. υπάρχει δυνατότητα ταυτόχρονης προσπέλασης των δεδομένων από πολλούς χρήστες. Ο κάθε χρήστης έχει

διαφορετικά δικαιώματα και βλέπει διαφορετικό κομμάτι της βάσης δεδομένων, ανάλογα με τον σκοπό για τον οποίο συνδέεται.

- Οι χρήστες (users) μιας βάσης δεδομένων χωρίζονται στις εξής κατηγορίες :

o Τελικοί χρήστες (end users). Χρησιμοποιούν κάποια εφαρμογή για να παίρνουν στοιχεία από μια βάση δεδομένων, έχουν τις λιγότερες δυνατότητες επέμβασης στα στοιχεία της βάσης δεδομένων, χρησιμοποιούν ειδικούς κωδικούς πρόσβασης και το σύστημα τούς επιτρέπει ανάλογα πρόσβαση σε συγκεκριμένο κομμάτι της βάσης δεδομένων.

o Προγραμματιστές εφαρμογών (application programmers). Αναπτύσσουν τις εφαρμογές του ΣΒΔ σε κάποια από τις γνωστές γλώσσες προγραμματισμού.

o Διαχειριστής δεδομένων (data administrator – DA). Έχει τη διοικητική αρμοδιότητα και ευθύνη για την οργάνωση της βάσης δεδομένων και την απόδοση δικαιωμάτων πρόσβασης στους χρήστες.

o Διαχειριστής βάσης δεδομένων (database administrator – DBA). Λαμβάνει οδηγίες από τον διαχειριστή δεδομένων και είναι αυτός που διαθέτει τις τεχνικές γνώσεις και αρμοδιότητες για τη σωστή και αποδοτική λειτουργία του ΣΔΒΔ.

3.3 Η Αρχιτεκτονική των ΣΔΒΔ

Όπως είδαμε νωρίτερα, ένα ΣΔΒΔ (Σύστημα Διαχείρισης Βάσης Δεδομένων) έχει σαν αποστολή τη διαχείριση των δεδομένων των αρχείων της βάσης, δηλ. την προσθήκη, διαγραφή, τροποποίηση εγγραφών, την αναζήτηση μέσα στις εγγραφές κ.ά.). Το ΣΔΒΔ δέχεται αιτήσεις από τους χρήστες των εφαρμογών και επικοινωνεί με τα αρχεία της βάσης δεδομένων για να τις διεκπεραιώσει.

Αυτή η κοινή διεπαφή (interface) των εφαρμογών με τα αρχεία αποκαλείται λογική διεπαφή. Οι εφαρμογές που δημιουργούμε δεν απασχολούνται με τον τρόπο που είναι αποθηκευμένα τα δεδομένα, πόσο χώρο καταλαμβάνουν κοκ και αυτή η ιδιότητα είναι γνωστή ως ανεξαρτησία δεδομένων.

Αυτό σημαίνει πρακτικά ότι οποιαδήποτε αλλαγή στον τρόπο οργάνωσης των αρχείων της βάσης δεδομένων δεν θα συνεπάγεται και αλλαγή στις εφαρμογές• ένα πρόβλημα που ταλαιπωρούσε πολύ τους προγραμματιστές παλαιοτέρων εποχών. Ακόμη, η προσθήκη, η κατάργηση ή και η τροποποίηση κάποιων εφαρμογών δεν θα έχει καμία επίπτωση στον τρόπο οργάνωσης των αρχείων της βάσης δεδομένων. Στα ΣΔΒΔ έχει επικρατήσει η

λεγόμενη αρχιτεκτονική των τριών επιπέδων (βαθμίδων), όπου τα τρία επίπεδα είναι τα εξής:

- Εσωτερικό επίπεδο (internal level), έχει να κάνει με την αποθήκευση των αρχείων στον σκληρό δίσκο, δηλ. την πραγματική ή φυσική κατάστασή τους.
- Εξωτερικό επίπεδο (external level), έχει να κάνει με τους χρήστες είτε αυτοί είναι απλοί χειριστές, είτε προγραμματιστές ή και οι διαχειριστές της βάσης δεδομένων.
- Εννοιολογικό επίπεδο (conceptual level), είναι ένα ενδιάμεσο επίπεδο που διασυνδέει τα δύο άλλα επίπεδα και έχει να κάνει με
- τη λογική σχεδίαση των αρχείων της βάσης δεδομένων.

Οι Οντότητες (Entities)

Με τον όρο οντότητα (entity) εννοούμε ένα αντικείμενο, ένα πρόσωπο, μια κατάσταση και γενικά ο,τιδήποτε μπορεί να προσδιορισθεί σαν ανεξάρτητη ύπαρξη (αυτόνομη μονάδα του φυσικού κόσμου). Για παράδειγμα, σε μια βάση δεδομένων μιας εμπορικής εταιρείας, οντότητες μπορεί να είναι οι εργαζόμενοι, οι πελάτες, οι προμηθευτές, οι παραγγελίες, τα είδη της αποθήκης (προϊόντα) κ.ά.

Το Μοντέλο Οντοτήτων Συσχετίσεων (Entity Relationship Model, ER Model) είναι μια διαγραμματική αναπαράσταση της δομής μιας βάσης δεδομένων και χρησιμοποιείται κατά τη φάση του λογικού σχεδιασμού της βάσης. Δηλαδή, δεν ασχολείται με τον τρόπο που αποθηκεύονται τα δεδομένα της βάσης, αλλά με την ταυτοποίηση των δεδομένων και με τον τρόπο με τον οποίο αυτά συσχετίζονται μεταξύ τους.

Θα δούμε ένα παράδειγμα μιας εταιρείας, η οποία περιέχει δεδομένα που αφορούν τους υπαλλήλους της (employees), τα τμήματά της (departments) και τα έργα (projects) που έχουν αναλάβει αυτά τα τμήματα. Ένα τμήμα της εταιρείας μπορεί να εποπτεύει ένα ή περισσότερα έργα (projects) και ένας υπάλληλος ανήκει σ’ ένα μόνο τμήμα της εταιρείας αλλά μπορεί να απασχολείται ταυτόχρονα σε πολλά έργα, τα οποία δεν είναι υποχρεωτικό να παρακολουθούνται από το ίδιο τμήμα.

Ιδιότητες (Attributes)

Με τον όρο ιδιότητα ή χαρακτηριστικό ή και πεδίο (attribute) μιας οντότητας, αναφερόμαστε σ’ ένα από τα συστατικά της στοιχεία που την περιγράφουν και την κάνουν να ξεχωρίζει από τα άλλα στοιχεία της ίδιας οντότητας. Για παράδειγμα, η οντότητα

ΠΕΛΑΤΗΣ μπορεί να έχει ως ιδιότητες (χαρακτηριστικά) τον κωδικό, το επώνυμο, το όνομα, τη διεύθυνση, το τηλέφωνο, το ΑΦΜ κ.ά., με τη βοήθεια των οποίων μπορούμε να ξεχωρίσουμε τους πελάτες μεταξύ τους.

Επίσης, η οντότητα ΠΑΡΑΓΓΕΛΙΑ μπορεί να έχει ως ιδιότητες (χαρακτηριστικά) τον κωδικό, τον αριθμό παραστατικού, την ημερομηνία, τον κωδικό πελάτη, το προϊόν κ.ά., με τη βοήθεια των οποίων μπορούμε να ξεχωρίσουμε τις παραγγελίες μεταξύ τους Στο παράδειγμα της εταιρείας, μπορούμε να ορίσουμε έναν τύπο οντότητας για τους υπαλλήλους της εταιρείας (EMPLOYEE), έναν τύπο οντότητας για τα τμήματα που έχει η εταιρεία (DEPARTMENT) και έναν τύπο οντότητας για τα έργα που έχει αναλάβει η εταιρεία (PROJECT). Καθένας από τους παραπάνω τύπους οντοτήτων περιγράφεται από ένα όνομα και από το σύνολο των πεδίων που περιέχει. Οι πληροφορίες αυτές αποτελούν το σχήμα (schema) της οντότητας.

Πρωτεύον Κλειδί (Primary Key)

Πρωτεύον κλειδί ή πεδίο κλειδί (primary key) μιας οντότητας καλείται εκείνη η ιδιότητα (ή ο συνδυασμός ιδιοτήτων) που έχει μοναδική τιμή για όλα τα στιγμιότυπα (εμφανίσεις) της οντότητας. Για παράδειγμα, στην οντότητα ΠΕΛΑΤΗΣ πρωτεύον κλειδί είναι ο κωδικός πελάτη, στην οντότητα ΠΑΡΑΓΓΕΛΙΑ πρωτεύον κλειδί μπορεί να είναι ο κωδικός παραγγελίας ή ο αριθμός παραστατικού κοκ.

Υπάρχουν περιπτώσεις όπου το πεδίο κλειδί ενός τύπου οντότητας μπορεί να μην είναι απλό αλλά σύνθετο, να αποτελείται δηλαδή από πολλά απλά πεδία και τότε η συνθήκη της μοναδικότητας για την τιμή του κλειδιού δεν εφαρμόζεται σε κάθε πεδίο του σύνθετου κλειδιού αλλά στο σύνολο του συνδυασμού αυτών των πεδίων.

Συσχετίσεις (Relationships)

Με τον όρο συσχέτιση (relationship) αναφερόμαστε στον τρόπο σύνδεσης (επικοινωνίας) δύο ξεχωριστών οντοτήτων, ώστε να μπορούμε να αντλούμε στοιχεία (πληροφορίες) από τον συνδυασμό τους.

Για παράδειγμα, η οντότητα ΓΙΑΤΡΟΣ συσχετίζεται με την οντότητα ΑΣΘΕΝΗΣ αλλά και με την οντότητα ΚΛΙΝΙΚΗ στη βάση δεδομένων ενός νοσοκομείου. Μπορούμε να δεχθούμε ότι ένας γιατρός παρακολουθεί (συσχετίζεται με) πολλούς ασθενείς, αλλά ένας ασθενής παρακολουθείται από (συσχετίζεται με) έναν μόνο γιατρό και επίσης ένας γιατρός συσχετίζεται με (ανήκει σε) μία μόνο κλινική, αλλά μια κλινική συσχετίζεται με (απασχολεί) πολλούς γιατρούς.

Στο παράδειγμα της εταιρείας, η οντότητα EMPLOYEE συσχετίζεται με την οντότητα DEPARTMENT και η οντότητα DEPARTMENT συσχετίζεται με την οντότητα PROJECTS. Ένας υπάλληλος ανήκει σ' ένα μόνο τμήμα και ένα τμήμα μπορεί να έχει πολλούς υπαλλήλους. Επίσης, ένα τμήμα εποπτεύει πολλά έργα αλλά ένα έργο εποπτεύεται από ένα μόνο τμήμα.

Τα Κλειδιά

Όπως είδαμε και νωρίτερα, με τον όρο κλειδί (key) ή πιο σωστά πρωτεύον κλειδί (primary key) αναφερόμαστε σε μια ιδιότητα (πεδίο), ή σπανιότερα σ' ένα σύνολο ιδιοτήτων (πεδίων), η τιμή της οποίας είναι μοναδική σ' ολόκληρη την οντότητα (πίνακας). Στην πράξη, το πρωτεύον κλειδί έχει διαφορετική τιμή για κάθε εμφάνιση της οντότητας ή για κάθε γραμμή (εγγραφή) του πίνακα και ποτέ δεν μπορεί να έχει μηδενική (κενή) τιμή (null). Προσοχή, άλλο πράγμα είναι ο αριθμός 0 και άλλο πράγμα είναι η κενή τιμή (null), δηλ. η μη ύπαρξη τιμής.

Ο συνδυασμός δύο ή και περισσοτέρων ιδιοτήτων (πεδίων) για τη δημιουργία ενός πρωτεύοντος κλειδιού αποκαλείται σύνθετο κλειδί. Ένα παράδειγμα σύνθετου κλειδιού θα μπορούσε να είναι ο συνδυασμός των ιδιοτήτων Επώνυμο, Όνομα και Πατρώνυμο, εφόσον φυσικά είμαστε απολύτως βέβαιοι ότι δεν υπάρχουν δύο ή και περισσότερα άτομα με κοινές τιμές στις παραπάνω ιδιότητες.

Ξένο κλειδί αποκαλείται μια ιδιότητα (πεδίο) που είναι πρωτεύον κλειδί σε μια οντότητα (πίνακας) αλλά που υπάρχει και σε μια άλλη οντότητα (πίνακας) σαν απλή ιδιότητα. Τα ξένα κλειδιά είναι απαραίτητα για να μπορέσουμε να κάνουμε τις συσχετίσεις (συνδέσεις, επικοινωνίες) ανάμεσα στις οντότητες (πίνακες).

3.3 Γλώσσα Server Side PHP

Η PHP, της οποίας τα αρχικά αντιπροσωπεύουν το "PHP: Hypertext Preprocessor" είναι μια ευρέως χρησιμοποιούμενη, ανοιχτού κώδικα, γενικού σκοπού scripting γλώσσα προγραμματισμού, η οποία είναι ειδικά κατάλληλη για ανάπτυξη εφαρμογών για το Web και μπορεί να ενσωματωθεί στην HTML.

Αυτό που είναι διαφορετικό από ένα script γραμμένο σε άλλες γλώσσες προγραμματισμού όπως η Perl ή η C : Αντί να γράφετε ένα πρόγραμμα με πολλές εντολές για να εξάγετε

HTML, γράφετε ένα HTML script με κάποιο ενσωματωμένο κώδικα για να κάνει κάτι (σε αυτή την περίπτωση, να εμφανίζει κάποιο κείμενο). Ο κώδικας PHP είναι εσώκλειστος σε ειδικά tags (ετικέτες) αρχής και τέλους που σας επιτρέπουν να μεταφέρεστε μέσα και έξω από το "PHP mode" (PHP τρόπο λειτουργίας).

Αυτό που διαχωρίζει την PHP από κάτι σαν client-side Javascript είναι ότι ο κώδικας εκτελείται στον server (εξηπηρετητή). Αν είχατε ένα script σαν το παραπάνω στον server σας, ο client θα έπαιρνε τα αποτελέσματα της εκτέλεσης αυτού του script, χωρίς να υπάρχει κανένας τρόπος να καταλάβει τι κώδικας υπάρχει από κάτω. Μπορείτε ακόμη να ρυθμίσετε τον web server σας να χειρίζεται όλα τα HTML αρχεία σας με την PHP, και τότε πραγματικά δεν υπάρχει τρόπος ο χρήστης να καταλάβει τι έχετε κάτω από το μανίκι σας.

