ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ ΚΑΙ ΟΡΓΑΝΙΣΜΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

"Ασφάλεια ηλεκτρονικών συναλλαγών με έμφαση στα ιατρικά δεδομένα"

Φοιτητής: Τσώνης Βασίλειος

Επιβλέπων Καθηγητής
Κοτσιλιέρης Θεόδωρος

Καλαμάτα 2015

Αφιέρωση

Στη σύζυγο μου Βάλια

Ευχαριστίες

Θα ήθελα να εκφράσω τις ευχαριστίες μου στον επιβλέποντα καθηγητή μου κ. Κοτσιλιέρη Θεόδωρο, για την καθοδήγηση και την αμέριστη βοήθεια που μου έδωσε σε κάθε φάση της εκπόνησης αυτής της πτυχιακής εργασίας, για την υπομονή που επέδειξε σε όλη τη διάρκεια της συνεργασίας μας αλλά κυρίως για τον τρόπο αντιμετώπισης, σεβασμό και εμπιστοσύνης που επέδειξε απέναντι στο άτομό μου.

Επίσης θα ήθελα να ευχαριστήσω πολύ τους γονείς μου για την υποστήριξη τους καθόλη τη διάρκεια των σπουδών μου.

Ένα μεγάλο ευχαριστώ στη σύζυγο μου για τη συμπαράστασή της και την υπομονή της σε όλη τη διάρκεια της εκπόνησης της εργασίας μου.

Τέλος θα ήθελα να ευχαριστήσω τον ξαδελφό μου Α. Δεληγάκη για τις συμβουλές του.

Περίληψη

Ο τομέας της υγειονομικής περίθαλψης αποτελεί πρόκληση και ταυτόχρονα έχει γίνει ένα δύσκολο πεδίο εξέτασης για την ασφάλεια των πληροφοριών, λόγω της πολύπλοκης φύσης των δεδομένων της υγειονομικής περίθαλψης και της ιδιωτικής ζωής. Από τότε που τα συστήματα υγειονομικής περίθαλψης έχουν εφαρμοστεί, η ασφάλεια τους εξετάζεται ως ένα σημαντικό θέμα, ιδίως υπό το πρίσμα του γεγονότος ότι τα δεδομένα τους θεωρείται ότι περιλαμβάνουν εξαιρετικά ευαίσθητες πληροφορίες. Η προοπτική της αποθήκευσης πληροφοριών υγείας σε ηλεκτρονική μορφή εγείρει ανησυχίες για την προστασία της ιδιωτικής ζωής και την ασφάλεια των δεδομένων. Οποιαδήποτε προσπάθεια να δημιουργηθούν ηλεκτρονικά πληροφοριακά συστήματα υγειονομικής περίθαλψης,ως εκ τούτου, πρέπει να διασφαλίζεται από επαρκή προστασία της εμπιστευτικότητας και της ακεραιότητας των πληροφοριών του ασθενούς. Ταυτόχρονα, οι πληροφορίες του ασθενή πρέπει να είναι άμεσα διαθέσιμες σε όλους τους εξουσιοδοτημένους παρόχους υπηρεσιών υγειονομικής περίθαλψης, προκειμένου να εξασφαλίσουν τη σωστή θεραπεία-νοσηλεία του.

Ο κύριος σκοπός της παρούσας εργασίας ωστόσο, δεν είναι να αποτελέσει μια νέα συνεισφορά στο θέμα της ασφάλειας, αλλά να δώσει μια γενική εικόνα των σημερινών τάσεων στις πτυχές της ασφάλειας των ιατρικών δεδομένων και κατ' επέκταση των πληροφοριακών συστημάτων υγειονομικής περίθαλψης.

Abstract

The domain of healthcare has become a challenging testing ground for information security due to the complex nature of healthcare information and patient's privacy. Ever since healthcare information systems have been implemented, their security is being considered an important issue, especially in the light of the fact that their data are deemed to comprise extremely sensitive information. The prospect of storing health information in digital form raises concerns about patient privacy and data security. Any attempt to introduce health-care information systems should, therefore, guarantee adequate protection of the confidentiality and integrity of patient information. At the same time, the patient information also needs to be readily available to all authorised health-care providers, in order to ensure the proper treatment of the patient.

However the principal aim of this thesis is, not to make a new contribution to the subject of security, but rather to offer an overview of current trends in the security aspects of sensitive medical data and therefore the health-care information systems.

Πίνακας περιεχομένων

ΚΕΦΑΛΑΙΟ 1

Ηλεκτρονικό Επιχειρείν (E-Business)

Ηλεκτρονικό Επιχειρείν

Ηλεκτρονικό Επιχειρείν (e-business) ονομάζεται το σύνολο από επιχειρηματικές στρατηγικές που σκοπό έχουν να υποστηρίξουν και να μετασχηματίσουν συγκεκριμένους τομείς επιχειρηματικής δραστηριότητας, με τη χρήση νέων τεχνολογιών και τη διεκπεραίωση συναλλαγών με ηλεκτρονικά μέσα. Είναι αναγκαίο να διαχωρίσουμε τους όρους "ηλεκτρονικό επιχειρείν" και "ηλεκτρονικό εμπόριο". Αυτοί οι δύο όροι αρκετά συχνά προκαλούν σύγχυση, λόγω της δημοσιότητας και της αύξησης της χρήσης του ηλεκτρονικού εμπορίου σε σχέση με άλλους τομείς οι οποίοι αποτελούν το ηλεκτρονικό επιχειρείν. Ο όρος "ηλεκτρονικό επιχειρείν" συμπεριλαμβάνει όλες τις οικονομικές λειτουργίες και δράσεις που υποστηρίζονται με τη χρήση ηλεκτρονικών μέσων. Αντιθέτως, ο όρος "ηλεκτρονικό εμπόριο" αποτελεί μέρος του παραπάνω συνόλου, πρόκειται για μία εφαρμογή η οποία απευθύνεται σε πιο ευρύ αγοραστικό κοινό με σκοπό να συμβάλει στην επικοινωνία αγοραστών και επιχειρήσεων (Chondrocoukis,2004).

Μικρό Ιστορικό ΗΕ

Στις αρχές της δεκαετίας του 1970, ο όρος ηλεκτρονικό εμπόριο αναφερόταν στην ηλεκτρονική ανταλλαγή δεδομένων για την αποστολή επιχειρηματικών εγγράφων, όπως π.χ. εντολές αγοράς κ.λπ. Αργότερα με την βιομηχανική ανάπτυξη ο όρος ηλεκτρονικό εμπόριο χρησιμοποιούνταν για την συναλλαγή αγαθών και υπηρεσιών μέσω του διαδικτύου. Το πρώτο Παγκόσμιο Δίκτυο εισήχθη το 1994 και σύντομα έγινε αναπόσπαστο κομμάτι της παγκόσμιας οικονομίας. Χρειάστηκαν να περάσουν τέσσερα έτη ώσπου τα πρωτόκολλα http να μπορούν να είναι ευρέως διαθέσιμα στους χρήστες. Το πρώτο ηλεκτρονικό εμπόριο δημιουργήθηκε στις Ηνωμένες Πολιτείες Αμερικής και σε ορισμένες Ευρωπαϊκές χώρες το 1998. Το ηλεκτρονικό εμπόριο διαδόθηκε πολύ γρήγορα στις περισσότερες πόλεις των Η.Π.Α., στην Ευρώπη και την ανατολική Ασία το 2005. Αναφέρεται ότι το ηλεκτρονικό εμπόριο προϋπήρχε του διαδικτύου, αλλά εξαιτίας του κόστους αυτού του είδους επιχειρηματικότητας, μόνο επιχειρήσεις, χρηματοπιστωτικά ιδρύματα και εταιρείες μπορούσαν να το χρησιμοποιήσουν. Όμως με

την ευρεία χρήση του διαδικτύου από όλους τους ανθρώπους και την αλλαγή της δομής του ηλεκτρονικού εμπορίου, αυτού του είδους η επιχειρηματικότητα άλλαξε εντελώς τη μέχρι τότε μορφή(Nanehkaran,2013). Με την εμπορευματοποίηση του Internet στις αρχές της δεκαετίας του 90 και την ταχεία εξέλιξη σε πολλούς δυνητικούς πελάτες, δημιουργήθηκε ο όρος Ηλεκτρονικό Επιχειρείν και οι εφαρμογές του αυξήθηκαν γρήγορα.

Μοντέλα Ηλεκτρονικού Επιχειρείν

Επιχειρηματικό μοντέλο ονομάζεται η επιχειρηματική μέθοδος με την οποία διατηρείται η εταιρία και κατά κύριο λόγο βγάζει κέρδη. Το ηλεκτρονικό επιχειρηματικό μοντέλο αποτελεί το πιο σύγχρονο μοντέλο του ηλεκτρονικού επιχειρείν. Τα κύρια μοντέλα ηλεκτρονικού επιχειρείν είναι:

- **Brokerage model (χρηματομεσιτικό μοντέλο)**: Στον τύπο του μοντέλου αυτού, προκειμένου να διευκολυνθούν οι συναλλαγές, η επικοινωνία των αγοραστών και των καταναλωτών γίνεται από τους χρηματομεσίτες. Συχνά διαδραματίζουν σημαντικό ρόλο στις αγορές επιχείρησης προς επιχείρηση (business to business), επιχείρησης προς πελάτη (business to customer) και πελάτη προς πελάτη (customer to customer). Οι υπηρεσίες που παρέχονται από τον χρηματομεσίτη χρεώνονται από ένα ποσό.
  - **Advertising model (διαφημιστικό μοντέλο)**: Το διαφημιστικό μοντέλο του Internet αποτελεί προέκταση του παραδοσιακού διαφημιστικού μοντέλου εκπομπής μέσου. Το περιεχόμενο και οι υπηρεσίες που προβάλλονται στο μοντέλο αυτό συνδυάζονται με διαφημιστικά μηνύματα, δεδομένου του ότι η διαφήμιση αποτελεί έναν από τους κυριότερους παράγοντες που αποφέρουν εισοδήματα στις επιχειρήσεις.
  - **Infomediary model (πληροφοριακό μοντέλο)**: Τα δεδομένα που αφορούν τους πελάτες καθώς και τις καταναλωτικές τους συνήθειες είναι απαραίτητα για την επιχείρηση. Το πληροφοριακό μοντέλο αναγνωρίζει ότι υπάρχει αξία σε αυτά τα προσωπικά δεδομένα και επιδιώκει να δράσει ως ένα αξιόπιστο μέσο, που παρέχει τη δυνατότητα και τα μέσα στους

πελάτες να κερδίσουν και να επωφεληθούν από το δικό τους προφίλ των πληροφοριών(Sarkar,2002).

- **Merchant model (εμπορικό μοντέλο)**: Ο τύπος του μοντέλου αυτού αναφέρεται στην παροχή προϊόντων και υπηρεσιών από πωλητές χονδρικής και λιανικής. Οι πωλήσεις μπορεί να γίνονται με βάση τις τιμές καταλόγου ή μέσω δημοπρασιών.
- **Manufacturer model (κατασκευαστικό μοντέλο)**: Το κατασκευαστικό μοντέλο (ή αλλιώς και άμεσο μοντέλο) στηρίζεται στη δύναμη του διαδικτύου και δίνει τη δυνατότητα στον κατασκευαστή να έχει άμεση επικοινωνία με τον πελάτη και με τον τρόπο αυτό να συμπιέσει το κανάλι διανομής. Το κατασκευαστικό μοντέλο μπορεί να βασίζεται στην αποδοτικότητα, τη βελτίωση της εξυπηρέτησης των πελατών καθώς και στην καλύτερη κατανόηση των προτιμήσεων των πελατών(Rappa,2010).
- **Affiliate model (εταιρικό μοντέλο)**: Το εταιρικό μοντέλο παρέχει την δυνατότητα στον πελάτη να πραγματοποιήσει αγοραστικές ευκαιρίες οποιαδήποτε στιγμή συνδεθεί στο διαδίκτυο. Αυτό επιτυγχάνεται με την παροχή οικονομικών κινήτρων ώστε να συνδεθεί με θυγατρικές ιστοσελίδες. Το μοντέλο των θυγατρικών είναι εγγενώς προσαρμοσμένο στο διαδίκτυο, γεγονός που εξηγεί και τη δημοτικότητά του(Rappa,2010).
- **Community model (κοινοτικό μοντέλο)**: Η βιωσιμότητα του κοινοτικού μοντέλου βασίζεται στην πίστη του χρήστη. Οι χρήστες επενδύουν αρκετά σε χρόνο και συναίσθημα. Τα έσοδα μπορεί να βασίζονται στις πωλήσεις βοηθητικών προϊόντων και υπηρεσιών ή σε εθελοντικές συνεισφορές. Επίσης τα έσοδα ενδέχεται να συνδέονται με συμφραζόμενη διαφήμιση και συνδρομές για πριμοδοτούμενες υπηρεσίες. Σήμερα το διαδίκτυο αποτελεί μια από τις πιο εύφορες περιοχές ανάπτυξης, όπως διαφαίνεται από την αύξηση της κοινωνικής δικτύωσης(Rappa,2010).
- **Subscription model (συνδρομητικό μοντέλο)**: Οι χρήστες επιβαρύνονται με περιοδική (ημερήσια, μηνιαία, ετήσια) συνδρομή, προκειμένου να εγγραφούν σε μια υπηρεσία. Δεν είναι ασυνήθιστο για τους δικτυακούς τόπους να συνδυάσουν δωρεάν περιεχόμενο με υψηλής ποιότητας

περιεχόμενο. Τα συνδρομητικά τέλη πραγματοποιούνται ανεξάρτητα από τα πραγματικά ποσοστά χρήσης των υπηρεσιών. Επίσης ο συνδυασμός συνδρομής και διαφημιστικών μοντέλων είναι συχνός(Rappa,2010).

- **Utility model (μοντέλο χρηστικότητας)**: Το μοντέλο χρηστικότητας (ή αλλιώς μοντέλο ζήτησης) βασίζεται στη μέτρηση χρήσης της υπηρεσίας ή σε μία προσέγγιση τύπου «πληρώνεις-όσο-χρησιμοποιείς». Σε αντίθεση με τις υπηρεσίες συνδρομής, οι υπηρεσίες υπολογισμού βασίζονται σε πραγματικά ποσοστά χρήσης. Οι υπηρεσίες υπολογισμού έχουν χρησιμοποιηθεί για βασικές υπηρεσίες (ΔΕΗ, ΔΕΥΑ, Τηλεφωνικές υπηρεσίες). Οι πάροχοι υπηρεσιών διαδικτύου σε ορισμένα μέρη του κόσμου λειτουργούν ως επιχειρήσεις κοινής ωφελείας, χρεώνοντας τους πελάτες με το χρόνο σύνδεσης, σε αντίθεση με το συνδρομητικό μοντέλο των Η.Π.Α(Rappa,2010).

Στόχοι Ηλεκτρονικού Επιχειρείν

Οι στόχοι του ηλεκτρονικού επιχειρείν εκτείνονται σε όλους τους οικονομικούς τομείς. Οι βασικότερες χρήσεις του σήμερα περιλαμβάνουν την αυτοματοποίηση, την απλοποίηση και τον επανακαθορισμό επιχειρηματικών διεργασιών, τη δημιουργία εξατομικευμένων σχέσεων, τη βελτίωση της ποιότητας και τη δημιουργία υπηρεσιών/προϊόντων, τη μείωση του κόστους και την αύξηση του περιθωρίου κέρδους.

Οι στόχοι του ηλεκτρονικού επιχειρείν επικεντρώνονται στο να βελτιστοποιήσει τις υπάρχουσες δομές εισάγοντας την αυτοματοποίηση στις επιχειρήσεις αλλά και να δημιουργήσει και να ελέγξει νέα προϊόντα και υπηρεσίες (Δεληγιάννης,2006).

Οι ηλεκτρονικές συναλλαγές μέσω του διαδικτύου μπορεί να οριστούν ως ένα σύστημα που παρέχει στις επιχειρήσεις μια πλατφόρμα σύνδεσης με τους πελάτες τους επιχειρηματικούς εταίρους, τους εργαζόμενους και τους προμηθευτές. Η εσωτερική και εξωτερική συνδεσιμότητα του ηλεκτρονικού επιχειρείν δίνει τη δυνατότητα στις εταιρείες να είναι πιο αποτελεσματικές μειώνοντας το κόστος, αυξάνοντας την

παραγωγικότητα και επιτυγχάνοντας τους επιχειρηματικούς στόχους γρηγορότερα. Επιπρόσθετα, η ανταπόκριση στις ανάγκες των πελατών, η επικοινωνία με τις επιχειρήσεις και οι σχέσεις με τους προμηθευτές μπορεί να βελτιωθούν. Τα οφέλη ένταξης στο ηλεκτρονικό επιχειρείν υπερκαλύπτουν τις δαπάνες για τους περισσότερους οργανισμούς(Barau et al 2001, Lefebvre et al 2005, Straub,2001). Ωστόσο από την ανασκόπηση της βιβλιογραφίας φαίνεται ότι οι μικρομεσαίες επιχειρήσεις χρησιμοποιούν το διαδίκτυο κατά ένα μεγάλο ποσοστό για το ηλεκτρονικό ταχυδρομείο και τη διαφήμιση χωρίς να αξιοποιούν εξολοκλήρου την τεχνολογία του ηλεκτρονικού επιχειρείν εν συγκρίσει με τους μεγάλους οργανισμούς(Fillis et al. 2004, Pee et al. 2002, Quayle 2002, Grandon 2004). Η κατανόηση του πως μια εταιρεία μπορεί να επωφεληθεί από το ηλεκτρονικό επιχειρείν είναι το κλειδί για την εφαρμογή του ηλεκτρονικού επιχειρείν. Οι μικρομεσαίες επιχειρήσεις θα πρέπει να είναι βέβαιες ότι το ηλεκτρονικό επιχειρείν θα είναι ευθυγραμμισμένο με τους δικούς τους οργανωτικούς στόχους και ότι θα έχουν θετικά αποτελέσματα για την επιχείρηση. Μια καλά αναπτυγμένη στρατηγική που να περιλαμβάνει την ευελιξία και προσαρμοστικότητα για την έναρξη, διατήρηση και επικαιροποίηση του ηλεκτρονικού επιχειρείν είναι ζωτικής σημασίας. Η στρατηγική του ηλεκτρονικού επιχειρείν μπορεί να οριστεί ως η ανάπτυξη και υλοποίηση ενός σχεδίου για μια επιχείρηση να συναλλάσσεται ηλεκτρονικά. Κατά την ανάπτυξη μιας στρατηγικής ηλεκτρονικού επιχειρείν, οι εταιρείες θα πρέπει να εντοπίσουν τους τομείς της επιχειρηματικής δραστηριότητας που θα επηρεαστούν από την εφαρμογή του ηλεκτρονικού επιχειρείν. Ο ιδιοκτήτης της επιχείρησης καθώς και οι εργαζόμενοι θα πρέπει να συμμετέχουν στην ανάπτυξη ενός σχεδίου για την εφαρμογή του ηλεκτρονικού επιχειρείν και να εντοπίσουν τα οφέλη και τις αλλαγές που απαιτούνται από την εφαρμογή αυτού του συστήματος. Οι manager θα πρέπει να ενθαρρύνουν τη συμμετοχή των πελατών και των προμηθευτών στη φάση αυτή, δεδομένου ότι η ετοιμότητα και για τις δυο πλευρές για ηλεκτρονικό επιχειρείν είναι ουσιαστικής σημασίας για την επιτυχία του σχεδιασμού αυτού. Το σχέδιο θα πρέπει να περιλαμβάνει την τεχνολογία της πληροφορίας και της επικοινωνίας, τα μέτρα ασφαλείας που απαιτούνται καθώς και την παροχή μεθόδων για να κερδίσει την εμπιστοσύνη των πελατών, συνεργατών και προμηθευτών. Η μείωση των τιμών πρώτης ύλης, η μείωση των αποθεμάτων, η μείωση του χρόνου παράδοσης των προϊόντων, η μείωση του κόστους συναλλαγής και η

ευρύτερη γεωγραφική κάλυψη με την είσοδο σε νέες αγορές, αποτελούν πλεονεκτήματα που μπορούν να αποκομίσουν οι επιχειρήσεις μέσω του ηλεκτρονικού επιχειρείν. Επιπλέον,πρέπει να αναπτυχθεί μια στρατηγική εισόδου. Η είσοδος στο ηλεκτρονικό επιχειρείν σε λάθος στιγμή μπορεί να αποδειχθεί επιζήμια για τις μικρομεσαίες επιχειρήσεις(Evans 1999, Wright 2000, Sanderson 2004, Cote et al. 2005).

Οι απαιτήσεις και οι ανάγκες των πελατών αλλάζουν με την πάροδο του χρόνου. Ως εκτούτου μια εταιρεία θα πρέπει να είναι προετοιμασμένη να ενημερώσει το σύστημα της σε εύθετο χρόνο προκειμένου να συμβαδίσει με τη μεταβαλλόμενη ζήτηση της αγοράς. Η ικανοποίηση των αναγκών των πελατών απαιτεί μια αποτελεσματική στρατηγική μάρκετινγκ που θα περιλαμβάνει μια βάση δεδομένων πελατειακών σχέσεων που θα εμπεριέχει πληροφορίες σχετικά με την αγοραστική συμπεριφορά και τις προτιμήσεις των πελατών. Αυτήν η βάση δεδομένων παρέχει τη δυνατότητα οι προσπάθειες μάρκετινγκ να κατευθύνονται προς τις ανάγκες των πελατών. Ένα ολοκληρωμένο πρόγραμμα παρέχει τη δυνατότητα στο τμήμα πωλήσεων να καταγράφει την αντίδραση των υπαρχόντων αλλά και μελλοντικών πελατών σε νέα προγράμματα, τι αγοράζει ο κάθε πελάτης και πως αισθάνονται σχετικά με την κοστολόγηση των προϊόντων και την εξυπηρέτηση. Η ικανότητα καλύτερης εξυπηρέτησης του πελάτη, έχει ως αποτέλεσμα την αφοσίωση του πελάτη καθώς επίσης και της βελτίωσης των προϊόντων και υπηρεσιών που παρέχονται από την επιχείρηση. Η ένταξη του ηλεκτρονικού επιχειρείν στις επιχειρηματικές διαδικασίες περιλαμβάνει την ενσωμάτωση της τεχνολογίας της πληροφορίας και της επικοινωνίας σε επιχειρηματικές δραστηριότητες, έτσι ώστε οι συναλλαγές να διενεργούνται online. Σε γενικές γραμμές, η ανάπτυξη και εφαρμογή στρατηγικών μάρκετινγκ για το ηλεκτρονικό επιχειρείν, απαιτούν ουσιαστική αναδιάρθρωση και επανεξέταση των υφιστάμενων διαδικασιών. Οι manager θα πρέπει να εμφυσήσουν τη σημασία των εφαρμογών του ηλεκτρονικού επιχειρείν στους υπαλλήλους τους καθώς και στη συνεχιζόμενη κατάρτισή τους.

Ένα μοντέλο ηλεκτρονικού επιχειρείν είναι οι ηλεκτρονικές μέθοδοι και δομές που χρησιμοποιούνται από μια εταιρεία για να παραμείνει ανταγωνιστική και να παράγει έσοδα. Υπάρχουν διάφορα μοντέλα ηλεκτρονικού επιχειρείν που μπορεί να χρησιμοποιηθούν από έναν οργανισμό. Οι εταιρείες θα πρέπει να αναλύουν προσεκτικά

τις επιχειρήσεις τους και να αξιολογούν τα οφέλη και το κόστος του κάθε μοντέλου, προκειμένου να εξασφαλιστεί ότι γίνεται χρήση του καλύτερου συστήματος για την επιχείρησή τους. Η επιλογή του κατάλληλου μοντέλου μπορεί να μειώσει το κόστος διαμεσολάβησης, το κόστος αγοράς και να βελτιώσει τη σχέση μεταξύ αγοραστή-προμηθευτή(Barau et al. 2001).

Ηλεκτρονική Επιχειρηματικότητα και Internet

Η εξάπλωση του διαδικτύου έχει προσδώσει μια μοναδική ευκαιρία για τις μικρομεσαίες επιχειρήσεις να διεξάγουν συναλλαγές ηλεκτρονικά, να είναι πιο ανταγωνιστικές και να αναπτύσσουν επιχειρηματικότητα παγκοσμίως. Η διαδικτυακή παρουσία και η εφαρμογή του ηλεκτρονικού επιχειρείν μπορεί να είναι ευεργετική για πολλές εταιρείες, με την κατάλληλη προετοιμασία πριν από την εφαρμογή. Η χρήση του διαδικτύου στην Ευρωπαϊκή Ένωση και τη Σουηδία αυξήθηκε σε ένα ποσοστό της τάξης του 68% αντίστοιχα μεταξύ των ετών 2000 και 2005. Περίπου ο μισός πληθυσμός στην Ευρωπαϊκή Ένωση και το 75% των Σουηδών χρησιμοποιούν το διαδίκτυο(Internet Usage in Europe, 2006). Το διαδίκτυο έχει επιφέρει τρομακτικές αλλαγές στον τρόπο διεξαγωγής των επιχειρηματικών δραστηριοτήτων και απόρροια τούτου είναι η αύξηση των πιθανοτήτων εξάπλωσης των ηλεκτρονικών συναλλαγών μεταξύ των επιχειρήσεων αποτελώντας αναπόσπαστο κομμάτι του εμπορίου.

Ασφάλεια και ιδιωτικότητα του Ηλεκτρονικού Επιχειρείν

Κατά τη διεξαγωγή ηλεκτρονικών συναλλαγών μέσω του διαδικτύου, η ασφάλεια των μεταβιβαζόμενων στοιχείων των αγοραστών, επιχειρηματικών εταίρων και των προμηθευτών είναι ένα πολύ κρίσιμο ζήτημα για τις επιχειρήσεις. Η ακεραιότητα και το απόρρητο των πληροφοριών που ανταλλάσσονται μεταξύ των πελατών και των πωλητών θα πρέπει να προστατεύονται ανά πάσα στιγμή. Προκειμένου να εξασφαλιστεί η εμπιστοσύνη των πελατών για την ασφάλεια του διαδικτυακού χώρου, πολλοί οργανισμοί εμφανίζουν σφραγίδες ασφαλείας στην ιστοσελίδα τους(Hu et al.,2003). Θέματα ιδιωτικότητας και ασφάλειας θα πρέπει να διέπουν την στρατηγική του ηλεκτρονικού επιχειρείν καθώς και την ανάπτυξη δήλωσης πολιτικής ασφαλείας(Patton, 2004, Thuraisinham, 2005, Shih, 2005). Οι μικρομεσαίες επιχειρήσεις διατρέχουν μεγαλύτερο κίνδυνο δεδομένου του ότι δεν διαθέτουν την εμπειρία και τα οικονομικά

μέσα για να προστατευτούν από μη εξουσιοδοτημένη πρόσβαση σε εμπιστευτικές πληροφορίες από υπαλλήλους, εξωτερικές απειλές ή και από τους χάκερ. Οι manager θα πρέπει να λαμβάνουν μέτρα για την ασφάλεια του δικτύου τους κατά τη διενέργεια των συναλλαγών που πραγματοποιούνται online προκειμένου να διασφαλίσουν τους επιχειρηματικούς εταίρους και τους πελάτες τους(Beheshti,2007).

