Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Συστήματα διαχείρισης εγγράφων πολυεπίπεδης ασφάλειας με ενσωματωμένη ψηφιακή υπογραφή**
Ονοματεπώνυμο Φοιτητή	**Αλμαλής Νικόλαος**
Πατρώνυμο	**Δημήτριος**
Αριθμός Μητρώου	**ΜΠΠΛ/ 08002**
Επιβλέπων	**Νικόλαος Αλεξανδρής, Καθηγητής**

Ημερομηνία Παράδοσης **28 Σεπτεμβρίου 2010**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Νικόλαος Αλεξανδρής Καθηγητής	Δεσπότης Δημήτριος Καθηγητής	Κωνσταντόπουλος Χ. Λέκτορας

ΠΕΡΙΛΗΨΗ

Είναι γενικά γνωστό ότι η επιστήμη των υπολογιστών παρουσιάζει μια ραγδαία ανάπτυξη τα τελευταία χρόνια. Σε αυτή τη νέα εποχή, οι επιχειρήσεις, οι οργανισμοί, οι κυβερνήσεις, αλλά και μεμονωμένα άτομα χρησιμοποιούν όλο και περισσότερο εφαρμογές που βασίζονται σε πληροφοριακά συστήματα, τα οποία δομούνται πάνω σε δίκτυα. Αυτή η επιλογή προσφέρει αποδοτικότερες, αποτελεσματικότερες και φθηνότερες λύσεις στις προκλήσεις της επικοινωνίας, στις συναλλαγές αλλά και στις ενδο-επιχειρησιακές λειτουργιές.

Στις μέρες μας, τα δεδομένα αποτελούν έναν από τους σημαντικότερους πόρους πολλών οργανισμών. Επομένως, η αποδοτική τους προσπέλαση, ο διαμοιρασμός τους, η εξαγωγή πληροφοριών από τα δεδομένα και η αξιοποίηση των πληροφοριών, έχει γίνει επιτακτική ανάγκη καταλυτικής σημασίας για την επιβίωση του ίδιου του οργανισμού ως οντότητα. Επίσης οι δυνατότητες που προσφέρει το διαδίκτυο, καθώς και οι εξελίξεις στο χώρο των δικτύων γενικότερα, έχουν επιφέρει επαναστατικές αλλαγές στον τρόπο πρόσβασης στα δεδομένα και στις πληροφορίες που ενδιαφέρουν έναν οργανισμό και όχι μόνο. Πλέον οι χρήστες μπορούν να έχουν πρόσβαση σε μεγάλο όγκο πληροφοριών, σε σύντομο χρονικό διάστημα και με ευκολότερο τρόπο. Όλα λοιπόν συνηγορούν στο ότι έχουμε εισέλθει σε μια νέα εποχή, όπου η πληροφορία διαδραματίζει καθοριστικό ρόλο ή ακόμη και πρωταγωνιστικό, για κάποιους ιδεαλιστές τεχνοκράτες.

Λύση στα παραπάνω θέματα προσφέρουν τα Συστήματα Ψηφιακής Αρχειοθέτησης και Διαχείρισης Εγγράφων (Document Management Systems). Μέσω αυτών, τα έγγραφα συλλέγονται, ψηφιοποιούνται, ταξινομούνται και αρχειοθετούνται σε αποθηκευτικά μέσα, από όπου, με το πάτημα ενός κουμπιού, μπορούν να ανακτηθούν, να προβληθούν και να εκτυπωθούν. Τα σημαντικά πλεονεκτήματα που απορρέουν από τη χρήση τους αποτελούν σημαντική παράμετρο καλής λειτουργίας ενός οργανισμού και τους προσδίδουν τον τίτλο της πλέον σύγχρονης και αποτελεσματικής προσέγγισης του προβλήματος της συσσώρευσης εγγράφων και της γραφειοκρατίας.

Από την άλλη πλευρά ο χρήστης που χρησιμοποιεί ένα τέτοιο σύστημα απαιτεί τα δεδομένα (π.χ. ένα μήνυμα ή ένα κείμενο) που χειρίζεται να μην μπορούν να αποκαλυφθούν ή να διατεθούν σε μη εξουσιοδοτημένα γι' αυτό άτομα (εμπιστευτικότητα). Επίσης να είναι μην δυνατόν να αλλοιωθούν κατά την μετάδοσή τους (ακεραιότητα). Επιπλέον, σε μία τέτοια διαδικασία, είναι απαραίτητο όποιος λαμβάνει τα δεδομένα να είναι σίγουρος για την ταυτότητα του δημιουργού (αυθεντικότητα). Τέλος, αυτός που έχει συντάξει ένα μήνυμα ή ένα κείμενο να μην μπορεί να αρνηθεί ότι είναι ο δημιουργός (μη αποποίηση ευθύνης). Σε όλα αυτά την λύση έρχεται να δώσει η ψηφιακή υπογραφή, που εφαρμόζοντας αρχές της θεωρίας αριθμών και της θεωρίας πολυπλοκότητας, οικοδομεί μια ανθεκτική και στέρεα κατασκευή τουλάχιστον για το προσεχές μέλλον.

Επίσης αν λάβουμε υπόψη, ότι η ζήτηση για δεδομένα συνεχώς αυξάνεται και ότι η επεξεργασία των δεδομένων παράγει χρήσιμες πληροφορίες - οικονομικής αξίας - για τους οργανισμούς, γίνεται ολοένα και κρισιμότερη η ανάγκη για διατήρηση της ασφάλειας στα μέσα που διαχειρίζονται αυτά τα δεδομένα και τις πληροφορίες, όπως είναι οι βάσεις δεδομένων, οι εφαρμογές και τα πληροφοριακά συστήματα. Χάρη στους διάφορους μηχανισμούς προστασίας και ανίχνευσης παρεισφρήσεων που αναπτύσσονται από επιχειρήσεις ασφάλειας δικτύων, δεν είναι πλέον εύκολο να παραβιαστούν οι περίμετροι ασφάλειας και να επιτευχθεί μη εξουσιοδοτημένη πρόσβαση στο δίκτυο ενός οργανισμού. Δυστυχώς όμως, οι κακόβουλοι συνεχώς αυξάνονται βελτιώνοντας παράλληλα τις μεθόδους τους.

Μια νέα προσέγγιση στο θέμα της ασφάλεια είναι η πολυεπίπεδη ασφάλεια, δηλαδή δεν δημιουργούμε ένα μεγάλο τείχος προστασίας αλλά πολλά διαδοχικά τείχη μεγάλης αντοχής, με σκοπό να κάμπτεται σταδιακά η επιθετική ισχύς των επίδοξων χάκερς. Επίσης η ίδια η ψηφιακή υπογραφή μπορεί να αποτελέσει από μόνη της επίπεδο ασφάλειας χρησιμοποιούμενη κατάλληλα στην δόμηση του πληροφοριακού συστήματος.

Μέσα από την ενοποίηση των τριών θεμάτων που αναφέραμε παραπάνω, προκύπτει σε μια ολοκληρωμένη ενότητα ένα σύστημα που διαθέτει τα πλεονεκτήματα όλων, ενώ παράλληλα εξουδετερώνει τις αδυναμίες των επιμέρους. Έτσι λοιπόν προκύπτει αυτό που θα παρουσιάσουμε αναλυτικά στην παρούσα εργασία, ένα σύστημα διαχείρισης εγγράφων πολυεπίπεδης ασφάλειας με ενσωματωμένη ψηφιακή υπογραφή.

ABSTRACT

It is generally known that computer science is rapidly developing in recent years. In this new era, companies, organizations, governments, and individuals are increased using applications based on information systems that are structured on networks. This option provides efficient, effective and cheaper solutions to the challenges of communication, in trade and in intra-operation.

Nowadays, data is one of the greatest resources of many organizations. Therefore, the efficient access, extraction of information from data and the use of information has become imperative of great importance for the survival of the organization itself as an entity. Also the potential of the Internet and developments in the networking area in general, have brought about revolutionary changes in the way of access to data and information of interest to an organization and beyond. Now users can have access to large volumes of information quickly and easily as possible. Everything indicates that we have entered in a new era where information plays a key role or even more leading role, for some idealistic technocrat.

Solution to these problems offered by the systems of digital archiving and document management systems. Through these documents are collected, digitized, sorted and stored in storage media, where at the touch of a button can be retrieved, viewed and printed. The major advantages of using them is an important aspect of good functioning of an organization and give them the title of the most modern and effective approach to the problem of accumulation of documents and related bureaucracy.

On the other hand, the user using such a system requires data (eg a message or a text) that handles cannot be disclosed or made available to unauthorized therefore persons (confidentiality). Also it is not possible to alter in their transmission (integrity). Moreover, such a procedure, it is necessary that receives the data to be sure of the identity of the author (accuracy). Finally, anyone who has written a message or a text cannot deny that he is the creator (no disclaimer). In all this the solution comes in the digital signature, that implementing the principles of number theory and complexity theory build a robust and solid construction at least for the foreseeable future.

Also considering that the demand for data is constantly growing and the processing of useful information - economic value - for organizations is becoming more critical need for maintaining security in the middle who manages data and information, such as databases, applications and information systems. Thanks to various protection mechanisms, intrusion detection developed by network security companies are no longer easy to violate security perimeters and achieve unauthorized access to the network of an organization. Unfortunately, malicious constantly increases while improving their methods.

A new approach to security is layered security that does not create a great firewall, but several successive heavy walls, designed to bend out the offensive power of the would-be hackers. Also, the same digital signature can be alone adequate level of security used in building the information system.

Through the integration of the three issues mentioned above shows a complete section a system that has all the advantages of overlap and eliminating the weaknesses of the individual. So what follows we will present in detail in this work is a document management system layered security with integrated digital signature.

ΕΥΧΑΡΙΣΤΙΕΣ

Οφείλω να εκφράσω τις θερμές μου ευχαριστίες στον επιβλέποντα καθηγητή κ. Αλεξανδρή Νικόλαο για την δυνατότητα που μου έδωσε να ασχοληθώ με ένα τόσο ενδιαφέρον θέμα. Η καθοδήγηση, η συνεργασία και η βοήθεια που απλόχερα μου πρόσφερε ήταν πολύτιμη για την ολοκλήρωση αυτής της μεταπτυχιακής εργασίας.

Επίσης, θα ήθελα να ευχαριστήσω τον κ. Πατσάκη Κωνσταντίνο για το χρήσιμο υλικό μελέτης και τη βοήθεια που μου προσέφερε καθ' όλη την διάρκεια της εργασίας μου.

Τέλος, ένα πολύ μεγάλο ευχαριστώ στους φίλους και τους συμφοιτητές μου που ήταν πάντα δίπλα μου σε όλη τη διάρκεια αυτής της επίμοχθης προσπάθειας.

Αλμαλής Νικόλαος

Πειραιάς, Φθινόπωρο 2010

Αφιερωμένο στη σύζυγο μου και στα
παιδιά μου για την στήριξη που μου
προσφέρουν σε κάθε βήμα της ζωής μου.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΙΝΑΚΑΣ ΣΧΗΜΑΤΩΝ

ΚΕΦΑΛΑΙΟ 1^{Ο}

ΕΙΣΑΓΩΓΗ

Στις μέρες μας, τα δεδομένα αποτελούν έναν από τους σημαντικότερους πόρους πολλών οργανισμών. Επομένως, η αποδοτική τους προσπέλαση, ο διαμοιρασμός τους, η εξαγωγή πληροφοριών από τα δεδομένα και η αξιοποίηση των πληροφοριών, έχει γίνει επιτακτική ανάγκη καταλυτικής σημασίας για την επιβίωση του ίδιου του οργανισμού ως οντότητα.

Επίσης οι δυνατότητες που προσφέρει το διαδίκτυο, καθώς και οι εξελίξεις στο χώρο των δικτύων γενικότερα, έχουν επιφέρει επαναστατικές αλλαγές στον τρόπο πρόσβασης στα δεδομένα και στις πληροφορίες, που ενδιαφέρουν έναν οργανισμό και όχι μόνο. Πλέον οι χρήστες μπορούν να έχουν πρόσβαση σε μεγάλο όγκο πληροφοριών, σε σύντομο χρονικό διάστημα και με ευκολότερο τρόπο. Όλα λοιπόν συνηγορούν στο ότι έχουμε εισέλθει σε μια νέα εποχή, όπου η πληροφορία διαδραματίζει καθοριστικό ρόλο ή ακόμη και πρωταγωνιστικό, για κάποιους ιδεαλιστές τεχνοκράτες.

Λαμβάνοντας υπόψη, ότι η ζήτηση για δεδομένα συνεχώς αυξάνεται και ότι η επεξεργασία των δεδομένων παράγει χρήσιμες πληροφορίες - οικονομικής αξίας - για τους οργανισμούς, γίνεται ολοένα και κρισιμότερη η ανάγκη για διατήρηση της ασφάλειας, στα μέσα που διαχειρίζονται αυτά τα δεδομένα και τις πληροφορίες, όπως είναι οι βάσεις δεδομένων, οι εφαρμογές και τα πληροφοριακά συστήματα. Με την εμφάνιση του παγκόσμιου ιστού, γίνεται ακόμα πιο σημαντική η προστασία των δεδομένων και των πληροφοριών, καθώς πολυάριθμα άτομα έχουν τώρα πρόσβαση σε αυτά. Χάρη στους διάφορους μηχανισμούς προστασίας και ανίχνευσης παρεισφρήσεων που αναπτύσσονται από επιχειρήσεις ασφάλειας δικτύων, δεν είναι πλέον εύκολο να παραβιαστούν οι περίμετροι ασφάλειας και να επιτευχθεί μη εξουσιοδοτημένη πρόσβαση στο δίκτυο ενός οργανισμού. Δυστυχώς όμως, κακόβουλοι προσπαθούν συνεχώς να επιτύχουν τους εγκληματικούς τους στόχους, ψάχνοντας να βρουν κενά ασφαλείας στις υποδομές των οργανισμών και να τις εκμεταλλευτούν προς όφελος των ιδίων ή προς όφελος τρίτων.

Από τα παραπάνω διαπιστώνουμε, ότι η ύπαρξη συστημάτων που θα επιτρέπουν στο σύνολο του προσωπικού ενός οργανισμού, να διαχειρίζεται δεδομένα και πληροφορίες, με τρόπο ασφαλή και συνάμα εύκολο και λειτουργικό, είναι αυτό που επιτάσσει η εποχή μας προς τους μηχανικούς ανάπτυξης λογισμικού. Ιδιαιτέρως, αυτό εμφανίζεται άκρως απαραίτητο σε στρατιωτικά περιβάλλοντα, όπου για τα

ελληνικά δεδομένα το γραφειοκρατικό σύστημα χρήζει επαναπροσδιορισμό και επομένως ένα ολοκληρωμένο πληροφορικό σύστημα διαχείρισης πληροφοριών θα μπορούσε να αποτελέσει μια λύση, ενώ από την άλλη πλευρά η ασφάλεια που θα παρείχε το σύστημα, καθόσον αυτή αποτελεί παράγοντα ζωτικής σημασίας σε πόλεμο αλλά και ειρήνη, θα πληρούσε τις προϋποθέσεις που υπαγορεύονται από τα σχετικά εγχειρίδια και κανονισμούς ασφαλείας.

1.1 Συστήματα διαχείρισης εγγράφων πολυεπίπεδης ασφάλειας με ενσωματωμένη ψηφιακή υπογραφή.

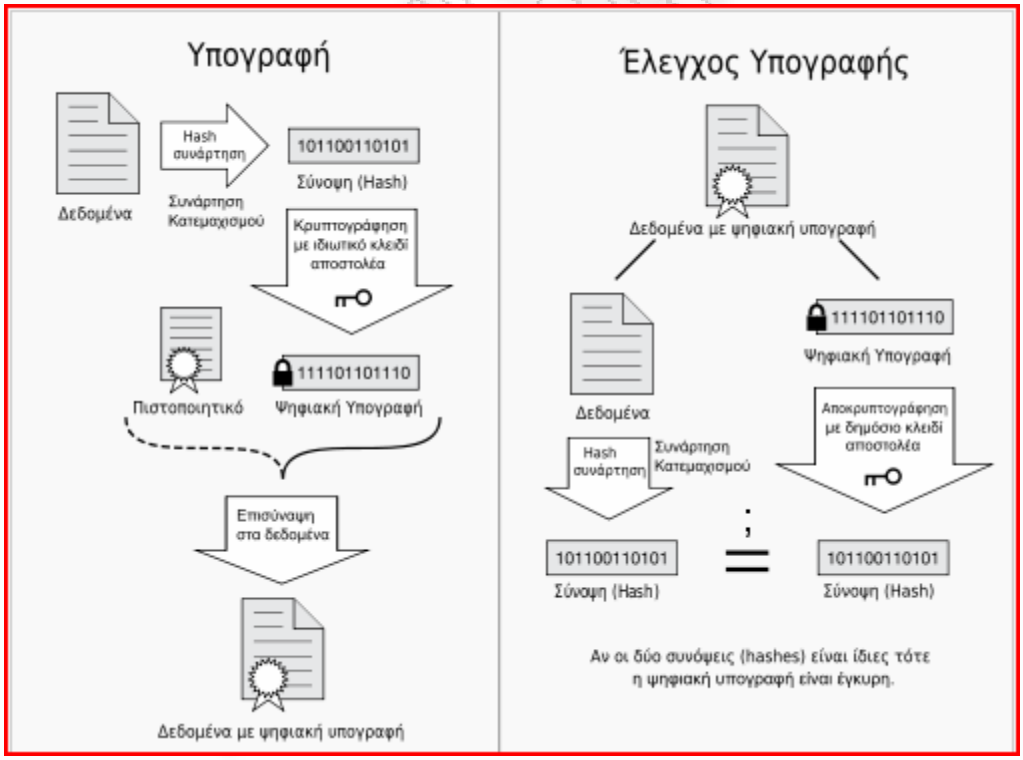
Σήμερα παρατηρούμε σε πολλούς κρατικούς οργανικούς ή μεγάλες εταιρείες, ιδιαίτερα στο εξωτερικό, να χρησιμοποιούνται συστήματα διαχείρισης εγγράφων, δηλαδή ολοκληρωμένα πληροφοριακά συστήματα εγκατεστημένα σε ένα σύνολο υπολογιστών, που είναι συνδεμένοι μεταξύ τους σε δίκτυο (LAN,WAN, intranet κ.α.), ώστε να αποτελούν ένα ενιαίο και αυτόνομο σύστημα επικοινωνίας και χρησιμοποιούνται από το προσωπικό του οργανισμού ή της εταιρείας για την παρακολούθηση και την αποθήκευση ηλεκτρονικών εγγράφων. Στην παρούσα εργασία τον όρο «ηλεκτρονικό έγγραφο» θα το χρησιμοποιήσουμε με την ευρύτερη έννοια του, δηλαδή θα αντιπροσωπεύει κάθε ψηφιακό αρχείο πχ αρχείο κειμένου, εικόνας, ήχου κ.α.

Ένα σύστημα διαχείρισης εγγράφων δύναται να βελτιστοποιήσει την απόδοση του φορέα που θα το αξιοποιήσει, διότι παρέχει σε ένα ολοκληρωμένο περιβάλλον, δυνατότητες, οι οποίες υπάρχουν στα λειτουργικά συστήματα των υπολογιστών, καθώς και σε διάφορες εφαρμογές χρήστη, όμως στέκονται μεμονωμένα και χωριστά. Αντίθετα οι δυνατότητες που παρέχονται από ένα ολοκληρωμένο σύστημα διαχείρισης εγγράφων και είναι οργανωμένες σε ένα ενιαίο, εύκολα χρησιμοποιήσιμο, σύνολο φαίνονται παρακάτω:

- Εργαλείο δημιουργίας ή επεξεργασίας του ψηφιακού αρχείου, πχ ένας κειμενογράφος, αν πρόκειται για διαχείριση αρχείων κειμένου
- Αποθήκευση των ψηφιακών αρχείων
- Πίνακας ιστορικού ενεργειών επί του αρχείου
- Διαχείριση εκδόσεων ψηφιακού αρχείου
- Δημιουργία μεταδεδομένων
- Δημιουργία ευρετηρίων
- Δυνατότητα ανάκτησης
- Ασφάλεια

Τελευταία στο λογισμικό των συστημάτων διαχείρισης εγγράφων έχει προστεθεί μια ακόμη πολύ σπουδαία δυνατότητα, εκείνη της ψηφιακής υπογραφής. Η ψηφιακή υπογραφή κερδίζει συνεχώς έδαφος και έτσι ενώ μέχρι τώρα είχαμε μόνο την χειρόγραφη υπογραφή πλέον στους περισσότερους φορείς υπάρχει και η ψηφιακή και σίγουρα στο μακρινό μέλλον θα απομείνει μόνο η ψηφιακή, όμως και εδώ η δυνατότητα αυτή στέκεται μεμονωμένα.

Η νέα αυτή δυνατότητα δεν αυξάνει μόνο ποσοτικά τον αριθμό των υπαρχουσών δυνατοτήτων αλλά τις βελτιώνει και ποιοτικά, πχ αυξάνει το επίπεδο ασφάλειας του συστήματος σημαντικά αλλά και την προστασία των αρχείων ως πνευματική ιδιοκτησία, εφόσον παρέχει εμπιστευτικότητα, ακεραιότητα, αυθεντικότητα και μη αποποίηση της ευθύνης. Βέβαια και σε άλλους τομείς η ψηφιακή υπογραφή συνεισφέρει τον καθόλου ευκαταφρόνητο οβολό της, όπως στην δημιουργία των μεταδεδομένων και στην αναζήτηση των αρχείων, θέματα που δεν είναι στο επίκεντρο ανάλυσης της παρούσης εργασίας, πάνω στα οποία όμως επιδρά καταλυτικά όσον αφορά την βελτίωση τους.



Σχήμα 1-1: Περιγραφή ψηφιακής υπογραφής και ελέγχου.
Πηγή: www.el.wikipedia.org

Η ασφάλεια σε ένα τέτοιο σύστημα διακρίνεται σε ψηφιακή και φυσική, η κάθε μια από τις οποίες έχει πολλές προεκτάσεις. Συγκεκριμένα για την φυσική υπάρχουν πλήθος εγχειριδίων που εξηγούν αναλυτικά τις σχετικές μεθόδους. Ομοίως και για την ψηφιακή ασφάλεια έχουν γραφεί πολλά, όμως συνεχώς εμφανίζονται νέοι τρόποι ή εντοπίζονται ψηφιακά κενά μέσω των οποίων εξαπολύουν τις ψηφιακές τους επιθέσεις κάποιοι με υψηλά συμφέροντα. Ο μόνος τρόπος για να δομηθεί επαρκής θωράκιση σε ψηφιακές οντότητες είναι η ύπαρξη επιπέδων ασφαλείας, που θα κλιμακώνονται σε βάθος και πλάτος με σκοπό την κάμψη της ισχύος του επιτιθέμενου.

Τελικά διαπιστώνουμε ότι ένα σύστημα διαχείρισης εγγράφων με ενσωματωμένη ψηφιακή υπογραφή είναι όχι μόνο μια τάση ή μόδα της εποχής αλλά μια λύση την οποία θα πρέπει να υιοθετήσουμε προκειμένου να αυξήσουμε το επίπεδο ασφάλειας, το οποίο σε κάποιους φορείς κατέχει εξέχουσα θέση, ιδιαιτέρως δε σε στρατιωτικά περιβάλλοντα είναι πρωτεύουσας σημασίας. Αυτό που προτείνουμε σαν λύση για την κάλυψη του υπάρχοντος κενού στον τομέα αυτό είναι η ανάπτυξη ενός συστήματος διαχείρισης εγγράφων πολυεπίπεδης ασφάλειας με ενσωματωμένη ψηφιακή υπογραφή.

1.2 Στόχος της εργασίας

Ο στόχος της παρούσας εργασίας είναι η ενσωμάτωση ψηφιακής υπογραφής σε συστήματα διαχείρισης εγγράφων, με σκοπό την ενίσχυση της υπάρχουσας ασφάλειας, μέσω της δημιουργίας διαφορετικών επιπέδων, που θα πηγάζουν από την ασφάλεια που παρέχει η ψηφιακή υπογραφή ως κρυπτογραφικό μέσο αλλά και από την εξασφάλιση της ίδιας της ψηφιακής υπογραφής ως οντότητας που πρέπει να διαφυλαχτεί. Τα επίπεδα ασφάλειας που θα δημιουργήσουμε είναι:

i. Η ύπαρξη μοναδικού usb memory stick για κάθε χρήστη που θα το παραλαμβάνει – χρεώνεται από τον διαχειριστή του συστήματος και θα περιέχει το ιδιωτικό κλειδί της προσωπικής του ψηφιακής υπογραφής.

ii. Η εξασφάλιση του περιεχομένου του usb memory stick με κρυπτογράφηση του, ώστε σε περίπτωση απώλειας να μην είναι δυνατή η ανάγνωση του ιδιωτικού κλειδιού.

iii. Μοναδικά στοιχεία για την είσοδο του χρήστη στο σύστημα (username-password).

iv. Για την είσοδο στο σύστημα απαιτείται η τοποθέτηση του προσωπικού usb memory stick.

v. Διασταύρωση στοιχείων χρήστη και ιδιωτικού κλειδιού ώστε να επιτρέψει το σύστημα την περεταίρω χρήση του.

vi. Δενδροειδής διάταξη φακέλων με δυνατότητα εφαρμογής δικαιωμάτων.

Τα παραπάνω επίπεδα ασφάλειας θα εξασφαλίζονται στην πλειοψηφία τους από το ίδιο το σύστημα με αυτόματο τρόπο αρκεί ο χρήστης να κατέχει το προσωπικό του usb memory stick με το ιδιωτικό του κλειδί το οποίο θα τοποθετεί στον υπολογιστή που εργάζεται και επίσης να γνωρίζει το username και password για την είσοδο του στο σύστημα.

1.3 Δομή της εργασίας

Η δομή της εργασίας είναι διαρθρωμένη με τρόπο που να αναπτύσσει εύληπτα τους τρεις άξονες στους οποίους στηρίζεται. Αυτοί οι τρεις κεντρικοί άξονες είναι: τα συστήματα διαχείρισης εγγράφων, η ψηφιακή υπογραφή και η πολυεπίπεδη ασφάλεια. Εύκολα λοιπόν αντιλαμβάνεται ο αναγνώστης την προέλευση του τίτλου που καλύπτει πλήρως τις τρεις διαστάσεις του θέματος. Ενοποιημένοι πλέον οι άξονες συνθέτουν μια νέα οντότητα στο χώρο της πληροφορικής.

Συγκεκριμένα στην εισαγωγή γίνεται μια σύντομη περιγραφή του συστήματος που αναπτύχθηκε και επίσης αναφέρονται τα κίνητρα και οι στόχοι, καθώς και η δομή της εργασίας, ώστε ο αναγνώστης μετά την εισαγωγή να μπορεί να επικεντρωθεί απευθείας σε όποιο κεφάλαιο επιθυμεί.

Έπειτα ο κάθε άξονας αναπτύσσεται και σε ένα κεφάλαιο, με τρόπο που να μπορούν αυτά τα τρία κεφάλαια να σταθούν ως αυτοτελής τμήματα, χωρίς παράλληλα να χάνουν την συνδεσιμότητας τους με το όλο θέμα της εργασίας.

Έτσι λοιπόν στο δεύτερο κεφάλαιο αναπτύσσεται και τεκμηριώνεται εκτενώς η ψηφιακή υπογραφή, στο τρίτο κεφάλαιο περιγράφονται λεπτομερώς τα συστήματα διαχείρισης εγγράφων κα τέλος στο τέταρτο κεφάλαιο αιτιολογείται η επιλογή της ασφάλειας πολλών επιπέδων.

Στη συνέχεια στο πέμπτο κεφάλαιο παρουσιάζεται η υλοποίηση της εφαρμογής. Αρχικά αναλύεται η δικτυακή υποδομή που απαιτείται για να λειτουργήσει μαζί με τα διάφορα τεχνικά μέσα που χρησιμοποιήθηκαν π.χ. γλώσσες προγραμματισμού, ενώ

στην συνέχεια παρουσιάζονται αναλυτικά πως αναπτύχθηκαν όλα τα επιμέρους τμήματα.

Στο έκτο κεφάλαιο σημειώνεται η συνεισφορά της εργασίας στην επιστήμη της πληροφορικής και συγκεκριμένα στην ψηφιακή ασφάλεια, ενώ παράλληλα θίγονται θέματα για προβληματισμό και μελλοντική μελέτη. Τέλος η εργασία ολοκληρώνεται με χρήσιμα συμπεράσματα που προέκυψαν από την επίπονη και επίμονη ενασχόληση του γράφοντα με το εν λόγω θέμα.

ΚΕΦΑΛΑΙΟ 2^{Ο}

ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ

Η ψηφιακή υπογραφή είναι μια ανάγκη που την δημιούργησε η εισχώρηση των ηλεκτρονικών υπολογιστών σε κάθε έκφανση της επιχειρηματικής και ιδιωτικής μας ζωής. Η παραδοσιακή χειρόγραφη υπογραφή είναι πλέον ανεπαρκής, αδυνατεί να καλύψει τις ανάγκες της νέα ψηφιακή πραγματικότητας και έτσι δίνει την θέση της σε μια νέα μορφή, την ψηφιακή υπογραφή, που διαθέτει περισσότερες δυνατότητες και λειτουργίες από τον προγονό της. Αρχικά θα παρουσιάσουμε την κρυπτογραφία δημοσίου κλειδιού, τις συναρτήσεις κατακερματισμού και έπειτα την ψηφιακή υπογραφή και θα κλείσουμε το κεφάλαιο περιγράφοντας τις διαστάσεις στις οποίες μπορεί να κινηθεί.

2.1 Κρυπτογραφία δημοσίου κλειδιού και RSA.

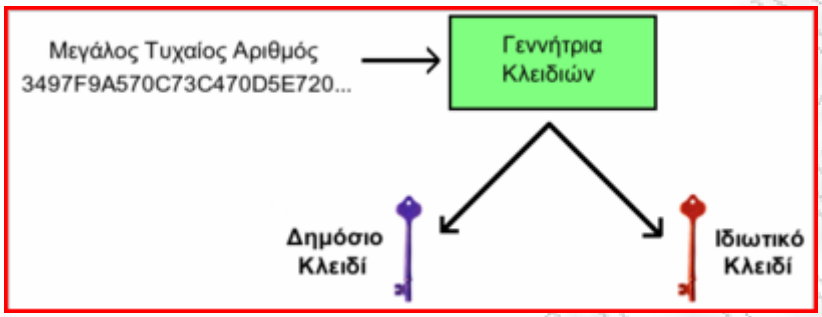
Γενικά για την κρυπτογράφηση δημοσίου κλειδιού.

Η κρυπτογράφηση δημοσίου κλειδιού (Public Key Cryptography) ή ασύμμετρου κλειδιού (Asymmetric Cryptography) επινοήθηκε στο τέλος της δεκαετίας του 1970 από τους Whitfield Diffie και Martin Hellman και παρέχει έναν εντελώς διαφορετικό μοντέλο χειρισμού των κλειδιών κρυπτογράφησης. Η βασική ιδέα είναι ότι ο αποστολέας και ο παραλήπτης δεν μοιράζονται ένα κοινό μυστικό κλειδί, όπως στην περίπτωση της κρυπτογράφησης συμμετρικού κλειδιού, αλλά διαθέτουν διαφορετικά κλειδιά για τις διαφορετικές λειτουργίες της κρυπτογράφησης και αποκρυπτογράφησης.

