Σημειώσεις για το μάθημα Ασφάλεια Πληροφοριακών Συστημάτων

http://thalis.cs.unipi.gr/~dpolemi

Δρ. Δέσποινα Πολέμη
Λέκτορας
dpolemi@unipi.gr

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ[1]

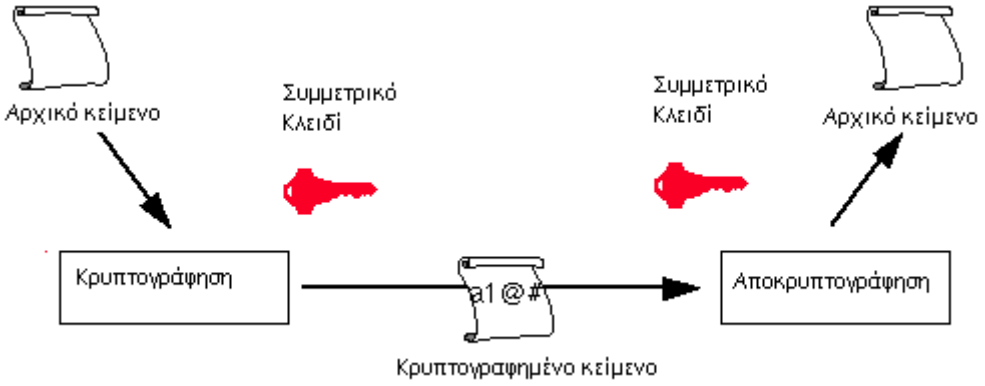
[1] *Τα κεφάλαια **1,4,5** είναι βασισμένα στην υπό προετοιμασία διδακτορική διατριβή του υποψήφιου διδάκτορα Αλέξανδρου Καλιοντζόγλου [8].*

1. ΣΤΟΙΧΕΙΑ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

Η *κρυπτογραφία* μπορεί να χρησιμοποιηθεί προκειμένου μηνύματα που κινούνται πάνω απο ανοιχτά δίκτυα να προστατευθούν απο υποκλοπή. Αυτό σημαίνει ότι ένα κρυπτογραφημένο μήνυμα αποτρέπει οποιονδήποτε να διαβάσει το μήνυμα καθώς αυτό περνάει απο τους διάφορους κόμβους του δικτύου μέχρι να φτάσει στον παραλήπτη του. Η κρυπτογραφία επίσης μπορεί να εξασφαλίσει την ακεραιότητα του μηνύματος, δηλαδή μπορεί να αποτρέψει κάποιον απο το να μεταβάλλει, διαγράψει ή εισάγει bits στα δεδομένα ενός μηνύματος χωρίς αυτό να γίνει αντιληπτό απο τον παραλήπτη. Τα *κρυπτογραφικά κλειδιά* είναι επί της ουσίας μεγάλοι τυχαίοι αριθμοί που ελέγχουν την διαδικασία της κρυπτογράφησης.

1.1 ΣΥΜΜΕΤΡΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

Στην παραδοσιακή κρυπτογραφία, το ίδιο κρυπτογραφικό κλειδί χρησιμοποιείται για να κρυπτογραφήσει και να αποκρυπτογραφήσει πληροφορία. Αυτό είναι πλέον γνωστό ως *μυστικό κλειδί (secret key)* και ο τύπος της κρυπτογραφία ως *συμμετρική κρυπτογραφία* επειδή δύο οντότητες που θέλουν να επικοινωνήσουν ασφαλώς, χρησιμοποιούν το ίδιο κλειδί για να την υλοποιήσουν. Ειδικότερα, οι οντότητες λαμβάνουν και οι δύο τα κλειδιά τους με χρήση ενός ασφαλούς μέσου (ίσως και εκτός δικτύου) και πρέπει να τα προστατεύσουν προκειμένου να εξασφαλίσουν ότι μόνο εξουσιοδοτημένες οντότητες μπορούν να χρησιμοποιήσουν την πληροφορία.



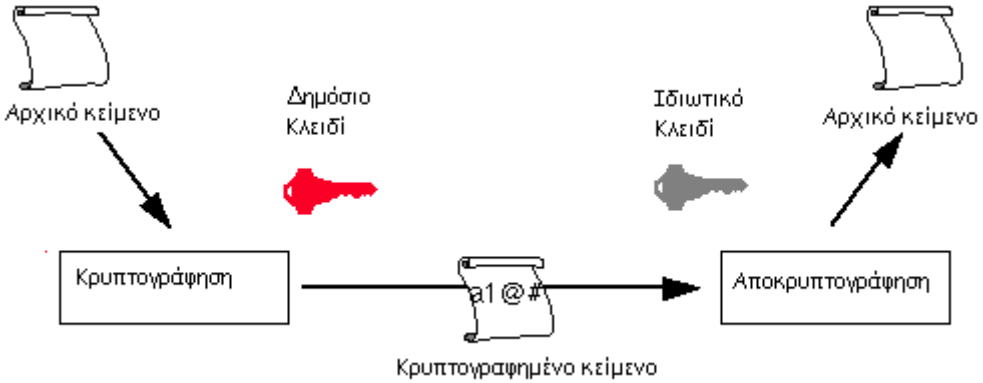
Συμμετρική κρυπτογράφηση

Η συμμετρική κρυπτογραφία διακρίνεται απο τα προβλήματα ότι όσο μεγαλώνει ο αριθμός των οντοτήτων, η διαχείριση των κλειδιών γίνεται όλο και πιο δύσκολη και ότι επειδή και οι δύο οντότητες χρησιμοποιούν το ίδιο κλειδί δεν μπορεί κάποιος να αποδείξει απο που ξεκίνησε το κρυπτογραφημένο μήνυμα. Συνηθισμένοι αλγόριθμοι συμμετρικής κρυπτογραφία είναι ο Data Encryption Standard – DES (NIST 1988), ο Triple DES – 3DES, ο Advanced Encryption Standard – AES (NIST 2001).

1.2 ΚΡΥΠΤΟΓΡΑΦΙΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

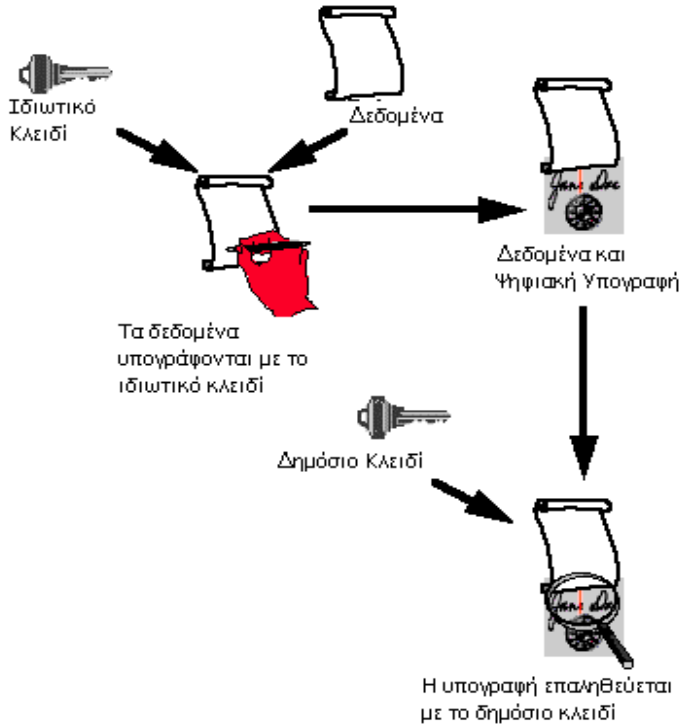
Μια διαφορετική προσέγγιση της κρυπτογραφίας ονομάζεται *κρυπτογραφία δημοσίου κλειδιού ή ασύμμετρη κρυπτογραφία*. Αυτή η μορφή, χρησιμοποιεί δύο διαφορετικά αλλά μαθηματικά συσχετιζόμενα κλειδιά. Το ένα μπορεί να χρησιμοποιηθεί χωρίς να μπορεί να ανακαλυφθεί το άλλο. Με την κρυπτογραφία δημοσίου κλειδιού, το *δημόσιο κλειδί* μπορεί, όπως λέει και το όνομά του, να δημοσιοποιηθεί σε οποιονδήποτε θέλει να κάνει μια συναλλαγή με την οντότητα που κρατάει το *ιδιωτικό κλειδί*. Η διανομή του δημοσίου κλειδιού είναι εύκολη. Το ιδιωτικό κλειδί πρέπει να κρατηθεί κρυφό και να μπορεί να το χρησιμοποιήσει μόνο ο ιδιοκτήτης του. Ένας δημοφιλής αλγόριθμος κρυπτογραφίας

δημοσίου κλειδιού είναι ο RSA, τον οποίον ανακάλυψαν ο R. Rivest, ο A. Shamir και ο L. Adleman.
Στην κρυπτογραφία δημοσίου κλειδιού προκειμένου να κρυπτογραφηθούν κάποια δεδομένα, γίνεται χρήση του δημοσίου κλειδιού και το ιδιωτικό κλειδί χρησιμοποιείται μόνο για την αποκρυπτογράφησή τους. Οποιαδήποτε απο τις οντότητες που γνωρίζουν το δημόσιο κλειδί μπορεί να κρυπτογραφήσει δεδομένα με παραλήπτη τον ένα και μοναδικό κάτοχο του ιδιωτικού κλειδιού.



Κρυπτογράφηση με κρυπτογραφία δημοσίου κλειδιού

Η κρυπτογραφία δημοσίου κλειδιού, μπορεί επίσης να χρησιμοποιηθεί για την δημιουργία μη παραποιούμενων *ψηφιακών υπογραφών* βασισμένων στο ιδιωτικό κλειδί κάποιου χρήστη. Το γεγονός ότι το ιδιωτικό κλειδί το έχει μόνο ο ιδιοκτήτης του, σημαίνει ότι το αποτέλεσμα οποιασδήποτε συνάρτησης χρησιμοποιεί το κλειδί αυτό, μπορεί να θεωρηθεί ότι έχει επιτελεστεί απο τον συγκεκριμένο ιδιοκτήτη και κανέναν άλλο. Μια ψηφιακή υπογραφή δημιουργείται απο την χρήση του ιδιωτικού κλειδιού προκειμένου να «υπογραφούν» ηλεκτρονικά δεδομένα με τέτοιο τρόπο που να μην μπορεί να πλαστογραφηθεί.



Παραγωγή ψηφιακών υπογραφών με κρυπτογραφία δημοσίου κλειδιού

Οι ψηφιακές υπογραφές είναι ισχυρότερες απο τις γραπτές διότι η υπογραφή είναι μαθηματικά δεμένη με τα υπογεγραμμένα δεδομένα. Η ψηφιακή υπογραφή δεν μπορεί να μεταφερθεί απο ένα κείμενο σε άλλο και οποιαδήποτε αλλαγή στα υπογεγραμμένα δεδομένα, ακυρώνει την υπογραφή. Η ψηφιακή υπογραφή δημιουργείται απο τα προς υπογραφή δεδομένα και το ιδιωτικό κλειδί και προστίθεται στο μήνυμα. Οποιοσδήποτε λαμβάνει το μήνυμα επιτελεί μια διαφορετική συνάρτηση που χρησιμοποιεί το δημόσιο κλειδί και την υπογραφή ή τα δεδομένα ως είσοδο, ανάλογα με τον αλγόριθμο. Εάν η εφαρμογή αυτής της συνάρτησης δίνει το αναμενόμενο αποτέλεσμα, η υπογραφή θεωρείται έγκυρη.

Οι ψηφιακές υπογραφές υλοποιούν έναν αριθμό υπηρεσιών ασφάλειας. Προσδίδουν έλεγχο αυθεντικότητας ή *αυθεντικοποίηση* σε ένα μήνυμα, εξασφαλίζοντας ότι αυτό έχει προέλθει απο έναν συγκεκριμένο χρήστη, ο οποίος είναι ο μοναδικός κάτοχος του ιδιωτικού κλειδιού. Η ψηφιακή υπογραφή προστατεύει το μήνυμα απο μη εξουσιοδοτημένη μεταποίηση προσδίνοντας έναν έλεγχο ακεραιότητας. Παρόλο που απο μόνη της η υπογραφή δεν είναι αρκετή για να επιτύχει την υπηρεσία *μη-άρνησης συμμετοχής (non-repudiation)*, μια ψηφιακή υπογραφή κατασκευασμένη σε συνδυασμό με κατάλληλα δεδομένα μπορεί να παρέχει ένα μέρος της υπηρεσίας μη-άρνησης.

Το αρνητικό χαρακτηριστικό της κρυπτογραφίας δημοσίου κλειδιού είναι το αυξημένο υπολογιστικό κόστος της. Ακόμη και με σύγχρονους υπολογιστές, θεωρείται αργή λόγω των πολύπλοκων υπολογισμών που περιλαμβάνει. Γι' αυτό το λόγο, στην πράξη, αλγόριθμοι κρυπτογραφίας δημοσίου κλειδιού χρησιμοποιούνται μόνο για την κρυπτογράφηση περιορισμένου μεγέθους πληροφορίας, όπως για παράδειγμα ένα κλειδί συμμετρικού αλγορίθμου όπως ο DES ή ο 3DES. Το δεύτερο αυτό κλειδί χρησιμοποιείται με έναν αλγόριθμο συμμετρικής κρυπτογραφίας ο οποίος αναλαμβάνει να κρυπτογραφήσει μεγαλύτερους όγκους δεδομένων με πιο αποδοτικό τρόπο.

Προκειμένου να λειτουργήσει σωστά η κρυπτογραφία δημοσίου κλειδιού, τα ιδιωτικά κλειδιά πρέπει να προστατεύονται. Διάφοροι τρόποι έχουν βρεθεί προκειμένου να υπάρχει αυξημένο επίπεδο προστασίας, ώστε ένας χρήστης να μπορεί να μεταφέρει ασφαλώς το ιδιωτικό κλειδί του. Οι *έξυπνες κάρτες* είναι ένας απ' αυτούς που θεωρούνται αποτελεσματικοί τρόποι. Οι τεχνολογίες για έξυπνες κάρτες και αναγνώστες έξυπνων καρτών για προσωπικούς υπολογιστές είναι ήδη διαθέσιμες και μέσα σε λογικά πλαίσια κόστους.

1.3 ΒΑΣΙΚΟΙ ΜΗΧΑΝΙΣΜΟΙ ΚΑΙ ΔΙΑΔΙΚΑΣΙΕΣ ΑΣΦΑΛΕΙΑΣ

Η παράγραφος αυτή έχει ως στόχο την συνοπτική περιγραφή των βασικών μηχανισμών και διαδικασιών εκείνων που λαμβάνουν χώρα κατά την διεκπεραίωση κρυπτογραφικών λειτουργιών. Συνήθως η χρήση των μηχανισμών αυτών αποτελεί στοιχειώδες βήμα μιας συνολικότερης κρυπτογραφικής λειτουργίας. Οι μηχανισμοί που περιγράφονται εδώ είναι βασισμένοι σε ευρέως διαδεδομένα πρότυπα.

Συμφωνία κλειδιών

Με τον όρο συμφωνία κλειδιών εννοούμε την διαδικασία επίλυσης του ακόλουθου προβλήματος: δύο οντότητες θέλουν να συμφωνήσουν στην πληροφορία κρυπτογραφικών κλειδιών μυστικά πάνω απο ένα ανοιχτό κατανεμημένο δίκτυο. Προκειμένου να επιτευχθεί η ασφαλής συμφωνία χρησιμοποιούνται πρωτόκολλα συμφωνίας κλειδιών (key agreement protocols) τα οποία είναι θεμιτό να έχουν τα ακόλουθα χαρακτηριστικά:

- Γνωστά κλειδιά συνόδου: ένα πρωτόκολλο επιτυγχάνει το στόχο του παρά το γεγονός ότι κάποιος έχει υποκλέψει κάποια απο τα κλειδιά προηγούμενων συνόδων.
- (Τέλεια) πρόσθια μυστικότητα (perfect forward secrecy): Εάν κάποιο απο τα κρυπτογραφικά μυστικά που χρησιμοποιούνται για μια ή περισσότερες οντότητες υποκλαπούν, η μυστικότητα προηγούμενων κλειδιών συνόδων δεν επηρεάζεται.
- Άγνωστο μοίρασμα κλειδιού: η οντότητα i δεν μπορεί να εξαναγκαστεί να μοιραστεί τον κλειδί της με την οντότητα j χωρίς η i να το γνωρίζει, για παράδειγμα όταν ο i πιστεύει ότι το κλειδί το μοιράζεται με μια οντότητα l που είναι διαφορετική της j.

- Απομίμηση με υποκλοπή κλειδιού: Εάν υποθέσουμε ότι το κρυπτογραφικό μυστικό του i που χρησιμοποιείται στην συμφωνία υποκλέπτεται, τότε ο υποκλοπέας που γνωρίζει την τιμή του μπορεί να υποδυθεί τον i, εφόσον αυτή η τιμή ακριβώς χαρακτηρίζει τον i. Ενδέχεται παρ' όλα αυτά, ότι αυτή η απώλεια δεν επιτρέπει στον υποκλοπέα να υποδυθεί τον ρόλο άλλων οντοτήτων πέραν του i.
- Απώλεια πληροφορίας: Η υποκλοπή άλλης πληροφορίας που δεν θα ήταν υπο κανονικές συνθήκες διαθέσιμη στον υποκλοπέα, δεν επηρεάζει την ασφάλεια του πρωτοκόλλου.
- Ανεξαρτησία μηνυμάτων: Ανεξάρτητες ροές ενός πρωτοκόλλου που τρέχουν ανάμεσα σε δύο έντιμες οντότητες είναι άσχετες μεταξύ τους.

Ένα απο τα πιο γνωστά πρωτόκολλα συμφωνία κλειδιών είναι αυτό των Diffie-Helman το οποίο περιγράφεται στο RFC 2631 (Diffie-Hellman Key Agreement Method).

Συναρτήσεις κατακερματισμού

Μια συνάρτηση *κατακερματισμού (hash function)* Η είναι ένας μετασχηματισμός που λαμβάνει μια είσοδο μεταβλητού μήκους m και επιστρέφει μια συμβολοακολουθία σταθερού μήκους, που ονομάζεται *τιμή της συνάρτησης* h, δηλαδή h = H(m). Οι συναρτήσεις κατακερματισμού με αυτή την ιδιότητα βρίσκουν εφαρμογή σε μια πληθώρα περιπτώσεων, αλλά όταν χρησιμοποιούνται στην κρυπτογραφία συνήθως επιλέγονται ώστε να διαθέτουν και επιπλέον ιδιότητες.
Οι βασικές απαιτήσεις απο μια κρυπτογραφική συνάρτηση κατακερματισμού είναι οι ακόλουθες:

- Η είσοδος να είναι οσοδήποτε μήκους.
- Η έξοδος να έχει σταθερό μέγεθος.
- Η H(x) να είναι εύκολο να υπολογιστεί για οποιοδήποτε δεδομένο x.
- Η H(x) είναι *μονόδρομη (one-way)*.
- Η H(x) είναι *ανθεκτική σε συγκρούσεις (collision-free)*.

Μια συνάρτηση κατακερματισμού Η είναι μονόδρομη όταν είναι δύσκολο να αντιστραφεί, όπου ο όρος «δύσκολο» σημαίνει ότι για μια δεδομένη τιμή της συνάρτηση h, είναι υπολογιστικά αδύνατο να βρεθεί κάποια είσοδος x έτσι ώστε H(x)=h.
Εάν για ένα δεδομένο μήνυμα x, είναι υπολογιστικά αδύνατο να βρεθεί ένα μήνυμα y το οποίο είναι διαφορετικό απο το x έτσι ώστε H(x) = H(y), τότε η Η χαρακτηρίζεται ως μια συνάρτηση κατακερματισμού ασθενώς ανθεκτική στις συγκρούσεις (weakly collision-free).
Μια ισχυρά ανθεκτική στις συγκρούσεις (strongly collision-free) συνάρτηση κατακερματισμού Η χαρακτηρίζεται αυτή για την οποία είναι υπολογιστικά αδύνατο να βρεθούν οποιαδήποτε δύο μηνύματα x και y για τα οποία H(x)=H(y).
Η τιμή της συνάρτησης κατακερματισμού (η οποία αναφέρεται στην βιβλιογραφία και ως hash ή message digest) αναπαριστά με συνέπεια το μήνυμα ή έγγραφο απο το οποίο υπολογίστηκε. Κάποιος θα μπορούσε να θεωρήσει την τιμή αυτή ως ένα «ψηφιακό δακτυλικό αποτύπωμα» του εγγράφου. Παραδείγματα των πλέον διαδεδομένων συναρτήσεων κατακερματισμού είναι οι MD2, MD5 και SHA1.
Ο κύριος ρόλος των κρυπτογραφικών συναρτήσεων κατακερματισμού είναι στην παροχή ψηφιακών υπογραφών όπως περιγράφηκαν στην παράγραφο 1.2. Επιπλέον η τιμή μιας συνάρτησης μπορεί να δημοσιευθεί χωρίς να αποκαλύπτονται τα περιεχόμενα του εγγράφου απο το οποίο προκύπτει. Αυτό βρίσκει εφαρμογή στην *ψηφιακή χρονοσφράγιση (digital timestamping)*, όπου χρησιμοποιώντας συναρτήσεις κατακερματισμού, κάποιος μπορεί να λάβει ένα χρονοσφραγισμένο έγγραφο χωρίς να αποκαλύπτει τα περιεχόμενα του εγγράφου στην υπηρεσία χρονοσφράγισης.

Αλγόριθμοι Κρυπτογράφησης βασισμένοι Σε Τμήματα

Οι *αλγόριθμοι κρυπτογράφησης βασισμένοι σε τμήματα (block ciphers)* είναι ένας τύπος αλγόριθμου συμμετρικής κρυπτογράφησης που μετατρέπει ένα block μη κρυπτογραφημένου

καθορισμένου μήκους κειμένου (plaintext), σε block κρυπτογραφημένου του ίδιου μήκους κειμένου (ciphertext). Αυτός ο μετασχηματισμός πραγματοποιείται με την βοήθεια ενός μυστικού κλειδιού που χορηγείται από τον χρήστη. Η αποκρυπτογράφηση γίνεται με την εφαρμογή του αντίστροφου μετασχηματισμού στο κρυπτογραφημένο κείμενο χρησιμοποιώντας το ίδιο μυστικό κλειδί. Το καθορισμένο μήκος καλείται *μέγεθος τμήματος (block size)*.
Οι block ciphers λειτουργούν επαναληπτικά, κρυπτογραφώντας ένα block διαδοχικά αρκετές φορές. Σε κάθε γύρο, ο ίδιος μετασχηματισμός εφαρμόζεται στα δεδομένα χρησιμοποιώντας ένα υπο-κλειδί. Το σύνολο των υπο-κλειδιών προέρχεται από το μυστικό κλειδί που χορήγησε ο χρήστης, με ειδική συνάρτηση. Το σύνολο των υπο-κλειδιών καλείται πρόγραμμα κλειδιών.
Ο αριθμός των επαναλήψεων του επαναληπτικού cipher εξαρτάται από το επίπεδο της επιθυμητής ασφάλειας και την απόδοση του συστήματος. Στις περισσότερες περιπτώσεις, ο αυξημένος αριθμός επαναλήψεων βελτιώνει την προσφερόμενη ασφάλεια, αλλά για μερικούς ciphers ο αριθμός των επαναλήψεων για να επιτευχθεί ικανοποιητική ασφάλεια θα είναι πολύ μεγάλος για να πραγματοποιηθεί.
Οι Feistel ciphers είναι ειδικές περιπτώσεις επαναληπτικών ciphers όπου το κρυπτογραφημένο κείμενο υπολογίζεται ως εξής: το κείμενο χωρίζεται στο μισό. Η συνάρτηση f εφαρμόζεται στο ένα μισό με χρήση ενός υπο-κλειδιού και η έξοδος της f περνάει από λογική πράξη X-OR με το άλλο μισό. Έπειτα, το αποτέλεσμα της λογικής πράξης γίνεται είσοδος της f και το προηγούμενο μισό το οποίο μετασχηματίστηκε γίνεται μία από τις εισόδους της επόμενης X-OR. Η άλλη είσοδος της X-OR είναι το αποτέλεσμα του δεύτερου μετασχηματισμού, ο οποίος χρησιμοποιεί νέο υπο-κλειδί. Ο αλγόριθμος συνεχίζεται με το ίδιο τρόπο. Στο τέλος της τελευταίας επανάληψης, τα δύο κρυπτογραφημένα μισά συνενώνονται.
Ένα σημαντικό χαρακτηριστικό του Feistel είναι ότι η αποκρυπτογράφηση είναι δομικά ταυτόσημε με την κρυπτογράφηση. Τα υπο-κλειδιά χρησιμοποιούνται σε αντίστροφη σειρά στην αποκρυπτογράφηση. Οι Feistel ciphers καλούνται και DES-like ciphers.

Αλγόριθμοι κρυπτογράφησης βασισμένοι σε Ροές

Ένας *αλγόριθμος κρυπτογράφησης βασισμένος σε ροές (Stream cipher)* είναι ένας τύπος αλγόριθμου συμμετρικής κρυπτογράφησης. Είναι εξαιρετικά ταχύς αλγόριθμοι, κατά πολύ ταχύτεροι από τους block ciphers. Σε αντίθεση με τους block ciphers που λειτουργούν με μεγάλα κομμάτια δεδομένων (blocks), οι stream ciphers τυπικά λειτουργούν με μικρότερες μονάδες απλού κειμένου, συνήθως με bits. Η κρυπτογράφηση ενός συγκεκριμένου κειμένου με έναν block cipher θα καταλήγει πάντα στο ίδιο αποτέλεσμα όταν χρησιμοποιείται το ίδιο κλειδί. Με έναν stream cipher, ο μετασχηματισμός των μικρότερων αυτών μονάδων θα ποικίλει, ανάλογα με πότε αντιμετωπίζονται κατά την διάρκεια της κρυπτογράφησης.
Ένας stream cipher παράγει μια ακολουθία από bits που χρησιμοποιείται σαν κλειδί και καλείται *ροή-κλειδί (keystream)*. Η κρυπτογράφηση επιτυγχάνεται με τον συνδυασμό του keystream με το plaintext, συνήθως μέσω X-OR πράξης. Η παραγωγή του keystream μπορεί να είναι ανεξάρτητη του plaintext και του ciphertext (*οπότε μιλάμε για σύγχρονο αλγόριθμο – synchronous stream cipher*) ή μπορεί να εξαρτάται από αυτά (οπότε μιλάμε για *αυτοσυγχρονιζόμενο αλγόριθμο - self-synchronizing stream cipher*). Οι περισσότεροι stream ciphers είναι σύγχρονοι.
Οι stream ciphers βασίζονται στις θεωρητικές ιδιότητες ενός one-time pad. One-time pads (καμιά φορά καλούνται και Vernam ciphers) είναι ciphers που χρησιμοποιούν μια ακολουθία bits (keystream) που παράγεται τελείως στην τύχη. Το keystream είναι του ίδιου μήκους με το μη κρυπτογραφημένο κείμενο και συνδυάζεται μέσω μιας X-OR πράξης με το αυτό για την παραγωγή του ciphertext. Επειδή το keystream είναι τελείως τυχαίο και είναι του ίδιου μήκους με το plaintext, η εύρεση του κειμένου είναι αδύνατη ακόμα και με την διάθεση τεράστιας υπολογιστικής ισχύς. Ένας τέτοιος cipher προσφέρει τέλεια μυστικότητα και ασφάλεια και έχει χρησιμοποιηθεί σε μεγάλη κλίμακα σε καιρό πολέμου για την διασφάλιση διπλωματικών καναλιών. Το γεγονός, όμως, ότι το μυστικό κλειδί (δηλαδή το keystream),

που χρησιμοποιείται μόνο μία φορά, είναι του ίδιου μήκους με του μήνυμα, εισάγει σημαντικό πρόβλημα στην διαχείριση του κλειδιού. Παρ' όλη την ασφάλεια που προσφέρει, ο one-time pad δεν μπορεί να εφαρμοστεί στην πράξη.
Οι stream ciphers αναπτύχθηκαν σαν μια προσέγγιση της λειτουργίας ενός one-time pad. Βέβαια δεν είναι σε θέση παρέχουν την θεωρητική ασφάλεια ενός time-pad είναι τουλάχιστον πρακτικοί. Ο πιο ευρέως χρησιμοποιούμενος stream cipher είναι ο RC4. Ενδιαφέρον παρουσιάζει το γεγονός ότι συγκεκριμένοι τρόποι λειτουργίας ενός block cipher προσομοιάζουν ένα stream cipher όπως για παράδειγμα ο DES σε CFB και OFB modes. Ακόμα και έτσι, οι αυθεντικοί stream ciphers είναι αρκετά ταχύτεροι.
Ένας μηχανισμός για την παραγωγή του keystream είναι ο *Καταχωρητής Γραμμικής Ολίσθησης με Ανάδραση (Linear Feedback Shift Register – LFSR)*. Ο καταχωρητής αποτελείται από μία σειρά κελιών (cells) το καθένα από τα οποία αποτελείται από ένα bit. Τα περιεχόμενα των κελιών καθορίζονται από ένα *Διάνυσμα Αρχικοποίησης (Initialization Vector)* που λειτουργεί σαν το μυστικό κλειδί. Το keystream δεν αποτελεί πλέον το μυστικό κλειδί (όπως στους one-time pads) λόγω του μεγέθους του. Η συμπεριφορά του καταχωρητή ρυθμίζεται από ένα ρολόι και σε κάθε χρονική στιγμή τα bits μετακινούνται μία θέση δεξιά, την στιγμή που το X-OR αποτέλεσμα μερικών από αυτών τοποθετείται στο αριστερότερο κελί. Κάθε αλλαγή του ρολογιού δίνει ένα bit εξόδου.
Η κατασκευή των LFSR είναι εύκολη τόσο υπό μορφή software όσο και υπό μορφή hardware, ενώ η λειτουργίας τους είναι ταχύτατη. Η ακολουθίες bit, όμως, που δημιουργούνται από ένα και μοναδικό LFSR δεν είναι ασφαλής καθ' ότι τον τελευταίο καιρό έχει αναπτυχθεί ένας δυνατή μαθηματική φόρμουλα που επιτρέπει την ανάλυση του μηχανισμού και εύρεση του keystream. Απαιτείται, λοιπόν, η συνδυασμένη χρήση πολλών LFSRs.
Ένας συνδυασμός LFSRs είναι ο Shift Register Cascade. Αποτελείται από εάν σύνολο από LFSRs που συνδέονται μεταξύ τους με τέτοιο τρόπο ώστε η συμπεριφορά του ενός να εξαρτάται από την συμπεριφορά του άλλου. Αυτό επιτυγχάνεται συνήθως με την χρήση του ενός LFSR να ελέγχει το ρολόι του άλλου. Άλλο παράδειγμα τέτοιου συνδυασμού είναι ο Shrinking Generator που αναπτύχθηκε από τους Coppersmith, Krawczyk και Mansour. Βασίζεται στην αλληλεπίδραση των εξόδων δύο LFSRs. Τα bits της μιας εξόδου χρησιμοποιούνται για να καθορίσουν, μέσω κατάλληλης τεχνικής, εάν τα bits της δεύτερης εξόδου θα συμπεριληφθούν στο keystream. Είναι απλός και έχει καλά χαρακτηριστικά ασφαλείας.

Κώδικες Αυθεντικοποίησης μηνυμάτων

Ένας *Κώδικας Αυθεντικοποίησης Μηνύματος ΚΑΜ (Message Authentication Code – MAC)* είναι μια ετικέτα αυθεντικοποίησης (ή αλλιώς άθροισμα ελέγχου) που παράγεται απο την εφαρμογή σε ένα μήνυμα μιας διαδικασίας αυθεντικοποίησης, μαζί με ένα μυστικό κλειδί. Οι ΚΑΜ υπολογίζονται και επαληθεύονται με το ίδιο κλειδί, οπότε μπορούν να επαληθευτούν μόνο απο τον παραλήπτη που το έχει, σε αντίθεση με τις ψηφιακές υπογραφές που μπορούν να επαληθευτούν απο οποιονδήποτε. Οι ΚΑΜ μπορούν να κατηγοριοποιηθούν ως:

- Ασφαλείς χωρίς συνθήκες
- Βασισμένοι σε συναρτήσεις κατακερματισμού
- Βασισμένοι σε αλγορίθμους ροής (stream ciphers)
- Βασισμένοι σε αλγορίθμους τμημάτων (block ciphers)

Οι Simmons και Stinson πρότειναν έναν ασφαλή χωρίς συνθήκες ΚΑΜ που βασίζεται σε κρυπτογράφηση με χρήση ενός one-time pad. Το ciphertext του μηνύματος αυθεντικοποιεί τον εαυτό του εφόσον κανένας άλλος δεν έχει πρόσβαση στο one-time pad. Παρ’ όλα αυτά, θα πρέπει να υπάρχει πλεονασμός πληροφορίας στο μήνυμα. Ένας ασφαλής ΚΑΜ χωρίς συνθήκες μπορεί να ληφθεί επίσης με την χρήση ενός μυστικού κλειδιού μιας χρήσης (one-time secret key).

Οι ΚΑΜ βασισμένοι σε συναρτήσεις κατακερματισμού χρησιμοποιούν ένα ή περισσότερα κλειδιά σε συνδυασμό με μια συνάρτηση κατακερματισμού για να παράγουν ένα άθροισμα ελέγχου που προστίθεται στο μήνυμα. Ένα παράδειγμα είναι ο αλγόριθμος keyed-MD5.

2 ΛΥΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

2.1 ΥΠΟΔΟΜΗ ΔΗΜΟΣΙΩΝ ΚΛΕΙΔΙΩΝ (ΥΔΚ)

Η ασφάλεια της πληροφορίας μπορεί να επιτευχθεί βάσει κρυπτοσυστημάτων δημόσιου κλειδιού με ανάλογους αλγόριθμους και κλειδιά. Για την απρόσκοπτη λειτουργία των συστημάτων αυτών απαιτείται για κάθε ζεύγος ιδιωτικού – δημόσιου κλειδιού:

- Ασφαλής δημιουργία και διαφύλαξη του ιδιωτικού κλειδιού, έτσι ώστε να μην έχει πρόσβαση σε αυτό κανείς άλλος εκτός του κατόχου του. Κάτι τέτοιο μπορεί να επιτευχθεί με την αποθήκευση του ιδιωτικού κλειδιού σε ασφαλή «ιδιωτικά» μέσα (π.χ. έξυπνες κάρτες).

- Πιστοποίηση του τρόπου δημιουργίας και εγκυρότητας του δημόσιου κλειδιού, έτσι ώστε να εξασφαλίζεται πως το τελευταίο ταυτίζεται πραγματικά με το κάτοχο του (προς αποφυγή πλαστοπροσωπίας).

Για τη κάλυψη των παραπάνω, αλλά και άλλων σχετικών απαιτήσεων, πρέπει να υπάρχει το κατάλληλο *πλαίσιο «εμπιστοσύνης»* μέσα στο οποίο θα κινούνται όλες οι εμπλεκόμενες οντότητες του συστήματος κατά την εκτέλεση κρυπτογραφικών λειτουργιών όπως η ψηφιακή υπογραφή.

Η εμπιστοσύνη αυτή αποτελεί τη βάση λειτουργίας του όλου κρυπτοσυστήματος και έγκειται στην αποδοχή των υποκείμενων μηχανισμών παραγωγής και χρήσης των κλειδιών, όπως π.χ. των μηχανισμών αναγνώρισης των εμπλεκόμενων οντοτήτων, διαφύλαξης των ιδιωτικών κλειδιών, πιστοποίησης της εγκυρότητας των δημόσιων κλειδιών, διάθεσης των δημόσιων κλειδιών, κλπ.
Ένα τέτοιο πλαίσιο μπορεί να παρέχεται μέσω των *Υποδομών Δημόσιου Κλειδιού* που στηρίζουν τη λειτουργία τους σε μία ή περισσότερες *Έμπιστες Τρίτες Οντότητες*.

2.2 ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΚΑΙ ΟΡΙΣΜΟΙ

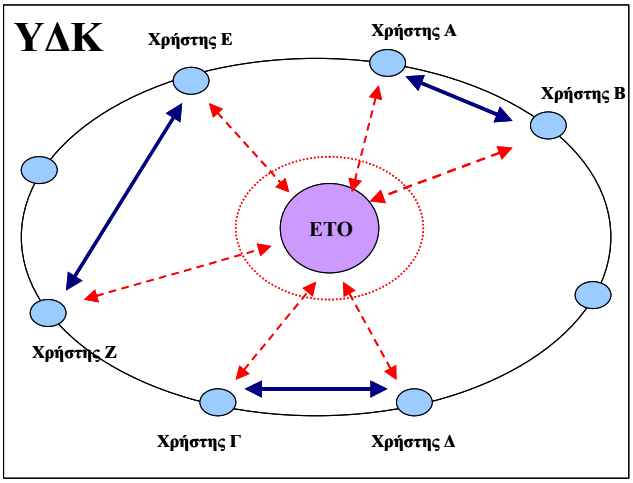
Ως Υποδομή Δημόσιου Κλειδιού (ΥΔΚ) ορίζεται: «ένα σύστημα ψηφιακών πιστοποιητικών, Αρχών Πιστοποίησης και άλλων αρχών εγγραφής που επιβεβαιώνουν και αυθεντικοποιούν την ισχύ του κάθε εμπλεκόμενου μέρους σε μία δικτυακή συναλλαγή» .

Σύμφωνα με το παραπάνω ορισμό, μία ΥΔΚ αποτελεί το υπόβαθρο ανάπτυξης κρυπτοσυστημάτων δημόσιου κλειδιού, με απώτερο σκοπό τη παροχή λειτουργιών ασφαλείας, όπως η κρυπτογράφηση και η ψηφιακή υπογραφή. Αντίστροφα, κάθε ομάδα χρηστών αναπόφευκτα χρειάζεται την ανάπτυξη της κατάλληλης ΥΔΚ ως πλαίσιο για τις απαιτούμενες υπηρεσίες ασφαλείας (π.χ. ως πλαίσιο πιστοποίησης δημόσιων κλειδιών).

Για τη λειτουργία του συστήματος μιας ΥΔΚ είναι απαραίτητη η εμπλοκή μίας τουλάχιστον κοινά αποδεκτής οντότητας που θα αποτελεί το *κεντρικό σημείο εμπιστοσύνης* σε όλη την ΥΔΚ. Η οντότητα αυτή, που καλείται **Έμπιστη Τρίτη Οντότητα** (ΕΤΟ), είναι ουσιαστικά ο φορέας που εμπιστεύονται όλοι οι χρήστες κατά την είσοδο τους στην ΥΔΚ. Πιο συγκεκριμένα:

Ως Έμπιστη Τρίτη Οντότητα (ΕΤΟ) ορίζεται «μια αρχή ασφαλείας ή ο αντιπρόσωπος της η οποία θεωρείται έμπιστη από τους χρήστες με σκοπό τη παροχή δράσεων σχετικών με ασφάλεια, όπως π.χ. την υποστήριξη της χρήσης ψηφιακών υπογραφών και την εμπιστευτικότητα των υπηρεσιών».

Το επόμενο Σχήμα απεικονίζει γραφικά το ρόλο μιας ΕΤΟ μέσα σε μία Υποδομή Δημόσιου Κλειδιού.



Υποδομή Δημόσιου Κλειδιού και ΕΤΟ

Όπως φαίνεται στο παραπάνω Σχήμα, η ΕΤΟ είναι το κεντρικό στοιχείο της ΥΔΚ, καθώς η ανάπτυξη σχέσεων εμπιστοσύνης μεταξύ των χρηστών της ΥΔΚ (π.χ. χρήστες Α-Β, Γ-Δ, Ε-Ζ) στηρίζεται στην εμπιστοσύνη των τελευταίων ως προς την ΕΤΟ. Έτσι, η επιλογή της ΕΤΟ ως κεντρικό σημείο εμπιστοσύνης της ΥΔΚ ουσιαστικά καθορίζει και την όλη λειτουργία της τελευταίας. Αυτή ακριβώς η επιλογή οδηγεί σε σημαντικές οργανωτικές, θεσμικές ή και ακόμα «φιλοσοφικές» τοποθετήσεις σχετικά με το «ποιός μπορεί να θεωρηθεί έμπιστος σε μία ΥΔΚ», «πώς επιλέγεται η έμπιστη οντότητα», κλπ.

Έτσι για παράδειγμα, σε μία Υποδομή Δημόσιου Κλειδιού του τομέα της Ιατρικής Φροντίδας (π.χ. στα πλαίσια ενός περιφερειακού πληροφοριακού συστήματος υγείας), ως Έμπιστη Τρίτη Οντότητα θα μπορούσε να θεωρηθεί ένα κεντρικό Περιφερειακό Νοσοκομείο ή μία δημόσια σχετική αρχή. Σε άλλες περιπτώσεις έμπιστος μπορεί να θεωρείται κάποιος φορέας εντελώς εξωγενής του τομέα Ιατρικής Φροντίδας, π.χ. ένας ανεξάρτητος οργανισμός παροχής υπηρεσιών ΕΤΟ.

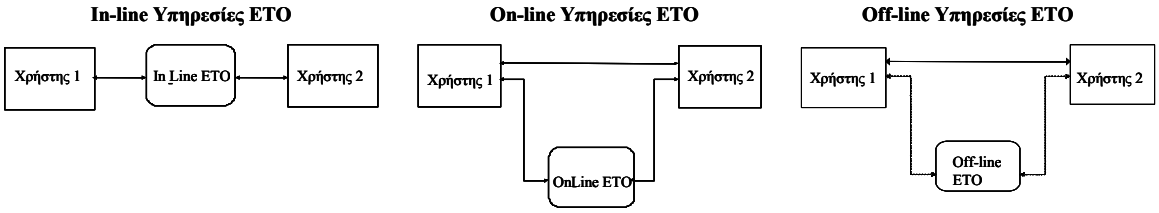
Χρόνος και θέσεις λειτουργίας Έμπιστων Τρίτων Οντοτήτων

Ως «χρόνος λειτουργίας» μίας ΕΤΟ εννοείται η *χρονική στιγμή* κατά την οποία απαιτείται η παρέμβαση - λειτουργία της τελευταίας στις ηλεκτρονικές συναλλαγές των χρηστών.

- *Λειτουργία πριν τις συναλλαγές*: η ΕΤΟ δημιουργεί ή/και αποδίδει ιδιότητες και μέσα στους χρήστες που είναι απαραίτητες προϋποθέσεις για τη πραγματοποίηση των συναλλαγών (όπως π.χ. η έκδοση κλειδιών και πιστοποιητικών).
- *Λειτουργία κατά τη διάρκεια των συναλλαγών*: η ΕΤΟ παρεμβαίνει στις συναλλαγές (μετά από κλήση των χρηστών ή αυτόματα) με σκοπό την πιστοποίηση και εξακρίβωση στοιχείων των τελευταίων.
- *Λειτουργία μετά τη συναλλαγή*: η ΕΤΟ καλείται να επιλύσει τυχόν διαφωνίες και προβλήματα που προέκυψαν λόγω αποτυχίας ολοκλήρωσης μιας συναλλαγής.

Ως «θέση λειτουργίας» μίας ΕΤΟ εννοείται *ο τρόπος* με τον οποίο παρεμβάλλεται η ΕΤΟ κατά τις ηλεκτρονικές συναλλαγές των χρηστών:

- *«In-line» υπηρεσίες ΕΤΟ*: η ΕΤΟ παρεμβάλλεται άμεσα στη διαδρομή επικοινωνίας των συναλλασσόμενων μερών, ή αλλιώς αποτελεί υποχρεωτικό μέρος αυτής της επικοινωνίας.
- *«On-line» υπηρεσίες ΕΤΟ*: η ΕΤΟ παρεμβάλλεται έμμεσα στη διαδρομή επικοινωνίας μετά από σχετική απαίτηση/κλήση ενός των δύο συναλλασσόμενων μερών.
- *«Off-line» υπηρεσίες ΕΤΟ*: η ΕΤΟ δε παρεμβαίνει στις συναλλαγές και απλά παρέχει τα απαραίτητα μέσα για την ομαλή διεκπεραίωση τους.