ΚΕΦΑΛΑΙΟ 2
Ασφάλεια Δεδομένων

2.1 Απαιτήσεις Ασφάλειας

Οι πολιτικές ασφαλείας της πληροφορίας παρέχουν ζωτικής σημασίας υποστήριξη για την διασφάλιση των επαγγελματιών καθώς προσπαθούν να μειώσουν το προφίλ κινδύνου μιας επιχείρησης και να αποκρούσουν εσωτερικές και εξωτερικές απειλές. Το θέμα είναι ότι πολύ λίγοι οργανισμοί αφιερώνουν χρόνο στη δημιουργία πολιτικών ασφαλείας. Το χάος που μπορεί να προκύψει δεν ενεργεί προς όφελος κανενός και συχνά εκθέτουν την επιχείρηση σε απρόβλεπτα ζητήματα. Πρωταρχικό παράδειγμα παραγωγής καλών και κακών πολιτικών ασφαλείας της πληροφορίας αποτελεί η Εθνική Υπηρεσία Υγείας των Η.Π.Α. Ο οργανισμός αυτός μοιράζεται και καταναλώνει μεγάλο όγκο πολύ ευαίσθητων πληροφοριών σε καθημερινή βάση, έτσι ώστε να υπάρχει απαίτηση από εκείνους που διαχειρίζονται τα δεδομένα αυτά να διαθέτουν την υποστήριξη των πολιτικών ασφαλείας των πληροφοριών, οι οποίες με τη σειρά τους υπόκεινται σε ετήσιο έλεγχο (Scott,2013).

2.2 Κίνδυνοι Ασφάλειας

Τα συστήματα πληροφοριών υπόκεινται σε σοβαρές απειλές που μπορεί να έχουν αρνητικές επιπτώσεις στις οργανωτικές λειτουργίες, στα στοιχεία και σε άλλους οργανισμούς, αξιοποιώντας τόσο γνωστές όσο και άγνωστες αδυναμίες με σκοπό να θέσουν σε κίνδυνο την εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα της πληροφορίας που υποβάλλεται σε επεξεργασία, αποθήκευση ή μεταδίδεται από τα συστήματα αυτά. Οι κίνδυνοι για την πληροφορία ή τα πληροφοριακά συστήματα μπορεί να περιλαμβάνουν σκόπιμες επιθέσεις, ανθρώπινα ή μηχανικά λάθη με αποτέλεσμα την πρόκληση βλάβης στην ασφάλεια των εθνικών και οικονομικών συμφερόντων. Ως εκ τούτου κρίνεται επιτακτική η ανάγκη της κατανόησης σε όλα τα επίπεδα των ευθυνών για τη διαχείριση του κινδύνου της ασφάλειας των πληροφοριών, κίνδυνος που συνδέεται με τη λειτουργία και τη χρήση των πληροφοριακών συστημάτων που υποστηρίζουν τις αποστολές και επιχειρηματικές λειτουργίες των οργανισμών τους.

Οι κίνδυνοι μπορεί να περιλαμβάνουν πολλούς τύπους π.χ. κίνδυνος διαχείρισης του προγράμματος, κίνδυνος ασφαλείας κ.λ.π. Ο κίνδυνος ασφαλείας που σχετίζεται με τη λειτουργία και τη χρήση των πληροφοριακών συστημάτων, είναι μόνο μια από τις

πολλές συνιστώσες κινδύνου του οργανισμού που οι διαχειριστές θα πρέπει να αντιμετωπίζουν ως μέρος της συνεχιζόμενης ευθύνης τους για τη διαχείρισή του. Η αποτελεσματική διαχείριση του κινδύνου ανάγεται στο ότι οι οργανισμοί λειτουργούν σε εξαιρετικά πολύπλοκα, διασυνδεδεμένα περιβάλλοντα που χρησιμοποιούν την τελευταία λέξη της τεχνολογίας και κληρονομικά συστήματα πληροφοριών, συστήματα που οι οργανισμοί εξαρτώνται για την ολοκλήρωση των αποστολών τους και τη διενέργεια λειτουργιών που σχετίζονται με την επιχειρηματικότητα (National Institute of Standards and Technology, 2011).

2.3 Υπηρεσίες Ασφαλείας (Security services)

Το πρότυπο ISO 7498-2 καθορίζει μια σειρά υπηρεσιών για την προστασία της επικοινωνίας μεταξύ των ανοικτών συστημάτων. Καθορίζει τα σχετιζόμενα με την ασφάλεια στοιχεία και δημιουργεί κατευθυντήριες οδηγίες και περιορισμούς για την βελτίωση των υπαρχόντων προτύπων ή την ανάπτυξη νέων. Στόχος του προτύπου είναι η ασφαλής επικοινωνία και η παροχή συνεχούς προσέγγισης στην ασφάλεια της Ανοικτής Διασύνδεσης Συστημάτων. Το πρότυπο ISO 7498-2 προσδιορίζει τις βασικές υπηρεσίες ασφάλειας (Weidong, 1997). Οι υπηρεσίες αυτές κατηγοριοποιούνται ως εξής:

- **Υπηρεσίες αυθεντικοποίησης**
- **Υπηρεσίες προστασίας ακεραιότητας**
- **Υπηρεσίες υποστήριξης μη αποποίησης ευθύνης**
- **Υπηρεσίες προστασίας εμπιστευτικότητας**
- **Υπηρεσίες ελέγχου πρόσβασης**
- **Υπηρεσίες εξασφάλισης συνεχούς λειτουργίας**
- **Υπηρεσίες Αυθεντικοποίησης (authentication):** Η υπηρεσία αυθεντικοποίησης (Authentication service) παρέχει τη διασφάλιση ότι η επικοινωνία είναι αυθεντική. Στην περίπτωση ενός μηνύματος, όπως είναι ένα σήμα προειδοποίησης συναγερμού, η λειτουργία της αυθεντικοποίησης εγγυάται στη διαβεβαίωση του παραλήπτη ότι το μήνυμα είναι από την πηγή που ισχυρίζεται ότι είναι. Στην περίπτωση της συνεχούς αλληλεπίδρασης, όπως είναι η σύνδεση ενός τερματικού σε έναν ξενιστή, εμπλέκονται δυο πτυχές : Πρώτον, κατά την έναρξη της σύνδεσης, η υπηρεσία διαβεβαιώνει ότι οι δυο οντότητες είναι

αυθεντικές. Δεύτερον, η υπηρεσία θα πρέπει να εξασφαλίζει ότι η σύνδεση δεν παρεμβάλλεται κατά τέτοιο τρόπο ώστε ένα τρίτο μέρος μπορεί να μεταμφιεστεί ως ένα από τα δύο νόμιμα μέρη με σκοπό τη μη εξουσιοδοτημένη μεταβίβαση ή λήψη. Υπάρχουν δύο υπηρεσίες ελέγχου ταυτότητας:

- Εξακρίβωση ταυτότητας χρήστη (user authentication): Παρέχεται για χρήση κατά την εγκατάσταση ή κατά τη διάρκεια της φάσης μεταφοράς δεδομένων μιας σύνδεσης. Παρέχει εμπιστοσύνη ότι μια οντότητα δεν επιχειρεί είτε μεταμφίεση είτε μια μη εξουσιοδοτημένη επανάληψη προηγούμενης σύνδεσης.
- Εξακρίβωση ταυτότητας προέλευσης δεδομένων (data origin authentication) Παρέχει τη δυνατότητα επιβεβαίωσης της πηγής μιας μονάδας δεδομένων. Δεν παρέχει προστασία έναντι στην αντιγραφή ή την τροποποίηση μιας μονάδας δεδομένων. Αυτού του είδους η υπηρεσία υποστηρίζει εφαρμογές όπως το ηλεκτρονικό ταχυδρομείο, όπου δεν υπάρχουν προηγούμενες αλληλεπιδράσεις μεταξύ των οντοτήτων που επικοινωνούν(Stallings,2011).

- **Υπηρεσίες Ακεραιότητας (integrity):** Η υπηρεσία ακεραιότητας (Integrity service) πρέπει να εξασφαλίσει την ακεραιότητα (integrity) ενός μηνύματος. Επιβεβαιώνει δηλαδή ότι τα μηνύματα που λαμβάνονται δεν έχουν παραποιηθεί, τροποποιηθεί, αναδιαταχθεί ή επαναληφθεί. Η καταστροφή των δεδομένων επίσης καλύπτεται από την υπηρεσία αυτή. Αφενός η υπηρεσία ακεραιότητας εξυπηρετεί τη ροή τροποποίησης των μηνυμάτων αλλά και την άρνηση εξυπηρέτησης. Αφετέρου μια ασυνδεσμική υπηρεσία ακεραιότητας ασχολείται με μεμονωμένα μηνύματα χωρίς να λαμβάνεται υπόψη οποιοδήποτε ευρύτερο πλαίσιο και γενικά παρέχει προστασία έναντι μόνο στην τροποποίηση μηνυμάτων. Σε περίπτωση ανίχνευσης παραβίασης της ακεραιότητας, η υπηρεσία απλώς αναφέρει την παραβίαση και κάποια άλλη παρέμβαση από λογισμικό ή ανθρώπινη απαιτείται για να ανακάμψει από την παραβίαση. Εναλλακτικά, υπάρχουν διαθέσιμοι μηχανισμοί για την ανάκτηση της απώλειας της ακεραιότητας των δεδομένων. Η ενσωμάτωση αυτοματοποιημένων μηχανισμών ανάκτησης είναι συνήθως η πιο ελκυστική εναλλακτική λύση(Stallings,2011).

- **Υπηρεσίες μη αποποίηση ευθύνης (nonrepudiation):** Αποτρέπει τον αποστολέα ή τον δέκτη από την άρνηση συμμετοχής. Έτσι, όταν αποστέλλεται ένα μήνυμα, ο δέκτης μπορεί να αποδείξει ότι ο φερόμενος ως αποστολέας είναι στην πραγματικότητα αυτός που έχει αποστείλει το μήνυμα. Παρομοίως όταν γίνεται λήψη ενός μηνύματος, ο αποστολέας μπορεί να αποδείξει ότι ο φερόμενος ως δέκτης στην πραγματικότητα έχει λάβει το μήνυμα(Stallings,2011).
- **Υπηρεσίες Εμπιστευτικότητας (confidentiality):** Αφορούν στην προστασία των δεδομένων που μεταβιβάζονται από παθητικές επιθέσεις. Απώτερος στόχος της υπηρεσίας αυτής είναι η προστασία των δεδομένων από μη εξουσιοδοτημένες οντότητες. Μεγάλη είναι η σημασία της υπηρεσίας της εμπιστευτικότητας και στο χώρο της υγείας. Η άλλη όψη της υπηρεσίας εμπιστευτικότητας είναι η προστασία της ροής της κυκλοφορίας από την ανάλυση. Αυτό προϋποθέτει ότι ένας εισβολέας δεν θα είναι σε θέση να παρατηρεί την πηγή και τον προορισμό, τη συχνότητα, τη διάρκεια ή άλλα χαρακτηριστικά της κυκλοφορίας σε μια εγκατάσταση επικοινωνιών(Stallings,2011).
- **Υπηρεσίες ελέγχου πρόσβασης:** Στο πλαίσιο της ασφάλειας του δικτύου, η υπηρεσία ελέγχου πρόσβασης έχει τη δυνατότητα να περιορίζει και να ελέγχει την πρόσβαση σε ξενιστές και εφαρμογές μέσω συνδέσμων επικοινωνίας. Για να επιτευχθεί αυτό, κάθε οντότητα που προσπαθεί να αποκτήσει πρόσβαση, θα πρέπει πρώτα να ταυτοποιείται, ούτως ώστε τα δικαιώματα πρόσβασης να μπορούν να προσαρμοστούν στο άτομο(Stallings,2011).

ΚΕΦΑΛΑΙΟ 3
Κρυπτογραφία (Cryptography)

3.1. Κρυπτογραφία

Το συνοπτικό λεξικό της Οξφόρδης (2006), ορίζει την κρυπτογραφία ως την τέχνη γραφής και επίλυσης κωδικών. Ο ορισμός αυτός μπορεί ιστορικά να είναι ακριβής, αλλά δεν συλλαμβάνει την ουσία της σύγχρονης κρυπτογραφίας. Πρώτον, επικεντρώνεται αποκλειστικά και μόνο στο πρόβλημα της μυστικής επικοινωνίας. Αυτό αποδεικνύεται από το γεγονός ότι ο ορισμός καθορίζει κώδικες, που ορίζονται ως ένα σύστημα προκαθορισμένων σημάτων, που χρησιμοποιούνται κυρίως για την εξασφάλιση της μυστικότητας στη μετάδοση μηνυμάτων. Δεύτερον, ο ορισμός αναφέρεται στην κρυπτογραφία ως μια μορφή τέχνης. Πράγματι μέχρι τον $20^{ο}$ αιώνα και αναμφισβήτητα μέχρι τα τέλη του αιώνα αυτού, η κρυπτογραφία ήταν τέχνη. Η δημιουργία κωδικών ή το «σπάσιμο» των υφιστάμενων στηριζόταν στη δημιουργικότητα και τις ατομικές δεξιότητες. Ελάχιστη θεωρία υπήρχε που θα μπορούσε κανείς να επικληθεί και δεν υπήρχε καν μια καθορισμένη έννοια από το τι συνιστάται ένας καλός κωδικός. Μια πλούσια θεωρία αναδύθηκε, μετατρέποντας τη μελέτη της κρυπτογραφίας ως επιστήμη. Επιπλέον, ο τομέας της κρυπτογραφίας περιλαμβάνει τώρα πολλά περισσότερα από τη μυστική επικοινωνία, συμπεριλαμβανομένης την αυθεντικοποίηση του μηνύματος, ψηφιακές υπογραφές, πρωτόκολλα για την ανταλλαγή μυστικών κλειδιών, πρωτόκολλα ελέγχου ταυτότητας, ηλεκτρονικές δημοπρασίες καθώς και ψηφιακά μετρητά. Στην πραγματικότητα η σύγχρονη κρυπτογραφία μπορεί να ειπωθεί ότι ασχολείται με προβλήματα που μπορεί να προκύψουν σε οποιοδήποτε κατανεμημένο σύστημα που μπορεί να δεχτεί εσωτερικές και εξωτερικές επιθέσεις. Εν ολίγοις, η σύγχρονη κρυπτογραφία είναι η επιστημονική μελέτη των τεχνικών για την διασφάλιση των ψηφιακών πληροφοριών, τις συναλλαγές και τα κατανεμημένα συστήματα.

Άλλη πολύ σημαντική διαφορά μεταξύ της κλασσικής κρυπτογραφίας (πριν τη δεκαετία του 1980) και της μοντέρνας κρυπτογραφίας έγκειται στο ποιος την χρησιμοποιεί. Ιστορικά, οι μεγαλύτεροι χρήστες της κρυπτογραφίας ήταν οι στρατιωτικές και μυστικές υπηρεσίες. Στη σημερινή εποχή ωστόσο η κρυπτογραφία βρίσκεται παντού. Μηχανισμοί ασφαλείας που στηρίζονται στην κρυπτογραφία αποτελούν αναπόσπαστο μέρος σχεδόν

όλων των υπολογιστικών συστημάτων. Οι χρήστες, συχνά εν αγνοία τους βασίζονται στην κρυπτογραφία κάθε φορά που αποκτούν πρόσβαση σε μια ασφαλή ιστοσελίδα. Κρυπτογραφικές μέθοδοι χρησιμοποιούνται για την επιβολή του ελέγχου πρόσβασης στα λειτουργικά συστήματα πολλών χρηστών και να αποτρέψουν την κλοπή. Μέθοδοι προστασίας του λογισμικού χρησιμοποιούν την κρυπτογράφηση, τον έλεγχο ταυτότητας και άλλα εργαλεία για να αποτρέψουν την αντιγραφή.

Εν ολίγοις, η κρυπτογραφία έχει περάσει από μια μορφή τέχνης που καταπιάστηκε με τη μυστική επικοινωνία για το στρατό σε μια επιστήμη που βοηθά στην ασφάλεια των συστημάτων παγκοσμίως. Αυτό επίσης σημαίνει ότι η κρυπτογραφία γίνεται όλο και πιο κεντρικό θέμα στην επιστήμη των υπολογιστών(Katz, 2007).

Η κρυπτογραφία είναι η επιστήμη που έχει ως σκοπό, μέσω της χρήσης μαθηματικών τεχνικών, την ασφάλεια των ηλεκτρονικών συναλλαγών. Η ιστορία της κρυπτογραφίας έχει μακρά ιστορία. Ίχνη της ανευρίσκονται στην αρχική και περιορισμένη χρήση της από τους Αιγυπτίους περίπου 4000 χρόνια πριν, με τον εικοστό αιώνα που έπαιξε καθοριστικό ρόλο στην έκβαση των δυο παγκοσμίων πολέμων. Η εφαρμογή της τέχνης αυτής υιοθετήθηκε από το στρατό, τις διπλωματικές υπηρεσίες και την κυβέρνηση γενικότερα. Η κρυπτογραφία χρησιμοποιήθηκε ως εργαλείο για την προστασία των εθνικών μυστικών και στρατηγικών. Η ανάπτυξη των ηλεκτρονικών υπολογιστών και των συστημάτων επικοινωνίας τη δεκαετία του 1960, έφερε μαζί και την ανάγκη μέσων προστασίας από τον ιδιωτικό τομέα της πληροφορίας σε ψηφιακή μορφή και την παροχή υπηρεσιών ασφαλείας.

Σημαντικός σταθμός στην ιστορία της κρυπτογραφίας αποτέλεσε το έτος 1976 όταν οι Diffie και Hellman δημοσίευσαν νέες κατευθύνσεις στην κρυπτογραφία. Η μελέτη αυτή εισήγαγε την επαναστατική ιδέα της κρυπτογραφίας δημόσιου κλειδιού και επίσης παρείχε μια ευφυή μέθοδο για την ανταλλαγή κλειδιού, η ασφάλεια της οποίας βασίζεται στο δυσεπίλυτο πρόβλημα του διακριτού λογάριθμου. Αν και οι μελετητές δεν είχαν καμία πρακτική υλοποίηση του καθεστώτος της κρυπτογραφίας δημόσιου κλειδιού, η ιδέα ήταν σαφής και έγειρε έντονο ενδιαφέρον και δραστηριότητα στην κοινότητα της κρυπτογραφίας. Το 1978 οι Rivest, Shamir και Adleman ανακάλυψαν το πρώτο πρακτικό σχήμα κρυπτογράφησης δημοσίου κλειδιού και υπογραφής(Menezes,1996).

3.2 Συμμετρική κρυπτογραφία (Symmetric cryptography)

Η κρυπτογραφία ιστορικά σχετιζόταν με την απόρρητη επικοινωνία. Συγκεκριμένα, η κρυπτογραφία ασχολείται με τη δημιουργία αλγορίθμων κρυπτογράφησης (σήμερα ονομάζονται συστήματα κρυπτογράφησης) για την παροχή απόρρητης επικοινωνίας μεταξύ δυο μερών, που μοιράζονται κάποια πληροφορία. Η ρύθμιση με την οποία τα δυο επικοινωνούντα μέρη μοιράζονται κάποια απόρρητη πληροφορία είναι σήμερα γνωστή ως ιδιωτικό κλειδί ή συμμετρικό κλειδί.

Στη ρύθμιση του συμμετρικού κλειδιού, δύο μέρη μοιράζονται κάποια απόρρητη πληροφορία που ονομάζεται κλειδί και χρησιμοποιούν αυτό το κλειδί όταν επιθυμούν να έχουν μια απόρρητη επικοινωνία μεταξύ τους. Ένα σύστημα που αποστέλλει ένα μήνυμα χρησιμοποιεί το κλειδί για να κρυπτογραφήσει το μήνυμα πριν την αποστολή και ο δέκτης χρησιμοποιεί το ίδιο κλειδί για να αποκρυπτογραφήσει το μήνυμα. Το μήνυμα αποκαλείται απλό κείμενο και η κωδικοποιημένη πληροφορία η οποία μεταδίδεται από τον αποστολέα στον δέκτη ονομάζεται κρυπτογραφημένο κείμενο. Το κλειδί χρησιμεύει για τη διάκριση των επικοινωνούντων συστημάτων από άλλα συστήματα που μπορεί να υποκλέπτουν την επικοινωνία τους (η οποία θεωρείται ότι λαμβάνει χώρα μέσω ενός δημόσιου καναλιού). Τονίζεται ότι σε αυτή τη ρύθμιση, το ίδιο κλειδί χρησιμοποιείται για να μετατρέψει το απλό κείμενο σε κρυπτογραφημένο και το αντίστοιχο. Αυτό εξηγεί γιατί η ρύθμιση αυτή είναι γνωστή και ως ρύθμιση συμμετρικού κλειδιού, όπου η συμμετρία έγκειται στο γεγονός ότι και τα δυο συστήματα έχουν το ίδιο κλειδί το οποίο χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση. Αυτό έρχεται σε αντίθεση με την ασύμμετρη κρυπτογράφηση όπου αποστολέας και δέκτης δεν μοιράζονται απόρρητες πληροφορίες και διαφορετικά κλειδιά χρησιμοποιούνται για την κρυπτογράφηση και αποκρυπτογράφηση. Μια σιωπηρή παραδοχή σε κάθε σύστημα που χρησιμοποιεί την κρυπτογράφηση συμμετρικού κλειδιού είναι ότι τα επικοινωνούντα συστήματα διαθέτουν κάποιο τρόπο να μοιράζονται αρχικά ένα κλειδί με κρυφό τρόπο. Σημειώνεται ότι εάν η μια οντότητα στείλει το κλειδί στην άλλη μέσω ενός δημόσιου καναλιού, ο υποκλοπέας θα το κατέχει επίσης. Στις στρατιωτικές εγκαταστάσεις, αυτό δεν αποτελεί σοβαρό πρόβλημα, διότι οι οντότητες που επικοινωνούν έχουν τη δυνατότητα συνάντησης εξ επαφής σε μια ασφαλή τοποθεσία προκειμένου να αποφασίσουν για το κλειδί. Σε πολλές σύγχρονες εγκαταστάσεις, ωστόσο οι οντότητες

δεν έχουν τη δυνατότητα της συνάντησης εξ επαφής. Αυτό δημιουργεί μεγάλη ανησυχία και στην πραγματικότητα περιορίζει την εφαρμογή των συστημάτων κρυπτογράφησης, που βασίζονται αποκλειστικά σε μεθόδους ιδιωτικού κλειδιού. Παρά το γεγονός αυτό, υπάρχουν αρκετές ρυθμίσεις όπου οι μέθοδοι του ιδιωτικού κλειδιού επαρκούν και είναι σε ευρεία χρήση.

Ένα σύστημα κρυπογράφησης ιδιωτικού κλειδιού, αποτελείται από τρεις αλγόριθμους : Ο πρώτος είναι μια διαδικασία αναπαραγωγής κλειδιών, ο δεύτερος μια διαδικασία κρυπτογράφησης και ο τρίτος μια διαδικασία αποκρυπτογράφησης. Οι αλγόριθμοι αυτοί έχουν την ακόλουθη λειτουργικότητα :

1. Ο αλγόριθμος αναπαραγωγής κλειδιού (Gen) είναι ένας πιθανολογούμενος αλγόριθμος που παράγει ένα κλειδί (K) που έχει επιλεγεί σύμφωνα με διανομή που έχει καθοριστεί από το σύστημα.
2. Ο αλγόριθμος κρυπτογράφησης (Enc) εισάγει ένα κλειδί και ένα απλό κείμενο και εξάγει ένα κρυπτοκείμενο.
3. Ο αλγόριθμος αποκρυπτογράφησης (Dec) εισάγει ένα κλειδί και ένα κρυπτοκείμενο και εξάγει ένα απλό κείμενο.

Το 1977 υιοθετήθηκε από το National Bureau of Standards των Η.Π.Α. ο αλγόριθμος DES. Η χρήση ισχυρών υπολογιστών δύναται να σπάσει τον αλγόριθμο αυτό καθώς επίσης και ειδικά Hardware. Το triple-DES, μπορεί να παρέχει μεγαλύτερη ασφάλεια και βασίζεται στη χρήση του DES τρεις φορές.

Το Νοέμβριο του 2001 υιοθετήθηκε από τις Ηνωμένες Πολιτείες Αμερικής ο Advanced Encryption Algorithm, ο οποίος αντικατέστησε τον DES.

Η ταχύτητα αποτελεί ένα από τα σημαντικότερα πλεονεκτήματα της συμμετρικής κρυπτογραφίας. Επίσης, οι εφαρμογές συμμετρικής κρυπτογραφίας μπορεί να έχουν μικρές απαιτήσεις υπολογιστικής ισχύος και μνήμης, ώστε να πραγματοποιούνται και σε περιβάλλον όπου η μνήμη και η ισχύς επεξεργαστή είναι περιορισμένες (π.χ. σε έξυπνες κάρτες).

Η ασφαλής διανομή του συμμετρικού κλειδιού αποτελεί ένα από τα σημαντικότερα μειονεκτήματα της συμμετρικής κρυπτογραφίας. Η διατήρηση της μυστικότητας του συμμετρικού κλειδιού αποτελεί τη βάση ασφάλειας των μηχανισμών της συμμετρικής

κρυπτογραφίας. Η συμμετρική κρυπτογραφία αποτελεί την παλαιότερη μορφή κρυπτογραφίας και τη μοναδική, μέχρι τη δεκαετία του 1970 με την ανακάλυψη της κρυπτογραφίας δημόσιου κλειδιού (Katz,2007).

3.3 Ασύμμετρη κρυπτογραφία ή δημοσίου κλειδιού (asymmetric or Public-key cryptography)

Στην ιστορία της κρυπτογραφίας, τα δύο μέρη βασίζονται σε ένα κλειδί που θα ανταλλάσσουν μεταξύ τους μέσω μιας ασφαλούς αλλά μη κρυπτογραφημένης μεθόδου. Το 1874 ένα βιβλίο που εκδόθηκε από τον William Stanley Jevons, περιέγραφε τη σχέση μονόδρομων συναρτήσεων στην κρυπτογραφία (Jevons,1874). Το 1970 ο James H.Ellis, Βρετανός κρυπτογράφος στο Αρχηγείο Επικοινωνιών της Κυβέρνησης του Ηνωμένου Βασιλείου, συνέλαβε την ιδέα της μη μυστικής κρυπτογράφησης (σήμερα ονομάζεται κρυπτογραφία δημόσιου κλειδιού) χωρίς όμως να μπορεί να την εφαρμόσει. Το 1973 ο συνεργάτης του Clifford Cocks εφηύρε αυτό που έγινε γνωστό ως αλγόριθμος κρυπτογράφησης RSA (Rivest, Shamir, Adleman) δηλαδή έναν κρυπταλγόριθμο ασσύμμετρου κλειδιού, ο οποίος πήρε το όνομα του από τους δημιουργούς του. Ο αλγόριθμος εκτός από την κωδικοποίηση των μηνυμάτων χρησιμοποιούνταν και ως ψηφιακή υπογραφή. Το 1974 ένας άλλος μαθηματικός και κρυπτογράφος ο Malcolm J. Williamson ανέπτυξε αυτό που τώρα είναι γνωστό ως πρωτόκολλο ανταλλαγής κλειδιού Diffie-Hellman. Τίποτα από τα παραπάνω δεν φαινόταν να έχουν πρακτική χρήση και όταν ανακαλύφθηκαν δεν έτυχαν δημόσιας αναγνώρισης ώσπου η έρευνα αποχαρακτηρίστηκε από τη Βρετανική Κυβέρνηση το 1997(Singh,1997).

