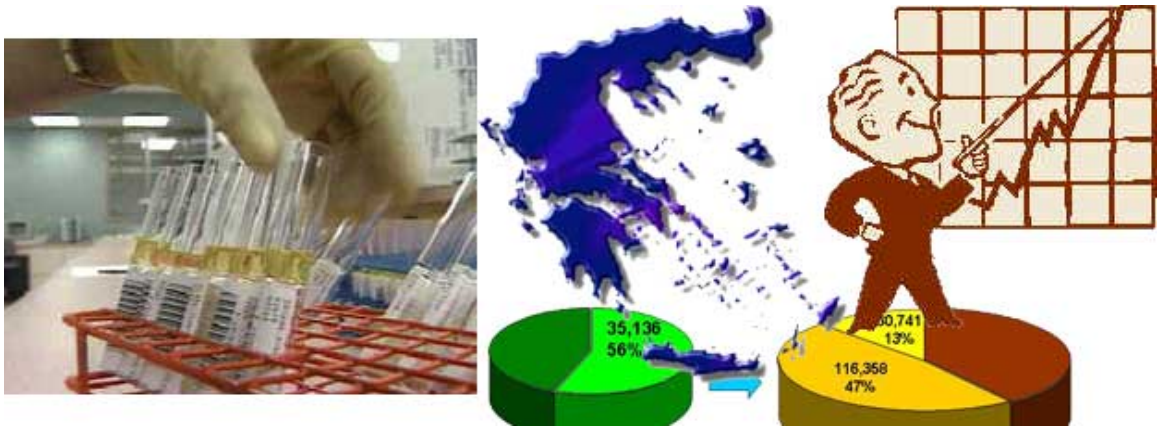
ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ



ΑΣΦΑΛΗΣ ΠΑΡΟΥΣΙΑΣΗ ΑΠΟΤΕΛΕΣΜΑΤΩΝ ΙΑΤΡΙΚΩΝ ΕΡΕΥΝΩΝ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ.

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ξυλάς Νέστορας

Επιβλέπων: Δ. Κουτσούρης
Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2005

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

ΑΣΦΑΛΗΣ ΠΑΡΟΥΣΙΑΣΗ ΑΠΟΤΕΛΕΣΜΑΤΩΝ ΙΑΤΡΙΚΩΝ ΕΡΕΥΝΩΝ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ.

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Νέστορας Ξυλάς

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την ..... Ιουλίου 2005.

.....	.....	.....
Δ. Κουτσούρης Καθηγητής Ε.Μ.Π.	Π. Τσανάκας Καθηγητής Ε.Μ.Π.	Κ. Νικήτα Αν. Καθηγήτρια Ε.Μ.Π.

Αθήνα, Ιούλιος 2005

Περίληψη

Η παρούσα εργασία αφορά στη μελέτη και ανάπτυξη μιας εφαρμογής για την καταχώρηση και αναζήτηση δεδομένων ιατρικών ερευνών (στην περίπτωσή μας αφορούν νευροψυχιατρικές παθήσεις) μέσω διαδικτύου. Στόχος είναι η δυνατότητα εύκολης πρόσβασης και αξιοποίησης των στοιχείων αυτών από ιατρικά κέντρα, επιστήμονες αλλά και απλούς ιατρούς, σε ότι αφορά τη στατιστική πλευρά αλλά και για την άμεση λήψη ιατρικών μέτρων όπου υπάρχει ανάγκη

Σε αυτό το πλαίσιο, πραγματοποιήθηκε αρχικά μια γενικότερη μελέτη των εμπλεκόμενων τεχνολογιών, που περιλαμβανουν μεταξύ άλλων τεχνολογίες βάσεων δεδομένων, γλώσσες προγραμματισμού διαδικτυακών εφαρμογών και εξυπηρετητές ιστοσελίδων. Εξετάστηκαν συγκριτικά διάφορες λύσεις και τελικά επιλέχτηκε για υλοποίηση η γλώσσα ASP, η χρήση του *MySQL* για την υλοποίηση της βάσης δεδομένων και του εξυπηρετητη ιστοσελίδων IIS. Επίσης, λόγω της ιδιαίτερα ευαίσθητης φύσης των ιατρικών δεδομένων, μελετήθηκε διεξοδικά το θέμα της ασφάλειας σε ιατρικα πληροφοριακά συστήματα καθώς και θεμάτα κρυπτογραφίας. Ειδικότερα, μελετήθηκαν τεχνικές ασφάλειας με χρήση του πρωτοκόλλου SSL και ψηφιακών πιστοποιητικών, καθώς φαίνεται να αποτελούν την defacto επιλογή για διαδικτυακές εφαρμογές.

Στα πλαίσια της υλοποίησης, δημιουργήθηκε μια βάση δεδομένων, όπου καταχωρούνται όλα τα στοιχεία της έρευνας συμπεριλαμβανομένων και των ευαίσθητων στοιχείων των ασθενών. Στη συνέχεια αναπτύχθηκε μια διαδικτυακή εφαρμογή, χρησιμοποιώντας τη γλώσσα δικτυακού προγραμματισμού ASP, που επιτρέπει την ασφαλή πρόσβαση των εξουσιοδοτημένων χρηστών (ερευνητών, ιατρών, κλπ) στα δεδομένα των ερευνών και την αναζήτηση και παρουσίαση των αποτελεσμάτων. Βασικά χαρακτηριστικά τόσο της εφαρμογής όσο και της βάσης δεδομένων είναι η ασφάλεια και η απλότητα. Με αυτό τον τρόπο εξασφαλίζεται η προστασία των ευαίσθητων ιατρικών δεδομένων, αλλά και η ευρεία χρήση της εφαρμογής χωρίς να απαιτείται ιδιαίτερο γνωστικό υπόβαθρο ή εκπαίδευση για τον χειρισμό της.

Λέξεις Κλειδιά

Βάσεις Δεδομένων, Ασφάλεια, Κρυπτογραφία, Ψηφιακή Υπογραφή, ASP, My SQL,SSL-πρωτόκολλο, SSL πιστοποιητικό.

Abstract

This thesis was primarily focused on the development of a method of keeping and searching data as a result of medical research through the internet. The main goal is the ability of easy access and use of these elements from medical centers, scientists, doctors, as far as the statistical point of view is concerned in order to take measures whenever is needed.

At this basis, a study of databases, languages concerning internet programming, security in medical informatics systems as well as cryptography took place. Several methods were examined and finally an ASP-based program was created, My SQL language was used for building a database, and also IIS Web Server was used. Because of the extremely sensitive nature of the data security issues were taken under very serious consideration and the SSL protocol was used because of its unique characteristics as well as the certificate method and the method of digital signatures.

The database contains general and sensitive medical information. The program offers an environment where statistical information can be edited after certain calculations through the database. Also, sensitive information can be acquired with safety only by authorized users (Doctors, Medical Labs etc). This is accomplished by the use of digital signatures, through an SSL – certificate and passwords. The basic characteristics of the program and the database are security and ease. That means that the safety of sensitive medical data is ensured, while at the same time the program remains simple and easy to use for non-expert personnel that will need no special training.

Keywords

Databases, Security, Cryptography, Digital Signature, ASP, My SQL, SSL - protocol, SSL - certificate.

Ευχαριστίες

Η διπλωματική αυτή εργασία εκπονήθηκε στο Εργαστήριο Βιοϊατρικής Τεχνολογίας του Τμήματος Ηλεκτρολόγων Μηχανικών και Μηχανικών Η/Υ του Εθνικού Μετσόβιου Πολυτεχνείου.

Οφείλω καταρχήν να ευχαριστήσω τον κ. Δημήτρη Κουτσούρη, Καθηγητή Ε.Μ.Π. και επιβλέποντα της διπλωματικής μου εργασίας, για την καθοδήγηση και την βοήθεια που μου πρόσφερε, καθώς και για την απλόχερη διάθεση του εργαστηρίου κάθε φορά που αυτό ήταν αναγκαίο.

Θερμές ευχαριστίες οφείλω στον προσωπικό μου γιατρό Δημήτριο Κουντούρη, ο οποίος με ενέπνευσε για το συγκεκριμένο θέμα, δίνοντάς μου τη δυνατότητα να αξιοποιήσω τα αποτελέσματα της επιστημονικής του μελέτης. Επιπλέον τον ευχαριστήσω και δημόσια για την απολύτως καθοριστική συμβολή του στην προσωπική μου υγεία.

Θερμές ευχαριστίες οφείλω επίσης στον υποψήφιο διδάκτορα Άγγελο Γεωργούλα που, μου έδωσε από την αρχή τη δυνατότητα να ζητώ οποτεδήποτε το χρειαζόμουν την πολύτιμη βοήθειά του χωρίς την οποία θα ήταν πολύ δύσκολη η εκπόνηση της συγκεκριμένης εργασίας.

Τέλος, θέλω να ευχαριστήσω τον συνάδελφο Φουντά Γιώργο και τον απόφοιτο πλέον Παγανέλη Κώστα για την κατά καιρούς συνεργασία και υπομονή τους για τις χρήσιμες προτάσεις και συμβουλές τους, καθώς και την οικογένειά μου για την διαρκή συμπαράσταση και ενθάρρυνσή της.

Πίνακας Περιεχομένων

Πίνακας Σχημάτων

Κατάλογος Στιγμιοτύπων (Screenshots) της εφαρμογής

Κατάλογος Πινάκων

Εισαγωγή

Σε αυτή τη διπλωματική εργασία δημιουργήθηκε μια εφαρμογή παρουσίασης στατιστικών και ευαίσθητων ιατρικών δεδομένων, που προκύπτουν από συγκεκριμένες μελέτες σε περιοχές της Ελλάδας, μέσω διαδικτύου. Τα δεδομένα αυτά καταχωρούνται σε μια βάση δεδομένων από την οποία στη συνέχεια ανακαλούνται και παρουσιάζονται αναλόγως με τις επιλογές του χρήστη. Στόχος είναι η αξιοποίησή τους από ιατρικά κέντρα, επιστήμονες αλλά και απλούς χρήστες σε ότι αφορά τη στατιστική πλευρά αλλά και για την άμεση λήψη ιατρικών μέτρων όπου υπάρχει ανάγκη.

Επίσης, μελετήθηκαν τα προβλήματα ασφαλείας που μπορεί να προκύψουν σε ένα τέτοιο ιατρικό πληροφοριακό σύστημα. Αναλύθηκαν οι επιπτώσεις και προτάθηκαν πιθανές λύσεις για αρκετά από αυτά. Μια τέτοια λύση είναι η χρήση ψηφιακού SSL πιστοποιητικού ψηφιακά υπογεγραμμένου, που αμέσως μετά την αποδοχή του από το χρήστη, εγκαθιστά μια κρυπτογραφημένη επικοινωνία σε συνδυασμό με τη χρήση κωδικού πρόσβασης.

Στη συνέχεια, σχεδιάστηκε και υλοποιήθηκε μια εφαρμογή που προσφέρει στον χρήστη την δυνατότητα αναζήτησης και παρουσίασης των στατιστικών αποτελεσμάτων από την περιοχή που επιθυμεί και στην οποία έχει γίνει η αντίστοιχη ιατρική έρευνα και το είδος των παθήσεων που θέλει να παρακολουθήσει στο προεπιλεγμένο δείγμα. Αν πρόκειται για εξουσιοδοτημένο χρήστη, τότε μπορεί με τη χρήση ειδικού κωδικού ασφαλείας που του παρέχεται από το ιατρικό κέντρο που χρησιμοποιεί την εφαρμογή, να αναζητήσει και τα προσωπικά δεδομένα (Ονοματεπώνυμο, Ταμείο Ασφάλισης κτλ) των ασθενών της προηγούμενης αναζήτησης. Επίσης μπορεί να καταχωρήσει τα δικά του στοιχεία από ειδική φόρμα καταχώρησης. Τέλος, υπάρχει επίσης η δυνατότητα επικοινωνίας, αποστολής άμεσης ιατρικών συμβουλών από τους εξουσιοδοτημένους χρήστες.

Η εργασία χωρίζεται σε δύο μέρη: Στο πρώτο μέρος υπάρχει η θεωρητική μελέτη και επεξεργασία, ενώ στο δεύτερο παρουσιάζεται ο τρόπος υλοποίησης της σε ότι αφορά τη βάση δεδομένων, βασικά τμήματα λειτουργίας του προγράμματος, θέματα ασφάλειας και το περιβάλλον παρουσίασης.

ΜΕΡΟΣ 1^{ο} Θεωρητική μελέτη

1. Βάσεις Δεδομένων

1.1. Γενικά

Οι βάσεις δεδομένων και τα συστήματα των βάσεων δεδομένων αποτελούν ένα σημαντικό στοιχείο της καθημερινής ζωής στη σύγχρονη κοινωνία. Για παράδειγμα, αν πάμε στην τράπεζα για κατάθεση η ανάληψη χρημάτων, αν κάνουμε κράτηση ξενοδοχείου η αεροπορικού ταξιδιού, αν ψάχνουμε βιβλιογραφικά στοιχεία από έναν κατάλογο βιβλιοθήκης η αν παραγγέλνουμε μια συνδρομή περιοδικού σ' έναν εκδότη, υπάρχει πιθανότητα η δραστηριότητα μας να περιλαμβάνει κάποια προσπέλαση σε βάση δεδομένων. Ακόμη και η αγορά αντικειμένων από ένα σούπερ μάρκετ σήμερα περιλαμβάνει σε πολλές περιπτώσεις ενημέρωση της βάσης δεδομένων όπου καταχωρούνται τα αποθέματα των προϊόντων του σούπερ μάρκετ.

Αυτές οι διεπαφές είναι παραδείγματα αυτού που αποκαλούμε **παραδοσιακές εφαρμογές των βάσεων δεδομένων**, όπου οι περισσότερες αποθηκευμένες πληροφορίες είναι ή σε μορφή text ή σε μορφή αριθμών. Τα τελευταία χρόνια η πρόοδος στην τεχνολογία έχει οδηγήσει σε συναρπαστικές νέες εφαρμογές των συστημάτων βάσεων δεδομένων. Οι **βάσεις δεδομένων πολυμέσων** μπορούν σήμερα να αποθηκεύσουν εικόνες, video και μηνύματα ήχου. **Τα γεωγραφικά πληροφοριακά συστήματα (GIS)** μπορούν να αποθηκεύσουν και να αναλύσουν δεδομένα καιρού και δορυφορικές εικόνες. Οι **αποθήκες δεδομένων** και τα **on-line συστήματα αναλυτικής επεξεργασίας (OLAP)** χρησιμοποιούνται σε πολλές εταιρείες για την εξαγωγή και ανάλυση χρήσιμων πληροφοριών από μεγάλες βάσεις δεδομένων για λήψη αποφάσεων. Οι **βάσεις δεδομένων πραγματικού χρόνου** και **η τεχνολογία των ενεργών βάσεων δεδομένων** χρησιμοποιούνται για τον έλεγχο των βιομηχανικών και παραγωγικών διαδικασιών. Οι τεχνικές αναζήτησης των βάσεων δεδομένων έχουν εφαρμοσθεί στο WEB για τη βελτίωση της αναζήτησης πληροφοριών για τις οποίες ερευνούν οι χρήστες που περιηγούνται το διαδύκτιο.

Οι βάσεις δεδομένων και η τεχνολογία βάσεων δεδομένων εξασκούν σημαντική επίδραση στην αυξανόμενη χρήση των υπολογιστών. Είναι εύλογο να ειπωθεί ότι οι βάσεις δεδομένων θα διαδραματίσουν κρίσιμο ρόλο σε όλες τις περιοχές όπου χρησιμοποιούνται υπολογιστές όπως στις επιχειρήσεις, στη μηχανική, στην ιατρική, στα νομικά, στην εκπαίδευση και στη βιβλιοθηκονομία, για να αναφέρουμε μερικές μόνο από αυτές.

Βάση δεδομένων (database) είναι μια συλλογή από σχετιζόμενα δεδομένα. Με τον όρο **δεδομένα** εννοούμε γνωστά γεγονότα που μπορούν να καταγραφούν και που έχουν κάποια

υπονοούμενη σημασία. Για παράδειγμα θεωρήστε τα ονόματα, τους αριθμούς τηλεφώνων και τις διευθύνσεις των ανθρώπων που γνωρίζετε. Μπορεί να έχετε καταγράψει αυτά τα δεδομένα σ' ένα ευρετήριο διευθύνσεων ή μπορεί να τα έχετε αποθηκεύσει σε μια δισκέτα χρησιμοποιώντας έναν προσωπικό υπολογιστή και λογισμικό όπως το DBASE IV ή V, το PARADOX ή το EXCEL. Αυτή είναι μια συλλογή από σχετιζόμενα δεδομένα με υπονοούμενη σημασία και, επομένως, μια βάση δεδομένων.

Ο πιο πάνω ορισμός της βάσης δεδομένων είναι αρκετά γενικός. Για παράδειγμα, μπορούμε να θεωρήσουμε ότι οι λέξεις του κειμένου αυτής της σελίδας σχετίζονται μεταξύ τους και κατά συνέπεια συνιστούν μια βάση δεδομένων. Ωστόσο, η συνήθης χρήση του όρου βάση δεδομένων είναι αρκετά πιο περιορισμένη. Μια βάση δεδομένων έχει τις ακόλουθες υπονοούμενες ιδιότητες:

- Μια βάση δεδομένων αναπαριστά κάποια άποψη του πραγματικού κόσμου η οποία μερικές φορές λέγεται μικρόκοσμος (miniworld) ή πεδίο αναφοράς (Universe of Discource, UoD). Οι αλλαγές στον μικρόκοσμο αντανακλώνται στη βάση δεδομένων.
- Μια βάση δεδομένων είναι μια λογικά συνεκτική συλλογή δεδομένων που έχει κάποια εγγενή σημασία. Μια τυχαία διευθέτηση δεδομένων δεν είναι σωστό να αναφέρεται ως βάση δεδομένων.
- Μια βάση δεδομένων σχεδιάζεται, χτίζεται και γεμίζει με δεδομένα για κάποιο συγκεκριμένο σκοπό. Προορίζεται για μια συγκεκριμένη ομάδα χρηστών και για κάποιες προκαθορισμένες εφαρμογές για τις οποίες οι χρήστες αυτοί ενδιαφέρονται.

Με άλλα λόγια, κάθε βάση δεδομένων έχει κάποια πηγή από την οποία παράγονται τα δεδομένα, αλληλεπιδρά σε κάποιο βαθμό με γεγονότα του πραγματικού κόσμου και απευθύνεται σ' ένα ακροατήριο που ενδιαφέρεται ενεργά για το περιεχόμενο της.

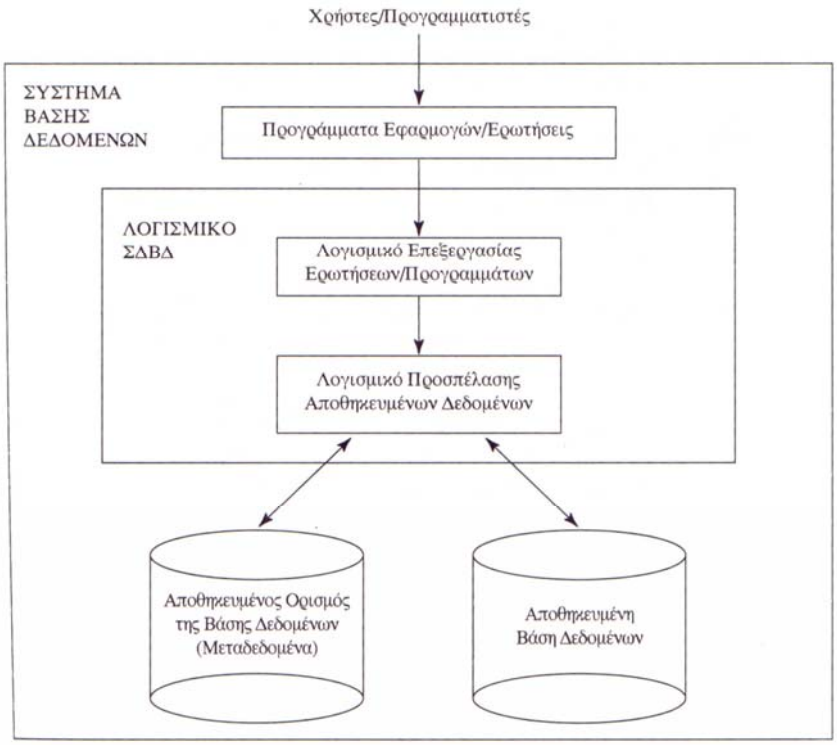
Μια βάση δεδομένων μπορεί να έχει οποιοδήποτε μέγεθος και κυμαινόμενη πολυπλοκότητα. Για παράδειγμα, η λίστα ονομάτων και διευθύνσεων που αναφέρθηκε προηγουμένως μπορεί να αποτελείται μόνο από λίγες εκατοντάδες εγγραφές, που κάθε μια τους έχει κάποια απλή δομή. Από την άλλη πλευρά, ο κατάλογος με τις κάρτες μιας μεγάλης βιβλιοθήκης μπορεί να περιέχει μισό εκατομμύριο κάρτες αποθηκευμένες υπό διαφορετικές κατηγορίες ως προς το όνομα του βασικού συγγραφέα, ως προς το θέμα, ως προς τον τίτλο βιβλίου με κάθε κατηγορία οργανωμένη κατά αλφαβητική σειρά. Μια βάση δεδομένων ακόμη μεγαλύτερου μεγέθους και πολυπλοκότητας διατηρεί η Εφορία για να διαχειρίζεται τις δηλώσεις που υποβάλλουν οι φορολογούμενοι στις Ηνωμένες Πολιτείες. Αν υποθέσουμε ότι υπάρχουν 100 εκατομμύρια φορολογούμενοι και ότι κάθε φορολογούμενος συμπληρώνει κατά μέσον όρο πέντε φόρμες με

200 χαρακτήρες πληροφορίας σε κάθε φόρμα, θα έχουμε μια βάση δεδομένων με 100*(10^6)*200*5 χαρακτήρες ή μπάιτ (Bytes) πληροφοριών. Υποθέτοντας ότι η Εφορία κρατά στοιχεία για τις τελευταίες τρεις δηλώσεις κάθε φορολογούμενου καθώς και για την τρέχουσα δήλωση, θα είχαμε μια βάση δεδομένων με 4*(10") μπάιτ. Αυτόν τον τεράστιο όγκο πληροφοριών πρέπει να τον οργανώσουμε και να τον διαχειριστούμε κατά τέτοιον τρόπο ώστε οι χρήστες να μπορούν να αναζητήσουν, να ανακτήσουν και να ενημερώσουν τα δεδομένα που χρειάζονται.

Μια βάση δεδομένων μπορεί να δημιουργηθεί και να συντηρηθεί είτε χειρόγραφα είτε με χρήση μηχανών. Ο κατάλογος καρτών μιας βιβλιοθήκης είναι παράδειγμα βάσης δεδομένων που μπορεί να δημιουργηθεί και να συντηρείται χειρόγραφα. Μια βάση δεδομένων σε υπολογιστή μπορεί να δημιουργηθεί και να συντηρείται είτε από μια ομάδα προγραμμάτων εφαρμογών που έχουν γραφεί ειδικά για το σκοπό αυτόν, είτε από ένα σύστημα διαχείρισης βάσεων δεδομένων.

Σύστημα Διαχείρισης Βάσεων Δεδομένων (ΣΔΒΔ) (DataBase Management System-DBMS) είναι μια συλλογή από προγράμματα που επιτρέπουν στους χρήστες να δημιουργήσουν και να συντηρήσουν μια βάση δεδομένων. Επομένως, το **ΣΔΒΔ** είναι ένα γενικής χρήσης (general-purpose) σύστημα λογισμικού που διευκολύνει τις διαδικασίες ορισμοί), *κατασκευής* και χειρισμού βάσεων δεδομένων για διάφορες εφαρμογές. Ο **ορισμός** (definition) μιας βάσης δεδομένων περιλαμβάνει την προδιαγραφή των τύπων, των δομών και των περιορισμών των δεδομένων που θα αποθηκευτούν στη βάση. **Κατασκευή** (construction) μιας βάσης δεδομένων είναι η διαδικασία αποθήκευσης των ίδιων των δεδομένων σ' ένα μέσο αποθήκευσης που ελέγχεται από το ΣΔΒΔ. Ο **χειρισμός** (manipulation) μιας βάσης δεδομένων περιλαμβάνει λειτουργίες όπως υποβολή επερωτήσεων (queries) προς τη βάση για ανάκτηση συγκεκριμένων δεδομένων, ενημέρωση της βάσης ώστε να αντανακλά αλλαγές στο μικρόκοσμο και παραγωγή αναφορών από τα δεδομένα.

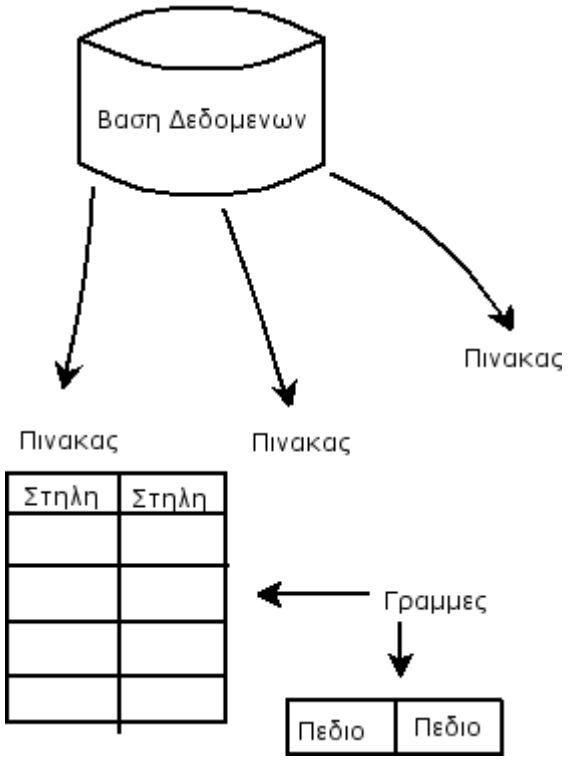
Δεν είναι απαραίτητο να χρησιμοποιήσουμε γενικής χρήσης λογισμικό ΣΔΒΔ για την υλοποίηση μιας βάσης δεδομένων σε υπολογιστή, θα μπορούσαμε να γράψουμε ένα δικό μας σύνολο προγραμμάτων για τη δημιουργία και τη συντήρηση της βάσης δεδομένων, δημιουργώντας στην πραγματικότητα ένα δικό μας ειδικού *σκοπού* (special-purpose) λογισμικό ΣΔΒΔ. Σε κάθε περίπτωση - είτε δουλεύουμε με ένα γενικής χρήσης ΣΔΒΔ είτε όχι πρέπει συνήθως, εκτός από την ίδια τη βάση δεδομένων, να χρησιμοποιήσουμε κι ένα μεγάλο όγκο λογισμικού για το χειρισμό της. Μια βάση δεδομένων, μαζί με το αντίστοιχο λογισμικό, θα την ονομάσουμε **σύστημα βάσης δεδομένων** (database - system). Η εικόνα που ακολουθεί επεξηγεί αυτές τις ιδέες.[i]



Σχήμα 1:Ένα απλουστευμένο περιβάλλον συστήματος βάσης δεδομένων που δείχνει τις έννοιες. και την ορολογία του εδαφίου 1.1

Μια βάση δεδομένων οργανώνεται με τον ακόλουθο ιεραρχικά τρόπο, από την κορυφή προς τη βάση. Ξεκινάμε από μια βάση δεδομένων που περιέχει ένα αριθμό πινάκων. Κάθε πίνακας αποτελείται από μια σειρά στήλες. Τα δεδομένα αποθηκεύονται σε γραμμές και η τοποθεσία όπου κάθε γραμμή intersects μια στήλη είναι γνωστά σαν πεδίο.

Για παράδειγμα στο βιβλιοπωλείο μας υπάρχει μια βάση δεδομένων. Αυτή η βάση, αποτελείται από πολλούς πίνακες. Κάθε πίνακας περιέχει συγκεκριμένα δεδομένα. Θα μπορούσε δηλαδή να υπάρχει ο πίνακας "Συγγραφείς" ή ο πίνακας "Βιβλία". Αυτοί οι πίνακες δημιουργούνται από ονομαζόμενες στήλες που μας πληροφορούν σχετικά με το τι δεδομένα είναι αποθηκευμένα σε αυτές. Όταν γίνει μια εγγραφή γίνει στον πίνακα δημιουργείται μια γραμμή δεδομένων. Όταν μια γραμμή και μια στήλη intersects τότε δημιουργείται ένα πεδίο (field)[106]



Σχήμα 2: Ανατομία μιας βάσης δεδομένων.

1.2. *MySQL* – Τι είναι; Γιατί χρησιμοποιήθηκε;

Η *MySQL* που προφερόταν "My Ess Que El" είναι ένα ανοικτού κώδικα (open source), επιπέδου *Enterprise*, πολύ-νηματικό (multi-threaded) σχεσιακό σύστημα διαχείρισης βάσης δεδομένων. Η *MySQL* αναπτύχθηκε από μια εταιρία συμβούλων στη Σουηδία που ονομάζεται TcX. Χρειαζόταν ένα σύστημα βάσης δεδομένων το οποίο θα ήταν εξαιρετικά γρήγορο και ευέλικτο. Έτσι δημιουργήθηκε η *MySQL* που κατα βάση στηρίζεται σε ένα άλλο σύστημα διαχείρισης βάσεων δεδομένων που αποκαλούνταν *mSQL*. Το προϊόν το οποίο δημιουργήθηκε είναι γρήγορο, αξιόπιστο, και εξαιρετικά ευέλικτο. Χρησιμοποιείται σε πολλά μέρη του κόσμου, σε οργανισμούς όπως Πανεπιστήμια, παροχείς υπηρεσιών Internet και μη κερδοσκοπικούς οργανισμούς κυρίως λόγω του χαμηλού κόστους της (γενικά είναι δωρεάν). Εντούτοις, τελευταία έχει αρχίσει να διεισδύει και στον εμπορικό κόσμο σαν ένα αξιόπιστο και γρήγορο σύστημα βάσεων δεδομένων. Ο λόγος της ανάπτυξης της φήμης της *MySQL* είναι το αποτέλεσμα του κινήματος λογισμικού ανοικτού κώδικα στην βιομηχανία των υπολογιστών. Το κίνημα του λογισμικού ανοικτού κώδικα είναι το αποτέλεσμα διαφόρων παραγωγών λογισμικού υπολογιστών που παρέχουν όχι μόνο ένα προϊόν αλλά και τον κώδικα με τον οποίο αυτό έχει δημιουργηθεί (source code). Αυτό επιτρέπει στους καταναλωτές να διαπιστώσουν πως το πρόγραμμά τους λειτουργεί και να το τροποποιήσουν όπου θέλουν. Σκοπός της *MySQL* γλώσσας ήταν να είναι εύχρηστη και η

σύνταξή της να μοιάζει πολύ στη σύνταξη της Αγγλικής γλώσσας. Και πράγματι έτσι και έγινε. Για παράδειγμα αν θέλουμε να μάθουμε όλα τα ονόματα ατόμων που γεννήθηκαν τον Γενάρη σε μια βάση δεδομένων η SQL δήλωση θα ήταν κάπως έτσι:

```
    SELECT First_Name, Last_Name FROM Customers WHERE DOB=
"January"
```

Για να ξεκινήσουμε να "μιλάμε" στη βάση μας πρέπει πρώτα να ανοίξουμε μια γραμμή επικοινωνίας με αυτή. Η *MySQL* παρέχει μια εφαρμογή για να επιτευχθεί αυτό το *MySQL monitor*. Είναι πολύ σημαντικό να γνωρίζουμε ότι στη *MySQL* αφού κάνεις μια ερώτηση η δώσεις μια εντολή δεν υπάρχει περίπτωση να ανακληθεί. Η εντολή εκτελείται χωρίς κανένα δισταγμό ή προειδοποίηση. Δεν είναι λίγες οι περιπτώσεις απώλειας δεδομένων από μια απρόσεκτη εντολή *DELETE*.

Άλλα προγράμματα που διαχειρίζονται βάσεις δεδομένων είναι ο SQL Server της Microsoft, ο Sybase Adaptive Server και ο DB2.[ii]

1.3. Σύνδεση με τη βάση δεδομένων.

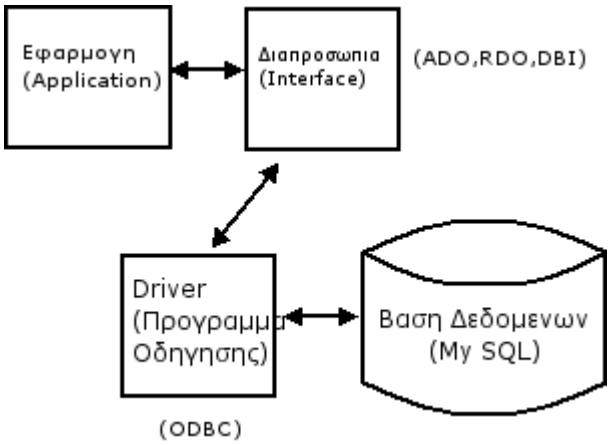
Μια εφαρμογή παρουσίασης (όπως αυτή που αναπτύχθηκε στα πλαίσια της εργασίας) "συναλλάσσεται" με κάποιο τρόπο με τη βάση δεδομένων. Ο εξυπηρετητής της βάση (database server) είναι ένα πρόγραμμα το οποίο τρέχει συνεχώς στο παρασκήνιο. Είναι γνωστοί σαν υπηρεσίες ή δαίμονες (deamons) ανάλογα με το πιο σύστημα επικοινωνίας χρησιμοποιείται. Για να αξιοποιήσουμε τη βάση δεδομένων πρέπει πρώτα να εγκαθιδρύσουμε μια σύνδεση με αυτό το πρόγραμμα του εξυπηρετητή. Αυτή συνήθως εξασφαλίζεται διαμέσου κάποιου είδους διαπροσωπίας (interface).

Μια διαπροσωπία είναι ένα υπόστρωμα (layer) ανάμεσα στο πρόγραμμά μας και τη βάση δεδομένων το οποίο λειτουργεί κατά κάποιο τρόπο σαν διαμεσολαβητής. Οι εντολές οι οποίες δίνονται από το πρόγραμμά μας αναπαριστώνται διαμέσου αυτού του διαμεσολαβητή, και μεταφράζονται για τη βάση δεδομένων. Το υπόστρωμα είναι απλά μια συλλογή λειτουργιών (Functions) οι οποίες είναι διαθέσιμες στον προγραμματιστή. Μπορεί να τις χρησιμοποιήσει για να πετύχει συγκεκριμένες εργασίες σχετικά με τη βάση.

Υπάρχουν γενικά δυο ειδών υποστρώματα. Το ένα μέρος είναι ουσιαστικά ο κώδικας που χρησιμοποιούμε στην εφαρμογή μας. Αυτό το μέρος περιλαμβάνει τις μεταβλητές και τις καλούμενες λειτουργίες. Επίσης το μέρος αυτό είναι κοινό, που σημαίνει ότι ανεξάρτητα

από το πια βάση δεδομένων χρησιμοποιείς, οι λειτουργίες και οι μεταβλητές παραμένουν ίδιες.

Το δεύτερο κομμάτι αποκαλείται πρόγραμμα οδήγησης της βάση δεδομένων (Driver). Αυτό το κομμάτι παίρνει τις κλήσεις για διάφορες λειτουργίες από το πρώτο κομμάτι, τις μεταφράζει και στη συνέχεια αλληλεπιδρά με τη βάση για να παράγει τα ζητούμενα αποτελέσματα. Τα προγράμματα οδήγησης συνήθως φτιάχνονται από τους κατασκευαστές των βάσεων δεδομένων και είναι συγκεκριμένα για τη βάση.



Σχήμα 3: Από την εφαρμογή στην βάση δεδομένων.

Υπάρχουν πολλές διαπροσωπίες / προγράμματα οδήγησης διαθέσιμα για την *MySQL*. Οι Perl, PHP, C++, Python και ODBC είναι μόνο μερικοί από τις διαπροσωπίες. Τέλος, όπως φαίνεται αναλυτικά και παρακάτω, εμείς έχουμε εγκαταστήσει για την εφαρμογή μας το πρόγραμμα οδήγησης ODBC.

Πέρα όμως από το πρόγραμμα οδήγησης της βάσης, υπάρχουν και άλλα στοιχεία που είναι απαραίτητα για το πρόγραμμα οδήγησης προκειμένου να έχει πρόσβαση στη βάση μας. Ένα από αυτά είναι το όνομα ή η διεύθυνση του εξυπηρετητή όπου η βάση εδράζεται. Επίσης η IP διεύθυνσή του εξυπηρετητή ή αν χρησιμοποιείται δυναμική IP το όνομα του εξυπηρετητή. Τέλος, απαιτείται όνομα χρήστη (username) και κωδικός πρόσβασης (password) για λόγους ασφάλειας.

2. Ασφάλεια της Πληροφορίας στον τομέα της Ιατρικής Φροντίδας

2.1. Παραβίαση της ηλεκτρονικής ασφάλειας σε Νοσοκομεία

Είναι δεδομένο πως η πληροφορία που σχετίζεται με ένα σύστημα Ιατρικής Φροντίδας είναι ζωτικής σημασίας και ο χειρισμός της πρέπει να γίνεται με τη μεγαλύτερη δυνατή ασφάλεια. Για να γίνει κάτι τέτοιο όμως πρέπει να κατανοήσουμε πρώτα ποιες ακριβώς μπορεί να είναι οι ενδεχόμενες απειλές. Είναι σημαντικό να πληροφορούμαστε και να κατανοούμε που και πως συνέβησαν περιστατικά παραβίασης της ηλεκτρονικής ασφάλειας, προκειμένου να θωρακίσουμε πιο αποτελεσματικά το σχεδιαζόμενο σύστημα.

