ΑΣΦΑΛΕΣ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ: ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ ΚΑΙ ΣΥΣΤΗΜΑΤΑ PKI

Η εργασία υποβάλλεται για τη μερική κάλυψη των απαιτήσεων
με στόχο την απόκτηση του διπλώματος

ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ: ΕΦΟΔΙΑΣΜΟΣ ΚΑΙ ΔΙΑΚΙΝΗΣΗ ΠΡΟΪΟΝΤΩΝ (LOGISTICS)

από

ΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ ΚΑΙ ΤΟ ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΑΡΑΝΤΗΣ Χ. ΣΑΚΑΡΙΔΗΣ

ΤΜΗΜΑ ΒΙΟΜΗΧΑΝΙΚΗΣ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ 2002

ΠΡΟΛΟΓΟΣ

Η παρούσα διατριβή εκπονήθηκε για τη μερική κάλυψη των απαιτήσεων με στόχο την απόκτηση του διπλώματος στο Μεταπτυχιακό Πρόγραμμα Σπουδών με αντικείμενο την "Οργάνωση και διοίκηση βιομηχανικών συστημάτων" στην ειδίκευση "Logistics". Το Μεταπτυχιακό αυτό Πρόγραμμα συνδιοργανώνεται από το Πανεπιστήμιο Πειραιά και το Εθνικό Μετσόβιο Πολυτεχνείο.

Το θέμα της εργασίας είναι: **"Ασφαλές Ηλεκτρονικό Εμπόριο: Ψηφιακές Υπογραφές και Συστήματα PKI"**. Η εργασία εκπονήθηκε υπό την επίβλεψη του Επίκουρου Καθηγητή του Πανεπιστημίου Πειραιά κ. Γρηγ. Χονδροκούκη και ολοκληρώθηκε τον Οκτώβριο του 2002.

Προς τον επιβλέποντα Επίκουρο Καθηγητή κ. Γρηγ. Χονδροκούκη αισθάνομαι την υποχρέωση να εκφράσω τις θερμές μου ευχαριστίες, για την συμπαράστασή του και τη συμβολή του σε όλα τα στάδια της εργασίας, από την έναρξη έως και την ολοκλήρωσή της.

Σαράντης Σακαρίδης

Οκτώβριος 2002

ΠΕΡΙΕΧΟΜΕΝΑ

1. ΕΙΣΑΓΩΓΗ

1.1. Γενικά

Οι ραγδαίες τεχνολογικές εξελίξεις στον τομέα της Πληροφορικής σε συνδυασμό με την ταχύτατη εξάπλωση του Internet τα τελευταία χρόνια, έχουν προκαλέσει ουσιαστικά μια επανάσταση στο χώρο του επιχειρείν και έχουν φέρει τις επιχειρήσεις αντιμέτωπες με μια σειρά προκλήσεων. Η χρήση των νέων τεχνολογιών και του Internet (E-Commerce, E-Business κλπ) προσφέρει στις επιχειρήσεις, μέσα από προσεκτική ανασχεδίαση των επιχειρηματικών διαδικασιών (Business Process Reengineering), την ευκαιρία για μεγάλες μειώσεις κόστους, καθιέρωση νέων διαύλων με πελάτες και εταίρους και καλύτερη ολοκλήρωση της εφοδιαστικής αλυσίδας. Τα παραπάνω ενισχύονται, αν ληφθεί υπ'όψη η άρση πολλών εμπορικών περιορισμών στα πλαίσια της απελευθέρωσης των αγορών και της παγκοσμιοποίησης, γεγονός όμως που έχει σαν συνέπεια την ένταση του ανταγωνισμού και τη μείωση των περιθωρίων κέρδους.

Σε ένα τέτοιο περιβάλλον, η πληροφορία αποτελεί συχνά κρίσιμο παράγοντα επιτυχίας και σπουδαίο επιχειρηματικό κεφάλαιο. Κατά συνέπεια θα πρέπει αυτή να προστατευθεί. Καθώς οι επιχειρήσεις επωφελούνται όλο και περισσότερο από τις ευκαιρίες που παρουσιάζονται και προχωρούν στην ηλεκτρονική διεξαγωγή των επιχειρηματικών διαδικασιών σε παγκόσμια κλίμακα, ο κίνδυνος απώλειας της πληροφορίας αυξάνεται και οι συνέπειες τέτοιων απωλειών μπορεί να αποδειχτούν πολύ σοβαρές. Οι κλοπές ιδιωτικών και εμπιστευτικών επιχειρηματικών πληροφοριών και δεδομένων δεν είναι σπάνιες, ενώ αυξημένος παρουσιάζεται και ο κίνδυνος της βιομηχανικής κατασκοπείας. Έτσι οι επιχειρήσεις βρίσκονται αντιμέτωπες με την εξής κατάσταση: Από τη μια θα πρέπει να αξιοποιήσουν τις δυνατότητες του Internet προκειμένου να παραμείνουν ανταγωνιστικές, ενώ από την άλλη εκθέτουν κατ' αυτόν τον τρόπο κρίσιμες επιχειρηματικές τους πληροφορίες σε σοβαρούς κινδύνους. Αυτό συμβαίνει επειδή όσο πιο πολύ ένα εταιρικό δίκτυο ανοίγεται στον κόσμο του E-Business τόσο περισσότερο είναι εκτεθειμένο σε πιθανές επιθέσεις.

Γενικότερα, το ζητούμενο σήμερα δεν είναι πλέον η απαγόρευση ή ο περιορισμός της πρόσβασης στα εταιρικά πληροφοριακά συστήματα, αλλά η μεγιστοποίηση της δυνατότητας πρόσβασης, με ελεγχόμενο όμως τρόπο.

Για την υλοποίηση μηχανισμών ασφαλείας των εταιρικών πληροφοριακών συστημάτων έχουν αναπτυχθεί πολλές τεχνικές και επιμέρους μηχανισμοί, όπως για παράδειγμα τα Firewalls (συστήματα για την επιβολή περιορισμών και ελέγχων, τόσο για τους εισερχομένους στο εταιρικό δίκτυο, όσο και για τους εξερχομένους), τα συστήματα ανίχνευσης εισβολών (Intrusion Detection Systems – IDS) κλπ. Οι μηχανισμοί αυτού του είδους, παρ' ότι εξακολουθούν να είναι χρήσιμοι, διέπονται από μια "αμυντική" φιλοσοφία που εστιάζει στην έννοια της περιμέτρου και επικεντρώνεται στην προστασία των συστημάτων που βρίσκονται στο εσωτερικό της περιμέτρου.

Από την άλλη πλευρά όμως, το σύγχρονο επιχειρηματικό μοντέλο έχει μια αρκετά διαφορετική μορφή: Η πρόσβαση στα δεδομένα της επιχείρησης επιτρέπεται στους

συνεργαζόμενους εταίρους (partners), προκειμένου να χαραχθούν από κοινού στρατηγικές και να διευκολυνθεί η κοινή χρήση τεχνολογιών για ανάπτυξη νέων προϊόντων. Ανάλογη πρόσβαση έχουν και οι πελάτες της επιχείρησης, για να προβούν π.χ. σε on-line παραγγελίες ή να προσπελάσουν χρήσιμες πληροφορίες σχετικά με την τεχνική υποστήριξη των προϊόντων. Εξάλλου, διάφορες εταιρίες συμβούλων, αλλά και ανάδοχοι κατασκευής έργων ή παροχής υπηρεσιών βάσει συμβάσεων, έχουν επίσης ανάγκη πρόσβασης στα πληροφοριακά συστήματα της επιχείρησης. Τέλος, είναι δυνατόν ορισμένες επιχειρηματικές διαδικασίες να διεκπεραιώνονται μέσω πληροφορικού εξοπλισμού και λογισμικού που δεν είναι ιδιοκτησία της επιχείρησης, αλλά βρίσκεται στις εγκαταστάσεις (και υπό τον έλεγχο και την ευθύνη) ενός τρίτου μέρους (application service providers).

Εχοντας υπ' όψη τα παραπάνω, είναι εξαιρετικά δύσκολο έως πρακτικά αδύνατο να ορισθεί η "περίμετρος" που θα οριοθετήσει το "εσωτερικό" της επιχείρησης και, κατά συνέπεια, τα συστήματα που θα έπρεπε να προστατευθούν. Στην πραγματικότητα απαιτείται μια διαφορετική προσέγγιση στο θέμα της ασφάλειας, η οποία θα εστιάζει περισσότερο στην ίδια την πληροφορία και στα χαρακτηριστικά που συνοδεύουν τη διακίνησή της.

Κατ' αναλογία με το παραδοσιακό περιβάλλον, ένα περιβάλλον ηλεκτρονικού εμπορίου περιλαμβάνει διάφορες οντότητες (φυσικά πρόσωπα, οργανισμούς, αλλά και μηχανές) που συναλλάσσονται μεταξύ τους, ανταλλάσσουν ηλεκτρονικά έγγραφα και διεκπεραιώνουν μια σειρά από διαδικασίες, βάσει προκαθορισμένων κανόνων. Η επικοινωνία μεταξύ των εμπλεκομένων είναι αφ' ενός ψηφιακής μορφής και αφ' ετέρου μερικώς ή και πλήρως αυτοματοποιημένη, διεξάγεται δε μέσω του Internet, το οποίο είναι εξ ορισμού ένα ανασφαλές μέσο. Τέλος, είναι δυνατόν να απαιτηθεί ανταλλαγή πληροφοριών μεταξύ οντοτήτων (π.χ. χρηστών) που δεν έχουν κάποια προηγούμενη άλλου είδους γνωριμία, αλλά "συναντώνται" για πρώτη φορά στα πλαίσια μιας ηλεκτρονικής συναλλαγής.
Κατά συνέπεια, είναι απαραίτητο οι εμπλεκόμενοι να διαθέτουν ένα είδος "ψηφιακής ταυτότητας", προκειμένου να μπορούν να συμμετάσχουν "επώνυμα" σε μια ηλεκτρονική συναλλαγή. Η ύπαρξη ταυτοτήτων, οι οποίες μπορούν να επιδειχθούν σε κάθε ενδιαφερόμενο συντελεί στη δημιουργία εμπιστοσύνης, η οποία είναι απαραίτητη για τη διενέργεια συναλλαγών. Τίθεται βεβαίως το ζήτημα του ποιός είναι υπεύθυνος για την έκδοση τέτοιου είδους ταυτοτήτων. Εξάλλου, οι εμπλεκόμενοι θα πρέπει να μπορούν να υπογράψουν ηλεκτρονικά έγγραφα ή να δεσμευτούν απέναντι σε τρίτους για την εκπλήρωση των υποχρεώσεων που αναλαμβάνουν, με χρήση π.χ. **ψηφιακών υπογραφών**.

1.2. Βασικές αρχές ασφάλειας πληροφοριών και συστήματα PKI

Γενικότερα, η πληροφορία που δημιουργείται ή διακινείται κατά τη διεξαγωγή μιας ηλεκτρονικής συναλλαγής σχετίζεται άμεσα με τους εμπλεκόμενους στην υπ' όψη συναλλαγή και θα πρέπει να διασφαλιστεί απέναντι σε όλους τους πιθανούς κινδύνους, όπως υποκλοπή, αλλοίωση, ανεπιθύμητη κοινοποίηση σε τρίτους κλπ. Για το σκοπό αυτό απαιτείται η δημιουργία ενός περιβάλλοντος ηλεκτρονικών συναλλαγών, το οποίο, επιπλέον της ασφάλειας των συστημάτων, θα δίνει έμφαση στην ασφάλεια των ίδιων των πληροφοριών και θα διασφαλίζει τις εξής *βασικές αρχές*:

1. **Επιβεβαίωση ταυτότητας (authentication)**, ώστε να αποδεικνύεται η ταυτότητα ενός ατόμου ή μιας εφαρμογής λογισμικού ή ενός μηχανήματος (π.χ. server).
2. **Εμπιστευτικότητα (confidentiality)**, ώστε να εξασφαλίζεται ο ιδιωτικός χαρακτήρας της πληροφορίας.
3. **Ακεραιότητα (integrity)**, ώστε να βεβαιώνεται ότι η πληροφορία δεν έχει αλλοιωθεί κατά τη μετάδοσή της.
4. **Μη αποκήρυξη (non-repudiation)**, ώστε να αποκλειστεί το ενδεχόμενο κάποιος από τους συμμετέχοντες σε μια συναλλαγή να αρνηθεί εκ των υστέρων την εμπλοκή του σ' αυτήν ή τα αποτελέσματά της.

Με βάση τα σημερινά τεχνολογικά δεδομένα, η πλήρης διασφάλιση των πιο πάνω βασικών αρχών είναι δυνατόν να επιτευχθεί μόνο με τη χρήση της **κρυπτογραφίας**, η οποία επιπλέον θα πρέπει να συνδυάζεται με **πολιτικές ασφάλειας**, που να καθορίζουν τους κανόνες με τους οποίους λειτουργεί ένα σύστημα κρυπτογράφησης, **προϊόντα** (software και hardware), τα οποία να επιτρέπουν την δημιουργία, αποθήκευση και διαχείριση των κλειδιών ασφαλείας, που θα χρησιμοποιούνται κατά την κρυπτογράφηση / αποκρυπτογράφηση και, τέλος, **διαδικασίες**, που να περιγράφουν τους τρόπους δημιουργίας, διανομής και χρήσης των κλειδιών ασφαλείας.

Η σύγχρονη προσέγγιση στις παραπάνω απαιτήσεις είναι γνωστή με τον όρο **Συστήματα Υποδομής Δημοσίου Κλειδιού (Public Key Infrastructure Systems – Συστήματα PKI)**, τα οποία ενσωματώνουν ως αναπόσπαστο τμήμα τους και διάφορες τεχνικές κρυπτογραφίας και επιτρέπουν την ασφαλή διεξαγωγή των εμπορικών συναλλαγών μέσω του Internet, επιτυγχάνοντας την τήρηση των τεσσάρων βασικών αρχών που προαναφέρθηκαν.

Πιο συγκεκριμένα και σε σχέση με τις τέσσερις βασικές αρχές, ένα σύστημα PKI λειτουργεί ως εξής:

Επιβεβαίωση ταυτότητας (authentication)

Η επιβεβαίωση ταυτότητας σε ένα ηλεκτρονικό σύστημα είναι απαραίτητη, προκειμένου η πρόσβαση σ' αυτό να επιτρέπεται μόνο σε όσους μπορούν να παράσχουν τα σχετικά διαπιστευτήρια. Στα περισσότερα συστήματα η επιβεβαίωση ταυτότητας διεκπεραιώνεται με τη χρήση ενός κωδικού χρήστη και ενός συνθηματικού (password), τεχνική η οποία παρουσιάζει πλήθος αδυναμιών από πλευράς ασφάλειας. Σε ένα περιβάλλον PKI, για την επιβεβαίωση ταυτότητας χρησιμοποιούνται τα "ψηφιακά πιστοποιητικά" (ή ψηφιακές ταυτότητες). Τα συνηθέστερα σημεία αποθήκευσης ενός ψηφιακού πιστοποιητικού είναι είτε ο μαγνητικός δίσκος του υπολογιστή του χρήστη είτε μια ειδική κάρτα (έξυπνη κάρτα) μικρού μεγέθους, που ο χρήστης έχει πάντα μαζί του. Με ψηφιακά πιστοποιητικά εξάλλου εφοδιάζονται όχι μόνο τα φυσικά πρόσωπα, αλλά και ορισμένα μηχανήματα, π.χ. ο Web server μιας επιχείρησης, ώστε να μπορεί να "αποδείξει" στον εν δυνάμει χρήστη που τον έχει επισκεφθεί μέσω του Internet ότι πράγματι εκπροσωπεί μια συγκεκριμένη εταιρία και έχει κατά συνέπεια το δικαίωμα να προβαίνει σε νόμιμες ηλεκτρονικές συναλλαγές (πωλήσεις κλπ).

Εμπιστευτικότητα (confidentiality)

Βασικό χαρακτηριστικό μιας ασφαλούς συναλλαγής μεταξύ δύο μερών είναι το περιεχόμενό της να παραμείνει μυστικό και απροσπέλαστο για οποιονδήποτε τρίτο. Τα προς προστασία δεδομένα μπορεί να αφορούν επιχειρηματικά σχέδια, οικονομικές συναλλαγές, πνευματική ιδιοκτησία, εμπιστευτικές πληροφορίες σχετικές με το προσωπικό κλπ. Ενα σύστημα PKI χρησιμοποιεί διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης, στηριζόμενες σε κατάλληλα "κλειδιά", προκειμένου να κρατήσει τα ευαίσθητα δεδομένα προστατευμένα από κάθε ανεπιθύμητη πρόσβαση. Ετσι ακόμη και αν τα δεδομένα υποκλαπούν, θα είναι εξαιρετικά δύσκολο έως αδύνατο να αξιοποιηθούν, διότι θα πρέπει προηγουμένως να αποκρυπτογραφηθούν.

Ακεραιότητα δεδομένων (data integrity)

Η αρχή αυτή διασφαλίζει ότι τα δεδομένα που έφθασαν στον παραλήπτη ενός μηνύματος είναι τα ίδια με αυτά που απέστειλε ο απόστολέας και δεν έχουν αλλοιωθεί καθ' οδόν. Η σημασία της ακεραιότητας των δεδομένων μιας ηλεκτρονικής συναλλαγής γίνεται εύκολα αντιληπτή αν σκεφθεί κανείς το παράδειγμα μιας ηλεκτρονικά μεταδιδόμενης οικονομικής προσφοράς για 1000 μονάδες ενός συγκεκριμένου είδους, προς 5 ευρώ ανά μονάδα. Αν η τιμή μονάδας αλλοιωθεί σε 50 ευρώ, τότε αμφισβητείται η ίδια η υπόσταση της προσφοράς. Ενα σύστημα PKI χρησιμοποιεί τους λεγόμενους αλγόριθμους κατατεμαχισμού και την έννοια του "αποτυπώματος" ενός μηνύματος, σε συνδυασμό με ψηφιακές υπογραφές, προκειμένου να επιτρέψει στον παραλήπτη να βεβαιωθεί ότι το μήνυμα δεν έχει αλλοιωθεί ούτε κατ' ελάχιστον σε σχέση με αυτό που πράγματι απέστειλε ο αποστολέας. Ακόμη και στην περίπτωση που δεν υφίσταται κίνδυνος κακόβουλης ενέργειας εκ μέρους τρίτων, η βεβαιότητα για την ακρίβεια και την πληρότητα ενός ηλεκτρονικού μηνύματος είναι σημαντική.

Μη αποκήρυξη (non-repudiation)

Η αρχή της μη αποκήρυξης σημαίνει ότι εάν προκύψει διαφωνία ή αμφισβήτηση σχετικά με τη διεξαγωγή μιας ηλεκτρονικής συναλλαγής, υπάρχουν (στα πλαίσια του συγκεκριμένου ηλεκτρονικού περιβάλλοντος) διαθέσιμα αδιάψευστα αποδεικτικά στοιχεία, τα οποία μπορούν να χρησιμοποιηθούν από ένα τρίτο ουδέτερο μέρος, προκειμένου να διαπιστωθεί τι ακριβώς έχει συμβεί. Πρόκειται ουσιαστικά για το συνδυασμό "επιβεβαίωση ταυτότητας – ακεραιότητα δεδομένων", ο οποίος παρέχει στον παραλήπτη την βεβαιότητα ότι ο αποστολέας δεν θα μπορέσει να αρνηθεί (ψευδώς) ότι έχει δημιουργήσει, υπογράψει και αποστείλει ένα ηλεκτρονικό έγγραφο ή έχει συμμετάσχει σε μια συναλλαγή. Αυτό είναι ιδιαίτερα σημαντικό σε οικονομικές ιδίως συναλλαγές, όπου το ένα από τα δύο μέρη θα μπορούσε πιθανόν να αρνηθεί την πληρωμή π.χ. ενός λογαριασμού για παροχή υπηρεσιών, με τον ισχυρισμό ότι οι σχετικές υπηρεσίες δεν είχαν ποτέ ζητηθεί. Σε ένα περιβάλλον PKI, η μη αποκήρυξη χρησιμοποιεί μεν την έννοια των ψηφιακών υπογραφών, προϋποθέτει όμως και ένα γενικότερο πλαίσιο λειτουργίας που καθορίζεται από συγκεκριμένες πολιτικές και διαδικασίες. Με τα δεδομένα αυτά, ένα τέτοιο ηλεκτρονικό περιβάλλον θα μπορούσε να χρησιμοποιηθεί ακόμη και για την ψηφιακή υπογραφή συμβάσεων. Φυσικά, σημαντικό ρόλο παίζει στην περίπτωση αυτή και το ισχύον κάθε φορά νομικό πλαίσιο, το οποίο θα πρέπει να ληφθεί σοβαρά υπ' όψη.

Γενικότερα, τα συστήματα PKI στηρίζονται σε μια σειρά από κοινά αποδεκτά πρότυπα (standards) και παρέχουν μια κοινή υποδομή ασφάλειας, η οποία μπορεί να αξιοποιηθεί από οποιοδήποτε επιμέρους πληροφοριακό υποσύστημα που υλοποιεί μια συγκεκριμένη επιχειρηματική διαδικασία (π.χ. υποσύστημα παραγγελιών, υποσύστημα αποθεμάτων κλπ). Ετσι η ασφάλεια των πληροφοριών αποτελεί τελικά μέρος της υποδομής της επιχείρησης (όπως η τηλεφωνική υποδομή ή η υποδομή παροχής ηλεκτρικής ενέργειας), με αποτέλεσμα κάθε επιμέρους υποσύστημα να μην "κτίζει" το δικό του περιβάλλον ασφάλειας, αλλά απλώς να χρησιμοποιεί με κατάλληλο τρόπο τις ήδη διαθέσιμες υπηρεσίες ασφάλειας.

1.3. Πίνακας χρησιμοποιουμένων όρων

Ελληνικός όρος	Συντομογραφία	Αγγλικός όρος	Συντομογραφία
Αρχή Καταχώρησης	ΑΚ	Registration Authority	RA
Αρχή Πιστοποίησης	ΑΠ	Certification Authority	CA
Δήλωση Διαδικασιών Πιστοποίησης	ΔΔΠ	Certification Practice Statement	CPS
Δημόσιο Κλειδί		Public Key	
Εμπιστη Τρίτη Οντότητα	ΕΤΟ	Trusted Third Party	TTP
Εξαρτώμενο Μέρος		Relying Party	
Ιδιωτικό Κλειδί		Private Key	
Κάτοχος Πιστοποιητικού		Certificate Subject (Subscriber)	
Πολιτική Πιστοποιητικών	ΠΠ	Certificate Policy	CP
Πιστοποιητικό		Certificate	
Πίνακας Ανάκλησης Πιστοποιητικών	ΠΑΠ	Certificate Revocation List	CRL
Συμμετρικό Κλειδί		Symmetric Key	
Υποδομή Δημοσίου Κλειδιού	ΥΔΚ	Public Key Infrastructure	PKI
Ψηφιακή Υπογραφή		Digital Signature	
Ψηφιακό Πιστοποιητικό		Digital Certificate	

1.4. Σκοπός και δομή της εργασίας

Σκοπός της εργασίας είναι.η διερεύνηση των δυνατοτήτων των ψηφιακών υπογραφών και της τεχνολογίας των συστημάτων PKI προς την κατεύθυνση της δημιουργίας ενός περιβάλλοντος ασφαλούς ηλεκτρονικού εμπορίου. καθώς επίσης και των νομικών προεκτάσεων της εφαρμογής τους.

Η εργασία αναπτύσσεται ως εξής:
Αρχικά, στο κεφάλαιο 2, παρουσιάζονται τα διάφορα κρυπτογραφικά συστήματα με τα πλεονεκτήματα και τις αδυναμίες που παρουσιάζει το καθένα, ενώ εξετάζεται επιπλέον και η δυνατότητα συνδυασμένης χρησιμοποίησής τους, προκειμένου να αξιοποιηθούν τα πλεονεκτήματα του καθενός. Επίσης εισάγεται και η έννοια της ψηφιακής υπογραφής και εξηγείται η λειτουργία της. Στο κεφάλαιο 3 που ακολουθεί, τεκμηριώνεται η ανάγκη για ψηφιακές ταυτότητες και για έμπιστες τρίτες οντότητες (ή Αρχές Πιστοποίησης) που θα είναι υπεύθυνες για την έκδοση και διαχείρισή τους.
Στο κεφάλαιο 4 εξετάζονται τα βασικά χαρακτηριστικά και η αρχιτεκτονική ενός συστήματος PKI, τα κεφάλαια 5 και 6 ασχολούνται με τη διαχείριση των κρυπτογραφικών κλειδιών και των ψηφιακών πιστοποιητικών αντίστοιχα, ενώ το κεφάλαιο 7 καλύπτει το θέμα των ιεραρχιών πιστοποίησης που πιθανόν θα απαιτηθεί να δημιουργηθούν, ιδιαίτερα σε ένα εκτεταμένο σύστημα PKI με πολλούς συμμετέχοντες.
Το κεφάλαιο 8 εξετάζει το θέμα της επιβεβαίωσης ταυτότητας σε ένα ηλεκτρονικό περιβάλλον και διερευνά ειδικότερα τις διαθέσιμες μεθόδους και τη σχέση τους με τα συστήματα PKI.
Οι πολιτικές και οι διαδικασίες που θα πρέπει να διέπουν τη λειτουργία ενός PKI, καθώς και το πώς αυτές δομούνται και διατυπώνονται, είναι το θέμα που καλύπτει το κεφάλαιο 9, όπου επίσης εξετάζονται και τα διάφορα μοντέλα PKI που μπορεί να υιοθετηθούν, ανάλογα με τις εκάστοτε απαιτήσεις. Στη συνέχεια (κεφάλαιο 10) προτείνονται διάφορες εναλλακτικές επιλογές για την υλοποίηση μιας Αρχής Πιστοποίησης, η οποία αποτελεί το κυριότερο συστατικό στοιχείο ενός συστήματος PKI.
Το κεφάλαιο 11 παρουσιάζει τις κυριότερες από τις PKI υπηρεσίες, καθώς και τις εφαρμογές μέσω των οποίων είναι δυνατόν να αξιοποιηθούν οι ως άνω υπηρεσίες, ενώ το κεφάλαιο 12 αποτελεί μια κωδικοποιημένη καταγραφή των βημάτων που απαιτούνται για την υλοποίηση ενός ολοκληρωμένου συστήματος PKI.
Το κεφάλαιο 13 είναι αφιερωμένο στη νομική προσέγγιση των ζητημάτων που σχετίζονται με ψηφιακές υπογραφές και PKI, ενώ ιδιαίτερη έμφαση δίνεται στη σχετική οδηγία της Ευρωπαϊκής Ενωσης.
Τέλος, τα συμπεράσματα της εργασίας και η συζήτησή τους αποτελούν το αντικείμενο του κεφαλαίου 14, με το οποίο και ολοκληρώνεται η εργασία.

2. ΣΥΣΤΗΜΑΤΑ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

Η ασφαλής ανταλλαγή μηνυμάτων θα μπορούσε πιθανόν να στηριχθεί στη διακίνησή τους μέσα από διαύλους, οι οποίοι να είναι ελεγχόμενοι αφ'ενός και δεδομένης ασφάλειας αφ'ετέρου. Στην περίπτωση όμως του Internet κάτι τέτοιο δεν είναι δυνατόν, κατά συνέπεια θα πρέπει η έμφαση να δοθεί όχι στο δίαυλο, αλλά στο ίδιο το μήνυμα. Αυτό πρακτικά σημαίνει ότι αυτό που θα διακινηθεί δεν θα πρέπει να είναι το ίδιο το μήνυμα σε μορφή αναγνώσιμη από οποιονδήποτε, αλλά μια κωδικοποιημένη μορφή του, η οποία να είναι αναγνωρίσιμη μόνο από τα ενδιαφερόμενα μέρη.

Την ανάγκη αυτή έρχονται να καλύψουν τα συστήματα κρυπτογραφίας, τα οποία επιτρέπουν την επικοινωνία ανάμεσα σε δύο μέρη, παρέχοντας ταυτόχρονα τη δυνατότητα του αποκλεισμού της πρόσβασης τρίτων μερών στο περιεχόμενο του μεταφερομένου μηνύματος. Αυτό συνήθως επιτυγχάνεται με τη μετατροπή (κωδικοποίηση / κρυπτογράφηση) του μηνύματος σε μη κατανοητή μορφή, τη μεταφορά του και τελικώς την εκ νέου μετατροπή του (αποκωδικοποίηση / αποκρυπτογράφηση) σε κατανοητή μορφή, ώστε να γίνει αντιληπτό από τον παραλήπτη.

Η μετατροπή του περιεχομένου ενός μηνύματος σε μη αναγνώσιμη μορφή (κρυπτογράφηση), καθώς και η αντίστροφη μετατροπή (αποκρυπτογράφηση) επιτυγχάνεται με τη χρήση πολύπλοκων μαθηματικών διαδικασιών, που είναι γνωστές ως κρυπτογραφικοί αλγόριθμοι. Οι αλγόριθμοι αυτοί χωρίζονται σε δύο μεγάλες κατηγορίες, τους συμμετρικούς και τους ασύμμετρους. Κατ' επέκταση, τα συστήματα κρυπτογραφίας, ανάλογα με το είδος των αλγορίθμων που χρησιμοποιούν, ανήκουν είτε στη **Συμμετρική** είτε στην **Ασύμμετρη Κρυπτογραφία**, χωρίς να αποκλείεται και η συνδυασμένη χρήση και των δύο κατηγοριών.

2.1. Συμμετρική Κρυπτογραφία

Το σύστημα αυτό (γνωστό και ως σύστημα συμμετρικού κλειδιού ή σύστημα μυστικού κλειδιού - secret key cryprography) είναι το πλέον γνωστό και έχει χρησιμοποιηθεί κατά κόρον, από την αρχαιότητα μέχρι και σήμερα.

Χαρακτηρίζεται από την ύπαρξη ενός και μόνο κώδικα ή κλειδιού (key), το οποίο χρησιμοποιείται τόσο για την κρυπτογράφηση του μηνύματος από τον αποστολέα (πριν την αποστολή) όσο και για την αποκρυπτογράφηση του από τον παραλήπτη (μετά τη μεταφορά). Για τον λόγο αυτό άλλωστε ονομάζεται και συμμετρικό. Επίσης είναι γνωστό και με τα ονόματα κρυπτογραφία μυστικού κλειδιού (secret key) ή διαμοιραζομένου μυστικού (shared secret), δεδομένου ότι το κλειδί θα πρέπει να παραμείνει μυστικό, αλλά να είναι γνωστό και στα δύο μέρη που ανταλλάσσουν μηνύματα.

Ενδεικτικά αναφέρεται εδώ το σύστημα κρυπτογράφησης που είχε επινοήσει και χρησιμοποιούσε ο Ιούλιος Καίσαρ. Σύμφωνα με το σύστημα αυτό, κάθε γράμμα του μηνύματος αντικαθίσταται από το αντίστοιχο που βρίσκεται Ν θέσεις παρακάτω στο

αλφάβητο, όπου N είναι το κλειδί που χρησιμοποιείται κάθε φορά. Ετσι για παράδειγμα, η φράση "please ignore" θα κρυπτογραφηθεί ως "rngcug kipqtg" για N=2 και ως "sohdvh ljqruh" για N=3.

Τα κρυπτογραφικά κλειδιά παρουσιάζουν πολλές ομοιότητες με τα φυσικά κλειδιά της καθημερινής ζωής, που χρησιμοποιούνται π.χ. για να κλειδώσουν ή να ξεκλειδώσουν μια πόρτα. Για κάθε τύπο κλειδαριάς, υπάρχει ένα κλειδί ειδικού σχήματος που ταιριάζει σ'αυτήν και το οποίο πρέπει να έχει το σωστό μήκος και τη σωστή μορφολογία. Ενα κλειδί για κλειδαριές συγκεκριμένου κατασκευαστή είναι πολύ πιθανόν να ταιριάζει σε οποιαδήποτε κλειδαριά αντίστοιχου τύπου, αλλά μόνο το σωστό κλειδί, αυτό με το κατάλληλο μήκος και μορφολογία μπορεί να περιστραφεί και να ανοίξει την κλειδαριά.
Κατ' αναλογία, και στα σύγχρονα συστήματα κρυπτογραφίας που λειτουργούν με χρήση υπολογιστών, κάθε κρυπτογραφικός αλγόριθμος χρειάζεται ένα κλειδί με το σωστό μήκος, δηλ. με το σωστό αριθμό bits. Ενας κρυπτογραφικός αλγόριθμος μπορεί να λειτουργήσει με οποιοδήποτε κλειδί έχει το κατάλληλο μήκος, αλλά η εφαρμογή του αλγορίθμου θα έχει ως αποτέλεσμα την αποκρυπτογράφηση ενός κρυπτογραφημένου μηνύματος μόνο με το κλειδί που διαθέτει τη σωστή ακολουθία bits.

Οι συμμετρικοί αλγόριθμοι κρυπτογράφησης δέχονται σαν είσοδο κανονικό αναγνώσιμο κείμενο (clear text - plain text) και με τη χρήση του συμμετρικού κλειδιού παράγουν σαν αποτέλεσμα (εξαγόμενο) μια κρυπτογραφημένη μορφή του αρχικού κειμένου. Το συμμετρικό κλειδί δεν είναι παρά ένας τυχαίος αριθμός με το σωστό μέγεθος. Ετσι, αν ο αλγόριθμος είναι συμμετρική κρυπτογράφηση των 40 bits, το συμμετρικό κλειδί θα είναι μήκους 40 bits, ενώ αν πρόκειται για αλγόριθμο συμμετρικής κρυπτογράφησης των 128 bits, τότε το συμμετρικό κλειδί θα είναι μήκους 128 bits.

Είναι ζωτικής σημασίας το συμμετρικό κλειδί να δημιουργείται με τη χρήση μιας καλής γεννήτριας τυχαίων αριθμών. Αυτό σημαίνει ότι η γεννήτρια θα πρέπει να επιλέγει αριθμούς ομοιόμορφα κατανεμημένους σε όλο το πεδίο τιμών που επιτρέπει το μήκος του κλειδιού και να μην "προτιμά" (ή "αποφεύγει") κάποιες τιμές, οπότε εξασθενεί η ισχύς της κρυπτογράφησης.

Η κρυπτογραφία γενικά περιλαμβάνει δύο επιμέρους κλάδους, την *κρυπτολογία* και την *κρυπτανάλυση*. Η κρυπτολογία ασχολείται με την επινόηση νέων και διαρκώς ισχυρότερων κρυπτογραφικών αλγορίθμων, ενώ η κρυπτανάλυση έχει σαν αντικείμενο την εξέταση των κρυπτογραφικών αλγορίθμων με χρήση ειδικών εργαλείων και τεχνικών, με σκοπό να εντοπίσει πιθανά αδύνατα σημεία τους, που θα τους καθιστούσαν ευάλωτους σε επιθέσεις. Κατά συνέπεια, κάθε κρυπτογραφικός αλγόριθμος που επινοείται από τους ειδικούς της κρυπτολογίας, θα πρέπει να τίθεται στη διάθεση των κρυπταναλυτών, προκειμένου να διασφαλιστεί ότι δεν έχει (λόγω σχεδιασμού ή εφ'όσον χρησιμοποιηθεί με κάποιο ειδικό τρόπο) κενά ή τρόπους παραβίασης. Αν ο πιο πάνω διεξοδικός έλεγχος δεν πραγματοποιηθεί (πιθανόν για λόγους μη δημοσιοποίησης της χρησιμοποιούμενης τεχνικής), υπάρχει πάντα το ενδεχόμενο τα πιθανά αδύνατα σημεία του να εντοπισθούν από τρίτους, αφού έχει τεθεί σε χρήση, οπότε τα αποτελέσματα για όσους στηρίζονται σ'αυτόν να είναι μέχρι και καταστροφικά.

Επομένως ένας κρυπτογραφικός αλγόριθμος χαρακτηρίζεται ως ασφαλής, εφ'όσον έχει προηγηθεί ο εξαντλητικός έλεγχός του από τους κρυπταναλυτές, χωρίς να εντοπισθούν αδυναμίες. Υπ' αυτές τις προϋποθέσεις, ο μόνος τρόπος να παραβιαστεί ένα κρυπτογραφημένο μήνυμα, είναι να δοκιμαστούν όλες οι πιθανές τιμές κλειδιών που αντιστοιχούν στο συγκεκριμένο μέγεθος. Αυτό αποκαλείται επίθεση ωμής βίας (brute force attack). Στατιστικά θα χρειαστεί να δοκιμαστούν μόνο οι μισές από τις πιθανές τιμές του κλειδιού, προκειμένου να εντοπισθεί το σωστό κλειδί. Τα μεγέθη των κλειδιών επιλέγονται έτσι ώστε να είναι πρακτικά αδύνατο να δοκιμαστούν έστω και οι μισές πιθανές τιμές του κλειδιού, ακόμη και με χρήση τεράστιου αριθμού υπολογιστών, μέσα στο χρονικό διάστημα κατά το οποίο τα υπό προστασία δεδομένα πρέπει να παραμείνουν ασφαλή. Είναι φυσικά αδύνατο να προβλεφθεί με ακρίβεια η εξέλιξη της τεχνολογίας των υπολογιστών οπότε είναι απαραίτητο να γίνουν κάποιες υποθέσεις σχετικά με την πιθανή αύξηση της επεξεργαστικής τους ισχύος.

Για παράδειγμα, ένα κλειδί με μήκος 2 bits μπορεί να έχει 2^2 = 4 πιθανές τιμές, ενώ σε μήκος κλειδιού 40 bits αντιστοιχούν 2^40 = 1.1E12 τιμές (περισσότερα από 1.000.000.000.000 - 1 τρις πιθανά κλειδιά). Τέλος, για κλειδί μήκους 128 bits, που είναι το standard μέγεθος για τα συμμετρικά κλειδιά σήμερα, υπάρχουν περίπου 3.4E38 πιθανές τιμές.

Υπάρχουν δύο κατηγορίες συμμετρικών αλγορίθμων κρυπτογράφησης:

Α. Οι αλγόριθμοι, οι οποίοι χωρίζουν τα προς κρυπτογράφηση δεδομένα σε πακέτα των 64 bits και είναι γνωστοί ως "block ciphers". Οι πιο γνωστός από αυτούς είναι ο DES (Data Encryption Standard), ο οποίος έχει σταθερό μέγεθος κλειδιού 56 bits και αναπτύχθηκε αρχικά από την IBM στη δεκαετία του 1970, ενώ στη συνέχεια υιοθετήθηκε και από την κυβέρνηση των ΗΠΑ ως το επίσημο πρότυπο κρυπτογράφησης απορρήτων πληροφοριών. Ο DES υπήρξε εν χρήσει για μεγάλο διάστημα και χρησιμοποιήθηκε σε πολλά κρυπτογραφικά συστήματα, όπως το σύστημα Kerberos, το οποίο αναπτύχθηκε στο MIT. Λόγω όμως της αυξανόμενης ισχύος των υπολογιστών, το μήκους 56 bits κλειδί του αρχίζει να γίνεται ευάλωτο σε επιθέσεις τύπου "ωμής βίας". Οι προσπάθειες για βελτίωση του DES οδήγησαν στη δημιουργία του 3-DES (triple DES), όπου τα δεδομένα κρυπτογραφούνται τρεις φορές.
Πολύ γνωστός επίσης είναι ο αλγόριθμος RC2 (αναπτύχθηκε από τον Ron Rivest), ο οποίος μπορεί να αντικαταστήσει τον DES, ενώ είναι δύο έως τρεις φορές πιο γρήγορος.
Ο RC5 είναι ένας ακόμη συμμετρικός αλγόριθμος με δημιουργό τον Ron Rivest και ο οποίος χωρίζει τα δεδομένα σε πακέτα των 64 ή των 128 bits, ενώ υποστηρίζει κλειδιά μεταβλητού μήκους μέχρι και 2048 bits. Το πλεονέκτημα στην περίπτωση αυτή είναι ότι όσο μεγαλύτερο μήκος κλειδιού επιλεγεί, τόσο πιο ισχυρή είναι η κρυπτογράφηση, αν και απαιτείται προφανώς μεγαλύτερη υπολογιστική ισχύς για να εκτελεστεί η κρυπτογράφηση. Ετσι παρέχεται η δυνατότητα επιλογής, ανάλογα με τις εκάστοτε απαιτήσεις.

Β. Οι αλγόριθμοι που δεν εφαρμόζονται σε πακέτα δεδομένων συγκεκριμένου μεγέθους (64 ή128 bits), αλλά σε ακολουθίες bits (stream ciphers).

Ο πιο γνωστός από αυτούς είναι ο RC4, με κυριότερα χαρακτηριστικά του την ταχύτητα (είναι ταχύτερος από όλους της προηγούμενης κατηγορίας) και την υποστήριξη κλειδιών μεταβλητού μήκους.

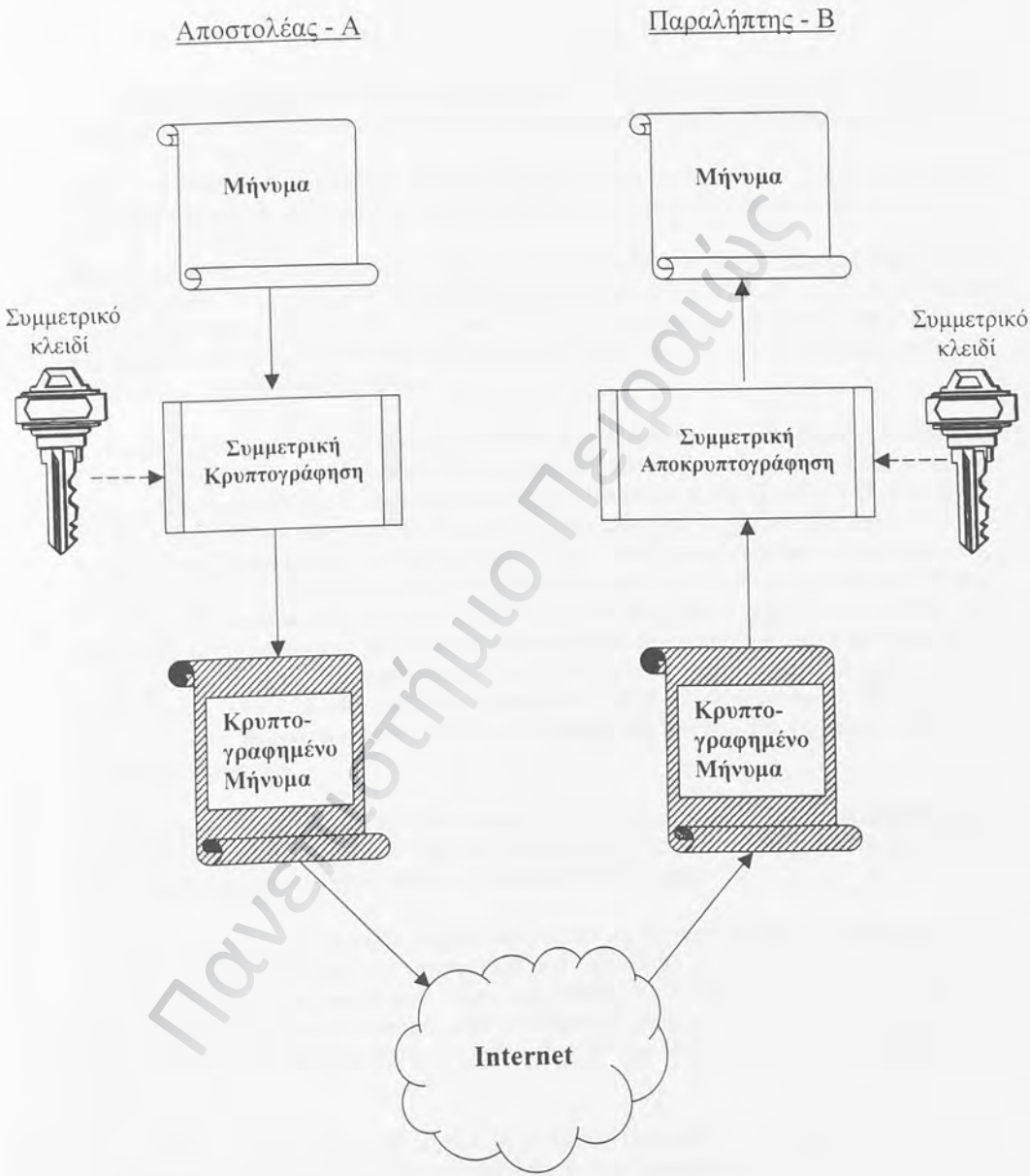
Τέλος, κοινές σε όλους τους συμμετρικούς αλγόριθμους είναι οι εξής δύο ιδιότητες:

- Είναι γενικά γρήγοροι στην εκτέλεσή τους
- Είναι συμπαγείς (compact), με την έννοια ότι το παραγόμενο κρυπτογραφημένο μήνυμα έχει γενικά το ίδιο μέγεθος με το αρχικό μήνυμα.

Με βάση τα παραπάνω, εάν δύο πρόσωπα Α και Β θέλουν να επικοινωνήσουν (έστω ότι ο Α επιθυμεί να στείλει ένα μυστικό μήνυμα στον Β), θα πρέπει να κινηθούν ως εξής:

- Επιλέγεται ένας συμμετρικός αλγόριθμος
- Επιλέγεται το συμμετρικό κλειδί
- Το κλειδί πρέπει να γίνει γνωστό και στους δύο: εάν το έχει επιλέξει ο Α, θα πρέπει να το αποστείλει εκ των προτέρων στον Β.
- Ο Α κρυπτογραφεί το μήνυμα με τη χρήση του κλειδιού
- Ο Α αποστέλλει το κρυπτογραφημένο μήνυμα στον Β
- Ο Β αποκρυπτογραφεί το μήνυμα

Σχηματική αναπαράσταση της διαδικασίας της συμμετρικής κρυπτογράφησης και αποκρυπτογράφησης φαίνεται στο Σχήμα 1. που ακολουθεί.



Σχήμα 1. Συμμετρική κρυπτογράφηση και αποκρυπτογράφηση

Η συμμετρική κρυπτογραφία χαρακτηρίζεται από την απλότητά της, δεδομένου ότι απαιτεί την ύπαρξη ενός μόνο κλειδιού. Παρουσιάζει όμως ορισμένα σημαντικά προβλήματα.

Πρέπει να υπάρχει ένας ασφαλής δίαυλος για την αρχική μεταφορά του μυστικού κλειδιού. Αν το μυστικό κλειδί υποκλαπεί, τότε όλες οι επόμενες επικοινωνίες θα είναι επισφαλείς.

Βασική προϋπόθεση επιτυχούς λειτουργίας είναι η ύπαρξη αμοιβαίας εμπιστοσύνης μεταξύ των δύο μερών. Σε σχέση με το παράδειγμα που προαναφέρθηκε (βλ. Σχήμα 1), αν ο Β είναι "διπλός πράκτορας", είναι πιθανόν να αποκαλύψει το μυστικό κλειδί του Α στους εχθρούς του ή να διαβάσει κρυπτογραφημένα μηνύματα του Α που δεν απευθύνονται σ' αυτόν ή ακόμη και να προσποιηθεί ότι είναι ο Α.

Το πρόβλημα θα μπορούσε να επιλυθεί μερικώς, αν ο Α χρησιμοποιήσει διαφορετικό μυστικό κλειδί για κάθε ένα από τα πρόσωπα με τα οποία επικοινωνεί. Ετσι, αν ο Α επικοινωνεί με τρία άλλα πρόσωπα (τα Β, Γ, Δ), θα πρέπει να έχει τρία διαφορετικά κλειδιά (Α-Β, Α-Γ, Α-Δ). Το ίδιο φυσικά ισχύει και για τον καθένα από τους άλλους τρεις (π.χ. Β-Α, Β-Γ, Β-Δ). Δηλαδή η χρήση της συμμετρικής κρυπτογραφίας μεταξύ τεσσάρων προσώπων συνεπάγεται την ύπαρξη 4 x (4 -1) = 12 κλειδιών, ενώ αν τα μέρη που ανταλλάσσουν μηνύματα είναι 100, τότε το πλήθος των κλειδιών φθάνει στα 100 x (100 - 1) = 9.900. Παρατηρούμε ότι το πλήθος των απαιτουμένων κλειδιών είναι περίπου ανάλογο του τετραγώνου των συμμετεχόντων μερών. Σ' αυτό προστίθενται και τα προβλήματα διαχείρισης των κλειδιών, ενώ η χρήση τυχόν μικρότερου πλήθους κλειδιών θα δημιουργούσε εξ αρχής συνθήκες μειωμένης ασφάλειας. Κατά συνέπεια υπάρχει σοβαρό πρόβλημα επέκτασης του συστήματος για την εξυπηρέτηση μεγάλων πληθυσμών.

Τα πράγματα γίνονται ακόμη πιο δύσκολα, αν ληφθεί υπ'όψη η αρχή της μη χρησιμοποίησης του ίδιου κλειδιού για παραπάνω από μια επικοινωνίες, έστω και αν αυτές γίνονται με το ίδιο πρόσωπο, δεδομένου ότι τότε αυξάνουν οι κίνδυνοι υποκλοπής του.

Τέλος, σε σχέση με τις βασικές αρχές ασφάλειας που προαναφέρθηκαν στην εισαγωγή, η συμμετρική κρυπτογραφία δεν διασφαλίζει την επιβεβαίωση ταυτότητας (authentication), αλλά ούτε και την μη αποκήρυξη (non-repudiation). Κάθε ένα από τα δύο μέρη έχει τη δυνατότητα να τροποποιήσει κακοβούλως τα δεδομένα (ενός μηνύματος ή μιας συναλλαγής), έχοντας συγχρόνως τη βεβαιότητα ότι ένας τρίτος δεν θα είναι σε θέση να προσδιορίσει τον ένοχο.

Απάντηση σε πολλά από τα προβλήματα αυτά έρχονται να δώσουν τα συστήματα ασύμμετρης κρυπτογραφίας, τα οποία περιγράφονται στη συνέχεια.

2.2. Ασύμμετρη Κρυπτογραφία

Σε αντίθεση με την κρυπτογραφία μυστικού κλειδιού, η ασύμμετρη κρυπτογραφία ή κρυπτογραφία δημοσίου κλειδιού (Public key cryptography), όπως είναι πιο γνωστή, είναι σχετικά πιο πρόσφατη. Οι αλγόριθμοι και τα συστήματα της κατηγορίας αυτής, σχεδιάστηκαν με κύριο σκοπό να δώσουν μια λύση στο πρόβλημα της ασφαλούς διανομής κλειδιού, που παρουσίαζε η συμμετρική κρυπτογραφία. Χαρακτηριστικό τους είναι η ύπαρξη ζεύγους κλειδιών, τα οποία έχουν την ιδιότητα ότι είναι πρακτικά αδύνατος ο υπολογισμός του ενός κλειδιού γνωρίζοντας το άλλο. Ο πρώτος αλγόριθμος ασύμμετρης κρυπτογραφίας αναπτύχθηκε από τους Diffie-Hellman στα μέσα της δεκαετίας του 1970 και στηριζόταν σε μαθηματικά διακριτών λογαρίθμων.

Ο πιο διαδεδομένος αλγόριθμος ασύμμετρης κρυπτογραφίας δημιουργήθηκε το 1977 από τους Rivest, Shamir και Adleman, καθηγητές του MIT, οι οποίοι βασίστηκαν σε αρχές της θεωρίας των πεπερασμένων πεδίων. Ο αλγόριθμος είναι γνωστός με το όνομα RSA (από τα αρχικά των δημιουργών του) και έχει τύχει ευρείας υλοποίησης, ενώ ταυτόχρονα έχει αποδειχθεί εξαιρετικά ασφαλής, έχοντας αντισταθεί με επιτυχία σε πολλές επιθέσεις. Σήμερα χρησιμοποιεί κλειδιά μήκους τουλάχιστον 1024 bits και είναι πιθανόν ο πιο πολύπλοκος και απαιτητικός σε υπολογιστική ισχύ από όλους τους εν χρήσει κρυπτογραφικούς αλγορίθμους. Επίσης πολύ γνωστός είναι ο αλγόριθμος ελλειπτικών καμπυλών (Elliptic curve cryptography - ECC), ο οποίος είναι σχετικά πιο πρόσφατος. Είναι λιγότερο πολύπλοκος και απαιτητικός σε σχέση με τον RSA και μπορεί να χρησιμοποιήσει μικρότερου μήκους κλειδιά, επιτυγχάνοντας το ίδιο επίπεδο ασφάλειας με τον RSA.

Για να γίνει πιο κατανοητή η σημασία του μήκους των κρυπτογραφικών κλειδιών σε σχέση με το επιδιωκόμενο επίπεδο ασφάλειας, παρατίθεται ο πιο κάτω πίνακας, στον οποίο απεικονίζονται συγκριτικά τα μήκη κλειδιών (σε bits) των διαφόρων αλγορίθμων, σε συνδυασμό με τον χρόνο που απαιτείται προκειμένου να επιτευχθεί η παραβίαση ("σπάσιμο") του κλειδιού. Η υπόθεση που έχει γίνει είναι ότι υπάρχει διαθέσιμο ποσό 10 εκατ. δολλαρίων για αγορά εξοπλισμού (υπολογιστών) και ότι η μνήμη κοστίζει περίπου 0.5 δολ. ανά MB.

Συμμετρικό κλειδί DES	Ασύμμετρο κλειδί ECC	Ασύμμετρο κλειδί RSA	Απαιτούμενος χρόνος	Πλήθος Μηχανών	Μνήμη
56	112	420	5 λεπτά	10.000	Ελάχιστη
80	160	760	600 μήνες	4.300	4 GB
96	192	1020	3 εκατ.έτη	114	170 GB
128	256	1620	10E16 έτη	0.16	120 TB

Από τον πίνακα αυτό μπορεί να γίνει αντιληπτό γιατί αρχίζει να εγκαταλείπεται ο αλγόριθμος DES με υποχρεωτικό σταθερό μήκος κλειδιού 56 bits, καθώς και γιατί τα προτιμητέα μήκη κλειδιών στον αλγόριθμο RSA είναι πλέον 1024 και άνω.

Εδώ θα άξιζε να αναφερθεί ότι όλοι οι κατασκευαστές λογισμικού ασύμμετρης κρυπτογράφησης υποστηρίζουν πολλαπλούς αλγορίθμους. Έτσι αν κάποια στιγμή βρεθεί ένα αδύνατο σημείο σε κάποιο αλγόριθμο, το οποίο να επιτρέπει την παραβίασή του, υπάρχει πάντα η επιλογή της ενεργοποίησης ενός άλλου εναλλακτικού αλγορίθμου, ο οποίος να είναι ασφαλής.

2.2.1. Δημόσια (public) και ιδιωτικά (private) κλειδιά

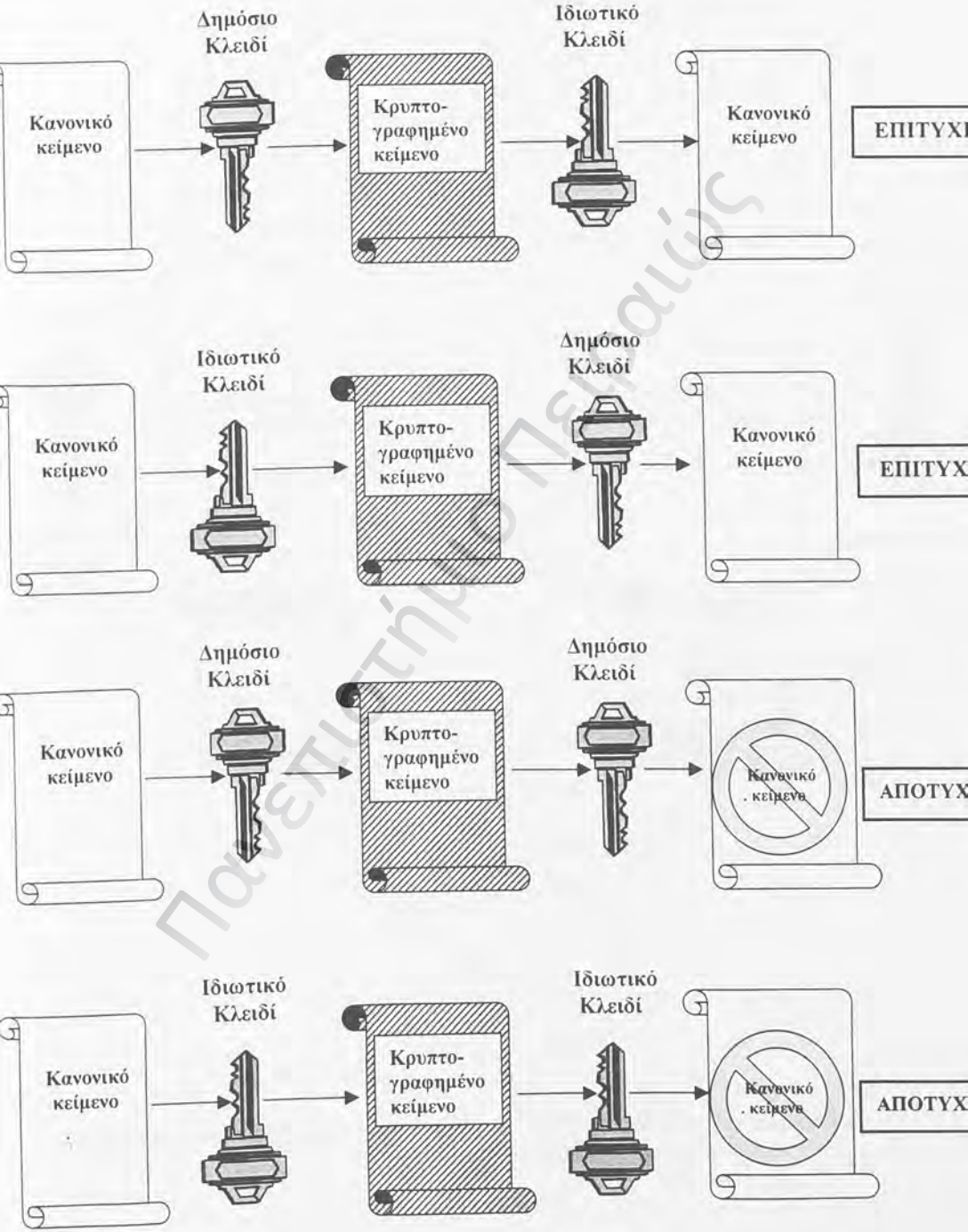
Οι ασύμμετροι αλγόριθμοι διαφέρουν από τους συμμετρικούς κατά ένα πολύ σημαντικό τρόπο. Όταν δημιουργείται ένα συμμετρικό κλειδί, το μόνο που χρειάζεται είναι να επιλεγεί ένας τυχαίος αριθμός με κατάλληλο μήκος (bits). Αντίθετα, η δημιουργία ασύμμετρων κλειδιών είναι πιο πολύπλοκη διαδικασία. Οι ασύμμετροι αλγόριθμοι ονομάζονται έτσι επειδή ακριβώς, αντί για τη χρήση ενός και μόνο κλειδιού για την εκτέλεση και της κρυπτογράφησης και της αποκρυπτογράφησης, χρησιμοποιούνται δύο διαφορετικά κλειδιά: το ένα για την κρυπτογράφηση και το άλλο για την αποκρυπτογράφηση. Αυτά τα δύο διαφορετικά, αλλά μαθηματικώς συσχετιζόμενα κλειδιά δημιουργούνται πάντοτε μαζί και είναι γνωστά ως ζεύγος δημόσιου/ιδιωτικού κλειδιού (public / private key-pair). Η διαδικασία είναι αρκετά διαφορετική και πιο περίπλοκη από την απλή επιλογή ενός τυχαίου αριθμού, αλλά εμπεριέχει πάντα την έννοια της τυχαιότητας. Όταν ολοκληρωθεί η δημιουργία ενός ασύμμετρου κλειδιού, υπάρχουν δύο κλειδιά: ένα δημόσιο (public key) και ένα ιδιωτικό (private key).

Το ιδιωτικό πρέπει να παραμένει κρυφό, φυλασσόμενο με ασφάλεια. Σε κάποιες μάλιστα περιπτώσεις, ούτε ο κάτοχος του κλειδιού δεν έχει τη δυνατότητα να μάθει ποιό ακριβώς είναι το ιδιωτικό του κλειδί. Αντίθετα, το δημόσιο κλειδί είναι επιθυμητό να γίνει ευρέως γνωστό, ώστε να είναι διαθέσιμο σε κάθε ενδιαφερόμενο. Δεδομένου ότι είναι πρακτικά αδύνατος ο υπολογισμός του ιδιωτικού κλειδιού, όταν είναι γνωστό το αντίστοιχο δημόσιο, η δημοσιοποίηση αυτή δεν δημιουργεί κινδύνους, ούτε θέτει σε αμφισβήτηση την ασφάλεια του συστήματος.

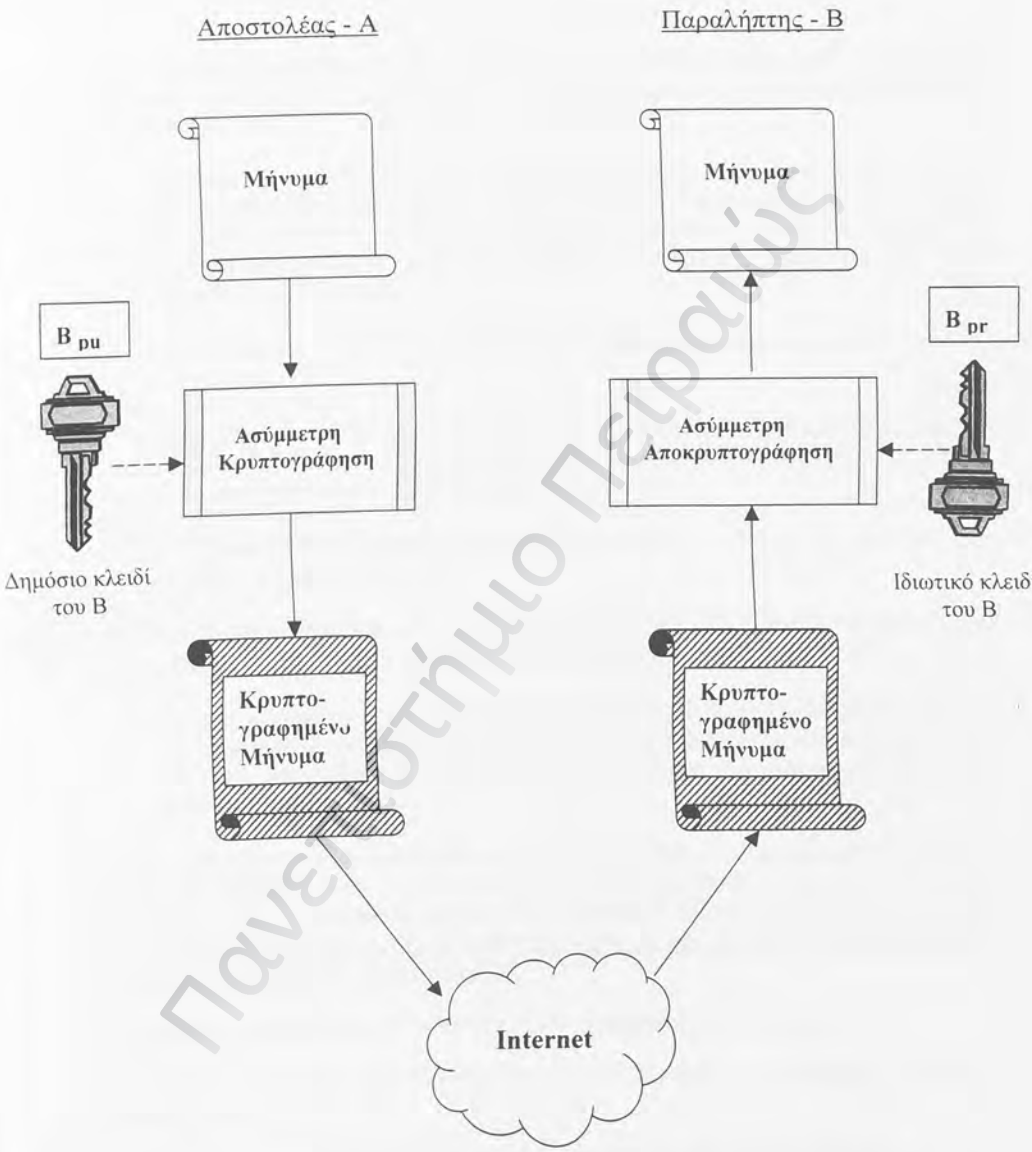
Τα ασύμμετρα κλειδιά έχουν την χαρακτηριστική ιδιότητα πως ό,τι κρυπτογραφείται με το ένα κλειδί μπορεί να αποκρυπτογραφηθεί με το άλλο, ενώ το ίδιο κλειδί (π.χ. το ιδιωτικό) δεν μπορεί να αποκρυπτογραφήσει ό,τι το ίδιο κρυπτογράφησε. Η ιδιότητα αυτή παρουσιάζεται παραστατικά στο Σχήμα 2.

Επιπλέον πρέπει να είναι σαφές πως ό,τι κρυπτογραφήθηκε με το ένα μέλος του ζεύγους μπορεί να αποκρυπτογραφηθεί **μόνο** με το άλλο μέλος του ίδιου ζεύγους, ενώ οποιοδήποτε τρίτο κλειδί δοκιμαστεί, είναι βέβαιο ότι θα αποτύχει.

Η λειτουργία του ασύμμετρου κλειδιού αποδίδεται διαγραμματικά στο Σχήμα 3, που ακολουθεί.



Σχήμα 2. Δημόσια και ιδιωτικά κλειδιά και σχετικές λειτουργίες



Σχήμα 3. Ασύμμετρη κρυπτογραφία - Κρυπτογράφηση και αποκρυπτογράφηση με χρήση δημόσιου και ιδιωτικού κλειδιού

Πιο συγκεκριμένα, υποθέτουμε ότι εξετάζουμε την επικοινωνία μεταξύ δύο εμπλεκομένων προσώπων, του Α και του Β, από τα οποία ο Α είναι ο αποστολέας ενός μηνύματος και ο Β ο παραλήπτης.