Συγκεκριμένα κάθε χρήστης διαθέτει δύο κλειδιά κρυπτογράφησης, το ένα ονομάζεται ιδιωτικό κλειδί (private key) και το άλλο δημόσιο κλειδί (public key). Το ιδιωτικό κλειδί θα πρέπει ο κάθε χρήστης να το προφυλάσσει από απώλεια ή κλοπή και επίσης να το κρατάει κρυφό από τρίτους, ενώ αντίθετα το δημόσιο κλειδί θα πρέπει να το ανακοινώνει σε όλη την διαδικτυακή κοινότητα. Ο τρόπος γνωστοποίησης του δημοσίου κλειδιού γίνεται από ειδικούς εξυπηρετητές δημοσίων κλειδιών (public key servers), στους οποίους μπορεί κανείς να απευθυνθεί για να βρει το δημόσιο κλειδί του χρήστη που τον ενδιαφέρει ή να ανεβάσει το δικό του δημόσιο κλειδί για να είναι διαθέσιμο στο κοινό για οποιοδήποτε έλεγχο.

Τα δύο αυτά κλειδιά (ιδιωτικό και δημόσιο) έχουν μαθηματική εξάρτηση μεταξύ τους. Εάν το ένα χρησιμοποιηθεί για την κρυπτογράφηση κάποιου μηνύματος, τότε το άλλο

χρησιμοποιείται για την αποκρυπτογράφηση του ίδιου μηνύματος. Η ευφυής σύλληψη αυτού του είδους κρυπτογραφικών αλγορίθμων βασίζεται στο γεγονός ότι η γνώση του δημόσιου κλειδιού κρυπτογράφησης δεν επιτρέπει με κανέναν τρόπο, σύμφωνα με τα υπάρχοντα δεδομένα, τον υπολογισμό του ιδιωτικού κλειδιού κρυπτογράφησης. Επίσης ο τρόπος που αναπαρίσταται ένα δημόσιο κλειδί π.χ. 1024 bits είναι μία ακολουθία αλφαριθμητικών χαρακτήρων [1].



Σχήμα 2-1: Δημιουργία δημοσίου και ιδιωτικού κλειδιού
Πηγή: www.el.wikipedia.org

Η κρυπτογράφηση δημοσίου κλειδιού λύνει ένα σημαντικότατο πρόβλημα που υπήρχε στους κρυπτογραφικούς αλγόριθμους συμμετρικού κλειδιού και ανοίγει νέους ορίζοντες στην σύγχρονη κρυπτογραφία και ασφάλεια. Συγκεκριμένα, οι κρυπτογραφικοί αλγόριθμοι συμμετρικού κλειδιού χρησιμοποιούν ένα κοινό μυστικό κλειδί, το οποίο το γνωρίζουν τόσο ο αποστολέας του κρυπτογραφημένου μηνύματος όσο και ο παραλήπτης. Αυτό το κοινό μυστικό κλειδί χρησιμοποιείται και κατά την διαδικασία της κρυπτογράφησης και κατά την διαδικασία της αποκρυπτογράφησης του μηνύματος.

Προκύπτει όμως ένα σοβαρό πρόβλημα στην περίπτωση που υποθέσουμε ότι το κανάλι επικοινωνίας δεν είναι ασφαλές. Δηλαδή όταν ο αποστολέας στείλει το κλειδί κρυπτογράφησης στον παραλήπτη για να μπορέσει αυτός με την σειρά του να αποκρυπτογραφήσει το μήνυμα, αν το κλειδί υποκλαπεί από κάποιον τρίτο, αυτό το τρίτο πρόσωπο θα μπορεί να αποκρυπτογραφεί μηνύματα αφού πλέον κατέχει το μυστικό κλειδί. Με άλλα λόγια υπάρχει μια αδυναμία στην παλαιά διαδικασία που περιγράψαμε παραπάνω. Αυτό το πρόβλημα είναι ιδιαίτερα έντονο στις σύγχρονες ψηφιακές επικοινωνίες όπου σε πολλές περιπτώσεις ο αποστολέας δεν γνωρίζει καν τον παραλήπτη και απέχει από αυτόν αρκετές χιλιάδες χιλιόμετρα. Οι κρυπτογραφικοί αλγόριθμοι δημοσίου κλειδιού ξεπερνούν αυτή την αδυναμία και

ανοίγουν νέους ορίζοντες για εφαρμογές κρυπτογράφησης όπως ηλεκτρονική αλληλογραφία, e-banking κ.α. .

Όσον αφορά την δημιουργία του δημόσιου και του ιδιωτικού κλειδιού αυτή γίνεται από ειδικές συναρτήσεις οι οποίες δέχονται ως είσοδο έναν μεγάλο τυχαίο αριθμό και στην έξοδο τους παράγουν το ζεύγος των κλειδιών (σχήμα 2-1). Είναι προφανές ότι όσο πιο τυχαίος είναι ο αριθμός που δίνεται ως είσοδος στην γεννήτρια κλειδιών τόσο πιο ασφαλή είναι τα κλειδιά που παράγονται. Σε σύγχρονα προγράμματα κρυπτογράφησης ο τυχαίος αριθμός παράγεται ως εξής: κατά την διαδικασία κατασκευής των κλειδιών, το πρόγραμμα σταματάει ένα μικρό χρονικό διάστημα π.χ. για 5 λεπτά και προτρέπει τον χρήστη να συνεχίσει να χειρίζεται τον υπολογιστή. Έπειτα για να παραγάγει τον τυχαίο αριθμό συγκεντρώνει, από τα 5 αυτά λεπτά που «περίμενε», τυχαία δεδομένα που εξαρτώνται από την συμπεριφορά του χρήστη, όπως κινήσεις ποντικιού, πλήκτρα που πατήθηκαν στο πληκτρολόγιο, κύκλοι μηχανής που καταναλώθηκαν κ.α. . Με βάση αυτά τα πραγματικά τυχαία δεδομένα υπολογίζεται ο τυχαίος αριθμός και εισάγεται στην γεννήτρια κλειδιών για να κατασκευαστεί το δημόσιο και το ιδιωτικό κλειδί του χρήστη.

Ο αλγόριθμος κρυπτογράφησης RSA.

Ο RSA είναι ένας αλγόριθμος κρυπτογράφησης ασύμμετρου κλειδιού, το όνομα του οποίου προέρχεται από τους δημιουργούς του Ron Rivest, Adi Shamir and Len Adleman. Ο RSA μπορεί να χρησιμοποιηθεί όχι μόνο για την κωδικοποίηση μηνυμάτων αλλά μπορεί επίσης να χρησιμοποιηθεί και για την ψηφιακή υπογραφή εγγράφων. Η ασφάλεια του RSA βασίζεται στην δυσκολία παραγοντοποίησης πολύ μεγάλων αριθμών, εκτενεστέρα θα αναφερθούμε στην ενότητα 2-4 για την ισχύ του αλγορίθμου. Επίσης για την λειτουργία του RSA όπως και κάθε αλγόριθμου κρυπτογράφησης ασύμμετρου κλειδιού χρησιμοποιούνται δυο κλειδιά, ένα δημόσιο κατά την διάρκεια της κρυπτογράφησης και ένα κρυφό για την αποκρυπτογράφηση.

Παρακάτω μπορούμε να δούμε τα βήματα που απαιτεί η δημιουργία κλειδιών και η οποία δομείται καθαρά πάνω σε ένα μαθηματικό υπόβαθρο:

1. Επιλέγουμε δυο μεγάλους τυχαίους πρώτους αριθμούς «p» και «q» έτσι ώστε $p \neq q$.
2. Υπολογίζουμε το $n=p*q$.
3. Υπολογίζουμε την τιμή $\Phi(n)=(p-1)(q-1)$.
4. Επιλέγουμε έναν αριθμό $e>1$ έτσι ώστε e και $\Phi(n)$ να είναι σχετικά πρώτοι.

5. Υπολογίζουμε τον αριθμό *d* έτσι ώστε d*e≡1 mod Φ(n).

Για την εύρεση πρώτων αριθμών χρησιμοποιούνται πιθανοθεωρητικοί αλγόριθμοι, ενώ οι πιο συνηθισμένες επιλογές για το e είναι το 3, 7 και 2^{16} + 1. Αντίθετα αν επιλεγούν μικροί αριθμοί οδηγούν σε γρηγορότερους υπολογισμούς αλλά μειώνεται ασφάλεια. Τέλος τα κλειδιά που προκύπτουν είναι, για το δημόσιο ο συνδυασμός των αριθμών (n,e) ενώ για το ιδιωτικό ο συνδυασμός των (n,d). Μπορούμε να δημοσιεύσουμε το πρώτο κλειδί (δημόσιο), δίνοντας έτσι την δυνατότητα σε οποιονδήποτε να μας στείλει κρυπτογραφημένα μηνύματα, που μόνο εμείς που διαθέτουμε το ιδιωτικό κλειδί μπορούμε να αποκρυπτογραφήσουμε [2].

Όσον αφορά την διαδικασία που ακλουθούμε για να κρυπτογραφήσουμε ένα μήνυμα που αντιπροσωπεύεται από έναν αριθμό «m» φαίνεται παρακάτω. Το κρυπτογραφημένο μήνυμα «c» υπολογίζεται με τον εξής τρόπο:

$$c=m^e \bmod n$$

δηλαδή χρειάστηκε πέρα από το μήνυμα «m» μόνο το δημόσιο κλειδί (n,e). Από την άλλη πλευρά εάν ληφθεί ένα κρυπτογραφημένο μήνυμα «c», για να διαβάσουμε το αρχικό μήνυμα εκτελούμε στον ακόλουθο υπολογισμό:

$$m=c^d \bmod n$$

δηλαδή ο παραλήπτης για να αποκρυπτογράφηση το κρυπτογραφημένο μήνυμα «c» χρησιμοποιεί μόνο το ιδιωτικό του κλειδί.

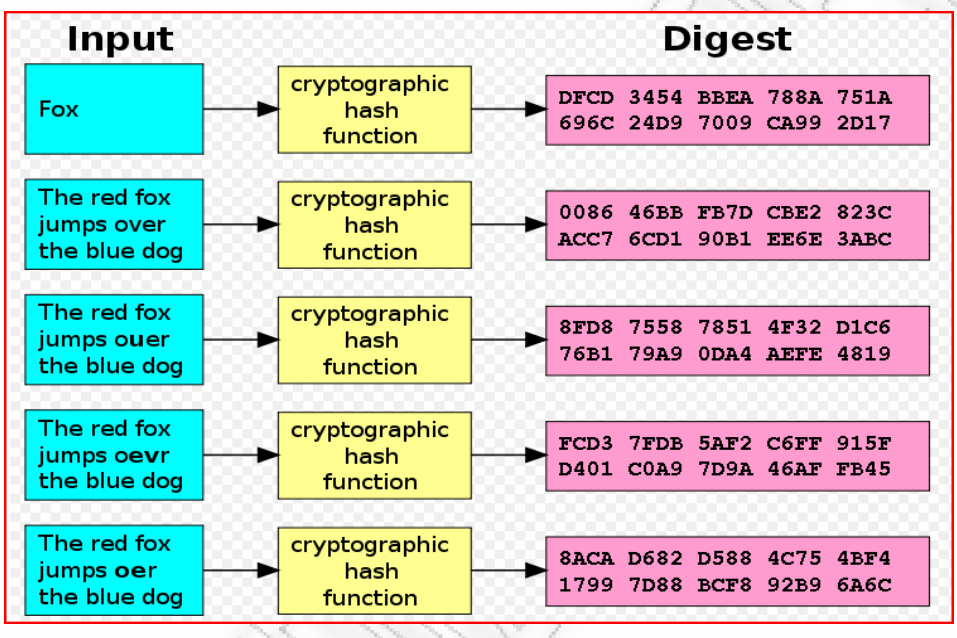
2.2 Συναρτήσεις κατακερματισμού και SHA1

Οι συναρτήσεις κατακερματισμού (hash functions) αποτελούν ένα πολύ σπουδαίο κρίκο στην αλυσίδα που ονομάζεται ασφάλεια, κατέχουν δε εξέχουσα θέση στην επιστήμη της κρυπτολογίας, δικαιολογημένα λοιπόν εμπλέκονται στην ψηφιακή υπογραφή εφόσον αυξάνουν και αυτές με την σειρά τους το επίπεδο ασφάλειας.

Τι είναι όμως συνάρτηση κατακερματισμού; Γιατί δημιουργήθηκαν; Πως επιτυγχάνουν τον σκοπό τους; Είναι μερικά ερωτήματα που θα προσεγγίσουμε στην συνέχεια με σκοπό να τεκμηριώσουμε τον λόγο που επιλέξαμε να χρησιμοποιήσουμε την συνάρτηση κατακερματισμού sha1 στην ανάπτυξη της εφαρμογής «Συστήματα διαχείρισης εγγράφων πολυεπίπεδης ασφάλειας με ενσωματωμένη ψηφιακή υπογραφή».

Η συνάρτηση κατακερματισμού SHA-1 σχεδιάστηκε από την NSA (National Security Agency) και δημοσιεύτηκε από την NIST ως U.S FIPS (Federal Information

Processing Standard), εφόσον αποδεδειγμένα καλύπτει τις προδιαγραφές SHS (Secure Hash Standards) που έχουν θέσει για τις συναρτήσεις κατακερματισμού. Η SHA-1 είναι μια ντετερμινιστική διαδικασία, κατά την οποία λαμβάνεται ως είσοδο ένα οποιοδήποτε μπλοκ δεδομένων και επιστρέφεται στη έξοδο μία σταθερού μεγέθους συμβολοσειρά. Η αξία της συνάρτησης κατακερματισμού έγκειται στο γεγονός ότι μια τυχαία ή σκόπιμη αλλαγή των δεδομένων θα άλλαζε την τιμή της έξοδο κατά τρόπο συνολικό και ολοκληρωτικό. Επίσης τα προς κωδικοποίηση στοιχεία αποκαλούνται «μήνυμα» ενώ το αποτέλεσμα της συνάρτησης «σύνοψη», αυτή την ορολογία θα χρησιμοποιούμε και στην παρούσα εργασία [3].



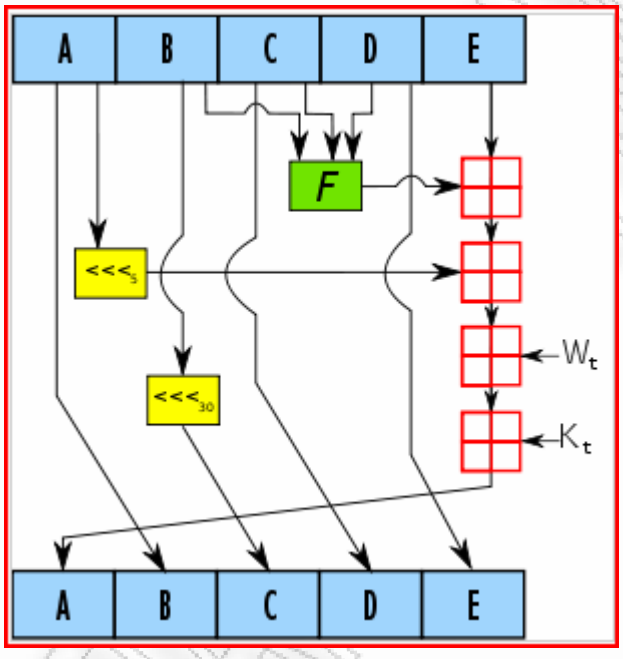
Σχήμα 2-2: Το αποτέλεσμα χιονοστιβάδας στον sha-1
Πηγή: www.wikipedia.org

Η ιδανική κρυπτογραφική συνάρτηση κατακερματισμού θα πρέπει να έχει τέσσερις βασικές ιδιότητες:

- Να είναι εύκολο να υπολογιστεί η τιμή της για οποιοδήποτε «μήνυμα».
- Να είναι ανέφικτο να βρεθεί ένα «μήνυμα» που να έχει μια δεδομένη τιμή.
- Να είναι ανέφικτο να τροποποιηθεί ένα «μήνυμα» χωρίς να αλλάξει η «σύνοψη» του.
- Να είναι ανέφικτο να βρεθούν δύο διαφορετικά «μηνύματα» με την ίδια «σύνοψη».

Όλα τα παραπάνω σίγουρα δεν έχουν κατορθώσει να επιτύχουν πολλές από τις μέχρι τώρα συναρτήσεις κατακερματισμού. Επίσης πολλοί επιστήμες ερευνούν νέες τεχνικές, προκειμένου να καταργήσουν τον μύθο της «ιδανικής συνάρτησης» που δόθηκε σε ορισμένες από αυτές από τους δημιουργούς τους. Πρόσφατα έγινε μία δημοσίευση από τους επιστήμονες Tao Xie του State Key Lab of Information Security, Chinese Academy of Sciences, Beijing, China και Dengguo Feng του The Center for Soft-Computing and Cryptology, NUDT, Changsha,China με τίτλο «How To Find Weak Input Differences For MD5 Collision Attacks», σύμφωνα με την οποία, πλέον η συνάρτηση κατακερματισμού MD5 δεν είναι ασφαλής.

Στην συνάρτηση κατακερματισμού SHA-1 παρατηρούμε το φαινόμενο της χιονοστιβάδας στο μέγιστο δυνατό βαθμό, όταν ένας και μόνο χαρακτήρας τροποποιείται τότε η σύνοψη που προκύπτει είναι τελείως διαφορετική, συγκεκριμένα στο παράδειγμα μας που φαίνεται στο σχήμα 2-2 αλλάζει μόνο ο χαραχτήρας «v» στην λέξη «over». Το αποτέλεσμα είναι ριζικά διαφορετικό.



Σχήμα 2-3: Μία επανάληψη στα πλαίσια λειτουργίας του SHA-1.
Πηγή: www.wikipedia.org

Η συνάρτηση κατακερματισμού SHA-1 αποτελεί μέρος πολλών ευρέως χρησιμοποιούμενων εφαρμογών ασφαλείας και πρωτοκόλλων, συμπεριλαμβανομένων: TLS (Transport Layer Security), SSL (Secure Socket Layer), PGP (Pretty Good Privacy), SSH (Secure Shell) κ.α., επιλέχτηκε μεταξύ ενός

αριθμού άλλων συναρτήσεων, διότι καλύπτει – τουλάχιστον μέχρι σήμερα – τις προδιαγραφές ασφάλειας που έχουμε θέση για την ανάπτυξη της εφαρμογής «Συστήματα διαχείρισης εγγράφων πολυεπίπεδης ασφάλειας με ενσωματωμένη ψηφιακή υπογραφή» στην παρούσα εργασία.

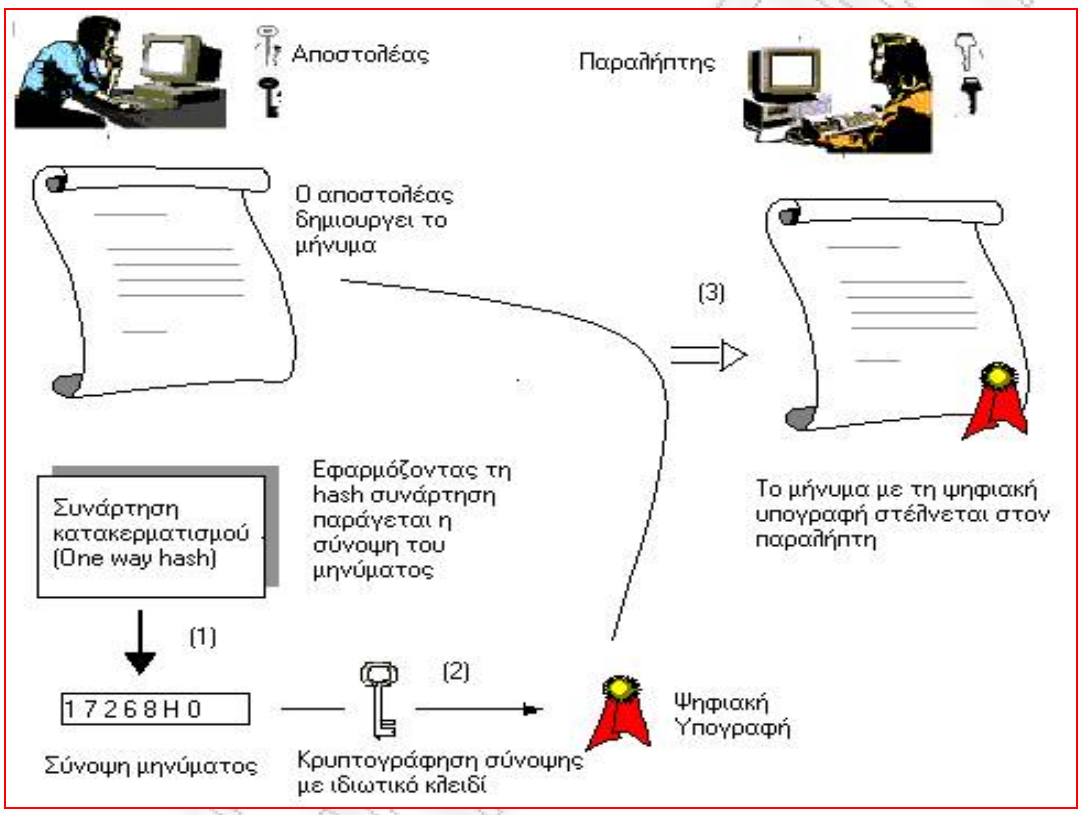
2.3 Θεωρητική προσέγγιση της ψηφιακής υπογραφής

Τι είναι όμως η υπογραφή αυτή; Δοσμένου ενός ηλεκτρονικού εγγράφου, η ψηφιακή του υπογραφή είναι μία πληροφορία που σχηματίζεται με βάση το έγγραφο και ενός προσωπικού αριθμού (ιδιωτικό κλειδί) του αποστολέα.

Ενώ η κλασική υπογραφή βασίζεται στο ότι ο γραφικός χαρακτήρας ενός ανθρώπου είναι απίθανο να μοιάζει με το γραφικό χαρακτήρα κάποιου άλλου, η ψηφιακή υπογραφή βασίζεται στο ότι ο προσωπικός αριθμός ενός ατόμου δεν δημοσιοποιείται σε άλλα άτομα, αλλά ούτε και είναι εύκολο να υπολογιστεί με κάποιον τρόπο. Όμως πώς μπορεί ένας αλγόριθμος κρυπτογραφίας δημόσιου κλειδιού, όπως είναι ο RSA που περιγράψαμε στην ενότητα 2.1, να χρησιμοποιηθεί για την πιστοποίηση της υπογραφής σε ηλεκτρονικά μηνύματα ή έγγραφα [2].

Αρχικά, σε καθέναν που επιθυμεί να χρησιμοποιήσει ηλεκτρονική υπογραφή αντιστοιχίζεται ένας μοναδικός αριθμός, η «ταυτότητα» του. Για να γίνει πιο κατανοητή η θεωρία της ψηφιακής υπογραφής θα χρησιμοποιήσουμε ένα πολύ αγαπητό παράδειγμα στους κύκλους της κρυπτογραφίας αυτό με την Αλίκη και τον Μπόμπο. Έστω ότι η Αλίκη θέλει να στείλει στον Μπόμπο ένα μήνυμα, με τέτοιον τρόπο ώστε ο Μπόμπος να καταλάβει ότι το μήνυμα προέρχεται από την Αλίκη και όχι από κάποιον άλλον που προσποιείται ότι είναι η Αλίκη. Αρχικά, η Αλίκη χρησιμοποιεί μία ειδική συνάρτηση κατακερματισμού (hash function) που αντιστοιχίζει το μήνυμα της σε ένα παραλλαγμένο μήνυμα συγκεκριμένου μήκους (και μικρότερου από το αρχικό). Στη συνέχεια, υπογράφει το παραλλαγμένο μήνυμα, δηλαδή το κρυπτογραφεί, με χρήση του αλγόριθμου RSA. Όμως εδώ είναι η ιδιομορφία, η κρυπτογράφηση αυτή γίνεται με βάση το *κρυφό* της κλειδί (ιδιωτικό). Όπως είχαμε αναφέρει στην ενότητα 2.1, στο σχήμα κρυπτογράφησης δημόσιου κλειδιού RSA τα μηνύματα κρυπτογραφούνται με βάση το δημόσιο κλειδί ενός χρήστη και αποκωδικοποιούνται με βάση το ιδιωτικό του κλειδί. Το να γίνουν αυτά αντίστροφα, όπως θα δούμε, είναι το μυστικό των ψηφιακών υπογραφών. Μετά από τα παραπάνω, η Αλίκη στέλνει στον Μπόμπο δύο πράγματα: την κωδικοποίηση της παραλλαγμένης έκδοσης του μηνύματος της και το αρχικό μήνυμα (το οποίο, εάν επιθυμεί, μπορεί να το κρυπτογραφήσει).

Ο Μπόμπος, τώρα, εφαρμόζει την ίδια συνάρτηση κατακερματισμού που είχε χρησιμοποιήσει η Αλίκη στο αρχικό της μήνυμα και χρησιμοποιώντας το δημόσιο κλειδί της αποκωδικοποιεί το κρυπτογραφημένο μέρος του μηνύματος της. Στη συνέχεια, ο Μπόμπος συγκρίνει τα δύο αποτελέσματα και, εάν είναι τα ίδια, αυτό σημαίνει ότι ο αποστολέας ήταν πράγματι η Αλίκη, καθώς μόνο αυτή μπορεί να έχει το αντίστοιχο κρυφό κλειδί που ταίριαξε με το δημόσιο κλειδί που χρησιμοποίησε ο Μπόμπος. Στο σχήμα που παραθέτουμε φαίνεται η όλη διαδικασία:



Σχήμα 2-4: Διαδικασία ψηφιακής υπογραφής και επαλήθευσης.
Πηγή: www.eett.gr

Ο χρήστης της ψηφιακής υπογραφής κρυπτογραφεί το μήνυμα του με το κρυφό του (ιδιωτικό) κλειδί. Ο λόγος που το κάνει αυτό είναι για να προσομοιώσει την υπογραφή με το χέρι, είναι σαν να βάζει στο ηλεκτρονικό έγγραφο κάτι που ανήκει μόνο σε αυτόν, που είναι άγνωστο και διαφορετικό στους άλλους, όπως είναι ο γραφικός του χαρακτήρας που είναι «έμφυτος» στην ιδιοσυγκρασία του, στην φυσιολογία της κίνησης του χεριού του. Αυτό το ξεχωριστό που προσθέτει είναι το κρυφό (ιδιωτικό) κλειδί του. Κάποιος άλλος που θα λάβει το κρυπτογραφημένο μήνυμα απλώς το αποκρυπτογραφεί με το δημόσιο κλειδί του χρήστη που το υπέγραψε. Σύμφωνα με

αυτά που αναφέραμε στην ενότητα 2-1, τα δύο κλειδιά, ιδιωτικό και δημόσιο, έχουν μία σχέση «αντίστροφου» μεταξύ τους, το ένα «αναιρεί» τη δράση του άλλου. Συνεπώς, σε ένα νόμιμο ιδιοκτήτη της ψηφιακής υπογραφής, η αποκρυπτογράφηση με το αντίστοιχο δημόσιο κλειδί θα αποκαλύψει το υπογεγραμμένο μήνυμα.

Οι ψηφιακές υπογραφές είναι μόνο μία από τις δυνατές εφαρμογές των σχημάτων κρυπτογράφησης δημόσιου κλειδιού, εκτός από την προφανή τους χρήση για κρυπτογράφηση δεδομένων. Υπάρχουν πάρα πολλές πιο ασυνήθιστες εφαρμογές, που δείχνουν το πόσες προεκτάσεις μπορεί να έχει μία απλή ιδέα κρυπτογράφησης, όπως αυτή στην οποία στηρίζεται το σχήμα RSA.

2.4 Η πηγή ισχύος της ψηφιακής υπογραφής

Η πηγή ισχύος της ψηφιακής υπογραφής σχετίζεται άμεσα με την ισχύ του αλγόριθμου RSA. Ο RSA είναι ασφαλής διότι η σημερινή υπολογιστική ισχύς καθιστά το πρόβλημα της παραγοντοποίησης του «n» - το «n» είναι το γινόμενο δυο τυχαίων μεγάλων πρώτων αριθμών (ενότητα 2-1) - δύσκολο ή καλύτερα πάρα πολύ χρονοβόρο να επιλυθεί, απατούνται χρόνια. Βέβαια η παραπάνω προσέγγιση ισχύει για μεγάλες τιμές του n. Διάφοροι επιστήμες που προσπάθησαν να «σπάσουν» το ασφαλέστερο, κατά τον δημιουργό του, αλγόριθμο κρυπτογράφησης, τελικά κατέληξαν στο συμπέρασμα πως η ασφάλεια είναι υπαρκτή μόνο κάτω από συγκεκριμένες προϋποθέσεις.

Με αυτό τον τίτλο «The magic words are squeamish ossifrage», το άρθρο των Derek Atkins, Michael Graff, Arjen Lenstra και Paul Leyland, το 1995 περιέγραφε μια διαδικασία που κλόνιζε την ανθεκτικότητα του σχήματος RSA απέναντι στις επιθέσεις παραγοντοποίησης του διαιρέτη. Επίσης το 1977, σε στήλη του περιοδικού «Scientific American», στην οποία αρθρογραφούσε ο Martin Gardner, γνωστός στην επιστημονική κοινότητα για την προσπάθεια του να αναδείξει την ομορφιά των μαθηματικών μέσα από σειρά εκλαϊκευμένων άρθρων και βιβλίων, ο Gardner είχε παρουσιάσει έναν αριθμό 129 δεκαδικών ψηφίων, ο οποίος είπε ότι ήταν γινόμενο δύο πρώτων αριθμών 64 και 65 ψηφίων αντίστοιχα [4]. Ο αριθμός 129 ψηφίων, ο RSA-129 όπως χαρακτηρίστηκε φαίνεται παρακάτω:

11438 1625 7578 8886 7669 2357 7997 6146 6120 1021 8296 7212 4236 2562 5618 4293 5706 9352 4573 3897 8305 9712 3563 9587 0505 8989 07514759 9290 0268 7954 3541

Ο αριθμός αυτός είναι ο δημόσιος διαιρέτης «n» του αλγόριθμου RSA και έστω ότι το δημόσιο κλειδί του χρήστη είναι (n,e) με *e* = 9007, ο εκθέτης στην κωδικοποίηση κατά RSA.Το πρόβλημα που έθεσε ο Martin Gardner ήταν να βρεθεί το μήνυμα που αντιστοιχεί στο κρυπτογραφημένο μήνυμα που φαίνεται παρακάτω:

9686 9613 7546 2206 1477 1409 2225 4355 8829 0575 9991 1245 7431 9874 2093 0816 2982 2514 3569 3147 6622 8839 8962 8013 3919 9055 1829 9451 5774 5154

Το αρχικό μήνυμα μετασχηματίστηκε σε δεκαδικό αριθμό μέσα από το μετα-σχηματισμό A=01, B=02,..., Z=26 και με το 00 να αντιστοιχεί στον κενό χαρακτήρα μεταξύ των λέξεων. Ο διαιρέτης έχει 129 δεκαδικά ψηφία και δίνεται ότι είναι το γινόμενο ενός πρώτου ακεραίου «p» 64 ψηφίων και ενός πρώτου ακεραίου «q» 65 ψηφίων, τέτοιων ώστε οι ακέραιοι «p-1» και «q-1» να είναι πρώτοι ως προς τον εκθέτη e. Εάν γίνουν γνωστά τα p και q, τότε το σχήμα «σπάει» και η αποκωδικοποί-ηση του μηνύματος είναι εύκολη.

