3. ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

3.1 Εισαγωγή

Η ασφάλεια της πληροφορίας στο διαδίκτυο είναι ένα μείζον ζήτημα που συνοδεύει την εξέλιξή του, και μάλιστα αποκτά μέρα με τη μέρα αύξουσα σημασία. Σήμερα, τόσο η χωρική όσο και η ποιοτική εξάπλωση του διαδικτύου έχουν αναγάγει το ζήτημα της ασφάλειας σε κυρίαρχο πρόβλημα της τεχνολογίας του. Μια προσπάθεια παροχής ασφάλειας στην κίνηση του διαδικτύου είναι η αρχιτεκτονική IPsec (Internet Protocol Security), η οποία παρουσιάζεται στη συνέχεια του κεφαλαίου.

Το πρόβλημα της ασφάλειας προκύπτει άμεσα από τον ρόλο που έχει αποκτήσει το διαδίκτυο σε επαγγελματικές κυρίως δραστηριότητες, αφού πλέον δεν αποτελεί μόνο μια απέραντη βάση δεδομένων, αλλά έχει αλλάξει ριζικά τον τρόπο με τον οποίο εργαζόμαστε. Το Διαδίκτυο παρέχει τον συνδυασμό της γρήγορης και φτηνής επικοινωνίας, με αποτέλεσμα όλο και περισσότερες επιχειρήσεις να το εκμεταλλεύονται σαν μέσο για την αποδοτικότερη λειτουργία και εξέλιξή τους. Ο τρόπος με τον οποίο χρησιμοποιείται το Διαδίκτυο ποικίλει: μέσω του Διαδικτύου μια επιχείρηση έρχεται σε επαφή με συνεργάτες, προμηθευτές ή πελάτες. Ο φτηνός και γρήγορος τρόπος της επικοινωνίας μέσω διαδικτύου αντικαθιστά τις ακριβές και συχνά αργές τηλεφωνικές γραμμές που χρησιμοποιούνται μέχρι σήμερα για τον ίδιο σκοπό.

Επίσης, αποτελεί πλέον κοινό τόπο ότι τα διασκορπισμένα γεωγραφικά τμήματα κάθε εταιρίας και οι σταθμοί εργασίας που βρίσκονται εκεί διασυνδέονται μέσω ενός ιδιωτικού δικτύου. Το Διαδίκτυο μπορεί να αντικαταστήσει το ιδιωτικό δίκτυο και να αποτελέσει μια φτηνή λύση συγκρινόμενο με τις μέχρι τώρα χρησιμοποιούμενες μισθωμένες γραμμές. Η συνεισφορά του γίνεται πιο σημαντική και πιο εμφανής όσο πιο απομακρυσμένα είναι τα προς σύνδεση τμήματα.

Τέλος, κάθε εταιρία, μέσω του Διαδικτύου, μπορεί να παρέχει πρόσβαση στα δεδομένα της σε οποιοδήποτε απομακρυσμένο χρήστη, χωρίς ο τελευταίος να είναι απαραίτητα μέλος του δικτύου της. Αλλά και οποιοδήποτε μέλος της ίδιας της εταιρίας, μπορεί να διαχειριστεί τα δεδομένα της από οποιοδήποτε μέρος του κόσμου. 'Ενα στέλεχος μπορεί να συνδεθεί μέσω του Διαδικτύου από ένα απομακρυσμένο σταθμό εργασίας, με τις εγκαταστάσεις της εταιρίας του, μπορεί να δώσει εντολές για την λειτουργία της αλλά και να ζητήσει πληροφορίες πολλές φορές απόρρητες. Στην τελευταία περίπτωση δημιουργείται η απαίτηση ώστε η δυνατότητα πρόσβασης να παρέχεται μόνο σε εξουσιοδοτημένα στελέχη και όχι σε οποιοδήποτε μπορεί παρουσιάζεται σαν στέλεχος. Με άλλα λόγια, ζητείται η πιστοποίηση της ταυτότητας του χρήστη.

Η δεύτερη απαίτηση για ασφάλεια προκύπτει από το παράδειγμα όπου μια επιχείρηση επικοινωνεί με τα κατά τόπους παρατμήματά της μέσω του Διαδικτύου. Αν χρησιμοποιούσε το δικό της κλειστό δίκτυο με τις δικές της γραμμές, δεν θα υπήρχε φόβος υποκλοπής των δεδομένων που μεταφέρονται. Με το Διαδίκτυο όμως πρέπει να διασφαλιστεί ότι η

μεταδιδόμενη πληροφορία δεν θα μπορεί να διαβασθεί ή ακόμα περισσότερο να αλλαχθεί, κατά την διάρκεια της μετάδοσης, από τον οποιοσδήποτε εξωτερικό χρήστη. Και επειδή στην περίπτωση του Διαδικτύου η απαγόρευση πρόσβασης στα φυσικά κανάλια επικοινωνίας είναι αδύνατη, επιδιώκεται η απαγόρευση πρόσβασης στην ίδια την πληροφορία. Αυτό σημαίνει ότι το σύστημα ασφαλείας θα πρέπει να φροντίζει ώστε η πληροφορία να κυκλοφορεί σε μορφή μη κατανοητή (κωδικοποιημένη μορφή) για οποιονδήποτε δεν έχει την αρμοδιότητα να την χειριστεί.

Στις μέρες μας η παροχή ασφάλειας στο διαδίκτυο είναι σημαντική υπόθεση. Πρώτα γιατί όλο και περισσότεροι φορείς γίνονται μέλη της παγκόσμιας αυτής κοινότητας, κάτι που τείνει να γίνει προϋπόθεση για την ανάπτυξή τους. Αυτό συνεπάγεται περισσότερη κίνηση πληροφορίας, περισσότερη κίνηση σημαντικής πληροφορίας, και συνεπώς απαίτηση για ασφάλεια σε όλο και μεγαλύτερο αριθμό περιπτώσεων. Δεύτερον, οι χρήστες αρχίζουν να αποκτούν μεγάλη οικειότητα με τη λειτουργία του διαδικτύου, που καμιά φορά χρησιμοποιείται εις βάρος και του ίδιου του Διαδικτύου. Οι επίδοξοι υποκλοπείς πληροφορίας είναι πια τόσο ενημερωμένοι και ικανοί που η αντιμετώπισή τους είναι συχνά αδύνατη. Ταυτόχρονα δε με αυτούς εκσυγχρονίζονται και εξαπλώνονται και οι ειδικές εφαρμογές (προγράμματα-ιοί) που κάνουν την υποκλοπή πιο εύκολη, και την αποστολή του πιθανού κώδικα ασφαλείας πιο δύσκολη.

3.2 Το Πρωτόκολλο IPsec

3.2.1 Γενικές αρχές

Το πρωτόκολλο IPsec είναι η παραλλαγή του IP που σκοπό έχει να επιλύσει το πρόβλημα της ασφάλειας στο Διαδίκτυο. ‘Οπως και το IP, το IPsec αναφέρεται στο στρώμα δικτύου της διαστρωμάτωσης του TCP/IP, που σημαίνει ότι παρέχει ασφάλεια σε αυτό το στρώμα και στα ιεραρχικά ανώτερά του.

Το IPsec μπορεί να εγκατασταθεί σε ένα σύστημα με έναν από τους παρακάτω τρόπους:

- Με απευθείας επέμβαση στον κώδικα του IP ώστε αυτό να μεταλλαχθεί σε Ipsec
- Με εγκατάσταση του IPsec αμέσως μετά το IP αλλά πάντα στο στρώμα δικτύου
- Με εγκατάσταση του IPsec σε έναν άλλο σταθμό, από τον οποίο όμως θα περνά όλη η κίνηση από και προς το Internet.

Πλεονέκτημα του IPsec αποτελεί το γεγονός ότι οποιαδήποτε εγκατάστασή του αφορά αποκλειστικά το στρώμα δικτύου και δεν επηρεάζει καθόλου τις ήδη εγκατεστημένες εφαρμογές του συστήματος.

Οι υπηρεσίες που προσφέρονται από το IPsec στο δίκτυο, είναι:

- ‘Ελεγχος πρόσβασης χρηστών σε δεδομένα.
- Πιστοποίηση ακεραιότητας δεδομένων.

- Πιστοποίηση ταυτότητας χρηστών.
- Αποφυγή επανεκπομπής πακέτων.
- Απόκρυψη δεδομένων.

Για τις υπηρεσίες αυτές το IPsec χρησιμοποιεί δύο πρωτόκολλα ασφαλούς μετάδοσης. Το πρωτόκολλο Πιστοποίησης Επικεφαλίδας (Authentication Header, AH), και το πρωτόκολλο Ασφαλούς Ενθυλάκωσης Πακέτου (Encapsulating Security Payload, ESP). Και στα δύο πρωτόκολλα εμπλέκουν διαδικασίες κρυπτογραφημένου κλειδιού (Cryptographic Key).

Το IPsec μπορεί να χρησιμοποιηθεί για την προστασία ενός ή περισσότερων δρόμων, μεταξύ δύο πελατών (Host), μεταξύ δύο Κόμβων Ασφαλείας (Security Gateway) ή μεταξύ ενός πελάτη και ενός κόμβου. Με τον όρο Κόμβο Ασφαλείας εννοούμε ένα ενδιάμεσο σύστημα στο οποίο εφαρμόζεται το πρωτόκολλο IPsec. Πολλοί πελάτες μπορούν να συνδέονται σε έναν κόμβο, και μέσω αυτού να επικοινωνούν με το δίκτυο (Routers, Firewalls).

Η ακριβής λειτουργία και η συνεργασία των πρωτοκόλλων AH και ESP, καθορίζεται πάντα από τον χρήστη και τις εκάστοτε εφαρμογές του. Ο διαχειριστής του συστήματος, στο οποίο θα εφαρμοστεί το Ipsec, έχει την ευχέρεια να διαλέξει για κάθε παρεχόμενη υπηρεσία, τα ακριβή πρωτόκολλα ασφαλείας, να ορίσει τους αλγόριθμους και να επιλέξει τα κλειδιά. Δημιουργείται λοιπόν σε κάθε σταθμό, μια βάση δεδομένων, στην οποία ορίζονται ποιες ακριβώς υπηρεσίες ασφαλείας θα παρέχονται σε κάθε πακέτο δεδομένων, αλλά και ποια θα είναι τα κριτήρια (selectors) με τα οποία κατηγοριοποιούνται τα πακέτα. Αυτή η βάση δεδομένων ονομάζεται Βάση Δεδομένων της Πολιτικής της Ασφάλειας (Security Policy Database, SPD).

