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

Πτυχιακή εργασία

«Ασφάλεια στο διαδίκτυο και τις ηλεκτρονικές συναλλαγές»

Του φοιτητή
Πολυχρονόπουλου Άγγελου
Αρ. Μητρώου 02/2056

Επιβλέπων καθηγητής
Σαλαμπάσης Μιχαήλ

Θεσσαλονίκη 2009

Περιεχόμενα

Περιεχόμενα σχημάτων

Περιεχόμενα πινάκων

Εισαγωγή

Στα τέλη της δεκαετίας του ‘60 το Υπουργείο Άμυνας των ΗΠΑ, με θέμα τις ψηφιακές τηλεπικοινωνίες σε περίπτωση πολέμου, δημιούργησε ένα πειραματικό αποκεντρωμένο δίκτυο υπολογιστών που αποκαλείτο ARPANET. Το ARPANET ήταν ένα μεγάλο δίκτυο ευρείας περιοχής (WAN) που δημιουργήθηκε με πόρους του προγράμματος ARPA (*Advanced Research Project Agency*) του Υπουργείου Άμυνας και σκοπός του ήταν να συνδέσει το Υπουργείο με στρατιωτικούς ερευνητικούς οργανισμούς. Την επόμενη δεκαετία διευρύνθηκε προς μη στρατιωτικές χρήσεις αφού επιτράπηκε να το χρησιμοποιούν διάφορα Αμερικάνικα πανεπιστήμια και ερευνητικά κέντρα. Το 1973 συνδέθηκαν και τα πρώτα Ευρωπαϊκά Πανεπιστήμια. Η μεγάλη του ανάπτυξη υποβοηθήθηκε μέχρι τις αρχές της δεκαετίας του 1980 από την παράλληλη ανάπτυξη του UNIX από τα Πανεπιστήμια.

Στα μέσα περίπου της δεκαετίας του ‘80 όλο και περισσότερα πανεπιστήμια αρχίζουν και συνδέονται πάνω στο ARPANET με αποτέλεσμα την επιβάρυνσή του και την διαίρεσή του σε δύο άλλα δίκτυα. Στο MILNET, που ήταν μόνο για στρατιωτικές επικοινωνίες και στο νέο ARPANET, που χρησιμοποιούνταν πλέον μόνο από τα πανεπιστήμια και για ερευνητικούς σκοπούς στο θέμα της δικτύωσης. Μερικά έτη πιο μετά το National Science Foundation (NSF) δημιουργεί ένα δικό του δίκτυο, το NSFNET με αποτέλεσμα στο τέλος της δεκαετίας του 80 όλο και περισσότερες χώρες να συνδέονται στο NSFNET. Έτσι χιλιάδες δίκτυα άρχισαν να συνδέονται μεταξύ τους, μέχρι να φτάσουμε τελικά στο γνωστό πλέον σε όλους μας Internet. Παράλληλα έχουμε και την κατάργηση του ARPANET περί το 1990.

Οι δυνατότητες του Διαδικτύου (*Internet*) επεκτάθηκαν την δεκαετία του ‘70 με την εισαγωγή του ηλεκτρονικού ταχυδρομείου και την δυνατότητα

μεταφοράς αρχείων. Στην συνέχεια, στην αρχή της δεκαετίας του ‘80 άρχισε η χρήση του συστήματος ονοματολογίας DNS.

Το Διαδίκτυο παρουσιάζει τα τελευταία χρόνια εξαιρετική ανάπτυξη. Αν και ξεκίνησε ως δίκτυο μεταφοράς δεδομένων κειμένου, σήμερα, με την συνεχή σχεδίαση νέων δεδομένων οι δυνατότητες του Διαδικτύου έχουν αυξηθεί τρομερά. Η μεταφορά φωνής και κινούμενης εικόνας είναι πλέον μια κοινή διαδικασία. Η ποιότητα της εξυπηρέτησης διαρκώς βελτιώνεται και ολοένα και περισσότερα δίκτυα συνδέονται σε αυτό. Καθώς νέοι χρήστες συνδέουν τα PC τους στο Διαδίκτυο, νέες εφαρμογές εμφανίζονται. Από τις πιο πρόσφατες υπηρεσίες του είναι το World Wide Web που αναπτύχθηκε στις αρχές τις δεκαετίας του ‘90.

Το World Wide Web είναι ένας τρόπος πρόσβασης σε πληροφορίες μέσω του Internet. Είναι ένα μοντέλο διαμοιρασμού πληροφοριών που είναι κτισμένο στην κορυφή του Internet. Πρόκειται για ένα σύστημα διασύνδεσης πληροφοριών σε μορφή πολυμέσων (*multimedia*) που βρίσκονται αποθηκευμένες σε χιλιάδες υπολογιστές του Internet σε ολόκληρο τον κόσμο και παρουσίασής τους σε ηλεκτρονικές σελίδες, στις οποίες μπορεί να περιηγηθεί κανείς χρησιμοποιώντας το ποντίκι. Επίσης έχουμε την προώθηση για την ανάπτυξη μιας μεγάλης κλίμακας εμπορικών πλέον εφαρμογών online, όπως οι τηλε-αγορές, το ηλεκτρονικό εμπόριο και υπηρεσίες μετάδοσης ήχου και κινούμενης εικόνας.

Η ανάπτυξη του ηλεκτρονικού εμπορίου είναι ένας σημαντικός παράγοντας της διάδοσης του Διαδικτύου, καθώς πλέον ολοένα και περισσότερες επιχειρήσεις και οργανισμοί ανά τον κόσμο διεκπεραιώνουν ένα μεγάλο αριθμό από εμπορικές συναλλαγές καθημερινώς με την χρήση του Διαδικτύου. Το ηλεκτρονικό εμπόριο αφορά κυρίως την αγοραπωλησία αγαθών, πληροφοριών και υπηρεσιών μέσα από δίκτυα ηλεκτρονικών υπολογιστών.

Εν όψη αυτής της εμπορικής εκμετάλλευσης του Διαδικτύου είναι ζωτικής σημασίας ο επαναπροσδιορισμός των κανόνων λειτουργίας του. Πολλές ευαίσθητες πληροφορίες ταξιδεύουν τώρα στο Διαδίκτυο, όπως αριθμοί πιστωτικών καρτών και άλλες προσωπικές πληροφορίες, που πρέπει να προστατευθούν από πιθανές υποκλοπές. Η ανοιχτή φύση του Διαδικτύου, έχει επιτρέψει σε ικανούς χρήστες να ερευνήσουν και να ανακαλύψουν αδυναμίες του, που συνδέονται με την μη παροχή προστασίας των επικοινωνούντων δεδομένων. Συνεπώς, η εκμετάλλευση του πρέπει να γίνεται με τέτοιο τρόπο ώστε σε καμία περίπτωση να μην διακινδυνεύονται οι εμπιστευτικές πληροφορίες των χρηστών.

Στόχος της παρούσας εργασίας είναι η αναφορά των πιθανών κινδύνων που αντιμετωπίζει ο μέσος χρήστης κατά τη διάρκεια μιας ηλεκτρονικής συναλλαγής καθώς και η παρουσίαση τρόπων αντιμετώπισής των.

Αρχικά, στα δύο πρώτα κεφάλαια της εργασίας κάνουμε μία εισαγωγή σε γενικότερες έννοιες όπως είναι το η-Επιχειρείν καθώς και το Ηλεκτρονικό Εμπόριο, το οποίο είναι η συνηθέστερη μορφή ηλεκτρονικών συναλλαγών.

Στη συνέχεια, στο Κεφάλαιο 3 παρουσιάζουμε μερικά ενδεικτικά μοντέλα ηλεκτρονικών πληρωμών καθώς και παραδείγματα τέτοιων μοντέλων στην ελληνική αγορά.