Από τη δεκαετία του 1970 ένας μεγάλος αριθμός και ποικίλων μορφών κρυπτογράφησης, ψηφιακής υπογραφής, συμφωνία κλειδιού και άλλων τεχνικών αναπτύχθηκαν στον τομέα της κρυπτογραφίας δημόσιου κλειδιού. Το κρυπτοσύστημα ElGamal, που ανακαλύφθηκε από τον Taher ElGamal, βασίζεται στο παρόμοιο και υψηλής δυσκολίας επίπεδο πρόβλημα του διακριτού λογάριθμου.

Το σύστημα της κρυπτογραφίας δημόσιου κλειδιού, ονομάζεται επίσης και ασσύμμετρο λόγω της ασσυμετρίας σε βασικές πληροφορίες που κατέχουν οι οντότητες. Δηλαδή, η μια οντότητα έχει ένα μυστικό κλειδί ενώ μια άλλη οντότητα έχει το δημόσιο κλειδί που ταιριάζει με αυτό το μυστικό κλειδί. Αυτό έρχεται σε αντίθεση με το σύστημα του

συμμετρικού ιδιωτικού κλειδιού, όπου και οι δυο οντότητες έχουν το ίδιο κλειδί. Η ασύμμετρη κρυπτογραφία είναι επομένως μια άλλη ονομασία για την κρυπτογράφηση δημόσιου κλειδιού, ο μηχανισμός για την επίτευξη της προστασίας των προσωπικών δεδομένων στο δημόσιο κλειδί ή την ασύμμετρη ρύθμιση.

Υπάρχουν δυο κύριες χρήσεις της κρυπτογραφίας δημόσιου κλειδιού:

- Κρυπτογράφηση δημόσιου κλειδιού, στην οποία ένα μήνυμα κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη. Το μήνυμα δεν μπορεί να αποκρυπτογραφηθεί από οποιονδήποτε που δεν έχει την αντιστοιχία του ιδιωτικού κλειδιού, ο οποίος ως εκ τούτου θεωρείται ότι είναι ο ιδιοκτήτης του κλειδιού αυτού και το πρόσωπο που συνδέεται με το δημόσιο κλειδί. Αυτό χρησιμοποιείται σε μια προσπάθεια να διασφαλιστεί η εμπιστευτικότητα.
- Ψηφιακές υπογραφές, στις οποίες ένα μήνυμα έχει υπογραφεί με το ιδιωτικό κλειδί του αποστολέα και μπορεί να ελεγχθεί από οποιονδήποτε έχει πρόσβαση στο δημόσιο κλειδί του αποστολέα. Η επαλήθευση αυτήν επιβεβαιώνει ότι ο αποστολέας έχει πρόσβαση στο ιδιωτικό κλειδί και ως εκ τούτου είναι πιθανό να είναι το πρόσωπο που συνδέεται με το δημόσιο κλειδί. Αυτό επίσης διασφαλίζει ότι το μήνυμα δεν έχει παραποιηθεί, καθώς οποιαδήποτε παραποίηση του μηνύματος θα οδηγήσει σε αλλαγές του κωδικοποιημένου μηνύματος, το οποίο διαφορετικά παραμένει αμετάβλητο μεταξύ του αποστολέα και του παραλήπτη.

Μια αναλογία κρυπτογράφησης δημόσιου κλειδιού είναι αυτή του κλειδωμένου γραμματοκιβώτιου με την υποδοχή για αλληλογραφία. Η υποδοχή για την αλληλογραφία είναι εκτεθειμένη και προσβάσιμη στο κοινό, είναι κατ' ουσίαν το δημόσιο κλειδί. Ο οποιοσδήποτε γνωρίζει τη διεύθυνση της οδού μπορεί να πάει και να ρίξει ένα γραπτό μήνυμα στο γραμματοκιβώτιο. Ωστόσο μόνο το άτομο που κατέχει το κλειδί μπορεί να ανοίξει το γραμματοκιβώτιο και να το διαβάσει.

Μια αναλογία ψηφιακών υπογραφών είναι το σφράγισμα των φακέλων με μια προσωπική σφραγίδα από κερί. Το μήνυμα μπορεί να ανοιχτεί από οποιονδήποτε, αλλά η παρουσία της μοναδικής σφραγίδας επαληθεύει την ταυτότητα του αποστολέα.

Ένα πρόβλημα που προκύπτει με τη χρήση της κρυπτογραφίας δημόσιου κλειδιού είναι η εμπιστευτικότητα/απόδειξη ότι το συγκεκριμένο δημόσιο κλειδί είναι αυθεντικό, υπό την

έννοια ότι είναι σωστό και ανήκει στην οντότητα που ισχυρίζεται ότι είναι και δεν έχει αλλοιωθεί ή αντικατασταθεί από μια τρίτη οντότητα. Η συνήθης προσέγγιση στο πρόβλημα αυτό είναι η χρήση ενός δημόσιου κλειδιού υποδομής, κατά το οποίο ένα ή περισσότερα τρίτα μέρη, γνωστά ως αρχές έκδοσης πιστοποιητικών, πιστοποιούν την κατοχή του ζεύγους κλειδιών(Ferguson,2003).

Στα υπέρ της ασύμμετρης κρυπτογραφίας καταλογίζεται το γεγονός ότι δεν κρίνεται απαραίτητη η γνώση του κοινού κλειδιού από τον αποστολέα και τον παραλήπτη, κάτι που συμβαίνει στη συμμετρική κρυπτογραφία.

Στα κατά της ασύμμετρης κρυπτογραφίας καταλογίζεται ότι υστερεί σε ταχύτητα και το κρυπτοκείμενο έχει μεγαλύτερο μέγεθος από το αρχικό απλό κείμενο.

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

Στην ασύμμετρη κρυπτογράφηση ο αλγόριθμος RSA θεωρείται ο πιο σημαντικός και είναι ευρέως διαδεδομένος, σε γενικές γραμμές θεωρείται ασφαλής και χρησιμοποιείται και στην ψηφιακή υπογραφή (Katz,2007).

3.4 Ψηφιακές υπογραφές (Digital signatures)

Η χρήση *ψηφιακών υπογραφών*, κατά την ανταλλαγή πληροφοριών, εγγυάται την αυθεντικότητα της ταυτότητας του αποστολέα και την ακεραιότητα της πληροφορίας. Τα πρωτόκολλα ψηφιακής υπογραφής επιτρέπουν στον προσυπογράφοντα ο οποίος έχει δημιουργήσει ένα δημόσιο κλειδί, να υπογράψει ένα μήνυμα με τέτοιο τρόπο ώστε οποιοδήποτε άλλο μέρος γνωρίζει το δημόσιο κλειδί (και γνωρίζει ότι αυτό το δημόσιο κλειδί έχει δημιουργηθεί από αυτόν που υπογράφει) μπορεί να επαληθεύσει ότι το μήνυμα προέρχεται από αυτόν που το υπογράφει και δεν έχει τροποποιηθεί με τον οποιοδήποτε τρόπο.

Οι κώδικες αυθεντικοποίησης του μηνύματος και τα πρωτόκολλα ψηφιακών υπογραφών χρησιμοποιούνται για την διασφάλιση της ακεραιότητας ή αυθεντικότητας των μεταβιβαζόμενων μηνυμάτων. Η χρήση των ψηφιακών μηνυμάτων αντί της χρήσεως κωδικών αυθεντικότητας του μηνύματος, απλοποιεί τη διαχείριση του κλειδιού σε

περίπτωση που ένας αποστολέας χρειάζεται να επικοινωνήσει με πολλαπλούς δέκτες. Συγκεκριμένα, κάνοντας χρήση ενός πρωτοκόλλου ψηφιακής υπογραφής ο αποστολέας έχει τη δυνατότητα να αποφύγει τη δημιουργία ενός ξεχωριστού μυστικού κλειδιού με κάθε δυνητικό δέκτη και να αποφύγει να υπολογίσει ένα ξεχωριστό κώδικα αυθεντικοποίησης. Αντ' αυτού ο αποστολέας χρειάζεται μόνο να υπολογίσει μια υπογραφή που μπορεί να επαληθευτεί από όλους τους δέκτες.

Ένα ποιοτικό πλεονέκτημα των ψηφιακών υπογραφών σε σχέση με τους κώδικες αυθεντικοποίησης είναι ότι οι υπογραφές είναι επαληθεύσιμες δημοσίως. Αυτό σημαίνει ότι εάν ο δέκτης επαληθεύσει την υπογραφή σε ένα μήνυμα ως νόμιμη, τότε διασφαλίζεται ότι όλα τα υπόλοιπα μέρη που θα λάβουν αυτό το υπογεγραμμένο μήνυμα θα το επιβεβαιώσουν ως νόμιμο επίσης. Το χαρακτηριστικό αυτό δεν επιτυγχάνεται με τους κώδικες αυθεντικοποίησης, όταν αυτός που υπογράφει μοιράζεται ένα ξεχωριστό κλειδί με τον κάθε δέκτη. Σε μια τέτοια ρύθμιση ένας κακόβουλος αποστολέας μπορεί να υπολογίσει μια σωστή ετικέτα MAC σε σχέση με το κλειδί του δέκτη Α, αλλά με μια λανθασμένη ετικέτα MAC σε σχέση με ένα διαφορετικό κλειδί του χρήστη Β. Στην περίπτωση αυτή, ο δέκτης Α γνωρίζει ότι έχει λάβει ένα αυθεντικό μήνυμα από τον αποστολέα αλλά δεν έχει καμία εγγύηση ότι οι άλλοι παραλήπτες θα συμφωνήσουν. Η δημόσια επαλήθευση συνεπάγεται ότι οι υπογραφές είναι μεταβιβάσιμες. Η υπογραφή σε ένα μήνυμα από έναν συγκεκριμένο υπογράφοντα μπορεί να είναι ορατή από ένα τρίτο μέρος, το οποίο μπορεί να επαληθεύσει ότι η υπογραφή είναι νόμιμη σε σχέση με το δημόσιο κλειδί του υπογράφοντα. Αντιγράφοντας την υπογραφή, το τρίτο μέρος μπορεί έπειτα να δείξει την υπογραφή σε άλλο μέρος και να τους πείσει ότι το μήνυμα έχει την αυθεντική υπογραφή. Η δυνατότητα μεταβίβασης και η δημόσια επαλήθευση είναι απαραίτητες στην εφαρμογή των ψηφιακών υπογραφών, στα πιστοποιητικά και στην υποδομή του δημοσίου κλειδιού. Τα πρωτόκολλα ψηφιακών υπογραφών παρέχουν επίσης την πολύ σημαντική ιδιότητα της μη αποποίησης της ευθύνης. Έτσι, αν ο υπογράφων δημοσιοποιήσει ευρέως το δημόσιο κλειδί, από τη στιγμή που ο υπογράφων θα υπογράψει ένα μήνυμα, δεν μπορεί να αρνηθεί ότι δεν το έκανε. Η πτυχή αυτή των ψηφιακών υπογραφών είναι ζωτικής σημασίας για τις περιπτώσεις όπου ο δικαιούχος πρέπει να αποδείξει σε τρίτους ότι ένας υπογράφων πιστοποίησε στην πραγματικότητα

ένα συγκεκριμένο μήνυμα. Οι κώδικες αυθεντικοποίησης δεν παρέχουν τη λειτουργία αυτή(Katz,2007).

3.5 Νομικό πλαίσιο ψηφιακών υπογραφών

Όταν χρησιμοποιείται ένα σύστημα ασφαλείας ψηφιακών υπογραφών, θα πρέπει να λαμβάνεται υπόψη το ισχύον νομικό πλαίσιο. Μεγάλη έμφαση θα πρέπει να δίνεται στο ιατρικό πληροφοριακό σύστημα, όπου θα πρέπει να καθίσταται σαφές τι μέλλει γενέσθαι σε περιπτώσεις άρνησης λήψης ή αποστολής συγκεκριμένων εγγράφων.

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

1. ***Ηλεκτρονική υπογραφή*** ("ασθενής" ή "ελαφριά" υπογραφή): Η ηλεκτρονική υπογραφή είναι ουσιαστικά το ισοδύναμο της χειρόγραφης υπογραφής, με τα δεδομένα να είναι σε ηλεκτρονική μορφή που συνδέονται με άλλα δεδομένα (τιμολόγιο, απόδειξη πληρωμής, σύμβαση κ.λ.π.) ως μέσο πιστοποίησης της γνησιότητας. Χρησιμοποιεί κρυπτογραφία ασύμμετρου κλειδιού. Χρησιμοποιείται για τον έλεγχο της ταυτότητας, για την επιβεβαίωση ότι το άτομο που στέλνει το μήνυμα είναι ο κάτοχος της ηλεκτρονικής υπογραφής, αν και δεν μπορεί να εξασφαλιστεί με βεβαιότητα. Ο κάτοχος του κλειδιού είναι μια οντότητα που έχει την πρακτική χρήση της ηλεκτρονικής υπογραφής και είναι αυτός που έχει το δικαίωμα να το χρησιμοποιήσει. Συνήθως ο κάτοχος του κλειδιού είναι ένας διακομιστής που δημιουργεί υπογραφές π.χ. το λογισμικό μιας εταιρείας. Η εταιρεία ή ο υπάλληλος θα είναι ο κάτοχος του κλειδιού. Η ρητή αυτή διαφορά προκύπτει από την Ρωμαϊκή εποχή και τα δικαιώματα του κατόχου της υπογραφής έναντι του ιδιοκτήτη αποτελεί τη βάση του αστικού δικαίου για πολλές χώρες, Ευρωπαϊκές και μη. Ένα πράγμα καθίσταται σαφές στη διαφορά αυτή. Υπάρχουν περιπτώσεις όπου ο κάτοχος του κλειδιού μπορεί να είναι μια φυσική οντότητα, αν και αυτό είναι λιγότερο πιθανό. Για παράδειγμα, εάν ένας manager είναι ο ιδιοκτήτης του κλειδιού, η γραμματέας του θα μπορούσε να είναι ο κάτοχος της ηλεκτρονικής υπογραφής που έχει το πραγματικό κλειδί υπογραφής και τις συσκευές. Ωστόσο η γραμματέας θα μπορούσε να υπογράψει χρησιμοποιώντας την άδεια του manager. Μια ηλεκτρονική υπογραφή γίνεται

δεκτή ως αποδεικτικό στοιχείο σε νομικές διαδικασίες, αλλά ο δικαστής θα κρίνει την αξία της. Οι ηλεκτρονικές υπογραφές υπόκεινται στην ίδια νομοθεσία που διέπει τις χειρόγραφες υπογραφές(Mazzeo,2012).

2. ***Προηγμένη ηλεκτρονική υπογραφή***: Διέπεται από τα ακόλουθα χαρακτηριστικά γνωρίσματα:
    - Συνδέεται με τον υπογράφοντα και μόνο αυτόν.
    - Είναι ικανή να λειτουργήσει ως αναγνωριστικό του υπογράφοντος.
    - Η δημιουργία της γίνεται με μέσα που ο υπογράφων διατηρεί υπό τον έλεγχό του και μόνο.
    - Συνδέεται με τα δεδομένα στα οποία αναφέρεται με τέτοιο τρόπο ώστε κάθε αλλαγή στα δεδομένα αυτά να είναι ανιχνεύσιμη (άρθρο 2.2 της Οδηγίας 1999/93/EC).

Η προηγμένη ψηφιακή υπογραφή έχει σημαντικότερη αξία από την απλή ψηφιακή υπογραφή: Εγγυάται την ακεραιότητα του κειμένου, αλλά και την αυθεντικοποίηση (Mazzeo, 2012).

3. ***Προηγμένη ηλεκτρονική υπογραφή που βασίζεται σε ένα κατάλληλο πιστοποιητικό και που δημιουργείται από μια Αρχή δημιουργίας ασφαλών υπογραφών*** (ασφαλής ή ισχυρή ψηφιακή υπογραφή). Η Αρχή δημιουργίας ασφαλών υπογραφών είναι η Certification Authority ή CA και πρέπει να έχει τα κατάλληλα τεχνικά χαρακτηριστικά που απαιτούνται ώστε, να εξασφαλιστεί το γεγονός, ότι το κλειδί δεν θα μπορεί να αναπαραχθεί, ούτε να πλαστογραφηθεί, μέσα σε ένα λογικό χρονικό διάστημα. Το χρονικό διάστημα αυτό, θα πρέπει να είναι μεγαλύτερο σε διάρκεια από την περίοδο εγκυρότητας της υπογραφής. Οι απαιτήσεις αυτές καθορίζονται ξεκάθαρα από την Επιτροπή Ψηφιακών Υπογραφών (Electronic Signature Committee), που βοηθά την ανάλυση τεχνικών θεμάτων.

Οι απαιτήσεις μια τέτοιας ασφαλούς υπογραφής είναι σημαντικά: τα κατάλληλα κλειδιά και λογισμικό, έξυπνες κάρτες και κάθε άλλο απαραίτητο μέσο πρέπει να είναι της τελευταίας τεχνολογίας (σύμφωνα με την δικανική αρχή “meliores scientia et

conoscientia" δηλαδή με την τελευταία λέξη της τεχνολογίας). Οι απαιτήσεις για ένα κατάλληλο πιστοποιητικό είναι (σύμφωνα με το παράρτημα I της Οδηγίας 1999/93/EC):

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

Η ασφαλής υπογραφή μπορεί να περιέχει επίσης και άλλα στοιχεία, όπως ένας όρος για κάποιο ιδιαίτερο χαρακτηριστικό του υπογράφοντος. Για παράδειγμα ένας ιατρός μιας κλινικής μπορεί να έχει μια ασφαλή υπογραφή. Μπορεί να υπάρχουν περιορισμοί που να προσδιορίζουν ότι μπορούν να υπογραφούν γνωματεύσεις μόνο σε ορισμένους ασθενείς.

Αυτός ο τύπος ψηφιακής υπογραφής έχει μεγάλη νομική αξία: Εγγυάται την αυθεντικοποίηση, ακεραιότητα, εμπιστευτικότητα καθώς και εμποδίζει την δυνατότητα άρνησης της αποστολής/λήψης ενός εγγράφου.

Συμπερασματικά, οι ψηφιακές υπογραφές στηρίζονται από έγκυρους Ευρωπαϊκούς νόμους και έτσι οι ασφαλείς ψηφιακές υπογραφές έχουν αποκτήσει σημαντική νομική αξία. Μπορούμε να πούμε ότι είναι πλέον απαραίτητο στοιχείο για εφαρμογές που απαιτούν την διακίνηση πληροφορίας με ασφάλεια και υπευθυνότητα(Mazzeo,2012).

ΚΕΦΑΛΑΙΟ 4
Υποδομή Δημόσιου Κλειδιού

4.1. Υποδομή "Δημοσίου Κλειδιού (PKI)

Ο όρος *Υποδομή "Δημόσιου Κλειδιού (PKI)* αναφέρεται σε ένα σύνολο ισχυρών υπηρεσιών ασφάλειας, οι οποίες στηρίζονται σε θεμελιώδεις *μηχανισμούς κρυπτογραφίας*. Οι θεμελιώδεις μηχανισμοί του PKI είναι ο έλεγχος αυθεντικότητας, ο έλεγχος ακεραιότητας και η διατήρηση της εμπιστευτικότητας, μέσω της χρήσης ψηφιακών υπογραφών, ψηφιακών πιστοποιητικών, συμμετρικής και ασύμμετρης κρυπτογράφησης. Η κρυπτογραφία δημόσιου κλειδιού δεν επαρκεί από μόνη της για να εξασφαλίσει την ασφάλεια των συναλλαγών του ηλεκτρονικού επιχειρείν. Οι επιχειρήσεις χρειάζονται ένα πλαίσιο που να παρέχει πολιτικές αναπαραγωγής κλειδιών και των διαδικασιών για τη διανομή αυτών των κλειδιών. Η υποδομή δημόσιου κλειδιού παρέχει ένα τέτοιο πλαίσιο. Η υποδομή δημόσιου κλειδιού είναι ένα πλαίσιο που αποτελείται από πολιτικές ασφαλείας, μηχανισμούς κρυπτογράφησης και εφαρμογές που παράγουν, αποθηκεύουν και διαχειρίζονται κλειδιά. Επίσης παρέχει διαδικασίες για την αναπαραγωγή, διανομή αξιοποίησης κλειδιών και πιστοποιητικών. Παρέχει ένα μηχανισμό δημοσίευσης των δημοσίων κλειδιών που αποτελούν μέρος της κρυπτογραφίας δημόσιου κλειδιού. Περιγράφει τις πολιτικές, τα standards και το λογισμικό που χρησιμοποιείται για τη ρύθμιση των πιστοποιητικών, δημοσίων και ιδιωτικών κλειδιών.

Η εμπιστοσύνη αποτελεί τη βάση για όλες τις επικοινωνίες, είτε πρόκειται για φυσική είτε για ηλεκτρονική. Στη φυσική επικοινωνία, η οικοδόμηση της εμπιστοσύνης είναι σχετικά εύκολη καθώς μπορεί να αναγνωριστεί το πρόσωπο ή η οντότητα, είτε με την πρόσωπο με πρόσωπο αλληλεπίδραση ή ορισμένα σημεία αναγνώρισης, όπως υπογραφές, σφραγίδα συμβολαιογράφου ή ακόμα και το επιστολόχαρτο. Ωστόσο στην περίπτωση της ηλεκτρονικής επικοινωνίας, η οικοδόμηση αυτής της εμπιστοσύνης είναι αρκετά δύσκολη, διότι η ταυτότητα της άλλης οντότητας παραμένει κρυφή και επίσης οι περισσότερες από τις μεθόδους ταυτοποίησης ή ασφάλειας που θεωρούνται ως δεδομένες σε μια μη ηλεκτρονική ή φυσική επικοινωνία δεν υφίστανται. Αυτή η εμπιστοσύνη δεν μπορεί να προσδιοριστεί μέχρι ότου και εκτός οι δυο οντότητες να βεβαιωθούν για τις

ταυτότητες τους και ότι η πληροφορία που ανταλλάσσουν μέσω δικτύου είναι απολύτως ασφαλής από κάθε είδους αλλοίωση. Ένα παράδειγμα που δίνεται είναι όταν βρισκόμαστε μέσα σε ένα κατάστημα είμαστε απολύτως σίγουροι για τη νομιμότητα της εταιρείας. Μπορούμε να δούμε και να αγγίξουμε ένα προϊόν, μπορούμε να γνωρίζουμε τον πωλητή και όταν δίνουμε την πιστωτική κάρτα στο ταμείο μπορεί να μην αισθανόμαστε τον κίνδυνο ότι θα γίνει κατάχρησή της με τον οποιονδήποτε τρόπο. Ωστόσο όταν πραγματοποιούμε παρόμοια συναλλαγή στο διαδίκτυο, δεν είμαστε απολύτως σίγουροι για την νομιμότητα της εταιρείας ή του προϊόντος. Δεν είμαστε ακόμη σίγουροι για την ταυτότητα του ατόμου στο οποίο στέλνουμε τον αριθμό της πιστωτικής κάρτας. Η χρήση υποδομής δημόσιου κλειδιού έρχεται για να αντιμετωπίσει αυτά τα βασικά προβλήματα εμπιστοσύνης, αυθεντικοποίησης και ασφάλειας στο διαδίκτυο. Η υποδομή δημόσιου κλειδιού επιφέρει την ασφάλεια και εμπιστοσύνη του φυσικού κόσμου στον ηλεκτρονικό κόσμο, παρέχοντας τη δυνατότητα ασφαλών ηλεκτρονικών επικοινωνιών και συναλλαγών.

Οι βασικές λειτουργίες ασφαλείας που παρέχονται από την κρυπτογραφία είναι η εμπιστευτικότητα, η μη αποποίηση της ευθύνης, η αυθεντικοποίηση και η ακεραιότητα. Επιπρόσθετα σε αυτές τις βασικές λειτουργίες ασφαλείας, είναι απαραίτητο να υφίστανται τα ακόλουθα για ασφαλή και αξιόπιστη ηλεκτρονική αλληλεπίδραση :

- Πολιτικές που καθορίζουν κανόνες για τη λειτουργία των κρυπτογραφικών συστημάτων.
- Μηχανισμοί για τη διαχείριση, αποθήκευση και δημιουργία κλειδιών.
- Κατευθυντήριες οδηγίες για τη διαχείριση, αποθήκευση, διανομή και δημιουργία κλειδιών και πιστοποιητικών.

Με άλλα λόγια, αυτό που χρειάζεται είναι η υποδομή δημόσιου κλειδιού. Συνοψίζοντας η υποδομή δημόσιου κλειδιού είναι ένα πλαίσιο που αποτελείται από υλικό, λογισμικό, πολιτικές και διαδικασίες που απαιτούνται για τη διαχείριση, τη δημιουργία, την αποθήκευση και τη διανομή κλειδιών και ψηφιακών πιστοποιητικών. Για να ενσωματωθούν όλες αυτές οι οντότητες αυτού του πλαισίου, υπάρχουν ποικίλα στοιχεία της υποδομής δημόσιου κλειδιού(Choudhury,2002).

4.2 "Δομικά Μέρη της Υποδομής "Δημοσίου Κλειδιού στην υγεία

Η Υποδομή Δημοσίου Κλειδιού για δίκτυο τηλεματικών υπηρεσιών στην υγεία αποτελείται από:

- Αρχές Πιστοποίησης (CAs), είναι ένα αξιόπιστο τρίτο μέρος που πιστοποιεί τις οντότητες που λαμβάνουν μέρος σε μια ηλεκτρονική συναλλαγή. Για την αυθεντικοποίηση της οντότητας, η αρχή πιστοποίησης εκδίδει ένα ψηφιακό πιστοποιητικό. Αυτό το πιστοποιητικό είναι ένα ψηφιακό έγγραφο που καθορίζει τα διαπιστευτήρια των οντοτήτων που λαμβάνουν μέρος σε μια συναλλαγή. Τα ψηφιακά πιστοποιητικά που εκδίδονται από την αρχή πιστοποίησης περιέχουν πληροφορίες, όπως το όνομα του συνδρομητή, το δημόσιο και ιδιωτικό κλειδί του συνδρομητή και την έκδοση του δημόσιου κλειδιού από την αρχή πιστοποίησης. Η πληροφορία αυτή εξαρτάται από την πολιτική της εταιρείας που εκδίδει τα πιστοποιητικά. Πριν την έκδοση ενός ψηφιακού πιστοποιητικού, η αρχή πιστοποίησης επαληθεύει το αίτημα για πιστοποιητικό με την Αρχή Εγγραφής. Για την επικύρωση των αιτήσεων, η αρχή πιστοποίησης χρησιμοποιεί τις δικές τις διαδικασίες. Οι διαδικασίες αυτές εξαρτώνται από την πολιτική της εταιρείας και της διαθέσιμης υποδομής για την επικύρωση της αίτησης. Εάν η αίτηση επικυρωθεί, η αρχή πιστοποίησης εκδίδει το πιστοποιητικό.
- Αρχές εγγραφής (RAs), είναι υπεύθυνες για την αλληλεπίδραση μεταξύ των πελατών και των αρχών πιστοποίησης. Συχνά εξαιτίας του όγκου των αιτημάτων για πιστοποιητικό, δεν καθίσταται δυνατό για την αρχή πιστοποίησης να δεχτεί τα αιτήματα πιστοποιητικών, την επικύρωση των αιτήσεων και την έκδοση των πιστοποιητικών. Σε τέτοιες περιπτώσεις, η αρχή εγγραφής ενεργεί ως μεσάζων μεταξύ της αρχής πιστοποίησης και του πελάτη. Το έργο που διενεργείται από την αρχή εγγραφής είναι :
  - Λήψη αιτήσεων των οντοτήτων και επικύρωσή τους
  - Αποστολή των αιτήσεων στην αρχή πιστοποίησης
  - Λήψη του επεξεργασμένου πιστοποιητικού από την αρχή πιστοποίησης
  - Αποστολή του πιστοποιητικού στη σωστή οντότητα

  Η αρχή εγγραφής είναι εξαιρετικά χρήσιμη για την κλιμάκωση των εφαρμογών της υποδομής δημόσιου κλειδιού σε διάφορες γεωγραφικές τοποθεσίες.