Τα καλύτερο στην PHP είναι ότι είναι εξαιρετικά απλή αλλά προσφέρει πολλά προηγμένα χαρακτηριστικά για ένα επαγγελματία προγραμματιστή.

Η PHP επικεντρώνεται κυρίως στο server-side scripting, έτσι μπορείτε να κάνετε οτιδήποτε ένα άλλο CGI πρόγραμμα μπορεί να κάνει, όπως να μαζέψει δεδομένα, να παράγει δυναμικό περιεχόμενο σελίδων, ή να στείλει και να πάρει cookies. Η PHP μπορεί να κάνει πολύ περισσότερα.

Υπάρχουν τρεις κύριοι τομείς που χρησιμοποιείται ένα PHP script.

Server-side scripting. Αυτό είναι το πιο παραδοσιακό και το κύριο πεδίο για την PHP. Χρειάζεστε τρία πράγματα για να δουλέψει. Τον PHP μεταγλωττιστή (parser) (CGI ή server module), ένα webserver (εξηπηρετητή σελίδων) και ένα web browser ("φυλλομετρητή"). Πρέπει να τρέξετε τον webserver, με μια συνδεδεμένη εγκατάσταση της PHP. Μπορείτε να προσπελάσετε τα αποτελέσματα του PHP προγράμματος με ένα web browser, βλέποντας την σελίδα PHP μέσα από τον server

Command line scripting. Μπορείτε να φτιάξετε ένα PHP script για να το τρέχετε χωρίς server ή browser. Χρειάζεστε μόνο τον PHP μεταγλωττιστή για να την χρησιμοποιήσετε με αυτό τον τρόπο. Αυτός ο τύπος είναι ιδανικός για script που εκτελούνται συχνά με τη χρήση της cron (σε *nix ή Linux) ή με τον Task Scheduler (στα Windows). Αυτά τα script μπορούν επίσης να χρησιμοποιηθούν για απλές εργασίες επεξεργασίες κειμένου.

Εγγραφή client-side GUI εφαρμογών (Γραφικά περιβάλλοντα χρηστών). Η PHP ίσως να μην είναι η πιο καλή γλώσσα για να γράψει κανείς παραθυριακές εφαρμογές, αλλά αν ξέρετε PHP πολύ καλά και θέλετε να χρησιμοποιήσετε κάποια προχωρημένα χαρακτηριστικά της PHP στις client-side εφαρμογές σας, μπορείτε επίσης να χρησιμοποιήσετε το PHP-GTK για

αυτού του είδους τα προγράμματα. Έχετε επίσης τη δυνατότητα να γράφετε cross-platform εφαρμογές με αυτό τον τρόπο. Το PHP-GTK είναι μια επέκταση της PHP και δεν συμπεριλαμβάνεται στην κύρια διανομή.

Βασικό πλεονέκτημα της PHP είναι ότι, μπορεί να χρησιμοποιηθεί σε όλα τα κύρια λειτουργικά συστήματα, συμπεριλαμβανομένου του Linux, πολλών εκδοχών του Unix (HP-UX, Solaris και OpenBSD), Microsoft Windows, Mac OS X, RISC OS και πιθανώς σε άλλα. Η PHP υποστηρίζει επίσης τους Apache, Microsoft Internet Information Server, Personal Web Server, Netscape και iPlanet servers, Oreilly Website Pro server, Caudium, Xitami, OmniHTTPd, Sambar και πολλούς άλλους webserver. Για την πλειοψηφία των server η PHP έχει ένα module, για τους υπόλοιπους η PHP μπορεί να λειτουργήσει ως ένας CGI επεξεργαστής.

Έτσι με την PHP έχουμε την ελευθερία επιλογής ενός λειτουργικού συστήματος και ενός web server. Επιπλέον, έχουμε επίσης την ελευθερία να χρησιμοποιήσουμε συναρτησιακό (procedural) ή αντικειμενοστρεφή (object oriented) προγραμματισμό ή μια ανάμειξη τους. Αν και η παρούσα έκδοση δεν υποστηρίζει όλα τα πρότυπα χαρακτηριστικά, μεγάλες βιβλιοθήκες κώδικα και μεγάλες εφαρμογές (συμπεριλαμβανομένης και της βιβλιοθήκης PEAR) είναι γραμμένες μόνο με αντικειμενοστρεφή κώδικα.

Με την PHP δεν είμαστε περιορισμένοι να εξάγουμε HTML. Οι δυνατότητες της PHP συμπεριλαμβάνουν την εξαγωγή εικόνων, αρχείων PDF, ακόμη και ταινίες Flash (χρησιμοποιώντας τα libswf και Ming) παράγονται αμέσως. Μπορούμε επίσης να εξάγουμε εύκολα οποιοδήποτε κείμενο όπως XHTML και οποιοδήποτε άλλο XML αρχείο. Η PHP μπορεί να δημιουργεί αυτόματα αυτά τα αρχεία και να τα αποθηκεύει στο σύστημα αρχείων, αντί να τα εκτυπώνει, αποτελώντας έτσι μια server-side cache για το δυναμικό μας περιεχόμενο.

Ένα από τα πιο δυνατά και σημαντικά χαρακτηριστικά της PHP είναι η υποστήριξη που έχει για ένα μεγάλο σύνολο βάσεων δεδομένων. Η συγγραφή μιας σελίδας που υποστηρίζει βάσεις δεδομένων είναι εξαιρετικά απλή. Οι εξής βάσεις δεδομένων υποστηρίζονται μέχρι στιγμής:

Adabas D	Ingres	Oracle (OCI7 and OCI8)

DBase	InterBase	Ovrimos
Empress	FrontBase	PostgreSQL
FilePro (read-only)	mSQL	Solid
Hyperwave	Direct MS-SQL	Sybase
IBM DB2	MySQL	Velocis
Informix	ODBC	Unix dbm

Έχουμε επίσης μια αφαιρετική επέκταση DBX βάσεων δεδομένων (DBX database abstraction extension) που μας επιτρέπει διάφανα να χρησιμοποιήσουμε οποιαδήποτε βάση δεδομένων υποστηρίζεται από αυτή την επέκταση. Επιπλέον η PHP υποστηρίζει το ODBC, το Open Database Connection standard (Ανοιχτό πρότυπο Σύνδεσης Βάσεων δεδομένων) έτσι μπορούμε να συνδέσουμε σε οποιαδήποτε βάση δεδομένων που υποστηρίζει αυτό το παγκόσμιο πρότυπο.

Η PHP έχει επίσης υποστήριξη για επικοινωνία με άλλες υπηρεσίες χρησιμοποιώντας πρωτόκολλα όπως LDAP, IMAP, SNMP, NNTP, POP3, HTTP, COM (στα Windows) και αμέτρητα άλλα. Μπορούμε επίσης να ανοίξουμε raw network sockets και να αλληλεπιδράσουμε με οποιοδήποτε άλλο πρωτόκολλο. Η PHP έχει ακόμη υποστήριξη για την περίπλοκη ανταλλαγή δεδομένων WDDX μεταξύ σχεδόν όλων των Web programming γλωσσών. Μιλώντας για δια-επικοινωνία, η PHP υποστηρίζει instantiation αντικειμένων Java και τα χρησιμοποιεί διάφανα σαν αντικείμενα PHP. Μπορείτε επίσης να χρησιμοποιήσουμε την CORBA επέκταση μας για να προσπελάσετε remote (απομακρυσμένα) αντικείμενα.

Η PHP έχει εξαιρετικά χρήσιμα χαρακτηριστικά επεξεργασίας κειμένων, από την POSIX επέξταση ή τις Perl regular expressions μέχρι XML parsing αρχείων. Για τη μεταγλώττιση και την πρόσβαση αρχείων XML, υποστηρίζουμε τα πρότυπα SAX και DOM. Μπορούμε να χρησιμοποιήσουμε την XSLT επέκταση μας για να μετατρέψουμε τα XML αρχεία σε άλλες μορφές.

Καθώς χρησιμοποιούμε την PHP στον τομέα του ηλεκτρονικού εμπορίου, θα βρούμε τις Cybercash payment, CyberMUT, VeriSign Payflow Pro και CCVS συναρτήσεις χρήσιμες για τα online προγράμματα πληρωμής σας.

Η επικοινωνία της PHP με μία βάση δεδομένων είναι αρκετά εύκολη μια και το μόνο που χρειάζεται είναι να καλέσουμε εντολές SQL και να εκτελέσουμε στο DATABASE SERVER.

3.4 Κρυπτογράφηση στο Διαδίκτυο

Όπως αναφέραμε και προηγουμένως, η κρυπτογράφηση είναι ένας τρόπος ενίσχυσης της ασφάλειας ενός μηνύματος ή ενός αρχείου κατά τον οποίο τα περιεχόμενα αλλάζουνε με τέτοιο τρόπο ώστε να μπορεί να τα διαβάσει μόνο κάποιος που έχει το κατάλληλο κλειδί κρυπτογράφησης. Για παράδειγμα στο ηλεκτρονικό εμπόριο που είναι ευρέως διαδεδομένο στο διαδίκτυο, εάν αγοράσει κάποιος κάτι μέσω κάποιας τοποθεσίας στο web, τότε οι πληροφορίες για την συναλλαγή (όπως η διεύθυνση, ο αριθμός τηλεφώνου και ο αριθμός της πιστωτικής κάρτας) συνήθως κρυπτογραφούνται για την εξασφάλισή τους.

Στο διαδίκτυο χρησιμοποιούνται σειρά αλγορίθμων κρυπτογράφησης όπως και MD5 που αναφέραμε προηγουμένως. Ειδικά στις ηλεκτρονικές ψηφοφορίες και ειδικά σε αυτές που έχουν μυστική ψηφοφορία είναι ιδιαίτερα σημαντικό να κρυπτογραφούνται τα δεδομένα ώστε να μην μπορεί κανείς να βρίσκει τα στοιχεία των ατόμων που συμμετέχουν και να κάνει προσπάθειες να τα επηρεάσει ή να αλλάξει την πιθανή ψήφο τους.

Όμως όταν ο χρήστης θέλει να δει τα στοιχεία που καταχώρησε τότε θα πρέπει να μπορεί να τα βλέπει (εξαιρώντας το password). Έτσι χρειαζόμαστε και αλγόριθμους αναστρέψιμους δηλαδή που να μπορούν να κρυπτογραφούνται αλλά και να αποκρυπτογραφούνται.

Για να μπορέσουμε να έχουμε αποκρυπτογράφηση πρέπει να χρησιμοποιήσουμε ασύμμετρους ή συμμετρικούς αλγόριθμους όπου αυτοί χρησιμοποιούνται στις ηλεκτρονικές ψηφοφορίες.

Στους συμμετρικούς αλγόριθμους το κλειδί κρυπτογράφησης μπορεί να υπολογιστεί από το κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση και το ανάποδο. Μάλιστα στις περισσότερες περιπτώσεις τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης είναι τα ίδια. Αυτοί οι αλγόριθμοι χρειάζονται την συμφωνία μεταξύ του αποστολέα και του παραλήπτη για το κλειδί που θα χρησιμοποιηθεί, για να μπορέσουν να επικοινωνήσουν με ασφάλεια. Η ασφάλεια των αλγόριθμων βασίζεται στην μυστικότητα αυτού του κλειδιού.

Για όσο καιρό επιθυμούμε η επικοινωνία να παραμείνει μυστική, για τον ίδιο καιρό πρέπει και το κλειδί να παραμείνει μυστικό.

Οι συμμετρικοί αλγόριθμοι μπορούν να διαιρεθούν σε δύο υποκατηγορίες: α) αλγόριθμοι ροής (stream ciphers) οι οποίοι λειτουργούν bit προς bit και β) μπλοκ αλγόριθμοι (block ciphers) οι οποίοι λειτουργούν πάνω σε κομμάτια δεδομένων (συνήθως των 64 bit).

Παραδείγματα συμμετρικών αλγορίθμων είναι οι DES, IDEA, RC5 και SAFER.

Οι ασύμμετροι αλγόριθμοι ή αλγόριθμοι δημόσιου κλειδιού είναι σχεδιασμένοι έτσι ώστε το κλειδί που χρησιμοποιείται για την κρυπτογράφηση να είναι διαφορετικό από το κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση. Πέρα από αυτό, το κλειδί αποκρυπτογράφησης δεν μπορεί να υπολογιστεί από το κλειδί κρυπτογράφησης. Οι αλγόριθμοι αυτοί καλούνται και "δημόσιου κλειδιού" γιατί το κλειδί κρυπτογράφησης μπορεί να δημοσιοποιηθεί. Ο καθένας μπορεί να κρυπτογραφήσει ένα μήνυμα με το δημόσιο κλειδί αλλά μόνο αυτός που διαθέτει το αντίστοιχο ιδιωτικό κλειδί μπορεί να το αποκρυπτογραφήσει.

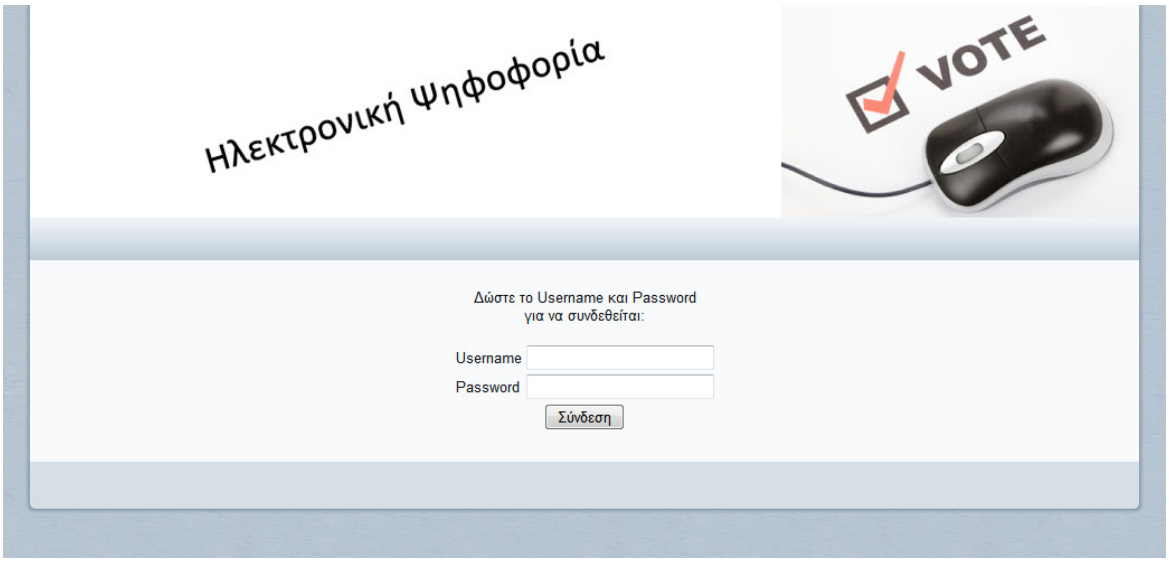
Οι συμμετρικοί αλγόριθμοι είναι πολύ πιο γρήγοροι, εφαρμοσμένοι είτε σε υλικό είτε σε λογισμικό. από τους ασύμμετρους αλγόριθμους. Ως εκ τούτου οι συμμετρικοί αλγόριθμοι χρησιμοποιούνται για την κρυπτογράφηση του κυρίου μέρους των δεδομένων, ενώ οι αλγόριθμοι δημόσιου κλειδιού βρίσκουν κατάλληλη εφαρμογή σε πρωτόκολλα ανταλλαγής κλειδιών και ψηφιακών υπογραφών.