Το μονοπάτι επικοινωνίας δύο σταθμών που προστατεύεται από κάποιο πρωτόκολλο ασφαλείας, ονομάζεται Συσχετισμός Ασφαλείας (Security Association, SA). Ο Συσχετισμός Ασφαλείας υπάρχει σε δύο μορφές:

- SA - Tunnel Mode: ‘Οταν το ένα ή και τα δύο άκρα της σύνδεσης είναι ενδιάμεσος κόμβος.
- SA - Transport Mode: ‘Οταν και τα δύο άκρα της σύνδεσης είναι τερματικοί σταθμοί.

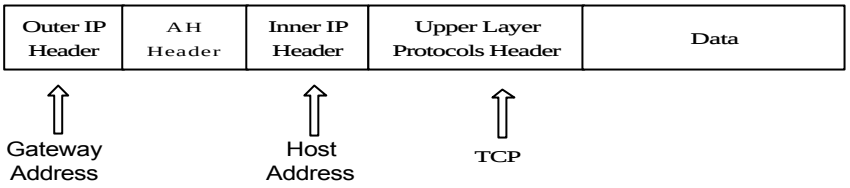
Τα πακέτα που κινούνται σε μονοπάτια του τύπου tunnel mode, έχουν δύο επικεφαλίδες IP. Την εξωτερική, η οποία περιέχει την διεύθυνση του κόμβου, και την εσωτερική που περιέχει την διεύθυνση του τελικού παραλήπτη. Αντίθετα, τα πακέτα που κινούνται σε transport mode έχουν μόνο μια επικεφαλίδα IP με την διεύθυνση του τερματικού σταθμού.

3.2.2 Το πρωτόκολλο Πιστοποίησης Επικεφαλίδας (Authentication Header, AH)

Με το πρωτόκολλο AH το IPsec ικανοποιεί την πρώτη απαίτηση για παροχή ασφάλειας στο διαδίκτυο, την πιστοποίηση της ταυτότητας του

αποστολέα. Με το AH, το IPsec πιστοποιεί ότι το πακέτο όντως έρχεται από τον υπολογιστή που φαίνεται στην διεύθυνση IP του αποστολέα. Το AH πραγματοποιείται με την εισαγωγή μιας δικιάς του επικεφαλίδας στο πακέτο. Η θέση της νέας αυτής επικεφαλίδας είναι:

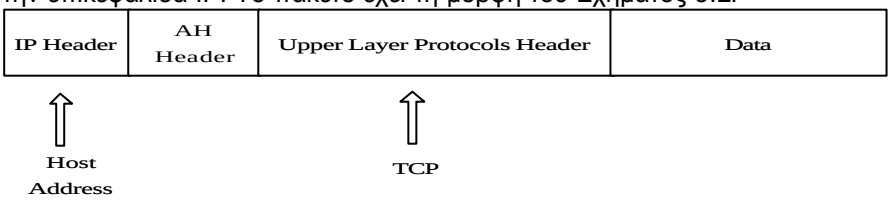
Περίπτωση Tunnel Mode: Σε πακέτο που ανήκει σε τέτοια σύνδεση, η επικεφαλίδα AH μπαίνει ανάμεσα στις δύο επικεφαλίδες IP, στην εξωτερική και στην εσωτερική. Το πακέτο παίρνει την μορφή που φαίνεται στο Σχήμα 3.1:



Σχήμα 3.1
AH-Tunnel Mode

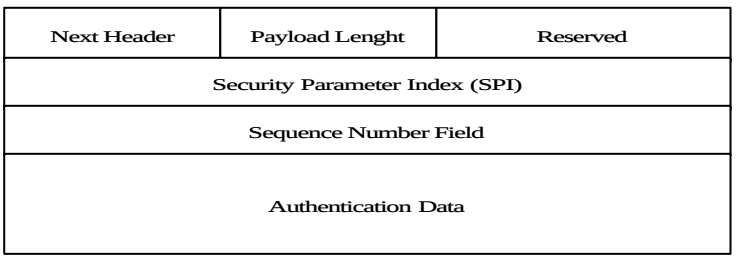
Οι αλγόριθμοι του AH εφαρμόζονται πάνω στην εξωτερική επικεφαλίδα IP, οπότε η παρεχόμενη ασφάλεια λαμβάνεται από όλο το υπόλοιπο πακέτο (Inner IP header, TCP header, Data).

Περίπτωση Transport Mode: Η επικεφαλίδα AH μπαίνει ακριβώς μετά την επικεφαλίδα IP. Το πακέτο έχει τη μορφή του Σχήματος 3.2:



Σχήμα 3.2
AH-Transport Mode

Ο αλγόριθμος του AH εφαρμόζεται πάνω στην επικεφαλίδα IP και προσφέρει ασφάλεια σε όλο το υπόλοιπο πακέτο (TCP header, Data).



Σχήμα 3.3
Η επικεφαλίδα του πρωτοκόλλου AH

Η επικεφαλίδα του πρωτοκόλλου AH έχει την μορφή του Σχήματος 3.3, όπου:

- Next Header: Τιμή που δείχνει τον τύπο των δεδομένων που ακολουθούν την AH επικεφαλίδα.
- Payload Length: Δείχνει το μήκος του AH σε bytes.
- Reserved: Πεδίο για μελλοντική χρήση. Παίρνει πάντα την τιμή 0.
- Security Parameters Index: Η τιμή αυτής της μεταβλητής μαζί με την διεύθυνση IP του προορισμού και το πρωτόκολλο AH ορίζουν τον τρέχοντα Συσχετισμό Ασφαλείας (SA). Η τιμή SPI, με μήκος 32 bit, καθορίζει το ακριβές σύνολο λειτουργιών ασφαλείας που ισχύουν στον συγκεκριμένο SA.
- Sequence Number: Είναι ο αριθμός που μηδενίζεται με την εγκατάσταση μιας νέας SA και που αυξάνει κατά ένα σε κάθε πακέτο που εκπέμπεται. Χρησιμοποιείται για να αποφεύγεται η κατά λάθος επανεκπομπή του ίδιου πακέτου. Αυτό γίνεται με το να μην επιτρέπεται στο Sequence Number να επαναληφθεί. Ο αριθμός αυτός παίρνει τιμές κανονικά από τον αποστολέα ακόμα και όταν η υπηρεσία είναι απενεργοποιημένη από τον παραλήπτη.
- Authentication Data: Στην περιοχή αυτή υπολογίζεται η Τιμή Ελέγχου Ακεραιότητας (Integrity Check Value, ICV). Είναι η τιμή με την οποία γίνεται η πιστοποίηση της ταυτότητας του χρήστη, δηλαδή η «καρδιά» του πρωτοκόλλου AH. Ο τρόπος υπολογισμού της ICV αναφέρεται στην συνέχεια.

3.2.2.1 Επεξεργασία εξερχόμενων πακέτων

‘Οταν ένα πακέτο προς εκπομπή φτάσει στο στρώμα του IPsec, ελέγχεται μέσω της βάσης SPD (βλέπε §3.2.1) η πολιτική ασφαλείας που ακολουθεί ο σταθμός για την κατηγορία πακέτων στην οποία ανήκει το συγκεκριμένο πακέτο. Αν το πακέτο πρέπει να ασφαλιστεί, εφαρμόζονται σε αυτό τα αντίστοιχα πρωτόκολλα (AH, ESP). Σε άλλη περίπτωση το πακέτο αγνοείται από το IPsec και προχωρά στο επόμενο στάδιο προς την εκπομπή του. Θα ασχοληθούμε μόνο με την πρώτη περίπτωση.

‘Εστω ότι στο πακέτο πρέπει να εφαρμοστεί το πρωτόκολλο AH. Με την επιλογή του κατάλληλου Συσχετισμού Ασφαλείας και την εγκατάσταση αυτού, η πρώτη πράξη είναι να μηδενιστεί η τιμή του Sequence Number. Η επιλογή του κατάλληλου συσχετισμού SA γίνεται μέσα από τη Βάση Δεδομένων Συσχετισμού Ασφάλειας (Security Association Database, SAD), που υπάρχει σε κάθε σταθμό. Σε αυτή, κάθε συνδυασμός υπηρεσιών ασφαλείας που μπορεί να εφαρμοστεί σε ένα πακέτο, αντιστοιχεί και σε έναν SA. Οι υπηρεσίες που στηρίζονται από τον κάθε SA προκύπτουν από την τιμή SPI του εκάστοτε πρωτοκόλλου ασφαλείας.

Η Τιμή Ελέγχου Ακεραιότητας (ICV) υπολογίζεται σύμφωνα με μεταβλητές που περιέχονται στην επικεφαλίδα IP, στην επικεφαλίδα AH και σε επικεφαλίδες ανωτέρων στρωμάτων. Για οποιαδήποτε από αυτές τις μεταβλητές αναμένεται να αλλάξει η τιμή της κατά την μετάδοση του πακέτου, στον υπολογισμό του ICV παίρνει την τιμή μηδέν. Στις

μεταβλητές που δεν αναμένεται να αλλάξουν, λαμβάνεται υπόψη η τρέχουσα τιμή τους, ενώ σε αυτές που αναμένεται να αλλάξουν αλλά η τιμή που θα πάρουν μπορεί να προβλεφθεί, λαμβάνεται υπόψη η προβλεπόμενη τιμή τους. Ο αλγόριθμος με τον οποίο υπολογίζεται η τιμή ICV από τις παραπάνω μεταβλητές, είναι μέρος του SA που χρησιμοποιεί το πακέτο στην συγκεκριμένη μετάδοση. Είναι πιθανό η SA να προβλέπει και κάποιο «κλειδί» για την κωδικοποιημένη μετάδοση του ICV.