- Συστήματα διαχείρισης πιστοποιητικών (Certificate management systems/CMS) για τη διαχείριση των πιστοποιητικών των επαγγελματιών υγείας καθόλη τη διάρκεια ισχύς τους. Οι Αρχές Πιστοποίησης χρησιμοποιούν και ελέγχουν τα συστήματα διαχείρισης πιστοποιητικών (CMS).
- Καταλόγους X.500 (directories), όπου αποθηκεύονται τα πιστοποιητικά των επαγγελματιών υγείας όπως επίσης και δημόσια πληροφορία για τους κατόχους των πιστοποιητικών και χρησιμοποιούνται κατά την επαλήθευση των ψηφιακών πιστοποιητικών(Choudhury,2002).

4.3 Υπηρεσίες πιστοποίησης Ιατρικού προσωπικού

Οι λειτουργίες που είναι απαραίτητες για την παροχή υπηρεσιών πιστοποίησης (Certificate Services) των επαγγελματιών υγείας για σύστημα ασφαλείας τηλεματικού δικτύου υγείας είναι οι παρακάτω:

4.3.1. Ηλεκτρονική δήλωση (Electronic registration)

Ως Αρχή Εγγραφής (Registration Authority) θεωρείται η υπηρεσία που παρέχεται από εξουσιοδοτημένο προσωπικό με σκοπό τη συλλογή των απαραίτητων έγγραφων πιστοποιητικών, τα οποία πρέπει να προσκομίσουν οι επαγγελματίες υγείας προκειμένου να αποδειχθεί η ταυτότητα τους. Τα στοιχεία που θεωρούνται απαραίτητα αποστέλλονται στην αρχή πιστοποίησης για να εκδοθούν τα ηλεκτρονικά πιστοποιητικά. Σε πολλές περιπτώσεις ένας επαγγελματίας υγείας είναι δηλωμένος (registered) σαν χρήστης σε ορισμένες ιατρικές εφαρμογές. Ο όρος εφαρμογή (application) χρησιμοποιείται εδώ με την ευρεία του έννοια. Μπορεί για παράδειγμα να έχει πρόσβαση σε ένα τοπικό και σε ένα καθολικό πληροφοριακό σύστημα. Προκειμένου ο επαγγελματίας υγείας να δηλωθεί ως χρήστης θα πρέπει να αποδείξει την ταυτότητα και την ιδιότητα του. Μια προσέγγιση είναι να εκδίδονται οι εξουσιοδοτήσεις (authorizations) με τη μορφή υπογεγραμμένων ψηφιακών πιστοποιητικών χρησιμοποιώντας την ίδια προσέγγιση όπως και στα πιστοποιητικά των δημοσίων κλειδιών. Κατά αρχήν μπορεί να γίνει προσθέτοντας κάποια πληροφορία για την επαγγελματική κατάσταση στο πιστοποιητικό του δημόσιου κλειδιού. Η χρήση της γενικής δομής του X.509 λειτουργεί ως πλεονέκτημα λόγω του ότι είναι στη διάθεση μας διάφορα προϊόντα. Παραδείγματος χάρη υπάρχουν διάφορα προϊόντα που μπορούν να χρησιμοποιηθούν για Υπηρεσίες Καταλόγου (Directory

services) ακόμα και αν δεν είναι απαραίτητο να πιστοποιηθεί το δημόσιο κλειδί ξανά, αλλά μόνο η σύνδεση μεταξύ του διακεκριμένου ονόματος (distinguished name) και της ιατρικής επαγγελματικής κατάστασης (professional status). Πρέπει να παρατηρήσουμε ότι αν το πιστοποιητικό της επαγγελματικής κατάστασης χρησιμοποιηθεί μαζί με το πιστοποιητικό δημόσιου κλειδιού, το πιστοποιητικό της επαγγελματικής κατάστασης πρέπει να χρησιμοποιεί το ίδιο διακεκριμένο όνομα με το πιστοποιητικό δημόσιου κλειδιού.

4.3.2 Ονομασία (Naming)

Πρέπει να υπογραμμιστεί ότι είναι απαραίτητο να αναπτυχθεί ένα σχήμα ονομασίας που να είναι ανεξάρτητο από μια συγκεκριμένη περιοχή (domain) και να μπορεί να χρησιμοποιηθεί γενικά. Το σχήμα της ονομασίας (naming scheme) πρέπει να υποστηρίζει μια ονομασία που να παραμένει έγκυρη για πολύ μεγάλο χρονικό διάστημα. Ο στόχος είναι να συνδεθεί η μακράς διάρκειας εγκυρότητα με ένα μοναδικό αναγνωριστικό (identifier) και ένα όνομα, το οποίο να είναι κατανοητό από τους ανθρώπους. Η έξυπνη κάρτα των Επαγγελματιών Υγείας (Health care Professional Card) χρησιμοποιείται σαν κάρτα μοναδικής ταυτοποίησης. Το σχήμα που προτείνουμε για ονομασία είναι το ιεραρχικό σχήμα του ονοματολογικού δένδρου του X.500 [RFC 1422] γιατί μας δίδει τη δυνατότητα να υποστηρίξουμε μοναδικά ονόματα.

Κάθε επαγγελματίας θα έχει ένα μοναδικό όνομα, και εάν είναι δυνατό παγκοσμίως μοναδικό. Το μοναδικό όνομα για να προσδιορίζουμε τον ιατρικό κλάδο θα χρησιμοποιείται για το "διακεκριμένο όνομα" (Distinguished Name/ DN) του X.509 v3 πιστοποιητικού. Τα διακεκριμένα ονόματα περιέχουν αλφαριθμητικά strings που έχουν νόημα και τα οποία προσδιορίζουν μοναδικά και με ακρίβεια τους επαγγελματίες υγείας που είναι κάτοχοι των πιστοποιητικών.

4.3.3. Εξατομίκευση & Αποθήκευση κλειδιού (Key Personalization & Key repository)

Η έξυπνη κάρτα του επαγγελματία υγείας αποτελεί το κλειδί για πρόσβαση, έλεγχο και εξουσιοδότηση (access control and authorization token). Παρακάτω παρουσιάζεται η ακολουθία από φάσεις που περιγράφουν την εξατομίκευση (personalization) της έξυπνης κάρτας.

Φάση	Περιγραφή
1. Εισαγωγή των δεδομένων για τον χρήστη (user data)	Τα δεδομένα του χρήστη εισάγονται από ένα τερματικό. Η πληροφορία μπορεί επίσης να ληφθεί σαν αρχείο από μια εξωτερική βάση δεδομένων.
2. Εξατομίκευση (Personalisation)	Οι κάρτες εξατομικεύονται, γράφοντας πάνω τους πληροφορία που είναι μοναδική.
3. Διανομή της κάρτας	Η κάρτα διανέμεται στο χρήστη. Μπορεί να δοθεί απευθείας στο χρήστη από ένα χειριστή, ή να παραδοθεί ταχυδρομικώς.
4. Αρχειοθέτηση	Πληροφορία για όλες τις κάρτες που παράχθηκαν σώζεται σε ένα αρχείο.

Πίνακας 1. Φάσεις της εξατομίκευσης (Personalisation) της έξυπνης κάρτας

4.3.4 "Δομή Πιστοποιητικού Ταυτότητας Επαγγελματία Υγείας

Το πρότυπο X.509 συνίσταται για τη δομή (format) των πιστοποιητικών των επαγγελματιών υγείας.

Τα πιστοποιητικά δημοσίων κλειδιών εκδίδονται σε ένα επαγγελματία υγείας, ο όποιος χρησιμοποιεί το πιστοποιητικό αυτό σαν ηλεκτρονική ιατρική ταυτότητα σε διάφορες ιατρικές εφαρμογές.

Τα πιστοποιητικά δημοσίων κλειδιών περιέχουν την εξής πληροφορία:

- Τον αριθμό έκδοσης (version number) του πιστοποιητικού (προτείνουμε X.509 version3).
- Το σειριακό αριθμό (serial number) του πιστοποιητικού.
- Το όνομα του αλγόριθμου που χρησιμοποιείται για την υπογραφή του πιστοποιητικού (προτείνουμε να χρησιμοποιηθεί σαν αλγόριθμος σύνοψης μηνύματος ο SHA-1 και ο RSA σαν κρυπτογραφικός αλγόριθμος).

- Το όνομα της Αρχής Πιστοποίησης που έχει υπογράψει και εκδώσει το πιστοποιητικό (διακεκριμένο όνομα X.500 ("distinguished name").
- Το χρονικό διάστημα ισχύος του πιστοποιητικού (προτείνεται διάστημα ενός έτους).
- Το όνομα του κατόχου του πιστοποιητικού (διακεκριμένο όνομα X.500 ("distinguished name").
- Το δημόσιο κλειδί του κατόχου του πιστοποιητικού και του αλγορίθμου με τον οποίο χρησιμοποιείται το δημόσιο κλειδί (προτείνεται ο αλγόριθμος RSA).
- Το αναγνωριστικό του κλειδιού της Αρχής Πιστοποίησης, το οποίο δίνει τη δυνατότητα να προσδιοριστεί το δημόσιο κλειδί της Αρχής Πιστοποίησης με το οποίο υπογράφηκε το πιστοποιητικό. Αυτό το πεδίο χρησιμοποιείται μόνο αν η Αρχή Πιστοποίησης έχει πολλαπλά κλειδιά για να υπογράφει διαφορετικές κατηγορίες πιστοποιητικών.
- Πληροφορία για τη χρήση του κλειδιού που περιγράφει τους σκοπούς που το πιστοποιημένο δημόσιο κλειδί μπορεί να χρησιμοποιηθεί (προαιρετικό πεδίο). Χρησιμοποιείται αν το κλειδί χρησιμοποιείται για συγκεκριμένους σκοπούς μόνο και η Αρχή Πιστοποίησης θέλει να τους προσδιορίσει (π.χ. υπογραφή ιατρικών πράξεων και αποκρυπτογράφηση μηνυμάτων).
- Πληροφορία για την πολιτική πιστοποίησης που υποδεικνύει την πολιτική ασφαλείας που ίσχυε όταν εκδόθηκε το πιστοποιητικό και τους σκοπούς που μπορεί να χρησιμοποιηθεί το πιστοποιητικό (προαιρετικό πεδίο).
- Τα σημεία διανομής Λιστών Ακύρωσης Πιστοποιητικών (CRL distribution points) τα οποία προσδιορίζουν πως και που μπορούμε να λάβουμε πληροφορία για τις Λίστες Ακύρωσης Πιστοποιητικών.

4.4 "Διαχείριση Πιστοποιητικών Επαγγελματιών Υγείας

Η διαχείριση των πιστοποιητικών επαγγελματιών υγείας περιλαμβάνει τα εξής:

- Δημιουργία Πιστοποιητικών επαγγελματιών υγείας
- Διανομή και αποθήκευση Πιστοποιητικών επαγγελματιών υγείας
- Ακύρωση Πιστοποιητικών επαγγελματιών υγείας

4.4.1 "Δημιουργία Πιστοποιητικών επαγγελματιών υγείας

Ανάλογα με τις πολιτικές που ακολουθούνται σε κάθε τομέα, η Αρχή Πιστοποίησης του τηλεματικού δικτύου υγείας, είναι δυνατό να επιτρέπει τη χρήση του ίδιου κλειδιού σε διαφορετικού τύπου εφαρμογές ή να δύναται η χρήση διαφορετικών κλειδιών σε διαφορετικές εφαρμογές. Προκειμένου να διασφαλιστεί η ασφάλεια, είναι προτιμότερη η χρήση διαφορετικών κλειδιών. Εν προκειμένω η Αρχή Πιστοποίησης θα πρέπει να προβαίνει στην έκδοση ξεχωριστού πιστοποιητικού, το οποίο θα είναι ανάλογο με το σκοπό που πρόκειται να χρησιμοποιηθεί. Τα δεδομένα που είναι απαραίτητα για τη δημιουργία του πιστοποιητικού, εξαρτώνται από τη χρήση του δημόσιου κλειδιού που πιστοποιεί.

4.4.2. Επικύρωση δεδομένων και συντακτικός έλεγχος (Data validation and syntax control)

Τα δεδομένα που απαιτούνται προκειμένου να δημιουργηθεί ένα πιστοποιητικό αφού πρώτα συλλεχθούν θα πρέπει να επικυρωθούν. Η επικύρωση και ο έλεγχος των στοιχείων γίνεται από την Αρχή Εγγραφής.

4.4.3. Έλεγχος για μοναδικό κωδικό επαγγελματία υγείας / λειτουργίες κανόνων (Control of unique user id/ rules functions)

Η μοναδικότητα των πιστοποιητικών που δημιουργούνται για τους επαγγελματίες υγείας είναι ζωτικής σημασίας, η οποία δύναται να εξασφαλιστεί από ένα σειριακό αριθμό. Μπορεί να υπάρχουν ειδικοί κανόνες, που να δηλώνουν ότι πρέπει να υπάρχει το πολύ ένα έγκυρο πιστοποιητικό που να έχει εκδοθεί με το ίδιο όνομα. Η διατήρηση ενός καταλόγου των πιστοποιητικών που έχουν εκδοθεί ή η καταγραφή των στοιχείων των επαγγελματιών υγείας στους οποίους έχουν εκδοθεί τα πιστοποιητικά, μπορεί να προσδώσουν λύσεις σε τέτοιου είδους περιπτώσεις.

4.4.4. Λειτουργία δημιουργίας πιστοποιητικών (Certificate generation function)

Ανάλογα με την πολιτική που ακολουθείται από το τηλεματικό δίκτυο υγείας τα πιστοποιητικά δημοσίων κλειδιών είναι προγραμματισμένα να εκδίδουν κλειδιά κατά τη

διάρκεια της διαδικασίας δημιουργίας του πιστοποιητικού ή μπορούν και να χρησιμοποιούν κλειδιά που έχουν δημιουργηθεί από πριν. Τα δεδομένα που έχουν συλλεχθεί για τη δημιουργία ενός πιστοποιητικού προστατεύονται από κρυπτογραφικά μέσα, τα οποία κατόπιν πακετάρονται και κωδικοποιούνται σύμφωνα με το πρότυπο του X.509 v3. Ανάλογα με τον αλγόριθμο που έχει επιλεγεί τα δεδομένα που έχουν πια κωδικοποιηθεί, υπογράφονται. Τα κωδικοποιημένα δεδομένα μαζί με την υπογραφή της Αρχής Πιστοποίησης του τηλεματικού δικτύου υγείας, κωδικοποιούνται κατόπιν περαιτέρω όπως ορίζει το πρότυπο X.509 v3. Το πιστοποιητικό ιατρικής ταυτότητας είναι το δυαδικό αλφαριθμητικό (binary string) που παίρνουμε σαν αποτέλεσμα.

4.5. "Διανομή και αποθήκευση και ανάκτηση πιστοποιητικών επαγγελματιών υγείας

Η αποθήκευση των πιστοποιητικών μόνο σε κάρτες μπορεί να μην είναι αρκετή.

Μερικοί λόγοι για αυτό είναι:

- Ένα πιστοποιητικό δεν πρέπει να είναι κρυφό.
- Η μνήμη των έξυπνων καρτών είναι μικρή με αποτέλεσμα ένας ελάχιστος αριθμός πιστοποιητικών να μπορεί να αποθηκευτεί.
- Η έκδοση του πιστοποιητικού δεν συνεπάγεται απαραίτητα την ύπαρξη έξυπνων καρτών σε συγκεκριμένα μέρη για να γίνει η αποθήκευση.
- Μόλις εκδοθεί το πιστοποιητικό, πρέπει να διανεμηθεί σε βάση δεδομένων δημόσιας πρόσβασης.
- Ο παραλήπτης δεν αρκεί να γνωρίζει το πιστοποιητικό του αποστολέα αλλά και όλα τα πιστοποιητικά του πλήρους μονοπατιού πιστοποίησης (certification path) από τον αποστολέα προς τα πάνω έως και την Αρχή Πιστοποίησης της οποίας το δημόσιο κλειδί είναι αυθεντικά διαθέσιμο στον παραλήπτη.
- Τα πιστοποιητικά πρέπει να έχουν σφραγίδα χρόνου (time stamp) και να μπορούν να ανακληθούν. Συνεπώς, ο παραλήπτης ενός πιστοποιητικού πρέπει να έχει πρόσβαση στην αντίστοιχη λίστα ανάκλησης. Σε ένα τηλεματικό δίκτυο υγείας η αποθήκευση των πιστοποιητικών δεν πρέπει να γίνεται μόνο σε έξυπνες κάρτες. Τα πιστοποιητικά των επαγγελματιών υγείας θα πρέπει να είναι δημόσια διαθέσιμα στους χρήστες του ιατρικού δικτύου μέσω ενός καταλόγου X.500. Τα πιστοποιητικά επίσης θα πρέπει να διαφυλάσσονται σε ένα ασφαλή χώρο αποθήκευσης (repository) και σε εφεδρικό

αντίγραφο, για την περίπτωση που πρέπει να ανακτηθούν λόγω βλάβης του καταλόγου.

4.6. Ακύρωση πιστοποιητικών επαγγελματιών υγείας

Μετά την πάροδο της ημερομηνίας λήξης των πιστοποιητικών, η αυθεντικότητα της πληροφορίας παύει να καθίσταται έγκυρη. Υπάρχει η πιθανότητα πολλές φορές ένα πιστοποιητικό να μην είναι έγκυρο ακόμη και αν δεν έχει παρέλθει η ημερομηνία λήξεως του. Τέτοια περίπτωση, κατά την οποία μπορεί να ανακληθεί ένα πιστοποιητικό επαγγελματία υγείας είναι αν το ιδιωτικό κλειδί χαθεί ή εκτεθεί σε κινδύνους, σε περιπτώσεις μεταβολής των στοιχείων του κατόχου του πιστοποιητικού ή οποιασδήποτε άλλης πληροφορίας. Η ανάκληση των πιστοποιητικών αυτών, αποθηκεύεται σε μια δομή δεδομένων η οποία ονομάζεται Λίστα Ανάκλησης Πιστοποιητικών(Certificate Revocation List/ CRL). Θα πρέπει να αναφερθεί ότι η λίστα ανάκλησης πιστοποιητικών, είναι μια λίστα που περιέχει τον σειριακό αριθμό των πιστοποιητικών που έχουν ανακληθεί. Η Αρχή Πιστοποίησης, είναι η αρμόδια αρχή για τη δημιουργία καθώς και τη συντήρηση της Λίστας ανάκλησης Πιστοποιητικών, τα οποία εκδίδονται από την ίδια όσον αφορά το δίκτυο τηλεματικών υπηρεσιών υγείας. Η σφραγίδα χρόνου θα πρέπει να συμπεριλαμβάνεται στις λίστες ανάκλησης πιστοποιητικών καθώς επίσης και να είναι υπογεγραμμένα από την Αρχή Πιστοποίησης του Τηλεματικού δικτύου.

4.7. "Δομή λίστας ανάκλησης πιστοποιητικών επαγγελματιών υγείας

Προτείνεται η μορφή CRL version 2 (format) για τις Λίστες Ανάκλησης των Πιστοποιητικών των επαγγελματιών υγείας. Η μορφή αυτή αντιστοιχεί στο πιστοποιητικό X.509 version 3.

Η λίστα ανάκλησης πιστοποιητικών για επαγγελματίες υγείας στο δίκτυο τηλεματικών υπηρεσιών στην υγεία περιέχει την παρακάτω πληροφορία:

- Τον αριθμό έκδοσης του CRL (version 2).
- Το όνομα του αλγόριθμου ο οποίος χρησιμοποιείται για να υπογραφεί το CRL.
- Το όνομα της οντότητας που έχει υπογράψει και εκδώσει τη CRL.
- Την ημερομηνία έκδοσης της CRL.
- Την ημερομηνία που η επόμενη CRL θα εκδοθεί.

- Τη λίστα των σειριακών αριθμών των πιστοποιητικών που ακυρώνονται. Προσδιορίζεται και η ημερομηνία που έγινε η κάθε ακύρωση.
- Το αναγνωριστικό του κλειδιού της Αρχής Πιστοποίησης του ιατρικού δικτύου, με το οποίο υπόγραψε τη CRL. Αυτό το αναγνωριστικό χρησιμοποιείται στην περίπτωση που η Αρχή Πιστοποίησης έχει πολλά κλειδιά για να υπογράφει.
- Το σημείο διανομής της CRL (issuing distribution point).

4.7.1. Συντήρηση λίστας ανάκλησης πιστοποιητικών επαγγελματιών υγείας

Θα πρέπει να διεξάγεται τακτική ενημέρωση της λίστας ανάκλησης πιστοποιητικών καθώς και των πιστοποιητικών δημόσιου κλειδιού από την Αρχή Πιστοποίησης του Τηλεματικού δικτύου, έτσι ώστε να παρέχεται η δυνατότητα στους χρήστες από τις πιο πρόσφατες πληροφορίες.

4.7.2 "Διανομή και αποθήκευση λίστας ανάκλησης πιστοποιητικών επαγγελματιών υγείας

Η έκδοση της λίστας ανάκλησης πιστοποιητικών αφενός είναι διαθέσιμη στους χρήστες του τηλεματικού δικτύου υγείας και αφετέρου παρέχεται η δυνατότητα στους χρήστες να ελέγχουν αν τα πιστοποιητικά είναι έγκυρα. Στα υπέρ της μεθόδου ανάκλησης συμπεριλαμβάνεται το γεγονός ότι οι λίστες ανάκλησης πιστοποιητικών δύνανται να διανεμηθούν με τα ίδια ακριβώς μέσα όπως και των πιστοποιητικών, όπως π.χ. μέσω μη έμπιστων επικοινωνιακών μέσων ή συστήματα εξυπηρετητών. Ένας πιθανολογούμενος κίνδυνος που ανακύπτει από τις λίστες ανάκλησης πιστοποιητικών είναι αρκετά μεγάλες. Οι χρήστες του τηλεματικού δικτύου υγείας, υπάρχει πιθανότητα να είναι χιλιάδες. Απόρροια τούτου είναι να προκληθεί πρόβλημα όσον αφορά στη μετάδοση και αποθήκευση.

4.8 Υπηρεσία Προστασίας Εμπιστευτικών Ιατρικών "Δεδομένων με χρήση USB Token

Η διασφάλιση της προστασίας των εμπιστευτικών ιατρικών δεδομένων είναι ζωτικής σημασίας στις υπηρεσίες υγείας, με απώτερο σκοπό την εξασφάλιση του απόρρητου των ευαίσθητων δεδομένων, που διέπονται από τον κώδικα δεοντολογίας και το εκάστοτε

νομικό πλαίσιο. Η χρήση ψηφιακών πιστοποιητικών σκληρής αποθήκευσης, αποτελεί έναν τρόπο διασφάλισης της προστασίας των ευαίσθητων δεδομένων. Η χρήση του USB Token αποδεικνύει την ηλεκτρονική ταυτότητα κάποιου. Επιπρόσθετα χρησιμοποιείται ως ή στη θέση, ενός κωδικού προκειμένου να αποδείξει ο πελάτης ότι είναι αυτός που ισχυρίζεται ότι είναι. Το USB Token λειτουργεί σαν ένα ηλεκτρονικό κλειδί για την πρόσβαση σε κάποια πληροφορία. Μερικά μπορεί να αποθηκεύουν κρυπτογραφικά κλειδιά, όπως ψηφιακή υπογραφή, βιομετρικά δεδομένα κ.α. Είναι σχεδιασμένα για να αποθηκεύουν με ασφάλεια την ψηφιακή ταυτότητα ενός ατόμου και συγκεκριμένα τα ψηφιακά πιστοποιητικά και κλειδιά. Όταν ο χρήστης προσπαθεί να συνδεθεί με εφαρμογές μέσω του desktop, VPN/WLAN, ή διαδικτυακή πύλη, θα πρέπει να εισάγει τον μοναδικό κωδικό PIN. Αν ο κωδικός PIN που θα εισαχθεί ταιριάζει με το PIN του USB Token τα κατάλληλα ψηφιακά διαπιστευτήρια διοχετεύονται στο δίκτυο και η πρόσβαση επιτρέπεται. Οι αριθμοί PIN που αποθηκεύονται στο Token είναι κρυπτογραφημένοι για επιπρόσθετη ασφάλεια

Ένα τέτοιο σύστημα εξασφαλίζει ότι σε ευαίσθητα ιατρικά δεδομένα έχει πρόσβαση μόνο ο αρμόδιος χρήστης τη σωστή στιγμή, στην κατάλληλη μορφή και στο σωστό πλαίσιο(Sengupta,2012).

ΚΕΦΑΛΑΙΟ 5
Ασφάλεια Δεδομένων

5.1 Βασικές Αρχές Ασφαλείας

Η όλο και μεγαλύτερη χρήση των πληροφοριακών συστημάτων με σκοπό την αποθήκευση, επεξεργασία και μετάδοση ψηφιακής πληροφορίας γίνεται συνεχώς όλο και πιο αναγκαία. Η πληροφορία από μόνη της δεν είναι τίποτα, αλλά μέσα σε ένα πληροφοριακό σύστημα είναι ένα αντικείμενο ζωτικής σημασίας όπως το οξυγόνο για τον άνθρωπο. Για το λόγο αυτό είναι αρκετά σημαντικό και ευαίσθητο, η προστασία αυτής της πληροφορίας. Η πληροφορία διατίθεται σε πολλές μορφές όπως έντυπη ή χειρόγραφη, σε ηλεκτρονική μορφή, αποθηκευμένη σε συστήματα υπολογιστών ή διακινούμενη σε διαφόρων ειδών δίκτυα, μέσω ηλεκτρονικού ταχυδρομείου ακόμη και με χρήση προφορικού λόγου.

Οι 3 βασικές ιδέες(Perrin,2008) οι οποίες είναι απαραίτητες για την ορθή λειτουργία ενός πληροφοριακού συστήματος είναι οι παρακάτω:

Ακεραιότητα (Integrity): Στην ασφάλεια των πληροφοριών, η ακεραιότητα των δεδομένων σημαίνει διατήρηση και διασφάλιση. Αυτό σημαίνει ότι τα δεδομένα δεν μπορούν να τροποποιηθούν, να γίνουν αφαιρέσεις ή προσθήκες από άτομα που δεν είναι εξουσιοδοτημένα καθώς και να αποτραπεί η πρόσβαση ή χρήση από άτομα που δεν έχουν άδεια(Boritz,2011).