Κεφάλαιο 4. Εφαρμογή Ηλεκτρονικής Ψηφοφορίας

4.1 Περιγραφή της Εφαρμογής

Με βάση όσα εξετάσαμε στα παραπάνω κεφάλαια έχουμε δημιουργήσαμε κατάλληλη εφαρμογή ώστε να μπορεί να χρησιμοποιηθεί για μια σειρά ψηφοφοριών.

Στην εφαρμογή μας καθορίζονται χρήστες που ανήκουν σε δύο βασικές κατηγορίες. Τους διαχειριστές και τους απλούς χρήστες. Οι απλοί χρήστες είναι οι ψηφοφόροι ενώ οι διαχειριστές είναι οι εξουσιοδοτημένοι χρήστες που ορίζουν όλες τις παραμέτρους του προγράμματος. Οι παράμετροι είναι οι ομάδες των χρηστών, οι ψηφοφορίες, οι χρήστες κ.α.



Παραπάνω φαίνεται η αρχική οθόνη της εφαρμογής.

Ανάλογα με τον κωδικό του χρήστη η εφαρμογή διακρίνει ποιος ακριβώς είναι ο χρήστης και έτσι εμφανίζει το ανάλογο μενού. Υπάρχουν δύο μενού το μενού του χρήστη και το μενού του διαχειριστή.

Έτσι ανάλογα με το είδος του χρήστη με βάση το μενού διακρίνονται οι διαδικασίες που μπορεί να χρησιμοποιήσει ο χρήστης και ποιες ο διαχειριστής.

4.3 Περιγραφή της Βάσης – ER Διάγραμμα

Για την περιγραφή της βάση έχουμε τα παρακάτω : Υπάρχουν θέματα προς ψήφιση, που έχουν συγκεκριμένες προτάσεις. Οι χρήστες (ψηφοφόροι) που ψηφίζουν τις προτάσεις.

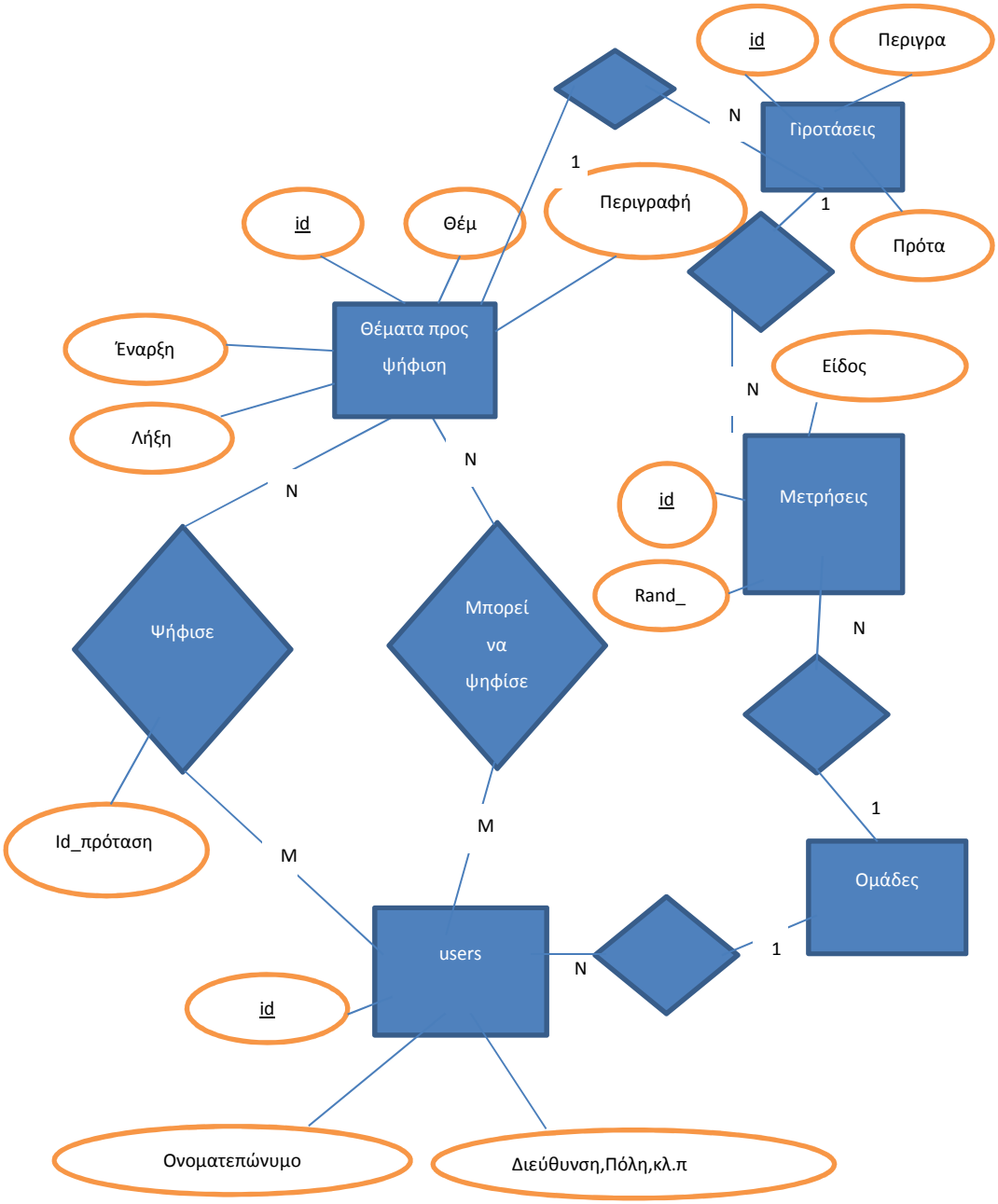
Κάθε χρήστης ανήκει σε μία κατηγορία (π.χ. ηλικιακή π.χ. από 18-30, 30-50, 50-70, 70 και πάνω).

Το εκλογικό σώμα ενός θέματος καθορίζεται από την σχέση πολλά προς πολλά του θέματος προς ψήφιση με τους χρήστες. Έτσι ένας χρήστης μπορεί να ανήκει στο εκλογικό σώμα ενός θέματος αλλά μπορεί να μην ανήκει σε κάποιο άλλο θέμα.

Κάθε φορά που ψηφίζει ένα χρήστης ένα θέμα καταχωρείται μέσα από την σχέση ψήφισε και έτσι δεν τον αφήνει να ψηφίσει πάλι (εξασφάλιση μιας μόνο ψήφου).

Στην σχέση αυτή δεν κρατάμε τι ψήφισε ο χρήστης όταν η ψήφος είναι μυστική. Διαφορετικά κρατάμε το id_rand ένα τυχαίο αριθμό που τον χαρακτηρίζει που τον περιγράφουμε στον πίνακα Μετρήσεις. Κάθε φορά που ψηφίζει ένας χρήστης στον πίνακα μετρήσεις καταχωρείται το είδος ψήφου για την πρόταση που ψήφισε (συνήθως είναι θετικό αλλά το είδος εξασφαλίζει περίπτωση ψηφοφορίας και με αρνητική ψήφο). Στον πίνακα καταχωρείται και η κατηγορία ώστε να μπορούμε να εξάγουμε και στατιστικά στοιχεία. Επίσης για να εξασφαλίσουμε και την περίπτωση ψηφορίας με πολλαπλές επιλογές (π.χ. μπορεί ο ψηφοφόρος να βάλει σταυρό σε 2 ή περισσότερα πρόσωπα ή προτάσεις) δημιουργούμε ένα id_rand δηλαδή ένα τυχαίο μοναδικό αριθμό που κατά την ψήφιση που κάνει ένας ψηφοφόρος να μένει μυστική η ψηφοφορία του (δεν καταχωρούμε δηλ το id του χρήστη)

Το παρακάτω ER διάγραμμα περιγράφει το σχήμα της βάσης δεδομένων για μια ηλεκτρονική ψηφοφορία:



4.4 Αρχιτεκτονική της εφαρμογής

Ουσιαστικά η εφαρμογή μας είναι σχεδιασμένη με τον παρακάτω τρόπο. Η εφαρμογή είναι μία ιστοσελίδα που συνδέει τα δεδομένα της βάσης με τις οθόνες που εμφανίζονται στον client μέσω PHP. Σαν σύστημα εγκατάστασης της βάσης είναι το σύστημα MYSQL.

Αρχικά το πρόγραμμα μας επισκέπτεται την σελίδα index.php. Η σελίδα αυτή καθορίζει τα σταθερά μέρη της ιστοσελίδας , την σύνδεση με την βάση , το μενού του χρήστη κ.λ.π. Το αρχείο index.php είναι το παρακάτω:

<?php

```
include ("connect.php");

include ("up.php");

include ("menu.php");

include ("media.php");

include ("main.php");

include ("down.php");

?>
```

Όπως βλέπουμε καλεί το αρχείο up.php, το αρχείο menu.php , το αρχείο media.php, το αρχείο main.php, το αρχείο down.php.

Τα αρχεία up.php, down.php καθορίζουν τα σταθερά κομμάτια της ιστοσελίδας μας.

Το main.php και menu.php καθορίζουν τα αρχεία που αφορούν το μενού του χρήστη καθώς και την σελίδα που έχει επισκεφτεί εκείνη την στιγμή. Το media είναι απλά ένα αρχείο που καθορίζει μόνο την ενδιάμεση σελίδα μεταξύ μενού και main (απλά κλείνει κάποια divisions).

Το βασικότερο αρχείο είναι το connect.php που ουσιαστικά καθορίζει σε ποια βάση συνδεόμαστε, ποιος είναι ο τύπος του χρήστη που συνδέθηκε όπου με βάση αυτό οι σελίδες main,menu έχουν ανάλογες συμπεριφορές.

Ο κώδικας του αρχείου connect είναι ο παρακάτω:

```
<?php

function encrypt_text($value)

{

  if(!$value) return false;



  $crypttext = mcrypt_encrypt(MCRYPT_RIJNDAEL_256, '1123434aksjdhfkw3#ed', $value, MCRYPT_MODE_ECB, 'SECURE_STRING_2');

  return trim(base64_encode($crypttext));
```

```
}

function decrypt_text($value)
{
  if(!$value) return false;

  $crypttext = base64_decode($value);
  $decrypttext = mcrypt_decrypt(MCRYPT_RIJNDAEL_256, '1123434aksjdhfkw3#ed', $crypttext, MCRYPT_MODE_ECB, 'SECURE_STRING_2');
  return trim($decrypttext);
}

session_start();  // enarxi session
$host="localhost";  // syndesi me tin vasi ston server
$database="geo_gbase";
$username="geo_userpsif";
$password="1q2w3e";

$cn=mysql_connect($host,$username,$password);   // syndesi
if (!$cn) {
die ('Error in connection');
```

```
}else

mysql_select_db($database);

mysql_query("set names 'utf8'");  // orismos to oti tha xrisimopoiisoume utf8



$role=0;            // o rolos tou xristi ..

$login=0;  // metavliti pou deixnei an eimaste syndemenoi i oxi

$kodikos_xristi=0;   // o kodikos tou xristi diaxeiristi

$page='';



 $usr='';

 $pss='';

if (isset($_GET['logout']))

{



session_regenerate_id ();                    // arxikopoiei to session

$_SESSION['usr']='';                  // apothikevetai to username kai to password me keno oste na min einai syndemenos kapoios meta

$_SESSION['pss']='';

$login=0;



}



if (isset($_GET['page']))

{
```

```
  $page=$_GET['page'];

}

if (isset($_POST['login_button']))            // an exei patithei to login_button

{

            $usr=$_POST['username'];                    // apothikevetai stis metavlites to username
kai password

            $pss=md5($_POST['password']);



            $_SESSION['usr']=$usr;

            $_SESSION['pss']=$pss;

}

else

{

            if (isset($_SESSION['usr']))          //

            {

                        $usr=$_SESSION['usr'];

                        $pss=$_SESSION['pss'];

            }




}



// kaloume me sql ena erwtima gia to an yparxei xristis me usr kai pss
```

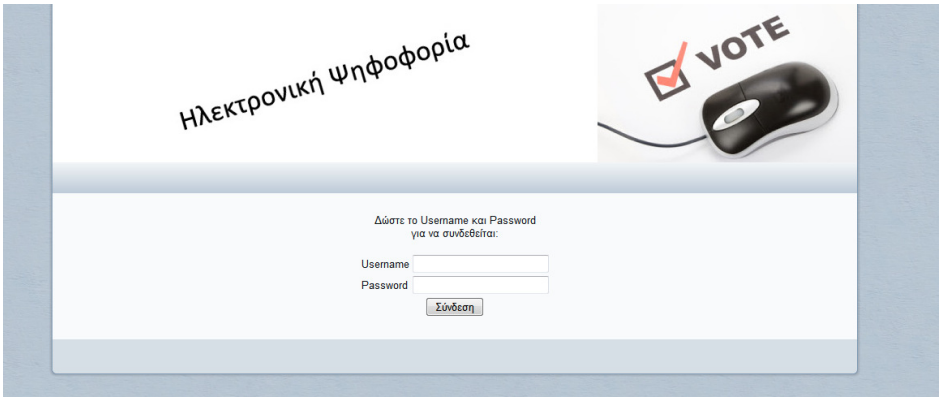
```
if ($usr!='')
{
        $sql="select * from users where username='$usr' and password='$pss'";
        $res=mysql_query($sql);   // pinakas apotelesmatwn
        if (mysql_num_rows($res)>0)   // an exoume estw ki ena apotelesma
        {
                $row=mysql_fetch_array($res);
                $kodikos_xristi=$row['id'];
                $login=1;
          $role=$row['type'];



        }
        else
        {


          $login=2;
          session_regenerate_id ();
          $_SESSION['usr']='';
    $_SESSION['pss']='';
        }
}
```

Όπως παρατηρούμε στο αρχείο έχουμε και τους δύο κώδικες που αφορούν την κρυπτογράφηση των στοιχείων.