- Εφ'όσον γίνεται χρήση ασύμμετρης κρυπτογραφίας, κάθε ένας από τους δύο εμπλεκόμενους διαθέτει ήδη το δικό του ζεύγος δημόσιου / ιδιωτικού κλειδιού (Apu/Apr για τον Α, Bpu/Bpr για τον Β). Η δημιουργία του ζεύγους κλειδιών στα σύγχρονα συστήματα κρυπτογραφημένης επικοινωνίας γίνεται με τη χρήση κατάλληλου λογισμικού.

- Ο Α (όπως και ο Β) φυλάσσει (και δεν αποκαλύπτει σε κανέναν) το ιδιωτικό (private) κλειδί του.

- Ο Α (όπως και ο Β) δημοσιοποιεί (κοινοποιεί στους ενδιαφερόμενους) το δημόσιο (public) κλειδί του. Αυτό μπορεί να γίνει είτε με απ'ευθείας αποστολή του Apu στον Β είτε μέσω κάποιου συστήματος δημόσιου καταλόγου.

- Ο Α αποκτά ένα αντίγραφο του δημόσιου κλειδιού του Β (Bpu) με έναν από τους τρόπους που προαναφέρθηκαν.

- Ο Α κρυπτογραφεί το προς αποστολή μήνυμα, χρησιμοποιώντας το δημόσιο κλειδί του Β και στη συνέχεια αποστέλλει το κρυπτογραφημένο μήνυμα στον Β.

- Ο Β παραλαμβάνει το μήνυμα και χρησιμοποιώντας το δικό του ιδιωτικό κλειδί (Bpr) το αποκρυπτογραφεί. Σημειώνεται ότι, όπως προαναφέρθηκε, το ιδιωτικό κλειδί του Β είναι το μοναδικό κλειδί παγκοσμίως το οποίο μπορεί να εκτελέσει επιτυχώς αυτήν την αποκρυπτογράφηση.

Αν το ζητούμενο ήταν η αποστολή από τον Β ενός μηνύματος με παραλήπτη τον Α, η παραπάνω διαδικασία θα ακολουθείτο σε αντίστροφη κατεύθυνση, χωρίς ιδιαίτερες διαφοροποιήσεις. Προκύπτει βέβαια από όλα τα παραπάνω ότι για την πλήρη και αμφίδρομη επικοινωνία μεταξύ δύο μερών **απαιτείται η ύπαρξη και χρήση τεσσάρων συνολικά κλειδιών**, δύο δημοσίων και δύο ιδιωτικών.

2.2.2. Πλεονεκτήματα / Μειονεκτήματα της ασύμμετρης κρυπτογραφίας

Σε σχέση με τη συμμετρική κρυπτογραφία, η ασύμμετρη παρουσιάζει μια σειρά πλεονεκτημάτων:

Δεν απαιτείται η ύπαρξη ασφαλούς διαύλου για την αρχική μετάδοση του δημόσιου κλειδιού. Αν κάποιος (π.χ. το πρόσωπο Β παραπάνω) βρει ή υποκλέψει το δημόσιο κλειδί ενός προσώπου Α, μπορεί μεν να το χρησιμοποιήσει για να στείλει στον Α ένα ιδιωτικό μήνυμα, όχι όμως για να προσποιηθεί προς τρίτους ότι είναι ο Α ούτε για να αποκρυπτογραφήσει μηνύματα τρίτων που έχουν σταλεί στον Α κρυπτογραφημένα με το δημόσιο κλειδί του Α.

Βεβαίως, εκτός από πλεονεκτήματα, η ασύμμετρη κρυπτογραφία παρουσιάζει και ορισμένα μειονεκτήματα.
Κατ' αρχήν, επειδή οι ασύμμετροι αλγόριθμοι έχουν πολύ μεγαλύτερες απαιτήσεις σε μαθηματικούς υπολογισμούς από ότι οι συμμετρικοί, με αποτέλεσμα να είναι συγκριτικά πιο αργοί και μάλιστα 10 έως 100 φορές πιο αργοί σε σχέση με αντίστοιχης κρυπτογραφικής ισχύος συμμετρικούς. Παρά το γεγονός ότι οι όποιες απαιτούμενες διαδικασίες υπολογισμών διεκπεραιώνονται σήμερα με τη βοήθεια ηλεκτρονικών υπολογιστών και τη χρήση κατάλληλων προγραμμάτων λογισμικού, η παραπάνω διαφορά αποκτά ιδιαίτερη σημασία, ιδίως αν τα προς κρυπτογράφηση (και αποκρυπτογράφηση) δεδομένα δεν είναι τα περιεχόμενα ενός μηνύματος λίγων γραμμών, αλλά πληροφορίες για ένα πολύ μεγάλο έργο, όπως π.χ. κάποιο έργο γενετικής μηχανικής.

Επιπλέον, με τη χρήση ασύμμετρων αλγορίθμων το μέγεθος του κρυπτογραφημένου μηνύματος είναι μεγαλύτερο από το αντίστοιχο αρχικό. Αυτό μπορεί να αποτελέσει ένα σοβαρό ζήτημα όταν χρησιμοποιούνται πολλαπλά επίπεδα κρυπτογράφησης. Π.χ. μια εφαρμογή λογισμικού κρυπτογραφεί δεδομένα (και επομένως διογκώνει το μέγεθός τους), τα οποία στη συνέχεια αποστέλλονται μέσω μιας ασφαλούς σύνδεσης Web (secure Web session), οπότε και πάλι θα διογκωθεί το μέγεθός τους. Εξάλλου είναι πιθανόν η αποστολή να γίνει μέσα από ένα κρυπτογραφημένο δίαυλο (IPSec tunnel), με αποτέλεσμα την παραπέρα διόγκωση του μεγέθους των δεδομένων.

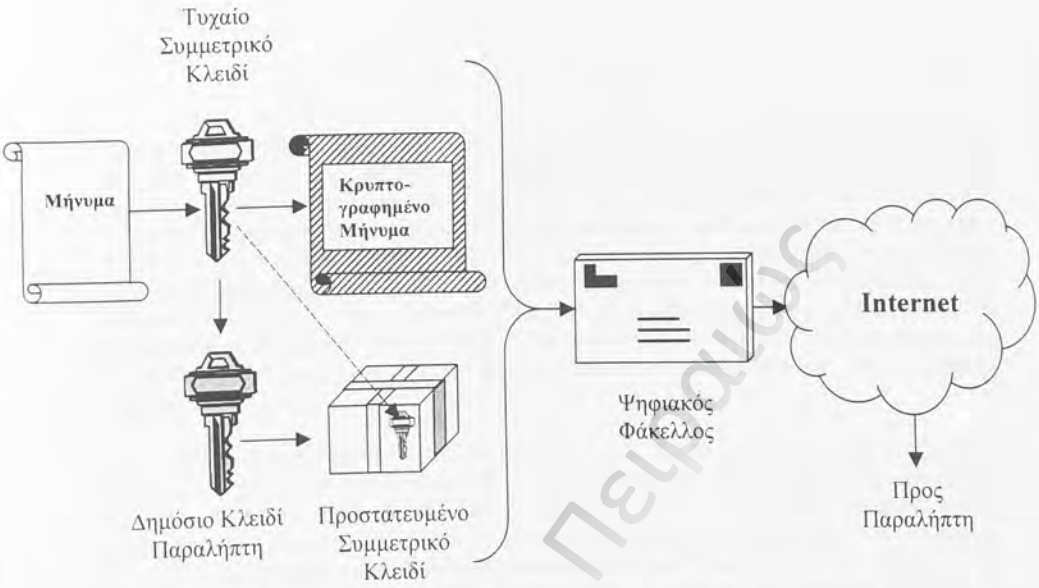
2.3. Συνδυασμένη χρήση συμμετρικής και ασύμμετρης κρυπτογραφίας

Είναι εμφανές από τα παραπάνω ότι κάθε ένα από τα δύο συστήματα κρυπτογραφίας παρουσιάζει πλεονεκτήματα και μειονεκτήματα. Μάλιστα είναι χαρακτηριστικό ότι υπάρχει μια συμπληρωματικότητα, με την έννοια ότι όπου υπερτερεί το ένα υστερεί το άλλο. Επομένως θα ήταν δυνατό να γίνει ένας συνδυασμός των δύο που να εκμεταλλεύεται τα πλεονεκτήματα του καθενός, χωρίς να κληρονομεί τα αντίστοιχα μειονεκτήματα. Ενας τέτοιος συνδυασμός θα πρέπει να συγκεντρώνει τις εξής ιδιότητες:

- Η προσφερόμενη λύση να είναι ασφαλής
- Η κρυπτογράφηση να είναι ταχεία
- Το κρυπτογραφημένο κείμενο να είναι συμπαγές
- Η λύση να μπορεί να επεκταθεί για την εξυπηρέτηση μεγάλων πληθυσμών
- Η λύση να μην είναι ευάλωτη ως προς την υποκλοπή του κλειδιού
- Η λύση να μην απαιτεί προϋπάρχουσα σχέση μεταξύ των δύο μερών
- Η λύση να μπορεί να υποστηρίξει ψηφιακές υπογραφές και μη-αποκήρυξη

Η συνδυασμένη αυτή χρήση συμμετρικής και ασύμμετρης κρυπτογραφίας περιγράφεται στο παράδειγμα που ακολουθεί (Σχήματα 4. και 5.)

Ο αποστολέας (έστω Α) δημιουργεί ένα τυχαίο συμμετρικό κλειδί, το οποίο και χρησιμοποιείται για την κρυπτογράφηση του μηνύματος. Το ζήτημα είναι πώς θα μεταφερθεί το κλειδί αυτό στον παραλήπτη (έστω Β).



Σχήμα 4. Συνδυασμός συμμετρικής και ασύμμετρης κρυπτογραφίας – Κρυπτογράφηση και αποστολή

Σχήμα 5. Συνδυασμός συμμετρικής και ασύμμετρης κρυπτογραφίας – Παραλαβή και αποκρυπτογράφηση

Αυτό επιτυγχάνεται με αξιοποίηση της ασύμμετρης κρυπτογραφίας και με εντοπισμό του δημόσιου κλειδιού του παραλήπτη με τη βοήθεια κάποιου καταλόγου δημοσίων κλειδιών. Το δημόσιο κλειδί του παραλήπτη χρησιμοποιείται για την κρυπτογράφηση του συμμετρικού κλειδιού. Βεβαίως η ασύμμετρη κρυπτογραφία είναι αργή, αλλά δεδομένου ότι το συμμετρικό κλειδί είναι πολύ μικρού μεγέθους (128 bits), αυτό δεν αποτελεί πρόβλημα. Το αποτέλεσμα είναι ένα τυχαίο συμμετρικό κλειδί κρυπτογραφημένο (προστατευμένο) με τη βοήθεια ενός ασύμμετρου κλειδιού. Το τελευταίο βήμα είναι η επισύναψη του προστατευμένου συμμετρικού κλειδιού στο κρυπτογραφημένο μήνυμα, έτσι ώστε τα δύο μαζί να αποτελούν ένα "αντικείμενο" προς αποστολή και το οποίο είναι γνωστό ως ψηφιακός φάκελος (digital envelope).

Στη συνέχεια ο ψηφιακός φάκελος αποστέλλεται στον παραλήπτη μέσω του Internet. Το πρώτο βήμα μετά την παραλαβή είναι ο διαχωρισμός του περιεχομένου του ψηφιακού φακέλου και η ανάκτηση αφ'ενός του κρυπτογραφημένου μηνύματος και αφ'ετέρου του προστατευμένου συμμετρικού κλειδιού. Ο παραλήπτης χρησιμοποιεί το δικό του ιδιωτικό κλειδί για την ανάκτηση / αποκρυπτογράφηση του συμμετρικού κλειδιού. Τέλος, με τη χρήση του συμμετρικού κλειδιού αποκρυπτογραφεί το κείμενο του μηνύματος. Το συμμετρικό κλειδί δεν είναι πλέον χρήσιμο και μπορεί να αχρηστευτεί.

Κίνδυνος υποκλοπής του μηνύματος δεν υφίσταται, ακόμη και αν κάποιος τρίτος αποκτήσει πρόσβαση στον ψηφιακό φάκελο, ενώ αυτός βρίσκεται καθ'οδόν προς τον παραλήπτη. Ο πιθανός υποκλοπέας δεν μπορεί σε καμμιά περίπτωση να επωφεληθεί, δεδομένου ότι θα πρέπει να λάβει γνώση του συμμετρικού κλειδιού, το οποίο όμως είναι κρυπτογραφημένο και είναι δυνατόν να αποκωδικοποιηθεί μόνο με το ιδιωτικό κλειδί του παραλήπτη, το οποίο είναι ούτως ή άλλως απόρρητο.

Παρ'όλα αυτά, η μέθοδος αυτή παρουσιάζει το εξής πρόβλημα: Ενας τρίτος μπορεί να εντοπίσει το δημόσιο κλειδί του παραλήπτη Β (μέσω καταλόγου) και στη συνέχεια να δημιουργήσει ένα συμμετρικό κλειδί, με το οποίο να κρυπτογραφήσει ένα τελείως διαφορετικό μήνυμα, το οποίο και να αποστείλει στον Β με τη μορφή του ψηφιακού φακέλου όπως παραπάνω. Ο Β θα παραλάβει τον ψηφιακό φάκελο, θα αποκωδικοποιήσει το συμμετρικό κλειδί με χρήση του δικού του ιδιωτικού κλειδιού και τέλος θα αποκρυπτογραφήσει το μήνυμα με το συμμετρικό κλειδί. Το μήνυμα όμως αυτό δεν έχει καμμία σχέση με το πραγματικώς αναμενόμενο και βεβαίως δεν έχει προέλθει από τον Α.

Προκύπτει επομένως <u>πρόβλημα πιστοποίησης της ταυτότητας του αποστολέα</u>. Η απάντηση στο πρόβλημα αυτό μπορεί να δοθεί με τη βοήθεια των ψηφιακών υπογραφών, οι οποίες προϋποθέτουν τη χρήση των λεγομένων αλγορίθμων κατατεμαχισμού (hash algorithms). Τα θέματα αυτά εξετάζονται στη συνέχεια.

2.3.1. Αλγόριθμοι κατατεμαχισμού (hash algorithms)

Ενας αλγόριθμος κατατεμαχισμού (hash algorithm, hash function) είναι μια μονόδρομη διαδικασία, η οποία μπορεί να αντιστοιχήσει ένα αυθαιρέτου μεγέθους μήνυμα σε μια συγκεκριμένη, μικρού σχετικά μεγέθους, τιμή, η οποία είναι γνωστή ως σύνοψη ή αποτύπωμα του μηνύματος (message digest, message fingerprint). Ετσι το μήνυμα μπορεί να περιλαμβάνει από λίγες λέξεις μέχρι εκατοντάδες ή χιλιάδες γραμμές, ενώ το αποτύπωμα έχει μέγεθος 128 ή 160 bits, ανάλογα με τον αλγόριθμο. Οι αλγόριθμοι κατατεμαχισμού έχουν την ιδιότητα ότι αν το αρχικό μήνυμα αλλοιωθεί έστω και κατ'ελάχιστο (έστω και κατά ένα bit), τότε το παραγόμενο από τον αλγόριθμο αποτύπωμα θα έχει μια εντελώς διαφορετική τιμή, σε σχέση με το αποτύπωμα του αρχικού-αυθεντικού μηνύματος.

Οι αλγόριθμοι κατατεμαχισμού που χρησιμοποιούνται στην κρυπτογραφία σχεδιάζονται έτσι ώστε να διαθέτουν ορισμένες ειδικές ιδιότητες:

- Ο αλγόριθμος δεν μπορεί να εκτελεστεί με αντίστροφη κατεύθυνση και να αποκαλύψει έστω και μέρος του αρχικού μηνύματος
- Ο αλγόριθμος δεν παρουσιάζει συγκρούσεις (collisions): έτσι είναι υπολογιστικά αδύνατη η ύπαρξη δύο διαφορετικών μηνυμάτων με το ίδιο αποτύπωμα.
- Το προκύπτον αποτύπωμα (digest) δεν αποκαλύπτει τίποτε σε σχέση με το αρχικό μήνυμα
- Είναι πρακτικό αδύνατο να δημιουργηθεί / ανακαλυφθεί κείμενο, το οποίο να παράγει ένα συγκεκριμένο επιθυμητό αποτύπωμα. Αυτό εμποδίζει οποιονδήποτε τρίτο να υποκαταστήσει ένα μήνυμα χωρίς να προκαλέσει ασυμφωνία στο αποτύπωμα.

Οι συνηθέστερα χρησιμοποιούμενοι αλγόριθμοι είναι ο MD5 της RSA, ο οποίος παράγει αποτύπωμα (digest) μεγέθους 128 bits και προορίζεται για χρήση σε επεξεργαστές 32-bits (σε αντίθεση με τον παλαιότερο MD2, που είχε αναπτυχθεί για χρήση σε επεξεργαστές 8-bits) και ο SHA-1 (Secure Hash Algorithm), με αποτύπωμα 160 bits και ο οποίος απευθύνεται επίσης σε σύγχρονους μεγάλης ισχύος επεξεργαστές.

2.3.2. Ψηφιακές υπογραφές

Οι ψηφιακές υπογραφές αποτελούν μια ειδική κατηγορία των ηλεκτρονικών υπογραφών και δημιουργήθηκαν με σκοπό να καταστήσουν εφικτή την πιστοποίηση ταυτότητας στις ηλεκτρονικές συναλλαγές μέσω του Internet. Αποτελούν το ψηφιακό ανάλογο των φυσικών υπογραφών που χρησιμοποιούνται στην καθημερινή πρακτική και διαθέτουν μια σειρά πλεονεκτήματα. Παρουσιάζουν όμως και ορισμένες αβεβαιότητες, κυρίως σε σχέση με την νομική τους ισχύ, την ισοδυναμία τους με τις φυσικές υπογραφές, αλλά και την αποδοχή τους από το ευρύ κοινό. Εκτενέστερη αναφορά στα παραπάνω γίνεται σε επόμενα κεφάλαια, ενώ εδώ εξετάζεται κυρίως η τεχνική πλευρά του θέματος και η χρήση τους σε σχέση με την πιστοποίηση ταυτότητας του αποστολέα ενός ηλεκτρονικού μηνύματος, προκειμένου να διασφαλιστεί ο παραλήπτης από κινδύνους πλαστοπροσωπίας κατά την ανταλλαγή μηνυμάτων.

Ουσιαστικά **μια ψηφιακή υπογραφή είναι** ορισμένα δεδομένα που συνοδεύουν ή συσχετίζονται λογικά με ένα ψηφιακά κωδικοποιημένο μήνυμα και τα οποία δεδομένα μπορούν να χρησιμοποιηθούν για να εξακριβωθεί τόσο ο αποστολέας του μηνύματος όσο και το ότι το μήνυμα δεν έχει κατά οποιονδήποτε τρόπο αλλοιωθεί αφ'ότου έπαυσε να είναι υπό τον έλεγχο του αποστολέα.

Οι ψηφιακές υπογραφές λειτουργούν μέσα σε ένα περιβάλλον ασύμμετρης κρυπτογραφίας και προϋποθέτουν την χρησιμοποίηση τόσο αλγορίθμων κατατεμαχισμού όσο και αλγορίθμων υπογραφής με χρήση του ιδιωτικού κλειδιού του υπογράφοντος. Σε πρώτη φάση το αρχικό μήνυμα (και συγκεκριμένα η ηλεκτρονική δυαδική του μορφή) υποβάλλεται στον αλγόριθμο κατατεμαχισμού, οπότε προκύπτει το λεγόμενο αποτύπωμα (message digest), το οποίο είναι μια ακολουθία δυαδικών ψηφίων (bits, 0-1), μήκους 128 ή 160 bits, η οποία είναι μοναδική σε σχέση με το αρχικό μήνυμα. Στη συνέχεια το αποτύπωμα υπογράφεται ψηφιακά από τον αποστολέα, με χρήση του ιδιωτικού του κλειδιού, εφαρμόζεται δηλ. ο αλγόριθμος υπογραφής πάνω στο αποτύπωμα. Η ακολουθία ψηφίων που προκύπτει αποτελεί την ψηφιακή υπογραφή. Το ιδιωτικό κλειδί του υπογράφοντος ενσωματώνεται μέσα στον αλγόριθμο υπογραφης κατά τη διαδικασία της υπογραφής, ενώ το αντίστοιχο δημόσιο κλειδί ενσωματώνεται στη διαδικασία επαλήθευσης της υπογραφής, η οποία θα εκτελεστεί από τον παραλήπτη. Για την κατανόηση του μηχανισμού παρατίθεται το εξής απλουστευμένο παράδειγμα:

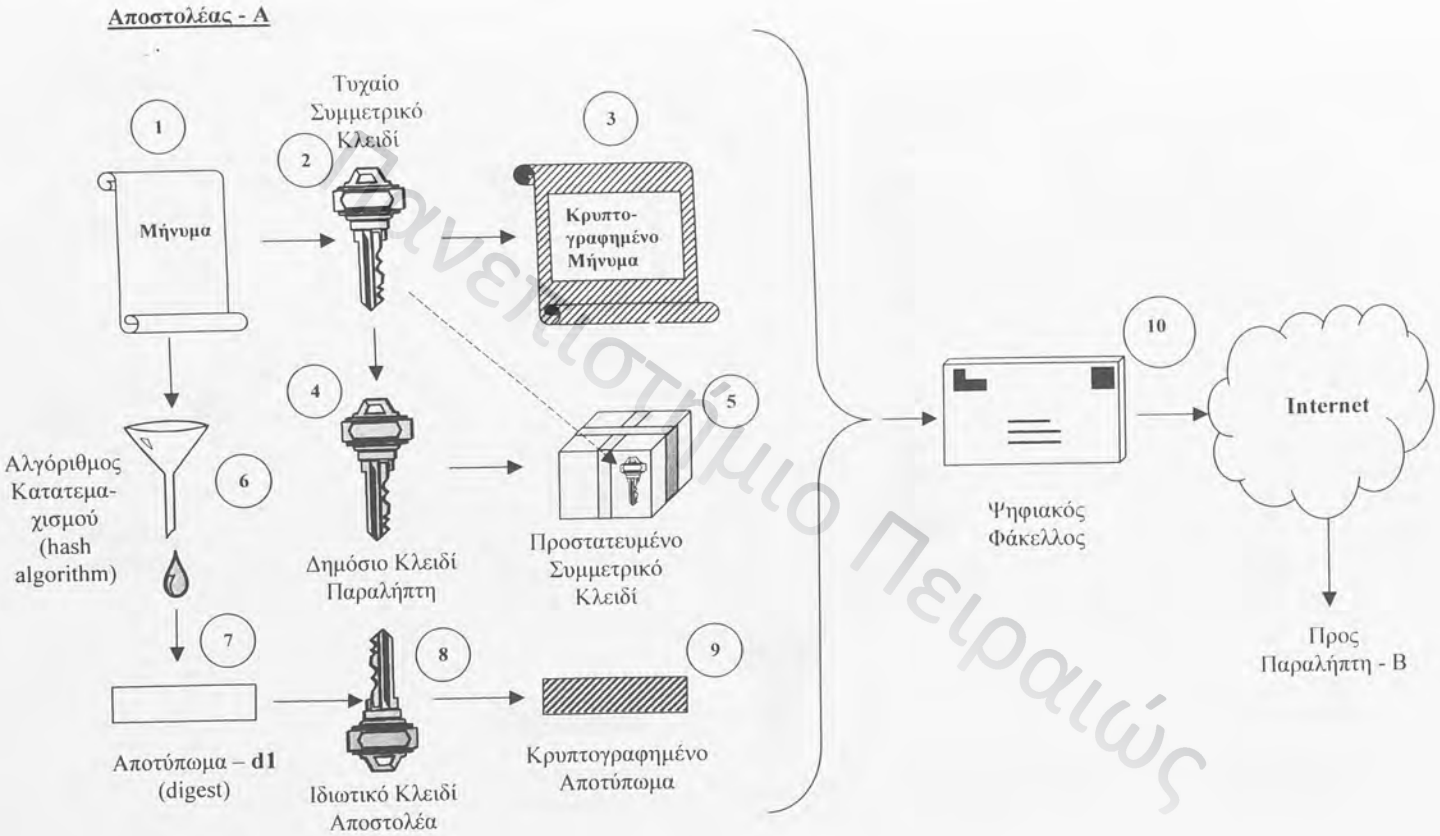
Αρχικό μήνυμα:	**100**
Αλγόριθμος κατατεμαχισμού:	Πολλαπλασιασμός επί 2
Αποτύπωμα (digest):	**200**
Ιδιωτικό κλειδί:	3
Αλγόριθμος υπογραφής:	Πολλαπλασιασμός του αποτυπώματος με τη δύναμη με βά το 2 και εκθέτη το ιδιωτικό κλειδί
Ψηφιακή υπογραφή:	**1600** (= 200 x 2 ^ 3)

Είναι προφανές ότι η ψηφιακή υπογραφή δεν έχει καμμία σχέση με το όνομα του υπογράφοντος, αλλά ούτε και με την χειρόγραφη υπογραφή του. Στην πραγματικότητα είναι ένας μετασχηματισμός του ίδιου του μηνύματος, ο οποίος ενσωματώνει ένα "μυστικό" γνωστό μόνο στον υπογράφοντα. Κατά συνέπεια είναι άρρηκτα συνδεδεμένο και με τον υπογράφοντα, αλλά και με το μήνυμα το οποίο υπογράφεται. Είναι επίσης προφανές ότι, σε αντίθεση με την χειρόγραφη υπογραφή, η ψηφιακή υπογραφή ενός υπογράφοντος θα είναι διαφορετική για κάθε μήνυμα (ψηφιακό έγγραφο) που υπογράφει. Ετσι, αν στο πιο πάνω παράδειγμα το αρχικό μήνυμα ήταν το 110 (αντί 100), τότε η αντίστοιχη ψηφιακή υπογραφή θα ήταν το 1760 (αντί 1600).

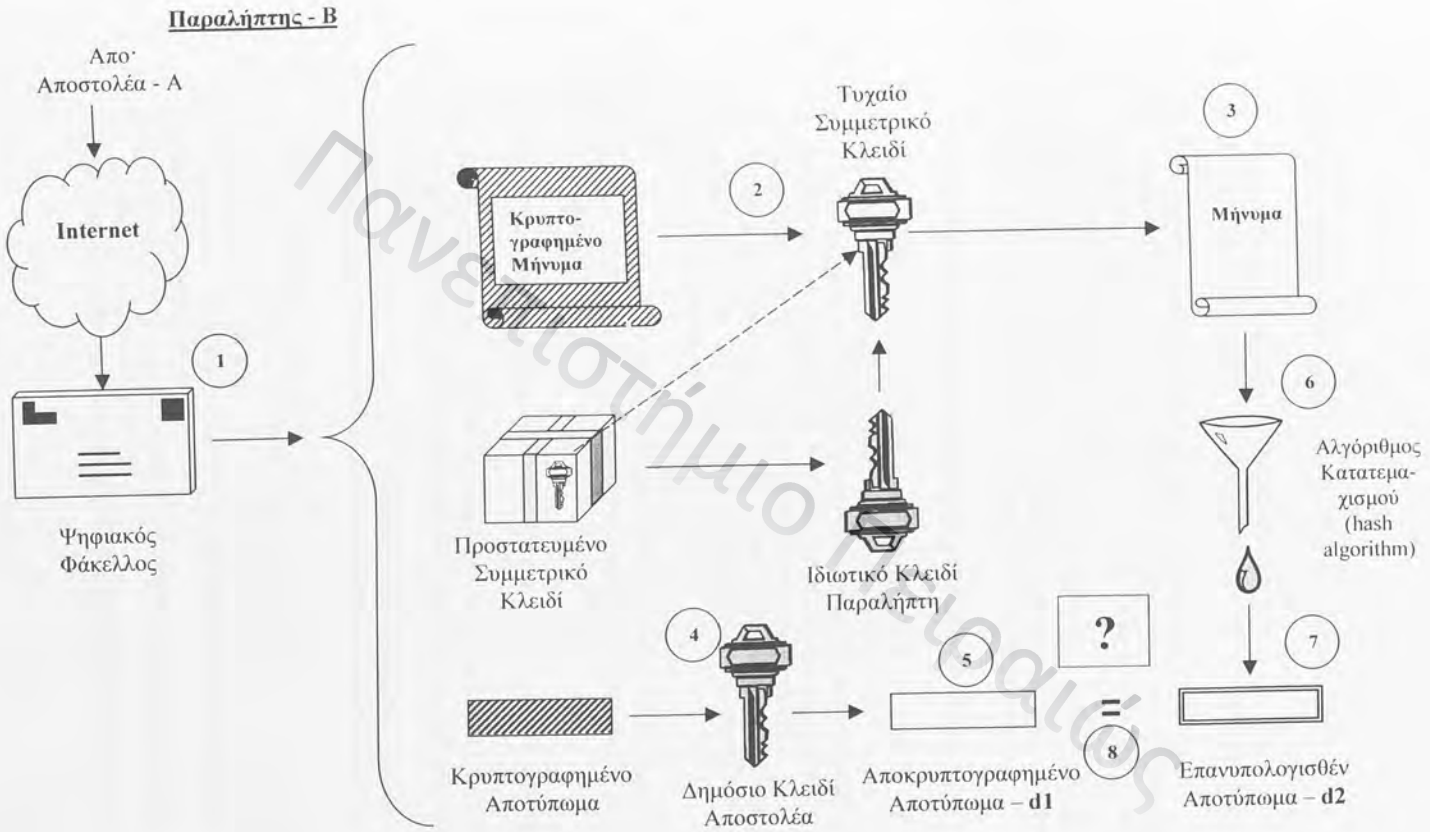
Προκειμένου ένα μήνυμα να διαβιβαστεί με ασφάλεια από τον αποστολέα στον παραλήπτη και να έχει ο δεύτερος βέβαιη γνώση για την ταυτότητα του αποστολέα, δεν αρκεί το μήνυμα

να υπογραφεί ψηφιακά από τον αποστολέα, αλλά θα πρέπει και ο παραλήπτης να είναι σε θέση να επαληθεύσει την ψηφιακή υπογραφή που συνοδεύει το μήνυμα, δηλαδή να μπορεί να βεβαιωθεί για την ταυτότητα του αποστολέα.

Στα δύο σχήματα που ακολουθούν παριστάνονται διαγραμματικά όλα τα βήματα της διαδικασίας.
Συγκεκριμένα, στο Σχήμα 6 απεικονίζεται η δημιουργία, η κρυπτογράφηση και η υπογραφή ενός μηνύματος από τον αποστολέα (έστω Α). Το μήνυμα αποστέλλεται στη συνέχεια (π.χ. μέσω του Internet, άρα μέσα από μη ελεγχόμενους και πιθανότατα ανασφαλείς διαύλους επικοινωνίας) στον παραλήπτη (έστω Β).
Στη συνέχεια, στο Σχήμα 7 περιγράφεται η διαδικασία που ακολουθεί ο Β, αφού παραλάβει το μήνυμα.



Σχήμα 6. **Ψηφιακές υπογραφές – δημιουργία υπογραφής και αποστολή υπογεγραμμένου μηνύματος**



Σχήμα 7. **Ψηφιακές υπογραφές – Παραλαβή υπογεγραμμένου μηνύματος και επαλήθευση υπογραφής**

Εάν: d1 = d2, τότε:	I. Το μήνυμα προέρχεται από τον Α II. Το μήνυμα δεν έχει αλλοιωθεί κατά τη μεταφορά

Αναλυτικά τα βήματα που ακολουθούνται στο Σχήμα 6 είναι τα εξής:

1. Ο αποστολέας Α δημιουργεί το αρχικό μήνυμα
2. Στη συνέχεια δημιουργείται (με τη βοήθεια του λογισμικού) ένα τυχαίο συμμετρικό κλειδί
3. Με χρήση του συμμετρικού κλειδιού κρυπτογραφείται το μήνυμα
4. Ο αποστολέας Α αποκτά το δημόσιο κλειδί του παραλήπτη Β (πιθανόν από κάποια υπηρεσία καταλόγου ή μπορεί να το έχει ήδη στη διάθεσή του από κάποια προηγούμενη επικοινωνία με τον Β)
5. Με χρήση του δημόσιου κλειδιού του Β κρυπτογραφείται το συμμετρικό κλειδί και προκύπτει το λεγόμενο προστατευμένο συμμετρικό κλειδί, το οποίο μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί του παραλήπτη.

Τα υπόλοιπα βήματα αφορούν τη δημιουργία της ψηφιακής υπογραφής:

6. Στο αρχικό μήνυμα εφαρμόζεται ο αλγόριθμος κατατεμαχισμού
7. Προκύπτει το αποτύπωμα (digest) του μηνύματος, έστω d1
8. Το αποτύπωμα του μηνύματος κρυπτογραφείται με το ιδιωτικό κλειδί του αποστολέα
9. Προκύπτει η κρυπτογραφημένη μορφή του αποτυπώματος, η οποία είναι δυνατόν να αποκρυπτογραφηθεί μόνο με το δημόσιο κλειδί του αποστολέα.
10. Τελικώς, το κρυπτογραφημένο μήνυμα, το προστατευμένο συμμετρικό κλειδί και το κρυπτογραφημένο αποτύπωμα του μηνύματος αποστέλλονται και τα τρία, με τη μορφή του ψηφιακού φακέλου, στον παραλήπτη.

Σημ. Είναι πολλές φορές δυνατό, αλλά και επιθυμητό, να αποσταλεί μαζί και το ψηφιακό πιστοποιητικό του αποστολέα. Η έννοια του ψηφιακού πιστοποιητικού εξετάζεται στα επόμενα κεφάλαια.

Από την πλευρά του παραλήπτη Β τα βήματα που εκτελούνται είναι τα παρακάτω (Σχήμα 7):

1. Παραλαβή του ψηφιακού φακέλου και διαχωρισμός του περιεχομένου στα τρία μέρη: κρυπτογραφημένο μήνυμα, προστατευμένο συμμετρικό κλειδί και κρυπτογραφημένο αποτύπωμα.
2. Με χρήση του ιδιωτικού κλειδιού του παραλήπτη αποκωδικοποιείται το προστατευμένο συμμετρικό κλειδί και καθίσταται διαθέσιμο το ίδιο το συμμετρικό κλειδί.
3. Με χρήση του συμμετρικού κλειδιού αποκρυπτογραφείται το κρυπτογραφημένο μήνυμα και προκύπτει το μήνυμα στην κανονική αναγνώσιμη μορφή του.
4. Εντοπίζεται το δημόσιο κλειδί του αποστολέα (μέσω καταλόγου κλπ)
5. Με χρήση του δημόσιου κλειδιού του αποστολέα αποκρυπτογραφείται το αποτύπωμα (digest) του μηνύματος
6. Εφαρμόζεται από τον παραλήπτη ο αλγόριθμος κατατεμαχισμού πάνω στην κανονική αναγνώσιμη μορφή του μηνύματος.
7. Προκύπτει ένα δεύτερο αποτύπωμα (digest) του μηνύματος, έστω d2.

8. Τέλος, συγκρίνονται τα δύο αποτυπώματα (digests), d1 και d2. Αν είναι ίδια, τότε ο παραλήπτης Β έχει βεβαιωθεί για δύο πράγματα:
   I. το μήνυμα προέρχεται από τον Α (**επιβεβαίωση ταυτότητας αποστολέα**)
   II. το μήνυμα δεν έχει αλλοιωθεί κατά τη μεταφορά (**επιβεβαίωση για την ακεραιότητα του μηνύματος**).

Τα δύο πιο πάνω συμπεράσματα τεκμηριώνονται ως εξής:

Το κρυπτογραφημένο αποτύπωμα του μηνύματος αποκρυπτογραφήθηκε επιτυχώς (δεδομένου ότι συγκρίθηκε και βρέθηκε ίδιο με το επανυπολογισθέν αποτύπωμα) με το δημόσιο κελιδί του Α, άρα μόνο ο Α θα μπορούσε να είχε στείλει αυτό το μήνυμα, εφ'όσον μόνο αυτός κατέχει το άλλο μέλος του ζεύγους: "δημόσιο/ιδιωτικό κλειδί του Α", δηλαδή το αντίστοιχο ιδιωτικό κλειδί.

Εξάλλου, είναι βέβαιο ότι το μήνυμα δεν έχει τροποποιηθεί από κάποιον τρίτο κατά τη μεταφορά, διότι αν είχε συμβεί αυτό, τότε το δεύτερο αποτύπωμα (d2) που υπολογίζεται από τον παραλήπτη θα διέφερε από το πρώτο (d1), λόγω των ιδιοτήτων των αλγορίθμων κατατεμαχισμού, οι οποίοι δίνουν διαφορετικό αποτέλεσμα (αποτύπωμα), εάν το μήνυμα αλλοιωθεί έστω και κατ' ελάχιστο.

Σε ό,τι αφορά την δυνατότητα τα δύο μέρη να εκτελέσουν τον ίδιο αλγόριθμο κατατεμαχισμού (ώστε να είναι συγκρίσιμα τα αποτελέσματα) και το πώς ο Α ενημερώνει τον Β για το ποιόν ακριβώς αλγόριθμο χρησιμοποίησε, σημειώνεται ότι αυτό επιτυγχάνεται με τη μεταφορά (μαζί με το κρυπτογραφημένο αποτύπωμα) και μιας συμπληρωματικής πληροφορίας, η οποία αναφέρει τον αλγόριθμο που χρησιμοποίησε ο αποστολέας.

Θα πρέπει να αναφερθεί στο σημείο αυτό ότι για τη διεξαγωγή της διαδικασίας που περιγράφηκε πιο πάνω χρησιμοποιείται σήμερα κατάλληλος πληροφορικός εξοπλισμός (π.χ. ένας ισχυρός προσωπικός υπολογιστής), ενώ απαιτείται και κατάλληλο λογισμικό που να υποστηρίζει κρυπτογραφικές λειτουργίες και ψηφιακές υπογραφές (Παράδειγμα τέτοιου λογισμικού είναι τα σύγχρονα προγράμματα πλοήγησης στο Internet: MS-Internet Explorer, Netscape κλπ). Για τον ίδιο το χρήστη η όλη διαδικασία δεν γίνεται ιδιαίτερα αντιληπτή (είναι όπως λέγεται διαφανής - transparent). Μπορεί όμως να χρειαστεί η συμμετοχή του στη φάση της αρχικής διαμόρφωσης του περιβάλλοντος, όπως και σε κάποια παραπέρα παραμετροποίηση. Επιπλέον, πιθανόν να απαιτηθεί και η χρήση ειδικών συσκευών (π.χ. έξυπνες κάρτες - smart cards), στις οποίες μπορεί να βρίσκονται αποθηκευμένα κρυπτογραφικά κλειδιά.

Ενα σύστημα κρυπτογράφησης και ψηφιακών υπογραφών, όπως αναλύθηκε παραπάνω, εξασφαλίζει σε μεγάλο βαθμό την ασφαλή διακίνηση μηνυμάτων. Δεν παρέχει όμως πλήρη προστασία απέναντι σε κάθε κακόβουλη προσπάθεια τρίτων. Εξετάζοντας και πάλι τη σειρά των ενεργειών κατά τη φάση της επαλήθευσης από τον παραλήπτη Β της ψηφιακής υπογραφής του αποστολέα Α, παρατηρούμε τα εξής:

(1) Ο παραλήπτης Β εντοπίζει το δημόσιο κλειδί του Α, μέσω κάποιου καταλόγου δημοσίων κλειδιών
(2) Ο παραλήπτης χρησιμοποιεί αυτό το κλειδί για την αποκρυπτογράφηση του κρυπτογραφημένου αποτυπώματος
(3) Το κρυπτογραφημένο αποτύπωμα δημιουργήθηκε από τον Α με χρήση του ιδιωτικού του κλειδιού
(4) Ο αποστολέας Α έχει στην κατοχή του το ένα και μοναδικό αντίγραφο του ιδιωτικού του κλειδιού
(5) Επομένως αν το κρυπτογραφημένο αποτύπωμα d1 και το επανυπολογισθέν αποτύπωμα d2 ταυτίζονται, τότε το μήνυμα πρέπει να προέρχεται από τον Α.

Ο κίνδυνος εντοπίζεται στο σημείο (1) : αν ένας τρίτος (π.χ. ο Γ) αποκτήσει πρόσβαση στον κατάλογο, θα μπορούσε να τοποθετήσει το δικό του δημόσιο κλειδί στη θέση του δημόσιου κλειδιού του Α, δημιουργώντας μια εγγραφή στον κατάλογο, η οποία δίπλα στο όνομα του Α θα αναφέρει το δημόσιο κλειδί του Γ (ψευδώς). Στη συνέχεια έχει τη δυνατότητα να δημιουργεί μηνύματα, τα οποία να τα υπογράφει με το δικό του (δηλ. του Γ) ιδιωτικό κλειδί και τα οποία μετά να τα αποστέλλει στον Β, προσποιούμενος ότι είναι ο Α. Οταν ο Β προσπαθήσει να αποκρυπτογραφήσει το πλαστό μήνυμα (την πλαστότητα του οποίου αγνοεί), θα ανακτήσει από τον κατάλογο το δημόσιο κλειδί του αποστολέα (ο οποίος φέρεται να είναι ο Α), λαμβάνοντας όμως ψευδώς το δημόσιο κλειδί του Γ. Τα υπόλοιπα βήματα θα εκτελεστούν με "επιτυχία" (ταύτιση αποτυπωμάτων d1 και d2 κλπ), αφήνοντας τον Β με την εσφαλμένη εντύπωση ότι έλαβε ένα μήνυμα υπογεγραμμένο από τον Α.

Επομένως το ζήτημα που ανακύπτει είναι ότι απαιτείται ένας μηχανισμός που να διασφαλίζει με απόλυτη βεβαιότητα ότι ένα συγκεκριμένο δημόσιο κλειδί ανήκει σε ένα συγκεκριμένο πρόσωπο.

Η παρατήρηση αυτή μας εισάγει στην έννοια των ψηφιακών πιστοποιητικών, τα οποία παρουσιάζονται αναλυτικά στη συνέχεια.

3. Η ΑΝΑΓΚΑΙΟΤΗΤΑ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ PKI

3.1. Οι ανεπάρκειες της κρυπτογραφίας

Η κρυπτογραφία δημοσίου κλειδιού παρέχει τα εργαλεία με τα οποία καθίσταται δυνατή η υλοποίηση λειτουργιών ασφαλείας, όπως είναι οι ψηφιακές υπογραφές. Αν και η σχετική τεχνολογία είναι διαθέσιμη εδώ και αρκετό καιρό (από τα τέλη της δεκαετίας του 1970), εντούτοις δεν είναι από μόνη της επαρκής για τη δημιουργία ενός ασφαλούς ηλεκτρονικού περιβάλλοντος, που θα προσφέρει με πλήρη και αποτελεσματικό τρόπο όλο το εύρος των απαιτουμένων υπηρεσιών.

Για παράδειγμα, τα ηλεκτρονικά έγγραφα δεν διαθέτουν, από τη φύση τους, ένα εύκολο τρόπο που να επιτρέπει στο συντάκτη τους να επικυρώσει τα περιεχόμενα ή να βεβαιωθεί ότι τα περιεχόμενα αυτά δεν έχουν τροποποιηθεί, σε σχέση με το πρωτότυπο. Οι ψηφιακές υπογραφές υποστηρίζουν και τις δύο αυτές δυνατότητες. Ετσι, θα μπορούσαν να χρησιμοποιηθούν για λόγους ελέγχου, όπως για να διασφαλίσουν ότι κάποιος έχει λάβει γνώση των περιεχομένων ενός εγγράφου ή για να προσφέρουν κάποια νομική υπόσταση σε ένα συμβόλαιο, δεδομένου ότι στην περίπτωση αυτή απαιτείται από το νόμο τα συμβαλλόμενα μέρη να παράσχουν ένα χαρακτηριστικό τους σημείο-σημάδι, το οποίο να είναι εύκολα αναγνωρίσιμο. Φυσικά η χρήση και αποδοχή των ψηφιακών υπογραφών συνδυάζεται με την ύπαρξη αντίστοιχης νομοθεσίας, θέμα το οποίο εξετάζεται αναλυτικά στο Κεφ. 13.

Η δημιουργία μιας ψηφιακής υπογραφής απαιτεί κατ' αρχήν τη δημιουργία του κρυπτογραφικού αποτυπώματος, με εφαρμογή του σχετικού αλγορίθμου επί του περιεχομένου του εγγράφου (ή επί των τμημάτων του εγγράφου, τα οποία θεωρούνται σημαντικά), προκειμένου να διασφαλιστεί ότι αυτό δεν θα τροποποιηθεί. Για παράδειγμα, στην περίπτωση ενός συμβολαίου, το σημαντικό μέρος του εγγράφου αφορά το σύνολο του περιεχομένου του. Αντίθετα, σε μια ηλεκτρονική φόρμα που συμπληρώνει κάποιος, όταν πραγματοποιεί συναλλαγές μέσω του Web server μιας επιχείρησης, το σημαντικό μέρος περιλαμβάνει κυρίως τα προς συμπλήρωση πεδία, όπως ο κωδικός και η περιγραφή του προϊόντος, η ποσότητα, καθώς και οι πληροφορίες που έχουν σχέση με την ταυτότητα του χρήστη και τον τρόπο πληρωμής, αλλά όχι τα στοιχεία εκείνα που καθορίζουν τον τρόπο εμφάνισης της φόρμας στην οθόνη του χρήστη (HTML tags). Στη συνέχεια, σε κάθε περίπτωση, το αποτύπωμα κρυπτογραφείται τελικά με χρήση του ιδιωτικού κλειδιού του υπογράφοντος.

Για την επαλήθευση της ψηφιακής υπογραφής, απαιτείται η εκ νέου δημιουργία του αποτυπώματος του σημαντικού μέρους του εγγράφου. Το αρχικό αποτύπωμα που είχε κρυπτογραφηθεί με το ιδιωτικό κλειδί του υπογράφοντος πρέπει να αποκρυπτογραφηθεί με χρήση του αντίστοιχου δημόσιου κλειδιού και στη συνέχεια τα δύο αποτυπώματα συγκρίνονται και εφ' όσον είναι ίδια, η υπογραφή θεωρείται ότι έχει επαληθευτεί.

που μπορεί να ζητηθούν από ένα άτομο, όταν αυτό επιθυμεί να έχει μια συνεργασία (ή γενικώς να συνάψει κάποιου είδους σχέση) με κάποιο οργανισμό ή επιχείρηση. Στην περίπτωση αυτή, οι συστατικές επιστολές πρέπει να προέρχονται από κάποιο ευϋπόληπτο και αξιόπιστο πρόσωπο (π.χ. καθηγητή πανεπιστημίου, γνωστό δικηγόρο, διευθυντή κάποιας μεγάλης επιχείρησης κλπ), ευρύτερα γνωστό και αποδεκτό.

Η ανάγκη για κάποιου είδους διαβεβαίωση, σε ό,τι αφορά τα χαρακτηριστικά και την αξιοπιστία κάποιου ατόμου, είναι όμως γενικότερη. Ετσι, πέρα από τις προσωπικές συστάσεις, που χρησιμοποιούνται μόνο σε ορισμένες περιπτώσεις, έχει καθιερωθεί γενικότερα η έννοια της ταυτότητας, με τη μορφή ενός συγκεκριμένου εγγράφου. Το έγγραφο αυτό, το οποίο περιλαμβάνει μια σειρά πληροφοριών που αφορούν ένα συγκεκριμένο άτομο, εκδίδεται και υπογράφεται από κάποια οντότητα-αρχή, ο ρόλος της οποίας είναι αποδεκτός από όλους (ή από ένα ευρύτερο σύνολο ανθρώπων) και η αξιοπιστία της θεωρείται δεδομένη. Η αρχή αυτή παίζει το ρόλο του τρίτου μέρους, που είναι πολλές φορές απαραίτητο, προκειμένου να διευκολύνει διάφορες μορφές επικοινωνίας και συναλλαγών. Ετσι, η ταυτότητα είναι ένα έγγραφο, που περιέχει μια σειρά πληροφοριών που προσδιορίζουν τον κάτοχό της, ενώ το ακριβές και αληθές των πληροφοριών αυτών επιβεβαιώνεται από την αρχή που την έχει εκδώσει.

Στην πραγματικότητα, η παρεμβολή του τρίτου μέρους-αρχής επιτρέπει τη "μεταφορά εμπιστοσύνης" από το ένα συναλλασσόμενο μέρος στο άλλο. Μια ταυτότητα που εκδίδεται από μια τέτοια αρχή αποτελεί ουσιαστικά μια κωδικοποιημένη μέθοδο για τη διευκόλυνση αυτής της "μεταφοράς εμπιστοσύνης" και στηρίζεται στην προϋπόθεση ότι και τα δύο ενδιαφερόμενα μέρη εμπιστεύονται την παραπάνω αρχή.

Χαρακτηριστικά παραδείγματα ταυτότητας στην καθημερινή ζωή αποτελούν οι εθνικές ταυτότητες που χρησιμοποιούνται στο εσωτερικό μιας χώρας και τα διαβατήρια, που χρησιμεύουν για την επαλήθευση ταυτότητας ενός ατόμου, όταν αυτό μετακινείται σε άλλες χώρες. Επίσης ταυτότητες κάποιας μορφής εκδίδουν διάφορες επαγγελματικές ενώσεις, σύλλογοι, τράπεζες κλπ. Γενικά, μια ταυτότητα μπορεί να απαιτεί κάποια διαδικασία ανανέωσης μετά από ορισμένο χρόνο ή μπορεί επίσης να ανακληθεί, αν αυτό κριθεί απαραίτητο.

Μια αρχή που εκδίδει ταυτότητες έχει σαφώς αναγνωρισμένο το σχετικό δικαίωμα, με άλλα λόγια ταυτότητες δεν μπορεί να εκδίδει ο οποιοσδήποτε. Εξάλλου, η αναγνώριση μιας ταυτότητας ως αξιόπιστης συνδυάζεται με τη διαδικασία που η αρμόδια αρχή ακολουθεί κατά την έκδοσή της, προκειμένου να συγκεντρώσει και να επαληθεύσει τα στοιχεία που η ταυτότητα περιλαμβάνει. Επιπλέον, οι ταυτότητες, ανάλογα με το ποιός τις εκδίδει, έχουν και αντίστοιχη αναγνώριση και πεδίο εφαρμογής.

3.3. Αρχές Πιστοποίησης και ο ρόλος τους σε ένα σύστημα PKI

Με δεδομένο το ρόλο του δημόσιου κλειδιού στα πλαίσια της ασύμμετρης κρυπτογραφίας, το κύριο ζητούμενο είναι ένας αξιόπιστος μηχανισμός για τη διανομή των κλειδιών αυτών .

Ο μηχανισμός αυτός δεν μπορεί παρά να στηρίζεται στη σύνδεση ενός δημόσιου κλειδιού με ορισμένες πληροφορίες που προσδιορίζουν την ταυτότητα του κατόχου του. Ο συνδυασμός αυτός δημιουργεί τη λεγόμενη "ψηφιακή ταυτότητα" (digital identity) ή όπως είναι πιο γνωστό, το "ψηφιακό πιστοποιητικό" (digital certificate). Τα ψηφιακά πιστοποιητικά αποτελούν το ψηφιακό ανάλογο των κλασσικών ταυτοτήτων και αποτελούν τη βάση για τη δημιουργία ενός ασφαλούς ηλεκτρονικού περιβάλλοντος, διότι επιτρέπουν την διασφάλιση ενός επιπέδου εμπιστοσύνης, σχετικά με το ποιός είναι ο πραγματικός κάτοχος ενός δεδομένου δημόσιου κλειδιού.

Οι φορείς που είναι υπεύθυνοι για την έκδοση ψηφιακών πιστοποιητικών (ψηφιακών ταυτοτήτων) στα πλαίσια ενός συστήματος PKI ονομάζονται **Αρχές Πιστοποίησης** - ΑΠ (Certification Authorities - CA). Μια ΑΠ εφαρμόζει συγκεκριμένες διαδικασίες, οι οποίες επαληθεύουν την ταυτότητα του υποψηφίου και στη συνέχεια εκδίδει ένα ψηφιακό πιστοποιητικό, που μπορεί να χρησιμοποιηθεί σαν απόδειξη αυτής της ταυτότητας. Τα ψηφιακά πιστοποιητικά εκδίδονται με προκαθορισμένη διάρκεια ισχύος και είναι δυνατόν να ανακληθούν, αν αυτό χρειαστεί.
Οι Αρχές Πιστοποίησης παίζουν το ρόλο του έμπιστου τρίτου μέρους, όπως αυτός περιγράφηκε παραπάνω, καθιστώντας δυνατή και διευκολύνοντας την επικοινωνία ανάμεσα σε δύο άλλα μέρη και για το λόγο αυτό είναι γνωστές και ως "Εμπιστες Τρίτες Οντότητες - ΕΤΟ (Trusted Third Parties - TTP)".

Οι κλασσικές ταυτότητες της καθημερινής ζωής έχουν μακρόχρονη προϊστορία σχετικά με το ποιούς φορείς εμπιστευόμαστε για την έκδοσή τους και το τι διαδικασίες ακολουθούν οι φορείς αυτοί. Εντούτοις, ανακύπτουν ορισμένα ζητήματα σχετικά με τις ΑΠ, των οποίων ο ρόλος είναι να δημιουργούν ταυτότητες που θα χρησιμοποιούνται σε ένα ηλεκτρονικό περιβάλλον. Τα ζητήματα αυτά είναι:

- Σε ποιούς θα πρέπει να ανατεθεί η λειτουργία μιας ΑΠ
- Πόσο ευρέως θα χρησιμοποιούνται οι ψηφιακές ταυτότητες
- Τι διαδικασίες και αποδεικτικές μέθοδοι θα ακολουθούνται κατά την έκδοση των ταυτοτήτων
- Ποιούς μηχανισμούς μπορεί να προσφέρει ένα ψηφιακό δίκτυο για να διασφαλίσει, σε λογικά πλαίσια, ότι μια ταυτότητα δεν μπορεί να πλαστογραφηθεί

Σε πρώτη προσέγγιση, θα ήταν λογικό να λειτουργήσουν ως ΑΠ οι φορείς που ήδη ασχολούνται με έκδοση ταυτοτήτων, όπως κάποιες κρατικές αρχές, τράπεζες, επαγγελματικές ενώσεις κλπ. Αυτό θα ήταν πιθανόν αποδεκτό, αλλά με κάποιες επιφυλάξεις ως προς το σκοπό χρήσης αυτών των ψηφιακών πιστοποιητικών. Για παράδειγμα, θα ήταν σωστό το Υπουργείο Μεταφορών να εκδίδει πιστοποιητικά που θα μπορούσαν να χρησιμοποιηθούν ως άδειες οδήγησης, αλλά μάλλον δεν θα ήταν επιθυμητό τα πιστοποιητικά αυτά να έχουν οποιαδήποτε σχέση με τραπεζικές συναλλαγές.

Αυτό πάντως που παρατηρείται σήμερα στην πράξη είναι ότι, παράλληλα με τις παραδοσιακές έμπιστες οντότητες, έχουν αναδειχθεί νέες μορφές φορέων, εμπορικού χαρακτήρα, που λειτουργούν ως ΑΠ. Οι φορείς αυτοί παρέχουν, έναντι αμοιβής, τις

λεγόμενες "υπηρεσίες πιστοποίησης" και έχουν επιτύχει να καθιερωθούν στο χώρο αυτό χωρίς να διαθέτουν προηγούμενη φήμη, στην οποία να στηριχθούν. Η ανάδειξή τους οφείλεται κυρίως σε λόγους, όπως τεχνογνωσία, κατασκευή και χρήση εγκαταστάσεων υψηλής ασφαλείας, ιδιαίτερα προσεκτική επιλογή προσωπικού και υιοθέτηση και εφαρμογή εξαιρετικά αυστηρών διαδικασιών και ελέγχων.

Είναι σαφές ότι στο σημείο αυτό υπάρχει ένα ζήτημα γενικότερου κοινωνικού και πολιτικού ενδιαφέροντος, το οποίο θα πρέπει να αντιμετωπιστεί πολύ προσεκτικά σε όλες του τις διαστάσεις. Η ανάπτυξη ενός ασφαλούς ηλεκτρονικού περιβάλλοντος με τα πλεονεκτήματα που μπορεί να προσφέρει είναι μια εξέλιξη, η οποία θα πρέπει να διευκολυνθεί. Απαιτεί βέβαια, μεταξύ άλλων, υψηλή εξειδίκευση και τεχνολογική γνώση σε ταχύτατα εξελισσόμενους τομείς, γεγονός που τοποθετεί σε πλεονεκτική θέση ορισμένους ιδιωτικούς φορείς, οι οποίοι ήδη λειτουργούν de facto ως ευρύτερα αποδεκτές ΑΠ. Με δεδομένο τον κρίσιμο ρόλο των ΑΠ, θα πρέπει να τεθεί ένα πλαίσιο λειτουργίας τους, το οποίο να διασφαλίζει τη συμμόρφωσή τους με κάποιους κανόνες, προς όφελος του κοινωνικού συνόλου γενικότερα. Προς την κατεύθυνση αυτή έχουν γίνει ήδη ορισμένα βήματα, σε επίπεδο νομοθεσίας, ενώ σχετικές αναφορές υπάρχουν παρακάτω, στο Κεφ. 13.

4. ΒΑΣΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΑΙ ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΣΥΣΤΗΜΑΤΟΣ PKI

4.1. Θεμελιώδεις προϋποθέσεις

Οπως προκύπτει από τα παραπάνω, το ζήτημα της διανομής των δημόσιων κλειδιών, σε ένα περιβάλλον ασύμμετρης κρυπτογραφίας, ανάγεται τελικά στην ανάγκη για ύπαρξη ενός μηχανισμού, σε επίπεδο υποδομής, ο οποίος θα επιτρέπει την έκδοση, διανομή και γενικά τη διαχείριση των ψηφιακών πιστοποιητικών, μέσω των οποίων κάθε κλειδί συνδέεται εγγυημένα με ένα συγκεκριμένο πρόσωπο. Ο μηχανισμός αυτός θα πρέπει να διαθέτει τα εξής χαρακτηριστικά:

- να είναι εύχρηστος
- να στηρίζεται σε ευρέως αποδεκτά πρότυπα
- να είναι αποτελεσματικός
- να είναι ασφαλής
- να εξασφαλίζει διαλειτουργικότητα
- να ενσωματώνεται αποτελεσματικά μέσα σε ήδη λειτουργούντα περιβάλλοντα
- να είναι όσο το δυνατό διαφανής (transparent) για τους χρήστες
- να είναι επεκτάσιμος, προκειμένου να καλύψει μεγάλους πληθυσμούς χρηστών

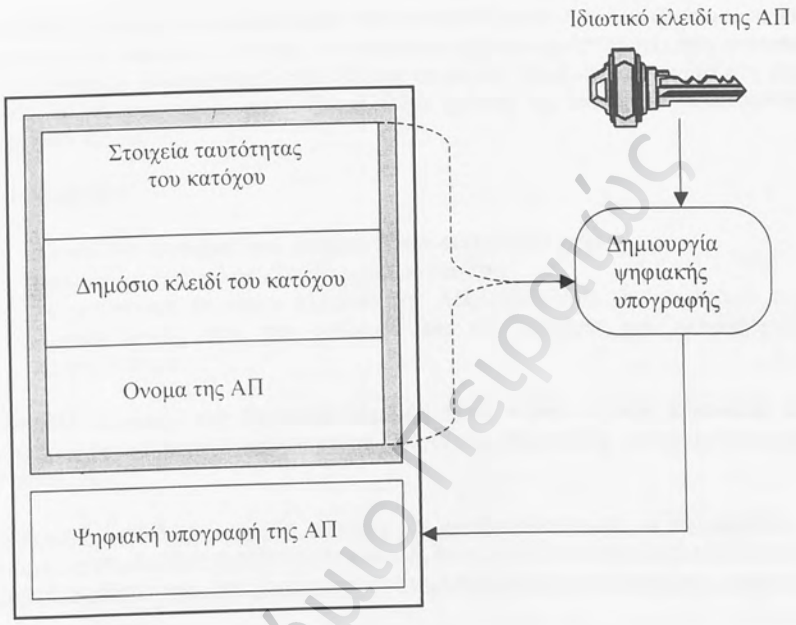
Ενα σύστημα PKI αποτελεί ακριβώς την υλοποίηση ενός τέτοιου μηχανισμού και στηρίζεται σε **δύο θεμελιώδεις προϋποθέσεις:**

1. Υπάρχει μια έμπιστη οντότητα, η οποία μπορεί να δημιουργήσει μια ψηφιακή ταυτότητα που να είναι επαληθεύσιμη και άρρηκτα συνδεδεμένη με ένα δημόσιο κλειδί. Η οντότητα αυτή είναι η λεγόμενη Αρχή Πιστοποίησης (ΑΠ).
2. Υπάρχει κάποιο ιδιωτικό κλειδί, για το οποίο μπορεί να υποτεθεί με βεβαιότητα ότι βρίσκεται στην κατοχή του χρήστη, του οποίου η ταυτότητα βεβαιώνεται μέσω του ψηφιακού πιστοποιητικού και κανενός άλλου. Η έννοια αυτή της ύπαρξης ενός μόνο αντιγράφου του ιδιωτικού κλειδιού αναφέρεται ως μοναδικότητα (singularity) του κλειδιού.

Σημ. Η ανάγκη για διασφάλιση της μοναδικότητας του ιδιωτικού κλειδιού δημιουργεί μια σειρά ειδικών επιπλέον προϋποθέσεων και απαιτήσεων, σχετικά με τη χρήση του και γενικά τη διαχείρισή του, στις οποίες θα γίνει αναφορά σε παρακάτω κεφάλαια.

4.2. Τα ψηφιακά πιστοποιητικά και ο ρόλος τους

Η ΑΠ πρέπει εξ ορισμού να τυγχάνει της εμπιστοσύνης των χρηστών και είναι αυτή που δημιουργεί, αλλά και υπογράφει τις ψηφιακές ταυτότητες (ή ψηφιακά πιστοποιητικά). Η δομή ενός ψηφιακού πιστοποιητικού σε πολύ απλή μορφή είναι αυτή που φαίνεται στο Σχήμα 8:



Σχήμα 8. Απλουστευμένη μορφή ψηφιακού πιστοποιητικού

Η καθιέρωση ψηφιακών πιστοποιητικών του τύπου αυτού διευκολύνει ιδιαίτερα τη διανομή επιβεβαιωμένων δημόσιων κλειδιών. Με δεδομένο ότι ένας χρήστης έχει ήδη αποκτήσει με ασφαλή τρόπο το δημόσιο κλειδί της ΑΠ, την οποία και εμπιστεύεται, μπορεί στη συνέχεια να μάθει το δημόσιο κλειδί οποιουδήποτε άλλου χρήστη, του οποίου το πιστοποιητικό έχει εκδοθεί από την ΑΠ.

Για το σκοπό αυτό:

- ✓ αποκτά ένα αντίγραφο του πιστοποιητικού εκείνου του χρήστη
- ✓ απομονώνει το δημόσιο κλειδί που τον ενδιαφέρει
- ✓ με χρήση του δημόσιου κλειδιού της ΑΠ, επαληθεύει την υπογραφή της ΑΠ, εξασφαλίζοντας έτσι την ορθότητα και την ακρίβεια των πληροφοριών του πιστοποιητικού.

Το μοντέλο διανομής των δημόσιων κλειδιών μέσω πιστοποιητικών προσφέρει μεγάλες δυνατότητες επέκτασης και ευρείας χρήσης, λόγω μιας σημαντικής ιδιότητας των ψηφιακών πιστοποιητικών:

Τα ψηφιακά πιστοποιητικά είναι δυνατόν να αποθηκευθούν και να διανεμηθούν μέσω συστημάτων και διαύλων που δεν είναι ασφαλή, δηλαδή δεν προστατεύονται απαραίτητα από μηχανισμούς ασφάλειας, όπως εμπιστευτικότητα, επιβεβαίωση ταυτότητας και ακεραιότητα.

Αυτό συμβαίνει για τους εξής λόγους:

- ➢ Το δημόσιο κλειδί δεν είναι εμπιστευτικό, επομένως το ίδιο ισχύει και για το ψηφιακό πιστοποιητικό
- ➢ Το πιστοποιητικό είναι αυτο-προστατευόμενο. Η ψηφιακή υπογραφή της ΑΠ που περιλαμβάνεται σ' αυτό παρέχει προστασία σε ό,τι αφορά την επιβεβαίωση ταυτότητας (δηλ. την προέλευσή του), αλλά και την ακεραιότητα του ίδιου του πιστοποιητικού. Αν κάποιος τρίτος αλλοιώσει το πιστοποιητικό, την ώρα που αυτό βρίσκεται καθ' οδόν προς το χρήστη, ο ενδιαφερόμενος χρήστης θα ανιχνεύσει την πιθανή αλλοίωση, διότι η ψηφιακή υπογραφή της ΑΠ δεν θα επαληθεύεται πλέον σωστά.

Συμπερασματικά, το κύριο όφελος από τη χρήση των ψηφιακών πιστοποιητικών είναι ότι ένας χρήστης δημοσίου κλειδιού μπορεί να μάθει με σιγουριά το δημόσιο κλειδί ενός μεγάλου αριθμού άλλων χρηστών, έχοντας αρχικά γνωστό μόνο ένα δημόσιο κλειδί, αυτό της ΑΠ.

4.3. Το PKI ως σύστημα διαχείρισης ψηφιακών πιστοποιητικών

Ενα σύστημα PKI είναι ουσιαστικά ένα σύστημα διαχείρισης ψηφιακών πιστοποιητικών, το οποίο θα πρέπει να καλύψει θέματα, όπως:

- Ασφαλής δημιουργία καλής ποιότητας κλειδιών
- Ελεγχος εγκυρότητας των αρχικών στοιχείων ταυτότητας, που θα συμπεριληφθούν σε ένα πιστοποιητικό
- Εκδοση, ανανέωση και λήξη ισχύος πιστοποιητικών
- Ελεγχος εγκυρότητας πιστοποιητικών
- Διανομή πιστοποιητικών
- Ασφαλής αρχειοθέτηση και ανάκτηση κλειδιών
- Δημιουργία υπογραφών και χρονοσημάνσεων
- Καθιέρωση και διαχείριση σχέσεων εμπιστοσύνης (με άλλα συστήματα PKI)

Τα συστατικά στοιχεία ενός συστήματος PKI θα πρέπει να διακριθούν σε δύο κατηγορίες:

Τεχνικό επίπεδο: Περιλαμβάνει εξοπλισμό πληροφορικής και επικοινωνιών και αντίστοιχο εξειδικευμένο λογισμικό, το οποίο να ικανοποιεί τις απαιτήσεις του συγκεκριμένου περιβάλλοντος. Εδώ εντάσσονται και τυχόν ειδικές συσκευές που θα κριθούν απαραίτητες για τη διασφάλιση του επιθυμητού βαθμού ασφάλειας (π.χ. έξυπνες κάρτες).