Διαθεσιμότητα (Availability): Οι πληροφορίες θα πρέπει να είναι διαθέσιμες, όποτε απαιτείται η χρήση τους. Αυτό σημαίνει ότι τα πληροφοριακά συστήματα που χρησιμοποιούνται για την αποθήκευση και την επεξεργασία των πληροφοριών, οι έλεγχοι ασφαλείας που χρησιμοποιούνται για την προστασία των πληροφοριών και τα κανάλια επικοινωνίας που χρησιμοποιούνται για την πρόσβαση σε αυτές θα πρέπει να λειτουργούν ορθά. Τα συστήματα υψηλής διαθεσιμότητας έχουν ως στόχο να είναι διαθέσιμα οποιαδήποτε στιγμή, να προλαμβάνουν διαταραχές των παρεχόμενων υπηρεσιών καθώς και την αναβάθμιση του συστήματος. Η διασφάλιση της διαθεσιμότητας περιλαμβάνει και την πρόληψη επίθεσης άρνησης υπηρεσιών, π.χ. μεγάλος όγκος εισερχόμενων μηνυμάτων στο σύστημα στόχο, με σκοπό να τεθούν εκτός λειτουργίας οι στοχευμένοι πόροι, είτε προσωρινά είτε μόνιμα(Loukas,2009,2010).

Εμπιστευτικότητα (Confidentiality):Στην εμπιστευτικότητα οι πληροφορίες δεν αποκαλύπτονται σε άτομα που δεν είναι εξουσιοδοτημένα. Από αιώνες είναι γνωστό στην ανθρωπότητα ότι η πληροφορία αποτελεί δύναμη, και στην εποχή μας που είναι η εποχή της πληροφορίας, η πρόσβαση σε αυτή είναι πιο σημαντική από ποτέ. Η μη επιτρεπόμενη πρόσβαση σε εμπιστευτικές πληροφορίες μπορεί να έχει καταστρεπτικές συνέπειες όχι μόνο σε εφαρμογές εθνικής ασφάλειας, αλλά και στο εμπόριο και τη βιομηχανία. Οι κύριοι μηχανισμοί προστασίας της εμπιστευτικότητας στα πληροφοριακά συστήματα είναι η κρυπτογραφία και οι έλεγχοι πρόσβασης(Boritz,2011).

5.2 Κίνδυνοι ηλεκτρονικών συναλλαγών

Προκειμένου να εστιάσουμε στους κινδύνους που απειλούν τις ηλεκτρονικές συναλλαγές καλό είναι να ορισθεί τι είναι κίνδυνος.

«Κίνδυνος, είναι κάθε απειλή που σκοπό έχει να βλάψει την ακεραιότητα των ηλεκτρονικών συναλλαγών και να εκμεταλλευτεί οποιαδήποτε πληροφορία, που μπορεί να αποκομίσει παραβιάζοντας την ιδιωτικότητα τους».

Οι κίνδυνοι λοιπόν που ελλοχεύουν κατά τη διάρκεια των ηλεκτρονικών συναλλαγών είναι:

- Η υποκλοπή δεδομένων, δηλαδή η αποκάλυψη πληροφοριών. Το γεγονός αυτό, συμβαίνει όταν ο χρήστης καταφέρνει να υποκλέψει δεδομένα που μεταδίδονται σε μια διαδικτυακή επικοινωνία.

  Ενδεχόμενη ζημία: Η παράνομη υποκλοπή μπορεί να προξενήσει βλάβη, τόσο ως παραβίαση ιδιωτικής ζωής των ατόμων όσο και ως μέσω εκμετάλλευσης των δεδομένων που έχουν υποκλαπεί, όπως συναισθηματικών ή στοιχείων από πιστωτικές κάρτες για εμπορικό κέρδος ή δολιοφθορά.
- Η καταστροφή/μαζική αλλοίωση δεδομένων, δηλαδή όταν ο χρήστης τροποποιεί ή πλαστογραφεί δεδομένα, καθώς και όταν εισάγει παραποιημένα και πλαστά δεδομένα σε μεταδιδόμενα μηνύματα.
- Οι απάτες (ψεύτικες συναλλαγές), η περίπτωση όπου κάποιος έχει μπει στο σύστημα κάποιου ηλεκτρονικού καταστήματος και έχει γράψει στοιχεία για ανύπαρκτες συναλλαγές ή τροποποιεί τη διεύθυνση παράδοσης κάποιας παραγγελίας, με σκοπό το προϊόν να πάει αλλού.

- Η άρνηση παροχής υπηρεσίας, όταν ένας χρήστης ενεργεί με σκοπό να αποτρέψει τη διάθεση πόρων και υπηρεσιών προς νόμιμους χρήστες. Στα δικτυακά περιβάλλοντα, είναι συνηθισμένη η παρεμπόδιση της μετάδοσης πληροφοριών, είτε με τη μετατροπή τους, είτε με τη καθυστέρηση τους. Επιπλέον, η κατανάλωση, κλοπή και καταστροφή των πόρων είναι και αυτά παραδείγματα κινδύνων αυτού του είδους.

  Ενδεχόμενη ζημία: Είναι επιθέσεις που έχουν σαν στόχο να προκαλέσουν προβλήματα στη λειτουργία του συστήματος ή του δικτύου που πλήττουν ώστε να το εμποδίσουν να προσφέρει τις υπηρεσίες για τις οποίες είναι προορισμένο στους νόμιμους χρήστες του.
- Η μεταμφίεση, όταν ένας χρήστης υποκρίνεται ότι είναι κάποιος άλλος προκειμένου να έχει εξουσιοδοτήσεις τέτοιες ώστε να μπορεί να κλέψει πληροφορίες ή να εκμεταλλευτεί υπηρεσίες ή να εκκινήσει συναλλαγές που προκαλούν οικονομικές απώλειες ή δυσχέρειες σε οργανισμό.

  Ενδεχόμενη ζημία: Η παραπλάνηση ατόμων φορέων, είναι επιζήμια κατά διαφορετικούς τρόπους. Οι πελάτες ενδέχεται να τηλεφορτώσουν κακόβουλο λογισμικό, από δικτυακό τόπο που παρουσιάζεται ως έμπιστη πηγή. Ενδέχεται να δοθούν εμπιστευτικές πληροφορίες σε λάθος άτομα. Η παραπλάνηση, είναι δυνατόν να οδηγήσει σε άρνηση αναγνώρισης ηλεκτρονικών συμβάσεων και άλλα. Η μεγαλύτερη ίσως ζημιά είναι το γεγονός, ότι η έλλειψη επαλήθευσης ταυτότητας αποτρέπει δυνητική πελατεία.
- Η κατάχρηση, δηλαδή η χρήση πληροφοριακών αγαθών αλλά και των υπολοίπων πόρων για διαφορετικούς σκοπούς από τους προκαθορισμένους, είναι γεγονός που προκαλεί άρνηση εξυπηρέτησης, αύξηση κόστους λειτουργίας και δυσφήμηση.
- Μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές και δίκτυα υπολογιστών (hacking, cracking). Η μη εξουσιοδοτημένη πρόσβαση σε έναν υπολογιστή ή σε ένα δίκτυο υπολογιστών πραγματοποιείται συνήθως κακόβουλα με την πρόθεση αντιγραφής, τροποποίησης ή καταστροφής δεδομένων (παρείσφρηση).

  Ενδεχόμενη ζημία: ενώ η εξουσιοδοτημένη παρείσφρηση αρχίζει ως μια διαδικασία παρενόχλησης, αναδεικνύει τα τρωτά σημεία των δικτύων

πληροφοριών και παρακινεί άτομα με εγκληματική ή δόλια πρόθεση να εκμεταλλευτούν αυτές τις αδυναμίες.

- Τα Spyware, είναι μικρά προγράμματα που μπαίνουν στον ηλεκτρονικό υπολογιστή χωρίς να το καταλαβαίνουμε και στέλνουν πληροφορίες στον αποστολέα τους σχετικά με το λειτουργικό μας σύστημα.
- Οι Dialers, είναι προγράμματα που χρησιμοποιούν την τηλεφωνική γραμμή για να καλέσουν ένα τηλεφωνικό αριθμό, που δημιουργεί υψηλότερα κόστη (για παράδειγμα 090), ώστε να πληρωθεί η εταιρία για τις υπηρεσίες που προσφέρει από εμάς.
- Το Phising, με τον όρο phising δεν χαρακτηρίζεται κάποιο πρόγραμμα, αλλά η προσπάθεια ορισμένων να εκμαιεύσουν κρίσιμα δεδομένα (όπως είναι οι αριθμοί πιστωτικών καρτών, password κ.λ.π..), προσποιούμενοι ότι είναι κάποιος φορέας, που το υποψήφιο θύμα τους εμπιστεύεται (Τράπεζες, εταιρείες τηλεφωνίας κ.λ.π.).
- Τα αυτόνομα κακόβουλα προγράμματα, όπως οι Ιοί, τα Σκουλήκια και οι Δούρειοι Ίπποι (Trojan horses). Τα συγκεκριμένα αποτελούν την μεγαλύτερη απειλή.

5.3. Λύσεις που διασφαλίζουν τις ηλεκτρονικές μας συναλλαγές στο διαδίκτυο

Ένα σύστημα ασφαλείας έχει ως σκοπό την παρεμπόδιση κάποιου να αποσπάσει ή να καταστρέψει δεδομένα που υπάρχουν σε ένα δίκτυο. Παρά το γεγονός αυτό αρκετοί χρήστες βρίσκουν τρόπους προκειμένου να εκμαιεύσουν πληροφορίες ακόμα και αν αυτές είναι απόρρητες. Οι πιο πιθανές λύσεις για την διασφάλιση των ηλεκτρονικών συναλλαγών στο διαδίκτυο είναι :

- Κρυπτογράφηση (cryptography): Η κρυπτογραφία είναι η επιστήμη που χρησιμοποιεί τα μαθηματικά για την κρυπτογράφηση και αποκρυπτογράφηση δεδομένων. Μέσω της κρυπτογράφησης παρέχεται η δυνατότητα αποθήκευσης ή μετάδοσης ευαίσθητων πληροφοριών καθώς και η διασφάλιση της εμπιστευτικότητας τους. Μέσω της κρυπτογράφησης η πρόσβαση στις πληροφορίες γίνεται από τον αποδέκτη και όχι από τον οποιονδήποτε(Mollin,2006).

- Περιλήψεις μηνυμάτων και ψηφιακές υπογραφές (message digest & digital signatures): Συντελούν στην ακεραιότητα των δεδομένων, διότι παρέχουν τη δυνατότητα εντοπισμού παραποίησης και ανάκτησης δεδομένων. Σαφώς με τη βοήθεια της κρυπτογράφησης.
- Ψηφιακά πιστοποιητικά (certificates): Τα ψηφιακά πιστοποιητικά αποτελούν βασικό συστατικό στην παροχή ασφαλών δεδομένων επικοινωνίας. Παρέχουν ένα μηχανισμό για τον έλεγχο της ταυτότητας και την ασφάλεια των πληροφοριών στα ανοικτά δίκτυα. Οι εφαρμογές που κάνουν χρήση του μηχανισμού αυτού περιλαμβάνουν την ασφάλεια του ηλεκτρονικού ταχυδρομείου, την ασφαλή διαδικτυακή επικοινωνία, την ψηφιακή υπογραφή αρχείων λογισμικού, έλεγχο της ταυτότητας της έξυπνης κάρτας και την κρυπτογράφηση συστημάτων αρχείων. Αποτελούν βασικό δομικό στοιχείο για την παροχή υπηρεσιών ασφαλείας στο πλαίσιο μιας υποδομής που αναφέρεται ως υποδομή δημόσιου κλειδιού(Public Key Infrastructure (PKI)(Brien, 2008).
- Αναγνώριση και πιστοποίηση (identification & authentication): Η αναγνώριση παρέχει στον χρήστη ταυτότητα στο σύστημα ασφαλείας. Αυτή η ταυτότητα είναι συνήθως υπό την μορφή ενός αναγνωριστικού χρήστη. Το σύστημα ασφαλείας αναζητά και αναγνωρίζει τη συγκεκριμένη ταυτότητα του χρήστη και γίνεται ταυτοποίηση. Η πιστοποίηση είναι η διαδικασία επικύρωσης της ταυτότητας του χρήστη. Προκειμένου ο χρήστης να αποκτήσει δικαιώματα και άδειες θα πρέπει να παρέχει αποδεικτικά στοιχεία για να αποδείξει την ταυτότητα του στο σύστημα, δηλαδή να γίνει εξακρίβωση και επαλήθευση των δηλωθέντων στοιχείων(Todorov, 2007).
- Έλεγχος προσπέλασης και εξουσιοδοτήσεις (access control & authorizations): Ο έλεγχος προσπέλασης είναι απαραίτητο και ζωτικής σημασίας στοιχείο για την ασφάλεια σε οποιαδήποτε εφαρμογή. Μια διαδικτυακή εφαρμογή θα πρέπει να προστατεύει δεδομένα και πόρους μέσω της εφαρμογής των περιορισμών ελέγχου πρόσβασης για το τι μπορούν να κάνουν οι χρήστες, σε ποιες πηγές θα έχουν πρόσβαση και ποιες ενέργειες τους επιτρέπονται να εκτελούν στα δεδομένα. Σε ιδανικές περιπτώσεις ένα σύστημα ελέγχου πρόσβασης θα πρέπει να προστατεύει

έναντι της μη επιτρεπόμενης ανάγνωσης, τροποποίησης ή αντιγραφής των δεδομένων.

Η εξουσιοδότηση και ο έλεγχος πρόσβασης είναι όροι που συχνά χρησιμοποιούνται λανθασμένα. Η εξουσιοδότηση αφορά στον έλεγχο για το αν ένας χρήστης έχει την κατάλληλη άδεια πρόσβασης σε κάποιο συγκεκριμένο αρχείο ή να εκτελέσει μια συγκεκριμένη δράση, με την προϋπόθεση ότι ο χρήστης έχει επιτυχώς ταυτοποιηθεί(Baier,2011).

- Επίβλεψη και υπευθυνότητα (auditing & accountability): Γίνεται καταγραφή των δηλώσεων ταυτότητας καθώς και των ενεργειών των χρηστών που έχουν πρόσβαση σε προστατευόμενους πόρους.
- Ελέγχου και αποδοτικότητας του δικτύου (efficiency controls): προκειμένου να αποτραπούν καταστάσεις άρνησης εξυπηρέτησης, γίνεται χρήση μηχανισμών μέσω των οποίων γίνεται καταγραφή και παρακολούθηση τόσο της απόδοσης τους συστήματος όσο και της διαδικτυακής κίνησης.
- Υποστήριξης συνεργασίας των υπηρεσιών ασφαλείας που προσφέρονται από εφαρμογές: Η έννοια υποστήριξης ενός βασικού πλαισίου συνεργασίας ασφαλών εφαρμογών, προωθείται μέσω τεχνολογιών Generic Security Service API, Generic Cryptographic Service API και Generic Audit Service API.
- Antivirus: Η χρήση αντιϊκών προγραμμάτων θεωρείται από τους κυριότερους τρόπους προστασίας του λογισμικού. Ο εντοπισμός ιών και άλλων κακόβουλων απειλών προλαμβάνονται και ως εκ τούτου προστατεύεται το λογισμικό σύστημα.
- SSL και IPsec: Τα IP Security(IPsec) και Secure Socket Layer (SSL) αποτελούν τα πιο ισχυρά διαθέσιμα εργαλεία για την προστασία της επικοινωνίας στο διαδίκτυο. Η IPsec επιτρέπει την αποστολή και λήψη προστατευμένων κρυπτογραφικών πακέτων οποιουδήποτε είδους (TCP, UDP, ICMP) χωρίς τροποποίηση. Το πρωτόκολλο SSL, αποτελεί χρήσιμο βήμα για τη διασφάλιση ορισμένου επίπεδου τήρησης του απορρήτου. Χρησιμοποιείται κυρίως για την προστασία των HTTP συναλλαγών αλλά και για άλλους σκοπούς όπως IMAP, POP3 κ.λ.π.(Alshamsi,2005).
- Firewalls: Το τείχος προστασίας είναι ένα σύστημα ασφαλείας του δικτύου που ελέγχει την εισερχόμενη και εξερχόμενη κίνηση και βασίζεται σε ένα εφαρμόσιμο

σύνολο κανόνων. Το τείχος προστασίας δημιουργεί εμπόδιο ανάμεσα σε ένα αξιόπιστο ασφαλές εσωτερικό δίκτυο και σε ένα άλλο δίκτυο που θεωρείται ότι δεν είναι ασφαλές και αξιόπιστο. Ωστόσο λόγω του ότι υπάρχει περιορισμένη προστασία θα πρέπει να συμπληρώνεται και από άλλους ελέγχους ασφαλείας όπως η αναγνώριση επίθεσης, η ανίχνευση παρείσφρησης και οι έλεγχοι στο επίπεδο εφαρμογής(Oppliger,1997).

ΚΕΦΑΛΑΙΟ 6
ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ - SMART CARDS

6.1 Ιστορία της Ανάπτυξης των έξυπνων καρτών

Οι έξυπνες κάρτες ανάγονται στα τέλη της δεκαετίας του 1968, όταν η χρήση πλαστικών καρτών με μικροτσίπ αναπτύχθηκε για πρώτη φορά από τους γερμανούς εφευρέτες Jurgen Dethloff και Helmut Grotrupp. Δυο χρόνια αργότερα, το 1970, ο Ιάπωνας εφευρέτης Kunitaka Arimura, ανέπτυξε μια παρόμοια εφαρμογή. Η υλοποίηση της τεχνολογίας των έξυπνων καρτών ανάγεται στον ανεξάρτητο εφευρέτη και ερευνητή από τη Γαλλία Roland Moreno το 1974. Με τις πατέντες του, οι βιομηχανίες ημιαγωγών μπορούσαν να κατασκευάζουν και να προμηθεύουν τα ολοκληρωμένα κυκλώματα σε μια λογική τιμή. Η πρώτη πιλοτική δοκιμή πραγματοποιήθηκε με επιτυχία από τις γαλλικές ταχυδρομικές και τηλεπικοινωνιακές υπηρεσίες, με τη χρήση τηλεφωνικών καρτών το 1984. Η Γερμανία διεξήγαγε δοκιμές στη χρήση τηλεφωνικών καρτών τρία χρόνια αργότερα. Η χρήση των έξυπνων καρτών στην οικονομική βιομηχανία, όπως παραδείγματος χάριν οι τραπεζικές κάρτες, είχε πιο αργή πρόοδο λόγω της πολυπλοκότητας και των υφιστάμενων υποδομών των τραπεζικών συστημάτων. Ο θεσμός της έξυπνης κάρτας άρχισε να λαμβάνεται υπόψη από τις ενώσεις τραπεζών μετά τις εξελίξεις των τελευταίων ετών στην τεχνολογία της σύγχρονης κρυπτογράφησης, η οποία παρείχε στις έξυπνες κάρτες υψηλό βαθμό ασφαλείας. Άλλες βιομηχανίες, όπως η υγεία, η εκπαίδευση, το λιανικό εμπόριο, οι τηλεπικοινωνίες και οι μεταφορές κάνουν χρήση των έξυπνων καρτών ως μέρος μιας συνολικής λύσης. Καθώς προχωρούμε στον 21^{ο} αιώνα η χρήση της έξυπνης κάρτας θα έχει ένα πιο κυρίαρχο ρόλο στο ηλεκτρονικό επιχειρείν(Ferrari et al, 1998).

6.2 Εφαρμογές των smart cards στην Υγεία

Τα συστήματα αυτοματισμού στα νοσοκομεία και ιατρικά κέντρα εξυπηρετούν τον σκοπό της παροχής ενός αποτελεσματικού περιβάλλοντος εργασίας για τους επαγγελματίες υγείας. Η άμεση πρόσβαση σε ακριβή δεδομένα υγείας είναι μια από τις κύριες λειτουργίες των συστημάτων αυτών. Τα συστήματα αυτά περιέχουν ένα δίκτυο πληροφοριών επεξεργασίας και αποθήκευσης δεδομένων του ασθενούς. Οι πληροφορίες που αφορούν τον ασθενή μπορεί να ληφθούν από πολλές πηγές όπως π.χ. τον ίδιο τον ασθενή, αποτελέσματα εξετάσεων που σχετίζονται με τον ασθενή, ιατρικές γνωματεύσεις ή παλαιότερες αποθηκευμένες πληροφορίες(Tunali,2002). Επιπρόσθετα με τη διάγνωση των συμπτωμάτων , είναι πολύ σημαντικό ο ιατρός να μπορέσει να ανακτήσει πληροφορίες από το ιστορικό του ασθενούς κατά τη διάρκεια της κλινικής εξέτασης. Ο πιο συνηθισμένος τρόπος ανάκτησης των δεδομένων του ασθενούς είναι η σύνδεση με τη βάση δεδομένων του νοσηλευτικού ιδρύματος. Σε μερικές περιπτώσεις, η ταυτόχρονη πρόσβαση στη βάση δεδομένων από διαφορετικά τερματικά που βρίσκονται εντός ιατρείων, είναι δυνατό να προκαλέσουν προβλήματα στην απόδοση λειτουργίας λόγω του μεγάλου όγκου δεδομένων. Σε άλλες περιπτώσεις τα δεδομένα των ασθενών μπορεί να χρειαστούν σε μέρος που δεν υπάρχει δικτυακή σύνδεση(π.χ. μέσα στο ασθενοφόρο) ή σε άλλο νοσηλευτικό ίδρυμα όπου ο ασθενής δεν έχει αριθμό μητρώου. Τέτοιου είδους προβλήματα μπορούν να επιλυθούν αυξάνοντας τη δυνατότητα των αυτόματων συστημάτων κάνοντας χρήση μηχανισμών αποθήκευσης και ανάκτησης. Τα φορητά μέσα κατέχουν ρόλο κλειδί στο να εναλλάσσουν περιορισμό αριθμό συγκεκριμένων πληροφοριών, τα οποία με τη σειρά τους μπορούν να προσδώσουν ένα σημαντικό αριθμό δεδομένων στο αυτοματοποιημένο σύστημα του νοσηλευτικού ιδρύματος(Pagetti,2001). Τα μέσα αυτά θα πρέπει ο ασθενής να τα μεταφέρει μαζί του πάντα και να είναι διαθέσιμα όταν του ζητηθεί.

Τα μέσα που θα χρησιμοποιηθούν για τον σκοπό αυτό θα πρέπει να είναι φθηνά, ευκολόχρηστα, να μεταφέρονται εύκολα, να μην καταστρέφονται εύκολα και να αναβαθμίζονται. Η έξυπνη κάρτα φαντάζει ως το πιο κατάλληλο μέσο για να χρησιμοποιηθεί στα συστήματα υγείας, όταν λαμβάνονται υπόψη τέτοιες απαιτήσεις. Οι έξυπνες κάρτες μπορούν να περιγραφούν ως φορητές ενσωματωμένες συσκευές που αποθηκεύουν και επεξεργάζονται δεδομένα. Αυτοί οι μικροσκοπικοί υπολογιστές έχουν

ευρεία χρήση, ιδίως στον τομέα των τηλεπικοινωνιών και στα συστήματα των μέσων μαζικής μεταφοράς(Chen,2000). Η ταχύτητα, η ασφάλεια και η φορητότητα αναγάγουν τις έξυπνες κάρτες σε ένα δυνητικό εργαλείο για τα συστήματα υγείας. Πολλές χώρες εφαρμόζουν ή συνεχίζουν να αναπτύσσουν τέτοια συστήματα, συμπεριλαμβανομένων και των έξυπνων καρτών. Οι Ηνωμένες Πολιτείες Αμερικής άργησαν να υιοθετήσουν την τεχνολογία των έξυπνων καρτών, αφού οι επιχειρήσεις έχουν ήδη επενδύσει σε μεγάλο βαθμό στην τεχνολογία καρτών μαγνητικής λωρίδας που χρησιμοποιούνται στις πιστωτικές κάρτες(Anderson,1997). Ωστόσο, όπως και σε άλλους τομείς, η χρήση της έξυπνης κάρτας στην υγεία έχει αρχίσει να γίνεται δημοφιλής και σε αυτή τη χώρα(Health Smart Card).

6.3 Ηλεκτρονικός Ιατρικός Φάκελος

Στην Αμερική χρησιμοποιείται ο όρος computer-based patient record κι αφορά στη διαχείριση της ιατρικής πληροφορίας, με δυνατότητα άμεσης πρόσβασης σε ακριβή στοιχεία του φακέλου, τη σύνδεση με προγράμματα επιβοήθησης της διάγνωσης και τη χρήση πηγών γνώσης που θα βοηθήσουν στη κλινική εκτίμηση κι αντιμετώπιση του ασθενή.

Στην Ευρώπη χρησιμοποιείται πλέον ο όρος Φάκελος Υγείας του Πολίτη (citizen health record), τονίζοντας την αλλαγή θεώρησης του ασθενή ως πολίτη, ο οποίος χαρακτηρίζεται ως καταναλωτής των υπηρεσιών υγείας, οι οποίες έχουν κύριο άξονά τους την πρόληψη και διακρίνονται για την ηλεκτρονική μηχανογράφηση του ιατρικού φακέλου. Ο ηλεκτρονικός ιατρικός φάκελος διακρίνεται για την καταγραφή και συντήρηση των στοιχείων του ασθενή, τη διασφάλιση της ιδιωτικότητας κι απορρήτου των ιατρικών πληροφοριών, την ασφαλή μεταφορά κι επεξεργασία του ιατρικού δεδομένου από άλλους ιατρούς σε οποιοδήποτε μέρος κι αν βρίσκονται και, τέλος, την διαθεσιμότητα όλων των δυνατών μορφών αρχείων για την υποστήριξη και την εισαγωγή πολλών τύπων δεδομένων(Kay,1996, Tange,1995, Tang, 1994).

6.4 Ιστορική Αναδρομή

Η έννοια της ηλεκτρονικής αποθήκευσης των ιατρικών πληροφοριών του ασθενούς αντί της καταγραφής τους σε χαρτί δεν είναι κάτι νέο. Η ιδέα του Ηλεκτρονικού φακέλου

ξεκίνησε το 1969 από τον Dr. William Edward Hammond II ως το *μέρος* όπου αποθηκεύονται για πάντα όλες οι πληροφορίες για έναν ασθενή, προσφέροντας του έτσι τις καλύτερες υπηρεσίες, παρέχοντας δηλαδή τη δυνατότητα της γνώσης κάθε λεπτομέρειας του ιστορικού του ασθενή (εξετάσεις, διαγνώσεις, φάρμακα κ.λ.π.) και συνεπώς τη συνολική αντίληψη των προβλημάτων υγείας. Στη δεκαετία του 1960, καθώς η ιατρική περίθαλψη έγινε πιο περίπλοκη, οι γιατροί συνειδητοποίησαν ότι σε ορισμένες περιπτώσεις το πλήρες ιστορικό υγείας του ασθενούς δεν ήταν προσβάσιμα σε αυτούς. Η διαθεσιμότητα της συνολικής ιατρικής πληροφορίας όταν χρειάζεται έφερε την καινοτομία για την αποθήκευση των πληροφοριών του ασθενούς ηλεκτρονικά. Η βελτίωση της ιατρικής περίθαλψης των ασθενών ήταν και είναι ο καταλύτης του ηλεκτρονικού φακέλου..