3.2.2.2 Επεξεργασία εισερχόμενων πακέτων

Με την παραλαβή του πακέτου από το δίκτυο, ο τερματικός σταθμός διαβάζει την διεύθυνση IP του αποστολέα, το πρωτόκολλο ασφαλείας (AH) και την τιμή SPI. Από τον συνδυασμό των τριών αποφαίνεται για το ποιος SA από την SAD πρέπει να έχει χρησιμοποιηθεί. Ο SA στον οποίο καταλήγει του καθορίζει τα επόμενα βήματα:

1. Αν υποστηρίζεται η υπηρεσία αποφυγής επανάληψης πακέτου, ο σταθμός ελέγχει την τιμή Sequence Number, η οποία αν συμπίπτει με την τιμή κάποιου προηγούμενου πακέτου, το καινούργιο πακέτο απορρίπτεται. Στην πραγματικότητα, ο παραλήπτης ανοίγει ένα παράθυρο αποδεκτών τιμών Sequence Number, με άνω όριο του παραθύρου, την τιμή του τελευταίου πακέτου που δέχτηκε και κάτω όριο καθορισμένο από τον ίδιο το χρήστη. Τα νέα πακέτα με τιμή Sequence Number μικρότερη του κάτω ορίου απορρίπτονται, με τιμή μεγαλύτερη του άνω ορίου γίνονται δεκτά, ενώ με τιμή εντός του παραθύρου, ελέγχονται για το αν έχουν παραληφθεί ξανά.
2. Υποδεικνύεται ο αλγόριθμος με τον οποίο θα υπολογιστεί εκ νέου η τιμή ICV, καθώς και κάποιο πιθανό κλειδί για την κωδικοποίησή της. Με το ίδιο σκεπτικό με τον αποστολέα για τον μηδενισμό κάποιων μεταβλητών, ο παραλήπτης υπολογίζει την τιμή του ICV, την κωδικοποιεί και την συγκρίνει με αυτή που ήρθε στο πακέτο. Αν οι δύο τιμές συμπίπτουν, το πακέτο γίνεται δεκτό.
3. Αν το πακέτο είχε σταλεί από λάθος διεύθυνση, ο παραλήπτης θα είχε αποφανθεί για μια SA η οποία δεν θα είχε χρησιμοποιηθεί. Θα χρησιμοποιούσε άλλο αλγόριθμο υπολογισμού του ICV, θα κατέληγε σε διαφορετικό ICV από αυτό με το οποίο ήρθε το πακέτο και τελικά θα απέρριπτε το πακέτο.

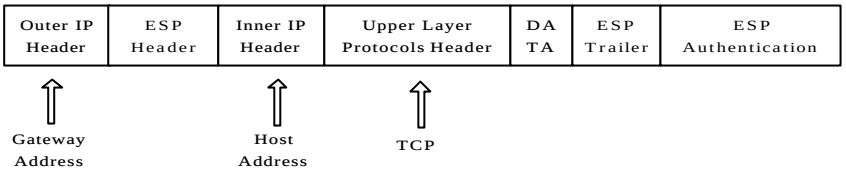
3.2.3 Το πρωτόκολλο Ασφάλειας Ενθυλακώμενης στα Δεδομένα (Encapsulating Security Payload, ESP)

Με το πρωτόκολλο Ασφάλειας Ενθυλακώμενης στα Δεδομένα (Encapsulating Security Payload, ESP) το IPsec ικανοποιεί την δυνατότητα για κρυπτογραφημένη μετάδοση των δεδομένων. Σύμφωνα με το πρωτόκολλο, ο αποστολέας και ο παραλήπτης έχουν τον ίδιο αλγόριθμο κωδικοποίησης με τον οποίο ο αποστολέας κωδικοποιεί το πακέτο, το στέλνει, και ο παραλήπτης το αποκωδικοποιεί και το διαβάζει.

Οποιοσδήποτε παρακολουθεί το κανάλι επικοινωνίας των δύο δεν μπορεί να καταλάβει το περιεχόμενο του πακέτου.

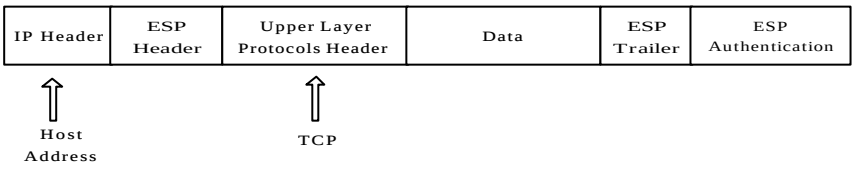
‘Οπως και στην περίπτωση του AH, το ESP πραγματοποιείται με την εισαγωγή της επικεφαλίδας ESP στο πακέτο. Και πάλι η επικεφαλίδα του πρωτοκόλλου ασφαλείας μπαίνει μετά την επικεφαλίδα IP. Η διαφορά με το AH είναι ότι το ESP εκτός από την επικεφαλίδα έχει και «ουρά», προσθέτει δηλαδή ένα επιπλέον κομμάτι στο τέλος του πακέτου. ‘Εχουμε τις εξής περιπτώσεις:

Περίπτωση Tunnel Mode: Το πακέτο έχει την μορφή του Σχήματος 3.4:



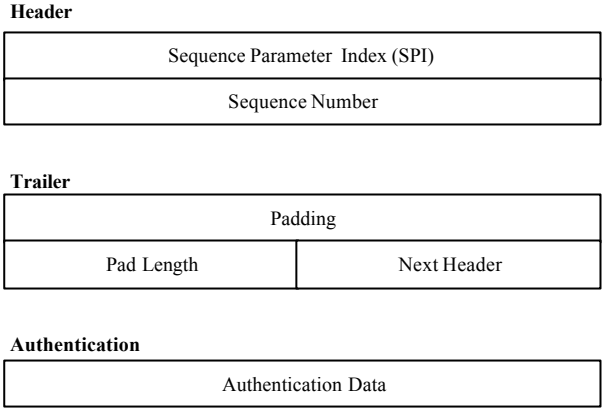
Σχήμα 3.4
ESP – Tunnel Mode

Περίπτωση Transport Mode: Το πακέτο έχει την μορφή που φαίνεται στο Σχήμα 3.5:



Σχήμα 3.5
ESP- Transport Mode

Σε κάθε περίπτωση το κομμάτι που κρυπτογραφείται είναι ότι εμφανίζεται μετά την επικεφαλίδα ESP και πριν το ESP authentication. Οι επικεφαλίδες ESP, trailer και authentication έχουν την μορφή που φαίνεται στο Σχήμα 3.6

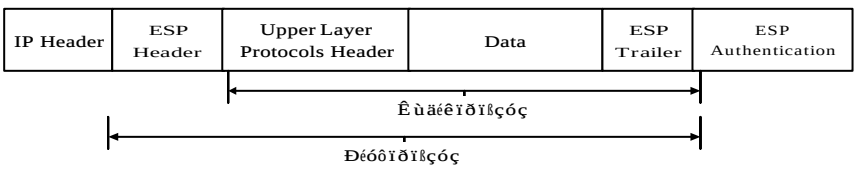


Σχήμα 3.6
Header, Trailer και Authentication του ESP

Οι μεταβλητές που εμφανίζονται έχουν την ίδια σημασία με τις αντίστοιχες του AH, δηλαδή:

- SPI: Η τιμή SPI, η διεύθυνση IP και το πρωτόκολλο ασφαλείας (ESP) ορίζουν μονοσήμαντα τον SA που χρησιμοποιείται.
- Sequence Number: Είναι η μεταβλητή που αυξάνει κατά ένα σε κάθε πακέτο που αποστέλλεται και χρησιμοποιείται για την υποστήριξη της υπηρεσίας αποφυγής λανθασμένων επαναλήψεων πακέτων.
- Padding: Πολλές φορές ο αλγόριθμος που απαιτείται για την κωδικοποίηση της πληροφορίας, απαιτεί αυτή να έχει μήκος πολλαπλάσιο κάποιου αριθμού bytes. Αν αυτό δεν ικανοποιείται από την αρχική πληροφορία, προστίθενται στο padding τόσα μηδενικά όσα χρειάζονται για να ικανοποιηθεί η συνθήκη.
- Pad Length: Είναι η τιμή που δείχνει το μήκος του padding σε bytes.
- Authentication Data: Και εδώ περιέχεται ο Αριθμός Ελέγχου Ακεραιότητας (Integrity Check Value - ICV) όπως και στο AH. Αυτό σημαίνει ότι το πρωτόκολλο ESP έχει την ιδιότητα πιστοποίησης της ακεραιότητας των δεδομένων, αφού σε αυτήν την περίπτωση η τιμή ICV υπολογίζεται επάνω σε όλο το πακέτο (επικεφαλίδα και δεδομένα).

Η προστασία λοιπόν που παρέχει το ESP σε ένα πακέτο, φαίνεται στο Σχήμα 3.7:



Σχήμα 3.7
Προστασία που παρέχει το ESP σε ένα πακέτο

3.2.3.1 Επεξεργασία εξερχόμενων πακέτων

‘Εστω το πακέτο προς αποστολή φτάνει στο στρώμα IPsec. Αυτό συμβουλεύεται την πολιτική ασφαλείας από την βάση SPD για τον τύπο του πακέτου, καταλήγει σε συγκεκριμένη SA και εφαρμόζει το πρωτόκολλο ESP στο πακέτο, όπου:

1. Συγχωνεύει στα δεδομένα (data) οτιδήποτε υπάρχει μετά την επικεφαλίδα ESP, που είναι :
   - Πρωτόκολλα ανώτερου στρώματος (Transport Mode).
   - Πρωτόκολλα ανώτερου στρώματος + Inner IP header (Tunnel Mode).
   - Προσθέτει ότι χρειάζεται στο πεδίο Padding.
2. Κωδικοποιεί το διαμορφωμένο πακέτο. Η κωδικοποίηση γίνεται πάνω στις περιοχές data, padding, pad length και next header. Δεν περιλαμβάνεται φυσικά η επικεφαλίδα ESP και το Authentication Δata. Ο αλγόριθμος κωδικοποίησης ορίζεται από τον SA.
3. Υπολογίζεται η τιμή του Sequence Number ανεξάρτητα από το αν είναι επιλεγμένη η υπηρεσία αποφυγής επαναλήψεων.
4. Υπολογίζεται η τιμή ICV στο Authentication data αν είναι επιλεγμένη η υπηρεσία πιστοποίησης δεδομένων για το πρωτόκολλο ESP.