Το καλοκαίρι του 2000, ένας χάκερ με το ψευδώνυμο Kane, κατέλαβε μεγάλο μέρος του εσωτερικού δικτύου του Ιατρικού κέντρου του Πανεπιστημίου της Ουάσιγκτον και απέκτησε πρόσβαση σε περίπου 4.000 έγγραφα που αφορούσαν ισάριθμους ασθενείς με καρδιολογικά προβλήματα [iii]. Τα αρχεία αυτά περιείχαν ονοματεπώνυμο, διεύθυνση, ημερομηνία γέννησης, αριθμό κοινωνικής ασφάλισης, ύψος και βάρος για καθέναν από τους ασθενείς καθώς και την περιγραφή της ιατρικής αγωγής που έλαβαν. Άλλο αρχείο περιείχε παρόμοιες πληροφορίες για περίπου 700 άτομα που υποβάλλονταν σε φυσιοθεραπεία. Ένα ακόμη αρχείο απαριθμεί τις εισαγωγές, τα εξιτήρια και τις μεταφορές του κάθε ασθενούς στο νοσοκομείο για ένα διάστημα πέντε μηνών.

Τα κίνητρα του Kane, σύμφωνα με τα λεγόμενά του, είναι η αποκάλυψη των ελλείψεων στην ασφάλεια ευαίσθητων δεδομένων. Η δράση του αυτή ξεκίνησε ύστερα από μια συζήτηση που είχε με έναν συμφοιτητή του, κατά τη διάρκεια της οποίας αναρωτήθηκαν κατά πόσον προστατεύονται πραγματικά, τα ανά τον κόσμο απόρρητα δεδομένα. "Η συζήτηση κατέληξε στα ιατρικά δεδομένα, που είναι όντως απόρρητα και σκέφτηκα να ρίξω μια ματιά τριγύρω" αναφέρει ο Kane. Το συγκεκριμένο νοσοκομείο είχε λάβει την δέκατη τρίτη θέση στην ετήσια λίστα που δημοσιεύει η "U.S. News & World Report's" με τα καλύτερα νοσοκομεία σε όλη την επικράτεια των Ενωμένων Πολιτειών.

Το συγκεκριμένο παράδειγμα δείχνει πόσο ευάλωτοι είναι κάποιοι στόχοι που θα έπρεπε να είναι ασφαλείς. Τα πράγματα θα ήταν πολύ χειρότερα εάν ο εισβολέας μετέβαλε κάποια δεδομένα και στη συνέχεια αποχωρούσε χωρίς να αφήσει ίχνη: Ένα παρόμοιο περιστατικό φαίνεται να έγινε το 1998 και μάλιστα σε ιατρική βάση δεδομένων του Υπουργείου Άμυνας (DoD) των Ενωμένων Πολιτειών[iv]. Χάκερς διείσδυσαν στην βάση δεδομένων και άλλαξαν τις ομάδες αίματος ασθενών. Αργότερα ο εκπρόσωπος του

Πενταγώνου ξεκαθάρισε ότι αυτή η ενέργεια ήταν μέρος άσκησης που σκοπό είχε να δοκιμάσει την ασφάλεια του συστήματος, η οποία μάλιστα, βρισκόταν ακόμα σε στάδιο ανάπτυξης και δεν είχε τελειοποιηθεί. Σύμφωνα με τις ίδιες δηλώσεις, δεν μεταβλήθηκαν στην πραγματικότητα οποιαδήποτε ηλεκτρονικά δεδομένα. Η άσκηση αυτή ήταν μέρος μιας γενικότερης προσομοίωσης "ηλεκτρονικού πολέμου". Υπό φυσιολογικές συνθήκες αυτή η βάση δεδομένων δεν συνδέεται καν με το Ίντερνετ για λόγους ασφαλείας.

Στην εργασία αυτή θα ασχοληθούμε με το πως μπορούμε να προστατέψουμε ένα σύστημα από την μη εξουσιοδοτημένη πρόσβαση με τη χρήση κωδικών ασφαλείας. Όπως θα δούμε, η κρυπτογραφία και έννοιες όπως η ψηφιακή υπογραφή, μπορούν να αποδειχτούν πολύ ισχυρά μέσα θωράκισης των δεδομένων μας.

2.2. Κρισιμότητα της πληροφορίας και βασικές αρχές ασφάλειας

Στον τομέα της Ιατρικής Φροντίδας η κρισιμότητα της πληροφορίας είναι ένα βασικό χαρακτηριστικό, αφού αυτή μπορεί να αφορά άμεσα την ανθρώπινη ζωή. Ο βαθμός της κρισιμότητας της πληροφορίας ποικίλει ανάλογα με το περιεχόμενό της (για παράδειγμα η διάγνωση για AIDS είναι προφανώς πολύ πιο κρίσιμη από τη διάγνωση ενός κρυολογήματος). Με βάση αυτά τα χαρακτηριστικά καθορίζονται οι απαιτήσεις ασφάλειας ενός πληροφοριακού συστήματος Ιατρικής Φροντίδας. Μπορούμε να ταξινομήσουμε τις απαιτήσεις αυτές όπως παρουσιάζονται συνοπτικά παρακάτω [v]:

<u>Εμπιστευτικότητα</u>

Ως εμπιστευτικότητα ορίζεται «η αποφυγή διάθεσης ή αποκάλυψης πληροφορίας σε μη εξουσιοδοτημένα πρόσωπα, οντότητες ή διεργασίες». Στον τομέα της Ιατρικής φροντίδας η εμπιστευτικότητα ερμηνεύεται ως διαφύλαξη της προσωπικής πληροφορίας και του ιατρικού απορρήτου. Το θέμα αυτό είναι ιδιαίτερα σημαντικό σε ιατρικά πληροφοριακά συστήματα, όπου περιλαμβάνονται δεδομένα άμεσα συνδεόμενα με αναγνωρίσιμα άτομα, τις ασθένειες, τις θεραπείες τους και συχνά τις κοινωνικές τους συνήθειες. Τα δεδομένα αυτά θεωρούνται αυστηρώς εμπιστευτικά και η αποκάλυψή τους μπορεί να έχει σημαντικές επιπτώσεις στη κοινωνική θέση, στην υγεία ή ακόμα και στη ζωή των σχετιζόμενων ατόμων.

<u>Ακεραιότητα</u>

Ως ακεραιότητα ορίζεται «η αποφυγή μεταβολής ή καταστροφής δεδομένων με μη εξουσιοδοτημένο τρόπο». Στον τομέα της Ιατρικής φροντίδας όπου τα δεδομένα π.χ. εξετάσεων ή οι διαγνώσεις και οι συνταγογραφήσεις γιατρών είναι συχνά το βασικό μέσο

απόφασης σχετικά με τη θεραπεία και τον τρόπο ζωής των ασθενών, η ακεραιότητα της πληροφορίας (πληρότητα, ορθότητα και ακρίβεια) είναι ζωτικής σημασίας.

Αναγνώριση και αυθεντικοποίηση

Ως αναγνώριση εννοείται η διαδικασία που επιτρέπει την αποδοχή της ταυτότητας μιας οντότητας από ένα πληροφοριακό σύστημα. Ως αυθεντικοποίηση ορίζεται «η διαδικασία της αξιόπιστης αναγνώρισης οντοτήτων μέσω της ασφαλούς συσχέτισης ενός πιστοποιημένου αναγνωριστικού με τις οντότητες αυτές». Στον τομέα της Ιατρικής φροντίδας το θέμα της αυθεντικοποίησης είναι ιδιαίτερα σημαντικό σε περιπτώσεις συστημάτων όπου η πρόσβαση πρέπει να επιτρέπεται μόνο σε εξειδικευμένο ιατρικό προσωπικό. (π.χ. η διαχείριση ιατρικού φακέλου ασθενούς).

Μη άρνηση αποστολής/λήψης πληροφορίας

Ως μη άρνηση αποστολής πληροφορίας ορίζεται η διαδικασία κατά την οποία η οντότητα που λαμβάνει τα δεδομένα μπορεί να αποδείξει ότι αυτά εστάλησαν από συγκεκριμένο αποστολέα, έτσι ώστε αυτός να μη μπορεί να δηλώσει ψευδώς ότι δεν τα έστειλε. Αντίστροφα μη άρνηση λήψης πληροφορίας ορίζεται η διαδικασία κατά την οποία η οντότητα που στέλνει δεδομένα μπορεί να αποδείξει ότι τα δεδομένα έφτασαν στον παραλήπτη, έτσι ώστε αυτός να μη μπορεί ψευδώς να δηλώσει ότι δεν τα έλαβε. Οι απαιτήσεις αυτές είναι ιδιαίτερα σημαντικές σε συστήματα ανταλλαγής πληροφοριών δεδομένων, όπως για παράδειγμα στην περίπτωση επικοινωνίας δύο γιατρών σχετικά με μία εμπιστευτική υπόθεση όπου και τα δύο συναλλασσόμενα μέρη πρέπει να είναι εξασφαλισμένα σχετικά με την ορθή αποστολή και λήψη της πληροφορίας.

Απόδειξη χρόνου αποστολής – λήψης πληροφορίας

Ο χρόνος αποστολής λήψης πληροφορίας στον τομέα της Ιατρικής φροντίδας σε κάποιες περιπτώσεις όπως π.χ. κατά την έκδοση επιδημιολογικών αποτελεσμάτων εργαστηρίων μπορεί να είναι ιδιαίτερα κρίσιμος και έτσι θα πρέπει να μπορεί να αποδεικνύεται τόσο από την πλευρά του αποστολέα, όσο και από την πλευρά του παραλήπτη. Η απαίτηση αυτή ουσιαστικά εξασφαλίζει και τη μοναδικότητα της διακινούμενης πληροφορίας μέσω της σύνδεσής της με μία μοναδική στιγμή στο χρόνο.

Διαθεσιμότητα

Ως διαθεσιμότητα ορίζεται «η δυνατότητα άμεσης πρόσβασης και χρήσης ενός πληροφοριακού συστήματος, όποτε αυτό απαιτείται». Σε ιατρικά πληροφοριακά συστήματα, η απαιτούμενη διαθεσιμότητα είναι σε πολλές περιπτώσεις 24 ώρες το εικοσιτετράωρο για 7 μέρες την εβδομάδα με συχνές αλλαγές του υπεύθυνου προσωπικού. Έστω και λίγα λεπτά διακοπής της λειτουργίας σε αυτές τις περιπτώσεις είναι δυνατόν να θέσουν ανθρώπινες ζωές σε κίνδυνο (π.χ. σε μονάδες εντατικής θεραπείας).

Υπευθυνότητα

Ως υπευθυνότητα ορίζεται «η διασφάλιση ότι οι πράξεις μιας οντότητας μπορούν να αποδοθούν μοναδικά στην οντότητα αυτή». Στον τομέα της Ιατρικής Φροντίδας, όπου κάθε δράση μπορεί να έχει αντίκτυπο σε κρίσιμα δεδομένα, είναι απαραίτητη η καταγραφή όλων των δράσεων, έτσι ώστε να μπορούν ανά πάσα στιγμή να ανιχνευθούν τα εμπλεκόμενα μέρη κατά την απόδοση ευθυνών.

Ο βαθμός σημαντικότητας των παραπάνω απαιτήσεων στον τομέα της Ιατρικής Φροντίδας μεταβάλλεται κάθε φορά, ανάλογα με το σκοπό και την χρήση του αντίστοιχου πληροφοριακού συστήματος. Έτσι για παράδειγμα, η διαθεσιμότητα είναι πρωταρχική απαίτηση ασφαλείας στη λειτουργία μονάδων εντατικής θεραπείας, σε αντίθεση με ένα σύστημα ψυχολογικής υποστήριξης ασθενών, όπου η εμπιστευτικότητα των ευαίσθητων προσωπικών δεδομένων είναι πιο σημαντική. Έτσι, σε κάθε περίπτωση θα πρέπει να εξετάζονται οι ειδικές απαιτήσεις ασφάλειας και να λαμβάνονται τα κατάλληλα μέτρα.

2.3. Μηχανισμοί για την υλοποίηση της ασφάλειας πληροφορίας

Για να εξασφαλιστούν οι αρχές που παρουσιάστηκαν στο προηγούμενο κεφάλαιο σχετικά με την ασφάλεια της πληροφορίας, χρησιμοποιούμε μέτρα που βασίζονται σε κρυπτογραφικούς μηχανισμούς και παρουσιάζονται αναλυτικά για κάθε μία από τις απαιτήσεις ασφαλείας που αναφέραμε [v]

- Εμπιστευτικότητα: Κρυπτογράφηση συμμετρικού ή και δημοσίου κλειδιού και χρησιμοποίηση ασφαλών καναλιών επικοινωνίας όπως το SSL [vi]. Οι κίνδυνοι σε αυτή την περίπτωση είναι η αποκάλυψη προσωπικών δεδομένων και η ρήξη του ιατρικού απορρήτου.

- Ακεραιότητα: Ψηφιακή υπογραφή, η οποία λειτουργεί ως σφραγίδα ακεραιότητας της πληροφορίας. Σε αυτή την περίπτωση οι κίνδυνοι είναι η αλλοίωση, σκόπιμη ή μη, του περιεχομένου της πληροφορίας .

- Αναγνώριση και Αυθεντικοποίηση (απόδειξη γνησιότητας): Χρήση κωδικών πρόσβασης (passwords) και αυθεντικοποίηση βάση ψηφιακής υπογραφής (με ή χωρίς τη χρήση έξυπνης κάρτας). Εδώ ο κίνδυνος σχετίζεται με την πιθανότητα μη εξουσιοδοτημένης χρήσης υπηρεσιών.

- Μη άρνηση αποστολής/λήψης πληροφορίας: Και σε αυτή την περίπτωση η ψηφιακή υπογραφή λειτουργεί ως σφραγίδα εγκυρότητας του αποστολέα. Πιθανές απειλές είναι η απόκρυψη της πηγής πληροφορίας ή η άρνηση της αποστολής/λήψης της πληροφορίας.

- Απόδειξη χρόνου αποστολής/λήψης: Εδώ χρησιμοποιείται ο μηχανισμός της χρονικής σφραγίδας, κατά τον οποίο επικολλείται στα δεδομένα η ημερομηνία και η ακριβής ώρα της δημιουργίας και αποστολής των δεδομένων. Η υλοποίηση του μηχανισμού αυτού στηρίζεται στις ψηφιακές υπογραφές και σε λειτουργίες κρυπτογράφησης. Εάν αυτά δεν εφαρμοστούν, είναι δυνατόν να έχουμε φαινόμενα άρνησης του χρόνου αποστολής/λήψης ή άρνηση της μοναδικότητας της πληροφορίας.

- Διαθεσιμότητα: Αρχιτεκτονικές Backup, Firewall, Intrusion Detection κ.α. είναι απαραίτητες σε συστήματα με συνεχή λειτουργία. Στην περίπτωση αυτή υπάρχουν κίνδυνοι μη εξουσιοδοτημένης πρόσβασης, αλλά και να εμποδίζεται η συνεχής λειτουργία του συστήματος π.χ. με επιθέσεις Denial of Service.

- Υπευθυνότητα: Συστήματα παρακολούθησης και καταγραφής κίνησης, μηχανισμοί logging. Εάν δεν λειτουργούν σωστά αυτά τα συστήματα υπάρχει κίνδυνος άρνησης ευθυνών.

Στην εργασία αυτή θα ασχοληθούμε με (την έκδοση ενός προσωπικά υπογεγραμμένου SSL ψηφιακού πιστοποιητικού) τις ψηφιακές υπογραφές που μπορούν να εξασφαλίσουν (την ακεραιότητα, την εμπιστευτικότητα, την αναγνώριση και αυθεντικοποίηση, την μη άρνηση αποστολής/λήψης καθώς και την απόδειξη του χρόνου αποστολή λήψης.) την ακεραιότητα,

την αναγνώριση και αυθεντικοποίηση, την μη άρνηση αποστολής/λήψης καθώς και την απόδειξη του χρόνου αποστολή λήψης. Στον παρακάτω πίνακα [vii] (Πίνακας 1) συνοψίζονται οι κυριότεροι κίνδυνοι, ανάγκες αλλά και πιθανές λύσεις για πληροφοριακά συστήματα στον τομέα της υγείας.

Κίνδυνοι	**Υπηρεσίες ασφάλειας**	**Λύσεις**	**Παρατηρήσεις**
Μη εξουσιοδοτημένη χρήση υπηρεσιών περιορισμένης χρήσης	Ταυτοποίηση και αυθεντικοποίηση	Κωδικός πρόσβασης	Αυθεντικοποίηση με κάτι που ο χρήστης γνωρίζει
		Έξυπνη κάρτα με κρυπτοεπεξεργαστή και χρήση PIN	Αυθεντικοποίηση με κάτι που χρήστης κατέχει και κάτι που γνωρίζει, σε χρήση μηχανισμού δημοσίου κλειδιού
Αθέμιτη εκμετάλλευση της πληροφορίας	Έλεγχος ακεραιότητας της πληροφορίας καθώς και της αυθεντικότητάς της (ότι όντως προέρχεται από συγκεκριμένη πηγή)	Αλγόριθμος hash και ψηφιακή υπογραφή του αποστολέα	Μηχανισμός υποδομής δημοσίου κλειδιού (π.χ. με χρήση έξυπνης κάρτας)
Απόκρυψη της πηγής της πληροφορίας	Μη αποποίηση ευθύνης ως προς την πηγή της πληροφορίας	Ψηφιακή υπογραφή του αποστολέα	Μηχανισμός υποδομής δημοσίου κλειδιού (π.χ. με χρήση έξυπνης κάρτας)
Αποποίηση ευθύνης ως προς την πληροφορία που παραλήφθηκε	Απόδειξη παραλαβής της πληροφορίας	Ψηφιακή υπογραφή του παραλήπτη	Μηχανισμός υποδομής δημοσίου κλειδιού (π.χ. με χρήση έξυπνης κάρτας)
Ρήγμα εμπιστευτικότητας	Κρυπτογράφηση	Συμμετρικοί αλγόριθμοι και	Κρυπτογράφηση από τελικό χρήστη σε τελικό

		αλγόριθμοι δημοσίου κλειδιού	χρήστη (εξαρτώμενη από το χρήστη μέσω της έξυπνης κάρτας του) και κρυπτογράφηση από σημείο σε σημείο(μη εξαρτώμενη από χρήστες αλλά από στοιχεία του δικτύου)
Μη εξουσιοδοτημένη χρήση, αθέμιτη εκμετάλλευση της πληροφορίας, ρήγμα εμπιστευτικότητας για μη εξουσιοδοτημένες υπηρεσίες	Κρυπτογράφηση και αυθεντικοποίηση	Ολοκληρωμένο εργαλείο ή υποδομή κρυπτογράφησης και διαχείρισης ζευγών κλειδιών.	Ασφάλεια στο ηλεκτρονικό ταχυδρομείο (e-mail), και πιστοποίηση από τρίτο φορέα που μπορεί να οριστεί σαν υπέρ-χρήστης
		Privacy Enhanced Mail (PEM)	Ασφάλεια στο ηλεκτρονικό ταχυδρομείο (e-mail)
	Κρυπτογράφηση και αυθεντικοποίηση τόσο του εξυπηρετητή όσο και του πελάτη	Secure Socket Layer (SSL)	Ασφάλεια στην επικοινωνία ανά κανάλι επικοινωνίας (π.χ. WWW, FTP, Telnet)
Μη εξουσιοδοτημένη χρήση, αθέμιτη εκμετάλλευση της πληροφορίας, ρήγμα εμπιστευτικότητας, και αποποίηση ευθύνης για μη εξουσιοδοτημένες υπηρεσίες.	Κρυπτογράφηση, αυθεντικοποίηση και μη αποποίηση ευθύνης	Secure Hypertext Transfer Protocol (S-HTTP)	Ασφάλεια σε σχέση με κείμενα και πληροφορία σε υπηρεσίες WWW
Εξωτερική μη	Firewall	Ποικιλία προϊόντων με	Απαγορεύεται η απευθείας

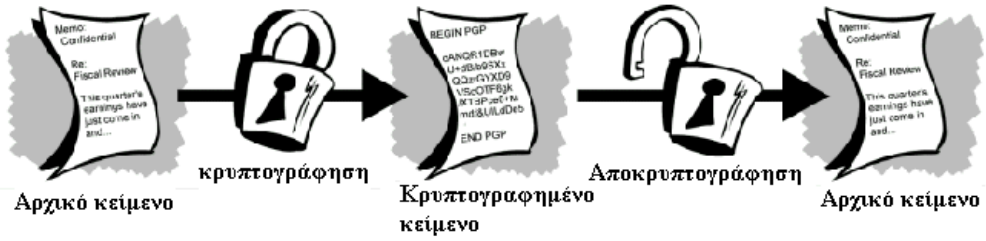
εξουσιοδοτημένη πρόσβαση σε εσωτερικά στοιχεία του συστήματος		διαφορετικές λειτουργικότητες.	επικοινωνία μεταξύ των εσωτερικών κι εξωτερικών στοιχείων του συστήματος (φιλτράρισμα), διαχειρίζεται διευθύνσεις και δικαιώματα πρόσβασης

Πίνακας 1: Παρουσίαση των κινδύνων, αναγκών και πιθανών λύσεων σε πληροφοριακά συστήματα υγείας.

3. Κρυπτογραφία

3.1. Γενικές αρχές – Ιστορική αναδρομή

Η διαδικασία μετατροπής της μορφής των δεδομένων, έτσι ώστε το περιεχόμενό τους να αποκρύπτεται, λέγεται κρυπτογράφηση. Ο αντίστοιχος αγγλικός όρος που χρησιμοποιείται περισσότερο είναι encryption, ενώ για την αντίστροφη διαδικασία, της αποκάλυψης του περιεχομένου του μηνύματος, χρησιμοποιείται η λέξη decryption - αποκρυπτογράφηση (Αν και σύμφωνα με το ISO 7498-2 πρέπει να χρησιμοποιούνται οι όροι "encipher" και "decipher", αφού σε ορισμένους πολιτισμούς οι όροι "encrypt" και "decrypt" θεωρούνται προσβλητικοί καθώς αναφέρονται σε νεκρούς)[viii].



Σχήμα 4: Κρυπτογράφηση και αποκρυπτογράφηση μηνύματος.

Η τέχνη και επιστήμη που εξασφαλίζει την ασφάλεια των μηνυμάτων λέγεται κρυπτογραφία, ενώ αντίστροφα, η τέχνη και επιστήμη που προσπαθεί να διαβάσει κρυπτογραφημένα μηνύματα αναλύοντάς τα, "σπάζοντας" δηλαδή την κρυπτογράφηση, λέγεται κρυπτανάλυση [ix].

Μια από τις παλαιότερες αναφορές στην κρυπτογραφία ανάγεται εποχή της αρχαίας Σπάρτης, όπου οι έφοροι επικοινωνούσαν με τους στρατηγούς χρησιμοποιώντας μακριές και στενές κορδέλες τις οποίες τύλιγαν γύρω από μία σκυτάλη (κύλινδρο) και μετά έγραφαν το μήνυμα κατά μήκος της σκυτάλης. Για να διαβάσει κάποιος το μήνυμα έπρεπε να έχει μια παρόμοια σκυτάλη με αυτήν που είχε χρησιμοποιηθεί για την κωδικοποίηση και να τυλίξει την κορδέλα γύρω από την σκυτάλη με παρόμοιο τρόπο. Αυτό το σύστημα κρυπτογραφίας (διπλής κατεύθυνσης) είναι ένα κλασικό σύστημα με ένα κλειδί (τη σκυτάλη) [x].

Ο Ιούλιος Καίσαρας χρησιμοποιούσε ένα εξαιρετικά απλό και ανασφαλές σύστημα απλής αντικατάστασης, όπου κάθε χαρακτήρας του αρχικού κειμένου αντικαθίσταται από ένα αντίστοιχο γράμμα (συγκεκριμένα το 3ο γράμμα δεξιά, για παράδειγμα το "A" από το "D", το "X" από το "A" κ.ο.κ). Σε πολλά συστήματα Unix βρίσκει κανείς ένα παρόμοιο σύστημα κωδικοποίησης που λέγεται ROT13 όπου το κάθε γράμμα μετατοπίζεται κατά 13

χαρακτήρες (το μισό των 26 του λατινικού αλφαβήτου, με αποτέλεσμα, αν εφαρμόσουμε την ίδια ολίσθηση στο κωδικοποιημένο κείμενο, να πάρουμε την αρχική μορφή). Φυσικά τέτοια απλά σχήματα κωδικοποίησης δεν παρέχουν καμία ασφάλεια αφού δεν κρύβουν καθόλου τις συχνότητες εμφάνισης των διαφόρων γραμμάτων, με αποτέλεσμα να είναι σχετικά εύκολο για έναν κρυπταναλυτή να "σπάσει" έναν τέτοιο κώδικα [xi]. Παραλλαγές αυτού του συστήματος είναι η "ομοφωνική" αντικατάσταση (όπου κάθε γράμμα αντικαθίσταται από πολλούς κωδικούς, π.χ. το "Α" μπορεί να είναι 3,8,14, ή 19), η "πολυγραμμική" αντικατάσταση, όπου αντικαθίστανται ακολουθίες χαρακτήρων (π.χ. "ABA" αντικαθίσταται από "QWE" κ.ο.κ), και η "πολυαλφαβητική" αντικατάσταση που αποτελείται από διαδοχικές απλές αντικαταστάσεις με διαφορετικό όμως αντικαταστάτη κάθε φορά. Στην τελευταία κατηγορία ανήκει η γερμανική μηχανή Αίνιγμα που χρησιμοποιήθηκε στο 2ο Παγκόσμιο Πόλεμο.

Το 1917 αναπτύχθηκε ο πρώτος πραγματικά άθραυστος κώδικας, ο κώδικας Vernam, πιο γνωστός με το όνομα "μπλοκάκι μιας χρήσης" (one-time pad). Σε αυτή την περίπτωση το κλειδί πρέπει να έχει το ίδιο μήκος με το μήνυμα και να μην χρησιμοποιείται πάνω από μια φορά. Όταν το 1967 ο Βολιβιανός στρατός συνέλαβε και εκτέλεσε τον επαναστάτη Che Guevara, βρήκαν στην κατοχή του ένα χαρτί που έδειχνε ότι προετοίμαζε ένα μήνυμα, για την κωδικοποίηση του οποίου χρησιμοποιούσε τον άσπαστο κώδικα Verman [xii].

Ένα σύστημα που χρησιμοποιήθηκε ευρύτατα για πολλά χρόνια πρωτοεμφανίστηκε το 1974, όταν η IBM πρότεινε ένα κρυπτογραφικό σύστημα που στηριζόταν στον αλγόριθμο Lucifer [ix] και που αργότερα (1977) τέθηκε σε ισχύ με το όνομα DES (Data Encryption Standard). Το 1993 προτάθηκε μια βελτίωση αυτού του αλγορίθμου (Triple-DES), ενώ το 1997 ξεκίνησε η προσπάθεια ανάπτυξης του AES (Advanced Encryption Standard) που θα αντικαθιστούσε το DES. Το AES τέθηκε σε ισχύ από το αμερικάνικο Υπουργείο Εμπορίου το Μάιο του 2002.

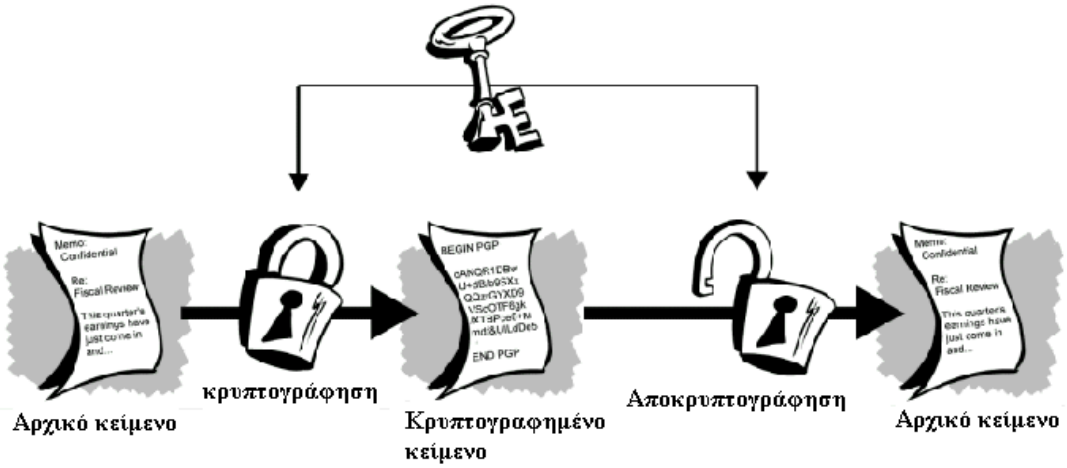
Παράλληλα, το 1976 οι W.Diffie, M.Hellman και ανεξάρτητα ο R.Merkle, πρότειναν την ιδέα της κρυπτογραφίας δημόσιου κλειδιού. Πιο δημοφιλείς αλγόριθμοι είναι οι RSA[ix] (από τα ονόματα των Rivest, Shamir και Adleman), ο ElGamal[ix] και ο DSA[ix],[xiii]. Η ιδέα αυτή ήταν πραγματικά πρωτοποριακή και πάνω σε αυτήν βασίζεται και η ιδέα της ψηφιακής υπογραφής.

3.2. Ασύμμετρη και συμμετρική κρυπτογράφηση

Στην παραδοσιακή κρυπτογραφία αναφερόμαστε σε ένα κλειδί: Με αυτό μπορούμε να κρυπτογραφήσουμε ένα μήνυμα, αλλά και να το αποκρυπτογραφήσουμε. Φυσικά το κλειδί

αυτό θα πρέπει να είναι μυστικό και να το μοιράζονται μονάχα οι δύο πλευρές που θέλουν να επικοινωνήσουν. Οι αλγόριθμοι σε αυτή την περίπτωση λέγονται συμμετρικοί, ακριβώς επειδή χρησιμοποιούμε το ίδιο κλειδί για κρυπτογράφηση και αποκρυπτογράφηση. Παραδείγματα τέτοιων αλγορίθμων είναι οι DES (που δεν θεωρείται πια ως η πιο ασφαλής λύση[xiv]), TripleDES, AES[xv], IDEA[ix], BlowFish[ix], SKIPJACK[xvi] κ.α.

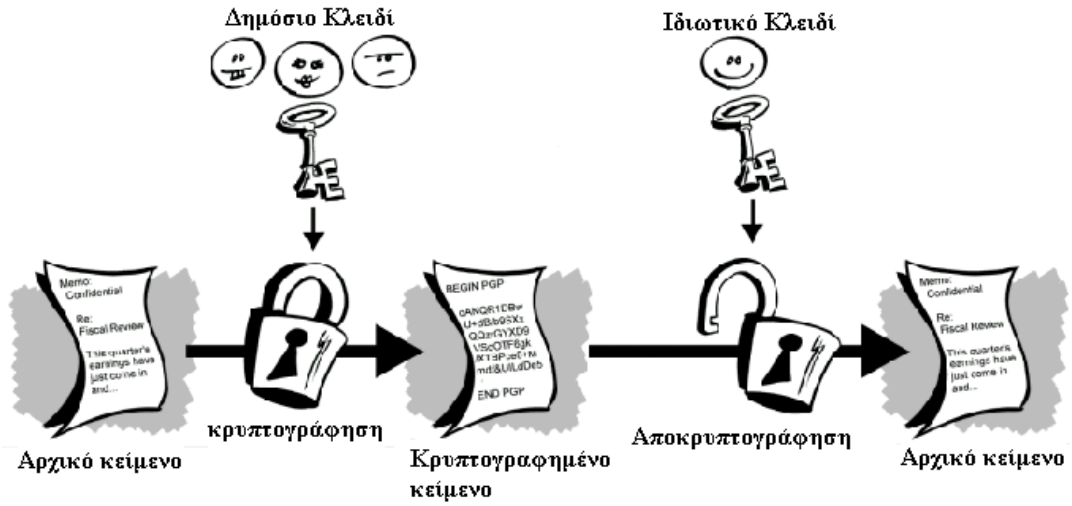
Ο AES (Advanced Encryption Algorithm) είναι ένα πρότυπο που υιοθετήθηκε από τις Η.Π.Α. τον Οκτώβρη του 2000, προκειμένου να αντικαταστήσει τον DES. Ως βάση του προτύπου χρησιμοποιήθηκε ο κρυπτογραφικός αλγόριθμος Rijndael [xvii][xviii], που αναπτύχθηκε από τους Βέλγους Joan Daemen και Vincent Rijmen. Αξίζει να αναφέρουμε ότι ο αλγόριθμος αυτός επιλέχθηκε από το NIST (National Institute of Standards and Technology) του Υπουργείο Εμπορίου των Η.Π.Α., ανάμεσα από άλλους 5 υποψήφιους αλγόριθμους, ένας εκ των οποίων (γνωστός ως MARS) αναπτύχθηκε από μια πολυμελή ομάδα εργασίας της IBM.



Σχήμα 5: Συμμετρική κρυπτογράφηση – αποκρυπτογράφηση.

Αντίθετα, η κρυπτογράφηση Δημόσιου κλειδιού ή αλλιώς ασύμμετρη κρυπτογράφηση βασίζεται στην ύπαρξη ενός ζεύγους κλειδιών: Ενός Δημόσιου κλειδιού, στο οποίο μπορεί να έχει πρόσβαση ο καθένας, και του αντίστοιχου ιδιωτικού κλειδιού που το έχει μόνο ένας. Το Δημόσιο κλειδί κρυπτογραφεί τα δεδομένα, ενώ η αποκρυπτογράφηση μπορεί να γίνει μόνο με το αντίστοιχο Ιδιωτικό κλειδί. Αν λοιπόν υποθέσουμε ότι ο Α θέλει να στείλει ένα κρυπτογραφημένο μήνυμα στον Β, τότε αρκεί να πάρει το Δημόσιο κλειδί του Β (που είναι διαθέσιμο) και να κρυπτογραφήσει το μήνυμα. Στη συνέχεια ο Β αρκεί να χρησιμοποιήσει το ιδιωτικό του κλειδί (στο οποίο μόνο αυτός έχει πρόσβαση) και να αποκωδικοποιήσει το μήνυμα.

Οποιοσδήποτε έχει ένα δημόσιο κλειδί μπορεί να κρυπτογραφήσει ένα μήνυμα. Ωστόσο μετά, δεν θα είναι σε θέση να το αποκρυπτογραφήσει. Αυτό μπορεί να γίνει μονάχα από αυτόν που διαθέτει το αντίστοιχο ιδιωτικό κλειδί.



Σχήμα 6: Ασύμμετρη κρυπτογράφηση ή κρυπτογράφηση Δημοσίου κλειδιού

Η κρυπτογραφία δημόσιου κλειδιού βασίζεται στην έννοια των συναρτήσεων μονής κατεύθυνσης. Μια συνάρτηση $f(x)$ ονομάζεται μονής κατεύθυνσης αν είναι εύκολο να υπολογίσουμε το $f(x)$ από το x, ενώ ο αντίστροφος υπολογισμός, δηλαδή του x από το $f(x)$, είναι δύσκολος. Για παράδειγμα, το να υψώσουμε έναν αριθμό στο τετράγωνο είναι σχετικά εύκολο, όμως το αντίστροφο, δηλαδή ο υπολογισμός της ρίζας ενός αριθμού, είναι πιο δύσκολη διαδικασία.

Το πόσο εύκολο ή δύσκολο είναι ένα πρόβλημα φαίνεται από τον *υπολογιστικό χρόνο* που χαρακτηρίζει τον αλγόριθμο επίλυσής του και μπορεί να είναι γραμμικός, πολυωνυμικός, εκθετικός κ.ο.κ. Στην συγκεκριμένη περίπτωση θέλουμε ο υπολογισμός του x από το $f(x)$ να είναι *απρόσιτος*. Αυτό σημαίνει ότι το πρόβλημα πρέπει να είναι τουλάχιστον τόσο δύσκολο, όσο και τα δυσκολότερα προβλήματα NP τάξης (μη πολυωνυμικού χρόνου). Είναι σημαντικό να τονίσουμε ότι η έννοια του υπολογιστικά απρόσιτου είναι στενά συνδεδεμένη με την υπάρχουσα υπολογιστική ισχύ. Έτσι, μια συνάρτηση μιας κατεύθυνσης που σήμερα θεωρείται ασφαλής μπορεί σε μια δεκαετία να θεωρείται ανασφαλής.