Στο Κεφάλαιο 4 παρουσιάζουμε εναλλακτικές μεθόδους με τις οποίες μπορούμε να διεκπεραιώσουμε μια ηλεκτρονική συναλλαγή. Επίσης γίνεται μία μικρή αναφορά σε διαδεδομένες μεθόδους ηλεκτρονικής απάτης.

Στο Κεφάλαιο 5, το οποίο είναι και η βασική ενότητα της παρούσας εργασίας, αναλύουμε την έννοια της Κρυπτογράφησης και τα είδη της και παρουσιάζουμε διάφορα κρυπτογραφικά εργαλεία. Επίσης περιγράφουμε τη διαδικασία αυθεντικοποίησης ενός μέλους σε ένα σύστημα επικοινωνίας με την χρήση της υποδομής δημόσιου κλειδιού (PKI). Ακόμη, γίνεται ανάλυση διαφόρων κρυπτογραφικών συστημάτων.

Τέλος, στο Κεφάλαιο 6 γίνεται η ανάλυση του SSL, ένα από τα ευρέως χρησιμοποιούμενα πρωτόκολλα κρυπτογράφησης στις μέρες μας.

Κεφάλαιο 1^{ο}: η-Επιχειρείν

Εισαγωγή

Τα τελευταία χρόνια έχει σημειωθεί μια σημαντική αλλαγή στον επιχειρηματικό κόσμο. Εταιρείες κάθε είδους και μεγέθους έκαναν μεγάλα άλματα στην αποδοχή των τεχνολογιών της πληροφορίας και των τηλεπικοινωνιών. Η πρόσβαση στο Διαδίκτυο και το ηλεκτρονικό ταχυδρομείο (*e-mail*) είναι σήμερα ένα αναπόσπαστο κομμάτι της εργασίας μας, ενώ τα ενδοδίκτυα εξωτερικής πρόσβασης (*extranets*) και η ηλεκτρονική ανταλλαγή δεδομένων έχουν αρχίσει να μεταλλάσσουν τις σχέσεις των προμηθευτών και των πελατών. Η πρόκληση που αντιμετωπίζουν τώρα οι επιχειρήσεις είναι η εξεύρεση τρόπων υποβοήθησης του προσωπικού τους, ώστε αυτό να αποκομίσει τα μέγιστα από τις υπάρχουσες τεχνολογίες. Επίσης, μέλημά τους είναι η προώθηση μεγαλύτερων επενδύσεων στις νέες τεχνολογίες, διατηρώντας παράλληλα την ισορροπία ανάμεσα στα οφέλη της υιοθέτησής τους και στο σχετικό κόστος και ρίσκο που αυτή συνεπάγεται.

Η έννοια e-Business (*ηλεκτρονικό Επιχειρείν*) στη συνείδησή μας έχει καταγραφεί με μία ευρεία ποικιλία ερμηνειών. Η ερμηνεία του η-Επιχειρείν σήμερα εμπίπτει σε δύο μεγάλες κατηγορίες.

- **Πρώτον** είναι η χρήση της τεχνολογίας για τον επανασχεδιασμό (reengineering) των επιχειρησιακών διαδικασιών, οι οποίες κυρίως είναι εσωτερικές στην επιχείρηση (internal focus).
- **Δεύτερον** συσχετίζει σαν ενδιάμεσο τεχνολογικό σύστημα την επιχείρηση με το εξωτερικό της περιβάλλον κυρίως προμηθευτές, προμηθευτική αλυσίδα, πελάτες (*external focus*). Για παράδειγμα ένα σύστημα το οποίο θα επιτρέπει στους πελάτες μιας επιχείρησης να συναλλάσσονται μέσω του internet ή να δημιουργεί ένα νέο επιχειρησιακό μοντέλο το οποίο αναφέρεται σαν «εικονική επιχείρηση» στους πελάτες.

Στην πραγματικότητα το e-Business εμπεριέχει πρωτοβουλίες που περιλαμβάνουν και τις δύο παραπάνω κατηγορίες.

Το e-Business απευθύνεται σε ένα ευρύ φάσμα επιχειρήσεων και οργανισμών. Μπορεί να προσαρμοστεί στις εξατομικευμένες ανάγκες και επιλογές των πελατών για να προσφέρει εφαρμογές βασισμένες στις τεχνολογικές λύσεις που ταιριάζουν σε κάθε μέλος της ψηφιακής οικονομίας.

Πολλές εταιρίες είδαν μεγάλες επενδύσεις στον τομέα του ηλεκτρονικού επιχειρείν να αποδίδουν ελάχιστα γιατί η ποιότητα των παρεχόμενων υπηρεσιών δεν ήταν υψηλή. Βασική παράμετρος ποιότητας αποτελεί η ευχρηστία η οποία προϋποθέτει την προσήλωση στις αρχές του άνθρωπο-κεντρικού σχεδιασμού. Είναι κοινά αποδεκτό ότι για τις αναπτυξιακές ομάδες διαδραστικών συστημάτων στον τομέα του ηλεκτρονικού επιχειρείν, η ευχρηστία έχει την ίδια βαρύτητα με άλλα κριτήρια ποιότητας λογισμικού, όπως είναι η λειτουργικότητα, η αξιοπιστία, η αποδοτικότητα, η συντηρησιμότητα και η μεταφερσιμότητα.

Μια επιχείρηση που είναι οργανωμένη γύρω από τις έννοιες ERP και CRM είναι μια e-επιχείρηση (e-business), η οποία προσαρμόζεται πιο γρήγορα στις αλλαγές της αγοράς, στις ανάγκες των καταναλωτών, λειτουργεί με το μικρότερο κόστος και χειρίζεται πιο σωστά και με ευελιξία τις σχέσεις της αγοράς έναντι των παραδοσιακών επιχειρήσεων.

1.1 Πρακτικές η-Επιχειρείν και Διοίκησης

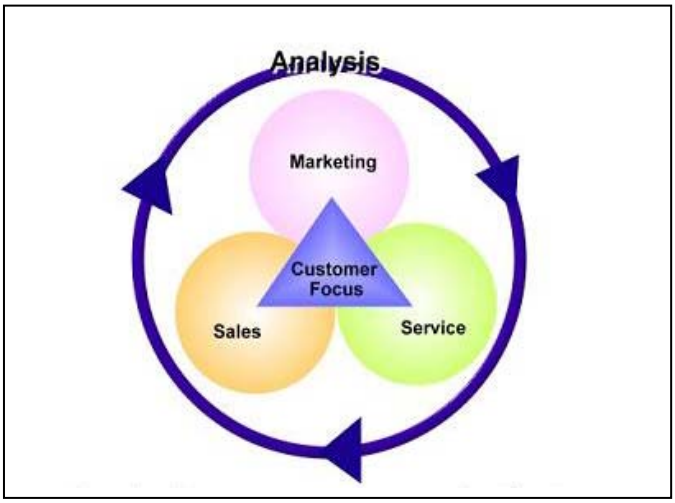
1.1.1 Διαχείριση πελατειακών σχέσεων (Customer Relationship Management --CRM)

Τα ποσοστά απώλειας πελατών είναι σήμερα υψηλότερα από ποτέ, και οι περισσότερες επιχειρήσεις δεν έχουν ακόμη βρει τον τρόπο να σταματήσουν την «αιμορραγία». Η αιτία είναι ότι μολονότι οι επιχειρήσεις δηλώνουν προσηλωμένες στην «αφοσίωση» των πελατών τους, τα

συστήματα διοίκησης και οι προϋπολογισμοί τους δεν φαίνεται να συνηγορούν σε αυτό.

Μια πρόσφατη έρευνα σε 352 ανώτερα διευθυντικά στελέχη σχετικά με τις απόψεις τους για τις επιπτώσεις του Internet στη δυνατότητα διαχείρισης των πελατειακών τους σχέσεων (CRM, Customer Relationships Management), προσφέρει αρκετά πειστικά στοιχεία ότι οι ανησυχίες (ως προς το ότι τα περιθώρια κέρδους και η αφοσίωση των καταναλωτών θα περιορίζονταν με τη χρήση του Διαδικτύου), υποχωρούν.