Διοικητικό-οργανωτικό επίπεδο: Αφορά τις λειτουργικές διαδικασίες, αλλά και τις πολιτικές που καθορίζουν το πώς εκδίδονται τα πιστοποιητικά και ποιές είναι οι επιτρεπτές χρήσεις τους. Εδώ περιλαμβάνονται και η γενικότερη διαμόρφωση των σχετικών εγκαταστάσεων, καθώς και θέματα που έχουν σχέση με το προσωπικό (επιλογή, υποχρεώσεις, επίβλεψη κλπ).

Επιπρόσθετα, ένα σύστημα PKI πρέπει να ενσωματωθεί ομαλά και ολοκληρωμένα μέσα στους εσωτερικούς και εξωτερικούς μηχανισμούς ασφάλειας, που ήδη διαθέτει ένας οργανισμός ή μια επιχείρηση, προκειμένου να είναι αποτελεσματικό και αποδοτικό.

Ενα σύστημα PKI, όπως προκύπτει εμφανώς και από το ίδιο του το όνομα (Public Key Infrastructure: **Υποδομή** Δημοσίου Κλειδιού - ΥΔΚ), δεν είναι τίποτε άλλο παρά μια υποδομή. Η υποδομή αυτή δεν προσθέτει αξία αφ΄εαυτού της, αλλά μόνο εφ' όσον ενταχθεί ομαλά και ολοκληρωμένα μέσα στο επιχειρηματικό περιβάλλον, ώστε να υποστηρίξει τις διαδικασίες που αυτό περιλαμβάνει. Αυτό σημαίνει ότι ένα επιτυχημένο σύστημα PKI θα πρέπει:

- να είναι εύκολο στη χρήση του
- να είναι όσο το δυνατόν λιγότερο "ορατό" στους χρήστες, με την έννοια ότι αυτοί δεν θα πρέπει να εμπλέκονται καθόλου (εάν είναι δυνατόν) με αυτό, κατά την εκτέλεση των εργασιών τους
- να συνεργάζεται αρμονικά με τις εφαρμογές λογισμικού που χρησιμοποιεί η επιχείρηση
- να προσφέρει διαλειτουργικότητα με άλλα αντίστοιχα προϊόντα λογισμικού (PKI software)

4.4. Αρχιτεκτονική ενός συστήματος PKI

Η αρχιτεκτονική ενός συστήματος PKI, όπως παριστάνεται και διαγραμματικά στο Σχήμα 9, περιλαμβάνει τα εξής συστατικά στοιχεία:

- Αρχή Καταχώρησης - ΑΚ (Registration Authority - RA)
- Αρχή Πιστοποίησης - ΑΠ (Certification Authority - CA)
- Αποθετήριο (Repository)

και παρέχει το σύνολο των υπηρεσιών που απαιτούνται για ένα ασφαλές ηλεκτρονικό περιβάλλον, το οποίο καλύπτει τις τέσσερεις βασικές αρχές της εμπιστευτικότητας, της επιβεβαίωσης ταυτότητας, της ακεραιότητας και της μη αποκήρυξης.

Οι "πελάτες" (clients) ή τελικές οντότητες (end-entities), δηλαδή αυτοί που επωφελούνται από την ύπαρξη ενός συστήματος PKI και από τις υπηρεσίες που αυτό προσφέρει, εντάσσονται και αυτοί στο σύστημα και διακρίνονται σε δύο κατηγορίες:

- Τελικοί χρήστες (πρόσωπα) ή συστήματα που είναι κάτοχοι ψηφιακών πιστοποιητικών
- Χρήστες των ψηφιακών πιστοποιητικών, δηλαδή αυτοί που στηρίζονται στα πιστοποιητικά και εμπιστεύονται τις πληροφορίες που αυτά περιέχουν, προκειμένου να εμπλακούν σε μια ασφαλή επικοινωνία ή να προβούν σε κάποια συναλλαγή με τον κάτοχο του πιστοποιητικού.

Αρχή Καταχώρησης – ΑΚ (Registration Authority – RA)

Η οντότητα αυτή, η ύπαρξη της οποίας είναι προαιρετική σε ένα σύστημα PKI, είναι κυρίως υπεύθυνη για τα θέματα που σχετίζονται με την αρχική επιβεβαίωση της ταυτότητας ενός υποψηφίου. Στην περίπτωση που δεν υπάρχει ΑΚ, το χειρισμό των σχετικών θεμάτων αναλαμβάνει η Αρχή Πιστοποίησης - ΑΠ (βλ. παρακάτω).

Οι λειτουργίες που εκτελεί η ΑΚ μπορεί να ποικίλλουν, ανάλογα με τις ανάγκες του συγκεκριμένου περιβάλλοντος, αλλά κατά κανόνα περιλαμβάνουν:

- Παραλαβή των αιτήσεων για έκδοση πιστοποιητικών
- Επιβεβαίωση της ταυτότητας αυτού που καταθέτει την αίτηση
- Επαλήθευση του κατά πόσο είναι έγκυρες οι πληροφορίες που παρέχονται από τον υποψήφιο κάτοχο και του κατά πόσο ο υποψήφιος έχει δικαίωμα να κάνει χρήση αυτών των πληροφοριών
- Επαλήθευση του ότι ο υποψήφιος πράγματι κατέχει το ιδιωτικό κλειδί, αντίστοιχο του δημοσίου κλειδιού που θα περιλαμβάνεται στο πιστοποιητικό (proof of possession)
- Αναφορά προς την ΑΠ τυχόν παραβίασης κλειδιού ή άλλων περιπτώσεων που απαιτούν την ανάκληση πιστοποιητικού
- Δημιουργία ζεύγους κλειδιών (δημόσιο/ιδιωτικό)
- Ενεργοποίηση, για λογαριασμό του υποψήφιου κατόχου, της διαδικασίας έκδοσης του πιστοποιητικού, σε επικοινωνία με την ΑΠ
- Αρχειοθέτηση των ιδιωτικών κλειδιών
- Ενεργοποίηση της διαδικασίας ανάκτησης κλειδιού
- Διανομή ειδικών συσκευών (όπως έξυπνες κάρτες) που περιέχουν τα ιδιωτικά κλειδιά.

Γενικώς η ΑΚ χειρίζεται θέματα συναλλαγών μεταξύ του υποψήφιου κατόχου και του συστήματος PKI που αφορούν τη φάση της αρχικής εγγραφής, της παράδοσης του πιστοποιητικού στον κάτοχο, καθώς και άλλες διαδικασίες σχετικές με τη διαχείριση του

κύκλου ζωής του πιστοποιητικού. Σε κάθε περίπτωση όμως, αρμόδια για την έκδοση ή την ανάκληση ενός πιστοποιητικού είναι μόνο η ΑΠ.

Οι λειτουργίες μιας ΑΚ μπορεί να είναι είτε χειροκίνητες είτε αυτοματοποιημένες (με τη βοήθεια κατάλληλου λογισμικού διασύνδεσης) ή ακόμη να έχουν και μικτή μορφή.

Το κατά πόσο θα υπάρχει ΑΚ είναι κυρίως ζήτημα επιχειρηματικών διαδικασιών, σχετικών με τη λειτουργία του συστήματος PKI. Για παράδειγμα, είναι δυνατόν να έχει εκχωρηθεί (outsourcing) σε τρίτο φορέα η ΑΠ και η λειτουργία της, αλλά η ΑΚ να λειτουργεί στις εγκαταστάσεις της επιχείρησης. Εναλλακτικά, μπορεί η έκδοση των πιστοποιητικών να γίνεται από την ίδια την επιχείρηση, αλλά οι λειτουργίες της ΑΚ να έχουν κατανεμηθεί στις συνεργαζόμενες με αυτήν εταιρίες, που κάνουν χρήση του συστήματος PKI της επιχείρησης.

Αρχή Πιστοποίησης – ΑΠ (Certification Authority – CA)

Αποτελεί την καρδιά ενός συστήματος PKI και είναι υπεύθυνη για την δημιουργία και έκδοση ψηφιακών πιστοποιητικών. Οπως έχει προαναφερθεί, τα πιστοποιητικά συσχετίζουν την ταυτότητα του κατόχου, όπως αυτή εκφράζεται μέσω του ονόματος που αναφέρεται στη σχετική αίτηση του υποψηφίου κατόχου, με το δημόσιο κλειδί που αντιστοιχεί στο ιδιωτικό που βρίσκεται στα χέρια του κατόχου. Ακόμη είναι αρμόδια για την ανανέωση ισχύος και την ανάκληση των πιστοποιητικών, όταν αυτό κριθεί αναγκαίο. Επιπλέον, η ΑΠ έχει την αρμοδιότητα της τήρησης κατάλληλων αρχείων πιστοποιητικών, τα οποία μπορεί να χρησιμοποιηθούν ακόμη και μετά την τυχόν ανάκληση ενός πιστοποιητικού, προκειμένου να εξυπηρετηθούν πιθανές απαιτήσεις, που θα προκύψουν σε μεταγενέστερο χρόνο.

Χαρακτηριστικό στοιχείο του εξοπλισμού μιας ΑΠ είναι ο λεγόμενος "certificate server", που πολλές φορές εσφαλμένα χρησιμοποιείται ως συνώνυμο της ΑΠ. Πρόκειται για έναν κεντρικό υπολογιστή (ή γενικώς υπηρεσία), εφοδιασμένο με ειδικό λογισμικό, στον οποίο φθάνουν τελικώς τα στοιχεία των υπό έκδοση πιστοποιητικών, ανεξάρτητα αν αυτά έχουν συλλεγεί με χειρόγραφες ή αυτοματοποιημένες διαδικασίες. Στη συνέχεια το δημόσιο κλειδί του υποψήφιου συνδυάζεται με τις αντίστοιχες πληροφορίες που προσδιορίζουν την ταυτότητά του και η σύνθετη δομή που προκύπτει υπογράφεται με το ιδιωτικό κλειδί της ΑΠ. Εννοείται ότι τα χαρακτηριστικά ασφαλείας που αφορούν τον υπολογιστή αυτό είναι εξαιρετικά αυξημένα.

Γενικότερα, οι διαδικασίες και τα χαρακτηριστικά λειτουργίας της ΑΠ (αλλά και της ΑΚ, εφ' όσον υπάρχει) πρέπει να ορίζονται και να περιγράφονται με σαφήνεια. Σχετικά επίσημα κείμενα που ασχολούνται με τέτοιου είδους ζητήματα είναι η "Δήλωση Διαδικασιών Πιστοποίησης (ΔΔΠ)" και η "Πολιτική Πιστοποιητικών (ΠΠ)", οι οποίες αναλύονται σε παρακάτω κεφάλαιο (Κεφ.9).

Τέλος σημειώνεται ότι είναι δυνατόν, ανάλογα με τις απαιτήσεις του κάθε περιβάλλοντος, να υπάρχουν περισσότερες από μια ΑΠ σε ένα σύστημα PKI. Στην περίπτωση αυτή, μια ΑΠ, η πρώτη, είναι αυτή που παίζει τον κύριο ρόλο και χαρακτηρίζεται ως "πρωταρχική ΑΠ (root

CA)", ενώ οι υπόλοιπες ΑΠ χαρακτηρίζονται ως "υφιστάμενες ΑΠ (subordinate CA)". Οι υφιστάμενες ΑΠ μπορεί να διαρθρώνονται σε πολλά επίπεδα και να αντιστοιχούν, για παράδειγμα, στα διάφορα τμήματα ή τις γεωγραφικές υποδιαιρέσεις μιας επιχείρησης. Κάθε υφιστάμενη ΑΠ χρειάζεται ένα ψηφιακό πιστοποιητικό, το οποίο εκδίδεται από την πρωταρχική ΑΠ (αν η υφιστάμενη ΑΠ βρίσκεται στο πρώτο επίπεδο) ή από κάποια άλλη "ανώτερη" από τη συγκεκριμένη. Επίσης, κάθε υφιστάμενη ΑΠ μπορεί με τη σειρά της να εκδίδει πιστοποιητικά είτε για τελικούς χρήστες είτε για άλλες ΑΠ, των οποίων προϊσταται. Το θέμα αυτό αφορά τις λεγόμενες "ιεραρχίες πιστοποίησης" και εξετάζεται αναλυτικότερα παρακάτω (βλ. Κεφ.7).

Το παραπάνω μοντέλο με πολλαπλά επίπεδα ΑΠ μπορεί να εξυπηρετεί διάφορες λειτουργικές ανάγκες της επιχείρησης, κυρίως όμως υιοθετείται προκειμένου να αυξηθεί ο βαθμός ασφαλείας του συστήματος συνολικά. Το ενδεχόμενο να παραβιαστεί το ιδιωτικό κλειδί μιας ΑΠ δεν είναι δυνατόν να αποκλειστεί εντελώς. Αν αυτό συμβεί σε ένα σύστημα PKI με μια μόνο ΑΠ, τότε ολόκληρο το υπ' όψη σύστημα βρίσκεται σε κίνδυνο και θα πρέπει άμεσα να αλλάξει το ιδιωτικό κλειδί της ΑΠ, πράγμα που σημαίνει ότι αχρηστεύονται αμέσως όλα τα πιστοποιητικά που είχε εκδώσει η ΑΠ.

Αντίθετα, αν τα πιστοποιητικά των χρηστών δεν εκδίδονται κατ' ευθείαν από την πρωταρχική ΑΠ, αλλά από άλλες υφιστάμενες ΑΠ, τότε είναι εφικτό η πρωταρχική ΑΠ να παραμένει στο μεγαλύτερο μέρος του χρόνου απενεργοποιημένη (άρα περισσότερο ασφαλής) και να χρησιμοποιείται μόνο όταν χρειάζεται να πιστοποιήσει μια υφιστάμενη ΑΠ. Στην περίπτωση που παραβιαστεί το ιδιωτικό κλειδί μιας υφιστάμενης ΑΠ, οι συνέπειες είναι σαφώς μικρότερες, καθώς θα αχρηστευθεί μόνο το υποσύνολο των πιστοποιητικών που αυτή είχε εκδώσει.

Αποθετήριο (Repository)

Τα πιστοποιητικά και τα αντίστοιχα δημόσια κλειδιά θα πρέπει να γίνουν ευρύτερα γνωστά (να "δημοσιευθούν"), προτού αρχίσουν να χρησιμοποιούνται. Το αποθετήριο είναι ένας μηχανισμός που επιτρέπει την αποθήκευση των πιστοποιητικών και τη δημόσια πρόσβαση σ' αυτά. Τα αποθετήρια που συνήθως χρησιμοποιούνται σε ένα σύστημα PKI έχουν τη μορφή καταλόγων (directories), οι οποίοι προσφέρουν υπηρεσίες πρόσβασης μέσω του πρωτοκόλλου LDAP, όπως περιγράφεται αναλυτικότερα στην εξέταση της λειτουργίας της διανομής πιστοποιητικών.

Μια άλλη κατηγορία πληροφοριών που επίσης είναι διαθέσιμη μέσω του αποθετηρίου είναι αυτές που αφορούν τις ανακλήσεις πιστοποιητικών και οι οποίες έχουν τη μορφή πινάκων, που είναι γνωστοί ως "πίνακες ανάκλησης πιστοποιητικών (certificate revocation lists - CRLs)". Το θέμα αυτό παρουσιάζεται διεξοδικά στα επόμενα, κατά την ανάλυση της λειτουργίας της διανομής.

4.5. Λειτουργίες ενός συστήματος PKI

Καθένα από τα παραπάνω δομικά στοιχεία, έχει το δικό του ρόλο κατά την εκτέλεση των διαφόρων λειτουργιών του συστήματος. Οι κυριότερες λειτουργίες ενός συστήματος PKI είναι οι εξής:

- Εκδοση πιστοποιητικών
- Διανομή πιστοποιητικών
- Ελεγχος εγκυρότητας πιστοποιητικών
- Ανανέωση πιστοποιητικών
- Ανάκληση πιστοποιητικών
- Δημιουργία κλειδιών
- Ενημέρωση κλειδιών
- Αρχειοθέτηση και ανάκτηση κλειδιών
- Διαπιστοποίηση (επικοινωνία με άλλες ΑΠ)

Είναι εμφανές ότι οι λειτουργίες αυτές μπορούν να διακριθούν λογικά σε δύο επιμέρους κατηγορίες:

- Διαχείριση πιστοποιητικών
- Διαχείριση κλειδιών

Για να εκδοθεί όμως ένα πιστοποιητικό πρέπει προηγουμένως να δημιουργηθεί και να είναι διαθέσιμο το αντίστοιχο ζεύγος δημόσιου/ιδιωτικού κλειδιού. Επομένως θα εξετασθούν πρώτα οι λειτουργίες που αφορούν τον κύκλο ζωής των κλειδιών και στη συνέχεια εκείνες που σχετίζονται με τον κύκλο ζωής των πιστοποιητικών.

5. ΔΙΑΧΕΙΡΙΣΗ ΚΛΕΙΔΙΩΝ – ΣΧΕΤΙΚΕΣ ΛΕΙΤΟΥΡΓΙΕΣ

Ο ρόλος των κρυπτογραφικών κλειδιών στη δημιουργία ενός ασφαλούς ηλεκτρονικού περιβάλλοντος είναι καίριας σημασίας. Επομένως οι λειτουργίες που έχουν σχέση με τη διαχείρισή τους πρέπει να είναι προσεκτικά σχεδιασμένες, ώστε να ικανοποιούν τις προϋποθέσεις για την ασφαλή και αποδοτική χρήση τους. Οι κυριότερες από τις λειτουργίες αυτές είναι η δημιουργία των κλειδιών, η διανομή τους, η αρχειοθέτηση και ανάκτηση τους, ενώ σοβαρά ζητήματα που έχουν σχέση με τις λειτουργίες αυτές είναι η φύλαξη και η προστασία των κλειδιών, καθώς και η δυνατότητα ασφαλούς μεταφοράς τους, όταν αυτό απαιτείται.

5.1. Δημιουργία κλειδιών

Το μέγεθος των κρυπτογραφικών κλειδιών έχει ιδιαίτερη βαρύτητα, δεδομένου ότι απ' αυτό εξαρτάται σε μεγάλο βαθμό η δυσκολία παραβίασής τους και συνεπώς και το επίπεδο ασφάλειας που προσφέρει η χρήση τους. Θεωρητικά οποιοδήποτε κλειδί είναι δυνατό να παραβιαστεί, εφ' όσον υπάρχει διαθέσιμη πολλή υπολογιστική ισχύς και επαρκής χρόνος. Στην πράξη βέβαια, εάν κάτι τέτοιο απαιτεί εξαιρετικά πολύ χρόνο (της τάξεως των εκατομμυρίων ετών), ο κίνδυνος είναι μηδαμινός (βλ. Κεφ. 2.2.).

Μέχρι πρόσφατα, λόγω περιορισμών που ίσχυαν στις ΗΠΑ σχετικά με την εξαγωγή κρυπτογραφικής τεχνολογίας σε άλλες χώρες, τα μεγέθη κλειδιών που ήταν διαθέσιμα δεν εξασφάλιζαν επαρκή προστασία από πιθανή παραβίαση. Οι περιορισμοί όμως αυτοί έχουν ήδη αρθεί και επομένως είναι δυνατόν να επιλεγούν μεγέθη κλειδιών απεριορίστου μεγέθους. Παρ' όλα αυτά, σε πρακτικό επίπεδο, προτείνεται η χρήση κλειδιών μήκους 1024 bits για προσωπικές χρήσεις, ενώ για περιπτώσεις όπου οι απαιτήσεις είναι υψηλότερες, (π.χ. το κρυπτογραφικό κλειδί με το οποίο μια ΑΠ υπογράφει τα πιστοποιητικά των χρηστών) συνιστάται μήκος κλειδιού 2048 bits. Ο λόγος είναι ότι η επιλογή πολύ μεγάλων κλειδιών αυξάνει υπέρμετρα το χρόνο και την υπολογιστική ισχύ που απαιτούνται για την κρυπτογραφική επεξεργασία ψηφιακών δεδομένων.

Ενα άλλο ζήτημα αφορά τον ακριβή μηχανισμό και τη μέθοδο που θα χρησιμοποιηθεί για την δημιουργία του ζεύγους ασύμμετρων κρυπτογραφικών κλειδιών (δημόσιο/ιδιωτικό), από τα οποία το δημόσιο είναι αυτό που θα περιληφθεί στο αντίστοιχο ψηφιακό πιστοποιητικό. Το ζεύγος αυτό μπορεί να δημιουργηθεί από την ΑΠ που θα εκδώσει το πιστοποιητικό (σαν ένα επιμέρους βήμα της διαδικασίας έκδοσης), είναι όμως δυνατό να έχει ήδη δημιουργηθεί εκ των προτέρων από τον ίδιο τον ενδιαφερόμενο.

Γενικά, υπάρχουν δύο προσεγγίσεις:

Κεντροποιημένο σύστημα δημιουργίας κλειδιών

Σε ένα τέτοιο σύστημα τα ζεύγη κλειδιών δημιουργούνται κεντρικά με τη βοήθεια εξειδικευμένου εξοπλισμού μεγάλης ισχύος και στη συνέχεια μεταφέρονται στο περιβάλλον του κατόχου του κλειδιών. Προσφέρεται ιδιαίτερα για τις περιπτώσεις όπου τα κλειδιά των

χρηστών αποθηκεύονται μεν σε κατάλληλες ειδικές συσκευές, οι οποίες όμως έχουν περιορισμένες δυνατότητες (π.χ. επεξεργαστική ισχύ και μνήμη), οπότε δεν μπορούν να χρησιμοποιηθούν για τη δημιουργία κλειδιών, η οποία είναι μια ιδιαίτερα απαιτητική διαδικασία. Αν δεν χρησιμοποιούνται ειδικές συσκευές, τα κλειδιά του χρήστη φυλάσσονται συνήθως στον προσωπικό του υπολογιστή (μέθοδος που παρουσιάζει σοβαρά προβλήματα από πλευράς ασφάλειας). Στην περίπτωση αυτή, υπάρχει διαθέσιμη υπολογιστική ισχύς και τα κλειδιά μπορούν να δημιουργηθούν στον υπολογιστή του χρήστη, με χρήση κατάλληλου λογισμικού (π.χ. τα προγράμματα πλοήγησης στο Internet - Web browsers έχουν ενσωματωμένες τέτοιες δυνατότητες). Παρ' όλα αυτά, ένα κεντροποιημένο σύστημα δημιουργίας κλειδιών προσφέρει, ακόμη και στην περίπτωση αυτή, πλεονεκτήματα που αφορούν κυρίως την λειτουργία της αρχειοθέτησης και ανάκτησης των κλειδιών. Η λειτουργία αυτή διευκολύνεται από την χρήση ενός κεντρικού συστήματος, δεδομένου ότι τα κλειδιά, αμέσως μετά τη δημιουργία τους, αρχειοθετούνται και είναι εύκολο να ανακτηθούν αργότερα, αν για παράδειγμα ο χρήστης χάσει κάποια στιγμή το ιδιωτικό του κλειδί ή την πρόσβαση σ' αυτό.

Κατανεμημένο σύστημα δημιουργίας κλειδιών

Η προσέγγιση αυτή προβλέπει ότι τα κλειδιά δημιουργούνται στο περιβάλλον του χρήστη, δηλαδή εκεί όπου τα κλειδιά τελικώς θα αποθηκευτούν, ενώ στη συνέχεια μόνο το δημόσιο κλειδί μεταφέρεται στην ΑΠ και συμμετέχει στην έκδοση του πιστοποιητικού. Η εφαρμογή της μεθόδου αυτής μάλιστα πιθανόν να είναι υποχρεωτική (και όχι απλώς μια δυνατότητα), όταν τα υπ' όψη κλειδιά πρόκειται να χρησιμοποιηθούν για να υποστηρίξουν εφαρμογές και υπηρεσίες μη αποκήρυξης. Στην περίπτωση αυτή, αυστηρή προϋπόθεση είναι το ιδιωτικό κλειδί να μη γίνει ποτέ γνωστό σε κανέναν άλλο, εκτός από τον ίδιο τον χρήστη. Βέβαια το σύστημα αυτό δημιουργεί προβλήματα στη λειτουργία της αρχειοθέτησης και ανάκτησης κλειδιών, όπου αυτή είναι απαραίτητη.

Εναλλακτικά είναι δυνατό να υιοθετηθεί ένα μικτό μοντέλο για τη δημιουργία των κλειδιών, που θα συνδυάζει τις ιδιότητες και των δύο, ικανοποιώντας παράλληλα τις υπάρχουσες απαιτήσεις. Το όλο θέμα έχει σχέση με τον τρόπο χρήσης κάθε ζεύγους κλειδιών (επιγραμματικά: κλειδιά που χρησιμοποιούνται για κρυπτογράφηση και κλειδιά που χρησιμοποιούνται για ψηφιακές υπογραφές) και διερευνάται διεξοδικότερα παρακάτω (βλ. "Είδη κλειδιών").

5.2. Αποθήκευση - μεταφορά - προστασία του ιδιωτικού κλειδιού

Οπως έχει προαναφερθεί, η χρήση των ψηφιακού πιστοποιητικού είναι ασφαλής, εφ' όσον το αντίστοιχο ιδιωτικό κλειδί βρίσκεται στον απόλυτο έλεγχο του κατόχου του και κανενός άλλου. Κατά συνέπεια, η προστασία του ιδιωτικού κλειδιού είναι εξαιρετικά μεγάλης σπουδαιότητας και συνδυάζεται με τα αποθηκευτικά μέσα που χρησιμοποιούνται για τη φύλαξη του ιδιωτικού κλειδιού.

Πολλές φορές το ζεύγος δημόσιου/ιδιωτικού κλειδιού φυλάσσεται σε μορφή αρχείου στο μαγνητικό δίσκο του υπολογιστή του κατόχου του. Η μεθοδος αυτή χρησιμοποιείται συνήθως από τα διάφορα προγράμματα πλοήγησης στο Internet (Web browsers), καθώς και τα προγράμματα ηλεκτρονικού ταχυδρομείου. Στην περίπτωση αυτή, θα πρέπει το αρχείο αυτό να προστατεύεται τουλάχιστον με τη χρήση κάποιου password, το οποίο να έχει επιλεγεί και να συντηρείται σύμφωνα με αυστηρές και καλά σχεδιασμένες διαδικασίες. Παρ' όλα αυτά, η χρήση των passwords σαν μοναδικής μεθόδου προστασίας παρουσιάζει πολλές αδυναμίες (σχετικές λεπτομέρειες αναφέρονται στο Κεφ. 8), δεδομένου ότι, εκτός των άλλων, πρόκειται για διαδικασία επιβεβαίωσης ταυτότητας με χρήση ενός μόνο παράγοντα (single factor authentication). Στην ακραία μάλιστα περίπτωση είναι πιθανόν ο κάτοχος του κλειδιού να αποφασίσει ότι δεν θα χρησιμοποιήσει καν password για την πρόσβαση στο υπ' όψη αρχείο, επικαλούμενος "λόγους ευκολίας". Αν ισχύει κάτι τέτοιο, τότε οποιοσδήποτε τρίτος αποκτήσει πρόσβαση στον υπολογιστή του κατόχου του κλειδιού, θα έχει τη δυνατότητα να κάνει χρήση του ιδιωτικού κλειδιού, σαν να επρόκειτο για τον ίδιο τον κάτοχο.
Είναι επόμενο ότι ένα περιβάλλον που η αποθήκευση και προστασία των κλειδιών γίνεται με τον παραπάνω τρόπο δεν μπορεί να παράσχει υψηλό επίπεδο ασφάλειας.

Ενα πρόσθετο ζήτημα σχετικά με την αποθήκευση κλειδιών με την πιο πάνω μέθοδο, αφορά τη δυνατότητα χρήσης του ίδιου ιδιωτικού κλειδιού από διαφορετικά προϊόντα και εφαρμογές λογισμικού. Αν και υπάρχουν σχετικά πρότυπα, οι διάφοροι κατασκευαστές λογισμικού χρησιμοποιούν συνήθως ο καθένας τις δικές του μεθόδους και παραδοχές για τον τρόπο και τη μορφή αποθήκευσης των κλειδιών. Το αποτέλεσμα είναι να υπάρχει σοβαρή δυσκολία στην κοινή χρήση των κλειδιών από διαφορετικές εφαρμογές. Βέβαια έχει αναπτυχθεί ένα σχετικό πρότυπο (PKCS #12), το οποίο επιτρέπει την "εξαγωγή" (export) ενός κλειδιού με τρόπο που αυτό να είναι στη συνέχεια αναγνωρίσιμο από άλλες εφαρμογές. Ετσι, όταν ένα κλειδί που ήδη χρησιμοποιείται από μια εφαρμογή Α απαιτείται να χρησιμοποιηθεί και από μια δεύτερη εφαρμογή Β, το αρχείο που περιέχει το κλειδί αντιγράφεται σε ένα νέο "ενδιάμεσο" αρχείο, με διαφορετική όμως μορφή απ' ότι το αρχικό. Στη συνέχεια το νέο αυτό αρχείο θα πρέπει να "εισαχθεί" (import) στην εφαρμογή Β, προκειμένου αυτή να μπορεί να κάνει χρήση του υπ' όψη κλειδιού.

Μια τέτοια διαδικασία δεν είναι ιδιαίτερα εύχρηστη και φιλική για τον τυπικό χρήστη, με αποτέλεσμα η αποδοχή της να είναι περιορισμένη. Επιπλέον, παρουσιάζει πρόσθετα προβλήματα ασφάλειας, δεδομένου ότι τα "ενδιάμεσα" αρχεία που δημιουργούνται περιέχουν το ιδιωτικό κλειδί και θα πρέπει να διαγράφονται με σχολαστικότητα.

Παρά τις αδυναμίες της, η παραπάνω μέθοδος προσφέρει μια λύση στο πρόβλημα της μεταφοράς των κλειδιών. Για παράδειγμα, ανάγκη για μεταφορά του ιδιωτικού κλειδιού υπάρχει στην περίπτωση που ένας χρήστης πρέπει να εργαστεί σε κάποιο υπολογιστή διαφορετικό από το δικό του (δηλ. σε ένα διαφορετικό σταθμό εργασίας στο χώρο της επιχείρησης ή πιθανόν στον υπολογιστή του σπιτιού του). Στην περίπτωση αυτή, μια λύση είναι η διαδικασία της "εξαγωγής/εισαγωγής", όπως περιγράφηκε πιο πάνω.

Αν οι απαιτήσεις ασφαλείας του περιβάλλοντος είναι υψηλές, το ιδιωτικό κλειδί θα πρέπει να φυλάσσεται σε κάποια ειδική συσκευή, όπως είναι οι λεγόμενες "έξυπνες κάρτες", οι οποίες

υλοποιούν μέθοδο επιβεβαίωσης ταυτότητας δύο παραγόντων (two factor authentication), όπως περιγράφεται αναλυτικά στο Κεφ. 8. Οι έξυπνες κάρτες, μεταξύ άλλων, έχουν τη δυνατότητα να δημιουργούν και να αποθηκεύουν εσωτερικά το απαιτούμενο ζεύγος κλειδιών. Επομένως, το μόνο που χρειάζεται είναι να μεταφερθεί προς τα έξω το δημόσιο κλειδί, ώστε η ΑΠ να το χρησιμοποιήσει για την έκδοση του αντίστοιχου πιστοποιητικού, ενώ το ιδιωτικό κλειδί δεν αποθηκεύεται πουθενά αλλού, πέρα από το χώρο όπου αρχικά δημιουργήθηκε. Επιπλέον, επειδή οι έξυπνες κάρτες μεταφέρονται εύκολα, μπορούν να χρησιμοποιηθούν για την πρόσβαση στο ιδιωτικό κλειδί, ανεξάρτητα από το χώρο που βρίσκεται κάθε φορά ο ιδιοκτήτης του. Το μειονέκτημα βέβαια των έξυπνων καρτών είναι ότι απαιτούν πρόσθετο ειδικό εξοπλισμό, προκειμένου να χρησιμοποιηθούν.

5.3. Είδη κλειδιών

Ενα κρυπτογραφικό κλειδί (δηλ. ένα ζεύγος κλειδιών "δημόσιο/ιδιωτικό") μπορεί να χρησιμοποιηθεί είτε για την κρυπτογράφηση/αποκρυπτογράφηση ηλεκτρονικών εγγράφων είτε για τη δημιουργία ψηφιακών υπογραφών (πιθανόν και για τα δύο, ανάλογα με τον κρυπτογραφικό αλγόριθμο). Υπάρχουν όμως αντικρουόμενες απαιτήσεις χρήσης και ασφάλειας, ανάλογα με τη χρήση του κάθε κλειδιού. Συγκεκριμένα:

1. Ενα ιδιωτικό κλειδί ψηφιακών υπογραφών πρέπει να φυλάσσεται με τρόπο ώστε μόνο ο κάτοχός του να έχει πρόσβαση σ' αυτό. Η προϋπόθεση αυτή είναι απαραίτητη, προκειμένου να υποστηριχθεί η μη αποκήρυξη. Συνιστάται επομένως (και πολλές φορές είναι υποχρεωτικό) το ιδιωτικό κλειδί ψηφιακών υπογραφών να μην "εγκαταλείπει" ποτέ την συσκευή (έξυπνη κάρτα) στην οποία αρχικά δημιουργήθηκε.

2. Δεν είναι απαραίτητο να δημιουργείται αντίγραφο ασφαλείας (back-up) ενός ιδιωτικού κλειδιού ψηφιακών υπογραφών, με σκοπό να αντιμετωπιστεί το ενδεχόμενο απώλειάς του. Αν το κλειδί χαθεί, ένα νέο ζευγος κλειδιών μπορεί εύκολα να δημιουργηθεί. Αλλωστε, η δημιουργία αντιγράφου παραβαίνει την πιο πάνω απαίτηση 1. Εξάλλου, η επαλήθευση υπογραφής μπορεί να συνεχιστεί για έγγραφα που είχαν υπογραφεί με το χαμένο ιδιωτικό κλειδί, δεδομένου ότι το αντίστοιχο δημόσιο κλειδί και το σχετικό ψηφιακό πιστοποιητικό είναι ακόμη διαθέσιμα.

3. Για ένα ιδιωτικό κλειδί κρυπτογράφησης πιθανόν να πρέπει να λαμβάνεται αντίγραφο ασφαλείας (back-up). Το αντίγραφο αυτό θα χρησιμοποιηθεί για να επιτρέψει την πρόσβαση σε κρυπτογραφημένες πληροφορίες, στην περίπτωση απώλειας του κλειδιού. Διαφορετικά, η απώλεια του κλειδιού συνεπάγεται ουσιαστικά και την απώλεια κάθε πληροφορίας που είχε κρυπτογραφηθεί με αυτό, πράγμα απαράδεκτο.

Ειναι προφανές ότι οι απαιτήσεις 1. και 2. έρχονται σε σύγκρουση με την απαίτηση 3. Αν λοιπόν κάποιος χρησιμοποιεί το ίδιο ζεύγος κλειδιών και για ψηφιακές υπογραφές και για κρυπτογράφηση, είναι αδύνατο να ικανοποιηθούν όλες οι απαιτήσεις.

Το πρόβλημα μπορεί να λυθεί με τη χρησιμοποίηση δύο διαφορετικών ζευγών κλειδιών: **Το ένα από αυτά θα αφορά ψηφιακές υπογραφές και το άλλο διαδικασίες κρυπτογράφησης / αποκρυπτογράφησης**. Εννοείται βέβαια ότι θα πρέπει να εκδοθούν και τα αντίστοιχα ψηφιακά πιστοποιητικά.

5.4. Αρχειοθέτηση και ανάκτηση κλειδιών

Η δημιουργία αντιγράφων ασφαλείας (back-up) για τα κρυπτογραφικά κλειδιά κατά κανόνα επιβάλλεται από την ανάγκη να μπορούν αυτά να χρησιμοποιηθούν ακόμη και σε περίπτωση απώλειάς τους. Για παράδειγμα, ένας χρήστης μπορεί να χάσει το κλειδί του ή να πέσει θύμα ατυχήματος ή να εγκαταλείψει για κάποιο λόγο την επιχείρηση κλπ. Κατά συνέπεια, είναι απαραίτητο να υπάρχει ένα σύστημα, στο οποίο θα αποθηκεύονται με ασφάλεια τα αντίγραφα των κλειδιών, συνήθως αμέσως μετά τη δημιουργία τους. Αν υπάρχει ήδη ένα σύστημα κεντρικής δημιουργίας κλειδιών, αυτό θα πρέπει να επικοινωνεί με το σύστημα αρχειοθέτησης, διαφορετικά θα πρέπει να σχεδιαστεί μια ασφαλής διαδικασία, η οποία θα μεταφέρει τα κλειδιά στο σύστημα αρχειοθέτησης, μόλις αυτά δημιουργηθούν στο περιβάλλον του χρήστη. Εννοείται ότι το σύστημα αρχειοθέτησης θα διαθέτει αυξημένα χαρακτηριστικά ασφαλείας, ενώ η πρόσβαση σ' αυτό θα είναι αυστηρά ελεγχόμενη και θα απαιτεί την ταυτόχρονη παρουσία και συμμετοχή περισσότερων του ενός ατόμων.
Τέλος, αν η διαδικασία ανάκτησης είναι σχεδιασμένη έτσι ώστε να απαιτεί και την ταυτόχρονη ανάκτηση του αντίστοιχου ψηφιακού πιστοποιητικού, τότε θα πρέπει να αρχειοθετείται και αυτό.

Η ανάκτηση, όπως και η αρχειοθέτηση, αφορά κυρίως τα κλειδιά κρυπτογράφησης και όχι τα κλειδιά ψηφιακών υπογραφών, για τους λόγους που αναλύθηκαν πιο πάνω. Η ανάκτηση κατά κανόνα έχει σχέση με την επαναφορά σε χρήση του τρέχοντος κλειδιού, δηλαδή αυτό που τώρα χρησιμοποιεί ο χρήστης και το οποίο έχει πιθανόν χαθεί ή καταστραφεί. Στην περίπτωση αυτή, η ανάκτηση είναι απαραίτητη, προκειμένου να είναι διαθέσιμα τα έγγραφα των οποίων η κρυπτογράφηση είχε στηριχθεί στο χαμένο κλειδί.

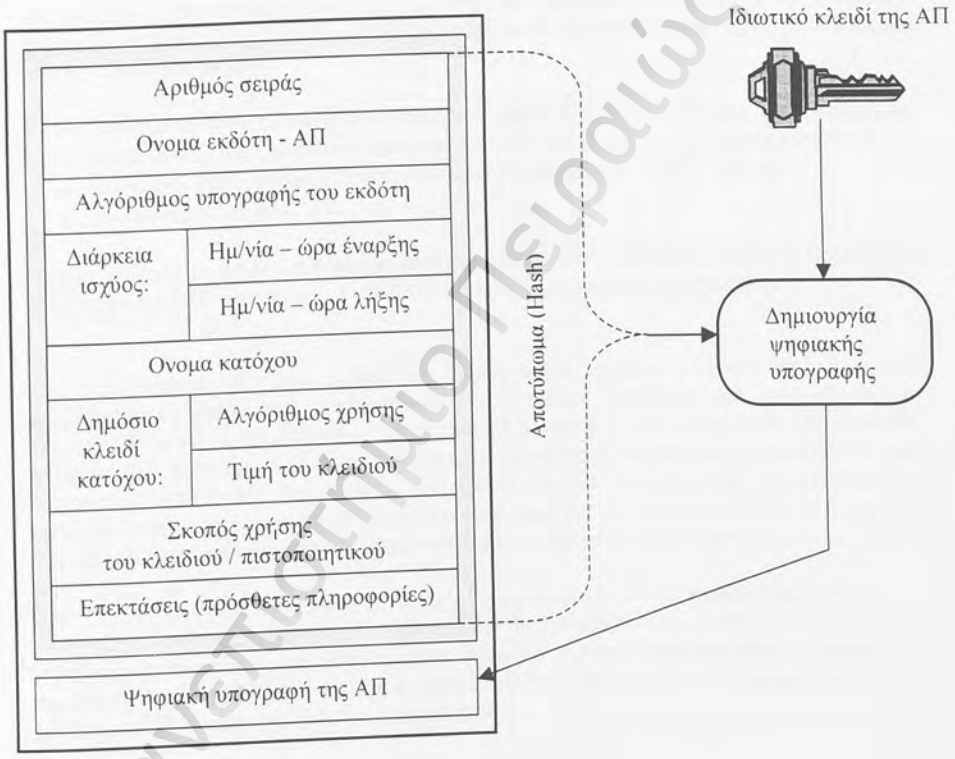
Ομως η διάρκεια ζωής των κλειδιών δεν είναι απεριόριστη και αυτό αποτελεί μέτρο προστασίας, δεδομένου ότι όσο περισσότερο χρησιμοποιείται το ίδιο κλειδί, τόσο αυξάνεται ο κίνδυνος παραβίασής του από τρίτους. Το αποτέλεσμα είναι ότι μπορεί ένας χρήστης να χρειαστεί το κλειδί που είχε πριν από κάποιο διάστημα, για παράδειγμα για να διαβάσει ένα κρυπτογραφημένο έγγραφο ηλεκτρονικού ταχυδρομείου που είχε λάβει παλαιότερα. Στην περίπτωση αυτή, θα χρειαστεί η ανάκτηση του λεγόμενου "προηγούμενου κλειδιού", η αποία πιθανόν να απαιτήσει την εμπλοκή αντίστοιχου εξειδικευμένου ατόμου. Γενικά τα συστήματα ανάκτησης συνεπάγονται μεγάλες απαιτήσεις σε πολύ καλά εκπαιδευμένο και έμπιστο προσωπικό, με αποτέλεσμα η αποδοχή τους να είναι συζητήσιμη.

6. ΔΙΑΧΕΙΡΙΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ – ΣΧΕΤΙΚΕΣ ΛΕΙΤΟΥΡΓΙΕΣ

6.1. Δομή ψηφιακού πιστοποιητικού

Ενα ψηφιακό πιστοποιητικό είναι μια σύνθεση ψηφιακών δεδομένων, τα οποία αφορούν αφ' ενός το δημόσιο κλειδί του υποψήφιου κατόχου και αφ' ετέρου ορισμένες πληροφορίες που προσδιορίζουν την ταυτότητα του κατόχου του. Η ψηφιακή αυτή δομή υπογράφεται με το ιδιωτικό κλειδί της εκδίδουσας Αρχής Πιστοποίησης (ΑΠ), ώστε να καταστεί αυτοπροστατευόμενη, με την έννοια ότι δεν είναι δυνατόν να αλλοιωθεί κατά οποιονδήποτε τρόπο, χωρίς αυτό να γίνει αντιληπτό. Η ακριβής μορφή ενός ψηφιακού πιστοποιητικού καθορίζεται από συγκεκριμένο πρότυπο, το οποίο κατά κανόνα είναι το X.509 (ITU X.509). Η γενική δομή ενός πιστοποιητικού παριστάνεται στο Σχήμα 10 και περιγράφεται αναλυτικά παρακάτω. Συγκεκριμένα, τα πεδία που περιλαμβάνονται είναι:

Αριθμός σειράς (serial number)
Ο αριθμός αυτός προσδιορίζει με μοναδικό τρόπο το πιστοποιητικό, ώστε αυτό να μπορεί να διακριθεί σε σχέση με κάποιο άλλο πιστοποιητικό που πιθανόν περιέχει τις ίδιες ακριβώς πληροφορίες
Ονομα εκδότη-ΑΠ (issuer name)
Προσδιορίζει την έμπιστη οντότητα (Αρχή Πιστοποίησης) που δημιουργεί και εκδίδει το πιστοποιητικό.
Αλγόριθμος υπογραφής του εκδότη (issuer's signature algorithm)
Αναφέρει τον αλγόριθμο ψηφιακής υπογραφής που χρησιμοποιεί ο εκδότης για να υπογράψει το πιστοποιητικό.
Διάρκεια ισχύος (validity period)
Δεδομένου ότι τα πιστοποιητικά δεν ισχύουν για απεριόριστο χρόνο (για λόγους ασφαλείας), η πληροφορία αυτή καθορίζει την ακριβή ημερομηνία και ώρα έναρξης και λήξης της ισχύος του πιστοποιητικού.
Ονομα κατόχου (subject's name)
Αναφέρει το όνομα του κατόχου (προσώπου ή οντότητας) του ιδιωτικού κλειδιού, για τον οποίο εκδίδεται το πιστοποιητικό.
Δημόσιο κλειδί κατόχου (subject's public key)
Εδώ περιλαμβάνεται το δημόσιο κλειδί που αντιστοιχεί στο ιδιωτικό κλειδί του κατόχου του πιστοποιητικού, καθώς και ο αλγόριθμος με τον οποίο αυτό χρησιμοποιείται.
Σκοπός χρήσης (key/certificate usage)
Αναφέρει τις χρήσεις για τις οποίες θα χρησιμοποιηθεί το πιστοποιητικό και το αντίστοιχο κλειδί, όπως για ψηφιακές υπογραφές εγγράφων, ψηφιακές υπογραφές πιστοποιητικών, κρυπτογράφηση δεδομένων κλπ.
Επεκτάσεις (extensions)
Εδώ μπορούν να περιληφθούν πρόσθετες πληροφορίες που πιθανόν απαιτούνται. Μια επέκταση αποτελείται από τρία πεδία (είδος, ένδειξη κρισιμότητας, τιμή) και μπορεί να αναφέρεται σε θέματα σχετικά με την ακολουθούμενη πολιτική πιστοποιητικών, τον έλεγχο εγκυρότητας του πιστοποιητικού, ειδικότερες απαιτήσεις σε ό,τι αφορά τη λειτουργία της ανάκλησης κλπ.



Σχήμα 10. **Δομή ενός ψηφιακού πιστοποιητικού**

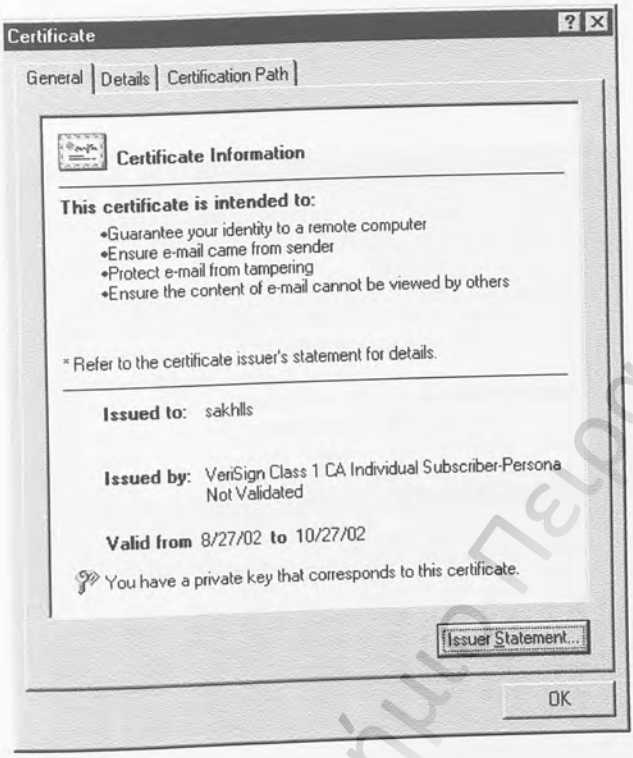
Ειδικότερα σε ότι αφορά την μορφή που πρέπει να έχουν τα ονόματα (εκδότη, κατόχου) που περιλαμβάνονται στο πιστοποιητικό, οι παλαιότερες εκδόσεις του προτύπου X.509 απαιτούσαν συμμόρφωση με τις προδιαγραφές του προτύπου X.500, το οποίο έχει σχέση με πληροφορίες καταλόγου. Σύμφωνα με αυτές, ένα "διακεκριμένο όνομα" (distinguished name), όπως λέγεται, περιλαμβάνει στοιχεία όπως χώρα, οργανισμό, ονοματεπώνυμο, θέση που κατέχει το άτομο κλπ. Η τρίτη όμως έκδοση του προτύπου X.509 (X.509 v3) προσφέρει περισσότερες δυνατότητες και αναγνωρίζει ονόματα που μπορεί να έχουν, μεταξύ άλλων, μια από τις παρακάτω μορφές:

- Διεύθυνση ηλεκτρονικού ταχυδρομείου (Internet E-mail address), π.χ. saradis@bog.gr
- Δικτυακό όνομα στο Internet (Internet domain name), π.χ. www.mycompany.com
- Δικτυακή διεύθυνση στο Internet (Internet IP address), π.χ. 194.123.3.101
- Ονομα τύπου X.500 κλπ

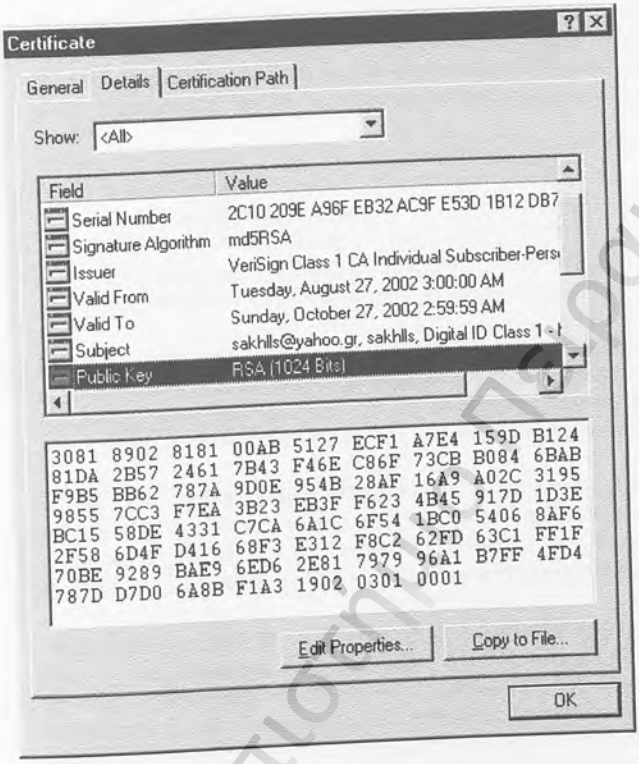
Η μόνη κρίσιμη απαίτηση που υπάρχει είναι το όνομα να προσδιορίζει μοναδικά την υπ' όψη οντότητα μέσα στο συγκεκριμένο περιβάλλον που αυτή υφίσταται και λειτουργεί.

Στο σημείο αυτό και προκειμένου να καταστεί πιο σαφής η έννοια του ψηφιακού πιστοποιητικού, καθώς και η απεικόνιση και ο τρόπος χειρισμού του, παρατίθενται οι επόμενες δύο εικόνες (βλ. Σχήμα 11 και Σχήμα 12 παρακάτω). Οι εικόνες αυτές αφορούν ένα συγκεκριμένο πιστοποιητικό κάποιου χρήστη, το οποίο έχει αποθηκευτεί στο περιβάλλον ενός προσωπικού υπολογιστή, έτσι ώστε να είναι προσβάσιμο από το πρόγραμμα πλοήγησης (Web browser) Internet Explorer. Οι δύο αυτές εικόνες μπορούν να συσχετισθούν με το Σχήμα 10 (πιο πάνω), προκειμένου να κατανοηθεί καλύτερα η έννοια του πιστοποιητικού.

Στο Σχήμα 11 παρουσιάζονται οι γενικές πληροφορίες του πιστοποιητικού, όπου και φαίνονται ο σκοπός χρήσης ("This certificate is intended to:"), καθώς και συνοπτικές ενδείξεις για τον κάτοχο, τον εκδότη και τη διάρκεια ισχύος. Λεπτομερέστερες πληροφορίες περιλαμβάνονται στο Σχήμα 12, όπου, μεταξύ άλλων, φαίνεται και το δημόσιο κλειδί του χρήστη που περιέχεται στο υπ' όψη πιστοποιητικό.



Σχήμα 11. Απεικόνιση πιστοποιητικού σε περιβάλλον Internet Explorer – Γενικές πληροφορίες



Σχήμα 12. **Απεικόνιση πιστοποιητικού σε περιβάλλον Internet Explorer – Λεπτομέρειες**

6.2. Είδη ψηφιακών πιστοποιητικών

Ενα ψηφιακό πιστοποιητικό προσδιορίζει την ταυτότητα μιας συγκεκριμένης οντότητας, προκειμένου αυτή να μπορεί να επικοινωνήσει με ασφαλή τρόπο με άλλες οντότητες. Συνήθως η οντότητα αυτή είναι ένα συγκεκριμένο πρόσωπο, υπάρχουν όμως και ορισμένες άλλες περιπτώσεις. Γενικά, το υποκείμενο (δηλ. ο κάτοχος) ενός πιστοποιητικού μπορεί να είναι:

- Ενα πρόσωπο
- Ενας οργανισμός ή επιχείρηση
- Μια Αρχή Πιστοποίησης
- Ενα στοιχείο εξοπλισμού, όπως ένας υπολογιστής (π.χ. Web server), μια συσκευή επικοινωνίας (π.χ. δρομολογητής-router)

Μια επιχείρηση που συμμετέχει σε αυτοματοποιημένες διαδικασίες ηλεκτρονικού εμπορίου μέσω Internet πρέπει να μπορεί να παρέχει στους συναλλασσόμενους με αυτήν διαβεβαιώσεις σχετικά με την ταυτότητα της και τις δεσμεύσεις που αναλαμβάνει. Για το σκοπό αυτό χρειάζεται (ως οντότητα) το αντίστοιχο ψηφιακό πιστοποιητικό.

Επίσης, ένας ασφαλής Web server (έστω Α) πρέπει να διαθέτει ψηφιακό πιστοποιητικό, προκειμένου οι χρήστες που τον επισκέπτονται να μπορούν να είναι βέβαιοι ότι επικοινωνούν με το σωστό σημείο και όχι με κάποιον τρίτο, π.χ. τον Β, που προσποιείται ότι είναι ο Α, έχοντας χρησιμοποιήσει ειδικές τεχνικές παραπλάνησης (DNS spoofing).

Τέλος, πιστοποιητικό χρειάζεται και η ίδια η Αρχή Πιστοποίησης. Η ΑΠ υπογράφει η ίδια το δικό της πιστοποιητικό, αν είναι η μόνη ΑΠ που υπάρχει σε ένα σύστημα PKI. Είναι όμως δυνατόν να υπάρχουν και άλλες ΑΠ (υφιστάμενες της πρώτης). Στην περίπτωση αυτή το πιστοποιητικό μιας υφιστάμενης ΑΠ υπογράφεται από την πρωταρχική ΑΠ ή γενικώς από κάποια προϊστάμενη ΑΠ (βλ. και Κεφ.7 - ιεραρχίες πιστοποίησης). Εξάλλου υπάρχει το ενδεχόμενο δύο διαφορετικά συστήματα PKI να επικοινωνήσουν μεταξύ τους. Τότε η ΑΠ του ενός συστήματος υπογράφει το πιστοποιητικό της ΑΠ του άλλου (δια-πιστοποίηση - cross certification).

6.3. Κατηγορίες πιστοποιητικών και επίπεδα διαβεβαιώσεων

Κάθε πιστοποιητικό εκδίδεται με σκοπό να εξυπηρετήσει καθορισμένες χρήσεις και να παράσχει ένα επίπεδο διαβεβαιώσεων στους πιθανούς χρήστες του (αυτούς που προτίθενται να στηριχθούν στις πληροφορίες που περιέχει), στα πλαίσια συγκεκριμένων πολιτικών που ακολουθεί η ΑΠ. Οι διαβεβαιώσεις αυτές εξαρτώνται από τους εξής παράγοντες:

- από το πόσο αυστηρή και διεξοδική είναι η διαδικασία που εφαρμόζει η ΑΠ κατά την φάση της εξακρίβωσης των στοιχείων ταυτότητας του κατόχου του πιστοποιητικού.
- από τα μέτρα προστασίας του ιδιωτικού κλειδιού του κατόχου του πιστοποιητικού

- από τις λειτουργικές και διοικητικές απαιτήσεις που διέπουν τη λειτουργία της ΑΠ

Ανάλογα με τα παραπάνω, μια ΑΠ μπορεί να εκδίδει πιστοποιητικά τα οποία να είναι διαβαθμισμένα σε κατηγορίες-κλάσεις **(certificate classes)**, με βάση μια αριθμητική κατάταξη, όπου η υψηλότερη γενικώς κατηγορία αντιστοιχεί σε μεγαλύτερα επίπεδα ασφάλειας. Για παράδειγμα, είναι δυνατόν να υπάρχουν τρείς κατηγορίες πιστοποιητικών, με τα εξής χαρακτηριστικά η κάθε μια:

- 1η κατηγορία: Προσωπικά πιστοποιητικά, τα οποία δεν προϋποθέτουν ιδιαίτερες διαδικασίες εξακρίβωσης των στοιχείων ταυτότητας του κατόχου και μπορούν να χρησιμοποιηθούν σε μη εμπορικές συναλλαγές ή συναλλαγές χαμηλής αξίας όπου δεν απαιτείται απόδειξη της ταυτότητας.

- 2η κατηγορία: Πιστοποιητικά που αντιστοιχούν σε μεσαίου επιπέδου διαβεβαιώσεις και κατά την έκδοσή τους τα στοιχεία ταυτότητας που περιλαμβάνονται στη αίτηση του υποψηφίου διασταυρώνονται με κάποιες επίσημες πηγές σχετικών πληροφοριών. Μπορούν να χρησιμοποιηθούν για κρυπτογράφηση και δημιουργία ψηφιακών υπογραφών, όπως σε περιπτώσεις εμπορικών συναλλαγών μέσης αξίας που απαιτούν απόδειξη ταυτότητας.

- 3η κατηγορία: Πιστοποιητικά που παρέχουν το υψηλότερο επίπεδο διαβεβαιώσεων και για τα οποία η διαδικασία έκδοσής τους απαιτεί προσωπική φυσική παρουσία του ενδιαφερόμενου και προσκόμιση συγκεκριμένων επίσημων εγγράφων, αποδεικτικών της ταυτότητας του υποψηφίου. Τα στοιχεία ταυτότητας του υποψηφίου ελέγχονται διεξοδικά. Τα πιστοποιητικά αυτά αφορούν συνήθως οργανισμούς ή επιχειρήσεις και μπορούν να χρησιμοποιηθούν για έλεγχο πρόσβασης, δημιουργία ψηφιακών υπογραφών και κρυπτογράφηση, ακόμη και σε εμπορικές συναλλαγές υψηλής αξίας που απαιτούν απόδειξη ταυτότητας.

6.4. Εκδοση πιστοποιητικών (certificate issuance)

Η διαδικασία της έκδοσης ενός ψηφιακού πιστοποιητικού περιλαμβάνει τα ακόλουθα βήματα:

1. Η Αρχή Πιστοποίησης - ΑΠ παραλαμβάνει από τον υποψήφιο μια σχετική αίτηση, στην οποία περιέχονται οι πληροφορίες που πρόκειται να περιληφθούν στο πιστοποιητικό.
2. Η ΑΠ επιβεβαιώνει την ακρίβεια των στοιχείων που κατέθεσε ο υποψήφιος, σύμφωνα και με τις πολιτικές και τα πρότυπα που ακολουθεί.
3. Το πιστοποιητικό υπογράφεται ψηφιακά με το ιδιωτικό κλειδί της ΑΠ, με χρήση κατάλληλου εξοπλισμού (π.χ. certificate server)
4. Ενα αντίγραφο του πιστοποιητικού αποστέλλεται στον κάτοχό του, ενώ μπορεί να ζητηθεί από τον κάτοχο η ρητή επιβεβαίωση της αποδοχής του πιστοποιητικού.
5. Ενα αντίγραφο του πιστοποιητικού υποβάλλεται συνήθως στο σχετικό αποθετήριο πιστοποιητικών για δημοσίευση.

6. Προαιρετικά, ένα αντίγραφο του πιστοποιητικού μπορεί να αρχειοθετηθεί από μια ΑΠ ή άλλη οντότητα, για να χρησιμοποιηθεί σαν αποδεικτικό στοιχείο σε περιπτώσεις π.χ. μη αποκήρυξης.
7. Η ΑΠ καταγράφει τις λεπτομέρειες της διαδικασίας έκδοσης σε κατάλληλα αρχεία.

Αν υπάρχει Αρχή Καταχώρησης, ορισμένα από τα παραπάνω βήματα (π.χ. 1., 2., 4.) θα διεκπεραιωθούν από αυτήν.

Ανάλογα με τον τρόπο οργάνωσης των διαδικασιών της ΑΠ και τις πολιτικές που αυτή ακολουθεί, η κατάθεση της αίτησης από τον υποψήφιο μπορεί να διεξαχθεί εξ ολοκλήρου ηλεκτρονικά (π.χ. με τη χρήση μιας ηλεκτρονικής φόρμας και την υποστήριξη ενός Web server) ή να απαιτεί την φυσική παρουσία του υποψήφιου στα γραφεία της ΑΠ.

Ιδιαίτερης σπουδαιότητας είναι η διαδικασία που εφαρμόζει η ΑΠ (ή η αντίστοιχη ΑΚ) για την επιβεβαίωση των στοιχείων ταυτότητας του υποψήφιου. Η έκταση και το βάθος που μπορεί να έχει η διαδικασία αυτή εξαρτάται από το επίπεδο διαβεβαιώσεων που παρέχει το υπό έκδοση πιστοποιητικό.

Για την εξακρίβωση της ταυτότητας χρησιμοποιούνται συνήθως μια ή περισσότερες από τις παρακάτω τεχνικές και μεθόδους:

Επίδειξη γνώσης εμπιστευτικών πληροφοριών προσωπικού χαρακτήρα:
Ο υποψήφιος δέχεται μια σειρά ερωτήσεων που θα μπορούσαν να απαντηθούν μόνο από αυτόν. Στη συνέχεια οι απαντήσεις συγκρίνονται με δεδομένα που είναι ήδη γνωστά στην ΑΠ με κάποιο τρόπο και εφ' όσον είναι ορθές, αυτό θεωρείται ότι επιβεβαιώνει την ταυτότητά του. Για παράδειγμα, οι ερωτήσεις μπορεί να αφορούν ένα αριθμό λογαριασμού ή ένα password ή PIN ή το πατρικό επώνυμο της μητέρας του υποψήφιου ή τέλος την ημερομηνία της τελευταίας συναλλαγής ενός συγκεκριμένου λογαριασμού.

Προσωπική παρουσία:
Η φυσική παρουσία του υποψήφιου αναγνωρίζεται ευρέως ως ισχυρό μέσο για την απόδειξη της ταυτότητάς του, διότι επιτρέπει στην ΑΠ να βεβαιωθεί για την ύπαρξη και τα ιδιαίτερα χαρακτηριστικά του, αλλά και να εκτιμήσει την πρόθεσή του να καταθέσει τη σχετική αίτηση και την ικανότητά του να συμμορφωθεί με τις ακολουθούμενες πολιτικές και διαδικασίες. Για παράδειγμα, είναι δυνατόν να αξιολογηθεί κατά πόσο ένα άτομο είναι ή όχι ενήλικο, είναι μειωμένων ικανοτήτων ή ότι καταλαβαίνει την γλώσσα και αντιλαμβάνεται τις απαιτήσεις και τις υποχρεώσεις που συνεπάγεται η αίτηση.

Έγγραφα που αποδεικνύουν την ταυτότητα:
Τέτοιου είδους έγγραφα, όπως η εθνική (αστυνομική) ταυτότητα, το διαβατήριο, η άδεια οδήγησης κλπ, μπορούν να χρησιμοποιηθούν από την ΑΠ, σε συνδυασμό με την αντίστοιχη φυσική παρουσία για να επιβεβαιώσουν την ταυτότητα του υποψηφίου. Η χρήση ενός ή και περισσοτέρων παρόμοιων εγγράφων, ιδίως όσων φέρουν και σχετική φωτογραφία, είναι ευρέως αποδεκτή ως αξιόπιστη.

Απόδειξη κατοχής του ιδιωτικού κλειδιού (proof of possession)

Επιπλέον των ανωτέρω, ο υποψήφιος θα πρέπει να αποδείξει ότι πράγματι κατέχει το ιδιωτικό κλειδί που αντιστοιχεί στό δημόσιο που πρόκειται να συμπεριληφθεί στο υπό έκδοση πιστοποιητικό.
Στην περίπτωση που το υπ' όψη κλειδί πρόκειται να χρησιμοποιηθεί για δημιουργία ψηφιακών υπογραφών, τότε συνήθως ο υποψήφιος υπογράφει με αυτό την αίτηση και η ΑΠ ελέγχει την υπογραφή του χρησιμοποιώντας το δημόσιο κλειδί που έχει συνυποβληθεί με την αίτηση. Αν πάλι πρόκειται για κλειδί κρυπτογράφησης, τότε η ΑΠ δημιουργεί μια τυχαία τιμή-"πρόκληση" (challenge value), την οποία κρυπτογραφεί με το δημόσιο κλειδί του υποψηφίου. Αν ο υποψήφιος είναι σε θέση να αποκρυπτογραφήσει την "πρόκληση", αυτό αποδεικνύει ότι πράγματι κατέχει το αντίστοιχο ιδιωτικό κλειδί.

6.5. Ανανέωση πιστοποιητικών (certificate renewal)

Οπως είναι γνωστό, η διάρκεια ισχύος ενός πιστοποιητικού είναι περιορισμένη. Οταν αυτή λήξει, θα πρέπει το πιστοποιητικό να αντικατασταθεί. Ενας άλλος λόγος ανανέωσης του πιστοποιητικού μπορεί να είναι η λήξη της ισχύος του σχετικού ζεύγους κλειδιών (δημόσιο/ιδιωτικό), ακόμη και όταν η διάρκεια ισχύος του ίδιου του πιστοποιητικού δεν έχει ακόμη εξαντληθεί.