3.2.3.2 Επεξεργασία εισερχόμενων πακέτων

Με τον ερχομό του πακέτου, το IPsec του παραλήπτη διαβάζει τη μεταβλητή SPI, τη διεύθυνση IP του αποστολέα και το πρωτόκολλο ESP, συμβουλεύεται την SPD και καταλήγει στον SA που έχει χρησιμοποιηθεί. Στη συνέχεια, με οδηγό την SA προχωρεί στα εξής βήματα:

- Αν είναι επιλεγμένη η υπηρεσία αποφυγής επαναλήψεων ελέγχει την τιμή Sequence Number. Φτιάχνει ένα παράθυρο αποδεκτών τιμών αυτής, όπου το άνω όριο του παραθύρου δείχνει τον αριθμό του πακέτου που παρελήφθη τελευταία, ενώ το κάτω όριο καθορίζεται από τον χρήστη. Αν ο αριθμός του πακέτου βρίσκεται πάνω από το άνω όριο, το πακέτο γίνεται δεκτό, κάτω από το κάτω όριο απορρίπτεται, ενώ μέσα στο παράθυρο ελέγχεται αν το πακέτο αν έχει ξαναέρθει.

- Αν είναι επιλεγμένη η υπηρεσία πιστοποίησης του πακέτου, υπολογίζεται ξανά η τιμή ICV σύμφωνα με τον αλγόριθμο που ορίζει ο SA και συγκρίνεται με αυτή που περιέχεται στο πακέτο. Σημειώνεται ότι τόσο στον αποστολέα όσο και στον παραλήπτη, η τιμή ICV υπολογίζεται πάνω σε κωδικοποιημένα δεδομένα.
- Γίνεται η αποκωδικοποίηση των κρυπτογραφημένων δεδομένων με την βοήθεια του αλγόριθμου που ορίζει ο SA, και τελικά λαμβάνεται το γνήσιο πακέτο.

3.2.4 Αλγόριθμοι και κλειδιά

Τόσο στο πρωτόκολλο AH όσο και στο ESP γίνεται χρήση συγκεκριμένων αλγορίθμων για τον υπολογισμό της μεταβλητής ICV και για την

κωδικοποίηση. Επιπλέον γίνεται χρήση προσυμφωνηθέντων λειτουργιών και κλειδιών στον υπολογισμό και στην σύγκριση των τιμών. Υπάρχουν δύο δυνατότητες για την ανταλλαγή των αλγορίθμων και των κλειδιών μεταξύ αποστολέα και παραλήπτη. Η πρώτη είναι η αυτόματη μεταβίβαση όπου, όπως έχει περιγραφεί, οι αλγόριθμοι και τα κλειδιά αποτελούν κομμάτι του SA. Με την εγκατάσταση ενός νέου SA υιοθετούνται και οι αλγόριθμοι που αυτός περιέχει. Η όλη λειτουργία γίνεται αυτόματα χωρίς καμία ανάμιξη του χρήστη.

Δεύτερος τρόπος είναι ο εκ των προτέρων ορισμός των συγκεκριμένων αλγορίθμων και κλειδιών που θα χρησιμοποιηθούν, κάτι που προϋποθέτει το μοίρασμα αυτών με την εγκατάσταση του δικτύου. Η συμφωνία γίνεται μεταξύ των χρηστών και όχι αυτόματα από τα μηχανήματα. Ο τρόπος αυτός έχει το πλεονέκτημα ότι είναι πιο ασφαλής, καθώς κανένα κλειδί ή αλγόριθμος δεν κινείται στο δίκτυο ώστε να κινδυνεύει να κλαπεί. Περιορίζεται όμως ο τρόπος αυτός σε μικρό αριθμό χρηστών λόγω της δυσκολίας του αρχικού μοιράσματος σε πολλούς σταθμούς.

3.2.5 Απόρριψη πακέτων

Μεγάλη σημασία για το δίκτυο έχει η ενεργοποίηση της υπηρεσίας με την οποία ενημερώνεται ο αποστολέας για την απόρριψη του πακέτου από τον παραλήπτη και κυρίως για την αιτία της απόρριψης. Θα ξέρει έτσι αν αξίζει να ξαναστείλει το ίδιο πακέτο ή αν πρέπει να αλλάξει κάτι για να έχει περισσότερες πιθανότητες αποδοχής. Αν, για παράδειγμα, το πακέτο απερρίφθη λόγω μη αναγνώρισης της ταυτότητας του χρήστη, τότε είναι ανώφελο να ξαναστείλει το πακέτο.

3.3 Η Υποδομή Δημοσίου Κλειδιού (Public Key Infrastructure, PKI)

Στις ενότητες που ακολουθούν θα δοθεί ένας ορισμός της Υποδομής Δημοσίου Κλειδιού (Public Key Infrastructure, PKI) και θα παρουσιαστούν τα βασικά χαρακτηριστικά που λίγο πολύ είναι κοινά σε όλες τις παραλλαγές του PKI. Αρχικά θα αναφερθούν οι βασικές κρυπτογραφικές τεχνικές, οι οποίες χρησιμοποιούν το μοντέλο του Κρυφού Κλειδιού.

3.3.1 Κρυπτογραφία Κρυφού Κλειδιού (Secret-Key Cryptography)

Η κρυπτογραφία μέχρι τα μέσα του 1970 και για τουλάχιστον 3500 χρόνια πριν, χρησιμοποιούσε ένα απλό τρόπο για την μυστική επικοινωνία δύο οντοτήτων έστω Α, Β. Για να είναι επιτυχής η επικοινωνία του έπρεπε οι Α, Β να μοιράζονται ένα μυστικό, το κλειδί το οποίο θα χρησιμοποιηθεί για την κωδικοποίηση και αποκωδικοποίηση του μεταξύ τους μηνύματος. Αυτό απαιτεί μία προηγούμενη επικοινωνία ανάμεσα στην οντότητα Α και Β, διαμέσου ενός ασφαλούς διαύλου και εμπεριέχει σοβαρό κίνδυνο υποκλοπής του μυστικού κλειδιού από κάποιον, που παρακολουθεί την

επικοινωνία των Α και Β, κατά την διάρκεια που αυτή πραγματοποιείται διαμέσου του ασφαλούς καναλιού.

Τα γνωστά συστήματα της Κρυπτογραφίας Κρυφού Κλειδιού είναι το Σύστημα Κρυπτογράφησης Δεδομένων (Data Encryption System, DES) και το kerberos (REC 1510) του MIT. Ο κυριότερος λόγος για τον οποίο αυτά τα συστήματα δεν επικράτησαν είναι διότι για την εφαρμογή τους απαιτούνται επιπλέον διαδικασίες ασφαλείας που ανταποκρίνονται σε περισσότερο κεντρικοποιημένα συστήματα παρά σε ανοικτά (ανάγκη ύπαρξης κεντρικού εξυπηρετητή ασφαλείας στον οποίο φυλάγονται τα μυστικά κλειδιά). Επίσης για λόγους ασφαλείας απαιτείται για κάθε διαφορετική οντότητα Β, με την οποία θα επιθυμούσε να επικοινωνήσει ο Α, να χρησιμοποιείται διαφορετικό κλειδί, το οποίο για ένα οργανισμό με 100 μόνο υπαλλήλους σημαίνει ότι απαιτούνται εκατομμύρια διαφορετικά κλειδιά για να καλύψουν τους πιθανούς συνδυασμούς, με την συνεπαγόμενη επίπτωση στον αποθηκευτικό χώρο και την υπολογιστική ισχύ του συστήματος του οργανισμού.

Εξέλιξη της Κρυπτογραφίας Κρυφού Κλειδιού είναι η Κρυπτογραφία Δημοσίου Κλειδιού (Public Key Cryptography). Σε αντίθεση με την πρώτη, η κρυπτογράφηση με δημόσιο κλειδί πρωτοεμφανίζεται 1976 από τον Diffie και Helman, ενώ η πρώτη υλοποίηση της πρότασης τους γίνεται το 1977 από τους Rivest, Sammir και Adleman, οι οποίοι ανακάλυψαν αυτό που σήμερα είναι γνωστό ως RSA Cryptosystem. Από τότε και ως σήμερα πολλές προτάσεις έχουν τεθεί προς συζήτηση με σημαντικότερες την Elgamal Cryptosystem και την Elliptic Curve Cryptosystem.

‘Ομως τι είναι αυτό που διαφοροποιεί την Κρυπτογραφία Δημόσιου Κλειδιού από την Κρυπτογραφία Μυστικού Κλειδιού; Στο PKI χρησιμοποιούνται δύο διαφορετικά κλειδιά, ένα για την κρυπτογράφηση και ένα για την αποκρυπτογράφηση. Το ένα κλειδί παραμένει ιδιωτικό (private) και ως εκ τούτου κρυφό, ενώ το άλλο δημοσιοποιείται (public) σε οποιονδήποτε ενδιαφερόμενο με μια διαδικασία που θα δούμε στην συνέχεια. Το όλο σύστημα είναι έτσι σχεδιασμένο ώστε η γνώση του δημόσιου κλειδιού να μην επιτρέπει σε κανέναν να μπορεί να υπολογίσει το ιδιωτικό κλειδί, το οποίο θεωρούμε ότι ελέγχεται από μία μόνο οντότητα.