Ένα σύστημα CRM θα μπορούσε να οριστεί ως, ένα σύστημα κανόνων και μια συλλογή από συστήματα και τεχνολογίες πληροφορικής που εστιάζονται στην αυτοματοποίηση και βελτίωση των επιχειρηματικών διαδικασιών που σχετίζονται με τη διαχείριση των σχέσεων με τους πελάτες και έχουν σχέση με τα τμήματα των πωλήσεων, marketing, εξυπηρέτησης και υποστήριξης πελατών (*Σχήμα 1.1*).



Σχήμα 1.1 Σύστημα CRM

Οι στρατηγικές διαχείρισης πελατειακών σχέσεων δίνουν έμφαση στη στενότερη σύνδεση με τους πελάτες, ενώ οι πρωτοπόροι στο χώρο οργανισμοί αναμένεται να αξιοποιήσουν το Internet για να ενισχύσουν το

συγκριτικό αυτό πλεονέκτημα. Προκειμένου μια επιχείρηση να αξιολογήσει τις πιθανότητες που υπάρχουν να ωφεληθεί ή να χάσει τη «μάχη» στο χώρο της διαχείρισης πελατειακών σχέσεων, θα πρέπει να συνεκτιμήσει τα παρακάτω:

- Οι πρωτοπόροι στο χώρο της Διαχείρισης Πελατειακών Σχέσεων (CRM) σίγουρα θα αξιοποιήσουν το Διαδίκτυο για να ενισχύσουν τη διαφορά τους από τους υπόλοιπους.
- Ο αντίκτυπος από το μετασχηματισμό που θα προκύψει από τα νέα μοντέλα αγορών θα είναι μικρής κλίμακας.
- Το Internet θα λειτουργήσει συμπληρωματικά στα υφιστάμενα κανάλια διανομής.

Ενδεικτικά οφέλη των συστημάτων CRM:

- Απόκτηση νέων πελατών, ελάττωση των παραπόνων πελατών, αύξηση της πελατειακής πίστης.
- Μείωση κόστους και αύξηση εσόδων. Η μείωση του κόστους επέρχεται λόγω της άμεσης παροχής των συγκεκριμένων υπηρεσιών.
- Παροχή ολοκληρωμένης άποψης για τον πελάτη και για το κατάλληλο επίπεδο πληροφοριών που θα οδηγήσει στην επίλυση τυχόν προβλημάτων.
- Μεγιστοποίηση της αποτελεσματικότητας και παραγωγικότητας όλων των καναλιών επικοινωνίας και διασφάλιση συνέπειας στην εξυπηρέτηση από όλα τα κανάλια.
- Αυτόματη αναγνώριση των ευκαιριών πώλησης συμπληρωματικών ή συνδυαστικών προϊόντων με βάση το προφίλ των πελατών.
- Παροχή του υψηλότερου βαθμού ακριβείας και αξιοπιστίας στο σχεδιασμό και τη λήψη αποφάσεων.
- Διευκόλυνση της επικοινωνίας και της κοινής χρήσης πληροφοριών μεταξύ των τμημάτων πωλήσεων, εξυπηρέτησης και marketing.

1.1.2 Συστήματα Διαχείρισης Επιχειρησιακών Πόρων (Enterprise Resource Planning -- ERP)

Τα Συστήματα Διαχείρισης Επιχειρησιακών Πόρων (ERP) αποτελούν ολοκληρωμένα πληροφοριακά συστήματα που έχουν στόχο την υποστήριξη όλων των επιχειρησιακών δραστηριοτήτων. Τα συστήματα αυτά ενοποιούν όλες τις σημαντικές δραστηριότητες της επιχείρησης καθώς και όλες τις διαδικασίες σε ένα κεντρικό σύστημα ελέγχου που παρέχει μια συνολική εικόνα για την λειτουργία της επιχείρησης.

Την σημερινή εποχή, τα ERP διαδραματίζουν σπουδαίο ρόλο στην υποστήριξη της επιχειρηματικής δράσης, αφού αυτοματοποιούν τις λειτουργίες της επιχείρησης και ενοποιούν τις επιχειρηματικές διαδικασίες μέσα από μια κοινή βάση δεδομένων. Η δομή ενός συστήματος ERP αποτελείται από λειτουργικά προγράμματα επιτρέποντας στην επιχείρηση να εγκαταστήσει μόνο εκείνα που κρίνει ότι της είναι απαραίτητα.

Ένα σύστημα ERP είναι ένα ολοκληρωμένο πληροφοριακό σύστημα που παρέχει τη δυνατότητα επικοινωνίας μεταξύ όλων των τμημάτων μιας επιχείρησης. Ένα σύστημα ERP επιτελεί ουσιαστικά προσομοίωση της πραγματικότητας των καθημερινών πρακτικών. Οι λόγοι που οι επιχειρήσεις προμηθεύονται συστήματα ERP είναι οι εξής:

1. Συγκρότηση όλων των μηχανογραφικών διαδικασιών κάτω από ένα ενιαίο μηχανογραφικό σύστημα.
2. Αύξηση της παραγωγικότητας και της αποδοτικότητας.
3. Βελτίωση της ποιότητας.
4. Ολοκλήρωση επιχειρησιακών διαδικασιών.
5. Μείωση κόστους σε όλη την εφοδιαστική αλυσίδα (αποθεμάτων, προμηθειών, logistics, πληροφοριακών πόρων).
6. Ακεραιότητα και ακρίβεια πληροφοριών.
7. Ταχύτητα.
8. Βασική υποδομή για διευρυμένη επιχείρηση (extended enterprise) και e-business.

Τα κυριότερα προβλήματα που παρουσιάζονται στην εγκατάσταση ενός ERP είναι: οι απαιτήσεις σε εκπαιδευμένο και εξειδικευμένο προσωπικό, η υιοθέτηση νέων τεχνολογιών, το υψηλό κόστος καθώς και η ανάγκη επιχειρησιακής αναδιοργάνωσης. Μπορούμε δηλαδή σε γενικές γραμμές να κατατάξουμε τα προβλήματα των συστημάτων ERP σε τέσσερις μεγάλες κατηγορίες:

1) τεχνολογικά,
2) οργανωτικά,
3) οικονομικά και
4) ανθρώπινου δυναμικού.

Στην Ελλάδα, την σημερινή εποχή, πολλές εταιρίες πληροφορικής έχουν στρέψει τη στρατηγική τους στην ανάπτυξη ERP συστημάτων. Μερικές από αυτές είναι: LogicDIS, SAP, SINGULAR, Altec.

Κεφάλαιο 2ο: Ηλεκτρονικό Εμπόριο

Εισαγωγή

Το ηλεκτρονικό εμπόριο αποτελεί αναπόσπαστο κομμάτι του παγκοσμίου εμπορίου στις ημέρες μας. Για πολλούς θεωρείται ίσως η δεύτερη μεγαλύτερη τεχνολογική εξέλιξη μετά τη βιομηχανική επανάσταση, καθώς εξοικονομεί χρόνο και χρήμα και μπορεί να μεταμορφώσει μια μικρή εταιρία ακόμα και σε κολοσσό. Αυτή τη στιγμή περισσότεροι από 40.000.000 άνθρωποι σε όλο τον κόσμο δραστηριοποιούνται στο ηλεκτρονικό εμπόριο και σε πολύ λίγα χρόνια ο αριθμός αυτός αναμένεται να αυξηθεί ραγδαία. Υπολογίζεται πως το αργότερο σε 10 χρόνια όλες οι συναλλαγές θα γίνονται ηλεκτρονικά. Με άλλα λόγια, το ηλεκτρονικό εμπόριο είναι το εμπόριο του μέλλοντος.

