ΠΑΝΕΠΙΣΤΗΜΙΟ
ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ
ΠΛΗΡΟΦΟΡΙΚΗΣ & ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

# Μελέτη Μεθόδων Ασφάλειας Ιατρικών Δεδομένων


**Του Παγωμένου Απόστολου**

**ΑΜ: 85**


**Διπλωματική Εργασία**

**Επιβλέπων Καθηγητής**

**Αγγελίδης Παντελής**

**Κοζάνη 2013**

ΠΑΝΕΠΙΣΤΗΜΙΟ
ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ
ΠΛΗΡΟΦΟΡΙΚΗΣ & ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

UOWM-ICTE-GR

# Μελέτη Μεθόδων Ασφάλειας Ιατρικών Δεδομένων

# ΠΕΡΙΛΗΨΗ

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 ασθενή 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 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 ασθενούς.

Ο κύριος σκοπός της παρούσας εργασίας ωστόσο, δεν είναι να κάνει 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.

**Λέξεις κλειδιά:** Ασφάλεια, Ιατρική Πληροφορία, Κρυπτογραφία, Ηλεκτρονική Υγεία, Πληροφοριακά Συστήματα Υγείας, Έξυπνες Κάρτες.

# ABSTRACT

The domain of healthcare has become a challenging testing ground for information security due to the complex nature of healthcare information and individual privacy. Ever since health-care 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 electronic form raises concerns about patient privacy and data security. Any attempt to introduce computerised 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.

The principal aim of the present paper is, however, not to make a new contribution to the subject of security, but rather to give an overview of current trends in the security aspects of sensitive medical data and therefore the health-care information systems.

**Key Words:** Security, Medical Information, Cryptography, e-Health, Health-Care Information Systems, Smart Cards.

# ΠΡΟΛΟΓΟΣ

Η παρούσα διπλωματική εργασία αποτελεί μια μελέτη των μεθόδων που χρησιμοποιούνται για την ασφαλεία της ιατρικής πληροφορίας καθώς και των Πληροφοριακών Συστημάτων Υγείας με στόχο την προστασία των ευαίσθητων προσωπικών - ιατρικών δεδομένων των ασφαλισμένων – ασθενών από τρίτους χρήστες.

Η παρακάτω μελέτη περιλαμβάνει πιο αναλυτικά τα εξής στοιχεία:

Στο 1ο κεφάλαιο γίνεται μια γενική αναφορά στις απαιτήσεις ασφάλειας που θα πρέπει να υπάρχουν σε ένα σύτημα-δίκτυο ανάλογα με την κρισιμότητα των δεδομένων του, στους κινδύνους που θα εμφανιστούν σε μια πιθανή “εισβολή”, καθώς επίσης και στις υπηρεσίες ασφάλειας που με τη χρήση κατάλληλων μηχανισμών ασφάλειας φροντίζουν ώστε να παρέχονται συνεχώς οι υπηρεσίες στο επίδεδο και στην ποιότητα που απαιτούνται.

Στο 2ο κεφάλαιο αναλύεται η έννοια της Κρυπτογραφίας ξεκινώντας από το παρελθόν μέχρι και σήμερα καθώς και τεχνικές κρυπτογράφησης.

Στο 3ο κεφάλαιο παρουσιάζεται αναλυτικά η υποδομή Δημόσιου Κλειδιού καθώς και η εφαρμογή της στον τομέα της Υγείας.

Σο 4ο κεφάλαιο αποτυπώνονται οι εφαρμογές της Πληροφορικής στον τομέα της Υγείας.

Στο 5ο κεφάλαιο αναλύεται η χρήση και εφαρμογή των έξυπνων καρτών στον τομέα της Υγείας.

Στο 6ο κεφάλαιο παρατίθεται το Ευρωπαϊκό και όχι μόνο Νομικό πλαίσιο που διέπει την προστασία των ιατρικών ευαίσθητων δεδομένων.

Συμπεράσματα και προτάσεις για μελλοντική έρευνα παρατίθονται ως επίλογος της εργασίας.

Στο τέλος της εργασίας  δίνονται οι πηγές και οι αναφορές της μελέτης.

# ΠΕΡΙΕΧΟΜΕΝΑ

# ΚΕΦΑΛΑΙΟ 3 – ΥΠΟΔΟΜΗ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ (PKI)

## ΚΕΦΑΛΑΙΟ 4 – ΗΛΕΚΤΡΟΝΙΚΗ ΥΓΕΙΑ (E-HEALTH)



## ΚΕΦΑΛΑΙΟ 5 – ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ (SMART CARDS)

## ΚΕΦΑΛΑΙΟ 6 - ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΙΑΤΡΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

# ΚΕΦΑΛΑΙΟ 1

# ΑΣΦΑΛΕΙΑ ΔΕΔΟΜΕΝΩΝ

## 1.1 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. Αυτό ισχύει πότε σε μικρό ή σε μεγάλο βαθμό για όλους τους οργανισμούς ανεξάρτητα από το είδος, το μέγεθος, και τον τομέα που δραστηριοποιείται ο κάθε οργανισμός. 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 οι οποίες είναι απαραίτητες για την ορθή λειτουργία ενός Π.Σ είναι οι παρακάτω:

**Ακεραιότητα (Integrity):** Η ακεραιότητα αναφέρεται στη διατήρηση των δεδομένων ενός πληροφοριακού συστήματος σε μια γνωστή κατάσταση χωρίς ανεπιθύμητες τροποποιήσεις, αφαιρέσεις ή προσθήκες από μη εξουσιοδοτημένα άτομα, καθώς και την αποτροπή της πρόσβασης ή/και χρήσης των υπολογιστών και δικτύων του συστήματος από άτομα χωρίς άδεια.

**Διαθεσιμότητα (Availability):** Η διαθεσιμότητα των δεδομένων και των υπολογιστικών πόρων είναι η εξασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα θα είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους. Μία τυπική απειλή που αντιμετωπίζουν

τα σύγχρονα πληροφοριακά συστήματα είναι η επίθεση άρνησης υπηρεσιών (DOS attack), που έχει ως σκοπό να τεθούν εκτός λειτουργίας οι στοχευμένοι πόροι, είτε προσωρινά είτε μόνιμα. Η άρνηση υπηρεσιών δεν προκαλείται αναγκαία από εχθρική επίθεση.

**Εμπιστευτικότητα (Confidentiality):** Η εμπιστευτικότητα σημαίνει ότι ευαίσθητες πληροφορίες δεν θα πρέπει να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα. Η διαρροή ευαίσθητων πληροφοριών μπορεί να γίνει με πιο παραδοσιακές μεθόδους από την ψηφιακή υποκλοπή.

Η πληροφορία λοιπόν, αποτελεί ένα επαπειλούμενο αντικείμενο και οι απειλές μπορούν να προέρχονται από πηγές είτε εσωτερικές είτε εξωτερικές. Μπορούν να είναι συμπτωματικές ή να προέρχονται από ηθελημένη κακή πρόθεση πρόκλησης ζημιών στον εκάστοτε οργανισμό. Δημιουργείται λοιπόν η ανάγκη για προστασία της κρίσιμης πληροφορίας του καθενός, καθώς και της πληροφορίας που αφορά τους πελάτες του, αναπτύσσοντας την κατάλληλη Πολιτική Ασφάλειας Πληροφοριών και λαμβάνοντας όλα τα απαραίτητα μέτρα για την υλοποίηση της.

Οι απαιτήσεις ασφάλειας του οργανισμού προκύπτουν ύστερα από καταγραφή των κινδύνων που αντιμετωπίζει ο οργανισμός. Το κόστος των μηχανισμών ασφάλειας θα πρέπει να δικαιολογείται από την πιθανή ζημιά στον οργανισμό σε περίπτωση που παραβιαστεί η ασφάλεια του.

## 1.2 Κίνδυνοι Ασφάλειας

Η αποτίμηση των κινδύνων ασφάλειας είναι μια σε βάθος εξέταση των παρακάτω παραγόντων:

1. Της πιθανής ζημιάς που θα υποστεί ο οργανισμός σε περίπτωση που προκύψει κάποιος κίνδυνος ασφάλειας, συμπεριλαμβανομένων των συνεπειών από την απώλεια της εμπιστευτικότητας, της ακεραιότητας ή της διαθεσιμότητας της πληροφορίας.

2. Της ρεαλιστικής εκτίμησης της πιθανότητας να εμφανιστεί ένας τέτοιος κίνδυνος ασφάλειας σε σχέση με τους υπάρχοντες μηχανισμούς ελέγχου.
3. Τα αποτελέσματα του προηγούμενου παράγοντα καθορίζουν τις κατάλληλες ενέργειες και προτεραιότητες που πρέπει να κάνει και να έχει ο οργανισμός, καθώς και τους τρόπους υλοποίησης των μηχανισμών ελέγχου της ασφάλειας απέναντι σε αυτούς τους κινδύνους. Η διαδικασία αποτίμησης των κινδύνων και η επιλογή των κατάλληλων μηχανισμών ελέγχου μπορεί να επαναληφθεί πολλές φορές προκειμένου να καλύψει διαφορετικά τμήματα του οργανισμού.
4. Είναι σημαντικό λοιπόν, να γίνεται σε τακτά χρονικά διαστήματα έλεγχος των κινδύνων ασφάλειας όπως και των μηχανισμών προστασίας ώστε να επιτυγχάνεται προσαρμογή στις ανάγκες και τις προτεραιότητες του οργανισμού, επέκταση στην προστασία από νέους κινδύνους, καθώς και επιβεβαίωση της ορθής και αποτελεσματικής λειτουργίας των υπαρχόντων μηχανισμών προστασίας.

## 1.3 Υπηρεσίες Ασφαλείας (Security services)

Το πρότυπο ISO 7498-2 καθορίζει μια σειρά υπηρεσιών που πρέπει να υποστηρίζονται από το δίκτυο.

Σκοπός τους είναι να εξασφαλίσουν ότι το δίκτυο θα μπορεί να παρέχει συνεχώς τις υπηρεσίες του στο επίπεδο και με την ποιότητα που απαιτούνται για να ανταποκριθεί στο σκοπό που εξυπηρετεί. Μπορούν περισσότερο να εξειδικευτούν λέγοντας ότι στοχεύουν στην αντιμετώπιση των κινδύνων της «άρνησης παροχής υπηρεσιών».

Οι κύριες υπηρεσίες ασφαλείας είναι οι εξής:

**Υπηρεσίες Αυθεντικοποίησης (Authentication service):** Παρέχουν εγγύηση για την ταυτότητα μιας οντότητας. Αυτό σημαίνει ότι όταν ισχυρίζεται κάποιος ότι έχει μια συγκεκριμένη ταυτότητα (ή αλλιώς user name), η υπηρεσία εξακρίβωσης ταυτότητας θα παρέχει τα μέσα για να επιβεβαιώσει την ορθότητα του ισχυρισμού. Υπάρχουν δύο είδη εξακρίβωσης ταυτότητας, ανάλογα με το αν εξακριβώνουμε την ταυτότητα οντότητας ή την

ταυτότητα προέλευσης δεδομένων. Κατά την *εξακρίβωση ταυτότητας προέλευσης δεδομένων (data origin authentication)* ο αποστολέας και ο νόμιμος παραλήπτης επιζητούν να επιβεβαιώνει ο ένας την ταυτότητα του άλλου, έτσι ώστε ο παραλήπτης να μπορεί να είναι σίγουρος ότι ο αποστολέας είναι πράγματι αυτός που ισχυρίζεται π.χ. εάν ο χρήστης Β λάβει ένα μήνυμα από το χρήστη Α, θα πρέπει να είναι σε θέση να πιστοποιήσει την ταυτότητα του Α και να ξέρει ότι το μήνυμα που έλαβε είναι πράγματι από αυτόν.

**Υπηρεσίες Ακεραιότητας (Integrity service):** Σκοπός τους είναι η εξασφάλιση της ακεραιότητας (integrity) ενός μηνύματος. Δηλαδή ότι το μήνυμα δεν έχει παραποιηθεί και ότι προέρχεται από το γνήσιο αποστολέα του. Επομένως, πρέπει να προστατευτούν τα δεδομένα των υπολογιστικών και επικοινωνιακών πόρων από την τροποποίηση, διαγραφή ή αντικατάσταση τους από μη εξουσιοδοτημένους χρήστες, χωρίς αυτό να γίνει αντιληπτό. Οποιοδήποτε μη εξουσιοδοτημένο άτομο δε θα πρέπει να είναι σε θέση να παραποιήσει την πληροφορία κατά τη μετάδοση της. Η ακεραιότητα δεδομένων από μόνη της δεν έχει νόημα, γιατί δεν αρκεί η πληροφορία να μην μεταβάλλεται κατά την μετάδοση της, αλλά πρέπει ταυτόχρονα και η πηγή προέλευσης της να είναι αυθεντική. Για το λόγο αυτό οι υπηρεσίες ακεραιότητας των δεδομένων πρέπει να συνδυάζονται με την εξακρίβωση ταυτότητας της πηγής προέλευσης των δεδομένων. Τα δεδομένα σε κάθε σύστημα πρέπει να παραμένουν πλήρη και ορθά.

**Υπηρεσίες μη αποποίησης ευθύνης (non-repudiation):** Σκοπός τους είναι να προστατεύουν από την άρνηση συμμετοχής μιας οντότητας σε μια σύνοδο επικοινωνίας. Επίσης, σκοπός τους είναι να εξασφαλίσουν ότι η οντότητα που έλαβε το μήνυμα να μην μπορεί να αρνηθεί ότι πράγματι το έλαβε. Με λίγα λόγια, ο αποστολέας της πληροφορίας δεν μπορεί, σε κάποια μεταγενέστερη χρονική στιγμή, να αρνηθεί την πρόθεση, τη δημιουργία και την αποστολή της πληροφορίας. Αντίστοιχα, ο παραλήπτης της πληροφορίας δεν μπορεί σε κάποια μεταγενέστερη χρονική στιγμή να αρνηθεί την παραλαβή και την επεξεργασία της πληροφορίας. Η μη αποποίηση ευθύνης μαζί με τον έλεγχο της προέλευσης των δεδομένων προστατεύει από τις προσπάθειες του αποστολέα να αρνηθεί ότι έστειλε το μήνυμα, ενώ μαζί με τον έλεγχο παράδοσης προστατεύει από προσπάθειες του παραλήπτη να αρνηθεί, ψευδώς,

την παραλαβή του μηνύματος. Ο πιο διαδεδομένος και ταυτόχρονα αποτελεσματικός τρόπος μη αποποίηση ευθύνης είναι κάνοντας χρήση των ψηφιακών υπογραφών.

**Υπηρεσίες Εμπιστευτικότητας (confidentiality):** Ο σκοπός των υπηρεσιών αυτών είναι να προστατεύσουν τα δεδομένα που διακινούνται στο δίκτυο από αποκάλυψη σε μη εξουσιοδοτημένες οντότητες. Αν δεν υπάρχει εμπιστευτικότητα παραβιάζεται το δικαίωμα των ατόμων και των εταιριών για μυστικότητα. Η εμπιστευτικότητα παίζει πρωταγωνιστικό ρόλο στο χώρο της υγείας. Η πληροφορία πρέπει να γίνεται κατανοητή μόνο από τον νόμιμο αποδέκτη της. Για κάθε άλλον η πληροφορία πρέπει να παραμένει σε ακατανόητη μορφή.

**Υπηρεσίες ελέγχου πρόσβασης:** Ο σκοπός των υπηρεσιών αυτών είναι να προστατεύσουν τους πόρους, τα αρχεία, τα δεδομένα και τις εφαρμογές του δικτύου από μη εξουσιοδοτημένη προσπέλαση. Πιθανότατα είναι οι υπηρεσίες εκείνες που έρχονται πρώτες στη σκέψη μας, όταν αναφερόμαστε σε ασφάλεια υπολογιστών ή δικτύων. Ο υπηρεσίες αυτές, που σχετίζονται πολύ στενά με την αναγνώριση χρήστη και την αυθεντικοποίηση, χρησιμοποιούνται σε δικτυακά περιβάλλοντα για να ελέγξουν τη πρόσβαση σε πόρους και υπηρεσίες του δικτύου, σε εφαρμογές και σε δεδομένα.

## 1.3 Μηχανισμοί ασφάλειας στο μοντέλο OSI

Οι υπηρεσίες ασφάλειας που περιγράψαμε πιο πάνω υλοποιούνται με ένα σύνολο μηχανισμών ασφάλειας. Οι μηχανισμοί περιγράφονται παρακάτω με λεπτομέρεια και είναι:

**Κρυπτογράφηση:** Χρησιμοποιείται για την υλοποίηση της υπηρεσίας εμπιστευτικότητας, είτε πρόκειται για δεδομένα είτε για πληροφορίες δρομολόγησης. Ο μηχανισμός ωστόσο χρησιμοποιείται και από άλλους μηχανισμούς ασφάλειας. Οι αλγόριθμοι κρυπτογράφησης είναι αντιστρέψιμοι ή μη αντιστρέψιμοι. Οι αντιστρέψιμοι αλγόριθμοι διακρίνονται σε συμμετρικούς και ασύμμετρους. Οι συμμετρικοί αλγόριθμοι χρησιμοποιούν ένα μυστικό κλειδί κρυπτογράφησης και η γνώση του κλειδιού αυτού συνεπάγεται και γνώση του επίσης μυστικού κλειδιού αποκρυπτογράφησης. Αντίθετα, οι ασύμμετροι αλγόριθμοι

κρυπτογράφησης χρησιμοποιούν ένα δημόσιο κλειδί κρυπτογράφησης, του οποίου η γνώση δε συνεπάγεται τη γνώση του ιδιωτικού κλειδιού αποκρυπτογράφησης. Οι μη αντιστρέψιμοι αλγόριθμοι κρυπτογράφησης είναι δυνατόν να μη χρησιμοποιούν κλειδί. Αν χρησιμοποιείται κλειδί, αυτό μπορεί να είναι δημόσιο ή ιδιωτικό.

**Ψηφιακές υπογραφές:** Αποδεικνύει σε κάποιον τρίτο ότι αυτός που υπογράφει, και μόνο αυτός ήταν δυνατόν να παραγάγει την υπογραφή αυτή. Ο μηχανισμός εμπεριέχει δύο διαδικασίες: τη διαδικασία υπογραφής μιας ομάδας δεδομένων και τη διαδικασία επαλήθευσης της υπογραφής που συνοδεύει μια ομάδα δεδομένων. Η διαδικασία υπογραφής χρησιμοποιεί το ιδιωτικό κλειδί του υπογράφοντα για να κρυπτογραφήσει ολόκληρη τη ομάδα δεδομένων ή μια κρυπτογραφική τιμή που παράγεται από τη ομάδα δεδομένων. Η διαδικασία επαλήθευσης χρησιμοποιεί το δημόσιο κλειδί του υπογράφοντα για να καθορίσει αν πράγματι η υπογραφή παράχθηκε από το ιδιωτικό του κλειδί.

**Έλεγχος πρόσβασης:** Οι μηχανισμοί αυτοί καθορίζουν και επιβάλλουν τα δικαιώματα πρόσβασης μιας οντότητας, χρησιμοποιώντας την αυθεντικοποιημένη ταυτότητα της οντότητας, πληροφορίες σχετικές με την οντότητα. Οι απόπειρες προσπέλασης ενός πόρου χωρίς να υπάρχει η ανάλογη εξουσιοδότηση, καθώς και οι απόπειρες προσπέλασης ενός πόρου με μη εξουσιοδοτημένο τύπο προσπέλασης, απορρίπτονται και το σχετικό γεγονός μπορεί να καταγραφεί ως ίχνος ελέγχου ασφάλειας. Οι μηχανισμοί αυτοί μπορεί να χρησιμοποιούν βάσεις πληροφοριών ελέγχου πρόσβασης, στις οποίες είναι αποθηκευμένα τα δικαιώματα πρόσβασης των οντοτήτων, πληροφορίες αυθεντικοποίησης, δυνατότητες, ετικέτες ασφάλειας, χρόνος απόπειρας πρόσβασης, διαδρομή απόπειρας πρόσβασης, διάρκεια πρόσβασης. Μηχανισμοί ελέγχου πρόσβασης μπορεί να απαιτούνται είτε στο αρχικό σημείο σύνδεσης της οντότητας είτε και σε ενδιάμεσα σημεία του διαδρόμου επικοινωνίας με το τελικό σύστημα, έτσι ώστε να είναι δυνατός ο καθορισμός του δικαιώματος πρόσβασης στην απαιτούμενη υπηρεσία επικοινωνίας και η παροχή της εξουσιοδότησης για επικοινωνία με το άλλο μέρος.

**Ακεραιότητα δεδομένων:** Οι μηχανισμοί αυτοί χρησιμοποιούνται για την εξασφάλιση της ακεραιότητας μιας και μόνο μονάδας (ή ενός πεδίου) δεδομένων ή μιας ακολουθίας μονάδων (ή πεδίων) δεδομένων. Υπάρχουν δύο διαδικασίες που καθορίζουν την ακεραιότητα μιας μόνο μονάδας δεδομένων. Η πρώτη διαδικασία εφαρμόζεται στην πηγή των δεδομένων και παράγει μια τιμή που την επισυνάπτει στη μονάδα δεδομένων. Η τιμή αυτή μπορεί να παράγεται από έναν απλό κώδικα ελέγχου δεδομένων (π.χ. CRC) ή από κάποιο αλγόριθμο κρυπτογράφησης. Η δεύτερη διαδικασία εφαρμόζεται στο δέκτη των δεδομένων και δημιουργεί την αντίστοιχη τιμή χρησιμοποιώντας τη ληφθείσα μονάδα δεδομένων. Συγκρίνοντας τις δύο τιμές, αντιλαμβανόμαστε αν υπήρξε τροποποίηση των δεδομένων κατά τη μετάδοση. Αν πρόκειται για μετάδοση δεδομένων μέσω σύνδεσης, είναι δυνατή η χρήση τεχνικών αρίθμησης σειράς, χρονοσφράγισης ή κρυπτογραφικών δεσμών. Αν πρόκειται για μετάδοση δεδομένων χωρίς σύνδεση, η χρήση χρονοσφράγισης παρέχει περιορισμένη προστασία εναντίον επιθέσεων αναμετάδοσης μεμονωμένων μονάδων δεδομένων.

**Έλεγχος δρομολόγησης:** Ο μηχανισμός αυτός καλύπτει θέματα δρομολόγησης δεδομένων σε δίκτυα. Δύο τελικά συστήματα μπορούν να επιλέξουν να συνδεθούν μέσω διαφορετικών δρομολογίων, για να εμποδίσουν την εκδήλωση επιθέσεων εναντίον τους. Πολλές φορές είναι κρίνεται αναγκαία η απαγόρευση διέλευσης δεδομένων που φέρουν συγκεκριμένες ετικέτες ασφάλειας μέσω συγκεκριμένων ζεύξεων. Τέλος, είναι επιθυμητή η χρήση προσυμφωνημένων, φυσικά ασφαλών, δικτύων για μετάδοση πληροφοριών, αντί δυναμικά καθοριζόμενων δρομολογίων.

**Αρχές Πιστοποίησης (CAs/Certification Authorities):** Παρέχει εξασφάλιση ότι τα δεδομένα που μεταδίδονται μεταξύ δύο ή περισσότερων πλευρών έχουν κάποιες ιδιότητες, π.χ. ακεραιότητα των δεδομένων, αυθεντικότητα προέλευσης και προορισμού, ορθότητα χρόνου αποστολής. Η εξασφάλιση αυτή παρέχεται από ένα τρίτο συμβαλλόμενο μέρος. Κάθε επικοινωνιακό στιγμιότυπο μπορεί να προστατεύεται χρησιμοποιώντας τους μηχανισμούς των ψηφιακών υπογραφών, της κρυπτογράφησης, της ακεραιότητας, ή οποιουσδήποτε άλλους μηχανισμούς που είναι διαθέσιμοι από τις Αρχές Πιστοποίησης.

# ΚΕΦΑΛΑΙΟ 2

# ΚΡΥΠΤΟΓΡΑΦΙΑ

## 2.1 Η εξέλιξη της Κρυπτογραφίας

Οι Diffie και Hellman, το 1975, με τη δημοσίευση της εργασίας «New Directions in Cryptography», μίλησαν για την απαρχή μιας επανάστασης στην επιστήμη της Κρυπτογραφίας. Όντως, από τότε μέχρι και σήμερα έχουν δημοσιευτεί μυριάδες επιστημονικά άρθρα. Τα θέματα που κυριαρχούν σε αυτά τα ερευνητικά άρθρα αναφέρονται στον ορισμό της ασφάλειας, στην αναζήτηση ασφαλών κρυπτογραφικών συστημάτων, σε κρυπτογραφικές δυνατότητες, όπως ψηφιακές υπογραφές και κρυπτογραφικά πρωτόκολλα, όπως μηχανισμούς γνησιότητας, ακεραιότητας, ελέγχου πρόσβασης και μη αμφισβήτησης. Η όλη εξέλιξη υποβοηθήθηκε από την επίσης ραγδαία ανάπτυξη της Πληροφορικής και των Επικοινωνιών, και ιδιαίτερα των τηλεματικών υπηρεσιών, όπως εφαρμογών ηλεκτρονικού εμπορίου και τηλεϊατρικής, που αποτελούν, ακόμα, σημαντικά κίνητρα για την περαιτέρω ανάπτυξη της Θεωρητικής και Εφαρμοσμένης Κρυπτογραφίας.

Το 1920 δημοσιεύτηκε η μονογραφία του William F. Friedman με τίτλο «The Index of Coincidence and Its Applications in Cryptography», που έτυχε μεγάλης προσοχής από την επιστημονική κοινότητα. Τη δεκαετία του 1920 κατατέθηκαν και αιτήσεις απονομής διπλωμάτων ευρεσιτεχνίας που αφορούσαν μια μηχανή ρότορα, πρώτα από τον Edward H. Hebern και αργότερα από τον Arthur Scherbius. Παραλλαγές της συσκευής αυτής χρησιμοποιήθηκαν για περίπου 50 χρόνια από στρατιωτικούς οργανισμούς. Σε αυτές συγκαταλέγεται και η συσκευή «ENIGMA», που χρησιμοποιήθηκε από τους Γερμανούς κατά το Β' Παγκόσμιο πόλεμο. Πολωνοί και Βρετανοί είχαν κατορθώσει να «σπάσουν» τους κώδικες αυτής της συσκευής.

Το 1949 ακολούθησε η δημοσίευση της εργασίας του Claude Shannon με τίτλο «The Communication Theory of Secrecy Systems». Ο Shannon σ’ αυτή την εργασία ορίζει ένα

μαθηματικό μοντέλο ασφαλών συστημάτων κρυπτογραφίας. Διακρίνει τα ανεπιφύλακτα και τα υπολογιστικά ασφαλή συστήματα και εισάγει τις τεχνικές της διάχυσης και σύγχυσης ως απαραίτητα συστατικά στοιχεία σύγχρονων κρυπτογραφικών συστημάτων. Επίσης, ορίζει με τη βοήθεια της Θεωρίας της Πληροφορίας, της οποίας θεωρείται ο θεμελιωτής, την απόσταση μοναδικότητας (unicity distance). Η απόσταση μοναδικότητας αναφέρεται στο μήκος του κωδικοποιημένου μηνύματος που απαιτείται να έχει στη διάθεσή του κάποιος που επιχειρεί να το «σπάσει», για να είναι δυνατή μια μοναδική εύλογη λύση, δηλαδή ένα μόνο μήνυμα σε εύληπτη μορφή.

Το τέλος της δεκαετίας του 1960 και η αρχή της επόμενης χαρακτηρίστηκε από την εργασία του Horst Feistel, στην IBM, πάνω στο σύστημα LUCIFER, που αποτέλεσε τη βάση του γνωστού κρυπτογραφικού συστήματος DES (Data Encryption Standard). Το σύστημα DES υιοθετήθηκε ως ομοσπονδιακό πρότυπο των ΗΠΑ για χρήση κατά την επικοινωνία μη διαβαθμισμένων (unclassified) μηνυμάτων μεταξύ κυβερνητικών υπηρεσιών. Επίσης, το Αμερικανικό Εθνικό Ινστιτούτο Τυποποίησης (American National Standards Institute) ενέκρινε αυτό και ως πρότυπο του ιδιωτικού τομέα (ANSI X3.92).

Η επόμενη αξιόλογη συμβολή παρουσιάστηκε το 1975. Τότε προτάθηκε από τους Whitfield Diffie και Martin Hellman η Κρυπτογραφία κοινόχρηστου κλειδιού. Το άρθρο – σταθμός στην εξέλιξη της Κρυπτογραφίας είχε τον τίτλο «New Directions in Cryptography».

Η πραγματική επανάσταση στην επιστήμη της κρυπτογραφίας όμως δεν είναι άλλη από την **Κβαντική κρυπτογραφία.** Η κβαντική κρυπτογραφία διαφέρει ριζικά από τα συστήματα ασφάλειας που χρησιμοποιούν τα σημερινά δίκτυα και τα οποία, παρά τις πολύπλοκες διαδικασίες στις οποίες βασίζονται, μπορούν τελικά να παραβιαστούν από όποιον έχει στα χέρια του χρόνο, χρήμα και μεγάλη υπολογιστική δύναμη. Η κβαντική κρυπτογραφία χρησιμοποιεί τους νόμους της κβαντικής φυσικής, οι οποίοι θεωρούνται εγγενώς απαραβίαστοι. Η αρχική ιδέα της κβαντικής κρυπτογραφίας ξεκίνησε πριν 25 χρόνια από τον Τσαρλς Μπένετ της IBM και τον Ζιλ Μπρασάρ του Πανεπιστημίου του Μόντρεαλ. Βασίζεται στη γνωστή κβαντική αρχή της απροσδιοριστίας του Χάιζενμπεργκ, δηλαδή στο γεγονός ότι ένας παρατηρητής δεν μπορεί να μετρήσει την κβαντική πληροφορία χωρίς να την αλλοιώσει. Η νέα τεχνολογία λειτουργεί στέλνοντας δέσμες σωματιδίων φωτονίων, οι οποίες διαταράσσονται αν κάποιος επιχειρήσει να υποκλέψει το μήνυμα. Το σύστημα

χρησιμοποιεί κλειδιά που δημιουργούνται και διανέμονται μέσω τεχνολογιών κβαντικής κρυπτογράφησης. Κάθε μεταδιδόμενο φωτόνιο μεταφέρει ένα απόλυτα μυστικό κλειδί που κωδικοποιεί τα μεταφερόμενα δεδομένα, όπως συμβαίνει στα συνηθισμένα δίκτυα ηλεκτρονικών υπολογιστών. Το πλεονέκτημα είναι ότι κανείς, πέραν από τους δύο χρήστες στο συγκεκριμένο επικοινωνιακό κανάλι, δεν μπορεί να κρυφακούσει για να μάθει το κλειδί, χωρίς να αποκαλύψει τον εαυτό του.

Στη Βιέννη παρουσιάσθηκε το καινοτόμο σύστημα από επιστήμονες του Ευρωπαϊκού προγράμματος SECOQC. Η νέα μέθοδος, που αξιοποιεί τις μυστηριώδεις κβαντικές ιδιότητες των φωτονίων, μπορεί να χρησιμοποιηθεί μελλοντικά από κυβερνητικές και στρατιωτικές υπηρεσίες, χρηματοοικονομικούς οργανισμούς και άλλες εταιρίες με δίκτυο θυγατρικών, προκειμένου να πετύχουν τον ανώτερο δυνατό βαθμό ασφάλειας στα εμπιστευτικά μηνύματά τους. Σύμφωνα με τον Αυστριακό συντονιστή του προγράμματος Κρίστιαν Μόνικ, η εμπορική αξιοποίηση της νέας μεθόδου αναμένεται τα επόμενα χρόνια. Η μετάδοση των δεδομένων, ανάμεσα σε έξι διαφορετικά κτίρια στη Βιέννη, πραγματοποιήθηκε μέσω κοινών καλωδίων οπτικών ινών.

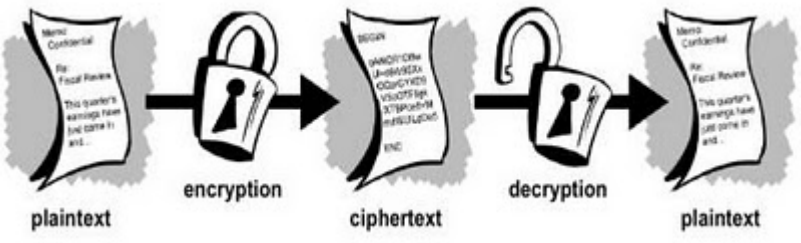
## 2.2 Η επιστήμη της Κρυπτογραφίας (Cryptography)

Η επιθυμία προστασίας του περιεχομένου μηνυμάτων οδήγησε στην επινόηση και χρήση κρυπτογραφικών τεχνικών και συστημάτων, τα οποία επιτρέπουν το μετασχηματισμό μηνυμάτων ή δεδομένων κατά τέτοιον τρόπο ώστε να είναι αδύνατη η υποκλοπή του περιεχομένου τους κατά τη μετάδοσή ή αποθήκευσή τους και βεβαίως, την αντιστροφή του μετασχηματισμού. Η ανάγκη διατήρησης της μυστικότητας μιας πληροφορίας είναι βασική και στις σύγχρονες τηλεπικοινωνίες.

Η Κρυπτογραφία είναι η επιστήμη που αποσκοπεί, χρησιμοποιώντας μαθηματικές τεχνικές, στο να εγγυηθεί την εμπιστευτικότητα, την ακεραιότητα, την αυθεντικότητα των πληροφοριών και τη μη αποποίηση ευθύνης (non-repudiation) των ηλεκτρονικών συναλλαγών. Αντίστροφα, η επιστήμη που προσπαθεί να διαβάσει κρυπτογραφημένα μηνύματα αναλύοντάς τα, λέγεται Κρυπτανάλυση. Μαζί με τον κλάδο της Κρυπτανάλυσης, που ασχολείται με τη μελέτη τρόπων παραβίασης αυτών, απαρτίζουν την Επιστήμη της

Κρυπτολογίας. Η διαδικασία μετασχηματισμού καλείται κρυπτογράφηση και η αντίστροφη της αποκρυπτογράφηση. Ο αντίστοιχος αγγλικός όρος που χρησιμοποιείται περισσότερο είναι encryption - κρυπτογράφηση, ενώ για την αντίστροφη διαδικασία, της αποκάλυψης του περιεχομένου του μηνύματος, χρησιμοποιείται η λέξη decryption - αποκρυπτογράφηση (Αν και σύμφωνα με το ISO 7498-2 πρέπει να χρησιμοποιούνται οι όροι “encipher” και “decipher”, αφού σε ορισμένους πολιτισμούς οι όροι “encrypt” και “decrypt” θεωρούνται προσβλητικοί καθώς αναφέρονται σε νεκρούς).

Η συνάρτηση ή αλλιώς το σύνολο των κανόνων, στοιχείων και βημάτων που προσδιορίζουν την κρυπτογράφηση και την αποκρυπτογράφηση καλείται κρυπτογραφικός αλγόριθμος. Η υλοποίηση του αλγόριθμου καλείται κρυπτογραφικό σύστημα.




*Σχήμα 2.1: Κρυπτογράφηση και αποκρυπτογράφηση μηνύματος.*

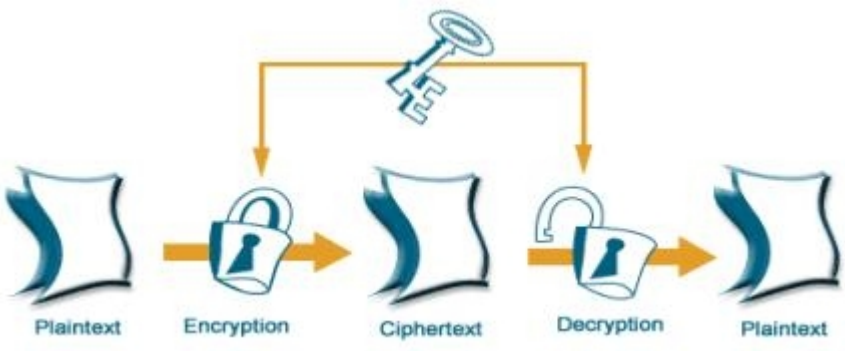
Κατά τη διαδικασία της κρυπτογράφησης, ένας κρυπτογραφικός αλγόριθμος σε συνδυασμό με ένα μυστικό κλειδί, μετατρέπει το αρχικό κατανοητό κείμενο που περιέχει την μυστική πληροφορία, το λεγόμενο απλό κείμενο (plaintext), σε κρυπτοκείμενο (cipher-text), το οποίο για τον μη νόμιμο αποδέκτη είναι ακατανόητο. Μόνο ο νόμιμος αποδέκτης του κρυπτογραφημένου μηνύματος, μπορεί να μετατρέψει το κρυπτοκείμενο σε απλό κείμενο και έτσι να ανακτήσει τη μυστική πληροφορία, μια διαδικασία που ονομάζεται αποκρυπτογράφηση. Ο μετασχηματισμός της κρυπτογράφησης παίρνει ως είσοδο εκτός από το απλό κείμενο και το κρυπτογραφικό κλειδί. Όμοια, και για την αποκρυπτογράφηση χρειάζεται το κατάλληλο κλειδί αποκρυπτογράφησης. Τα κλειδιά αυτά είναι ένας αριθμός από τυχαία ψηφία (random bit vector). Στην σύγχρονη κρυπτογραφία, η δυνατότητα να διατηρείται κρυφή η κρυπτογραφημένη πληροφορία δεν βασίζεται στον κρυπτογραφικό αλγόριθμο, ο οποίος είναι ευρέως γνωστός, αλλά στο κλειδί που χρησιμοποιείται με τον αλγόριθμο για την κρυπτογράφηση ή την αποκρυπτογράφηση. Η αποκρυπτογράφηση με το σωστό κλειδί είναι πολύ απλή. Αλλά χωρίς το σωστό κλειδί είναι πολύ δύσκολη, και στις

περισσότερες περιπτώσεις αδύνατη. Για αυτό είναι πολύ σημαντικό να διαχειριζόμαστε σωστά τα κλειδιά και να τα κρατάμε μυστικά όταν είναι απαραίτητο. Το κρυπτογραφικό σύστημα παρέχει διασφάλιση του απόρρητου των πληροφοριών (confidentiality) που στέλνονται μεταξύ των συναλλασσόμενων οντοτήτων. Έτσι, αν βρεθούν στα "χέρια" τρίτων, θα τους είναι άχρηστες, μιας και δεν θα μπορούν να αντιληφθούν το περιεχόμενο τους, αφού δεν θα γνωρίζουν το κλειδί αποκρυπτογράφησης.

Οι δύο πιο διαδεδομένοι τύποι κρυπτογραφίας είναι η συμμετρική (symmetric cryptography) και η ασύμμετρη ή δημόσιου κλειδιού (asymmetric ή public key cryptography) κρυπτογραφία.

## 2.3 Συμμετρική κρυπτογραφία (Symmetric cryptography)

Η συμμετρική κρυπτογραφία βασίζεται στην ιδέα ότι για την ανταλλαγή κρυπτογραφημένων μηνυμάτων, ο αποστολέας και ο παραλήπτης είναι οι μοναδικές οντότητες που γνωρίζουν μια συγκεκριμένη μυστική πληροφορία. Η μυστική αυτή πληροφορία αποτελεί το συμμετρικό κλειδί του συμμετρικού κρυπτογραφικού αλγόριθμου και χρησιμοποιείται για την κρυπτογράφηση και την αποκρυπτογράφηση του μηνύματος. Οι αλγόριθμοι σε αυτή την περίπτωση λέγονται συμμετρικοί, ακριβώς επειδή χρησιμοποιούμε το ίδιο κλειδί για κρυπτογράφηση και αποκρυπτογράφηση.




*Σχήμα 2.2. Ένα συμμετρικό κρυπτογραφικό σύστημα*

Για να διασφαλιστεί το απόρρητο των πληροφοριών (confidentiality) που στέλνονται μεταξύ των συναλλασσόμενων οντοτήτων, το συμμετρικό σύστημα λειτουργεί ως εξής. Έστω ότι τα συστήματα Α και Β θέλουν να έχουν μια ασφαλή επικοινωνία. Τότε πρέπει μόνο αυτά

τα δύο να γνωρίζουν το κλειδί κρυπτογράφησης. Το κλειδί πρέπει να διατηρείται κρυφό από όλα τα άλλα συστήματα. Έτσι τα μηνύματα που στέλνονται από το σύστημα Α στο Β κρυπτογραφούνται με αυτό το κλειδί, και κανένα άλλο σύστημα δεν μπορεί να τα αποκρυπτογραφήσει.

Ο πιο γνωστός αλγόριθμος για συμμετρική κρυπτογράφηση είναι ο DES (Data Encryption Standard), που υιοθετήθηκε το 1977 από το Αμερικανικό NBS (National Bureau of Standards). Ο DES είναι αλγόριθμος κρυπτογράφησης μπλοκ, με μέγεθος μπλοκ 64 bits και χρησιμοποιεί κλειδί 56, το οποίο δυστυχώς είναι μικρού μήκους.

Γενικά ο DES μπορεί να σπάσει αν χρησιμοποιηθούν πολύ ισχυροί υπολογιστές ή ειδικό hardware. Είναι ακόμα ισχυρός για hackers που προσπαθούν να τον σπάσουν με τυχαίες προσπάθειες, αλλά κυβερνήσεις που κατέχουν ειδικό hardware, μεγάλοι οργανισμοί ή εγκληματικές οργανώσεις μπορούν να τον σπάσουν εύκολα. Για αυτό το λόγο δεν θα πρέπει να χρησιμοποιείται σε καινούργιες εφαρμογές. Μεγαλύτερη ασφάλεια μπορεί να επιτευχθεί με τη χρήση του triple-DES. Με τον triple-DES χρησιμοποιούμε αποτελεσματικά κλειδί 112 bits, το οποίο είναι επαρκώς μεγάλο. Ο triple-DES βασίζεται στη χρησιμοποίηση του DES τρεις φορές.

Ο AES (Advanced Encryption Algorithm) είναι ένα πρότυπο που υιοθετήθηκε από τις Η.Π.Α. τον Νοέμβριο του 2001, σε αντικατάσταση του DES. Ως βάση του προτύπου χρησιμοποιήθηκε ο κρυπτογραφικός αλγόριθμος Rijndael, που αναπτύχθηκε από τους Βέλγους Joan Daemen και Vincent Rijmen. Αξίζει να αναφερθεί ότι ο αλγόριθμος αυτός επιλέχθηκε από το NIST (National Institute of Standards and Technology) του Υπουργείου Εμπορίου των Η.Π.Α., ανάμεσα από άλλους 5 υποψήφιους αλγόριθμους, ένας εκ των οποίων (γνωστός ως MARS) αναπτύχθηκε από μια πολυμελή ομάδα εργασίας της IBM. Σημαντικότερο πλεονέκτημα της συμμετρικής κρυπτογραφίας είναι η ταχύτητα, τόσο κατά την κρυπτογράφηση, όσο και κατά την αποκρυπτογράφηση, που μπορεί να ξεπεράσει τα δεκάδες megabytes/sec. Επίσης, οι εφαρμογές συμμετρικής κρυπτογραφίας μπορεί να έχουν μικρές απαιτήσεις υπολογιστικής ισχύς και μνήμης, ώστε να πραγματοποιούνται και σε περιβάλλον όπου η μνήμη και η ισχύς επεξεργαστή είναι περιορισμένες (π.χ. σε έξυπνες κάρτες).