Η κρυπτογραφία με δημόσιο κλειδί μπορεί να καλύψει δύο μεγάλες ανάγκες: την ανάγκη της ανάπτυξης εμπιστοσύνης ανάμεσα σε δύο μέρη, και την επικύρωση ηλεκτρονικών εγγράφων διαμέσου της ηλεκτρονικής υπογραφής. ‘Εστω ότι μια οντότητα Α έχει δημιουργήσει ένα ζεύγος κλειδιών, και έστω ότι τηρεί το κλειδί, το οποίο χρησιμοποιεί για την αποκωδικοποίηση, μυστικό και δημοσιοποιεί το κλειδί, το οποίο χρησιμοποιεί για την κωδικοποίηση. Σε αυτή τη περίπτωση οποιοσδήποτε μπορεί να κρυπτογραφήσει ένα μήνυμα χρησιμοποιώντας το δημόσιο κλειδί του Α, αλλά αυτό το μήνυμα μπορεί να διαβαστεί μόνο από τον Α, αφού πρώτα εφαρμοστεί πάνω σ’ αυτό το ιδιωτικό του κλειδί. ‘Ετσι αναπτύσσεται εμπιστοσύνη ανάμεσα στους Α και Β, διότι ο Β είναι σίγουρος ότι το κρυπτογραφημένο μήνυμα προς τον Α μπορεί να διαβαστεί μόνο από αυτόν. ‘Εστω τώρα ότι ο Α έχει διατηρήσει κρυφό το κλειδί με το οποίο κωδικοποιεί ένα μήνυμα και έχει δημοσιοποιήσει το κλειδί το οποίο

το αποκωδικοποιεί, τότε οποιοσδήποτε με το δημόσιο κλειδί του Α μπορεί να αποκωδικοποιήσει ένα μήνυμα το οποίο ο Α και μόνο ο Α θα μπορούσε να κωδικοποιήσει. Επειδή όμως η τεχνική κωδικοποίησης όλου του μηνύματος με δημόσιο κλειδί είναι ιδιαίτερα χρονοβόρα έχει αναπτυχθεί η μεθοδολογία της μεταφοράς του μυστικού κλειδιού με τη χρήση δημοσίου κλειδιού. Το αρχικό μήνυμα κωδικοποιείται με το μυστικό κλειδί του Α και στη συνέχεια το μυστικό κλειδί κωδικοποιείται με το δημόσιο κλειδί του Β. Με αυτό τον τρόπο κερδίζουμε σε χρόνο επεξεργασίας διότι συνήθως το μυστικό κλειδί είναι σημαντικά μικρότερο από το προς αποστολή μήνυμα.

Η παραπάνω διαδικασία περιγράφει αυτό που σήμερα είναι αποδεκτό ως ηλεκτρονική υπογραφή. Η ηλεκτρονική υπογραφή είναι αρκετά διαφορετική από αυτό που έχουμε ως σήμερα συνηθίσει να εννοούμε με τον όρο υπογραφή, διότι η ηλεκτρονική υπογραφή αυτό που εξασφαλίζει είναι το ότι το μήνυμα δεν έχει αλλαχθεί από τη στιγμή που εφαρμόστηκε σε αυτό το ιδιωτικό κλειδί του Α. Ωστόσο δεν μας παρέχει καμιά πληροφορία για το ποιος είναι στην πραγματικότητα ο Α.

Συνήθως πριν μαρκάρουμε ηλεκτρονικά ένα μήνυμα εφαρμόζουμε σε αυτό ένα είδος συναρτήσεων οι οποίες ονομάζονται Hash και έχουν την ιδιότητα να αντιστοιχούν σε ένα μήνυμα ένα προκαθορισμένο αριθμό από bit. Επίσης είναι υπολογιστικά αδύνατο δύο διαφορετικά μηνύματα να έχουν την ίδια τιμή Hash. 'Ετσι η ηλεκτρονική υπογραφή κωδικοποιείται σε δύο επίπεδα. Στην αρχή στο μήνυμα εφαρμόζεται μια κρυπτογραφική συνάρτηση Hash και το αποτέλεσμα αυτής κωδικοποιείται με το ιδιωτικό κλειδί του Α.

'Ετσι γίνεται κατανοητό ότι δεν αρκεί η ύπαρξη του ιδιωτικού και δημόσιου κλειδιού για να μπορούν δύο οντότητες να συναλλάσσονται. Απαιτείται η ύπαρξη μιας υποδομής από πρωτόκολλα, πρότυπα και υπηρεσίες οι οποίες να υποστηρίζουν τις εφαρμογές της κρυπτογραφίας δημόσιου κλειδιού.

3.3.2 Βασικά Χαρακτηριστικά της Υποδομής Δημοσίου Κλειδιού (PKI)

Στην ενότητα που ακολουθεί θα αναλύσουμε τα βασικά χαρακτηριστικά της υποδομής δημοσίου κλειδιού, θα αναφερθούμε στα δομικά στοιχεία της αρχιτεκτονικής του, στις λειτουργίες, μεθόδους και χαρακτηριστικά της PKI.

Η PKI είναι ένα σύστημα για τη δημοσίευση των τιμών των δημοσίων κλειδιών που χρησιμοποιούνται από οποιονδήποτε στα πλαίσια της κρυπτογραφίας δημοσίου κλειδιού. Στα πλαίσια αυτού του συστήματος διακρίνονται δύο βασικές λειτουργίες:

1. Χορήγηση ηλεκτρονικών πιστοποιητικών (Certification)() είναι η διαδικασία με την οποία συνδέουμε ένα ιδιώτη, μία εταιρεία ή κάποια άλλη οντότητα ή ακόμη και μία σημαντική πληροφορία με την τιμή ενός δημοσίου κλειδιού.
2. Επαλήθευση (Validation) είναι η διαδικασία επαλήθευσης ότι ένα πιστοποιητικό ισχύει ακόμη.

Οι παραπάνω διαδικασίες εμφανίζονται σε όλες τις παρραλλαγές της PKI, όπως και τα δομικά στοιχεία της αρχιτεκτονικής PKI που εξετάζουμε στη συνέχεια.

3.3.2.1 Αρχιτεκτονική

Τα στοιχεία που αποτελούν την αρχιτεκτονική της PKI (Πίνακας 3.1), μπορούν να ομαδοποιηθούν στις παρακάτω ευρείες λειτουργικές κατηγορίες:

1. Υπηρεσίες που ενεργοποιούν την ασφάλεια του συστήματος (System Security Enabling Services). Είναι υπηρεσίες, οι οποίες παρέχουν την λειτουργικότητα, που επιτρέπει τη συσχέτιση ενός χρήστη ή άλλης οντότητας με τις πράξεις της στο σύστημα. Τέτοιες λειτουργίες μπορούν να είναι οι διεργασίες του λειτουργικού συστήματος, οι οποίες απαιτούνται για την εξυπηρέτηση του logon του χρήστη.

Πίνακας 3.1
Αρχιτεκτονική του PKI

<table>
<tr><td colspan="3">APPLICATIONS</td></tr>
<tr><td rowspan="3">System Security Enabling Services</td><td>Secure Protocol</td><td rowspan="2">Security Policy Services</td></tr>
<tr><td>Protocol Security Services</td></tr>
<tr><td>Long Term Key Services</td><td rowspan="3">Supporting Services</td></tr>
<tr><td rowspan="2"></td><td>Crypto Services</td></tr>
<tr><td>Crypto primitives Services</td></tr>
</table>

2. Στοιχεία Υπηρεσίας της Κρυπτογραφίας (Crypto Primitives Services). Είναι υπηρεσίες οι οποίες παρέχουν τις κρυπτογραφικές διεργασίες, στις οποίες βασίζεται η ασφάλεια του δημοσίου κλειδιού. Τέτοιες είναι η δημιουργία του κλειδιού, η εφαρμογή συνάρτησης hash στα δεδομένα που περιέχονται σε έναν ενταμιευτή, η κρυπτογράφηση των δεδομένων ενός ενταμιευτή με τη χρήση αλγορίθμου μυστικού ή δημοσίου κλειδιού καθώς και οι αντίστοιχες διαδικασίες αποκρυπτογράφησης.
3. Υπηρεσίες Κλειδιού Μακράς Διαρκείας (Long Term Key Services). Είναι υπηρεσίες, οι οποίες επιτρέπουν στους χρήστες και άλλες οντότητες να διαχειρίζονται τα κλειδιά και τα πιστοποιητικά τους καθώς και τη δυνατότητα να ανακτούν και να ελέγχουν την εγκυρότητα πιστοποιητικών άλλων οντοτήτων. Οι υπηρεσίες αυτές είναι:
   (i) Διαχείριση Κύκλου Ζωής Κλειδιού (Key Lifecycle Management). Σε αυτή την υπηρεσία περιλαμβάνονται η κατάργηση ενός κλειδιού, η λήξη ενός κλειδιού κλπ.

(ii) Ανάκτηση Κλειδιού (Key Recovery). Η υπηρεσία αυτή υποστηρίζει την προετοιμασία ενός κλειδιού για την ανάκτησή του.