Επίσης, ο Gardner είχε προσφέρει χρηματικό βραβείο 100 δολαρίων σε οποιονδήποτε κατόρθωνε να ανακαλύψει τους δύο αυτούς αριθμούς. Αυτό που ήταν ιδιαίτερα αποθαρρυντικό για τους φιλόδοξους κυνηγούς ήταν ότι ο Ronald Rivest, ένας από τους τρεις επινοητές του αλγόριθμου RSA, είχε εκτιμήσει την ίδια χρονιά ότι η παραγοντοποίηση ενός αριθμού 125 ψηφίων που είναι το γινόμενο δύο πρώτων αριθμών 63 ψηφίων θα χρειαζόταν τουλάχιστον 40 τετράκις εκατομμύρια χρόνια, χρησιμοποιώντας τον καλύτερο τότε γνωστό αλγόριθμο και υποθέτοντας ότι η ποσότητα:

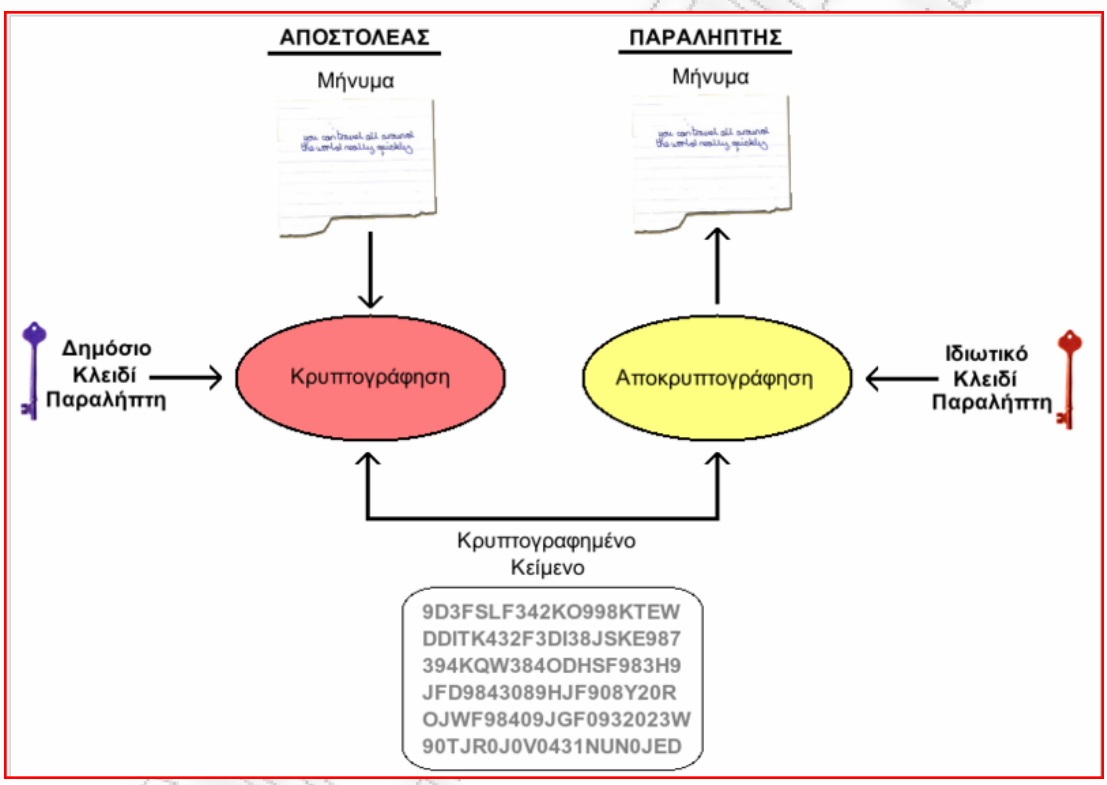
$$a*b \bmod c$$

δηλαδή το υπόλοιπο της διαίρεσης του *a*b* από το c, είναι δυνατό να υπολογιστεί μέσα σε 1 nanosecond για ακεραίους a, *b* και c 125 ψηφίων.

Τελικά τον Μάρτιο του 1994 το πρόβλημα του RSA-129 λύθηκε με την εύρεση των p και q, διαψεύδοντας τις αισιόδοξες προβλέψεις και ελπίδες ότι η παραγοντοποίηση ακεραίων τέτοιου μεγέθους ήταν πρακτικά αδύνατη. Η διαδικασία παραγοντοποίησης του RSA-129 συντελέστηκε μέσα σε μία περίοδο οκτώ μηνών και τεχνικά, επιτεύχθηκε με τον αλγόριθμο *quadratic sieve* [5]. Οι άνθρωποι που συνέβαλαν στους υπολογισμούς ήταν απλοί εθελοντές που διέθεσαν χρόνο των υπολογιστών τους κατά τη διάρκεια της νύχτας καθώς και τα Σαββατοκύριακα.

Συνολικά συμμετείχαν 600 εθελοντές με 1.600 συνολικά υπολογιστές και αποτέλεσαν το μεγαλύτερο στα χρονικά (μέχρι τότε) αναφερόμενο για ειδικό σκοπό *ιδεατό* πολυεπεξεργαστικό σύστημα. Αυτό είναι ένα μόνο κλάσμα του μεγέθους και

της δύναμης όλου του διαδικτύου. Μια έστω και χοντρική εκτίμηση της διαθέσιμης δύναμης είναι πολύ δύσκολη. Παρόλ' αυτά εάν υποθέσουμε ότι το διαδίκτυο απαρτίζεται από 3 εκατομμύρια υπολογιστές, η υπολογιστική ισχύς του είναι τόσο μεγάλη που εκτιμάται ότι μπορεί να παραγοντοποιηθεί ο ακέραιος RSA-129 μέσα σε 3 μόνο ώρες, εάν η ισχύς αυτή αφιερωθεί για το σκοπό αυτό. Το τελικό συμπέρασμα των ερευνητών που παραγοντοποίησαν τον RSA-129 ήταν ότι οι συνήθεις ακέραιοι των 512 bits που χρησιμοποιούνται σήμερα σε αρκετές εφαρμογές δεν είναι καθόλου ασφαλείς, απέναντι σε έναν οργανισμό που είναι διατεθειμένος να ξοδέψει εκατομμύρια δολάρια και να περιμένει μερικούς μήνες [6].



Σχήμα 2-5: Διαδικασία κρυπτογράφησης με αλγόριθμο δημοσίου κλειδιού.
Πηγή: www.el.wikipedia.org

Οι προσπάθειες παραγοντοποίησης μεγάλων αριθμών που γίνονται ακόμη και σήμερα, οδηγούν στο συμπέρασμα ότι ο αριθμός που θεωρείται δύσκολο να παραγοντοποιηθεί τώρα δεν είναι σίγουρο ότι θα είναι το ίδιο δύσκολο να παραγοντοποιηθεί και μετά από ορισμένα χρόνια. Βέβαια, μπορεί κανείς να πει ότι το μόνο που χρειάζεται είναι να επιλέγει κανείς όλο και μεγαλύτερα κλειδιά. Ίσως με το να επιλεγεί ένα υπερβολικά μεγάλο μήκος κλειδιού να καταστούν ασφαλή τα κλειδιά

των κρυπτογραφικών εφαρμογών για πάντα, στην πράξη, ένας αριθμός με 2.000 δεκαδικά ψηφία όχι μόνο θα ήταν αδύνατο να παραγοντοποιηθεί ακόμη και εάν επιστρατεύονταν όλοι οι υπολογιστές του κόσμου.

Τα πράγματα, όμως, δεν είναι τόσο απλά. Μεγάλο μήκος κλειδιού σημαίνει και αυξημένες υπολογιστικές απαιτήσεις για την κωδικοποίηση και αποκωδικοποίηση μηνυμάτων και δεν είναι πάντα εφικτό να είναι διαθέσιμη η ισχύς αυτή, ιδιαίτερα σε εφαρμογές πραγματικού χρόνου. Συνεπώς, η ρεαλιστική τακτική χειρισμού του μεγέθους του κλειδιού είναι να αφουγκράζεται κανείς τον τεχνολογικό παλμό της εποχής του και εκτιμώντας τα αντίστοιχα οικονομικά δεδομένα, να είναι σε θέση να εκτιμά ποιο είναι το καλύτερο δυνατό σύστημα που μπορεί να είναι εφικτό να κατασκευαστεί και να αγοραστεί, ώστε να προσδιορίσει το ελάχιστο μέγεθος κλειδιού που θα τον προφυλάξει για ένα ορισμένο χρονικό διάστημα.

2.5 Οι τέσσερις διαστάσεις στην εφαρμογή της ψηφιακής υπογραφής

Τα τελευταία χρόνια, τη θέση του εγγράφου και του συμβατικού ταχυδρομείου τείνει όλο και περισσότερο να καταλάβει το *ηλεκτρονικό αρχείο* και το *ηλεκτρονικό ταχυδρομείο* αντίστοιχα. Τα πιο πολλά έγγραφα που αποστέλλονται σήμερα ακόμη και από επίσημους φορείς, όπως είναι τα υπουργεία είναι σε ηλεκτρονική μορφή και φτάνουν στους παραλήπτες τους συνημμένα σε ένα ηλεκτρονικό μήνυμα (e-mail). Η ανάπτυξη του διαδικτύου, το ηλεκτρονικό εμπόριο και οι συναλλαγές μέσω ανοιχτών δικτύων κάνουν επιτακτική την ανάγκη ασφάλειας στις συναλλαγές και στις ανταλλαγές εγγράφων.

Ο χρήστης που συναλλάσσεται ηλεκτρονικά απαιτεί τα δεδομένα π.χ. ένα μήνυμα ή ένα κείμενο, που στέλνει να μην μπορούν να αποκαλυφθούν ή να διατεθούν σε μη εξουσιοδοτημένα γι αυτό άτομα (εμπιστευτικότητα).

Τα δεδομένα, δεν θα πρέπει να είναι δυνατόν να αλλοιωθούν κατά την μετάδοσή τους. Ο παραλήπτης θα πρέπει να τα λάβει όπως ακριβώς ο αποστολέας τα έστειλε και να είναι σίγουρος ότι τα δεδομένα που λαμβάνει είναι αυτά που ο αποστολέας έχει στείλει (ακεραιότητα).

Επιπλέον, σε μία τέτοια συναλλαγή, είναι απαραίτητο ο παραλήπτης να είναι σίγουρος για την ταυτότητα του αποστολέα (αυθεντικότητα). Δηλαδή, να γνωρίζει με σιγουριά ότι το μήνυμα που λαμβάνει και φαίνεται να το υπογράφει ο κ. Ν.Α., είναι όντως από τον κ. Ν.Α και όχι από κάποιον που παριστάνει τον κ. Ν.Α.

Τέλος, συμμετέχοντας σε μία ηλεκτρονική συναλλαγή π.χ. ηλεκτρονικό εμπόριο, θα πρέπει να μην είναι δυνατόν τα εμπλεκόμενα μέρη να αρνηθούν εκ των υστέρων την συμμετοχή τους στη συναλλαγή αυτή (μη αποποίηση ευθύνης).

Οι παραπάνω ιδιότητες εμπιστευτικότητα, ακεραιότητα, αυθεντικότητα, μη αποποίηση στον ηλεκτρονικό κόσμο, αποτελούν αντικείμενο της επιστήμης που ασχολείται με την ασφάλεια των πληροφοριών. Διάφοροι μηχανισμοί, τεχνικές και τεχνολογίες έχουν αναπτυχθεί αποσκοπώντας να διασφαλίσουν τις ιδιότητες αυτές σε μία ηλεκτρονική συναλλαγή, όχι μόνο οικονομική. Συγκεκριμένα η ψηφιακή υπογραφή μπορεί και δίνει απάντηση και στα τέσσερα παραπάνω θέματα και καλύπτει πλήρως τις απαιτήσεις που τίθενται στα σύγχρονα επιχειρησιακά πεδία. Βασιζόμενοι σε αυτήν την φιλοσοφία ενσωματώσαμε την ψηφιακή υπογραφή σε ένα σύστημα διαχείρισης εγγράφων με σκοπό να παρέχουμε την δυνατότητα στον χρήστη, τα έγγραφα που συντάσσει και αποστέλλει ή που δέχεται, να διέπονται από τις τέσσερις βασικές ιδιότητες που αναπτύχθηκαν παραπάνω [7].

ΚΕΦΑΛΑΙΟ 3^{Ο}

ΣΥΣΤΗΜΑΤΑ ΔΙΑΧΕΙΡΗΣΗΣ ΕΓΓΡΑΦΩΝ

Στις αρχές της δεκαετίας του ’80 κάνουν δειλά τα πρώτα τους βήματα τα συστήματα που διαχειρίζονται έγγραφα. Τα συστήματα αυτά διαχειρίζονται το έντυπο υλικό που χρησιμοποιείται από οργανισμούς και το οποίο δεν περιλαμβάνει μόνο έγγραφα που περιέχουν κείμενο αλλά και άλλες μορφές εγγράφων που χρησιμοποιούν χαρτί όπως οι φωτογραφίες, τα περιοδικά, οι εφημερίδες κ.α. .

Αργότερα, αρχίζουν να επεκτείνονται οι δυνατότητες και το πεδίο δράσης αυτών των συστημάτων με αποτέλεσμα να εμφανιστούν τα πρώτα συστήματα για τη διαχείριση των ηλεκτρονικών εγγράφων, όπως αρχικά ονομάστηκαν. Όλα αυτά τα ηλεκτρονικά έγγραφα που ουσιαστικά αποτελούσαν ψηφιακά αρχεία, δημιουργούνταν σε υπολογιστές και απαιτούνταν η αποθήκευση τους σε κάποιο σύστημα αρχείων, ώστε να έχουν πρόσβαση όσοι χρήστες ήταν κατάλληλα εξουσιοδοτημένοι. Αυτά τα πρώτα συστήματα διαχείρισης ηλεκτρονικών αρχείων κατασκευάζονταν για να καλύπτουν τις ανάγκες ενός τύπου αρχείου, αυτόν που χρησιμοποιούσε ένας οργανισμός στην ηλεκτρονική του καθημερινότητα ή λίγο αργότερα κάλυπτε ένα περιορισμένο αριθμό τύπων αρχείων με σχετική συνάφεια μεταξύ τους.

Τελικά φθάνουμε στα σημερινής μορφής συστήματα διαχείρισης εγγράφων, λαμβάνοντας παράλληλα και την σημερινή τελική τους ονομασία, βέβαια με λιγότερες λειτουργιές από τα σύγχρονα, που όμως υποστήριζαν τις τέσσερις βασικές δυνατότητες: σάρωση, αρχειοθέτηση, αναζήτηση, πρόσβαση. Επίσης τα συστήματα αυτά έχουν εξελιχθεί σε τέτοιο σημείο που δομούνται πάνω σε δίκτυα με κεντρικά μέσα αποθήκευσης για όλους τους σταθμούς εργασίας, με διάφορα εργαλεία συνεργασίας με άλλες εφαρμογές, με αυξημένη ασφάλεια και βελτιωμένες δυνατότητες ελέγχου.

Ο λόγος που έγιναν όλα αυτά τα βήματα ήταν γιατί ο τρόπος συλλογής, ταξινόμησης και επεξεργασίας των εγγράφων επηρεάζει σε μεγάλο βαθμό τη λειτουργία μιας επιχείρησης. Όταν οι εργασίες αρχειοθέτησης πραγματοποιούνται με τον παραδοσιακό "χειροκίνητο" και χειρόγραφο τρόπο, τότε τα προβλήματα είναι αναπόφευκτα. Σοροί εγγράφων, στοιβαγμένοι με τρόπο δυσλειτουργικό, παραπεταμένοι σε κάποιο χώρο που χαρακτηρίζεται ως αρχείο ή έστω τακτοποιημένοι σε κάποιο ντουλάπι, συνθέτουν μια κατάσταση, η οποία αποτελεί ξεκάθαρα τροχοπέδη στην εύρυθμη επιχειρηματική λειτουργία. Οι εργαζόμενοι αναγκάζονται συχνά να αναζητούν επί ώρα κάποιο λιγότερο ή περισσότερο

σημαντικό έγγραφο, με αποτέλεσμα να χάνεται πολύτιμος χρόνος, να μειώνεται η παραγωγικότητα και να παρατηρούνται δυσλειτουργίες στις εσωτερικές και εξωτερικές συναλλαγές της επιχειρήσεις.

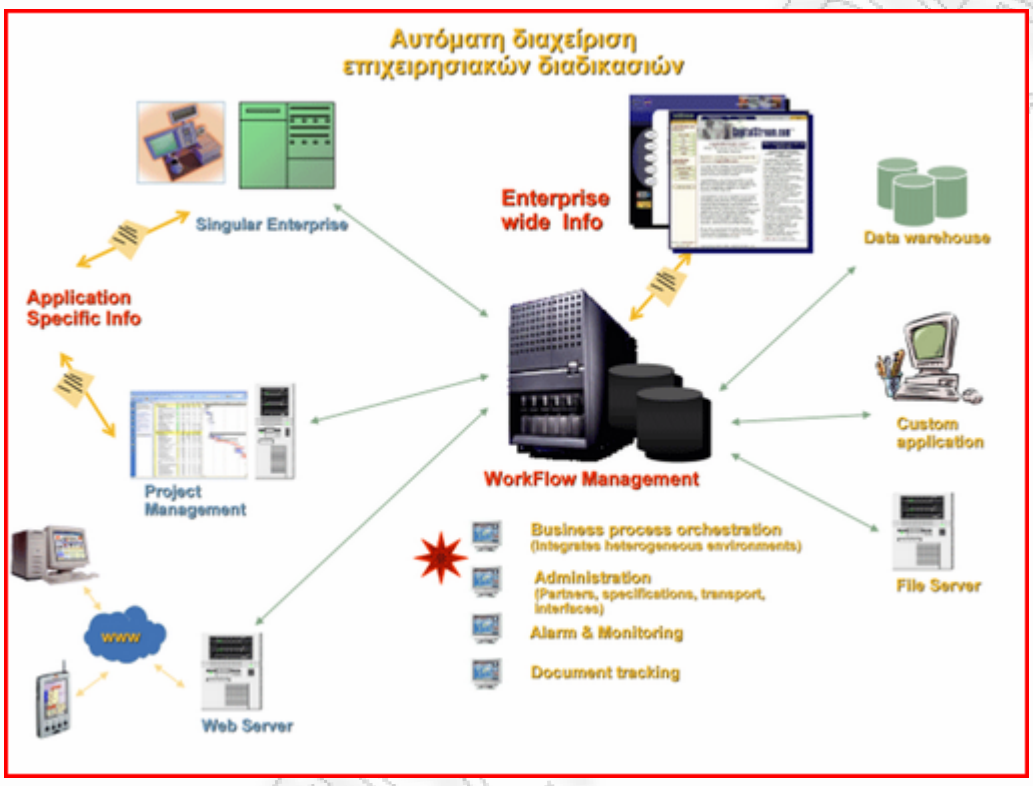
Λύση στα παραπάνω προβλήματα προσφέρουν τα Συστήματα Ψηφιακής Αρχειοθέτησης και Διαχείρισης Εγγράφων (Document Management Systems). Μέσω αυτών τα έγγραφα συλλέγονται, ψηφιοποιούνται, ταξινομούνται και αρχειοθετούνται σε αποθηκευτικά μέσα, από όπου, με εύκολο και γρήγορο τρόπο, μπορούν να ανακτηθούν, να προβληθούν και να εκτυπωθούν. Τα σημαντικά πλεονεκτήματα που απορρέουν από τη χρήση τους αποτελούν σημαντική παράμετρο καλής λειτουργίας ενός εταιρικού μηχανισμού και τους προσδίδουν τον τίτλο της σύγχρονης και αποτελεσματικής προσέγγισης του προβλήματος της συσσώρευσης εγγράφων και της γραφειοκρατίας.

3.1 Τι είναι το Σύστημα Διαχείρισης Εγγράφων

Για να δούμε όμως πως οι ειδικοί έχουν σύνθεση τον ορισμό των Συστημάτων Διαχείρισης Εγγράφων; Παρατηρούμε λοιπόν ότι προσεγγίζουν τα συστήματα αυτά ως συνώνυμα της αρχειοθέτησης και της διαχείρισης εγγράφων, φωτογραφιών, σχεδίων, αρχείων πολυμέσων, βίντεο, ήχου, ιστοσελίδων κ.λπ. με ηλεκτρονικό τρόπο [8]. Έχουν αναπτυχθεί για να αντικαταστήσουν τα παραδοσιακά μέσα (χειροκίνητη - χειρόγραφη αρχειοθέτηση), που μεταφράζονται σε ογκώδεις ντουλάπες, στοίβες φακέλων και φθαρμένα από την πάροδο του χρόνου έγγραφα. Η σύγχρονη μέθοδος που εισάγει η καινοτόμος ιδέα στην χρήση των υπολογιστών συνίσταται σε εικονικά ψηφιακά «συρτάρια και ντουλάπες» και σε έγγραφα που βρίσκονται σε ηλεκτρονική μορφή σε κάποιον server ή δίσκο, μαγνητικό ή οπτικό. Η ψηφιακή αρχειοθέτηση και διαχείριση τις οποίες επιτελούν τα συστήματα διαχείρισης εγγράφων, βασίζονται σε δύο άξονες στην υποδομή (hardware): servers, επεξεργαστές, αποθηκευτικά μέσα, σαρωτές και στο κατάλληλο λογισμικό (software) που αρχειοθετεί και διαχειρίζεται τα έγγραφα.

Παρ' όλα τα θετικά στοιχεία που υπόσχεται αυτή η νέα βελτιωμένη έκδοση των συστημάτων διαχείρισης εγγράφων, η ιδέα αυτή ιδιαίτερα στον ελληνικό χώρο δεν έχει απασχολήσει και πάρα πολλούς οργανισμούς, πλην ορισμένων εξαιρέσεων όπως τράπεζες και νοσοκομεία, και ελάχιστα έως καθόλου μικρομεσαίες επιχειρήσεις. Ωστόσο, την τελευταία πενταετία τα επιχειρήματα και οι «φωνές» που υποστηρίζουν την ενσωμάτωση ενός συστήματος διαχείρισης εγγράφων στην επιχείρηση κερδίζουν συνεχώς έδαφος. Αφενός το διεθνές εταιρικό οργανωτικό

μοντέλο, όπου τα συστήματα αυτά βρίσκονται σε περίοπτη θέση, αφετέρου ο όγκος του χαρτιού που αυξάνει απειλητικά, φυσική εξέλιξη της πορείας του χρόνου και της αύξησης του μεγέθους των επιχειρήσεων και ο επίσης ολοένα αυξανόμενος χρόνος που δαπανούν οι εργαζόμενοι για αρχειοθέτηση και διαχείριση εγγράφων, οδηγούν στην ανάγκη εξεύρεσης λύσεων που θα θεραπεύσουν τα προβλήματα.



Σχήμα 3-1: Αυτόματη διαχείριση επιχειρησιακών διαδικασιών
πηγη:http://www.bluedev.eu/t2c/Technology/PLMManagement/eFabmetal/tabid/118/language/en-US/Default.aspx

Προβλήματα καθημερινά και συνηθισμένα, τα οποία αποκαλύπτουν την πραγματική διάσταση, την ουσία της διαχείρισης εγγράφων όταν αυτή πραγματοποιείται με τον παραδοσιακό τρόπο. Η ουσία είναι ότι αποτελεί μια εργασία που δεν αποφέρει έσοδα, δεν σχετίζεται με τη στρατηγική, δεν εξοικονομεί πόρους, αλλά παρ' όλα αυτά απαιτεί τουλάχιστον το 1/5 του χρόνου των εργαζομένων. Όπως έχουν καταδείξει σχετικές έρευνες, ένας υπάλληλος τεχνικού γραφείου, για παράδειγμα, ο οποίος χρησιμοποιεί την παραδοσιακή μέθοδο αρχειοθέτησης, δαπανά ημερησίως από μία έως μιάμιση ώρα για να αναζητήσει και να εντοπίζει κάποιο έγγραφο, να καταχωρήσει κάποιο καινούργιο κ.α. . Άλλοι εργαζόμενοι, που η καθημερινότητά τους

συνδέεται στενά με υψηλό όγκο εγγράφων, χωρίς αυτό να είναι το αποκλειστικό τους καθήκον αναφέρουν ακόμα μεγαλύτερη σπατάλη χρόνου.

Είναι λοιπόν είναι φανερό ότι η διαχείριση εγγράφων με το παραδοσιακό τρόπο συνιστά «φύρα» και λειτουργικό έξοδο, η διαχείριση του οποίου πρέπει να τίθεται στη βάση του πώς θα υλοποιηθεί στο λιγότερο δυνατό χρόνο και με το μικρότερο δυνατό κόστος. Πέραν αυτού, τα συστήματα διαχείρισης εγγράφων μεταμορφώνουν την αρχειοθέτηση και τα έγγραφα από αναγκαίο κακό σε πολύτιμο πληροφοριακό υλικό και βάση για τη λήψη των αποφάσεων σε επιχειρηματικό πλαίσιο [8].

3.2 Δομή λειτουργίας ενός συστήματος διαχείρισης εγγράφων.

Η λειτουργία των συστημάτων Ψηφιακής Διαχείρισης Εγγράφων ξεκινά από ένα φυσικό έντυπο έγγραφο, το οποίο πρέπει πρώτα να ψηφιοποιηθεί και κατόπιν να εισαχθεί στο σύστημα, και φθάνει μέχρι την ανάκτηση ενός ψηφιακού εγγράφου που πρέπει να εντοπιστεί, να προβληθεί στην οθόνη και να εκτυπωθεί, αλλά και ακόμα περαιτέρω. Ας πάρουμε για παράδειγμα μία προσφορά, από τις πολλές που εκδίδει καθημερινά μια εμπορική επιχείρηση προς υποψήφιους πελάτες. Με τον παραδοσιακό τρόπο θα έπρεπε ο υπάλληλος να πάρει το αντίγραφο της προσφοράς, να ανοίξει το ντουλάπι ή το συρτάρι, να βρει κάποιο από τα ντοσιέ που καταχωρεί τις προσφορές και να καταχωρίσει το έγγραφο στη σωστή σειρά. Αν στο μέλλον θελήσει να ανασύρει το ίδιο έγγραφο θα πρέπει να ακολουθήσετε την αντίστροφη πορεία.

Η ίδια διαδικασία μέσα από κάποιο σύστημα διαχείρισης εγγράφων είναι κατά πολύ ταχύτερη. Το καινούργιο φυσικό έντυπο έγγραφο σαρώνεται μέσω ενός οπτικού αναγνώστη χειρός και αυτόματα καταχωρείται στο σύστημα, σε συγκεκριμένη θέση με βάση τις παραμέτρους που έχουν τεθεί. Μέσα σε λίγα δευτερόλεπτα είναι δυνατή και η αναζήτηση κάποιου εγγράφου, η προβολή του στην οθόνη και η εκτύπωσή του. Το σύστημα εντοπίζει το έγγραφο που αναζητά ο υπάλληλος ανάμεσα σε εκατοντάδες ή χιλιάδες παρόμοια έγγραφα και το εκτυπώνει αφού δοθεί η σχετική εντολή.

Τα περισσότερα συστήματα διαχείρισης εγγράφων επιτελούν τουλάχιστον 4 βασικές λειτουργίες [9]:

i. *Σάρωση* οποιουδήποτε φυσικού εγγράφου μέσω συσκευής χειρός ή επιτραπέζια, με ταυτόχρονη ψηφιοποίηση, εισαγωγή στο σύστημα και αποθήκευση σε σκληρούς, μαγνητικούς ή οπτικούς δίσκους.

ii. *Αρχειοθέτηση* του εγγράφου βάσει των κριτηρίων που θέτει ο ίδιος ο χρήστης και συνοδεία σχετικών πληροφοριών όπως: ημερομηνία καταχώρησης, είδος, περίληψη εγγράφου κ.α.

iii. *Αναζήτηση* καταχωρημένων εγγράφων με διάφορα κριτήρια και εντοπισμός τους σε πολύ μικρό χρόνο.

iv. *Πρόσβαση* και προβολή του επιθυμητού εγγράφου, εκτύπωση, αποστολή με φαξ ή με ηλεκτρονικό ταχυδρομείο.

Για να δούμε όμως αναλυτικά όλες τις λειτουργίες που μπορούμε να συναντήσουμε σε ένα σύστημα διαχείρισης εγγράφων, βέβαια δεν υπάρχει ένα τέτοιο σύστημα που να περιλαμβάνει όλα αυτά μαζί, παρόλ' αυτά σε ένα εξιδανικευμένο σύστημα μιας φανταστικής επιχείρησης θα μπορούσαμε να δούμε όλες τις παρακάτω λειτουργίες.

Σάρωση

Η σάρωση περιλαμβάνει κατά κύριο λόγο την αποδοχή και επεξεργασία των εικόνων των εγγράφων (σε χαρτί) από σαρωτές ή εκτυπωτές πολλαπλών λειτουργιών. Το λογισμικό οπτικής αναγνώρισης χαρακτήρων (OCR) που χρησιμοποιείται συχνά, είτε ενσωματωμένο στο υλικό είτε ως αυτόνομο λογισμικό, μετατρέπει τις ψηφιακές εικόνες σε αναγνώσιμο και κατ' επέκταση επεξεργάσιμο κείμενο από τον υπολογιστή. Το λογισμικό οπτικής αναγνώρισης σήματος (OMR), χρησιμοποιείται για να εξάγονται τιμές από τα πλαίσια ελέγχου ή από φυσαλίδες ερωτηματολογίου ή κατάλληλα διαμορφωμένου κειμένου. Η σάρωση μπορεί επίσης να αφορά την αποδοχή των ηλεκτρονικών εγγράφων και άλλων ψηφιακών αρχείων τα όποια χειρίζονται υπολογιστές.

Μεταδεδομένα

Τα μεταδεδομένα είναι πληροφορίες που αποθηκεύονται για κάθε έγγραφο. Τα μεταδεδομένα μπορούν, για παράδειγμα, να περιλαμβάνουν την ημερομηνία δημιουργίας του εγγράφου ή και τα στοιχεία ταυτότητας του χρήστη. Το σύστημα διαχείρισης εγγράφων μπορεί επίσης να εξαγάγει τα μεταδεδομένα από το έγγραφο αυτόματα ή έπειτα από εντολή του χρήστη να προσθέτει μεταδεδομένα. Επίσης μερικά συστήματα χρησιμοποιούν οπτική αναγνώριση χαρακτήρων για σαρωμένες εικόνες εγγράφων ή εκτελούν εξαγωγή κειμένου για τα ηλεκτρονικά έγγραφα. Το αποτέλεσμα που είναι ένα συμπίλημα του κείμενου μπορεί να χρησιμοποιηθεί για να βοηθήσει τους χρήστες στον εντοπισμό των εγγράφων με την αναζήτηση λέξης-κλειδί ή ακόμη και δυνατότητα αναζήτησης κειμένου. Αποσπασματικό κείμενο μπορεί επίσης να αποθηκευτεί ως μεταδεδομένο.

Ολοκληρωμένη διαχείριση

Πολλά συστήματα διαχείρισης εγγράφων ενσωματώνονται απευθείας σε άλλες εφαρμογές, ώστε οι χρήστες να μπορούν να ανακτούν τα υπάρχοντα έγγραφα από τον χώρου αποθήκευσης του συστήματος διαχείρισης εγγράφου, να κάνουν αλλαγές και να αποθηκεύουν το έγγραφο ως νέα έκδοση και όλα αυτά χωρίς την έξοδο από την εφαρμογή. Η λειτουργία αυτή είναι συνήθως διαθέσιμη για σουίτες γραφείου, e-mail ή λογισμικό groupware. Η ολοκληρωμένη διαχείριση συχνά χρησιμοποιεί ανοικτά πρότυπα, όπως ODMA, LDAP, WebDAV και SOAPto τα οποία επιτρέπουν την ενσωμάτωση με άλλα λογισμικά και την τήρηση των εσωτερικών ελέγχων.

