Πανεπιστήμιο Κρήτης

Σχολή Θετικών Επιστημών

Τμήμα Επιστήμης Υπολογιστών

Σχεδιασμός και Υλοποίηση Υπηρεσιών Ασφαλείας για Δίκτυο Τηλεματικών Υπηρεσιών στην Υγεία με χρήση Έξυπνων Κρυπτογραφικών Καρτών

Κατερίνα Γ. Χατζάκη

Μεταπτυχιακή Εργασία

Ηράκλειο, Νοέμβριος 2001

Πανεπιστήμιο Κρήτης
Σχολή Θετικών Επιστημών
Τμήμα Επιστήμης Υπολογιστών

Σχεδιασμός και Υλοποίηση Υπηρεσιών Ασφαλείας για Δίκτυο Τηλεματικών Υπηρεσιών στην Υγεία με χρήση Έξυπνων Κρυπτογραφικών Καρτών

Εργασία που υποβλήθηκε από την
Κατερίνα Γ. Χατζάκη
ως μερική εκπλήρωση των απαιτήσεων για την απόκτηση
ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΔΙΠΛΩΜΑΤΟΣ ΕΙΔΙΚΕΥΣΗΣ

Συγγραφέας:

_____
Κατερίνα Γ. Χατζάκη
Τμήμα Επιστήμης Υπολογιστών
Πανεπιστήμιο Κρήτης

Εισηγητική Επιτροπή:

_____
Στέλιος Ορφανουδάκης
Καθηγητής, Επόπτης

_____
Απόστολος Τραγανίτης
Αναπληρωτής Καθηγητής, Μέλος

_____
Γεώργιος Γεωργακόπουλος
Επίκουρος Καθηγητής, Μέλος

_____
Μανόλης Τσικνάκης
Ερευνητής Ι.Π. Ι.Τ.Ε, Μέλος
Δεκτή:

_____
Πάνος Κωνσταντόπουλος, Καθηγητής
Πρόεδρος Επιτροπής Μεταπτυχιακών Σπουδών

Ηράκλειο, Νοέμβριος 2001

Στην μητέρα μου

Σχεδιασμός και Υλοποίηση Υπηρεσιών Ασφαλείας για Δίκτυο Τηλεματικών Υπηρεσιών στην Υγεία με χρήση Έξυπνων Κρυπτογραφικών Καρτών

Κατερίνα Γ. Χατζάκη

Μεταπτυχιακή Εργασία

Τμήμα Επιστήμης Υπολογιστών
Πανεπιστήμιο Κρήτης

ΠΕΡΙΛΗΨΗ

Η ύπαρξη ασφαλών μεθόδων εξακρίβωσης της ταυτότητας του χρήστη των εφαρμογών και υπηρεσιών σε ένα δίκτυο τηλεματικών υπηρεσιών στην υγεία είναι απαραίτητη για την αποτελεσματικότητα του μηχανισμού της προστασίας του απορρήτου και της διασφάλισης υπευθυνότητας (accountability), τόσο στο επίπεδο της ασφάλειας κατά την επικοινωνία όσο και στο επίπεδο ασφάλειας των εφαρμογών. Η ασφαλής εξακρίβωση της ταυτότητας του χρήστη είναι θεμελιώδης προϋπόθεση για την σωστή και ασφαλή λειτουργία των συστημάτων ελέγχου πρόσβασης. Συνεπώς η εξακρίβωση της ταυτότητας των χρηστών τηλεματικών υπηρεσιών και ιατρικών πληροφοριακών συστημάτων, είναι μια κρίσιμη παράμετρος, η οποία επηρεάζει και τον βαθμό αποδοχής των νέων αυτών τεχνολογιών από τους επαγγελματίες υγείας.

Μια άλλη υπηρεσία που είναι άκρως απαραίτητη για την ασφάλεια ενός δικτύου τηλεματικών υπηρεσιών στην υγεία είναι η δημιουργία και η επαλήθευση ηλεκτρονικών υπογραφών. Οι ηλεκτρονικές υπογραφές είναι απαραίτητες για την υπογραφή της ευαίσθητης ιατρικής πληροφορίας, ώστε να είναι δυνατή μελλοντικά η εξακρίβωση της αυθεντικότητας της, της ακεραιότητας της, καθώς και η εξασφάλιση της μη άρνησης από τον υπογράφοντα της πράξης της υπογραφής.

Στα πλαίσια της παρούσας μεταπτυχιακής εργασίας μελετήθηκε (α) το ζήτημα της εξακρίβωσης ταυτότητας και (β) των ηλεκτρονικών υπογραφών σε ένα δίκτυο τηλεματικών υπηρεσιών στην υγεία. Έγινε αξιολόγηση και επιλογή του κατάλληλου

τεχνολογικού πλαισίου. Τέλος σχεδιάστηκε και υλοποιήθηκε το μοντέλο ισχυρής εξακρίβωσης ταυτότητας και του μηχανισμού παραγωγής και επαλήθευσης αναγνωρισμένων ηλεκτρονικών υπογραφών (βάση της Ευρωπαϊκής Κοινοτικής Οδηγίας). Το τεχνολογικό πλαίσιο που επιλέχθηκε για την εξασφάλιση του ύψιστου δυνατού επίπεδου ασφαλείας για τον σχεδιασμό και την υλοποίηση των δύο παραπάνω υπηρεσιών βασίζεται στην υποδομή δημοσίου κλειδιού PKI (Public Key Infrastructure). Χρησιμοποιήθηκε ασυμμετρική κρυπτογραφία με δημόσια και ιδιωτικά κλειδιά. Η πιστοποίηση των χρηστών και των αντίστοιχων δημοσίων κλειδιών τους έγινε με την χρήση πιστοποιητικών X.509 που εκδίδονται από Έμπιστη Αρχή Πιστοποίησης. Για μέγιστη ασφάλεια πριν από κάθε χρήση πιστοποιητικού δημοσίου κλειδιού εκτελείται έλεγχος της εγκυρότητας και της κατάστασης ανάκλησης του εν λόγω πιστοποιητικού. Τέλος για την απόλυτη ασφάλεια των ιδιωτικών κλειδιών η παραγωγή τους, η αποθήκευση τους, και η εκτέλεση των αντίστοιχων απαραίτητων κρυπτογραφικών λειτουργιών γίνεται πάνω σε έξυπνες κάρτες (smart cards) με κρυπτογραφικές δυνατότητες.

Επόπτης: Στέλιος Ορφανουδάκης

Καθηγητής Επιστήμης Υπολογιστών

Πανεπιστήμιο Κρήτης

Design and implementation of security services in a healthcare telematics network using cryptographic smart cards

Katerina G. Chatzaki

Master of Science Thesis

Computer Science Department
University Of Crete

ABSTRACT

The existence of secure methods for authenticating user identity in applications and services of a healthcare telematics network is necessary for protecting the confidentiality and accountability, both in the application and communication level. The secure user authentication is a fundamental requirement for the proper and secure function of access control systems. Consequently, the authentication of users of telematic services and healthcare information systems is a critical parameter, which also influences the degree of acceptance of the new telematic technologies from the healthcare professional users.

Another service, which is absolutely necessary for the security of a healthcare telematic services network, is the generation and verification of electronic signatures. Electronic signatures are necessary for signing sensitive medical information, to guarantee authentication of the origin, integrity, and non-repudiation of the signed data.

This master thesis researches the fundamental problem of (a) user authentication and (b) electronic signatures in a healthcare telematics services network. The suitable technological framework was selected after evaluation of different technological solutions. Finally, a model for strong user authentication and a mechanism for generation and verification of qualified electronic signatures (based on the European Community Directive) were designed and implemented. The technological framework was selected to

provide the maximum possible security level for designing and implementing the above two services. The framework is based on the Public Key Infrastructure (PKI), asymmetric cryptography, and X.509 Certificates. The Certificates are generated and managed by a Trusted Certification Authority, which acts as a Trusted Third Party (TTP). For the provision of maximum security level the public key certificate of the user is checked every time that it is used for its validity and revocation status. Finally, the user private keys are generated, stored and used for executing cryptographic functions on a smart card with cryptographic co-processor. Smart cards provide mobility and full protection of private keys in a physical device.

Supervisor: Stelios Orphanoudakis
Professor of Computer Science
University of Crete

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Κεφάλαιο 1

Εισαγωγή

Οι τεχνολογίες της Πληροφορικής και των Επικοινωνιών δίνουν πλέον νέες δυνατότητες για την άρση της απομόνωσης και την ανάπτυξη απομακρυσμένων και νησιωτικών περιοχών. Ιδιαίτερα στον τομέα της υγείας η ανάπτυξη και λειτουργία Ολοκληρωμένων Δικτύων Τηλεματικών Υπηρεσιών αποτελεί ένα στόχο στρατηγικής σε εθνικό και Ευρωπαϊκό επίπεδο. Η ανάπτυξη τέτοιων δικτύων, όπως το δίκτυο HYGEIAnet στην Περιφέρεια Κρήτης, έχει να επιδείξει απτά αποτελέσματα, όσον αφορά στη δυνατότητα και αποτελεσματικότητα χρήσης νέων τεχνολογιών τηλεματικής στο χώρο της υγείας, με σημαντικά οικονομικά και κοινωνικά οφέλη. Χαρακτηριστικά παραδείγματα αποτελούν η κατ' οίκον παροχή υπηρεσιών υγείας, η τηλεματική υποστήριξη των απομακρυσμένων πρωτοβάθμιων φορέων υγείας, η χρήση των νέων τεχνολογιών και τηλεματικών υπηρεσιών από το ΕΚΑΒ για την αποτελεσματικότερη διαχείριση των επειγόντων περιστατικών, και τέλος η ανάπτυξη ολοκληρωμένων πληροφοριακών συστημάτων διαχείρισης του ηλεκτρονικού φακέλου υγείας του πολίτη, και η εκτεταμένη χρήση τηλεματικής για βελτίωση της λειτουργίας των περιφερειακών συστημάτων υγείας.

Η διασφάλιση του απορρήτου είναι ύψιστης σημασίας σε κάθε περίπτωση κατά την οποία γίνεται χειρισμός ευαίσθητης προσωπικής πληροφορίας. Η μη εξουσιοδοτημένη πρόσβαση σε ιατρικά δεδομένα μπορεί να οδηγήσει σε παραβίαση του ιατρικού απορρήτου ή και σε σοβαρές μη εξουσιοδοτημένες μετατροπές των ιατρικών δεδομένων που είναι δυνατόν να θέσουν σε κίνδυνο την υγεία και την ασφάλεια ενός ασθενή.

Άρα, είναι ιδιαίτερα σημαντικό, στα πλαίσια ενός δικτύου τηλεματικών υπηρεσιών στην υγεία, να αναπτυχθεί όλη εκείνη η τεχνολογική υποδομή που είναι

απαραίτητη ώστε να εξασφαλίζεται (α) το ιατρικό απόρρητο (confidentiality), (β) η ακεραιότητα (integrity) και (γ) η διαθεσιμότητα (availability) των προσωπικών ιατρικών δεδομένων του πολίτη-ασθενή. Απαιτείται επίσης η υποδομή να εξασφαλίζει την υπευθυνότητα (accountability) για τις πράξεις που εκτελούνται πάνω στα ευαίσθητα προσωπικά δεδομένα των ασθενών. Πρέπει επίσης να υπάρχει προστασία της εγκυρότητας και αυθεντικότητας της ιατρικής πληροφορίας, και τέλος να διασφαλίζεται η μη Άρνηση της Πράξης (Non-Repudiation).

Η διασφάλιση της μη Άρνησης Πράξης δεν επιτρέπει στα συναλλασσόμενα μέρη να αρνηθούν την συμμετοχή τους σε μια τηλεματική επικοινωνία ή την μη παραδοχή της εκτέλεσης κάποιας πράξης. Η διασφάλιση του απορρήτου είναι ύψιστης σημασίας, ιδιαίτερα όταν γίνεται χειρισμός ευαίσθητης προσωπικής πληροφορίας του ασθενή. Η μη εξουσιοδοτημένη πρόσβαση σε ιατρικά δεδομένα μπορεί να οδηγήσει σε παραβίαση του ιατρικού απορρήτου ή και σε σοβαρές μη εξουσιοδοτημένες μετατροπές των ιατρικών δεδομένων που θέτουν σε κίνδυνο την υγεία και την ασφάλεια του ασθενή.

Η ασφάλεια σε δίκτυο τηλεματικών υπηρεσιών στην υγεία μπορεί να διακριθεί σε δύο επίπεδα: στο επίπεδο της ασφάλειας κατά την επικοινωνία (communication security) και στο επίπεδο της ασφάλειας εφαρμογών (application security). Η ασφάλεια κατά την επικοινωνία έχει να αντιμετωπίσει θέματα όπως η αναγνώριση ταυτότητας (user identification), η εξακρίβωση ταυτότητας (user authentication), και η πιστοποίηση του χρήστη (certification) με την επίδειξη εμπιστοσύνης σε «τρίτη έμπιστη οντότητα» (TTP/Trusted Third Party). Η ασφάλεια σε επίπεδο εφαρμογής ασχολείται κυρίως με τον έλεγχο πρόσβασης (access control) και την ποιότητα δεδομένων (data quality).

Η ύπαρξη ασφαλών μεθόδων εξακρίβωσης της ταυτότητας του χρήστη των εφαρμογών και υπηρεσιών σε ένα δίκτυο τηλεματικών υπηρεσιών στην υγεία είναι απαραίτητη για την αποτελεσματικότητα του μηχανισμού της προστασίας του απορρήτου και της διασφάλισης υπευθυνότητας (accountability), τόσο στο επίπεδο της ασφάλειας κατά την επικοινωνία όσο και στο επίπεδο ασφάλειας των εφαρμογών. Η ασφαλής εξακρίβωση της ταυτότητας του χρήστη είναι επίσης απαραίτητη για την σωστή και ασφαλή λειτουργία των συστημάτων ελέγχου πρόσβασης. Συνεπώς η λειτουργία της εξακρίβωσης της ταυτότητας των ιατρικών επαγγελματιών, που κάνουν χρήση των τηλεματικών υπηρεσιών και των ιατρικών πληροφοριακών συστημάτων, είναι μια κρίσιμη παράμετρος, η οποία επηρεάζει και τον βαθμό αποδοχής των νέων αυτών τεχνολογιών από τους επαγγελματίες υγείας. Στο άμεσο μέλλον η υπηρεσία της ασφαλούς εξακρίβωσης ταυτότητας προβλέπεται να επεκταθεί και θα είναι απαραίτητη και για τον πολίτη-ασθενή που έρχεται σε επαφή με το σύστημα υγείας.

Ο πιο κοινός μηχανισμός εξακρίβωσης ταυτότητας σήμερα είναι το να ζητείται από τον χρήστη να δώσει τον προσωπικό του κρυφό κωδικό πρόσβασης (password) για να αποδείξει την ταυτότητα του. Το μειονέκτημα αυτού του μηχανισμού είναι το γεγονός ότι είναι ευάλωτος σε επιθέσεις κατά τις οποίες ο επιτιθέμενος κρυφάκουει την επικοινωνία που γίνεται για να δοθεί ο κωδικός. Για αυτό τον λόγο η εξακρίβωση ταυτότητας με την χρήση κωδικών ονομάζεται και «ασθενής εξακρίβωση ταυτότητας» (weak authentication). Η ασθενής εξακρίβωση ταυτότητας παρουσιάζει και άλλα μειονεκτήματα, όπως (α) οι χρήστες αποκαλύπτουν σε άλλους χρήστες τους προσωπικούς κρυφούς τους κωδικούς, (β) είναι δύσκολη η απομνημόνευση ενός ασφαλούς κρυφού κωδικού, (γ) είναι δυνατή η εξαντλητική αναζήτηση αυτών των κωδικών βάση λεξικών και (δ) η διαχείριση τους παρουσιάζει σημαντικά προβλήματα ιδιαίτερα σε μεγάλους σύνθετους οργανισμούς. Συνεπώς η εξακρίβωση ταυτότητας με κωδικούς πρόσβασης (passwords) δεν είναι ο βέλτιστος τρόπος σε ένα σύγχρονο δικτυακό περιβάλλον και ιδιαίτερα για την προστασία πολύ ευαίσθητων προσωπικών δεδομένων. Άρα είναι απαραίτητη η ισχυρή εξακρίβωση ταυτότητας με τη χρήση κρυπτογραφικά παραγόμενων διαπιστευτηρίων.

Μια άλλη υπηρεσία που είναι άκρως απαραίτητη για την ασφάλεια ενός δικτύου τηλεματικών υπηρεσιών στην υγεία είναι η δημιουργία και η επαλήθευση ηλεκτρονικών υπογραφών. Οι ηλεκτρονικές υπογραφές είναι απαραίτητες για την υπογραφή της ευαίσθητης ιατρικής πληροφορίας ώστε να είναι δυνατή μελλοντικά η εξακρίβωση της αυθεντικότητας της, της ακεραιότητας της, καθώς και η εξασφάλιση της μη άρνησης από τον υπογράφοντα της πράξης της υπογραφής.

Η θέσπιση ενός τεχνικού πλαισίου για τις ηλεκτρονικές υπογραφές σε ευαίσθητα ιατρικά δεδομένα απαιτεί γνώσεις, οικειότητα και αυξημένες δεξιότητες τόσο στο πεδίο της ασφάλειας των υπολογιστών όσο και στο ανάλογο νομικό πεδίο. Ο συνδυασμός αυτών των δυο τομέων επιστημονικής γνώσης δεν είναι εύκολος. Οι έννοιες από τον τομέα της ασφάλειας πληροφοριών αντιστοιχούν συχνά μόνο αόριστα στις έννοιες από το νομικό τομέα, ακόμη και στις περιπτώσεις όπου η ορολογία είναι παρόμοια.

Στα πλαίσια της παρούσας μεταπτυχιακής εργασίας μελετήθηκε (α) το ζήτημα της εξακρίβωσης ταυτότητας και (β) των ηλεκτρονικών υπογραφών σε ένα δίκτυο τηλεματικών υπηρεσιών στην υγεία. Έγινε αξιολόγηση και επιλογή του κατάλληλου τεχνολογικού πλαισίου. Τέλος σχεδιάστηκε και υλοποιήθηκε το μοντέλο ισχυρής εξακρίβωσης ταυτότητας και του μηχανισμού παραγωγής και επαλήθευσης αναγνωρισμένων ηλεκτρονικών υπογραφών (βάση της Ευρωπαϊκής Κοινοτικής Οδηγίας

[ΚΟΙΝ. ΟΔΗΓΙΑ 99]). Το τεχνολογικό πλαίσιο που επιλέχθηκε για την εξασφάλιση του ύψιστου δυνατού επίπεδου ασφαλείας για τον σχεδιασμό και την υλοποίηση των δύο παραπάνω υπηρεσιών βασίζεται στην υποδομή δημοσίου κλειδιού PKI (Public Key Infrastructure). Χρησιμοποιήθηκε ασυμμετρική κρυπτογραφία με δημόσια και ιδιωτικά κλειδιά. Η πιστοποίηση των χρηστών και των αντίστοιχων δημοσίων κλειδιών τους έγινε με την χρήση πιστοποιητικών X.509 που εκδίδονται από Έμπιστη Αρχή Πιστοποίησης. Για μέγιστη ασφάλεια πριν από κάθε χρήση πιστοποιητικού δημοσίου κλειδιού εκτελείται έλεγχος της εγκυρότητας και της κατάστασης ανάκλησης του εν λόγω πιστοποιητικού βάση Αλυσίδων Πιστοποίησης (Certification Chains) και των Λιστών Ανάκλησης Πιστοποιητικών CRL (Certificate Revocation Lists) που εκδίδονται από την Έμπιστη Αρχή Πιστοποίησης. Για την απόλυτη ασφάλεια των ιδιωτικών κλειδιών η παραγωγή, η αποθήκευση και η εκτέλεση των αντίστοιχων απαραίτητων κρυπτογραφικών λειτουργιών γίνεται πάνω σε έξυπνες κάρτες (smart cards) με κρυπτογραφικές δυνατότητες.

Συγκεκριμένα, στο κεφάλαιο 2 αναλύονται οι υπηρεσίες ασφαλείας που απαιτούνται σε ένα δίκτυο τηλεματικών υπηρεσιών στην υγεία. Η υλοποίηση των υπηρεσιών ασφαλείας γίνεται με τη χρήση κρυπτογραφικών μεθόδων, ψηφιακών υπογραφών και ψηφιακών πιστοποιητικών. Εισαγωγή στην κρυπτογραφία γίνεται στο κεφάλαιο 3, ενώ στο κεφάλαιο 4 γίνεται εισαγωγή στην Υποδομή Δημοσίου Κλειδιού PKI (Public Key Infrastructure). Στο κεφάλαιο 5 γίνεται εισαγωγή και ανάλυση των Ψηφιακών Πιστοποιητικών. Για μεγαλύτερη ασφάλεια τα ιδιωτικά (κρυφά) κρυπτογραφικά κλειδιά αποθηκεύονται σε έξυπνες κρυπτογραφικές κάρτες. Οι κάρτες αυτές δίνουν την δυνατότητα εκτέλεσης των κρυπτογραφικών μεθόδων πάνω στις κάρτες και έτσι παρέχεται μέγιστη ασφάλεια επειδή τα ιδιωτικά κλειδιά δεν εγκαταλείπουν ποτέ το ασφαλές περιβάλλον της κάρτας. Τα ψηφιακά πιστοποιητικά δημόσιων κλειδιών γίνονται δημόσια διαθέσιμα με τη χρήση Καταλόγων X.500 (directories). Στο κεφάλαιο 6 γίνεται εισαγωγή και ανάλυση των Καταλόγων X.500 και στο κεφάλαιο 7 στην τεχνολογία των έξυπνων καρτών. Στο κεφαλαίο 8 παρουσιάζονται και αναλύονται οι Υπηρεσίες Πιστοποίησης για δίκτυο τηλεματικών υπηρεσιών στην υγεία που βασίζονται στην Υποδομή Δημοσίου Κλειδιού. Στο κεφάλαιο 9 παρουσιάζεται το μοντέλο ισχυρής εξακρίβωσης που σχεδιάστηκε και υλοποιήθηκε. Στο κεφάλαιο 10 παρουσιάζεται το τεχνολογικό πλαίσιο και οι μηχανισμοί δημιουργίας και επαλήθεύσης ηλεκτρονικών υπογραφών που σχεδιάστηκαν και υλοποιήθηκαν.

Κεφάλαιο 2

Υπηρεσίες ασφαλείας

Στο παγκόσμιο διαδίκτυο, η πληροφορία που στέλνουμε από ένα υπολογιστή σε ένα άλλο περνά από πολλούς ενδιάμεσους σταθμούς μέχρι να φτάσει στον τελικό προορισμό της. Λόγω της αρχιτεκτονικής του παγκόσμιου διαδίκτυου, απόρρητη και εμπιστευτική πληροφορία μπορεί να αποκαλυφθεί σε οντότητες, οι οποίες δεν είναι εξουσιοδοτημένες να την λάβουν. Επίσης είναι δυνατή η κακόβουλη παρεμπόδιση και η αντικατάσταση των δεδομένων κατά τη μετάδοση τους. Η κρυπτογραφία χρησιμοποιείται για την παροχή υπηρεσιών ασφαλείας (security services), που στοχεύουν στην προστασία των χρηστών και στην ασφαλή μετάδοση των πληροφοριών, με διασφάλιση του απορρήτου των δεδομένων.

2.1 Υπηρεσίες Ασφαλείας (Security services)

Οι κύριες υπηρεσίες ασφαλείας είναι οι εξής :

- Εξακρίβωση ταυτότητας (authentication)
- Ακεραιότητα δεδομένων (data integrity)
- Μη άρνηση πράξης (non-repudiation)
- Απόρρητο των δεδομένων (data confidentiality)

2.2 Εξακρίβωση ταυτότητας (Authentication)

Η υπηρεσία εξακρίβωσης ταυτότητας (Authentication service) παρέχει εγγύηση για την ταυτότητα μιας οντότητας. Αυτό σημαίνει ότι όταν ισχυρίζεται κάποιος ότι έχει μια συγκεκριμένη ταυτότητα (ή ένα συγκεκριμένο user name), η υπηρεσία εξακρίβωσης ταυτότητας θα παρέχει τα μέσα για να επιβεβαιώσει την ορθότητα αυτού του ισχυρισμού.

Υπάρχουν δύο είδη εξακρίβωσης ταυτότητας, ανάλογα με το αν εξακριβώνουμε την ταυτότητας οντότητας ή την ταυτότητα προέλευσης δεδομένων. Αυτά είναι τα εξής :

- Εξακρίβωση ταυτότητας χρήστη (user authentication)
- Εξακρίβωση ταυτότητας προέλευσης δεδομένων (data origin authentication)

2.2.1 Εξακρίβωση ταυτότητας χρήστη (User authentication)

Η εξακρίβωση ταυτότητας ενός χρήστη γίνεται συνήθως :

- Με κάτι που γνωρίζει (για παράδειγμα ένα κωδικό πρόσβασης)
- Με κάτι που έχει στην κατοχή του (π.χ. μια έξυπνη κάρτα)
- Με συνδυασμό και των δύο παραπάνω (π.χ. ο χρήστης να έχει μια έξυπνη κάρτα και να γνωρίζει το PIN (Personal Identification Number) για να μπορεί να κάνει χρήση της κάρτας)

Η τελευταία περίπτωση είναι αυτή που μας προσφέρει τη μεγαλύτερη ασφάλεια.

Χρησιμοποιείται ευρέως η τεχνική πρόκλησης/απόκρισης (challenge-response) για την εξακρίβωση της ταυτότητας του χρήστη. Το σύστημα σε αυτή την περίπτωση στέλνει στο χρήστη ένα τυχαίο αριθμό (challenge), ο χρήστης το μετατρέπει χρησιμοποιώντας την μυστική πληροφορία που κατέχει για να πιστοποιεί την ταυτότητα του, και το αποτέλεσμα το στέλνει σαν απάντηση (response) πίσω στο σύστημα.

Με χρήση της ασυμμετρικής κρυπτογραφίας η επιβεβαίωση της ταυτότητας του χρήστη γίνεται χωρίς να χρειάζεται το σύστημα να γνωρίζει το μυστικό των χρηστών, δηλαδή το ιδιωτικό τους κλειδί, αλλά αρκεί για να γίνει η εξακρίβωση της ταυτότητας με τη γνώση του δημόσιου κλειδιού. Για παράδειγμα το σύστημα στέλνει ένα τυχαίο challenge στο χρήστη, ο οποίος με χρήση έξυπνης κρυπτογραφικής κάρτας το

κρυπτογραφεί με το ιδιωτικό του κλειδί, και το στέλνει πίσω στο σύστημα ως response. Το σύστημα κάνει πιστοποίηση ταυτότητας αποκρυπτογραφώντας το response με το δημόσιο κλειδί του υποτιθέμενου χρήστη, και συγκρίνοντας το αποτέλεσμα της αποκρυπτογράφησης με το αρχικό challenge. Αν το αρχικό challenge και το αποτέλεσμα της αποκρυπτογράφησης είναι ίδια, τότε έχει γίνει επιτυχώς η πιστοποίηση ταυτότητας του χρήστη.

2.2.2 Εξακρίβωση της ταυτότητας προέλευσης δεδομένων (Data origin authentication)

Πρέπει να εξακριβώσουμε ο αποστολέας των δεδομένων είναι αυθεντικός. Με τη χρήση της κρυπτογραφίας μπορούμε να εξακριβώσουμε αν κάποιος έχει εμποδίσει το μήνυμα του αυθεντικού αποστολέα, και το έχει αντικαταστήσει με ένα πλαστό μήνυμα.

2.3 Ακεραιότητα δεδομένων (Data integrity)

Η υπηρεσία ακεραιότητας δεδομένων (data integrity service) πρέπει να προστατεύσει τα δεδομένα από την αλλαγή, διαγραφή ή αντικατάσταση τους χωρίς εξουσιοδότηση. Η ακεραιότητα δεδομένων από μόνη της δεν έχει νόημα, γιατί δεν αρκεί η πληροφορία να μην μεταβάλλεται κατά την μεταφορά της, αλλά πρέπει ταυτόχρονα και η πηγή προέλευσης της να είναι αυθεντική. Για αυτό το λόγο η υπηρεσία ακεραιότητας των δεδομένων πρέπει να συνδυάζεται με την εξακρίβωση ταυτότητας της πηγής προέλευσης των δεδομένων.

2.4 Μη άρνηση πράξης (Non-repudiation)

Η μη άρνηση πράξης (non-repudiation) προστατεύει από την άρνηση μιας οντότητας που έλαβε μέρος σε μια επικοινωνία (communication), να παραδεχτεί ότι έχει λάβει μέρος σε αυτήν. Η μη άρνηση πράξης μαζί με τον έλεγχο της προέλευσης των δεδομένων προστατεύει από τις προσπάθειες του αποστολέα να αρνηθεί ότι έστειλε το μήνυμα, ενώ μαζί με την έλεγχο παράδοσης προστατεύει από προσπάθειες του παραλήπτη να αρνηθεί, ψευδώς, την παραλαβή του μηνύματος.

Μπορούμε να έχουμε μη άρνηση πράξης με τη χρήση των ψηφιακών υπογραφών.

2.5 Απόρρητο των δεδομένων (Data confidentiality)

Το απόρρητο των δεδομένων προστατεύει από το να αποκαλυφθεί πληροφορία σε οντότητες, οι οποίες δεν είναι εξουσιοδοτημένες να λάβουν αυτήν την πληροφορία. Αν δεν υπάρχει απόρρητο των δεδομένων παραβιάζεται το δικαίωμα των ατόμων και των εταιριών για μυστικότητα. Το απόρρητο των δεδομένων είναι πολύ σημαντικό για τον ιατρικό κόσμο και τον τραπεζικό τομέα.

Για την παροχή του απορρήτου των δεδομένων είναι απαραίτητη η κρυπτογράφηση των μηνυμάτων

Κεφάλαιο 3

Κρυπτογραφία

Οι κρυπτογραφικές τεχνικές, όπως η κρυπτογράφηση και οι ψηφιακές υπογραφές, είναι οι δομικοί λίθοι στην υλοποίηση των υπηρεσιών ασφαλείας. Σε αυτό το κεφάλαιο παρουσιάζουμε τις κύριες κρυπτογραφικές τεχνικές που χρησιμοποιούνται για τις υπηρεσίες ασφαλείας.

3.1 Κρυπτογράφηση και Αποκρυπτογράφηση

Το βασικότερο μέρος της κρυπτογραφίας είναι το κρυπτογραφικό σύστημα (cryptosystem). Το κρυπτογραφικό σύστημα ορίζει ένα ζεύγος από μετασχηματισμούς δεδομένων. Ο πρώτος μετασχηματισμός, που ονομάζεται κρυπτογράφηση (encryption), χρησιμοποιείται για να μετασχηματίσει απλό κείμενο (plaintext) σε ένα format, το οποίο δεν μπορεί να διαβαστεί, και το ονομάζουμε κρυπτογραφημένο κείμενο (ciphertext). Εφαρμόζοντας το δεύτερο μετασχηματισμό, ο οποίος ονομάζεται αποκρυπτογράφηση (decryption) στο κρυπτογραφημένο κείμενο, παίρνουμε ως αποτέλεσμα το αρχικό απλό κείμενο.

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 bitvector). 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.

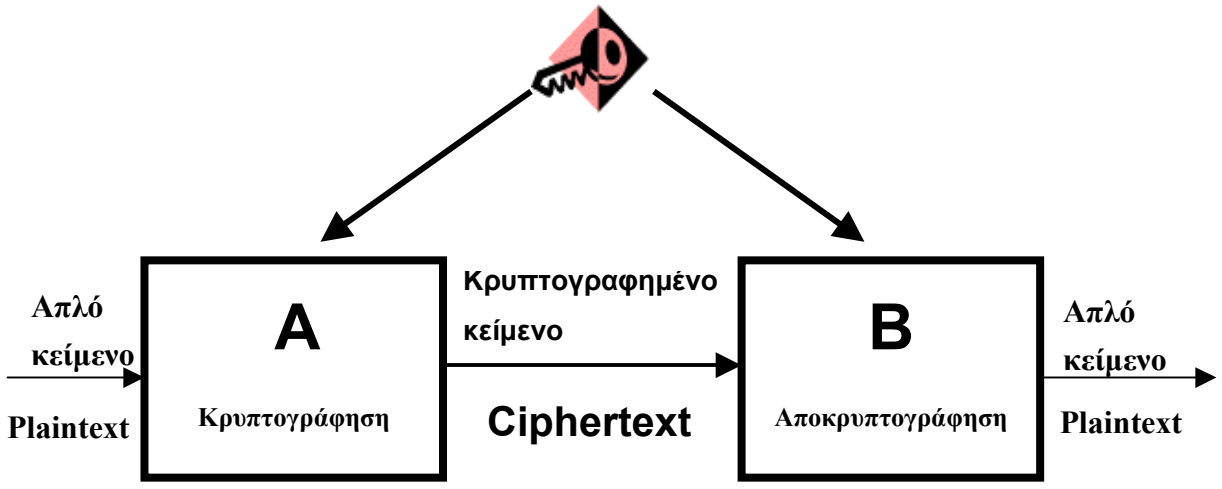
Το κρυπτογραφικό σύστημα παρέχει διασφάλιση του απόρρητου των πληροφοριών (confidentiality) που στέλνονται μεταξύ των συναλλασσόμενων μερών. Έτσι, αν βρεθούν στα "χέρια" τρίτων, θα τους είναι άχρηστες, μια και δεν θα μπορούν να αντιληφθούν το περιεχόμενο τους, αφού δεν θα γνωρίζουν το κλειδί αποκρυπτογράφησης.

Υπάρχουν δύο βασικά είδη κρυπτογράφησης. Η συμμετρική και η ασυμμετρική (ή κρυπτογράφηση με δημόσιο κλειδί / public-key cryptography).

3.2 Συμμετρική κρυπτογραφία (Symmetric cryptography)

Στη συμμετρική κρυπτογραφία, το κλειδί κρυπτογράφησης είναι το ίδιο με το κλειδί αποκρυπτογράφησης. Για να διασφαλιστεί το απόρρητο των πληροφοριών (confidentiality) που στέλνονται μεταξύ των συναλλασσόμενων μερών, το συμμετρικό σύστημα δουλεύει 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.



Σχήμα 3.2. Ένα συμμετρικό κρυπτογραφικό σύστημα

Ο πιο γνωστός αλγόριθμος για συμμετρική κρυπτογράφηση είναι ο DES [FIPS 46-2] (Data Encryption Standard), που υιοθετήθηκε το 1977 από το Αμερικανικό NBS (National Bureau of Standards) ως FIPS 46.

Ο DES είναι αλγόριθμος κρυπτογράφησης μπλοκ, με μέγεθος μπλοκ 64 ψηφίων (64 bits). Ο DES χρησιμοποιεί κλειδί 56 ψηφίων (56-bit), το οποίο δυστυχώς είναι μικρού μήκους. Έχει υπολογιστεί ότι για να γίνει διεξοδική αναζήτηση όλων των πιθανών τιμών του κλειδιού σε μία μέρα απαιτείται μια επένδυση US$200,000. Για να γίνει η παραπάνω διαδικασία είναι αρκετός μόνο μικρός αριθμός απλών κειμένων με το αντίστοιχο κρυπτογραφημένο κείμενο. 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.

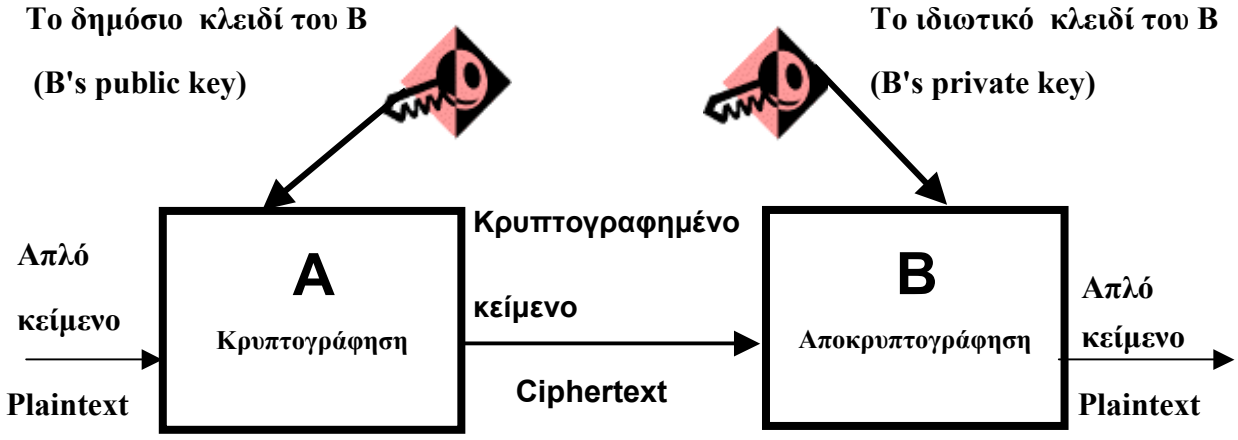
Μεγαλύτερη ασφάλεια μπορεί να επιτευχθεί με τη χρήση του triple-DES. Με τον triple-DES χρησιμοποιούμε αποτελεσματικά κλειδί 112 ψηφίων (112 bits), το οποίο είναι επαρκώς μεγάλο. Ο triple-DES βασίζεται στη χρησιμοποίηση του DES τρεις φορές [kaliski94].

Δεν είναι αρκετό να διαλέξουμε ένα ασφαλή αλγόριθμο κρυπτογράφησης, αν δεν προσδιορίσουμε μία ασφαλή μέθοδο εφαρμογής. Ανάλογα με το είδος του καναλιού επικοινωνίας ή του χώρου αποθήκευσης, πρέπει να επιλέξουμε μεταξύ των μεταξύ του CIPHER-Block-Chaining (CBC), του Cipher-Feedback (CFB), και του Output-Feedback (OFB) (όπως έχει προσδιοριστεί από το FIPS 81). Η κρυπτογράφηση κατά μπλοκ (ή Electronic Code Book (ECB) mode) χρησιμοποιείται μόνο για την κρυπτογράφηση κλειδιών.

3.3 Ασυμμετρική κρυπτογραφία (Public-key cryptography)

Η ασυμμετρική κρυπτογραφία ή αλλιώς κρυπτογραφία δημόσιου κλειδιού (public-key cryptography), είναι η πιο πρόσφατη μέθοδος κρυπτογραφίας. Αντίθετα με τα συμμετρικά συστήματα το κλειδί που χρησιμοποιείται για την κρυπτογράφηση είναι διαφορετικό από αυτό που χρησιμοποιείται για την αποκρυπτογράφηση. Κάθε άτομο έχει ένα ζεύγος μοναδικών κλειδιών. Ένα μήνυμα που κρυπτογραφήθηκε με ένα από αυτά τα κλειδιά μπορεί να αποκρυπτογραφηθεί μόνο το άλλο κλειδί του ίδιου ζεύγους.

Το ένα κλειδί του ζεύγους, το οποίο ονομάζεται ιδιωτικό κλειδί (private key) διατηρείται κρυφό, ενώ το άλλο το δημόσιο κλειδί (public key) πρέπει να είναι διαθέσιμο στους άλλους χρήστες, για να χρησιμοποιείται για την κρυπτογράφηση της πληροφορίας που στέλνεται στον κάτοχο του κλειδιού. 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. Πρέπει να τονίσουμε ότι το ασυμμετρικό σύστημα έχει την ιδιότητα, ότι δομένου του δημόσιου κλειδιού δεν είναι δυνατόν να βρεθεί το αντίστοιχο ιδιωτικό κλειδί.



Σχήμα 3.3. Ένα ασυμμετρικό κρυπτογραφικό σύστημα

Οι ασυμμετρικές μέθοδοι είναι σημαντικές γιατί μπορούν να χρησιμοποιηθούν για τη μεταβίβαση κλειδιών κρυπτογράφησης ή άλλων δεδομένων χωρίς να χρειάζεται οι συναλλασσόμενοι να συμφωνήσουν εκ των προτέρων για ένα κοινό μυστικό κλειδί. Όλες οι γνωστές μέθοδοι ασυμμετρικής κρυπτογράφησης είναι αρκετά αργές, και χρησιμοποιούνται συνήθως μόνο για να κρυπτογραφήσουν κλειδιά που χρησιμοποιούνται μόνο για μία επικοινωνία (session keys), με τα οποία κατόπιν κρυπτογραφείται μεγάλος όγκος δεδομένων χρησιμοποιώντας συμμετρική κρυπτογράφηση.

Ο RSA (Rivest-Shamir-Adelman) [PKCS#1] είναι ο πιο σημαντικός και ευρέως διαδεδομένος αλγόριθμός για ασυμμετρική κρυπτογράφηση. Χρησιμοποιείται εκτός από

την κρυπτογράφηση και για ηλεκτρονική 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.

Η κρυπτογράφηση με τον αλγόριθμο RSA προσδιορίζεται στο PKCS-1 [PKCS#1], το οποίο είναι μέρος της ομάδας των standards για την ασυμμετρική κρυπτογραφία.

3.4 Σύγκριση συμμετρικής και ασυμμετρικής κρυπτογράφησης

Τα πλεονεκτήματα των ασυμμετρικών συστημάτων κρυπτογράφησης είναι τα εξής:

- Δεν είναι απαραίτητη η ανταλλαγή και η γνώση ενός κοινού (κρυφού) κλειδιού από τον αποστολέα και τον παραλήπτη όπως στα συμμετρικά συστήματα. Άρα είναι δυνατή η αυθόρμητη επικοινωνία με οποιοδήποτε άλλον χρησιμοποιώντας ένα πιστοποιητικό (κεφάλαιο 5) για την εύρεση και πιστοποίηση δημόσιου κλειδιού που ανήκει στο άτομο με το οποίο θέλουμε να επικοινωνήσουμε.

- 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 το τετράγωνο του αριθμού των χρηστών.

- Δεν υπάρχει πρόβλημα στην προσθήκη νέων μελών όπως υπάρχει στη συμμετρική κρυπτογράφηση, που κάθε χρήστης πρέπει να ανταλλάξει ένα κρυφό κλειδί με κάθε νέο χρήστη.

- Οι ασυμμετρικές μέθοδοι προσφέρονται για τη δημιουργία ηλεκτρονικών 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.

Τα μειονεκτήματα των ασυμμετρικών συστημάτων κρυπτογράφησης είναι:

- Μέχρι τώρα δεν υπάρχει ασυμμετρικό σύστημα κρυπτογράφησης που να είναι ασφαλές και ταυτόχρονα τόσο γρήγορο όσο τα συμμετρικά.

- Είναι απαραίτητη η διαχείριση των δημόσιων κλειδιών στα ασυμμετρικά συστήματα. 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 της Αρχής Πιστοποίησης η οποία τα δημοσιοποιεί σε ένα κατάλογο (directory).

Επειδή οι ασυμμετρικές μέθοδοι που είναι γνωστοί σήμερα είναι πιο αργοί 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.

3.5 Αλγόριθμοι σύνοψης μηνύματος (message digest algorithms)

Μια συνάρτηση κατακερματισμού (hash function) είναι μια αριθμητική συνάρτηση που μετατρέπει είσοδο οποιουδήποτε μήκους σε έξοδο σταθερού μήκους, που ονομάζεται τιμή κατακερματισμού (hash value). Όταν υπογράφουμε ηλεκτρονικά ένα μήνυμα, χρησιμοποιούμε την συνάρτηση κατακερματισμού για να παράγουμε την τιμή κατακερματισμού του μηνύματος. Η τιμή κατακερματισμού είναι ένα αλφαριθμητικό σταθερού μήκους, που δεν εξαρτάται από το μήκος του μηνύματος και είναι μικρότερο από αυτό.

Η τιμή κατακερματισμού ονομάζεται και σύνοψη μηνύματος (message digest). Επειδή η συνάρτηση κατακερματισμού παράγει την σύνοψη ενός μηνύματος, οι συναρτήσεις αυτές ονομάζονται και αλγόριθμοι σύνοψης μηνύματος (message digest algorithms).

Ο σκοπός ενός αλγόριθμου σύνοψης μηνύματος είναι να παράγει μια αναπαράσταση του μηνύματος, που να είναι μικρότερη από αυτό και να κρυπτογραφείται γρηγορότερα.

Οι αλγόριθμοι σύνοψης μηνύματος πρέπει να είναι μονόδρομες συναρτήσεις (one-way functions). Αυτό σημαίνει ότι η συνάρτηση πρέπει να μπορεί 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 το γεγονός, ότι άτομα που έχουν πρόσβαση στην σύνοψη του μηνύματος είναι δύσκολο να ανακαλύψουν το μήνυμα από την σύνοψη του.

Οι αλγόριθμοι σύνοψης μηνύματος πρέπει επίσης να παράγουν μοναδική τιμή κατακερματισμού για κάθε μήνυμα. Δηλαδή πρέπει να είναι σχεδόν αδύνατο να βρεθούν δυο διαφορετικά μηνύματα με λογικό νόημα που να έχουν την ίδια σύνοψη μηνύματος. Με αυτές τις προϋποθέσεις εξασφαλίζουμε ότι κανένας δεν θα μπορεί να αντικαταστήσει το μεταδιδόμενο μήνυμα με ένα άλλο μήνυμα της εκλογής που να έχει την ίδια σύνοψη.

Δύο παραδείγματα αλγορίθμων σύνοψης μηνύματος είναι :

- MD5 (Message Digest Algorithm 5) που αναπτύχθηκε από τα RSA Laboratories. Ο MD5 παράγει σύνοψη μηνύματος μήκους 128 ψηφίων (128 bits). Το περισσότερο λογισμικό που διαχειρίζεται πιστοποιητικά υποστηρίζει μόνο τον MD5 [MD5].

- Ο SHA-1 (secure hash Algorithm), ένας αλγόριθμος σύνοψης μηνύματος που αναπτύχθηκε από το NIST (National Institute of Standards and Technology) και το NSA (National Security Agency). Ο SHA-1 παράγει σύνοψη μηνύματος μήκους 160-bit. Είναι πιο αργός από τον MD5, αλλά το μήκος της σύνοψης μηνύματος που παράγει είναι μεγαλύτερο, πράγμα που τον κάνει πιο ανθεκτικό σε επιθέσεις που διαλέγουν μηνύματα τυχαία, προσπαθώντας να παράγουν την ίδια σύνοψη μηνύματος [FIPS 180-1].

3.6 Ψηφιακές υπογραφές (Digital signatures)

Η ψηφιακή υπογραφή μας δίδει τη δυνατότητα να επιβεβαιώνουμε ότι :

- Ένα συγκεκριμένο άτομο έστειλε ένα μήνυμα. Δηλαδή ότι το μήνυμα το έστείλε ο "πραγματικός" αποστολέας και όχι κάποιος άλλος.

- Ότι το "αρχικό" μήνυμα που στάλθηκε από τον αποστολέα δεν το άλλαξε κάποιος άλλος κατά τη μετάδοση του πριν να φτάσει στον παραλήπτη.

Η παρακάτω διαδικασία εξηγεί συνοπτικά πως δημιουργείται και χρησιμοποιείται η ψηφιακή υπογραφή (βλ. Σχήμα 3.6.1):

1) Ο αποστολέας χρησιμοποιεί ένα αλγόριθμο σύνοψης μηνύματος (παρ. 3.5) για να δημιουργήσει μια μικρότερη έκδοση του μηνύματος, η οποία μπορεί να κρυπτογραφηθεί. Αυτή η συντομότερη έκδοση ονομάζεται σύνοψη του μηνύματος (message digest).

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

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

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

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

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

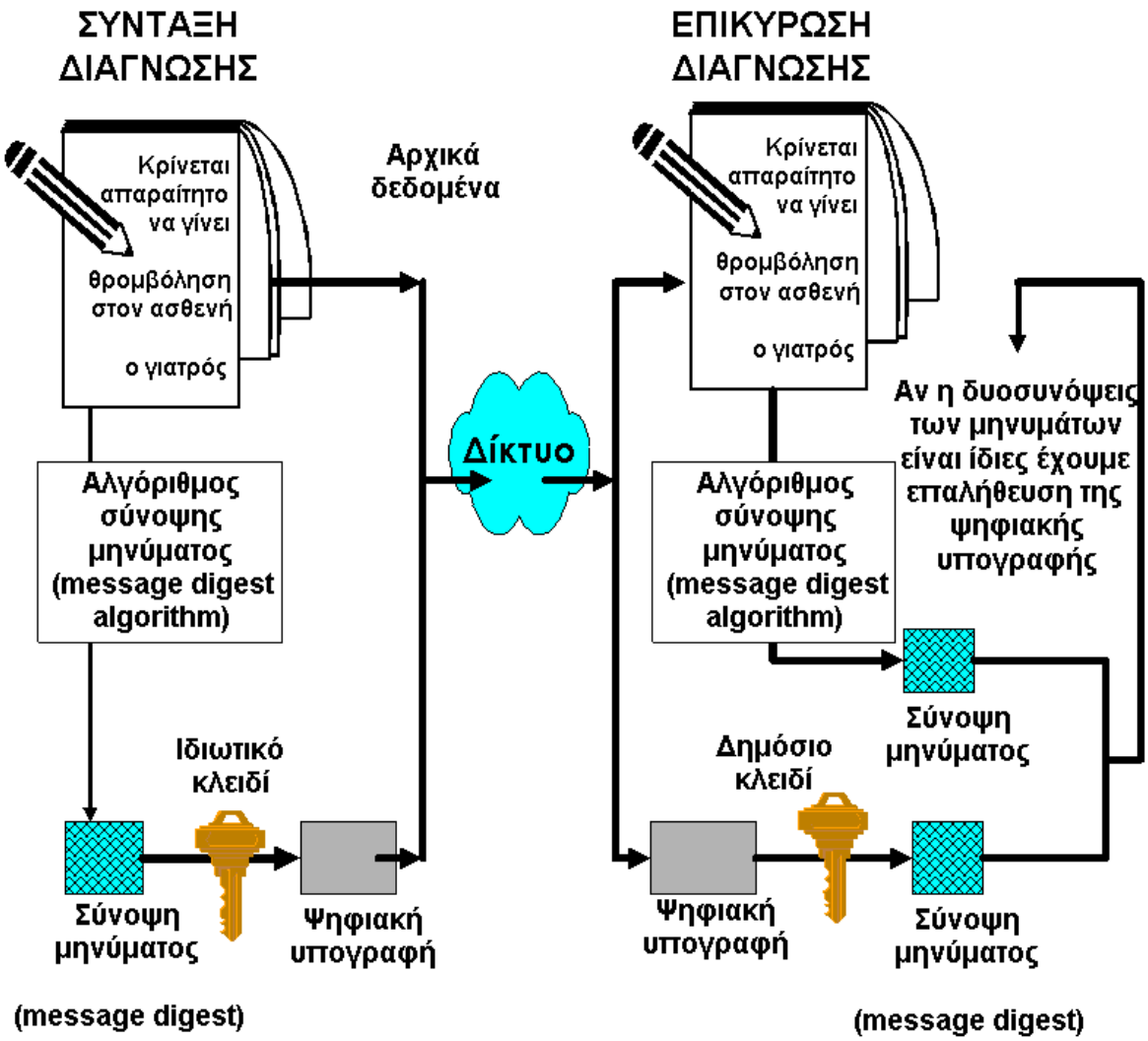
- Αν οι δύο συνόψεις είναι ίδιες, ο παραλήπτης ξέρει ότι το μήνυμα στάλθηκε πραγματικά από το πρόσωπο που ισχυρίζεται ότι είναι ο αποστολέας και ότι το μήνυμα δεν αλλάχθηκε κατά την μετάδοση του.