Το σημαντικότερο μειονέκτημα της συμμετρικής κρυπτογραφίας είναι η ανάγκη ασφαλούς διανομής του συμμετρικού κλειδιού. Ολόκληρη η ασφάλεια των μηχανισμών συμμετρικής κρυπτογραφίας βασίζεται στη διατήρηση της μυστικότητας του συμμετρικού κλειδιού, το οποίο πρέπει να είναι γνωστό μόνο στον αποστολέα και στον παραλήπτη, πριν από τη μετάδοση του μηνύματος. Συνεπώς, απαιτείται ένας ξεχωριστός μηχανισμός ασφαλούς μεταφοράς του κλειδιού, στόχος που δεν είναι πάντοτε εφικτός, εξαιτίας γεωγραφικών, πολιτικών ή λειτουργικών δυσκολιών. Το πρόβλημα γίνεται δυσκολότερο, όταν αποστολέας και παραλήπτης είναι άγνωστες μεταξύ τους οντότητες. Σε αυτήν την περίπτωση, προκύπτει επιπλέον η ανάγκη πιστοποίησης της αυθεντικότητας της κάθε οντότητας, για να αποφευχθεί η γνωστοποίηση του συμμετρικού κλειδιού σε μη εξουσιοδοτημένες οντότητες. Τέλος, η συμμετρική κρυπτογραφία χαρακτηρίζεται από δυσκολία κλιμάκωσης της μεθόδου, έτσι ώστε να υποστηρίξει ασφαλή επικοινωνία μεταξύ μεγάλης ομάδας χρηστών. Όπως προαναφέρθηκε για την επικοινωνία μεταξύ δύο οντοτήτων απαιτείται ένα συμμετρικό κλειδί. Εάν οι οντότητες γίνουν τρεις, τότε τα συμμετρικά κλειδιά που απαιτούνται γίνονται τρία, για τέσσερις οντότητες απαιτούνται έξι κλειδιά κ.ο.κ. Γίνεται εύκολα κατανοητό, ότι για *n* οντότητες απαιτείται *n*(n-1)/2* πλήθος συμμετρικών κλειδιών. Το πλήθος των συμμετρικών κλειδιών γίνεται ακόμα μεγαλύτερο, συγκεκριμένα *n*(n+1)/2*, αν ο κάθε χρήστης θέλει και ένα κλειδί για προσωπική χρήση. Επομένως, το πλήθος των απαιτούμενων κλειδιών αυξάνεται περίπου με το τετράγωνο του αριθμού των χρηστών και συνεπώς γίνεται εξαιρετικά δύσκολη η υποστήριξη κρυπτογραφημένης επικοινωνίας σε ομάδες με πλήθος 1000 ή 10000 μελών.

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

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

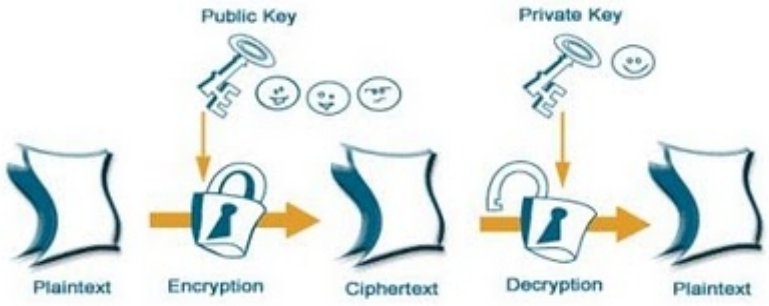
Στα μέσα της δεκαετίας του 1970 οι Whitfield Diffie και Martin Hellman πρότειναν μια νέα τεχνική για τον περιορισμό των προβλημάτων της συμμετρικής κρυπτογραφίας. Η

τεχνική αυτή, γνωστή ως κρυπτογραφία δημοσίου κλειδιού ή ασύμμετρη κρυπτογραφία, βασίζεται στην ύπαρξη ενός ζεύγους κλειδιών (key pair), το οποίο αποτελούν το δημόσιο κλειδί (public key) και το ιδιωτικό κλειδί (private key).

Τα δύο κλειδιά, αν και διαφορετικά, σχετίζονται με έναν ορισμένο μαθηματικό τρόπο. Η γνώση του ενός κλειδιού δεν επιτρέπει την παραγωγή ή τον υπολογισμό του άλλου. Επίσης, το ζεύγος κλειδιών έχει την ιδιότητα, το ένα κλειδί να μπορεί να αποκρυπτογραφήσει, ότι κρυπτογράφησε το άλλο κλειδί, δηλαδή αν η κρυπτογράφηση γίνεται με το δημόσιο κλειδί, η αποκρυπτογράφηση γίνεται με το ιδιωτικό και αντίστροφα. Ο κάτοχος του ζεύγους κλειδιών διανέμει το δημόσιο κλειδί ελεύθερα, χωρίς αυτό να υπονομεύει την ασφάλεια του συστήματος, ενώ είναι υποχρεωμένος να προστατεύει με αυστηρότητα το ιδιωτικό κλειδί, καθώς διαρροή του ιδιωτικού κλειδιού συνεπάγεται κατάρρευση των μηχανισμών ασφάλειας του ζεύγους κλειδιών.

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

Αν ο χρήστης Α θέλει να στείλει ένα μήνυμα στο Β, το κρυπτογραφεί με το δημόσιο κλειδί του Β. Επειδή ο Β είναι ο μόνος που έχει πρόσβαση στο ιδιωτικό του κλειδί, μόνο αυτός μπορεί να αποκρυπτογραφήσει το μήνυμα και να το διαβάσει.




*Σχήμα 2.3. Ένα ασυμμετρικό κρυπτογραφικό σύστημα*

Τα πλεονεκτήματα της ασύμμετρης κρυπτογραφίας είναι, ότι δεν είναι απαραίτητη η ανταλλαγή και η γνώση ενός κοινού (κρυφού) κλειδιού από τον αποστολέα και τον παραλήπτη όπως στα συμμετρικά συστήματα, εφόσον το δημόσιο κλειδί διανέμεται

ελεύθερα. Είναι απαραίτητος ένας μικρός μόνο αριθμός ζευγών κλειδιών (ίσος με τον αριθμό των χρηστών), ενώ στη συμμετρική κρυπτογράφηση ο αριθμός των κλειδιών που απαιτούνται είναι περίπου το τετράγωνο του αριθμού των χρηστών. Άρα καλύπτει εύκολα τις επικοινωνιακές ανάγκες μεγάλων ομάδων χρηστών, αφού το απαιτούμενο πλήθος κλειδιών είναι ίσο με το πλήθος της ομάδας. Οι ασυμμετρικές μέθοδοι προσφέρονται για τη δημιουργία ψηφιακών υπογραφών, ενώ οι συμμετρικές μέθοδοι όχι. Στο συμμετρικό σύστημα κρυπτογράφησης το κρυφό κλειδί πρέπει να είναι γνωστό σε κάθε χρήστη που θέλει να επιβεβαιώσει μια υπογραφή. Συνεπώς στο συμμετρικό σύστημα δεν διασφαλίζεται η αυθεντικότητα της υπογραφής γιατί μπορεί να υπογράψει οποιοσδήποτε από αυτούς που γνωρίζουν το κρυφό κλειδί.

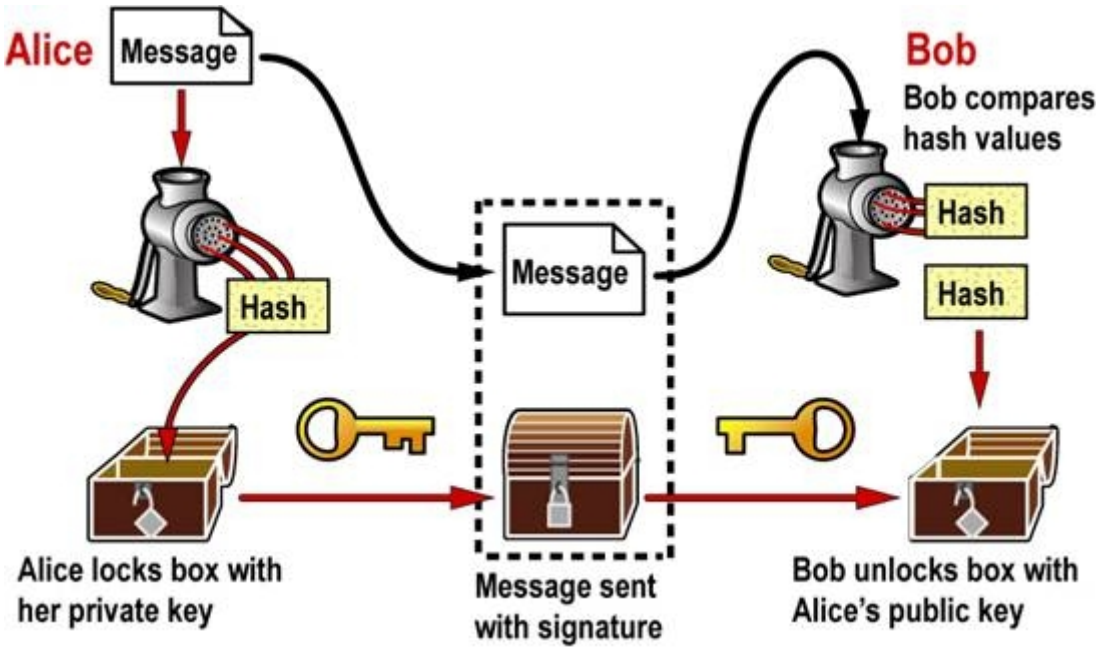
Όμως, τα μειονεκτήματα είναι ότι υστερεί σε ταχύτητα, σε σύγκριση με τη συμμετρική κρυπτογραφία και ότι το κρυπτοκείμενο που προκύπτει είναι μεγαλύτερο σε μέγεθος από το αρχικό απλό κείμενο (plain text). Είναι απαραίτητη η διαχείριση των δημόσιων κλειδιών στα ασύμμετρα κρυπτοσυστήματα. Τα δημόσια κλειδιά δεν είναι απαραίτητο να μεταδίδονται κρυφά, αλλά απαιτείται να είναι απαραιτήτως αυθεντικά. Για αυτό το σκοπό χρησιμοποιούνται τα πιστοποιητικά δημόσιων κλειδιών (public key certificates) που είναι δημόσια διαθέσιμα μέσω μιας Αρχής Πιστοποίησης, η οποία τα δημοσιοποιεί σε ένα κατάλογο (directory). 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).

Η κρυπτογράφηση με τον αλγόριθμο RSA (Rivest-Shamir-Adelman) προσδιορίζεται στο [PKCS#1], το οποίο είναι μέρος της ομάδας των standards για την ασύμμετρη κρυπτογραφία. Είναι ο πιο σημαντικός και ευρέως διαδεδομένος αλγόριθμος για ασύμμετρη κρυπτογράφηση και χρησιμοποιείται εκτός από την κρυπτογράφηση και για ψηφιακή υπογραφή. Γενικά θεωρείται ασφαλής όταν χρησιμοποιούνται αρκετά μεγάλα κλειδιά. Προς το παρόν, τα κλειδιά των 512 ψηφίων θεωρούνται ανίσχυρα, τα κλειδιά των 1024 ψηφίων είναι αρκετά ισχυρά για τις περισσότερες εφαρμογές, και τα κλειδιά 2048 ψηφίων πιθανότατα θα παραμείνουν ασφαλή για δεκαετίες. Επειδή οι γνωστές ασυμμετρικές μέθοδοι είναι πιο αργές από τις συμμετρικές μεθόδους συχνά χρησιμοποιείται ο συνδυασμός και των δύο

μεθόδων: Το κρυφό κλειδί του συμμετρικού συστήματος που χρησιμοποιείται μόνο για μια φορά (session key), μεταδίδεται αφού κρυπτογραφηθεί ασυμμετρικά. Η κρυπτογράφηση και η αποκρυπτογράφηση του συνολικού μηνύματος γίνεται με συμμετρικό σύστημα με χρήση του παραπάνω κλειδιού.

## 2.5 Ψηφιακές υπογραφές (Digital signatures)

Η χρήση *ψηφιακών υπογραφών*, κατά την ανταλλαγή πληροφοριών, εγγυάται την αυθεντικότητα της ταυτότητας του αποστολέα και την ακεραιότητα της πληροφορίας. Οι ψηφιακές υπογραφές βασίζονται στις συναρτήσεις κατακερματισμού και σε τεχνικές κρυπτογραφίας δημόσιου κλειδιού. Το ιδιωτικό κλειδί χρησιμοποιείται για τη δημιουργία των ψηφιακών υπογραφών, ενώ το δημόσιο κλειδί χρησιμοποιείται για την επαλήθευση της εγκυρότητάς τους.




*Σχήμα 2.4: Ψηφιακή Υπογραφή και Επαλήθευση*

Στο παραπάνω σχήμα παρουσιάζεται αναλυτικά η διαδικασία δημιουργίας και επαλήθευσης ψηφιακής υπογραφής. Όπως αναφέρθηκε και προηγουμένως, η κρυπτογράφηση

ενός μηνύματος με το δημόσιο κλειδί, παράγει το κρυπτογραφημένο κείμενο, που μπορεί να διαβαστεί μονάχα με την βοήθεια του ιδιωτικού κλειδιού. Ωστόσο μια ιδιότητα που έχουν ορισμένοι αλγόριθμοι (π.χ. ο RSA) επιτρέπουν την ακριβώς αντίστροφη διαδικασία: την κωδικοποίηση μηνυμάτων με το ιδιωτικό κλειδί έτσι ώστε η αποκωδικοποίηση να μπορεί να γίνει μόνο με το αντίστοιχο δημόσιο. Η διαδικασία για την κατασκευή των ψηφιακών υπογραφών προσδιορίζεται στο [PKCS#1] που είναι μέρος των προτύπων των RSA Laboratories για την κρυπτογραφία. Οι πιο γνωστοί αλγόριθμοι ψηφιακών υπογραφών είναι οι RSA και DSA. [PKCS#1]

Η παρακάτω διαδικασία εξηγεί συνοπτικά πως δημιουργείται και χρησιμοποιείται η ψηφιακή υπογραφή:

1) Ο αποστολέας Bob χρησιμοποιεί ένα αλγόριθμο σύνοψης μηνύματος για να δημιουργήσει μια σύνοψη μηνύματος (message digest), η οποία μπορεί να κρυπτογραφηθεί.

2) Ο Bob χρησιμοποιεί το ιδιωτικό του κλειδί για να κρυπτογραφήσει την σύνοψη του μηνύματος.

3) Ο Bob στέλνει μαζί με το αρχικό μήνυμα και την κρυπτογραφημένη σύνοψη του μηνύματος στον παραλήπτη.

4) Όταν λάβει το μήνυμα ο παραλήπτης Alice αποκρυπτογραφεί την σύνοψη του μηνύματος με το δημόσιο κλειδί του αποστολέα.

5) Η Alice εφαρμόζει τη αλγόριθμο σύνοψης στο αρχικό μήνυμα για να υπολογίσει την σύνοψη του.

6) Η Alice συγκρίνει την αποκρυπτογραφημένη σύνοψη του μηνύματος με τη σύνοψη που έχει παράγει ο ίδιος.

- Αν οι δύο συνόψεις είναι ίδιες, ο παραλήπτης ξέρει ότι το μήνυμα στάλθηκε πραγματικά από το πρόσωπο που ισχυρίζεται ότι είναι ο αποστολέας και ότι το μήνυμα δεν αλλάχθηκε κατά την μετάδοση του.

- Αν οι συνόψεις είναι διαφορετικές, ο αποστολέας ξέρει ότι είτε το μήνυμα στάλθηκε από κάποιον άλλον που ισχυρίζεται ότι είναι ο αποστολέας ή ότι το μήνυμα μεταβλήθηκε ή καταστράφηκε κατά τη μετάδοση του. Απαραίτητη προϋπόθεση για

την ταυτοποίηση του αποστολέα, είναι να γνωρίζει με βεβαιότητα ο παραλήπτης, ότι το δημόσιο κλειδί που χρησιμοποιεί για τον έλεγχο εγκυρότητας της ψηφιακής υπογραφής και το αντίστοιχο ιδιωτικό κλειδί ανήκουν πράγματι σε εκείνον, που εμφανίζεται ως αποστολέας του μηνύματος. διαφορετικά, η ψηφιακή υπογραφή αποδεικνύει μόνο την ακεραιότητα του μηνύματος. Γίνεται, λοιπόν, εμφανής η ανάγκη ύπαρξης ενός μηχανισμού, ο οποίος θα συσχετίζει με μοναδικό και εγγυημένο τρόπο το δημόσιο και το αντίστοιχο ιδιωτικό κλειδί με την οντότητα, στην οποία αυτά ανήκουν. Ο μηχανισμός αυτός είναι τα ψηφιακά πιστοποιητικά (digital certificates) και περιγράφονται στη συνέχεια.

### 2.5.1 Νομικό πλαίσιο ψηφιακών υπογραφών

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

Ο ιδιοκτήτης του κλειδιού δεν είναι και απαραίτητα και ο διαχειριστής του. Ο ιδιοκτήτης είναι αυτός που έχει το δικαίωμα χρήσης του κλειδιού. Ο διαχειριστής είναι η οντότητα που πρακτικά διαχειρίζεται το κλειδί και μπορεί να είναι ακόμα και ο server που δημιουργεί τις υπογραφές. Σύμφωνα λοιπόν με την 1999/93/ΕΚ αναγνωρίζονται τρία είδη ψηφιακών υπογραφών, η κάθε μία με διαφορετική δικαστική αξία:

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

**2. *Προηγμένη ηλεκτρονική υπογραφή*:** Είναι η ηλεκτρονική υπογραφή που ακολουθεί τα παρακάτω κριτήρια:

1. Συνδέεται αποκλειστικά με τον υπογράφοντα και μόνο με αυτόν.

2. Είναι ικανή να λειτουργήσει ως αναγνωριστικό του υπογράφοντος.

3. Η δημιουργία της γίνεται με μέσα που ο υπογράφων διατηρεί υπό τον έλεγχό του και μόνο. Συνδέεται με τα δεδομένα στα οποία αναφέρεται με τέτοιο τρόπο ώστε να είναι ανιχνεύσιμη κάθε αλλαγή.

4. Η προηγμένη ψηφιακή υπογραφή έχει πιο βαρυσήμαντη αξία από την απλή: Εγγυάται εκτός από την ακεραιότητα του κειμένου και την αυθεντικοποίηση. *Η Προηγμένη ηλεκτρονική υπογραφή βασίζεται σε ένα κατάλληλο πιστοποιητικό που δημιουργείται από μια Αρχή δημιουργίας ασφαλών υπογραφών*.

Η Αρχή δημιουργίας ασφαλών υπογραφών (Certification Authority ή CA) πρέπει να έχει τα κατάλληλα τεχνικά χαρακτηριστικά που απαιτούνται ώστε, να εξασφαλιστεί πως το κλειδί δεν θα μπορεί να αναπαραχθεί, ούτε να πλαστογραφηθεί, εντός ενός εύλογου χρονικού διαστήματος. Αυτό το χρονικό διάστημα, θα πρέπει φυσικά να είναι μεγαλύτερο από την περίοδο εγκυρότητας της υπογραφής. Οι απαιτήσεις αυτές καθορίζονται από την Επιτροπή Ψηφιακών Υπογραφών (Electronic Signature Committee), που βοηθά στην ανάλυση τέτοιων τεχνικών θεμάτων.

Οι απαιτήσεις για ένα κατάλληλο πιστοποιητικό είναι:

*1. Η ένδειξη ότι το πιστοποιητικό εκδίδεται ως κατάλληλο πιστοποιητικό (qualified certificate)*

*2. Αναγνωριστικό της CA καθώς και του κράτους (Ευρωπαϊκού ή μη) στο οποίο εκδόθηκε*

*3. Το όνομα (ή ψευδώνυμο) του υπογράφοντα.*

*4. Δεδομένα για την επαλήθευση της υπογραφής που αντιστοιχούν σε δεδομένα που δημιουργήθηκαν με την δημιουργία της υπογραφής και βρίσκονται κάτω από τον έλεγχο του υπογράφοντα.*

*5. Ένδειξη που δηλώνει την περίοδο εγκυρότητας της υπογραφής.*

*6. Αναγνωριστικό του πιστοποιητικού.*

*7. Η προηγμένη υπογραφή της CA.*

Η ασφαλής υπογραφή μπορεί να περιέχει ακόμα στοιχεία όπως κάποιο ιδιαίτερο χαρακτηριστικό του υπογράφοντος. Μπορεί να υπάρχουν περιορισμοί στους γιατρούς που να προσδιορίζουν ότι μπορούν να υπογραφούν γνωματεύσεις μόνο σε ορισμένους ασθενείς. Αυτός ο τύπος ψηφιακής υπογραφής έχει μεγάλη νομική αξία γιατί εγγυάται 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 απαραίτητα στοιχεία για εφαρμογές που απαιτούν την διακίνηση πληροφορίας με ασφάλεια και υπευθυνότητα.

## 2.6 Συναρτήσεις Κατακερματισμού (Hash Functions ή Message Digest)

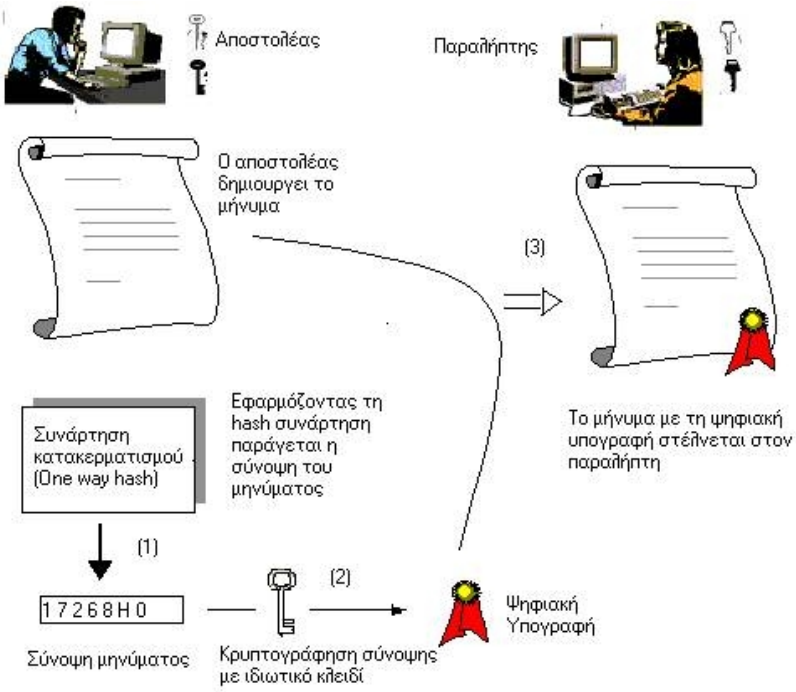
Η ψηφιακή υπογραφή έχει όμως το μειονέκτημα να απαιτεί την κρυπτογράφηση όλου του μηνύματος και την αποστολή του αποτελέσματος, καθώς και του αρχικού μηνύματος. Αυτό έχει σαν αποτέλεσμα να αποστέλλουμε κάθε φορά την διπλάσια τουλάχιστον ποσότητα πληροφορίας, σε σχέση με το αρχικό μήνυμα. Εκτός του ότι θα ήταν εξαιρετικά χρονοβόρο,

προσθέτει σημαντικό φόρτο στο εκάστοτε δίκτυο. Έτσι επινοήθηκαν κάποιες μονόδρομες μαθηματικές συναρτήσεις που δημιουργούν με μοναδικό τρόπο μια “περίληψη” του αρχικού μηνύματος, (Hash ή Message Digest), οπότε αρκεί να υπογράψουμε μονάχα αυτό.

Ο όρος *συνάρτηση κατακερματισμού* (hash function) υποδηλώνει ένα μετασχηματισμό *H* ο οποίος παίρνει ως είσοδο ένα μήνυμα *m* ανεξαρτήτου μήκους και δίνει ως έξοδο μία ακολουθία χαρακτήρων h, και περιγράφεται ως $h = H(m)$ . Η έξοδος *h* μιας συνάρτησης κατακερματισμού ονομάζεται *τιμή κατακερματισμού (hash value)* ή *σύνοψη μηνύματος (message digest)* και έχει συγκεκριμένο μήκος ανάλογα με το είδος του αλγόριθμου κατακερματισμού που χρησιμοποιείται, συνήθως πολύ μικρότερο από αυτό του αρχικού μηνύματος. Επειδή η συνάρτηση κατακερματισμού παράγει την σύνοψη ενός μηνύματος, οι συναρτήσεις αυτές ονομάζονται αλγόριθμοι σύνοψης μηνύματος. Η σύνοψη μηνύματος πολλές φορές τη βρίσκουμε στη βιβλιογραφία και ως “ψηφιακό αποτύπωμα” (“digital fingerprint”) ενός εγγράφου.

Οι αλγόριθμοι σύνοψης μηνύματος πρέπει να είναι μονόδρομες συναρτήσεις (one-way functions). Ο σκοπός ενός αλγόριθμου σύνοψης μηνύματος είναι να παράγει μια αναπαράσταση του μηνύματος, που να είναι μικρότερη από αυτό για να κρυπτογραφείται γρηγορότερα. Έτσι η συνάρτηση πρέπει να μπορεί να υπολογίσει εύκολα την σύνοψη του μηνύματος όταν της δίνουμε το μήνυμα, αλλά πρέπει να είναι σχεδόν αδύνατο να υπολογίσει το μήνυμα όταν της δίνουμε την σύνοψη του μηνύματος. Με αυτήν την προϋπόθεση εξασφαλίζουμε ότι, άτομα που έχουν πρόσβαση στην σύνοψη του μηνύματος είναι δύσκολο να ανακαλύψουν το μήνυμα από την σύνοψη του. Όταν λοιπόν θέλουμε να υπογράψουμε ένα μήνυμα, πρώτα δημιουργούμε την σύνοψη του μηνύματος και ύστερα το κρυπτογραφούμε με το ιδιωτικό μας κλειδί. Ύστερα επισυνάπτουμε στο μήνυμα τη υπογεγραμμένη σύνοψη του μηνύματος και το αποστέλλουμε. Ο αποδέκτης θα δημιουργήσει και αυτός μια σύνοψη του μηνύματος με τον ίδιο αλγόριθμο που χρησιμοποιήσαμε και εμείς, μετά θα αποκρυπτογραφήσει με το δημόσιο μας κλειδί τη κρυπτογραφημένη σύνοψη του μηνύματος που στείλαμε και θα το συγκρίνει με αυτό που υπολόγισε ο ίδιος. Οποιαδήποτε διαφορά θα σημαίνει παραποίηση του μηνύματος.

**Χαρακτηριστικά Αλγόριθμου Σύνοψης Μηνύματος**




*Σχήμα 2.5: Ψηφιακή υπογραφή με message digest*

• Δεν είναι δυνατή η αντιστροφή μιας συνάρτησης κατακερματισμού, έτσι ώστε από τη σύνοψη να προκύψει το αρχικό κείμενο.

• Η σύνοψη δεν δίνει καμιά πληροφορία για το αρχικό κείμενο.

• Είναι υπολογιστικά ανέφικτο *(computationally infeasible)* να βρεθεί απλό κείμενο, που να έχει ως σύνοψη μια συγκεκριμένη τιμή.

• Διαφορετικό απλό κείμενο, πρέπει να δίνει πάντοτε διαφορετική σύνοψη. Σε περίπτωση που δύο διαφορετικά αρχικά κείμενα δίνουν την ίδια σύνοψη, έχουμε το φαινόμενο των συγκρούσεων *(conflicts)* της συνάρτησης κατακερματισμού που είναι σπάνια και προβληματική.

Οι πιο γνωστοί αλγόριθμοι κατακερματισμού είναι οι MD5 (Message Digest Algorithm 5) με σύνοψη μηνύματος 128 bit που αναπτύχθηκε από τα RSA Laboratories, ο RIPEMD-160 με σύνοψη 160 bits, ο SHA-1 (Secure Hash Algorithm) με σύνοψη 160 bits που αναπτύχθηκε από το NIST (National Institute of Standards and Technology) σε συνεργασία με την NSA (National Security Agency) και ο SHA-2. Οι νέες εκδόσεις του αλγορίθμου SHA, SHA-256, SHA- 384 και SHA-512 δίνουν σύνοψη μηνύματος 256, 384 και 512 bits αντίστοιχα.

## 2.7 Ψηφιακά πιστοποιητικά (digital certificates)

Τα δημόσια κλειδιά (public keys) μας δίνουν τη δυνατότητα να πιστοποιήσουμε την ταυτότητα ενός χρήστη. Πρέπει όμως να υπάρχει η εγγύηση ότι το δημόσιο κλειδί που κατέχουμε είναι αυθεντικό και ανήκει στον χρήστη που θέλουμε. Έως τώρα έχουμε υποθέσει ότι, όταν ο Bob θέλει να στείλει ένα μήνυμα ψηφιακά υπογεγραμμένο στην Alice τότε, αρκεί να χρησιμοποιήσει το δημόσιο κλειδί της Alice. Αν όμως η Trudy θέλει να υποκλέψει αυτή την ανταλλαγή μηνυμάτων μεταξύ Bob και Alice, θα μπορούσε να διαθέσει το δικό της δημόσιο κλειδί, υποκρινόμενη ότι είναι η Alice. Έτσι ο Bob θα υπέγραφε ψηφιακά το μήνυμα του με το δημόσιο κλειδί της Trudy (νομίζοντας ότι είναι το δημόσιο κλειδί της Alice). Άρα η Trudy δεν θα είχε παρά να χρησιμοποιήσει το δικό της ιδιωτικό κλειδί, να διαβάσει το μήνυμα και μετά να το υπογράψει με το δημόσιο κλειδί της Alice (που φυσικά είναι διαθέσιμο), να της το στείλει υποκρινόμενη ότι είναι ο Bob κ.ο.κ. Πρέπει λοιπόν να εξασφαλίσουμε έναν τρόπο να αναγνωρίζεται με σαφήνεια ο ιδιοκτήτης ενός δημοσίου κλειδιού.

Για να είμαστε σίγουροι ότι το δημόσιο κλειδί ανήκει σε ένα συγκεκριμένο άτομο πρέπει να υπάρχει ένα πιστοποιητικό από μια έγκυρη αρχή που να το βεβαιώνει. Ένα πιστοποιητικό δημοσίου κλειδιού είναι μια ψηφιακά υπογεγραμμένη δήλωση από μια οντότητα, που λέει ότι το δημόσιο κλειδί (ή κάποια άλλη πληροφορία) κάποιας άλλης οντότητας, έχει μια συγκεκριμένη τιμή. Με τον όρο “οντότητα” εννοούμε κάποιο φυσικό πρόσωπο, οργανισμό, πρόγραμμα, εταιρία, υπολογιστή ή οποιονδήποτε άλλο που μπορούμε να εμπιστευτούμε ως ένα βαθμό. Με λίγα λόγια εισάγουμε μια τρίτη οντότητα που λειτουργεί ως εγγυητής. Αυτό το πιστοποιητικό μπορεί ταυτόχρονα να χρησιμεύσει σαν πιστοποίηση επιβεβαίωσης της ταυτότητας του χρήστη.

Τα *ψηφιακά πιστοποιητικά* [ISO 9594-8] είναι δομές δεδομένων, υπογεγραμμένες ψηφιακά, οι οποίες αντιστοιχίζουν κατά μοναδικό τρόπο, μια οντότητα με το δημόσιο κλειδί της. Αυτό το δημόσιο κλειδί αντιστοιχεί στο ιδιωτικό κλειδί το οποίο ο κάτοχος του χρησιμοποιεί για να κρυπτογραφεί ή για να υπογράφει ηλεκτρονικά. Ένα ψηφιακό πιστοποιητικό περιέχει διάφορα πεδία, μεταξύ των οποίων την ονομασία του ιδιοκτήτη του

πιστοποιητικού, το δημόσιο κλειδί του και πιθανότατα κάποια άλλα χαρακτηριστικά. Η δομή του πιστοποιητικού υπογράφεται ψηφιακά από μια *έμπιστη οντότητα*. Τον ρόλο της έμπιστης οντότητας αναλαμβάνει κατάλληλη οντότητα, ανάλογα με τις ανάγκες της εφαρμογής και τις δυνατότητες της εκάστοτε υποδομής. Η σύνδεση ενός δημόσιου κλειδιού με μια οντότητα πιστοποιείται από μια Αρχή Πιστοποίησης (Certification Authority) η οποία υπογράφει το πιστοποιητικό με το ιδιωτικό της κλειδί.

### 2.7.1 Αρχή Πιστοποίησης (CA/Certification Authority)

Τα πιστοποιητικά εκδίδονται από Αρχές Πιστοποίησης (CAs/Certification Authorities). Πρόκειται συνήθως για εταιρίες που θεωρείται ότι μπορεί κανείς να τις εμπιστευτεί ώστε να υπογράφουν (δηλαδή να εκδίδουν) πιστοποιητικά για κάποια άλλη οντότητα. Υπάρχουν αρκετές CAs που είναι διαθέσιμες, όπως η VeriSign, Thawte, Entrust, κ.α. Υπάρχει επίσης η δυνατότητα να δημιουργήσει κανείς την δική του Αρχή έκδοσης πιστοποιητικών χρησιμοποιώντας προϊόντα όπως “Certificate Servers” της Netscape ή το “Entrust CA” της Microsoft. Τις Αρχές Πιστοποίησης τις αποκαλούμε εν συντομία CAs. Είναι σαφές ότι εφόσον οι δύο πλευρές που θέλουν να επικοινωνήσουν έχουν πιστοποιητικά στην ίδια CA η διαδικασία είναι απλή: Αρκεί ο ένας να επαληθεύσει την υπογραφή της CA που βρίσκεται πάνω στο πιστοποιητικό του άλλου. Αν όμως χρησιμοποιούν διαφορετική CA τότε τα πράγματα είναι πιο περίπλοκα. Οι διάφορες CAs σχετίζονται μεταξύ τους με ένα είδος δομής δέντρου. Η Αρχή Πιστοποίησης βεβαιώνει για την ακεραιότητα του δημόσιου κλειδιού και την αυθεντικότητα της ταυτότητας του φερόμενου ως ιδιοκτήτη του, υπογράφοντας ψηφιακά τη δομή του πιστοποιητικού με το ιδιωτικό της κλειδί. Για τον έλεγχο της εγκυρότητας ενός πιστοποιητικού, υπογεγραμμένου από την Αρχή Πιστοποίησης, απαιτείται, σύμφωνα με τα προαναφερθέντα για τις ψηφιακές υπογραφές, το δημόσιο κλειδί της Αρχής. Ο ενδιαφερόμενος ανακτά το πιστοποιητικό της Αρχής, το οποίο περιέχει το ζητούμενο δημόσιο κλειδί και είναι ψηφιακά υπογεγραμμένο από το αντίστοιχο ιδιωτικό κλειδί. Τα πιστοποιητικά CA είναι τα μοναδικά, που έχουν ως ιδιότητα να υπογράφονται από το ιδιωτικό κλειδί του ζεύγους κλειδιών, στο οποίο ανήκει το δημόσιο κλειδί που περιέχουν.

Όπως κάθε είδος ταυτοποίησης, ένα ψηφιακό πιστοποιητικό είναι αξιόπιστο μόνο εάν η αρχή που το έχει εκδώσει είναι αξιόπιστη.

Αρχή πιστοποιητικών CA μπορεί να είναι κάθε έμπιστη κεντρική διοίκηση που προτίθεται να εγγυηθεί για τις ταυτότητες των ατόμων στα όποια έχει εκδώσει πιστοποιητικό. Αυτό το κεντρικό διοικητικό σώμα μπορεί να είναι μια νοσηλευτική μονάδα που εκδίδει πιστοποιητικά στους επαγγελματίες υγείας της, ένα πανεπιστήμιο που εκδίδει πιστοποιητικά στους φοιτητές του ή μία τρίτη εταιρία που εκδίδει πιστοποιητικά σε πελάτες. Κάθε χρήστης παρέχει στην Αρχή Πιστοποίησης το δημόσιο κλειδί του και πληροφορίες για το άτομο του. Οι πληροφορίες αυτές επιβεβαιώνονται με τον τρόπο που ορίζει η συγκεκριμένη Αρχή Πιστοποίησης και κατόπιν το ψηφιακό πιστοποιητικό εκδίδεται με την επίσημη έγκριση της συγκεκριμένης αρχής.

Οι Αρχές Πιστοποίησης (CAs) ονομάζονται επίσης και έμπιστες τρίτες οντότητες (Trusted third parties / TTPs) γιατί παίζουν τον ρόλο ενός έμπιστου τρίτου διαμεσολαβητή, τον οποίο οι δύο πλευρές που θέλουν να επιβεβαιώσουν μεταξύ τους τις ταυτότητες τους δεν έχουν ποτέ τους συναντήσει.

Μεταξύ των διαφόρων ειδών ψηφιακών πιστοποιητικών συμπεριλαμβάνονται τα X.509 πιστοποιητικά δημόσιου κλειδιού, τα SPKI (Simple Public Key Infrastructure) πιστοποιητικά και τα PGP (Pretty Good Privacy) πιστοποιητικά.

### 2.7.2 Πρότυπα για την μορφή των πιστοποιητικών και των Λιστών Ακύρωσης Πιστοποιητικών

Σημαντικές μορφές πιστοποιητικών:

- **X.509 certificates [RFC2459]**
- **SDSI [SDSI]**
- **PGP certificate formats [RFC1991]**
- **DNS Security Extension [RFC2065]**

Μέχρι σήμερα τα πιστοποιητικά που έχουν αναπτυχθεί περισσότερο είναι το PGP και το X.509. Το πρώτο είναι πολύ απλό γιατί αναπαριστά ένα δημόσιο κλειδί και μία ηλεκτρονική διεύθυνση (e-mail address). Εντούτοις, στα πιστοποιητικά τύπου PGP παρουσιάζονται πολλά προβλήματα όταν πρόκειται να χρησιμοποιηθούν για ανοικτά κατανεμημένα περιβάλλοντα, διότι δεν είναι επεκτάσιμα.

Δεν μπορούν να συνδεθούν ενέργειες με τα κλειδιά. Για αυτό το λόγο θα δώσουμε έμφαση στη χρήση των πιστοποιητικών X.509, και ιδιαίτερα στα πιστοποιητικά X.509 v.3 (version 3).

Η ITU-T (International Telecommunications Union) έχει θεσπίσει ένα πρότυπο για τα ψηφιακά πιστοποιητικά, το Recommendation X.509 (ISO/IEC 9594- 8:1998). Το X.509 είναι ένα σχήμα πιστοποίησης σχεδιασμένο για να υποστηρίζει υπηρεσίες καταλόγου X.500. Τα πρωτόκολλα X.509 και X.500 είναι μέρος της σειράς X standards που έχει προταθεί από το ISO και το ITU. Το πρότυπο X.500 σχεδιάστηκε με στόχο να παρέχει παγκόσμιας εμβέλειας Υπηρεσίες Καταλόγου (directory services) ενώ το πρότυπο X.509 σχεδιάστηκε με στόχο να παρέχει πιστοποίηση στα X.500 services. Το X.509 (version 1) αναπτύχθηκε για πρώτη φορά το 1988. Για αυτό το λόγο είναι το παλαιότερο πρότυπο για ένα καθολικό σύστημα υποδομής δημοσίου κλειδιού PKI που έχει υιοθετηθεί από πολλές εταιρίες. Η Visa και η Master Card το υιοθέτησαν για το δικό τους Ασφαλές Πρότυπο Ηλεκτρονικών Συναλλαγών (Secure Electronic Transactions/ SET), ενώ η Netscape και η Microsoft το χρησιμοποίησαν για την υλοποίηση του δικού τους Certificate Server. Ήδη το πρότυπο X.509 έχει διαδοθεί τόσο ευρέως που είναι πολύ δύσκολο να αντικατασταθεί από ένα άλλο πρότυπο. Αν και το X.509 παρουσιάζει ορισμένες ελλείψεις, ιδιαίτερα όσον αφορά το θέμα της διαλειτουργικότητας, αναμένεται στο μέλλον να επικρατήσουν στις υλοποιήσεις των συστημάτων ασφαλείας PKI μόνο καινούργιες εκδόσεις αυτού του προτύπου, ή επεκτάσεις αυτού. Η έκδοση 3 είναι η πιο πρόσφατη έκδοση του πρότυπου X.509. Το κύριο πλεονέκτημα των X.509 v3 πιστοποιητικών σε σχέση με τις άλλες δυο παλαιότερες εκδόσεις (v1 και v2) των πιστοποιητικών είναι ότι παρέχει τα μέσα για την μη αναγκαστική χρησιμοποίηση μιας ιεραρχίας που να περιγράφει και να προσαρμόζεται μόνο σε συγκεκριμένο τομέα (domain). Τα X.509 v1 και X.509 v2 πιστοποιητικά είναι περισσότερο κατάλληλα για τη χρήση σε περιορισμένο τομέα (domain) όπως για παράδειγμα ενός νοσοκομείου. Αυτός είναι ένας περιορισμός που εμποδίζει την

ευρεία ανάπτυξη αυτών των πιστοποιητικών. Σύμφωνα με το πρότυπο ITU X.509, ένα πιστοποιητικό αποτελείται από δύο μέρη: τα δεδομένα που περιέχει το πιστοποιητικό και την υπογραφή από την Αρχή Πιστοποίησης που εξέδωσε αυτό το πιστοποιητικό.

Περιέχει τα εξής χαρακτηριστικά:

***Version:*** Η έκδοση του X.509. Ανάλογα με αυτή, καθορίζεται τι είδους πληροφορίες θα μπορούν να υπάρχουν στο συγκεκριμένο πιστοποιητικό. Υπάρχουν τρεις εκδόσεις του.

***Serial Number:*** Η οντότητα που δημιούργησε το πιστοποιητικό δίνει έναν μοναδικό αριθμό στο κάθε πιστοποιητικό που εκδίδει.

***Signature Algorithm Identifier:*** Ο αλγόριθμος που χρησιμοποίησε η Αρχή έκδοσης του πιστοποιητικού (CA) για να το υπογράψει. Για παράδειγμα PKCS #1 MD5 with RSA Encryption. Αυτό σημαίνει ότι η κρυπτογράφηση γίνεται σύμφωνα με το πρότυπο κρυπτογράφησης PKCS#1, χρησιμοποιείται ο αλγόριθμος κατακερματισμού MD5 και ο αλγόριθμος κρυπτογράφησης RSA.

***Issuer Name*:** Το όνομα (γραμμένο σύμφωνα με το πρότυπο X.500) της οντότητας που υπέγραψε το πιστοποιητικό, δηλαδή της CA. (Το πρότυπο X.500 εξασφαλίζει την μοναδικότητα του ονόματος στο Internet), για παράδειγμα, (Αρχή Πιστοποιητικών HYGEIAnet, O=Γ.Ν. Παπανικολάου, OU=Νοσοκομεία, ST=Θεσσαλονίκη, O=Τομέας Υγείας, C=GR)

***Validity Period:*** Η χρονική περίοδος μέσα στην οποία το πιστοποιητικό θεωρείται έγκυρο. Η διάρκειά της μπορεί να ποικίλει από μερικά δευτερόλεπτα μέχρι σχεδόν έναν αιώνα και εξαρτάται από διάφορους παράγοντες, όπως το πόσο ασφαλές θεωρείται το ιδιωτικό κλειδί που χρησιμοποιείται για την υπογραφή του πιστοποιητικού, ή το χρηματικό ποσό που κάποιος θα καταβάλει για το πιστοποιητικό.