Δημιουργία ευρετηρίων

Η δημιουργία ευρετηρίων μπορεί να είναι μια απλή υπόθεση που αφορά την παρακολούθηση ενός μοναδικού στοιχείου που ταυτοποιεί το έγγραφο, όμως συχνά παίρνει μια πιο σύνθετη μορφή λόγω της πολυπλοκότητας των μεταδεδομένων, τα οποία περιλαμβάνουν ένα πλήθος στοιχείων. Οπότε τα στοιχεία αυτά πρέπει ταξινομηθούν βάσει των διαφορετικών πεδίων που χαρακτηρίζουν το έγγραφο. Η ευρετηρίαση υπάρχει κυρίως για την υποστήριξη της ανάκτησης, ένας τομέας ζωτικής σημασίας για έναν οργανισμό εφόσον άπτεται του θέματος του χρόνου.

Αποθήκευση

Η αποθήκευση των εγγράφων είναι ένα πολύ σπουδαίο κεφάλαιο που συχνά περιλαμβάνει και τη διαχείριση των ίδιων των εγγράφων, ως οντοτήτων. Συγκεκριμένα αφορά πέρα από την αποθήκευση, το χρονικό διάστημα που θα αποθηκευτούν τα αρχεία, την μετακίνηση τους από το ένα μέσο αποθήκευσης στο άλλο (ιεραρχική διαχείριση αποθήκευσης) και την ενδεχόμενη καταστροφή του εγγράφου. Για όλα τα παραπάνω ένα σύστημα διαχείρισης εγγράφων έχει κατάλληλο υλικό και λογισμικό που να τα υποστηρίζει.

Ανάκτηση

Ανακτά τα ηλεκτρονικά έγγραφα που είναι αποθηκευμένα. Παρά το γεγονός ότι η έννοια της ανάκτησης ενός συγκεκριμένου εγγράφου είναι απλή, η ανάκτηση στο πλαίσιο των ηλεκτρονικών εγγράφων μπορεί να είναι αρκετά περίπλοκη και ισχυρή (ευρετήρια). Απλή ανάκτηση μεμονωμένων εγγράφων μπορεί να υποστηριχθεί, επιτρέποντας στο χρήστη να καθορίσει το μοναδικό αναγνωριστικό στοιχείο ενός έγγραφου, και αφού το σύστημα χρησιμοποιεί το βασικό δείκτη ανακτά το έγγραφο. Πιο ευέλικτη ανάκτηση επιτρέπει στο χρήστη να καθορίσει επιμέρους όρους αναζήτησης που αφορούν το αναγνωριστικό ενός έγγραφου ή τμημάτων από τα

μεταδεδομένα. Αυτό θα επιστρέψει συνήθως μια λίστα εγγράφων τα οποία ανταποκρίνονται στους όρους αναζήτησης του χρήστη. Μερικά συστήματα παρέχουν τη δυνατότητα να καθορίσετε μια λογική έκφραση ή πολλαπλές λέξεις-κλειδιά ή φράσεις, που αναμένεται να υπάρχουν εντός του περιεχομένου των εγγράφων. Έτσι λοιπόν η ανάκτηση γίνεται ταχύτατα εφόσον το σύστημα υποστηρίζει την δημιουργία ευρετηρίων, εάν όχι τότε οι αναζητήσεις ενδέχεται να είναι πιο χρονοβόρες.

Διανομή

Ένα έγγραφο που δημοσιεύεται για διανομή πρέπει να είναι σε μορφή που δεν μπορεί εύκολα να αλλάξει. Ως κοινή πρακτική ένα πρωτότυπο ή κύριο αντίγραφο του εγγράφου, που συνήθως δεν χρησιμοποιείται για διανομή, αρχειοθετείται. Εάν ένα έγγραφο πρέπει να διανέμεται ηλεκτρονικά σε ένα περιβάλλον, τότε ο εξοπλισμός που χρησιμοποιείται για την εκτέλεση της εργασία πρέπει να παρέχει την δυνατότητα του ελέγχου της εμπιστευτικότητας, αυθεντικότητας, ακεραιότητα και μη αποποίησης της ευθύνης. Στις παραπάνω απαιτήσεις έρχεται να δώσει λύση η ψηφιακή υπογραφή.

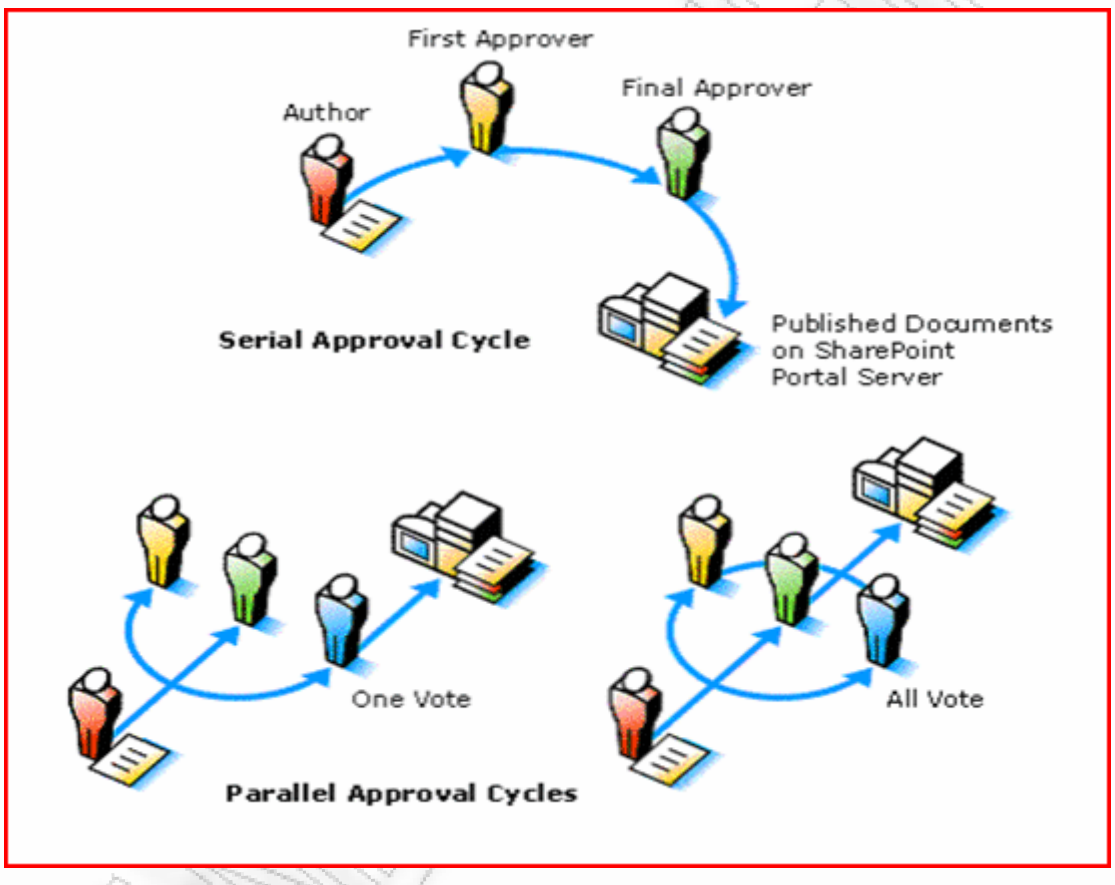
Ασφάλεια

Η ασφάλεια ενός εγγράφου είναι ζωτικής σημασίας σε πολλές εφαρμογές διαχείρισης εγγράφων. Οι απαιτήσεις συμμόρφωσης για ορισμένα έγγραφα μπορεί να είναι αρκετά περίπλοκες, ανάλογα με το είδος των εγγράφων. Για παράδειγμα, στις Ηνωμένες Πολιτείες έγγραφα που σχετίζονται με την ασφάλιση υγείας ο νόμος υπαγορεύει συγκεκριμένες απαιτήσεις ασφαλείας. Σχεδόν όλα συστήματα διαχείρισης εγγράφων έχουν μια ενότητα, τη διαχείριση των δικαιωμάτων που επιτρέπει σε έναν διαχειριστή να επιτρέπει την πρόσβαση στα έγγραφα σε ορισμένα άτομα ή ομάδες ανθρώπων. Έγγραφο με ειδική σήμανση κατά τη στιγμή της εκτύπωσης ή σε μορφή PDF κατά την δημιουργία, αποτελεί βασικό στοιχείο για να αποκλειστεί η τροποποίηση ή ακούσια χρήση τους.

Ροη εργασίας

Η ροη εργασίας είναι ένα σύνθετο πρόβλημα και υπάρχει σε μερικά εξελιγμένα συστήματα διαχείρισης εγγράφων, τα οποία συναντάμε ένα εσωτερικά δομημένο σύστημα ροής εργασίας. Υπάρχουν διάφοροι τύποι ροής εργασίας. Ποιος τύπος θα χρησιμοποιηθεί εξαρτάται από το περιβάλλον και τις απαιτήσεις που καλείται ένα σύστημα να καλύψει. Έτσι λοιπόν υπάρχει η χειροκίνητη ροη εργασίας όπου ο χρήστης αποφασίζει ποιος θα δει το έγγραφο και από την άλλη πλευρά υπάρχει η ροη εργασίας που βασίζεται σε κανόνες τους οποίους ρυθμίζει ο διαχειριστής του συστήματος σύμφωνα με τους αντίστοιχους κανόνες που διέπουν τον οργανισμό.

Επίσης υπάρχει η δυνατότητα η ροή εργασίας να ρυθμίζεται δυναμικά μέσω κανόνων που έχουν προηγούμενος ορισθεί πχ. εάν το ποσό ενός τιμολόγιου είναι μεγαλύτερο από κάποιο ορισμένο το έγγραφο ακολουθεί μια άλλη διαδρομή σε σχέση με αυτό το τιμολόγιο που το ποσό είναι μικρότερο. Τέλος προηγμένοι μηχανισμοί ροής εργασίας μπορούν να διαχειριστούν το περιεχόμενο ή να ενεργοποιηθούν με σήμα έπειτα από συγκεκριμένη εξωτερική διαδικασία. Η ύπαρξη κανόνων ροής εργασίας σε ένα σύστημα διαχείρισης εγγράφων αυξάνει κατακόρυφα την δυναμική του.



Σχήμα 3-2: Κύκλος ζωής εγγραφού
Πηγη:http://www.bluedev.eu/t2c/Technology/PLMManagement/eFabmetal/tabid/118/language/en-US/Default.aspx

Συνεργασία

Η συνεργασία είναι μια δυνατότητα που να εμπεριέχεται στα περισσότερα συστήματα διαχείρισης εγγράφων. Στη βασική του μορφή, ένα συνεργατικό σύστημα διαχείρισης εγγράφων θα επιτρέψει έγγραφα να ανακτηθούν και να δουλευθούν μόνο από

εξουσιοδοτημένο χρήστη. Η πρόσβαση θα πρέπει να εμποδιστεί σε άλλους χρήστες, καθόσον εργασίες εκτελούνται στο έγγραφο. Άλλες προηγμένες μορφές συνεργασίας επιτρέπουν σε πολλούς χρήστες να δουν και να τροποποιήσουν (ή σημάνουν) ένα έγγραφο που χρησιμοποιείτε την ίδια στιγμή σε μια συνεδρία συνεργασίας. Το έγγραφο που προέκυψε θα πρέπει να μπορεί να προβληθεί στην τελική του μορφή, ενώ παράλληλα αποθηκεύονται όλες οι σημειώσεις, διορθώσεις ή προσθήκες κάθε μεμονωμένου χρήστη που έγινε κατά τη διάρκεια της ίδιας συνεδρίας συνεργασίας.

Εκδόσεις αρχείων

Ο δυνατότητα της δημιουργίας και αποθήκευσης εκδόσεων των εγγράφων είναι μια διαδικασία με την οποία τα έγγραφα ελέγχονται μέσα ή έξω από το σύστημα διαχείρισης εγγράφων και επιτρέπει στους χρήστες να ανακτήσουν τις προηγούμενες εκδόσεις και να συνεχίσουν το έργο από ένα επιλεγμένο σημείο. Οι εκδόσεις είναι χρήσιμες για έγγραφα που μεταβάλλονται με την πάροδο του χρόνου και απαιτούν ενημέρωση, αλλά μπορεί να φανεί χρήσιμο όταν θέλουμε να πάμε πίσω σε μια παλαιότερη αναφορά του εγγράφου ή να λάβουμε ένα προηγούμενο αντίγραφο.

Επιπλέον, τα εν λόγω συστήματα προσφέρουν μια πλειάδα εφαρμογών, που δίνουν την ευκαιρία διαχείρισης των εγγράφων κατά την κρίση του χρήστη, τη συνεργασία με άλλα συστήματα που τυχόν υπάρχουν στην επιχείρηση και την εξασφάλιση ότι τα δεδομένα ούτε πρόκειται να χαθούν αλλά ούτε και να πέσουν στην αντίληψη μη εξουσιοδοτημένων χρηστών, μέσα από τον καθορισμό δικαιωμάτων πρόσβασης.

3.3 Οφέλη ενός συστήματος διαχείρισης εγγράφων.

Πολλά και σημαντικά είναι τα κέρδη που αποφέρει σε έναν οργανισμό η χρήση συστημάτων διαχείρισης εγγράφων. Είναι αξιοσημείωτο ότι τα κέρδη αυτά δεν περιορίζονται μόνο σε ένα τομέα αλλά επηρεάζουν θετικά το σύνολο του οργανισμού, καθώς την εφοδιάζουν με νέες εργασιακές πρακτικές, πιο σύγχρονες, πιο ευέλικτες και πιο έξυπνες. Ο οργανισμός εθίζεται έτσι σε ένα νέο τρόπο λειτουργίας, που χαρακτηρίζεται από ορθολογικότητα, εργατικότητα και διαφάνεια. Αποτέλεσμα, η αύξηση της ανταγωνιστικότητας και η διαμόρφωση καλύτερων οικονομικών μεγεθών. Αν, μάλιστα, η ενσωμάτωση συστημάτων διαχείρισης εγγράφων συνδυαστεί με άλλα προγράμματα λογισμικού όπως: συστήματα ροής εργασίας, τότε τα αποτελέσματα είναι ακόμα πιο εντυπωσιακά.

Πριν από μερικά χρόνια, οι επιχειρήσεις έδιναν περισσότερο βάρος στην παραγωγική τους ικανότητα και στις πωλήσεις και πολύ λιγότερο στο προσωπικό. Σταδιακά, και

καθώς οι νέες συνθήκες επιβάλλουν την καλύτερη δυνατή στελέχωση, την αμεσότητα στη διαθεσιμότητα του κατάλληλου προσωπικού, και όλα αυτά σε συνδυασμό με τις διαδικασίες παραγωγής να δίνουν το ελάχιστο δυνατό κόστος, οι επιχειρήσεις διαπίστωσαν ότι η οργάνωση και διαχείριση του ανθρώπινου δυναμικού είναι εξαιρετικά σημαντικό στοιχείο για την επιβίωσή τους. Ξεκινώντας από τις ιδιαιτερότητες της σύγχρονης οικονομίας, φθάνουμε στην προμήθεια και αξιοποίηση εργαλείων και μεθόδων οργάνωσης που αφορούν το προσωπικό, ενώ η διαχείρισή του γίνεται πλέον από την αναβαθμισμένη διεύθυνση ανθρώπινου δυναμικού.

Η διείσδυση της τεχνολογίας στις λειτουργίες μιας επιχείρησης έχει πλέον φθάσει σε υψηλά επίπεδα ευχρηστίας και λειτουργικότητας, και τείνει να καταστεί ανάγκη για όλες τις εταιρίες ανεξαρτήτως κλάδου και μεγέθους. Είναι προφανές ότι η εκάστοτε διοίκηση είναι σε θέση να γνωρίζει τους τομείς όπου υπάρχει μεγαλύτερη ανάγκη εγκατάστασης ανάλογων συστημάτων, π.χ. ένα μικρό επιχείρηση πιθανότατα δεν χρειάζεται τμήμα ανθρωπίνων πόρων, αφού οι ανάγκες του σε προσωπικό αλλά και σε εξειδίκευση είναι περιορισμένες, σε αντίθεση με κάποια επιχείρηση που δραστηριοποιείται ως εταιρία συμβούλων, η οποία κάνει και την επιλογή των δικών της συνεργατών. Είναι σημαντικό οι μεγάλες και μικρές εταιρίες να καταγράψουν κατ' αρχάς τις ανάγκες και προτεραιότητές τους (σημερινές και μελλοντικές) και στη συνέχεια να προβούν στην υλοποίηση των αντίστοιχων λύσεων, λαμβάνοντας πάντοτε υπόψη τη σχέση κόστους - αξίας.

Μεταξύ άλλων, τα συστήματα διαχείρισης εγγράφων εξοικονομούν πολύτιμο χρόνο, μειώνουν τα λειτουργικά έξοδα λόγω της εξοικονόμησης ανθρώπινων και υλικών πόρων και συντελούν στην αύξηση της παραγωγικότητας των εργαζομένων. Συγκεκριμένα, οι ατέρμονες αναζητήσεις αρχείων και εγγράφων παραχωρούν τη θέση τους στη γρήγορη εύρεση και προβολή, οι επίπονες προσπάθειες ομαδοποίησης αντικαθίστανται από την «αεικίνητη» και εύκολη ψηφιακή διαχείριση, οι διπλές ή οι πολλαπλές εγγραφές εντοπίζονται και διαγράφονται. Ο χρήστης μπορεί οποιαδήποτε στιγμή να αναζητήσει ένα ή περισσότερα έγγραφα, καθώς επίσης και να τα κατανείμει σε συναδέλφους του στο τοπικό δίκτυο (intranet) της επιχείρησης.

Από την άλλη πλευρά, οι εργαζόμενοι μπορούν απερίσπαστοι να αφοσιώνονται σε άλλους εργασιακούς στόχους, πιο προσοδοφόρους και πιο κρίσιμους για την ευρωστία του οργανισμού. Ο χρόνος που απαιτείται για την επιτέλεση μιας εργασίας μειώνεται στο ελάχιστο δυνατό, και μερικά δευτερόλεπτα αρκούν για την ολοκλήρωσή της. Στο ελάχιστο αναγκαίο μειώνεται και το κόστος δημιουργίας και διανομής φωτοτυπιών.

Η αρχειοθέτηση εισερχόμενων και εξερχόμενων φαξ και μηνυμάτων ηλεκτρονικού ταχυδρομείου πραγματοποιείται αυτόματα από το σύστημα χωρίς ανθρώπινη παρέμβαση. Επιπλέον, μολονότι συχνά διαφεύγει της προσοχής, η ηλεκτρονική αρχειοθέτηση λύνει πολλά χωροταξικά προβλήματα, περιορίζοντας τις ανάγκες αποθηκευτικών χώρων και συμβάλλοντας στη δημιουργία ενός μινιμαλιστικού και άνετου εργασιακού περιβάλλοντος. Επίσης, δεν θα πρέπει να ξεχνάμε ότι τα φυσικά έγγραφα και η χειροκίνητη αρχειοθέτηση είναι περισσότερο ευάλωτα στη φθορά και στην καταστροφή έναντι της ψηφιακής και ότι συχνά πολύτιμα έγγραφα χάνονται, με δυσάρεστες συνέπειες για την επιχείρηση και τους εργαζομένους [8].

Συμπερασματικά, η ψηφιακή αρχειοθέτηση είναι ανάγκη και όχι πολυτέλεια για έναν οργανισμό, ασχέτως του ότι πολλοί μπορεί να το θεωρήσουν ως πολυτέλεια και ανταγωνιστικό πλεονέκτημα.

3.4 Προτυποποίηση συστημάτων διαχείρισης εγγράφων

Όπως σε όλους τους τομείς τις επιχειρηματικής δραστηριότητας υπάρχουν επίπεδα ποιότητα (standards) έτσι και στα συστήματα διαχείρισης εγγράφων από πολύ νωρίς η προτυποποίηση άγγιξε τα όρια της. Δεν θα υπεισέλθουμε σε μακροσκελή αναφορά των προτύπων ISO που πρέπει να λαμβάνουν υπόψη αυτοί που αναπτύσσουν τέτοια συστήματα άπλα θα τα παραθέσουμε με τις αντίστοιχες παραπομπές όπου ο αναγνώστης μπορεί να ανατρέξει για περισσότερες πληροφορίες.

- ISO 2709:1996 Information and documentation - Format for information exchange
- ISO 15836:2009 which replaces ISO 15836:2003 Information and documentation - The Dublin Core metadata element set
- ISO 15489: 2001 Information and documentation -Records management
- ISO 21127:2006 Information and documentation - A reference ontology for the interchange of cultural heritage information
- ISO 23950:1998 Information and documentation - Information retrieval (Z39.50) - Application service definition and protocol specification.
- ISO/CD 10244 Document management - Business process/workflow baselining and analysis associated with EDMS technologies
- ISO 32000 - portable document format

Αναλυτικά θα παρουσιάσουμε το ISO 17025 που αποτελεί την βάση για την ανάπτυξη τέτοιων συστημάτων.

Το πρότυπο ISO 17025 χρησιμοποιείται για τη δημιουργία, οργάνωση και διαπίστευση εργαστηριακών μετρήσεων, δοκιμών και διακριβώσεων. Τέτοια είναι τα εργαστήρια αναλύσεων τροφίμων, προϊόντων του κλάδου μεταποίησης καθώς και αναλυτικά εργαστήρια που άπτονται του κλάδου υγείας [10].

Διαπίστευση ενός εργαστηρίου από έναν ανεξάρτητο επίσημο φορέα, που στην Ελλάδα συνηθίζεται να είναι το Ε.ΣΥ.Δ. – Εθνικό Συμβούλιο Διαπίστευσης, σύμφωνα με το πρότυπο ISO 17025 σημαίνει ότι το εργαστήριο έχει τις τεχνικές και διοικητικές ικανότητες να διεξάγει συγκεκριμένες δοκιμές, μετρήσεις και διακριβώσεις σύμφωνα με συγκεκριμένες πρότυπες ή ενδοεργαστηριακές μεθόδους, με συγκεκριμένο εξοπλισμό και εντός συγκεκριμένων και δηλωμένων ορίων ακρίβειας.

Η διαπίστευση ενός εργαστηρίου αποτελεί την επίσημη αναγνώριση της τεχνικής επάρκειας και της αξιοπιστίας του, χαρακτηριστικά ιδιαίτερα σημαντικά για τη διεξαγωγή δοκιμών που σχετίζονται με δημόσιες και ιδιωτικές επιχειρήσεις και προϊόντα ή κατασκευές.

Αυτό το γεγονός συνεπάγεται ότι η παροχή των υπηρεσιών του σε επίπεδο αναλύσεων είναι τόσο αναγνωρίσιμη και αξιόπιστη που τα αποτελέσματα μπορούν να χρησιμοποιηθούν από τους πελάτες του σε οποιαδήποτε διαφωνία, αμφισβήτηση ή διατροφική κρίση. Κάτι τέτοιο είναι ομολογουμένως η ειδοποιός διαφορά έναντι του ανταγωνισμού και το κίνητρο των επιχειρήσεων με αποτέλεσμα την αύξηση του πελατειακού εύρους. Τα οφέλη από την εφαρμογή ενός τέτοιου συστήματος είναι:

- Αύξηση του κύρους του εργαστηρίου σε εθνικό και διεθνές επίπεδο
- Έγκυρα αποτελέσματα, τα οποία μπορεί ο πελάτης - εσωτερικός και εξωτερικός - να εμπιστευθεί
- Καλύτερη οργάνωση του εργαστηρίου
- Αναγνώριση της ικανότητας του προσωπικού
- Αναγνώριση των δυνατοτήτων του εξοπλισμού του εργαστηρίου
- Διερεύνηση των δυνατοτήτων βελτίωσης των παρεχόμενων υπηρεσιών
- Αύξηση του πελατολογίου λόγω της συγκριτικής διαφοράς με τον ανταγωνισμό (διαπιστευμένο εργαστήριο σε σχέση με τα συμβατικά)
- Ανάληψη εξειδικευμένων εργασιών για φορείς (Κρατικούς ελεγκτικούς φορείς-Ιδιωτικές επιχειρήσεις), ιδιαίτερα σε περιοχές που απουσιάζουν κρατικά εργαστήρια ελέγχων.

Από όλα τα παραπάνω που αφορούν την προτυποποίηση και ιδιαίτερα από την τελευταία, προκύπτει ένα πολύ σημαντικό συμπέρασμα που σχετίζεται άμεσα με την επιλογή ενός συστήματος διαχείρισης εγγράφων. Όταν μια επιχείρηση ή ένας

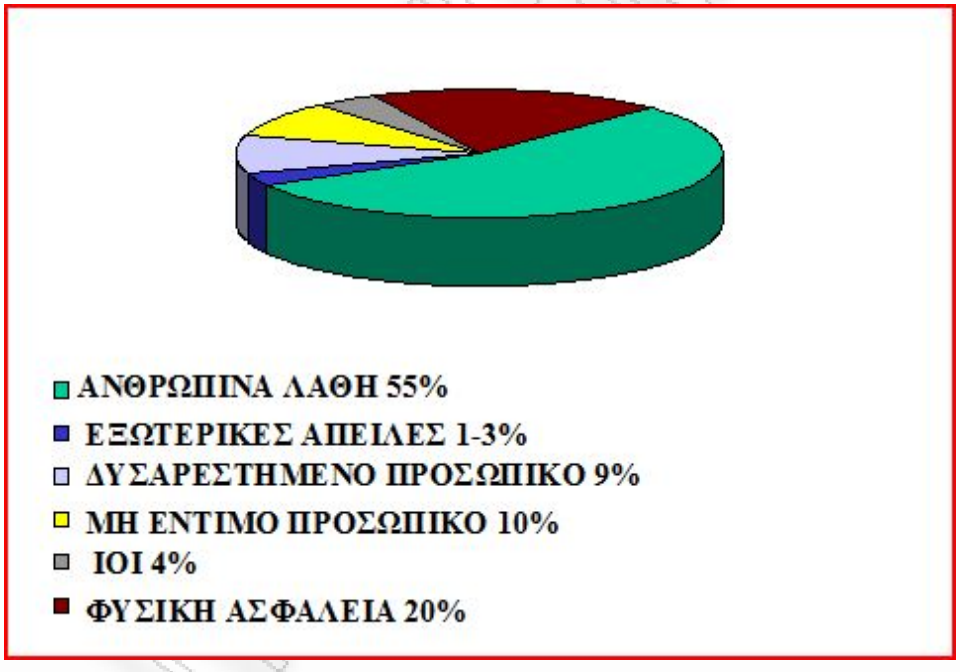
οργανισμός αποφασίσει να αγοράσει κάποιο έτοιμο σύστημα ή να αναπτύξει μέσω κάποιας εταιρείας ανάπτυξης εφαρμογών ένα προσαρμοσμένο στις ανάγκες της, θα πρέπει να λάβει υπόψη όλες τις ανωτέρω προτυποποιήσεις, ούτως ώστε το αποτέλεσμα να είναι θετικό. Υπάρχουν πολλές περιπτώσεις επιχειρήσεων που «πλήρωσαν» κυριολεκτικά και μεταφορικά το κόστος των αδυναμιών του συστήματος που εγκατέστησαν. Αυτός είναι ο λόγος που κάναμε αυτή την εκτεταμένη αναφορά στα πρότυπα των συστημάτων διαχείρισης εγγράφων, διότι είναι ο πιο αξιόπιστος τρόπος να διαπιστωθεί εάν μια εταιρεία έχει την δυνατότητα να αναπτύξει κάτι πραγματικά λειτουργικό.

ΚΕΦΑΛΑΙΟ 4^{Ο}

ΠΟΛΥΕΠΙΠΕΔΗ ΑΣΦΑΛΕΙΑ

Τα δίκτυα υπολογιστών αποτελούν την βάση ανάπτυξης της κοινωνίας της πληροφορίας. Βασικά χαρακτηριστικά των επικοινωνιακών υποδομών αποτελούν η ταχύτητα ανάπτυξης τους και η μεγάλη τους διεισδυτικότητα. Όλο και περισσότεροι απλοί χρήστες ή οργανισμοί χρησιμοποιούν δίκτυο προκειμένου να διεκπεραιώσουν τις προσωπικές ή επαγγελματικές τους ανάγκες. Ως φυσικό επακόλουθο το πρόβλημα της ασφάλειας αναδεικνύεται σε ένα καθοριστικό παράγοντα επιτυχούς ανάπτυξης και λειτουργίας των σύγχρονων πληροφοριακών συστημάτων.

Οι απειλές για την ασφάλεια ενός δικτύου μπορούν να προέλθουν από ένα αριθμό πηγών, με ποικίλους διαφορετικούς τρόπους, καλύπτοντας ένα ευρύτατο φάσμα περιπτώσεων. Η υπάρχουσα τάση για την μεγαλύτερη δυνατή αυτοματοποίησης των εσωτερικών και εξωτερικών διαδικασιών λειτουργίας των οργανισμών, αποτελεί ταυτόχρονα και την αχίλλειο πτέρνα πολλών διασυνδεδεμένων πληροφοριακών συστημάτων.



Σχήμα 4-1: Απειλές ασφάλειας πληροφοριακών συστημάτων.
Πηγή: Από έρευνα της εταιρείας Trust-IT Ασφάλεια Πληροφοριακών Συστημάτων.

Στην διόγκωση του προβλήματος της ασφάλειας συμβάλλουν επίσης και σύγχρονες τεχνολογικές εξελίξεις. Ισχυρότεροι υπολογιστές και λογισμικό, πολλές εφαρμογές διαδικτύου, ταχύτερα δίκτυα, η ραγδαία αύξηση διασυνδεδεμένων υπολογιστών και

έμπειρων χρηστών, οι οποίοι δύναται να χαρακτηριστούν εν δυνάμει χάκερς, είναι όλα αυτά μεταξύ άλλων παράγοντες που αυξάνουν τις δυνατότητες στην παραβίαση ασφάλειας ενός πληροφοριακού συστήματος και επομένως τις πιθανότητες να υπάρξει παραβίαση της ασφάλειας ενός δικτύου.