Όσο αφορά την Ελλάδα, το ηλεκτρονικό εμπόριο δείχνει να προχωρά με κάπως αργά βήματα, αν και τα τελευταία χρόνια αναπτύσσεται σταθερά. Σε άλλα σημεία του πλανήτη, στα οποία η διείσδυση του Διαδικτύου στην καθημερινή ζωή είναι μεγάλη, η σύγχρονη αυτή μορφή αγοράς εμφανίζει αλματώδη άνοδο.

2.1 Τι είναι το ηλεκτρονικό εμπόριο

Πρόκειται για μια νέα επιχειρηματική πρακτική. Σύγχρονες τεχνολογίες και μέθοδοι συνδυάζονται προκειμένου οι επιχειρήσεις να αυξήσουν την αξία τους να ελαχιστοποιήσουν τα κόστη τους και να μεγιστοποιηθεί η δυνατότητα προσέγγισης όσο το δυνατό περισσότερων πελατών.

Πιο ειδικά θα μπορούσαμε να πούμε ότι, **ηλεκτρονικό εμπόριο** εννοείται κάθε εμπορική συναλλαγή, η οποία εκτελείται αποκλειστικά σε ηλεκτρονικό επίπεδο, δηλαδή με τη χρήση ηλεκτρονικών υπολογιστών που συνδέονται μέσω τηλεφωνικών γραμμών. Για την πραγματοποίηση μιας τέτοιας συναλλαγής χρησιμοποιούνται πολύπλοκοι προγραμματιστικοί

μηχανισμοί και το κατάλληλο λογισμικό το οποίο επιτρέπει την Ηλεκτρονική Ανταλλαγή Δεδομένων (Electronic Data Interchange- EDI) ανάμεσα στις δύο πλευρές (μεταξύ επιχειρήσεων αλλά και μεταξύ επιχειρήσεων και καταναλωτών) που εμπλέκονται στη συγκεκριμένη συναλλαγή.

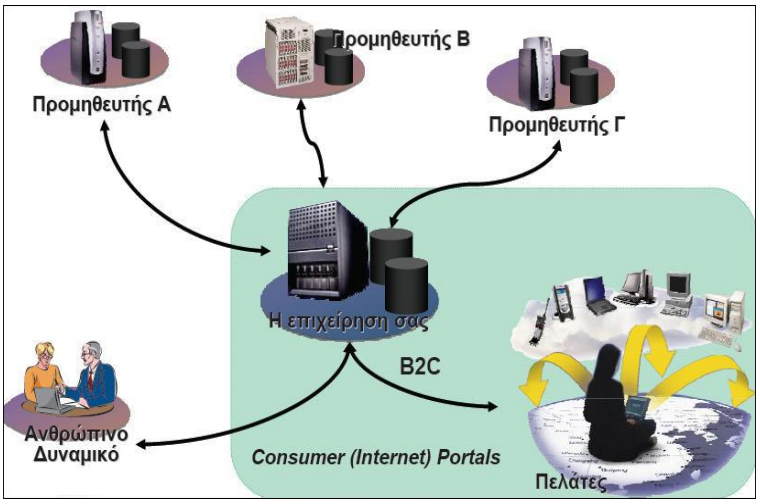
2.2 Τεχνολογική προσέγγιση του ηλεκτρονικού εμπορίου

Στο σημείο αυτό θα ορίσουμε το μέσο επικοινωνίας πάνω στο οποίο θα λειτουργήσει το τεχνολογικό μοντέλο κάθε εφαρμογής ηλεκτρονικού εμπορίου. Οι βασικές κατηγορίες των μέσων, που χρησιμοποιούνται για τις διάφορες εφαρμογές ηλεκτρονικού εμπορίου, είναι τρεις και χαρακτηρίζονται ως το Τηλεπικοινωνιακό Επίπεδο. Στο επίπεδο αυτό περιλαμβάνονται οι εναλλακτικοί μηχανισμοί διασύνδεσης των επιχειρηματικών εταίρων που διεκπεραιώνουν ηλεκτρονικές συναλλαγές.

Οι κατηγορίες αυτές είναι οι εξής:

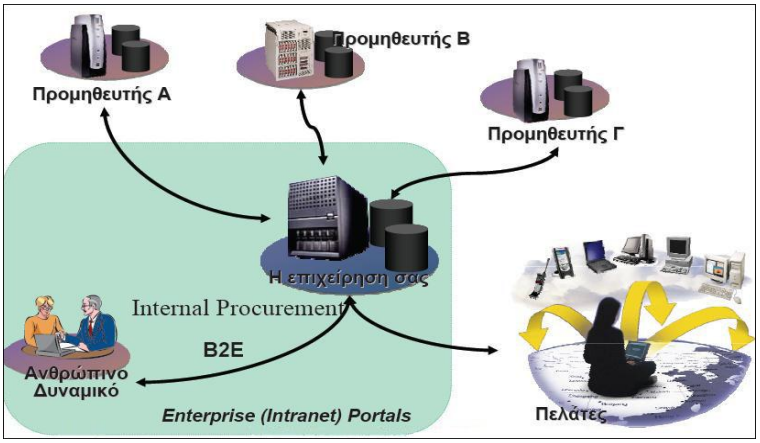
1. **Internet.** Το Internet θεωρείται ως το πιο διαδεδομένο μέσο για τις εφαρμογές του ηλεκτρονικού εμπορίου καθώς έχει πλέον κερδίσει το ενδιαφέρον όλων των επιχειρήσεων. Η εξέλιξη των εφαρμογών του και η βελτίωση της αξιοπιστίας του από πλευράς ασφάλειας και διαθεσιμότητας μετέτρεψε το Internet σε ένα πρόσφορο μέσο για ηλεκτρονικές συναλλαγές. Τα τελευταία χρόνια έχει αναπτυχθεί ένας μεγάλος αριθμός αξιόλογων εφαρμογών, οι οποίες βασίζονται στο Διαδίκτυο και έχουν ως κύριο μέλημά τους την υποστήριξη επιχειρήσεων σε διάφορους τομείς όπως αυτός της πώλησης προϊόντων, της παράδοσης υπηρεσιών καθώς και σ' αυτόν της διαφήμισης. Κύριος λόγος της εξάπλωσης του Διαδικτύου σε παγκόσμια κλίμακα είναι το μικρό κόστος καθώς και το γραφικό περιβάλλον που χρησιμοποιείται για την διεπαφή του χρήστη με τις διάφορες υπηρεσίες που προσφέρει το Διαδίκτυο (Graphical User

Interface, GUI). Εντούτοις η έλλειψη ασφάλειας και η μη ύπαρξη ενός κεντρικού διαχειριστή που θα εγγυάται την ποιότητα της υπηρεσίας μπορούν να σημειωθούν ως τα μειονεκτήματα του Internet.



