ΑΛΕΞΑΝΔΡΕΙΟ Τ.Ε.Ι. ΘΕΣΣΑΛΟΝΙΚΗΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πτυχιακή Εργασία

Δημιουργία οδηγού για την ασφαλή διακίνηση ηλεκτρονικού ταχυδρομείου και εγγράφων

Του φοιτητή
Σταλίδη Παναγιώτη
Αρ. Μητρώου**: 1284**

Επιβλέπων Καθηγητής
Βαφειάδης Αντώνης
Καθηγητής

Θεσσαλονίκη 2010

ΠΡΟΛΟΓΟΣ

Την τελευταία δεκαετία, η χρήση των ηλεκτρονικών υπολογιστών και του διαδικτύου, δεν περιορίζεται στους ειδικούς, αλλά έχει εξαπλωθεί σε ανθρώπους όλων των επαγγελματικών και κοινωνικών ομάδων. Η ταχύτητα ανάπτυξης νέων τεχνολογιών, δεν επιτρέπει στους νέους χρήστες να ακολουθήσουν τις εξελίξεις, με αποτέλεσμα πολλές από αυτές τις τεχνολογίες να μένουν ουσιαστικά ανεκμετάλλευτες. Η ραγδαία ανάπτυξη του ηλεκτρονικού εμπορίου αλλά και η μετάβαση παραδοσιακών υπηρεσιών σε αντίστοιχες ηλεκτρονικές, κάνουν επίσης το θέμα της ασφάλειας και ηλεκτρονικής ταυτοποίησης πρωτεύον. Η χρήση ηλεκτρονικών πιστοποιητικών ασφάλειας και ταυτοποίησης καθώς και η νομική εγκυρότητα των ηλεκτρονικών συναλλαγών προδιαγράφονται από την Ευρωπαϊκή νομοθεσία με την Οδηγία 99/93/ ΕΚ, ενώ και η ελληνική νομοθεσία προσαρμόζεται με την οδηγία αυτή με την έκδοση δύο Προεδρικών Διαταγμάτων. Πιο συγκεκριμένα, στο Π.Δ. 150/2001 ορίζονται η ηλεκτρονική υπογραφή, το ψηφιακό πιστοποιητικό καθώς και οι πάροχοι αυτών, ενώ με το Π.Δ.342/2002 επιβάλλεται η ηλεκτρονική υπογραφή για την διακίνηση εγγράφων μέσω ηλεκτρονικού ταχυδρομείου, είτε πρόκειται για έγγραφα μεταξύ υπηρεσιών, είτε πρόκειται για συναλλαγές υπηρεσιών με φυσικά πρόσωπα.

Είναι φανερό, ότι η αφομοίωση των νέων αυτών τεχνολογιών είναι πλέον επιτακτική και η χρήση τους από ένα συνεχώς αυξανόμενο κύκλο χρηστών είναι επιβεβλημένη. Ήταν λοιπόν σκόπιμο να δημιουργηθεί ένας πληροφοριακός οδηγός προς τους χρήστες του διαδικτύου και ειδικότερα προς αυτούς που χρησιμοποιούν το ηλεκτρονικό ταχυδρομείο, που να τους καθοδηγεί σχετικά με την υιοθέτηση τεχνολογιών ασφάλειας στο ηλεκτρονικό ταχυδρομείο. Στον οδηγό αυτό παρουσιάζονται οι βασικές διαθέσιμες τεχνολογίες ασφάλειας και ταυτοποίησης ηλεκτρονικού ταχυδρομείου, τα κύρια χαρακτηριστικά τους και οι τρόποι αποτελεσματικής χρήσης τους στην καθημερινή πράξη.

ΠΕΡΙΛΗΨΗ

Ο σκοπός της εργασίας αυτής είναι η δημιουργία ενός «Οδηγού Ασφάλειας» για το ηλεκτρονικό ταχυδρομείο, που να περιγράφει τις βασικές διαθέσιμες τεχνολογίες ασφάλειας και ταυτοποίησης και να καθοδηγεί τους χρήστες ηλεκτρονικού ταχυδρομείου στην υιοθέτησή τους. Ο Οδηγός αυτός αναφέρεται στις βασικές αρχές, τα κυριότερα χαρακτηριστικά και τον τρόπο εφαρμογής των επικρατέστερων τεχνολογιών, ώστε να αποτελεί χρήσιμη αναφορά, τόσο για τον μη ειδικό σε θέματα υπολογιστών χρήστη, όσο και για αυτόν που αναζητά κάτι πιο εξειδικευμένο.

Ο απλός χρήστης ηλεκτρονικού ταχυδρομείου εισάγεται στη φιλοσοφία της ηλεκτρονικής ασφάλειας και μπορεί να αποκτήσει μια ολοκληρωμένη εικόνα για το σκοπό και την εφαρμοσιμότητα των διαθέσιμων τεχνολογιών. Για το σκοπό αυτό έχει χρησιμοποιηθεί απλή γλώσσα και μεγάλος αριθμός από διαγράμματα. Ο εξειδικευμένος αναγνώστης μπορεί να βρει περισσότερες λεπτομέρειες, όπως περιγραφές αλγορίθμων, προηγμένες τεχνικές για ειδικές εφαρμογές και επίσης αναφορές για εκτενέστερη έρευνα.

Ο Οδηγός επίσης περιλαμβάνει αναλυτικές οδηγίες σε μορφή «Βήμα προς Βήμα» για την εγκατάσταση πιστοποιητικών ασφαλείας. Έτσι ο αναγνώστης καθοδηγείται με πρακτικό και απλό τρόπο στη χρήση μιας από τις βασικότερες και συνηθέστερες τεχνολογίες ασφάλειας ηλεκτρονικού ταχυδρομείου.

ABSTRACT

Computer security has been a field of study mainly for theoretical computer scientists for a long time. Due to the proliferation of computer systems in general and the Internet and World Wide Web in particular, this situation has changed dramatically. Today, computer and network practitioners are equally interested in computer security.

Having this in mind, the scope of this paper is to give these people a deeper understanding of the technologies and solutions available to them today.

Through the first, second and third chapters, the reader can learn about technologies and protocols concerning the exchange of electronic mail (email) and the threats hidden there. He can learn about the OSI protocol stack and the secure versions of communication protocols through the use of Secure Socket Layer (SSL). He can also learn how data can be encrypted and decrypted and the protocols used for the process.

In chapters four and five, the history and use of PGP (Pretty Good Privacy) and S/MIME (Secure / Multipurpose Internet Mail Extensions) are explained.

Chapter six contains information concerning system and network administrators on setting up websites and servers for the use of SSL, Certificates and Digital Signatures.

Finally, chapter seven illustrates through an easy to follow guide, the steps necessary, for an email service user, to send and receive cryptographically secure and digitally signed messages.

ΕΥΧΑΡΙΣΤΙΕΣ

Θέλω να ευχαριστήσω τον καθηγητή μου κ. Βαφειάδη, για την πολύτιμη βοήθειά του καθώς και για την υπομονή του ώστε αυτή η εργασία να γίνει πραγματικότητα.

Επίσης, θέλω να ευχαριστήσω την οικογένεια και τους φίλους μου για την επιμονή τους και την στήριξή τους.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΡΟΛΟΓΟΣ....5
ΠΕΡΙΛΗΨΗ....6
ABSTRACT....7
ΕΥΧΑΡΙΣΤΙΕΣ....9
ΠΕΡΙΕΧΟΜΕΝΑ....11
ΕΙΣΑΓΩΓΗ....17
1. ΗΛΕΚΤΡΟΝΙΚΟ ΤΑΧΥΔΡΟΜΕΙΟ....19
1.1 Ο ΜΗΧΑΝΙΣΜΟΣ ΜΕΤΑΦΟΡΑΣ ΜΗΝΥΜΑΤΩΝ....19
Αποστολή μηνύματος....20
Μεταφορά μηνύματος....20
Παραλαβή μηνύματος....21
1.2 ΑΠΕΙΛΕΣ ΚΑΙ ΕΠΙΘΕΣΕΙΣ....21
Παθητικές επιθέσεις....21
Ενεργές επιθέσεις....22
Κίνδυνοι που δημιουργούνται....22
1.3 ΑΣΦΑΛΗΣ ΕΠΙΚΟΙΝΩΝΙΑ....23
Υλοποίηση....23
2. ΤΟ ΠΡΩΤΟΚΟΛΛΟ SSL....25
2.1 ΤΕΧΝΙΚΕΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ....25
2.2 ΣΥΝΟΨΕΙΣ ΜΗΝΥΜΑΤΩΝ....26
2.3 ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ....27
2.4 ΠΙΣΤΟΠΟΙΗΤΙΚΑ....28
2.5 ΠΕΡΙΕΧΟΜΕΝΑ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ....28
2.6 ΑΡΧΕΣ ΠΙΣΤΟΠΟΙΗΣΗΣ....31
Αλυσίδες Πιστοποιητικών....31
Δημιουργία μιας Υψηλότερου Επιπέδου Γονικής Αρχής Πιστοποίησης....31
Διαχείριση Πιστοποιητικών....32
2.7 ΤΟ ΠΡΩΤΟΚΟΛΛΟ SSL....32
Εδραίωση Συνεδρίας....33
Μέθοδος ανταλλαγής κλειδιού....34
Κρυπτογραφική μέθοδος για μεταφορά δεδομένων....34
Συνάρτηση Σύνοψης....35
Πρωτόκολλο Ακολουθίας Χειραψίας....35
Μεταφορά Δεδομένων....36
3. ΚΡΥΠΤΟΓΡΑΦΙΑ....37
3.1 ΣΥΜΜΕΤΡΙΚΟ ΚΛΕΙΔΙ....37
3.2 Ο ΑΛΓΟΡΙΘΜΟΣ DES....38
3.3 ΑΣΥΜΜΕΤΡΟ ΚΛΕΙΔΙ....42
3.4 Ο ΑΛΓΟΡΙΘΜΟΣ RSA....43
4. ΤΟ ΠΡΩΤΟΚΟΛΛΟ PGP....45
4.1 ΙΣΤΟΡΙΑ ΚΑΙ ΑΝΑΠΤΥΞΗ....45

4.2 ΠΕΡΙΓΡΑΦΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ....45
Εισαγωγή....46
Υποστηριζόμενοι αλγόριθμοι....47
Επεξεργασία μηνύματος....47
Κρυπτογραφικά κλειδιά....48
4.3 ΔΙΚΤΥΟ ΕΜΠΙΣΤΟΣΥΝΗΣ....49
Πιστοποιητικά PGP....49
Θεμελίωση εμπιστοσύνης....50
Ανάκληση κλειδιού....50
Διακομιστές πιστοποιητικών PGP....51
Συμπεράσματα....51
4.4 ΠΡΟΙΟΝΤΑ ΥΛΟΠΟΙΗΣΗΣ....51
5. S/MIME....52
5.1 ΙΣΤΟΡΙΑ ΚΑΙ ΑΝΑΠΤΥΞΗ....52
5.2 ΠΕΡΙΓΡΑΦΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ....53
Εισαγωγή....53
Υποστηριζόμενοι αλγόριθμοι....54
Επεξεργασία μηνύματος....54
Κρυπτογραφικά κλειδιά....55
5.3 ΥΠΟΔΟΜΗ ΔΙΑΧΕΙΡΙΣΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ....56
Θεμελίωση εμπιστοσύνης....57
Ανάκληση πιστοποιητικού....58
Παροχείς πιστοποιητικών....59
Συμπεράσματα....59
5.4 ΠΡΟΪΟΝΤΑ ΥΛΟΠΟΙΗΣΗΣ....59
6. ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ....60
6.1 ΧΡΗΣΕΙΣ ΤΩΝ ΨΗΦΙΑΚΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ....60
Εμπιστευτικότητα....60
Πιστοποίηση....60
Ακεραιότητα....61
Μη Άρνηση Αποδοχής....61
6.2 ΧΡΗΣΗ ΤΩΝ ΨΗΦΙΑΚΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΑΠΟ ΔΙΑΚΟΜΙΣΤΕΣ....62
Χρήση των ψηφιακών πιστοποιητικών στην υπηρεσία παγκόσμιου ηλεκτρονικού ιστού....62
Δημιουργία κλειδιών και έκδοση πιστοποιητικού....62
Δημιουργία κλειδιού....62
Δημιουργία αίτησης για έκδοση πιστοποιητικού....63
Αποστολή της αίτησης και έκδοση πιστοποιητικού....63
Εργασίες με πιστοποιητικά....63
Πιστοποίηση ταυτότητας πελάτη με χρήση πιστοποιητικών....65
Χρήση των ψηφιακών πιστοποιητικών στην υπηρεσία διαμεταγωγής ηλεκτρονικού ταχυδρομείου....66
Μεταγλώττιση του λογισμικού sendmail με υποστήριξη TLS....66
Έκδοση ψηφιακών πιστοποιητικών για διακομιστή....67
Ρύθμιση του λογισμικού sendmail....67
Ορισμός του περιέχοντος φακέλου των πιστοποιητικών και των κλειδιών....67

Χρήση των ψηφιακών πιστοποιητικών σε άλλες υπηρεσίες.....67
Έκδοση ψηφιακών πιστοποιητικών για διακομιστή.....68
Δημιουργία βοηθητικών διαύλων.....68
7. ΧΡΗΣΗ ΨΗΦΙΑΚΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΑΠΟ ΠΕΛΑΤΕΣ.....70
7.1 ΕΓΚΑΤΑΣΤΑΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ ΣΤΟΝ INTERNET EXPLORER.....71
7.2 ΕΓΚΑΤΑΣΤΑΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ ΣΤΟ MOZILLA FIREFOX.....79
7.3 ΧΡΗΣΗ ΤΟΥ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ ΣΤΟ MICROSOFT OUTLOOK.....84
ΑΠΟΣΤΟΛΗ ΜΗΝΥΜΑΤΟΣ.....89
ΛΗΨΗ ΜΗΝΥΜΑΤΟΣ.....93
7.4 ΧΡΗΣΗ ΤΟΥ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ ΣΤΟ MOZILLA THUNDERBIRD.....96
ΑΠΟΣΤΟΛΗ ΜΗΝΥΜΑΤΟΣ.....98
ΣΥΜΠΕΡΑΣΜΑΤΑ.....103
ΒΙΒΛΙΟΓΡΑΦΙΑ.....104

Ευρετήριο Πινάκων

Πίνακας 2.1: Πληροφορίες Πιστοποιητικού.....28
Πίνακας 2.2: Πληροφορίες Διακεκριμένου Ονόματος.....30
Πίνακας 2.3: Εκδόσεις Του Πρωτοκόλλου SSL.....33

Ευρετήριο Σχημάτων

Σχήμα 2.1: Το πρωτόκολλο εγγραφής SSL (SSL record protocol) 36
Σχήμα 3.2: Η συνολική δομή του αλγορίθμου DES.....39
Σχήμα 3.3: Διαδικασία του Feistel.....40
Σχήμα 3.4: Αλγόριθμος προγραμματισμού κλειδιών.....41
Σχήμα 3.5: Ασύμμετρο Κλειδί.....43

ΕΙΣΑΓΩΓΗ

Στο πρώτο κεφάλαιο, ο αναγνώστης εισάγεται στα πρωτόκολλα και τον τρόπο λειτουργίας του ηλεκτρονικού ταχυδρομείου. Παρουσιάζονται τα εγγενή προβλήματα ασφαλείας που περιέχουν καθώς και οι κίνδυνοι που συνάγουν.

Στο δεύτερο κεφάλαιο παρουσιάζεται το πρωτόκολλο SSL. Η χρήση αυτού του πρωτοκόλλου επιτρέπει την ασφαλή ανταλλαγή πληροφοριών μεταξύ χρηστών και διακομιστών καθώς και στη δημιουργία κλειδιών κρυπτογράφησης.

Οι λεπτομέρειες των αλγορίθμων κρυπτογράφησης παρουσιάζονται στο τρίτο κεφάλαιο. Οι αλγόριθμοι αυτοί αφορούν πιο εξειδικευμένους αναγνώστες.

Στα κεφάλαια τέσσερα και πέντε περιγράφονται τα πρωτόκολλα PGP και S/MIME. Αναπτύσσεται η ιστορική τους διαδρομή, η νοοτροπία στη χρήση τους και ο τρόπος με τον οποίο παρέχουν ασφάλεια στην επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου.

Στο έκτο κεφάλαιο παρουσιάζεται η χρήση των ψηφιακών πιστοποιητικών και της ψηφιακής υπογραφής από τους παρόχους περιεχομένου στο διαδίκτυο καθώς και οι απαραίτητες ενέργειες των διαχειριστών ενός ιστοτόπου για την παροχή ασφαλών υπηρεσιών προς τους χρήστες.

Τέλος, στο έβδομο κεφάλαιο, δίνονται οδηγίες “Βήμα προς Βήμα” προς τους χρήστες υπηρεσιών ηλεκτρονικού ταχυδρομείου, κατά περίπτωση λογισμικού που χρησιμοποιούν, ώστε η επικοινωνία τους να γίνεται με ασφάλεια και εγκυρότητα.

1. ΗΛΕΚΤΡΟΝΙΚΟ ΤΑΧΥΔΡΟΜΕΙΟ

Η σύγχρονη πραγματικότητα του 21ου αιώνα, επιβάλλει όλο και περισσότερο την χρήση των ηλεκτρονικών υπολογιστών καθώς και την επικοινωνία μέσω αυτών. Ο πιο διαδεδομένος τρόπος ώστε να επιτευχθεί αυτή η επικοινωνία, είναι η χρήση του ηλεκτρονικού ταχυδρομείου. Αντίστοιχα με την παραδοσιακή αλληλογραφία, το ηλεκτρονικό ταχυδρομείο αποτελείται από δύο τμήματα, την διεπαφή της υπηρεσίας με τον χρήστη και την εσωτερική διανομή της αλληλογραφίας. Παρόλα αυτά, η επικοινωνία με ηλεκτρονικό ταχυδρομείο (email) δεν είναι ιδιαίτερα ασφαλής. Πολλοί είναι αυτοί που χρησιμοποιούν το email στην καθημερινή επαγγελματική ή προσωπική τους επικοινωνία έχοντας την ψευδαίσθηση ότι οι πληροφορίες που μεταφέρονται παραμένουν εμπιστευτικές. Αυτό που ίσως προκαλεί έκπληξη, είναι ότι το email αποτελεί τον παράδεισο του επίδοξου υποκλοπέα. Στην πραγματικότητα, χωρίς να ληφθούν ειδικά μέτρα η ασφάλεια είναι ανύπαρκτη. Για παράδειγμα, μηνύματα που ο αποστολέας του νομίζει ότι έχουν διαγραφεί, ίσως βρίσκονται ακόμα σε κάποιο server στην άλλη πλευρά του πλανήτη και να τα διαβάζει οποιοσδήποτε. Επίσης, στο δρομολόγιο τους μέχρι τον τελικό παραλήπτη, τα μηνύματα μπορεί να τροποποιηθούν χωρίς αυτό να γίνει αντιληπτό. Εκτός από τα ίδια τα μηνύματα, ακόμα και τα στοιχεία πιστοποίησης του χρήστη στον παροχέα του, μπορούν να κλαπούν και να χρησιμοποιηθούν από τρίτους. Σήμερα όλο και περισσότερες επαγγελματικές και προσωπικές επικοινωνίες πραγματοποιούνται σχεδόν αποκλειστικά μέσω email, επομένως η ασφάλεια, αλλά και η ακεραιότητα των πληροφοριών είναι μια διαρκώς αυξανόμενη απαίτηση.

1.1 Ο ΜΗΧΑΝΙΣΜΟΣ ΜΕΤΑΦΟΡΑΣ ΜΗΝΥΜΑΤΩΝ

Η διαδικασία αποστολής ενός email μπορεί να παρομοιαστεί με τον τρόπο που στέλνουμε γράμματα. Συγκεκριμένα οι παροχείς email αντιστοιχούν στα διάφορα υποκαταστήματα ταχυδρομείου. Το πρωτόκολλο SMTP (Small Message Transfer

Protocol), στο οποίο βασίζεται το email, είναι αντίστοιχο με τον τρόπο που δέχονται αυτά τα υποκαταστήματα γράμματα είτε από τους πελάτες τους, είτε από άλλα γειτονικά υποκαταστήματα ώστε να τα προωθήσουν μέχρι να φτάσουν στον τελικό προορισμό τους. Αναλυτικότερα, η διαδικασία μεταφοράς ενός μηνύματος είναι η παρακάτω:

Αποστολή μηνύματος

Για την πλειοψηφία των χρηστών υπάρχουν δύο τρόποι αποστολής email:

Χρήση εξειδικευμένου προγράμματος αποστολής email όπως είναι το MS Outlook ή το Mozilla Thunderbird.

Χρήση ενός προγράμματος πλοήγησης μέσω μιας διαδικτυακής διεπαφής.

Στην πρώτη περίπτωση, ο προσωπικός υπολογιστής του χρήστη επικοινωνεί απευθείας με τον διακομιστή του παροχέα χρησιμοποιώντας το πρωτόκολλο SMTP. Στη δεύτερη περίπτωση ο παροχέας προσφέρει στο χρήστη μια διαδικτυακή διεπαφή με την οποία ο τελευταίος επικοινωνεί με χρήση του WEB. Στη συνέχεια, αυτή η διεπαφή αναλαμβάνει να επικοινωνήσει με τον διακομιστή του παροχέα χρησιμοποιώντας το πρωτόκολλο SMTP. Αφού λοιπόν το email φτάσει, με οποιονδήποτε τρόπο, στον διακομιστή του παροχέα του αποστολέα, πρέπει με κάποιο τρόπο να προωθηθεί μέχρι τον παροχέα του παραλήπτη, απ’ όπου ο τελευταίος θα το παραλάβει.

Μεταφορά μηνύματος

Κάθε φορά που ένας παροχέας email παραλαμβάνει ένα μήνυμα με διεύθυνση διαφορετική από τη δική του, θα πρέπει να το προωθήσει σε άλλο παροχέα ο οποίος βρίσκεται πιο κοντά στο τελικό προορισμό. Και στο σημείο αυτό μας είναι χρήσιμος ο παραλληλισμός με την διαδικασία που ακολουθούν τα ταχυδρομεία. Όταν παραλαμβάνουν ένα γράμμα του οποίου ο προορισμός είναι σε άλλη περιοχή, το προωθούν σε άλλο υποκατάστημα που βρίσκεται πιο κοντά στην περιοχή προορισμού. Αντίστοιχα ένας SMTP Server έχει μια προκαθορισμένη λίστα που περιλαμβάνει περιοχές προορισμού, τους αντίστοιχους ενδιάμεσους παροχείς και τους εφεδρικούς τους. Εφόσον για οποιοδήποτε λόγο, πχ απώλεια ρεύματος, ο διακομιστής δεν μπορεί να στείλει το email στον προεπιλεγμένο διακομιστή για τη συγκεκριμένη περιοχή προορισμού, τότε το προωθεί στον πρώτο δηλωμένο εφεδρικό διακομιστή. Η ίδια διαδικασία ακολουθείται και όταν ο εφεδρικός διακομιστής αδυνατεί να παραλάβει το email, μέχρι να τελειώσει η λίστα με τους εφεδρικούς. Σε περίπτωση που συμβεί αυτό, η διαδικασία ξεκινά από την αρχή μετά από ένα προκαθορισμένο χρονικό διάστημα κατά το οποίο τα μηνύματα παραμένουν σε μια ουρά αναμονής.

Όταν το email φτάσει στο διακομιστή του παραλήπτη, τοποθετείται στη θυρίδα του παραλήπτη, όπου και θα παραμείνει μέχρι αυτός να το παραλάβει. Στη διαδικασία προώθησης των μηνυμάτων, κάθε διακομιστής που παραλαμβάνει το μήνυμα, έχει προσθέσει σε αυτό μετα-πληροφορίες σχετικά με την ώρα παραλαβής και το

διακομιστή που το προώθησε σε αυτόν.

Σε γενικές γραμμές πρέπει να γίνει κατανοητό, ότι:

- μέχρι ένα email να φτάσει από τον αποστολέα στη θυρίδα του παραλήπτη, όλες οι επικοινωνίες γίνονται με χρήση του πρωτοκόλλου SMTP
- είναι αδύνατο να γνωρίζεις εκ των προτέρων το χρονικό διάστημα που θα χρειαστεί για να φτάσει το email στο προορισμό του
- μπορεί το μήνυμα να βρίσκεται σε ένα πλήθος διακομιστών για ακαθόριστο χρονικό διάστημα
- όλοι οι παραλήπτες μπορούν να ξέρουν τη διεύθυνση και το όνομα του υπολογιστή απ' όπου στάλθηκε το email , αλλά και όλων των ενδιάμεσων διακομιστών.

Παραλαβή μηνύματος

Η παραλαβή του email από τη θυρίδα του παραλήπτη μπορεί να γίνει με τη χρήση ενός εκ των δύο διαφορετικών πρωτοκόλλων επικοινωνίας, του IMAP(Internet Message Access Protocol) και του POP(Post Office Protocol).

Ανεξάρτητα από το πρωτόκολλο που χρησιμοποιεί ο παραλήπτης, η παραλαβή του μηνύματος μπορεί να γίνει με δύο τρόπους

Απευθείας με ένα εξειδικευμένο πρόγραμμα, όπως το MS Outlook ή το Mozilla Thunderbird.

Μέσω μια διαδικτυακής διεπαφής και χρήση ενός προγράμματος πλοήγησης χρησιμοποιώντας το πρωτοκόλλο HTTP.

1.2 ΑΠΕΙΛΕΣ ΚΑΙ ΕΠΙΘΕΣΕΙΣ

Το ηλεκτρονικό ταχυδρομείο δεν σχεδιάστηκε με γνώμονα την ασφάλεια. Αυτό ισχύει για τα δημόσια και ιδιωτικά ταχυδρομεία και ακόμα περισσότερο για το ηλεκτρονικό ταχυδρομείο που χρησιμοποιείται στο διαδίκτυο. Η αποστολή πλαστών μηνυμάτων, η τροποποίηση μηνυμάτων κατά την μετάδοσή τους, όπως και η ανάγνωση ξένων μηνυμάτων είναι μια απλή διαδικασία με τον τρόπο που έχει σχεδιαστεί το ηλεκτρονικό ταχυδρομείο.

Παθητικές επιθέσεις

Οι παθητικές επιθέσεις απειλούν την εμπιστευτικότητα των μηνυμάτων που μεταδίδονται. Κατά την διάρκεια της μετάδοσης πληροφοριών από τον αποστολέα προς τον παραλήπτη, ο εισβολέας μπορεί να διαβάζει και να παρατηρεί τα δεδομένα. Αυτά μπορεί να είναι το ίδιο το μήνυμα, αλλά μπορεί να είναι και ο κωδικός του αποστολέα που μεταδίδεται στον διακομιστή. Επιπλέον, ο εισβολέας μπορεί απλά να συλλέγει στατιστικά για την επικοινωνία που πραγματοποιείται. Μια τέτοια επίθεση

μπορεί να έχει ως στόχο την ανάγνωση των πληροφοριών, αλλά μπορεί και απλά με την συχνότητα με την οποία ανταλλάσσονται μηνύματα να εξαχθούν συμπεράσματα για την σχέση μεταξύ του αποστολέα και του παραλήπτη.

Ενεργές επιθέσεις

Οι ενεργές επιθέσεις απειλούν την ακεραιότητα και διαθεσιμότητα των δεδομένων. Ο εισβολέας έχει την δυνατότητα να ελέγξει πλήρως τις πληροφορίες που μεταδίδονται. Μπορεί να τις τροποποιήσει, να τις επεκτείνει, να τις διαγράψει και να τις αναπαράγει κατά βούληση.

Ο συνδυασμός των δύο μορφών επιθέσεων χρησιμοποιείται για την εισβολή σε ιδιωτικά δίκτυα και την συλλογή κρίσιμων δεδομένων.

Κίνδυνοι που δημιουργούνται

Ο επίδοξος υποκλοπέας μπορεί να αξιοποιήσει την ολιγωρία μας για να δημιουργήσει προβλήματα με τους εξής τρόπους:

- Το τεράστιο πλήθος από email που κυκλοφορεί στον παγκόσμιο ιστό, αλλά και ο μεγάλος αριθμός χρηστών συνδεδεμένων σε αυτόν, καθιστούν πολύ εύκολη για κάποιον την πρόσβαση στους υπολογιστές και τα δίκτυα απ’ όπου περνά ένα email, ώστε να αποσπάσει αυτό το μήνυμα και να το διαβάσει, με τον ίδιο τρόπο που κάποιος στο διπλανό δωμάτιο μπορεί να κρυφακούει μια συζήτηση.
- Μια επιτυχημένη υποκλοπή πληροφοριών κατά τη διάρκεια πιστοποίησης του χρήστη στο διακομιστή, μπορεί να αποδώσει στον υποκλοπεά το ψευδώνυμο αλλά και τον κωδικό σύνδεσης που χρησιμοποιείται από τον χρήστη. Το αποτέλεσμα είναι ότι μπορεί πλέον κάποιος πέραν από το νόμιμο χρήστη, να στέλνει και να λαμβάνει email στο όνομά του.
- Κάθε διαχειριστής (νόμιμος ή μη) σε οποιοδήποτε διακομιστή email απ’ όπου περνά το μήνυμα έχει τη δυνατότητα, όχι μόνο να διαβάσει το μήνυμα, αλλά αν θέλει να το τροποποιήσει πριν αυτό συνεχίσει την πορεία του, χωρίς ο παραλήπτης να μπορεί να καταλάβει διαφορά. Μπορεί ακόμα και να το διαγράψει, οπότε και να μην φτάσει ποτέ αυτό στον προορισμό του.
- Είναι ιδιαιτέρως απλό να κατασκευάσει κάποιος ένα email με ψεύτικο αποστολέα, άρα και να χρησιμοποιηθεί ως όνομα αποστολέα το δικό μας. Στην πραγματικότητα πολλοί ιοί χρησιμοποιούν αυτό το τρόπο για να εξαπλωθούν. Είναι αδύνατο να γνωρίζεις αν ένα email έχει σταλεί από αυτόν που φαίνεται να το έχει στείλει.
- Η δημιουργία αντιγράφων ασφαλείας απο τους διαχειριστές των διακομιστών email μπορεί να οδηγήσει στην αποθήκευση μηνυμάτων για μεγάλα χρονικά διαστήματα. Παρόλο που μπορεί να θεωρούμε ότι έχουμε διαγράψει κάποιο μήνυμα, αυτό μπορεί να αναγνωστεί ή να αποσταλεί ξανά μετά από μήνες ή χρόνια.
- Τέλος, αφού ένα email είναι τόσο εύκολο να «κατασκευαστεί» ο παραλήπτης του είναι αδύνατο να αποδείξει ότι έχει λάβει ένα email από κάποιο χρήστη,

αφού ο τελευταίος μπορεί να το αρνηθεί. Αυτό έχει αρνητικό αντίκτυπο στην αξιοπιστία της χρήσης του email για δημιουργία συμβολαίων, εταιρικές συναλλαγές αλλά και στο ηλεκτρονικό εμπόριο.

1.3 ΑΣΦΑΛΗΣ ΕΠΙΚΟΙΝΩΝΙΑ

Αφού αντιληφθούμε τους κινδύνους που εγκυμονεί η χρήση του ηλεκτρονικού ταχυδρομείου, πρέπει να βρούμε τρόπους ώστε να επιτύχουμε ασφάλεια στην επικοινωνία μας. Με τον όρο ασφαλής επικοινωνία εννοούμε ότι θα πρέπει να εξασφαλίζονται τουλάχιστον:

- Πιστοποίηση της πηγής των δεδομένων, δηλαδή εξασφάλιση της ταυτότητας του αποστολέα.
- Πιστοποίηση της εμπιστευτικότητας των δεδομένων, δηλαδή κάθε μήνυμα γίνεται γνωστό μόνο στον αποστολέα και τους παραλήπτες του.
- Πιστοποίηση της ακεραιότητας των δεδομένων, δηλαδή κάθε μήνυμα παραλαμβάνεται ακριβώς ίδιο με αυτό που στάλθηκε.
- Μη αμφισβήτηση των δεδομένων, δηλαδή για κάθε μήνυμα που παραλαμβάνεται να αποδεικνύεται ο αποστολέας.

Οι τέσσερις αυτές συνθήκες μπορούν να εφαρμοστούν σε κάθε ένα μεμονωμένο μήνυμα ηλεκτρονικού ταχυδρομείου χωρίς να απαιτείται επέμβαση ή τροποποίηση του μέσου που χρησιμοποιείται για την μετάδοση των δεδομένων και μπορούν να υλοποιηθούν στις εφαρμογές ανάγνωσης και αποστολής email.

Επιπλέον ασφάλεια μπορεί να επιτευχθεί με διάφορους τρόπους, όπως για παράδειγμα με ένα σύστημα ενημέρωσης του αποστολέα για τον χρόνο και τόπο παράδοσης του μηνύματος.

Μέχρι τον χρόνο που γράφεται αυτή η εργασία, υπάρχουν δύο μέθοδοι υλοποίησης ασφαλούς επικοινωνίας στο ηλεκτρονικό ταχυδρομείο, η χρήση ψηφιακών υπογραφών και η χρήση κρυπτογράφησης δεδομένων σε συνδυασμό με ψηφιακούς φακέλους.

Υλοποίηση

Εφόσον το υπάρχον σύστημα ανταλλαγής μηνυμάτων ηλεκτρονικού ταχυδρομείου δεν παρέχει χαρακτηριστικά ασφαλείας, υπάρχουν δύο τρόποι να διορθωθούν τα πράγματα. Είτε θα πρέπει να επανασχεδιαστούν απ' την αρχή τα πρωτόκολλα που χρησιμοποιούνται στο ηλεκτρονικό ταχυδρομείο, είτε θα πρέπει να επεκταθούν τα ήδη υπάρχοντα με χαρακτηριστικά τέτοια που να παρέχουν ασφάλεια. Θεωρητικά, η επανασχεδίαση των πρωτοκόλλων είναι ο σωστότερος τρόπος για να υλοποιηθούν τόσο μεγάλες αλλαγές. Σε πρακτικό επίπεδο όμως αυτό θα απαιτούσε την επανασχεδίαση, υλοποίηση και αντικατάσταση όλου του υλισμικού και λογισμικού που χρησιμοποιείται για την χρήση του ηλεκτρονικού ταχυδρομείου σήμερα. Με την επέκταση των ήδη υπαρχόντων πρωτοκόλλων έχουμε μια οικονομικότερη λύση που μπορεί να υλοποιηθεί εξ ολοκλήρου στις εφαρμογές ηλεκτρονικού ταχυδρομείου.