- 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.

Η κρυπτογραφημένη σύνοψη του μηνύματος χρησιμεύει σαν ψηφιακή υπογραφή για το μήνυμα. Η υπογραφή επαληθεύει την ταυτότητα του αποστολέα και τα περιεχόμενα του μηνύματος.

Η διαδικασία για την κατασκευή των ψηφιακών υπογραφών προσδιορίζεται στο PKCS-1 [PKCS#1], που είναι μέρος των προτύπων των RSA Laboratories' για την κρυπτογραφία.

Στο Κεφάλαιο 10, παρουσιάζεται και αναλύεται σε βάθος το θέμα των ψηφιακών υπογραφών.



Σχήμα 3.6.1. Παράδειγμα κατασκευής και επικύρωσης ψηφιακής υπογραφής στην περίπτωση παροχής τηλεσυμβούλευσης στην καρδιολογία

Κεφάλαιο 4

Υποδομή Δημοσίου Κλειδιού (PKI)

Η Υποδομή Δημοσίου Κλειδιού PKI (Public Key Infrastructure) [PKI], χρησιμοποιείται για να μπορέσουν δύο άτομα που δεν γνωρίζονται να ανταλλάξουν ευαίσθητη πληροφορία και χρηματικές μονάδες πάνω από ένα ανασφαλές δίκτυο όπως είναι το Internet. Οι Αρχές Πιστοποίησης ελέγχουν την Υποδομή Ασφαλείας που χρησιμοποιεί Ασύμμετρη Κρυπτογραφία δηλαδή δημοσία και ιδιωτικά κλειδιά. Η Υποδομή Δημοσίου Κλειδιού PKI είναι το συνολικό σύστημα το οποίο αποτελείται από:

- Αρχές Πιστοποίησης (CAs), οι οποίες ελέγχουν και διαχειρίζονται την Υποδομή Δημοσίου Κλειδιού PKI, εκδίδουν πιστοποιητικά δημοσίων κλειδίων, και επιβάλλουν πολιτικές στην περιοχή τους (domain).
- Αρχές εγγραφής (RAs), που ενεργούν εκ μέρους των Αρχών Πιστοποίησης (CAs) για να δηλώνουν εγγραφόμενους στην περιοχή που διαχειρίζεται η Αρχή Πιστοποίησης.
- Συστήματα διαχείρισης πιστοποιητικών (Certificate management systems/CMS) για τη διαχείριση των πιστοποιητικών καθ' όλη τη διάρκεια ισχύς τους. Η Αρχή Πιστοποίησης χρησιμοποιεί και ελέγχει το σύστημα διαχείρισης πιστοποιητικών (CMS).
- Καταλόγους X.500 (directories), που είναι χώροι αποθήκευσης των πιστοποιητικών δημοσίων κλειδιών κρυπτογράφησης όπως επίσης και δημόσιας πληροφορίας για τους κατόχους των πιστοποιητικών.

Η Υποδομή Δημοσίου Κλειδιού είναι ένα δίκτυο όπου υπάρχουν σχέσεις εμπιστοσύνης. Οι εγγραφόμενοι δημιουργούν σχέση εμπιστοσύνης (trust relationship) με την Αρχή Πιστοποίησης. Οι Αρχές Πιστοποίησης 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 (verified) είναι αρκετό για να δημιουργηθεί σχέση εμπιστοσύνης μεταξύ των δύο αυτών πλευρών.

Η Υποδομή Συστήματος Ασφαλείας χρήση Δημοσίων Κλειδιών (PKI) με κατάλληλη ασφάλεια, διαχείριση και τεχνολογία μπορεί να χρησιμοποιηθεί για να επιβάλλει πολιτικές για την ίδια πληροφορία και για τον έλεγχο ροής της πληροφορίας. Χρησιμοποιείται ακόμη για την αναγνώριση πιθανών απειλών για την ασφάλεια και επίσης παρέχει υπηρεσίες ψηφιακής χρόνο-σφραγίδας (digital timestamping services). Μπορεί επίσης να χρησιμεύσει για την ασφαλή αποθήκευση της πληροφορίας.

Το Υποδομή Δημοσίου Κλειδιού είναι απαραίτητη για να δημιουργήσει ένα αξιόπιστο περιβάλλον για συναλλαγές ηλεκτρονικού εμπορίου και ασφαλείς επικοινωνίες τόσο για τα άτομα όσο και για τους οργανισμούς.

Καθώς όλο και περισσότερες επιχειρήσεις παγκοσμίως αντιλαμβάνονται τις δυνατότητες που τους παρέχει το Internet και αρχίζουν να επεκτείνονται 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 (e-mail address), είναι το κύριο εμπόδιο στη χρήση των ψηφιακών δικτύων για τις επιχειρήσεις. Για να ξεπεραστούν αυτά τα προβλήτα αξιοπιστίας χρησιμοποιείται η Υποδομή Δημοσίου Κλειδιού.

Πολλοί οργανισμοί χρειάζονται καθολικές λύσεις όσον αφορά την Υποδομή Δημοσίου Κλειδιού οι οποίες βασίζονται σε ανοιχτά συστήματα (open standards) για να τους παρέχουν ένα ευρύ φάσμα από ασφαλείς δικτυακές εφαρμογές.

Κεφάλαιο 5

Πιστοποιητικά

Τα δημόσια κλειδιά (public keys) μας δίνουν τη δυνατότητα να πιστοποιήσουμε την ταυτότητα ενός χρήστη (authenticate user). Πρέπει όμως να υπάρχει η εγγύηση ότι το δημόσιο κλειδί που κατέχουμε είναι αυθεντικό και ανήκει στον χρήστη που θέλουμε.

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. Αυτό το πιστοποιητικό μπορεί ταυτόχρονα να χρησιμεύσει σαν πιστοποίηση επιβεβαίωσης της ταυτότητας του χρήστη.

5.1 Τι είναι το πιστοποιητικό (certificate) ;

Ένα πιστοποιητικό (certificate) [ISO 9594-8] είναι ένα ψηφιακό κείμενο που εγγυάται για την ταυτότητα ενός ατόμου, ενός υπολογιστικού συστήματος ή μίας επιχείρησης. Το πιστοποιητικό συνδέει την ταυτότητα του κατόχου του με ένα συγκεκριμένο δημόσιο κλειδί. Αυτό το δημόσιο κλειδί αντιστοιχεί στο ιδιωτικό κλειδί το οποίο ο κάτοχος του χρησιμοποιεί για να κρυπτογραφεί ή για να υπογράφει ηλεκτρονικά. 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.

5.2 Αρχή Πιστοποίησης (CA/Certification Authority)

Τα πιστοποιητικά εκδίδονται από Αρχές Πιστοποίησης (CAs/Certification Authoroties) [ISO 9594-8]. Τις Αρχές Πιστοποίησης θα τις αποκαλούμε συντομευμένα CAs από εδώ και στο εξής. Αυτές οι αρχές είναι υπεύθυνες για να ελέγξουν την

ταυτότητα μιας οντότητας και το γεγονός ότι κατέχει ένα ζεύγος κλειδιών, το ιδιωτικό κλειδί και το αντίστοιχο δημόσιο, πριν εκδώσουν το αντίστοιχο πιστοποιητικό.

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

Αρχή πιστοποιητικών μπορεί να είναι κάθε έμπιστη κεντρική διοίκηση που προτίθεται να εγγυηθεί για τις ταυτότητες των ατόμων στα όποια έχει δώσει πιστοποιητικό. Αυτό το κεντρικό διοικητικό σώμα μπορεί να είναι μια εταιρία που εκδίδει πιστοποιητικά στους εργαζόμενους 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.

5.3 Βασικές λειτουργίες της Αρχής Πιστοποίησης

Οι συστάσεις για τη δομή των Αρχών Πιστοποίησης προσδιορίζουν ένα σύνολο από λειτουργίες, το οποίο υποστηρίζει τη διαδικασία πιστοποίησης. Οι βασικές, τυπικές λειτουργίες είναι:

5.3.1 Ηλεκτρονική Εγγραφή (Electronic Registration)

Κάθε χρήστης ο οποίος επιθυμεί να επικοινωνήσει με μια οντότητα σε μία συγκεκριμένη δικτυακή ομάδα πρέπει να εγγραφεί στην κατάλληλη Αρχή Πιστοποίησης. Πρακτικά, το πρώτο βήμα της διαδικασίας ηλεκτρονικής εγγραφής περιλαμβάνει την προώθηση της αίτησης εγγραφής στην Αρχή Πιστοποίησης. Έπειτα η Αρχή Πιστοποίησης απαντά ορίζοντας ποια πληροφορία της είναι απαραίτητη. Όταν λάβει την απαραίτητη πληροφορία, ελέγχει την ταυτότητα του χρήστη επιβεβαιώνει τα στοιχεία του, τα καταχωρεί και προωθεί την αίτηση για πιστοποιητικό.

5.3.2 Ονομασία (Naming)

Για να παρέχει κάποιος ουσιαστικές υπηρεσίες πιστοποίησης, κάθε οντότητα μέσα στην περιοχή (domain) πρέπει να είναι μοναδικά αναγνωρίσιμη από ένα όνομα. Εάν υπάρχουν πολλοί συμμετέχοντες, η χρήση απλά κάποιου ονόματος δεν είναι αρκετή, και είναι απαραίτητη μια υπηρεσία η οποία θα εγγυάται σαφή ονόματα ή ψευδώνυμα (aliases).

5.3.3 Δημιουργία και διανομή κλειδιών (Key generation and Distribution)

Η Αρχή Πιστοποίησης δημιουργεί ένα ζεύγος από ένα δημόσιο κλειδί και ένα ιδιωτικό κλειδί και επικοινωνεί με τον αιτών πάνω από ένα ασφαλές δίκτυο για να του τα γνωστοποιήσει. Ιδιαίτερα το ιδιωτικό κλειδί πρέπει να μεταδίδεται στην αιτούσα οντότητα με ασφαλή τρόπο. Για παράδειγμα μπορούμε να το γράψουμε σε μια έξυπνη κάρτα, ή σε μια κάρτα PCMCIA, είτε αφού το κρυπτογραφήσουμε σε μια δισκέτα.

5.3.4 Διαχείριση Πιστοποιητικών

Η διαχείριση των πιστοποιητικών περιλαμβάνει τα εξής:

- *Δημιουργία Πιστοποιητικών*
- *Διανομή, αποθήκευση και επανάκτηση πιστοποιητικών*

5.3.4.1 Δημιουργία Πιστοποιητικών (Certificate Generation)

Μία από τις βασικές υπηρεσίες που παρέχονται από τις Αρχές Πιστοποίησης είναι η δημιουργία των πιστοποιητικών. Με τη δημιουργία του πιστοποιητικού γίνεται η σύνδεση της ταυτότητας του αιτούντος με το δημόσιο κλειδί του. Τα πιστοποιητικά υπογράφονται από την Αρχή Πιστοποίησης με το ιδιωτικό της κλειδί. Αυτή η υπογραφή δείχνει ότι η Αρχή Πιστοποίησης εγγυάται για την αυθεντικότητα της πληροφορίας που περιέχει το πιστοποιητικό.

Τα πιστοποιητικά συνήθως περιέχουν το αναγνωριστικό (identifier) της οντότητας, το νούμερο της έκδοσης του πιστοποιητικού (version number), το δημόσιο κλειδί της οντότητας και τη διάρκεια ισχύος του πιστοποιητικού (lifetime). Το X.509 [X.509] είναι χρήσιμο για τη δομή (format) των δεδομένων του πιστοποιητικού.

5.3.4.2 Διανομή, αποθήκευση και επανάκτηση πιστοποιητικών (Certificate Distribution Storage and Retrieval)

Οι Αρχές Πιστοποίησης πρέπει να παρέχουν ένα αντίγραφο του πιστοποιητικού στον κάτοχο του μόλις αυτό δημιουργηθεί. Επίσης είναι υπεύθυνες για να δημοσιοποιήσουν αντίτυπα των πιστοποιητικών που παράγουν στον κατάλληλο Κατάλογο (Directory Server) (Κεφάλαιο 6). Η Αρχή Πιστοποίησης θα πρέπει να αποθηκεύει και να μπορεί να επανακτήσει (revoke) τα πιστοποιητικά που έχει παράγει. Πρέπει να διατηρεί ένα εφεδρικό αντίγραφο (back-up) των πιστοποιητικών, σε περίπτωση που ο Κατάλογος παρουσιάσει βλάβη και χρειαστεί να επανακτήσει την πληροφορία που είχε, ή σε περίπτωση που χρειαστεί η ίδια η Αρχή Πιστοποίησης να επανακτήσει την πληροφορία λόγω δική της βλάβης.

5.3.5 Διαχείριση Λιστών Ανάκλησης Πιστοποιητικών (CRLs/Certificate Revocation Lists)

Οι Αρχές Πιστοποίησης πρέπει να παράγουν Λίστες Ανάκλησης Πιστοποιητικών οι οποίες δείχνουν ποια πιστοποιητικά δεν είναι έγκυρα πλέον. Ένα πιστοποιητικό ακυρώνεται όταν το κλειδί που πιστοποιεί είναι ανάγκη να αποσυρθεί πριν λήξει το πιστοποιητικό. Ένα δημόσιο κλειδί πρέπει να αποσυρθεί όταν πάψει να έχει νόημα χρήσης και ύπαρξης (όταν για παράδειγμα ο εργαζόμενος απολυθεί), ή όταν το αντίστοιχο ιδιωτικό κλειδί έχει εκτεθεί σε κινδύνους ή δεχθεί κρυπτό-αναλυτική επίθεση. Κάθε Αρχή Πιστοποίησης θα παράγει Λίστες Ακύρωσης για τα πιστοποιητικά που αυτή έχει δημιουργήσει.

Η διαχείριση Λιστών Ακύρωσης Πιστοποιητικών περιλαμβάνει:

- *Δημιουργία και συντήρηση Λίστας Ανάκλησης Πιστοποιητικών*
- *Διανομή, αποθήκευση και επανάκτηση της Λίστας Ανάκλησης Πιστοποιητικών*

5.3.5.1 Δημιουργία και συντήρηση Λίστας Ανάκλησης Πιστοποιητικών (CRL Generation and Maintenance)

Οι Λίστες Ανάκλησης Πιστοποιητικών όπως και τα πιστοποιητικά μέσα σε μια υποδομή (infrastructure) πρέπει να έχουν όλα την ίδια μορφή (format). Οι Λίστες Ανάκλησης Πιστοποιητικών περιέχουν πληροφορία όπως για παράδειγμα το αναγνωριστικό (identifier) της αρχής που τις έχει εκδώσει, τους σειριακούς αριθμούς των πιστοποιητικών που ακυρώνονται και την ημερομηνία που κάθε πιστοποιητικό

ακυρώθηκε. Η αυθεντικότητα και η ακεραιότητα της Λίστας Ανάκλησης Πιστοποιητικών είναι πολύ σημαντική για το σύστημα ασφαλείας. Για αυτό τον λόγο η Αρχή Πιστοποίησης πρέπει να υπογράφει τις Λίστες Ανάκλησης Πιστοποιητικών με το ιδιωτικό της κλειδί (όπως τα πιστοποιητικά). Η Αρχή Πιστοποίησης πρέπει επίσης να εξασφαλίσει ότι η πληροφορία που περιέχεται στη Λίστα Ανάκλησης Πιστοποιητικών είναι όσο πιο πρόσφατη γίνεται, κάνοντας περιοδική ενημέρωση των Λιστών Ανάκλησης Πιστοποιητικών για να προσθέτει σε αυτές νέα πληροφορία.

5.3.5.2 Διανομή, αποθήκευση και επανάκτηση της Λίστας Ανάκλησης Πιστοποιητικών (CRL Distribution Storage and Retrieval)

Οι χρήστες πρέπει να έχουν την πιο πρόσφατη πληροφορία για τα πιστοποιητικά, τα οποία δεν είναι πλέον έγκυρα. Για να ικανοποιήσει αυτή την ανάγκη, η Αρχή Πιστοποίησης θα πρέπει περιοδικά να δημοσιεύσει την Λίστα Ακύρωσης Πιστοποιητικών στον κατάλληλο Κατάλογο (Directory Server). Οι Αρχές Πιστοποίησης πρέπει να αποθηκεύουν και να μπορούν να επανακτήσουν τις Λίστες Ακύρωσης Πιστοποιητικών που έχουν οι ίδιες δημιουργήσει. Επίσης πρέπει να έχουν τη δυνατότητα να τις επανακτήσουν για να τις ενημερώσουν, να τις αντικαταστήσουν ή να τις διανείμουν.

5.3.6 Διαχείριση του Καταλόγου Πιστοποιητικών (Certificate Directory Management)

Η Αρχή Πιστοποίησης θα πρέπει να παρέχει Καταλόγους στο διαδίκτυο (on-line directories) οι οποίοι θα παρέχουν τα δημόσια κλειδιά και τα αντίστοιχα πιστοποιητικά, καθώς και τις Λίστες Ανάκλησης Πιστοποιητικών για δημόσια πρόσβαση. Για αυτό το σκοπό θα μπορούσαν να χρησιμοποιηθούν X.500 Directories (Κεφάλαιο 6). Αυτοί οι Κατάλογοι είναι πολύ χρήσιμοι στα μεγάλα δίκτυα και στα κατανεμημένα συστήματα.

5.3.7 Υπηρεσία για παροχή σφραγίδων ημερομηνίας και ώρας (Date and Time Stamping Services)

Σε μερικές εφαρμογές, σφραγίδες για την ώρα και την ημερομηνία πρέπει να επισυνάπτονται στο έγγραφο για να δείξουν πότε το έγγραφο στάλθηκε ή ελήφθη. Εάν το έγγραφο δημιουργήθηκε και στάλθηκε με ηλεκτρονικά μέσα, η σφραγίδα ημερομηνίας και ώρας πρέπει επίσης να παραχθεί και να προστεθεί στο κείμενο ηλεκτρονικά. Οι σφραγίδες αυτές χρησιμοποιούνται σαν εγγύηση ότι το έγγραφο είναι πρόσφατο.

5.4 Ιεραρχία εμπιστοσύνης

Όταν η κοινότητα των χρηστών μεγαλώνει, μία και μόνη Αρχή Πιστοποίησης (CA) θα υπερφορτωθεί γιατί θα έχει να διαχειριστεί ένα μεγάλο αριθμό πιστοποιητικών. Επιπροσθέτως, κάθε εταιρία από τον ιδιωτικό ή τον δημόσιο τομέα θέλει να ελέγχει τον τρόπο που οι χρήστες της δημιουργούν πιστοποιητικά, και την περίοδο ισχύος των πιστοποιητικών. Αυτό προκαλεί την ανάγκη για δημιουργία διαφόρων ειδών Αρχών Πιστοποίησης, κάθε μία από τις οποίες έχει διαφορετική πολιτική ασφάλειας. Για να επικοινωνήσουν οι οντότητες που εμπιστεύονται διαφορετικές Αρχές Πιστοποίησης, πρέπει να έχει οργανωθεί ένας τρόπος για να πιστοποιούνται μεταξύ τους οι Αρχές Πιστοποίησης κατά τέτοιο τρόπο ώστε να υπάρχει ένα αποδεκτό επίπεδο εμπιστοσύνης μεταξύ τους. Αυτό γίνεται με τη δημιουργία μιας ιεραρχίας εμπιστοσύνης που είναι στην ουσία μια ιεραρχία από Αρχές Πιστοποίησης. Κάθε Αρχή Πιστοποίησης πιστοποιείται από μια άλλη Αρχή Πιστοποίησης που βρίσκεται σε υψηλότερο επίπεδο, και με αυτό τον τρόπο έχουμε μία ιεραρχία εμπιστοσύνης. Κάθε πιστοποιητικό καθίσταται έγκυρο διασχίζοντας (traversing) την αλυσίδα υπογραφών (signature chain), και επιβεβαιώνοντας τα πιστοποιητικά μέχρι τη ρίζα (root). Το μονοπάτι αυτό που ακολουθείται για την επιβεβαίωση των πιστοποιητικών ονομάζεται μονοπάτι πιστοποίησης (certification path).

5.5 Διαχείριση Πιστοποιητικών (Certificate Management)

Οι βασικές λειτουργίες διαχείρισης κατά τον κύκλο ζωής ενός πιστοποιητικού είναι οι ακόλουθες:

- *Δημιουργία Πιστοποιητικών*
- *Διανομή Πιστοποιητικών*
- *Αποθήκευση και Ανάκτηση Πιστοποιητικών*
- *Ανάκληση Πιστοποιητικών*

5.5.1 Δημιουργία Πιστοποιητικών

Στη διαδικασία δημιουργίας πιστοποιητικών παρέχουμε ως είσοδο τα δεδομένα, τα οποία πρέπει να έχουν την κατάλληλη μορφή (format) που ορίζει η φόρμα δήλωσης (registration form), και παίρνουμε ως έξοδο ένα έγκυρο πιστοποιητικό.

Τον σημαντικότερο ρόλο στη Δημιουργία των πιστοποιητικών παίζει η μορφή του πιστοποιητικού (certificate format). Παρά το γεγονός ότι η διαδικασία αυτή είναι εντελώς αυτοματοποιημένη σε πολλά προϊόντα λογισμικού (π.χ. στο Netscape Certificate Server και στον Microsoft Certificate Server), δεν έχει ακόμη υιοθετηθεί ένα κοινό format για το ίδιο το πιστοποιητικό. Κατά τη διάρκεια της τελευταίας δεκαετίας, έχουν προταθεί πολλά διαφορετικά σχήματα για το σύστημα ασφαλείας PKI. Κάθε ένα από αυτά χρησιμοποιεί μια ειδική μορφή (format) για τα πιστοποιητικά. Θα αναφερθούμε αναλυτικά στις μορφές (format) των πιστοποιητικών στην παράγραφο 5.6.

5.5.2 Διανομή πιστοποιητικών

Για τη διαδικασία της διανομής των πιστοποιητικών παρέχουμε ως είσοδο ένα έγκυρο πιστοποιητικό και παίρνουμε ως έξοδο μια δυαδική τιμή που δείχνει αν το καινούργιο πιστοποιητικό που έχει παραχθεί έχει παραδοθεί επιτυχώς στον κάτοχο του ή όχι, και ένα αλφαριθμητικό (string) που επισημαίνει τους λόγους αποτυχίας.

Έχοντας παράγει το πιστοποιητικό, η Αρχή Πιστοποίησης είναι υπεύθυνη για να το παραδώσει στον κάτοχο του. Η διαδικασία Διανομής των Πιστοποιητικών περιλαμβάνει και τις ενέργειες που η Αρχή Πιστοποίησης πρέπει να κάνει, για να παραδώσει πληροφορία για το πιστοποιητικό:

- Στον κάτοχο του πιστοποιητικού
- Σε πολυπληθή κοινότητα οντοτήτων

Σε αυτήν την παράγραφο θα επικεντρώσουμε στον πρώτο τύπο οντότητας ενώ ο δεύτερος τύπος θα περιγραφεί στην παράγραφο που θα αναλύει την Αποθήκευση και την Ανάκληση Πιστοποιητικών.

Όπως είπαμε στη διαδικασία της Διανομής Πιστοποιητικών παρέχουμε ως είσοδο το καινούργιο πιστοποιητικό που έχουμε δημιουργήσει και παίρνουμε ως έξοδο μια δυαδική τιμή που μας δείχνει αν το πιστοποιητικό παραδόθηκε στην οντότητα που έκανε αίτηση για την δημιουργία του, συμφώνα με τις προσδιορισμένες διαδικασίες, ή όχι. Το επίπεδο αξιοπιστίας, που έχει προσδιοριστεί για το συγκεκριμένο πιστοποιητικό, καθορίζει τις διαδικασίες που θα ακολουθήσουν. Όσο υψηλότερο είναι το επίπεδο αξιοπιστίας τόσο πιο ασφαλή μέσα πρέπει να χρησιμοποιηθούν.

Τα μέσα που χρησιμοποιούνται για να παραδοθεί το καινούργιο πιστοποιητικό που έχει δημιουργηθεί μπορεί να είναι ένα φυσικό κουπόνι ή ένα ηλεκτρονικό μήνυμα προς τον αιτών.

Ένα φυσικό κουπόνι (token) είναι για παράδειγμα μια δισκέτα ή μία έξυπνη κάρτα (smart card). Αυτά τα tokens μπορούν να παραδοθούν ταχυδρομικώς. Εναλλακτικά ο αιτών μπορεί να πάει ο ίδιος στα γραφεία της Αρχής Πιστοποίησης και να παραλάβει το κουπόνι. Αυτό γίνεται συνήθως στην περίπτωση υψηλού επιπέδου αξιοπιστίας πιστοποιητικών.

Για να παραδώσουμε το πιστοποιητικό μπορούμε να στείλουμε ένα ηλεκτρονικό μήνυμα προς τον αιτών χρησιμοποιώντας ηλεκτρονικό ταχυδρομείο (e-mail), ή το παγκόσμιο διαδίκτυο (WWW) ή συνδυασμό και των δύο. Για παράδειγμα, ο αιτών μπορεί να ειδοποιηθεί για την ολοκλήρωση της παραγωγής του πιστοποιητικού με ένα μήνυμα ηλεκτρονικού ταχυδρομείου που να περιέχει το URL που βρίσκεται το πιστοποιητικό. Επιλέγοντας (κάνοντας click) στο URL ο αιτών μπορεί να αποθηκεύσει το πιστοποιητικό στο δίσκο του.

Ώς επιπλέον μέτρο ασφάλειας, τα πιστοποιητικά, αν και είναι κρυπτογραφημένα, πρέπει να προστατεύονται από ένα μηχανισμό εξακρίβωσης ταυτότητας π.χ. από ένα κωδικό πρόσβασης (password). Αυτό γίνεται για λόγους ασφάλειας όταν το πιστοποιητικό έχει αποθηκευτεί σε μαγνητικό μέσο. Για παράδειγμα όταν μια οντότητα έχει αποθηκεύσει το πιστοποιητικό της στο σκληρό δίσκο του υπολογιστή και ο υπολογιστής αυτός χρησιμοποιείται και από μια άλλη οντότητα, η τελευταία οντότητα πρέπει να ξέρει τον κωδικό πρόσβασης για να χρησιμοποιήσει το πιστοποιητικό.

Τελικά, κάποια βοηθητική πληροφορία μπορεί να προστεθεί στο πιστοποιητικό κατά τη διαδικασία διανομής του. Αυτή η πληροφορία μπορεί να αναφέρεται στο δημόσιο κλειδί της Αρχής Πιστοποίησης, στο πιστοποιητικό της Αρχής Πιστοποίησης, στην ηλεκτρονική του διεύθυνση (e-mail) και το νούμερο του fax της, και στα μέσα που πρέπει να χρησιμοποιηθούν για να αποθηκευτεί το πιστοποιητικό όπως π.χ. ένα αρχείο κ.τ.λ..

5.5.3 Αποθήκευση και Ανάκληση Πιστοποιητικών

Αυτή η διαδικασία αναφέρεται στις ενέργειες που πρέπει να κάνει η Αρχή Πιστοποίησης για να ανταποκριθεί σε μια αίτηση για πληροφορία που αφορά ένα συγκεκριμένο πιστοποιητικό.

Η διαδικασία παίρνει σαν είσοδο ένα πιστοποιητικό και δίδει ως έξοδο μια τιμή που δείχνει αν το πιστοποιητικό που στείλαμε για αποθήκευση αποθηκεύτηκε και μπορεί να ανακληθεί επιτυχώς ή όχι, και αν όχι του λόγους αποτυχίας.

Η Αρχή Πιστοποίησης, αρχικά, πρέπει να αποθηκεύσει ασφαλώς τη λίστα των πιστοποιητικών που έχει παράγει. Πρέπει να υπάρχουν τουλάχιστο δύο αντίγραφα της λίστας. Ένα που θα χρησιμοποιείται για on-line requests και ένα άλλο που θα χρησιμοποιείται ως εφεδρικό αντίγραφο (backup).

Μόλις αποθηκευτεί η λίστα των πιστοποιητικών η Αρχή Πιστοποίησης πρέπει να παρέχει στους χρήστες του συστήματος ασφαλείας PKI τη δυνατότητα να κάνουν αιτήσεις για πληροφορία σχετικά με τα πιστοποιητικά. Δεν θα ήταν αποδοτικό για την υπηρεσία διαχείρισης των πιστοποιητικών (certificate management service) να αναλάβει τη δημοσιοποίησης της πληροφορίας σχετικά με τα πιστοποιητικά. Για αυτό τον λόγο η υπηρεσία διαχείρισης των πιστοποιητικών πρέπει να στέλνει τη λίστα των πιστοποιητικών σε μια υπηρεσία δημοσιοποίησης (publication service). Πρέπει να επισημάνουμε ότι εδώ ο όρος υπηρεσία δημοσιοποίησης αναφέρεται στην ευρύτερη έννοια και δεν μπορεί να είναι μόνο η πολύ διαδεδομένη υπηρεσία καταλόγου (directory service), αλλά θα μπορούσε να είναι για παράδειγμα ένας FTP server.

Οι τελικές οντότητες μπορούν να επικοινωνούν με την υπηρεσία δημοσιοποίησης για να παίρνουν την πληροφορία που θέλουν. Αυτή η επικοινωνία μπορεί να γίνει χρησιμοποιώντας διάφορα υπάρχοντα πρωτόκολλα όπως:

- Directory service protocol
- E-mail protocol
- FTP
- HTTP

Διάφοροι μηχανισμοί μπορούν να χρησιμοποιηθούν για να υλοποιηθεί η υπηρεσία δημοσιοποίησης όπως για παράδειγμα:

- Directory (π.χ. X.500 κάνοντας χρήση του πρωτοκόλλου LDAP)
- FTP site
- Web site

- Με χρήση finger server

Μπορούμε να φανταστούμε την δημοσιοποίηση σαν ένα μέρος αποθήκευσης (repository) και την υπηρεσία δημοσιοποίησης ως την διεπιφάνεια χρήσης (interface) μεταξύ της των τελικών οντοτήτων και της αποθήκευσης. Έχει προταθεί ως πιο κατάλληλη και λειτουργική λύση για αποθήκευση ο συνδυασμός ενός HTTP service και μια Υπηρεσία Καταλόγου (Directory service). Η τελική οντότητα θα μπορεί να χρησιμοποιεί το HTTP σαν interface την Υπηρεσία Καταλόγου ενώ η Υπηρεσία Καταλόγου είναι το interface μεταξύ της τελικής οντότητας και του χώρου αποθήκης των πιστοποιητικών (certificate repository). Η τελική οντότητα στέλνει τις αιτήσεις χρησιμοποιώντας το HTTP και η πραγματική αναζήτηση στο repository γίνεται από την Υπηρεσία Καταλόγου. Τα αποτελέσματα δίνονται στον αιτών χρησιμοποιώντας HTTP. Αυτή η λύση φαίνεται να είναι πιο αποτελεσματική από άλλες λόγω του φιλικού interface που προσφέρεται από το HTTP και της αποτελεσματικής αναζήτησης που προσφέρει Υπηρεσία Καταλόγου. Επιπλέον, η τελική οντότητα μπορεί να ζήτα πληροφορία χρησιμοποιώντας διαφορετικά και σύνθετα κριτήρια ευρέσεως. Μόνο οι Υπηρεσίες Καταλόγου μπορούν να προσφέρουν τέτοια ευκολία.

Με στόχο τον έλεγχο της πρόσβαση στον Κατάλογο (directory), μπορεί να χρησιμοποιηθεί ένα σχήμα εξακρίβωσης ταυτότητας όπως για παράδειγμα κωδικός πρόσβασης (password). Σε κάθε περίπτωση το κλειδί που χρησιμοποιείται για να έχουμε πρόσβαση στο publication service πρέπει να είναι κρυπτογραφημένο κατά τη μετάδοση του προς το site της Αρχής Πιστοποίησης.

Υπάρχουν δύο τρόποι για να είναι η πληροφορία των πιστοποιητικών δημόσια διαθέσιμη: Με παράδοση των λιστών πιστοποιητικών σε όλα τα μέλη του PKI και με διανομή μόνο έπειτα από αίτηση.

Έχει προταθεί ο δεύτερος τρόπος γιατί ο πρώτος αυξάνει πολύ τον όγκο της πληροφορίας που διακινείται στο δίκτυο. Είναι αναμενόμενο ότι οι τελικές οντότητες θα κάνουν συχνά αιτήσεις για πληροφορία σχετικά με συγκεκριμένα πιστοποιητικά, ελαχιστοποιώντας με αυτόν τον τρόπο την ανάγκη για μια μεταφορά της συνολικής λίστας των πιστοποιητικών στα site τους.

5.5.4 Ανάκληση Πιστοποιητικών

Η διαδικασία της ανάκλησης των πιστοποιητικών παίρνει ως είσοδο ένα έγκυρο πιστοποιητικό και δίδει σαν έξοδο μία τιμή που δείχνει αν το πιστοποιητικό έχει ανακληθεί επιτυχώς ή όχι και τους λόγους τυχόν αποτυχίας της ανάκλησης.

Όταν η διάστημα εγκυρότητας του πιστοποιητικού λήξει το πιστοποιητικό ακυρώνεται και πρέπει να ανακληθεί. Για να αποτραπεί η επικοινωνία με οντότητες που η εξακρίβωση της ταυτότητας τους δεν γίνεται πλέον από την Αρχή Πιστοποίησης, τα μέλη του συστήματος ασφαλείας PKI πρέπει να είναι ενήμερα για τα πιστοποιητικά που έχουν ανακληθεί. Επιπλέον, μια οντότητα μπορεί να απαιτήσει την ακύρωση του πιστοποιητικού της κατά τη δική της βούληση. Αυτό θα συμβαίνει κανονικά σε περίπτωση που μια τελική οντότητα υποψιαστεί ότι το πιστοποιητικό της έχει εκτεθεί σε κινδύνους.

Τα θέματα που πρέπει να συζητηθούν σε αυτή την παράγραφο περιλαμβάνουν:

1. *Την διαδικασία αίτησης για ανάκληση*
2. *Τον μηχανισμό ανάκλησης*
3. *Το CRL format*
4. *Τα μέσα που χρησιμοποιούνται για την αποθήκευση της CRL*

5.5.4.1 Διαδικασία αίτησης για ανάκληση

Σε περίπτωση που μια τελική οντότητα υποψιάζεται ότι το ιδιωτικό κλειδί της έχει εκτεθεί σε κινδύνους πρέπει αμέσως να ακυρώσει το αντίστοιχο πιστοποιητικό για να μην θέσει σε κίνδυνο άλλες οντότητες της Υποδομής Δημοσίου Κλειδιού PKI. Σε αυτή την περίπτωση η τελική οντότητα στέλνει μια αίτηση ανάκλησης στην Αρχή Πιστοποίησης. Σε κάθε περίπτωση η Αρχή Πιστοποίησης θα αναλάβει όλες αυτές τις ενέργειες που χρειάζονται για να ανακληθεί το πιστοποιητικό. Όταν το πιστοποιητικό ακυρωθεί, η Αρχή Πιστοποίησης πρέπει να κάνει δημόσια γνωστό αυτό το γεγονός. Επίσης πρέπει να ειδοποιήσει την τελική οντότητα για την ανάκληση του πιστοποιητικού χρησιμοποιώντας ένα standard μηχανισμό (για παράδειγμα e-mail, s-mail).

Η μορφή (format) της αίτησης ανάκλησης του πιστοποιητικού πρέπει να είναι εντελώς συμβατή με τη διεπιφάνεια χρήσης που χρησιμοποιείται μεταξύ της τελικής οντότητας και της Αρχής Πιστοποίησης. Τα μέσα που χρησιμοποιούνται για την

μετάδοση της αίτησης ανάκλησης πιστοποιητικού μπορεί να είναι ηλεκτρονικά (π.χ. e-mail, HTTP), ή και όχι (π.χ. απλή αλληλογραφία). Η δομή των δεδομένων της αίτησης ακύρωσης έχει περιγραφεί από το PKIX Internet Drafts. Το πρότυπο X.509 [X.509] περιγράφει τα πεδία που πρέπει να συμπεριληφθούν σε μια τέτοια αίτηση.

Όταν η Αρχή Πιστοποίησης λάβει μια αίτηση ανάκλησης πιστοποιητικού πρέπει να ελέγξει την αυθεντικότητα της αίτησης χρησιμοποιώντας ένα σχήμα εξακρίβωσης ταυτότητας (π.χ. κωδικό πρόσβασης, challenge response, call back).

Αφού ακυρώσει το πιστοποιητικό η Αρχή Πιστοποίησης πρέπει να ειδοποιήσει τον αιτών. Η ειδοποίηση μπορεί να γίνει χρησιμοποιώντας διάφορα μέσα επικοινωνίας, όπως αναφέραμε παραπάνω.

Τελικά η Αρχή Πιστοποίησης πρέπει να κάνει δημόσια διαθέσιμη την πληροφορία που έχει σχέση με την ακύρωση. Αυτό μπορεί να επιτευχθεί κάνοντας χρήση μηχανισμών ανάκλησης από την ίδια την Αρχή Πιστοποίησης. Οι μηχανισμοί που χρησιμοποιεί η Αρχή Πιστοποίησης για να κάνει δημόσια διαθέσιμη την πληροφορία για τα ακυρωμένα πιστοποιητικά, θα συζητηθεί στο επόμενο μέρος.

5.5.4.2 Μηχανισμός Ανάκλησης

Υπάρχει μεγάλη επιστημονική διαμάχη σχετικά για το πιο είναι το αποτελεσματικότερο σχήμα ανάκλησης για να υιοθετηθεί [RFC2459]. Παρακάτω παραθέτουμε μερικά σχήματα ακύρωσης τα οποία έχουν προταθεί με στόχο να λυθεί το πρόβλημα της ενημέρωσης σχετικά με την ακύρωση (revocation update problem).

5.5.4.2.1 Λίστες Ανάκλησης Πιστοποιητικών (Certificate Revocation Lists/ CRLs)

Η Αρχή Πιστοποίησης εκδίδει, σε περιοδικά διαστήματα, μια πλήρης λίστα με όλα τα πιστοποιητικά που έχουν ανακληθεί. Η τελική οντότητα πρέπει να λάβει τη Λίστα Ακύρωσης Πιστοποιητικών (CRL) και να αποφασίσει αν ένα συγκεκριμένο πιστοποιητικό έχει ανακληθεί ή όχι. Εναλλακτικά η τελική οντότητα πρέπει να στείλει σχετική αίτηση για να λάβει απάντηση αν ένα συγκεκριμένο πιστοποιητικό έχει ανακληθεί. Αν και το σχήμα είναι απλό στην υλοποίηση του συμβάλλει στην αύξηση της κίνησης του δικτύου μεταξύ της τελικής οντότητας και της Αρχής Πιστοποίησης. Για αυτό το λόγο, έχουν προταθεί τα delta CRLs τα οποία στοχεύουν να κάνουν αυτό το σχήμα ανάκλησης πιο αποδοτικό και ευέλικτο. Σε αυτή την περίπτωση διατηρούμε μόνο την τελευταία ενημέρωση (update) της Λίστας Ανάκλησης Πιστοποιητικών. Κάθε τελική

οντότητα πρέπει να λάβει μια ολοκληρωμένη Λίστα Ανάκλησης Πιστοποιητικών, την πρώτη φορά που επικοινωνεί με την Αρχή Πιστοποίησης και να κατεβάζει (download) την delta CRL από τότε και μετά. Γενικά, χρησιμοποιώντας κατανεμημένες Λίστες Ανάκλησης Πιστοποιητικών είναι δύσκολο να εγγυηθούμε την ακεραιότητα (integrity) της καθολικής Λίστας Ανάκλησης Πιστοποιητικών. Παρόλα αυτά το σχήμα των Λιστών Ανάκλησης Πιστοποιητικών είναι το πιο ευρέως διαδεδομένο, προς το παρόν, και έχει υιοθετηθεί από πολλά πρότυπα, όπως για παράδειγμα το X.509.

5.5.4.2.2 Σύστημα Ανάκλησης Πιστοποιητικών (Certificate Revocation System)

Αυτό το σχήμα έχει προταθεί με σκοπό να μειώσει το κόστος της επικοινωνίας και του όγκου της πληροφορίας που διακινείται στο δίκτυο για τις Λίστες Ανάκλησης Πιστοποιητικών. Η υποκείμενη ιδέα είναι να υπογράφεται ένα μήνυμα για κάθε πιστοποιητικό που να δηλώνει εάν το πιστοποιητικό έχει ακυρωθεί ή όχι, και να χρησιμοποιείται ένα off-line/on-line σχήμα υπογραφής για να μειώσει το κόστος του να γίνονται αυτές οι υπογραφές περιοδικά update. Το πλεονέκτημα αυτού του σχήματος είναι ότι μειώνει το κόστος επικοινωνίας μεταξύ της τελικής οντότητας και της Αρχής Πιστοποίησης. Το μειονέκτημα του είναι η αύξηση της επικοινωνίας μεταξύ της Αρχής Πιστοποίησης και του Κατάλογου (directory).

5.5.4.2.3 Δένδρα Ανάκλησης Πιστοποιητικών (Certificate Revocation Trees)

Αυτό το σχήμα βασίζεται στην ιδέα των δένδρων κατακερματισμού (hash trees) και χρησιμοποιείται για να δώσει μια γρήγορη απόδειξή ότι το πιστοποιητικό δεν έχει ανακληθεί. Ένα CRT (Certificate Revocation Tree) είναι ένα δένδρο κατακερματισμού με φύλλα που ανταποκρίνονται σε ένα σύνολο από δηλώσεις για πιστοποιητικά με συγκεκριμένους σειριακούς αριθμούς. Όταν μια οντότητα στείλει μια αίτηση στην Αρχή Πιστοποίησης, τότε το δένδρο κατακερματισμού αναλύεται για να αποδειχθεί η εγκυρότητα του πιστοποιητικού. Το κύριο πλεονέκτημα αυτού του σχήματος για τις Λίστες Ανάκλησης Πιστοποιητικών είναι ότι δεν είναι ανάγκη να διατηρείται ολόκληρο η λίστα ανάκλησης και ο αιτών μπορεί να λαμβάνει μια γρήγορη απόδειξη της ισχύος του πιστοποιητικού. Το κύριο μειονέκτημα είναι ότι το υπολογιστικό κόστος του υπολογισμού του δένδρου κατακερματισμού και της αναπροσαρμογής του, κάθε φορά που έχουμε ανάκληση ενός πιστοποιητικού.

Παρά το γεγονός ότι υπάρχουν πολλά διαφορετικά σχήματα ανάκλησης, με τα πλεονεκτήματα και τα μειονεκτήματα τους, η Λίστα Ανάκλησης Πιστοποιητικών (CRL)

είναι το πιο ευρέως διαδεδομένο σχήμα. Για αυτό το λόγο θα το τονίσουμε και θα το αναλύσουμε.

5.5.4.3 Μέσα που χρησιμοποιούνται για αποθήκευση της Λίστας Ανάκλησης Πιστοποιητικών (CRL)

Τα μέσα που χρησιμοποιούνται για την αποθήκευση της Λίστας Ανάκλησης Πιστοποιητικών εξαρτούνται από τον τρόπο που γίνεται η ενημέρωση της (update). Υπάρχουν δύο μέθοδοι, προς το παρόν, για να ενημερωθεί μια τελική οντότητα εάν ένα πιστοποιητικό είναι έγκυρο ή όχι.

Η πρώτη μέθοδο είναι να κατεβάσουμε (download) όλη την Λίστα Ανάκλησης Πιστοποιητικών (CRL). Σε αυτή την περίπτωση η CRL αποθηκεύεται στο site της Αρχής Πιστοποίησης και η τελική οντότητα μπορεί να χρησιμοποιεί ένα πρωτόκολλο για να προμηθεύεται (κάνει download) τη CRL. Τα πρωτόκολλα FTP και e-mail είναι τέτοιοι μηχανισμοί. Σε αυτή την περίπτωση η CRL αποθηκεύεται στον σκληρό δίσκο της τελικής οντότητας. Μπορούν επίσης να χρησιμοποιηθούν και μη ηλεκτρονικοί μηχανισμοί όπως το ταχυδρομείο.

Η δεύτερη μέθοδος είναι να στείλουμε μια αίτηση για να ρωτήσει για την ισχύ ενός συγκεκριμένου πιστοποιητικού και λαβαίνοντας μια απάντηση. Σε αυτή την περίπτωση η CRL δεν αποθηκεύεται από την τελική οντότητα. Το πρωτόκολλο για το directory service (π.χ. το LDAP) [RFC1777] μπορεί να χρησιμοποιηθεί σε αυτήν τη περίπτωση. Στο site της Αρχής Πιστοποίησης η αναζήτηση γίνεται χρησιμοποιώντας ένα από τους μηχανισμούς που περιγράφονται στην παράγραφο που αναφέρεται στους μηχανισμούς Ανάκλησης.

Με στόχο την αύξηση της λειτουργικότητας του μηχανισμού ανάκλησης μπορεί στο site της τελικής οντότητας να χρησιμοποιηθεί η cache memory. Τα πιο πρόσφατα tokens (για παράδειγμα τα ολοκληρωμένα CRLs ή οι απαντήσεις για τυχόν ακύρωση (revocation responses)) μπορούν να αποθηκευτούν στην cache memory για γρήγορη ανάκληση. Εάν το πιστοποιητικό δεν βρεθεί σε αυτή τη λίστα τότε η τελική οντότητα θα συμβουλευθεί την Αρχή Πιστοποίησης.

5.6 Πρότυπα για την μορφή των πιστοποιητικών και των Λιστών Ακύρωσης Πιστοποιητικών

5.6.1 Μορφή Πιστοποιητικών

Οι σημαντικές μορφές (format) πιστοποιητικών είναι:

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

Μέχρι σήμερα τα format πιστοποιητικών 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). Παρόλο που τα πιστοποιητικά τύπου PGP είναι πολύ απλά, παρουσιάζονται πολλά προβλήματα όταν πρόκειται να χρησιμοποιηθούν για ανοικτά κατανεμημένα περιβάλλοντα επειδή 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).

Το X.509 είναι ένα σχήμα πιστοποίησης σχεδιασμένο για να υποστηρίζει υπηρεσίες καταλόγου X.500 (X.500 directory services). 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 Υπηρεσίας 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 ασφάλειας 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 (interoperability), αναμένεται στο μέλλον να επικρατήσουν στις υλοποιήσεις των συστημάτων ασφαλείας PKI μόνο καινούργιες εκδόσεις αυτού του προτύπου, ή επεκτάσεις αυτού.

Η έκδοση 3 (v3) 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 μια μικρή περιοχή (domain). Τα X.509 v1 και X.509 v2 πιστοποιητικά είναι περισσότερο κατάλληλα για τη χρήση σε μικρή περιοχή (domain) όπως για παράδειγμα ενός οργανισμού. Αυτός είναι ένας περιορισμός που εμποδίζει την ευρεία ανάπτυξη αυτών των πιστοποιητικών.

Σύμφωνα με το πρότυπο ITU X.509, ένα πιστοποιητικό περιέχει πληροφορία για τον κάτοχο του πιστοποιητικού και για την Αρχή Πιστοποίησης που εξέδωσε το πιστοποιητικό.

Ένα πιστοποιητικό αποτελείται από δύο μέρη: τα δεδομένα που περιέχει το πιστοποιητικό και την υπογραφή από την Αρχή Πιστοποίησης που εξέδωσε αυτό το πιστοποιητικό.

Τα δεδομένα σε ένα πιστοποιητικό περιέχουν την ακόλουθη πληροφορία:

1) Το νούμερο έκδοσης (version number), για συμβατότητα με μελλοντικές βελτιωμένες εκδόσεις του πρότυπου X.509

2) Το σειριακό νούμερο (serial number) του πιστοποιητικού (κάθε πιστοποιητικό που έχει εκδοθεί από μία Αρχή Πιστοποιητικών πρέπει να έχει μοναδικό σειριακό αριθμό)

3) Τον αλγόριθμο που χρησιμοποιεί η Αρχή Πιστοποιητικών για να υπογράψει το πιστοποιητικό (για παράδειγμα PKCS #1 MD5 with RSA Encryption- Αυτό σημαίνει ότι η κρυπτογράφηση γίνεται σύμφωνα με το πρότυπο κρυπτογράφησης PKCS #1 [PKCS#1], χρησιμοποιείται ο αλγόριθμος κατακερματισμού MD5 και ο αλγόριθμος κρυπτογράφησης RSA)

4) Το διακεκριμένο όνομα (distinguished name) της Αρχής Πιστοποιητικών που εκδίδει το πιστοποιητικό (για παράδειγμα, (CN=Αρχή Πιστοποιητικών HYGEIAnet, O=Βενιζελείο, OU=Νοσοκομεία, ST= Κρήτη, O=Τομέας Υγείας, C=GR)

5) Την περίοδο εγκυρότητας του πιστοποιητικού (για παράδειγμα, μεταξύ 15 Νοεμβρίου 1996 και 15 Νοεμβρίου 1997)

6) Το διακεκριμένο όνομα του υποκείμενου πιστοποίησης (certificate subject) (για παράδειγμα, CN=Γεώργιος Γεωργίου, O=Βενιζελείο, OU=Νοσοκομεία, ST= Κρήτη, O=Τομέας Υγείας, C=GR)

7) Πληροφορία για το δημόσιο κλειδί που πιστοποιείται; αυτή η πληροφορία περιλαμβάνει: Τον αλγόριθμο για το δημόσιο κλειδί και μια αναπαράσταση με αλφαριθμητικά ψηφία (bit-string) του δημόσιου κλειδιού (εφαρμόζεται μόνο για RSA κλειδιά).

Το format ενός X.509 v3 certificate απεικονίζεται στην παρακάτω εικόνα.

Σχήμα 5.6.1. Μορφή X.509 Πιστοποιητικού (X.509 Certificate format)

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) παρέχουν 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.

Οι κανονικές προεκτάσεις που έχουν προταθεί από τον ISO μπορούν να κατηγοριοποιηθούν ως εξής:

1) **Πολιτικές πιστοποιητικών και απεικόνιση τους (Certificate policies and policy mapping)**

   Αυτά τα extensions χρησιμοποιούνται με σκοπό να βοήσουν τις Έμπιστες Τρίτες Οντότητες (TTPs) στο να παρέχουν στο χρήστη τις προδιαγραφές της πολιτικής (policy specifications) που χρησιμοποιούνται για να δημιουργηθεί ένα πιστοποιητικό. Η απεικόνιση της πολιτικής (policy mapping) χρησιμοποιείται με σκοπό να προσδιοριστούν ισοδύναμες πολιτικές άλλων TTPs.