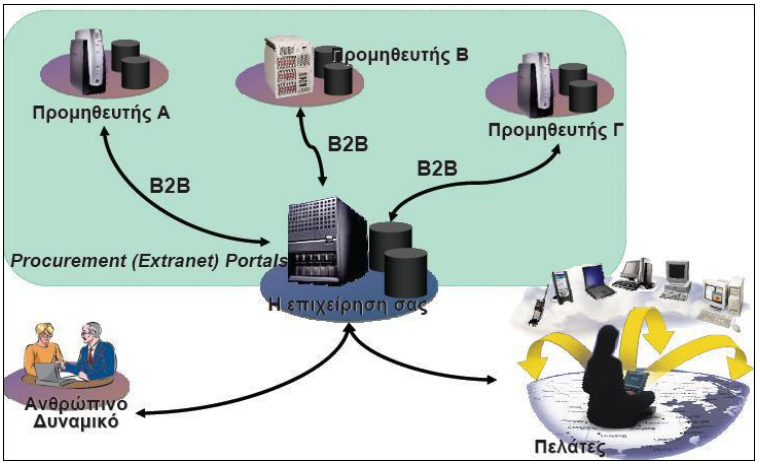
Σχήμα 2.1 Συστατικά Ηλεκτρονικού Εμπορίου (Internet)

2. **Intranet.** Μοιάζει με το Internet, λειτουργεί περίπου το ίδιο, με τη διαφορά ότι απευθύνεται σε πολύ λιγότερους χρήστες και είναι ιδιωτικό. Το Intranet είναι ένα δίκτυο υπολογιστών που βρίσκεται εγκατεστημένο σε μια επιχείρηση, προκειμένου να εξυπηρετήσει τις ανάγκες της για εσωτερική πληροφόρηση και οργάνωση. Αποτελείται από ηλεκτρονικούς υπολογιστές οι οποίοι συνδέονται μεταξύ τους. Τα Intranets, αν και δεν είναι τοπικά δίκτυα, προσφέρουν υπηρεσίες όπως η κοινή χρήση περιφερειακών (πχ εκτυπωτές) μέσω διαφόρων πρωτοκόλλων επικοινωνίας, τα οποία χρησιμοποιούνται και στο Internet, όπως το TCP/IP, HTTP. Λόγω των ομοιοτήτων αυτών, το Intranet αποκαλείται και «Internet της επιχείρησης». Τέλος πρέπει να αναφέρουμε ότι βασικό πλεονέκτημα του Intranet απέναντι στο Internet είναι η ασφάλεια.



Σχήμα 2.2 Συστατικά Ηλεκτρονικού Εμπορίου (Intranet)

3. **Extranet.** Το Extranet (στα ελληνικά θα μπορούσε να αποδοθεί ως «εξωδίκτυο») είναι εκείνο το κομμάτι του Intranet το οποίο μπορεί να προσεγγιστεί από πελάτες, προμηθευτές και εξωτερικούς συνεργάτες της εταιρίας μέσω Διαδικτύου, με τη χρήση κωδικού πρόσβασης. Ουσιαστικά πρόκειται για ένα μικρό ιδιωτικό τοπικό δίκτυο που επικοινωνεί τόσο με το Intranet όσο και με το Internet, ευρισκόμενο στο μέσο και λειτουργώντας συνδετικά. Ως κατασκευή έχει παρόμοια χαρακτηριστικά με το Intranet, με τη διαφορά ότι για τη δημιουργία του απαιτείται πρόσθετο υλικό (hardware) και λογισμικό (software), όπως firewalls και δρομολογητές (routers).



Σχήμα 2.3 Συστατικά Ηλεκτρονικού Εμπορίου (Extranet)

2.3 Σύγκριση των ειδών δικτύων

Όπως είναι φανερό καμία από τις παραπάνω κατηγορίες δικτύων δεν υπερτερεί, σε γενικές γραμμές, των άλλων καθώς η καθεμία από αυτές έχει σχεδιαστεί με κριτήριο κάθε φορά τις ανάγκες της εφαρμογής. Ο *Πίνακας 2.1* δείχνει συνοπτικά μερικά από τα χαρακτηριστικά των τριών αυτών κατηγοριών.

Χαρακτη-ριστικό	INTERNET	EXTRANET	INTRANET
Τύπος η-Εμπορίου	Business-to-Consumer	Business-to-Business	Εσωτερικός Εφοδιασμός
Προσπέλαση Δεδομένων	Απεριόριστη	Περιορισμένη	Περιορισμένη
Ασφάλεια	Ελάχιστη	Firewalls & Περιορισμένη Πρόσβαση	Firewalls & Περιορισμένη Πρόσβαση
Τρόπος Πληρωμής	Πιστωτική Κάρτα	Προκαθορισμένη Συμφωνία Πίστωσης	Στις Χρεώσεις της Εταιρείας

Πίνακας 2.1 Σύγκριση των Internet, Intranet και Extranet

2.4 Υλοποίηση του Ηλεκτρονικού Εμπορίου

Παρόλο που είναι εύκολο να περιγράψεις τα πλεονεκτήματα των εμπορικών συστημάτων, δεν είναι το ίδιο εύκολο να τα αναπτύξεις καθώς ούτε και να τα παρατάξεις. Κάθε εταιρία, που θα επιχειρήσει να αναπτύξει ένα εμπορικό σύστημα, θα έρθει αντιμέτωπη με σημαντικά ζητήματα υλοποίησής του. Μερικά από αυτά είναι τα εξής:

1. **Κόστος (Cost)**: Το ηλεκτρονικό εμπόριο απαιτεί ουσιώδεις επενδύσεις σε νέες τεχνολογίες, οι οποίες να επηρεάσουν θετικά τις βασικές λειτουργίες μιας επιχείρησης. Όπως συμβαίνει με όλα τα βασικά συστήματα μιας επιχείρησης, έτσι και το σύστημα του ηλεκτρονικού εμπορίου απαιτεί σημαντικές επενδύσεις σε υλικό (hardware), λογισμικό (software), στελέχωση (staffing) και εκπαίδευση (training) του προσωπικού. Οι επιχειρήσεις χρειάζονται μεγάλο εύρος λύσεων με

μεγαλύτερη ευκολία χρήσης, έτσι ώστε να είναι σε θέση να αναπτύξουν οικονομικώς αποδοτικά μέτωπα.

2. **Αξία (Value)**: Οι επιχειρήσεις πρέπει να γνωρίζουν ότι οι επενδύσεις, που θα πραγματοποιήσουν στο σύστημα του ηλεκτρονικού εμπορίου, θα αποφέρουν κέρδος. Οι αντικειμενικοί στόχοι μιας επιχείρησης όπως η δημιουργία πρωτοτυπίας (lead generation), ο αυτοματισμός των επιχειρησιακών διαδικασιών (business-process automation) καθώς και η μείωση του κόστους (cost reduction) πρέπει οπωσδήποτε να επιτυγχάνονται. Συστήματα τα οποία χρησιμοποιούνται για την επίτευξη των σκοπών αυτών, απαιτείται να είναι αρκετά ευέλικτα σε πιθανές αναπροσαρμογές της επιχείρησης.
3. **Ασφάλεια (Security)**: Η χρησιμοποίηση του Διαδικτύου παρέχει παγκόσμια άδεια εισόδου, έτσι η επιχείρηση πρέπει να παρέχει προστασία στα περιουσιακά της στοιχεία, σε περίπτωση κάποιας απροσδόκητης ή κακόβουλης ενέργειας. Ωστόσο η ασφάλεια του συστήματος δεν πρέπει να δημιουργεί πολυπλοκότητα ή να μειώνει την ευελιξία του συστήματος. Οι πληροφορίες των πελατών πρέπει να προστατεύονται από εσωτερικές ή εξωτερικές κακόβουλες χρήσεις.
4. **Αύξηση κεφαλαίου του υπάρχοντος συστήματος (Leveraging Existing Systems)**: Οι περισσότερες επιχειρήσεις χρησιμοποιούν την Πληροφορική, (information technology -- IT) για να διαχειρίζονται τις αρμοδιότητές τους, σε περιβάλλοντα που δεν έχουν σχέση με το Διαδίκτυο, όπως το Marketing, η διαχείριση παραγγελιών (order management), η εξόφληση λογαριασμών (billing), η απογραφή (inventory), η διανομή (distribution) και η εξυπηρέτηση πελατών (customer service). Το Διαδίκτυο αποτελεί έναν εναλλακτικό και συμπληρωματικό τρόπο για την πραγματοποίηση επιχειρηματικής δραστηριότητας, αλλά είναι κανόνας ότι τα συστήματα ηλεκτρονικού εμπορίου ενοποιούν τα υπάρχοντα συστήματα με αποτέλεσμα την αποφυγή παρόμοιων λειτουργικοτήτων και την επικράτηση ευχρηστίας, αποδοτικότητας και αξιοπιστίας.