Με γνώμονα αυτόν τον δεύτερο τρόπο έχουν αναπτυχθεί δύο κύρια σχήματα επέκτασης του ηλεκτρονικού ταχυδρομείου, το “Pretty Good Privacy” (PGP) και το Secure MIME (S/MIME). Και το PGP και το S/MIME προσπαθούν να προσφέρουν ασφαλές ηλεκτρονικό ταχυδρομείο χρησιμοποιώντας τις ίδιες βασικές τεχνικές όπως η κρυπτογραφία δημοσίου κλειδιού και οι ψηφιακοί φάκελοι, δεν μπορούν όμως να συνεργαστούν μεταξύ τους, αφ' ενός επειδή χρησιμοποιούν διαφορετικά συστήματα κωδικοποίησης μηνυμάτων και αφ' ετέρου επειδή χρησιμοποιούν τα δημόσια κλειδία και τα ψηφιακά πιστοποιητικά που προκύπτουν από αυτά με τελείως διαφορετικό τρόπο.

Αφού μελετήσουμε τα πρωτόκολλα κρυπτογραφίας που χρησιμοποιούνται θα εξετάσουμε κάθε ένα από τα δύο αυτά σχήματα και πως μπορούμε να τα χρησιμοποιήσουμε στην δική μας εφαρμογή ηλεκτρονικού ταχυδρομείου ώστε να αποκτήσουμε ασφαλέστερη επικοινωνία με τους φίλους και συνεργάτες μας.

2. ΤΟ ΠΡΩΤΟΚΟΛΛΟ SSL

΄Όπως προαναφέρθηκε, η ασφάλεια αποτελεί μια ιδιαίτερα σημαντική παράμετρο για τη χρήση του Διαδικτύου. Είτε μοιράζονται οικονομικές, επαγγελματικές, ή άλλες προσωπικές πληροφορίες, οι άνθρωποι θέλουν να γνωρίζουν με ποιον επικοινωνούν (πιστοποίηση) καθώς επίσης και να είναι βέβαιοι ότι αυτό το οποίο στέλνεται από τον αποστολέα είναι και αυτό το οποίο παραλαμβάνεται από τον παραλήπτη (ακεραιότητα). Επιθυμούν επίσης να αποτρέψουν τρίτα μη εξουσιοδοτημένα πρόσωπα από το να παρεισφρύσουν στην επικοινωνία μεταξύ τους (μυστικότητα - εμπιστευτικότητα). Το πρωτόκολλο SSL (Secure Sockets Layer) παρέχει τα μέσα για την επίτευξη των παραπάνω στόχων και αποτελεί το αντικείμενο ανάλυσης της παρούσας ενότητας.

Για την εξοικείωση με το πρωτόκολλο SSL απαιτείται η κατανόηση των αλγόριθμων κρυπτογράφησης, των συναρτήσεων σύνοψης μηνυμάτων, και της έννοιας των ψηφιακών υπογραφών. Οι τεχνικές αυτές παρέχουν τη βάση ώστε να επιτευχθεί μυστικότητα, εμπιστευτικότητα, ακεραιότητα και πιστοποίηση.

2.1 ΤΕΧΝΙΚΕΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

Ας υποθέσουμε ότι ο χρήστης Χ επιθυμεί να στείλει ένα μήνυμα στην τράπεζά του για την μεταφορά κάποιου χρηματικού ποσού. Ο χρήστης Χ θα ήθελε το μήνυμα του να είναι εμπιστευτικό, εφόσον περιλαμβάνει ευαίσθητες πληροφορίες όπως είναι ο αριθμός του τραπεζικού του λογαριασμού και το προς μεταφορά χρηματικό ποσό. Μία λύση θα ήταν, να χρησιμοποιήσει έναν αλγόριθμο κρυπτογράφησης, μία τεχνική η οποία θα μετέτρεπε το μήνυμά του σε κρυπτογραφημένη μορφή, και το οποίο δεν θα μπορούσε να διαβαστεί από κανέναν άλλο εκτός από εκείνους προς τους οποίους απευθυνόταν. Όντας σε αυτή την μορφή, το μήνυμα θα μπορούσε να μεταφραστεί μόνο με τη χρήση ενός μυστικού κλειδιού. Χωρίς την ύπαρξη του κλειδιού αυτού το μήνυμα θα ήταν άχρηστο. Ισχυροί αλγόριθμοι κρυπτογράφησης, καθιστούν ιδιαίτερα

χρονοβόρα και δύσκολη την αποκωδικοποίηση του αρχικού κειμένου από μη εξουσιοδοτημένα πρόσωπα.

Υπάρχουν δύο κατηγορίες αλγόρθιμων κρυπτογράφησης : Η συμβατική (conventional – symmetric) και εκείνη του δημόσιου κλειδιού (public key).

- *Συμβατική κρυπτογράφηση*, γνωστή επίσης και με το όνομα συμμετρική, απαιτεί τόσο από τον αποστολέα όσο και από τον παραλήπτη να μοιράζονται ένα κλειδί (ένα μυστικό κομματι πληροφορίας το οποίο μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση – αποκρυπτογράφηση του μηνύματος). Εάν το κλειδί είναι μυστικό, τότε κανείς άλλος εκτός του αποστολέα και του παραλήπτη δεν μπορεί να διαβάσει το μήνυμα. Στο παράδειγμά μας λοιπόν, εφόσον ο χρήστης Χ και η τράπεζα γνωρίζουν το μυστικό κλειδί μπορούν να ανταλλάσσουν μεταξύ τους εμπιστευτικά μηνύματα. Η διαδικασία όμως επιλογής, κάθε φορά, ενός κλειδιού, πριν την επικοινωνία μεταξύ τους, μπορεί να καταστεί προβληματική.
- *Κρυπτογράφηση δημόσιου κλειδιού*, γνωστή επίσης και με το όνομα μη συμμετρική ή ασύμμετρη, λύνει το πρόβλημα της ανταλλαγής κλειδιών με τον καθορισμό ενός αλγόριθμου ό οποίος χρησιμοποιεί δύο κλειδιά για την κρυπτογράφηση του μηνύματος. Εάν ένα κλειδί χρησιμοποιείται για την κρυπτογράφηση του μηνύματος τότε το άλλο θα χρησιμοποιηθεί για την αποκρυπτογράφησή του. Το γεγονός αυτό καθιστά εφικτή την αποστολή ασφαλών μηνυμάτων με την δημοσιοποίηση του ενός κλειδιού (το δημόσιο κλειδί) και την μυστική διατήρηση του άλλου κλειδιού (το ιδιωτικό κλειδί). Ο οποιοσδήποτε μπορεί να κρυπτογραφήσει ένα μήνυμα χρησιμοποιώντας το δημόσιο κλειδί ενώ μόνο ο ιδιοκτήτης του ιδιωτικού κλειδιού μπορεί να διαβάσει το μήνυμα αυτό. Με τον τρόπο αυτό ο χρήστης Χ, στο παράδειγμά μας, μπορεί να στέλνει εμπιστευτικά μηνύματα – κρυπτογραφημένα με το δημόσιο κλειδί - στον ιδιοκτήτη του ζεύγους κλειδιών (στην προκειμένη περίπτωση την τράπεζα). Μόνο η τράπεζα έχει την δυνατότητα να αποκρυπτογραφήσει το μήνυμα.

2.2 ΣΥΝΟΨΕΙΣ ΜΗΝΥΜΑΤΩΝ

Παρά το γεγονός ότι, ο χρήστης Χ μπορεί να κρυπτογραφήσει το μήνυμά του ώστε να το κάνει μυστικό, υπάρχει πάντοτε το ενδεχόμενο κάποιος τρίτος να τροποποιήσει το αρχικό μήνυμα ή ακόμη και να το αντικαταστήσει με κάποιο εντελώς διαφορετικό, με σκοπό να μεταφέρει το χρηματικό ποσό στο όνομα του, για παράδειγμα. ΄Ενας τρόπος για να εγγυηθεί η ακεραιότητα του μηνύματος του χρήστη Χ είναι, να δημιουργηθεί μια συνοπτική και συμπαγής περιγραφή του μηνύματος από τον χρήστη Χ, η οποία θα αποσταλεί μαζί με το μήνυμα στην τράπεζα. Με την παραλαβή του μηνύματος, η τράπεζα δημιουργεί μία δική της περιγραφή, του παραληφθέντος από τον χρήστη Χ μηνύματος, και την συγκρίνει με εκείνη την οποία έχει επισυνάψει ο χρήστης Χ στο μήνυμά του. Μόνο σε περίπτωση ταύτισης των δύο συνοπτικών περιγραφών το μήνυμα γίνεται αποδεκτό.

Μία τέτοια περίληψη καλείται σύνοψη μηνύματος (*message digest)*, ή αλλιώς μονοσήμαντος κερματισμός (*one-way hash)*. Οι συνόψεις μηνυμάτων χρησιμοποιούνται για τη δημιουργία σύντομων, καθορισμένου μεγέθους αναπαραστάσεων, μεγαλύτερων - μεταβλητού μεγέθους - μηνυμάτων. Οι αλγόριθμοι για τη δημιουργία συνόψεων έχουν σχεδιαστεί κατά τέτοιο τρόπο ώστε να παράγουν μοναδικές περιλήψεις για διαφορετικά μηνύματα. Ο σχεδιασμός αυτός καθιστά πρακτικά αδύνατο τον καθορισμό του μηνύματος από την περίληψή του καθώς επίσης και την εύρεση δύο διαφορετικών μηνυμάτων τα οποία έχουν δημιουργήσει την ίδια ακριβώς περίληψη. Εξαλείφεται έτσι η πιθανότητα αντικατάστασης ενός μηνύματος με κάποιο άλλο το οποίο θα έχει την ίδια σύνοψη με αυτήν του αρχικού μηνύματος.

Μια άλλη πρόκληση, την οποία αντιμετωπίζει ο χρήστης Χ, είναι η εύρεση ενός τρόπου, ο οποίος θα καταστήσει εφικτή την αποστολή της σύνοψης του μηνύματος στην τράπεζα, με έναν ασφαλή τρόπο. ΄Οταν ο στόχος αυτός επιτευχθεί η ακεραιότητα του μηνύματος θεωρείται εξασφαλισμένη. Μια λύση στο παραπάνω πρόβλημα είναι να συμπεριληφθεί η σύνοψη του μηνύματος στη ψηφιακή υπογραφή.

2.3 ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

Όταν ο χρήστης Χ στέλνει ένα μήνυμα στην τράπεζα, η τράπεζα πρέπει να επιβεβαιώσει ότι το μήνυμα προέρχεται από εκείνον, ώστε να αποκλεισθεί το ενδεχόμενο κάποιος εισβολέας να αιτείται συναλλαγή η οποία αφορά στον προσωπικό λογαριασμό του χρήστη Χ. Μία ψηφιακή υπογραφή (*digital signature)* η οποία δημιουργείται από τον χρήστη Χ και συμπεριλαμβάνεται στο μήνυμά του, το οποίο αποστέλλει στην τράπεζα, επιτελεί αυτόν ακριβώς το σκοπό.

Οι ψηφιακές υπογραφές δημιουργούνται με την κρυπτογράφηση της σύνοψης ενός μηνύματος καθώς και άλλων πληροφοριών (όπως για παράδειγμα μία αλληλουχία αριθμών) μέσω του ιδιωτικού κλειδιού του αποστολέα.. Παρά το γεγονός ότι, ο οποιοσδήποτε θα μπορούσε να αποκρυπτογραφήσει την υπογραφή με το δημόσιο κλειδί, μόνο ο υπογράφων γνωρίζει το ιδιωτικό κλειδί. Ενσωματώνοντας λοιπόν τη σύνοψη του μηνύματος στην υπογραφή, σημαίνει ότι η υπογραφή είναι αξιοποιήσιμη μόνο για το συγκεκριμένο μήνυμα καθώς επίσης και ότι εξασφαλίζεται η ακεραιότητα του μηνύματος αφού κανείς δεν μπορεί να αλλάξει τη σύνοψη του μηνύματος και παράλληλα να το υπογράψει. Για να προφυλαχθεί ο χρήστης από τυχόν παρεμβολή και επαναχρησιμοποίηση της υπογραφής από ενδεχόμενο εισβολέα, σε μεταγενέστερο χρόνο, η υπογραφή περιέχει μία μοναδική αλληλουχία αριθμών. Η διαδικασία αυτή προστατεύει την τράπεζα από μια «απατηλή» απαίτηση του χρήστη Χ ότι δεν έστειλε το μήνυμα εφόσον μόνο εκείνος θα μπορούσε να το έχει υπογράψει. Η διαδικασία αυτή είναι γνωστή με τον όρο «μη άρνηση αποδοχής» (non-repudiation).

2.4 ΠΙΣΤΟΠΟΙΗΤΙΚΑ

Παρά το γεγονός ότι, χρήστης Χ θα μπορούσε να έχει στείλει ένα μυστικό μήνυμα στην τράπεζα, να το έχει υπογράψει και να έχει εξασφαλίσει την ακεραιότητά του, χρειάζεται ακόμα να βεβαιωθεί ότι η τράπεζα είναι ο ιδιοκτήτης του δημόσιου κλειδιού. Με παρόμοιο τρόπο, η τράπεζα χρειάζεται να πιστοποιήσει ότι η υπογραφή του μηνύματος αντιστοιχεί στην υπογραφή του χρήστη Χ. Εάν κάθε συμβαλλόμενο μέρος είχε στην κατοχή του ένα πιστοποιητικό το οποίο πιστοποιεί την ταυτότητα του έτερου συμβαλλόμενου, επιβεβαιώνει το δημόσιο κλειδί και είναι υπογεγραμμένο από μία ανεξάρτητη αρχή με την οποία κάθε συμβαλλόμενος έχει σχέσεις εμπιστοσύνης, τότε και τα δύο συμβαλλόμενα μέρη θα εξασφάλιζαν το γεγονός ότι πραγματικά επικοινωνούν με εκείνον με τον οποίο θεωρούν ότι επικοινωνούν. Μια τετοια εκδότρια αρχή πιστοποιητικών ονομάζεται Αρχή Πιστοποίησης (*Certificate Authority)*, και τα πιστοποιητικά τα οποία αυτή εκδίδει χρησιμοποιούνται με τον προαναφερθέντα τρόπο.

Πίνακας 2.1: Πληροφορίες Πιστοποιητικού

Υποκείμενο	Διακεκριμένο Όνομα, Δημόσιο Κλειδί
Εκδότρια Αρχή	Διακεκριμένο Όνομα, Υπογραφή
Περίοδος Εγκυρότητας	Όχι πριν την Ημέρα, Όχι μετά την Ημέρα
Διαχειριστικές Πληροφορίες	Έκδοση, Σειριακός Αριθμός
Εκτεταμένες Πληροφορίες	

2.5 ΠΕΡΙΕΧΟΜΕΝΑ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

΄Ενα πιστοποιητικό συσχετίζει ένα δημόσιο κλειδί με την πραγματική ταυτότητα ενός ατόμου, εξυπηρετητή, ή οποιασδήποτε άλλης οντότητας γνωστά με το χαρακτηρισμό υποκείμενο (subject). Όπως φαίνεται στον Πίνακα 2.1, η πληροφορία για το υποκείμενο περιλαμβάνει τα στοιχεία ταυτοποίησης (διακεκριμένο όνομα) και το δημόσιο κλειδί. Περιλαμβάνει ακόμη τον καθορισμό και την υπογραφή της Αρχής Πιστοποίησης που εξέδωσε το πιστοποιητικό καθώς και την χρονική περίοδο για την οποία το πιστοποιητικό αυτό είναι έγκυρο. Μπορεί τέλος να περιέχει

συμπληρωματικές πληροφορίες (ή επεκτάσεις) καθώς επίσης και διαχειριστικές πληροφορίες για χρήση από την Αρχή Πιστοποίησης όπως για παράδειγμα ο σειριακός αριθμός του πιστοποιητικού.

΄Ενα διακεκριμένο όνομα χρησιμοποιείται για να παρέχει μια ταυτότητα σε ένα καθορισμένο πλαίσιο (context) – για παράδειγμα ένα άτομο μπορεί να έχει ένα προσωπικό πιστοποιητικό και ένα πιστοποιητικό το οποίο τον ταυτοποιεί ως υπάλληλο. Η δομή των διακεκριμένων ονομάτων καθορίζεται από το πρότυπο X.509, το οποίο ορίζει τα πεδία και τα ονόματά τους καθώς επίσης και τις συντμήσεις οι οποίες αναφέρονται στα πεδία αυτά (βλέπε Πίνακα 2.2).

Η Αρχή Πιστοποίησης μπορεί να καθορίσει την πολιτική η οποία προσδιορίζει τη χρήση των διακεκριμένων ονομάτων και πιο συγκεκριμένα ποια πεδία είναι προαιρετικά και ποια πρέπει απαραίτητα να συμπληρώνονται. Μπορεί επίσης να ορίσει συγκεκριμένες απαιτήσεις για το περιεχόμενο των πεδίων και για τους χρήστες των πιστοποιητικών. Για παράδειγμα το πρόγραμμα ιχνηλάτησης παγκόσμιου ιστού Netscape απαιτεί το κοινό όνομα (Common Name) για ένα πιστοποιητικό το οποίο αντιπροσωπεύει έναν εξυπηρετητή να αντιστοιχεί σε μια έκφραση για το όνομα περιοχής (domain name) του συγκεκριμένου εξυπηρετητή, όπως για παράδειγμα *www.teithe.gr*.

Η δυαδική μορφή (*binary format)* ενός πιστοποιητικού καθορίζεται με τη χρήση μιας σημειογραφίας ASN.1. Η σημειογραφία αυτή ορίζει τον τρόπο με τον οποίο στοιχειοθετούνται τα περιεχόμενα, ενώ οι κανόνες κωδικοποίησης ορίζουν το τρόπο με τον οποίο οι πληροφορίες αυτές μετατρέπονται σε δυαδική μορφή. Η δυαδική κωδικοποίηση (*binary encoding)* του πιστοποιητικού πραγματοποιείται με τη χρήση κανόνων διακεκριμένης κωδικοποίησης (Distinguished Encoding Rules (DER)), ενώ οι τελευταίοι βασίζονται με τη σειρά τους σε πιο γενικούς (βασικούς) κανόνες κωδικοποίησης (Basic Encoding Rules (BER)). Σε εκείνη την περίπτωση κατά την οποία η επικοινωνία δεν μπορεί να χειριστεί δυαδικές πληροφορίες, οι τελευταίες μετατρέπονται σε ASCII μορφή με χρήση κωδικοποίησης Base64. Αυτή η κωδικοποιημένη έκδοση καλείται PEM. Υπόδειγμα ενός τέτοιου πιστοποιητικού ακολουθεί παρακάτω:

```
-----BEGIN CERTIFICATE-----
MIIC7jCCAlegAwIBAgIBATANBgkqhkiG9w0BAQQFADCBqTELMAkGA1UEBhMCWFkx
FTATBgNVBAgTDFNuYWtlIERlc2VydDETMBEGA1UEBxMKU25ha2UgVG93bjEXMBUG
A1UEChMOU25ha2UgT2lsLCBMdGQxHjAcBgNVBAsTFUNlcnRpZmljYXRlIEF1dGhv
cml0eTEVMBMGA1UEAxMMU25ha2UgT2lsIENBMR4wHAYJKoZIhvcNAQkBFg9jYUBz
bmFrZW9pbC5kb20wHhcNOTgxMDIxMDg1ODM2WhcNOTkxMDIxMDg1ODM2WjCBpzEL
MAkGA1UEBhMCWFkxFTATBgNVBAgTDFNuYWtlIERlc2VydDETMBEGA1UEBxMKU25h
a2UgVG93bjEXMBUGA1UEChMOU25ha2UgT2lsLCBMdGQxFzAVBgNVBAsTDldlYnNl
cnZlciBUZWFtMRkwFwYDVQQDExB3d3cuc25ha2VvaWwuZG9tMR8wHQYJKoZIhvcN
AQkBFhB3d3dAc25ha2VvaWwuZG9tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDH9Ge/s2zcH+da+rPTx/DPRp3xGjHZ4GG6pCmvADIEtBtKBFAcZ64n+Dy7Np8b
vKR+yy5DGQiijsH1D/j8HlGE+q4TZ8OFk7BNBFazHxFbYI4OKMiCxdKzdif1yfaa
lWoANFlAzlSdbxeGVHoT0K+gT5w3UxwZKv2DLbCTzLZyPwIDAQABoyYwJDAPBgNV
HRMECDAGAQH/AgEAMBEGCWCGSAGG+EIBAQQEAwIAQDANBgkqhkiG9w0BAQQFAAOB
gQAZUIHAL4D09oE6Lv2k56Gp38OBDuILvwLg1v1KL8mQR+KFjghCrtpqaztZqcDt
2q2QoyulCgSzHbEGmi0EsdkPfg6mp0penssIFePYNI+/8u9HT4LuKMJX15hxBam7
dUHzICxBVC1lnHyYGjDuAMhe396lYAn8bCld1/L4NMGBCQ==
-----END CERTIFICATE-----
```

Σχήμα 2.1: Περιεχόμενο Πιστοποιητικού PEM

Πίνακας 2.2: Πληροφορίες Διακεκριμένου Ονόματος

Πεδίο	**Σύντμηση**	**Περιγραφή**	**Παράδειγμα**
Κοινό Ονομα	CN	Ονομα το οποίο πιστοποιείται	CN=Thanos Makrandreou
Οργανισμός ή Εταιρεία	O	Ονομα το οποίο σχετίζεται με τον Οργανισμό	O=AGRICULTURAL UNIVERSITY OF ATHENS
Οργανική Μονάδα	OU	Ονομα το οποίο σχετίζεται με τον Οργανική Μονάδα, όπως είναι το Τμήμα	OU=Informatics Laboratory
Πόλη/Εντοπιότητα	L	Πόλη στην οποία βρίσκεται το ΄Ονομα	L=Athens
Νομός/Περιοχή	SP	Νομός/Περιοχή στην οποία βρίσκεται το ΄Ονομα	SP=ATTICA
Χώρα	C	Χώρα στην οποία βρίσκεται το ΄Ονομα (σύμφωνα με τον κώδικα ISO για τη Χώρα)	C=GR

2.6 ΑΡΧΕΣ ΠΙΣΤΟΠΟΙΗΣΗΣ

Αφού πρώτα επαληθεύσει τις πληροφορίες σε μια αίτηση για έκδοση πιστοποιητικού (certificate request), η Αρχή Πιστοποίησης επιβεβαιώνει την ταυτότητα του ιδιοκτήτη του ιδιωτικού κλειδιού ενός ζεύγους κλειδιών. Για παράδειγμα, εάν ο χρήστης Χ αιτηθεί την έκδοση ενός προσωπικού πιστοποιητικού, η Αρχή Πιστοποίησης βεβαιώνεται ότι ο συγκεκριμένος χρήστης είναι πραγματικά εκείνος στον οποίο αναφέρεται η αίτηση έκδοσης πιστοποιητικού.

Αλυσίδες Πιστοποιητικών

Μια Αρχή Πιστοποίησης μπορεί επίσης να εκδώσει ένα πιστοποιητικό για μια άλλη Αρχή Πιστοποίησης. Όταν εξετάζει ο χρήστης Χ ένα πιστοποιητικό, μπορεί να χρειαστεί να εξετάσει τον εκδότη του πιστοποιητικού για κάθε γονική Αρχή Πιστοποίησης, έως ότου φθάσει σε κάποια με την οποία διατηρεί δεσμούς απόλυτης εμπιστοσύνης. Μπορεί τέλος να αποφασίσει να εμπιστεύεται πιστοποιητικά τα οποία προέρχονται από μια αυστηρά καθορισμένη αλυσίδα εκδιδουσών Αρχών, ώστε να ελαχιστοποιήσει το κίνδυνο ύπαρξης ενός «κακού» πιστοποιητικού μεταξύ της αλυσίδας.

Δημιουργία μιας Υψηλότερου Επιπέδου Γονικής Αρχής Πιστοποίησης

Όπως αναφέρθηκε νωρίτερα, κάθε πιστοποιητικό απαιτεί την ύπαρξη μιας εκδίδουσας αρχής η οποία θα εγγυηθεί την εγκυρότητα της ταυτότητας του υποκειμένου του πιστοποιητικού μέχρι την ανώτατη (top-level) Αρχή Πιστοποίησης. Το γεγονός αυτό παρουσιάζει ένα πρόβλημα το οποίο συνοψίζεται στο ερώτημα: Ποιος πιστοποιεί την ανώτατη Αρχή Πιστοποίησης; Σ’ αυτή τη μοναδική περίπτωση το πιστοποιητικό είναι αυθυπόγραφο «self-signed», και κατά συνέπεια ο εκδότης του πιστοποιητικού ταυτίζεται με το υποκείμενο του. Σαν αποτέλεσμα, καθένας ο οποίος αντιμετωπίζει παρόμοια κατάσταση πρέπει να τη χειριστεί με ιδιαίτερη προσοχή ώστε να μπορέσει να εμπιστευτεί ένα αυθυπόγραφο πιστοποιητικό. Η ευρεία δημοσιοποίηση του δημόσιου κλειδιού από την ανώτατη Αρχή μειώνει τον κίνδυνο στην αποδοχή του συγκεκριμένου κλειδιού. Τα περισσότερα προγράμματα ιχνηλάτησης παγκόσμιου ιστού έχουν ρυθμιστεί ώστε να εμπιστεύονται εγνωσμένου κύρους Αρχές Πιστοποίησης.

Ένας αριθμός εταιρειών όπως είναι η VeriSign έχουν χαρακτηρισθεί ως Αρχές Πιστοποίησης. Οι εταιρείες αυτές παρέχουν τις παρακάτω υπηρεσίες:

- Επαλήθευση αιτήσεων έκδοσης πιστοποιητικών
- Επεξεργασία αιτήσεων έκδοσης πιστοποιητικών
- Έκδοση και διαχείριση πιστοποιητικών

Είναι επίσης δυνατό να δημιουργήσει ένας Οργανισμός, ή μια οντότητα γενικότερα, τη δική του Αρχή Πιστοποίησης. Παρά το γεγονός ότι αυτό μπορεί να αποδειχθεί επικίνδυνο στο περιβάλλον του Διαδικτύου, μπορεί επίσης να αποδειχθεί εξαιρετικά χρήσιμο στο περιβάλλον ενός Intranet στο οποίο ο Οργανισμός μπορεί με ευκολία να

επαληθεύει την ταυτότητα φυσικών προσώπων, εξυπηρετητών και κάθε άλλου είδους οντοτήτων τα οποία βρίσκονται υπό την εποπτεία του.

Διαχείριση Πιστοποιητικών

Η εγκατάσταση μιας Αρχής Πιστοποίησης είναι μια υπευθυνότητα η οποία απαιτεί ένα στιβαρό διαχειριστικό και τεχνικό πλαίσιο. Οι Αρχές Πιστοποίησης δεν εκδίδουν μόνο πιστοποιητικά αλλά τα διαχειρίζονται κιόλας, πράγμα πού με απλά λόγια σημαίνει ότι η Αρχή καθορίζει το χρονικό διάστημα εγκυρότητας κάθε πιστοποιητικού, την ανανέωσή του, τη διατήρηση και την ενημέρωση αρχείων των πιστοποιητικών που έχουν ήδη εκδοθεί καθώς και εκείνων που δεν είναι πλέον έγκυρα, συντηρώντας λίστες ανακληθέντων πιστοποιητικών (certificate revocation lists - CRLs). Για παράδειγμα έστω ότι ο χρήστης Χ δικαιούται ενός πιστοποιητικού ως υπάλληλος στην εταιρεία στην οποία εργάζεται. Έστω τώρα ότι ο ίδιος υπάλληλος σε κάποια χρονική στιγμή εγκαταλείπει την εργασία του. Κατά συνέπεια το πιστοποιητικό του πρέπει να ανακληθεί. Για να ελεγχθεί, λοιπόν, οι εγκυρότητα των υφιστάμενων πιστοποιητικών πρέπει να ελεγχθούν οι λίστες ανακληθέντων πιστοποιητικών, διαδικασία η οποία σε καμιά περίπτωση δεν μπορεί να χαρακτηριστεί αυτοματοποιημένη.

2.7 ΤΟ ΠΡΩΤΟΚΟΛΛΟ SSL

Το πρωτόκολλο SSL (Secure Sockets Layer) ορίζεται ως ένα επίπεδο πρωτοκόλλου (protocol layer) το οποίο μπορεί να τοποθετηθεί σε μια αξιόπιστη δικτυακή σύνδεση μεταξύ ενός πρωτοκόλλου TCP/IP σε επίπεδο δικτύου (network layer) και ενός πρωτοκόλλου π.χ HTTP σε επίπεδο εφαρμογής (application layer) και να παρέχει ασφαλή επικοινωνία μεταξύ πελάτη και εξυπηρετητή προσφέροντας αφ’ ενός αμοιβαία πιστοποίηση και χρήση ψηφιακών υπογραφών για να εξασφαλισθεί η ακεραιότητα και αφ’ ετέρου κρυπτογράφηση για να εξασφαλισθεί η μυστικότητα και η εμπιστευτικότητα.

Το πρωτόκολλο αυτό έχει σχεδιαστεί κατά τέτοιο τρόπο ώστε να υποστηρίζει μια μεγάλη γκάμα αλγόριθμων οι οποίοι χρησιμοποιούνται για κρυπτογράφηση, συνόψεις, και ψηφιακές υπογραφές. Το γεγονός αυτό επιτρέπει την επιλογή συγκεκριμένων αλγόριθμων για συγκεκριμένους εξυπηρετητές ανάλογα με θέματα νομιμότητας, εξαγωγής τεχνολογιών κρυπτογράφησης κλπ. Επιτρέπει επίσης την αξιοποίηση νέων αλγόριθμων που έχουν αναπτυχθεί πρόσφατα. Οι επιλογή των αλγόριθμων είναι αποτέλεσμα διαπραγμάτευσης (negotiation) μεταξύ πελάτη και εξυπηρετητή κατά της διάρκεια μιας συνεδρίας του πρωτοκόλλου.

Υπάρχουν τρεις εκδόσεις του πρωτοκόλλου SSL, όπως φαίνεται στον Πίνακα 2.3.

Πίνακας 2.3: Εκδόσεις Του Πρωτοκόλλου SSL

Έκδοση	**Πηγή**	**Περιγραφή**	**Υποστήριξη Φυλλομετρητή**
SSL 2.0	Δημοσιεύθηκε από την εταιρεία Netscape	Αρχική έκδοση του πρωτοκόλλου	NS Navigator 1.x/2.x - MS IE 3.x - Lynx/2.8+OpenSSL
SSL 3.0	Internet Draft του οποίου η εγκυρότητα έχει λήξει	Αναθεωρήσεις ώστε να αντιμετωπιστούν συγκεκριμένοι τύποι επιθέσεων, προσθήκη νέων αλγόριθμων,και υποστήριξη αλυσίδων πιστοποιητικών	- NS Navigator 2.x/3.x/4.x - MS IE 3.x/4.x - Lynx/2.8+OpenSSL
TLS 1.0	IETF Draft	Αναθεώρηση του πρωτοκόλλου SSL 3.0 και επέκταση των δυνατοτήτων του	

Όπως φαίνεται στον Πίνακα 2.3, ένα από τα πλεονεκτήματα της SSL 3.0 αποτελεί το γεγονός ότι προσθέτει υποστήριξη για φόρτωση αλυσίδων πιστοποιητικών. Το χαρακτηριστικό αυτό επιτρέπει στον εξυπηρετητή να «περνάει» το πιστοποιητικό του μαζί με τα πιστοποιητικά της εκδίδουσας Αρχής στον πελάτη (browser). Η «φόρτωση» αλυσίδων πιστοποιητικών επιτρέπει στον πελάτη να επαληθεύσει το πιστοποιητικό του εξυπηρετητή, έστω κι' αν η Αρχή Πιστοποίησης δεν είναι εγκατεστημένη για τις ενδιάμεσες εκδίδουσες Αρχές πιστοποιητικών, εφόσον αυτές συμπεριλαμβάνονται στην αλυσίδα.. Το πρωτόκολλο SSL 3.0 αποτελεί τη βάση για την ανάπτυξη του πρωτοκόλλου TLS (Transaction Layer Security) το οποίο αναπτύσσεται από την IETF (Internet Engineering Task Force).

Εδραίωση Συνεδρίας

Η εδραίωση μία συνεδρίας SSL πραγματοποιείται μέσω μιας ακολουθίας χειραψίας (*handshake sequence)* μεταξύ πελάτη και εξυπηρετητή όπως αυτή περιγράφεται στο Σχήμα 1. Η ακολουθία αυτή ποικίλλει ανάλογα με το εάν ο εξυπηρετητής είναι ρυθμισμένος να παρέχει ένα πιστοποιητικό ή να ζητάει τη λήψη ενός πιστοποιητικού από τον πελάτη. Παρά το γεγονός ότι παρατηρούνται περιπτώσεις στις οποίες επιπρόσθετα βήματα χειραψίας απαιτούνται για τη διαχείριση της πληροφορίας κρυπτογράφησης, τα προαναφερθέντα συνθέτουν ένα ρεαλιστικό σενάριο.

Όταν εδραιωθεί μία συνεδρία SSL, μπορεί να χρησιμοποιηθεί ξανά, από επακόλουθες διεργασίες, αυξάνοντας την απόδοση και αποφεύγοντας με τον τρόπο αυτό την επανάληψη των ίδιων βημάτων που απαιτούνται για να ξεκινήσει μια νέα συνεδρία.

Τα στοιχεία της ακολουθίας χειραψίας, όπως αυτά χρησιμοποιούνται από πελάτη και εξυπηρετητή αναφέρονται παρακάτω:

1. Διαπραγμάτευση της κρυπτογραφικής μεθόδου (Cipher Suite) η οποία θα χρησιμοποιηθεί κατά τη διάρκεια της μεταφοράς δεδομένων
2. Εδραίωση και μοίρασμα ενός κλειδιού συνεδρίας μεταξύ πελάτη και εξυπηρετητή
3. Προαιρετική πιστοποίηση του εξυπηρετητή από τον πελάτη
4. Προαιρετική πιστοποίηση του πελάτη από τον εξυπηρετητή

Κατά το πρώτο βήμα, η διαπραγμάτευση της κρυπτογραφικής μεθόδου, επιτρέπει στον πελάτη και τον εξυπηρετητή να επιλέξουν μία μέθοδο η οποία υποστηρίζεται και από τους δύο. Η προδιαγραφή του πρωτοκόλλου SSL 3.0 ορίζει 31 κρυπτογραφικές μεθόδους. Κάθε κρυπτογραφική μέθοδος προσδιορίζεται από τα παρακάτω συστατικά:

- Μέθοδος ανταλλαγής κλειδιού (Key exchange method)
- Κρυπτογραφική μέθοδος για μεταφορά δεδομένων
- Σύνοψη μηνύματος για την δημιουργία Κωδικού Πιστοποίησης Μηνύματος (Message Authentication Code - MAC)

Τα τρία αυτά στοιχεία αναλύονται στις παραγράφους που ακολουθούν:

Μέθοδος ανταλλαγής κλειδιού

Η μέθοδος ανταλλαγής κλειδιού (*key exchange method)* καθορίζει τον τρόπο με τον οποίο, ο πελάτης και ο εξυπηρετητής θα διαπραγματευτούν την διαμοίραση του μυστικού συμμετρικού κλειδιού κρυπτογράφησης για τη μεταφορά των δεδομένων εφαρμογής μεταξύ τους. Το πρωτόκολλο SSL 2.0 υποστηρίζει ανταλλαγή κλειδιών RSA, ενώ το πρωτόκολλο SSL 3.0 επιτρέπει την επιλογή του αλγόριθμου για την ανταλλαγή κλειδιών συμπεριλαμβανομένης και ανταλλαγής κλειδιών RSA όταν χρησιμοποιούνται πιστοποιητικά, καθώς επίσης και ανταλλαγή κλειδιών Diffie-Hellman όταν δεν χρησιμοποιούνται πιστοποιητικά χωρίς πρότερη επικοινωνία μεταξύ πελάτη εξυπηρετητή.