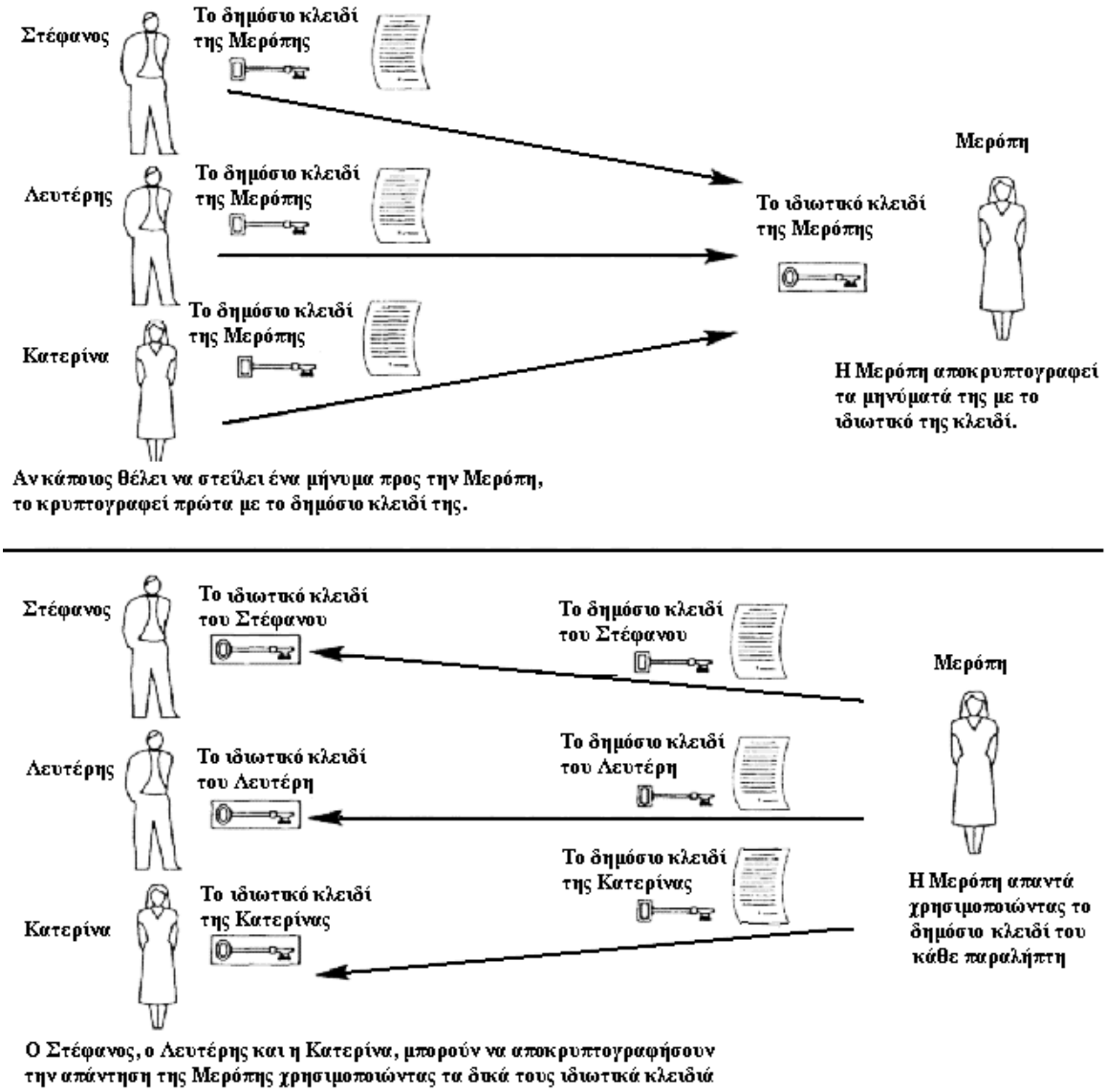
Σε ένα είδος συναρτήσεων μιας κατεύθυνσης παρουσιάζεται μια χρήσιμη ιδιότητα: Είναι μεν δύσκολο να υπολογιστεί το $f(x)$ από το x, όμως εάν γνωρίζουμε μια συγκεκριμένη πληροφορία, η διαδικασία αυτή γίνεται εύκολη. Για παράδειγμα είναι εύκολο να αποσυναρμολογήσει κανείς ένα μηχανικό ρολόι, ενώ η αντίστροφη διαδικασία της

συναρμολόγησης είναι πολύ δύσκολη. Ωστόσο, εάν έχουμε μια συγκεκριμένη πληροφορία (τις αναλυτικές οδηγίες συναρμολόγησης), τότε αυτό μπορεί να γίνει πολύ πιο εύκολα. Στην κρυπτογραφία Δημόσιου κλειδιού μπορούμε να πούμε ότι η μετάβαση από το x στην $f(x)$ γίνεται εύκολα με το δημόσιο κλειδί, ενώ η αντίστροφη διαδικασία είναι πολύ δύσκολη χωρίς την κατοχή μιας πληροφορίας: του ιδιωτικού κλειδιού.

Οι πιο γνωστοί αλγόριθμοι ασύμμετρης κρυπτογραφίας βασίζονται σε γνωστά προβλήματα της Θεωρίας Αριθμών: Οι RSA, Rabin βασίζονται στην δυσκολία παραγοντοποίησης του γινομένου δύο μεγάλων πρώτων αριθμών, ενώ ο ElGamal στο πρόβλημα Διακριτού Λογαρίθμου (DLP).

Για λόγους πληρότητας πρέπει να σημειώσουμε ότι οι αλγόριθμοι ασύμμετρης κρυπτογραφίας είναι πρακτικά πολύ πιο αργοί σε σχέση με την κρυπτογραφία με ένα κλειδί. Έτσι συστήματα που χρησιμοποιούν αμιγώς κρυπτογραφία δημοσίου κλειδιού, είναι κυρίως αυτά στα οποία η πληροφορία είναι πεπερασμένου μεγέθους και δεν υπάρχει ανάγκη επικοινωνίας σε πραγματικό χρόνο. Για παράδειγμα το ηλεκτρονικό ταχυδρομείο με το σύστημα PGP[xix]. Στο Σχήμα 7 βλέπουμε αναλυτικά ένα παράδειγμα επικοινωνίας όπου χρησιμοποιείται κρυπτογραφία δημοσίου κλειδιού:

Σε ένα σύστημα επικοινωνίας που χρειάζεται ταχύτητα, χρησιμοποιείται μια υβριδική μέθοδος, όπου, τεχνικές δημοσίου κλειδιού χρησιμοποιούνται για την ανταλλαγή ενός συμμετρικού κλειδιού (session key), με το οποίο θα κρυπτογραφούνται τα δεδομένα της επικοινωνίας, χωρίς να υπάρχει χρονική επιβάρυνση. Η μέθοδος αυτή λέγεται ψηφιακός φάκελος (digital envelope)[xx]. Στην εργασία μας χρησιμοποιήθηκε αυτό το στυλ κρυπτογράφησης μέσω του πρωτοκόλλου SSL όπως θα φανεί και παρακάτω.



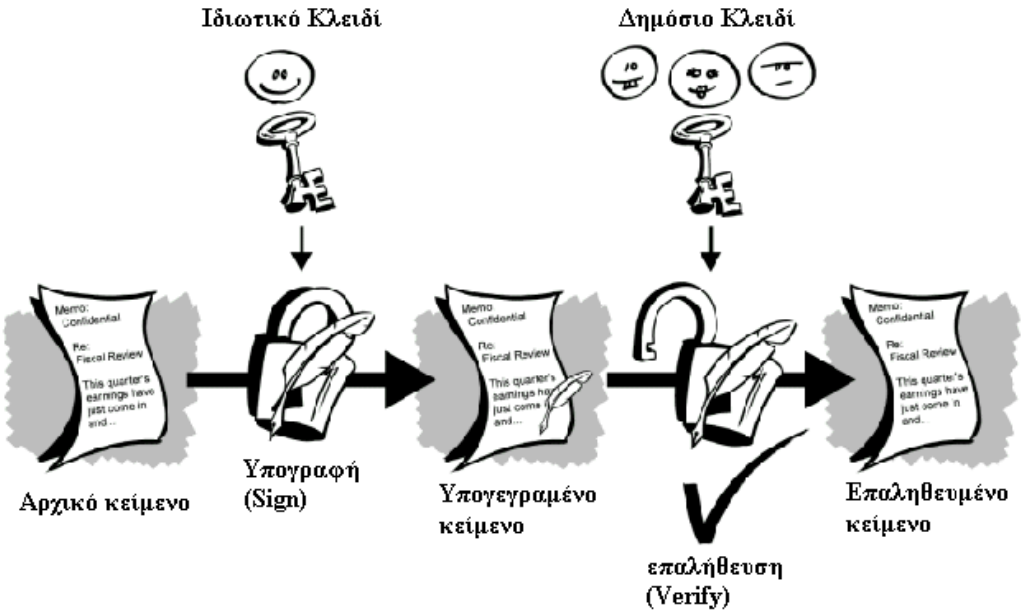
Σχήμα 7: Επικοινωνία με κρυπτογραφία δημοσίου κλειδιού

3.3. Γενικές αρχές Ψηφιακών Υπογραφών

Όπως αναφέρθηκε και προηγουμένως, η κρυπτογράφηση ενός μηνύματος με το δημόσιο κλειδί, παράγει το κρυπτογραφημένο κείμενο, που μπορεί να διαβαστεί μονάχα με την βοήθεια του ιδιωτικού κλειδιού. Ωστόσο μια ιδιότητα που έχουν ορισμένοι αλγόριθμοι (π.χ. ο RSA) επιτρέπουν την ακριβώς αντίστροφη διαδικασία: την κωδικοποίηση μηνυμάτων με το ιδιωτικό κλειδί έτσι ώστε η αποκωδικοποίηση να μπορεί να γίνει μόνο με το αντίστοιχο δημόσιο.

Ας υποθέσουμε ότι ο Α θέλει να υπογράψει ψηφιακά ένα μήνυμα Μ: Το κρυπτογραφεί με το ιδιωτικό του κλειδί, οπότε προκύπτει το κρυπτογραφημένο μήνυμα Κ(Μ). Εάν θέλει να στείλει αυτό το μήνυμα στον Β, τότε πρέπει να στείλει μαζί με το μήνυμα Μ και το

αποτέλεσμα της κρυπτογράφησης K(M). Έτσι, ο Β αν αποκρυπτογραφήσει το K(M) με το δημόσιο κλειδί του Α, θα πάρει το αρχικό μήνυμα Μ, το οποίο μπορεί να συγκρίνει με το μη κρυπτογραφημένο μήνυμα που έλαβε. Εάν είναι όμοια, σημαίνει ακριβώς ότι το μήνυμα ήταν κρυπτογραφημένο με το ιδιωτικό κλειδί του Α, οπότε προήλθε από τον Α. Το γεγονός αυτό εξασφαλίζει την *πιστοποίηση* του αποστολέα, αλλά και την *ακεραιότητα* των δεδομένων, ότι δηλαδή δεν μεταβλήθηκαν κατά την αποστολή τους (σκόπιμα ή μη).



Σχήμα 8: Ψηφιακή Υπογραφή και Επαλήθευση

3.4. Αλγόριθμοι hash ή Message Digest

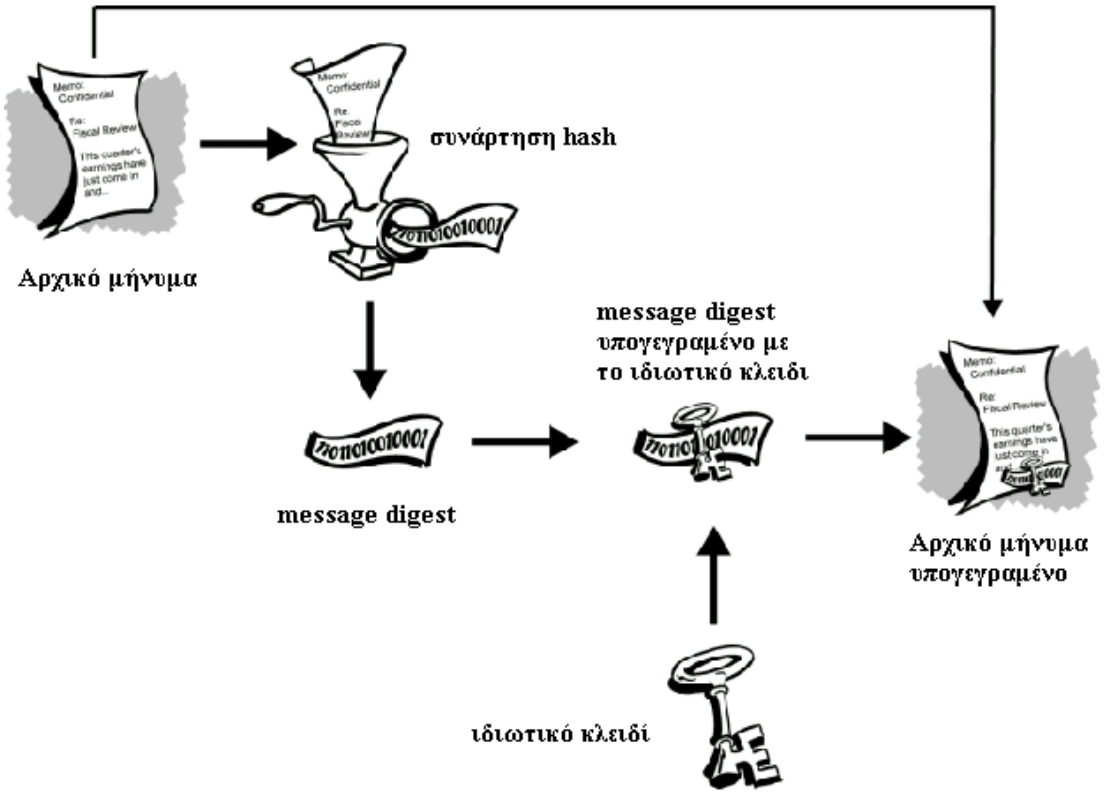
Με βάση την περιγραφή της προηγούμενης παραγράφου, η ψηφιακή υπογραφή απαιτεί την κρυπτογράφηση ολόκληρου του μηνύματος και την αποστολή του αποτελέσματος, καθώς και του αρχικού μηνύματος. Κάτι τέτοιο ωστόσο σημαίνει ότι θα πρέπει να αποστέλλουμε κάθε φορά την διπλάσια τουλάχιστον ποσότητα πληροφορίας, σε σχέση με το αρχικό μήνυμα. Αυτό, εκτός του ότι θα ήταν εξαιρετικά χρονοβόρο, προσθέτει σημαντικό φόρτο στο δίκτυο. Έτσι λοιπόν χρησιμοποιούμε κάποιες μονόδρομες μαθηματικές συναρτήσεις που δημιουργούν με μοναδικό τρόπο μια "περίληψη" του αρχικού μηνύματος, το λεγόμενο hash ή message digest, οπότε αρκεί να υπογράψουμε αυτό μονάχα.

Μια *κρυπτογραφική συνάρτηση κατακερματισμού* (ή συνάρτηση κατακερματισμού μονής διεύθυνσης [x]) παίρνει ως είσοδο μια ποσότητα δεδομένων, για παράδειγμα ένα μήνυμα τυχαίου μήκους και δίνει αποτέλεσμα προκαθορισμένου μεγέθους, για παράδειγμα 160 bits. Εάν η πληροφορία που δώσαμε στην είσοδο αλλάξει, ακόμα και ένα bit, το

αποτέλεσμα θα είναι εντελώς διαφορετικό. Μπορούμε να πούμε ότι πρόκειται για ένα είδος "δακτυλικού αποτυπώματος" της πληροφορίας. Το message digest "αντιπροσωπεύει" το αρχικό μήνυμα όπως περίπου συμβαίνει και με τους κώδικες που υπάρχουν για τον εντοπισμό λαθών ("checksum",CRC) με τη διαφορά ότι, για τους κώδικες αυτούς, είναι εύκολο να βρει κανείς ένα άλλο αρχικό μήνυμα που να παράγει το ίδιο ακριβώς checksum.

Όταν λοιπόν θέλουμε να υπογράψουμε ένα μήνυμα, πρώτα δημιουργούμε το hash του μηνύματος και ύστερα το κρυπτογραφούμε με το ιδιωτικό μας κλειδί όπως αναλυτικά περιγράψαμε. Ύστερα επισυνάπτουμε στο μήνυμα το υπογεγραμμένο αυτό hash και το αποστέλλουμε, μαζί με πληροφορίες ως προς το ποιόν ακριβώς αλγόριθμο χρησιμοποιήσαμε. Ο αποδέκτης θα δημιουργήσει και αυτός ένα hash του μηνύματος με τον αλγόριθμο που χρησιμοποιήσαμε και εμείς, μετά θα αποκρυπτογραφήσει με το δημόσιο μας κλειδί το κρυπτογραφημένο hash που στείλαμε και θα το συγκρίνει με αυτό που βρήκε ο ίδιος. Οποιαδήποτε διαφορά θα σημαίνει ότι υπήρξε παραποίηση του μηνύματος. Η διαδικασία αυτή φαίνεται στο **Error! Reference source not found.**.

Γνωστοί αλγόριθμοι hash είναι οι MD5 [xxi] και ο SHA-1 [xxii]. Ο MD5 δημιουργεί hash μήκους 128 bits και θεωρείται πλέον ανασφαλής αλγόριθμος[xxiii]. Δημιουργήθηκε από τον καθηγητή του MIT R. Rivest ως μέρος μιας σειράς παρόμοιων αλγορίθμων (MD4, MD2 κλπ). Ο SHA δημιουργήθηκε από το NIST (National Institute of Standards and Technology) σε συνεργασία με την NSA (National Security Agency) για να εξασφαλίσει την ασφάλεια των ψηφιακών υπογραφών DSA. Δημιουργεί hash μήκους 160 bits ή και μεγαλύτερο στις εκδόσεις SHA-256, SHA-384 και SHA-512.



Σχήμα 9: Ψηφιακή υπογραφή με message digest

3.5. Ψηφιακά πιστοποιητικά (digital certificates)

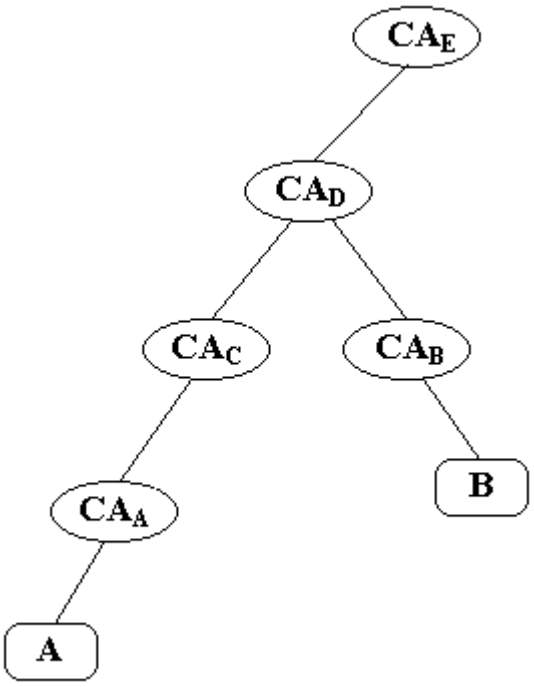
Έως τώρα έχουμε υποθέσει ότι, όταν ο Α θέλει να στείλει ένα μήνυμα ψηφιακά υπογεγραμμένο στην Β τότε, αρκεί να χρησιμοποιήσει το δημόσιο κλειδί της Β. Αν όμως ο Γ θέλει να υποκλέψει αυτή την ανταλλαγή μηνυμάτων μεταξύ Α και Β, θα μπορούσε να διαθέσει το δικό του δημόσιο κλειδί, υποκρινόμενος ότι είναι ο Β. Έτσι θα ο Α θα υπέγραφε ψηφιακά το μήνυμα του με το δημόσιο κλειδί του Γ (νομίζοντας ότι είναι το δημόσιο κλειδί της Β). Άρα ο Γ δεν θα είχε παρά να χρησιμοποιήσει το δικό του ιδιωτικό κλειδί, να διαβάσει το μήνυμα και μετά να το υπογράψει με το δημόσιο κλειδί της Β (που φυσικά είναι διαθέσιμο), να της το στείλει υποκρινόμενος ότι είναι ο Α κ.ο.κ. Πρέπει λοιπόν να εξασφαλίσουμε έναν τρόπο να αναγνωρίζεται με σαφήνεια ο ιδιοκτήτης ενός δημοσίου κλειδιού.

Ένα πιστοποιητικό δημοσίου κλειδιού είναι μια ψηφιακά υπογεγραμμένη δήλωση από μια οντότητα, που λέει ότι το δημόσιο κλειδί (ή κάποια άλλη πληροφορία) κάποιας άλλης οντότητας, έχει μια συγκεκριμένη τιμή. Με τον όρο "οντότητα" εννοούμε κάποιο φυσικό πρόσωπο, οργανισμό, πρόγραμμα, εταιρία, υπολογιστή ή οποιονδήποτε άλλο που μπορούμε

να εμπιστευτούμε ως ένα βαθμό. Με λίγα λόγια εισάγουμε μια τρίτη οντότητα που λειτουργεί ως εγγυητής.

Τα πιστοποιητικά αυτά εκδίδονται από κάποια Αρχή που λέγεται CA (Certification Authority). Πρόκειται συνήθως για εταιρίες που θεωρείται ότι μπορεί κανείς να τις εμπιστευτεί ώστε να υπογράφουν (δηλαδή να εκδίδουν) πιστοποιητικά για κάποια άλλη οντότητα. Υπάρχουν αρκετές CAs που είναι διαθέσιμες: VeriSign [xxiv], Thawte[xxv], Entrust[xxvi], κ.α. Υπάρχει επίσης η δυνατότητα να δημιουργήσει κανείς την δική του Αρχή έκδοσης πιστοποιητικών χρησιμοποιώντας προϊόντα όπως "Certificate Servers" της Netscape ή της Microsoft και το "Entrust CA".

Είναι σαφές ότι εφόσον οι δύο πλευρές που θέλουν να επικοινωνήσουν έχουν πιστοποιητικά στην ίδια Certificate Authority η διαδικασία είναι απλή: Αρκεί ο ένας να επαληθεύσει την υπογραφή της CA που βρίσκεται πάνω στο πιστοποιητικό του άλλου. Αν όμως χρησιμοποιούν διαφορετική CA τότε τα πράγματα είναι πιο περίπλοκα [ix]. Οι διάφορες CAs σχετίζονται μεταξύ τους με ένα είδος δομής δέντρου, όπως ακριβώς φαίνεται στο Σχήμα 6. Κάθε CA έχει ένα πιστοποιητικό υπογεγραμμένο από την CA που βρίσκεται από κάτω της. Έτσι λοιπόν αν ο Α έχει πιστοποιητικό που εκδίδεται από την CA_A ενώ της Β από την CA_B, τότε για να επικοινωνήσουν θα γίνουν τα εξής: Ο Α ξέρει το δημόσιο κλειδί της CA_A και η CA_C έχει ένα πιστοποιητικό υπογεγραμμένο από την CA_A, οπότε ο Α μπορεί να το επαληθεύσει. Όμοια η CA_D έχει ένα πιστοποιητικό υπογεγραμμένο από την CA_C. Και το πιστοποιητικό της Β είναι υπογεγραμμένο από την CA_B. Ο Α πρέπει δηλαδή να κινηθεί κατά μήκος του δέντρου προς τα πάνω μέχρι το κοινό σημείο CA_D, και ύστερα προς τα κάτω μέχρι την Β.



Σχήμα 10: Ιεραρχία των Certificate Authorities

3.6. Είδη πιστοποιητικών

Πέντε είδη πιστοποιητικών χρησιμοποιούνται συνήθως:

1. SSL Πιστοποιητικά Πελάτη (Client SSL certificates).

Χρησιμοποιούνται για να αναγνωρίζονται οι πελάτες(clients) από τους εξυπηρετητές (Servers) δια μέσου SSL (πιστοποίηση πελάτη – client authentication). Τυπικά η ταυτότητα του πελάτη υποτίθεται πως είναι ίδια με αυτή του χρήστη, όπως για παράδειγμα ενός υπαλλήλου σε μια εταιρία.

Αυτή η μέθοδος χρησιμοποιείται όταν για παράδειγμα μια τράπεζα δίνει σε κάποιο πελάτη της ένα SSL πιστοποιητικό πελάτη (client) που επιτρέπει στον εξυπηρετητή της τράπεζας να αναγνωρίζει τον πελάτη και να του δίνει πρόσβαση στους λογαριασμούς του. Το ίδιο μπορεί να συμβεί για να αναγνωρίζεται και κάποιος υπάλληλος της εταιρίας ώστε να εξουσιοδοτείται να έχει πρόσβαση στον εξυπηρετητη της εταιρίας.

2. SSL Πιστοποιητικά Εξυπηρετητή (Server SSL certificates).

Χρησιμοποιούνται για να αναγνωρίζονται οι εξυπηρετητές (servers) από τους πελάτες (clients) μέσω SSL. Η μέθοδος αυτή ονομάζεται πιστοποίηση εξυπηρετητή (Server Authentication).

Χαρακτηριστικό παράδειγμα της μεθόδου είναι η χρησιμοποίησή της από sites τα οποία συνδυάζουν ηλεκτρονική διαφήμιση (e-commerce) όπου χρησιμοποιείται αυθεντικοποίηση εξυπηρετητή βασισμένη σε πιστοποιητικό για να εγκατασταθεί μια κρυπτογραφημένη SSL σύνδεση (όπως περιγράφηκε αναλυτικά πριν) για να διαβεβαιώσει τους καταναλωτές ότι έχουν να κάνουν με μια ιστοσελίδα αξιόπιστη η οποία ανήκει σε μια συγκεκριμένη εταιρία. Η κρυπτογραφημένη σύνδεση διασφαλίζει ότι προσωπικές πληροφορίες, όπως αριθμοί πιστωτικών καρτών, δεν μπορεί να υποκλαπούν.

3. Πιστοποιητικά S/MIME.

Χρησιμοποιούνται για υπογεγραμμένα και κρυπτογραφημένα ηλεκτρονικά μηνύματα. Όπως με τα πιστοποιητικά πελάτη, η ταυτότητα του πελάτη τυπικά θεωρείται ίδια με την ταυτότητα του χρήστη, όπως ένας υπάλληλος σε μια εταιρία. Ένα πιστοποιητικό μπορεί να χρησιμοποιηθεί σαν ένα S/MIME πιστοποιητικό και ταυτόχρονα σαν ένα SSL πιστοποιητικό.

Μια εταιρία χρησιμοποιεί συνδυασμένα τέτοιου είδους πιστοποιητικά μόνο για να πιστοποιήσει τις ταυτότητες των υπαλλήλων της, ώστε να επιτρέπει υπογεγραμμένο ηλεκτρονικό ταχυδρομείο και πιστοποίηση μέσω SSL του πελάτη. Άλλη περίπτωση είναι η έκδοση S/MIME πιστοποιητικών είναι για το διπλό λόγο υπογραφής και κρυπτογράφησης ηλεκτρονικού ταχυδρομείου που έχει να κάνει με ευαίσθητα οικονομικά ή νομικά ζητήματα.

4. Object-signing certificates.

Χρησιμοποιούνται για να την αναγνώριση αυτών που υπογράφουν κώδικα Java, JavaScript Scripts ή άλλα υπογεγραμμένα αρχεία.

Για παράδειγμα μια εταιρία λογισμικού υπογράφει λογισμικό το οποίο παρουσιάζεται στο διαδίκτυο για να διασφαλίσει στους χρήστες ότι το εν λόγω λογισμικό είναι legitimate προϊόν αυτής της εταιρίας. Χρησιμοποιώντας πιστοποιητικά και ψηφιακές υπογραφές με αυτό τον τρόπο δίνεις τη δυνατότητα στους χρήστες να αναγνωρίζουν και να ελέγχουν το είδος της πρόσβασης που έχει το κατεβασμένο από το διαδίκτυο λογισμικό στους υπολογιστές τους.

5. Πιστοποιητικά Αρχών Πιστοποίησης (CA certificates).

Χρησιμοποιούνται για να αναγνωρίζουν τις αρχές πιστοποίησης (CAs). Το λογισμικό του πελάτη και του εξυπηρετητή χρησιμοποιεί τέτοια πιστοποιητικά για να καθορίσει ποια άλλα πιστοποιητικά μπορούν να είναι αξιόπιστα.

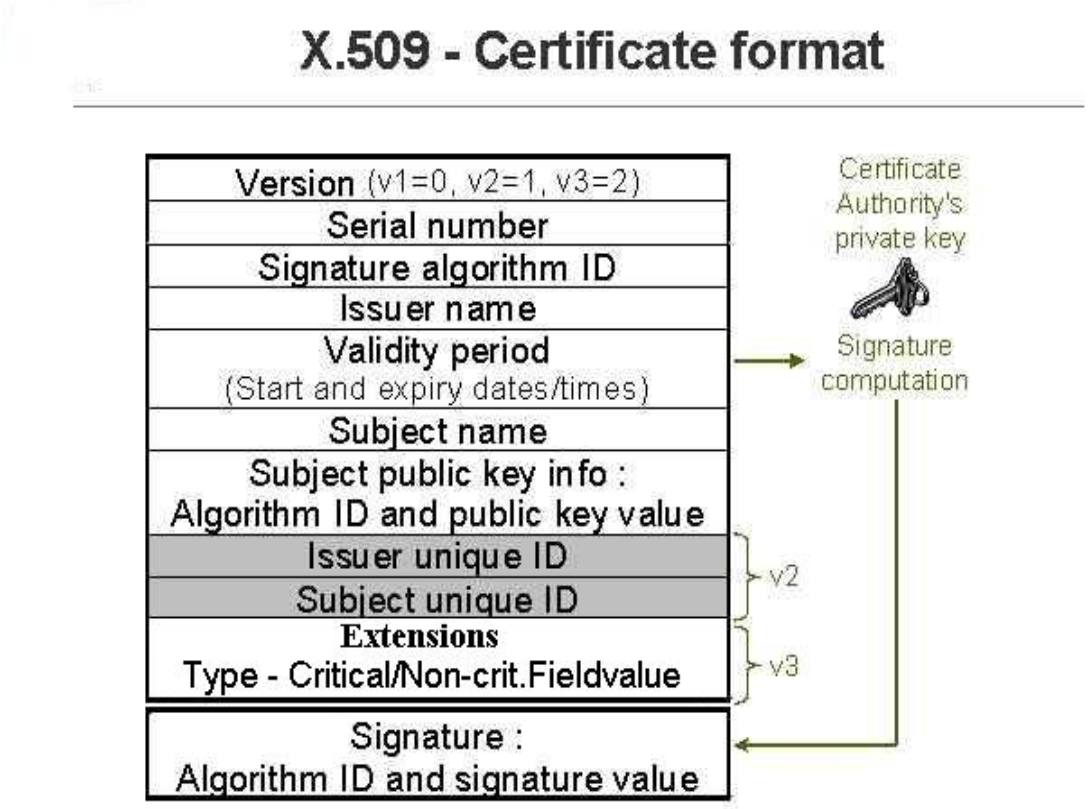
3.7. Πιστοποιητικό X.509

Η ITU-T (International Telecommunications Union) έχει θεσπίσει ένα πρότυπο για τα ψηφιακά πιστοποιητικά, το Recommendation X.509 [xxvii] (ISO/IEC 9594-8:1998). Περιέχει τα εξής χαρακτηριστικά:

- Version: Η έκδοση του X.509. Ανάλογα με αυτή, καθορίζεται τι είδους πληροφορίες θα μπορούν να υπάρχουν στο συγκεκριμένο πιστοποιητικό. Υπάρχουν τρεις εκδόσεις του.
- Serial Number: Η οντότητα που δημιούργησε το πιστοποιητικό δίνει έναν μοναδικό αριθμό στο κάθε πιστοποιητικό που εκδίδει.
- Signature Algorithm Identifier: Ο αλγόριθμος που χρησιμοποίησε η Αρχή έκδοσης του πιστοποιητικού (CA) για να το υπογράψει.
- Issuer Name: Το όνομα (γραμμένο σύμφωνα με το πρότυπο X.500) της οντότητας που υπέγραψε το πιστοποιητικό, δηλαδή της CA. (Το πρότυπο X.500 εξασφαλίζει την μοναδικότητα του ονόματος στο Internet)
- Validity Period: Η χρονική περίοδος μέσα στην οποία το πιστοποιητικό θεωρείται έγκυρο. Η διάρκειά της μπορεί να ποικίλει από μερικά δευτερόλεπτα μέχρι σχεδόν έναν αιώνα και εξαρτάται από διάφορους παράγοντες, όπως το πόσο ασφαλές θεωρείται το ιδιωτικό κλειδί που χρησιμοποιείται για την υπογραφή του πιστοποιητικού, ή το χρηματικό ποσό που κάποιος θα καταβάλει για το πιστοποιητικό.
- Subject (User) Name: Το όνομα (σύμφωνα πάντα με το X.500) της οντότητας της οποίας το δημόσιο κλειδί αναγνωρίζει το πιστοποιητικό.
- Subject Public Key Information: Αναγνωριστικά για το δημόσιο κλειδί, τον αλγόριθμο του κλειδιού και άλλες πληροφορίες που μπορεί να είναι απαραίτητες.
- Issuer unique identifier (στις εκδόσεις 2 και 3 μόνο): Αναγνωριστικό της Αρχής που εκδίδει το πιστοποιητικό.
- Subject unique identifier (στις εκδόσεις 2 και 3 μόνο): Αναγνωριστικό της οντότητας της οποίας το δημόσιο κλειδί αναγνωρίζει το πιστοποιητικό.

- Extensions (στην έκδοση 3 μόνο): Επιπλέον αναγνωριστικά που μπορεί να καθορίσει ο χρήστης. Μερικά παραδείγματα που συναντώνται συχνά είναι: KeyUsage (περιορίζει την χρήση του κλειδιού μόνο για συγκεκριμένες ενέργειες), AlternativeNames (εναλλακτικά ονόματα που μπορεί να σχετίζονται με αυτό το δημόσιο κλειδί, όπως email, διευθύνσεις ιστοσελίδων κ.λ.π.). Αυτά τα extensions μπορούν να χαρακτηριστούν ως κρίσιμα (critical) έτσι ώστε να ελέγχονται και να είναι υποχρεωτική η χρήση τους. Για παράδειγμα αν το KeyUsage χαρακτηριστεί ως κρίσιμο και έχει την τιμή "keyCertSign" τότε εάν επιχειρηθεί να χρησιμοποιηθεί αυτό το πιστοποιητικό σε μια επικοινωνία με SSL, θα απορριφθεί, αφού η τιμή του υποδηλώνει ότι το ιδιωτικό κλειδί πρέπει να χρησιμοποιείται μόνο για την υπογραφή πιστοποιητικών και όχι για χρήση με SSL.
- Τέλος, υπογραφή για όλα τα παραπάνω πεδία

Στο Σχήμα 11 βλέπουμε συγκεντρωτικά τα παραπάνω πεδία που περιέχονται σε ένα πιστοποιητικό X.509. Φαίνεται επίσης ποια στοιχεία έχουν προστεθεί στις εκδόσεις 2 και 3.



Σχήμα 11: Πιστοποιητικό X.509

3.8. Ερωτήματα γύρω από την ασφάλεια των ψηφιακών υπογραφών

Όταν μία οντότητα υπογράφει ψηφιακά ένα μήνυμα, όπως γνωρίζουμε χρησιμοποιεί το ψηφιακό της κλειδί. Για να το κάνει αυτό κάποιος, χρειάζεται προφανώς έναν υπολογιστή για να αποθηκεύσει το κλειδί, αλλά και για να εκτελέσει όλους τους πολύπλοκους μαθηματικούς υπολογισμούς που εμπλέκονται σε μια τέτοια διαδικασία. Όμως από τη στιγμή που χρησιμοποιεί τον υπολογιστή, θα πρέπει να εμπιστευτεί το λειτουργικό σύστημά του. Ακόμα και αν χρησιμοποιεί την τεχνολογία των έξυπνων καρτών για την αποθήκευση του κλειδιού, το λειτουργικό σύστημα είναι αυτό που διαχειρίζεται την πληροφορία, δέχεται τα δεδομένα και που τελικά τα παρουσιάζει στον χρήστη.

Τα σημερινά λειτουργικά συστήματα όμως είναι εξαιρετικά πολύπλοκα, προκειμένου να δίνουν στον απλό χρήστη ένα εύχρηστο και φιλικό περιβάλλον GUI (Graphical User Interface). Όσο όμως αυξάνεται η πολυπλοκότητα ενός συστήματος, τόσο πιο ανασφαλές αυτό καθίσταται. Έτσι τόσο στα Windows όσο και στο Linux υπάρχουν ιοί, σκουλήκια (worms, δηλαδή προγράμματα που έχουν την ικανότητα να αυτοαναπαράγονται και να εξαπλώνονται μέσω του ίντερνετ), Backdoors (προγράμματα που μπορούν να παρέχουν μη εξουσιοδοτημένη πρόσβαση σε έναν υπολογιστή).

Έχουμε λοιπόν την "σύγκρουση" δύο στοιχείων: Η ασφάλεια του συστήματος και το γραφικό - φιλικό προς τον χρήστη περιβάλλον. Είναι όμως και απαραίτητα: Ένα ικανοποιητικό περιβάλλον εργασίας UI (User Interface) προκειμένου να μπορούν να γίνουν οι διάφορες, ενδεχομένως πολύπλοκες δοσοληψίες, αλλά ταυτόχρονα, ασφάλεια, που θα εγγυάται την προστασία του ιδιωτικού κλειδιού και θα εξασφαλίζει το ότι ο χρήστης θα βλέπει ακριβώς τι υπογράφει.

Σχήμα 12: Δυο αντικρουόμενα αλλά απαραίτητα χαρακτηριστικά

Τα μαθηματικά λοιπόν που χρησιμοποιούνται στην κρυπτογραφία, όσο ισχυρά και αν είναι, δεν μπορούν να γεφυρώσουν το κενό μεταξύ του χρήστη και του υπολογιστή του. Εάν ο υπολογιστής δεν είναι αξιόπιστος, τότε κανένα μέτρο δεν μπορεί να εγγυηθεί ασφάλεια.

Μια μερική λύση σε αυτό το πρόβλημα είναι για παράδειγμα η έννοια της συνυπογράφουσας αρχής (co-signing registry) [xxviii], δηλαδή μια παρόμοια προσέγγιση με το αντίστοιχο πρόβλημα των απλών υπογραφών: χρειάζεται ένας μάρτυρας που βεβαιώνει ότι υπογράψαμε ένα κείμενο. Η υπογραφή δεν θεωρείται έγκυρη εάν δεν έχει πρώτα συνυπογραφεί. Ο χρήστης θα πρέπει να έχει τη δυνατότητα να δει εύκολα και ανά πάσα στιγμή, τι έγγραφα έχει υπογράψει με το κλειδί του. Επίσης η Αρχή θα πρέπει να ειδοποιεί τον χρήστη οποτεδήποτε το κλειδί του χρησιμοποιείται για να υπογράψει κάτι.

Επίσης μια ακόμη πρόταση είναι η καθιέρωση κλειδιών μιας χρήσης για υπογραφές. Έτσι περιορίζονται οι κίνδυνοι σε περίπτωση κλοπής του κλειδιού. Η CA θα αρνείται να συνυπογράψει κάτι εφόσον το κλειδί έχει ξαναχρησιμοποιηθεί. Μπορούμε να πούμε ότι με μέτρα σαν τα παραπάνω, πλησιάζουμε τα όσα ισχύουν και για τις φυσικές υπογραφές, όπου, η παρουσία μαρτύρων τις καθιστά πιο ισχυρές.