Η Κλινική Μάγιο στο Ρότσεστερ της Μινεσότα, και το ιατρικό κέντρο του Βέρμοντ ήταν μερικές από τις κλινικές που χρησιμοποίησαν ένα το ηλεκτρονικό ιατρικό αρχείο. Τα συστήματα τους αναπτύχθηκαν στις αρχές της δεκαετίας του 1960. Κατά τη διάρκεια των επόμενων δύο δεκαετιών, περισσότερες πληροφορίες και λειτουργίες προστέθηκαν στο ηλεκτρονικό ιατρικό σύστημα καταγραφής, προκειμένου να βελτιωθεί η φροντίδα των ασθενών. Δοσολογίες φαρμάκων, παρενέργειες, αλλεργίες, και αλληλεπιδράσεις φαρμάκων ήταν διαθέσιμα ηλεκτρονικά στους γιατρούς, δίνοντας τη δυνατότητα η πληροφορία να ενσωματωθεί στα ηλεκτρονικά συστήματα υγειονομικής περίθαλψης. Η ηλεκτρονική διάγνωση και το πλάνο θεραπείας, τα οποία παρείχαν στους γιατρούς πληροφορίες για τη φροντίδα του ασθενούς, πολλαπλασιάστηκαν και εντάχθηκαν στα ηλεκτρονικά ιατρικά αρχεία. Πολλά ακαδημαϊκά και ερευνητικά ινστιτούτα ανέπτυξαν τα δικά τους συστήματα ιατρικών αρχείων καθώς και εργαλεία για τη θεραπεία του ασθενούς. Συνολικά, η αξιοποίηση και ανάπτυξη αυτών των μοντέλων ηλεκτρονικών υπολογιστών ήταν να αυξηθεί η ποιότητα της φροντίδας του ασθενούς.

6.5 Ο ηλεκτρονικός ιατρικός φάκελος στην Ελλάδα

Η εφαρμογή της πληροφορικής στην Ελλάδα αναπτύχθηκε με πολύ αργούς ρυθμούς. Στα τέλη της δεκαετίας του 1980 η χρήση της άρχισε να βρίσκει εφαρμογή στα νοσηλευτικά ιδρύματα των μεγάλων αστικών κέντρων, κυρίως στον οικονομικό τομέα. Ο θεσμός του

τμήματος πληροφορικής δεν υφίσταται στους περισσότερους οργανισμούς ή όπου υπήρχε το εξειδικευμένο προσωπικό δεν επαρκούσε.

Η ανάπτυξη των τοπικών δικτύων στη δεκαετία 1990-2000 παρέχουν τη δυνατότητα διασύνδεσης, επικοινωνίας καθώς και την ανταλλαγή πληροφοριών σε απομακρυσμένους υπολογιστές, ενώ σε παράλληλη βάση αναπτύσσονται οι βάσεις δεδομένων. Αρχικά οι βάσεις δεδομένων χρησίμευαν απλά στην αυτοματοποίηση μιας υπάρχουσας εργασίας, ενώ οι εργαζόμενοι εκπαιδεύονταν στην εισαγωγή δεδομένων στο νέο σύστημα, χωρίς να γνωρίζουν τον τρόπο λειτουργίας, αφού οι χρησιμοποιούμενοι αλγόριθμοι θεωρούνταν πολύ δύσκολοι. Παράλληλα δεν υπήρχαν ενιαίες βάσεις διαχειριστικών δεδομένων, με συνέπεια κάθε νοσοκομείο να επιλέγει εφαρμογές χωρίς σχεδιασμό αποφεύγοντας τον άμεσο ανασχεδιασμό ζητημάτων οργάνωσης, κατευθύνοντας την νοσοκομειακή διαχείριση σε μια οργανωτική «μαύρη τρύπα», ενώ ελάχιστη σημασία δόθηκε στην συλλογή και ηλεκτρονική καταγραφή των κλινικών δεδομένων ή στην έρευνα για τη δομή του ιατρικού φακέλου.

Ακόμα και σήμερα στα περισσότερα νοσηλευτικά ιδρύματα της χώρας μας, οι ιατρικοί φάκελοι εξακολουθούν να είναι χειρόγραφοι, να καταλαμβάνουν μεγάλο χώρο, δεν ανευρίσκονται εύκολα, πολλές φορές χάνονται και υφίστανται φθορές και αλλοιώσεις. Η αναζήτηση ιστορικών και κλινικών δεδομένων είναι πολύ δύσκολη, ενώ η εξαγωγή στατιστικών συμπερασμάτων εντελώς αβέβαιη και πολύπλοκη. Ακόμα και στις ελάχιστες περιπτώσεις που υπάρχει ατομικός ηλεκτρονικός φάκελος, τα περιεχόμενα δεδομένα δεν μπορούν να επικοινωνήσουν ακόμα και με το εσωτερικό δίκτυο του ιδίου νοσοκομείου, με κυριότερη αιτία το ότι ο ηλεκτρονικός φάκελος και το πληροφοριακό διαχειριστικό σύστημα δεν έχουν ούτε την κατάλληλη διασύνδεση ούτε την απαραίτητη διαλειτουργικότητα (Hendrickson et al,1992).

6.7 Κωδικοποίηση της ιατρικής πληροφορίας

Τα πρότυπα για την κωδικοποίηση μιας πληροφορίας μπορεί να είναι είτε «τεχνικά» για να εξασφαλίζουν την ανταλλαγή στοιχείων μεταξύ των υπολογιστών (πρότυπα επικοινωνίας), είτε «σημασιολογικά» (πρότυπα κωδικοποίησης και αναγνώρισης) που πρέπει να εξασφαλίζουν για παράδειγμα ότι «το άσθμα» σε ένα πληροφοριακό σύστημα δεν μεταφράζεται με «βρογχίτιδα» σε ένα άλλο.

Έχει πολύ μεγάλη σημασία ο βαθμός τελειότητας και ακρίβειας της κωδικοποίησης της ιατρικής πληροφορίας, αφού η διαφοροποίηση μπορεί να αντανακλά σε πραγματικές διαφορές ποιότητας. Μέτριας ποιότητας κωδικοποιήσεις μπορεί να μην ανταποκρίνονται στην εγκυρότητα, αφού περιορίζουν την ικανότητα ορθών εκτιμήσεων από τα διαχειριστικά δεδομένα. Το πόσο έγκυρη είναι μια κωδικοποίηση δεν επιδέχεται μια τόσο σαφή απάντηση της απόλυτης κατάφασης ή απόρριψης. Ο τρόπος κωδικοποίησης δεν θα πρέπει απλά να κάνει τα δεδομένα χρήσιμα για περιγραφικούς σκοπούς, αλλά θα πρέπει να διερευνάται σε μεγαλύτερο βάθος με στόχο την αξιοποίηση κλινικών και οικονομικών πληροφοριών. Είναι πιθανό ότι οι νοσοκομειακοί γιατροί μπορεί να χρησιμοποιούν ίδιες λέξεις για διαφορετικές έννοιες, ακόμη και αν έχουν την ίδια ειδικότητα.

Απαιτείται συνεπώς περαιτέρω έρευνα που θα καθορίσει τις περιοχές στις οποίες οι περισσότεροι γιατροί συμφωνούν σχετικά με την έννοια των όρων για τις διαγνώσεις. Απαιτείται μια κοινή γλώσσα ιατρικής ορολογίας τόσο σε επίπεδο κωδικοποίησης όσο και σε επίπεδο ονοματολογίας, έτσι ώστε να αποδίδεται *αξιοπιστία* και *ποιότητα* στην παραγόμενη ιατρική πληροφορία.

Η αξιοπιστία κατά Krippendorff παράγεται μέσω της σταθερότητας, ικανότητας αναπαραγωγής και ακρίβειας, ενώ η ποιότητα με την συνέπεια των δεδομένων, δηλαδή σωστή απόδοση των όρων έτσι ώστε να επιτρέπεται η ανάκτηση των δεδομένων με έναν συνεπή τρόπο(Krippendorff,1980).

6.8 Θέματα ασφαλείας ιατρικών δεδομένων

Στις μέρες μας η ιατρική περίθαλψη βασίζεται σε μεγάλο βαθμό στη διαχείριση ψηφιακής πληροφορίας. Οι πρόσφατες εξελίξεις στις τεχνολογίες πληροφορικής και επικοινωνιών παρέχουν νέους τρόπους πρόσβασης, διαχείρισης και μετάδοσης ιατρικών εικόνων και φακέλων, αυξάνοντας όμως παράλληλα τον κίνδυνο σε ότι αφορά την ασφάλεια της διακινούμενης και κατανεμημένης πληροφορίας.

Η συμβολή του ηλεκτρονικού ιατρικού φακέλου στην παροχή ποιοτικής φροντίδας υγείας, στην μείωση του κόστους των υπηρεσιών υγείας, στην αύξηση της αποδοτικότητας των επαγγελματιών υγείας συντελεί στην αναγνώριση της αξίας του και στην πλήρη εφαρμογή του σε περιβάλλοντα υγειονομικής περίθαλψης. Η

αυτοματοποίηση όλων των διαδικασιών που συμβάλλουν στην παροχή υπηρεσιών υγείας, στη λήψη κρίσιμων αποφάσεων για την ζωή του ασθενούς, στην εκπαίδευση και στην έρευνα, καθιστά επιτακτική την ανάγκη ασφάλειας των συστημάτων ηλεκτρονικών φακέλων προκειμένου να εξασφαλίζεται η εγκυρότητα, η αξιοπιστία, η διαθεσιμότητα των πληροφοριών φροντίδας υγείας αλλά και το δικαίωμα του ασθενούς στην τήρηση του απορρήτου των προσωπικών ευαίσθητων δεδομένων.

Ο ηλεκτρονικός φάκελος ασθενούς είναι μια εξελισσόμενη ιδέα προσδιοριζόμενη ως μια μακροπρόθεσμη συλλογή πληροφοριών φροντίδας υγείας για τους ασθενείς. Είναι ξεκάθαρο ότι το δικαίωμα του ασθενούς για διασφάλιση της εμπιστευτικότητας των προσωπικών του δεδομένων δεν μπορεί να υποβιβασθεί εξαιτίας της χρήσης του ηλεκτρονικού φακέλου υγείας. Ο καθορισμός ηθικών και νομικών διαδικασιών και κριτηρίων όσο αφορά στην ηλεκτρονική συλλογή, επεξεργασία και διακίνηση των προσωπικών ευαίσθητων δεδομένων ασθενών από τους επαγγελματίες υγείας είναι απαραίτητος, αφού τυχόν αποκάλυψή τους θέτει σε κίνδυνο την σχέση τόσο του επαγγελματία υγείας - ασθενή, όσο και των μελών ολόκληρης της κοινωνίας αφού είναι πιθανό από τον φόβο αποκάλυψης τους, ο ασθενής να μην εμπιστευθεί κρίσιμες πληροφορίες που αφορούν όχι μόνο την υγεία του αλλά και την δημόσια υγεία.

Αποτελεί πλέον συνήθη πρακτική, η μετάδοση και αποθήκευση ιατρικών δεδομένων όχι μόνο στα πλαίσια ενός τοπικού δικτύου νοσοκομείου, αλλά και μεταξύ διαφορετικών μονάδων περίθαλψης μέσω ανοικτών μη ασφαλών συνδέσεων δικτύων. Είναι φανερή επομένως η ανάγκη υιοθέτησης πρόσθετων μέτρων και πρωτοκόλλων ασφαλείας στα σύγχρονα ιατρικά πληροφοριακά συστήματα. Οι βασικές απαιτήσεις που προκύπτουν ως προς την ασφάλεια των ιατρικών δεδομένων αποτυπώνονται σε κανονισμούς που έχουν θεσπιστεί σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο. Στις επόμενες ενότητες του κεφαλαίου, παρουσιάζονται τα πρότυπα και οι οδηγίες που αφορούν τη διαχείριση και αποθήκευση των ιατρικών δεδομένων και περιγράφονται οι βασικές απαιτήσεις ασφάλειας ως προς τη διαχείριση της παραγόμενης και διακινούμενης πληροφορίας σε συστήματα υπηρεσιών υγείας.

Τα δεδομένα σχετικά με την κατάσταση υγείας του ατόμου αποτελούν μέρος της προσωπικότητας του ατόμου και όχι ιδιοκτησία του φορέα που τα συλλέγει και τα επεξεργάζεται. Έτσι η επεξεργασία των δεδομένων πρέπει να συνάδει με τις σχετικές

διατάξεις για την προστασία των προσωπικών ευαίσθητων δεδομένων και του ιατρικού απορρήτου.

6.9 Βασικές απαιτήσεις ασφαλείας της ιατρικής πληροφορίας

Το εκάστοτε νομοθετικό πλαίσιο ορίζει τα δικαιώματα των πολιτών καθώς και τη διασφάλιση των ευαίσθητων προσωπικών δεδομένων επιβάλλοντας μια σειρά μέτρων ασφαλείας για τον έλεγχο πρόσβασης στην ιατρική πληροφορία, την προστασία της από τυχαία ή εσκεμμένη διαρροή σε μη εξουσιοδοτημένα άτομα και την αποφυγή μη εγκεκριμένης τροποποίησης, καταστροφής ή απώλειας.

Παρακάτω παρουσιάζονται οι βασικές απαιτήσεις ασφάλειας στα ιατρικά πληροφοριακά συστήματα:

Αναγνώριση και αυθεντικοποίηση: Ως αναγνώριση εννοείται η διαδικασία που επιτρέπει την αποδοχή της ταυτότητας μιας οντότητας από ένα πληροφοριακό σύστημα. Η αυθεντικοποίηση είναι η διαδικασία της δημιουργίας ή επιβεβαίωσης των ισχυρισμών που προκύπτουν αν είναι αληθινοί και αυθεντικοί. Η αυθεντικοποίηση της πληροφορίας μπορεί να δημιουργήσει ιδιαίτερα προβλήματα και συχνά εφαρμόζεται με την αναγνώριση ταυτότητας. Τα περισσότερα πρωτόκολλα κρυπτογράφησης περιλαμβάνουν μια μορφή ταυτότητας τελικού σημείου προκειμένου να αποτρέψουν τις man-in-the-middle επιθέσεις. Για παράδειγμα η Transport Layer Security και ο προκάτοχός της Secure Sockets Layer, είναι πρωτόκολλα κρυπτογράφησης που παρέχουν ασφάλεια στις επικοινωνίες μέσω δικτύων όπως είναι το διαδίκτυο. Διάφορες εκδοχές των πρωτοκόλλων έχουν ευρεία χρήση σε εφαρμογές όπως η περιήγηση στο διαδίκτυο, το ηλεκτρονικό ταχυδρομείο κ.α. Τα πρωτοκόλλα αυτά μπορεί να χρησιμοποιηθούν για τον έλεγχο της ταυτότητας του διακομιστή κάνοντας χρήση μια αμοιβαία έμπιστη αρχή πιστοποίησης. Σε ένα σύστημα υγείας, η πληροφορία της υγείας που από τους παρόχους και τις ταυτότητες των πελατών θα πρέπει να επαληθεύεται στην έναρξη της κάθε πρόσβασης(Zhang,2010).

Μη αποποίηση ευθύνης αποστολής/λήψης πληροφορίας: Συνεπάγεται την πρόθεση κάποιου να εκπληρώσει τις υποχρεώσεις του σε μια δέσμευση. Επιπρόσθετα συνεπάγεται ότι ένα μέρος μιας συναλλαγής δεν μπορεί να αρνηθεί τη συμμετοχή σε μια συναλλαγή, τόσο ο αποδέκτης όσο και ο αποστολέας. Το ηλεκτρονικό εμπόριο

χρησιμοποιεί τεχνολογία όπως είναι οι ψηφιακές υπογραφές και η κρυπτογράφηση για να καθιερώσει την αυθεντικότητα και την μη αποποίηση της ευθύνης(Zhang,2010).

Απόδειξη χρόνου αποστολής – λήψης πληροφορίας: Η απόδειξη του χρόνου αποστολής- λήψης μιας πληροφορίας δύναται να είναι πολύ κρίσιμη κυρίως κατά την έκδοση εργαστηριακών εξετάσεων. Για το λόγο αυτό θα πρέπει να αποδεικνύεται τόσο για τον αποστολέα όσο και για τον παραλήπτη. Μέσω της απαιτήσεως αυτής εξασφαλίζεται και η μοναδικότητα της διακινούμενης πληροφορίας(Zhang,2010).

Διαθεσιμότητα και χρησιμότητα: Για να εξυπηρετηθεί ο σκοπός του κάθε συστήματος ηλεκτρονικού φακέλου του ασθενή, η πληροφορία θα πρέπει να είναι διαθέσιμή όταν αυτή είναι αναγκαία. Αυτό σημαίνει ότι τα συστήματα πληροφορικής που χρησιμοποιούνται για την αποθήκευση και επεξεργασία των δεδομένων των ηλεκτρονικών φακέλων, οι έλεγχοι ασφαλείας που χρησιμοποιούνται για την προστασία και οι δίαυλοι επικοινωνίας που χρησιμοποιούνται για την πρόσβαση θα πρέπει να λειτουργούν ορθά. Τα συστήματα υψηλής διαθεσιμότητας έχουν ως στόχο να παραμένουν διαθέσιμα ανά πάσα στιγμή, εμποδίζοντας τη διαταραχή των υπηρεσιών λόγω διακοπών ρεύματος, ανεπάρκειες του υλικού και αναβαθμίσεις του συστήματος. Η διασφάλιση της διαθεσιμότητας περιλαμβάνει επίσης την πρόληψη από επιθέσεις άρνησης υπηρεσίας και τη διατήρηση της χρησιμότητας των δεδομένων του ηλεκτρονικού φακέλου. Η χρησιμότητα εδώ αναφέρεται στην ικανότητα διατήρησης της δυνατότητας χρήσης των δεδομένων του ηλεκτρονικού φακέλου μετά την επιβολή της ασφάλειας και προστασίας της ιδιωτικότητας(Zhang,2010).

Υπευθυνότητα: Ως υπευθυνότητα ορίζεται «η διασφάλιση ότι οι πράξεις μιας οντότητας μπορούν να αποδοθούν μοναδικά στην οντότητα αυτή». Κρίνεται απαραίτητη η καταγραφή όλων των δράσεων, με σκοπό την εύκολη ανίχνευση των μερών που εμπλέκονται έτσι ώστε να αποδοθούν οι ευθύνες. Ο βαθμός σημαντικότητας των άνωθι απαιτήσεων είναι μεταβαλλόμενος ανάλογα με το σκοπό και τη χρήση του αντίστοιχου πληροφοριακού συστήματος. Παραδείγματος χάριν η διαθεσιμότητα αποτελεί την πρωταρχική απαίτηση ασφαλείας στη λειτουργία των Μ.Ε.Θ. ενώ αντιθέτως σε ένα σύστημα ψυχολογικής υποστήριξης ασθενών η εμπιστευτικότητα των ευαίσθητων προσωπικών δεδομένων είναι πιο σημαντική. Έτσι, σε κάθε περίπτωση θα πρέπει να

εξετάζονται οι ειδικές απαιτήσεις ασφάλειας και να λαμβάνονται τα κατάλληλα μέτρα(Zhang,2010).

6.10 Παραβίαση της ηλεκτρονικής ασφάλειας σε Νοσοκομεία

Η πληροφορία που συνδέεται με ένα σύστημα Ιατρικής Φροντίδας είναι ιδιαίτερα ευαίσθητη και για το λόγο αυτό η ασφάλεια κατέχει τον κυρίαρχο ρόλο όσον αφορά το χειρισμό της. Η αποτελεσματική θωράκιση ενός συστήματος κρίνεται ζωτικής σημασίας, προκειμένου να αποφευχθούν απειλές, όπως π.χ. η παραβίαση της ηλεκτρονικής ασφάλειας.

Ένα περιστατικό που καταγράφηκε το καλοκαίρι του 2000, αφορούσε την παραβίαση του συστήματος του Ιατρικού κέντρου του πανεπιστημίου της Ουάσιγκτον, όπου χάκερ απέκτησε πρόσβαση σε ευαίσθητα δεδομένα αρκετών πελατών. Σύμφωνα με τα λεγόμενα του χάκερ, στόχος της παραβίασης αυτής ήταν να αποδείξει την ευκολία με την οποία μπορεί να παραβιαστεί ένα σύστημα ασφαλείας και βέβαια οι ελλείψεις που υπάρχουν στην ασφάλεια των ευαίσθητων δεδομένων. Το εγχείρημα αυτό από τον χάκερ έγινε μετά από συζήτηση που είχε με έναν συμφοιτητή του για το γεγονός αν τα ευαίσθητα δεδομένα και κυρίως το ιατρικό απόρρητο προστατεύονται επαρκώς. Αξίζει να αναφερθεί ότι το νοσηλευτικό ίδρυμα έλαβε την δέκατη τρίτη θέση με τα καλύτερα νοσοκομεία στις Η.Π.Α.

Το παραπάνω γεγονός καταδεικνύει το πόσο εύκολα μπορεί να παραβιαστεί ένα σύστημα ασφαλείας και συγκεκριμένα τα συστήματα που περιέχουν πληροφορίες με ευαίσθητα δεδομένα τα οποία θα μπορούσαν να έχουν τροποποιηθεί από τον εισβολέα. Παρόμοιο περιστατικό αναφέρεται και το έτος 1998 στην ιατρική βάση δεδομένων του Υπουργείου Άμυνας των Ηνωμένων Πολιτειών, όπου χάκερς παραβίασαν τη βάση δεδομένων και άλλαξαν τις ομάδες αίματος των ασθενών.

ΚΕΦΑΛΑΙΟ 7

Πληροφοριακά συστήματα υγείας διεθνώς

7.1 Αυστρία

Το Δεκέμβριο του 2012 η Αυστρία εισήγαγε τον Ηλεκτρονικό φάκελο. Οι διατάξεις αποτελούν τη νομική βάση για ένα Εθνικό Σύστημα Ηλεκτρονικού φακέλου, βασιζόμενο σε εθνικό ενδιαφέρον σύμφωνα με το άρθρο 8(4) της οδηγίας για την προστασία των δεδομένων 95/46/ΕΚ. Το Αυστριακό άρθρο για τον Ηλεκτρονικό Φάκελο επιδιώκει μια προσέγγιση προκειμένου να εναρμονίσει τα συμφερόντα των θεμάτων της δημόσιας υγείας και της ιδιωτικής ζωής. Δοκιμές διεξάγονται σε τρεις περιοχές και το σύστημα θα είναι σε πλήρη λειτουργία έως το 2017. Η εφαρμογή του νέου συστήματος έχει ακολουθήσει μια σειρά άλλων ελέγχων και πιλοτικών προγραμμάτων. Μια ανεξάρτητη επιστημονική μελέτη που διεξήχθη στην Αυστρία για τον Ηλεκτρονικό φάκελο, παρουσιάστηκε το 2012. Σκοπός της πιλοτικής μελέτης «e-Medikation» ήταν η παροχή υποστήριξης σε ιατρούς σχετικά με την ηλεκτρονική συνταγογράφηση με τέτοιο τρόπο ώστε να συμβάλλει σημαντικά στην ασφάλεια των ασθενών. Καθόλη τη διάρκεια της πιλοτικής μελέτης συμμετείχαν 5341 ασθενείς, 41 γενικοί γιατροί, 31 ειδικοί, 50 φαρμακεία, 13 γενικοί γιατροί ιδιώτες και 4 νοσοκομεία. Κατά μέσο όρο, σε κάθε δεύτερη επίσκεψη ενός ασθενή στο γιατρό ή σε φαρμακοποιό, οι τελευταίοι θα λάμβαναν μήνυμα προειδοποίησης σε περίπτωση αλληλεπίδρασης με φάρμακα. Σε κάθε έκτη επίσκεψη, το σύστημα θα προειδοποιούσε με μήνυμα σε περίπτωση που τα διαστήματα ανάμεσα στις αγωγές δεν είχαν τηρηθεί. Και σε κάθε ένατη επίσκεψη, ο γιατρός και ο φαρμακοποιός θα προειδοποιούνταν για μια ενδεχόμενη διπλή συνταγογράφηση. Χάρη στην πιλοτική αξιολόγηση του προγράμματος διάφορες προσεγγίσεις για την αύξηση της ασφάλειας των ασθενών αλλά και της ελαχιστοποίησης του χρόνου που ξοδευόταν από τους γιατρούς και φαρμακοποιούς στη συνταγογράφηση, είχε προταθεί(Passarani,2013). Στην Αυστρία, η στρατηγική της ηλεκτρονικής υγείας είναι επικεντρωμένη γύρω από την εφαρμογή ΕΛΓΑ. Αυτό δεν συνεπάγεται μόνο την εφαρμογή ενός ηλεκτρονικού ιατρικού φακέλου, αλλά και την ανάπτυξη ενός πλαισίου της Τεχνολογίας των πληροφοριών και επικοινωνιών για το σύστημα υγειονομικής περίθαλψης. Ένα πρώτο βήμα προς την καθιέρωση ενός τέτοιου συστήματος έγινε το 2005, όταν

εισήχθη η Αυστριακή ηλεκτρονική κάρτα. Παρά το γεγονός ότι δεν αποθηκεύονται δεδομένα που σχετίζονται με την υγεία, αλλά διοικητικές πληροφορίες, θα πρέπει να συνδεθεί με την ηλεκτρονική υποδομή. Επιπλέον, οι υπηρεσίες ηλεκτρονικής διακυβέρνησης ξεκίνησαν σε μορφή πλατφόρμας, κάρτα του πολίτη και την ταυτοποίηση των ηλεκτρονικών υπογραφών. Ο αριθμός κοινωνικής ασφάλισης χρησιμοποιείται στα νοσηλευτικά ιδρύματα για την αναγνώριση του ασθενούς. Για την διαδικασία πρόσβασης στα δεδομένα του ΕΛΓΑ, ο κώδικος ασφαλείας της ταυτότητας συνδυάζεται με ένα σύστημα που δημιουργεί μια μοναδική, ανώνυμη ταυτότητα. Αυτό εξασφαλίζει ότι οι ηλεκτρονικές συναλλαγές είναι ασφαλείς και ανώνυμες. Εν ολίγοις, ο στόχος του ΕΛΓΑ και το αντίστοιχο σχέδιο δράσης καθορίζονται με σαφήνεια στο χρονικό αυτό σημείο. Αυτό δίνει τις κατευθυντήριες οδηγίες για την ανάπτυξη πολιτικών σχετικά με τα επόμενα βήματα που χρειάζεται να γίνουν και παρέχει διαφάνεια η οποία τελικά οδηγεί σε μεγαλύτερο βαθμό αποδοχής από τους επαγγελματίες υγείας και τους ασθενείς. Μελλοντικά μέτρα θα περιλαμβάνουν την επίλυση ζητημάτων διαλειτουργικότητας που συνδέονται με πρότυπα που αφορούν την τεχνική καθώς και την ορολογία, αλλά και περαιτέρω ανάπτυξη κανονισμών για τις ηλεκτρονικές επικοινωνίες στον τομέα της τηλεϊατρικής(Pfeiffer,2010).