Μία σημαντική παράμετρος στην επιλογή της μεθόδου ανταλλαγής κλειδιών είναι οι ψηφιακές υπογραφές. (αν πρέπει ή όχι να χρησιμοποιηθούν, τι τύπου θα είναι κλπ.). Υπογράφοντας με ένα μυστικό κλειδί παρέχεται ασφάλεια από επιθέσεις του τύπου «man-in-the-middle-attack» κατά τη διάρκεια ανταλλαγής πληροφοριών οι οποίες χρησιμοποιούνται στη δημιουργία του κοινού κλειδιού.

Κρυπτογραφική μέθοδος για μεταφορά δεδομένων

Το πρωτόκολλο SSL χρησιμοποιεί αλγόριθμους συμβατικής κρυπτογράφησης (symmetric cryptography) για να κρυπτογραφήσει μηνύματα σε μια συνεδρία. Υπάρχουν εννέα επιλογές αλγορίθμων περιλαμβανομένης και της δυνατότητας μη χρήσης κρυπτογράφησης:

- Μη Κρυπτογράφηση

- Stream Ciphers
- RC4 με μέγεθος κλειδιών 40-bit
- RC4 με μέγεθος κλειδιών 128-bit
- CBC Block Ciphers
- RC2 με μέγεθος κλειδιών 40 bit
- DES40, DES, 3DES_EDE
- IDEA
- Fortezza

Ο όρος «CBC» ή αλλιώς «Cipher Block Chaining», δηλώνει ότι ένα μέρος του προηγούμενου κρυπτογραφημένου τμήματος χρησιμοποιείται για την κρυπτογράφηση του τρέχοντος τμήματος. Ο Ορος «DES» ή αλλιώς «Data Encryption Standard» περιλαμβάνει μια ποικιλία παραλλαγών (DES40 και 3DES_EDE). Ο αλγόριθμος «Idea» αποτελεί έναν από τους ισχυρότερους διαθέσιμους αλγόριθμους κρυπτογράφησης, ενώ ο αλγόριθμος «RC2» είναι ο αλγόριθμος ο οποίος αναπτύχθηκε από την RSA.

Συνάρτηση Σύνοψης

Η επιλογή της συνάρτησης σύνοψης (digest function) καθορίζει τον τρόπο με τον οποίο δημιουργείται μια περίληψη από μία μονάδα εγγραφής (record unit). Το πρωτόκολλο SSL υποστηρίζει τις παρακάτω συναρτήσεις σύνοψης:

- Μη δημιουργία σύνοψης (επιλογή Null)
- MD5, κερματισμός (hash) 128-bit
- Secure Hash Algorithm (SHA), κερματισμός (hash) 160-bit ο οποίος εχει σχεδιαστεί για χρήση με το πρότυπο DSS (Digital Signature Standard)

Η δημιουργία σύνοψης μηνύματος παράγει έναν Κωδικό Επαλήθευσης Μηνύματος (Message Authentication Code - MAC), ο οποίος κρυπρογραφείται μαζί με το μήνυμα ώστε να επιτευχθεί η ακεραιότητα του και να αποφευχθούν μη εξουσιοδοτημένες ενέργειες αλλοίωσης η επανάληψής του.

Πρωτόκολλο Ακολουθίας Χειραψίας

Η ακολουθία χειραψίας χρησιμοποιεί τρία επιμέρους πρωτόκολλα:

- Το «SSL Handshake Protocol», για την εδραίωση μίας συνεδρίας SSL μεταξύ πελάτη και εξυπηρετητή.
- Το «SSL Change Cipher Spec Protocol», το οποίο στην πραγματικότητα αποκαθιστά συμφωνία για τη μέθοδο κρυπτογράφησης η οποία θα χρησιμοποιηθεί στην τρέχουσα συνεδρία SSL
- Το «SSL Alert Protocol» υπεύθυνο για την αποστολή μηνυμάτων λάθους ανάμεσα σε πελάτη κα εξυπηρετητή.

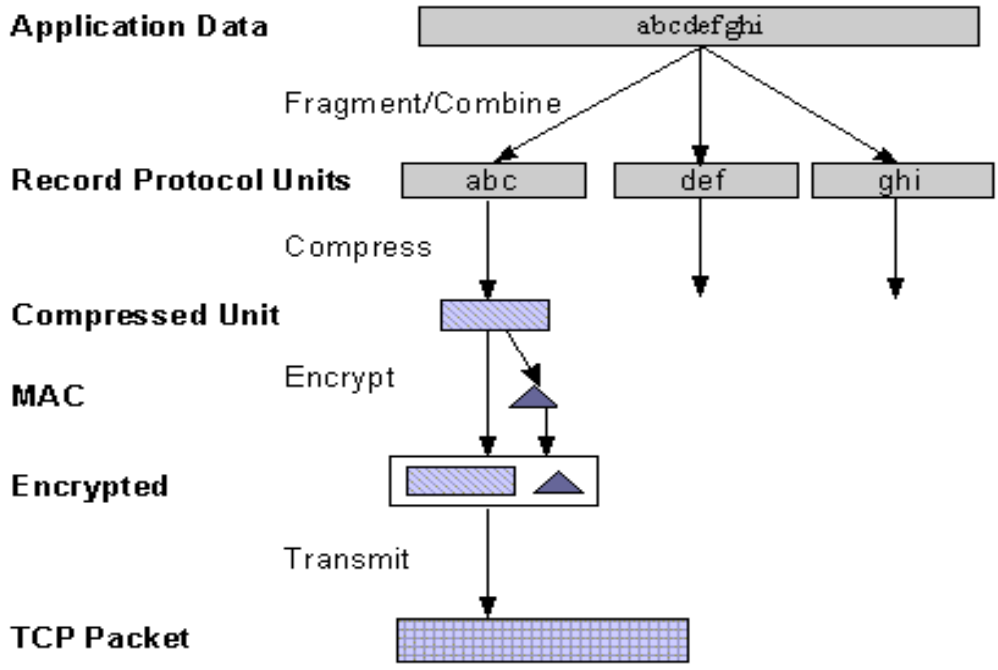
Τα παραπάνω πρωτόκολλα, όπως επίσης και τα δεδομένα από το πρωτόκολλο εφαρμογής ενθυλακώνονται σε ένα πρωτόκολλο το οποίο λέγεται «Πρωτόκολλο Εγγραφής SSL» (SSL Record Protocol), και περιγράφεται στο Σχήμα 2. Ένα ενθυλακωμένο πρωτόκολλο μεταφέρεται με την μορφή δεδομένων (data) από το

πρωτόκολλο χαμηλότερου επιπέδου, το οποίο δεν εξετάζει αυτά καθεαυτά τα δεδομένα. Το ενθυλακωμένο πρωτόκολλο δεν γνωρίζει επίσης τίποτα για το πρωτόκολλο από το οποίο προήλθε.

Η ενθυλάκωση των πρωτοκόλλων ελέγχου SSL (SSL control protocols) από το πρωτόκολλο εγγραφής σημαίνει με απλά λόγια ότι, αν μια ενεργή συνεδρία SSL επαναδιαπραγματευτεί (renegotiate), τα πρωτόκολλα ελέγχου θα μεταδοθούν με ασφαλή πλέον τρόπο. Στην περίπτωση που δεν υπήρχε ενεργή συνεδρία πρωτύτερα, τότε, δεν χρησιμοποιείται καμία μέθοδος κρυπτογράφησης (NULL Cipher Suite) και τα μηνύματα δεν έχουν συνόψεις ακεραιότητας μέχρις ότου αποκατασταθεί η συνεδρία SSL.

Μεταφορά Δεδομένων

Το πρωτόκολλο εγγραφής SSL (SSL Record Protocol), όπως φαίνεται στο Σχήμα 2.1, χρησιμοποιείται για την μεταφορά δεδομένων εφαρμογής αλλά και δεδομένων ελέγχου μεταξύ πελάτη και εξυπηρετητή, πιθανά κερματίζοντας αυτά τα δεδομένα σε μικρότερες ενότητες (units) ή συνδυάζοντας διάφορα πρωτόκολλα υψηλότερου επιπέδου ή ακόμα συμπιέζοντας, προσθέτοντας ψηφιακές υπογραφές και κρυπτογραφόντας τα δεδομένα αυτά πριν τη μεταφορά τους.



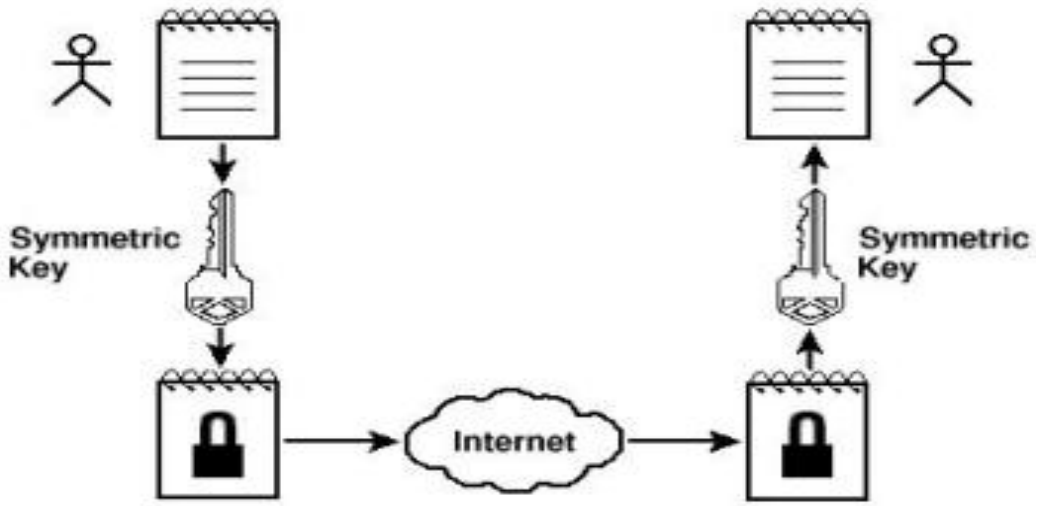
Σχήμα 2.1: Το πρωτόκολλο εγγραφής SSL (SSL record protocol)

3. ΚΡΥΠΤΟΓΡΑΦΙΑ

Στο κεφάλαιο αυτό περιγράφονται αναλυτικότερα οι σημαντικότεροι αλγόριθμοι κρυπτογραφίας. Όπως αναφέρθηκε στο προηγούμενο κεφάλαιο, ένας αντιστρέψιμος αλγόριθμος κρυπτογράφησης έχει ως στόχο να παίρνει στην είσοδο μια σειρά από χαρακτήρες ή σύμβολα και να βγάζει στην έξοδο μια νέα σειρά που να μπορεί με την αντίστροφη διαδικασία να επανέλθει στην αρχική σειρά από χαρακτήρες. Για να είναι αποτελεσματικός απαιτείται η χρήση ενός κλειδιού κρυπτογράφησης και αποκρυπτογράφησης. Όταν χρησιμοποιείται το ίδιο κλειδί και για την κρυπτογράφηση και για την αποκρυπτογράφηση, έχουμε συμμετρική κρυπτογραφία. Ασύμμετρη κρυπτογραφία έχουμε όταν χρησιμοποιείται ένα ζεύγος κλειδιών.

3.1 ΣΥΜΜΕΤΡΙΚΟ ΚΛΕΙΔΙ

Στη συμμετρική κρυπτογραφία ο αποστολέας και ο παραλήπτης γνωρίζουν και οι δύο το ίδιο κλειδί. Ο αποστολέας πριν στείλει το email, το κρυπτογραφεί χρησιμοποιώντας το κοινό κλειδί και μετατρέπει το κείμενο σε μια σειρά από χαρακτήρες που φαινομενικά δεν βγάζουν νόημα. Οποιοσδήποτε δεν γνωρίζει το κλειδί, δεν μπορεί να αποκρυπτογραφήσει το μήνυμα και άρα δεν μπορεί να διαβάσει το email. Το αποτέλεσμα είναι ότι ακόμα και αν κάποιος αποκτήσει ένα αντίγραφο του email δεν μπορεί να αποκτήσει πληροφορίες από το κείμενο, αλλά ούτε και να το τροποποιήσει σε άλλο κατανοητό κείμενο. Το μεγάλο πρόβλημα στην όλη διαδικασία είναι ότι τα δύο μέρη πρέπει να γνωρίζουν το ίδιο κλειδί. Πρέπει να βρεθεί ένας ασφαλής τρόπος ανταλλαγής του κλειδιού, γρήγορος και μη ανιχνεύσιμος, που είναι δύσκολο. Χαρακτηριστικό παράδειγμα αυτού του είδους κρυπτογραφίας είναι ο αλγόριθμος DES.



Σχήμα 3.1: Συμμετρικό κλειδί

3.2 Ο ΑΛΓΟΡΙΘΜΟΣ DES

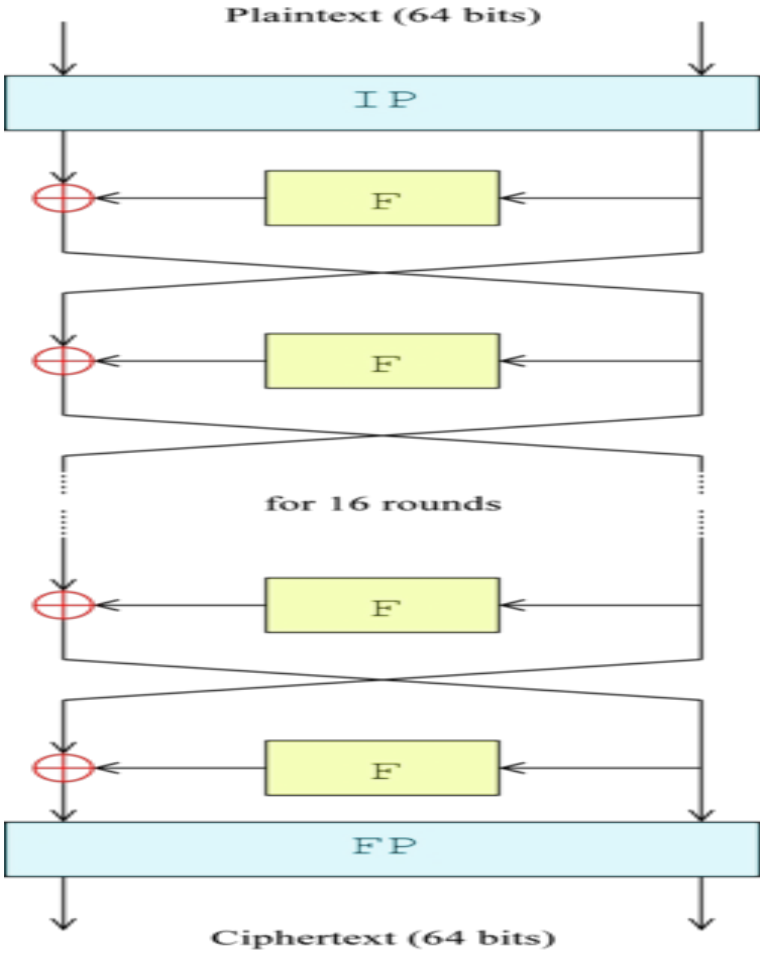
Ο αλγόριθμος DES (Data Encryption Standard) είναι μια μέθοδος κρυπτογράφησης πληροφοριών που επιλέχθηκε από τις ΗΠΑ ως το επίσημο ομοσπονδιακό πρότυπο επεξεργασίας πληροφοριών το 1976. Όταν πρωτοπαρουσιάστηκε, θεωρήθηκε ότι τα διαβαθμισμένα χαρακτηριστικά του καθώς και το σχετικά μικρό μήκος κλειδιού που επιλέχθηκαν, αποτελούσαν ένα δούρειο ίππο της NSA και έτσι η επιστημονική κοινότητα τον δέχθηκε επικριτικά. Το γεγονός αυτό οδήγησε σε επίμονη και αναλυτική μελέτη του αλγορίθμου και στην παγκόσμια ώθηση στην έρευνα για την κατανόηση των αλγορίθμων κρυπτογράφησης με μπλοκ.

Ο DES πλέον θεωρείται μη ασφαλής αλγόριθμος για την πλειοψηφία των εφαρμογών. Ο κύριος λόγος είναι το πολύ μικρό μήκος κλειδιού που ορίζεται στο πρωτόκολλο σε σχέση με την πολύ υψηλή ισχύ που επιδεικνύουν οι σύγχρονοι επεξεργαστές. Με χρήση ωμής δύναμης τα κλειδιά που χρησιμοποιεί ο DES έχουν σπάσει σε ορισμένες περιπτώσεις ακόμα και σε διάστημα 24 ωρών. Ο αλγόριθμος αυτός προσφέρει ικανή ασφάλεια στη μοντέρνα εκδοχή του που είναι ο Triple-DES. Αυτός, χρησιμοποιεί τον DES τρείς φορές με διαφορετικό κλειδί κάθε φορά για να κρυπτογραφήσει τα δεδομένα. Ακόμα καλύτερα αποτελέσματα έχουμε από τον αλγόριθμο που αντικατέστησε τον DES ως πρότυπο, τον AES (Advanced Encryption Standard).

Ο αλγόριθμος DES είναι ο πρότυπος αλγόριθμος κρυπτογράφησης σε ομάδες. Έχει ως είσοδο σταθερού μεγέθους γραμματοσειρές από το μη κρυπτογραφημένο κείμενο τις οποίες μετατρέπει με μια σειρά από πολύπλοκες λειτουργίες σε κωδικοποιημένες γραμματοσειρές του ιδίου μεγέθους. Στην περίπτωση του DES το μήκος της γραμματοσειράς είναι τα 64bits. Επίσης χρησιμοποιεί κλειδί εξατομικεύοντας την

μετατροπή ώστε να μπορεί να αποκρυπτογραφηθούν τα δεδομένα μόνο από αυτούς που γνωρίζουν το κλειδί κρυπτογράφησης. Το κλειδί αυτό είναι επίσης μήκους 64bits αλλά μόνο τα 56bits χρησιμοποιούνται από τον αλγόριθμο DES. Τα υπόλοιπα 8bits χρησιμοποιούνται αποκλειστικά για έλεγχο ορθότητας του κλειδιού και αγνοούνται από τον αλγόριθμο.

Η συνολική δομή του αλγορίθμου φαίνεται στο παρακάτω Σχήμα 3.2. Υπάρχουν 16 όμοια στάδια επεξεργασίας που ονομάζονται γύροι F. Για την φόρτωση και ανάγνωση των δεδομένων πριν και μετά από αυτά τα στάδια, υπάρχουν ακόμα δύο, τα IP (Initial Permutation) και FP (Final Permutation) που είναι αντίστροφα μεταξύ τους. Αν και τα IP και FP δεν έχουν κάποια κρυπτογραφική σημασία, χρησιμοποιούνται για την κατάλληλη εισαγωγή και εξαγωγή των ομάδων από bit σε σωστή μορφή. Πριν τους κυρίως γύρους, η ομάδα δεδομένων χωρίζεται σε δύο μισά των 32bit που υπόκεινται επεξεργασία διαδοχικά.



Σχήμα 3.2: Η συνολική δομή του αλγορίθμου DES

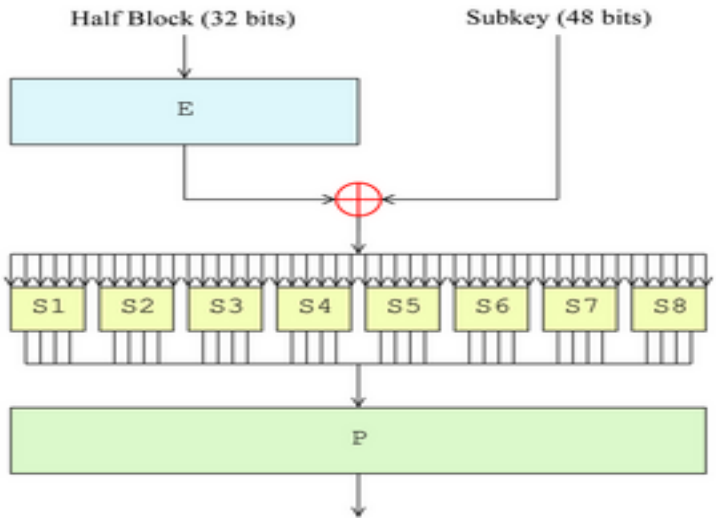
Με αυτή τη μέθοδο, γνωστή ως το σχήμα του Feistel, εξασφαλίζεται ότι η διαδικασία κρυπτογράφησης είναι ίδια με την διαδικασία αποκρυπτογράφησης. Η

διαφοροποίηση έγκειται στην αντίστροφη σειρά χρήσης των τμημάτων του κλειδιού. Ο υπόλοιπος αλγόριθμος παραμένει ο ίδιος. Οπότε δεν χρειάζεται ξεχωριστή εφαρμογή ή μηχανή για την κρυπτογράφηση ή αποκρυπτογράφηση.

Η διαδικασία του Feistel εφαρμόζεται κάθε φορά σε ένα τμήμα των 32bit και αποτελείται από 4 στάδια:

- Επέκταση: Το τμήμα των 32bit επεκτείνεται στα 48bit εφαρμόζοντας την επεκτατική μετατροπή αναπαράγοντας κάποια από τα bit.
- Σύνθεση με το Κλειδί: Η έξοδος της επέκτασης συνδυάζεται με ένα υποκλειδί με τη χρήση μιας XOR. 16 υποκλειδιά 48bit, ένα για κάθε γύρο, προέρχονται από το κυρίως κλειδί χρησιμοποιώντας τη μέθοδο παραγωγής υποκλειδιών που περιγράφεται παρακάτω.
- Αντικατάσταση: Η ομάδα των 32bit, αφού ανακατευτεί με το κλειδί, χωρίζεται σε 8 τμήματα των 6bit πριν την επεξεργασία από τα S-boxes ή κουτιά αντικατάστασης. Κάθε ένα από τα 8 S-boxes αντικαθιστά τα 6 bit εισόδου με 4 bit εξόδου. Η αντικατάσταση γίνεται βάση μιας μη γραμμικής συνάρτησης μετασχηματισμού που παρέχεται στη μορφή πίνακα αναζήτησης. Τα κουτιά αντικατάστασης είναι ο πυρήνας ασφάλειας του DES, αφού χωρίς αυτά η κρυπτογράφηση θα ήταν γραμμική και πολύ εύκολα αντιστρέψιμη.
- Μετατροπή: Τέλος, τα 32 bit εξόδου από τα S-boxes επανατοποθετούνται σύμφωνα με μια προαποφασισμένη μετατροπή στο P-box.

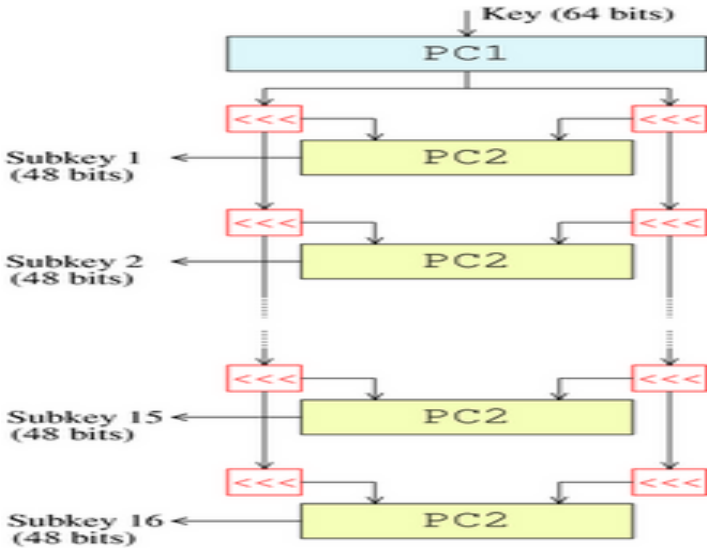
Τα τέσσερα αυτά βήματα παρέχουν δύο βασικά χαρακτηριστικά, απαραίτητα για μια ασφαλή αλλά και πρακτική κρυπτογράφηση, τη σύγχυση και τη διάχυση.



Σχήμα 3.3: Διαδικασία του Feistel

Ο αλγόριθμος *προγραμματισμού κλειδιών* είναι αυτός που παράγει τα υποκλειδιά που χρησιμοποιούνται στη σύνθεση, με βάση το κλειδί κρυπτογράφησης που επιλέγεται. Από τα 64 bit του κλειδιού, αφαιρούνται τα 8 bit που χρησιμεύουν για τον

έλεγχο του κλειδιού. Τα 56 bit που μένουν, χωρίζονται σε δύο ομάδες των 28 bit. Η κάθε ομάδα πλέον αξιοποιείται ξεχωριστά. Σε κάθε φάση οι δύο ομάδες περιστρέφονται αριστερόστροφα κατά μία ή δύο θέσεις. Από το αποτέλεσμα, επιλέγονται υποκλειδιά μήκους 48bit με τα 24bit από το ένα μισό και τα άλλα 24 από το άλλο. Οι περιστροφές εξασφαλίζουν ότι σε κάθε φάση θα χρησιμοποιηθεί διαφορετική ομάδα από bit για την κατασκευή του υποκλειδιού. Κατά μέσο όρο, κάθε bit χρησιμοποιείται στα 14 από τα 16 υποκλειδιά. Η διαδικασία κατασκευής των υποκλειδιών για την αποκρυπτογράφηση είναι η ίδια, αλλά οι ομάδες των 28bit περιστρέφονται δεξιόστροφα αντί για αριστερόστροφα.



Σχήμα 3.4: Αλγόριθμος προγραμματισμού κλειδιών

Παρόλο που περισσότερη προσπάθεια έχει δαπανηθεί στην κρυπτανάλυση του DES απ' ότι σε οποιοδήποτε άλλο αλγόριθμο κρυπτογράφησης σε ομάδες, ακόμα και σήμερα η αποτελεσματικότερη μέθοδος σπασίματος της κρυπτογράφησης αυτής είναι η επίθεση με ωμή βία. Διάφορες μικρές κρυπταναλυτικές ιδιότητες είναι γνωστές για τον αλγόριθμο και τρεις διαφορετικοί τρόποι επίθεσης έχουν εφευρεθεί. Παρόλο που αυτοί οι τρόποι επίθεσης έχουν μικρότερο βαθμό πολυπλοκότητας από την επίθεση ωμής βίας, η ποσότητα γνωστών ή επιλεγμένων δεδομένων που απαιτούν για την εφαρμογή τους, καθίστανται μη εφαρμόσιμοι και δεν αποτελούν απειλή.

Για κάθε αλγόριθμο κρυπτογράφησης η βασικότερη μέθοδος επίθεσης είναι αυτή της ωμή βίας. Στην επίθεση της ωμής βίας, πολύ απλά δοκιμάζονται όλα τα πιθανά κλειδία μέχρι να βρεθεί το σωστό. Το πλήθος των ενδεχόμενων κλειδιών είναι ανάλογο του μήκους κλειδιού που χρησιμοποιείται. Όσον αφορά τον αλγόριθμο DES, ερωτηματικά υπήρχαν ακόμα και πριν καθιερωθεί ως πρότυπο, σχετικά με το μήκος κλειδιού που επιλέχθηκε και την αποτελεσματικότητά του. Τελικά το μήκος του κλειδιού ήταν που οδήγησε στην αντικατάστασή του παρά η όποια κρυπτανάλυση. Είναι γνωστό ότι η NSA προέτρεψε την IBM να μειώσει το μήκους κλειδιού αρχικά

από τα 128bit στα 64bit και τελικά στα 56bit, γεγονός που αποτελεί μια ένδειξη ότι η NSA είχε την επεξεργαστική ισχύ για το σπάσιμο ενός κλειδιού αυτού του μήκους ήδη από τα μέσα του 1970. Το 1998 η Electronic Frontier Foundation, μια ομάδα υπέρ των δικαιωμάτων του χρήστη στο διαδίκτυο, κατασκεύασε μια εξειδικευμένη μηχανή κόστους $250000 με στόχο να αποδείξει πόσο εύκολο είναι να σπάσει ένα κλειδί του DES. Ο χρόνος που χρειάστηκε αυτή η μηχανή για να τα καταφέρει ήταν λίγο πάνω από 2 μέρες.

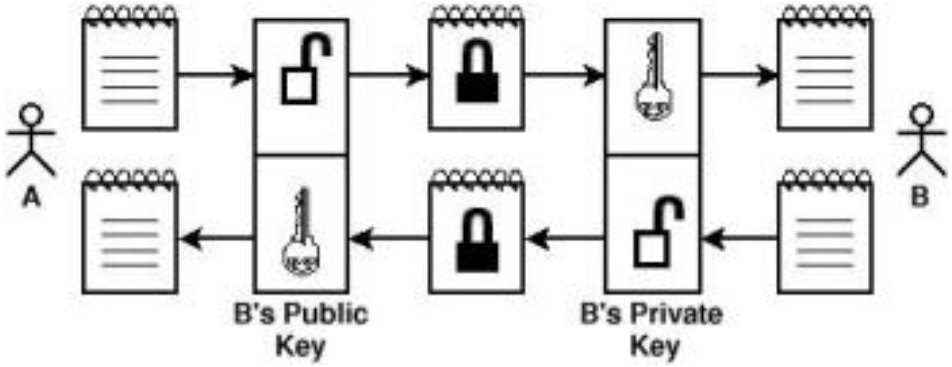
Όπως αναφέρθηκε, υπάρχουν 3 επιθέσεις που θεωρητικά είναι γρηγορότερες από τη δοκιμή όλων των ενδεχόμενων κλειδιών. Αυτές βασίζονται στο σχεδιασμό του αλγορίθμου DES έπειτα από μελέτη του τρόπου λειτουργίας του. Πάντως αυτές οι επιθέσεις είναι θεωρητικές και μη εφαρμόσιμες σην πράξη.

- Διαφορική Κρυπτανάλυση: Ανακαλύφθηκε στα τέλη του 1980 από τους Eli Biham και Adi Shamir, παρόλο που ήταν γνωστή και στην IBM και την NSA κατά το σχεδιασμό του DES. Αν και κρατήθηκε μυστικό, ο DES σχεδιάστηκε για να είναι ανθεκτικός σε αυτή τη μορφή επίθεσης. Για να σπάσουν και οι 16 γύροι του αλγορίθμου απαιτούνται 2^{47} επιλεγμένα μη κρυπτογραφημένα κομμάτια δεδομένων.
- Γραμμική Κρυπτανάλυση: Ανακαλύφθηκε από τον Mitsuru Matsui το 1993 και αναλύθηκε μέχρι το τέλος του 1994 από τους Kaliski, Robshaw και Biryukov στη μορφή της πολλαπλής γραμμικής κρυπτανάλυσης. Η μέθοδος αυτή απαιτεί 2^{43} γνωστά μη κρυπτογραφημένα κομμάτια δεδομένων. Η ανάλυση του Biryukov δείχνει ότι η χρήση της πολλαπλής γραμικής κρυπτανάλυσης μειώνει την πολυπλοκότητα στο 2^{41}. Το 2000 οι Knudsen και Mathiassen απέδειξαν ότι η ίδια βελτίωση μπορεί να υπάρξει με χρήση επιλεγμένων μη κρυπτογραφημένων τμημάτων δεδομένων. Ο Junod κάνοντας εκτενή πειράματα το 2001 έφτασε στο συμπέρασμα ότι η χρονική πολυπλοκότητα είναι στην πράξη λίγο μικρότερη και ότι χρειάζονται από 2^{39} ως 2^{41} δοκιμές του DES για να σπάσει ένα κλειδί.
- Επίθεση του Davies: Η επίθεση του Davies, σε αντίθεση με την Διαφορική ή Γραμμική Κρυπτανάλυση είναι μια εξειδικευμένη στον DES επίθεση. Στην τελική και ισχυρότερη μορφή της, απαιτεί $2^{\mathbf{50}}$ γνωστά μη κρυπτογραφημένα κομμάτια δεδομένων και έχει υπολογιστική πολυπλοκότητα $2^{\mathbf{50}}$ με επίπεδα επιτυχίας της τάξης του 51%.

3.3 ΑΣΥΜΜΕΤΡΟ ΚΛΕΙΔΙ

Στην ασύμμετρη κρυπτογραφία, κάθε χρήστης έχει δύο κλειδιά. Τα κλειδιά αυτά ονομάζονται, κοινώς, το ένα δημόσιο και άλλο ιδιωτικό. Το δημόσιο κλειδί κυκλοφορεί ελεύθερα, όπως λέει και το όνομά του, ενώ το ιδιωτικό παραμένει κρυφό και στη γνώση μόνο του ιδιοκτήτη. Κάθε μήνυμα που κωδικοποιείται από το ένα από τα δύο κλειδιά μπορεί να αποκωδικοποιηθεί από το άλλο και μόνο από αυτό. Έτσι, μπορεί κάποιος να κρυπτογραφήσει ένα email χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη και να είναι σίγουρος ότι θα μπορεί να το διαβάσει μόνο αυτός. Αντίστοιχα αν ένα τμήμα του email (ή ολόκληρο) κρυπτογραφηθεί με το ιδιωτικό

κλειδί του αποστολέα, αυτό μπορεί να αποκρυπτογραφηθεί μόνο με χρήση του δημοσίου κλειδιού του αποστολέα, αρά ο παραλήπτης μπορεί να είναι σίγουρος για την προέλευση του email. Η καλύτερη τακτική είναι να χρησιμοποιηθούν οι δύο μέθοδοι σε συνδυασμό. Δηλαδή να υπογράψει ο αποστολέας το email κρυπτογραφώντας ένα τμήμα του με το ιδιωτικό του κλειδί και μετά να κρυπτογραφήσει το σύνολο με το δημόσιο κλειδί του παραλήπτη. Το αποτέλεσμα είναι να μπορεί να αναγνωσθεί το email μόνο από τον επιθυμητό παραλήπτη και συγχρόνως να είναι σίγουρος ο παραλήπτης ότι το email προέρχεται από τον αποστολέα. Ο συνηθέστερος αλγόριθμος που χρησιμοποιείται είναι ο RSA.