3.9. Νομικό πλαίσιο ψηφιακών υπογραφών

Μια σημαντική παράμετρος που πρέπει να ληφθεί υπόψη όταν πρόκειται να χρησιμοποιηθεί ένα σύστημα ασφαλείας ψηφιακών υπογραφών, είναι το ισχύον νομικό πλαίσιο. Ιδιαίτερα σε ένα Ιατρικό σύστημα θα πρέπει να είναι σαφές τι συμβαίνει σε περίπτωση που κάποιος π.χ. αρνείται ότι έλαβε ή έστειλε ένα συγκεκριμένο έγγραφο.

Στην Ευρωπαϊκή Ένωση υπάρχει η οδηγία 1999/93/ΕΚ του Ευρωπαϊκού κοινοβουλίου καθώς και τα πορίσματα του Συμβουλίου της 13^{ης} Δεκεμβρίου 1999 πάνω στις ψηφιακές υπογραφές. Έχει εφαρμοστεί σε αρκετές ευρωπαϊκές χώρες και στην Ελλάδα, σύμφωνα με το Προεδρικό Διάταγμα 150/2001 "Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές", αρμόδια αρχή για τον έλεγχο και την εποπτεία των εγκατεστημένων στην Ελλάδα παρόχων υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής καθώς και για την διαπίστωση της συμμόρφωσης προς τις "ασφαλείς διατάξεις δημιουργίας υπογραφής" είναι η Ε.Ε.Τ.Τ. (Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων).

Πρέπει να σημειώσουμε ότι δίνεται ιδιαίτερη έμφαση στη διαφορά μεταξύ του *ιδιοκτήτη* ενός κλειδιού και του *διαχειριστή* αυτού. Ο ιδιοκτήτης είναι αυτός που έχει το δικαίωμα χρήσης του κλειδιού. Ο διαχειριστής είναι η οντότητα που πρακτικά διαχειρίζεται το κλειδί και μπορεί να είναι για παράδειγμα, ο server που δημιουργεί τις υπογραφές.

Υπάρχουν βέβαια και περιπτώσεις όπου ο διαχειριστής του κλειδιού είναι κάποιο άτομο. Για παράδειγμα αν κάποια είναι ιδιοκτήτρια ενός ιδιωτικού κλειδιού, τότε ο γραμματέας της μπορεί να είναι ο διαχειριστής του κλειδιού και μπορεί μάλιστα να το χρησιμοποιήσει χωρίς την άδεια της, παράνομα φυσικά. Αν και σε ένα δικαστήριο μια ηλεκτρονική υπογραφή είναι δεκτή ως πειστήριο, ο δικαστής είναι αυτός που καθορίζει τη βαρύτητά του.

Σύμφωνα λοιπόν με την οδηγία 1999/93/ΕΚ αναγνωρίζονται τριών ειδών ψηφιακές υπογραφές, η κάθε μία με διαφορετική δικαστική αξία:

1. Ηλεκτρονική υπογραφή (καλείται και "ασθενής" ή "ελαφριά" υπογραφή): "Πρόκειται για δεδομένα σε ηλεκτρονική μορφή που βρίσκονται μαζί ή συνδέονται λογικά με άλλα ηλεκτρονικά δεδομένα και για τα οποία λειτουργούν ως μέσο αυθεντικοποίησης" (άρθρο 2.1 της Οδηγίας 1999/93/ΕC). Χρησιμοποιεί κρυπτογραφία ασύμμετρου κλειδιού και χρησιμεύει ως μέσο αυθεντικοποίησης, με την έννοια ότι εξασφαλίζει ότι το άτομο που έστειλε τα υπογεγραμμένα δεδομένα είναι και ο *διαχειριστής* του κλειδιού. Ωστόσο δεν μπορούμε να είμαστε βέβαιοι ότι είναι και ο *ιδιοκτήτης* του.

2. Προηγμένη ηλεκτρονική υπογραφή: "Είναι η ηλεκτρονική υπογραφή που πληροί τα παρακάτω κριτήρια:

1. Συνδέεται με τον υπογράφοντα και μόνο αυτόν.
2. Είναι ικανή να λειτουργήσει ως αναγνωριστικό του υπογράφοντος.
3. Η δημιουργία της γίνεται με μέσα που ο υπογράφων διατηρεί υπό τον έλεγχό του και μόνο.
4. Συνδέεται με τα δεδομένα στα οποία αναφέρεται με τέτοιο τρόπο ώστε κάθε αλλαγή στα δεδομένα αυτά είναι ανιχνεύσιμη" (άρθρο 2.2 της Οδηγίας 1999/93/ΕC).

Η προηγμένη ψηφιακή υπογραφή έχει σημαντικότερη αξία από την απλή ψηφιακή υπογραφή: Εγγυάται την *ακεραιότητα* του κειμένου, αλλά και την *αυθεντικοποίηση*.

3. Προηγμένη ηλεκτρονική υπογραφή που βασίζεται σε ένα κατάλληλο πιστοποιητικό και που δημιουργείται από μια Αρχή δημιουργίας ασφαλών υπογραφών (καλείται επίσης ασφαλής ή ισχυρή ψηφιακή υπογραφή). Η Αρχή δημιουργίας ασφαλών υπογραφών είναι η Certification Authority ή CA και πρέπει να έχει τα κατάλληλα τεχνικά χαρακτηριστικά που απαιτούνται ώστε, να εξασφαλιστεί το γεγονός, ότι το κλειδί δεν θα μπορεί να αναπαραχθεί, ούτε να πλαστογραφηθεί, μέσα σε ένα λογικό χρονικό διάστημα. Το

χρονικό διάστημα αυτό, θα πρέπει να είναι μεγαλύτερο σε διάρκεια από την περίοδο εγκυρότητας της υπογραφής. Οι απαιτήσεις αυτές καθορίζονται ξεκάθαρα από την Επιτροπή Ψηφιακών Υπογραφών (Electronic Signature Committee), που βοηθά την ανάλυση τεχνικών θεμάτων.

Οι απαιτήσεις μια τέτοιας ασφαλούς υπογραφής είναι σημαντικά: τα κατάλληλα κλειδιά και λογισμικό, έξυπνες κάρτες και κάθε άλλο απαραίτητο μέσο πρέπει να είναι της τελευταίας τεχνολογίας (σύμφωνα με την δικανική αρχή "meliores scientia et conoscientia" δηλαδή με την τελευταία λέξη της τεχνολογίας). Οι απαιτήσεις για ένα κατάλληλο πιστοποιητικό είναι (σύμφωνα με το παράρτημα I της Οδηγίας 1999/93/EC):

5. Η ένδειξη ότι το πιστοποιητικό εκδίδεται ως κατάλληλο πιστοποιητικό (qualified certificate)
6. Ένα αναγνωριστικό της αρχής CA καθώς και του κράτους (Ευρωπαϊκού ή μη) στο οποίο εκδόθηκε
7. Το όνομα (ή ψευδώνυμο) του υπογράφοντα.
8. Δεδομένα για την επαλήθευση της υπογραφής που αντιστοιχούν σε δεδομένα που δημιουργήθηκαν κατά την δημιουργία της υπογραφής και βρίσκονται κάτω από τον έλεγχο του υπογράφοντα.
9. Ένδειξη που δηλώνει την περίοδο εγκυρότητας της υπογραφής.
10. Αναγνωριστικό του πιστοποιητικού.
11. Η προηγμένη υπογραφή της αρχής CA.

Η ασφαλής υπογραφή μπορεί να περιέχει επίσης και άλλα στοιχεία, όπως ένας όρος για κάποιο ιδιαίτερο χαρακτηριστικό του υπογράφοντος. Για παράδειγμα ένας δικηγόρος μιας εταιρίας μπορεί να έχει μια ασφαλή υπογραφή. Μπορεί να υπάρχουν περιορισμοί που να προσδιορίζουν ότι μπορούν να υπογραφούν συμβόλαια μόνο με ορισμένες χώρες ή μπορεί να υπάρχουν όρια στην χρηματική αξία των υπογραφόμενων συμβολαίων.

Αυτός ο τύπος ψηφιακής υπογραφής έχει μεγάλη νομική αξία: Εγγυάται αυθεντικοποίηση, ακεραιότητα, εμπιστευτικότητα καθώς και εμποδίζει την δυνατότητα άρνησης της αποστολής/λήψης ενός εγγράφου. Πρέπει ωστόσο να χρησιμοποιείται με τον σωστό τρόπο, δηλαδή ο υπογράφων έχει κάποια καθήκοντα[xxix]:

1. <u>Καθήκοντα φύλαξης</u> των απαραίτητων εργαλείων, όπως η έξυπνη κάρτα, ώστε να μην μπορεί να έχει κανείς μη εξουσιοδοτημένη πρόσβαση σε αυτά. Εάν κάποιος δεν

προστατεύει την κάρτα ψηφιακής υπογραφής, τότε αυτός καθίσταται υπεύθυνος σε περίπτωση κλοπής. Συνήθως μια έξυπνη κάρτα προστατεύεται από κωδικό pin. Αν όμως για παράδειγμα, ένας γιατρός αφήσει την κάρτα του, με την οποία υπογράφει ψηφιακά ιατρικές συνταγές, επάνω στο γραφείο του και έχει γραμμένο το pin επάνω στην κάρτα, ενώ ταυτόχρονα το γραφείο είναι ανοιχτό και γεμάτο κόσμο και κλαπεί η κάρτα του, τότε ο γιατρός αυτός φέρει μεγάλο μερίδιο ευθύνης. Ανάλογη νομοθεσία ισχύει και για τις γνωστές πιστωτικές κάρτες.

2. Καθήκοντα πληροφόρησης. Πρέπει ο χρήστης να έχει πληροφορήσει την Αρχή έκδοσης πιστοποιητικών για το πλαίσιο λειτουργίας της υπογραφής και τους περιορισμούς που οριοθετούν την χρήση της. Πρέπει επίσης η CA να ενημερωθεί για κάθε απώλεια αξίας της ψηφιακής υπογραφής. Αυτό περικλείει για παράδειγμα την κλοπή της έξυπνης κάρτας μαζί με το pin, την απόσυρση ενός υπαλλήλου από μια εταιρία που του έδινε το δικαίωμα να υπογράφει ψηφιακά εκ μέρους της, ή μια χρεοκοπία της εταιρείας που αντιπροσωπεύουν οι υπογραφές. Σε όλες αυτές τις περιπτώσεις, εάν ο χρήστης δεν ενημερώσει την CA τότε αυτός καθίσταται υπόλογος. Άλλο ένα χαρακτηριστικό παράδειγμα είναι το εξής: Ένας υπάλληλος μιας εταιρίας έχει την δυνατότητα με μια ασφαλή ψηφιακή υπογραφή να υπογράφει συμβόλαια αξίας μέχρι και 10.000 ευρώ. Όμως η εταιρία αυτή δεν έχει αναφέρει αυτόν τον περιορισμό στην CA. Σε περίπτωση σύναψης συμβολαίου αξίας 1.000.000 ευρώ, δεν μπορούμε να το θεωρήσουμε άκυρο, δηλαδή τα χρήματα δεν μπορούν να ζητηθούν από την εταιρία με την οποία συνάφθηκε το συμβόλαιο, αλλά μόνο από τον υπάλληλο που το έκανε.

3. Καθήκον ανανέωσης. Κανένα κλειδί δεν είναι ασφαλές για πάντα, αφού η πρόοδος της τεχνολογίας οδηγεί στην ανακάλυψη νέων αλγορίθμων και καθιστά τους παλαιότερους αλγορίθμους ανασφαλείς. Η ψηφιακή υπογραφή είναι έγκυρη μονάχα μέσα στο χρονικό διάστημα που καθορίζεται ως έγκυρη. Αυτό πρέπει να είναι πολύ μικρότερο από τον χρόνο που θα χρειαζόταν ένας κρυπταναλυτής να "σπάσει" την κρυπτογράφηση. Μετά το πέρας της περιόδου εγκυρότητας, η CA δεν θα εγγυάται πλέον την ασφάλεια της υπογραφής. Πρέπει λοιπόν στο τέλος αυτής της περιόδου, ο χρήστης να ανανεώνει την ψηφιακή υπογραφή και αυτό σημαίνει ότι πρέπει να παραλάβει ένα καινούριο κλειδί. Συνέχιση της χρήσης μιας ασφαλούς ψηφιακής υπογραφής και μετά το τέλος της περιόδου εγκυρότητας, απαξιώνει την νομική του αξία και μετατρέπεται σε "ασθενής" ψηφιακή υπογραφή.

Συμπερασματικά, οι ψηφιακές υπογραφές στηρίζονται από έγκυρους Ευρωπαϊκούς νόμους και έτσι οι ασφαλείς ψηφιακές υπογραφές έχουν αποκτήσει σημαντική νομική αξία.

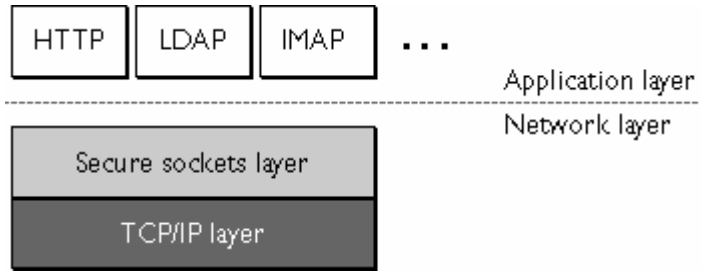
Μπορούμε να πούμε ότι είναι πλέον απαραίτητο στοιχείο για εφαρμογές που απαιτούν την διακίνηση πληροφορίας με ασφάλεια και υπευθυνότητα.

4. Secure Socket Layer (SSL) xxx

4.1. Το πρωτόκολλο SSL.

Το πρωτόκολλο SSL, το οποίο αναπτύχθηκε αρχικά από την Netscape Communications είναι ένα πακέτο από κανόνες που ελέγχουν την πιστοποίηση του εξυπηρετητή, την πιστοποίηση του πελάτη και την κρυπτογραφημένη επικοινωνία ανάμεσα σε εξυπηρετητές και σε πελάτες. Το SSL χρησιμοποιείται ευρέως στο διαδίκτυο ειδικά σε εφαρμογές που περιλαμβάνουν εμπιστευτική συναλλαγή πληροφοριών όπως για παράδειγμα τον αριθμό πιστωτικών καρτών. Το πρωτόκολλο SSL απαιτεί κατ' ελάχιστο ένα πιστοποιητικό εξυπηρετητή SSL. Σαν μέρος της αρχικής διαδικασίας της "χειραψίας" (Handshake), ο εξυπηρετητής παρουσιάζει το πιστοποιητικό του στον πελάτη ώστε να πιστοποιηθεί η ταυτότητά του. Η διαδικασία της πιστοποίησης χρησιμοποιεί τη μέθοδο κρυπτογράφησης δημοσίου κλειδιού και ψηφιακών υπογραφών για να επιβεβαιώσει ότι ο εξυπηρετητής είναι αυτός που ισχυρίζεται ότι είναι. Μόλις ο εξυπηρετητής έχει πιστοποιηθεί, πελάτης και εξυπηρετητής χρησιμοποιούν τεχνικές κρυπτογράφησης συμμετρικού κλειδιού, η οποία είναι πολύ γρήγορη για να κρυπτογραφήσουν τις πληροφορίες που ανταλλάσσουν για το υπόλοιπο της συνόδου και τον όποια παραποίηση μπορεί να παρουσιαστεί. Οι εξυπηρετητές μπορεί προαιρετικά να ρυθμιστούν να απαιτούν πιστοποίηση πελάτη όπως και πιστοποίηση εξυπηρετητή. Σε αυτή την περίπτωση μετά την επιτυχή πιστοποίηση του εξυπηρετητή ο πελάτης επίσης παρουσιάζει το δικό του πιστοποιητικό στον εξυπηρετητή για να πιστοποιηθεί η δική του ταυτότητα πριν εγκαθιδρυθεί η κρυπτογραφημένη SSL σύνδεση.

Το πρωτόκολλο TCP/IP ελέγχει τη μεταφορά και δρομολόγηση δεδομένων στο διαδίκτυο. Άλλα πρωτόκολλα όπως τα Hyper Text Transport Protocol (HTTP), Lightweight Directory Access Protocol (LDAP), Internet Messaging Access Protocol (IMAP), τρέχουν πάνω από το TCP/IP με την έννοια ότι όλα χρησιμοποιούν το TCP/IP για να υποστηρίξουν τυπικές εφαρμογές όπως την αναπαραγωγή ιστοσελίδων.



Σχήμα 13:Το SSL τρέχει πάνω από το πρωτόκολλο TCP/IP και κάτω από πρωτόκολλα ψηλού επιπέδου εφαρμογών.

Η SSL Αυθεντικοποίηση εξυπηρετητή επιτρέπει στον χρήστη να επιβεβαιώσει την ταυτότητα του εξυπηρετητή. Το SSL ενεργοποιημένο λογισμικό του πελάτη μπορεί να χρησιμοποιήσει δεδομένες τεχνικές κρυπτογράφησης δημοσίου κλειδιού προκειμένου να ελέγξει ότι το πιστοποιητικό του εξυπηρετητή και το δημόσιο κλειδί του είναι έγκυρα και έχουν εκδοθεί από μια αρχή πιστοποίησης που είναι έμπιστη για τον πελάτη.

Η SSL Αυθεντικοποίηση πελάτη επιτρέπει στον εξυπηρετητή να επιβεβαιώσει την ταυτότητα του χρήστη. Χρησιμοποιώντας τις ίδιες τεχνικές όπως αυτές που χρησιμοποιούνται για την αυθεντικοποίηση του εξυπηρετητή, το SSL ενεργοποιημένο λογισμικό του εξυπηρετητή μπορεί να ελέγξει ότι του πελάτη το πιστοποιητικό και το δημόσιο κλειδί είναι έγκυρα και έχουν εκδοθεί από μια Αρχή Πιστοποίησης που συγκαταλέγεται στις έμπιστες Αρχές Πιστοποίησης του εξυπηρετητή.

Μια κρυπτογραφημένη SSL σύνδεση απαιτεί όλες οι πληροφορίες που στέλνονται ανάμεσα σε ένα πελάτη και ένα εξυπηρετητή να κρυπτογραφούνται από το απεσταλμένο λογισμικό και να αποκρυπτογραφούνται από το λαμβανόμενο λογισμικό, ώστε να προσφέρεται υψηλός βαθμός εμπιστευτικότητας που είναι σημαντική και για τα δυο μέρη σε κάθε ιδιωτική συναλλαγή. Επιπροσθέτως, τα δεδομένα που στέλνονται δια μέσου μιας κρυπτογραφημένης SSL σύνδεσης προστατεύονται με ένα μηχανισμό που ανιχνεύει το **tampering**, δηλαδή την αυτόματη ανίχνευση του αν τα δεδομένα έχουν αλλοιωθεί κατά τη μεταφορά.

4.2. Αλγόριθμοι Κρυπτογράφησης που χρησιμοποιούνται με το SSL πρωτόκολλο.

Το SSL πρωτόκολλο υποστηρίζει μια ποικιλία διαφορετικών αλγορίθμων κρυπτογράφησης (Ciphers), για χρήση σε επικοινωνίες όπως η αυθεντικοποίηση ανάμεσα στον πελάτη και τον εξυπηρετητή, τη μετάδοση πιστοποιητικών, και την δημιουργία

κλειδιών συνόδων. Πελάτες και εξυπηρετητές μπορεί να υποστηρίζουν διαφορετικές μεθόδους ή πακέτα αλγορίθμων ανάλογα με παράγοντες όπως η έκδοση (Version) του SSL πρωτοκόλλου που υποστηρίζουν, ταχτικές εταιριών που έχουν να κάνουν με συγκεκριμένη αποδεκτή ισχύ κρυπτογράφησης και περιορισμοί των κυβερνήσεων στην έκδοση του λογισμικού του SSL. Μεταξύ άλλων λειτουργιών του, το πρωτόκολλο χειραψίας SSL καθορίζει πως ο πελάτης και ο εξυπηρετητής διαπραγματεύονται ποιους αλγόριθμους κρυπτογράφησης (Cipher Suites) θα χρησιμοποιήσουν για να αυθεντικοποιήσουν ο ένας τον άλλο, να αποστείλουν πιστοποιητικά και να εγκαθιδρύσουν κλειδιά σε συνόδους.

Παρακάτω περιγράφονται ενδεικτικά μερικοί από τους αλγόριθμους κρυπτογράφησης.

- **DES (Data Encryption Standard)**. Πρότυπο κρυπτογράφησης δεδομένων. Ένας αλγόριθμος κρυπτογράφησης που χρησιμοποιείται από την κυβέρνηση των ΗΠΑ.
- **DSA (Digital Signature Algorithm)** Αλγόριθμος ψηφιακής υπογραφής. Τμήμα της ψηφιακής πιστοποίησης χρησιμοποιείται από τις ΗΠΑ.
- **KEA (Key Exchange Algorithm)** Αλγόριθμος εναλλαγής κλειδιού. Ένας αλγόριθμος που χρησιμοποιήθηκε για την εναλλαγή κλειδιού από την κυβέρνηση των ΗΠΑ.
- **MD5 (Message Digest Algorithn)** Αναπτύχθηκε από τον Rivest.
- **RC2 και RC4** Αλγόριθμοι Κρυπτογράφησης του Rivest που αναπτύχθηκαν για την ασφάλεια δεδομένων του αλγόριθμου RSA.
- **RSA** ένας αλγόριθμος δημοσίου κλειδιού για κρυπτογράφηση και αυθεντικοποίηση που αναπτύχθηκε από τους Rivest, Shamir και Adleman.
- **RSA εναλλαγή κλειδιού (RSA key exchange).**Ένας αλγόριθμος εναλλαγής κλειδιού για SSL που βασίζεται στον αλγόριθμο RSA.
- **SHA1 (Secure Hash Algorithm)** μια λειτουργία Hash που χρησιμοποιήθηκε και πάλι από την κυβέρνηση των ΗΠΑ.
- **SKIPJACK** Ένας απόρρητος αλγόριθμος συμμετρικού κλειδιού.
- **Τριπλός DES (Triple DES)** Αλγόριθμος DES που εφαρμόζεται τρεις φορές.

Αλγόριθμοι ανταλλαγής κλειδιού όπως οι KEA και RSA ελέγχουν τον τρόπο με τον οποίο εξυπηρετητής και πελάτης καθορίζουν τα συμμετρικά κλειδιά που θα χρησιμοποιήσουν κατά τη διάρκεια μιας SSL συνόδου. Οι πιο κοινά χρησιμοποιούμενοι SSL αλγόριθμοι κρυπτογράφησης χρησιμοποιούν εναλλαγή κλειδιού με τον αλγόριθμο RSA. Οι

διαχειριστές δικτύων μπορούν να ενεργοποιούν ή να απενεργοποιούν οποιοδήποτε από τους υποστηριζόμενους αλγόριθμους κρυπτογράφησης για τους εξυπηρετητές και τους πελάτες. Όταν ένας συγκεκριμένος πελάτης και εξυπηρετητής ανταλλάσσουν πληροφορίες κατά τη διάρκεια μιας SSL χειραψίας αναγνωρίζουν τον ισχυρότερο ενεργοποιημένο αλγόριθμο που υποστηρίζουν από κοινού και χρησιμοποιούν αυτές για την SSL σύνοδο. Την απόφαση σχετικά με το ποιους αλγόριθμους κρυπτογράφησης αποφασίζει να ενεργοποιήσει ένας οργανισμός εξαρτάται την ευαισθησία των δεδομένων, την ταχύτητα του αλγόριθμου κτλ.

4.3. Η μέθοδος της χειραψίας του SSL (The SSL Handshake)

Το SSL πρωτόκολλο χρησιμοποιεί ένα συνδυασμό δημοσίου κλειδιού και συμμετρικού κλειδιού κρυπτογράφησης. Η κρυπτογράφηση συμμετρικού κλειδιού είναι πολύ γρηγορότερη από την κρυπτογράφηση δημοσίου κλειδιού αλλά η κρυπτογράφηση δημοσίου κλειδιού προσφέρει καλύτερες τεχνικές αυθεντικοποίησης. Μια SSL σύνοδος πάντα ξεκινά με μια ανταλλαγή μηνυμάτων που αποκαλούνται SSL χειραψία (SSL Handshake). Η χειραψία επιτρέπει στον εξυπηρετητή να αυθεντικοποιήσει τον εαυτό του στον πελάτη χρησιμοποιώντας τεχνικές δημοσίου κλειδιού και στην συνέχεια επιτρέπει στον πελάτη να και τον εξυπηρετητή να συνεργαστούν στην δημιουργία κλειδιών που θα χρησιμοποιηθούν για τη γρήγορη κρυπτογράφηση, αποκρυπτογράφηση και ανίχνευση παραποίησης κατά τη διάρκεια της συνόδου που ακολουθεί. Προαιρετικά όπως προαναφέρθηκε η χειραψία επιτρέπει επίσης και στον εξυπηρετητή να αυθεντικοποιήσει την ταυτότητα του πελάτη.

Κάνοντας μια περίληψη των βημάτων κατά τη διάρκεια μιας SSL χειραψίας και υποθέτοντας ως αλγόριθμο κρυπτογράφησης τον RSA όπως αναλύθηκε προηγουμένως έχουμε:

Ο πελάτης στέλνει στον εξυπηρετητή τον αριθμό έκδοσης (version number) του πιστοποιητικού SSL, ρυθμίσεις σχετικά με την κρυπτογράφηση, τυχαία ενεργοποιημένα δεδομένα και άλλες πληροφορίες που χρειάζεται ο εξυπηρετητής για να επικοινωνήσει με τον πελάτη χρησιμοποιώντας το SSL.

Ο εξυπηρετητής στέλνει στον πελάτη τον αριθμό έκδοσης (version number) του πιστοποιητικού SSL, ρυθμίσεις σχετικά με την κρυπτογράφηση, τυχαία ενεργοποιημένα δεδομένα και άλλες πληροφορίες που χρειάζεται ο πελάτης προκειμένου να επικοινωνήσει μέσω SSL με τον εξυπηρετητή. Ο εξυπηρετητής επίσης στέλνει το πιστοποιητικό του και, αν ο πελάτης ζητά μια πηγή του εξυπηρετητή που απαιτεί πιστοποίηση του πελάτη, ζητά το πιστοποιητικό του πελάτη.

1. Ο πελάτης χρησιμοποιεί κάποιες από τις πληροφορίες που έχουν σταλεί από τον εξυπηρετητή για να πιστοποιήσει τον εξυπηρετητή. Εάν αυτό δεν επιτευχθεί ο χρήστης προειδοποιείται για το πρόβλημα και ενημερώνεται ότι δεν μπορεί να εγκατασταθεί μια κρυπτογραφημένη και πιστοποιημένη σύνδεση. Εάν η πιστοποίηση του εξυπηρετητή γίνει με επιτυχία τότε ο πελάτης πηγαίνει στο βήμα 4 που ακολουθεί.
2. Χρησιμοποιώντας όλα τα δεδομένα που έχουν παραχθεί από τη μέθοδο της χειραψίας έως τώρα, ο πελάτης (με τη συνεργασία του εξυπηρετητή, ανάλογα και με τη μέθοδο κρυπτογράφησης που χρησιμοποιείται) δημιουργεί το premaster secret για το σύνοδος, το κρυπτογραφεί με το κλειδί του εξυπηρετητή το δημόσιο κλειδί (που έχει αποκτηθεί στο βήμα 2) και στέλνει το κρυπτογραφημένο premaster secret στον εξυπηρετητή.
3. Εάν ο εξυπηρετητής έχει ζητήσει αυθεντικοποίηση πελάτη (προαιρετικό βήμα στη μέθοδο), ο πελάτης επίσης υπογράφει ένα κομμάτι δεδομένων το οποίο είναι μοναδικό σε αυτή τη χειραψία και γνωστό από τον πελάτη και τον εξυπηρετητή. Σε αυτή την περίπτωση ο πελάτης στέλνει τα υπογεγραμμένα δεδομένα και το πιστοποιητικό του στον εξυπηρετητή μαζί και τον κρυπτογραφημένο premaster secret.
4. Εάν ο εξυπηρετητής έχει ζητήσει αυθεντικοποίηση πελάτη, επιχειρεί να αυθεντικοποιήσει τον πελάτη. Εάν ο πελάτης δεν μπορεί να αυθεντικοποιηθεί η σύνοδος τερματίζεται. Εάν ο πελάτης αυθεντικοποιηθεί με επιτυχία, ο εξυπηρετητής χρησιμοποιεί το ιδιωτικό του κλειδί για να αποκρυπτογραφήσει το premaster secret, μετά παρουσιάζει μια σειρά βημάτων (την οποία ο πελάτης επίσης παρουσιάζει, ξεκινώντας από το ίδιο premaster secret) για να δημιουργήσει το master secret.
5. Και ο εξυπηρετητής αλλά και ο πελάτης χρησιμοποιούν το master secret για να παράγουν τα κλειδιά της συνόδου τα οποία είναι συμμετρικά κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση και την αποκρυπτογράφηση των πληροφοριών που ανταλλάσσονται κατά τη διάρκεια της SSL συνόδου και για να επιβεβαιώσει την ακεραιότητα δηλαδή, να ανιχνεύσει όποιες αλλαγές δεδομένων ανάμεσα στην ώρα που στάλθηκαν και την ώρα που λήφθηκαν δια μέσου της συνόδου.
6. Ο πελάτης στέλνει ένα μήνυμα στον εξυπηρετητή ενημερώνοντάς τον ότι στο μέλλον τα μηνύματα από τον πελάτη θα κρυπτογραφούνται με το κλειδί της συνόδου. Μετά στέλνει ένα ξεχωριστό (κρυπτογραφημένο) μήνυμα υποδηλώνοντας ότι το μερίδιο του πελάτη της χειραψίας έχει τελειώσει.
7. Ο εξυπηρετητής στέλνει ένα μήνυμα στον πελάτη ενημερώνοντάς τον ότι στο μέλλον τα μηνύματα στον εξυπηρετητή θα κρυπτογραφούνται με το κλειδί της συνόδου. Μετά

στέλνει ένα ξεχωριστό (κρυπτογραφημένο) μήνυμα υποδηλώνοντας ότι η πλευρά του εξυπηρετητή έχει τελειώσει.

8. Η μέθοδος της χειραψίας έχει τελειώσει και η SSL σύνοδος έχει ξεκινήσει. Ο πελάτης και ο εξυπηρετητής χρησιμοποιούν τα κλειδιά της συνόδου για να κρυπτογραφούν και να αποκρυπτογραφούν τα δεδομένα που ανταλλάσσουν και να επικυρώνουν την ακεραιότητά τους.
9. Είναι σημαντικό να υπογραμμίσουμε ότι η αυθεντικοποίηση πελάτη και εξυπηρετητή περιλαμβάνει κρυπτογράφηση δεδομένων με ένα κλειδί ενός δημοσίου – ιδιωτικού ζευγαριού και η αποκρυπτογράφησή του γίνεται με το άλλο κλειδί:

Στην περίπτωση της αυθεντικοποίησης εξυπηρετητών, ο πελάτης κρυπτογραφεί το premaster secret με το δημόσιο κλειδί του εξυπηρετητή. Μόνο το ιδιωτικό κλειδί μπορεί σωστά να αποκρυπτογραφήσει το secret, έτσι ώστε ο πελάτης να έχει κάποια διαβεβαίωση ότι η ταυτότητα που σχετίζεται με το δημόσιο κλειδί είναι στην ουσία ο εξυπηρετητής με τον οποίο ο πελάτης είναι συνδεδεμένος.

Στην περίπτωση της αυθεντικοποίησης του πελάτη, ο πελάτης κρυπτογραφεί μερικές τυχαία δεδομένα με το ιδιωτικό κλειδί του πελάτη, δηλαδή, δημιουργεί μια ψηφιακή υπογραφή. Το δημόσιο κλειδί στο πιστοποιητικό του πελάτη μπορεί σωστά να επικυρώσει την ψηφιακή υπογραφή μόνο εάν το ιδιωτικό κλειδί χρησιμοποιήθηκε. Αλλιώς, ο εξυπηρετητής δεν μπορεί να επικυρώσει την ψηφιακή υπογραφή και η σύνοδος τερματίζεται.

5. Η γλώσσα ASP

5.1. Γιατί χρειαζόμαστε την ASP και με ποιον τρόπο λειτουργεί;

Θα μπορούσε κανείς να αναρωτηθεί γιατί χρειαζόμαστε την ASP τη στιγμή που μπορούμε να χρησιμοποιήσουμε Hyper Text Markup Language (HTML) κώδικα. Ο λόγος είναι ότι θέλουμε να αναπαραστήσουμε πληροφορίες που αλλάζουν δυναμικά. Όταν για παράδειγμα γράφουμε μια σελίδα που παρέχει διαρκώς μεταβαλλόμενες πληροφορίες στους επισκέπτες όπως για παράδειγμα δελτία καιρού, η HTML δεν μπορεί πλέον να ικανοποιήσει αυτή την ανάγκη. Χρειαζόμαστε κάποιο σύστημα που μπορεί να παρουσιάζει δυναμικές πληροφορίες.

Στην γλώσσα της Microsoft, Active Server Pages είναι ένα ανοικτό, μη μεταγλωττισμένο (compile – free) περιβάλλον εφαρμογών, στο οποίο μπορούμε να συνδυάσουμε HTML κώδικα και επαναχρησιμοποιήσιμα στοιχεία του εξυπηρετητή ActiveX για να δημιουργήσουμε δυναμικές και ισχυρές δικτυακές λύσεις. Οι Active Server Pages επιτρέπουν το scripting από την πλευρά του εξυπηρετητή για τον Internet Information Service (IIS) (Web Server). Ο IIS προσφέρει επίσης και υποστήριξη για VBScript και Jscript.

Με απλά λόγια οι Active Server Pages (ASPs) είναι δικτυακές σελίδες που περιέχουν server side scripts παράλληλα με κείμενο και HTML ετικέτες (tags). Τα Server side scripts είναι ειδικές εντολές που μπαίνουν σε δικτυακές σελίδες που υφίστανται επεξεργασία πριν σταλούν από τον εξυπηρετητή στον πρόγραμμα πλοήγησης ιστοσελίδας (Web Browser). Όταν για παράδειγμα πληκτρολογούμε μια διεύθυνση που ψάχνουμε στο διαδίκτυο, τότε το πρόγραμμα πλοήγησης ιστοσελίδων που χρησιμοποιούμε (πρόγραμμα πελάτης) στέλνει μια αίτηση σε έναν εξυπηρετητή (Web Server) και ο τελευταίος του αποστέλλει την ιστοσελίδα. Εάν η ιστοσελίδα περιέχει απλό HTML κώδικα τότε αποστέλλεται χωρίς περαιτέρω επεξεργασία. Αφού το αρχείο ληφθεί ο Web Browser αναπαριστά τα περιεχόμενά του σαν συνδυασμό κειμένου, εικόνων και ήχων. Αντίθετα στην περίπτωση των Active Server Pages η διαδικασία είναι παρόμοια εκτός του ότι υπάρχει ένα επιπλέον βήμα που λαμβάνει χώρα ακριβώς πριν ο εξυπηρετητής στείλει το αρχείο.

Τρέχει όλα τα server side scripts που περιέχονται στη σελίδα και κατόπιν δημιουργείται HTML κώδικας ο οποίος αποστέλλεται στο πρόγραμμα πελάτη (client). Μερικά στοιχεία του κώδικα μπορεί να αναπαριστούν την τρέχουσα ημερομηνία, ώρα και άλλες πληροφορίες. Μπορούμε επίσης να γράψουμε δικό μας κώδικα βάζοντας

οποιεσδήποτε δυναμικές πληροφορίες θέλουμε. Οι Active Server Pages ξεχωρίζουν από τις HTML σελίδες από την προέκταση .asp.

Υπάρχουν πολλά πράγματα τα οποία μπορούμε να επιτύχουμε με τις Active Server Pages, όπως να αναπαραστήσουμε την ημερομηνία την ώρα και άλλες πληροφορίες με διαφορετικούς τρόπους, να έχουμε πρόσβαση σε μια βάση δεδομένων μέσω διαδικτύου. Να παίρνουμε πληροφορίες από αυτή, να την ανανεώνουμε ή να συμπληρώνουμε πληροφορίες. Μπορούμε επίσης να θέτουμε υπό προστασία, με κωδικούς ασφαλείας, συγκεκριμένους τομείς της ιστοσελίδας μας όπου μόνο εξουσιοδοτημένοι χρήστες μπορούν να εισέλθουν.

Τα server side scripts ξεκινούν με <% και τελειώνουν με %>. Το σύμβολο <% ονομάζεται ετικέτα έναρξης και το %> ετικέτα τέλους. Ανάμεσά τους υπάρχουν τα server side scripts. Μπορούμε να εισάγουμε server side scripts οπουδήποτε μέσα στην ιστοσελίδα μας ακόμα και μέσα σε HTML ετικέτες.[xxxi]

5.2. Internet Information Services (IIS).

Η πλατφόρμα στην οποία τρέχουν οι asp σελίδες είναι ο IIS. Εκεί φυλάσσονται σε εικονικούς καταλόγους (Virtual Directories).

Στην εφαρμογή μας εγκαταστήσαμε τον IIS (Version 5.1). Αυτός παρέχει λειτουργίες εξυπηρετητή ιστοσελίδων (World Wide Web Server), εξυπηρετητή μεταφοράς αρχείων (File Transfer Protocol Server), εξυπηρετητή υπηρεσιών ομαδικής αλληλογραφίας (Network News Transfer Protocol Server), διακομιστή ηλεκτρονικής αλληλογραφίας (Simple Mail Transfer Protocol Server), σε συνδυασμό με το λειτουργικό σύστημα των Windows XP.

Ο IIS 5.1 έχει μια εντελώς διαφορετική διαπροσωπία από προηγούμενες εκδόσεις του IIS αλλά και βελτιωμένες δυνατότητες. Το κεντρικό εργαλείο διαχείρισης του IIS 5.1, ο Internet Service Manager (ISM) αποτελείται από την κονσόλα διαχείρισης (Microsoft Management Console (MMC)) και από την υπηρεσία διαχείρισης μέσω ιστοσελίδας(Web – Based Internet Service Manager (HTML)).