***Subject (User) Name:*** Το όνομα (σύμφωνα πάντα με το X.500) της οντότητας της οποίας το δημόσιο κλειδί αναγνωρίζει το πιστοποιητικό, (για παράδειγμα, CN=Γεώργιος Παπαδόπουλος, O= Γ.Ν. Παπανικολάου, OU=Νοσοκομεία, ST= Θεσσαλονίκη, O=Τομέας Υγείας, C=GR)

***Subject Public Key Information:*** Αναγνωριστικά για το δημόσιο κλειδί, τον αλγόριθμο του κλειδιού και άλλες πληροφορίες που μπορεί να είναι απαραίτητες.

***Issuer unique identifier*** *(στις εκδόσεις 2 και 3 μόνο):* Αναγνωριστικό της Αρχής που εκδίδει το πιστοποιητικό.

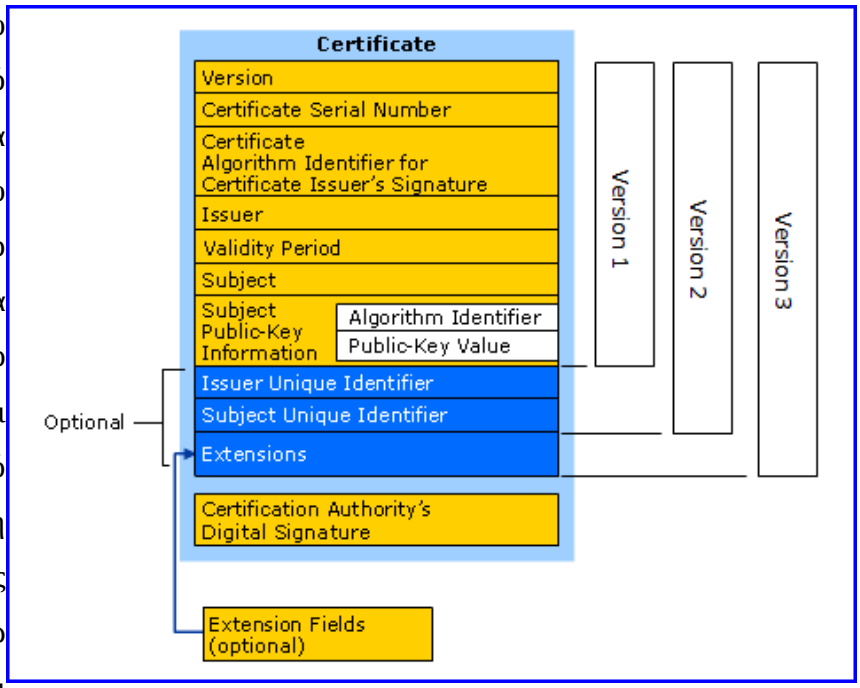
***Subject unique identifier*** *(στις εκδόσεις 2 και 3 μόνο):* Αναγνωριστικό της οντότητας της οποίας το δημόσιο κλειδί αναγνωρίζει το πιστοποιητικό.

***Extensions*** *(στην έκδοση 3 μόνο):* Ένα άλλο σημαντικό χαρακτηριστικό των X.509 πιστοποιητικών είναι η επιπρόσθετη λειτουργικότητα (functionality) που προσφέρεται από τις «Κανονικές Προεκτάσεις» (Standard Extensions). Τα extensions είναι στην ουσία πεδία που παρέχουν διάφορους ελέγχους για τη διοίκηση και διαχείριση (management and administrative controls), οι οποίοι είναι χρήσιμοι για την πιστοποίηση που χρησιμοποιείται για διάφορους σκοπούς σε μεγάλης κλίμακας περιβάλλοντα. Οι κανονικές προεκτάσεις (standard extensions) περιέχουν πληροφορία που σχετίζεται με τα κλειδιά, ενημέρωση για την πολιτική (policy information), χαρακτηριστικά πεδία για τον εκδότη και τον κάτοχο του πιστοποιητικού, περιορισμούς για το μονοπάτι πιστοποίησης (certification path constraints) και αυξημένη λειτουργικότητα όσον αφορά τις λίστες ανάκλησης πιστοποιητικών CRL. Μερικά παραδείγματα που συναντώνται συχνά είναι: KeyUsage (περιορίζει την χρήση του κλειδιού μόνο για συγκεκριμένες ενέργειες), Alternative Names (εναλλακτικά ονόματα που μπορεί να σχετίζονται με αυτό το δημόσιο κλειδί, όπως email, διευθύνσεις ιστοσελίδων κ.λ.π.). Αυτά τα extensions μπορούν να χαρακτηριστούν ως κρίσιμα (critical) έτσι ώστε να ελέγχονται και να είναι υποχρεωτική η χρήση τους. Για παράδειγμα αν το KeyUsage χαρακτηριστεί ως κρίσιμο και έχει την τιμή “keyCertSign” τότε εάν επιχειρηθεί να χρησιμοποιηθεί αυτό το πιστοποιητικό σε μια επικοινωνία με SSL, θα απορριφθεί, αφού η τιμή του υποδηλώνει ότι το ιδιωτικό κλειδί πρέπει να χρησιμοποιείται μόνο για την υπογραφή πιστοποιητικών και όχι για χρήση με SSL.

Τέλος υπογραφή για όλα τα παραπάνω πεδία

Το πρότυπο X.509 v3 προέβλεψε όχι μόνο για τα «standard» extensions αλλά και για «private» extensions που ορίζονται από τον χρήστη. Επομένως, οι χρήστες μπορούν να κατασκευάσουν τα δικά τους extensions και με αυτό τον τρόπο να προσθέσουν επιπλέον λειτουργικότητα στα πρότυπα.

Έχει προταθεί αυτά τα extensions να παρέχονται από τα πιστοποιητικά που εκδίδονται από τα ευρωπαϊκά PKI. Με τον τρόπο αυτό θα παρέχεται στους χρήστες η δυνατότητα να προσαρμόζουν τα πιστοποιητικά τους στις δικές τους ιδιαίτερες ανάγκες. Ένα άλλο σημαντικό θέμα όσον αφορά τα extensions είναι το ζήτημα της *κρισιμότητας (criticality)*. Η *κρισιμότητα* είναι μια δυαδική τιμή (αληθές ή ψευδές) που έχει ανατεθεί σε κάθε extension από το TTP. Όταν ένα συγκεκριμένο extension έχει αληθή τιμή *κρισιμότητας* σημαίνει ότι κάθε οντότητα που επικυρώνει το πιστοποιητικό πρέπει να έχει γνώση για τους σκοπούς που χρησιμοποιείται αυτό το extension και πληροφορία για το πως πρέπει να το χειριστεί. Αν δεν συμβαίνει αυτό, τότε το πιστοποιητικό θεωρείται άκυρο. Αν η τιμή του extension είναι ψευδής τότε η παραπάνω προϋπόθεση είναι προαιρετική.




*Σχήμα 2.7: Μορφή X.509 Πιστοποιητικού (X.509 Certificate format)*

Έχει προταθεί ότι κάθε TTP θα πρέπει να αναθέτει τιμή κατά βούληση.

# ΚΕΦΑΛΑΙΟ 3

# PUBLIC KEY INFRASTRUCTURE (PKI)

## 3.1 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. Χάρη σε αυτούς τους μηχανισμούς, μπορούν να επιτευχθούν οι βασικοί στόχοι ασφάλειας των πληροφοριακών συστημάτων, που είναι η εγγύηση της αυθεντικότητας (authentication), η διαφύλαξη της ακεραιότητας (integrity) και η τήρηση της εμπιστευτικότητας (confidentiality).

Η Υποδομή Δημοσίου Κλειδιού PKI είναι απαραίτητη για να δημιουργήσει ένα αξιόπιστο περιβάλλον για ασφαλείς συναλλαγές και επικοινωνίες τόσο για άτομα όσο και για οργανισμούς. Καθώς όλο και περισσότεροι οργανισμοί παγκοσμίως αντιλαμβάνονται τις δυνατότητες που τους παρέχει το Internet και αρχίζουν να επενδύουν σε αυτό, η ανάγκη για ταυτοποίηση και πιστοποίηση στις ηλεκτρονικές συναλλαγές έχει γίνει πολύ σημαντική. Η φυσική ανωνυμία που παρέχει το Internet, όπου τα άτομα ως ταυτότητα έχουν συνήθως μια ηλεκτρονική διεύθυνση, είναι το κύριο εμπόδιο στη χρήση των ψηφιακών δικτύων για τους οργανισμούς. Για να ξεπεραστούν αυτά τα προβλήματα αξιοπιστίας χρησιμοποιείται η Υποδομή Δημοσίου Κλειδιού. Οι Αρχές Πιστοποίησης ελέγχουν την Υποδομή Ασφάλειας που χρησιμοποιεί η Ασύμμετρη Κρυπτογραφία.

Σε ένα δίκτυο με Υποδομή Δημοσίου Κλειδιού υπάρχουν σχέσεις εμπιστοσύνης. Οι εγγραφόμενοι δημιουργούν σχέση εμπιστοσύνης με την Αρχή Πιστοποίησης CA. Οι CAs με τη σειρά τους δημιουργούν σχέση εμπιστοσύνης με άλλες Αρχές Πιστοποίησης για να κάνουν δυνατή την ασφαλή επικοινωνία μεταξύ διαφορετικών περιοχών (domains) στα πλαίσια του PKI. Σε μια συναλλαγή μεταξύ δυο ατόμων που είναι άγνωστα μεταξύ τους οι Αρχές

Πιστοποίησης λειτουργούν σαν έμπιστες τρίτες οντότητες (Trusted Third Parties). Όταν η συναλλαγή γίνεται μεταξύ δύο πλευρών που είναι άγνωστες μεταξύ τους, ένα πιστοποιητικό υπογεγραμμένο και επιβεβαιωμένο είναι αρκετό για να δημιουργηθεί σχέση εμπιστοσύνης μεταξύ των δύο αυτών πλευρών.

Χρησιμοποιείται ακόμη για την αναγνώριση πιθανών απειλών για την ασφάλεια και επίσης παρέχει υπηρεσίες ψηφιακής χρονοσφραγίδας (digital timestamping services). Μπορεί επίσης να χρησιμεύσει για την ασφαλή αποθήκευση της πληροφορίας.

## 3.2 Δομικά Μέρη της Υποδομής Δημοσίου Κλειδιού στην υγεία

Οι υπηρεσίες πιστοποίησης (Certificate Services) που απαιτούνται για την πιστοποίηση ιατρικού προσωπικού σε ένα δίκτυο τηλεματικών υπηρεσιών στην υγεία βασίζονται στην Υποδομή Δημοσίου Κλειδιού PKI.
Η Υποδομή Δημοσίου Κλειδιού για ένα δίκτυο τηλεματικών υπηρεσιών στην υγεία αποτελείται από:

• Αρχές Πιστοποίησης (CAs), οι οποίες ελέγχουν και διαχειρίζονται την Υποδομή Δημοσίου Κλειδιού PKI του τηλεματικού δικτύου υγείας, εκδίδουν πιστοποιητικά ιατρικού προσωπικού, και επιβάλλουν πολιτικές στην περιοχή τους (domain). Το σύστημα ασφαλείας τηλεματικού δικτύου υγείας μπορεί ανάλογα με την πολιτική πιστοποίησης να έχει μια ή περισσότερες Αρχές Πιστοποίησης.

• Αρχές εγγραφής (RAs), που ενεργούν εκ μέρους των Αρχών Πιστοποίησης (CAs) για να δηλώνουν τους επαγγελματίες υγείας στην περιοχή του τηλεματικού δικτύου που διαχειρίζεται η Αρχή Πιστοποίησης.

• Συστήματα διαχείρισης πιστοποιητικών (Certificate management systems/CMS) για τη διαχείριση των πιστοποιητικών των επαγγελματιών υγείας καθ’ όλη τη διάρκεια

που είναι σε ισχύ. 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.

## 3.3 Υπηρεσίες πιστοποίησης Ιατρικού προσωπικού

### 3.3.1 Ηλεκτρονική δήλωση (Electronic registration)

Ως Αρχή Εγγραφής (Registration Authority) μπορεί να θεωρηθεί η υπηρεσία που προσφέρεται από ένα εξουσιοδοτημένο προσωπικό που έχει ως έργο του να συλλέγει τα απαραίτητα έγγραφα πιστοποιητικά που πρέπει να προσκομίσουν οι επαγγελματίες υγείας για να αποδείξουν την ταυτότητα και την ιδιότητα τους και να ελέγχει την αυθεντικότητα τους. Έπειτα προωθούνται τα απαραίτητα στοιχεία στις Αρχές Πιστοποίησης για να εκδοθούν τα Ηλεκτρονικά Πιστοποιητικά για τους επαγγελματίες υγείας.

Σε πολλές περιπτώσεις ένας επαγγελματίας υγείας είναι δηλωμένος (registered) σαν χρήστης σε ορισμένες ιατρικές εφαρμογές. Ο όρος εφαρμογή (application) χρησιμοποιείται με την ευρύτερη έννοια. Μπορεί π.χ. να έχει πρόσβαση σε ένα τοπικό και σε ένα καθολικό πληροφοριακό σύστημα. Για την δήλωση του ως χρήστης (user registration) ο επαγγελματίας υγείας πρέπει να αποδείξει την ταυτότητα του και την ιδιότητα του ως επαγγελματίας υγείας. ***Απαιτείται η απόδειξή και των δύο.***

Μια προσέγγιση είναι να εκδίδονται οι εξουσιοδοτήσεις 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. Ένα πλεονέκτημα που έχουμε επειδή χρησιμοποιούμε τη γενική δομή του X.509 είναι ότι

υπάρχει πληθώρα διάφορων διαθέσιμων προϊόντων που μπορούν να χρησιμοποιηθούν. Για παράδειγμα 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.

### 3.3.2 Ονομασία (Naming)

Ακόμη καλό είναι 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 προτείνεται για ονομασία είναι το ιεραρχικό σχήμα του ονοματολογικού δένδρου του X.500 γιατί δίνει τη δυνατότητα να υποστηριχτούν 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.

### 3.3.3 Φάσεις Εξατομίκευσης Έξυπνης Κάρτας

*1. Εισαγωγή των δεδομένων για τον χρήστη*

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.

### 3.3.4 Δομή Πιστοποιητικού Ταυτότητας Επαγγελματία Υγείας

Το πρότυπο X.509 συνίσταται για τη δομή (format) των πιστοποιητικών των επαγγελματιών υγείας. Συγκεκριμένα επιλέγεται η δομή του πιστοποιητικού X.509-v3.

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

Τα πιστοποιητικά δημοσίων κλειδιών περιέχουν τις εξής πληροφορίες:

Α) Τον αριθμό έκδοσης (version number) του πιστοποιητικού (συνήθως X.509 version3)

Β) Το σειριακό αριθμό (serial number) του πιστοποιητικού

Γ) Το όνομα του αλγόριθμου που χρησιμοποιείται για την υπογραφή του πιστοποιητικού (Πιο ευέλικτοι και ταυτόχρονα ασφαλείς, ο αλγόριθμος σύνοψης μηνύματος SHA-1 και ο RSA σαν κρυπτογραφικός αλγόριθμος)

Δ) Το όνομα της Αρχής Πιστοποίησης που έχει υπογράψει και εκδώσει το πιστοποιητικό (διακεκριμένο όνομα X.500)

Ε) Το χρονικό διάστημα ισχύος του πιστοποιητικού (συνήθως ενός έτους)

Στ) Το όνομα του κατόχου του πιστοποιητικού (διακεκριμένο όνομα X.500)

Ζ) Το δημόσιο κλειδί του κατόχου του πιστοποιητικού και τον αλγορίθμο με τον οποίο χρησιμοποιείται το δημόσιο κλειδί (προτείνεται ο RSA)

Η) Το αναγνωριστικό του κλειδιού της Αρχής Πιστοποίησης, το οποίο δίνει τη δυνατότητα να προσδιοριστεί το δημόσιο κλειδί της Αρχής Πιστοποίησης με το οποίο υπογράφτηκε το πιστοποιητικό. Αυτό το πεδίο χρησιμοποιείται μόνο αν η Αρχή Πιστοποίησης έχει πολλαπλά κλειδιά για να υπογράφει διαφορετικές κατηγορίες πιστοποιητικών.

Θ) Πληροφορία για τη χρήση του κλειδιού που περιγράφει τους σκοπούς που το πιστοποιημένο δημόσιο κλειδί μπορεί να χρησιμοποιηθεί (προαιρετικό). Χρησιμοποιείται όταν το κλειδί χρησιμοποιείται για συγκεκριμένους σκοπούς μόνο και αν η Αρχή Πιστοποίησης θέλει να τους προσδιορίσει όπως η υπογραφή ιατρικών πράξεων και αποκρυπτογράφηση μηνυμάτων.

Ι) 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).

Ια) Τα σημεία διανομής Λιστών Ακύρωσης Πιστοποιητικών (CRL distribution points) τα οποία προσδιορίζουν πως και που μπορούμε να λάβουμε πληροφορία για τις Λίστες Ακύρωσης Πιστοποιητικών

### 3.3.5 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

#### 3.3.5.1 Δημιουργία Πιστοποιητικών επαγγελματιών υγείας

Ανάλογα με την πολιτική της, η Αρχή Πιστοποίησης του τηλεματικού δικτύου υγείας μπορεί να επιτρέπει τη χρήση του ίδιου κλειδιού σε εφαρμογές διαφορετικού τύπου, ή να χρησιμοποιούνται διαφορετικά κλειδιά σε διαφορετικές εφαρμογές. Συνίσταται η χρησιμοποίηση διαφορετικών κλειδιών για λόγους μεγαλύτερης ασφάλειας. Σε αυτήν την περίπτωση η Αρχή Πιστοποίησης πρέπει να εκδίδει ένα ξεχωριστό πιστοποιητικό, που να είναι ανάλογο με τους σκοπούς χρήσης του κάθε δημόσιου κλειδιού του επαγγελματία υγείας. Ακριβώς το τι δεδομένα χρειάζονται για να φτιαχτεί ένα πιστοποιητικό, εξαρτάται από τη χρήση του δημόσιου κλειδιού που πιστοποιεί. Όμως τα βήματα που απαιτούνται είναι σχεδόν τα ίδια.

#### 3.3.5.1.1 Επικύρωση δεδομένων και συντακτικός έλεγχος (Data validation and syntax control)

Όταν τα δεδομένα που απαιτούνται για να κατασκευαστεί ένα πιστοποιητικό συλλέγονται, πρέπει να επικυρωθούν. Η επικύρωση και ο έλεγχος των στοιχείων γίνεται από την εκάστοτε Αρχή Εγγραφής.

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

Όλα τα πιστοποιητικά των επαγγελματιών υγείας που δημιουργούνται πρέπει να είναι μοναδικά. Στη γενική περίπτωση, η μοναδικότητα εξασφαλίζεται 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.

Σε τέτοιες περιπτώσεις πρέπει να διατηρείται ένας κατάλογος (record) των πιστοποιητικών που έχουν δημιουργηθεί προηγουμένως, ή τουλάχιστον να αρχειοθετούνται τα ονόματα των επαγγελματιών υγείας στα οποία εκδόθηκαν πιστοποιητικά.

#### 3.3.5.1.3 Λειτουργία δημιουργίας πιστοποιητικών (Certificate generation function)

Τα πιστοποιητικά δημοσίων κλειδιών είναι σχεδιασμένα να δημιουργούν κλειδιά κατά τη διάρκεια της διαδικασίας δημιουργίας του πιστοποιητικού ή μπορούν και να χρησιμοποιούν κλειδιά που έχουν δημιουργηθεί από πριν, ανάλογα με την πολιτική που ακολουθεί το τηλεματικό δίκτυο υγείας.

Εφόσον η συλλογή των δεδομένων που σχηματίζουν ένα πιστοποιητικό προστατεύεται από κρυπτογραφικά μέσα, πρέπει να πακεταριστεί και να κωδικοποιηθεί σύμφωνα με το πρότυπο του X.509 v3 που έχει επιλεγεί. Τα κωδικοποιημένα δεδομένα μετά θα υπογραφούν με τον κατάλληλο αλγόριθμο (SHA-1 αλγόριθμος σύνοψης, και RSA

κρυπτογραφικός αλγόριθμος). Τα κωδικοποιημένα δεδομένα μαζί με την υπογραφή της Αρχής Πιστοποίησης του τηλεματικού δικτύου υγείας, κωδικοποιούνται περαιτέρω όπως ορίζει το πρότυπο X.509 v3. Το πιστοποιητικό ιατρικής ταυτότητας είναι το δυαδικό αλφαριθμητικό (binary string) που λαμβάνεται σαν αποτέλεσμα.

### 3.3.5.2 Διανομή, αποθήκευση και ανάκτηση πιστοποιητικών επαγγελματιών υγείας

Η αποθήκευση των πιστοποιητικών μόνο σε κάρτες όμως μπορεί να μην είναι αρκετή. Μερικοί λόγοι είναι ότι:

1) Ένα πιστοποιητικό δεν πρέπει να είναι κρυφό. Είναι αδύνατο να διαχειριστείς ένα πιστοποιητικό, χωρίς αυτό να αποκαλυφθεί.
2) Δεδομένης της μικρής χωρητικότητας της μνήμης των έξυπνων καρτών, μόνο μικρός αριθμός πιστοποιητικών μπορεί να αποθηκευτεί σε κάρτες.
3) Η έκδοση του πιστοποιητικού δεν συνεπάγεται απαραίτητα την ύπαρξη έξυπνων καρτών σε συγκεκριμένα μέρη για να γίνει η αποθήκευση.
4) Μόλις εκδοθεί το πιστοποιητικό, πρέπει να διανεμηθεί σε βάση δεδομένων δημόσιας πρόσβασης. Η αποθήκευση των πιστοποιητικών σε κάρτες είναι μια επιπλέον απαίτηση. Αυτή η αποθήκευση διευκολύνει τη διαθεσιμότητα σε διάφορα σενάρια εφαρμογών και δεν έχει καμιά επίπτωση σε θέματα ασφαλείας. Αυτό συμβαίνει γιατί το πιστοποιητικό είναι πάντα υπογεγραμμένο άρα μπορεί να διαπιστωθεί εάν δέχθηκε επίθεση. Συνεπώς δεν απαιτείται επιπλέον ασφάλεια κατά την αποθήκευση του.
5) Ο παραλήπτης δεν αρκεί να γνωρίζει το πιστοποιητικό του αποστολέα αλλά και όλα τα πιστοποιητικά του πλήρους μονοπατιού πιστοποίησης από τον αποστολέα προς τα πάνω έως και την Αρχή Πιστοποίησης της οποίας το δημόσιο κλειδί είναι αυθεντικά διαθέσιμο στον παραλήπτη.
6) Τα πιστοποιητικά πρέπει να έχουν χρονσφραγίδα (time-stamp) και να μπορούν να ανακληθούν. Συνεπώς, ο παραλήπτης ενός πιστοποιητικού πρέπει να έχει πρόσβαση στην αντίστοιχη λίστα ανάκλησης. Οι τελευταίες (up-to-date) λίστες ακύρωσης πρέπει

να δίνονται όχι από τον ίδιο τον αποστολέα αλλά από κάποιον άλλον. Έτσι, πρέπει να χρησιμοποιεί τις υπηρεσίες κατάλογου (directory service) οπωσδήποτε. Μία παρεμφερής υπηρεσία μπορεί να διανέμει τα πιστοποιητικά που απαιτούνται εξίσου καλά. Η αποθήκευση των λιστών ακύρωσης σε κάρτες δεν είναι ρεαλιστική.

Άρα 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 έναν ασφαλή χώρο αποθήκευσης και σε εφεδρικό αντίγραφο, για την περίπτωση που πρέπει να ανακτηθούν λόγω βλάβης του καταλόγου.

### 3.3.5.3 Ακύρωση πιστοποιητικών επαγγελματιών υγείας

Τα πιστοποιητικά περιέχουν την ημερομηνία λήξης τους, μετά την οποία δεν εγγυόνται πλέον την αυθεντικότητα της πληροφορίας που πιστοποιούν. Υπάρχουν διάφορες περιστάσεις, που όταν συμβούν σ' ένα πιστοποιητικό επαγγελματία υγείας δεν πρέπει να δηλώνεται πλέον ως έγκυρο έστω και αν δεν έχει λήξει η κανονική περίοδος εγκυρότητας του.

Περιπτώσεις που προκαλούν την ανάκληση του πιστοποιητικού ενός επαγγελματία υγείας είναι αν το ιδιωτικό κλειδί χαθεί ή εκτεθεί σε κινδύνους, αν αλλάξει η κατάσταση του ιδιοκτήτη του πιστοποιητικού (όταν αλλάζουν οι ιατρικές αρμοδιότητες του κατόχου του), ή αν μεταβληθεί κάποια άλλη πληροφορία του πιστοποιητικού του επαγγελματία υγείας. Τα πιστοποιητικά που έχουν ανακληθεί αποθηκεύονται σαν μία υπογεγραμμένη δομή δεδομένων, που ονομάζεται Λίστα Ανάκλησης Πιστοποιητικών (Certificate Revocation List/ CRL). Υπενθυμίζουμε ότι η CRL είναι μια λίστα που περιέχει τον σειριακό αριθμό των πιστοποιητικών που έχουν ανακληθεί. Η CRL δημιουργείται και συντηρείται από την Αρχή Πιστοποίησης του δικτύου τηλεματικών υπηρεσιών στην υγεία για τα πιστοποιητικά που εκδίδει η ίδια. Οι Λίστες Ανάκλησης Πιστοποιητικών πρέπει να έχουν χρονοσφραγίδα (time-stamp) και να έχουν υπογραφεί από την Αρχή Πιστοποίησης του Τηλεματικού δικτύου.

#### 3.3.5.3.1 Δομή λίστας ανάκλησης πιστοποιητικών επαγγελματιών υγείας

Προτείνεται η μορφή CRL version 2 για τις Λίστες Ανάκλησης των Πιστοποιητικών των επαγγελματιών υγείας. Η μορφή αυτή αντιστοιχεί στο πιστοποιητικό X.509 version 3 που έχει επιλεγεί για τα πιστοποιητικά των επαγγελματιών υγείας.

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

- Αριθμό έκδοσης του CRL (version 2)
- Όνομα του αλγόριθμου ο οποίος χρησιμοποιείται για να υπογραφεί το CRL (προτείνεται ο MD5 με RSA-Encryption)
- Όνομα της οντότητας που έχει υπογράψει και εκδώσει τη CRL
- Η ημερομηνία έκδοσης της CRL
- Η ημερομηνία που η επόμενη CRL θα εκδοθεί
- Η λίστα των σειριακών αριθμών των πιστοποιητικών των ιατρικών επαγγελματιών 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

#### 3.3.5.3.2 Συντήρηση Διανομή και Αποθήκευση λίστας ανάκλησης πιστοποιητικών επαγγελματιών υγείας

Οι CRLs και τα πιστοποιητικά δημόσιου κλειδιού πρέπει να ενημερώνονται τακτικά από την Αρχή Πιστοποίησης του Τηλεματικού Δικτύου, για να εξασφαλιστεί ότι οι χρήστες

έχουν την πιο πρόσφατη πληροφορία. Το χρονικό διάστημα της ανανέωσης της CRL είναι μέρος της πολιτικής της Αρχής Πιστοποίησης του δικτύου υγείας. Προτείνεται η CRL να ενημερώνεται στο δίκτυο μας κάθε ώρα.

Η CRL πρέπει να εκδίδεται έτσι ώστε να είναι διαθέσιμη στους χρήστες του τηλεματικού δικτύου υγείας και αυτοί να μπορούν να ελέγξουν την εγκυρότητα των πιστοποιητικών. Επειδή η CRL περιέχει την ημερομηνία και την ώρα που εκδόθηκε καθώς και την ημερομηνία που θα εκδοθεί η επόμενη CRL, ο χρήστης του τηλεματικού δικτύου μπορεί να αποφασίσει αν το αντίγραφο της CRL ισχύει ακόμη. Όμως, είναι ευθύνη του χρήστη να ελέγξει την πρόσφατη λίστα ανάκλησης για να μπορεί να είναι σίγουρος για την εγκυρότητα ενός πιστοποιητικού. Το πλεονέκτημα αυτής της μεθόδου ανάκλησης είναι ότι οι Λίστες Ανάκλησης Πιστοποιητικών μπορούν να διανέμονται με ακριβώς τα ίδια μέσα όπως και τα πιστοποιητικά, δηλαδή μέσω μη έμπιστων μέσων επικοινωνίας και συστήματα εξυπηρετητών.

Ένα πιθανό πρόβλημα που υπάρχει με τα CRLs είναι ο κίνδυνος το CRL να γίνει υπερβολικά μεγάλο. Στις εκδόσεις του 1988 και 1993 του X.509, η CRL για τα πιστοποιητικά των τελικών χρηστών έπρεπε να καλύψουν μία Αρχή Πιστοποίησης. Υπάρχει περίπτωση αυτοί οι χρήστες του τηλεματικού δικτύου υγείας να είναι χιλιάδες. Άρα υπάρχει ο κίνδυνος η CRL των επαγγελματιών υγείας να γίνει πάρα πολύ μεγάλη και να δημιουργεί προβλήματα μετάδοσης και αποθήκευσης. Με το version 2 CRL format, το οποίο επιλέξαμε, είναι δυνατό να διαιρεθεί ο συνολικός πληθυσμός των πιστοποιητικών αυθαίρετα σε ένα αριθμό από μέρη, και κάθε μέρος να έχει ένα δικό του σημείο διανομής από όπου θα διανέμονται οι αντίστοιχες CRLs.

Άρα, το μέγιστο μέγεθος της CRL μπορεί να ελεγχθεί από την Αρχή Πιστοποίησης του τηλεματικού δικτύου υγείας. Ξεχωριστά σημεία διανομής CRL μπορούν επίσης να υπάρχουν για διάφορους άλλους λόγους.

### 3.4.1 Υπηρεσία Προστασίας Εμπιστευτικών Ιατρικών Δεδομένων με χρήση USB Token

Η επεξεργασία ιατρικών δεδομένων από ιατρούς ή άλλα πρόσωπα που παρέχουν υπηρεσίες υγείας απαιτεί την εφαρμογή σημαντικών διαδικασιών που θα εξασφαλίσουν το απόρρητο των συγκεκριμένων πληροφοριών. Σκοπός των διαδικασιών αυτών είναι να διαφυλαχθούν δεδομένα που καλύπτονται από το ιατρικό απόρρητο ή άλλο απόρρητο που προβλέπει ο νόμος ή κώδικας δεοντολογίας ώστε τα δεδομένα αυτά να μην διαβιβάζονται ούτε κοινοποιούνται σε τρίτους χωρίς προηγούμενη έγγραφη ανάθεση.

Προκειμένου να διασφαλισθεί το απόρρητο της επεξεργασίας Ιατρικών δεδομένων έχουν πλέον υιοθετηθεί και εφαρμόζονται αυστηροί νόμοι τόσο στην Ευρωπαϊκή Ένωση όσο και στην Ελλάδα. Ειδικότερα η Οδηγία της Ευρωπαϊκής Ένωσης 95/46/EC ορίζει συγκεκριμένους κανόνες που θα πρέπει να εφαρμόζονται προκειμένου να διασφαλισθεί η ακεραιότητα και η εμπιστευτικότητα αυτών. Επίσης ο Νόμος 2472/1997 περί προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα ορίζει αυστηρές κυρώσεις σε περίπτωση μη συμμόρφωσης σε όσα αναφέρονται σε αυτόν. [Dir 95/46/EC]

Μια εφαρμογή Προστασίας Εμπιστευτικών Ιατρικών Δεδομένων βασίζεται σε διεθνή πρότυπα ασφάλειας και εναρμονίζεται με τις απαιτήσεις Εθνικών και Ευρωπαϊκών κανονισμών σχετικά με την διαφύλαξη της Εμπιστευτικότητας Ιατρικών Δεδομένων που καταχωρούνται σε Πληροφοριακά Συστήματα.

Η συγκεκριμένη εφαρμογή βασίζεται σε τεχνολογική λύση του κατασκευαστικού οίκου Utimaco με το προϊόν SafeGuard Easy. Η λύση SafeGuard Easy της Utimaco, προσφέρει απόλυτη κρυπτογράφηση των δεδομένων και προστασία πρόσβασης στα συστήματα από μη εξουσιοδοτημένους χρήστες. Ο μεγάλος αριθμός εγκαταστάσεων που έχει γίνει παγκοσμίως σε περισσότερα από 2.5 εκατομμύρια laptops και PCs καθώς και η πιστοποίηση του προϊόντος με τα αυστηρότερα πρότυπα ασφάλειας Common Criteria EAL3 & FIPS 140-2 επιβεβαιώνουν την επιλογή της βέλτιστης τεχνολογικής λύσης για την παροχή της υπηρεσίας.

Με την συγκεκριμένη λύση παρέχεται πλήρης προστασία από μη εξουσιοδοτημένη πρόσβαση σε συστήματα ακόμα και αν αυτά κλαπούν με απώτερο σκοπό την πρόσβαση σε

πληροφορίες που αποθηκεύονται σε σκληρούς δίσκους, μέσα μεταφοράς δεδομένων όπως USB sticks, floppy disks, συσκευές backup κλπ.

Η απόλυτη κρυπτογράφηση των δεδομένων και η προηγμένη ασφάλεια πρόσβασης κατά την εκκίνηση του συστήματος πριν την πρόσβαση στο λειτουργικό σύστημα με χρήση USB Token και Personal Identification Number (PIN), διασφαλίζουν το απόρρητο των πληροφοριών σε μη εξουσιοδοτημένους χρήστες.

Στο Ορλάντο το Μαρτίο του 2008 παρουσιάστηκε με επιτυχία από τους MEDNET και GE Healthcare εφαρμογή ταυτοποίησης χρήστη βασιζόμενη σε PKI πιστοποιητικό που επιτρέπει την πρόσβαση σε ιατρικούς φακέλους ασθενών μόνο από εξουσιοδοτημένους επαγγελματίες υγείας. Η παρουσίαση έδειξε ότι χρήστες με διαφορετικούς ρόλους (Χειριστές, νοσηλεύτριες, γραμματείς) θα μπορούσαν να έχουν πρόσβαση σε ιατρικά έγγραφα στα GE Healthcare συστήματα, χρησιμοποιώντας MEDNET ψηφιακά πιστοποιητικά που εκδίδονται και αποθηκεύονται σε μια έξυπνη κάρτα ή ένα USB token.

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.

### 3.4.2 Βασικά Χαρακτηριστικά eToken

- Pre-boot authentication με χρήση eToken
- Μερική ή πλήρης κρυπτογράφηση του σκληρού δίσκου ανεξαρτήτως file system (NTFS, FAT κλπ)
- Κρυπτογράφηση δεδομένων που περιέχονται σε εξωτερικές συσκευές αποθήκευσης
- Χρήση των πλέον ισχυρών αλγόριθμων κρυπτογράφησης AES (256 and 128 bit), IDEA (128 bit) κ.α
- Καταγραφή συμβάντων προσπαθειών παραβίασης του συστήματος
- Δυνατότητα πιστοποίησης σε 2ο επίπεδο στο λειτουργικό σύστημα με χρήση eToken και όχι απλού username & password
- Διάφανη λειτουργία χωρίς να απαιτείται τεχνογνωσία και παρέμβαση από τον χρήστη
- Πιστοποιημένη λύση κατά Common Criteria EAL3 & FIPS 140-2

# ΚΕΦΑΛΑΙΟ 4

## E – HEALTH

### 4.1 Ηλεκτρονική Υγεία

Στις μέρες μας γίνεται μεγάλη συζήτηση για την ηλεκτρονική υγεία (e-health), αλλά λίγοι είναι σε θέση να διατυπώσουν ένα σαφή ορισμό για αυτόν τον νέο όρο. Ο όρος αυτός, κυρίως από το 1999 και μετά, χρησιμοποιείται για να περιγράψει οτιδήποτε έχει σχέση με υπολογιστές και ιατρική. Πρόκειται για την απόρροια μιας προσπάθειας να επεκταθούν οι αρχές και οι «υποσχέσεις» του ηλεκτρονικού εμπορίου στο χώρο της υγείας και να τονιστούν οι νέες δυνατότητες που παρέχει το διαδίκτυο στο χώρο της ιατρικής περίθαλψης, οι οποίες μπορούν να συνοψιστούν ως εξής:

- Δυνατότητα των πολιτών να αλληλεπιδρούν online με τα συστήματά τους (B2C = “business to consumer”)
- Βελτιωμένες δυνατότητες μεταφοράς δεδομένων ανάμεσα σε οργανισμούς υγείας (B2B = “business to business”)
- Νέες δυνατότητες για peer-to-peer επικοινωνίας των πολιτών (C2C = “consumer to consumer”).

Αν επιχειρούσαμε έναν ευρύτερο ορισμό του όρου e-Health, αυτός θα μπορούσε να είναι κάπως έτσι:

*Η Ηλεκτρονική Υγεία (e-health) είναι ένας τομέας της ιατρικής πληροφορικής και των τηλεματικών εφαρμογών της, της δημόσιας υγείας και της βιομηχανίας, που αναφέρεται σε υπηρεσίες υγείας και πληροφορικής, οι οποίες προσφέρονται ή ενισχύονται μέσω του διαδικτύου και των σχετικών με αυτό τεχνολογιών.*

Τα κύρια χαρακτηριστικά της ηλεκτρονικής υγείας:

- ✓ ***Αποδοτικότητα (Efficiency):*** Μια από τις υποσχέσεις της ηλεκτρονικής υγείας είναι να αυξήσει την αποδοτικότητα της ιατρικής περίθαλψης, μειώνοντας το κόστος. Ένας πιθανός τρόπος μείωσης του κόστους είναι η αποφυγή διπλών ή μη απαραίτητων διαγνωστικών ή θεραπευτικών επεισοδίων μέσω επικοινωνίας ανάμεσα στους φορείς υγείας και τον πολίτη.
- ✓ ***Βελτίωση της ποιότητας περίθαλψης:*** Η αύξηση της αποδοτικότητας δεν μειώνει μόνο το κόστος αλλά βελτιώνει ταυτόχρονα και την ποιότητα. Η ηλεκτρονική υγεία μπορεί να βελτιώσει την ποιότητα της ιατρικής περίθαλψης επιτρέποντας για παράδειγμα συγκρίσεις ανάμεσα στους παροχείς υγείας.
- ✓ ***Επιστημονική τεκμηρίωση (Evidence based):*** Οι ενέργειες της ηλεκτρονικής υγείας πρέπει να τεκμηριώνονται με την έννοια ότι η αποδοτικότητά τους πρέπει να αποδεικνύεται με επιστημονικές μεθόδους.
- ✓ ***Ενδυνάμωση πολιτών και ασθενών:*** Καθιστώντας τις βάσεις δεδομένων υγείας και τον προσωπικό ηλεκτρονικό ιατρικό φάκελο προσβάσιμο από το διαδίκτυο, ανοίγονται νέοι ορίζοντες για ανθρωποκεντρικά συστήματα υγείας και διευκολύνεται ο ασθενής στις επιλογές του.
- ✓ ***Ενθάρρυνση νέων σχέσεων ασθενή και επαγγελματία υγείας,*** ώστε οι αποφάσεις να λαμβάνονται με κοινό τρόπο.
- ✓ ***Εκπαίδευση ιατρών και παραιατρικού προσωπικού από online πηγές*** (συνεχής ιατρική εκπαίδευση) ***αλλά και των πολιτών (***π.χ. ιατρικές πληροφορίες πρόληψης).
- ✓ ***Διευκόλυνση της ανταλλαγής της πληροφορίας και της επικοινωνίας με προτυποποιημένο τρόπο ανάμεσα στους φορείς υγείας.*** Με αυτό τον τρόπο υπάρχει μια μορφή διαλειτουργικότητας. Δίνεται η δυνατότητα προσπέλασης και ελέγχου σε δεδομένα όλων των συστημάτων με την ταυτόχρονη ύπαρξη ενός ενιαίου σημείου διαχείρισης και διοίκησης.
- ✓ ***Επέκταση της εμβέλειας της ιατρικής περίθαλψης πέρα από τα συμβατικά όρια,*** τόσο με την γεωγραφική όσο και με την μεταφορική έννοια του όρου. Οι πολίτες

έχουν τη δυνατότητα να χρησιμοποιούν online ιατρικές υπηρεσίες που παρέχονται από διεθνείς παροχείς. Οι υπηρεσίες αυτές είναι είτε συμβουλευτικές είτε και πιο ουσιαστικές, π.χ. προμήθεια φαρμακευτικών προιόντων.

- ✓ ***Ασφάλεια:*** Η ηλεκτρονική υγεία περιλαμβάνει νέες μορφές αλληλεπίδρασης ασθενή – ιατρού και δημιουργεί νέες προκλήσεις σε θέματα ασφαλείας όπως το ιατρικό απόρρητο.
- ✓ ***Ισότητα:*** Μια από τις υποσχέσεις της ηλεκτρονικής υγείας είναι η πιο ισότιμη ιατρική περίθαλψη.

## 4.2 Τηλεϊατρική

Σύμφωνα με την Παγκόσμια Οργάνωση Υγείας η Τηλεϊατρική είναι:

*Η παροχή ιατρικής περίθαλψης – σε περιπτώσεις που η απόσταση αποτελεί κρίσιμο παράγοντα – από όλους τους επαγγελματίες του χώρου της Υγείας χρησιμοποιώντας τεχνολογίες πληροφοριών και επικοινωνιών για την ανταλλαγή έγκυρης πληροφορίας για τη διάγνωση, αγωγή και πρόληψη ασθενειών, την έρευνα και εκτίμηση, όπως και την συνεχή εκπαίδευση των επαγγελματιών Υγείας των ατόμων και των κοινοτήτων τους.*

Ο όρος τηλεϊατρική, με την ευρύτερη έννοια, αναφέρεται στην εφαρμογή σύγχρονων τεχνολογιών των τηλεπικοινωνιών και της πληροφορικής, κυρίως προς την κατεύθυνση της αμφίδρομης επικοινωνίας με μετάδοση ήχου και εικόνας με στόχο την παροχή ιατρικής φροντίδας, σε απομακρυσμένους ασθενείς, της τηλεμετρίας και της διακίνησης της ιατρικής γνώσης μεταξύ των ιατρικών λειτουργών.

- Με τον όρο ιατρική πληροφορική αναφερόμαστε στο σύνολο των πληροφορικών τεχνολογιών (Συστήματα Η/Υ, βάσεις δεδομένων, Λογισμικό, εφαρμογές πολυμέσων, κλπ) που χρησιμοποιούνται στην παροχή υπηρεσιών υγείας και στην ιατρική εκπαίδευση.