5. **Διαλειτουργικότητα (Interoperability)**: Η ανταλλαγή πληροφοριών μεταξύ δύο ή περισσοτέρων επιχειρήσεων, δίχως χειρωνακτική επέμβαση έχει ως αποτέλεσμα την μείωση του κόστους, την βελτίωση της απόδοσης και την ενδυνάμωση των αλυσίδων αξίας (value chains). Η αποτυχία διεύθυνσης οποιουδήποτε από τα παραπάνω, θα έχει ως αποτέλεσμα και την αποτυχία οποιασδήποτε προσπάθειας υλοποίησης του συστήματος. Επομένως, η εμπορική στρατηγική των εταιρειών, θα πρέπει να σχεδιάζεται με τέτοιο τρόπο, ώστε να είναι σε θέση η εταιρία να διαχειριστεί όλα αυτά τα θέματα. Με αυτόν τον τρόπο η εταιρία θα βοηθήσει τους πελάτες της να εκμεταλλευθούν τα οφέλη που προσφέρει το ηλεκτρονικό εμπόριο.

2.5 Πλεονεκτήματα του Ηλεκτρονικού Εμπορίου

2.5.1 Πλεονεκτήματα του ηλεκτρονικού εμπορίου για τον καταναλωτή

Πολλά είναι τα πλεονεκτήματα που προσφέρει το ηλεκτρονικό εμπόριο στον καταναλωτή. Παρακάτω παραθέτουμε μερικά απ' αυτά:

1. Τα ηλεκτρονικά καταστήματα είναι ανοιχτά 24 ώρες το 24ωρο. Με άλλα λόγια ο εκάστοτε αγοραστής οποιαδήποτε στιγμή το επιθυμεί, μπορεί ν' αγοράσει π.χ. ένα CD, ένα αεροπορικό εισιτήριο, βιβλία κ ά.
2. Το κόστος των προϊόντων που πωλούνται μέσω Internet είναι κατά γενικό κανόνα πολύ χαμηλότερο από τις τιμές του εμπορίου, αφού ένα ηλεκτρονικό κατάστημα είναι απαλλαγμένο από μεγάλο μέρος του λειτουργικού κόστους ενός πραγματικού καταστήματος (ενοικίαση χώρου, ηλεκτρικό, νερό κλπ.) και γενικά απαιτεί πολύ λιγότερο υπαλληλικό προσωπικό.
3. Η αγορά είναι πραγματικά παγκόσμια. Με άλλα λόγια, είναι δυνατό μέσω του υπολογιστή να γίνονται αγορές προϊόντων τα οποία δεν κυκλοφορεί για παράδειγμα στην Ελλάδα.

4. Η συναλλαγή είναι γρήγορη και άμεση. Με άλλα λόγια, από την ολοκλήρωση της παραγγελίας, η παραλαβή πραγματοποιείται μέσα σε μικρό χρονικό διάστημα.
5. Αλλά το πιο πρακτικό και πιο σημαντικό όφελος για τον καταναλωτή από το ηλεκτρονικό εμπόριο είναι το ότι: Ο καθένας βρίσκει αυτό που θέλει, όποτε το θέλει, χωρίς να κάνει βήμα, χωρίς δηλαδή κόπο και χωρίς καμία σπατάλη χρόνου.

2.5.2 Πλεονεκτήματα του ηλεκτρονικού εμπορίου για την εταιρία

Πολλά είναι τα πλεονεκτήματα και για την εταιρία. Παραθέτουμε μερικά από αυτά:

1. Κάθε εταιρία που έχει ηλεκτρονική παρουσία μπορεί να διευρύνει τον κύκλο εργασιών της επεκτείνοντας τα γεωγραφικά όρια των συναλλαγών της. Αυτό σημαίνει πως κάθε επιχείρηση που διαθέτει τα προϊόντα της online μπορεί και αποκτά πελάτες σε περιοχές που βρίσκονται μακριά από την έδρα της, ακόμα και στο εξωτερικό. Με άλλα λόγια, κάθε επιχείρηση που έχει ένα ηλεκτρονικό κατάστημα, είναι σαν να έχει υποκαταστήματα σε πολλές περιοχές και μάλιστα με ελάχιστο λειτουργικό κόστος.
2. Κάθε εταιρία που χρησιμοποιεί τις νέες τεχνολογίες- όπως το Internet- γίνεται εξ ορισμού πιο ανταγωνιστική, αφού μπορεί να ενημερώνεται πιο εύκολα για τις τρέχουσες εξελίξεις στο χώρο της. Με άλλα λόγια και με δεδομένο το ότι σε λίγα χρόνια όλες οι εμπορικές δραστηριότητες θα γίνονται μέσω Internet, το ηλεκτρονικό εμπόριο είναι η νέα μεγάλη πρόκληση για κάθε εταιρία που θέλει να είναι ανταγωνιστική.
3. Οι ηλεκτρονικές συναλλαγές επιτρέπουν την αμφίδρομη σχέση μεταξύ επιχείρησης και καταναλωτή (interaction). Αυτό σημαίνει πως κάθε εταιρία μέσω των ηλεκτρονικών συναλλαγών μπορεί να συλλέξει

πολλά στοιχεία για τις συνήθειες, τις ανάγκες και τις προτιμήσεις των καταναλωτών και σύμφωνα με αυτά να αναπροσαρμόσει την πολιτική της προς το θετικότερο.

4. Τέλος, γνωρίζοντας τις συγκεκριμένες ανάγκες των πελατών τους, οι εταιρίες μπορούν να προχωρήσουν στη δημιουργία συγκεκριμένων προϊόντων είτε ανταποκρινόμενων σ' έναν καταναλωτή, είτε σε μια ομάδα καταναλωτών που χρειάζονται ένα νέο προϊόν το οποίο δεν υπάρχει ακόμα στην αγορά.

2.6 Κατάσταση του Ηλεκτρονικού Εμπορίου σε παγκόσμια κλίμακα

Με ραγδαίους ρυθμούς συνεχίζει να αναπτύσσεται διεθνώς το ηλεκτρονικό εμπόριο, σύμφωνα με πρόσφατη έρευνα που πραγματοποίησε η Forester Research για λογαριασμό του Shop.org, του ψηφιακού παραρτήματος της Εθνικής Ομοσπονδίας Λιανοπωλητών των ΗΠΑ. Σύμφωνα με τα ευρήματα της έρευνας, το ηλεκτρονικό εμπόριο συνεχίζει να αναπτύσσεται με διψήφιους ρυθμούς ανάπτυξης, οι οποίοι το 2006 ξεπέρασαν τις πιο αισιόδοξες προβλέψεις και ανήλθαν στο 25%. Το ποσοστό αυτό είναι υψηλότερο κατά πέντε ποσοστιαίες μονάδες σε σχέση με την αρχική πρόβλεψη. Θα πρέπει πάντως να σημειωθεί ότι αναμένεται μία σχετική ύφεση αυτών των ρυθμών ανάπτυξης μέσα στα επόμενα χρόνια, καθώς η αγορά αρχίζει να ωριμάζει όλο και περισσότερο. Ενδεικτικά αναφέρεται ότι ο ρυθμός ανάπτυξης των online πωλήσεων το 2007 αναμένεται να αυξηθεί κατά 18% σε σχέση με το προηγούμενο έτος, με τη συνολική αξία τους όμως να αυξάνεται περαιτέρω.