4. Υπηρεσίες Ασφάλειας Πρωτοκόλλων (Protocol Security Services). Είναι υπηρεσίες, οι οποίες παρέχουν λειτουργίες όπως αυθεντικότητα της προέλευσης των δεδομένων, προστασία της ακεραιότητας των δεδομένων, προστασίας της μυστικότητας των δεδομένων, σε εφαρμογές όπως τα πρωτόκολλα ασφαλείας.
   Οι παραπάνω λειτουργίες διακρίνονται σε δύο θεμελιώδεις κατηγορίες: την Προσανατολισμένη στη Σύνοδο (Session Oriented) και την Αποθήκευση και Προώθηση (Store and Forward). Η κύρια διαφορά τους είναι ότι η δεύτερη ενθυλακώνει όλες τις απαραίτητες για την ασφάλεια πληροφορίες εντός των προστατευμένων στοιχείων δεδομένων που δημιουργούν, ενώ η πρώτη απαιτεί την χρησιμοποίηση κάποιων οντοτήτων, τις οποίες δημιουργεί για την διατήρηση των πληροφοριών ασφαλείας, και οι οποίες σχετίζονται με τις ανταλλαγές των πρωτοκόλλων.
5. Ασφαλή Πρωτόκολλα (Secure Protocols) Προσφέρουν ασφαλείς επικοινωνίες ανάμεσα στις εφαρμογές. Διακρίνονται σε τρεις βασικές κατηγορίες:
   (i) Ομότιμο προς Ομότιμο Προσανατολισμένα σε Σύνδεση (Connection Oriented Peer To Peer). Αυτά τα πρωτόκολλα επιτρέπουν σε δύο μόνο οντότητες, οι οποίες πρέπει να είναι on line, να επικοινωνούν με ασφάλεια (secure RPC, SSL, SHTTP)
   (ii) Ομότιμο προς Ομότιμο Ανευ Συνδέσεως (Connectionless Peer To Peer). Αυτά τα πρωτόκολλα επιτρέπουν σε δύο μόνο οντότητες, από τις οποίες η μία να είναι off line, για κάποιο χρονικό διάστημα να επικοινωνούν με ασφάλεια (IPSEC)
   (iii) Πολλαπλών Προορισμών Ανευ Συνδέσεως (Connectionless Multicast). Αυτά τα πρωτόκολλα επιτρέπουν σε μία οντότητα, να επικοινωνεί ταυτόχρονα και με ασφάλεια με άλλες οντότητες εκ των οποίων, μία ή περισσότερες από αυτές μπορούν για κάποιο χρονικό διάστημα να είναι off line (secure Email)
6. Υπηρεσίες Πολιτικής Ασφάλειας (Security Policy Services). Οι υπηρεσίες αυτές διαχειρίζονται πληροφορίες σχετικές με τα προνόμια των χρηστών, την πολιτική ελέγχου πρόσβασης αυτών σε πηγές και τον τρόπο λήψης αποφάσεων με γνώμονα τις παραπάνω πληροφορίες
7. Υποστηρίζουσες Υπηρεσίες (Supporting Services). Είναι υπηρεσίες, που παρέχουν λειτουργίες απαραίτητες είτε στις υπηρεσίες ασφαλείας, είτε στην ασφαλή λειτουργία του υπολογιστικού συστήματος, υπηρεσίες όμως που δεν είναι συστατικά της διαδικασίας ασφαλείας.

3.3.2.2 Μέθοδοι και χαρακτηριστικά της PKI

‘Οπως διαπιστώσαμε οι δύο βασικές λειτουργίες, οι οποίες απαντώνται σε όλες τις θεωρήσεις PKI είναι η έκδοση πιστοποιητικών και η επαλήθευση της ισχύος αυτών. Στις ενότητες που ακολουθούν θα ερευνήσουμε τις διαδικασίες έκδοσης και επαλήθευσης πιστοποιητικών, θα εξετάσουμε τι είναι πιστοποιητικό και από τι αυτό αποτελείται, και θα ασχοληθούμε με την αρχή έκδοσης πιστοποιητικών και τον τρόπο σύνδεσης πολλών τέτοιων αρχών στα πλαίσια μίας παγκόσμιας υποδομής δημοσίου κλειδιού. Επίσης θα εξετασθεί η διαδικασία επαλήθευσης της ισχύος ενός πιστοποιητικού, θα παρουσιάσουμε τις λίστες ανακληθέντων κλειδιών (revocation lists) και τις διαδικασίες ανάκλησης.

‘Εκδοση πιστοποιητικών

Η έκδοση πιστοποιητικών είναι μια θεμελιώδης λειτουργία σε όλα τις PKI, και αποτελείται από τα μέσα με τα οποία, οι τιμές δημοσίων κλειδιών καθώς και πληροφορίες που κωδικοποιούνται με αυτά δημοσιοποιούνται. Κύριο εργαλείο αυτής της διαδικασίας είναι το Πιστοποιητικό (Certificate).

Στη βασική του μορφή ένα πιστοποιητικό δεν είναι τίποτε άλλο παρά μόνο η τιμή ενός δημοσίου κλειδιού. Στην πραγματικότητα ένα πιστοποιητικό είναι μία συλλογή πληροφοριών, οι οποίες έχουν υπογραφεί ηλεκτρονικά από τον εκδότη τους.

Τα πιστοποιητικά ανάλογα με το περιεχόμενό τους, διακρίνονται σε δύο κατηγορίες: α) Πιστοποιητικά Ταυτότητας (Identity Certificates), τα οποία δηλώνουν την ταυτότητα μίας οντότητας και τη συσχετίζουνε με την τιμή ενός δημόσιου κλειδιού και β) Πιστωτικά Πιστοποιητικά (Credential Certificates), τα οποία δεν αντιστοιχούν σε οντότητες αλλά περιγράφουν άδειες χρήσης ή πιστωτικά υπόλοιπα.

Χρήστης Πιστοποιητικού καλείται μία οντότητα, η οποία εξαρτάται από τις πληροφορίες, που περιέχονται σε ένα πιστοποιητικό. Ο χρήστης πιστοποιητικών εμπιστεύεται μία αρχή έκδοσης πιστοποιητικών, (Certification Authority). Κύρια λειτουργία της αρχής έκδοσης πιστοποιητικών (εφεξής “CA”) είναι να αποδέχεται αιτήσεις για πιστοποίηση της ταυτότητας διαφόρων οντοτήτων, στη συνέχεια, με γνώμονα την πολιτική της, να πιστοποιεί ή όχι την ταυτότητα της αιτούσας οντότητας και να εκδίδει ανάλογο πιστοποιητικό. Τα πιστοποιητικά που εκδίδει, τα αποθηκεύει σε δημόσια ευρετήρια από τα οποία μπορεί κάθε ενδιαφερόμενος να τα ανακτήσει προκειμένου να εξετάσει την ισχύ μίας ηλεκτρονικής υπογραφής ή να κρυπτογραφήσει ένα μήνυμα. Τα περισσότερα PKI ευρετήρια βασίζονται στο πρότυπο X.500 (βλέπε §3.3.3).

‘Αλλη μία λειτουργία της CA είναι να ανακαλεί πιστοποιητικά. ‘Ομως και αυτή η λειτουργία θα εξετασθεί στην §3.4.2.3, η οποία αναφέρεται στην επαλήθευση πιστοποιητικών. Επειδή οι υπηρεσίες των CA, είναι ανάλογες με τις υπηρεσίες που παρέχουν τα γραφεία εκδόσεως διαβατηρίων ή αδειών οδήγησης, κάθε CA θα πρέπει να ελέγχεται από κάποιους, οι οποίοι συγκεντρώνουν υψηλά επίπεδα εμπιστοσύνης και για αυτό το λόγο οι CA συναντώνται και ως Εμπιστευόμενα Τρίτα Μέρη (Trusty Third Parties, TTP).

Το κυριότερο πρόβλημα που αντιμετωπίζει το Διαδίκτυο σήμερα είναι η έλλειψη διαφάνειας ως προς την ταυτότητα, δύο οντοτήτων που συμμετέχουν σε μία συναλλαγή. Αυτή την έλλειψη διαφάνειας έρχεται να καλύψει η PKI. Ωστόσο εξαιτίας της πολυπλοκότητας του Διαδικτύου δεν είναι δυνατόν να υπάρξει ένας παγκόσμιος TTP, ο οποίος να εκδίδει πιστοποιητικά για όλους τους χρήστες, σε όλες τις χώρες του κόσμου.

Για την αντιμετώπιση του ως άνω προβλήματος έχουν αναπτυχθεί τρεις διαφορετικές αρχιτεκτονικές, η PKI με μια CA,το ιεραρχικό μοντέλο CA και το μικτό μοντέλο CA.

A. PKI με μόνο μία CA

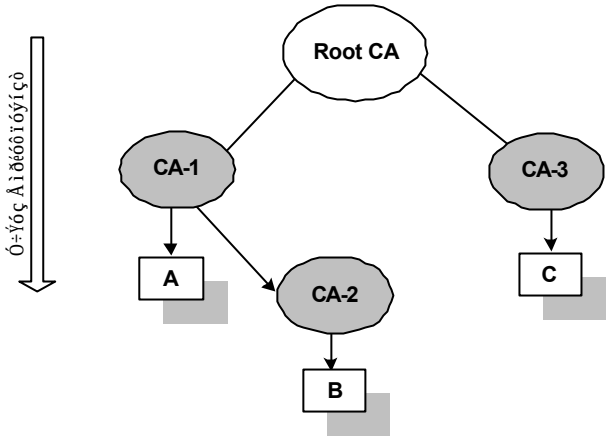
Σε αυτήν την αρχιτεκτονική θεωρούμε ότι μια μόνο CA έχει εκδώσει τα πιστοποιητικά δύο οντοτήτων A και B. Συνεπώς για να επικοινωνήσει με ασφάλεια ο A με τον B αρκεί να έχει το δημόσιο κλειδί της CA, την οποία εμπιστεύεται, κατ' αυτόν τον τρόπο μεταβατικά η εμπιστοσύνη αυτή μεταφέρεται από την CA στον B. Αυτή η θεώρηση είναι εφαρμόσιμη για μικρό αριθμό χρηστών, διότι όσο μεγαλύτερη είναι η ομάδα χρηστών που εξυπηρετείται από την CA, τόσο δυσκολότερο είναι για αυτήν να υποστηρίξει τεχνικά τις λειτουργίες PKI. Σαν φυσικό επακόλουθο των ανωτέρω έρχεται η δημιουργία πολλών CA, οι οποίες εξυπηρετούν πολλούς χρήστες και η ανάπτυξη σχέσεων εμπιστοσύνης ανάμεσά τους. Ο συσχετισμός των CA's μπορεί να γίνει με δύο βασικούς τρόπους είτε αναπτύσσοντας σχέση προϊσταμένου – υφισταμένου είτε αναπτύσσοντας σχέση ομοτίμων.Κάθε μέθοδος παρουσιάζει πλεονεκτήματα και μειονεκτήματα, στην πραγματικότητα όμως οι δύο παραπάνω μέθοδοι συνδυάζονται για την κατασκευή σύνθετων δομών PKI.