2) **Εναλλακτικά ονόματα (Alternative names)**

   Αυτά τα extensions χρησιμοποιούνται για να προσδιορίσουν εναλλακτικά διακεκριμένα ονόματα (distinguished names) για τον κάτοχο και τον ιδιοκτήτη του πιστοποιητικού.

3) **Χαρακτηριστικά πεδία του directory για τον κάτοχο του πιστοποιητικού (Subject directory attributes)**

Χρησιμοποιώντας αυτά τα extensions ο ιδιοκτήτης ενός πιστοποιητικού μπορεί να δώσει επιπρόσθετη πληροφορία για την ταυτότητα του, εκτός από το όνομα του.

4) **Περιορισμοί για το μονοπάτι πιστοποίησης (Certification path constraints)**

Αυτό το extension χρησιμοποιείται με σκοπό να βοηθήσει τα TTPs να συνδέσουν τις υποδομές τους με τρόπους που έχουν νόημα, επιβάλλοντας συγκεκριμένους κανόνες σε αυτή την σύνδεση.

Επιπλέον έχει προσδιοριστεί μια ομάδα από extensions σχετικά με τις Λίστες Ακύρωσης Πιστοποιητικών (CRLs). Σε αυτή την παράγραφο απλώς αναφέρουμε αυτά τα extensions, αφήνοντας την περιγραφή τους να γίνει παρακάτω που θα περιγράψουμε την διαδικασία της Ακύρωσης των Πιστοποιητικών.

Τα extensions αυτά είναι :

- Αριθμητικοί κωδικοί και κωδικοί αιτίας της λίστας ανάκλησης (CRL number and reason codes)
- Σημεία διανομής της λίστας ανάκλησης (CRL distribution points)
- Delta CRLs
- Έμμεσα CRLs (Indirect CRLs)

Το πρότυπο X.509 v3 προέβλεψε όχι μόνο για τα «standard» extensions αλλά και για «private» extensions που ορίζονται από τον χρήστη. Χρησιμοποιώντας την παραπάνω παροχή 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. Έχει προταθεί ότι κάθε TTP θα πρέπει να αναθέτει τιμή κατά βούληση.

5.6.2 Μορφή Λιστών Ακύρωσης Πιστοποιητικών (CRL Format)

Η μορφή (format) που χρησιμοποιείται ευρέως για τις λίστες ακύρωσης πιστοποιητικών είναι το X.509 v2 (revocation list format). Το X.509 v2 format απεικονίζεται στο σχήμα 5.6.2.

Η ώρα που εκδόθηκε η Λίστα Ακύρωσης Πιστοποιητικών χρησιμοποιείται για να δηλώσει το χρόνο, σύμφωνα με το ρολόι της Αρχής Πιστοποίησης, που η λίστα δημιουργήθηκε. Με αυτόν τον τρόπο μπορούμε να πούμε, ότι η Λίστα Ανάκλησης Πιστοποιητικών περιλαμβάνει υποδομή για την υποστήρίξη στοιχείων χρόνο-σφράγισης (time stamping).

Σε αυτό το σημείο πρέπει να αναφερθούμε στις προεκτάσεις (extensions) της Λίστα Ανάκλησης Πιστοποιητικών (CRL) του X.509 πιστοποιητικού. Αυτές οι προεκτάσεις μπορούν να χρησιμοποιηθούν για να προσθέσουν ευελιξία στον τρόπο που διαχειρίζονται οι Λίστες Ακύρωσης Πιστοποιητικών. Οι προεκτάσεις αυτές είναι:

1) **Νούμερα CRL και κώδικές αιτίας (CRL number and reason codes)**

   Αυτή η προέκταση (extension αναθέτει ένα σειριακό αριθμό σε κάθε Λίστα Ανάκλησης Πιστοποιητικών (CRL) για να βοηθήσει την τελική οντότητα να αποφασίσει εάν η CRL λείπει από την συλλογή της ή όχι. Επιπλέον κάθε πιστοποιητικό που έχει ανακληθεί μπορεί να έχει πάνω του την αιτία ανάκλησης του.

2) **Σημεία διανομής των CRL (CRL Distribution points)**

   Αυτή η προέκταση δίδει τη δυνατότητα στις τελικές οντότητες να κάνουν download τις Λίστες Ανάκλησης Πιστοποιητικών από διαφορετικά σημεία.

3) **Δέλτα CRLs (Delta CRLs)**

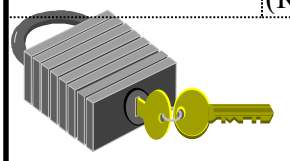
   Αυτή η προέκταση μπορεί να χρησιμοποιηθεί για να δίδει την δυνατότητα στο χρήστη να προμηθεύεται (κάνει download) μόνο τις ενημερώσεις (updates)

μιας Λίστας Ανάκλησης Πιστοποιητικών (CRL) και όχι ολόκληρο τη λίστα απαραίτητα. Αυτό συμβάλλει στη μείωση της κίνησης του δικτύου.

4) Έμμεσα CRLs (Indirect CRLs)

Αυτή η προέκταση δίδει τη δυνατότητα να γίνει ένα συνολικό μάζεμα όλων των Λιστών Ανάκλησης Πιστοποιητικών CRLs σε ένα συγκεκριμένο σημείο. Με αυτό τον τρόπο πολλές Αρχές Πιστοποίησης μπορούν να παραθέσουν τις Λίστες Ανάκλησης Πιστοποιητικών τους για να σχηματίσουν μια κεντρική Λίστα Ανάκλησης Πιστοποιητικών.

Παρά το γεγονός ότι αυτές οι προεκτάσεις (extensions) προσφέρουν ευελιξία στη διαχείριση των πιστοποιητικών που ακυρώνονται, και ιδιαίτερα συμβάλλουν στην μείωση της κινήσεως του δικτύου, δεν λύνουν εντελώς το πρόβλημα της χρονικής διαφοράς (time granularity). Αυτό το πρόβλημα αναφέρεται στο χρονικό παράθυρο μεταξύ δυο διαδοχικών ενημερώσεων ενός URL. Υπάρχει πιθανότητα για μια τελική οντότητα να αντιμετωπίσει προβλήματα ασφάλειας κατά τη διάρκεια αυτού του χρονικού παράθυρου.

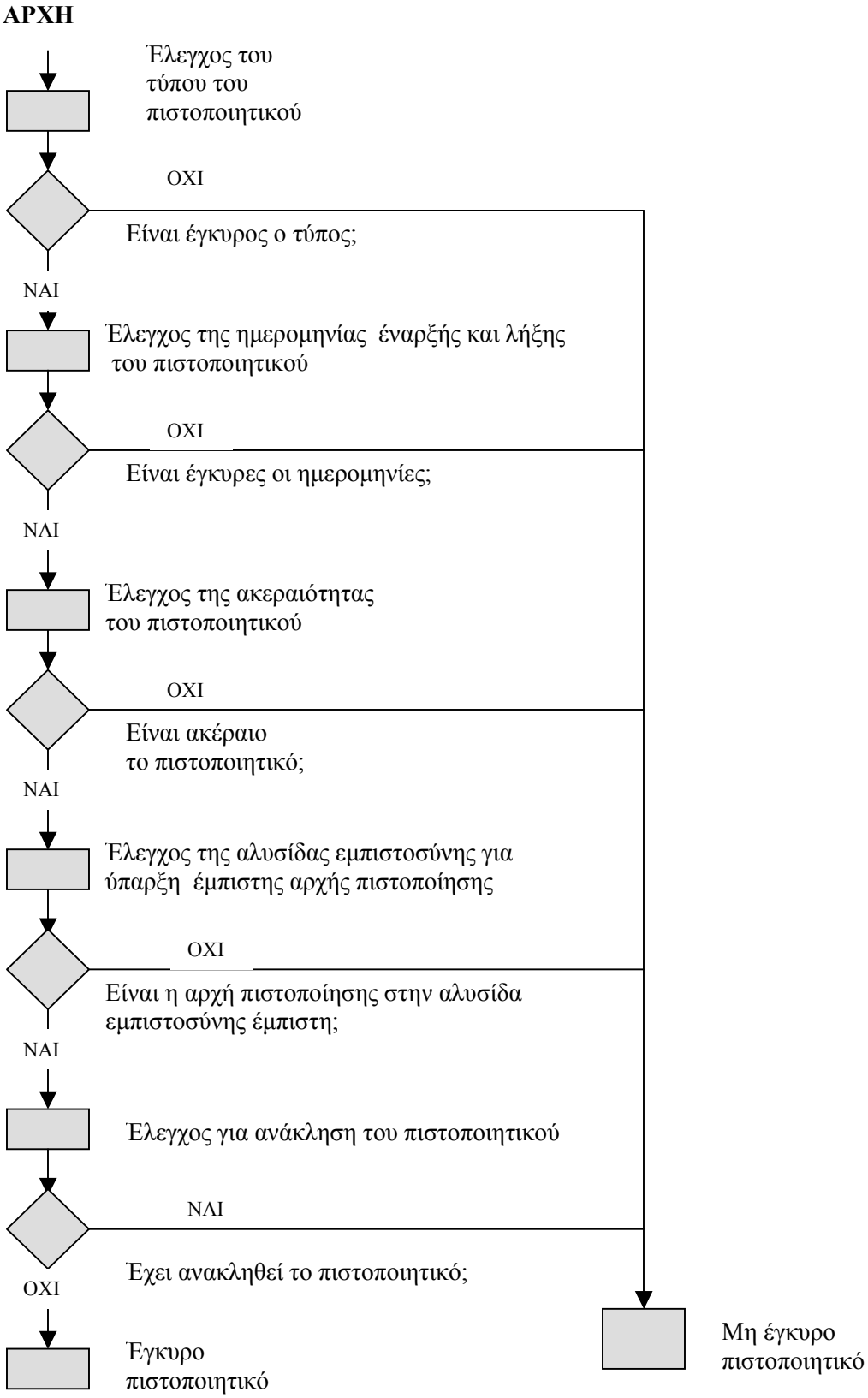
<table>
<tr><td colspan="3">Έκδοση (Version)
Υπογραφή (Signature)
Αρχή Έκδοσης (Issuer)
Ημερομηνία ενημέρωσης (Date of this update)
Ημερομηνία επόμενης ενημέρωσης (Date of next update)</td></tr>
<tr><td>Σειριακός αριθμός
(Serial number)</td><td>Ημερομηνία
ακύρωσης
(Revocation Date)</td><td>Προεκτάσεις
(Extensions)</td></tr>
<tr><td></td><td>Ημερομηνία
ακύρωσης
(Revocation Date)</td><td>Προεκτάσεις
(Extensions)</td></tr>
<tr><td colspan="3">…….</td></tr>
<tr><td></td><td>Ημερομηνία
Ακύρωσης
(Revocation Date)</td><td>Προεκτάσεις
(Extensions)</td></tr>
<tr><td colspan="3"> 
Έχει υπογραφεί με το ιδιωτικό κλειδί της Έμπιστης Τρίτης Οντότητας (TTP)</td></tr>
</table>

Σχήμα 5.6.2. Μορφή (format) της Λίστας Ανάκλησης Πιστοποιητικών X.509 v2 CRL

5.7 Διαδικασία έλεγχου εγκυρότητας του πιστοποιητικού

Για να εμπιστευτούμε ένα πιστοποιητικό πρέπει να ελέγξουμε την εγκυρότητα του. Η διαδικασία για τον έλεγχο εγκυρότητας του πιστοποιητικού είναι η εξής:

1. Ελέγχουμε αν είναι έγκυρος ο τύπος του.
2. Ελέγχουμε αν η παρούσα χρονική στιγμή βρίσκεται εντός της χρονικής περιόδου που ορίζεται από τις ημερομηνίες έναρξης και λήξης του, δηλαδή αν την παρούσα χρονική στιγμή το πιστοποιητικό βρίσκεται σε ισχύ.
3. Ελέγχουμε την ακεραιότητα του βάση της ψηφιακής υπογραφής.
4. Ελέγχουμε την εγκυρότητα όλου του μονοπατιού πιστοποίησης (certification path) μέχρί να φτάσουμε στην ρίζα για να διαπιστώσουμε εάν το υπό έλεγχο πιστοποιητικό είναι έγκυρο. Το πιστοποιητικό καθίσταται έγκυρο αν διασχίσουμε (traversing) την αλυσίδα υπογραφών (signature chain), και επιβεβαιώσουμε την εγκυρότητα όλων των πιστοποιητικών μέχρι να φτάσουμε στη ρίζα (root) της αλυσίδας. Αν το πιστοποιητικό στη ρίζα της αλυσίδας είναι έγκυρο και έχει εκδοθεί από μια Αρχή Πιστοποίησης που εμπιστευόμαστε (Trusted Root Authority) τότε το υπό έλεγχο πιστοποιητικό είναι έγκυρο.
5. Ελέγχουμε αν έχει ανακληθεί το πιστοποιητικό (βλέπε υποπαράγραφο 5.7.1).



Σχήμα 5.7. Διαδικασία Ελέγχου Εγκυρότητας Πιστοποιητικού

5.7.1 Έλεγχος Ανάκλησης Πιστοποιητικού

Η διαδικασία για τον έλεγχο της ανάκλησης των πιστοποιητικών είναι η εξής:

1. Επιβεβαιώνουμε την υπογραφή της Λίστας Ανάκλησης Πιστοποιητικών (CRL) χρησιμοποιώντας το δημόσιο κλειδί του εκδότη του πιστοποιητικού και τις κατάλληλες παραμέτρους που αναφέρονται εκεί. Αν η υπογραφή της Λίστας δεν είναι έγκυρη ο χρήστης πρέπει να ενημερωθεί ότι η Λίστα Ανάκλησης Πιστοποιητικών δεν ισχύει πλέον και πρέπει να λάβει την νέα Λίστα Ανάκλησης Πιστοποιητικών (ή η διαδικασία αυτή να γίνει αυτοματοποιημένα).
2. Επιβεβαιώνουμε το μονοπάτι πιστοποίησης του πιστοποιητικού με το οποίο υπογράφει ο εκδότης της Λίστας Ανάκλησης των Πιστοποιητικών.
3. Επιβεβαιώνουμε ότι ο τύπος της Λίστας Ανάκλησης Πιστοποιητικών είναι έγκυρος.
4. Επιβεβαιώνουμε αν η παρούσα χρονική στιγμή έχει τιμή μεταξύ των τιμών των πεδίων της Παρούσας Ενημέρωσης (thisUpdate) και της επομένης Ενημέρωσης (nextUpdate).
5. Εάν υπάρχει πεδίο για τον Αριθμό της Λίστας Ανάκλησης CRLNumber, επιβεβαιώνουμε ότι η τιμή του αριθμού της Λίστας Ανάκλησης είναι μεγαλύτερη από την τιμή του αριθμού της τελευταίας Λίστας Ανάκλησης την οποία έχει ο χρήστης.
6. Επιβεβαιώνουμε ότι το Όνομα του Αντικειμένου (subject name) στο πιστοποιητικό του εκδότη της Λίστας Ανάκλησης Πιστοποιητικών είναι ίδιο με το όνομα του εκδότη της Λίστας Ανάκλησης.
7. Αν υπάρχει το πεδίο προέκτασης της χρήσης του κλειδιού (keyUsage extension) στο πιστοποιητικό του εκδότη της Λίστας Ανάκλησης, πρέπει να περιέχει τη δυνατότητα υπογραφής λιστών ανάκλησης.
8. Ελέγχουμε αν ο σειριακός αριθμός του πιστοποιητικού (το οποίο θέλουμε να ελέγξουμε αν έχει ανακληθεί) βρίσκεται στη λίστα ανάκλησης. Αν βρίσκεται στη λίστα ανάκλησης ο χρήστης ενημερώνεται ότι το πιστοποιητικό έχει ανακληθεί και συνεπώς δεν ισχύει πλέον.

Κεφάλαιο 6

Κατάλογος X.500

Ένας Κατάλογος X.500 (X.500 Directory) είναι απαραίτητος για να μπορούν οι χρήστες να βρίσκουν την πληροφορία που χρειάζονται για την ασφαλή επικοινωνία και διεξαγωγή ηλεκτρονικού εμπορίου μέσα σε πιθανά εχθρικά περιβάλλοντα όπως είναι το παγκόσμιο διαδύκτιο (Internet).

Ο κατάλογος X.500 είναι μια ειδική κατανεμημένη βάση δεδομένων με ιεραρχικό σχήμα. Πολλοί κατάλογοι X.500 μπορούν να συνδεθούν μεταξύ τους για να σχηματίσουν ένα καθολικό κατάλογο απαραίτητης πληροφορίας για την διεξαγωγή ασφαλών επικοινωνιών. Μια υλοποίηση που αποτελείται από επιμέρους καταλόγους συνδεμένους καθολικά αποκαλείται "Directory". Ο καθολικός κατάλογος μπορεί να περιέχει διάφορα είδη πληροφορίας όπως για παράδειγμα ηλεκτρονικές διευθύνσεις (e-mail), τηλέφωνα, δημόσια κρυπτογραφικά κλειδιά και ψηφιακά πιστοποιητικά. Ένας μεμονωμένος κατάλογος X.500 μπορεί να είναι φυσικά κατανεμημένος (physically distributed) σε πολλά συστήματα που κάθε κομμάτι του να ανήκει και να διαχειρίζεται από διαφορετική χώρα ή οργανισμό. Επιπρόσθετη πληροφορία μπορεί να συμπεριληφθεί σε ένα κατάλογο X.500 για να τον προσαρμόσει σε ένα ειδικό περιβάλλον.

Οι κατάλογοι X.500 είναι επεκτάσιμοι, κατανεμημένοι, έχουν ιεραρχικό σχήμα, απαιτούν την πιστοποίηση του χρήστη (user authentication) και δίνουν την δυνατότητα αναζήτησης στο καθολικό κατάλογο.

Το όνομα "X.500" έχει υιοθετηθεί από το αντίστοιχο διεθνές πρότυπο το οποίο περιγράφει την χρήση και το σχεδιασμό του. Το X.500 standard [X.500] είναι μια συλλογή από πρότυπα του Διεθνούς Οργανισμού Προτύπων (ISO/International Standard Organization) τα οποία είναι συμφωνά με τις υποδείξεις της Διεθνούς Ένωσης

Επικοινωνιών (ICU/ International Communications Union). Επίσης προσδιορίζει μοντέλα για αποθήκευση δεδομένων και πρωτόκολλα για ανάκληση δεδομένων.

6.1 Αναπαράσταση πληροφορίας – Μοντελο δεδομένων του καταλόγου X.500

Ένα από τα κύρια έργα του X.500 ήταν να αναπτύξει μία δομή αντίστοιχη με τη δομή ενός οργανισμού, για να αποθηκεύσει την πληροφορία στη βάση δεδομένων του directory, που είναι γνωστή σαν "Directory Information Base" (DIB). Η δομή αυτή δίνει τη δυνατότητα της μοναδικής ονομασίας σε κάθε καταχώρηση του Καταλόγου χωρίς να χρειάζεται οι διαχειριστές (administrators) να συμβουλεύονται ο ένας τον άλλο. Μια δενδρική δομή, το "Directory Information Tree" (DIT), ήταν η λύση που έγινε αποδεκτή. Σε αυτήν την περίπτωση η ρίζα (root) είναι στην κορυφή και τα κλαδιά εκτείνονται προς τα κάτω. Δεν επιτρέπεται να κάνουμε καταχωρήσεις στη ρίζα του δένδρου. Τα υψηλότερα επίπεδα στο ιεραρχικό δένδρο περιλαμβάνουν τους οργανισμούς, τις χώρες ή τις κυβερνήσεις. Τα άτομα, οι servers, οι συσκευές (devices), οι εφαρμογές λογισμικού, οι διαδικασίες (processes), κ.τ.λ. είναι γνωστά ως «αντικείμενα» (objects) στο Directory Standard, και έχουν κάθε μια τη δική της καταχώρηση στο δένδρο. Κάθε object έχει χαρακτηριστικά πεδία (attributes) που περιγράφουν και δίνουν πληροφορία για το αντικείμενο της καταχώρησης. Μπορούν να οριστούν νέα χαρακτηριστικά πεδία και κλάσεις αντικειμένων από τον χρήστη. Οι χρήστες ή οτιδήποτε από τις υπόλοιπες καταχωρήσεις τυπικά αναπαριστάνονται ως φύλλα στο δένδρο.

Για να γίνει κατανοητή πλήρως η λειτουργικότητα ενός συστήματος καταλόγου X.500, πρέπει να γίνει κατανοητή η έννοια του διακεκριμένου ονόματος (DN/ Distinguished Name). Η καταχώρηση κάθε χρήστη στο Directory έχει ένα μοναδικό διακεκριμένο όνομα (DN). Αυτό δημιουργείται εάν συμπεριλάβουμε σε αυτό ένα χαρακτηριστικό πεδίο (attribute) το οποίο χαρακτηρίζει μοναδικά αυτό το αντικείμενο στον πραγματικό κόσμο. Για παράδειγμα:

cn= Γιώργος Γεωργίου, o=Βενιζέλειο, ou=Νοσοκομείο, st=Κρήτη, o=Τομέας Υγείας, c=GR

όπου

cn = common name (κοινό όνομα)
o = organization (οργανισμός)

ou= organizational unit (μονάδα οργανισμού)
st = state (περιοχή)
c = country (χώρα)

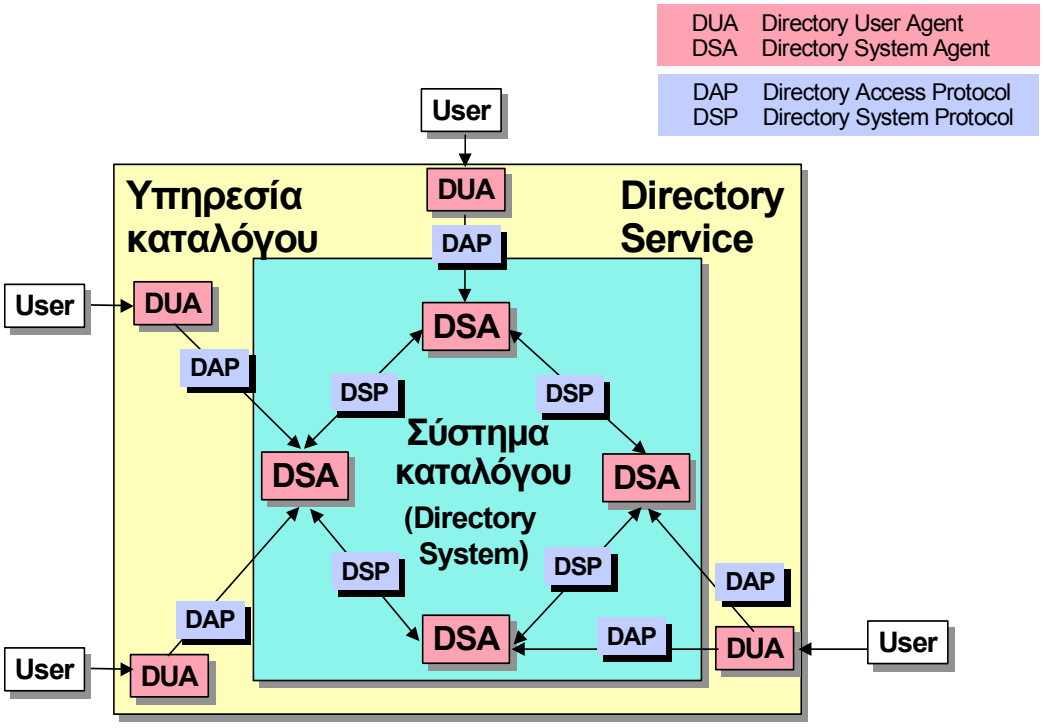
6.2 Κατανεμημένο μοντέλο λειτουργιών του Καταλόγου X.500

Η τεχνική δομή του X.500 Directory Service βασίζεται στο αρχιτεκτονικό μοντέλο του εξυπηρετητή/πελάτη (client-server). Ο χρήστης χρησιμοποιεί τον «Πράκτορα Καταλόγου του Χρήστη» DUA (Directory User Agent), μια εφαρμογή λογισμικού που βρίσκεται στον υπολογιστή του χρήστη (client computer), και δίνει στους χρήστες τη δυνατότητα να έχουν άμεση πρόσβαση στην πληροφορία που είναι αποθηκευμένη στον Κατάλογο. Ο εξυπηρετητής (server) της υπηρεσίας Καταλόγου είναι ο «Πράκτορας Καταλόγου του Συστήματος» DSA (Directory System Agent). Μεμονωμένες συλλογές ή υπό-τμήματα των δεδομένων που φυλάγονται σε ένα X.500 Directory, διαχειρίζονται από DSAs. Οι DSAs επικοινωνούν μεταξύ τους με το «Πρωτόκολλο του Συστήματος Καταλόγου» DSP (Directory System Protocol). Σε τελική ανάλυση οι DSAs παρέχουν ουσιαστικά στους χρήστες και στους διαχειριστές τις υπηρεσίες των καταλόγων (directory services). Γενικά, οι DSAs βρίσκονται σε ένα υπολογιστή, τον οποίο οι χρήστες δεν είναι ανάγκη να γνωρίζουν. Η επικοινωνία μεταξύ του DUA και του DSA γίνεται μέσω του "Directory Access Protocol" (DAP), ή της απλοποιημένης παραλλαγής του που είναι το Lightweight Directory Access Protocol (LDAP) [RFC1777]. Το τελευταίο μπορεί να χρησιμοποιηθεί για πελάτες (clients) σε δίκτυα που βασίζονται στο πρωτόκολλο TCP/IP όπως είναι το Internet ή τα Intranets. Η αρχιτεκτονική του καταλόγου φαίνεται στο Σχήμα 6.2.1.

Η πρόσβαση σε ένα X.500 Directory ως εξής:

Οι χρήστες μπορούν να έχουν πρόσβαση σε ένα καθολικό και κατανεμημένο Directory μέσω ενός μοναδικού σημείου πρόσβασης.

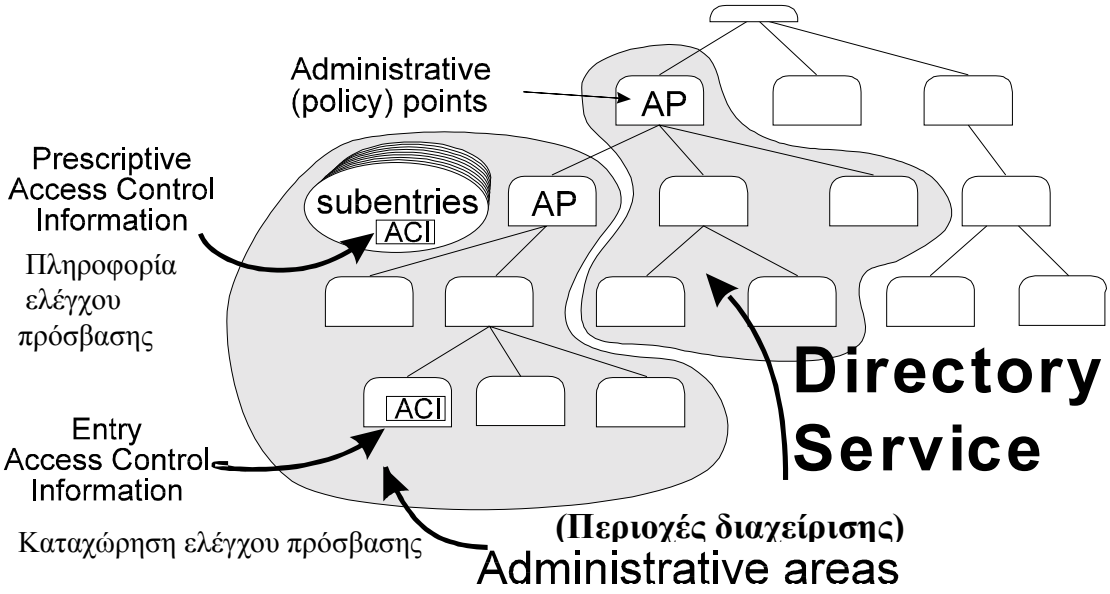
Όταν ένας χρήστης κάνει αίτηση στο Directory, ο DUA του χρήστη θα επικοινωνήσει με ένα συγκεκριμένο DSA και θα μεταφέρει την αίτηση χρησιμοποιώντας DAP ή LDAP. Εάν ο DSA έχει την πληροφορία τοπικά και μπορεί να ικανοποιήσει την αίτηση, θα το κάνει. Εάν ο DSA δεν μπορεί να ικανοποιήσει την αίτηση μπορεί να προωθήσει την αίτηση σε άλλο DSA χρησιμοποιώντας DSP (request chaining). Εναλλακτικά μπορεί να επιστρέψει στο DUA μια αναφορά (reference) σε ένα DSA, ο οποίος είναι πιθανό να έχει την πληροφορία που ζητήθηκε (request referral).



Σχήμα 6.2.1. Λειτουργικό μοντέλο του κατανεμημένου X.500 directory

Ο DSA πρέπει να υποστηρίζει όλους τους τύπους χαρακτηριστικών πεδίων (attributes) και τους κανόνες ταύτισης (matching rules) του X.520, και όλα τα καθορισμένα χαρακτηριστικά πεδία (defined attributes) του X.400 καθώς επίσης και πεδία που ορίζονται από τον χρήστη (user defined attributes). Επίσης υποστηρίζει τους κανόνες ταύτισης του X.521. Ο DSA υποστηρίζει επιπλέον όλες τις κλάσεις αντικειμένων (object classes) του X.521 καθώς επίσης και name forms, και πρέπει να έχει δυνατότητα να διαμορφώνεται (be configured) ώστε να υποστηρίζει κάθε κλάση αντικειμένων ή name form που ορίζεται από τον χρήστη ή είναι προκαθορισμένες (standard). Ο DSA πρέπει να υποστηρίζει το Σχήμα του Συστήματος (System Schema), όπως αυτό έχει οριστεί στα Directory Standards. Επειδή ο DSA έχει ευαίσθητη πληροφορία για το configuration στην δική του εσωτερική βάση δεδομένων, αυτή η πληροφορία πρέπει να προστατεύεται. Ο DSA πρέπει να υποστηρίζει τους standard τύπους της εξακρίβωσης ταυτότητας (authentication); την απλή εξακρίβωση ταυτότητας (όνομα και κωδικός πρόσβασης), την ισχυρή μέθοδο εξακρίβωσης ταυτότητας (strong

authentication), και λειτουργίες για υπογραφή (αιτήματα και αποτελέσματα των οποίων η προέλευση και η ακεραιότητα είναι εγγυημένα). Πρέπει να υποστηρίζεται έλεγχος πρόσβασης (access control) όπως προσδιορίζεται για τον Κατάλογο. Οι πολιτικές ελέγχου πρόσβασης είναι εφαρμόσιμες μέσα σε μια "Διοικητική Περιοχή" (Administrative Area), ένα μέρος όπου τα λειτουργικά χαρακτηριστικά πεδία (operational attributes) για να εκτελεστεί η Πληροφορία για Εντεταλμένο Έλεγχο Πρόσβασης (Prescriptive Access Control Information) αποθηκεύονται σε ειδικές καταχωρήσεις, που συνδέονται με τις Διοικητικές Καταχωρήσεις (Administrative Entries) στο υψηλότερο μέρος της Διοικητικής Περιοχής (Administrative Area).



Σχήμα 6.2.2. Το μοντέλο διοικητικής περιοχής (Administrative Model)

6.3 Χρήση του καταλόγου X.500 σε σύστημα ασφαλείας

Για να κρυπτογραφηθεί πληροφορία και να σταλθεί με ασφάλεια σε κάποιον άλλον χρήστη, πρέπει να υπάρχει πρόσβαση στο πιστοποιητικό δημοσίου κλειδιού του παραλήπτη.

Οι κατάλογοι X.500 μπορούν να χρησιμοποιηθούν για την αποθήκευση πιστοποιητικών δημοσίων κλειδιών κρυπτογράφησης και δημόσιας πληροφορίας για τους κατόχους των πιστοποιητικών.

Ο Κατάλογος X.500 χρησιμοποιείται ευρέως για την αποθήκευση και την εύρεση των πιστοποιητικών δημοσίων κλειδιών. Κατά την επιβεβαίωση της εγκυρότητας ενός πιστοποιητικού, ο χρήστης πρέπει να ελέγξει ότι το πιστοποιητικό δεν έχει ανακληθεί. Για αυτό τον λόγο στον Κατάλογο X.500 αποθηκεύουμε επίσης και τη Λίστα Ακύρωσης Πιστοποιητικών (CRL) η οποία μας λεει ποια πιστοποιητικά έχουν αποσυρθεί. Ο Κατάλογος επίσης χρησιμοποιείται για να εκδίδει γενική πληροφορία που αφορά την Αρχή Πιστοποίησης (CA) στο κοινό.

Σε μια Υποδομή Ασφαλείας Δημοσίου Κλειδιού PKI οι κατάλογοι (directories) παρέχουν ασφαλή αποθήκευση και διάθεση στο κοινό των παρακάτω δεδομένων:

1. Πιστοποιητικά δημόσιων και ιδιωτικών κλειδιών για να είναι δημοσίως προσβάσιμα
2. Λίστες Ανάκλησης Πιστοποιητικών για να είναι διαθέσιμες σε όλους τους χρήστες
3. Πληροφορίες που ενημερώνουν τους χρήστες σχετικά με τις Αρχές Πιστοποίησης και τους χώρους αποθήκευσης τους (repositories)
4. Οδηγίες προς τους χρήστες για πρόσβαση, πολιτική και χρέωση

Κεφάλαιο 7

Τεχνολογία Έξυπνων Καρτών

Οι έξυπνες κάρτες (smartcards) αναμένεται, ότι θα γίνουν τόσο σημαντικές στο μέλλον όσο είναι σήμερα οι υπολογιστές [SSDD]. Στην ουσία οι έξυπνες κάρτες είναι μικροί υπολογιστές. Σε αυτό το κεφάλαιο θα περιγράψουμε την ιστορία των έξυπνων καρτών, τους διάφορους τύπους καρτών που υπάρχουν, τις ιδιότητες τους, τα πρότυπα (standards) που επηρεάζουν την υιοθέτηση τους, και πώς αυτές σχετίζονται με τα σημερινά συστήματα ασφαλείας των υπολογιστών.

Επειδή οι έξυπνες κάρτες είναι στην ουσία μικροσκοπικοί υπολογιστές, είναι δύσκολο να προβλέψουμε το πλήθος των εφαρμογών που θα υλοποιούνται με τη χρήση τους. Είναι πολύ πιθανό ότι οι έξυπνες κάρτες θα έχουν την ίδια ραγδαία εξέλιξη σε υπολογιστική ισχύ με τους υπολογιστές, και κάθε δεκαοκτώ μήνες θα διπλασιάζονται οι επιδόσεις τους ενώ θα υποδιπλασιάζεται το κόστος τους [SSDD].

Οι έξυπνες κάρτες είναι πολύ χρήσιμες σαν 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 μετρητού χρήματος. Μπορούν να περιέχουν διάφορα πιστοποιητικά για αναγνώριση της ταυτότητας μας και να χρησιμοποιηθούν οπουδήποτε είμαστε και σε οποιοδήποτε δίκτυο έχουμε συνδεθεί ως αποδεικτικό ταυτότητας.

Οι έξυπνες κάρτες έχουν το μέγεθος και το σχήμα των πιστωτικών καρτών, αλλά περιέχουν μικροεπεξεργαστή και μνήμη. Αυτά τα δύο στοιχεία επιτρέπουν τη αποθήκευση και επεξεργασία πληροφορίας στην κάρτα.

Η έξυπνη κάρτα έχει 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.

Μερικές κάρτες έχουν μόνο μνήμη; μια εφαρμογή μπορεί να αυξήσει ή να μειώσει μετρητές στην κάρτα. Αυτές οι κάρτες αναφέρονται ως κάρτες μνήμης (memory cards) [IBMSC].

Μόνο αυτές οι κάρτες που περιέχουν μικροεπεξεργαστή είναι στην ουσία έξυπνες κάρτες.

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).

Δεν υπάρχουν μπαταρίες στην έξυπνη κάρτα. Ηλεκτρική ενέργεια παρέχεται εξωτερικά από την συσκευή ανάγνωσης, είτε αυτή είναι επαφής είτε όχι. Επίσης και ο χρονισμός της CPU παρέχεται από τη συσκευή ανάγνωσης.

Τα δύο κύρια χαρακτηριστικά των έξυπνων καρτών είναι η ασφάλεια και η φορητότητα. 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 πάνω στην κάρτα.

Οι έξυπνες κάρτες χρησιμοποιούνται σε μια μεγάλη ποικιλία εφαρμογών:

- Αυτόνομη συλλογή εισιτηρίων στα λεωφορεία, τρένα και αεροπλάνα
- Οικονομικές συναλλαγές
- Ηλεκτρονικό χρηματικό κεφάλαιο (electronic purse) [IBMSC]

- Βιομετρική αναγνώριση ταυτότητας (biometric identification)
- Έλεγχος πρόσβασης
- Τηλέφωνα

Κυβερνητικές, οικονομικές, μεταφορικές, τηλεπικοινωνιακές, εκπαιδευτικές υπηρεσίες και υπηρεσίες περίθαλψης πρόκειται να χρησιμοποιήσουν ή χρησιμοποιούν ήδη έξυπνες κάρτες ως μέσα παροχής καλύτερης ασφάλειας και βελτιωμένες υπηρεσίες στους πελάτες και στους χρήστες τους.

7.1 Ιστορία των έξυπνων καρτών

Το 1968, οι γερμανοί εφευρέτες Jurgen Dethloff και Helmut Grotrupp δημιούργησαν την πρώτη κάρτα με ολοκληρωμένο κύκλωμα (ICC/ integrated circuit card). Παρόμοιες εφαρμογές ακολούθησαν στην Ιαπωνία το 1970 και στη Γαλλία το 1974. Το 1984, η Γαλλική Υπηρεσία Ταχυδρομείων και Τηλεπικοινωνιών PTT (Postal and Telecommunications services) εισήγαγε δοκιμαστικά τις τηλεκάρτες. Έως το 1986, είχαν κυκλοφορήσει εκατομμύρια γαλλικές τηλεκάρτες. Ο αριθμός τους έφτασε σχεδόν τα 60 εκατομμύρια το 1990, και τα 150 εκατομμύρια το 1996 [IBMSC].

Οι εξελίξεις τα τελευταία χρόνια στην μοντέρνα κρυπτογραφία, οι οποίες έδωσαν τη δυνατότητα σε έξυπνες κάρτες να έχουν υψηλό βαθμό ασφαλείας, έκαναν τις τραπεζικές επιχειρήσεις να πάρουν στα σοβαρά τις έξυπνες κάρτες. Οι άλλες υπηρεσίες, όπως της υγείας, της εκπαίδευσης, των τηλεπικοινωνιών και των μεταφορών έχουν ήδη αρχίσει να χρησιμοποιούν έξυπνες κάρτες. Οι Γαλλικές τράπεζες παρουσίασαν πρώτες τραπεζική κάρτα με ενσωματωμένο μικροεπεξεργαστή το 1984. Μια άλλη εφαρμογή που έλαβε μέρος στη Γερμανία έκανε χρήση 70 εκατομμυρίων έξυπνων καρτών που περιείχαν πληροφορία ιατρικής ασφάλισης [IBMSC]. Καθώς προχωράμε στον 21^{ο} αιώνα, οι έξυπνες κάρτες θα έχουν πολύ βασικό ρόλο στην ηλεκτρονική επιχειρησιακή δραστηριότητα, γιατί είναι αποδεδειγμένα ένα ιδανικό μέσο για την ασφαλή αποθήκευση κρυπτογραφικών κλειδιών και αλγορίθμων.

7.2 Τύποι έξυπνων καρτών

Το πρότυπο ISO/IEC 7810 [ISO 7810] για «Κάρτες Αναγνώρισης Ταυτότητας – Φυσικά Χαρακτηριστικά» από το Διεθνή Οργανισμό Τυποποίησης (ISO/ International Organization for Standardization) προσδιορίζει τις φυσικές ιδιότητες όπως την ευκαμψία, την αντοχή στην θερμοκρασία, και τις διαστάσεις για τρία διαφορετικά είδη καρτών (ID-1, ID-2, και ID-3). Το πρότυπο για έξυπνες κάρτες, ISO 7816 [ISO 7816], βασίζεται στο format ID-1. Με στόχο να δώσουμε μια ευρύτερη εικόνα θα περιγράψουμε διάφορους τύπους καρτών του τύπου ID-1. Θα επικεντρωθούμε ιδιαίτερα στις κρυπτογραφικές κάρτες με συνεπεξεργαστή γιατί είναι πολύ σημαντικές για τα συστήματα ασφαλείας των υπολογιστικών συστημάτων και δικτύων.

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). Ο όρος «έξυπνη κάρτα» χρησιμοποιείται κυρίως για τις κάρτες με μικροεπεξεργαστή. Αυτές είναι οι πιο καινούργιες και πιο έξυπνες της οικογένειας των ID-1, που ακολουθούν τις προδιαγραφές του ISO 7816. Αυτοί οι τύποι κάρτας δίνουν τη δυνατότητα να έχουμε πολύ μεγαλύτερο χώρο για αποθήκευση δεδομένων, καθώς κάρτες τέτοιου τύπου, με μνήμη πάνω από 64 Kbytes, είναι ήδη διαθέσιμες. Το σημαντικότερο είναι το γεγονός ότι τα αποθηκευμένα δεδομένα μπορούν να προστατευθούν από μη εξουσιοδοτημένη πρόσβαση και παραποίηση τους. 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 (hardware).

7.2.1 Κάρτες μνήμης (memory cards)

Αν και αναφέρονται ως έξυπνες κάρτες, οι κάρτες μνήμης είναι τυπικά πολύ φθηνότερες και πολύ λιγότερο λειτουργικές από τις κάρτες με μικροεπεξεργαστή. Η απλή τεχνολογία τους, τους δίδει την δυνατότητα να κατασκευάζονται πολύ φθηνά και να κοστίζουν κάτω από US $1 η μία, σε μεγάλες ποσότητες. Περιέχουν μνήμη EEPROM και ROM, καθώς επίσης και κάποια λογική για ασφάλεια και για διευθυνσιοδότηση. Στα απλούστερα μοντέλα, υπάρχει λογική για να εμποδίζει την εγγραφή και την διαγραφή των δεδομένων. Τα πιο περίπλοκα μοντέλα δίνουν τη δυνατότητα να έχουμε περιορισμένη πρόσβαση για ανάγνωση (restricted read access). Η μνήμη της κάρτας για

την αποθήκευση δεδομένων ποικίλει από λίγα εκατοντάδες bytes έως 8 KB. Τυπική εφαρμογή των καρτών μνήμης είναι οι τηλεκάρτες και οι κάρτες για ιατρική ασφάλιση [IBMSC].

7.2.2 Κάρτες με μικροεπεξεργαστή (Microprocessor cards)

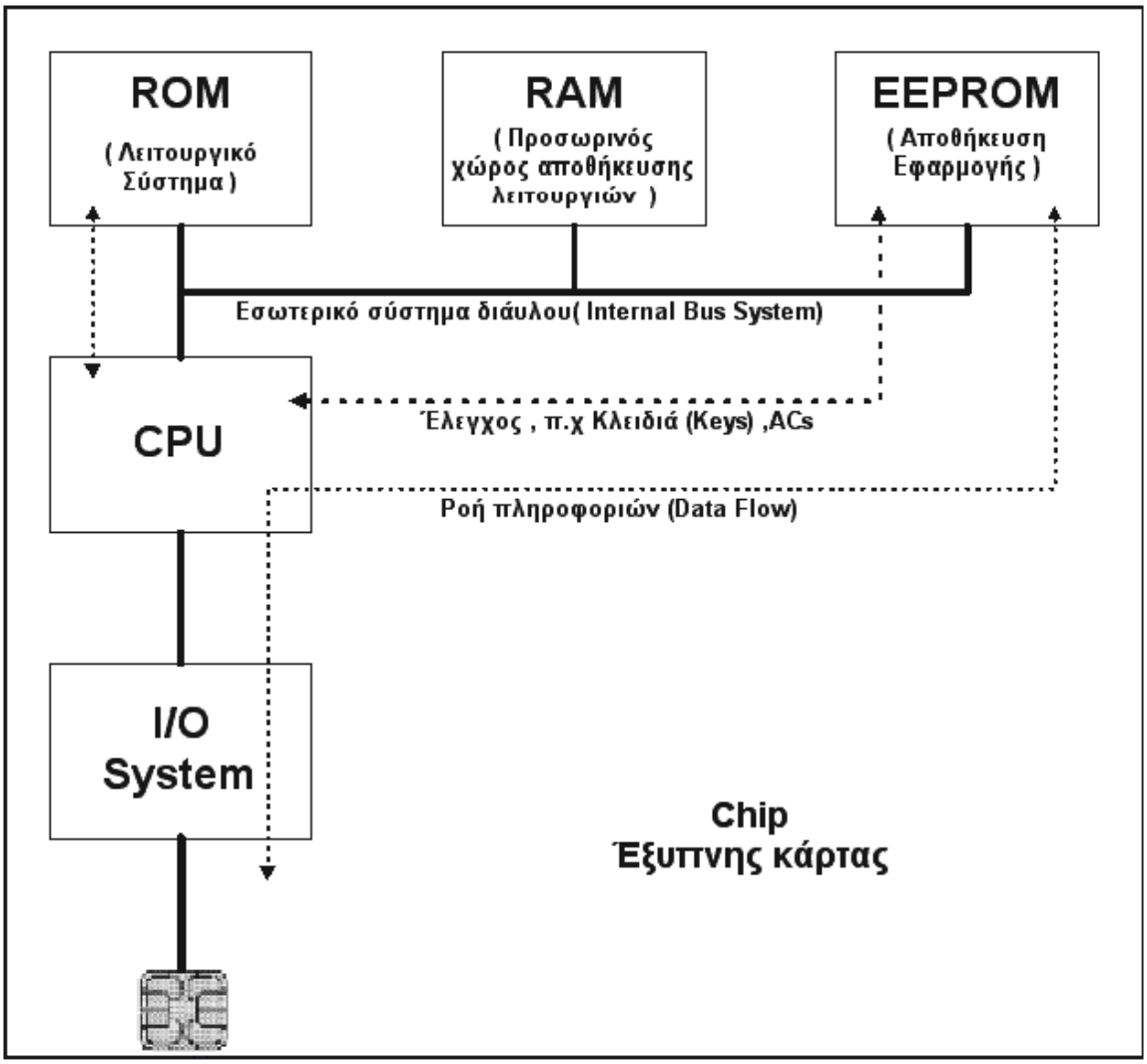
Οι κάρτες με μικροεπεξεργαστή έχουν CPU, RAM, ROM και EEPROM. Έχουν δυνατότητα ανάγνωσης/ εγγραφής καθώς και υψηλή ασφάλεια που επιτυγχάνεται με τον μικροεπεξεργαστή. Είναι πιο ακριβές από τις κάρτες μνήμης και κοστίζουν περίπου μεταξύ US $5–15. Το λειτουργικό σύστημα είναι αποθηκευμένο στη ROM, η CPU 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	9600BPS

ΠΙΝΑΚΑΣ 7.2.2. ΤΥΠΙΚΗ ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΈΞΥΠΝΩΝ ΚΑΡΤΩΝ

Η CPU των έξυπνων καρτών είναι συνήθως ένας μικροεπεξεργαστής 8-bit. Η RAM παρέχει χώρο εργασίας για την CPU. Συνήθως 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 προσδιορισμό (specification) 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 κρατάει 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.



Σχήμα 7.2.2.1. Αρχιτεκτονική έξυπνων καρτών

Η είσοδος/ έξοδος (I/O) χρησιμοποιείται για να μεταφέρονται δεδομένα σειριακά, κατά bit. Η διαδεδομένη ταχύτητα είναι 9600 bits/sec.

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

7.2.3 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 και στην λειτουργικότητα. Επειδή οι κοινοί ασύμμετροι κρυπτογραφικοί αλγόριθμοι (όπως ο RSA) απαιτούν πάρα πολλούς 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 στην τάξη των 100 μικροδευτερολέπτων. 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 καθώς οι μικροεπεξεργαστές χρησιμοποιούνται ευρέως. Παρά το υψηλό κόστος, τα πλεονεκτήματα που προσφέρει η προσθήκη του μικροεπεξεργαστή στη ασφάλεια των συστημάτων είναι τεράστια, γιατί το ιδιωτικό κλειδί δεν χρειάζεται ποτέ να απομακρυνθεί από την έξυπνη κάρτα. Όπως θα δούμε και παρακάτω, αυτό γίνεται ένας κρίσιμος παράγοντας 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 αυτού του τύπου των καρτών θα μειωθεί. Οι βασικοί επεξεργαστές θα γίνουν αρκετά ισχυροί για να εκτελούν εντατικούς μαθηματικούς υπολογισμούς, ή θα διαδοθούν ευρέως οι αλγόριθμοι που βασίζονται στην τεχνολογία των ελλειπτικών καμπυλών. Οι αλγόριθμοι των ελλειπτικών καμπυλών (Elliptic Curves) παρέχουν ισχυρή ασφάλεια χωρίς να χρειάζεται μεγάλοι υπολογισμοί ακεραίων, αλλά δεν έχει βρεθεί ακόμα τρόπος για να χρησιμοποιηθούν ευρέως [IBMSC].

7.2.4 Έξυπνες κάρτες άνευ επαφής (contactless smart cards)

Αν και η αξιοπιστία των έξυπνων καρτών που δουλεύουν με επαφή έχει βελτιωθεί πάρα πολύ τα τελευταία χρόνια, τα σημεία επαφής είναι ένα από τα πιο συχνά σημεία αποτυχίας κάθε ηλεκτρονικού μέσου που οφείλεται στην ακαθαρσία και την φθορά λόγω της συχνής χρήσης. Οι έξυπνες κάρτες άνευ επαφής λύνουν αυτό το πρόβλημα και επίσης παρέχουν ενδιαφέρουσες καινούργιες δυνατότητες κατά την χρήση. Οι κάρτες δεν χρειάζονται πλέον να εισαχθούν στην συσκευή ανάγνωσης, πράγμα που βολεύει τους τελικούς χρήστες. Αυτές οι κάρτες είναι κατάλληλες για εφαρμογές που απαιτούν μεγαλύτερη ταχύτητα συναλλαγής από αυτή που προσφέρουν οι κάρτες με επαφή, όπως στα μέσα μαζικής μεταφοράς ή στον έλεγχο πρόσβασης σε κτίρια. Το κόστος αυτών των καρτών είναι υψηλότερο και δεν υπάρχει ακόμα αρκετή εμπειρία για να κάνει την τεχνολογία αυτή αρκετά αξιόπιστη.