Οι υπόλοιποι κώδικες των αρχείων φαίνονται στο παράρτημα.

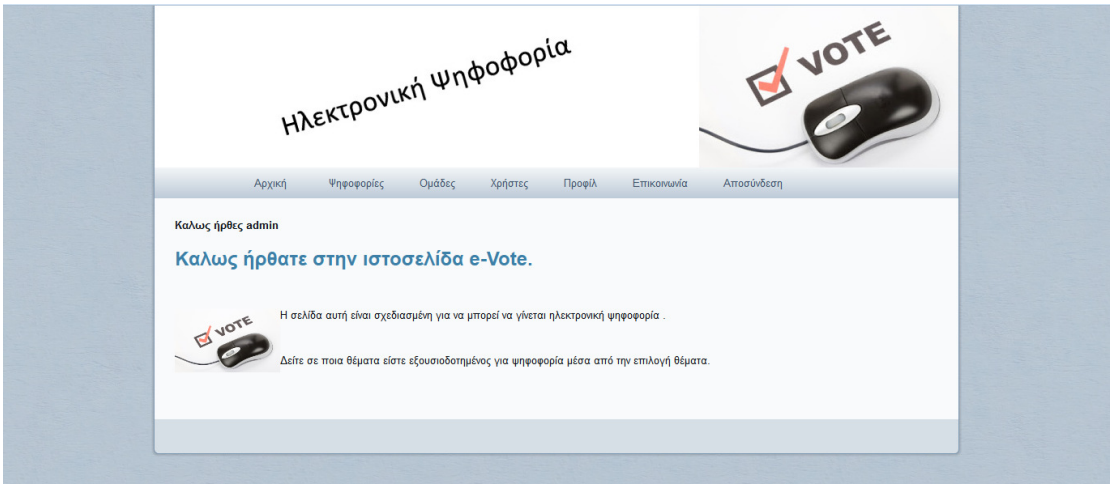
Η εφαρμογή

Όταν ανοίγουμε την εφαρμογή εμφανίζεται η πρώτη οθόνη που είναι η παρακάτω:

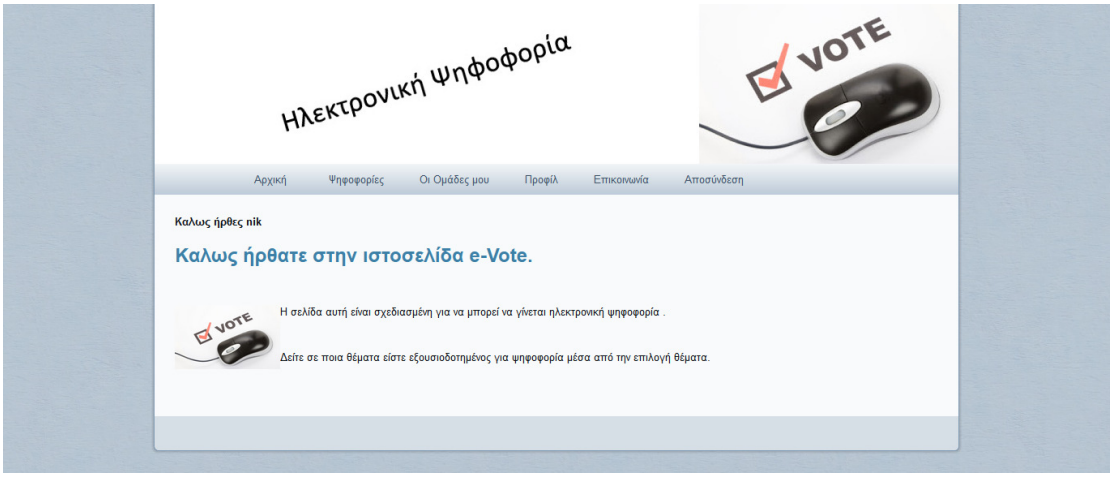


Αρχική οθόνη

Ο χρήστης δίνει τα στοιχεία του και ανάλογα με το τι χρήστης είναι εμφανίζεται το ανάλογο μενού

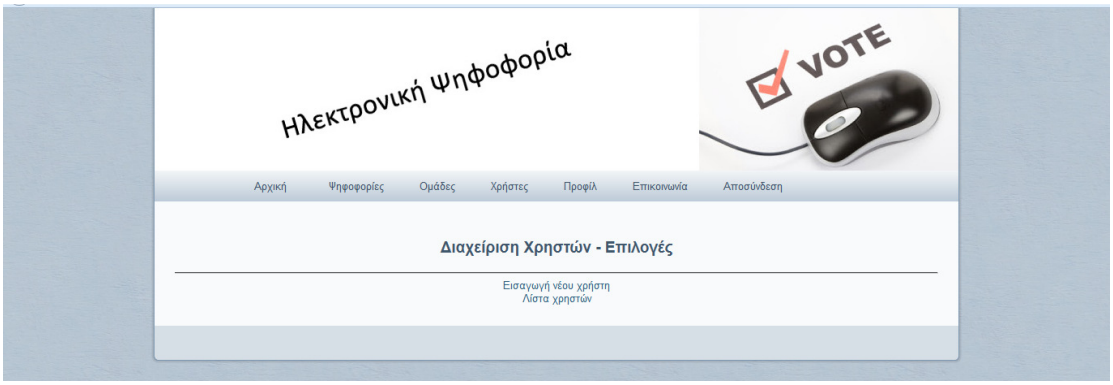


Βασική Οθόνη και μενού διαχειριστή



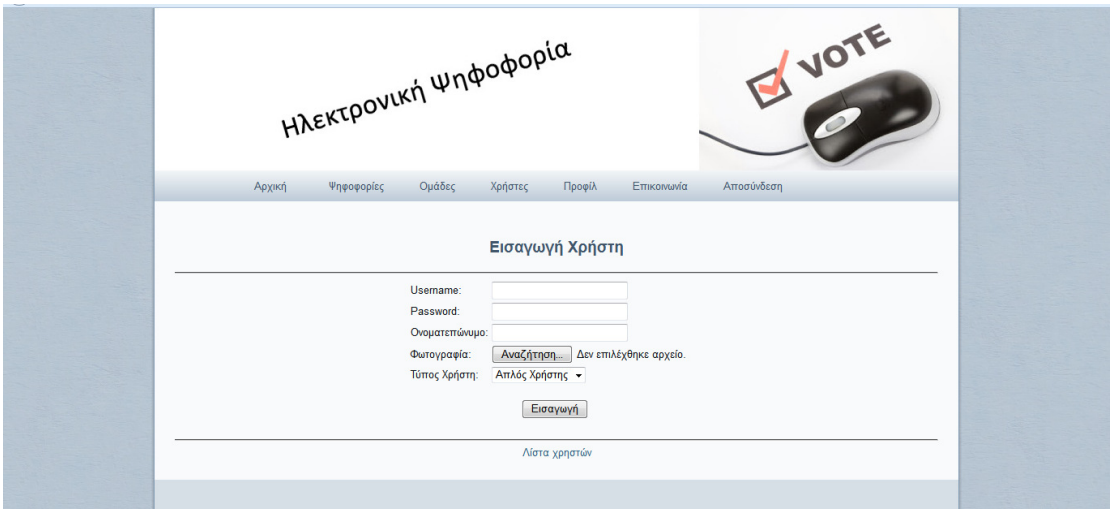
Βασική οθόνη και μενού χρήστη

Ο διαχειριστής μπορεί να εισάγει χρήστες μέσα από την παρακάτω οθόνη:



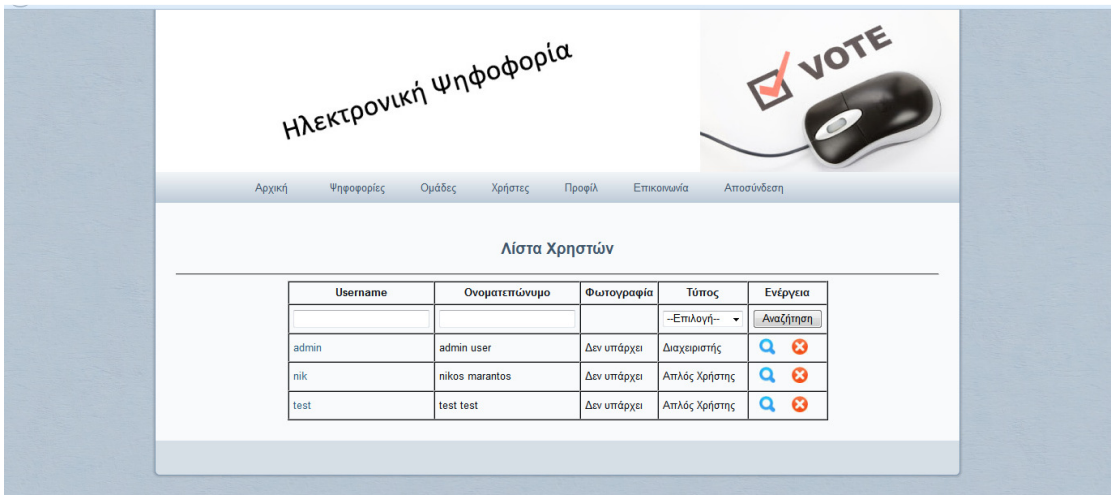
Βασική οθόνη για διαχείριση Χρηστών

Για να εισάγουμε ένα χρήστη πατάμε εισαγωγή νέου χρήστη και εμφανίζεται η παρακάτω οθόνη



Εισαγωγή Χρηστών

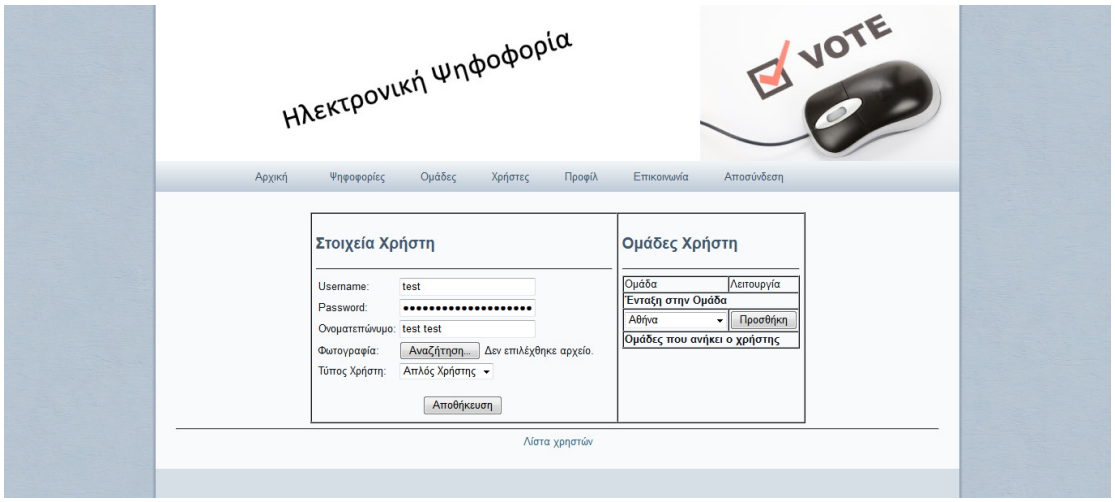
Μετά την εισαγωγή μπορούμε να δούμε τον νέο χρήστη στην λίστα χρηστών και να τον επεξεργαστούμε:



Λίστα χρηστών

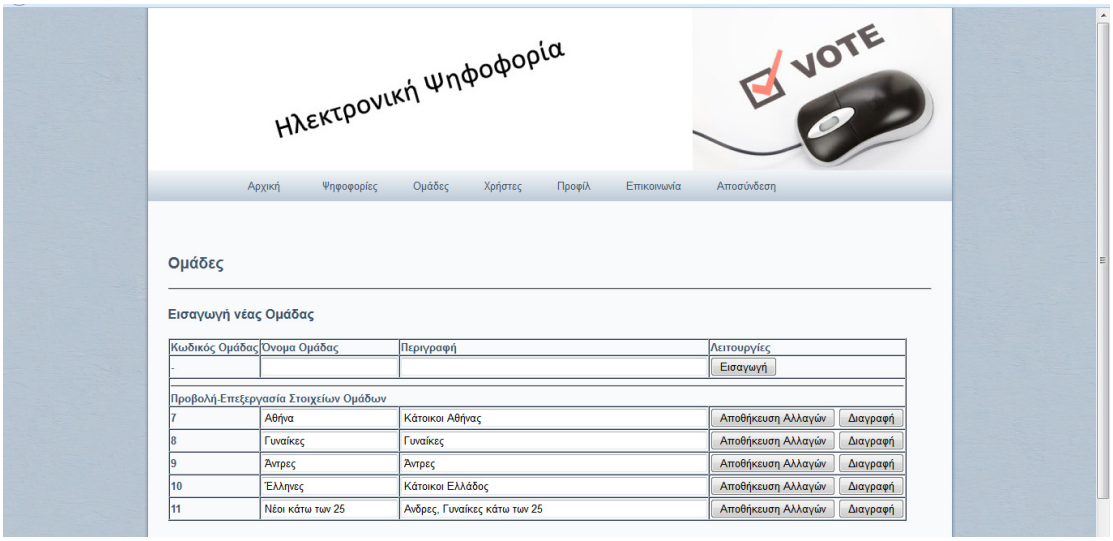
Μετά επιλέγοντας τον χρήστη μπορούμε να τον εισάγουμε σε ομάδες όπου τελικά καθορίζουν σε ποιο εκλογικό σώμα ανήκει.