Η ISM διαπροσωπία των Windows χρησιμοποιεί την MMC. Η ISM επικεντρώνει όλες τις επιλογές ρυθμίσεων ιεραρχικά σε ένα δέντρο από κόμβους (περιέχει υπηρεσίες, ιστοσελίδες, και εικονικούς φακέλους)

Η ISM χρησιμοποιεί ένα πρόγραμμα παρουσίασης ιστοσελίδων πελάτη (client browser) για να παρέχει πρόσβαση διαχείρισης δια μέσου των asp σελίδων. Ο IIS παρέχει ένα φάσμα νέων χαρακτηριστικών για να συνδυάσει τη διαχείριση ιστοσελίδων στο διαδίκτυο, την ανάπτυξη και στήσιμο δικτυακών εφαρμογών.

Νέα χαρακτηριστικά του IIS περιλαμβάνουν:

- Κληρονομούμενες βασικές ιδιότητες που εφαρμόζονται σε όλες τις ιστοσελίδες ή σε όλες τις τοποθεσίες FTP.
- Ρύθμιση ανά ιστοσελίδα για όλες τις ρυθμίσεις ασφαλείας και επικοινωνίας για κάθε ιστοσελίδα ή σε τοποθεσίες FTP.
- Ρύθμιση παραμέτρων ανά εικονικό κατάλογο σε ζητήματα επικοινωνίας και ασφάλειας.
- Ρύθμιση παραμέτρων ανά κατάλογο, της ασφάλειας καταλόγου και τοποθεσίας περιεχομένου (content location) του καταλόγου, των κεφαλίδων HTTP και μηνυμάτων σφάλματος για κάθε κατάλογο ιστοσελίδας.
- Ρύθμιση παραμέτρων ανά αρχείο, όσον αφορά την ασφάλεια και την τοποθεσία του, των κεφαλίδων HTTP, μηνύματα σφάλματος για όλα τα αρχεία των ιστοσελίδων.

Ο IIS υποστηρίζει τις δυνατότητες της έκδοσης 1.1 του πρωτοκόλλου HTTP 1.1, συμπεριλαμβανομένων των persistent connections, pipelining, χειρισμό της συμπεριφοράς της λανθάνουσας μνήμης(caching directives), και ανακατευθύνσεις HTTP (HTTP redirects).

Τέλος, παρέχει ενσωματωμένη ασφάλεια με διαχείριση πιστοποίησης και υπηρεσίες πιστοποίησης. [xxxii]

ΜΕΡΟΣ 2^{ο} Υλοποίηση εφαρμογής

6. Ανάπτυξη της Βάσης Δεδομένων

6.1. Περιγραφή – Schema.

Η βάση μας δημιουργήθηκε με χρήση του *MySQL* (Server Version 3.23.42, Client Version 3.23.3 –alpha), το οποίο όπως προαναφέρθηκε είναι ανοικτού κώδικα γλώσσα.[xxxiii] Χρησιμοποιήσαμε σαν πρόγραμμα πελάτη την *MySQLGUI* – Version 1.7.5. Ένα γραφικό περιβάλλον που συνδεόταν με τη βάση σαν client μέσα από το οποίο γινόταν πιο φιλικός ο χειρισμός ης βάσης μας.

Η βάση μας αποτελείται από τρία μέρη που περιγράφονται αμέσως μετά:

ΠΡΩΤΟ ΜΕΡΟΣ:

Περιλαμβάνει το υπό εξέταση **δείγμα** (όνομα επώνυμο, περιοχή ασφάλιση), καθώς και κάποια άλλα στοιχεία (Δυσκοιλιότητα, Καφές, Ούρηση, Εγχειρήσεις, Ασφάλιση). Τα στοιχεία του πίνακα αυτού είναι ένα id auto_increment, το οποίο δηλαδή αριθμεί αυτόματα τα νεοεισαγχθέντα στοιχεία. Στο δείγμα, το στοιχείο περιοχή, δηλώνεται ως ακέραιος που αντιστοιχεί στο πεδίο περιοχή όπως αυτό έχει οριστεί σε ξεχωριστό πίνακα.

ΔΕΥΤΕΡΟ ΜΕΡΟΣ:

Σε ένα πίνακα με το όνομα **παθήσεις** περιλαμβάνονται όλα τα ονόματα των ασθενειών. (Νευρολογικές, Νευροψυχολογικές, Ψυχικές). Ο ορισμός του περιλαμβάνει τα όνομα πάθησης και id πάθησης.

Στον επόμενο πίνακα κρατούνται στοιχεία που έχουν να κάνουν με όλες τις **ενδείξεις** της κατάστασης τους δείγματος. Περιλαμβάνει ονομαστικά για ποια ένδειξη πρόκειται καθώς και το id της.

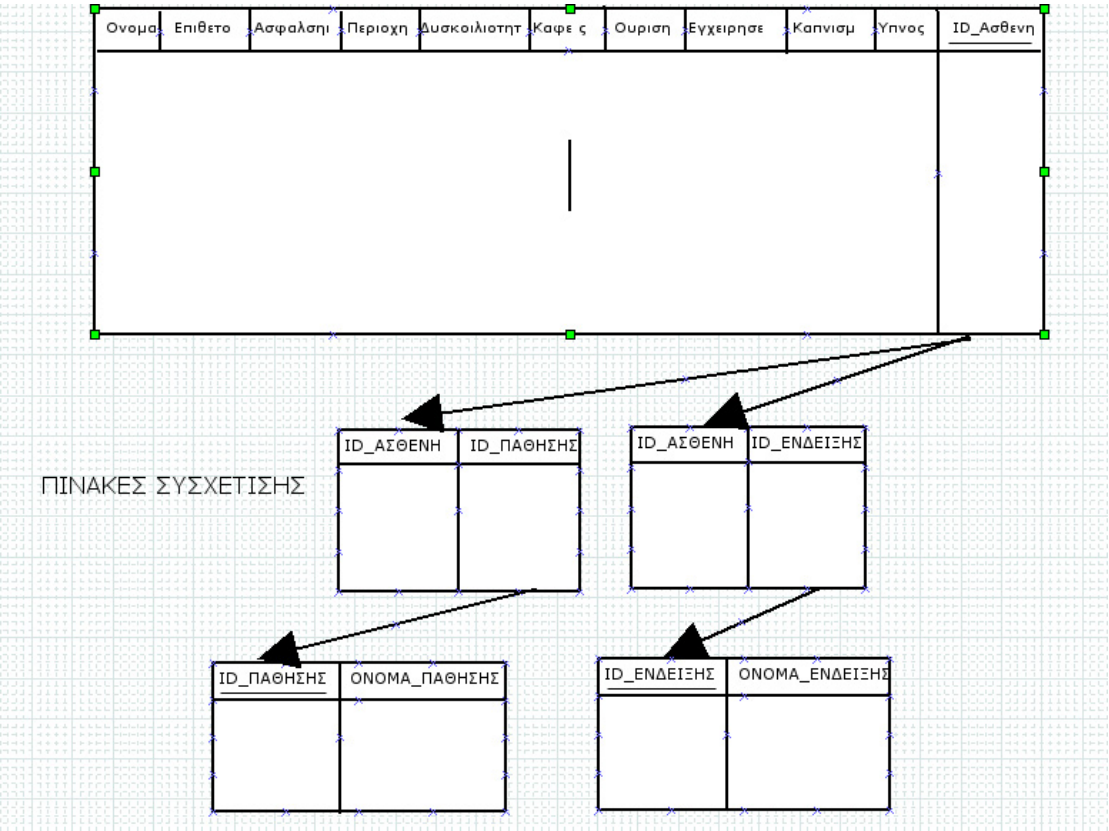
Τα στοιχεία της περιοχής αποθηκεύονται σε ένα άλλο πίνακα περισσότερο βοηθητικό. Τον **πίνακα "Περιοχές"** (όνομα περιοχής, id περιοχής). Ουσιαστικά ο πίνακας αυτός δεν χρησιμοποιείται κάπου. Απλά τα id κάθε περιοχής που βρίσκονται και σαν στοιχείο στο δείγμα, δηλώνουν την περιοχή από την οποία κατάγεται ο κάθε εξεταζόμενος.

Τέλος υπάρχει ο **πίνακας "Authorization"** που καταχωρούνται τα στοιχεία των εξουσιοδοτημένων χρηστών. Το Όνομα Χρήστη (Username) ο Κωδικός Πρόσβασης (Password) καθώς και ένα id που μετρά αυτόματα όσους καταχωρούνται.

ΤΡΙΤΟ ΜΕΡΟΣ (ΠΙΝΑΚΕΣ ΣΥΣΧΕΤΙΣΗΣ):

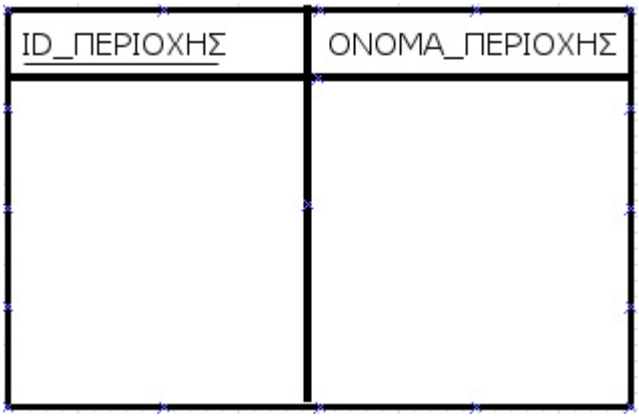
Για να συνδεθεί το κομμάτι του δείγματος με τα στοιχεία των παθήσεων και των ενδείξεων από το δεύτερο κομμάτι με το δείγμα, πρέπει να υπάρξει μια κάποιου είδους συσχέτιση με βάση τα id's των διαφόρων στοιχείων. Έτσι, έχουμε τον 1.**πίνακα συσχέτισης του δείγματος με τις παθήσεις (μέσω της συσχέτισης id ασθενή – id πάθησης)**, τον 2. **πίνακα συσχέτισης του δείγματος με τις ενδείξεις (id ασθενή – id ένδειξης).**

Το σχήμα (schema) της βάσης με βάση και τα παραπάνω στοιχεία ακολουθεί αμέσως (είναι υπογραμμισμένα τα πεδία που αποτελούν Primary Keys για τους αντίστοιχους πίνακες.)

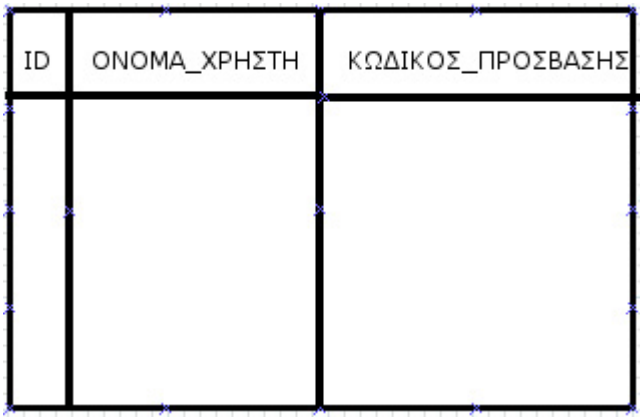


Σχήμα 14: Σχήμα της βάσης δεδομένων μας.

Οι επιπλέον δυο πίνακες που αναφέρονται στο δεύτερο μέρος (Περιοχές, Authorization) φαίνονται παρακάτω:



Σχήμα 15: Πίνακας "Περιοχές".

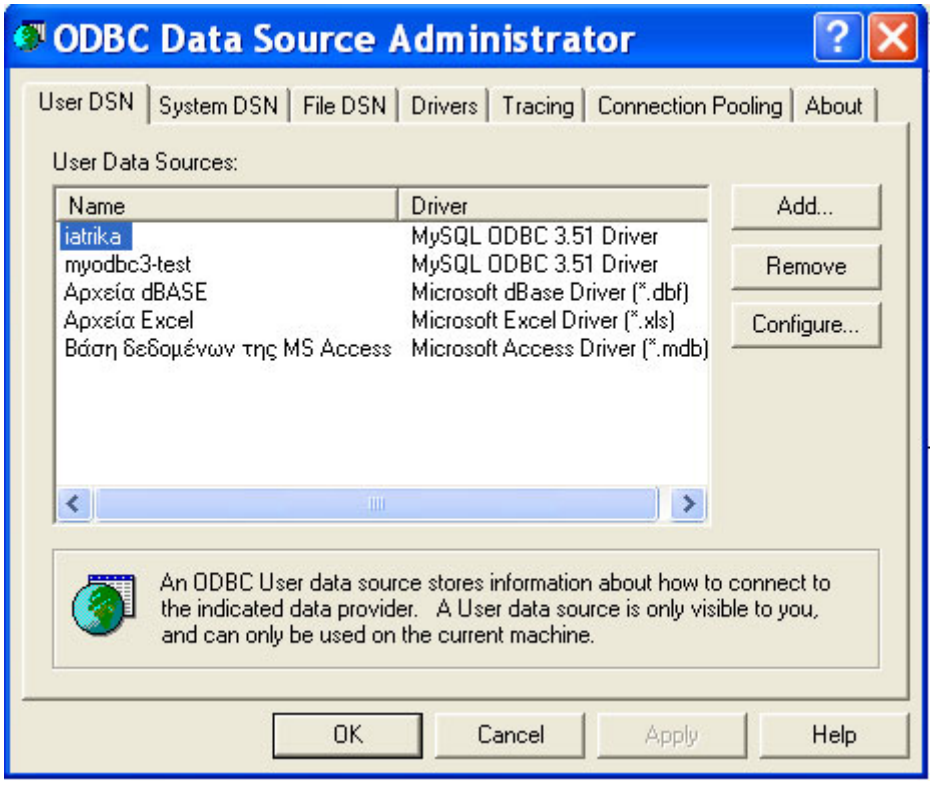


Σχήμα 16: Πίνακας "Authorization"..

6.2. Ρύθμιση παραμέτρων για τον ODBC Driver.

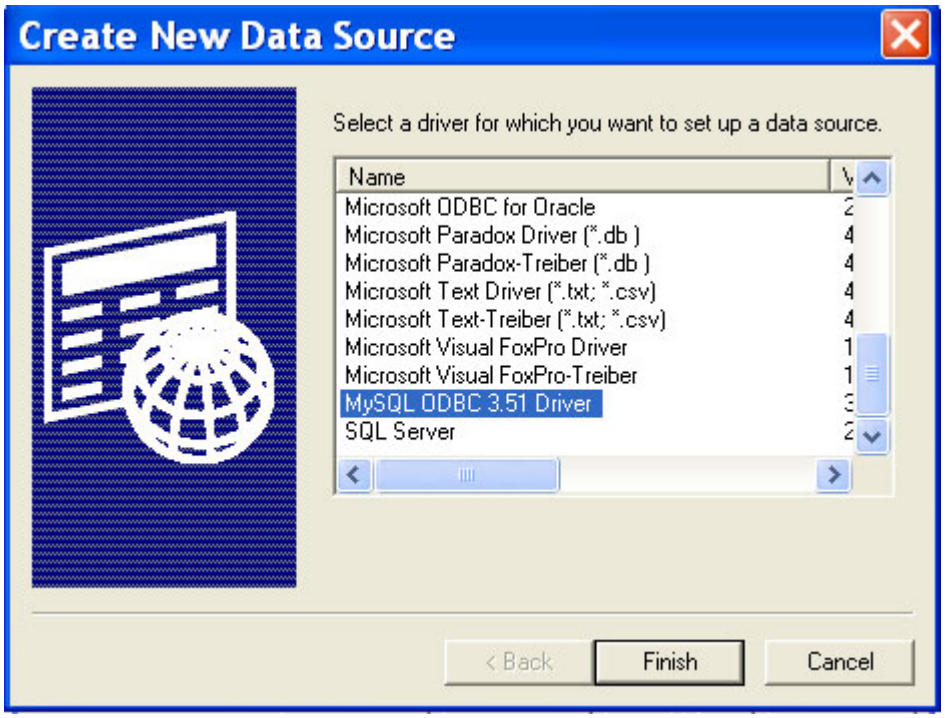
Όπως προαναφέρθηκε η σύνδεση με τη βάση δεδομένων είναι απαραίτητη και γίνεται μέσω του προγράμματος οδήγησης της βάσης δεδομένων. Ως πρόγραμμα οδήγησης χρησιμοποιήθηκε ο ODBC Driver. Τα βήματα της διαδικασίας εγκατάστασης – ρύθμισης παραμέτρων περιγράφονται αναλυτικά παρακάτω. Αρχικά λοιπόν εγκαθιστούμε στον υπολογιστή τον Driver ODBC (ODBC 3.51 Driver)[xxxiv]

Ρυθμίζουμε τις παραμέτρους του ODBC driver μέσα από τα administrative tools των Windows που βρίσκονται στον πίνακα ελέγχου. Εκεί επιλέγουμε Data Sources και βλέπουμε:



Σχήμα 17: Περιβάλλον διαχείρισης για τον ODBC Driver.

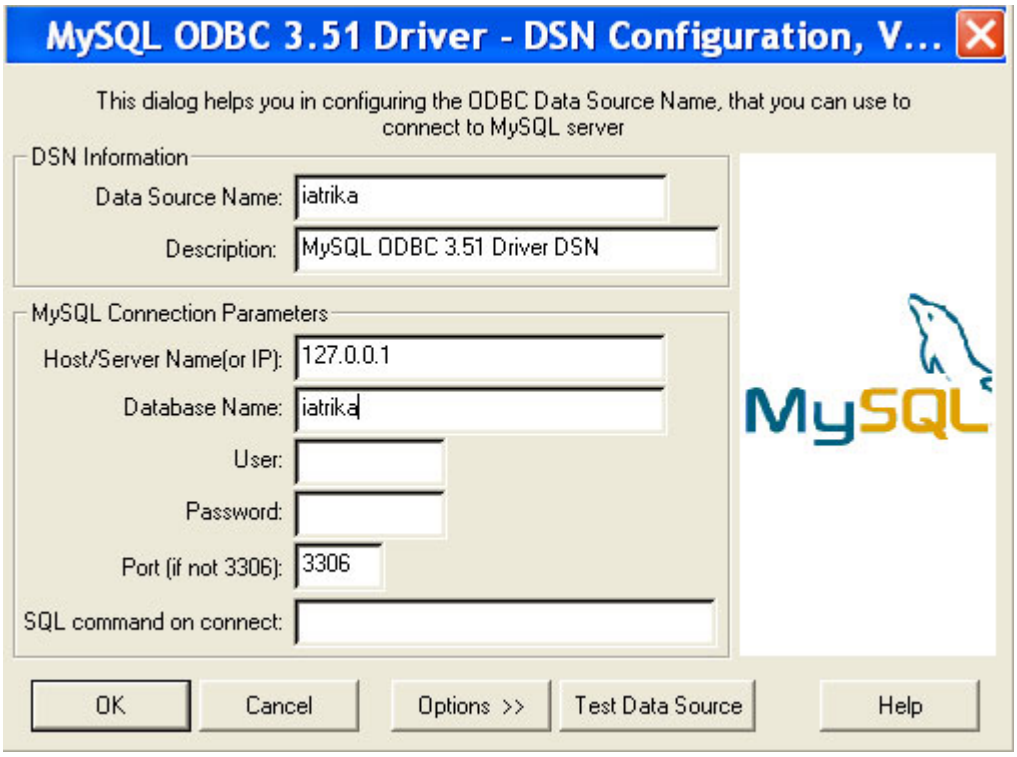
Αφού επιλέγουμε *add* βλέπουμε τα παρακάτω:



Σχήμα 18: Επιλογή νέας πηγής δεδομένων.

Επιλέγουμε τον driver μας από την διαθέσιμη λίστα και κατόπιν πατάμε *Finish*.

Στη συνέχεια ρυθμίζουμε τις πληροφορίες για το όνομα πηγής δεδομένων (Data Source Name) του ODBC που θα χρησιμοποιήσουμε για να συνδεθούμε στον My SQL Server. Πληροφορίες για το όνομα πηγής δεδομένων (όνομα βάσης και περιγραφή του driver) και στη συνέχεια τις παραμέτρους σύνδεσης για την MySQL την IP διεύθυνση του MySQL Server (127.0.0.1) καθώς και το όνομα της βάσης (iatrika), όπως φαίνεται ση συνέχεια:



Σχήμα 19: Επιλογή νέας πηγής δεδομένων.

Πατώντας *Test data source* βλέπουμε το μήνυμα:

Σχήμα 20: Μήνυμα για την επιτυχή σύνδεση με τη βάση δεδομένων

6.3. Εγκατάσταση του IIS σε περιβάλλον Windows XP Professional και τρέξιμο της πρώτης ASP σελίδας μας.

Βάζουμε το CD του λειτουργικού και πηγαίνουμε **Start→Settings→Control Panel**. Εκεί επιλέγουμε **Add/Remove Programs** και στο παράθυρο που εμφανίζεται **Add/Remove Windows Components**. Επιλέγουμε **Internet Information Services** και πατάμε **ok**. Δημιουργείται ένα αρχείο **InetPub** στο σκληρό μας δίσκο. Το ανοίγουμε και βρίσκουμε το φάκελο **wwwroot**. Κάνουμε Create New Folder στο wwwroot (πχ My Web). Φτιάχνουμε ένα κομμάτι απλού κώδικα σε ASP όπως φαίνεται παρακάτω και τον σώζουμε στο αρχείο **test1.asp** μέσα στο My Web φάκελο. Το παρακάτω πρόγραμμα εμφανίζει πέντε φορές την ημερομηνία και την ώρα διαχωριζόμενες από ένα κενό.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<title>Untitled Document</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-
8859-7">

</head>
<body>
<%
for R=1 to 5
        for F=1 to 5
              Response.Write "Date:" & Date
              Response.Write "Time:" & Time
        next
Response.Write vbCrLf
next
 %>
</body>
</html>
```

Εξασφαλίζουμε ότι ο Web Server τρέχει. Η κατάσταση στην οποία αυτός βρίσκεται μπορεί να ελεγχθεί πηγαίνοντας **Control Panel→Administrative Tools** και κάνουμε διπλό κλικ στην ένδειξη **IIS Manager**. Τέλος ανοίγουμε το πρόγραμμα πλοήγησης μας (Web

Browser) και πληκτρολογούμε **http://localhost/MyWeb/test1.asp**, για να δούμε το αποτέλεσμα που παρουσιάζει η πρώτη μας ASP σελίδα.

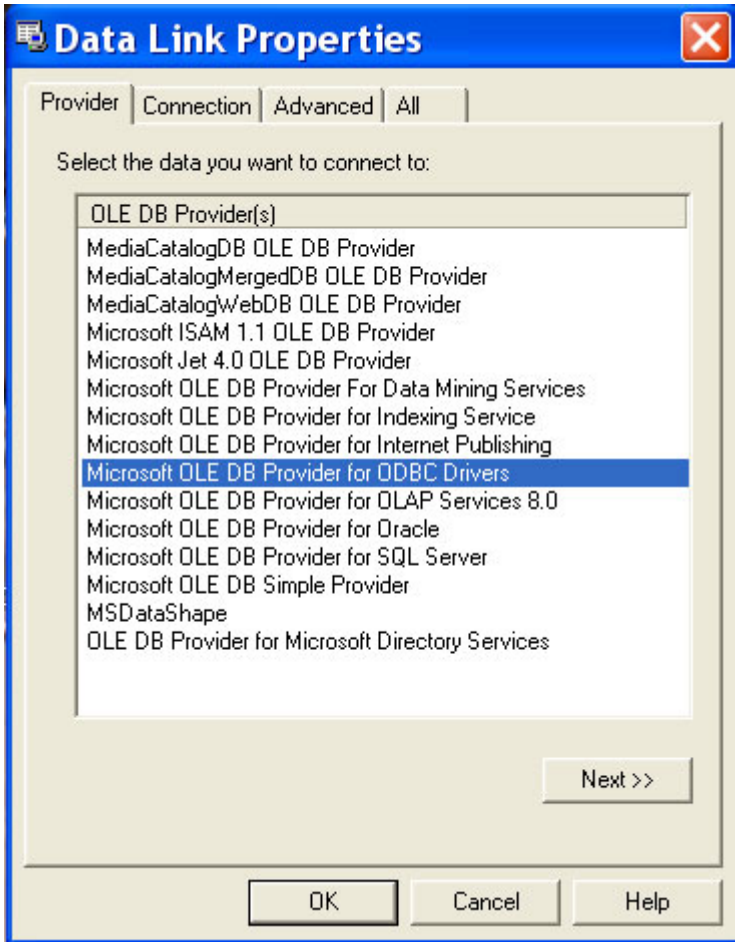
6.4. Σύνδεση με τον εξυπηρετητή της βάσης δεδομένων μέσω της ASP.

Μέσω της ASP όπως είπαμε, μπορούμε να διαχειριστούμε τη βάση δεδομένων. Για να επιτευχθεί αυτό, χρειάζεται συγκεκριμένος κώδικας ο οποίος περιλαμβάνει τα στοιχεία που εδράζεται η βάση μας. Ο κώδικας αυτός περιλαμβάνεται στις ASP σελίδες και τρέχει μόλις ο Web Server (IIS) τις τρέχει. Με αυτό τον τρόπο συνδεόμαστε με τη βάση μας. Για να επιτευχθεί αυτό ακολουθήσαμε την εξής διαδικασία:

Φτιάξαμε ένα αρχείο με προέκταση connection.udl και το τρέξαμε. Σκοπός ήταν να βρούμε τα στοιχεία που θα χρησιμοποιήσουμε στον κώδικά μας για την σύνδεση.

Η διαδικασία φαίνεται παρακάτω αναλυτικά:

Τρέχουμε το connection.udl αρχείο.



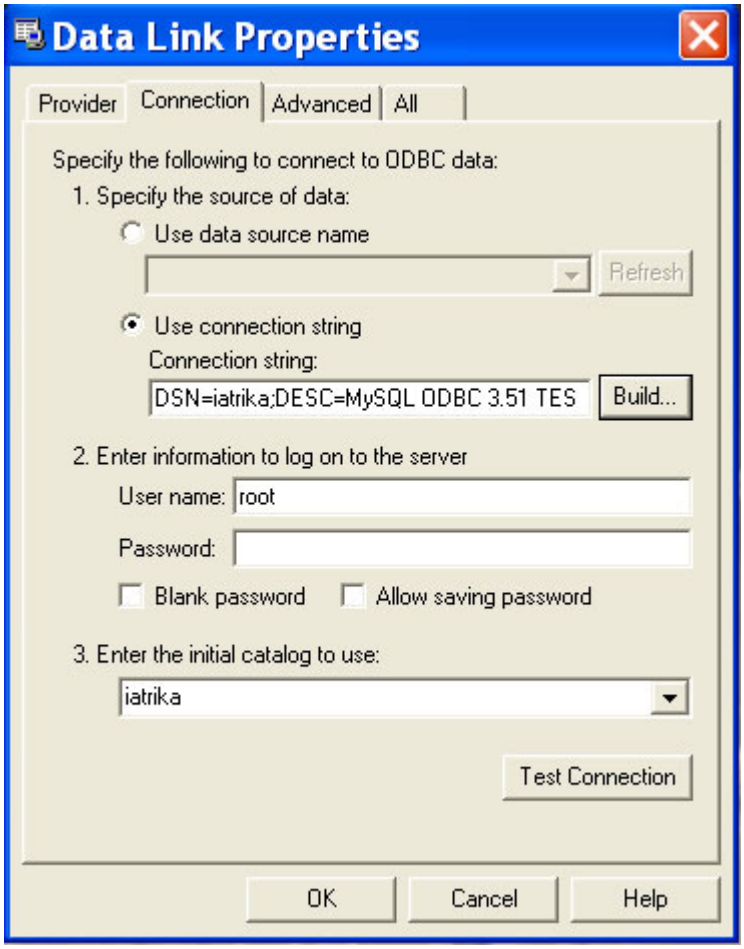
Σχήμα 21: Επιλογή νέας πηγής δεδομένων.

Στην παραπάνω φάση φαίνονται όλοι οι παροχείς (providers) που υπάρχουν στον υπολογιστή μας. Επιλέγουμε Microsoft OLE DB Provider for ODBC Drivers και στη συνέχεια την επιλογή next.

Ορίζουμε το όνομα της βάσης μας (iatrika). Στην καρτέλα connectionstring φαίνεται το connectionstring το οποίο χρησιμοποιείται στην ASP για να συνδέομαι με τη βάση δεδομένων στον δικτυακό προγραμματισμό και είναι το:

```
    DRIVER= {MySQL ODBC 3.51 Driver} ; DESC=; DATABASE=iatrika;
SERVER=127.0.0.1; UID=; PASSWORD=; PORT=; OPTION=; STMT=;
```

Στον παραπάνω κώδικα ορίζεται ο τύπος του driver που χρησιμοποιούμε (MySQL ODBC 3.51), το όνομα της βάσης (iatrika), η ip του Web Server (127.0.0.1) με βάση την ρύθμιση των παραμέτρων του ODBC driver έτσι όπως περιγράφηκε πριν.



Σχήμα 22: Επιλογή νέας πηγής δεδομένων.

Κάνοντας Test Connection διαπιστώνουμε ότι η βάση μας έχει επιτυχώς συνδεθεί!

Μετά από αυτό το test ο κώδικας σε ASP (χρησιμοποιώντας το connectionstring που έχουμε) ο οποίος εξασφαλίζει τη σύνδεση είναι ο εξής:

```
<?xml version="1.0" encoding="iso-8859-7"?>
<!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">

<head>
<title> Connection attempt</title>

<meta http-equiv="Content-Type" content="text/html; charset=iso-
8859-7" />
</head>

<body>
<!-- #include File="adovbs.inc" -->
<% dim conn
set conn=server.createobject ("ADODB.connection")
conn.mode = admodereadwrite
conn.connectionstring="DRIVER={MySQL ODBC 3.51 Driver};
DESC=;DATABASE=iatrika;SERVER=127.0.0.1;UID=;PASSWORD=;PORT=;OPTION=
;STMT=;"
conn.open %>