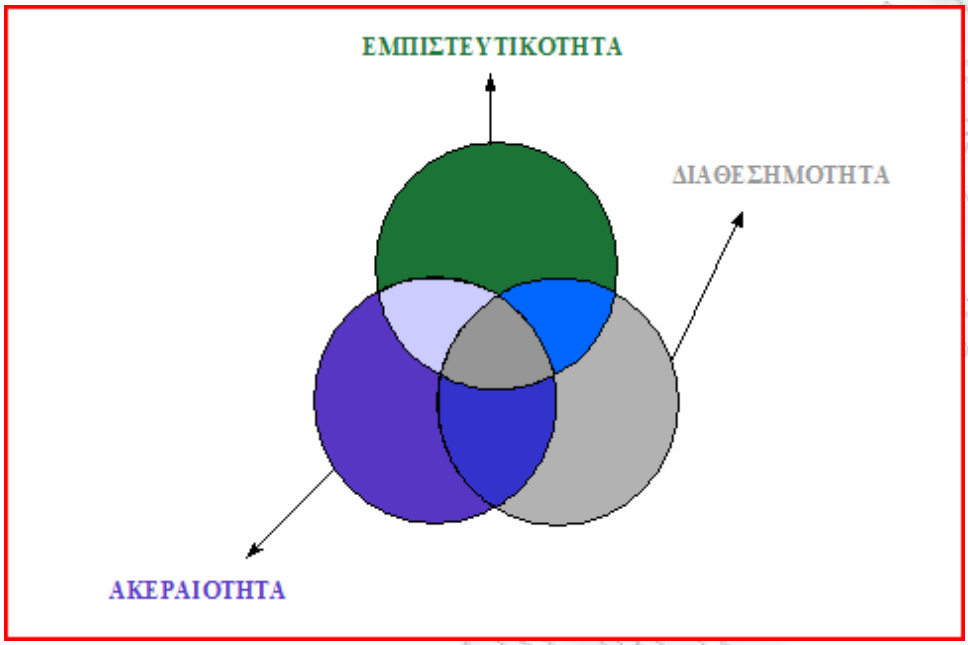
Στο πρόσφατο παρελθόν ένας κωδικός πρόσβασης μπορούσε να εξασφαλίσει σε μεγάλο βαθμό, την προστασία ενός συστήματος. Σήμερα η προσφερόμενη υπολογιστική ισχύς, η ταχύτητα επικοινωνίας, και η ύπαρξη εξειδικευμένου λογισμικού για παραβιάσεις ασφαλείας, συνθέτουν ένα εντελώς διαφορετικό σκηνικό και επιβάλλουν μια νέα συνολική και περισσότερο αποτελεσματική στρατηγική και αρχιτεκτονική ασφαλείας. Η ασφάλεια πληροφοριακών συστημάτων στηρίζεται σε τρεις βασικές ιδέες: στην ακεραιότητα, στην διαθεσιμότητα και στην εμπιστευτικότητα.

Εάν θέλαμε να παρουσιάσουμε την σχέση της κάθε ιδιότητας με τις υπόλοιπες θα καταλήγαμε στο σχήμα 4-2. Κάθε ιδιότητα λοιπόν έχει ένα μεγάλο τμήμα το οποίο αφορά την ιδιότητα αυτή την ίδια και περιλαμβάνει όλα εκείνα τα μετρά και στοιχεία που την υποστηρίζουν, όμως υπάρχουν και κάποια μικρότερα τμήματα που εξαρτώνται είτε από μια άλλη ιδιότητα είτε και από τις άλλες δυο μαζί. Αυτό είναι ένα πολύ σπουδαίο στοιχείο που πρέπει οι υπεύθυνοι ασφάλειας να λαμβάνουν υπόψη προκειμένου να μην αφήνουν «κερκόπορτες» σε θέματα ασφάλειας του συστήματος.

Η ανωτέρω προσέγγιση των ιδιοτήτων της ασφάλειας συνθέτει μια εικόνα πολυδιάστατη η οποία είναι περισσότερη ικανή να αντιμετώπιση τις νέες απειλές της σημερινής κοινωνίας της πληροφορίας σε σχέση με το μονοδιάστατο μοντέλο των προηγούμενων δεκαετιών. Η πολυεπίπεδη ασφάλεια που υλοποιήσαμε στην παρούσα εργασία δομείται ακριβώς σε αυτή την φιλοσοφία για να μπορεί να αντιμετωπίσει αποτελεσματικά τις προκλήσεις της εποχής μας. Ας δούμε αναλυτικά σε τι αναφέρεται η κάθε ιδιότητα.

Η *ακεραιότητα* αναφέρεται στη διατήρηση των δεδομένων ενός πληροφοριακού συστήματος σε μια γνωστή κατάσταση χωρίς ανεπιθύμητες τροποποιήσεις, αφαιρέσεις ή προσθήκες από μη εξουσιοδοτημένα άτομα, καθώς και την αποτροπή της πρόσβασης ή/και χρήσης των υπολογιστών και δικτύων του συστήματος από άτομα χωρίς άδεια [11]. Για παράδειγμα, μια εφημερίδα που δημοσιεύει τα άρθρα της και στο Διαδίκτυο θα ήθελε αυτά τα άρθρα να είναι ασφαλή από μετατροπές ενός χάκερ που επιθυμεί να εισάγει λανθασμένες πληροφορίες στα κείμενα. Ακριβώς αυτό συνέβη το 1995, όταν άγνωστα άτομα κατάφεραν να εξουδετερώσουν τα μέτρα ασφάλειας της Ελευθεροτυπίας και να εισαγάγουν πρωτοσέλιδο άρθρο για τον

πρόωρο θάνατο του Ανδρέα Παπανδρέου, που εκείνη τη στιγμή νοσηλευόταν στο Ωνάσειο [12].



Σχήμα 4-2 Βασικές ιδιότητες ασφάλειας ενός πληροφοριακού συστήματος

Η *διαθεσιμότητα* των δεδομένων και των υπολογιστικών πόρων είναι η εξασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα θα είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους [11]. Μία τυπική απειλή που αντιμετωπίζουν τα σύγχρονα πληροφοριακά συστήματα είναι η επίθεση άρνησης υπηρεσιών (DOS attack), που έχει ως σκοπό να τεθούν εκτός λειτουργίας οι στοχευμένοι πόροι είτε προσωρινά είτε μόνιμα. Η άρνηση υπηρεσιών δεν προκαλείται αναγκαία από εχθρική επίθεση. Το φαινόμενο Slashdot, κατά το οποίο ένας σύνδεσμος προς μια ιστοσελίδα φιλοξενούμενη σε διακομιστή με σύνδεση χαμηλής χωρητικότητας δημοσιεύεται σε δημοφιλή ιστότοπο, με συνέπεια εκατοντάδες χιλιάδες αναγνώστες να υπερφορτώσουν τη σύνδεση της αναφερομένης ιστοσελίδας, προκαλεί το ίδιο αποτέλεσμα [13].

Τέλος η *εμπιστευτικότητα* σημαίνει ότι ευαίσθητες πληροφορίες δεν θα έπρεπε να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα [11]. Η διαρροή ευαίσθητων πληροφοριών μπορεί να γίνει με πιο παραδοσιακές μεθόδους από την ψηφιακή υποκλοπή, π.χ. με την κλοπή φορητών υπολογιστών από το κατάλληλο τμήμα μιας

εταιρίας. Το 2006 μια μελέτη με τη συνεργασία 480 εταιριών έδειχνε ότι 80% των εταιριών είχε πρόβλημα με διαρροή πληροφοριών λόγο κλοπής φορητού.

Η αρχιτεκτονική που παρουσιάζεται στην παρούσα εργασία και αναλυτικά ξεδιπλώνεται στις παρακάτω παραγράφους είναι εκείνη της πολυεπίπεδης ασφάλειας. Σκοπός της δημιουργίας μιας τέτοιας αρχιτεκτονικής είναι να μπορέσει να καλυφτεί το πληροφοριακό σύστημα και κατ' επέκταση και ο οργανισμός που υποστηρίζει, από όλους εκείνους τους παράγοντες που φαίνονται στο σχήμα 3.1 με τα αντίστοιχα ποσοστά, από το οποίο παρατηρούμε ότι δεν υπάρχουν μόνο εξωτερικές απειλές αλλά και εσωτερικές. Άρα θα πρέπει να υπάρχει η δυνατότητα να εντοπιστούν και αυτές πριν να προκαλέσουν εκτεταμένη παραβίαση.

Θα αναπτύξουμε αρχικά την ασφάλεια από την φυσική της διάσταση και έπειτα από την ψηφιακή, στην συνέχεια θα αναφερθούμε στην ανάλυση κινδύνου και στα πρότυπα πιστοποίησης ασφαλείας, ώστε τέλος από τις παραπάνω προσεγγίσεις να φτάσουμε στην σύνθεση της αρχιτεκτονική της πολυεπίπεδης ασφάλειας που υλοποιήθηκε στην παρούσα εργασία στα πλαίσια ενός συστήματος διαχείρισης εγγραφών.

Σχήμα 4-3: Τομείς ασφάλειας πληροφορικής.
Πηγή: Εγχειρίδιο διαχείρισης κρίσεων του Fairfax County Public Schools

4.1 Φυσική ασφάλεια

Η ανάγκη για ασφάλεια δεν συμβαδίζει με την ίδια την φύση ενός δικτύου, το οποίο χαρακτηρίζεται από χαλαρό έλεγχο, τεχνολογική ετερογένεια, και προσπάθεια ανοιχτών περιβαλλόντων με παροχή πρόσβασης σε μεγάλο αριθμό χρηστών. Προκύπτει λοιπόν το συμπέρασμα ότι η ανάγκη για συνεχή επαγρύπνηση σε θέματα

ασφαλείας αλλά και το κόστος για την επίλυση αυτών των θεμάτων, είναι το τίμημα που πρέπει να πληρώσουμε για να έχουμε τα οφέλη που μας προσφέρει ένα δικτυωμένο πληροφοριακό σύστημα. Όμως τι ακριβώς περιλαμβάνει η φυσική ασφάλεια.

Η φυσική ασφάλεια αναφέρεται στο σύνολο των μέτρων που απαιτούνται για την προστασία των εγκαταστάσεων Η/Υ (κτιρίων, αίθουσας Η/ Υ, του ίδιου του Η/Υ και του συνοδεύοντος αυτού εξοπλισμού, μέσων και υποδομής λειτουργίας του συστήματος πληροφορικής). Ο σωστός σχεδιασμός φυσικής ασφάλειας λαμβάνει υπόψη τις πιθανές απειλές προς το χώρο των Η/Υ και γενικότερα του συστήματος πληροφορικής από φυσικές καταστροφές, ανθρώπινα λάθη, ατυχήματα, βανδαλισμούς, κλοπή, ηλεκτρονική παρακολούθηση, κατασκοπία [14].

Τα μέτρα της φυσικής ασφάλειας είναι πολύ σημαντικά και θα πρέπει να λαμβάνονται σοβαρά υπόψη από τους υπεύθυνους, διότι αποτελούν την πρώτη βαθμίδα ασφάλειας, που αν παραβιαστεί δίνει την δυνατότητα σε κάθε επίδοξο χάκερ να εισέλθει στον ψηφιακό τμήμα και κατ' επέκταση στο οικοδόμημα της ψηφιακή ασφάλεια, δηλαδή το πρώτο κάστρο ασφάλειας θα έχει αλωθεί. Αναλυτικά τα μέτρα που αφορούν την φυσική ασφάλεια και που έχουν προκύψει έπειτα από χρόνιες μελέτες και από την αντιμετώπιση πραγματικών περιστατικών είναι:

Ο χώρος εγκατάστασης των αυτοματοποιημένων πληροφοριακών συστημάτων πρέπει να παρέχει τις κατάλληλες περιβαλλοντολογικές συνθήκες θερμοκρασίας και υγρασίας για την ομαλή και απρόσκοπτη λειτουργία τους. Θα πρέπει να αποφεύγεται η επιλογή χώρων που βρίσκονται κοντά σε εγκαταστάσεις που παράγουν ηλεκτρομαγνητικά πεδία όπως: μηχανοστάσια, ηλεκτρικές εγκαταστάσεις υψηλής τάσης, ανελκυστήρες κ.α.. Επίσης θα πρέπει να εξασφαλίζεται ότι η ηλεκτρική εγκατάσταση του χώρου είναι η προβλεπόμενη και λειτουργεί κανονικά. Ακόμη όσον αφορά την προστασία του εξοπλισμού από μικροδιακοπές και αυξομειώσεις τάσης είναι σκόπιμο να χρησιμοποιούνται τροφοδοτικά αδιάλειπτης λειτουργίας (Uninterrupted Power Supply - UPS).

Σχετικά με την προστασία των συστημάτων από τον κίνδυνο πυρκαγιάς απαιτείται κατ' αρχήν η ύπαρξη φορητών πυροσβεστήρων, σε αριθμό ανάλογο με το μέγεθος και τη σπουδαιότητα του πληροφοριακού συστήματος. Θα πρέπει να γίνει εξέταση της ανάγκης εγκατάστασης αυτοματοποιημένου συστήματος ανίχνευσης και κατάσβεσης πυρκαγιών, διότι μπορεί να προκαλέσει μεγαλύτερα προβλήματα από αυτά για τα όποια είναι προορισμένο να λύση. Επίσης η ένταξη των συστημάτων πληροφορικής στο γενικότερο σχέδιο πυρασφαλείας του φορέα είναι μια λύση που

έχει υιοθετηθεί από όλα τα ανεπτυγμένα κράτη έτσι ώστε να αντιμετωπίζονται θέματα πυρασφαλείας από ειδικά συστήματα που λαμβάνουν αποφάσεις σχετικά με τον τρόπο αντιμετώπισης γρήγορα και αυτόματα, τουλάχιστον κατά το αρχικό στάδιο.

Ιδιαίτερη μέριμνα θα πρέπει να λαμβάνεται για την αποφυγή ηλεκτρονικής παρακολούθησης των διαβαθμισμένων πληροφοριακών συστημάτων. Γι' αυτό επιδιώκεται ώστε ο χώρος εγκατάστασης των διαβαθμισμένων πληροφοριακών συστημάτων αίθουσα, κλωβός κ.α. να πληρεί τις απαιτήσεις που καθορίζουν οι σχετικοί κανονισμοί ασφαλείας έκαστης εταιρείας.

Τα τοπικά δίκτυα (LAN) θα πρέπει να αναπτύσσονται σύμφωνα με τους κανόνες της δομημένης καλωδίωσης. Ο διαχειριστής του πληροφοριακού συστήματος ή ο υπεύθυνος σε θέματα πληροφορικής θα πρέπει να σχεδιάζει και να αναπτύσσει τα τοπικά δίκτυα εξασφαλίζοντας κατάλληλη δρομολόγηση των καλωδιώσεων ώστε να είναι δυνατός ο φυσικός έλεγχος και επίβλεψή της. Όσον αφορά στα δίκτυα ευρείας περιοχής (WAN) θα πρέπει να τηρούνται οι ισχύοντες κανόνες και διαδικασίες ασφαλείας επικοινωνίας, ένα θέμα που η περεταίρω ανάπτυξη του είναι έξω από τα πλαίσια της παρούσης εργασίας.

Από την άλλη πλευρά τα πληροφοριακά συστήματα πρέπει να προστατεύονται με ελέγχους πρόσβασης ικανοποιητικού βαθμού και αναλόγως με το επίπεδο διαβάθμισης των συστημάτων. Τα μέτρα που πρέπει να λαμβάνονται, ανάλογα με το επίπεδο διαβάθμισης του συστήματος, είναι αυτά που περιγράφονται στον Κανονισμό Ασφαλείας Εθνικού Διαβαθμισμένου Υλικού για υλικό αντίστοιχης διαβάθμισης. Επιπλέον τα πληροφοριακά συστήματα δεν επιτρέπεται να βρίσκονται ανεπίβλεπτα σε κατάσταση λειτουργίας, χωρίς να χρησιμοποιούνται οι μηχανισμοί του συστήματος που απαγορεύουν τη χρησιμοποίησή του από μη εξουσιοδοτημένο προσωπικό πχ. κλείδωμα πληκτρολογίου, οθόνης κ.α. .

Η διαμόρφωση ενός ασφαλούς προβάλλοντος είναι ευθύνη και του προσωπικού ώστε να διασφαλίζεται η εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των πληροφοριών των συστημάτων πληροφορικής του οργανισμού. Απαιτείται η συνεχής επαγρύπνηση και περιφρούρηση του συστήματος προστασίας και ασφαλούς λειτουργίας των μέσων πληροφορικής έκαστης εσωτερικής υπηρεσίας. Θα πρέπει να υπάρχουν οδηγίες και κανόνες τόσο φυσικής όσο και ψηφιακής ασφάλειας. Η ανανέωση των κανόνων, για εξασφάλιση επαρκούς ασφάλειας του συστήματος αλλά και του χώρου που αυτό στεγάζεται, είναι επιβεβλημένη.

Ακόμη θα πρέπει να λαμβάνεται μέριμνα ώστε να χρησιμοποιούνται μόνο τα προβλεπόμενα προγράμματα (λογισμικό) και το κατάλληλο υλικό στο σύστημα και

όχι άλλα, μη εγκεκριμένα, από την προϊστάμενη αρχή πληροφορικής του οργανισμού. Επίσης αποτελεί προϋπόθεση για τη διαμόρφωση ασφαλούς περιβάλλοντος εργασίας πληροφορικής η εφαρμογή και σχολαστική τήρηση της πολιτικής, των αρχών και των μέτρων ασφαλείας που καθορίζονται μέσα στα σχετικά έγγραφα και εγχειρίδια που συντάσσονται και επιδίδονται στου χρήστες του οργανισμού από τον προϊστάμενο σε θέματα ασφάλειας πληροφορικής έκαστου οργανισμού.

4.2 Ψηφιακή ασφάλεια

Η ψηφιακή ασφάλεια περιλαμβάνει τα αναγκαία μέτρα που αποτρέπουν τη μη εξουσιοδοτημένη πρόσβαση στις πληροφορίες και τις διαδικασίες επεξεργασίας, διακίνησης και αποθήκευσής τους ώστε να διασφαλίζεται η διαθεσιμότητα και ακεραιότητα των δεδομένων και πληροφοριών του συστήματος. Για τη διασφάλιση της διαθεσιμότητας και ακεραιότητας αλλά και το διαρκή έλεγχο των πληροφοριών απαιτείται κατ' ελάχιστο η τήρηση των παρακάτω [14]:

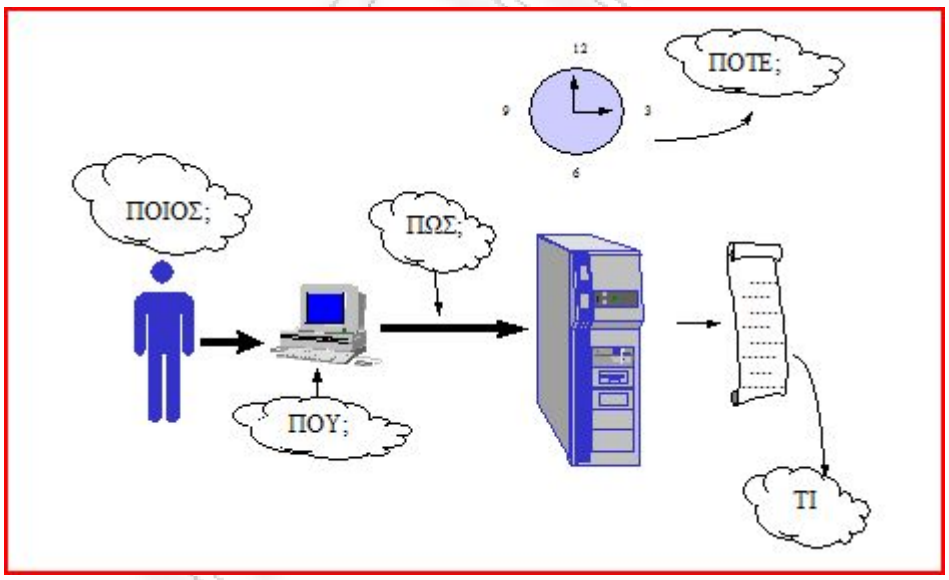
- Χρησιμοποίηση προσωπικού κωδικού ασφαλείας από κάθε χρήστη.
- Απαγόρευση πρόσβασης στα πληροφοριακά συστήματα σε μη εξουσιοδοτημένους χρήστες.
- Απαγόρευση πρόσβασης σε διαβαθμισμένα συστήματα πληροφορικής προσωπικού χωρίς τον ανάλογο βαθμό διαβάθμισης ασφαλείας.
- Καταγραφή των ενεργειών κάθε χρήστη ώστε να είναι δυνατόν να προσδιορίζεται ο χρήστης που παραβίασε την ασφάλεια του συστήματος.
- Χρησιμοποίηση της αρχής "δύο χρήστες δύο κωδικοί ασφαλείας" για πρόσβαση στις πληροφορίες που έχουν σχέση με τα μέτρα ασφαλείας του συστήματος.
- Συνεχής έλεγχος του συστήματος για ύπαρξη ιών.
- Ελεγχόμενη εγκατάσταση λογισμικού από τους φορείς πληροφορικής και απαγόρευση εγκατάστασης λογισμικού μη εγκεκριμένου από την Υπηρεσία και από αναρμόδια προς τούτο άτομα.
- Πιστή τήρηση των διαδικασιών λήψης αντιγράφων ασφαλείας (backup), που έχουν καθορισθεί για κάθε πληροφοριακό σύστημα.

Δεν πρέπει να λησμονούμε ότι ένα πληροφοριακό σύστημα δημιουργείται από τον άνθρωπο και λειτουργεί μόνο αν συμμετέχει στη λειτουργία του και ο άνθρωπος. Συνεπώς αναπτύσσεται μια στενή σχέση μεταξύ ανθρώπου και προστασίας-

ασφαλείας του συστήματος. Δύο είναι οι σχέσεις εμπλοκής: η προφύλαξη του συστήματος από απειλές προερχόμενες από τον ίδιο τον άνθρωπο και η ασφάλεια και προστασία του προσωπικού που εργάζεται μέσα στο σύστημα. Και οι δυο αυτές σχέσεις δομούνται πάνω στην ψηφιακή ασφάλεια.

Έτσι οι θεμελιώδεις αρχές που διέπουν την ασφάλεια προσωπικού και σχετίζονται με την ψηφιακή ασφάλεια είναι η «Αρχή του Δικαιώματος Γνώσης» όπου κάθε χρήστης δικαιούται να γνωρίζει μόνο στις πληροφορίες που είναι απαραίτητες για να επιτελέσει το έργο - αποστολή του, η «Αρχή της Πρόσβασης» όπου το προσωπικό ανεξαρτήτως θέσης δικαιούται φυσική πρόσβαση στο πληροφοριακό σύστημα σε όση έκταση επιβάλλεται για την εκτέλεση της αποστολής του και η «Αρχή των Δύο Ατόμων» για την εξάλειψη της πιθανότητας να παραβιασθεί η ασφάλεια του συστήματος από ένα χρήστη.

Σε διαδικασίες που απαιτείται ειδική πρόσβαση, η ταυτόχρονη παρουσία δύο ατόμων καθίσταται αναγκαία. Η παραπάνω αρχή είναι σχετική κυρίως με θέματα ασφαλείας όπως έλεγχος των διαδικασιών ελέγχου πρόσβασης, εκκίνηση - τερματισμός του συστήματος, επεξεργασία διαβαθμισμένων δεδομένων, τροποποίηση ή συντήρηση λογισμικού και υλικού, τήρηση αντιγράφων ασφαλείας (backup) διαβαθμισμένων συστημάτων πληροφορικής κ.α. .



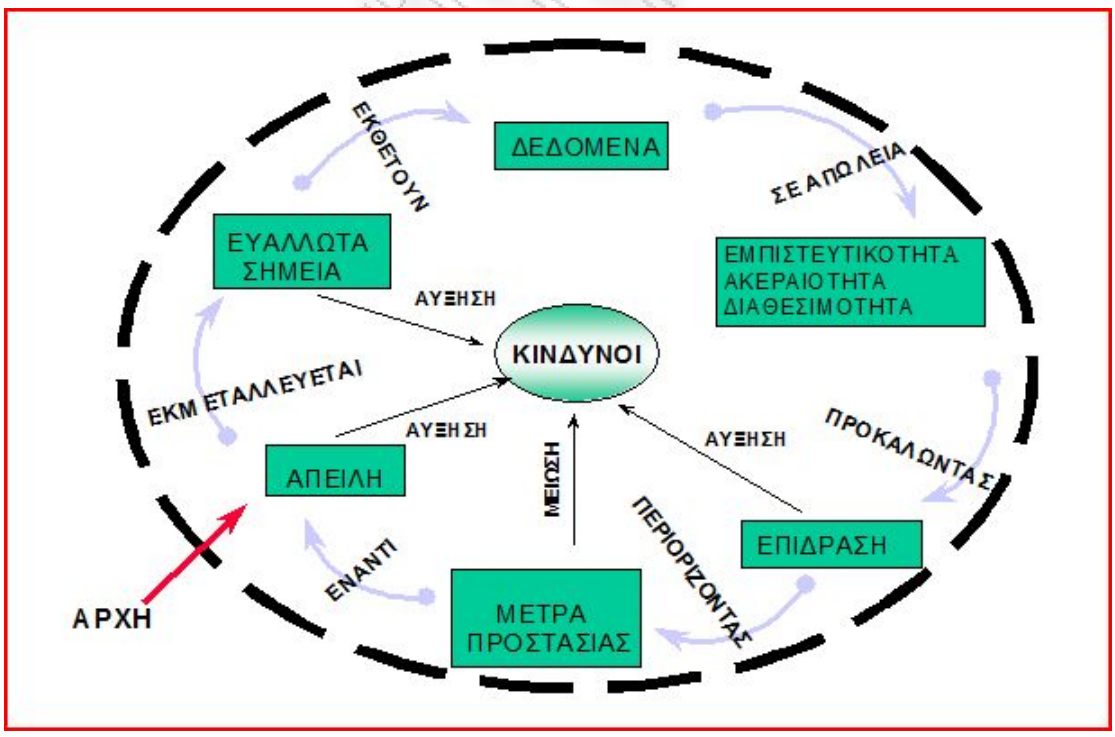
Σχήμα 4-4: Ερωτήματα πλήρους καταγραφής συμβάντων
Πηγή: Εγχειρίδιο ασφάλειας ΠΣ αμερικανικού στρατού

4.3 Ανάλυση βαθμού κινδύνου ασφάλειας

Ελάχιστοι είναι οι οργανισμοί που μπορούν να ανταποκριθούν στο κόστος προστασίας έναντι όλων των κινδύνων (εάν αυτό είναι εφικτό). Αντιθέτως επιδιώκεται η ισορροπία μεταξύ του κόστους μέτρων προστασίας και των πιθανών κινδύνων από τη μη λήψη μέτρων. Η παραπάνω διαδικασία ανάλυσης και απόφασης καλείται ανάλυση βαθμού κινδύνου. Ο αποκαλούμενος «αποδεκτός κίνδυνος» καθορίζει και το ελάχιστο απαραίτητο επίπεδο προστασίας που απαιτεί ένας οργανισμός. Τρεις βασικές συνιστώσες της παραπάνω διαδικασίας είναι η απειλή, το ευπαθές σημείο και τα μέτρα προστασίας [15].

Η *απειλή* είναι κάθε πιθανός κίνδυνος που είναι δυνατόν να προσβάλλει τον Η/Υ ή γενικότερα το πληροφοριακό σύστημα. Ο κίνδυνος μπορεί να προέρχεται από πρόσωπο το οποίο μπορεί να είναι εργαζόμενος, κατάσκοπος, επαγγελματίας, υλικό (λογισμικό ή συσκευή) ή και συμβάν (φωτιά, κεραυνός, σεισμός εχθρική προσβολή) που μπορεί να προσβάλλει το σύστημα σε αναμενόμενο ή μη χρόνο.

Το *ευπαθές σημείο* είναι κάθε στοιχείο του συστήματος που είναι ιδιαίτερα πιθανό να υποστεί προσβολή όπως το προσωπικό που εργάζεται και χρησιμοποιεί το σύστημα, οι επικοινωνίες, οι εγκαταστάσεις ή οποιοδήποτε άλλο μέρος ενός συστήματος πληροφορικής.



Σχήμα 4-5: Κύκλος ανάλυσης κινδύνου.
Πηγή: Εγχειρίδιο διαχείρισης κρίσεων του Fairfax County Public Schools.

Τα *μέτρα προστασίας* είναι το σύνολο των τεχνικών και διαδικασιών που εφαρμόζονται για την προστασία του συστήματος πχ. κωδικοί ασφαλείας, προστασία καλωδιώσεων, συστήματα ασφαλείας, κλειδαριές στις πόρτες κ.α.. Υπάρχουν δύο βασικές κατηγορίες προστασίας ενός συστήματος η προληπτική προστασία και η κατασταλτική προστασία.

Η προληπτική προστασία αφορά την προστασία από πιθανές παραβιάσεις πριν προλάβουν να πραγματοποιηθούν και για το λόγο αυτό έχει μεγαλύτερη αξία καθώς το σύστημα δεν έχει υποστεί ακόμη τις δυσμενείς συνέπειες της προσβολής. Υλοποιείται με την πιστή εφαρμογή των αρχών και της πολιτικής ασφαλείας πληροφορικής. Ενώ η κατασταλτική προστασία υλοποιείται μέσω συγκεκριμένων διαδικασιών οι οποίες αποσκοπούν στην καταγραφή των γεγονότων. Επιτυγχάνεται με μια σειρά από ενέργειες όπως είναι η παρακολούθηση της λειτουργίας και αποτελεσματικότητας των διαδικασιών ασφαλείας, η έγκαιρη αποκάλυψη των παραβιάσεων και αναφορά τους και η αντιμετώπιση της παραβίασης και καταλογισμός ευθυνών εάν υπάρχουν.

Το βασικό σημείο είναι η ανάλυση δηλαδή μια διαδικασία καθορισμού, των απειλών, προσδιορισμού των ευπαθών σημείων και ανάπτυξης των μέτρων προστασίας για να αντιμετωπισθούν τα εκτιμώμενα ως πιθανά ενδεχόμενα. Εμπεριέχει επίσης αξιολόγηση του βαθμού προετοιμασίας ενός οργανισμού για την αντιμετώπιση της χειρότερης των περιπτώσεων που καλείται Σχεδιασμός Έναντι Απρόοπτου (Contingency Planning) ή Χειρισμός Κρίσεων (Crisis Management) [16]. Γενικά υπάρχουν δύο τρόποι ανάλυσης από πλευράς χρονικού προσδιορισμού: η προληπτική εκτίμηση η οποία εκτελείται πριν λάβει χώρα ένα περιστατικό. Και η αποτίμηση αντίδρασης η οποία εκτελείται αφού λάβει χώρα ένα περιστατικό. Και στους δύο τρόπους ακολουθείται η παρακάτω διαδικασία:

i. Προσδιορισμός της Απειλής.
ii. Ανάλυση των ευπαθών σημείων.
iii. Ανάπτυξη μέτρων προστασίας.
iv. Τεκμηρίωση των ευρημάτων και αποφάσεων.

Τα συμπεράσματα που προκύπτουν από την διεξαγωγή μελετών ανάλυσης κινδύνου αναδεικνύονται σε απαραίτητο στοιχείο για τον καθορισμό των παραμέτρων που εξασφαλίζουν την απρόσκοπτη λειτουργία ενός συστήματος σε όλες τις φάσεις του κύκλου ζωής του. Μέσω των μελετών αυτών καθορίζονται οι τομείς στους οποίους

πρέπει να δοθεί ιδιαίτερη προσοχή, αλλά και εκείνοι στους οποίους πιθανόν εφαρμόζονται αδικαιολόγητα αυστηρά μέτρα ασφαλείας που περιορίζουν τη λειτουργικότητα και απόδοση του συστήματος. Δεδομένων των διαφόρων μεθοδολογιών ανάλυσης κινδύνου η υιοθέτηση της πλέον κατάλληλης μεθόδου αποτελεί αντικείμενο προσεκτικής επιλογής και απαιτεί στενή συνεργασία με εξειδικευμένο προσωπικό. Σχηματικά ο κύκλος ανάλυσης κινδύνου σε γενική μορφή δύναται να αποδοθεί όπως φαίνεται στο σχήμα 4-5.