Παράλληλα έχουμε και την συνεχή αύξηση του ανταγωνισμού μεταξύ των εταιρειών που δραστηριοποιούνται στο ηλεκτρονικό εμπόριο. Οι περισσότερες από τις μεγάλες εταιρείες που δραστηριοποιούνται στο ηλεκτρονικό εμπόριο έγιναν 10 χρόνων πρόσφατα. Σε αυτές περιλαμβάνονται η eBay, η Yahoo και η Amazon.com που κατάφεραν να

επιβιώσουν από τα πολλά προβλήματα που αντιμετώπισε ο κλάδος, ιδιαίτερα μετά την πτώση των μετοχών του κλάδου της τεχνολογίας το 2000. Στόχος αυτών των μεγάλων εταιρειών και των ανταγωνιστών τους είναι πλέον να καταφέρουν να προσελκύσουν ακόμη περισσότερους χρήστες του Ίντερνετ, οι οποίοι θα αναζητήσουν τα διαθέσιμα μέσω Διαδικτύου προϊόντα και θα τα αγοράσουν. Δεν είναι τυχαίο ότι στο παιχνίδι του ηλεκτρονικού εμπορίου προσπαθεί τώρα να μπει και η Google, κίνηση που αν τελικά πραγματοποιηθεί μπορεί να αλλάξει τον χάρτη.

Στην **Ευρώπη,** ειδικότερα, όλο και περισσότεροι πολίτες προχωρούν σε διασυνοριακές αγορές, καθιστώντας το ηλεκτρονικό εμπόριο ως έναν ιδιαίτερα δημοφιλή τρόπο αγοράς προϊόντων. Σύμφωνα με τα στοιχεία του Ευρωβαρόμετρου, το 26% των πολιτών στους «25» έχει προβεί, τουλάχιστον, σε μια διασυνοριακή αγορά τους τελευταίους 12 μήνες. Σε ότι αφορά το ηλεκτρονικό εμπόριο τους τελευταίους 12 μήνες στην Ε.Ε., το 50% των ατόμων που διαθέτουν στο σπίτι πρόσβαση στο διαδίκτυο αγόρασε ένα προϊόν ή μία υπηρεσία.

Επίσης, στις **ΗΠΑ** παρατηρείται αύξηση στο τζίρο του ηλεκτρονικού εμπορίου, φέρνοντας τον κλάδο όλο και πιο κοντά σε φάση ωρίμανσης. Όπως δείχνει έρευνα της eMarketer, οι καταναλωτές ψωνίζουν όλο και περισσότερο online και μάλιστα δεν αγοράζουν απλώς περισσότερα από τα προϊόντα που είθισται να αγοράζει κανείς μέσω Διαδικτύου, αλλά αγοράζουν πλέον και αγαθά μεγαλύτερης αξίας. Σύμφωνα με τις εκτιμήσεις της eMarketer, μεταξύ 2005 και 2009 ο τζίρος του ηλεκτρονικού λιανεμπορίου θα σημειώσει ετήσια αύξηση της τάξεως του 18,6%. Πρόκειται για εκτίμηση που σηματοδοτεί δυναμική ανάπτυξη του κλάδου, ωστόσο δείχνει πως το e-commerce επιβραδύνει, αφού η αντίστοιχη ετήσια αύξηση μεταξύ 2001 και 2005 ήταν 26%. Η πτώση αυτή δεν θα πρέπει να προκαλέσει ανησυχία αφού όπως επισημαίνουν πολλοί έμπειροι αναλυτές δεν είναι παρά ένα σημάδι ωρίμανσης του ηλεκτρονικού λιανεμπορίου.

Στην **Ελλάδα**, τέλος, οι αναλυτές περιμένουν «έκρηξη» του ηλεκτρονικού εμπορίου. Ακόμα και σήμερα, ο «τυπικός» Έλληνας μικρομεσαίος επιχειρηματίας βρίσκεται σε κατάσταση σύγχυσης όσον αφορά την εικόνα που έχει στο μυαλό του για όρους όπως «ηλεκτρονικό εμπόριο» και «νέες τεχνολογίες». Παράγοντες όπως η οικονομική ύφεση, οι αβέβαιες παγκόσμιες οικονομικές εξελίξεις, ο βομβαρδισμός του από την τεχνολογική επανάσταση, η όξυνση του ανταγωνισμού, διαμορφώνουν δυσνόητες συνθήκες, οι οποίες αφήνουν λιγοστά περιθώρια για εκτίμηση των μελλοντικών εξελίξεων και προσαρμογή σε αυτές από τους μικρομεσαίους Έλληνες επιχειρηματίες.

Σύμφωνα με τις τελευταίες έρευνες πάντως οι αυξητικές τάσεις στις αγορές μέσω Διαδικτύου που παρατηρούνται μεταξύ των Ελλήνων καταναλωτών τα τελευταία δύο χρόνια αναμένεται να συνεχιστούν, και γι' αυτό όλο και περισσότερες επιχειρήσεις επιλέγουν να χρησιμοποιήσουν το Internet ως ένα ακόμη μέσο διανομής των προϊόντων τους.

Ωστόσο, τον τελευταίο ενάμιση χρόνο έχουν γίνει τα πρώτα βήματα στην υιοθέτηση στρατηγικών B2B (Business-to-Business) στην Ελλάδα. Ήδη, περισσότερες από οκτώ στις δέκα μεγάλες ελληνικές επιχειρήσεις έχουν δική τους ιστοσελίδα στο Διαδίκτυο, ενώ οι δύο στις δέκα δραστηριοποιούνται και στο ηλεκτρονικό εμπόριο. Αυτό προκύπτει μεταξύ άλλων από έρευνα που πραγματοποιήθηκε από το Εργαστήριο Μάρκετινγκ του Οικονομικού Πανεπιστημίου Αθηνών για λογαριασμό του Εθνικού Δικτύου Έρευνας και Τεχνολογίας μεταξύ των 500 μεγαλύτερων ελληνικών επιχειρήσεων. Η έρευνα δείχνει ότι όλες ανεξαιρέτως οι εταιρείες επενδύουν στις νέες τεχνολογίες. Όλες οι εταιρείες του δείγματος χρησιμοποιούν το Διαδίκτυο, ενώ οι επτά στις δέκα εταιρείες έχουν πλήρη διασύνδεση. Βασικοί λόγοι της χρήσης του Διαδικτύου, σύμφωνα με τα αποτελέσματα της έρευνας, είναι η αναζήτηση πληροφοριών και η ενημέρωση, καθώς και οι συναλλαγές με τις τράπεζες και το Δημόσιο.

2.7 Τεχνολογίες για το ηλεκτρονικό εμπόριο

Οι περισσότερες από τις τεχνολογίες του ηλεκτρονικού εμπορίου χρησιμοποιούνται εδώ και αρκετά χρόνια από συγκεκριμένες επιχειρήσεις ή κλάδους. Αυτό που τις έδωσε την απαιτούμενη ώθηση και έκανε την αντιμετώπισή τους ενιαία, κάτω από τη μορφή του ηλεκτρονικού εμπορίου, ήταν η αποδοχή διεθνών προτύπων και η ανάγκη για νέες μορφές οργάνωσης και λειτουργικής διαχείρισης. Έτσι, οι επιχειρήσεις θα μπορούσαν στο εξής να ανταπεξέλθουν στις συνθήκες που επιβάλλονται από τη διεθνοποίηση των αγορών, τις νέες καταναλωτικές αντιλήψεις και κοινωνικές συνθήκες.

Σε ότι αφορά την τεχνολογία και τις τηλεπικοινωνίες, υπάρχουν σήμερα πολλές εναλλακτικές δυνατότητες για την υποστήριξη εφαρμογών Ηλεκτρονικού Εμπορίου (π.χ. μέσω Internet, μέσω κινητών τηλεφώνων, μέσω ψηφιακής τηλεόρασης κλπ.). Επομένως, είναι αναγκαίο στην περίπτωση που η τεχνογνωσία που απαιτείται δεν υπάρχει στην επιχείρηση, να αποκτηθεί με τη βοήθεια εξειδικευμένων συμβούλων και τεχνολογικών προμηθευτών. Όσο και αν παρουσιάζεται έλλειψη εξοικείωσης με την τεχνολογία, είναι απαραίτητη η κατάλληλη ενημέρωση, καθώς αρκετές κρίσιμες αποφάσεις θα πρέπει να ληφθούν όπως π.χ. με ποια μέσα θα γίνεται η επικοινωνία με τον καταναλωτή (πχ Internet, κινητή τηλεφωνία κλπ.), ποιες ακριβώς δυνατότητες θα έχει ο πελάτης μέσα στο ηλεκτρονικό κατάστημα (π.χ. αναζήτηση προϊόντων, εκπτώσεις - προσφορές, σύγκριση τιμών κλπ.).