Σχήμα 3.5: Ασύμμετρο Κλειδί

3.4 Ο ΑΛΓΟΡΙΘΜΟΣ RSA

Ο αλγόριθμος RSA περιγράφηκε το 1977 από τους Ron Rivest, Adi Shamir και Len Adleman στο MIT. Από τα επώνυμα τους προέρχεται και το όνομα του αλγορίθμου. Είναι ο πρώτος αλγόριθμος κατάλληλος για την κρυπτογράφηση αλλά και την υπογραφή ενός κειμένου. Θεωρείται μια από τις μεγαλύτερες ανακαλύψεις στο χώρο της κρυπτογραφίας δημοσίου κλειδιού. Είναι ιδιαίτερα διαδεδομένος ακόμα και σήμερα, αφού με μεγάλο μήκος κλειδιού είναι ικανοποιητικά ασφαλής. Αν και ο αλγόριθμος έγινε πατέντα από το MIT το 1983 στις ΗΠΑ, στον υπόλοιπο πλανήτη παρέμεινε ελεύθερος αφού είχε ήδη εκδοθεί πολύ νωρίτερα. Η πατέντα αυτή έληξε το Σεπτέμβριο του 2000.

Πώς όμως δουλεύει ο RSA. Ας θεωρήσουμε ότι η Alice θέλει να επιτρέψει στον Bob να της στέλνει ιδιαίτερα μηνύματα μέσω ενός μη ασφαλούς μέσου επικοινωνίας. Θα πρέπει να ακολουθήσει κάποια βήματα για την κατασκευή ενός δημόσιου και ενός ιδιωτικού κλειδιού.

- Επιλογή δύο μεγάλων πρώτων αριθμών, *p* και *q* τέτοιων ώστε *p#q*, τυχαίων και ανεξαρτήτων μεταξύ τους.
- Υπολογισμός του *n=p*q*.
- Υπολογισμός του totient *φ(n)=(p-1)(q-1)*
- Επιλογή ενός πρώτου αριθμού *1<e<φ(n)* που να είναι πρώτος σε σχέση με το

φ(n).
- Υπολογισμός του d τέτοιο ώστε *d*e=1 (modφ)*.

Το δημόσιο κλειδί αποτελείται από τα *n* και *e, ενώ το* ιδιωτικό κλειδί είναι τα *n* και *d*, αλλά συνήθως αποθηκεύονται τα *p* και *q* που χρησιμοποιήθηκαν για την έκδοση του κλειδιού, το *d mod (p-1)* και το *d mod (q-1)* πιο γνωστά ως dmp1 και dmq1 αντίστοιχα και το *(1/q) mod p* γνωστό ως iqmp.
Στη δεύτερη μορφή που ονομάζεται από το Κινέζικο Θεώρημα για το Υπόλοιπο CRT (Chinese Remainder Theorem) όλα τα τμήματα του ιδιωτικού κλειδιού πρέπει να παραμείνουν κρυφά.

Ο Bob λοιπόν αποφασίζει να στείλει ένα μήνυμα M στην Alice. Μετατρέπει το M σε έναν αριθμό m μικρότερο από το n. Αυτό γίνεται χρησιμοποιώντας μια προαπαφασισμένη συνάρτηση που ονομάζεται μέθοδος πρόσφυσης. Ο Bob, γνωρίζοντας τα n και e που έχει ανακοινώσει η Alice, και έχοντας υπολογίσει το m που θέλει να κρυπτογραφήσει, υπολογίζει το τελικό c βάσει του τύπου:

c=m^e mod n

Αυτό μπορεί να γίνει ταχύτατα με την μέθοδο ύψωσης σε δύναμη με τετραγωνισμό. Τέλος το c αποστέλλεται στην Alice.

Όταν η Alice παραλάβει το c που έστειλε ο Bob, αφού γνωρίζει το ιδιωτικό της κλειδί d μπορεί να υπολογίσει το m ακολουθώντας τη διαδικασία *m=e^d mod n*.

4. ΤΟ ΠΡΩΤΟΚΟΛΛΟ PGP

4.1 ΙΣΤΟΡΙΑ ΚΑΙ ΑΝΑΠΤΥΞΗ

Σε αντίθεση με άλλα πρωτόκολλα κρυπτογράφησης όπως το PEM και το MOSS, το PGP (Pretty Good Privacy) είναι συγχρόνως και ένα πρόγραμμα υπολογιστή που παρέχει κρυπτογραφική ασφάλεια και αυθεντικοποίηση. Η αρχική του μορφή σχεδιάστικε και αναπτύχθηκε από τον Phil Zimmermann το 1991. Αποδείχθηκε τόσο αποτελεσματικό ώστε οι αλγόριθμοι και τύποι δεδομένων του έγιναν πρότυπο για την καλύτερη συνεργασία λογισμικού διαφορετικών κατασκευαστών. Τελικά το PGP μετατράπηκε σε ανοιχτό πρότυπο που χρησιμοποιείται και από τα GNU Privacy Guard (GnuPG), Hushmail, Veridis και Authora ενώ μετονομάστηκε σε OpenPGP. Σε όλα τα μήκη και πλάτη του πλανήτη είναι το πιο ευρέως χρησιμοποιούμενο πρωτόκολλο κρυπτογράφησης.

Παρόλο που το PGP μπορεί να κρυπτογραφήσει οποιοδήποτε αρχείο ή δεδομένα, η συνηθέστερη χρήση του είναι στην κρυπτογράφηση και υπογραφή ηλεκτρονικού ταχυδρομείου. Είναι το ένα από τα δύο πρωτόκολλα που υιοθετήθηκαν από την NIST ως συστήματα ασφαλείας ηλεκτρονικού ταχυδρομείου. Το άλλο είναι το S/MIME που παρουσιάζεται στο επόμενο κεφάλαιο.

4.2 ΠΕΡΙΓΡΑΦΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ

Το PGP ενσωματώθηκε στον τρόπο λειτουργίας του ηλεκτρονικού ταχυδρομείου, προσθέτοντας μια ειδική μορφοποίηση (ASCII armor) στο σώμα του μηνύματος. Οι περισσότερες εφαρμογές πελάτη για ηλεκτρονικό ταχυδρομείο προσφέρουν τη δυνατότητα χρήσης του PGP με την υλοποίηση πρόσθετων για την εφαρμογή τους.

Σε αρκετές από αυτές τις εφαρμογές δίνεται η δυνατότητα να επιλέξει ο χρήστης ανάμεσα σε διαφορετικές υλοποιήσεις του PGP.

Από πλευράς ασφαλείας κάθε ένα από αυτά τα πρόσθετα παρέχει διαφορετικό επίπεδο προστασίας, ανεξάρτητο από τη σχεδίαση του PGP. Αυτό οφείλεται στην υλοποίηση του PGP που μπορεί να έχει κατασκευαστικά λάθη ή να συνεργάζεται με λιγότερο ασφαλή τρόπο με το PGP και τα υπόλοιπα προγράμματα σε έναν υπολογιστή. Η ασφαλέστερη είναι να κρυπτογραφηθεί και υπογραφεί το μήνυμα πριν την αποστολή του, με χειροκίνητο τρόπο. Επειδή αυτή η λύση δεν είναι πρακτική, συνίσταται η δοκιμή διάφορων συνδυασμών εφαρμογής και πρόσθετου με την αποστολή δοκιμαστικών μηνυμάτων από τον χρήστη είτε στον εαυτό του είτε σε κάποιο γνωστό. Όποιο και αν είναι το επίπεδο που προσφέρει ένας τέτοιος συνδυασμός και ανεξάρτητα από τους κινδύνους ασφαλείας που μπορεί να παραμένουν, η χρήση του PGP είναι πάντα καλύτερη από τη μη χρήση κανενός συστήματος.

Εισαγωγή

Το PGP χρησιμοποιεί συγχρόνως και την συμμετρική και την ασύμμετρη κρυπτογραφία, καθώς και ένα σύστημα για τη σύνδεση των δημοσίων κλειδιών με κάποιο χρήστη γνωστό ως ιστός εμπιστοσύνης (Web of Trust). Στο PGP χρησιμοποιείται το ζεύγος κλειδιών που έχει προκατασκευασμένα ο αποδέκτης ενός μηνύματος. Ο αποστολέας κρυπτογραφεί, με το δημόσιο κλειδί του παραλήπτη, ένα κρυφό κλειδί συμμετρικής κρυπτογραφίας το οποίο και χρησιμοποιεί για να κρυπτογραφήσει το αποστελλόμενο μήνυμα. Το δημόσιο κλειδί ενός χρήστη μπορεί να το αποκτήσει κάποιος είτε με την αποστολή του από τον ιδιοκτήτη σε προηγούμενο μήνυμα, είτε από έναν από τους πολυάριθμους διακομιστές κλειδιών PGP ανά τον πλανήτη.
Ο παραλήπτης του μηνύματος αποκρυπτογραφεί το κλειδί που χρησιμοποιήθηκε για να κρυπτογραφηθεί το μήνυμα χρησιμοποιώντας το ιδιωτικό του κλειδί. Ο λόγος που χρησιμοποιούνται και οι δύο αλγόριθμοι και δεν κρυπτογραφείται ολόκληρο το μήνυμα με το δημόσιο κλειδί, είναι η μεγάλη διαφορά στην ταχύτητα που έχουν οι αλγόριθμοι συμμετρικής και ασύμμετρης κρυπτογραφίας. Οι αλγόριθμοι συμμετρικής κρυπτογραφίας είναι πολύ πιο γρήγοροι στη χρήση τους και επιλέγονται για την κρυπτογράφηση του μεγάλου σε όγκο σώματος του μηνύματος. Η ασύμμετρη κρυπτογραφία δίνει τη δυνατότητα να ανταλλαγεί το κλειδί της κρυπτογράφησης του μηνύματος με ασφαλή τρόπο.
Μια παρόμοια τακτική μπορεί να χρησιμοποιηθεί για να αντιληφθεί ο παραλήπτης του μηνύματος αν αυτό έχει τροποποιηθεί μετά την αποστολή του. Συγχρόνως μπορεί να χρησιμοποιηθεί αυτή η τακτική και για την υπογραφή του μηνύματος από τον αποστολέα. Δημιουργείται ένα άθροισμα του μηνύματος βάση μιας συνάρτησης μονόδρομης αντικατάστασης. Έπειτα, αυτό το άθροισμα κρυπτογραφείται με το ιδιωτικό κλειδί του αποστολέα. Η αποκρυπτογράφηση του αθροίσματος μπορεί να γίνει από τον παραλήπτη μόνο με τη χρήση του σωστού δημοσίου κλειδιού. Παράλληλα, αν έχει τροποποιηθεί το μήνυμα θα έχει αλλάξει το άθροισμα, οπότε ο παραλήπτης μπορεί να το αντιληφθεί αμέσως.

Υποστηριζόμενοι αλγόριθμοι

Το PGP, όπως και το OpenPGP, στηρίζουν τη λειτουργία τους σε αλγορίθμους που προϋπήρχαν το 1991 και έχουν έκτοτε δοκιμαστεί εκτενώς. Τέτοιοι αλγόριθμοι, όπως οι MD5, IDEA και RSA, μπορούν να θεωρηθούν ασφαλείς, αφού τουλάχιστον ως τώρα, δεν υπάρχει κάποια ανακοινωμένη εγγενής έλλειψη ασφαλείας. Λόγω της ύπαρξης πατεντών σε αυτούς τους αλγορίθμους, το PGP ακόμα δεν έχει γίνει πρότυπο από την IETF. Για να ξεπεραστεί αυτό το πρόβλημα στο OpenPGP, το πρότυπο επιτρέπει τη χρήση πολλών διαφορετικών αλγορίθμων για την δημιουργία κλειδιών, την υπογραφή αλλά και την κρυπτογράφηση και αποκρυπτογράφηση των μηνυμάτων. Τέτοιοι αλγόριθμοι είναι οι SHA-1, 3DES, DSA, CAST, Blowfish, ElGamal και άλλοι.

Επεξεργασία μηνύματος

Ο αλγόριθμος PGP επεξεργάζεται ένα μήνυμα πριν την αποστολή του με έναν συνδυασμό από τους παραπάνω αλγορίθμους ανάλογα με το ποιες λειτουργίες θα εφαρμοστούν. Για την δημιουργία μιας ψηφιακής υπογραφής απαιτείται η χρήση ενός αλγορίθμου σύνοψης και τουλάχιστον ενός αλγορίθμου δημοσίου κλειδιού. Το PGP ορίζει την υποχρεωτική χρήση των αλγορίθμων MD5 για την δημιουργία της σύνοψης και του RSA για τη σύνδεσή του με το δημόσιο κλειδί, ενώ το OpenPGP προτείνει την χρήση αντίστοιχα των SHA-1 και DSA. Η πλήρης λειτουργία ολοκληρώνεται σε τρία βήματα:

- πρώτον, ο αποστολέας χρησιμοποιεί μια μονόδρομη συνάρτηση κωδικοποίησης για τη δημιουργία της σύνοψης του μηνύματος
- δεύτερον, ο αποστολέας κρυπτογραφεί την σύνοψη με τη χρήση του ιδιωτικού του κλειδιού και
- τρίτον, ο αποστολέας προσαρτά την κρυπτογραφημένη σύνοψη, η οποία αποτελεί την ψηφιακή υπογραφή, στο μήνυμα

Ο παραλήπτης του μηνύματος έχει πλέον το αρχικό μήνυμα, καθώς και την κρυπτογραφημένη σύνοψη. Αρχικά, μπορεί να αποκρυπτογραφήσει την ψηφιακή υπογραφή χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα. Το κλειδί αυτό περιλαμβάνεται στο κομμάτι της υπογραφής. Στη συνέχεια, από το αρχικό μήνυμα ο παραλήπτης δημιουργεί με τη σειρά του την σύνοψη του μηνύματος. Μπορεί συγκρίνοντας την αποκρυπτογραφημένη σύνοψη με αυτήν που δημιούργησε μόνος του , εφόσον είναι ίδιες, να θεωρήσει ότι η ψηφιακή υπογραφή επαληθεύτηκε και ότι το μήνυμα είναι αυθεντικό.

Σε περίπτωση που ο χρήστης θέλει να συμπιέσει το μήνυμα, αυτό σύμφωνα με το πρωτόκολλο PGP αυτό θα συμβεί μετά την υπογραφή του μηνύματος και πριν την κρυπτογράφησή του. Υπάρχουν δύο λόγοι για αυτό. Ο πρώτος είναι ότι για την επαλήθευση της ψηφιακής υπογραφής θα απαιτούνταν είτε η συνύπαρξη του συμπιεσμένου και του ασυμπίεστου μηνύματος είτε η επανασυμπίεση του κάθε φορά που θέλουμε να κάνουμε επαλήθευση. Δεύτερον, ο αλγόριθμος που χρησιμοποιείται για την συμπίεση, επιτρέπει να ορίσει ο χρήστης το βαθμό συμπίεσης με αποτέλεσμα

να μπορούμε να έχουμε διαφορετικά συμπιεσμένα μηνύματα μεταξύ τους που θα μας οδηγήσουμε σε διαφορετικές συνόψεις ακόμη και αν χρησιμοποιήσουμε τον ίδιο αλγόριθμο συμπίεσης. Προφανώς η συμπίεση του μηνύματος προηγείται της κρυπτογράφησης, καθώς όταν ο αλγόριθμος κρυπτογράφησης που χρησιμοποιείται είναι κρυπτογραφικά σωστός, τότε το αποτέλεσμα της κρυπτογράφησης δεν θα έπρεπε να συμπιέζεται.

Η κρυπτογράφηση ενός μηνύματος σύμφωνα με το PGP μπορεί να γίνει είτε με τη χρήση δημοσίου κλειδιού είτε με τη χρήση κρυφού κλειδιού. Ο κάθε χρήστης μπορεί να επιλέξει όποια μέθοδο προτιμά. Όταν ο χρήστης επιλέγει τη μέθοδο του δημοσίου κλειδιού , στην αρχή παράγει έναν τυχαίο αριθμό ο οποίος χρησιμοποιείται ως κλειδί συνεδρίας. Έπειτα το μήνυμα κρυπτογραφείται με τη χρήση αυτού του κλειδιού συνεδρίας σε κάποιον αλγόριθμο κρυπτογράφησης. Τέλος, το κλειδί συνεδρίας κρυπτογραφείται για κάθε παραλήπτη ξεχωριστά, χρησιμοποιώντας το δημόσιο κλειδί αυτού και το αποστέλλει μαζί με το κρυπτογραφημένο μήνυμα. Ο κάθε παραλήπτης με τη χρήση του ιδιωτικού του κλειδιού μπορεί να αποκρυπογραφήσει το κλειδί συνεδρίας και έπειτα με αυτό το κλειδί να αποκρυπτογραφήσει το κρυπτογραφημένο μήνυμα. Όταν χρησιμοποιείται η μέθοδος του κρυφού κλειδιού, το μήνυμα μπορεί να κρυπτογραφηθεί είτε απευθείας με ένα κρυφό κλειδί που προκύπτει από μια συνθηματική φράση γνωστή σε όλα τα μέρη είτε με την παραγωγή ενός τυχαίου κλειδιού όπως στην προηγούμενη μέθοδο και την κρυπτογράφηση αυτού του τυχαίου κλειδιού με την κοινή συνθηματική φράση.

Σε κάθε περίπτωση μπορούν συγχρόνως στο ίδιο μήνυμα, να συνυπάρχουν ψηφιακή υπογραφή και κρυπτογράφηση.

Κρυπτογραφικά κλειδιά

Όπως είδαμε ως τώρα, το PGP χρησιμοποιεί τρεις τύπους κλειδιών:

- κλειδιά συνεδρίας, που χρησιμοποιούνται μόνο μία φορά
- κλειδιά παραγόμενα από κάποια συνθηματική φράση
- ζεύγη δημοσίου και ιδιωτικού κλειδιού

Το κάθε είδος από αυτά τα κλειδιά έχει διαφορετικές απαιτήσεις όσον αφορά τη δημιουργία αλλά και διαχείρισή τους.

Τα κλειδιά συνεδρίας είναι κλειδιά που παράγονται από κάποια μηχανή κρυπατανάλυσης. Το σημαντικότερο σε αυτά είναι η παραγωγή τους να είναι όσο το δυνατόν πιο απρόβλεπτη σ' οποιονδήποτε τρίτο. Συνήθως, παράγονται από μια μηχανή παραγωγής τυχαίων αριθμών.

Τα κλειδιά που παράγονται από κάποια συνθηματική φράση, χρησιμοποιούνται για κρυπτογράφηση και για την προστασία δημοσίων και ιδιωτικών κλειδιών. Όπως είναι φυσικό οι συνθηματικές φράσεις που χρησιμοποιούνται για την παράγωγή τέτοιων κλειδιών είναι καλό να είναι εύκολα απομνημονεύσιμες αλλά δύσκολα μαντεύσιμες και δεν θα έπρεπε να τις έχουμε κάπου σημειωμένες.

Τέλος, το πρωτόκολλο PGP προτείνει τα ζεύγη δημοσίων και ιδιωτικών κλειδιών να

αποθηκεύονται σε δύο διαφορετικές δομές από τον κάθε χρήστη. Στην πρώτη δομή ο χρήστης αποθηκεύει τα δικά του ζεύγη κλειδιών, ενώ στην δεύτερη αποθηκεύει τα δημόσια κλειδιά όλων των υπολοίπων. Για την διαχείρισή αυτών των δύο δομών προτείνεται η χρήση ενός μοντέλου εμπιστοσύνης το οποίο ονομάζεται Web Of Trust (Δίκτυο Εμπιστοσύνης).

4.3 ΔΙΚΤΥΟ ΕΜΠΙΣΤΟΣΥΝΗΣ

Το πρωτόκολλο PGP όπως και το openPGP ορίζουν ένα δικό τους μοντέλο εμπιστοσύνης για τη διαχείριση διευθύνσεων emai, ταυτοτήτων και ζυγών δημοσίων και ιδιωτικών κλειδιών. Το μοντέλο αυτό ορίζει το μέγεθος και τη μορφή των κλειδιών, τον τρόπο θεμελίωσης εμπιστοσύνης, τον τρόπο ακύρωσης κλειδιών και τον τρόπο ανταλλαγής αυτών.

Πιστοποιητικά PGP

Σύμφωνα με το πρωτόκολλο PGP η σύνδεση μεταξύ της ταυτότητας ενός χρήστη, της διεύθυνσης ηλεκτρονικού ταχυδρομείου που χρησιμποιεί και ενός ζεύγους δημοσίου και ιδιωτικού κλειδιού γίνεται με τη χρήση ενός πιστοποιητικού που το ονομάζουμε πιστοποιητικό PGP.΄Οπως θα δούμε στο επόμενο κεφάλαιο, πιστοποιητικά χρησιμοποιεί και το S/MIME, τα οποία ονομάζονται πιστοποιητικά X.509.Τα πιστοποιητικά PGP εκδίδονται για ένα ζεύγος κλειδιών και μπορούν να περιέχουν περισσότερες από μια ηλεκτρονικές διευθύνσεις και υπογραφές. Επίσης, περισσότερες από μία ψηφιακές υπογραφές μπορούν να βεβαιώνουν ότι η συγκεκριμένη ηλεκτρονική διεύθυνση σχετίζεται με το συγκεκριμένο δημόσιο κλειδί.

Το πιστοποιητικό PGP είναι μια δομή δεδομένων που περιλαμβάνει τα παρακάτω πεδία:

- version number: αυτό το πεδίο χρησιμοποιείται για την αναγνώριση της έκδοσης του PGP που χρησιμποιήθηκε για την έκδοση του ζεύγους κλειδιών
- Public key: σε αυτό το πεδίο υπάρχει το δημόσιο κλειδί και ο αντίστοιχος αλγόριθμος για τη χρήση του
- certificate owner information: αυτό το πεδίο χρησιμοποιείται για τις πληφορίες ταυτότητας του ιδιοκτήτη του πιστοποιητικού, δηλαδή αυτού που έχει το αντίστοιχο ιδιωτικό κλειδί
- self signature: σε αυτό το πεδίο ο ιδιοκτήτης του πιστοποιητικού υπογράφει ο ίδιος, χρησιμοποιώντας το ιδιωτικό του κλειδί, το πιστοποιητικό
- validity period: σε αυτό το πεδίο περιγράφεται η ημερομηνία έναρξης και λήξης της ισχύος του συγκεκριμένου πιστοποιητικού
- preferred encryption algorithm: σε αυτό το πεδίο ο ιδιοκτήτης του πιστοποιητικού αναγράφει τον προτιμώμενο από αυτόν αλγόριθμο κωδικοποίησης

Όπως προαναφέρθηκε, τη συσχέτιση μεταξύ μιας ηλεκτρονικής ταυτότητας και ενός ψηφιακού πιστοποιητικού μπορούν να την πιστοποιήσουν περισσότεροι από ένας άνθρωποι υπογράφοντας ηλεκτρονικά το ψηφιακό πιστοποιητικό.

Θεμελίωση εμπιστοσύνης

Στην πραγματική ζωή κάθε άνθρωπος εμπιστεύεται κάποιους άλλους τους οποίους γνωρίζει, αλλά όχι απαραίτητα όλους αυτούς που το περιβάλλον του με τη σειρά του εμπιστεύεται. Συμπεραίνουμε λοιπόν ότι η εμπιστοσύνη δεν είναι ένα χαρακτηριστικό το οποίο μεταφέρεται. Αυτό το συμπέρασμα υλοποιείται και από το το πρωτόκολλο PGP.

Κάθε χρήστης του πρωτοκόλλου υπογράφοντας το πιστοποιητικό δηλώνει παράλληλα την εμπιστοσύνη προς τον ιδιοκτήτη του πιστοποιητικού. Τα επίπεδα εμπιστοσύνης είναι τρία:

- απόλυτη εμπιστοσύνη έχει ο χρήστης για ένα πιστοποιητικό για το οποίο γνωρίζει και το δημόσιο και το ιδιωτικό κλειδί, δηλαδή το πιστοποιητικό του ανήκει
- οριακή εμπιστοσύνη έχει ο χρήστης για ένα πιστοποιητικό για το οποίο γνωρίζει το δημόσιο κλειδί και την ηλεκτρονική διεύθυνση με την οποία σχετίζεται
- έλλειψη εμπιστοσύνης έχει ο χρήστης για τα πιστοποιητικά για τα οποία δεν γνωρίζει κάποια πληροφορία

Ο κάθε χρήστης για να αποφασίσει αν εμπιστεύεται το πιστοποιητικό το οποίο του παρουσιάζεται πρέπει να ισχύει μία από τις εξής συνθήκες:

- δύο ή περισσότεροι χρήστες τους οποίους εμπιστεύεται να συνυπογράφουν το υπό εξέταση πιστοποιητικό με τουλάχιστον οριακή εμπιστοσύνη
- ένας ή περισσότεροι χρήστες τους οποίους εμπιστεύεται να συνυπογράφουν το υπό εξέταση πιστοποιητικό με απόλυτη εμπιστοσύνη

Ανάκληση κλειδιού

Η δημιουργία των πιστοποιητικών PGP έχει ημερομηνία έκδοσης καθώς και ημερομηνία λήξης της ισχύος τους. Μπορούμε λοιπόν να γνωρίζουμε αν κατά τη χρήση του πιστοποιητικού ισχύει ή όχι. Παρόλα αυτά υπάρχει περίπτωση να θέλουμε να καταργήσουμε ένα πιστοποιητικό είτε επειδή έχει διαρραγεί η ασφάλεια του ζεύγους των κλειδιών είτε για οποιοδήποτε άλλο λόγο. Πρέπει λοιπόν να υπάρχει ένας τρόπος ν' ανακληθεί κάποιο πιστοποιητικό. Θα μπορούσε να υπάρχει μία λίστα με όλα τα πιστοποιητικά τα οποία ισχύουν. Κάτι τέτοιο θα δημιουργούσε τεράστιο φόρτο εργασίας σ' οποιονδήποτε τα διαχειρίζεται. Το πρωτόκολλο PGP λοιπόν ορίζει μια μέθοδο για την ανάκληση πιστοποιητικών. Αυτή γίνεται με την έκδοση ενός πιστοποιητικού ανάκλησης, το οποίο είναι υπογεγραμμένο από τον ιδιοκτήτη του πιστοποιητικού PGP το οποίο ανακαλεί. Αυτό το πιστοποιητικό ανάκλησης μετά πρέπει να το μοιράσει σ' όλους αυτούς που έχουν το PGP πιστοποιητικό του ώστε να

τους ενημερώσει να μην χρησιμοποιούν πλέον το συγκεκριμένο ζεύγος κλειδιών.

Επίσης για την έκδοση πιστοποιητικών αλλά και για την ανάκληση τους το πρωτόκολλο PGP πλέον ορίζει τη χρήση διακομιστών πιστοποιητικών PGP.

Διακομιστές πιστοποιητικών PGP

Στον αρχικό ορισμό του πρωτοκόλλου PGP η κυκλοφορία των πιστοποιητικών επαφίετο στον εκάστοτε χρήστη. Σήμερα κυριώς λόγω της πολυπλοκότητας της διαδικασίας και λόγω των εκτεταμένων δικτύων εμπιστοσύνης ο ορισμός του πρωτοκόλλου PGP περιλαμβάνει την ύπαρξη διακομιστών ευρετηρίων καταλόγου με πιστοποιητικά PGP. Στα ευρετήρια αυτά μπορεί ο κάθε χρήστης να έχει πρόσβαση μέσω του πρωτοκόλλου LDAP. Για την ανάκτηση του δημοσίου κλειδιού που σχετίζεται με κάποια ηλεκτρονική διεύθυνση που γνωρίζει. Επίσης, σε αυτά τα ευρετήρια μπορεί κάποιος να στείλει το πιστοποιητικό ανάκλησης που έχει εκδώσει για ταχύτερη κυκλοφορία του.

Συμπεράσματα

Το πρωτόκολλο PGP παρέχει στους χρήστες του μεθόδους για την ψηφιακή υπογραφή ηλεκτρονικών εγγράφων και πιο συγκεκριμένα μηνυμάτων ηλεκτρονικού ταχυδρομείου, καθώς και τη δυνατότητα για την κρυπτογράφηση αυτών. Όλα τα κλειδιά τα οποία μπορεί να χρειαστεί ο χρήστης βρίσκονται συγκεντρωμένα σε ένα πιστοποιητικό το οποίο είναι συνδεδεμένο με μια ή περισσότερες ηλεκτρονικές διευθύνσεις και υπογράφεται από έναν ή περισσότερους άλλους χρήστες οι οποίοι με αυτόν τον τρόπο πιστοποιούν την εμπιστοσύνη τους προς τα στοιχεία του πιστοποιητικού. Παρέχει επίσης τη δυνατότητα για την σωστή και ολοκληρωμένη διαχείριση αυτών των πιστοποιητικών, ίσως όμως όχι για το τεράστιο εύρος του Διαδικτύου.

4.4 ΠΡΟΙΟΝΤΑ ΥΛΟΠΟΙΗΣΗΣ

Προιόντα που υλοποιούν το πρωτόκολλο PGP σήμερα υπάρχουν για όλα τα γνωστά συστήματα, όπως είναι τα Macintos, Windows και Unix's. Υλοποιήσεις κυκλοφορούν και από την NAI την εταιρία που έχει τα δικαιώματα του πρωτοκόλλου PGP αλλά και από άλλους κατασκευαστές λογισμικού που το έχουν ενσωματώσει στα προγράμματα αλληλογραφίας τους όπως είναι τα Microsoft Exchange, Qualcomm Eudora, Novell Groupwise, Lotus Notes, Microsoft Outlook και Mozilla Thunderbird μεταξύ άλλων.

5. S/MIME

5.1 ΙΣΤΟΡΙΑ ΚΑΙ ΑΝΑΠΤΥΞΗ

Οι Γενικές Επεκτάσεις Μηνυμάτων Internet (Multipurpose Internet Mail Extensions) καθορίστηκαν με στόχο να επιτρέψουν τη μετάδοση μέσω ηλεκτρονικού ταχυδρομείου δεδομένων που δεν είναι σε μορφή ASCII. Το MIME δεν αλλάζει το SMTP ή το POP3, ούτε τα αντικαθιστά. Αντίθετα, το MIME επιτρέπει την κωδικοποίηση τυχαίων δεδομένων σε μορφή ASCII, και στη συνέχεια τη μετάδοσή τους σε ένα τυπικό μήνυμα ηλεκτρονική αλληλογραφίας. Για να μπορούν να αντιμετωπιστούν οι τυχαίοι τύποι και αναπαραστάσεις δεδομένων, κάθε μήνυμα MIME περιλαμβάνει πληροφορίες που γνωστοποιούν στον παραλήπτη τον τύπο των δεδομένων και την κωδικοποίηση που χρησιμοποιείται. Οι πληροφορίες MIME βρίσκονται στη κεφαλίδα του μηνύματος αλληλογραφίας. Οι γραμμές της κεφαλίδας καθορίζουν την έκδοση του MIME που χρησιμοποιείται, τον τύπο των δεδομένων που στέλνονται και την κωδικοποίηση που χρησιμοποιείται για τη μετατροπή των δεδομένων σε μορφή ASCII.

Στα μέσα της δεκαετίας του 1990 μια ομάδα εργασίας με επικεφαλής την RSA Security Inc ξεκίνησε την ανάπτυξη ενός πρωτοκόλλου για την μετάδοση ψηφιακά υπογεγραμμένων ή/και κρυπτογραφημένων δεδομένων μέσα σε ψηφιακό φάκελο σύμφωνα με το πρωτόκολλο MIME. Το πρωτόκολλο το οποίο προέκυψε από αυτή την προσπάθεια ονομάστηκε Secure Multipurpose Internet MaiL Extensions (S/MIME). Παρόμοια με τα πρωτόκολλα PEM και MOSS και σε αντίθεση με το PGP το S/MIME είναι ένα πρότυπο και όχι μια εφαρμογή. Το S/MIME σχεδιάστηκε για να επεκτείνει το MIME το οποίο σημαίνει ότι δεν μπορεί να χρησιμοποιηθεί από κάποια εφαρμογή που δεν υποστηρίζει το MIME. Μέχρι τώρα το S/MIME έχει περάσει από τρεις εκδόσεις . Η πρώτη έκδοση ολοκληρώθηκε και παρουσιάστηκε επίσημα το 1995, ενώ η δεύτερη έκδοση ορίστηκε από δύο RFC's τα 2311 και 2312 το 1998. Τον

Ιούνιο του 1999 ανακοινώθηκε η έκδοση 3 με μια ομάδα 5 RFC's, ενώ κατατέθηκε και αίτηση για την αναγνώριση του S/MIME ως πρωτόκολλο της IETF. Η αίτηση αυτή αναμένεται να γίνει αποδεκτή μιας και οι πατέντες που αφορούσαν στους αλγορίθμους κρυπτογράφησης που χρησιμοποιούνται στο S/MIME είτε έχουν λήξει είτε θα λήξουν σύντομα.

5.2 ΠΕΡΙΓΡΑΦΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ

Εισαγωγή

Το S/MIME είναι ένα σύνολο από πρωτόκολλα που συνδυάζουν το MIME με την χρήση ψηφιακών πιστοποιητικών βασισμένων στα X.509. Ο στόχος του είναι να επιτρέψει στους χρήστες να στέλνουν ψηφιακά υπογεγραμμένα, κρυπτογραφημένα ή συγχρόνως ψηφιακά υπογεγραμμένα και κρυπτογραφημένα μηνύματα σε άλλους χρήστες. Αρχικά απαιτείται η έκδοση ενός ή περισσοτέρων πιστοποιητικών από κάποια πιστοποιημένη αρχή. Τέτοιες αρχές είναι για παράδειγμα η Thawte και η Verisign. Ένα ψηφιακό πιστοποιητικό περιέχει πληροφορίες σχετικά με τον ιδιοκτήτη του πιστοποιητικού, την εκδούσα αρχή, την κατάσταση του πιστοποιητικού καθώς και το δημόσιο κλειδί που αντιστοιχεί στο ιδιωτικό κλειδί του κατόχου. Ένα τέτοιο πιστοποιητικό μπορεί να αποκτήσει κάποιος από την Thawte δωρεάν και μέσα σε λίγα λεπτά. Αρχικά αυτό το πιστοποιητικό δεν αναφέρει τα στοιχεία του κατόχου, αλλά μέσα από την διαδικασία του Δικτύου Εμπιστοσύνης της Thawte αναβαθμίζεται σε άλλο που να περιέχει το όνομα του κατόχου.

Αφού αποκτηθεί ένα ψηφιακό πιστοποιητικό αυτό εισάγεται στην εφαρμογή που αξιοποιεί το S/MIME, στην προσωπική κλειδοθήκη του χρήστη. Αυτό το πιστοποιητικό μπορεί να χρησιμοποιηθεί πλέον για να υπογραφούν τα email που θα αποσταλούν. Αρχικά θα πρέπει να αποσταλεί το πιστοποιητικό μαζί με το μήνυμα ώστε ο παραλήπτης να αποκτήσει ένα αντίγραφο. Όταν αυτό το email φτάσει στον προορισμό του, ο παραλήπτης μπορεί να ελέγξει τα στοιχεία του πιστοποιητικού και να συνδέσει το πιστοποιητικό του αποστολέα με τα υπόλοιπα στοιχεία στις επαφές του. Πλέον μπορεί να στέλνει όλα τα email του προς τον αποστολέα κρυπτογραφημένα. Αυτός είναι και ο συνηθέστερος τρόπος για την αποστολή ενός ψηφιακού πιστοποιητικού από τον ένα χρήστη στον άλλο. Πρέπει να γίνει κατανοητό ότι πριν αποκτηθεί το ψηφιακό πιστοποιητικό ενός χρήστη δεν μπορεί να του στείλει ένας άλλος χρήστης κρυπτογραφημένο μήνυμα. Ορισμένες εφαρμογές υποστηρίζουν την ανάκτηση ενός ψηφιακού πιστοποιητικού με χρήση του LDAP και απευθείας εισαγωγή του στα στοιχεία της επαφής.