Διάκριση ΕΤΟ ως προς τη θέση της κατά τις συναλλαγές των χρηστών

2.3 ΥΠΗΡΕΣΙΕΣ ΚΑΙ ΠΡΟΤΥΠΑ ΣΕ ΥΠΟΔΟΜΕΣ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

2.3.1. Γενικές υπηρεσίες ΥΔΚ

Οι βασικές υπηρεσίες ΕΤΟ που παρέχονται από τις περισσότερες Υποδομές Δημόσιου Κλειδιού περιλαμβάνουν την *Εγγραφή*, τη *Πιστοποίηση*, την *Υπηρεσία Κλειδιών* και την *Υπηρεσία Καταλόγου*. Μία υπηρεσία πρόσθετης-αξίας που συχνά απαντάται σε ΥΔΚ είναι η *Υπηρεσία Χρονικής Σφραγίδας*, ενώ ιδιαίτερα σημαντικές θεωρούνται οι υπηρεσίες *Διαπιστοποίησης ΕΤΟ*, καθώς επίσης και οι λειτουργίες ολοκλήρωσης με άλλες τεχνολογίες, όπως η τεχνολογία έξυπνων καρτών. Στη συνέχεια αναλύονται περισσότερο οι παραπάνω υπηρεσίες. Σημειώνεται ότι οι όροι «υπηρεσίες ΕΤΟ» και «υπηρεσίες ΥΔΚ» χρησιμοποιούνται στα επόμενα εναλλακτικά με το ίδιο νόημα.

Εγγραφή
Ο βασικός στόχος της εγγραφής, που λαμβάνει χώρα κατά την είσοδο ενός καινούργιου χρήστη στην Υποδομή Δημόσιου Κλειδιού, είναι η κατάλληλη αναγνώριση και αυθεντικοποίηση του τελευταίου, έτσι ώστε να πραγματοποιηθεί η αξιόπιστη σύνδεση του με το δημόσιο κλειδί του . Η υπηρεσία αυτή εκτελείται από ειδική αρχή της ΥΔΚ που καλείται Αρχή Εγγραφής .

Πιστοποίηση
Ως πιστοποιητικό θεωρείται ένα ηλεκτρονικό μέσο που διασφαλίζει τη σύνδεση μεταξύ μιας οντότητας και του δημόσιου κλειδιού της . Για το λόγο αυτό τα πιστοποιητικά αποτελούν το βασικό στοιχείο εγκυρότητας στις συνδιαλλαγές των χρηστών της ΥΔΚ (π.χ. κατά την επιβεβαίωση των ψηφιακών υπογραφών, κατά την αυθεντικόποιηση, κλπ) και επομένως καθορίζουν το ίδιο το «προφίλ» λειτουργίας της ΥΔΚ.

Κάτω από το παραπάνω πρίσμα, ο βασικός σκοπός της υπηρεσίας πιστοποίησης είναι η έκδοση πιστοποιητικών για το δημόσιο κλειδί των εγγεγραμμένων χρηστών και η διασφάλιση της ακεραιότητας για την κατάσταση των πιστοποιητικών αυτών μέσω αποτελεσματικής διαχείρισης των τελευταίων. Η υπηρεσία αυτή υλοποιεί το *πλαίσιο εμπιστοσύνης* της ΥΔΚ και έτσι βρίσκεται στο κέντρο λειτουργίας της τελευταίας. Η εκτέλεση της υπηρεσίας

πιστοποίσης γίνεται από ειδική αρχή της ΥΔΚ που καλείται *Αρχή Πιστοποίησης (ΑΠ)* και αποτελεί το βασικό σημείο εμπιστοσύνης της όλης υποδομής.

Η πιστοποίηση περιλαμβάνει τις παρακάτω ειδικότερες λειτουργίες:

- Έκδοση/ανανέωση πιστοποιητικών βάσει συγκεκριμένων προτύπων
- Διανομή πιστοποιητικών στους χρήστες
- Αποθήκευση πιστοποιητικών στο Κατάλογο για κοινή χρήση.
- Ανάκληση πιστοποιητικών με έκδοση *Λίστας ανάκλησης πιστοποιητικών (ΛΑΠ)*, η οποία περιέχει όλα τα πιστοποιητικά που δεν ισχύουν ή που έχουν λήξει .

Υπηρεσία Κλειδιών
Η υπηρεσία αυτή δεν είναι υποχρεωτική υπηρεσία σε μια ΥΔΚ και εξαρτάται από την απόφαση της ΕΤΟ να την προσφέρει εφόσον ζητηθεί από τους χρήστες . Οι βασικές λειτουργίες της υπηρεσίας κλειδιών είναι :

- Έκδοση/ προσωποποίηση ζεύγους κλειδιών
- Διανομή/αποθήκευση/ανάκτηση κλειδιών: τα ιδιωτικά κλειδιά πρέπει να διαφυλάσσονται σε ασφαλή μέσα, όπως έξυπνες κάρτες.

Κάποιες επιπλέον υπηρεσίες κλειδιών που ενδέχεται να προσφέρονται από μια ΥΔΚ, αλλά συχνά αμφισβητούνται λόγω κινδύνων διέρευσης μυστικής πληροφορίας , είναι η διαφύλαξη αντιγράφων ιδιωτικών κλειδιών και η ανακατασκευή κλειδιών .

Υπηρεσία Καταλόγου
Η υπηρεσία αυτή μέσω κατάλληλου Εξυπηρετητή Καταλόγου (Directory Server) χρησιμοποιείται, όπως προαναφέρθηκε, για την αποθήκευση και διάθεση των εκδοθέντων από την ΕΤΟ πιστοποιητικών και δημόσιων κλειδιών. Στο Κατάλογο εναποθέτονται και οι Λίστες Ανάκλησης Πιστοποιητικών για έλεγχο της εγκυρότητας και ισχύος πιστοποιητικών. Η οργάνωση του Καταλόγου γίνεται βάσει κατάλληλων προτύπων και πρωτοκόλλων .

Υπηρεσία Χρονοσφραγίδας
Η υπηρεσία αυτή σχετίζεται με την επικόλληση ημερομηνίας και ώρας σε δεδομένα, με σκοπό την απόδειξη ότι τα τελευταία δημιουργήθηκαν ή απεστάλησαν σε μία συγκεκριμένη χρονική στιγμή. Με το τρόπο αυτό ουσιαστικά αποδεικνύεται και η μοναδικότητα των ίδιων των δεδομένων. Η υπηρεσία εκτελείται από ειδική *Αρχή Χρονικής Σφραγίδας* της ΥΔΚ, βάσει κατάλληλων μεθόδων και προτύπων .

Υπηρεσία Διαπιστοποίησης
Η διαπιστοποίηση είναι ένα ιδιαίτερα σημαντικό θέμα για τη δια-λειτουργικότητα των ΕΤΟ και τη διασφάλιση των συναλλαγών μεταξύ χρηστών εγγεγραμμένων σε διαφορετικές ΥΔΚ. Ως «δια-πιστοποιητικό» εννοείται το πιστοποιητικό που εκδίδεται από μία Αρχή Πιστοποίησης Α σε μία άλλη Αρχή Πιστοποίησης Β και εκφράζει την εμπιστοσύνη της Α ως προς τη Β. Έτσι, βάσει του «δια-πιστοποιητικού», ένας χρήστης Χ που εμπιστεύεται την ΑΠ Α, μπορεί να εμπιστευτεί κάθε χρήστη Υ που πιστοποιείται από την ΑΠ Β. Τα δια-πιστοποιητικά μπορεί να είναι μονόδρομα ή αμφίδρομα. Κατά τη δεύτερη περίπτωση η εμπιστοσύνη μεταξύ δύο χρηστών των ΑΠ Α και ΑΠ Β είναι αμοιβαία.

2.3.3. Ειδικές υπηρεσίες ΥΔΚ

Λόγω των ειδικών απαιτήσεων ασφαλείας της πληροφορίας σε διάφορους τομείς (π.χ. Ιατρικής Φροντίδας, Η-Διακυβέρνησης) ορισμένες επιπρόσθετες υπηρεσίες ΥΔΚ μπορεί να είναι οι εξής:

- *Εγγραφή και πιστοποίηση της επαγγελματικής ιδιότητας*: Η υπηρεσία αυτή στηρίζεται στην έκδοση επαγγελματικών πιστοποιητικών από αρμόδιους φορείς (π.χ. το Υπουργείο Υγείας, Πρόνοιας και Κοινωνικών Ασφαλείας στην Ελλάδα) και αφορά την ηλεκτρονική εξουσιοδότηση των επαγγελματιών υγείας βάση του διπλώματος τους και ενδεχομένως βάση της ειδικότητας τους . Το θέμα αυτό έχει ιδιαίτερα οργανωτικά προβλήματα και μέχρι στιγμής έχει βρει εφαρμογή σε λίγες χώρες, όπως η Γερμανία, όπου και εκδίδονται ειδικές έξυπνες κάρτες επαγγελματιών Ιατρικής Φροντίδας .

- *Καθορισμός ρόλων και ειδικοτήτων εμπλεκόμενων οντοτήτων*: Η υπηρεσία αυτή μπορεί να παρέχεται από μια κατάλληλη *Αρχή Ιδιοτήτων*, η οποία καθορίζει τους ρόλους των διαφόρων οντοτήτων στα πλαίσια της ΥΔΚ μέσω ειδικών πιστοποιητικών που καλούνται *πιστοποιητικά ιδιοτήτων*. Καθώς η έκδοση πολλαπλών πιστοποιητικών ιδιοτήτων μπορεί να οδηγήσει σε πολύπλοκα σχήματα εξουσιοδοτήσεων στις υπηρεσίες ενός πληροφοριακού συστήματος είναι δυνατός ο καθορισμός ρόλων και ειδικοτήτων να γίνεται στο ίδιο το πιστοποιητικό δημόσιου κλειδιού των χρηστών μέσο κατάλληλων πεδίων επέκτασης .

Όπως φαίνεται, και οι δύο παραπάνω ειδικές υπηρεσίες σχετίζονται με διαβαθμίσεις πρόσβασης και εξουσιοδοτήσεων σε συγκεκριμένα συστήματα πληροφοριών (π.χ. Ιατρικής Φροντίδας, η-επιχειρείν) τα οποία εξαρτώνται σημαντικά από τα προφίλ των χρηστών και τη δομή της ΥΔΚ. Οι υπηρεσίες αυτές θα μπορούσαν να ενσωματωθούν στις λειτουργίες της Αρχής Εγγραφής, ή να υλοποιηθούν ξεχωριστά.

Κάποιες άλλες υπηρεσίες ΥΔΚ βάσει των τελευταίων τεχνολογικών εξελίξεων αφορούν λειτουργία σε επίπεδο κινητού δικτύου, ολοκλήρωση με ιατρικές συσκευές προσωπικών ψηφιακών βοηθών (Personal Digital Assistant – PDA) , ολοκλήρωση με τεχνολογίες κινητών τηλεφώνων , κ.α.

2.3.4. Τεχνικά πρότυπα σε Υποδομές Δημόσιου Κλειδιού

Τα βασικά πρότυπα που σχετίζονται με την ανάπτυξη και λειτουργία Υποδομών Δημόσιου Κλειδιού αναφέρονται συνοπτικά στο παρακάτω Πίνακα 2.1 ανά οργανισμό προτυποποίησης. Οι πρώτες τέσσερις περιπτώσεις προτύπων αφορούν ΥΔΚ και ψηφιακές υπογραφές, ενώ οι τρεις τελευταίες αφορούν αλγορίθμους κρυπτογράφησης.

Οργανισμός προτυποποίησης	**Περιγραφή προτύπων**
1. ITU – SG7	Η Ομάδα Εργασίας 7 (SG7) της Διεθνούς Ένωσης Τηλεπικοινωνιών (International Telecommunication Union, ITU) έχει εκδόσει τη σύσταση για το *πρότυπο X.509 (X.509 Recommendation)*, που αποτελεί το βάση ανάπτυξης Υποδομών Δημόσιου Κλειδιού. Το πρότυπο αυτό καθορίζει το πλαίσιο πιστοποιητικού δημόσιου κλειδιού και πιστοποιητικού ιδιοτήτων, ενώ αποτελεί το βασικό στοιχείο της *σειράς X.500* για λειτουργία του Καταλόγου . Η τελευταία έκδοση του προτύπου έγινε το 2000.
2. IEFT – PKIX	Η ομάδα εργασίας «Public Key Infrastructure X.509» (PKIX) του οργανισμού Internet Engineering Task Force (IETF) ιδρύθηκε το 1995, με σκοπό την ανάπτυξη προτύπων για το διαδίκτυο βάσει του ITU-X.509. Από τα πρότυπα αυτά αξίζει να τονιστεί το «RFC 2459: X.509 Certificate and CRL Profile», το οποίο προδιαγράφει μία ακριβή δομή πιστοποιητικού και Λίστας Ανάκλησης Πιστοποιητικού με υποχρεωτικά

	πεδία και πεδία επέκτασης . Πρόσφατα έχει εκδοθεί και το πρότυπο «RFC 3039: Qualified Certificates Profile» που προδιαγράφει τη μορφή των «qualified» πιστοποιητικών για φυσικά πρόσωπα, βάσει των νόμιμων δικαιωμάτων και του νομικού πλαισίου της Χώρας . Κάποια άλλα σημαντικά πρότυπα του PKIX είναι τα: «RFC 2527: Certificate Policy and Certification Practice Framework» για ανάπτυξη *Πολιτικών Πιστοποιητικού* και «RFC 3161: Time Stamp Protocol» για δημιουργία χρονικής σφραγίδας. Άλλες ομάδες του IETF, εκτός του PKIX, για ανάπτυξη προτύπων ασφαλείας αφορούν τις περιοχές SNMPv3 , TLS , L2TP , IPSEC .
3. ISO/IEC	Ο Διεθνής Οργανισμός Τυποποίησης (ISO) έχει εκδόσει αρκετά πρότυπα για ασφάλεια συστημάτων και Υποδομές Δημόσιου Κλειδιού, για κάποια από τα οποία έχει συνεργαστεί με την Διεθνή Ηλεκτροτεχνική Επιτροπή (IEC). Βασικά πρότυπα είναι τα: • JCS 35.100.01, «ISO/IEC 7498, Parts 1-4» για το βασικό πλασίο ορισμών και υποδομής ασφαλείας ΥΔΚ • TC 215, «(DTS) 17090 "Health Informatics – Public Key Infrastructure» για ΥΔΚ στο τομέα Ιατρικής Φροντίδας Σημαντικές ενέργειες στην ευρύτερη περιοχή της ασφαλείας και ΥΔΚ έχουν επίσης γίνει από την επιτροπή 27 «Security» του ISO , καθώς επίσης και από τις ομάδες εργασίας JTC1/SG6, SG17 .
4. ETSI/SEC	Η Τεχνική Επιτροπή Ασφάλειας SEC του Ευρωπαϊκού Ινστιτούτου Προτυποποίησης Τηλεπικοινωνιών (ETSI - European Telecommunication Standards Institute) ασχολείται με πρότυπα Υποδομής Δημόσιου Κλειδιού, σε συνεργασία με την Ευρωπαϊκή Πρωτοβουλία για Ηλεκτρονικές Υπογραφές (European Electronic Signature Initiative, CEN/ISSS.) Τα πρότυπα του ETSI σχετίζονται με τη χρήση του προτύπου X.509 για «qualified» πιστοποιητικά (TS 101 862 v 1.2.1) , την ανάπτυξη Πολιτικών Πιστοποιητικού (TS 101 042, TS 101 456 v1.2.1) , την μορφή της ψηφιακής υπογραφής (TS 101 733 v 1.3.1) , κ.α
5. RSA Laboratories - PKCS	Τα πρότυπα κρυπτογράφησης δημόσιου κλειδιού (Public-Key Cryptography Standards, PKCS) προέκυψαν ως μια προσπάθεια της RSA για δημιουργία ενός τυποποιημένου βιομηχανικού interface για την κρυπτογράφηση δημόσιου κλειδιού. Περιλαμβάνουν όλη τη σειρά προτύπων PKCS#1 - PKCS#12 .
6. NIST	Ο οργανισμός National Institute of Standards and Technology (NIST) εργάζεται πάνω σε θέματα κρυπτογραφικών αλγορίθμων σε συνεργασία με τον Αμερικανικό Οργανισμό Τυποποίησης ANSI. Από τα πρότυπα αυτά αξίζει να σημειωθούν τα: • FIPS 197: Advanced Encryption Standard (AES) • FIPS – 46-3, FIPS 81: Data Encryption Standard (DES), που

	καθορίζει τους αλγόριθμους DES και TripleDES • FIPS 186-2, 180-1: Digital Signature Standard (DSS), που καθορίζουν τους αλγόριθμους ψηφιακής υπογραφής RSA, DSA .
7. IEEE	Η ομάδα εργασίας του IEEE P1363 διατυπώνει πρότυπα και αλγορίθμους κρυπτογράφησης, ψηφιακής υπογραφής, κλπ .

Τεχνικά πρότυπα σε Υποδομές Δημόσιου Κλειδιού

2.4 Οργανωτικά θέματα ΥΔΚ

2.4.1 Αρχιτεκτονική ΥΔΚ και Πολιτική Πιστοποιητικού

Η αρχιτεκτονική μιας ΥΔΚ περιλαμβάνει όλους τους δομικούς συντελεστές που σχετίζονται με την ανάπτυξη και λειτουργία της τελευταίας. Κάποιοι τέτοιοι συντελεστές είναι οι παρακάτω:

- Τύποι εμπλεκόμενων οντοτήτων και ανάγκες πιστοποίησης.
- Προφίλ πιστοποιητικών και ειδικές απαιτήσεις
- Οντότητες που λειτουργούν ως Αρχές Πιστοποίησης και Εγγραφής.
- Μέθοδος διάθεσης/δημοσίευσης πιστοποιητικών και δημόσιων κλειδιών

Για τον ακριβή προσδιορισμό των παραπάνω και άλλων σχετικών συντελεστών της ΥΔΚ, είναι απαραίτητη η συγγραφή και διατήρηση της *Πολιτικής Πιστοποιητικού*.

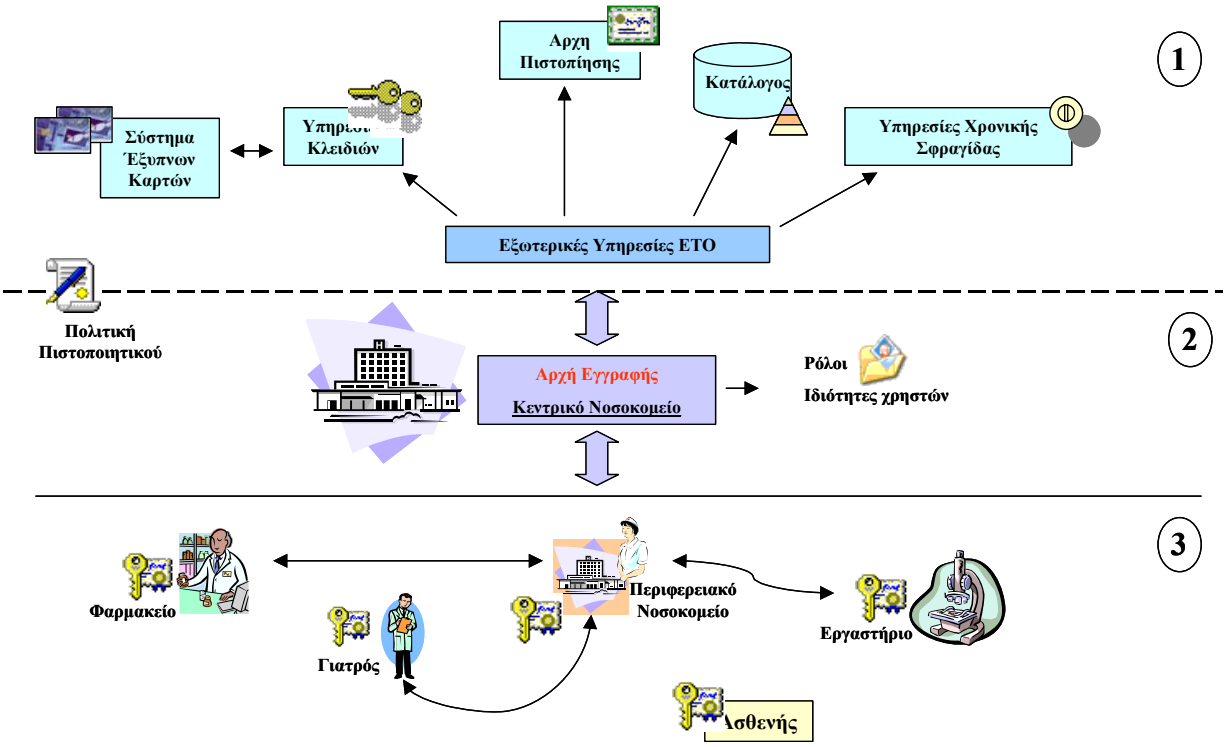
Ο επίσης ορισμός της Πολιτικής Πιστοποιητικού είναι: «ένα σύνολο κανόνων που καθορίζουν την δυνατότητα εφαρμογής ενός πιστοποιητικού σε μια συγκεκριμένη κοινότητα ή/και ομάδα χρηστών με κοινές απαιτήσεις ασφαλείας.» Το κείμενο αυτό, με άλλα λόγια, καθορίζει ουσιαστικά το *προφίλ των πιστοποιητικών* της ΥΔΚ, συμπεριλαμβάνοντας θέματα αναγνώρισης και εγγραφής χρηστών, έκδοσης, διανομής, διάθεσης και ανάκλησης και αποτελεί τη βάση λειτουργίας της ΥΔΚ.

Βάσει της Πολιτικής Πιστοποιητικού, η Αρχή Πιστοποίησης υποχρεούται να συντάσσει μια πιο εξιδικευμένη δήλωση των μεθόδων που ακολουθεί κατά τη παροχή των υπηρεσιών της, η οποία καλείται *Κανονισμός Πιστοποίησης* .

2.4.2 Μία αρχιτεκτονική ΥΔΚ για το τομέα της Ιατρικής Φροντίδας

Μία πιθανή αρχιτεκτονική ΥΔΚ, στα πλαίσια ενός πληροφοριακού δικτύου Ιατρικής Φροντίδας (π.χ. σε ένα Περιφερειακό Σύστημα Υγείας) μπορεί να είναι η

παρακάτω:



Μία αρχιτεκτονική ΥΔΚ στο τομέα της Ιατρικής Φροντίδας

Στο δίκτυο του παραπάνω Σχήματος συμμετέχουν ένα Κεντρικό Νοσοκομείο, Περιφερειακά Νοσοκομεία ή Κέντρα Υγείας, Ιατρικά Εργαστήρια, Φαρμακεία και Ασθενείς. Όλες αυτές οι *εμπλεκόμενες οντότητες* επικοινωνούν μεταξύ τους και ανταλλάσσουν πληροφορία σε διάφορα σενάρια ροής, χρησιμοποιώντας κλειδιά και πιστοποιητικά από την ΥΔΚ.

Η αρχιτεκτονική δομή της ΥΔΚ είναι κατανεμημένη και αποτελείται από τρία επίπεδα:

- Το πρώτο επίπεδο περιλαμβάνει την Αρχή Πιστοποίησης και όλες τις υπηρεσίες ΥΔΚ εκτός της Εγγραφής, οι οποίες παρέχονται από μία ή περισσότερες εξωτερικές διαπιστευμένες ΕΤΟ.

- Το δεύτερο επίπεδο περιλαμβάνει το Κεντρικό Νοσοκομείο, το οποίο λειτουργεί ταυτόχρονα και ως Αρχή Εγγραφής των χρηστών στην ΥΔΚ. Το Νοσοκομείο αποτελεί την διαπροσωπεία της ΥΔΚ με τους χρήστες, ενώ παράλληλα είναι υπεύθυνο για τη διαχείριση των εξιδικευμένων υπηρεσιών ΥΔΚ στο τομέα της Ιατρικής Φροντίδας, όπως π.χ. την απόδοση ρόλων και εξουσιοδοτήσεων.

- Το τρίτο επίπεδο αποτελείται από όλους τους υπόλοιπους χρήστες τις ΥΔΚ (Περιφερειακό Νοσοκομείο, Ασθενής, Γιατρός, Φαρμακείο, Εργαστήριο), οι οποίο αφού προμηθευτούν κλειδιά και πιστοποιητικά από την ΥΔΚ μέσω του Κεντρικού Νοσοκομείου, ανταλλάσσουν μεταξύ τους με ασφάλεια την απαιτούμενη πληροφορία.

Σημειώνεται ότι οι Αρχές Εγγραφής θα μπορούσαν να είναι περισσότερες από μία, για παράδειγμα θα μπορούσαν να λειτουργούν ως Αρχές Εγγραφής όλα τα Περιφερειακά Νοσοκομεία μαζί με το Κεντρικό. Επίσης οι εξωτερικές υπηρεσίες ΕΤΟ θα μπορούσαν να είναι μέρος μιας ευρύτερης δομής ΕΤΟ σε δια-συνοριακό ή και σε παγκόσμιο επίπεδο.

Οι απαιτήσεις λειτουργίας της ΥΔΚ καθορίζονται από το προφίλ των εμπλεκομένων οντοτήτων, δηλαδή των νοσοκομείων, γιατρών, ασθενών, κλπ. Οι απαιτήσεις αυτές ορίζουν και τη μορφή των εκδιδόμενων πιστοποιητικών, η οποία περιγράφεται αναλυτικά στη Πολιτική Πιστοποιητικού της ΥΔΚ. Η Πολιτική Πιστοποιητικού φαίνεται στο Σχήμα μεταξύ του επιπέδου 2 και 1, καθώς συνήθως προδιαγράφεται από το πρώτο και εξυπηρετείται από το δεύτερο.

Το παραπάνω κατανεμημένο μοντέλο αρχιτεκτονικής για το τομέα της Ιατρικής Φροντίδας είναι συχνά προτεινόμενο καθώς:

- Μειώνει το κόστος και τη πολυπλοκότητα συντήρησης των υπηρεσιών ΕΤΟ από οργανισμούς του τομέα της Ιατρικής Φροντίδας.
- Αυξάνει την εμπιστοσύνη των χρηστών στις προσφερόμενες υπηρεσίες λόγω του υψηλότερου επιπέδου αντικειμενικότητας της εξωτερικής ΕΤΟ.
- Διατηρεί την εγγραφή και το εξιδικευμένο θέμα της απόδοσης ρόλων οντοτήτων σε «οικείους» φορείς του τομέα της Ιατρικής Φροντίδας με τον οποίους οι χρήστες έχουν συνηθίσει να συναλλάσσονται.

Κάποια άλλα εναλλακτικά μοντέλα αρχιτεκτονικής ΥΔΚ στο τομέα της Ιατρικής Φροντίδας εκτός του προαναφερθέντος είναι:

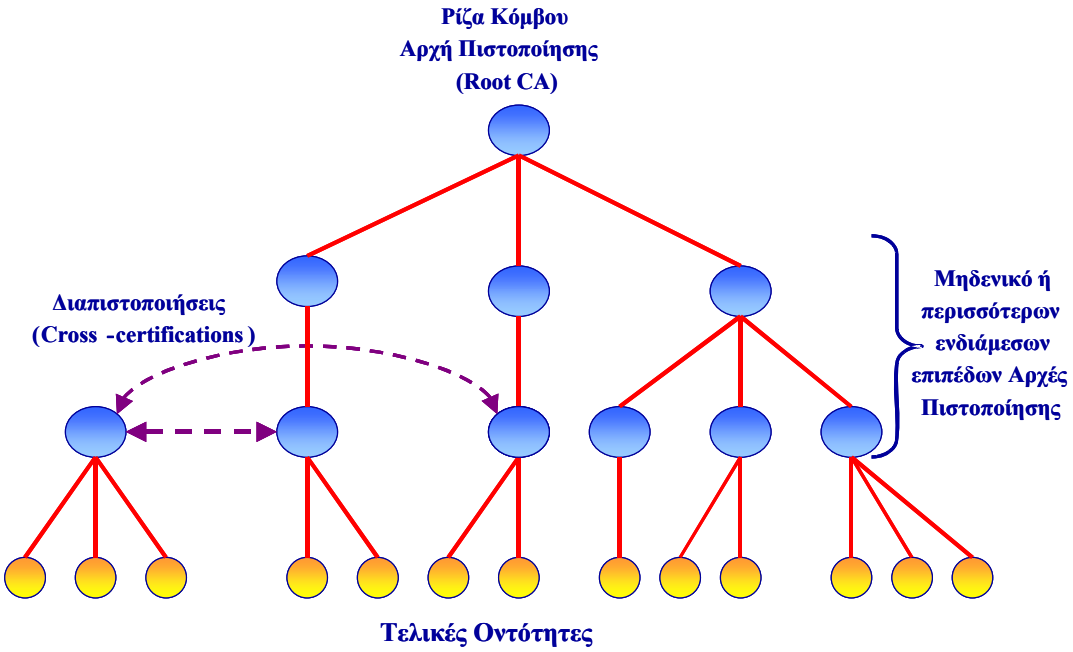
- Διατήρηση όλων των υπηρεσιών ΕΤΟ σε οργανισμούς Ιατρικής Φροντίδας: το μοντέλο αυτό έχει ιδιαίτερες τεχνικές και οικονομικές απαιτήσεις, ενώ παράλληλα ενδέχεται να μειώσει το επίπεδο εμπιστοσύνης των χρηστών .

- Απόδοση όλων των υπηρεσιών σε εξωτερικές ΕΤΟ: το μοντέλο αυτο απλουστεύει τις λειτουργίες, αλλά έχει μικρότερη ευελιξία κατά την εγγραφή των χρηστών και την απόδοση ρόλων και ιδιοτήτων του κάθε τομέα..

2.4.3 Θέματα δια-λειτουργικότητας ΥΔΚ και δια-πιστοποίησης

Σε μία ΥΔΚ υπάρχουν διάφορα μοντέλα εμπιστοσύνης, όπως το *αυστηρά ιεραρχικό μοντέλο (Strict Hierarchy model)* και το *κατανεμημένο μοντέλο εμπιστοσύνης (Distributed Trust Architecture),* το *πλήρες διασυνδεδεμένο μοντέλο (Mesh Model), το διαδικτυακό μοντέλο (Web Model)* και το *μοντέλο χρήστη (User Centric Trust Model).*

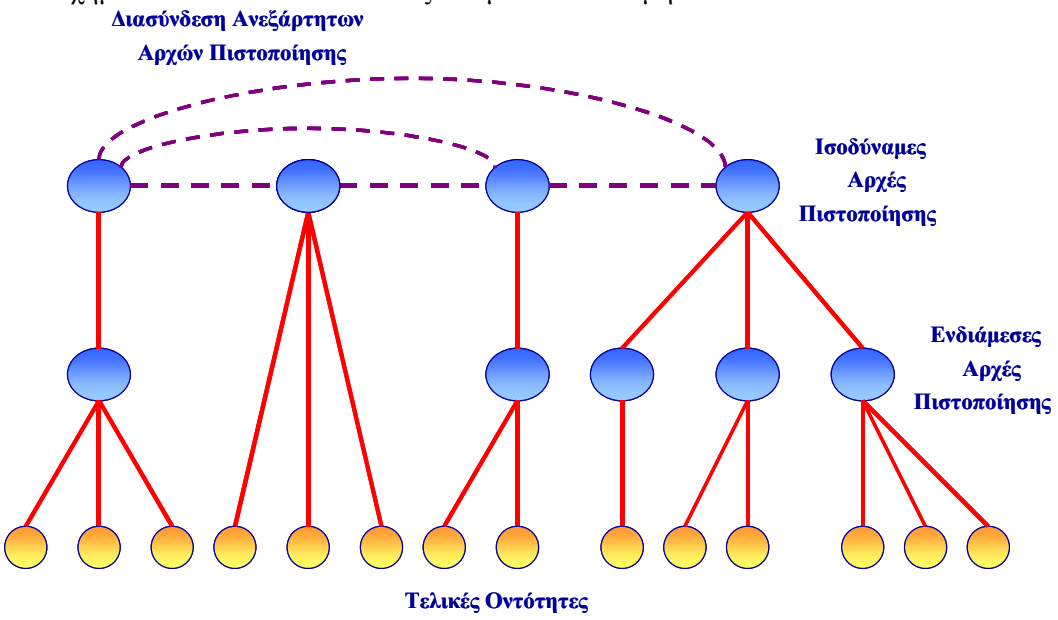
Σύμφωνα με το αυστηρά ιεραρχικό μοντέλο εμπιστοσύνης όπως μπορούμε να διαπιστώσουμε και στο σχήμα που το απεικονίζει παρακάτω, μοιάζει με ένα αντεστραμμένο δένδρο, με την ρίζα του στην κορυφή, τα κλαδιά να ακολουθούν από κάτω της και τα φύλλα του στο κατώτερο σημείο.



Αυστηρά Ιεραρχικό Μοντέλο Εμπιστοσύνης

Στο αντεστραμμένο αυτό δένδρο, την ρίζα αντιπροσωπεύει μία συγκεκριμένη *Αρχή Πιστοποίησης (Certification Authority - CA)*, η οποία φέρει συνήθως την ονομασία ρίζα κόμβου CA και δρα σαν η κύρια ρίζα εμπιστοσύνης στην υπόλοιπη ΥΔΚ των οντοτήτων που βρίσκονται σε κατώτερο επίπεδο από αυτή. Κάτω από την ρίζα κόμβου υπάρχουν ένα ή περισσότερα επίπεδα *υφισταμένων αρχών πιστοποίησης (subordinate CAs)*, τα οποία αντιπροσωπεύονται από τις ενδιάμεσες οντότητες από όπου διαχέονται περισσότερα κλαδιά της δενδρικής δομής που περιγράφεται. Τα φύλλα αντιπροσωπεύουν τις οντότητες εκείνες της ΥΔΚ που δεν έχουν να κάνουν με πιστοποίηση και είναι απλά οι τελικές οντότητες ή οι τελικοί χρήστες.

Όπως αναφέρθηκε και προηγουμένως, μία άλλη μορφή μοντέλου είναι το κατανεμημένο μοντέλο εμπιστοσύνης, όπου σε αντίθεση με την ιεραρχική δομή που περιγράφηκε αμέσως πριν, η εμπιστοσύνη κατανέμεται μεταξύ δύο ή περισσοτέρων αρχών πιστοποίησης (*CAs)*. Στο σχήμα που ακολουθεί απεικονίζεται μία τέτοια δομή:



Κατανεμημένο Μοντέλο Εμπιστοσύνης

Ομοίως στο πλήρες διασυνδεδεμένο μοντέλο όλες ρίζες κόμβου αρχές πιστοποίησης είναι δυναμικά συνδεδεμένες μεταξύ τους διαπιστεύοντας η μία την άλλη. Σε αυτή την περίπτωση, όταν υπάρχουν *n* αρχές πιστοποίησης, χρειάζονται n^2 διαπιστεύσεις μεταξύ των αρχών πιστοποίησης ή μερικές φορές λίγες λιγότερες, ανάλογα με το ποιο είναι το απαραίτητο σημείο να υπάρχουν ασφαλείς διασυνδέσεις.

Στο διαδικτυακό μοντέλο ένας αριθμός από αρχές πιστοποίησης, τις οποίες ο φυλλομετρητής της τελικής οντότητας ή του τελικού χρήστη, αρχικά εμπιστεύεται να δρουν σαν ρίζες κόμβου για επαλήθευση του εκάστοτε πιστοποιητικού. Το σημαντικό σε αυτό το μοντέλο εμπιστοσύνης είναι το γεγονός ότι ο χρήστης μπορεί να αλλάξει, αυξάνοντας ή ελαττώνοντας τον αριθμό αυτό των έμπιστων αρχών πιστοποίησης που αρχικά χρησιμοποιούσε στον φυλλομετρητή του.

Τέλος στο μοντέλο χρήστη, καθένας από αυτούς είναι απευθείας και ολοκληρωτικά υπεύθυνος στο να αποφασίσει ποια πιστοποιητικά μπορεί να εμπιστευτεί και ποια εξ αυτών δεν αποδέχεται ως έμπιστα. Αυτή η απόφαση μπορεί να καθοριστεί από πολλούς ενδιάμεσους παράγοντες, αν και το αρχικό σύνολο των έμπιστων κλειδιών περιλαμβάνει αυτά που ανήκουν και κατέχουν πρόσωπα του πολύ κοντινού με το χρήστη περιβάλλοντος. Η πιο διαδεδομένη υλοποίηση του μοντέλου αυτού είναι η λεγόμενη *PGP*.

Η επιλογή ενός από τα παραπάνω μοντέλα εμπιστοσύνης λαμβάνει υπόψη παράγοντες που αφορούν το κόστος, την απόδοση και την λειτουργικότητα για μία συγκεκριμένη κατάσταση. Σε κάθε περίπτωση όμως είναι πολύ σημαντικοί οι μηχανισμοί *διαπιστοποίησης (cross-certification)*, οι οποίοι είναι υλοποιημένοι μεταξύ των αρχών πιστοποίησης που ανήκουν σε διαφορετικές ΥΔΚ με σκοπό την ασφαλή τους σύνδεση και επικοινωνία. Οι μηχανισμοί αυτοί μπορεί να είναι και λειτουργούν με σχετικά παρόμοιο τρόπο, όπως οι αντίστοιχοι μηχανισμοί πιστοποίησης που περιγράφονται παρακάτω, μόνο που σε αυτή την περίπτωση η διαπιστοποίηση γίνεται μεταξύ αρχών πιστοποίησης. Οι μηχανισμοί αυτοί χρησιμοποιούνται με κύριο σκοπό την επέκταση μιας ΥΔΚ έτσι ώστε η εμπιστοσύνη μεταξύ δύο ή περισσοτέρων κοινοτήτων να είναι δυνατή και υλοποιήσιμη. Στην ουσία με τους μηχανισμούς διαπιστοποίησης μεταξύ δύο αρχών πιστοποίησης, η μία μπορεί να αναγνωρίζει την άλλη και τα πιστοποιητικά που η τελευταία εκδίδει στους χρήστες που βρίσκονται από κάτω της. Η διαλειτουργικότητα μεταξύ των διαφόρων ΥΔΚ μπορεί να λάβει σάρκα και οστά με την σωστή υλοποίηση των παραπάνω μηχανισμών.

2.4 WAP ΕΡΓΑΛΕΙΑ ΥΠΟΔΟΜΗΣ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

Εφόσον οι ΥΔΚ αποκτούν τέτοια σημασία στην ασφάλεια των ηλεκτρονικών επικοινωνιών και συστημάτων και εφόσον οι υπάρχουσες λοιπές τεχνολογίες απέτυχαν να δώσουν λύση στην ανάπτυξη ικανοποιητικών μηχανισμών ασφάλειας στο ασύρματο περιβάλλον, έγινε η προσπάθεια να ενσωματωθούν στα υπάρχοντα πρωτόκολλα και προτυποποιήσεις. Συγκεκριμένα μία τέτοια προσπάθεια παρατηρείται στην τεχνολογία *WAP*, καθώς οι ίδιοι οι προμηθευτές ΥΔΚ παρέχουν λύσεις για την υλοποίηση τέτοιων υποδομών στην ασύρματη επικοινωνία και ειδικά σε υπηρεσίες που υλοποιούνται πάνω σε τέτοια πρότυπα.

Τα θεμελιώδη στοιχεία μιας ΥΔΚ δεν αλλάζουν στα ασύρματα περιβάλλοντα, στα οποία, όπως ειπώθηκε και σε προηγούμενα κεφάλαια, κυριαρχούν διαφορετικά χαρακτηριστικά μετάδοσης δεδομένων. Οι ίδιες αρχές, οι οποίες με επιτυχία έχουν εφαρμοστεί στα σταθερά *TCP/IP* δικτυακά περιβάλλοντα, χρησιμοποιούνται απευθείας στα ασύρματα περιβάλλοντα. Οι τεχνολογίες ωστόσο του *TCP/IP* και της ΥΔΚ όπως αυτή παρουσιάστηκε παραπάνω απαιτούν μεγάλες υπολογιστικές δυνατότητες για να εφαρμοστούν εφόσον διαχειρίζονται μεγάλη επικοινωνιακή πληροφορία, πράγμα που είναι μη επιθυμητό στα ασύρματα περιβάλλοντα. Παρόλα αυτά, τα βασικά στοιχεία μιας ΥΔΚ και των πιστοποιητικών παραμένουν ίδια.

Μία ΥΔΚ θεωρείται ασύρματη *(Α.ΥΔΚ - Wireless Public Key Infrastructure - WPKI)* όταν τουλάχιστον η συσκευή από τη μεριά του χρήστη που εγκαθιστά την επικοινωνία με τα υπόλοιπα στοιχεία του δικτύου είναι ασύρματη. Έτσι για παράδειγμα μπορούμε να έχουμε μία ασύρματη ΥΔΚ όταν ο χρήστης έχει μία ανάλογη συσκευή επικοινωνίας με τον εξυπηρετητή παρά το γεγονός ότι ο τελευταίος συνδέεται με τα υπόλοιπα στοιχεία του δικτύου με ενσύρματα μέσα.

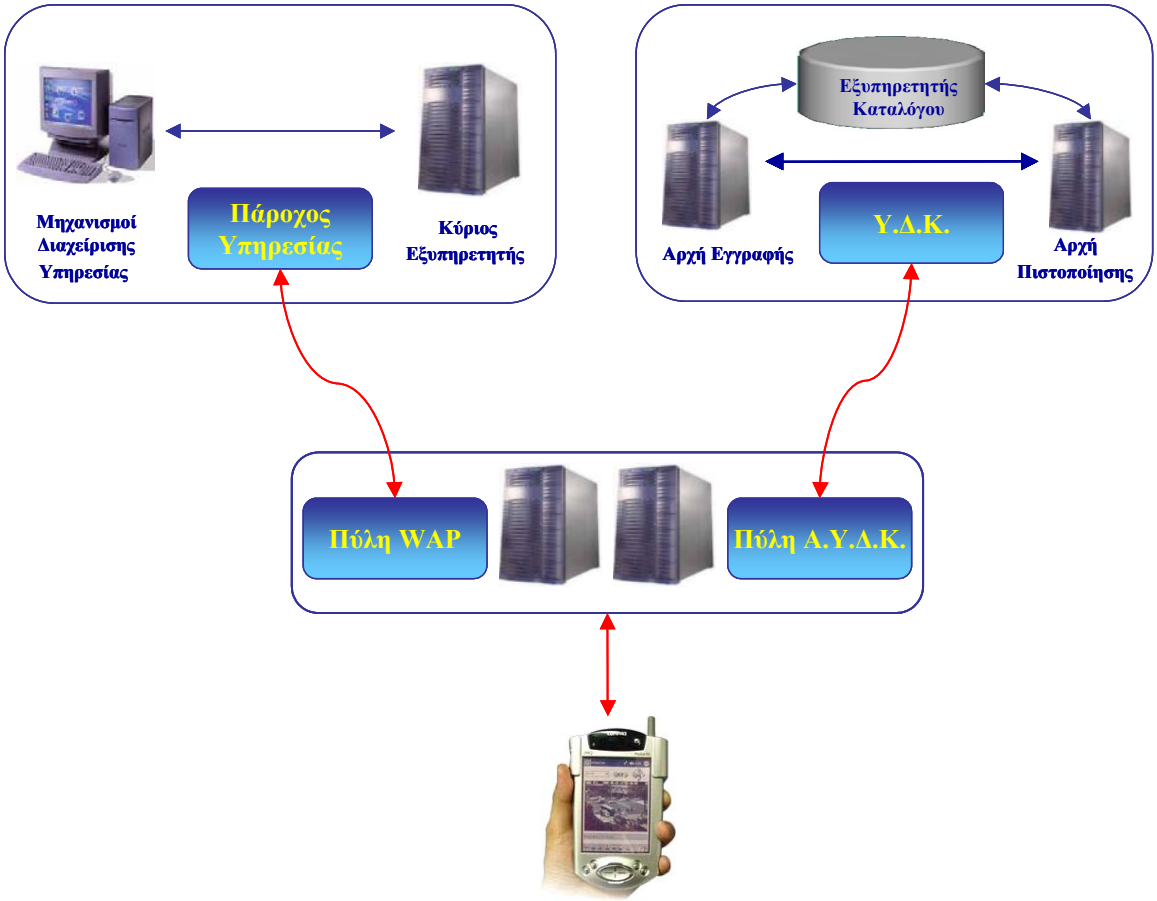
Μία Α.ΥΔΚ μπορεί να χρησιμοποιηθεί στις ίδιες εφαρμογές, σαν αυτές που συναντά κανείς στα ενσύρματα δίκτυα. Παρόλα αυτά, τα χαρακτηριστικά του ασύρματου περιβάλλοντος μπορούν να οδηγήσουν τις υλοποιήσεις, σε εντελώς καινούργιο σύνολο επαναστατικών για την εποχή, εφαρμογών συμπεριλαμβάνοντας διατραπεζικές συναλλαγές, πληρωμές κάθε είδους, ηλεκτρονικές αγορές μηχανισμούς δημόσιας διοίκησης κ.α.. Συγκρινόμενες οι δύο τεχνολογίες ΥΔΚ, σε σχέση με τις εφαρμογές που μπορούν να τρέχουν στα δύο αυτά περιβάλλοντα, είναι αναμενόμενο στο ασύρματο περιβάλλον, να απαιτούνται εφαρμογές ικανές να προσφέρουν την απαιτούμενη λειτουργικότητά τους, σε λιγότερο δυνατές υπολογιστικές μηχανές, με λιγότερη μνήμη, με περιορισμούς στην απόδοση και στην δυνατότητα έκθεσης της πληροφορίας. Εντούτοις, παρά τις παραπάνω δεσμεύσεις, οι ασύρματοι εξοπλισμοί θα πρέπει να είναι ικανοί να δημιουργούν και να εγγράφουν κλειδιά, να διαχειρίζονται τις ταυτότητες των τελικών χρηστών και να θέτουν σε λειτουργία μηχανισμούς κρυπτογράφησης και αποκρυπτογράφησης μηνυμάτων, να μπορούν να παραλαμβάνουν, να επαληθεύουν, να αποθηκεύουν και να στέλνουν πιστοποιητικά και ψηφιακά υπογεγραμμένα δεδομένα.