Τέλος θα πρέπει να τονίσουμε ότι στην ανάλυση κινδύνου λαμβάνεται ιδιαίτερα υπόψη το πιο ευάλωτο σημείο αλλά και η μεγαλύτερη απειλή σε ένα πληροφοριακό σύστημα που είναι ο ίδιος ο άνθρωπος. Η απειλή που ο καθένας αντιπροσωπεύει για τους Η/Υ αντιστοιχεί με το είδος πρόσβασης, δηλαδή το μέγεθος της βλάβης που είναι δυνατόν να προκληθεί εξαρτάται σημαντικά από το ποιο είναι το επίπεδο πρόσβασης με βάση την αρχή του δικαιώματος γνώσης. Με την αρχή αυτή αποτρέπεται η εσκεμμένη απόκτηση, καταγραφή ή καταστροφή μεγάλης σημασίας διαβαθμισμένων πληροφοριών ή και η εξ' αμελείας καταστροφή αρχείων.

Το μέγεθος εξειδικευμένης γνώσης δηλαδή το επίπεδο γνώσης του συστήματος από τον χρήστη που επιχειρεί την πρόσβαση, είναι ανάλογο της βλάβης που μπορεί να προκληθεί. Ένας χρήστης, αναλυτής ή και προγραμματιστής μπορεί να μολύνει το σύστημα με ένα καταστροφικό πρόγραμμα προκαλώντας σοβαρή βλάβη. Αλλά και η ελλιπής γνώση μπορεί να εκθέσει σε σοβαρό κίνδυνο την ασφάλεια του πληροφοριακού συστήματος καθώς και το κίνητρο, δηλαδή το αψυχολόγητο του ανθρώπινου παράγοντα αποτελεί σοβαρό κίνδυνο, δεδομένου ότι προσωπικό το οποίο είναι δυσαρεστημένο από πολιτική προσωπικού ενός οργανισμού όπως θέματα συμπεριφοράς, δικαιοσύνης προαγωγών κ.α. είναι πιο ευάλωτο στην ηθελημένη πρόκληση βλάβης στο πληροφοριακό σύστημα.

Επομένως η προστασία προσωπικού είναι πολύ σπουδαία, λαμβάνοντας υπόψη ότι ο άνθρωπος είναι το βασικό στοιχείο του πληροφοριακού συστήματος. Ασφάλεια και προστασία σημαίνει κατ' ελάχιστον την προστασία της ψυχικής και σωματικής ακεραιότητας του ανθρώπου χρήστη του συστήματος, την προστασία από εξαναγκασμούς και εκβιασμούς, την προφύλαξη του προσωπικού από το να διαχειρίζεται δεδομένα χωρίς ειδική εξουσιοδότηση, την εκπαίδευση, διευκόλυνση και εθισμό στο να διαχειρίζεται και μεταβιβάζει σωστά τις πληροφορίες του συστήματος σύμφωνα με την πολιτική και πρακτική ασφαλείας του οργανισμού [17].

Η εκπαίδευση του προσωπικού είναι βασική προϋπόθεση για την επίτευξη ασφάλειας, η οποία κοστίζει σε χρόνο και χρήμα χρήσης του συστήματος. Θέματα και

αντικείμενα εκπαίδευσης που πρέπει να ακολουθούνται από την διεύθυνση ενός οργανισμού είναι: θέματα πολιτικής ασφαλείας, οι διαδικασίες και ο τρόπος εφαρμογής αυτών, η ακολουθούμενη πολιτική για τα αντίγραφα ασφαλείας δεδομένων, την αποθήκευσή τους και τη χρήση του λογισμικού, την χρησιμοποίηση τεχνικών και ελέγχων για την προστασία του συστήματος, την επιτήρηση των συστημάτων και του λογισμικού για εντοπισμό "παράξενης συμπεριφοράς", διαδικασία αναφοράς και χειρισμού του συμβάντος, τις διαδικασίες διατήρησης και ανάκτησης των δεδομένων. Η εξοικείωση με τα παραπάνω θέματα καθιστά το προσωπικό φύλακα του συστήματος και στην ανάλυση κινδύνου μικρό «πονοκέφαλο» για τους αναλυτές.

4.4 Πρότυπα πιστοποίησης

Τα αυτοματοποιημένα πληροφοριακά συστήματα χρησιμοποιούνται σε χώρους εργασίας διαφόρων απαιτήσεων διαβάθμισης ασφαλείας, από τις πλέον υψηλές μέχρι το εντελώς αδιαβάθμητο. Το γεγονός αυτό οδήγησε στην ανάγκη καθιέρωσης ολοκληρωμένης μεθοδολογίας για την ενιαία αξιολόγηση των συστημάτων με βάση πρότυπα που παρέχουν αντικειμενικά κριτήρια για τον καθορισμό του επιπέδου διαβάθμισής τους. Γι’ αυτό το λόγο αναπτύχθηκε το πρότυπο κριτηρίων αξιολόγησης ασφαλών πληροφοριακών συστημάτων TCSEC (Trusted Computer Systems Evaluation Criteria) στις ΗΠΑ, ενώ στην Ευρωπαϊκή Ένωση αναπτύσσεται αντίστοιχα το πρότυπο κριτηρίων αξιολόγησης ασφαλείας τεχνολογίας πληροφορικής ITSEC (Information Technology Security Evaluation Criteria) [4-7].

Τα Επίπεδα Εμπιστοσύνης Πληροφοριακών Συστημάτων και τα γενικά χαρακτηριστικά των συστημάτων που εντάσσονται σε κάθε επίπεδο εμπιστοσύνης από πλευράς ασφαλείας είναι:

α. Επίπεδο "Δ" (D Level of Trust)

Τα συστήματα που εντάσσονται στο επίπεδο αυτό, χαρακτηρίζονται από την παροχή στοιχειώδους ή καμίας ασφάλειας και εντάσσονται σε αυτό τα συστήματα που αποτυγχάνουν να ενταχθούν σε ανώτερο. Κλασικό παράδειγμα αυτής της κατηγορίας είναι ο προσωπικός υπολογιστής με το λειτουργικό σύστημα MS-DOS.

β. Επίπεδο "Γ" (C Level of Trust)

Τα συστήματα που ανήκουν στο επίπεδο εμπιστοσύνης "Γ" επιτρέπουν τη συνεργασία χρηστών και την επεξεργασία δεδομένων μιας διαβάθμισης. Στο

υποεπίπεδο "Γ1" (διακριτή προστασία, "C1") υπάγονται συστήματα τα οποία έχουν τη δυνατότητα να αναγνωρίσουν θετικά τους υποψήφιους χρήστες και να προστατεύσουν τα δεδομένα τους από άλλους. Στο υποεπίπεδο "Γ2" (ελεγχόμενη πρόσβαση, "C2") ανήκουν συστήματα που μπορούν να καταγράφουν και ανακαλούν τα στοιχεία κάθε πρόσβασης των χρηστών για κάθε αντικείμενο του συστήματος. Τα διαβαθμισμένα συστήματα πληροφορικής του Στρατού πρέπει να ανήκουν τουλάχιστον στο υποεπίπεδο Γ2.

γ. Επίπεδο "Β" (B Level of Trust)

Τα συστήματα που εντάσσονται στο επίπεδο αυτό ακολουθούν τυποποιημένες διαδικασίες ελέγχου πρόσβασης. Στο υποεπίπεδο Β1 (διαβαθμισμένη προστασία) κάθε χρήστης ή στοιχείο του συστήματος πρέπει να έχει διαβαθμιστεί ανάλογα. Αντίθετα δεν είναι απαραίτητο να έχει διαβαθμιστεί ένα στοιχείο ή χρήστης που δεν προβλέπεται να ελέγχεται. Στα συστήματα του υποεπιπέδου Β2 (δομημένη προστασία) πρέπει να είναι δυνατός ο έλεγχος της πρόσβασης σε όλα τα στοιχεία και τους χρήστες. Πρέπει να γίνεται έλεγχος για την αποκάλυψη συγκαλυμμένων διαύλων και να ορίζεται πρόσωπο υπεύθυνο για την ασφάλειά τους. Στο υποεπίπεδο Β3 (προστατευόμενα πεδία) εντάσσονται τα συστήματα που είναι σχεδιασμένα με βάση συστηματική μεθοδολογία για τις λειτουργίες ασφαλείας. Τα συστήματα αυτά είναι πολύ ανθεκτικά σε προσβολές "εξειδικευμένων ομάδων" και περιλαμβάνουν εργαλεία λογισμικού για τον εκ των υστέρων εντοπισμό μιας προσβολής.

δ. Επίπεδο "Α"

Αποτελεί το υψηλότερο επίπεδο εμπιστοσύνης και είναι γνωστό και ως "Πιστοποιημένη Σχεδίαση". Περιλαμβάνει όλα τα χαρακτηριστικά ασφαλείας των προηγουμένων επιπέδων και επιπλέον απαιτεί τη λεπτομερή εξέταση της σχεδίασης του συστήματος ασφαλείας. Η σχεδίαση αυτή απαιτείται να αναλυθεί και εγκριθεί από άριστα εκπαιδευμένο και εξειδικευμένο προσωπικό ασφαλείας. Επιπλέον απαιτείται να εξασφαλίζεται ότι όλα τα εξαρτήματα, που συνθέτουν το σύστημα, προέρχονται από ασφαλείς πηγές και δεν υπάρχει καμιά ανάμειξη με αυτά κατά τη διακίνησή τους.

4.5 Πολυεπίπεδη ασφάλεια

Η ασφάλεια αποτελεί βασικό στοιχειό σε κάθε οργανισμό διότι η διασφάλιση των πληροφοριών που βρίσκονται στην κατοχή του οργανισμού αποτελούν περιουσιακό στοιχείο ζωτική σημασίας. Η ίδια φιλοσοφία διέπει και τα στρατιωτικά περιβάλλοντα

σχετικά με την διασφάλιση των πληροφοριών με την διαφορά ότι η αποκάλυψη τους θέτει σε κίνδυνο την εθνική ασφάλεια.

Η λύση που προτείνουμε στην διασφάλιση των πληροφοριών που διακινούνται στο ολοκληρωμένο πληροφοριακό σύστημα που παρουσιάζουμε «σύστημα διαχείρισης εγγράφων με ενσωματωμένη ψηφιακή υπογραφή», είναι η δημιουργία πολλών επιπέδων ασφαλείας που δομούνται στο ψηφιακό επίπεδο ασφάλειας και σκοπό έχουν τα επίπεδα αυτά να δημιουργήσουν επαναλαμβανόμενα στρώματα θωράκισης της εισόδου του πληροφορικού συστήματος.

Από την άλλη πλευρά με την δομή αυτή επιτυγχάνεται μια ακόμη πολύ σπουδαία δικλείδα ασφαλείας που προστατεύει το σύστημα από εσωτερικούς κινδύνους. Η εσωτερική ασφάλεια είναι ένα πρόβλημα που πάντα απασχολούσε τους αρμόδιους, μετά από στατιστικές μελέτες κατέληξαν στο ότι οι περισσότεροι κίνδυνοι προέρχονται από εσωτερικούς παράγοντες και ιδιαίτερα από ανεκπαίδευτους χρήστες ή δυσαρεστημένους υπαλλήλους από την πολιτική χειρισμού του προσωπικού.

Με την λύση που παρουσιάζουμε οποιοσδήποτε επιχειρήσει να ενεργήσει επιθετικά εν γνώση ή αγνοία μπορεί και ο ίδιος να εντοπιστεί και οι ενέργειες του να προσδιοριστούν και να ελέγχουν, χωρίς κατ' ουσία να προκληθεί καμία βλάβη στο σύστημα. Συγκεκριμένα δεν υπάρχουν αποθηκευτικές συσκευές εξόδου προκειμένου να απομακρυνθούν ψηφιακά έγγραφα, τηρείται back up σε περίπτωση διαγραφής αρχείων και επίσης κάποιο έγγραφο που είναι για να αποθηκευτεί στο σύστημα ελέγχεται για υιούς από τον διαχειριστή και εφόσον διαπιστωθεί ότι είναι καθαρό τότε αποθηκεύεται οριστικά.

Αναλυτικά τα επίπεδα που δημιουργήσαμε είναι:

- Η ύπαρξη μοναδικού usb memory stick για κάθε χρήστη που θα το παραλαμβάνει – χρεώνεται από τον διαχειριστή του συστήματος και θα περιέχει το ιδιωτικό κλειδί της προσωπικής του ψηφιακής υπογραφής.

- Η εξασφάλιση του περιεχομένου του usb memory stick με κρυπτογράφηση του, ώστε σε περίπτωση απώλειας να μην είναι δυνατή η ανάγνωση του ιδιωτικού κλειδιού.

- Μοναδικά στοιχεία για την είσοδο του χρήστη στο σύστημα (username-password).

- Για την είσοδο στο σύστημα απαιτείται η τοποθέτηση του προσωπικού usb memory stick.

- Διασταύρωση στοιχείων χρήστη και ιδιωτικού κλειδιού ώστε να επιτρέψει το σύστημα την περεταίρω χρήση του.
- Δενδροειδής διάταξη φακέλων με δυνατότητα εφαρμογής δικαιωμάτων.

Το κάθε επίπεδο περιγράφεται αναλυτικά παρακάτω στο κεφάλαιο 5 στην σχετική ενότητα όπου αναφέρεται η υλοποίηση της πολυεπίπεδης ασφάλειας στο συγκεκριμένο σύστημα που συζητάμε.

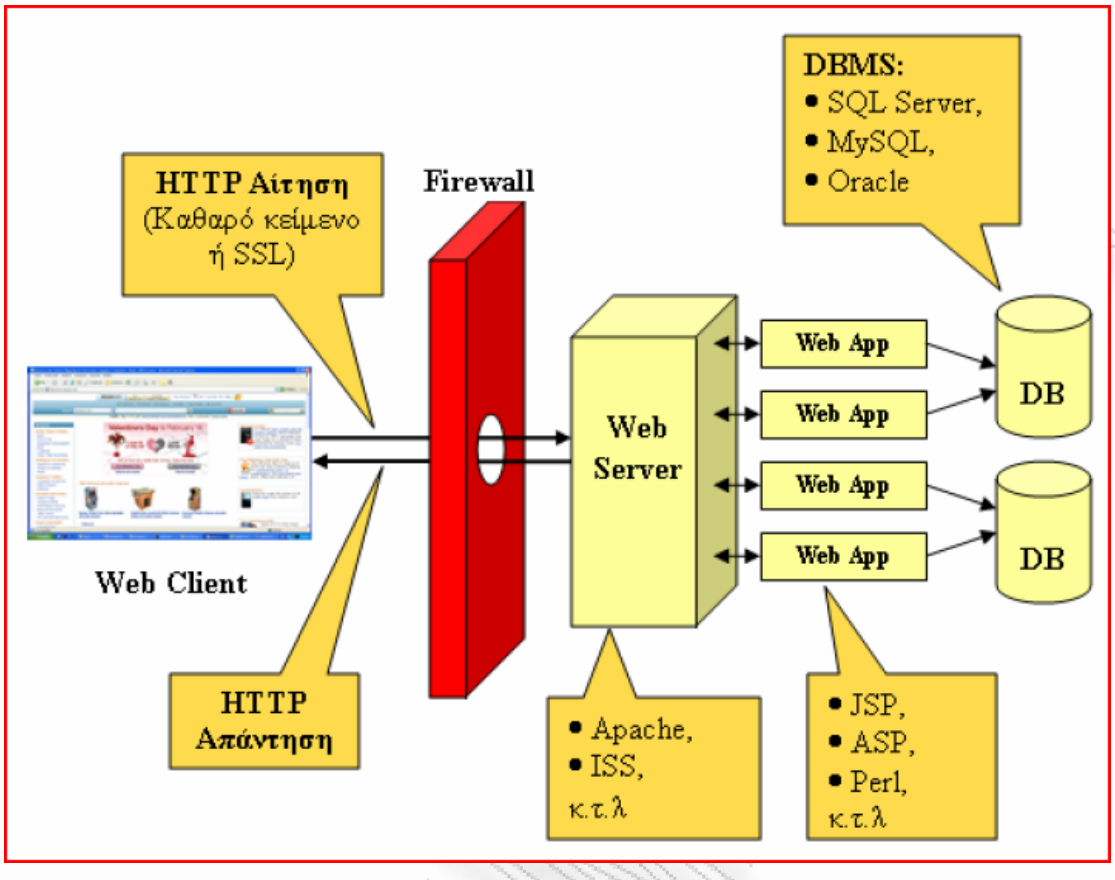
ΚΕΦΑΛΑΙΟ 5ο

ΥΛΟΠΟΙΗΣΗ ΕΦΑΡΜΟΓΗΣ

Στα προηγούμενα κεφάλαια προσεγγίσαμε θεωρητικά τους τρεις βασικούς άξονες του συστήματος που αναπτύσσουμε σε αυτή την εργασία. Σε αυτό το κεφάλαιο θα παρουσιάσουμε αναλυτικά την υλοποίηση του. Η υλοποίηση κινείται όπως αναφέραμε και προηγουμένως σε τρεις άξονες: ο πρώτος αφορά την επιλογή του συστήματος διαχείρισης εγγράφων και της γενικότερης υποδομής που απαιτείται για να λειτουργήσει, ο δεύτερος αφορά την ενσωμάτωση της ψηφιακής υπογραφής στο σύστημα και ο τρίτος και τελευταίος άξονας αφορά την υλοποίηση των επιπέδων ασφαλείας που σχεδιάσαμε για να θωρακίσουμε το συστήματος ως οντότητα.

5.1 Τεχνική υποδομή δικτυακής – προγραμματιστικής υλοποίησης

Αρχικά θα παρουσιάσουμε την δικτυακή υποδομή και έπειτα τις προγραμματιστικές απαιτήσεις που προέκυψαν. Στόχος αυτής της παρουσίασης είναι να δείξουμε το πόσο σύνθετο είναι να αναπτυχθεί μια τέτοια εφαρμογή καθόσον απαιτεί την γνώση πολλών επιμέρους στοιχείων που σχετίζονται με την πληροφορική γενικότερα.



Σχήμα 5-1: Τυπικό παράδειγμα εφαρμογής ιστού.

5.1.1 Δικτυακή υποδομή

Στο Σχήμα 1-1 παρουσιάζεται ένα τυπικό παράδειγμα εφαρμογής ιστού, όπου ο πελάτης αλληλεπιδρά με μια εφαρμογή, που βρίσκεται εγκατεστημένη στην πλευρά του διακομιστή, στέλνοντας αιτήσεις και αναμένοντας την απάντηση της εφαρμογής. Η εφαρμογή ιστού αλληλεπιδρά με την υποκείμενη βάση δεδομένων για να ανακτήσει τα δεδομένα που προκύπτουν από την επεξεργασία του αιτήματος και στη συνέχεια επιστρέφει τα δεδομένα αυτά, ώστε να εμφανιστούν στο περιβάλλον του χρήστη. Η πρόσβαση στη βάση δεδομένων γίνεται με την εκτέλεση δυναμικών SQL ερωτημάτων που δημιουργούνται κατά το χρόνο εκτέλεσης και διαμορφώνονται ανάλογα με τα δεδομένα του χρήστη σε πεδία εισόδου της εφαρμογής.

5.1.2 HTML, PHP, JAVASRCIPT, SQL, XML

Για την ανάπτυξη της εφαρμογής χρησιμοποιήθηκαν οι εξής γλώσσες: HTML, PHP, JAVASRCIPT, SQL, XML. Για κάθε μια από αυτές θα κάνουμε μια πολύ σύντομη αναφορά απλά και μόνο για να δείξουμε σε πιο σημείο η κάθε μια δόμησε το σύστημα.

HTML

Τα αρχικά HTML προέρχονται από τις λέξεις Hyper Text Markup Language. Η html δεν είναι μια γλώσσα προγραμματισμού. Είναι μια γλώσσα σήμανσης (markup language), δηλαδή ένας ειδικός τρόπος γραφής κειμένου. Αποτελεί υποσύνολο της γλώσσας SGML (Standard Generalized Markup Language) που επινοήθηκε από την IBM προκειμένου να λυθεί το πρόβλημα της μη τυποποιημένης εμφάνισης κειμένων στα διάφορα υπολογιστικά συστήματα. Ο φυλλομετρητής αναγνωρίζει αυτόν τον τρόπο γραφής και εκτελεί τις εντολές που περιέχονται σε αυτόν. Αξίζει να σημειωθεί ότι η html είναι η πρώτη και πιο διαδεδομένη γλώσσα περιγραφής της δομής μιας ιστοσελίδας. Η html χρησιμοποιεί ειδικές ετικέτες «tags» για να δώσει τις απαραίτητες οδηγίες στον φυλλομετρητή. Οι ετικέτες είναι εντολές που συνήθως ορίζουν την αρχή ή το τέλος μιας λειτουργίας. Τα tags βρίσκονται πάντα μεταξύ των συμβόλων « < » και « >», π.χ. *<BODY>.* Οι οδηγίες δεν επηρεάζονται από το αν έχουν γραφτεί με πεζά (μικρά) ή κεφαλαία. Ένα αρχείο HTML πρέπει να έχει κατάληξη htm ή html [18].

PHP

Η PHP είναι μια γλώσσα προγραμματισμού για τη δημιουργία σελίδων ιστού με δυναμικό περιεχόμενο. Μια σελίδα PHP περνά από επεξεργασία από ένα συμβατό διακομιστή του Παγκόσμιου Ιστού (π.χ. Apache), ώστε να παραχθεί σε πραγματικό χρόνο το τελικό περιεχόμενο, που θα σταλεί στο πρόγραμμα περιήγησης των επισκεπτών σε μορφή κώδικα HTML.

Ένα αρχείο με κώδικα PHP θα πρέπει να έχει την κατάλληλη επέκταση π.χ. *.php, *.php4, *.phtml κ.ά. . Επίσης ακόμη κι όταν ένα αρχείο έχει την επέκταση .php, θα πρέπει ο server να είναι ρυθμισμένος για να επεξεργάζεται κώδικα PHP. Ο διακομιστής Apache, που χρησιμοποιείται σήμερα ευρέως σε συστήματα με τα λειτουργικά συστήματα Linux και Microsoft Windows, υποστηρίζει εξ ορισμού την εκτέλεση κώδικα PHP [19].

JAVASRCIPT

JavaScript είναι γλώσσα προγραμματισμού η οποία έχει σαν σκοπό την παραγωγή δυναμικού περιεχομένου και την εκτέλεση κώδικα στην πλευρά του πελάτη (client-side) σε ιστοσελίδες. Το πρότυπο της γλώσσας κατά τον οργανισμό τυποποίησης ECMA ονομάζεται ECMAscript.

Όπως και η PHP, η Javascript έχει βασιστεί όσον αφορά τον τρόπο σύνταξης του κώδικά της στη γλώσσα προγραμματισμού C, με την οποία παρουσιάζει πολλές ομοιότητες. Όμως ενώ η PHP είναι μια γλώσσα προγραμματισμού που «τρέχει»

στην πλευρά του εξυπηρετητή, η Javascript είναι μια γλώσσα που «τρέχει» στην πλευρά του πελάτη.

Αυτό σημαίνει ότι η επεξεργασία του κώδικα Javascript και η παραγωγή του τελικού περιεχομένου HTML δεν πραγματοποιείται στον server, αλλά στο πρόγραμμα περιήγησης των επισκεπτών. Αυτή η διαφορά έχει και πλεονεκτήματα και μειονεκτήματα για καθεμιά από τις δύο γλώσσες. Συγκεκριμένα, η Javascript δεν έχει καμία απαίτηση από πλευράς δυνατοτήτων του εξυπηρετητή για να εκτελεστεί πχ επεξεργαστική ισχύ, συμβατό λογισμικό διακομιστή κ.α., αλλά βασίζεται στις δυνατότητες του φυλλομετρητήhttp://el.wikipedia.org/wiki/Web_browser των επισκεπτών. Επίσης μπορεί να ενσωματωθεί σε στατικές σελίδες HTML. Παρόλα αυτά, οι δυνατότητές της είναι σημαντικά μικρότερες από αυτές της PHP και δεν παρέχει συνδεσιμότητα με βάσεις δεδομένων [20].

SQL

Η SQL (Structured Query Language) είναι μία γλώσσα υπολογιστών, που σχεδιάστηκε για τη διαχείριση δεδομένων, σε ένα σύστημα διαχείρισης σχεσιακών βάσεων δεδομένων (Relational Database Management System, RDBMS) και η οποία, αρχικά, βασίστηκε στη σχεσιακή άλγεβρα. Η γλώσσα περιλαμβάνει δυνατότητες ανάκτησης και ενημέρωσης δεδομένων, δημιουργίας και τροποποίησης σχημάτων και σχεσιακών πινάκων, αλλά και ελέγχου πρόσβασης στα δεδομένα.

Η SQL αναπτύχθηκε στην IBM από τους Andrew Richardson, Donald C. Messerly και Raymond F. Boyce, στις αρχές της δεκαετίας του 1970. Αυτή η έκδοση, αποκαλούμενη αρχικά SEQUEL, είχε ως σκοπό να χειριστεί και να ανακτήσει τα στοιχεία που αποθηκεύτηκαν στο πρώτο RDBMS της IBM, το System R.

Το πρώτο σύστημα διαχείρισης σχεσιακών βάσεων δεδομένων (RDBMS) ήταν το RDMBS που αναπτύχθηκε στο MIT, στις αρχές της δεκαετίας του 1970 και η Ingres, που αναπτύχθηκε το 1974 στο Πανεπιστήμιο Μπέρκλεϋ. Η Ingres εφάρμοσε μία γλώσσα διατύπωσης ερωτήσεων γνωστή ως QUEL, το οποίο αντικαταστάθηκε αργότερα στην αγορά από την SQL.

Η γλώσσα SQL υποδιαιρείται σε διάφορα γλωσσικά στοιχεία, που περιλαμβάνουν: εκφράσεις, που μπορούν να παραγάγουν είτε τις κλιμακωτές τιμές είτε πίνακες που αποτελούνται από στήλες και σειρές στοιχείων, κατηγορήματα, που διευκρινίζουν τους όρους που μπορούν να αξιολογηθούν σαν σωστό ή λάθος, ερωτήματα, που ανακτούν τα στοιχεία βασισμένες σε ειδικά κριτήρια και δηλώσεις, που μπορούν να

έχουν μια επίδραση στα σχήματα και τα στοιχεία, ή που μπορούν να ελέγξουν τη ροή του προγράμματος και τις συνδέσεις από άλλα προγράμματα [21].

XML

Η XML (Extensible Markup Language) είναι μία γλώσσα σήμανσης, που περιέχει ένα σύνολο κανόνων για την ηλεκτρονική κωδικοποίηση κειμένων. Ορίζεται, κυρίως, στην προδιαγραφή XML 1.0, που δημιούργησε ο διεθνής οργανισμός προτύπων W3C (World Wide Web Consortium), αλλά και σε διάφορες άλλες σχετικές προδιαγραφές ανοιχτών προτύπων.

Η XML σχεδιάστηκε δίνοντας έμφαση στην απλότητα, τη γενικότητα και τη χρησιμότητα στο Διαδίκτυο. Είναι μία μορφοποίηση δεδομένων κειμένου, με ισχυρή υποστήριξη Unicode για όλες τις γλώσσες του κόσμου. Αν και η σχεδίαση της XML εστιάζει στα κείμενα, χρησιμοποιείται ευρέως για την αναπαράσταση αυθαίρετων δομών δεδομένων, που προκύπτουν για παράδειγμα στις υπηρεσίες ιστού.

Υπάρχει μία ποικιλία διεπαφών προγραμματισμού εφαρμογών, που μπορούν να χρησιμοποιούν οι προγραμματιστές, για να προσπελαύνουν δεδομένα XML, αλλά και διάφορα συστήματα σχημάτων XML, τα οποία είναι σχεδιασμένα για να βοηθούν στον ορισμό γλωσσών, που προκύπτουν από την XML. Έως το 2009, έχουν αναπτυχθεί εκατοντάδες γλώσσες που βασίζονται στην XML, συμπεριλαμβανομένων του RSS, του SOAP και της XHTML.

Οι χαρακτήρες που απαρτίζουν ένα κείμενο XML, αποτελούν είτε τη σήμανση είτε το περιεχόμενό του. Η σήμανση και το περιεχόμενο, μπορούν να επισημανθούν και να διακριθούν, ύστερα από την εφαρμογή κάποιων απλών συντακτικών κανόνων. Όλα τα αλφαριθμητικά που συνιστούν τη σήμανση, είτε ξεκινούν με το χαρακτήρα "<" και καταλήγουν στο χαρακτήρα ">", είτε ξεκινούν με το χαρακτήρα "&" και καταλήγουν στο χαρακτήρα ";". Ακολουθίες χαρακτήρων που δε συνιστούν τη σήμανση, αποτελούν το περιεχόμενο ενός κειμένου XML [22].

5.2 Υλοποίηση συστήματος διαχείρισης εγγράφων

Στην παρούσα ενότητα θα παρουσιάσουμε το σύστημα διαχείρισης εγγράφων που επιλέξαμε να εγκαταστήσουμε, προκειμένου να ενσωματώσουμε σε αυτό την ψηφιακή υπογραφή και να δημιουργήσουμε τα επίπεδα ασφαλείας. Το jsmallfib είναι ένα πακέτο ανοιχτού κώδικα που επιτρέπει σε οποιοιδήποτε χρήστη να κάνει τις

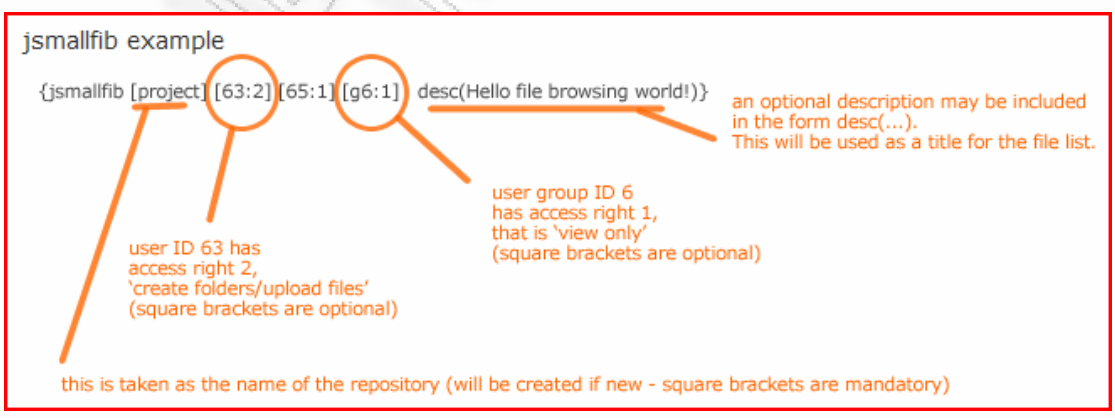
δίκες του παρεμβάσεις, προσθήκες-αφαιρέσεις για να καλύψει τις ανάγκες που ενδεχομένως να μην καλύπτει το υπάρχων.

Το jsmallfib είναι ένα πρόσθετο που μπορεί να συμπεριληφθεί σε μια εφαρμογή ιστού που δομείτε με το λογισμικό ανοιχτού κώδικα Joomla. Με το πρόσθετο αυτό εξάρτημα αρχεία και φάκελοι μπορούν να τοποθετηθούν εντός συγκεκριμένου σημείου του συστήματος αρχείων της εφαρμογής διαδικτύου και ανάλογα με τα δικαιώματα του χρήστη ή της ομάδας να γίνει φόρτωση, μεταφόρτωση, δημιουργία φακέλων, μετονομασία ή διαγραφή αρχείων και φακέλων. Επίσης μπορεί να γίνει καταγραφή των ενεργειών, τις οποίες για να τις παρακολουθήσει κάποιος πρέπει να έχει τα ανάλογα δικαιώματα.