Έτσι εμφανίζεται η παρακάτω εικόνα:



Εισαγωγή μονάδες χρηστών

Οι ομάδες που μπορεί να οριστούν για ένα χρήστη ορίζονται από τον διαχειριστή μέσα από την επιλογή για τις ομάδες:

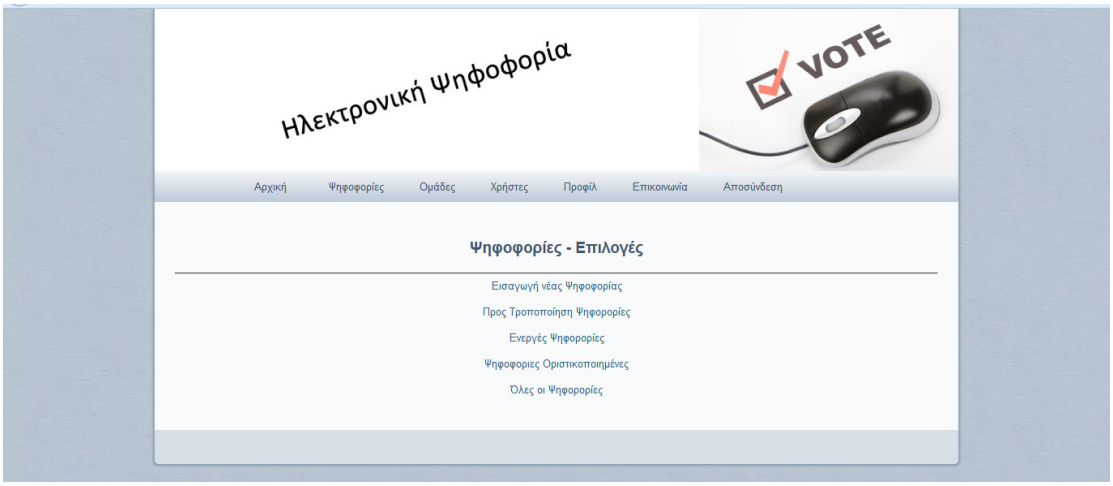


Διαχείριση Ομάδων

Όπως βλέπουμε μέσα από την παραπάνω οθόνη έχουμε την δυνατότητα προσθήκης ομάδων , την διαγραφή τους και την αλλαγή στην περιγραφή και όνομα της ομάδας.

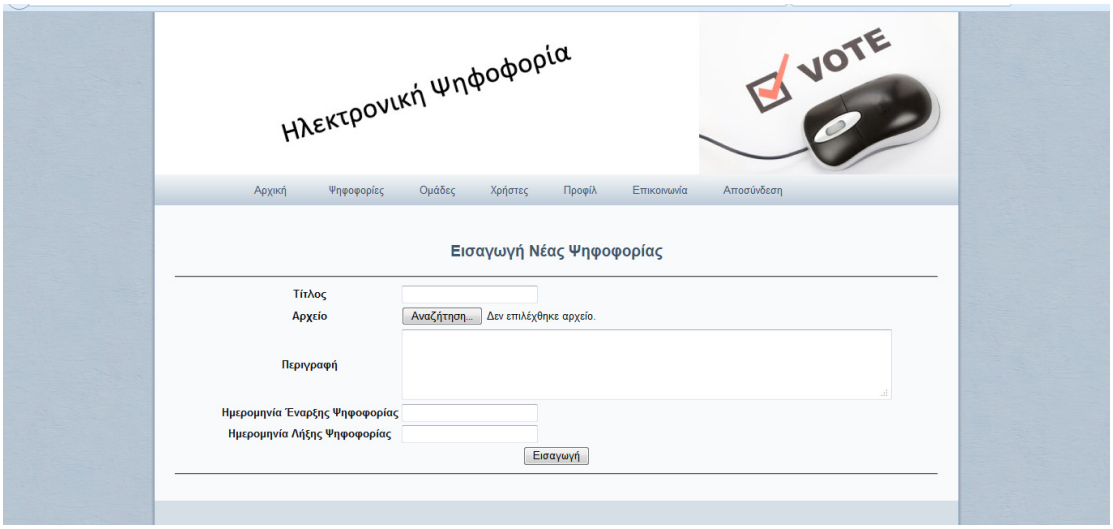
Όταν έχουν οριστεί οι χρήστες και οι ομάδες τότε ο διαχειριστής μπορεί να εισάγει ψηφοφορίες.

Οι ψηφοφορίες αυτές καθορίζονται από όπως παρακάτω. Στην επιλογή ψηφοφορίες εμφανίζεται η παρακάτω εικόνα:



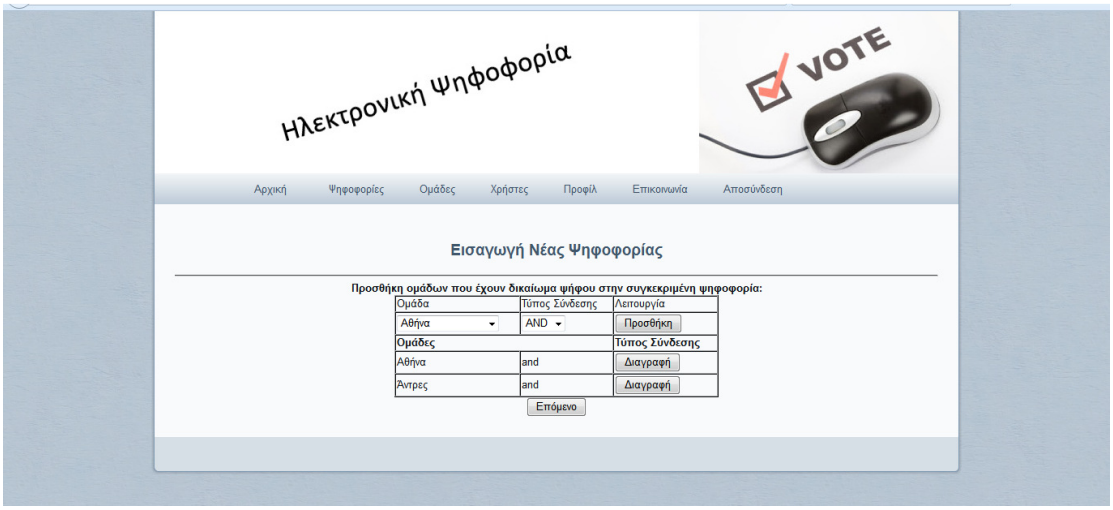
Εκεί ο χρήστης μπορεί να εισάγει μία ψηφοφορία με τον παρακάτω τρόπο:

Αρχικά δίνει τον τίτλο της ψηφοφορίας, ένα αρχείο που περιγράφει τι ακριβώς ψηφίζεται σε αυτή την ψηφοφορία, μία περιγραφή της ψηφοφορίας, Ημερομηνία έναρξης και λήξης της ψηφοφορίας.

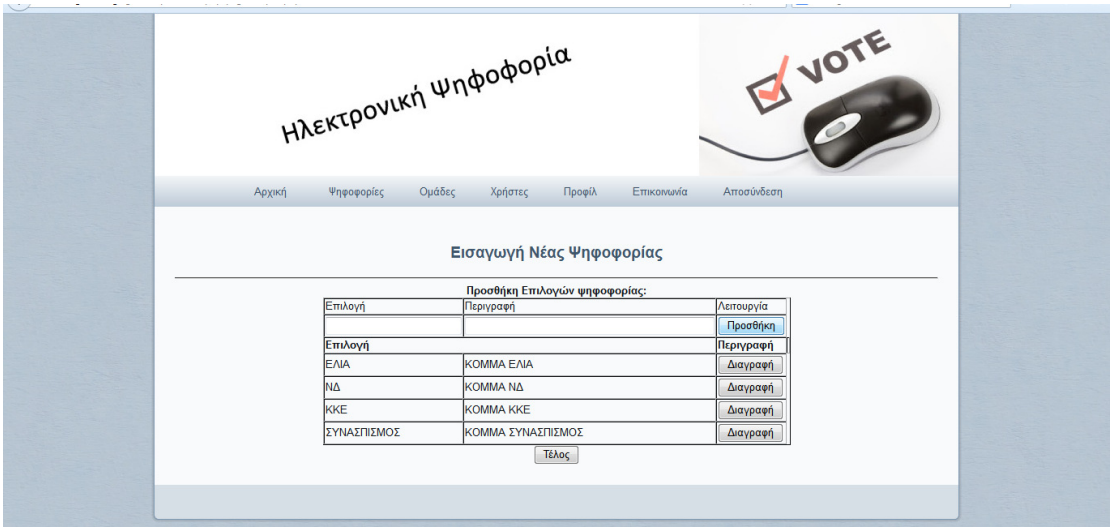


Στην συνέχεια ορίζουμε τις ομάδες που τελικά θα καθορίσουν το εκλογικό σώμα.

Οι ομάδες μεταξύ τους συνδέονται με σχέσεις AND και OR. Δηλαδή αν προσθέσουμε την ομάδα ΑΘΗΝΑ με σχέση OR την ομάδα ΠΑΤΡΑ τότε το εκλογικό σώμα είναι οι ψηφοφόροι που είναι κάτοικοι Πατρών και Αθηνών. Αν καθορίσουμε την ομάδα ΑΘΗΝΑ με σχέση AND με την ομάδα ΑΝΤΡΕΣ τότε είναι οι άντρες κάτοικοι Αθηνών. Στην παρακάτω οθόνη φαίνεται ο τρόπος καθορισμού του εκλογικού σώματος.



Στην συνέχεια καθορίζονται οι επιλογές που έχει ο ψηφοφόρος για την συγκεκριμένη ψηφοφορία.



Πλέον η ψηφοφορία είναι διαθέσιμη για ψήφισμα.

Οι ψηφοφορίες χωρίζονται στους παρακάτω τύπους:

- Προς Τροποποίηση Ψηφοφορίες
- Ενεργές Ψηφοφορίες
- Ψηφοφορίες Οριστικοποιημένες

Οι Ψηφοφορίες προς Τροποποίηση είναι αυτές όπου η ημερομηνία έναρξης και λήξης είναι μικρότερη της σημερινής που σημαίνει ότι δεν είναι ενεργή και την βλέπει μόνο ο διαχειριστής. Σε αυτές μπορούμε να κάνουμε αλλαγές όπως και να τις αποσύρουμε.

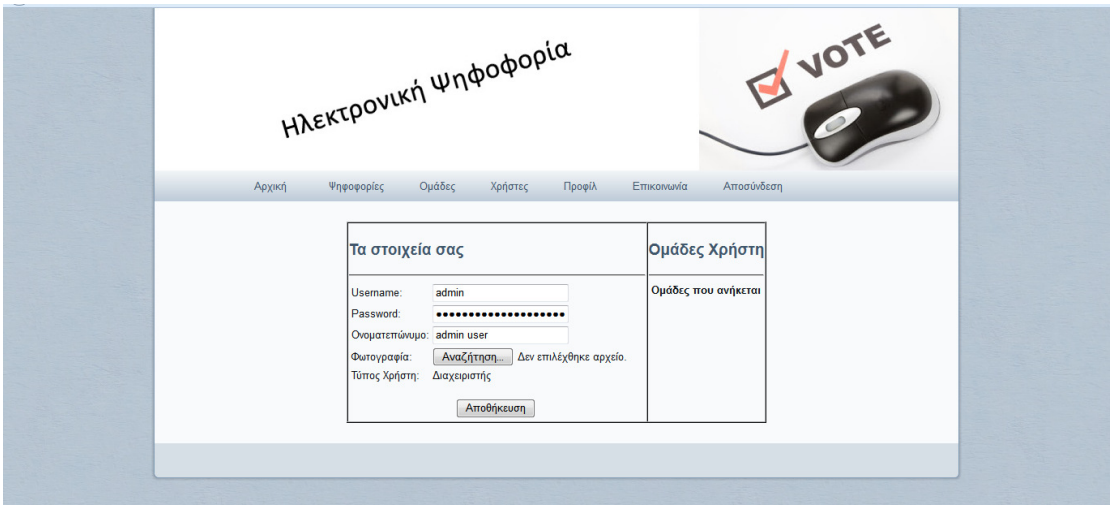
Οι ενεργές ψηφοφορίες είναι αυτές που η ημερομηνία έναρξης και λήξης είναι μεταξύ της σημερινής που σημαίνει ότι πλέον δεν μπορεί ο διαχειριστής να τροποποιήσει τίποτα και οι ψηφοφόροι μπορούν να ψηφίζουν.

Οι οριστικοποιημένες ψηφοφορίες είναι αυτές όπου η ημερομηνία λήξης είναι μεταγενέστερη της σημερινής και πλέον εκδίδονται τα αποτελέσματα.

Ο ψηφοφόρος λοιπόν ψηφίζει μόνο στις ενεργές ψηφοφορίες και μόνο αν ανήκει στο εκλογικό σώμα της συγκεκριμένης ψηφοφορίας . Επιλέγει μία από τις επιλογές και τότε του έρχεται sms που του δίνει ένα κωδικό με στόχο να ψηφίσει. Ο κωδικός αυτός έχει ισχύει για 30 λεπτά.

Επίσης κάθε χρήστης έχει δυνατότητα να δει τα στοιχεία του μέσα από την επιλογή ΠΡΟΦΙΛ καθώς και τις ομάδες που ανήκει. Αν θέλει να αλλάξει ομάδα πρέπει να επικοινωνήσει με τον διαχειριστή ώστε να του προσθέσει ή να του αλλάξει ομάδα. Αυτό γίνεται ώστε οι

χρήστες να μην μπορούν να παίζουν με τις ομάδες παρά μόνο οι αρμόδιες αρχές (διαχειριστές) που θα επιβεβαιώνουν τα στοιχεία κατόπιν κατάθεσης και ανάλογων δικαιολογητικών.



Οι επιλογές Επικοινωνία και Αποσύνδεση αφορούν τις πληροφορίες για επικοινωνία με τους διαχειριστές και Αποσύνδεση να αποσυνδεθεί ένας χρήστης από το σύστημα.

Συμπεράσματα

Με τον όρο ηλεκτρονική ψηφοφορία (electronic voting / e-voting), εννοούμε την άσκηση του εκλογικού δικαιώματος, με τη χρήση ηλεκτρονικών μεθόδων. Η εννοιολόγηση αυτή, σε μία πρώτη προσέγγιση είναι εξαιρετικά γενική, καθώς περιλαμβάνει μία μεγάλη κλίμακα επιμέρους θεμάτων και διαδικασιών που εμπίπτουν στο πεδίο της διεξαγωγής μιας εκλογικής διαδικασίας, τα οποία μπορεί να εκτείνονται από την αυτοματοποίηση στην καταμέτρηση των ψήφων έως την άσκηση του ηλεκτρονικού δικαιώματος με τη βοήθεια του τηλεφώνου.