Στις περισσότερες των περιπτώσεων όμως, οι συσκευές των χρηστών δεν μπορούν να αντεπεξέλθουν σε αυτές τις απαιτήσεις λειτουργίας και μηχανισμών με αποτέλεσμα οι προτεινόμενες λύσεις για εφαρμογή Α.ΥΔΚ να υιοθετούν την λογική των *ενδιάμεσων οντοτήτων των δικτύων (agents)* ώστε οι τελευταίες να αναλαμβάνουν να εκπληρώνουν ορισμένες βασικές λειτουργίες. Με αυτόν τον τρόπο η συσκευή του χρήστη απελευθερώνεται από ένα σύνολο λειτουργιών και αναλαμβάνει μόνο να παρέχει ψηφιακές υπογραφές ώστε να επιτρέπει την εγκαθίδρυση μιας Α.ΥΔΚ. Οι υπόλοιπες βασικές λειτουργίες μιας ΥΔΚ αναλαμβάνονται από τις ενδιάμεσες οντότητες δικτύου, όπως η επαλήθευση, η αρχειοθέτηση και η παράδοση των πιστοποιητικών.

Μία πιθανή υλοποίηση των παραπάνω μπορεί να είναι αυτή, στην οποία τα ιδιωτικά κλειδιά είναι αποθηκευμένα σε έναν πληρεξούσιο εξυπηρετητή ή εναλλακτικά συμπεριλαμβάνονται σε ισχυρές υπομονάδες, όπως η *WIM/SWIM* των διαφόρων συσκευών των χρηστών. Δυστυχώς, η υπομονάδα *WIM/SWIM* δεν έχει φτάσει το απαραίτητο σημείο εξέλιξης, ώστε η περιοχή δημιουργίας των ζευγαριών των κλειδιών από τους τελικούς χρήστες να είναι ικανοποιητική και απόλυτα ασφαλής. Επιπλέον η έλλειψη προτυποποίησης αποτελεί από μόνη της ένα μεγάλο τροχοπέδη στην εξέλιξη των Α.ΥΔΚ καθώς η διαφορετική υλοποίηση των διαφόρων μηχανισμών και λειτουργιών στη κινητή συσκευή έχει σαν αποτέλεσμα τη μη δυνατή διαλειτουργικότητα των εφαρμοζόμενων λύσεων.

Όπως φαίνεται στο σχήμα παρακάτω μία Α.ΥΔΚ απαιτεί τα ίδια στοιχεία με μία παραδοσιακή ΥΔΚ:

- Εφαρμογή Τελικού χρήστη
- Αρχή Εγγραφής
- Αρχή Πιστοποίησης
- Κατάλογος ΥΔΚ



Γενική Αρχιτεκτονική Α.ΥΔΚ

Παρατηρώντας την παραπάνω γενική απεικόνιση μιας Α.ΥΔΚ εύκολα κανείς αντιλαμβάνεται ότι η δομή αυτής της ΥΔΚ είναι υλοποιημένη διαφορετικά σε μερικά της σημεία σε σχέση με την πρώτη που περιγράφηκε προηγουμένως. Γίνεται λοιπόν αντιληπτή μία καινούργια οντότητα η οποία αναφέρεται ως *Πύλη ΥΔΚ (PKI Portal)* η ύπαρξη της οποίας θεωρείται απαραίτητη.

Η εφαρμογή που τρέχει στην κινητή συσκευή του τελικού χρήστη της Α.ΥΔΚ είναι υλοποιημένη με τέτοιο τρόπο ώστε να παρουσιάζεται σαν βελτιστοποιημένο λογισμικό το οποίο τρέχει πάνω στην *WAP* συσκευή. Η υλοποίηση αυτή βασίζεται στην τεχνολογία *WML Script Crypto API (WLSCrypt API),* η οποία χρησιμοποιείται για ανάπτυξη υπηρεσιών κλειδιού και κρυπτογραφικών λειτουργιών γενικότερα. Είναι υπεύθυνη για την ανάπτυξη των ίδιων λειτουργιών και μηχανισμών με τις αντίστοιχες εφαρμογές των τελικών χρηστών στις παραδοσιακές ΥΔΚ. Χαρακτηριστικά θα μπορούσαμε να αναφέρουμε ορισμένες από αυτές:

- Δημιουργία, αποθήκευση και είσοδο πρόσβασης στο ζευγάρι δημοσίου κλειδιού

Ολοκλήρωση, υπογραφή και καταχώρηση εφαρμογών πιστοποιητικών

- Ολοκλήρωση, υπογραφή και καταχώρηση αιτήσεων ανανέωσης πιστοποιητικών
- Ολοκλήρωση, υπογραφή και καταχώρηση αιτήσεων ανάκλησης πιστοποιητικών
- Επαλήθευση πιστοποιητικών και πληροφορία ανάκλησης

Η οντότητα που φέρει την ονομασία '*Πύλη ΥΔΚ*' είναι ένας δικτυακός εξυπηρετητής, όπως η ενδιάμεση '*Πύλη WAP'*, η οποία ενεργεί σαν μία αρχή εγγραφής και είναι υπεύθυνη για την μετάφραση των αιτήσεων προερχόμενες από τον πελάτη *WAP*. Η *Πύλη ΥΔΚ* ουσιαστικά συμπεριλαμβάνει τις λειτουργίες και τους μηχανισμούς της αρχής εγγραφής και διαλειτουργεί με τις συσκευές *WAP* στο ασύρματο δίκτυο και την αρχή πιστοποίησης στο ενσύρματο δίκτυο.

Η παραδοσιακή μέθοδος που χρησιμοποιείται για τον χειρισμό των υπηρεσιών ΥΔΚ βασίζεται στους βασικούς κανόνες κωδικοποίησης *ASN.1 (ASN.1 Basic Encoding Rules - BER)* και *Διακριτούς κανόνες κωδικοποίησης (Distinguished Encoded Rules – DER)*. Οι *BER/DER* προϋποθέτουν την ύπαρξη κατάλληλου υπολογιστικού περιβάλλοντος, που η τεχνολογία *WAP* δεν μπορεί να εξασφαλίσει λόγω των περιορισμών που έχουν ήδη αναφερθεί. Το πρωτόκολλο Α.ΥΔΚ είναι υλοποιημένο χρησιμοποιώντας το *WMLSCrypt*. Συγκεκριμένα η *WML* τεχνολογία με την ιδιότητα και τον μηχανισμό γνωστό ως *signText* παρέχει τις απαραίτητες προϋποθέσεις για την ανάπτυξη ειδικών μηχανισμών αποθήκευσης, κωδικοποίησης και καταχώρησης των αιτήσεων σε μία Α.ΥΔΚ, συγκρινόμενη με την αντίστοιχη λειτουργία σε παραδοσιακές ΥΔΚ.

Επιπλέον η τεχνολογία Α.ΥΔΚ κάνει χρήση διαφορετικής μορφής πιστοποιητικών λόγω των περιορισμών αποθήκευσης στο ασύρματο περιβάλλον. Ένας από τους μηχανισμούς ήταν ο ορισμός της νέας μορφής πιστοποιητικών στην πλευρά του εξυπηρετητή, τα οποία είναι της μορφής *WTLS Certificate Format* και ελαττώνουν σημαντικά το μέγεθος των αντίστοιχων πιστοποιητικών της μορφής *X.509*. Μία ακόμα σημαντική διαφορά στις Α.ΥΔΚ μπορεί να παρατηρηθεί στην *Ελλειψοειδής Κρυπτογράφηση (Elliptic Curve Cryptography - ECC)*. Πιο συγκεκριμένα, με την χρήση της τελευταίας το συνολικό μέγεθος ενός πιστοποιητικού δεν είναι περισσότερο από *100 bytes* λόγω του μικρότερου μεγέθους κλειδιών σε σύγκριση με οποιαδήποτε άλλο σχήμα υπογραφών. Τα κλειδιά των ελλειπτικών καμπύλων είναι περίπου έξι φορές μικρότερα από αυτά των άλλων σχημάτων (*164 bits vs. 1024 bits*). Η τεχνολογία Α.ΥΔΚ ελαχιστοποίησε και σε μεγάλο βαθμό ορισμένα πεδία δεδομένων της μορφοποίησης πιστοποιητικών *IETF PKIX* .

2.7 Νομικό πλαίσιο Υποδομής Δημόσιου Κλειδιού

2.7.1. Νομοθεσία για την ασφάλεια προσωπικών δεδομένων

Η πρώτη ολοκληρωμένη νομική πράξη για την προστασία των προσωπικών δεδομένων στην Ευρώπη τέθηκε με την *Οδηγία 95/46/EC (Data Protection Directive)*, η οποία αποτελεί μια προσπάθεια αναγνώρισης του δικαιώματος για μυστικότητα και στοχεύει στον εναρμονισμό των αντίστοιχων εθνικών νόμων.

Σε συνέχεια της Οδηγίας αυτής το 1997 ψηφίστηκε η *Οδηγία 97/66/EC (Data Protection in the Telecommunications Sector)* , η οποία αφορά τη προστασία δεδομένων που διακινούνται μέσω δικτύων και τηλεπικοινωνιακών συστημάτων.

Ακολουθώντας την Οδηγία 95/46/ΕC, το Συμβούλιο της Ευρώπης εξέδωσε το 1997 την *Σύσταση R(97) 5 (Protection of Medical Data*) για τη προστασία των ιατρικών δεδομένων. Η Σύσταση αυτή αφορά την επεξεργασία ιατρικών και γενετικών δεδομένων και, παρά το ότι η εφαρμογή της δεν είναι υποχρεωτική για τις χώρες μέλη, μπορεί να χρησιμοποιείται σε εθνικά δικαστήρια ως εργαλείο μετάφρασης της Οδηγίας 95/46/ΕC για το τομέα της Ιατρικής Φροντίδας.

Στην Ελλάδα ο κύριος νόμος για τη προστασία προσωπικών δεδομένων είναι η Πράξη 2472/1997 , που υλοποιεί την Οδηγία 95/46/ΕC σε επίπεδο εθνικής νομοθεσίας. Σύμφωνα με αυτή τη νομοθετική πράξη τα ιατρικά δεδομένα θεωρούνται «ευαίσθητα» και η επεξεργασία τους μπορεί να γίνεται μόνο μετά από άδεια της αρμόδιας Αρχής Προστασίας Προσωπικών Δεδομένων. Στο τομέα των τηλεπικοινωνιών επίσης υπάρχει ο νόμος προστασίας δεδομένων 2774/1999 που υλοποιεί την αντίστοιχη Κοινοτική Οδηγία 97/66/ΕC.

Ειδικότεροι κανόνες σχετικά με το ιατρικό απόρρητο στην Ελλάδα περιέχονται στη νομοθετική πράξη για το Εθνικό Σύστημα Υγείας , καθώς επίσης και στον Ιατρικό Κώδικα Δεοντολογίας . Πρέπει πάντως να σημειωθεί ότι οι παραπάνω πράξεις είναι αρκετά παλιές και δεν συμπεριλαμβάνουν τις απαιτούμενες θεσμικές ρυθίσεις για επεξεργασία και

μετάδοση ιατρικών δεδομένων βάσει των εξελίξεων της τεχνολογίας σε πληροφοριακά συστήματα και δίκτυα .

2.6.2. Νομοθεσία για ηλεκτρονικές υπογραφές

Το βασικό νομικό πλαίσιο για τη λειτουργία ΥΔΚ τέθηκε στην Ευρώπη το 1999 με την Οδηγία 1999/93/ΕC για Ηλεκτρονικές Υπογραφές . Η Οδηγία αυτή θεσμοθετεί τη χρήση ηλεκτρονικών υπογραφών ως μέσο εγκυρότητας ηλεκτρονικών δεδομένων. Σκοπός της Οδηγίας είναι η διευκόλυνση της ηλεκτρονικής επικοινωνίας και του ηλεκτρονικού εμπορίου, τα οποία πρέπει να βασίζονται στην νομική αναγνώριση των ηλεκτρονικών υπογραφών ως ισάξιων των συνήθων υπογραφών σε χαρτί.

Παρά το ότι δεν αναφέρεται σε άλλες υπηρεσίες ασφαλείας εκτός της ηλεκτρονικής υπογραφής, η Οδηγία μπορεί να εφαρμοστεί και για την υλοποίηση λειτουργιών αυθεντικοποίησης, εμπιστευτικότητας και χρονικής σφραγίδας. Επίσης, αν και θέτει ζητήματα τεχνολογικής ουδετερότητας, η Οδηγία ουσιαστικά επικεντρώνεται στη χρήση δομών ΥΔΚ για τη παροχή υπηρεσιών ηλεκτρονικής υπογραφής .

Η Οδηγία υποστηρίζει τόσο απλές ηλεκτρονικές υπογραφές βάσει πιστοποιητικών δημόσιου κλειδιού, όσο και «προηγμένες» (advanced) ηλεκτρονικές υπογραφές βάσει «qualified» πιστοποιητικών με ή χωρίς ασφαλή συσκευή υπογραφής.

Στην Ελλάδα η Οδηγία υλοποιήθηκε ως εθνικός νόμος το έτος 2001 με το Προεδρικό Διάταγμα 150/2001 . Το διάταγμα αυτό αποτελεί ουσιαστικά μια «κατά λέξη» μετάφραση της Ευρωπαϊκής Οδηγίας και για το λόγο αυτό απαιτείται ακόμα αρκετή δουλειά ως προς τη διευκρίνηση συγκεκριμένων σημείων και αντιφάσεων που ανακύπτουν. Με άλλα λόγια, το νομικό πλαίσιο υπάρχει, αλλά ακόμα δε θεωρείται ώριμο σε σύγκριση με άλλων Ευρωπαϊκών χωρών, όπως π.χ. της Γερμανίας .

Ενδεικτικά αναφέρεται η περίπτωση του άρθρου 7 (το οποίο αποτελεί ακριβή μετάφραση του άρθρου 8 της Οδηγίας) που δηλώνει ότι οι παροχείς υπηρεσιών πιστοποίησης, οι εποπτεύουσες αρχές καθώς και οι φορείς διαπίστευσης υπόκεινται στην νομολογία την προστασίας δεδομένων, βάσει των νόμων 2472/1997 (προστασία προσωπικών δεδομένων) και 2774/1999 (προστασία δεδομένων στις τηλεπικοινωνίες).

Το άρθρο αυτό είναι στην ουσία αντιφατικό καθώς, σύμφωνα με τους δύο παραπάνω νόμους, οι υπηρεσίες ενός φορέα που υπόκειται στην νομολογία της προστασίας δεδομένων, δεν υπόκεινται απαραίτητα στη νομολογία που αφορά την προστασία δεδομένων στις τηλεπικοινωνίες . Πρακτικά αυτό σημαίνει, ότι ένα φορέας πιστοποίησης δεν θεωρείται απαραίτητα παροχέας τηλεπικοινωνιακών υπηρεσιών, ούτε υπηρεσιών πρόσβασης. Αυτός ο περιορισμός όμως, ένδέχεται να δυσχεραίνει τη λειτουργία του φορέα πιστοποίησης, π.χ. κατά την online διατήρηση Λιστών Ανάκλησης Πιστοποιητικών .

Άλλα θέματα που απαιτούν διευκρινήσεις στην Ελληνική νομολογία περί ηλεκτρονικών υπογραφών είναι οι νομικές ευθύνες για έκδοση «qualified» πιστοποιητικών στο κοινό και η ένταξη των επαγγελματιών Ιατρικής Φροντίδας σε μία Υποδομή Δημόσιου Κλειδιού.

Η *Ελληνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.)* αναμένεται σύντομα να εκδώσει πιο λεπτομερείς προσεγγίσεις για τις ηλεκτρονικές υπογραφές, τη παροχή υπηρεσιών πιστοποίησης και την εθελοντική διαπίστευση στη Χώρα, έτσι ώστε να διασαφηνιστούν τα παραπάνω προβλήματα .

Εκτός της Οδηγίας 1999/93/ΕC, ενέργειες *διεθνούς νομικής κατοχύρωσης* των ηλεκτρονικών υπογραφών γίνονται από το Διεθνή Οργανισμό Εμπορίου (UNIITRAL) .

Πέραν δε της νομολογίας που έχει ρυθμίσει ειδικότερα πρακτικά ζητήματα δεν υπάρχουν νομοθετήματα προσαρμοσμένα στις ιδιαιτερότητες της ελληνικής αγοράς. Βέβαια, παρά τα όποια προβλήματα διαφαίνεται η σταδιακή δημιουργία ενός νομοθετικού πλαισίου που θα αποτελέσει την βάση για την ρύθμιση του ηλεκτρονικού εμπορίου εν γένη και των ηλεκτρονικών πληρωμών ειδικότερα.

Προεδρικό Διάταγμα 33.2000: Το παρόν διάταγμα έχει σαν σκοπό τη προσαρμογή της Ελληνικής Νομοθεσίας προς τις διατάξεις της Οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου 97/5/ΕΚ της 27ης Ιανουαρίου 1997 "για τις διασυνοριακές μεταφορές πιστώσεων".

Υπουργική Απόφαση Ζ1-178/2001: Σκοπός αυτής της απόφασης είναι η εναρμόνιση προς τις διατάξεις της Σύστασης 97/489/ΕΚ της Επιτροπής της 30ης Ιουλίου 1997 "σχετικά με τις συναλλαγές που γίνονται με μέσα ηλεκτρονικής πληρωμής και ιδίως όσον αφορά τις σχέσεις μεταξύ του εκδότη και του κατόχου" και η προσαρμογή της Κοινής Υπουργικής Απόφασης Φ1-983/91 για την καταναλωτική πίστη (ΦΕΚ Β΄ 172), όπως ισχύει, προς τις διατάξεις της Οδηγίας 98/7/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 16ης Φεβρουαρίου 1998 "σχετικά με την τροποποίηση της οδηγίας 87/102/ΕΟΚ.

Πράξη Συμβουλίου Νομισματικής Πολιτικής 50/31.7.2002: Η παρούσα Πράξη καθορίζει το πλαίσιο επίβλεψης των συστημάτων πληρωμών. Ειδικότερα περιλαμβάνονται οι ορισμοί των εννοιών ηλεκτρονική πληρωμή, ηλεκτρονικό χρήμα, πιστωτικός κίνδυνος, διαχειριστής συστημάτων πληρωμών καθώς και άλλες βασικές έννοιες. Στην Πράξη αυτή ορίζεται το σύστημα πληρωμών ως σύστημα που συνίσταται σε σύνολο μέσων και τραπεζικών διαδικασιών που χρησιμοποιούνται, με βάση συμβάσεις και σύμφωνα με τους σχετικούς κανονισμούς λειτουργίας, από ομάδα προσώπων και οργανισμών για να εξυπηρετηθεί, διευκολυνθεί και διασφαλισθεί η ομαλή μεταφορά κεφαλαίων και κυκλοφορία του χρήματος σε μία περιοχή, συνήθως σε μία χώρα. Υπό την έννοια αυτή το σύστημα πληρωμών περιλαμβάνει: (ί) τα πιστωτικά ιδρύματα και τους χρηματοδοτικούς οργανισμούς, (ίί) τα μη πιστωτικά ιδρύματα που παρέχουν υπηρεσίες για τη διενέργεια πληρωμών, (ίίί) την τεχνική υποδομή, (ίν) το δίκτυο διασύνδεσης των φορέων που μεσολαβούν στις πληρωμές, (ν) τις διαδικασίες εκκαθάρισης, συμψηφισμού και διακανονισμού των πληρωμών και (νί) τους κανόνες που διέπουν τα μέσα πληρωμής και την εν γένει λειτουργία του συστήματος.

Επιπλέον, η Πράξη Αριθ. 50/31.7.2002 προσδιορίζει τις γενικές αρχές λειτουργίας των συστημάτων ηλεκτρονικού χρήματος καθώς και την σκοπιμότητα της άσκησης εποπτείας από μέρους της Τράπεζας της Ελλάδος.

Επιπλέον, η Πράξη Αριθ. 50/31.7.2002 προσδιορίζει τις γενικές αρχές λειτουργίας των συστημάτων ηλεκτρονικού χρήματος καθώς και την σκοπιμότητα της άσκησης εποπτείας από μέρους της Τράπεζας της Ελλάδος. μών και ηλεκτρονικού χρήματος στην Τράπεζα της Ελλάδος, διεύθυνση Νομισματικής Πολιτικής και Τραπεζικών Εργασιών, Γραφείο Επίβλεψης Συστημάτων Πληρωμών πριν από την έναρξη λειτουργίας τους, σε εξαμηνιαία βάση, σε ετήσια βάση, και σε περιπτώσεις έκτακτων περιστατικών. Ειδικότερα, σε ότι αφορά στα συστήματα πληρωμών, πριν από την έναρξη λειτουργίας του συστήματος υποβάλλονται τα παρακάτω στοιχεία:

1. Νομικό πλαίσιο λειτουργίας του συστήματος όπως αυτό εκφράζεται από το καταστατικό του ή/και οποιοδήποτε άλλο σχετικό νομοθέτημα ή συμφωνητικό που περιγράφει τα δικαιώματα και τις υποχρεώσεις του διαχειριστή και των μελών του συστήματος.
2. Οργανωτικό σχήμα και τρόπος διοίκησης του συστήματος.
3. Κανονισμός λειτουργίας του συστήματος, καθώς και οποιοδήποτε άλλο έγγραφο περιγράφει τις προϋποθέσεις συμμετοχής στο σύστημα, την τιμολογιακή πολιτική, τον τρόπο διακανονισμού των πληρωμών, τη χρονική στιγμή, κατά την οποία ο διακανονισμός καθίσταται αμετάκλητος, τις διαδικασίες διαχείρισης των πιστωτικών κινδύνων και των κινδύνων ρευστότητας.
4. Κατάλογος μελών στο σύστημα (για όσα λειτουργούν).
5. Τεχνική υποδομή του συστήματος με αναφορά στις ακολουθούμενες διαδικασίες διασφάλισης της λειτουργικής αξιοπιστίας και ασφάλειάς του.
6. Κόστος ανάπτυξης του συστήματος (για νέα συστήματα πληρωμών).
7. Ενδεχόμενη αξιολόγηση από εσωτερικούς ή εξωτερικούς φορείς.

Σε μηνιαία βάση, υποβάλλονται στοιχεία για κάθε μέσο πληρωμής (π.χ. εντολή μεταφοράς, επιταγή), συγκεντρωτικά και ανά μέλος του συστήματος. Σε ετήσια βάση, υποβάλλονται στοιχεία που αφορούν στο κόστος βελτιώσεων και συντήρησης του συστήματος καθώς και στο λειτουργικό κόστος. Σε περιπτώσεις έκτακτων περιστατικών, υποβάλλονται, εντός 24 ωρών από τη διαπίστωση του προβλήματος, στοιχεία όπως χρόνος, περιγραφή και αίτια του προβλήματος, ενδεχόμενες ζημίες των μελών του συστήματος και μέτρα που λήφθηκαν ή πρόκειται να ληφθούν για την αποκατάσταση του προβλήματος.

Αντίστοιχα, για τα συστήματα ηλεκτρονικού χρήματος υποβάλλονται τα ακόλουθα στοιχεία πριν από την έναρξη λειτουργίας τους:

1. Στοιχεία ταυτότητας του διαχειριστή (επιχειρηματικό σχέδιο, ίδια κεφάλαια, οργανωτικό σχήμα, προσωπικό, τεχνική υποδομή).
2. Κανονισμός λειτουργίας του συστήματος.
3. Τρόποι και προϋποθέσεις συμμετοχής στο σύστημα (για τον εκδότη, έμπορο, κάτοχο ηλεκτρονικού χρήματος).
4. Δικαιώματα και υποχρεώσεις συμμετεχόντων (του εκδότη, εμπόρου, κατόχου ηλεκτρονικού χρήματος).
5. Χαρακτηριστικά συστήματος (χρήσεις ηλεκτρονικού χρήματος, γεωγραφική κάλυψη, τρόποι έκδοσής του, όριο χρηματικής αξίας, δυνατότητα εξαργύρωσης, δυνατότητα μεταφοράς χρηματικής αξίας
μεταξύ πελατών, διαδικασία πληρωμής εμπόρων).
6. Κόστος ανάπτυξης του συστήματος.
7. Προβλεπόμενα μέτρα ασφάλειας για την πρόληψη περιστατικών πλαστογραφίας, απάτης και νομιμοποίησης χρημάτων από εγκληματικές δραστηριότητες.
8. Προβλεπόμενη διαδικασία αποζημίωσης συμμετεχόντων σε περίπτωση πτώχευσης του εκδότη.
9. Ενδεχόμενη αξιολόγηση από εσωτερικούς ή εξωτερικούς φορείς. Σε εξαμηνιαία βάση, υποβάλλονται στοιχεία που αφορούν στον αριθμό συμβεβλημένων εμπορικών
επιχειρήσεων, στον αριθμό τερματικών που αποδέχονται τις κάρτες (για τα συστήματα ηλεκτρονικού χρήματος που βασίζονται σε κάρτα). Ενώ σε ετήσια βάση, υποβάλλονται στοιχεία που αφορούν στο κόστος ανάπτυξης και λειτουργίας του συστήματος και στα έσοδα του συστήματος. Τέλος σε περιπτώσεις έκτατων περιστατικών κοινοποιούνται στην αρμόδια αρχή τα ίδια στοιχεία με τα συστήματα πληρωμών.

Πράξη Διοικητή 2501/31.10.2002. Η εν λόγω πράξη ρυθμίζει την ενημέρωση των συναλλασσομένων με τα πιστωτικά ιδρύματα για τους όρους που διέπουν τις συναλλαγές τους. Στην πράξη αυτή γίνεται ειδική μνεία για τις διενεργούμενες μέσω του διαδικτύου τραπεζικές συναλλαγές και ρυθμίζεται η πληροφορία που παρέχεται από τα τραπεζικά ιδρύματα προκειμένου να συμμορφώνεται με τις απαιτήσεις της πράξης. Αυτό, σύμφωνα με την πράξη, επιτυγχάνεται είτε με την άμεση γνωστοποίηση στο διαδίκτυο των σχετικών στοιχείων είτε με παραπομπή σε εναλλακτικό τρόπο παροχής της σχετικής πληροφόρησης (αρμόδιος υπάλληλος, διεύθυνση, αριθμός τηλ.) σε επίπεδο καταστήματος. Επιπλέον, προβλέπεται να παρέχονται από τα τραπεζικά ιδρύματα στις ιστοσελίδες τους: α) στοιχεία της ταυτότητας του πιστωτικού ιδρύματος και ειδικότερα της άδειας της Τράπεζας της Ελλάδος ή της λειτουργίας του μέσω του κοινοτικού διαβατηρίου σύμφωνα με το Ν. 2076/92 και τη δεύτερη συντονιστική τραπεζική Οδηγία 89/646/ΕΟΚ/15.12.89, β) πληροφορίες σχετικά με την ασφαλή διεξαγωγή των συναλλαγών μέσω του διαδικτύου (μορφή και βαθμός της παρεχόμενης ασφάλειας).

Νόμος 3148/2003 Επιτροπή Λογιστικής Τυποποίησης και Ελέγχων: Ο νόμος αυτός ρυθμίζει τη σύσταση και τις αρμοδιότητες της Επιτροπής Λογιστικής Τυποποίησης και Ελέγχων (Ε.Λ.Τ.Ε.). Επίσης έχει γίνει προσθήκη ειδικού κεφαλαίου στον νόμο για τα ιδρύματα ηλεκτρονικού χρήματος. Ειδικότερα, σε ότι αφορά στα ιδρύματα ηλεκτρονικού χρήματος με το Νόμο 3148/2003 σκοπείται η ενσωμάτωση στην ελληνική τραπεζική νομοθεσία των διατάξεων της 2000/12/ΕΚ Οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου «σχετικά με την ανάληψη και την άσκηση δραστηριότητας πιστωτικών ιδρυμάτων» (L 126/ 26.5.2000), των διατάξεων της 2000/46/ ΕΚ Οδηγίας του Ευρωπαϊκού

Κοινοβουλίου και του Συμβουλίου «για την ανάληψη, άσκηση και προληπτική εποπτεία δραστηριότητας ιδρύματος ηλεκτρονικού χρήματος» (L 275/27.10.2000).

Σχέδιο Νόμου που ψηφίστηκε στις 21 Οκτωβρίου 2003. Κανόνες τιμολόγησης , ρυθμίσεις Φ.Π.Α. ηλεκτρονικών υπηρεσιών και άλλες διατάξεις. Το εν λόγω σχέδιο νόμου έχει στόχο να εναρμονίσει την ελληνική νομοθεσία με τους όρους που επιβάλλονται στην τιμολόγηση με τις διατάξεις της οδηγίας 2001/115/ΕΚ (20 Δεκεμβρίου 2001) του Συμβουλίου της Ευρωπαϊκής Ένωσης .

ΕΕ Οδηγία 2001/115/ΕC (Προσθήκη της 77/388/ΕC) για η-τιμολόγια / η-αποθήκευση τιμολογίων. Τα οφέλη της οδηγίας αυτής ήταν ο δια-Ευρωπαϊκός, αδιάβλητος συντονισμός και έλεγχος του ΦΠΑ.

Υπουργική απόφαση 1023404/1363/0016 του 2001 για την είσπραξη του Φόρου Προστιθέμενης Αξίας (Φ.Π.Α.) που υποβάλλεται ηλεκτρονικά, με χρέωση Τραπεζικών λογαριασμών των υποκειμένων. Αναφέρει αναλυτικά τις διαδικασίες και τους όρους σύμφωνα με τους οποίους εισπράττεται το ΦΠΑ με χρέωση των τραπεζικών λογαριασμών ή των πιστωτικών καρτών που τηρούν οι φορολογούμενοι.

Νόμος 3148/2003 (ΦΕΚ Α΄ 136/5,6,2003) Επιτροπή Λογιστικής Τυποποίησης και Ελέγχων, αντικατάσταση και συμπλήρωση των διατάξεων για τα ιδρύματα ηλεκτρονικού χρήματος και άλλες διατάξεις. Με τον νόμο αυτό αποσκοπείται η ενσωμάτωση στην τραπεζική ελληνική νομοθεσία των διατάξεων της 2000/12/ΕΚ Οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου «σχετικά με την ανάληψη και την άσκηση δραστηριότητας πιστωτικών ιδρυμάτων» (L 126/26.5.2000), των διατάξεων της 2000/46/ΕΚ Οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου «για την ανάληψη, άσκηση και προληπτική εποπτεία δραστηριότητας ιδρύματος ηλεκτρονικού χρήματος» (L 275/27.10.2000)».

3 ΑΣΦΑΛΕΙΑ ΤΕΧΝΟΛΟΓΙΩΝ

3.1 ΈΞΥΠΝΕΣ ΚΑΡΤΕΣ

Η έξυπνη κάρτα είναι πλαστική, σε μέγεθος πιστωτικής κάρτας που ενσωματώνει είτε με έναν μικροεπεξεργαστή και ένα τσιπ μνήμης, είτε μόνο με ένα τσιπ μνήμης με τη μη-προγραμματιζόμενη λογική η-υπολογιστή. Η κάρτα μικροεπεξεργαστών μπορεί να προσθέσει, να διαγράψει, και να χειριστεί τις πληροφορίες για την κάρτα, ενώ μια κάρτα μνήμη-τσιπ (παραδείγματος χάρη, προπληρωμένες τηλεφωνικές κάρτες) μπορεί να αναλάβει μόνο μια προκαθορισμένη λειτουργία.

Οι έξυπνες κάρτες, αντίθετα από τις μαγνητικές κάρτες, μπορούν να έχουν όλες τις απαραίτητες λειτουργίες και τις πληροφορίες για την κάρτα. Επομένως, δεν απαιτούν πρόσβαση σε μακρινές βάσεις δεδομένων κατά την διάρκεια της συναλλαγής.

Σήμερα, υπάρχουν τρεις κατηγορίες έξυπνων καρτών, οι οποίες εξελίσσονται γρήγορα στις νέες αγορές και στις εφαρμογές:

- Οι **κάρτες μικροεπεξεργαστών** (Integrated Circuit Microprocessor Cards -IC) ("κάρτες τσιπ") προσφέρουν μεγαλύτερη αποθήκευση μνήμης και ασφάλεια των δεδομένων από μια παραδοσιακή κάρτα stripe mag. Οι κάρτες τσιπ μπορούν επίσης να επεξεργαστούν τα δεδομένα όσο αφορά την κάρτα. Η τρέχουσα παραγωγή των καρτών τσιπ έχει έναν 8 bit επεξεργαστή, 16KB ανάγνωση μνήμης, και 512 bytes μνήμης random-access. Αυτό τους δίνει ίση δύναμη επεξεργασίας του αρχικού IBM-XT υπολογιστή, αν και με ελαφρώς λιγότερη ικανότητα μνήμης. Αυτές οι κάρτες χρησιμοποιούνται για ποικίλες εφαρμογές, ειδικά εκείνες που ενσωματώνουν το σύστημα κρυπτογραφίας, το οποίο απαιτεί το χειρισμό μεγάλων αριθμών. Κατά συνέπεια, οι κάρτες τσιπ είναι η κύρια πλατφόρμα για τις κάρτες που κρατούν μια ασφαλή ψηφιακή ταυτότητα. Μερικά παραδείγματα αυτών των καρτών είναι:
    - Κάρτες που έχουν χρήματα (“stored value cards”)
    - Κάρτες που κρατούν χρηματικές ισοδυναμίες (πχ “affinity cards”)
    - Κάρτες που παρέχουν ασφαλή πρόσβαση στο δίκτυο

    - Κάρτες για ασφαλή χρήση κινητών τηλεφώνων
    - Κάρτες που επιτρέπουν στους μετασχηματιστές της τηλεόρασης να παραμείνουν ασφαλείς από τις πειρατείες
- Οι **κάρτες μνήμης** (Integrated Circuit -IC) Memory Card ολοκληρωμένου κυκλώματος μπορούν να κρατήσουν πάνω από 1-4 KB δεδομένων, αλλά δεν έχουν κανέναν επεξεργαστή στην κάρτα με την οποία να χειριστεί εκείνο το δεδομένο. Κατά συνέπεια, εξαρτώνται από τον αναγνώστη καρτών (συσκευή αποδοχής κάρτας) για την επεξεργασία τους και είναι κατάλληλοι για τις χρήσεις όπου η κάρτα εκτελεί μια σταθερή λειτουργία. Οι κάρτες μνήμης αντιπροσωπεύουν τον όγκο των 600 εκατομμυρίων έξυπνων καρτών που πωλήθηκαν πέρυσι, για τις προπληρωμένες εφαρμογές μίας χρήσης-καρτών όπως τις προπληρωμένες τηλεφωνικές κάρτες. Οι κάρτες μνήμης είναι δημοφιλείς ως εναλλακτικές λύσεις υψηλής ασφάλειας στις μαγνητικές κάρτες.
- Οι **οπτικές κάρτες μνήμης** μοιάζουν με ένα κομμάτι του CD που κολλιέται στην κορυφή. Οι οπτικές κάρτες μνήμης μπορούν να αποθηκεύσουν μέχρι 4 MB δεδομένων. Μόλις γραφτούν τα στοιχεία δεν μπορούν να αλλάξουν ή να αφαιρεθούν. Κατά συνέπεια, αυτός ο τύπος κάρτας είναι ιδανικός για την τήρηση αρχείων - παραδείγματος χάρη ιατρικά αρχεία, driving records, ή οδηγίες ταξιδιού.

Σημαντικές χρήσεις των έξυπνων καρτών περιλαμβάνουν την παροχή των ενισχυμένων οικονομικών υπηρεσιών, την αύξηση της ασφάλειας και της ευελιξίας των κινητών τηλεφώνων, και την εξασφάλιση των μεταδόσεων δορυφόρων και καλωδίων στους μετασχηματιστές TV.

Java κάρτες

Οι προδιαγραφές της κάρτας Java επιτρέπουν στην τεχνολογία της Java να τρέξει τις έξυπνες κάρτες και άλλες συσκευές με περιορισμένη μνήμη. Στη περίπτωση μιας κάρτας Java βασισμένης σε πλατφόρμα, εφαρμογές βασισμένες στη τεχνολογία της Java, υπό μορφή κώδικα-byte, φορτώνονται στη ζώνη μνήμης της έξυπνης κάρτας όπου οργανώνονται από την εικονική μηχανή. Ο εκτελέσιμος κώδικας είναι ανεξάρτητος πλατφόρμας έτσι ώστε οποιαδήποτε κάρτα που ενσωματώνει έναν διερμηνέα καρτών της Java να μπορεί να τρέξει την ίδια εφαρμογή.

Το περιβάλλον εφαρμογής της κάρτας Java (JCAE) είναι χορηγημένο σε μια βάση OEM στους κατασκευαστές έξυπνων καρτών, που αντιπροσωπεύουν περισσότερο από το 90% της παγκόσμιας κατασκευής έξυπνων καρτών.

Υπάρχουν διάφορα μοναδικά οφέλη της κάρτας Java, όπως:

- **Ανεξάρτητη Πλατφόρμας** - μικροεφαρμογές της Java κάρτας οι οποίες συγκλίνουν με την προδιαγραφή καρτών API της Java, θα τρέξουν στις κάρτες που αναπτύσσονται χρησιμοποιώντας το JCAE – επιτρέποντας στους προγραμματιστές να χρησιμοποιήσουν την ίδια μικροεφαρμογή τεχνολογίας καρτών της Java για να τρέξουν τις κάρτες διαφορετικών προμηθευτών.
- **Υποστήριξη Πολλαπλών Εφαρμογών** – Οι έξυπνες κάρτες ήταν αρχικά κάρτες ενιαίας λειτουργίας. Οι σημαντικές ανακαλύψεις που φέρνουν περισσότερες τεχνολογικές προόδους στις κάρτες καθιστούν πιθανό να βάλουν πολλές εφαρμογές σε μια ενιαία κάρτα.
- **Ευελιξία στην αλλαγή Εφαμογών** - Η εγκατάσταση των εφαρμογών, αφού έχει εκδοθεί η κάρτα, παρέχει στους εκδότες καρτών τη δυνατότητα να ανταποκριθεί δυναμικά στις μεταβαλλόμενες ανάγκες του πελάτη τους. Παραδείγματος χάρη, εάν ένας πελάτης αποφασίσει να αλλάξει το πρόγραμμα που συνδέεται με την κάρτα, ο εκδότης καρτών μπορεί να κάνει αυτήν την αλλαγή, χωρίς να πρέπει να εκδοθεί μια νέα κάρτα. Ευελιξία - η μεθοδολογία object-oriented τεχνολογίας καρτών της Java παρέχει ευελιξία στις έξυπνες κάρτες προγραμματισμού.
- **Συμβατότητα** - η κάρτα API Java είναι συμβατή με τα επίσημα διεθνή πρότυπα, όπως, ISO7816, και τα συγκεκριμένα βιομηχανικά πρότυπα, όπως, Europay/Master Card/Visa (EMV).

Βιομηχανίες που δέχονται τη Java κάρτα: σχεδόν οποιοσδήποτε τύπος έξυπνης κάρτας μπορεί να εγκατασταθεί με την τεχνολογία της κάρτας Java, συμπεριλαμβανομένων.

- Κινητή τηλεφωνία GSM, μια διεθνής ασύρματη τηλεφωνία που καλύπτει την Ευρώπη, τη Μέση Ανατολή, την Αφρική, και την Ασία, με εξαίρεση την Ιαπωνία.
- Οικονομικές συναλλαγές, online και offline,
- Κάρτες πρόσβασης σε Πανεπιστήμια,
- Έλεγχος λογικής πρόσβασης στα συστήματα IT.

Στη βιομηχανία κινητής τηλεφωνίας GSM, απαιτούνται οι έξυπνες κάρτες για να ενεργοποιήσουν το τηλέφωνο. Η κάρτα επικυρώνει το χρήστη και παρέχει τα κλειδιά κρυπτογράφησης για την ψηφιακή μετάδοση φωνής. Όταν εγκαθίστανται με την Java κάρτα, οι έξυπνες κάρτες GSM μπορούν επίσης να παρέχουν υπηρεσίες συναλλαγών όπως οι μακρινές τραπεζικές εργασίες και έκδοση εισιτηρίων. Στην τραπεζική βιομηχανία, οι έξυπνες κάρτες δίνουν στους χρήστες ασφαλή πρόσβαση σε μια ευρεία σειρά δικτυωμένων οικονομικών υπηρεσιών συμπεριλαμβανομένων των μηχανών πληρωμής μετρητών, της πληρωμής λογαριασμών, και των κομίστρων διοδίων. Η κάρτα Java που βασίζεται στην έξυπνη κάρτα, μπορεί να προσαρμόσει πολλές οικονομικές εφαρμογές σε μια ενιαία κάρτα και να παραδώσει τις υπηρεσίες προστιθέμενης αξίας όπως τα προγράμματα απόστασης σε μίλια ή ασφάλειας, κάνοντας on-line εμπόριο.

Μια ευρεία ποικιλία άλλων εφαρμογών είναι διαθέσιμη όπου η ασφάλεια και η πιστοποίηση ταυτότητας είναι σημαντικές, όπως η παροχή της πρόσβασης στις εγκαταστάσεις και τα ιατρικά αρχεία. Η τεχνολογία καρτών της Java θα ενισχύσει την καταναλωτική πρόσβαση στις νέες υπηρεσίες ηλεκτρονικού επιχειρείν μέσο μιας σειράς Web-aware συσκευών. Τα κινητά τηλέφωνα και ο εξοπλισμός καλωδιακής τηλεόρασης είναι παραδείγματα των αγορών όπου η πλειοψηφία των διαθέσιμων προϊόντων περιλαμβάνει τις ενσωματωμένες έξυπνες κάρτες. Οι μελλοντικές εφαρμογές, που περιγράφονται σε CardTech/SecurTech, χρησιμοποιούν την τεχνολογία της κάρτας Java στη βιομηχανία βιομετρικών, με εφαρμογές στην αναγνώριση δακτυλικών αποτυπωμάτων και αναγνώριση προσώπου, και τις ανέπαφες εφαρμογές για τις έξυπνες κάρτες.