Τα ψηφιακά πιστοποιητικά X.509 θα τα δούμε εκτενέστερα παρακάτω. Πρέπει όμως εδώ να σημειωθεί ότι λόγω των διαφορών με τα πιστοποιητικά PGP τουλάχιστον προς το παρόν δεν μπορεί να υπάρξει συνεργασία μεταξύ τους.

Υποστηριζόμενοι αλγόριθμοι

Το πρωτόκολλο S/MIME όπως και το PGP χρησιμοποιεί μια πληθώρα αλγορίθμων. Για την δημιουργία συνόψεων ορίζει την χρήση του αλγορίθμου SHA-1, ενώ επιτρέπει και τη χρήση του MD5. Ως αλγορίθμους κρυπτογράφησης ο 40bit-RC2 ορίζεται ως εξ ορισμού, ενώ προτείνεται η υποστήριξη και των DES και 3DES. Αρχικά οι περισσότεροι κατασκευαστές λογισμικού στις διεθνείς εκδόσεις των εφαρμογών τους χρησιμοποιούσαν μόνο των RC2 ενώ μετά την απελευθέρωση εξαγωγής προϊόντων ασφαλείας από τις ΗΠΑ, πλέον υποστηρίζονται όλοι οι αλγόριθμοι. Παρατηρούμε ότι οι αλγόριθμοι που χρησιμοποιεί το S/MIME είναι οι ίδιοι που χρησιμοποιεί και το PGP, ενώ και από τα δύο πρωτόκολλα επιτρέπεται η χρήση και επιπλέον αλγορίθμων επιλογής του χρήστη.

Επεξεργασία μηνύματος

Από τη στιγμή που το S/MIME είναι σχεδιασμένο για να επεκτείνει τις δυνατότητες του MIME συμπεραίνουμε εύκολα ότι το μήνυμα θα επεξεργαστεί με τις ίδιες αρχές που θα το επεξεργαζόταν το MIME. Το προς επεξεργασία μήνυμα προετοιμάζεται σύμφωνα με το πρωτόκολλο MIME, έπειτα προστίθενται η ψηφιακή υπογραφή και η όποια κρυπτογράφηση και το αποτέλεσμα μπαίνει σ' ένα νέο φάκελο του MIME για αποστολή.

Για τη δημιουργία της ψηφιακής υπογραφής το S/MIME απαιτεί την χρήση τουλάχιστον ενός αλγορίθμου για τη δημιουργία σύνοψης απ' αυτούς που αναφέρθηκαν παραπάνω. Από την πλευρά του αποστολέα η διαδικασία εκτελείται σε τέσσερα βήματα:

- πρώτον, ο αποστολέας χρησιμοποιεί έναν αλγόριθμο για να δημιουργήσει μια σύνοψη του μηνύματος
- δεύτερον, η σύνοψη αυτή κρυπτογραφείται χρησιμοποιώντας ένα από τα ιδιωτικά κλειδιά του αποστολέα. Η κρυπτογραφημένη αυτή σύνοψη αντιπροσωπεύει την ψηφιακή υπογραφή
- τρίτον, ο αποστολέας προετοιμάζει ένα μπλοκ πληροφοριών αποστολέα το οποίο περιλαμβάνει το πιστοποιητικό με το δημόσιο κλειδί του αποστολέα, ένα αναγνωριστικό του αλγορίθμου δημιουργίας σύνοψης, ένα αναγνωριστικό του αλγορίθμου κρυπτογράφησης και την κρυπτογραφημένη σύνοψη
- τέταρτον, το αρχικό μήνυμα και το μπλοκ πληροφοριών συνενώνονται για να δημιουργήσουν ένα αντικείμενο MIME τύπου signed-data (υπογεγραμμένα δεδομένα).

Το αντικείμενο MIME μπορεί πλέον να αποσταλεί στον παραλήπτη ο οποίος για να επιβεβαιώσει την ψηφιακή υπογραφή πρέπει:

- αρχικά να αποκρυπτογραφήσει την ψηφιακή υπογραφή χρησιμοποιώντας το κατάλληλο κλειδί και αλγόριθμο που μπορεί να βρει στο μπλοκ πληροφοριών για να αποκτήσει ένα αντίγραφο της σύνοψης του μηνύματος
- έπειτα να δημιουργήσει χρησιμοποιώντας τον ίδιο αλγοριθμο δημιουργίας

σύνοψης που αναφέρεται στο μπλοκ πληροφοριών ένα δεύτερο αντίγραφο της σύνοψης του μηνύματος

Συγκρίνοντας τις δύο συνόψεις, εφόσον αυτές είναι ίδιες μεταξύ τους επιβεβαιώνει την ψηφιακή υπογραφή και αποδέχεται το μήνυμα ως αυθεντικό.

Για να θεωρηθεί το ψηφιακό πιστοποιητικό ως γνήσιο θα πρέπει να υπάρχει έγκυρη αλυσίδα πιστοποιητικών από το πιστοποιητικό-ρίζα μέχρι το πιστοποιητικό που έχει λάβει.

Για την κρυπτογράφηση του περιεχομένου ενός μηνύματος το S/MIME ορίζει ότι αυτό πρέπει πρώτα να τοποθετηθεί σ' έναν ψηφιακό φάκελο, όπως αυτός ορίζεται στο MIME, και έπειτα αυτός ο φάκελος να κρυπτογραφηθεί το περιεχόμενό του με τα παρακάτω πέντε βήματα:

- πρώτον, ο αποστολέας παράγει ένα τυχαίο κλειδί κατάλληλο για χρήση με τον αλγόριθμο κωδικοποίησης που προτιμά
- δεύτερον, κρυπτογραφεί τον ψηφιακό φάκελο με αυτόν τον αλγόριθμο και το κλειδί
- τρίτον, για κάθε ένα παραλήπτη ο αποστολέας κρυπτογραφεί το τυχαίο κλειδί χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη
- τέταρτον, για κάθε ένα παραλήπτη ο αποστολέας ετοιμάζει ένα μπλοκ πληροφοριών παραλήπτη το οποίο περιλαμβάνει το δημόσιο κλειδί του αποστολέα, ένα αναγνωριστικό του αλγορίθμου κωδικοποίησης του τυχαίου κλειδιού και το κρυπτογραφημένο κλειδί
- πέμπτον, για κάθε ένα παραλήπτη ο κρυπτογραφημένος ψηφιακός φάκελος και το μπλοκ πληροφοριών παραλήπτη συνενώνονται για να δημιουργήσουν ένα νέο αντικείμενο MIME του τύπου enveloped-data (ενθυλακωμένα δεδομένα).Επιπλέον, ένας ακόμη κρυπτογραφημένος ψηφιακός φάκελος πρέπει να δημιουργηθεί και για τον αποστολέα , ώστε να μπορεί να ανακτήσει το μήνυμα.

Όταν ο ψηφιακός φάκελος φτάσει στους παραλήπτες, ο καθένας από αυτούς, αφού αποκρυπτογραφήσει το τυχαίο κλειδί από το μπλοκ πληροφοριών που έχει λάβει χρησιμοποιώντας το ιδιωτικό του κλειδί μπορεί να το χρησιμοποιήσει για την αποκρυπτογράφηση του αρχικού μηνύματος.

Κρυπτογραφικά κλειδιά

Παρόμοια με το PGP το S/MIME χρησιμοποιεί και αυτό ένα μεγάλο αριθμό κρυπτογραφικών κλειδιών τα οποία ο χρήστης πρέπει να μπορεί να διαχειριστεί. Το S/MIME ορίζει και αυτό μεθόδους για την σωστή διαχείριση των κλειδιών και των πιστοποιητικών, τις οποίες θα εκθέσουμε παρακάτω.

5.3 ΥΠΟΔΟΜΗ ΔΙΑΧΕΙΡΙΣΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

Ήδη στο προηγούμενο κεφάλαιο παρουσιάσαμε την ιδέα ύπαρξης ψηφιακών πιστοποιητικών που περιλαμβάνουν πληροφορίες συσχετισμού ενός ανθρώπου, της ψηφιακής του ταυτότητας και του δημοσίου από ένα ζεύγος δημοσίου και ιδιωτικού κλειδιού. Τέτοια πιστοποιητικά είναι τα πιστοποιητικά PGP τα οποία ήδη μελετήσαμε, αλλά και τα πιστοποιητικά X.509 τα οποία χρησιμοποιεί το S/MIME. Τα πιστοποιητικά X.509 βρίσκονται πλέον στην τρίτη έκδοσή τους, η οποία σε σχέση με την αρχική περιλαμβάνει και ένα πλήθος επεκτάσεων. Ένα πιστοποιητικό περιλαμβάνει τα παρακάτω πεδία:

- version: ένας ακέραιος αριθμός που αναφέρεται στην έκδοση του πιστοποιητικού X.509 με την οποία συμμορφώνεται το παρόν πιστοποιητικό. Σημειωτέον ότι, ο ακέραιος αριθμός είναι κατά 1 μικρότερος από την πραγματική έκδοση, καθώς η αρίθμηση ξεκινά από το 0.
- serialNumber: στο πεδίο αυτό υπάρχει ένας σειριακός αριθμός μοναδικός για κάθε πιστοποιητικό ανά εκδότρια αρχή.
- signature: περιέχει ένα αναγνωριστικό αλγορίθμου που περιγράφει τον αλγόριθμο που χρησιμοποιήθηκε από την εκδότρια αρχή για να υπογράψει το πιστοποιητικό (OID)
- issuer: χρησιμοποιείται για να κωδικοποιήσει ένα διακεκριμένο όνομα κατά το πρωτόκολλο X.500 (DN) του εκδότη του πιστοποιητικού
- validity:στο πεδίο αυτό αναφέρονται ο χρόνος έναρξης και λήξης ισχύος του πιστοποιητικού
- subject: περιλαμβάνει το κατά X.500 διακεκριμένο όνομα του ιδιοκτήτη του πιστοποιητικού
- subjectPublicKeyInfo: στο πεδίο αυτό περιλαμβάνεται το δημόσιο κλειδί το οποίο πιστοποιείται και ένα αναγνωριστικό του αλγορίθμου με τον οποίο χρησιμοποιείται αυτό το κλειδί
- issuerUniqueID: προαιρετικό πεδίο για να συμπεριληφθούν επιπλέον πληροφορίες σχετικά με τον εκδότη του πιστοποιητικού
- subjectUniqueID: προαιρετικό πεδίο για να συμπεριληφθούν επιπλέον πληροφορίες σχετικά με τον ιδιοκτήτη του πιστοποιητικού
- extensions: προαιρετικό πεδίο που ορίζεται στην έκδοση 3 για την κωδικοποίηση επιπλέον πληροφοριών σχετικά με την ιδιοκτησία του πιστοποιητικού τα δημόσια κλειδιά και τον τρόπο διαχείρισης του πιστοποιητικού. Ο κάθε χρήστης μπορεί να ορίσει τις δικές του μεταβλητές. Η αρχή ISO έχει προτείνει μια πρότυπη ομάδα μεταβλητών που μπορεί ,αν κάποιος θέλει, να ακολουθήσει.

Παρ' ότι το πρωτόκολλο X.509 καθορίζει αυτές τις μεταβλητές, το περιεχόμενό τους είναι σχετικά ασαφές και δεκτικό άπειρων προσθηκών. Συνεπώς, κάθε ομάδα ανθρώπων ή οργανισμός που έχει προσπαθήσει ως τώρα να χρησιμοποιήσει τα

πιστοποιητικά X.509 έχει δημιουργήσει το δικό του προφίλ. Δυστυχώς, έως τώρα δεν έχει υπάρξει κάποιος τρόπος καθορισμού του προφίλ που χρησιμοποιείται, οπότε είναι δύσκολο για τον ιδιοκτήτη κάποιου πιστοποιητικού να γνωρίζει πως ακριβώς θα αξιοποιηθεί το πιστοποιητικό του. Το πρωτόκολλο S/MIME απαιτεί στο πεδίο subjectAltName να περιέχεται η διεύθυνση ηλεκτρονικού ταχυδρομείου του ιδιοκτήτη του πιστοποιητικού.

Θεμελίωση εμπιστοσύνης

Στο προηγούμενο κεφάλαιο μελετήσαμε τον τρόπο με τον οποίο κάποιος μπορεί να θεμελιώσει εμπιστοσύνη στο πρωτόκολλο PGP. Είδαμε ότι για να εμπιστευθούμε ένα πιστοποιητικό PGP πρέπει να είναι υπογεγραμμένο από κάποιον που εμπιστευόμαστε απόλυτα ή από τουλάχιστον δύο που εμπιστευόμαστε οριακά. Η θεμελίωση εμπιστοσύνης στο πρωτόκολλο S/MIME λειτουργεί διαφορετικά.

Εμπιστευόμαστε και θεωρούμε έγκυρο ένα πιστοποιητικό εφόσον υπάρχει μια έγκυρη αλυσίδα πιστοποιητικών μέχρι ένα πιστοποιητικό ρίζας κάποιου τον οποίο εμπιστευόμαστε απόλυτα. Επομένως, μπορούμε να θεωρήσουμε ότι το μοντέλο εμπιστοσύνης των πιστοποιητικών X.509 που χρησιμοποιεί το S/MIME είναι ιεραρχικό. Η υποκείμενη ιεραρχία εμπιστοσύνης μπορεί φαίνεται με δύο τρόπους, εντός ή εκτός πλαισίου.

Όταν η εμπιστοσύνη παρουσιάζεται εντός πλαισίου η αλυσίδα πιστοποιητικών και τα σχετικά ενδιάμεσα πιστοποιητικά περιλαμβάνονται ως τμήμα του μηνύματος το οποίο είναι ψηφιακά υπογεγραμμένο. Συνεπώς η εφαρμογή αποστολής ηλεκτρονικού ταχυδρομείου πρέπει να συμπεριλάβει τις πληροφορίες για τα σχετικά πιστοποιητικά μέσα στο μήνυμα και τα σχετικά πιστοποιητικά με τη σειρά τους πρέπει να περιλαμβάνουν πληροφορίες για όλα τα υπόλοιπα πιστοποιητικά που αποτελούν μέρος της αλυσίδας. Το πλεονέκτημα αυτής της μεθόδου είναι ότι παρέχονται στον παραλήπτη όλες οι απαραίτητες πληροφορίες για να επιβεβαιώσει την εγκυρότητα ενός πιστοποιητικού που λαμβάνει. Το μειονέκτημα είναι ότι σε κάθε μήνυμα που αποστέλλεται περιλαμβάνεται ένας αριθμός από πιστοποιητικά τα οποία καταλαμβάνουν αρκετό χώρο. Αυτό δυσκολεύει τη μετάδοση των μηνυμάτων, αλλά και την αποθήκευσή τους.

Όταν η εμπιστοσύνη παρουσιάζεται εκτός πλαισίου, αντί να αποστέλλεται ολόκληρη η αλυσίδα πιστοποιητικών, στο μήνυμα περιλαμβάνεται μόνο το πιστοποιητικό του αποστολέα και δίνονται πληροφορίες για το που μπορεί να βρει ο παραλήπτης τα ενδιάμεσα πιστοποιητικά της αλυσίδας. Με αυτή τη μέθοδο ο παραλήπτης πρέπει να έχει έναν τρόπο ανάκτησης πιστοποιητικών ώστε να αποκτήσει πρόσβαση στα απαραίτητα πιστοποιητικά.

Η απόφαση για το ποια από τις δύο μεθόδους προτιμά να χρησιμοποιήσει ένας χρήστης εξαρτάται από διάφορες παραμέτρους, όπως είναι το πλήθος των παραληπτών ενός μηνύματος, η συχνότητα επικοινωνίας και η ταχύτητα επικοινωνίας. Σε γενικές γραμμές, όταν το πλήθος των παραληπτών είναι μικρό, η επιβάρυνση που προκαλεί η πρώτη μέθοδος δεν είναι τόσο σημαντική, όσο τα οφέλη που αποκομίζει ο χρήστης. Ενώ αντίθετα, όταν το πλήθος των παραληπτών αυξάνει

συνήθως είναι προτιμότερο να χρησιμοποιείται η δεύτερη μέθοδος.

Ανάκληση πιστοποιητικού

Με τον όρο ανάκληση πιστοποιητικού αναφερόμαστε στη διαδικασία με την οποία ένας χρήστης ανακοινώνει δημόσια ότι ένα πιστοποιητικό δεν είναι πλέον έγκυρο και δεν θα πρέπει πλέον να χρησιμοποιείται. Στην πράξη υπάρχουν διάφοροι λόγοι που μπορούν να οδηγήσουν στην ανάκληση ενός πιστοποιητικού, όπως για παράδειγμα ότι το ιδιωτικό κλειδί του χρήστη ή της εκδότριας αρχής έχει υποκλαπεί ή ότι ο χρήστης έχει πάψει να πιστοποιείται πλέον από τη συγκεκριμένη εκδότρια αρχή.

Σε γενικές γραμμές, η έκδοση αλλά και η ανάκληση ενός πιστοποιητικού αφορά τρία μέρη, την εκδότρια αρχή του πιστοποιητικού, τους χρήστες του πιστοποιητικού αλλά και το όποιο ή όποια ευρετήρια το συμπεριλαμβάνουν. Συνήθως η εκδότρια αρχή δεν παρέχει άμεσες πληροφορίες σχετικά με την κατάσταση ενός πιστοποιητικού προς τους χρήστες, αλλά μπορεί να ενημερώνει περιοδικά τα ευρετήρια παροχής πιστοποιητικών. Αυτά όμως είναι διαρκώς προσβάσιμα σε όλους τους χρήστες άρα υπάρχει ο κίνδυνος η πληροφορίες που παρέχουν σχετικά με την εγκυρότητα ενός πιστοποιητικού να μην είναι ενήμερες. Επειδή η εμπιστοσύνη προς την εκδότρια αρχή είναι μεγαλύτερη απ' ότι προς ένα ευρετήριο δημιουργείται ένα σύνθετο πρόβλημα όσον αφορά τους χρήστες που δεν θέλουν απλά να ανακτήσουν ένα πιστοποιητικό, αλλά χρειάζονται και κάποιου είδους πληροφόρηση σχετικά με την εγκυρότητά του.

Υπάρχουν τέσσερις προσεγγίσεις για την αντιμετώπιση αυτού του προβλήματος:

- η πρώτη προσέγγιση είναι τα πιστοποιητικά να έχουν σύντομο χρόνο λήξης και να πρέπει να έχουν περιοδική ανανέωση
- η δεύτερη προσέγγιση είναι να υπάρχει μια λίστα όλων των μη ανακληθέντων πιστοποιητικών σε ένα διαρκώς προσβάσιμο ευρετήριο και οι χρήστες να αποδέχονται μόνο τα πιστοποιητικά που βρίσκονται εκεί
- η τρίτη προσέγγιση είναι να κυκλοφορούν περιοδικά οι εκδότριες αρχές λίστες των πιστοποιητικών που έχουν ανακληθεί και δεν πρέπει πλέον να χρησιμοποιούνται
- η τέταρτη προσέγγιση είναι να παρέχεται ένας μηχανισμός ελέγχου εγκυρότητας πιστοποιητικών ο οποίος θα ενημερώνει τους χρήστες αν ένα συγκεκριμένο πιστοποιητικό είναι ακόμη σε ισχύ ή έχει ανακληθεί.

Οι τέσσερις αυτές προσεγγίσεις δεν είναι αμοιβαία αποκλειόμενες, αλλά μπορούν να συνδυαστούν για τη δημιουργία ενός αποτελεσματικότερου μηχανισμού ανάκλησης πιστοποιητικών..Στην πράξη σήμερα εφαρμόζονται η τρίτη και η τέταρτη προσέγγιση. Ένας χρήστης που ενδιαφέρεται να ελέγξει την εγκυρότητα ενός πιστοποιητικού πρώτα το αναζητά στην κατάλληλη λίστα ανακληθέντων πιστοποιητικών και εφόσον δεν το βρει εκεί το αναζητά σε ένα ευρετήριο που έχει δημιουργήσει γι' αυτό το σκοπό η IETF PKIX WG το οποίο ονομάζεται Online Certficate Status Protocol (OCSP) πριν αποφασίσει για την εγκυρότητά του.

Παροχείς πιστοποιητικών

Υπάρχει ένα μεγάλο πλήθος εταιριών οι οποίες παρέχουν υπηρεσίες και προϊόντα εκδότριας αρχής για το S/MIME. Τέτοιες εταιρίες είναι για παράδειγμα η Verisign και η Entrust στις ΗΠΑ και η Swisskey στην Ελβετία. Πολλές από αυτές τις εταιρίες έχουν τα πιστοποιητικά-ρίζες τους προεγκατεστημένα σε εμπορικά προϊόντα πλοήγησης διαδικτύου, αλλά και εφαρμογές ηλεκτρονικού ταχυδρομείου. Η εξασφάλιση ενός πιστοποιητικού από μία από αυτές τις εταιρίες μπορεί να κοστίζει από ελάχιστα μέχρι αρκετές εκατοντάδες Ευρώ το χρόνο.

Συμπεράσματα

Το πρωτόκολλο S/MIME όπως το PGP δίνει τη δυνατότητα στους χρήστες του να ανταλλάσσουν μηνύματα ηλεκτρονικού ταχυδρομείο τα οποία περιλαμβάνουν ψηφιακές υπογραφές ή/και είναι κρυπτογραφημένα. Παρέχει επίσης όλα τα εργαλεία που χρειάζεται ένας χρήστης για να διαχειριστεί τα απαραίτητα πιστοποιητικά, αλλά και να ελέγχει ανά πάσα στιγμή την εγκυρότητα αυτών. Ο τρόπος με τον οποίο διαχειρίζεται αυτά τα πιστοποιητικά δίνει τη δυνατότητα το σύνολο των πιστοποιητικών και ο φόρτος εργασίας για τη διαχείρισή τους να είναι κατανεμημένος σ' ένα πλήθος από εκδότριες αρχές. Είναι ,λοιπόν, ιδανικό για χρήση στο Διαδίκτυο το οποίο είναι τόσο εκτενές. Μειονέκτημά του μπορεί να θεωρηθεί το γεγονός ότι οι περισσότερες από τις διεθνώς αναγνωρισμένες εκδότριες αρχές που υπάρχουν σήμερα είναι ιδιωτικές εταιρίες, οι οποίες χρεώνουν την έκδοση ενός πιστοποιητικού πολλές φορές με υπέρογκα ποσά.

5.4 ΠΡΟΪΟΝΤΑ ΥΛΟΠΟΙΗΣΗΣ

Όπως έχουμε ήδη αναφέρει, η υλοποίηση του πρωτοκόλλου S/MIME μπορεί να διαφέρει από κατασκευαστή σε κατασκευαστή. Κάποιες από τις υλοποιήσεις προσφέρουν επιπλέον δυνατότητες με τη χρήση του S/MIME, όπως για παράδειγμα η ψηφιακά υπογεγραμμένη απόδειξη παραλαβής. Γίνεται αμέσως αντιληπτό ότι η δυνατότητα συνεργασίας μεταξύ προϊόντων που υλοποιούν το πρωτόκολλο είναι ένα διαρκώς αυξανόμενο πρόβλημα. Στο εμπόριο κυκλοφορούν ένα μεγάλο πλήθος εφαρμογών ηλεκτρονικού ταχυδομείου που ενσωματώνουν τη δυνατότητα χρήσης του S/MIME, όπως για παράδειγμα το Mozilla Thundrbird και το Microsoft Outlook 2007, ενώ υπάρχουν ένα πλήθος επεκτάσεων για να προστεθεί η δυνατότητα αλληλογραφίας με το S/MIME ακόμη και για παλιότερες εφαρμογές, όπως το TrustedMIME της Siemens για το Microsoft Outlook 2000.

6. ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ

6.1 ΧΡΗΣΕΙΣ ΤΩΝ ΨΗΦΙΑΚΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

Τα ψηφιακά πιστοποιητικά χρησιμοποιούνται από τις δικτυακές οντότητες για να πετύχουμε την Εμπιστευτικότητα και την Ακεραιότητα των δεδομένων, την Πιστοποίηση της ταυτότητας της οντότητας και την Μη Άρνηση Αποδοχής της αποστολής δεδομένων.

Εμπιστευτικότητα

Ως εμπιστευτικότητα ορίζεται η προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη πρόσβαση ή γνωστοποίηση τους. Η υπηρεσία αυτή υλοποιείται μέσω μηχανισμών ελέγχου πρόσβασης στην περίπτωση αποθήκευσης δεδομένων και μέσω κωδικοποίησης κατά την αποστολή δεδομένων. Η Υποδομή Δημοσίου Κλειδιού παρέχει κωδικοποίηση, αφού οι μηχανισμοί ελέγχου πρόσβασης υλοποιούνται κατά βάση από τον συνδυασμό μεθόδων πιστοποίησης (authentication) και εξουσιοδότησης (authorization).

Η εμπιστευτικότητα μπορεί να παρομοιασθεί με έναν αδιαφανή φάκελο. Το μήνυμα που περιλαμβάνει δεν είναι ορατό χωρίς να ανοίξει ο φάκελος. Φυσικά, ο φάκελος μπορεί να ανοιχθεί από τον οποιονδήποτε και να παραβιασθεί το απόρρητο της αλληλογραφίας. Η κρυπτογραφία είναι ένας απολύτως ασφαλής φάκελος που πολύ δύσκολα, σχεδόν ακατόρθωτα, είναι εφικτό να ανοιχτεί από οποιονδήποτε άλλον εκτός από τον νόμιμο παραλήπτη.

Πιστοποίηση

Πιστοποίηση είναι η επιβεβαίωση της ταυτότητας ενός ατόμου ή η επιβεβαίωση της

πηγής αποστολής των πληροφοριών. Δηλαδή, το άτομο που επιθυμεί να επιβεβαιώσει την ταυτότητά ενός άλλου ατόμου ή κάποιου εξυπηρετητή με το οποίο επικοινωνεί, βασίζεται στην πιστοποίηση.

Η πιστοποίησης μπορεί να υλοποιηθεί με τρεις βασικές μεθόδους:

- Κάτι που γνωρίζουμε, π.χ. το PIN μιας τραπεζικής κάρτας ή το μυστικό κωδικό ενός λογαριασμού (password).
- Κάτι που έχουμε στην ιδιοκτησία μας, π.χ. το κλειδί μιας πόρτας ή μια τραπεζική κάρτα.
- Κάτι που έχουμε εκ γενετής, π.χ. δακτυλικά αποτυπώματα, φωνή κτλ.

Η Πιστοποίηση, πιο απλά, είναι ο τρόπος με τον οποίο δημοσιεύονται οι τιμές των δημόσιων κλειδιών και η πληροφορία που αντιστοιχεί στις τιμές αυτές. Ένα πιστοποιητικό (certificate) είναι ο τρόπος με τον οποίο η Υποδομή Δημοσίου Κλειδιού μεταδίδει τις τιμές των δημόσιων κλειδιών, ή πληροφορία που σχετίζεται με αυτά, ή και τα δύο. Γενικά, ένα πιστοποιητικό είναι μία συλλογή πληροφοριών που έχει υπογραφεί ψηφιακά από την οντότητα που το εκδίδει. Τα πιστοποιητικά αυτά χαρακτηρίζονται από το είδος της πληροφορίας που περιέχουν. Η εκδότρια αρχή των πιστοποιητικών ονομάζεται Αρχή Πιστοποίησης (Certificate Authority - CA).

Ακεραιότητα

Ακεραιότητα (Integrity) είναι η προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη τροποποίηση ή αντικατάσταση τους. Η υπηρεσία αυτή παρέχεται από μηχανισμούς κρυπτογραφίας όπως είναι οι ψηφιακές υπογραφές.

Ας εξετάσουμε την ακεραιότητα ενός διαφανούς φακέλου. Το μήνυμα που περιέχει ο φάκελος μπορεί να διαβαστεί από τον οποιονδήποτε, οπότε και παραβιάζεται η εμπιστευτικότητα, όπως αυτή ορίστηκε παραπάνω. Ο φάκελος θεωρείται ενδεικτικό στοιχείο παραβίασης. Ο παραλήπτης βλέποντας τον φάκελο είναι σε θέση να επιβεβαιώσει ότι ο φάκελος δεν έχει ανοιχθεί ή παραβιαστεί.

Μη Άρνηση Αποδοχής

Η Μη Άρνηση Αποδοχής (Non-Repudiation) συνδυάζει τις υπηρεσίες της πιστοποίησης και της ακεραιότητας που παρέχονται σε μια τρίτη οντότητα. Έτσι, ο αποστολέας δεδομένων δεν μπορεί να αρνηθεί την δημιουργία και αποστολή του μηνύματος. Η ασύμμετρη κρυπτογραφία παρέχει ψηφιακές υπογραφές, τέτοιες ώστε μόνο ο αποστολέας του μηνύματος θα μπορούσε να κατέχει την συγκεκριμένη ψηφιακή υπογραφή, πρόκειται δηλαδή για μια αμφιμονοσήμαντη σχέση. Με αυτόν τον τρόπο, ο οποιοσδήποτε, και φυσικά και ο παραλήπτης του ψηφιακά υπογεγραμμένου μηνύματος μπορεί να επιβεβαιώσει την ψηφιακή υπογραφή του αποστολέα.

6.2 ΧΡΗΣΗ ΤΩΝ ΨΗΦΙΑΚΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΑΠΟ ΔΙΑΚΟΜΙΣΤΕΣ

Τα ψηφιακά πιστοποιητικά χρησιμοποιούνται από τους διακομιστές για την επιβεβαίωση της ταυτότητας του διακομιστή στον πελάτη, την εμπιστευτικότητα της επικοινωνίας και την ακεραιότητα των δεδομένων που αποστέλλονται στο πελάτη.

Χρήση των ψηφιακών πιστοποιητικών στην υπηρεσία παγκόσμιου ηλεκτρονικού ιστού

Θα περιγραφεί η δημιουργία ενός ασφαλούς διακομιστή της υπηρεσίας παγκόσμιου ηλεκτρονικού ιστού με τη χρήση του λογισμικού Apache HTTP Server και της επέκτασης του mod_ssl σε λειτουργικό σύστημα Unix. Η επέκταση mod_ssl παρέχει της υπηρεσίες της βιβλιοθήκης OpenSSL. Τα παραδείγματα υποθέτουν την εγκατάσταση του λογισμικού OpenSSL στο φάκελο `/etc/ssl` και την εγκατάσταση των ρυθμίσεων του διακομιστή Apache στο φάκελο `/etc/httpd`.

Δημιουργία κλειδιών και έκδοση πιστοποιητικού

Για τη έκδοση ενός πιστοποιητικού για το διακομιστή πρέπει να ακολουθηθούν τα παρακάτω βήματα:

- Δημιουργία και ασφαλή αποθήκευση ενός μυστικού κλειδιού και του αντίστοιχου δημόσιου κλειδιού.
- Δημιουργία αίτησης για έκδοση πιστοποιητικού βασισμένης στο δημόσιο κλειδί.
- Αποστολή της αίτησης στην αρχή πιστοποίησης.
- Έκδοση του ψηφιακού πιστοποιητικού από την αρχή πιστοποίησης.

Δημιουργία κλειδιού

Πρέπει να είστε διαχειριστής του συστήματος για να δημιουργήσετε κλειδί.

Διαγράψτε τα κλειδιά και πιστοποιητικά που πιθανόν να υπάρχουν ήδη στο σύστημα. Προσοχή μην διαγράψετε κλειδιά που τα χρειάζεστε.

```
rm /etc/httpd/conf/ssl.key/server.key
```

```
rm /etc/httpd/conf/ssl.crt/server.crt
```

Στο φάκελο

```
/usr/share/ssl/certs
```

εκτελέστε

```
/usr/bin/openssl genrsa -des3 1024 >
/etc/httpd/conf/ssl.key/server.key.
```

Όταν δημιουργηθεί το κλειδί θα σας ζητηθεί ο μυστικός κωδικός για την ασφαλή αποθήκευση του. Ο μυστικός κωδικός θα πρέπει να εισάγεται κάθε φορά που χρησιμοποιείται το κλειδί. Το κλειδί αποθηκεύεται στο αρχείο

`/etc/httpd/conf/ssl.key/server.key.`

Δημιουργία αίτησης για έκδοση πιστοποιητικού

Για τη δημιουργία της αίτησης εκτελέστε

`/usr/bin/openssl -req -new -key /etc/httpd/conf/ssl.key/server.key -out /etc/httpd/conf/ssl.csr/server.csr.`

Θα σας ζητηθεί ο μυστικός κωδικός για το κλειδί και οι πληροφορίες που θα αποτελούν το Διακεκριμένο Όνομα του πιστοποιητικού σας. Ένα τμήμα του διακεκριμένου ονόματος μπορεί να απαιτείται από την αρχή πιστοποίησης να είναι συγκεκριμένο. Για παράδειγμα το όνομα χώρας και ο οργανισμός να πρέπει να είναι

`o=Alexandreio University of Thessaloniki, c=GR.`

Το σημαντικότερο στοιχείο είναι το Κοινό Όνομα (cn) το οποίο ελέγχεται από τους πελάτες κατά την εξακρίβωση των στοιχείων του πιστοποιητικού και πρέπει να είναι ίδιο με το όνομα του διακομιστή π.χ. www.teithe.gr.

Η αίτηση για την έκδοση του πιστοποιητικού βρίσκεται στο αρχείο

`/etc/httpd/conf/ssl.csr/server.csr`

και είναι σε μορφή PEM, δηλαδή κείμενο.