Η παρούσα μελέτη επικεντρώθηκε στην ηλεκτρονική άσκηση του εκλογικού δικαιώματος, η οποία πραγματοποιείται μέσω της χρήσης είτε του Διαδικτύου (on line voting) είτε άλλων δικτύων, παρέχοντας στους ψηφοφόρους τη δυνατότητα να προβούν στην κατάθεση μίας ασφαλούς και μυστικής ψήφου, με τη βοήθεια υπολογιστικών συστημάτων. Σύμφωνα με την ανωτέρω οριοθέτηση, επομένως, δυο είναι τα θεμελιώδη στοιχεία που συνθέτουν την ιδιαίτερη φύση της ηλεκτρονικής ψήφου και τη διαφοροποιούν σε μεγάλο βαθμό από τα υπάρχοντα συστήματα της εκλογικής διαδικασίας:

1) Η δυνατότητα άσκησης του εκλογικού δικαιώματος από απόσταση, χωρίς την αυτοπρόσωπη, επομένως, παρουσία του ψηφοφόρου στο εκλογικό τμήμα.

2) Η χρήση υπολογιστικού συστήματος και κατά συνέπεια αυτοματοποιημένων μεθόδων, για την οργάνωση και διεξαγωγή της όλης εκλογικής διαδικασίας.

Όπως είδαμε τα στοιχεία της ψηφοφορίας, όπως τα στοιχεία των προσώπων που συμμετέχουν, οι κωδικοί πρόσβασης κ.α. πρέπει να είναι κρυπτογραφημένα στην εφαρμογής και γι’ αυτό τον λόγο χρησιμοποιήθηκαν αλγόριθμοι κρυπτογράφησης όπως ο MD5 και ο αλγόριθμος SHA-256.

Στη εφαρμογή ορίστηκε τρόπος που καθορίζει το εκλογικό σώμα κάθε ψηφοφορίας μέσα από την σύνθεση ομάδων όπως την χώρα που ανήκει κάποιος, την πόλη, το φύλο κ.α.

Επίσης καθορίστηκε τρόπος διασφάλισης της ταυτοπροσωπίας μέσα από την χρήση SMS στο κινητό τηλέφωνο που χρησιμοποιεί κάποιος. Πιο συγκεκριμένα, για την ταυτοπροσωπία χρησιμοποιούμε τις κινητές συσκευές των χρηστών (κινητό τηλέφωνο) όπου με την χρήση απλών SMS στέλνεται κωδικός που ο χρήστης τον καταχωρεί και δίνει στο σύστημα για να του δώσει δικαίωμα ψήφου. Σε περίπτωση που ο χρήστης δεν έχει κινητό τότε ο χρήστης μπορεί να ψηφίσει σε εξουσιοδοτημένες υπηρεσίες όπου εκεί γίνεται αποστολή του κωδικού σε εξουσιοδοτημένο email.

Η εφαρμογή θα μπορούσε να επεκταθεί με την χρήση πρόσθετων στοιχείων κρυπτογράφησης καθώς και στοιχείων όπως την χρήση μόνο mobile εφαρμογών όπου όλη η διαδικασία να μπορεί να γίνεται εύκολα μόνο με την χρήση ενός smart phone. Επίσης είναι σημαντικό να διερευνηθούν τρόποι που για την δυνατότητα μεγαλύτερης ευκολίας σε χρήστες με πολύ λίγες δεξιότητες στο τρόπο χειρισμού των υπολογιστών καθώς και σε περιπτώσεις ατόμων με ειδικές ανάγκες. Στην παρούσα εφαρμογή αυτό αντιμετωπίζεται με την επίσκεψη τους σε εξουσιοδοτημένους φορείς όπως τα ΚΕΠ ή άλλες υπηρεσίες. Παρόλα αυτά η ευκολία να για την άσκηση του εκλογικού δικαιώματος από όποιο χώρο επιθυμεί κάποιος φαίνεται να μην ισχύει στις περιπτώσεις των παραπάνω κατηγοριών γεγονός που δημιουργεί διακριτή αδικία του συστήματος.

Βιβλιογραφία

1. D. Gritzalis (Ed.), Secure Electronic Voting: Trends and Perspectives, Capabilities and Limitations. Kluwer Academic Publishers, 2002.
2. Mitrou, L. Gritzalis, D. and Katsikas S. (2002*) Revisiting legal and regulatory requirements for secure e-voting.* Proc. of the 16th IFIP International Information Security Conference (IFIP/SEC-2002) M. el Hadidi, et al. (Eds.), Egypt, 6-8 May 2002. Kluwer Academics Publishers.
3. Ikonomopoulos S., Lambrinoudakis C., Gritzalis D., Kokolakis S. and Vassiliou K., "*Functional Requirements for a Secure Electronic Voting System*", Proc. of the 16th IFIP International Information Security Conference (IFIP/SEC-2002) M. el Hadidi, et al. (Eds.), Egypt, 6-8 May 2002. Kluwer Academics Publishers.
4. Philips, D., von Spakovsky H., "Gauging the risks of Internet elections", in Com. of the ACM, Vol. 44, No.1, pp. 73-85, January 2001.
5. SEQUOIA voting systems: http://www.sequoiavote.com/
6. Votehere: http://www.votehere.net/
7. Virtual Voting: http://www.acm.org/technews/articles/2003-5/0625w.html#item12
8. Putting the 'E' in Elections: http://www.acm.org/technews/articles/2003-5/0203m.html#item18
9. L.Welling – L.Thomson: Ανάπτηξη Web εφαρμογών με PHP
10. L.Lemay: Πλήπες εγχειρίδιο της HTML 4
11. Learning Javascript, http://www.w3schools.com/js/DEFAULT.asp

Παράρτημα – Κώδικας προγράμματος

Αρχείο Index.php

```
<?php

include ("connect.php");

include ("up.php");

include ("menu.php");

include ("media.php");

include ("main.php");

include ("down.php");

?>
```

Αρχείο Connect.php

```
<?php

function encrypt_text($value)

{

  if(!$value) return false;


  $crypttext = mcrypt_encrypt(MCRYPT_RIJNDAEL_256, '1123434aksjdhfkw3#ed', $value, MCRYPT_MODE_ECB, 'SECURE_STRING_2');

  return trim(base64_encode($crypttext));

}


function decrypt_text($value)

{
```

```
  if(!$value) return false;


  $crypttext = base64_decode($value);

  $decrypttext = mcrypt_decrypt(MCRYPT_RIJNDAEL_256, '1123434aksjdhfkw3#ed', $crypttext, MCRYPT_MODE_ECB, 'SECURE_STRING_2');

  return trim($decrypttext);

}
```

```
session_start();  // enarxi session

$host="localhost";  // syndesi me tin vasi ston server

$database="geo_gbase";

$username="geo_userpsif";

$password="1q2w3e";


$cn=mysql_connect($host,$username,$password);   // syndesi

if (!$cn) {

die ('Error in connection');

}else

mysql_select_db($database);

mysql_query("set names 'utf8'");  // orismos to oti tha xrisimopoiisoume utf8
```

```
$role=0;            // o rolos tou xristi ..

$login=0;  // metavliti pou deixnei an eimaste syndemenoi i oxi

$kodikos_xristi=0;   // o kodikos tou xristi diaxeiristi

$page='';



 $usr='';

 $pss='';

if (isset($_GET['logout']))

{



session_regenerate_id ();                    // arxikopoiei to session

$_SESSION['usr']='';                  // apothikevetai to username kai to password me keno oste na min einai syndemenos kapoios meta

$_SESSION['pss']='';

$login=0;



}



if (isset($_GET['page']))

{

  $page=$_GET['page'];

}

if (isset($_POST['login_button']))           // an exei patithei to login_button

{
```

```
	$usr=$_POST['username'];		// apothikevetai stis metavlites to username
kai password
	$pss=md5($_POST['password']);

	$_SESSION['usr']=$usr;
	$_SESSION['pss']=$pss;
}
else
{
	if (isset($_SESSION['usr']))	//
	{
		$usr=$_SESSION['usr'];
		$pss=$_SESSION['pss'];
	}

}

// kaloume me sql ena erwtima gia to an yparxei xristis me usr kai pss

if ($usr!='')
{
	$sql="select * from users where username='$usr' and password='$pss'";
```

```
        $res=mysql_query($sql);   // pinakas apotelesmatwn
        if (mysql_num_rows($res)>0)   // an exoume estw ki ena apotelesma
        {
                $row=mysql_fetch_array($res);
                $kodikos_xristi=$row['id'];
                $login=1;
          $role=$row['type'];



        }
        else
        {

          $login=2;
          session_regenerate_id ();
          $_SESSION['usr']='';
    $_SESSION['pss']='';
        }
}
```

Αρχείο up.php

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" dir="ltr" lang="en-US" xml:lang="en">
```

```
<head>
  <!--
  Created by Artisteer v3.0.0.33215
  Base template (without user's data) checked by http://validator.w3.org : "This page is valid XHTML 1.0 Transitional"
  -->
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
  <title>e-Vote </title>

  <link rel="stylesheet" href="style.css" type="text/css" media="screen" />
  <!--[if IE 6]><link rel="stylesheet" href="style.ie6.css" type="text/css" media="screen" /><![endif]-->
  <!--[if IE 7]><link rel="stylesheet" href="style.ie7.css" type="text/css" media="screen" /><![endif]-->

  <script type="text/javascript" src="jquery.js"></script>
  <script type="text/javascript" src="script.js"></script>
</head>
<body>
<div id="art-page-background-glare">
    <div id="art-page-background-glare-image">
  <div id="art-main">
    <div class="art-sheet">
      <div class="art-sheet-tl"></div>
      <div class="art-sheet-tr"></div>
```

```
        <div class="art-sheet-bl"></div>
        <div class="art-sheet-br"></div>
        <div class="art-sheet-tc"></div>
        <div class="art-sheet-bc"></div>
        <div class="art-sheet-cl"></div>
        <div class="art-sheet-cr"></div>
        <div class="art-sheet-cc"></div>
        <div class="art-sheet-body">
          <div class="art-header">
            <div class="art-header-center">
              <div class="art-header-jpeg"></div>
            </div>
            <div class="art-logo">
             <h1 id="name-text" class="art-logo-name"><a href="#"></a></h1>
             <h2 id="slogan-text" class="art-logo-text"></h2>
            </div>
          </div>
          <div class="art-nav">
                  <div class="l"></div>
                  <div class="r"></div>
?>
```

Αρχείο down.php

```
                  </div>
```

```
            </div>
            <div class="cleared"></div>
          </div>
        </div>
      </div>
      <div class="cleared"></div>
      <div class="art-footer">
        <div class="art-footer-t"></div>
        <div class="art-footer-l"></div>
        <div class="art-footer-b"></div>
        <div class="art-footer-r"></div>
        <div class="art-footer-body">

          <div class="art-footer-text">

          </div>
                    <div class="cleared"></div>
        </div>
      </div>
            <div class="cleared"></div>
    </div>
</div>
<div class="cleared"></div>
```

```
   </div>
      </div>
   </div>
```

```
</body>
</html>
```

Αρχείο Menu.php

```
<?php
if ($role==0)
{
echo "
";

}

if ($role==1)
{
echo "
```

<ul class='art-menu'>

<span class=\"l\"><span class=\"r\"><span class=\"t\">Αρχική

<span class=\"l\"><span class=\"r\"><span class=\"t\">Ψηφοφορίες

<span class=\"l\"><span class=\"r\"><span class=\"t\">Ομάδες

<span class=\"l\"><span class=\"r\"><span class=\"t\">Χρήστες

<span class=\"l\"><span class=\"r\"><span class=\"t\">Προφίλ

<span class=\"l\"><span class=\"r\"><span class=\"t\">Επικοινωνία

<span class=\"l\"><span class=\"r\"><span class=\"t\">Αποσύνδεση

";

}

if ($role==2)

{

echo "

<ul class='art-menu'>

<span class=\"l\"><span class=\"r\"><span class=\"t\">Αρχική

<span class=\"l\"><span class=\"r\"><span class=\"t\">Ψηφοφορίες

<span class=\"l\"><span class=\"r\"><span class=\"t\">Οι Ομάδες μου

<span class=\"l\"><span class=\"r\"><span class=\"t\">Προφίλ

<span class=\"l\"><span class=\"r\"><span class=\"t\">Επικοινωνία

<span class=\"l\"><span class=\"r\"><span class=\"t\">Αποσύνδεση

";

}

?>

Αρχείο main.php

<?php

if ($login==0)

{

echo "

Δώστε το Username και Password

για να συνδεθείται:

<form action='' method='post'>

<table align=center>

<tr><td>Username</td><td><input type='text' name='username'></td></tr>

<tr><td>Password</td><td><input type='password' name='password'></td></tr>

```
        <tr><td colspan=2 align=center><input type=submit name='login_button' value='Σύνδεση'></td></tr>

        </table>

        </form>

        </center>";

}

if ($login==1)

{


    if ($page=='')

        {

          echo "<b>Καλως ήρθες $usr</b>";

          include "details.php";

        }

        else

          include ($page);




}

if ($login==2)

{


         echo "<center><b>Λάθος username ή Password ! Προσπάθησε ξανά</b><br><br>

        Δώστε το Username και Password <br>
```

```
για να συνδεθείται:<br><br>

<form action='' method='post'>

<table align=center>

<tr><td>Username</td><td><input type='text' name='username'></td></tr>

<tr><td>Password</td><td><input type='password' name='password'></td></tr>

<tr><td colspan=2 align=center><input type=submit name='login_button' value='Σύνδεση'></td></tr>

</table>

</form>

</center>";


}

?>
```

Αρχείο insertuser.php

```
<center>

<script language='javascript'>

function check()

{

s="";

f=true;

if (document.getElementById('username').value=="")

{

  s=s+"You must give username\n";

  f=false;
```

```
}
if (document.getElementById('password').value=="")
{
  s=s+"You must give password\n";
  f=false;
}
if (document.getElementById('onoma').value=="")
{
  s=s+"You must give Name\n";
  f=false;
}
if (f==false) alert (s);
return f;

}

</script>
<?php
if (isset($_POST['insert_button']))
{
        if ($_FILES["photo"]["name"]=="")
        {
        $sql="insert into users(username,password,onoma,type)
```

```
values
('$_POST[username]','".md5($_POST['password'])."','".encrypt_text($_POST['onoma'])."',
'$_POST[type]')";
if (mysql_query($sql))
   echo "Η εισαγωγή χρήστη έγινε επιτυχώς!";
else
   echo "Πρόβλημα στην εισαγωγή χρήστη !";
}
else
{



$sql="insert into users(username,password,onoma,filephoto,type)
values
('$_POST[username]','".md5($_POST['password'])."','".encrypt_text($_POST['onoma'])."','".$
_POST['username']."_".$_FILES["photo"]["name"]."', '$_POST[type]')";
if (mysql_query($sql))
{
   echo "Η εισαγωγή χρήστη έγινε επιτυχώς!";
    move_uploaded_file($_FILES["photo"]["tmp_name"],
"images/" .$_POST['username']."_".$_FILES["photo"]["name"]);
}
else
   echo "Έχετε το username που υπάρχει !";
}
```