Δεδομένου ότι έχει ήδη προηγηθεί η αρχική διαδικασία έκδοσης πιστοποιητικού για τον ενδιαφερόμενο (με όλους τους σχετικούς ελέγχους που αυτή περιλαμβάνει), η διαδικασία ανανέωσης είναι συνήθως απλούστερη, μπορεί μάλιστα σε ορισμένες περιπτώσεις να αυτοματοποιηθεί (αυτό φυσικά ισχύει εφ' όσον δεν έχει συμβεί παραβίαση του σχετικού ιδιωτικού κλειδιού). Για παράδειγμα, είναι δυνατόν η ΑΠ να ζητεί την προσωπική παρουσία του κατόχου μόνο για κάθε τρίτη ανανέωση του πιστοποιητικού, απλώς σαν ένα επιπλέον έλεγχο, ενώ για τις υπόλοιπες ο κάτοχος κάνει χρήση του κλειδιού του προηγούμενου πιστοποιητικού, προκειμένου να υπογράψει την αίτηση ανανέωσης.

6.6. Διανομή πιστοποιητικών (certificate distribution)

Οι υπηρεσίες ασφάλειας που στηρίζονται στην κρυπτογραφία δημοσίου κλειδιού απαιτούν πρόσβαση στο ψηφιακό πιστοποιητικό το οποίο συνδέει την ταυτότητα του κατόχου με το ζεύγος κλειδιών (δημόσιο/ιδιωτικό) που αυτός κατέχει. Συγκεκριμένα, προκειμένου ένας χρήστης να επαληθεύσει την ψηφιακή υπογραφή μιας άλλης οντότητας με την οποία επικοινωνεί ή να κρυπτογραφήσει δεδομένα που αυτή θα παραλάβει και θα αποκρυπτογραφήσει, πρέπει να γνωρίζει το δημόσιο κλειδί αυτής της οντότητας, το οποίο περιέχεται στο αντίστοιχο πιστοποιητικό.

Ορισμένες φορές είναι δυνατόν η ανάγκη αυτή να αντιπετωπισθεί με κατάλληλες πρόσθετες ενέργειες από τους ίδιους τους χρήστες, χωρίς την ύπαρξη ενός γενικού μηχανισμού. Για παράδειγμα, όταν κάποιος υπογράφει ψηφιακά ένα έγγραφο, επισυνάπτει σ' αυτό και ένα

αντίγραφο του πιστοποιητικού του, έτσι ώστε ο παραλήπτης να το έχει κατ' ευθείαν στη διάθεσή του για άμεση αξιοποίηση. Αυτό βέβαια μπορεί να θεωρηθεί σπατάλη δικτυακών πόρων, δεδομένου ότι ο παραλήπτης πιθανόν να είχε ήδη (από παλαιότερη επικοινωνία) το υπ' όψη πιστοποιητικό. Επιπλέον, ίσως ο παραλήπτης να χρειάζεται περισσότερα του ενός πιστοποιητικά, προκειμένου να επαληθεύσει την υπογραφή του αποστολέα (το θέμα αυτό έχει σχέση με τις λεγόμενες "ιεραρχίες πιστοποίησης" - βλ. και Κεφ. 7).

Επομένως το ζητούμενο είναι ένας γενικός μηχανισμός στηριγμένος σε κατάλληλα πρότυπα, ο οποίος να είναι συνεχώς διαθέσιμος σε on-line μορφή και να παρέχει στους ενδιαφερόμενους εύκολη αναζήτηση πιστοποιητικών, προσφέροντας ένα είδος υπηρεσιών καταλόγου (directory services), ανάλογο π.χ. με αυτό του τηλεφωνικού καταλόγου. Σε ένα σύστημα PKI το ρόλο αυτό τον παίζει το λεγόμενο "αποθετήριο" (repository). Πρόκειται για ένα μηχανισμό, που επιτρέπει την αποθήκευση-δημοσιοποίηση των πιστοποιητικών που εκδίδει μια ΑΠ και τα οποία είναι στη συνέχεια διαθέσιμα στους χρήστες με τη βοήθεια τυποποιημένων μεθόδων.

Ενα πρότυπο για on-line υπηρεσίες καταλόγου είχε δημιουργηθεί από παλαιότερα και προέβλεπε τη δυνατότητα αναζήτησης, μεταξύ άλλων, πληροφοριών για φυσικά πρόσωπα, στοιχεία εξοπλισμού δικτύου, εφαρμογές λογισμικού, άλλα αυτοματοποιημένα συστήματα, αλλά και ψηφιακά πιστοποιητικά. Εντούτοις, το πρότυπο αυτό, γνωστό ως X.500 (ITU X.500 directory standard), είναι πολύπλοκο και ιδιαίτερα δύσκολο στην υλοποίησή του, με αποτέλεσμα να μην τύχει ευρύτερης αποδοχής και διάδοσης.

Με την εξάπλωση του Internet, αναπτύχθηκε ένα διαφορετικό μοντέλο, το οποίο είναι γνωστό ως "Lightweight Directory Access Protocol – LDAP". Το LDAP είναι συμβατό με το X.500, αλλά κατά πολύ απλούστερο και ευκολότερο στην υλοποίηση και παρέχει παρόμοιες υπηρεσίες, οι οποίες περιλαμβάνουν την αναζήτηση ψηφιακών πιστοποιητικών. Ετσι σήμερα είναι αυτό που συνήθως χρησιμοποιείται για την πρόσβαση σε ένα αποθετήριο πιστοποιητικών, ώστε να εξυπηρετήσει τη σχετική λειτουργία της διανομής τους. Να διευκρινιστεί ότι το LDAP είναι απλώς ένα πρωτόκολλο πρόσβασης και δεν απαιτεί τη χρήση συγκεκριμένης τεχνολογίας για τη δημιουργία της βάσης πληροφοριών του καταλόγου. Αυτό έχει ιδιαίτερη σημασία, διότι ενισχύει τη δυνατότητα συνεργασίας (διαλειτουργικότητα) μεταξύ διαφόρων ετερογενών συστημάτων.

Παράλληλα, σε ένα περιβάλλον Internet είναι δυνατόν να χρησιμοποιηθούν και ορισμένες άλλες λύσεις για τη διανομή πιστοποιητικών, οι οποίες δεν κάνουν χρήση του LDAP, όπως π.χ. μέσω Web ή FTP. Τέλος, είναι δυνατόν, πιστοποιητικά τα οποία χρησιμοποιούνται συχνά, να αποθηκευτούν τοπικά στο σύστημα από το οποίο γίνεται η χρήση τους.

6.7. Ανάκληση πιστοποιητικών (certificate revokation)

Ενα ψηφιακό πιστοποιητικό ισχύει (είναι έγκυρο) για ένα συγκεκριμένο χρονικό διάστημα που καθορίζεται από τις ημερομηνίες έναρξης και λήξης ισχύος, οι οποίες περιλαμβάνονται στο υπογεγραμμένο τμήμα του πιστοποιητικού. Η διάρκεια ισχύος έχει σχέση με την πολιτική που ακολουθεί η αρμόδια ΑΠ και μπορεί να είναι από μερικούς μήνες μέχρι μερικά χρόνια. Παρ' όλα αυτά, υπάρχουν περιπτώσεις όπου, για διάφορους λόγους, οι χρήστες δεν θα πρέπει να βασίζονται σε ένα πιστοποιητικό, ακόμη και όταν δεν έχει εξαντληθεί η διάρκεια ισχύος του. Στις περιπτώσεις αυτές, η ΑΠ μπορεί να διακόψει πρόωρα την ισχύ του πιστοποιητικού, προβαίνοντας, όπως λέγεται, σε "ανάκλησή" του.

Οι πιθανές αιτίες ανάκλησης ενός πιστοποιητικού είναι:

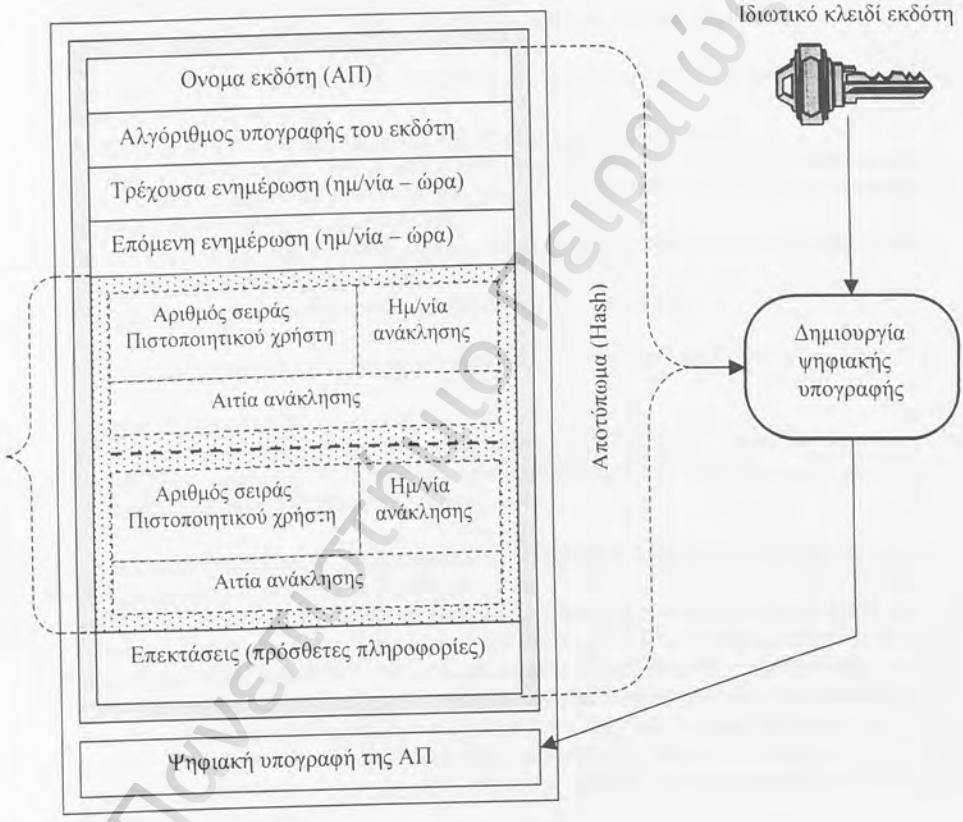
- Παραβίαση (ή υποψία παραβίασης) του ιδιωτικού κλειδιού του κατόχου του πιστοποιητικού
- Παραβίαση (ή υποψία παραβίασης) του ιδιωτικού κλειδιού της ΑΠ που υπογράφει το πιστοποιητικό
- Αλλαγή στοιχείων: το όνομα του κατόχου ή άλλη πληροφορία που προσδιορίζει τον κάτοχο έχει αλλάξει
- Αντικατάσταση του πιστοποιητικού από άλλο
- Παύση λειτουργίας: το πιστοποιητικό δεν χρησιμοποιείται πλέον για το σκοπό που είχε αρχικά εκδοθεί

Η απόφαση για την ανάκληση ενός πιστοποιητικού είναι αρμοδιότητα της ΑΠ και συνήθως λαμβάνεται μετά από σχετική αίτηση του κατόχου του πιστοποιητικού. Είναι όμως δυνατόν η ΑΠ να πάρει η ίδια την πρωτοβουλία για την ανάκληση, όταν για παράδειγμα ο κάτοχος παραβεί κάποιες από τις υποχρεώσεις που έχει αναλάβει απέναντι στη ΑΠ. Πριν προβεί στην ανάκληση, η ΑΠ θα πρέπει να επιβεβαιώσει την ταυτότητα του αιτούντος. Γενικά, η αξιολόγηση και η έγκριση ή απόρριψη μιας αίτησης ανάκλησης μπορεί να ανήκουν στην αρμοδιότητα της ΑΚ, εφ' όσον αυτή υπάρχει.

6.7.1. Πίνακες ανάκλησης πιστοποιητικών - ΠΑΠ (Certificate Revocation Lists - CRLs)

Μετά την απόφαση για ανάκληση ενός πιστοποιητικού, η ΑΠ πρέπει να ενημερώσει σχετικά τους πιθανούς χρήστες του πιστοποιητικού. Η συνήθης μέθοδος που ακολουθείται είναι η περιοδική δημοσιοποίηση μιας ψηφιακής δομής, η οποία ονομάζεται "Πίνακας Ανάκλησης Πιστοποιητικών – ΠΑΠ". Ενας ΠΑΠ είναι ένας χρονοσημασμένος κατάλογος ανακληθέντων πιστοποιητικών που έχει υπογραφεί ψηφιακά από την ΑΠ και έχει διανεμηθεί στους χρήστες. Η διανομή του ΠΑΠ (όπως και των ίδιων των πιστοποιητικών) στηρίζεται κατά κανόνα στο μηχανισμό του αποθετηρίου που έχει περιγραφεί στα προηγούμενα και εξυπηρετείται συνήθως με χρήση πρωτοκόλλου X.500 ή LDAP.

Η γενική δομή ενός ΠΑΠ παριστάνεται στο Σχήμα 13 και περιγράφεται αναλυτικά παρακάτω.



Σχήμα 13. Δομή ενός Πίνακα Ανάκλησης Πιστοποιητικών (ΠΑΠ)

Ονομα εκδότη (issuer name)
Προσδιορίζει την αρχή (συνήθως Αρχή Πιστοποίησης) που εκδίδει τον ΠΑΠ και της οποίας η υπογραφή εμφανίζεται στον υπ' όψη ΠΑΠ.
Αλγόριθμος υπογραφής του εκδότη (issuer's signature algorithm)
Αναφέρει τον αλγόριθμο ψηφιακής υπογραφής που χρησιμοποιεί ο εκδότης για να υπογράψει τον ΠΑΠ.
Τρέχουσα ενημέρωση (this update)
Εδώ αναφέρεται η ημερομηνία και ώρα της έκδοσης του συγκεκριμένου ΠΑΠ.
Επόμενη ενημέρωση (next update)
Αναφέρει την ημερομηνία και ώρα της έκδοσης του επόμενου ΠΑΠ, δεδομένου ότι ο ΠΑΠ δημοσιεύεται περιοδικά.
Αριθμός σειράς πιστοποιητικού χρήστη (user certificate serial number)
Είναι ο αριθμός σειράς του ανακληθέντος πιστοποιητικού (όπως έχει προαναφερθεί, ο αριθμός αυτός προσδιορίζει με μοναδικό τρόπο το πιστοποιητικό - βλ. δομή πιστοποιητικού).
Ημερομηνία ανάκλησης (revocation date)
Είναι η ημερομηνία από την οποία ισχύει η ανάκληση του συγκεκριμένου πιστοποιητικού.
Αιτία ανάκλησης (revocation reason)
Αναφέρεται ο λόγος για τον οποίο ανακλήθηκε το πιστοποιητικό

(Τα τρία προηγούμενα πεδία επαναλαμβάνονται για κάθε ανακληθέν πιστοποιητικό)

Επεκτάσεις (extensions)
Εδώ περιλαμβάνονται πρόσθετες πληροφορίες που πιθανόν απαιτούνται, όπως για παράδειγμα η κατηγορία πιστοποιητικών που αφορά ο υπ' όψη ΠΑΠ, ο τρόπος με τον οποίο είναι ταξινομημένος ο ΠΑΠ (order method) κλπ.

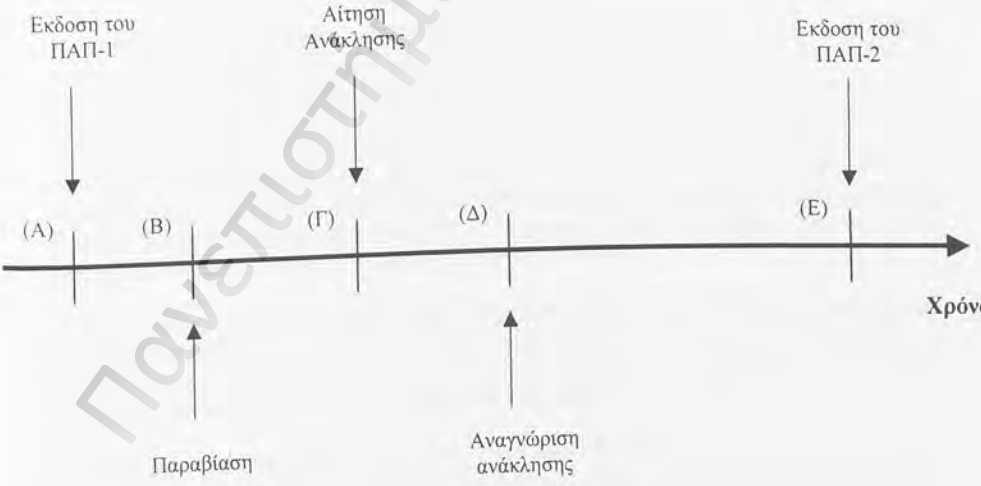
Γενικά, όταν ένα σύστημα χρησιμοποιεί ένα πιστοποιημένο δημόσιο κλειδί (προκειμένου π.χ. να επαληθεύσει την ψηφιακή υπογραφή ενός χρήστη), δεν αρκεί μόνο να ελέγξει την εγκυρότητα του ίδιου του πιστοποιητικού, αλλά θα πρέπει επιπλέον να ανατρέξει σε έναν πρόσφατο ΠΑΠ και να επιβεβαιώσει ότι το πιστοποιητικό δεν περιλαμβάνεται σ' αυτόν. Η έννοια του "πρόσφατου" δεν είναι τυποποιημένη και κατά κανόνα σημαίνει τον τελευταίο εκδοθέντα ΠΑΠ. Μια ΑΠ εκδίδει πίνακες ανάκλησης σε περιοδική βάση, που μπορεί να είναι ωριαία, ημερήσια ή εβδομαδιαία και καθορίζεται από την σχετική πολιτική της ΑΠ. Η περιοδική έκδοση του ΠΑΠ συνεχίζεται κανονικά, άσχετα αν υπάρχουν ή όχι νέες ανακλήσεις, προκειμένου οι χρήστες να είναι βέβαιοι ότι χρησιμοποιούν έναν ΠΑΠ τελευταίας ενημέρωσης.

Ενα σημαντικό πλεονέκτημα της μεθόδου ανάκλησης που στηρίζεται σε ΠΑΠ είναι ότι η διανομή της πληροφορίας εξυπηρετείται με τα ίδια μέσα και μηχανισμούς όπως και η διανομή των πιστοποιητικών, δεδομένου ότι και ο ΠΑΠ είναι ψηφιακά υπογεγραμμένος και εγγυημένης ακεραιότητας. Ετσι δεν απαιτείται ιδιαίτερος εξοπλισμός υψηλού κόστους για υποδομές υψηλής ασφάλειας, προκειμένου να διακινηθούν οι σχετικές με ανάκληση πιστοποιητικών πληροφορίες.

Εντούτοις, η μέθοδος αυτή έχει ένα σοβαρό περιορισμό, ο οποίος έχει σχέση με τη συχνότητα δημοσίευσης των ΠΑΠ. Για παράδειγμα, αν μια αίτηση ανάκλησης κατατεθεί και εγκριθεί αμέσως μετά την έκδοση ενός ΠΑΠ, τότε η σχετική πληροφορία θα είναι διαθέσιμη στους χρήστες του αντίστοιχου πιστοποιητικού με κάποια καθυστέρηση, δηλ. μόνο όταν δημοσιευθεί ο επόμενος ΠΑΠ. Η καθυστέρηση αυτή, ανάλογα με την πολιτική της ΑΠ, μπορεί να είναι μια ώρα ή μια μέρα ή μια εβδομάδα, με αποτέλεσμα να είναι υπάρχει ενδεχόμενο πρόκλησης ζημιών από τη χρήση πιστοποιητικών, των οποίων το ιδιωτικό κλειδί έχει πιθανόν παραβιασθεί. Κατά συνέπεια, αν υπάρχει ανάγκη για πιο άμεση πληροφόρηση σχετικά με την εγκυρότητα ή μη των πιστοποιητικών, απαιτείται κάποια διαφορετική μέθοδος (βλ. Κεφ. 6.8.).

6.7.2. Χρονική εξέλιξη της διαδικασίας ανάκλησης

Προκειμένου να αποσαφηνιστούν ορισμένες επιπτώσεις της λειτουργίας ανάκλησης πιστοποιητικών, στην περίπτωση που για το σκοπό αυτό χρησιμοποιούνται πίνακες ανάκλησης (ΠΑΠ), είναι σκόπιμο να εξετασθεί μια τυπική αλληλουχία γεγονότων, όπως αυτά εξελίσσονται χρονικά. Σχετικό είναι τα παράδειγμα που ακολουθεί (βλ. και Σχήμα 14), κατά τη συζήτηση του οποίου εξετάζεται και η νομική διάσταση ορισμένων σημείων.



Σχήμα 14. Χρονική εξέλιξη της διαδικασίας ανάκλησης πιστοποιητικού

Η ακολουθία των γεγονότων είναι γενικώς η εξής:

(Α) Εκδοση του ΠΑΠ-1: Εκδίδεται ένας ΠΑΠ πρίν από την ανάκληση του πιστοποιητικού

(Β) Παραβίαση: Συμβαίνει ένα γεγονός που οδηγεί στη ανάγκη για ανάκληση του πιστοποιητικού, όπως "εισβολή" τρίτων σε κάποιο ευαίσθητο χώρο ή περιβάλλον, που δημιουργεί υποψίες για πιθανή παραβίαση του ιδιωτικού κλειδιού που φυλάσσεται σε ένα σταθμό εργασίας (υπολογιστή), ο οποίος βρίσκεται στο συγκεκριμένο χώρο. Ο ακριβής χρόνος του συμβάντος δεν είναι γνωστός, δηλ. είναι πιθανόν το γεγονός αυτό να έχει συμβεί πρίν από το γεγονός (Α).

(Γ) Αίτηση ανάκλησης: Ενα εξουσιοδοτημένο πρόσωπο καταθέτει μια αίτηση ανάκλησης στην ΑΠ (ή στην αρμόδια ΑΚ), η οποία προβαίνει σε επιβεβαίωση ταυτότητας και είτε εγκρίνει είτε απορρίπτει την αίτηση. Το γεγονός αυτό μπορεί να είναι προγενέστερο ή μεταγενέστερο του γεγονότος (Α).

(Δ) Αναγνώριση ανάκλησης: Η ΑΠ αναγνωρίζει επίσημα την ανάκληση και καταγράφει τον ακριβή χρόνο ανάκλησης.

(Ε) Εκδοση του ΠΑΠ-2: Ο ΠΑΠ που περιέχει την συγκεκριμένη ανάκληση εκδίδεται και δημοσιοποιείται.

Αν το πιστοποιητικό χρησιμοποιηθεί για την επαλήθευση του δημοσίου κλειδιού οποιαδήποτε στιγμή μετά το γεγονός (Β), είναι σαφές ότι το αντίστοιχο ιδιωτικό κλειδί δεν βρίσκεται απαραίτητα κάτω από τον απόλυτο έλεγχο του κατόχου του πιστοποιητικού. Επομένως είναι ενδεχόμενο να προκληθεί σημαντική ζημία στον χρήστη του πιστοποιητικού (που πολλές φορές αναφέρεται και ως "εξαρτώμενο μέρος" - relying party) ή σε κάποιο τρίτο μέρος. Προκειμένου να αντιμετωπισθούν παρόμοιες περιπτώσεις, θα πρέπει τα ενδιαφερόμενα μέρη να κατανείμουν τον κίνδυνο μεταξύ τους. Το μεγαλύτερο μερίδιο κινδύνου είναι λογικό να το αναλάβει η πλευρά εκείνη που είναι σε θέση να τον ελέγξει καλύτερα ή έχει αναλάβει συμβατική δέσμευση για μια συγκεκριμένη κατανομή ευθύνης.

Σε μια περίπτωση ανάκλησης μέσω ΠΑΠ, ο προσδιορισμός του μέρους εκείνου που μπορεί να ελέγξει καλύτερα τον κίνδυνο δεν είναι ευχερής. Για παράδειγμα, αν υποτεθεί ότι η ανάκληση οφείλεται στην παραβίαση του ιδιωτικού κλειδιού, τότε η κατάσταση σε κάθε ένα από τα προαναφερθέντα χρονικά διαστήματα θα μπορούσε να είναι η εξής:

Διάστημα (Β)-(Γ): Η παραβίαση έχει συμβεί, αλλά η ΑΠ δεν έχει ενημερωθεί. Το εξαρτώμενο μέρος δεν είναι πιθανόν να έχει γνώση της παραβίασης. Ο κάτοχος του πιστοποιητικού μπορεί να γνωρίζει την παραβίαση, αλλά αυτό δεν είναι βέβαιο. Με αυτά τα δεδομένα, είναι λογικό το μεγαλύτερο μερίδιο του κινδύνου κατά τη διάρκεια αυτής της περιόδου να το αναλάβει ο κάτοχος του πιστοποιητικού.

Διάστημα (Γ)-(Δ): Η παραβίαση έχει γνωστοποιηθεί στην ΑΠ, αλλά δεν έχει εκδοθεί ακόμη ένας ενημερωμένος ΠΑΠ. Ο χρήστης του πιστοποιητικού δεν είναι πιθανόν να έχει γνώση της παραβίασης. Είναι λογικό το μεγαλύτερο μερίδιο κινδύνου να το αναλάβει η ΑΠ στο διάστημα αυτής της περιόδου.

Διάστημα (Δ)-(Ε): Η ΑΠ έχει δημοσιεύσει την ανάκληση, αλλά το εξαρτώμενο μέρος δεν αποκλείεται να μην έχει ακόμη λάβει γνώση της ανάκλησης. Η κατανομή του κινδύνου εξαρτάται από τον συγκεκριμένο μηχανισμό ανάκλησης που χρησιμοποιείται (και ενδεχομένως έχει συμφωνηθεί μεταξύ των εμπλεκομένων μερών). Στην περίπτωση των περιοδικών ΠΑΠ, ο χρήστης του πιστοποιητικού δεν θα λάβει σχετική γνώση παρά μόνο μετά τη δημοσίευση του ΠΑΠ-2. Με τη μέθοδο του απ' ευθείας ελέγχου εγκυρότητας του πιστοποιητικού (On-line status checking) είναι λογικό ότι ο χρήστης του πιστοποιητικού θα έχει λάβει γνώση της ανάκλησης κατά το διάστημα αυτό.

Μετά το (Ε): Η ΑΠ έχει τώρα εκπληρώσει τις υποχρεώσεις της για τη δημοσίευση της ανάκλησης του πιστοποιητικού. Αν το εξαρτώμενο μέρος εξακολουθεί στο διάστημα αυτό να χρησιμοποιεί το ήδη ανακληθέν πιστοποιητικό, τότε είναι λογικό να φέρει αυτός τη μεγαλύτερη ευθύνη για τις πιθανές συνέπειες.

Η επίλυση ζητημάτων σχετικών με ανάκληση πιστοποιητικών εξαρτάται σε μεγάλο βαθμό από την ακρίβεια με την οποία προσδιορίζεται η χρονική στιγμή κάθε συμβάντος. Προς την κατεύθυνση αυτή, σημαντικό ρόλο παίζει η χρονοσήμανση των υπογεγραμμένων συναλλαγών ή μηνυμάτων, γεγονός που αναδεικνύει τη σπουδαιότητα των σχετικών υπηρεσιών αξιόπιστης χρονοσήμανσης που μπορεί να προσφέρει ένα σύστημα PKI.

6.8. Ελεγχος εγκυρότητας πιστοποιητικών (certificate validation)

Ο έλεγχος εγκυρότητας πιστοποιητικού είναι η διαδικασία εκείνη μέσω της οποίας εξακριβώνεται ότι ένα πιστοποιητικό μπορεί να χρησιμοποιηθεί με ασφάλεια σε κάποια δεδομένη χρονική στιγμή και ότι είναι κατάλληλο για τη συγκεκριμένη χρήση. Για να επιτευχθούν τα παραπάνω, θα πρέπει:

- ✓ Το πιστοποιητικό να φέρει μια κρυπτογραφικά έγκυρη υπογραφή, ώστε να διασφαλίζεται ότι τα περιεχόμενά του δεν έχουν αλλοιωθεί
- ✓ Να χρησιμοποιηθεί το δημόσιο κλειδί του εκδότη του πιστοποιητικού, για να επαληθευθεί η υπογραφή που φέρει το πιστοποιητικό
- ✓ Να ελεγχούν οι ημερομηνίες έναρξης και λήξης ισχύος, προκειμένου να διαπιστωθεί ότι το πιστοποιητικό είναι (κατ' αρχήν) σε ισχύ
- ✓ Η προτιθέμενη χρήση του πιστοποιητικού να είναι συμβατή με το σκοπό για τον οποίο αυτό έχει εκδοθεί. Για παράδειγμα, κλειδιά και πιστοποιητικά που προορίζονται για δημιουργία ψηφιακών υπογραφών, δεν θα πρέπει να χρησιμοποιούνται για κρυπτογράφηση δεδομένων.
- ✓ Το πιστοποιητικό να μην έχει ανακληθεί. Ο σχετικός έλεγχος γίνεται μέσω των πινάκων ανάκλησης πιστοποιητικών (ΠΑΠ).

Οπως έχει προαναφερθεί (Κεφ. 6.7.1., 6.7.2.), η χρήση των ΠΑΠ παρουσιάζει ορισμένα μειονεκτήματα, τα οποία έχουν κυρίως σχέση με τη συχνότητα δημοσίευσής τους.

Μια απάντηση στο ζήτημα αυτό προσφέρει ο απ' ευθείας έλεγχος σε πραγματικό χρόνο της κατάστασης του πιστοποιητικού (on-line status checking), με τη βοήθεια ειδικής υπηρεσίας την οποία μπορεί να παρέχει η ΑΠ. Για το σκοπό αυτό απαιτείται ειδικός επιπλέον εξοπλισμός (server) και χρησιμοποιείται κατάλληλο πρωτόκολλο επικοινωνίας (Online Certificate Status Protocol - OCSP). Σε μια συναλλαγή του είδους αυτού, ο χρήστης υποβάλλει μια ερώτηση σχετικά με την εγκυρότητα ενός πιστοποιητικού, πριν το χρησιμοποιήσει, ενώ η απάντηση πρέπει να είναι ψηφιακά υπογεγραμμένη από την ΑΠ και να προέρχεται από ένα περιβάλλον με υψηλές προδιαγραφές ασφαλείας. Είναι δυνατόν η παραπάνω υπηρεσία να παρέχεται, όχι απ' ευθείας από την ΑΠ, αλλά από κάποιον τρίτο, ο οποίος έχει εξουσιοδοτηθεί σχετικά από την ΑΠ. Γενικά, η υποδομή για την παροχή μιας τέτοιας υπηρεσίας έχει μεγάλο κόστος απόκτησης και λειτουργίας, διότι πρέπει να υποστηριχθεί η συνεχής και αδιάκοπη δημιουργία ψηφιακών υπογραφών για τις παρεχόμενες απαντήσεις, διαδικασία ως γνωστόν ιδιαίτερα απαιτητική σε υπολογιστική ισχύ.

7. ΙΕΡΑΡΧΙΕΣ ΠΙΣΤΟΠΟΙΗΣΗΣ ΚΑΙ ΜΟΝΤΕΛΑ ΕΜΠΙΣΤΟΣΥΝΗΣ (trust models)

7.1. Γενικά

Στα περισσότερα συστήματα PKI επιτρέπεται μια αρχή πιστοποίησης (ΑΠ) να πιστοποιεί μια άλλη αρχή πιστοποίησης. Τα πιστοποιητικά που χρησιμοποιούνται στην περίπτωση αυτή είναι γνωστά ως πιστοποιητικά αρχής πιστοποίησης (CA certificates), σε αντίθεση με τα πιστοποιητικά των χρηστών (user certificates). Ετσι, μια ΑΠ, την οποία εμπιστεύεται ένας χρήστης, επιβεβαιώνει την εγκυρότητα της ταυτότητας μιας άλλης ΑΠ. Σε ένα περιβάλλον μεγάλης κλίμακας είναι κατά συνέπεια πιθανόν μερικές ΑΠ να έχουν ως μόνο έργο τον προσδιορισμό της ταυτότητας άλλων ΑΠ, ενώ ορισμένες ΑΠ θεωρούνται κατώτερες (υποκείμενες ΑΠ) από άλλες, στις οποίες και υπάγονται ιεραρχικά .

Επιπλέον, μια ΑΠ η οποία επιβεβαιώνει η ίδια την εγκυρότητα της δικής της ταυτότητας (υπογράφοντας με το δικό της ιδιωτικό κλειδί το δικό της πιστοποιητικό - self-signed certificate) είναι γνωστή ως πρωταρχική ΑΠ (root CA - trust anchor CA). Ταυτόχρονα, στα πλαίσια της λειτουργίας του συστήματος PKI, ο χρήστης εμπιστεύεται μια τουλάχιστον πρωταρχική ΑΠ και έχει στη διάθεσή του το δημόσιο κλειδί της.

Ενα από τα κύρια ζητούμενα σε ένα περιβάλλον PKI είναι να μπορεί ο χρήστης ενός ψηφιακού πιστοποιητικού να επαληθεύσει την εγκυρότητά του. Για να συμβεί αυτό, θα πρέπει να βρεθεί και να επαληθευτεί μια πλήρης **διαδρομή πιστοποίησης (certification path)**, η οποία ξεκινά από το υπό έλεγχο πιστοποιητικό και διασχίζοντας μια ή περισσότερες ΑΠ καταλήγει σε μια πρωταρχική ΑΠ, την οποία και εμπιστεύεται ο χρήστης. Κατά τη σχεδίαση και υλοποίηση ενός μεγάλου συστήματος PKI, το οποίο θα πρέπει να διαθέτει και δυνατότητες επέκτασης, μια από τις μεγαλύτερες προκλήσεις είναι το να διασφαλιστεί ότι η εύρεση και επαλήθευση των διαδρομών πιστοποίησης θα είναι απλή, εύκολη και αποδοτική. Αυτό εξαρτάται σε μεγάλο βαθμό από την καθιέρωση κανόνων και συμβάσεων για τη δόμηση σχέσεων με βάση τις οποίες οι ΑΠ πιστοποιούν άλλες ΑΠ. Οι πιο πάνω κανόνες και συμβάσεις οδηγούν στη δημιουργία των μοντέλων επιστοσύνης (trust models), στα οποία στηρίζεται η λειτουργία των συστημάτων PKI.

Στη συνέχεια εξετάζονται δύο από τα κυριότερα μοντέλα που έχουν προταθεί και χρησιμοποιούνται: απλές ιεραρχίες και "δάση ιεραρχιών (forests of hierachies) ή πολλαπλές ιεραρχίες". Τα περισσότερα συστήματα PKI που έχουν αναπτυχθεί στηρίζονται στα μοντέλα αυτά, τα οποία υλοποιούνται σχετικά εύκολα και επιτρέπουν την άμεση αξιοποίησή τους από μεγάλο αριθμό εφαρμογών λογισμικού. Επιπρόσθετα γίνεται αναφορά και σε περισσότερο πολύπλοκα μοντέλα, τα οποία παρουσιάζουν αυξημένες δυσκολίες υλοποίησης και υψηλότερο κόστος, αλλά η χρήση τους πιθανόν να επιβάλλεται εξαιτίας των εξειδευμένων απαιτήσεων ορισμένων ειδικών εφαρμογών.

Στο σημείο αυτό κρίνεται σκόπιμο να εξηγηθεί ο όρος "δια-πιστοποίηση (cross-certification)", ο οποίος χρησιμοποιείται στα πλαίσια αυτά. Ουσιαστικά σημαίνει την έκδοση ενός πιστοποιητικού από μια ΑΠ προς μια άλλη ΑΠ, προκειμένου αυτό να χρησιμοποιηθεί σε μια διαδρομή πιστοποίησης, ανεξάρτητα από τη μορφή της δομής (ιεραρχική ή μη ιεραρχική).

7.2. Απλές ιεραρχίες (δένδρα)

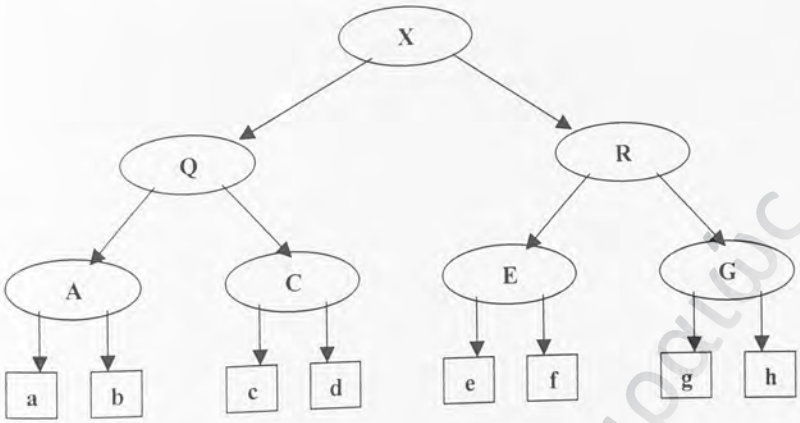
Προκειμένου να ελαχιστοποιηθεί το πρόβλημα των διαδρομών πιστοποίησης απαιτείται ένας μηχανισμός που να συνδέει τα μέλη μιας μεγάλης κοινότητας με ένα μικρό αριθμό πρωταρχικών ΑΠ, μέσω σχετικά μικρών διαδρομών, όπου κάθε διαδρομή διέρχεται από μια σειρά ΑΠ.

Το Σχήμα 15 παριστάνει μια τυπική ιεραρχική δομή. Οι οντότητες με τα κεφαλαία γράμματα είναι αρχές πιστοποίησης, ενώ οι οντότητες με πεζά είναι τελικές οντότητες (end-entities), π.χ. χρήστες. Τα βέλη σημαίνουν ότι μια ΑΠ έχει εκδόσει ένα ψηφιακό πιστοποιητικό για την οντότητα (ΑΠ ή τελική οντότητα) στην οποία καταλήγει το βέλος.

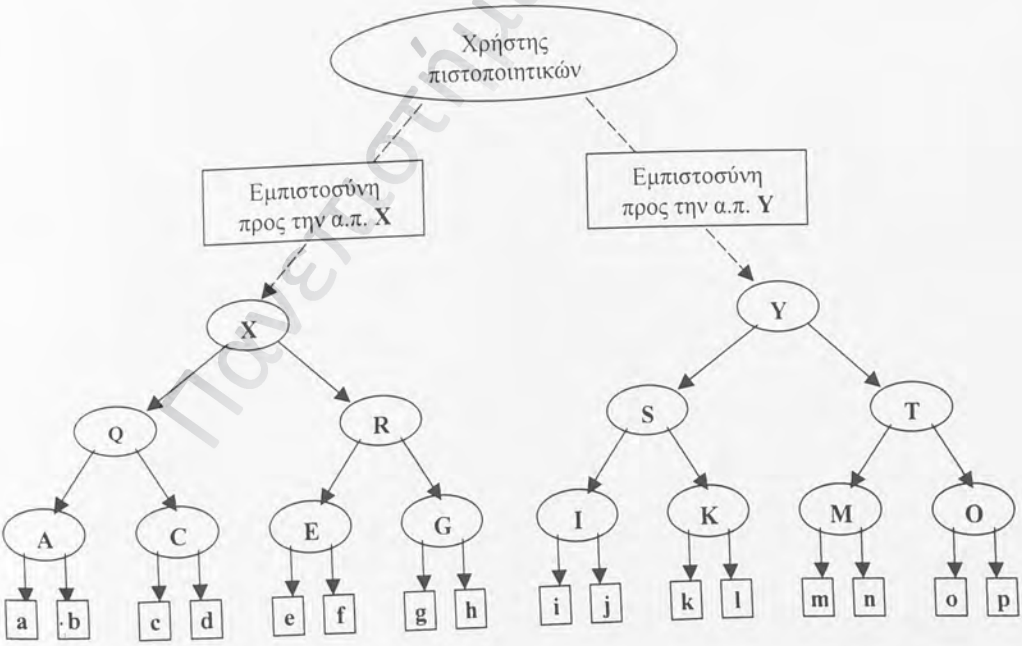
Ολες οι διαδρομές πιστοποίησης αρχίζουν από την πρωταρχική ΑΠ (τύπου root CA) με το όνομα Χ. Οι χρήστες πιστοποιητικών είναι αρκετό να έχουν μόνο την ΑΠ Χ ως "trust anchor", δηλ. ως βασική πηγή εμπιστοσύνης. Με άλλα λόγια, είναι αρκετό να κατέχουν ένα αξιόπιστο αντίγραφο του δημόσιου κλειδιού της ΑΠ Χ, ελεγμένο για την εγκυρότητά του με κάποιο ασφαλή τρόπο. Στη συνέχεια είναι εύκολο να δημιουργηθεί μια διαδρομή πιστοποίησης προς οποιαδήποτε τελική οντότητα. Για παράδειγμα, οποιοσδήποτε χρήστης μπορεί να αποκτήσει ένα επιβεβαιωμένο αντίγραφο του δημόσιου κλειδιού του a χρησιμοποιώντας μια διαδρομή πιστοποίησης αποτελούμενη από τρία πιστοποιητικά:

- Ενα πιστοποιητικό για την ΑΠ Q, το οποίο έχει εκδοθεί από την ΑΠ Χ
- Ενα πιστοποιητικό για την ΑΠ Α, το οποίο έχει εκδοθεί από την ΑΠ Q
- Ενα πιστοποιητικό για την τελική οντότητα a, το οποίο έχει εκδοθεί από την ΑΠ Α

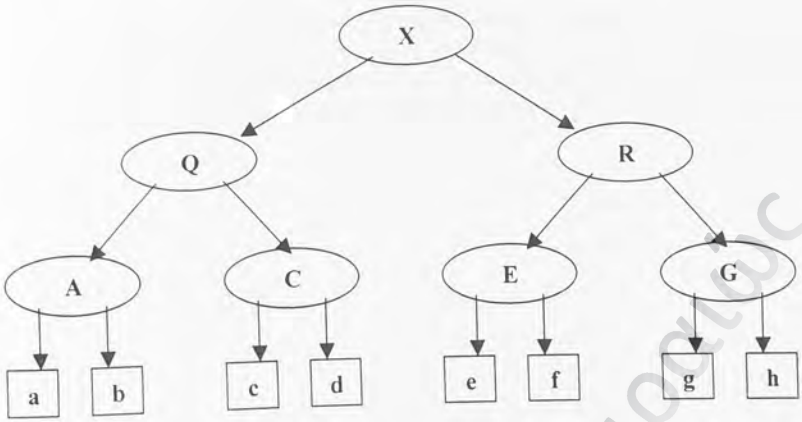
Ενα ψηφιακό πιστοποιητικό είναι βέβαια υπογεγραμμένο από μια ΑΠ, πρέπει όμως (πριν χρησιμοποιηθεί) να επαληθευτεί. Για το σκοπό αυτό απαιτείται το δημόσιο κλειδί της ΑΠ που το υπογράφει. Στο παραπάνω παράδειγμα, για να επαληθευτεί το πιστοποιητικό της a, απαιτείται το δημόσιο κλειδί της ΑΠ Α, το οποίο όμως περιλαμβάνεται στο πιστοποιητικό της ΑΠ Α, το οποίο έχει εκδώσει η ΑΠ Q κ.ο.κ. Η αλυσιδωτή αυτή διαδικασία αναζήτησης του κατάλληλου κάθε φορά δημόσιου κλειδιού για την επαλήθευση ενός πιστοποιητικού τερματίζεται όταν εντοπισθεί ένα πιστοποιητικό στο οποίο η ΑΠ και ο πιστοποιούμενος είναι η ίδια οντότητα, δηλαδή μια ΑΠ τύπου root CA (στο παράδειγμα αυτή είναι η ΑΠ Χ). Ενα τέτοιο πιστοποιητικό είναι, όπως λέγεται, "αυτο-υπογραφόμενο (self-signed)", δηλαδή ο ίδιος ο υπογράφων διαβεβαιώνει για την ορθότητα, την αξιοπιστία και την ακεραιότητα του δικού του πιστοποιητικού (εννοείται ότι τέτοια πιστοποιητικά έχουν δικαίωμα να εκδίδουν μόνο οι ΑΠ τύπου root CA).



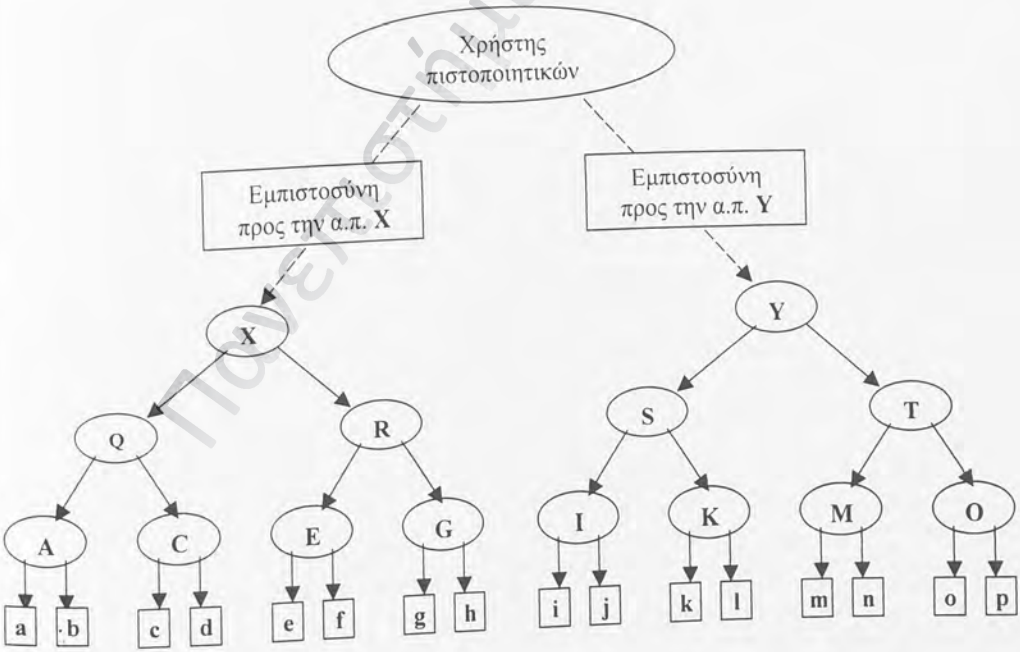
Σχήμα 15. Ιεραρχική δομή πιστοποίησης



Σχήμα 16. Δάση ιεραρχιών πιστοποίησης

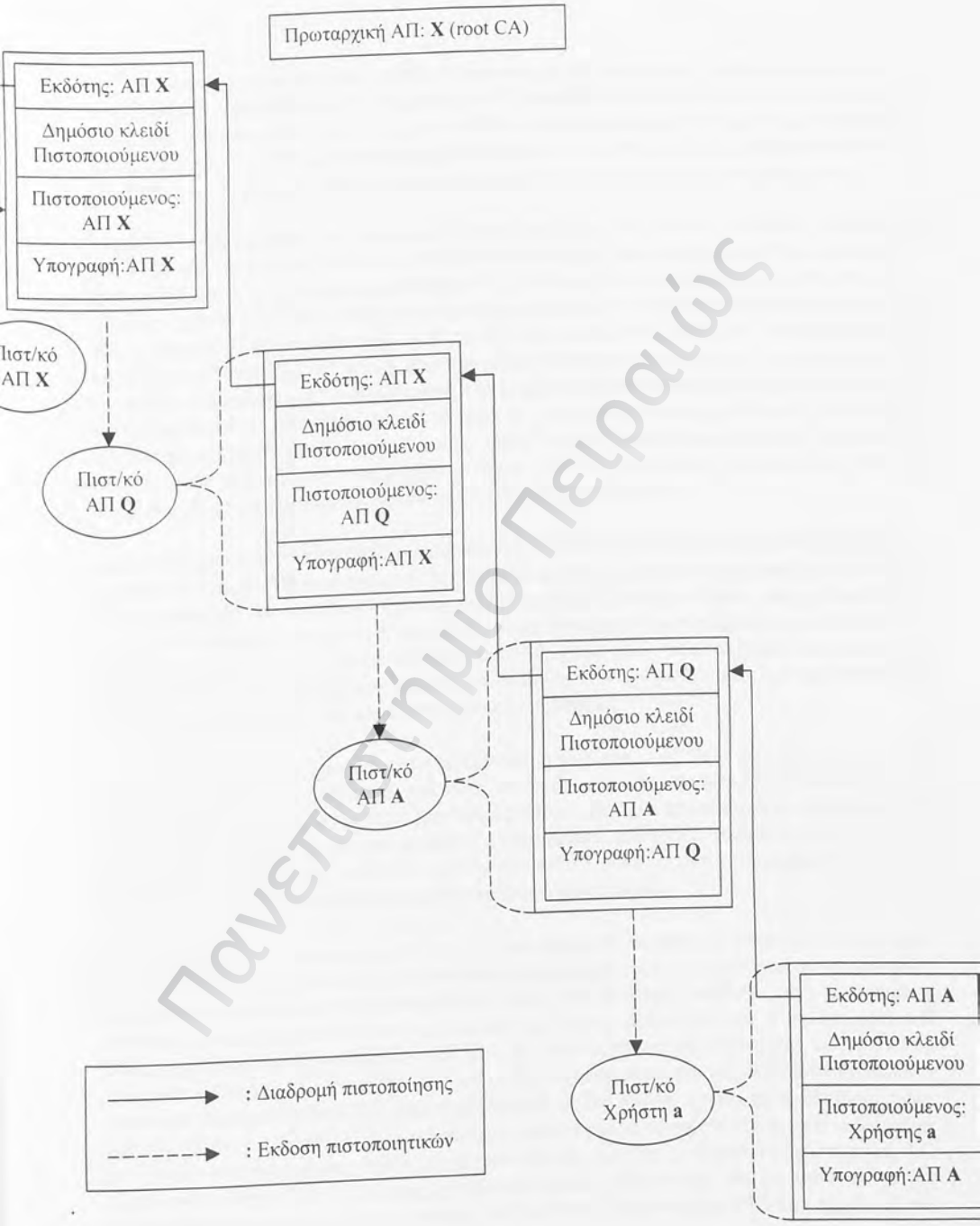


Σχήμα 15. Ιεραρχική δομή πιστοποίησης



Σχήμα 16. Δάση ιεραρχιών πιστοποίησης

Στο Σχήμα 17 (βλ. παρακάτω) παριστάνεται διαγραμματικά η διαδρομή πιστοποίησης (συνεχόμενες γραμμές) που θα ακολουθήσει ο χρήστης ενός πιστοποητικού της a, προκειμένου να το επαληθεύσει, ενώ απεικονίζεται επίσης και η ιεραρχική σειρά έκδοσης (διακεκομμένες γραμμές) των πιστοποιητικών που περιλαμβάνονται στη διαδρομή.



Σχήμα 17. Επαλήθευση πιστοποιητικού – διαδρομή πιστοποίησης

Το μοντέλο αυτό επεκτείνεται εύκολα. Προφανώς είναι δυνατόν να υπάρχουν περισσότερες από δύο οντότητες υποκείμενες σε μια άλλη. Για παράδειγμα, κάθε ΑΠ μπορεί να πιστοποιεί μέχρι και 100 υποκείμενες ΑΠ ή μέχρι 10.000 τελικές οντότητες. Μια δομή τριών επιπέδων, όπως αυτή του Σχ. 15 θα μπορούσε κατά συνέπεια να υποστηρίξει μέχρι 100.000.000 τελικές οντότητες, με τη μέγιστη διαδρομή πιστοποίησης να περιλαμβάνει τρία πιστοποιητικά.

Επιπλέον, υπάρχει μόνο μία διαδρομή πιστοποίησης για κάθε τελική οντότητα, οπότε είναι πολύ εύκολο να εντοπισθούν οι διαδρομές πιστοποίησης που θα ζητηθούν. Έτσι μια τελική οντότητα όπως η a, μπορεί να αποθηκεύσει τη διαδρομή των πιστοποιητικών από την ΑΠ X μέχρι τον εαυτό της και να διανέμει τη διαδρομή αυτή σε οποιαδήποτε άλλη τελική οντότητα την χρειαστεί. Για παράδειγμα, η a μπορεί να επισυνάψει αυτά τα πιστοποιητικά σε οποιοδήποτε "αντικείμενο" έχει η ίδια υπογράψει ψηφιακά, προκειμένου αυτός ο οποίος θα χρειαστεί να επαληθεύσει την υπογραφή της a να έχει άμεσα διαθέσιμα όλα τα απαιτούμενα πιστοποιητικά. Η διαδρομή πιστοποίησης θα μπορούσε επίσης να αποθηκευτεί στην αντίστοιχη εγγραφή καταλόγου (directory entry) της a, οπότε οποιοσδήποτε χρειαστεί να στείλει στην a ένα κρυπτογραφημένο μήνυμα, έχει τη δυνατότητα να αντλήσει από τον κατάλογο όλα τα απαιτούμενα πιστοποιητικά σε μια μόνο κίνηση.

Κατά την χρήση μιας διαδρομής πιστοποίησης, ο χρήστης του πιστοποιητικού θα πρέπει να εμπιστεύεται κάθε ΑΠ που συναντά, με την έννοια ότι αυτή (η ΑΠ) έχει προβεί στην έκδοση των πιστοποιητικών της μέσα από αυστηρές διαδικασίες και έχει λάβει όλα τα κατάλληλα μέτρα ώστε κανείς τρίτος να μην μπορεί να πλαστογραφήσει πιστοποιητικά που προέρχονται απ' αυτήν. Όλοι οι συμμετέχοντες σε μια δομή όπως αυτή που περιγράφηκε παραπάνω δεσμεύονται στην αποδοχή και χρήση διαδικασιών που ορίζονται από την κοινότητα της οποίας τα μέλη εντάσσονται μέσα στην πιο πάνω ιεραρχία.

Σε μια ιεραρχική δομή, η πρωταρχική ΑΠ (τύπου root), όπως η X, είναι ιδιαίτερα κρίσιμη από άποψη εμπιστοσύνης, δεδομένου ότι όλες οι διαδρομές πιστοποίησης εξαρτώνται από το πόσο έμπιστη είναι η X. Αν κάποιος εισβολέας ήταν σε θέση να παραβιάσει το ιδιωτικό κλειδί της X, θα μπορούσε να πλαστογραφήσει την ψηφιακή υπογραφή οποιουδήποτε από τους συμμετέχοντες στην πιο πάνω δομή και να πείσει κάποιον που ενδιαφέρεται για την επαλήθευσή της ότι η πλαστογραφημένη υπογραφή είναι νόμιμη.

Κατά συνέπεια, το ιδιωτικό κλειδί της πρωταρχικής ΑΠ πρέπει να είναι εξαιρετικά καλά προστατευμένο, για παράδειγμα να είναι απενεργοποιημένο και φυλασσόμενο σε μια ασφαλή εγκατάσταση και να ενεργοποιείται μόνο κάτω από αυστηρή επίβλεψη και ελεγχόμενες συνθήκες. Κάτι τέτοιο δεν αποτελεί σοβαρό πρόβλημα, δεδομένου ότι η πρωταρχική ΑΠ (τύπου root) πιστοποιεί μόνο άλλες ΑΠ (και όχι τελικές οντότητες - χρήστες), οπότε σπάνια χρειάζεται να εκδώσει πιστοποιητικά. Κατ' αντιστοιχία, οι περισσότερες ΑΠ που πιστοποιούν τελικές οντότητες εκδίδουν πιστοποιητικά αρκετά συχνά και θα πρέπει είναι διαθέσιμες on-line. Με βάση τα παραπάνω, είναι κοινά αποδεκτό ότι μια ιεραρχία PKI θα πρέπει να δομείται έτσι ώστε να περιλαμβάνει δύο τουλάχιστον επίπεδα, με μια τουλάχιστον πρωταρχική ΑΠ (τύπου root), στην οποία να μην παρέχεται πρόσβαση (ΑΠ off-line), και με μια τουλάχιστον ΑΠ σε κατάσταση κανονικής λειτουργίας (ΑΠ on-line). Ενα σύστημα PKI που περιλαμβάνει

μόνο μια μεμονωμένη ΑΠ δεν είναι γενικώς βιώσιμο, εκτός αν εξυπηρετεί μια πολύ μικρή κοινότητα ή ένα περιβάλλον με χαμηλό επίπεδο εμπιστοσύνης.

7.3. Πολλαπλές ιεραρχίες (Δάση ιεραρχιών - forests of hierarchies)

Σε μια ιεραρχική δομή PKI, όλοι οι συμμετέχοντες οφείλουν να δεσμεύονται ως προς τη διατήρηση ενός συγκεκριμένου επιπέδου αξιοπιστίας και την εφαρμογή μιας σειράς διαδικασιών. Αυτό δεν είναι ιδιαίτερα δύσκολο σε ένα περιβάλλον σχεδιασμένο για μια συγκεκριμένη κοινότητα, όπως είναι οι εργαζόμενοι σε έναν οργανισμό ή οι πελάτες μιας επιχείρησης. Εντούτοις δεν είναι πάντοτε εφικτό να δημιουργηθεί μια μοναδική ιεραρχία που να περιλαμβάνει όλα τα μέρη που συμμετέχουν σε ένα ευρύτερο περιβάλλον, το οποίο είναι επιθυμητό να παρέχει και υπηρεσίες ασφαλείας. Μια εναλλακτική προσέγγιση είναι η διαμόρφωση ενός συστήματος χρήσης πιστοποιητικών, το οποίο να αναγνωρίζει πολλαπλές ιεραρχίες, όπως αυτό που φαίνεται στο Σχήμα 16 (βλ. παραπάνω).

Καταστάσεις που οδηγούν στη διαμόρφωση ενός τέτοιου συστήματος θα μπορούσαν να είναι οι εξής:

- Οι χρήστες πιστοποιητικών είναι διατεθειμένοι να αποδεχθούν-εμπιστευθούν πιστοποιητικά, τα οποία έχουν εκδοθεί από ορισμένους εξωτερικούς οργανισμούς προς τις δικές τους "τοπικές" κοινότητες, π.χ. τους εργαζόμενους της επιχείρησης ή τους πελάτες της

- Οι χρήστες πιστοποιητικών είναι διατεθειμένοι να αποδεχθούν-εμπιστευθούν πιστοποιητικά, τα οποία έχουν εκδοθεί από ανεξάρτητες ΑΠ, οι οποίες λειτουργούν π.χ. με εμπορικούς σκοπούς (δηλ. πωλούν υπηρεσίες ΑΠ προς τρίτους ενδιαφερομένους).

Υπάρχουν διάφοροι μηχανισμοί για την εγκαθίδρυση κάποιων αρχικών σημείων ιεραρχιών (roots of hierarchies) ως σημείων εμπιστοσύνης. Οι μηχανισμοί αυτοί δεν υπόκεινται σε κάποια ευρέως διαδεδομένη τυποποίηση, αλλά είναι θέμα που αφορά τους κατασκευαστές των προϊόντων λογισμικού ή τις επιλογές που θα κάνει ο πελάτης (χρήστης) του συγκεκριμένου λογισμικού και μπορούν να πάρουν μια από τις εξής μορφές:

Μηχανισμός απ'ευθείας διαμόρφωσης, ελεγχόμενος από το χρήστη (User-controlled direct): Ο χρήστης της εφαρμογής λογισμικού η οποία χρησιμοποιεί πιστοποιητικά ενεργοποιεί ο ίδιος ορισμένα βασικά σημεία εμπιστοσύνης (trusted roots), τα οποία θα εμπιστεύεται στη συνέχεια η εφαρμογή. Κατά κανόνα, οι εφαρμογές λογισμικού διατίθενται με προεγκατεστημένο ένα πίνακα από "trusted roots", ενώ ο χρήστης μπορεί να αφαιρέσει ή να προσθέσει στοιχεία στον πίνακα αυτό. Το μοντέλο αυτό υλοποιείται για παράδειγμα από τα προγράμματα πλοήγησης στο Internet (Web browsers) και είναι αρκετά ελκυστικό, δεδομένου ότι παρέχει πλήρη έλεγχο στο χρήστη. Μπορεί όμως να αποδειχθεί προβληματικό, διότι οι χρήστες δεν είναι συνήθως καλά εκπαιδευμένοι ή δεν έχουν τις απαραίτητες εξουσιοδοτήσεις για να ασκήσουν τέτοιο έλεγχο.

Μηχανισμός απ'ευθείας διαμόρφωσης, κεντρικά ελεγχόμενος (Domain-controlled direct): Ο υπεύθυνος διαχειριστής ενός περιβάλλοντος (domain-administrator) επιβάλλει σε όλα τα τοπικά συστήματα που έχει υπό τον έλεγχό του και τα οποία χρησιμοποιούν πιστοποιητικά (όπως προγράμματα πλοήγησης στο Internet ή προγράμματα ηλεκτρονικού ταχυδρομείου) να αναγνωρίζουν ένα προκαθορισμένο σύνολο σημείων εμπιστοσύνης (trusted roots). Η προσέγγιση αυτή είναι κατάλληλη για το περιβάλλον μιας επιχείρησης. Εκχωρεί τις αποφάσεις που έχουν σχέση με θέματα πολιτικής στην δικαιοδοσία του υπεύθυνου διαχειριστή, ενώ απαλλάσσει τους χρήστες από την εμπλοκή τους στη διαχείριση των σημείων εμπιστοσύνης.

Μηχανισμός δια-πιστοποίησης, ελεγχόμενος από το χρήστη (User-controlled cross-certification): Ο χρήστης της εφαρμογής λογισμικού λειτουργεί ως μια μικρή ΑΠ και εκδίδει τοπικά υπογεγραμμένα πιστοποιητικά για τις αναγνωρισμένες ΑΠ τύπου "root". Αυτό ουσιαστικά παρεμβάλλει ένα νέο επίπεδο ΑΠ τύπου "root" πάνω από το αρχικό σύνολο των roots, μετατρέποντας την δομή τύπου δάσους (πολλαπλές ιεραρχίες) σε μια απλή ιεραρχική δενδρική δομή. Στη συνέχεια οι εφαρμογές που χρησιμοποιούν πιστοποιητικά είναι αρκετό να αναγνωρίζουν μόνο μια "root" και μπορούν να βρίσκουν και να επεξεργάζονται εύκολα διαδρομές πιστοποίησης όπως θα έκαναν με μια απλή ιεραρχία (Ο μηχανισμός αυτός έχει χρησιμοποιηθεί για παράδειγμα στο προϊόν Lotus Notes).

Μηχανισμός δια-πιστοποίησης,κεντρικά ελεγχόμενος (Domain-controlled cross-certification): Αυτό το μοντέλο είναι όμοιο με το προηγούμενο, με τη διαφορά ότι η παρεμβολή μιας επιπλέον ΑΠ ανωτάτου επιπέδου γίνεται μια και μόνο φορά, σε επίπεδο επιχείρησης, από τον υπεύθυνο διαχειριστή και όχι από τον κάθε χρήστη ξεχωριστά. Παρουσιάζει πλεονεκτήματα σε ό,τι αφορά τη λήψη και εφαρμογή αποφάσεων σχετικά με τη διαχείριση των "roots", δεδομένου ότι αυτές μεταφέρονται σε κεντρικό επίπεδο για όλη την επιχείρηση και δεν εμπλέκονται οι χρήστες.

7.4. Γενικευμένο μοντέλο

Όλοι οι παραπάνω μηχανισμοί έχουν δοκιμαστεί επαρκώς και έχουν αποδειχθεί αποτελεσματικοί, εξυπηρετώντας με επιτυχία τη μεγάλη πλειοψηφία των συστημάτων PKI που έχουν υλοποιηθεί. Παρ'όλα αυτά, υπάρχει ένα γενικότερο μοντέλο το οποίο έχει στόχο να καλύψει περιπτώσεις που απαιτούν τη συνεργασία μεταξύ συστημάτων PKI που έχουν αναπτυχθεί ξεχωριστά και ακολουθούν διαφορετικές πολιτικές και διαδικασίες ή τη δημιουργία συστημάτων PKI που να μπορούν να υποστηρίζουν ταυτόχρονα διαφορετικές εφαρμογές που απαιτούν διαφορετικές πολιτικές. Το μοντέλο αυτό είναι ιδιαίτερα πολύπλοκο και δεν θα εξετασθεί εδώ σε λεπτομέρειες. Σε γενικές γραμμές προσπαθεί να επιλύσει δύο θεμελιώδη προβλήματα: Πώς μπορεί να εντοπισθεί μια κατάλληλη διαδρομή πιστοποίησης και πώς μπορεί στη συνέχεια η διαδρομή αυτή να επαληθευτεί. Οι λειτουργίες αυτές θα πρέπει να υλοποιηθούν και να υποστηρίζονται σε κάθε σύστημα που χρησιμοποιεί ψηφιακά πιστοποιητικά. Τα δύο αυτά ζητήματα αντιμετωπίζονται ξεχωριστά το ένα από το άλλο, επειδή η επαλήθευση μιας διαδρομής πιστοποίησης είναι μια κρίσιμη από πλευράς ασφάλειας λειτουργία, ενώ η ανακάλυψη μιας διαδρομής δεν έχει ιδιαίτερες απαιτήσεις ασφαλείας.

8. ΕΠΙΒΕΒΑΙΩΣΗ ΤΑΥΤΟΤΗΤΑΣ (authentication)

8.1. Παράγοντες επιβεβαίωσης ταυτότητας

Οταν δύο πρόσωπα πρόκειται να επικοινωνήσουν ή να διεξάγουν μια συναλλαγή, το κάθε πρόσωπο επιθυμεί να επαληθεύσει την ταυτότητα του άλλου, δηλαδή ζητεί να βεβαιωθεί ότι το άλλο πρόσωπο είναι όντως αυτό που ισχυρίζεται ότι είναι. Αυτό ισχύει γενικά, αλλά η ανάγκη είναι ακόμη πιο επιτακτική όταν δεν υπάρχει τοπική εγγύτητα που να διευκολύνει την διαδικασία αναγνώρισης, όπως συμβαίνει π.χ. σε μια ηλεκτρονικού τύπου επικοινωνία εξ αποστάσεως. Στη γενικότερη περίπτωση η επικοινωνία μπορεί να είναι ανάμεσα σε δύο οντότητες, κάθε μια από τις οποίες μπορεί να είναι φυσικό πρόσωπο, οργανισμός ή κάποιο ηλεκτρονικό σύστημα, π.χ. υπολογιστής. Στα πλαίσια λειτουργίας ενός ηλεκτρονικού περιβάλλοντος, όπως είναι ένα σύστημα PKI, η επιβεβαίωση ταυτότητας επιτυγχάνεται με διάφορες μεθόδους, οι οποίες μπορεί να κάνουν χρήση ενός ή περισσοτέρων παραγόντων, που είναι γνωστοί ως παράγοντες επαλήθευσης ταυτότητας (authentication factors). Οι τρείς συνηθέστεροι παράγοντες αφορούν τη γνώση κάποιου στοιχείου, την κατοχή κάποιου στοιχείου και κάποια μοναδική φυσική ιδιότητα που χαρακτηρίζει ένα άτομο.