</body>
</html>
```

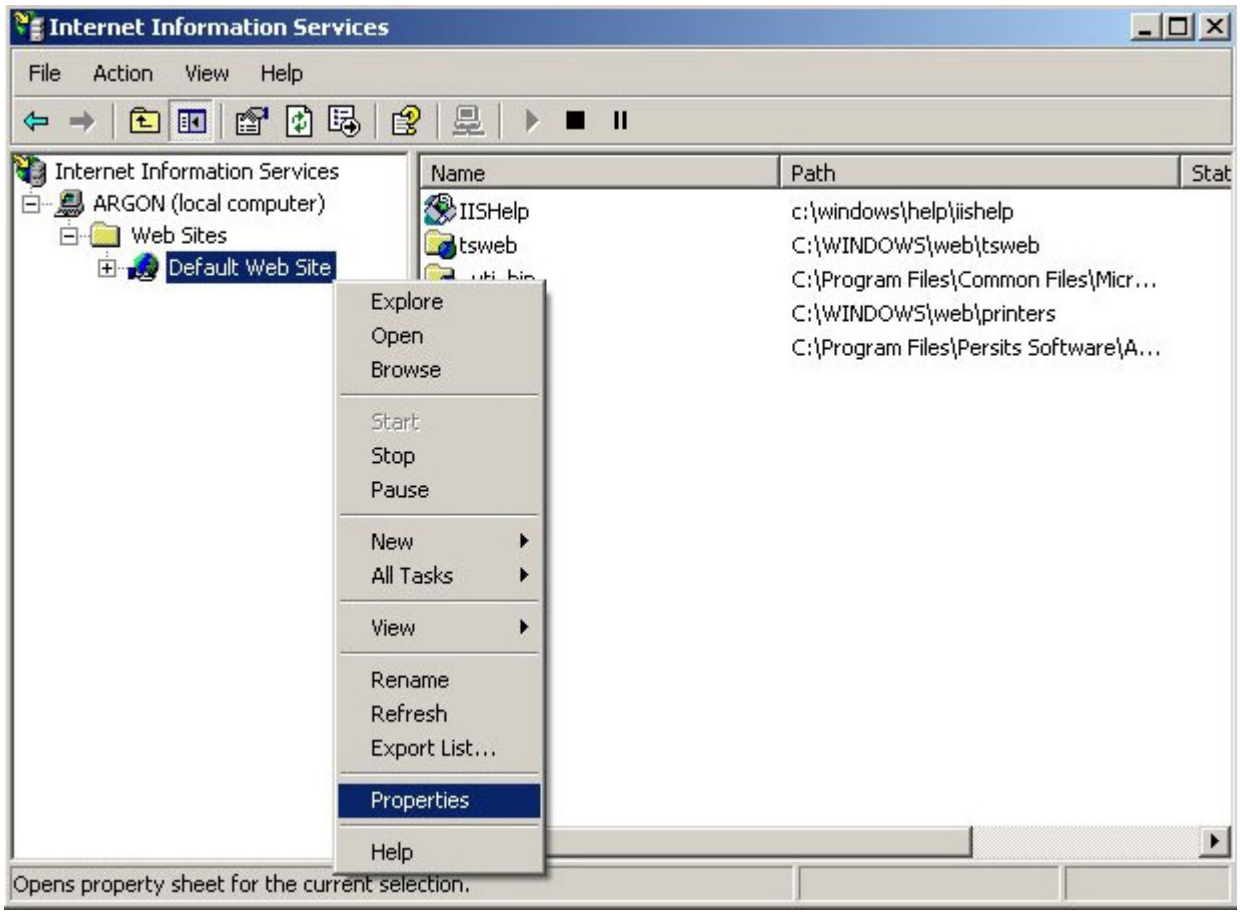
Ο παραπάνω κώδικας αποθηκεύτηκε δοκιμαστικά αρχικά στο αρχείο *conn.asp* το οποίο μπήκε μέσα στον IIS. Πράγματι η προσπάθεια που έγινε μέσα από τον inernet explorer πληκτρολογώντας τη διεύθυνση //localhost/conn.asp για να τρέξουμε το asp αρχείο που βρισκόταν μέσα στον IIS και περιείχε τον κώδικα σύνδεσης ήταν επιτυχής.

7. Δημιουργία ενός ιδιο- υπογεγραμμένου SSL πιστοποιητικού (SSL certificate) για τον IIS.

7.1. Δημιουργώντας μια αίτηση υπογραφής πιστοποιητικού.

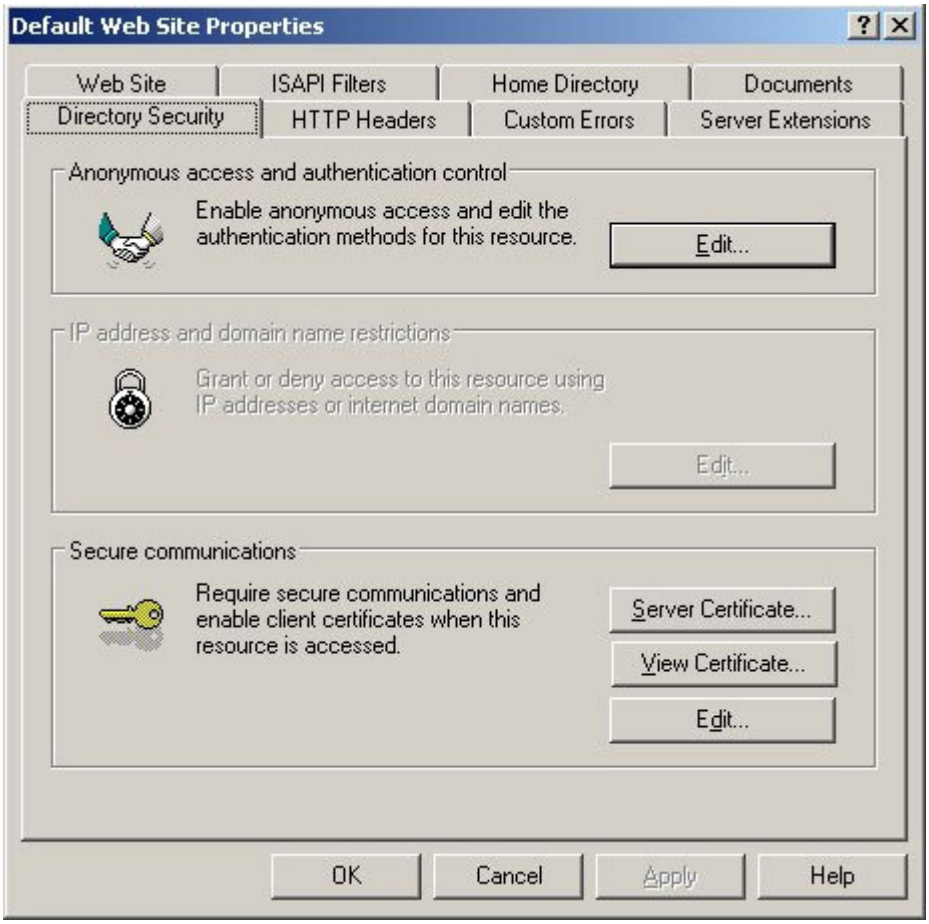
Παρακάτω φαίνονται αναλυτικά τα βήματα για την δημιουργία ενός ιδιο-υπογεγραμμένου SSL πιστοποιητικού για την πιστοποίηση του εξυπηρετητή. Σε πρώτη φάση λοιπόν δημιουργούμε μια αίτηση για υπογραφή ενός πιστοποιητικού μέσω του IIS οδηγού..

Ανοίγουμε τον πίνακα ελέγχου→εργαλεία διαχείρισης→IIS. Κάνουμε δεξί κλικ στην επιλογή Default Web Site→Properties.



Σχήμα 23: Κώδικας ASP για τη σύνδεση με τη βάση δεδομένων

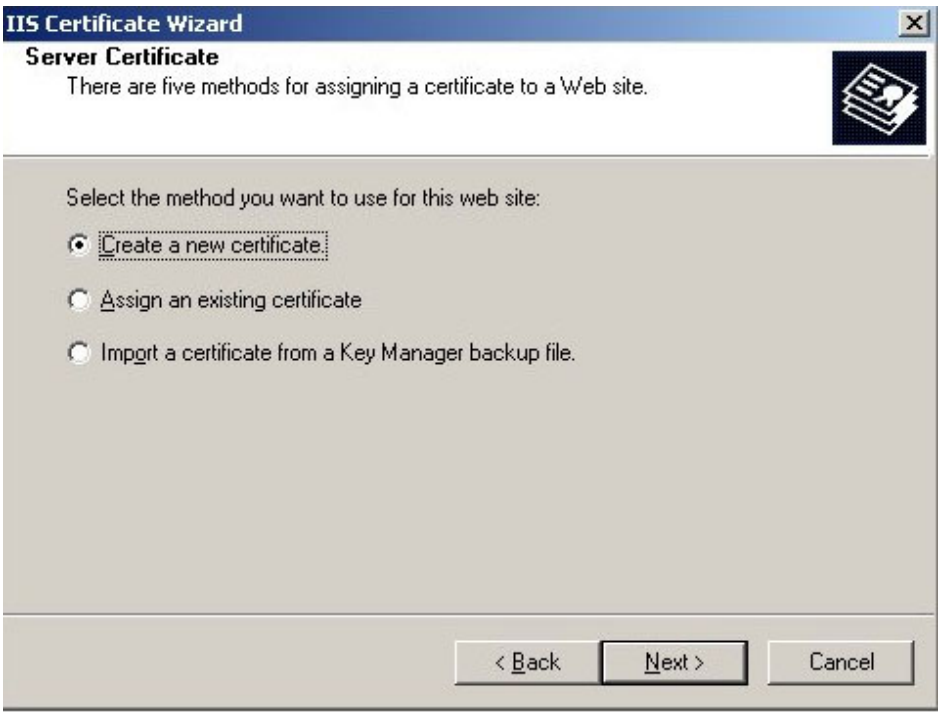
Το παράθυρο διαλόγου της επιλογής "properties" φαίνεται παρακάτω. Επιλέγουμε Directory Security (Ασφάλεια Φακέλου). Κάνοντας κλικ στην επιλογή Server Certificate εμφανίζεται ο οδηγός του Web Server.



Σχήμα 24: Καρτέλα για την επιλογή πιστοποιητικού εξυπηρετητή.

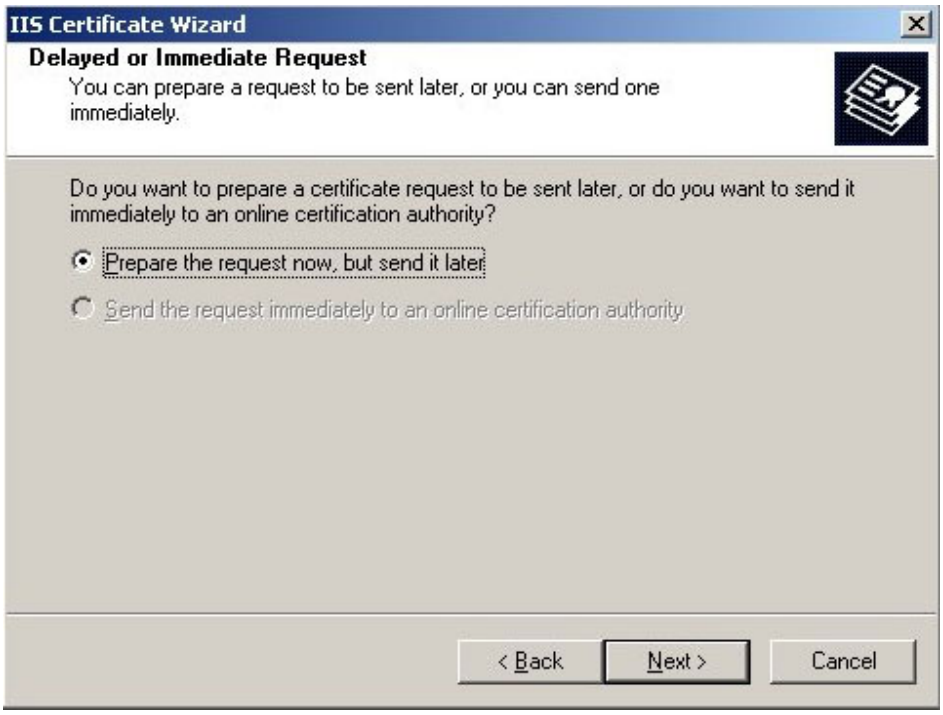
Σχήμα 25: Έναρξη οδηγού του IIS για το πιστοποιητικό εξυπηρετητή.

Επιλέγουμε Next. → Create New Certificate (Δημιουργία Νέου Πιστοποιητικού) και πάλι Next.



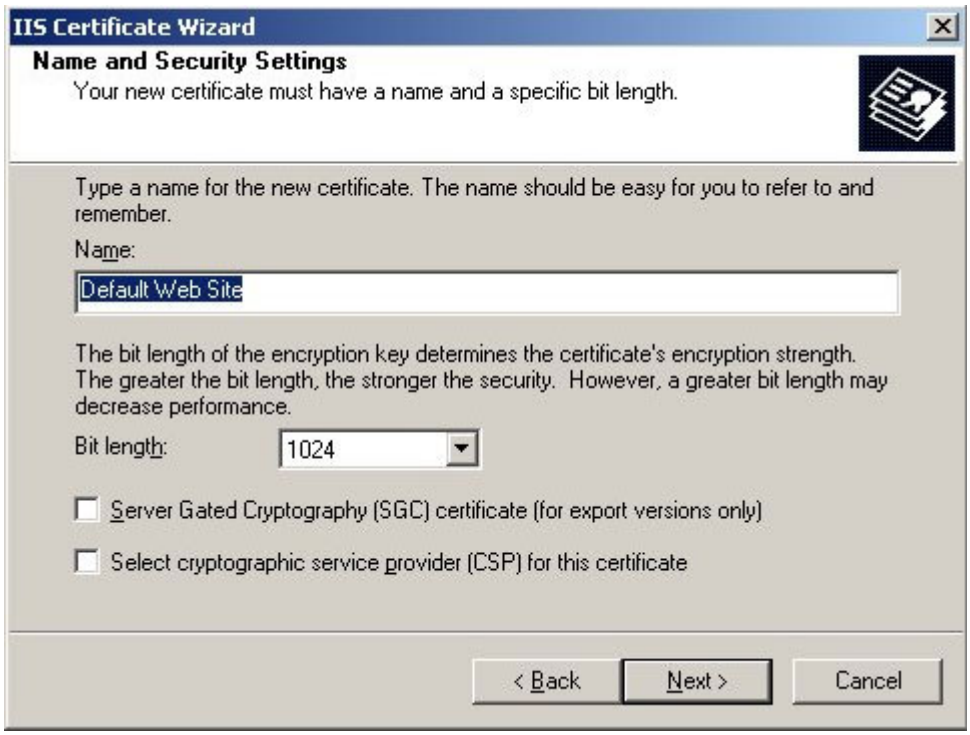
Σχήμα 26: Μέθοδος για assigning ένα πιστοποιητικό σε μια ιστοσελίδα.

Επιλέγουμε "Prepare the request now but send it later" (Ετοίμασε την αίτηση τώρα αλλά στείλε τη αργότερα). Επιλέγουμε Next.



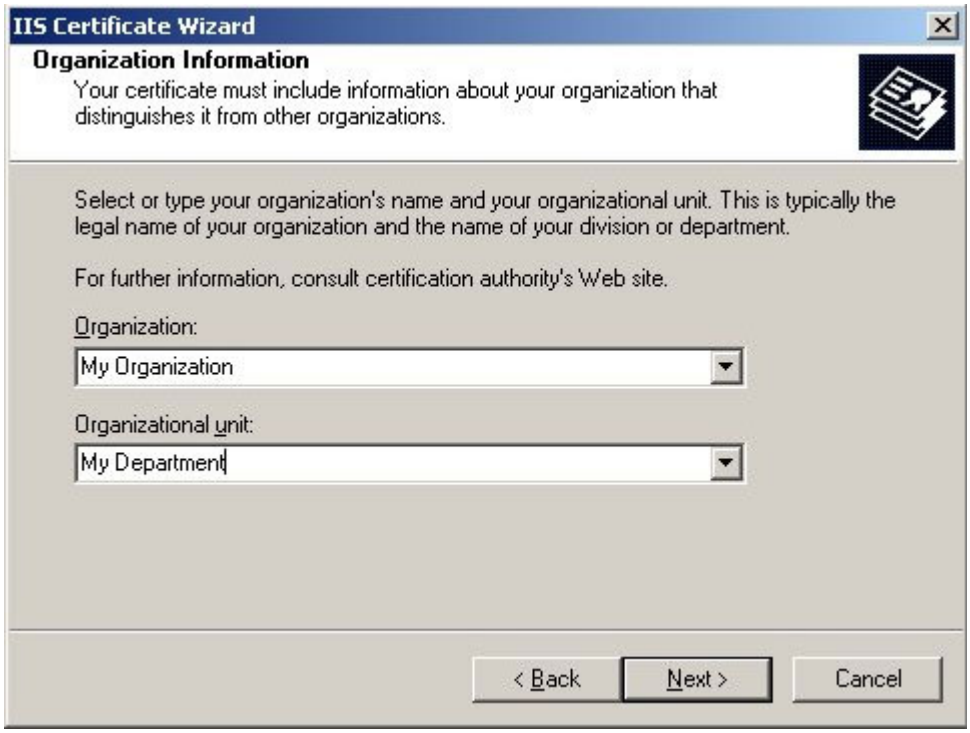
Σχήμα 27: Ορισμός ετοιμασίας της αίτησης και στάλσιμό της αργότερα

Δίνουμε στο Πιστοποιητικό μας το όνομα που επιθυμούμε. Επίσης καθορίζουμε το μήκος του bit (bit length) το οποίο καθορίζει την ισχύ σε κρυπτογράφηση του πιστοποιητικού. Όσο μεγαλύτερο το μήκος του τόσο μεγαλύτερη η ασφάλειά μας. Εμείς επιλέγουμε για μήκος τα 1024 bit αφού μεγαλύτερο μήκος μπορεί να προκαλέσει προβλήματα στην παρουσίαση. Πατάμε *next*.



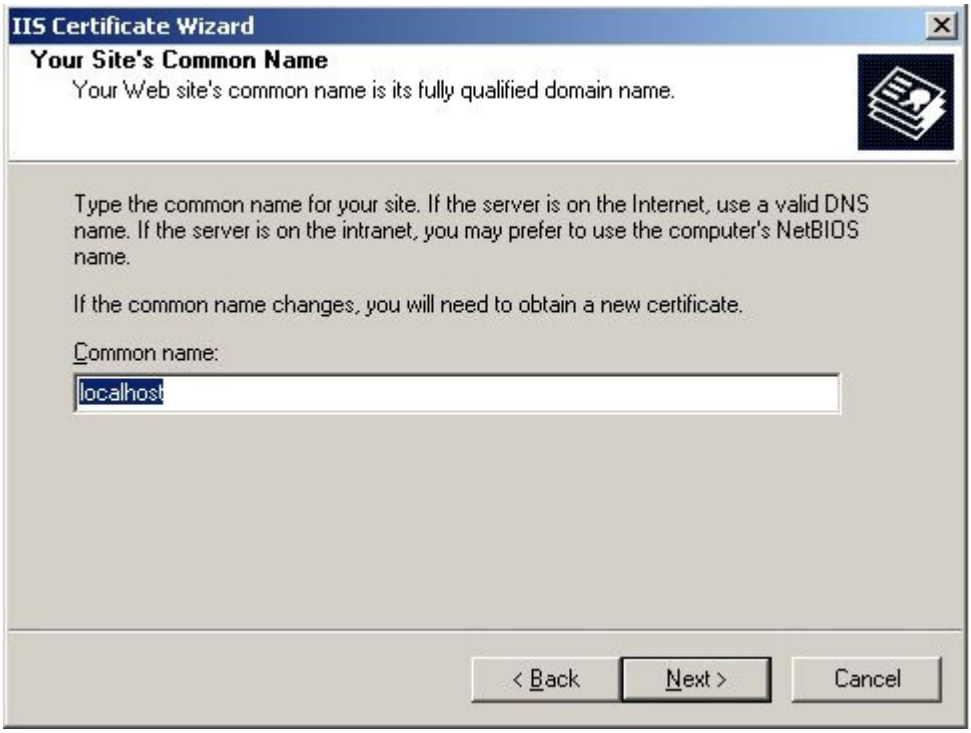
Σχήμα 28: Ορισμός ονόματος πιστοποιητικού καθώς και ορισμός μήκους κλειδιού κρυπτογράφησης.

Το επόμενο βήμα είναι να συμπληρώσουμε ορισμένα επιπλέον στοιχεία που θα περιέχονται στο πιστοποιητικό όπως τον οργανισμό στο οποίο ανήκουμε ή την εταιρία, το αντίστοιχο τμήμα στο οποίο θα εκδοθεί το πιστοποιητικό. Αυτό γίνεται για να διασφαλιστεί η μοναδικότητα του πιστοποιητικού μας, από άλλους οργανισμούς κτλ. Επιλέγουμε *Next*.



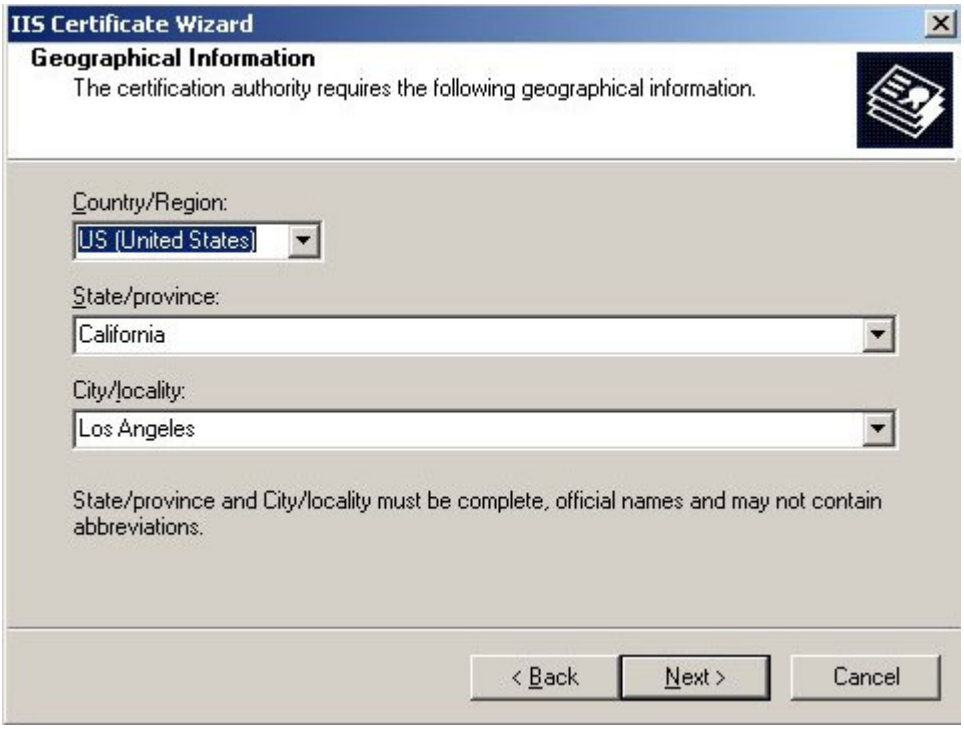
Σχήμα 29: Ορισμός πληροφοριών σχετικά με το νόμιμο όνομα και τμήμα του οργανισμού που ανήκει το πιστοποιητικό.

Το «κοινό όνομα» (Common Name) είναι η διεύθυνση της ιστοσελίδας μας την οποία το πιστοποιητικό πρόκειται να καλύψει. Χρειαζόμαστε ένα έγκυρο όνομα όταν πρόκειται για πρόσβαση μιας ιστοσελίδας που βρίσκεται στο διαδίκτυο (πχ www.mycompany.com). Στην περίπτωση όμως αυτή χρησιμοποιούμε εξυπηρετητή που βρίσκεται τοπικά στον υπολογιστή μας. Αυτό σημαίνει ότι θα έχουμε τοπική πρόσβαση και δεν υπάρχει κίνδυνος ασφάλειας, όμως μας ενδιαφέρει η προσομοίωση μιας τέτοιας περίπτωσης. Επομένως χρησιμοποιούμε όπως φαίνεται παρακάτω σαν κοινό όνομα το localhost. Κάνουμε κλικ στο *Next*.



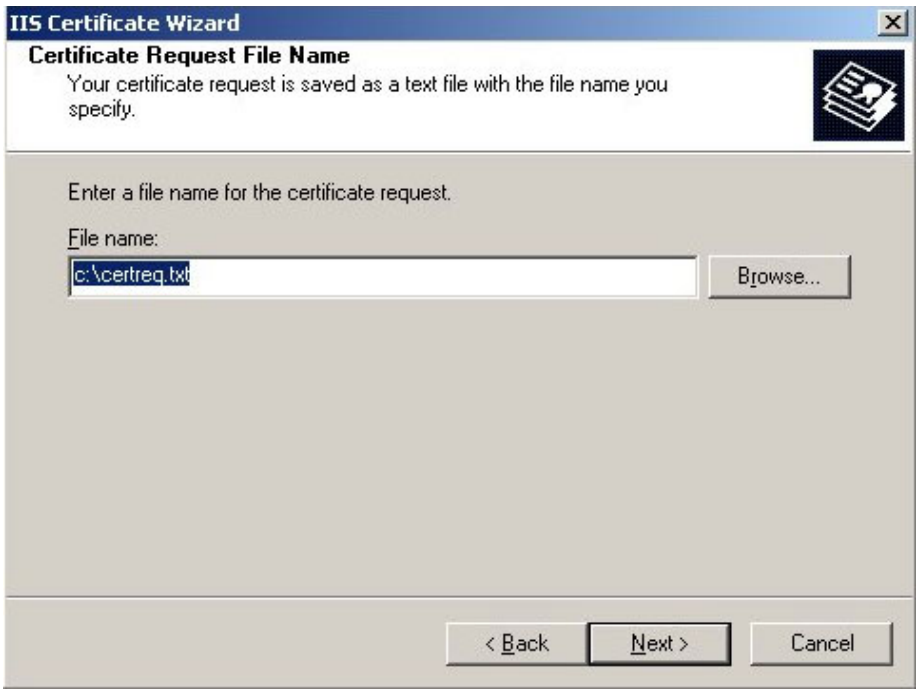
Σχήμα 30: Ορισμός κοινού ονόματος της ιστοσελίδας μας.

Σε αυτό το βήμα δηλώνουμε την τοποθεσία στην οποία βρίσκεται ο Server μας. Κάνουμε κλικ στο κουμπί *Next*.



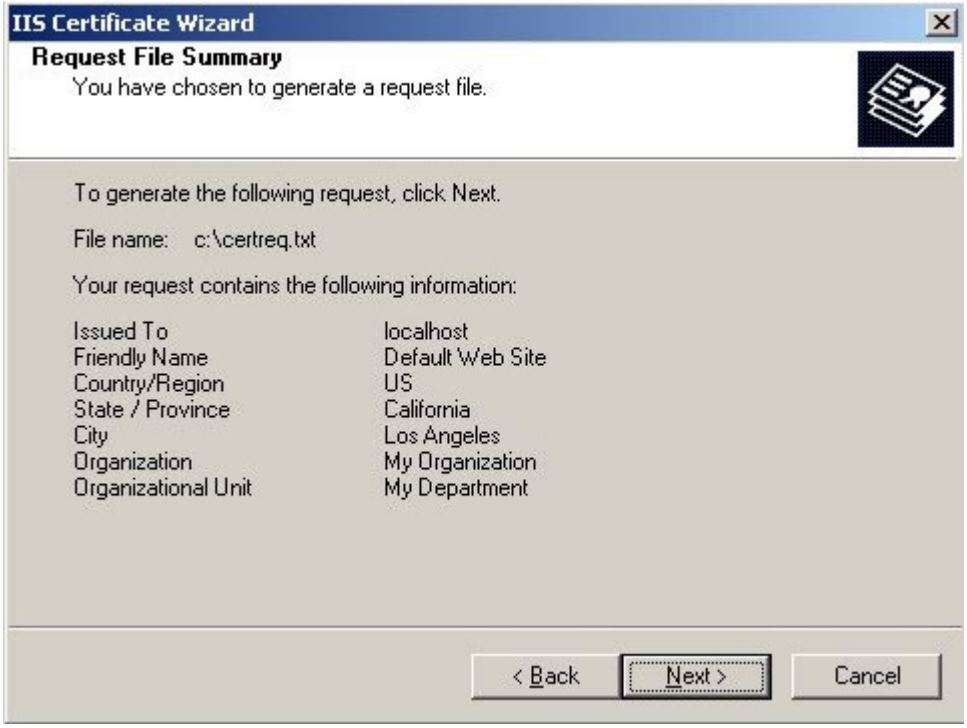
Σχήμα 31: Ορισμός γεωγραφικών πληροφοριών που απαιτούνται από την αρχή πιστοποίησης.

Βάζουμε ένα όνομα στο txt αρχείο που αναπαριστά την αίτηση για το πιστοποιητικό μας και πατάμε *Next*.



Σχήμα 32:Ονομασία της αίτησης για πιστοποιητικό.

Η επόμενη εικόνα δείχνει τα στοιχεία που θέλουμε να περιλαμβάνονται στο πιστοποιητικό μας. Κάνουμε κλικ στο κουμπί *Next*.



Σχήμα 33:Προεπισκόπηση της αίτησής μας.

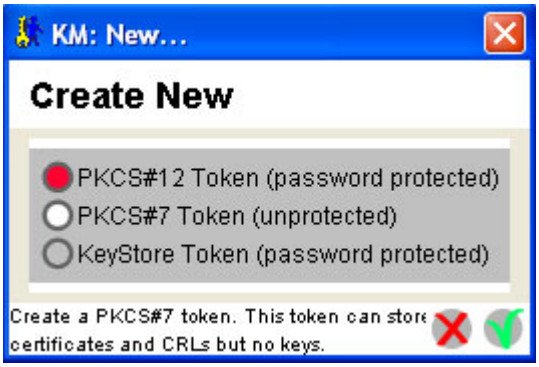
Έχουμε δημιουργήσει ήδη μια αίτηση για πιστοποιητικό. Κάνουμε κλικ στην επιλογή *Finish*.

Σχήμα 34: Τελικό βήμα για την ολοκλήρωση της αίτησής μας.

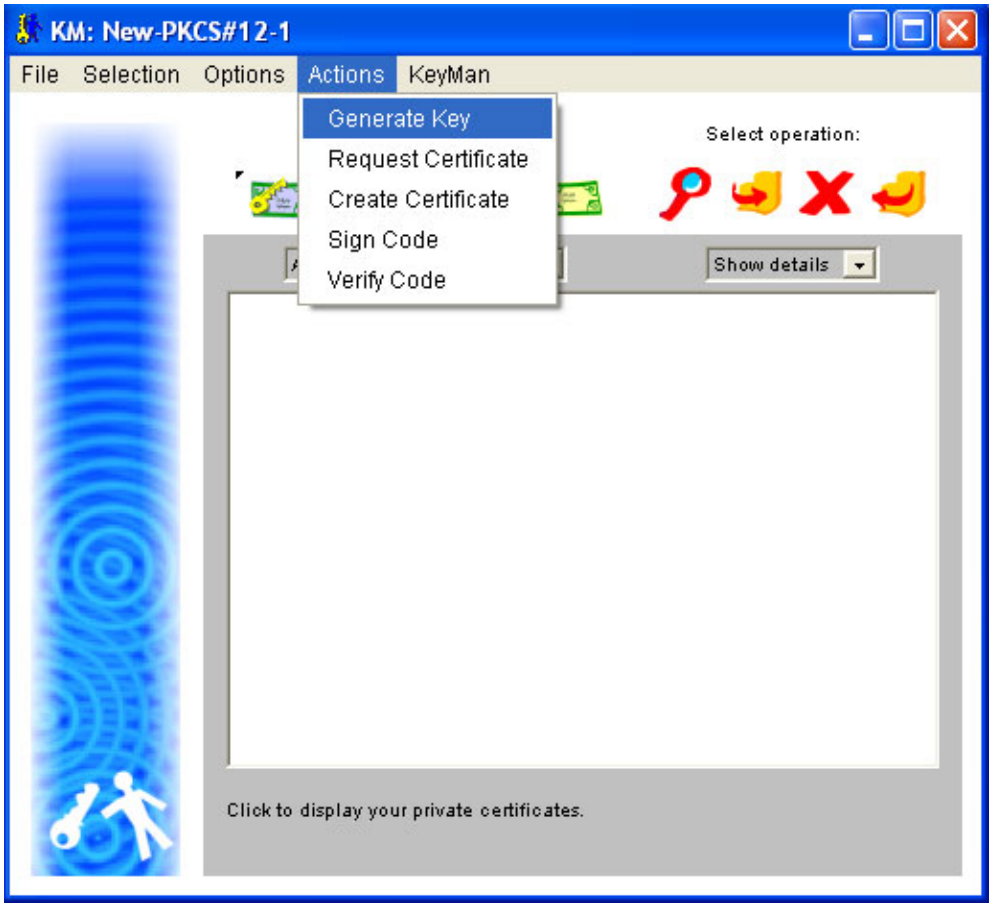
7.2. Δημιουργία και υπογραφή του πιστοποιητικού μας.

Για την υπογραφή του πιστοποιητικού μας χρησιμοποιήθηκε το πρόγραμμα την IBM KeyMan (version 1.60.000 by IBM Zurich Reseach Laboratory)[xxxv]. Αφού εγκαταστήσουμε το πρόγραμμα το τρέχουμε και επιλέγουμε ανάμεσα στις δυο επιλογές Create New.

Σχήμα 35: Δημιουργία και υπογραφή πιστοποιητικού – Βήμα 1.

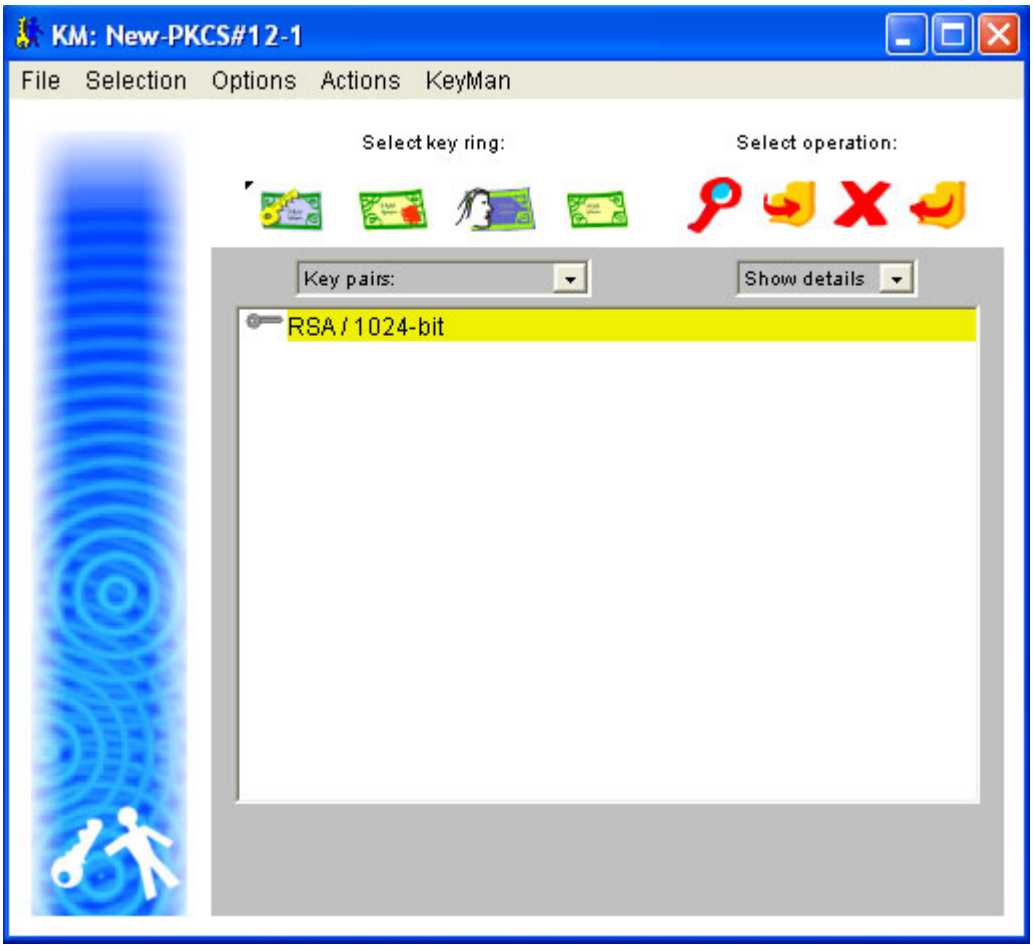


Σχήμα 36: Δημιουργία και υπογραφή πιστοποιητικού – Βήμα 2.



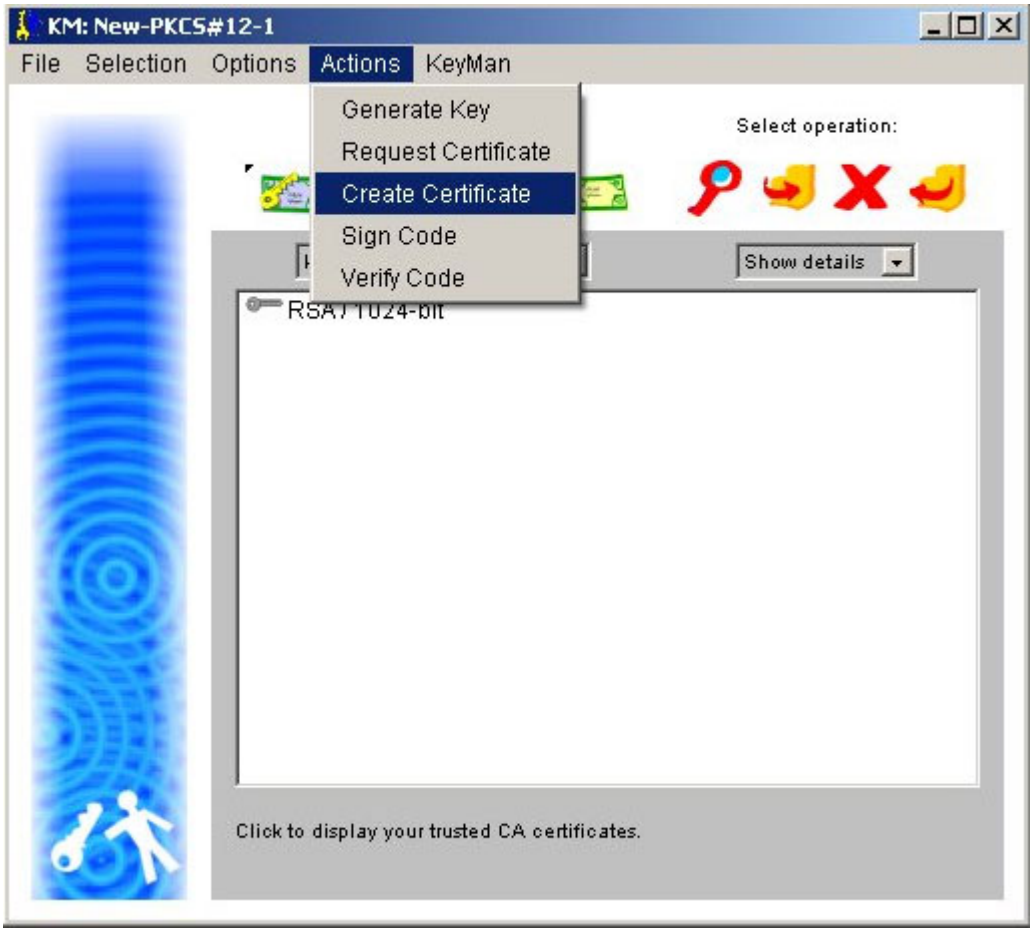
Σχήμα 37: Δημιουργία κλειδιού – Βήμα 3

Σχήμα 38: Ενεργοποίηση κλειδιού με τον αλγόριθμο κρυπτογράφησης RSA και μήκος κλειδιού 1024 bits – Βήμα 4.



Σχήμα 39:Μετά την ενεργοποίηση του κλειδιού φαίνεται το παραπάνω μήνυμα– Βήμα 5.

Επόμενο βήμα η δημιουργία παροχέα πιστοποιητικού. Αν δημιουργούσαμε μια πραγματική αίτηση υπογραφής δεν θα κάναμε αυτό το βήμα. Θα στέλναμε κατευθείαν την αίτηση υπογραφής σε μια αρχή πιστοποίησης. Επιλέγουμε το menu Actions και επιλέγουμε *Create Certificate*.



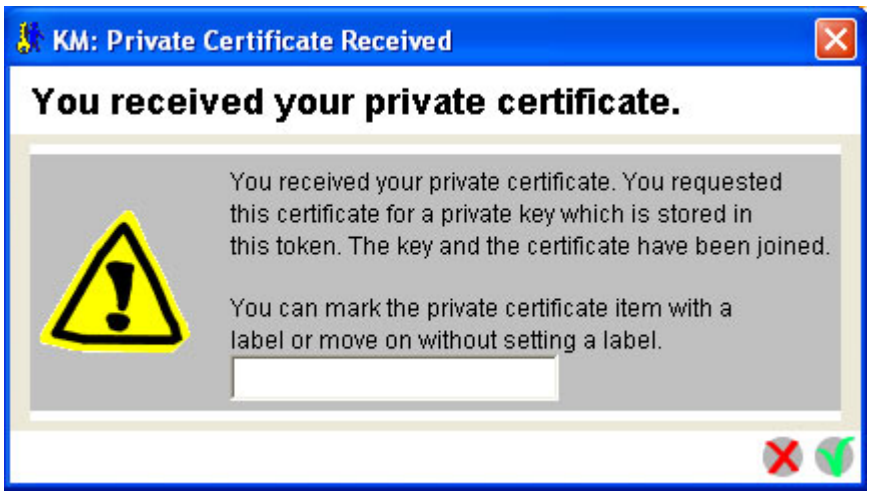
Σχήμα 40: Δημιουργία παροχέα πιστοποιητικού – Βήμα 6

Σχήμα 41: Ιδιο-υπογεγραμμένο πιστοποιητικό – Βήμα 7

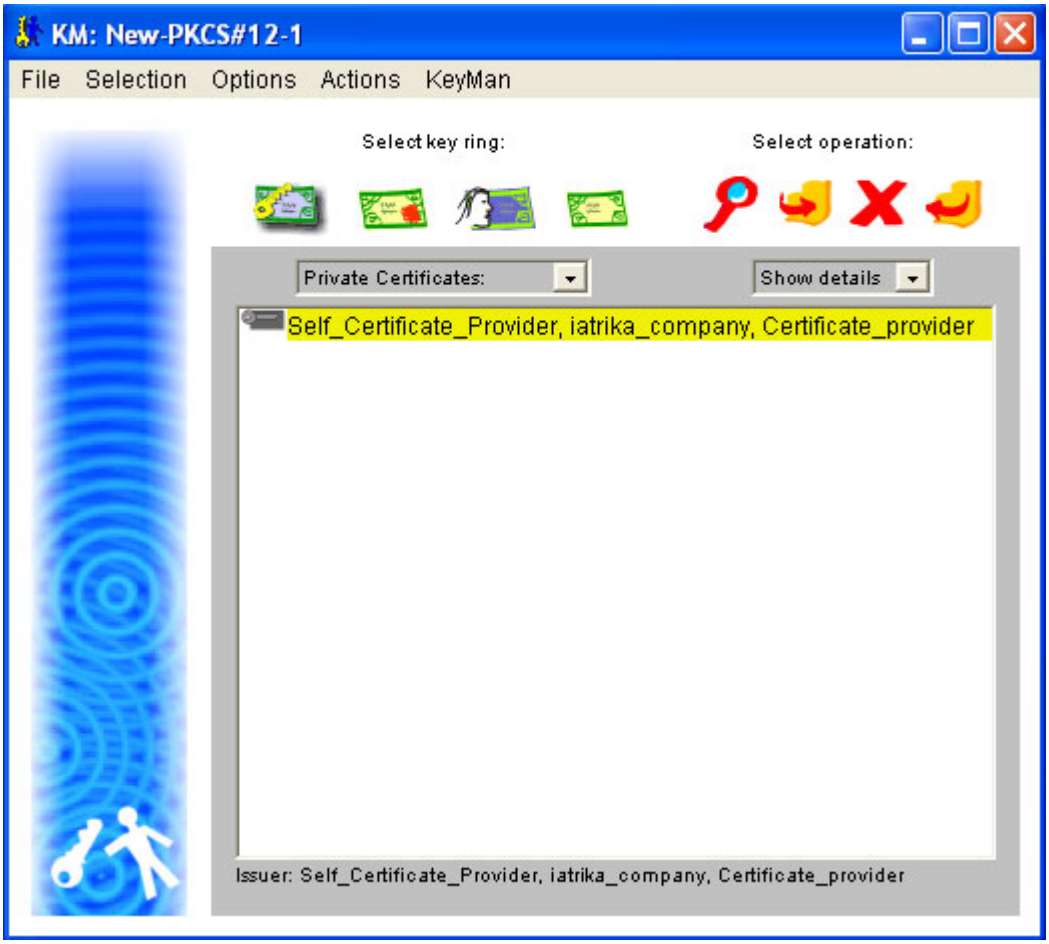
Στο επόμενο βήμα συμπληρώνουμε τιμές οι οποίες θα περιέχονται στο πιστοποιητικό μας, όπως το όνομά μας, την ημερομηνία λήξης του, την τοποθεσία στην οποία βρισκόμαστε κτλ.

Σχήμα 42: Στοιχεία πιστοποιητικού – Βήμα 8

Στο επόμενο βήμα ενημερωνόμαστε ότι λάβαμε το ιδιωτικό μας πιστοποιητικό μαζί με το ιδιωτικό μας κλειδί. Μπορούμε προαιρετικά να βάλουμε μια ετικέτα στο πιστοποιητικό μας. Προτιμούμε να αφήσουμε τον χώρο κενό.

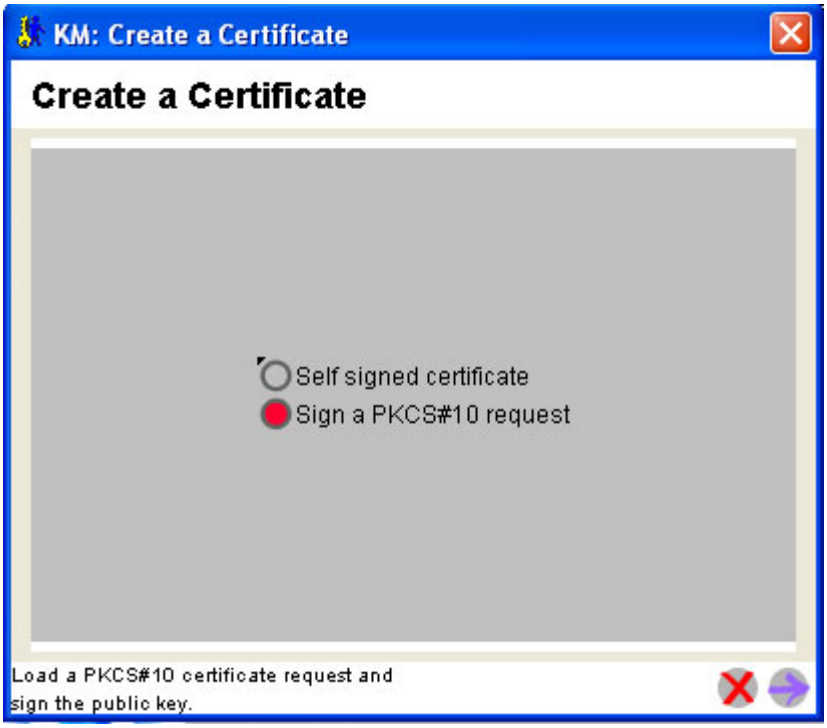


Σχήμα 43: Μήνυμα λήψης ιδιωτικού πιστοποιητικού και κλειδιού– Βήμα 9



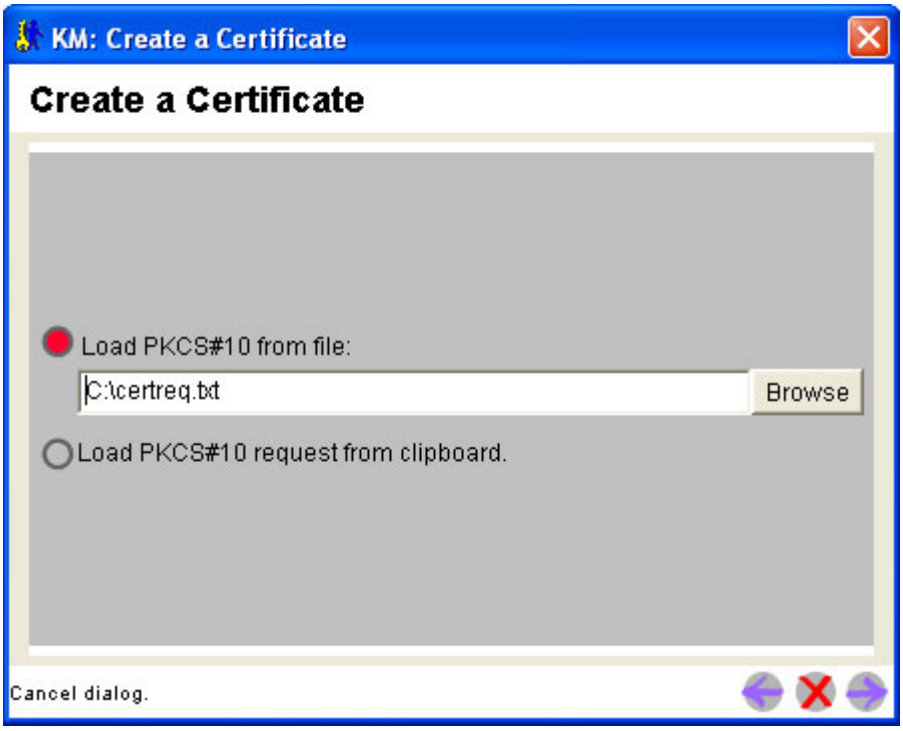
Σχήμα 44: Το πιστοποιητικό από τον παροχέα πιστοποίησης μας– Βήμα 10

Τώρα που έχουμε ένα πιστοποιητικό από μια αρχή πιστοποίησης καθώς και την αίτηση για υπογραφή μπορούμε ουσιαστικά να υπογράψουμε την αίτηση υπογραφής που κάναμε στον IIS. Επιλέγουμε το menu *Actions* και επιλέγουμε και πάλι την επιλογή *Create New Certificate* (βλ. Σχήμα 45). Εμφανίζεται η παρακάτω καρτέλα και αυτή τη φορά επιλέγουμε Sign a PKCS #10 request.



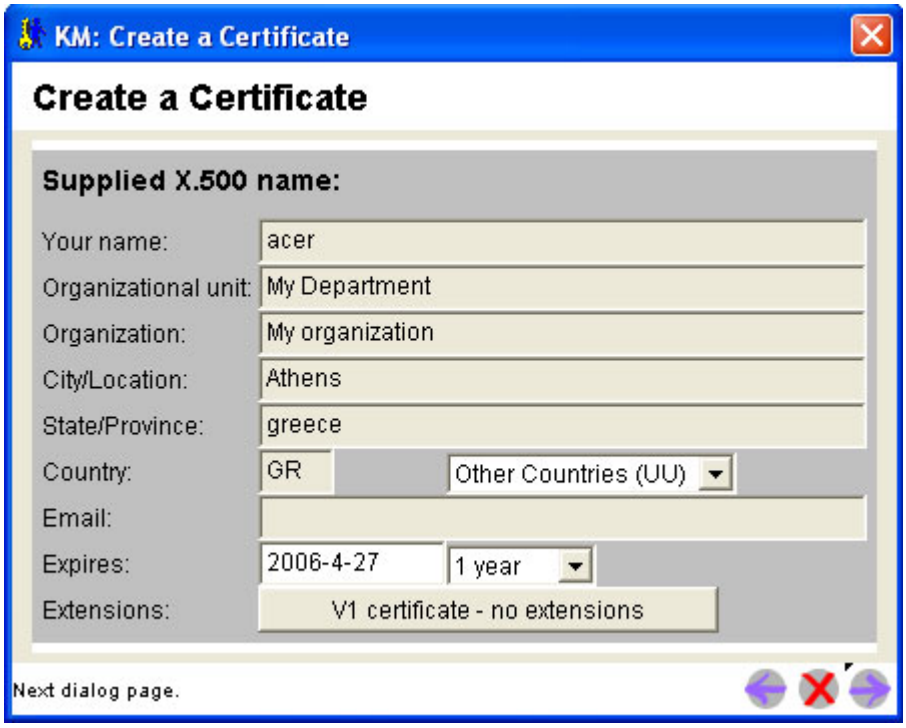
Σχήμα 45: Ενημέρωση για υπογραφή πιστοποιητικού– Βήμα 11

Η επόμενη κίνηση είναι η επιλογή *Load PKCS#10* όπου καθορίζουμε το μονοπάτι του αρχείου που περιέχει την αίτηση υπογραφής για το πιστοποιητικό μας. Στη συνέχεια επιλέγουμε *Next*.



Σχήμα 46: Καθορισμός μονοπατιού (path) αρχείου που περιέχει την αίτηση υπογραφής για το πιστοποιητικό– Βήμα 12.

Το Keyman διαβάζει τις πληροφορίες από το αρχείο της αίτησης και μας τις παρουσιάζει. Επιλέγουμε *Next*.



Σχήμα 47: Πληροφορίες από το αρχείο αίτησης του πιστοποιητικού– Βήμα 13

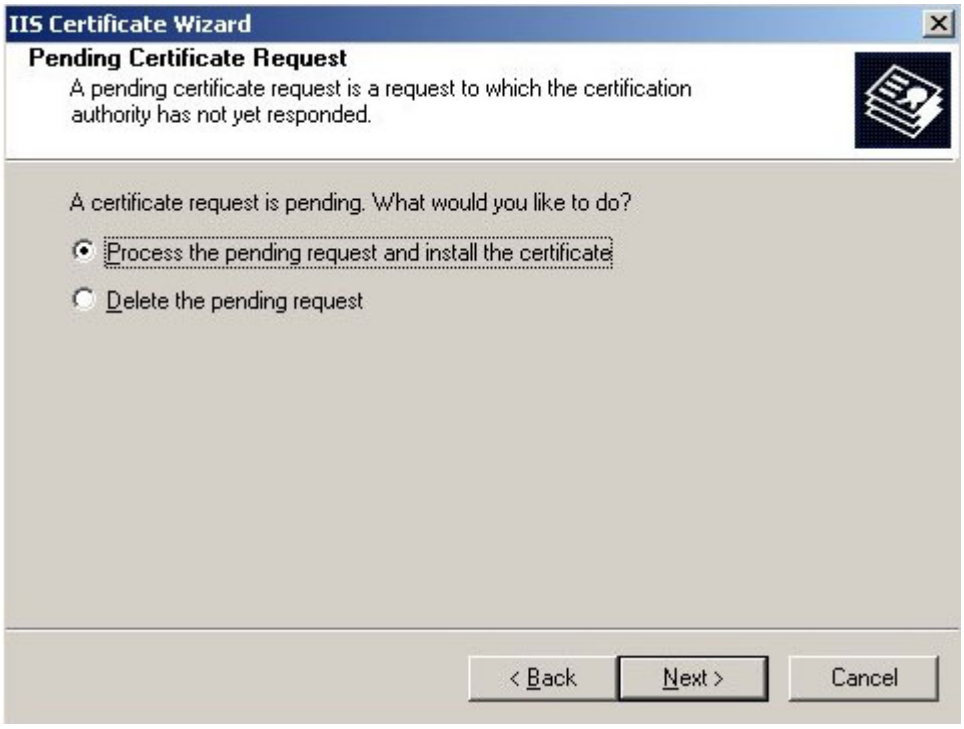
Επιλέγουμε *Save certificate to file* και καθορίζουμε το μονοπάτι και το όνομα για το υπογεγραμμένο πιστοποιητικό. Χρησιμοποιούμε την προέκταση *.cer* γιατί αυτή θα αναμένεται από τον IIS. Επιλέγουμε και πάλι *Next*.

Σχήμα 48: Αποθήκευση πιστοποιητικού– Βήμα 14

Τώρα είμαστε έτοιμοι να εγκαταστήσουμε το υπογεγραμμένο πιστοποιητικό μας στον IIS.

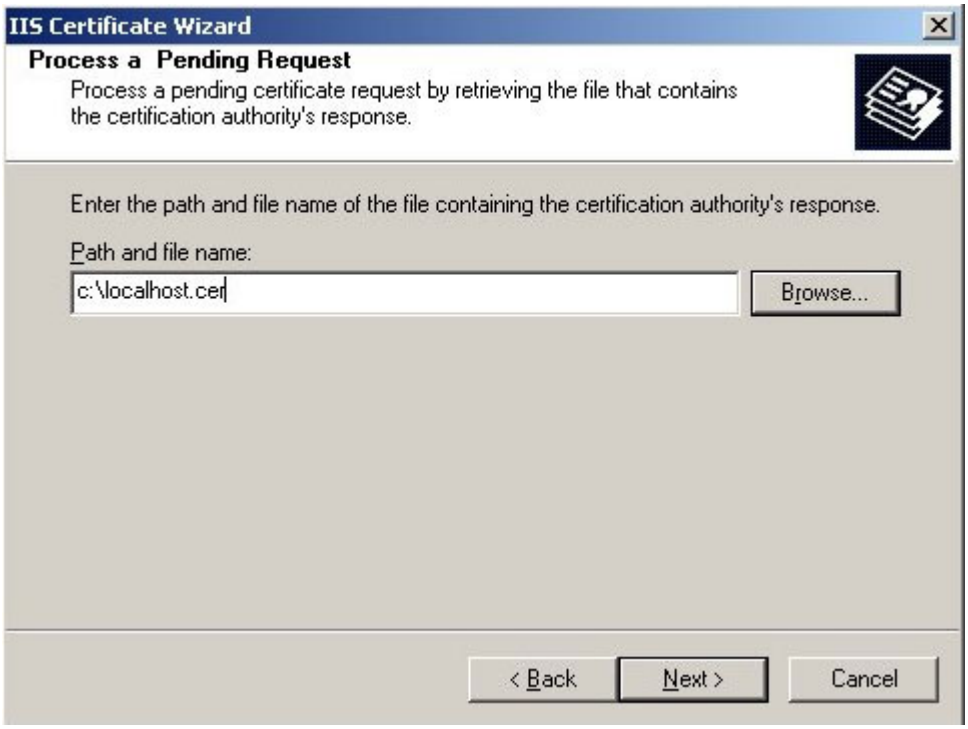
7.3. Ενημέρωση του IIS για την εγκατάσταση του πιστοποιητικού μας.

Ανοίγουμε και πάλι τον πίνακα ελέγχου→ εργαλεία διαχείρισης και ανοίγουμε τον IIS. Επεκτείνουμε το δέντρο στα αριστερά της οθόνης και κάνουμε δεξί κλικ στο Default Web Site→ιδιότητες. Πηγαίνουμε στην καρτέλα ασφάλεια αρχείου (Directory Security) και κάνουμε κλικ στο κουμπί Πιστοποιητικό εξυπηρετητή (Server Certificate). Εμφανίζεται ο οδηγός εγκατάστασης του πιστοποιητικού όπως φαίνεται παρακάτω. Επιλέγουμε Process the pending request and install the certificate.



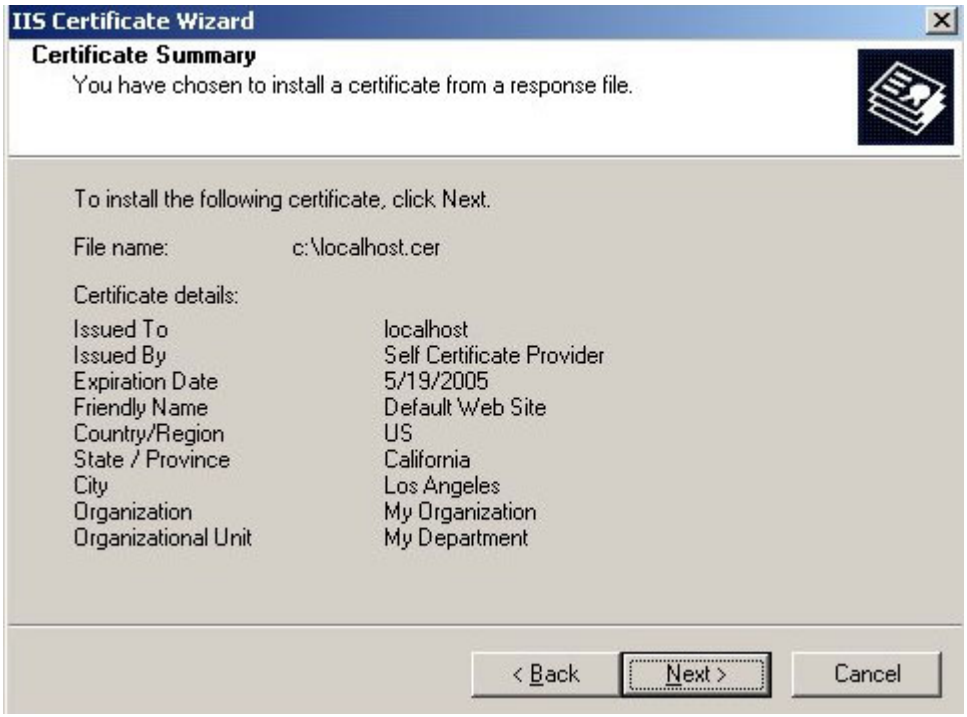
Σχήμα 49:Αίτηση για την εγκατάσταση του πιστοποιητικού.

Δηλώνουμε το μονοπάτι στο οποίο βρίσκεται το πιστοποιητικό μας και πατάμε Next.



Σχήμα 50: Δήλωση του μονοπατιού (path) όπου βρίσκεται το αρχείο που περιέχει την απάντηση της αρχής πιστοποίησης.

Ο IIS αναπαριστά τα στοιχεία του πιστοποιητικού μας. Πατάμε *Next*.



Σχήμα 51: Τελική προεπισκόπηση για την εγκατάσταση του πιστοποιητικού.

Ο IIS έχει εγκαταστήσει το πιστοποιητικό μας. Πατάμε *Finish*.

Σχήμα 52: Καρτέλα επιτυχημένης εγκατάστασης του πιστοποιητικού.

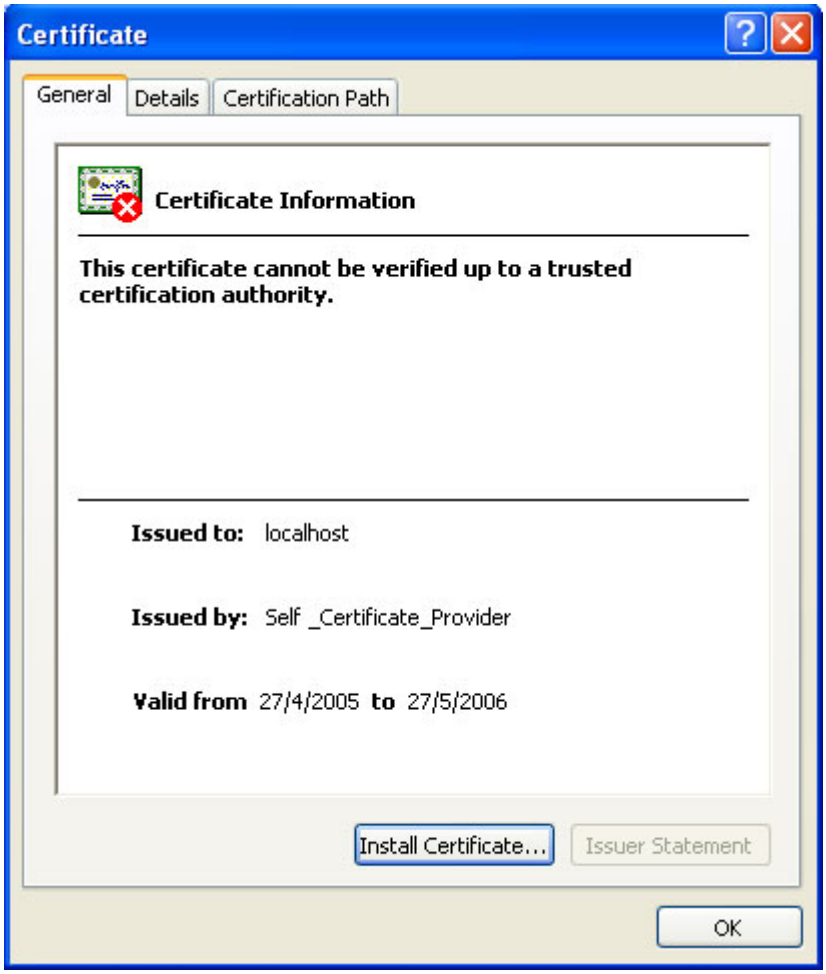
7.4. Δοκιμή πρόσβασης στο κομμάτι που καλύπτεται από το πιστοποιητικό μας.

Δοκιμάζοντας το πιστοποιητικό μας, ανοίγουμε το πρόγραμμα πλοήγησης και πληκτρολογούμε την διεύθυνση της ιστοσελίδας μας (το κοινό όνομα – Common Name - όπως το έχουμε δηλώσει που ανταποκρίνεται στο πιστοποιητικό) όπως φαίνεται παρακάτω. Φαίνεται επίσης πως είναι απαραίτητη η χρήση του https:// πρωτοκόλλου προκειμένου να έχουμε πρόσβαση στο ασφαλές κομμάτι της ιστοσελίδας μας. Αμέσως μετά, εμφανίζεται ο διάλογος Συναγερμού Ασφάλειας (Security Alert). Αυτός μας ενημερώνει ότι είμαστε έτοιμοι να επικοινωνήσουμε με μια ασφαλή ιστοσελίδα αλλά το πιστοποιητικό δεν έχει υπογραφεί από μια Αρχή Πιστοποίησης (Certificate Authority) που έχουμε δηλώσει ότι εμπιστευόμαστε. Επιβεβαιώνεται επίσης η χρονική του ισχύς. Αν είχε υπογραφεί το πιστοποιητικό μας από μια αληθινή αρχή τότε αυτός ο διάλογος δεν θα εμφανιζόταν. Επιλέγουμε Yes και έχουμε εισέλθει στην ασφαλή ιστοσελίδα.

Παρακάτω φαίνονται τα σχήματα μήνυμα ασφάλειας του πιστοποιητικού καθώς και το πιστοποιητικό.

Σχήμα 53: Μήνυμα ασφάλειας πιστοποιητικού.

Στην επιλογή view certificate βλέπουμε το πιστοποιητικό μας καθώς και τα στοιχειά του όπως ημερομηνία λήξης, εκδούσα αρχή κτλ., όπως φαίνεται παρακάτω:



Σχήμα 54: Τα στοιχεία του πιστοποιητικού μας.

Το κομμάτι αυτό, όπως θα φανεί στην ενότητα "Παρουσίαση της εφαρμογής", συνδέεται με την είσοδο ονόματος και κωδικού ασφαλείας για να μας πληροφορήσει ότι πρόκειται να εισέλθουμε σε χώρο ασφαλές.

8. Βασικά στοιχεία της εφαρμογής [xxxvi].

8.1. Τεχνολογία sessions.

Στην εφαρμογή μας χρησιμοποιήθηκε η τεχνολογία των sessions. Με την τεχνολογία αυτή αποθηκεύονται στην πλευρά του Εξυπηρετητή (Web Server) μεταβλητές στις οποίες βρίσκονται αποθηκευμένα δεδομένα τα οποία υπολογίζονται μετά από αναζητήσεις (queries) στη βάση μας ή ύστερα από άλλους απαραίτητους υπολογισμούς όπως πχ την εξεύρεση ενός ποσοστού. Η τεχνολογία των sessions μας βοηθά ώστε οι μεταβλητές αυτές να επαναχρησιμοποιούνται σε διαφορετικές asp σελίδες.

Για παράδειγμα όταν ο χρήστης επιλέξει μια περιοχή (πχ Χίος) αυτή μπορούμε να την αποθηκεύσουμε σε μια μεταβλητή "Περιοχή". Στη συνέχεια τη δηλώνουμε στο session ως εξής:

```
session("Επιλεχθείσα Περιοχή")=Περιοχή
```

Τώρα είμαστε σε θέση οποτεδήποτε θέλουμε να τυπώνουμε την επιλεχθείσα περιοχή με την εντολή:

```
<%=Session.contents("Επιλεχθείσα Περιοχή")%> ή
Response.write(Session.contents("Επιλεχθείσα Περιοχή"))
```

Η τεχνολογία αυτή είναι ακόμη χρησιμότερη όταν έχουμε να διαχειριστούμε όχι ένα αλλά σειρά δεδομένων. Στην περίπτωση αυτή τα δεδομένα αποθηκεύονται σε ένα πίνακα τον οποίο βάζουμε στο session. Για παράδειγμα χρειάστηκε η αποθήκευση όλων των ονομάτων, επιθέτων και ασφαλιστικών ταμείων όλων όσων πάσχουν από κάποια πάθηση την οποία επέλεξε ο χρήστης και στη συνέχεια σε διαφορετική asp σελίδα να τα τυπώσουμε. Ας υποθέσουμε ότι τα ονόματα αποθηκεύονται στον "Πίνακα1", τα επίθετα στον "Πίνακα2" και τα ταμεία στον "Πίνακα3". Αποθηκεύουμε τους πίνακες αυτή τη φορά στο session ως εξής:

```
Session("Ονόματα")=Πινακας1
Session("Επίθετα")=Πινακας2
Session("Ασφάλιση")=Πινακας3
```

Το μήκος των προηγούμενων πινάκων το έχουμε και πάλι αποθηκεύσει στην μεταβλητή “Μήκος_Πίνακα” στο session. Στην καινούρια asp σελίδα αποθηκεύουμε τα στοιχεία από το session σε νέους πίνακες:

```
Πίνακας_εμφάνιση_ονόματα=session.contents(“Ονόματα”)
Πίνακας_εμφάνιση_επίθετα=session.contents(“Επίθετα”)
Πίνακας_εμφάνιση_ασφάλιση=session.contents(“Ασφάλιση”)
```

Άρα με την βοήθεια ενός for loop μπορούμε να τυπώσουμε τα παραπάνω στοιχεία ως εξής:

```
<%
for i=0 to session.contents("Μήκος_Πίνακα")-1
            Response.write(Πίνακας_εμφάνιση_ονόματα(i))
            Response.write(Πίνακας_εμφάνιση_επίθετα(i))
            Response.write(Πίνακας_εμφάνιση_ασφάλιση(i))
Next
%>
```

8.2. Ενδεικτικό τμήμα κώδικα εκτέλεσης των queries και αποθήκευσης αποτελεσμάτων.

Παρακάτω φαίνεται ενδεικτικά ένα τμήμα από τον κώδικά μας το οποίο χρησιμοποιήθηκε πολύ συχνά για την εκτέλεση αναζητήσεων μέσα στη βάση δεδομένων.

```
<%
     Set rs=Server.CreateObject ("ADODB.recordset")

     rs.Open "select count(*) from deigma d, pathiseis p,
sysxetish_pathiseis s where p.pathisi_name='" &Σχιζοφρένεια& "' AND
p.pathisi_id=s.id_pathishs AND s.id_asthenh=d.id_deigma ", conn

     if  rs.fields(0)=0 then

     pinakas1(i)=rs.fields(0)
     i=i+1
              rs.close
     else
     rs.Movefirst
     While not rs.EOF
     pinakas1(i)=rs.fields(0)
     i=i+1
     rs.movenext
     Wend
     rs.close
```

```
      end if
%>
```

Το query στο παραπάνω παράδειγμα είναι το:

```
select count(*) from deigma d, pathiseis p, sysxetish_pathiseis s
where p.pathisi_name='" &Σχιζοφρένεια& "' AND
p.pathisi_id=s.id_pathishs AND s.id_asthenh=d.id_deigma
```

Από το συγκεκριμένο query καταμετρούνται από το δείγμα όσοι έχουν Σχιζοφρένεια. Όπως φαίνεται ταυτίζεται το id_πάθησης από τον πίνακα παθήσεων με το id_πάθησης του πίνακα συσχέτισης με τις παθήσεις και το id_ασθενή του πίνακα συσχέτισης με τις παθήσεις με το id_δείγματος του κάθε ασθενή από το δείγμα (βλ. και σχήμα βάσης).

Το αποτέλεσμα του query επιστρέφει στο *rs.fields(0)*. Αν αυτό είναι μηδέν δηλαδή δεν υπάρχει κανένας ασθενής με Σχιζοφρένεια τότε στον πίνακα που αναμένει να αποθηκεύσει τα δεδομένα μας βάζουμε το μηδέν. Αλλιώς, μετακινούμε ένα-ένα τα στοιχεία τα οποία βρίσκονται (ουσιαστικά έναν αύξοντα αριθμό) στον πίνακά μας και τελικά τον τυπώνουμε. Φυσικά πέρα από ένα απλό νούμερο στην εργασία έγιναν και πιο πολύπλοκα queries όπως η αναζήτηση ονομάτων κτλ.

9. Παρουσίαση της εφαρμογής.

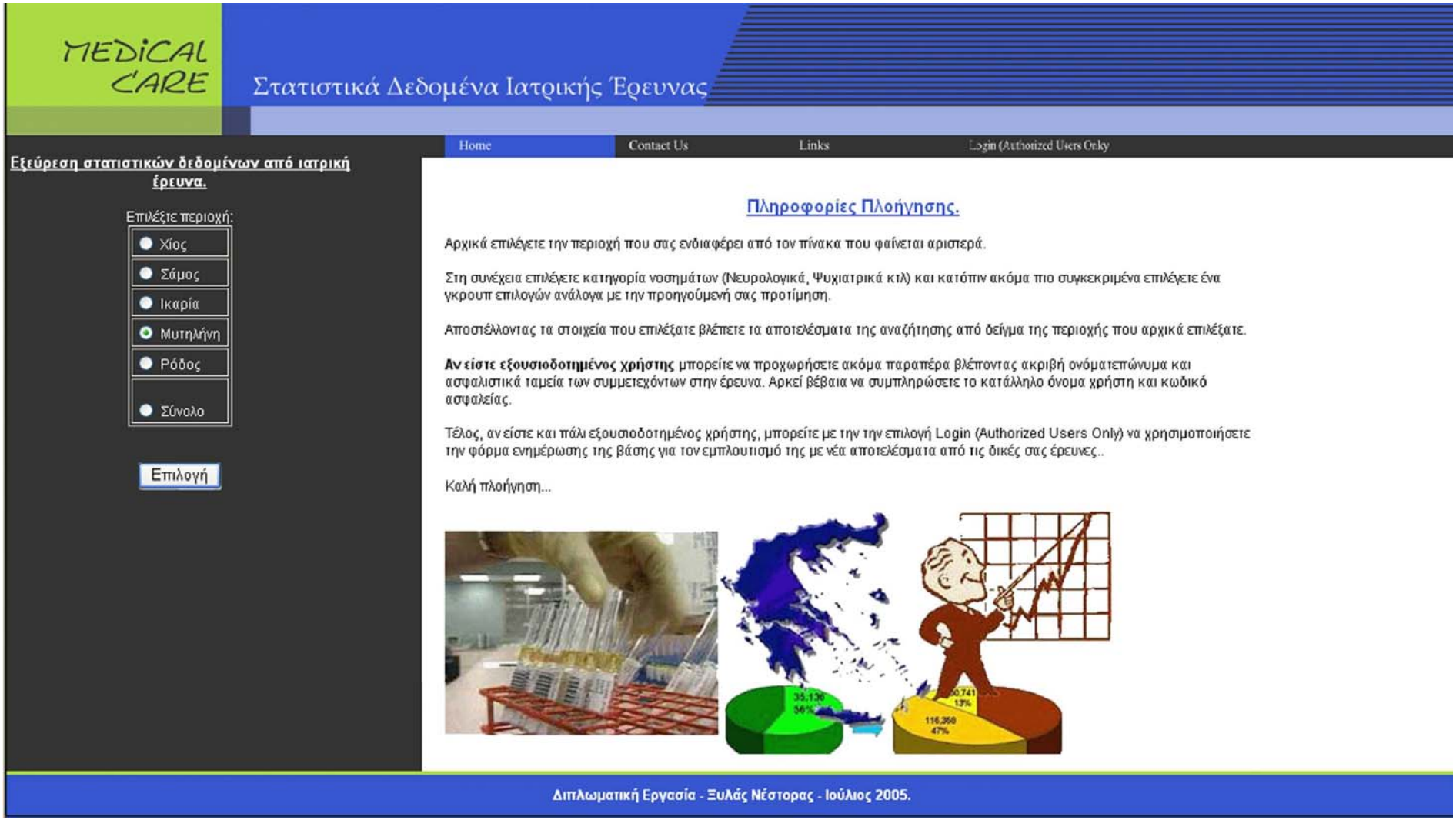
9.1. Γενικά για το λογισμικό που χρησιμοποιήθηκε.

Θα πρέπει να αναφέρουμε ότι για την δημιουργία της ιστοσελίδας μας χρησιμοποιήθηκε το πρόγραμμα Xara WebStyle (Version 4.0), και ότι ο προγραμματισμός σε ASP έγινε στο περιβάλλον του προγράμματος Dreamweaver MX (Version 6.0).

9.2. Ξεκινώντας.

Αρχικά και αφού έχουμε ενεργοποιήσει τον εξυπηρετητή της βάσης δεδομένων καθώς και τον IIS, πληκτρολογούμε στην μπάρα διευθύνσεων του προγράμματος πλοήγησης http://localhost/iatrika/index.html. Είναι η πρώτη σελίδα της εφαρμογής μας. Σε αυτή υπάρχει ένα menu από τέσσερις επιλογές που βρίσκονται στη διάθεση του χρήστη καθ' όλη τη διάρκεια της περιήγησής του. **Αρχική Σελίδα (Home)**, **Επικοινωνία (Contact Us)** που οδηγεί κατευθείαν στην ηλεκτρονική διεύθυνση του ιατρικού κέντρου που διαχειρίζεται την ιστοσελίδα, **Σύνδεσμοι (Links)** που δείχνουν σε άλλες χρήσιμες ιστοσελίδες με ερευνητικό – ιατρικό περιεχόμενο και τέλος η επιλογή **Login (Authorized Users Only)** που δίνει τη δυνατότητα στους εξουσιοδοτημένους μόνο χρήστες να χρησιμοποιήσουν μια φόρμα ενημέρωσης της βάσης δεδομένων δίνοντας αναλυτικά τα αποτελέσματα δικής τους έρευνας και με αυτό τον τρόπο να κάνουν πληρέστερη τη μελέτη.

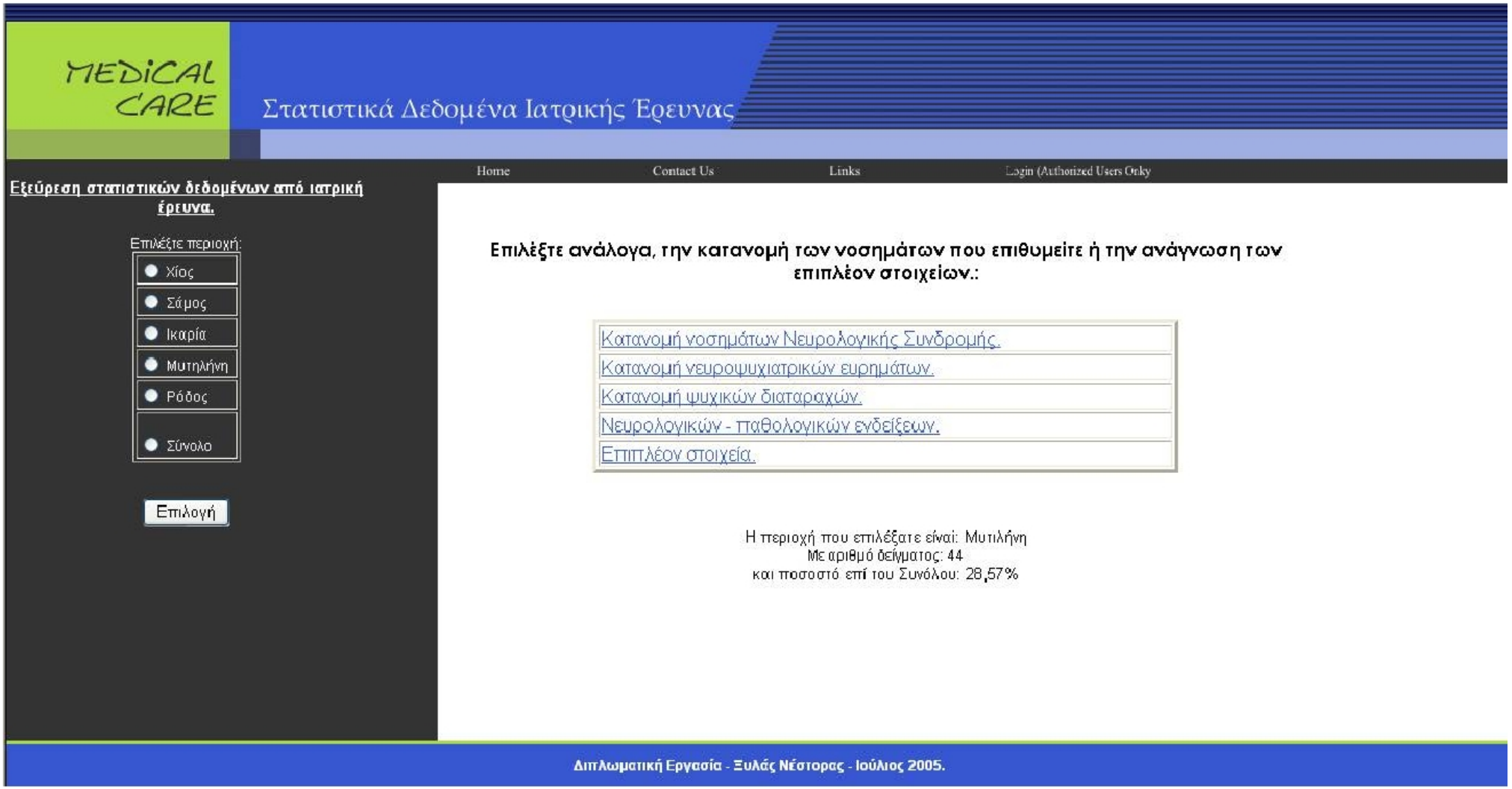
Όπως φαίνεται παρακάτω στη δεξιά πλευρά ο χρήστης πληροφορείται αναλυτικά για την περιήγησή του στο υπόλοιπο της εφαρμογής και αριστερά φαίνονται οι τοποθεσίες στις οποίες έχουν γίνει ιατρικές έρευνες. (Στιγμιότυπο 1: Κεντρική σελίδα της παρουσίασης μας - Home Page.)



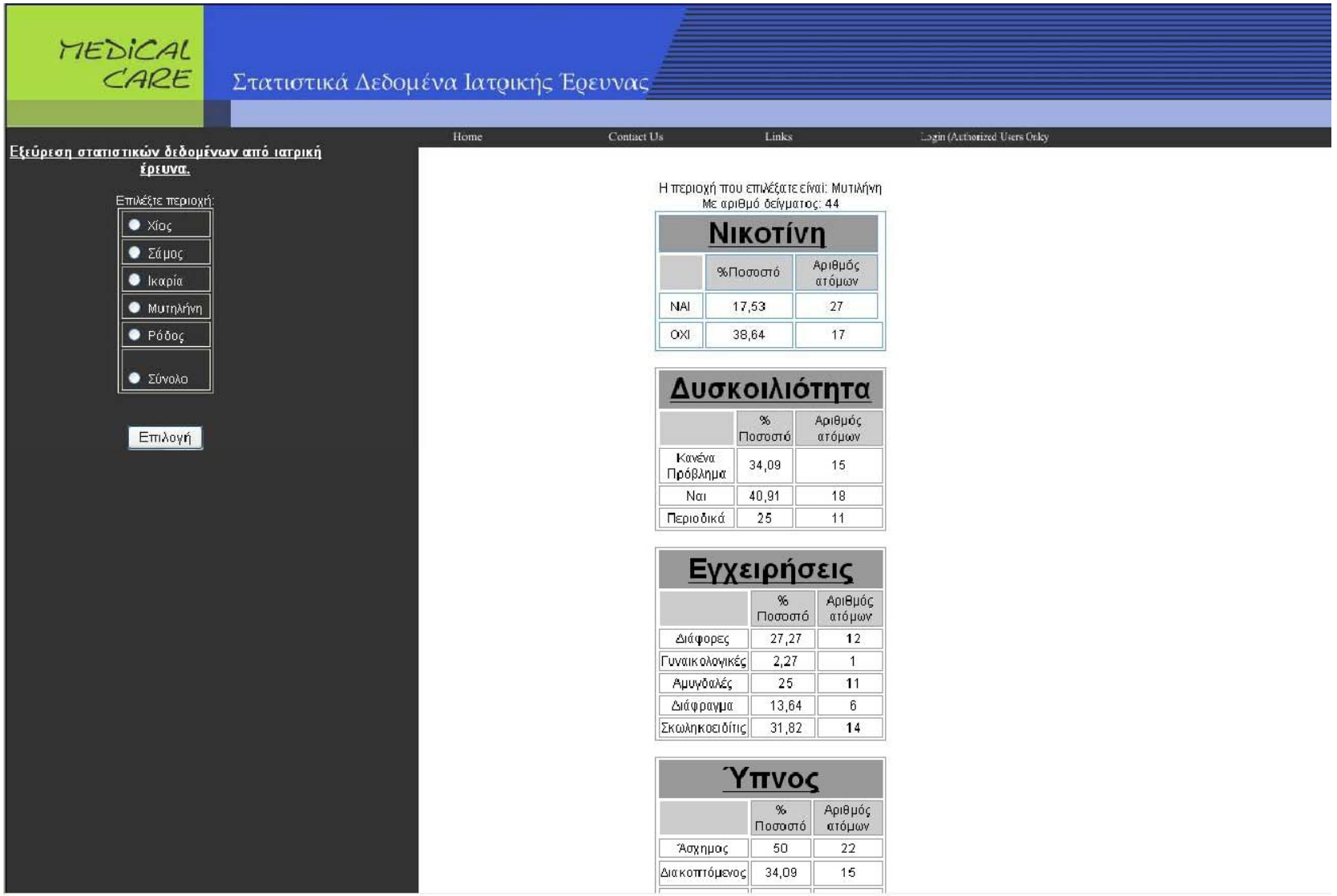
Στιγμιότυπο 1: Κεντρική σελίδα της παρουσίασης μας - Home Page.

Στη συνέχεια επιλέγει την περιοχή που επιθυμεί., για παράδειγμα Μυτιλήνη. Αμέσως πληροφορείται τον πληθυσμό της και το ποσοστό του πληθυσμού αυτού επί του συνόλου του δείγματος. Ο χρήστης τώρα είναι έτοιμος να επιλέξει την κατηγορία παθήσεων για την οποία επιθυμεί να ενημερωθεί με βάση την περιοχή που επέλεξε (πχ Κατανομή Νοσημάτων Νευρολογικής Συνδρομής, Κατανομή Νευροψυχιατρικών Νοσημάτων κτλ) όπως φαίνονται στο πίνακα στα δεξιά του σχήματος που ακολουθεί.

Υπάρχει επίσης και οι επιλογή των επιπλέον στοιχείων που συμπεριλαμβάνει γενικά στατιστικά δεδομένα σχετικά με το επιλεχθέν δείγμα (πχ στοιχεία για το κάπνισμα, ούρηση, καφέ, εγχειρήσεις κτλ), όπως φαίνεται εξίσου παρακάτω.

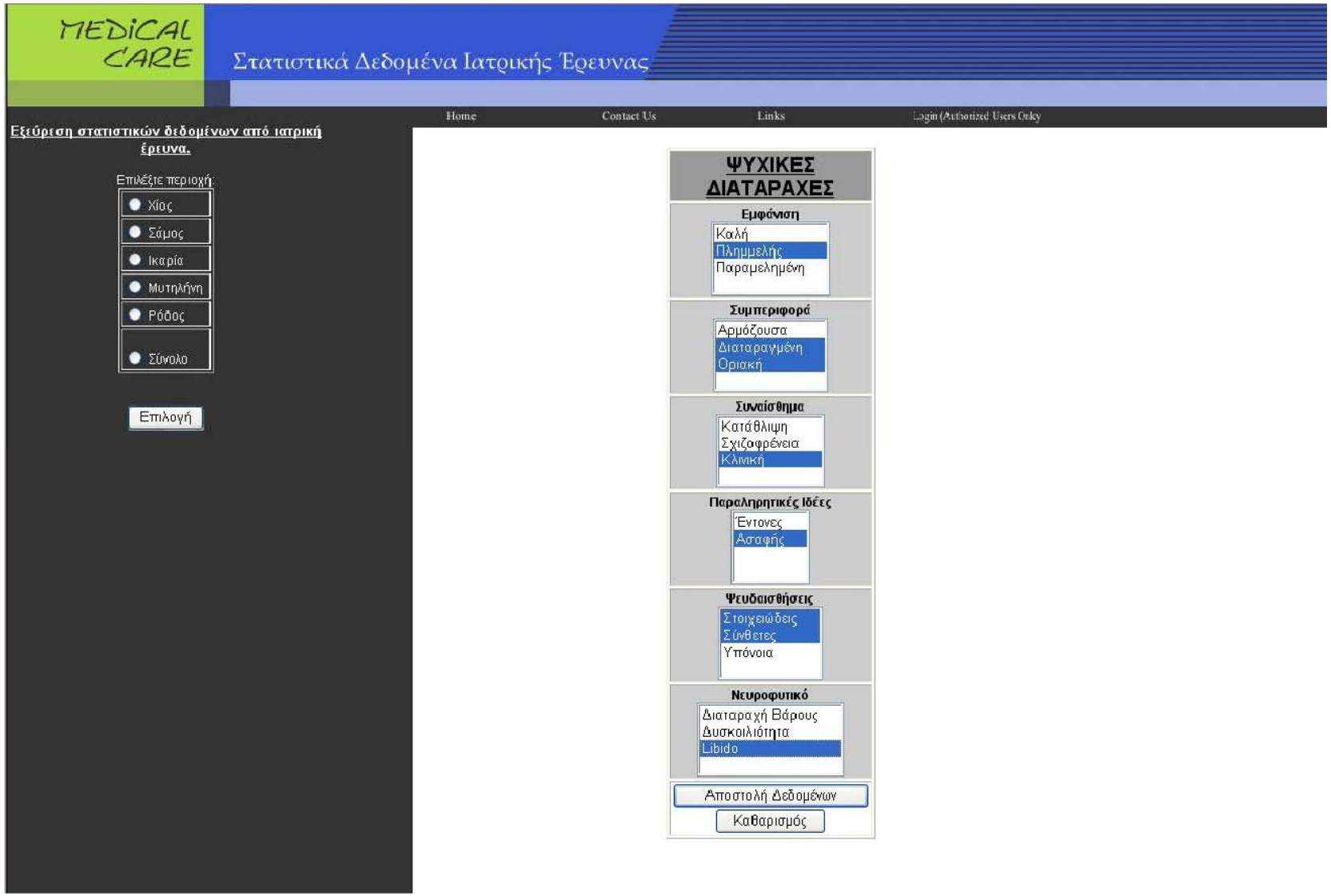


Στιγμιότυπο 2: Επιλογή περιοχής Μυτιλήνη.

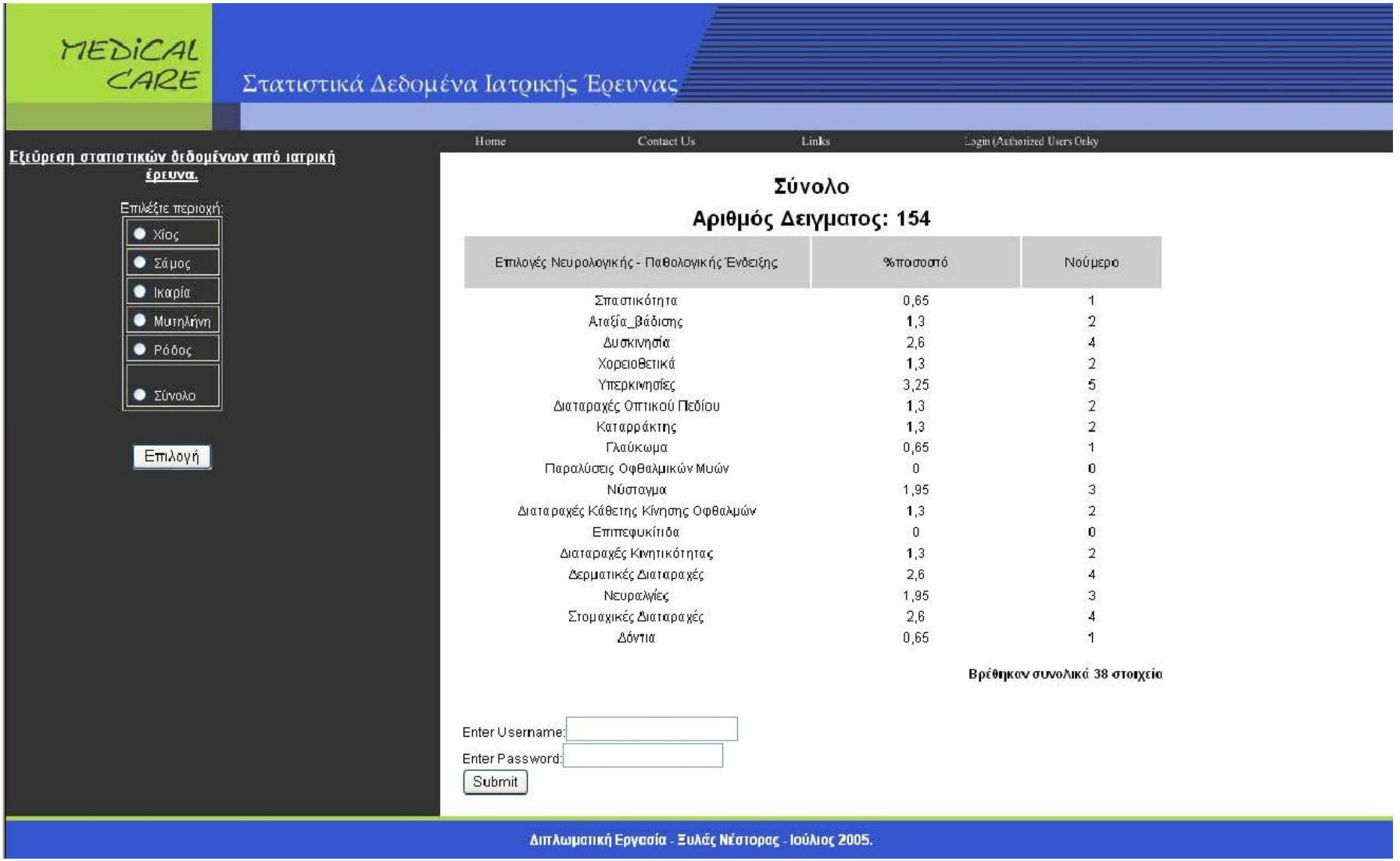


Στιγμιότυπο 3: Επιλογή επιπλέον στοιχείων.

Αν ο χρήστης επιλέξει κατανομή παθήσεων τότε βρίσκεται μπροστά σε αναλυτικούς πίνακες με επιλογές από τη συγκεκριμένη κατανομή (πχ στην **Κατανομή Ψυχικών Διαταραχών** βλέπει διαταραχές που έχουν να κάνουν με την **Εμφάνιση** την **Συμπεριφορά**, το **Συναίσθημα** κτλ) όπως φαίνονται παρακάτω. Ο χρήστης μπορεί να κάνει πολλαπλές επιλογές και με την εντολή **"Αποστολή Στοιχείων"** ενεργοποιεί την asp σελίδα όπου γίνεται η αναζήτηση και η επιστροφή των στοιχείων που επέλεξε. Ακολουθεί στιγμιότυπο της αναζήτησης επί του **Συνόλου** σε επιλογές **Νευρολογικών – Παθολογικών ενδείξεων**.



Στιγμιότυπο 4: Πολλαπλές επιλογές (Ψυχικές Διαταραχές).

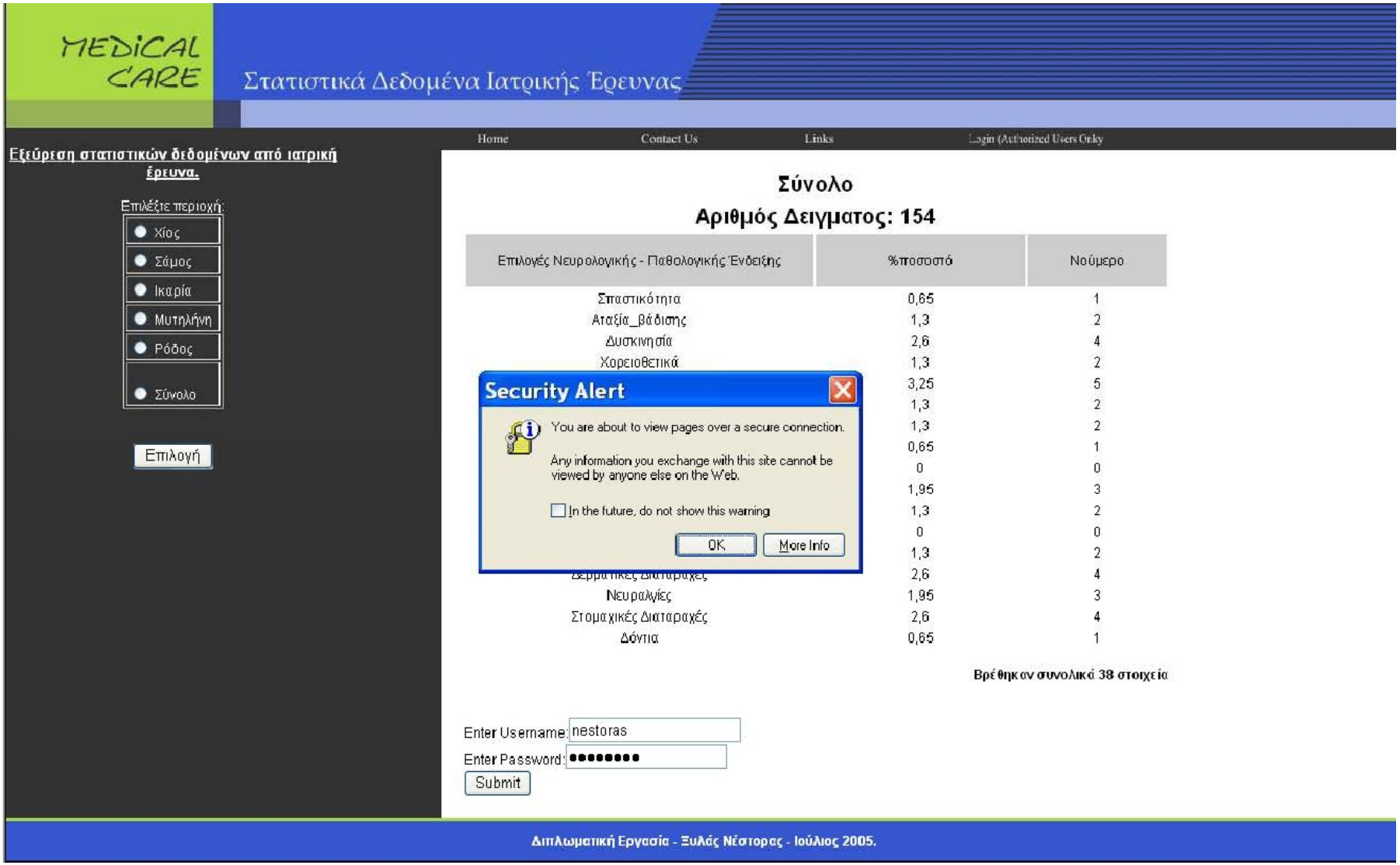


Στιγμιότυπο 5: Πολλαπλές επιλογές (Νευρολογικής – Παθολογικής Ένδειξης) και αποστολή στοιχείων.

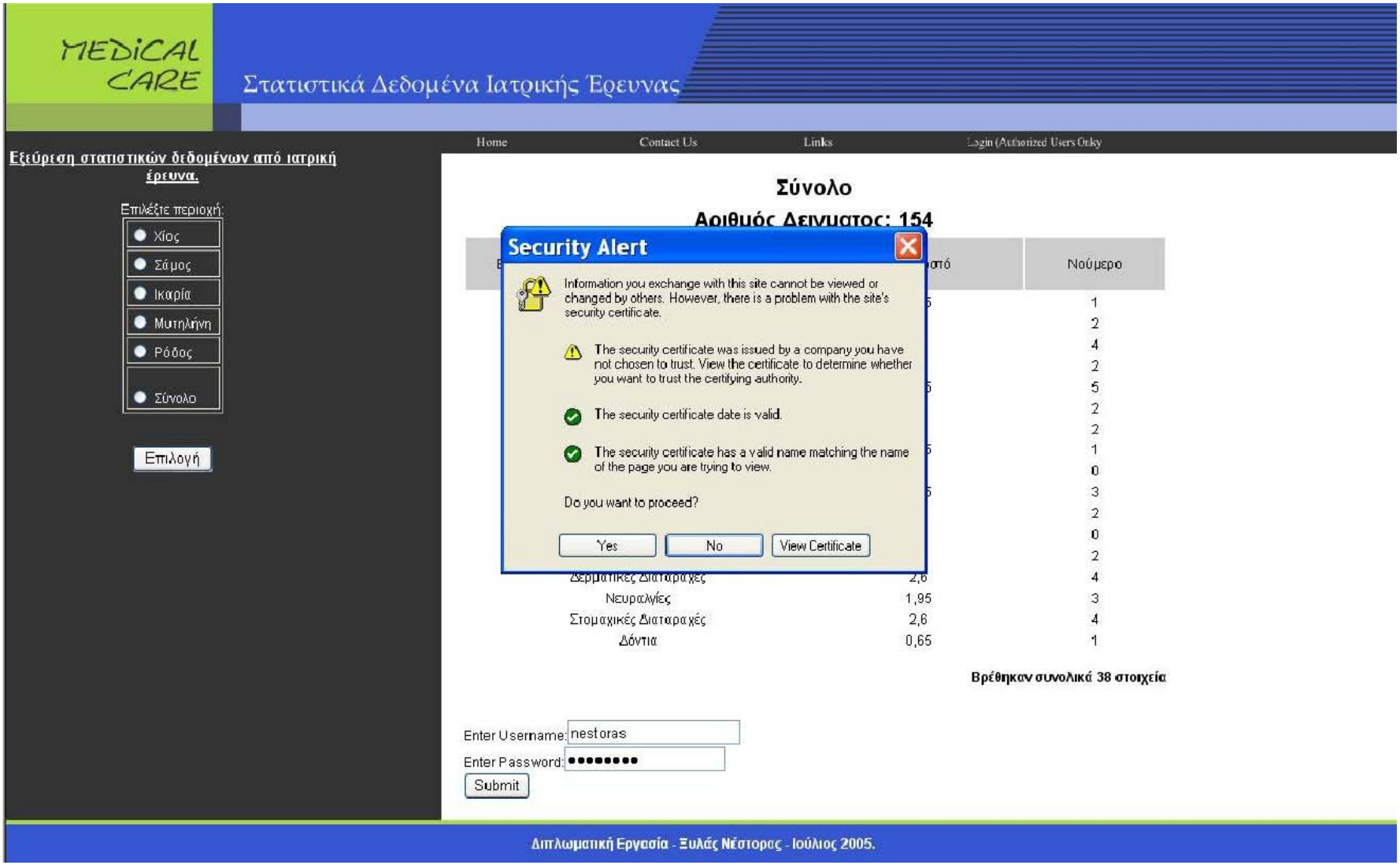
9.3. Για εξουσιοδοτημένους χρήστες.

Αν μετά από την αμέσως προηγούμενη επιλογή υπάρξουν αποτελέσματα, δηλαδή ασθενείς με τις συγκεκριμένες ενδείξεις τότε στην οθόνη εμφανίζεται η επιλογή Enter Username και Enter Password που απευθύνεται σε εξουσιοδοτημένους χρήστες. Με την επιτυχή συμπλήρωση των στοιχείων αυτών, εμφανίζεται ο διάλογος ενημέρωσης και παρουσίασης του πιστοποιητικού μας όπως περιγράφηκε πριν. Είναι το επίμαχο κομμάτι που αφορά την ασφάλεια Με την αποδοχή του πιστοποιητικού, φαίνονται τα στοιχεία των ασθενών από την τελευταία στατιστική αναζήτηση (Α/Α, Ονομ/μο, Ένδειξη, Ασφαλιστικό ταμείο). Στα τρια στιγμιότυπα που ακολουθούν φαίνεται η ένδειξη Security Alert, η πιστοποίηση του εξυπηρετητή και τα ονόματα των ασθενών με τις συγκεκριμένες παθολογικές ενδείξεις αντίστοιχα.

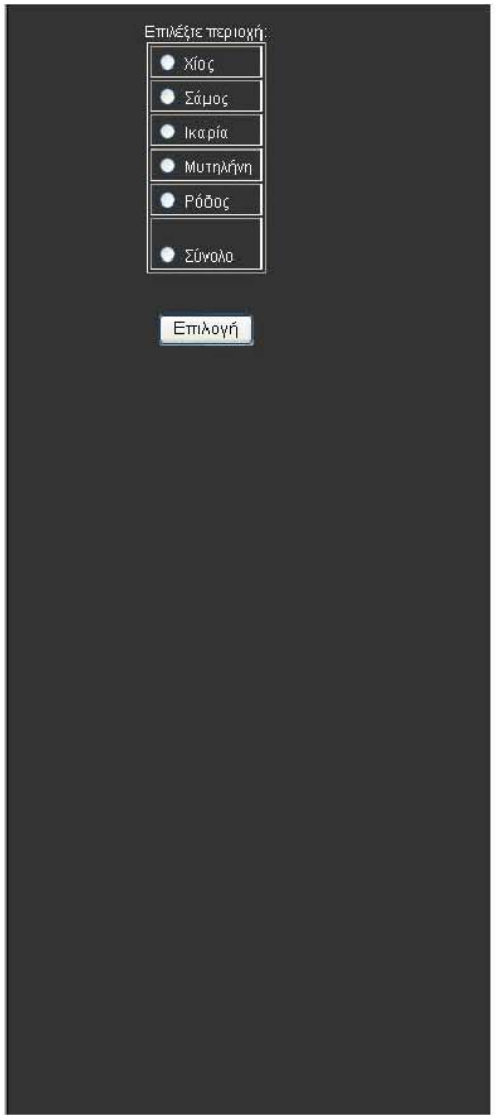
Αξίζει να αναφερθεί ότι καθ' όλη τη διάρκεια της αναζήτησής του και ανά πάσα στιγμή ο χρήστης μπορεί να αλλάζει την περιοχή που έχει επιλέξει. Αυτές βρίσκονται συνεχώς στα αριστερά της οθόνης. Έτσι υπάρχει η δυνατότητα να ξεκινούν εκ νέου αναζητήσεις σε διαφορετικές περιοχές.



Στιγμιότυπο 6: Security Alert.



Στιγμιότυπο 7: Εμφάνιση Πιστοποίησης εξυπηρετητή.

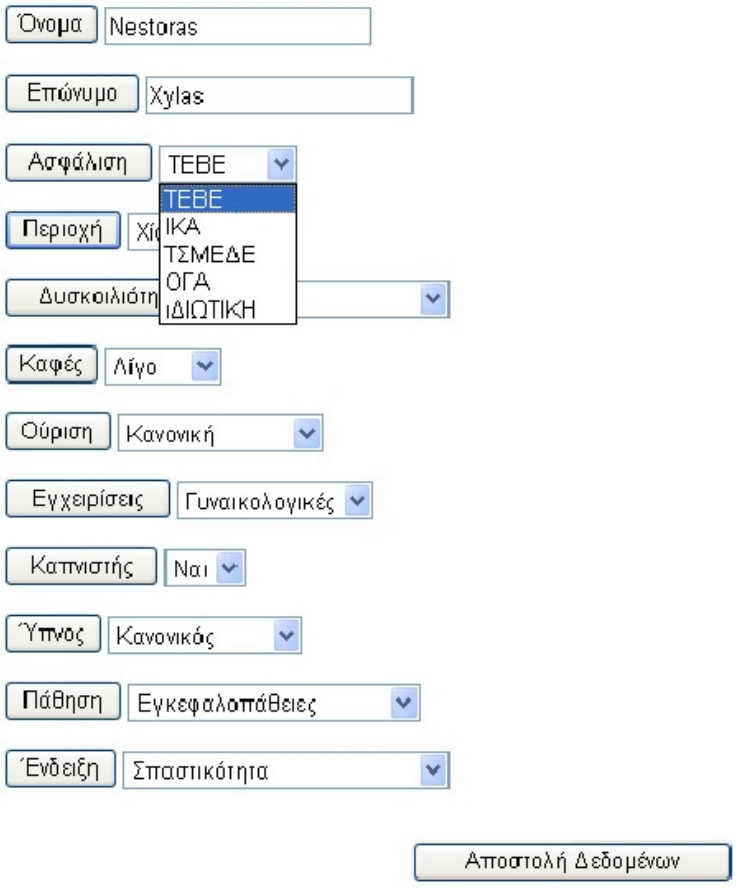


Α/Α	Ένδειξη	Όνομα	Επώνυμο	Ταμείο
1	Σπαστικότητα	Αικατερίνη	Παπαρούνα	Ιδιωτική
2	Αταξία_βάδισης	Πάτροκλος	Ζαμπάρας	ΤΣΑ
3	Αταξία_βάδισης	Αικατερίνη	Παπαρούνα	Ιδιωτική
4	Δυσκινησία	Ιωάννα	Παγώνη	ΤΣΑ
5	Δυσκινησία	Γεώργιος	Παλανδρής	ΟΓΑ
6	Δυσκινησία	Αρχοντία	Σουλελέ	ΤΣΑ
7	Δυσκινησία	Μαρία	Ξηρομερίτη	ΤΣΑ
8	Χορειοθετικά	Λουκάς	Στούφης	ΤΣΜΕΔΕ
9	Χορειοθετικά	Γεώργιος	Παλανδρής	ΟΓΑ
10	Υπερκινησίες	Στέφανος	Ράπτης	ΤΕΒΕ
11	Υπερκινησίες	Αλέξανδρος	Ζευγώλης	ΤΣΑ
12	Υπερκινησίες	Κωνσταντίνος	Ιακωβίδης	ΙΚΑ
13	Υπερκινησίες	Βασιλική	Σαββάκη	ΤΣΜΕΔΕ
14	Υπερκινησίες	Αρχοντία	Παπαρούνα	ΤΣΜΕΔΕ
15	Διαταραχές Οπτικού Πεδίου	Αρχοντία	Καπετανάκη	ΤΣΑ
16	Διαταραχές Οπτικού Πεδίου	Ηλίας	Επιτροπάκης	ΟΓΑ
17	Καταρράκτης	Κωνσταντίνος	Σαββάκης	ΟΓΑ
18	Καταρράκτης	Αλέξανδρος	Παλαμίδας	ΤΣΑ
19	Γλαύκωμα	Πέτρος	Στούφης	ΤΣΜΕΔΕ
20	Νύσταγμα	Γεώργιος	Καπετανάκης	ΙΚΑ
21	Νύσταγμα	Ηλίας	Ζαμπάρας	ΙΚΑ
22	Νύσταγμα	Αικατερίνη	Παγώνη	ΤΣΜΕΔΕ
23	Διαταραχές Κάθετης Κίνησης Οφθαλμών	Αρχοντία	Κάραλη	ΤΣΜΕΔΕ
24	Διαταραχές Κάθετης Κίνησης Οφθαλμών	Βασίλειος	Ιακωβίδης	ΟΓΑ
25	Διαταραχές Κινητικότητας	Ελισάβετ	Ιακωβίδη	ΤΣΑ
26	Διαταραχές Κινητικότητας	Δννα	Στούφη	ΤΣΜΕΔΕ
27	Δερματικές Διαταραχές	Ιωάννα	Παπαρούνα	ΤΕΒΕ
28	Δερματικές Διαταραχές	Ελένη	Παπαρούνα	ΟΓΑ
29	Δερματικές Διαταραχές	Πέτρος	Επιτροπάκης	Ιδιωτική
30	Δερματικές Διαταραχές	Αρχοντία	Παπαρούνα	ΤΣΜΕΔΕ
31	Νευραλγίες	Γεώργιος	Παγώνης	ΙΚΑ
32	Νευραλγίες	Ελισάβετ	Ράπτη	ΤΣΜΕΔΕ
33	Νευραλγίες	Ηλίας	Ζαμπάρας	ΙΚΑ
34	Στομαχικές Διαταραχές	Πέτρος	Ζαμπάρας	ΙΚΑ
35	Στομαχικές Διαταραχές	Γεώργιος	Ξηρομερίτης	ΟΓΑ
36	Στομαχικές Διαταραχές	Βασιλική	Σαββάκη	ΤΣΜΕΔΕ
37	Στομαχικές Διαταραχές	Πέτρος	Επιτροπάκης	Ιδιωτική
38	Δόντια	Μαρία	Παγώνη	ΤΣΜΕΔΕ

Στιγμιότυπο 8: Αποτέλεσμα αναζήτησης ευαίσθητων δεδομένων.

9.4. Χρήση της φόρμας ενημέρωσης.

Με τη χρήση της επιλογής Login (Authorized Users Only) φαίνεται η φόρμα που μπορεί να συμπληρώσει ο χρήστης με βάση τα αποτελέσματα των δικών του ερευνών. και να εμπλουτίσει τη βάση δεδομένων. ένα χαρακτηριστικό παράδειγμα φαίνεται στα δυο στιγμιότυπα που ακολουθούν.



Στιγμιότυπο 9: Φόρμα εμπλουτισμού βάσης δεδομένων.

Στιγμιότυπο 10: Επιτυχής είσοδος στοιχείου στη φόρμα.

10. Συμπεράσματα.

Η εφαρμογή μας όπως είδαμε, προσφέρει τη δυνατότητα άμεσης αναζήτησης αποτελεσμάτων ιατρικών ερευνών που έχουν διεξαχθεί σε διάφορες τοποθεσίες στην Ελλάδα μέσω του διαδικτύου. Με απλό τρόπο και ασφαλή τρόπο, ο εξουσιοδοτημένος χρήστης (ιατρικό κέντρο, ερευνητικό κέντρο κτλ) μπορεί να υπεισέλθει σε περισσότερο ευαίσθητα δεδομένα ώστε να μπορεί να έρθει σε επαφή και με ασθενείς για την περαιτέρω ερευνητική του δραστηριότητα, αλλά και να αποστείλει δικά του επιστημονικά συμπεράσματα εμπλουτίζοντας τη βάση δεδομένων. Δίνει επιπλέον τη δυνατότητα συνεργασίας ανάμεσα στους διάφορους φορείς για τον καλύτερο ιατρικό έλεγχο και φροντίδα πληθυσμιακών ομάδων με εμπιστευτική ανταλλαγή στοιχείων. Αυτό βοηθά στη συγκέντρωση και ενοποίηση σειράς ερευνητικών αποτελεσμάτων για μεγάλα τμήματα του πληθυσμού και στην άμεση λήψη μέτρων ιατρικής βοήθειας σε περιοχές όπου υπάρχουν ανησυχητικά αποτελέσματα από πλευράς υγιεινής και χρίζουν περαιτέρω επεξεργασίας.

Έμφαση δόθηκε στην απλότητα της εφαρμογής, ώστε ο χρήστης με τις ελάχιστες δυνατές ενέργειες να μπορεί να εκτελέσει όλες τις βασικές λειτουργίες που θα χρειαστεί, χωρίς να απαιτούνται από μέρους του ειδικές γνώσεις ή εκπαίδευση. Ένα από τα ισχυρά χαρακτηριστικά της εφαρμογής είναι τόσο ο δυναμικός τρόπος με τον οποίο παρουσιάζονται τα αποτελέσματα των αναζητήσεων του χρήστη, όσο και η ασφάλεια μέσω του πιστοποιητικού αλλά και του κωδικού πρόσβασης που απολαμβάνει ο χρήστης και φυσικά ο συμμετέχων στην έρευνα. Με αυτό τον τρόπο διατηρείται το ιατρικό απόρρητο αλλά και η σιγουριά από πλευράς των χρηστών ότι πρόκειται να αντικρίσουν αξιόπιστα και όχι παραποιημένα ιατρικά δεδομένα.

Υπάρχει βέβαια και δυνατότητα επέκτασης της εφαρμογής με ανάπτυξη των ερευνών σε πανελλαδικό επίπεδο αλλά και δυνατότητες επέκτασης της βάσης και σε διαφορετικά πεδία παθήσεων πέρα των νευρολογικών όπου βρίσκονται στην εφαρμογή. Επίσης θα μπορούσε να ενισχυθεί η ασφάλεια της εφαρμογής με αυθεντικοποίηση όχι μόνο του εξυπηρετητή αλλά και του πελάτη.

ΒΙΒΛΙΟΓΡΑΦΙΑ

i R.ELMASRI – S.B. NAVATHE "Θεμελιώδης Αρχές Συστημάτων Βάσεων Δεδομένων. ΤΟΜΟΣ Α' 2000 σελ 29,30,31,32

ii Mark Maslakowski "Sam's Teach Yourself MySQL in 21 Days" 2000, σελ 9,71,107, http://www.mysql.com

iii Kevin Poulsen "Hospital Records Hacked" Security Focus 6/12/2000 www.securityfocus.com/news/122

iv Bob Brewin "Pentagon says attack on blood data banks 'simulated'" 30/9/1998 www.fcw.com

v Α. Μπούρκα "Προηγμένες υπηρεσίες Υποδομής Δημοσίου Κλειδιού για την Υγεία: Ανάπτυξη ασφαλούς εφαρμογής διακίνησης ηλεκτρονικών ιατρικών κειμένων. Υλοποίηση πρότυπης μεθόδου αυτοματοποιημένης σύγκρισης πολιτικών

vi SSL v3 Specifications, NETSCAPE http://www.netscape.com/eng/ssl3/

vii Β. Γώγου «Μελέτη, σχεδιασμός και ανάπτυξη έξυπνης κάρτας πολλαπλών εφαρμογών για χρήση διαβητικού κέντρου" Διδακτορική διατριβή 2002

viii ISO 7498-2: www.iso.org

ix Bruce Schneier "Applied Cryptography", John Wiley & Sons Inc, 1996

x Ε. Ζάχος "Σημειώσεις στη Θεωρία Αριθμών και την Κρυπτογραφία" 2003 .

xi J. Thompson "Monoalphabetic Cryptanalysis" Phrack Magazine Issue 51 1997.

xii Charles H. Bennett, Gilles Brassard και Artur K. Ekert "Quantum Cryptography" Scientific American Οκτώβρης 1992 Τεύχος 267, No 4, σελ.28.

xiii NIST FIPS 186 Digital Signature Standard (DSS) 1994 www.itl.nist.gov/fipspubs/fip186.htm

xiv Electronic Frontier Foundation "Cracking DES" 1998

xv NIST FIPS 197 "Advanced Encryption Standard" http://csrc.nist.gov/CryptoToolkit/aes

xvi NIST FIPS 185 "Escrowed Encryption Standard (EES)" 1994 http://www.itl.nist.gov/fipspubs/fip185.htm

xvii Η ιστοσελίδα του rijndael http://www.esat.kuleuven.ac.be/~rijmen/rijndael/

xviii Η ιστοσελίδα του rijndael "fun club" http://rijndael.com

xix "The International PGP Home Page" www.pgpi.org

xx Wenbo Mao "Modern Cryptography - Theory & Practice" 2004 Hewlett Packard σελ. 279.

xxi R. Rivest http://theory.lcs.mit.edu/~rivest/Rivest-MD5.txt Internet RFC 1321, 1992

xxii NIST FIPS 180-1 "Secure Hash Standard" 1995 http://csrc.nist.gov/CryptoToolkit/tkhash.html

xxiii Hans Dobbertin "The Status of MD5 After a Recent Attack" CryptoBytes Volume 2, Number 2 — 1996, ftp://ftp.rsasecurity.com/pub/cryptobytes/

xxiv VeriSign: www.verisign.com

xxv Thawte: www.thawte.com

xxvi Entrust: www.entrust.com

xxvii ITU-T Recommendation X.509 (08/1997) www.itu.int/ITU-T/asn1/database/itu-t/x/x509/1997

xxviii R. Rivest "Issues in Cryptography" Σύντομη ομιλία που έγινε στις 7 Μαρτίου, 2001 στο "Computers, Freedom, and Privacy 2001 Conference".

xxix Mirella Mazzeo "Digital Signatures and European Laws" Security Focus Ιανουάριος 2004 http://securityfocus.com

xxx Introduction to SSL http://www.iplanet.com/documentation/documentation_8_0.html

xxxi Manas Tungare "A Practical Guide to Active Server Pages 3.0" 2000 http://manastungare.com

xxxii Πληροφορίες για τον IIS http://windowsitlibrary.com

xxxiii Το ποιο πρόσφατο manual της MySQL στη διεύθυνση βρέθηκε στην διεύθυνση http://www.mysql.com/documentation/

xxxiv http://www.mysql.com/products/myodbc/manual_toc.html http://www.mysql.com/products/myodbc/faq_toc.html

xxxv http://www.alphaworks.ibm.com/tech/keyman

xxxvi Διεύθυνση με πληροφορίες από tutorials για την ASP http://www.w3schools.com