Προκειμένου να επιτευχθεί αυτή η λειτουργικότητα το άρθρο πρέπει να περιέχει μια γραμμή κειμένου με τη μορφή:

Jsmallfib [repository]

όπου «jsmallfib» είναι η εντολή, η οποία πρέπει να γράφεται ακριβώς όπως φαίνεται, επίσης μπορούν χρησιμοποιηθούν κεφαλαία γράμματα και θα πρέπει να ακολουθεί αμέσως μετά αγκύλη, χωρίς κενό διάστημα και «[repository]» είναι μια προαιρετική παράμετρος που δείχνει τον αρχικό φάκελο του χώρου αποθήκευσης. Αυτός ο φάκελος θα πρέπει να βρίσκεται μέσα στη διαδρομή που καθορίζεται στις παραμέτρους που ρυθμίζονται από το panel διαχείρισης του εξαρτήματος. Η διαδρομή μπορεί να ορίζεται σε σχέση με το ριζικό φάκελο της διαδικτυακής εφαρμογής, ή να εκφραστεί ως μια απόλυτη διαδρομή (χρήσιμο εάν η διαδρομή είναι έξω από το web root directory).



Σχήμα 5-2: Βασική γραμμή κώδικα ενεργοποίησης καταλόγου χρήστη.
Πηγή: Εγχειρίδιο χρήσης Jsmallfib.

Επίσης αυτό σύστημα διαχείρισης εγγράφων υποστηρίζει την δυνατότητα να ορισθεί μια αποθήκη (κατάλογος) που ονομάζεται [USERBOUND], η οποία επιτρέπει πρόσβαση μόνο σε χρήστες που έχουν δικαίωμα σε αυτό τον τομέα. Η εντολή για την δημιουργία αυτού του χώρου είναι:

Jsmallfib [USERBOUND]

Επίσης υποστηρίζει την δυνατότητα να ορισθεί μια αποθήκη που ονομάζεται [GROUPBOUND], το οποίο παρέχει σε μια συγκεκριμένη ομάδα χρηστών την πρόσβαση σε μια ειδική περιοχή η οποία εξαρτάται από ην διαδικτυακή εφαρμογή.

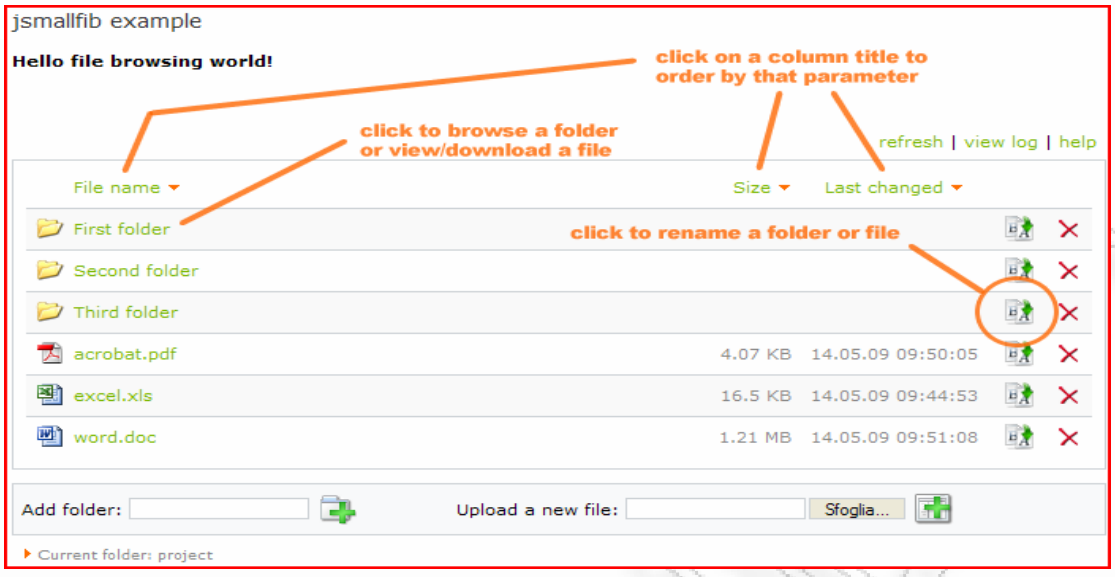
Jsmallfib [GROUPBOUND]

Όσον αφορά τα δικαιώματα, οι προεπιλεγμένες ρυθμίσεις είναι διαμορφώσιμες παράμετροι εντός του plugin, τόσο για την επίσκεψη όσο και για την χρήση από εγγεγραμμένους χρήστες. Οι ρυθμίσεις για την εφαρμογή των δικαιωμάτων πρόσβασης μπορούν προαιρετικά να παρακαμφθούν με την προσθήκη κατάλληλων εντολών μετά την παράμετρο προσδιορισμού του καταλόγου στην βασική εντολή, χρησιμοποιώντας αυτή τη μορφή:

{Jsmallfib [repository] [ID 1: permission1] ... [IDN:] permissionN}

όπου ID είναι ο κωδικός που δίνει η διαδικτυακή εφαρμογή στον χρήστη που ανοίγει λογαριασμό. Μέσω αυτού του κωδικού καθορίζονται και τα δικαιώματα του στον κατάλογο «αποθήκη». Στο σχήμα 5-2 φαίνεται ένα παράδειγμα. Ειδικότερα τα δικαιώματα, κατά αύξουσα σειρά, είναι τα εξής:

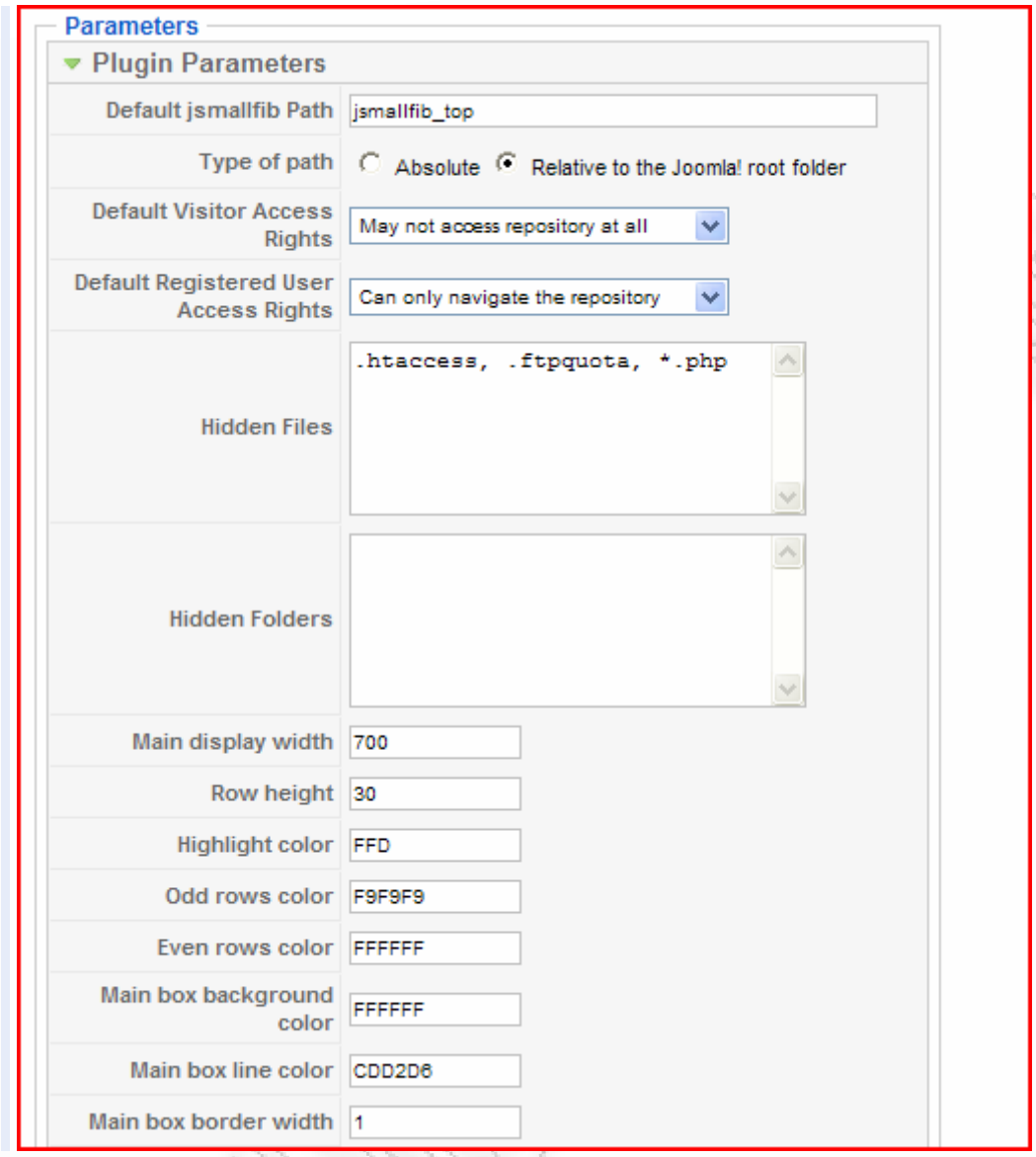
0 -> δεν έχουν πρόσβαση.
1 -> έχουν πρόσβαση (μπορούν να επισκέπτονται μόνο τον ορισθέντα κατάλογο)
2 -> δυνατότητα να δημιουργήσουν φακέλους, να ανεβάσουν αρχεία και να μετονομάζουν τα αρχεία και τους φακέλους.
3 -> μπορείτε να διαγράψετε τα αρχεία, αλλά όχι τους φακέλους.
4 -> μπορείτε να διαγράψετε αρχεία και φακέλους.
5 -> μπορείτε επιπλέον να δείτε αρχεία καταγραφής



Σχήμα 5-3: Διεπαφή jsmallfib χρήστη

Εάν χρησιμοποιηθεί το πρόθεμα G τότε αφορά το σύνολο των χρηστών που έχουν καταχωρηθεί σε κάποια κατηγορία της διαδικτυακής εφαρμογής «επικοινωνία». Κάθε ομάδα χρηστών στην κατηγορία επικοινωνία έχει τον δικό της κωδικό. Αυτός ο κωδικός ακλουθεί μετά το γράμμα G, οπότε τα δικαιώματα αφορούν όλους τους χρήστες της συγκεκριμένης ομάδας

Μπορεί επίσης, να ορισθεί μια περιγραφή για τον αποθηκευτικό χώρο, με την μορφή «desc» εντός των αγκύλων. Αυτό θα πρέπει να συμπεριληφθεί κάτω από τον τίτλο και πριν από τα αρχεία ή τους φακέλους.



Σχήμα 5-4: Διεπαφή jsmallfib διαχειριστή.

Όσον αφορά τα εικονίδια που αντιπροσωπεύουν τις επεκτάσεις αρχείων, αυτά μπορούν να βρεθούν στο φάκελο plugins / content / jsmallfib εντός της κύριας εφαρμογής. Τα εικονίδια είναι PNG αρχεία εικόνας και ονομάζονται ext.png, όπου πριν την επέκταση αρχείου είναι η επέκταση που εκπροσωπεί. Οπότε σύμφωνα με αυτό το στοιχείο γίνεται η επιλογή και εμφάνιση του κατάλληλου εικονιδίου στον πίνακα των περιεχομένων (σχήμα 5.3)

Τέλος στο panel του διαχειριστή για το πρόσθετο εξάρτημα που αντιπροσωπεύει το σύστημα διαχείρισης εγγράφων υπάρχει η δυνατότητα να ρυθμιστεί και η εμφάνιση του συστήματος π.χ. μέγεθος κελιών, χρώμα γραμμών, χρώμα φόντου κ.α. (σχήμα 5.4) [23].

5.3 Υλοποίηση της ψηφιακής υπογραφής της εφαρμογής

Παρακάτω παρουσιάζεται αναλυτικά η υλοποίηση της ψηφιακής υπογραφής, η οποία είναι χωρισμένη σε τρία τμήματα: στην δημιουργία του δημόσιου και του ιδιωτικού κλειδιού, στην ψηφιακή υπογραφή των εγγράφων που αποθηκεύονται στο σύστημα και τέλος στην αποθήκευση των μεταδεδομένων που σχετίζονται με την υπογραφή κάθε εγγράφου.

Ιδιαίτερο ρόλο στην υλοποίηση της ψηφιακής υπογραφής διαδραματίζει και η βιβλιοθήκη εξασφάλισης επικοινωνιών «phpseclib», όπως ονομάζεται από τον δημιουργό της, η οποία χρησιμοποιήθηκε και περιλαμβάνει όλες εκείνες τις συναρτήσεις που δημιουργούν τα δημόσια και ιδιωτικά κλειδιά, καθώς και για να γίνει η κρυπτογράφηση με το αλγόριθμο RSA. Λόγω της σπουδαιότητα αφιερώνεται μια ενότητα για την παρουσίαση της.

5.3.1 Η βιβλιοθήκη εξασφάλισης επικοινωνιών «phpseclib»

Η βιβλιοθήκη phpseclib είναι ένα πακέτο που προωθείται μέσω της κοινότητας ανοιχτού λογισμικού PEAR και απευθύνεται σε προγραμματιστές που δημιουργούν εφαρμογές ιστού. Στην κοινότητα ανήκουν ένας μεγάλος αριθμός προγραμματιστών που προσφέρουν τις γνώσεις τους εθελοντικά ενώ τα λειτουργικά έξοδα καλύπτονται από τις δωρεές των χρηστών. Η γλώσσα που χρησιμοποιείται για την ανάπτυξη των πακέτων είναι μόνο η PHP. Επίσης τα στοιχεία που χαρακτηρίζουν το πακέτο phpseclib είναι:

- category Crypt
- package Crypt_RSA
- author Jim Wigginton <terrafrost@php.net>
- copyright MMIX Jim Wigginton
- license http://www.gnu.org/licenses/lgpl.txt
- version $Id: RSA.php,v 1.15 2010/04/10 15:57:02 terrafrost Exp $
- link http://phpseclib.sourceforge.net

Για περισσότερες πληροφορίες σχετικά με την κοινότητα και το πακέτο phpseclib υπάρχουν στις διευθύνσεις: http://pear.php.net/ και http://phpseclib.sourceforge.net/.

Όπως προαναφέρθηκε η phpseclib περιλαμβάνει ένα σύνολο συναρτήσεων για την υλοποίηση κρυπτογραφικών αλγορίθμων, οι οποίοι είναι: RSA, DES, 3DES, RC4, Rijndael, AES, SSH-1, SSH-2, και SFTP. Η εφαρμογή που παρουσιάζεται στην παρούσα εργασία χρησιμοποιεί το αρχείο RSA.php, BigInteger.php, Random.php, και Hash.php. Το πρώτο περιλαμβάνει όλες τις συναρτήσεις που αφορούν τον συγκεκριμένο αλγόριθμο ενώ το δεύτερο επιτρέπει τις πράξεις πολύ μεγάλων ακεραίων, οι οποίοι απαιτούνται για την δημιουργία των κλειδιών. Για να μπορεί να γίνει κλήση των συναρτήσεων μέσα από το κυρίως πρόγραμμα θα πρέπει να υπάρχουν οι παρακάτω γραμμές κώδικα, προκειμένου να καθοριστεί η διαδρομή:

```
<?php
        include ('Crypt/RSA.php');
?>
```

Και επίσης λόγω της αντικειμενοστραφούς δομής του πακέτου οι μέθοδοι καλούνται μέσω ενός αντικείμενου – στιγμιότυπου – της κλάσης Crypt_RSA(), δηλαδή:

```
<?php
        $rsa = new Crypt_RSA();
?>
```

Οι συναρτήσεις που χρησιμοποιήθηκαν είναι :

i. function createKey($bits = 1024, $timeout = false, $partial = array())
ii. function loadKey($key, $type = CRYPT_RSA_PRIVATE_FORMAT_PKCS1)
iii. function encrypt($plaintext)
iv. function decrypt($ciphertext)
v. function sign($message)
vi. function verify($message, $signature)

Αναλυτικά παρουσιάζονται παρακάτω:

function createKey($bits = 1024, $timeout = false, $partial = array())

Δημιουργεί το ζευγάρι του ιδιωτικού και δημόσιου κλειδιού. Η συνάρτηση είναι public και λαμβάνει τρεις προαιρετικούς παραμέτρους: Integer $bits, Integer $timeout, Math_BigInteger $p, των οποίων οι default τιμές φαίνονται στην δήλωση της

συνάρτησης, τέλος επιστρέφει έναν πίνακα με τα παρακάτω δύο στοιχεία: 'privatekey' – ιδιωτικό κλειδί και 'publickey' – δημόσιο κλειδί.

function loadKey($key, $type = CRYPT_RSA_PRIVATE_FORMAT_PKCS1)

Φορτώνει το ιδρωτικό ή το δημόσιο κλειδί και επιστρέφει «true» σε περίπτωση επιτυχούς φόρτωσης και «false» σε περίπτωση αποτυχίας. Η συνάρτηση είναι public και δέχεται δυο παραμέτρους την String $key και μια δεύτερη προαιρετική την Integer $type που αφορά τον τύπο του κλειδιού. Η προκαθορισμένη τιμή είναι «CRYPT_RSA_PRIVATE_FORMAT_PKCS1»

CRYPT_RSA_PRIVATE_FORMAT_PKCS1:

```
-----BEGIN RSA PRIVATE KEY-----
MIICWgIBAAKBgHx5XHa3LjiugtNq2xkd0oFf2SdsJ04hQYLoeRR3bqAei3Gc+PSy
AvynCIh/03JCvBsUHaCe8BwjwaTYrpq5QunGo/wvIzvx2d3G9dlrpOIFLiatZYOf
h07+CkSfaRXhBUKkul/gU87WPhKEcbnPDJS10uD1HqLsHfSKLNitGOf7AgElAoGA
ENIhQHmedlzFkjEI2eFveURNxw6dhxlANEjtxH7XmRjiaUyQWGsVKQ+nNQpa2Bbb
JkD9FbSc/OI8wz/gPmwP9eJN29CriebhaV3ebM1L1gbb5r7Vf/D/6rxB0BG/h2lA
jyZWEZrV/Gi9ZCaw/J+IUu1pAskKid84yHphvszywCUCQQDigrtr+cVkwkUsxOGd
B378yQCroXmybAD7FQHwVslafuFfTHkaMQSU/ZZLVY1ioMs1VVzzq/vOu0RstZOY
AfHFAkEAjK3mIWdG4JOM44/SrDkACNatsMtXKOi4K3SlXu9ie6ikXPD+GSZ+bWCX
GstFaXr9cHRvZPF3qYtK+j2N9UXOvwJBALeoRO/DmSFDkgifoixLRF5CHDgiD6Vs
U9J/vGIBLaNSHoSe3rtKVr3+CyhTNF3Oe0AABi1bA4UGioGn+yFNr0UCQBbQF3sJ
1CRq9ECT3PlVWfOYbzFtFQ2NhaYul1uAw9yzkEZsROF73SZ+XbFRZTOzFFds08su
E2eaDCiUXDWcnhECQQCRUQn2huHlssj8kt35NAVwiHCNfaeSQ5tiDcwfOywA4YXl
Q+kpuWq5U3V8j/9/n7pE/DL0nXEG/3QpKHJEYV5T
-----END RSA PRIVATE KEY-----
```

Σχήμα 5-5: Άποψη ιδιωτικού κλειδιού

CRYPT_RSA_PUBLIC_FORMAT_PKCS1:

```
-----BEGIN PUBLIC KEY-----
MIGGAoGAfHlcdrcuOK6C02rbGR3SgV/ZJ2wnTiFBguh5FHduoB6LcZz49LIC/KcIiH/TckK8GxQd
oJ7wHCPBpNiumrlC6caj/C8jO/HZ3cb12Wuk4gUuJq1lg5+HTv4KRJ9pFeEFQqS6X+BTztY+EoRx
uc8MlLXS4PUeouwd9Ios2K0Y5/sCASU=
-----END PUBLIC KEY-----
```

Σχήμα 5-6: Άποψη δημοσίου κλειδιού.

function encrypt($plaintext)

Κρυπτογραφεί το καθαρό κείμενο που δίνεται ως παράμετρο. Είναι public και δέχεται μόνο μια παράμετρο την String $plaintext, επιστρέφει μια συμβολοσειρά με το κρυπτογραφημένο κείμενο.

function decrypt($ciphertext)

Αποκρυπτογραφεί το κρυπτογραφημένο κείμενο που δέχεται ως παράμετρο. Είναι public και δέχεται μόνο μια παράμετρο την String $ciphetext, επιστρέφει μια συμβολοσειρά με το αποκρυπτογραφημένο κείμενο.

function sign($message)

Δημιουργεί την ψηφιακή υπογραφή για το μήνυμα που δίνεται ως παράμετρο. Είναι public και δέχεται μόνο μια παράμετρο την String $message, επιστρέφει μια συμβολοσειρά με την ψηφιακή υπογραφή. Η συνάρτηση κατακερματισμού που χρησιμοποιεί είναι η sha-1 .

function verify($message, $signature)

Εξακριβώνει το γνήσιο της υπογραφής για ένα μήνυμα. Είναι public και δέχεται δυο παραμέτρους την String $message και την String $signature και επιστρέφει true αν η εξακρίβωση είναι σωστή διαφορετικά «false».

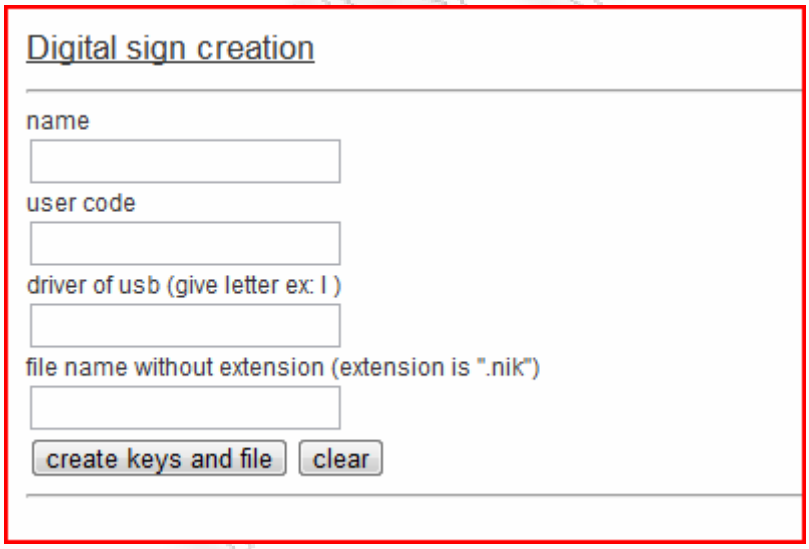
Υπάρχει ένα μεγάλο πλήθος συναρτήσεων που περιέχονται στο πακέτο και δεν αναφέρθηκαν, διότι δεν απατούνται στην υλοποίηση της εφαρμογής. Το εγχειρίδιο του πακέτου έχει πλήρη και αναλυτική τεκμηρίωση για όλες της συναρτήσεις, σε περίπτωση που ο αναγνώστης θέλει να ασχοληθεί περεταίρω.

5.3.2 Δημιουργία δημόσιου και ιδιωτικού κλειδιού

Η δημιουργία των κλειδιών (δημόσιου και ιδιωτικού) αποτελεί μια ξεχωριστή διαδικασία μείζονος σημασίας, που πραγματοποιείται από τον διαχειριστή του συστήματος. Η λειτουργιά αυτή παρέχεται μέσα από το μενού στης κεντρική σελίδας και εμφανίζεται – ενεργοποιείται μόνο στον διαχειριστή μετά την επιτυχή του είσοδο στο σύστημα.

Σχήμα 5-7: Επιλογή δημιουργίας κλειδιών από το κεντρικό μενού.

Με την επιλογής Create Keys από το κεντρικό μενού εμφανίζεται μια φόρμα όπου συμπληρώνονται τα στοιχεία που είναι απαραίτητα για την δημιουργία των κλειδιών, όλα τα πεδία είναι υποχρεωτικά και οι ενέργειες γίνονται από τον διαχειριστή μόνο έπειτα από αίτηση του χρήστη και παρουσία του αιτούμενου, προκειμένου να παραλάβει στο τέλος της διαδικασίας το usb memory stick με το ιδιωτικό του κλειδί.



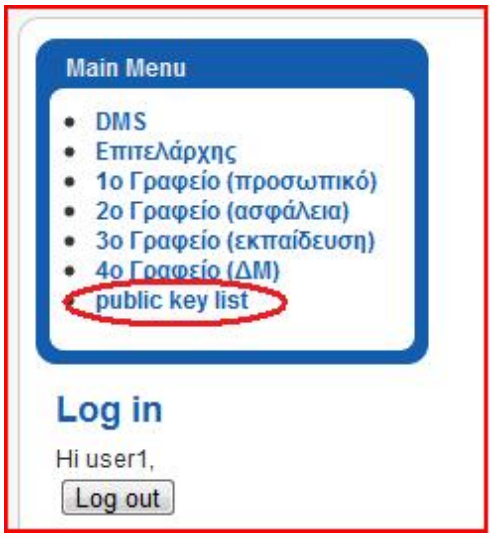
Σχήμα 5-8: Διεπαφή διαχειριστή για την δημιουργία κλειδιών.

Το αρχείο create_keys.html που υλοποιεί την διεπαφή που φαίνεται στο σχήμα 5.3 είναι:

```
<html>
	<head>
		<script language="javascript">

		function check1()
		{
		if (isNaN(form1.code.value))
			{
			alert("user code must be a number");
			return false;
			}
		}
		</script>
	</head>
	<body>
		<center><u><h2>Digital sign creation</h2></u></center> <hr/>

		<form name="form1" action="create_keys.php"  method="post" 
onSubmit="return check1();">
		<div valign="top">name</div><input type="text"  name="name" 
/><br/>
		<div valign="top">user code</div><input type="text"  name="code" 
/><br/>
		<div valign="top">driver of usb (give letter ex: I )</div><input 
type="text" name="driver"  /><br/>
		<div valign="top">file name without extension (extension is 
".nik")</div><input type="text" name="fname"  /><br/>
		<input type="submit" value="create keys and file" ><input type="reset" 
value="clear"><hr/>

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

Τα στοιχεία αποστέλλονται στο αρχείο create_keys.php του οποίου ο κώδικας φαίνεται παρακάτω:

```
<?php

include('Crypt/RSA.php');

$rsa = new Crypt_RSA();

extract($rsa->createKey());    // create keys
$hashprivatekey=sha1($privatekey);    //creates the hash value of the private key
$name=$_POST['name'];
$userid=$_POST['code'];

mysql_connect("localhost","dmslab","123456") ;
mysql_select_db("dmslab");
//stores in database the following values
mysql_query( "insert into jos_keys (userid,hash_private_key,username,public_key)
values ('$userid','$hashprivatekey','$name','$publickey')");

$myFile = $_POST['driver'].":".$_POST['fname'].".nik";
$fh = fopen($myFile, 'w') or die("can't open file");
fwrite($fh, $privatekey);
fclose($fh)
?>
<script language="javascript">

        function box()
        {
        alert("Hash value of private key and public key stored in database, also
        private key stored in given file succefully");
        window.location="http://localhost/dmslab/index.php?option=com_php&Itemid
=9";
        }
        box();
</script>
```



Σχήμα 5-9: Επιλογή εμφάνισης λίστας δημοσίων κλειδιών από το κεντρικό μενού.

Κατά την υποβολή της φόρμας γίνονται κάποιοι σχετικοί έλεγχοι, οπότε εάν κάποιο δεδομένο δεν πληρεί τις προϋποθέσεις του πεδίου εμφανίζεται το αντίστοιχο μήνυμα.

Σχήμα 5-10: Λίστα με τα δημόσια κλειδιά και τους κατόχους.

Όταν όλα είναι σύμφωνα τότε δημιουργούνται τα κλειδιά, το δημόσιο κλειδί αποθηκεύεται στην βάση δεδομένων και μπορεί να έχει πρόσβαση σε αυτό οποιοσδήποτε εξουσιοδοτημένος χρήστης του συστήματος, ενώ το ιδιωτικό κλειδί αποθηκεύεται σε αρχείο με όνομα αυτό που δόθηκε στο αντίστοιχο πεδίο της φόρμας και επέκταση «.nik» . Η αποθήκευση του αρχείου γίνεται στο προσωπικό usb memory stick.

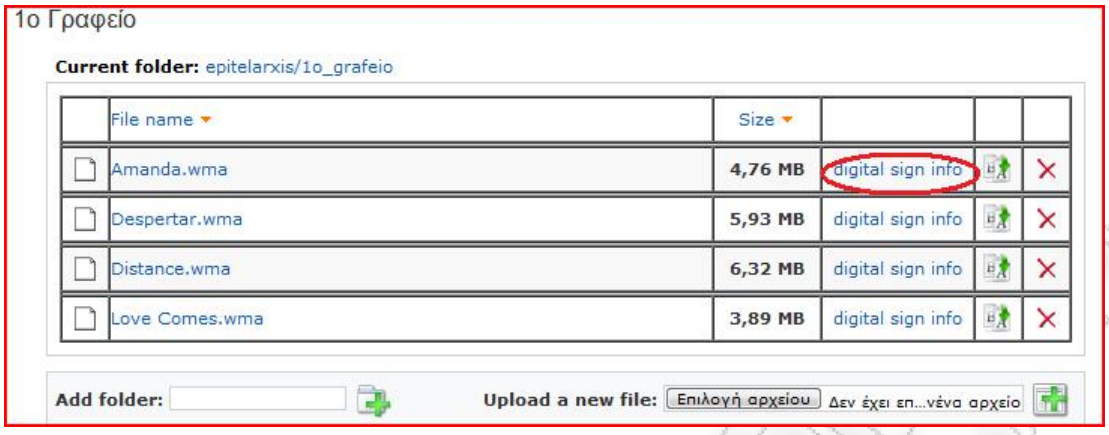
```
<?php
// no direct access
defined( '_JEXEC' ) or die( 'Restricted access' );

// retrieve user instance
$my =& JFactory::getUser();

mysql_connect("localhost","root","") ;
mysql_select_db("dmslab");
$result=mysql_query( "select * from jos_keys");

                while ( $row = mysql_fetch_array ( $result ))
                {
                    echo  $row [ 'username']."<br/>"."<br/>";
                    echo  $row [ 'public_key']."<br/><hr />";
                }
?>
```

5.3.3 Δημιουργία της ψηφιακής υπογραφής

Για την δημιουργία της ψηφιακής υπογραφής χρησιμοποιούνται οι παρακάτω γραμμές κώδικα:

```
 $hv=hash_file("sha1",$dir.DS.$a_file["name"]);   //hash value of the uploaded file
                $full_path= addslashes($dir.DS.$a_file["name"]);   //full path
                $fl=$a_file["name"];              //file name
                $today = getdate();
                $datetime=  $today[year]."-".$today[mon]."-".$today[mday]."
".$today[hours].":".$today[minutes];
```

```
//find the file with private key
                    if ($handle = opendir('I:'))
                     {
                              while (false !== ($file = readdir($handle)))
                              {
                               if (strstr( $file, ".nik" ))
                                 {
                                                  break;
                                   }
                              }
                              closedir($handle);
                     }

//read the private key from the correct file
                      $myFile="I:".$file;
                      $fh = fopen($myFile, 'r');
                      $privatekey = fread($fh, filesize($myFile));
                      fclose($fh);