```
}
else
{
        echo "
        <h3>Εισαγωγή Χρήστη</h3>
        <hr>
        <form action='' method='post' enctype='multipart/form-data' onsubmit='return check();'>
        <table>
        <tr><td>Username:</td><td><input type='text' name=username id=username></td></tr>
        <tr><td>Password:</td><td><input type='password' name=password id=password><td></tr>
        <tr><td>Ονοματεπώνυμο:</td><td><input type='text' name=onoma id=onoma></td></tr>
        <tr><td>Φωτογραφία:</td><td><input type='file' name=photo></td></tr>
        <tr><td>Τύπος Χρήστη:</td><td><select name=type>
        <option value=2>Απλός Χρήστης</option>
        <option value=1>Διαχειριστής</option>
        </select>
        </td></tr>
```

```
        <tr><td colspan=2><br><center><input type=submit value='Εισαγωγή' name=insert_button></center></td>

        </tr>

        </table>

        </form>";




}

?>

  <br>

        <hr>

        <a href='index.php?page=listuser.php'>Λίστα χρηστών</a><br>


</center>
```

Αρχείο updateuser.php

```
<center>

<script language='javascript'>

function check()

{

s="";

f=true;

if (document.getElementById('username').value=="")

{
```

```
  s=s+"You must give username\n";
  f=false;
}
if (document.getElementById('password').value=="")
{
  s=s+"You must give password\n";
  f=false;
}
if (document.getElementById('onoma').value=="")
{
  s=s+"You must give Name\n";
  f=false;
}
if (f==false) alert (s);
return f;

}

</script>
<?php
if (isset($_POST['vins']))
{
```

```
	$sql34="insert into users_omades(id_user,id_omadas) values ($_GET[id],$_POST[vid])";


	mysql_query($sql34);
}
if (isset($_POST['vdel']))
{
	$sql34="delete from users_omades where id=$_POST[vid]";
	mysql_query($sql34);
}



if (isset($_POST['update_button']))
{
if ($pss!=$_POST['password']){$pssupdate=md5($_POST['password']);
$_SESSION['pss']=md5($_POST['password']);}
else  $pssupdate=$pss;
	if ($_FILES["photo"]["name"]=="")
	{
	$sql="update users
	set username='$_POST[username]',
	password='$pssupdate',
	onoma='".encrypt_text($_POST['onoma'])."',
	type='$_POST[type]'
```

```
 where id=$_POST[id]

";

if (mysql_query($sql))

   echo "Η αποθήκευση έγινε επιτυχώς!";

else

   echo "Έχετε δώσει username που υπάρχει !";

}

else

{


$sql="update users

set username='$_POST[username]',

password='$pssupdate',

onoma='".encrypt_text($_POST['onoma'])."',

type='$_POST[type]',

filephoto='".$_POST['username']."_".$_FILES["photo"]["name"]."'

 where id=$_POST[id]

";


if (mysql_query($sql))

{

   echo "Η αποθήκευση έγινε επιτυχώς!";

    move_uploaded_file($_FILES["photo"]["tmp_name"],

"images/" .$_POST['username']."_".$_FILES["photo"]["name"]);
```

```
        }

        else

           echo "Έχετε δώσει username που υπάρχει !";

        }




}


echo "<table border=1 cellspacing=0 cellpadding=5><tr><td valign=top>";

$sql4="select * from  users where id=$_GET[id]";

$res4=mysql_query($sql4);

$row4=mysql_fetch_array($res4);


        echo "<h3>Στοιχεία Χρήστη</h3>

        <hr>

        <form action='' method='post' enctype='multipart/form-data' onsubmit='return check();'>

        <table>

        <tr><td>Username:</td><td><input type='text' name=username id=username value='$row4[username]'></td></tr>

        <tr><td>Password:</td><td><input type='password' name=password id=password value='$row4[password]'><td></tr>

        <tr><td>Ονοματεπώνυμο:</td><td><input type='text' name=onoma id=onoma value='".decrypt_text($row4['onoma'])."'></td></tr>";
```

```
if ($row4['filephoto']!="") echo "

 <tr><td>Φωτογραφία:</td><td><img src='images/$row4[filephoto]'
width=160px><br><input type='file' name=photo></td ></tr>";

else

echo "

 <tr><td>Φωτογραφία:</td><td><input type='file' name=photo></td ></tr>";


echo "

<tr><td>Τύπος Χρήστη:</td><td><select name=type>";

if ($row4['type']==1)

echo "

<option value=1>Διαχειριστής</option>

<option value=2>Απλός Χρήστης</option>";


if ($row4['type']==2)

echo "

<option value=2>Απλός Χρήστης</option>

<option value=1>Διαχειριστής</option>

";


echo"

</select>

<input type=hidden name=id value=$row4[id]>

</td></tr>
```

```
        <tr><td colspan=2><br><center><input type=submit value='Αποθήκευση' name=update_button></center></td>

        </tr>

        </table>

        </form>";


echo "</td>";

echo "<td valign=top>";

        echo "<h3>Ομάδες Χρήστη</h3>";

        echo "<hr>";

        echo "<table border=1 cellspacing=0>";

        echo "<tr><td>Ομάδα</td><td>Λειτουργία</td></tr>";

   echo "<tr><td colspan=2><b>Ένταξη στην Ομάδα</b></td></tr>";

            echo "<tr>

                <form action='' method=post><td><select name=vid>";

                $sql3="select * from omada";

                $res4=mysql_query($sql3);

                while ($row4=mysql_fetch_array($res4))

                {

                        echo "<option value='$row4[id]'>$row4[titlos]</option>";

                }


                echo "

                </select>
```

```
                </td>
                <td><input type=submit name=vins value='Προσθήκη'></td></form>
                </tr>";

                $sql4="select *,users_omades.id as vid from users_omades,omada where users_omades.id_user=$_GET[id] and users_omades.id_omadas=omada.id ";
                $res4=mysql_query($sql4);

  echo "<tr><td colspan=2><b>Ομάδες που ανήκει ο χρήστης</b></td></tr>";
        while ($row4=mysql_fetch_array($res4))
        {
                echo "<tr><td>$row4[titlos]

                </td>
                <td>
                <form action='' method=post>
                <input type=submit name=vdel value='Διαγραφή'>
                <input type=hidden value=$row4[vid] name=vid>
                </form>
                </td>
                </tr>";
        }
        echo "</table>";
```

```
echo "</td>";

echo "</tr>";

echo "</table>";

?>

   <hr>

          <a href='index.php?page=listuser.php'>Λίστα χρηστών</a><br>


</center>
```

Αρχείο xristes.php

```
<?php

echo "

<center>

<h3>Διαχείριση Χρηστών - Επιλογές</h3>

<hr>


<a href='index.php?page=insertuser.php'>Εισαγωγή νέου χρήστη</a><br>

<a  href='index.php?page=listuser.php'>Λίστα χρηστών</a><br>

</center>

";

?>
```

Αρχείο deleteuser.php

```
<center>

<?php
```

```
if (isset($_POST['delete_button']))

{

$sql4="select * from  users where id=$_GET[id]";

$res4=mysql_query($sql4);

$row4=mysql_fetch_array($res4);

$fn="images/$row4[filephoto]";




        $sql="delete from users where id=$_POST[id]     ";

        if (mysql_query($sql))

        {

           echo "Η Διαγραφή έγινε επιτυχώς!";




        }

        else

           echo "Πρόβλημα στην Διαγραφή !";




}

else

{

$sql4="select * from  users where id=$_GET[id]";
```

```
$res4=mysql_query($sql4);

$row4=mysql_fetch_array($res4);


        echo "<h3>Στοιχεία Χρήστη</h3>

        <hr>

        <form action='' method='post' enctype='multipart/form-data' onsubmit='return check();'>

        <table>

        <tr><td>Username:</td><td><input type='text' readonly name=username id=username value='$row4[username]'></td></tr>

        <tr><td>Ονοματεπώνυμο:</td><td><input type='text' readonly name=onoma id=onoma value='$row4[onoma]'></td></tr>";

        if ($row4['filephoto']!="") echo "

         <tr><td>Φωτογραφία:</td><td><img src='images/$row4[filephoto]' width=160px></td ></tr>";


        echo "

        <tr><td>Τύπος Χρήστη:</td><td>";

        if ($row4['type']==1)

        echo "Διαχειριστής";


        if ($row4['type']==2)

        echo "Απλός Χρήστης    ";


        echo"
```

```
        <input type=hidden name=id value=$row4[id]>

        </td></tr>

        <tr><td colspan=2><br><center><input type=submit value='Διαγραφή' name=delete_button><input type=reset value='Επιστροφή στη Λίστα' onclick=\"location.href='index.php?page=listuser.php'\" name=rs_button></center></td>

        </tr>

        </table>

        </form>";




}

?>

  <hr>

        <a href='index.php?page=listuser.php'>Λίστα χρηστών</a><br>


</center>
```

Αρχείο psifofories.php

```
<?php

echo "

<center>

<h3>Ψηφοφορίες - Επιλογές</h3>

<hr>";
```

```
if ($role==1) echo "<a href='index.php?page=inspsif.php'>Εισαγωγή νέας Ψηφοφορίας</a><br><br>";

echo "<a href='index.php?page=energespsif.php&typee=3'>Προς Τροποποίηση Ψηφορορίες</a><br><br>";

echo "<a href='index.php?page=energespsif.php&typee=1'>Ενεργές Ψηφορορίες</a><br><br>";

echo "<a href='index.php?page=energespsif.php&typee=2'>Ψηφοφοριες Οριστικοποιημένες</a><br><br>";

echo "<a href='index.php?page=energespsif.php'>Όλες οι Ψηφορορίες</a><br><br>";

echo "</center>";

?>
```

Αρχείο inspsif.php

```
<script>

function check()

{

s="";

f=true;

if (document.getElementById('titlos').value=="")

{

  s=s+"Δεν έδωσες Τίτλο\n";

  f=false;

}



if (document.getElementById('hmerominia1').value=="")
```

```
{
  s=s+"Δεν έδωσες Ημερομηνία έναρξης\n";
  f=false;
}
if (document.getElementById('hmerominia2').value=="")
{
  s=s+"Δεν έδωσες Ημερομηνία Λήξης\n";
  f=false;
}

if (f==false) alert (s);
return f;

}
</script>
<?php
$ins=0;
$msg="";



if (isset($_POST['vins']))
{
$f=0;
```

```
        $varxeio=$usr."_".$_FILES["varxeio"]["name"];
    if (move_uploaded_file($_FILES["varxeio"]["tmp_name"],
      "yliko/" .$usr."_".$_FILES["varxeio"]["name"])) $f=1;

        if ($f==1) {
                $sql45="insert into thema
(id_user,titlos,perigrafi,arxeio,hmerominia_enarxis,hmerominia_lixis)
                values
($kodikos_xristi,'$_POST[vtitlos]','$_POST[vperigrafi]','$varxeio','$_POST[vhmerominia1]','$_
POST[vhmerominia2]')";

                if (mysql_query($sql45))
                $msg= "<h3>Επιτυχής Καταχώρηση </h3>";
                else
                $msg="<h3>Η καταχώρηση απέτυχε ! </h3>";
        }
        else
        {
                $sql45="insert into thema
(id_user,titlos,perigrafi,hmerominia_enarxis,hmerominia_lixis)
                values
($kodikos_xristi,'$_POST[vtitlos]','$_POST[vperigrafi]','$_POST[vhmerominia1]','$_POST[vhm
erominia2]')";
```

```
                if (mysql_query($sql45))

                $msg= "<h3>Επιτυχής Καταχώρηση </h3>";

                else

                $msg="<h3>Η καταχώρηση απέτυχε ! </h3>";



        }

        $ins=1;

}




if (isset($_POST['vinsom']))

{

                $sql46="insert into thema_omada (id_thema,id_omada,typecon) values ($_POST[lstid],$_POST[vid],$_POST[typecon])";


        mysql_query($sql46);




                $ins=1;

}


if (isset($_POST['vdel']))

{

                $sql46="delete from thema_omada where id=$_POST[vid] ";
```

```
		mysql_query($sql46);



			$ins=1;
}
if (isset($_POST['vinsepil']))
{
			$sql46="insert into epiloges (epilogi,perigrafi,id_thema) values ('$_POST[vepilogi]','$_POST[vperigrafi]',$_POST[thmid])";

		mysql_query($sql46);



			$ins=2;
}
if (isset($_POST['vdelep']))
{
			$sql46="delete from epiloges where id=$_POST[vid] ";

		mysql_query($sql46);



			$ins=2;
```

```
}



echo "

<center>

<h3>Εισαγωγή Νέας Ψηφοφορίας</h3>

<hr>";

if (isset($_POST['vepomeno']))

{




$ins=2;

}




if (isset($_POST['vepomeno2']))

{

$msg= "<center>Η ψηφοφορία καταχωρήθηκε επιτυχώς</center>";



$ins=3;

}



echo $msg;

if ($ins==0)
```

```
{



echo "<form method=post action='' enctype='multipart/form-data' onsubmit=\"return check();\"><table>";

echo "   <tr><th>Τίτλος</th><td><input type=text name=vtitlos id=titlos></td></tr>

                <tr><th>Αρχείο</th><td><input type=file name=varxeio id=arxeio></td></tr>

                ";

echo "  <tr>

                <th>Περιγραφή</th>

                <td><textarea cols=80 rows=4 name=vperigrafi></textarea></td>

                </tr>

                <tr>

                <th>Ημερομηνία Έναρξης Ψηφοφορίας</th>

                <td><input type=date name=vhmerominia1 id=hmerominia1></td>

                </tr>

                <th>Ημερομηνία Λήξης Ψηφοφορίας</th>

                <td><input type=date name=vhmerominia2 id=hmerominia2></td>

                </tr>



                <tr><td colspan=2><center><input type=submit value='Εισαγωγή' name=vins></center></td></tr>

                ";
```

```
echo "</table></form>";

echo "<hr>";



}

if ($ins==1)

{


echo " <b> Προσθήκη ομάδων που έχουν δικαίωμα ψήφου στην συγκεκριμένη ψηφοφορία:</b><br>";


                echo "<table border=1 cellspacing=0 width=400px>";

        echo "<tr><td>Ομάδα</td><td>Τύπος Σύνδεσης</td><td>Λειτουργία</td></tr>";


        if (!isset($_POST['vinsom']))

                $thmid=mysql_insert_id();

                else

                $thmid=$_POST['lstid'];


          echo "<tr>

                <form action='' method=post><td><select name=vid>";