Παράγοντες γνώσης (knowledge factors – "something you know"): Πρόκειται για κάτι το οποίο έχει χαρακτήρα μυστικού (secret) και το οποίο ένα άτομο γνωρίζει, όπως είναι π.χ. ένα password ή ο προσωπικός αριθμός ταυτότητας (PIN) που χρησιμοποιείται σε τραπεζικές συναλλαγές με χρήση πλαστικής κάρτας. Και τα δύο μέρη (αυτός που ζητεί πρόσβαση σε κάποια υπηρεσία και αυτός που απαιτεί την επαλήθευση ταυτότητας του αιτούντος) έχουν από κοινού γνώση του password ή του PIN. Για παράδειγμα ένας χρήστης (ο αιτών) πληκτρολογεί ένα password, προκειμένου να αποκτήσει πρόσβαση σε ένα κεντρικό υπολογιστή (server). Ο server πρέπει να γνωρίζει το password του χρήστη, ώστε να το επαληθεύσει και να επιτρέψει την πρόσβαση. Η ασφάλεια του συστήματος στηρίζεται στην υπόθεση ότι το password είναι γνωστό μόνο σ'αυτόν που ζητεί την πρόσβαση και σ'αυτόν που επαληθεύει την ταυτότητα του αιτούντος και φυλάσσεται μυστικό από όλους τους άλλους. Ετσι ένα PIN που πληκτρολογείται σε ένα τραπεζικό τερματικό είναι κρυπτογραφημένο και αποστέλλεται στο σύστημα της Τράπεζας για επαλήθευση.

Παράγοντες κατοχής (possesion factors – "something you have"): Είναι κάτι που ένα άτομο έχει, όπως ένα κλειδί, ένα ειδικό σήμα, μια ειδική ηλεκτρονική συσκευή (token) και γενικά κάποιο αντικείμενο και το οποίο βρίσκεται στην κατοχή του ατόμου που ζητεί πρόσβαση σε κάποιο περιβάλλον ή υπηρεσία. Το γεγονός ότι το συγκεκριμένο αντικείμενο βρίσκεται στην κατοχή ενός ατόμου προσφέρει τη διαβεβαίωση ότι το άτομο αυτό είναι το εξουσιοδοτημένο πρόσωπο για τη ζητούμενη επικοινωνία. Χαρακτηριστικό παράδειγμα της περίπτωσης αυτής είναι οι πλαστικές κάρτες που χρησιμοποιούνται στις αυτόματες τραπεζικές συναλλαγές και οι οποίες βρίσκονται στην κατοχή του ατόμου που έχει εξουσιοδοτηθεί από την Τράπεζα, ώστε να μπορεί να εκτελεί τέτοιου είδους συναλλαγές (Στην πραγματικότητα η χρήση των καρτών αυτών συνδυάζεται και με τη γνώση κάποιου PIN).

Βιομετρικοί παράγοντες (biometric factors – "something you are"): Πρόκειται για ορισμένα μοναδικά βιολογικά χαρακτηριστικά του ατόμου (π.χ. δακτυλικά αποτυπώματα), τα οποία με τη βοήθεια κατάλληλης τεχνολογίας μπορούν να παίξουν ρόλο αντίστοιχο με τα passwords, με τη διαφορά ότι επειδή δεν τα διαθέτει κανείς άλλος, δεν είναι δυνατόν να χρησιμοποιηθούν παρά μόνο από το συγκεκριμένο άτομο.

Οι διαδικασίες επαλήθευσης ταυτότητας είναι δυνατόν να χρησιμοποιούν ένα ή και περισσότερους από τους τρείς παραπάνω παράγοντες. Στην τελευταία περίπτωση γίνεται λόγος για διαδικασία επαλήθευσης με χρήση πολλών παραγόντων (multi-factor authentication). Γενικά τα συστήματα με αυξημένες απαιτήσεις ασφάλειας, χρησιμοποιούν σχήματα επαλήθευσης δύο ή και τριών παραγόντων (two-, three-factor authentication schemes).

Χαρακτηριστικό παράδειγμα επαλήθευσης ταυτότητας δύο παραγόντων είναι η μέθοδος που χρησιμοποιείται στις αυτόματες τραπεζικές συναλλαγές με πλαστικές κάρτες. Αυτό που γνωρίζει ο χρήστης είναι ο μυστικός του κωδικός (PIN), τον οποίο και πληκτρολογεί, ενώ αυτό που έχει είναι η ίδια η πλαστική κάρτα, η οποία πρέπει οπωσδήποτε να εισαχθεί στο τραπεζικό τερματικό, προκειμένου να καταστεί δυνατή η διεξαγωγή της συναλλαγής.

8.2. Συνθηματικά (passwords) και προσωπικοί αριθμοί ταυτότητας (PINs)

Οι συνθηματικές λέξεις ή φράσεις (passwords) και οι προσωπικοί αριθμοί ταυτότητας (Personal Identification Numbers - PINs) είναι όλα παραλλαγές του ίδιου βασικού μηχανισμού επιβεβαίωσης ταυτότητας και θα αναφέρονται παρακάτω ως passwords.

Σχεδόν όλα τα σχήματα επιβεβαίωσης ταυτότητας στηρίζονται σε κάποιο βαθμό στα passwords, τα οποία ανήκουν στην κατηγορία των παραγόντων γνώσης. Εντούτοις, τα passwords είναι μια από τις κυριότερες αιτίες που καθιστούν ευάλωτα τα συστήματα ηλεκτρονικού εμπορίου και αποτελούν την πηγή των περισσότερων κινδύνων.

Οι μεγαλύτερες απειλές που σχετίζονται με τη χρήση passwords για την επιβεβαίωση ταυτότητας είναι:

Εξωτερική αποκάλυψη: Ο επιτιθέμενος (επίδοξος εισβολέας) υποκλέπτει ένα password με χρήση μέσων εξωτερικών ως προς το σύστημα ή το δίκτυο. Για παράδειγμα, κάποιος χρήστης καταγράφει το password του πάνω σε ένα κομμάτι χαρτί ή σε ένα αυτοκόλλητο το οποίο επικολλά σε κάποιο σημείο στην άκρη της οθόνης του ή σημειώνει το PIN του πάνω στην πλαστική κάρτα που χρησιμοποιεί, οπότε αποτελεί εύκολο στόχο για τον υποψήφιο εισβολέα. Αλλη μέθοδος είναι η παρακολούθηση πάνω από τον ώμο του χρήστη (shoulder surfing) την ώρα που πληκτρολογεί το password, με σκοπό να εντοπιστούν οι χαρακτήρες που αποτελούν το password. Ακόμη είναι δυνατόν να υποκλαπούν passwords με έρευνα στα δοχεία απορριμάτων (trashing) ή και με χρήση μεθόδων **"κοινωνικής μηχανικής" (social engineering)**, ώστε να πεισθεί ένας χρήστης να γνωστοποιήσει το password του σε κάποιον τρίτο, διότι δήθεν αυτό είναι απαραίτητο να γίνει (π.χ. η παραχώρηση του password ενός

υπολογιστή κεντρικής εξυπηρέτησης server μιας επιχείρησης στον μηχανικό της εταιρίας που έχει αναλάβει την τεχνική υποστήριξη, προκειμένου να επιλυθεί κάποιο υπαρκτό τεχνικό πρόβλημα).

Επαναληπτικές δοκιμές (guessing): Δοκιμάζονται διάφορα passwords, έως ότου κάποιο από αυτά να αποδειχθεί επιτυχημένο. Αν τα passwords που επιλέγουν οι χρήστες είναι δύσκολα και υπακούουν γενικά σε κανόνες καλής επιλογής passwords, τότε η μέθοδος αυτή δεν έχει ιδιαίτερες πιθανότητες επιτυχίας. Συνήθως όμως οι χρήστες επιλέγουν passwords τα οποία είναι εύκολο να απομνημονευτούν, όπως ημερομηνίες γέννησης, το όνομα της/του συζύγου ή ακόμα και την ίδια τη λέξη "password", ενώ πάρα πολλοί χρήστες καρτών επιλέγουν σαν PIN τον αριθμό "1234". Ετσι είναι πολλές φορές εύκολο για τον επίδοξο εισβολέα να παραβιάσει ένα σύστημα δοκιμάζοντας κατ' αρχήν αυτές τις συνήθεις τιμές.

Υποκλοπή επικοινωνιών (communications eavesdropping): Ενας τρίτος που παρακολουθεί τις επικοινωνίες ενός συστήματος με τους σταθμούς εργασίας ή με άλλα συστήματα μπορεί να μάθει τα passwords που χρησιμοποιούνται, αν αυτά μεταδίδονται απροστάτευτα (σε μορφή clear text), εκμεταλλευόμενος διάφορες τεχνικές και εργαλεία (packet sniffers κλπ)

Τεχνικές επαναχρησιμοποίησης (replay attacks): Ακόμη και αν τα passwords μεταδίδονται κρυπτογραφημένα, είναι δυνατόν κάποιος που παρακολουθεί τις επικοινωνίες να καταγράψει το κρυπτογραφημένο password, το οποίο στη συνέχεια να το αποστείλει εκ νέου όταν αυτό του ζητηθεί, προσποιούμενος ότι είναι ο νόμιμος κάτοχός του.

Παραβίαση κεντρικού υπολογιστή (host compromise): Ο επίδοξος εισβολέας είναι δυνατόν να διεισδύσει με κάποιο τρόπο σε ένα σύστημα και να υποκλέψει το αρχείο ή τη βάση δεδομένων στην οποία φυλάσσονται (σε απλή ή κρυπτογραφημένη μορφή) τα passwords των χρηστών, τα οποία στη συνέχεια μπορεί να τα εκμεταλλευθεί (αφού πιθανόν τα αποκρυπτογραφήσει, αν χρειαστεί).

Για την αντιμετώπιση αυτών των απειλών απαιτούνται αυστηρές πολιτικές σχετικά με τα passwords και αντίστοιχες αποτελεσματικές διαδικασίες, εκπαίδευση των χρηστών και υπεύθυνη συμπεριφορά εκ μέρους τους, καθώς και προσεκτικός σχεδιασμός του συστήματος επιβεβαίωσης ταυτότητας.

8.3. Πρωτόκολλα επιβεβαίωσης ταυτότητας (authentication protocols)

Η αντιμετώπιση απειλών, όπως αυτές που περιγράφηκαν παραπάνω και ειδικά εκείνων που σχετίζονται με τα δεδομένα που αφορούν επιβεβαίωση ταυτότητας, απαιτεί τη σχεδίαση και χρήση ειδικών πρωτοκόλλων, βάσει των οποίων θα γίνεται η ανταλλαγή των ευαίσθητων δεδομένων μεταξύ μιας οντότητας που ζητεί να γίνει αποδεκτή η ταυτότητά της (συνήθως ένα τερματικό ή σταθμός εργασίας του χρήστη - client system) και της οντότητας που λαμβάνει την απόφαση για την αποδοχή της (συνήθως ένας υπολογιστής κεντρικής εξυπηρέτησης - server system). Οι κυριότερες τεχνικές για τη δημιουργία ενός πρωτοκόλλου επιβεβαίωσης ταυτότητας είναι οι εξής:

Μετασχηματισμένο password: Το password που πληκτρολογεί ο χρήστης στο τερματικό του υποβάλλεται σε επεξεργασία μέσω μιας μονόδρομης συνάρτησης, ώστε να προκύψει ένα μετασχηματισμένο password, το οποίο είναι αυτό που τελικά μεταδίδεται στον server. Ο server εφαρμόζει την ίδια συνάρτηση στο αποθηκευμένο αντίγραφο του password που διαθέτει και αν τα δύο αποτελέσματα ταυτίζονται συμπεραίνει ότι ο χρήστης έδωσε το σωστό password. Ενας "ωτακουστής" (eavesdropper) δεν έχει τη δυνατότητα να ανακτήσει το αρχικό password εκμεταλλευόμενος την μετασχηματισμένη μορφή του που μεταδόθηκε και την οποία πιθανόν ήταν σε θέση να υποκλέψει. Εναλλακτικά, ο server μπορεί να έχει αποθηκευμένο μόνο το μετασχηματισμένο password.

Πρόκληση-απάντηση (challenge-response): Ο server αποστέλλει προς το τερματικό μια τυχαία τιμή, γνωστή ως "πρόκληση" (challenge), η οποία είναι διαφορετική για κάθε αίτηση επιβεβαίωσης ταυτότητας. Η τιμή αυτή πρέπει να ενσωματωθεί στην απάντηση του τερματικού, για παράδειγμα ως πρόσθετη παράμετρος σε μια μονόδρομη συνάρτηση , η οποία υπολογίζει ένα μετασχηματισμένο password. Κατά την επεξεργασία της απάντησης, ο server επιβεβαιώνει ότι η σωστή "πρόκληση" έχει χρησιμοποιηθεί. Η μέθοδος αυτή παρέχει προστασία απέναντι σε επιθέσεις τύπου "replay attack".

Χρονοσήμανση (time stamp): Η αίτηση επιβεβαίωσης ταυτότητας από το τερματικό προς τον server έχει ενσωματωμένη τη σωστή ημερομηνία και ώρα, για παράδειγμα ως πρόσθετη παράμετρο σε μια μονόδρομη συνάρτηση, η οποία υπολογίζει ένα μετασχηματισμένο password. Κατά την επεξεργασία της απάντησης ο server ελέγχει αν η ώρα που έχει χρησιμοποιηθεί είναι αποδεκτή. Η μέθοδος αυτή προσφέρει επίσης προστασία από επιθέσεις τύπου "replay attack", αλλά έχει πρακτικούς περιορισμούς, διότι στηρίζεται στο ότι όλα τα συστήματα έχουν ακριβή και συγχρονισμένα ρολόγια.

Password μιας φοράς (one-time password): Ενα password μιας φοράς είναι παρόμοιο με ένα μετασχηματισμένο password, αλλά παρέχει προστασία τόσο απέναντι σε "replay attacks" όσο και "communications eavesdropping". Ο μηχανισμός αυτός δημιουργεί ένα διαφορετικό κάθε φορά on-line password, διοχετεύοντας το password που δίνει ο χρήστης μέσω μιας μονόδρομης συνάρτησης N φορές, όπου το N μειώνεται κατά 1 σε κάθε νέα προσπάθεια σύνδεσης με τον server (login). Ο server παρακολουθεί τις τιμές του N, καθώς και το τελευταίο on-line password που έχει χρησιμοποιηθεί. Ενας "ωτακουστής" που παρατηρεί ένα on-line password δεν μπορεί να συμπεράνει τίποτε σχετικά με ένα μελλοντικό on-line password, διότι η μονόδρομη συνάρτηση δεν είναι δυνατόν να εκτελεσθεί με αντίστροφη φορά. Το σύστημα που προκύπτει βάσει του πιο πάνω μηχανισμού είναι σχετικά απλό στην υλοποίησή του, τόσο στον server όσο και στα τερματικά - σταθμούς εργασίας και δεν απαιτεί την αποθήκευση των passwords σε μη κρυπτογραφημένη μορφή (clear text) σε κανένα από τα δύο εμπλεκόμενα μέρη.

Ψηφιακή υπογραφή: Οι ψηφιακές υπογραφές αποτελούν τη βάση πολλών από τα σύγχρονα πρωτόκολλα επιβεβαίωσης ταυτότητας. Η πλευρά που ζητεί να επιβεβαιωθεί η ταυτότητά της αποδεικνύει κατοχή ενός συγκεκριμένου ιδιωτικού κλειδιού υπογράφοντας ένα μήνυμα με χρήση του ως άνω κλειδιού. Τα δεδομένα που υπογράφονται μπορεί να περιέχουν μια τιμή

τύπου "πρόκλησης" ή μια χρονοσήμανση, παρέχοντας με τον τρόπο αυτό προστασία απέναντι σε επιθέσεις τύπου "replay attack".

8.4. Ειδικές προσωπικές συσκευές επιβεβαίωσης ταυτότητας (Personal tokens)

Οπως έχει προαναφερθεί, οι διάφορες μέθοδοι επαλήθευσης ταυτότητας βασίζονται σε ένα ή περισσότερους δεδομένους παράγοντες. Οι ειδικές προσωπικές συσκευές επαλήθευσης ταυτότητας, γνωστές με τον όρο "personal tokens", χρησιμοποιούν τον παράγοντα της κατοχής από τον χρήστη κάποιου αντικειμένου και συγκεκριμένα μιας μικρής ηλεκτρονικής συσκευής. Ο παράγοντας όμως αυτός συνδυάζεται συνήθως με την επίδειξη από τον ενδιαφερόμενο της γνώσης κάποιου άλλου στοιχείου και συγκεκριμένα ενός password ή ενός PIN. Ενας τρίτος, προκειμένου να προσποιηθεί ότι είναι ο νόμιμος χρήστης, δεν είναι αρκετό να αποκτήσει γνώση του PIN (πιθανώς μέσω μεθόδων "κοινωνικής μηχανικής"), αλλά θα πρέπει επιπλέον να επιτύχει και την κατοχή του token. Μόνο τότε θα είναι σε θέση να ανταποκριθεί με επιτυχία σε μια διαδικασία επαλήθευσης ταυτότητας με χρήση δύο παραγόντων (two-factor authentication). Με βάση τα παραπάνω, οι πιθανότητες επιτυχίας μιας κακόβουλης προσπάθειας τέτοιου τύπου μειώνονται αρκετά.

Οι συσκευές αυτές είναι δύο κυρίως τύπων:

"Πρόκλησης/απάντησης" (challenge/response tokens): Στην περίπτωση αυτή, η συσκευή υλοποιεί τη μια πλευρά ενός πρωτοκόλλου "challenge/response", συνθέτοντας μια απάντηση που υπολογίζεται με την εφαρμογή μιας μονόδρομης συνάρτησης με παραμέτρους μια τιμή-"πρόκληση" που αποστέλλεται από τον server στο τερματικό του χρήστη και μια σταθερή μυστική τιμή που βρίσκεται αποθηκευμένη στη συσκευή. Οι συσκευές του τύπου αυτού φέρουν μια μικρή οθόνη υγρών κρυστάλλων (LCD) και ένα υποτυπώδες πληκτρολόγιο (keypad). Η τιμή-"πρόκληση" εμφανίζεται στην οθόνη του τερματικού και ο χρήστης την πληκτρολογεί μαζί με το PIN του στο πληκτρολόγιο του token. Η υπολογιζόμενη απάντηση (response) εμφανίζεται στην οθόνη του token, οπότε ο χρήστης την πληκτρολογεί στο πληκτρολόγιο του τερματικού (αυτή τη φορά) για αποστολή στον κεντρικό υπολογιστή.

Χρονογεννήτριες passwords (time-based password generators): Οι συσκευές αυτές φέρουν επίσης μια μικρή οθόνη LCD (όχι όμως πληκτρολόγιο) και δημιουργούν ένα νέο password σε τακτά χρονικά διαστήματα (π.χ. κάθε ένα λεπτό), το οποίο εμφανίζουν στην οθόνη της συσκευής. Το password αυτό υπολογίζεται με την εφαρμογή μιας μονόδρομης συνάρτησης με παραμέτρους την τρέχουσα ώρα της ημέρας και μια σταθερή μυστική τιμή αποθηκευμένη μέσα στη συσκευή. Ο χρήστης χρησιμοποιεί το μιας χρήσης password (που εμφανίζεται στην LCD οθόνη της συσκευής) για την επιβεβαίωση ταυτότητας απέναντι σε έναν κεντρικό υπολογιστή, ο οποίος υποστηρίζει τη μέθοδο αυτή πληκτρολογώντας το μαζί με το PIN του στο πληκτρολόγιο του τερματικού του. Το μιας χρήσης password αντικαθιστά το συνηθισμένο password που θα χρησιμοποιούσε σε άλλη περίπτωση ο χρήστης.
Ο κεντρικός υπολογιστής που εκτελεί επιβεβαίωση ταυτότητας και οι αντίστοιχες συσκευές (tokens) αυτού του τύπου που απευθύνονται σ'αυτόν πρέπει να παραμένουν συγχρονισμένοι ως προς την ώρα που χρησιμοποιούν.

Υλοποίηση tokens μέσω λογισμικού: η λειτουργία ενός token μπορεί να εξομοιωθεί με τη χρήση λογισμικού, το οποίο εκτελείται σε προσωπικούς υπολογιστές, σε συσκευές τύπου PDA (Personal Digital Assistants), αλλά και σε κινητά τηλέφωνα, επιτρέποντας στις συσκευές αυτές να χρησιμοποιηθούν ως tokens.

8.5. Έξυπνες κάρτες (smart cards)

Οι έξυπνες κάρτες είναι μια ειδική περίπτωση της πιο πάνω κατηγορίας. Είναι εξειδικευμένες ηλεκτρονικές συσκευές μικρού μεγέθους (αναλόγου με αυτό των γνωστών πιστωτικών καρτών), οι οποίες όμως φέρουν εσωτερικά ένα μικροεπεξεργαστή, καθώς και αντίστοιχη μνήμη. Έτσι είναι σε θέση να δέχονται δεδομένα, να τα επεξεργάζονται μέσω προγραμμάτων που βρίσκονται αποθηκευμένα στη μνήμη τους και να παράγουν κάποιο αποτέλεσμα, το οποίο στη συνέχεια μεταδίδεται προς τα έξω μέσα από θύρα επικοινωνίας που διαθέτουν. Η χρήση των έξυπνων καρτών προϋποθέτει την ύπαρξη ειδικών συσκευών ανάγνωσης (smart card readers). Με τη βοήθεια της συσκευής ανάγνωσης η έξυπνη κάρτα τροφοδοτείται με ρεύμα (μέσω ειδικών επαφών) και μπορεί να επικοινωνήσει με το περιβάλλον της. Η συσκευή ανάγνωσης τοποθετείται με τη μορφή περιφερειακού σε κάποιο υπολογιστή, οπότε είναι δυνατή η πλήρης αξιοποίηση της έξυπνης κάρτας.

Οι έξυπνες κάρτες υλοποιούν επιβεβαίωση ταυτότητας δύο παραγόντων, δεδομένου ότι ο κάτοχός τους πρέπει επιπλέον να γνωρίζει και το PIN που του επιτρέπει πρόσβαση στην κάρτα.

Υπάρχουν τρεις κυρίως κατηγορίες έξυπνων καρτών:

1. Κάρτες αποθηκευμένης τιμής (stored value cards): Είναι οι κάρτες με τις λιγότερες δυνατότητες και οι πιο φθηνές. Διαθέτουν περιορισμένη μνήμη (τύπου EEPROM) και μικροεπεξεργαστή πολύ μικρής ισχύος (8 bits) και χρησιμοποιούνται κυρίως για την αποθήκευση ορισμένων προκαθορισμένων δεδομένων σε κρυπτογραφημένη μορφή.

2. Μη κρυπτογραφικές κάρτες (non-crypto cards): Διαθέτουν αρκετά ισχυρότερο επεξεργαστή (συνήθως 16 bits) και μεγαλύτερη μνήμη (EEPROM, ROM και RAM), καθώς και ειδικό λειτουργικό σύστημα. Όλες οι επικοινωνίες με τη μνήμη της κάρτας διέρχονται μέσω του επεξεργαστή και συντονίζονται με ευθύνη του λειτουργικού συστήματος. Επιπλέον διαθέτουν αυξημένα χαρακτηριστικά ασφαλείας για την παρεμπόδιση πιθανών προσπαθειών παραβίασης της κάρτας μέσω πρόσβασης στα ηλεκτρονικά κυκλώματα που την αποτελούν.

3. Κρυπτογραφικές κάρτες (crypto cards): Οι κάρτες της κατηγορίας αυτής διαθέτουν όλα τα χαρακτηριστικά της προηγούμενης, αλλά επιπλέον είναι εφοδιασμένες με ειδικό επιταχυντή κρυπτογραφικών λειτουργιών (crypto accelerator). Χάρη σ' αυτόν είναι σε θέση να υποστηρίζουν λειτουργίες ασύμμετρης κρυπτογραφίας,οπότε προσφέρονται περισσότερο για χρήση σε ένα περιβάλλον PKI. Πρόσφατα έχουν εμφανιστεί κρυπτογραφικές κάρτες με ακόμη πιο ισχυρούς επεξεργαστές (32 bits

τύπου RISC), ενώ καθιερώνονται λειτουργικά συστήματα ανοικτού τύπου (JavaCard, MULTOS, Windows for Smart Card).

8.6. Βιομετρικές μέθοδοι (biometrics)

Οι μέθοδοι αυτές στηρίζονται στην αξιοποίηση κάποιων μοναδικών βιολογικών χαρακτηριστικών του ατόμου, προκειμένου να γίνει η ζητούμενη επαλήθευση ταυτότητας. Έχουν αναπτυχθεί διάφορες βιομετρικές τεχνολογίες με σκοπό να αξιοποιηθούν στην επαλήθευση ταυτότητας, κάθε μια από τις οποίες ασχολείται με κάποιο συγκεκριμένο φυσικό χαρακτηριστικό, όπως:

- Δακτυλικό αποτύπωμα (fingerprint recognition)
- Φωνητική χροιά (voice recognition)
- Γεωμετρία προσώπου (face recognition)
- Γεωμετρία χειρός (hand geometry recognition)
- Εικόνα αμφιβληστροειδούς (retinal scan)
- Εικόνα ίριδας (iris scan)
- Τρόπος γραφής (hand-writing recognition)

Σε γενικές γραμμές η τεχνική που χρησιμοποιείται περιλαμβάνει την μέτρηση ενός φυσικού χαρακτηριστικού του προσώπου που ζητεί την πρόσβαση, με τη βοήθεια ειδικού βιομετρικού αναγνώστη (biometric reader). Στη συνέχεια η ληφθείσα μέτρηση-εικόνα συγκρίνεται με μια άλλη προαποθηκευμένη εικόνα αναφοράς (του χαρακτηριστικού αυτού για το συγκεκριμένο πρόσωπο) και εφ'όσον υπάρχει ικανοποιητικός βαθμός ταύτισης των δύο εικόνων, η επαλήθευση ταυτότητας θεωρείται επιτυχής.

Τα βιομετρικά χαρακτηριστικά ενός ατόμου είναι πιθανόν να μεταβάλλονται για διάφορους λόγους (π.χ. αλλοίωση αποτυπώματος λόγω τραυματισμού, διαφοροποίηση της εικόνας του αμφιβληστροειδούς με την πάροδο του χρόνου κλπ). Κατά συνέπεια, το λογισμικό που χρησιμοποιείται για την ταύτιση μιας τρέχουσας μέτρησης με την προαποθηκευμένη εικόνα λειτουργεί με σχετικά και όχι με απόλυτα κριτήρια. Ετσι, πάνω από ένα ποσοστό ταύτισης η επαλήθευση θεωρείται επιτυχής, ενώ στην αντίθετη περίπτωση υπάρχει αποτυχία. Λόγω της σχετικότητας των κριτηρίων, είναι επίσης πιθανόν να γίνει δεκτός ένας χρήστης, ο οποίος θα έπρεπε κανονικά να απορριφθεί. Μεταξύ άλλων επομένως ένα σύστημα βιομετρικής αναγνώρισης χαρακτηρίζεται και από το "ποσοστό εσφαλμένων αποδοχών" (false accept ratio - FAR), ενώ η αντίστοιχη παράμετρος για την αντίστροφη περίπτωση είναι το "ποσοστό εσφαλμένων απορρίψεων" (false reject ratio - FRR).

Οι βιομετρικές μέθοδοι προσφέρουν σημαντική ευκολία χρήσης, όταν χρησιμοποιούνται από μόνες τους με τη μορφή της επαλήθευσης ενός παράγοντα (one-factor authentication). Το σχήμα αυτό είναι δυνατόν αξιοποιηθεί για την εκχώρηση δικαιωμάτων πρόσβασης σε κάποιο περιβάλλον με χαμηλές απαιτήσεις ασφαλείας. Οταν όμως πρωταρχικό κριτήριο είναι η

ασφάλεια και όχι η ευκολία χρήσης, τότε οι βιομετρικές μέθοδοι συνδυάζονται με ένα ή δύο ακόμη παράγοντες, με τη μορφή σχημάτων δύο ή τριών παραγόντων.

8.7. Χρήση μεθόδων επιβεβαίωσης ταυτότητας σε ένα σύστημα PKI

Θα πρέπει να γίνει σαφές ότι ένα σύστημα PKI δεν καταργεί την ανάγκη για επιβεβαίωση ταυτότητας, αλλά μάλλον την καθιστά πιο επιτακτική. Η ισχύς και το επίπεδο ασφάλειας ενός συστήματος PKI εξαρτάται σε μεγάλο βαθμό από δύο παράγοντες:

- την εμπιστοσύνη προς την Αρχή Πιστοποίησης (σε σχέση με τις διαδικασίες που εφαρμόζει, τις πολιτικές που ακολουθεί και τα μέτρα ασφαλείας που λαμβάνει).

- την ισχύ-αυστηρότητα των διαδικασιών επιβεβαίωσης ταυτότητας που ακολουθούν οι χρήστες, προκειμένου να αποκτήσουν πρόσβαση στο ιδιωτικό τους κλειδί.

Σε σχέση με τη δεύτερη από τις παραπάνω παρατηρήσεις, υπενθυμίζεται εδώ ότι **θεμελιώδης προϋπόθεση** της λειτουργίας ενός συστήματος PKI (που υποστηρίζει ψηφιακές υπογραφές και λοιπές υπηρεσίες) είναι ότι **ο κάτοχος ενός ζεύγους κλειδιών (δημόσιο/ιδιωτικό) είναι το μοναδικό πρόσωπο παγκοσμίως που έχει πρόσβαση στο ιδιωτικό του κλειδί.** Αν αυτό δεν μπορεί να διασφαλιστεί, τότε τίθεται εν αμφιβόλω η συνολική ασφάλεια και χρησιμότητα του συστήματος.

Αναφορικά με τις μεθόδους επιβεβαίωσης ταυτότητας που περιγράφηκαν παραπάνω και τη χρήση τους σε ένα περιβάλλον PKI ισχύουν σε γενικές γραμμές τα εξής:

8.7.1. Passwords:

Οι πιο διαδεδομένες εφαρμογές λογισμικού που συναντά κανείς σε ένα περιβάλλον PKI είναι τα προγράμματα πλοήγησης στο Internet (Web browsers), καθώς και τα προγράμματα ηλεκτρονικού ταχυδρομείου (E-mail). Οι εφαρμογές αυτές χρησιμοποιούν ορισμένα αρχεία ως χώρο αποθήκευσης/φύλαξης των ιδιωτικών κλειδιών των χρηστών, κάνοντας κατά κανόνα χρήση passwords, προκειμένου να προστατεύσουν τα πιο πάνω αρχεία. Με δεδομένο το ότι δεν υπάρχει συνήθως συγκεκριμένη και αποτελεσματική πολιτική σχετικά με τον τρόπο επιλογής και συντήρησης των passwords, καθώς και την έλλειψη εκπαίδευσης των χρηστών σε θέματα PKI, προκύπτει σοβαρός κίνδυνος για την ασφάλεια των χρησιμοποιούμενων σε τέτοια περιβάλλοντα ιδιωτικών κλειδιών. Ο επίδοξος υποκλοπέας "απέχει μόλις ένα password" από το ιδιωτικό κλειδί του νόμιμου χρήστη. Κατά συνέπεια τα passwords αυτά θα πρέπει να επιλέγονται και να συντηρούνται με όσο γίνεται πιο σχολαστικές διαδικασίες, ώστε τουλάχιστον να μην είναι εύκολο να παραβιαστούν, επειδή π.χ. ήταν πολύ εύκολο να τα μαντέψει κάποιος (ή ακόμη χειρότερα, επειδή ο χρήστης προτίμησε, για "ευκολία", να αφήσει το password κενό).

8.7.2. Personal tokens:

Η συνηθέστερη χρήση των ειδικών προσωπικών συσκευών επαλήθευσης ταυτότητας (personal tokens) είναι αυτή που περιγράφεται παρακάτω:

Συνήθως σε μια τυπική επικοινωνία ασφαλούς μορφής ενός χρήστη (client) με ένα Web server απαιτείται να γίνει επαλήθευση ταυτότητας και από τις δύο πλευρές, Αυτό μεταξύ άλλων σημαίνει ότι πρέπει να γίνει ανταλλαγή και έλεγχος ψηφιακών πιστοποιητικών, με όλη την επιβάρυνση που αυτό συνεπάγεται, κυρίως στην πλευρά των client PCs, σε σχέση με την εγκατάσταση και συντήρηση κατάλληλου λογισμικού για τη διαχείριση κλειδιών και πιστοποιητικών. Αν όμως αυτό που πραγματικά χρειάζεται είναι απλώς η επαλήθευση ταυτότητας του χρήστη και όχι υπηρεσίες ψηφιακών υπογραφών, τότε η κατάσταση μπορεί να αντιμετωπιστεί πολύ πιο απλά, με τη χρήση των personal tokens. Ετσι, για την ασφαλή πρόσβαση στον συγκεκριμένο Web server, ο κάθε χρήστης εφοδιάζεται με ένα token και όταν ζητήσει πρόσβαση στον server, τότε (λόγω του ειδικού πρωτοκόλλου SSL που χρησιμοποιείται), η σύνδεση αυτή θα είναι εξ ορισμού ασφαλής (κρυπτογραφημένη). Ο server παρουσιάζει το ψηφιακό του πιστοποιητικό στο λογισμικό του χρήστη για έλεγχο και επιβεβαίωση ταυτότητας, ενώ ταυτόχρονα ζητεί από τον χρήστη να πληκτρολογήσει το κατάλληλο password, για να αποδείξει τη δική του ταυτότητα. Τότε ο χρήστης χρησιμοποιεί ως password αυτό που του προτείνει το token του, οπότε και τα δύο μέρη έχουν επαληθεύσει το ένα την ταυτότητα του άλλου.

Μια άλλη χρήση των personal tokens είναι αυτή που σχετίζεται για την προστασία των αρχείων που χρησιμοποιούνται για την αποθήκευση των ιδιωτικών κλειδιών των χρηστών (βλ. και παραπάνω: passwords). Στην περίπτωση αυτή σχετικά αρχεία που αφορούν το χρήστη φυλάσσονται κρυπτογραφημένα σε ένα ασφαλή κεντρικό υπολογιστή (και όχι στο PC του χρήστη). Ο ενδιαφερόμενος χρήστης πρέπει να ανταποκριθεί επιτυχώς σε μια διαδικασία (δύο παραγόντων) επιβεβαίωσης της ταυτότητάς του, κάνοντας χρήση του token που έχει στη διάθεσή του (και το οποίο φυσικά προστατεύεται με κάποιο PIN). Μετά απ' αυτό, τα απαιτούμενα αρχεία μεταφέρονται στο PC του χρήστη και αποκρυπτογραφούνται. Τότε το ιδιωτικό κλειδί του χρήστη είναι πλέον διαθέσιμο στον ενδιαφερόμενο ώστε να χρησιμοποιηθεί για την αξιοποίηση όλων των σχετικών κρυπτογραφικών υπηρεσιών.

8.7.3. Εξυπνες κάρτες (smart cards):

Οπως προαναφέρθηκε, οι έξυπνες κάρτες υλοποιούν μέθοδο δυό παραγόντων για την επαλήθευση ταυτότητας (η ίδια η κάρτα και το PIN που τη συνοδεύει). Παράλληλα, έχουν κατασκευαστικά αυξημένα χαρακτηριστικά ασφαλείας και μπορούν να αποθηκεύσουν ευαίσθητες πληροφορίες, όπως ιδιωτικά κλειδιά ασύμμετρης κρυπτογραφίας. Επιπλέον, είναι σε θέση να εκτελέσουν εσωτερικά (χωρίς ανάγκη επικοινωνίας με άλλες εξωτερικές συσκευές) κρυπτογραφικούς υπολογισμούς. Κατά συνέπεια, είναι ίσως οι πιο κατάλληλες εξειδικευμένες συσκευές για χρήση σε ένα περιβάλλον PKI. Για παράδειγμα μπορούν να χρησιμοποιηθούν για την αρχική δημιουργία του ζεύγους κλειδιών (δημόσιο/ιδιωτικό) ενός χρήστη και στη συνέχεια το μεν ιδιωτικό κλειδί να αποθηκευτεί με ασφάλεια στη μνήμη της κάρτας, ενώ το δημόσιο να αποσταλεί σε μια Αρχή Πιστοποίησης (ΑΠ), προκειμένου να

εκδοθεί βάσει αυτού το σχετικό ψηφιακό πιστοποιητικό. Με τον τρόπο αυτό, ούτε ο ίδιος ο χρήστης δεν "βλέπει" ούτε μαθαίνει ποτέ το ιδιωτικό του κλειδί, το οποίο δεν μεταφέρεται ποτέ εκτός της κάρτας, πράγμα το οποίο αυξάνει το επίπεδο ασφάλειας ενός συστήματος PKI που στηρίζεται σε έξυπνες κάρτες. Τέλος χάρη στην αυξημένη μνήμη που διαθέτουν είναι δυνατόν να αποθηκεύσουν και άλλα δεδομένα, όπως για παράδειγμα τα ψηφιακά πιστοποιητικά του κατόχου.

Εξάλλου, όλες οι κρυπτογραφικές λειτουργίες που απαιτούν τη χρήση του ιδιωτικού κλειδιού (π.χ. δημιουργία ψηφιακής υπογραφής) εκτελούνται στο εσωτερικό της κάρτας. Βέβαια δεν είναι σκόπιμο, για παράδειγμα, να εκτελείται στην κάρτα ο αλγόριθμος κατατεμαχισμού (hash algorithm) για ένα μήνυμα μεγέθους 1 MB, γιατί κάτι τέτοιο δεν θα ήταν καθόλου αποδοτικό, εξαιτίας της μικρής σχετικά επεξεργαστικής ισχύος της κάρτας. Μπορεί όμως κάλλιστα, μετά την διεκπεραίωση του πιο πάνω αλγορίθμου από το PC του χρήστη, να μεταφερθεί το παραγόμενο αποτύπωμα (message digest) στην κάρτα, όπου και να υπογραφεί ψηφιακά με το ιδιωτικό κλειδί του χρήστη.

Οι έξυπνες κάρτες είναι ιδανικές για χρήση σε ένα περιβάλλον PKI, δεδομένου ότι λόγω του μικρού μεγέθους τους είναι ιδιαίτερα εύχρηστες σε ό,τι αφορά τη μεταφορά τους από το χρήστη. Ετσι ο χρήστης ενός συστήματος PKI μπορεί να έχει πάντοτε μαζί του (π.χ. μέσα στο πορτοφόλι του) τα ιδιωτικά του κλειδιά, αλλά και τα ψηφιακά πιστοποιητικά του.

Υπάρχουν φυσικά και ορισμένα προβλήματα σχετικά με τη χρήση των έξυπνων καρτών, τα οποία έχουν να κάνουν κυρίως με την περιορισμένη, προς το παρόν, διάδοση των απαιτούμενων συσκευών ανάγνωσης (smart card readers), λόγω του υψηλού κόστους τους. Επίσης επικρατεί σχετική αβεβαιότητα για τα standards που θα πρέπει να ακολουθεί το λογισμικό που χρησιμοποιείται για τη λειτουργία τους. Ελπίζεται όμως ότι σύντομα τα προβλήματα αυτά θα ξεπεραστούν, δεδομένου του ρυθμού εξέλιξης της αντίστοιχης τεχνολογίας και έτσι τα συστήματα PKI θα μπορέσουν να επωφεληθούν από τις μεγάλες, πράγματι, δυνατότητες που προσφέρουν οι έξυπνες κάρτες.

8.7.4. Biometrics:

Οι βιομετρικές μέθοδοι θα μπορούσαν να χρησιμοποιηθούν για να ελέγξουν την πρόσβαση του χρήστη προς το ιδιωτικό του κλειδί, το οποίο βρίσκεται αποθηκευμένο σε μια έξυπνη κάρτα, υποκαθιστώντας πιθανόν την ανάγκη για την χρήση κάποιου PIN. Αυτό θα μπορούσε να υλοποιηθεί ως εξής: Η ειδική συσκευή ανάγνωσης (smart card reader) έχει πιο εξελιγμένα χαρακτηριστικά και είναι σε θέση να "διαβάσει" όχι μόνο την ίδια την έξυπνη κάρτα, αλλά και το βιομετρικό χαρακτηριστικό του χρήστη. Η έξυπνη κάρτα, επιπλέον των κρυπτογραφικών δεδομένων, φέρει προαποθηκευμένη και την "εικόνα αναφοράς" του υπό μέτρηση βιομετρικού χαρακτηριστικού, προς την οποία και συγκρίνει την "τιμή" που "διάβασε" από το χρήστη. Αν υπάρξει ταύτιση των δύο, τότε επιτρέπεται η πρόσβαση του χρήστη προς τα κρυπτογραφικά δεδομένα (ιδιωτικό κλειδί κλπ) που περιέχει η κάρτα. Σήμερα πάντως υπάρχουν μόνο πρόδρομες τεχνολογικές μορφές της πιο μεθόδου, δεδομένου ότι η πλήρης υλοποίηση απαιτεί εξαιρετικά ισχυρές κρυπτογραφικές κάρτες, που να μπορούν να επεξεργαστούν αυτόνομα και με επαρκή ταχύτητα τα βιομετρικά δεδομένα.

9. ΠΟΛΙΤΙΚΕΣ ΚΑΙ ΔΙΑΔΙΚΑΣΙΕΣ

9.1. Πολιτικές και διαδικασίες στο παραδοσιακό περιβάλλον

Στον παραδοσιακό κόσμο τα άτομα κινούνται ανάμεσα σε διαφορετικά περιβάλλοντα, στα οποία ποικίλες πολιτικές και διαδικασίες καθορίζουν την αλληλεπίδρασή τους με άλλους. Για παράδειγμα, οι κυβερνήσεις έχουν να αντιμετωπίσουν το θέμα της διασυνοριακής μετακίνησης και της μετανάστευσης. Για το σκοπό αυτό, υπάρχουν νομοθεσίες και πολιτικές, οι οποίες απαιτούν από όσους διασχίζουν σύνορα να κατέχουν διαβατήρια, τα οποία καθιερώνουν και αποδεικνύουν υπηκοότητα και ταυτότητα. Ένα διαβατήριο περιλαμβάνει ορισμένες πληροφορίες σχετικά με το άτομο, οι οποίες αποτυπώνονται σε ένα ειδικά σχεδιασμένο "έγγραφο", το οποίο έχει εκδοθεί από μια συγκεκριμένη αρχή και φέρει ένα χαρακτηριστικό αριθμό.

Η αρχή που εκδίδει τα διαβατήρια ακολουθεί ορισμένες πολιτικές και διαδικασίες κατά την έκδοσή τους. Οι διαδικασίες αυτές πιθανόν να απαιτούν από το πρόσωπο που επιθυμεί να αποκτήσει διαβατήριο, να παρουσιαστεί αυτοπροσώπως στο αρμόδιο γραφείο, να συμπληρώσει μια αίτηση επί χάρτου, να παρουσιάσει ορισμένα έγγραφα αποδεικτικά της ταυτότητάς του, να προσκομίσει φωτογραφίες, να υπογράψει ιδιοχείρως μια υπεύθυνη δήλωση και κατόπιν να αναμένει, μέχρις ότου όλες αυτές οι πληροφορίες εξετασθούν και επαληθευτούν. Αφού ολοκληρωθεί μια σειρά διαδικασιών και ελέγχων, που καθορίζονται από τις ισχύουσες πολιτικές, το άτομο θα παραλάβει το διαβατήριο με όποιο τρόπο καθορίζουν οι σχετικές πολιτικές (αυτοπροσώπως ή μέσω ταχυδρομείου).

Ακόμη, οι ισχύουσες πολιτικές πιθανόν να καθορίζουν και άλλα θέματα, πέρα από την ίδια την έκδοση του διαβατηρίου, όπως την υποχρέωση του ατόμου να φυλάσσει το διαβατήριο, να αναφέρει τυχόν απώλειά του, να κάνει σωστή χρήση του κλπ. Παράλληλα, οι άλλες χώρες, στις οποίες θα επιδειχθεί το διαβατήριο, έχουν τις δικές τους πολιτικές που διέπουν την αποδοχή του και πιθανόν να απαιτούν πρόσθετα έγγραφα, π.χ. μια βίζα, πριν επιτρέψουν την είσοδο στον κάτοχο του διαβατηρίου.

Επιπλέον, η χώρα που εκδίδει το διαβατήριο έχει ορίσει κάποια μέθοδο ανάκλησης ή απόσυρσης, όταν αυτό είναι αναγκαίο, ενώ τα διαβατήρια έχουν επίσης ημερομηνία λήξης της ισχύος τους, ώστε να διευκολύνεται η πιθανή αλλαγή πολιτικών της εκδίδουσας αρχής, αλλά και ο επανέλεγχος των στοιχείων του κατόχου, όπως και η αποτύπωση πιθανών αλλαγών σ' αυτά.

Τα παραπάνω αποτελούν παράδειγμα πολιτικών και διαδικασιών, που είτε προβλέπονται από τη νομοθεσία είτε έχουν εθιμικό χαρακτήρα. Η θέσπισή τους έχει σκοπό να διασφαλίσει ένα επίπεδο εμπιστοσύνης, επιτρέποντας τη διαχείριση κινδύνων που προκύπτουν ή σχετίζονται με ορισμένες δραστηριότητες. Επίσης είναι σαφής η ύπαρξη και ο ρόλος τριών διαφορετικών οντοτήτων:

- της αρχής που εκδίδει ένα διαβατήριο
- του κατόχου του διαβατηρίου και, τέλος,
- όσων στηρίζονται σ' αυτό.

Ανάλογες οντότητες καθώς και κανόνες και διαδικασίες που διέπουν τις σχέσεις μεταξύ των οντοτήτων υπάρχουν και σε ένα σύστημα PKI, όπως περιγράφεται αναλυτικότερα παρακάτω.

9.2. Πολιτικές και διαδικασίες σε ένα περιβάλλον PKI

Πολλές φορές η συζήτηση για ένα σύστημα PKI εστιάζεται στα τεχνολογικά χαρακτηριστικά του, δηλαδή στη χρήση κρυπτογραφίας δημοσίου κλειδιού και στα στοιχεία εξοπλισμού και λογισμικού που υλοποιούν ψηφιακές υπογραφές, επιβεβαίωση ταυτότητας, ακεραιότητα δεδομένων, εμπιστευτικότητα και μη αποκήρυξη.
Εντούτοις, οι τεχνολογίες αυτές, για να λειτουργήσουν αποδοτικά, απαιτούν μια συγκεκριμένη υποδομή (PKI: **Υποδομή** Δημοσίου Κλειδιού). Η υποδομή αυτή δεν αφορά μόνο κρυπτογραφική τεχνολογία και πρωτόκολλα επικοινωνίας, αλλά περιλαμβάνει και τις πολιτικές που ορίζουν και κατευθύνουν τη χρήση του PKI, τη διαχείριση κινδύνου και τις επιχειρηματικές διαδικασίες που είναι απαραίτητες, προκειμένου να καταστήσουν δυνατή τη λειτουργία των συστημάτων PKI και των εφαρμογών που εξυπηρετούν τις νέες ψηφιακές μορφές των συναλλακτικών σχέσεων, σε αντικατάσταση των αντίστοιχων παραδοσιακών.

Οπως είναι γνωστό, ένα περιβάλλον PKI στηρίζεται στην ύπαρξη ενός ζεύγους κλειδιών για κάθε χρήστη. Το ένα από αυτά, το ιδιωτικό, φυλάσσεται προσεκτικά από τον κάτοχό του. Το άλλο (το δημόσιο), συνδέεται με πληροφορίες (όνομα κλπ) που προσδιορίζουν την ταυτότητα του υποκειμένου, όπου το υποκείμενο είναι ο κάτοχος του ζεύγους "δημόσιο/ιδιωτικό κλειδί". Η σύνδεση των δύο αυτών στοιχείων (δημόσιο κλειδί / πληροφορίες που προσδιορίζουν ταυτότητα) καθίσταται δυνατή με το να περιληφθούν τα δύο ως άνω στοιχεία σε ένα ψηφιακού τύπου έγγραφο, το οποίο έχει συνήθως τη μορφή ενός αρχείου με κατάλληλη δομή και δημιουργείται με βάση ορισμένα ισχύοντα πρότυπα. Το έγγραφο αυτό αποτελεί το λεγόμενο ψηφιακό πιστοποιητικό (ή απλώς πιστοποιητικό) του χρήστη.

Στη συνέχεια, το ίδιο το πιστοποιητικό και το ζεύγος "δημόσιο/ιδιωτικό κλειδί" μπορούν να χρησιμοποιηθούν σε συστήματα και διαδικασίες, προκειμένου να εκπροσωπήσουν το άτομο (ή την οντότητα γενικώς) που είναι το υποκείμενο του πιστοποιητικού, σε ορισμένες μάλιστα περιπτώσεις είναι δυνατόν να χρησιμοποιηθούν για τη δημιουργία και την επαλήθευση ψηφιακών υπογραφών. Κατά συνέπεια, είναι εξαιρετικά σημαντικό για έναν τρίτο και συγκεκριμένα για την πλευρά που στηρίζεται στο πιστοποιητικό (relying party, σε αντιδιαστολή με τον κάτοχο του πιστοποιητικού) να μπορεί να έχει εμπιστοσύνη ότι το πιστοποιητικό προσδιορίζει με ορθό και ακριβή τρόπο το υποκείμενο (δηλ. τον κάτοχο) και το δημόσιο κλειδί του, καθώς και την ίδια την αρχή (Αρχή Πιστοποίησης-ΑΠ) που εκδίδει το πιστοποιητικό.

Με δεδομένη τη σπουδαιότητα της ορθής σύνδεσης "δημόσιου κλειδιού / υποκειμένου", η οποία σε ορισμένες περιπτώσεις θα πρέπει να τυγχάνει εγγυήσεως, είναι προφανής η ανάγκη να καθιερωθεί ένα σύνολο από πολιτικές. Οι πολιτικές αυτές θα πρέπει να καθορίζουν το

επίπεδο εμπιστοσύνης (level of trust) το οποίο εκπροσωπεί ένα πιστοποιητικό, όταν αυτό παρουσιάζεται/"προτείνεται" σε κάποιον που πρόκειται να το χρησιμοποιήσει και να στηριχθεί (relying party) στις πληροφορίες που το πιστοποιητικό ενσωματώνει. Το ως άνω επίπεδο εμπιστοσύνης συνδέεται απ' ευθείας με τις διαβεβαιώσεις που παρέχονται σχετικά με την όλη διαδικασία έκδοσης και διαχείρισης του πιστοποιητικού.

Οι πολιτικές θα πρέπει επίσης να καθορίζουν τις ευθύνες των εμπλεκομένων μερών στις διαδικασίες έκδοσης, διαχείρισης και επεξεργασίας των πιστοποιητικών. Ο ρόλος των πολιτικών σε ένα σύστημα PKI είναι κρίσιμος, δεδομένου ότι προσδιορίζουν το επίπεδο του κινδύνου που αντιμετωπίζουν όσοι στηρίζονται στα πιστοποιητικά. Παρ' όλα αυτά, οι πολιτικές σε ένα σύστημα PKI δεν είναι τίποτε το μυστηριώδες, καθώς σχετίζονται ευθέως με πολιτικές εμπιστοσύνης που είναι ήδη εν χρήσει στον παραδοσιακό κόσμο και πολλές φορές θεωρούνται δεδομένες.

9.3. Τα εμπλεκόμενα μέρη

Ο τρόπος υλοποίησης ενός συστήματος PKI αντανακλά συνήθως συγκεκριμένες απαιτήσεις πολιτικής, οι οποίες στοχεύουν στην εξυπηρέτηση όσων κάνουν χρήση των υπηρεσιών του συστήματος. Οπως και στα παραδοσιακά επιχειρηματικά περιβάλλοντα, υπάρχουν διάφορα εμπλεκόμενα μέρη, με ποικίλα συμφέροντα και, επομένως, πολλά ζητήματα τα οποία πρέπει να ρυθμιστούν μέσω κατάλληλων πολιτικών.

Σε ένα σύστημα PKI τα πιθανά μέρη που εμπλέκονται προκειμένου να επιτευχθεί το κατάλληλο επίπεδο εμπιστοσύνης, αναφορικά με τη δημιουργία και χρήση πιστοποιητικών δημοσίου κλειδιού περιλαμβάνουν:

- Το άτομο ή την οντότητα που προσδιορίζεται από το πιστοποιητικό (υποκείμενο, κάτοχος του πιστοποιητικού)
- Τον εκδότη (εκδίδουσα αρχή - Αρχή Πιστοποίησης) του πιστοποιητικού, του οποίου οι δραστηριότητες μπορεί να περιλαμβάνουν επίσης την επαλήθευση των στοιχείων που περιέχονται στο πιστοποιητικό (Αρχή Καταχώρησης -ΑΚ), πριν αυτό εκδοθεί
- Την οντότητα που παρέχει υπηρεσίες ελέγχου εγκυρότητας του πιστοποιητικού
- Την επιχείριση/οργανισμό/άτομο που στηρίζεται στο πιστοποιητικό (χρήστης - relying party)

Από τα παραπάνω αναφερθέντα μέρη, απαιτούνται τουλάχιστον τα εξής τρία, προκειμένου να υποστηρίξουν μια πολιτική PKI:

1. Αρχή Πιστοποίησης (ΑΠ)
2. Υποκείμενο (κάτοχος πιστοποιητικού - subject/subscriber)
3. Εξαρτώμενο μέρος - Χρήστης (η πλευρά που στηρίζεται στο πιστοποιητικό: relying party)

Οι αρμοδιότητες, τα καθήκοντα και οι ευθύνες των μερών αυτών διατυπώνονται στην πολιτική του PKI και πιο συγκεκριμένα σε μια "Πολιτική Πιστοποιητικών" (ή πολιτική πιστοποίησης).

9.4. Πολιτική Πιστοποιητικών - ΠΠ (Certificate Policy - CP)

Μια πολιτκή πιστοποιητικών είναι ένα συγκεκριμένο σύνολο κανόνων, που καθορίζει το κατά πόσο ένα πιστοποητικό μπορεί να χρησιμοποιηθεί από μια κοινότητα ή από μια κατηγορία εφαρμογών με κοινές απαιτήσεις ασφάλειας. Γενικότερα, η πολιτική πιστοποιητικών καθορίζει τους όρους και τις προϋποθέσεις χρήσης των πιστοποιητικών.

Σε πρακτικό επίπεδο, το εξαρτώμενο μέρος (δηλ. ο χρήστης - relying party) είναι αυτό που "δημιουργεί αξία", κατά συνέπεια ενδιαφέρεται περισσότερο για την πολιτική που διέπει τη δημιουργία και χρήση του πιστοποιητικού. Η πολιτική είναι το κύριο όχημα για να καθοριστεί το πότε ένα πιστοποιητικό είναι κατάλληλο για το σκοπό για τον οποίο παρουσιάζεται. Είναι κρίσιμο για το εξαρτώμενο μέρος (δηλαδή μια εφαρμογή λογισμικού ή ένα πρόσωπο), το πιστοποιητικό να προσδιορίζει ορθά και με ακρίβεια το υποκείμενο, το δημόσιο κλειδί του υποκειμένου και τα χαρακτηριστικά (διαπιστευτήρια) του εκδότη του πιστοποιητικού.

Μια δημόσια αρχή ή μια τράπεζα μπορεί, κατά τη διεξαγωγή συναλλαγών, να δέχεται πιστοποιητικά για σκοπούς όπως επαλήθευση ταυτότητας πελατών ή αποδοχής ψηφιακών υπογραφών. Αυτό γίνεται σύμφωνα με όσα καθορίζει η νομοθεσία, οι κανονισμοί, διάφορες γενικώς αποδεκτές πρακτικές και απαιτήσεις διαδικασιών ελέγχου. Οσο αυξάνει η αξία ή ο βαθμός ευαισθησίας των διαφόρων συναλλαγών, τόσο γίνεται πιο κρίσιμη η σημασία της πολιτικής που διέπει τις συναλλαγές. Οι σχετικές απαιτήσεις ποικίλλουν, ανάλογα με το σκοπό για τον οποίο χρησιμοποιείται το πιστοποιητικό.

Για παράδειγμα, ένας φορέας παροχής υπηρεσιών υγείας μπορεί να θεσπίσει πολιτικές σχετικά με την έκδοση και διαχείριση πιστοποιητικών που χορηγεί στο ιατρικό προσωπικό, π.χ. στους παθολόγους. Οι σχετικές απαιτήσεις θα είναι πολύ διαφορετικές από εκείνες που αφορούν έκδοση πιστοποιητικών σε απλούς εργαζόμενους που δεν συνταγογραφούν ελεγχόμενες φαρμακευτικές ουσίες. Οι χρήσεις των πιστοποιητικών μπορούν να είναι ποικίλες και κατά συνέπεια ο κίνδυνος που σχετίζεται με τη χρήση τους πρέπει να αντιμετωπιστεί μέσω των κατάλληλων απαιτήσεων που περιλαμβάνονται σε μια πολιτική.

Οι Αρχές Πιστοποίησης (ΑΠ) παίζουν σημαντικό ρόλο στην καθιέρωση πολιτικής πιστοποιητικών. Για παράδειγμα, μια ΑΠ είναι δυνατόν να συνεργαστεί με μια ομάδα επιχειρήσεων ή έναν τομέα της βιομηχανίας, προκειμένου να εκπονήσει μια πολιτική πιστοποιητικών βασισμένη σε ένα μοντέλο που θεωρείται κατάλληλο για τον τομέα αυτό. Τα εξαρτώμενα μέρη (relying parties) μπορούν στη συνέχεια να συντάξουν τις δικές τους επιμέρους πολιτικές, που ουσιαστικά θα αντανακλούν το συγκεκριμένο μοντέλο.

Σε άλλες περιπτώσεις, οι Αρχές Πιστοποίησης πιθανόν να πρέπει να ορίσουν, με δική τους πρωτοβουλία, μια συγκεκριμένη πολιτική. Για παράδειγμα, οι εκδότες πιστοποιητικών τα οποία χρησιμοποιούνται για την επαλήθευση ταυτότητας των Web servers μέσω του

πρωτοκόλλου SSL (Secure Sockets Layer) μπορούν να ζητούν, μεταξύ άλλων, τα έγγραφα σύστασης της εταιρίας που λειτουργεί τον Web server και αιτείται το πιστοποιητικό ή και άλλα επίσημα έγγραφα, πριν εκδόσουν το πιστοποιητικό. Τα εξαρτώμενα μέρη, είτε είναι μεμονωμένοι χρήστες είτε υπάλληλοι άλλων εταιριών, μπορούν στη συνέχεια να προσπελαύνουν τον υπ' όψη Web server, έχοντας την πεποίθηση ότι αυτός πράγματι ανήκει στην πιο πάνω εταιρία, αλλά δεν σημαίνει ότι θα πρέπει να έχουν άγνοια των πολιτικών, βάσει των οποίων έχει γίνει η έκδοση του πιστοποιητικού.

Η καθιέρωση μιας πολιτικής συνοδεύεται συνήθως από την απονομή σ' αυτήν ενός αριθμού ταυτότητας (αναγνωριστικό αντικειμένου - object identifier-OID), ο οποίος έχει μια συγκεκριμένη δομή τύπου ASN.1. Στη συνέχεια, τα πιστοποιητικά που εκδίδονται μπορούν να κάνουν αναφορά σ' αυτήν με τη βοήθεια του πιο πάνω αριθμού. Ετσι, τα εξαρτώμενα μέρη έχουν τη δυνατότητα να συμβουλεύονται την αντίστοιχη πολιτική, προκειμένου να αποφασίσουν για το κατά πόσο το υπό εξέταση πιστοποιητικό είναι αποδεκτό από αυτά για το σκοπό της συγκεκριμένης συναλλαγής.

9.5. Δήλωση Διαδικασιών Πιστοποίησης - ΔΔΠ (Certification Practice Statement - CPS)

Μια Αρχή Πιστοποίησης ακολουθεί συγκεκριμένες διαδικασίες κατά την έκδοση και γενικά τη διαχείριση των πιστοποιητικών. Η "δήλωση διαδικασιών πιστοποίησης" είναι ακριβώς μια περιγραφή των διαδικασιών που εφαρμόζει μια ΑΠ κατά την έκδοση των πιστοποιητικών. Η δήλωση αυτή περιγράφει με σαφήνεια τα μέτρα που εφαρμόζει μια ΑΠ για τη διαχείριση του κύκλου ζωής των πιστοποιητικών, για να ελέγξει τα στοιχεία των υποψηφίων που ζητούν πιστοποιητικά και για να περιγράψει τις σχετικές τεχνικές, διοικητικές και νομικές απαιτήσεις που συνεισφέρουν στην αξιοπιστία της ΑΠ. Το ακριβές περιεχόμενο μιας ΔΔΠ ποικίλλει και εξαρτάται απο μια σειρά παράγοντες, όπως:

- τις παρεχόμενες υπηρεσίες
- τις εφαρμογές που υποστηρίζονται
- το περιβάλλον
- την αρχιτεκτονική ασφάλειας
- άλλους παράγοντες

Με δεδομένες τις ανεπάρκειες στη σχετική με ψηφιακές υπογραφές και πιστοποιητικά νομοθεσία, μια ΔΔΠ είναι απαραίτητη, προκειμένου να καλύψει τα πιθανά κενά και να δημιουργήσει τη νομική βεβαιότητα που απαιτείται, ώστε να λειτουργήσουν ορθά οι αντίστοιχες υπηρεσίες πιστοποίησης.

Σε ένα περιβάλλον ηλεκτρονικού εμπορίου, η ενδεχόμενη εμπλοκή πολλών οντοτήτων (βλ. και παραπάνω) με ποικίλες σχέσεις δημιουργεί σύνθετα νομικά ζητήματα, τα οποία πρέπει να τύχουν της δέουσας προσοχής. Κατά συνέπεια, μια σοβαρή και υπεύθυνη ΔΔΠ θα πρέπει να περιλαμβάνει, μεταξύ άλλων, σαφή και πλήρη περιγραφή των δικαιωμάτων και υποχρεώσεων

των εμπλεκομένων μερών και συστηματική καταγραφή των ακολουθουμένων λειτουργικών διαδικασιών και του τεχνολογικού εξοπλισμού που χρησιμοποιείται.

9.6. Σχέση μεταξύ Πολιτκής Πιστοποιητικών (ΠΠ) και Δήλωσης Διαδικασιών Πιστοποίησης (ΔΔΠ)

Η διάκριση ανάμεσα σε ΠΠ και ΔΔΠ δεν είναι απόλυτα σαφής. Η γενική ιδέα είναι ότι μια ΔΔΠ είναι πολύ πιο λεπτομερής από μια ΠΠ και μπορεί να υποστηρίζει πολλαπλές ΠΠ. Με άλλα λόγια, μια ΠΠ αναφέρεται συνήθως στο "τι πρέπει να γίνεται", ενώ μια ΔΔΠ περιγράφει το "πώς πρέπει να γίνεται". Συγκεκριμένα:

- Απαιτήσεις και διαδικασίες: Μια ΠΠ αποτελεί μια δήλωση απαιτήσεων, ενώ μια ΔΔΠ είναι μια δήλωση διαδικασιών. Για παράδειγμα, μια ΠΠ μπορεί να καθορίζει το επίπεδο βεβαιότητας που σχετίζεται με μια κατηγορία πιστοποιητικών και η αντίστοιχη ΔΔΠ να προσδιορίζει τα χαρακτηριστικά και την υποδομή που θα διασφαλίσουν το ζητούμενο επίπεδο βεβαιότητας.

- Βαθμός εξειδίκευσης: Η ΔΔΠ είναι πιο αναλυτική και εκτεταμένη σε ό,τι αφορά τις ακολουθούμενες από μια ΑΠ διαδικασίες, σε σχέση με την αντίστοιχη ΠΠ. Για το λόγο αυτό, σε ορισμένα περιβάλλοντα, γίνεται χρήση μιας περίληψης της ΔΔΠ, η οποία περιλαμβάνει αφ' ενός τα πιο κρίσιμα σημεία της και αφ' ετέρου μια αναφορά στο πλήρες κείμενο της ΔΔΠ.

- Πεδίο εφαρμογής: Ο ορισμός του είναι συνήθως στη διακριτική ευχέρεια της δημοσιεύουσας αρχής (π.χ. ΑΠ), λαμβάνοντας υπ' όψη τη σχετική νομοθεσία και τις απαιτήσεις αυτών που θα εξυπηρετήσει. Κατά κανόνα, μια ΠΠ καλύπτει παρόμοια θέματα με μια ΔΔΠ, αλλά σε γενικότερο επίπεδο και μικρότερο βαθμό λεπτομέρειας, επειδή πιθανόν προσπαθεί να εξασφαλίσει διαλειτουργικότητα μεταξύ διαφορετικών κοινοτήτων.

- Αλληλοσυσχέτιση: Μια ΔΔΠ μπορεί να καλύπτει πολλές ΠΠ, αν π.χ. η ΑΠ υποστηρίζει πολλές διαφορετικές εφαρμογές ή πολλές κοινότητες. Από την άλλη, είναι πιθανόν πολλές ΑΠ (με διαφορετικές μεταξύ τους ΔΔΠ) να είναι προσαρμοσμένες σε μια κοινή ΠΠ.

- "Πατρότητα": Μια ΠΠ δεν συσχετίζεται κατ' ανάγκη με μια ΑΠ, αλλά μπορεί να έχει δημιουργηθεί από μια κοινότητα, η οποία κάνει χρήση των υπηρεσιών πιστοποίησης που προσφέρει ένας τρίτος φορέας. Αντίθετα, μια ΔΔΠ προέρχεται από μια ΑΠ.

Συμπερασματικά, θα μπορούσε να λεχθεί ότι η ΠΠ αφορά περισσότερο εκείνους, οι οποίοι είναι υπεύθυνοι για αποφάσεις σχετικά με το πόσο ασφαλής είναι η χρήση των πιστοποιητικών από τις διάφορες εφαρμογές, ενώ η ΔΔΠ σχετίζεται άμεσα με την ΑΠ, δηλαδή με αυτόν που δημιουργεί και εκδίδει τα πιστοποιητικά, έχοντας και την ευθύνη για την ασφάλεια των αντίστοιχων διαδικασιών και λειτουργιών.