7.2.5 Οπτικές μνημονικές κάρτες (optical memory cards)

Τα πρότυπα για τις οπτικές κάρτες μνήμης είναι τα ISO/IEC 11693 [ISO 11693] και 11694 [ISO 11694-1]. Αυτές οι κάρτες μπορούν να αποθηκεύσουν από 1,6 έως 40 megabytes δεδομένων (οι συνηθισμένες 4), αλλά γράφονται μόνο μια φορά και δεν μπορούν να σβηστούν με την σημερινή τεχνολογία. 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. Αν και οι συσκευές ανάγνωσης και γραφής αυτών των καρτών είναι ακόμα πολύ ακριβές, οι κάρτες αυτές μπορούν να χρησιμοποιηθούν για ιατρικές εφαρμογές όπου μεγάλες ποσότητες δεδομένων πρέπει να αποθηκευτούν, όπως για παράδειγμα οι ακτινογραφίες ενός ασθενή.

7.2.6 Υβριδικές κάρτες (hybrid cards)

Αυτές οι κάρτες έχουν κατάλληλη διεπιφάνεια για να λειτουργήσουν και ως κάρτες που λειτουργούν με επαφή (contact) και ως κάρτες άνευ επαφής (contactless). Η διεπιφάνεια επαφής χρησιμοποιείται από τον μικροεπεξεργαστή και η διεπιφάνεια άνευ επαφής χρησιμοποιείται από το chip της μνήμης. Δεν υπάρχει φυσική σύνδεση ανάμεσα στα δύο αυτά chips και για αυτό δεν διατίθεται μνήμη που να διαμοιράζεται μεταξύ των δύο αυτών chip.

Τεχνολογία καρτών	Μνήμη	Ασφάλεια μνήμης	Κόστος
Κάρτα μνήμης	Έως 8 Kbytes (R/W)	Προστασία από εγγραφή και διαγραφή	Κάρτες πολύ φτηνές
			Συσκευή ανάγνωσης/ εγγραφής φθηνή
Κάρτα με μικροεπεξεργαστή	Έως 64 Kbytes (R/W)	Περιορισμός πρόσβασης (PIN)	Κάρτα από μεσαίο κόστος έως ακριβή
		Δυνατότητες κρυπτογράφησης	Συσκευή ανάγνωσης/ εγγραφής πολύ φθηνή
Οπτική κάρτα	60 Mbytes (WORM)	Περιορισμός πρόσβασης (σε εξελιγμένα μοντέλα)	Κάρτα φτηνή
			Συσκευή ανάγνωσης/ εγγραφής πολύ ακριβή

ΠΙΝΑΚΑΣ 7.2.6. ΤΕΧΝΟΛΟΓΙΑ ΚΑΙ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΑΡΤΩΝ

7.3 Κατασκευαστές έξυπνων καρτών

Η παρακάτω πληροφορία είναι για ενημερωτικούς σκοπούς και αναφέρει μερικούς από τους κατασκευαστές και τους προμηθευτές έξυπνων καρτών :

7.3.1 Κατασκευαστές Chip

- Atmel (www.amtel.co.uz)
- Hitachi (www.nsa-hitachi.com)
- Mikron (www.micron.net)
- Motorola (www.motor.com)
- NEC (www.nec.com)
- Oki (www.oki.org)
- Philips (www.philips.com)
- ST Microelectronics (www.protel.com)

- Siemens (www.sni.com)

7.3.2 Κατασκευαστές καρτών

- Bull CP8 (www.cp8.bull.gr)
- De La Rue Card Systems (www.delarue.com)
- Gemplus (www.gemplus.com)
- G&D (Giesecke & Devrient GmbH) (www.gdm.de)
- IBM (www.chipcard.ibm.com)
- Oberthur (www.oberthur)
- ODS (www.ods.com)
- Orga (www.orga.com)
- Schlumberger (ww.slb.com)
- Toshiba (www.toshiba.com)

7.4 Το Λειτουργικό σύστημα των έξυπνων καρτών

Ο πυρήνας της έξυπνης κάρτας είναι το λειτουργικό της σύστημα. Αυτός είναι ο κώδικας που διαχειρίζεται το σύστημα αρχείων, την ασφάλεια, την είσοδο/ έξοδο (I/O), και την διαχείριση διάφόρων άλλων εφαρμογών. Είναι παρόμοιο με το λειτουργικό σύστημα των PCs, με τη διαφορά ότι είναι περιορισμένο σε λίγες χιλιάδες bytes.

Τα πιο γνωστά λειτουργικά συστήματα είναι :

- Bull : SmartTB, CC, Odyssey I (Javacard) (www.cp8.bull.gr)
- DeLaRue : DS, DX, DXPLUS, CC, Mondex Card, JavaCard (www.delarue.com)
- Gemplus : 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) (ww.slb.com)
- Siemens : Card OS (www.sni.com)

Υπάρχουν περιπτώσεις εταιριών που πληρώνουν άδεια (license) για λειτουργικά συστήματα καρτών άλλων κατασκευαστών, και τα επεκτείνουν ή μετατρέπουν εντολές και εφαρμογές. Για παράδειγμα, η Gemplus και η Schlumberger εκμισθώνουν το MFC της IBM.

7.5 Πρότυπα, προδιαγραφές και διεπιφάνειες προγραμματισμού εφαρμογών έξυπνων καρτών (Standards, Specifications and smart card application programming interface)

Οι έξυπνες κάρτες συνήθως είναι ένα μικρό μέρος ενός πολύ πιο σύνθετου συστήματος. Χωρίς κάποια πρότυπα, προϊόντα διαφορετικών κατασκευαστών δεν θα συνεργάζονταν. Συνεπώς τα συστήματα καρτών δεν θα γινόταν αποδεκτά από τους χρήστες.

Το να περιγράψουμε εδώ όλα τα πρότυπα που υπάρχουν δεν είναι εφικτό. Θα περιγράψουμε τα πιο σπουδαία πρότυπα, και αυτά τα οποία έχουν περισσότερη σχέση με το θέμα της ασφάλειας των ιατρικών δικτύων.

7.5.1 Γενικά πρότυπα έξυπνων καρτών (Smart Card Standards)

Υπάρχουν πολλά πρότυπα, προδιαγραφές (specifications) και υποδείξεις (recommendations) για έξυπνες κάρτες. Κάποια από αυτά τα πρότυπα είναι διεθνών οργανισμών όπως ο ISO. Κάποια άλλα προέρχονται από βιομηχανικούς οργανισμούς και άλλα από εταιρίες.

Μπορούμε να κατηγοριοποιήσουμε τα πρότυπα στις παρακάτω ομάδες βασιζόμενοι στους πρότυπους οργανισμούς :

- Τα πρότυπα του Διεθνή Οργανισμού Προτύπων (ISO) :
  - ISO 7810: plastic ID cards, dimensions [ISO 7810]
  - ISO 7811: Parts 1-6: ID cards [ISO 7811]
  - ISO 7816: Parts 1-8: contact integrated circuit (IC) cards [ISO7816]

- Τα πρότυπα των χωρών και των βιομηχανιών. Μερικά από αυτά δεν είναι πρότυπα έξυπνων καρτών, αλλά χρησιμοποιούνται από εφαρμογές που τρέχουν σε έξυπνες κάρτες.
  - CCITT X.509: Directory for certificates (Κατάλογος για πιστοποιητικά)
  - EN726 Parts 1-7: for telecommunications IC cards and terminals (IC κάρτες τηλεπικοινωνιών και τερματικά)
  - ANSI (US Standard body) X9 series: for digital signature, secure hash, RSA, and data encryption algorithms (Αλγόριθμους για ψηφιακή υπογραφή, ασφαλή κατακερματισμό, RSA, κρυπτογράφησης δεδομένων)
  - US Government standards:
    - FIPS-46: Data Encryption Standards (Πρότυπα για κρυπτογράφηση δεδομένων)
    - FIPS-81: DES Modes of Operation (Καταστάσεις λειτουργίας του DES)
    - FIPS-180-1: Secure Hash Standards (SHA-1) (Πρότυπα ασφαλούς κατακερματισμού)
    - FIPW-186: Digital Signature Standards (DSS) (Πρότυπα ψηφιακής υπογραφής)
  - GSM 11.11-11.12: European digital cellular telecommunications system (Ευρωπαϊκές ψηφιακές κυψελοειδείς επικοινωνίες)
  - Europay, Mastercard, and Visa (EMV) Parts 1-3 : IC card specification for payment systems (Προσδιορισμός της IC κάρτας για συστήματα πληρωμής)
  - International Airline Transportation Association (IATA) Resolution 791: using smart card for electronic ticketing (Χρήση της έξυπνης κάρτας ως ηλεκτρονικό εισητήριο)
  - PC/SC: specification for connection of smart card readers to PCs running Windows operating system (Προσδιορισμός για την σύνδεσης

συσκευών ανάγνωσης έξυπνων καρτών στο λειτουργικό σύστημα των Windows) [PC/SC]

- G7: International health organization for health card (Διεθνής οργανισμός για έξυπνες κάρτες)
- Opencard Framework: architecture specification framework for terminals and cards (Προσδιορισμός αρχιτεκτονικής για τερματικά και κάρτες) [OpenCard]
- JavaCard: Specification for JAVA virtual machine (Προσδιορισμός για την ιδεατή μηχανή της JAVA)

7.5.2 Πρότυπο ISO7816

Το πρότυπο ISO 7816 [ISO7816] του Διεθνούς Οργανισμού Προτύπων (International Organization for Standardization/ISO) είναι ένα σύνολο από οκτώ έγγραφα που περιγράφουν τις φυσικές ιδιότητες των καρτών με ολοκληρωμένο κύκλωμα. Το ISO 7816 είναι η συνέχεια των προτύπων ISO 7810, 7811, 7812 και 7813 τα οποία έθεσαν τη βάση για τις κάρτες πιστοποίησης ταυτότητας (identification card) "μεγέθους πιστωτικής κάρτας" τύπου ID-1. Η κάρτα μεγέθους ID-1 είχε χρησιμοποιηθεί ήδη πριν από καιρό για πιστωτικές κάρτες, κάρτες τραπέζης κ.τ.λ.

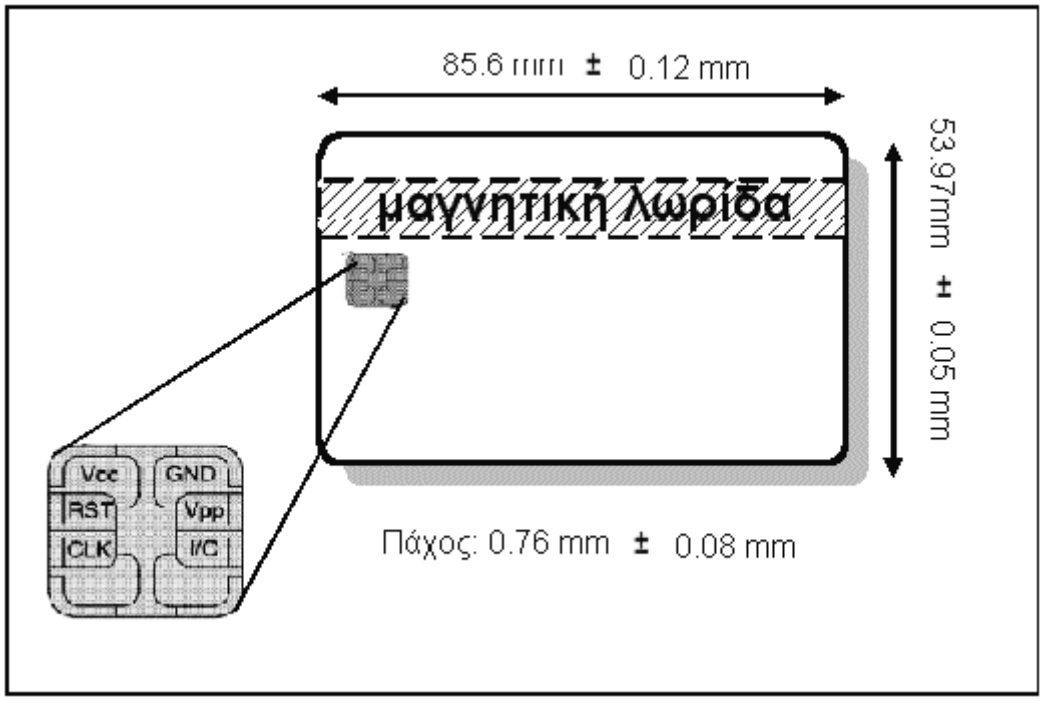
Η καθιέρωση προτύπων για τις έξυπνες κάρτες άρχισε το 1983 και η πρώτη από τις προδιαγραφές (specifications) του ISO 7816 βγήκε το 1987. Η όγδοη βγήκε το 1998 και γίνεται δουλειά ακόμα για να υπάρξουν νέες εκδόσεις της.

Η ομάδα των εγγράφων που ονομάζεται "ISO 7816 Κάρτες πιστοποίησης ταυτότητας – Κάρτες ολοκληρωμένου κυκλώματος με επαφές" (ISO 7816 Identification Cards – Integrated Circuit(s) Cards with Contacts) αποτελείται από τα εξής μέρη:

- Μέρος 1: Φυσικά χαρακτηριστικά (Physical characteristics) (βλ. Σχήμα 7.5.2)
- Μέρος 2: Διαστάσεις και θέση των επαφών (Dimensions and location of the contacts)
- Μέρος 3: Ηλεκτρονικά σήματα και πρωτόκολλα μετάδοσης (Electronic signals and transmission protocols)
- Μέρος 4: Εντολές για ανταλλαγή (Inter-industry commands for interchange)

- Μέρος 5: Σύστημα αρίθμησης και διαδικασία καταχώρησης για τα αναγνωριστικά των εφαρμογών (Numbering system and registration procedure for application identifiers)
- Μέρος 6: Στοιχεία δεδομένων (Inter-industry data elements)
- Μέρος 7: Εμπλουτισμένες εντολές (Enhanced inter-industry commands)
- Μέρος 8: Αρχιτεκτονική ασφάλειας (Inter-industry security architecture)

Η πλειοψηφία των έξυπνων καρτών στην αγορά ακολουθεί τα μέρη 1,2 και 3 του πρότυπου ISO 7816.



Σχήμα 7.5.2. ISO 7816-2 Διαστάσεις και θέση επαφών της κάρτας

7.5.3 PC/SC (Personal Computer/Smart Card)

Η ομάδα καθορισμού του πρότυπου PC/SC [PC/SC] ιδρύθηκε το Μάη του 1996 για να ορίσει τις προδιαγραφές για τις έξυπνες κάρτες και της συσκευές ανάγνωσης τους, που θα χρησιμοποιούνταν με υπολογιστές PC. Η Microsoft κατέχει και διατηρεί τις προδιαγραφές του προτύπου PC/SC.

Η ομάδα του PC/SC τυποποίησε τρεις περιοχές:

- Την διεπιφάνεια των τερματικών έξυπνων καρτών στο PC (Interfacing of card terminals). Τα οποία είναι γνωστά στο PC/SC specification ως Interface Device ή IFD
- Την διεπιφάνεια υψηλού επιπέδου προγραμματισμού εφαρμογών (high-level application programming interface) για να έχουμε διαλειτουργικότητα στην πρόσβαση των έξυπνων καρτών
- Τους μηχανισμούς που επιτρέπουν πολλαπλές εφαρμογές να μοιράζονται αποτελεσματικά τους πόρους (resources) μίας μοναδικής κάρτας ολοκληρωμένου κυκλώματος (Integrated Circuit Card /ICC) και ενός IFD (Interface Device)

Οι τελικές προδιαγραφές (specifications) του PC/SC ανακοινώθηκαν τον Απρίλιο του 1998 στο συνέδριο CardTech/Securtech. Χωρίζονται σε οκτώ μέρη. Δίνουμε παρακάτω μια σύντομη περίληψη του κάθε μέρους [PS/SC]:

- Μέρος 1: Παρέχει μια περίληψη της αρχιτεκτονικής του συστήματος και των συστατικών μερών του
- Μέρος 2: Λεπτομερής περιγραφή των χαρακτηριστικών των ICC-IFD που ακολουθούν το πρότυπο και απαιτήσεις διαλειτουργικότητας
- Μέρος 3: Περιγράφει τη διεπιφάνεια (interface) για τις συσκευές IFD και την απαιτούμενη λειτουργικότητα αυτών των συσκευών
- Μέρος 4: Μελέτη σχεδιασμού των συσκευών IFD
- Μέρος 5: Περιγράφει τις διεπιφάνειες και την λειτουργικότητα που υποστηρίζει ο Διαχειριστής Πόρων του ICC (ICC Resource Manager)
- Μέρος 6: Περιγράφει το μοντέλο του ICC παροχέα υπηρεσιών (ICC Service Provider)
- Μέρος 7: Περιγράφει μελέτες για ανάπτυξη λογισμικού

- Μέρος 8: Περιγράφει την λειτουργικότητα των ICCs που έχουν κρυπτογραφική υποστήριξη

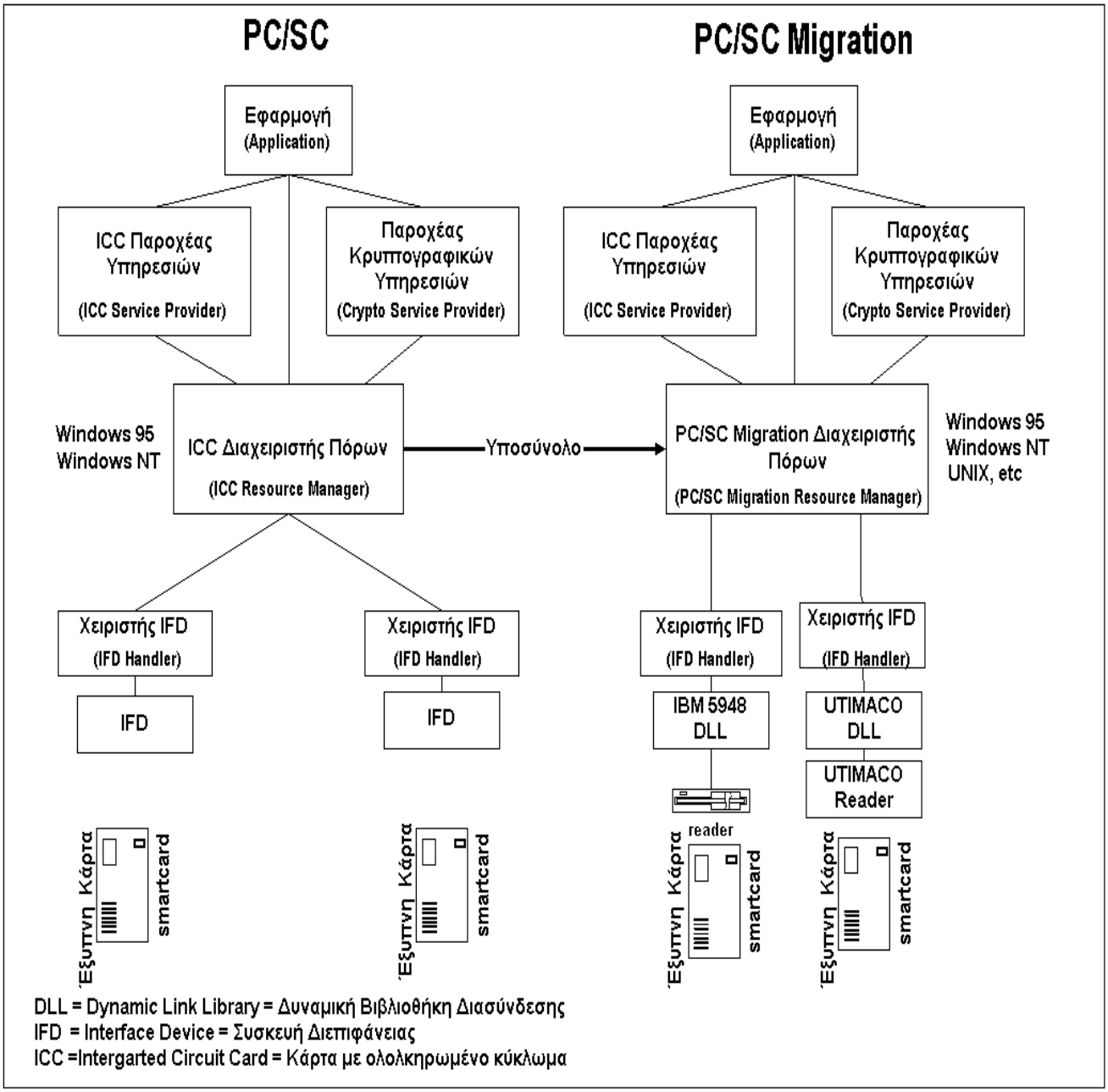
Η Microsoft έχει εκδώσει μια ολοκληρωμένη λίστα των συσκευών ανάγνωσης έξυπνων καρτών που ακολουθούν το πρότυπο PC/SC στο web site της [PC/SC].

7.5.3.1 PC/SC Migration Interface

Το PC/SC Migration Interface δίνει την δυνατότητα στον υπεύθυνο ανάπτυξης εφαρμογών να γράψει στο PC/SC Interface specification και να χρησιμοποιήσει τις ισοδύναμες υπηρεσίες σε ένα περιβάλλον που δεν έχει λειτουργικό Windows. Ο κατασκευαστής της συσκευής ανάγνωσης πρέπει να παρέχει τον οδηγό για το υλικό (hardware driver) ο οποίος δουλεύει με το PC/SC Migration Interface σε μια συγκεκριμένη πλατφόρμα. Ο PC/SC Migration Resource Manager υλοποιεί μόνο ένα υποσύνολο των λειτουργιών του API των προτύπων του PC/SC. Η εικόνα που ακολουθεί μας δείχνει μια σύγκριση μεταξύ του PC/SC και του PC/SC Migration.

Μερικά παραδείγματα εφαρμογών που χρησιμοποιούν το PC/SC Migration interface είναι :

- Opencard Framework [OpenCard]
- IBM Smart Card Toolkit [IBMtoolkit]



Σχήμα 7.5.3.1. PC/SC vs PC/SC Migration interface

7.5.4 OpenCard Framework

Δώδεκα κορυφαίοι κατασκευαστές (Bull Personal Transaction Systems, Dallas Semiconductor Corporation, First Access, Gemplus, IBM, NCI, Netscape Communications Corp., Schlumberger, SCM Microsystems, Sun Microsystems,Inc., UbiQ Inc., and Visa International) ένωσαν τις δυνάμεις τους για να φτιάξουν ένα καινούργιο specification, το οποίο ονομάζεται OpenCard Framework [OpenCard] και βοηθά τους υπεύθυνους ανάπτυξης λογισμικού να αναπτύξουν εφαρμογές για έξυπνες κάρτες που μπορούν να χρησιμοποιηθούν σε διαφόρων ειδών συσκευές καθώς και σε PC.

Η πρώτη έκδοση Version 1.0 του Opencard Framework Reference, εκδόθηκε τον Απρίλιο του 1998.

Το OpenCard Framework παρέχει ένα κοινό interface για την έξυπνη κάρτα και για την συσκευή ανάγνωσης της. Επειδή βασίζεται στην αρχιτεκτονική της Java παρέχει μεταφερσιμότητα και διαλειτουργικότητα, τα οποία είναι τα κλειδιά για την ευρεία διάδοση του. Η Version 1.0 παρέχει επίσης αλληλεπίδραση (interaction) με τις ήδη υπάρχουσες Personal Computer/Smart Card (PC/SC) 1.0 συσκευές ανάγνωσης.

Το OpenCard Framework χωρίζεται στα δυο παρακάτω μέρη :

- CardTerminal
- CardService

Το CardTerminal περιέχει κλάσεις και διεπιφάνειες που δίνουν την δυνατότητα πρόσβασης στις συσκευές ανάγνωσης και στις θυρίδες τους (slots). Χρησιμοποιώντας αυτές τις κλάσεις μπορούμε να διαπιστώσουμε αν μια κάρτα εισήχθηκε στη συσκευή ανάγνωσης.

Αυτά τα δύο μέρη κρύβουν τις συγκεκριμένες λεπτομέρειες του τερματικού και της κάρτας και δίνουν τη δυνατότητα να αναπτυχθούν εφαρμογές ανεξάρτητες από την κάρτα ή τη συσκευή ανάγνωσης.

7.5.5 Cryptoki

Τα πρότυπα της κρυπτογραφίας δημόσιου κλειδιού PKCS (Public-Key Cryptography Standards ανήκουν και διαχειρίζονται από τα RSA Laboratories. Υπάρχουν 13 specifications στην οικογένεια του PKCS. Το ενδέκατο από αυτά, είναι το PKCS #11 [PKCS#11], που προσδιορίζει μια προγραμματιστική διεπιφάνεια ανεξάρτητη τεχνολογίας, (technology-independent programming interface), που ονομάζεται cryptoki. Το Cryptoki είναι συντομογραφία του "Cryptographic Token Interface". Το cryptoki είναι μια διεπιφάνεια προγραμματισμού εφαρμογών που κρύβει τις λεπτομέρειες του hardware των κρυπτογραφικών συσκευών και παρουσιάζει στην εφαρμογή ένα μοντέλο κρυπτογραφικής συσκευής, που ονομάζεται κρυπτογραφικό κουπόνι (cryptographic token). Μία έξυπνη κάρτα είναι ένα κρυπτογραφικό κουπόνι. Οι εφαρμογές έχουν πρόσβαση στα κουπόνια μέσω των "θυρών" (slots). Περισσότερα από ένα thread εφαρμογών μπορούν ταυτόχρονα να έχουν πρόσβαση σε ένα ή περισσότερα κουπόνια μέσα από τις αντίστοιχες "θύρες". Συνεπώς το cryptoki υλοποιεί ένα πολυπρογραμματιστικό περιβάλλον για πρόσβαση κουπονιών.

7.5.6 Microsoft Crypto-API

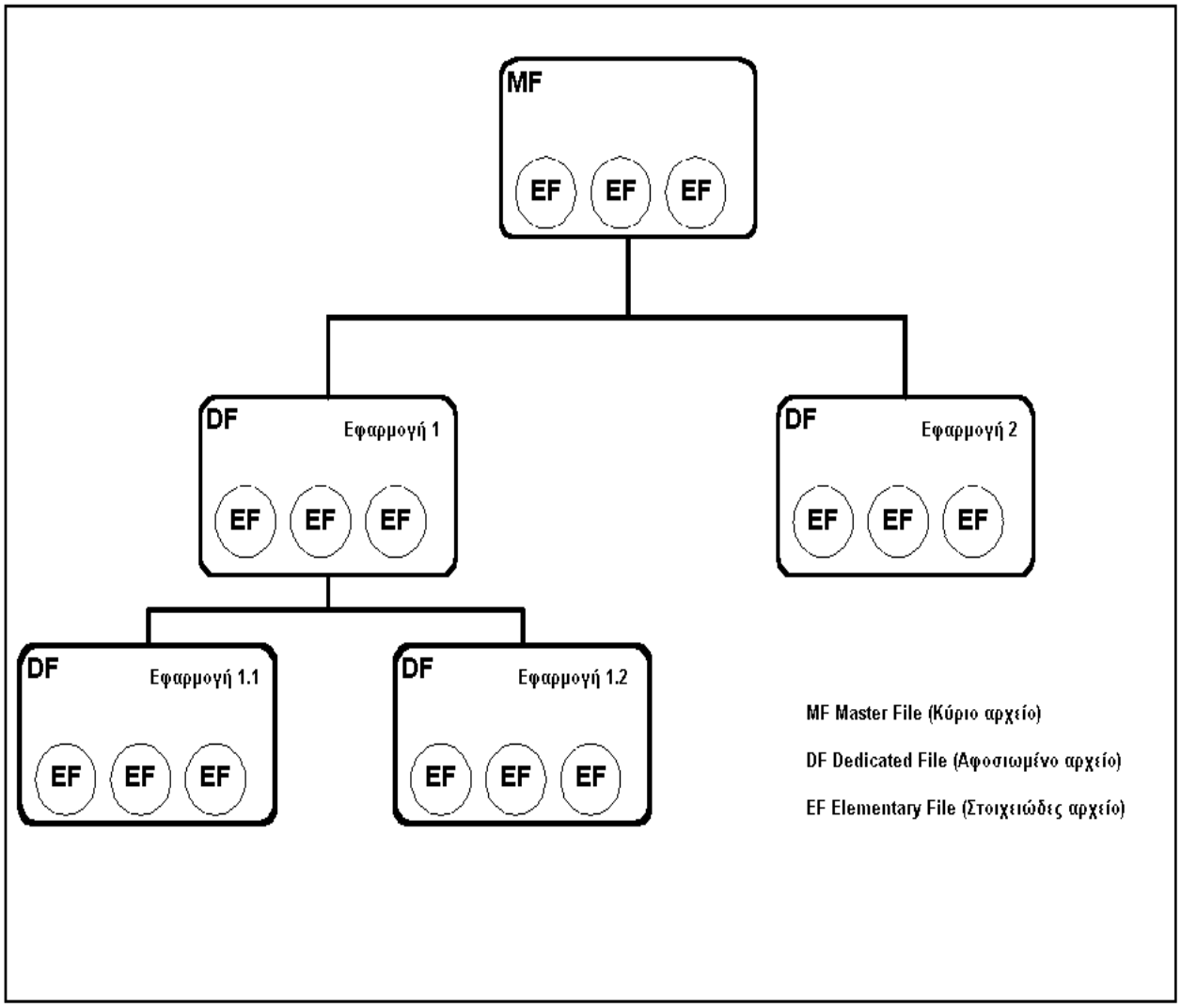
Το κρυπτογραφικό API της Microsoft [MS CryptoAPI] είναι μια προγραμματιστική διεπιφάνεια εφαρμογών, η οποία παρέχει μια ομάδα λειτουργιών που δίνουν τη δυνατότητα σε εφαρμογές να κρυπτογραφήσουν ή να υπογράψουν ψηφιακά δεδομένα, ενώ ταυτόχρονα παρέχουν προστασία στο ιδιωτικό κλειδί του χρήστη. Όλες οι κρυπτογραφικές λειτουργίες εκτελούνται από ανεξάρτητες υπομονάδες (modules), οι οποίες είναι γνωστές ως Παροχείς Κρυπτογραφικών Υπηρεσιών (CSP/Cryptographic Service Providers). Ένας CSP, ο οποίος είναι ο Βασικός RSA Παροχέας της Microsoft, θα συνδέεται με το λειτουργικό σύστημα των Windows NT ή των Windows 95.

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

Τα δεδομένα της κάρτας αποθηκεύονται στην μνήμη EEPROM της κάρτας με τον παρόμοιο τρόμο που αποθηκεύονται στο σύστημα αρχείων του σκληρού δίσκου του υπολογιστή, το οποίο έχει καταλόγους που σχηματίζουν ένα δένδρο ιεραρχικής δομής. Στην κορυφή αυτού του δένδρου, είναι το Κύριο Αρχείο (MF/Master File). Η ύπαρξη αυτού του αρχείου είναι υποχρεωτική. Κάτω από το Κύριο Αρχείο μπορούν να υπάρχουν είτε Αφιερωμένα Αρχεία (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 για παράδειγμα κωδικούς 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 παρακάτω στο δένδρο. Τα αρχεία που χρησιμοποιούνται από την κάρτα για σκοπούς διαχείρισης και έλεγχου ονομάζονται Εσωτερικά Στοιχειώδη Αρχεία (Internal EFs), και τα αρχεία που έχουν πληροφορία προσβάσιμη από τον έξω κόσμο ονομάζονται Εξωτερικά Στοιχειώδη Αρχεία (External EFs).



Σχήμα 7.6. Σύστημα αρχείων έξυπνης κάρτας

7.7 Συσκευές ανάγνωσης/τερματικά έξυπνων καρτών (Smart card readers/terminals)

Υπάρχουν πολλά διαφορετικά είδη συσκευών ανάγνωσης έξυπνων καρτών. Ο όρος "συσκευή ανάγνωσης" είναι παραπλανητικός γιατί αυτές οι συσκευές χρησιμοποιούνται και για να γράφουμε στις κάρτες. Η βασική λειτουργία της συσκευής ανάγνωσης είναι να παρέχει ηλεκτρική ενέργεια και σήματα χρονισμού (clock) στην έξυπνη κάρτα και να εγκαθιστά κανάλι επικοινωνίας μεταξύ της εφαρμογής (application) και της έξυπνης κάρτας.

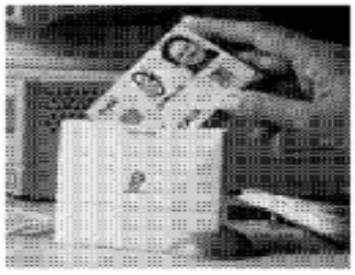
Οι συσκευές ανάγνωσης είναι γνωστές επίσης και ως: Τερματικά Καρτών (Card Terminals), Συσκευές Αποδοχής Έξυπνων Καρτών (Smart Card Accepting Devices), Συσκευές Διεπιφάνειας Χρήστη IFD (Interface Device), CAD (Chip-card Accepting Device), CCR (Chip-Card Reader), ή Προσαρμογέας Έξυπνης Κάρτας (Smart Card Adapter).

7.7.1 Τύποι και χρήση συσκευών ανάγνωσης έξυπνων καρτών

Οι συσκευές ανάγνωσης ποικίλουν από πολύ χαμηλού κόστους απλές συσκευές ανάγνωσης έως περίπλοκες, προγραμματιζόμενες υψηλής ασφάλειας συσκευές με κρυπτογραφικά κλειδιά. Επειδή οι έξυπνες κάρτες έχουν εφαρμογές σε πάρα πολλούς τομείς, πρέπει να υπάρχουν συσκευές ανάγνωσης για όλες τις ανάγκες. Οι συσκευές ανάγνωσης έξυπνων καρτών κατατάσσονται στις εξής κατηγορίες :

- Χαμηλού κόστους readers
- Συσκευές ανάγνωσης ισολογισμού
- Συσκευές ανάγνωσης προσαρτούμενοι /διασυνδεόμενοι με PC
- Ανεξάρτητες (stand-alone), γενικής χρήσης συσκευές ανάγνωσης
- Συσκευές ανάγνωσης ηλεκτρονικού πορτοφολιού (Electronic Purse Readers)
- Συσκευές εφοδιασμού μετρητών (Cash Loading Devices)
- EFTPOS συσκευές ανάγνωσης
- Συσκευές ανάγνωσης για κατασκευές (Building blocks)
- Υβριδικές Συσκευές ανάγνωσης (Hybrid readers)
- Συσκευές ανάγνωσης άνευ επαφής (contactless readers)

7.7.1.1 Χαμηλού κόστους συσκευές ανάγνωσης



Σχήμα 7.7.1.1 GCR410 Reader από την Gemplus

Αυτές οι συσκευές ανάγνωσης κοστίζουν έως US$ 100 και έχουν ένα απλό σειριακό καλώδιο για να συνδέονται με το PC. Η λειτουργία τους είναι βασική και συνήθως αυτές οι συσκευές ανάγνωσης δεν έχουν πληκτρολόγιο (για να εισάγουμε για παράδειγμα το PIN) ή οθόνη. Η συσκευή ανάγνωσης εξαρτάται από το πρόγραμμα εφαρμογής (application program) στο PC, το οποίο διεξάγει την διαχείριση όλων των επικοινωνιών με την κάρτα.

Τυπική χρήση : Τραπεζικές συναλλαγές από το σπίτι (home banking), αγορά προϊόντων από το σπίτι μέσω Internet.

7.7.1.2 Συσκευές ανάγνωσης ισολογισμού (Balance readers)

Σχήμα 7.7.1.2 Reader ισολογισμού για την τσέπη

Πολύ χαμηλού κόστους συσκευές ανάγνωσης (με τιμή έως περίπου US$ 10), που ονομάζονται reader ισολογισμού. Είναι προ-προγραμματισμένοι να διαβάζουν το ποσό από ένα ηλεκτρονικό πορτοφόλι (electronic purse) ή από την τηλεκάρτα.

Επιπρόσθετες λειτουργίες μπορούν να περιλαμβάνουν την παρουσίαση των τελευταίων συναλλαγών. Συνήθως πωλούνται με τη μορφή μπρελόκ για τα κλειδιά.

Τυπική χρήση : Ηλεκτρονικό πορτοφόλι (electronic purse)

7.7.1.3 Συσκευές ανάγνωσης προσαρτούμενες / διασυνδεόμενες με PC

Σχήμα 7.7.1.3. Readers από την Gemplus και την Verifone (Mobile, PCMCIA, PDA)

Αυτοί οι readers είναι σχεδιασμένοι για να προσαρτούνται σε φορητούς υπολογιστές ή υπολογιστές γραφείου. Υπάρχουν διάφορες δυνατότητες για τη σύνδεση με τον υπολογιστή. Παίρνουν ηλεκτρικό ρεύμα από μια εσωτερική μπαταρία, την σειριακή (serial port), ή εξωτερικό προσαρμογέα ρεύματος (power adapter).

Για τους φορητούς υπολογιστές, υπάρχουν συσκευές ανάγνωσης καρτών που μπαίνουν στην θύρα PCMCIA (slot).

Τυπική χρήση : Έλεγχος πρόσβασης (access control), testing

7.7.1.4 Ανεξάρτητοι (stand-alone), γενικής χρήσης συσκευές ανάγνωσης

Σχήμα 7.7.1.4 Gemplus GCR500

Αυτά τα τερματικά έξυπνων καρτών λειτουργούν offline και έχουν τον κώδικα για τις εφαρμογές και την ασφάλεια φορτωμένο στην προγραμματιζόμενη μνήμη της συσκευής ανάγνωσης.

Τυπική χρήση : Έλεγχος πρόσβασης, εφαρμογές υγείας

7.7.1.5 Συσκευές ανάγνωσης ηλεκτρονικού πορτοφολιού (Electronic Purse Readers)

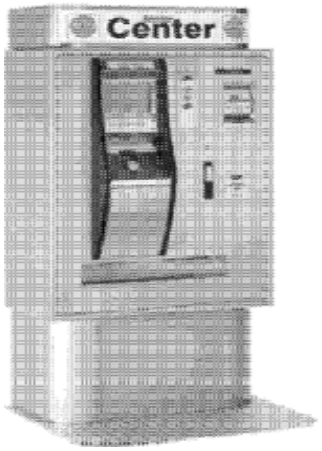
Σχήμα 7.7.1.5 Ηλεκτρονικό πορτοφόλι από την Verifone

Μικρό και φορητό, το ηλεκτρονικό πορτοφόλι είναι σχεδιασμένο για να υποστηρίζει διάφορους τύπους πληρωμής χωρίς μετρητά, συμπεριλαμβανόμενης και της μεταφοράς από κάρτα σε κάρτα. Μπορεί να λειτουργήσει σαν offline τερματικό, μεταφέροντας αυτόματα την τιμή από την έξυπνη κάρτα του πελάτη στην έξυπνη κάρτα του εμπόρου, η οποία είναι τοποθετημένη μέσα στο Security Application Module (SAM) του τερματικού. Υποστηρίζουν ακόμα παρουσίαση στην οθόνη του ποσού που περιέχει η

κάρτα, δυνατότητα κλειδώματος/ξεκλειδώματος της κάρτας και παρουσίασης στην οθόνη των τελευταίων 5-10 συναλλαγών.

Τυπική χρήση : Λιανική πώληση, εστιατόρια, αεροδρόμια, ταξί, δημόσια μεταφορά

7.7.1.6 Συσκευές εφοδιασμού μετρητών (Cash Loading Devices)



Σχήμα 7.7.1.6 Συσκευή εφοδιασμού μετρητών

Αυτή η συσκευή χρησιμοποιείται για να το ηλεκτρονικό πορτοφόλι μιας έξυπνης κάρτας. Μπορεί να δεχτεί χαρτονομίσματα και κέρματα. Η οθόνη χρησιμοποιείται για να δείξει το παρόν ποσό και το ποσό που βάζουμε. Μπορεί επίσης να αφαιρέσει ποσό από την έξυπνη κάρτα και να το δώσει σε μετρητά στο χρήστη.

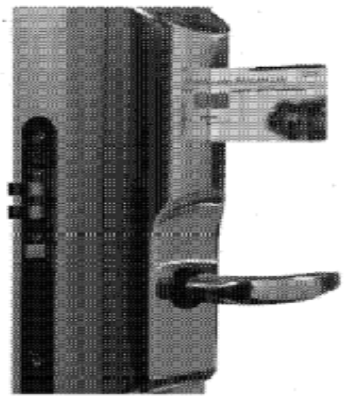
Τυπική χρήση : Τράπεζες, καφετέριες ή μεγάλοι οργανισμοί

7.7.1.7 EFTPOS (Electronic Fund Transfer and Point of Sale) συσκευές ανάγνωσης

Αυτά είναι τερματικά που επιτρέπουν ασφαλείς μεταφορές ηλεκτρονικών κεφαλαίων, για να δώσουν την δυνατότητα της πληρωμής αγαθών από μια έξυπνη κάρτα. Τα τερματικά μπορεί να είναι εξοπλισμένα να εξουσιοδοτούν πληρωμές μέσω dial-up ή ασύρματης επικοινωνίας χρησιμοποιώντας δίκτυα GSM SMS.

Τυπική χρήση : εμπόριο

7.7.1.8 Συσκευές ανάγνωσης για κατασκευές (Building blocks)



Σχήμα 7.7.1.8 Door lock Reader

Αυτές οι συσκευές ανάγνωσης περιέχουν σκέτα μηχανικά και ηλεκτρονικά συστατικά για την ενσωμάτωση σε διάφορα προϊόντα.

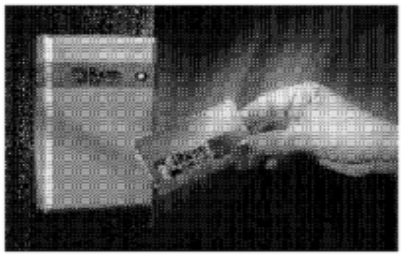
Τυπική χρήση : ATMs, kiosks, αυτόματος πωλητής, door lock, καρτοτηλέφωνα

7.7.1.9 Υβριδικές συσκευές ανάγνωσης

Εκτός από το να διαβάζουν chips, αυτοί οι readers έχουν την δυνατότητα να κάρτες με μαγνητική λωρίδα, ή οπτικές κάρτες. Παράδειγμα τέτοιου reader είναι ο Kyoto reader από την OMRON.

Τυπική χρήση : ATMs, kiosks, εφαρμογές στην υγεία

7.7.1.10 Συσκευές ανάγνωσης άνευ επαφής (contactless readers)



Σχήμα 7.7.1.10 Contactless reader από την RACOM

Οι συσκευές ανάγνωσης άνευ επαφής λειτουργούν αν η κάρτα έρθει σε μια απόσταση από 1mm έως μερικά εκατοστά. Λόγω της έλλειψης προτύπων, αυτοί οι readers μπορούν να λειτουργήσουν μόνο με την αντίστοιχη κάρτα του κατασκευαστή τους.

7.7.2 Πρωτόκολλο επικοινωνίας της συσκευής ανάγνωσης με τις κάρτες

Με την παροχή ενέργειας η κάρτα ανταποκρίνεται αμέσως με ένα κωδικό που ονομάζεται ATR, και ο οποίος προσδιορίζει το πρωτόκολλο επικοινωνίας που θα χρησιμοποιήσει η κάρτα. Τα πρότυπα (standards) έχουν προβλέψει για 15 δυνατά πρωτόκολλα μετάδοσης, τα οποία κωδικοποιούνται ως "T=" και ακολουθεί ο ανάλογος αριθμός που παίρνει τιμές από το 1 έως και το 15. Σήμερα τα πρωτόκολλα που χρησιμοποιούνται κυρίως είναι το T=0 και το T=1.

Το πρωτόκολλο T=0 χρησιμοποιήθηκε αρχικά στη Γαλλία για τις τηλεκάρτες. Σχεδιάστηκε για τα πρώτα συστήματα και χρησιμοποιεί μια τεχνική μετάδοσης byte προς byte, η οποία έχει τις ελάχιστες απαιτήσεις σε μνήμη. Το πρωτόκολλο T=1 χρησιμοποιεί ένα μπλοκ (ακολουθία από bytes) κατά την μετάδοση και είναι πιο κατάλληλο για ασφαλή ανταλλαγή μηνυμάτων και για μοντέρνες συσκευές ανάγνωσης.

Κάποιες συσκευές ανάγνωσης (readers) είναι σχεδιασμένοι να χειρίζονται μόνο το ένα πρωτόκολλο, ενώ άλλοι μπορούν να χρησιμοποιούν και τα δύο πρωτόκολλα και να προσαρμόζονται αυτόματα στο πρωτόκολλο που απαιτεί η κάρτα.

Όταν επιλέγουμε κάρτα συνήθως υιοθετούμε το πρωτόκολλο T=1 εκτός αν υπάρχει απαίτηση να χρησιμοποιήσουμε κάρτες του τύπου T=0 για να διατηρήσουμε τη συμβατότητα με τη δομή της συσκευής ανάγνωσης.

7.7.3 Λογισμικό πλατφόρμας (Platform Software)

Οδηγός Συσκευής (Device Driver)

Οι συσκευές ανάγνωσης προμηθεύονται από τους κατασκευαστές συνήθως με τους οδηγούς τους, οι οποίοι έχουν την μορφή DLLs (dynamic link libraries). Αυτοί λειτουργούν σε μια συγκεκριμένη πλατφόρμα σταθμού εργασίας (workstation platform).

Διεπιφάνεια χρήσης προγραμματισμού εφαρμογών (Application programming interface)

Όπως γνωρίζουμε κάθε συσκευή ανάγνωσης απαιτεί τους δικούς του οδηγούς. Το πρόβλημα του χειρισμού αυτών των οδηγών μεταβιβάζεται στο επίπεδο λογισμικού και η εφαρμογή χρησιμοποιεί μία καθορισμένη συλλογή από APIs όπως προσδιορίζεται στο πρότυπο PC/SC (για τα Windows 95/NT) ή το OCF (για την Java, NC, UNIX και τα Windows 95/NT).

7.7.4 Συμβατότητα με το PC/SC

Αν η συσκευή ανάγνωσης συνδέεται με πλατφόρμα PC, θα πρέπει να έχει συμβατότητα με το πρότυπο PC/SC. Ο κατασκευαστής του reader πρέπει να προμηθεύσει τους κατάλληλους οδηγούς συσκευής για να παρέχει αυτή τη δυνατότητα.

7.8 Κρυπτογραφικές δυνατότητες έξυπνων καρτών

Σήμερα οι έξυπνες κάρτες έχουν αρκετές κρυπτογραφικές δυνατότητες για να υποστηρίξουν δημοφιλείς εφαρμογές και πρωτόκολλα ασφαλείας. Εδώ θα περιγράψουμε κοινές ιδιότητες που βρίσκουμε στις έξυπνες κάρτες με κρυπτογραφικές δυνατότητες.

Οι έξυπνες κρυπτογραφικές κάρτες παρέχουν τη δυνατότητα ψηφιακής υπογραφής RSA με μήκος κλειδιού 512, 768, ή 1024 bit. Οι αλγόριθμοι τυπικά χρησιμοποιούν το θεώρημα CRT (Chinese Remainder Theorem) με σκοπό να γίνει πιο γρήγορη η επεξεργασία. Ακόμη και με μήκος κλειδιού 1024 bit, ο χρόνος που χρειάζεται για να υπογράψουμε κάτι είναι τυπικά κάτω από ένα δευτερόλεπτο. Συνήθως το αρχείο της EPROM που περιέχει το ιδιωτικό κλειδί είναι σχεδιασμένο έτσι ώστε το ιδιωτικό κλειδί να μην εγκαταλείπει ποτέ το chip. Ακόμα και ο κάτοχος της κάρτας δεν μπορεί να έχει πρόσβαση στο κλειδί και να γνωρίζει πιο είναι, αλλά μόνο να το χρησιμοποιεί. Η χρήση του ιδιωτικού κλειδιού προστατεύεται από το PIN (Personal Identification

Number) του χρήστη, έτσι ώστε η κατοχή της κάρτας να μην σημαίνει ικανότητα να υπογράφεις και με αυτήν.

Αν και οι έξυπνες κάρτες έχουν την δυνατότητα να δημιουργήσουν ζεύγη κλειδιών RSA, αυτό γίνεται με πολύ αργή ταχύτητα. Τυπικοί χρόνοι που απαιτούνται για ένα ζεύγος κλειδιών RSA των 1024 bit είναι μεταξύ των 8 δευτερολέπτων και των 3 λεπτών. Οι μεγαλύτεροι χρόνοι παραβιάζουν τις προδιαγραφές του ISO για την αναμονή των επικοινωνιών (communications timeout) και για αυτό τον λόγο χρειάζεται μερικές φορές ειδικό hardware και λογισμικό. Επίσης, η ποιότητα των ζευγών κλειδιών μπορεί να μην είναι ιδιαίτερα υψηλή. Η έλλειψη υπολογιστικής ισχύς συνεπάγεται αδυναμία στην παραγωγή τυχαίων αριθμών και σχετική αδυναμία στην επιλογή μεγάλων πρώτων αριθμών.

Ο αλγόριθμός για ψηφιακή υπογραφή DSA (Digital Signature Algorithm) είναι λιγότερο ευρέως υλοποιημένος στην έξυπνες κάρτες από τον RSA. Και όταν αυτός υλοποιείται είναι τυπικά διαθέσιμος μόνο με μήκος κλειδιού των 512 bit.

Οι έξυπνες κάρτες υποστηρίζουν τη δυνατότητα να έχουν πολλαπλά PINs, τα οποία χρησιμοποιούνται για διαφορετικούς σκοπούς και εφαρμογές. Κάθε εφαρμογή προσδιορίζει ένα PIN, το οποίο είναι το λεγόμενο "Security Officer" PIN, το οποίο ξεμπλοκάρει το PIN του χρήστη, μετά από μια σειρά αποτυχημένων να δοθεί το σωστό PIN, ή ξανά-αρχικοποιεί (re-initialize) την κάρτα. Άλλα PINs μπορούν να προσδιοριστούν για να ελέγχουν την πρόσβαση σε ευαίσθητα αρχεία ή συναρτήσεις.

Ο Πρότυπος Αλγόριθμος Κρυπτογράφησης Δεδομένων DES (Data Encryption Standard) και ο triple DES υπάρχουν στις κάρτες των κύριων κατασκευαστών. Επειδή η σειριακή διεπιφάνεια της έξυπνης κάρτας έχει μικρό εύρος ζώνης (bandwidth), η συμμετρική κρυπτογράφηση μεγάλης ποσότητας δεδομένων (bulk encryption) είναι πολύ αργή.

Στις έξυπνες κάρτες των κύριων εταιριών υπάρχουν διάφοροι μέθοδοι για να παρακολουθείται η ασφάλεια του hardware (security monitoring), με στόχο να μην μπορεί να γίνει εξαγωγή πληροφορίας από το λειτουργικό σύστημα του chip και το σύστημα αρχείων. Μια αμετάκλητη ηλεκτρική ασφάλεια (one-time, irreversible fuse) δεν επιτρέπει να κατασκευαστεί κανένας δοκιμαστικός κωδικός (test code) στην EEPROM. Με σκοπό να αποφευχθεί η κλωνοποίηση των καρτών εγγράφεται ένας αμετάβλητος σειριακός αριθμός στην μνήμη. Οι κάρτες έχουν σχεδιαστεί να επαναφέρουν τον εαυτό τους στην αρχική κατάσταση (reset), όταν ανιχνεύσουν διακύμανση στην τάση του

ρεύματος, στη θερμοκρασία ή στη συχνότητα του ρολογιού. Η ανάγνωση ή η εγγραφή στην ROM είναι συνήθως αδύνατη.