Βιομετρικές Έξυπνες Κάρτες

Η βιομετρική είναι μια μεθοδολογία για την αναγνώριση και τον προσδιορισμό των ανθρώπων βασισμένη στα μεμονωμένα και ευδιάκριτα χαρακτηριστικά φυσιολογικά συμπεριφοράς. Τα βιομετρικά γνωρίσματα περιλαμβάνουν τα δακτυλικά αποτυπώματα, το σχήμα του προσώπου, την αναγνώριση της ίριδας, την αναγνώριση του αμφιβληστροειδή, τη γεωμετρία χεριών, την ομιλία, τη γραφή, και τον τρόπο πληκτρολόγησης, ακόμη και την αναγνώριση φλεβών των καρπών. Η βιομετρική είναι ενδιαφέρουσα σε οποιαδήποτε περιοχή όπου είναι σημαντικό να ελεγχθεί η αληθινή ταυτότητα ενός ατόμου. Η χρήση της βιομετρικής συνεχίζει να επεκτείνεται πέρα από το ευρύ φάσμα εφαρμογών σε όλο τον κόσμο. Από τις τραπεζικές εργασίες, οι εταιρίες όλο και περισσότερο αναγνωρίζουν ότι ο ακριβής προσδιορισμός και η πιστοποίηση ταυτότητας χρηστών είναι βασικές απαιτήσεις για την μείωση της απάτης και για την αύξηση ασφάλειας πληροφοριών της επιχείρησης. Σημαντικοί κατασκευαστές ηλεκτρονικής τεχνολογίας ενσωματώνουν αυτή την τεχνολογία στα πληκτρολόγιά τους, ATMs, PCs και άλλες φορητές συσκευές για αυξανόμενη ευελιξία και ασφάλεια χρηστών.

Η βιομετρική ασφάλεια είναι πιο δυνατή από τις μεθόδους όπως οι κωδικοί πρόσβασης, οι αριθμοί PIN, οι έξυπνες κάρτες, τα σύμβολα ή η Υποδομή Δημόσιου Κλειδιού (ΥΔΚ) επειδή η βιομετρική προσδιορίζει τα άτομα παρά τις συσκευές. Αυτοί οι μέθοδοι ασφάλειας μπορούν να χαθούν ή να κλεφτούν και επομένως να βρεθούν στα χέρια των αναρμόδιων χρηστών. Ένας βιομετρικός έλεγχος, όπως ένα δακτυλικό αποτύπωμα, είναι ένα κλειδί που δεν μπορεί ποτέ να χαθεί. Η βιομετρική τεχνολογία έχει συνδυαστεί με τη τεχνολογία των έξυπνων καρτών για να προωθήσει τις βιομετρικές έξυπνες κάρτες. Δηλαδή, η βιομετρική χρησιμοποιείται για την επικύρωση στα πρότυπα ασφάλειας έξυπνων καρτών. Με την προσθήκη της βιομετρικής τεχνολογίας σε μια λύση έξυπνων καρτών, βελτιώνουν την ασφάλεια των καρτών και προστατεύουν την ιδιοκτησία του κατόχου κάρτας. Η προσθήκη

της βιομετρικής τεχνολογίας σε μια έξυπνη κάρτα βελτιώνει πολύ την ασφάλεια της κάρτας. Η βιομετρική τεχνολογία επιτρέπει στις εταιρίες που εκδίδουν την κάρτα να είναι βέβαιες ότι το άτομο που επιτρέπουν να έχουν πρόσβαση στις πληροφορίες ή μια θέση, είναι το ίδιο άτομο. Τα βιομετρικά χαρακτηριστικά γνωρίσματα είναι μοναδικά σε ένα πρόσωπο και δεν μπορούν να αναπαραχθούν από έναν απατεώνα, όπως μπορούν τα PINs και οι κωδικοί πρόσβασης. Χρησιμοποιώντας περισσότερα από ένα βιομετρικά προσδιοριστικά, τα ψεύτικα ποσοστά αποδοχής, καθώς επίσης και τα ψεύτικα ποσοστά απόρριψης, παρουσιάζουν εντυπωσιακή πτώση.

Οι βιομετρικές πληροφορίες που αποθηκεύονται στην έξυπνη κάρτα επιτρέπουν στον τελικό χρήστη να μεταφέρει τα δικά του βιο-δεδομένα. Ο κάτοχος κάρτας γράφει τα βιο-στοιχεία του (δακτυλικό αποτύπωμα, φωνή ή/και πρόσωπο) και αυτές οι πληροφορίες οργανώνονται μέσο ενός αλγορίθμου, ο οποίος δημιουργεί έναν αριθμό που κρυπτογραφείται και αποθηκεύεται στην κάρτα. Η πιστοποίηση ταυτότητας εκτελείται με τη σύγκριση τσιπ των βιομετρικών προτύπων που αποθηκεύονται στην έξυπνη κάρτα με τα βιομετρικά δεδομένα που συγκεντρώνονται σε κάθε συναλλαγή. Ο χρήστης κρατά την κάρτα με αυτά, χρησιμοποιώντας την σε περίπτωση ανάγκης. Ο χρήστης διατηρεί τον πλήρη έλεγχο των προσωπικών βιομετρικών δεδομένων τους. Εάν η κάρτα χαθεί ή κλαπεί, δεν μπορεί να χρησιμοποιηθεί από οποιονδήποτε άλλον. Ο βιομετρικός προσδιορισμός μπορεί να χρησιμοποιηθεί για να αποτρέψει την αναρμόδια πρόσβαση σε κτίρια, στις μηχανές του ATM, στον υπολογιστή PC, στους τερματικούς σταθμούς, στα κινητά τηλέφωνα, στις ασύρματες συσκευές, στα αρχεία υπολογιστών, στις βάσεις δεδομένων, και στα κλειστά και ανοικτά δίκτυα υπολογιστών.

Έξυπνες Κάρτες ΥΔΚ

Οι άνθρωποι συνήθιζαν να βασίζουν την εμπιστοσύνη τους σε συνεργάτες με φυσική επαφή ή/και σε γραπτές υπογραφές. Σε έναν ηλεκτρονικό δικτυωμένο κόσμο, αυτοί οι τρόποι δεν είναι πλέον δυνατοί. Ο στόχος μιας Υποδομής Δημοσίου Κλειδιού (**ΥΔΚ**) είναι να αντικατασταθούν εκείνες οι παραδοσιακές μορφές εμπιστοσύνης. Μία ΥΔΚ είναι δυνατό να επιτρέψει τους τέσσερις ακρογωνιαίους λίθους της ηλεκτρονικής ασφάλειας: αυθεντικότητα, ακεραιότητα, εμπιστευτικότητα, και μη-άρνηση ευθύνης. Η λειτουργία μιας ΥΔΚ είναι βασισμένη στην ασύμμετρη κρυπτογράφηση.

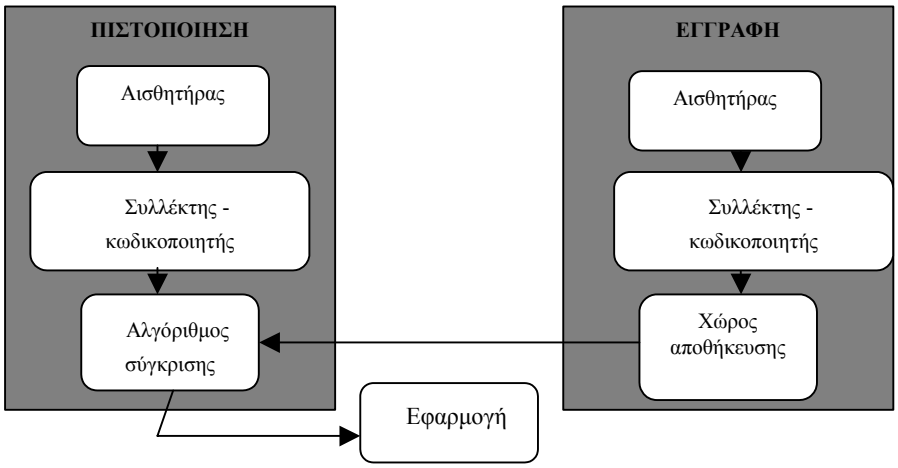
Σε έναν κόσμο ΥΔΚ, ο καθένας θα είχε τουλάχιστον ένα κρυπτογραφικό βασικό ζευγάρι. Κάθε βασικό ζευγάρι θα περιείχε ένα μυστικό (ιδιωτικό) και ένα δημόσιο κρυπτογραφικό κλειδί. Αυτά τα κλειδιά είναι χαρακτηριστικά 1024-bit ή 2048-bit των δυαδικών ψηφίων με μια μοναδική ιδιότητα: όταν ένα χρησιμοποιείται με έναν αλγόριθμο κωδικοποίησης για να κρυπτογραφήσει τα δεδομένα, το άλλο μπορεί να χρησιμοποιηθεί με τον ίδιο αλγόριθμο για να αποκρυπτογραφήσει τα δεδομένα. Το κλειδί κωδικοποίησης δεν μπορεί να χρησιμοποιηθεί για την αποκωδικοποίηση. Τα δημόσια κλειδιά πιστοποιούνται από ένα αρμόδιο συμβαλλόμενο μέρος όπως ένα κοινό συμβολαιογράφο, ένα γραφείο διαβατηρίων, μια κυβερνητική αντιπροσωπεία ή μια **Έμπιστη Τρίτη Οντότητα (ΕΤΟ)**. Το **δημόσιο κλειδί** διανέμεται ευρέως, συχνά μέσο ενός καταλόγου ή μιας βάσης δεδομένων που μπορεί να αναζητηθεί από το κοινό. Το **ιδιωτικό κλειδί** παραμένει ένα στενά φυλαγμένο μυστικό από τον ιδιοκτήτη. Υπάρχουν μερικές δυνατότητες για την ιδιωτική βασική αποθήκευση (τα κλειδιά είναι μακριές σειρές κομματιών και η απομνημόνευση τους είναι αδύνατη). Υπάρχουν τρεις δυνατότητες αποθήκευσης: σκληρός δίσκος, δισκέτα και έξυπνη κάρτα. Η αποθήκευση έξυπνων καρτών παρουσιάζει το καλύτερο σενάριο. Είναι ο τρόπος που προτιμάται, για να αποθηκευτεί το ιδιωτικό κλειδί κάποιου. Χωρίς μια έξυπνη κάρτα, το ιδιωτικό κλειδί θα έπρεπε να αποθηκευτεί σε δίσκο. Αν και προστατεύεται με μια pass-phrase, μπορεί να αντιγραφεί εύκολα.

Μερικοί σύγχρονοι επεξεργαστές έξυπνων καρτών έχουν ακόμη και τους ενσωματωμένους κρυπτογραφικούς επεξεργαστές που επιτρέπουν την υπογραφή και τη βασική παραγωγή να γίνουν εξ ολοκλήρου στην κάρτα, έτσι ώστε το ιδιωτικό κλειδί να μην αποκαλυφθεί ή να ακυρωθεί ποτέ. Ο μικροεπεξεργαστής δίνει στην έξυπνη κάρτα ένα μεγάλο πλεονέκτημα πέρα από τα μαγνητικά ή οπτικά μέσα αποθήκευσης. Μια έξυπνη κάρτα **ΥΔΚ** μπορεί να

είναι πολύ ασφαλής, εξαλείφοντας οποιασδήποτε δυνατότητα του βασικού ζευγαριού που είναι έξω κατά τη διάρκεια της δημιουργίας και της μεταφοράς. Η αρχική δαπάνη είναι υψηλότερη, δεδομένου ότι οι έξυπνες κάρτες απαιτούν έναν αναγνώστη. Αλλά αυτό το συμπληρωματικό κόστος αντισταθμίζεται από πολύ υψηλότερη ασφάλεια ιδιωτικού κλειδιού και από κατάλληλη μεταφορά. Έτσι, οι έξυπνες κάρτες προσφέρουν μια πρακτική στρατηγική για **ΥΔΚ** στο υλικό παρά στο λογισμικό, για μεγαλύτερη ασφάλεια. Μια έξυπνη κάρτα μπορεί να περιέχει το ιδιωτικό κλειδί του χρήστη, που μπορεί να χρησιμοποιηθεί μόνο από κάποιο με τη φυσική κατοχή του σημείου (ΤΙ ΕΧΕΤΕ), και τη γνώση μιας μυστικής μεταβίβασης φράσης (ΤΙ ΞΕΡΕΤΕ) και ίσως ένα βιομετρικό προσδιοριστικό (ΠΟΙΟΣ ΕΙΣΤΕ). Η σύνδεση της **ΥΔΚ** με τις έξυπνες κάρτες, αναμένεται να γίνει σημαντική.

3.2 ΒΙΟΜΕΤΡΙΚΑ ΣΥΣΤΗΜΑΤΑ

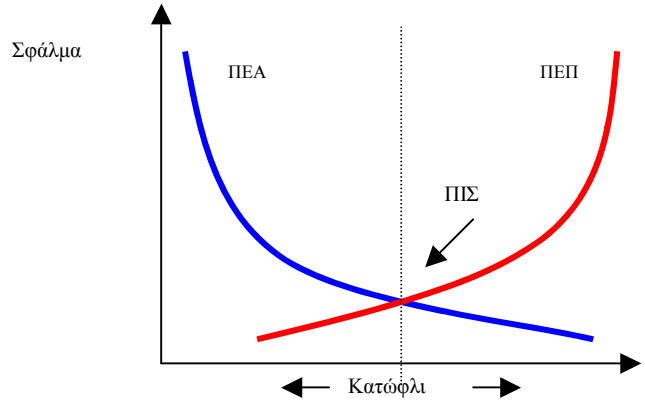
Ένα τυπικό και απλοποιημένο μοντέλο βιομετρικού συστήματος παρουσιάζεται στο επόμενο σχήμα:



Τυπικό μοντέλο βιομετρικού συστήματος

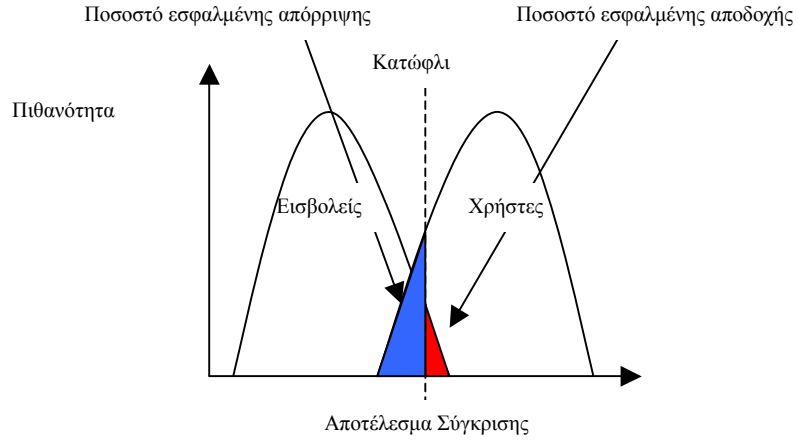
Ο χρήστης αρχικά εγγράφεται στο σύστημα, μέσα από μια διαδικασία δειγματοληψίας των χαρακτηριστικών του. Ο αισθητήρας αποτυπώνει τα χαρακτηριστικά του χρήστη (μπορεί να είναι μία κάμερα, ή ένας οπτικός ή επαγωγικός αισθητήρας δακτυλικών αποτυπωμάτων). Ο συλλέκτης εξάγει τα ζητούμενα (ανάλογα με τον αλγόριθμο) στοιχεία των χαρακτηριστικών και τα κωδικοποιεί με μία μονόδρομη συνάρτηση. Το αποτέλεσμα, ονομάζεται βιομετρικό δείγμα (biometric template). Επισημαίνουμε ότι το βιομετρικό δείγμα δεν αποτελεί το αυτό καθεαυτό χαρακτηριστικό του χρήστη. Δεν είναι για παράδειγμα μια εικόνα του δακτυλικού του αποτυπώματος ή του προσώπου του, αλλά μία κωδικοποιημένη μορφή της δειγματοληψίας αυτών, που υλοποιείται με μία συνάρτηση που δεν επιτρέπει την αναδημιουργία του χαρακτηριστικού από αυτή. Το βιομετρικό δείγμα, αποθηκεύεται σε κάποια κεντρική βάση δεδομένων ή σε κάποια έξυπνη κάρτα.
Για να πιστοποιηθεί, η ταυτότητα του χρήστη, συλλέγονται τα χαρακτηριστικά του από τον αισθητήρα, δημιουργείται η κωδικοποιημένη μορφή τους και συγκρίνεται με την πρωτύτερα αποθηκευμένη. Ο αλγόριθμος σύγκρισης, εξάγει το ποσοστιαίο αποτέλεσμα της σύγκρισης. Η απόφαση για το αν η πιστοποίηση ταυτότητας είναι επιτυχής ή όχι είναι ευθύνη του συστήματος, ή της εφαρμογής (ανάλογα με την υλοποίηση). Για παράδειγμα 70% ομοιότητα μπορεί να είναι αποδεκτό αποτέλεσμα για μία εφαρμογή που στοχεύει στη διευκόλυνση κάποιας διαδικασίας, αλλά μη αποδεκτό για μια εφαρμογή που υλοποιεί την ασφάλεια στο σύστημα.
Τα βιομετρικά συστήματα παραμετροποιούνται ανάλογα με την εφαρμογή. Δύο βασικές παράμετροι, είναι το Ποσοστό Εσφαλμένης Παραδοχής (False Acceptance Rate) και το Ποσοστό Εσφαλμένης Απόρριψης (False Rejection Rate), ενώ το σημείο τομής τους ονομάζεται Ποσοστό Ίσου Σφάλματος (ΠΙΣ - Equal Error Rate).Το Ποσοστό Εσφαλμένης

Παραδοχής (ΠΕΠ) είναι η πιθανότητα λανθασμένης έγκρισης ενός μη εξουσιοδοτημένου χρήστη. Το Ποσοστό Εσφαλμένης Απόρριψης (ΠΕΑ) είναι η πιθανότητα απόρριψης ενός εξουσιοδοτημένου χρήστη.



Σφάλματα

Τα σύγχρονα βιομετρικά έχουν ΠΙΣ της τάξης του 0.1% (κυμαίνεται ανάλογα με την τεχνική), ποσοστό το οποίο μειώνεται συνεχώς με τη βελτίωση της τεχνολογίας των βιομετρικών.
Όσο αφορά στην παραμετροποίηση , για δεδομένο σύστημα, όσο μειώνεται το ΠΕΠ, τόσο πιο αυστηρό γίνεται το σύστημα και τόσο αυξάνει το ΠΕΑ και το αντίστροφο. Μεγάλο ΠΕΠ για δεδομένο σύστημα, σημαίνει υψηλότερο επίπεδο ασφάλειας, αλλά και περισσότερους δυσαρεστημένους χρήστες, που πιθανώς απορρίπτονται λανθασμένα από το σύστημα. Η επιλογή του σημείου λειτουργίας ή αλλιώς του κατωφλίου φαίνεται στο επόμενο σχήμα.



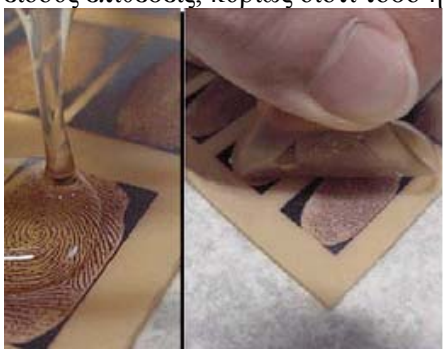
Παραμετροποίηση βιομετρικού συστήματος

Συνήθη μεγέθη παραμετροποίησης για εφαρμογές ασφάλειας είναι: ΠΕΠ=0,001% και ΠΕΑ<1%.
Τα παραπάνω ποσοστά, δίνουν μία εικόνα για το επίπεδο απόδοσης των βιομετρικών, δεν είναι όμως αρκετά για την αξιολόγηση των βιομετρικών συστημάτων. Παρακάτω, εξετάζουμε κάποια τεχνολογικά ζητήματα και κάποια ζητήματα υλοποίησης που αφορούν στο επίπεδο ασφάλειας των βιομετρικών, αλλά δεν καθορίζουν τα ΠΕΠ, ΠΕΑ και ΠΙΣ.

Επιθέσεις σε Βιομετρικά – Τεχνολογικά Ζητήματα

Τα σύγχρονα βιομετρικά συστήματα, εμφανίστηκαν πριν από περίπου τρεις δεκαετίες. Η τεχνολογία των βιομετρικών έχει εξελιχθεί σε μεγάλο βαθμό, αλλά κάποια προβλήματα παραμένουν. Ένα από τα σημαντικότερα, είναι η δυνατότητα του συστήματος να ξεχωρίσει ένα πραγματικό χαρακτηριστικό, από ένα αντίγραφο. Το πρόβλημα αυτό, εμφανίζεται

μάλιστα πολύ έντονο, στο είδος των βιομετρικών που έχει τη μεγαλύτερη ιστορία και το συντριπτικό μερίδιο στην αγορά, αυτό της αναγνώρισης δακτυλικών αποτυπωμάτων.
Πρόσφατα πειράματα έδειξαν ότι σύγχρονα βιομετρικά είναι εύκολο να ξεγελαστούν από αντίγραφα δακτυλικών αποτυπωμάτων. Τα τεχνητά δακτυλικά αποτυπώματα, είναι σχετικά εύκολο να δημιουργηθούν από πυρίτιο ή ζελατίνη, με μία διαδικασία που διαρκεί από μερικές ώρες, ως το πολύ μερικές μέρες. Ακόμα πιο εύκολο είναι να βρούμε τα δακτυλικά αποτυπώματα ενός χρήστη (σε πόμολα, ποτήρια, γυάλινες επιφάνειες). Τα βιομετρικά συστήματα (παρά τις διαβεβαιώσεις των κατασκευαστών) δείχνουν αδύναμα σε τέτοιου είδους επιθέσεις, κυρίως διότι τόσο η επιδερμίδα, όσο και το πυρίτιο είναι <<νεκρά>>υλικά.



Δημιουργώντας τεχνητά αποτυπώματα

Ανάλογα πειράματα είχαν διεξαχθεί στο παρελθόν σε οπτικούς αισθητήρες δακτυλικών αποτυπωμάτων. Οι επιθέσεις είχαν ονομαστεί επιθέσεις εναπομένουσας εικόνας. Όταν ένας νόμιμος χρήστης χρησιμοποιούσε το σύστημα, άφηνε πάνω στον οπτικό αισθητήρα το αποτύπωμά του (όπως συμβαίνει, όταν ακουμπήσουμε το δάκτυλό μας σε μιας γυάλινη επιφάνεια). Στη συνέχεια, η τοποθέτηση μιας λεπτής σακούλας ζεστού νερού πάνω στον αισθητήρα, ενεργοποιούσε το σύστημα, το οποίο έδινε και πάλι πρόσβαση στον μη εξουσιοδοτημένο χρήστη.
Η επιστημονική κοινότητα έρευνας και ανάπτυξης βιομετρικών συστημάτων, είναι πλέον απασχολημένη με την ανάπτυξη ενός υποσυστήματος ανίχνευσης ζωτικότητας. Το υποσύστημα αυτό βασίζεται στη μέτρηση μερικών ακόμα χαρακτηριστικών, όπως η σχετική διηλεκτρική σταθερά, η αγωγιμότητα, οι καρδιακοί παλμοί, ή η ροή του οξυγονωμένου αίματος. Η υλοποίηση του υποσυστήματος ανίχνευσης ζωτικότητας βρίσκεται ήδη σε τελικά στάδια από αρκετούς κατασκευαστές.
Παρόμοια ευπαθή σημεία χαρακτηρίζουν και άλλες βιομετρικές τεχνικές. Εξελιγμένα συστήματα σύνθεσης ομιλίας, μπορεί να ξεγελάσουν τα βιομετρικά αναγνώρισης φωνής. Φωτογραφίες προσώπου και εικόνες ίριδας, ξεγελούν συστήματα αναγνώρισης προσώπου και ίριδας αντίστοιχα. Η λύση σε αυτά τα προβλήματα είναι και πάλι πολύ κοντά στην υλοποίησή της, με την ανάπτυξη βιομετρικών εξελιγμένης τρισδιάστατης αναγνώρισης προσώπου, με εξελιγμένους ανιχνευτές της τυχαίας συστολής και διαστολής της κόρης του ματιού που δεν οφείλεται σε εξωτερικά ερεθίσματα, με αλληλεπιδραστικά συστήματα που ζητούν συγκεκριμένη συμπεριφορά από το χρήστη και με τη δημιουργία συνδυασμένων βιομετρικών συστημάτων που μετρούν ταυτόχρονα δύο χαρακτηριστικά (π.χ. πρόσωπο και κίνηση χειλιών κατά την ομιλία).
Μικρότερης σημασίας τεχνολογικά προβλήματα, που σχετίζονται κυρίως με την απόδοση, σε μη ελεγχόμενα περιβάλλοντα μέτρησης, όπως για παράδειγμα οι μεταβλητές συνθήκες φωτισμού που επηρεάζουν τα συστήματα αναγνώρισης προσώπου, ή ο θόρυβος που επηρεάζει τα συστήματα αναγνώρισης φωνής, μένουν να λυθούν από τους κατασκευαστές των υπόλοιπων βιομετρικών τεχνικών. Ας δούμε όμως πέρα από την τεχνολογία πόσο ρόλο παίζει η υλοποίηση αυτής στα βιομετρικά.

Επιθέσεις σε Βιομετρικά – Ζητήματα Υλοποίησης

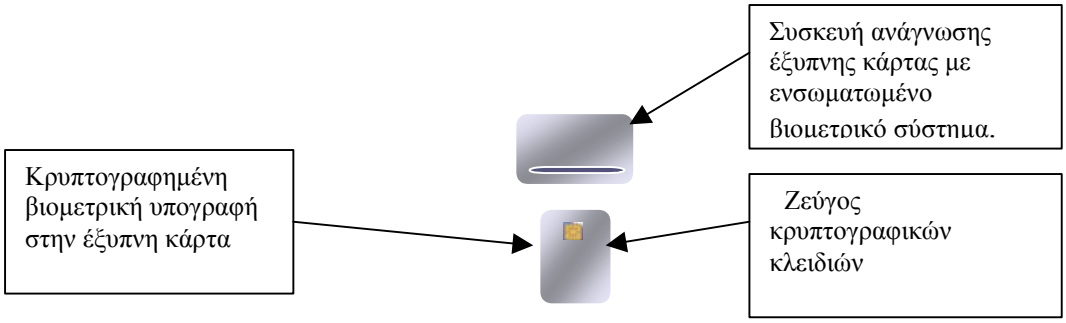
Μερικά σημαντικά ζητήματα κατά την υλοποίηση των βιομετρικών, αφορούν στο αν χρησιμοποιείται κεντρική ή διανεμημένη αποθήκευση των βιομετρικών υπογραφών, στο αν ο αλγόριθμος σύγκρισης είναι ενσωματωμένος ή όχι στο υπόλοιπο σύστημα, στον τρόπο επικοινωνίας των διαφόρων συστατικών του βιομετρικού και στο πως είναι υλοποιημένη η διαδικαστική ασφάλεια για τη χρήση του συστήματος. Λάθος υλοποίηση σε κάποιο από τα παραπάνω, οδηγεί σε ευπάθειες που εκθέτουν το σύστημα σε σημαντικούς κινδύνους.
Παρακάτω αναφέρονται ενδεικτικά μερικές από τις επιθέσεις που βασίζονται σε τέτοιου είδους ευπάθειες.

- **Επιθέσεις υποκλοπής και επανεκπομπής:** η πληροφορία που μεταδίδεται μεταξύ των διαφόρων τμημάτων του βιομετρικού συστήματος, μπορεί να υποκλαπεί και να επαναληφθεί η εκπομπή της. Για παράδειγμα, αν η σύγκριση των βιομετρικών υπογραφών γίνεται σε ένα υποσύστημα εξωτερικό της συσκευής μέτρησης, μπορεί να υποκλαπεί η βιομετρικό δείγμα από το κανάλι επικοινωνίας κατά τη μεταφορά της και να επιχειρηθεί η εκπομπή της μελλοντικά για διείσδυση στο σύστημα.
- **Επιθέσεις αντικατάστασης βιομετρικού δείγματος:** Αν το βιομετρικό δείγμα είναι αποθηκευμένη σε κάποια κεντρική βάση δεδομένων, επίθεση στη βάση και αντικατάσταση της βιομετρικού δείγματος του χρήστη με αυτή του επιτιθέμενου, δίνει πρόσβαση στον δεύτερο, με το όνομα του πρώτου.
- **Επιθέσεις κατά τη στιγμή της εγγραφής:** Φτωχά οργανωμένες διαδικασίες εγγραφής του χρήστη στο σύστημα, μπορεί να οδηγήσουν από την εισαγωγή μιας βιομετρικού δείγματος στο σύστημα με άλλο όνομα, ως και σε διαρροή βιομετρικών στοιχείων λόγω ανεπαρκούς αρχιτεκτονικής ασφάλειας.
- **Επιθέσεις στα επιμέρους συστήματα του βιομετρικού**: Αν το βιομετρικό σύστημα δεν είναι σωστά θωρακισμένο, κάποιος δούρειος ίππος μπορεί να εγκατασταθεί για παράδειγμα στο σύστημα κωδικοποίησης και να αλλοιώσει το αποτέλεσμα της μέτρησης, παράγοντας διαφορετικές βιομετρικές υπογραφές. Αντίστοιχα μπορεί να επηρεαστεί ο αλγόριθμος σύγκρισης.
- **Επιθέσεις από το προσωπικό διαχείρισης του συστήματος:** Όπως σε οποιοδήποτε σύστημα, οι διαχειριστές μπορεί να εκμεταλλευτούν τη δικαιοδοσία τους και να υποκλέψουν βιομετρικά δεδομένα.

Από τα παραπάνω απλοποιημένα παραδείγματα, είναι σαφές ότι η συνολική σχεδίαση του συστήματος πιστοποίησης ταυτότητας του χρήστη πρέπει να γίνεται πολύ προσεκτικά, ώστε να προστατεύονται στο μέγιστο, ευαίσθητα δεδομένα, όπως τα βιομετρικά. Μία ισχυρή πολιτική ασφάλειας πρέπει να θωρακίζει το σύστημα και διέπει τη λειτουργία του. Ας εξετάσουμε όμως ένα σωστά σχεδιασμένο σύστημα πιστοποίησης ταυτότητας, που είναι ικανό να προσφέρει πολύ υψηλά επίπεδα ασφάλειας.

Ενοποιημένα Συστήματα Πιστοποίησης Ταυτότητας

Τα βιομετρικά, δεν αποτελούν αυτόνομη λύση ασφάλειας στον τομέα της πιστοποίησης της ταυτότητας του χρήστη. Πρέπει να συμπληρωθούν και να συμπληρώσουν άλλες τεχνολογίες ασφάλειας, υλοποιώντας ένα ενοποιημένο σύστημα πιστοποίησης ταυτότητας. Ο συνδυασμός κρυπτογραφίας, έξυπνων καρτών και βιομετρικών, υλοποιεί τέτοια συστήματα που όταν είναι σωστά σχεδιασμένα, είναι ευέλικτα και πρακτικά. Ένα τέτοιο σύστημα, το οποίο μπορεί να εφαρμοστεί ευρέως σε ηλεκτρονικές εφαρμογές στο διαδίκτυο παρουσιάζεται στο επόμενο σχήμα.



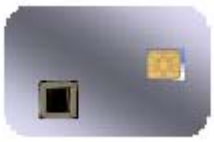
Ενοποιημένο σύστημα πιστοποίησης ταυτότητας

Το βιομετρικό δείγμα αποθηκεύεται συμμετρικά κρυπτογραφημένη στην έξυπνη κάρτα του χρήστη. Η συσκευή ανάγνωσης έξυπνης κάρτας έχει ενσωματωμένο το βιομετρικό σύστημα για καλύτερη προστασία των μεταξύ τους διαύλων επικοινωνίας. Στην έξυπνη κάρτα μπορεί να είναι αποθηκευμένο και ένα ζεύγος κλειδιών για την υλοποίηση ψηφιακών υπογραφών και κρυπτογραφίας. Η πιστοποίηση της ταυτότητας του χρήστη με τη χρήση βιομετρικής, δίνει πρόσβαση στη χρήση του ζεύγους των κλειδιών, μέσω των οποίων η ταυτότητα του χρήστη πιστοποιείται τελικά στο διαδίκτυο, για παράδειγμα με κάποια υλοποίηση του πρωτοκόλλου SSL.
Με τη σχεδίαση αυτή αποφεύγεται η κεντρικοποιημένη αποθήκευση προσωπικών δεδομένων, με όλα τα νομικά της προβλήματα και επιλέγεται ένα μέσο αποθήκευσης ανεπηρέαστο από δικτυακές επιθέσεις. Επιπρόσθετα, η διακίνηση των βιομετρικών υπογραφών, περιορίζεται μεταξύ της συσκευής ανάγνωσης και της έξυπνης κάρτας. Όσο αφορά στις προδιαγραφές της έξυπνης κάρτας και τις απαιτήσεις των βιομετρικών, επικρατεί πλήρης συμβατότητα μεταξύ των δύο, όπως φαίνεται και στον Πινάκα.

Τυπικά Χαρακτηριστικά Μέσου Κόστους Έξυπνης Κάρτας		**Τυπικό Μέγεθος Βιομετρικής Υπογραφής**	
Ασφάλεια	**Μνήμη**	**Δακτυλικό Αποτύπωμα**	**Πρόσωπο**
1 Κρυπτο-επεξεργαστής με δυνατότητα κρυπτογραφίας δημοσίου κλειδιού. 2 Φυσικά και λογικά προστατευμένη μνήμη.	48KB ROM 16KB EEPROM	1KB -> 6 KB	80B -> 4.5KB

Τυπικά χαρακτηριστικά έξυπνων καρτών – απαιτήσεις βιομετρικών

Η πρόοδος άλλωστε στο επίπεδο ασφάλειας των μνημών των έξυπνων καρτών είναι εντυπωσιακή και απαιτεί πολύ εξελιγμένες και δαπανηρές τεχνικές επιθέσεων που σχετίζονται με την σύλληψη της εκπομπής της ηλεκτρομαγνητικής ακτινοβολίας από τον επεξεργαστή της κάρτας. Η ιδανική μάλιστα σχεδίαση του συστήματος απαιτεί όλα τα υποσυστήματα του βιομετρικού, να υλοποιούνται μέσα στην έξυπνη κάρτα.



Βιομετρική έξυπνη κάρτα

Χαρακτηριστικό παράδειγμα, αποτελεί η έξυπνη κάρτα με ενσωματωμένο βιομετρικό αισθητήρα δακτυλικών αποτυπωμάτων. Το προϊόν αυτό έχει ακόμα μερικά λειτουργικά

προβλήματα (κυρίως όσο αφορά στην απόδοση), που αναμένεται να ξεπεραστούν με την πρόοδο στο χώρο της μικροηλεκτρονικής.
Τα παραπάνω, φανερώνουν μία τάση τεχνολογικής δυναμικής στο χώρο, που ωθεί συνεχώς στην υιοθέτηση των ενοποιημένων συστημάτων πιστοποίησης ταυτότητας του χρήστη, από την αγορά. Απαραίτητη, όμως είναι και η αντίστροφη διαδικασία αφομοίωσης των νέων τεχνολογιών από την αγορά, μέσα από επιχειρηματικά σχέδια και στρατηγικές προώθησης.

3.3 ACTIVEX

Το ActiveX είναι ένα πλαίσιο εργασίας για τη τεχνολογία λογισμικού της Microsoft που επιτρέπει στα προγράμματα που τοποθετούνται σε μονάδες, να ενσωματώνονται σε ιστοσελίδες. Ένας προγραμματιστής μπορεί να αναπτύξει ένα πρόγραμμα, να το βάλει σε μια διεπαφή ActiveX, να το συντάξει, και να το τοποθετήσει σε μια σελίδα. Όταν οι τελικοί χρήστες δείχνουν τους browser Ιστού τους (που υποστηρίζει το ActiveX) στις ιστοσελίδες, ο έλεγχος ActiveX θα κατεβάσει και θα προσπαθήσει να εκτελέσει πάνω στη μηχανή τους. Επειδή οι έλεγχοι ActiveX είναι απλά προγράμματα που κατεβάζουν και εκτελούν στο σύστημα ενός χρήστη, δεν μπορούν να κάνουν απολύτως τίποτα που είναι προγραμματισμένοι να κάνουν, συμπεριλαμβανομένης της ζημιάς στο σύστημά σας με την αφαίρεση των κρίσιμων αρχείων. Έπειτα θα περιγραφούν τα μέτρα ασφάλειας με σκοπό να αποτρέψουν τους untrusted ελέγχους ActiveX από την εκτέλεση στις τοπικές μηχανές των χρηστών. Τα μέτρα ασφάλειας με σκοπό να αποτρέψουν τους έμπιστους ελέγχους ActiveX από την καταστροφή ενός συστήματος, δεν υπάρχουν. Οι έλεγχοι ActiveX διαμορφώνουν τη βασική συστατική τεχνολογία του πλαισίου εργασίας ActiveX. Άλλες τεχνολογίες ActiveX όπως τα ActiveX containers και scripts θέτουν επίσης τους κινδύνους ασφάλειας για τον τελικό χρήστη.

Το ActiveX είναι ανεξάρτητο γλώσσας, αλλά με συγκεκριμένη πλατφόρμα. Αυτό σημαίνει ότι αν και οι έλεγχοι ActiveX μπορούν να γραφτούν σε διαφορετικές γλώσσες συμπεριλαμβανομένου του C, C++ VisualBasic, Delphi, ακόμη και Java, έλεγχοι ActiveX μπορούν να εκτελεσθούν μόνο σε μια 32-bit πλατφόρμα Windows. Οι browsers Ιστού που υποστηρίζουν ActiveX δεν φροντίζουν σε ποια γλώσσα γράφεται ο έλεγχος εφ' όσον ο κώδικας αντικειμένου είναι προσιτός μέσο μιας διεπαφής ActiveX. Αντίθετα με την Java, οι έλεγχοι ActiveX δεν είναι φορητοί σε διαφορετικές αρχιτεκτονικές μηχανών. Στην πραγματικότητα, ακόμη και τα applets της Java μέσα σε έναν έλεγχο ActiveX θα εκτελέσουν μόνο στις μηχανές Win32 (μερικές φορές ονομάζονται μηχανές Wintel) επειδή το ActiveX είναι μηχανή συγκεκριμένου κώδικα αντικειμένου.

Και οι τρεις τεχνολογίες ActiveX θέτουν σοβαρές ανησυχίες ασφάλειας για τον τελικό χρήστη. Οι χρήστες πρέπει να γνωρίζουν αυτούς τους κινδύνους πριν κατεβάσουν και εκτελέσουν το περιεχόμενο ActiveX. Με οποιαδήποτε ενεργό εφαρμογή, η κατάλληλη θέση ασφάλειας που υποθέτει, θα εξαρτηθεί από τον κίνδυνο για τα προτερήματα που θέτει το ενεργό περιεχόμενο. Στην περίπτωση των ελέγχων ActiveX, τα προτερήματα σε κίνδυνο περιλαμβάνουν όλα τα αρχεία στον τοπικό σκληρό δίσκο της μηχανής πελατών, καθώς επίσης και οποιαδήποτε συστήματα αρχείων κοινά πέρα από τους δικτυωμένους υπολογιστές. Δεδομένου ότι οι έλεγχοι ActiveX έχουν τη δυνατότητα να εκτελέσουν οποιοδήποτε άλλο πρόγραμμα για έναν υπολογιστή, οι έλεγχοι ActiveX μπορούν να χρησιμοποιηθούν για να πλαστογραφήσουν το ηλεκτρονικό ταχυδρομείο, για να ελέγξουν τη χρήση Ιστού, για να στείλουν τα αρχεία μέσο του Διαδικτύου, για να γράψουν τα αρχεία, και για να αλληλεπιδράσουν με άλλα προγράμματα. Για να αξιολογήσετε τον κίνδυνό σας όταν χρησιμοποιείτε ActiveX και άλλων μορφών ενεργού περιεχομένου που κατεβαίνουν από το Διαδίκτυο, αποφασίστε αρχικά ποια προτερήματα διατρέχουν τον κίνδυνο. Εάν ο υπολογιστής που χρησιμοποιείτε για να σερφάρετε στο Διαδίκτυο και να κατεβάσετε τους ελέγχους ActiveX είναι ένας αυτόνομος υπολογιστής που δεν εξυπηρετεί καμία κρίσιμη λειτουργία, μπορεί να είναι δυνατό να εκτελεσθεί το ενεργό περιεχόμενο χωρίς φόβο. Αφ' ετέρου, εάν σερφάρετε στο δίκτυο από την εργασία, πρέπει να ξανασκεφτείτε την εκτέλεση

των ενεργών εφαρμογών των οποίων δεν ξέρετε ή δεν εμπιστεύεστε τη συμπεριφορά τους. Η απάντηση της Microsoft στην εξέταση των προβλημάτων ασφάλειας σε χρήση της τεχνολογίας ActiveX είναι το Authenticode. Το Authenticode μπορεί να χρησιμοποιηθεί για να αποτρέψει την αυτόματη εκτέλεση των μη-εμπιστευτικών ελέγχων ActiveX.

3.4 AUTHENTICODE: ΚΑΘΙΕΡΩΣΗ ΕΜΠΙΣΤΟΣΥΝΗΣ ΓΙΑ ACTIVEX

Το Authenticode είναι μια τεχνολογία της Microsoft η οποία εμποδίζει τους καταστροφικούς κωδικούς από τις πλατφόρμες των Windows. Το Authenticode μπορεί να παρέχει δύο ελέγχους πριν κάνει τους ελέγχους ActiveX:

- μπορεί να ελέγξει ποιος υπογράφει τον κώδικα,
- μπορεί να ελέγξει εάν έχουν αλλάξει τον κώδικα από τη στιγμή που υπογράφηκε.

Είναι σημαντικό να γίνει ένας διαχωρισμός μεταξύ του συντάκτη του κώδικα και του προσώπου που υπογράφει τον κώδικα επειδή μπορεί να μην είναι το ίδιο πρόσωπο. Μια ψηφιακή υπογραφή αντιπροσωπεύει μόνο μια επικύρωση του κώδικα. Προτού ένα άτομο ή μια εμπορική εταιρία υπογράψει τον κώδικα, κάθε ένας πρέπει να κάνει αίτηση για να λάβει ένα πιστοποιητικό εκδοτών λογισμικού (SPC) σε μια από τις διάφορες Αρχές Πιστοποίησης (ΑΠς) που εξυπηρετούν αυτήν την λειτουργία. Το VeriSign είναι το πιο γνωστό παράδειγμα μιας ΑΠ που παρέχει SPCS.

Η διαδικασία απαιτεί από τον εκδότη λογισμικού να παράγει ένα δημόσιο/ιδιωτικό ζευγάρι κλειδιών που χρησιμοποιείται για να υπογράψει το λογισμικό. Το ιδιωτικό κλειδί παραμένει μυστικό στον εκδότη, το δημόσιο κλειδί διανέμεται με κάθε πιστοποιητικό. Ο ρόλος της ΑΠ είναι να γεφυρωθεί το χάσμα εμπιστοσύνης μεταξύ του τελικού χρήστη και του εκδότη λογισμικού. Καθένας μπορεί να παράγει ένα δημόσιο/ιδιωτικό ζευγάρι κλειδιών και μπορεί να υποθέσει οποιαδήποτε ταυτότητα, απλά ελέγχοντας ότι το υπογεγραμμένο έγγραφο δεν παρέχει οποιαδήποτε διαβεβαίωση ως προς την ταυτότητα του εκδότη. Το CA παρέχει την ταυτότητα ελέγχοντας τους τελικούς χρήστες και θα επικυρώσει τις ταυτότητες του ατόμου ή της εταιρίας. Υπό τον όρο ότι οι έλεγχοι εγκρίνονται, της ΑΠ θα υπογράψει το δημόσιο κλειδί του εκδότη λογισμικού και θα επιστρέψει ένα αντίγραφο από αυτό στον εκδότη υπό μορφή πιστοποιητικού εκδοτών λογισμικού. Με την υπογραφή του SPC, η ΑΠ επικυρώνει την ταυτότητα του εκδότη λογισμικού που είναι συνδεδεμένος με το δημόσιο κλειδί.