- Με τον όρο τηλεϊατρική αναφερόμαστε στην χρήση των τηλεπικοινωνιών και πληροφορικής για την παροχή των παραπάνω υπηρεσιών. Λόγω του γεγονότος ότι οι περισσότερες τηλεϊατρικές εφαρμογές συμπεριλαμβάνουν στοιχεία ιατρικής πληροφορικής, η διάκριση των δύο είναι συχνά δύσκολη.

### 4.2.1 Τηλεϊατρική για την υποστήριξη διακομιστικών σταθμών

Στον Ελλαδικό χώρο σήμερα, οι υπηρεσίες άμεσης βοήθειας παρέχονται από το Εθνικό Κέντρο Άμεσης Βοήθειας (Ε.Κ.Α.Β.). Οι υπηρεσίες αυτές συνίστανται τόσο στην παροχή άμεσης βοήθειας για την προσωρινή ιατρική αντιμετώπιση του προβλήματος, όσο και στην κατά το δυνατόν υποστηριγμένη μεταφορά των ασθενών σε οργανωμένο χώρο επείγουσας ιατρικής όπως είναι οι σταθμοί πρώτων βοηθειών, τα εξωτερικά ιατρεία επειγόντων περιστατικών (Τ.Ε.Π.), οι μονάδες εντατικής θεραπείας (Μ.Ε.Θ.), τα χειρουργεία, οι χώροι 24ωρης νοσηλείας, κ.λ.π.

Από το χαρακτήρα της πρώτης φροντίδας, οι υπηρεσίες άμεσης βοήθειας αποτελούν αντικείμενο της επείγουσας ιατρικής. Τα προβλήματα επείγουσας ιατρικής στη χώρα μας εντείνονται από τη γεωγραφική ανομοιομορφία της Ελλάδας (ορεινά χωριά, μεγάλος αριθμός νησιών) και από την ανομοιόμορφη πληθυσμιακή κατανομή.

Η ποιότητα της περίθαλψης πρώτης φροντίδας του ασθενούς, κατά τη διαδικασία της διακομιδής του σε χώρο επείγουσας ιατρικής, εξαρτάται κυρίως από την σύμφωνα με το ιατρικό ιστορικό αρχική αντιμετώπιση του περιστατικού και τις πρωτοβουλίες που λαμβάνει το προσωπικό του διακομιστικού σταθμού. Στην πλειονότητα των περιστατικών, η αντιμετώπιση αυτή αφορά εξειδικευμένης μορφής περίθαλψη. Σε ορισμένα περιστατικά, η αντιμετώπιση αυτή αφορά σύνθετης μορφής περίθαλψη και επιβάλλεται η συνεργασία περισσοτέρων της μιας ιατρικών ειδικοτήτων. Βεβαίως, σε κάθε περίπτωση, είναι αναγκαία η γνώση του ιατρικού ιστορικού του ασθενούς κατά τη διαδικασία της παροχής πρώτης βοήθειας.

Όμως, όπως είναι γνωστό, οι ιατρικού περιεχομένου πληροφορίες βρίσκονται διασκορπισμένες σε διάφορες μορφές όπως επί παραδείγματι σε έντυπα, βιβλιοθήκες, αρχεία συνοικιακών ιατρών, αρχεία κλινικών, αρχεία Νοσοκομείων κ.λ.π. Επίσης, το ιστορικό υγείας

ενός πολίτη εξαρτάται από την χρονική περίοδο και το φορέα υγείας που αντιμετώπισε το πρόβλημά του. Δυστυχώς, με την πάροδο του χρόνου και κυρίως από την έλλειψη βοηθητικών χώρων (είναι σύνηθες φαινόμενο η έλλειψη αποθηκευτικών χώρων στα Νοσοκομεία) τα αρχεία αυτά καταστρέφονται, με αποτέλεσμα το νοσηλευτικό σύστημα σήμερα καθόλου ή σπανίως να χρησιμοποιεί το ιστορικό υγείας του πολίτη. Έτσι, στο σύνολο των περιπτώσεων, το ιστορικό γίνεται εκάστοτε γνωστό μόνο από τη μαρτυρία και τη δήλωση του πολίτη. Είναι προφανές ότι η εφαρμογή συγχρόνων τεχνολογιών στην ιατρική και ειδικότερα η τηλεϊατρική μπορεί να επιλύσει αυτά τα προβλήματα.

Έχει διαπιστωθεί η ανάγκη διασύνδεσης σε ενοποιημένο τηλεπικοινωνιακό δίκτυο των κεντρικών νοσοκομειακών μονάδων με περιφερειακά νοσοκομεία, κέντρα υγείας, σταθμούς πρώτων βοηθειών, αγροτικά ιατρεία κ.λ.π., σε συνδυασμό με την υποστήριξη των διακομιστικών σταθμών επειγόντων περιστατικών για τη λήψη βέλτιστης απόφασης σε σύντομο χρονικό διάστημα με χρήση ηλεκτρονικών υπολογιστών. Επίσης, έχει διαπιστωθεί η ανάγκη καταγραφής του ιατρικού ιστορικού όλων των Ελλήνων πολιτών (υποχρεωτική κάρτα υγείας με τον αντίστοιχο κωδικό αριθμό του πολίτη), ώστε κατά τη διάρκεια της διακομιδής του σε οργανωμένο χώρο επείγουσας ιατρικής να δίνεται η δυνατότητα παροχής σημαντικής και ουσιαστικής βοήθειας για τη μετέπειτα εξέλιξη της υγείας του από το προσωπικό του διακομιστικού σταθμού. Με τον τρόπο αυτό μπορεί να δοθεί η δυνατότητα συνεργασίας με τη μονάδα που θα υποδεχθεί τον ασθενή, ώστε να είναι κατάλληλα προετοιμασμένη για την άμεση αντιμετώπιση του περιστατικού, ή στη χειρότερη περίπτωση να έχει προετοιμαστεί η αναγκαία τεχνική υποστήριξη, χωρίς απώλεια πολύτιμου χρόνου (π.χ. εξετάσεις για ομάδα αίματος κ.λ.π).

Μέχρι σήμερα, υπάρχουν αρκετές περιπτώσεις απώλειας συνανθρώπων μας από την καθυστερημένη παροχή ουσιαστικής πρώτης φροντίδας, όπως αποκαλύπτεται από τα περιστατικά θανάτων κατά τη διάρκεια της διακομιδής ασθενών από ακριτικές περιοχές και μικρά νησιά σε οργανωμένα νοσοκομειακά κέντρα, που έρχονται στο φως της δημοσιότητας. Δεδομένου ότι η αξία της ανθρώπινης ζωής δεν είναι δυνατόν να κοστολογηθεί, μπορεί κανείς να οδηγηθεί στη διαπίστωση της αναγκαιότητας εφαρμογής της τηλεϊατρικής για την υποστήριξη διακομιστικών σταθμών σε εθνική κλίμακα.

## 4.3 Ηλεκτρονικός Φάκελος

Είναι κοινή διαπίστωση ότι ο όγκος των πληροφοριών που σχετίζονται με την φροντίδα του ασθενούς έχει αυξηθεί κατά πολύ τα τελευταία χρόνια, πράγμα που σε μεγάλο βαθμό οφείλεται στην ενσωμάτωση αυξημένου αριθμού εργαστηριακών και παρα-κλινικών εξετάσεων στους φακέλους των ασθενών. Επιπλέον, τα διαχειριστικά καθήκοντα των γιατρών γίνονται διαρκώς περισσότερα, καθώς η πολυπλοκότητα των ιδρυμάτων παροχής υπηρεσιών υγείας αυξάνει.

Φυσικό επακόλουθο είναι η αδυναμία δημιουργίας και διαχείρισης των "κλασσικών" φακέλων των ασθενών, που βασίζονται στην καταγραφή των δεδομένων σε χαρτί, συνοδευόμενο από τις σχετικές εξετάσεις. Τα λογισμικά Ηλεκτρονικού Ιατρικού Φακέλου (**ΗΙΦ**), αποτελούν συστήματα διαχείρισης ιατρικών φακέλων που βασίζονται σε ηλεκτρονικούς υπολογιστές. Ως εκ τούτου, η αποθήκευση και ανάκληση των δεδομένων γίνεται γρήγορα και με ασφάλεια. Επιπλέον, καθίσταται δυνατή η επεξεργασία των δεδομένων και η άμεση μεταφορά τους με ηλεκτρονικά μέσα, σε οποιαδήποτε απόσταση. Το σύστημα καταγραφής των δεδομένων που σχετίζεται με τους ασθενείς γίνεται πιο αποτελεσματικό, αλλά και εμπλουτίζεται εκμεταλλευόμενο τις δυνατότητες των νέων τεχνολογιών. Ο ΗΙΦ ενός ασθενούς πρέπει να περιέχει όλα τα δεδομένα που σχετίζονται με αυτόν, άσχετα με την μορφή στην οποία βρίσκονται:

• Το ιστορικό, η κλινική εξέταση και τα αποτελέσματα εργαστηριακών εξετάσεων, βρίσκονται σε μορφή κειμένου

• Οι απεικονιστικές εξετάσεις [ακτινογραφίες, τομογραφίες (αξονικές, μαγνητικές, απλές), υπέρηχοι κ.ο.κ.] βρίσκονται σε μορφή στατικών εικόνων

• Τα ηλεκτροκαρδιογραφήματα βρίσκονται σε μορφή βιο-σημάτων (ηλεκτρονικά κωδικοποιημένη έξοδος κάποιας καταγραφικής συσκευής)

• Τα αποτελέσματα ενδοσκοπικών εξετάσεων (γαστροσκόπηση, κωλονοσκόπηση κλπ.) βρίσκονται σε μορφή βίντεο

• Το ηχοκαρδιογράφημα βρίσκεται σε μορφή ήχου

Η συνήθης τακτική, είναι να συνοδεύουν τον φάκελο του ασθενούς οι αντίστοιχες εξετάσεις, στην μορφή με την οποία παράγονται από το Εργαστήριο (ακτινογραφικό φιλμ, έντυπα με αποτελέσματα βιοχημικών εξετάσεων, χαρτί ηλεκτροκαρδιογράφου κ.ο.κ.). Έτσι ο φάκελος καθίσταται ογκώδης, η πιθανότητα να χαθούν δεδομένα μεγαλύτερη, ενώ η χρονική συσχέτιση των διαφόρων εξετάσεων με το ιστορικό και την κλινική εξέταση δεν γίνεται άμεσα προφανής.

Σε έναν ΗΙΦ, όλα τα δεδομένα ενσωματώνονται στον φάκελο του ασθενούς χωρίς να παίζει σημαντικό ρόλο η μορφή τους. Σε διάφορα σημεία του κειμένου του ιστορικού και της κλινικής εξετάσεως ενσωματώνονται ακτινολογικές ή βιοχημικές εξετάσεις, πράγμα που κάνει αμέσως εμφανή την συσχέτιση των εν λόγω εξετάσεων με την γενικότερη κατάσταση του ασθενούς.

Αν και δεν υπάρχει μέχρι σήμερα ένα και μοναδικό πρότυπο στην ιατρική, ένας τέτοιος φάκελος χρειάζεται να συνδυάζει μια πλειάδα από διαφορετικού τύπου πληροφορίες. Αυτές οι πληροφορίες είναι:

- ✓ Δημογραφικά στοιχεία
- ✓ Ιατρικό ιστορικό – Παράγοντες κινδύνου (risk factors)
- ✓ Κλινικά δεδομένα φυσικής εξέτασης – διαγνώσεις και σημεία
- ✓ Νοσηλείες – Εγχειρήσεις
- ✓ Ιατροφαρμακευτική περίθαλψη
- ✓ Εργαστηριακές εξετάσεις (ανάλυση αίματος, ούρων, κλπ)
- ✓ Καταγραφές βιοδυναμικών (ηλεκτροκαρδιογράφημα, ηλεκτρομυογράφημα, κλπ.)
- ✓ Ιατρικές πράξεις
- ✓ Παραπεμπτικά – Γνωματεύσεις

- ✓ Διαγνωστικές εξετάσεις και ιατρικές εικόνες (Ακτινογραφίες, μαγνητικές τομογραφίες, αξονικές τομογραφίες, κλπ)
- ✓ Διαχειριστικά – οικονομικά στοιχεία ιατρικών πράξεων και νοσηλειών
- ✓ Πιθανά αρχεία παλιών ιατρικών φακέλων

Αν αναλύσουμε τα παραπάνω δεδομένα είναι εμφανές ότι ένας πλήρης ηλεκτρονικός ιατρικός φάκελος αποτελεί μια πολυμεσική οντότητα, η οποία αποτελείται από στοιχεία κειμένου, εικόνων, ήχων κλπ. Η κωδικοποίηση των στοιχείων αυτών αποτελεί ακόμα στοιχείο έρευνας καθώς προκύπτουν διαρκώς νέες τεχνολογίες διαχείρισης πληροφοριών. Αξίζει ωστόσο να σημειώσουμε τουλάχιστον τρεις προσπάθειες οι οποίες στοιχειοθετούν τον κορμό των σημερινών εφαρμογών και τη βάση για τις επερχόμενες βελτιωμένες κωδικοποιήσεις (metadata coding).

Αυτές είναι:

1. **Το πρωτόκολλο HL7 – Health Level 7**

2. **Το πρωτόκολλο DICOM 3.0** (Digital imaging communication in Medicine) με αντικείμενο τη διαχείριση ιατρικών εικόνων.

3. **Το Ευρωπαϊκό πρότυπο ENV 12265** το οποίο στηρίζεται στα ευρήματα των Ευρωπαϊκών έργων GEHR και NUCLEUS, και προτείνεται από την CEN TC251 (European Standardisation Committee).

**Αναλυτικότερη περιγραφή του ΗΙΦ**

***Σημείωση: Η περιγραφή βασίζεται στην αρχιτεκτονική Ηλεκτρονικού Ιατρικού Φακέλου που έχει προτείνει το Ευρωπαϊκό Ερευνητικό Πρόγραμμα Good European Health Record.***

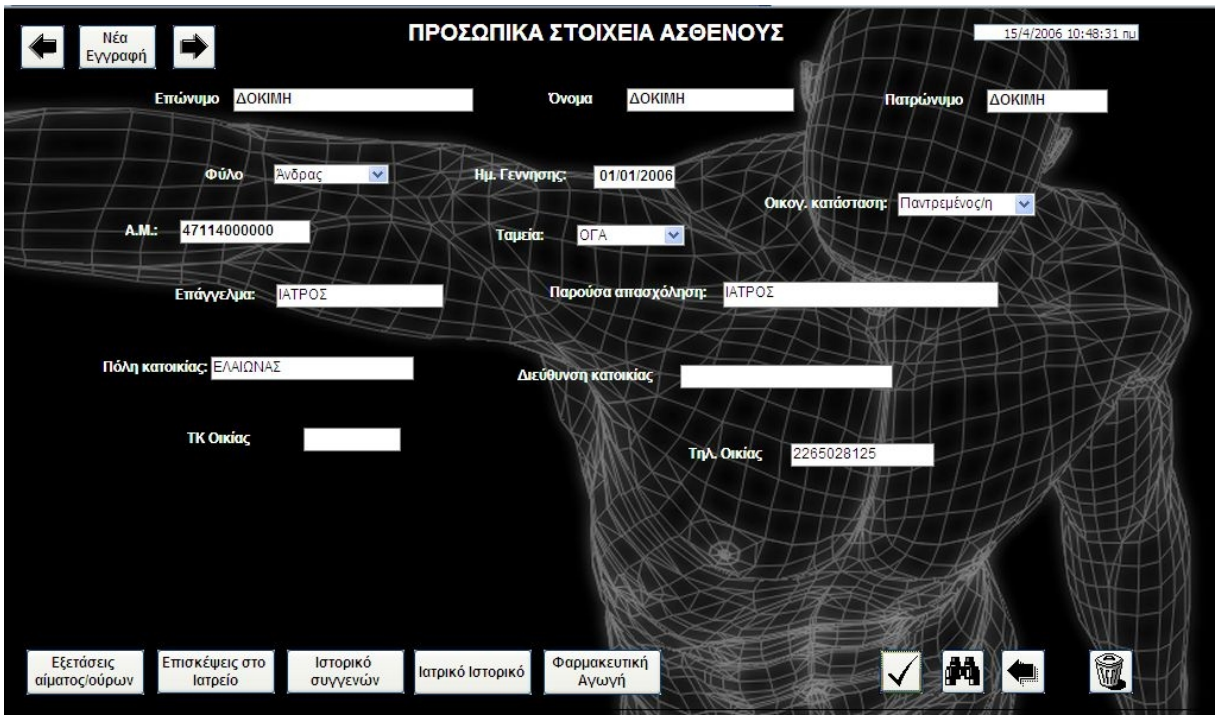
Ορισμός του Ιατρικού Φακέλου (κείμενο CEN/TC25/WG1/N8 της Ευρωπαϊκής Επιτροπής Προτυποποίησης):

*"Ο Ιατρικός Φάκελος είναι η "αποθήκη" όλων των πληροφοριών που αφορούν στο ιατρικό ιστορικό του ασθενούς. Αποτελεί επομένως την βάση της διάγνωσης και της θεραπευτικής αντιμετώπισης του ασθενούς αλλά και την βάση επιδημιολογικών ερευνών. Επιπλέον, παρέχει πληροφορίες διοικητικής, οικονομικής και στατιστικής φύσεως, καθώς και ποιοτικού ελέγχου".*

Ο φάκελος είναι ένα πρόγραμμα διαχείρισης βάσεως δεδομένων, αλλά όχι οποιοδήποτε πρόγραμμα. Εφόσον ο φάκελος του ασθενούς περιέχει δεδομένα διαφόρων μορφών, αυτά πρέπει να καταχωρηθούν στον ΗΙΦ με τέτοιο τρόπο, ώστε να βρίσκονται σε απόλυτη συσχέτιση μεταξύ τους, προκειμένου να διατηρηθούν οι πληροφορίες που εμπεριέχονται σε αυτή την συσχέτιση.

### 4.3.1 Ιατρικές Διαχειριστικές Πληροφορίες (Medical Administrative Information)

Το σύνολο των επαφών ενός φακέλου, μαζί με τις βασικές (αμετάβλητες) παραμέτρους του ασθενούς (ατομικό αναμνηστικό, κληρονομικό ιστορικό, ομάδα αίματος κλπ.) αποτελεί το ιατρικό τμήμα του φακέλου. Εκτός του ιατρικού, το διαχειριστικό τμήμα του φακέλου τον συμπληρώνει, αφού είναι εκείνο που περιέχει πληροφορίες όπως το όνομα και επώνυμο του ασθενούς, ασφαλιστικές πληροφορίες κ.τ.λ. Αφορά στις διοικητικές ενέργειες που σχετίζονται με τον ασθενή.




*Παράδειγμα ενός ιατρικού φακέλου ασθενή*

## 4.4 Νοσοκομειακά πληροφοριακά συστήματα

Τα πληροφοριακά συστήματα νοσοκομείου (ΠΣΝ) είναι μεγάλα, περίπλοκα συστήματα υπολογιστών που έχουν σχεδιαστεί για να βοηθούν στην επικοινωνία και στη διαχείριση των αναγκών πληροφόρησης ενός νοσοκομείου. Αποτελούν εργαλεία για ενδοτομεακή και διατομεακή χρήση. Ένα πληροφοριακό σύστημα νοσοκομείου έχει εφαρμογή σε θέματα εισαγωγής ασθενών, σε ιατρικά αρχεία, σε λογιστικές πληροφορίες, επιχειρησιακές υπηρεσίες, νοσηλευτική, εργαστήρια, ακτινολογικό, φαρμακείο, κεντρικές προμήθειες, διαιτολογικές υπηρεσίες, προσωπικό και μισθοδοσία. Πολλές άλλες εφαρμογές μπορούν να υπάρξουν για κάθε τμήμα και ουσιαστικά για κάθε σκοπό.

Οι εφαρμογές που αφορούν την εισαγωγή ασθενών περιλαμβάνουν προγραμματισμό ασθενών, προεισαγωγική φάση, φάση εισαγωγής, φάση εξόδου από το νοσοκομείο, μεταφορές και διαδικασίες καταγραφής. Ορισμένες εφαρμογές που αφορούν ιατρικά αρχεία περιλαμβάνουν την τήρηση γενικού μητρώου ασθενών, έγγραφα, αλληλογραφία και

διαδικασίες εντοπισμού ιατρικών αρχείων. Οι επιχειρησιακές και λογιστικές διαδικασίες περιλαμβάνουν επιβεβαίωση ασφάλειας ασθενούς, χρέωση παρεχομένων υπηρεσιών, παρακολούθηση μετά τη χρέωση, επίλυση απορίων όσον αφορά τις χρεώσεις, λογαριασμούς πληρωτέους, λογαριασμούς εισπρακτέους, διαχείριση μετρητών και τήρηση αρχείου υπηρεσιών και τρίτων φορέων.

Από τη χρήση ενός πληροφοριακού συστήματος νοσοκομείου μπορούν να εξαχθούν χρήσιμα συμπεράσματα ως προς τον τρόπο λειτουργίας του νοσοκομείου. Η εξαγωγή των συμπερασμάτων αυτών μπορεί να γίνει με την ανάλυση των στατιστικών δεδομένων του συστήματος καθώς και με τη χρήση εργαλείων, τα οποία παρέχουν τη δυνατότητα προσομοίωσης της λειτουργίας του νοσοκομείου μετά την υλοποίηση μιας ή και περισσοτέρων αλλαγών. Το κύριο πλεονέκτημα των εργαλείων αυτών είναι η δυνατότητα παροχής της εικόνας της λειτουργίας του νοσοκομείου καθώς και των συνεπειών πριν από την πραγματική τους υλοποίηση.

Τα πληροφοριακά συστήματα νοσοκομείου τείνουν να αναπτύσσονται με κεντρικό υπολογιστή και τερματικά, παρόλο που σήμερα παρατηρείται μια στροφή προς τον περιορισμό του μεγέθους και τη διασπορά των δικτύων δεδομένων. Η επιλογή, η ανάπτυξη και η υλοποίηση ενός νοσοκομειακού πληροφοριακού συστήματος μπορεί να διαρκέσει χρόνια. Τα πλεονεκτήματα και τα μειονεκτήματα κάθε στρατηγικής “ζυγίζονται” πριν υλοποιηθεί κάποιο πληροφοριακό σύστημα. Το χρονικό διάστημα ποικίλλει ανάλογα με το σύστημα και την πολυπλοκότητα των εφαρμογών του. Στην ουσία μπορεί να είναι μια συνεχής διαδικασία. Το αρχικό κόστος για την εξασφάλιση των μηχανημάτων και του λογισμικού, καθώς και η ετήσια διαρκής συντήρηση απαιτεί την καταβολή πολύ υψηλών χρηματικών ποσών.

### 4.4.1 Ιστορία πληροφοριακών συστημάτων νοσοκομείων (ΠΣΝ)

Η εμφάνιση των ΠΣΝ έγινε στη δεκαετία του 1960. Από τη δεκαετία αυτή μέχρι σήμερα σημειώθηκαν σημαντικές εξελίξεις, κύρια ώθηση στις οποίες έδωσαν η πρόοδος της επιστήμης και της τεχνολογίας της πληροφορικής καθώς και οι βελτιώσεις που επήλθαν στη διοίκηση και τη λειτουργία των νοσοκομείων.

**Πρώτη γενιά (1960-1970):** Κατά την περίοδο αυτή τα πληροφοριακά συστήματα νοσοκομείων που αναπτύχθηκαν αφορούσαν κυρίως εφαρμογές για την υποστήριξη περισσότερο των κλινικών και λιγότερο των διοικητικών διαδικασιών του νοσοκομείου. Ο στόχος ήταν η βελτίωση της παρεχόμενης περίθαλψης. Τα συστήματα αυτά ήταν ιδιαίτερα ακριβά και χρησιμοποιήθηκαν κατά κύριο λόγο από τα μεγάλα νοσοκομεία.

**Δεύτερη γενιά (1970-1980):** Κατά την περίοδο αυτή, στην οποία έγινε και η εμφάνιση των μικροϋπολογιστών, τα ΠΣΝ άρχισαν να περιλαμβάνουν εφαρμογές για την υποστήριξη των οικονομικών και διοικητικών διαδικασιών του νοσοκομείου. Τα συστήματα αυτά χρησιμοποιήθηκαν και από τα νοσοκομεία μικρότερης κλίμακας μεγέθους καθώς το κόστος τους αλλά και ο όγκος τους είχε μειωθεί σημαντικά. Επίσης, κατά την περίοδο αυτή, εκτός από την εμφάνιση των μικροϋπολογιστών, άρχισε και η χρήση των βάσεων δεδομένων, η οποία έδωσε την δυνατότητα άμεσης διαθεσιμότητας των δεδομένων και παραγωγής αναφορών. Τα συστήματα αυτά ήταν κατά κύριο λόγο εφαρμογές, η λειτουργία και η χρησιμότητα των οποίων περιορίζονταν στα πλαίσια ενός συγκεκριμένου λειτουργικού τμήματος (stand-alone). Συνήθως, βασίζονταν σε τοπικές βάσεις δεδομένων ενώ η δυνατότητα σύνδεσης μεταξύ τους αντιμετωπιζόταν ως δευτερεύον θέμα. Ένα παράδειγμα ενός stand-alone συστήματος είναι ο προσωπικός υπολογιστής στο φαρμακείο ενός νοσοκομείου στον οποίο λειτουργεί μια εφαρμογή για την καταχώρηση των ιατρικών συνταγών, την έκδοση αποδείξεων και τη διαχείριση της αποθήκης του φαρμακείου. Το σύστημα αυτό είναι stand-alone καθώς δεν υπάρχει επικοινωνία (σύνδεση) με τα κλινικά τμήματα του νοσοκομείου ούτε με το λογιστήριο στο οποίο γίνεται και η χρέωση των ασθενών. Εάν το σύστημα αυτό δεν ήταν stand-alone, δεν θα απαιτούνταν η επαναπληκτρολόγηση των συνταγών καθώς αυτές θα ήταν άμεσα διαθέσιμες (μέσω της επικοινωνίας των συστημάτων) από τη χρονική στιγμή έκδοσης τους στο κλινικό τμήμα. Επίσης, ο λογαριασμός του ασθενή θα ενημερωνόταν για οποιαδήποτε χρέωση από τη χρονική στιγμή εκτέλεσης μιας συνταγής.

**Τρίτη γενιά (1980-1991):** Κατά την περίοδο αυτή έγινε η εμφάνιση των προσωπικών υπολογιστών και η χρήση των τοπικών δικτύων υπολογιστών (Local Area Networks – LAN). Έτσι, πολλοί προμηθευτές πληροφοριακών συστημάτων αναγκάστηκαν να δώσουν στα συστήματα τους τη δυνατότητα επικοινωνίας με άλλα συστήματα. Επίσης, κατά το χρονικό αυτό διάστημα άρχισε και η θεμελίωση των πρώτων προτύπων λειτουργικών συστημάτων, πρωτοκόλλων δικτύων και συστημάτων διαχείρισης αρχείων δεδομένων. ;ς αποτέλεσμα, οι προμηθευτές ΠΣΝ άρχισαν να χρησιμοποιούν συστήματα διαχείρισης βάσεων δεδομένων άλλων προμηθευτών, μερικά από τα οποία συμπεριλάμβαναν και γλώσσες διαχείρισης δεδομένων μέσω των οποίων δινόταν η δυνατότητα ανάκτησης δεδομένων που διαχειρίζονταν άλλες εφαρμογές

**Τέταρτη γενιά (1991 έως σήμερα):** Από το 1991 έχει αρχίσει να εμφανίζεται μια νέα γενιά ΠΣΝ, αν και τα χαρακτηριστικά της προηγούμενης γενιάς δεν έχουν εκλείψει εντελώς. Υπάρχουν διάφοροι παράγοντες που επηρεάζουν τη γενιά αυτή, όπως η αύξηση της δυνατότητας σύνδεσης δικτύων υπολογιστών, η δυνατότητα εγκατάστασης και χρήσης ενός συστήματος διαχείρισης βάσεων δεδομένων σε περισσότερα από ένα σημεία και η αύξηση και η καθιέρωση προτύπων στη λειτουργία των πληροφοριακών συστημάτων. Με τον όρο πρότυπο, εννοούμε τον κοινό τρόπο θεώρησης και αντιμετώπισης ενός συγκεκριμένου θέματος. Έτσι, στον χώρο της πληροφορικής στο διάστημα αυτό εμφανίστηκαν πρότυπα επικοινωνίας υπολογιστών, τα οποία έδωσαν τη δυνατότητα επικοινωνίας διαφορετικών πληροφοριακών συστημάτων (στο ίδιο γεωγραφικό σημείο ή σε διαφορετικά). Από τη μελέτη των τεσσάρων γενιών πληροφοριακών συστημάτων παρατηρούμε ότι οι αλλαγές στη λειτουργία και τη δομή των νοσοκομείων (οι οποίες υπαγορεύονται από την οικονομική πολιτική, τις κοινωνικές πιέσεις, τη συγχώνευση των προμηθευτών, κλπ.) δημιουργούν συχνά την ανάγκη για τεχνολογική αλλαγή. Ένα πληροφοριακό σύστημα έχει σχεδιαστεί και υλοποιηθεί με βάση κάποιο μοντέλο, το οποίο αναπαριστά τη δομή του νοσοκομείου σε συγκεκριμένη χρονική στιγμή. Η πρόκληση που αντιμετωπίζει ένα νοσοκομείο είναι η επιλογή συστημάτων των οποίων το μοντέλο είναι όσο το δυνατόν περισσότερο προσαρμοσμένο στην πραγματική κατάσταση. Κάθε γενιά πληροφοριακών συστημάτων βασίζεται σε συγκεκριμένη τεχνολογία με δυνατότητες και περιορισμούς. Ακόμη και τα

νοσοκομεία που αναγνωρίζουν έγκαιρα τις αλλαγές και την ανάγκη προσαρμογής των συστημάτων τους ή την απόκτηση νέων δεν μπορούν εύκολα να ικανοποιήσουν την ανάγκη αυτή.

### 4.4.2 Ενδονοσοκομειακά πληροφοριακά συστήματα

Ο βιοϊατρικός εξοπλισμός ενός σύγχρονου νοσοκομείου αποτελείται από ένα πλήθος ετερογενών συσκευών οι οποίες μπορούν να ταξινομηθούν σε γενικές κατηγορίες, ανάλογα με τη λειτουργία τους. Τα δεδομένα που παράγονται από κάθε κατηγορία παρουσιάζουν ένα μεγάλο βαθμό ανομοιομορφίας (εικόνες, κυματομορφές, αριθμητικά δεδομένα, κλπ.). Οι συσκευές που ανήκουν σε κάθε κατηγορία μπορούν να συνδεθούν μεταξύ τους με δίκτυο, αποτελώντας έτσι ξεχωριστά συστήματα συλλογής και αποθήκευσης ενός τύπου δεδομένων.

### 4.4.3 Αυτοματοποιημένα συστήματα νοσοκομείου

Αντιπροσωπευτικά συστήματα συλλογής και επεξεργασίας δεδομένων είναι τα παρακάτω:

• ***Picture Archiving and Communication System (PACS):*** Είναι ένα σύστημα που παρέχει τη δυνατότητα συλλογής εικόνων (από CT, MRI, ψηφιακούς αγγειογράφους, συσκευές υπερήχων) αποθήκευσης και ανάκτησής τους και συμπεριλαμβάνει συσκευές απεικόνισης και διαχείρισης εικόνων, συνδεδεμένες με συσκευές αποθήκευσης.

• ***Pharmacy Information System (PIS):*** Το σύστημα αυτό αυτοματοποιεί τις διαδικασίες φαρμακείου ενός νοσοκομείου (επεξεργασία συνταγών, συντήρηση της βάσης δεδομένων των φαρμάκων, παρακολούθησης της χρήσης τους, κλπ.).

• ***Material Management Information System (MMIS):*** Χρησιμοποιείται για τη διαχείριση και τον έλεγχο όλων των διαδικασιών που αφορούν την προμήθεια υλικών (αγορά, λήψη, ταξινόμηση, απογραφή, κλπ.).

• ***Anesthesia Information Management System (AIMS):*** Το σύστημα αυτό συλλέγει δεδομένα από πολυάριθμες πηγές σχετικά με την παρακολούθηση των διαδικασιών στα τμήματα αναισθησιολογίας, παρέχει τη δυνατότητα ανάλυσης των δεδομένων αυτών και παράγει διάφορους τύπους αναφορών.

• ***Laboratory Information System (LIS):*** Χρησιμοποιείται για τη συλλογή πληροφοριών από ένα πλήθος συσκευών (Clinical Chemistry Analyzers, Blood Culture Analyzers, κλπ.), για την αποθήκευση κλινικών δεδομένων, την επαλήθευση της ακρίβειας των εξετάσεων, τη βαθμονόμηση των οργάνων και τη δημιουργία (και την ενημέρωση) αρχείων ασθενών.

• ***Radiology Information System (RIS):*** Είναι ένα σύστημα που συλλέγει και αποθηκεύει δεδομένα από ακτινολογικές συσκευές.

• ***Hospital Information System (HIS):*** Είναι το κεντρικό σύστημα ενός νοσοκομείου, που συλλέγει δεδομένα από το σύνολο των συστημάτων και επιτρέπει την πρόσβαση σε όλες τις επιμέρους διαδικασίες, παρέχοντας τη δυνατότητα για συνολική διαχείριση του νοσοκομείου.

Η δικτύωση των συσκευών μίας κατηγορίας, όταν δεν υπακούουν σε κάποιο standard, απαιτεί συνήθως την ύπαρξη ειδικών interfaces (hardware ή/και software) και μετατροπείς πρωτοκόλλων. Το πρόβλημα της δικτύωσης μεταξύ των συσκευών διαφορετικών προμηθευτών αντιμετωπίζεται με την εφαρμογή επικοινωνιακών standards (π.χ. για συστήματα PACS χρησιμοποιείται το DICOM 3.0), που εξασφαλίζουν ανταλλαγή δεδομένων μεταξύ διαφορετικών τύπων συσκευών. Επίσης, η ανάγκη δικτύωσης όλων των συστημάτων που συνιστούν το HIS, απαιτεί την ύπαρξη ενός standard για την ανταλλαγή δεδομένων μεταξύ των ετερογενών αυτών συστημάτων. Ένα τέτοιο standard είναι το Electronic Data Interchange Health Level 7 (HL7), που παρέχει υπηρεσίες ανταλλαγής κλινικών δεδομένων μεταξύ όλων των ετερογενών συστημάτων του νοσοκομείου, καθώς επίσης και λειτουργίες όπως καταχώρηση ασθενών, Admission/Discharge/Transfer (ADT), κλπ.

### 4.4.4 Πληροφοριακά συστήματα εργαστηρίου

Το 1988 δημοσιεύτηκαν από το U.S. Department of Health and Human Services Clinical Laboratory Improvement Act (CLIA) οδηγίες που αφορούν τη σύνδεση ιατρικών συσκευών εργαστηρίου με συστήματα LIS ή/και HIS, καθώς επίσης και το είδος των δεδομένων που συλλέγονται και αποθηκεύονται. Αν και το CLIA δεν υποχρεώνει την ύπαρξη συστημάτων δημιουργίας αναφορών με υπολογιστή στα νοσοκομειακά εργαστήρια, απαιτεί εντούτοις την ύπαρξη ενός συστήματος που θα εξασφαλίζει συμβατότητα με τα πρότυπα ποιότητας, που έχουν θεσπιστεί από το CLIA, για έλεγχο και εξασφάλιση ποιότητας των μηχανημάτων εξέτασης των ασθενών και των διαδικασιών. Ένα LIS σύστημα προσφέρει ένα γρήγορο και αποτελεσματικό τρόπο για τη διαχείριση του μεγάλου όγκου δεδομένων που παράγονται καθημερινώς από ένα εργαστήριο εξετάσεων, καθώς επίσης και την οργάνωση και αποθήκευση των δεδομένων που απαιτούνται για τη συμμόρφωση με τις απαιτήσεις του CLIA και άλλων υπηρεσιών ελέγχου.

Στην Ελλάδα, προς το παρόν, δεν έχουν εφαρμοστεί αντίστοιχοι κανονισμοί για τη λειτουργία των νοσοκομειακών εργαστηρίων. Εντούτοις, η συνεχής παρακολούθηση των χαρακτηριστικών λειτουργίας των συσκευών εξέτασης προσφέρει μεγάλα οφέλη, παρέχοντας τις εξής δυνατότητες:

- εκτίμησης της αξιοπιστίας και ακρίβειας των εξετάσεων,
- υπολογισμού του κόστους ανά εξέταση,
- υπολογισμού του μέσου χρόνου λειτουργίας κάθε συσκευής,
- μέτρηση της συχνότητας εφαρμογής ελέγχων ποιότητας και βαθμονόμησης και καταχώρηση των αποτελεσμάτων για μακροπρόθεσμο έλεγχο ποιότητας (π.χ. σε μηνιαία βάση).

### 4.4.5 Πληροφοριακό σύστημα Μηχανογράφησης διαγνωστικών εργαστηρίων (LIS)

Τα διαγνωστικά εργαστήρια είναι εφοδιασμένα με το πληροφοριακό σύστημα LIS, παρέχοντας τη δυνατότητα διαχείρισης εργαστηριακών εξετάσεων σε ηλεκτρονική μορφή. Με αυτόν τον τρόπο επιτρέπεται η εισαγωγή στοιχείων των εξεταζόμενων και του ιστορικού, των αιτούμενων εξετάσεων, η έκδοση αποτελεσμάτων, η αρχειοθέτηση, ο έλεγχος ποιότητας και η στατιστική επεξεργασία.

Εφαρμόζονται επιπλέον προγράμματα αναγνώρισης με τη βοήθεια barcode, για να επιτυγχάνεται η ταυτοποίηση των εξεταζόμενων και των δειγμάτων, με τέτοιο τρόπο ώστε να αποτρέπονται τα σφάλματα.

Το κόστος εγκατάστασης και λειτουργίας ενός πληροφοριακού συστήματος LIS μπορεί να αποσβεστεί εντός λίγων ετών μέσω της εξοικονόμησης χρόνου, τη μείωση της χειρωνακτικής εργασίας, την αποφυγή σφαλμάτων, λόγω της αυτόματης επικοινωνίας του ιατροτεχνολογικού εξοπλισμού με μια βάση δεδομένων και της ηλεκτρονικής διακίνησης των αποτελεσμάτων.

### 4.4.6 Πληροφοριακό σύστημα αρχειοθέτησης και επικοινωνίας ιατρικών εικόνων (PACS)

Η αρχειοθέτηση των films σε ένα ακτινολογικό εργαστήριο εμφανίζει πολλά προβλήματα. Τα πιο σημαντικά είναι: η αργή πρόσβαση, η απώλεια των εικόνων λόγω κακής κατάστασης των films και κακής αρχειοθέτησης, η δυσκολία να βρεθεί η συγκεκριμένη εικόνα σε συγκεκριμένο χρόνο ενώ δεν υπάρχει καμία δυνατότητα να συνδυαστεί με άλλες ηλεκτρονικά καταγεγραμμένες πληροφορίες. Αυτά είναι μερικά από τα αίτια που δημιούργησαν την ανάγκη για ένα σύστημα αρχειοθέτησης των εικόνων και επικοινωνίας (Picture Archiving and Communication System [PACS]) εδώ και μερικά χρόνια.

Οι εικόνες που παράγονται από τις εξετάσεις αποθηκεύονται σε ψηφιακή μορφή στον κεντρικό υπολογιστή, που αποτελεί και τη βάση δεδομένων του συστήματος. Από τον

κεντρικό υπολογιστή οι εξετάσεις μπορούν να ανακληθούν από άλλους σταθμούς εργασίας, για διάγνωση, επεξεργασία και παραγωγή ψηφιακών αντιγράφων για εκπαιδευτικούς σκοπούς. Τα PACS είναι μια καινούργια κατάκτηση στον χώρο της Ιατρικής και έρχονται να ικανοποιήσουν ένα πλήθος αναγκών των ασθενών και των επαγγελματιών υγείας. Η χρήση του συστήματος PACS έλυσε πολλά προβλήματα που είχαν προκύψει με τις μέχρι σήμερα μεθόδους αρχειοθέτησης εικόνων ασθενών. Ο χρόνος εύρεσης σημαντικών εικόνων περιορίστηκε δραματικά, δεν υπάρχει απώλεια εικόνων και η παραγωγή εκπαιδευτικού υλικού έγινε ευκολότερη.

### 4.4.7 Ασφάλεια πληροφοριακών συστημάτων νοσοκομείων (ΠΣΝ)

Τα ΠΣΝ ανήκουν στην κατηγορία εκείνη των Πληροφοριακών Συστημάτων που χαρακτηρίζονται ότι λειτουργούν σε περιβάλλοντα υψηλής ευπάθειας, λόγω τόσο των χαρακτηριστικών αλλά και της φύσης των πληροφοριών που διαχειρίζονται, όσο και των ιδιαίτερων χαρακτηριστικών του περιβάλλοντος λειτουργίας τους.

Είναι σαφές ότι όλοι οι τύποι των δεδομένων που χρησιμοποιούνται από τα υπάρχοντα σήμερα ΠΣΝ, χειρόγραφα ή αυτοματοποιημένα, δεν παρουσιάζουν την ίδια ευπάθεια.

Επιπροσθέτως, ορισμένοι τύποι δεδομένων είναι δυνατόν άλλοτε να χαρακτηρίζονται ως ευπαθείς και άλλοτε όχι. Είναι, επίσης σαφές, ότι η διαφορά της ευπάθειας διαφόρων τύπων δεδομένων δεν οφείλεται μόνο στα ιδιαίτερα χαρακτηριστικά των ΠΣ τα οποία χρησιμοποιούν τα δεδομένα, αλλά οφείλεται, επίσης, και στην ίδια τη φύση ή την ιδιαιτερότητα των δεδομένων αυτών. Η ευπάθεια των δεδομένων μπορεί, πιο συγκεκριμένα, να χαρακτηρισθεί με δύο τρόπους:

Α) Η ευπάθεια ορισμένων τύπων δεδομένων, που είναι ανεξάρτητη από το ΠΣΝ στο οποίο χρησιμοποιούνται τα δεδομένα αυτά, ορίζεται ως εγγενής ευπάθεια στα πλαίσια ενός συγκεκριμένου κοινωνικού συστήματος. Τα δεδομένα που αφορούν τη σωματική και ψυχική υγεία έχουν αξιοποιηθεί –με κοινωνικά αποδεκτό τρόπο- από αυτοματοποιημένα ΠΣΝ. Υπάρχουν βάσιμες ενδείξεις ότι η αξιοποίηση τους αυτή θα συνεχιστεί με αυξανόμενο ρυθμό

και στο άμεσο μέλλον, τόσο στις τεχνολογικά προηγμένες, όσο και στις αναπτυσσόμενες χώρες. Άρα, τα δεδομένα που αφορούν στη σωματική και ψυχική υγεία ενός πολίτη είναι τα μόνα που συγκεντρώνουν τις εξής ιδιότητες:

- Αποτελούν συνολικά και εγγενώς ευπαθή δεδομένα, άρα ακρότατο στιγμιότυπο δεδομένων προς προστασία και εξασφάλιση.
- Αποτελούν δεδομένα τα οποία χρησιμοποιούνται ευρέως από αυτοματοποιημένα ΠΣΝ και των οποίων η αξιοποίηση διευρύνεται διαρκώς.
- Αποτελούν δεδομένα των οποίων η αξιοποίηση συναντά τη γενική αποδοχή του κοινωνικού συνόλου, παρόλη τη δεδομένη ευπάθειά τους.
- Αποτελούν την πρώτη ύλη για την εφαρμογή της Ιατρικής επιστήμης, θεμελιώδες γνώρισμα της οποίας είναι επιτακτική ανάγκη λήψης αποφάσεων υπό συνθήκες αβεβαιότητας.