'Εστω ότι έχουμε τρεις οντότητες A, B, C, οι οποίες συνδέονται με τις CA-1, CA-2 και CA-3 αντίστοιχα. Αυτές οι τρεις οντότητες δεν μπορούν να αλληλεπιδράσουν μεταξύ τους με σχέση εμπιστοσύνης καθώς δεν υπάρχουν σχέσεις ανάμεσα στις CA τους. Προς άρση αυτής της αδυναμίας θα αναζητήσουμε τρόπους σύνδεσης ανάμεσα στις παραπάνω CA.

B. Ιεραρχικό μοντέλο PKI

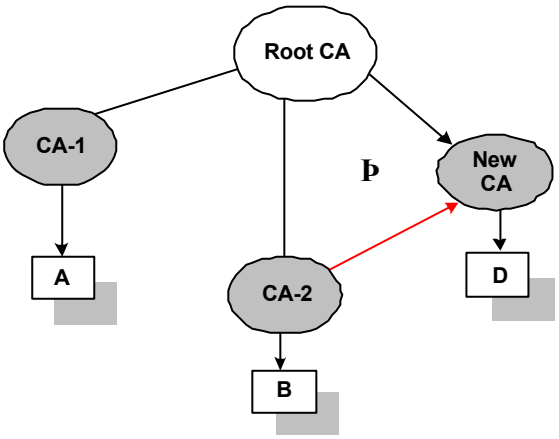
Μία PKI με σχέση προϊσταμένου – υφισταμένου ανάμεσα στις CA της αποκαλείται ιεραρχική PKI. Σε αυτή τη μεθοδολογία, όλοι οι χρήστες εμπιστεύονται την ίδια ρίζα CA. Κατ' αυτόν τον τρόπο όλοι οι χρήστες ξεκινούν τη διαδρομή των πιστοποιητικών τους με το δημόσιο κλειδί της ρίζας CA.

Γενικά η ρίζα CA δεν εκδίδει πιστοποιητικά σε μεμονωμένους χρήστες αλλά σε υφιστάμενες CA, οι οποίες μπορούν να εκδίδουν πιστοποιητικά σε χρήστες ή άλλες CA, που είναι υφιστάμενες αυτών. Συνεπώς στο ιεραρχικό μοντέλο PKI η σχέση εμπιστοσύνη είναι προς μία κατεύθυνση μόνον, από τη ρίζα CA προς τις υφισταμένες της CA, όπως άλλωστε παρουσιάζεται και στο Σχήμα 3.7.



Σχήμα 3.7
Ιεραρχικό μοντέλο PKI

Το ιεραρχικό μοντέλο PKI παρουσιάζει τέσσερις βασικές ιδιότητες, οι οποίες οφείλονται στην απλή δομή του και στο γεγονός ότι η σχέση εμπιστοσύνης ανάμεσα στις CA είναι μίας μόνο κατεύθυνσης. Η πρώτη ιδιότητα είναι η εύκολη επεκτασιμότητά του. Για να δημιουργηθεί σχέση εμπιστοσύνης με μια νέα CA το μόνο που απαιτείται είναι είτε η CA ρίζα να αποκτήσει σχέση εμπιστοσύνης με τη νέα CA είτε μια υφιστάμενη CA.



Σχήμα 3.8
Προσθήκη νέου CA σε ιεραρχικό μοντέλο PKI

Η δεύτερη ιδιότητα είναι ότι οι διαδρομές από το Πιστοποιητικό έως τη ρίζα είναι εύκολα αναγνωρίσιμες.

Η τρίτη ιδιότητα είναι ότι οι διαδρομές είναι μικρές. Η μεγαλύτερη διαδρομή είναι ίση με το βάθος του δέντρου συν ένα (1), δηλαδή το πιστοποιητικό CA για κάθε υφιστάμενη της CA ρίζα συν το πιστοποιητικό του χρήστη.

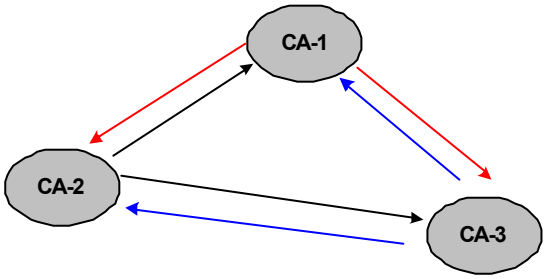
Η τέταρτη ιδιότητα είναι ότι τα πιστοποιητικά είναι μικρότερα και απλούστερα από αυτά που αναπτύσσονται στο μοντέλο μεικτού PKI.

Εκτός όμως από πλεονεκτήματα η ιεραρχική δομή PKI έχει και μειονεκτήματα τα οποία πηγάζουν κυρίως από το γεγονός ότι όλα εξαρτώνται από ένα σημείο αναφοράς (ρίζα CA). Εάν η ρίζα δεχθεί πλήγμα τότε όλα το οικοδόμημα PKI που στηρίζεται σε αυτή χάνει την αξιοπιστία της. 'Αλλο σημαντικό μειονέκτημα είναι ότι στο σημερινό ανταγωνιστικό εταιρικό περιβάλλον είναι σχεδόν αδύνατον να υπάρξει συμφωνία για το ποία θα είναι η ρίζα CA. Τελευταίο και σημαντικότερο μειονέκτημα είναι ότι η μετάβαση από ένα μοντέλο απομονωμένης CA PKI σε ένα μοντέλο ιεραρχικής CA PKI, μπορεί να είναι πρακτικά ή οικονομικά ασύμφορη επειδή όλοι οι χρήστες που ανήκουν στην PKI της απομονωμένης CA πρέπει να αλλάξουν το σημείο εμπιστοσύνης τους, τοποθετώντας το στη ρίζα CA. Παραδοσιακά εναλλακτική πρόταση στο ιεραρχικό μοντέλο PKI είναι το μοντέλο ομότιμη προς ομότιμη.

Γ. Μικτό μοντέλο PKI

Μία PKI που είναι δομημένη με σχέση ομότιμη προς ομότιμη ανάμεσα στις CA του λέγεται δίκτυο ή δίκτυο εμπιστοσύνης PKI.

Σε αυτό το μοντέλο όλες οι CA θεωρούνται ως σημεία εμπιστοσύνης. Οι CA εκδίδουν πιστοποιητικά για τους χρήστες τους, αλλά και πιστοποιητικά μεταξύ τους, στα οποία περιγράφουν την αμφίδρομη σχέση εμπιστοσύνης ανάμεσά τους.



Σχήμα 3.9
Διάγραμμα των σχέσεων ανάμεσα στους CA ενός δικτύου PKI

Τα δίκτυα PKI έχουν αρκετές χρήσιμες ιδιότητες. Κατ' αρχήν εύκολα προσθέτουν στη δομή τους καινούργιες CA, αρκεί μια υπάρχουσα CA να αναπτύξει σχέση εμπιστοσύνης με αυτή, ενώ είναι και ιδιαιτέρως ευπροσάρμοστο μοντέλο μιας και αποτελείται από πολλά σημεία εμπιστοσύνης. 'Ετσι τυχόν απώλεια της αξιοπιστίας μιας CA δεν οδηγεί στην κατάρρευση της PKI αφού αυτή εύκολα απομονώνεται από τις υπόλοιπες. Ακόμη μπορεί εύκολα να σχηματισθεί από απομονωμένες CA επειδή οι χρήστες που υπάγονται σε αυτές δεν απαιτείται να αλλάξουν το σημείο εμπιστοσύνης τους.

Παρ' όλες αυτές τις ελκυστικές ιδιότητες τα μοντέλα δικτύου PKI, παρουσιάζουν και κάποιες ανεπιθύμητες ιδιότητες που οφείλονται στην αμφίδρομη δόμηση των σχέσεων εμπιστοσύνης τους. Εν πρώτοις οι διαδρομές δεν είναι μοναδικές, καθώς είναι δυνατή η παρακολούθηση περισσοτέρων από μίας διαδρομής, που κάποιες από αυτές οδηγούν σε έγκυρες διαδρομές, ενώ άλλες οδηγούν σε αδιέξοδα. Τέλος η επεκτασιμότητα εκτός από μεγάλο πλεονέκτημα αποτελεί και τεράστιο μειονέκτημα για το μοντέλο δικτύου PKI, διότι το μέγιστο μήκος μιας διαδρομής είναι θεωρητικά ίσο με το πλήθος των CA που υπάρχουν στο μοντέλο.

3.3.2.3 Επικύρωση πιστοποιητικών

Η δεύτερη βασική λειτουργία PKI είναι η επικύρωση. Τα πιστοποιητικά περιέχουν πληροφορίες, οι οποίες δεν είναι στατικές αλλά μεταβαλλόμενες. 'Ετσι κάποιος ο οποίος πρόκειται να χρησιμοποιήσει ένα πιστοποιητικό, πρέπει να είναι σίγουρος ότι τα δεδομένα που περιέχονται σε αυτό δεν έχουν μεταβληθεί. Υπάρχουν δύο τρόποι για τον έλεγχο της ισχύος των πιστοποιητικών. Ο πρώτος τρόπος είναι η on line επαλήθευση, δηλαδή κάθε φορά που ένας χρήστης πρόκειται να χρησιμοποιήσει ένα πιστοποιητικό ρωτά την CA που το εξέδωσε εάν αυτό είναι σε ισχύ ή όχι. Ο δεύτερος τρόπος είναι η off line επαλήθευση.

Κάθε πιστοποιητικό περιλαμβάνει στις πληροφορίες του τη χρονική περίοδο για την οποία ισχύει. 'Αμεσα σχετιζόμενη με την επαλήθευση της ισχύος είναι η ανάκληση των πιστοποιητικών.

Ανάκληση είναι η διαδικασία γνωστοποίησης στους χρήστες των πιστοποιητικών που κατέστησαν άκυρα. Αυτό συμβαίνει στην περίπτωση που είτε το ιδιωτικό κλειδί ενός χρήστη έχει υποκλαπεί ή συχνότερα, όταν αλλάζει κάποια από τις προσωπικές πληροφορίες του χρήστη που περιλαμβάνεται στο πιστοποιητικό.