Αποστολή της αίτησης και έκδοση πιστοποιητικού

Η αίτηση πρέπει να αποσταλεί στην αρχή πιστοποίησης σύμφωνα με τις διαδικασίες που έχει ορίσει. Συνήθεις τρόποι αποστολής είναι μέσω ηλεκτρονικού ταχυδρομείου ή υποβολή της από μια ιστοσελίδα. Η αρχή πιστοποίησης θα εξακριβώσει τα στοιχεία του διακομιστεί σύμφωνα με τη πολιτική πιστοποίησης της και θα εκδώσει το πιστοποιητικό. Το πιστοποιητικό σε μορφή PEM θα πρέπει να εγκατασταθεί στο αρχείο

`/etc/httpd/conf/ssl.crt/server.crt.`

Τα πιστοποιητικά της ιεραρχίας πιστοποίησης θα πρέπει να αποθηκευθούν σε μορφή PEM, το ένα μετά το άλλο, στο αρχείο

`/etc/httpd/conf/ssl.crt/ca.crt.`

Εργασίες με πιστοποιητικά

Διαχείριση της συνθηματικής φράσης (pass-phrase) στο ιδιωτικό κλειδί

Η αλλαγή της συνθηματικής φράσης στο ιδιωτικό κλειδί πραγματοποιείται σε δύο στάδια. Πρώτα διαβάζεται το κλειδί με την παλαιά συνθηματική φράση και στη συνέχεια γράφεται με τη χρήση μιας νέας. Οι εντολές που απαιτούνται είναι οι παρακάτω:

`# openssl rsa -des3 -in server.key -out server.key.new<Enter>`

`# mv server.key.new server.key<Enter>`

Η διαγραφή της κρυπτογράφησης του ιδιωτικού κλειδιού RSA γίνεται κατά παρόμοιο

τρόπο. Ακολουθούν οι αντίστοιχες εντολές::

```
# cp server.key server.key.org<Enter>
```

```
# openssl rsa -in server.key.org -out server.key<Enter>
```

Απαραίτητη είναι η εξασφάλιση ότι το αρχείο `server.key` είναι αναγνώσιμο μόνο από τον χρήστη `root`:

```
# chmod 400 server.key <Enter>
```

Τώρα το αρχείο `server.key` περιέχει ένα μή κρυπτογραφημένο αντίγραφο του ιδιωτικού κλειδιού RSA, γεγονός ιδιαίτερα επικίνδυνο για τη περίπτωση κατά την οποία το κλειδί βρεθεί σε λάθος χέρια.

Μετατροπή του τύπου ενός πιστοποιητικού από PEM σε DER

Ο προκαθορισμένος τύπος πιστοποιητικών για το λογισμικό SSLeay/OpenSSL είναι ο τύπος PEM, ο οποίος στην πραγματικότητα αποτελεί μια κωδικοποίηση της μορφής Base64 του τύπου DER μαζί με γραμμές κεφαλίδων και υποσέλιδων (header και footer). Για κάποιες εφαρμογές όπως είναι ο Microsoft Internet Explorer απαιτείται το πιστοποιητικό να είναι τύπου DER. Η μετατροπή ενός αρχείου τύπου PEM με όνομα `cert.pem` στο αντίστοιχο αρχείο `cert.der` τύπου DER επιτυγχάνεται με την παρακάτω εντολή:

```
# openssl x509 -in cert.pem -out cert.der -outform DER <Enter>
```

Επαλήθευση της συσχέτισης ενός ιδιωτικού κλειδιού με το πιστοποιητικό του

Το ιδιωτικό κλειδί αποτελείται από μία σειρά αριθμών. Δύο από αυτούς τους αριθμούς συνθέτουν το δημόσιο κλειδί ενώ οι υπόλοιποι αριθμοί είναι μέρος του ιδιωτικού κλειδιού. Τα στοιχεία του δημόσιου κλειδιού έχουν επίσης ενσωματωθεί στο πιστοποιητικό (το οποίο ελήφθη από την CSR). Για να ελέγξει κάποιος αν το δημόσιο κλειδί (το οποίο βρίσκεται μέσα στο πιστοποιητικό) ταυτίζεται με το δημόσιο τμημα του ιδιωτικού κλειδιού, πρέπει να εξετάσει τόσο το πιστοποιητικό όσο και το κλειδί. Αυτό επιτυγχάνεται με τις παρακάτω εντολές:

```
# openssl x509 -noout -text -in server.crt<Enter>
```

```
# openssl rsa -noout -text -in server.key <Enter>
```

Τα προαναφερθέντα τμήματα του κλειδιού και του πιστοποιητικού, γνωστά με τους όρους «modulus» και «public exponent» αντίστοιχα, πρέπει να ταυτίζονται. Επειδή όμως τα τμήματα αυτά είναι συνήθως 65537 και είναι ιδιαίτερα κουραστικό να ελέγχονται τόσο μεγάλοι αριθμοί, μπορεί κάποιος να ακολουθήσει την παρακάτω προσέγγιση δίνοντας τις ακόλουθες εντολές:

```
# openssl x509 -noout -modulus -in server.crt | openssl md5<Enter>
```

```
# openssl rsa -noout -modulus -in server.key | openssl md5<Enter>
```

και στη συνέχεια να συγκρίνει πραγματικά μικρότερους αριθμούς. Σχεδόν σίγουρα τα αποτελέσματα θα διαφέρουν αν τα κλειδιά δεν συσχετίζονται πλήρως μεταξύ τους. Τέλος, εάν κάποιος επιθυμεί να ελέγξει ποιο κλειδί ή πιστοποιητικό ανήκει σε μια συγκεκριμένη CSR το πραγματοποιεί με την εντολή:

```
# openssl req -noout -modulus -in server.csr | openssl md5 <Enter>
```

Ρύθμιση της διαμόρφωσης του διακομιστή

Για τη ρύθμιση της διαμόρφωσης του διακομιστή θα χρησιμοποιήσουμε το αρχείο `/etc/httpd/conf.d/ssl.conf` το οποίο θα πρέπει να περιλαμβάνετε από το αρχείο ρυθμίσεων του διακομιστή `/etc/httpd/conf/httpd.conf` με την εντολή

`#include conf.d/ssl.conf.`

```
LoadModule ssl_module modules/mod_ssl.so
Listen 443

AddType application/x-x509-ca-cert .crt
AddType application/x-pkcs7-crl    .crl

SSLPassPhraseDialog  builtin
SSLSessionCache         dbm:/var/cache/mod_ssl/scache
SSLSessionCacheTimeout  300
SSLMutex  file:logs/ssl_mutex
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin

<VirtualHost _default_:443>

DocumentRoot "/var/www/html"
ServerName new.host.name:443
ServerAdmin you@your.address
ErrorLog logs/ssl_error_log
TransferLog logs/ssl_access_log

SSLEngine on

SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:
+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL

SSLCertificateFile /etc/httpd/conf/ssl.crt/server.crt
SSLCertificateKeyFile
/etc/httpd/conf/ssl.key/server.key
```

Ενδεικτικό αρχείο `/etc/httpd/conf.d/ssl.conf` ρυθμίσεων του διακομιστή.

Πιστοποίηση ταυτότητας πελάτη με χρήση πιστοποιητικών

Για την πιστοποίηση της ταυτότητας του πελάτη, σε συγκεκριμένες σελίδες του διακομιστή, πρέπει να συμπεριλάβουμε την ακόλουθη διαμόρφωση στις ρυθμίσεις του διακομιστή:

```
SSLVerifyClient      none
```

```
<Directory /usr/local/apache2/htdocs/secure/area>

  SSLVerifyClient      require
  SSLVerifyDepth       5
  SSLCACertificateFile conf/ssl.crt/ca.crt
  SSLCACertificatePath conf/ssl.crt
  SSLOptions           +FakeBasicAuth
  SSLRequireSSL
  SSLRequire       %{SSL_CLIENT_S_DN_O}  eq "Alexandreio University
of Thessaloniki" and %{SSL_CLIENT_S_DN_OU} in {"Staff”,"Professors"}
</Directory>
```

Με αυτή τη διαμόρφωση επιτρέπουμε την πρόσβαση σε πελάτες που κατέχουν ψηφιακό πιστοποιητικό από την αρχή πιστοποίησης, το πιστοποιητικό της οποίας βρίσκεται στο `conf/ssl.crt/ca.crt` και το διακεκριμένο όνομα περιέχει τα στοιχεία

`o= Alexandreio University of Thessaloniki`

και

`ou=Staff ή ou=Professors.`

Χρήση των ψηφιακών πιστοποιητικών στην υπηρεσία διαμεταγωγής ηλεκτρονικού ταχυδρομείου

Τα ψηφιακά πιστοποιητικά χρησιμοποιούνται στην υπηρεσία διαμεταγωγής ηλεκτρονικού ταχυδρομείου για την εμπιστευτικότητα των μεταδιδόμενων δεδομένων, την πιστοποίηση της ταυτότητας του διακομιστή και την εξακρίβωση της ταυτότητας του πελάτη στο εξυπηρετητή.

Θα περιγραφεί η διαδικασία ρύθμισης του ελεύθερου λογισμικού sendmail για την υποστήριξη της προδιαγραφής STARTTLS. Απαραίτητη προϋπόθεση είναι η εγκατάσταση του λογισμικού OpenSSL, η μεταγλώττιση του ελεύθερου λογισμικού sendmail με υποστήριξη TLS και η έκδοση ψηφιακών πιστοποιητικών για διακομιστή.

Μεταγλώττιση του λογισμικού sendmail με υποστήριξη TLS

Για να μεταγλωττίσουμε το λογισμικό sendmail με υποστήριξη TLS προσθέτουμε τις ακόλουθες γραμμές στο αρχείο

`devtools/Site/site.config.m4 :`

```
# STARTTLS
APPENDDEF(`confINCDIRS', `-I/etc/ssl/include')
APPENDDEF(`confLIBDIRS', `-L/etc/ssl/include')
APPENDDEF(`conf_sendmail_ENVDEF', `-DSTARTTLS -DHASURANDOMDEV')
APPENDDEF(`conf_sendmail_LIBS', `-lssl -lcrypto')
```

Έκδοση ψηφιακών πιστοποιητικών για διακομιστή

Για την έκδοση πιστοποιητικών ακολουθούμε τη διαδικασία που περιγράφεται σε προηγούμενη παράγραφο. Αν το όνομα του διακομιστή για τη συγκεκριμένη υπηρεσία είναι ίδιο με αυτό άλλης υπηρεσίας για την οποία έχουν ήδη εκδοθεί πιστοποιητικά, μπορούμε να χρησιμοποιήσουμε τα υπάρχοντα πιστοποιητικά.

Ρύθμιση του λογισμικού sendmail

Ακολουθούν οι ρυθμίσεις που πρέπει να γίνουν στο αρχείο `.mc` του εξυπηρετητή της υπηρεσίας, μαζί με σχόλια που εξηγούν το σκοπό της κάθε ρύθμισης.

```
dnl
dnl STARTTLS support
dnl
```

```
define(`CERT_DIR', `MAIL_SETTINGS_DIR`'certs')dnl
```

Ορισμός του περιέχοντος φακέλου των πιστοποιητικών και των κλειδιών.

```
define(`confCACERT_PATH', `CERT_DIR')dnl
```

```
define(`confCACERT', `CERT_DIR/CAcert.pem')dnl
```

Το πιστοποιητικό της αρχής πιστοποίησης που έχει υπογράψει τα πιστοποιητικά των χρηστών.

```
define(`confSERVER_CERT', `CERT_DIR/SMcert.pem')dnl
define(`confSERVER_KEY', `CERT_DIR/SMkey.pem')dnl
```

Το πιστοποιητικό του εξυπηρετητή και το αντίστοιχο κλειδί. Το πιστοποιητικό αυτό παρουσιάζει ο εξυπηρετητής στους πελάτες.

```
define(`confCLIENT_CERT', `CERT_DIR/SMcert.pem')dnl
define(`confCLIENT_KEY', `CERT_DIR/SMkey.pem')dnl
```

Το πιστοποιητικό που παρουσιάζει το λογισμικό, όταν δρα ως πελάτης, σε αντίστοιχους εξυπηρετητές.

```
dnl define(`confTLS_SRV_OPTIONS', `V')dnl
```

Όταν συνδεθεί κάποιος πελάτης στον εξυπηρετητή και δώσει STARTTLS, ο εξυπηρετητής τον ρωτάει αν έχει και αυτός "πιστοποιητικό πελάτη". Το αποτέλεσμα μπορεί να είναι ενοχλητικό για τους πελάτες που δεν έχουν ψηφιακό πιστοποιητικό. Με την παραπάνω γραμμή ρύθμισης απενεργοποιούμε την ερώτηση και αφήνουμε στο χρήστη την επιλογή παρουσίασης κάποιου πιστοποιητικού.

Χρήση των ψηφιακών πιστοποιητικών σε άλλες υπηρεσίες

Τα λογισμικά ορισμένων υπηρεσιών δεν προβλέπουν την ενσωματωμένη χρήση

ασφαλών συνδέσεων και ψηφιακών πιστοποιητικών. Οποιαδήποτε δικτυακή υπηρεσία που χρησιμοποιεί σύνδεση TCP μπορεί να χρησιμοποιήσει ψηφιακά πιστοποιητικά για να διασφαλίσει την εμπιστευτικότητα των μεταδιδόμενων δεδομένων και την πιστοποίηση της ταυτότητας του διακομιστή. Η χρήση των πιστοποιητικών επιτυγχάνεται με την δημιουργία βοηθητικού ασφαλούς διαύλου με το ελεύθερο λογισμικό stunnel. Ο βοηθητικός δίαυλος χρησιμοποιείται για την επικοινωνία μέσω του δικτύου, ενώ τα δεδομένα αποστέλλονται εσωτερικά στον εξυπηρετητή στο λογισμικό της υπηρεσίας.

Απαραίτητη προϋπόθεση για τη χρήση του λογισμικού stunnel είναι η εγκατάσταση του λογισμικού OpenSSL και η έκδοση ψηφιακών πιστοποιητικών για διακομιστή.

Έκδοση ψηφιακών πιστοποιητικών για διακομιστή

Για την έκδοση πιστοποιητικών ακολουθούμε τη διαδικασία που περιγράφεται σε προηγούμενη παράγραφο. Αν το όνομα του διακομιστή για τη συγκεκριμένη υπηρεσία είναι ίδιο με αυτό άλλης υπηρεσίας για την οποία έχουν ήδη εκδοθεί πιστοποιητικά, μπορούμε να χρησιμοποιήσουμε τα υπάρχοντα πιστοποιητικά.

Δημιουργία βοηθητικών διαύλων

Για τη δημιουργία ενός βοηθητικού διαύλου για την ασφαλή υπηρεσία που χρησιμοποιεί την πόρτα ‘PORT’ TCP και λογισμικό χειρισμού της υπηρεσίας ‘SERVICE_EXECUTABLE’ εκτελούμε :

```
/usr/local/sbin/stunnel -P /etc/ -p \
     /path-to-stunnel-key.pem  -d ‘PORT’ \
     -Q /path-to-CA-cert.pem  -l ‘SERVICE_EXECUTABLE’
```

Το πιστοποιητικό που παρουσιάζει ο διακομιστής στους πελάτες καθώς και το μυστικό κλειδί βρίσκονται στο αρχείο `/path-to-stunnel-key.pem`, ενώ στο αρχείο `/path-to-CA-cert.pem` είναι αποθηκευμένα τα πιστοποιητικά των αρχών πιστοποίησης της ιεραρχίας πιστοποίησης.

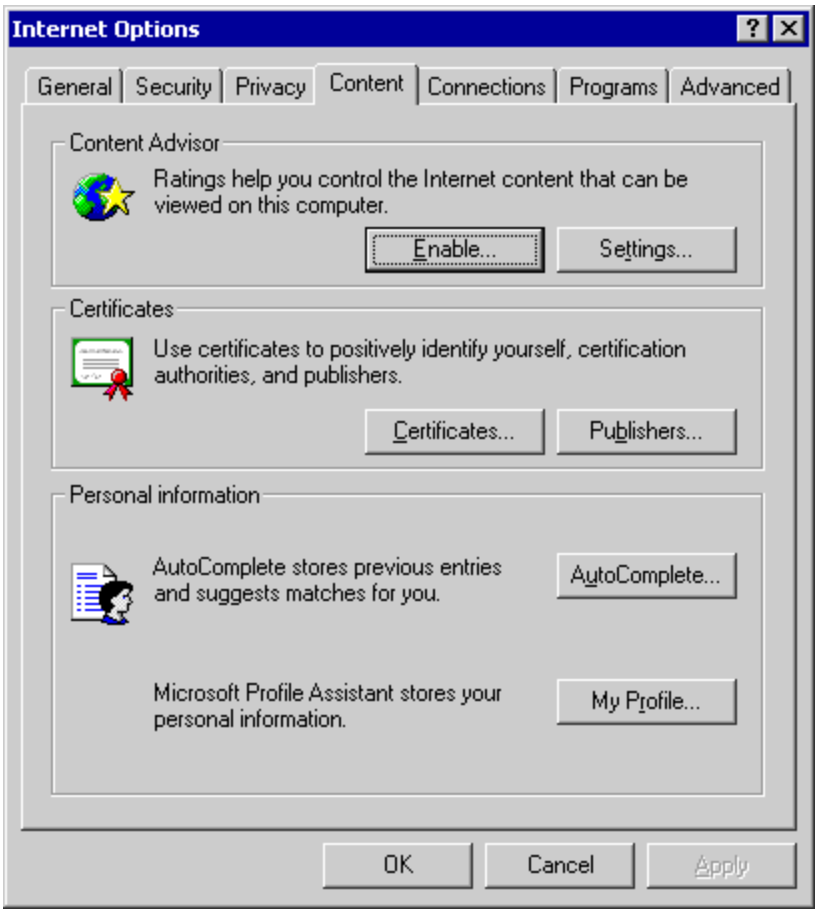
```
if [ -f /etc/stunnel.ipop3d.pid ]; then
echo  “Warning:  stunnel  POP  redirection  was  not
     previously cleanly shutdown”
/bin/rm -f /etc/stunnel.ipop3d.pid
fi
echo "Starting SIPOP (stunnel)-IPOP port mapping."
     /usr/local/sbin/stunnel -P /etc/ -p \
     /path-to-stunnel-key.pem  -d 995 \
     -Q /path-to-CA-cert.pem  \
     -l /usr/etc/mail/ipop3d ipop3d
fi
```

Αρχείο εντολών για την εκκίνηση βοηθητικού διαύλου για την υπηρεσία Secure POP3

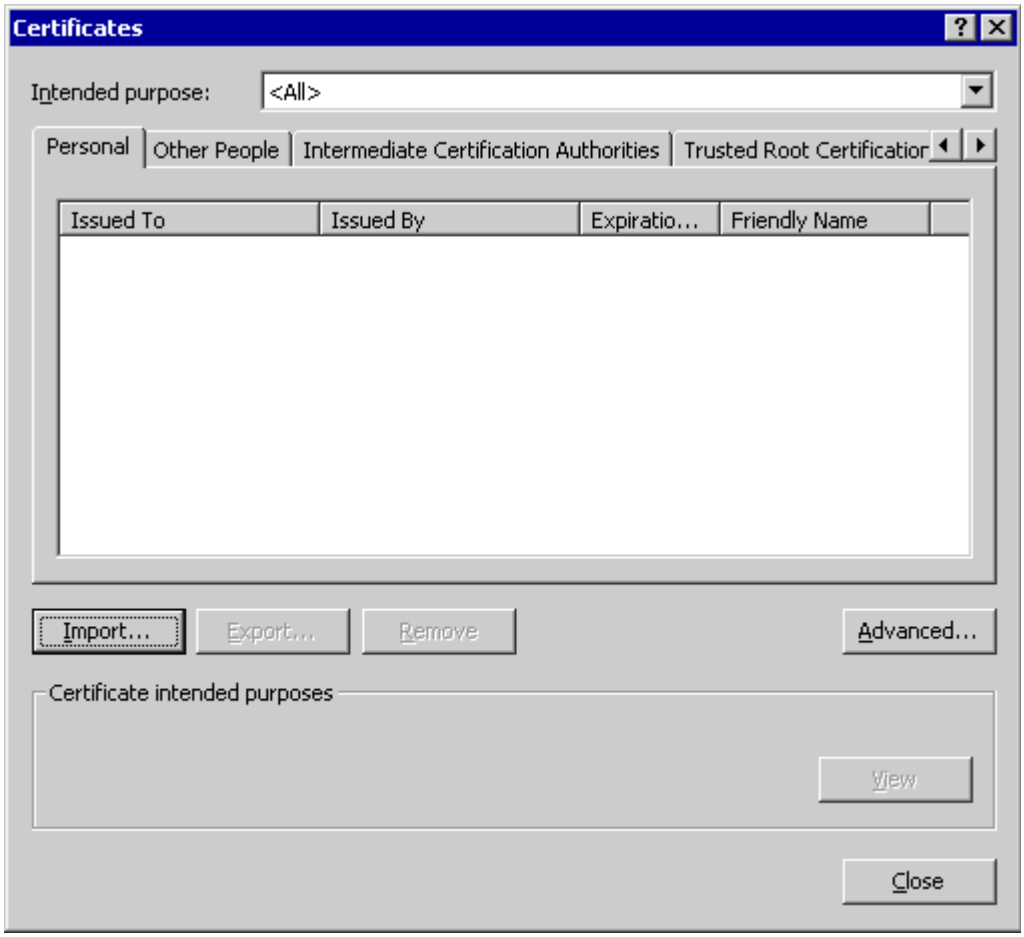
7. ΧΡΗΣΗ ΨΗΦΙΑΚΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΑΠΟ ΠΕΛΑΤΕΣ

Τα ψηφιακά πιστοποιητικά χρησιμοποιούνται από τους διακομιστές για την επιβεβαίωση της ταυτότητας τους στους διακομιστές, την εμπιστευτικότητα της επικοινωνίας μεταξύ πελατών, την ακεραιότητα των δεδομένων που αποστέλλονται μεταξύ πελατών και τη μη άρνηση αποδοχής δεδομένων που απέστειλε ο πελάτης.

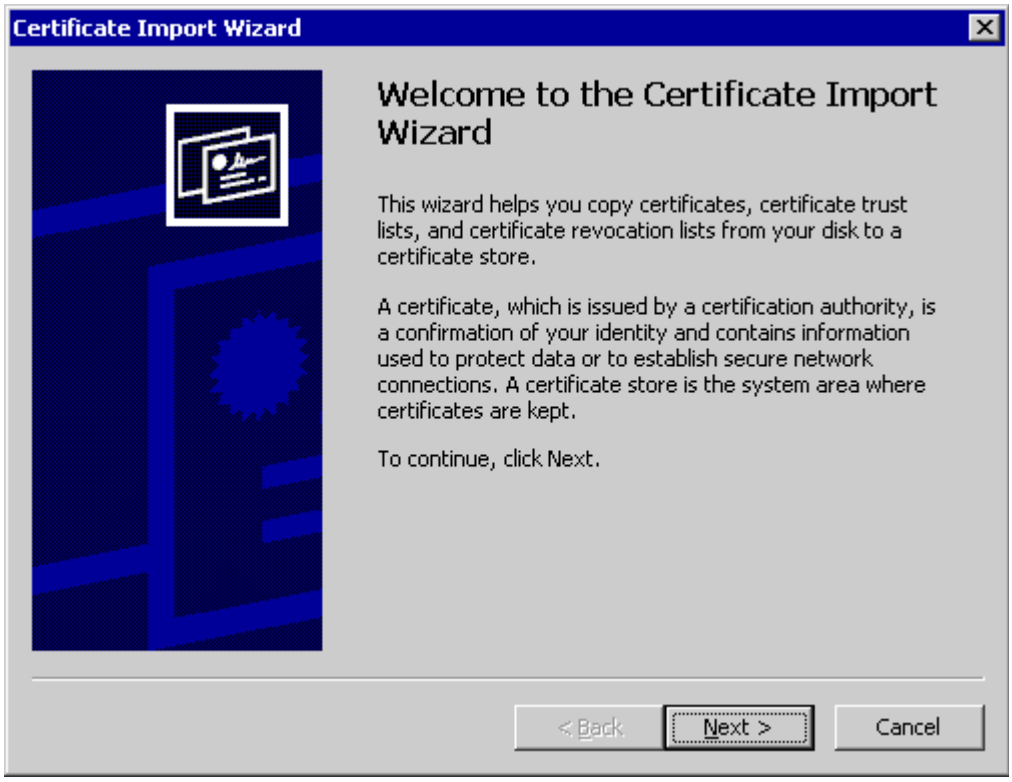
7.1 ΕΓΚΑΤΑΣΤΑΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ ΣΤΟΝ INTERNET EXPLORER



Καρτέλα 1: Από το βασικό μενού του Internet Explorer πηγαίνετε στο Tools -> Internet Options... και επιλέγετε το Certificates... από την καρτέλα Content

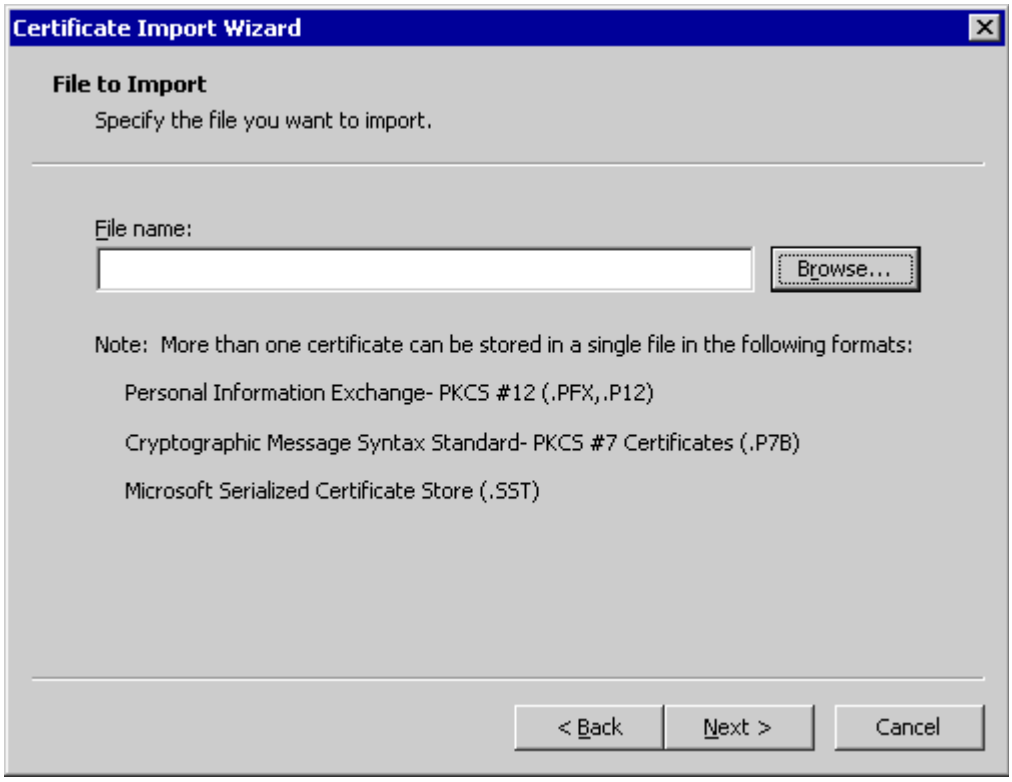


Καρτέλα 2: Στο παραπάνω παράθυρο επιλέξτε Import...:

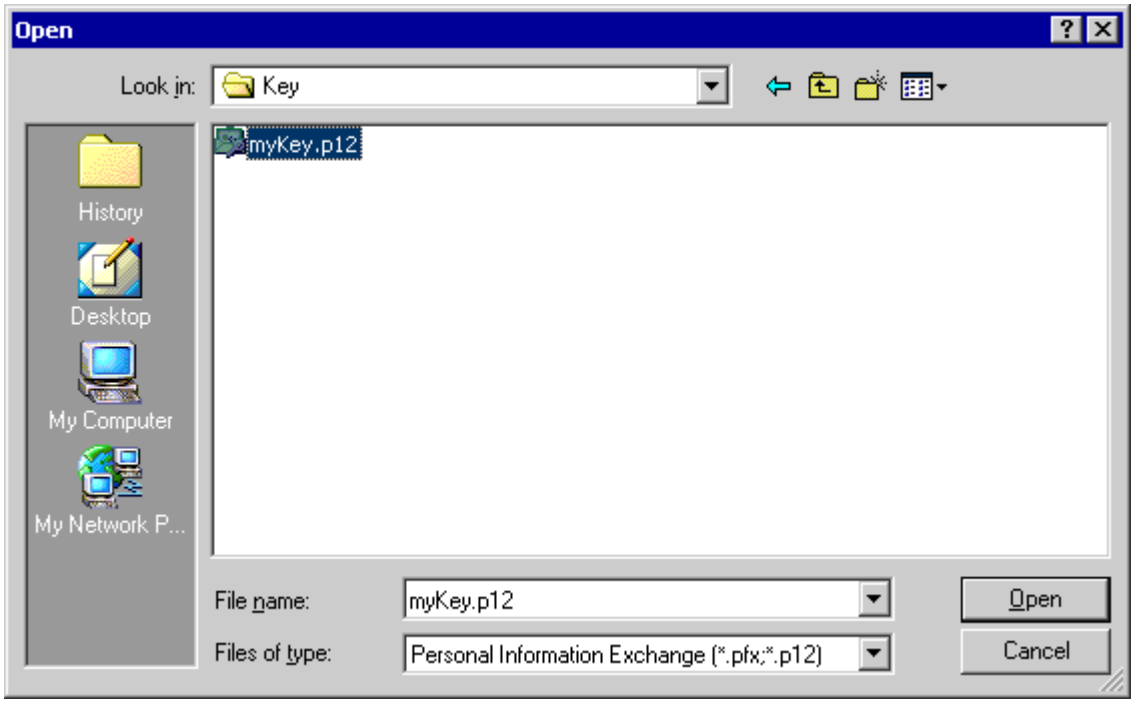


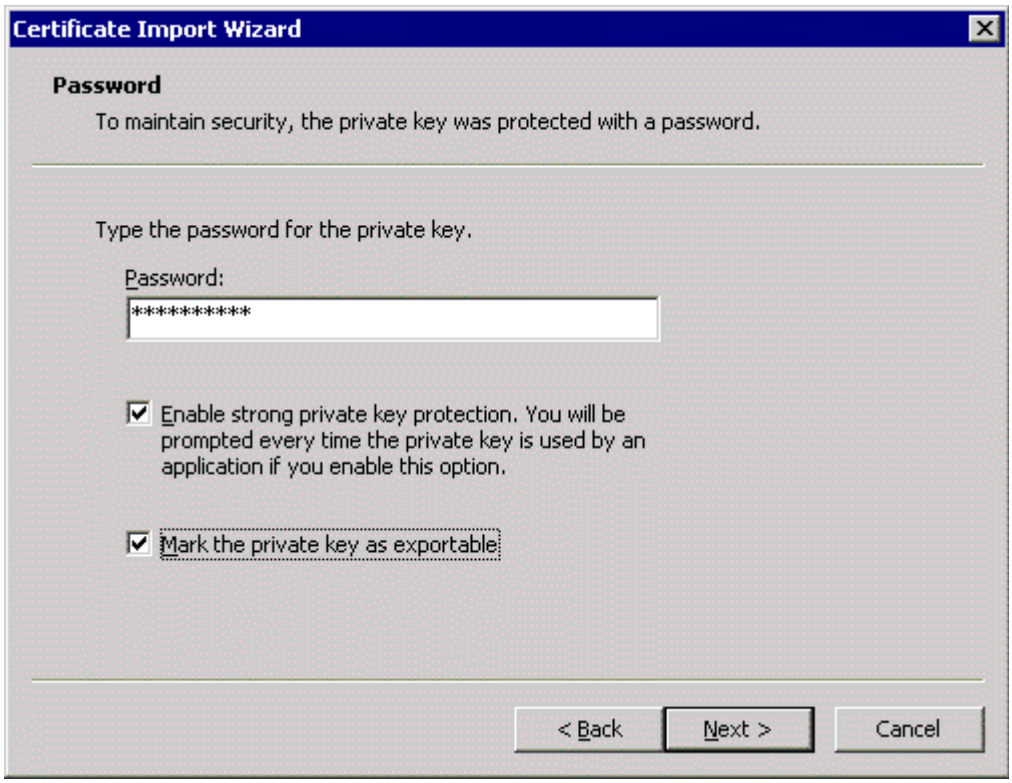
Καρτέλα 3: Πατήστε το Import a Certificate.... Θα ξεκινήσει ένας οδηγός για την εισαγωγή του ψηφιακού πιστοποιητικού σας

Πατήστε Next και θα σας ζητηθεί να επιλέξετε το πιστοποιητικό σας από τον χώρο αποθήκευσης του



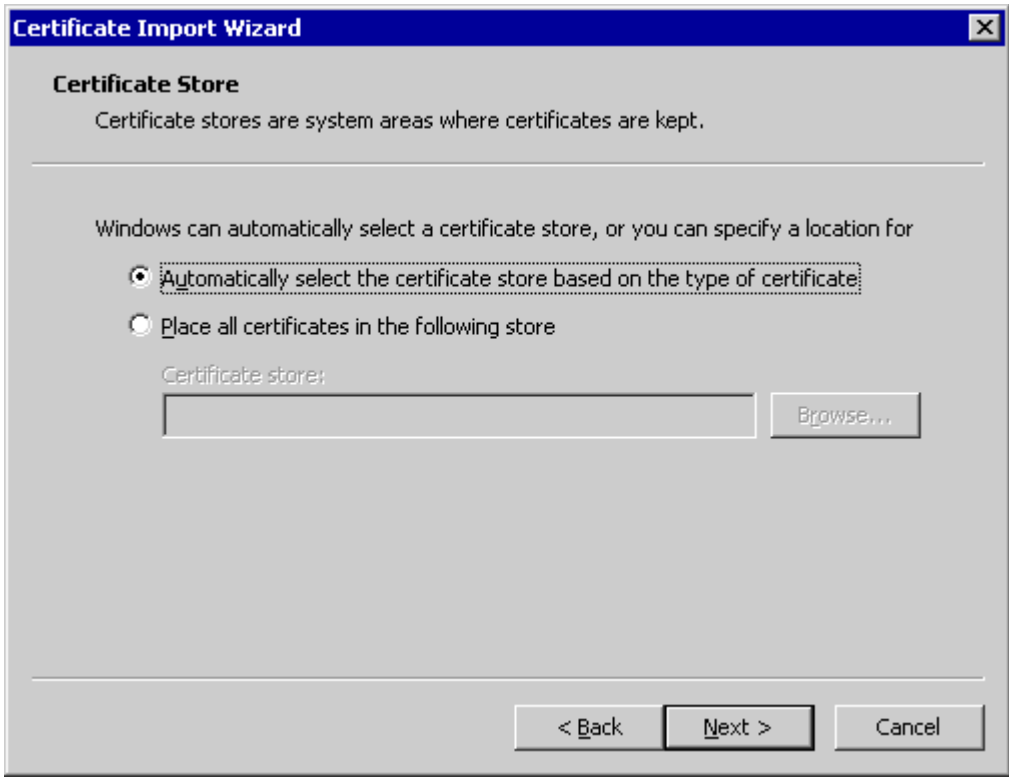
Καρτέλα 4: Πατώντας το Browse... μπορείτε να αναζητήσετε και να επιλέξετε το πιστοποιητικό σας





Καρτέλα 5: Αφότου επιλέξετε το πιστοποιητικό σας και πατήσετε Next θα σας ζητηθεί να δώσετε τον κωδικό που προστατεύει το συγκεκριμένο αρχείο

Κατόπιν επιλέξτε το Enable strong private protection και το Mark the private key as exportable και κατόπιν πατήστε το Next:



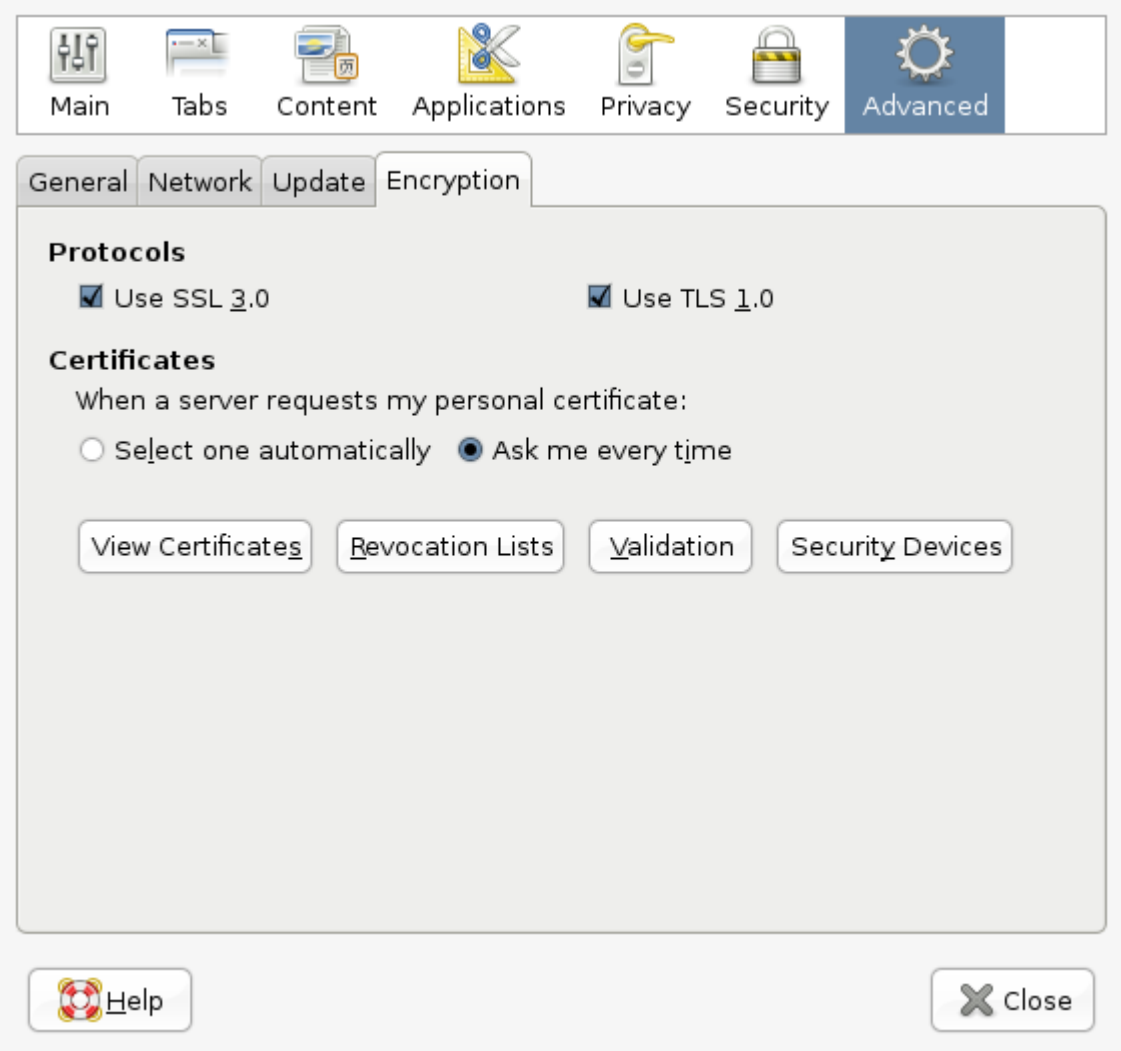
Καρτέλα 6: Επιλέξτε το Automatically... και πατήστε Next

Καρτέλα 7: Στο σημείο αυτό επιλέξτε Finish και θα σας εμφανιστεί το παρακάτω παράθυρο

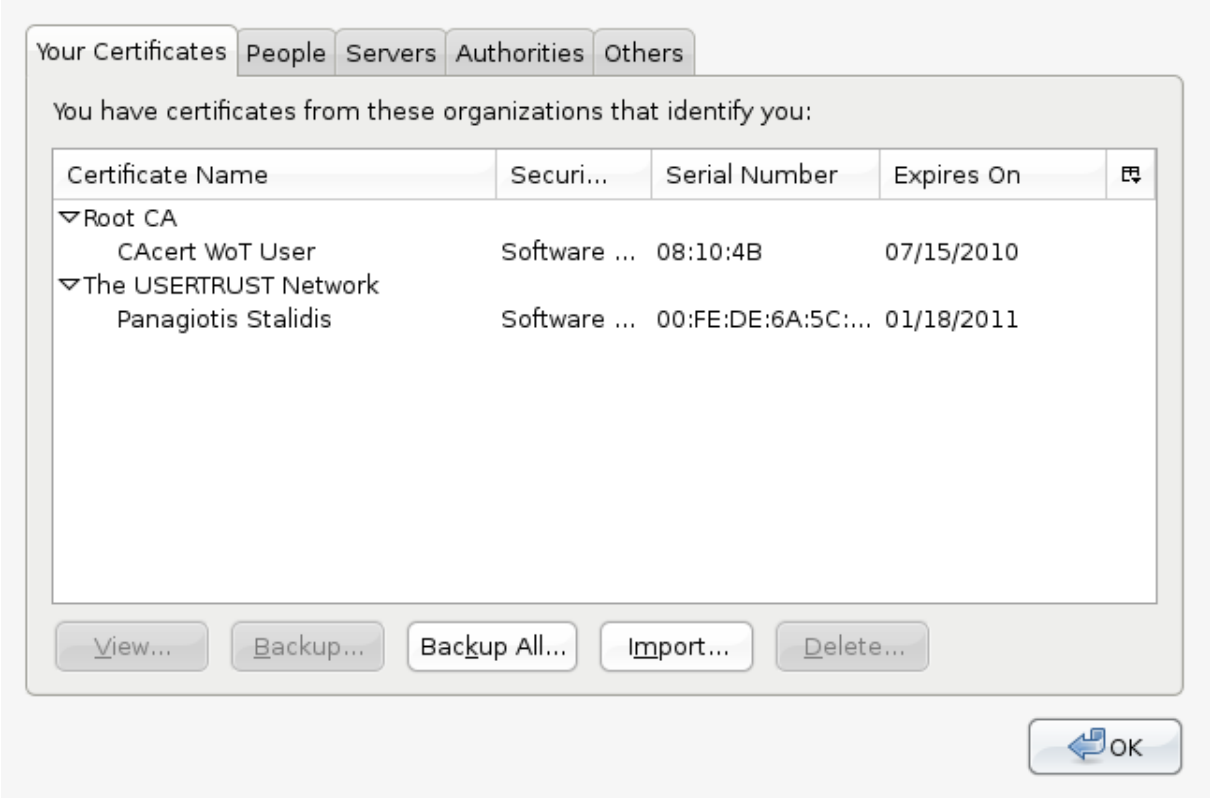
Καρτέλα 8: Πατήστε το Οκ. Ενδεχομένως να εμφανιστούν μηνύματα που θα σας ρωτούν αν θέλετε να σβήσετε τυχόν υπάρχοντα πιστοποιητικά για να προσθέσετε καινούρια. Πατήστε Yes

Καρτέλα 9: Θα εμφανιστεί ένα μήνυμα που θα σας πληροφορεί ότι το πιστοποιητικό σας εγκαταστάθηκε επιτυχώς

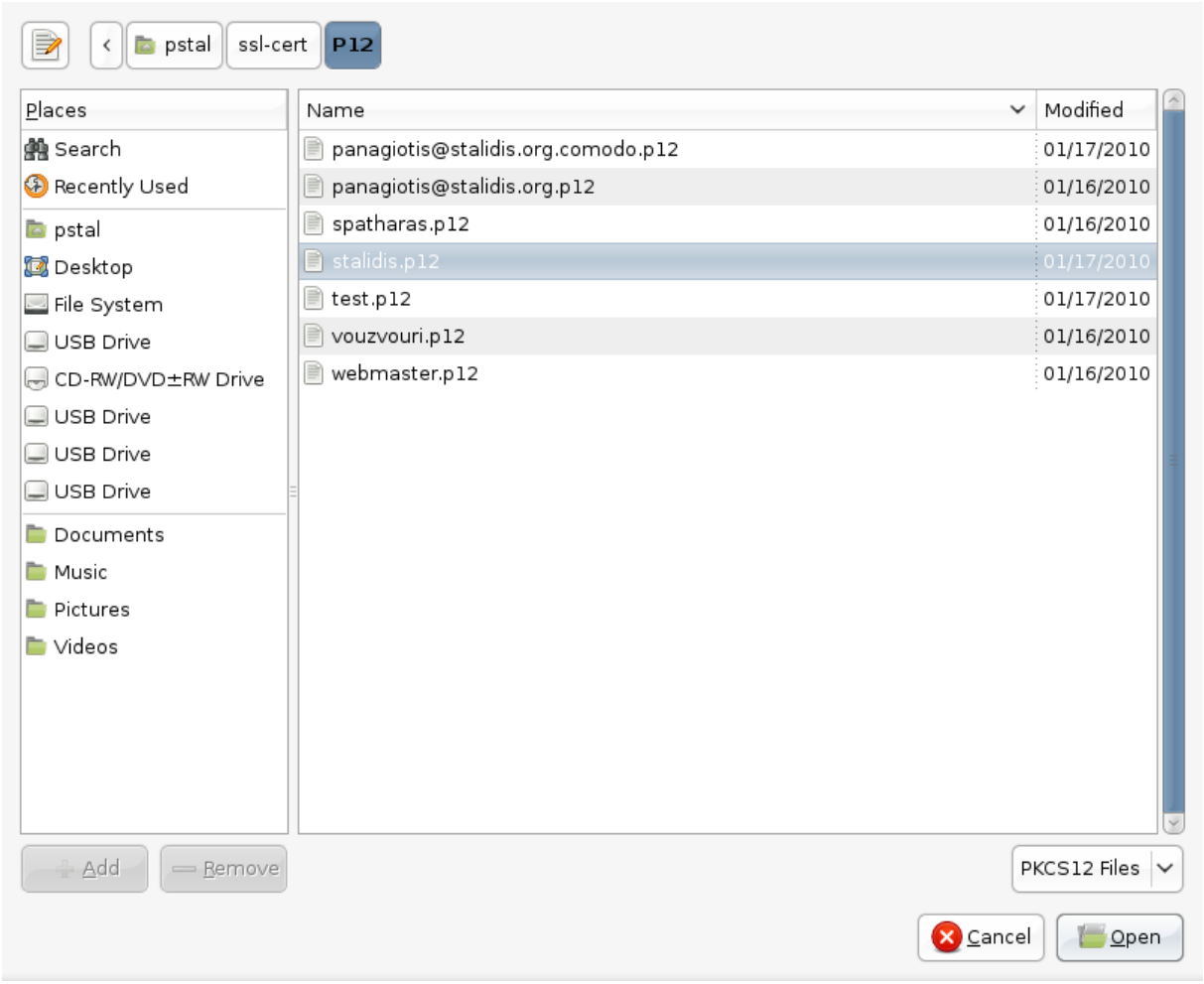
7.2 ΕΓΚΑΤΑΣΤΑΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ ΣΤΟ MOZILLA FIREFOX



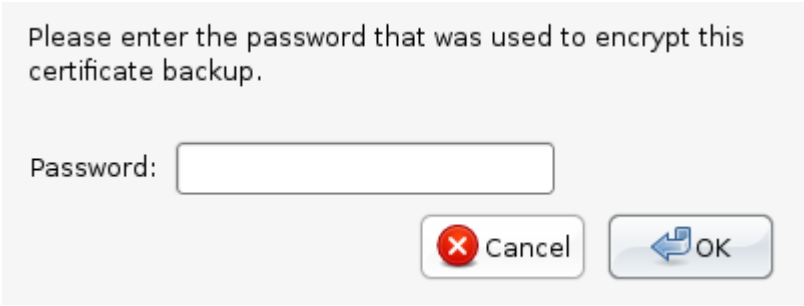
Καρτέλα 10: Από το βασικό μενού του Firefox πηγαίνετε στο Edit -> Preferences... και επιλέγετε το View Certificates... από την καρτέλα Encryption στο Advanced



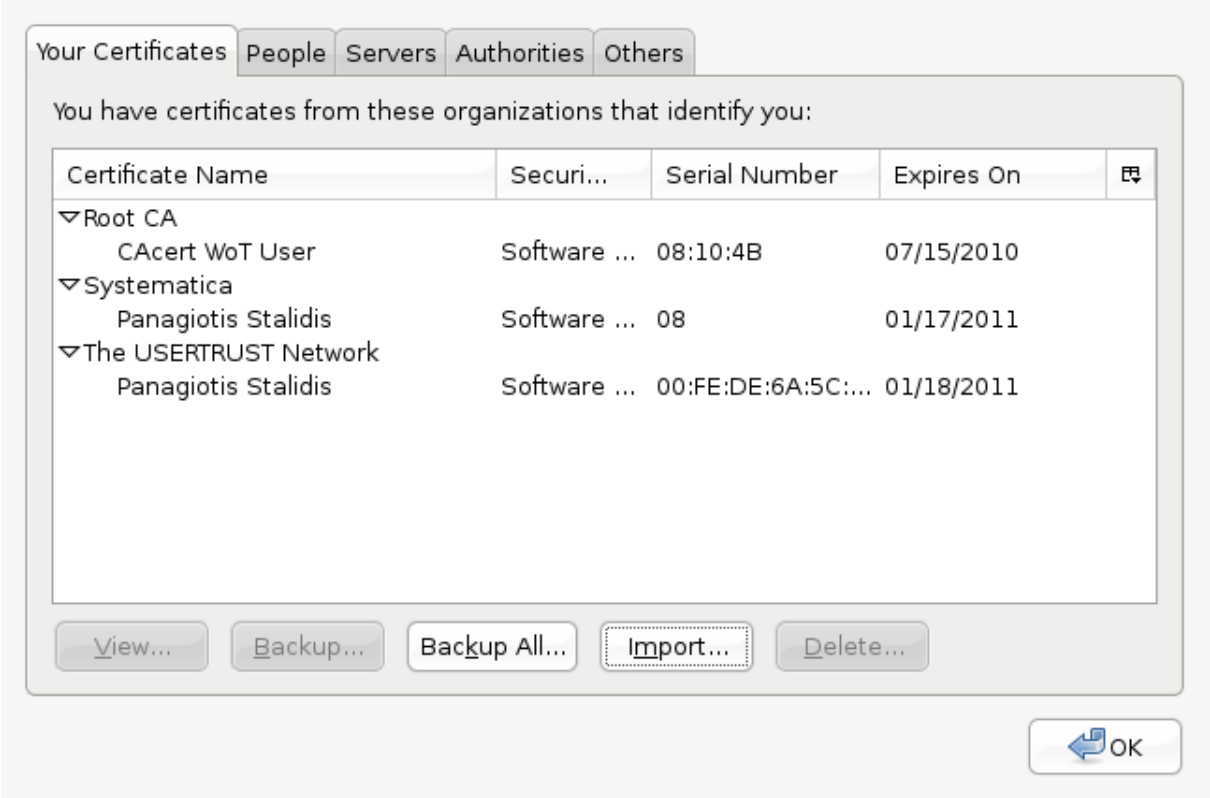
Καρτέλα 11: Στο παραπάνω παράθυρο επιλέξτε Import...



Καρτέλα 12: Μπορούμε να αναζητήσουμε το πιστοποιητικό από το σημείο αποθήκευσής του

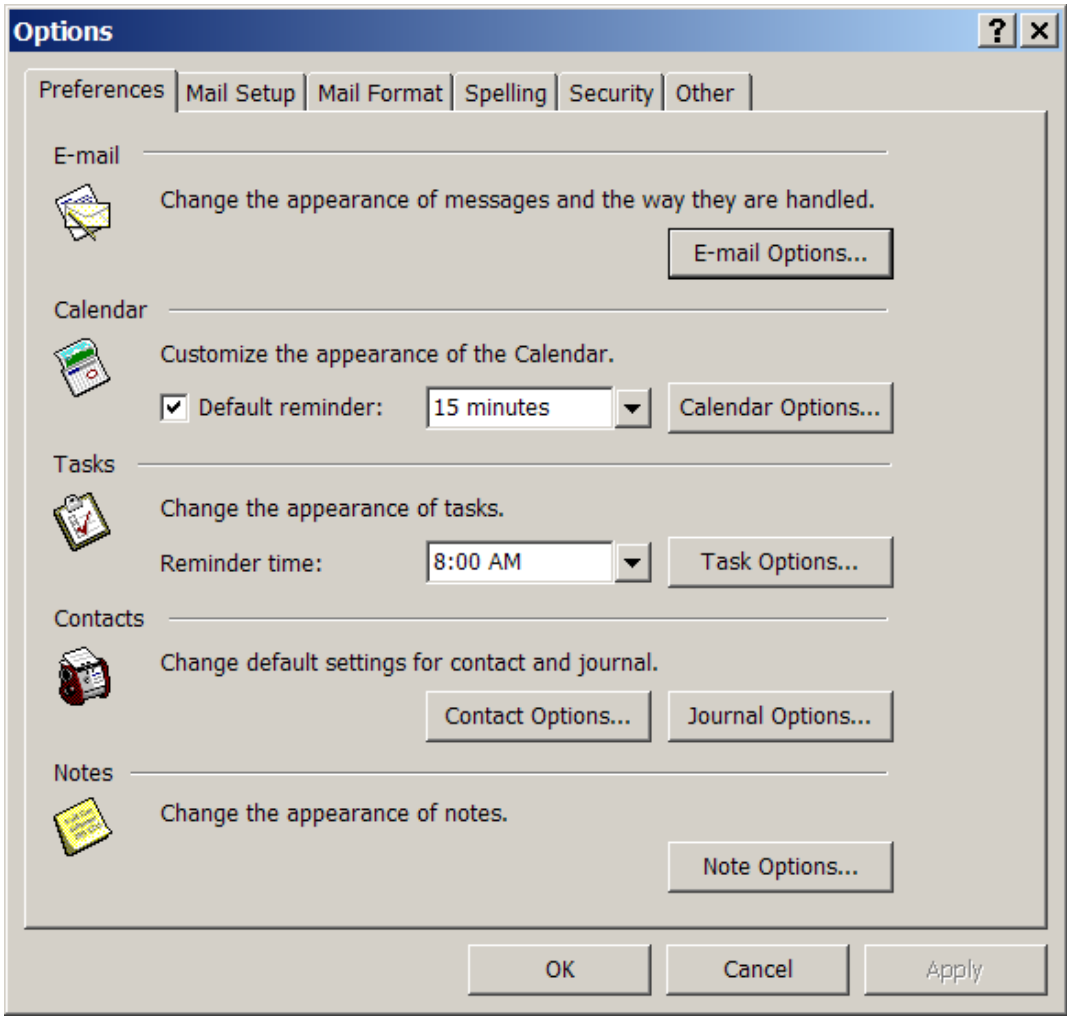


Καρτέλα 13: Θα μας ζητηθεί ο κωδικός που προστατεύει το πιστοποιητικό

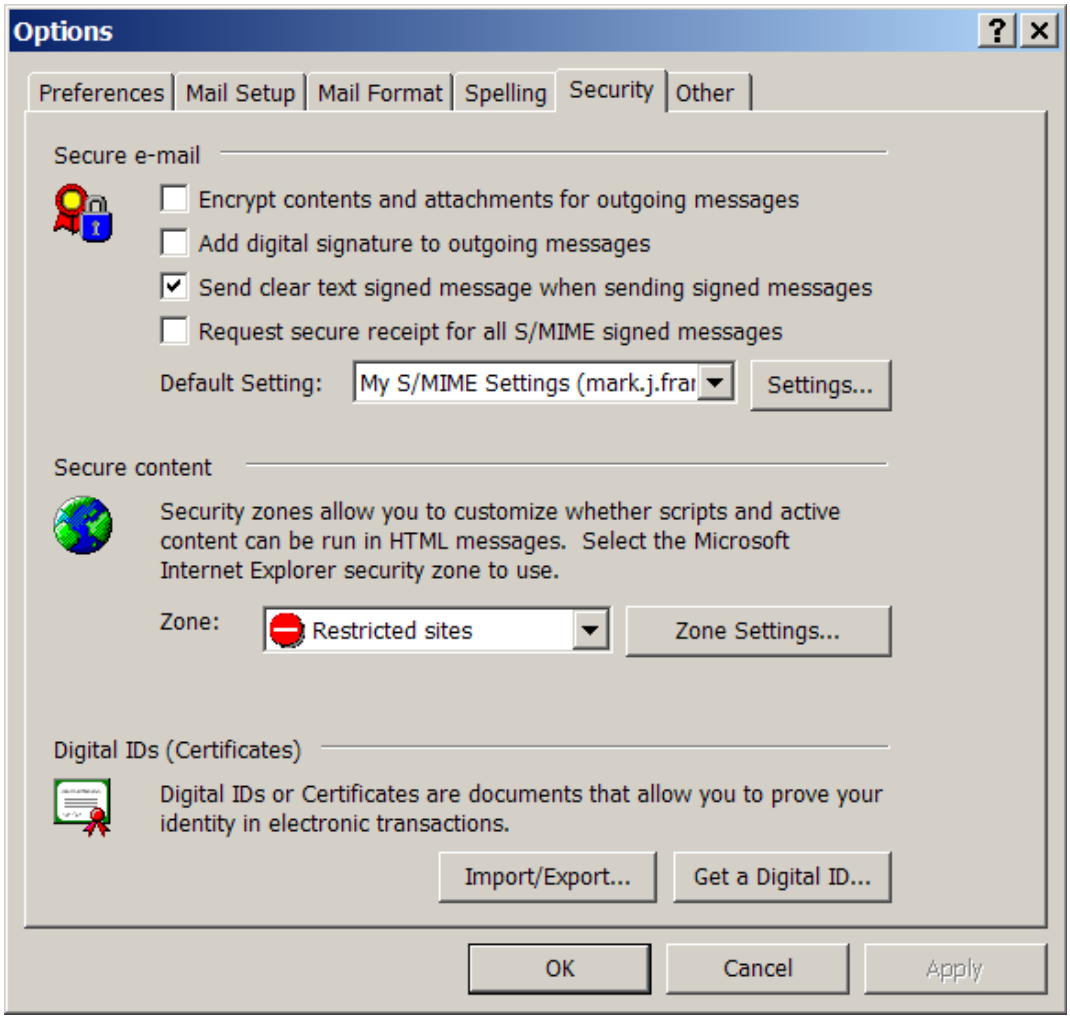


Καρτέλα 14: Η εγκατάσταση του πιστοποιητικού έγινε με επιτυχία

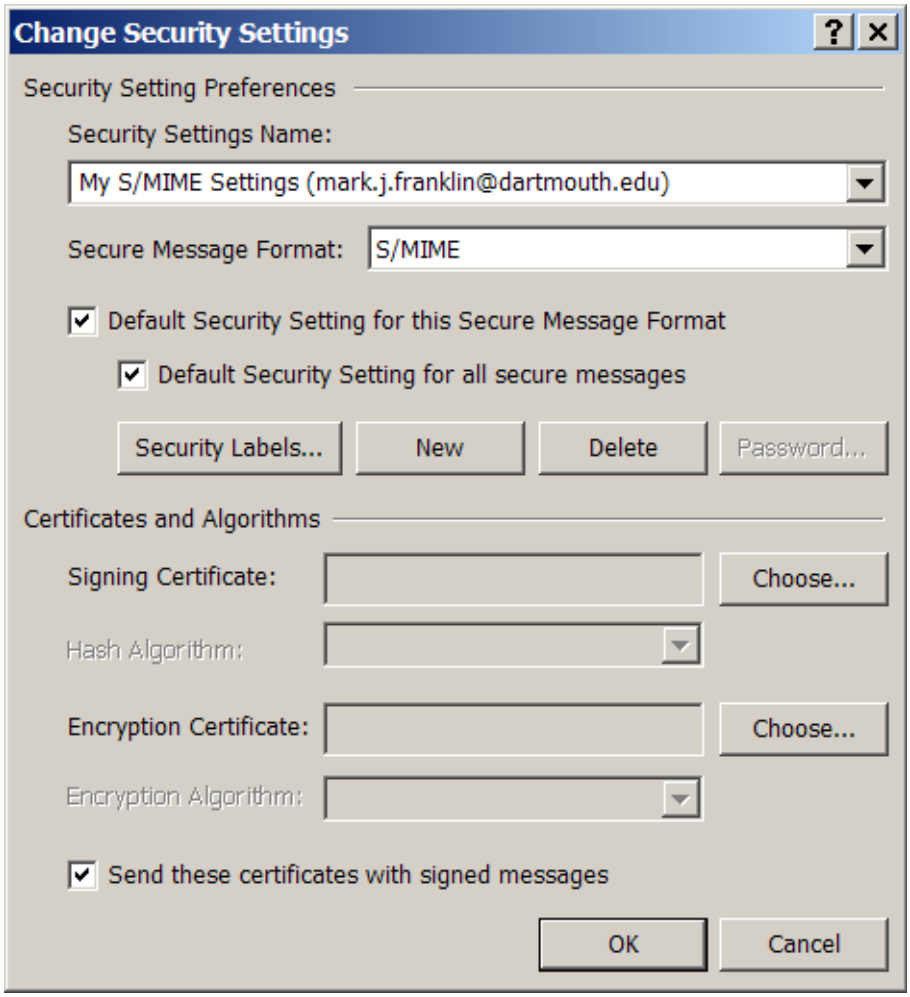
7.3 ΧΡΗΣΗ ΤΟΥ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ ΣΤΟ MICROSOFT OUTLOOK



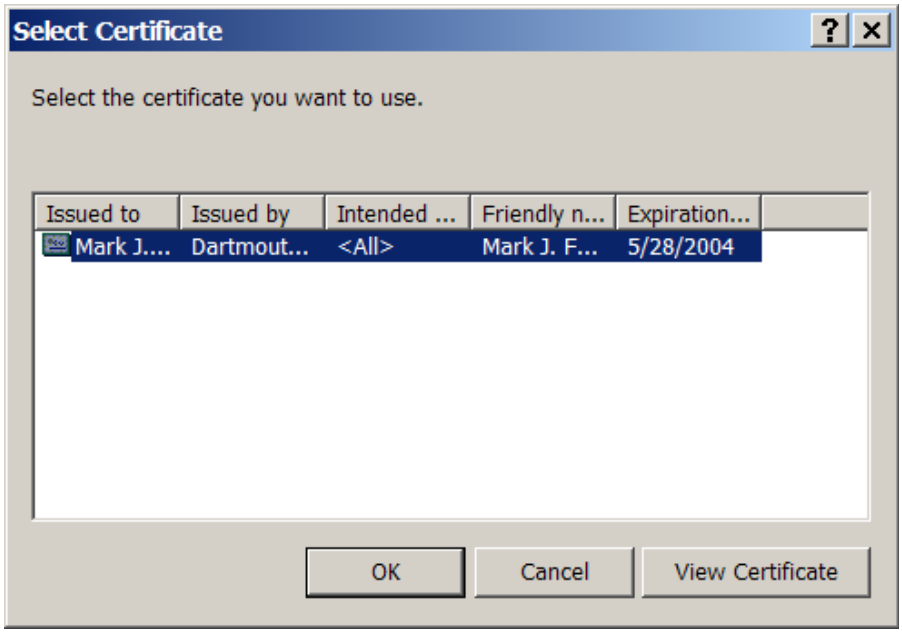
Καρτέλα 15: Από το κύριο μενού του Microsoft Outlook πηγαίνετε στο Tools -> Internet Options... και επιλέγετε Security



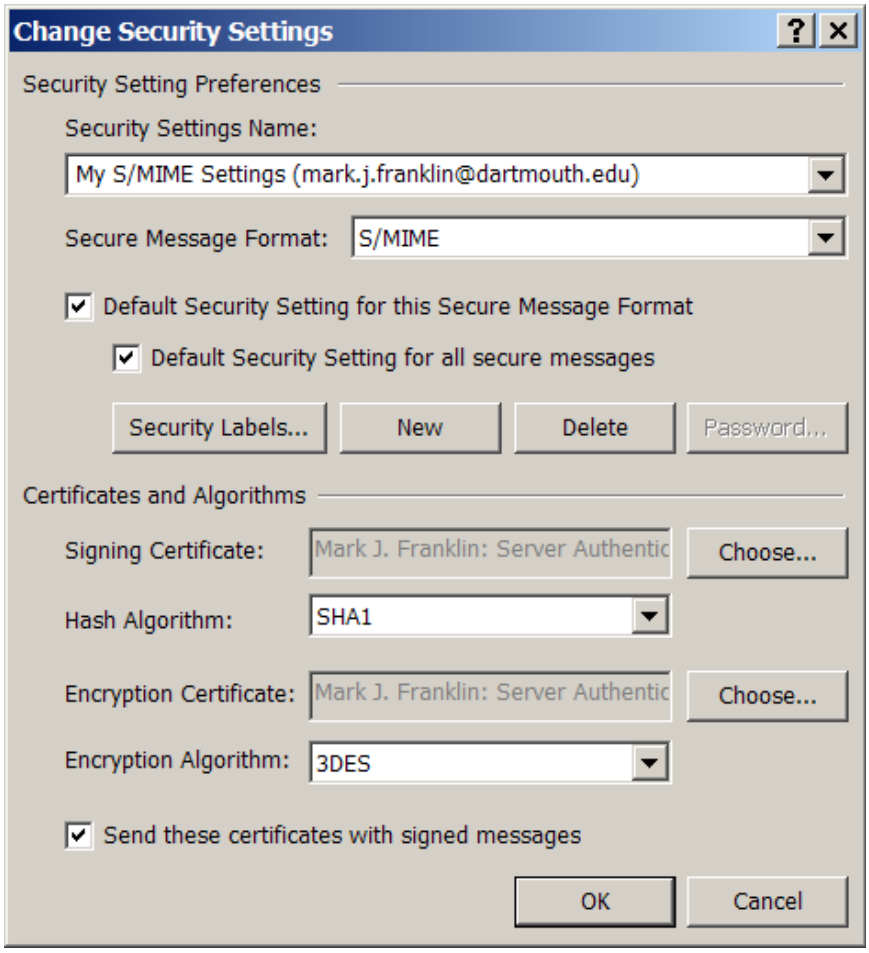
Καρτέλα 16: Επιλέξτε το Settings



Καρτέλα 17: Αφού βεβαιωθείτε ότι είναι επιλεγμένα τα παραπάνω Chechboxes, επιλέξτε το Choose



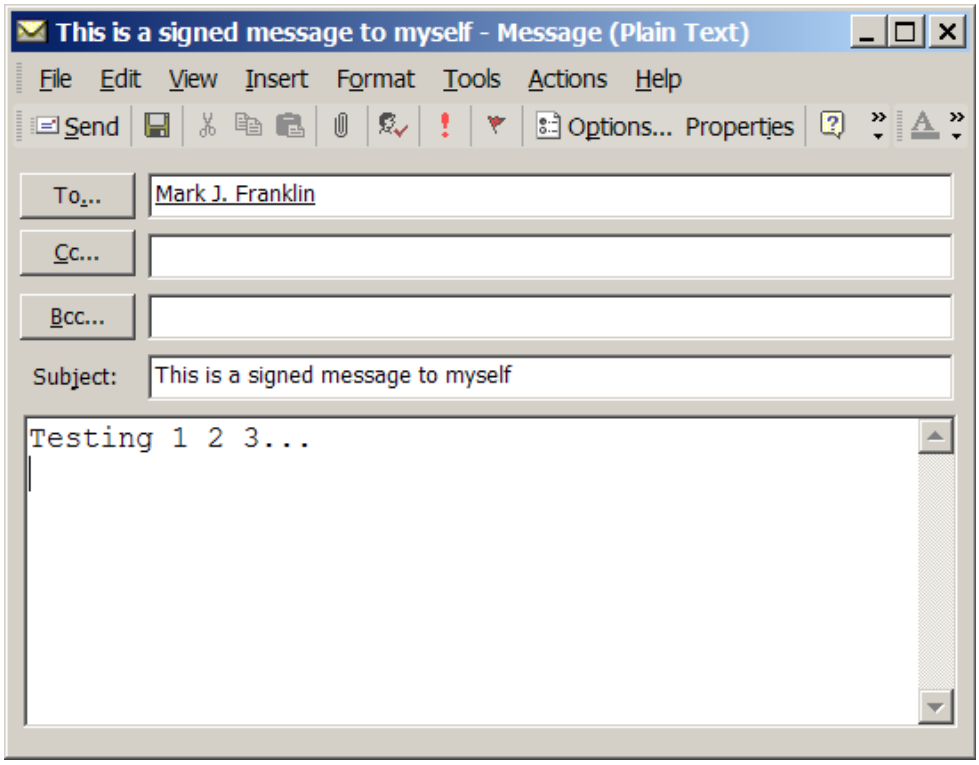
Καρτέλα 18: Μπορείτε να επιλέξετε ένα από τα πιστοποιητικά που έχουν εισαχθεί στον Internet Explorer



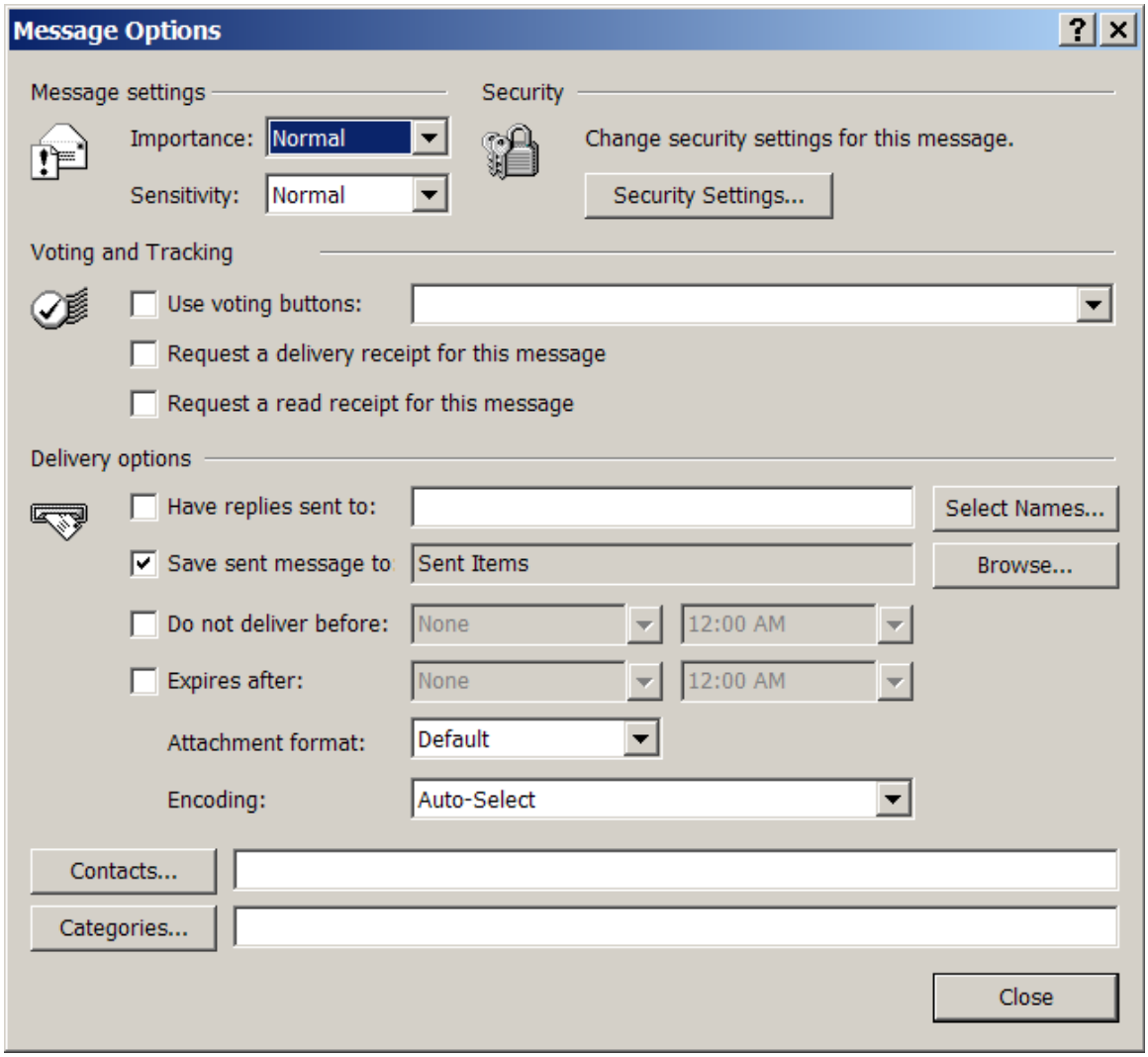
Καρτέλα 19: Από τα στοιχεία του πιστοποιητικού έχει επιλεγεί αυτόματα ο αλγόριθμος δημιουργίας σύνοψης.