//if the key belong to owner continue   sign the the file
                  if ($hash_private==sha1($privatekey))
                  {

                    $rsa = new Crypt_RSA();

                    $rsa->loadKey($privatekey);
                    $signature = utf8_encode($rsa->encrypt($hv));

                   $a= mysql_query ( "insert into jos_dig_sign (userid, username, hash,
sign, full_path,timestamp,filename)
                    values ('$userid','$username','$hv','$signature', '$full_path',
'$datetime','$fl')");
```



Σχήμα 5-11: Σύνδεσμος μεταδεδομένων ψηφιακής υπογραφής.

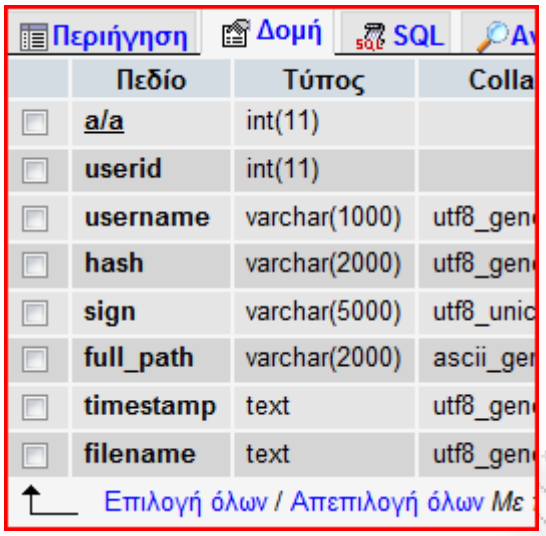
5.3.4 Αποθήκευση και παρουσίαση μεταδεδομένων ψηφιακής υπογραφής.

Η αποθήκευση και παρουσίαση των μεταδεδομένων που αφορούν την ψηφιακή υπογραφή ενός εγγράφου είναι από τα σημαντικότερα στοιχεία που παρέχει ένα σύστημα διαχείρισης εγγράφων. Αναλυτικά περιγράψαμε στο 3ο κεφάλαιο την χρησιμότητα των μεταδεδομένων, ιδιαιτέρως όμως θα πρέπει να τονίσουμε ότι στην ψηφιακή υπογραφή τα μεταδεδομένα - τα οποία για την συγκεκριμένη εφαρμογή που αναπτύξαμε είναι: ο αύξων αριθμός του υπογεγραμμένου εγγράφου (a/a), ο αναγνωριστικός κωδικός του συστήματος (userid), το διακριτικό όνομα του χρήστη (username), η τιμή της συνάρτησης κατακερματισμού του αρχείου εγγράφου (hash), η ψηφιακή υπογραφή (sign), η πλήρης διαδρομή της θέσης του εγγράφου (full_path), η χρονοσφραγίδα της υπογραφής (timestamp) και το όνομα του αρχείου (filename) - θα πρέπει να είναι σε θέση να διαβαστούν από τους έχοντας τα κατάλληλα δικαιώματα, περάν του δημιουργού του εγγράφου, ώστε να χρησιμοποιηθούν για εξακρίβωση της γνησιότητας της υπογραφής και κατ' επέκταση για θέματα ασφάλειας του συστήματος.

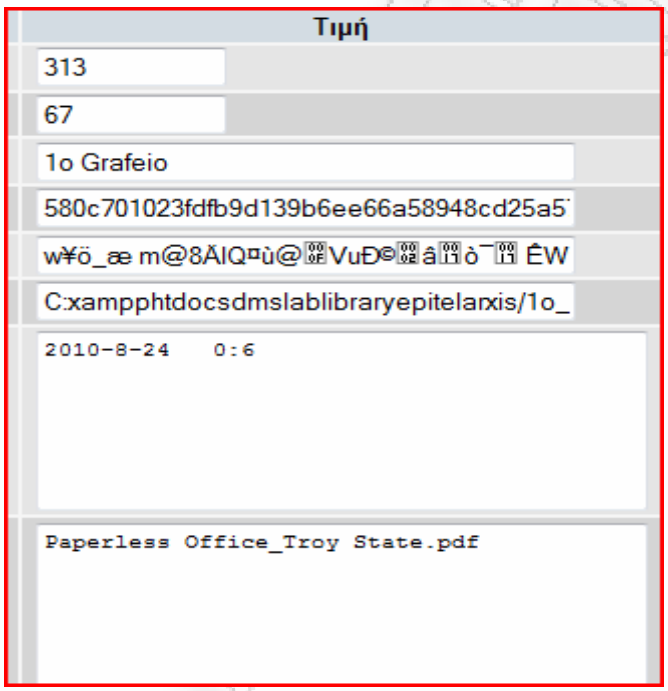
Στο παρακάτω σχήμα βλέπουμε τα πεδία του πίνακα «jos_dig_sign» που αποθηκεύονται τα στοιχεία που προαναφέρθηκαν και αμέσως μετά μια εγγραφή στον πίνακα. Σημειώνεται ότι με το ανέβασμα – αποθήκευση ενός εγγράφου στο σύστημα, το έγγραφο υπογράφεται αυτόματα και ταυτόχρονα αποθηκεύονται τα στοιχειά.

Όσον αφορά την διεπαφή του χρήστη, τα προηγούμενα σχήματα και στοιχεία προέρχονται από τον περιβάλλον του διαχειριστή του συστήματος, υπάρχει η δυνατότητα να εξακριβωθούν τα όσα αναφέραμε σχετικά με την γνησιότητα της ψηφιακής υπογραφής ενός εγγράφου. Έτσι λοιπόν στον φάκελο όπου ένας χρήστης έχει πρόσβαση υπάρχει ένα κελί όπως φαίνεται στο σχήμα 5.8 όπου λειτουργεί

σύνδεσμος με την επιγραφή «digital sign info» προς ένα νέο παράθυρο με όλα τα μεταδεδομένα της ψηφιακής υπογραφής του συγκεκριμένου εγγράφου.



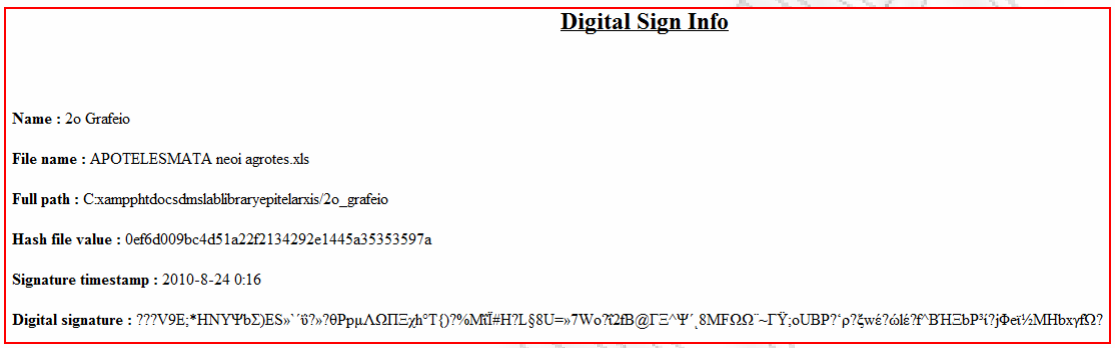
Σχήμα 5-12: Πεδία πίνακα αποθήκευσης μεταδιδομένων.



Σχήμα 5-13: Μια τυχαία εγγραφή στο πίνακα μεταδεδομένων.

5.4 Υλοποίηση των επιπέδων ασφαλείας του συστήματος

Αυτός ο τρόπος προσέγγισης της ασφάλειας παρουσιάζει πολλά πλεονεκτήματα όπως θεωρητικά αναφέρθηκαν στο κεφάλαιο 5. Όμως ιδιαίτερο ενδιαφέρον έχει η προγραμματιστική υλοποίηση, διότι εάν δεν γίνει με προσοχή ενδέχεται να υπάρξουν κενά, τα όποια θα δύνανται να εκμεταλλευτούν κακόβουλοι χρήστες. Παρακάτω θα δείξουμε τον τρόπο υλοποίησης του κάθε επιπέδου.



Digital Sign Info

Name : 2o Grafeio

File name : APOTELESMATA neoi agrotes.xls

Full path : C:xampphtdocsdmslablibraryepitelarxis/2o_grafeio

Hash file value : 0ef6d009bc4d51a22f2134292e1445a35353597a

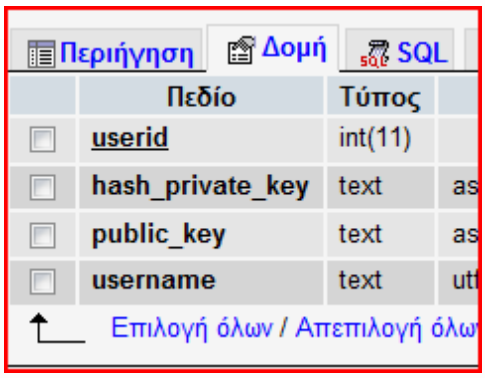
Signature timestamp : 2010-8-24 0:16

Digital signature : ???V9E;*HNYΨbΣ)ES»`´ö?»?θPpμΛΩΠΞχh°T{)?%MΪ#H?L§8U=»7Wo?t2fB@ΓΞ^Ψ´¸8MFΩΩ¨~ΓŸ;oUBP?'ρ?ξwé?ώlé?f^B'HΞbP³i?jΦeï½MHbxγfΩ??

Σχήμα 5.14: Άποψη εμφάνισης μεταδεδομένων εγγράφου.

Πρώτο επίπεδο ασφάλειας: ύπαρξη μοναδικού usb flash driver για κάθε χρήστη.

Η ύπαρξη μοναδικού usb flash driver για κάθε χρήστη που θα το παραλαμβάνει – χρεώνεται από τον διαχειριστή του συστήματος και θα περιέχει το ιδιωτικό κλειδί της προσωπικής του ψηφιακής υπογραφής. Αυτό το πρώτο επίπεδο εξασφαλίζει τόσο το σύστημα όσο και τον ίδιο τον χρήστη από κάποιον κακόβουλο διαχειριστή. Συγκεκριμένα γίνεται μια αντιστοίχηση «ένα προς ένα» μεταξύ χρήστη και ζεύγους κλειδιών και επίσης αποθηκεύεται στην βάση δεδομένων του συστήματος η τιμή της συνάρτησης κατακερματισμού για το ιδιωτικό κλειδί, οπότε πραγματικά ο μόνος που το γνωρίζει είναι ο χρήστης. Οποιοσδήποτε άλλος που θα μπορούσε να δει την βάση δεδομένων του συστήματος το μονό που θα έβλεπε θα ήταν η τιμή της συνάρτησης κατακερματισμού, από την όποια δεν μπορεί να εξαχθεί το αρχικό κείμενο. Στα σχήματα 5.1 και 5.2 βλέπουμε τα πεδία του πίνακα «jos_keys» και της βάσης δεδομένων «dmslab» του συστήματος. Ο κώδικας που τα δημιουργεί έχει παρουσιαστεί στην ενότητα 5.3.1 .

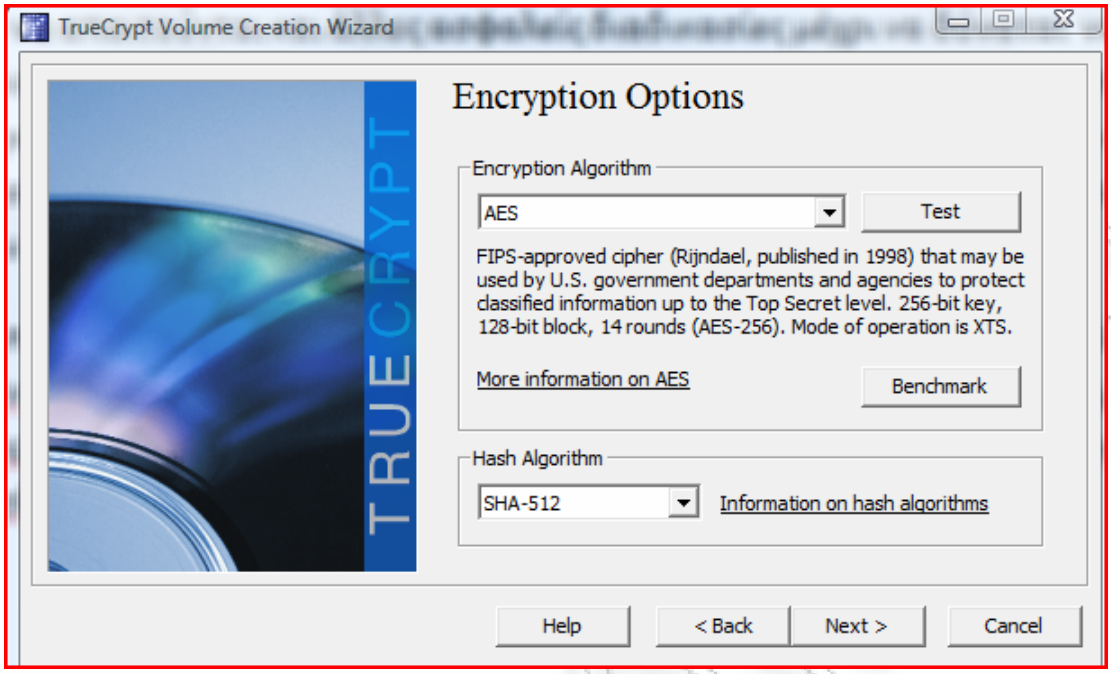


Σχήμα 5-15: Πεδία πίνακα αποθήκευσης στοιχείων κλειδιών.

Σχήμα 5-16: Εγγραφές στον πίνακα στοιχείων κλειδιών χρήστη.

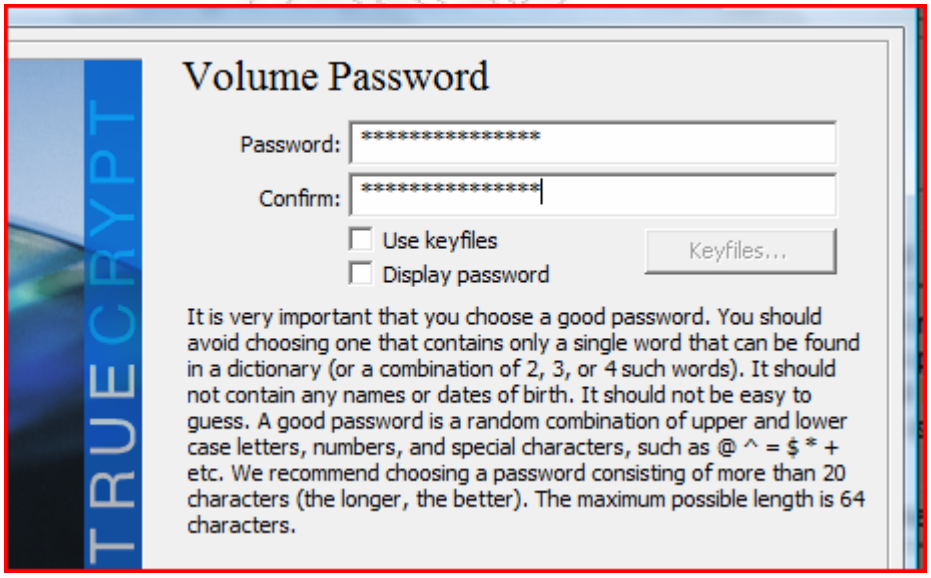
Δεύτερο επίπεδο ασφάλειας: Κρυπτογράφηση του usb flash driver που περιέχει το ιδιωτικό κλειδί

Αυτό το επίπεδο ασφάλειας υλοποιήθηκε με σκοπό να προστατεύσει το ιδιωτικό κλειδί από κακόβουλη κλοπή ή τυχαία απώλεια από λάθος του χρήστη. Βέβαια το σύστημα είναι δομημένο με τέτοιο τρόπο που ακόμη και αν το ιδιωτικό κλειδί βρεθεί στα χέρια τρίτου προσώπου να απαιτούνται και άλλες ασφαλείς διαδικασίες μέχρι να δύναται να χρησιμοποιηθεί. Τελικά με την λύση αυτή, δηλαδή την κρυπτογράφηση της συσκευής που έχει αποθηκευμένο το ιδιωτικό κλειδί, αποτρέπεται να διαρρεύσει το ιδιωτικό κλειδί τόσο σε άτομα με κακούς σκοπούς όσο και σε περιέργους που θα έχει βρεθεί στα χέρια τους και θα θελήσουν να δουν ή να κρατήσουν το περιεχόμενο.



Σχήμα 5-17: Επιλογή αλγορίθμου κρυπτογράφησης και συνάρτησης κατακερματισμού στην κρυπτογράφηση του μέσου αποθήκευσης ιδιωτικού κλειδιού.

Τώρα για την κρυπτογράφηση της συσκευής χρησιμοποιήθηκε το ελεύθερο λογισμικό TrueCrypt [24] το οποίο δίνει την δυνατότητα να κρυπτογραφηθεί ολόκληρος δίσκος ή και τμήμα του με γνωστούς κρυπτογραφικούς αλγόριθμους αποδεδειγμένης ασφάλειας. Συγκεκριμένα χρησιμοποιήθηκε ο AES και η συνάρτηση κατακερματισμού SHA-512



Σχήμα 5-18: Εισαγωγή κωδικού στην κρυπτογράφηση του μέσου.

Επίσης κατά την διαδικασία κρυπτογράφησης της συσκευής εισάγεται και προσωπικός κωδικός με δυνατότητα μέχρι 64 χαρακτήρες. Τελικά για να γίνει χρήση της συσκευής που έχει αποθηκευμένο το ιδιωτικό κλειδί, θα πρέπει μετά από την τοποθέτηση της συσκευής να πληκτρολογηθεί ο προσωπικός κωδικός. Τότε μόνο είναι δυνατή η ανάγνωση του περιεχομένου και επομένως και η χρήση του ιδιωτικού κλειδιού.

Τρίτο επίπεδο ασφάλειας: Μοναδικά στοιχεία για την είσοδο του χρήστη στο σύστημα (username-password).

Ο χρήστης πριν από οποιαδήποτε διαδικασία θα πρέπει να δημιουργήσει και τον προσωπικό του λογαριασμό, δηλαδή καταχωρεί τα προσωπικά του στοιχεία και μαζί με αυτά επιλέγει και ένα username-password. Τα στοιχεία αυτά καταχωρούνται στο σύστημα εκτός από το password για το οποίο αποθηκεύεται η τιμή της συνάρτησης κατακερματισμού. Η διαδικασία δημιουργίας λογαριασμού είναι ίδια με εκείνη που γίνεται στο διαδίκτυο για την απόκτηση λογαριασμού ηλεκτρονικού ταχυδρομείου, μέλος ενός γκρουπ κ.α. Δεν θα γίνει περεταίρω αναφορά στο επίπεδο αυτό διότι η συγκεκριμένη διαδικασία είναι κοινώς γνωστή και επίσης χρησιμοποιήθηκε αυτούσια όπως ακριβώς υποστηρίζεται από το ελεύθερο λογισμικό joomla.

Τέταρτο επίπεδο ασφάλειας: Για την είσοδο στο σύστημα απαιτείται η τοποθέτηση του προσωπικού usb memory stick.

Όταν ανοίγει η κεντρική σελίδα του συστήματος εμφανίζεται μήνυμα που προειδοποιεί τον χρήστη να τοποθετήσει το προσωπικό usb memory stick στον υπολογιστή. Μετά από αυτή την προτροπή το σύστημα ελέγχει για την ύπαρξη κατάλληλου εξωτερικού δίσκου που να περιέχει αρχείο με κατάληξη «.nik», δηλαδή με ιδιωτικό κλειδί. Έπειτα από αυτήν ενέργεια διαβάζει το αρχείο και εξάγει την τιμή κατακερματισμού την οποία συγκρίνει με εκείνη που είναι αποθηκευμένη για τον συγκεκριμένο χρήστη στη βάση δεδομένων. Εάν όλα είναι εντάξει τότε επιτρέπει την είσοδο στο σύστημα διαφορετικά εμφανίζεται ευδιάκριτο μήνυμα (σχήμα 5-19), ώστε να μπορεί να εντοπιστεί εύκολα και από άλλους συναδέλφους ότι κάτι δεν λειτούργει

σωστά σε εκείνο το σταθμό εργασίας. (Αναφέρθηκε στο κεφάλαιο 4 ότι η ασφάλεια είναι ευθύνη και του προσωπικού).

Σχήμα 5-19: Μήνυμα παράνομης ή λανθασμένης χρήσης ιδιωτικού κλειδιού.

Πέμπτο επίπεδο ασφάλειας: Δενδροειδής διάταξη φακέλων με δυνατότητα εφαρμογής δικαιωμάτων.

Το σύστημα που αναπτύξαμε προορίζεται για να καλύψει ανάγκες σε ένα περιβάλλον με στρατιωτική δομή, συγκεκριμένα σε ένα επιτελείο μονάδος. Οπότε η διάταξη που δημιουργήσαμε στους φακέλους και τα δικαιώματα που δόθηκαν έχουν σχέση με την δομή ενός επιτελείου, δηλαδή υπάρχουν τα τέσσερα γραφεία που ασχολούνται με τα θέματα: προσωπικού, ασφάλειας, εκπαίδευσης και διοικητικής μεριμνάς με τους αριθμούς $1^{ο}$, $2^{ο}$, $3^{ο}$, $4^{ο}$ αντίστοιχα για λόγους κωδικοποίησης και ευκολίας χρήσης. Ο υπεύθυνος του κάθε γραφείου έχει πλήρη δικαιώματα στον φάκελο εργασίας του. Επίσης υπάρχει και ο προϊστάμενος των υπεύθυνων γραφείων, ο οποίος έχει πρόσβαση σε όλους τους φακέλους των γραφείων, όμως με περιορισμένα δικαιώματα.

Έτσι λοιπόν στηριζόμενοι σε μια τυπική δομή επιτελείου δημιουργήσαμε μια δενδροειδής διάταξη φακέλων, όπου ο κάθε χρήστης έχει συγκεκριμένα δικαιώματα στον φάκελο του (πλήρη), ενώ στους φακέλους που μπορεί να εισέλθει λόγο

δενδροειδούς διάταξης τα δικαιώματα του διαφοροποιούνται (περιορισμένη πρόσβαση).

ΚΕΦΑΛΑΙΟ 6ο

ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΜΕΛΛΟΝΤΙΚΗ ΜΕΛΕΤΗ

Στο κεφάλαιο αυτό θα παρουσιάσουμε τα συμπεράσματα τα οποία πρόεκυψαν από την ανάπτυξη του «Ολοκληρωμένου συστήματος διαχείρισης έγγραφων πολυεπίπεδης ασφάλειας με ενσωματωμένη ψηφιακή υπογραφή» και τα οποία αποτελούν τα σημαντικότερα σημεία της συνεισφορά της παρούσας εργασίας στον τομέα αυτού του είδους των πληροφοριακών συστημάτων, ενός είδους συστημάτων που δύνανται να αντιμετωπίσουν το πρόβλημα της συσσώρευσης εγγράφων και της γραφειοκρατίας, που σκιάζει την εσωτερική λειτουργία των οργανισμών και των επιχειρήσεων.

6.1 Συνεισφορά της εργασίας

Ο στόχος της εργασίας ήταν να παρουσιάσουμε ένα ολοκληρωμένο σύστημα, το οποίο να συνδυάζει πολλές λειτουργιές σε ένα ενοποιημένο περιβάλλον, το οποίο αποτελεί την έξοδο από το τέλμα της σημερινής γραφειοκρατικής πραγματικότητας. Οι παραδοσιακές δομές λειτουργίας με την χειροκίνητη δημιουργία, αποθήκευση και αναζήτηση των εγγράφων, δεσπόζουν στο χώρο των οργανισμών και των επιχειρήσεων και «κουβαλούν» μαζί τους όλες εκείνες τις αδυναμίες ενός μη αποτελεσματικού πλέον συστήματος.

Η λύση που προτείναμε ήταν τα συστήματα διαχείρισης εγγράφων, τα οποία παρουσιάσαμε αναλυτικά στο κεφάλαιο 3 και συγκεκριμένα μιλήσαμε για την δομή τους, τις λειτουργίες τους και τα οφέλη τους, τα οποία μπορούν να βελτιωθούν ακόμη περισσότερο μέσω μιας ακόμη λειτουργιάς εκείνης της ψηφιακής υπογραφής. Έτσι λοιπόν ενσωματώσαμε την δυνατότητα αυτή και μάλιστα τη συνδυάσαμε με το θέμα της ασφάλειας. Η ψηφιακή υπογραφή λοιπόν προστέθηκε με τρόπο που να προσδίδει διττή σημασία στο εν λόγω πληροφοριακό σύστημα.

Οπότε από την μια πλευρά η ψηφιακή υπογραφή επαύξησε την λειτουργικότητα και την αποτελεσματικότητα της εφαρμογής με το να καλύψει κενά που σχετίζονταν με την ακεραιότητα, την αυθεντικότητα, την εμπιστευτικότητα και την μη αποποίηση της ευθύνης των δημιουργημένων ή ληφθέντων ψηφιακών εγγράφων και μηνυμάτων που διακινούνται εντός ή εκτός ενός οργανισμού. Ενώ παράλληλα η ψηφιακή υπογραφή χρησιμοποιήθηκε ως ένα ακόμη επίπεδο ασφάλειας μιας και η ίδια η οντότητα της σχετίζεται με την κρυπτογραφία, δηλαδή το μέγεθος των κλειδιών που χρησιμοποιεί προκειμένου να υπάρξει ασφάλεια στην αποκάλυψη του κρυπτογραφημένου μηνύματος, λειτουργεί και ως μέσο θωράκισης της εισόδου στο ίδιο το σύστημα. Αναλυτικά παρουσιάστηκε η προαναφερθείσα προσέγγιση στο κεφάλαιο 2 και στην ενότητα 5.3 .

Επίσης παρουσιάσαμε ένα διαφορετικό, πιο αποτελεσματικό τρόπο προσέγγισης στο θέμα της ασφάλειας των συστημάτων αυτής της μορφής. Το πολυεπίπεδο σύστημα ασφάλειας φαίνεται να μπορεί να αντιμετωπίσει αποτελεσματικότερα τις νέες προκλήσεις και απειλές της σύγχρονης κοινωνίας της πληροφορίας και να θωρακίσει ένα σύστημα κατά τρόπο διαδοχικά ισχυρό. Ουσιαστικά χτίζεται μια άμυνα που έχει βάθος, με σκοπό να κάμπτει την ισχύ του επιτιθέμενου έως ότου την εξουδετερώσει ολοκληρωτικά.

6.2 Μελλοντική εργασία

Με έναυσμα την παρούσα εργασία προκύπτουν διάφορες κατευθύνσεις προς μελλοντική ερεύνα. Αυτές θα μπορούσαν να είναι η προσθήκη νέων λειτουργιών στα συστήματα διαχείρισης εγγράφων καθώς και η βελτίωση των υπαρχόντων ώστε να μπορούν να συνεργαστούν με εφαρμογές που χρησιμοποιούνται ήδη π.χ. η ενσωμάτωση ενός σχεδιαστικού προγράμματος στο σύστημα διαχείρισης εγγράφων.

Επίσης στον τομέα της ασφάλειας, ένα πεδίο που έχει ιδιαίτερο ενδιαφέρον για μελλοντική έρευνα είναι η επαύξηση της ανθεκτικότητας της ψηφιακής υπογραφής όχι μονό με την αύξηση του μεγέθους του κλειδιού, το οποίο επηρεάζει σημαντικά την αύξηση του χρόνου κρυπτογράφησης του μηνύματος αλλά με βελτίωση του αλγόριθμου ή ακόμη και επινόηση ενός άλλου.

Ακόμη η υιοθέτηση της μεθόδου θωράκισης της ασφάλειας μέσω της δημιουργίας πολλών επιπέδων ασφάλειας και η επινόηση νέων επιπέδων χωρίς να γίνεται πολύπλοκη η είσοδος του χρήστη στο σύστημα, δηλαδή μια ισορροπημένη

προσέγγιση τόσο σε θεωρητικό όσο κα σε προγραμματιστικό επίπεδο, είναι ένα ακόμη πεδίο μελλοντικής μελέτης και έρευνας.

Κλείνοντας πιστεύουμε ότι η παρούσα θέση, η οποία εκπονήθηκε με περίσσιο μεράκι και όσο το δυνατό μεγαλύτερη επιστημονική ακρίβεια, να αποτελέσει πηγή έμπνευσης για τους νέους μελετητές της επιστήμης της πληροφορικής. Η ρήση ενός αρχαίου Έλληνα σοφού θα μας θυμίζει τον αέναο αγώνα για την κατάκτηση της γνώσης.

«Δῶς μοί πᾶ στῶ καί τάν γᾶν κινάσω» Αρχιμήδης

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. «The first ten years of public-key cryptography. Proceedings of the IEEE», W. Diffie, pp: 560-577, 1988.

2. «A method for obtaining digital signatures and public-key cryptosystems», R.L. Rivest, A. Shamir and L.M. Adleman, *Communications of the ACM,* 21(2): 120-126, February 1978.

3. www.en.wikipedia.org/wiki/Cryptographic_hash_function

4. «The magic words are squeamish ossifrage», D. Atkins, M. Graff, A.K. Lenstra, P.C. Leylana, In *Proc. Advances in Cryptology Asiacrypt '94,* pp. 263-277, 1995.

5. www.mathworld.wolfram.com/QuadraticSieve.html

6. «A New Kind of Cipher That Would Take Millions of Years to Break», M. Gardner, *Scientific American,* August 1977.

7. «Σύγχρονη Κρυπτογραφία» Π. Ναστού – Π. Σπυράκης – Γ. Σταματίου, ΕΛΛΗΝΙΚΑ ΓΡΑΜΜΑΤΑ – 2003.

8. «The Paperless Office: Accepting Digitized data», Miles L. Mathieu, Ernest A. Capozzoli, Troy State University (2002).

9. www.en.wikipedia.org/wiki/Document_management_system

10. www.quality.co.uk/custpage.htm

11. «Πρακτικά θέματα Ασφαλείας Πληροφοριακών Συστημάτων και Εφαρμογών», Νινέτα Πολέμη - Αλέξανδρος Καλιαντζόγλου, Αθήνα 2008.

12. www.hri.org/info/articles

13. www.slashdot.org/faq

14. «Ασφάλεια Δικτύων Υπολογιστών», Στ. Γκριτζάλη, Σ. Κατσίκα, Δ. Γκριτζάλη, Παπασωτηρίου 2003, Αθήνα.

15. «Crisis Management Workbook», Office of Security and Risk Management Services (October 2007), Fairfax County Public Schools.

16. «Code Red in the Boardroom: Crisis Management as Organizational DNA», Coombs, W. T. (2006), . Westport, CT Praeger.

17. «Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων με χρήση υπηρεσιών Έμπιστης Τρίτης Οντότητας» Διδακτορική διατριβή - Δημήτρη Π. Λέκκα 2002

18. «Using html» , Savola Tom, Westenbroek Alan, Heck, Joseph, 1967- . Que, 1995.

19. «Εισαγωγή στην PHP : για windows με εικόνες», Ullman, Larry E. (Larry Edward), Καρτσακλής Δημήτρης, Κλειδάριθμος, 2005.

20. «Javascript : the definitive guide», Flanagan, David O'Reilly, 2002.

21. «The SQL standard : a complete reference», Lans, Rick F., van Prentice Hall, 1989

22. «Profetional xml» υπο Anderson, Richard Wrox Press , 2000

23. «jsmallfib manual», www.jsmallsoftware.com

24. «TrueCrypt user guide», www.truecrypt.org