Δυνατότητες ηλεκτρονικού πορτοφολιού (electronic purse) παρέχονται συνήθως, αλλά βασίζονται τυπικά στις τεχνολογίες ηλεκτρονικού κλειδιού όπως ο DES και ο triple DES. Έτσι ένα κοινό κλειδί δίνει τη δυνατότητα ασφάλειας πολλών τέτοιων σχημάτων. Αλγόριθμοι κατακερματισμού (hashing algorithms) που περιέχονται συνήθως στις κάρτες είναι ο SHA-1 και ο MD-5; αλλά ξανά το χαμηλό εύρος ζώνης της σειριακής σύνδεσης (low bandwidth serial connection) εμποδίζει την αποτελεσματική χρήση των αλγόριθμων κατακερματισμού για μεγάλο όγκο δεδομένων (bulk hashing) πάνω στην κάρτα.

Η παραγωγή τυχαίων αριθμών (RNG/Random Number Generation) ποικίλει ανάλογα με τους κατασκευαστές της κάρτας. Άλλες κάρτες έχουν hardware RNG και άλλες pseudo RNG. Πρέπει να ψάξουμε λεπτομέρειες του συγκεκριμένο κατασκευαστή για το αν η γεννήτρια τυχαίων αριθμών είναι αρκετά ισχυρή για να χρησιμοποιηθεί για κρυπτογραφικά ευαίσθητα δεδομένα.

Τα πρωτόκολλα επικοινωνίας των έξυπνων καρτών πολλές φορές έχουν ενσωματωμένο πρωτόκολλο ασφαλείας. Τυπικά βασίζονται στην τεχνολογία συμμετρικού κλειδιού και δίνουν την δυνατότητα στην έξυπνη κάρτα να πιστοποιεί την αυθεντικότητα της στο τερματικό ανάγνωσης και εγγραφής (read/write terminal) ή το αντίστροφο. Όμως τα κρυπτογραφήματα και οι αλγόριθμοι για αυτά τα πρωτόκολλα είναι συνήθως συγκεκριμένοι για κάθε εφαρμογή και κάθε τερματικό.

7.9 Πλεονεκτήματα και σπουδαιότητα της χρήσης των έξυπνων καρτών σε συστήματα ασφαλείας

Τα πλεονεκτήματα και η σπουδαιότητα της χρήσης των έξυπνων καρτών σε συστήματα ασφαλείας περιγράφεται στις παρακάτω παραγράφους.

7.9.1 Θεμελιώδης απαιτήσεις ασφάλειας

Επειδή τα υπολογιστικά συστήματα και δίκτυα γίνονται όλο και σημαντικότερα στη ζωή μας, προκύπτουν πολλές προκλήσεις και απαιτήσεις στο θέμα της ασφάλειας. Οι έξυπνες κάρτες μας δίδουν την δυνατότητα να τις έχουμε μαζί μας και να τις χρησιμοποιούμε οπουδήποτε και για οτιδήποτε χρειαστεί και ταυτόχρονα μας προσφέρουν ασφάλεια.

Στο παγκόσμιο διαδίκτυο, οι έξυπνες κάρτες αυξάνουν την ασφάλεια στα σημαντικά θέματα της Πιστοποίησης (Authentication), Ακεραιότητας (Integrity), και της Μη Άρνησης Πράξης (Non-repudiation). Αυτό συμβαίνει κυρίως γιατί το ιδιωτικό κλειδί δεν χρειάζεται ποτέ να εγκαταλείπει την κάρτα και συνεπώς είναι πολύ δύσκολο να υποκλαπεί το ιδιωτικό κλειδί με παραβίαση του κεντρικού υπολογιστικού συστήματος (host computer system).

Στα εταιρικά δίκτυα (intranets), πολλές φορές πολλαπλά μη συνδεδεμένα συστήματα βασίζουν τη ασφάλεια τους σε διαφορετικές τεχνολογίες. Οι έξυπνες κάρτες είναι πολύ σημαντικές σε αυτήν την περίπτωση γιατί μπορούν να αποθηκεύουν πολλαπλά πιστοποιητικά και κωδικούς πρόσβασης (passwords). Με αυτό τον τρόπο κάθε χρήστης χρειάζεται να έχει μόνο μια κάρτα για να έχει πρόσβαση σε όλα τα συστήματα. Η ηλεκτρονική αλληλογραφία και η πρόσβαση στο διαδίκτυο, η τηλεφωνική πρόσβαση στο δίκτυο (dial-up network access), η κρυπτογράφηση των αρχείων και οι ηλεκτρονικά υπογεγραμμένες φόρμες του παγκόσμιου ιστού μπορούν να βελτιώσουν την ασφάλεια που προσφέρουν με την χρήση των έξυπνων καρτών.

Σε περιπτώσεις μη εσωτερικών εταιρικών δικτύων (extranet), που μια εταιρία θα ήθελε να παρέχει ασφάλεια σε συνεργάτες της και στους προμηθευτές της, μπορούν να μοιραστούν έξυπνες κάρτες για να επιτρέπουν την πρόσβαση σε πόρους της επιχείρησης. Η μεγάλη σημασία των έξυπνων καρτών σε αυτήν την περίπτωση είναι προφανής λόγω της ανάγκης για όσο το δυνατότερο ισχυρή ασφάλεια όταν επιτρέπεται σε όλους να διαπερνούν το firewall της επιχείρησης. Όταν διαμοιράζονται διαπιστευτήρια (credentials) πάνω στην έξυπνη κάρτα, μια εταιρία έχει καλύτερη εγγύηση ότι αυτά τα διαπιστευτήρια δεν μπορούν να διαμοιραστούν, να αντιγραφούν, ή να εκτεθούν με κάποιον άλλο τρόπο.

7.9.2 Τα πλεονεκτήματα των καρτών στην ασφάλεια

Μερικοί λόγοι που οι έξυπνες κάρτες έχουν προάγει την ασφάλεια των μοντέρνων συστημάτων σήμερα είναι :

7.9.2.1 Οι έξυπνες κάρτες προάγουν τη υποδομή PKI

Τα συστήματα με Υποδομή Δημόσιου Κλειδιού (PKI/ Public Key Infrastructure) είναι πιο ασφαλή από τα συστήματα που βασίζονται σε κωδικό πρόσβασης (password), γιατί με τη χρήση των έξυπνων καρτών δεν υπάρχει διαμοιρασμένη γνώση ενός μυστικού. Το ιδιωτικό κλειδί χρειάζεται να είναι γνωστό μόνο σε ένα μέρος, και όχι σε δύο ή περισσότερα. Εάν το ιδιωτικό κλειδί είναι πάνω στην κάρτα, και δεν την

εγκαταλείπει ποτέ, το κρίσιμο μυστικό για το σύστημα δεν μπορεί να εκτεθεί σε καμία περίπτωση εύκολα. Η έξυπνη κάρτα δίνει τη δυνατότητα να χρησιμοποιούμε το ιδιωτικό κλειδί χωρίς αυτό να εμφανίζεται ποτέ στο δίκτυο ή στον υπολογιστή που χρησιμοποιούμε.

7.9.2.2 Οι έξυπνες κάρτες αυξάνουν την ασφάλεια των συστημάτων που βασίζονται σε κωδικούς πρόσβασης (Password Based Systems)

Αν και οι έξυπνες κάρτες έχουν προφανή πλεονεκτήματα για συστήματα με υποδομή PKI, μπορούν επίσης να αυξήσουν την ασφάλεια των συστημάτων που βασίζονται σε κωδικούς πρόσβασης. Ένα από τα μεγαλύτερα προβλήματα στα τυπικά συστήματα με κωδικούς πρόσβασης είναι ότι οι χρήστες γράφουν τον κωδικό τους και τον κολλάνε πάνω στην οθόνη ή στο πληκτρολόγιο. Επίσης συνήθως επιλέγουν εύκολους κωδικούς, και λένε τους κωδικούς τους και σε άλλα άτομα. Εάν χρησιμοποιηθεί έξυπνη κάρτα για να αποθηκευτούν οι πολλαπλοί κωδικοί των χρηστών, οι χρήστες θα χρειάζεται να θυμούνται μόνο το PIN (Personal Identification Number) της κάρτας για να έχουν πρόσβαση σε όλους τους κωδικούς. Επίσης, εάν ο υπεύθυνος για την ασφάλεια αρχικοποιεί την έξυπνη κάρτα, θα επιλέγονται και θα αποθηκεύονται στην κάρτα πολύ ισχυροί κωδικοί. Ο τελικός χρήστης δεν χρειάζεται ούτε καν να γνωρίζει τους κωδικούς, και συνεπώς δεν θα τους γράφει ούτε θα τους λεει σε άλλους.

7.9.2.3 Εξακρίβωση ταυτότητας με δύο παράγοντες (Two factor Authentication)

Τα συστήματα ασφαλείας ενισχύονται από την εξακρίβωση ταυτότητας με πολλαπλούς παράγοντες.

Οι παράγοντες που χρησιμοποιούνται συνήθως είναι :

- Κάτι που γνωρίζουμε
- Κάτι που έχουμε στην κατοχή μας
- Ένα χαρακτηριστικό μας
- Κάτι που κάνουμε

Τα συστήματα που βασίζονται σε μηχανισμό επαλήθευσης κωδικού πρόσβασης τυπικά κάνουν χρήση μόνο του πρώτου παράγοντα, "κάτι που γνωρίζουμε". Οι έξυπνες κάρτες προσθέτουν ένα επιπλέον παράγοντα, κάτι που έχουμε στην κατοχή μας. Η εξακρίβωση ταυτότητας με δύο παράγοντες έχει αποδειχτεί ότι είναι πολύ πιο αποτελεσματική από αυτή με ένα παράγοντα, γιατί ο παράγοντας, "κάτι που γνωρίζουμε", εκτίθεται ή διαμοιράζεται με κάποιον άλλο πολύ εύκολα. Οι έξυπνες κάρτες μπορούν να εμπλουτιστούν έτσι ώστε να περιλαμβάνουν και τους υπόλοιπους δύο παράγοντες που αναφέραμε. Υπάρχουν πρωτότυπα μοντέλα που είναι διαθέσιμα, και τα οποία δέχονται ένα δακτυλικό αποτύπωμα στην επιφάνεια της κάρτας καθώς επίσης και το PIN για να ξεκλειδώσουν τις υπηρεσίες (services) της κάρτας. Εναλλακτικά, φόρμα με το δακτυλικό αποτύπωμα, φόρμα με τον αμφιβληστροειδή χιτώνα του ματιού, ή άλλη βιομετρική πληροφορία μπορεί να αποθηκευτεί στην κάρτα, για να συγκρίνεται με τα δεδομένα μιας ξεχωριστής συσκευής εισόδου βιομετρικών μετρήσεων. Ομοίως, κάτι που κάνουμε όπως το να πληκτρολογούμε πρότυπα, τα χαρακτηριστικά της χειρόγραφης υπογραφής μας, ή φόρμες με το κυμάτισμα της φωνής μας μπορούν να αποθηκευτούν στην κάρτα και να συγκριθούν με τα δεδομένα που λαμβάνονται από εξωτερικές συσκευές εισόδου.

7.9.2.4 Φορητά κλειδιά και πιστοποιητικά

Τα πιστοποιητικά δημόσιου κλειδιού και τα ιδιωτικά κλειδιά μπορούν να χρησιμοποιηθούν από προγράμματα περιήγησης του παγκοσμίου ιστού (web browser) και άλλα δημοφιλή πακέτα λογισμικού, αλλά κατά κάποια έννοια προσδιορίζουν την ταυτότητα του σταθμού εργασίας (work station) και όχι τον ίδιο τον χρήστη. Τα δεδομένα του κλειδιού και του πιστοποιητικού αποθηκεύονται σε μία ιδιόκτητη περιοχή αποθήκευσης για τον χρήστη και πρέπει να εξάγονται / εισάγονται για να μετακινηθούν από τον ένα σταθμό εργασίας στον άλλο. Με τις έξυπνες κάρτες τα πιστοποιητικά και τα ιδιωτικά κλειδιά είναι φορητά, και μπορούν να χρησιμοποιηθούν σε πολλαπλούς σταθμούς εργασίας, που είναι είτε στη δουλεία, είτε στο σπίτι, είτε είναι φορητοί υπολογιστές. Εάν τα χαμηλότερα επίπεδα λογισμικού το υποστηρίζουν, τα πιστοποιητικά και τα ιδιωτικά κλειδιά στις κάρτες μπορούν να χρησιμοποιηθούν από διάφορα προγράμματα λογισμικού διαφορετικών κατασκευαστών, σε διαφορετικές πλατφόρμες, όπως Windows, Unix, και Mac.

7.9.2.5 Αυτό-απενεργοποιούμενα PINs (Auto-disabling PINs)

Αν ένα ιδιωτικό κλειδί είναι αποθηκευμένο σε ένα αρχείο στο σκληρό δίσκο, προστατεύεται τυπικά από ένα κωδικό πρόσβασης (password). Μπορεί να γίνει επίθεση σε αυτό το αρχείο, με αλλεπάλληλες δοκιμές των πιο κοινών κωδικών πρόσβασης, μέχρι ο "κωδικός πρόσβασης" να σπάσει, και να υπάρξει διαρροή του απόρρητου, του μυστικού κλειδιού. Οι έξυπνες κάρτες όμως θα κλειδωθούν μόνες τους εάν δοθεί συνεχόμενα κάποιος αριθμός από λάθος PINs (10 για παράδειγμα). Συνεπώς το ιδιωτικό κλειδί προστατεύεται πιο αποτελεσματικά αν αποθηκευτεί σε μια έξυπνη κάρτα.

7.9.2.6 Μη Άρνηση Πράξης (Non Repudiation)

Με τη χρήση των έξυπνων καρτών για την αποθήκευση ων ιδιωτικών κλειδιών που χρησιμοποιούνται για την ηλεκτρονική υπογραφή έχουμε εξασφαλίσει για το σύστημα μας την υπηρεσία ασφάλειας της Μη Άρνησης Πράξης (Non Repudiation). Γιατί αν το ιδιωτικό κλειδί που χρησιμοποιείται από ένα άτομο για να υπογράφει ηλεκτρονικά υπάρχει μόνο σε μια μοναδική έξυπνη κάρτα, είναι πολύ δύσκολο να πλαστογραφηθεί η ηλεκτρονική υπογραφή χρησιμοποιώντας το ιδιωτικό κλειδί αυτού του ατόμου. Πολλά συστήματα ψηφιακής υπογραφής απαιτούν "Μη Άρνηση Πράξης με ισχύ σε επίπεδο hardware" (hardware strength Non Repudiation), που σημαίνει ότι το ιδιωτικό κλειδί προστατεύεται πάντα μέσα στα στενά όρια ασφάλειας του κουπονιού υλικού (hardware token) και δεν μπορεί να χρησιμοποιηθεί χωρίς γνώση του κατάλληλου PIN. Οι έξυπνες κάρτες μπορούν να παρέχουν "Μη Άρνηση Πράξης με ισχύ σε επίπεδο υλικού (hardware)".

Κεφάλαιο 8

Υπηρεσίες πιστοποίησης για δίκτυο τηλεματικών υπηρεσιών στην υγεία

Στο κεφάλαιο αυτό θα παρουσιάσουμε τις υπηρεσίες πιστοποίησης (Certificate Services) που απαιτούνται για την πιστοποίηση ιατρικού προσωπικού σε ένα δίκτυο τηλεματικών υπηρεσιών στην υγεία. Οι υπηρεσίες πιστοποίησης αυτές βασίζονται στην Υποδομή Δημοσίου Κλειδιού PKI.

8.1 Δομικά Μέρη της Υποδομής Δημοσίου Κλειδιού για δίκτυο τηλεματικών υπηρεσιών στην υγεία

Η Υποδομή Δημοσίου Κλειδιού για 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 την πολιτική πιστοποίησης να έχει μια ή περισσότερες Αρχές Πιστοποίησης, όπως θα δούμε παρακάτω αναλυτικότερα.

- Αρχές εγγραφής (RAs), που ενεργούν εκ μέρους των Αρχών Πιστοποίησης (CAs) για να δηλώνουν εγγραφόμενο ιατρικό προσωπικό στην περιοχή του τηλεματικού δικτύου που διαχειρίζεται η Αρχή Πιστοποίησης.

- Συστήματα διαχείρισης πιστοποιητικών (Certificate management systems/CMS) για τη διαχείριση των πιστοποιητικών του ιατρικού προσωπικού καθ' όλη τη διάρκεια ισχύς τους. Οι Αρχές Πιστοποίησης χρησιμοποιούν και ελέγχουν το συστήματα διαχείρισης πιστοποιητικών (CMS).

- Καταλόγους X.500 (directories), όπου αποθηκεύονται τα πιστοποιητικά του ιατρικού προσωπικού όπως επίσης και δημόσια πληροφορία για τους κατόχους των πιστοποιητικών και χρησιμοποιούνται κατά την επαλήθευση των ψηφιακών πιστοποιητικών.

8.2 Υπηρεσίες πιστοποίησης Ιατρικού προσωπικού

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

8.2.1 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 ιατρικοί επαγγελματίες για να αποδείξουν την ταυτότητα και την ιατρική τους ιδιότητα, και να ελέγχει ότι είναι αυθεντικά. Έπειτα προωθούνται τα απαραίτητα στοιχεία στις Αρχές Πιστοποίησης για να εκδοθούν τα Ηλεκτρονικά Πιστοποιητικά για τον ιατρικό επαγγελματία.

Η δήλωση του προσωπικού από την Αρχή Πιστοποίησης Προσωπικού, είναι μεγάλης σπουδαιότητας για τα ιατρικά πληροφοριακά συστήματα. Στις περισσότερες περιπτώσεις, οι επαγγελματίες του ιατρικού κλάδου έχουν ένα γενικό τρόπο δήλωσης ως επαγγελματίες μιας ιατρικής ειδικότητας. Ένας τρόπος είναι μέσω της συμμετοχής τους στον ιατρικό σύλλογο και τη σύμβαση εργασίας σε οργανισμό υγείας. Όταν δηλωθεί ένας

ιατρικός επαγγελματίας ως χρηστής ενός πληροφοριακού συστήματος ή σε μια εφαρμογή (application), πρέπει να αποδείξει την ταυτότητα του και την ιατρική του ιδιότητα.

Σε πολλές περιπτώσεις ένας ιατρικός επαγγελματίας είναι δηλωμένος (registered) σαν χρήστης σε ορισμένα είδη ιατρικών εφαρμογών. Ο όρος εφαρμογή (application) χρησιμοποιείται εδώ με την ευρεία του έννοια. Μπορεί για παράδειγμα να έχει πρόσβαση σε ένα τοπικό και σε ένα καθολικό πληροφοριακό σύστημα, ή να χρησιμοποιεί μια εφαρμογή για ιατρικές ασφάλειες κ.τ.λ.. Για την δήλωση του ως χρήστης (user registration) ο ιατρικός επαγγελματίας πρέπει να αποδείξει την ταυτότητα του και την ιδιότητα του ως ιατρικός επαγγελματίας. Απαιτείται η απόδειξή και των δύο.

Το σημαντικό σημείο εδώ είναι εάν είναι απαραίτητο ο ιατρικός επαγγελματίας να πιστοποιηθεί (authenticated) αργότερα μόνο σε σχέση με την ταυτότητα του, γιατί η εφαρμογή σε αυτό το σημείο ήδη γνωρίζει την ιατρική του ιδιότητα.

Μια προσέγγιση είναι να εκδίδονται οι εξουσιοδοτήσεις (authorizations) με τη μορφή υπογεγραμμένων ψηφιακών πιστοποιητικών χρησιμοποιώντας την ίδια προσέγγιση όπως και στα πιστοποιητικά των δημόσιων 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 υπάρχουν διάφορα διαθέσιμα προϊόντα που μπορούν να χρησιμοποιηθούν. Παραδείγματος χάρη υπάρχουν διάφορα προϊόντα που μπορούν να χρησιμοποιηθούν για Υπηρεσίες Καταλόγου (Directory services) ακόμα και αν δεν είναι απαραίτητο να πιστοποιηθεί το δημόσιο κλειδί ξανά αλλά μόνο η σύνδεση μεταξύ του διακεκριμένου ονόματος (distinguished name) και της ιατρικής επαγγελματικής κατάστασης (professional status). Πρέπει να παρατηρήσουμε ότι αν το πιστοποιητικό της επαγγελματικής κατάστασης χρησιμοποιηθεί μαζί με το πιστοποιητικό δημόσιου κλειδιού, το πιστοποιητικό της επαγγελματικής κατάστασης πρέπει να χρησιμοποιεί το ίδιο διακεκριμένο όνομα με το πιστοποιητικό δημόσιου κλειδιού.

8.2.2 Ονομασία (Naming)

Πρέπει να υπογραμμιστεί ότι είναι απαραίτητο να αναπτυχθεί ένα σχήμα ονομασίας που να είναι ανεξάρτητο από μια συγκεκριμένη περιοχή (domain) και να μπορεί να χρησιμοποιηθεί γενικά. Το σχήμα της ονομασίας (naming scheme) πρέπει να υποστηρίζει μια ονομασία που να παραμένει έγκυρη για πολύ μεγάλο χρονικό διάστημα. Ο στόχος είναι να συνδεθεί η μακράς διάρκειας εγκυρότητα με ένα μοναδικό αναγνωριστικό (identifier), και ένα όνομα, το οποίο να είναι κατανοητό από τους

ανθρώπους. Η έξυπνη κάρτα των Ιατρικών Επαγγελματιών (Health care Professional Card (smartcard)) χρησιμοποιείται σαν κάρτα μοναδικής ταυτοποίησης.

Το σχήμα που προτείνουμε για ονομασία είναι το ιεραρχικό σχήμα του ονοματολογικού δένδρου του X.500 [RFC 1422] γιατί μας δίδει τη δυνατότητα να υποστηρίξουμε μοναδικά ονόματα.

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

8.2.3 Εξατομίκευση & Αποθήκευση κλειδιού (Key Personalization & Key repository)

Αφού το κλειδί για πρόσβαση, έλεγχο και εξουσιοδότηση (access control and authorization token) είναι η έξυπνη κάρτα ιατρικού επαγγελματία (health care professional smart card), παρουσιάζουμε την παρακάτω ακολουθία από φάσεις που περιγράφουν την εξατομίκευση (personalization) της έξυπνης κάρτας.

Φάση	**Περιγραφή**
1. Εισαγωγή των δεδομένων για τον χρήστη (user data)	Τα δεδομένα του χρήστη εισάγονται από ένα τερματικό. Η πληροφορία μπορεί επίσης να ληφθεί σαν αρχείο από μια εξωτερική βάση δεδομένων.
2. Εξατομίκευση (Personalization)	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.

ΠΙΝΑΚΑΣ 8.2.4. ΦΑΣΕΙΣ ΤΗΣ ΕΞΑΤΟΜΙΚΕΥΣΗ Σ(PERSONALIZATION) ΤΗΣ ΕΞΥΠΝΗΣ ΚΑΡΤΑΣ

8.2.4 Δομή Πιστοποιητικού Ιατρικής Ταυτότητας

Το πρότυπο X.509 συνίσταται για τη δομή (format) των πιστοποιητικών του ιατρικού προσωπικού. Συγκεκριμένα επιλέγουμε την δομή του πιστοποιητικού X.509-v3 (version 3).

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

Τα πιστοποιητικά δημόσιων κλειδιών περιέχουν την εξής πληροφορία:

- Τον αριθμό έκδοσης (version number) του πιστοποιητικού (προτείνουμε X.509 version3)
- Το σειριακό αριθμό (serial number) του πιστοποιητικού
- Το όνομα του αλγόριθμου που χρησιμοποιείται για την υπογραφή του πιστοποιητικού (προτείνουμε να χρησιμοποιηθεί σαν αλγόριθμος σύνοψης μηνύματος ο SHA-1 και ο RSA σαν κρυπτογραφικός αλγόριθμος)
- Το όνομα της Αρχής Πιστοποίησης που έχει υπογράψει και εκδώσει το πιστοποιητικό (διακεκριμένο όνομα X.500 ("distinguished name"), βλέπε

κεφάλαιο 5, π.χ. ou= HYGEIANET, o= Τομέας Υγείας, st=Κρήτη, c=GR). Στο σχεδιασμό αυτό χρησιμοποιούμε μια Αρχή Πιστοποίησης για όλο το τηλεματικό δίκτυο υγείας.

- Το χρονικό διάστημα ισχύος του πιστοποιητικού (προτείνουμε διάστημα ενός έτους)
- Το όνομα του κατόχου του πιστοποιητικού (διακεκριμένο όνομα X.500 ("distinguished name"), βλέπε κεφάλαιο 5)
- Το δημόσιο κλειδί του κατόχου του πιστοποιητικού και το τον αλγορίθμου με τον οποίο χρησιμοποιείται το δημόσιο κλειδί (προτείνουμε τον αλγόριθμο RSA)
- Το αναγνωριστικό του κλειδιού της Αρχής Πιστοποίησης, το οποίο δίνει τη δυνατότητα να προσδιοριστεί το δημόσιο κλειδί της Αρχής Πιστοποίησης με το οποίο υπογράφηκε το πιστοποιητικό. Αυτό το πεδίο χρησιμοποιείται μόνο αν η Αρχή Πιστοποίησης έχει πολλαπλά κλειδιά για να υπογράφει διαφορετικές κατηγορίες πιστοποιητικών.
- Πληροφορία για τη χρήση του κλειδιού που περιγράφει τους σκοπούς που το πιστοποιημένο δημόσιο κλειδί μπορεί να χρησιμοποιηθεί (προαιρετικό πεδίο). Χρησιμοποιείται αν το κλειδί χρησιμοποιείται για συγκεκριμένους σκοπούς μόνο και η Αρχή Πιστοποίησης θέλει να τους προσδιορίσει. (π.χ. υπογραφή ιατρικών πράξεων και αποκρυπτογράφηση μηνυμάτων)
- Πληροφορία για την πολιτική πιστοποίησης που υποδεικνύει την πολιτική ασφαλείας που ίσχυε όταν εκδόθηκε το πιστοποιητικό και τους σκοπούς που μπορεί να χρησιμοποιηθεί το πιστοποιητικό (προαιρετικό πεδίο).
- Τα σημεία διανομής Λιστών Ακύρωσης Πιστοποιητικών (CRL distribution points) τα οποία προσδιορίζουν πως και που μπορούμε να λάβουμε πληροφορία για τις Λίστες Ακύρωσης Πιστοποιητικών

8.2.5 Διαχείρηση Πιστοποιητικών Ιατρικών επαγγελματιών

Η διαχείριση των πιστοποιητικών ιατρικών επαγγελματιών περιλαμβάνει τα εξής:

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

8.2.5.1 Δημιουργία Πιστοποιητικών Ιατρικών επαγγελματιών

Ανάλογα με την πολιτική της, η Αρχή Πιστοποίησης του τηλεματικού δικτύου υγείας μπορεί να επιτρέπει τη χρησιμοποίηση 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 ιατρικού επαγγελματία. 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.

8.2.5.1.1 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 Αρχή Εγγραφής.

8.2.5.1.2 Έλεγχος για μοναδικό κωδικό ιατρικού επαγγελματία/ λειτουργίες κανόνων (Control of unique user id/ rules functions)

Όλα τα πιστοποιητικά των ιατρικών επαγγελματιών 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 διατηρούμε ένα κατάλογο (record) των πιστοποιητικών που έχουν δημιουργηθεί προηγουμένως, ή τουλάχιστον να κρατάμε τα ονόματα των ιατρικών επαγγελματιών στα οποία εκδόθηκαν πιστοποιητικά.

8.2.5.1.3 Λειτουργία δημιουργίας πιστοποιητικών (Certificate generation function)

Τα πιστοποιητικά δημόσιων 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 τα με το πρότυπο του X.509 v3 που έχουμε επιλέξει. Τα κωδικοποιημένα δεδομένα μετά θα υπογραφούν με τον αλγόριθμο που έχουμε επιλέξει (SHA-1 αλγόριθμος σύνοψης, και RSA κρυπτογραφικός αλγόριθμος). Τα κωδικοποιημένα δεδομένα μαζί με την υπογραφή της Αρχής Πιστοποίησης του τηλεματικού δικτύου υγείας, κωδικοποιούνται κατόπιν περαιτέρω όπως ορίζει το πρότυπο X.509 v3. Το πιστοποιητικό ιατρικής ταυτότητας είναι το δυαδικό αλφαριθμητικό (binary string) που παίρνουμε σαν αποτέλεσμα.

8.2.5.2 Διανομή και αποθήκευση και ανάκτηση πιστοποιητικών ιατρικών επαγγελματιών

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

1) Ένα πιστοποιητικό δεν πρέπει να είναι κρυφό. Δεν είναι δυνατό 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 την 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 (certification path) 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 σφραγίδα χρόνου (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 δίδονται όχι από τον ίδιο τον αποστολέα αλλά από κάποιον άλλον. Έτσι, πρέπει να χρησιμοποιεί τις υπηρεσίες κατάλογου (directory service) οπωσδήποτε. Μία παρεμφερής υπηρεσία (service) μπορεί να διανέμει τα πιστοποιητικά που απαιτούνται εξίσου καλά. Η αποθήκευση των λιστών ακύρωσης σε κάρτες δεν είναι ρεαλιστική.

Αρά στο τηλεματικό δίκτυο υγείας προτείνουμε η αποθήκευση των πιστοποιητικών να μην γίνεται μόνο σε κάρτες.

Τα πιστοποιητικά των ιατρικών επαγγελματιών θα πρέπει να είναι δημόσια διαθέσιμα στους χρήστες του ιατρικού δικτύου μέσω ενός Καταλόγου X.500 (Κεφάλαιο 5). Τα πιστοποιητικά επίσης θα πρέπει να διαφυλάσσονται σε ένα ασφαλή χώρο αποθήκευση (repository) και σε εφεδρικό αντίγραφο, για την περίπτωση που πρέπει να ανακτηθούν λόγω βλάβης του Καταλόγου.

8.2.5.3 Ακύρωση πιστοποιητικών ιατρικών επαγγελματιών

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

Περιπτώσεις που προκαλούν την ανάκληση του πιστοποιητικού ενός ιατρικού επαγγελματία είναι αν το ιδιωτικό κλειδί χαθεί ή εκτεθεί σε κινδύνους, αν αλλάξει η κατάσταση του ιδιοκτήτη του πιστοποιητικού (για παράδειγμα όταν αλλάζουν οι ιατρικές αρμοδιότητες του κατόχου του), ή αν μεταβληθεί κάποια άλλη πληροφορία του πιστοποιητικού του ιατρικού επαγγελματία.

Τα πιστοποιητικά που έχουν ανακληθεί αποθηκεύονται σαν μία υπογεγραμμένη δομή δεδομένων, που ονομάζουμε Λίστα Ανάκλησης Πιστοποιητικών (Certificate Revocation List/ CRL), στην όποια έχουμε ήδη αναφερθεί στο Κεφάλαιο 4. 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 Πιστοποιησης του δικτύου τηλεματικών υπηρεσιών στην υγεία για τα πιστοποιητικά που εκδίδει η ίδια. Οι Λίστες Ανάκλησης Πιστοποιητικών πρέπει να έχουν σφραγίδα χρόνου (timestamp) και να έχουν υπογραφεί από την Αρχή Πιστοποίησης του Τηλεματικού δικτύου.

8.2.5.3.1 Δομή λίστας ανάκλησης πιστοποιητικών ιατρικών επαγγελματιών

Προτείνουμε την μορφή CRL version2 (format) για τις Λίστες Ανάκλησης των Πιστοποιητικών των ιατρικών επαγγελματιών. Η μορφή αυτή αντιστοιχεί στο πιστοποιητικό X.509 version3 που επιλέξαμε για τα πιστοποιητικά των ιατρικών επαγγελματιών.

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

- Τον αριθμό έκδοσης του CRL (version 2)
- Το όνομα του αλγόριθμου ο ποίος χρησιμοποιείται για να υπογραφεί το CRL (προτείνεται ο MD5 με RSA-Encryption)
- Το όνομα της οντότητας που έχει υπογράψει και εκδώσει τη CRL (X.500 "distinguished name", κεφάλαιο 5)
- Την ημερομηνία έκδοσης της CRL
- Την ημερομηνία που η επόμενη CRL θα εκδοθεί
- Τη 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 (issuing distribution point)

8.2.5.3.2 Συντήρηση λίστας ανάκλησης πιστοποιητικών ιατρικών επαγγελματιών

Οι CRLs και τα πιστοποιητικά δημόσιου κλειδιού πρέπει να ενημερώνονται (be updated) 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. Προτείνουμε η CRL να ενημερώνεται στο δίκτυο μας κάθε ώρα.

8.2.5.3.3 Διανομή και αποθήκευση λίστας ανάκλησης πιστοποιητικών ιατρικών επαγγελματιών

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 ιατρικών επαγγελματιών 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 (Κεφάλαιο 4). 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.

8.2.6 Διαχείριση του κατάλογου με τα πιστοποιητικά και τις Λίστες Ανάκλησης Πιστοποιητικών

Η διαχείριση του καταλόγου με τα πιστοποιητικά γίνεται όπως περιγράφουμε στο κεφάλαιο 5 (Κατάλογοι X.500).

Κεφάλαιο 9

Ισχυρή εξακρίβωση ταυτότητας με τη χρήση έξυπνων καρτών

Η ισχυρή προστασία της ασφάλειας, της ακεραιότητας και του απόρρητου των ιατρικών δεδομένων είναι απαραίτητη και επιβάλλεται από το νόμο. Ευαίσθητη πληροφορία όπως τα προσωπικά ιατρικά δεδομένα πρέπει να μεταδίδεται μόνο μεταξύ υπευθύνων εξακριβωμένης ταυτότητας μερών (χρηστών, εφαρμογών & συστημάτων). Αυτό πρέπει να γίνεται με ασφαλή τρόπο, εξασφαλίζοντας την ακεραιότητα και το απόρρητο της πληροφορίας. Άρα απαραίτητη για την αποτελεσματικότητα του μηχανισμού της προστασίας του απορρήτου είναι η ύπαρξη ασφαλών μέσων εξακρίβωσης ταυτότητας των χρηστών (strong authentication of users) των ιατρικών πληροφορικών συστημάτων τόσο στις υπηρεσίες ασφαλείας των εφαρμογών όσο και στις υπηρεσίες ασφαλείας κατά την επικοινωνία

9.1 Τύποι Εξακρίβωσης ταυτότητας

Στην Αρχιτεκτονική Ασφαλείας OSI (OSI Security Architecture ISO 7498-2) [ISO 7498-2] ορίζονται οι εξής δύο τύποι εξακρίβωσης ταυτότητας:

1. *Εξακρίβωση ταυτότητας ισότιμων μερών (peer entity authentication):* ονομάζεται η επιβεβαίωση ότι το ισότιμο μέρος στο κάθε άκρο ενός συνδέσμου είναι όντως αυτό που ισχυρίζεται. Αυτό αναφέρεται στην περίπτωση της εξακρίβωσης ταυτότητας των χρηστών σε μια περίπτωση διασυνδεδεμένης επικοινωνίας στο διαδίκτυο (connection-oriented online situation)

2. *Εξακρίβωση της ταυτότητας προέλευσης των δεδομένων (data origin authentication):* ονομάζεται η επιβεβαίωση ότι η πηγή προέλευσης των δεδομένων που λαμβάνομε είναι όντως αυτή που ισχυρίζεται. Αυτό αναφέρεται στην εφαρμογή των «ηλεκτρονικών υπογραφών» στα ψηφιακά κείμενα (βλέπε Κεφάλαιο 10).

Σε αυτό το κεφάλαιο αναφερόμαστε στον πρώτο τύπο εξακρίβωσης ταυτότητας. Από εδώ και στο εξής όταν χρησιμοποιείται στο παρόν κεφάλαιο ο όρος «εξακρίβωση ταυτότητας» θα εννοούμε την Εξακρίβωση ταυτότητας ισότιμων μερών (peer entity authentication).

9.2 Ασθενής Εξακρίβωση Ταυτότητας

Ο πιο κοινός μηχανισμός εξακρίβωσης ταυτότητας είναι το να ζητείται από τον χρήστη να δώσει τον κρυφό κωδικό (password) που μόνο αυτός γνωρίζει για να αποδείξει την ταυτότητα του. Τα μειονεκτήματα αυτού του μηχανισμού είναι ότι ο κρυφός κωδικός μεταδίδεται κάθε φορά συνεπώς είναι ευάλωτος σε επιθέσεις, όπου ο επιτεθέμενος κρυφάκουει την επικοινωνία που γίνεται για να δοθεί ο κωδικός. Για αυτό τον λόγο η εξακρίβωση ταυτότητας με την χρήση κωδικών ονομάζεται και «ασθενής εξακρίβωση ταυτότητας» (weak authentication).

Η ασθενής εξακρίβωση ταυτότητας παρουσιάζει και άλλα μειονεκτήματα τα οποία είναι ότι οι χρήστες αποκαλύπτουν σε άλλους χρήστες τους προσωπικούς κρυφούς τους κωδικούς, η απομνημόνευση ενός ασφαλούς κρυφού κωδικού είναι δύσκολη και ότι η διαχείριση των κρυφών κωδικών παρουσιάζει σημαντικά προβλήματα ιδιαίτερα σε μεγάλους σύνθετους οργανισμούς.

Για να αποφευχθούν αυτά τα προβλήματα και οι επιθέσεις που βασίζονται σε αυτά, χρησιμοποιείται η ισχυρή εξακρίβωση ταυτότητας.

9.3 Ισχυρή Εξακρίβωση Ταυτότητας

Η ισχυρή εξακρίβωση ταυτότητας πραγματοποιείται με τη χρήση κρυπτογραφικά παραγόμενων διαπιστευτηρίων και ορίζεται στο πρότυπο ISO/IEC 9594-8 (X.509) «Εξακρίβωση Ταυτότητας με τη χρήση κρυπτογραφικά παραγόμενων διαπιστευτηρίων (Authentication by means of cryptographically derived credentials)» [ISO 9594-8]. Η

ισχυρή εξακρίβωση ταυτότητας βασίζεται σε κρυπτογραφικά πρωτόκολλα πρόκλησης/ απόκρισης τα οποία επιτρέπουν την απόδειξη της γνώσης ενός μυστικού χωρίς να χρειάζεται να το αποκαλύψουν (zero knowledge protocols). Η ισχυρή εξακρίβωση ταυτότητας μπορεί να υλοποιηθεί χρησιμοποιώντας την συμμετρική ή την ασυμμετρική κρυπτογραφία.

9.3.1 Ισχυρή Εξακρίβωση Ταυτότητας με τη χρήση Συμμετρικής Κρυπτογραφίας

Κατά την ισχυρή εξακρίβωση ταυτότητας με την χρήση συμμετρικής κρυπτογραφίας απαιτείται ένα κρυφό συμμετρικό κλειδί. Το κλειδί αυτό είναι γνωστό στο χρήστη και στο σύστημα που εκτελεί την εξακρίβωση ταυτότητας (authenticating system). Μια τυχαία πρόκληση (random challenge) παράγεται από το σύστημα εξακρίβωσης της ταυτότητας. Η πρόκληση κρυπτογραφείται από το χρήστη με το κρυφό του κλειδί. Αυτή η απόκριση (response) μπορεί να επαληθευτεί από το σύστημα εξακρίβωσης ταυτότητας χρησιμοποιώντας το ίδιο κρυφό κλειδί. Συνεπώς, για να επιτευχθεί η εξακρίβωση της ταυτότητας χρησιμοποιείται ένας μηχανισμός κρυπτογράφησης. Το μειονέκτημα αυτής της μεθόδου είναι το γεγονός ότι για να γίνει η εξακρίβωση ταυτότητας του κάθε χρήστη, ένα ξεχωριστό κρυφό κλειδί για κάθε χρήστη πρέπει να παραχθεί, να διανεμηθεί και να προστατευτεί τόσο από το χρήστη όσο και από όλα τα συστήματα εξακρίβωσης ταυτότητας. Η ισχυρή εξακρίβωση ταυτότητας που βασίζεται στην συμμετρική κρυπτογράφηση χρησιμοποιείται κυρίως σε κλειστά περιβάλλοντα τα οποία έχουν μόνο ένα σύστημα εξακρίβωσης ταυτότητας, όπως για παράδειγμα τα τραπεζικά συστήματα.

9.3.2 Ισχυρή Εξακρίβωση Ταυτότητας με τη χρήση Ασυμμετρικής Κρυπτογραφίας

Κατά την ισχυρή εξακρίβωση ταυτότητας με τη χρήση ασυμμετρικής κρυπτογραφίας απαιτείται η παραγωγή ενός ζεύγους ιδιωτικού-δημόσιου κλειδιού για κάθε χρήστη. Ο χρήστης υπογράφει την τυχαία πρόκληση που του στέλνει το σύστημα εξακρίβωσης ταυτότητας με το ιδιωτικό του κλειδί και στέλνει την υπογραφή στο σύστημα εξακρίβωσης ταυτότητας. Το σύστημα εξακρίβωσης της ταυτότητας κάνει επαλήθευση της απόκρισης χρησιμοποιώντας το αντίστοιχο δημόσιο κλειδί. Το δημόσιο κλειδί περιέχεται στο πιστοποιητικό δημοσίου κλειδιού του χρήστη. Το σύστημα εξακρίβωσης ταυτότητας λαμβάνει το δημόσιο κλειδί αφού επαληθεύσει την γνησιότητα του πιστοποιητικού. Συνεπώς, ο μηχανισμός ψηφιακής υπογραφής χρησιμοποιείται για να γίνει η ισχυρή εξακρίβωση ταυτότητας. Το πλεονέκτημα αυτής της μεθόδου είναι ότι

διαφορετικά συστήματα μπορούν να κάνουν ισχυρή εξακρίβωση της ταυτότητας του χρήστη χωρίς να χρειάζεται να έχουν πρόσβαση στα αντίστοιχα κρυφά κλειδιά. Η μόνη απαίτηση είναι η πρόσβαση στα πιστοποιητικά δημοσίων κλειδιών και ικανότητα επαλήθευσης της εγκυρότητας τους. Η ισχυρή εξακρίβωση ταυτότητας βασίζεται στις ψηφιακές υπογραφές και για αυτό το λόγο χρησιμοποιείται κυρίως στα ανοικτά δίκτυα, στα οποία χρήστες επικοινωνούν με πολλά διαφορετικά συστήματα εξακρίβωσης ταυτότητας, όπως για παράδειγμα το παγκόσμιο διαδίκτυο (internet).

9.4 Η χρήση των έξυπνων καρτών

Για τις υπηρεσίες εξακρίβωσης ταυτότητας τις οποίες περιγράψαμε παραπάνω, ο χρήστης πρέπει να διατηρήσει και να προστατεύσει το ιδιωτικό ασυμμετρικό κλειδί του (ή το κρυφό συμμετρικό του αντίστοιχα). Αυτό γίνεται προτιμότερα χρησιμοποιώντας μια έξυπνη κάρτα με μικροεπεξεργαστή και ένα κρυπτογραφικό συνεπεξεργαστή, οποίος προστατεύεται με ένα Προσωπικό Κωδικό Ταυτότητας PIN, για τους παρακάτω λόγους:

1. ***Ασφάλεια (Security):*** Το ιδιωτικό κλειδί προστατεύεται μέσα σε μια φυσική συσκευή, η οποία τη μεταφέρει μαζί του ο χρήστης. Με αυτό τον τρόπο εξασφαλίζεται ο απόλυτος έλεγχος του ιδιωτικού κλειδιού του κάθε νόμιμου κατόχου. Το ιδιωτικό κλειδί δεν εγκαταλείπει ποτέ την έξυπνη κάρτα. Η έξυπνη κάρτα δεν μπορεί να αντιγραφεί, και το ένα και μοναδικό αντίγραφο του ιδιωτικού κλειδιού του χρήστη βρίσκεται μέσα της. Για να εξακριβωθεί εάν ο χρήστης της κάρτας είναι ο νόμιμος κάτοχος, ζητείται πάντα ο Προσωπικός Κωδικός Ταυτοποίησης (PIN) σε κάθε χρήση της κάρτας για την εκτέλεση μιας πράξης υπογραφής.

2. ***Φορητότητα (Mobility):*** Ο χρήστης μπορεί να χρησιμοποιήσει το ιδιωτικό του κλειδί για να πιστοποιήσει την ταυτότητα του σε κάθε περιβάλλον το οποίο διαθέτει το κατάλληλο λογισμικό. Η φορητότητα είναι ένας βασικός λόγος για τη χρήση των έξυπνων καρτών στην ασφάλεια των ιατρικών πληροφοριακών συστημάτων, όπου ο ιατρικός επαγγελματίας χρειάζεται να μετακινείται.

3. ***Ενημερότητα του χρήστη (User awareness):*** Ο χρήστης κάνοντας χρήση των έξυπνων καρτών συνειδητοποιεί τις όψεις της ασφάλειας και το νόημα των ψηφιακών υπογραφών με απτό τρόπο. Ενημερώνεται για το πότε γίνεται μια

πράξη υπογραφής με το ιδιωτικό του κλειδί για την εξακρίβωση της ταυτότητας του γιατί πάντα του ζητείται ο Προσωπικός Κωδικός Ταυτοποίησης του (PIN).

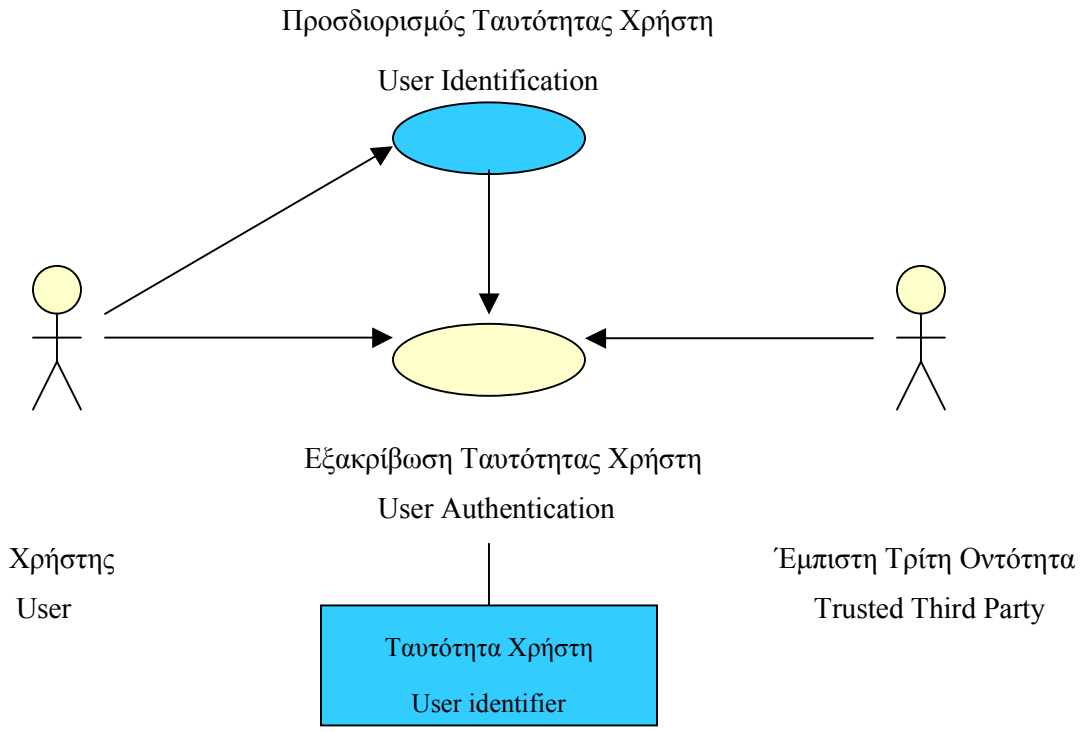
9.5 Μοντέλο ισχυρής εξακρίβωσης ταυτότητας

Το μοντέλο ισχυρής εξακρίβωσης ταυτότητας που σχεδιάσαμε και υλοποιήσαμε στην παρούσα μεταπτυχιακή εργασία βασίζεται στο Ευρωπαϊκού Προτύπου ENV 13729 «Ιατρικά Πληροφοριακά – Ασφαλής Ταυτοποίηση του χρήστη –Ισχυρή Εξακρίβωση της ταυτότητας με τη χρήση καρτών με μικροεπεξεργαστή (Health Informatics – Secure user identification – Strong authentication using microprocessor cards)» [ENV 13729].

Το μοντέλο μας εξακρίβωσης ταυτότητας βασίζεται στο γεγονός ότι κάθε χρήστης κατέχει την αυστηρά προσωπική του έξυπνη κάρτα και στη χρησιμοποίηση ενός κρυπτογραφικού πρωτοκόλλου πρόκλησης απόκρισης (cryptographic challenge response protocol).

9.5.1 Γενική περίπτωση εξακρίβωσης ταυτότητας

Το επόμενο διάγραμμα παρουσιάζει τη διαδικασία της εξακρίβωσης ταυτότητας σε υψηλό επίπεδο.



Σχήμα 9.5.1. Γενικό Διάγραμμα Εξακρίβωσης Ταυτότητας

Η διαδικασία Προσδιορισμού της Ταυτότητας του Χρήστη (User Identification process) απαιτεί από το χρήστη να προσδιορίσει την ταυτότητα του. Η διαδικασία Εξακρίβωσης της Ταυτότητας του Χρήστη (User Authentication process) επιβεβαιώνει (verifies) την ισχυριζόμενη ταυτότητα του χρήστη, βασιζόμενη στην πληροφορία εξακρίβωσης ταυτότητας (authentication information) η οποία παρέχεται από τον χρήστη και από την Έμπιστη Τρίτη Οντότητα (Trusted Third Party) η οποία λειτουργεί ως παροχέας Υπηρεσιών Πιστοποίησης (Certificate Service Provider). Το αποτέλεσμα της συνολικής διαδικασίας είναι το εξακριβωμένο αναγνωριστικό Ταυτότητας του Χρήστη (verified User Identifier).