Μόλις ο εκδότης λογισμικού λάβει το πιστοποιητικό από την ΑΠ, μπορεί να χρησιμοποιήσει το ιδιωτικό κλειδί του για να υπογράψει οποιοδήποτε κώδικα λογισμικού που θα διανείμει, ανεξάρτητα από ποιος το έγραψε. Για να παρέχει τους ελέγχους ακεραιότητας του λογισμικού, ο εκδότης λογισμικού παράγει one-way hash του κώδικα, ο οποίος δεν μπορεί να αντιστραφεί. Δηλαδή ο κώδικας δεν μπορεί να δημιουργηθεί ξανά από το προκύπτον hash, γνωστό ως digest. Μια άλλη ιδιότητα της hash λειτουργίας είναι ότι είναι επαναλαμβανόμενη. Εφ' όσον δεν αλλάζουν κανένα από τα κομμάτια στον κώδικα, το τρέξιμο του ίδιου κώδικα μέσο της ίδιας hash λειτουργίας θα παράγει πάντα την ίδια digest. Αυτή η ιδιοκτησία χρησιμοποιείται για να ελέγξει τον κώδικα όταν έχει ληφθεί από τον τελικό χρήστη. Μόλις δημιουργηθεί η digest, ο εκδότης λογισμικού μπορεί να υπογράψει ψηφιακά την digest που παράγεται για ένα ιδιαίτερο πρόγραμμα. Η υπογεγραμμένη digest συνδυάζεται με το SPC σε έναν φραγμό υπογραφών που είναι συνδεμένος με το λογισμικό.

Οι εργασίες Authenticode, υποθέτουν ότι ένας εκδότης λογισμικού έχει δημιουργήσει έναν φραγμό υπογραφών που συνδέεται με το τμήμα λογισμικού, ο τελικός χρήστης του τμήματος λογισμικού μπορεί να ελέγξει την ταυτότητα του εκδότη και την ακεραιότητά του συστατικού όταν το κατεβάζει. Όταν το λογισμικό κατεβαίνει στη μηχανή του τελικού χρήστη, ο browser μπορεί να αποσυνδέσει το φραγμό υπογραφών και να εκτελέσει ελέγχους χρησιμοποιώντας Authenticode. Για να καθορίσει την ταυτότητα του υπογράφοντος, ο browser περνά σε δύο στάδια διαδικασίας. Στην αρχή, ο browser θα εξετάσει το συνημμένο SPC για να καθορίσει εάν έχει υπογραφεί από μια εμπιστευμένη Αρχή Πιστοποίησης. Οι browsers έχουν μια λίστα των "έμπιστων" ΑΠς μέσα σε αυτούς. Εάν η υπογραφή ταιριάξει με την αντίστοιχη δημόσια

βασική υπογραφή CA που αποθηκεύεται στον browser, κατόπιν ο browser θα δεχτεί το δημόσιο κλειδί στο SPC καθώς ανήκει στην ταυτότητα που ονομάζεται στο πιστοποιητικό.

Το δεύτερο βήμα χρησιμοποιεί το δημόσιο κλειδί του εκδότη λογισμικού για να ελέγξει την υπογεγραμμένη digest και να καθορίσει με βεβαιότητα εάν ο εκδότης λογισμικού υπέγραψε τον κώδικα που έχει κατεβάσει. Υπό τον όρο ότι ο έλεγχος ήταν επιτυχής, ο browser θα επιδείξει το ισοδύναμο SPC. Αυτή η επίδειξη παρέχει τη θετική διαβεβαίωση τελικών χρηστών ότι ο εκδότης πράγματι επικύρωσε τον κώδικα.

Ο άλλος έλεγχος που παρέχεται από το Authenticode καθορίζει εάν το ενεργό περιεχόμενο άλλαξε κατά τη μεταφορά. Ο browser θα αναπαράγει την digest του κινητού κώδικα χρησιμοποιώντας τον ίδιο hash αλγόριθμο. Εάν η αναπαραγμένη digest ταιριάζει με την υπογεγραμμένη digest που στέλνεται στον κώδικα, ο τελικός χρήστης θα έχει τη θετική διαβεβαίωση ότι ο κώδικας δεν πειράχτηκε από το χρόνο που υπογράφεται έως ότου εκτελείται στη μηχανή του τελικού χρήστη. Αυτή η ολόκληρη διαδικασία είναι συγγενής στον έλεγχο της σφραγίδας σε έναν φάκελο επιστολών για να εξασφαλίσει ότι δεν έχει πειραχτεί κατά τη διάρκεια της διέλευσης και έπειτα γίνεται έλεγχος της υπογραφής στην επιστολή για να ελέγξει ποιος το έστειλε.

Τα Authenticode 2.0 έχουν δύο νέα χαρακτηριστικά γνωρίσματα για να παρέχουν πρόσθετη προστασία τελικών χρηστών. Κατ' αρχήν, οι υπογραφές εκδοτών λογισμικού θα είναι έτσι ώστε οι τελικοί χρήστες να μπορούν να καθορίσουν εάν οι υπογραφές έγιναν, ενώ το SPC ίσχυε ακόμα. Δεδομένου ότι οι ΑΠ απαιτούν ανανέωση, χαρακτηριστικά σε ετήσια βάση, η χρονοσφράγιση μπορεί να χρησιμοποιηθεί για να επιβάλει την ανανέωση. Εκτός από τη υποστήριξη εισοδήματος για την ΑΠ, πρέπει οι εκδότες λογισμικού να καλύψουν τις ελάχιστες απαιτήσεις που χορηγούνται στο SPC κάθε έτος. Εάν μετά τη χορήγηση του πιστοποιητικού, ένας εκδότης λογισμικού διανέμει καταστροφικό κώδικα, η ΑΠ που πιστοποίησε τον εκδότη έχει το δικαίωμα να μην ανανεώσει το πιστοποιητικό. Μετά, οποιοδήποτε συστατικό που ο εκδότης λογισμικού υπογράφει θα περιέχουν μια χρονοσφράγιση η οποία δεν θα ισχύει σύμφωνα με το ληγμένο πιστοποιητικό. Ο browser του τελικού χρήστη θα σημειώσει την άκυρη χρονοσφράγιση και θα προειδοποιήσει το χρήστη πριν εκτελέσει το λογισμικό. Αυτό είναι το πρότυπο, που χρησιμοποιείται από πολλά διαφορετικά σχέδια χορήγησης αδειών σε άλλες βιομηχανίες, όπως στα ιατρικά και νομικά επαγγέλματα. Η βασική διαφορά είναι ότι ελέγχεται μόνο η ταυτότητα του εκδότη. Φυσικά, εάν ο εκδότης λογισμικού έχει μια ιστορία διανομής του καταστροφικού κώδικα, θα υπάρχει σοβαρός λόγος να μην επανεκδώσει το πιστοποιητικό. Αυτό είναι επίσης το πρότυπο που χρησιμοποιείται από τους πολίτες της U.S. που συνεχίζουν να ανανεώνουν τις άδειες των κρατικών οδηγών τους κάθε λίγα χρόνια. Φυσικά, στις Ηνωμένες Πολιτείες, τα κράτη συνεργάζονται για να εξασφαλίσουν ότι όταν σε ένα κράτος μια άδεια οδήγησης έχει απορριφθεί λόγω ποινικού αδικήματος, δεν θα γίνει δεκτή σε ένα άλλο κράτος. Αυτή τη περίοδο, είναι άγνωστο εάν η ΑΠ θα μοιραστεί τα στοιχεία για να αποτρέψει έναν απορριφθέντα εκδότη λογισμικού από τη λήψη ενός πιστοποιητικού από μια άλλη ΑΠ.

Το δεύτερο νέο χαρακτηριστικό γνώρισμα που παρέχουν τα Authenticode 2.0 (Authenticode 1.0) είναι η δυνατότητα να ακυρωθούν τα πιστοποιητικά. Ένα πιστοποιητικό εκδοτών λογισμικού μπορεί να ακυρωθεί από την ΑΠ, εάν ο εκδότης παραβιάζει τον κώδικα υπογράφοντας τη συμφωνία που έκανε με την ΑΠ. Οι περισσότερες συμφωνίες απαιτούν από τους εκδότες λογισμικού να μην διανείμουν σκόπιμα τον καταστροφικό κώδικα. Εάν γίνει γνωστό ότι ένας εκδότης λογισμικού έχει διανείμει σκόπιμα τον καταστροφικό κώδικα, η ΑΠ μπορεί όχι μόνο να αρνηθεί να ανανεώσει το πιστοποιητικό, αλλά και να το ακυρώσει αμέσως. Ο Internet Explorer θα ελέγξει το πιστοποιητικό πριν κατεβάσει το περιεχόμενο για να εξασφαλίσει ότι δεν έχει ακυρωθεί. Εάν ένας εκδότης θεωρεί ότι το ιδιωτικό κλειδί του έχει εκτεθεί, ο εκδότης μπορεί να ζητήσει να ακυρωθεί το πιστοποιητικό του. Αυτή η ακύρωση ενός πιστοποιητικού πρέπει να διαδοθεί ευρέως στους browsers των χρηστών. Η ΑΠ μπορεί να εξυπηρετήσει το ρόλο της διάδοσης αυτών των πληροφοριών που λαμβάνει είτε από τους τελικούς χρήστες, είτε από τους εκδότες για τα πιστοποιητικά που πρέπει να ακυρωθούν. Εφ' όσον οι browsers διαμορφώνονται για να ενημερώσουν περιοδικά τους καταλόγους ακυρωμένων πιστοποιητικών, ο τελικός χρήστης θα προστατευθεί από τα

τμήματα λογισμικού που υπογράφονται από τους προγραμματιστές που έχουν ακυρώσει τα πιστοποιητικά τους.

Όπου το Authenticode αποτυγχάνει στερούμενης της ασφάλειας Το σύνολο και η έννοια που το Authenticode παρέχει, είναι η επικύρωση της ταυτότητας του προσώπου που υπέγραψε τον έλεγχο και η εξέταση για ακεραιότητα του λογισμικού ώστε να εξασφαλίσει ότι δεν έχουν αλλάξει από τη στιγμή που υπογράφηκαν. Άρα, τι παρέχουν αυτοί οι δύο έλεγχοι και πού υπολείπονται; Εάν ο ActiveX εκδότης υπογράψει το συστατικό, ο τελικός χρήστης ξέρει ποιο είναι εκείνο το πρόσωπο και εάν το συστατικό έχει πειραχτεί αφότου υπογράφηκε. Ωστόσο, η υπογραφή δεν παρέχει καμία διαβεβαίωση ότι ο έλεγχος δεν θα συμπεριφερθεί καταστροφικά. Η τεχνολογία Authenticode λειτουργεί απλώς σε ένα πρότυπο εμπιστοσύνης. Δηλαδή εάν εμπιστεύεστε αυτόν που υπογράφει τον κώδικα, κατόπιν, αφήνετε τον έλεγχο να κάνει οτιδήποτε στη μηχανή σας. Εάν δεν εμπιστεύεστε τον εκδότη του ελέγχου, απορρίπτετε την εκτέλεσή της. Δυστυχώς, δεν υπάρχει κανένα μέσο έδαφος για να αφήσει τον έλεγχο να εκτελέσει σε ένα περιορισμένο περιβάλλον όπου μπορεί πρώτα να παρατηρηθεί, πριν έχει πλήρη πρόσβαση. Μόλις εμπιστευθείτε τον έλεγχο να τρέξει στη μηχανή σας, θα έχει ελεύθερο να κάνει οποιεσδήποτε καταστροφικές δραστηριότητες όπως να σβήσει το σκληρό δίσκο σας ή να στείλει τα αντίγραφα των αρχείων σας σε διαφορετικούς ιστοχώρους. Αντίθετα από τα μη έμπιστα applets της Java, που περιορίζονται στα "sandbox" (θα δούμε παρακάτω) οι έλεγχοι ActiveX έχουν τη δύναμη και το προνόμιο οποιουδήποτε προγράμματος που τρέχει στη μηχανή σας.

3.5 JAVA

Η Java είναι ένα object-oriented πρόγραμμα γλώσσας από την Sun Microsystems, μια εταιρία η οποία είναι γνωστή για την υψηλή ποιότητα σταθμών εργασίας. Διαμορφωμένη μετά από το C ++, η γλώσσα της Java είχε ως σκοπό να είναι μικρή, απλή, και φορητή στις πλατφόρμες και τα λειτουργικά συστήματα, και στην πηγή και στο δυαδικό επίπεδο.

Από την πλευρά ενός προγραμματιστή, η Java προσφέρει τον αληθινό object-oriented προγραμματισμό, παρά τις επεκτάσεις σε μια γλώσσα. Στον Ιστό surfer, οι σελίδες που ενσωματώνονται με τα applets της Java ενεργοποιούνται όταν τις έχουμε φέρει στην οθόνη. Τα applets της Java κάνουν τον Ιστό μια εμπειρία, παρά ένα χόμπι. Οι επιχειρήσεις υιοθετούν τη Java γρήγορα για διάφορους λόγους. Κατ' αρχήν, είναι μια αληθινή γλώσσα πολυ-πλατφορμών. Αυτό σημαίνει ότι τα προγράμματα της Java που είναι γραμμένα σε μια πλατφόρμα (πχ το Unix) θα τρέξουν και σε άλλη (πχ Windows). Δεύτερον, η δυνατότητα να τρέχουν τα applets της Java στις μηχανές πελατών, προσθέτει νέα στρώματα της λειτουργίας στον Ιστό. Οι πρακτικές επιχειρησιακές εφαρμογές, όπως η διεξαγωγή συναλλαγών, μπορούν να προγραμματιστούν μια φορά και να τρέξουν στις μηχανές πελατών οπουδήποτε, ανεξάρτητα από την πλατφόρμα πελατών. Τρίτον, η Java είχε ως σκοπό να είναι μια πλήρης γλώσσα που τρέχει στα ενσωματωμένα συστήματα (παραδείγματος χάρη CardJava - ένα υποσύνολο της γλώσσας της Java- ενσωματώθηκε στις έξυπνες κάρτες). Αυτό το είδος cross-platform μεταφερσιμότητας, κάνει τη Java μια πολύ ενδιαφέρουσα γλώσσα ανάπτυξης για την επιχείρηση.

Η βιασύνη για ανάπτυξη και για τρέξιμο της Java έχουν γίνει από τον Ιστό. Επειδή τα προγράμματα της Java είναι, σύμφωνα με JavaSoft, “write once, run anywhere”, ο Ιστός έγινε το ιδανικό περιβάλλον για να διανείμει τα προγράμματα της Java, αποκαλούμενα applets της Java, και να αλλάξει πλήρως τη φύση των εγγράφων HTML. Για να εξετάσουν αυτές τις ανησυχίες ασφάλειας, δημιούργησαν ένα πρότυπο ασφάλειας, αποκαλούμενο μερικές φορές sandbox της Java, από το οποίο οποιοδήποτε untrusted applet της Java πρέπει να μένει εκεί. Το Sandbox αποτρέπει τα untrusted applets της Java για πρόσβαση των ευαίσθητων πόρων συστημάτων. Όπως οποιοδήποτε άλλο πρόγραμμα, οι εφαρμογές της Java έχουν απεριόριστη πρόσβαση στους πόρους συστημάτων. Οι εφαρμογές της Java δεν τηρούν τα sandbox της Java. Κατά συνέπεια, οι εφαρμογές της Java μπορούν να γραφτούν για να εκτελέσουν οποιοδήποτε αριθμό λειτουργιών που στέλνονται στην παραδοσιακή ανάπτυξη λογισμικού. Από αυτή την άποψη, οι εφαρμογές της Java είναι όπως το C και τα

προγράμματα C++ ακόμη και οι έλεγχοι ActiveX. Δίνεται πλήρως η εντολή για να εκτελέσουν οποιαδήποτε προγραμματισμένη λειτουργία. Τα applets της Java, αφ' ετέρου, που ενσωματώνονται στα έγγραφα HTML, θα εκτελέσουν μόνο από τους browsers Ιστού, και πρέπει να εκτελέσουν μέσα στα όρια sandbox της Java.

Το Sandbox της Java είναι το πρότυπο ασφάλειας της Java. Ο όρος "Sandbox" χρησιμοποιείται για να αντιπροσωπεύσει μια περιοχή στην οποία ένα applet της Java μπορεί να παίξει, αλλά να μην δραπετεύσει. Παραδείγματος χάρη, το sandbox αποτρέπει τα applets από την εκτέλεση οποιουδήποτε αρχείου που εισάγει/εξάγει λειτουργίες όπως η ανάγνωση ή το γράψιμο στο σύστημα αρχείων. Η μόνη σύνδεση δικτύων που επιτρέπεται για τα applets της Java είναι η σύνδεση στον υπολογιστή υπηρεσίας από τον οποίο προήλθε το applet. Το Sandbox της Java αντιπροσωπεύει μια τεχνολογική λύση για παρεμπόδιση της καταστροφικής συμπεριφοράς του κώδικα και επιβάλλει τρεις τεχνολογίες: η επικύρωση bytecode, ο φορτωτής κατηγορίας applet, και ο διαχειριστής ασφάλειας. Οι τρεις τεχνολογίες λειτουργούν μαζί, για να εμποδίσουν ένα applet να κάνει κατάχρηση των περιορισμένων προνομίων της. Επειδή κάθε μια παρέχει μια διαφορετική λειτουργία, μια ρωγμή σε κάποια, μπορεί να σπάσει ολόκληρο το sandbox. Για αυτό το λόγο, όχι μόνο πρέπει το σχέδιό τους να είναι ακλόνητο, αλλά και οι εφαρμογές τους πρέπει να μην έχουν κανένα ψεγάδι. Η πολυπλοκότητα των λειτουργιών που κάθε τεχνολογία παρέχει, κάνει μια σωστή εφαρμογή να επιτυγχάνει ένα δύσκολο στόχο. Τα προβλήματα ασφάλειας της Java, είναι άμεσο αποτέλεσμα των ρωγμών στην εφαρμογή αυτών των λειτουργιών.

Η εμφάνιση της υπογραφής applet έχει αλλάξει τους περιορισμούς που επιβάλλονται στα υπογεγραμμένα applets της Java. Αυτό είναι η επόμενη ενσωμάτωση της ασφάλειας της Java: η υπογραφή κώδικα. Το πρότυπο ασφάλειας sandbox πολύ απλά και αυστηρά εμποδίζει τα κατεβασμένα από το δίκτυο applets της Java να χρησιμοποιήσουν ευαίσθητες υπηρεσίες συστημάτων. Η πολιτική ασφάλειας για τα μη έμπιστα applets είναι γραπτή. Εάν τα applets κατεβάζονται από μια σύνδεση δικτύων, πρέπει να τηρήσουν τους ακριβείς περιορισμούς sandbox. Εάν τα applets φορτώνονται από το τοπικό σύστημα αρχείων, είναι εντελώς ελεύθερα στο σύστημα, όπως με τις εφαρμογές της Java. Οι περιορισμοί στις υπηρεσίες συστημάτων που τα δικτυωμένα applets της Java μπορούν να χρησιμοποιήσουν, περιορίζουν τις εφαρμογές για τις οποίες τα applets της Java μπορούν να προγραμματιστούν. Παραδείγματος χάρη, οποιαδήποτε εφαρμογή, όπως ένας επεξεργαστής λέξεων που απαιτεί το αρχείο I/O, δεν μπορεί να προγραμματιστεί σε ένα applet της Java. Η πολιτική ασφάλειας για τα δικτυωμένα applets ισχύει εξίσου για όλα τα applets, ανεξάρτητα από την πηγή. Έτσι, ένα applet κατεβασμένο από ένα εταιρικό σύστημα ενδοδικτύου δεν δίνει άλλα προνόμια πρόσβασης αρχείων από ένα applet που κατεβάζεται από μια untrusted πηγή Διαδικτύου. Αν και αυτό είναι πράγματι μια συντηρητική πολιτική ασφάλειας, υπάρχει σύγχυση σε πολλούς προγραμματιστές της Java εξαιτίας της ανικανότητας του applets προγράμματος να εκτελέσει χρήσιμες διαδικασίες λόγω της δυαδικής πολιτικής ασφάλειας.

Για να παρέχει μεγαλύτερη ευελιξία ώστε να τρέξουν τα applets της Java σε ένα έμπιστο περιβάλλον, η JavaSoft παρέχει τη δυνατότητα να υπογραφούν τα applets χρησιμοποιώντας crypto API που απελευθερώνεται με το Java Developers Kit version 1.1 (JKD 1.1). Το Crypto API παρέχει τη δυνατότητα να υπογραφούν ψηφιακά τα applets με την απόδειξη της ταυτότητας. Πρέπει να είναι σε θέση να επιτρέψει την πρόσβαση applets στους πόρους συστημάτων βασισμένο στο ποιος τους υπογράφει. Παραδείγματος χάρη, τα applets που διανεμήθηκαν από ένα εταιρικό ενδοδίκτυο θα μπορούσαν να υπογραφούν από την εταιρική αρχή που είναι αρμόδια για την έγκριση της εσωτερικής ανάπτυξης applet. Οι browsers για τους χρήστες της επιχείρησης θα διαμορφώνονταν έπειτα για να δεχτούν, να εκτελέσουν, και να παρέχουν ενδεχομένως τους πλήρεις πόρους συστημάτων σε οποιοδήποτε applet που υπογράφονται από την οριζόμενη αρχή υπογραφών. Αφ' ετέρου, αυτή η μέθοδος πολιτικής ασφαλείας, είναι παρόμοια με την επιβολή ασφάλειας της Microsoft Authenticode. Είναι μια πολιτική βασισμένη στην εμπιστοσύνη και στην ανθρώπινη κρίση.

Στο JDK 1.1, η πολιτική ασφάλειας για την εκτέλεση των applets, είναι άσπρο και μαύρο. Δηλαδή στα applets της Java που ανακτώνται από τις ενσωματωμένες κατηγορίες δίνονται ελεύθερα στο σύστημα, ενώ τα untrusted applets της Java που κατεβάζονται από το δίκτυο

κρατιούνται σε μια ομάδα μέσα στο sandbox. Μόλις ελεγχθεί η υπογραφή ενός applet, δίνεται στο applet πλήρης περιορισμός των πόρων συστημάτων. Ωστόσο, αυτό δεν αλλάζει το γραπτό πρότυπο της ασφάλειας. Αυτή η γραπτή πολιτική θα αλλάξει με τις νεώτερες εκδόσεις JDK που υποστηρίζουν τον έλεγχο πρόσβασης. Έτσι, ανάλογα με το επίπεδο εμπιστοσύνης που ορίζεται σε ένα applet, θα χορηγηθούν διαφορετικά επίπεδα πρόσβασης στους πόρους συστημάτων.

3.6 CORBA

Η παροχή της διαλειτουργικότητας μεταξύ των εφαρμογών και η σύνδεση πολλών συστημάτων αντικειμένου που βρίσκονται σε διαφορετικές μηχανές στα ετερογενή διανεμημένα περιβάλλοντα, είναι μια θεμελιώδης απαίτηση στο ηλεκτρονικό επιχειρείν. Το Common Object Request Broker Architecture (CORBA) είναι ένα διανεμημένο υπολογιστικό περιβάλλον αντικειμένου που παρέχει έναν μηχανισμό από τον οποίο τα ετερογενή αντικείμενα λογισμικού μπορούν να ζητήσουν και να λάβουν απαντήσεις μέσο της χρήσης των δημόσιων ονομάτων και των διεπαφών. Η CORBA είναι μια ανοικτή αρχιτεκτονική που τυποποιείται από τη Object Management Group (OMG). Στο CORBA, οι πελάτες και τα αντικείμενα αλληλεπιδρούν χρησιμοποιώντας ένα ή περισσότερα ORBs (Object Request Brokers). Ένα αντικείμενο είναι μια αναγνωρίσιμη οντότητα όπως ένας κεντρικός υπολογιστής που παρέχει υπηρεσίες σε άλλους πελάτες. Τα ORBs μπορούν να έχουν πρόσβαση σε έναν κατάλογο των υπηρεσιών που παρέχονται από διάφορα αντικείμενα στο σύστημα, και να καθορίσουν τα καταλληλότερα μέσα για πρόσβαση. Κατά συνέπεια, η ενεργοποίηση αντικειμένου θέσης εφαρμόζεται στο CORBA. Ένας πελάτης CORBA δεν έχει πρόσβαση στις ίδιες πληροφορίες με έναν ORB. Εντούτοις, ξέρει πώς να έρθει σε επαφή με έναν τουλάχιστον τοπικό ORB στον οποίο υποβάλλει το αίτημα, το οποίο μπορεί έπειτα να περάσει μέσο ενός ή περισσότερων ORBS. Οι κοινές υπηρεσίες αντικειμένου όπως η ανακάλυψη των διαθέσιμων υπηρεσιών και της παροχής ασφάλειας αντικειμένου είναι διαθέσιμες στα διανεμημένα προγράμματα αντικειμένου μέσο των περιοχών ανεξάρτητων διεπαφών. Οι προδιαγραφές υπηρεσιών είναι διαθέσιμες για την ονομασία, τις εμπορικές συναλλαγές, τη διαχείριση κύκλου της ζωής, την ασφάλεια, τις συναλλαγές, την ανακοίνωση γεγονότος, τον έλεγχο συνεργασίας, τις ερωτήσεις, τις ιδιότητες, και τη χορήγηση αδειών. Οι κοινές εγκαταστάσεις είναι vertically και horizontally oriented, αλλά αντίθετα από τις υπηρεσίες αντικειμένου είναι προσανατολισμένες προς τις εφαρμογές τελικών χρηστών. Ένα παράδειγμα μιας κοινής δυνατότητας αντικειμένου είναι DDCF (Distributed Document Component Facility) που είναι βασισμένο σε OpenDoc. Το DDCF επιτρέπει την παρουσίαση και την ανταλλαγή των αντικειμένων βασισμένων σε ένα πρότυπο εγγράφων. Οι διεπαφές εγγράφων είναι προσανατολισμένες προς τις συγκεκριμένες περιοχές εφαρμογής. Τα παραδείγματα διεπαφών εγγράφων περιλαμβάνουν RFPs (Request for Products) από το OMG όπως τα PDM (Product Data Management) για την κατασκευή, και τα RFPs για τις τηλεπικοινωνίες, τα ιατρικά, και τα οικονομικά. Δεδομένου ότι οι διεπαφές εγγράφων είναι συγκεκριμένη εφαρμογή, δεν είναι διαθέσιμο κανένα πρότυπο από OMG. Εντούτοις, οι μελλοντικές τυποποιήσεις OMG μπορούν να περιλάβουν τις ευρέως καθορισμένες υπηρεσίες για τις συγκεκριμένες περιοχές εφαρμογής. Μια σημαντική εργασία που απαιτείται για το CORBA στο μέλλον, είναι να καθιερωθεί μια αρχιτεκτονική ασφάλειας που εφαρμόζεται σε επίπεδο αντικειμένου. Η ασφάλεια συστημάτων όπως αυτή που παρέχεται από DSSA (Distributed Systems Security Architecture) και η ασφάλεια μεταξύ RPCs (Remote Procedure Calls) έχουν προταθεί. Εντούτοις, είναι απαραίτητο να αναπτυχθούν οι μηχανισμοί ασφάλειας για την επικύρωση και τον έλεγχο πρόσβασης για τα αντικείμενα που έχουν διαφορετικές απαιτήσεις ασφάλειας. Από τη δημιουργία πελατών και αντικειμένου, η κατανομή, και η καταστροφή γίνονται δυναμικά σε CORBA, οι πληροφορίες ασφάλειάς τους πρέπει επίσης να παραχθούν και να ρυθμιστούν δυναμικά.

4 ΑΣΦΑΛΕΙΑ XML

Η γλώσσα XML αποτελεί απόγονο της γλώσσας Standard General Markup Language (SGML), η οποία χρησιμοποιείται από το 1986 σε διεθνές επίπεδο ως πρότυπο για τον προσδιορισμό ηλεκτρονικών δεδομένων.

Οι λόγοι που οδήγησαν στην ανάπτυξη της γλώσσας XML είναι πολλοί. Η γλώσσα αυτή αφαίρεσε πολλές από τις πολυπλοκότητες της αρχικής γλώσσας SGML διατηρώντας όμως τα αρχικά πλεονεκτήματα:

- Η XML είναι μια γενικευμένη markup γλώσσα η οποία επιτρέπει σε αυτόν που την χρησιμοποιεί να προσδιορίσει τη δική του συλλογή από tags.
- Τα έγγραφα της XML μπορούν να αυτό-προσδιοριστούν. Αυτό σημαίνει ότι ένα έγκυρο έγγραφο περιέχει τα δικά του σύνολα κανόνων στους οποίους τα έγγραφα πρέπει να υπακούσουν.
- Τα έγγραφα της XML μπορούν να ελεγχθούν για την εγκυρότητα τους. Αυτό μπορεί να γίνει με τη χρήση ενός προγράμματος (XML validator) το οποίο ελέγχει εάν το έγγραφο είναι δομημένο σύμφωνα με τους κανόνες που περιγράφονται στο DTD αρχείο.

Σε αυτό το σημείο πρέπει να επισημάνουμε ότι η XML δεν είναι μόνο ένα «υποκατάστατο» της HTML για μεταφορά πληροφορίας στο διαδίκτυο. Θα παραθέσουμε μερικούς από τους αρχικούς σκοπούς της ομάδας που ανέπτυξε την XML για να γίνει κατανοητή η προτιθέμενη χρήση της.

- Η XML πρέπει να είναι απευθείας χρησιμοποιήσιμη μέσω του Διαδικτύου. Αυτό σημαίνει ότι ο καθορισμός της καινούργιας γλώσσας πρέπει να απλοποιεί την ήδη υπάρχουσα δομή της SGML. Επιπλέον η καινούργια γλώσσα πρέπει να λάβει υπόψη της τις ανάγκες των εφαρμογών οι οποίες τρέχουν σε ένα περιβάλλον δικτύου.
- Η XML πρέπει να υποστηρίζει ένα ευρύ πλήθος εφαρμογών. Αυτό σημαίνει ότι η xml δεν προτίθεται μόνο ως γλώσσα διαδικτύου, αλλά ως μια γλώσσα η οποία μπορεί να χρησιμοποιηθεί για μια ευρεία κλίμακα υλικού (software), η οποία θα μπορεί να ποικίλει από απλούς κειμενογράφους μέχρι και προγράμματα βάσεων δεδομένων.
- Η XML πρέπει να είναι συμβατή με την SGML. Η ιδέα πίσω από αυτό είναι ότι κάθε έγκυρο XML-έγγραφο είναι επίσης και ένα έγκυρο SGML-έγγραφο. Δηλαδή ένα αρχείο xml μπορεί να ελεγχθεί για την εγκυρότητα του σχετικά με το DTD εκτελώντας το μέσω ενός SGML validator. Το αντίστροφο δεν ισχύει πάντα καθώς ένας XML validator δεν περιέχει όλα τα στοιχεία της SGML.
- Θα πρέπει να είναι εύκολο να γράφονται προγράμματα τα οποία επεξεργάζονται XML έγγραφα. Αυτός είναι ένας από τους αρχικούς σκοπούς γιατί θεωρείται ότι όσο πιο απλή είναι η γλώσσα τόσο περισσότερα εργαλεία θα είναι διαθέσιμα. Η υιοθέτηση της XML σαν ένα standard βασίζεται κυρίως στην ελευθερία των προγραμμάτων να μπορούν να χρησιμοποιούν την καινούργια γλώσσα και οι χρήστες να μπορούν να παράγουν τα δικά τους εργαλεία χωρίς να απαιτείται πολύ προσπάθεια.
- Ο αριθμός των προαιρετικών γνωρισμάτων πρέπει να είναι ο ελάχιστος δυνατός και στην ιδανική περίπτωση μηδέν. Αυτό ήταν και ένα από τα προβλήματα που αντιμετώπιζε η SGML, ο μεγάλος αριθμός δηλαδή των προαιρετικών γνωρισμάτων.
- Τα XML έγγραφα θα πρέπει να είναι ευανάγνωστα.
- Ο σχεδιασμός XML θα πρέπει να προετοιμάζεται γρήγορα.
- Ο σχεδιασμός XML θα πρέπει να είναι τυπικός και περιεκτικός.
- Τα XML έγγραφα θα πρέπει να δημιουργούνται εύκολα.
- Η περιεκτικότητα στον XML συμβολισμό είναι μικρής σημασίας

Η XML είναι μια δομημένη γλώσσα, κάτι που σημαίνει ότι ένα έγγραφο XML δεν περιέχει μόνο δεδομένα αλλά καθορίζει επίσης τις δομικές σχέσεις ανάμεσα στα δεδομένα αυτά. Αυτή είναι η δύναμη της XML, που επιτρέπει την αναπαράσταση οποιουδήποτε είδους δεδομένων, εφόσον έχει οριστεί το δομικό τους σχήμα. Οι προδιαγραφές της δομής ενός εγγράφου XML

μπορεί να επιτευχθεί με την βοήθεια μοντέλων: είτε με το *μοντέλο Ορισμού Τύπων Εγγράφου (Document Type Definitions – DTD)*, ή με τα *Σχήματα XML (XML Schemas)*, τα οποία εξασφαλίζουν ότι δύο ή περισσότερα έγγραφα είναι του ίδιου «τύπου». Σε ότι αφορά στην αναπαράσταση της πληροφορίας μέσα σε ένα έγγραφο, η XML χαρακτηρίζεται απο ανεξαρτησία απο υποκείμενες πλατφόρμες, διότι όλη η πληροφορία αποθηκεύεται σε μορφή απλού κειμένου. Αυτή είναι μια απο τις πολύ ισχυρές της ιδιότητες, που κάνει τα έγγραφα XML αναγνώσιμα και απο μηχανές και απο ανθρώπους και εύκολα ενσωματώσιμα σε ροές εργασιών (workflows).

Σύμφωνα με τα παραπάνω, η XML σε ένα σύστημα χρησιμοποιείται για να προδιαγραφούν έγγραφα και μηνύματα που ανταλλάσσονται μεταξύ οντοτήτων. Αυτό συνεπάγεται ότι η ασφάλεια XML ασχολείται με την ασφάλεια σε επίπεδο μηνυμάτων και οι κύριες τεχνικές που χρησιμοποιούνται είναι η κρυπτογράφηση και οι ψηφιακές υπογραφές. Παρόλο που υπάρχουσες τεχνικές για κρυπτογράφηση ηλεκτρονικού ταχυδρομείου ή αρχείων μπορούν να χρησιμοποιηθούν και για μηνύματα XML, τεχνικές που είναι εξειδικευμένες για την XML θεωρούνται πιο κατάλληλες γι' αυτό το σκοπό. Την προσπάθεια προτυποποίησης στον τομέα αυτό οδηγεί ο οργανισμός W3C. Ένα πρότυπο για την παραγωγή ψηφιακών υπογραφών σε XML υπάρχει στη μορφή πρότασης του W3C (W3C recommendation) καθώς και ως RFC απο την IETF (RFC 3275 XML-Signature Syntax and Processing). Υπάρχει επίσης μια υποψήφια πρόταση του W3C για κρυπτογράφηση XML. Στην Ευρωπαϊκή πλευρά, ο οργανισμός προτυποποίησης ETSI έχει εκδώσει το πρότυπο "XML Advanced Electronic Signatures – XAdES", το οποίο κάνει χρήση του παραπάνω προτύπου του W3C για ψηφιακές υπογραφές XML και έχει ως στόχο την δημιουργία προηγμένων υπογραφών που εμπεριέχουν τα απαραίτητα δεδομένα, όπως χρονοσφραγίδες (timestamps), προκειμένου να μπορούν να επαληθευτούν μακροπρόθεσμα.

4.1 Κρυπτογράφηση XML

Το υποψήφιο πρότυπο για *Σύνταξη και Επεξεργασία Κρυπτογράφησης XML (XML Encryption Syntax and Processing)* περιγράφει μια διαδικασία για την κρυπτογράφηση ψηφιακών δεδομένων και τον τρόπο με τον οποίο το αποτέλεσμα της κρυπτογράφησης θα έπρεπε να αναπαρασταθεί σε XML. Η μέθοδος αυτή είναι πιο κατάλληλη για την κρυπτογράφηση των ίδιων των δεδομένων XML, αλλά μπορεί να εφαρμοστεί και στην γενική περίπτωση. Η Κρυπτογράφηση XML υποστηρίζει την κρυπτογράφηση ενός ολόκληρου κειμένου XML ή μόνο επιλεγμένων κομματιών του. Η μικρότερη μονάδα πληροφορίας που μπορεί να κρυπτογραφηθεί είναι ένα *στοιχείο XML (XML element)*. Υποστηρίζεται επίσης η επανακρυπτογράφηση δεδομένων, δηλαδή δεδομένα που έχουν ήδη κρυπτογραφηθεί μια φορά μπορούν να επανακρυπτογραφηθούν. Η μέθοδος επίσης παρέχει την αναγνώριση ή μεταφορά πληροφορίας για τα κλειδιά αποκρυπτογράφησης.

Η πρόταση του W3C επικεντρώνει στον καθορισμό της διαδικασίας δημιουργίας και αναπαράστασης των κρυπτογραφημένων δεδομένων XML, καθώς φυσικά και της διαδικασίας αποκρυπτογράφησης. Δεν προδιαγράφει νέους αλγορίθμους. Χρησιμοποιεί υπάρχοντες αλγορίθμους για την κρυπτογράφηση / αποκρυπτογράφηση, την συμφωνία κλειδιών, τις συναρτήσεις κατακερματισμού, την αυθεντικοποίηση μηνυμάτων και άλλες κρυπτογραφικές εφαρμογές (εκτός απο την διαδικασία παραγωγής ψηφιακών υπογραφών που καλύπτονται απο άλλο πρότυπο) όπως περιγράφονται στην παράγραφο. Περιγράφει την χρήση συμμετρικής και ασύμμετρης κρυπτογραφίας.

Μορφή / Δομή

Τα έγγραφα XML αποτελούνται απο ένα σύνολο *στοιχείων (tags)* τα οποία απαρτίζουν την δομή του εγγράφου. Σύμφωνα με το πρότυπο για την κρυπτογράφηση, τα κρυπτογραφημένα δεδομένα περιέχονται στο στοιχείο EncryptedData. Το EncryptedData επί της ουσίας αντικαθιστά τα προς κρυπτογράφηση δεδομένα μέσα στο έγγραφο. Η δομή του βασίζεται στο σχήμα του EncryptedType όπως φαίνεται στο επόμενο σχήμα:

```
<complexType name='EncryptedType' abstract='true'>
  <sequence>
```

```
    <element name='EncryptionMethod' type='xenc:EncryptionMethodType'
          minOccurs='0'/>
    <element ref='ds:KeyInfo' minOccurs='0'/>
    <element ref='xenc:CipherData'/>
    <element ref='xenc:EncryptionProperties' minOccurs='0'/>
  </sequence>
  <attribute name='Id' type='ID' use='optional'/>
  <attribute name='Type' type='anyURI' use='optional'/>
  <attribute name='MimeType' type='string' use='optional'/>
  <attribute name='Encoding' type='anyURI' use='optional'/>
 </complexType>
```

Το σχήμα για τον τύπο EncryptedType

Το EncryptedData κατ' ελάχιστον αποτελείται απο τα κρυπτογραφημένα δεδομένα εντός ενός στοιχείου CipherData.

```
 <element name='CipherData' type='xenc:CipherDataType'/>
 <complexType name='CipherDataType'>
   <choice>
     <element name='CipherValue' type='base64Binary'/>
     <element ref='xenc:CipherReference'/>
   </choice>
 </complexType>
```

Το σχήμα για το στοιχείο CipherData

Επιπρόσθετα μπορεί να περιλαμβάνει τα στοιχεία EncryptionMethod, KeyInfo και EncryptionProperties, τα οποία είναι όλα προαιρετικά και περιγράφονται στην συνέχεια της παρούσας παραγράφου. Η Κρυπτογράφηση XML επιτρέπει στον αποστολέα και τον παραλήπτη των κρυπτογραφημένων δεδομένων να προεπιλέξουν κρυπτογραφικές παραμέτρους, συμπεριλαμβανομένου των κλειδιών , έτσι ώστε οι παράμετροι δεν χρειάζονται να ανταλλαχθούν την ίδια τη στιγμή που επιτελείται η κρυπτογράφηση.
Όπως φαίνεται απο το **Error! Reference source not found.**, το στοιχείο CipherData μπορεί να αναπαρασταθεί με δύο τρόπους. Ο πρώτος είναι να περιέχει το ίδιο το κρυπτογραφημένο κείμενο ως XML, που είναι και η πιο συνηθισμένη περίπτωση. Τα κρυπτογραφημένα δεδομένα δεν είναι πλέον κατανοητά αφού το κείμενο είναι κωδικοποιημένο σε μορφή base64 (βλ. παράγραφο **Error! Reference source not found.**). Ο δεύτερος τρόπος είναι η δομή CipherData να περιέχει μια *αναφορά (reference)* στο κρυπτογραφημένο αντικείμενο και όχι το ίδιο το αντικείμενο.

Το στοιχείο EncryptionMethod περιέχει τον αλγόριθμο κρυπτογράφησης και το μέγεθος του κλειδιού. Ο τύπος στον οποίο βασίζεται είναι ο EncryptedMethodType ο οποίος φαίνεται στο ακόλουθο σχήμα:

```
 <complexType name='EncryptionMethodType' mixed='true'>
  <sequence>
    <element name='KeySize' minOccurs='0' type='xenc:KeySizeType'/>
    <element name='OAEPparams' minOccurs='0' type='base64Binary'/>
    <any namespace='##other' minOccurs='0' maxOccurs='unbounded'/>
  </sequence>
  <attribute name='Algorithm' type='anyURI' use='required'/>
 </complexType>
```

Ο τύπος EncryptionMethodType

Το στοιχείο KeyInfo παρέχει την πληροφορία που απαιτείται απο την εφαρμογή του παραλήπτη προκειμένου να αποκρυπτογραφήσει τα δεδομένα. Εάν παραλείπεται, αναμένεται απο την εφαρμογή να γνωρίζει πώς θα υλοποιήσει την αποκρυπτογράφηση, συμπεριλαμβανομένου της επιλογής του κλειδιού που θα χρησιμοποιήσει.

```
<element name="KeyInfo" type="ds:KeyInfoType"/>
<complexType name="KeyInfoType" mixed="true">
  <choice maxOccurs="unbounded">
    <element ref="ds:KeyName"/>
    <element ref="ds:KeyValue"/>
    <element ref="ds:RetrievalMethod"/>
    <element ref="ds:X509Data"/>
    <element ref="ds:PGPData"/>
    <element ref="ds:SPKIData"/>
    <element ref="ds:MgmtData"/>
    <any processContents="lax" namespace="##other"/>
    <!-- (1,1) elements from (0,unbounded) namespaces -->
  </choice>
  <attribute name="Id" type="ID" use="optional"/>
</complexType>
```

Το σχήμα για το στοιχείο KeyInfo

Η Κρυπτογράφηση XML υποστηρίζει όλες τις επιλογές που προδιαγράφονται απο το πρότυπο Ψηφιακής Υπογραφής XML για τον προσδιορισμό των κλειδιών. Ο προσδιορισμός μπορεί να επιτευχθεί με ένα αναγνωριστικό κλειδιού, το ίδιο το κλειδί αποκρυπτογράφησης, μια αναφορά σε μια τοποθεσία όπου βρίσκεται το κλειδί, ή το πιστοποιητικό δημοσίου κλειδιού του παραλήπτη που χρησιμοποιήθηκε για την κρυπτογράφηση των δεδομένων. Υποστηρίζονται διάφοροι τύποι πιστοποιητικών, συμπεριλαμβανομένου των X504. Παρ' όλα αυτά, ορισμένες αναπαραστάσεις κλειδιών δεν είναι χρήσιμες στην περίπτωση της Κρυπτογράφησης XML. Για παράδειγμα, η αποστολή του ίδιου του κλειδιού αποκρυπτογράφησης μαζί με τα δεδομένα που αυτό αποκαλύπτει προφανώς δεν ωφελεί. Ως εναλλακτική λύση, η Κρυπτογράφηση XML επεκτείνει τις επιλογές της Ψηφιακής Υπογραφής XML και προσθέτει την επιλογή για ένα EncryptedKey. Εάν η δομή KeyInfo δεν περιλαμβάνεται, η εφαρμογή του παραλήπτη θα πρέπει να γνωρίζει ποιο κλειδί να χρησιμοποιήσει για να αποκρυπτογραφήσει το μήνυμα. Εν κατακλείδι, το στοιχείο EncryptionProperties περιέχει επιπρόσθετες πληροφορίες σχετικές με την διαδικασία.