7.2 Βέλγιο

Στο τέλος του 2004, η κυβέρνηση του Βελγίου δημιούργησε το BeHealth, μια πλατφόρμα για την οργάνωση και το συντονισμό «την αμοιβαία ηλεκτρονική ανταλλαγή πληροφοριών μεταξύ όλων των ενδιαφερόμενων μερών στον τομέα της υγείας. Ως δημόσιο ίδρυμα, η πλατφόρμα του BeHealth ως κύρια εντολή είχε να επιτρέπει σε αρκετά συστήματα ανταλλαγής δεδομένων υγείας να ευδοκιμήσουν σε διάφορες περιοχές της χώρας, εξασφαλίζοντας παράλληλα ότι όλοι πρόκειται να συνδεθούν. Επί του παρόντος απαγορεύεται η λειτουργία σε τοπικό επίπεδο. Το BeHealth συνδέει τους πέντε υφιστάμενους πόλους (ένας για τη Βαλλονία, ένας για τις Βρυξέλλες και τρεις για τη Φλάνδρα) μέσω του έργου “Hub-Metahub” στη Γαλλία. Για παράδειγμα τον Απρίλιο του 2012, το σύστημα υγειονομικής περίθαλψης της Βαλλονίας, το κομβικό σημείο της Βαλλονίας, συμπεριέλαβε 30000 ασθενείς, 4000 επαγγελματίες υγείας και 17

νοσοκομεία. Κατά τη διάρκεια των ετών 2011-2012, σχεδόν 900000 έγγραφα ανταλλάχθηκαν μέσω του διαδικτύου(Passarani,2013).

Το Βέλγιο έχει ήδη αναπτύξει μια καλή υποδομή για την περαιτέρω ανάπτυξη της ηλεκτρονικής υγείας. Η κυβέρνηση με νομικό πλαίσιο έχει συστήσει τα κριτήρια ποιότητας για τα πιστοποιημένα συστήματα ηλεκρονικών φακέλων που είναι σε θέση να εξάγουν μια περίληψη του ασθενούς μέσα από ένα ειδικό πρότυπο σύνταξης. Μέχρι τώρα, πάνω από το 80% των ιατρείων γενικών ιατρών είναι εξοπλισμένα με τα συστήματα αυτά, αν και η χρήση τους στα νοσηλευτικά ιδρύματα δεν έχει φτα΄σει ακόμη σε αυτό το επίπεδο. Το επόμενο βήμα θα ήταν να δημιουργηθεί πρόσβαση σε εθνικό επίπεδο στα δεδομένα των ασθενών. Η πλατφόρμα ηλεκτρονικής υγείας, η οποία βρίσκεται σε νομική ισχή από το 2008, βρίσκεται σε καλό δρόμο για την επίτευξη αυτού του στόχου, παρέχοντας υπηρεσίες εντοπισμού και δεικτών μέσω των υπηρεσιών διαδικτυακής πλατφόρμας. Η πλατφόρμα ηλεκτρονικής υγείας υποχρεούται από το νόμο να σχεδιάσει μια στρατηγική και το όραμα για την ανταλλαγή δεδομένων της ηλεκτρονικής υγείας, ηλεκτρονικών φακέλων και ηλεκτρονικής συνταγογράφησης. Η χρήση των πιστοποιημένων συστημάτων ηλεκτρονικών φακέλων επιχορηγείται από το Υπουργείο Υγείας και το Εθνικό Ινστιτούτο Ασφάλισης Υγείας. Η επέκταση της λειτουργικότητας των συστημάτων αυτών παρέχουν πλήρη πρόσβαση στον ηλεκτρονικό φάκελο. Η ταυτοποίηση και εξουσιοδότηση για την παροχή υπηρεσιών από την πλατφόρμα ηλεκτρονικής υγείας προβλέπεται να χειρίζονται μέσω των εθνικών ηλεκτρονικών καρτών που έχουν εισαχθεί από το 2009. Οι πολλαπλών χρήσεων eCards διαθέτουν λειτουργίες κρυπτογραφικών και ηλεκτρονικών υπογραφών και μπορεί να παράσχουν ταυτοποίηση για την πρόσβαση σε ένα ευρύ φάσμα ηλεκτρονικών υπηρεσιών Τα συνδυασμένα στοιχεία ενός ειδικού, νομίμως εντεταλμένου οργανισμού ηλεκτρονικής υγείας, η εξασφάλιση χρηματοδότησης και η ευρεία διείσδυση στα τυποποιημένα συστημάτων ηλεκτρονικών φακέλων μπορούν να συμβάλουν στην περαιτέρω υλοποίηση των στόχων του σχεδίου δράσης της ΕΕ στην ηλεκτρονική υγεία κατά τα επόμενα έτη(Devlies,2010).

7.3 Δανία

Από το 2003, οι ασθενείς στη Δανία είχαν πρόσβαση στον ηλεκτρονικό τους φάκελο μέσω μιας εθνικής ηλεκτρονικής πύλης υγείας ονομαζόμενη www.sundhed.dk. Η πύλη παρέχει μια κοινή υποδομή στο σύστημα υγειονομικής περίθαλψης της Δανίας που δίνει τη δυνατότητα σε όλα τα μέρη του τομέα υγείας να συνεργάζονται μεταξύ τους έχοντας ως επίκεντρο τον ασθενή. Η εθνική αυτή πύλη μεταμόρφωσε τον τομέα του εθνικού συστήματος υγείας της Δανίας από ατομοκεντρική δομή σε δομή με επίκεντρο των ασθενή. Η αλλαγή αυτή στον προσανατολισμό είχε επιτευχθεί με μια προσέγγιση που έδινε έμφαση στη βελτιστοποίηση της εργασίας, την πρόληψη ασθενειών, την έγκαιρη παρέμβαση, υποστηρίζοντας τη σωστή θεραπεία, χρησιμοποιώντας την ικανότητα του ασθενούς καθώς και τη συνεργασία με τον τομέα. Η πύλη Sundhed.dk είναι μια δημόσια, διαδικτυακή πύλη που συλλέγει και διανέμει πληροφορίες υγειονομικής περίθαλψης μεταξύ των πολιτών και των επαγγελματιών υγείας. Όλοι οι Δανοί πολίτες έχουν πρόσβαση στην πύλη αυτή, παρέχοντας τη δυνατότητα στους επαγγελματίες υγείας να επικοινωνούν και οι ασθενείς με τις οικογένειές τους να έχουν μια γενική εικόνα σωστών και ενημερωμένων πληροφοριών υγειονομικής περίθαλψης, κάνοντας τις υπηρεσίες υγείας πιο ανοικτές. Κάθε πολίτης έχει τη δική του σελίδα (διαθέσιμη μέσω ταυτοποίησης) η οποία αντανακλά την ιδιαίτερη κατάσταση του ατόμου. Ο καθένας μπορεί να βρει ακριβείς και ενημερωμένες πληροφορίες υγειονομικής περίθαλψης π.χ. προηγούμενες θεραπείες, διαγνώσεις, την αποστολή με ασφάλεια ηλεκτρονικού ταχυδρομείου στις αρχές υγειονομικής περίθαλψης, την ανανέωση συνταγογραφούμενων φαρμάκων, την ανεύρεση της συντομότερης λίστας αναμονής, την αξιολόγηση της ποιότητας των νοσηλευτικών ιδρυμάτων, την εγγραφή ως δότης οργάνων και την πρόσβαση σε τοπικά συστήματα διαχείρισης της νόσου σε εξωτερικά ιατρεία. Οι πολίτες επίσης ενθαρρύνονται να συμμετέχουν πιο ενεργά στις δικές τους θεραπείες χάρη στην ανάπτυξη υπηρεσιών για συγκεκριμένες καταστάσεις και ασθένειες όπως ο σακχαρώδης διαβήτης και υποστηρίζοντας ένα αριθμό από chat rooms όπου οι ασθενείς και οι συγγενείς τους μπορούν να μιλήσουν με άλλους πολίτες που πάσχουν από την ίδια ασθένεια καθώς επίσης και να αναζητήσουν συμβουλές από επαγγελματίες υγείας στον τομέα που τους αφορά. Επιπλέον η πύλη παρέχει στους 150000 Δανούς επαγγελματίες υγείας, καλύτερη πληροφόρηση προκειμένου να λαμβάνουν τεκμηριωμένες αποφάσεις.

Δίνοντας στους επαγγελματίες υγείας εύκολη πρόσβαση σε πρόσφατες πληροφορίες που αφορούν τον ασθενή, από τα περισσότερα νοσοκομεία και εργαστήρια στη χώρα μέσω μιας ασφαλούς πύλης, έχουν την ευκαιρία να πάρουν έγκαιρες και θεμελιωμένες αποφάσεις σε συγκεκριμένες καταστάσεις κατά τη διάρκεια της θεραπείας. Με τον τρόπο αυτό ο ασθενής θα βιώσει την αλληλεπίδραση με τα συστήματα υγειονομικής περίθαλψης. Μετά την αρχική έναρξη λειτουργίας της πύλης το 2003, τέσσερεις σημαντικές εξελίξεις έχουν λάβει χώρα, όσον αφορά τη χρήση της:

- Μια συνεχιζόμενη αύξηση της κυκλοφορίας. Κατά μέσο όρο κάθε Δανός ενήλικας επισκέπτεται περίπου 6 με 7 σελίδες της πύλης κατά τη διάρκεια του χρόνου.
- Δεν υφίσταται πλέον το χάσμα του βαθμού της χρήσης της πύλης διαφόρων ηλικιακών ομάδων. Ενώ ο πληθυσμός μεταξύ 30 και 40 ετών κάνανε την πιο εκτεταμένη χρήση, τώρα χρησιμοποιείται εξίσου από τον πληθυσμό μεταξύ 60 και 70 ετών.
- Η χρήση από τους πολίτες των προσωπικών υπηρεσιών και η πρόσβαση σε προσωπικά δεδομένα υγείας έχει αυξηθεί.
- Ενώ ο αρχικός εστιασμός ήταν να καταστήσουν χρήσιμα τα υπάρχοντα δεδομένα και να είναι προσβάσιμα στους πολίτες και στους επαγγελματίες υγείας που αναλαμβάνουν τη θεραπεία τους, τώρα δίνεται μεγαλύτερη έμφαση στο γεγονός να επιτρέπουν τους ασθενείς να συμβάλλουν στην πύλη με διαφορετικούς τρόπους(Passarani,2013).

Το σύστημα ηλεκτρονικής υγείας της Δανίας έχει δύο χαρακτηριστικά, τα οποία καθιστούν τη χώρα πρωτοπόρο στον τομέα σε σύγκριση με άλλα κράτη μέλη της ΕΕ: Πρώτον, η εφαρμογή της τεχνολογίας της πληροφορίας στον τομέα της υγείας είναι ήδη βαθιά ριζωμένη σε τοπικό ή περιφερειακό επίπεδο. Αυτό σημαίνει ότι ώριμα συστήματα είναι σε θέση όχι μόνο για την επικοινωνία μεταξύ των επαγγελματιών υγείας αλλά επίσης και για την πρόσβαση των ασθενών και τη διαχείριση των δεδομένων, το οποίο οδηγεί σε μεγάλο βαθμό εμπιστοσύνης στην τεχνολογία της υγείας. Δεύτερον, η Δανία έχει μια μακρά ιστορία στη χρηματοδότηση και την ανάπτυξη νέων εφαρμογών πληροφορικής στη διακυβέρνηση και την υγεία. Αλλά τα ώριμα τοπικά συστήματα πληροφορικής αποτελούν επίσης μια πρόκληση για το μέλλον στην εξέλιξη της

ηλεκτρονικής υγείας στη Δανία, καθώς η δημιουργία εθνικής πλατφόρμας και ο συνδυασμός διαφορετικών συστημάτων είναι ένα δύσκολο έργο. Συγκεκριμένα θα πρέπει να διασφαλιστεί η ανάπτυξη του κεντρικού server συνταγογράφησης, του ιατρικού προφίλ, της διαλειτουργικότητας και της συνοχής των συστημάτων αυτών. Εν ολίγοις, η Δανία ξεχωρίζει λόγω της: α) έγκαιρης υιοθέτησης της τεχνολογίας της πληροφορικής και της επικοινωνίας, της επικοινωνίας μέσω ηλεκτρονικών μυνημάτων μεταξύ των γενικών ιατρών, εν μέρει λόγω των μηχανισμών χρηματοδότησης και εν μέρει, λόγω της ρεαλιστικής προσέγγισης, β) τα εθνικά μητρώα, μερικά εκ των οποίων ιδρύθηκαν πριν από πολλά χρόνια γ) την εκπόνηση κοινών υπηρεσιών π.χ. το προφίλ του φαρμάκου και το ηλεκτρονικό περιοδικό, καθώς και κοινές λύσεις / έργα, όπως η εθνική δικτυακή πύλη ηλεκτρονικής υγείας (sundhed.dk), το συστήμα χρηματοδότησης και η εκτεταμένη ανάπτυξη των δεδομένων των ασθενών και η πρόσβασης στις πλατφόρμες. Αυτά τα μοναδικά χαρακτηριστικά καθιστούν το ηλεκτρονικό σύστημα υγείας της Δανίας πρωτοπόρο στην Ευρώπη και δίνει καλό παραδείγμα για τα άλλα ευρωπαϊκά κράτη μέλη(Doupi,2010).

7.4 Φινλανδία

Το Φινλαδικό σύστημα δεδομένων για τις υπηρεσίες υγείας, τα φαρμακεία και τους πολίτες ονομάζεται KanTa, το Εθνικό Αρχείο πληροφοριών υγείας. Οι υπηρεσίες περιλαμβάνουν την ηλεκτρονική συνταγογράφηση, φαρμακευτική βάση δεδομένων, πληροφορίες για την υγεία, καθώς και τα αρχεία των ασθενών. Σύμφωνα με το νόμο στην ηλεκτρονική επεξεργασία των δεδομένων των πελατών των κοινωνικών και υγειονομικών υπηρεσιών, οι δημόσιοι οργανισμοί υποχρεούνται να εισάγουν τα δεδομένα των ασθενών σε ένα εθνικό συγκεντρωτικό αρχείο. Η ανάπτυξη ενός κεντρικού αρχείου είναι υποχρεωτική για τους ιδιωτικούς οργανισμούς παροχής υγείας, εάν διαθέτουν ένα ηλεκτρονικό σύστημα για τη μακροπρόθεσμη αποθήκευση των φακέλων των ασθενών. Η ανάπτυξη κεντρικού αρχείου για της μονάδες υγείας στην Aland είναι προαιρετική. Σύμφωνα με μια αλλαγή στη νομοθεσία που ισχύει από τον Ιανουάριο του 2001, το Υπουργείο Υγείας, είναι υπεύθυνο για τη στρατηγική καθοδήγηση της ηλεκτρονικής διαχείρισης των δεδομένων που σχετίζονται με τις κοινωνικές και

υγειονομικές υπηρεσίες καθώς και στη λήψη αποφάσεων για την εκτέλεση σημαντικών έργων. Από την 1 Ιανουαρίου του 2012 το Υπουργείο Υγείας επίσης προωθεί και στηρίζει την ανάπτυξη των υπηρεσιών του συστήματος δεδομένων. Το Ίδρυμα Κοινωνικών Ασφαλίσεων της Φινλανδίας είναι επιφορτισμένο με την κατασκευή της ηλεκτρονικής συνταγογράφησης, τα αρχεία των ασθενών καθώς επίσης για τις πληροφορίες υγείας για τους πολίτες. Το κέντρο έγγραφής του πληθυσμού είναι υπεύθυνο για την υπηρεσία πιστοποίησης για την υγειονομική περίθαλψη, ενώ η Εθνική Εποπτική Αρχή για την υγεία και πρόνοια είναι υπεύθυνη για τον ρόλο και τις ιδιότητες των υπηρεσιών και της συναφούς κωδικοποίησης. Τα αρχεία των ασθενών χρησιμοποιούνται μέσω των φαρμακείων και τις υπηρεσίες υγειονομικής περίθαλψης(Passarani,2013).

Η Φινλανδία έχει εργαστεί για την ανάπτυξη και εξάπλωση της πληροφορικής στον τομέα της υγείας από τις αρχές της δεκαετίας του 1990 και έκτοτε συνεχώς ανέκυπταν ζητήματα που αφορούσαν τα κεντρικά συστήματα και τη διαλειτουργικότητα των αρχείων στην αποθήκευση δεδομένων και την πρόσβαση. Η έναρξη των ζητημάτων αυτών συνενώθηκε σε ένα γενικό σχέδιο των ηλεκτρονικών αρχείων των ασθενών, το οποίο περιλαμβάνει διαφορετικούς τύπους εφαρμογών ηλεκτρονικής υγείας και της ανάπτυξης του συστήματος. Δια του παρόντος, το τεχνικό πλαίσιο βασίζεται στην τοπική τεχνολογία της πληροφορίας της υγείας,η οποία έχει αναπτυχθεί από τους δήμους σε πρώιμο στάδιο. Η εξέλιξη αυτή, ιδιαίτερα η πρώιμη πολιτική δέσμευση και ο σχεδιασμός πάνω στα ήδη υπάρχοντα συστήματα, καθιστά τη Φινλανδία μια καλά προετοιμασμένη χώρα για οποιοδήποτε δέσμευση στην ηλεκτρονική υγεία. Τα τελευταία χρόνια, έγινε φανερό ότι τα κυριότερα εμπόδια που θα αντιμετωπίσει ή αντιμετωπίζει η Φινλανδία είναι θέματα διαλειτουργικότητας των διαφόρων τοπικών συστημάτων και το υψηλό επίπεδο της διαχείρισης και της αποκέντρωσης της λήψης αποφάσεων, καθώς αυτό οδηγεί σε επικαλυπτόμενες επενδύσεις στην τεχνολογία της πληροφορίας και στην έλλειψη ενιαίας ορολογίας. Προς το παρόν η εφαρμογή είναι σε εξέλιξη. Το σύστημα eArchiving για τα δεδομένα των πολιτών, συμπεριλαμβανομένων και των πληροφοριών υγείας και της φαρμακευτικής αγωγής, είναι το κομβικό σημείο των δεδομένων. Η Φινλανδική κυβέρνηση έχει ως στόχο να καταστήσει τη χρήση του συστήματος υποχρεωτική και δηλώνει την πλήρη εφαρμογή το 2015. Εν κατακλείδι, μπορούμε να

πούμε ότι η πλήρης ανάπτυξη του ηλεκτρονικού φακέλου των ασθενών θα μεταβάλει σημαντικά την ηλεκτρονική υγεία της Φινλανδίας και μένει να δούμε πώς οι πτυχές της αποκέντρωσης και της διαλειτουργικότητας θα παρακωλύουν την πλήρη ανάπτυξη και την ομαλή λειτουργία του συστήματος γενικότερα(Doupi,2010).

7.5 Γαλλία

Η Γαλλία έχει εφαρμόσει τον φάκελο ιατρικού προσωπικού, ο οποίος είναι προσβάσιμος στους ασθενείς μέσω υπηρεσιών του διαδικτύου και την ευθύνη των περιφερειακών οργανισμών. Προκειμένου να υπάρξει πρόσβαση στον φάκελο, ο επαγγελματίας υγείας χρειάζεται τη συγκατάθεση του ασθενούς, ο οποίος μπορεί επίσης να επιλέξει να αρνηθεί η πρόσβαση σε συγκεκριμένους επαγγελματίες υγείας. Ο φάκελος αποτέλεσε το αντικείμενο διαμάχης στη Γαλλία με προσφυγή στο συμβούλιο της Επικρατείας για να κηρυχτεί αντισυνταγματικός. Το Συμβούλιο απέρριψε το αίτημα. Επιπρόσθετα η Γαλλία έχει εφαρμόσει τον φαρμακευτικό φάκελο. Σύμφωνα με τη Γαλλική Ένωση φαρμακοποιών, περισσότεροι από 25 εκατομμύρια φαρμακευτικοί φάκελοι έχουν αναπτυχθεί και 97,6 των φαρμακείων είναι συνδεδεμένα(Passarani,2013).

Η ηλεκτρονική υγεία έχει μακριά ιστορία στη Γαλλία, αρχίζοντας από τις αρχές δεκαετίας του ενενήντα με την carte vitale έργο για τις διοικητικές διαδικασίες της υγειονομικής περίθαλψης και των πρώτων σχεδίων της τηλεϊατρικής. Η πρώτη μεγάλη ώθηση στην ηλεκτρονική υγεία, με την έννοια του σχεδίου δράσης για τν ηλεκτρονική υγεία, δόθηκε από το νόμο για τη μεταρρύθμιση της κοινωνικής ασφάλισης το 2004, η οποία έθεσε τα θεμέλια για το γαλλικό ηλεκτρονικό φάκελο. Η τηλεϊατρική στη Γαλλία, που τεκμηριώθηκε μέσω διάφορων εκθέσεων, κινείται από την πιλοτική φάση σε πιο τακτική χρήση. Η νομική και ρυθμιστική δραστηριότητα καθώς και οι αλλαγές στα συστήματα αποζημίωσης για την παροχή υπηρεσιών τηλεϊατρικής βρίσκονται υψηλά στην πολιτική ατζέντα. Ένα μέρος των νομικών και ρυθμιστικών διαμεσολαβητών είναι σε θέση να διαβεβαιώσουν ότι οι ηλεκτρονικές υπηρεσίες υγείας μπορούν να αποδοθούν ασφαλώς και με ασφάλεια. Επιρόσθετα ο κώδικας δημόσιας υγείας καθορίζει σαφώς τα δικαιώματα των ασθενών καθώς και τις λεπτομέρειες της συναίνεσης του ασθενούς. Πολύ πρόσφατα, η πρώτη υπηρεσία αντιστοίχησης για τους προμηθευτές λογισμικού,

δόθηκε στη δημοσιότητα, ενόψει της δημιουργίας του πρώτου κύματος των εθνικών αναγνωριστικών υγείας (INC-C)(Artmann,2010).

7.6 Γερμανία

Παρά το γεγονός ότι σχέδια για την καθιέρωση ενός συστήματος ηλεκτρονικού φακέλου φιλοξενούνται από το Ομοσπονδιακό Υπουργείο Υγείας για πάνω από δέκα χρόνια, εξακολουθούν να μην υπάρχουν ηλεκτρονικά μητρώα υγείας στη Γερμανία. Υπάρχει ευρεία συζήτηση σχετικά με το θέμα αλλά η πρόοδος έχει αμαυρωθεί από τις τρέχουσες συζητήσεις μεταξύ των ενδιαφερόμενων μερών, συμπεριλαμβανομένων και των πολιτικών, των ασφαλιστών, των επαγγελματιών υγείας καθώς και των εμπειρογνώμων σε θέματα προστασίας δεδομένων. Αυτό επίσης συνέβαλε στην ευρεία αντίσταση και ανησυχία για την ασφάλεια των δεδομένων στα μέσα μαζικής ενημέρωσης και στο γενικό πληθυσμό. Ωστόσο ως συμβιβαστική λύση μια βασική ηλεκτρονική κάρτα υγείας εισήχθη το 2011. Είναι διαθέσιμη στους πολίτες και έχει δυνατότητες ανάπτυξης, αλλά επί του παρόντος πληρεί μόνο περιορισμένες λειτουργίες. Δεν υπάρχει ακόμη η δυνατότητα για τους ασθενείς να παρακολουθούν τα αρχεία τους, αλλά δοκιμές βρίσκονται σε εξέλιξη για την επέκταση χρησιμότητας της κάρτας(Passarani,2013).

Η Γερμανία αποτελεί ένα χαρακτηριστικό παράδειγμα για τα πολύπλευρα προβλήματα και ζητήματα που προκύπτουν κατά την προσπάθεια εισαγωγής μιας πανεθνικής υποδομής ηλεκτρονικής υγείας σε μια αρκετά μεγάλη ομοσπονδιακά δομημένη χώρα, με πολύ διαφορετικό και πολύπλοκο σύστημα υγείας. Οι συζητήσεις για την ηλεκτρονική υγεία ξεκίνησαν στις αρχές της δεκαετίας του 1990, οι αρχικές ιδέες και σχέδια συντάχθηκαν ήδη από το 1995, το 2003 υιοθετήθηκε νόμος για τη θέσπιση της βασικής υποδομής που βασιζόταν στην ηλεκτρονική κάρτα τόσο για τους ασθενείς όσο και για τους επαγγελματίες υγείας και το 2010 η χώρα εξακολουθεί να αγωνίζεται να «κυλήσει» αυτές τις εφαρμογές σε όλους τους φορείς του συστήματος υγείας. Οι υποδομές αυτές αναμένεται στα επόμενα έτη να διευκολύνουν σε μεγάλο βαθμό την ευρεία διάδοση των προηγμένων συστημάτων ηλεκτρονικής υγείας σε όλους τους παρόχους υγειονομικής περίθαλψης και τους επαγγελματίες υγείας και να επιτρέψουν την εύκολη ανταλλαγή, ίσως ακόμη και ελεγχόμενη ασφαλή κοινή πρόσβαση στα δεδομένα των ασθενών από όλους που εμπλέκονται στη φροντίδα ενός συγκεκριμένου ατόμου(Stroetmann,2010).

7.7 Ιταλία

Το Υπουργείο Υγείας πρόσφατα εξέδωσε νέες κατευθυντήριες οδηγίες για τον ηλεκτρονικό φάκελο και τα θέματα ασφαλείας. Η ιδέα είναι να δημιουργηθεί για την ιταλική Υπηρεσία Υγείας ένα εθνικό διαδραστικό δίκτυο όπου οι παθολόγοι είναι οι πιο σημαντικοί παράγοντες. Σε περιφερειακό επίπεδο λειτουργούν πιλοτικά αρχεία ασθενών και είναι ιδιαίτερα αναπτυγμένα. Μερικά έχουν αναπτύξει πλήρως τα αρχεία ασθενών και περιλαμβάνουν διοικητικά δεδομένα και το ιατρικό ιστορικό. Σε εθνικό επίπεδο, υπάρχουν επίσης αρκετά πιλοτικά αρχεία ασθενών που είναι άρρηκτα συνδεδεμένα με το eGovernment Plan 2012. Η Ιταλία συμμετέχει επίσης στο πρόγραμμα epSOS, όπου οι ιταλικές δραστηριότητες επικεντρώνονται στη διαπεριφερειακή μεταφορά ιατρικών δεδομένων και τη δημιουργία αρχείων ασθενών καθώς επίσης και την ηλεκτρονική συνταγογράφηση(Passarani,2013).

Στην Ιταλία θα πρέπει να σημειωθεί ότι σε περιφερειακό επίπεδο η ανάπτυξη της ηλεκτρονικής υγείας έχει προχωρήσει και πολλές εφαρμογές βρίσκονται σε τελικό στάδιο πιλοτικής εφαρμογής ή είναι ήδη σε χρήση. Όλα αυτά τα συστήματα θα πρέπει να ενσωματωθούν όσον αφορά σε διάφορα θέματα: την τεχνολογική διαλειτουργικότητα, την εννιαία ορολογία καθώς και τις δομές επικοινωνίας μεταξύ των διαφόρων μονάδων υγείας. Συνολικά, οι φορείς που λαμβάνουν αποφάσεις σε εθνικό επίπεδο, προσπαθούν να μάθουν από εκτιμήσεις των πιλοτικών περιφερειακών προγραμμάτων, προκειμένου να δημιουργήσουν μια υποδομή σε εθνικό επίπεδο στους τομείς των ασθενών και της ένταξης σε ένα σύστημα ηλεκτρονικού ιατρικού φακέλου, της τηλεϊατρικής και της ηλεκτρονικής συνταγογράφησης. Μελλοντικές προκλήσεις θα περιλαμβάνουν την ευρεία αποδοχή των νέων εφαρμογών στην ηλεκτρονική υγεία σε διαφορετικά οργανωτικά επίπεδα και θεσμούς(Tamburini,2010).