Β) Η ευπάθεια ορισμένων τύπων δεδομένων, που είναι ανεξάρτητη από το ΠΣΝ στο οποίο χρησιμοποιούνται και η οποία ισχύει για όλα τα μέλη του κοινωνικού συνόλου, ορίζεται ως συνολική και εγγενής ευπάθεια στα πλαίσια ενός συγκεκριμένου κοινωνικού συστήματος. Η συνολική και εγγενής ευπάθεια είναι αυτή που προκαλεί θεσμικές και κοινωνικές παρεμβάσεις είτε υπό τη μορφή νόμων είτε υπό τη μορφή κανόνων δεοντολογίας. Επιπροσθέτως, είναι αυτή που καθορίζει ότι τα δεδομένα χρήζουν ιδιαίτερης προστασίας. Τα δεδομένα και οι πληροφορίες για τις οποίες θα πρέπει να υπάρχει υψηλός βαθμός εμπιστευτικότητας και προστασίας είναι οι εξής:

- Οι πληροφορίες του ιατρικού ιστορικού ενός ασθενή, οι διαγνώσεις, καθώς και τα αποτελέσματα των εργαστηριακών εξετάσεων.
- Τα νοσοκομεία στα οποία έχει νοσηλευθεί ένας ασθενής κατά το παρελθόν, τα στοιχεία του οικογενειακού γιατρού.
- Τα στοιχεία των εργαζομένων στο νοσοκομείο, οι οικονομικές απολαβές τους, τα στοιχεία των νοσηλευόμενων, οι λογαριασμοί νοσηλείας, καθώς και οι καταστάσεις με το πρόγραμμα επισκέψεων στους γιατρούς.

- Το δικαίωμα προσπέλασης στις παραπάνω πληροφορίες εξαρτάται από τη φύση της πληροφορίας, την ειδικότητα αυτού που αιτείται την προσπέλαση, καθώς και τη φύση της επαγγελματικής σχέσης του με τον ασθενή.

### 4.4.8 Αρχές για την προστασία των ΠΣΝ

Με μια σειρά συνθηκών, το Ευρωπαϊκό Συμβούλιο υπαγορεύει ρητά ότι ιατρικά δεδομένα πολιτών δεν πρέπει να επεξεργάζονται αυτόματα (χωρίς τη συγκατάθεση των ενδιαφερομένων) από κυβερνητικές υπηρεσίες ή οργανισμούς και απαιτεί από τα κράτη-μέλη να εναρμονίσουν τις νομοθεσίες τους. Το ιατρικό απόρρητο και η απόλυτη εμπιστευτικότητα αποβλέπουν στην προστασία των ανθρώπινων δικαιωμάτων, στην προστασία δικαιωμάτων των ασθενών, στη διασφάλιση της ποιότητας των ιατρικών πληροφοριών και στην υποστήριξη της ιατρικής έρευνας. Για την υλοποίηση των στόχων αυτών χρησιμοποιείται ένας κώδικας δεοντολογίας, καθώς και ένα πλήθος άλλων γενικών αρχών. Η τήρηση των αρχών για την προστασία των ΠΣΝ επαφίεται σε φορείς που έχουν αρμοδιότητα είτε σε τοπικό επίπεδο (π.χ. νοσοκομείο), είτε σε εθνικό επίπεδο (π.χ. Εθνική επιτροπή προστασίας δεδομένων), είτε σε διεθνές επίπεδο.

Οι γενικές αρχές για την ανάπτυξη ενός ΠΣΝ είναι οι παρακάτω σύμφωνα με την
*Ελληνική Εταιρία Επιστημόνων Ηλεκτρονικών Υπολογιστών και Πληροφορικής (1995)*

**ΑΡΧΗ 1:** Κώδικας δεοντολογίας. Κάθε νοσοκομείο πρέπει να συγκροτήσει και να υιοθετήσει έναν Κώδικα δεοντολογίας, ο οποίος θα καθορίζει τις εθιμικές αρχές που πρέπει να διέπουν την ασφαλή λειτουργία των ΠΣΝ του χώρου αυτού, με ταυτόχρονο σεβασμό της ιδιωτικής ζωής του κάθε ασθενή.
**ΑΡΧΗ 2:** Συμβατικές δεσμεύσεις. Τα καθήκοντα και οι υποχρεώσεις των εργαζομένων στα Νοσοκομεία, που σχετίζονται με θέματα ασφάλειας ΠΣΝ, πρέπει να καθορίζονται με συμφωνία διοίκησης Νοσοκομείου και εργαζομένου.

**ΑΡΧΗ 3:** Συγκρότηση φορέα προστασίας των δεδομένων. Η επίβλεψη της τήρησης των γενικών αρχών για την ασφάλεια των ΠΣΝ θα πρέπει να ανατίθεται σε φορέα λειτουργικά και οικονομικά ανεξάρτητο, του οποίου η αρμοδιότητα εκτείνεται σε όλες τις υπηρεσίες του Νοσοκομείου.

**ΑΡΧΗ 4:** Εκπαίδευση-ενημέρωση-ευαισθητοποίηση. Το προσωπικό του Νοσοκομείου θα πρέπει να ενημερώνεται και να εκπαιδεύεται, τόσο σε θέματα που αφορούν την ασφάλεια των ΠΣΝ, όσο και σε θέματα που αφορούν την προστασία της προσωπικής ζωής των ασθενών.

**ΑΡΧΗ 5:** Περιορισμός των κυκλοφορούντων δεδομένων. Η κυκλοφορία των ιατρικών δεδομένων, που πραγματοποιείται για την πραγμάτωση κάποιου στόχου, θα πρέπει να είναι η ελάχιστη δυνατή.

**ΑΡΧΗ 6:** Διασφάλιση των δικαιωμάτων των ασθενών. Τα ΠΣΝ λειτουργούν με στόχο την παροχή υπηρεσιών υγείας υψηλής ποιότητας, με ταυτόχρονο σεβασμό των δικαιωμάτων των ασθενών και του ισχύοντος θεσμικού πλαισίου.

**ΑΡΧΗ 7:** Διασφάλιση της ποιότητας των δεδομένων. Η ακεραιότητα και η ακρίβεια των δεδομένων που χρησιμοποιούνται στα ΠΣΝ πρέπει να είναι υψηλή.

**ΑΡΧΗ 8:** Υποστήριξη της ιατρικής έρευνας. Τα δεδομένα που χρησιμοποιούνται για την πραγματοποίηση ιατρικής ή επιδημιολογικής έρευνας πρέπει να καθίστανται ανώνυμα και ο σκοπός της επεξεργασίας τους να μην αντίκειται προς τα ανθρώπινα δικαιώματα ή τα δικαιώματα των ασθενών.

**ΑΡΧΗ 9:** Τεχνικές ρυθμίσεις. Η επεξεργασία των ιατρικών δεδομένων πρέπει να γίνεται με τη συνοδεία κατάλληλων τεχνικών ρυθμίσεων που στόχο έχουν να εγγυηθούν την ασφαλή λειτουργία των ΠΣΝ.

# ΚΕΦΑΛΑΙΟ 5

## ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ - SMART CARDS

### 5.1 Ιστορία της Ανάπτυξης των πλαστικών καρτών

Η χρήση των πλαστικών καρτών ξεκίνησε στις Η.Π.Α στις αρχές της δεκαετίας του 1950. Η χαμηλή τιμή του συνθετικού υλικού του PVC επέτρεψε την μαζική παραγωγή και με μεγάλη διάρκεια ζωής καρτών. Αυτές οι κάρτες άρχισαν να είναι περισσότερο βολικές έναντι του χαρτιού που χρησιμοποιούταν μέχρι τότε, το οποίο προφανώς δεν είναι το ίδιο ανθεκτικό, όσο οι πλαστικές κάρτες. Η πρώτη πλαστική κάρτα πληρωμής γενικού σκοπού εκδόθηκε από την Diners Club το 1950. Προοριζόταν για μια συγκεκριμένη υψηλή τάξη ανθρώπων και είχε τον χαρακτήρα επικύρωσης της ισχυρής οικονομικής κατάστασης. Η εισαγωγή της Visa και της MasterCard στο πεδίο, οδήγησε στην εξάπλωση της χρησιμοποίησης του πλαστικού χρήματος, αρχικά στις Η.Π.Α, με την Ευρώπη και τον υπόλοιπο κόσμο να ακολουθεί αυτή την τάση λίγα χρόνια αργότερα.

Αρχικά η λειτουργία των καρτών ήταν σχετικά τετριμμένη, καθώς αποτελούσαν φορείς δεδομένων, οι οποίοι παρείχαν ασφάλεια ενάντια της πλαστογραφίας. Γενικές πληροφορίες, όπως το όνομα του κατόχου της κάρτας, ήταν τυπωμένες πάνω στην επιφάνεια της, ενώ τα προσωπικά δεδομένα του κατόχου της και ο αριθμός της ήταν σε ανάγλυφη μορφή. Επιπλέον πολλές κάρτες είχαν ένα πεδίο προκειμένου ο κάτοχος της κάρτας να έχει την δυνατότητα να υπογράφει. Οι κάρτες αυτές ήταν της πρώτης γενιάς και παρείχαν προστασία κατά της πλαστογραφίας μέσω μεθόδων που κυρίως ήταν εμφανείς, δηλαδή μέσω του πεδίου της υπογραφής και των εκτυπωμένων πεδίων που περιγράψαμε. Άρα η ασφάλεια του συστήματος είχε να κάνει κυρίως με την ποιότητα του και την ευσυνειδησία του υπαλλήλου που δεχόταν ή όχι, τις κάρτες αυτού του είδους. Αρχικά αυτό δεν ήταν τόσο μεγάλο πρόβλημα, αφού οι κάρτες ήταν λίγες σε αριθμό, ωστόσο καθώς η χρησιμοποίηση των καρτών αυξανόταν, μεγαλύτερος γινόταν και ο κίνδυνος για κακόβουλη χρήση της κάρτας κάνοντας επιτακτική την ανάγκη ύπαρξης νέων μεθόδων ασφαλείας.

Στην πραγματικότητα, η ιστορική προέλευση των έξυπνων καρτών μας οδηγεί στη δεκαετία του 70. Το 1968, οι γερμανοί εφευρέτες Jurgen Dethloff και Helmut Grotrupp δημιούργησαν την πρώτη κάρτα με ολοκληρωμένο κύκλωμα (ICC/ integrated circuit card). Δύο χρόνια αργότερα, το 1970 στην Ιαπωνία, ο εφευρέτης Kunitaka Arimura διατύπωσε μία παρόμοια πατέντα στην ιδέα της έξυπνης κάρτας.

Τα πραγματικά θεμέλια όμως για την υλοποίηση της τεχνολογίας των έξυπνων καρτών μπήκαν το 1974 στη Γαλλία από τον ανεξάρτητο εφευρέτη και ερευνητή Roland Moreno. Ο Moreno υλοποίησε πιλοτικά την ένωση πλαστικής κάρτας και μικροτσίπ, το παρουσίασε σε κάποιες τράπεζες στη Γαλλία και τον επόμενο χρόνο το κατοχύρωσε και ως πατέντα.

Η πρώτη έξυπνη κάρτα κατασκευάστηκε το 1979 από τη Motorola για εμπορική χρήση στο γαλλικό τραπεζικό σύστημα. Στη Γαλλία το 1984 εφαρμόστηκε με επιτυχία ένα μεγάλο πιλοτικό πρόγραμμα με έξυπνες τηλεφωνικές κάρτες. Τα ολοκληρωμένα κυκλώματα που χρησιμοποιούνται σε μία τηλεκάρτα είναι σχετικά μικρά, απλά και φτηνά ολοκληρωμένα κυκλώματα μνήμης, τα οποία είναι κατάλληλα σχεδιασμένα ώστε το διαθέσιμο χρηματικό υπόλοιπο της κάρτας να μειώνεται ανάλογα με τη χρήση.

Ολοκληρωμένα κυκλώματα με μικροεπεξεργαστή, που είναι αρκετά μεγαλύτερα και πιο πολύπλοκα, χρησιμοποιήθηκαν αρχικά σε μεγάλες ποσότητες, σε εφαρμογές τηλεπικοινωνιών και συγκεκριμένα κινητών τηλεπικοινωνιών.

Πρωτοπόρος στον τομέα αυτό υπήρξε το Γερμανικό Ταχυδρομείο χρησιμοποιώντας το 1988 μία κάρτα με μικροεπεξεργαστή που παρείχε εξουσιοδοτημένη πρόσβαση στο αναλογικό δίκτυο κινητής τηλεφωνίας C-Netz. Η κίνηση αυτή άνοιξε το δρόμο για τη χρήση των έξυπνων καρτών στα μετέπειτα ψηφιακά GSM δίκτυα κινητής τηλεφωνίας. Μια άλλη εφαρμογή που έλαβε μέρος στη Γερμανία έκανε χρήση 70 εκατομμυρίων έξυπνων καρτών που περιείχαν πληροφορίες ιατρικής ασφάλισης.

Στις ΗΠΑ η τεχνολογία των έξυπνων καρτών δεν είχε την ίδια ανταπόκριση που είχε στην Ευρώπη. Για να εξοικειωθεί ο κόσμος με τη νέα αυτή τεχνολογία, η Visa εξέδωσε στους Ολυμπιακούς Αγώνες της Ατλάντα το 1996 πάνω από 1,5 εκατομμύριο κάρτες VISACash. Την ίδια χρονιά η Visa και η MasterCard επιχορηγούν έρευνες με σκοπό την επίλυση του

προβλήματος της συμβατότητας των καρτών με περιβάλλοντα προγραμματισμού με αποτέλεσμα την δημιουργία της JavaCard.

Καθώς προχωράμε στον 21ο αιώνα, οι έξυπνες κάρτες θα έχουν σημαίνοντα ρόλο στην ηλεκτρονική επιχειρησιακή δραστηριότητα, διότι είναι αποδεδειγμένα ένα ιδανικό μέσο για την ασφαλή αποθήκευση κρυπτογραφικών κλειδιών και αλγορίθμων.

Οι εξελίξεις τα τελευταία χρόνια στην σύγχρονη κρυπτογραφία, οι οποίες έδωσαν τη δυνατότητα σε έξυπνες κάρτες να έχουν υψηλό βαθμό ασφαλείας, οδήγησαν τις τράπεζες και επιχειρήσεις να πάρουν στα σοβαρά τις έξυπνες κάρτες. Σε άλλες εφαρμογές, όπως στην υγεία, στην εκπαίδευση, στις τηλεπικοινωνίες και στις μεταφορές έχουν ήδη ξεκινήσει να χρησιμοποιούν έξυπνες κάρτες. Η βιομηχανία των έξυπνων καρτών εξαπλώνεται με πολύ μεγάλο ρυθμό και έχει φτάσει σε βαθμό παραγωγής καρτών σχεδόν ίσο με 1.000.000.000 το χρόνο, ενώ πλέον οι έξυπνες κάρτες χρησιμοποιούνται σε διάφορες εφαρμογές σε περισσότερες από 90 χώρες παγκοσμίως. Το μεγαλύτερο μερίδιο της αγοράς των έξυπνων καρτών κατέχουν οι εφαρμογές τηλεφωνίας, οι τραπεζικές εφαρμογές και εφαρμογές που αφορούν το χώρο της Υγείας.

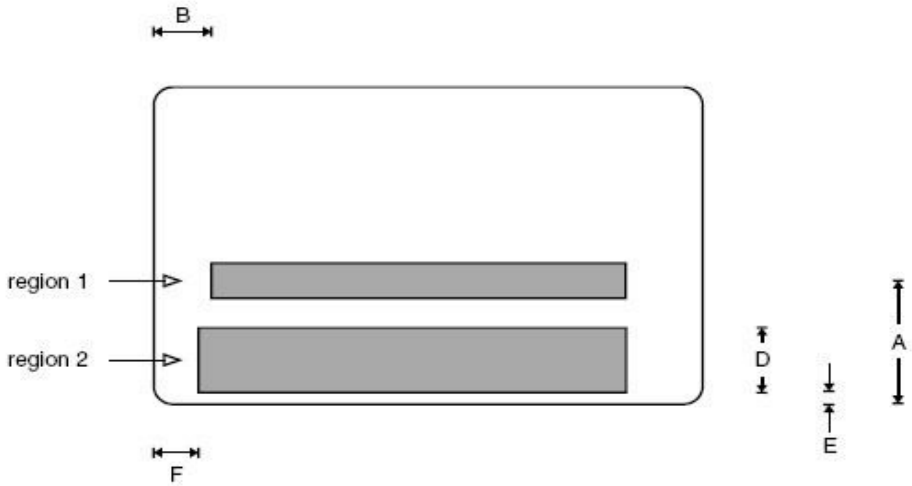
## 5.2 Τεχνολογία καρτών

### 5.2.1 Ανάγλυφες Κάρτες

Η ανάγλυφη μορφή είναι η παλιότερη τεχνική για την αναγνώριση ταυτότητας. Οι ανάγλυφοι χαρακτήρες στην κάρτα μπορούν να μεταφερθούν σε χαρτί χρησιμοποιώντας απλές και οικονομικές συσκευές. Η οπτική ανάγνωση της ανάγλυφης μορφής είναι πολύ απλή και η φύση και η τοπολογία της θέσης των ανάγλυφων χαρακτήρων καθορίζονται από το ISO standard 7811, Identification Cards - Recording Technique.

Το [ISO 7811 Part 1] καθορίζει τις απαιτήσεις για τους ανάγλυφους χαρακτήρες, όπως για παράδειγμα την μορφή τους, το μέγεθος τους και διάφορα άλλα χαρακτηριστικά. Το τρίτο

τμήμα [ISO 7811 Part 3] ορίζει την ακριβή θέση των χαρακτήρων στην κάρτα, και ορίζει επίσης δύο ξεχωριστές περιοχές.




*Σχήμα 5.1: Οι ανάγλυφες περιοχές σύμφωνα με το ISO 7811-3*

*A = 21.42 ± 0.12 mm, B = 10.18 ± 0.25 mm, D = 14.53 mm, E = 2.41−3.30 mm, F = 7.65 ± 0.25 mm*

Η πρώτη περιοχή (region 1) διατηρείται για την τοποθέτηση του Αριθμού Αναγνώρισης της Κάρτας, Identification Card Number (19 χαρακτήρες) το οποίο ταυτοποιεί τόσο την κάρτα όσο και τον χρήστη της. Η δεύτερη περιοχή (region 2) διατηρείται για επιπλέον δεδομένα που αφορούν τον ιδιοκτήτη της κάρτας, όπως για παράδειγμα το όνομα και τη διεύθυνση (4 x 27 χαρακτήρες).

Με μια πρώτη ματιά, η μεταφορά δεδομένων με αποτύπωση ανάγλυφων χαρακτήρων μπορεί να φαίνεται πρωτόγονη, ωστόσο η απλότητα της την έκανε αποδεκτή ακόμα και σε τεχνολογικά εξελιγμένες χώρες.

### 5.2.2 Εισαγωγή στις Έξυπνες κάρτες (smart cards)

Η έξυπνη κάρτα είναι μια μικρή κάρτα ή παρόμοια συσκευή με ενσωματωμένο τσιπ ολοκληρωμένου κυκλώματος. Οι έξυπνες κάρτες συνήθως μοιάζουν με μια πιστωτική κάρτα, αν και μπορεί να πάρει διάφορες μορφές.

Αυτό που κάνει την έξυπνη κάρτα είναι το ενσωματωμένο chip. Το chip είναι ένας ισχυρός μικροϋπολογιστής που μπορεί να προγραμματιστεί για διάφορες εφαρμογές.

Το chip επιτρέπει μια έξυπνη κάρτα να αποθηκεύει και να παρέχει πρόσβαση σε δεδομένα και εφαρμογές με ασφάλεια και ανταλλαγή δεδομένων με ασφάλεια με τους αναγνώστες και άλλα συστήματα. Η τεχνολογία των έξυπνων καρτών μπορεί να παρέχει υψηλά επίπεδα ασφάλειας και προστασία της ιδιωτικής ζωής, κάνοντας τις έξυπνες κάρτες ιδανικές για τον χειρισμό ευαίσθητων πληροφοριών, όπως η ταυτότητα και προσωπικές πληροφορίες υγείας.

Η έξυπνη κάρτα μπορεί να διαθέτει Ηλεκτρικά Διαγράψιμη Προγραμματιζόμενη Μνήμη Μόνο Ανάγνωσης (EEPROM/Electrical Erasable Programmable Read Only Memory), η οποία διατηρεί τα περιεχόμενα ακόμα και όταν δεν παρέχεται ηλεκτρική τάση. Δεν υπάρχουν μπαταρίες στην έξυπνη κάρτα. Ενέργεια παρέχεται εξωτερικά από την συσκευή ανάγνωσης, είτε αυτή είναι επαφής είτε όχι. Επίσης και ο χρονισμός της CPU παρέχεται από τη συσκευή ανάγνωσης.

Οι έξυπνες κάρτες περιέχουν λειτουργικό σύστημα, όπως και οι προσωπικοί υπολογιστές και μπορούν να αποθηκεύσουν και να επεξεργάζονται τις πληροφορίες που είναι πλήρως διαδραστικές. Πολύπλοκες έξυπνες κάρτες περιέχουν επίσης μια δομή μυστικών κλειδιών κρυπτογράφησης και αλγορίθμων.

***Λόγω του υψηλού επιπέδου ασφάλειας έξυπνων καρτών και της off-line φύσης τους είναι εξαιρετικά δύσκολο να προσβληθούν από hacker. Επειδή είναι δύσκολο να ανακτηθούν δεδομένα χωρίς έγκριση, μια έξυπνη κάρτα είναι μοναδικά κατάλληλη για την ασφαλή και κατάλληλη αποθήκευση δεδομένων.***

Χωρίς άδεια του κατόχου καρτών, τα στοιχεία δεν θα μπορούσαν να ληφθούν ή να τροποποιηθούν. Επομένως, η έξυπνη κάρτα θα μπορούσε περαιτέρω να ενισχύσει την ιδιωτικότητα του χρήστη.

Η ευκολία μεταφοράς και χρήσης τους, η δυνατότητα αποθήκευσης μεγάλου όγκου πληροφοριών, η υπολογιστική ισχύς, η ασφάλεια των δεδομένων που προσφέρουν, το χαμηλό τους κόστος είναι μερικά από τα χαρακτηριστικά που κάνουν τις έξυπνες κάρτες να χρησιμοποιούνται σε όλο και περισσότερες εφαρμογές. Οι έξυπνες κάρτες είναι πολύ χρήσιμες ως μέσο συναλλαγών, εξουσιοδότησης και αναγνώρισης ταυτότητας. Καθώς οι

δυνατότητες τους μεγαλώνουν, μπορούν να αντικαταστήσουν ότι περιέχεται στα πορτοφόλια μας, συμπεριλαμβανομένου των πιστωτικών καρτών, διπλωμάτων και μετρητών.

***Ποια έξυπνα χαρακτηριστικά ασφαλείας της κάρτας μπορούν να προστατεύσουν τις προσωπικές πληροφορίες υγειονομικής περίθαλψης;***

Η μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα προσωπικά δεδομένα υγείας είναι μια κρίσιμη ανησυχία, δεδομένου ότι όλο και περισσότερα ιατρικά δεδομένα μετατρέπονται σε ψηφιακή μορφή. Πολλαπλά χαρακτηριστικά ασφαλείας επιτρέπουν τις έξυπνες κάρτες να προστατεύουν τα δεδομένα, όχι μόνο τις πληροφορίες που “κατοικούν”στην κάρτα αλλά και τις πληροφορίες που “κατοικούν” σε έναν απομακρυσμένο διακομιστή προσβάσιμο μέσω του διαδικτύου.

Η κύρια γραμμή άμυνας είναι η χρήση των μεθόδων ελέγχου ταυτότητας που προστατεύει από μη εξουσιοδοτημένη πρόσβαση σε δεδομένα που είναι αποθηκευμένα στην κάρτα. Οι έξυπνες κάρτες συνήθως έχουν προγραμματιστεί να απαιτούν ένα προσωπικό αριθμό αναγνώρισης (PIN). Για την προστασία των πιο ευαίσθητων δεδομένων όπως τα ιατρικά, οι έξυπνες κάρτες μπορούν να απαιτούν πολυπαραγοντική ταυτότητα, η οποία είναι ενεργοποιημένη, απαιτώντας το συνδυασμό τριών παραγόντων για πρόσβαση: κάτι που το πρόσωπο γνωρίζει (π.χ., ένα PIN), κάτι που το άτομο έχει (π.χ. η ίδια η έξυπνη κάρτα), και κάτι το οποίο το άτομο είναι (π.χ., ένα βιομετρικό χαρακτηριστικό, όπως ένα δακτυλικό αποτύπωμα). Οι έξυπνες κάρτες μπορούν επίσης να προγραμματιστούν για την επιβολή των κανόνων πρόσβασης χρήστη, επιτρέποντας μόνο σε γιατρούς, νοσοκομεία και συγκεκριμένο ιατρικό προσωπικό να έχουν πρόσβαση σε όλη ή μέρος της ιατρικής πληροφορίας ενός ασθενούς.

Οι έξυπνες κάρτες μπορούν να προστατεύσουν τα αποθηκευμένα δεδομένα μέσω της χρήσης της κρυπτογράφησης και άλλων μεθόδους κρυπτογραφησης ενεργοποιημένων από μικροεπεξεργαστή της κάρτας, όπως η δημιουργία κλειδιού, ασφαλή αποθήκευση κλειδιών, hashing, και ψηφιακές υπογραφές.

Έξυπνες κάρτες μπορούν να επικυρώσουν την αυθεντικότητά τους κάνοντας χρήση ψηφιακών υπογραφών. Οι ψηφιακές υπογραφές μπορούν να επιβεβαιώσουν ότι η έξυπνη κάρτα έχει εκδοθεί από μια νόμιμη οργάνωση και ότι τα δεδομένα στην κάρτα δεν έχουν μεταβληθεί από άλλη αρχή.. Μια έξυπνη κάρτα μπορεί επίσης να προγραμματιστεί ώστε να πιστοποιήσει την εγκυρότητα ενός αναγνώστη κάρτας ή άλλης συσκευής που έχει πρόσβαση σε πληροφορίες της.

Οι έξυπνες κάρτες κατασκευάζονται με αντίμετρα ασφαλείας που ματαιώνουν τις πιθανότητες κλωνοποίησης, παραχάραξης, και αλλοίωσης. Built-in χαρακτηριστικά ασφαλείας περιλαμβάνουν μεταλλικά στρώματα, αισθητήρες που ανιχνεύουν τις θερμικές και υπεριώδεις με φως επιθέσεις,

Ανάλογα με την ευαισθησία των δεδομένων, τα χαρακτηριστικά ασφαλείας που υποστηρίζονται από έξυπνες κάρτες μπορούν να χρησιμοποιηθούν μεμονωμένα ή σε συνδυασμό, δημιουργώντας μια πολυεπίπεδη προσέγγιση. Η ποικιλία και η αποτελεσματικότητα αυτών των χαρακτηριστικών ασφαλείας καθιστούν την τεχνολογία έξυπνων καρτών εξαιρετικά ανθεκτική στην κλωνοποίηση, πλαστογραφία και παραποίηση.

Επίσης, επιτρέπουν πλέον τη δημιουργία RSA κλειδιών μήκους 1024 ή και 2048 bit από τον επεξεργαστή της κάρτας σε εύλογο χρονικό διάστημα (10 – 20 δευτερόλεπτα). Σχεδόν όλες οι εφαρμογές που χρησιμοποιούν έξυπνες κάρτες βασίζονται στο γεγονός ότι είναι πολύ δύσκολο να πλαστογραφηθεί η κάρτα ή να υπάρξει μη εξουσιοδοτημένη πρόσβαση στα προστατευόμενα δεδομένα που περιέχονται στην κάρτα.

Το κυριότερο μειονέκτημα της τεχνολογίας είναι η απαίτηση για την ύπαρξη συσκευής ανάγνωσης (smart card reader) στον υπολογιστή που θα χρησιμοποιηθεί η κάρτα. Μέχρι σήμερα η πλειονότητα των κατασκευαστών υπολογιστών δεν περιλαμβάνει συσκευές ανάγνωσης στις βασικές συνθέσεις των προϊόντων τους, παρόλο που το κόστος των συσκευών έχει μειωθεί σημαντικά.

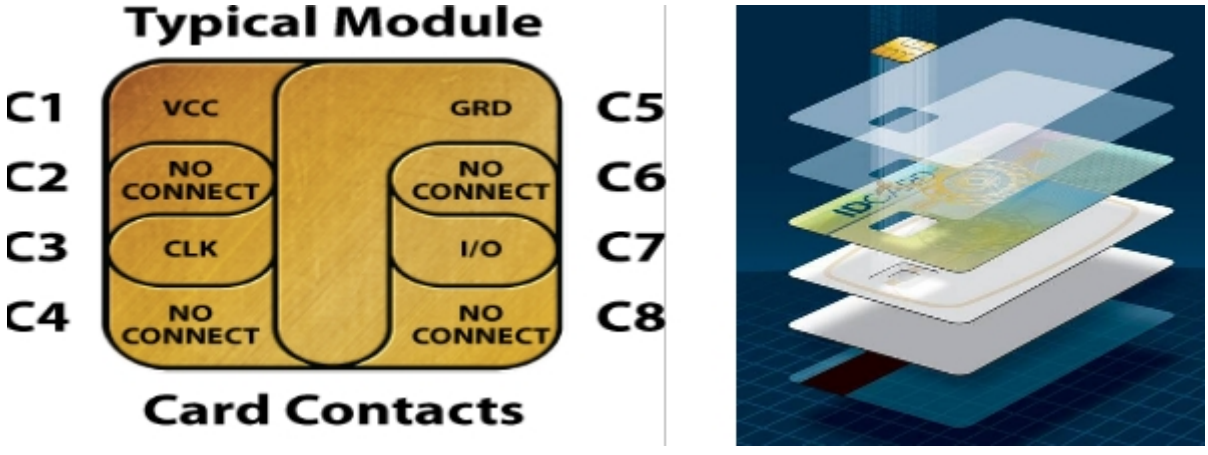
Λύση σε αυτό το πρόβλημα φαίνεται να δίνει η τεχνολογία των USB tokens, δηλαδή έξυπνων καρτών σε μέγεθος “μπρελόκ”, που συνδέονται σε υπολογιστή μέσω θύρας USB. Με την συγκεκριμένη λύση παρέχεται πλήρης προστασία από μη εξουσιοδοτημένη πρόσβαση σε συστήματα ακόμα και αν τα συστήματα αυτά κλαπούν με απώτερο σκοπό την πρόσβαση σε πληροφορίες που αποθηκεύονται σε σκληρούς δίσκους και μέσα μεταφοράς δεδομένων όπως USB sticks, floppy disks, συσκευές backup κλπ. Η απόλυτη κρυπτογράφηση των δεδομένων και η προηγμένη ασφάλεια πρόσβασης κατά την εκκίνηση του συστήματος πριν την πρόσβαση στο λειτουργικό σύστημα με χρήση USB Token και Personal Identification Number (PIN), διασφαλίζουν το απόρρητο των πληροφοριών σε μη εξουσιοδοτημένους χρήστες.

Ο όρος «έξυπνη κάρτα» χρησιμοποιείται κυρίως για τις κάρτες με μικροεπεξεργαστή. Αυτές είναι οι πιο καινούργιες και πιο έξυπνες της οικογένειας ID-1, που ακολουθούν τις

προδιαγραφές του ISO 7816. Το χαρακτηριστικό τους στοιχείο είναι η ύπαρξη ενός ολοκληρωμένου κυκλώματος πάνω στην κάρτα, το οποίο διαθέτει στοιχεία για μετάδοση, αποθήκευση και επεξεργασία δεδομένων. Οι λειτουργίες της μνήμης όπως η ανάγνωση, η εγγραφή και η διαγραφή μπορούν να γίνουν κάτω από ειδικές συνθήκες, που ελέγχονται τόσο από το λογισμικό όσο και από το υλικό. Αυτοί οι τύποι κάρτας μας δίνουν τη δυνατότητα να έχουμε πολύ μεγαλύτερο χώρο για αποθήκευση δεδομένων.

Καθώς η πρόσβαση στα δεδομένα λαμβάνει χώρα μόνο από μια σειριακή διεπαφή, η οποία ελέγχεται από ένα λειτουργικό σύστημα ασφαλείας, είναι δυνατόν να εγγραφούν εμπιστευτικά δεδομένα στην κάρτα, με τέτοιο τρόπο ώστε να μην μπορούν να υποκλαπούν. Αυτά τα εμπιστευτικά δεδομένα μπορεί κανείς να τα επεξεργαστεί μόνο εσωτερικά μέσω της υπολογιστικής μονάδας.

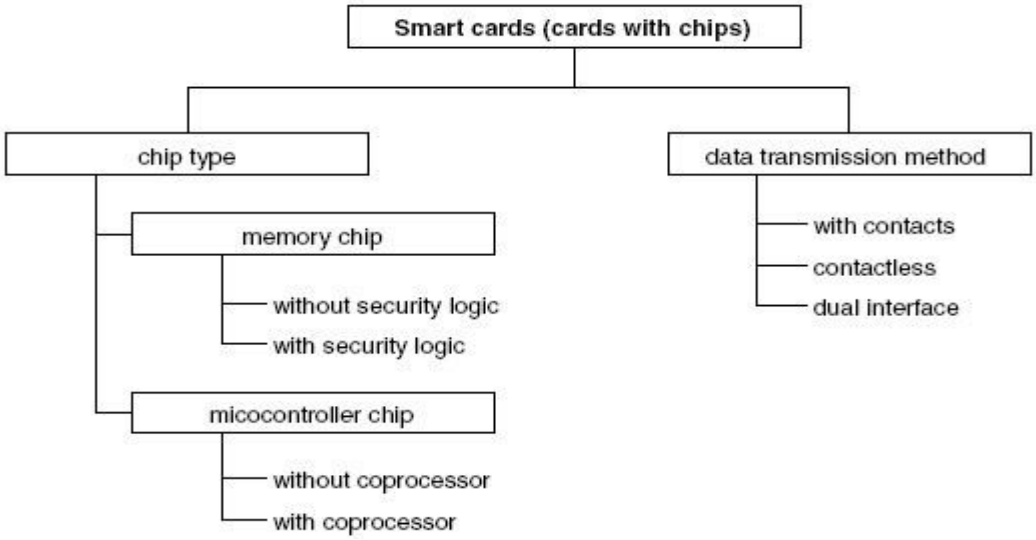
Το πρότυπο για έξυπνες κάρτες, ISO 7816, βασίζεται στο format ID-1. Το μέγεθος της κάρτας καθώς και τα υπόλοιπα φυσικά χαρακτηριστικά της, η ανθεκτικότητα της κάρτας στην θερμοκρασία, η ελαστικότητά της, η θέση των ηλεκτρικών επαφών και η λειτουργία τους, ο τρόπος επικοινωνίας του ολοκληρωμένου κυκλώματος με τον έξω κόσμο καθορίζονται από τον Διεθνή Οργανισμό Τυποποίησης (International Organization for Standardization, ISO).




*Σχήμα 5.2 Εξωτερική όψη μιας smart card και οι επαφές της*

Η ταξινόμηση των έξυπνων καρτών μπορεί να γίνει βάσει πληθώρας κριτηρίων και συγκεκριμένα, ανάλογα με το είδος της λογικής που περιέχουν, ανάλογα με τον τύπο των

επαφών τους και ανάλογα με το είδος και το πλήθος των εφαρμογών που υποστηρίζουν. Οι έξυπνες κάρτες μπορούν να ταξινομηθούν όπως φαίνεται στο παρακάτω σχήμα:




*Σχήμα 5.3: Ταξινόμηση έξυπνων καρτών*

Οι έξυπνες κάρτες χωρίζονται σε δύο κατηγορίες ανάλογα με το αν έχουν μικροεπεξεργαστή (CPU) ή όχι. Οι κάρτες χωρίς μικροεπεξεργαστή ονομάζονται κάρτες μνήμης (memory cards). Οι κάρτες με ολοκληρωμένο κύκλωμα (Integrated Circuit Cards) είναι γνωστές επίσης και ως κάρτες με μικροεπεξεργαστή (microprocessor cards) ή ως κάρτες με chip (chip cards).

Σύμφωνα με το σχήμα, η έξυπνη κάρτα ανταλλάσσει δεδομένα με τον έξω κόσμο με δύο τρόπους:

1) Μέσω επιχρυσωμένων επαφών (gold plated contacts). Αυτές οι κάρτες ονομάζονται κάρτες επαφής (contact smartcards).

2) Με εκπομπή ραδιοσυχνότητας (radio frequency) χρησιμοποιώντας μια κεραία ενσωματωμένη στην κάρτα. Αυτές οι κάρτες ονομάζονται έξυπνες κάρτες άνευ επαφής (contactless smartcards).

Για να έχουμε ανταλλαγή πληροφορίας εάν έχουμε κάρτα επαφής, η κάρτα πρέπει να εισαχθεί στη συσκευή ανάγνωσης (reader). Όταν έχουμε κάρτα άνευ επαφής πρέπει να τοποθετηθεί κοντά στην ειδική συσκευή ανάγνωσης άνευ επαφής (contactless reader).

Βασικός σκοπός των έξυπνων καρτών στο πλαίσιο της ηλεκτρονικής ταυτότητας είναι να πραγματοποιούν ευαίσθητες από άποψη ασφάλειας, κρυπτογραφικές λειτουργίες (δημιουργία ζεύγους κλειδιών, αποθήκευση και ελεγχόμενη πρόσβαση στο ιδιωτικό κλειδί του ζεύγους) στο προστατευόμενο εσωτερικό τους περιβάλλον. Λόγω των κρυπτογραφημένων αρχείων συστήματος, το ιδιωτικό κλειδί δεν αποθηκεύεται στη μνήμη ή σε δίσκο ηλεκτρονικού υπολογιστή, δηλαδή σε περιοχή από όπου οι πιθανότητες διαρροής του είναι συγκριτικά μεγαλύτερες. Τα δεδομένα μπορούν πλέον να αποθηκεύονται σε αρχεία με ασφάλεια.

Επίσης, οι έξυπνες κάρτες μπορούν να κάνουν τον έλεγχο αυθεντικότητας κατά την πρόσβαση σε ηλεκτρονικές υπηρεσίες πιο ασφαλή. Συνήθως, ο έλεγχος αυθεντικότητας με έξυπνες κάρτες γίνεται με χρήση ψηφιακών πιστοποιητικών, που βρίσκονται αποθηκευμένα στην κάρτα. Π.χ. αντί για όνομα χρήστη και κωδικό ασφαλείας, ο κάτοχος της έξυπνης κάρτας και του ψηφιακού πιστοποιητικού μπορεί να ακολουθήσει μια διαδικασία πρόκλησης - απόκρισης (challenge - response). Κατά τη διαδικασία αυτή, ο χρήστης αρχικά παρουσιάζει το πιστοποιητικό του. Στη συνέχεια, στον χρήστη παρουσιάζεται μια τυχαία συμβολοσειρά κρυπτογραφημένη με το δημόσιο κλειδί του (πρόκληση). Ο χρήστης αποκρυπτογραφεί την πρόκληση με το ιδιωτικό του κλειδί και την επιστρέφει (απόκριση). Ο έλεγχος αυθεντικότητας επιτυγχάνεται, καθώς αφενός αποδεικνύεται η γνησιότητα και το αναλλοίωτο του πιστοποιητικού (με την υπογραφή της Αρχής Πιστοποίησης) και αφετέρου αποδεικνύεται ότι ο χρήστης είναι πράγματι ο ιδιοκτήτης του πιστοποιητικού, αφού μόνο ο ιδιοκτήτης έχει πρόσβαση στο ιδιωτικό κλειδί για την αποκρυπτογράφηση της πρόκλησης, με την προϋπόθεση βέβαια να μην έχει διαρρεύσει το ιδιωτικό κλειδί. Επίσης, στην περίπτωση της δημιουργίας ψηφιακών υπογραφών, η αυξημένη προστασία που παρέχουν οι έξυπνες κάρτες στο ιδιωτικό κλειδί, καθιστούν τις ψηφιακές υπογραφές περισσότερο αξιόπιστες.

Οι έξυπνες κάρτες προσφέρουν ένα αριθμό πλεονεκτημάτων σε σύγκριση με τις κάρτες μαγνητικής ταινίας. Για παράδειγμα, η μέγιστη αποθηκευτική ικανότητα μιας έξυπνης κάρτας είναι πολλές φορές μεγαλύτερη από αυτή μιας κάρτας με μαγνητική ταινία. Μόνο οι οπτικές κάρτες που θα αναφέρονται παρακάτω έχουν τη δυνατότητα μεγαλύτερης αποθηκευτικής ικανότητας. Επιπλέον, τα πλεονεκτήματα των έξυπνων καρτών έχουν να

κάνουν με την υψηλό βαθμό αξιοπιστίας που προσφέρουν και την μεγάλη διάρκεια ζωής που διαθέτουν σε σύγκριση με αυτή των μαγνητικών καρτών.

#### 5.2.2.1 Κάρτες μνήμης (memory cards)

Οι πρώτες έξυπνες κάρτες που δημιουργήθηκαν ήταν οι κάρτες μνήμης που αποτελούν ακόμα και σήμερα την πλειονότητα των καρτών που χρησιμοποιούνται. Μία κάρτα μνήμης δεν έχει ενσωματωμένο μικροεπεξεργαστή και μπορεί να χρησιμοποιηθεί μόνο για αποθήκευση δεδομένων. Η μνήμη που χρησιμοποιείται ονομάζεται EEPROM (Electrically Erasable Programmable Read-Only Memory).

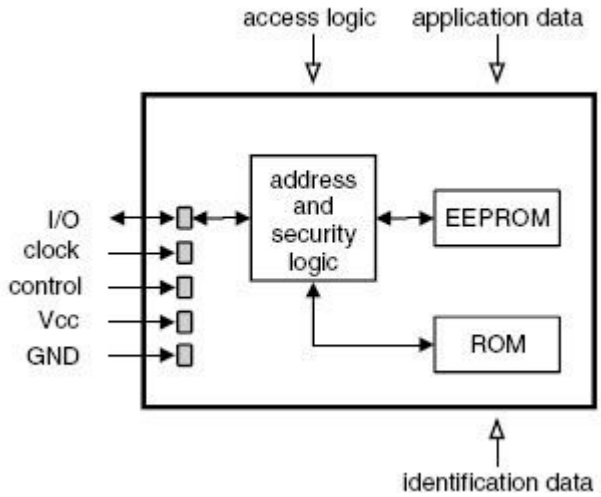
Μπορούν να αποθηκεύσουν από μερικές εκατοντάδες bit συνήθως 16Kbyte πληροφορίας. Η πρόσβαση στην μνήμη ελέγχεται από μια μονάδα έλεγχου λογικής (security logic), η οποία στην πιο απλή περίπτωση αποτελείται από προστασία γραφής ή διαγραφής για όλη ή για ορισμένες περιοχές μνήμης. Τα πιο περίπλοκα μοντέλα μπορούν να εκτελέσουν απλές κρυπτογραφικές λειτουργίες και περιορίζουν την πρόσβαση για ανάγνωση (restricted read access).