Διαδικασία κρυπτογράφησης και αποκρυπτογράφησης

Για να κρυπτογραφηθούν στοιχεία XML ακολουθείται η παρακάτω διαδικασία:

1. Επιλέγεται ο αλγόριθμος κρυπτογράφησης και οι παράμετροί του.
2. Ανακτάται το κλειδί. Αν το κλειδί πρόκειται να αναγνωριστεί, δημιουργείται ένα στοιχείο KeyInfo. Το κλειδί κρυπτογραφείται αν πρόκειται να αποσταλεί μαζί με τα κρυπτογραφημένα δεδομένα και δημιουργείται ένα στοιχείο EncryptedKey, το οποίο τοποθετείται μέσα στο στοιχείο KeyInfo, ή κάποιο άλλο σημείο μέσα στο έγγραφο.
3. Κρυπτογραφούνται τα δεδομένα. Για δεδομένα XML, αυτό μπορεί να εμπλέκει την μετατροπή σε κωδικοποίηση UTF-8 και σειριοποίηση, δηλαδή την μετατροπή της δομής σε μια ακολουθία απο bytes. Το αποτέλεσμα είναι ένα octet string.
4. Δημιουργείται το στοιχείο EncryptedData. Στην περίπτωση που τα κρυπτογραφημένα δεδομένα αποθηκεύονται μέσα στο έγγραφο αντί να υπάρχει απλά μια αναφορά σε αυτά, τότε πρέπει να είναι κωδικοποιημένα στη μορφή base64.
5. Αντικαθίστανται τα προς κρυπτογράφηση δεδομένα μέσα στο ίδιο το έγγραφο XML, με το στοιχείο EncryptedData.

Προκειμένου να επιτευχθεί η αποκρυπτογράφηση των δεδομένων, ακολουθούνται τα επόμενα βήματα.

1. Γίνεται επεξεργασία του στοιχείου EncryptedData. Απροσδιόριστες παράμετροι, παρέχονται απο την εφαρμογή.
2. Ανακτάται το κλειδί αποκρυπτογράφησης. Αυτό μπορεί να περιλαμβάνει πρώτα την αποκρυπτογράφηση ενός συμμετρικού κλειδιού απο ένα ιδιωτικό ή την ανάκτηση απο μια τοπική αποθήκη κλειδιών, στο δίσκο του χρήστη ή μια έξυπνη κάρτα.
3. Αποκρυπτογραφούνται τα δεδομένα στη δομή CipherData.
4. Γίνεται επεξεργασία των αποκρυπτογραφημένων δεδομένων. Αυτό μπορεί να απαιτεί απο την εφαρμογή την επαναφορά των δεδομένων, που μπορεί να έχουν κωδικοποιηθεί ως UTF-8, στην αρχική τους μορφή. Επίσης, γίνεται αντικατάσταση των δεδομένων στην αρχική τους θέση μέσα στη δομή του εγγράφου XML. Σε μερικές περιπτώσεις, ενδέχεται να απαιτείται και περαιτέρω επεξεργασία.

Παράδειγμα

Το κομμάτι κώδικα που ακολουθεί είναι ένα παράδειγμα κρυπτογραφημένου περιεχομένου.

```
<PaymentInfo xmlns='http://example.org/paymentv2'>
        <Name>John Smith</Name>
        <CreditCard Limit='5,000' Currency='USdollars'>
        <EncryptedData xmlns='http://www.w3.org/2001/04/xmlenc#'
Type='http://www.w3.org/2001/04/xmlenc#Content'>
                <EncryptionMethod      Algorithm='http://www.w3.org/2001/04/xmlenc#3des-
cbc'/>
                        <ds:KeyInfo xmlns:ds='http://www.w3.org/2000/09/xmldsig#'>
                                <ds:KeyName>mykey</ds:KeyName>
                        </ds:KeyInfo>
                        <CipherData>
                                <CipherValue>423EE256</CipherValue>
                        </CipherData>
        </EncryptedData>
</PaymentInfo>
```

Παράδειγμα κρυπτογράφησης XML

Το κρυπτογραφημένο περιεχόμενο αντικαθιστά το αρχικό μέσα στο έγγραφο XML. Στην περίπτωση του παραδείγματος, το κρυπτογραφημένο κομμάτι αναπαριστά ευαίσθητη πληροφορία για μια πληρωμή. Το ονοματεπώνυμο στην πιστωτική κάρτα και το όριο, μεταδίδονται χωρίς επεξεργασία, ενώ ο αριθμός της κάρτας είναι κρυπτογραφημένος. Ο αλγόριθμος κρυπτογράφησης που χρησιμοποιείται είναι ο 3DES σε μορφή cipher block chaining – CBC. Το κλειδί που θα χρησιμοποιηθεί για να αποκρυπτογραφηθούν τα δεδομένα ονομάζεται mykey. Στην περίπτωση αυτή, θεωρείται ότι ο παραλήπτης του μηνύματος γνωρίζει το κλειδί απο προηγούμενη επικοινωνία. Τα κρυπτογραφημένα δεδομένα εμφανίζονται μέσα στη δομή CipherValue.

4.2 Ψηφιακή Υπογραφή XML

Το πρότυπο Ψηφιακής Υπογραφής XML καθορίζει πώς ψηφιακά δεδομένα υπογράφονται και πως το αποτέλεσμα της υπογραφής μπορεί να αναπαρασταθεί σε XML. Η Ψηφιακή Υπογραφή XML προορίζεται κυρίως για δεδομένα XML, αλλά μπορεί να εφαρμοστεί και γενικότερα με όλες τις μορφές ψηφιακών δεδομένων. Με την Ψηφιακή Υπογραφή XML μπορεί να υπογραφεί ένα ολόκληρο έγγραφο XML ή επιλεγμένα κομμάτια του.

Το πρότυπο καθορίζει την διαδικασία για την δημιουργία και αναπαράσταση μιας υπογραφής XML και την επαλήθευση της εγκυρότητάς της. Βασίζεται σε υπάρχοντες αλγορίθμους για την υπογραφή, τις συναρτήσεις κατακερματισμού, και τους Κώδικες Αυθεντικοποίησης

Μηνυμάτων – ΚΑΜ (message authentication codes - MACs) (βλ. παράγραφο **0**). Μπορεί να συνδυαστεί με αρκετά ευρέως διαδεδομένα είδη πιστοποιητικών, συμπεριλαμβανομένου των πιστοποιητικών X504. Μπορεί επίσης να χρησιμοποιηθεί χωρίς πιστοποιητικά, κάτι που αποκλίνει απο την γενική περίπτωση κρυπτοσυστημάτων δημοσίου κλειδιού, αλλά που μπορεί να δικαιολογηθεί υπό ορισμένες προϋποθέσεις. Το πρότυπο κάνει αναφορά σε άλλα πρότυπα για μετασχηματισμούς όπως είναι η *κανονικοποίηση*, η οποία φέρνει τα δεδομένα σε μια πρότυπη μορφή που εξαλείφει οποιεσδήποτε δευτερεύουσες και ασήμαντες διαφορές στην αναπαράσταση και κωδικοποίηση.
Οι ψηφιακές υπογραφές είναι αρκετά πιο πολύπλοκες στην υλοποίηση απο την κρυπτογράφηση. Η δημιουργία τους πρέπει να γίνεται με ιδιαίτερη προσοχή, διότι είναι άρρηκτα δεμένες με την αναπαράσταση των δεδομένων που υπογράφονται. Αυτό σημαίνει ότι η αναπαράσταση των υπογεγραμμένων δεδομένων και των δεδομένων που διαβάζονται προκειμένου να επαληθευτεί η υπογραφή πρέπει να είναι συνεπή. Η επεξεργασία της υπογραφής είναι πολύ ευαίσθητη σε αλλαγές στην αναπαράσταση των δεδομένων και την διάταξη των βημάτων επεξεργασίας. Ακόμη και αν υπογραφή ήταν έγκυρη τη στιγμή της δημιουργίας της, υπάρχει το ενδεχόμενο να μην μπορεί να επαληθευτεί στη συνέχεια απο τον παραλήπτη, λόγω αλλαγών που συνέβησαν κατά τη μεταφορά ενός μηνύματος.

Μορφή / Δομή
Μια Υπογραφή XML αποτελείται απο δυο απαραίτητα στοιχεία XML, το στοιχείο SignedInfo και το στοιχείο SignatureValue όπως φαίνεται στο ακόλουθο σχήμα XML:

```
<element name="Signature" type="ds:SignatureType"/>
<complexType name="SignatureType">
  <sequence>
    <element ref="ds:SignedInfo"/>
    <element ref="ds:SignatureValue"/>
    <element ref="ds:KeyInfo" minOccurs="0"/>
    <element ref="ds:Object" minOccurs="0" maxOccurs="unbounded"/>
  </sequence>
  <attribute name="Id" type="ID" use="optional"/>
</complexType>
```

Το σχήμα του στοιχείου Signature
Υπάρχουν επίσης και δυο προαιρετικά στοιχεία, τα KeyInfo και Object, το οποία εξηγούνται στη συνέχεια.

SignedInfo. Περιλαμβάνει το στοιχείο CanonicalizationMethod, που είναι στην ουσία η μέθοδος κανονικοποίησης που θα εφαρμοστεί στο ίδιο το στοιχείο SignedInfo, στους αλγορίθμους που χρησιμοποιούνται για την παραγωγή της υπογραφής (συνήθως έναν αλγόριθμο κατακερματισμού και έναν αλγόριθμο ψηφιακής υπογραφής), και σε μια ή περισσότερες αναφορές (δηλ. στοιχεία Reference) στα δεδομένα που υπογράφονται.

```
<element name="SignedInfo" type="ds:SignedInfoType"/>
<complexType name="SignedInfoType">
  <sequence>
    <element ref="ds:CanonicalizationMethod"/>
    <element ref="ds:SignatureMethod"/>
    <element ref="ds:Reference" maxOccurs="unbounded"/>
  </sequence>
  <attribute name="Id" type="ID" use="optional"/>
</complexType>
```

Το σχήμα του στοιχείου SignedInfo

Κάθε στοιχείο αναφοράς Reference περιλαμβάνει ένα URI που αναγνωρίζει τα δεδομένα που υπογράφονται, τους μετασχηματισμούς που αυτά υπόκεινται (κάποιοι απο τους οποίους αναλύονται στη συνέχεια), ένα αναγνωριστικό του αλγορίθμου μετασχηματισμού που θα χρησιμοποιηθεί στα προς μετασχηματισμό δεδομένα και την τιμή του αποτελέσματος της συνάρτησης κατακερματισμού.
SignatureValue. Αποτελεί την τιμή της ψηφιακής υπογραφής.

```
<element name="SignatureValue" type="ds:SignatureValueType"/>
<complexType name="SignatureValueType">
 <simpleContent>
  <extension base="base64Binary">
   <attribute name="Id" type="ID" use="optional"/>
  </extension>
 </simpleContent>
</complexType>
```

Το σχήμα του στοιχείου SignatureValue

Όπως φαίνεται απο το σχήμα, η τιμή είναι κωδικοποιημένη στη μορφή base64.
KeyInfo. Αυτό παρέχει την πληροφορία που χρειάζεται απο την εφαρμογή του παραλήπτη για να επαληθεύσει την υπογραφή και το XML σχήμα του έχει ήδη παρουσιαστεί στο **Error! Reference source not found.**. Εάν παραληφθεί, θεωρείται ότι η εφαρμογή γνωρίζει τον τρόπο για την επαλήθευση. Για παράδειγμα, μπορεί δύο συνεργάτες να έχουν προ-ανταλλάξει δημόσια κλειδιά με κάποιον άλλο τρόπο, εξαλείφοντας την ανάγκη για εισαγωγή του δημοσίου κλειδιού ως στοιχείο-παιδί του KeyInfo. Αν αυτό δεν έχει συντελεστεί, το KeyInfo μπορεί να περιλαμβάνει ένα αναγνωριστικό κλειδιού, ή το δημόσιο κλειδί του υπογράφοντος, ή μια αναφορά στην τοποθεσία όπου το κλειδί είναι διαθέσιμο, ή το ίδιο το ψηφιακό πιστοποιητικό δημοσίου κλειδιού. Υποστηρίζεται ένας ικανός αριθμός τύπων πιστοποιητικών.
Object. Είναι μια δομή που μπορεί να περιέχει οποιασδήποτε άλλης μορφής πληροφορία για την υποστήριξη της υπογραφής.
Μετασχηματισμοί
Προτού τα δεδομένα υπογραφούν, υπόκεινται συνήθως σε μια ή περισσότερες διαδικασίες μετασχηματισμού. Οι μετασχηματισμοί αυτοί καθιστούν τα δεδομένα κατάλληλα προς υπογραφή. Για παράδειγμα, ένας πολύ γνωστός μετασχηματισμός, ο οποίος αρχικά χρησιμοποιήθηκε για το ηλεκτρονικό ταχυδρομείο, είναι η αποκωδικοποίηση base64. Η αποκωδικοποίηση base64 χρησιμοποιείται προκειμένου να υπογραφεί η αρχική έκδοση δεδομένων που έχουν κωδικοποιηθεί με base64. Για παράδειγμα, προκειμένου να εισαχθούν δυαδικά δεδομένα στο XML έγγραφο, αυτά κωδικοποιούνται με base64, απο την οποία κωδικοποίηση προκύπτει μια συμβολοσειρά. Συνήθως όμως σε συναρτήσεις κατακερματισμού θέλουμε να δώσουμε ως όρισμα την αρχική δυαδική μορφή των δεδομένων, άρα είναι απαραίτητο να περάσουν απο έναν μετασχηματισμό αποκωδικοποίησης base64. Επιπρόσθετα, υπάρχουν αρκετοί ακόμη μετασχηματισμοί που είναι σημαντικοί για την XML και τις Υπογραφές XML. Θα αναλυθούν στη συνέχεια οι μετασχηματισμοί *XPath (XPath Transform)*, *Κανονικοποίησης XML (Canonical XML Transform)*, και ο *Μετασχηματισμός Αποκρυπτογράφησης για την Υπογραφή XML (Decryption Transform for XML Signature)*.

Ο μετασχηματισμός κανονικοποίησης XML μπορεί να εφαρμοστεί στο στοιχείο SignedInfo. Επιπρόσθετα, κάθε στοιχείο Reference μέσα στο SingedInfo ενδέχεται να περιέχει μετασχηματισμούς που καθορίζονται στο ίδιο το στοιχείο. Η παράμετρος εισόδου στον πρώτο μετασχηματισμό είναι τα δεδομένα που καθορίζονται απο το URI του SignedInfo. Η έξοδος του μετασχηματισμού αυτού, γίνεται είσοδος του επόμενου, και ούτω καθεξής, μέχρι η έξοδος του τελευταίο μετασχηματισμού να γίνει είσοδος της συνάρτησης κατακερματισμού.

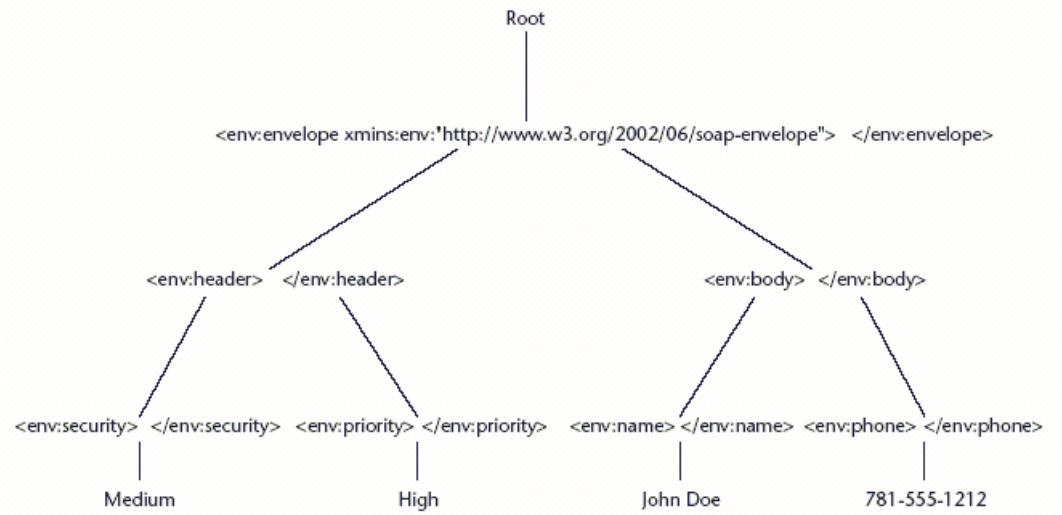
Παρόλο που η Υπογραφή XML δεν επιβάλει την χρήση των συγκεκριμένων αυτών μετασχηματισμών, η λειτουργικότητα που προσφέρουν είναι απαραίτητη προκειμένου να εκτελεστεί σωστά η συνάρτηση της υπογραφής. Ακόμη και αν ο σχεδιαστής μιας εφαρμογής δεν θέλει να χρησιμοποιήσει τους συγκεκριμένους αλγορίθμους, θα πρέπει να βρει κάτι αντίστοιχο με παρόμοια λειτουργικότητα. Η χρήση εναλλακτικών λύσεων αποθαρρύνεται γενικότερα διότι μειώνει την διαλειτουργικότητα των Υπογραφών XML.

XPath / XPointer

Υπάρχει η ανάγκη για επιλεκτική υπογραφή περιοχών μέσα στο έγγραφο XML. Σε αντίθεση με το ηλεκτρονικό ταχυδρομείο ή αρχεία, όπου ολόκληρα τα έγγραφα προορίζονται για έναν παραλήπτη, στην περίπτωση των εγγράφων XML, υπάρχει το ενδεχόμενο πολλοί παραλήπτες να πρέπει να επεξεργαστούν ένα έγγραφο, και κάθε ένας να πρέπει να υπογράψει ή να επαληθεύσει ένα συγκεκριμένο μέρος του. Αυτό είναι διαφορετικό απο την ιδιότητα επιλεκτικής απόκρυψης της Κρυπτογράφησης XML. Με την Κρυπτογράφηση XML, τα κρυπτογραφημένα δεδομένα παίρνουν την θέση των αρχικών μέσα στο έγγραφο και είναι εμφανές τι είναι κρυπτογραφημένο. Στις ψηφιακές υπογραφές XML, τα υπογεγραμμένα δεδομένα δεν αντικαθιστούν κάτι. Άντ' αυτού, δημιουργείται μια επιπρόσθετη δομή και προστίθεται μέσα στο έγγραφο, πολύ πιθανόν σε κάποιο άλλο σημείο. Χρειάζεται λοιπόν μια μέθοδος αναγνώρισης των στοιχείων του εγγράφου που έχουν υπογραφεί και ποια υπογραφή αντιστοιχεί σε αυτά. Γι' αυτό το σκοπό χρησιμοποιείται η γλώσσα XPath. Η XPath μπορεί να χρησιμοποιηθεί για διάφορες λειτουργίες, αλλά οι Ψηφιακές Υπογραφές XML την χρησιμοποιούν προκειμένου να αναγνωρίσουν τους υπογεγραμμένους κόμβους.

Η γλώσσα XPath (XML Path Language – XPath) είναι μια γλώσσα αναζητήσεων, η οποία ψάχνει, βρίσκει και αναγνωρίζει κομμάτια ενός εγγράφου XML. Αρχικά υλοποιήθηκε για χρήση σε συνδυασμό με την Επεκτάσιμη Γλώσσα Μετασχηματισμών Διαμόρφωσης (Extensible StyleSheet Language Transformations – XSLT). Το αναγνωριστικό της XPath είναι http://www.w3.org/TR/1999/REC-xpath-1999116. Επιτελείται επίσης εργασία πάνω στο Φίλτρο XPath Ψηφιακής Υπογραφής (XML Signature XPath Filter), το οποίο είναι μια εξειδικευμένη έκδοση της XPath για την εφαρμογή της σε ψηφιακές υπογραφές. Η ανάλυση που ακολουθεί αναφέρεται στην έκδοση 1.0 της XPath.

Προκειμένου να λειτουργήσει η XPath, το έγγραφο XML θα πρέπει να είναι οργανωμένο σε δενδρική δομή. Στο επόμενο σχήμα έχει μοντελοποιηθεί ένα έγγραφο XML ως ένα τέτοιο δέντρο. Τα περιεχόμενα αυτό το δέντρου είναι παρόμοια αλλά όχι ακριβώς ίδια με το αρχικό έγγραφο XML. Περιέχει τα στοιχεία, σχόλια, χώρους ονομάτων και εντολές επεξεργασίας του εγγράφου XML. Έχει επίσης έναν κόμβο ρίζα, ο οποίος βρίσκεται λογικά πάνω απο αυτό που θεωρούμε ρίζα του εγγράφου. Αυτό μας επιτρέπει να συμπεριλάβουμε σχόλια που εμφανίζονται πριν απο την αρχή του εγγράφου XML. Παρ' όλα αυτά, δεν περιέχει την δήλωση της XML <?xml version="1.0"?>.



Δέντρο XML

Το *μονοπάτι εύρεσης θέσης* αναγνωρίζει έναν κόμβο μέσα στο δέντρο καθορίζοντας διαδρομές για να φτάσουμε στον κόμβο αυτό απο έναν άλλον αρχικό κόμβο. Το μονοπάτι θέσης μπορεί να είναι απόλυτο ή σχετικό. Εάν είναι απόλυτο, ξεκινά απο τον κόμβο ρίζα του εγγράφου. Αν είναι σχετικό, ξεκινά απο έναν άλλο κόμβο, ο οποίος καλείται συναφής κόμβος στο δέντρο.
Απο το σημείο αυτό, η XPath προχωράει μέσα στο δέντρο για να εντοπίσει κόμβους που μας ενδιαφέρουν. Κάθε βήμα αποτελείται απο μια κατεύθυνση, που ονομάζεται άξονας, για αναζήτηση με σημείο αναφοράς τον συναφή κόμβο. Αναζητήσεις μπορεί να κατευθύνονται προς τα πάνω ή προς τα κάτω σε σχέση με τον αρχικό κόμβο και έτσι λαμβάνονται συγκεκριμένες σχέσεις. Για ψηφιακές υπογραφές, οι μόνοι κόμβοι που μας ενδιαφέρουν είναι οι απόγονοι του συναφή κόμβου. Σε κάθε βήμα επίσης γίνεται ένας έλεγχος του κόμβου και εφαρμόζονται λογικοί τελεστές (ίσον, άνισο, μεγαλύτερο από κλπ). Με χρήση των τελεστών αυτών ελέγχεται το περιεχόμενο των κόμβων. Τα αποτελέσματα ενός ελέγχου μπορεί να τροφοδοτηθούν σε έναν επόμενο κ.ο.κ.
Το πρότυπο XPointer αποτελεί επίσης Recommendation του W3C και επεκτείνει το XPath προκειμένου να μπορεί να γίνει χρήση των αναγνωριστικών URI στις αναζητήσεις. Η πιο ενδιαφέρουσα είναι η μορφή «απλού ονόματος» (bare name) του XPointer. Ένα «απλό όνομα» κάνει αναφορά σε ένα στοιχείο μέσα στο έγγραφο το οποίο έχει ένα χαρακτηριστικό (attribute) ID με το ίδιο όνομα. Στο παράδειγμα που ακολουθεί, το στοιχείο Test έχει ένα χαρακτηριστικό ID με το όνομα referencedNode. Κατ' αυτόν τον τρόπο, η αναφορά στο στοιχείο Test γίνεται μέσω του referencedNode:

Δήλωση στοιχείου Test:
<Test ID =”referencedNode”>
…
</Test>

Αναφορά στο στοιχείο Test:
<signedInfoRef URI=”#referencedNode”>
…
</signedInfoRef >

Η μορφή αυτή «απλού ονόματος» του XPointer χρησιμοποιείται μόνο όταν η αναφορά στο referencedNode βρίσκεται μέσα στο ίδιο έγγραφο που βρίσκεται και το Test. Όταν ο κόμβος είναι σε εξωτερικό έγγραφο, τότε το «απλό όνομα» προστίθεται στο URI που αναγνωρίζει το εξωτερικό έγγραφο. Ο XPointer «απλού ονόματος» χρησιμεύει στον προσδιορισμό των υπογεγραμμένων στοιχείων μέσα στο έγγραφο XML.

Κανονικοποίηση XML

Όπως προαναφέρθηκε, οι ψηφιακές υπογραφές εξαρτώνται απο την αναπαράσταση των δεδομένων που υπογράφονται. Για παράδειγμα, η προσθήκη ενός κατά τ' άλλα ασήμαντου χαρακτήρα σε ένα έγγραφο, όπως είναι ένα κενό, θα θεωρηθεί απο μια εφαρμογή επαλήθευσης ως αλλαγή του υπογεγραμμένου εγγράφου και η επαλήθευση της υπογραφής θα αποτύχει. Για να αποφύγουμε τέτοιες καταστάσεις, τα έγγραφα XML μετασχηματίζονται σε μια πρότυπη μορφή προτού υπογραφούν και προτού γίνει η επαλήθευση της υπογραφής.
Η *Κανονικοποιημένη XML (Canonical XML)* παρέχει έναν πρότυπο τρόπο ώστε να αποφανθεί κάποιος αν δύο έγγραφα είναι όμοια. Καθορίζει κανόνες προκειμένου να μετασχηματιστεί ένα έγγραφο XML σε μια πρότυπη αναπαράσταση. Ένα άλλο έγγραφο με την ίδια κανονικοποιημένη αναπαράσταση θεωρείται όμοιο με το πρώτο. Υπάρχουν δύο παραλλαγές της Κανονικοποιημένης XML. Μια έκδοση δεν περιλαμβάνει σχόλια και το αναγνωριστικό της είναι http://www.w3.org/TR/2001/REC-xml-c14-20010315. Η άλλη έκδοση περιλαμβάνει σχόλια και το αναγνωριστικό της είναι http://www.w3.org/TR/2001/REC-xml-c14-20010315#WithComments.

Ένα δεύτερο πρότυπο, η *Αποκλειστική Κανονικοποίηση XML (Exclusive XML Canonicalization)* είναι ακόμη υπό προτυποποίηση και καλύπτει την ανάγκη για την υπογραφή κομματιών ενός εγγράφου με τέτοιο τρόπο ώστε το υπογεγραμμένο κομμάτι να μπορεί να εξαχθεί και να τοποθετηθεί σε ένα άλλο έγγραφο. Για παράδειγμα, αν το υπογεγραμμένο κομμάτι του εγγράφου χρησιμοποιεί έναν προκαθορισμένο *Χώρο Ονομάτων (namespace)*, η Αποκλειστική Κανονικοποίηση XML αντιγράφει τον χώρο ονομάτων στο υπο-κομμάτι του εγγράφου που υπογράφεται.
Η κανονικοποιημένη μορφή ενός εγγράφου είναι αυτή που τελικά υπογράφεται, επειδή οι κανόνες της κανονικοποίησης που έχουν εφαρμοστεί στο ληφθέν έγγραφο XML εξαλείφουν αλλαγές που τυχόν μπορεί να συμβούν κατά τη μεταφορά διαμέσου κόμβων και διατηρούν μια σταθερή μορφή του εγγράφου.
Η Κανονικοποίηση XML μετατρέπει τα δεδομένα χρησιμοποιώντας ένα σταθερό σύνολο χαρακτήρων, το UTF-8. Κανονικοποιεί γραμμές και χαρακτηριστικά, αντικαθιστά αναφορές, αφαιρεί περιττές αναφορές χώρων ονομάτων, προσθέτει προκαθορισμένα χαρακτηριστικά και εφαρμόζει όλες εκείνες τις συναρτήσεις που εξαλείφουν περιττές δομές και ξεκαθαρίζουν διφορούμενες εκφράσεις.
Όταν χρησιμοποιείται με τις ψηφιακές υπογραφές, η κανονικοποίηση πρέπει να μετασχηματίσει τα δεδομένα πριν εκτελεστεί η υπογραφή. Επίσης χρησιμοποιείται για να μετασχηματίσει τα δεδομένα πριν γίνει και η επαλήθευση της υπογραφής. Επειδή η κανονικοποίηση μπορεί να έχει υψηλό κόστος σε υπολογιστικούς πόρους, μόνο τα κομμάτια του εγγράφου που πρόκειται να υπογραφούν κανονικοποιούνται.

4.3 Μετασχηματισμός Αποκρυπτογράφησης για την Ψηφιακή Υπογραφή XML

Όταν η ψηφιακή υπογραφή συνδυάζεται με κρυπτογράφηση, είναι απαραίτητο να γνωρίζουμε αν η υπογραφή εφαρμόστηκε σε κρυπτογραφημένα δεδομένα ή αν ήταν αναγνώσιμα δεδομένα που υπεγράφησαν και κρυπτογραφήθηκαν στη συνέχεια. Στην πρώτη περίπτωση, τα κρυπτογραφημένα δεδομένα πρέπει να παραμείνουν ως έχουν προκειμένου να επαληθευτεί η υπογραφή. Στην δεύτερη περίπτωση, πρέπει πρώτα να επιτελεστεί η αποκρυπτογράφηση πριν γίνει η επαλήθευση. Ο Μετασχηματισμός Αποκρυπτογράφησης για την Ψηφιακή Υπογραφή XML είναι μια υπό προτυποποίηση πρόταση του W3C που καθορίζει πώς ο υπογράφων ένα έγγραφο μπορεί να πληροφορήσει τον παραλήπτη που θα επαληθεύσει την υπογραφή, ποια υπογεγραμμένα τμήματα του εγγράφου πρέπει να παραμείνουν κρυπτογραφημένα πριν την επαλήθευση. Όλα τα υπόλοιπα τμήματα πρέπει να αποκρυπτογραφηθούν και μετά ο παραλήπτης να προχωρήσει σε επαλήθευση.
Η διαδικασία δεν είναι ένας ξεχωριστός μετασχηματισμός. Αντίθετα, είναι μια οδηγία στην εφαρμογή επαλήθευσης που χρησιμοποιείται κατά την διάρκεια του μετασχηματισμού αποκρυπτογράφησης. Συνεπώς, ένα στοιχείο που περιλαμβάνει έναν κρυπτογραφημένο κόμβο που εξαιρείται, πρέπει να εισαχθεί ας στοιχείο-παιδί στο στοιχείο του μετασχηματισμού. Ένα παράδειγμα είναι το ακόλουθο:

```
<Transform Algorithm=”http://www.w3.org/2001/04/decrypt#”>
        <Except xmlns=http://www.w3.org/2001/04/decrypt# URI=”#enc1”/>
</Transform>
```

Στο παράδειγμα αυτό, ο κόμβος enc1 κρυπτογραφήθηκε πριν λάβει χώρα η υπογραφή. Άλλα τμήματα του εγγράφου κρυπτογραφήθηκαν μετά την υπογραφή. Για να γίνει η επαλήθευση της υπογραφής, όλα τα άλλα τμήματα πρέπει πρώτα να αποκρυπτογραφηθούν, αλλά ο κόμβος enc1 πρέπει να αφεθεί άθικτος μέχρι να έχει τελειώσει η διαδικασία επαλήθευσης. Αν χρειάζεται στα πλαίσια της εκάστοτε εφαρμογής, μπορεί να αποκρυπτογραφηθεί κατόπιν της ολοκλήρωσης της διαδικασίας επαλήθευσης.

Διαδικασία δημιουργίας / επαλήθευσης Υπογραφής
Για τη δημιουργία μιας Ψηφιακής Υπογραφής XML επιτελούνται τα ακόλουθα βήματα:

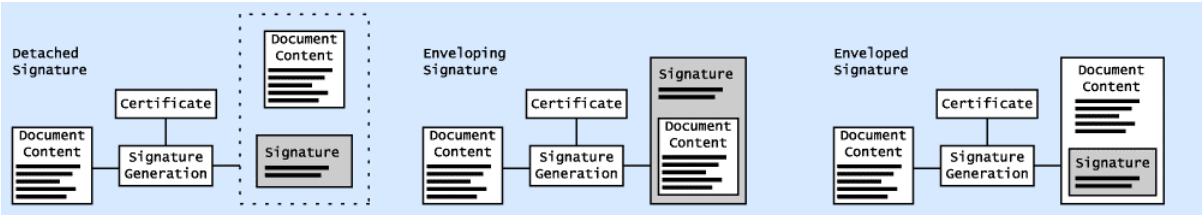
1. Εφαρμόζονται οι επιλεγμένοι μετασχηματισμοί στα αντικείμενα που πρόκειται να υπογραφούν. Οι μετασχηματισμοί εφαρμόζονται στη σειρά που έχει προδιαγραφεί.
2. Υπολογίζεται η τιμή της συνάρτησης κατακερματισμού στο αποτέλεσμα των μετασχηματισμών.
3. Δημιουργείται ένα στοιχείο αναφοράς που περιλαμβάνει το URI των προς υπογραφή δεδομένων και τα αναγνωριστικά των μετασχηματισμών που χρησιμοποιήθηκαν, τη συνάρτηση κατακερματισμού καθώς επίσης και την τιμή της τελευταίας. Αυτό συμβαίνει αν η υπογραφή καλύπτει περισσότερους του ένα κόμβους μέσα στο έγγραφο XML.
4. Δημιουργείται το στοιχείο SignedInfo. Περιλαμβάνεται η μέθοδος υπογραφής με ένα στοιχείο SignatureMethod, η μέθοδος κανονικοποίησης με το στοιχείο CanonicalizationMethod και όλες οι αναφορές που δημιουργήθηκαν προηγουμένως.
5. Εφαρμόζεται η μέθοδος κανονικοποίησης στο στοιχείο SignedInfo.
6. Χρησιμοποιούνται οι αλγόριθμοι που καθορίστηκαν στο στοιχείο SignatureMethod για να δημιουργηθεί η υπογραφή. Αυτό συνήθως σημαίνει την εφαρμογή μιας συνάρτησης κατακερματισμού στο κανονικοποιημένο στοιχείο SignedInfo και υπογραφή της τιμής που προκύπτει.
7. Δημιουργείται το στοιχείο Signature που περιλαμβάνει το στοιχείο SignedInfo, το στοιχείο SignatureValue (στο οποίο τοποθετείται η τιμή που προκύπτει απο το βήμα 6), τα προαιρετικά στοιχεία KeyInfo και Object.
8. Επισημαίνεται ότι σε κάθε στοιχείο στο οποίο γίνεται αναφορά, ενδέχεται να εφαρμοστεί διαφορετικός αλγόριθμος συνάρτησης κατακερματισμού ή κανονικοποίησης.

Για να επαληθευθεί μια υπογραφή εκτελούνται οι ακόλουθες διαδικασίες:
1. Κανονικοποιείται το στοιχείο SignedInfo σύμφωνα με την μέθοδο κανονικοποίησης που αναφέρεται στο στοιχείο CanonicalizationMethod (που περιέχεται στο SignedInfo).
2. Για κάθε στοιχείο αναφοράς Reference, λαμβάνονται τα αντικείμενα στα οποία γίνεται η αναφορά.
3. Γίνεται επεξεργασία κάθε αντικειμένου σύμφωνα με τους μετασχηματισμούς που έχουν προδιαγραφεί.
4. Στο αποτέλεσμα εφαρμόζεται η συνάρτηση κατακερματισμού όπως έχει καθοριστεί. Γίνεται σύγκριση του αποτελέσματος με την τιμή που είναι αποθηκευμένη στο αντίστοιχο στοιχείο Reference. Αν οι δύο τιμές δεν είναι ίδιες, η επαλήθευση αποτυγχάνει.
5. Ανακτάται η απαραίτητη πληροφορία για τα κλειδιά που πρέπει να χρησιμοποιηθούν. Μπορεί να περιέχεται σε ένα στοιχείο KeyInfo, ή να είναι ήδη διαθέσιμη με κάποιον άλλο τρόπο.
6. Εφαρμόζεται η μέθοδος υπογραφής με χρήση του κλειδιού και το αποτέλεσμα συγκρίνεται με την τιμή υπογραφής του στοιχείου SignatureValue στο κανονικοποιημένο SignedInfo. Και πάλι αν τα αποτελέσματα δεν είναι τα ίδια, η επαλήθευση αποτυγχάνει.

Είδη Ψηφιακής Υπογραφής XML

Το πρότυπο Ψηφιακών Υπογραφών XML ενσωματώνει την λειτουργικότητα των υπογραφών στα έγγραφα μέσα απο τρία ισότιμα σχήματα: περικλειόμενες (enveloped), περικλείουσες (enveloping) και αποσπασμένες (detached) υπογραφές.

Σχηματικά, τα τρία είδη των υπογραφών αναπαρίστανται στο ακόλουθο διάγραμμα:



Αποσπασμένες, περικλείουσες και περικλειόμενες υπογραφές XML

Περικλειόμενες υπογραφές: Αποτελούν τον μηχανισμό υπογραφών που είναι πιο κοντά στην ανθρώπινη λογική. Όταν μια ιδιόχειρη υπογραφή μπαίνει σε ένα έγγραφο, το ίδιο το έγγραφο παραμένει εμφανές και χρησιμοποιήσιμο, και η υπογραφή είναι εμφανής (ενσωματωμένη) πάνω του. Το πρότυπο Ψηφιακών Υπογραφών XML επιτρέπει την παραγωγή περικλειόμενων υπογραφών, όπου το ίδιο έγγραφο περικλείει την υπογραφή. Το πλεονέκτημα αυτής της λύσης είναι ότι το έγγραφο παραμένει στην μορφή που ήταν και πριν και μπορεί να υποστεί επεξεργασία. Αυτό επιτρέπει σε συστήματα να συνεχίζουν να το χρησιμοποιούν όπως και πριν, έχοντας τώρα μια επιπλέον παράμετρο ασφάλειας.
Περικλείουσες υπογραφές: Οι περικλείουσες υπογραφές αποτελούν ένα «δοχείο» για το ίδιο το έγγραφο που υπογράφεται. Το βασικό έγγραφο είναι η ίδια η υπογραφή, που περιλαμβάνει το υπογεγραμμένο έγγραφο ως βασικό κομμάτι της. Το κύριο πρόβλημα αυτής της προσέγγισης είναι ότι τα υπογεγραμμένα δεδομένα πρέπει να εξαχθούν απο το «δοχείο» αυτό πριν γίνει η επεξεργασία τους απο μια εφαρμογή. Μια περικλείουσα υπογραφή είναι παρόμοια με σύγχρονα συστήματα παραγωγής υπογραφών όπως αυτά που βασίζονται στο PGP ή το S/MIME.
Αποσπασμένες υπογραφές: Οι αποσπασμένες υπογραφές αφήνουν το υπογεγραμμένο έγγραφο όπως ακριβώς είναι στην αρχική του μορφή, και τα δεδομένα της υπογραφής παρέχονται ξεχωριστά, σε άλλο έγγραφο. Οι δύο οντότητες, έγγραφο και υπογραφή, πρέπει να μεταφέρονται μαζί. Σε όρους συστήματος αρχείων, η υπογραφή αποθηκεύεται σε ένα ξεχωριστό αρχείο. Οι εφαρμογές μπορούν να επεξεργάζονται το αρχείο του υπογεγραμμένου εγγράφου όπως και πριν την παραγωγή της υπογραφής. Η χρήση ενός ξεχωριστού αντικειμένου για την υπογραφή έχει το αρνητικό ότι αυξάνει την πολυπλοκότητα της ενσωμάτωσης της ασφάλειας που προσφέρουν στο σύστημα λόγω του ότι πρέπει κάθε στιγμή να μεταφέρονται δύο διαφορετικά αρχεία.

Παράδειγμα
Το απόσπασμα κειμένου XML που ακολουθεί αποτελεί ένα παράδειγμα μιας αποσπασμένης Υπογραφής XML.

```
<Signature xmlns=”http://www.w3.org/2000/09/xmldsig#”>
        <SignedInfo>
            <CanonicalizationMethod Algorithm=”http://www.w3.org/TR/2001/RECxml-
c14n-20010315”/>
            <SignatureMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#dsasha1”/>
            <Reference URI=”http://www.mycompany.com/order/”>
                <Transforms>
                    <Transform Algorithm=”http://www.w3.org/TR/2001/REC-xmlc14n-
20010315”/>
                </Transforms>
                <DigestMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#sha1”/>
                    <DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
            </Reference>
        </SignedInfo>
        <SignatureValue>MC0CFFrVLtRlk=...</SignatureValue>
        <KeyInfo>
            <KeyValue>
              <DSAKeyValue>
                <P>...</P>
                <Q>...</Q>
                <G>...</G>
                <Y>...</Y>
              </DSAKeyValue>
```

```
                </KeyValue>
            </KeyInfo>
</Signature>
```

Παράδειγμα αποσπασμένης υπογραφής XML με DSA

Το στοιχείο SignatureMethod καθορίζει τον αλγόριθμο της υπογραφής και της συνάρτησης κατακερματισμού που στην προκειμένη περίπτωση είναι οι DSA και SHA-1 αντιστοίχως. Καθορίζεται επίσης ο μετασχηματισμός κανονικοποίησης. Τα δεδομένα που υπογράφονται αναγνωρίζονται απο το χαρακτηριστικό URI του στοιχείου αναφοράς Reference. Στο παράδειγμα υπάρχει μόνο ένα στοιχείο Reference και αναγνωρίζει ένα άλλο έγγραφο (ανεξάρτητο) που ονομάζεται order. Η συνάρτηση κατακερματισμού και ο μετασχηματισμός που εφαρμόζονται, περιέχονται σε στοιχεία παιδιά του στοιχείου αναφοράς. Επιπρόσθετα, το δημόσιο κλειδί DSA που θα χρησιμοποιηθεί για να επαληθευτεί η υπογραφή, είναι επίσης παρόν. Τονίζεται ότι το απλό αυτό παράδειγμα χρησιμοποιεί μόνο το κλειδί για την επαλήθευση και όχι ένα ολόκληρο πιστοποιητικό. Με τον τρόπο αυτό πετυχαίνεται η ελάχιστη ασφάλεια για την υπογραφή, αφού ο παραλήπτης του μηνύματος δεν έχει κάποιο τρόπο να επιβεβαιώσει ότι ο υπογράφων είναι κάποιο πρόσωπο που εμπιστεύεται. Στην περίπτωση που η χρήση μιας Υποδομής Δημοσίου Κλειδιού θεωρείται πολύπλοκη και δαπανηρή, ένας καλύτερος τρόπος χειρισμού του συγκεκριμένου μηνύματος είναι να έχει προηγηθεί η ανταλλαγή του κλειδιού με τον παραλήπτη και στο μήνυμα να υπάρχει μόνο μια αναφορά στο κλειδί.

4.4 Προηγμένες Ηλεκτρονικές Υπογραφές XML – XadES

Τα πρότυπα ETSI TS 101 733 και ETSI 101 903

Η Ευρωπαϊκή Οδηγία για το κοινοτικό πλαίσιο Ηλεκτρονικών Υπογραφών, καθορίζει την ηλεκτρονική υπογραφή ως: «δεδομένα σε ηλεκτρονική μορφή που είναι ενσωματωμένα ή είναι λογικά συσχετισμένα με άλλα ηλεκτρονικά δεδομένα και εξυπηρετούν ως ένα μέσο αυθεντικοποίησης.»