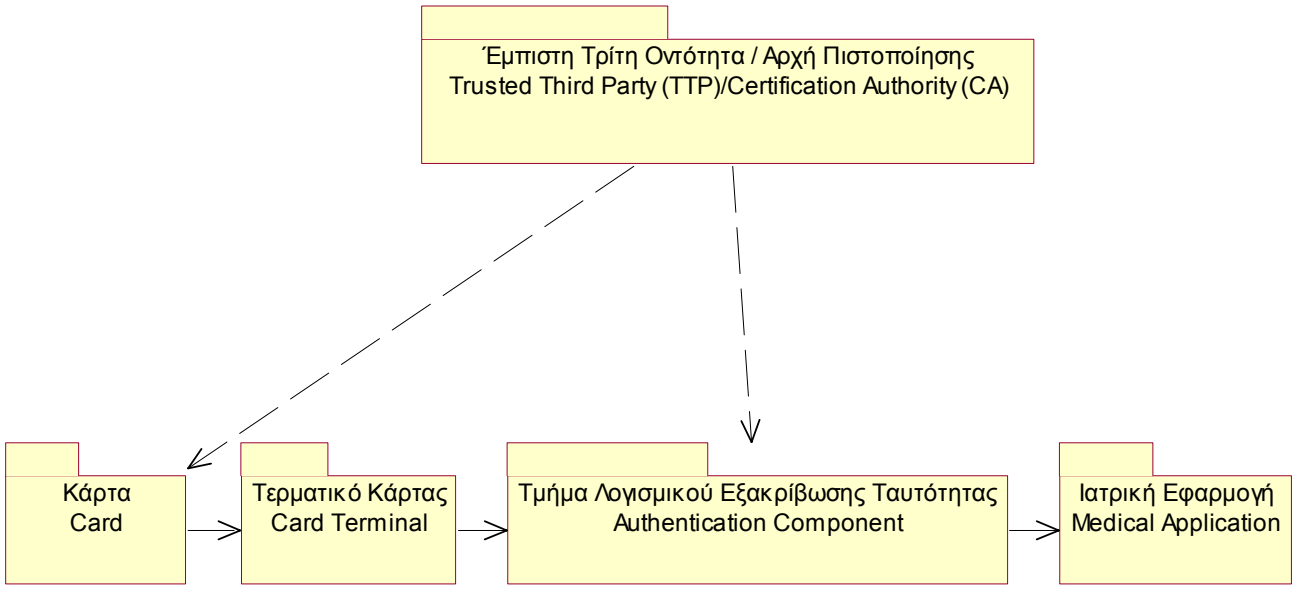
9.5.2 Εξακρίβωση ταυτότητας τοπικά και εξ' αποστάσεως

Στο περιβάλλον των ιατρικών εφαρμογών, διακρίνουμε δυο διαφορετικές περιπτώσεις εξακρίβωσης ταυτότητας:

1. *Εξακρίβωση ταυτότητας τοπικά (local authentication):Η εξακρίβωση της ταυτότητας του χρήστη γίνεται στο τοπικό σύστημα στο οποίο το τερματικό για τις κάρτες(card terminal) είναι απευθείας συνδεδεμένο. Το τοπικό σύστημα μπορεί για παράδειγμα να είναι ένας προσωπικός υπολογιστής (PC) ή ένας σταθμός εργασίας.*

2. *Εξακρίβωση ταυτότητας εξ' αποστάσεως (remote authentication): Η εξακρίβωση της ταυτότητας του χρήστη γίνεται σε ένα μακρινό σύστημα, το οποίο συνδέεται με τον προσωπικό υπολογιστή του χρήστη (ή με το σταθμό εργασίας στον οποίο δουλεύει) μέσω δικτύου.*

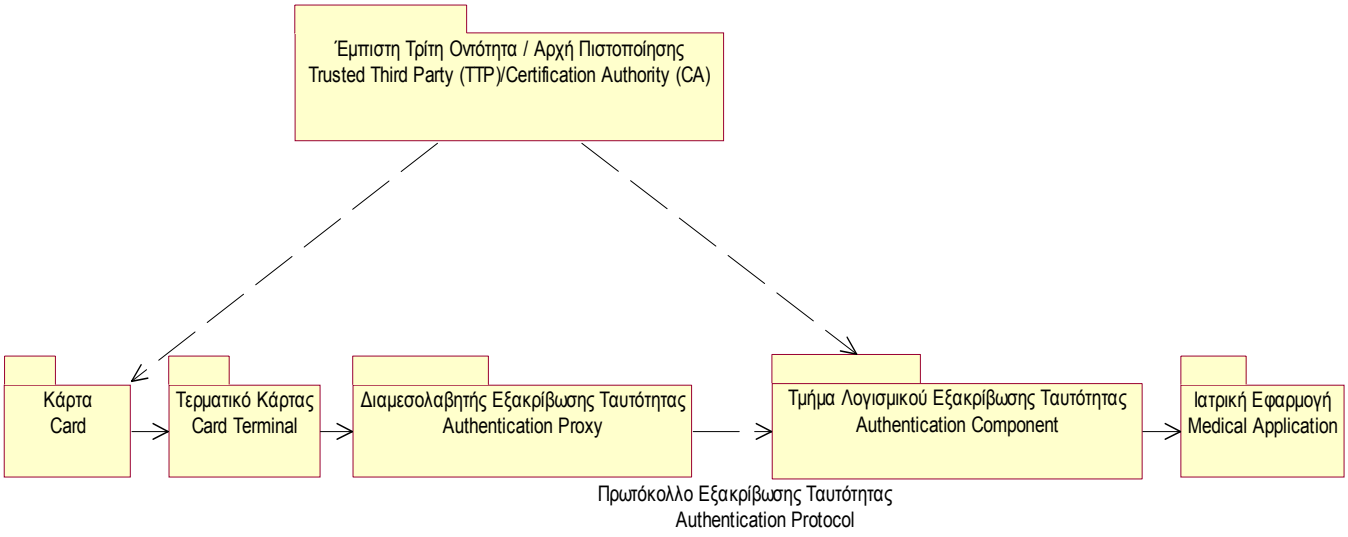
Στο παρακάτω διάγραμμα (Σχήμα 9.5.2.α) φαίνονται τα επιμέρους μέρη που χρησιμοποιούνται για την εξακρίβωση της ταυτότητας τοπικά.



Σχήμα 9.5.2.α. Διάγραμμα των επιμέρους μερών που χρησιμοποιούνται για την εξακρίβωση ταυτότητας τοπικά

Στην περίπτωση της *εξακρίβωσης ταυτότητας τοπικά*, η έξυπνη κάρτα του ιατρικού επαγγελματία περιέχει τα κλειδιά και τα πιστοποιητικά που η Έμπιστη Τρίτη Οντότητα (TTP) έχει εκδώσει για τον συγκεκριμένο χρήστη. Η κάρτα εισάγεται στο τοπικό Τερματικό Καρτών, μέσω του οποίου το τμήμα του λογισμικού που κάνει την εξακρίβωση της ταυτότητας (Authentication Component) μπορεί να έχει πρόσβαση στην κάρτα. Το εξακριβωμένο αναγνωριστικό Ταυτότητας του Χρήστη (verified User Identifier), το οποίο είναι το αποτέλεσμα της διαδικασίας της εξακρίβωσης ταυτότητας, μεταβιβάζεται στην Ιατρική Εφαρμογή.

Στο παρακάτω διάγραμμα (Σχήμα 9.5.2.β) φαίνονται τα επιμέρους μέρη που χρησιμοποιούνται για την εξακρίβωση της ταυτότητας εξ' αποστάσεως.



Σχήμα 9.5.2.β. Διάγραμμα των επιμέρους μερών για την εξακρίβωση της ταυτότητας εξ' αποστάσεως

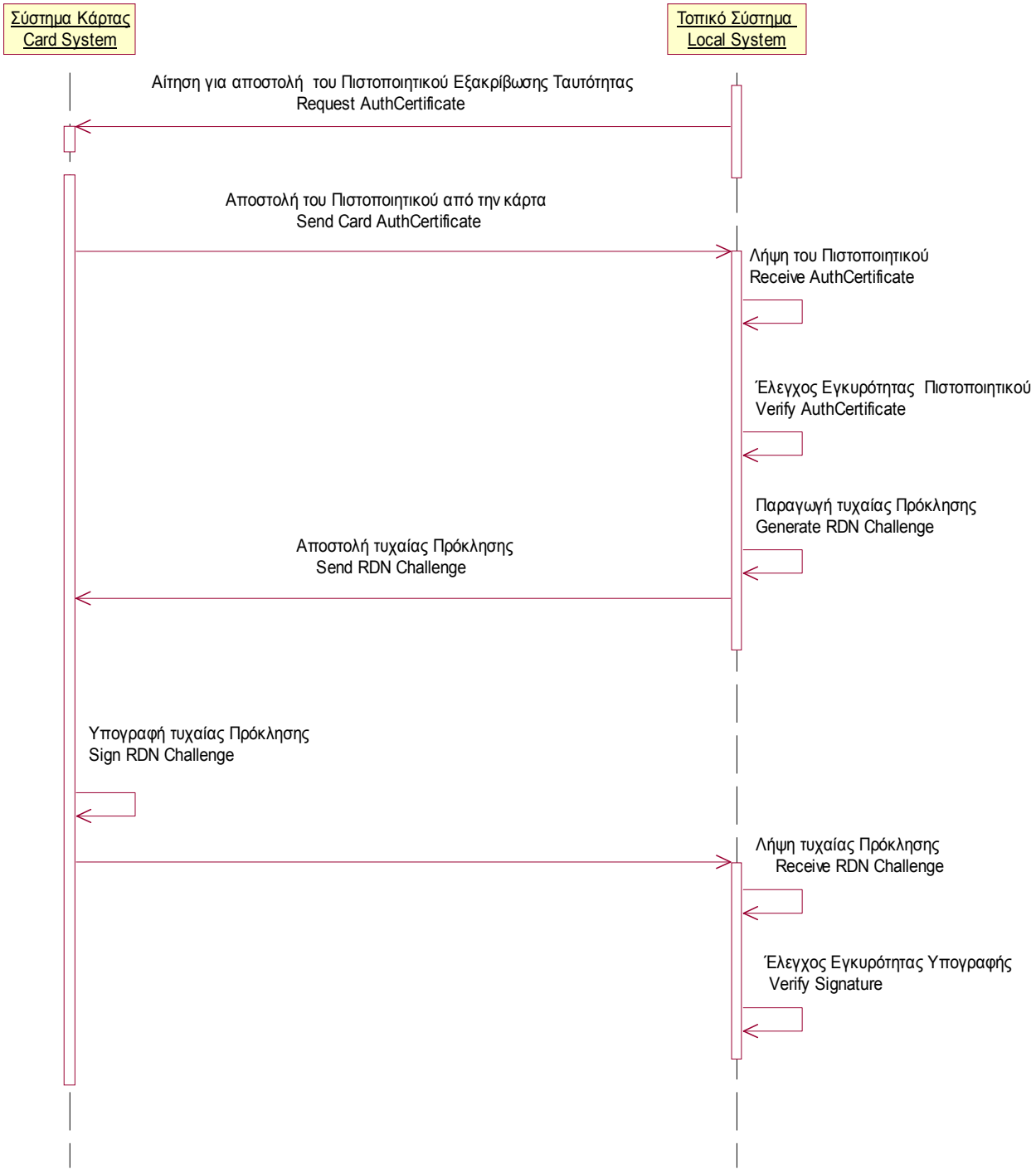
Στην περίπτωση της *εξακρίβωσης ταυτότητας εξ' αποστάσεως*, το τοπικό περιβάλλον διαθέτει ένα Διαμεσολαβητή Εξακρίβωσης Ταυτότητας (Authentication Proxy), ο οποίος ενεργεί εκ μέρους του απομακρυσμένου Τμήματος Λογισμικού Εξακρίβωσης Ταυτότητας (remote Authentication Component). Ο Διαμεσολαβητής Εξακρίβωσης Ταυτότητας επικοινωνεί με το απομακρυσμένο Τμήμα Λογισμικού Εξακρίβωσης Ταυτότητας μέσω ενός ασφαλούς Πρωτοκόλλου Εξακρίβωσης Ταυτότητας.

9.6 Διαδικασίες Εξακρίβωσης ταυτότητας (Authentication procedures)

Όπως αναφέραμε παραπάνω στο περιβάλλον των ιατρικών εφαρμογών, διακρίνουμε δυο διαφορετικές περιπτώσεις εξακρίβωσης ταυτότητας: την *Εξακρίβωση ταυτότητας τοπικά (local authentication)* και την *Εξακρίβωση ταυτότητας εξ' αποστάσεως (remote authentication)*. Σε αυτήν την παράγραφο θα παρουσιάσουμε τις δύο αντίστοιχες διαδικασίες για την εξακρίβωση της ταυτότητας για κάθε μια από αυτές τις περιπτώσεις.

9.6.1 Διαδικασία Εξακρίβωσης ταυτότητας τοπικά (Local Authentication Procedure)

Το παρακάτω διάγραμμα UML παρουσιάζει την σειρά αλληλεπιδράσεων για την εξακρίβωση ταυτότητας τοπικά.



Σχήμα 9.6.α Διάγραμμα της ακολουθίας αλληλεπιδράσεων για την εξακρίβωση της ταυτότητας τοπικά

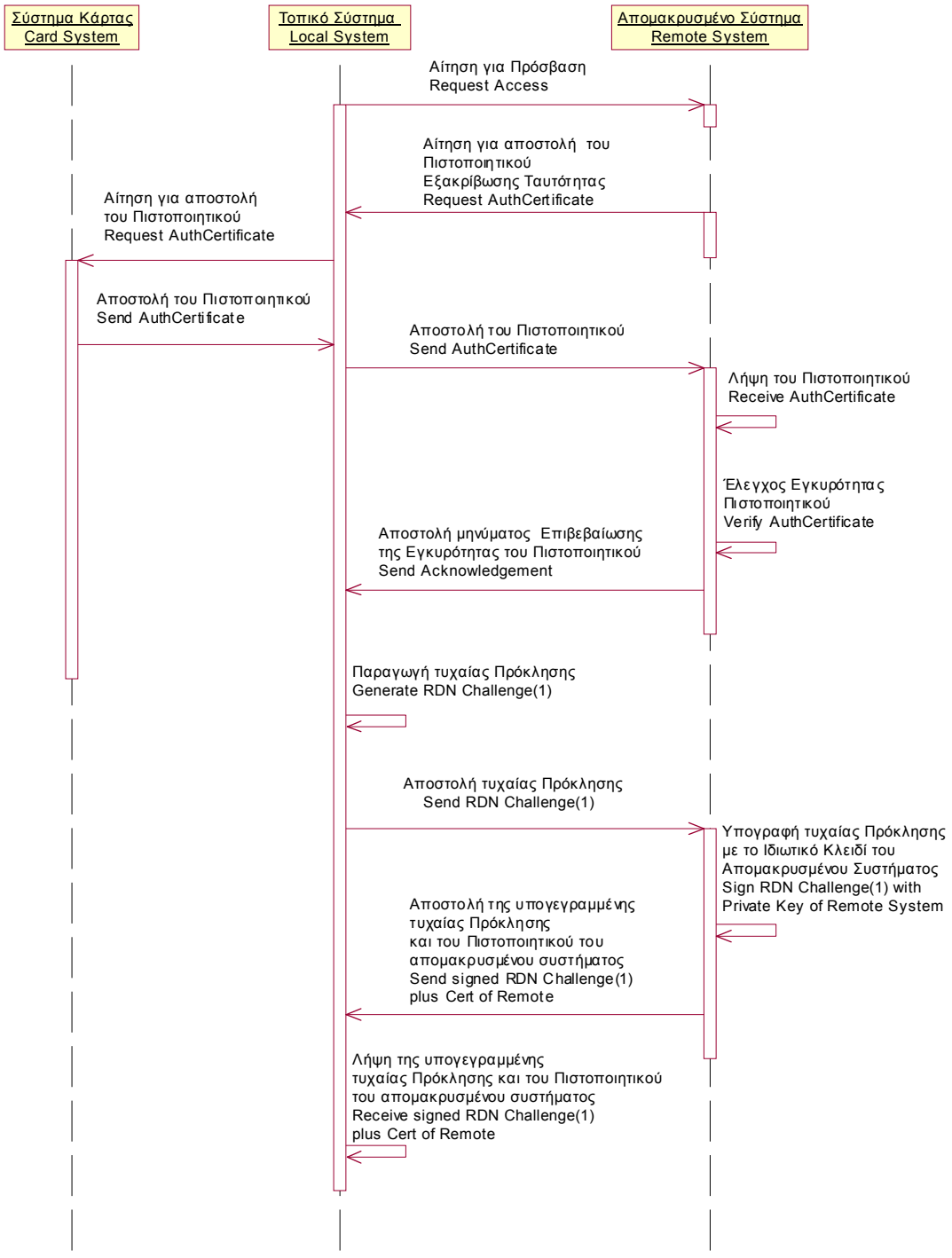
Η εξακρίβωση της ταυτότητας τοπικά γίνεται από το τμήμα λογισμικού εξακρίβωσης ταυτότητας το οποίο βρίσκεται τοπικά και το οποίο επικοινωνεί με το σύστημα της κάρτας όπου διαβάζονται τα δεδομένα που δίδει η κάρτα του χρήστη.

Η ακολουθία των αλληλεπιδράσεων για την εξακρίβωση της ταυτότητας τοπικά είναι η εξής:

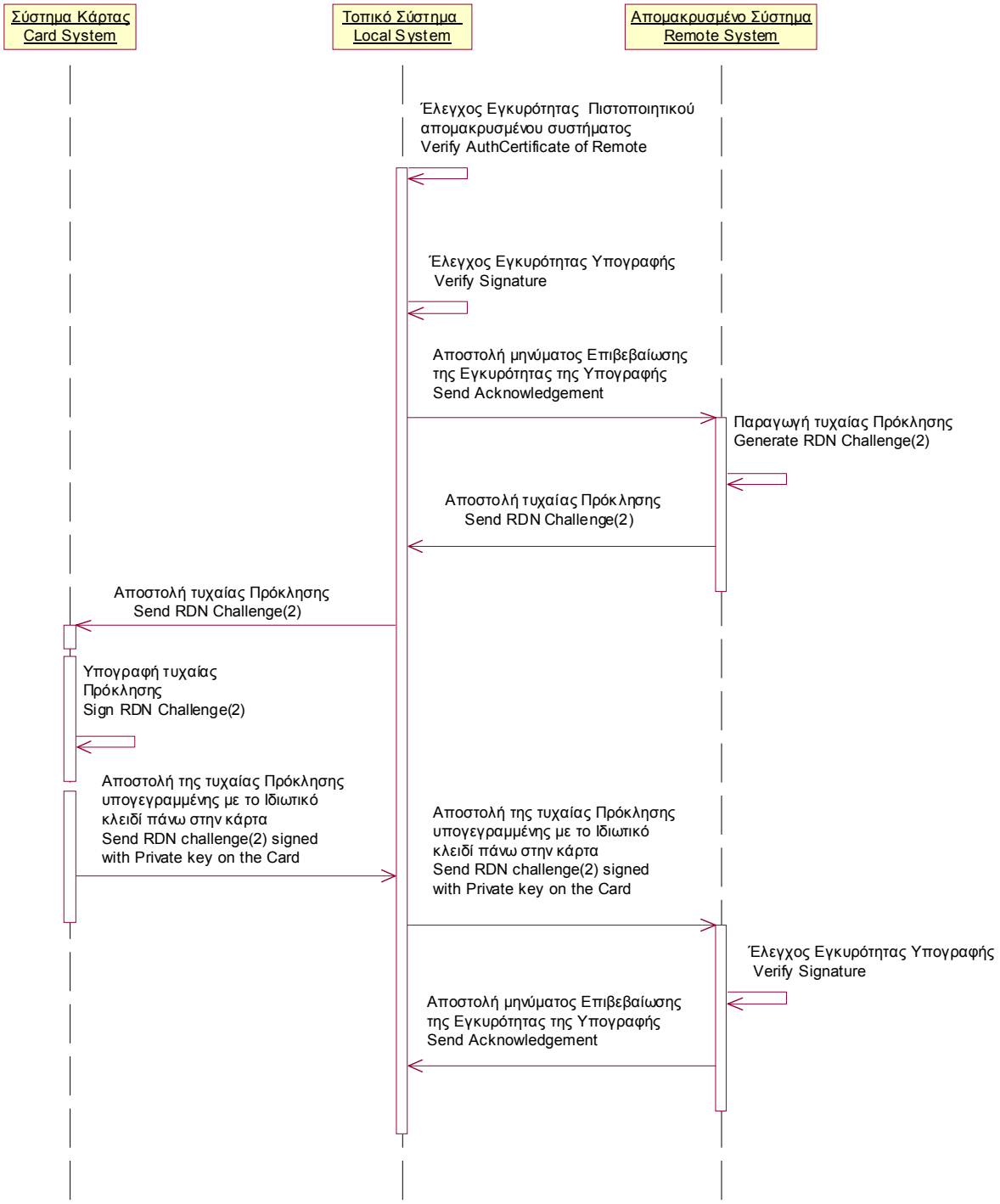
1. Το τμήμα του λογισμικού εξακρίβωσης ταυτότητας στέλνει αίτηση για αποστολή του Πιστοποιητικού Εξακρίβωσης Ταυτότητας (AuthCert - Authentication Certificate) στην κάρτα του χρήστη.
2. Το σύστημα της κάρτας στέλνει το Πιστοποιητικό Εξακρίβωσης Ταυτότητας του χρήστη στο λογισμικό εξακρίβωσης ταυτότητας.
3. Το λογισμικό εξακρίβωσης ταυτότητας λαμβάνει το Πιστοποιητικό του χρήστη από την κάρτα και ελέγχει την εγκυρότητα του.
4. Το λογισμικό εξακρίβωσης ταυτότητας παράγει μια τυχαία πρόκληση και την στέλνει στην κάρτα για να την υπογράψει.
5. Η κάρτα λαμβάνει την τυχαία πρόκληση την οποία της έστειλε το λογισμικό εξακρίβωσης ταυτότητας και την υπογράφει με το ιδιωτικό κλειδί του χρήστη το οποίο βρίσκεται προστατευμένο μέσα στην κάρτα. Αυτό γίνεται εφόσον ο χρήστης παρέχει τον σωστό Προσωπικό Κωδικό Ταυτοποίησης του (PIN) στην κάρτα για να αποδείξει ότι είναι ο νόμιμος κάτοχος της.
6. Η υπογραφή αυτή στέλνεται στο λογισμικό Εξακρίβωσης Ταυτότητας το οποίο εξακριβώνει την εγκυρότητα της υπογραφής κάνοντας χρήση του δημοσίου κλειδιού του χρήστη το οποίο λαμβάνει από το πιστοποιητικό του χρήστη.

9.6.3 Διαδικασία Εξακρίβωσης ταυτότητας εξ΄ αποστάσεως (Remote Authentication Procedure)

Τα επόμενα δύο διάγραμμα UML παρουσιάζουν την σειρά αλληλεπιδράσεων για την εξακρίβωση ταυτότητας εξ’ αποστάσεως.



Σχήμα 9.6.β.1. Διάγραμμα ακολουθίας αλληλεπιδράσεων (1) για την εξακρίβωση ταυτότητας εξ' αποστάσεως



Σχήμα 9.6.β.2. Διάγραμμα ακολουθίας αλληλεπιδράσεων (2) για την εξακρίβωση ταυτότητας εξ' αποστάσεως

Για να γίνει εξακρίβωσης ταυτότητας εξ' αποστάσεως απαιτείται η αμοιβαία εξακρίβωση ταυτότητας (mutual authentication) για να εξασφαλίσουμε την αυθεντικότητα της ταυτότητας και των δύο επικοινωνούντων μερών. Η εξακρίβωση της ταυτότητας εξ' αποστάσεως εκτελείται με τη χρήση δύο τμημάτων λογισμικού το ένα από αυτά είναι το Εξ΄ αποστάσεως Τμήμα του Λογισμικού Εξακρίβωσης Ταυτότητας (remote Authentication Component) το οποίο επικοινωνεί με τον τοπικό Διαμεσολαβητή Εξακρίβωσης Ταυτότητας (Authentication Proxy). Ο τοπικός Διαμεσολαβητής Εξακρίβωσης Ταυτότητας επικοινωνεί με το σύστημα της κάρτας όπου διαβάζονται τα δεδομένα που δίδει η κάρτα του χρήστη.

Η ακολουθία των αλληλεπιδράσεων για την εξακρίβωση της ταυτότητας εξ' αποστάσεως είναι η εξής:

1. Ο τοπικός Διαμεσολαβητή Εξακρίβωσης Ταυτότητας (Authentication Proxy) στέλνει αίτηση για πρόσβαση στο εξ΄ αποστάσεως Τμήμα του Λογισμικού Εξακρίβωσης Ταυτότητας (remote Authentication Component).
2. Το εξ' αποστάσεως Τμήμα του Λογισμικού Εξακρίβωσης Ταυτότητας ζήτα από τον τοπικό Διαμεσολαβητή Εξακρίβωσης Ταυτότητας να ανακτήσει το Πιστοποιητικού Εξακρίβωσης Ταυτότητας του χρήστη από την έξυπνη κάρτα του.
3. Το εξ΄ αποστάσεως Τμήμα του Λογισμικού Εξακρίβωσης Ταυτότητας λαμβάνει το Πιστοποιητικό του χρήστη από τον τοπικό Διαμεσολαβητή Εξακρίβωσης Ταυτότητας και ελέγχει την εγκυρότητα του. Αν το πιστοποιητικό είναι έγκυρο στέλνει μήνυμα Επιβεβαίωσης της εγκυρότητας (Acknowledgement Message) στον Διαμεσολαβητή Εξακρίβωσης Ταυτότητας. Διαφορετικά η διαδικασία σταματά αφού το πιστοποιητικό του χρήστη δεν είναι έγκυρο.
4. Ο τοπικός Διαμεσολαβητής Εξακρίβωσης Ταυτότητας παράγει μια τυχαία πρόκληση (Random Challenge) και την στέλνει στο απομακρυσμένο Τμήμα Λογισμικού Εξακρίβωσης Ταυτότητας ζητώντας του να υπογράψει με το ιδιωτικό του κλειδί. Αυτό και τα επόμενα δύο βήματα πραγματοποιούν την εξακρίβωση ταυτότητας του απομακρυσμένου Τμήματος Λογισμικού Εξακρίβωσης Ταυτότητας παρέχοντας έτσι αμοιβαία εξακρίβωση ταυτότητας στο μοντέλο.
5. Το απομακρυσμένο Τμήμα Λογισμικού Εξακρίβωσης Ταυτότητας υπογράφει με το ιδιωτικό κλειδί του την τυχαία Πρόκληση την οποία έλαβε από τον τοπικό Διαμεσολαβητή Εξακρίβωσης Ταυτότητας και στέλνει την υπογραφή μαζί με το

Πιστοποιητικό του πίσω σαν απόκριση στον τοπικό Διαμεσολαβητή Εξακρίβωσης Ταυτότητας.

6. Ο τοπικός Διαμεσολαβητής Εξακρίβωσης Ταυτότητας αφού λάβει το Πιστοποιητικό και την υπογραφή του απομακρυσμένου τμήματος Λογισμικού ελέγχει την εγκυρότητα του Πιστοποιητικού και κατόπιν εξακριβώνει την γνησιότητα της υπογραφής κάνοντας χρήση του ιδιωτικού κλειδιού του απομακρυσμένου τμήματος λογισμικού Εξακρίβωσης Ταυτότητας το οποίο παίρνει από Πιστοποιητικό του.
7. Εάν η υπογραφή και το Πιστοποιητικό του απομακρυσμένου τμήματος λογισμικού Εξακρίβωσης Ταυτότητας είναι έγκυρα τότε ο τοπικός Διαμεσολαβητής Εξακρίβωσης Ταυτότητας στέλνει μήνυμα στο απομακρυσμένο τμήμα λογισμικού Εξακρίβωσης Ταυτότητας ότι επαληθεύτηκε επιτυχώς η ταυτότητα του για να συνεχιστεί η διαδικασία της αμοιβαίας εξακρίβωσης ταυτότητας. Διαφορετικά η διαδικασία σταματά αφού το απομακρυσμένο τμήμα λογισμικού Εξακρίβωσης Ταυτότητας δεν είναι αυθεντικό.
8. Το απομακρυσμένο τμήμα λογισμικού Εξακρίβωσης Ταυτότητας συνεχίζει την διαδικασία εξακρίβωσης της ταυτότητας του χρήστη παράγοντας και στέλνοντας στον τοπικό Διαμεσολαβητή Εξακρίβωσης Ταυτότητας μια τυχαία πρόκληση την οποία ο Διαμεσολαβητής την μεταβιβάζει στην κάρτα του χρήστη για να την υπογράψει.
9. Η κάρτα λαμβάνει την τυχαία πρόκληση την οποία έστειλε το απομακρυσμένο τμήμα λογισμικού Εξακρίβωσης Ταυτότητας και την υπογράφει με το ιδιωτικό κλειδί του χρήστη το οποίο βρίσκεται προστατευμένο μέσα στην κάρτα. Αυτό γίνεται εφόσον ο χρήστης παρέχει τον σωστό Προσωπικό Κωδικό Ταυτοποίησης του (PIN) στην κάρτα για να αποδείξει ότι είναι ο νόμιμος κάτοχος της.
10. Η υπογραφή αυτή στέλνεται μέσω του Διαμεσολαβητή Εξακρίβωσης Ταυτότητας στο απομακρυσμένο τμήμα λογισμικού Εξακρίβωσης Ταυτότητας το οποίο εξακριβώνει την εγκυρότητα της υπογραφής κάνοντας χρήση του δημοσίου κλειδιού του χρήστη το οποίο λαμβάνει από το πιστοποιητικό του χρήστη.
11. Αν το Πιστοποιητικό και η υπογραφή είναι έγκυρα τότε το απομακρυσμένο τμήμα λογισμικού Εξακρίβωσης Ταυτότητας στέλνει μήνυμα στον Διαμεσολαβητή Εξακρίβωσης Ταυτότητας ότι η ταυτότητα του χρήστη

εξακριβώθηκε και είναι όντως η ισχυριζόμενη. Διαφορετικά η διαδικασία λήγει ανεπιτυχώς αφού η ταυτότητα του χρήστη δεν είναι η ισχυριζόμενη.

9.6.3 Παραγωγή της τυχαίας πρόκλησης

Η ασφάλεια του μοντέλου εξακρίβωσης ταυτότητας εξαρτάται από το μέγεθος της πρόκλησης και το πόσο τυχαία, απρόβλεπτη και μη επαναλαμβανόμενη είναι.

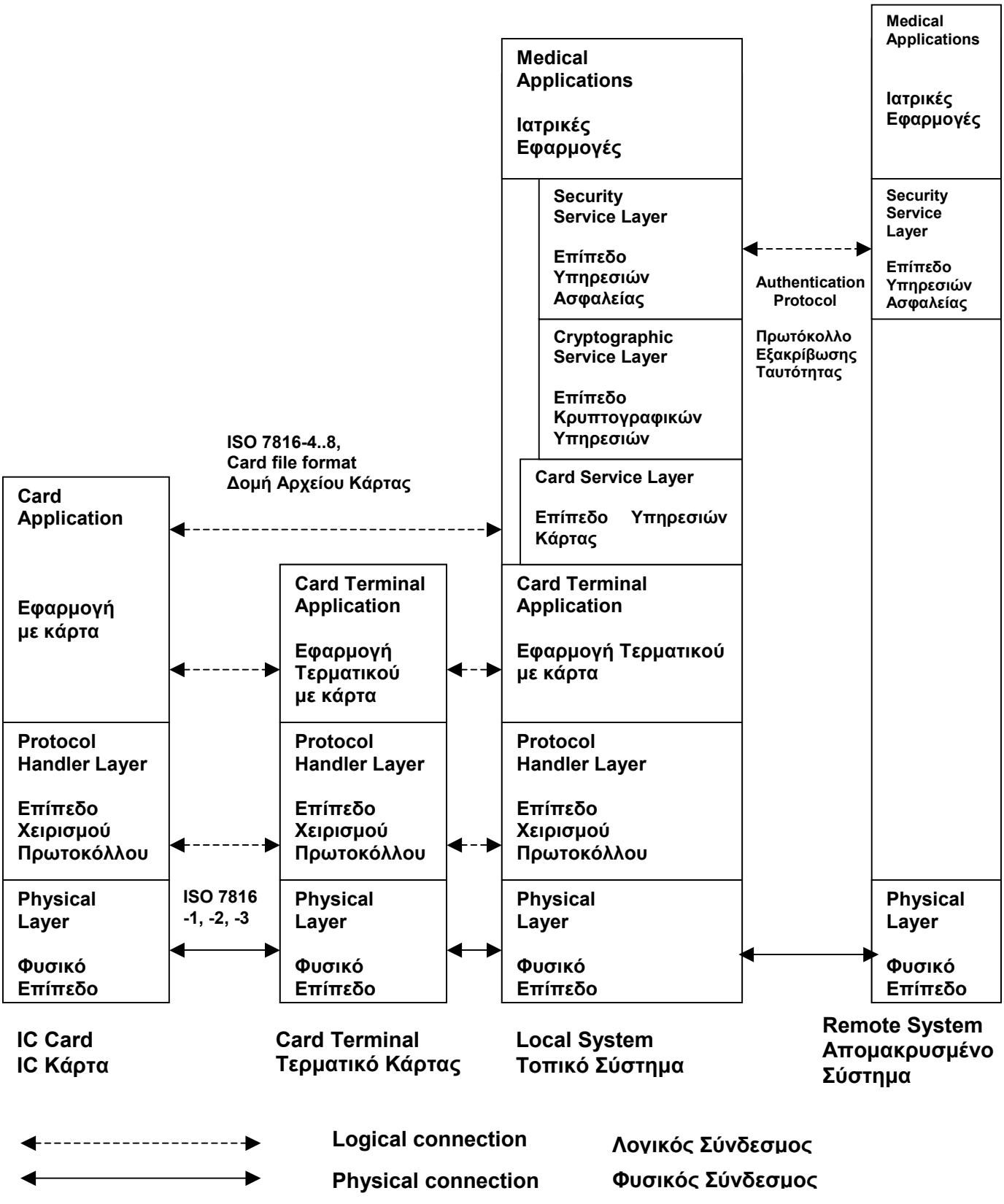
Για να είναι τυχαία η πρόκληση πρέπει να αποτελείται από τυχαίους αριθμούς. Οι τυχαίοι αριθμοί μπορούν να χρησιμοποιηθούν στους μηχανισμούς πρόκληση-απόκρισης, να παράσχουν τις διαβεβαιώσεις μοναδικότητας και επικαιρότητας, και να αποκλείσουν ορισμένες επιθέσεις επανάληψης (replay attacks). Οι τυχαίοι αριθμοί χρησιμεύουν για να παράσχουν τη μη προβλεψιμότητα, παραδείγματος χάριν, να αποκλείσουν τις επιθέσεις επιλεγμένων κειμένων (chosen text attacks). Ο όρος *τυχαίοι αριθμοί*, όταν χρησιμοποιείται στα πλαίσια των πρωτοκόλλων προσδιορισμού και επικύρωσης ταυτότητας, περιλαμβάνει τους ψευδοτυχαίους αριθμούς που είναι απρόβλεπτοι σε έναν αντίπαλο. Αυτοί διαφέρουν από το τυχαίους υπό την παραδοσιακή στατιστική έννοια. Δεν πρέπει να είναι απλώς τυχαίοι αλλά και απρόβλεπτοι. Άρα τους παράγουμε σαν αποτέλεσμα μιας συνάρτησης που λαμβάνει ως είσοδο τιμές που είναι εντελώς απρόβλεπτες (όπως π.χ. πόση είναι το ποσοστό χρήσης της μνήμης του υπολογιστή ή του επεξεργαστή του εκείνη τη χρονική στιγμή).Η πρόκληση στο σύστημα μας παράγεται με μια τέτοια συνάρτηση η όποια δίδει τυχαίους αριθμούς που έχουν όλες τις παραπάνω ιδιότητες.

Για να εξασφαλίσουμε ότι το μοντέλο εξακρίβωσης ταυτότητας που σχεδιάστηκε και υλοποιήθηκε στην παρούσα μεταπτυχιακή εργασία εξασφαλίζει την μη επαναληψημότητα της πρόκλησης συμπεριλάβαμε στην πρόκληση και μια χρόνο-σφραγίδα. Η χρόνο-σφραγίδα είναι πολύ ακριβής της τάξης των μικρό-δευτερόλεπτων και σε συνδυασμό με τους τυχαίους αριθμούς εξασφαλίζει τη μοναδικότητα, την μη προβλεψιμότητα και μη επαναληψιμότητα της πρόκλησης.

Για να εξασφαλίσουμε σε μέγιστο βαθμό τις παραπάνω ιδιότητες το μέγεθός της πρόκλησης στο σύστημα μας είναι μεγάλο (1024 ψηφία). Επίσης το μέγιστο επιτρεπόμενο χρονικό διάστημα μεταξύ των μηνυμάτων του πρωτοκόλλου μας είναι περιορισμένο ούτως ώστε να αποφύγουμε τις διάφορες επιθέσεις που αναφέραμε παραπάνω.

9.7 Το μοντέλο επίπεδων των υπηρεσιών ασφαλείας για την εξακρίβωση ταυτότητας με χρήση έξυπνων καρτών

Ένα μοντέλο με επίπεδα μπορεί επίσης να χρησιμοποιηθεί για να περιγράψει τις απαιτήσεις ασφαλείας που είναι αναγκαίες. Όσον αφορά την υπηρεσία εξακρίβωσης ταυτότητας των χρηστών ενός ιατρικού δικτύου το μοντέλο με επίπεδα που μπορεί να χρησιμοποιηθεί είναι αυτό που εικονίζεται στο επόμενο σχήμα. Στο παρακάτω σχήμα φαίνονται τα διάφορα επίπεδα, τα πρωτόκολλα επικοινωνίας μεταξύ τους και οι δομές των δεδομένων (data formats) που χρησιμοποιούνται, τα οποία θα αναλύσουμε αντίστοιχα στις επόμενες δύο υποπαραγράφους.



Σχήμα 9.7. Μοντέλο ασφαλείας (με χρήση έξυπνων καρτών) με επίπεδα

9.7.1 Τα Επίπεδα του μοντέλου υπηρεσιών ασφαλείας που βασίζεται στη χρήση έξυπνων καρτών

Τα επίπεδα του μοντέλου υπηρεσιών ασφαλείας που βασίζεται στη χρήση έξυπνων καρτών είναι τα εξής:

1. Το **Επίπεδο Υπηρεσιών Ασφαλείας (Security Service Layer)** προσφέρει υπηρεσίες σε εφαρμογές που έχουν πολύ μικρή επίγνωση του υποκείμενου μηχανισμού ασφαλείας. Παραδείγματα τέτοιων υπηρεσιών είναι «η κρυπτογράφηση δεδομένων μηνυμάτων», ή «η εξακρίβωση υπογραφών μηνυμάτων».

2. Το **Επίπεδο Κρυπτογραφικών Υπηρεσιών (Cryptographic Service Layer)** προσφέρει υπηρεσίες σε εφαρμογές που έχουν επίγνωση των υποκείμενων μηχανισμών ασφαλείας. Παραδείγματα τέτοιων υπηρεσιών είναι «η κρυπτογράφηση δεδομένων με συγκεκριμένους αλγόριθμους» ή «η δημιουργία σύνοψης μηνυμάτων από συγκεκριμένα δεδομένα».

3. Το **Επίπεδο Υπηρεσιών Κάρτας (Card Service Layer)** προσφέρει υπηρεσίες για να είναι δυνατή η χρησιμοποίηση της κάρτας σαν κρυπτογραφικό κουπόνι. Αυτό το επίπεδο κρύβει τις διαφορές των διαφορετικών λειτουργικών συστημάτων των καρτών στις εφαρμογές που είναι από πάνω τους και προσφέρει υπηρεσίες όπως το «Άνοιγμα κάρτας», «Επιλογή Αρχείου», «Ανάγνωση Αρχείου» και «Εκτέλεση Ασφαλούς Λειτουργίας». Είναι ευθύνη του Επιπέδου Υπηρεσιών της Κάρτας να μετατρέψει αυτές τις αιτήσεις υπηρεσίας (service request) στις συγκεκριμένες εντολές της κάρτας που χρησιμοποιείται.

4. Το **Επίπεδο Υπηρεσιών Τερματικού Κάρτας (Card Terminal Service Layer)** προσφέρει υπηρεσίες για την επικοινωνία μεταξύ μιας συγκεκριμένης κάρτας και ενός τερματικού κάρτας. Αυτό το επίπεδο κρύβει τις διαφορές μεταξύ των διαφορετικών υλοποιήσεων τερματικών καρτών (φυσικά χαρακτηριστικά, πρωτόκολλο μεταφοράς, πρωτόκολλο εφαρμογής) και των εφαρμογών που βρίσκονται από πάνω. Αυτό επιτυγχάνεται προσφέροντας υπηρεσίες όπως για

παράδειγμα «η Εκτέλεση Επερώτησης για την κατάσταση του τερματικού της κάρτας» ή «η Ανταλλαγή Δεδομένων Κάρτας».

5. Το **Επίπεδο Χειρισμού Πρωτοκόλλου (Protocol Handler Layer)** και το **Φυσικό Επίπεδο (Physical Layer)** προσφέρουν υπηρεσίες για την μεταφορά εντολών και αποκρίσεων μεταξύ του τοπικού συστήματος, του τερματικού κάρτας και της κάρτας (με επαφές), που βασίζεται στο πρότυπα ISO 7816-1, -2 και –3 [ISO 7816 –1,-2,-3].

9.7.2 Τα Πρωτόκολλα διεπαφής και οι δομές των δεδομένων (data formats) του μοντέλου ασφαλείας που βασίζεται στη χρήση έξυπνων καρτών

Τα Πρωτόκολλα διεπαφής και οι δομές των δεδομένων (data formats) που χρησιμοποιούνται στο μοντέλο υπηρεσιών ασφαλείας το οποίο βασίζεται στη χρήση έξυπνων καρτών στην περίπτωση της τοπικής εξακρίβωσης ταυτότητας είναι τα παρακάτω:

1. **Τα Πρωτόκολλα Φυσικού Επιπέδου (Physical Layer Protocols)** (ISO 7816-1, 2, 3) [ISO 7816 –1,-2,-3], τα οποία χειρίζεται το Φυσικό Επίπεδο (Physical Layer) και Επίπεδο Χειρισμού Πρωτοκόλλου (Protocol Handler Layer) στο τερματικό της κάρτας, στην κάρτα και στο τοπικό σύστημα.

2. **Τα Πρωτόκολλο Τερματικού Κάρτας (Card Terminal Protocol)**, το οποίο χειρίζεται το Επίπεδο Υπηρεσιών Τερματικού Κάρτας (Card Terminal Service Layer) στο τοπικό σύστημα, η Εφαρμογή Τερματικού Κάρτας (Card Terminal Application) στο τερματικό κάρτας και η Εφαρμογή Κάρτας (Card Application) στην κάρτα.

3. **Οι Εντολές και Δομές Καρτών IC (IC Card commands and formats** (ISO 7816-4) [ISO 7816 -4], τις οποίες χειρίζεται το Επίπεδο Υπηρεσιών Κάρτας (Card Service Layer) στο τοπικό σύστημα.

4. **Οι Δομές Αποθήκευσης των Αρχείων της Κάρτας (Card file storage format)** για τα ιδιωτικά κλειδιά και τα πιστοποιητικά πάνω στην έξυπνη κάρτα, τις οποίες χειρίζεται το Επίπεδο Υπηρεσιών Κάρτας (Card Service Layer) στο τοπικό σύστημα.

5. **Η Δομή Πιστοποιητικών (Certificate format),** την οποία χειρίζεται το Επίπεδο Υπηρεσιών Ασφαλείας (Security Service Layer).

Στην περίπτωση της εξακρίβωσης ταυτότητας εξ' αποστάσεως, το τοπικό περιβάλλον του χρήστη θα χειρίζεται τα τέσσερα πρώτα πρωτόκολλα. Την Δομή Πιστοποιητικών (Certificate Format) θα χειρίζεται το απομακρυσμένο τμήμα λογισμικού εξακρίβωσης ταυτότητας (remote authentication component). Σε αυτή την περίπτωση, το παρακάτω επιπλέον πρωτόκολλο μπορεί να προσδιοριστεί:

6. **Πρωτόκολλο Εξακρίβωσης Ταυτότητας Εξ' Αποστάσεως (Remote authentication protocol)** μεταξύ του τοπικού και του απομακρυσμένου περιβάλλοντος εφαρμογών.

9.8 Λειτουργίες και χαρακτηριστικά της υπηρεσία εξακρίβωσης ταυτότητας στο δίκτυο τηλεματικών υπηρεσιών στην υγεία

Αυτό το κεφάλαιο προσδιορίζει τις λειτουργίες που έχουν υλοποιηθεί, τα χαρακτηριστικά και τις απαιτήσεις που ικανοποιούνται στα τμήματα λογισμικού της υπηρεσίας εξακρίβωσης ταυτότητας που έχουμε υλοποιήσει στο τηλεματικό δίκτυο υγείας, καθώς επίσης και για τα πρωτόκολλα μεταξύ των τμημάτων αυτών του λογισμικού.

9.8.1 Λειτουργίες για την υπηρεσία της Έμπιστης Τρίτης Οντότητας (TTP service functions)

Ο παροχέας υπηρεσιών Έμπιστης Τρίτης Οντότητας στην υλοποίηση της υπηρεσίας εξακρίβωσης ταυτότητας παρέχει τις παρακάτω λειτουργίες οι οποίες περιγράφονται στις οδηγίες του ISO για τις υπηρεσίες της Έμπιστης Τρίτης Οντότητας [ISO PDTR 14516]:

1) Εγγραφή (Registration) και Εξακρίβωση της πληροφορίας για την ταυτότητα των ιατρικών επαγγελματιών (συμπεριλαμβανομένων και στοιχείων για τις ιατρικές τους ιδιότητες)
2) Έκδοση πιστοποιητικών των δημοσίων κλειδιών
3) Έκδοση καρτών στους ιατρικούς επαγγελματίες με ιδιωτικά κλειδιά και πιστοποιητικά για την εξακρίβωση της ταυτότητας του ατόμου
4) Παροχή υπηρεσίας για την ανάκληση των πιστοποιητικών
5) Παροχή υπηρεσίας καταλόγου η οποία περιέχει τα πιστοποιητικά δημοσίων κλειδιών και λιστών ανάκλησης

Επίσης οι παρακάτω απαιτήσεις εκπληρώνονται όσον αφορά την διαχείριση των πιστοποιητικών:

1) Η χρονική περίοδος εγκυρότητας ενός Πιστοποιητικού Ιατρικού Επαγγελματία πρέπει να είναι το μέγιστο 3 χρόνια.
2) Η Λίστα Ανάκλησης Πιστοποιητικών (Certificate Revocation List CRL) πρέπει να εκδίδεται με μέγιστο διάστημα μιας ώρας.

9.8.2 Χαρακτηριστικά Πιστοποιητικών

Τα πιστοποιητικά που εκδίδονται από την Έμπιστη Τρίτη Οντότητα για την Εξακρίβωση της Ταυτότητας είναι σύμφωνα με τα παρακάτω πρότυπα:

1) (X.509) – OSI Directory Authentication Framework [ISO 9594-8];
2) Profile for Internet PKIX X.509 certificate & CRL [RFC 2459];

Οι παρακάτω απαιτήσεις ικανοποιούνται για τους αλγόριθμους και τα κλειδιά:

1) Προπαρασκευή των μηνυμάτων σύνοψης των πιστοποιητικών: SHA-1 Secure hash algorithm [ISO 10118-3]
2) Υπογραφή των πιστοποιητικών: Ο αλγόριθμος δημοσίου κλειδιού RSA [PKCS #1]

3) Μήκος του ιδιωτικού κλειδιού το οποίο χρησιμοποιείται για την υπογραφή των πιστοποιητικών των ιατρικών επαγγελματιών: τουλάχιστον 2048 ψηφία (bits)

4) Μήκος του ιδιωτικού κλειδιού του χρήστη: τουλάχιστον 1024 ψηφία (bits)

9.8.3 Χαρακτηριστικά της έξυπνη κάρτα των ιατρικών επαγγελματιών

Η κάρτα του ιατρικού επαγγελματία είναι συμβατή με τα πρότυπα ISO 7816 -1, -2, -3 και –4 [ISO 7816 –1, -2, -3, -4] και έχει τα παρακάτω επιπλέον χαρακτηριστικά:

1) Υποστηρίζει τον ασυμμετρικό αλγόριθμο RSA

2) Περιέχει ένα ιδιωτικό κλειδί το οποίο να 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 να διαχειρίζεται σύμφωνα με τα πρότυπα ISO/IEC 9564-1 (Banking – PIN management and security – PIN protection principles and techniques) [ISO 9564-1] και το πρότυπο ISO/IEC 10202–6 (Financial Transaction Card –Security architecture of financial transaction systems using integrating circuit cards – Cardholder verification) [ISO 10202 –6].

6) Ο χρήστης επιτρέπεται να αλλάξει τον Προσωπικό Αριθμό Ταυτοποίησης του (PIN) όπως καθορίζεται στο πρότυπο ISO 10202-6 (υποπαράγραφος 4.2.1-Αλλαγή PIN).

7) Ούτε ο ιδιοκτήτης της κάρτας (cardholder) αλλά ούτε και ο εκδότης της (card issuer) δεν μπορούν να αλλάζουν το ιδιωτικό κλειδί που χρησιμοποιείται για την εξακρίβωση της ταυτότητας.

8) Η έξυπνη κάρτα του ιατρικού επαγγελματία περιέχει το πιστοποιητικό δημοσίου κλειδιού του ιατρικού επαγγελματία για την εξακρίβωση της ταυτότητας του, το οποίο θα μπορεί να διαβαστεί από μια εφαρμογή ενός ξενιστή (host application) χωρίς να χρειάζεται προηγουμένως να έχει δοθεί ο Προσωπικός Αριθμός Ταυτοποίησης (PIN).

9.8.4 Λειτουργίες του τοπικού συστήματος

Το τοπικό σύστημα, το οποίο αποτελείται από το σταθμό εργασίας του χρήστη και το τερματικό κάρτας (card terminal) υποστηρίζει τις παρακάτω λειτουργίες:

1) Υποστήριξη του πρωτοκόλλου του τερματικού της κάρτας
2) Έλεγχος του νόμιμου κατόχου της κάρτας, ζητώντας τον Προσωπικό Αριθμό Ταυτοποίησης (PIN) από τον χρήστη και παρουσιάζοντας τον στην έξυπνη κάρτα του ιατρικού επαγγελματία.
3) Χρησιμοποίηση του τοπικού πρωτοκόλλου εξακρίβωσης ταυτότητας για την εξακρίβωση της ταυτότητας τοπικά
4) Ανάκτηση του πιστοποιητικού από την κάρτα του ιατρικού επαγγελματία

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 (card's response) πίσω στο τμήμα του απομακρυσμένου λογισμικού εξακρίβωσης ταυτότητας.

9.8.5 Λειτουργίες του τμήματος λογισμικού εξακρίβωσης ταυτότητας

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 ιατρικού επαγγελματία.
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 έμπιστο πιστοποιητικό μιας Έμπιστης Αρχής Πιστοποίησης (CA certificate)).

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.

9.8.6 Λειτουργίες πρωτοκόλλου Εξακρίβωσης Ταυτότητας τοπικά

Το πρωτόκολλο εξακρίβωσης ταυτότητας τοπικά παρέχει τις παρακάτω λειτουργίες:

1) Μεταφορά μιας τυχαίας πρόκλησης από το τοπικό σύστημα λογισμικού εξακρίβωσης ταυτότητας στην κάρτα του ιατρικού επαγγελματία.
2) Παραλαβή της απόκρισης από την κάρτα του ιατρικού επαγγελματία.