Στην ουσία, το κανάλι επικοινωνίας ανάμεσα στο χρήστη και την κάρτα βρίσκεται πάντα υπό τον άμεσο έλεγχο της συσκευής ανάγνωσης. Τα δεδομένα μεταφέρονται στην κάρτα και από την κάρτα μέσω της θύρας Εισόδου/Εξόδου. Στις κάρτες μνήμης δεν υπάρχει κάποιος μηχανισμός ασφαλείας με αποτέλεσμα συχνά τα δεδομένα να είναι εκτεθειμένα σε μη εξουσιοδοτημένη πρόσβαση.

Οι κάρτες μνήμης είναι τυπικά πολύ φθηνότερες και πολύ λιγότερο λειτουργικές από τις κάρτες με μικροεπεξεργαστή και μειονεκτούν στα θέματα προστασίας και διαχείρισης δεδομένων. Η απλή τεχνολογία τους, τους δίδει την δυνατότητα να κατασκευάζονται πολύ φθηνά και να κοστίζουν κάτω από US $1 η μία σε μεγάλες ποσότητες.

Το τρίτο τμήμα του πρωτοκόλλου [ISO 7816 Part 3] ορίζει έναν ειδικό σύγχρονο τρόπο μεταφοράς, ο οποίος επιτρέπει την ανάπτυξη απλών και οικονομικών κυκλωμάτων. Ωστόσο κάποιες κάρτες χρησιμοποιούν το I2C bus, το οποίο χρησιμοποιείται κυρίως σε συνδυασμό με σειριακής πρόσβασης μνήμες. Οι κάρτες μνήμης χρησιμοποιούνται κυρίως για προπληρωμένες τηλεφωνικές συνδιαλέξεις και κάρτες ασφάλειας υγείας.

Το σχήμα στη συνέχεια περιγράφει τη δομή του αρχιτεκτονικού διαγράμματος μιας κάρτας μνήμης.




*Σχήμα 5.4: Το block διάγραμμα μιας κάρτας μνήμης.*

- I/O: Χρησιμοποιείται για μεταφορά δεδομένων μεταξύ κάρτας και αναγνώστη χωρίς να υπάρχει αμφίδρομη κατεύθυνση.

- Clock: Χρησιμοποιείται για την εφαρμογή εξωτερικού ρολογιού.

- Control: Χρησιμοποιείται για την μεταφορά των σημάτων ελέγχου.

- Vcc: Χρησιμοποιείται για την παροχή τάσης στο Ολοκληρωμένο.

- GND: Χρησιμοποιείται για τη σύνδεση με τη γη.

### 5.2.2.2 Κάρτες μαγνητικής ταινίας


*Σχήμα 5.5: Δύο όψεις κάρτας μαγνητικής ταινίας*

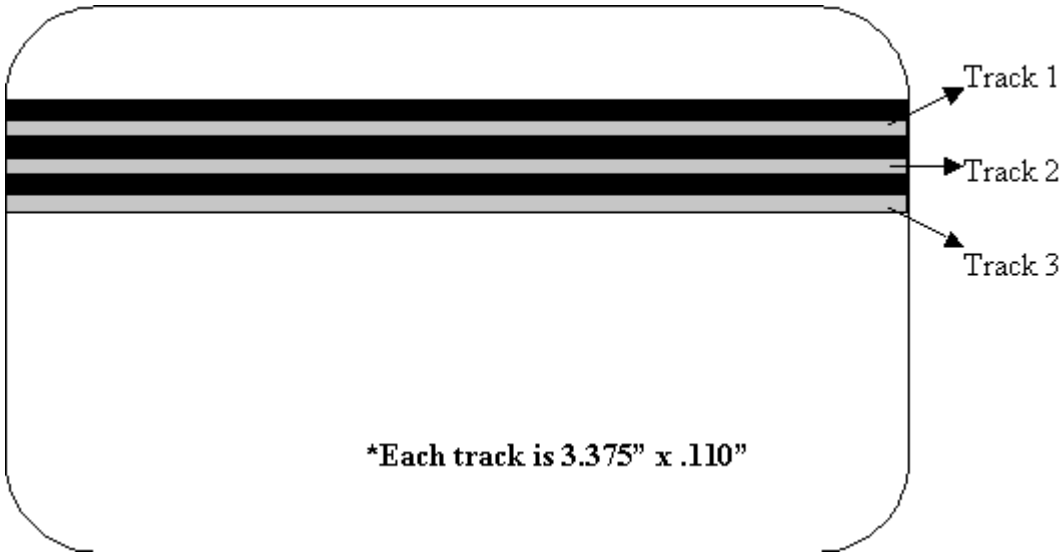
Το ουσιαστικό πρόβλημα των ανάγλυφων καρτών είναι ότι δημιουργούν ένα μεγάλο αριθμό από χάρτινες αποδείξεις, οι οποίες είναι δύσκολο να επεξεργαστούν. Μια λύση σε αυτό το θέμα είναι η ψηφιακή κωδικοποίηση των δεδομένων της κάρτας σε μια μαγνητική ταινία η οποία βρίσκεται στο πίσω μέρος της κάρτας. Η μαγνητική ταινία διαβάζεται αφού τη διαπεράσουμε κατά μήκος μιας συσκευής ανάγνωσης είτε με μηχανικό, είτε με αυτόματο τρόπο. Η επεξεργασία αυτή δεν απαιτεί την χρήση χαρτιού.

Τα μέρη [ISO 7811 2, 3, 4] καθορίζουν τις ιδιότητες μιας μαγνητικής κάρτας, τις τεχνικές κωδικοποίησης και την θέση των μαγνητικών ταινιών.

Η μαγνητική ταινία μπορεί να περιέχει μέχρι τρεις τομείς. Οι τομείς (1) και (2) είναι καθορισμένοι έτσι ώστε να έχουν μόνο δυνατότητα ανάγνωσης, ενώ ο τομέας (3) έχει και δικαιώματα γραφής. Ακόμα και αν η αποθηκευτική δυνατότητα μιας μαγνητικής ταινίας είναι περίπου 1000 bits, κάτι το οποίο δεν είναι πολύ, είναι ωστόσο υπεραρκετό για την αποθήκευση των στοιχείων που υπάρχουν στις ανάγλυφες κάρτες. Επιπλέον τα δεδομένα μπορούν να γραφούν ή να διαβαστούν στον τρίτο τομέα, όπως η τελευταία συναλλαγή που έλαβε χώρα.

Οι κάρτες μαγνητικής ταινίας είναι ευρέως διαδεδομένες και χρησιμοποιούνται από το μεγαλύτερο μέρος του πληθυσμού, όπως στις πιστωτικές κάρτες, στις κάρτες αυτόματης ανάληψης μετρητών, στις κάρτες ελέγχου πρόσβασης σε κτίρια. Οι κάρτες μαγνητικής ταινίας χρησιμοποιούνται για να αποθηκεύουν πληροφορίες σε μορφή αναγνώσιμη από μηχανές και έτσι έχουν αυτοματοποιήσει καθημερινές συναλλαγές και διαδικασίες. Η

εκτεταμένη τους χρήση έχει σαφώς διευκολύνει τον απλό χρήστη καθώς και διάφορους τραπεζικούς και εμπορικούς οργανισμούς, έχει όμως ταυτόχρονα επιδείξει σημαντικά μειονεκτήματα τα οποία δεν μπορούμε να παραβλέψουμε.




*Σχήμα 5.6: Οι περιοχές των μαγνητικών ταινιών σε κάρτα του [ID-1 format]*

Εξετάζοντας τα μειονεκτήματα αυτά έχουμε να παρατηρήσουμε ότι η κύρια πηγή προβλημάτων έγκειται στο γεγονός ότι τα δεδομένα που αποθηκεύονται στη μαγνητική ταινία μιας κάρτας μπορούν εύκολα να διαβαστούν και να τροποποιηθούν από οποιονδήποτε έχει πρόσβαση στο κατάλληλο εξοπλισμό. Έτσι είναι σαφές ότι εμπιστευτικές και κρίσιμες πληροφορίες, όπως ο κωδικός αναγνώρισης του κατόχου, δεν μπορούν να αποθηκεύονται στην ίδια τη κάρτα, αλλά αναγκαστικά καταχωρούνται σε κάποια κεντρική βάση δεδομένων. Αυτό σημαίνει ότι για να εκτελεστεί οποιαδήποτε συναλλαγή πρέπει το τερματικό συναλλαγής (π.χ. ATM) να είναι online συνδεδεμένο με κάποιο κεντρικό υπολογιστή για να γίνει πιστοποίηση αυθεντικότητας, διαδικασία χρονοβόρα και με υψηλό κόστος.

Έτσι, η χρήση των καρτών μαγνητικής ταινίας συνδυάζεται με την ύπαρξη και συντήρηση μεγάλων κεντρικών συστημάτων για τη διαφύλαξη και επεξεργασία των ευαίσθητων δεδομένων, καθώς και με τη συντήρηση κυκλωμάτων για τις απαραίτητες online συνδέσεις μεταξύ κεντρικών βάσεων δεδομένων και σημείων συναλλαγής.

Επιπλέον, οι κάρτες μαγνητικής ταινίας παρουσιάζουν ευαισθησία σε παράγοντες, όπως τα μαγνητικά πεδία, φθορά των επαφών από αιχμηρά αντικείμενα και η παρατεταμένη χρήση τους, οι οποίοι μπορούν να καταστρέψουν τη μαγνητική ταινία της κάρτας. Επίσης, οι κάρτες αυτές σχεδιάζονται για μία και μόνο εφαρμογή και οποιαδήποτε αλλαγή στα χαρακτηριστικά της εφαρμογής ή στα στοιχεία του κατόχου σημαίνει αντικατάσταση της ίδιας της κάρτας.

Τα παραπάνω στοιχεία, με κυριότερο θέμα την ασφάλεια δεδομένων και της εγκυρότητας των συναλλαγών, καθιστούν τις κάρτες μαγνητικής ταινίας ένα προϊόν που δεν μπορεί να καλύψει πλήρως τις συνεχώς αυξανόμενες ανάγκες και απαιτήσεις της σύγχρονης εποχής.

Οι κατασκευαστές αυτού του είδους καρτών χρησιμοποιούν διάφορα μέσα προκειμένου να μπορούν να προστατεύσουν τα δεδομένα που υπάρχουν στην μαγνητική ταινία από την πλαστογραφία. Για παράδειγμα, οι κάρτες German Eurocheck περιέχουν ένα αόρατο και χωρίς την δυνατότητα τροποποίησης του κώδικα στο σώμα της κάρτας, ο οποίος καθιστά αδύνατη την αλλοίωση ή την αναπαραγωγή της μαγνητικής ταινίας. Ωστόσο, αυτή όπως και άλλες τεχνικές απαιτούν ένα ειδικό αισθητήρα στο τερματικό της κάρτας, το οποίο αυξάνει το κόστος.

### 5.2.2.3 Κάρτες με μικροεπεξεργαστή (Microprocessor cards)

Σε εφαρμογές που η ασφάλεια έχει σημαντικό ρόλο χρησιμοποιούνται κάρτες με μικροεπεξεργαστή. Το κύριο γνώρισμα των καρτών με μικροεπεξεργαστή, είναι ότι περιλαμβάνουν στο σώμα τους, επεξεργαστή περιορισμένων δυνατοτήτων (8 bit ή 16 bit επεξεργαστή). Αυτές οι κάρτες είναι οι μόνες που μπορούν να χαρακτηριστούν τεχνικά ως έξυπνες κάρτες.

Οι μικροεπεξεργαστές λειτουργούν όπως ένας υπολογιστής με θύρα εισόδου / εξόδου, λειτουργικό σύστημα και σκληρό δίσκο. Μπορούν να αποθηκεύσουν και να επεξεργαστούν δεδομένα, κυρίως όμως ξεχωρίζουν λόγω της δυνατότητάς τους για δυναμική κρυπτογράφηση και για ενημερώσεις στις εφαρμογές τους. Αυτό σημαίνει ότι μπορεί να

προσθέσει ή να αφαιρέσει εφαρμογές ή ακόμα να βελτιώσει μία υπάρχουσα εφαρμογή, γεγονός που καθιστά τις κάρτες με μικροεπεξεργαστή πολύ ευέλικτες.


*Σχήμα 5.7: Έξυπνη κάρτα με μικροεπεξεργαστή και ηλεκτρικές επαφές*

Ο επεξεργαστής μπορεί να υποστηρίξει διαδικασίες εγγραφής, ανάγνωσης και ενημέρωσης πληροφορίας καθώς και κρυπτογράφησης / αποκρυπτογράφησης δεδομένων αποθηκευμένων στην EEPROM. Χειρίζεται την περιοχή της μνήμης και τη πρόσβαση σε αρχεία και οργανώνει την πληροφορία σε συγκεκριμένες δομές αρχείων μέσω ενός λειτουργικού συστήματος της κάρτας (Card Operating System – COS).

Η καρδιά του κυκλώματος σε μία κάρτα με μικροεπεξεργαστή είναι ένας επεξεργαστής, ο οποίος περιβάλλεται από τις εξής λειτουργικές μονάδες:

• **ROM.** Στη μνήμη ROM περιέχεται το λειτουργικό σύστημα της κάρτας, το οποίο εκτελεί τις εντολές που δίδονται από το τερματικό. Το περιεχόμενο της ROM είναι πανομοιότυπο για κάθε κύκλωμα κάθε παραγωγικού κύκλου και δεν μπορεί να αλλάξει κατά τη διάρκεια της ζωής του κυκλώματος.

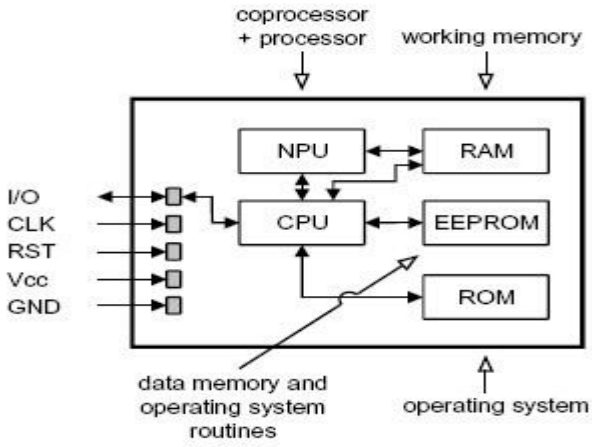
• **EEPROM (Electrically Erasable PROMs).** Αποτελεί έναν τύπο EPROM, στον οποίο τα περιεχόμενα μπορούν να σβηστούν με την εφαρμογή ηλεκτρικών παλμών και έτσι δε

χρειάζεται να τοποθετήσουμε το chip της μνήμης στον ειδικό θάλαμο με τις υπεριώδης ακτίνες. Όλη η διαδικασία ελέγχεται από ειδικό λογισμικό. Στη συνέχεια, μπορούν να αναπρογραμματιστούν όπως και οι απλές EPROMs. Οι EEPROMs διαφέρουν από τις μνήμες RAM στο ότι η εγγραφή, αλλά και η διαγραφή ενός byte απαιτεί περισσότερο χρόνο αν και οι χρόνοι προσπέλασης για την ανάγνωση ROM, PROM, EPROM, και RAM είναι συγκρίσιμοι (λίγες εκατοντάδες nanoseconds).

• **RAM**. Η μνήμη RAM είναι η βοηθητική μνήμη του μικροεπεξεργαστή και τα δεδομένα που είναι αποθηκευμένα σε αυτή χάνονται κάθε φορά που η κάρτα τίθεται εκτός λειτουργίας.

• **I/O port.** Η σειριακή I/O διεπαφή συνήθως αποτελείται από ένα καταχωρητή, δια μέσω του οποίου τα δεδομένα μεταφέρονται ανά bit από και προς την κάρτα.

• **NPU** (Numeric Processor Unit) Χρησιμοποιείται σε μεγάλους αριθμητικούς υπολογισμούς, όπως για παράδειγμα για τη δημιουργία ενός ζεύγους κλειδιών σε μία PKI εφαρμογή, χρησιμοποιείται και ένας βοηθητικός επεξεργαστής NPU για τον γρήγορο υπολογισμό των απαιτούμενων αλγορίθμων.




*Σχήμα 5.8: Το block διάγραμμα μιας κάρτας με μικροεπεξεργαστή*

Έχουν δυνατότητα ανάγνωσης/εγγραφής καθώς και υψηλή ασφάλεια που επιτυγχάνεται με τον μικροεπεξεργαστή. Είναι πιο ακριβές από τις κάρτες μνήμης και κοστίζουν περίπου US $5. Το λειτουργικό σύστημα είναι αποθηκευμένο στη ROM, η CPU χρησιμοποιεί την RAM σαν μνήμη εργασίας και τα περισσότερα δεδομένα είναι αποθηκευμένα στην EEPROM.

Τα τυπικά μεγέθη που είναι διαθέσιμα σε RAM, EEPROM, ROM φαίνονται στον πίνακα που ακολουθεί.

| | |
|---|---|
| **RAM** | **256 bytes έως 1 Kbyte** |
| **EEPROM** | **1 Kbytes έως 64 Kbytes** |
| **ROM** | **6 Kbytes έως 32 Kbytes** |
| **Μικροεπεξεργαστής** | **8 bits στα περίπου 5 MHz** |
| **Ταχύτητα διεπιφάνειας επικοινωνίας** | **9600 bits/sec** |

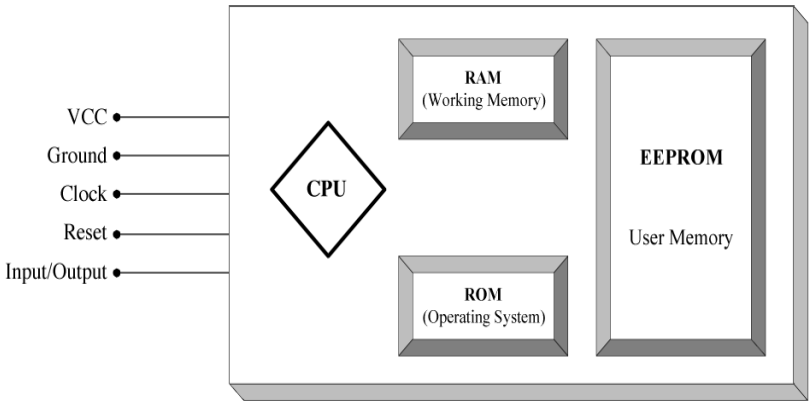
*Πίνακας 5.1 Τυπική αρχιτεκτονική Έξυπνων Καρτών*

Η CPU των έξυπνων καρτών είναι συνήθως ένας μικροεπεξεργαστής 8-bit και το μέγεθος της RAM που χρησιμοποιείται είναι 256 bytes. Ο λόγος που χρησιμοποιείται αυτό το μικρό μέγεθος RAM είναι ότι η μνήμη RAM απαιτεί περισσότερο χώρο για κάθε byte από την EEPROM ή την μνήμη ROM. Για αυτό το λόγο την διατηρούμε μικρή, έτσι ώστε να ικανοποιούμε τον περιορισμό για τα chips των έξυπνων καρτών, τα οποία πρέπει να έχουν μέγεθος 25mm. Το μέγεθος της ROM ποικίλει από λίγα KB έως περίπου 32 KB, ανάλογα με τις λειτουργίες του λειτουργικού συστήματος. Το λειτουργικό σύστημα φορτώνεται κατά την παράγωγη του chip της κάρτας. Επειδή το λειτουργικό σύστημα βρίσκεται στην ROM δεν μπορεί να αναβαθμιστεί σε νέα έκδοση έπειτα από την παραγωγή της κάρτας. Η EEPROM αντιστοιχεί στον σκληρό δίσκο του υπολογιστή και χρησιμοποιείται για να διατηρεί όλα τα δεδομένα και τα προγράμματα.

Το λειτουργικό σύστημα παρέχει προστασία των αρχείων της EEPROM περιορίζοντας την πρόσβαση σε αυτήν. Το μέγεθος της EEPROM ποικίλει ανάλογα με τις ανάγκες της εφαρμογής. Το πιο δημοφιλές μέγεθος σήμερα είναι τα 8 KB. Έως σήμερα το μεγαλύτερο μέγεθος EEPROM που είναι διαθέσιμο είναι 64 KB. Η είσοδος / έξοδος (I/O) χρησιμοποιείται για να μεταφέρονται δεδομένα σειριακά με τυπική ταχύτητα 9600 bits/sec.

Αν και το chip της κάρτας θεωρείται ένας μικρός υπολογιστής, η συσκευή που χρησιμοποιείται στην ανάγνωση και στην εγγραφή των έξυπνων καρτών, γνωστή ως αναγνώστης έξυπνων καρτών (smartcard reader) πρέπει να παρέχει την ηλεκτρική τάση, τη γείωση και το χρονισμό.

Οι κάρτες με μικροεπεξεργαστή είναι πολύ ευέλικτες στην χρήση. Στην πιο απλή περίπτωση περιέχουν ένα βελτιστοποιημένο λογισμικό για μια εφαρμογή κι έτσι μπορούν να χρησιμοποιηθούν μόνο για τη συγκεκριμένη εφαρμογή. Ωστόσο, το λειτουργικό σύστημα των σύγχρονων καρτών επιτρέπει την ενσωμάτωση πολλών διαφορετικών εφαρμογών σε μια κάρτα. Στην περίπτωση αυτή η ROM περιέχει μόνο βασικές εντολές του λειτουργικού συστήματος, και το ειδικό τμήμα για την εφαρμογή του προγράμματος φορτώνεται στην EEPROM. Ειδικά ολοκληρωμένα κυκλώματα με υψηλές δυνατότητες επεξεργασίας και μεγάλη αποθηκευτική ικανότητα έχουν αναπτυχθεί προκειμένου να εκτελούν υψηλής απόδοσης εφαρμογές με ασφάλεια και υπολογισμό περίπλοκων κρυπτογραφικών αλγορίθμων.




*Σχήμα 5.9: Αρχιτεκτονική έξυπνων καρτών*

### 5.2.2.4 Κρυπτογραφικές κάρτες με συνεπεξεργαστή (Cryptographic Coprocessor Cards)

Αν και τεχνικά αυτές οι κάρτες ανήκουν στην κατηγορία των καρτών με μικροεπεξεργαστή, τις διαχωρίζουμε επειδή έχουν διαφορές στο κόστος, στην λειτουργικότητα και περιλαμβάνουν κρυπτογραφικές επιπλέον λειτουργίες συνεπεξεργαστή.

Στις λειτουργίες αυτές συμπεριλαμβάνονται, η δημιουργία ζεύγους RSA κλειδιών (συνήθως μήκους 512 – 1024 bit), η δημιουργία και η επαλήθευση ψηφιακών υπογραφών, η κρυπτογράφηση και η αποκρυπτογράφηση καθώς και ο καθορισμός της πολιτικής χρήσης του ζεύγους κλειδιών.

Επειδή οι κοινοί ασύμμετροι κρυπτογραφικοί αλγόριθμοι (όπως ο RSA) απαιτούν πολύπλοκους μαθηματικούς υπολογισμούς, ένας μικροεπεξεργαστής 8 bit με πολλή λίγη RAM μπορεί να χρειαστεί χρόνο της τάξης μερικών λεπτών για να εκτελέσει μια λειτουργία με ιδιωτικό κλειδί των 1024 bit. Αν όμως προστεθεί ένας κρυπτογραφικός συνεπεξεργαστής στην αρχιτεκτονική, ο χρόνος που απαιτείται για την ίδια λειτουργία μειώνεται στα 100 μικροδευτερόλεπτα.

Οι συνεπεξεργαστές περιέχουν επιπρόσθετες αριθμητικές μονάδες που έχουν αναπτυχθεί ειδικά για πράξεις μεγάλων ακεραίων και τον γρήγορο υπολογισμό εκθετικών. Το μειονέκτημα αυτών των καρτών είναι το υψηλό τους κόστος. Η προσθήκη ενός κρυπτογραφικού συνεπεξεργαστή μπορεί να αυξήσει το κόστος της κάρτας από 50% έως 100%. Η αύξηση του κόστους μπορεί να μειωθεί φυσικά με τη εκτεταμένη χρήση τους. Παρά το υψηλό κόστος, τα πλεονεκτήματα που προσφέρει η προσθήκη του μικροεπεξεργαστή στην ασφάλεια των συστημάτων είναι τεράστια, διότι το ιδιωτικό κλειδί δεν χρειάζεται ποτέ να απομακρυνθεί από την έξυπνη κάρτα. Αυτό αποτελεί έναν κρίσιμο παράγοντα για εφαρμογές όπως οι ηλεκτρονικές υπογραφές, η εξακρίβωση ταυτότητας (authentication) και η μη άρνηση πράξης (non-repudiation).

Στο μέλλον δεν θα χρειάζεται να χρησιμοποιείται κρυπτογραφικός συνεπεξεργαστής και το κόστος των καρτών θα μειωθεί αρκετά. Οι βασικοί επεξεργαστές θα γίνουν αρκετά ισχυροί για να εκτελούν πολύπλοκους μαθηματικούς υπολογισμούς, όπως, οι αλγόριθμοι που βασίζονται στις ελλειπτικές καμπύλες (Elliptic Curves) παρέχουν ισχυρή ασφάλεια χωρίς να απαιτείται μεγάλη υπολογιστική ισχύ, αλλά δεν έχει ξεκινήσει ακόμα η εμπορική τους χρήση.

### 5.2.2.5 Έξυπνες κάρτες άνευ επαφής (contactless smart cards)

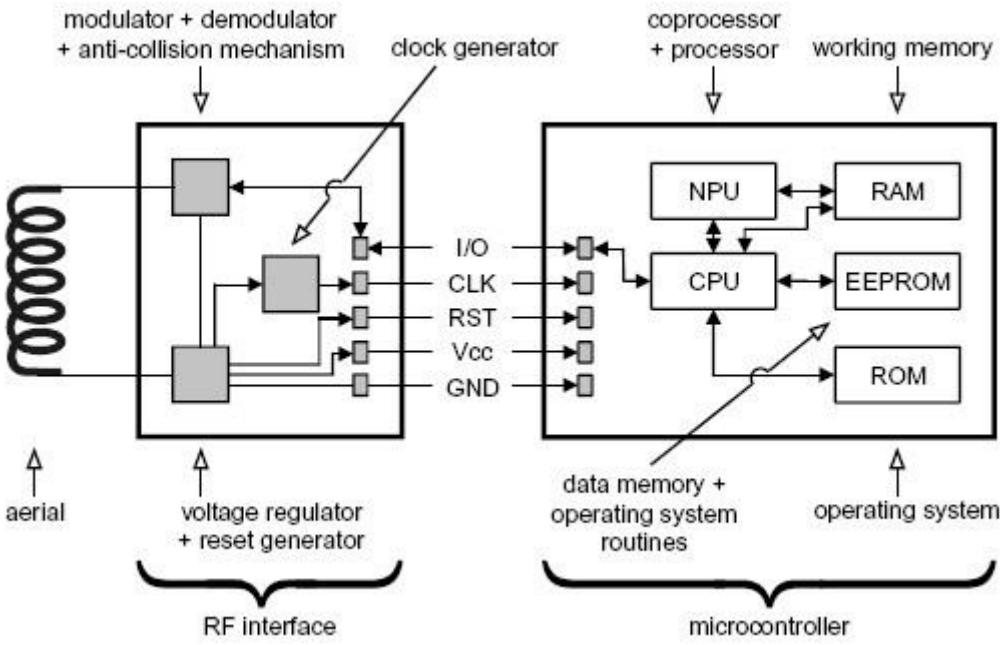
Το κύριο χαρακτηριστικό αυτών των καρτών είναι ότι δεν διαθέτουν ηλεκτρικές επαφές για τη μετάδοση δεδομένων, ηλεκτρικής ενέργειας και σημάτων ελέγχου μεταξύ της

κάρτας και της συσκευής ανάγνωσης. Η επικοινωνία της κάρτας με τη συσκευή ανάγνωσης και η τροφοδοσία της γίνεται μέσω ραδιοσυχνοτήτων που εκπέμπει και λαμβάνει μια κεραία που βρίσκεται ενσωματωμένη στο πλαστικό της έξυπνης κάρτας. Ανάλογα με τη συχνότητα εκπομπής και λήψης, η μέγιστη απόσταση μεταξύ κάρτας και συσκευής ανάγνωσης κυμαίνεται από μερικά εκατοστά για υψηλές συχνότητες μέχρι και ενάμιση μέτρο για χαμηλές συχνότητες.

Οι περισσότερες ασύρματες κάρτες δέχονται τροφοδοσία για τη λειτουργία του chip τους από το ηλεκτρομαγνητικό σήμα μεταξύ κάρτας και αναγνώστη. Στην παρακάτω εικόνα φαίνονται τα τρία στρώματα που στοιχειοθετούν μία ασύρματη κάρτα. Το πάνω και το κάτω στρώμα (εξωτερικά στρώματα) κλείνουν εσωτερικά το επίπεδο με την κεραία και το μικροτσίπ. Η κεραία είναι συνήθως 3 – 5 στροφές από πολύ λεπτό σύρμα (ή αγώγιμο μελάνι) που συνδέεται με το μικροτσίπ.

Οι κάρτες χωρίς επαφές προτιμώνται σε εφαρμογές κατά τις οποίες απαιτείται μεγάλος αριθμός συναλλαγών σε σύντομο χρονικό διάστημα, όπως για παράδειγμα σε εφαρμογές χρέωσης δημόσιων συγκοινωνιακών μέσων (ακυρωτικά μηχανήματα, σταθμοί διοδίων κ.τ.λ.). Είναι πιο ακριβές από τις κάρτες επαφής, αλλά έχουν μεγαλύτερη διάρκεια ζωής και είναι πιο αξιόπιστες. Οι έξυπνες κάρτες άνευ επαφής δεν χρειάζεται να εισαχθούν σε τερματικό αναγνώστη, αφού είναι συστήματα που λειτουργούν έως και ένα μέτρο μακριά. Αυτό είναι ένα πολύ σημαντικό πλεονέκτημα σε σύστημα ελέγχου πρόσβασης (access control). Έτσι για παράδειγμα μία πόρτα που χρειάζεται να ανοίξει, πλέον μπορεί να ανοίξει χωρίς να χρειάζεται να βγάλει από την τσέπη του ή το πορτοφόλι του την κάρτα, αφού δεν απαιτείται η εισαγωγή της κάρτας σε κάποιο μηχάνημα ανάγνωσης. Μια άλλη εμπορική εφαρμογή είναι της τοπικής δημόσιας συγκοινωνίας, κατά την οποία ένας μεγάλος αριθμός ανθρώπων χρειάζεται να αναγνωρισθεί στο μικρότερο δυνατό χρόνο. Ωστόσο, η ασύρματη τεχνολογία έχει πλεονέκτημα ακόμα και στην περίπτωση συστημάτων που απαιτούν την αναγκαστική εισαγωγή της κάρτας στον αναγνώστη, αφού ο τρόπος εισαγωγής δεν παίζει κανένα ρόλο. Αυτό έρχεται σε αντίθεση με τις μαγνητικές κάρτες, ή τις κάρτες με επαφή, οι οποίες πρέπει να εισάγονται με συγκεκριμένο τρόπο στο μηχάνημα του αναγνώστη.

Επομένως, η ελευθερία που προσφέρουν σε σχέση με τους περιορισμούς που θέτουν οι άλλες μορφές καρτών αυξάνει τη λειτουργικότητα των καρτών άνευ επαφής και συνεπώς την αποδοχή τους από τους απλούς χρήστες.




*Σχήμα 5.10: Το block διάγραμμα μιας έξυπνης κάρτας άνευ επαφής.*

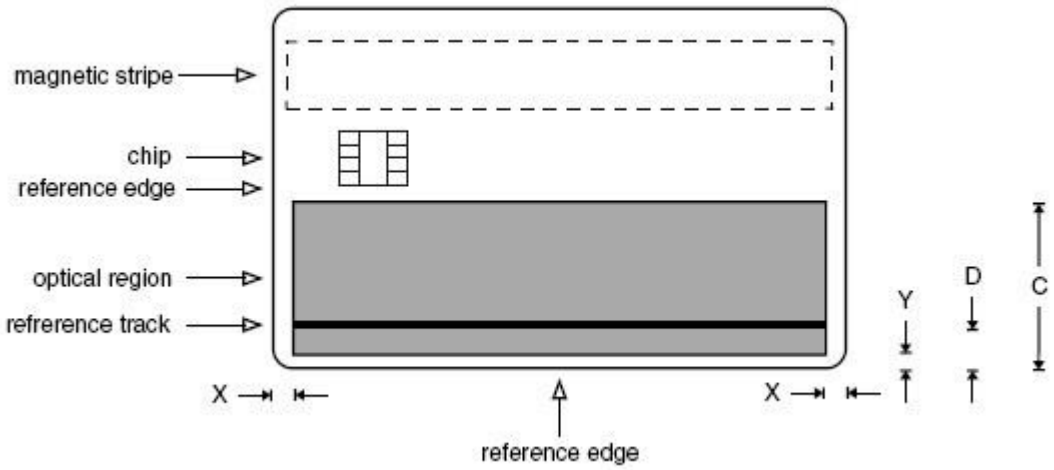
Οσον αφορά την εμπορική εκμετάλλευση των καρτών άνευ επαφής, υπάρχει το πλεονέκτημα ότι κανένα τεχνικό στοιχείο δεν είναι εμφανές στην επιφάνεια της κάρτας και έτσι ο οπτικός σχεδιασμός τέτοιων καρτών δεν περιορίζεται από μαγνητικές ταινίες ή επιφανειακές επαφές. Μέχρι τη δεδομένη στιγμή οι κάρτες αυτές χρησιμοποιούνται κυρίως για την τοπική συγκοινωνία, όπου λειτουργούν ως εισιτήρια. Τα σημερινά συστήματα χρησιμοποιούν κάρτες μιας κύριας λειτουργίας, για την οποία έχουν αναπτυχθεί κυκλώματα με οικονομική λογική. Ωστόσο υπάρχει η πεποίθηση ότι οι κάρτες με πολυλειτουργικότητα θα γίνουν σύντομα οι αντικαταστάτες των ήδη υπαρχόντων απλών καρτών.

### 5.2.2.6 Οπτικές κάρτες μνήμης (optical memory cards)

Η τεχνολογία των οπτικών έξυπνων καρτών χρησιμοποιεί τεχνολογία ανάλογη με αυτή των οπτικών δίσκων (CD-ROM). Μία οπτική έξυπνη κάρτα περιέχει ένα οπτικό μέσο εγγραφής ανάμεσα σε δύο διαφανή προστατευτικά στρώματα. Οι πληροφορίες αποθηκεύονται ψηφιακά σε μορφή 0 και 1 και από τη στιγμή που γράφονται στη μνήμη της κάρτας δεν μπορούν να διαγραφούν.

Τα πρότυπα για τις οπτικές κάρτες μνήμης είναι τα ISO/IEC 11693 και 11694 που καθορίζουν τις διαστάσεις και τα φυσικά χαρακτηριστικά των οπτικών καρτών, καθώς και την τεχνική εγγραφής δεδομένων. Αυτές οι κάρτες μπορούν να αποθηκεύσουν από 1,6 έως 40 megabytes δεδομένων (συνήθως 4). Η μνήμη τους είναι του τύπου write-once/read-many (WORM).

Έχουν συνήθως ένα μικροεπεξεργαστή και χρησιμοποιούν την ασφάλεια των έξυπνων καρτών για να προστατεύσουν τα δεδομένα από μη εξουσιοδοτημένη πρόσβαση.




*Σχήμα 5.11: Μορφή μιας οπτικής έξυπνης κάρτας.*

Ο συνδυασμός της υψηλής αποθηκευτικής ικανότητας των οπτικών καρτών με την ευφυΐα των έξυπνων καρτών έχει ως αποτέλεσμα την προσθήκη νέων ενδιαφέροντων χαρακτηριστικών. Για παράδειγμα, τα δεδομένα μπορούν να γραφούν κρυπτογραφημένα σε μία οπτική κάρτα, ενώ το ιδιωτικό κλειδί είναι ασφαλώς αποθηκευμένο στην μνήμη του

κυκλώματος της κάρτας. Έτσι τα δεδομένα της οπτικής κάρτας είναι προστατευμένα από αναρμόδια πρόσβαση.

Συγκριτικά με τη μνήμη των έξυπνων καρτών, η χωρητικότητα των οπτικών καρτών φαντάζει εξαιρετικά μεγάλη και προσφέρεται για την αποθήκευση ιατρικών δεδομένων (φωτογραφίες υψηλής ανάλυσης, ακτινογραφίες κ.α.). Μειονεκτήματα της τεχνολογίας είναι το υψηλό κόστος και η έλλειψη δυνατότητας επανεγγραφής στην οπτική περιοχή.

#### 5.2.2.7 Υβριδικές κάρτες (hybrid cards)

Αυτού του τύπου κάρτες συνδυάζουν δυο διαφορετικές τεχνολογίες έξυπνων καρτών στην ίδια κάρτα. Οι έξυπνες κάρτες επαφής έχουν το πιο υψηλό επίπεδο ασφάλειας και readily-available υποδομή, ενώ οι έξυπνες κάρτες άνευ επαφής παρέχουν ένα αποδοτικότερο και εύχρηστο περιβάλλον συναλλαγής. Προκειμένου να παρασχεθούν στους πελάτες τα πλεονεκτήματα αυτών των δύο καρτών, δύο μέθοδοι θα μπορούσαν να υιοθετηθούν.

Η πρώτη μέθοδος είναι να φτιαχτεί ένας υβριδικός αναγνώστης καρτών, ο οποίος θα μπορούσε να καταλάβει τα πρωτόκολλα και των δύο τύπων καρτών. Η δεύτερη μέθοδος είναι να δημιουργηθεί μια κάρτα που συνδυάζει τις λειτουργίες contact με τις contactless λειτουργίες. Επειδή το κόστος παραγωγής του υβριδικού αναγνώστη είναι πολύ ακριβό, επιλέγεται συνήθως η τελευταία λύση. Αυτές οι υβριδικές κάρτες έχουν κατάλληλη διεπιφάνεια για να λειτουργήσουν και ως κάρτες που λειτουργούν με επαφή (contact) και ως κάρτες άνευ επαφής (contactless). Δηλαδή, μπορεί να υπάρχει πρόσβαση στο ίδιο μικροτσίπ και μέσω ηλεκτρικών επαφών στην επιφάνεια της κάρτας και μέσω ασύρματης επικοινωνίας με τη χρήση της κεραίας. Στις κάρτες αυτές το επίπεδο ασφαλείας είναι αρκετά υψηλό.

Στην ίδια κάρτα το μικροτσίπ μπορεί να έχει επικοινωνία με τον εξωτερικό κόσμο μέσω των ηλεκτρικών επαφών στην επιφάνεια της κάρτας και μέσω της κεραίας που περιβάλλεται στο εσωτερικό στρώμα της κάρτας. Το ασύρματο τσιπ χρησιμοποιείται για εφαρμογές που χρειάζονται γρήγορες συναλλαγές και το τσιπ με τις ηλεκτρικές επαφές για εφαρμογές που απαιτούν μεγαλύτερη ασφάλεια.

Δεδομένου ότι οι υβριδικές κάρτες διαθέτουν τα πλεονεκτήματα και των contact και των contactless καρτών, ο μόνος λόγος που εμποδίζει την ευρεία αποδοχή τους είναι το

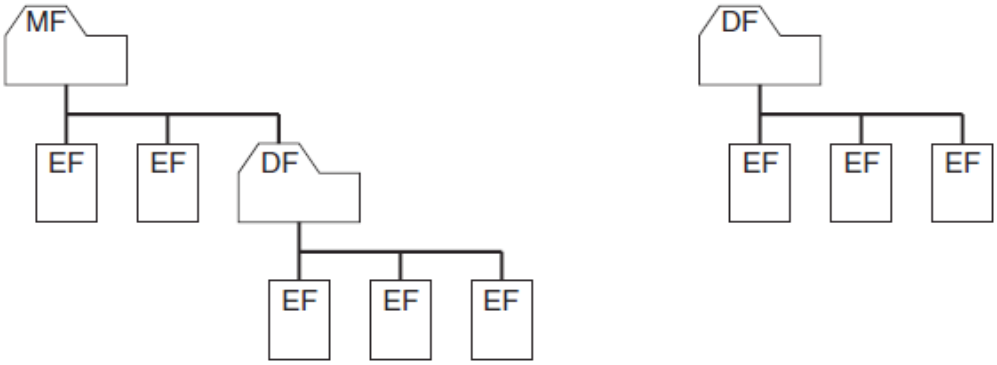
υψηλό κόστος. Όταν το κόστος και τα τεχνικά εμπόδια θα υπερνικηθούν, οι υβριδικές κάρτες θα αποτελούν μια δημοφιλής λύση έξυπνων καρτών. Οι κάρτες αυτές αναμένεται να έχουν μεγάλη απορρόφηση στο χώρο των μέσων μαζικής μεταφοράς και στο τραπεζικό τομέα.

### 5.2.3 Το σύστημα αρχείων των έξυπνων καρτών (Smart cards file system)

Για την οργάνωση των δεδομένων στις έξυπνες κάρτες χρησιμοποιούνται ιεραρχικά συστήματα αρχείων, η δομή των οποίων ορίζεται στο ISO/IEC 7816-4. Ορίζονται τα αρχεία καταλόγων που ονομάζονται Dedicated Files (DFs), τα αρχεία δεδομένων Elementary Files (EFs) και τα κύρια αρχεία Master Files (Mfs). Στην κορυφή αυτού του δένδρου, είναι το Κύριο Αρχείο (MF/Master File) που αποτελεί τον κατάλογο ρίζας (root directory) του συστήματος αρχείων. Η ύπαρξη αυτού του αρχείου είναι υποχρεωτική και περιέχει κάθε DF και EF.

Κάτω από το Κύριο Αρχείο μπορούν να υπάρχουν είτε Αρχεία Καταλόγων (DF/Dedicated Files), τα οποία θεωρούνται κατάλογοι εφαρμογών, είτε Στοιχειώδη Αρχεία (Elementary Files), τα οποία χρησιμοποιούνται για να αποθηκεύσουν τα δεδομένα του ιδιοκτήτη της κάρτας και άλλου είδους πληροφορία, όπως κωδικοί πρόσβασης και κλειδιά. Τα DFs χωρίζουν λογικά τα δεδομένα και δίνουν επίσης την δυνατότητα να προσδιοριστούν διαφορετικά επίπεδα ασφαλείας στα Στοιχειώδη Αρχεία (EFs), που βρίσκονται στο παρακάτω δένδρο.

Τα αρχεία που χρησιμοποιούνται από την κάρτα για σκοπούς διαχείρισης και έλεγχου ονομάζονται Εσωτερικά Στοιχειώδη Αρχεία (Internal EFs) τα οποία περιέχουν δεδομένα για αποκλειστική χρήση από το λειτουργικό σύστημα. Τα αρχεία που προσπελάσονται από διάφορες εφαρμογές ονομάζονται Εξωτερικά Στοιχειώδη Αρχεία (External Efs).