Το πρότυπο του ETSI TS 101 733, δημιουργήθηκε με σκοπό να καλύψει την παραγωγή και επαλήθευση ηλεκτρονικών υπογραφών για διάφορους τύπους συναλλαγών, συμπεριλαμβανομένων των εμπορικών συναλλαγών (για παράδειγμα αγορά, δημιουργία συμβολαίου ή τιμολογίων). Το πρότυπο μπορεί να χρησιμοποιηθεί για οποιαδήποτε συναλλαγή ανάμεσα σε έναν ιδιώτη και μια εταιρία, ανάμεσα σε δύο εταιρίες, έναν ιδιώτη και έναν δημόσιο οργανισμό κλπ.

Μια ηλεκτρονική υπογραφή που παράγεται σύμφωνα με το ETSI TS 101 733, παρέχει αποδεικτικά στοιχεία τα οποία μπορούν να υποστούν επεξεργασία προκειμένου να είναι κάποιος σίγουρος ότι μια συγκεκριμένη δέσμευση έχει γίνει αποδεκτή κάτω από μια δεδομένη *πολιτική υπογραφής*, σε μια δεδομένη χρονική στιγμή, από έναν υπογράφοντα με δεδομένο αναγνωριστικό όπως είναι ένα όνομα ή ένα ψευδώνυμο και προαιρετικά ένα ρόλο. Η πολιτική υπογραφής καθορίζει τις τεχνικές και διαδικαστικές απαιτήσεις για τη δημιουργία και επαλήθευση της υπογραφής προκειμένου να καλύπτεται μια συγκεκριμένη επιχειρηματική ανάγκη. Το υποκείμενο νομικό πλαίσιο μπορεί να αναγνωρίζει μια συγκεκριμένη πολιτική υπογραφής ως κατάλληλη γι' αυτό. Για παράδειγμα, μια συγκεκριμένη πολιτική υπογραφής μπορεί να αναγνωρίζεται από ένα δικαστήριο ως κατάλληλη για να καλύψει της ανάγκες της Ευρωπαϊκής Οδηγίας για το ηλεκτρονικό εμπόριο.

Το πρότυπο ETSI TS 101 733 καθορίζει τη μορφή των προηγμένων ηλεκτρονικών υπογραφών που παραμένουν έγκυρες για μεγάλα χρονικά διαστήματα, συμμορφώνονται με την Ευρωπαϊκή Οδηγία και ενσωματώνουν επιπρόσθετη χρήσιμη πληροφορία για συχνές και συνηθισμένες περιπτώσεις. Επί του παρόντος, το πρότυπο χρησιμοποιεί την Abstract Syntax Notation 1 (ASN.1) και βασίζεται στην δομή που καθορίζεται στο RFC 2630.

Η Ομάδα Εργασίας του W3C για τις υπογραφές XML, έχει παράγει μια σύνταξη για τις Ψηφιακές Υπογραφές XML. Η σύνταξη αυτή παρέχει την βασική λειτουργικότητα για την

ταυτόχρονη υπογραφή αρκετών αντικειμένων δεδομένων. Παρέχει επίσης τα βασικά μέσα για την ενσωμάτωση οποιασδήποτε επιπρόσθετης χαρακτηρίζουσας πληροφορίας.
Το πρότυπο ETSI TS 101 903 με τη σειρά του, καθορίζει μορφές εγγράφων XML για προηγμένες ηλεκτρονικές υπογραφές που παραμένουν έγκυρες μετά από μεγάλες χρονικές περιόδους, συμμορφώνονται με την Ευρωπαϊκή Οδηγία και ενσωματώνουν επιπρόσθετη χρήσιμη πληροφορία για συχνές και συνηθισμένες περιπτώσεις, υλοποιώντας τα εξής:

- ✓ Προτείνοντας τους ορισμούς ενός Σχήματος XML για νέους τύπους XML που θα μπορούν να περιέχουν την πληροφορία για να καλύψουν την απαίτηση για μακροπρόθεσμη εγκυρότητα καθώς και τις απαιτήσεις που επιβάλλονται από σύγχρονες επιχειρηματικές διαδικασίες και την Ευρωπαϊκή Οδηγία. Οι υπογραφές αυτές χτίζονται πάνω στο πρότυπο των Ψηφιακών Υπογραφών XML με την προσθήκη της παραπάνω πληροφορίας χρησιμοποιώντας το στοιχείο XML Object όπως αυτό ορίστηκε στο πρότυπο των Ψηφιακών Υπογραφών XML.
- ✓ Καθορίζοντας τους μηχανισμούς που χρησιμοποιούνται για την παραγωγή της προαναφερθείσας επιπρόσθετης χαρακτηρίζουσας πληροφορίας.

Το πρότυπο ETSI TS 101 903 (γνωστό και ως Προηγμένες Ψηφιακές Υπογραφές XML – XML Advanced Electronic Signatures ή XAdES), καθορίζει δύο βασικούς τύπους ιδιοτήτων: *υπογεγραμμένες ιδιότητες (signed properties)* και *μη υπογεγραμμένες ιδιότητες (unsigned properties)*. Οι πρώτες είναι πρόσθετα αντικείμενα δεδομένων που επίσης διασφαλίζονται από την υπογραφή που παράγεται από τον υπογράφοντα στο στοιχείο SignedInfo (βλ. και παράγραφο 2.2.2.1), κάτι που υπονοεί ότι ο υπογράφων έχει αυτά τα αντικείμενα δεδομένων, εφαρμόζει μια κρυπτογραφική συνάρτηση κατακερματισμού πάνω σε όλα και παράγει ένα αντίστοιχο στοιχείο αναφοράς Reference. Οι μη υπογεγραμμένες ιδιότητες είναι αντικείμενα δεδομένων που προστίθενται από τον υπογράφοντα, από τον επαληθευτή της υπογραφής ή άλλες οντότητες μετά την παραγωγή της υπογραφής. Δεν διασφαλίζονται από την υπογραφή στο στοιχείο Signature (που παράγεται από τον υπογράφοντα). Παρ' όλα αυτά, υπάρχει το ενδεχόμενο να υπογραφούν από άλλες οντότητες (χρονοσφραγίδες, πρόσθετες υπογραφές, πιστοποιητικά και λίστες ανάκλησης πιστοποιητικών ΛΑΣ είναι πιθανά περιεχόμενα των μη υπογεγραμμένων ιδιοτήτων).
Η επαλήθευση μια προηγμένης ηλεκτρονικής υπογραφής βάσει του XAdES απαιτεί:

- ✓ Μια προηγμένη ηλεκτρονική υπογραφή που έχει δημιουργηθεί βάσει του προτύπου Ψηφιακών Υπογραφών XML του W3C με την ενσωμάτωση της επιπρόσθετης χαρακτηρίζουσας πληροφορίας. Αυτή είναι:
  - Οι αναφορές στα **υπογεγραμμένα αντικείμενα**.
  - Οι **υπογεγραμμένες ιδιότητες** (που παρέχονται από τον υπογράφοντα).
  - Η ίδια η **υπογραφή** όπως καθορίζεται στο πρότυπο Ψηφιακών Υπογραφών XML.
- ✓ Δεδομένα επαλήθευσης, που αποτελούν τα επιπρόσθετα δεδομένα που απαιτούνται για την επαλήθευση της ηλεκτρονικής υπογραφής. Περιλαμβάνουν:
  - Ψηφιακά πιστοποιητικά.
  - Πληροφορία ανάκλησης πιστοποιητικών.
  - Χρονοσφραγίδες από Αρχές Χρονοσφράγισης.

Τα **υπογεγραμμένα αντικείμενα** αποτελούν τα έγγραφα, στοιχεία, κλπ που ο χρήστης ήθελε να υπογράψει.
Οι **υπογεγραμμένες ιδιότητες** περιλαμβάνουν οποιαδήποτε επιπρόσθετη πληροφορία που θα υπογραφεί από τον χρήστη προκειμένου να είναι συμβατή με την ακολουθούμενη πολιτική υπογραφής ή το ίδιο το πρότυπο (π.χ. τον χρόνο παραγωγής της υπογραφής).
Τα **δεδομένα επαλήθευσης** ενδέχεται να συλλέγονται είτε από τον υπογράφοντα ή από τον επαληθεύοντα ή και τους δύο και θα καλύπτουν τις απαιτήσεις της πολιτικής υπογραφής. Τα δεδομένα αυτά περιλαμβάνουν πιστοποιητικά ΑΠ και πληροφορία κατάστασης ανάκλησης πιστοποιητικών με τη μορφή ΛΑΠ ή πληροφορία όπως λαμβάνεται από μια online υπηρεσία (π.χ. μέσω των πρωτοκόλλων OCSP (Online Certificate Status Protocol) ή SCVP (Simple

Certificate Validation Protocol)). Επιπρόσθετα δεδομένα είναι χρονοσφραγίδες. Από το πρότυπο απαιτείται ως ελάχιστο, ότι είτε ο υπογράφοντας είτε ο επαληθεύων ζητούν μια χρονοσφραγίδα πάνω στα δεδομένα της υπογραφής.

Μορφή / Δομή
Το πρότυπο καθορίζει έξι μορφές προηγμένων ηλεκτρονικών υπογραφών XML με αυξανόμενο επίπεδο πολυπλοκότητας.
Οι τρεις πρώτες πιο απλές μορφές είναι:

- ✓ Η *Προηγμένη Ηλεκτρονική Υπογραφή XML (XML Advanced Electronic Signature – XAdES)*.
- ✓ Η *XAdES με Χρονοσφραγίδα (XAdES with Time-Stamp ή XAdES-T)*.
- ✓ Η *XAdES με πλήρη Δεδομένα Επαλήθευσης (XAdES with Complete Validation Data ή XAdES-C)*.

Οι δύο επόμενες μορφές καλύπτουν ένα πιο αυξημένο σύνολο απαιτήσεων και ονομάζονται *XAdES-X* και *XAdES-X-L* και θα περιγραφούν συνοπτικά στη συνέχεια. Το τελευταίο είδος ονομάζεται *XAdES-A* και αποτελεί μια μορφή για την ασφαλή αποθήκευση υπογραφών κατά έναν τρόπο ώστε να προστατεύονται αν η κρυπτογραφική πληροφορία αποδυναμωθεί (π.χ. με το σπάσιμο ενός αλγορίθμου κλπ.).

Προηγμένη Ηλεκτρονική Υπογραφή XML – XAdES
Η σχηματική αναπαράσταση της δομή μιας υπογραφής XAdES είναι η ακόλουθη.

Προηγμένη Ηλεκτρονική Υπογραφή XML - XAdES

Η υπογραφή XAdES προσθέτει τα στοιχεία SignedProperties και UnsignedProperties για να περιληφθούν οι υπογεγραμμένες και μη υπογεγραμμένες πληροφορίες σύμφωνα με το πρότυπο.
Συνοπτικά τα στοιχεία που απαρτίζουν τις υπογεγραμμένες ιδιότητες είναι τα εξής:

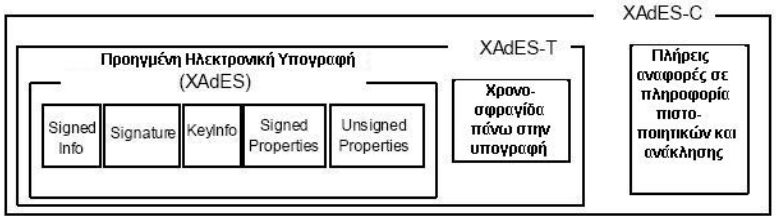
- ✓ Ο χρόνος υπογραφής (στοιχείο SigningTime).
- ✓ Το πιστοποιητικό υπογραφής (στοιχείο SigningCertificate).
- ✓ Το αναγνωριστικό της χρησιμοποιούμενης πολιτικής υπογραφής (στοιχείο SignaturePolicyIdentifier).
- ✓ Τα στοιχεία του τόπου παραγωγής της υπογραφής (στοιχείο SignatureProductionPlace).
- ✓ Ο ρόλος του υπογράφοντα (στοιχείο SingerRole).
- ✓ Μια χρονοσφραγίδα πάνω σε όλες τις αναφορές των υπογεγραμμένων δεδομένων (στοιχείο AllDataObjectsTimeStamp) ή εναλλακτικά μια χρονοσφραγίδα πάνω σε αναφορές ορισμένων από τα υπογεγραμμένα δεδομένα (IndividualDataObjectsTimeStamp).
- ✓ Τα χαρακτηριστικά των υπογεγραμμένων δεδομένων (στοιχείο DataObjectFormat).
- ✓ Τον τύπο της δέσμευσης (στοιχείο CommitmentTypeIndication).

Οι μη υπογεγραμμένες ιδιότητες περιλαμβάνουν μια υπογραφή αντισυμβαλλόμενου (στοιχείο CounterSignature).

Η μορφή XAdES καλύπτει τις νομικές προϋποθέσεις για προηγμένες ηλεκτρονικές υπογραφές όπως καθορίζονται στην Οδηγία της Ευρωπαϊκής Επιτροπής για ηλεκτρονικές υπογραφές. Παρέχει βασική αυθεντικοποίηση και προστασία ακεραιότητας και μπορεί να δημιουργηθεί χωρίς την πρόσβαση σε online υπηρεσίες Χρονοσφράγισης. Παρ' όλα αυτά χωρίς την προσθήκη μιας χρονοσφραγίδας στην υπογραφή ή ένα άλλο ασφαλές αρχείο χρόνου, η ηλεκτρονική υπογραφή δεν προστατεύει ενάντια στην απειλή ο υπογράφων αργότερα να αρνηθεί ότι δημιούργησε την υπογραφή, δηλαδή δεν παρέχει την μη-άρνηση συμμετοχής (non-repudiation).

XAdES με Χρονοσφραγίδα - XAdES-T και XAdES με Πλήρη Δεδομένα Επαλήθευσης – XAdES-C

Η Προηγμένη Ηλεκτρονική Υπογραφή με Χρονοσφραγίδα XAdES-T προσθέτει στη XAdES μια χρονοσφραγίδα, προκειμένου ο υπογράφων να κάνει τα πρώτα βήματα για την παροχή μακροπρόθεσμης επαλήθευσης. Αυτή η μορφή ή κάποιο άλλο στοιχείο χρόνου θα πρέπει να δημιουργείται κοντά στη χρονική στιγμή της παραγωγής της υπογραφής για να παρασχεθεί προστασία από άρνηση δημιουργίας της.
Η Προηγμένη Ηλεκτρονική Υπογραφή με Πλήρη Δεδομένα Επαλήθευσης – XAdES-C προσθέτει στην XAdES-T τις αναφορές σε ένα σύνολο δεδομένων που υποστηρίζουν την εγκυρότητα της υπογραφής, για παράδειγμα τις αναφορές σε πιστοποιητικά και την αντίστοιχη πληροφορία ανάκλησης των πιστοποιητικών αν υπάρχει. Σημειώνεται ότι στην υπογραφή ενσωματώνονται μόνο **αναφορές** στην πληροφορία και όχι το ίδιο το περιεχόμενο της πληροφορίας, που θα ήταν πολύ μεγαλύτερο.
Η σχηματική αναπαράσταση της XAdES-T και της XAdES-C είναι η ακόλουθη:



XAdES-T και XAdES-C

Η XAdES-T όπως προαναφέρθηκε θα πρέπει να δημιουργείται κοντά στο χρονικό σημείο που δημιουργήθηκε η XAdES για προστασία από άρνηση συμμετοχής στη δημιουργία της αργότερα. Στο χρονικό αυτό σημείο ενδέχεται να μην είναι διαθέσιμη ακόμη η πληροφορία για συνολική επαλήθευση της υπογραφής, ή να είναι διαθέσιμο κάποιο μέρος της με το οποίο μπορούν να γίνουν κάποιοι αρχικοί έλεγχοι.
Και για τις δύο περιπτώσεις υπογραφών, αν ο υπογράφων δημιουργήσει μόνο την βασική XAdES υπογραφή, ο επαληθεύων την υπογραφή θα πρέπει να δημιουργήσει τις XAdES-T και XAdES-C μορφές με την πρώτη ευκαιρία. Αυτό θα παρέχει τα επιπρόσθετα δεδομένα τουλάχιστον την στιγμή που πρώτη φορά η υπογραφή επαληθεύεται και η οποία θεωρητικά είναι κοντά στην στιγμή της δημιουργίας της.

Επεκτάσιμες μορφές XAdES

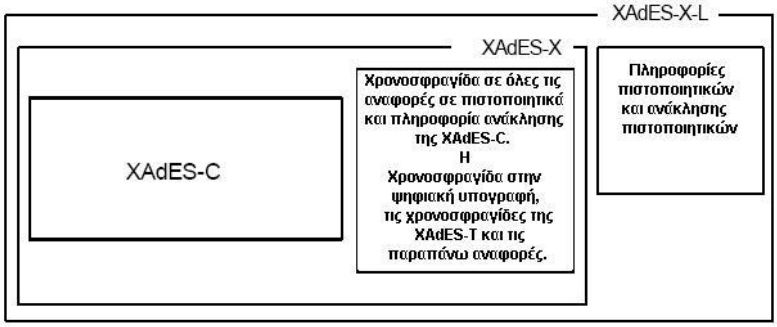
Η πρώτη επεκτάσιμη μορφή XAdES είναι η XAdES-X ή XAdES με Εκτεταμένα Δεδομένα Επαλήθευσης (XAdES with eXtended Validation Data).
Οι μορφές αυτές δημιουργούνται στις παρακάτω περιπτώσεις:

- ✓ Αν υπάρχει κίνδυνος ότι κάποια από τα κλειδιά που χρησιμοποιούνται στην αλυσίδα πιστοποιητικών ή στην πληροφορία ανάκλησης πιστοποιητικών έχουν αποκαλυφθεί. Η περίπτωση ενός σπασμένου αλγορίθμου είναι διαφορετική και καλύπτεται στη συνέχεια από την μορφή XAdES-A. Για την μορφή XAdES-X είναι απαραίτητο να χρονοσφραγισθούν όλες οι αναφορές σε πιστοποιητικά και πληροφορία ανάκλησης

πιστοποιητικών που περιέχονται στη XAdES-C. Εναλλακτικά, η χρονοσφραγίδα μπορεί να εφαρμοστεί στην ψηφιακή υπογραφή (το στοιχείο Signature), τις χρονοσφραγίδες που εμφανίζονται στην μορφή XAdES-T και τις παραπάνω αναφορές.

- ✓ Αν τα δεδομένα πιστοποιητικών και η πληροφορία ανάκλησης πιστοποιητικών δεν αποθηκεύονται για μεγάλο χρονικό διάστημα, τότε επιβάλλεται να προστεθούν στην ίδια την υπογραφή. Έτσι προκύπτει η XAdES-X-L μορφή.

Σχηματικά αναπαρίστανται στο ακόλουθο σχήμα:



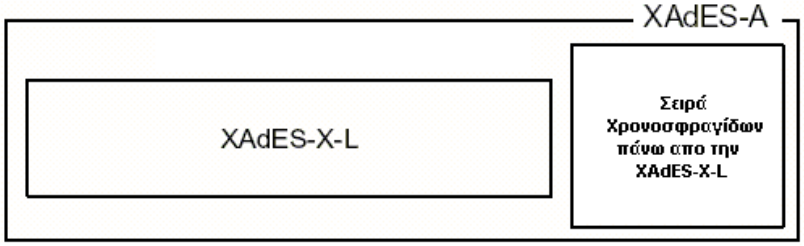
XAdES-X και XAdES-X-L

Οι προδιαγραφές του προτύπου καθορίζουν ότι η χρονοσφραγίδα πάνω στις αναφορές των πιστοποιητικών και πληροφορίας ανάκλησης μπορεί να παραληφθεί και να προστεθούν τα ίδια τα δεδομένα των πιστοποιητικών και ανάκλησης.

Η μορφή XAdES-X-L παράγεται επί της ουσίας με την ενσωμάτωση των δεδομένων αυτών ως στοιχεία XML αφότου μετασχηματιστούν κατά base64, εφόσον είναι δυαδικά δεδομένα τύπου ΛΑΠ ή απάντησης ενός εξυπηρετητή OCSP.

Μορφή XAdES Αρχειοθέτησης Δεδομένων Επαλήθευσης

Η μορφή Αρχειοθέτησης Δεδομένων Επαλήθευσης XAdES-A (Archive Validation Data) παρουσιάζεται στο ακόλουθο σχήμα:



XAdES-A

Προτού αλγόριθμοι, κλειδιά και τα υπόλοιπα κρυπτογραφικά δεδομένα που έχουν χρησιμοποιηθεί στη μορφή XAdES-C γίνουν παρωχημένα ή αδύναμα, η μορφή XAdES-X-L θα πρέπει να χρονοσφραγηθεί. Εάν είναι δυνατόν, αυτό θα πρέπει να γίνει με την εφαρμογή ισχυρότερων αλγορίθμων (ή μεγαλύτερα μήκη κλειδιών) από τα ήδη χρησιμοποιημένα για την παραγωγή των αρχικών χρονοσφραγίδων. Τα επιπρόσθετα αυτά δεδομένα και η χρονοσφραγίδα ονομάζονται μορφή Αρχειοθέτησης Δεδομένων Επαλήθευσης ή XAdES-A Η διαδικασία αυτή μπορεί να επαναλαμβάνεται κάθε φορά που η προστασία που χρησιμοποιήθηκε για την χρονοσφράγιση της προηγούμενης XAdES-A αποδυναμώνεται. Συνεπώς η XAdES-A μπορεί να φέρει πολλαπλές ενσωματωμένες χρονοσφραγίδες. Η υποστήριξη μια υλοποίησης του XAdES για την μορφή XAdES-A είναι προαιρετική.

5 ΠΡΌΤΥΠΑ ΥΠΗΡΕΣΙΏΝ ΙΣΤΟΎ

5.1 ΤΟ ΠΡΟΤΥΠΟ SOAP

Το *SOAP* (που αρχικά αποτελούσε ακρωνύμιο των όρων Απλό Πρωτόκολλο Πρόσβασης σε Αντικείμενα – Simple Object Access Protocol, αλλά στη συνέχεια παρέμεινε στην βιβλιογραφία απλά ως SOAP), είναι ένα πρωτόκολλο βασισμένο σε επικοινωνία με XML για την ανταλλαγή μηνυμάτων. Δημιουργήθηκε για να δώσει λύση σε προβλήματα διαλειτουργικότητας ανάμεσα σε κατανεμημένες εφαρμογές. Οι προδιαγραφές του μεγάλωσαν τα τελευταία τέσσερα χρόνια και αυτή τη στιγμή βρίσκεται στην έκδοση 1.2. Οι προδιαγραφές του επίσης έχουν κατατεθεί στο W3C προκειμένου να αποτελέσει πρότυπο παρόμοια με το HTTP και την XML.
Το βασικό χαρακτηριστικό του SOAP είναι η απλότητά του. Είναι σχετικά εύκολο για κάποιον να υλοποιήσει μια απλή εφαρμογή που να υποστηρίζει το SOAP χρησιμοποιώντας μια απο τις διαδεδομένες γλώσσες προγραμματισμού και να έχει πρόσβαση σε μια άλλη εφαρμογή εξυπηρετητή που υποστηρίζει SOAP και είναι γραμμένη σε μια άλλη γλώσσα.

Σκοπός

Το SOAP είναι μια μέθοδος για την αποστολή και λήψη πληροφορίας πάνω απο ένα δίκτυο, όπως το διαδίκτυο με χρήση της XML. Υπάρχουν διαφορετικοί τρόποι για να χρησιμοποιήσει κάποιος το SOAP. Στην πιο απλή μορφή του, μπορεί κάποιος να χρησιμοποιήσει έναν απλό φυλλομετρητή ιστού για να αποκτήσει πρόσβαση στον εξυπηρετητή ιστού μιας δικτυακής τοποθεσίας που προσφέρει μια διεπαφή για την κλήση αντικειμένων. Η τεχνική λύση που υποστηρίζει το SOAP είναι κρυμμένη πίσω απο την διεπαφή αυτή.
Ένας εναλλακτικός τρόπος χρήσης του SOAP είναι η ενσωμάτωσή του σε μια εφαρμογή η οποία χρησιμοποιεί μηνύματα XML για να αποστείλει πληροφορία σε έναν εξυπηρετητή που περιέχει αντικείμενα που χρησιμοποιούνται απο την εφαρμογή. Η εφαρμογή αποτελεί ένα «κέλυφος» που βρίσκεται στον τοπικό υπολογιστή και επιτρέπει τις κλήσεις στον εξυπηρετητή όπου βρίσκονται τα αντικείμενα και τα δεδομένα. Κατ' αυτόν τον τρόπο, οι εφαρμογές «πελάτες» δεν χρειάζεται να αλλάζονται κάθε φορά που γίνονται αλλαγές στα αντικείμενα. Επίσης έτσι εξασφαλίζεται ότι τα δεδομένα αποθηκεύονται σε ένα ασφαλές περιβάλλον και ελέγχεται η πρόσβαση σε αυτά.
Το SOAP έχει σχεδιαστεί με τρεις βασικούς σχεδιαστικούς στόχους:

- Να παρέχει ένα προτυποποιημένο πρωτόκολλο κλήσης αντικειμένων βασισμένο σε άλλα πρότυπα του Διαδικτύου, χρησιμοποιώντας το HTTP για μεταφορά και την XML για την δόμηση των δεδομένων.
- Να αποτελεί ένα επεκτάσιμο πρωτόκολλο και μορφή δεδομένων μηνυμάτων που μπορεί να εξελιχθεί.
- Να είναι απλό.

Ο πρώτος στόχος κάνει το SOAP ευέλικτο ώστε να μπορεί να ενσωματωθεί σε συστήματα και να υποστηριχθούν οι Υπηρεσίες Ιστού που έχουν υλοποιηθεί σε διαφορετικές πλατφόρμες και με διαφορετικές γλώσσες προγραμματισμού. Το οικοδόμημα των Υπηρεσιών Ιστού βασίζεται στην ικανότητα ακριβώς της αποστολής και λήψης μηνυμάτων σε μια προτυποποιημένη μορφή κατανοητή απο όλα τα συστήματα.

Μορφή / Δομή

Μια διαδικασία παράδειγμα που επιδεικνύει την δημιουργία και αποστολή ενός σύγχρονου μηνύματος SOAP περιλαμβάνει πέντε βήματα:

1. Δημιουργία της σύνδεσης SOAP.
2. Δημιουργία του μηνύματος SOAP.
3. Συμπλήρωση του μηνύματος με δεδομένα.
4. Αποστολή του μηνύματος.

5. Λήψη της απάντησης.

Οι κανόνες κωδικοποίησης που ορίζονται για διάφορους τύπους δεδομένων μπορούν να σειριοποιηθούν με χρήση *αιτήσεων SOAP (SOAP requests)*. Οι προδιαγραφές 1.1 του SOAP βασίζουν την κωδικοποίηση δεδομένων σε δομές Σχημάτων XML και τύπους δεδομένων Σχημάτων XML, αλλά επιτρέπουν και κωδικοποιήσεις όπως η RDF. Οι υποστηριζόμενοι τύποι περιλαμβάνουν απλούς τύπους όπως είναι οι συμβολοακολουθίες (strings), καθώς και πολύπλοκους τύπους όπως είναι οι δομές (structures) και οι πίνακες (arrays). Οι προδιαγραφές επίσης περιγράφουν μια σύμβαση για την υλοποίηση αλληλεπιδράσεων RPC με χρήση της XML. Τα μηνύματα SOAP μπορούν να αποσταλούν πάνω απο οποιοδήποτε πρωτόκολλο μεταφοράς συμπεριλαμβανομένων των HTTP(S), SMTP και FTP.
Ένα μήνυμα SOAP περιέχει τρία βασικά τμήματα:

- έναν *φάκελο (envelope)*
- μια *επικεφαλίδα (header)* για την προσθήκη στο μήνυμα SOAP χαρακτηριστικών που εξαρτώνται απο την εκάστοτε εφαρμογή (για παράδειγμα πληροφορίες αυθεντικοποίησης)
- ένα *σώμα (body)* που περιέχει την πληροφορία που ενδιαφέρει τον παραλήπτη του μηνύματος

Το επόμενο σχήμα επιδεικνύει πως θα μπορούσε να γραφτεί σε SOAP ένα παράδειγμα αίτησης και απάντησης απο μια υπηρεσία:

Request

```
POST /StockQuote HTTP/1.1
Host: www.stockquoteserver.com
Content-Type: text/xml
Content-Length: nnnn
SOAPAction: "Some-URI"

<SOAP:Envelope
xmlns:SOAP="urn:schemas.xmlsoap.org:soap.v1">
<SOAP:Header>
       <t:Transaction xmlns:t="URI"
mustUnderstand="1">5</t:Transaction>
     </SOAP:Header>
     <SOAP:Body>
          <m:GetLastTradePrice
xmlns:m="URI">
               <symbol>DIS</symbol>
          </m:GetLastTradePrice>
     </SOAP:Body>
</SOAP:Envelope>
```

Response

```
HTTP/1.1 200 OK
Content-Type: text/xml
Content-Length: nnnn

<SOAP:Envelope
xmlns:SOAP="urn:schemas.xmlsoap.org:soap.v1">
    <SOAP:Header>
       <t:Transaction xmlns:t="URI"
xsi-type="xsd:int"
mustUnderstand="=">5</t:Transaction>
</SOAP:Header>
<SOAP:Body>
<m:GetLastTradePriceResponse
xmlns:m="URI">
<return>34.5</return>
</m:GetLastTradePriceResponse>
</SOAP:Body>
</SOAP:Envelope>
```

Ένα παράδειγμα αίτησης και απάντησης με SOAP

Ένας εξυπηρετητής εφαρμογών που λαμβάνει ένα μήνυμα SOAP πρέπει να αναγνωρίσει όλα τα κομμάτια που περιέχει, να επαληθεύσει ότι είναι ολοκληρωμένα και να τα επεξεργαστεί. Επειδή ένα μήνυμα SOAP μπορεί να ταξιδέψει διαμέσου πολλών ενδιάμεσων σταθμών, ένα *χαρακτηριστικό δράστη (actor attribute)* χρησιμοποιείται για να υποδειχθεί ο τελικός παραλήπτης του μηνύματος. Οι προδιαγραφές επίσης καθορίζουν ένα *χαρακτηριστικό υποχρεωτικής κατανόησης (mustUnderstand attribute)*, το οποίο καθορίζει εάν μια συγκεκριμένη καταχώρηση στην επικεφαλίδα πρέπει να είναι κατανοητή και να υποστεί επεξεργασία από τον παραλήπτη.

5.2 ΓΛΩΣΣΑ ΠΕΡΙΓΡΑΦΗΣ ΥΠΗΡΕΣΙΩΝ ΙΣΤΟΥ

Η *Γλώσσα Περιγραφής Υπηρεσιών Ιστού (Web Services Description Language - WSDL)* αποτελεί μια μορφή εγγράφου σε XML η οποία είναι δημιουργούμενη απο υπολογιστές και

κατανοητή απο αυτούς για την περιγραφή υπηρεσιών δικτύου ως ένα σύνολο απο *σημεία τερματισμού (endpoint)* που βασίζονται σε μηνύματα με περιεχόμενο είτε πληροφορία *προσανατολισμένη σε έγγραφα (document-oriented)* είτε *προσανατολισμένη σε διαδικασίες (procedure-oriented)*. Τα έγγραφα WSDL περιγράφουν ορισμένες αφηρημένες και ορισμένες συγκεκριμένες λεπτομέρειες των υπηρεσιών δικτύου. Οι αφηρημένες λεπτομέρειες περιγράφουν λειτουργίες και χαρακτηριστικά μηνυμάτων των υπηρεσιών δικτύου που ισχύουν ανεξάρτητα απο την εκάστοτε υλοποίηση. Οι συγκεκριμένες λεπτομέρειες δεσμεύουν τις αφηρημένες σε ένα συγκεκριμένο δικτυακό πρωτόκολλο και μορφή μηνύματος, προκειμένου να ορίσουν το σημείο τερματισμού. Συνδυασμένα συσχετιζόμενα σημεία τερματισμού σχηματίζουν την δικτυακή υπηρεσία. Η WSDL είναι επεκτάσιμη για να επιτρέπει την περιγραφή των σημείων τερματισμού ανεξάρτητα απο την μορφή των μηνυμάτων ή το πρωτόκολλο επικοινωνίας. Οι προδιαγραφές *δεσμεύσεων (bindings)* που υπάρχουν μέχρι στιγμής, περιγράφουν πώς μπορεί να χρησιμοποιηθεί η WSDL σε συνδυασμό με το SOAP, HTTP GET/POST και το MIME.
Η WSDL (αυτή τη στιγμή στην έκδοση 2.0) είναι προσχέδιο προτύπου του W3C το οποίο έχει κατατεθεί απο τις Ariba, IBM και Microsoft ως πρόταση περιγραφής υπηρεσιών. Παρ' όλο που η τεχνολογία είναι ακόμη υπό σχεδιασμό, σχεδόν όλοι οι οργανισμοί που ασχολούνται με τις υπηρεσίες ιστού παρέχουν υποστήριξη για την WSDL και διαθέτουν εργαλεία για την παραγωγή αρχείων WSDL.

Σκοπός

Προτού μια εφαρμογή μπορέσει να έχει πρόσβαση σε μια υπηρεσία ιστού, θα πρέπει να μάθει με έναν δομημένο τρόπο τις διαθέσιμες λειτουργίες που προσφέρονται και τις δομές μηνυμάτων που χρησιμοποιούνται. Τα έγγραφα WSDL καλύπτουν αυτή την ανάγκη περιγραφής της διεπαφής ενός μηνύματος SOAP, παρέχοντας σε ένα έγγραφο XML τεχνικές πληροφορίες για τις λεπτομέρειες κλήσης μιας υπηρεσίας ιστού, την τοποθεσία της στο δίκτυο και τον ορισμό της δομής των μηνυμάτων που κατανοεί. Στα έγγραφα WSDL γίνεται αναφορά μέσω περιγραφών URL που αποθηκεύονται σε βάση δεδομένων που προσφέρουν υπηρεσίες αναζήτησης.
Τα έγγραφα WSDL παίζουν έναν σημαντικό ρόλο στις αλληλεπιδράσεις ανάμεσα σε υπηρεσίες ιστού. Όταν μια υπηρεσία ιστού δημοσιεύεται, ένας διαχειριστής τοποθετεί έναν δεσμό στην περιγραφή WSDL της υπηρεσίας σε μια σχετική βάση δεδομένων. Κατ' αυτό τον τρόπο, η περιγραφή WSDL είναι διαθέσιμη ως αποτέλεσμα σε αναζητήσεις εφαρμογών πελατών που ψάχνουν στην βάση για μια υπηρεσία. Μια εφαρμογή πελάτης αποκτά πρόσβαση στην περιγραφή WSDL για να βρει πληροφορίες για μια υπηρεσία και να μπορέσει να δημιουργήσει ένα μήνυμα SOAP με την κατάλληλη δομή. Στην συνέχεια, η εφαρμογή πελάτης καλεί την υπηρεσία.

Δομή

Ένα έγγραφο WSDL χρησιμοποιεί τα ακόλουθα στοιχεία για τον ορισμό υπηρεσιών ιστού:

- *Αφηρημένοι ορισμοί*
  Type: παρέχει ορισμούς για τους τύπους δεδομένων που περιέχουν μηνύματα SOAP.
  Message: παρέχει έναν ορισμό του μηνύματος που μεταφέρεται σε μια επικοινωνία.
  Operation: παρέχει την περιγραφή μιας πράξης που υποστηρίζεται απο την υπηρεσία.
  PortType: καθορίζει την διεπαφή υπηρεσιών των λειτουργιών που υποστηρίζει η υπηρεσία ιστού.
- *Συγκεκριμένοι ορισμοί*
  Binding: προδιαγράφει το πρωτόκολλο και την μορφή των δεδομένων για ένα συγκεκριμένο PortType.
  Port: προδιαγράφει την διεύθυνση μια συγκεκριμένης δέσμευσης.
  Service: προδιαγράφει την τοποθεσία URL της υπηρεσίας ιστού στον εξυπηρετητή που την φιλοξενεί.

Το επόμενο σχήμα παραθέτει ένα παράδειγμα μιας περιγραφής WSDL μιας υπηρεσίας για μετοχές χρηματιστηρίου. Η υπηρεσία ονομάζεται GetTradePrice και είναι βασισμένη σε

κωδικοποίηση SOAP. Η αίτηση λαμβάνει ένα σύμβολο τύπου συμβολοακολουθίας string και επιστρέφει την τιμή μιας μετοχής ως αριθμό κινητής υποδιαστολής float.

```
<?xml version="1.0"?>
<definitions name="StockQuote"
        targetNamespace="http://example.com/stockquote.wsdl"
        xmlns:tns="http://example.com/stockquote.wsdl"
        xmlns:xsd="http://www.w3.org/2000/10/XMLSchema"
        xmlns:xsd1="http://example.com/stockquote.xsd"
        xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
        xmlns="http://schemas.xmlsoap.org/wsdl/">
   <message name="GetTradePriceInput">
      <part name="tickerSymbol" element="xsd:string"/>
      <part name="time" element="xsd:timeInstant"/>
   </message>
   <message name="GetTradePriceOutput">
      <part name="result" type="xsd:float"/>
   </message>
   <portType name="StockQuotePortType">
      <operation name="GetTradePrice">
        <input message="tns:GetTradePriceInput"/>
        <output message="tns:GetTradePriceOutput"/>
      </operation>
   </portType>
   <binding name="StockQuoteSoapBinding"type="tns:StockQuotePortType">
          <soap:binding style="rpc" transport="http://schemas.xmlsoap.org/soap/http"/>
    <operation name="GetTradePrice">
        <soap:operation soapAction="http://example.com/GetTradePrice"/>
        <input>
<soap:body use="encoded" namespace="http://example.com/stockquote"
encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
        </input>
        <output>
          <soap:body use="encoded" namespace="http://example.com/stockquote"
           encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
        </output>
   </operation>
   </binding>
   <service name="StockQuoteService">
      <documentation>My first service</documentation>
      <port name="StockQuotePort" binding="tns:StockQuoteBinding">
        <soap:address location="http://example.com/stockquote"/>
      </port>
   </service>
</definitions>
```

Παράδειγμα εγγράφου περιγραφής WSDL

Είναι εύκολο να διαπιστωθεί ότι το έγγραφο WSDL σε σύγκριση με την περιγραφή της διεπαφής SOAP είναι αρκετά μεγαλύτερο. Αυτό οφείλεται στην πλεονάζουσα πληροφορία που οφείλεται στα ξεχωριστά οριζόμενα στοιχεία και την XML.

Πρωτόκολλο Περιγραφής, Ανακάλυψης και Ολοκλήρωσης

Οι προδιαγραφές του *Πρωτοκόλλου Περιγραφής, Ανακάλυψης και Ολοκλήρωσης (Universal Description Discovery & Integration - UDDI)* παρέχουν ένα σύστημα για την εγγραφή και εύρεση της πληροφορίας που απαιτείται για την χρήση μιας υπηρεσίας ιστού και της

πληροφορίας για τον παροχέα της υπηρεσίας. Η έμφαση στο UDDI δίνεται στον ορισμό ενός συνόλου υπηρεσιών που υποστηρίζουν την περιγραφή και αναζήτηση (1) επιχειρήσεων, οργανισμών και άλλων παρόχων υπηρεσιών ιστού, (2) των υπηρεσιών που αυτοί διαθέτουν και (3) των προγραμματιστικών διεπαφών που μπορούν να χρησιμοποιηθούν για πρόσβαση στις υπηρεσίες. Τα δεδομένα οργανώνονται με τέτοιο τρόπο ώστε οι επιχειρήσεις να μπορούν να προσφέρουν πολλαπλές υπηρεσίες και μια υπηρεσία να μπορεί να προσφερθεί απο πολλές επιχειρήσεις. Κάθε μια απο τις οντότητες που εμπεριέχονται σε ένα σύστημα UDDI αναγνωρίζεται μοναδικά απο ένα μοναδικό κλειδί προκειμένου να διευκολύνονται αναζητήσεις και ενημερώσεις της πληροφορίας που σχετίζεται με κάθε οντότητα.
Μια κοινοπραξία εταιριών, συμπεριλαμβανομένου της IBM, της Microsoft και της Ariba ξεκίνησαν την δημιουργία της ιδέας για έναν επιχειρηματικό κατάλογο στο διαδίκτυο που να καθορίζει βάσεις μέσα στις οποίες εταιρίες μπορούν να δημοσιεύσουν πληροφορίες για τις ίδιες και τις υπηρεσίες που προσφέρουν. Το αποτέλεσμα ήταν το έργο UDDI που κατατέθηκε στον οργανισμό OASIS για προτυποποίηση. Οι προδιαγραφές του UDDI έκδοση 2 έχουν ήδη γίνει πρότυπο του OASIS. Αυτή τη στιγμή είναι σε φάση σχεδιασμού η τρίτη έκδοση του προτύπου απο την αντίστοιχη τεχνική επιτροπή.

Σκοπός

Το UDDI αντιμετωπίζει το πρόβλημα του εντοπισμού κατάλληλων υπηρεσιών ιστού για κατανάλωση απο άλλες υπηρεσίες ή εφαρμογές. Αυτό επιτυγχάνεται με τον καθορισμό βάσεων που είναι ικανές να διαχειριστούν περιγραφές επιχειρησιακών δεδομένων. Τέτοιες βάσεις επίσης παρέχουν λειτουργίες όπως δυνατότητες αναζήτησης, προγραμματιστική πρόσβαση σε απομακρυσμένες εφαρμογές και μηχανισμούς που αμβλύνουν προβλήματα που συμβαίνουν κατά την πρόσβαση σε εγγεγραμμένες υπηρεσίες ιστού. Με την χρήση συστημάτων UDDI, μια οντότητα μπορεί να ανακαλύψει και να συγκρίνει τις υπηρεσίες ιστού που παρέχουν την ίδια λειτουργικότητα. Για παράδειγμα, μια εφαρμογή μπορεί να ανακαλύψει τις υπηρεσίες ιστού που παρέχουν επεξεργασία δεδομένων πληρωμών πιστωτικών καρτών, και συγκρίνοντάς τες να επιλέξει και χρησιμοποιήσει την πιο κατάλληλη.

Δομή

Τα δεδομένα ενός μητρώου UDDI βασίζονται στο HTTP και το SOAP και είναι προσβάσιμα μέσω δύο συνόλων διεπαφών SOAP. Η μια διεπαφή υποστηρίζει πιθανούς συνδρομητές που ανακαλύπτουν επιθυμητές υπηρεσίες και λαμβάνουν τις λεπτομέρειές τους, και η άλλη υποστηρίζει τους παρόχους υπηρεσιών ώστε να μπορούν να διαχειρίζονται την δημοσίευση των υπηρεσιών τους στο μητρώο.

Για τα μητρώα UDDI έχουν καθοριστεί πέντε δομές:

businessEntity: αναπαριστά την επιχείρηση / οργανισμό και παρέχει πληροφορίες όπως το μοναδικό *αναγνωριστικό της (UUID)*, το όνομα της εταιρίας, μια περιγραφή και τις σχετικές επαφές.

businessService: περιλαμβάνεται στην businessEntity και παρέχει δεδομένα για την συγκεκριμένη υπηρεσία που παρέχεται απο την επιχείρηση. Η δομή περιλαμβάνει ένα μοναδικό αναγνωριστικό, την περιγραφή της υπηρεσίας και την κατηγορία της.

bindingTemplate: περιλαμβάνεται στην businessService και αναγνωρίζει πώς και πού μπορεί κάποιος να αποκτήσει πρόσβαση στην υπηρεσία. Η δομή περιέχει ένα μοναδικό αναγνωριστικό και την διεύθυνση της υπηρεσίας ιστού (URL ή e-mail).

tModel: περιλαμβάνεται στο bindingTemplate και περιλαμβάνει τις τεχνικές προδιαγραφές της διεπαφής της υπηρεσίας ιστού. Η δομή περιέχει ένα μοναδικό αναγνωριστικό, ένα όνομα, μια περιγραφή και τα *αναγνωριστικά κατηγορίας (category descriptors)*.

publisherAssertion: παρέχει έναν τρόπο για δύο οντότητες να μπορέσουν να αποκτήσουν μια σχέση μεταξύ τους.