Στην περίπτωση της on line διαδικασίας επαλήθευσης δεν αντιμετωπίζονται ιδιαίτερα προβλήματα. Απλώς σε όποιο πιστοποιητικό παρουσιάζεται πρόβλημα, η CA δηλώνει ότι αποσύρει από αυτό την εμπιστοσύνη της. Το πρόβλημα εμφανίζεται όταν τα πιστοποιητικά έχουν συγκεκριμένη χρονική διάρκεια ισχύος. Η απάντηση σε αυτό το πρόβλημα είναι οι Λίστες Ανακληθέντων Πιστοποιητικών (Certificate Revocation List, εφεξής CRL).

Οι CRL είναι λίστες από άκυρα πιστοποιητικά , οι οποίες θεωρούνται από την CA και εκδίδονται από αυτή περιοδικά. 'Ομως και αυτή η θεώρηση του προβλήματος παρουσιάζει μερικές δυσκολίες. Η πρώτη από αυτές είναι το τι γίνεται στο διάστημα που μεσολαβεί μεταξύ δύο διαδοχικών εκδόσεων CRL. Η λύση αυτού του προβλήματος δίνεται από τις Delta CRL, οι οποίες είναι εκδόσεις CRL, που περιέχουν μόνον τα πιστοποιητικά που έχουν ανακληθεί από την τελευταία έκδοση του CRL μέχρι και την έκδοση της Delta CRL.

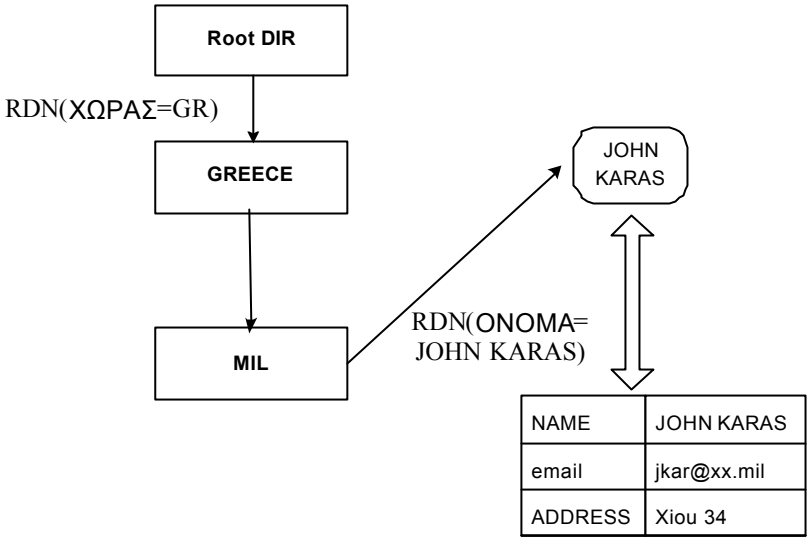
Το δεύτερο μεγάλο πρόβλημα είναι το μέγεθος των CRL. Το πρόβλημα αυτό σχετίζεται με τους χρόνους ανάκτησης των CRL από τους αποθηκευτικούς χώρους της CA. Πιθανή επίλυση αυτού του προβλήματος

θα ήταν η αύξηση του εύρους ζώνης των CA και η δημιουργία διαφορετικών CRL ανάλογα με το είδος του πιστοποιητικού και την αιτία ανάκλησής του. 'Ετσι διακρίνουμε σε CRL με μεταβολές επουσιωδών στοιχείων και σε CRL με μεταβολές στα θέματα ασφαλείας, που είναι και τα πλέον σημαντικά.

3.3.3 Το Πρότυπο X.500

Το X.500 είναι ένα ηλεκτρονικό ευρετήριο το οποίο έχει στηριχθεί στην δομή των κοινών τηλεφωνικών ευρετηρίων. Η μεγάλη αξία του X.500 και η οποία το διαφοροποιεί από τα κοινά ευρετήρια είναι ότι σε μια εγγραφή του μπορούμε να προσθέσουμε μια ομάδα ιδιοτήτων που μπορούν να περιέχουν επαγγελματικά στοιχεία ή οτιδήποτε άλλο επιθυμούμε. 'Αλλο ένα σημαντικό χαρακτηριστικό είναι ότι με αυτό μπορούμε να αναπαραστήσουμε όχι μόνο φυσικά πρόσωπα αλλά και κάθε άλλη οντότητα, όπως εταιρείες ή προϊόντα ή ακόμα και πληροφορίες για πιστοποιητικά στα πλαίσια της PKI. Η αναζήτηση σε αυτό το ευρετήριο γίνεται με ένα μοναδικό όνομα που λέγεται Ξεχωριστό 'Ονομα (Distinguished Name, DN). Η δομή του είναι ιεραρχική και καλείται Δένδρο Πληροφορίας Καταλόγου (Directory Information Tree, DIT). Κάθε κόμβος του δέντρου λέγεται ακμή (vertex), έχει ένα κατάλογο πατέρα (parent directory) και πολλούς καταλόγους παιδιά (children directory) και παίρνει ένα όνομα το οποίο λέγεται Ξεχωριστό 'Ονομα Συγγενή (Relative Distinguished Name, RDN) ενώ στην συνέχεια κάθε παιδί του vertex παίρνει το δικό του RD.

Σύμφωνα με το πρότυπο, υπό τον κατάλογο που αποτελεί τη ρίζα (root directory) υπάρχουν ακμές για όλα τα κράτη του κόσμου, τα οποία έχουν RDN τα δύο πρώτα γράμματα της χώρας κατά την τυποποίηση ISO. Κάτω από την ακμή κάθε χώρας υπάρχουν παιδιά για όλους τους οργανισμούς, υπηρεσίες και εταιρείες της χώρας στους οποίους αποδίδονται νέα μοναδικά RDN. Κάτω από αυτέ τις ακμές υπάρχουν και άλλα παιδιά και ούτω καθ' εξής ώσπου τελικά φτάνουμε στην τελευταία ακμή του κόμβου, η οποία και έχει το δικό της DN. Το Σχήμα 3.9 απεικονίζει τη δομή του X.500.



Σχήμα 3.9
Το σύστημα ονοματοδοσίας στο ευρετήριο X.500

Οι παραπάνω διαδικασίες λαμβάνουν χώρα με την βοήθεια του προτύπου X.509. Το X509 πρωτοεμφανίστηκε το 1988 με σκοπό την υποστήριξη καταλόγου του X.500, έχει καθιερωθεί ως πρότυπο πιστοποιητικών από τον οργανισμό ISO/ITU και χρησιμοποιείται από πολλές εταιρείες σε όλο τον κόσμο ως βάση για PKI. Σήμερα βρίσκεται στην έκδοση 3.

Τα βασικά χαρακτηριστικά των πιστοποιητικών και CRL που εκδίδονται σύμφωνα με αυτό παρουσιάζονται στα παραρτήματα Α και Β.

Παράρτημα Α

X.509v3 Certificate

Η τελευταία έκδοση του X.509 ξεπερνά τον ρόλο του ως μέσου υποστήριξης των ευρετηρίων X.500 διότι υποστηρίζει πολλαπλά ονόματα και ιδιότητες για κάθε οντότητα στην οποία ανήκει το πιστοποιητικό.

Τα κύρια χαρακτηριστικά του είναι:

Certificate Version	Η έκδοση X.509 με την οποία δημιουργήθηκε.
Certificate Serial Number	Μοναδικός αριθμός που εκδίδεται από την CA.
Certificate Path Constraints	Περιορισμός των Path διάδοσης του (CA's POLICY)
Certificate CA's Policy	Περιγράφεται η πολιτική της CA αν υπάρχει που αφορά στην έκδοση πιστοποιητικών
CA's Signature Algorithm ID	Πληροφορίες σχετικές με τον αλγόριθμο κωδικοποίησης της CA
CA's X.500 Name	Το X.500 όνομα της CA
CA's X.500 Additional Attributes	Πιθανό άλλο στοιχείο ταυτότητας της CA
CA's Alternative Name	Πιθανό άλλο όνομα της CA
Validity Period	Χρονική διάρκεια ισχύος της CA
Subject's X.500 Name	'Ονομα του ιδιοκτήτη του Cert
Subject's Additional Attributes	Πιθανό άλλο στοιχείο ταυτότητας του ιδιοκτήτη του Cert.
Subject's Alternative Name	Πιθανό άλλο όνομα του ιδιοκτήτη του Cert
SUBJECT'S PUBLIC KEY	Δημόσιο κλειδί του ιδιοκτήτη του Cert
Hash Function	Εφαρμογή Hash συνάρτησης στο Cert
CA's Private Key	Κωδικοποίηση με το ιδιωτικό κλειδί της CA

Παράρτημα Β

X.509v3 Revocation Certificate List

Τα κύρια χαρακτηριστικά των CRL εκδίδονται σύμφωνα με το πρότυπο X.509v3 είναι:

CRL Version	Η έκδοση X.509 με την οποία δημιουργήθηκε.
CRL Number and Reason Codes	Ο αριθμός του CRL και ο κωδικός που αντιστοιχεί στην αιτία έκδοσης
CRL Distribution Path	Περιορισμός των Path διάδοσης του (CA's POLICY)
CRL Delta Version	Αριθμός της DELTA αν υπάρχει
Issuers Signature Algorithm ID	Πληροφορίες σχετικές με τον αλγόριθμο κωδικοποίησης του εκδότη
Issuers X.500 Name	Το X.500 όνομα του εκδότη
Issuers Additional Attributes	Πιθανό άλλο στοιχείο ταυτότητας του εκδότη
Issuers Alternative Name	Πιθανό άλλο όνομα του εκδότη
Date & Time Of Current Update	Ημερομηνία και ώρα έκδοσης
Date & Time Of Next Update	Ημερομηνία και ώρα έκδοσης επόμενης έκδοσης
Certificate S/N — Revocation DATE . . . . Certificate S/N — Revocation DATE	ÁíáêëçèÝíôá ðéóôïðïéçôéêÜ
Hash Function	Εφαρμογή Hash συνάρτησης στη CRL
Issuer's Private Key	Κωδικοποίηση με το ιδιωτικό κλειδί του εκδότη