Επίσης έχει επιλεγεί το ίδιο πιστοποιητικό και για την κρυπτογράφηση. Αν θέλουμε μπορούμε να επιλέξουμε κάποιο άλλο.

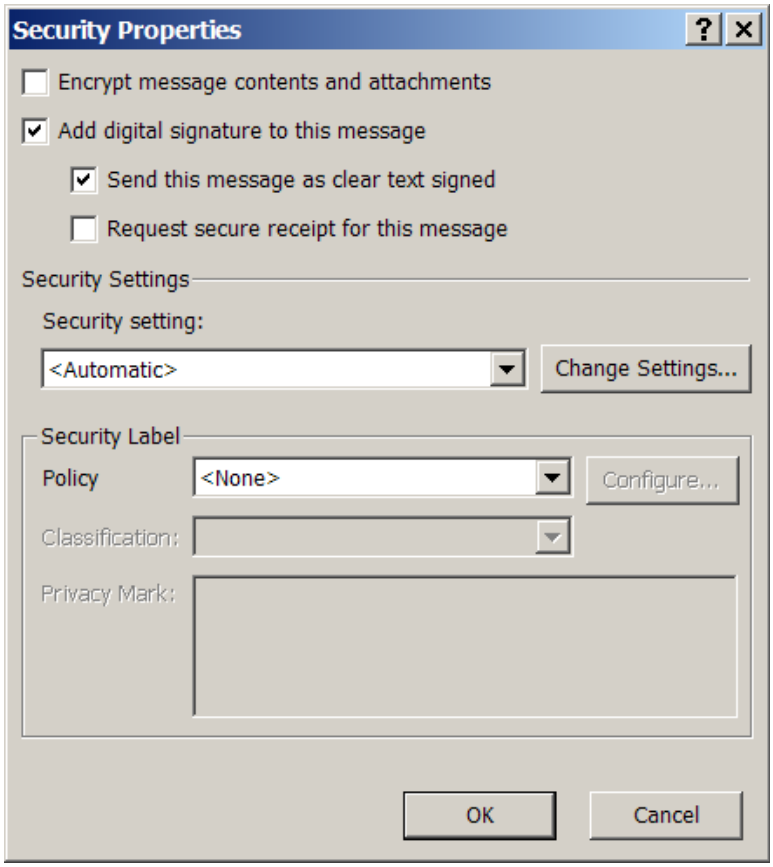
ΑΠΟΣΤΟΛΗ ΜΗΝΥΜΑΤΟΣ



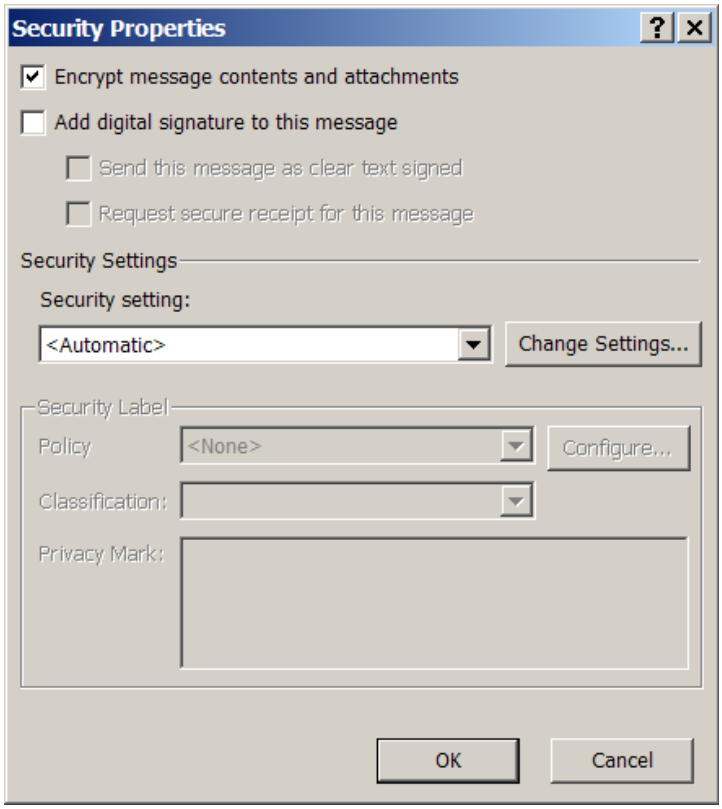
Καρτέλα 20: Η αποστολή ενός μηνύματος με ψηφιακή υπογραφή, γίνετε με τον παραδοσιακό τρόπο.



Καρτέλα 21: Στο παράθυρο σύνταξης μηνύματος, στο View -> Options… υπάρχουν πλέον επιλογές ασφαλείας στο Security Settings...



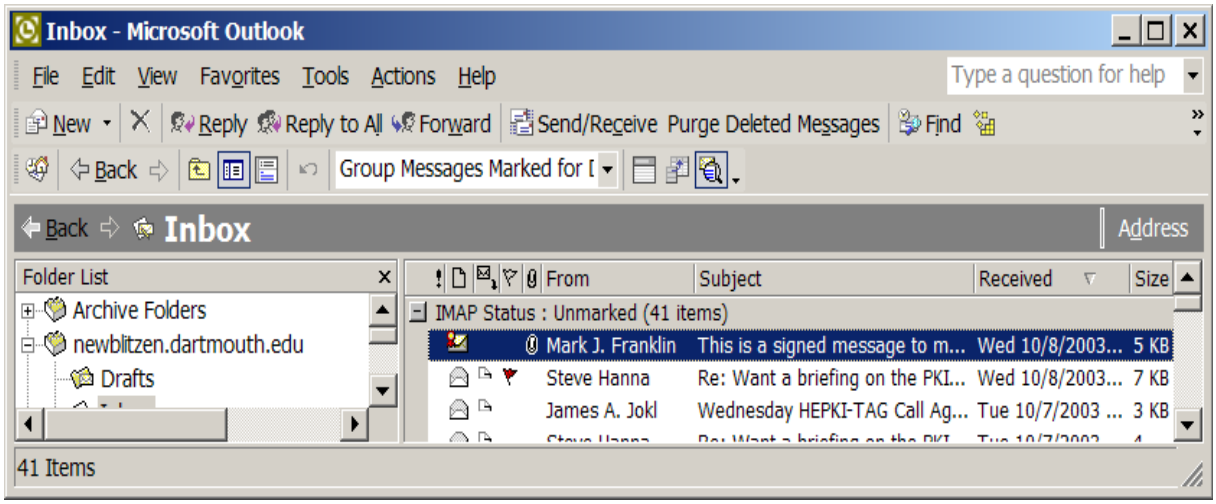
Καρτέλα 22: Εδώ μπορείτε να επιβεβαιώσετε ότι οι επιλογές Add digital signature και Send this message as clear text signed είναι επιλεγμένες



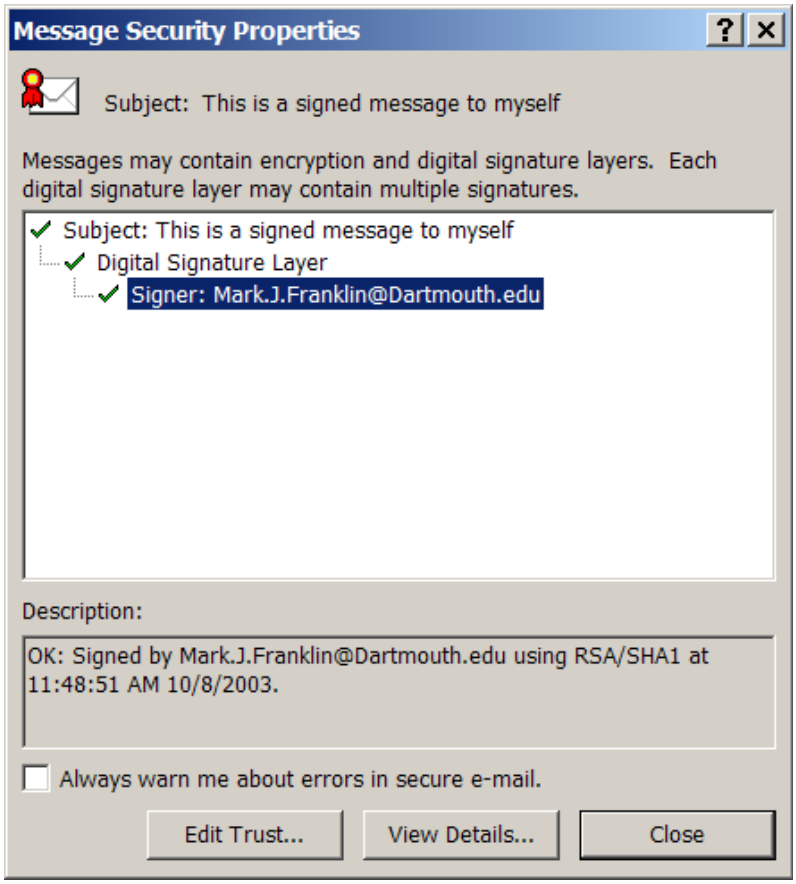
Καρτέλα 23: Με τον ίδιο τρόπο μπορείτε να στείλετε ένα κρυπτογραφημένο μήνυμα.

Για την αποστολή κρυπτογραφημένων μηνυμάτων απαιτείτε η χρήση του πιστοποιητικού του ***παραλήπτη***

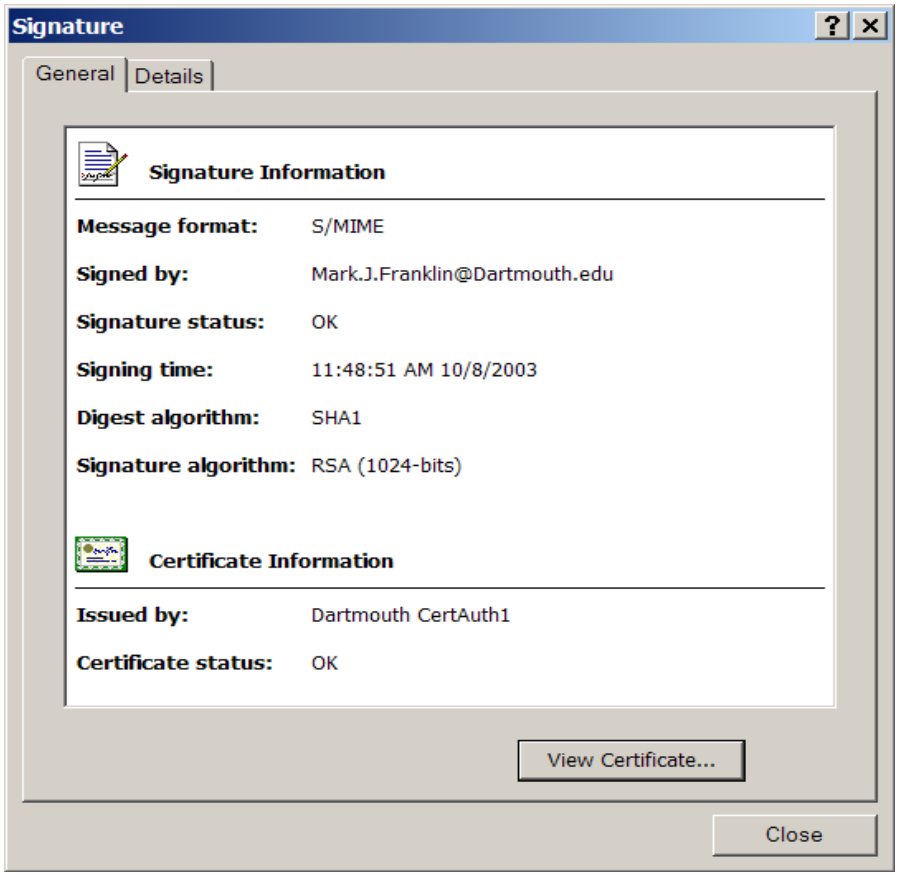
ΛΗΨΗ ΜΗΝΥΜΑΤΟΣ



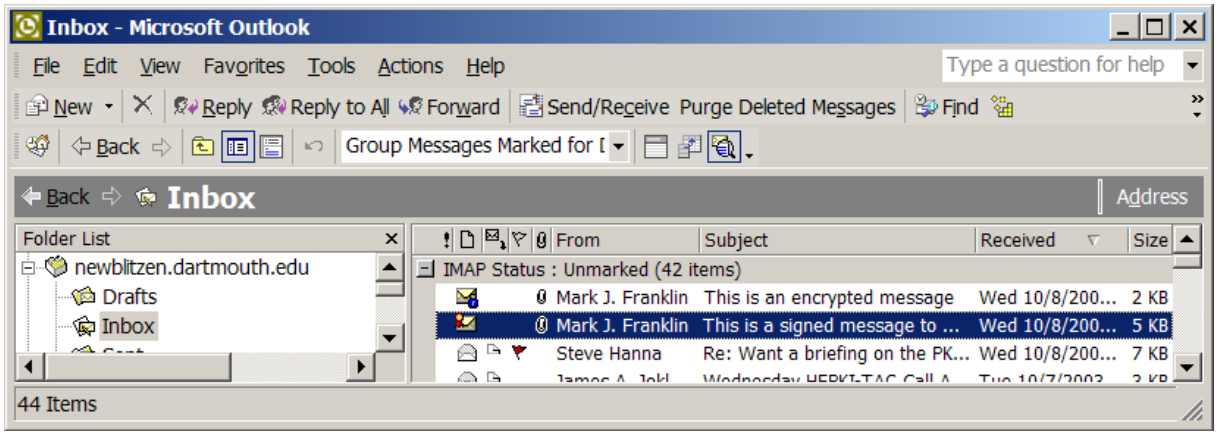
Καρτέλα 24: Όταν λαμβάνουμε ένα μήνυμα με ψηφιακή υπογραφή, στο εικονίδιο του φακέλου παρατηρούμε ότι υπάρχει μια μικρή κορδέλα.



Καρτέλα 25: Αν επιλέξουμε την κορδέλα, μπορούμε να δούμε πληροφορίες σχετικά με την υπογραφή του μηνύματος.

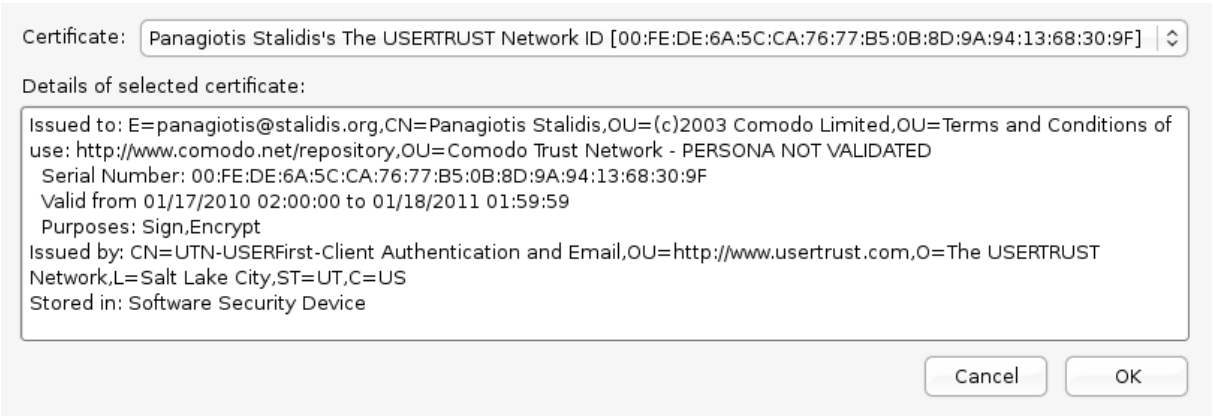


Καρτέλα 26: Επιλέγοντας View Details... μπορούμε να δούμε το πιστοποιητικό που χρησιμοποιήθηκε για την υπογραφή.

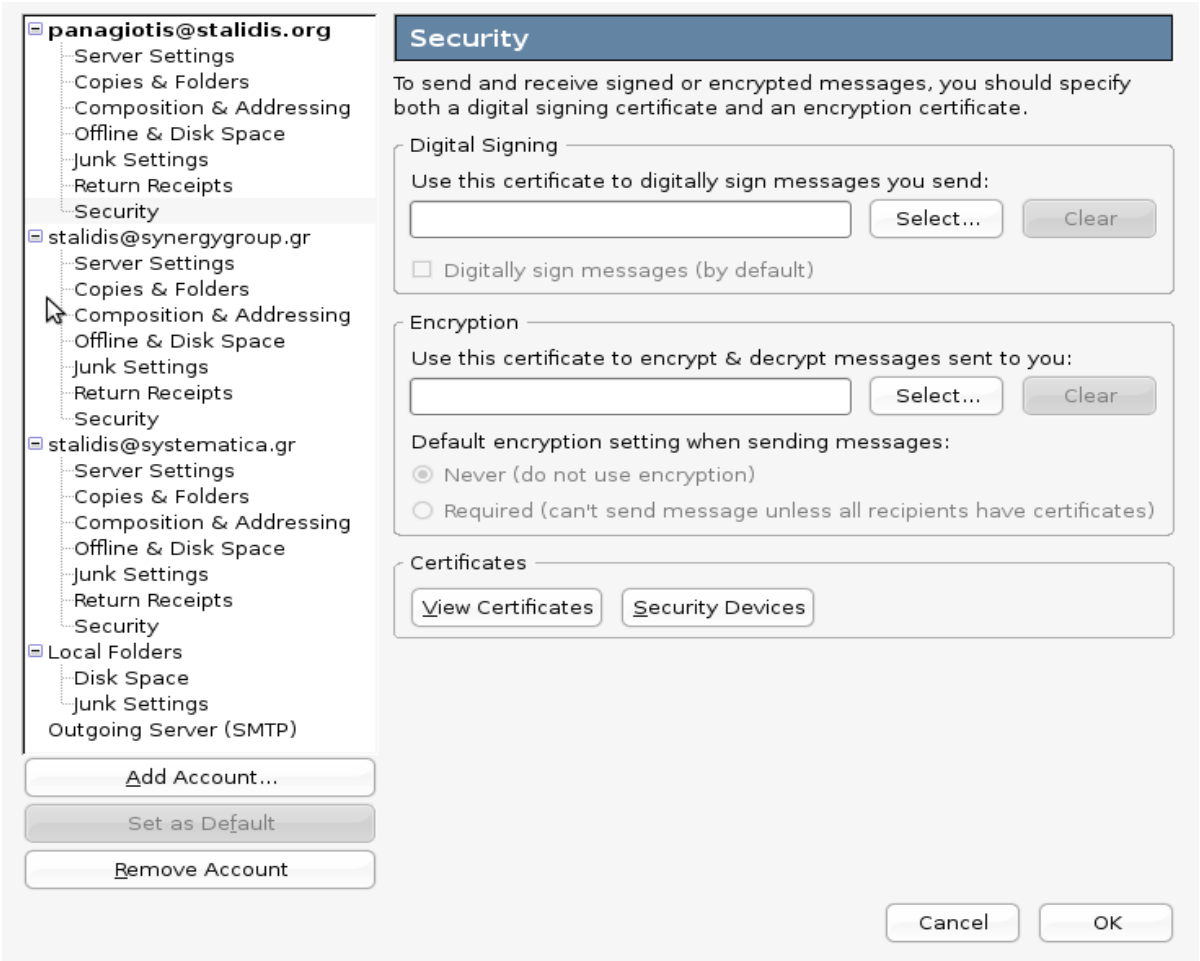


Καρτέλα 27: Όταν το μήνυμα είναι κρυπτογραφημένο, παρατηρούμε μια κλειδαριά στο εικονίδιο του φακέλου.

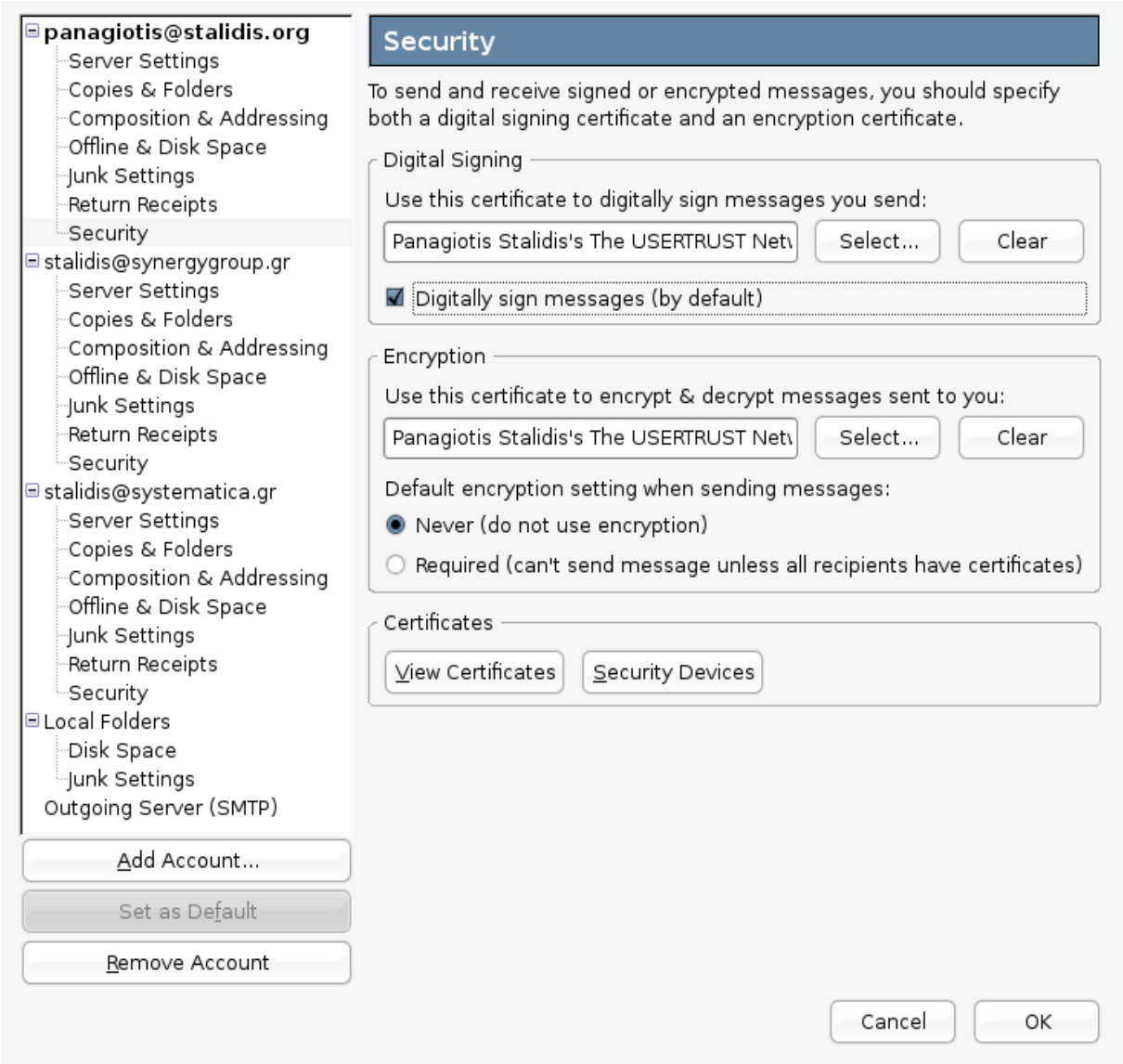
7.4 ΧΡΗΣΗ ΤΟΥ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ ΣΤΟ MOZILLA THUNDERBIRD



Καρτέλα 28: Από το drop-down μενού επιλέγουμε το κατάλληλο πιστοποιητικό από αυτά που έχουν εισαχθεί στο Firefox



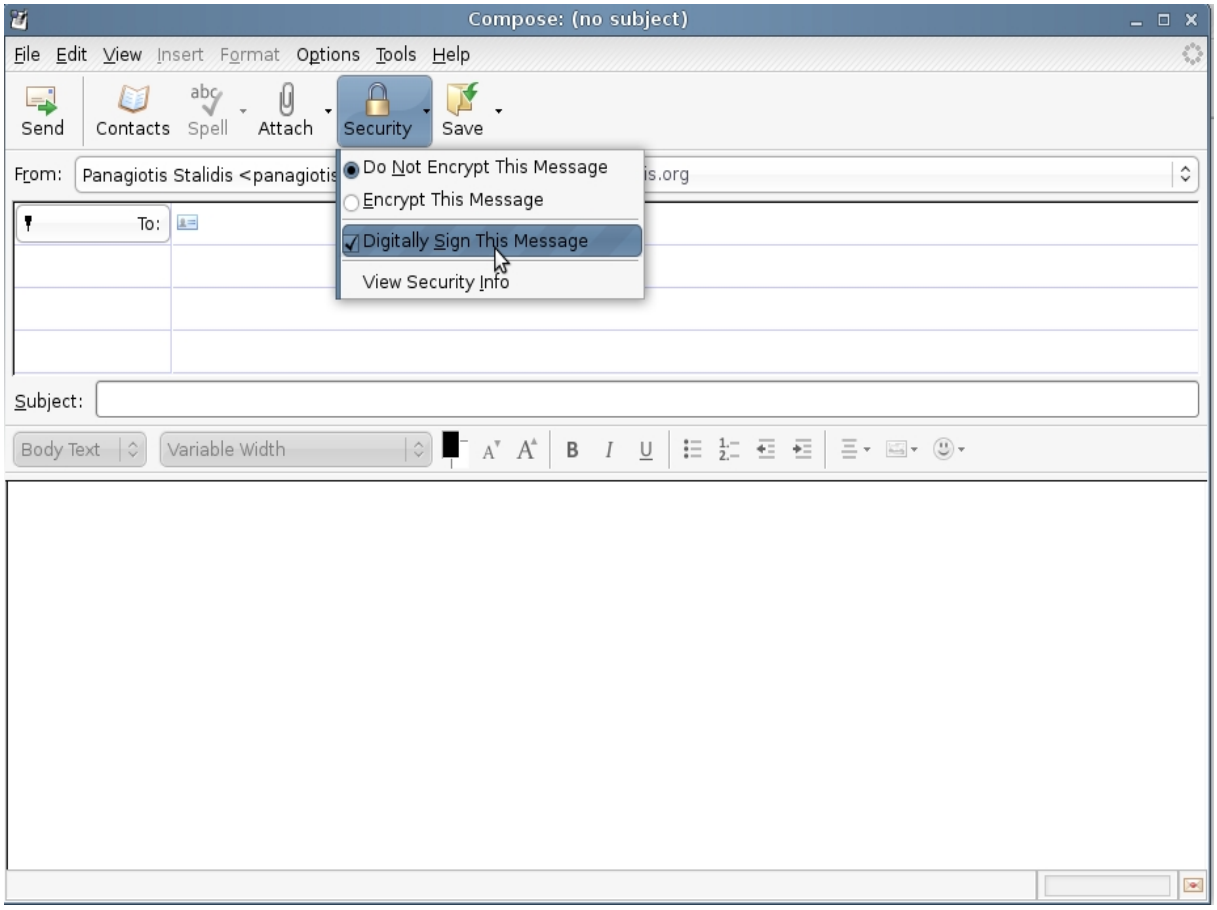
Καρτέλα 29: Από το κύριο μενού του Mozilla Thunderbird πηγαίνουμε στο Edit -> Account Settings... και από το Security επιλέγουμε Select...



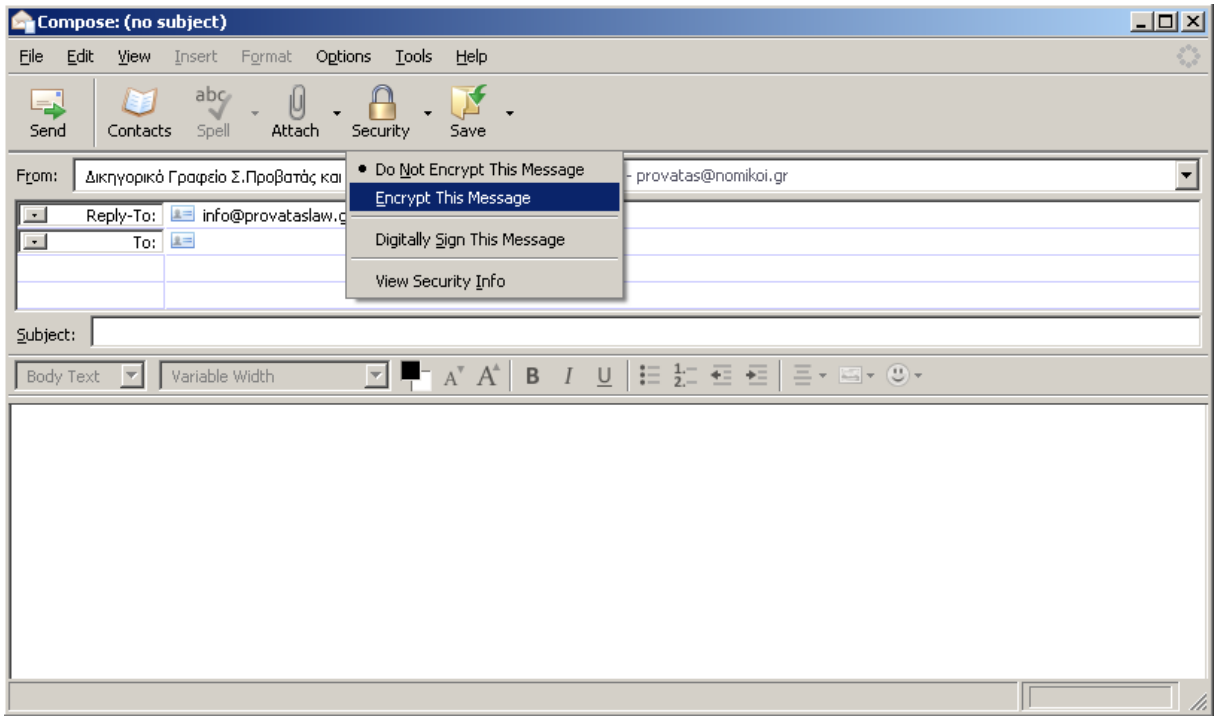
Καρτέλα 30: Το πιστοποιητικό μας έχει επιλεγεί και για ψηφιακή υπογραφή μηνυμάτων και για κρυπτογράφηση

Αν θέλουμε μπορούμε να επιλέξουμε άλλο πιστοποιητικό για κρυπτογράφηση.

ΑΠΟΣΤΟΛΗ ΜΗΝΥΜΑΤΟΣ



Καρτέλα 31: Η αποστολή ενός μηνύματος γίνετε με τον παραδοσιακό τρόπο. Επιλέγοντας το Security μπορούμε να επιβεβαιώσουμε ότι το Digitally Sign This Message είναι επιλεγμένο.



Καρτέλα 32: Με τον ίδιο τρόπο μπορείτε να στείλετε ένα κρυπτογραφημένο μήνυμα.

Για την αποστολή κρυπτογραφημένων μηνυμάτων απαιτείται η χρήση του πιστοποιητικού του ***παραλήπτη****.*

ΣΥΜΠΕΡΑΣΜΑΤΑ

Παρ όλους τους κινδύνους που ελλοχεύουν στο διαδίκτυο και τα πιθανά προβλήματα που μπορεί να προκληθούν από τα κενά ασφαλείας στους υφιστάμενους τρόπους επικοινωνίας, παρατηρούμε ότι η σύγχρονη τεχνολογία μας παρέχει δύο σημαντικά όπλα για να εξασφαλίσουμε την επικοινωνία μας. Αφενός με την διαρκώς μεγαλύτερη χρήση του πρωτοκόλλου SSL από τους διακομιστές, η εξερεύνηση του διαδικτύου καθώς και η αγορά αγαθών από ηλεκτρονικά καταστήματα γίνεται ικανοποιητικά ασφαλής. Παράλληλα η επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου μπορεί να γίνει και κρυπτογραφημένα, ώστε να γνωρίζουμε πόσοι και ποιοι θα διαβάσουν τα μηνύματά μας, ενώ έχουμε τη δυνατότητα να τα υπογράψουμε ώστε να μην υπάρχει καμιά αμφισβήτηση για την ταυτότητα του αποστολέα ενός μηνύματος. Όπως είδαμε η διαδικασία αυτή είναι απλή και ολοκληρώνεται με μερικά κατανοητά βήματα που ακόμα και κάποιος που δεν είναι ειδήμων στους υπολογιστές μπορεί να ακολουθήσει.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] L. Hughes, *Internet E-Mail: Protocols, Standards, and Implementations, Artech House*, 1998

[2] J. Linn, S.T. Kent, D.Balenson, *Privacy Enhancement for Internet Electronic Mail, RFC 1421, 1422, 1423*, 1993

[3] B. Schneier, *E-Mail Security: How to Keep Your Electronic Messages Private, John Wiley & Sons*, 1995

[4] A.S. Tanenbaum, *Computer Networks, Upper Saddle River,* 1996

[5] R. Oppliger, *Secure Messaging with PGP and S/Mime, Artech House*, 2000

[6] www.pgpi.org, 2006

[7] www.gnupg.org, 2006

[8] www.cacert.org, 2006

[9] www.verisign.com, 2005

[10] en.wikipedia.org/wiki/Public_key_certificate , 2005