*Σχήμα 5.12: Μορφή του λογικού συστήματος αρχείων μιας έξυπνης κάρτας*

Στην ορολογία έξυπνων καρτών, η ρίζα ή το κύριο αρχείο Master File (MF) εκτός από το μέρος επικεφαλίδων που περιέχει, περιλαμβάνει και τις επικεφαλίδες όλων των αφιερωμένων αρχείων και στοιχειωδών αρχείων που περιέχουν το κύριο αρχείο στη γονική τους ιεραρχία. Το αφιερωμένο αρχείο DF είναι μια λειτουργική ομαδοποίηση των αρχείων που αποτελείται από τον εαυτό και όλα τα αρχεία που είναι άμεσα παιδιά του. Το στοιχειώδες αρχείο EF αποτελείται απλά από την επικεφαλίδα του και το σώμα που καταχωρεί τα στοιχεία. Οι τρόποι με τους οποίους τα δεδομένα ρυθμίζονται μέσα σε ένα αρχείο διαφέρουν και εξαρτώνται από τα διαφορετικά λειτουργικά συστήματα που χρησιμοποιούνται. Μερικοί από τους τρόπους με τους οποίους τα δεδομένα μπορούν να διαχειριστούν είναι απλά μέσω του offset και του μήκους, ενώ άλλα μπορούν να οργανώσουν τα δεδομένα τους σε σταθερά ή μεταβλητά μήκη αρχείων, όπως το Global System Mobile Communication. Κάθε μια από αυτές τις περιπτώσεις απαιτεί το αρχείο να πρέπει να επιλεχθεί πριν εκτελεστεί οποιαδήποτε άλλη λειτουργία.

Οι λογικοί μηχανισμοί πρόσβασης και επιλογής ενεργοποιούνται αφότου διοχετευτεί τάση στην κάρτα, ενώ το κύριο αρχείο επιλέγεται αυτόματα. Η λειτουργία επιλογής επιτρέπει τη μετακίνηση γύρω από το δέντρο. Μπορεί να είναι κίνηση πτωτική με την επιλογή ενός από το EF ή DF ή μπορεί να είναι κίνηση προοδευτική με την επιλογή ενός MF ή DF. Η οριζόντια μετακίνηση μπορεί να γίνει με την επιλογή ενός EF. Μετά από την επιτυχία της επιλογής, η επικεφαλίδα του αρχείου μπορεί να ανακτηθεί και η ανάκτηση της θα μπορέσει να μας πληροφορήσει σχετικά με στοιχεία όπως ο αριθμός αναγνώρισης, περιγραφές, τύπους και το

μέγεθος. Ειδικότερα, η επικεφαλίδα καταχωρεί τις ιδιότητες του αρχείου που δηλώνουν τους όρους πρόσβασης και την παρούσα κατάσταση. Η πρόσβαση των δεδομένων στο αρχείο εξαρτάται από εάν οι όροι μπορούν να τηρηθούν ή όχι. Εν ολίγοις, η δομή αρχείων του λειτουργικού συστήματος έξυπνων καρτών είναι παρόμοια με άλλα κοινά λειτουργικά συστήματα, όπως το MS-DOS και το UNIX. Εντούτοις, προκειμένου να επιτευχθεί μεγαλύτερος έλεγχος ασφάλειας, η ιδιότητα κάθε αρχείου ενισχύεται με την προσθήκη όρων πρόσβασης, πεδίων θέσης αρχείων και πεδίων κατάστασης στην επικεφαλίδα αρχείων. Επιπλέον, δίνεται η δυνατότητα του κλειδώματος αρχείων για να αποτραπεί η μη εξουσιοδοτημένη πρόσβαση στο αρχείο.

### 5.2.4 Λειτουργικά Συστήματα έξυπνων καρτών

Ο πυρήνας της έξυπνης κάρτας είναι το λειτουργικό σύστημα, που είναι ο κώδικας που διαχειρίζεται το σύστημα αρχείων, εφαρμογές, την είσοδο / έξοδο (I/O) και την ασφάλεια. Τα λειτουργικά συστήματα έξυπνων καρτών σε αντίθεση με τα γνωστά λειτουργικά συστήματα των υπολογιστών δεν περιλαμβάνουν κάποιο περιβάλλον επικοινωνίας με το χρήστη ή τη δυνατότητα πρόσβασης από εξωτερικά μέσα. Η λειτουργία τους είναι τελείως διαφορετική. Η ασφάλεια κατά την εκτέλεση των προγραμμάτων και η πρόσβαση στα δεδομένα της κάρτας έχουν την υψηλότερη προτεραιότητα. Εξαιτίας των περιορισμών από πλευράς μνήμης, τα λειτουργικά συστήματα των έξυπνων καρτών διαθέτουν κώδικα από 3 ως 250 Kbyte. Ο κώδικας των λειτουργικών συστημάτων γράφεται σε μνήμη ROM. Το γεγονός αυτό εξηγεί γιατί δεν είναι δυνατή καμία απολύτως αλλαγή από τη στιγμή που ο μικροεπεξεργαστής προγραμματιστεί και κατασκευαστεί. Η διόρθωση ενός λάθους αποτελεί δαπανηρή διαδικασία.

Αυτά τα λειτουργικά συστήματα δεν πρέπει να περιέχουν σφάλματα αλλά πρέπει να είναι σταθερά, αξιόπιστα και ασφαλή. Κρυμμένα σημεία πρόσβασης (trap doors) συναντώνται συχνά σε «μεγάλα» λειτουργικά συστήματα, όμως στα λειτουργικά συστήματα των έξυπνων καρτών πρέπει να αποφεύγονται πάση θυσία. Η πιθανότητα κάποιος να ξεπεράσει το λειτουργικό σύστημα και να αποκτήσει, για παράδειγμα, μη εξουσιοδοτημένη πρόσβαση σε κάποιο αρχείο πρέπει να ελαχιστοποιηθεί στο μέτρο του δυνατού. Το

λειτουργικό σύστημα μιας έξυπνης κάρτας θα πρέπει να είναι σε θέση να εκτελεί σε μικρό χρόνο κρυπτογραφικές λειτουργίες, όπως η δημιουργία ενός ζεύγους δημοσίου-ιδιωτικού κλειδιού ή μιας ψηφιακής υπογραφής.

Συνοπτικά, ένα λειτουργικό σύστημα έξυπνων καρτών θα πρέπει να μπορεί να:

- ✔ Μεταφέρει δεδομένα από και προς την έξυπνη κάρτα.
- ✔ Ελέγχει την εκτέλεση των εντολών.
- ✔ Διαχειρίζεται αρχεία.
- ✔ Διαχειρίζεται και να εκτελεί κρυπτογραφικούς αλγόριθμους.
- ✔ Διαχειρίζεται και να εκτελεί κώδικα προγραμμάτων.

**Τα πιο γνωστά λειτουργικά συστήματα είναι τα εξής:**

| | |
|---|---|
| **Bull** | **SmartTB, CC, Odyssey I (Javacard) (www.cp8.bull.gr)** |
| **DeLaRue** | **DS, DX, DXPLUS, CC, Mondex Card, JavaCard (www.delarue.com)** |
| **Gemalto** | **PCOS, MPCOS, GemVersion, GemXpresso(JavaCard)** |
| **Giesecke & Devrient** | **Starcos S, Starcos PK, Staarcos X (www.gdm.de)** |
| **IBM** | **MFC (www.ibm.chipcard.com)** |
| **ODS** | **ODS-COS (www.ods.com)** |
| **ORGA** | **ICC (www.orga.com)** |
| **Schlumberger** | **ME2000, PayFlex, Multiflex, Cryptoflex, Cyberflex (JavaCard) (www.slb.com)** |
| **Siemens** | **Card OS (www.sni.com)** |

Υπάρχουν περιπτώσεις εταιριών που αγοράζουν την άδεια (license) για λειτουργικά συστήματα καρτών άλλων κατασκευαστών και τα επεκτείνουν ή μετατρέπουν εντολές και εφαρμογές όπως η Gemalto και η Schlumberger εκμισθώνουν το MFC της IBM.

### 5.2.5 Εφαρμογές των smart cards στην Υγεία

Λόγω της επεξεργαστικής δυνατότητας που έχουν μέσω του ενσωματωμένου μικροτσίπ, χρησιμοποιούνται παγκοσμίως για ένα μεγάλο εύρος καθημερινών εργασιών αλλά και προηγμένων εφαρμογών.

**Έλεγχος πρόσβασης**: Οι πιο κοινές συσκευές που χρησιμοποιούνται για να ελέγξουν την πρόσβαση στις ιδιωτικές περιοχές όπου η ευαίσθητη εργασία εκτελείται ή που τα δεδομένα φυλάσσονται, είναι κλειδιά, διακριτικά και μαγνητικές κάρτες. Όλα αυτά έχουν τα ίδια βασικά μειονεκτήματα, μπορούν εύκολα να αναπαραχθούν και όταν κλαπούν, μπορούν να επιτρέψουν την είσοδο σε μη εξουσιοδοτημένο άτομο. Η έξυπνη κάρτα εξαφανίζει αυτές τις αδυναμίες καθιστώντας πολύ δύσκολη την αναπαραγωγή και αποδοχή τους στη θέση των ψηφιοποιημένων προσωπικών χαρακτηριστικών. Με τον κατάλληλο εξοπλισμό επαλήθευσης, αυτό το στοιχείο μπορεί να χρησιμοποιηθεί στο σημείο της εισόδου που προσδιορίζει εάν ο χρήστης είναι ο εξουσιοδοτημένος κάτοχος κάρτας. Η κάρτα μπορεί επίσης να προσωποποιηθεί χωριστά για να επιτρέψει την πρόσβαση σε περιορισμένες εγκαταστάσεις, ανάλογα με το επίπεδο ασφαλείας του κατόχου. Μια καταγραφή των κινήσεων του κατόχου, μέσω ενός συστήματος ασφάλειας, μπορεί να αποθηκευτεί στην κάρτα ως διαδρομή του ελέγχου ασφάλειας.

**Computer Login:** Η πρόσβαση στο Computer room και τις υπηρεσίες του μπορεί να ελεγχθεί από την έξυπνη κάρτα. Από την άποψη της πρόσβασης στο δίκτυο, η έξυπνη κάρτα μπορεί να επικυρώσει το χρήστη στον host. Ακόμη, ανάλογα με το περιβάλλον που προστατεύεται η κάρτα πρόσβασης στο δίκτυο μπορεί επίσης να εκτελέσει λειτουργίες όπως, χειρισμός των διαφορετικών κωδίκων επικύρωσης για τα διαφορετικά επίπεδα ασφάλειας. χρήση των βιομετρικών τεχνικών ως προστιθέμενο μέτρο ασφάλειας. διατήρηση μιας διαδρομής του ελέγχου των αποτυχιών και των αποπειραθεισών παραβιάσεων.

Από την άποψη της πρόσβασης στο compter room, ο έλεγχος PIN μπορεί να γίνει στην κάρτα χωρίς την ανάγκη για σύνδεση των σημείων πρόσβασης σε έναν κεντρικό υπολογιστή. Ο προσδιορισμός ενός χρήστη γίνεται συνήθως με τη βοήθεια ενός (Personal Identification Number) PIN. Το PIN ελέγχεται από το μικροϋπολογιστή της κάρτας με το PIN να αποθηκεύεται σε RAM του. Εάν η σύγκριση είναι αρνητική, η CPU θα αρνηθεί να λειτουργήσει. Το chip κρατά επίσης τον αριθμό των διαδοχικών λανθασμένων καταχωρήσεων PIN. Εάν αυτός ο αριθμός φθάνει σε ένα προκαθορισμένο ανώτατο όριο, η κάρτα μπλοκάρεται για περαιτέρω χρήση.

**Υγεία:** Οι ιατρικές έξυπνες κάρτες προσφέρουν μία νέα οπτική στις εφαρμογές υγείας. Μέσα στην κάρτα μπορούν να αποθηκεύονται πληροφορίες που αφορούν προσωπικά δεδομένα του ασθενή, όπως από ποιο ασφαλιστικό ταμείο καλύπτεται, το ιατρικό του ιστορικό καθώς και χρήσιμες πληροφορίες σε περίπτωση έκτακτης ανάγκης, όπως πιθανές ευαισθησίες και αντιδράσεις σε συγκεκριμένη φαρμακευτική αγωγή. Με τον τρόπο αυτό, οι πληροφορίες είναι έγκαιρα και έγκυρα διαθέσιμες στους ασθενείς και ιατρούς, υποστηρίζοντας και διευκολύνοντας σημαντικά την ελεύθερη διακίνηση των ασθενών, οι οποίοι μπορούν να ταξιδεύουν στο εσωτερικό και στο εξωτερικό φέροντας μαζί τους τον ασφαλιστικό και ιατρικό τους φάκελο. Νοσοκομεία στην Αυστρία και τη Γερμανία έχουν αρχίσει να υλοποιούν αυτή την εφαρμογή έξυπνης κάρτας. Επιπλέον, οι έξυπνες κάρτες στον τομέα της υγείας χρησιμοποιούνται σε εφαρμογές ταυτοποίησης του ασθενούς και επαγγελματιών υγείας (ιατρών, νοσηλευτών κλπ.), σε εφαρμογές ηλεκτρονικών υπογραφών για την ακεραιότητα και την αυθεντικότητα των ιατρικών δεδομένων, για τη διασφάλιση δεδομένων, σε εφαρμογές της κρυπτογράφησης των health professional cards και σε εφαρμογές ασφαλούς πρόσβασης σε δίκτυα υγείας κλπ.

Η τάση της αγοράς και της βιομηχανίας είναι στην χρήση καρτών πολλαπλών εφαρμογών (multi-application cards). Οι κάρτες αυτές έχουν την δυνατότητα να υποστηρίξουν διαφορετικά είδη εφαρμογών έτσι ώστε ο χρήστης να κατέχει μία κάρτα για όλες τις εφαρμογές που χρησιμοποιεί αντί της μιας κάρτας για κάθε ξεχωριστή εφαρμογή. Η θέσπιση κοινών προτύπων και μια κοινή αρχιτεκτονική που θα επιτρέπει την προσθήκη εφαρμογών σε μια κάρτα χωρίς να επηρεάζει τις ήδη υπάρχουσες είναι απαραίτητες προϋποθέσεις για να γίνει η multi-application κάρτα πραγματικότητα.

### 5.2.6 Οι έξυπνες κάρτες στο χώρο της υγείας

Η επεξεργασία ιατρικών δεδομένων από ιατρούς ή άλλους επαγγελματίες υγείας απαιτεί την εφαρμογή αναλόγων διαδικασιών που θα εξασφαλίσουν το απόρρητο των συγκεκριμένων πληροφοριών. Σκοπός των διαδικασιών αυτών είναι να διαφυλαχθούν δεδομένα που καλύπτονται από το ιατρικό απόρρητο ή άλλο απόρρητο που προβλέπει ο νόμος ή κώδικας δεοντολογίας ώστε τα δεδομένα αυτά να μην μεταβληθούν ούτε να κοινοποιούνται σε τρίτους χωρίς προηγούμενη έγγραφη συγκατάθεση.

Οι έξυπνες κάρτες αποτελούν ολοκληρωμένη λύση διαχείρισης Ιατρικών και Ασφαλιστικών δεδομένων παρακολουθώντας τον ηλεκτρονικό φάκελο του κάθε ασφαλισμένου. Ο ηλεκτρονικός φάκελος περιλαμβάνει πληροφορίες που επεκτείνονται στην ουσιαστική διαχείριση των στοιχείων που καταγράφονται από τους εμπλεκόμενους παροχείς υγείας.

Η τάση των τελευταίων ετών είναι η μεταφορά από συστήματα πληροφοριών ιατρικής φροντίδας που βασίζονται σε χαρτιά και έγγραφα σε ηλεκτρονικά συστήματα βάσεων δεδομένων, τα οποία παρέχουν προστασία στα ευαίσθητα προσωπικά δεδομένα.

Η Κεντρική Βάση Δεδομένων περιέχει πληροφορίες σχετικά με τον ασφαλισμένο που αφορούν:

- ✔ Προσωπικά στοιχεία
- ✔ Βασικά στοιχεία Υγείας για αντιμετώπιση επειγόντων περιστατικών
- ✔ Πληροφορίες Ιατρικού Ιστορικού (για διαπίστωση χρόνιων νοσημάτων, κ.λ.π)
- ✔ Πλήρης Ιατρικός Φάκελος
- ✔ Δαπάνες χρέωσης νοσηλείας, ιατρική περίθαλψη, φαρμακευτική αγωγή, κ.λ.π.
- ✔ Συχνότητα επισκέψεων ασφαλισμένων, ειδικότητα ιατρού, νοσοκομείο, κ.λ.π

Η έξυπνη κάρτα Ασθενούς (Patient Data Card) έχει τυπωμένη πάνω της την φωτογραφία και το ονοματεπώνυμο του κατόχου της μαζί με τον αριθμό μητρώου ασφάλισης. Είναι εφοδιασμένη με ένα ηλεκτρονικό κύκλωμα, που περιέχει μικροεπεξεργαστή

και μνήμη EEPROM, έτσι ώστε να είναι δυνατή η αποθήκευση ευαίσθητων δεδομένων που αφορούν τον ασθενή. Η πρόσβαση στις πληροφορίες της βάσης καθώς και η εξασφάλιση του απόρρητου της πληροφορίας πραγματοποιείται με την ύπαρξη P.I.N.s. Τα P.I.N.s διαφοροποιούνται ανάλογα με το είδος της πληροφορίας στην οποία ζητάει πρόσβαση ο χρήστης. Έτσι σε κάθε περίπτωση εξασφαλίζεται η ταυτοπροσωπία του ασφαλισμένου με αυτή του αιτούντος.

Οι Ασθενείς – Ασφαλισμένοι έχουν :

- Έναν ενημερωμένο ασφαλή και φορητό Ιατρικό Φάκελο με δυνατότητα πρόσβασης σε αυτόν από εξουσιοδοτημένα άτομα 24 ώρες το 24ωρο και για όλες τις μέρες του χρόνου με τη χρήση της έξυπνης κάρτας.
- Επιπλέον η φύλαξη του ιατρικού τους φακέλου στην Κεντρική Βάση αποτελεί πλεονέκτημα προκειμένου να τύχουν καλύτερης ιατρικής φροντίδας από τους συμβεβλημένους φορείς παροχής υγείας.
- Μείωση της γραφειοκρατίας στις συναλλαγές τους με τους φορείς παροχής υγείας καθώς και με το Ταμείο Ασφάλισης.
- Ετοιμότητα στην αντιμετώπιση εκτάκτων περιστατικών (emergency data set).

Συγκεκριμένα, το Ταμείο Ασφάλισης αποκτά :

- Δυνατότητα on-line παρακολούθησης της παρουσίας των ασφαλισμένων στους διαφόρους παροχείς υγείας όπως εισαγωγές σε συγκεκριμένο νοσηλευτήριο.
- Δυνατότητα παρακολούθησης της τρέχουσας κατάστασης των ασφαλισμένων αναφορικά με την παροχή ιατρικής υπηρεσίας.
- Πλήρη στατιστική κάλυψη και έλεγχο των διαδικασιών.
- Δυνατότητα παραμετροποίησης, στατιστικοποίησης αναφορών.
- Πρόσβαση στον ιατρικό φάκελο ασφαλισμένων για ενημέρωση σε σχέση με χρόνιες ασθένειες και μεταβολή ασφαλιστικής σχέσης.
- Μείωση κόστους ιατροφαρμακευτικής περίθαλψης και κατ΄ επέκταση δυνατότητα ελέγχου του κόστους των ασφαλιστικών παροχών και των αποζημιώσεων.

- Δυνατότητα στατιστικής επεξεργασίας στοιχείων
- Ανάλυση Κέντρων Κόστους Συμβολαίων (Νοσήλεια / Φάρμακα & Εξετάσεις / Αμοιβές Γιατρών) ανά είδος νόσου , ανά νοσηλευτήριο, ανά ιατρό
- Συσχέτιση ποιότητας παρεχόμενων υπηρεσιών με συμβεβλημένους φορείς και αντίστοιχα κόστη

Οι πάροχοι μπορούν να αποκομίσουν τεράστια οφέλη από την εφαρμογή έξυπνων καρτών:

1. Ελαχιστοποίηση του κόστους.
2. Θετική ταυτοποίηση των ασθενών.
3. Διοικητική αποτελεσματικότητα.
4. Συμμόρφωση με τους κανονισμούς.
5. Ενισχυμένη ικανοποίηση των ασθενών & Βελτίωση των αποτελεσμάτων των ασθενών.
6. Νέες πηγές εσόδων.
7. Ανταγωνιστική διαφοροποίηση.

**Ελαχιστοποίηση του κόστους:** Η χρήση μιας έξυπνης κάρτας μπορεί να ελαχιστοποιήσει το κόστος από τη μείωση των σφαλμάτων ταυτοποίησης κατά τη διάρκεια της διαδικασίας εγγραφής, εξαλείφοντας την άρνηση των απαιτήσεων λόγω της ελλιπούς δημογραφικής ή ασφαλιστικής πληροφορίας, καθώς και την αυτοματοποίηση και τον εξορθολογισμό της διαδικασίας εγγραφής, επιτρέποντας προσωπικό που είναι υπεύθυνο για την καταχώριση να είναι πιο αποτελεσματικό και να επικεντρωθεί στο υψηλότερο σημείο των δυνατοτήτων του.

**Θετική ταυτοποίηση των ασθενών:** Όταν η ταυτοποίηση γίνεται από μια έξυπνη κάρτα, η σύνδεση μεταξύ της κάρτας και του κατόχου της κάρτας έχει επικυρωθεί, μετριάζοντας έτσι τους κινδύνους που προκύπτουν από λανθασμένες ή ψευδείς αξιώσεις της ταυτότητας. Τυχόν εσφαλμένα στοιχεία ταυτότητας μπορούν να οδηγήσουν σε περιττές ή δυνητικά επιβλαβείς ιατρικές διαδικασίες και ανακριβή ιατρικό αρχείο ιστορικού, που μπορεί να θέσει σε κίνδυνο τη μελλοντική φροντίδα για τον ασθενή τον οποίο το αρχείο αφορά.

**Διοικητική αποτελεσματικότητα:**Οι έξυπνες κάρτες μπορούν να συμβάλουν στη διοικητική αποτελεσματικότητα, εξαλείφοντας την επαναλαμβανόμενη εργασία της χειροκίνητης δημιουργίας και ελέγχου των εντύπων εγγραφής , απελευθερώνοντας διοικητικό προσωπικό να επικεντρωθεί στο υψηλότερο σημείο των δυνατοτήτων του. Λαμβάνοντας την πληροφορία της εγγραφής την πρώτη φορά εξαλείφεται το κόστος της χρήσης προσωπικού για την επίλυση ζητημάτων που καθυστερούν τις μετέπειτα χρονικά διαδικασίες. Οι έξυπνες κάρτες που εκδίδονται από τους παρόχους υγειονομικής περίθαλψης ως αναγνωριστικά των εργαζομένων μπορούν να επιτρέψουν άνετες, ασφαλείς multi-factor δυνατότητες ελέγχου ταυτότητας όσον αφορά την πρόσβαση σε πληροφοριακά συστηματα υγείας (π.χ. νοσοκομεία, κλινικές), μέσω εξουσιοδοτημένων φορητών συσκευών ή να παρέχουν VPN πρόσβαση.

**Συμμόρφωση με τους κανονισμούς:** Οι έξυπνες κάρτες μπορούν επίσης να διευκολύνουν όσον αφορά τη συμμόρφωση με τους κανονισμούς της εκάστοτε χώρας και τους κανόνες της βιομηχανίας. Η χρήση μιας έξυπνης κάρτας μπορεί να βοηθήσει στο να τηρούνται όλα όσα προβλέπονται και πρέπει να συνάδουν με τους κανόνες προστασίας προσωπικών δεδομένων και την ασφάλεια και την προστασία της ιδιωτικής ζωής.

**Ενισχυμένη ικανοποίηση των ασθενών και βελτίωση των αποτελεσμάτων:** Η ικανοποίηση των ασθενών θα αυξηθεί όταν ο ασθενής φέρει μια έξυπνη κάρτα υγείας. Επειδή οι έξυπνες κάρτες επιταχύνουν τη διαδικασία εγγραφής και κάνουν έγκαιρα και έγκυρα πληροφορίες σχετικά με την κατάσταση της υγείας του ασθενούς διαθέσιμα στον πάροχο, μπορούν να ελαχιστοποιηθούν τα προβλήματα των ασθενών και να μεγιστοποιηθεί η ποιότητα της αλληλεπίδρασης του ασθενούς με τον πάροχο. Με την ενεργοποίηση της θετικής ταυτοποίησης των ασθενών και την παροχή σχετικών και επακριβών δεδομένων για την υγεία του στον πάροχο, οι έξυπνες κάρτες παίζουν σημαντικό ρόλο στη διασφάλιση ότι η σωστή θεραπεία χορηγείται στο σωστό άτομο σε έγκαιρη βάση.

**Νέες πηγές εσόδων:**Η άνεση και η ποιότητα των παρεχόμενων υπηρεσιών τις οποίες οι έξυπνες κάρτες μπορούν να συνεισφέρουν οδηγούν στη δημιουργία εμπιστοσύνης των ασθενών, με αποτέλεσμα την απόδοση επισκέψεων και αυξημένη χρήση των υπηρεσιών παρόχου που ως εκ τούτου ενθαρρύνει νέες πηγές εσόδων. Και επειδή οι έξυπνες κάρτες

μπορούν να υποστηρίξουν λειτουργίες πληρωμής (είτε χρεωστικών είτε πιστωτικών), μπορούν να εκδίδονται για να διευκολύνουν αγορές αγαθών και υπηρεσιών.

**Ανταγωνιστική διαφοροποίηση:** Οι έξυπνες κάρτες μπορούν να προσφέρουν πραγματικά και αναμενόμενα οφέλη που μπορεί να διακρίνει ο καθένας. Η βελτίωση της ποιότητας των υπηρεσιών που σχετίζονται με τις έξυπνες κάρτες μπορεί να αυξήσει τα ποσοστά παραμονής ασθενών καθώς και να προσελκύσει νέους ασθενείς που ενδιαφέρονται για μια καλύτερη εμπειρία υγειονομικής περίθαλψης. Ένας εξελιγμένος πάροχος υγείας βασίζεται σε μια έξυπνη κάρτα που αντανακλά το ίδρυμα που την εκδίδει δίνοντας στον κάτοχο της κάρτας την αίσθηση ότι είναι ένα αξιόλογο μέλος ενός αναγνωρισμένου κύρους οργανισμού. Επιπλέον, οι έξυπνες κάρτες μπορούν να συνεργάζονται με ένα ευρύ φάσμα της κινητών συσκευών, παρέχοντας στους παρόχους υγειονομικής περίθαλψης έναν ασφαλή τρόπο ώστε να έχουν πρόσβαση σε πληροφορίες για την υγεία των ασθενών τους μέσω μιας πληθώρας πλατφόρμων και κινητών συσκευών. Έτσι, στρατηγικές όπως η "Bring Your Own Device" (BYOD) υιοθετούνται από πολλά ιδρύματα δίνοντας παράλληλα καινοτόμες τεχνολογίες για να γίνουν πιο παραγωγικά και ανταγωνιστικά.

#### 5.2.6.1 Χαρακτηριστικά της έξυπνης κάρτας των επαγγελματιών υγείας

Η έξυπνη κάρτα του επαγγελματία υγείας (Health Professional Card) είναι μια προσωπική κάρτα με τυπωμένη φωτογραφία του κατόχου πάνω της. Λειτουργεί ως κλειδί και επιτρέπει στον κάτοχο της να ξεκλειδώσει τα προσωπικά ιατρικά δεδομένα των ασθενών, τα οποία είναι αποθηκευμένα είτε στην κάρτα είτε σε ένα δίκτυο υγείας (e- health network).

Η κάρτα του επαγγελματία υγείας είναι συμβατή με τα πρότυπα ISO 7816 1, 2, 3, 4 και έχει τα εξής χαρακτηριστικά:

1) Υποστηρίζει τον ασύμμετρο αλγόριθμο RSA
2) Περιέχει ένα ιδιωτικό κλειδί το οποίο χρησιμοποιείται για την εξακρίβωση της ταυτότητας.
3) Το μήκος του κλειδιού του RSA είναι τουλάχιστον 1024 ψηφία.

4) Η χρήση του ιδιωτικού κλειδιού για εξακρίβωση ταυτότητας προστατεύεται με ένα Προσωπικό Αριθμό Ταυτοποίησης (Personal Identification Number - PIN).
5) Ο Προσωπικός Αριθμός Ταυτοποίησης (PIN), προστατεύεται και διαχειρίζεται σύμφωνα με τα πρότυπα ISO/IEC 9564-1 (Banking PIN management and security PIN protection principles and techniques) και το πρότυπο ISO/IEC 10202.6 (Financial Transaction Card, Security architecture of financial transaction systems using integrating circuit cards, Cardholder verification).
6) Ο χρήστης επιτρέπεται να αλλάξει τον Προσωπικό Αριθμό Ταυτοποίησης του (PIN) όπως καθορίζεται στο πρότυπο ISO 10202-6.
7) Ούτε ο ιδιοκτήτης της κάρτας αλλά ούτε και ο εκδότης της δεν μπορούν να αλλάζουν το ιδιωτικό κλειδί που χρησιμοποιείται για την εξακρίβωση της ταυτότητας.
8) Η έξυπνη κάρτα του επαγγελματία υγείας περιέχει το πιστοποιητικό δημοσίου κλειδιού του επαγγελματία υγείας για την εξακρίβωση της ταυτότητάς του, το οποίο θα μπορεί να διαβαστεί από μια εφαρμογή (host application) χωρίς να χρειάζεται προηγουμένως να έχει δοθεί ο PIN.

### 5.2.6.2 Λειτουργίες του τοπικού συστήματος διαχείρισης καρτών

Απαιτείται ένα ισχυρό τοπικό σύστημα, το οποίο θα αποτελείται από κάρτες, σταθμούς εργασίας των χρηστών, computer servers, αναγνώστες καρτών και ολοκληρωμένο σύστημα διαχείρισης καρτών, το οποίο θα υποστηρίζει τις παρακάτω λειτουργίες:

1) Υποστήριξη του πρωτοκόλλου του τερματικού της κάρτας
2) Έλεγχος του νόμιμου κατόχου της κάρτας, ζητώντας το PIN από τον χρήστη και παρουσιάζοντας τον στην έξυπνη κάρτα του επαγγελματία υγείας.
3) Χρήση τοπικού πρωτοκόλλου εξακρίβωσης ταυτότητας για την εξακρίβωση της ταυτότητας τοπικά
4) Ανάκτηση του πιστοποιητικού από την κάρτα του επαγγελματία υγείας
5) Ενημέρωση του ιατρικού φακέλου των ασθενών

Όταν το τοπικό σύστημα λειτουργεί και ως διαμεσολαβητής (proxy) για το τμήμα του απομακρυσμένου λογισμικού εξακρίβωσης ταυτότητας (remote authenticating component), μεταβιβάζει την πρόκληση (challenge) που λαμβάνει στην κάρτα και μεταφέρει την απόκριση της κάρτας (cards response) πίσω στο τμήμα του απομακρυσμένου λογισμικού εξακρίβωσης ταυτότητας.

#### 5.2.6.3 Λειτουργίες ταυτότητας του τμήματος λογισμικού εξακρίβωσης

Το απομακρυσμένο και τοπικό τμήμα λογισμικού εξακρίβωσης ταυτότητας (local & remote authenticating component) εκτελεί τις παρακάτω λειτουργίες:

1) Παράγει μια τυχαία πρόκληση (random challenge) για το πρωτόκολλο εξακρίβωσης ταυτότητας.
2) Επαληθεύει την απόκριση (verify response) από την κάρτα του επαγγελματία υγείας.
3) Ελέγχει την εγκυρότητα του πιστοποιητικού το οποίο περιέχεται στην απόκριση (ελέγχει επίσης την εγκυρότητα όλων των πιστοποιητικών που βρίσκονται στην αλυσίδα του μονοπατιού πιστοποιητικών που ανεβαίνουμε μέχρι να φτάσουμε στο πιστοποιητικό μιας έμπιστης αρχής Πιστοποίησης.
4) Εξακριβώνει ότι το πιστοποιητικό δεν έχει ανακληθεί επικοινωνώντας με την Έμπιστη Τρίτη Οντότητα (TTP).
5) Εξάγει την εξακριβωμένη ταυτότητα του χρήστη (authenticated user identity).

Το τελικό αποτέλεσμα είναι η παροχή της εξακριβωμένης ταυτότητας του χρήστη στο περιβάλλον της εφαρμογής.

### 5.2.6.4 Λειτουργίες πρωτοκόλλου Εξακρίβωσης Ταυτότητας τοπικά και εξ αποστάσεως

*Το πρωτόκολλο εξακρίβωσης ταυτότητας τοπικά παρέχει τις παρακάτω λειτουργίες:*

1) Μεταφορά μιας τυχαίας πρόκλησης από το τοπικό σύστημα λογισμικού εξακρίβωσης ταυτότητας στην κάρτα του επαγγελματία υγείας.

2) Παραλαβή της απόκρισης από την κάρτα του επαγγελματία υγείας.

*Το πρωτόκολλο εξακρίβωσης ταυτότητας εξ αποστάσεως παρέχει τις εξής λειτουργίες:*

1) Μεταφορά της τυχαίας πρόκλησης στο τοπικό σύστημα.
2) Λήψη της απόκρισης από το τοπικό σύστημα.
3) Λήψη του πιστοποιητικού του επαγγελματία υγείας από το τοπικό σύστημα.

## 5.3 Ποια είναι τα πλεονεκτήματα των έξυπνων καρτών σε σχέση με τη χρήση βιομετρικών στοιχείων για την πιστοποίηση ταυτότητας;

Οργανισμοί υγειονομικής περίθαλψης λαμβάνοντας υπόψη διαφορετικές προσεγγίσεις για τον έλεγχο της ταυτότητας του ασθενή και του παρόχου υγείας πρέπει να εξετάσουν τις επιπτώσεις στην ιδιωτική ζωή, την ασφάλεια, τη χρηστικότητα και την απόδοση των διαφόρων εναλλακτικών δυνατοτήτων.

Οι έξυπνες κάρτες υγείας είτε μόνες τους, είτε σε συνδυασμό με τη χρήση βιομετρικών στοιχείων, παρέχουν προστασία της ιδιωτικής ζωής, ασφαλή λύση, και επίσης προσφέρουν επιπλέον δυνατότητες και λειτουργίες που μπορούν να προσφέρουν σημαντικά οφέλη για τους παρόχους υγειονομικής περίθαλψης, σε σύγκριση με τη χρήση βιομετρικών στοιχείων.

Τα Βιομετρικά στοιχεία δεν είναι ιδανικά για τις ταυτότητες υγείας. Μια έξυπνη κάρτα υγείας με μια φωτογραφία παρέχει μια λύση στους ασθενείς που είναι ήδη εξοικειωμένοι και θα την αποδεχθούν αμέσως. Επιπλέον, η έξυπνη κάρτα υγείας προωθεί το εμπορικό σήμα του οργανισμού υγειονομικής περίθαλψης, μπορεί να υποστηρίξει μια ευρεία ποικιλία των εφαρμογών που προσθέτουν αξία, και μπορούν να είναι διαλειτουργικές και πιο χρηστικές ακόμη και μεταξύ διαφορετικών ομάδων.

Είτε μια απλή έξυπνη κάρτα ή μια έξυπνη κάρτα με βιομετρικά στοιχεία μπορεί να παρέχει στους οργανισμούς υγειονομικής περίθαλψης τα χαρακτηριστικά που απαιτούνται για τον έλεγχο ταυτότητας παρόχου και ασθενή και προσφέρει καλύτερη απόδοση από ό, τι μια χρήση μόνο βιομετρικών στοιχείων. Οι πάροχοι χρειάζονται μια λύση πιστοποίησης ταυτότητας που μπορεί να χρησιμοποιηθεί σε πολλαπλές κατατάσεις όπως σε καταστάσεις έκτακτης ανάγκης. Οι έξυπνες κάρτες υγειονομικής περίθαλψης χτισμένες πάνω σε πρότυπα, μπορούν να είναι διαλειτουργικές σε πολλές περιοχές, και μπορούν να χρησιμοποιηθούν από φορητές συσκευές ανάγνωσης σε καταστάσεις έκτακτης ανάγκης. Για πολλαπλά κριτήρια πιστοποίησης γνησιότητας, μία έξυπνη κάρτα υγειονομικής περίθαλψης με ένα PIN μπορεί να είναι σημαντικά πιο αποδοτική για έναν οργανισμό υγειονομικής περίθαλψης από μια βιομετρική λύση.

Συνδυάζοντας τις έξυπνες κάρτες και κάνοντας χρήση βιομετρικών στοιχείων μπορεί να έχουμε μια πλήρως χαρακτηριστική λύση για τον έλεγχο ταυτότητας ασθενή από τον πάροχο υγείας. Με την αποθήκευση των βιομετρικών στοιχείων και την εκτέλεση σύγκρισης των βιομετρικών αντιστοιχιών στην έξυπνη κάρτα υγείας, η προστασία της ιδιωτικής ζωής και η ασφάλεια των βιομετρικών στοιχείων πιστοποίησης είναι ενισχυμένη και η απόδοση του συστήματος είναι βελτιωμένη σε σχέση με τις τοπικές, offline τακτικές ελέγχου ταυτότητας.

Η τεχνολογία των έξυπνων καρτών χρησιμοποιείται παγκοσμίως για την ασφαλή προστασία της ταυτότητας, την πρόσβαση σε προσωπικά δεδομένα καθώς και αιτήσεις πληρωμών. Ως τεχνολογία βασισμένη σε πρότυπα η λύση των έξυπνων καρτών έχει ήδη αναπτυχθεί από πάρα πολλούς προμηθευτές σε ολόκληρο τον κόσμο. Η τεχνολογία των έξυπνων καρτών αποτελεί αναμφισβήτητα ένα ισχυρό θεμέλιο στον τομέα των ID cards ενεργοποιώντας βελτιώσεις των διαδικασιών περίθαλψης τόσο για τους ασθενείς –

ασφαλισμένους όσο και για τους παρόχους υγείας προστατεύοντας τις εμπλεκόμενες πληροφορίες της διεπαφής τους από μη εξουσιοδοτημένους χρήστες.

# ΚΕΦΑΛΑΙΟ 6

## ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΙΑΤΡΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

### 6.1 Εισαγωγή

Στις μέρες μας η ιατρική περίθαλψη βασίζεται σε μεγάλο βαθμό στη διαχείριση της 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 επανάσταση στον χώρο των νέων τεχνολογιών επιφέρει σημαντικές αλλαγές στον τρόπο με τον οποίο αντιλαμβανόμαστε την έννοια και το περιεχόμενο της παροχής φροντίδας υγείας. Η ιατρική πληροφορία είναι από τους πιο ευαίσθητους τύπους πληροφορίας και η κακή της χρήση επηρεάζει τη ζωή του ατόμου. Παλαιότερα αυτή η πληροφορία αποθηκευόταν στα γραφεία των ιατρών χωρίς κανένας να γνωρίζει την ύπαρξη της.

Προστατευόταν από το γεγονός ότι ήταν απομονωμένη, ήταν δύσκολη η πρόσβαση σ' αυτήν και ελάχιστοι γνώριζαν αν και τι συλλέγονταν και διατηρούνταν. Η πρόσβαση πλέον σε αυτή τη γνώση γίνεται μέσω των υπολογιστών ενώ λόγω των τεχνολογικών εξελίξεων και αυτή η παρεχόμενη πληροφορία έχει αυξηθεί. Για παράδειγμα υπάρχουν πλέον γενετικές πληροφορίες που παλαιότερα δεν ήταν διαθέσιμες. Η ενδεχόμενη διαρροή τέτοιων πληροφοριών σε τρίτους εγκυμονεί κινδύνους που μπορεί να επηρεάσουν ακόμη και την επαγγελματική ζωή του ατόμου (π.χ. αν θα προσληφθεί, πως θα εξελιχθεί η καριέρα του, ποιος θα είναι ο μισθός του, οι πιθανές προαγωγές του, η παραμονή του στην εργασία, κ.λπ.). Για αυτό το λόγο είναι απαραίτητη η διασφάλιση της εμπιστευτικότητας της χρήσης και η αποφυγή της διασποράς των πληροφοριών αυτών σε μη εξουσιοδοτημένους χρήστες. Οι πληροφορίες γύρω από το ιστορικό υγείας, όπως οι ασθένειες, τα νοσήματα και η περίθαλψη που έχει λάβει κάποιος είναι από τις πλέον ευαίσθητες και εμπιστευτικές.

Ο ηλεκτρονικός φάκελος υγείας αποτελεί έναν φάκελο φροντίδας υγείας (ή υποσύνολο του) για όλη τη διάρκεια ζωής του ατόμου και αποθηκευμένο σε ψηφιακή μορφή, με στόχο την υποστήριξη της συνέχειας της φροντίδας υγείας (ποιότητα, πρόσβαση, αποδοτικότητα), την εκπαίδευση και την έρευνα. Αντικαθιστά το χειρόγραφο φάκελο ως την κύρια πηγή πληροφοριών για τη φροντίδα υγείας εξασφαλίζοντας κλινικές, διοικητικές και νομικές απαιτήσεις. Τα συστήματα ηλεκτρονικού φακέλου υγείας υλοποιούνται και διατηρούνται με σκοπό τη συλλογή, αποθήκευση, ανάκτηση, επεξεργασία και διακίνηση δεδομένων που σχετίζονται με τη φροντίδα υγείας ασθενών. Στα δεδομένα αυτά συμπεριλαμβανομένων τα κλινικά, διοικητικά και οικονομικά δεδομένα.

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 τη σχέση τόσο του επαγγελματία υγείας - ασθενή, όσο και των μελών ολόκληρης της κοινωνίας αφού είναι πιθανό υπό το φόβο αποκάλυψής 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.

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.

## 6.2 Βασικές απαιτήσεις ασφαλείας της ιατρικής πληροφορίας

Η ισχύουσα νομοθεσία ορίζει ρητά τα δικαιώματα των πολιτών και διασφαλίζει την προστασία των ευαίσθητων προσωπικών δεδομένων επιβάλλοντας μια σειρά μέτρων ασφαλείας που αφορούν 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:

**Εμπιστευτικότητα:** Ως εμπιστευτικότητα ορίζεται «η αποφυγή διάθεσης ή αποκάλυψης πληροφορίας σε μη εξουσιοδοτημένα πρόσωπα, οντότητες ή διεργασίες». Η προστασία των προσωπικών δεδομένων από μη εξουσιοδοτημένα άτομα αποτελεί πρώτη προτεραιότητα και απαιτείται η εφαρμογή μέτρων που θα επιτρέπουν την πρόσβαση σε πληροφορία μόνο από αναγνωρισμένα και πιστοποιημένα άτομα. Το θέμα αυτό είναι

ιδιαίτερα σημαντικό σε ιατρικά πληροφοριακά συστήματα, όπου περιλαμβάνονται δεδομένα άμεσα συνδεόμενα με αναγνωρίσιμα άτομα, τις ασθένειες, τις θεραπείες τους και συχνά τις κοινωνικές τους συνήθειες. Τα δεδομένα αυτά θεωρούνται αυστηρώς εμπιστευτικά και η αποκάλυψή τους μπορεί να έχει σημαντικές επιπτώσεις στη κοινωνική θέση, στην υγεία ή ακόμα και στη ζωή των σχετιζόμενων ατόμων. Κάθε χρήστης πρέπει να έχει δικαίωμα πρόσβασης μόνο στην απολύτως απαραίτητη πληροφορία που χρειάζεται και να εκτελεί μόνο το σύνολο των λειτουργιών που απαιτούνται προκειμένου να επιτελέσει το έργο του, χωρίς ωστόσο να διακυβεύεται η παροχή σωστής περίθαλψης.