9.8.7 Λειτουργίες πρωτοκόλλου Εξακρίβωσης Ταυτότητας εξ' αποστάσεως

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 ιατρικού επαγγελματία από το τοπικό σύστημα.

9.9 Υλοποίηση Υπηρεσίας Εξακρίβωσης Ταυτότητας

Η Υπηρεσία Εξακρίβωσης Ταυτότητας έχει υλοποιηθεί στη γλώσσα προγραμματισμού C. Για την υλοποίηση των κρυπτογραφικών λειτουργιών χρησιμοποιήθηκε η διεπιφάνεια προγραμματισμού εφαρμογών CryptoAPI 2.0 της Microsoft. Οι κάρτες που χρησιμοποιήθηκαν είναι οι κρυπτογραφικές κάρτες GPK8000 της Gemplus και οι αναγνώστες καρτών GemPC410 της ίδιας εταιρείας (που υποστηρίζουν το πρότυπο PC/SC).

Κεφάλαιο 10

Ηλεκτρονικές Υπογραφές

Οι ηλεκτρονικές υπογραφές είναι απαραίτητες για την υπογραφή της ευαίσθητης ιατρικής πληροφορίας ώστε να είναι δυνατή η εξακρίβωση της αυθεντικότητας της, της ακεραιότητας της, καθώς και η εξασφάλιση της μη άρνησης από τον υπογράφοντα της πράξης της υπογραφής.

10.1 Αντιστοιχία νομικού και τεχνολογικού πλαισίου για τις ηλεκτρονικές υπογραφές

Σήμερα, η θέσπιση ενός τεχνολογικού πλαισίου για τις ηλεκτρονικές υπογραφές σε ευαίσθητα ιατρικά δεδομένα απαιτεί γνώσεις, οικειότητα και αυξημένες δεξιότητες τόσο στο πεδίο της ασφάλειας των υπολογιστών όσο και στο ανάλογο νομικό πεδίο.

Ο συνδυασμός αυτών των δυο τομέων επιστημονικής γνώσης δεν είναι εύκολος. Οι έννοιες από τον τομέα ασφάλειας πληροφοριών αντιστοιχούν συχνά μόνο αόριστα στις έννοιες από το νομικό τομέα, ακόμη και στις περιπτώσεις όπου η ορολογία είναι παρόμοια. Παραδείγματος χάριν, στα πλαίσια της ασφάλειας πληροφοριών, ψηφιακή υπογραφή σημαίνει το αποτέλεσμα της εφαρμογής σε συγκεκριμένες πληροφορίες ορισμένων συγκεκριμένων τεχνικών διαδικασιών. Η νομική έννοια της ηλεκτρονικής υπογραφής είναι όμως ευρύτερη. Παρακάτω θα δώσουμε τους ορισμούς για τις ηλεκτρονικές υπογραφές και τα δομικά τους μέρη σύμφωνα με την Οδηγία του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της Ευρωπαϊκής Ένωσης σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές [ΚΟΙΝ. ΟΔΗΓΙΑ 99], και θα εκφράσουμε αυτές τις απαιτήσεις σε τεχνική ορολογία ασφάλειας συστημάτων.

10.1.1 Ηλεκτρονική και Προηγμένη Ηλεκτρονική Υπογραφή

Η Ευρωπαϊκή Κοινοτική Οδηγία στο κοινοτικό πλαίσιο για τις Ηλεκτρονικές Υπογραφές ορίζει τα εξής δυο είδη ηλεκτρονικής υπογραφής:

(1) **«ηλεκτρονική υπογραφή**» : δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε, ή λογικά συσχετιζόμενα με άλλα ηλεκτρονικά δεδομένα και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας,

(2) **«προηγμένη ηλεκτρονική υπογραφή»** : ηλεκτρονική υπογραφή που ανταποκρίνεται στις εξής απαιτήσεις :

(α) συνδέεται μονοσήμαντα με τον υπογράφοντα,

(β) είναι ικανή να ταυτοποιήσει τον υπογράφοντα,

(γ) δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο, και

(δ) συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο ώστε να μπορεί να εντοπιστεί οποιαδήποτε επακόλουθη αλλοίωση των εν λόγω δεδομένων.

Όπου ο "υπογράφων" ορίζεται ως: φυσικό ή νομικό πρόσωπο που κατέχει διάταξη δημιουργίας υπογραφής και ενεργεί είτε για λογαριασμό του είτε εξ' ονόματος φυσικού ή νομικού προσώπου ή φορέα που αντιπροσωπεύει.

Στο σημερινό ψηφιακό περιβάλλον, η νομική έννοια της «ηλεκτρονικής υπογραφής» όπως ορίζεται στην Κοινοτική Οδηγία είναι πολύ ευρεία και τεχνολογικά ουδέτερη. Περιλαμβάνει πολλά εντελώς διαφορετικά δεδομένα που μπορούν αποτελέσουν μια ηλεκτρονική υπογραφή, όπως για παράδειγμα σαρωμένες εικόνες χειρόγραφων υπογραφών εγγράφων ή συνημμένες διευθύνσεις ηλεκτρονικού ταχυδρομείου.

Ο ορισμός της «προηγμένης ηλεκτρονικής υπογραφής» στην Κοινοτική Οδηγία είναι όμοιος με τον ορισμό της ψηφιακής υπογραφής στο πρότυπο ISO 7498-2 [ISO 7498-2], το οποίο είναι επίσης τεχνολογικά ουδέτερο. Οι ψηφιακές υπογραφές όπως ορίζονται στο πρότυπο ISO μπορούν να υλοποιηθούν τόσο με την χρήση συμμετρικής, όσο και με τη χρήση ασυμμετρικής κρυπτογραφίας σε συνδυασμό με αδιάβλητες διατάξεις παραγωγής και επαλήθευσης των υπογραφών. Ομοίως οι «προηγμένες ηλεκτρονικές υπογραφές» μπορούν να υλοποιηθούν με τη χρήση κάποιας από τις δύο αυτές τεχνολογίες. Άρα η «προηγμένη ηλεκτρονική υπογραφή» είναι στην

πραγματικότητα ισοδύναμη με την «ψηφιακή υπογραφή» όπως ορίζεται στο πρότυπο ISO.

10.1.2 Πάροχος υπηρεσιών πιστοποίησης

Πάροχος υπηρεσιών πιστοποίησης (Certification Service Provider - CSP) ονομάζεται ο φορέας ή φυσικό ή νομικό πρόσωπο που εκδίδει πιστοποιητικά ή παρέχει άλλες υπηρεσίες, συναφείς με τις ηλεκτρονικές υπογραφές.

Ο Πάροχος Υπηρεσιών Πιστοποίησης σε μια Υποδομή Δημοσίου Κλειδιού είναι η τυπική Αρχή Πιστοποίησης. Πάροχοι Υπηρεσιών Πιστοποίησης σύμφωνα με τον παραπάνω ορισμό θεωρούνται επίσης και άλλες αρχές που παρέχουν άλλες υπηρεσίες συναφείς με τις ηλεκτρονικές υπογραφές όπως για παράδειγμα οι Αρχές Καταχώρησης (Registration Authorities).

10.1.3 Προϊόν ηλεκτρονικής υπογραφής

Προϊόν ηλεκτρονικής υπογραφής ονομάζεται το υλικό ή λογισμικό ή συναφή συστατικά στοιχεία τους, που προορίζονται για χρήση από τον πάροχο υπηρεσιών πιστοποίησης για την παροχή υπηρεσιών ηλεκτρονικής υπογραφής ή προορίζονται να χρησιμοποιηθούν για τη δημιουργία ή επαλήθευση ηλεκτρονικών υπογραφών.

Στον ορισμό του προϊόντος ηλεκτρονικής υπογραφής, η Κοινοτική Οδηγία δίδει ένα πολύ ευρύ πεδίο. Μπορούν να χρησιμοποιηθούν ως προϊόντα ηλεκτρονικής υπογραφής οι έξυπνες κάρτες για την αποθήκευση των ιδιωτικών κλειδιών, ένα ηλεκτρονικό πρόγραμμα υπογραφών όπως αυτά που είναι ενσωματωμένα σε προγράμματα περιήγησης του παγκόσμιου ιστού (web browsers), ή βιομετρικές συσκευές για να επιτρέπουν την πρόσβαση στην συνάρτηση υπογραφής.

10.1.4 Δεδομένα δημιουργίας υπογραφής & διάταξη δημιουργίας υπογραφής

Δεδομένα δημιουργίας υπογραφής ονομάζονται τα μονοσήμαντα δεδομένα όπως κώδικες ή ιδιωτικά κλειδιά κρυπτογραφίας, που χρησιμοποιούνται από τον υπογράφοντα για τη δημιουργία ηλεκτρονικής υπογραφής.

Διάταξη δημιουργίας υπογραφής ονομάζεται το διατεταγμένο υλικό ή λογισμικό που χρησιμοποιείται για την εφαρμογή των δεδομένων δημιουργίας της υπογραφής.

Μια έξυπνη κάρτα, που χρησιμοποιείται όχι μόνο για να αποθηκεύει τα ιδιωτικά κλειδιά αλλά και για να υπογράφει αποτελεσματικά, είναι ένα παράδειγμα μιας διάταξη δημιουργίας υπογραφής. Εάν η διάταξη αυτή ικανοποιεί συγκεκριμένες απαιτήσεις ασφαλείας, οι οποίες αναφέρονται και αναλύονται στις παρακάτω δύο παραγράφους τότε μπορεί να θεωρηθεί «ασφαλής διάταξη δημιουργίας υπογραφής».

10.1.5 Ασφαλείς διατάξεις δημιουργίας υπογραφής

Οι απαιτήσεις για τις ασφαλείς διατάξεις δημιουργίας υπογραφής σύμφωνα με την Κοινοτική Οδηγία είναι οι εξής:

1. Οι ασφαλείς διατάξεις δημιουργίας υπογραφής πρέπει, μέσω ενδεδειγμένων τεχνικών και διαδικαστικών μέσων, να διασφαλίζουν τουλάχιστον, ότι :

   (α) τα δεδομένα δημιουργίας υπογραφής που χρησιμοποιούνται προς παραγωγή υπογραφών απαντούν κατ'ουσίαν μόνο μια φορά και ότι το απόρρητο είναι διασφαλισμένο,

   (β) τα δεδομένα δημιουργίας υπογραφής που χρησιμοποιούνται προς παραγωγή υπογραφών δεν μπορούν, με εύλογη βεβαιότητα, να αντληθούν από αλλού και ότι η υπογραφή προστατεύεται από πλαστογραφία με τα μέσα της σύγχρονης τεχνολογίας,

   (γ) τα δεδομένα δημιουργίας υπογραφής που χρησιμοποιούνται προς παραγωγή υπογραφών μπορούν να προστατεύονται αποτελεσματικά από τον νόμιμο υπογράφοντα κατά της χρησιμοποίησης από τρίτους,

2. Οι ασφαλείς διατάξεις δημιουργίας υπογραφής δεν μεταβάλλουν τα προς υπογραφή δεδομένα ούτε εμποδίζουν την υποβολή των δεδομένων αυτών στον υπογράφοντα πριν από τη διαδικασία υπογραφής.

Ακολούθως παρουσιάζουμε τα συμπεράσματα των παραπάνω απαιτήσεων στο τεχνικό πλαίσιο των σημερινών ψηφιακών υπογραφών και της υποδομής δημοσίου κλειδιού.

Διπλά σε κάθε απαίτηση στο τεχνικό πλαίσιο σημειώνουμε την αντίστοιχη απαίτηση στο νομικό πλαίσιο μέσα σε παρένθεση.

Η ασφαλής διάταξη δημιουργίας υπογραφής θα πρέπει να ικανοποιεί τις παρακάτω απαιτήσεις:

1. Οι μηχανισμοί παραγωγοί κλειδιών πρέπει να βασίζονται σε μια καλή γεννήτρια τυχαίων ή ψευδοτυχαίων αριθμών για να αποφευχθεί το γεγονός δυο χρήστες να έχουν το ίδιο ζευγάρι κλειδιών. (1.α)
2. Ο μηχανισμός αποθήκευσης για το ιδιωτικό κλειδί πρέπει να προστατεύεται ισχυρά από τις εξωτερικές επιθέσεις πρόσβασης. (1.α)
3. Αυστηρά ερμηνευμένα πρέπει να είναι αδύνατη η αναπαραγωγή ή αντιγραφή του ιδιωτικού κλειδιού, ή όλης της ασφαλής διάταξης δημιουργίας υπογραφής μαζί με το ιδιωτικό κλειδί. Αυτό συνεπάγεται ότι το ιδιωτικό κλειδί πρέπει να παράγεται από την ασφαλή διάταξη δημιουργίας και να μην την εγκαταλείπει ποτέ, το οποίο σημαίνει ότι η δημιουργία της υπογραφής πρέπει να γίνεται πάνω στην ασφαλή διάταξη δημιουργίας της υπογραφής. Μια δεύτερη ερμηνεία υποστηρίζει ότι το «κατ' ουσίαν μια φορά» που αναφέρεται στο νομικό πλαίσιο απαιτήσεων για τα δεδομένα δημιουργίας υπογραφής σημαίνει ότι αρκεί η τιμή των ιδιωτικών κλειδιών δυο χρηστών να είναι διαφορετική.(1.α)
3. Ο κρυπτογραφικός αλγόριθμος και το μήκος του κλειδιού πρέπει να είναι αρκετά ισχυρά για να είναι πρακτικά αδυνατός ο υπολογισμός του ιδιωτικού κλειδιού από το δημόσιο κλειδί ή από την ίδια την υπογραφή, τουλάχιστον κατά όλη την διάρκεια ισχύος του αντίστοιχου πιστοποιητικού. (1.β)
4. Ο αλγόριθμός κατακερματισμού πρέπει να είναι αρκετά ισχυρός για να είναι πρακτικά αδύνατος ο υπολογισμός ενός δεύτερού μηνύματος με μια δεδομένη τιμή κατακερματισμού η οποία είναι ίδια με την τιμή κατακερματισμού ενός άλλου μηνύματος, ή ενός ζεύγους μηνυμάτων με την ίδια τιμή κατακερματισμού. (1.β)
5. Η χρήση του ιδιωτικού κλειδιού πρέπει να προστατεύεται από ένα κρυφό κωδικό πρόσβασης (password) ή Προσωπικό Αριθμό Ταυτοποίησης (PIN), ο οποίος να είναι ανθεκτικός σε κοινές επιθέσεις (π.χ. να μην μπορεί να βρεθεί με την αναζήτηση βάση λεξικού ή κοινών χρησιμοποιούμενων λέξεων). (1.γ)
6. Πρέπει να υπάρχει μηχανισμός που να εμποδίζει την εξαντλητική αναζήτηση για την εύρεση του σωστού κρυφού κωδικού. (1.γ)
7. Πρέπει να υπάρχει μηχανισμός που να εμποδίζει την εξαντλητική αναζήτηση για την εύρεση του σωστού κρυφού κωδικού. (1.γ)

10.1.6 Δεδομένα επαλήθευσης υπογραφής & Διάταξή επαλήθευσης υπογραφής

Δεδομένα επαλήθευσης υπογραφής ονομάζονται τα δεδομένα, όπως κώδικες ή δημόσια κλειδιά κρυπτογραφίας, τα οποία χρησιμοποιούνται για την επαλήθευση της ηλεκτρονικής υπογραφής.

Διάταξη επαλήθευσης υπογραφής ονομάζεται το διατεταγμένο υλικό ή λογισμικό που χρησιμοποιείται για την εφαρμογή των δεδομένων επαλήθευσης υπογραφής.

10.1.7 Πιστοποιητικό & Αναγνωρισμένο Πιστοποιητικό

Πιστοποιητικό σύμφωνα με την Κοινοτική Οδηγία ονομάζεται η ηλεκτρονική βεβαίωση, η οποία συνδέει δεδομένα επαλήθευσης υπογραφής με ένα άτομο και επιβεβαιώνει την ταυτότητά του.

Αναγνωρισμένο Πιστοποιητικό ονομάζεται το πιστοποιητικό που ανταποκρίνεται στις οριζόμενες στο Παράρτημα Ι της Κοινοτικής Οδηγίας απαιτήσεις και εκδίδεται από πάροχο υπηρεσιών πιστοποίησης ο οποίος πληροί τις οριζόμενες στο Παράρτημα ΙΙ της Κοινοτικής Οδηγίας απαιτήσεις.

Τα αναγνωρισμένα Πιστοποιητικά είναι απαραίτητα για την νομική αναγνώριση των ηλεκτρονικών υπογραφών.

10.1.8 Απαιτήσεις για τα αναγνωρισμένα πιστοποιητικά

Τα αναγνωρισμένα πιστοποιητικά σύμφωνα με το Παράρτημα Ι της Κοινοτικής Οδηγίας πρέπει να περιλαμβάνουν :

(α) ένδειξη ότι το πιστοποιητικό εκδίδεται ως αναγνωρισμένο πιστοποιητικό,

(β) τα στοιχεία αναγνώρισης του παρόχου υπηρεσιών πιστοποίησης και το κράτος στο οποίο είναι εγκατεστημένος,

(γ) το όνομα του υπογράφοντος ή ψευδώνυμο που αναγνωρίζεται ως ψευδώνυμο,

(δ) πρόβλεψη ειδικού χαρακτηριστικού του υπογράφοντος, που θα περιληφθεί εφόσον είναι σημαντικό σε σχέση με τον σκοπό για τον οποίο προορίζεται το πιστοποιητικό,

(ε) δεδομένα επαλήθευσης υπογραφής που αντιστοιχούν σε δεδομένα δημιουργίας υπογραφής υπό τον έλεγχο του υπογράφοντος,

(στ) ένδειξη της έναρξης και τέλος της περιόδου ισχύος του πιστοποιητικού,

(ζ) τον κωδικό ταυτοποίησης του πιστοποιητικού,

(η) την προηγμένη ηλεκτρονική υπογραφή του παρόχου υπηρεσιών πιστοποίησης που το εκδίδει,

(θ) ενδεχομένως, περιορισμούς του πεδίου χρήσης του πιστοποιητικού, και

(ι) ενδεχομένως όρια στο ύψος των συναλλαγών για τις οποίες το πιστοποιητικό μπορεί να χρησιμοποιηθεί.

10.1.9 Απαιτήσεις για παρόχους υπηρεσιών πιστοποίησης που εκδίδουν αναγνωρισμένα πιστοποιητικά

Οι πάροχοι υπηρεσιών πιστοποίησης που εκδίδουν αναγνωρισμένα πιστοποιητικά πρέπει:

(α) να αποδεικνύουν την απαραίτητη αξιοπιστία για την παροχή υπηρεσιών πιστοποίησης,

(β) να διασφαλίζουν την παροχή ασφαλών και αμέσων υπηρεσιών καταλόγου και ανάκλησης,

(γ) να διασφαλίζουν ότι η ημερομηνία και ο χρόνος έκδοσης ή ανάκλησης πιστοποιητικού μπορεί να προσδιοριστεί επακριβώς,

(δ) να προβαίνουν, με κατάλληλα μέσα και σύμφωνα με το εθνικό δίκαιο, σε επαλήθευση, της ταυτότητας και ενδεχομένως, τυχόν ειδικών χαρακτηριστικών του ατόμου στο όνομα του οποίου έχει εκδοθεί αναγνωρισμένο πιστοποιητικό,

(ε) να απασχολούν προσωπικό που διαθέτει την εμπειρογνωμοσύνη, την εμπειρία και τα προσόντα που είναι απαραίτητα για τις παρεχόμενες υπηρεσίες, ιδίως ικανότητα σε διαχειριστικό επίπεδο, εμπειρογνωμοσύνη στην τεχνολογία ηλεκτρονικών υπογραφών και εξοικείωση με τις κατάλληλες διαδικασίες ασφαλείας· πρέπει επίσης να χρησιμοποιούν κατάλληλες διοικητικές και διαχειριστικές διαδικασίες οι οποίες να αντιστοιχούν προς αναγνωρισμένα πρότυπα,

(στ) να χρησιμοποιούν αξιόπιστα συστήματα και προϊόντα τα οποία προστατεύονται έναντι τροποποίησης και διασφαλίζουν την τεχνική και κρυπτογραφική ασφάλεια των διεργασιών πιστοποίησης οι οποίες υποστηρίζονται από αυτά,

(ζ) να λαμβάνουν μέτρα έναντι της πλαστογράφησης πιστοποιητικών και, σε περίπτωση που ο πάροχος υπηρεσιών πιστοποίησης παράγει δεδομένα δημιουργίας υπογραφής, να εγγυώνται την τήρηση του απορρήτου κατά τη διάρκεια της διεργασίας παραγωγής των εν λόγω δεδομένων,

(η) να διαθέτουν επαρκείς χρηματικούς πόρους ώστε να λειτουργούν σύμφωνα με τις απαιτήσεις που καθορίζονται στην οδηγία, ιδίως για την ανάληψη της ευθύνης ζημιών, π.χ. με τη σύναψη κατάλληλης ασφάλισης,

(θ) να καταγράφουν το σύνολο των συναφών πληροφοριών που αφορούν ένα αναγνωρισμένο πιστοποιητικό για κατάλληλη χρονική περίοδο, ιδίως για την παροχή αποδεικτικών στοιχείων πιστοποίησης σε νομικές διαδικασίες. Η καταγραφή αυτή δύναται να πραγματοποιείται με ηλεκτρονικά μέσα,

(ι) να μην αποθηκεύουν ή αντιγράφουν δεδομένα δημιουργίας υπογραφής του ατόμου προς το οποίο ο πάροχος υπηρεσιών πιστοποίησης παρέσχε υπηρεσίες διαχείρισης κλειδιών,

(ια) προτού συνάψουν συμβατική σχέση με πρόσωπο που ζητά πιστοποιητικό από αυτούς για να κατοχυρώσει την ηλεκτρονική του υπογραφή, να το ενημερώνουν με ανθεκτικά μέσα επικοινωνίας σχετικά με τους ακριβείς όρους και προϋποθέσεις χρησιμοποίησης του πιστοποιητικού, συμπεριλαμβανομένων ενδεχόμενων περιορισμών της χρήσης του πιστοποιητικού, της ύπαρξης μηχανισμού εθελοντικής διαπίστευσης και των διαδικασιών υποβολής παραπόνων και επίλυσης διαφορών. Οι πληροφορίες αυτές, οι οποίες δύνανται να διαβιβάζονται ηλεκτρονικώς, πρέπει να παρέχονται εγγράφως, σε εύκολα καταληπτή γλώσσα. Σχετικά αποσπάσματα των πληροφοριών αυτών καθίστανται επίσης προσιτά κατόπιν αιτήματος τρίτων οι οποίοι βασίζονται στο πιστοποιητικό αυτό,

ιβ) να χρησιμοποιούν αξιόπιστα συστήματα για την αποθήκευση πιστοποιητικών σε επαληθεύσιμη μορφή, ούτως ώστε :

- μόνον αρμόδιοι να μπορούν να διενεργούν εισαγωγές και τροποποιήσεις,
- να μπορεί να ελέγχεται η γνησιότητα των πληροφοριών,

- να είναι δυνατή η κοινόχρηστη ανάκτηση πιστοποιητικών μόνον στις περιπτώσεις εκείνες για τις οποίες έχει δοθεί η συγκατάθεση του κατόχου, και
- οι τυχόν τεχνικές αλλαγές που θέτουν σε κίνδυνο τις εν λόγω απαιτήσεις ασφαλείας να γίνονται εμφανώς αντιληπτές από τον χειριστή.

Οι παραπάνω απαιτήσεις αφορούν το θέμα διαχείρισης των πιστοποιητικών το οποίο είναι περά από τα πλαίσια της παρούσας μεταπτυχιακής εργασίας. Αναφέρονται εδώ μόνο για λόγους πληρότητας.

10.1.10 Συστάσεις για την ασφαλή επαλήθευση της υπογραφής

Η Κοινοτική Οδηγία δίδει τις παρακάτω συστάσεις για την επαλήθευση των ηλεκτρονικών υπογραφών στο Παράρτημα IV:

Κατά τη διαδικασία επαλήθευσης της υπογραφής θα πρέπει να διασφαλίζεται, με εύλογη βεβαιότητα, ότι :

(α) τα δεδομένα που χρησιμοποιούνται προς επαλήθευση της υπογραφής αντιστοιχούν στα δεδομένα που εμφανίζονται στον επαληθεύοντα,

(β) η υπογραφή επαληθεύεται με αξιοπιστία και ότι το αποτέλεσμα της επαλήθευσης εμφανίζεται με τον ορθό τρόπο,

(γ) ο επαληθεύων μπορεί, ενδεχομένως, να ορίσει με βεβαιότητα τα περιεχόμενα των δεδομένων που υπογράφονται,

(δ) η γνησιότητα και η εγκυρότητα του πιστοποιητικού που απαιτείται κατά τη στιγμή της επαλήθευσης της υπογραφής έχουν ελεγχθεί με αξιοπιστία,

(ε) το αποτέλεσμα της επαλήθευσης όπως και η ταυτότητα του υπογράφοντος εμφανίζονται με τον ορθό τρόπο,

(στ) η χρησιμοποίηση ψευδωνύμου δηλώνεται εμφανώς, και

(ζ) μπορούν να εντοπιστούν τυχόν τροποποιήσεις απτόμενες της ασφάλειας.

Είναι αξιοσημείωτο ότι οι παραπάνω συστάσεις δεν περιορίζονται μόνο στις διατάξεις επαλήθευσης υπογραφής αλλά αναφέρονται στην συνολική διαδικασία επαλήθευσής της υπογραφής.

Για την επαλήθευσή της υπογραφής, η Κοινοτική Οδηγία δίδει μόνο συστάσεις. Αυτές τις συστάσεις θα εκφράσουμε τώρα σε τεχνική ορολογία ασφάλειας συστημάτων.

Η διαδικασία εξακρίβωσης της υπογραφής θα πρέπει να ικανοποιεί τις παρακάτω απαιτήσεις:

1. Η πληροφορία η οποία χρησιμοποιείται για την επαλήθευση της υπογραφής θα πρέπει να παρουσιάζεται ορθώς στον επαληθευτή της υπογραφής.
2. Η μαθηματική επαλήθευση της υπογραφής πρέπει να γίνεται ορθώς. Ο επαληθευτής πρέπει να ειδοποιείται ευκρινώς για τυχόν σφάλματα.
3. Τα περιεχόμενα του μηνύματος πρέπει να παρουσιάζονται ορθά.
4. Πρέπει να ελέγχεται η εγκυρότητα της αλυσίδας πιστοποίησης.
5. Πρέπει να ελέγχεται η κατάσταση ανάκλησης.
6. Πρέπει να υπάρχει χρονοσήμανση της υπογραφής.
7. Η ταυτότητα του υπογράφοντα πρέπει να παρουσιάζεται.
8. Η παραβίαση της ακεραιότητας (π.χ. αλλαγή στα περιεχόμενα ενός υπογεγραμμένου μηνύματος)πρέπει να επισημαίνεται.

Όλα τα θέματα επαλήθευσης της υπογραφής είναι συστάσεις, και ως εκ' τούτου μπορούν να θεωρηθούν ως μέρος των ενισχύσεων των ηλεκτρονικών υπογραφών.

Η χρονοσήμανση (timestamping) της υπογραφής απαιτείται στην περίπτωση που η υπογραφή πρέπει να ισχύσει για χρονικό διάστημα μεγαλύτερο του διαστήματος ισχύος του πιστοποιητικού του υπογράφοντα. Με την χρονοσήμανση μπορεί να αποδειχθεί η εγκυρότητα της υπογραφής από τον επαληθευτή μετά την λήξη του πιστοποιητικού του υπογράφοντα. Η χρόνο-σφραγίδα μπορεί να ληφθεί από τον επαληθευτή, ή από τον υπογράφοντα.

Η επαλήθευση μιας υπογραφής μπορεί να εκτελεστεί μετά από μια μεγάλη χρονική περίοδο από την χρονική στιγμή δημιουργίας της υπογραφής, και για αυτό τον λόγο η τωρινή ισχύουσα πληροφορία ανάκλησης δεν μπορεί να εφαρμοστεί για την χρονική στιγμή της δημιουργίας της υπογραφής. Για να επαληθεύσουμε την εγκυρότητα και την αυθεντικότητα του πιστοποιητικού του υπογράφοντα την χρονική στιγμή

δημιουργίας της υπογραφής, πρέπει να αποδειχθεί ότι τα πιστοποιητικό υπήρχε και ήταν έγκυρο εκείνη την χρονική στιγμή.

Ο πρακτικός τρόπος για να αποδειχθεί, τόσο κατά την πρώτη επαλήθευση όσο και κατά μια μετέπειτα επαλήθευση, ότι το ιδιωτικό κλειδί του υπογράφοντα χρησιμοποιήθηκε κατά την διάρκεια της χρονικής περιόδου ισχύος του πιστοποιητικού είναι να γίνει χρονοσήμανση της υπογραφής από τον υπογράφοντα. Αυτό πρέπει να γίνει όσο το δυνατόν γρηγορότερα μετά την δημιουργία της υπογραφής. Εάν η χρονική στιγμή που προσδιορίζεται από την χρόνο-σφραγίδα εμπίπτει μέσα στην χρονική περίοδο ισχύος του πιστοποιητικού, και προηγείται της τυχόν χρονικής στιγμής ανάκλησης του πιστοποιητικού, τότε η υπογραφή δημιουργήθηκε πραγματικά κατά την χρονική διάρκεια ισχύος του πιστοποιητικού, και δηλώνεται ως έγκυρη. Αν όχι, η υπογραφή δηλώνεται ως άκυρη.

Ένας άλλος τρόπος για υλοποιηθεί η επαλήθευση των υπογραφών μετά από μεγάλο χρονικό διάστημα είναι με την υποστήριξη έμπιστων υπηρεσιών αρχειοθέτησης (trusted archival services). Αυτές οι υπηρεσίες μπορούν να διατηρούν ένα αρχείο όπου να αναγράφεται η ύπαρξη και η εγκυρότητα των ηλεκτρονικών υπογραφών κοντά στην χρονική στιγμή δημιουργίας τους. Αυτό μπορεί να χρησιμοποιηθεί ως απόδειξη της εγκυρότητας μετά από μεγάλο χρονικό διάστημα.

10.1.11 Έννομες συνέπειες των ηλεκτρονικών υπογραφών

Οι έννομες συνέπειες των ηλεκτρονικών υπογραφών ορίζονται στο Άρθρο 5 της Κοινοτικής Οδηγίας. Το άρθρο αυτό ορίζει τα εξής:

1. Τα κράτη μέλη διασφαλίζουν ότι οι προηγμένες ηλεκτρονικές υπογραφές που βασίζονται σε αναγνωρισμένο πιστοποιητικό και οι οποίες δημιουργούνται από ασφαλή διάταξη δημιουργίας υπογραφής:

   (α) ικανοποιούν τις νομικές απαιτήσεις υπογραφής σε σχέση με τα δεδομένα σε ηλεκτρονική μορφή κατά τον ίδιο τρόπο που μια ιδιόχειρη υπογραφή ικανοποιεί τις απαιτήσεις αυτές σε σχέση με τα δεδομένα που καταχωρούνται επί χάρτου, και

   (β) γίνονται δεκτές ως αποδεικτικό στοιχείο σε νομικές διαδικασίες.

2. Τα κράτη μέλη διασφαλίζουν ότι δεν απορρίπτεται η νομική ισχύς και το παραδεκτό μιας ηλεκτρονικής υπογραφής ως αποδεικτικού στοιχείου σε νομικές διαδικασίες μόνο λόγω του γεγονότος ότι :
   - είναι υπό μορφή ηλεκτρονικών δεδομένων, ή
   - δεν βασίζεται σε αναγνωρισμένο πιστοποιητικό, ή
   - δεν βασίζεται σε αναγνωρισμένο πιστοποιητικό που εξεδόθη από διαπιστευμένο παροχέα υπηρεσιών πιστοποίησης, ή
   - δεν δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής.

Σαν γενική Αρχή η Κοινοτική Οδηγία δηλώνει στην παράγραφο 2 του άρθρου 5 ότι τα Κράτη Μέλη δεν πρέπει να αρνούνται την νομική ισχύ μιας ηλεκτρονικής υπογραφής ή η υπογραφή να μην γίνεται παραδεκτή ως αποδεικτικό στοιχείο σε νομικές διαδικασίες μόνο λόγω του γεγονότος ότι δεν πληρεί τους όρους του Παραρτήματος Ι και ΙΙΙ της Κοινοτικής Οδηγίας.

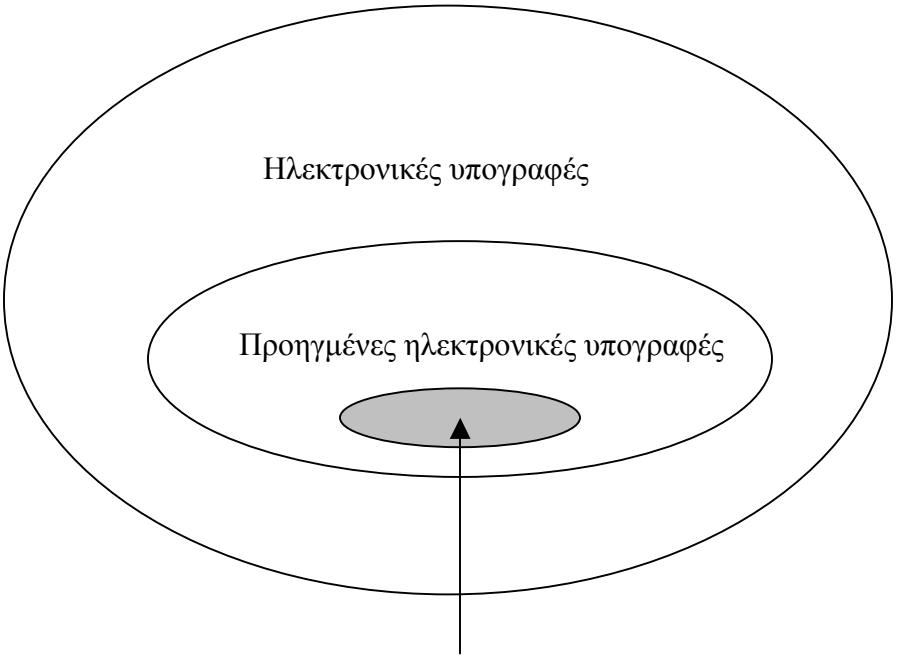
Ως εκ τούτου, αυτός ο γενικός κανόνας αποδοχής των ηλεκτρονικών υπογραφών σημαίνει ότι τα Κράτη Μέλη δεν πρέπει να απαγορεύουν με την νομοθεσία τους την χρήση των ηλεκτρονικών υπογραφών και των εργαλείων εξακρίβωσης ταυτότητας για νομικούς σκοπούς απλώς εξαιτίας της ηλεκτρονικής τους μορφής. Αυτό δεν επηρεάζει τους εθνικούς κανόνες για την ελεύθερη εκτίμηση των αποδεικτικών στοιχείων από τον δικαστή.

Η δεύτερη Αρχή της Κοινοτικής Οδηγίας είναι ότι τα Κράτη Μέλη είναι υποχρεωμένα να αναγνωρίζουν ότι συγκεκριμένοι τύποι ηλεκτρονικών υπογραφών έχουν την ίδια νομική ισχύ με τις χειρόγραφες υπογραφές (παράγραφος 1 του άρθρου 5 της Κοινοτικής Οδηγίας).

Η ισοδυναμία με τις χειρόγραφές υπογραφές θα ισχύει μόνο για ηλεκτρονικές υπογραφές που ικανοποιούν συγκεκριμένες τεχνικές απαιτήσεις ασφάλειας: μόνο οι «προηγμένες ηλεκτρονικές υπογραφές» ο οποίες βασίζονται σε «αναγνωρισμένα πιστοποιητικά» και παράγονται από μια «ασφαλή διάταξη δημιουργίας υπογραφής» θεωρούνται ισοδύναμες με τις χειρόγραφές. Αυτές οι ηλεκτρονικές υπογραφές είναι αποδεκτές ως αποδεικτικά στοιχεία σε νομικές διαδικασίες.

Οι ελάχιστες απαιτήσεις για την ικανοποίηση των τεχνικών απαιτήσεων υπάρχουν στον ορισμό της «προηγμένης ηλεκτρονικής υπογραφής» και στα

Παραρτήματα I, II, III της Κοινοτικής Οδηγίας. Αν και δεν ορίζεται στην Κοινοτική Οδηγία αυτό το είδος υπογραφής μπορεί να ονομαστεί «αναγνωρισμένη ηλεκτρονική υπογραφή»



Προηγμένες ηλεκτρονικές υπογραφές οι οποίες βασίζονται σε αναγνωρισμένα πιστοποιητικά και παράγονται από μια ασφαλή διάταξη δημιουργίας υπογραφής.

(αναγνωρισμένες ηλεκτρονικές υπογραφές)

Σχήμα 10.4 Επίπεδα νομικής ισχύς των ηλεκτρονικών υπογραφών

Το άρθρο 5 της Κοινοτικής Οδηγίας παρέχει δύο επίπεδα νομικής ισχύς των ηλεκτρονικών υπογραφών τα οποία βασίζονται στο επίπεδο της τεχνικής ασφάλειας των ηλεκτρονικών υπογραφών. Στο πρώτο επίπεδο, οι ηλεκτρονικές υπογραφές γενικά, θα έχουν νομική ισχύ. Στο δεύτερο επίπεδο, οι ηλεκτρονικές υπογραφές οι οποίες ικανοποιούν κάποιες ελάχιστες απαιτήσεις ασφαλείας θα έχουν την ίδια νομική ισχύ με τις χειρόγραφες υπογραφές.

Σε κάποιες περιπτώσεις και εφαρμογές οι τεχνικές λειτουργίες ασφάλειας που απαιτούνται από την Κοινοτική Οδηγία μπορεί να μην είναι επαρκείς. Σε αυτές τις περιπτώσεις, υπάρχουν επιπρόσθετες απαιτήσεις ασφαλείας. Για παράδειγμα η απαίτηση χρονοσήμανσης μπορεί να εισαχθεί από τους παραγωγούς υπηρεσιών και προϊόντων με στόχο την ενίσχυση της τεχνικής ασφαλείας όλων των τύπων ηλεκτρονικών υπογραφών, συμπεριλαμβανομένου και του τύπου της αναγνωρισμένης ηλεκτρονικής υπογραφής.

10.2 Τεχνολογικό Πλαίσιο για αναγνωρισμένες ηλεκτρονικές υπογραφές

Στην παρούσα μεταπτυχιακή εργασία έγινε σχεδιασμός και υλοποίηση των μηχανισμών και των τεχνολογιών που απαιτούνται για την παραγωγή και την επαλήθευση αναγνωρισμένων ηλεκτρονικών υπογραφών για ένα τηλεματικό δίκτυο υγείας όπως αυτές ορίζονται στην Ευρωπαϊκή Κοινοτική Οδηγία.

Το παρακάτω σύνολο από επιμέρους μηχανισμούς, οι οποίοι περιγράφονται σε πρότυπα και δημόσια διαθέσιμους προσδιορισμούς (specifications), επιλέχθηκε για αποτελέσει το τεχνολογικό πλαίσιο που χρησιμοποιήθηκε για τον σχεδιασμό και την υλοποίηση των μηχανισμών παραγωγής και επαλήθευσης των αναγνωρισμένων ηλεκτρονικών υπογραφών στην παρούσα μεταπτυχιακή εργασία.

Το τεχνολογικό πλαίσιο που επιλέχθηκε αποτελείται από τα εξής επιμέρους μέρη:

1. Πιστοποιητικά Δημοσίου κλειδιού και Λίστες Ανάκλησης Πιστοποιητικών X.509 (X.509 PKI Certificate and CRL Profile) [RFC 2459] (βλέπε Κεφάλαιο 5)
2. Ψηφιακές Υπογραφές με την χρήση του αλγορίθμου RSA (Digital signatures using the RSA algorithm) [ISO 14888-1, -3]
3. Οι συναρτήσεις Κατακερματισμού SHA-1 και MD5 (Hash functions SHA-1 and MD5) [ISO 10118 -3] (βλέπε Κεφάλαιο 3)
4. Σύνταξη Κρυπτογραφικών Μηνυμάτων (Cryptographic Message Syntax) [RFC2315] που βασίζεται στον δημόσια διαθέσιμο προσδιορισμό (specification) PKCS #7 από τον RSA
5. Χρήση έξυπνων καρτών [ISO 7816 part 4-7] για την ασφαλή αποθήκευση και χρήση των ιδιωτικών κλειδιών που είναι συμβατές με το πρότυπο PC/SC (Personal Computer/Smart Card) [PC/SC] (βλέπε Κεφάλαιο 7)

Ο λόγοι που επιλέχθηκε αυτό το συγκεκριμένο σύνολο τεχνολογιών είναι οι εξής:

1. Αυτές οι τεχνολογίες είναι γενικά αποδεκτές
2. Υπάρχουν πρότυπα για την χρήση όλων αυτών των τεχνολογιών
3. Το σύνολο αυτών των τεχνολογιών αποτελεί ένα τεχνολογικό πλαίσιο για τις αναγνωρισμένες ηλεκτρονικές υπογραφές σύμφωνα με την Ευρωπαϊκή Κοινοτική Οδηγία

10.2.1 Ασφαλής διάταξη δημιουργίας υπογραφής

Η τεχνολογία που επιλέχθηκε στην παρούσα μεταπτυχιακή εργασία για την υλοποίηση ασφαλούς διάταξης δημιουργίας υπογραφής, η οποία να ικανοποιεί όλες τις απαιτήσεις που ορίζονται από την κοινοτική οδηγία είναι η τεχνολογία των έξυπνων κρυπτογραφικών καρτών. Οι έξυπνές κάρτες χρησιμοποιούνται σε συνδυασμό με αναγνώστες έξυπνων καρτών.

Η ασφαλής διάταξη δημιουργίας που υλοποιήσαμε με την χρήση έξυπνης κρυπτογραφικής κάρτας εκτελεί τις παρακάτω λειτουργίες:

1. Τα «δεδομένα δημιουργίας της υπογραφής» δηλ. «το ιδιωτικό κρυπτογραφικό κλειδί το οποίο χρησιμοποιείται από τον υπογράφοντα στην δημιουργίας της ηλεκτρονικής υπογραφής», παράγεται πάνω στην έξυπνη κάρτα με μηχανισμούς παραγωγής κλειδιών οι οποίοι βασίζονται σε καλή γεννήτρια ψευδοτυχαίων αριθμών και έτσι αποφεύγεται το γεγονός δυο χρήστες να έχουν το ίδιο ζευγάρι κλειδιών.
2. Η αποθήκευση του ιδιωτικού κλειδιού γίνεται πάνω στην κάρτα και προστατεύεται ισχυρά από τις εξωτερικές επιθέσεις πρόσβασης.
3. Η αναπαραγωγή ή αντιγραφή του ιδιωτικού κλειδιού, ή όλης της κάρτας μαζί με το ιδιωτικό κλειδί είναι αδύνατη. Το ιδιωτικό κλειδί όπως αναφέραμε ήδη παράγεται από την έξυπνη κάρτα και δεν την εγκαταλείπει ποτέ, ούτε αποκαλύπτεται σε κανένα εξωτερικό παράγοντα. Το ιδιωτικό κλειδί δεν γνωρίζουν ούτε καν ο Πάροχος Υπηρεσιών Πιστοποίησης ο οποίος προσωποποιεί την κάρτα, ή ο ίδιος ο νόμιμος κάτοχος της κάρτας.
4. Η κρυπτογράφηση για την δημιουργία της υπογραφής εκτελείται πάνω στην κάρτα και με αυτό τον τρόπο το ιδιωτικό κλειδί δεν εγκαταλείπει ποτέ την κάρτα, ώστε να είναι απόλυτα ασφαλές.
5. Ο κρυπτογραφικός αλγόριθμος που χρησιμοποιούμε είναι ο RSA με μήκος κλειδιού 1024 ψηφία. Ο αλγόριθμος RSA με μήκος κλειδιού 1024 ψηφία είναι αρκετά ισχυρός ώστε να είναι πρακτικά αδύνατος, για τα σημερινά δεδομένα, ο υπολογισμός του ιδιωτικού κλειδιού από το δημόσιο κλειδί ή από την ίδια την υπογραφή, τουλάχιστον κατά όλη την διάρκεια ισχύος του αντίστοιχου πιστοποιητικού.
6. Ο αλγόριθμός κατακερματισμού που χρησιμοποιούμε είναι ο SHA-1 (ή ο MD5) οι οποίοι είναι αρκετά ισχυροί για να είναι πρακτικά αδύνατος ο

υπολογισμός ενός δεύτερού μηνύματος με μια δεδομένη τιμή σύνοψης η οποία είναι ίδια με την τιμή κατακερματισμού ενός άλλου μηνύματος, ή ενός ζεύγους μηνυμάτων με την ίδια τιμή κατακερματισμού. Ο υπολογισμός της σύνοψης του μηνύματος σήμερα δεν γίνεται πάνω στην κάρτα γιατί θα απαιτούσε πολύ χρόνο. Πιστεύουμε ότι στο μέλλον θα δημιουργηθούν ισχυρές κάρτες, οι οποίες θα έχουν την δυνατότητα υπολογισμού της σύνοψης του μηνύματος.

7. Η χρήση του ιδιωτικού κλειδιού στην κάρτα προστατεύεται από ένα Προσωπικό Αριθμό Ταυτοποίησης (PIN), ο οποίος αποτελείται από 4 έως 8 ψηφία είναι και ανθεκτικός σε επιθέσεις.
8. Ο Προσωπικός Αριθμός Ταυτοποίησης (PIN), ζητείται να δοθεί από τον κάτοχο της κάρτας κάθε φορά που εκτελείται η δημιουργία μιας υπογραφής ώστε να ελέγχεται αν ο χρήστης της κάρτας είναι ο μόνιμος κάτοχος της. Επίσης με αυτό τον τρόπο ο χρήστης συνειδητοποιεί κάθε φορά ότι εκτελεί μια πράξη υπογραφής και αποφεύγεται η εκτέλεση πράξεων υπογραφής χωρίς την συγκατάθεση του χρήστη.
9. Η εξαντλητική αναζήτηση για την εύρεση του σωστού Προσωπικού Αριθμού Ταυτοποίησης (PIN) εμποδίζεται από μηχανισμό μπλοκαρίσματος. Οι έξυπνές κάρτες κλειδώνουν μόνες τους εάν δοθεί συνεχόμενα 3 φορές λάθος PIN.

Με την χρήση των έξυπνων καρτών ως διάταξη δημιουργίας υπογραφής, την παραγωγή, αποθήκευση και εκτέλεση της υπογραφής πάνω στην κάρτα και την προστασία του ιδιωτικού κλειδιού με αυτό-απενεργοποιούμενα PIN εξασφαλίζουμε για το σύστημα μας την Υπηρεσία Ασφάλειας της Μη Άρνησης της Πράξης της Υπογραφής (Non Repudiation). Αυτό εξασφαλίζεται γιατί το ιδιωτικό κλειδί που χρησιμοποιείται από ένα άτομο για να υπογράφει ηλεκτρονικά υπάρχει μόνο στην μοναδική προσωπική του έξυπνη κάρτα, ή οποία δεν αντιγράφεται και το ιδιωτικό κλειδί όπως αναφέραμε παραπάνω προστατεύεται ισχυρά μέσα σε αυτή. Άρα με την χρήση των έξυπνων καρτών ως διάταξη δημιουργίας υπογραφής παρέχουμε την μη Άρνηση της Πράξης της Υπογραφής σε επίπεδο υλικού.

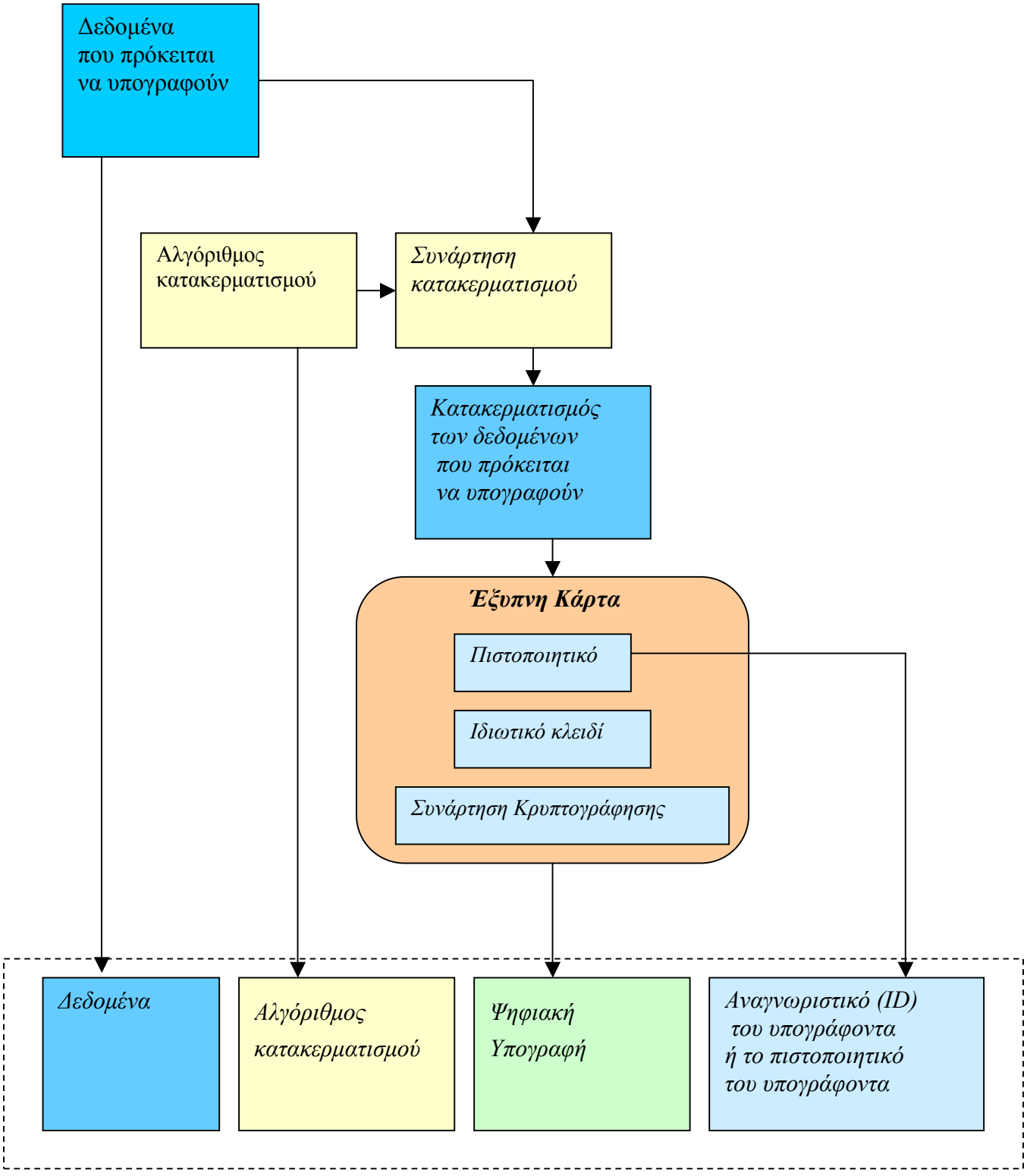
Άλλο σημαντικό πλεονέκτημα του συστήματος μας λόγω της χρησιμοποίησης των έξυπνων καρτών ως διάταξη δημιουργίας της υπογραφής είναι η φορητότητα των ιδιωτικών κλειδιών και των πιστοποιητικών. Ο χρήστης μπορεί να υπογράφει από πολλαπλούς σταθμούς εργασίας που είναι είτε στη δουλειά, είτε στο σπίτι, είτε φορητοί

υπολογιστές. Ταυτόχρονα με την φορητότητα εξασφαλίζεται όπως αναφέραμε παραπάνω και η μέγιστή ασφάλεια των ιδιωτικών κλειδιών.