9.7. Δομή ΠΠ/ΔΔΠ

Η δομή και τα ακριβή περιεχόμενα ενός κειμένου τύπου ΠΠ ή ΔΔΠ εξαρτώνται από πολλούς παράγοντες, όπως οι υποστηριζόμενες εφαρμογές, ο βαθμός επιδιωκόμενης ασφάλειας, οι απαιτήσεις αυτών που θα συμμετάσχουν στο υπ' όψη σύστημα PKI και τα νομικά αποτελέσματα που θα πρέπει να διασφαλίζονται από τις παρεχόμενες υπηρεσίες πιστοποίησης. Είναι δυνατόν να ακολουθηθούν διάφορες προσεγγίσεις, όπως:

- Λεπτομερής καταγραφή των δικαιωμάτων και υποχρεώσεων κάθε εμπλεκόμενου μέρους (ΑΠ, κάτοχοι πιστοποιητικών, εξαρτώμενα μέρη) χωριστά. Η μορφή αυτή είναι οικεία στους νομικούς για την σύνταξη συμβάσεων.

- Αντιμετώπιση των δικαιωμάτων και υποχρεώσεων των εμπλεκομένων μερών με τη σειρά που αυτές θα ανακύψουν φυσιολογικά, κατά τη διάρκεια του κύκλου ζωής των πιστοποιητικών. Συγκεκριμένα, καλύπτονται με τη σειρά τα θέματα που αφορούν την ίδρυση μιας ΑΠ και στη συνέχεια η αίτηση χορήγησης πιστοποιητικού, ο έλεγχος εγκυρότητας των στοιχείων που αυτή περιλαμβάνει, η έκδοση του πιστοποιητικού, η χρήση του, η πιθανή ανάκλησή του και η λήξη της ισχύος του.

- Συμμόρφωση με τις κατευθυντήριες γραμμές που προτείνονται από το διεθνώς αναγνωρισμένο σχετικό κείμενο (IETF/RFC2527). Η σύνταξη των ΠΠ και των ΔΔΠ με βάση το πρότυπο αυτό διευκολύνει τη σύγκριση των διαφόρων κειμένων αυτής της κατηγορίας και επιτρέπει να εντοπίζονται ομοιότητες και διαφορές. Αυτό μπορεί να αποδειχθεί ιδιαίτερα χρήσιμο, όταν ένας οργανισμός προσπαθεί να αξιολογήσει τις διαδικασίες και πρακτικές άλλων οργανισμών, σε σχέση με τις δικές του. Επιπλέον, η προσέγγιση αυτή είναι πιθανόν η καλύτερη, όταν επιδιώκεται διαλειτουργικότητα μεταξύ διαφορετικών συστημάτων PKI.

Η γενική δομή ενός κειμένου τύπου ΠΠ/ΔΔΠ, σύμφωνα με τον πιο πάνω οδηγό (IETF/RFC2527) είναι η εξής:

- Εισαγωγή: Αναφέρει το ποιοί μπορούν να χρησιμοποιήσουν τα εκδιδόμενα πιστοποιητικά (π.χ. μόνο οι εργαζόμενοι μιας επιχείρησης/οργανισμού ή τα μέλη μιας ευρύτερης κοινότητας, η οποία πρέπει να προσδιορίζεται), καθώς και τους σκοπούς για τους οποίους τα πιστοποιητικά μπορούν να χρησιμοποιηθούν (π.χ. μόνο για μηνύματα ηλεκτρονικού ταχυδρομείου ή για τη διενέργεια ηλεκτρονικών συναλλαγών συγκεκριμένης αξίας κλπ).

- Γενικές διατάξεις: Εδώ αναφέρονται τα σχετικά με τις εγγυήσεις που παρέχονται από τις Αρχές Πιστοποίησης και τις Αρχές Καταχώρησης, τυχόν περιορισμοί ευθύνης, ρυθμίσεις που αφορούν εμπιστευτικότητα και προστασία πνευματικής ιδιοκτησίας, καθώς και άλλα νομικής φύσεως θέματα.

- Προσδιορισμός ταυτότητας και αντίστοιχες διαδικασίες επαλήθευσης: Περιγράφονται οι διαδικασίες που ακολουθούνται από την ΑΠ (ή και την ΑΚ) για τη συλλογή και

επαλήθευση των απαιτούμενων στοιχείων ταυτότητας του υποψηφίου, προκειμένου να εκδοθεί το αντίστοιχο πιστοποιητικό. Επίσης, τα στοιχεία που χρησιμοποιούνται για τον προσδιορισμό του ονόματος που θα αναφέρεται στο πιστοποιητικό.

- Λειτουργικές απαιτήσεις: Αυτές αναφέρονται στον "κύκλο ζωής" του πιστοποιητικού και περιγράφουν, για παράδειγμα, τις διαδικασίες υποβολής αίτησης, έκδοσης και πιθανής ανάκλησης του πιστοποιητικού, τον τρόπο τήρησης σχετικών αρχείων (προκειμένου να διευκολύνονται οι αντίστοιχοι έλεγχοι) κλπ.

- Φυσικοί και διαδικαστικοί έλεγχοι, καθώς και έλεγχοι προσωπικού: Αναφέρονται τα λαμβανόμενα μέτρα που αφορούν την ασφάλεια των εγκαταστάσεων και τον έλεγχο πρόσβασης σ' αυτές, τα μέτρα ασφαλείας για την πρόσβαση στα μέσα φύλαξης των κρυπτογραφικών κλειδιών, τους ελέγχους για την πρόσβαση στο σύστημα μέσω δικτύου. Εδώ περιλαμβάνονται και τα μέτρα που αφορούν το προσωπικό, όπως αξιολόγηση, εκπαίδευση, εναλλαγή σε θέσεις εργασίας, κατάλληλη επιτήρηση, αλλά και κυρώσεις σε περίπτωση παραβίασης των δεδομένων εξουσιοδοτήσεων.

- Ελεγχοι ασφαλείας τεχνικής φύσεως: Περιλαμβάνονται μέτρα προστασίας της διαδικασίας δημιουργίας κλειδιών, δυνατότητες και μηχανισμοί ανάκτησης των κλειδιών σε περιπτώσεις ανάγκης, μέτρα προστασίας των ιδιωτικών κλειδιών υπογραφής κλπ.

- Δομή και περιεχόμενο των πιστοποιητικών και των πινάκων ανάκλησης πιστοποιητικών: Περιγράφονται αναλυτικά οι πληροφορίες που περιλαμβάνονται στα πιστοποιητικά, καθώς και οι τυχόν επεκτάσεις (σύμφωνα πάντα με τα πρότυπα) που έχουν υλοποιηθεί. Επίσης παρέχονται οι αντίστοιχες πληροφορίες σχετικά με τους πίνακες ανάκλησης πιστοποιητικών, εφ' όσον χρησιμοποιούνται.

- Καθορισμός τρόπου διαχείρισης: Εδώ καθορίζεται η διαδικασία διαχείρισης-συντήρησης της συγκεκριμένης πολιτικής, δηλαδή με ποιό τρόπο θα γίνονται τυχόν απαιτούμενες αλλαγές, ποιός θα τις εγκρίνει, ποιοί πρέπει να ενημερώνονται γι' αυτές (κάτοχοι και χρήστες πιστοποιητικών, άλλα συστήματα PKI με τα οποία υπάρχει συνεργασία) και με τι χρονικό περιθώριο.

9.8. Αλλα έγγραφα

Σε ορισμένες περιπτώσεις, μια πολιτική πιστοποιητικών πιθανόν να μην είναι νομικά δεσμευτική. Για το λόγο αυτό, οι Αρχές Πιστοποίησης που εκδίδουν τα πιστοποιητικά ζητούν πολλές φορές από τα άλλα εμπλεκόμενα μέρη να δεσμευτούν με επιπλέον συμφωνίες, όπως:

- η Σύμβαση Εξαρτώμενου Μέρους (Relying Party Agreement), που αφορά τους χρήστες των πιστοποιητικών και
- η Σύμβαση Υποκειμένου (Subscriber Agreement) που αφορά τους κατόχους των πιστοποιητικών.

Αυτό συμβαίνει, διότι μια πολιτική πιστοποιητικών έχει μικρή αξία αν δεν περιλαμβάνει ρητές αναφορές στην υπάρχουσα νομική υποδομή και τους κανονισμούς και τις διαδικασίες που υποστηρίζουν τις διάφορες συναλλαγές. Προς την κατεύθυνση αυτή, οι πρόσθετες συμφωνίες διαμορφώνουν μια νομική βάση για τον καθορισμό των υποχρεώσεων και ευθυνών των εμπλεκομένων μερών.

Για παράδειγμα, μια πολιτική πιθανόν να απαιτεί από ένα κάτοχο πιστοποιητικού να αποδεχθεί ορισμένες υπευθυνότητες σχετικά με τη χρήση του πιστοποιητικού ή σχετικά με την προστασία του αντίστοιχου ιδιωτικού κλειδιού. Αν και η πολιτική πιθανόν να δηλώνει αυτές τις απαιτήσεις, η επιβολή αυτών των όρων μπορεί να απαιτεί την σύναψη μιας νομικά δεσμευτικής σύμβασης ανάμεσα στην Αρχή Πιστοποίησης και τον κάτοχο του πιστοποιητικού. Μια τέτοια σύμβαση πιθανόν να είναι απαραίτητη, αφ' ενός για να καθορίσει τις υποχρεώσεις του κατόχου και αφ' ετέρου για να θεσπίσει ένα μηχανισμό επιβολής τους, στην περίπτωση που αυτές παραβιαστούν. Προφανώς η νομική ευθύνη του κατόχου του πιστοποιητικού προκύπτει σαν αποτέλεσμα αυτής της σύμβασης.

Αντίστοιχα μια σύμβαση Εξαρτώμενου Μέρους μπορεί, μεταξύ άλλων, να καθορίζει το είδος των συναλλαγών για τις οποίες μπορεί να χρησιμοποιηθεί ένα πιστοποιητικό ή να θέτει ένα όριο στην αξία των συναλλαγών που μπορούν να πραγματοποιηθούν με αυτό.

9.9. Διαχείριση πολιτικών και μοντέλα PKI

Με βάση τα παραπάνω, για την υλοποίηση ενός συστήματος PKI προτείνονται τα εξής μοντέλα:

1. Ενδοεταιρικό μοντέλο (Enterprise model)
Στην περίπτωση αυτή, μια επιχείρηση η οποία διαθέτει πλήθος εγκαταστάσεων, περιφερειακών γραφείων, υποκαταστημάτων κλπ, χρησιμοποιεί ένα σύστημα PKI προκειμένου να προσφέρει στους εργαζόμενους ελεγχόμενη πρόσβαση στα διάφορα πληροφοριακά συστήματα και εφαρμογές. Η πρόσβαση μπορεί να αφορά υπηρεσίες ηλεκτρονικού ταχυδρομείου και Web, χρήση εξειδικευμένων εφαρμογών, προσπέλαση σε βάσεις δεδομένων της επιχείρησης κλπ. Το σχήμα περιλαμβάνει μια "εσωτερική" Αρχή Πιστοποίησης, η οποία λειτουργεί στα πλαίσια της εταιρίας και εκδίδει πιστοποιητικά για τους εργαζόμενους. Χωρίς την υποστήριξη PKI, θα απαιτούνταν, μεταξύ άλλων, η διαχείριση ενός μεγάλου αριθμού passwords, διαφορετικών για κάθε υποσύστημα. Εννοείται ότι προϋπόθεση εφαρμογής του μοντέλου αυτού είναι η ύπαρξη δικτυακής υποδομής τύπου "Intranet".
Το μοντέλο αυτό προσφέρει, μεταξύ άλλων, απλουστευμένη πολιτική πιστοποιητικών και ευκολία διαχείρισης σε τεχνικό επίπεδο. Είναι όμως αμφίβολο αν θα μπορέσει πάντα να ανταποκριθεί στις ποικίλες επιχειρηματικές απαιτήσεις, που πιθανόν να προκύψουν.

2. Μοντέλο εμπορικών εταίρων (Trading Partner model)

Το μοντέλο αυτό εφαρμόζεται όταν μια σειρά από περιφερειακές επιχειρήσεις έχουν συνεργασία με ένα κεντρικό οργανισμό ή επιχείρηση, η οποία εκδίδει ήδη πιστοποιητικά. Η αρχή πιστοποίησης λειτουργεί στα πλαίσια και υπό τον έλεγχο της κεντρικής επιχείρησης και απαραίτητη προϋπόθεση είναι η ύπαρξη δικτυακής υποδομής (π.χ. τύπου "Extranet") που να επιτρέπει τη διασύνδεση των συμμετεχόντων.
Ενα παράδειγμα της κατηγορίας αυτής θα μπορούσε να είναι η περίπτωση μιας αυτοκινητοβιομηχανίας (έστω Α), η οποία υλοποιεί το δικό της σύστημα PKI και μέσω αυτού εκδίδει πιστοποιητικά στους προμηθευτές της, προκειμένου αυτοί να έχουν ελεγχόμενη πρόσβαση στα πληροφοριακά συστήματα της επιχείρησης. Στην πράξη, το μοντέλο αυτό μπορεί να παρουσιάσει αδυναμίες, όπως στην περίπτωση που ορισμένοι από τους προμηθευτές συνεργάζονται π.χ. και με άλλες δύο αυτοκινητοβιομηχανίες (έστω Β και Γ), κάθε μια από τις οποίες έχει υλοποιήσει το δικό της σύστημα PKI. Τότε οι προμηθευτές θα πρέπει να αποκτήσουν ένα πιστοποιητικό από κάθε αυτοκινητοβιομηχανία ή θα πρέπει να αναπτυχθεί μια λύση, σύμφωνα με την οποία η Α να αποδέχεται τα πιστοποιητικά της Β κλπ. Προς το παρόν, η πιο συχνή προσέγγιση στις περιπτώσεις αυτές είναι το εξαρτώμενο μέρος να εμπιστεύεται πολλούς εκδότες πιστοποιητικών.

3. Μοντέλο κοινότητας ενδιαφέροντος (Community of Interest model)

Στην περίπτωση αυτή, το σύστημα PKI λειτουργεί για την έκδοση πιστοποιητικών, τα οποία χρησιμοποιούνται από τα λεγόμενα "εξουσιοδοτημένα εξαρτώμενα μέρη (authorized relying parties-ARP)", στα πλαίσια μιας ευρύτερης κοινότητας ενδιαφέροντος (π.χ. υπηρεσιών υγείας, οικονομικών υπηρεσιών).

Στο μοντέλο αυτό, τα "εξουσιοδοτημένα εξαρτώμενα μέρη" εμπιστεύονται έναν ή περισσότερους εκδότες πιστοποιητικών (αρχές πιστοποίησης), οι οποίοι εκδίδουν πιστοποιητικά για τα μέλη μιας συγκεκριμένης κοινότητας. Το σχήμα βασίζεται στην εκπόνηση μιας κοινής πολιτικής πιστοποιητικών (Certificate Policy), η οποία υποστηρίζεται νομικά με κατάλληλες συμβάσεις. Οι σχετικοί κανόνες καθορίζονται από τα "εξουσιοδοτημένα εξαρτώμενα μέρη" (δεδομένου ότι αυτοί αναλαμβάνουν τη μεγαλύτερη ευθύνη με την αποδοχή των πιστοποιητικών) και δεσμεύουν όλα τα εμπλεκόμενα μέρη: αρχές πιστοποίησης, κατόχους πιστοποιητικών και εξαρτώμενα μέρη. Το μοντέλο αυτό είναι ιδιαίτερα αποτελεσματικό, καθώς διευκολύνει, για τα εξαρτώμενα μέρη, τη διαδικασία λήψης αποφάσεων κατά την αποδοχή ενός πιστοποιητικού. Εντούτοις, η εκπόνηση της κοινής πολιτικής πιστοποιητικών και της αντίστοιχης συμβατικής υποδομής απαιτεί χρόνο και συγκεντρωμένη προσπάθεια από την πλευρά των εξαρτώμενων μερών που συναποτελούν την κοινότητα ενδιαφέροντος.

Γενικά, οι υπεύθυνοι για την υλοποίηση ενός συστήματος PKI θα πρέπει να εκτιμήσουν τις απαιτήσεις της πολιτικής πιστοποιητικών, προτού προχωρήσουν στην επιλογή του κατάλληλου μοντέλου, καθώς όλα έχουν πλεονεκτήματα, αλλά και μειονεκτήματα.

9.10. Άλλα θέματα σχετικά με πολιτικές πιστοποιητικών

Τα συστήματα PKI είναι μια σχετικά νέα τεχνολογία, η οποία βρίσκεται ακόμη σε εξέλιξη. Παράλληλα, νέες εφαρμογές που χρησιμοποιούν την τεχνολογία αυτή προστίθενται συνεχώς, έχοντας τις δικές τους απαιτήσεις. Επομένως προκύπτουν διάφορα θέματα σχετικά με τις πολιτικές πιστοποιητικών, τα οποία θα πρέπει να επιλυθούν.

Για παράδειγμα, ένα σημαντικό ζήτημα αφορά τις περιπτώσεις χρήσης από τρίτους ενός πιστοποιητικού που έχει εκδοθεί προκειμένου να χρησιμοποιηθεί για συγκεκριμένο σκοπό και στα πλαίσια μιας ομάδας εξαρτώμενων μερών. Με δεδομένο ότι η δομή ενός πιστοποιητικού υπακούει σε ευρέως αποδεκτά πρότυπα (X.509, PKIX) και ότι αυξάνεται διαρκώς η διαλειτουργικότητα των διαφόρων προϊόντων λογισμικού PKI, είναι δυνατόν το ως άνω πιστοποιητικό να γίνει αποδεκτό και να χρησιμοποιηθεί από μια εταιρία, η οποία δεν ανήκει στην προαναφερθείσα ομάδα εξαρτωμένων μερών. Η τρίτη αυτή εταιρία δεν είναι εξουσιοδοτημένη για χρήση του πιστοποιητικού, οπότε μπορούν να προκύψουν νομικά ζητήματα, σε περιπτώσεις πρόκλησης ζημιών από τη χρήση του πιστοποιητικού. Τα ζητήματα αυτά δεν είναι πάντα δυνατόν να αντιμετωπιστούν απλώς και μόνο μέσω μιας πολιτικής πιστοποιητικών. Προς την κατεύθυνση της επίλυσης τέτοιου είδους προβλημάτων έχει αναπτυχθεί η έννοια του "εξουσιοδοτημένου εξαρτώμενου μέρους" (βλ. και παραπάνω), το οποίο δεσμεύεται συμβατικά να αποδέχεται μόνο συγκεκριμένους τύπους πιστοποιητικών.

Ενα άλλο θέμα αφορά αυτή καθ' εαυτή τη φύση των πιστοποιητικών. Για παράδειγμα, η Ευρωπαϊκή Ενωση έχει εισάγει τα λεγόμενα "αναγνωρισμένα πιστοποιητικά". Οι προϋποθέσεις δημιουργίας και χρήσης αυτών των πιστοποιητικών έχουν καθοριστεί έτσι ώστε να εξασφαλίζουν τη δυνατότητα μη αποκήρυξης σε συναλλαγές υψηλής ασφάλειας. Τα αντίστοιχα τεχνικά πρότυπα για τα πιστοποιητικά αυτά είναι υπό διαμόρφωση (IETF draft).

Ενδιαφέρον επίσης παρουσιάζει το ενδεχόμενο της αυτόματης (χωρίς τη μεσολάβηση του χρήστη) αξιολόγησης ενός πιστοποιητικού και της πολιτικής που συσχετίζεται με αυτό. Κάτι τέτοιο προϋποθέτει παραπέρα προτυποποίηση και κωδικοποίηση των πολιτικών και εμπλουτισμό του σχετικού λογισμικού με αντίστοιχες δυνατότητες.

Τέλος, ορισμένα ακόμη ζητήματα αφορούν την προστασία των δεδομένων προσωπικού χαρακτήρα, που συλλέγονται από την Αρχή Πιστοποίησης κατά την αρχική φάση της έκδοσης πιστοποιητικού, το είδος των πληροφοριών που χρησιμοποιούνται σε ένα πιστοποιητικό για να προσδιορίσουν την ταυτότητα του κατόχου, καθώς και την εν γένει εξέλιξη της σχετικής νομοθεσίας των διαφόρων χωρών και κατά πόσο γίνεται διάκριση ανάμεσα σε ηλεκτρονικές υπογραφές γενικά και σε ψηφιακές υπογραφές ασύμμετρης κρυπτογραφίας ειδικότερα.

10. ΥΛΟΠΟΙΗΣΗ ΑΠ – ΕΝΑΛΛΑΚΤΙΚΕΣ ΕΠΙΛΟΓΕΣ

Οπως έχει ήδη εξηγηθεί αναλυτικά στα προηγούμενα, ένα περιβάλλον PKI στηρίζεται κατά κύριο λόγο στην ύπαρξη και λειτουργία μιας (ή περισσοτέρων) Αρχής Πιστοποίησης (ΑΠ). Η ΑΠ αποτελεί την καρδιά του PKI συστήματος, μπορεί να διαμορφωθεί με ποικίλους τρόπους και παρέχει μια σειρά από υπηρεσίες, απαραίτητες για την αξιοποίηση των δυνατοτήτων του PKI. Κατά συνέπεια, μια επιχείρηση ή ένας οργανισμός που ενδιαφέρεται για την ανάπτυξη ενός PKI περιβάλλοντος θα πρέπει, μεταξύ άλλων, να αποφασίσει για το πώς ακριβώς θα παρέχονται οι σχετικές υπηρεσίες ΑΠ μέσα στο υπό ανάπτυξη περιβάλλον. Οι κυριότερες επιλογές στο σημείο αυτό μπορούν να συνοψισθούν στις εξής τρεις:

1. Χρήση υπηρεσιών Αρχής Πιστοποίησης εμπορικού τύπου (ΑΠ Δημόσιας Χρήσης – public CA)
2. Δημιουργία και χρήση ιδιόκτητης ΑΠ (in-house CA)
3. Εκχώρηση των λειτουργιών ΑΠ σε τρίτους (outsourced CA)

Κάθε μια από τις λύσεις αυτές παρουσιάζει συγκεκριμένα πλεονεκτήματα και εξυπηρετεί διαφορετικού τύπου απαιτήσεις. Μια επιχείρηση είναι δυνατόν να ξεκινήσει υιοθετώντας μια από τις επιλογές και στη συνέχεια να μεταπηδήσει σε κάποια άλλη ή ακόμη και να συνδυάσει τη χρήση περισσοτέρων από μια επιλογές.

10.1. Υπηρεσίες ΑΠ Δημόσιας Χρήσης (public CAs)

Μια ΑΠ δημόσιας χρήσης εκδίδει ψηφιακά πιστοποιητικά προς το κοινό γενικώς, ανεξάρτητα από το αν οι ενδιαφερόμενοι ανήκουν σε κάποιο οργανισμό ή επιχείρηση. Τα πιστοποιητικά αυτά προορίζονται για χρήση μέσα σε ένα δημόσιο περιβάλλον. Η περίπτωση αυτή είναι ανάλογη με τη χρήση ενός δημόσιου συστήματος παροχής ηλεκτρικής ενέργειας, αντί για τη δημιουργία ιδιόκτητων εγκαταστάσεων παραγωγής και διανομής ενέργειας εκ μέρους της ενδιαφερόμενης εταιρίας.

Το σπουδαιότερο ζήτημα στην περίπτωση αυτή είναι ότι απαιτείται η έκδοση ψηφιακών ταυτοτήτων για ένα πλήθος οντοτήτων, των οποίων τα στοιχεία δεν είναι συνήθως γνωστά εκ των προτέρων. Αντίθετα, στα στενά πλαίσια μιας επιχείρησης, υπάρχουν αρκετές πληροφορίες, αλλά και σχετική βεβαιότητα, για την ταυτότητα ενός χρήστη, π.χ. η γνώση που έχει για το συγκεκριμένο χρήστη ο προϊστάμενος του, οι αντίστοιχες πληροφορίες που διαθέτει το τμήμα προσωπικού κλπ.

Επομένως, σε ό, τι αφορά την έκδοση πιστοποιητικών προς τη μεγάλη μάζα των χρηστών του Internet, έχει μεγάλη σημασία η μέθοδος που ακολουθείται για την εξακρίβωση των στοιχείων των υποψηφίων κατόχων ψηφιακών πιστοποιητικών. Το μέγεθος της προσπάθειας (από την πλευρά της ΑΠ) προς την κατεύθυνση αυτή έχει άμεση σχέση με το βαθμό εμπιστοσύνης που μπορεί να έχει κάποιος για τα εκδιδόμενα πιστοποιητικά. Το πρόβλημα

αντιμετωπίζεται με την θέσπιση των λεγομένων κατηγοριών πιστοποιητικών (certificate classes), οι οποίες, μεταξύ άλλων, αντιπροσωπεύουν και διαφορετικά επίπεδα εμπιστοσύνης, ανάλογα με την κρισιμότητα των επιμέρους περιοχών εφαρμογής του κάθε πιστοποιητικού (βλ. και Κεφ. 6, κατηγορίες πιστοποιητικών). Το όλο σχήμα περιγράφεται στη Δήλωση Διαδικασιών Πιστοποίησης – ΔΔΠ (Certification Practice Statement) που εκπονεί η αντίστοιχη ΑΠ. Η πιο πάνω ΔΔΠ θα πρέπει να μελετηθεί προσεκτικά από την επιχείρηση που ενδιαφέρεται να κάνει χρήση των υπηρεσιών της υπ' όψη ΑΠ, ενώ παράλληλα η επιχείρηση θα πρέπει να εκπονήσει τη δική της Πολιτική Πιστοποιητικών (Certificate Policy).

Το μεγαλύτερο πλεονέκτημα των ΑΠ δημόσιας χρήσης είναι ότι τα πιστοποιητικά που αυτές εκδίδουν μπορούν να αναγνωρισθούν άμεσα από τα κυριότερα προγράμματα λογισμικού που εμπεριέχουν δυνατότητες PKI, όπως είναι τα προγράμματα ηλεκτρονικού ταχυδρομείου και τα προγράμματα πλοήγησης στο Internet (Web browsers). Αυτό συμβαίνει διότι οι κατασκευαστές των προγραμμάτων αυτών τα εφοδιάζουν εκ των προτέρων με τα πρωταρχικά πιστοποιητικά (root certificates) των πιο γνωστών ΑΠ δημόσιας χρήσης, θεωρώντας ότι οι ΑΠ αυτές είναι εξ ορισμού αξιόπιστες.

Μεταξύ των διαφόρων τύπων πιστοποιητικών που μπορεί να εκδώσει μια ΑΠ δημόσιας χρήσης ιδιαίτερο ενδιαφέρον παρουσιάζει η περίπτωση των λεγομένων "server-side SSL certificates" (πιστοποιητικά servers για ασφαλή επικοινωνία μέσω Web). Είναι εκείνη η μορφή πιστοποιητικών που χρησιμοποιείται για να αποδεικνύει την ταυτότητα ενός Web server, όταν κάποιος χρήστης συνδεθεί με αυτόν (βλ. και σχετικό παράδειγμα, Κεφ. 11 - υπηρεσίες και εφαρμογές PKI). Αν ο Web server είναι εφοδιασμένος με πιστοποιητικό που έχει εκδοθεί από μια γνωστή ΑΠ δημόσιας χρήσης, τότε αυτό αναγνωρίζεται αυτόματα από το λογισμικό (Web browser) του χρήστη, με συνέπεια να αυξάνεται ο βαθμός εμπιστοσύνης του χρήστη και με τελικό αποτέλεσμα να προχωρεί στην πραγματοποίηση μιας ηλεκτρονικής συναλλαγής. Κατά συνέπεια, είναι σκόπιμο ο Web server μιας επιχείρησης που θα εξυπηρετήσει ασφαλείς ηλεκτρονικές συναλλαγές, να διαθέτει ψηφιακό πιστοποιητικό που να έχει εκδοθεί από μια γνωστή ΑΠ δημόσιας χρήσης.

Φυσικά μια ΑΠ δημόσιας χρήσης μπορεί να καλύψει και άλλες περιπτώσεις, όπως πιστοποιητικά ηλεκτρονικού ταχυδρομείου, πιστοποιητικά χρηστών για ασφαλείς συναλλαγές μέσω Web (client-side SSL certificates) κλπ. Αν όμως οι ανάγκες της επιχείρησης επεκτείνονται πολύ περισσότερο από την χορήγηση ενός ψηφιακού πιστοποιητικού για τον Web server της ή μερικών πιστοποιητικών για ορισμένα στελέχη (π.χ. αν απαιτείται ο εφοδιασμός με ψηφιακά πιστοποιητικά όλων των υπαλλήλων της), τότε θα πρέπει να εξετασθούν και οι δύο επόμενες επιλογές.

10.2. Δημιουργία και χρήση ιδιόκτητης ΑΠ (in-house CA)

Μια ιδιόκτητη ΑΠ δημιουργείται για να εκδίδει και να διαχειρίζεται ψηφιακά πιστοποιητικά που πρόκειται να χρησιμοποιηθούν από ένα συγκεκριμένο οργανισμό ή επιχείρηση. Τα πιστοποιητικά αυτά μπορεί να αφορούν μέλη του οργανισμού ή υπαλλήλους της επιχείρησης, αλλά μπορεί να επεκταθούν και σε συνεργαζόμενες επιχειρήσεις, προμηθευτές ή και πελάτες.

Η επιχείρηση-ιδιοκτήτης της ΑΠ αναλαμβάνει πλήρως όλες τις λειτουργικές διαδικασίες και τη διαχείριση του κύκλου ζωής των πιστοποιητικών.

Δεδομένου ότι ένα σύστημα PKI ασχολείται κυρίως με τη δημιουργία και διαχείριση ψηφιακών ταυτοτήτων που χρησιμοποιούνται εν συνεχεία ως βάση για την παροχή άλλων υπηρεσιών ασφαλείας, πολλές επιχειρήσεις επιθυμούν να διατηρήσουν άμεσο έλεγχο των σχετικών διαδικασιών. Εξάλλου, η χρήση ιδιόκτητης ΑΠ παρέχει μεγαλύτερη ευελιξία σε ό, τι αφορά τους τύπους των εκδιδομένων πιστοποιητικών, καθώς και την εκπόνηση και εφαρμογή πολιτικών που εξυπηρετούν εξειδικευμένες ανάγκες της συγκεκριμένης επιχείρησης.

Επιπλέον, η προσέγγιση αυτή (ιδιόκτητη ΑΠ) επιτρέπει καλύτερη ενσωμάτωση και μεγαλύτερο βαθμό ολοκλήρωσης του συστήματος PKI με άλλα πληροφοριακά συστήματα της επιχείρησης, όπως π.χ. με το σύστημα προσωπικού. Στην περίπτωση αυτή είναι δυνατόν να αυτοματοποιηθεί η διαδικασία αίτησης και χορήγησης πιστοποιητικού, αξιοποιώντας όλα τα ήδη υπάρχοντα στοιχεία ταυτότητας του αιτούντος, ενώ το ρόλο της Αρχής Καταχώρησης (ΑΚ) θα μπορούσε να τον αναλάβει το τμήμα προσωπικού. Παράλληλα, απλοποιούνται και ορισμένες άλλες διαδικασίες, όπως για παράδειγμα η ανανέωση των πιστοποιητικών.

Φυσικά, ο σχεδιασμός και υλοποίηση μιας ιδιόκτητης ΑΠ απαιτεί ιδιαίτερα μεγάλη προσπάθεια και συνεπάγεται αυξημένο κόστος αρχικής εγκατάστασης. Επίσης, οι ανάγκες συντήρησης και υποστήριξης ενός συστήματος PKI με ιδιόκτητη ΑΠ είναι και αυτές σημαντικές. Σχετικές αναλυτικές πληροφορίες για τις διάφορες επιμέρους φάσεις ενός τέτοιου έργου και τις αντίστοιχες ειδικότερες απαιτήσεις και διαδικασίες παρουσιάζονται παρακάτω, στο Κεφ. 12.

10.3. Εκχώρηση των λειτουργιών ΑΠ σε τρίτους (outsourced CA)

Σε αντίθεση με μια ΑΠ δημόσιας χρήσης, η επιλογή αυτή σημαίνει ότι μια τρίτη εξειδικευμένη εταιρία αναλαμβάνει να δημιουργήσει μια ΑΠ, η οποία και θα λειτουργεί αποκλειστικά και μόνο για την εξυπηρέτηση των αναγκών της αναθέτουσας επιχείρησης. Ανάλογα με τις απαιτήσεις της επιχείρησης, αλλά και με τις προσφερόμενες (εκ μέρους της τρίτης εταιρίας) δυνατότητες, είναι δυνατόν να δημιουργηθούν διάφορα μοντέλα, που προβλέπουν την εκχώρηση ενός μέρους ή και του συνόλου των λειτουργιών μιας ΑΠ.

Σε επίπεδο γενικού σχεδιασμού, είναι δυνατόν η αναθέτουσα επιχείρηση να ενταχθεί μέσα στην ήδη υπάρχουσα ιεραρχία πιστοποίησης που διαθέτει ο φορέας παροχής υπηρεσιών ΑΠ (δηλ. η τρίτη εταιρία) ή να καθιερωθεί μια ανεξάρτητη ιεραρχία πιστοποίησης ειδικά για την αναθέτουσα επιχείρηση.

Κατά κανόνα, ένα σχήμα με εκχώρηση λειτουργιών ΑΠ σε τρίτους σημαίνει ότι η υπηρεσία έκδοσης πιστοποιητικών (και ο αντίστοιχος certificate server) βρίσκεται και λειτουργεί στις εγκαταστάσεις του φορέα παροχής υπηρεσιών ΑΠ. Δεδομένου ότι ένας τέτοιος φορέας διαθέτει ήδη τη σχετική υποδομή, αυτό εξασφαλίζει ότι εφαρμόζονται οι απαραίτητοι έλεγχοι ασφαλείας κατά την πρόσβαση στην ΑΠ, ότι χρησιμοποιείται ειδικός εξοπλισμός για την

αποθήκευση των κλειδιών της ΑΠ με τα οποία υπογράφονται τα πιστοποιητικά και ότι διατίθενται μηχανισμοί δημιουργίας αντιγράφων ασφαλείας (back-ups). Δεν παρέχεται απ' ευθείας πρόσβαση στην αναθέτουσα επιχείρηση, παρά μόνο μέσω της Αρχής Καταχώρησης (ΑΚ), η οποία αποτελεί ένα ελεγχόμενο σημείο επικοινωνίας, για την υποβολή αιτήσεων χορήγησης πιστοποιητικών.

Η ίδια η ΑΚ εξάλλου, είναι δυνατόν να βρίσκεται είτε στις εγκαταστάσεις του φορέα παροχής υπηρεσιών είτε (συνηθέστερα) στις εγκαταστάσεις της αναθέτουσας επιχείρησης, η οποία στην περίπτωση αυτή έχει και την ευθύνη της λειτουργίας της. Η επικοινωνία με την ΑΚ εξυπηρετείται με τη βοήθεια κατάλληλου εξειδικευμένου λογισμικού διαχείρισης της ΑΚ, το οποίο στηρίζεται στην τεχνολογία του Web. Το λογισμικό αυτό παρέχει τη δυνατότητα εξέτασης των σχετικών αιτήσεων και την προώθηση αυτών που θα εγκριθούν προς την ΑΠ για την έκδοση των αντίστοιχων πιστοποιητικών. Στο μοντέλο αυτό οι διαδικασίες που καθορίζουν τον τρόπο ελέγχου της ταυτότητας των υποψηφίων κατόχων πιστοποιητικών και η στελέχωση της ΑΚ με το κατάλληλο προσωπικό είναι αρμοδιότητες της ίδιας της αναθέτουσας επιχείρησης.

Πρόσθετες υπηρεσίες που μπορεί να παρέχονται στην επιχείρηση αφορούν την αρχειοθέτηση και την ανάκτηση κλειδιών. Δεδομένου όμως του κρίσιμου χαρακτήρα των λειτουργιών αυτών, κάτι τέτοιο θα πρέπει να γίνεται κάτω από ειδικά σχήματα που να εξασφαλίζουν ότι η αναθέτουσα επιχείρηση έχει κάποιο βαθμό ελέγχου κατά την εκτέλεση των αντίστοιχων διαδικασιών.

Τα διάφορα εναλλακτικά μοντέλα της κατηγορίας αυτής προσφέρουν φυσικά και διαφορετικά οφέλη, τα οποία θα πρέπει να εκτιμηθούν προσεκτικά. Έτσι σε ορισμένα μοντέλα η αναθέτουσα επιχείρηση είναι υπεύθυνη για την ουσιαστική λειτουργία της ΑΠ και αναλαμβάνει όλους τους σχετικούς κινδύνους, ενώ ο φορέας παροχής υπηρεσιών προσφέρει απλώς μια ασφαλή εγκατάσταση όπου δημιουργούνται τα πιστοποιητικά. Σε άλλες όμως περιπτώσεις η επιχείρηση απλώς παρέχει ένα κατάλογο χρηστών που δικαιούνται πιστοποιητικό, ενώ ο φορέας παροχής υπηρεσιών έχει την πλήρη ευθύνη και τον έλεγχο όλου του κύκλου ζωής των πιστοποιητικών (έκδοση, διαχείριση, ανανέωση κλπ).

Λαμβάνοντας υπ' όψη ότι η σχετική με συστήματα PKI τεχνογνωσία δεν είναι ακόμη ιδιαίτερα διαδεδομένη και ότι η εξεύρεση εξειδικευμένου και έμπειρου τεχνικού προσωπικού είναι αρκετά δύσκολη, θα αποτελούσε πιθανότατα σοφή επιλογή για μια επιχείρηση να υιοθετήσει αρχικά το πιο πάνω μοντέλο της εκχώρησης των υπηρεσιών ΑΠ σε μια τρίτη εξειδικευμένη εταιρία. Έτσι συντέμνεται ο απαιτούμενος χρόνος αρχικής ανάπτυξης και επισπεύδεται η έναρξη της λειτουργίας ενός συστήματος PKI. Ταυτόχρονα, η αναθέτουσα επιχείρηση έχει τη δυνατότητα να αξιοποιήσει τη διαδικασία της εκχώρησης υπηρεσιών ΑΠ σαν μια ευκαιρία μεταφοράς τεχνογνωσίας και εκπαίδευσης του δικού της προσωπικού στην πράξη (on job training). Όταν αποκτηθεί επαρκής εμπειρία από τη λειτουργία και χρήση του συστήματος, είναι δυνατόν (εφ' όσον αυτό κριθεί σκόπιμο) ορισμένες ή και όλες οι λειτουργίες της ΑΠ να μεταφερθούν υπό τον έλεγχο της αναθέτουσας επιχείρησης και στις δικές της εγκαταστάσεις.

11. ΥΠΗΡΕΣΙΕΣ ΚΑΙ ΕΦΑΡΜΟΓΕΣ ΣΥΣΤΗΜΑΤΟΣ PKI

11.1. Υπηρεσίες

Οπως έχει αναλυτικά εξηγηθεί στα προηγούμενα, ένα σύστημα PKI χρησιμοποιεί τις δυνατότητες της ασύμμετρης (αλλά και της συμμετρικής) κρυπτογραφίας και στηρίζεται καθοριστικά στις Αρχές Πιστοποίησης (ΑΠ), με στόχο τη δημιουργία ενός αξιόπιστου και ασφαλούς μηχανισμού για τη διανομή ψηφιακών πιστοποιητικών. Με τον τρόπο αυτό προσφέρει τελικά μια σειρά από υπηρεσίες υποδομής, οι οποίες μπορούν να χρησιμοποιηθούν στη συνέχεια από τα διάφορα επιμέρους πληροφοριακά υποσυστήματα, προκειμένου να εξυπηρετήσουν τις ποικίλες επιχειρηματικές διαδικασίες.

Οι κυριότερες υπηρεσίες που προσφέρει ένα σύστημα PKI είναι:

11.1.1. Ψηφιακές υπογραφές (digital signatures)

Η υπογραφή στην καθημερινή πρακτική είναι κάτι το σύνηθες και χρησιμοποιείται, για παράδειγμα, στις επιστολές, στις επιταγές, στα συμβόλαια κλπ. Η ψηφιακή υπογραφή είναι το ηλεκτρονικό ανάλογο της ιδιόχειρης υπογραφής: προσδιορίζει τον υπογράφοντα και δηλώνει μια σχέση ανάμεσα σ' αυτόν και το υπογεγραμμένο έγγραφο. Οπως έχει ήδη προαναφερθεί, μια ψηφιακή υπογραφή είναι στην ουσία το αποτέλεσμα που παράγεται από μια μαθηματική διαδικασία που έχει κάποια ιδιαίτερα χαρακτηριστικά. Η ασφάλειά της στηρίζεται στη χρήση της ασύμμετρης κρυπτογραφίας, όπου η κρυπτογράφηση και η αποκρυπτογράφηση χρησιμοποιούν διαφορετικά κλειδιά η κάθε μια. (βλ. Κεφ. 2 – δημόσια / ιδιωτικά κλειδιά). Τελικά, μια ψηφιακή υπογραφή παρέχει ισχυρή απόδειξη στον παραλήπτη ενός ψηφιακά υπογεγραμμένου μηνύματος ότι το περιεχόμενο του μηνύματος δεν έχει αλλοιωθεί.

Σημ. Οι νομικές πτυχές του θέματος εξετάζονται στο Κεφ.13.

Εξάλλου, με δεδομένο ότι ένα και μοναδικό ιδιωτικό κλειδί δημιουργεί την υπογραφή, το περιεχόμενο ενός μηνύματος μπορεί να συσχετιστεί με την ταυτότητα κάποιας οντότητας, η οποία είναι ο κάτοχος του συγκεκριμένου ιδιωτικού κλειδιού. Ο συσχετισμός αυτός γίνεται μέσω της επαλήθευσης της υπογραφής με το δημόσιο κλειδί της υπ' όψη οντότητας. Αν η επαλήθευση αποβεί επιτυχής και το δημόσιο κλειδί είναι συνδεδεμένο μέσω ενός ψηφιακού πιστοποιητικού με την πιο πάνω οντότητα, τότε η ψηφιακή υπογραφή μπορεί να χρησιμοποιηθεί ως απόδειξη ότι το υπογεγραμμένο μήνυμα προήλθε από την οντότητα που προσδιορίζεται στο σχετικό πιστοποιητικό.

Κατά συνέπεια, η υπηρεσία της ψηφιακής υπογραφής που προσφέρει ένα σύστημα PKI έχει δύο σκέλη:

1. δημιουργία ψηφιακής υπογραφής και
2. έλεγχο εγκυρότητας ψηφιακής υπογραφής.

Η δημιουργία ψηφιακής υπογραφής απαιτεί πρόσβαση στο ιδιωτικό κλειδί του υπογράφοντος. Το κλειδί αυτό έχει ιδιαίτερα κρίσιμη σημασία, εφ' όσον προσδιορίζει μοναδικά τον υπογράφοντα και θα πρέπει, επομένως, να προστατευθεί. Σε περίπτωση κλοπής του, θα μπορούσε κάποιος τρίτος να υπογράφει με αυτό και να προσποιείται ότι είναι ο νόμιμος κάτοχος του. Κατά συνέπεια, η δημιουργία ψηφιακής υπογραφής αποτελεί συνήθως τμήμα μιας ασφαλούς εφαρμογής λογισμικού, η οποία προβλέπει και ενσωματώνει μηχανισμούς ελεγχόμενης πρόσβασης στο ιδιωτικό κλειδί.

Αντίθετα, ο έλεγχος εγκυρότητας υπογραφής μπορεί να είναι μια πιο "ανοιχτή" διαδικασία. Τα δημόσια κλειδιά, εφ' όσον έχουν υπογραφεί από κάποια έμπιστη τρίτη οντότητα (δηλαδή ΑΠ), θεωρούνται δημοσιεύσιμα και σκοπός τους είναι να μπορούν να γίνουν γνωστά σε κάθε ενδιαφερόμενο. Η διαδικασία ελέγχου εγκυρότητας χρησιμοποιεί το υπογεγραμμένο μήνυμα, την υπογραφή του αποστολέα και το δημόσιο κλειδί του και επιστρέφει μια ένδειξη επιτυχίας ή αποτυχίας. Το επιτυχές αποτέλεσμα σημαίνει ότι πράγματι το μήνυμα προήλθε από τον συγκεκριμένο παραλήπτη.

11.1.2. Επιβεβαίωση ταυτότητας-ταυτοποίηση (authentication)

Η υπηρεσία αυτή χρησιμοποιεί ψηφιακές υπογραφές προκειμένου να "δημιουργήσει"-εξακριβώσει μια ταυτότητα. Κατά κανόνα η βασική διαδικασία περιλαμβάνει την αποστολή ενός τυχαίου κειμένου-"πρόκλησης" (challenge) προς την οντότητα της οποίας η ταυτότητα πρόκειται να επιβεβαιωθεί. Στη συνέχεια, η οντότητα αυτή θα πρέπει είτε να υπογράψει ψηφιακά είτε να κρυπτογραφήσει την "πρόκληση", ανάλογα με τον τρόπο χρήσης του κλειδιού. Αν αυτός που επιδιώκει την επιβεβαίωση ταυτότητας είναι σε θέση είτε να επαληθεύσει την υπογραφή είτε να αποκρυπτογραφήσει το τυχαίο κείμενο, τότε η ταυτότητα της υπό έλεγχο οντότητας επιβεβαιώνεται.

Εννοείται ότι ο ελέγχων θα πρέπει να έχει στη διάθεσή του το αντίστοιχο ψηφιακό πιστοποιητικό της υπό έλεγχο οντότητας, είτε αυτό έχει ήδη αποσταλεί από αυτήν είτε μέσω υπηρεσιών καταλόγου (certificate directory services). Αναπόσπαστο τμήμα της όλης διαδικασίας είναι φυσικά και ο σχετικός έλεγχος εγκυρότητας του ψηφιακού πιστοποιητικού.

11.1.3. Χρονοσήμανση (time-stamping)

Μια ασφαλής υπηρεσία χρονοσήμανσης παρέχει απόδειξη ότι ένα σύνολο δεδομένων υφίστατο σε μια δεδομένη χρονική στιγμή. Οι ασφαλείς χρονοσημάνσεις μπορούν να χρησιμοποιηθούν για να κατοχυρώσουν το πότε έλαβε χώρα μια ηλεκτρονική πράξη, όπως μια συναλλαγή ή μια υπογραφή ενός ηλεκτρονικού εγγράφου. Κάτι τέτοιο είναι ιδιαίτερα χρήσιμο όταν η πράξη αυτή έχει νομικές ή οικονομικές συνέπειες, όπως μια προσφορά που πρέπει να υποβληθεί πριν τη λήξη κάποιας προθεσμίας ή μια αμφισβητούμενη διαθήκη που θα πρέπει να αποδειχθεί ότι υπογράφηκε από τον αποθανόντα.

Γενικά, μια υπηρεσία χρονοσήμανσης υλοποιείται βάσει ενός μηχανισμού αίτησης-απάντησης. Η οντότητα που επιθυμεί τη χρονοσήμανση αποστέλλει μια σχετική αίτηση στην οποία περιέχεται το αποτύπωμα (digest) των δεδομένων που πρόκειται να χρονοσημανθούν. Με τη σειρά της η υπηρεσία χρονοσήμανσης "προμηθεύεται" μια ημερομηνία και ώρα υψηλής ακρίβειας και στη συνέχεια υπογράφει ψηφιακά με το δικό της ιδιωτικό κλειδί τον συνδυασμό του αποτυπώματος δεδομένων (που παρέλαβε με την αίτηση) και της πιο πάνω ακριβούς ημερομηνίας και ώρας. Εννοείται ότι η "πηγή" που παρέχει την ημερομηνία και ώρα θα πρέπει να είναι εξαιρετικά υψηλής ακρίβειας, όπως π.χ. μια υπηρεσία ώρας που στηρίζεται σε ατομικό ρολόι (atomic clock time source).

11.1.4. Μη αποκήρυξη (non-repudiation)

Η υπηρεσία μη αποκήρυξης έχει τη δυνατότητα να προσφέρει αδιάσειστα αποδεικτικά στοιχεία για μια ηλεκτρονική πράξη (π.χ. ηλεκτρονική συναλλαγή ή αποστολή/λήψη ενός ηλεκτρονικού εγγράφου), στην οποία λαμβάνουν μέρος δύο πλευρές. Σε αντίθεση με την επιβεβαίωση ταυτότητας, η μη αποκήρυξη επικεντρώνεται σε μια πράξη και στην επαλήθευση ότι οι δύο πλευρές συμμετείχαν πράγματι σ' αυτήν. Για παράδειγμα, ο πελάτης μιας τράπεζας που κάνει χρήση των τραπεζικών της υπηρεσιών μέσω Internet, επιθυμεί να έχει υπηρεσίες μη αποκήρυξης, όταν πραγματοποιεί μεταφορά ενός ποσού από το δικό του λογαριασμό στο λογαριασμό ενός προμηθευτή του, προκειμένου να εξοφλήσει κάποια οφειλή. Ο πελάτης θα έχει έτσι διασφαλίσει ότι η τράπεζα δεν θα μπορεί αργότερα να αρνηθεί το ότι έγινε η μεταφορά του ποσού, σε περίπτωση που ο προμηθευτής ισχυριστεί ότι η πιο πάνω πληρωμή δεν έχει γίνει. Αντίστοιχα, η τράπεζα επιθυμεί να διασφαλίσει ότι ο πελάτης της δεν θα έχει τη δυνατότητα να αρνηθεί ότι έκανε την πιο πάνω μεταφορά ποσού.

Η μη αποκήρυξη στηρίζεται βέβαια στην υπηρεσία των ψηφιακών υπογραφών και χρησιμοποιεί τους μηχανισμούς επιβεβαίωσης ταυτότητας (authentication) και ακεραιότητας δεδομένων (data integrity) που παρέχει ένα περιβάλλον PKI, αλλά επεκτείνεται και πέρα απ' αυτά. Ο τελικός της σκοπός είναι να προσφέρει δυνατότητες επίλυσης διαφορών μεταξύ δύο μερών, επιτρέποντας σε ένα τρίτο ουδέτερο μέρος (π.χ. διαιτησία, δικαστική αρχή κλπ) να κρίνει βάσει αποδεικτικών στοιχείων και να αποφασίσει για το τι πράγματι έχει συμβεί. Τα στοιχεία αυτά θα πρέπει να συλλεγούν και να καταγραφούν τη στιγμή που διεξάγεται μια συναλλαγή (όχι εκ των υστέρων), να περιλαμβάνουν όλες τις απαραίτητες πληροφορίες και να τηρούνται με οργανωμένο τρόπο, ώστε να είναι δυνατόν να χρησιμοποιηθούν, εάν χρειαστεί.

Γενικά, οι πληροφορίες που απαιτούνται αφορούν:

- την ταυτότητα αυτού που εκκινεί τη διαδικασία (π.χ. τον αποστολέα ενός μηνύματος)
- την ταυτότητα του αποδέκτη (π.χ. τον παραλήπτη ενός μηνύματος)
- το περιεχόμενο της συναλλαγής ή του μηνύματος
- την ακριβή ημερομηνία και ώρα της ηλεκτρονικής πράξης (η ώρα αποστολής μπορεί να διαφέρει από την ώρα λήψης, οπότε πρόκειται για δύο διαφορετικές πληροφορίες)
- την ταυτότητα ενός έμπιστου τρίτου μέρους που πιθανόν εμπλέκεται στην όλη διαδικασία (με κύριο ρόλο συνήθως την τήρηση των σχετικών στοιχείων).

11.2. Εφαρμογές

Υπηρεσίες υποδομής, όπως οι παραπάνω, που προσφέρονται από ένα σύστημα PKI, θα πρέπει να αξιοποιηθούν από συγκεκριμένες πληροφορικές εφαρμογές, προκειμένου να αποκτήσουν αξία. Ο συνηθέστερος τρόπος για να προστεθούν δυνατότητες PKI σε καινούργιες ή και υπάρχουσες εφαρμογές είναι με χρήση ειδικών βιβλιοθηκών – APIs (Application Programming Interfaces), οι οποίες ενσωματώνουν τις σχετικές κρυπτογραφικές λειτουργίες και επιτρέπουν την ευχερή αξιοποίησή τους σε υψηλό επίπεδο, χωρίς να απαιτείται λεπτομερής γνώση του τρόπου υλοποίησής τους.

Παράλληλα με την πιο πάνω προσέγγιση, υπάρχει μια σειρά προϊόντων λογισμικού που έχουν ήδη ενσωματωμένες δυνατότητες χρήσης υπηρεσιών PKI και μπορούν να χρησιμοποιηθούν για τη δημιουργία ασφαλών επιχειρηματικών διαδικασιών. Οι κυριότερες από τις περιπτώσεις αυτές παρουσιάζονται στη συνέχεια.

11.2.1. Ασφαλείς συναλλαγές μέσω Web

Οι συναλλαγές αυτές μπορούν να εφαρμοστούν σε περιβάλλοντα τύπου B2C (Business to Comsumer), B2B (Business to Business), αλλά και σε άλλες περιπτώσεις, όπως για παράδειγμα στην επικοινωνία μεταξύ διαφόρων κρατικών αρχών και φορέων με τους πολίτες. Το πρωτόκολλο που συνήθως χρησιμοποιείται είναι το SSL (Secure Sockets Layer) και το οποίο υποστηρίζεται από όλα τα σύγχρονα προϊόντα λογισμικού, δηλαδή τους Web servers και τα προγράμματα πλοήγησης στο Internet (Web browsers).
Το πρωτόκολλο SSL κάνει χρήση συμμετρικής και ασύμμετρης κρυπτογραφίας, ψηφιακών υπογραφών και ψηφιακών πιστοποιητικών, επιτυγχάνοντας έτσι διασφάλιση των τεσσάρων βασικών αρχών της ασφάλειας (βλ. Εισαγωγή). Το πρωτόκολλο αυτό αναπτύχθηκε μεν από την Netscape, είναι όμως δημόσια διαθέσιμο και έχει πλέον αποτελέσει πρότυπο (standard) για ασφαλείς επικοινωνίες μέσω Internet.

Από την πλευρά του Web Server, ο διαχειριστής θα πρέπει να αποκτήσει ένα ζεύγος κλειδιών (δημόσιο/ιδιωτικό), καθώς και το αντίστοιχο ψηφιακό πιστοποιητικό από κάποια γνωστή Αρχή Πιστοποίησης. Στη συνέχεια εγκαθιστά το ψηφιακό πιστοποιητικό και ενεργοποιεί τις ενσωματωμένες δυνατότητες ασφάλειας του Web Server, χρησιμοποιώντας ταυτόχρονα και ειδικούς συνδέσμους (links) για τις ασφαλείς περιοχές του server, οι οποίοι έχουν την μορφή:

<A HREF=https://myserver1.mycompany.gr/secret.html> Go into SSL</A>

Από την πλευρά του Web Browser, ο χρήστης το μόνο που έχει να κάνει για να ενεργοποιήσει μια ασφαλή σύνδεση (σύνδεση SSL) με τον Web Server είναι να χρησιμοποιήσει σαν πρόθεμα (prefix) της δικτυακής διεύθυνσης που τον ενδιαφέρει το https:// (αντί του συνήθους http://). Αυτό λειτουργεί σαν διέγερση προς τον Browser να ξεκινήσει μια προκαταρκτική διαδικασία διαπραγμάτευσης της ασφαλούς σύνδεσης με τον Web Server, η οποία δεν είναι αντιληπτή από το χρήστη (είναι, όπως λέγεται, transparent). Μόλις επιτευχθεί η ασφαλής σύνδεση, ο χρήστης έχει μία τουλάχιστον ένδειξη γι'αυτό, η οποία στις σύγχρονες εκδόσεις των Browsers είναι το εικονίδιο ενός κλειδωμένου λουκέτου, στο κάτω μέρος της οθόνης.

Γενικά, μια υπηρεσία χρονοσήμανσης υλοποιείται βάσει ενός μηχανισμού αίτησης-απάντησης. Η οντότητα που επιθυμεί τη χρονοσήμανση αποστέλλει μια σχετική αίτηση στην οποία περιέχεται το αποτύπωμα (digest) των δεδομένων που πρόκειται να χρονοσημανθούν. Με τη σειρά της η υπηρεσία χρονοσήμανσης "προμηθεύεται" μια ημερομηνία και ώρα υψηλής ακρίβειας και στη συνέχεια υπογράφει ψηφιακά με το δικό της ιδιωτικό κλειδί τον συνδυασμό του αποτυπώματος δεδομένων (που παρέλαβε με την αίτηση) και της πιο πάνω ακριβούς ημερομηνίας και ώρας. Εννοείται ότι η "πηγή" που παρέχει την ημερομηνία και ώρα θα πρέπει να είναι εξαιρετικά υψηλής ακρίβειας, όπως π.χ. μια υπηρεσία ώρας που στηρίζεται σε ατομικό ρολόι (atomic clock time source).

11.1.4. Μη αποκήρυξη (non-repudiation)

Η υπηρεσία μη αποκήρυξης έχει τη δυνατότητα να προσφέρει αδιάσειστα αποδεικτικά στοιχεία για μια ηλεκτρονική πράξη (π.χ. ηλεκτρονική συναλλαγή ή αποστολή/λήψη ενός ηλεκτρονικού εγγράφου), στην οποία λαμβάνουν μέρος δύο πλευρές. Σε αντίθεση με την επιβεβαίωση ταυτότητας, η μη αποκήρυξη επικεντρώνεται σε μια πράξη και στην επαλήθευση ότι οι δύο πλευρές συμμετείχαν πράγματι σ' αυτήν. Για παράδειγμα, ο πελάτης μιας τράπεζας που κάνει χρήση των τραπεζικών της υπηρεσιών μέσω Internet, επιθυμεί να έχει υπηρεσίες μη αποκήρυξης, όταν πραγματοποιεί μεταφορά ενός ποσού από το δικό του λογαριασμό στο λογαριασμό ενός προμηθευτή του, προκειμένου να εξοφλήσει κάποια οφειλή. Ο πελάτης θα έχει έτσι διασφαλίσει ότι η τράπεζα δεν θα μπορεί αργότερα να αρνηθεί το ότι έγινε η μεταφορά του ποσού, σε περίπτωση που ο προμηθευτής ισχυριστεί ότι η πιο πάνω πληρωμή δεν έχει γίνει. Αντίστοιχα, η τράπεζα επιθυμεί να διασφαλίσει ότι ο πελάτης της δεν θα έχει τη δυνατότητα να αρνηθεί ότι έκανε την πιο πάνω μεταφορά ποσού.

Η μη αποκήρυξη στηρίζεται βέβαια στην υπηρεσία των ψηφιακών υπογραφών και χρησιμοποιεί τους μηχανισμούς επιβεβαίωσης ταυτότητας (authentication) και ακεραιότητας δεδομένων (data integrity) που παρέχει ένα περιβάλλον PKI, αλλά επεκτείνεται και πέρα απ' αυτά. Ο τελικός της σκοπός είναι να προσφέρει δυνατότητες επίλυσης διαφορών μεταξύ δύο μερών, επιτρέποντας σε ένα τρίτο ουδέτερο μέρος (π.χ. διαιτησία, δικαστική αρχή κλπ) να κρίνει βάσει αποδεικτικών στοιχείων και να αποφασίσει για το τι πράγματι έχει συμβεί. Τα στοιχεία αυτά θα πρέπει να συλλεγούν και να καταγραφούν τη στιγμή που διεξάγεται μια συναλλαγή (όχι εκ των υστέρων), να περιλαμβάνουν όλες τις απαραίτητες πληροφορίες και να τηρούνται με οργανωμένο τρόπο, ώστε να είναι δυνατόν να χρησιμοποιηθούν, εάν χρειαστεί.

Γενικά, οι πληροφορίες που απαιτούνται αφορούν:

- την ταυτότητα αυτού που εκκινεί τη διαδικασία (π.χ. τον αποστολέα ενός μηνύματος)
- την ταυτότητα του αποδέκτη (π.χ. τον παραλήπτη ενός μηνύματος)
- το περιεχόμενο της συναλλαγής ή του μηνύματος
- την ακριβή ημερομηνία και ώρα της ηλεκτρονικής πράξης (η ώρα αποστολής μπορεί να διαφέρει από την ώρα λήψης, οπότε πρόκειται για δύο διαφορετικές πληροφορίες)
- την ταυτότητα ενός έμπιστου τρίτου μέρους που πιθανόν εμπλέκεται στην όλη διαδικασία (με κύριο ρόλο συνήθως την τήρηση των σχετικών στοιχείων).

Η υπηρεσία της μη αποκήρυξης περιλαμβάνει ορισμένες ειδικότερες κατηγορίες, οι σπουδαιότερες απο τις οποίες είναι:

- Μη αποκήρυξη προέλευσης (non-repudiation of origin): Η πλευρά που έχει εκκινήσει τη διαδικασία, π.χ. ο αποστολέας ενός μηνύματος, δεν μπορεί να αμφισβητήσει ούτε ότι έστειλε το μήνυμα ούτε και την χρονική στιγμή της αποστολής. Το σκέλος αυτό ενδιαφέρει περισσότερο τον παραλήπτη. Για παράδειγμα, όταν ένας προμηθευτής λάβει μια παραγγελία από κάποιον πελάτη του και ανταποκριθεί σ' αυτήν, επιθυμεί να διασφαλιστεί από το ενδεχόμενο ο πελάτης να αρνηθεί ότι πράγματι έστειλε τη συγκεκριμένη παραγγελία.

- Μη αποκήρυξη παράδοσης (non-repudiation of delivery): Ο παραλήπτης ενός μηνύματος δεν μπορεί να αμφισβητήσει ούτε ότι το παρέλαβε ούτε και την χρονική στιγμή της παραλαβής του. Εδώ ο ενδιαφερόμενος είναι ο αποστολέας, που επιδιώκει να αποκλείσει π.χ. το ενδεχόμενο να "απορριφθεί" μια προσφορά που αυτός αποστέλλει, επειδή δήθεν δεν έφθασε ποτέ στον παραλήπτη ή έφθασε εκπρόθεσμα.

Προκειμένου μια ηλεκτρονική πράξη να αποκτήσει χαρακτηριστικά μη αποκήρυξης, θα πρέπει κάποιος από τους εμπλεκόμενους να ζητήσει τη χρήση της σχετικής υπηρεσίας. Αυτό (δηλ. η χρήση μη αποκήρυξης) μπορεί να έχει θεσπιστεί σαν κανόνας για ορισμένες κατηγορίες συναλλαγών ή μπορεί να ζητηθεί κατ' εξαίρεση για μια συγκεκριμένη συναλλαγή.

Εφ' όσον γίνει χρήση της υπηρεσίας μη αποκήρυξης, τότε τα απαιτούμενα στοιχεία (βλ. παραπάνω) συλλέγονται και καταγράφονται, είτε από ένα από τα εμπλεκόμενα μέρη είτε από κάποιο τρίτο έμπιστο μέρος, το οποίο παρέχει αυτή την υπηρεσία. Η προσφυγή σε τρίτο μέρος, που είναι εξειδικευμένο στην παροχή τέτοιων υπηρεσιών, έχει το πλεονέκτημα της μεγαλύτερης αξιοπιστίας των τηρουμένων στοιχείων. Ετσι, στην περίπτωση που αργότερα προκύψει διαφορά και απαιτηθεί η επίλυσή της, ο κριτής θα αξιολογήσει σοβαρότερα τα σχετικά αποδεικτικά στοιχεία, αν αυτά τηρούνται από ένα τρίτο ουδέτερο μέρος, παρά αν η τήρησή τους ήταν στη αρμοδιότητα ενός από τους εμπλεκομένους.

Στην πραγματικότητα, τίποτε δεν μπορεί να εμποδίσει κάποιον που έχει λάβει μέρος σε μια επικοινωνία από το να αρνηθεί ότι απέστειλε ή παρέλαβε κάποια δεδομένα κατά τη διάρκειά της. Ουσιαστικά, ο ρόλος της υπηρεσίας μη αποκήρυξης είναι να προστατεύσει από την ψευδή, αλλά επιτυχή άρνηση των αποτελεσμάτων της επικοινωνίας, παρέχοντας ισχυρά αποδεικτικά στοιχεία για την επίλυση των σχετικών διαφορών από κάποιο τρίτο ουδέτερο μέρος. Επιπλέον, η ύπαρξη της υπηρεσίας μη αποκήρυξης αποθαρρύνει τα εμπλεκόμενα μέρη από το να επιχειρήσουν, έστω, ψευδή αποκήρυξη.

11.2. Εφαρμογές

Υπηρεσίες υποδομής, όπως οι παραπάνω, που προσφέρονται από ένα σύστημα PKI, θα πρέπει να αξιοποιηθούν από συγκεκριμένες πληροφορικές εφαρμογές, προκειμένου να αποκτήσουν αξία. Ο συνηθέστερος τρόπος για να προστεθούν δυνατότητες PKI σε καινούργιες ή και υπάρχουσες εφαρμογές είναι με χρήση ειδικών βιβλιοθηκών – APIs (Application Programming Interfaces), οι οποίες ενσωματώνουν τις σχετικές κρυπτογραφικές λειτουργίες και επιτρέπουν την ευχερή αξιοποίησή τους σε υψηλό επίπεδο, χωρίς να απαιτείται λεπτομερής γνώση του τρόπου υλοποίησής τους.

Παράλληλα με την πιο πάνω προσέγγιση, υπάρχει μια σειρά προϊόντων λογισμικού που έχουν ήδη ενσωματωμένες δυνατότητες χρήσης υπηρεσιών PKI και μπορούν να χρησιμοποιηθούν για τη δημιουργία ασφαλών επιχειρηματικών διαδικασιών. Οι κυριότερες από τις περιπτώσεις αυτές παρουσιάζονται στη συνέχεια.

11.2.1. Ασφαλείς συναλλαγές μέσω Web

Οι συναλλαγές αυτές μπορούν να εφαρμοστούν σε περιβάλλοντα τύπου B2C (Business to Comsumer), B2B (Business to Business), αλλά και σε άλλες περιπτώσεις, όπως για παράδειγμα στην επικοινωνία μεταξύ διαφόρων κρατικών αρχών και φορέων με τους πολίτες. Το πρωτόκολλο που συνήθως χρησιμοποιείται είναι το SSL (Secure Sockets Layer) και το οποίο υποστηρίζεται από όλα τα σύγχρονα προϊόντα λογισμικού, δηλαδή τους Web servers και τα προγράμματα πλοήγησης στο Internet (Web browsers).
Το πρωτόκολλο SSL κάνει χρήση συμμετρικής και ασύμμετρης κρυπτογραφίας, ψηφιακών υπογραφών και ψηφιακών πιστοποιητικών, επιτυγχάνοντας έτσι διασφάλιση των τεσσάρων βασικών αρχών της ασφάλειας (βλ. Εισαγωγή). Το πρωτόκολλο αυτό αναπτύχθηκε μεν από την Netscape, είναι όμως δημόσια διαθέσιμο και έχει πλέον αποτελέσει πρότυπο (standard) για ασφαλείς επικοινωνίες μέσω Internet.