                $sql3="select * from omada";

                $res4=mysql_query($sql3);

                while ($row4=mysql_fetch_array($res4))

                {
```

```
                echo "<option value='$row4[id]'>$row4[titlos]</option>";
        }

        echo "
        </select>
        </td>
        <td>
        <select name=typecon>
        <option value=1>AND</option>
        <option value=2>OR</option>
        </select>
        </td>
        <td>
        <input type=hidden name=lstid value=$thmid>
        <input type=submit name=vinsom value='Προσθήκη'></td></form>
        </tr>";

        $sql4="select *,thema_omada.id as vid from thema_omada,omada where thema_omada.id_thema=$thmid and thema_omada.id_omada=omada.id order by thema_omada.id";
        $res4=mysql_query($sql4);

  echo "<tr><td colspan=2><b>Ομάδες</b></td><td><b>Τύπος Σύνδεσης</b></td></tr>";
```

```
$ii=0;
        while ($row4=mysql_fetch_array($res4))
        {
                echo "<tr><td>$row4[titlos]</td><td>";
                if ($row4['typecon']==1) echo "and";
                if ($row4['typecon']==2) echo "or";

                echo "</td>
                <td>
                <form action='' method=post name=fid$ii>
                <input type=submit name=vdel value='Διαγραφή'>
                <input type=hidden name=lstid value=$thmid>
                <input type=hidden value=$row4[vid] name=vid>
                </form>
                </td>
                </tr>";
                $ii++;
        }
        echo "</table>";


        echo "<form action='index.php?page=inspsif.php' method='post'>";
        echo "   <input type=hidden name=thmid value=$thmid>";
        echo " <input type=submit name=vepomeno value=\"Επόμενο\">";
```

```
        echo "</form>";

}

if ($ins==2)
{

echo " <b> Προσθήκη Επιλογών ψηφοφορίας:</b><br>";

                echo "<table border=1 cellspacing=0 width=400px>";
        echo "<tr><td>Επιλογή</td><td>Περιγραφή</td><td>Λειτουργία</td></tr>";

                $thmid=$_POST['thmid'];

            echo "<tr>
                <form action='' method=post>
                <td><input type=text name=vepilogi></td><td><input type=text name=vperigrafi size=40></td>
                <td>
                <input type=hidden name=thmid value=$thmid>
                <input type=submit name=vinsepil value='Προσθήκη'></td></form>
```

```
                </tr>";



                $sql4="select *,epiloges.id as vid from epiloges where epiloges.id_thema=$thmid";
                $res4=mysql_query($sql4);


  echo "<tr><td colspan=2><b>Επιλογή</b></td><td><b>Περιγραφή</b></td><td></td></tr>";
  $ii=0;
        while ($row4=mysql_fetch_array($res4))
        {
                echo "<tr><td>$row4[epilogi]</td><td>$row4[perigrafi]</td>";

                echo "<td>
                <form action='' method=post name=fid$ii>
                <input type=submit name=vdelep value='Διαγραφή'>
                <input type=hidden name=thmid value=$thmid>
                <input type=hidden value=$row4[vid] name=vid>
                </form>
                </td>
                </tr>";
                $ii++;
        }
```

```
        echo "</table>";



        echo "<form action='index.php?page=inspsif.php' method='post'>";
        echo "   <input type=hidden name=thmid value=$thmid>";
        echo " <input type=submit name=vepomeno2 value=\"Τέλος\">";
        echo "</form>";

}



?>
```

Αρχείο omada.php

```
<?php

if (isset($_POST['vins']))
{
        $sql32="insert into        omada(titlos,perigrafi)
values('$_POST[vonoma]','$_POST[vperigrafi]')";

        $r=mysql_query($sql32);
```

```
}

if (isset($_POST['vdel']))
{
        $sql32="delete from      omada where id = $_POST[vid]";

        $r=mysql_query($sql32);

}

if (isset($_POST['vedit']))
{
        $sql32="update omada set
        titlos='$_POST[vonoma]',
        perigrafi='$_POST[vperigrafi]'
        where id = $_POST[vid]";

        $r=mysql_query($sql32);

}
```

```
echo "<h3>Ομάδες</h3>";

 echo "<hr>";

 if ($role==1) echo "<h4>Εισαγωγή νέας Ομάδας<h4>";

 echo "<table border=1 cellspacing=0>";

 if ($role==1) echo "<tr><th>Κωδικός Ομάδας</th><th>Όνομα Ομάδας</th><th>Περιγραφή</th><th>Λειτουργίες</th></tr>";

 else echo "<tr><th>Κωδικός Ομάδας</th><th>Όνομα Ομάδας</th><th>Περιγραφή</th></tr>";

if ($role==1)

{




 echo "<form action='' method=post>

 <tr><td>-</td><td><input type=text name=vonoma></td>

 <td><input size=50 type=text name=vperigrafi></td>

 <td><input type=submit value=\"Εισαγωγή\" name=vins></td>

 </form>";


 echo "<tr><td colspan=4><hr>Προβολή-Επεξεργασία Στοιχείων Ομάδων</td></tr>";

}
```

```
if ($role==1)      $sql33="select * from omada";

else $sql33="select * from omada,users_omades where users_omades.id_omadas=omada.id and users_omades.id_user=$kodikos_xristi";

        $res=mysql_query($sql33);

        while($row33=mysql_fetch_array($res))

        {


        if ($role==1)

                                echo "<tr>

                                <form action='' method=post style=\"display:inline\" name=v$row33[id]>

                                <td>$row33[id]</td><td><input type=text value='$row33[titlos]' name=vonoma></td>

                                <td><input type=text value='$row33[perigrafi]' name=vperigrafi size=50></td><td>

                                <input type=hidden value=$row33[id] name=vid>

                                <input type=submit name=vedit value='Αποθήκευση Αλλαγών'> </form>

                                <form action='' method=post style=\"display:inline\" name='vd$row33[id]'>

                                <input type=hidden value=$row33[id] name=vid>

                                <input type=submit name=vdel value='Διαγραφή'> </form>


                                </td></tr>";


        else
```

```
                                    echo "<tr>


                                    <td>$row33[id]</td><td><input type=text readonly value='$row33[titlos]' name=vonoma></td>

                                    <td><input type=text readonly value='$row33[perigrafi]' name=vperigrafi size=50></td></tr>";




            }

            echo "</table>";



?>
```

Αρχείο omada.php

```
<center>

<script language='javascript'>

function check()

{

s="";

f=true;

if (document.getElementById('username').value=="")

{

  s=s+"You must give username\n";
```

```
  f=false;
}
if (document.getElementById('password').value=="")
{
  s=s+"You must give password\n";
  f=false;
}
if (document.getElementById('onoma').value=="")
{
  s=s+"You must give Name\n";
  f=false;
}
if (f==false) alert (s);
return f;

}

</script>
<?php
if (isset($_POST['apothikefti_button']))
{
if                              ($pss!=$_POST['password']){$pssupdate=md5($_POST['password']);
$_SESSION['pss']=md5($_POST['password']);}
else  $pssupdate=$pss;
```

```
if ($_FILES["photo"]["name"]=="") // den exw allaxei onoma eikonas

{

$sql="update users set password='$pssupdate',onoma ='".ecrypt_text($_POST['onoma'])."' where id=$kodikos_xristi";

if (mysql_query($sql))

{

echo "Η εισαγωγή χρήστη έγινε επιτυχώς!";



}

else {

echo "Λάθος στην αποθήκευση !";

}

}

else  // enallaktika allazw kai eikona

{

if ($_POST['fname']!="") unlink("images/$_POST[fname]");

$sql="update users set password='$pssupdate',onoma ='".ecrypt_text($_POST['onoma'])."',filephoto='$_POST[username]_".$_FILES["photo"]["nam e"]."' where id=$kodikos_xristi";

if (mysql_query($sql))

{

echo "Η εισαγωγή χρήστη έγινε επιτυχώς!";

 move_uploaded_file($_FILES["photo"]["tmp_name"],

"images/" .$_POST['username']."_".$_FILES["photo"]["name"]);
```

```
                }
                else
                {
                        echo "Λάθος στην αποθήκευση !";
                }
        }
}

echo "<table border=1 cellspacing=0><tr><td valign=top>";
$sql33="select * from users where id=$kodikos_xristi";
$res33=mysql_query($sql33);
$row33=mysql_fetch_array($res33);
        echo "
        <h3>Τα στοιχεία σας</h3>
        <hr>
        <form action='' method='post' enctype='multipart/form-data' onsubmit='return check();'>
        <table>
        <tr><td>Username:</td><td><input type='text' name=username id=username value=$row33[username] readonly></td></tr>
```

```
<tr><td>Password:</td><td><input type='password' name=password id=password value=$row33[password]><td></tr>

<tr><td>Ονοματεπώνυμο:</td><td><input type='text' name=onoma id=onoma value='".decrypt_text($row33['onoma'])."'></td></tr>

<tr><td>Φωτογραφία:</td><td>";


if ($row33['filephoto']<>"") echo "<img src='images/$row33[filephoto]' width=100><br>";

echo "<input type='file' name=photo >";

echo "

<input type=hidden name=fname value='$row33[filephoto]'>

</td></tr>

<tr><td>Τύπος Χρήστη:</td><td>";

if ($row33['type']==1) echo "Διαχειριστής";

if ($row33['type']==2) echo "Απλός Χρήστης";


echo "

</td></tr>

<tr><td colspan=2><br><center><input type=submit value='Αποθήκευση' name=apothikefti_button></center></td>

</tr>

</table>

</form>";

echo "</td>";

echo "<td valign=top>";
```

```
		$sql4="select *,users_omades.id as vid from users_omades,omada where users_omades.id_user=$kodikos_xristi and users_omades.id_omadas=omada.id ";
		$res4=mysql_query($sql4);
	echo "<h3>Ομάδες Χρήστη</h3>";
	echo "<hr>";

  echo "<table><tr><td>";
	echo "<b>Ομάδες που ανήκεται</b></td></tr>";
	while ($row4=mysql_fetch_array($res4))
	{
		echo "<tr><td>$row4[titlos]</td></tr>";
	}
	echo "</table>";

echo "</td>";
echo "</table>";

?>

</center>
```

Αρχείο profil.php

```
<center>
<script language='javascript'>
function check()
{
s="";
f=true;
if (document.getElementById('username').value=="")
{
  s=s+"You must give username\n";
  f=false;
}
if (document.getElementById('password').value=="")
{
  s=s+"You must give password\n";
  f=false;
}
if (document.getElementById('onoma').value=="")
{
  s=s+"You must give Name\n";
  f=false;
}
if (f==false) alert (s);
return f;
```

```
}


</script>
<?php
if (isset($_POST['apothikefti_button']))
{
if ($pss!=$_POST['password']){$pssupdate=md5($_POST['password']);
$_SESSION['pss']=md5($_POST['password']);}
else  $pssupdate=$pss;

        if ($_FILES["photo"]["name"]=="") // den exw allaxei onoma eikonas
        {
                $sql="update users set password='$pssupdate',onoma
='".ecrypt_text($_POST['onoma'])."' where id=$kodikos_xristi";
                        if (mysql_query($sql))
                {
                        echo "Η εισαγωγή χρήστη έγινε επιτυχώς!";


                }
                else {
                        echo "Λάθος στην αποθήκευση !";
                }
        }
        else  // enallaktika allazw kai eikona
```

```
	{
		if ($_POST['fname']!="") unlink("images/$_POST[fname]");
		$sql="update users set password='$pssupdate',onoma
='".ecrypt_text($_POST['onoma'])."',filephoto='$_POST[username]_".$_FILES["photo"]["nam
e"]."' where id=$kodikos_xristi";
		if (mysql_query($sql))
		{
			echo "Η εισαγωγή χρήστη έγινε επιτυχώς!";
			 move_uploaded_file($_FILES["photo"]["tmp_name"],
			"images/" .$_POST['username']."_".$_FILES["photo"]["name"]);
		}
		else
		{
			echo "Λάθος στην αποθήκευση !";
		}
	}









}


echo "<table border=1 cellspacing=0><tr><td valign=top>";
$sql33="select * from users where id=$kodikos_xristi";
```

```
$res33=mysql_query($sql33);

$row33=mysql_fetch_array($res33);

        echo "

        <h3>Τα στοιχεία σας</h3>

        <hr>

        <form action='' method='post' enctype='multipart/form-data' onsubmit='return check();'>

        <table>

        <tr><td>Username:</td><td><input type='text' name=username id=username value=$row33[username] readonly></td></tr>

        <tr><td>Password:</td><td><input type='password' name=password id=password value=$row33[password]><td></tr>

        <tr><td>Ονοματεπώνυμο:</td><td><input type='text' name=onoma id=onoma value='".decrypt_text($row33['onoma'])."'></td></tr>

        <tr><td>Φωτογραφία:</td><td>";


        if ($row33['filephoto']<>"") echo "<img src='images/$row33[filephoto]' width=100><br>";

        echo "<input type='file' name=photo >";

        echo "

        <input type=hidden name=fname value='$row33[filephoto]'>

        </td></tr>

        <tr><td>Τύπος Χρήστη:</td><td>";

        if ($row33['type']==1) echo "Διαχειριστής";

        if ($row33['type']==2) echo "Απλός Χρήστης";
```

```
        echo "
        </td></tr>
        <tr><td colspan=2><br><center><input type=submit value='Αποθήκευση' name=apothikefti_button></center></td>
        </tr>
        </table>
        </form>";
echo "</td>";
echo "<td valign=top>";
                $sql4="select *,users_omades.id as vid from users_omades,omada where users_omades.id_user=$kodikos_xristi and users_omades.id_omadas=omada.id ";
                $res4=mysql_query($sql4);
        echo "<h3>Ομάδες Χρήστη</h3>";
        echo "<hr>";

   echo "<table><tr><td>";
        echo "<b>Ομάδες που ανήκεται</b></td></tr>";
        while ($row4=mysql_fetch_array($res4))
        {
                echo "<tr><td>$row4[titlos]</td></tr>";
        }
        echo "</table>";
```

```
echo "</td>";

echo "</table>";




?>
```

Αρχείο epikoinonia.php

```
</center>


<div align="justify">
  <h2>Σύστημα e-Vote.</h2>
  <p> </p>
  <p><img src="images/2010-10-13-votemouse.jpg" width="130" height="79" align="left">
        Κεντρική Διαχείριση: τηλ. 6947413489, email: email@evote.gr .</p>
  <p> </p>
  <p>Διοικητική Υπηρεσία: τηλ 6947413489, email: dioikisi@evote.gr</p>
<p> </p>
</div>
```