Για να εξασφαλίσουμε την ανεξαρτησία από τους κατασκευαστές των καρτών και των αναγνωστών καρτών και την διαλειτουργικότητα των προϊόντων διαφορετικών κατασκευαστών στο σύστημα μας χρησιμοποιήσαμε το πρότυπο PC/SC [PC/SC] (βλέπε παράγραφο 7.5.3).

10.2.2 Διαδικασία δημιουργίας ψηφιακής υπογραφής

Το παρακάτω σχήμα παρουσιάζει την διαδικασία δημιουργίας ψηφιακής υπογραφής. Τα βήματα απαιτούνται τη δημιουργία της υπογραφής απαριθμούνται μετά το σχήμα:



Σχήμα 10.2.2. Διαδικασία Δημιουργίας της Ψηφιακής Υπογραφής

Τα βήματα που πρέπει να ακολουθήσουμε για να υπογράψουμε κάποια συγκεκριμένα ψηφιακά δεδομένα είναι τα εξής:

1. Παίρνουμε τα δεδομένα που θέλουμε να υπογράψουμε.
2. Λαμβάνουμε το πιστοποιητικό του υπογράφοντα από την έξυπνη κάρτα του. Αν δεν είναι γραμμένο πάνω σε αυτή το αναζητούμε στην αποθήκη πιστοποιητικών (η οποία μπορεί να είναι για παράδειγμα ένας κατάλογος X.500) βάση του πεδίου του ονόματος του αντικειμένου (subject name) του πιστοποιητικού το οποίο δίδει ο χρήστης.
3. Κατακερματίζουμε τα δεδομένα με τη συνάρτηση κατακερματισμού χρησιμοποιώντας τον αλγόριθμο κατακερματισμού που προσδιορίστηκε από τον υπογράφοντα. Με αυτό τον τρόπο παράγουμε την τιμή σύνοψης (hash value) των δεδομένων.
4. Κρυπτογραφούμε την σύνοψη των δεδομένων πάνω στην κάρτα με το ιδιωτικό κλειδί του υπογράφοντα που αντιστοιχεί στο πιστοποιητικό και δημιουργούμε την ψηφιακή υπογραφή των δεδομένων.
5. Στο υπογεγραμμένο μήνυμα περιλαμβάνονται τα εξής:
    - Τα υπογεγραμμένα δεδομένα
    - Το αναγνωριστικό (ID) του αλγόριθμου κατακερματισμού
    - Η υπογραφή
    - Το αναγνωριστικό (ID) του υπογράφοντα ή/και το πιστοποιητικό του
    - Η λίστα ανάκλησης πιστοποιητικών (προαιρετικά)
    - Χρόνο-σφραγίδα (προαιρετικά)

Το αναγνωριστικό (ID) του υπογράφοντα αποτελείται από το όνομα της Αρχής Πιστοποίησης που εξέδωσε το πιστοποιητικό του και τον σειριακό αριθμό του πιστοποιητικού του.

Την Λίστα Ανάκλησης Πιστοποιητικών την συμπεριλαμβάνουμε προαιρετικά στα δεδομένα της υπογραφής για να είναι δυνατός ο έλεγχος της ανάκλήσης του πιστοποιητικού κατά την επαλήθευση της υπογραφής χωρίς να είναι απαραίτητη η ανάκληση της Λίστας Ανάκλησης από το Σημείο Διανομής της (βλέπε παράγραφο 10.2.5).

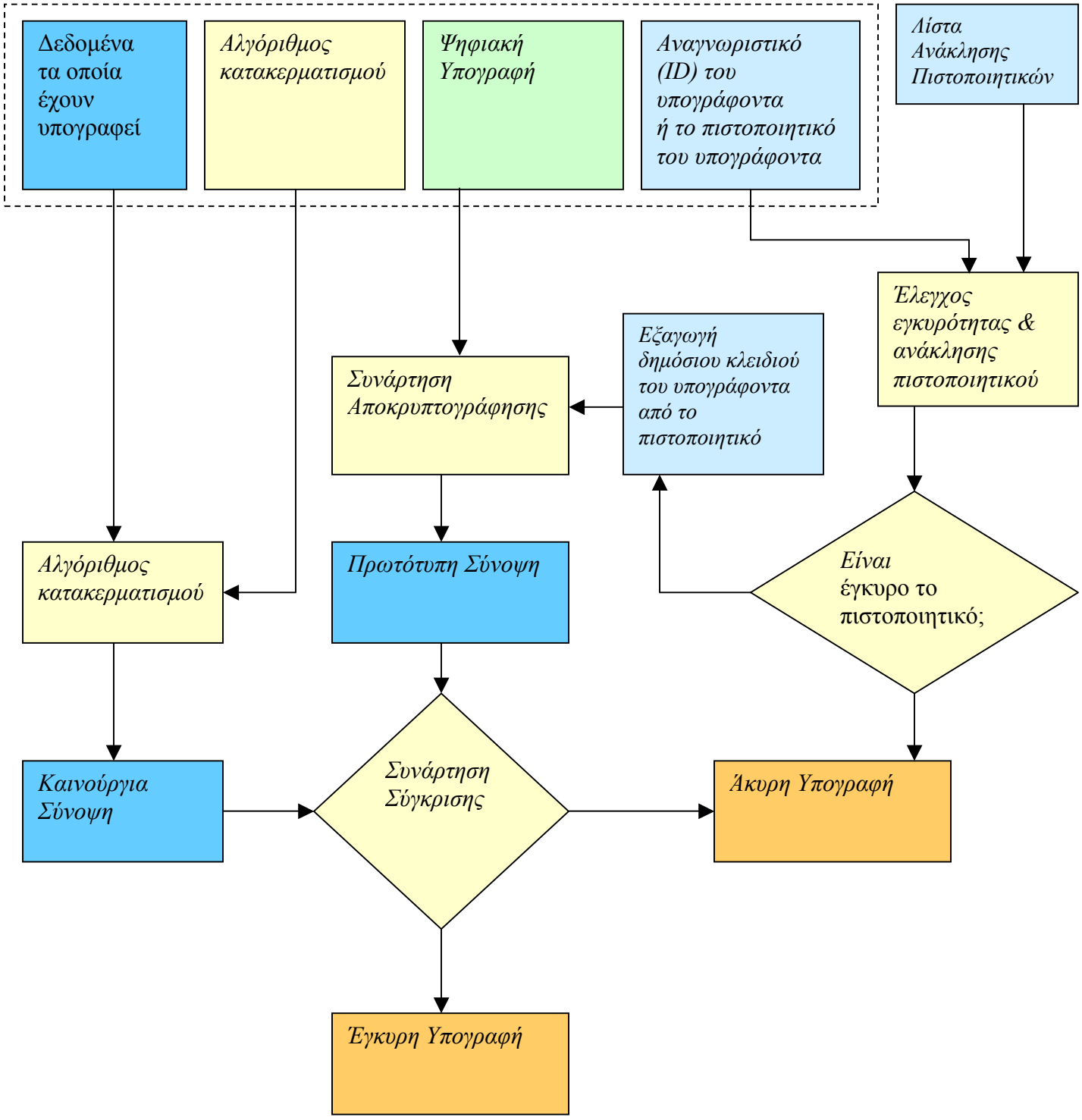
Μπορούμε να προσθέσουμε προαιρετικά χρόνο-σφραγίδα ως υπογεγραμμένο χαρακτηριστικό της υπογραφής ώστε να έχουμε ενισχυμένη ψηφιακή υπογραφή και να είναι δυνατή η επαλήθευση της υπογραφής μετά από μεγάλο χρονικό διάστημα.

10.2.3 Διαδικασία επαλήθευσης της ψηφιακής υπογραφής

Το Σχήμα 10.2.3 παρουσιάζει τη διαδικασία που πρέπει να εκτελεστεί για να επαληθευθεί η ψηφιακή υπογραφή των δεδομένων ενός μηνύματος. Τα βήματα που πρέπει να ακολουθηθούν είναι τα εξής:

1. Λαμβάνουμε τα αρχικά δεδομένα.
2. Ανακτούμε το πιστοποιητικό του υπογράφοντα και τη λίστα ανάκλησης πιστοποιητικών είτε από το υπογεγραμμένο μήνυμα είτε από το σημείο διανομής τους (που μπορεί να είναι ένας κατάλογος X.500 ή μια διεύθυνση URL).
3. Κάνουμε τον έλεγχο εγκυρότητας του πιστοποιητικού και τον έλεγχο ανάκλησης του. Εάν το πιστοποιητικό είναι έγκυρο συνεχίζουμε τη διαδικασία για την επαλήθευση της υπογραφής. Αν το πιστοποιητικό δεν είναι έγκυρο ή έχει ανακληθεί, η υπογραφή δεν είναι έγκυρη. Σε αυτή την περίπτωση σταματάμε την συνολική διεργασία δίδοντας μήνυμα στον επαληθευτή για την μη εγκυρότητα της υπογραφής.
4. Λαμβάνουμε το δημόσιο κλειδί του υπογράφοντα από το πιστοποιητικό, εφόσον το πιστοποιητικό είναι έγκυρο.
5. Χρησιμοποιώντας το δημόσιο κλειδί του υπογράφοντα, αποκρυπτογραφούμε την ψηφιακή υπογραφή και παράγουμε την πρωτότυπη σύνοψη των δεδομένων του μηνύματος.
6. Χρησιμοποιώντας τον αλγόριθμο κατακερματισμού που ορίζεται στο υπογεγραμμένο μήνυμα κατακερματίζουμε τα δεδομένα που περιέχονται στο μήνυμα. Έτσι παράγουμε μια νέα σύνοψη.
7. Συγκρίνουμε τη πρωτότυπη σύνοψη που ανακτήσαμε από το μήνυμα με την νέα σύνοψη που παραγάγαμε.
8. Αν οι δύο αυτές συνόψεις είναι ίδιες, η υπογραφή είναι έγκυρη. Αυτό σημαίνει ότι το ιδιωτικό κλειδί που χρησιμοποιήθηκε για να υπογραφούν τα δεδομένα είναι το ζεύγος του δημοσίου κλειδιού που χρησιμοποιήθηκε για να αποκρυπτογραφηθεί η υπογραφή και να γίνει ο έλεγχος της εγκυρότητας της. Επίσης ότι τα δεδομένα δεν έχουν μεταβληθεί από τότε που υπογράφηκαν. Άρα

έχει διαπιστωθεί η ακεραιότητα των υπογεγραμμένων δεδομένων και η αυθεντικότητα της υπογραφής.



Σχήμα 10.2.3. Διαδικασία επαλήθευσης της ψηφιακής υπογραφής

10.2.4 Χρήση του πιστοποιητικού X.509 ως αναγνωρισμένου πιστοποιητικού

Ένα πιστοποιητικό δημοσίου X.509 v3 [RFC 2459] με σωστή χρήση των πεδίων του είναι η καλύτερή και γενικά πιο αποδεκτή επιλογή σήμερα για να ικανοποιηθούν οι απαιτήσεις τις κοινοτική οδηγίας για το αναγνωρισμένο πιστοποιητικό. Για αυτό το λόγο επιλέχθηκε για το τεχνικό πλαίσιο των αναγνωρισμένων ηλεκτρονικών υπογραφών και την υλοποίηση του στην παρούσα μεταπτυχιακή εργασία.

Παρακάτω ορίζουμε ποια πεδία του πιστοποιητικού X.509 v3 και πως χρησιμοποιούνται ώστε να ικανοποιήσουμε τις απαιτήσεις που ορίζει η Κοινοτική Οδηγία για ένα αναγνωρισμένο πιστοποιητικό.

(α) Η ένδειξη ότι το πιστοποιητικό εκδίδεται ως αναγνωρισμένο πιστοποιητικό, ικανοποιείται θέτοντας την τιμή του Αναγνωριστικού της Πολιτικής Πιστοποιητικών (Certificate Policy Identifier) ίση με την πρότυπη «Πολιτική Πιστοποιητικών για Πάροχους Υπηρεσιών Πιστοποίησης οι οποίοι εκδίδουν αναγνωρισμένα πιστοποιητικά».

(β) Τα στοιχεία αναγνώρισης του παρόχου υπηρεσιών πιστοποίησης και το κράτος στο οποίο είναι εγκατεστημένος, γράφονται στο πεδίο του Ονόματος του Εκδότη (Issuer Name) όπου και γράφεται και το χαρακτηριστικό πεδίο της χώρας.

(γ) Το όνομα του υπογράφοντος ή ψευδώνυμο, γράφεται στο πεδίο του Ονόματος του Αντικειμένου (Subject Name). Στην περίπτωση ψευδωνύμου θέτουμε πρόθεμα ψευδώνυμο πριν το γράψουμε στο πεδίο του Ονόματος του Αντικειμένου ώστε να αναγνωρίζεται ως ψευδώνυμο.

(δ) Η πρόβλεψη ειδικού χαρακτηριστικού του υπογράφοντος, που θα περιληφθεί εφόσον είναι σημαντικό σε σχέση με τον σκοπό για τον οποίο προορίζεται το πιστοποιητικό, γράφεται είτε ως χαρακτηριστικό στο Διακεκριμένο όνομα (Distinguished name) είτε ως προέκταση (extension) του πιστοποιητικού.

(ε) Τα δεδομένα επαλήθευσης υπογραφής που αντιστοιχούν σε δεδομένα δημιουργίας υπογραφής υπό τον έλεγχο του υπογράφοντος, γράφονται στο πεδίο του πιστοποιητικού το οποίο ονομάζεται Πληροφορία Δημοσίου Κλειδιού του Αντικειμένου (Subject public key info).

(στ) Η ένδειξη της έναρξης και τέλος της περιόδου ισχύος του πιστοποιητικού, γράφεται στο πεδίο του πιστοποιητικού το οποίο ονομάζεται Ισχύς (Validity).

(ζ) Ο κωδικός ταυτοποίησης του πιστοποιητικού αποτελείται από τα πεδία του πιστοποιητικού του Ονόματος του Εκδότη (Issuer Name) και του Σειριακού Αριθμού του Πιστοποιητικού (Certificate Serial Number).

(η) Η προηγμένη ηλεκτρονική υπογραφή του παρόχου υπηρεσιών πιστοποίησης που το εκδίδει γράφεται στο πεδίο Τιμής Υπογραφής (Signature Value) του πιστοποιητικού.

(θ) Οι ενδεχόμενοι περιορισμοί του πεδίου χρήσης του πιστοποιητικού γράφονται στις προεκτάσεις του πιστοποιητικού οι οποίες ονομάζονται Χρήση Κλειδιού και Εκτεταμένη Χρήση Κλειδιού (Key Usage & Extended Key Usage extensions).

(ι) Τα ενδεχόμενα όρια στο ύψος των συναλλαγών για τις οποίες το πιστοποιητικό μπορεί να χρησιμοποιηθεί, γράφονται σε μια προέκταση του πιστοποιητικού.

10.2.5 Πληροφορία της Λίστας Ανάκλησης Πιστοποιητικών

Για τον έλεγχο της ανάκλησης των πιστοποιητικών με τη χρήση Λιστών Ανάκλησης Πιστοποιητικών, ο επαληθευτής πρέπει να είναι βέβαιος ότι παίρνει την χρονική στιγμή του πρώτου ελέγχου της εγκυρότητας του πιστοποιητικού την κατάλληλη πληροφορία για την ανάκληση των πιστοποιητικών από την Αρχή Πιστοποίησης του Υπογράφοντα. Αυτό πρέπει να γίνει όσο το δυνατό γρηγορότερα για να ελαχιστοποιηθεί η χρονική καθυστέρηση μεταξύ της δημιουργίας και του ελέγχου της εγκυρότητας της υπογραφής. Πρέπει να ελεγχθεί ότι ο σειριακός αριθμός του πιστοποιητικού του υπογράφοντα δεν περιλαμβάνεται μέσα στην λίστα ανάκλησης. Ο υπογράφοντας, ή ο επαληθευτής (ή οποιαδήποτε άλλο τρίτο μέρος) μπορούν να λάβουν την Λίστα Ανάκλησης. Εάν η Λίστα ληφθεί από τον υπογράφοντα πρέπει να μεταβιβαστεί και στον επαληθευτή.

Στο μοντέλο μας επιλέχθηκε η λίστα ανάκλησης να λαμβάνεται από τον υπογράφοντα και να αρχειοθετείται μαζί με την υπογραφή για να γίνεται πιο εύκολα ο μετέπειτα έλεγχος της εγκυρότητας των πιστοποιητικών από τον επαληθευτή. Επιπλέον εξασφαλίζεται ότι πάντα θα παρέχεται στον επαληθευτή η σωστή πληροφορία

ανάκλησης ακόμα και αν η χρονική καθυστέρηση μεταξύ της δημιουργίας και του ελέγχου της εγκυρότητας της υπογραφής είναι μεγάλη.

Εναλλακτικά, εάν επιλεχθεί η Λίστα Ανάκλησης των Πιστοποιητικών να αποθηκεύεται κάπου αλλού όπου να υπάρχει πρόσβαση από τον επαληθευτή τότε ο σειριακός αριθμός της Λίστας Ανάκλησης που χρησιμοποιείται θα πρέπει να περιλαμβάνεται μαζί με την υπογραφή.

10.2.6 Η σύνταξη και η δομή κωδικοποίησης των ηλεκτρονικών υπογραφών

Για να υποστηριχθεί η διαλειτουργικότητα (interoperability) των ηλεκτρονικών υπογραφών απαιτείται η μορφή και η δομή κωδικοποίησης τους να βασίζεται σε κάποιο πρότυπο.

Στο πλαίσιο της παρούσας μεταπτυχιακής εργασίας επιλέχθηκε το πρότυπο Συντάξεως Κρυπτογραφικού Μηνύματος CMS [RFC2315] (Cryptographic Message Syntax) το οποίο βασίζεται στην εξέλιξη του προτύπου PKCS#7 για την σύνταξη και την κωδικοποίηση των ηλεκτρονικών υπογραφών. Το πρότυπο CMS περιγράφει πως οι ηλεκτρονικές υπογραφές και η κρυπτογράφηση εφαρμόζονται σε κάθε είδους τεμαχίου (block) δεδομένων. Επίσης περιγράφει πως, επιπροσθέτως μαζί με τα δεδομένα, άλλες ιδιότητες, όπως για παράδειγμα η χρονική στιγμή της δημιουργίας της υπογραφής μπορεί να περιληφθεί στο υπογεγραμμένο μήνυμα και να προστατευτεί από την ίδια υπογραφή. Ακόμη βάση της κωδικοποίηση CMS μπορούν να συμπεριληφθούν στο υπογεγραμμένο μήνυμα πιστοποιητικά και Λίστες Ανάκλησης Πιστοποιητικών. Η σύνταξη βάση αυτού του προτύπου μπορεί να υποστηρίξει επίσης ψηφιακούς φακέλους. Αυτό σημαίνει ότι η σύνταξή υποστηρίζει αναδρομικότητα δηλαδή ότι, για παράδειγμα, ένας φάκελος μπορεί να συμπεριληφθεί σε ένα άλλο, και μπορούν να υπογραφούν υπογεγραμμένα δεδομένα μέσα σε ένα ψηφιακό φάκελο.

10.2.7 Υλοποίηση Ηλεκτρονικών Υπογραφών

Η υλοποίηση του λογισμικού δημιουργίας και εξακρίβωσης ηλεκτρονικών υπογραφών έγινε στη γλώσσα προγραμματισμού C. Για την υλοποίηση των κρυπτογραφικών λειτουργιών χρησιμοποιήθηκε η διεπιφάνεια προγραμματισμού εφαρμογών CryptoAPI 2.0 της Microsoft. Οι κάρτες που χρησιμοποιήθηκαν είναι οι κρυπτογραφικές κάρτες GPK8000 της Gemplus και οι αναγνώστες καρτών GemPC410 της ίδιας εταιρείας (που υποστηρίζουν το πρότυπο PC/SC).

Κεφάλαιο 11

Συμπεράσματα

Στα πλαίσια της παρούσας μεταπτυχιακής εργασίας μελετήθηκε (α) το ζήτημα της εξακρίβωσης ταυτότητας και (β) των ηλεκτρονικών υπογραφών σε ένα δίκτυο τηλεματικών υπηρεσιών στην υγεία. Έγινε αξιολόγηση και επιλογή του κατάλληλου τεχνολογικού πλαισίου. Τέλος σχεδιάστηκε και υλοποιήθηκε το μοντέλο ισχυρής εξακρίβωσης ταυτότητας και του μηχανισμού παραγωγής και επαλήθευσης αναγνωρισμένων ηλεκτρονικών υπογραφών (βάση της Ευρωπαϊκής Κοινοτικής Οδηγίας [ΚΟΙΝ. ΟΔΗΓΙΑ 99]).

Το τεχνολογικό πλαίσιο που επιλέχθηκε για την εξασφάλιση του ύψιστου δυνατού επίπεδου ασφαλείας για τον σχεδιασμό και την υλοποίηση των δύο παραπάνω υπηρεσιών βασίζεται στην υποδομή δημοσίου κλειδιού PKI (Public Key Infrastructure). Χρησιμοποιήθηκε ασυμμετρική κρυπτογραφία με δημόσια και ιδιωτικά κλειδιά. Η πιστοποίηση των χρηστών και των αντίστοιχων δημοσίων κλειδιών τους έγινε με την χρήση πιστοποιητικών X.509 που εκδίδονται από Έμπιστη Αρχή Πιστοποίησης. Για μέγιστη ασφάλεια πριν από κάθε χρήση πιστοποιητικού δημοσίου κλειδιού εκτελείται έλεγχος της εγκυρότητας και της κατάστασης ανάκλησης του εν λόγω πιστοποιητικού βάση Αλυσίδων Πιστοποίησης (Certificate Chains) και Λιστών Ανάκλησης Πιστοποιητικών CRL (Certificate Revocation Lists) που εκδίδονται από την Έμπιστη Αρχή Πιστοποίησης.

Η παραγωγή η αποθήκευση των ιδιωτικών κλειδιών και η εκτέλεση των αντίστοιχων απαραίτητων κρυπτογραφικών λειτουργιών γίνεται πάνω σε έξυπνες κάρτες (smart cards) με κρυπτογραφικές δυνατότητες. Έτσι επιτυγχάνουμε:

1. *Μέγιστη Ασφάλεια (Security):* Το ιδιωτικό κλειδί προστατεύεται μέσα σε μια φυσική συσκευή, την οποία μεταφέρει μαζί του ο χρήστης. Με αυτό τον τρόπο εξασφαλίζεται ο απόλυτος έλεγχος του ιδιωτικού κλειδιού του κάθε νόμιμου κάτοχου. Το ιδιωτικό κλειδί δεν εγκαταλείπει ποτέ την έξυπνη κάρτα. Οι κρυπτογραφικές λειτουργίες που κάνουν χρήση του ιδιωτικού κλειδιού εκτελούνται πάνω σε αυτή. Η έξυπνη κάρτα δεν μπορεί να αντιγραφεί, και το ένα και μοναδικό αντίγραφο του ιδιωτικού κλειδιού του χρήστη βρίσκεται μέσα της. Για να εξακριβωθεί εάν ο χρήστης της κάρτας είναι ο νόμιμος κάτοχος, ζητείται πάντα ο Προσωπικός Κωδικός Ταυτοποίησης (PIN) κατά κάθε χρήση της κάρτας για την εκτέλεση μιας πράξης υπογραφής.
2. *Φορητότητα (Mobility):* Ο χρήστης μπορεί να χρησιμοποιήσει το ιδιωτικό του κλειδί για να πιστοποιήσει την ταυτότητα του σε κάθε περιβάλλον το οποίο διαθέτει το κατάλληλο λογισμικό. Η φορητότητα είναι ένας βασικός λόγος για τη χρήση των έξυπνων καρτών στην ασφάλεια των ιατρικών πληροφοριακών συστημάτων, όπου ο ιατρικός επαγγελματίας χρειάζεται να μετακινείται.
3. *Ενημερότητα του χρήστη (User awareness):* Ο χρήστης κάνοντας χρήση των έξυπνων καρτών συνειδητοποιεί τις όψεις της ασφάλειας και το νόημα των ψηφιακών υπογραφών με απτό τρόπο. Ενημερώνεται και κάνει συνειδητά την πράξη της υπογραφής γιατί πάντα του ζητείται ο Προσωπικός Κωδικός Ταυτοποίησης του (PIN) για την χρήση του ιδιωτικού του κλειδιού.

Το μοντέλο της εξακρίβωσης ταυτότητας που σχεδιάστηκε και υλοποιήθηκε αποτελείται από δύο υπό-μοντέλα που καλύπτουν την εξακρίβωση ταυτότητας τοπικά (local authentication) και την αμοιβαία εξακρίβωση ταυτότητας εξ' αποστάσεως (mutual remote authentication).

Ο μηχανισμός παραγωγής και εξακρίβωσης υπογραφών εξασφαλίζει την παραγωγή αναγνωρισμένων υπογραφών ισοδύναμων νομικά με τις χειρόγραφές υπογραφές. Η κωδικοποίηση και η σύνταξη του υπογεγραμμένου μηνύματος βασίζεται στο πρότυπο «Σύνταξης Κρυπτογραφημένου Μηνύματος» CMS (Cryptographic Message Syntax) [CMS]. Έτσι εξασφαλίζουμε την διαλειτουργικότητα των υπογραφών.

Σαν προέκταση της παρούσας μεταπτυχιακής εργασίας προτείνεται η υπηρεσία της χρονοσήμανσης των υπογραφών να γίνεται από Έμπιστη Αρχή Χρονοσήμανσης ώστε να παράγονται ενισχυμένες ηλεκτρονικές υπογραφές.

ΕΛΛΗΝΙΚΟ ΓΛΩΣΣΑΡΙΟ

Ακεραιότητα (Integrity)

Η ιδιότητα ότι τα δεδομένα ή τα περιεχόμενα ενός μηνύματος δεν έχουν μεταβληθεί ή καταστραφεί με μη εξουσιοδοτημένο τρόπο [ISO 7498 - 2].

Απλή εξακρίβωση ταυτότητας (Simple authentication)

Εξακρίβωση ταυτότητας με χρήση απλών κωδικών πρόσβασης (password) [ISO 9594-8].

Απλό κείμενο (Plaintext)

Κατανοητά δεδομένα με σημασιολογικό περιεχόμενο.

Απόρρητο (Confidentiality)

Η παρεμπόδιση της μη εξουσιοδοτημένης αποκάλυψης πληροφορίας [ITSEC].

Αρχή Πιστοποίησης (Certification Authority)

Μια αρχή που την εμπιστεύεται μια ομάδα χρηστών για να δημιουργεί και να εκχωρεί πιστοποιητικά. Προαιρετικά η αρχή πιστοποίησης μπορεί να δημιουργεί και τα κλειδιά των χρηστών [ISO 9594-8].

Ασυμμετρικός κρυπτογραφικός αλγόριθμος (Assymetric cryptographic algorithm)

Ένας αλγόριθμος για την εκτέλεση κρυπτογράφησης ή της αντίστοιχης αποκρυπτογράφησης, όπου χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση [ISO 10181 - 1].

Ασφάλεια (Security)

Ο συνδυασμός της διαθεσιμότητας (availability), του απορρήτου (confidentiality) και της ακεραιότητας (integrity) [ITSEC].

Αυθεντικότητα (Authenticity)

Η αποφυγή της έλλειψης πληρότητας ή ακρίβειας σε εξουσιοδοτημένες αλλαγές της πληροφορίας.

Δημόσιο κλειδί (Public key)

Ένα κλειδί που χρησιμοποιείται από ασυμμετρικούς κρυπτογραφικούς αλγόριθμους και το οποίο είναι δημόσια διαθέσιμο [ISO 10181 - 1].

Διαθεσιμότητα (Availability)

Η ιδιότητα τα δεδομένα να είναι διαθέσιμα στο χρόνο και στον τόπο που χρειάζονται.

Εγκυρότητα (Validity)

Η πλήρης ακρίβεια και πληρότητα της πληροφορίας.

Έλεγχος Πρόσβασης (Access Control)

Η παρεμπόδιση μη εξουσιοδοτημένης χρήσης ενός πόρου, συμπεριλαμβανομένης και της χρήσης ενός πόρου με μη εξουσιοδοτημένο τρόπο [ISO7498 –2].

Έμπιστη Τρίτη Οντότητα (Trusted Third Party)

Μια οντότητα (ενός οργανισμού), την οποία εμπιστεύεται μια ομάδα χρηστών (domain of users) για να παρέχει υπηρεσία ασφαλείας στα μέλη που επικοινωνούν, χωρίς να εξαρτάται από τα μέλη που επικοινωνούν [EWOS/EGSEC/96/020].

Εξακρίβωση πηγής προέλευσης δεδομένων (Data origin authentication)

Η επιβεβαίωση ότι η πηγή προέλευσης των δεδομένων είναι αυθεντική [ISO 7498 - 2].

Εξακρίβωση ταυτότητας (Authentication)

Η επιβεβαίωση ότι μια οντότητα είναι αυτή που ισχυρίζεται [ISO7498 –2].

Εξουσιοδότηση (Authorization)

Η παραχώρηση δικαιωμάτων, συμπεριλαμβανομένης της παραχώρησης πρόσβασης που βασίζεται σε δικαιώματα πρόσβασης [ISO7498 –2].

Έξυπνη κάρτα (Smart Card)

Μια κάρτα με μικροεπεξεργαστή που διαβάζεται από μηχανή ανάγνωσης και περιέχει ένα chip με ολοκληρωμένο κύκλωμα , η οποία έχει την δυνατότητα να φυλάσσει δεδομένα και να εκτελεί υπολογισμούς.

Ιδιωτικό κλειδί (Private key)

Ένα κλειδί που χρησιμοποιείται από ασυμμετρικούς κρυπτογραφικούς αλγόριθμους και το οποίο κατέχουν ελάχιστα άτομα (συνήθως μια μόνο οντότητα) [ISO 10181 - 1].

Ισχυρή εξακρίβωση ταυτότητας (Strong authentication)

Εξακρίβωση ταυτότητας με κρυπτογραφικά μέσα [ISO 9594 - 8].

Κρυπτογραφημένο κείμενο (Ciphertext)

Τα δεδομένα που παράγονται με τη χρήση κωδικοποίησης. Το σημασιολογικό περιεχόμενο αυτών των δεδομένων δεν είναι κατανοητό [ISO 7498 - 2].

Κρυπτογράφηση (Encryption)

Η διαδικασία μετασχηματισμού απλού κειμένου (plain text), το οποίο μπορεί να διαβαστεί, σε κρυπτογραφημένο κείμενο (cipher text), το οποίο δεν μπορεί να διαβαστεί, για ασφάλεια ή διατήρηση του απορρήτου [ISO 7498 - 2].

Κρυπτογραφία (Cryptography)

Ο γνωστικός τομέας που περιλαμβάνει αρχές, μέσα και μεθόδους για το μετασχηματισμό των δεδομένων έτσι ώστε να αποκρυφτεί το πληροφοριακό της περιεχόμενο, και να εμποδιστεί η μη ανιχνεύσιμη μεταβολή και/ ή παρεμπόδιση της μη εξουσιοδοτημένης χρήσης [ISO7498 –2].

Κωδικός πρόσβασης (Password)

Απόρρητη πληροφορία για εξακρίβωση ταυτότητας που αποτελείται από ένα αλφαριθμητικό χαρακτήρων [ISO - 7498 -2].

Μη άρνηση πράξης (Non-repudiation)

Υπηρεσία ασφαλείας που παρέχει τη μη δυνατότητα άρνησης μιας από τις οντότητες που έχουν συμμετάσχει σε μια επικοινωνία, ότι έχουν συμμετάσχει στην όλη επικοινωνία ή σε μέρος αυτής της επικοινωνίας.

Μονόδρομη συνάρτηση (One-way function)

Μια (μαθηματική) συνάρτηση που είναι εύκολο να υπολογιστεί το αποτέλεσμα της αλλά, όταν είναι γνωστό το αποτέλεσμα, είναι υπολογιστικά αδύνατο να βρεθούν οι τιμές που είχαν δοθεί ως είσοδος για να πάρουμε αυτό το αποτέλεσμα [ISO 10181 - 1].

Μονοπάτι Πιστοποίησης (Certification Path)

Μια διατεταγμένη ακολουθία πιστοποιητικών στο Πληροφοριακό Δένδρο του Καταλόγου (Directory Information Tree), τα οποία επεξεργαζόμαστε μαζί με το δημόσιο κλειδί της αρχικής οντότητας (initial object) στο μονοπάτι για να ληφθεί το δημόσιο κλειδί της τελικής οντότητας στο μονοπάτι [ISO 9594-9].

Πιστοποίηση κλειδιού (Key certification)

Το να υπογραφεί ψηφιακά ένα κρυπτογραφικό κλειδί για να υποδηλωθεί σε τρίτα μέλη η ταυτότητα ή άλλα χαρακτηριστικά του κατόχου του κλειδιού.

Πιστοποιητικό (Certificate)

Το πιστοποιητικό συνδέει το μοναδικό όνομα μιας οντότητας με το δημόσιο κλειδί της, και περιέχει επίσης κάποια επιπλέον πληροφορία για τον κάτοχο του πιστοποιητικού και την Αρχή Πιστοποίησης. Το πιστοποιητικό κρυπτογραφείται με το ιδιωτικό κλειδί της Αρχής Πιστοποίησης και έτσι προστατεύεται από την πλαστογράφηση [ISO 9594-8].

Ποιότητα δεδομένων (Data quality)

Η ορθότητα, επικαιρότητα, ακρίβεια, πληρότητα, συνάφεια και η δυνατότητα πρόσβασης που κάνουν τα δεδομένα κατάλληλα για την χρήση τους.

Προσωπικός αριθμός ταυτοποίησης (Personal identification number)

Ένας κωδικός που αποτελείται από 4 έως 12 αλφαριθμητικούς χαρακτήρες, ο οποίος είναι ένας κωδικός πρόσβασης τον οποίο έχει ο κάτοχος μιας συσκευής για λόγους εξακρίβωσης ταυτότητας.

Συνάρτηση κατακερματισμού (Hash function)

Μια (μαθηματική) συνάρτηση που απεικονίζει τις τιμές από ένα (πιθανώς πολύ) μεγάλο σύνολο τιμών σε ένα μικρό εύρος τιμών [ISO 10181 - 1].

Ψηφιακή υπογραφή (Digital Signature)

Ο κρυπτογραφικός μετασχηματισμός μιας μονάδας δεδομένων, ο οποίος προσαρτείται σε αυτή την μονάδα δεδομένων, και δίδει την δυνατότητα στον παραλήπτη της να αποδείξει την πηγή προέλευσης των δεδομένων και την ακεραιότητα (integrity) τους. Επίσης τα προστατεύσει από πλαστογραφία (π.χ. από τον ίδιο τον παραλήπτη) [ISO 7998 - 2].

ΑΓΓΛΙΚΟ ΓΛΩΣΣΑΡΙΟ

Access Control (Έλεγχος Πρόσβασης)

Η παρεμπόδιση μη εξουσιοδοτημένης χρήσης ενός πόρου, συμπεριλαμβανομένης και της χρήσης ενός πόρου με μη εξουσιοδοτημένο τρόπο [ISO7498 –2].

Assymetric cryptographic algorithm (Ασυμμετρικός κρυπτογραφικός αλγόριθμος)

Ένας αλγόριθμος για την εκτέλεση κρυπτογράφησης ή της αντίστοιχης αποκρυπτογράφησης, όπου χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση [ISO 10181 - 1].

Authentication (Εξακρίβωση ταυτότητας)

Η επιβεβαίωση ότι μια οντότητα είναι αυτή που ισχυρίζεται [ISO7498 –2].

Authenticity (Αυθεντικότητα)

Η αποφυγή της έλλειψης πληρότητας ή ακρίβειας σε εξουσιοδοτημένες αλλαγές της πληροφορίας.

Authorization (Εξουσιοδότηση)

Η παραχώρηση δικαιωμάτων, συμπεριλαμβανομένης της παραχώρησης πρόσβασης που βασίζεται σε δικαιώματα πρόσβασης [ISO7498 –2].

Availability (Διαθεσιμότητα)

Η ιδιότητα τα δεδομένα να είναι διαθέσιμα στο χρόνο και στον τόπο που χρειάζονται.

Certificate (Πιστοποιητικό)

Το πιστοποιητικό συνδέει το μοναδικό όνομα μιας οντότητας με το δημόσιο κλειδί της, και περιέχει επίσης κάποια επιπλέον πληροφορία για τον κάτοχο του πιστοποιητικού και την Αρχή Πιστοποίησης. Το πιστοποιητικό κρυπτογραφείται με το ιδιωτικό κλειδί της Αρχής Πιστοποίησης και έτσι προστατεύεται από την πλαστογράφηση [ISO 9594-8].

Certification Authority (Αρχή Πιστοποίησης)

Μια αρχή που την εμπιστεύεται μια ομάδα χρηστών για να δημιουργεί και να εκχωρεί πιστοποιητικά. Προαιρετικά η αρχή πιστοποίησης μπορεί να δημιουργεί και τα κλειδιά των χρηστών [ISO 9594-8].

Certification Path (Μονοπάτι Πιστοποίησης)

Μια διατεταγμένη ακολουθία πιστοποιητικών στο Πληροφοριακό Δένδρο του Καταλόγου (Directory Information Tree), τα οποία επεξεργαζόμαστε μαζί με το δημόσιο κλειδί της αρχικής οντότητας (initial object) στο μονοπάτι για να ληφθεί το δημόσιο κλειδί της τελικής οντότητας στο μονοπάτι [ISO 9594-9].

Ciphertext (Κρυπτογραφημένο κείμενο)

Τα δεδομένα που παράγονται με τη χρήση κωδικοποίησης. Το σημασιολογικό περιεχόμενο αυτών των δεδομένων δεν είναι κατανοητό [ISO 7498 - 2].

Confidentiality (Απόρρητο)

Η παρεμπόδιση μη εξουσιοδοτημένης αποκάλυψης πληροφορίας [ITSEC].

Cryptography (Κρυπτογραφία)

Ο γνωστικός τομέας που περιλαμβάνει αρχές, μέσα και μεθόδους για το μετασχηματισμό των δεδομένων έτσι ώστε να αποκρυφτεί το πληροφοριακό της περιεχόμενο, και να εμποδιστεί η μη ανιχνεύσιμη μεταβολή και/ ή παρεμπόδιση της μη εξουσιοδοτημένης χρήσης [ISO7498 –2].

Data origin authentication (Εξακρίβωση πηγής προέλευσης δεδομένων)

Η επιβεβαίωση ότι η πηγή προέλευσης των δεδομένων είναι αυθεντική [ISO 7498 - 2].

Data quality (Ποιότητα δεδομένων)

Η ορθότητα, επικαιρότητα, ακρίβεια, πληρότητα, συνάφεια και η δυνατότητα πρόσβασης που κάνουν τα δεδομένα κατάλληλα για την χρήση τους.

Digital Signature (Ψηφιακή υπογραφή)

Ο κρυπτογραφικός μετασχηματισμός μιας μονάδας δεδομένων, ο οποίος προσαρτείται σε αυτή την μονάδα δεδομένων, και δίδει την δυνατότητα στον παραλήπτη της να αποδείξει την πηγή προέλευσης των δεδομένων και την ακεραιότητα (integrity) τους. Επίσης τα προστατεύσει από πλαστογραφία (π.χ. από τον ίδιο τον παραλήπτη) [ISO 7998 - 2].

Encryption (Κρυπτογράφηση)

Η διαδικασία μετασχηματισμού απλού κειμένου (plain text), το οποίο μπορεί να διαβαστεί, σε κρυπτογραφημένο κείμενο (cipher text), το οποίο δεν μπορεί να διαβαστεί, για ασφάλεια ή διατήρηση του απορρήτου [ISO 7498 - 2].

Hash function (Συνάρτηση κατακερματισμού)

Μια (μαθηματική) συνάρτηση που απεικονίζει τις τιμές από ένα (πιθανώς πολύ) μεγάλο σύνολο τιμών σε ένα μικρό εύρος τιμών [ISO 10181 - 1].

Integrity (Ακεραιότητα)

Η ιδιότητα ότι τα δεδομένα ή τα περιεχόμενα ενός μηνύματος δεν έχουν μεταβληθεί ή καταστραφεί με μη εξουσιοδοτημένο τρόπο [ISO 7498 - 2].

Key certification **(Πιστοποίηση κλειδιού)**

Το να υπογραφεί ψηφιακά ένα κρυπτογραφικό κλειδί για να υποδηλωθεί σε τρίτα μέλη η ταυτότητα ή άλλα χαρακτηριστικά του κατόχου του κλειδιού.

Non-repudiation **(Μη άρνηση πράξης)**

Υπηρεσία ασφαλείας που παρέχει τη μη δυνατότητα άρνησης μιας από τις οντότητες που έχουν συμμετάσχει σε μια επικοινωνία, ότι έχουν συμμετάσχει στην όλη επικοινωνία ή σε μέρος αυτής της επικοινωνίας.

One-way function **(Μονόδρομη συνάρτηση)**

Μια (μαθηματική) συνάρτηση που είναι εύκολο να υπολογιστεί το αποτέλεσμα της αλλά, όταν είναι γνωστό το αποτέλεσμα, είναι υπολογιστικά αδύνατο να βρεθούν οι τιμές που είχαν δοθεί ως είσοδος για να πάρουμε αυτό το αποτέλεσμα [ISO 10181 - 1].

Password **(Κωδικός πρόσβασης)**

Απόρρητη πληροφορία για εξακρίβωση ταυτότητας που αποτελείται από ένα αλφαριθμητικό χαρακτήρων [ISO - 7498 -2].

Personal identification number **(Προσωπικός αριθμός ταυτοποίησης)**

Ένας κωδικός που αποτελείται από 4 έως 12 αλφαριθμητικούς χαρακτήρες, ο οποίος είναι ένας κωδικός πρόσβασης τον οποίο έχει ο κάτοχος μιας συσκευής για λόγους εξακρίβωσης ταυτότητας.

Plaintext **(Απλό κείμενο)**

Κατανοητά δεδομένα με σημασιολογικό περιεχόμενο.

Private key **(Ιδιωτικό κλειδί)**

Ένα κλειδί που χρησιμοποιείται από ασυμμετρικούς κρυπτογραφικούς αλγόριθμους και το οποίο κατέχουν ελάχιστα άτομα (συνήθως μια μόνο οντότητα) [ISO 10181 - 1].

Public key **(Δημόσιο κλειδί)**

Ένα κλειδί που χρησιμοποιείται από ασυμμετρικούς κρυπτογραφικούς αλγόριθμους και το οποίο είναι δημόσια διαθέσιμο [ISO 10181 - 1].

Security **(Ασφάλεια)**

Ο συνδυασμός της διαθεσιμότητας (availability), του απορρήτου (confidentiality) και της ακεραιότητας (integrity) [ITSEC].

Simple authentication **(Απλή εξακρίβωση ταυτότητας)**

Εξακρίβωση ταυτότητας με χρήση απλών κωδικών πρόσβασης (password) [ISO 9594-8].

Smart Card **(Έξυπνη κάρτα)**

Μια κάρτα με μικροεπεξεργαστή που διαβάζεται από μηχανή ανάγνωσης και περιέχει ένα chip με ολοκληρωμένο κύκλωμα , η οποία έχει την δυνατότητα να φυλάσσει δεδομένα και να εκτελεί υπολογισμούς.

Strong authentication **(Ισχυρή εξακρίβωση ταυτότητας)**

Εξακρίβωση ταυτότητας με κρυπτογραφικά μέσα [ISO 9594 - 8].

Trusted Third Party **(Έμπιστη Τρίτη Οντότητα)**

Μια οντότητα (ενός οργανισμού), την οποία εμπιστεύεται μια ομάδα χρηστών (domain of users) για να παρέχει υπηρεσία ασφαλείας στα μέλη που επικοινωνούν, χωρίς να εξαρτάται από τα μέλη που επικοινωνούν.

Validity **(Εγκυρότητα)**

Η πλήρης ακρίβεια και πληρότητα της πληροφορίας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[FIPS 46-2] Federal Information Processing Standards Publication 46-2, “Data Encryption Standard (DES)”, December 1993

[Kaliski94] Jr. Kaliski, “On the Security and Performance of Several Triple-DES Modes”, RSA Laboratories, January 1994

[PKCS#1] PKCS#1: “RSA Cryptography Standard”, RSA Laboratories, version 2.0, September 1998

[PKCS#11] PKCS#11: “Cryptographic Token Interface Standard ‘Cryptoki’”, RSA Laboratories, version 2.01, December 1997

[MD5] R. Rivest, “The MD5 Message-Digest Algorithm”, MIT Laboratory for Computer Science and RSA Data Security Inc., April 1992

[FIPS 180-1] Federal Information Processing Standards Publication 46-2, “Secure Hash Standard (SHA-1)”, April 1995

[PKIXMAP] A. Arsenault, S. Turner, “Internet X.509 Public Key Infrastructure PKIX Roadmap”, IETF PKIX Working Group, March 1999

[RFC2459] R. Housley, W. Ford, W. Polk, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", January 1999

[X.500] CCITT Recommendation X.500: “The Directory – Overview of Concepts, Models, and Services”, 1998

[RFC1777] W. Yeong, T. Howes, S. Kille; “Lightweight Directory Access Protocol”, March 1995

[X.509] ITU-T Recommendation X.509 (1997 E): “Information Technology- Open Systems Interconnection - The Directory: Authentication Framework”, June 1997

[SDSI] Ronald L. Rivest, "SDSI - A Simple Distributed Security Infrastructure", Massachusetts Institute of Technology, October 1996

[RFC1991] D. Atkins, W. Stallings, P. Zimmermann, "PGP Message Exchange Formats”, August 1996

[RFC2065] D. Eastlake, C. Kaufman, "Domain Name System Security Extensions", January 1997

[RFC1422] S. Kent, ”Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management", February 1993

[PKI] “PUBLIC KEY INFRASTRUCTURE TECHNOLOGY”, ITL bulletin, National Institute of Standards and Technology (NIST), July 1997 (http://csrc.ncsl.nist.gov/pki)

[SSDD] L.C.Guillou, M.Ugon, J.J.Quisquater, “The Smart Card: A Standardized Security Device Dedicated to Public Cryptology”, pp. 561-614 in Contemporary Cryptology, ed. G.J.Simmons, IEEE Press 1991

[ENV12018] European Standard ENV12018, “Identification, administrative, and common clinical data structure for Intermittently Connected Devices used in health care”, 1997

[IBMSC] Jorge Ferrari, Robert Mackinnon, Susan Poh, Lakshman Yatawara, “Smart Cards: A Case Study”, October 1998

(http://www.redbooks.ibm.com)

[ISO 7816] ISO/IEC 7816, Identification Cards – Integrated Circuits with Contacts

Part 1: Physical Characteristics, 1998

Part 2: Dimensions and location of the contacts, 1999

Part 3: Electrical Signals and reset procedures, 1997

Part 4: Interindustry Commands for Interchage, 1995

Part 5: Numbering system and registration procedure for application identifiers, 1994

Part 6: Interindustry data elements, 1996

Part 7: Interindustry commands for Structured Card Query Language (SCQL), 1999

Part 8: Security Related Interindustry Commands, 1999

Part 10: Electronic Signals and Answers to Reset for Synchronous Cards, 1999

[MS CryptoAPI] Microsoft Cryptographic API, Application Programmer's Guide (http://www.microsoft.com)

[PC/SC] PC/SC Draft Rev. 0.9 (1996/1997) CP8 Transac, Gemplus, Hewlett-Packard, IBM Corporation, Microsoft, Schlumberger, Siemens Nixdorf Informationssysteme, Sun: "Interoperability Specification for ICCs and Personal Computer Systems" (http://www.smartcardsys.com)

[OpenCard] Network Computer Reference Profile (NCRP) 'OpenCard': Apple, IBM Corporation, Netscape, Oracle, Sun (http://www.opencard.org)

[IBMtoolkit] IBM Smart Card Toolkit: IBM Corporation (http://www.chipcard.ibm.com)

[ISO 7810] ISO/IEC 7810, "Identification cards - Physical characteristics", 1995

[ISO 7811] ISO/IEC 7811, "Identification cards - Recording technique"

Part 1: Embossing, 1995

Part 2: Magnetic stripe, 1995

Part 3: Location of embossed, 1995

Part 4: Location of read-only magnetic tracks - Tracks 1 and 2, 1995

Part 5: Location of read-write magnetic track - Track 3, 1995

Part 6: Magnetic stripe – High coercivity, 1996

[ISO 11693] ISO/IEC 11693, "Identification cards - Optical memory cards - General characteristics", July 1994

[ISO 11694-1] ISO/IEC 11694-1, "Identification cards - Optical memory cards-Linear recording method Part 1: Physical characteristics", July 1995

[ISO 7498-2] ISO/IEC 7498-2, "Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture", May 1996

[ITSEC] "Information Technology Security Evaluation Criteria", June 1991

[ISO 9594-8] ISO/IEC 9594-8, "Information technology – Open Systems Interconnection – The Directory: Authentication framework", 1994

[ISO10181-1] ISO/IEC 10181-1, "Information technology - Open Systems Interconnection – Security frameworks for open systems: Overview", 1995

[ENV 13729] European Standard ENV13729, "Health Informatics – Secure user identification – Strong authentication using microprocessor cards", 1999

[ISO PDTR 14516] ISO/IEC PDTR 14516, "Information technology- Security techniques Guidelines on the use and management of TTP services", 1996

[ISO 9564-1] ISO/IEC 9564-1, "Banking - Personal Identification Number management and security - Part 1: PIN protection principles and techniques", 1991

[ISO 10202–6] ISO/IEC 9564-6, "Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards - Part 6: Cardholder verification", 1994

[ISO 14888-1, -3] ISO/IEC 14888: "Information technology – Security techniques Digital signatures with appendix"

Part 1: General, 1998

Part 3: Certificate-based mechanisms, 1998

[ISO 10118-3] ISO/IEC 10118-3, “Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions”, 1998

[RFC2315] B. Kaliski, “PKCS #7: Cryptographic Message Syntax Version 1.5”, March 1998

[ΚΟΙΝ. ΟΔΗΓΙΑ 99] Οδηγία εκ του ευρωπαϊκού κοινοβουλίου και του συμβουλίου της ευρωπαϊκής ένωσης σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές, Δεκέμβριος 1999