Από την πλευρά του Web Server, ο διαχειριστής θα πρέπει να αποκτήσει ένα ζεύγος κλειδιών (δημόσιο/ιδιωτικό), καθώς και το αντίστοιχο ψηφιακό πιστοποιητικό από κάποια γνωστή Αρχή Πιστοποίησης. Στη συνέχεια εγκαθιστά το ψηφιακό πιστοποιητικό και ενεργοποιεί τις ενσωματωμένες δυνατότητες ασφάλειας του Web Server, χρησιμοποιώντας ταυτόχρονα και ειδικούς συνδέσμους (links) για τις ασφαλείς περιοχές του server, οι οποίοι έχουν την μορφή:

<A HREF=https://myserver1.mycompany.gr/secret.html> Go into SSL</A>

Από την πλευρά του Web Browser, ο χρήστης το μόνο που έχει να κάνει για να ενεργοποιήσει μια ασφαλή σύνδεση (σύνδεση SSL) με τον Web Server είναι να χρησιμοποιήσει σαν πρόθεμα (prefix) της δικτυακής διεύθυνσης που τον ενδιαφέρει το https:// (αντί του συνήθους http://). Αυτό λειτουργεί σαν διέγερση προς τον Browser να ξεκινήσει μια προκαταρκτική διαδικασία διαπραγμάτευσης της ασφαλούς σύνδεσης με τον Web Server, η οποία δεν είναι αντιληπτή από το χρήστη (είναι, όπως λέγεται, transparent). Μόλις επιτευχθεί η ασφαλής σύνδεση, ο χρήστης έχει μία τουλάχιστον ένδειξη γι'αυτό, η οποία στις σύγχρονες εκδόσεις των Browsers είναι το εικονίδιο ενός κλειδωμένου λουκέτου, στο κάτω μέρος της οθόνης.

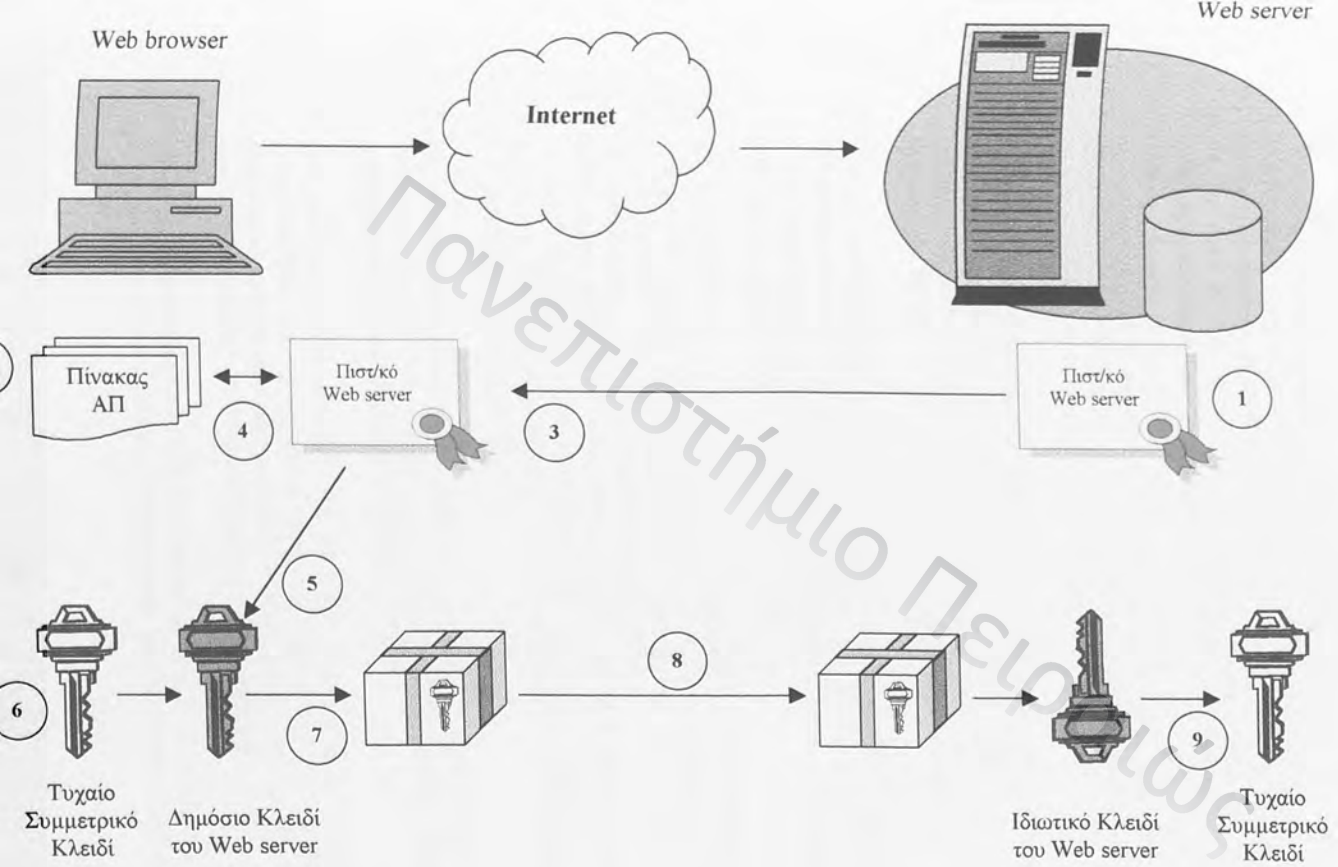
Γενικότερα πάντως, υπάρχουν περιπτώσεις όπου είναι απαραίτητο ο χρήστης να αποδείξει και αυτός την ταυτότητά του μέσω πιστοποιητικού. Για παράδειγμα, μια επιχείρηση μπορεί να διαμορφώσει ένα περιβάλλον που να προσφέρει πρόσβαση σε όλες τις εταιρικές πληροφορίες της μέσω Web, προκειμένου να διευκολύνει τη ελεγχόμενη χρήση τους από τους υπαλλήλους της ή από άλλες συνεργαζόμενες εταιρίες. Στην περίπτωση αυτή, θα επιτραπεί πρόσβαση στο χρήστη (είτε είναι υπάλληλος της επιχείρησης είτε είναι άλλη συνεργαζόμενη εταιρία) μόνο εφ' όσον αυτός αποδείξει την ταυτότητά του, παρουσιάζοντας το αντίστοιχο δικό του ψηφιακό πιστοποιητικό (SSL client-side authentication). Αυτό σημαίνει ότι θα πρέπει να έχει προηγηθεί η απόκτηση του πιστοποιητικού αυτού, καθώς και η εγκατάστασή του στο περιβάλλον του Web browser του χρήστη.

Εννοείται ότι σε ένα Web Site δεν είναι ανάγκη να προστατεύονται με μηχανισμούς ασφαλούς πρόσβασης όλες οι προσφερόμενες/εκτιθέμενες σελίδες, παρά μόνο αυτές μέσω των οποίων θα ανταλλαγούν ευαίσθητα στοιχεία (π.χ. φόρμα πληρωμής, όπου ζητείται και ο κωδικός της πιστωτικης κάρτας).

ΠΑΡΑΔΕΙΓΜΑ ΑΣΦΑΛΟΥΣ ΣΥΝΑΛΛΑΓΗΣ ΜΕΣΩ WEB:

Στη συνέχεια παρουσιάζεται ένα παράδειγμα ασφαλούς συναλλαγής μέσω Web και περιγράφονται αναλυτικά τα επιμέρους βήματα. Για λόγους απλοποίησης της περιγραφής, έχει επιλεγεί μια περίπτωση όπου μόνο η μια πλευρά (ο Web server) επιβεβαιώνει-αποδεικνύει την ταυτότητά της (SSL server-side authentication) στην άλλη. Βέβαια, για τη διεξαγωγή της συναλλαγής, δημιουργείται ένας ασφαλής (κρυπτογραφημένος) δίαυλος επικοινωνίας. Ομως, ο Web server δεν ζητεί από το πρόγραμμα πλοήγησης (δηλ. από το χρήστη) επιβεβαίωση ταυτότητας με τον ίδιο τρόπο. Αυτό είναι αρκετά συνηθισμένο σε περιπτώσεις συναλλαγών που εντάσσονται στην κατηγορία συναλλαγών B2C (Business to Consumer) και είναι αποδεκτό, δεδομένου ότι ο χρήστης-καταναλωτής υποχρεώνεται, κατά τη διάρκεια της συναλλαγής, να δώσει τον αριθμό και ορισμένα άλλα στοιχεία της πιστωτικής του κάρτας και επιβεβαιώνει την ταυτότητά του με τον τρόπο αυτό.

Η διαδικασία της ασφαλούς συναλλαγής αρχίζει όταν ο χρήστης, με τη βοήθεια του Web browser, επισκεφθεί μια δικτυακή διεύθυνση που έχει το πρόθεμα: https:// (βλ. παραπάνω). Η διαγραμματική αναπαράσταση της διαδικασίας φαίνεται στο Σχήμα 18 και τα βήματα που ακολουθούνται είναι αναλυτικά τα εξής:



Σχήμα 18. **Ασφαλής συναλλαγή μέσω Web**

1. Ο Web server είναι ήδη εφοδιασμένος με ένα ψηφιακό πιστοποιητικό που περιέχει την ταυτότητά του και το δημόσιο κλειδί του. Προφανώς ο server διαθέτει και το αντίστοιχο ιδιωτικό κλειδί.

2. Το πρόγραμμα πλοήγησης (Web browser) είναι προεφοδιασμένο (από τον κατασκευαστή) με ένα πίνακα Αρχών Πιστοποίησης (ΑΠ) ευρύτερα γνωστών, τις οποίες και εμπιστεύεται εξ ορισμού, περιέχει δηλαδή τα αντίστοιχα πιστοποιητικά γι' αυτές. (Σημ. Κατά συνέπεια, για να είναι ο Web server μιας επιχείρησης άμεσα επισκέψιμος από οποιονδήποτε ενδιαφερόμενο, θα πρέπει το ψηφιακό πιστοποιητικό που διαθέτει να έχει εκδοθεί από μια ευρέως γνωστή ΑΠ, η οποία και να περιλαμβάνεται στον πίνακα ΑΠ των πιο διαδεδομένων Web browsers. Σε διαφορετική περίπτωση θα απαιτηθεί ειδική διαδικασία προσαρμογής του Web browser, γεγονός που πιθανότατα θα αποθαρρύνει το χρήστη και θα τον οδηγήσει στο να διακόψει τη συναλλαγή).

3. Αμέσως μετά την έναρξη της επικοινωνίας, ο Web server στέλνει το πιστοποιητικό του στον Web browser. Στη φάση αυτή δεν έχει δημιουργηθεί ακόμη ένας ασφαλής δίαυλος επικοινωνίας, αλλά αυτό δεν ενοχλεί, δεδομένου ότι το πιστοποιητικό είναι ούτως ή άλλως πληροφορία δημόσιου χαρακτήρα, αλλά και αυτοπροστατευόμενη δομή.

4. Ο Web browser προβαίνει σε έλεγχο εγκυρότητας του πιστοποιητικού του Web server και ελέγχει αρχικά αν το πιστοποιητικό υπογράφεται από μια γνωστή ΑΠ, δηλαδή μια από τις ΑΠ με των οποίων τα πιστοποιητικά ο Web browser είναι προεφοδιασμένος. Εφ' όσον αυτό ισχύει, εκτελούνται τα εξής ειδικότερα βήματα:

   4.1. Ο Web browser αφ' ενός υπολογίζει εκ νέου το αποτύπωμα (hash) του πιστοποιητικού και αφ' ετέρου αποκρυπτογραφεί (με χρήση του δημόσιου κλειδιού της ΑΠ) το αποτύπωμα που ήδη περιέχεται στο πιστοποιητικό. Εάν τα δύο αποτυπώματα ταυτίζονται, το πιστοποιητικό δεν έχει αλλοιωθεί.
   4.2. Κατόπιν ελέγχονται οι ημερομηνίες έναρξης και λήξης ισχύος του πιστοποιητικού για να επιβεβαιωθεί ότι αυτό είναι έγκυρο στη δεδομένη χρονική στιγμή.
   4.3. Τέλος, ελέγχεται αν το δικτυακό όνομα του Web server (URL) είναι ίδιο με αυτό που αναφέρεται στο πιστοποιητικό.

5. Εάν οι παραπάνω έλεγχοι ολοκληρωθούν με επιτυχία, ο Web browser προχωρεί στην ανάκτηση-εξαγωγή του δημόσιου κλειδιού του Web server, δεδομένου ότι αυτό περιλαμβάνεται στα περιεχόμενα του πιστοποιητικού.

6. Στη συνέχεια ο Web browser δημιουργεί ένα τυχαίο συμμετρικό κλειδί, το οποίο θα χρησιμοποιηθεί για την κρυπτογράφηση της "συνομιλίας" του με τον Web server. Η συμμετρική κρυπτογράφηση προτιμάται, διότι είναι πολύ ταχύτερη από την ασύμμετρη και επιπλέον δεν αυξάνει τον όγκο των προς κρυπτογράφηση δεδομένων.

7. Το παραπάνω συμμετρικό κλειδί δεν αποστέλλεται ως έχει στον Web server, αλλά αφού προηγουμένως "προστατευθεί". Συγκεκριμένα, το συμμετρικό κλειδί κρυπτογραφείται με

χρήση του δημόσιου κλειδιού του Web server, το οποίο έχει εξαχθεί από το ψηφιακό πιστοποιητικό του Web server.

8. Το κρυπτογραφημένο συμμετρικό κλειδί αποστέλλεται στον Web server. Δεδομένου ότι ο Web server είναι η μοναδική οντότητα που κατέχει το σχετικό ιδιωτικό κλειδί που είναι απαραίτητο για την αποκρυπτογράφηση του συμμετρικού, δεν υπάρχει κίνδυνος υποκλοπής και παράνομης χρήσης του συμμετρικού κλειδιού.

9. Ο Web server παραλαμβάνει το κρυπτογραφημένο συμμετρικό κλειδί και χρησιμοποιεί το δικό του ιδιωτικό κλειδί για να το αποκρυπτογραφήσει.

Στο σημείο αυτό και τα δύο μέρη έχουν στη διάθεσή τους το συμμετρικό κλειδί, το οποίο και χρησιμοποιούν στη συνέχεια για την κρυπτογράφηση / αποκρυπτογράφηση των μηνυμάτων που θα ανταλλάξουν. Επομένως έχει δημιουργηθεί ένας δίαυλος επικοινωνίας, στον οποίο κανείς τρίτος, εκτός των δύο ενδιαφερομένων, δεν έχει πρόσβαση. Κατά συνέπεια, η συνομιλία μπορεί να διεξαχθεί με απόλυτη ασφάλεια.

Συμπληρωματικά και σε σχέση με το βήμα 4.3. παραπάνω, θα πρέπει να διευκρινιστούν τα εξής: Από μόνος του ο έλεγχος του δικτυακού ονόματος (URL) του Web server σε σύγκριση με την αντίστοιχη πληροφορία που περιέχεται στο πιστοποιητικό δεν είναι επαρκής. Είναι δυνατόν να επιχειρηθεί από τρίτους παραπλάνηση των χρηστών, με χρήση ειδικών τεχνικών (DNS spoofing), έτσι ώστε ένας Web server, έστω Β, να εμφανίζεται στο Internet (ψευδώς) με το όνομα ενός άλλου, π.χ. του Web server Α. Στην περίπτωση αυτή, η πληροφορία που προορίζεται για τον Web server Α ανακατευθύνεται στον Web server Β και ο ανυποψίαστος χρήστης έχει την εσφαλμένη εντύπωση ότι επικοινωνεί με τον Web server Α.

Στην πραγματικότητα, ο κίνδυνος αυτός εξαλείφεται χάρη στη συνδυασμένη χρήση συμμετρικής και ασύμμετρης κρυπτογραφίας, όπως εξηγήθηκε παραπάνω. Συγκεκριμένα, ο Web browser δημιούργησε ένα τυχαίο συμμετρικό κλειδί, το οποίο και κρυπτογράφησε στη συνέχεια, χρησιμοποιώντας το δημόσιο κλειδί του Web server. Το γεγονός ότι ο Web server κατάφερε να εμπλακεί με επιτυχία σε μια κρυπτογραφημένη συνομιλία με τον Web browser, απέδειξε στον τελευταίο (τον Web browser) ότι ο server είχε εν τω μεταξύ αποκρυπτογραφήσει επιτυχώς το "προστατευμένο" συμμετρικό κλειδί. Αυτό αποτελεί απόδειξη για τον Web browser (και κατά συνέπεια και για το χρήστη) ότι στην "άλλη άκρη" της σύνδεσης βρίσκεται ο σωστός Web server, δεδομένου ότι είναι ο μοναδικός δικτυακός κόμβος παγκοσμίως που διαθέτει το σωστό ιδιωτικό κλειδί για να πραγματοποιήσει την πιο πάνω αποκρυπτογράφηση.

11.2.2. Ασφαλές ηλεκτρονικό ταχυδρομείο (secure E-mail)

Το απλό ηλεκτρονικό ταχυδρομείο προσφέρει μεν ένα εύκολο και γρήγορο μηχανισμό για ανταλλαγή μηνυμάτων, δεν είναι όμως από μόνο του ασφαλές. Προκειμένου να αποκτήσει χαρακτηριστικά υψηλής ασφάλειας, γίνεται χρήση των δυνατοτήτων που παρέχει ένα σύστημα PKI, όπως η κρυπτογράφηση και οι ψηφιακές υπογραφές.

Ένα από τα βασικά ζητούμενα είναι η επιβεβαίωση της ταυτότητας του αποστολέα. Αυτό επιτυγχάνεται, εφ' όσον ο αποστολέας υπογράφει ψηφιακά το αποστελλόμενο μήνυμα. Ο αποστολέας δημιουργεί την ψηφιακή υπογραφή του χρησιμοποιώντας το ιδιωτικό του κλειδί και στη συνέχεια αποστέλλει το σχετικό πιστοποιητικό μαζί με το κύριο σώμα του μηνύματος. Έτσι ο παραλήπτης είναι σε θέση να ελέγξει την εγκυρότητα της ταυτότητας του υπογράφοντος (δηλ. του αποστολέα) και να επιβεβαιώσει ότι τα περιεχόμενα του μηνύματος δεν έχουν αλλοιωθεί καθ' οδόν.

Ομως, ο εμπιστευτικός χαρακτήρας ενός μηνύματος δεν διασφαλίζεται, αν το μήνυμα είναι απλώς υπογεγραμμένο, δεδομένου ότι είναι δυνατόν ένας τρίτος να υποκλέψει το μήνυμα κατά τη διαδρομή του και να αποκτήσει πρόσβαση στα περιεχόμενά του. Για το λόγο αυτό, είναι ανάγκη ο αποστολέας να κρυπτογραφήσει το μήνυμα πριν την αποστολή του, κάνοντας χρήση του δημόσιου κλειδιού του παραλήπτη. Έτσι διασφαλίζεται ότι το μήνυμα είναι δυνατόν να αναγνωσθεί μόνον από τον νόμιμο παραλήπτη, αφού αυτός είναι ο μοναδικός κάτοχος του αντίστοιχου ιδιωτικού κλειδιού, το οποίο και είναι απαραίτητο για την αποκρυπτογράφηση του μηνύματος. Φυσικά, ο αποστολέας θα πρέπει να χρησιμοποιήσει το ψηφιακό πιστοποιητικό του παραλήπτη για να αντλήσει από αυτό το αντίστοιχο δημόσιο κλειδί.

Σήμερα τα κυριότερα προγράμματα ηλεκτρονικού ταχυδρομείου έχουν ενσωματωμένη υποστήριξη για το πρωτόκολλο S/MIME (Secure / Multipurpose Internet Mail Extensions), το οποίο προσφέρει επιβεβαίωση ταυτότητας, ακεραιότητα δεδομένων και εμπιστευτικότητα κατά την ανταλλαγή ηλεκτρονικών μηνυμάτων. Επομένως διαθέτουν ήδη έτοιμες τις απαιτούμενες δυνατότητες, ώστε να κάνουν χρήση των υπηρεσιών που προσφέρει ένα περιβάλλον PKI. Παράλληλα, από την πλευρά του χρήστη, η δημιουργία ψηφιακής υπογραφής και η κρυπτογράφηση ενός μηνύματος διεκπεραιώνονται με ελάχιστους απλούς χειρισμούς, συνήθως με χρήση του ποντικιού (mouse).

Κατά συνέπεια, τα προγράμματα ηλεκτρονικού ταχυδρομείου μπορούν να χρησιμοποιηθούν άμεσα για την ασφαλή ανταλλαγή ηλεκτρονικών εγγράφων, στα πλαίσια των διάφορων επιχειρηματικών διαδικασιών, είτε ενδοεπιχειρησιακά είτε μεταξύ επιχειρήσεων. Φυσικά, κάτι τέτοιο προϋποθέτει ότι έχει προηγηθεί ο κατάλληλος σχεδιασμός και υλοποίηση της αντίστοιχης υποδομής.

11.2.3. Εικονικά ιδιωτικά δίκτυα (Virtual private networks – VPNs)

Παλαιότερα, η σύνδεση μεταξύ πληροφορικών συστημάτων που βρίσκονται σε διαφορετικές γεωγραφικές τοποθεσίες απαιτούσε συνήθως την χρήση επιλεγόμενων ή μισθωμένων γραμμών επικοινωνίας και αντίστοιχου εξειδικευμένου εξοπλισμού. Η μέθοδος αυτή προσφέρει βέβαια κάποιες δυνατότητες, παρουσιάζει όμως σημαντικά μειονεκτήματα, όπως αυξημένο κόστος εξοπλισμού, μεγάλες απαιτήσεις υποστήριξης και συντήρησης, μικρή ευελιξία και, κυρίως, δεν διασφαλίζει την διασύνδεση μεταξύ ετερογενών συστημάτων.

Με την εξάπλωση του Internet και των τεχνολογιών και προτύπων που το συνοδεύουν, είναι δυνατόν να διασυνδεθούν, σχετικά εύκολα, ποικίλα ετερογενή συστήματα, ακόμη και αν αυτά δεν ανήκουν σε μια επιχείρηση, αλλά σε περισσότερες. Ομως οι συνδέσεις μέσω Internet είναι γενικά ανασφαλείς και σε καμμιά περίπτωση δεν εξασφαλίζουν τα χαρακτηριστικά που απαιτούνται για ένα ασφαλές ηλεκτρονικό δίκτυο.

Τα εικονικά ιδιωτικά δίκτυα παρέχουν τη δυνατότητα να χρησιμοποιηθεί το Internet, σαν να ήταν ένα ιδιωτικό δίκτυο. Για το σκοπό αυτό, πρέπει, κατ' αρχήν, οι διακινούμενες πληροφορίες να είναι σε κρυπτογραφημένη μορφή. Ομως η πρόσβαση στο Internet δεν υπόκειται συνήθως σε συγκεκριμένους περιορισμούς και κανόνες και ένας οποιοσδήποτε κόμβος μπορεί να αποστείλει δεδομένα προς οποιονδήποτε άλλο. Απαιτείται επομένως η καθιέρωση και χρήση ταυτοτήτων για τους κόμβους που θα συμμετέχουν σε ένα ασφαλές δίκτυο. Στην περίπτωση λοιπόν των εικονικών ιδιωτικών δικτύων υπεισέρχεται η έννοια της ταυτότητας μιας μηχανής (ενός κόμβου) και όχι η ταυτότητα ενός χρήστη-προσώπου (αν και μπορεί επιπροσθετα να χρησιμοποιηθεί και αυτή).

Στην πραγματικότητα, η ταυτότητα ενός κόμβου προσδιορίζεται κυρίως από τη δικτυακή του διεύθυνση (IP address). Κατά συνέπεια, στα πλαίσια ενός περιβάλλοντος PKI, εκδίδεται για κάθε κόμβο ένα ψηφιακό πιστοποιητικό, το οποίο περιλαμβάνει την πιο πάνω διεύθυνση. Ενα εικονικό ιδιωτικό δίκτυο μπορεί να λειτουργήσει με διάφορους τρόπους, αλλά γενικά κάθε ένας από τους κόμβους έχει το ρόλο μιας τελικής οντότητας και αποδεικνύει την ταυτότητά του παρουσιάζοντας στους άλλους το ψηφιακό πιστοποιητικό του. Μέσω αυτού επαληθεύεται ότι ο υπ' όψη κόμβος "κατέχει" το αντίστοιχο ιδιωτικό κλειδί.

Μια επιχείρηση μπορεί να διαμορφώσει το δικό της εικονικό ιδιωτικό δίκτυο, ενοποιώντας τις γεωγραφικά διεσπαρμένες εγκαταστάσεις της ή να συμμετέχει μαζί με άλλες σε ένα ευρύτερο δίκτυο του παραπάνω τύπου. Η μέθοδος αυτή, μεταξύ των άλλων, προσφέρει πολύ μεγάλη ευελιξία, αλλά και δυνατότητα διασύνδεσης ποικίλων ετερογενών συστημάτων, εξασφαλίζοντας ταυτόχρονα όλα τα απαραίτητα χαρακτηριστικά ενός ηλεκτρονικού περιβάλλοντος υψηλής ασφάλειας.

11.2.4. Αλλες εφαρμογές

Οι δυνατότητες που προσφέρει ένα περιβάλλον PKI μπορούν να αξιοποιηθούν με ποικίλους τρόπους και να βρούν πλήθος διαφορετικών εφαρμογών, επιπλέον αυτών που αναφέρθηκαν παραπάνω. Ενα χαρακτηριστικό παράδειγμα είναι το ψηφιακά υπογρεγραμμένο λογισμικό (digitally signed software). Με δεδομένο ότι σήμερα ένα μεγάλο μέρος εφαρμογών λογισμικού διανέμεται μέσω του Internet (downloaded software), υπάρχει η ανάγκη της επιβεβαίωσης ότι το λογισμικό αυτό πράγματι προέρχεται από τον συγκεκριμένο κατασκευαστή και ότι δεν έχει υποστεί αλλοιώσεις κατά τη μεταφορά του. Με τη χρήση του PKI, ο κατασκευαστής ενός τέτοιου λογισμικού επισυνάπτει σ' αυτό την ψηφιακή υπογραφή του και, μαζί με το υπογεγραμμένο λογισμικό, αποστέλλει στους ενδιαφερόμενους και το ψηφιακό του πιστοποιητικό. Χρησιμοποιώντας το πιστοποιητικό αυτό, ο χρήστης που

παραλαμβάνει το λογισμικό μέσω του Internet μπορεί να βεβαιωθεί με ασφάλεια για την ταυτότητα του κατασκευαστή.

Ενα άλλο εξειδικευμένο παράδειγμα αφορά τη χρήση υπηρεσιών PKI σε συνδυασμό με το πολύ γνωστό λογισμικό SAP R/3, που ανήκει στην κατηγορία των συστημάτων ERP (Enterprise Resource Planning). Συγκεκριμένα, χρησιμοποιείται εξειδικευμένο λογισμικό (middleware) της εταιρίας SECUDE (τεχνολογικού εταίρου της SAP), μέρος του οποίου εγκαθίσταται στους προσωπικούς υπολογιστές των χρηστών. Το λογισμικό αυτό διαχειρίζεται, μεταξύ άλλων, τα ιδιωτικά κλειδιά των χρηστών και το αντίστοιχα ψηφιακά πιστοποιητικά, τα οποία και φυλάσσονται σε ειδικά προστατευμένα αρχεία (PSE files – Personal Security Environment files). Τα αρχεία PSE δημιουργούνται κεντρικά από τον διαχειριστή του SAP R/3 και στη συνέχεια διανέμονται στους χρήστες.

Ενας χρήστης, προκειμένου να χρησιμοποιήσει το SAP R/3, πρέπει προηγουμένως να έχει εφοδιαστεί με το αντίστοιχο αρχείο PSE, το οποίο εγκαθίσταται στο δίσκο του προσωπικού του υπολογιστή. Η κλασσική διαδικασία εισόδου στο σύστημα με χρήση password (logon procedure) καταργείται. Αντ' αυτής, ο χρήστης κάνει χρήση του λογισμικού SECUDE και πληκτρολογεί τον μυστικό κωδικό PIN που του έχει απονεμηθεί (επιβεβαιώνοντας την ταυτότητά του), ώστε να επιτραπεί η πρόσβαση στο αρχείο PSE. Αμέσως μετά το SECUDE αναλαμβάνει αφ' ενός να αποκαταστήσει μια κρυπτογραφημένη σύνδεση με τον SAP R/3 server και αφ' ετέρου να ενεργοποιήσει τον λεγόμενο SAP R/3 client, οπότε ο χρήστης έχει πλέον πλήρη, αλλά ασφαλή επικοινωνία με το σύστημα SAP R/3 και τις λειτουργίες του.

Γενικότερα, ένα σύστημα PKI προσφέρει τη δυνατότητα ενοποίησης των διαφόρων επιμέρους μηχανισμών ασφάλειας, όπως των ελέγχων πρόσβασης στα διάφορα υποσυστήματα. Για παράδειγμα, είναι δυνατόν ένας χρήστης να συνδεθεί και στο εταιρικό ERP σύστημα (SAP R/3 κλπ) και στο σύστημα ηλεκτρονικού ταχυδρομείου, χωρίς να εμπλακεί σε δύο διαφορετικές διαδικασίες αναγνώρισης τύπου "user-name/password" (όπως θα συνέβαινε σε ένα κλασσικό περιβάλλον), αλλά "επιδεικνύοντας" άπαξ το ψηφιακό του πιστοποιητικό και μόνο. Η τεχνική αυτή, γνωστή ως "single sign-on", είναι δυνατόν να επεκταθεί και σε περισσότερα των δύο υποσυστημάτων, με την προϋπόθεση ότι τα αντίστοιχα υποσυστήματα ενσωματώνουν (είτε εκ κατασκευής είτε με προσθήκη) δυνατότητες PKI.

12. ΣΤΑΔΙΑ ΥΛΟΠΟΙΗΣΗΣ ΟΛΟΚΛΗΡΩΜΕΝΟΥ ΣΥΣΤΗΜΑΤΟΣ PKI

Ενα εταιρικό σύστημα PKI χρησιμοποιείται από ένα οργανισμό για την υποστήριξη των διαδικασιών του, οι οποίες μπορεί να είναι είτε ενδοεταιρικής φύσεως είτε να σχετίζονται με τις συναλλαγές που πραγματοποιούνται με άλλες επιχειρήσεις είτε και τα δύο.
Ενα σύστημα PKI θα πρέπει να υλοποιηθεί με σκοπό να εξυπηρετήσει ξεκάθαρα καθορισμένους επιχειρηματικούς στόχους. Θεμελιώδη ερωτήματα που θα πρέπει να απαντηθούν είναι το ποιά είναι η φύση της επιχείρησης καθώς και το αν το υπό ανάπτυξη σύστημα PKI θα εξυπηρετήσει κυρίως εσωτερικές ανάγκες της επιχείρησης ή θα προσφέρει υπηρεσίες και στους πελάτες και τους προμηθευτές της ή πιθανόν και τα δύο.

Στη συνέχεια αναπτύσσονται τα διάφορα επιμέρους στάδια που απαιτούνται για την υλοποίηση ενός ολοκληρωμένου συστήματος PKI. Σε σχέση με τα προαναφερθέντα στο Κεφ. 10, η ανάπτυξη που ακολουθεί αναφέρεται περισσότερο στον 2ο τύπο υπηρεσιών Αρχής Πιστοποίησης, περιλαμβάνει όμως σημαντικές πληροφορίες που είναι χρήσιμες και για τους δύο άλλους τύπους ΑΠ.

1. Ανάλυση για τον καθορισμό των επιχειρησιακών απαιτήσεων (business requirements analysis)

Οι απαντήσεις που θα δοθούν στα παραπάνω ερωτήματα θα βοηθήσουν σημαντικά στον καθορισμό των επιχειρησιακών απαιτήσεων, οι οποίες και θα προσδιορίσουν τις προδιαγραφές, το σχεδιασμό και την υλοποίηση του συστήματος PKI.

Ο κυριότερος σκοπός αυτού του σταδίου είναι να προσδιοριστούν εκείνες οι επιχειρηματικές διαδικασίες (business processes), οι οποίες μπορούν να υποστηριχθούν από το σύστημα PKI, καθώς και το να καθοριστεί η φύση των αντίστοιχων υπηρεσιών PKI. Για παράδειγμα, η εξουσιοδότηση για την αγορά ενός είδους πιθανόν να απαιτεί την εξακρίβωση της ταυτότητας του ατόμου που εμπλέκεται, όπως επίσης να μπορεί να παρασχεθεί απόδειξη για το ότι η διαδικασία αγοράς ενεργοποιήθηκε από το συγκεκριμένο άτομο και τέλος να μπορεί να διασφαλιστεί η ακεραιότητα της προκύπτουσας συναλλαγής.

Είναι επίσης πιθανόν να αποφασιστεί η υλοποίηση ενός συστήματος PKI σε συνδυασμό με την ανάπτυξη μιας εφαρμογής, η οποία θα χρησιμοποιήσει υπηρεσίες ασφάλειας βασισμένες σε PKI. Στην περίπτωση αυτή θα πρέπει να γίνει συνολική θεώρηση των απαιτήσεων της επιχείρησης, προκειμένου να διασφαλιστεί ότι το υπό ανάπτυξη σύστημα PKI θα είναι σε θέση να εξυπηρετήσει γενικότερες ανάγκες και όχι μόνο τη συγκεκριμένη εφαρμογή.

2. Ανάλυση απαιτήσεων πολιτικής πιστοποιητικών (Certificate Policy requirements analysis)

Θα πρέπει να προσδιοριστεί η ποιότητα των υπηρεσιών ασφαλείας του PKI που χρειάζονται προκειμένου να υποστηριχθούν οι επιχειρηματικές διαδικασίες. Η ποιότητα αυτή συνήθως επιτυγχάνεται με τον καθορισμό πολιτικών πιστοποιητικών (Certificate Policies), οι οποίες καλύπτουν τα ακόλουθα θέματα:

- Υποχρεώσεις και ευθύνες που θα πρέπει να αναμένονται από τους κατόχους πιστοποιητικών, τους χρήστες των πιστοποιητικών και από την Αρχή Πιστοποίησης (ΑΠ).
- Διαδικασίες και πρακτικές για την εξακρίβωση και την επαλήθευση της ταυτότητας αυτών που καταθέτουν αιτήσεις και λαμβάνουν κλειδιά και πιστοποιητικά.
- Λειτουργικές διαδικασίες της Αρχής Πιστοποίησης (CA) για μια σειρά θεμάτων που περιλαμβάνουν την έκδοση και την ανάκληση πιστοποιητικών, την συλλογή εγγραφών ελέγχου (audit records) και την αρχειοθέτηση των εγγραφών.
- Φυσικοί και διαδικαστικοί έλεγχοι που περιλαμβάνουν μέτρα προστασίας για τις εγκαταστάσεις της Αρχής Πιστοποίησης, καθορισμό ρόλων της ΑΠ και αλλαγές και ανακτήσεις κλειδιών (key changeover and recovery).
- Ελεγχοι ασφαλείας για το προσωπικό της ΑΠ που περιλαμβάνουν άδειες φυσικής πρόσβασης, προσόντα, εμπειρίες και εκπαίδευση.
- Τεχνικά θέματα που αφορούν τη δημιουργία κλειδιών, την παράδοσή τους και τη χρήση τους,ειδικές κρυπτογραφικές διατάξεις, δεδομένα ενεργοποίησης διατάξεων καθώς και θέματα ασφαλείας υπολογιστών και δικτύων.
- Περιγραφή της δομής των πιστοποιητικών και των πινάκων ανάκλησης πιστοποιητικών – ΠΑΠ (CRLs).

Κατά το αρχικό αυτό στάδιο της διαδικασίας υλοποίησης δεν απαιτούνται σε βάθος λεπτομέρειες, όπως αυτές που υπάρχουν στις πολιτικές πιστοποιητικών. Θα μπορούσε πιθανόν να μην αναπτυχθεί καν πολιτική πιστοποιητικών, αλλά να υιοθετηθεί κάποια ήδη υπάρχουσα, η οποία να πλησιάζει στις ιδιαιτερότητες της επιχείρησης. Το σημαντικό είναι να σχηματισθεί μία εικόνα για την πολιτική πιστοποιητικών, η οποία να μπορεί να εκφραστεί σε γενικές γραμμές. Για παράδειγμα μπορεί να δηλώνει ότι τα πιστοποιητικά θα πρέπει να συμμορφώνονται προς το πρότυπο X.509, χωρίς να εξειδικεύει τα περιεχόμενα των διαφόρων πεδίων ή να αναγνωρίζει την ανάγκη για ισχυρούς κρυπτογραφικούς αλγόριθμους, χωρίς να προσδιορίζει επακριβώς το μήκος των κλειδιών. Αυτό το επίπεδο λεπτομέρειας θα βοηθήσει στον προσδιορισμό πιθανών λύσεων PKI και στην ανάλυση κόστους / οφέλους.

3. Διερεύνηση εναλλακτικών λύσεων PKI

Υπάρχει μια σειρά λύσεων PKI που είναι διαθέσιμες στην αγορά και ο αριθμός τους θα αυξάνεται με την πάροδο του χρόνου. Θα πρέπει τα προϊόντα αυτά να εξετασθούν και να εντοπισθούν εκείνα που μπορούν να ικανοποιήσουν τις απαιτήσεις της επιχείρησης. Ενδεικτικές παράμετροι που θα πρέπει να εξετασθούν είναι:

- η ωριμότητα του προϊόντος
- το πλήθος και το είδος των εγκαταστάσεων στις οποίες ήδη λειτουργεί
- το επίπεδο ικανοποίησης των χρηστών
- η συμμόρφωση με τα πρότυπα (PKI, κρυπτογραφία, επικοινωνίες, υπηρεσίες καταλόγου κλπ)
- η λειτουργικότητα του προϊόντος
- η διαθεσιμότητα ειδικών εργαλείων ολοκλήρωσης (integration tools) και η ευκολία χρήσης τους
- η διαθεσιμότητα και η ποιότητα προγραμμάτων εκπαίδευσης για το προϊόν
- η φιλοσοφία του κατασκευαστή για την εξέλιξη του προϊόντος και η στρατηγική των νέων εκδόσεων κλπ.

Στο τέλος αυτού του σταδίου θα έχει σχηματισθεί μια καθαρή εικόνα σχετικά με τις πιθανές διαθέσιμες λύσεις.

4. Ανασκόπηση της δικτυακής υποδομής

Το επόμενο βήμα είναι η ανασκόπηση της δικτυακής υποδομής και ο προσδιορισμός των απαιτούμενων εργασιών προκειμένου να επιτευχθεί η ολοκληρωμένη ένταξη (integration) των πιθανών λύσεων. Θα πρέπει να απαντηθούν ερωτήματα όπως:

- Ποιά είναι τα απαιτούμενα πρωτόκολλα
- Είναι ήδη σε χρήση ή θα πρέπει να υλοποιηθούν
- Υπάρχει διαθέσιμη μια συμβατή υπηρεσία καταλόγου (directory service)
- Θα απαιτηθεί πρόσβαση στις υπηρεσίες PKI της εταιρίας από το Internet
- Αν ναι, είναι ήδη η εταιρία συνδεδεμένη με το Internet
- Προστατεύονται με firewall τα σημεία εισόδου

5. Εκτίμηση κόστους / προσδοκώμενα οφέλη

Στο σημείο αυτό θα ήταν σκόπιμη η διεξαγωγή μιας ανάλυσης κόστους / οφέλους, η οποία μπορεί να αποβεί χρήσιμη προκειμένου να δικαιολογηθεί το κόστος της υλοποίησης του συστήματος PKI. Γενικά, η ύπαρξη μιας τέτοιας υποδομής (PKI) έχει ευρύτερες θετικές επιπτώσεις και μπορεί να μειώσει το κόστος ασφαλείας ολόκληρης της πληροφορικής (IT) υποδομής όλης της επιχείρησης.

Εκτίμηση κόστους

Τα επιμέρους στοιχεία κόστους για την υλοποίηση ενός συστήματος PKI μπορούν να διακριθούν σε τέσσερις κατηγορίες:

Προϊόντα / Τεχνολογίες
Εδώ περιλαμβάνονται το υλικό (hardware) και το λογισμικό (software) που είναι απαραίτητα για την διαμόρφωση και λειτουργία του συστήματος PKI και σε ό, τι αφορά τους κεντρικούς

υπολογιστές (servers), αλλά και τους σταθμούς εργασίας των χρηστών (client PCs). Εδώ υπάγεται και τυχόν εξειδικευμένος εξοπλισμός που θα απαιτηθεί, όπως έξυπνες κρυπτογραφικές κάρτες (smart cards), συσκευές βιομετρικής αναγνώρισης κλπ.

Εγκαταστάσεις
Με δεδομένο ότι η φιλοσοφία του PKI απαιτεί εξαιρετικά αυστηρούς μηχανισμούς ασφαλείας για τη λειτουργία των αντίστοιχων κεντρικών συστημάτων, είναι πιθανόν να χρειαστεί η βελτίωση των υφισταμένων εγκαταστάσεων ή η δημιουργία νέων

Προσωπικό
Στην κατηγορία αυτή θα περιληφθεί το κόστος του προσωπικού (είτε αυτό ανήκει στην επιχείρηση είτε προέρχεται από τρίτες εξειδικευμένες εταιρίες) που θα απασχοληθεί σε όλες τις φάσεις του έργου, όπως ανάλυση, σχεδίαση, ανάπτυξη, εφαρμογή, εκπαίδευση, υποστήριξη και συντήρηση.

Διαδικασίες
Κατά την ανάπτυξη ενός συστήματος PKI, η σχετική τεχνολογία θα πρέπει να ενσωματωθεί ομαλά μέσα στην ήδη υπάρχουσα πληροφορική υποδομή της επιχείρησης και θα πρέπει να διαμορφωθούν διαδικασίες λειτουργίας και υποστήριξης για το υπό ανάπτυξη παραγωγικό σύστημα. Σχετικά παραδείγματα είναι οι διαδικασίες αντιμετώπισης εκτάκτων περιστατικών, οι διαδικασίες έκδοσης πιστοποιητικών, οι διαδικασίες υποστήριξης των χρηστών κλπ.

Τα κόστη καθώς και τα υπέρ και τα κατά της υλοποίησης πιθανών λύσεων PKI θα πρέπει να διερευνηθούν. Θα μπορούσε επίσης να εξετασθεί η λήψη υπηρεσιών PKI από κάποιον αντίστοιχο παροχέα (provider), ενδεχόμενο το οποίο υπό προϋποθέσεις είναι δυνατόν να προσφέρει σημαντικές οικονομίες. Η ανάλυση θα πρέπει ξεκάθαρα να αναδεικνύει τα κόστη που συνεπάγεται για την επιχείρηση η υλοποίηση, η λειτουργία και η συντήρηση ενός ιδιόκτητου συστήματος PKI σε σχέση με το κόστος της αγοράς υπηρεσιών PKI από κάποια γνωστή και καθιερωμένη Αρχή Πιστοποίησης.

Προσδοκώμενα οφέλη

Η ύπαρξη ενός συστήματος PKI δεν προσφέρει αφ' εαυτής κάποια αξία. Τα οφέλη θα προέλθουν από τις επιχειρηματικές διαδικασίες, οι οποίες αξιοποιώντας τις δυνατότητες του PKI θα λειτουργήσουν με βελτιωμένη μορφή και θα είναι πιο αποδοτικές. Θα πρέπει λοιπόν πρώτα απ' όλα να αποφασιστεί κατά πόσο χαρακτηριστικά όπως επιβεβαίωση ταυτότητας, εμπιστευτικότητα δεδομένων, ακεραιότητα δεδομένων, ψηφιακές υπογραφές κλπ, τα οποία προσφέρει το PKI είναι απαραίτητα για τη διεξαγωγή των επιχειρηματικών διαδικασιών. Στη συνέχεια, η έμφαση θα πρέπει να δοθεί στά αναμενόμενα οφέλη από μια βελτιωμένη μορφή κάποιων συγκεκριμένων διαδικασιών, οι οποίες θα αξιοποιούν τα πιο πάνω χαρακτηριστικά ασφαλείας.

Γενικά, υπάρχουν τριών ειδών διαδικασίες που μπορούν να επωφεληθούν από τις δυνατότητες του PKI:

- Εσωτερικές (ενδο-εταιρικές)
- Σχετικές με πελάτες (B2C)
- Σχετικές με συνεργαζόμενες εταιρίες (B2B)

Αντίστοιχα, τα αναμενόμενα οφέλη μπορούν να διακριθούν, ανάλογα με τον τομέα που αφορούν, σε τέσσερις κατηγορίες:

- Οφέλη από αυξημένα έσοδα
- Οφέλη από μειώσεις κόστους
- Οφέλη από συμμόρφωση σε δεδομένες απαιτήσεις
- Οφέλη από περιορισμό κινδύνων

6. Επιλογή της βέλτιστης εναλλακτικής λύσης PKI

Είναι η στιγμή που η επιχείρηση, αξιοποιώντας την ανάλυση κόστους / οφέλους επιλέγει εκείνη την εναλλακτική λύση υλοποίησης του συστήματος PKI, η οποία προσιδιάζει περισσότερο προς τις ανάγκες της.

7. Στρατηγική ολοκλήρωσης-ενσωμάτωσης (integration) του συστήματος PKI

Ενα σύστημα PKI προσφέρει τη δυνατότητα να χρησιμοποιηθούν υπηρεσίες ασφαλείας που βασίζονται σε δημόσια κλειδιά προκειμένου να υποστηρίξουν τις λειτουργίες της επιχείρησης. Πριν όμως επωφεληθεί η επιχείρηση από τις υπηρεσίες αυτές, θα πρέπει να εντάξει τις κλήσεις προς αυτές μέσα στις πληροφορικές εφαρμογές της. Αυτό μπορεί να σημαίνει ότι οι εφαρμογές αυτές θα χρειαστεί να τροποποιηθούν ή να αναβαθμιστούν-αντικατασταθούν από άλλες που έχουν τέτοιου είδους κλήσεις ήδη ενσωματωμένες.

Είναι ιδιαίτερα σημαντικό να σχεδιαστεί έγκαιρα μια στρατηγική για την ομαλή ενσωμάτωση υπηρεσιών που βασίζονται στο PKI μέσα στο περιβάλλον της επιχείρησης. Ερωτήματα που θα πρέπει να απαντηθούν είναι τα εξής:

- Ποιοί είναι οι τύποι των εφαρμογών που διαθέτει η επιχείρηση
- Ποιά είναι τεχνικά η καλύτερη προσέγγιση για την ενσωμάτωση υπηρεσιών PKI (όπως αυτή εξηγήθηκε πιο πάνω)
- Θα τροποποιηθούν οι υπάρχουσες εφαρμογές ή θα γίνει αναβάθμιση σε PKI-ready πακέτα

Οι εφαρμογές που θα κάνουν χρήση των PKI υπηρεσιών θα ήταν προτιμότερο να εισαχθούν σταδιακά στην επιχείρηση, αρχίζοντας πιθανόν με το ηλεκτρονικό ταχυδρομείο (E-mail) και άλλες εφαρμογές αυτοματισμού γραφείου.

8. Ανασκόπηση πολιτικών και προτύπων

Αυτή η δραστηριότητα συνίσταται στην ανασκόπηση των πολιτικών και των διαδικασιών (policies and procedures), οι οποίες έχουν σχέση με τον τρόπο λειτουργίας της επιχείρησης, καθώς και όλων των προτύπων, πολιτικών και διαδικασιών που αφορούν την ασφάλεια, με σκοπό την κατανόηση του πλαισίου μέσα στο οποίο θα αναπτυχθούν οι πολιτικές πιστοποιητικών (certificate policies).

9. Ανάπτυξη / υιοθέτηση πολιτικής πιστοποιητικών

Τα αποτελέσματα της ανάλυσης των επιχειρησιακών απαιτήσεων (στάδιο 1.), της ανάλυσης απαιτήσεων πολιτικής πιστοποιητικών (στάδιο 2.) και της ανασκόπησης πολιτικών και προτύπων (στάδιο 8.) θα προσφέρουν την πληροφορίες που απαιτούνται ώστε είτε να υιοθετηθούν ήδη υπάρχουσες πολιτικές πιστοποιητικών είτε η επιχείρηση να αναπτύξει τις δικές της.

Οι πολιτικές πιστοποιητικών περιέχουν προδιαγραφές για ελέγχους ασφαλείας, διαδικασίες των αρχών πιστοποίησης (CA), πιστοποιητικά και κλειδιά, που θα πρέπει να υλοποιηθούν στα πλαίσια της υπό δημιουργία υποδομής. Εάν χρειάζεται να γίνονται αποδεκτά πιστοποιητικά που εκδίδει μια άλλη αρχή πιστοποίησης (CA), θα ήταν σκόπιμο να υιοθετηθούν ή να διαμορφωθούν πολιτικές που να συμμορφώνονται με το πλαίσιο που έχει καθοριστεί από την IETF (IETF Internet Public Key Infrastructure Certificate Policies and Certification Practices Framework - IETF PKIX Part 4).

10. Καθορισμός αρχιτεκτονικής του συστήματος PKI

Η αρχιτεκτονική του PKI είναι μια τυπική αρχιτεκτονική συστήματος. Θα πρέπει να καθορίζει, μεταξύ άλλων, τον εξοπλισμό (hardware), το λογισμικό (software), τα πρωτόκολλα επικοινωνίας, το λογισμικό για υλοποίηση υπηρεσιών καταλόγου (directory) και την αντίστοιχη δομή, κρυπτογραφικά πρότυπα, καθώς και την ασφάλεια των εγκαταστάσεων της Αρχής Πιστοποίησης.

11. Εκτίμηση απειλών και κινδύνων

Οι οργανισμοί του δημόσιου και του ιδιωτικού τομέα που διαθέτουν ήδη πολιτικές και πρότυπα για τη διαχείριση των κινδύνων για την ασφάλεια των πληροφοριακών συστημάτων πιθανόν να επιθυμούν να εκτιμήσουν την καταλληλότητα της αρχιτεκτονικής PKI και των τεχνικών και διοικητικών μέτρων ασφαλείας που προτίθενται να υλοποιήσουν, έτσι ώστε να προσδιορίσουν το επίπεδο του κινδύνου για τις λειτουργίες της Αρχής Πιστοποίησης, την οποία πρόκειται να δημιουργήσουν.

Μια μελέτη εκτίμησης απειλής και κινδύνου θα ήταν σκόπιμο να γίνει σ'αυτό το στάδιο της διαδικασίας, όπου η υλοποίηση του συστήματος PKI έχει εκφραστεί ήδη με επαρκείς λεπτομέρειες, είναι όμως ακόμη αρκετά νωρίς για να ενσωματωθούν στο σχεδιασμό του τα

συμπεράσματα της πιο πάνω μελέτης. Η μελέτη θα μπορούσε να οδηγήσει σε συστάσεις για την προσθήκη μέτρων ασφαλείας, εκεί όπου ο κίνδυνος προσδιορίζεται ως μη αποδεκτός.

12. Αναπροσαρμογή της πολιτικής πιστοποιητικών και της αρχιτεκτονικής PKI

Ανάλογα με τα αποτελέσματα της μελέτης εκτίμησης απειλών και κινδύνων (στάδιο 11.), πιθανόν να απαιτηθεί η τροποποίηση της πολιτικής πιστοποιητικών και της αρχιτεκτονικής PKI, έτσι ώστε να μειωθεί ο κίνδυνος σε ένα αποδεκτό επίπεδο.

13. Σχεδίαση του PKI

Η σχεδίαση του PKI της επιχείρησης θα εξαρτηθεί σε μεγάλο βαθμό από την πολιτική πιστοποιητικών που η (υπό δημιουργία) Αρχή Πιστοποίησης θα υποστηρίξει και από τη συγκεκριμένη λύση PKI που έχει επιλέξει η επιχείρηση.
Στο στάδιο αυτό θα γίνει η λεπτομερής περιγραφή της υλοποίησης του PKI που θα περιλαμβάνει τις προδιαγραφές και τη σύνθεση των διαφόρων τμημάτων του δικτύου (network segments), του εξοπλισμού (hardware) και του λογισμικού (software). Θα πρέπει να ετοιμαστεί ένας αναλυτικός κατάλογος που θα περιλαμβάνει υπολογιστές κεντρικής εξυπηρέτησης (servers), σταθμούς εργασίας, δρομολογητές (routers), συγκεντρωτές (hubs), καλώδια, κάρτες δικτύου, firewalls, συσκευές αδιάλειπτης παροχής ισχύος (UPS), καθώς και ο,τιδήποτε άλλο στοιχείο εξοπλισμού ή λογισμικού θα χρειαστεί να αγοραστεί. Επιπλέον θα πρέπει να συνταχθεί και ένας κατάλογος με τις μετατροπές που θα απαιτηθεί να γίνουν σε υπάρχοντα στοιχεία εξοπλισμού.

14. Σχεδιασμός των εγκαταστάσεων της Αρχής Πιστοποίησης

Με βάση τις πολιτικές πιστοποιητικών που έχουν αποφασιστεί, θα πρέπει να επιλεγούν και να σχεδιαστούν οι εγκαταστάσεις της Αρχής Πιστοποίησης. Ο σχεδιασμός τους θα πρέπει να καλύπτει τις κατασκευαστικές απαιτήσεις καθώς και τις προδιαγραφές για τα κατάλληλα μέτρα ασφαλείας. Επίσης θα πρέπει να περιλαμβάνει ένα κατάλογο με τον εξοπλισμό που θα πρέπει να αγοραστεί καθώς και ένα κατάλογο με τις μετατροπές που θα απαιτηθούν στην υπάρχουσα υποδομή.

15. Επιλογή προσωπικού που θα στελεχώσει το σύστημα PKI

Η αξιοπιστία των λειτουργιών της υπό δημιουργία Αρχής Πιστοποίησης θα εξαρτηθεί σε πολύ μεγάλο βαθμό από το προσωπικό που θα κληθεί να στελεχώσει το σύστημα PKI. Το ως άνω προσωπικό θα πρέπει να επιλεγεί με μεγάλη προσοχή και σύμφωνα με τα όσα έχουν συνομολογηθεί στις πολιτικές πιστοποιητικών.
Επιπλέον η επιλογή του προσωπικού στη φάση αυτή θα διασφαλίσει τη συμμετοχή του στις δραστηριότητες υλοποίησης, παρέχοντας ταυτόχρονα μια εξαιρετική ευκαιρία για εκπαίδευση στην πράξη (on-job training) και μεταφορά τεχνογνωσίας (knowledge transfer).

16. Εγχειρίδιο λειτουργίας Αρχής Πιστοποίησης (ΑΠ)

Τα εγχειρίδια που παρέχονται από τους προμηθευτές μαζί με τα σχετικά προϊόντα λογισμικού σπανίως προσφέρουν επαρκή τεκμηρίωση, διότι δεν περιλαμβάνουν τις λειτουργικές διαδικασίες που αφορούν τη συγκεκριμένη εγκατάσταση. Κατά συνέπεια, συνιστάται να διαμορφωθεί ένα εγχειρίδιο που να περιλαμβάνει λεπτομερείς διαδικασίες για τις καθημερινές λειτουργίες της υπ' όψη εγκατάστασης. Το εγχειρίδιο αυτό θα πρέπει επίσης να καλύπτει τη συντήρηση και την υποστήριξη.

17. Δήλωση διαδικασιών πιστοποίησης (Certification Practice Statement - CPS)

Προκειμένου να υποστηριχθούν οι νομικές απαιτήσεις, θα πρέπει να προετοιμαστεί και να δημοσιευτεί μια "Δήλωση Διαδικασιών Πιστοποίησης – ΔΔΠ", η οποία περιγράφει τις διαδικασίες και πρακτικές που θα ακολουθούνται από την υπό υλοποίηση Αρχή Πιστοποίησης κατά την έκδοση των πιστοποιητικών. Η δήλωση αυτή περιγράφει τον εξοπλισμό, τις πολιτικές και τις διαδικασίες που έχουν υιοθετηθεί και εφαρμόζονται, ώστε να ικανοποιούν τις προδιαγραφές των πολιτικών πιστοποιητικών (certificate policies).

Οπως και η πολιτική πιστοποιητικών, η δήλωση διαδικασιών πιστοποίησης θα πρέπει γενικά να είναι συνεπής με τη σύσταση IETF PKIX (Part 4). Ο βαθμός λεπτομέρειας θα πρέπει να είναι τέτοιος, ώστε η ΔΔΠ να μπορεί να δημοσιευτεί.

18. Λεπτομερές πρόγραμμα υλοποίησης συστήματος PKI

Οπως και για κάθε σύστημα πληροφορικής, θα πρέπει να προετοιμαστεί ένα λεπτομερές πρόγραμμα υλοποίησης, το οποίο θα καλύπτει δραστηριότητες όπως αγορά, εγκατάσταση, διαμόρφωση, δοκιμές, πιστοποίηση και εκπαίδευση. Το πρόγραμμα αυτό θα πρέπει επίσης να περιλαμβάνει λεπτομερές χρονοδιάγραμμα, με όλα τα επιμέρους έργα και τους απαιτούμενους πόρους, καθώς και ημερομηνίες έναρξης και ολοκλήρωσης για το καθένα.

19. Πρόγραμμα εκπαίδευσης

Θα πρέπει να διαμορφωθεί ένα πρόγραμμα εκπαίδευσης του προσωπικού και να προετοιμαστεί το κατάλληλο εκπαιδευτικό υλικό. Η εκπαίδευση θα περιλαμβάνει τις λειτουργίες, τη συντήρηση και την υποστήριξη του συστήματος. Ο "προμηθευτής της λύσης" (solution provider) πιθανόν να διαθέτει ήδη ένα επαρκές πρόγραμμα εκπαίδευσης, το οποίο θα πρέπει να προσαρμοστεί ώστε να περιλάβει όλες τις ειδικότερες διαδικασίες που έχουν σχέση με τη συγκεκριμένη εγκατάσταση.

20. Προμήθεια εξοπλισμού και λογισμικού

Στη φάση αυτή θα παραγγελθεί ο απαραίτητος εξοπλισμός και το απαιτούμενο λογισμικό. Η δραστηριότητα αυτή είναι δυνατόν να ξεκινήσει και νωρίτερα, προκειμένου να αποφευχθούν ανεπιθύμητες καθυστερήσεις.

21. Εγκατάσταση, διαμόρφωση και δοκιμές

Κατά τη διάρκεια αυτής της δραστηριότητας θα κατασκευαστούν οι εγκαταστάσεις της Αρχής Πιστοποίησης και θα εγκατασταθεί και ρυθμιστεί κατάλληλα ο εξοπλισμός και το λογισμικό, σύμφωνα με όσα προβλέπουν η τεκμηρίωση του σχεδιασμού και η δήλωση διαδικασιών πιστοποίησης.
Παράλληλα θα πρέπει να εκτελεστούν οι απαραίτητες δοκιμές. Αυτές θα περιλαμβάνουν ξεχωριστές δοκιμές των επιμέρους υποσυστημάτων κατά τη φάση της εγκατάστασης και ρύθμισης, καθώς και δοκιμές επιτυχούς ολοκληρωμένης λειτουργίας του συστήματος, μόλις όλα τα επιμέρους στοιχεία έχουν ρυθμιστεί κατάλληλα.

22. Εκπαίδευση

Η εκπαίδευση θα πρέπει να διεξαχθεί σύμφωνα με το πρόγραμμα που έχει καταρτισθεί σε προηγούμενο στάδιο (19.) Επιπλέον, το προσωπικό που θα στελεχώσει το σύστημα PKI είναι επιθυμητό να συμμετάσχει στις δραστηριότητες εγκατάστασης, διαμόρφωσης και δοκιμών του εξοπλισμού και λογισμικού.

23. Πιστοποίηση του συστήματος PKI

Η πιστοποίηση ενός συστήματος PKI είναι ιδιαίτερα σημαντική. Πρόκειται ουσιαστικά για μια διαδικασία με την οποία μετράται η πραγματική υλοποίηση του συστήματος PKI σε σχέση με τον αρχικό σχεδιασμό Η πιστοποίηση πιθανόν να πρέπει να γίνει λόγω καθιερωμένων επιχειρησιακών πολιτικών, οι οποίες υπαγορεύουν κάτι τέτοιο. Αυτός ο τύπος πιστοποίησης μπορεί να διεξαχθεί εσωτερικά. Εντούτοις, η διεξαγωγή της πιστοποίησης από μια ανεξάρτητη και ανεγνωρισμένη εταιρία θα συνεισφέρει αποφασιστικά στην αξιοπιστία των διαδικασιών της υπό υλοποίηση Αρχής Πιστοποίησης.

Είναι επίσης πιθανόν να απαιτηθεί η πιστοποίηση του συστήματος PKI στα πλαίσια ενός ανεξάρτητου προγράμματος, για παράδειγμα λόγω απαιτήσεων σχετικών με δια-πιστοποίηση (cross-certification). Στην περίπτωση αυτή η πιστοποίηση θα διεξαχθεί από ανεξάρτητους οργανισμούς που ακολουθούν μια τυποποιημένη διαδικασία.

Στοιχεία που θα αξιολογηθούν κατά τη διαδικασία της πιστοποίησης είναι οι πολιτικές πιστοποιητικών, η αρχιτεκτονική του συστήματος PKI, η φυσική σχεδίαση της Αρχής Πιστοποίησης και η δήλωση διαδικασιών πιστοποίησης. Οι διαδικασίες πιστοποίησης θα καλύψουν τα εξής:

- Εγκατάσταση και ρυθμίσεις του εξοπλισμού και του λογισμικού
- Εγκατάσταση και ρυθμίσεις των συστατικών στοιχείων του συστήματος PKI
- Εγκαταστάσεις της Αρχής Πιστοποίησης
- Δικτυακή πρόσβαση
- Προσωπικό και διαδικασίες λειτουργίας

Η πιστοποίηση λαμβάνει χώρα μετά την ολοκλήρωση των δοκιμών, αλλά πριν από την έναρξη της κανονικής λειτουργίας. Τυχόν ελλείψεις ή ανεπάρκειες πρέπει να καταγραφούν και να αναφερθούν και φυσικά να συνοδευτούν από διορθωτικές ενέργειες, ως αποτέλεσμα μιας αυστηρής διαδικασίας, η οποία θα περιλάβει τις αναγκαίες αναθεωρήσεις και ενημέρωση της σχετικής τεκμηρίωσης.

24. Λειτουργία

Στο σημείο αυτό μπορούν πλέον να γίνονται δεκτές αιτήσεις των ενδιαφερομένων και να εκδίδονται πιστοποιητικά, σύμφωνα με τις διαδικασίες που έχουν ήδη θεσμοθετηθεί, ολοκληρώνοντας τελικώς με επιτυχία την υλοποίηση του συστήματος PKI.

13. ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ ΚΑΙ ΣΥΣΤΗΜΑΤΑ PKI: Η ΝΟΜΙΚΗ ΔΙΑΣΤΑΣΗ

13.1. Γενικά περί υπογραφών: έννοια, μορφή, λειτουργία

Η χρήση της φυσικής ή χειρόγραφης υπογραφής αποτελεί κοινή πρακτική, αποδεκτή από όλους και έχει σκοπό π.χ. να επισημοποιήσει και να καταστήσει ισχυρή μια συμφωνία μεταξύ δύο μερών, δεσμεύοντάς τα ως προς την τήρηση των συμφωνηθέντων. Ταυτόχρονα, η κείμενη νομοθεσία περιλαμβάνει σειρά προβλέψεων για τα νομικά αποτελέσματα που παράγει μια υπογραφή.

Η χειρόγραφη υπογραφή σε ένα έγγραφο επί χάρτου (σε αντιδιαστολή με κάποιο ηλεκτρονικό έγγραφο) έχει τις εξής ιδιότητες:

- Μορφή: Είναι ένα πρόσθετο σημείο (σημάδι) που τίθεται πάνω στο ίδιο το έγγραφο. Συνήθως πρόκειται για την ιδιόχειρη αναγραφή του ονοματεπωνύμου του υπογράφοντος, μπορεί όμως να είναι οποιοδήποτε σημείο ή σύμβολο που προσδιορίζει την ταυτότητα του υπογράφοντος.
- Είναι ορατή "με τα μάτια".
- Προκαλεί μια "φυσική αλλοίωση" στο έγγραφο στο οποίο τίθεται.

Εξάλλου, οποιαδήποτε προσπάθεια εκ των υστέρων τροποποίησης του εγγράφου είναι δυνατόν να ανιχνευθεί, δεδομένων των φυσικών ιδιοτήτων του χάρτου και της μελάνης.

Η **λειτουργία της υπογραφής** που τίθεται σε ένα έγγραφο συνίσταται στο να προσφέρει **μαρτυρία για τρία πράγματα:**

1. Την ταυτότητα του υπογράφοντος: Είναι το σημαντικότερο στοιχείο που οποιαδήποτε μέθοδος υπογραφής πρέπει να παρέχει. Όταν ένα έγγραφο φέρει μια χειρόγραφη υπογραφή, τότε είναι αρκετό να προσκομισθεί μαρτυρία για την κανονική υπογραφή του υποτιθέμενου υπογράφοντος και την ομοιότητά της με την υπογραφή που φέρει το υπό εξέταση έγγραφο, ώστε να μετατεθεί το βάρος της απόδειξης για πιθανή πλαστογραφία στην πλευρά αυτού που φέρεται ως υπογράφων.
   Σημ. Στην περίπτωση μιας ηλεκτρονικής υπογραφής δεν παρέχεται τέτοιου είδους μαρτυρία, αλλά είναι δυνατόν να γίνει αποδεκτή κάποια εξωγενής μαρτυρία σχετικά π.χ. με το κρυπτογραφικό κλειδί του φερόμενου ως υπογράφοντος και η οποία να οδηγήσει σε αντίστοιχα συμπεράσματα.