7.8 Σουηδία

Στη Σουηδία υπάρχουν πολλά συστήματα καταγραφής των ασθενών αλλά δεν υπάρχει κάποιο εναρμονισμένο. Το συμβούλιο της κομητείας της Uppsala, παρέχει πρόσβαση σε 250000 πολίτες στον ηλεκτρονικό τους φάκελο. Έως τώρα υπάρχουν 20000 πραγματικοί χρήστες. Το σύστημα αναπτύχθηκε χωρίς διαβούλευση με τους ενδιαφερόμενους φορείς

σε σχέση με την εγκυρότητα των ιατρικών αρχείων και των πιθανών κινδύνων. Το συμβούλιο της πολιτείας Östergötland περιλαμβάνει περίπου 300 ασθενείς οι οποίοι είχαν πρόσβαση σε ορισμένα μέρη του ηλεκτρονικού τους φακέλου από το 2002. Μια αξιολόγηση το 2006 έδειξε ότι η πρόσβαση στον ηλεκτρονικό φάκελο συνέβαλε στην αύξηση της αλληλεπίδρασης των ασθενών με τους επαγγελματίες υγείας , παρά την έλλειψη πληροφοριών. Το πρόγραμμα επεσήμανε την ανάγκη να εξεταστούν με μεγαλύτερη προσοχή οι ειδικές ανάγκες των ευάλωτων ασθενών όπως είναι τα παιδιά ή θύματα ενδοοικογενειακής βίας(Passarani,2013).

Η Σουηδία βρίσκεται πάνω από το μέσο όρο όσον αφορά τις πτυχές αναπτυξιακής πολιτικής της υγείας. Στο μέλλον, αναμένεται πρόοδος στο τεχνολογικό επίπεδο όσον αφορά τις ηλεκτρονικές κάρτες. Εκτός από το ρόλο της παροχής βιομετρικών δεδομένων, σχεδιάζεται να ενσωματώσει ένα ηλεκτρονικό κύκλωμα στις ηλεκτρονικές κάρτες, το οποίο θα μπορεί να μεταφέρει ηλκεκτρονικές πληροφορίες, οι τόσο ονομαζόμενες υπηρεσίες ηλεκτρονικής ταυτότητας και έτσι θα αναγνωρίζεται ο κάτοχος ηλεκτρονικά.Ο στόχος που τίθεται από τη Σουηδική κυβέρνηση είναι να επιτύχει μια εθνική, διατομεακή λύση, ικανή να παρέχει ασφαλή ηλεκτρονική αναγνώριση, όταν οι ηλεκτρονικές υπηρεσίες χρησιμοποιούνται(Doupi,2010).

7.9 Ευρωπαϊκή Ένωση

7.9.1 Στρατηγική

Η Ευρωπαϊκή Ένωση προωθεί τη δημιουργία ενός "ευρωπαϊκού χώρου ηλεκτρονικής υγείας", συντονίζοντας δράσεις και διευκολύνοντας τη συνέργεια μεταξύ συναφών πολιτικών και ενδιαφερομένων φορέων με στόχο την εξεύρεση καλύτερων λύσεων, την αποφυγή του κατακερματισμού της αγοράς και τη διάδοση ορθών πρακτικών.

Για να είναι αξιόπιστες και αποδεκτές οι λύσεις στην ηλεκτρονική υγεία από τους ασθενείς και τους επαγγελματίες υγείας, είναι απαραίτητο το σύστημα να είναι ασφαλές και τα δεδομένα να είναι πλήρως προστατευμένα. Οι ασθενείς θα πρέπει να είναι υπεύθυνοι για τη δική τους υγεία, θα πρέπει να συνδέονται και να ελέγχουν. Επιλογή πρόσβαση στα δεδομένα αποτελεί θεμελιώδες δικαίωμα το οποίο είναι ενσωματωμένο στη νομοθεσία περί προστασίας των δεδομένων της Ευρωπαϊκής Ένωσης.

Θα πρέπει να παρέχονται στους ασθενείς όλες οι πληροφορίες για να δίνουν εν γνώσει τους τη συναίνεση τους, είτε πρόκειται για ανταλλαγή, ανάλυση, προσαρμογή ή κατάργηση των ιατρικών δεδομένων. Ορισμένες κατηγορίες δεδομένων προσωπικού χαρακτήρα για την υγεία, όπως η γενετική πληροφορία πρέπει να υποβληθούν σε ιδιαίτερα αυστηρούς ελέγχους πρόσβασης. Ένα σύστημα δεδομένων ή σφραγισμένοι φάκελοι θα μπορούσε να συμβάλει στη δημιουργία ενός διαφορετικού επιπέδου εμπιστευτικότητας και να περιορίσει την πρόσβαση σε ορισμένες πληροφορίες μόνο σε ορισμένους επαγγελματίες υγείας. Επιπλέον, η πρόσβαση στα αρχεία υγείας των ασθενών θα πρέπει να επιτρέπεται μόνο στους επαγγελματίες υγείας που εμπλέκονται άμεσα με την κατάσταση του ασθενούς όσον αφορά την ανάγκη επίγνωσης του βασικού ιστορικού του ασθενούς.

Οι ασθενείς θα πρέπει να έχουν τη δυνατότητα να γνωρίζουν ποιος έχει πρόσβαση στον ηλεκτρονικό τους φάκελο και να περιορίζουν την πρόσβαση, εφόσον το επιθυμούν και έχουν ενημερωθεί για τους κινδύνους ενός τέτοιου εγχειρήματος. Σε περίπτωση παραβίασης της ασφάλειας που οδηγεί σε τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση των προσωπικών δεδομένων υγείας, οι ενδιαφερόμενοι και οι εθνικές εποπτικές αρχές προστασίας των δεδομένων θα πρέπει να ενημερώνεται άμεσα. Είναι επίσης σημαντικό να ενθαρρυνθεί η ανάπτυξη των τεχνολογιών και υπηρεσιών βελτίωσης της ασφάλειας για να αποτρέψει την κλοπή ταυτότητας ή άλλων επιθέσεων παραβίασης της ιδιωτικότητας.

Η ποιότητα και η ασφάλεια της τεχνολογίας που χρησιμοποιείται, καθώς και η υπηρεσία που συνδέεται με αυτές, θα πρέπει να αξιολογηθούν προσεκτικά από τις αρμόδιες υπηρεσίες(Hoffman,2008). Η τεχνολογία θα πρέπει επίσης να εξασφαλίζει αξιόπιστη ταυτοποίηση των ασθενών και του επαγγελματία υγείας. Τα συστήματα ηλεκτρονικής υγείας θα πρέπει να είναι πλήρως ασφαλή, από τεχνική άποψη, κατά των παραβιάσεων. Η ποιότητα και η ασφάλεια των εφαρμογών της ηλεκτρονικής υγείας εξαρτάται επίσης από τις καλές υποδομές, συμπεριλαμβανομένων και των συνδέσεων στο ευρυζωνικό διαδίκτυο. Ο ηλεκτρονικός φάκελος θα πρέπει να είναι φιλικό προς το χρήστη και να έχει σχεδιαστεί για και γύρω από τις ανάγκες των χρηστών(Greenhalh,2010, Pyper,2008). Οι πληροφορίες που περιέχονται στον ηλεκτρονικό φάκελο υγείας, θα πρέπει να παρέχονται σε κατανοητή γλώσσα και με μια διάταξη που να είναι εύκολη για τα άτομα με ειδικές

ανάγκες, ηλικιωμένους κ.α. Ο ηλεκτρονικός φάκελος θα πρέπει να σχεδιάζεται με καθορισμένη δομή ή μορφή, με προκαθορισμένους όρους ή κωδικοποίηση, αλλά αυτό θα απαιτούσε σημαντικό συντονισμό και προσαρμογή των προσπαθειών από τους επαγγελματίες υγείας. Κατά την εφαρμογή ενός ηλεκτρονικού φακέλου επαρκή προσοχή πρέπει να δοθεί στις ανάγκες των ευάλωτων ομάδων όπως τα παιδιά, οι μετανάστες ή τα άτομα με ψυχικές και άλλες αναπηρίες.

Παρέχοντας στους ασθενείς πρόσθετα εργαλεία για να συμμετέχουν πιο ενεργά στις αποφάσεις που αφορούν την υγεία τους και την αύξηση της ευαισθητοποίησης σχετικά με τα οφέλη και τις ευκαιρίες της ηλεκτρονικής υγείας είναι ζωτικής σημασίας. Η εφαρμογή ενός συστήματος ηλεκτρονικού φακέλου θα πρέπει να συνοδεύεται με ενημερωτικές εκστρατείες και δράσεις κατάρτισης που θα απευθύνονται στο ευρύ κοινό και τους επαγγελματίες υγείας. Οι ασθενείς και οι επαγγελματίες υγείας πρέπει να είναι εκπαιδευμένοι σχετικά με τη φύση και το σκοπό του εξοπλισμού, με πιθανές παραβιάσεις της εμπιστευτικότητας που χαρακτηρίζουν τις τεχνολογίες που αναπτύσσονται. Από την άποψη αυτή, η γνώση πρέπει να αποκτηθεί σχετικά με το πώς να επηρεάσουν τα γνωστικά, τα σωματικά ή τα εμπόδια αναλφαβητισμού στην ροή εργασίας και την έκβαση από τη χρήση των ιατρικών φακέλων.

Με τους Ευρωπαίους να μετακινούνται όλο και περισσότερο εντός και μεταξύ των κρατών μελών της ΕΕ, η ανάπτυξη σαφών και πρακτικών προτύπων διαλειτουργικότητας είναι απαραίτητη. Επομένως, είναι επιτακτική ανάγκη να επιτραπεί η διαλειτουργικότητα μεταξύ των πληροφοριών υγείας που μοιράζεται μεταξύ διαφορετικών επαγγελματιών υγείας και μεταξύ διαφορετικών ρυθμίσεων των συστημάτων υγειονομικής περίθαλψης, αρκεί να εξασφαλίζουν επαρκές επίπεδο προστασίας των δεδομένων. Μια αλλαγή νοοτροπίας στο σύστημα διαχείρισης της υγειονομικής περίθαλψης και μεταξύ των επαγγελματιών υγείας είναι επίσης απαραίτητη: το σύστημα δεν θα πρέπει να σχεδιαστεί γύρω από τον γιατρό, το νοσοκομείο ή το ασφαλιστικό σύστημα, αλλά θα πρέπει να επικεντρώνεται στον ασθενή(Passarani,2013).

Συμπεράσματα

Ο καθορισμός των ηθικών αλλά και νομικών διαδικασιών και κριτηρίων όσο αφορά στην ηλεκτρονική συλλογή, επεξεργασία και διακίνηση προσωπικών ευαίσθητων δεδομένων σε πιθανούς δευτερεύοντες χρήστες δεδομένων υγείας, όπως είναι οι ασφαλιστικές και φαρμακευτικές εταιρείες είναι απαραίτητος. Τυχόν αποκάλυψη των δεδομένων αυτών θέτει σε κίνδυνο την σχέση επαγγελματιών υγείας – ασθενούς, αλλά και των μελών της κοινωνίας αφού είναι πιθανό από τον φόβο αποκάλυψης ο ασθενής να μην εμπιστευθεί κρίσιμες πληροφορίες που αφορούν όχι μόνο στην υγεία του αλλά και στην διατήρηση της δημόσιας υγείας.

Μέσα στο νοσοκομείο, όπου πολυάριθμες ειδικότητες και εξειδικεύσεις συνυπάρχουν, κανείς από τους συμμετέχοντες στη λειτουργία του δεν μπορεί να ικανοποιήσει τις ανάγκες του σε πληροφόρηση χωρίς την συμπληρωματική πληροφόρηση του. Ο καθένας έχει την ανάγκη να πληροφορείται και να πληροφορεί. Κάθε δυσλειτουργία στην ροή της πληροφορίας δημιουργεί έλλειμμα και περιορισμό δυνατοτήτων στην άσκηση του έργου του. Ο βαθμός και η ποιότητα της ενημέρωσης και της επικοινωνίας επιδρούν στην διαμόρφωση των σχέσεων του προσωπικού υγείας με τον ασθενή και καθορίζουν την ποιότητα της θεραπευτικής σχέσης. Οι επαγγελματίες υγείας καθώς επίσης και οι επαγγελματίες πληροφορικής υγείας είναι σημαντικό να γνωρίζουν ότι πρέπει να σέβονται την ιδιωτικότητα των ασθενών και ότι κάθε ρήγμα σε αυτή λόγω της χρήσης προσωπικών δεδομένων των ασθενών χωρίς την συγκατάθεση τους αποτελεί απειλή. Είναι ξεκάθαρο ότι το δικαίωμα του ασθενούς στη διασφάλιση της εμπιστευτικότητας των προσωπικών του δεδομένων δεν μπορεί να υποβιβασθεί από τη χρήση του ηλεκτρονικού φακέλου.

Επαγρύπνηση, συνεχής έλεγχος, ευαισθητοποίηση των χρηστών και λήψη κατάλληλων, αποδοτικών, λογικών και οικονομικά ανεκτών μέτρων είναι μερικά από τα απαραίτητα μέτρα για να διασφαλιστεί η τήρηση του ιατρονοσηλευτικού απορρήτου, να εξασφαλιστεί η εμπιστευτική χρήση των προσωπικών ευαίσθητων δεδομένων χωρίς να θίγεται η αυτονομία και η αυτοδιάθεση του ατόμου.

Η εφαρμογή πολιτικής ασφαλείας για τα πληροφοριακά συστήματα σε ένα οργανισμό όπως το νοσοκομείο αποτελεί νομική υποχρέωση για το ίδιο αφού πρέπει να ικανοποιεί τις απαιτήσεις για την προστασία των ευαίσθητων προσωπικών δεδομένων που

βρίσκονται αποθηκευμένα στο ιατρικό ηλεκτρονικό του φάκελο όπως αυτές διατυπώνονται στον Νόμο 2472 του 1997 για την «Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα». Η κατάσταση γίνεται ακόμη πιο περίπλοκη και κρίνεται η εφαρμογή της επιτακτικότερη με την συμμετοχή ανεξάρτητων οργανισμών υγείας στην ανταλλαγή ηλεκτρονικών φακέλων υγείας καθώς μέχρι τώρα η υλοποίηση παγκόσμιας πολιτικής ασφαλείας αποτελεί απλά ένα φιλόδοξο σχέδιο.

Η δημιουργία εμπιστοσύνης είναι προαπαιτούμενο για την ανάπτυξη της κοινωνίας της πληροφορίας. Οι πολίτες προτιμούν υπηρεσίες και πληροφορίες προσαρμοσμένες στις ανάγκες και τις απαιτήσεις τους, γνωρίζοντας ότι προστατεύεται το δικαίωμά τους στην ιδιωτική ζωή.

Η τεχνολογία έξυπνων καρτών έρχεται να καλύψει ένα μεγάλο κενό στη σύγχρονη υγειονομική περίθαλψη. Οι περισσότεροι ασθενείς έχουν έναν παθολόγο πρωτοβάθμιας περίθαλψης που διατηρεί το ιατρικό ιστορικό του ασθενή. Όταν ο ασθενής εξετάζεται από ειδικούς ή σε ένα νοσοκομείο θα ερωτηθεί για να συμπληρωθεί το ιατρικό ιστορικό, με προσωπικά και ασφαλιστικά στοιχεία, για λίστα φαρμάκων που του χορηγήθηκαν, αριθμούς έκτακτης ανάγκης και ούτω καθεξής. Οι γηραιότεροι ασθενείς μπορούν να μην γνωρίζουν ποιο φάρμακο λαμβάνουν, μπορεί να μην καταλαβαίνουν, ή μπορεί να μην θυμηθούν σημαντικά προβλήματα υγείας από το παρελθόν τους. 0εν είναι ασυνήθιστο για έναν ασθενή να έχει το ιατρικό ιστορικό του σε πέντε ή έξι διαφορετικά σημεία. Αυτό κάνει τη έγκαιρη συλλογή των στοιχείων σχεδόν αδύνατη. Σε περιπτώσεις επείγουσας ανάγκης, δεν υπάρχει άμεσα διαθέσιμο ιατρικό ιστορικό και πολύ σπάνια γίνονται γνωστές κρίσιμες πληροφορίες που απαιτούνται για να εξασφαλίσουν ότι ο ασθενής λαμβάνει την υψηλότερη ποιότητα παροχής υγείας. Μέσω της χρήσης των έξυπνων καρτών, οι κρίσιμες πληροφορίες τίθενται στην διάθεση των ασθενών και των επαγγελματιών υγείας αμέσως, προκειμένου να βελτιωθεί η γενική αποδοτικότητα στην υγειονομική περίθαλψη. Οι έξυπνες κάρτες μειώνουν σημαντικά την πιθανότητα του ανθρώπινου λάθους επιτρέποντας την αποθήκευση με ασφαλή, άμεσο και έγκυρο τρόπο των πρόσφατων και προηγούμενων ιατρικών εξετάσεων και πληροφοριών.

Δίχως αμφιβολία, το ιδανικό σχέδιο υποδομής είναι ένα εθνικό (ή περιφερειακό) κεντρικό δίκτυο δεδομένων, όπου όλοι οι πάροχοι υπηρεσιών υγείας και οι ασθενείς να μπορούν να ενημερώνουν και να αναθεωρούν το ιατρικό τους ιστορικό. Αυτό το όραμα

απαιτεί τεράστιες επενδύσεις, συνεργασία από όλα τα συμβαλλόμενα μέρη και αυστηρούς κανονισμούς. Τα οφέλη όμως θα ήταν τεράστια από την άποψη ανθρώπινων ζωών και πόρων. Πράγματι, οι έξυπνες κάρτες μπορούν να βοηθήσουν προς την κατεύθυνση αυτή, δημιουργώντας αξία σε κάθε βήμα.

Βιβλιογραφία

Alshamsi, A., Saito, T., (2005). A Technical Comparison of IPSec and SSL. Tokyo University of Technology.

Anderson, K., Marshall, N., Melnyk, M., Schaefer, L., (1997) Smart cards in health care industry, Manage. Technol. I.

Artmann, J., Giest, S., empirica; with the support of Jos Dumortier, (2010). EHealth Strategies. European Commission, DG Information Society and Media, ICT for Health Unit.

Baier, D., Bertocci, V., Brown, K., Densmore,S., Pace, E., Woloski, M., (2011). A guide to Claims-Based Identity and Access Control second edition. Authentication and Authorization or Services and the Web. Patterns & practices Microsoft Corporation

Barau, A., Konana, P., Whinston, A., Yin, F., (2001). Driving e-business excellence. MIT Sloan Manage Rev 43(1):36–44

Beheshti, HM., Salehi-Sangari, E., (2007). The benefits of e-business adoption: an empirical study of Swedish SMEs. Service Business 1:233–245

Boritz, J. Efrim.,(2001). "IS Practitioners' Views on Core Concepts of Information Integrity". International Journal of Accounting Information Systems. Elsevier.

Brien, O. M., Weir, RS.,G., (2008). Understanding digital certificates . Department of Computer and Information Sciences, University of Strathclyde.

Chen, Z., (2000). Java Card Technology for Smart Cards Architecture and Programmer's Guide, Addison-Wesley, MA, USA.

Chondrocoukis. G., (2004). "E-Commerce in Pharmacy – The Greek Reality", Journal of Interdisciplinary Mathematics, Vol. 7, No1, pp. 1-27.

Choudhury, S., Bhatnagar, K., and Wasim Haque, W., (2002). Public Key Infrastructure Implementation and Design. M&T Books . An imprint of Hungry Minds, Inc.

Cote, L., Vezina, M., Sabourin, V., (2005). The strategic management process in business. Ivey Bus J 1– 7.

Devlies, J., Walossek, J., Artmann, S., Giest, S., Dumortier, J., (2010). EHealth Strategies. European Commission, DG Information Society and Media, ICT for Health Unit.

Doupi, P., Renko, E., Giest, S., Dumortier, J., (2010). EHealth Strategies. European Commission, DG Information Society and Media, ICT for Health Unit.

Doupi, P., Renko, E., Hamalainem, P., Makela, M., Giest, S., Dumortier, J., (2010). EHealth Strategies. European Commission, DG Information Society and Media, ICT for Health Unit.

Evans, N., (1999). Flexibility, adaptability are key to e-business. InternetWeek, 16.

Ferguson, N., Schneier B., (2003). Practical Cryptography, Wiley, ISBN 0-471-22357-3.

Ferrari, J., Mackinnon, R., Poh, S., Yatawara, L.,(1998). Smart Cards: A Case Study. IBM Corporation, International Technical Support Organization.

Fillis, I., Johannson, U., Wagner, B., (2004). Factors impacting on e-business adoption and development in the smaller firm. Int J Entrep Behav Res 10(3):178–191

Grandon, E., Pearson, JM., (2004). Electronic commerce adoption: an empirical study of small and medium US businesses. Inf Manage 42:197–216

Greenhalgh, t., et al., (2010). Adoption,not adoption and abandonment of personal health record: case study of health Space, British Medical Journal. BMJ 2010;341:c5814 24

Health Smart Card, Health Smart Card, URL: www.healthsmartcard.net

Hendrickson, G., Anderson., RK., Clayton, PD., Cimino, J., Hripcsak, GM., Johnson, SB., et al.(1992). The integrated academic information management system at Columbia Presbyterian Medical Center. MD Comput;9:35-42

Hoffman, S., Podgurski, A., (2008). Finding a cure: the case of regulation and oversight of electronic health record systems, Harvard Journal of Law & Technology, Volume 22, Number 1.

Hu, X., Lin, Z., Zhang, H., (2003). Trust promoting seals in electronic markets: an exploratory study of their effectiveness for online sales promotion. J Promot Manage 9(1/2):163–180

Internet Usage in Europe (2006). Available at http://www.internetworldstats.com/stats4.htm

Jevons, W.S, (1874).The Principles of Science: A Treatise on Logic and Scientific Method p. 141, Macmillan & Co., London, 2nd ed. 1877, 3rd ed. 1879. Reprinted with a foreword by Ernst Nagel, Dover Publications, New York, NY, 1958.

Katz, J., Lindell, Y., (2007). Introduction to Modern Cryptography. Boca Raton London New York Washington, D.C.

Kosan, L., (2001). E-business eats up culture—firm's soft skills predict. eWeek, p. 58

Krippendorff, K., (1980). Content Analysis: An Introduction to Its Methodology. Newbury Park, C.A: Sage.

Lefebvre, LA., Lefebvre, E., Elia, E., Boeck, H., (2005). Exploring B-to-B e-commerce trajectories in manufacturing SMEs. Technovation 25:1443–1456

Loukas, G.; Oke, G. (September 2010) [August 2009]. "Protection Against Denial of Service Attacks: A Survey". Comput. J. **53** (7): 1020–1037. doi:10.1093/comjnl/bxp078

Mazzeo, M., 2012. Digital Signatures and European Laws. Security Focus.com.

Mendo, FA., Fitzgerald, G., (2005). A multidimensional framework for SME e-business progression. J Enterp Inf Manage 18(6):678–696

Menezes, A., Oorschot, P. C, Vanstone, S., (1996). Handbook of applied Cryprography.

Mollin, A. R., (2006). An Introduction to Cryptography, Second Edition (Discrete Mathematics and Its Applications). 2nd Edition.

Nanehkaran,Y.A.,(2013). An Introduction To Electronic Commerce. INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 2, ISSUE 4.

Oppliger, R.,(1997). "Internet Security: FIREWALLS and BEYOND". *Communications of the ACM* **40** (5): 94.

Pagetti, C., Mazini, C., Pierantoni, M., Gualandi, G., Schepel, H., (2001). A European Health Card Final Report, European Parliament, Directorate General for Research, Document for STOA Panel, pp. 16–29.

Passarani, I., 2013. Patient access to Electronic Health Records. Report of the eHealth Stakeholder Group.

Patton, MA., Josang, A., (2004). Technologies for trust in electronic commerce. Electron Commer Res 4:9–21

Peet, S., Brindley, C., Ritchie, B., (2002). The European Commission and SME support mechanisims for e-business. Eur Bus Rev 14(5):335–341

Perrin, Chad(2008) "The CIA Triad".

Pfeiffer, K.P., Giest, S., Dumortier, J., Artmann, J., (2010). EHealth Strategies. European Commission, DG Information Society and Media, ICT for Health Unit.

Pyper C., et Al, (2008). Patients' experiences when accessing their on-line electronic patient records in primary care, British Journal of General Practice.

Quayle, M., (2002). E:business: the challenge for UK SMEs in the twenty-first century. J Oper Prod Manage 22(10):1148–1161

Rappa, M., (2010). Business models on the web.Managing the digital enterprise. http://digitalenterprise.org/models/models.pdf

Sanderson, J.,(2004). Opportunity and constraint in business-to-business relationships: insights from strategic choice and zones of manoeuvre. Supply Chain Manage Int J 9(5):392–401.

Sarkar, C., (2002). "Infomediation: Interview with John Hagel"

Scott, A., (2013). How to create a good information security policy.

Sengupta, S., (2012). "Computer Scientists Break Security Token Key in Record Time". *New York Times*.

Shih, SC., Wen, HJ., (2005). Integrated e-enterprise security design and implementation: a case study of e-service in supply chain management. Int J Electron Bus 3(2):154–173.

Singh, S., (1999). *The Code Book*. Doubleday. pp. 279–292.

Stallings, W., (2011). Network Security Essentials: Applications and Standards. Fourth Edition. Pearson Education.

Straub, D., Klein, R., (2001). E-competitive transformations. Bus Horiz 44(3):3–12.

Stroetmann, A. K., Artmann, J., Giest, S., (2010). EHealth Strategies. European Commission, DG Information Society and Media, ICT for Health Unit.

Tamburini, S., Giest, J., Dumortier, J., Artmann, J., (2010). EHealth Strategies. European Commission, DG Information Society and Media, ICT for Health Unit.

Taylor, M., Murphy, A., (2004). SMEs and e-business. J Small Bus Enterp Dev 11(3):280–289.

Thuraisingham, B., (2005). Directions for security and privacy for semantic e-business applications. Commun ACM 48(12):71–73

Todorov, D., (2007). Mechanics of User Identification and Authentication. Fundamentals of Identity Management. Taylor & Francis Group, LLC

Tunali, T., Yildirim, S., Dalbasti, T., (2002). The use of smart cards in health care, Hermes Project Workshop, pp. 1–6.

Weidong, K., (1997). Networking Security and Standards.Kluwer Academic Publishers.

Wright B (2000) E-Business: the great IT catalyst. Manufacturing computer solutions: IT strategy issue 19–20.

Zhang, R., Liu, L., (2010). Security Models and Requirements for Healthcare Application Clouds.