Προδιαγραφές Διαχείρισης Κλειδιών με XML

Το πρότυπο *Διαχείρισης Κλειδιών με XML (XML Key Management Specifications – XKMS)* αποτελεί προδιαγραφές για την εγγραφή και διανομή δημόσιων κλειδιών. Είναι μια τεχνολογία βασισμένη στην XML με σκοπό την διευκόλυνση της ενσωμάτωσης ΥΔΚ

κάνοντας ευκολότερη την παραμετροποίηση, χρήση και διαχείρισή της. Αυτό επιτυγχάνεται αποφορτίζοντας την ΥΔΚ απο πολύπλοκες εργασίες διαχείρισης κλειδιών και την εδραίωση επικοινωνίας με την ΥΔΚ μέσω της XML, δίνοντας αντίστοιχες δυνατότητες ακόμα και σε ασύρματες συσκευές (κινητά τηλέφωνα κ.λ.π). Το πρότυπο XKMS σχεδιάστηκε για χρήση σε συνδυασμό με τις Ψηφιακές Υπογραφές XML και την Κρυπτογράφηση XML, αλλά και με μελλοντικά πρότυπα. Η συνδυασμένη χρήση της Ψηφιακής Υπογραφής XML και της Κρυπτογράφησης XML παρέχει ακεραιότητα και ιδιωτικότητα, αλλά δεν αντιμετωπίζει τα θέματα εμπιστοσύνης που έχουν να κάνουν με την διαχειρίση κλειδιών. Αυτά τα θέματα αντιμετωπίζονται απο το XKMS.

Το πρότυπο XMKS αποτελείται απο δύο κομμάτια:

- Τις *Προδιαγραφές Παροχής Υπηρεσιών Πληροφοριών με XML (XML Key Information Services Specification X-KISS)*: Καθορίζουν ένα πρωτόκολλο για μια υπηρεσία εμπιστοσύνης που τρέχει σαν Υπηρεσία Ιστού και επιστρέφει την πληροφορία που είναι σχετική με τα στοιχεία KeyInfo που περιέχονται στις δομές Ψηφιακών Υπογραφών XML και Κρυπτογράφησης XML (βλ. Παραγράφους 0 και 0).
- Τις *Προδιαγραφές Παροχής Υπηρεσιών Εγγραφής με XML (XML Key Registration Service Specification X-KRSS)*: Καθορίζουν ένα πρωτόκολλο για μια Υπηρεσία Ιστού που δέχεται πληροφορίες για εγγραφή, ανάκληση και ανάκτηση δημόσιων κλειδιών.

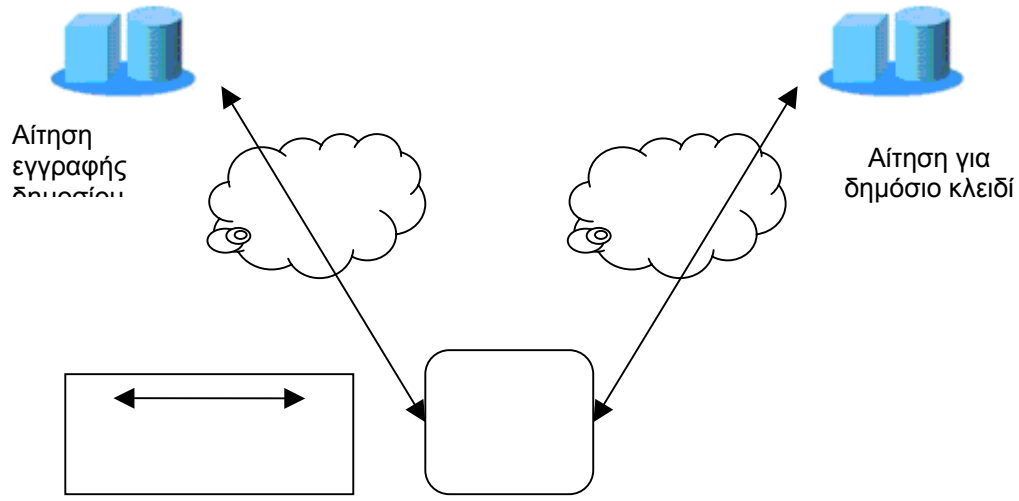
Οι αρχικές προδιαγραφές του XKMS δόθηκαν απο την Microsoft, τη Verisign και την WebMethods, αλλά αποτελούν πλέον μια Σημείωση του W3C.

Διεργασίες XKMS

Το XKMS απλουστεύει σύνθετες διεργασίες μιας ΥΔΚ ορίζοντας Προγραμματιστικές Διεπαφές (APIs), οι οποίες μπορούν να χρησιμοποιηθούν απο Υπηρεσίες Ιστού. Οι λειτουργίες που προσφέρονται απο της Υπηρεσίες Ιστού που υποστηρίζουν το XKMS περιλαμβάνουν τα εξής:

- Εγγραφή ενός δημόσιου κλειδιού (Πρωτόκολλο X-KRSS)
- Ανάκληση ενός κλειδιού (Πρωτόκολλο X-KRSS)
- Ανάκτηση ενός κλειδιού (Πρωτόκολλο X-KRSS)
- Εντοπισμός ενός κλειδιού (Πρωτόκολλο X-KISS)
- Έλεγχος εγκυρότητας ενός κλειδιού (Πρωτόκολλο X-KISS)

Οι μόνες κρυπτογραφικές λειτουργίες που πρέπει να υποστηρίζονται απο μια εφαρμογή είναι αυτές της Ψηφιακής Υπογραφής XML και της Κρυπτογράφησης XML. Η διαμόρφωση μιας τοπολογίας XKMS είναι όπως φαίνεται στο ακόλουθο σχήμα:



Διαμόρφωση τοπολογίας XKMS

Ο βασικός στόχος του πρωτοκόλλου X-KISS είναι η ελαχιστοποίηση της πολυπλοκότητας που συναντά μια εφαρμογή-πελάτης με το να μεταβιβάζει ένα μέρος των διεργασιών που χρειάζονται για την επεξεργασία ενός στοιχείου KeyInfo μιας δομής Ψηφιακής Υπογραφής XML ή Κρυπτογράφησης XML σε μια υπηρεσία εμπιστοσύνης. Ο υπογράφων μπορεί να συμπεριλάβει είτε ένα στοιχείο KeyInfo που καθορίζει το ίδιο το κλειδί (το όνομα ενός κλειδιού, ένα πιστοποιητικό X509, ένα αναγνωριστικό PGP κ.λ.π.) ή μια αναφορά στην τοποθεσία όπου τα πλήρη δεδομένα του στοιχείου KeyInfo μπορούν να βρεθούν. Στην περίπτωση της κρυπτογράφησης, η εφαρμογή-πελάτης μπορεί να μην γνωρίζει καν το δημόσιο κλειδί του παραλήπτη.

Το X-KRSS περιγράφει ένα πρωτόκολλο για την υποστήριξη της εγγραφής πληροφορίας ενός δημοσίου κλειδιού και του ιδιοκτήτη του σε μια υπηρεσία εμπιστοσύνης. Οι προδιαγραφές υποστηρίζουν την διαδικασία εγγραφής που υλοποιείται προκειμένου να δεθεί πληροφορία με ένα ζεύγος κλειδιών που έχουν δημιουργηθεί είτε απο τον πελάτη είτε απο τον εξυπηρετητή που παρέχει την υπηρεσία εμπιστοσύνης.

Παράδειγμα

Ένα παράδειγμα μια αίτησης για εγγραφή σε έναν εξυπηρετητή X-KRSS φαίνεται στο σχήμα που ακολουθεί, όπου το ζεύγος κλειδιών έχει δημιουργηθεί απο τον πελάτη.

```
<Register>
  <Prototype Id="keybinding">
    <Status>Valid</Status>
    <KeyID>mailto:Alice@cryptographer.test</KeyID>
    <ds:KeyInfo>
      <ds:KeyValue>
        <ds:RSAKeyValue>
          <ds:Modulus>
          998/T2PUN8HQlnhf9YIKdMHHGM7HkJwA56UD0a1oYq7E
          fdxSXAidruAszNqBoOqfarJIsfcVKLob1hGnQ/l6xw
          </ds:Modulus>
          <ds:Exponent>AQAB</ds:Exponent>
        </ds:RSAKeyValue>
      </ds:KeyValue>
      <ds:KeyName>mailto:Alice@cryptographer.test</ds:KeyName>
    </ds:KeyInfo>
    <PassPhrase>Pass</PassPhrase>
```

```
  </Prototype>
  <AuthInfo>
    <AuthUserInfo>
      <ProofOfPossession>
        <ds:Signature URI="#keybinding"
            [RSA-Sign (KeyBinding, Private)] />
      </ProofOfPossession>
      <KeyBindingAuth>
        <ds:Signature  URI="#keybinding"
            [HMAC-SHA1 (KeyBinding, Auth)] />
      </KeyBindingAuth>
    </AuthUserInfo>
  </AuthInfo>
  <Respond>
    <string>KeyName<string>
    <string>KeyValue</string>
    <string>RetrievalMethod</string>
  </Respond>
</Register>
```

Αίτηση εγγραφής ενός ζεύγους κλειδιών δημιουργημένων στην πλευρά του χρήστη

Τα στοιχεία της αίτησης εγγραφής είναι τα ακόλουθα:

Register: Περιέχει όλη την πληροφορία που είναι σχετική με το δημόσιο κλειδί και τον ιδιοκτήτη του.
Status: Καθορίζει την τρέχουσα κατάσταση του δημόσιου κλειδιού. Όταν το κλειδί εγγράφεται, το στοιχείο αυτό παίρνει την τιμή valid.
KeyID: Περιέχει ένα όνομα ή μια τοποθεσία που αναγνωρίζει μοναδικά το κλειδί.
PassPhrase: Περιέχει το αποτέλεσμα μια συνάρτησης κατακερματισμού πάνω στον κωδικό του χρήστη.
AthInfo: Περιέχει τα στοιχεία που αυθεντικοποιούν την αίτηση εγγραφής.
ProofOfPossesion: Περιέχει το στοιχείο Signature της Ψηφιακής Υπογραφής που αποδεικνύει την κατοχή του ιδιωτικού κλειδιού.
KeyBindingAuth: Περιέχει την αίτηση δέσμευσης του κλειδιού, αυθεντικοποιημένη απο μια υπογραφή.
Response: Καθορίζει πως θα πρέπει να απαντήσει ο εξυπηρετητής. Ο εξυπηρετητής επιστρέφει το όνομα του κλειδιού, την τιμή του και την μέθοδο ανάκτησης.

Γλώσσα Προδιαγραφής Ισχυρισμών Ασφάλειας

Η *Γλώσσα Προδιαγραφής Ισχυρισμών Ασφάλειας (Security Assertion Markup Language – SAML)* είναι ένα πλαίσιο βασισμένο στην XML που χρησιμοποιείται για την ανταλλαγή πληροφορία ασφάλειας στην μορφή *«ισχυρισμών» (assertions)* ασφάλειας για ταυτότητες οντοτήτων σε μια συγκεκριμένη διαχειριστική περιοχή ασφάλειας. Ένας ισχυρισμός SAML μπορεί να περιέχει πληροφορία για πράξεις *αυθεντικοποίησης (authentication assertion)* που επιτελούνται απο ταυτότητες, *χαρακτηριστικά ταυτοτήτων (attribute assertion)* και *αποφάσεις για έλεγχο πρόσβασης (authorization assertion)* σε συγκεκριμένους πόρους μιας περιοχής ασφάλειας. Ένα παράδειγμα ισχυρισμού χαρακτηριστικών φαίνεται στο ακόλουθο σχήμα:

```
<saml:assertion
 xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
 MajorVersion="1" MinorVersion="1"
 Issuer="https://idp.edu/saml/" ...>
 <saml:Conditions NotBefore="..." NotAfter="..."/>
 <saml:AuthenticationStatement
   AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:X509-PKI"
```

```
  AuthenticationInstant="...">
  <saml:Subject>...</saml:Subject>
 </saml:AuthenticationStatement>
 <saml:AttributeStatement>
  <saml:Subject>...</saml:Subject>
  <saml:Attribute
    AttributeName="urn:mace:dir:attribute-def:eduPersonScopedAffiliation"
    AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
    <saml:AttributeValue Scope="idp.edu">
      member
    </saml:AttributeValue>
    <saml:AttributeValue Scope="idp.edu">
      student
    </saml:AttributeValue>
  </saml:Attribute>
 </saml:AttributeStatement>
</saml:Assertion>
```

Παράδειγμα ισχυρισμού SAML

Στο παράδειγμα του σχήματος, γίνεται μια δήλωση χαρακτηριστικού η οποία μπορεί να υποδεικνύει ή όχι ότι ένα υποκείμενο έχει μια σχέση τύπου «μαθητής», την οποία κάποιος θα μπορούσε να χρησιμοποιήσει προκειμένου να επιτρέψει ή να απορρίψει την πρόσβαση σε ένα σύστημα.

Οι ισχυρισμοί εκδίδονται απο *αρχές SAML*, που μπορεί να δρουν ως *αρχές αυθεντικοποίησης, αρχές χαρακτηριστικών ή σημεία αποφάσεων πολιτικών*. Η SAML καθορίζει ένα πρωτόκολλο με το οποίο εφαρμογές-πελάτες μπορούν να ζητούν ισχυρισμούς απο Αρχές SAML και να λαμβάνουν απαντήσεις απο αυτές. Επιπρόσθετα, η SAML περιγράφει πως οι ισχυρισμοί μπορούν να μεταδοθούν απο εφαρμογές κάνοντας χρήση κάποιων προφίλ και «δεσμεύσεων» (bindings). Οι δεσμεύσεις περιγράφουν τον τρόπο με τον οποίο κάποιος κάνει μια αίτηση και λαμβάνει ισχυρισμούς απο μια Αρχή SAML, ενώ τα προφίλ περιγράφουν τον τρόπο με τον οποίο οι ισχυρισμοί SAML μπορούν να υποστηρίξουν την ασφάλεια συναλλαγών μεταξύ εφαρμογών. Οι προδιαγραφές της SAML αυτή τη στιγμή ορίζουν δεσμεύσεις μόνο για το SOAP και το HTTP POST.

Το πρωτόκολλο της SAML έχει προδιαγραφεί με το συνδυασμό της AuthXML της εταιρίας Securant Techonolgies και της γλώσσας Security Services Markup Language της Netegrity. Αυτή τη στιγμή είναι ένα πρότυπο του OASIS που παράγεται απο την Τεχνική Επιτροπή για τις Υπηρεσίες Ασφάλειας.

Σκοπός

Ο σκοπός της SAML είναι να καθορίσει μια πρότυπη αναπαράσταση δεδομένων ασφάλειας αναγνωρίσιμων απο διαφορετικές εφαρμογές υπηρεσιών ασφάλειας, ανεξάρτητα απο τις τεχνολογίες ασφάλειας ή τις πολιτικές που χρησιμοποιούν. Η SAML είναι ένα είδος Υποδομής Διαχείρισης Δικαιωμάτων (Permission Management Infrastructure – PMI). Πριν απο την SAML, οι υλοποιήσεις τέτοιων υποδομών έπρεπε να βασιστούν σε πολύπλοκων και ασύμβατων πακέτων λογισμικού απο διάφορες εταιρίες.

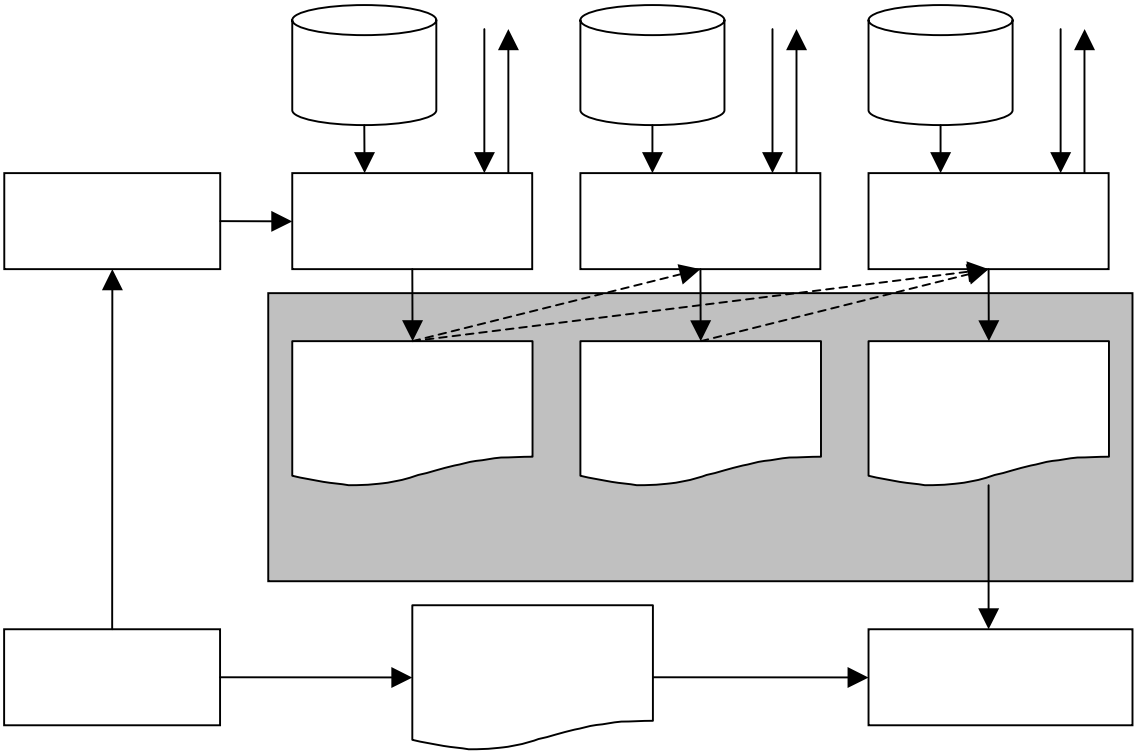
Η SAML καθορίζει τρία διαφορετικά είδη δηλώσεων ισχυρισμών που μπορούν να δημιουργηθούν απο μια Αρχή SAML:

- Αυθεντικοποίηση: Υποδεικνύει ότι η καθορισμένη ταυτότητα έχει αυθεντικοποιηθεί απο μια δεδομένη αρχή σε ένα δεδομένο χρόνο.
- Χαρακτηριστικό: Η καθορισμένη ταυτότητα είναι συνδεδεμένη με τα καθορισμένα χαρακτηριστικά.
- Απόφαση ελέγχου πρόσβασης: Μια συγκεκριμένη απόφαση ελέγχου πρόσβασης σε έναν πόρο βασισμένη σε μια αίτηση ελέγχου πρόσβασης.

Κάθε δήλωση ισχυρισμού επιστρέφεται στην οντότητα που την αιτεί, κατόπιν αποστολής μιας αίτησης αυθεντικοποίησης, ή χαρακτηριστικών ή ελέγχου πρόσβασης προς μια υπηρεσία έμπιστης τρίτης οντότητας. Η SAML είναι γραμμένη στην XML και ενσωματώνει όλα τα πλεονεκτήματα της XML για ανεξαρτησία απο πλατφόρμες και γλώσσες προγραμματισμού.

Διαδικασία χρήσης SAML

Το ακόλουθο σχήμα επιδεικνύει πως η SAML μπορεί να επιτρέψει σε μια οντότητα ενός συστήματος να επιτελέσει μια δραστηριότητα πάνω σε έναν συγκεκριμένο πόρο:



Μοντέλο διαχείρισης SAML

Τα βήματα που λαμβάνουν χώρα είναι τα ακόλουθα:

1. Ο πελάτης αυθεντικοποιείται και ζητά απο την αρχή αυθεντικοποίησης να του επιστρέψει έναν ισχυρισμό SAML ως απόδειξη της αυθεντικοποίησης.
2. Ο πελάτης εκδίδει μια αίτηση πρόσβασης στον πόρο και την στέλνει στον οργανισμό που διαχειρίζεται τον πόρο μαζί με τον ισχυρισμό αυθεντικοποίησης του βήματος 1.
3. Ο οργανισμός που θα δεχτεί την αίτηση, πρώτα εξετάζει τον ισχυρισμό αυθεντικοποίησης και έπειτα επικοινωνεί με την Αρχή Χαρακτηριστικών SAML, για να της δώσει τον ισχυρισμό αυθεντικοποίησης και να ζητήσει έναν ισχυρισμό χαρακτηριστικών.
4. Ο οργανισμός αποστέλλει μια αίτηση ελέγχου πρόσβασης SAML στην Αρχή Ελέγχου Πρόσβασης (σημείο ελέγχου πολιτικής) μαζί με τον πόρο στον οποίο ζητά πρόσβαση ο πελάτης και τον ισχυρισμό χαρακτηριστικών.
5. Η Αρχή Ελέγχου Πρόσβασης αποφαίνεται για το αν θα δώσει πρόσβαση ή όχι και επιστέφει μια απόφαση αποδοχής ή απόρριψης στη μορφή ενός ισχυρισμού απόφασης ελέγχου πρόσβασης.

Η SAML είναι ένα πρότυπο ανεξάρτητο απο τις υλοποιήσεις εταιριών και βασίζεται σε ευρέως αποδεκτά πρότυπα και πρωτόκολλα βασισμένα στην XML προκειμένου να επιτυγχάνει διαλειτουργικότητα ανάμεσα σε εφαρμογές.

5.3 ΕΠΕΚΤΑΣΙΜΗ ΓΛΩΣΣΑ ΕΛΕΓΧΟΥ ΠΡΟΣΒΑΣΗΣ

Η *Επεκτάσιμη Γλώσσα Ελέγχου Πρόσβασης (eXtensible Access Control Markup Language - XACML)* είναι μια γενικευμένη γλώσσα προδιαγραφής πολιτικών που βασίζεται στην XML για την έκφραση πληροφορίας ασφάλειας. Η XACML εστιάζει στην δημιουργία μιας πλούσιας γλώσσας για *πολιτικές ασφάλειας* και ένα *μοντέλο για έλεγχο πρόσβασης*, προσφέροντας μια μέθοδο για συνδυασμό μεμονωμένων κανόνων και πολιτικών σε ένα μοναδικό σύνολο πολιτικών που εφαρμόζεται σε μια συγκεκριμένη αίτηση για απόφαση. Η πολιτική που μπορεί να εφαρμοστεί σε μια αίτηση απόφασης μπορεί να συντεθεί απο έναν αριθμό ανεξάρτητων κανόνων η πολιτικών.

Σκοπός

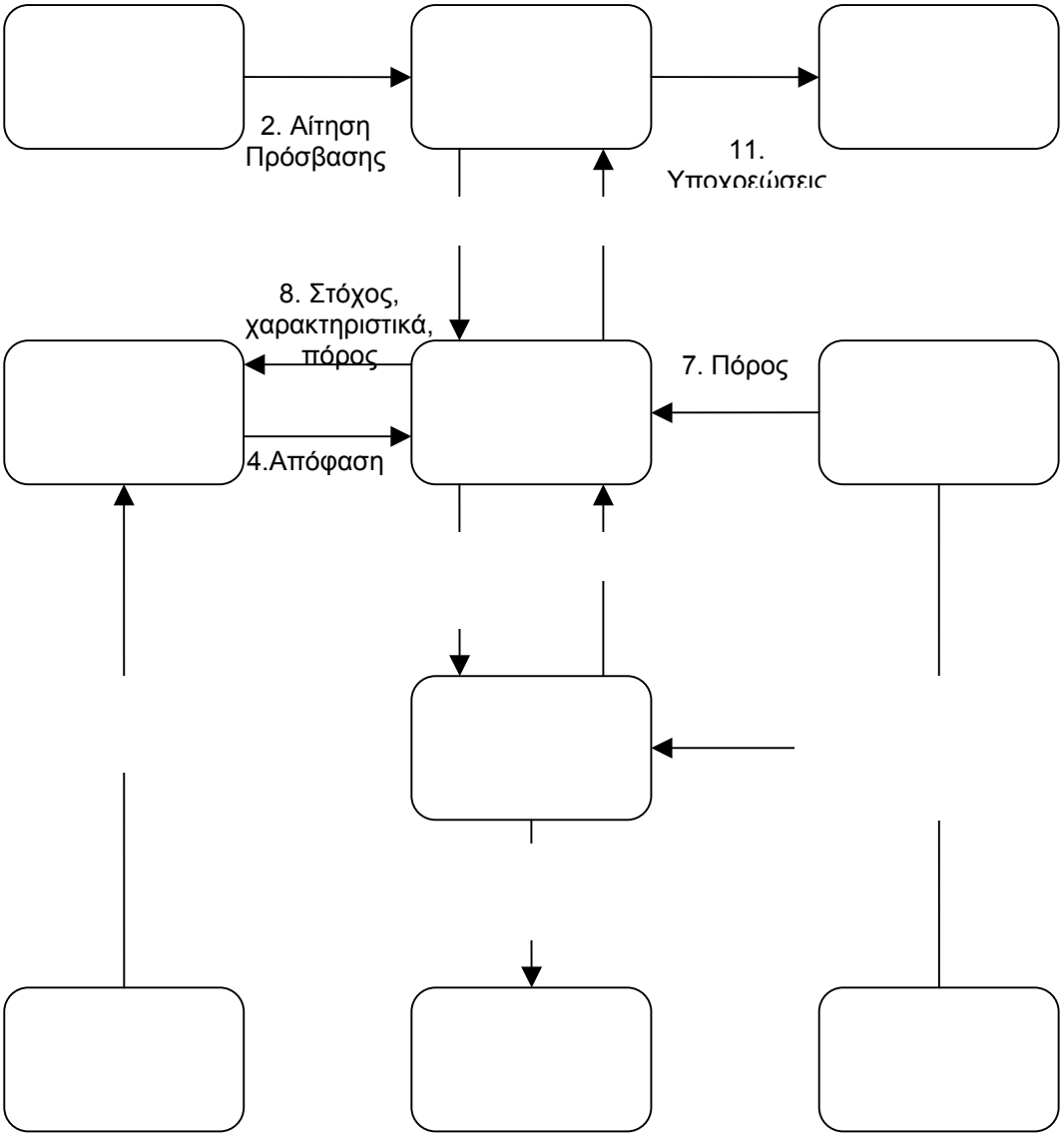
Η XACML είναι μια γλώσσα που επιτρέπει σε οργανισμούς να επικοινωνούν τις πολιτικές τους προς απόκτηση πρόσβασης σε πληροφορίες και πόρους.

Καθορίζει τρία στοιχεία πολιτικής υψηλότερου επιπέδου: τα Rule, Policy και PolicySet. Το στοιχείο Rule περιέχει μια έκφραση Boolean που μπορεί να αποτιμηθεί μεμονωμένα, το στοιχείο Policy περιέχει ένα σύνολο απο στοιχεία Rule και μια συγκεκριμένη διαδικασία για τον συνδυασμό των αποτελεσμάτων των αποτιμήσεών τους, και το στοιχείο PolicySet περιλαμβάνει ένα σύνολο απο στοιχεία Policy ή άλλα στοιχεία PolicySet και μια συγκεκριμένη διαδικασία για το συνδυασμό των αποτελεσμάτων των αποτιμήσεών τους.

Η XACML επίσης καθορίζει έναν αριθμό απο συνδυαστικούς αλγόριθμους που μπορούν να αναγνωριστούν απο τα χαρακτηριστικά RuleCombiningAlgId ή PolicyCombiningAlgId των στοιχείων Policy και PolicySet αντίστοιχα. Ο αλγόριθμος συνδυασμού των στοιχείων Rule και ο αλγόριθμος συνδυασμού των στοιχείων Policy καθορίζουν μια διαδικασία προκειμένου να ληφθεί μια απόφαση δεδομένου των μεμονωμένων αποτελεσμάτων της αποτίμησης των συνόλων απο κανόνες και πολιτικές αντίστοιχα.

Διαδικασίες χρήσης XACML

Οι κύριες οντότητες που εμπλέκονται σε μια περιοχή διαχείρισης που χρησιμοποιεί XACML φαίνονται στο ακόλουθο σχήμα:



Διάγραμμα ροής XACML

Η διαδικασία που φαίνεται στο σχήμα είναι η ακόλουθη:

1. Το Σημείο Διαχείρισης Πολιτικών – ΣΔΠ (Policy Administration Point – PAP) γράφει πολιτικές για τους πόρους που διαχειρίζεται και τις γνωστοποιεί στο Σημείο Απόφασης Πολιτικής – ΣΑΠ (Policy Decision Point – PDP), το οποίο αποτιμά τις πολιτικές και παίρνει τις αποφάσεις ελέγχου πρόσβασης.
2. Η οντότητα που ζητά την πρόσβαση σε κάποιο πόρο στέλνει μια αίτηση πρόσβασης στο Σημείο Εφαρμογής Πολιτικής - ΣΕΠ (Policy Enforcement Point – PEP) προκειμένου να υλοποιηθεί ο έλεγχος πρόσβασης.
3. Το ΣΕΠ αποστέλλει την αίτηση για πρόσβαση στον διαχειριστή περιβάλλοντος (context handler) σε μια μορφή που αυτός καταλαβαίνει. Ο διαχειριστής περιβάλλοντος κατασκευάζει μια αίτηση XACML βάσει της πληροφορίας που περιέχεται στην αίτηση.
4. Πληροφορίες για τον πόρο προς πρόσβαση και χαρακτηριστικά του περιβάλλοντος ενδέχεται να ζητηθούν απο έναν Σημείο Πληροφοριών Πολιτικών – ΣΠΠ (Policy Information Point – PIP), το οποίο τελεί χρέη πηγής τιμών χαρακτηριστικών.
5. Το ΣΠΠ αναζητά και λαμβάνει τα χαρακτηριστικά του υποκειμένου που ζητά πρόσβαση, τον πόρο που ζητείται προς πρόσβαση και το περιβάλλον.

6. Το ΣΠΠ επιστρέφει τα χαρακτηριστικά που έχουν ζητηθεί στον διαχειριστή περιβάλλοντος.
7. Ο διαχειριστής περιβάλλοντος ενδέχεται να συμπεριλάβει τον πόρο στην αίτηση.
8. Ο διαχειριστής περιβάλλοντος στέλνει την αίτηση για απόφαση πρόσβασης στο ΣΑΠ για να αποτιμήσει την πολιτική.
9. Το ΣΑΠ επιστρέφει την απάντηση.
10. Ο διαχειριστής περιβάλλοντος μεταφράζει την απάντηση απο XACML στην μορφή που κατανοεί το ΣΕΠ. Αποστέλλει την απάντηση αυτή στο ΣΕΠ.
11. Το ΣΕΠ εφαρμόζει την πολιτική. Εάν η πρόσβαση επιτρέπεται σύμφωνα με την απάντηση, τότε το ΣΕΠ επιτρέπει πρόσβαση στον πόρο, αλλιώς απορρίπτει την αίτηση πρόσβασης.

5.4 ΑΣΦΑΛΕΙΑ ΥΠΗΡΕΣΙΩΝ ΙΣΤΟΥ

Το πρότυπο Ασφάλειας Υπηρεσιών Ιστού (WS-Security) καθορίζει επεκτάσεις στο πρότυπο SOAP για να συμπεριλάβει πληροφορία κρυπτογράφησης και ψηφιακών υπογραφών, συμπεριλαμβανομένου διαπιστευτηρίων ασφάλειας όπως πιστοποιητικά ΥΔΚ και «εισιτήρια» Kerberos, σε ένα μήνυμα SOAP. Η πρώτη του έκδοση ήταν τον Απρίλιο του 2002 και στη συνέχεια υιοθετήθηκε ως πρότυπο του οργανισμού OASIS.

Η ασφάλεια που προσδίδει το πρότυπο στο επίπεδο αυτό (επίπεδο ανταλλαγής μηνυμάτων) είναι ανεξάρτητη απο κρυπτογράφηση στο «επίπεδο μεταφοράς» (transport layer) όπως αυτή που επιτυγχάνεται με το SSL, οπότε μπορεί να χρησιμοποιηθεί για παράδειγμα σε ένα εσωτερικό εταιρικό δίκτυο σαν μια κανονική σύνδεση HTTP.

Οι προδιαγραφές του WS-Security αναφέρονται στην ασφάλεια ενός μηνύματος, απο-άκρη-σε-άκρη (end-to-end). Περιγράφουν βελτιώσεις της διαδικασίας ανταλλαγής μηνυμάτων SOAP για την παροχή προστασίας με εξασφάλιση της ακεραιότητας, ιδιωτικότητας και αυθεντικοποίησης ενός μοναδικού μηνύματος SOAP. Το πρότυπο επίσης παρέχει έναν γενικής χρήσης μηχανισμό για την σύνδεση διαπιστευτηρίων ασφάλειας με μηνύματα και περιγράφει πώς κωδικοποιούνται τέτοια δυαδικά διαπιστευτήρια.

5.5 ΜΗΧΑΝΙΣΜΟΙ WS-SECURITY

Οι προδιαγραφές παρέχουν τρεις κύριους μηχανισμούς: μετάδοση διαπιστευτηρίων ασφάλειας, ακεραιότητα μηνυμάτων και ιδιωτικότητα μηνυμάτων. Οι μηχανισμοί αυτοί απο μόνοι τους δεν παρέχουν μια ολοκληρωμένη λύση ασφάλειας. Αποτελούν αντίθετα ένα συστατικό που μπορεί να χρησιμοποιηθεί σε συνδυασμό με άλλες επεκτάσεις Υπηρεσιών Ιστού και υψηλότερου επιπέδου πρωτόκολλα εφαρμογών προκειμένου να ικανοποιηθεί ένα ευρύ σύνολο μοντέλων ασφάλειας και τεχνολογιών κρυπτογράφησης. Οι μηχανισμοί αυτοί μπορούν να χρησιμοποιηθούν ανεξάρτητα ή όλοι μαζί.

Το πρότυπο παρέχει έναν μηχανισμό για τον καθορισμό κωδικοποιημένων δυαδικών διαπιστευτηρίων ασφάλειας και έναν γενικής χρήσης μηχανισμό για την σύνδεση των διαπιστευτηρίων αυτών με μηνύματα. Πιο συγκεκριμένα περιγράφει πως να κωδικοποιηθούν πιστοποιητικά X509 και «εισιτήρια» Kerberos καθώς και το πως να συμπεριληφθούν σε ένα μήνυμα κρυπτογραφημένα κλειδιά. Οι προδιαγραφές καθορίζουν ένα μοντέλο ασφάλειας μηνυμάτων με την έννοια των διαπιστευτηρίων ασφάλειας συνδυασμένων με ψηφιακές υπογραφές ως απόδειξη κατοχής του διαπιστευτηρίου.

Η ακεραιότητα μηνυμάτων επιτυγχάνεται χρησιμοποιώντας τις ψηφιακές υπογραφές XML σε συνδυασμό με διαπιστευτήρια ασφάλειας, για την εξασφάλιση ότι τα μηνύματα μεταδίδονται χωρίς αλλοιώσεις. Οι μηχανισμοί ακεραιότητας είναι σχεδιασμένοι κατά τέτοιον τρόπο ώστε να μπορούν να υποστηρίξουν πολλαπλές υπογραφές και επεκτάσιμοι ώστε να μπορούν να υποστηρίξουν επιπρόσθετες μορφές υπογραφών. Οι μηχανισμοί κρυπτογράφησης

υποστηρίζουν επιπρόσθετες τεχνολογίες και διαδικασίες κρυπτογραφίας και λειτουργίες απο πολλαπλούς δράστες.

Μορφή / Δομή

Το πρότυπο καθορίζει ένα στοιχείο ασφάλειας για ένα μήνυμα SOAP. Το στοιχείο ασφάλειας περιέχεται στην επικεφαλίδα του μηνύματος SOAP και αναφέρεται σε έναν συγκεκριμένο ρόλο. Αυτό σημαίνει ότι μπορούν να υπάρχουν περισσότερα του ενός στοιχεία ασφάλειας σε μια επικεφαλίδα. Το στοιχείο ασφάλειας Security περιέχει όλους τους ισχυρισμούς ή άλλο είδος πληροφορίας που είναι σχετική με τον ρόλο, όπως στοιχεία Signature και EncryptedKey. Το στοιχείο EncryptedKey πρέπει να περιλαμβάνει ένα στοιχείο ReferenceList έτσι ώστε ο παραλήπτης του μηνύματος να μπορεί να συνδέσει κλειδιά με τα αντίστοιχα κρυπτογραφημένα δεδομένα.

Το στοιχείο Security περιλαμβάνει τα ακόλουθα υπο-στοιχεία: UsernameToken, BinarySecurityToken, SecurityTokenReference, KeyInfo, Signature, ReferenceList και EncryptedData. Το στοιχείο UserNameToken χρησιμοποιείται για να συμπεριληφθεί το όνομα του χρήστη και ένας προαιρετικός κωδικός. Το στοιχείο BinarySecurityToken είναι ένα διαπιστευτήριο ασφάλειας (όχι σε μορφή XML), όπως ένα πιστοποιητικό X509 ή ένα «εισιτήριο» Kerberos. Το στοιχείο SecurityTokenReference περιλαμβάνει ένα σύνολο απο ισχυρισμούς ή μια αναφορά σε ισχυρισμούς. Τέλος το στοιχείο ReferenceList χρησιμοποιείται για να αναγνωριστούν τα κρυπτογραφημένα στοιχεία μέσα σε ένα μήνυμα που έχει κρυπτογραφηθεί με το ίδιο κλειδί.

Ο κύριος σκοπός των προδιαγραφών Ασφάλειας Υπηρεσιών Ιστού είναι να δώσουν σε εφαρμογές την ικανότητα να κατασκευάζουν ασφαλή μηνύματα SOAP και να παρέχουν ένα ευέλικτο σύνολο μηχανισμών που μπορούν να χρησιμοποιηθούν για να υλοποιηθεί ένα εύρος πρωτοκόλλων ασφάλειας.

Οι προδιαγραφές Ασφάλειας Υπηρεσιών Ιστού καθορίζουν πως χρησιμοποιούνται οι Ψηφιακές Υπογραφές XML και η Κρυπτογράφηση XML σε επικεφαλίδες μηνυμάτων SOAP. Οι ψηφιακές υπογραφές απο μόνες τους δεν μπορούν να δώσουν αυθεντικοποίηση μηνυμάτων, θα πρέπει να συνδυαστούν και με κατάλληλα μέσα που θα εξασφαλίζουν την μοναδικότητα των μηνυμάτων, όπως χρονοσφραγίδες ή σειριακοί αριθμοί. Έτσι μπορεί να αποφευχθούν επιθέσεις «επανάληψης». Οι υλοποιήσεις του προτύπου θα πρέπει να είναι επίσης ευαίσθητες στα θέματα που μπορεί να προκύψουν απο τη χρήση της Ψηφιακής Υπογραφής γενικότερα. Διαπιστευτήρια που μεταφέρονται με μηνύματα θα πρέπει να είναι και τα ίδια υπογεγραμμένα ώστε να εξασφαλίζεται η ακεραιότητά τους. Τέλος, ιδιαίτερη προσοχή θα πρέπει να δίνεται στον συνδυασμό υπογραφών με κρυπτογράφηση στα ίδια δεδομένα, διότι ο συνδυασμός αυτός ενδέχεται να δημιουργήσει κρυπτογραφική αδυναμία.

Η Ασφάλεια Υπηρεσιών Ιστού ξεπερνάει τα δύο πρότυπα των Ψηφιακών Υπογραφών XML και Κρυπτογράφησης XML, εφαρμόζοντάς τα πάνω σε μηνύματα SOAP. Με άλλα λόγια καλύπτει κάποια απο τα κενά που αφήνουν τα δύο αυτά πρότυπα όταν χρησιμοποιούνται με το SOAP και παρέχει επιπρόσθετες οδηγίες εφαρμογής.

6 ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Τεχνολογίες Διαδικτύου, Χ. Δουληγέρης, Ε. Κοπανάκη, Ρ. Μαυροπόδη
[2] http://www.w3.org/Encryption/2001
[3] http://www.w3.org/signature
[4] http://www.vordel.com/knowledgebase/tutorial_xml_security
[5] http://home.earthlink.net/~fjhirsch/xml/xmlsec/starting-xml-security.html
[6] http://www.nue.et-inf.uni-siegen.de/~geuer-pollmann/xml_security.html
[7] http://www.thalis.cs.unipi.gr/~dpolemi

[8] Α. Καλιοντζόγλου « Διαλειτουργικές, Ασφαλείς και Παραμετροποιήσημες Αρχιτεκτονικές Υπηρεσίων» Διδακτορική Διατριβή, Εθνικό Μετσόβιο Πολυτεχνείο (ΕΜΠ), 2006 (προς υποβολή) επιβλέπων Κοκούτσης,, συνεπιβλέπων Δ. Πολέμη
[9] Α. Καραντζίας « Ασφαλής, Διαλειτουργική, Παραμετροποιήσημη και ανοιχτή αρχιτεκτονική ασύρματων υπηρεσίων ανώτερης γενιάς» Διδακτορική Διατριβή, Εθνικό Μετσόβιο Πολυτεχνείο (ΕΜΠ), 2006, επιβλέπων Γ. Στασινόπουλος, συνεπιβλέπων Δ. Πολέμη
[10] Α. Μπούρκα « Ασφάλεια στο χώρο της ιατρικής φροντίδας» Διδακτορική Διατριβή, Εθνικό Μετσόβιο Πολυτεχνείο (ΕΜΠ), 2004, επιβλέπων Δ. Κουτσούρης, συνεπιβλέπων Δ. Πολέμη
[11] A. Kaliontzoglou, P. Sklavos, T. Karantjias, D. Polemi "A secure e-Government platform architecture for small to medium sized public organizations", Electronic Commerce Research & Applications, Elsevier, 2005 (Article in Press)
[12] B. Meneklis, A. Kaliontzoglou, D. Polemi, C. Douligeris "Applying the ISO RM-ODP standard in e-Government", Article submitted to the TED Conference on e-Government, March 2005, – review pending , 2005
[13] A.Karantjias, A. Kaliontzoglou, P. Sklavos, D. Polemi, "Secure applications for the Chambers of Commerce: functionality and technical assessment", Proceedings of EUROSEC' 2004 15th Forum on Information Systems and Security, 2004, Paris
[14] B. Hartman, D. Flinn, K. Beszosov, S. Kawamoto, "Mastering Web Services Security", Wiley Publishing, 2003
[15] Organization for the Advancement of Structured
[16] Information Science – OASIS, www.oasis-open.org
[17] ETSI Technical Specification, "ETSI TS 101 903 V1.1.1 - XML Advanced Electronic Signatures (XAdES)", 2002
[18] The World Wide Web Consortium, W3C,vwww.w3c.org
[19] H. Skogsrud, B. Benatallah, F. Casati, "Model-driven Trust Negotiation for Web Services", IEEE Internet Computing, vol. 7, no. 6, 2003, pp. 45-52
[20] S. Godik, T. Mosers, eds, "eXtensible Access Control Markup Language (XACML) version 2.0", OASIS Committee Specification, February 2005
[21] W. Ford et al, "XML Key Management Specification XKMS", W3C note, March 2001, www.w3.org/TR/xkms
[22] M. Kassoff, D. Kato, W. Mohsin, "Creating GUIs for Web Services", IEEE Internet Computing, vol. 7, no. 5, 2003, pp. 66-73
[23] D. Shaffer, B. Dayton, "Orchestrating Web Services: The case for a BPEL server", oracle whitε paper, June 2004 http://www.oracle.com/solutions/integration/BPEL_whitepaper.pdfT
[24] M B. Juric, B. Mathew, P. Sarang, "Business Process Execution Language for Web Services", Packt publishing, October 2004