**Ακεραιότητα:** Ως ακεραιότητα ορίζεται «η αποφυγή μεταβολής ή καταστροφής δεδομένων με μη εξουσιοδοτημένο τρόπο». Στα συστήματα διαχείρισης ιατρικής πληροφορίας πρέπει να διασφαλιστεί η ακρίβεια και ακεραιότητα των δεδομένων, καθώς σε αυτά βασίζεται η διάγνωση και η προτεινόμενη αγωγή. Προκειμένου να προστατευτεί η διαγνωστική αξία της ιατρικής πληροφορίας επιβάλλεται η χρήση κατάλληλων μηχανισμών ελέγχου της ακεραιότητας των δεδομένων, που να επιτρέπουν την παρακολούθηση ενδεχόμενων τροποποιήσεων. Για τον αποτελεσματικό έλεγχο και την προστασία των δεδομένων από μη εγκεκριμένη τροποποίηση χρειάζεται ένας μηχανισμός που θα δίνει τη δυνατότητα έλεγχου κάθε πληροφορίας χωριστά και που θα είναι ανεξάρτητος από το σύστημα.

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

**Μη αποποίηση ευθύνης αποστολής/λήψης πληροφορίας:** Στα πλαίσια του αυστηρού ελέγχου για την αξιοπιστία των δεδομένων απαιτείται επιπλέον η αναγνώριση και

πιστοποίηση των επικοινωνούντων οντοτήτων, που αποτελεί ένα βασικό μέτρο προφύλαξης από ενδεχόμενη μη εξουσιοδοτημένη διείσδυση στο σύστημα και αθέμιτη τροποποίηση στοιχείων ή πιστοποίηση μη αυθεντικών δεδομένων. Ένας ισχυρός μηχανισμός ελέγχου της αξιοπιστίας της διακινούμενης πληροφορίας είναι η λεγόμενη «μη αποποίηση ευθύνης» (non-repudiation), η αδυναμία δηλαδή των εμπλεκομένων σε μία συναλλαγή μερών να αρνηθούν τη συμμετοχή τους σε αυτή, η οποία αυξάνει την προστασία της ακεραιότητας των δεδομένων.

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

**Διαθεσιμότητα:** Ως διαθεσιμότητα ορίζεται «η δυνατότητα άμεσης πρόσβασης και χρήσης ενός πληροφοριακού συστήματος, όποτε αυτό απαιτείται». Σε ιατρικά πληροφοριακά συστήματα, υπό κανονικές συνθήκες λειτουργίας η ανάκτηση και διαχείριση πληροφορίας θα πρέπει να είναι εύκολη και ταχεία. Επιπλέον είναι απαραίτητο να γίνει πρόβλεψη για τη διασφάλιση της διαθεσιμότητας της πληροφορίας σε ηλεκτρονική μορφή ακόμη και σε έκτακτες περιπτώσεις, όπως για παράδειγμα στην περίπτωση βλάβης εξοπλισμού ή διακοπής ρεύματος. Έστω και λίγα λεπτά διακοπής της λειτουργίας σε αυτές τις περιπτώσεις είναι δυνατόν να θέσουν ανθρώπινες ζωές σε κίνδυνο (π.χ. σε μονάδες εντατικής θεραπείας).

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

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

## 6.3 Παραβίαση της ηλεκτρονικής ασφάλειας σε Νοσοκομεία

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

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

Τα κίνητρα του Kane, σύμφωνα με τα λεγόμενά του, είναι η αποκάλυψη των ελλείψεων στην ασφάλεια ευαίσθητων δεδομένων. Η δράση του αυτή ξεκίνησε ύστερα από μια συζήτηση που είχε με έναν συμφοιτητή του, κατά τη διάρκεια της οποίας αναρωτήθηκαν κατά πόσον προστατεύονται πραγματικά, τα ανά τον κόσμο απόρρητα δεδομένα. “Η συζήτηση κατέληξε στα ιατρικά δεδομένα, που είναι όντως απόρρητα και σκέφτηκα να ρίξω

μια ματιά τριγύρω" αναφέρει ο Kane. Το συγκεκριμένο νοσοκομείο είχε λάβει την δέκατη τρίτη θέση στην ετήσια λίστα που δημοσιεύει η "U.S. News & World Reports" με τα καλύτερα νοσοκομεία σε όλη την επικράτεια των Ενωμένων Πολιτειών.

Το συγκεκριμένο παράδειγμα δείχνει πόσο ευάλωτοι είναι κάποιοι στόχοι που θα έπρεπε να είναι ασφαλείς. Τα πράγματα θα ήταν πολύ χειρότερα εάν ο εισβολέας τροποποιούσε τα δεδομένα χωρίς να αφήσει ίχνη. Ένα παρόμοιο περιστατικό φαίνεται να έγινε το 1998 και μάλιστα σε ιατρική βάση δεδομένων του Υπουργείου Άμυνας των Ενωμένων Πολιτειών. Hackers διείσδυσαν στην βάση δεδομένων και άλλαξαν τις ομάδες αίματος ασθενών. Αργότερα, ο εκπρόσωπος του Πενταγώνου ξεκαθάρισε ότι αυτή η ενέργεια ήταν μέρος άσκησης που σκοπό είχε να δοκιμάσει την ασφάλεια του συστήματος, η οποία μάλιστα βρισκόταν ακόμα σε στάδιο ανάπτυξης και δεν είχε τελειοποιηθεί. Σύμφωνα με τις ίδιες δηλώσεις, δεν μεταβλήθηκαν στην πραγματικότητα οποιαδήποτε ηλεκτρονικά δεδομένα. Η άσκηση αυτή ήταν μέρος μιας γενικότερης προσομοίωσης "ηλεκτρονικού πολέμου". Υπό φυσιολογικές συνθήκες αυτή η βάση δεδομένων δεν συνδέεται καν με το Ίντερνετ για λόγους ασφαλείας.

## 6.4 Περιγραφή νομικού πλαισίου

### 6.4.1 Κανονισμοί σε Διεθνές Επίπεδο

Οι πρώτες αντιδράσεις στο πεδίο της προστασίας προσωπικών δεδομένων καταγράφονται σε διεθνές επίπεδο από τότε που καταγράφθηκε η ανάγκη νομοθετικής προστασίας της ιδιωτικότητας. Η ανάγκη της ιδιωτικότητας διατυπώθηκε στη Σύμβαση της Ρώμης της 4ης Νοεμβρίου 1950 για την προστασία των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών. Η Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ) του 1950 προστατεύει στο άρθρο 8 την ιδιωτική ζωή, στην οποία συγκαταλέγονται και τα προσωπικά δεδομένα.

Ως προς τα ιατρικά δεδομένα το Δικαστήριο των Ανθρωπίνων Δικαιωμάτων όρισε αυστηρές προϋποθέσεις για την ανακοίνωσή τους σε τρίτους. Οι πρώτες ανησυχίες για την ιδιωτικότητα τέθηκαν στον νόμο για την προστασία δεδομένων του 1970 (Hesse Data

Protection Act 1970), τον Σουηδικό νόμο για την προστασία των δεδομένων του 1973 (Swedish Privacy Act 1973) και τον νόμο περί ιδιωτικότητας των ΗΠΑ του 1974 (US Privacy Act 1974), οι οποίοι έθεσαν τις απαιτήσεις χωρίς όμως να έχουν καμία εξουσία γύρω από την προστασία των δεδομένων. Ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) ήταν ο δεύτερος διεθνής οργανισμός που το 1980 ασχολήθηκε με την προστασία προσωπικών δεδομένων, εκδίδοντας «Κατευθυντήριες Αρχές που διέπουν την προστασία της ιδιωτικότητας και τις διασυνοριακές ροές προσωπικών δεδομένων».

Οι Αρχές αυτές περιλαμβάνουν την αρχή της περιορισμένης συγκέντρωσης και συλλογής δεδομένων, την αρχή της ποιότητας των δεδομένων, την αρχή του προσδιορισμένου σκοπού, την αρχή της περιορισμένης χρήσης των προσωπικών δεδομένων, την αρχή μέτρων ασφαλείας των προσωπικών δεδομένων, την αρχή της διαφάνειας, την αρχή της συμμετοχής του ατόμου και την αρχή της ευθύνης. Είναι ένα πλαίσιο γενικών αρχών χωρίς δεσμευτικό χαρακτήρα που συγκέντρωσε για μεγάλο διάστημα τη συναίνεση πολλών χωρών και κυρίως εκείνων που στερούνταν ειδικής νομοθεσίας για την προστασία προσωπικών δεδομένων.

Νεότερα δεοντολογικά κείμενα αποτρέπουν τους γιατρούς από το να αποθηκεύουν τα προσωπικά στοιχεία των ασθενών σε ηλεκτρονικούς υπολογιστές ή αν αυτό συμβαίνει, να γίνεται κάτω από αυστηρές προϋποθέσεις. Τέτοια κείμενα είναι η Διακήρυξη της Ευρωπαϊκής Ένωσης των Γενικών Γιατρών για το Ιατρικό Απόρρητο (1979), η Απόφαση της Παγκόσμιας Ιατρικής Ένωσης για τη χρησιμοποίηση των Ηλεκτρονικών Υπολογιστών στην Ιατρική (1983) και η Διεθνής Συνδιάσκεψη Ιατρικών Συλλόγων, που επεξεργάστηκε τις Αρχές της Ευρωπαϊκής Ιατρικής δεοντολογίας (1987). Τη διαφύλαξη των ιατρικών αρχείων με ατομική ευθύνη των γιατρών και την προστασία απορρήτου ακόμα και από τον εργοδότη τους και τη διοίκηση, προστατεύουν άλλα δύο κείμενα Διεθνών Οργανώσεων, ο Χάρτης του Μισθωτού Γιατρού και ο Χάρτης του Νοσοκομειακού Γιατρού, που υιοθετήθηκαν από τη Γενική Συνέλευση της Διαρκούς Επιτροπής των Γιατρών της ΕΟΚ το 1984 και το 1985, αντίστοιχα.

Στις Η.Π.Α, η νομοθετική πράξη "Fair Health Information Practices Act" του 1994 απαιτούσε τον περιορισμό της χρήσης προσωπικών δεδομένων υγείας μόνο στα σημεία που είναι απαραίτητα. Την ίδια χρονιά, ο οργανισμός ACR (American College of Radiology)

εξέδωσε το Πρότυπο ACR για την τηλεραδιολογία (ACR Technical Standard for Teleradiology, Res. 21), το οποίο υπέστη διαδοχικές αναθεωρήσεις, με πιο πρόσφατη αυτήν το 2005 (Res. 39). Το πρότυπο αυτό περιλαμβάνει συστάσεις για τη χρήση και τους στόχους της τηλεραδιολογίας, τις προδιαγραφές τον εξοπλισμού, τις ικανότητες, την πιστοποίηση και την υπευθυνότητα του ιατρικού και παραϊατρικού προσωπικού, τον έλεγχο ποιότητας και την επικοινωνία. Το 1995, το Ινστιτούτο CPRI (Computer-based Patient Record Institute) εξέδωσε οδηγία για τον καθορισμό πολιτικών ασφαλείας, όπου αναφέρεται ότι κάθε οργανισμός που δημιουργεί, χρησιμοποιεί, αποθηκεύει ή μεταδίδει προσωποποιημένα δεδομένα υγείας, έχει ηθική και νομική υποχρέωση να διατηρεί το απόρρητο και την ακεραιότητα των δεδομένων αυτών.

Το Αμερικανικό Κογκρέσο θέσπισε την «Health Insurance Portability and Accountability Act (HIPAA)» το 1996 (Public Law 104-191). Διασαφηνίζεται μια σειρά διαχειριστικών θεμάτων στον τομέα της υγείας και ορίζεται ένα πλαίσιο προδιαγραφών που πρέπει να τηρούνται από τους φορείς υγείας κατά τη μετάδοση και αποθήκευση ιατρικής πληροφορίας με στόχο την ασφάλεια των δεδομένων και την προστασία των προσωπικών στοιχείων των ασθενών. Επιδιώκει να περιορίσει την δυνατότητα των εργοδοτών να αρνηθούν ασφαλιστική κάλυψη στους εργαζομένους με προϋπάρχοντα προβλήματα υγείας. Αυτός ο νόμος είχε ως αποτέλεσμα την διασφάλιση της ιδιωτικότητας του ασθενή αλλά και την αύξηση του κόστους παροχής φροντίδας υγείας. Ως HIPAA περιγράφηκε μια αρχή προστασίας του καταναλωτή που εκτός των άλλων δίνει στα άτομα το δικαίωμα να λάβουν τον προσωπικό ηλεκτρονικό τους φάκελο, να ζητήσουν τροποποιήσεις στον φάκελο τους και να μάθουν σε ποιους αποκαλύφτηκαν πληροφορίες από τον φάκελο τους.

Σύμφωνα με το νόμο αυτό, το Υπουργείο Υγείας (Department of Health and Human Services — HHS) όφειλε να θεσπίσει πρότυπα ασφάλειας βάσει του οριζόμενου πλαισίου. Ως απάντηση, το υπουργείο δημοσίευσε το 1998 πρότυπα για την ασφάλεια των ιατρικών δεδομένων και την ηλεκτρονική υπογραφή και έθεσε προθεσμία πέντε ετών στους αρμόδιους φορείς για πλήρη συμμόρφωση με τα πρότυπα αυτά. Τα πρότυπα ασφάλειας της HIPAA ισχύουν για τις προστατευμένες ιατρικές πληροφορίες που είτε αποθηκεύονται είτε μεταφέρονται ηλεκτρονικά. Προστατευμένες είναι αυτές οι πληροφορίες που οδηγούν στην αναγνώριση της ταυτότητας του ασθενούς δηλαδή τα ευαίσθητα προσωπικά δεδομένα. Στην

Αμερική το 2003 θεσμοθετήθηκε η νομική υποχρέωση της προάσπισης της ιδιωτικότητας και της εμπιστευτικότητας των δεδομένων του ασθενή υπό την αιγίδα του HIPAA. Οι κανονισμοί HIPAA θέτουν τις αρχές και τις διαδικασίες για την εξασφάλιση ότι η αποκάλυψη προσωπικών δεδομένων θα μειωθεί στο ελάχιστο δυνατό. Σύμφωνα με τις νομοθετικές ρυθμίσεις της HIPAA, οι ιατρικές πληροφορίες δεν πρέπει να αποκαλύπτονται χωρίς την συγκατάθεση του ασθενή, εκτός εάν απαιτείται η αποκάλυψη τους κάτω από ειδικές συνθήκες, όπως για ερευνητικούς σκοπούς. Η συναίνεση που απαιτείται για την αποκάλυψη των προσωπικών πληροφοριών του ασθενή εξαρτώνται από την αιτία της αποκάλυψής τους. Έτσι για την αποκάλυψη πληροφοριών, οι οποίες είναι απαραίτητες για τον καθορισμό της θεραπείας, της χρέωσης και της κάλυψης των υπηρεσιών για την παροχή φροντίδας του ατόμου, απαιτείται μια απλή, γενική συναίνεση από τον ίδιο τον ασθενή.

Η HIPAA απαιτεί από τα νοσοκομεία να έχουν μηχανισμούς για να μπορεί να ελέγχεται ποιο άτομο είχε πρόσβαση και σε ποια δεδομένα, την ημερομηνία και την ώρα που έγινε αυτό, εάν η πρόσβαση ήταν επιτυχής και με ποιο τρόπο έγινε αυτό, δηλαδή εάν απλά είδε τα δεδομένα, εάν έγραψε νέα, εάν έκανε αλλαγές ή εάν έσβησε κάποια δεδομένα. Οι απαιτήσεις είναι οι ίδιες και σε δεδομένα που δεν είναι σε μορφή κειμένου αλλά σε μορφή εικόνας (αξονική-μαγνητική-ακτινογραφία). Έτσι θέτει περιορισμούς στη χρήση των εικόνων και αποτρέπει την μη εξουσιοδοτημένη πρόσβαση σε αυτές.

Ο οργανισμός NEMA (National Electrical Manufacturers Association) έχει ιδρύσει μια Επιτροπή (Privacy and Security Committee), η οποία επιλαμβάνεται θεμάτων προστασίας και ασφάλειας των προσωπικών δεδομένων, αλλά και ειδικά της ιατρικής πληροφορίας που χρήζει ιδιαίτερης προσοχής. Η Επιτροπή αυτή μελετά τους σχετικούς κανονισμούς που έχουν θεσπιστεί στις ΗΠΑ, την Ευρώπη και την Ιαπωνία και επιχειρεί να αναδείξει στοιχεία ασυμβατότητας μεταξύ τους, τα οποία περιπλέκουν τη σχεδίαση και εφαρμογή λύσεων ασφάλειας που να είναι καθολικά αποδεκτές. Επιδιώκει να συμβάλει στην καθιέρωση διεθνών προτύπων εναρμονισμένων με τις διαφορετικές μεταξύ χωρών νομοθετικές ρυθμίσεις ως προς τη σχεδίαση και θεμιτή χρήση του ιατροτεχνολογικού εξοπλισμού και των ιατρικών πληροφοριακών συστημάτων, προκειμένου να διευκολυνθεί η συνεργασία και ανταλλαγή προϊόντων και να διασφαλιστεί η προστασία των ασθενών σε παγκόσμια κλίμακα. Για το σκοπό αυτό, συνεργάζεται στενά με την Ευρωπαϊκή Ομοσπονδία Κατασκευαστών Ιατρικού

Εξοπλισμού (European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry — COCIR) που αποτελεί τον αντίστοιχο φορέα στην Ευρώπη και επιδιώκει συνεργασία τόσο με τον αντίστοιχο ιαπωνικό οργανισμό JIRA (Japan Industries Association of Radiological Systems), όσο και με άλλους ενδιαφερόμενους οργανισμούς και εταιρείες. Από τη συνεργασία των οργανισμών NEMA και ACR προέκυψε η σύσταση της Επιτροπής Ψηφιακής Απεικόνισης και Μετάδοσης στην Ιατρική DICOM (Digital Image and Communication in Medicine), με στόχο την προτυποποίηση της μετάδοσης ιατρικών εικόνων και μεταδεδομένων.

Η ενότητα 15 του Πρότυπου DICOM εκδόθηκε το 2001 προκειμένου να παράσχει μια προτυποποιημένη μέθοδο για ασφαλή μετάδοση και ψηφιακή υπογραφή (PS 3.15-2001). Προδιαγράφει τα τεχνικά μέσα (επιλογή προτύπων ασφάλειας, αλγορίθμους και παραμέτρους) για οντότητες εφαρμογής που εμπλέκονται στην ανταλλαγή πληροφορίας για εφαρμογή πολιτικών ασφάλειας. Σε αυτήν την ενότητα του DICOM έχουν προστεθεί τέσσερα προφίλ ασφάλειας: ασφαλούς χρήσης, ασφαλούς σύνδεσης μετάδοσης (secure transport connection profile), ψηφιακής υπογραφής και ασφαλούς αποθήκευσης δεδομένων (media storage secure profiles). Τα παραπάνω προφίλ θέτουν θέματα όπως χρήση χαρακτηριστικών, ασφάλεια στις συνδέσεις, πιστοποίηση αντικειμένων και ασφάλεια των αρχείων.

Επιπλέον, ο Οργανισμός Εφαρμογών Πληροφορικής στην Ακτινολογία (Society of Computer Applications in Radiology - SCAR) εξέδωσε το 2000 την οδηγία «Θέματα ασφαλείας σε ψηφιακές ιατρικές επιχειρήσεις» (Security issues in the digital medical enterprise), προκειμένου να δώσει έμφαση στην επιτακτική ανάγκη αντιμετώπισης του συγκεκριμένου κρίσιμου ζητήματος. Με βάση τα παραπάνω, διεθνείς οργανισμοί έχουν καθορίσει μια σειρά από πρότυπα σχετικά με την ασφάλεια πληροφοριακών συστημάτων και δεδομένων στο χώρο της υγείας. Οι οργανισμοί αυτοί συνεργάζονται στενά μεταξύ τους και περιλαμβάνουν:

- την Ευρωπαϊκή Επιτροπή Τυποποίησης (European Standards Committee - CEN) που συνέστησε το 1990 την Τεχνική Επιτροπή 251 (TC 251) με στόχο την προτυποποίηση στον τομέα της ιατρικής Πληροφορικής

- το διεθνή οργανισμό τυποποίησης ISO (International Standards Organization) που συνέστησε το 1998 την Τεχνική Επιτροπή 215 (TC 215) για τον ίδιο σκοπό

- τον οργανισμό HL7 (Health Level 7) που ιδρύθηκε το 1987 στις Η.Π.Α., εγκρίθηκε από τον ANSI (American National Standards Institute) το 1994 ως Οργανισμός Ανάπτυξης Προτύπων (Standards Developing Organization - SDO) και πλέον έχει παραρτήματα σε όλον τον κόσμο

- την επιτροπή DICOM

- το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών IEEE (Institute of Electrical and Electronics Engineers) που ίδρυσε την επιτροπή 1073, η οποία στοχεύει στη διαμόρφωση προτύπων σχετικών με την επικοινωνία μεταξύ ιατρικών συσκευών.

Παρακάτω παρατίθεται μια ενδεικτική λίστα από πρότυπα που έχουν εκδοθεί με στόχο την ασφάλεια πληροφοριακών συστημάτων και δεδομένων στο χώρο της υγείας:

***Τα κείμενα εργασίας της Ευρωπαϊκής Επιτροπής Τυποποίησης CEN/TC251 για τα ιατρικά πληροφοριακά συστήματα. Ενδεικτικά αναφέρονται τα ακόλουθα:***

- ✓ ENV 12924: 1996 Health informatics - security categorization and protection for healthcare information systems

- ✓ ENV 12388: 1997 Health informatics - Algorithm for digital signature services in healthcare

- ✓ ENV 13608: 2000 Health informatics - Security for health care Communications

  - Part 1 Concepts and terminology ENV 13608 -1
  - Part 2 Secure data objects ENV 13608 – 2

- Part 3 Secure data channels ENV 13608 – 3

✔ ENV 13729: 2000 Health informatics - Secure user identification - strong authentication using microprocessor cards

✔ ENV 12551: 2000 Health informatics - Secure user authentication for health care - Management and security of authentication by passwords

✔ EN 14484: 2002 Health Informatics - International transfer of personal health data covered by the EU Data Protection Directive - High level security policy

✔ CR 13694: 1999 Health Informatics - Safety and security related software quality standards for healthcare

✔ CR 14301: 2002 Health Informatics - Framework for security protection of healthcare communication

✔ CR 14302: 2002 Health Informatics - Framework for security requirements for intermittently connected devices.

***Από το διεθνή οργανισμό τυποποίησης (ISO):***

- ISO DTS 17090 Health Informatics — Public Key Infrastructure

- ISO/IEC 17799: 2005 (=BS 7799) Information Technology – Security techniques

- Code of practice for information security management.

- Part 1: Code of Practice for information security management
- Part 2: Specification for information security management systems

- ISO/ CD TC 215: TR 21089, Health Informatics - Trusted end-to-end information flows

- ISO/IEC TR 13335 Guidelines for the Management of IT Security

o Part 1: Concepts and Models
o Part 2: Managing and Planning IT Security
o Part 3: Techniques for the management of IT Security

***Οι κατευθυντήριες γραμμές της ASTM (American Society for Testing and Materials) σχετικά με την ασφάλεια ιατρικών πληροφοριακών συστημάτων:***

✓ E 2086-00 Standard Guide for Internet and Intranet Healthcare Security

✓ E 2085-00a Standard Guide on Security Framework for Healthcare Information

✓ Τα Κοινά Κριτήρια (Common Criteria for Information Technology Security) που αναφέρονται στην αξιολόγηση της ασφάλειας πληροφοριακών συστημάτων:
ISO/IEC 15408-1: 1999 Information technology - Security techniques- Evaluation criteria for IT security.

### 6.4.2 Ευρωπαϊκή Νομοθεσία

#### 6.4.2.1 Διατάξεις και γνωμοδοτήσεις σε ευρωπαϊκό επίπεδο

Η Ευρωπαϊκή Σύμβαση των Δικαιωμάτων τον Ανθρώπου – ΕΣΔΑ (European Human Rights Convention - EHRC) του 1950. Το άρθρο 8 προστατεύει την ιδιωτική ζωή, στην οποία συγκαταλέγονται και τα προσωπικά δεδομένα. ως προς τα ιατρικά δεδομένα το Δικαστήριο Ανθρωπίνων Δικαιωμάτων όρισε αυστηρές προϋποθέσεις για την ανακοίνωσή τους σε τρίτους.

Οι κατευθυντήριες γραμμές που εξέδωσε το 1980 ο ΟΟΣΑ (Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης / Organization for Economic Cooperation and Development – OECD) για την προστασία των προσωπικών δεδομένων. Επίσης, το 1998 ο ΟΟΣΑ εξέδωσε μια οδηγία σχετικά με την υλοποίηση των παραπάνω γραμμών σε παγκόσμια δίκτυα, ενώ το 2002 υιοθέτησε κατευθυντήριες γραμμές για την Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων (OECD Guidelines for the Security of Information Systems and Networks), υποδεικνύοντας ότι η ασφάλεια εμπίπτει στην ευθύνη όλων των συμμετεχόντων, ανάλογα με το ρόλο τους.

Η Σύσταση 108 του Συμβουλίου της Ευρώπης (28/1/1981) για την προστασία ατόμων από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, η οποία ορίζει ότι τα ιατρικά δεδομένα δεν μπορούν να γίνουν αντικείμενο αυτοματοποιημένης επεξεργασίας, χωρίς εγγυήσεις για την προστασία τους βάσει νόμου. Η Σύσταση 108 έθεσε κανόνες για την προστασία των προσωπικών δεδομένων στην περίπτωση διασυνοριακής ροής πληροφοριών. Υπήρξε το πρώτο διεθνές δεσμευτικό κείμενο αλλά δεν ήταν αμέσου εφαρμογής. Η ισχύς της στο εσωτερικό δίκαιο των χωρών εξαρτιόταν από την κύρωσή της αλλά και την θέσπιση εσωτερικών ρυθμίσεων. Η Σύσταση 108 άρχισε να ισχύει στην Ελλάδα από την 01-01-1995, χωρίς ωστόσο να δημιουργεί ένα επαρκές καθεστώς προστασίας των προσωπικών δεδομένων. Μετά την έκδοση της οδηγίας 95/46/ΕΕ ωστόσο η Σύσταση αυτή έχει περιορισμένη σπουδαιότητα.

Η Διακήρυξη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (Charter of Fundamental Rights of the European Union), αποτελεί την πιο πρόσφατη εξέλιξη στον τομέα των θεμελιωδών δικαιωμάτων των πολιτών. Η διακήρυξη αυτή ορίζει ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση τη συγκατάθεση τον ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο. Επίσης, κάθε πρόσωπο έχει δικαίωμα να έχει πρόσβαση στα δεδομένα που το αφορούν και να τα διορθώνει.

Η Οδηγία 95/46/ΕΕ (Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data) της ΕΕ προς τα κράτη-μέλη, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία των δεδομένων αυτών. Με την Οδηγία αυτή εξασφαλίζεται η εναρμόνιση των εθνικών νομοθεσιών των κρατών-μελών ως προς την προστασία των προσωπικών δεδομένων και η ελεύθερη κυκλοφορία τους στα κράτη-μέλη. Η οδηγία της Ευρωπαϊκής Ένωσης 95/46/ΕΚ υιοθετήθηκε στις 24 Οκτωβρίου 1995. Η θέση της είναι αρκετά διαφορετική από το σύμφωνο και τις μέχρι τώρα προτάσεις του Συμβουλίου της Ευρώπης στο ότι η οδηγία είναι υποχρεωτική για όλες τις χώρες της Ευρωπαϊκής Ένωσης. Ωστόσο, η θέση της περιορίζεται στην νόμιμη ισχύ και αρμοδιότητα του Ευρωπαϊκού Νόμου σε κάθε κράτος-μέλος.

Η Οδηγία 2002/58/ΕΕ (2002/58/EC) για την προστασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών που αντικατέστησε την Οδηγία 97/66/ΕΕ (Directive 97/66/EC) για την προστασία των προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα.

Η Σύσταση No R (75)5 του Συμβουλίου της Ευρώπης. Το έργο του Συμβουλίου της Ευρώπης στην περιοχή της ιατρικής γενετικής και της βιοηθικής οδήγησε στην άποψη ότι ίσως υπάρξουν κάποια προβλήματα ανάμεσα στις απαιτήσεις για συμβουλευτική σε θέματα γενετικής και στην προστασία των δεδομένων που ανταλλάσσονται, με αποτέλεσμα την αναθεώρηση της Πρότασης για τις Αυτοματοποιημένες Τράπεζες Ιατρικών δεδομένων. Αυτό το έργο ήταν μια προσπάθεια να καταγραφεί η κατάσταση της παροχής υγείας στην Ευρώπη και να διασφαλιστεί ότι οι επαγγελματίες υγείας ακολουθούν τα πρότυπα κατά την διαχείριση των ιατρικών δεδομένων έτσι ώστε οι ασθενείς να μπορούν να είναι σίγουροι ότι τα

προσωπικά τους δεδομένα προστατεύονται με ένα ομοιόμορφο τρόπο. Αυτή η νέα Πρόταση υιοθετήθηκε στις 12 Φεβρουαρίου 1997 ως Πρόταση R (75)5 και αντικατέστησε την μέχρι τότε ισχύουσα προσφέροντας μια νέα βάση για τον τρόπο διαχείρισης ιατρικών προσωπικών δεδομένων συμπεριλαμβάνοντας και τα προσωπικά δεδομένων γύρω από την γενετική.

Η Σύσταση No R(81)1 έδινε ακριβείς οδηγίες για την χρήση των αυτόματων ιατρικών βάσεων δεδομένων, κάτι για το οποίο δεν είχε παρατηρηθεί μέχρι τότε το αντίστοιχο διεθνές ενδιαφέρον. Η οδηγία R(81)1 απαίτησε από τις ιατρικές βάσεις δεδομένων να αναπτύξουν ένα σύνολο από κανονισμούς που θα καθοδηγούν όλες τις λειτουργίες και καθόρισε ένα ελάχιστο μέγεθος περιεχομένου που πρέπει να αναφέρεται σε κάθε αναπτυσσόμενο κανονισμό για την νέα βάση ιατρικών δεδομένων κάτι που πρόσφατα περιγράφεται ως πολιτική ασφαλείας. Έθεσε τα κατάλληλα μέτρα ώστε να είναι δυνατή η πρόσβαση του υποκειμένου μέσω της παρέμβασης του γιατρού. [Council of Europe Recommendation, R(81)1]

Η Σύσταση No R(97) 5 (Recommendation No R(97) 5 on the protection of medical data), η οποία έγινε δεκτή από το Συμβούλιο της Ευρώπης το 1997 και αφορά την προστασία ιατρικών δεδομένων. [Council of Europe Recommendation, R(97)5]

Η Σύσταση No R(99) 5 (Recommendation No R(99) 5), η οποία έγινε δεκτή από το Συμβούλιο της Ευρώπης το 1999 και η οποία παρέχει κατευθυντήριες γραμμές (guidelines) για την προστασία των ατόμων σε σχέση με τη συλλογή και επεξεργασία προσωπικών δεδομένων σε «λεωφόρους πληροφοριών» (information highways).

Η Γνωμοδότηση του European Group on Ethics in Science and New Technologies (Opinion No 13 — Ethical issues of healthcare in the information society) του 1999, η οποία κατοχυρώνει τον ορισμό των προσωπικών ιατρικών δεδομένων. Η γνωμοδότηση δίνει έμφαση σε βασικές αρχές που αφορούν την επεξεργασία των ιατρικών δεδομένων, ορίζοντας μεταξύ άλλων ότι απαιτούνται τεχνικά και οργανωτικά μέτρα ασφαλείας και η εφαρμογή τεχνολογιών κρυπτογραφίας. Η γνωμοδότηση καταλήγει στο ότι τα θέματα αυτά πρέπει να κατοχυρωθούν νομικά, κατά προτίμηση μέσω κάποιας οδηγίας της Ευρωπαϊκής Ένωσης σχετικά με την προστασία των ιατρικών δεδομένων.

### 6.4.3 Ελληνική Νομοθεσία

Κατά την τελευταία αναθεώρηση του Συντάγματος κρίθηκε επιβεβλημένη η κατοχύρωση ενός νέου ειδικού δικαιώματος προστασίας των προσωπικών δεδομένων. Το νέο άρθρο 9Α του ελληνικού Συντάγματος 1975/86/01 που συμπεριλήφθηκε στο Σύνταγμα με την τελευταία αναθεώρηση του 2001 ορίζει ότι ο «καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών δεδομένων, όπως ο νόμος ορίζει». Στη νέα διάταξη αναδεικνύεται ωστόσο η ένταση των κινδύνων που εμπεριέχει η επεξεργασία δεδομένων με ηλεκτρονικά μέσα. Η προστασία προσωπικών δεδομένων ανήκει στην κατηγορία των νέων δικαιωμάτων που κατοχυρώνει το αναθεωρημένο Σύνταγμα, κοινό στοιχείο των οποίων είναι η εξασφάλιση όχι μόνο έναντι της κρατικής εξουσίας αλλά και έναντι των ιδιωτών. Καθώς αυτό το δικαίωμα είναι ευάλωτο σε προσβολές από τους ιδιώτες, το κράτος δεν μπορεί να αρκείται στην αποχή και την αποτροπή των προσβολών αυτών από τα όργανα του, αλλά πρέπει να μην επιτρέπει την προσβολή του από ιδιώτες, λαμβάνοντας μέτρα για το σκοπό αυτό. Η μόνη απόφαση του αναθεωρητικού νομοθέτη σχετικά με τις εγγυήσεις προστασίας των προσωπικών δεδομένων αφορά τη Συνταγματική κατοχύρωση της ανεξάρτητης αρχής με αποστολή τη διασφάλιση του δικαιώματος. Η ίδρυση ανεξάρτητων αρχών αποτυπώνεται ως εγγενές χαρακτηριστικό του συστήματος προστασίας προσωπικών δεδομένων σε διεθνή κείμενα, δεσμευτικά ή μη.

Η εναρμόνιση της ελληνικής νομοθεσίας προς τη σχετική Κοινοτική Οδηγία 95/46/ΕΕ (Data Protection Directive) σχετικά με την «προστασία του ατόμου όσον αφορά την επεξεργασία προσωπικών δεδομένων και την ελεύθερη διακίνησή τους» και τη σύσταση R 97 (5) περί προστασίας ιατρικών δεδομένων, έγινε με τη θέσπιση του Νόμου 2472/1997 περί «Προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα».

Ο Νόμος 2472/1997 μεταφέρει την Οδηγία 95/46/ΕΕ στο εσωτερικό δίκαιο και συγχρόνως εκπληρώνει την υποχρέωση της Ελλάδας που απορρέει από τη Σύμβαση 108 τον Συμβουλίου της Ευρώπης. Επιπλέον, η Οδηγία 97/66/ΕΕ, που εξειδικεύει την Οδηγία 95/46/ΕΕ ως προς ορισμένες πτυχές που συνδέονται με τη συγκεκριμένη κατηγορία εφαρμογής, μεταφέρεται στο εσωτερικό δίκαιο με τον ελληνικό νόμο 2774/99. Ειδικά για τα

ιατρικά δεδομένα, η προστασία τους διέπεται, εκτός από τις διατάξεις των νόμων 2472/97 και 2774/99, από το άρθρο 371 τον Ποινικού Κώδικα στο οποίο κατοχυρώνεται το ιατρικό απόρρητο. Η προστασία της ιδιωτικής ζωής του ασθενούς και ο απόρρητος χαρακτήρας του ιατρικού φακέλου κατοχυρώνονται επιπλέον στο Άρθρο 47 τον Ν. 2071/92 (Νόμος Ε.Σ.Υ.).

# ΕΠΙΛΟΓΟΣ

Ο Ουίνστον Τσόρτσιλ υποστήριζε ότι γνωρίζοντας τον εχθρό κάνεις το πρώτο βήμα για να τον νικήσεις. Έτσι λοιπόν και η γνώση και η καθημερινή επαγρύπνηση που απαιτείται για τη διατήρηση της ασφάλειας σε ένα σύστημα που διαχειρίζεται προσωπικές και εμπιστευτικές για την υγεία πληροφορίες πρέπει να ακολουθεί την ίδια γραμμή. Όπως τα περισσότερα πράγματα στη ζωή, η ισορροπία και η ορθή κρίση είναι οι καλύτεροι οδηγοί που απαιτούνται για την εξασφάλιση της ασφάλειας σε ένα σύστημα. Σε ορισμένες περιπτώσεις ωστόσο, μια πιθανή παραβίαση μπορεί να είναι λιγότερο επιβλαβής σε σύγκριση με το κόστος και της ροή εργασίας που χρειάστηκε για να δημιουργηθεί ένα σχέδιο ασφαλείας.

Παρ' όλα αυτά, σήμερα, καθολικό είναι το αίτημα αναβάθμισης των παρεχόμενων υπηρεσιών υγείας και του μετασχηματισμού της δομής τους προς ένα πιο ανθρωποκεντρικό μοντέλο λειτουργίας. Καθοριστικό ρόλο στην επίτευξη του στόχου αυτού διαδραματίζει η δυνατότητα ασφαλούς ανταλλαγής και αξιοποίησης της ιατρικής πληροφορίας. Μια πρόταση λοιπόν με πολλά υποσχόμενα και ενθαρρυντικά μηνύματα είναι οι έξυπνες κάρτες υγείας αφού “*μια από τις σημαντικότερες λειτουργίες των έξυπνων καρτών είναι η ασφάλεια και η ακεραιότητα των αποθηκευμένων πληροφοριών που παρέχονται με την κρυπτογράφηση των δεδομένων*”. [Καραπέτσης 1994].

Οι έξυπνες κάρτες παρέχουν ένα εύκολο και ασφαλή τρόπο αποθήκευσης ιατρικών πληροφοριών, δίνουν άμεση πρόσβαση στην ιατρική πληροφορία, διαφυλάσσουν το ιατρικό απόρρητο, παρέχουν ελεγχόμενη πρόσβαση στα στοιχεία της και είναι συμβατές με όλα τα ιατρικά πληροφοριακά συστήματα, τα δίκτυα και τις εφαρμογές τους. Σε περίπτωση απώλειας απενεργοποιούνται και αντικαθίστανται αμέσως. Ακόμα, υποστηρίζουν υπηρεσίες αποπληρωμής και περιέχουν στοιχεία για άτομα τα οποία χρειάζονται ειδική ιατρική μέριμνα. Είναι μια καινοτόμα τεχνολογία που αναπτύσσεται με ταχείς ρυθμούς σε όλο τον κόσμο και προσφέρει πρόσβαση όχι μόνο στις υπηρεσίες υγείας αλλά και στις ηλεκτρονικές πληρωμές, στις δημόσιες συγκοινωνίες, κ.λ.π,

Στο χώρο της υγείας οι έξυπνες κάρτες βρίσκουν εφαρμογή στην ταυτοποίηση του ασθενούς, στην εισαγωγή του ιατρικού ιστορικού , στις προπληρωμένες λύσεις κ.λ.π. Η χώρα μας παρακολουθώντας τις διεθνείς εξελίξεις ως μέλος της Ευρωπαϊκής Ένωσης ακολουθώντας πάντα το νομικό πλαίσιο προστασίας των ευαίσθητων προσωπικών δεδομένων, συμμετέχει στις προσπάθειες για την ανάπτυξη τω εφαρμογών των έξυπνων καρτών υγείας. Μέχρι σήμερα τα μηνύματα από την εφαρμογή προγραμμάτων έξυπνων καρτών υγείας είναι θετικά.

# ΒΙΒΛΙΟΓΡΑΦΙΑ – ΠΗΓΕΣ

1. "Εισαγωγή στη Βιοιατρική τεχνολογία και στην ανάλυση Ιατρικών Σημάτων" Δ.Κουτσούρης , Σ.Παυλόπουλος, Α.Πρέντζα Εκδόσεις Τζιόλα
2. Γρίβας Β., Κουκούμας Ν., Ξανθόπουλος Κ., Σφυρής Ν., Χρυσοχοΐδης Ι., "Οικονομική και Χρηματοδοτική Διαχείριση Υπηρεσιών Υγείας", Ελληνικό Ανοικτό Πανεπιστήμιο
3. "Πληροφοριακά Συστήματα Υγείας"Αποστολάκης Ι. Εκδόσεις Παπαζήση (2002)
4. Applied Cryptography by Bruce Schneier Second Edition John Wiley and Sons 1996
5. Understanding PKI Concepts, Standards, and Deployment Considerations by Carlisle Adams, Steve Lloyd. Second Edition Addison-Wesley Professional (2003)
6. Jr. Kaliski, .On the Security and Performance of Several Triple-DES Modes., RSA Laboratories, January 1994
7. The MD5 Message-Digest Algorithm by R.Rivest 1992
8. Digital Signatures and European Laws By Mirella Mazzeo Jan 12, 2004
9. Barber B., Patient data and security: an overview. International journal of Medical Informatics 1998 49(1):19-30.PubMed
10. Health Level 7,
11. Dr. David B Everett, Smart Card Technology: Introduction To Smart Cards Smart Card News Ltd., 2002
12. Smart Cards, Tokens, Security and Applications by Keith E. Mayes, Konstantinos Markantonakis Information Security Group Smart Card Centre Royal Holloway, University of London UK . 2008 Springer Science+Business Media, LLC
13. Καραπέτσης Σ.,κα (1994) Σύστημα ηλεκτρονικών καρτών υγείας
14. Χαρακτηριστικά κάρτας επαγγελματιών Υγείας
15. The Legal and Market Aspects of Electronic Signatures by the European Commission, final version.
16. Health Care Smart Cards:a Critical Review by Eleni Baltzi RN, BSc, MSc, PhD General Hospital «Sotiria», Athens

17. Smart Card Technology in U.S. Healthcare: Frequently Asked Questions A Smart Card Alliance Healthcare Council Publication September 2012 , Publication Number: HCC-12002 Smart Card Alliance 191 Clarksville Rd. Princeton Junction, NJ 08550

18. International Organization for Standardization

19. Smart Card Basics

20. The Smart Card Club

21. "Νομοθετική προστασία των ευαίσθητων προσωπικών δεδομένων στον ηλεκτρονικό φάκελο υγείας" Μαλλιαρού Μ. Λιάσκος Ι. 2007

22. [1] Οδηγία 95/46/ΕΚ

23. [2] Σύσταση R (81) 1

24. [3] Σύσταση R (97) 5