2. Την πρόθεση του υπογράφοντος να υπογράψει το έγγραφο

3. Το ότι ο υπογράφων εγκρίνει και υιοθετεί τα περιεχόμενα του εγγράφου

Η ουσιαστική έννοια της υπογραφής είναι να διασφαλίζει τα τρία παραπάνω στοιχεία. Επομένως η δικαστική κρίση που πιθανόν να απαιτηθεί ως προς την εγκυρότητα μιας υπογραφής μπορεί να μην επικεντρώνεται αποκλειστικά και μόνο στη μορφή της υπογραφής, αλλά στη λειτουργία της. Αυτή η αλλαγή προσανατολισμού καθίσταται επιτακτικότερη, προκειμένου να αντιπετωπισθούν νομικά τα θέματα που προκύπτουν λόγω της μεγάλης εξάπλωσης των ηλεκτρονικών επικοινωνιών και της ανταλλαγής ηλεκτρονικών εγγράφων, τα οποία υπογράφονται επίσης ηλεκτρονικά και όχι με τον παραδοσιακό τρόπο.

13.2. Οι ηλεκτρονικές υπογραφές

Οι ηλεκτρονικές υπογραφές χρησιμοποιούνται ως ανάλογο των φυσικών υπογραφών, όταν τα έγγραφα που ανταλλάσσονται είναι σε ηλεκτρονική μορφή. Μια περίπτωση ηλεκτρονικής υπογραφής είναι η ψηφιακή εικόνα (digitized image) μιας χειρόγραφης υπογραφής, η οποία μπορεί να συνοδεύει ένα ηλεκτρονικό έγγραφο, η αξιοπιστία της όμως είναι χαμηλή. Αντίθετα, οι ψηφιακές υπογραφές που παράγονται με τη βοήθεια της κρυπτογραφίας, όπως έχει ήδη περιγραφεί στα προηγούμενα, αποτελούν μια ιδιαίτερα αξιόπιστη μέθοδο για την υπογραφή ηλεκτρονικών εγγράφων.

Οι ηλεκτρονικές υπογραφές μπορούν να επιτελέσουν όλες τις σχετικές απαιτούμενες λειτουργίες. Εντούτοις το προς υπογραφή αντικείμενο, δηλαδή το ηλεκτρονικό έγγραφο, δεν αποτελεί ένα φυσικό αντικείμενο με την συνηθισμένη έννοια, αλλά στην πραγματικότητα είναι μια σειρά δυαδικών ψηφίων (bits) 0 και 1, αποθηκευμένο συνήθως σε κάποιο ψηφιακό μέσο, π.χ. στο μαγνητικό δίσκο ενός υπολογιστή. Κατά συνέπεια είναι δύσκολο μια μέθοδος ηλεκτρονικής υπογραφής να ανταποκριθεί στην απαίτηση να έχει συγκεκριμένη μορφή. Εάν ο νόμος επέμενε στην απαίτηση μια έγκυρη υπογραφή να έχει τη μορφή ενός σημαδιού που τίθεται πάνω σε ένα έγγραφο, τότε καμμία μέθοδος ηλεκτρονικής υπογραφής δεν θα μπορούσε να θεωρηθεί έγκυρη. Μια άλλη επίσης ιδιομορφία του ηλεκτρονικού εγγράφου είναι ότι όταν τροποποιείται η νέα του έκδοση μπορεί να αποθηκευτεί π.χ. στο μαγνητικό δίσκο, αντικαθιστώντας την προηγούμενη. Η αλλαγή στο σύνολο των δυαδικών ψηφίων που αποτελούν το έγγραφο δεν μπορεί να ανιχνευθεί εξετάζοντας το ίδιο το έγγραφο.

Θα πρέπει να γίνει μια διάκριση ανάμεσα στην πληροφορία που περιέχει ένα έγγραφο και στον φορέα αυτής της πληροφορίας. Στην περίπτωση μιας χειρόγραφης υπογραφής ενός εγγράφου επί χάρτου, η υπογραφή αφ' ενός προκαλεί μια φυσική αλλοίωση στον φορέα (δηλ. τίθεται μελάνη πάνω στο χαρτί) και αφ' ετέρου προσθέτει πληροφορία.

Στην περίπτωση των ηλεκτρονικών υπογραφών τύπου "ψηφιακής εικόνας", μια ηλεκτρονική υπογραφή σε ένα ηλεκτρονικό έγγραφο απλώς προσθέτει πληροφορία, με την έννοια ότι και η ίδια αποτελείται από μια σειρά δυαδικών ψηφίων, που προστίθενται στο έγγραφο. Βέβαια, η επισύναψη μιας τέτοιας υπογραφής προκαλεί και μια φυσική αλλοίωση στο αποθηκευτικό μέσο, αλλά αυτό συμβαίνει σε "μικροσκοπικό" επίπεδο και είναι τελείως διαφορετική από ότι στην περίπτωση της φυσικής υπογραφής.

13.3. Οι ψηφιακές υπογραφές και οι ιδιομορφίες τους

Σε ό,τι αφορά τις ψηφιακές υπογραφές που παράγονται με χρήση κρυπτογραφικών μεθόδων, αυτές, όπως έχει εξηγηθεί διεξοδικά στα προηγούμενα, δεν προσθέτουν κάτι στο ίδιο το ηλεκτρονικό έγγραφο ούτε προκαλούν κάποιου είδους αλλοίωση στο φορέα του. Αντίθετα, συνοδεύουν το έγγραφο και συσχετίζονται λογικά με αυτό και με τον υπογράφοντα και μάλιστα με τέτοιο τρόπο ώστε να μην επιτρέπουν την τροποποίηση του εγγράφου, χωρίς αυτή να αφήσει κάποια ίχνη.

Οι ψηφιακές υπογραφές μπορούν να ανταποκριθούν στις λειτουργικές απαιτήσεις του νόμου (βλ. 13.1. παραπάνω, σημεία 1,2,3) εξίσου καλά με τις φυσικές υπογραφές, παρουσιάζουν όμως, σε σχέση με αυτές, σημαντικές διαφορές. Κατ' αρχήν, η ίδια η ψηφιακή υπογραφή δεν παρέχει επαρκή μαρτυρία για την ταυτότητα του υπογράφοντος. Για να εξασφαλισθεί αυτό, απαιτείται επιπλέον μαρτυρία, η οποία να συνδέει το κλειδί υπογραφής (ή όποια άλλη συσκευή χρησιμοποιείται για το σκοπό αυτό) με τον ίδιο τον υπογράφοντα. Κάτι τέτοιο θα μπορούσε να αποδειχθεί με την επίκληση εξωτερικής μαρτυρίας, όπως συμβαίνει και με τις χειρόγραφες υπογραφές. Συνήθως όμως, στην πράξη, ο παραλήπτης ενός ψηφιακά υπογρεγραμμένου εγγράφου επιθυμεί να είναι σε θέση να στηριχθεί στην υπογραφή χωρίς επιπλέον ελέγχους.
Στο σημείο αυτό υπεισέρχονται οι Αρχές Πιστοποίησης (ο ρόλος και η λειτουργία των οποίων έχει αναλυτικά περιγραφεί στα προηγούμενα), οι οποίες εκδίδουν τα ψηφιακά πιστοποιητικά, τα οποία πληροφορούν για την ταυτότητα του κατόχου και το δημόσιο κλειδί που χρησιμοποιείται, προκειμένου να επαληθευτεί η υπογραφή του σε κάποιο έγγραφο. Φυσικά έχει προηγηθεί από την πλευρά της Αρχής Πιστοποίησης ο έλεγχος όλων εκείνων των στοιχείων που διασφαλίζουν την αυθεντικότητα της ταυτότητας του κατόχου του πιστοποιητικού, καθώς και ότι αυτός κατέχει το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που περιλαμβάνεται στο πιστοποιητικό. Το πιστοποιητικό χρησιμοποιείται από τον παραλήπτη, προκειμένου αυτός να βεβαιωθεί για την ταυτότητα του υπογράφοντος.

Μια άλλη διαφορά είναι ότι στη διαδικασία της φυσικής υπογραφής ο υπογράφων πρέπει να παρίσταται ο ίδιος προσωπικά και να έχει το προς υπογραφή έγγραφο εμπρός του. Αντίθετα, στην διαδικασία της ψηφιακής υπογραφής υπάρχουν οι εξής δύο δυνατότητες:

- Το κλειδί υπογραφής βρίσκεται αποθηκευμένο στον υπολογιστή του υπογράφοντος και η υπογραφή τίθεται με την ενεργοποίηση κάποιας επιλογής σε ένα πρόγραμμα λογισμικού.

- Το κλειδί υπογραφής βρίσκεται αποθηκευμένο σε κάποια ειδική συσκευή (π.χ. έξυπνη κάρτα), η οποία πρέπει να είναι παρούσα και διαθέσιμη, ώστε το πρόγραμμα λογισμικού να επισυνάψει την υπογραφή.

Σε οποιαδήποτε από τις δύο περιπτώσεις, ένας τρίτος που πιθανόν να έχει πρόσβαση στον υπολογιστή του χρήστη ή στην ειδική συσκευή φύλαξης του κλειδιού, είναι δυνατόν να υπογράψει εκείνος. Κατά συνέπεια, μια ψηφιακή υπογραφή θα έπρεπε ίσως να αντιμετωπιστεί ως περισσότερο ανάλογη με μια σφραγίδα προτυπωμένης υπογραφής,

Παράλληλα, η πλευρά που ενδιαφέρεται να στηριχθεί σε μια ψηφιακή υπογραφή πιθανόν να χρειαστεί να προσκομίσει εξωτερική μαρτυρία ότι η υπογραφή τέθηκε με την εξουδιοδότηση του υπογράφοντος.

Οπως προκύπτει από τα παραπάνω, το μόνο που δεν είναι δυνατόν να επιτευχθεί με τη χρήση των ψηφιακών υπογραφών είναι το να προσθέσουν ένα ορατό σημάδι πάνω στο ίδιο το προς υπογραφή έγγραφο. Αυτό όμως δεν είναι δυνατόν να αποτελέσει εμπόδιο στην υιοθέτηση των ψηφιακών υπογραφών, δεδομένου μάλιστα ότι οι σύγχρονες ψηφιακές επικοινωνίες αποτελούν πια μια ευρέως διαδεδομένη μέθοδο που προσφέρει πλήθος πλεονεκτημάτων. Αντίθετα, η έμφαση θα πρέπει να δοθεί στη λειτουργία και όχι στη μορφή της υπογραφής. Ούτως ή άλλως, η υπογραφή δεν είναι ένα "πράγμα", αλλά μια διαδικασία. Δεν έχει σημασία αν το αποτέλεσμα της διαδικασίας είναι ένα ορατό όνομα, ένα σημάδι ή ένας λογικός (όχι φυσικός) μετασχηματισμός του εγγράφου. Αν αυτή η διαδικασία παρέχει επαρκή μαρτυρία ότι ένα πρόσωπο αποδέχεται και υιοθετεί ένα έγγραφο και το έγγραφο που τίθεται στην κρίση ενός δικαστηρίου είναι το ίδιο με αυτό στο οποίο εφαρμόστηκε η διαδικασία της υπογραφής, τότε το έγγραφο έχει υπογραφεί.

13.4. Νομικά ζητήματα προς αντιμετώπιση

Τα γενικότερα ζητήματα που θα πρέπει να αντιμετωπισθούν είναι τα εξής:

- Ψηφιακές υπογραφές: πώς ορίζονται, τι σχέση έχουν με τις χειρόγραφες υπογραφές, τι νομικά αποτελέσματα παράγουν.

- Ψηφιακά πιστοποιητικά: πώς ορίζονται, ποιοί τα εκδίδουν, με ποιές διαδικασίες και προϋποθέσεις γίνεται η έκδοσή τους, ποιές συνέπειες έχει η χρήση τους

- Αρχές Πιστοποίησης: Ποιοί μπορούν να παρέχουν υπηρεσίες πιστοποίησης και ποιό είναι το νομικό πλαίσιο για τη χορήγηση σχετικών αδειών, αν αυτό κρίνεται απαραίτητο.

Χαρακτηριστικά κείμενα νομικού χαρακτήρα που ασχολούνται με τα παραπάνω ζητήματα και τα οποία έχουν και διεθνές ενδιαφέρον είναι τα εξής:

- United Nations Model Law on Electronic Commerce (UNCITRAL)
- The U.S. Federal E-Sign Act – Jan.2000
- European Union: Directive 1999/93/EC on a Community framework for electronic signatures

Το τελευταίο, λόγω του ειδικότερου ενδιαφέροντος που παρουσιάζει, εξετάζεται αναλυτικά λίγο παρακάτω.

13.5. Διαμόρφωση διεθνούς νομικού πλαισίου: κρίσιμοι παράγοντες

Η διαμόρφωση ενός διεθνούς νομικού πλαισίου για την ασφαλή διεξαγωγή του ηλεκτρονικού εμπορίου παρουσιάζει προφανώς γενικότερο ενδιαφέρον. Βασικά, το κυριότερο θέμα που πρέπει να αντιπετωπισθεί είναι το κατά πόσο οι ηλεκτρονικές υπογραφές έχουν την ίδια ισχύ και εγκυρότητα με τις χειρόγραφες υπογραφές. Ειδικότερα, υπάρχουν ορισμένοι παράγοντες που θα πρέπει να ληφθούν υπ' όψη κατά την εξέταση των σχετικών νομικών ζητημάτων, με κύριους άξονες αναφοράς τους εξής:

1. τη νομική δομή που επιλέγει μια χώρα όταν νομοθετεί σχετικά με τις ηλεκτρονικές υπογραφές
2. τη νομική αναγνώριση των ηλεκτρονικών υπογραφών
3. τη σχέση μεταξύ αδειοδότησης, διαπίστευσης και περιορισμών της ευθύνης (αφορά ΑΠ)
4. την αλληλεπίδραση τεχνικών προτύπων και νομοθεσίας
5. τη διασυνοριακή αναγνώριση

13.5.1. Η νομική δομή για τις ηλεκτρονικές υπογραφές

Γενικά αναγνωρίζεται ότι η θέσπιση νομικών κανόνων δεν θα πρέπει να παρεμποδίζει την ανάπτυξη και αποδοχή νέων τεχνολογιών, οι οποίες πιθανόν να μην έχουν ακόμη εφευρεθεί. Σχετικά με το ζήτημα αυτό, υπάρχουν τρείς διαφορετικές προσεγγίσεις.

1. Η προδιαγεγραμμένη προσέγγιση
Η Γερμανία, η Ιταλία και η Μαλαισία ήταν από τις πρώτες χώρες που έθεσαν σε ισχύ νομοθεσία, η οποία αναφέρεται συγκεκριμένα σε ψηφιακές υπογραφές στα πλαίσια ενός περιβάλλοντος PKI και μόνο. Η προσέγγιση αυτή δεν επιτρέπει την εισαγωγή άλλων μεθόδων ασφάλειας. Το αποτέλεσμα είναι ότι η νομοθεσία στις χώρες αυτές θα πρέπει πιθανόν να αλλάξει, όταν αναπτυχθούν νέες τεχνολογίες. Επιπλέον, για τις δύο πρώτες αυτό προκύπτει και λόγω της υποχρέωσής τους για συμμόρφωση με την εν εξελίξει κοινοτική νομοθεσία στα πλαίσια της Ευρωπαϊκής Ενωσης.

2. Η προσέγγιση δύο βαθμίδων (two-tier approach)
Η προσέγγιση αυτή υιοθετείται από την οδηγία της Ευρωπαϊκής Ενωσης σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές. Η οδηγία κάνει διάκριση ανάμεσα σε μια "ηλεκτρονική υπογραφή" και σε μια "προηγμένη ηλεκτρονική υπογραφή", η οποία πληροί τα τέσσερα κριτήρια της μοναδικότητας, της ταυτότητας, της ασφάλειας και της ακεραιότητας. Επιπλέον, ένα αναγνωρισμένο πιστοποιητικό που ικανοποιεί τις σχετικές απαιτήσεις (παράρτημα Ι της οδηγίας) μπορεί να προσδιορίσει την ταυτότητα ενός προσώπου. Οι χώρες-μέλη θα πρέπει να αποδέχονται μια προηγμένη ηλεκτρονική υπογραφή που στηρίζεται σε ένα αναγνωρισμένο πιστοποιητικό με τον ίδιο τρόπο που ισχύει για τις χειρόγραφες υπογραφές.

Την ίδια προσέγγιση έχει ακολουθήσει και η Σιγκαπούρη, η σχετική νομοθεσία (Electronic Transactions Bill) της οποίας κάνει διάκριση ανάμεσα σε ηλεκτρονικές εγγραφές και υπογραφές από τη μια και σε ασφαλείς ηλεκτρονικές εγγραφές και υπογραφές από την άλλη.

Μια ηλεκτρονική υπογραφή μπορεί να επαληθεύεται με οποιονδήποτε τρόπο. Αντίθετα μια ασφαλής ηλεκτρονική υπογραφή οφείλει να ικανοποιεί συγκεκριμένα κριτήρια (που καθορίζονται από τη νομοθεσία), οπότε και αποτελεί τεκμήριο για τα εξής: ακεραιότητα του εγγράφου που φέρει τέτοιου είδους υπογραφή, ότι η υπογραφή ανήκει στο πρόσωπο με το οποίο συσχετίζεται και ότι το πρόσωπο αυτό είχε την πρόθεση να υπογράψει και να υιοθετήσει το περιεχόμενο του εγγράφου.

3. Η μινιμαλιστική προσέγγιση

Η προσέγγιση αυτή έχει ακολουθηθεί για παράδειγμα από την Αυστραλία και βασίζεται στο ότι δεν υπάρχει ομοιόμορφη διεθνής αντιμετώπιση του ζητήματος. Ετσι θεωρείται αρκετό η νομοθεσία της χώρας να προβλέπει ότι, όπου απαιτείται υπογραφή, θα πρέπει να υπάρχει μια μέθοδος που να προσδιορίζει το πρόσωπο που υπογράφει και την έγκρισή του για το περιεχόμενο του εγγράφου και η αξιοπιστία της μεθόδου να είναι ανάλογη με το σκοπό για τον οποίο χρησιμοποιείται το έγγραφο. Η προσέγγιση αυτή αφήνει την αγορά να αποφασίσει για θέματα που έχουν σχέση με το επίπεδο της ασφάλειας και της αξιοπιστίας.

13.5.2. Η νομική αναγνώριση των ηλεκτρονικών υπογραφών

Θα πρέπει να ληφθούν υπ΄ όψη τρία επιμέρους σημεία:

- Γενικά, δεν υπάρχει από το νόμο, ξεκάθαρη απαίτηση για υπογραφή σε κάθε περίπτωση
- Η αξία των ηλεκτρονικών υπογραφών είναι διαφορετική από χώρα σε χώρα
- Κάποιο μέρος πιθανόν να μη διαθέτει την τεχνολογία που είναι απαραίτητη, προκειμένου να παράσχει ή να αποδεχθεί μια ηλεκτρονική υπογραφή

Είναι επομένως συζητήσιμο το κατά πόσο η ηλεκτρονική υπογραφή θα πρέπει να είναι ισοδύναμη με την χειρόγραφη. Επιπλέον, υπάρχει ήδη ένα σύνολο διαδικασιών και κανόνων που αναφέρονται στην παρεμπόδιση της απάτης σε σχέση με τις χειρόγραφες υπογραφές και δεν είναι σαφές αν χρειάζεται ένα χωριστό σύνολο αντίστοιχων διαδικασιών για τις ηλεκτρονικές υπογραφές.

13.5.3. Η σχέση μεταξύ αδειοδότησης, διαπίστευσης και περιορισμών της ευθύνης (αφορά ΑΠ)

Το κατά πόσο υπάρχει ανάγκη μια Αρχή Πιστοποίησης ή Εμπιστη Τρίτη Οντότητα να λαμβάνει σχετική άδεια ή απλώς να διαπιστεύεται σε κάποιο αρμόδιο φορέα, εξαρτάται από τις απόψεις που έχει η αντίστοιχη κυβέρνηση σχετικά με το ζήτημα της ευθύνης. Γενικά θεωρείται ότι η νομική ευθύνη είναι πιο εύκολο να οριοθετηθεί σε κλειστά συστήματα που διέπονται από συγκεκριμένους κανόνες λειτουργίας, αποδεκτούς από τους συμμετέχοντες, παρά σε ένα ανοικτό περιβάλλον PKI. Προτείνεται πάντως το ζήτημα της ευθύνης να αντιπετωπίζεται οπωσδήποτε από το νόμο, εφ' όσον ένα σύστημα PKI ανοικτού τύπου εφαρμοστεί ευρέως, διότι ένα πρόσωπο πιθανόν να διαθέτει ένα κλειδί για πολλές χρήσεις, οπότε η ευθύνη δεν μπορεί να κατανεμηθεί τόσο εύκολα όσο σε ένα κλειστό περιβάλλον.

Εξάλλου, η αδειοδότηση των ΑΠ προσφέρει μεγαλύτερες δυνατότητες ελέγχου, αλλά είναι πιθανόν να παρεμποδίσει την ελεύθερη εξέλιξη των υπηρεσιών πιστοποίησης. Πιο ευέλικτο κρίνεται ένα μοντέλο που να προβλέπει την διαπίστευση των ΑΠ, εθελοντικά ή υποχρεωτικά, ενώ ο φορέας που παρέχει τη διαπίστευση μπορεί να είναι κρατικός ή ιδιωτικός. Στη συνέχεια, και λόγω ανταγωνισμού μεταξύ των ΑΠ, εκτιμάται ότι θα προκύψει βελτίωση των προσφερομένων υπηρεσιών πιστοποίησης.

13.5.4. Αλληλεπίδραση τεχνικών προτύπων και νομοθεσίας

Τα τεχνικά πρότυπα παίζουν ένα κρίσιμο ρόλο στην ανάπτυξη της αγοράς, παρ' όλο που κάποιο πρότυπο πιθανόν να αποτελέσει εμπόδιο σε ενδεχόμενες αλλαγές και εξελίξεις. Η θέσπιση τεχνικών προτύπων συνήθως επαφίεται σε φορείς που έχουν ιδρυθεί για τέτοιους σκοπούς. Εντούτοις, η σχέση μεταξύ τεχνικών προτύπων και νόμου έχει αλλάξει με την πάροδο του χρόνου και αυτό έχει επιταχυνθεί με την ανάπτυξη και διάδοση του Internet. Το κρίσιμο σημείο που θα πρέπει πάντως να προσεχθεί είναι ότι οι τεχνικές προδιαγραφές δεν θα πρέπει να σχετίζονται με νομικούς κανόνες, διότι τότε θα μπορούσαν να παρεμποδίσουν την εξέλιξη της αγοράς.

13.5.5. Διασυνοριακή αναγνώριση

Σχετικά με το ζήτημα αυτό, δύο είναι τα κύρια σημεία:

Αν η νομοθεσία για τις ψηφιακές υπογραφές διαφέρει μεταξύ των χωρών ως προς την απόδειξη της γνησιότητας της υπογραφής αφ' ενός και τις απαιτήσεις για τη λειτουργία των Αρχών Πιστοποίησης αφ' ετέρου, τότε οι ηλεκτρονικές συναλλαγές μεταξυ χωρών ή μεταξύ υπηκόων διαφορετικών χωρών θα είναι δύσκολο να διεξαχθούν.

Επιπλέον, αν μια ΑΠ απαιτείται να συμμορφώνεται με τους εκάστοτε τοπικούς νόμους και πρότυπα, τότε κάθε ΑΠ θα έπρεπε να εξετάσει το ενδεχόμενο να αποκτήσει μια άδεια σε κάθε δικαιοδοτική περιοχή. Αναμφίβολα, κάτι τέτοιο θα ήταν και δύσκολο, αλλά και εξαιρετικά δαπανηρό. Η σχετική οδηγία της Ευρωπαϊκής Ενωσης έχει συγκεκριμένες προβλέψεις για το θέμα αυτό.

13.6. Η οδηγία 1999/93/ΕC της Ευρωπαϊκής Ενωσης

Η οδηγία αυτή ουσιαστικά καθορίζει μια ενιαία νομοθετική βάση, κοινή για όλες τις χώρες της Ευρωπαϊκής Ενωσης, η οποία περιγράφει τα σχετικά με ηλεκτρονικές υπογραφές, ψηφιακά πιστοποιητικά και παροχή υπηρεσιών πιστοποίησης και θέτει τα ελάχιστα απαιτούμενα επίπεδα ασφάλειας, ενώ παράλληλα φροντίζει να διασφαλίσει την ελεύθερη διακίνηση των σχετικών προϊόντων και υπηρεσιών στην ενιαία αγορά.
Η οδηγία εκδόθηκε αφού ήδη ορισμένες χώρες (κυρίως η Γερμανία και η Ιταλία) είχαν αρχίσει να θεσπίζουν σε εθνικό επίπεδο νομοθεσία περί ψηφιακών υπογραφών και είχε

αρχίσει να δημιουργείται ανησυχία για το πόσο αυτό θα οδηγούσε τελικά σε μια ανεπιθύμητη πολυμορφία στο εσωτερικό της Ενωσης. Στη συνέχεια αναλύονται τα σημαντικότερα σημεία της οδηγίας, τα οποία και συνοδεύονται από τα αντίστοιχα σχόλια.

Κατ' αρχήν, η οδηγία ακολουθεί το μοντέλο των δύο βαθμίδων (βλ. παραπάνω) και παράλληλα προσπαθεί να είναι τεχνολογικά ουδέτερη, με την έννοια ότι δεν υιοθετεί κάποια συγκεκριμένη τεχνολογία. Βέβαια είναι αρκετά εμφανές ότι έχουν ληφθεί υπ' όψη οι έννοιες και ο τρόπος λειτουργίας που χαρακτηρίζει ένα σύστημα PKI, όπως έχει περιγραφεί αναλυτικά στα προηγούμενα κεφάλαια. Ετσι για παράδειγμα περιλαμβάνονται οι παρακάτω όροι (και οι σχετικοί ορισμοί τους), που σαφώς υπονοούν ένα σύστημα PKI, χωρίς όμως και να αναφέρονται ευθέως σ'αυτό (σε παρένθεση ο αντίστοιχος PKI όρος):

- δεδομένα δημιουργίας υπογραφής (ιδιωτικό κλειδί)
- δεδομένα επαλήθευσης υπογραφής (δημόσιο κλειδί)
- πιστοποιητικό (ψηφιακό πιστοποιητικό)
- παροχέας υπηρεσιών πιστοποίησης (Αρχή Πιστοποίησης)

13.6.1. Ηλεκτρονικές υπογραφές

Η οδηγία κάνει διάκριση ανάμεσα σε "ηλεκτρονικές υπογραφές" και "προηγμένες ηλεκτρονικές υπογραφές". Για τις πρώτες ορίζεται απλώς ότι "είναι δεδομένα σε ηλεκτρονική μορφή, τα οποία είναι συνημμένα ή λογικά συσχετιζόμενα με άλλα ηλεκτρονικά δεδομένα και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας". Ο ορισμός είναι τόσο ευρύς που θα αρκούσε να προσθέσει κανείς το όνομά του κάτω από ένα κείμενο ηλεκτρονικού ταχυδρομείου και να έχει έτσι μια ηλεκτρονική υπογραφή. Βέβαια, αυτός ο ιδιαίτερα ευρύς ορισμός δεν έχει και πολλές νομικές συνέπειες, διότι όλες σχεδόν οι προβλέψεις της οδηγίας ασχολούνται με τις "προηγμένες ηλεκτρονικές υπογραφές" και τα "αναγνωρισμένα πιστοποιητικά".

Μια **"προηγμένη ηλεκτρονική υπογραφή"** πρέπει να ανταποκρίνεται στις εξής απαιτήσεις:

- να συνδέεται μονοσήμαντα με τον υπογράφοντα
- να μπορεί να ταυτοποιήσει τον υπογράφοντα
- να έχει δημιουργηθεί με μέσα που ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο
- να συνδέεται με τα δεδομένα στα οποία αναφέρεται με τέτοιο τρόπο ώστε να μπορεί να εντοπισθεί οποιαδήποτε επακόλουθη αλλοίωση των δεδομένων.

Στην πραγματικότητα υπάρχει σήμερα μόνο μια τεχνολογία που να ανταποκρίνεται στις τέσσερις αυτές απαιτήσεις, αυτή της ασύμμετρης κρυπτογραφίας ή κρυπτογραφίας δημοσίου κλειδιού (public key cryptography). Η Ενωση, μέσω άλλων αρμόδιων φορέων και πρωτοβουλιών της (European Telecommunications Standards Institute - ETSI, European Electronic Signatures Standardization Initiative - EESSI) , έχει προεκτείνει και εξειδικεύσει

τις παραπάνω απαιτήσεις, ώστε να είναι δυνατή η παροχή συγκεκριμένων υπηρεσιών χρονοσήμανσης (time-stamping), "μη αποκήρυξης (non-repudiation)" κλπ.

Στα πλαίσια της οδηγίας, ο "υπογράφων" ορίζεται ως "το φυσικό ή νομικό πρόσωπο που κατεχει μια διάταξη (συσκευή) δημιουργίας υπογραφής και ενεργεί είτε για λογαριασμό του είτε εξ ονόματος φυσικού ή νομικού προσώπου ή οντότητας που εκπροσωπεί". Η "διάταξη (συσκευή) δημιουργίας υπογραφής" ορίζεται ως "διαμορφωμένο υλικό ή λογισμικό που χρησιμοποιείται για την εφαρμογή των δεδομένων δημιουργίας της υπογραφής". Ενα παράδειγμα τέτοιας συσκευής είναι μια έξυπνη κάρτα, αλλά υπάρχουν και άλλες επιλογές, όπως ο μαγνητικός δίσκος ενός υπολογιστή σε συνδυασμό με το αντίστοιχο λογισμικό.

Τα "δεδομένα δημιουργίας υπογραφής" είναι "μονοσήμαντα δεδομένα, όπως κώδικες ή ιδιωτικά κλειδιά κρυπτογραφίας που χρησιμοποιούνται από τον υπογράφοντα για τη δημιουργία ηλεκτρονικής υπογραφής". Ο όρος αυτός, κατά συνέπεια, αναφέρεται στο ιδιωτικό κλειδί, ενώ ο όρος "δεδομένα επαλήθευσης υπογραφής" ("δεδομένα, όπως κώδικες ή δημόσια κρυπτογραφικά κλειδιά, τα οποία χρησιμοποιούνται με σκοπό την επαλήθευση μιας ηλεκτρονικής υπογραφής") χρησιμοποιείται ως ουδέτερο τεχνολογικά συνώνυμο για το δημόσιο κλειδί. Το υλικό ή λογισμικό που χρησιμοποιείται για την επαλήθευση του δημόσιου κλειδιού ορίζεται ως "διάταξη (συσκευή) επαλήθευσης υπογραφής".

13.6.2. Πιστοποιητικά

Ως "πιστοποιητικό (certificate)" ορίζεται "μια ηλεκτρονική βεβαίωση που συνδέει δεδομένα επαλήθευσης υπογραφής με ένα πρόσωπο και επιβεβαιώνει την ταυτότητά του", ενώ "αναγνωρισμένο πιστοποιητικό" είναι "το πιστοποιητικό που ανταποκρίνεται στις απαιτήσεις του παραρτήματος Ι της οδηγίας και το οποίο εκδίδεται από φορέα παροχής υπηρεσιών πιστοποίησης, ο οποίος πληροί τις οριζόμενες στο παράρτημα ΙΙ απαιτήσεις".

13.6.3. Νομικά αποτελέσματα των ηλεκτρονικών υπογραφών

Σε ότι αφορά τη νομική ισχύ των ηλεκτρονικών υπογραφών και τη πιθανή ισοδυναμία τους με τις χειρόγραφες υπογραφές, η οδηγία θεσμοθετεί την ισοδυναμία αυτή, αλλά ειδικά και μόνο για τις προηγμένες ηλεκτρονικές υπογραφές. Συγκεκριμένα, ορίζεται ότι:

"Οι προηγμένες ηλεκτρονικές υπογραφές" (όπως ορίστηκαν παραπάνω):

A. ικανοποιούν τις νομικές απαιτήσεις υπογραφής σε σχέση με δεδομένα ηλεκτρονικής μορφής με τον ίδιο τρόπο που μια χειρόγραφη υπογραφή ικανοποιεί τις απαιτήσεις αυτές σε σχέση με δεδομένα επί χάρτου
B. γίνονται δεκτές ως αποδεικτικό στοιχείο σε νομικές διαδικασίες

Επιπλέον, καθιερώνεται σαν γενική αρχή (για οποιαδήποτε μορφή ηλεκτρονικών υπογραφών) ότι:
η νομική ισχύς μιας ηλεκτρονικής υπογραφής και η αποδοχή της ως αποδεικτικού μέσου σε νομικές διαδικασίες δεν απορρίπτεται μόνο λόγω του γενονότος ότι:

- είναι σε ηλεκτρονική μορφή ή
- δεν βασίζεται σε αναγνωρισμένο πιστοποιητικό ή
- δεν βασίζεται σε αναγνωσμένο πιστοποιητικό που εκδόθηκε από διαπιστευμένο φορέα παροχής υπηρεσιών πιστοποίησης ή
- δεν έχει δημιουργηθεί από ασφαλή διάταξη δημιουργίας υπογραφής

Στο σημείο αυτό απομένει να προσδιοριστεί με θετικό (και όχι αποθετικό) τρόπο, το πώς μπορεί να τεκμηριωθεί η απουσία νομικής ισχύος. Με άλλα λόγια, πώς είναι δυνατόν η άρνηση αποδοχής μιας ηλεκτρονικής υπογραφής να γίνει με άλλο τρόπο (και όχι με αναφορά στην ηλεκτρονική της μορφή), χωρίς όμως να παραβιαστεί η οδηγία. Π.χ. είναι πιθανόν να γίνεται επίκληση της αναξιοπιστίας της χρησιμοποιούμενης τεχνολογίας ή ανάρμοστης συμπεριφοράς κλπ.

13.6.4. Φορείς παροχής υπηρεσιών πιστοποίησης (Αρχές Πιστοποίησης)

Ως "φορέας παροχής υπηρεσιών πιστοποίησης (certificate service provider)" ορίζεται "ο φορέας ή το φυσικό ή νομικό πρόσωπο που εκδίδει πιστοποιητικά ή παρέχει άλλες υπηρεσίες συναφείς με ηλεκτρονικές υπογραφές". Ο ορισμός αυτός αντιστοιχεί προφανώς στην έννοια της "Αρχής Πιστοποίησης (ΑΠ)", όπως αυτή παρουσιάστηκε αναλυτικά στα προηγούμενα.

Τα πιστοποιητικά που εκδίδει ένας φορέας παροχής υπηρεσιών πιστοποίησης μπορούν να θεωρηθούν "αναγνωρισμένα (qualified)", εφόσον ικανοποιούν τις απαιτήσεις του παραρτήματος Ι. Ταυτόχρονα, ο φορέας που τα εκδίδει πρέπει να πληροί τις προϋποθέσεις που ορίζονται στο παράρτημα ΙΙ, οι οποίες συνοπτικά αναφέρουν ότι ο φορέας:

- λειτουργεί με επαρκή ασφάλεια
- λαμβάνει κατάλληλα μέτρα για να επαληθεύσει την ταυτότητα αυτών για τους οποίους εκδίδει πιστοποιητικά
- απασχολεί εκπαιδευμένο προσωπικό, το οποίο διαθέτει κατάλληλα προσόντα
- χρησιμοποιεί αξιόπιστα συστήματα υπολογιστών
- λαμβάνει μέτρα ώστε να εμποδίσει πλαστογραφήσεις και να διατηρήσει την εμπιστευτικότητα των κλειδιών υπογραφής
- διαθέτει επαρκείς οικονομικούς πόρους
- τηρεί κατάλληλα αρχεία
- δεν αποθηκεύει τα δεδομένα δημιουργίας υπογραφών (δηλ. τα ιδιωτικά κλειδιά)
- παρέχει τις κατάλληλες πληροφορίες σχετικά με τους όρους και τις προϋποθέσεις, υπό τις οποίες εκδίδονται τα πιστοποιητικά

Σχετικά με την άδεια λειτουργίας που πιθανόν πρέπει να λαμβάνει ένας φορέας παροχής υπηρεσιών πιστοποίησης λειτουργίας από κάποια υπερκείμενη αρχή, η οδηγία απαγορεύει ρητά το να έχει η άδεια αυτή υποχρεωτικό χαρακτήρα. Ενας φορέας μπορεί να προσφέρει υπηρεσίες, χωρίς να έχει λάβει οποιασδήποτε μορφής έγκριση ή εξουσιοδότηση για το σκοπό αυτό. Η προσέγγιση αυτή έχει ως στόχο να διευκολύνει την ελεύθερη ανάπτυξη της σχετικής αγοράς υπηρεσιών και να δώσει έμφαση στον ανταγωνισμό.

Εντούτοις, προβλέπεται η δυνατότητα θέσπισης ειδικών μηχανισμών εθελοντικής διαπίστευσης, με τη μορφή ειδικών οργανισμών ή σωμάτων, με σκοπό την επίτευξη βελτιωμένου επιπέδου παροχής υπηρεσιών πιστοποίησης. Οι παραπάνω οργανισμοί μπορεί να είναι δημόσιου ή ιδιωτικού χαρακτήρα και οι προϋποθέσεις λειτουργίας τους θα πρέπει να είναι αντικειμενικές, διαφανείς, ανάλογες και να μη οδηγούν σε διακρίσεις. Οι φορείς παροχής υπηρεσιών διαπίστευσης μπορούν, μετά από σχετική αίτηση, να λάβουν διαπίστευση, στην οποία ορίζονται τα δικαιώματα και οι υποχρεώσεις που διέπουν την παροχή υπηρεσιών πιστοποίησης.

Το σκεπτικό στο οποίο βασίζεται ένα σχήμα εθελοντικής διαπίστευσης είναι ότι αυτό θα αποτελέσει κίνητρο για τους παροχείς υπηρεσιών, ώστε να προσφέρουν υψηλότερο επίπεδο υπηρεσιών, προκειμένου να ικανοποιήσουν τις απαιτήσεις της διαπίστευσης, με την απόκτηση της οποίας θα προσελκύσουν εν δυνάμει πελάτες. Επιπλέον, ένα σχήμα εθελοντικής διαπίστευσης εκτιμάται ότι θα έχει μεγαλύτερη ευελιξία προσαρμογής στις μεταβαλλόμενες συνθήκες του τεχνολογικού περιβάλλοντος.

13.6.5. Ευθύνη

Η οδηγία προβλέπει επίσης ότι οι φορείς παροχής υπηρεσιών πιστοποίησης υπέχουν ευθύνη για πιθανές ζημίες που θα προκληθούν σε βάρος οποιουδήποτε προσώπου ή φορέα από τη χρήση των αναγνωρισμένων πιστοποιητικών που εκδίδουν. Η ευθύνη αυτή αφορά την ορθότητα των πληροφοριών που περιέχονται σε ένα πιστοποιητικό, καθώς και την ακρίβεια των πινάκων ανάκλησης πιστοποιητικών – ΠΑΠ (CRLs).

Ακόμη προβλέπεται ότι ένας φορέας παροχής υπηρεσιών πιστοποίησης έχει τη δυνατότητα να αναφέρει στο πιστοποιητικό πιθανούς περιορισμούς της χρήσης του, δηλαδή σε ποιές περιπτώσεις μπορεί το πιστοποιητικό να χρησιμοποιηθεί, όπως επίσης και το επιτρεπόμενο ύψος των συναλλαγών, με την προϋπόθεση ότι τα παραπάνω χαρακτηριστικά είναι αναγνωρίσιμα από τρίτους. Σε κάθε περίπτωση πάντως, ο εν λόγω φορέας δεν έχει ευθύνη για τυχόν χρήση του πιστοποιητικού που υπερβαίνει τους αναγραφόμενους σε αυτό περιορισμούς.

Να σημειωθεί ότι τα παραπάνω αφορούν το ελάχιστο επίπεδο ευθύνης των φορέων παροχής υπηρεσιών πιστοποίησης. Κατά συνέπεια τα κράτη-μέλη έχουν τη δυνατότητα να θέσουν πιο αυστηρούς όρους στο θέμα αυτό, δεν μπορούν όμως να καθορίσουν μικρότερη έκταση ευθύνης για τους εν λόγω φορείς.

13.6.6. Διεθνείς πτυχές

Η οδηγία αναγνωρίζει ότι η ανάπτυξη του διεθνούς ηλεκτρονικού εμπορίου απαιτεί διασυνοριακές ρυθμίσεις με τρίτες χώρες και ότι για τη διασφάλιση της διαλειτουργικότητας σε παγκόσμιο επίπεδο, συμφωνίες αμοιβαίας αναγνώρισης υπηρεσιών πιστοποίησης θα είναι επωφελείς. Στο πνεύμα αυτό, ορίζει ότι αναγνωρισμένα πιστοποιητικά που έχουν εκδοθεί από φορέα παροχής υπηρεσιών πιστοποίησης εγκατεστημένο σε τρίτη χώρα θεωρούνται νομικώς

ισοδύναμα με τα αντίστοιχα που εκδίδονται από φορέα παροχής υπηρεσιών πιστοποίησης εγκατεστημένο σε χώρα της Κοινότητας, εφόσον ισχύει ένας από τους παρακάτω όρους:

- ο φορέας παροχής υπηρεσιών πιστοποίησης ικανοποιεί τις απαιτήσεις που περιλαμβάνονται στην οδηγία και έχει λάβει διαπίστευση από μηχανισμό διαπίστευσης εγκατεστημένο σε χώρα-μέλος
- κάποιος φορέας παροχής υπηρεσιών πιστοποίησης, εγκατεστημένος στην Κοινότητα και ο οποίος πληροί τις απαιτήσεις της οδηγίας, εγγυάται για το πιστοποιητικό
- το πιστοποιητικό του φορέα αναγνωρίζεται βάσει διμερούς ή πολυμερούς συμφωνίας μεταξύ της Κοινότητας και τρίτων χωρών ή διεθνών οργανισμών.

Πέρα από τα ανωτέρω αναφερθέντα, η οδηγία ασχολείται, μεταξύ άλλων, με το να διασφαλίσει ότι οι εθνικές νομοθεσίες των χωρών-μελών δεν θα παρεμποδίσουν την ελεύθερη διακίνηση υπηρεσιών και προϊόντων ηλεκτρονικών υπογραφών και πιστοποίησης, καθώς και με την προστασία των δεδομένων προσωπικού χαρακτήρα. Τέλος, ζητεί από τις χώρες-μέλη να προσαρμόσουν τις εθνικές τους νομοθεσίες, ώστε να συμμορφώνονται με την οδηγία.

Η Ελλάδα έχει προχωρήσει στην ζητούμενη προσαρμογή, με την έκδοση του Π.Δ. Αρ. 150 (ΦΕΚ: 125/25-6-2001). Το σχετικό κείμενο αποτελεί στο μεγαλύτερο μέρος του πιστή μεταφορά των αντίστοιχων αναφορών και προβλέψεων της οδηγίας, οπότε μπορεί να θεωρηθεί ότι τα παραπάνω αναφερθέντα ισχύουν και για την τρέχουσα Ελληνική Νομοθεσία.

14. ΣΥΖΗΤΗΣΗ – ΣΥΜΠΕΡΑΣΜΑΤΑ

Οι τεχνολογικές εξελίξεις στο χώρο των υπολογιστών και των επικοινωνιών (με έμφαση στο Internet) και η αξιοποίηση των σχετικών δυνατοτήτων από τις επιχειρήσεις έχει οδηγήσει στη σημαντική βελτίωση πολλών επιχειρηματικών διαδικασιών και έχει προσφέρει μια σειρά από πλεονεκτήματα, όπως ταχύτητα στη διεκπεραίωση των διαδικασιών, μεγαλύτερη αποτελεσματικότητα, αύξηση του επιπέδου εξυπηρέτησης πελατών, παγκόσμια εμβέλεια κλπ. Τα παραπάνω οφείλονται κυρίως στο γεγονός ότι, σε πολλές περιπτώσεις, η ροή των απαιτουμένων πληροφοριών, είτε ενδοεταιρικά είτε από και προς τους προμηθευτές και τους πελάτες της επιχείρησης, διεξάγεται πλέον ηλεκτρονικά με χρήση των τεχνολογιών που προαναφέρθηκαν.

Παρ'όλα αυτά, η ροή των πληροφοριών δεν μπορεί να αυτοματοποιηθεί πλήρως, διότι, μέχρι και σήμερα, ένα πολύ μεγάλο μέρος των επιχειρηματικών διαδικασιών στηρίζεται ακόμη στη δημιουργία και διακίνηση εγγράφων επί χάρτου. Αυτό είναι λογικό, αν σκεφθεί κανείς ότι οι παραδοσιακές διαδικασίες με χρήση χάρτου έχουν μεγάλη προϊστορία και έχουν ενσωματώσει, μεταξύ άλλων, επαρκείς μηχανισμούς ασφάλειας, οι οποίοι είναι γνωστοί, κατανοητοί και αποδεκτοί από όλους τους εμπλεκομένους (ιδιόχειρες υπογραφές, πρωτότυπα έγγραφα, σφραγισμένοι φάκελοι, συμβολαιογραφικές πράξεις κλπ). Παράλληλα, το αντίστοιχο νομικό υπόβαθρο είναι ήδη διαθέσιμο, ως αποτέλεσμα εμπειρίας δεκάδων ή και εκατοντάδων ετών.

Στο ψηφιακό περιβάλλον αντίθετα, οι μέχρι πρόσφατα διαθέσιμοι μηχανισμοί ασφάλειας παρουσίαζαν μια σειρά αδυναμίες, όπως η έλλειψη τυποποίησης, ο κατακερματισμός και η πολυμορφία των ελέγχων πρόσβασης στα πληροφοριακά συστήματα, η ανεπάρκεια και οι αυξημένες πιθανότητες παραβίασής τους κλπ. Ταυτόχρονα, η χρήση του Internet ως φορέα διακίνησης εμπιστευτικών πληροφοριών είναι πηγή επιπλέον κινδύνων, δεδομένου ότι το Internet από μόνο του είναι εξ ορισμού (λόγω σχεδιασμού) ανασφαλές. Επιπλέον, οποιαδήποτε προσπάθεια για την αύξηση του επιπέδου ασφάλειάς του είναι εξαιρετικά δύσκολη και αμφίβολης αποτελεσματικότητας, δεδομένης της αποκεντρωμένης φύσης του. Παράλληλα, το σχετικό νομικό πλαίσιο, όπου υπήρχε, ήταν μέχρι πρόσφατα περιορισμένο και ασαφές.

Οι ψηφιακές υπογραφές και τα συστήματα PKI έρχονται ουσιαστικά αφ'ενός να καλύψουν τις αδυναμίες και τα κενά που προαναφέρθηκαν και αφ'ετέρου να προσφέρουν τις δυνατότητες για τη δημιουργία ενός ολοκληρωμένου περιβάλλοντος ηλεκτρονικού εμπορίου, το οποίο θα διασφαλίζει τις τέσσερις βασικές αρχές της εμπιστευτικότητας, της επιβεβαίωσης ταυτότητας, της ακεραιότητας δεδομένων και της μη αποκήρυξης.

Το βασικό ζητούμενο σε ένα ψηφιακό περιβάλλον είναι η δημιουργία και χρήση κάποιου είδους ψηφιακών ταυτοτήτων (αναλόγων προς τις συνήθεις ταυτότητες), βάσει των οποίων θα μπορούν οι χρήστες (και γενικά οι εμπλεκόμενοι: φυσικά ή νομικά πρόσωπα ή μηχανές) να συμμετάσχουν σε ηλεκτρονικές συναλλαγές, φέροντας παράλληλα στο ακέραιο και όλες τις συνεπαγόμενες ευθύνες.

Είναι προφανές ότι οι ψηφιακές αυτές ταυτότητες θα πρέπει να έχουν συγκεκριμένες ιδιότητες και να εκδίδονται με τέτοιο τρόπο ώστε να μπορεί κάποιος να τις εμπιστευθεί (trusted identities). Στα πλαίσια ενός συστήματος PKI, μια ψηφιακή ταυτότητα ή ψηφιακό πιστοποιητικό είναι μια ηλεκτρονική διαβεβαίωση ότι ένας χρήστης (ή οντότητα γενικώς) είναι ο νόμιμος (και μοναδικός) κάτοχος ενός συγκεκριμένου κρυπτογραφικού κλειδιού. Η διαβεβαίωση αυτή σφραγίζεται/υπογράφεται ψηφιακά από μια ειδική οντότητα, γνωστή ως Αρχή Πιστοποίησης (ΑΠ), η οποία είναι και ο εκδότης της υπ' όψη ταυτότητας. Εάν οι χρήστες εμπιστεύονται την ΑΠ, τότε κατ' επέκταση εμπιστεύονται και τις ψηφιακές ταυτότητες που αυτή εκδίδει.

Η τεχνολογία πάνω στην οποία στηρίζονται οι ψηφιακές υπογραφές και τα συστήματα PKI (ασύμμετρη κρυπτογραφία, αλγόριθμοι κατατεμαχισμού κλπ) υπάρχει εδώ και είκοσι περίπου έτη, μόνο πρόσφατα όμως έχει γνωρίσει μεγάλη διάδοση και αξιοποίηση. Οι κυριότεροι λόγοι είναι αφ'ενός η μεγάλη εξάπλωση του Internet και η απαίτηση για ασφαλείς επικοινωνίες μέσω αυτού και αφ'ετέρου η εξέλιξη της τεχνολογίας των προσωπικών υπολογιστών που οδήγησε σε πολύ ισχυρούς (αλλά όχι ακριβούς) επεξεργαστές, οι οποίοι είναι σε θέση να εκτελούν γρήγορα και αποδοτικά τις απαιτούμενες κρυπτογραφικές λειτουργίες, ώστε αυτές να είναι διαθέσιμες για όλους. Παράλληλα, έχει αρχίσει και η διαμόρφωση του σχετικού νομικού πλαισίου αναφορικά με τις ψηφιακές υπογραφές και την αναγνώρισή τους, το ρόλο και τις προϋποθέσεις λειτουργίας των Αρχών Πιστοποίησης κλπ.

Γενικά, ένα σύστημα PKI αφορά τη δημιουργία και διαχείριση εμπιστοσύνης. Από τη σκοπιά αυτή, καίριος είναι ο ρόλος της Αρχής Πιστοποίησης (ΑΠ), η οποία στο ψηφιακό περιβάλλον δρά με τρόπο ανάλογο μιας υπηρεσίας διαβατηρίων και είναι επιφορτισμένη με μια σειρά καθηκόντων. Η υλοποίηση μιας ΑΠ είναι εφικτή μέσω συγκεκριμένων λύσεων που προσφέρουν διάφοροι κατασκευαστές, ειδικευμένοι στο αντικείμενο αυτό. Οι λύσεις αυτές περιλαμβάνουν εξειδικευμένο λογισμικό (αλλά και εξοπλισμό), μέσω του οποίου παρέχεται η δυνατότητα εκτέλεσης των λειτουργιών μιας ΑΠ.

Είναι σαφές ότι ένα σύστημα PKI δεν είναι μια ειδική εφαρμογή που εξυπηρετεί κάποιες συγκεκριμένες διαδικασίες, αλλά αποτελεί ουσιαστικά μια γενικότερη υποδομή ασφάλειας των πληροφοριακών συστημάτων μιας επιχείρησης, προς την κατεύθυνση της δημιουργίας ενός ασφαλούς περιβάλλοντος ηλεκτρονικού εμπορίου. Οπως συμβαίνει με μια υποδομή οποιουδήποτε τύπου, η ωφέλεια δεν προέρχεται από την υποδομή αυτή καθ' εαυτή, αλλά από την χρήση της και την αξιοποίηση των δυνατοτήτων που αυτή προσφέρει.

Εντούτοις, θα πρέπει να σημειωθεί ότι η πολυπλοκότητα ενός συστήματος PKI είναι ιδιαίτερα μεγάλη, ενώ η υλοποίησή του παρουσιάζει αρκετές δυσκολίες, λόγω του ότι θα πρέπει να ενταχθεί μέσα στο ήδη υπάρχον πληροφορικό περιβάλλον της επιχείρησης, πράγμα το οποίο θα απαιτήσει, ενδεχομένως, εκτεταμένο ανασχεδιασμό, με παράλληλη προσαρμογή του PKI στις ειδικές απαιτήσεις ασφάλειας της εταιρίας.

Με βάση τα παραπάνω και με δεδομένο το μεγάλο κόστος που συνεπάγεται η ανάπτυξη ενός πλήρους συστήματος PKI για όλη την επιχείρηση, η ορθότερη προσέγγιση είναι η οργάνωση ενός πιλοτικού έργου, μικρής κλίμακας, με προσεκτική επιλογή ορισμένων μόνο

επιχειρηματικών διαδικασιών, ο ανασχεδιασμός και η ένταξη των οποίων στο περιβάλλον του PKI αναμένεται να αποδώσει άμεσα και συγκεκριμένα οφέλη. Βέβαια, παρά το ότι η υλοποίηση στην περίπτωση αυτή αφορά ίσως ένα μόνο επιμέρους υποσύστημα, η σχεδίαση του PKI περιβάλλοντος θα πρέπει από τη φάση αυτή να γίνει έχοντας κατά νούν ότι αυτό πιθανότατα θα περιλάβει το σύνολο της επιχείρησης και των διαδικασιών της. Γενικότερα, η επιτυχής έκβαση ενός συγκεκριμένου έργου υλοποίησης PKI θα κριθεί από το πόσο ομαλά θα ενταχθεί μέσα στο υπάρχον πληροφορικό περιβάλλον της επιχείρησης και από το πόσο εύκολη θα είναι η χρήση του. Σε καμμιά περίπτωση δεν θα πρέπει οι χρήστες να είναι υποχρεωμένοι να αντιλαμβάνονται τα πολύπλοκα θέματα που σχετίζονται με τα κρυπτογραφικά κλειδιά και τα ψηφιακά πιστοποιητικά, ενώ στην ιδανική περίπτωση θα ήταν επιθυμητό η ύπαρξη του PKI να μην είναι "ορατή" στους χρήστες (PKI transparency).

Εξάλλου η λειτουργία της Αρχής Πιστοποίησης, η οποία μεταξύ άλλων προϋποθέτει και εγκαταστάσεις υψηλής ασφάλειας και αντίστοιχου κόστους, μπορεί αρχικά να εκχωρηθεί σε τρίτους φορείς που αναλαμβάνουν την παροχή τέτοιου είδους υπηρεσιών. Στη συνέχεια και ανάλογα με την πορεία του έργου, η επιχείρηση μπορεί είτε να συνεχίσει την εκχώρηση είτε, έχοντας πλέον και σχετική εμπειρία, να αναλάβει η ίδια τη λειτουργία της ΑΠ, εφ'όσον αυτό κριθεί απαραίτητο.

Σε κάθε περίπτωση, θα πρέπει, πριν από την έναρξη λειτουργίας του συστήματος, να έχουν εκπονηθεί και να είναι διαθέσιμα τα σχετικά συνοδευτικά κείμενα: "Πολιτική Πιστοποιητικών (ΠΠ)" και "Δήλωση Διαδικασιών Πιστοποίησης (ΔΔΠ)". Τα κείμενα αυτά καθορίζουν τους κανόνες λειτουργίας του συστήματος PKI και περιγράφουν το τι και το πώς, σχετικά με την έκδοση και χρήση των ψηφιακών πιστοποιητικών, στα πλαίσια του υπ' όψη συστήματος. Εννοείται ότι αν το υπ' όψη σύστημα PKI δεν προορίζεται να εξυπηρετήσει μια μόνο επιχείρηση, αλλά πρόκειται να καλύψει τις ανάγκες μιας ομάδας εταιριών που είναι, για παράδειγμα, μέλη μιας εφοδιαστικής αλυσίδας ή μιας χαλαρότερης "κοινότητας ενδιαφέροντος", τότε θα πρέπει οι παραπάνω πολιτικές και διαδικασίες να σχεδιαστούν από κοινού ή τουλάχιστον να γίνουν αποδεκτές από όλους τους συμμετέχοντες.

Θα πρέπει να γίνει απόλυτα κατανοητό ότι το PKI δεν είναι απλά μια ακόμα τεχνολογία Πληροφορικής (όπως π.χ. DBMS, ERP, Internet κλπ), αλλά περιλαμβάνει επίσης, ως αναπόσπαστο μέρος του, πολιτικές και διαδικασίες, έχει δε παράλληλα και νομικές προεκτάσεις. Οποιες επιχειρηματικές διαδικασίες στηρίζονται σε PKI και ιδιαίτερα αυτές που σχετίζονται με το εξωτερικό περιβάλλον της επιχείρησης θα πρέπει να έχουν ευθείες αναφορές στο υπάρχον νομικό πλαίσιο, είτε μέσω των τυποποιημένων συνοδευτικών κειμένων (ΠΠ, ΔΔΠ) είτε με χρήση πρόσθετων κειμένων/συμφωνιών (π.χ. Σύμβαση εξαρτώμενου μέρους – Relying party agreement κλπ).

Χωρίς αμφιβολία, οι ψηφιακές υπογραφές και τα συστήματα PKI αποτελούν μια σχετικά νέα και σχετικά πολύπλοκη τεχνολογία, της οποίας η διάδοση είναι σχετικά περιορισμένη. Παρ' όλα αυτά, είναι ουσιαστικά η μόνη τεχνολογία που μπορεί να διασφαλίσει τις τέσσερις θεμελιώδεις αρχές (εμπιστευτικότητα, επιβεβαίωση ταυτότητας, ακεραιότητα και μη αποκήρυξη) που απαιτούνται για τη δημιουργία ενός περιβάλλοντος ασφαλούς ηλεκτρονικού

εμπορίου. Κατά συνέπεια, η τεχνολογία αυτή παρουσιάζει μεγάλες προοπτικές ευρύτερης αποδοχής και εξάπλωσης, υπό τις εξής όμως προϋποθέσεις:

Α. Οι κατασκευαστές των σχετικών προϊόντων λογισμικού θα πρέπει να δώσουν μεγαλύτερη έμφαση στη συμμόρφωσή τους προς τα υπάρχοντα και τα αναπτυσσόμενα πρότυπα, ώστε να εξασφαλιστεί στο μεγαλύτερο δυνατό βαθμό η διαλειτουργικότητα (interoperability) μεταξύ των διαφόρων προϊόντων και να διευκολυνθεί η επικοινωνία μεταξύ εταιριών (ή μεταξύ ομαδων εταιριών) που χρησιμοποιούν προϊόντα PKI διαφορετικών κατασκευστών. Επίσης σημαντικός είναι και ο ρόλος των προσφερομένων εργαλείων (tool kits), με τη βοήθεια των οποίων επιταχύνεται η προσαρμογή ειδικών εφαρμογών της κάθε επιχείρησης, ώστε αυτές να ενταχθούν ομαλά μέσα στο υπό ανάπτυξη περιβάλλον PKI.

Β. Θα πρέπει να υπάρξει περαιτέρω ανάπτυξη προτύπων (standards) και ειδικότερα σε σχέση με τις πολιτικές πιστοποιητικών, την αυτόματη αναγνώριση και επεξεργασία τους χωρίς τη μεσολάβηση του χρήστη, καθώς και τη διαδικασία της διαπιστοποίησης (cross-certification).

Γ. Θα πρέπει να επιλυθεί το θέμα της ασφαλούς αποθήκευσης των ιδιωτικών κρυπτογραφικών κλειδιών και ιδιαίτερα αυτών που χρησιμοποιούνται για τη δημιουργία ψηφιακών υπογραφών. Προσφορότερη λύση φαίνεται να είναι η χρήση των έξυπνων κρυπτογραφικών καρτών (smart cards), η χρήση των οποίων θα επιλύσει ταυτόχρονα και το πρόβλημα της μεταφερσιμότητας (portability) του ιδιωτικού κλειδιού.

Δ. Τέλος, σημαντικό ρόλο θα παίξει και η εξέλιξη της νομοθεσίας, τόσο σε εθνικό όσο και σε διεθνές επίπεδο, έτσι ώστε να αναγνωρισθούν νομικά οι ψηφιακές υπογραφές και να διασφαλιστεί ότι οι ηλεκτρονικά υπογραφόμενες συναλλαγές θα έχουν δεσμευτικό αποτέλεσμα για τους υπογράφοντες. Επιπλέον, περαιτέρω επεξεργασία χρειάζεται και το πλαίσιο λειτουργίας των Αρχών Πιστοποίησης.

Από μια άλλη οπτική γωνία, οι ψηφιακές υπογραφές και τα συστήματα PKI έχουν να προσφέρουν κάτι σημαντικότερο από την απλή διασφάλιση των διακινουμένων πληροφοριών. Πρώτον, προσφέρουν τη δυνατότητα κατάργησης επιχειρηματικών διαδικασιών που βασίζονται σε ανταλλαγή παραδοσιακών εγγράφων επί χάρτου και αντικτάστασή τους με αντίστοιχες όπου θα χρησιμοποιούνται ψηφιακά έγγραφα, τα οποία, εφ'όσον χρειάζεται, θα υπογράφονται και ψηφιακά (π.χ. ηλεκτρονικά συμβόλαια ψηφιακά υπογεγραμμένα). Η δυνατότητα πλήρους αυτοματοποίησης των διαδικασιών και εξάλειψης της χρήσης χάρτου σαν μέσου αποθήκευσης και διακίνησης της πληροφορίας θα έχει μια σειρά ευεργετικών αποτελεσμάτων, όπως μεγάλες μειώσεις κόστους, αποφυγή λαθών, επιτάχυνση διαδικασιών, αύξηση αποτελεσματικότητας και αξιοπιστίας, αύξηση εσόδων κλπ.
Δεύτερον, προσφέροντας ασφαλή διακίνηση πληροφορίας πάνω από το Internet, θα οδηγήσουν στην υπέρβαση του φυσικού διαχωρισμού λόγω απόστασης και θα επιτρέψουν σε προμηθευτές και σε πελάτες (αλλά και σε απομακρυσμένους εργαζόμενους) να ανταλλάσσουν δεδομένα με το εσωτερικό εταιρικό δίκτυο, μέσω ασφαλούς και ελεγχόμενης πρόσβασης. Με τον τρόπο αυτό, το PKI προσφέρει τη δυνατότητα δημιουργίας ενός ασφαλούς περιβάλλοντος, μέσω του οποίου τα μέλη μιας εφοδιαστικής αλυσίδας μπορούν να αλληλοενημερώνονται συνεχώς, π.χ. σχετικά με προϊόντα και υπηρεσίες που υπόκεινται σε

διαρκείς αλλαγές και να πληροφορούνται σε πραγματικό χρόνο για το ύψος των αποθεμάτων. Επιτυγχάνοντας συνεπώς τη βελτιστοποίηση της ροής πληροφοριών, η εφοδιαστική αλυσίδα θα είναι σε θέση να ανταποκριθεί καλύτερα στις αυξημένες απαιτήσεις ενός επιχειρηματικού περιβάλλοντος το οποίο διαρκώς μεταβάλλεται.

Οι δύο παραπάνω παράγοντες, δηλ. η κατάργηση της χρήσης του χάρτου από τις επιχειρηματικές διαδικαδίες και η υπέρβαση του φυσικού διαχωρισμού λόγω απόστασης με παράλληλη βελτιστοποίηση της ροής πληροφοριών αναμένεται να είναι οι κινητήριες δυνάμεις που θα οδηγήσουν στην ευρύτερη αποδοχή των συστημάτων PKI και στην εξάπλωση της χρήσης των ψηφιακών υπογραφών στο άμεσο μέλλον.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Warwick Ford, Michael Baum: Secure Electronic Commerce – Copyright 2001 Prentice Hall

2. Andrew Nash et al: PKI – Implementing and managing E-Security – Copyright 2001 McGraw Hill

3. Thomas Austin: PKI - A Wiley Tech Brief - Jonh Wiley & sons, Dec.2000

4. PKI Forum: PKI Policy white paper – March 2001

5. PKI Forum: PKI Basics – A business perspective – April 2002
   URL: http://www.pkiforum.org/resources.html

6. Chris Reed: "What is a signature?" – October 2000
   URL: http://elj.warwick.ac.uk/jilt/00-3/reed.html

7. Stephen Mason: "Electronic Signatures in the EU and world e-commerce: technical and legal ramifications" – 1999
   URL: http://www.itsecurity.com/papers/digsig.htm

8. SANS Institute / Tim Kennedy: Aligning PKI technology and business goals – May 2001
   URL: http://rr sans.org/encryption/PKI_tech.php

9. SANS Institute / Keith Ainsworth: Non-repudiation – simple to understand, difficult to implement – November 2000
   URL: http://rr.sans.org/covertchannels/non-repudiation.php

10. IBM / Stacy Cannady, Thomas Stockton: How PKI can reduce the risks associated with e-business transactions – February 2001
    URL: http://www.ibm.com/developerworks/library/s-pain.html

11. Gartner Consulting: The evolution of E-Business security requirements – white paper - 2001

12. Diane E. Levine: PKI adds security to E-Business – Informationweek.com - May 2000

13. Barbara Depompa Reimers: PKI's are still tough to deploy – Internetweek.com - April.2001

14. RSA Security: Understanding Public Key Infrastructure – white paper – 2001
    URL: http://www.rsasecurity.com

15. Michael Ranger: PKI – Securing E-Business across the supply chain
URL: http://www.ascet.com/documents.asp?d_ID=223

16. Digital Signature Trust: Digital Signatures and Public Key Infrastructure
URL: http://www.digsigtrust.com/support/pki_basics.html

17. Linux Documentation Project (LDP): Smart Card HOWTO - "The relation of smart cards with PKI"
URL: http://linux.microstore.gr/LDP/HOWTO/Smart-Card-HOWTO/smartpki.html

18. Verisign Inc.: Public Key Infrastructure – The Verisign Difference
URL: http://www.verisign.com/whitepaper/enterprise/difference/introduction.html

19. Verisign's Certification Practice Statement
URL: http://www.verisign.com/repository/CPS

20. Verisign's Relying Party Agreement
URL: http://www.verisign.com/repository/rpa.html

21. Εφημερίδα των Ευρωπαϊκών Κοινοτήτων: Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 1999 σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές – 19.1.2000

22. Εφημερίς της Κυβερνήσεως της Ελληνικής Δημοκρατίας – Αρ. Φύλλου 125 – 25 Ιουνίου 2001 – Προεδρικό Διάταγμα υπ' αριθ. 150: Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.