Παρακάτω σας παρουσιάζουμε μερικές από τις τεχνολογίες που χρησιμοποιούνται στο ηλεκτρονικό εμπόριο:

1. **Ηλεκτρονική Ανταλλαγή Δεδομένων (EDI - Electronic Data Interchange)**: Η ηλεκτρονική Ανταλλαγή Δεδομένων που δημιουργήθηκε στις αρχές της δεκαετίας του '70, είναι μια κοινή δομή αρχείων που σχεδιάστηκε ώστε να επιτρέψει σε μεγάλους οργανισμούς να μεταδίδουν πληροφορίες μέσα από μεγάλα ιδιωτικά δίκτυα.

Πρόκειται για την ηλεκτρονική ανταλλαγή εμπορικών και διοικητικών δεδομένων από υπολογιστή σε υπολογιστή, με την ελάχιστη παρέμβαση χειρόγραφων διαδικασιών. Τα δεδομένα αυτά είναι οργανωμένα σε αυτοτελή μηνύματα (τιμολόγια, παραγγελίες, τιμοκατάλογοι, φορτωτικές κλπ.), το περιεχόμενο και η δομή των οποίων καθορίζονται από κάποιο κοινώς αποδεκτό πρότυπο. Τα πρότυπα που χρησιμοποιούνται σε παγκόσμιο επίπεδο προέρχονται από τον Οργανισμό Ηνωμένων Εθνών και καλύπτουν ένα ευρύ φάσμα επικοινωνιακών αναγκών των εμπορικών εταιριών. Το πρότυπο αυτό είναι το EDIFACT (EDI For Administration, Commerce and Transportation).

2. **Επίπεδο Ασφαλών Συνδέσεων (SSL - Secure Sockets Layer)**: Το πρωτόκολλο αυτό σχεδιάστηκε προκειμένου να πραγματοποιεί ασφαλή σύνδεση με τον εξυπηρετητή (server). Το SSL χρησιμοποιεί «κλειδί» δημόσιας κρυπτογράφησης, με σκοπό να προστατεύει τα δεδομένα καθώς «ταξιδεύουν» μέσα στο Internet.
3. **Ασφαλείς Ηλεκτρονικές Συναλλαγές (SET - Secure Electronic Transactions)**: Το SET κωδικοποιεί τους αριθμούς της πιστωτικής κάρτας που αποθηκεύονται στον εξυπηρετητή του εμπόρου. Το πρότυπο αυτό, που δημιουργήθηκε από τη Visa και τη MasterCard, απολαμβάνει μεγάλης αποδοχής από την τραπεζική κοινότητα.
4. **Γραμμωτός κώδικας (Barcode)**: Η τεχνολογία του γραμμωτού κώδικα αποτελεί τμήμα του γενικότερου τομέα των τεχνολογιών αυτόματης αναγνώρισης (Auto ID Technologies). Είναι ένα σύγχρονο εργαλείο, το οποίο βοηθά καταλυτικά στην ομαλή διακίνηση και διαχείριση (logistics) προϊόντων και υπηρεσιών.
5. **Έξυπνες κάρτες (Smart Cards)**: Οι «έξυπνες κάρτες» αποτελούν εξέλιξη των καρτών μαγνητικής λωρίδας (παθητικό μέσο αποθήκευσης, τα περιεχόμενα του οποίου μπορούν να διαβαστούν και να αλλαχθούν). Οι έξυπνες κάρτες μπορούν να αποθηκεύσουν μεγάλη ποσότητα

δεδομένων και παρέχουν δυνατότητες κρυπτογράφησης και χειρισμού ηλεκτρονικών υπογραφών για την ασφάλεια των περιεχομένων τους.

6. **Πιστοποίηση και ασφάλεια**: Για την ασφάλεια των ηλεκτρονικών συναλλαγών χρησιμοποιούνται ευρέως τα **firewalls**. Το firewall αποτελεί λογισμικό ή υλικό, που επιτρέπει μόνο στους εξωτερικούς χρήστες που έχουν τα κατάλληλα δικαιώματα, να προσπελάσουν το προστατευόμενο δίκτυο. Ένα firewall επιτρέπει στους εσωτερικούς χρήστες να έχουν πλήρη πρόσβαση στις παρεχόμενες υπηρεσίες, ενώ οι εξωτερικοί χρήστες πρέπει να πιστοποιηθούν. Υπάρχουν πολλοί τύποι firewalls, καθένας από τους οποίους παρέχει διαφορετικά επίπεδα προστασίας. Ο συνηθέστερος τρόπος χρησιμοποίησης ενός firewall είναι η τοποθέτηση ενός υπολογιστή ή δρομολογητή μεταξύ συγκεκριμένου δικτύου και του Internet, και η παρακολούθηση όλης της κυκλοφορίας μεταξύ του εξωτερικού και του τοπικού δικτύου.

Κεφάλαιο 3ο: EBPP (Electronic Bill Presentment and Payment)

Εισαγωγή

Το Electronic Bill Presentment and Payment (Ηλεκτρονική Παρουσίαση και Πληρωμή Λογαριασμών) είναι η υπηρεσία όπου με την χρήση του Διαδικτύου είναι δυνατόν να παρουσιαστεί ο λογαριασμός στον πελάτη και στη συνέχεια να εξοφληθεί online όπου αυτό είναι απαραίτητο. Παρόλο που το EBPP ανήκει σε αυτό που γενικά χαρακτηρίζουμε ηλεκτρονικό εμπόριο, εντούτοις δεν περιορίζεται μόνο στα προϊόντα και τις υπηρεσίες που παρέχονται μέσω Διαδικτύου.

Ένα χαρακτηριστικό παράδειγμα θα μπορούσε να είναι οι τηλεπικοινωνιακές υπηρεσίες που παρέχονται από τα δίκτυα κινητής τηλεφωνίας. Ενώ οι υπηρεσίες παρέχονται από ένα μέσο και με μία συγκεκριμένη διαδικασία, ωστόσο η παρουσίαση και πληρωμή του λογαριασμού μπορεί να γίνουν διαδικτυακά. Φυσικά, το EBPP μπορεί κάλλιστα να εφαρμοστεί και στις περιπτώσεις κατά τις οποίες ολόκληρη η συναλλαγή γίνεται μέσω Internet, για παράδειγμα όταν αγοράζουμε ένα ηλεκτρονικό βιβλίο (e-book) από ένα διαδικτυακό «μαγαζί».

Στις συναλλαγές που γίνονται εξ' ολοκλήρου, ή έστω σε μεγάλο βαθμό online, το EBPP μοιάζει ως λογική συνέχεια της συναλλαγής και κατά συνέπεια χρησιμοποιείται. Πώς μπορούμε όμως να εντάξουμε το EBPP σε συναλλαγές που δεν πραγματοποιούνται μέσω Internet; Την απάντηση στο ερώτημα αυτό μπορούμε να τη δώσουμε εύκολα, εάν αναλογιστούμε ότι στη συντριπτική πλειονότητα των συναλλαγών, τα στοιχεία δημιουργούνται ή/και τηρούνται με ηλεκτρονικό τρόπο. Από τη στιγμή που το κομμάτι που αφορά στα στοιχεία των λογαριασμών επιτρέπει την ηλεκτρονική διαχείριση, μπορούμε να κάνουμε εύκολα ηλεκτρονικά και την παρουσίαση του λογαριασμού προς τον πελάτη μέσω Internet, αλλά και την ηλεκτρονική εξόφλησή του.

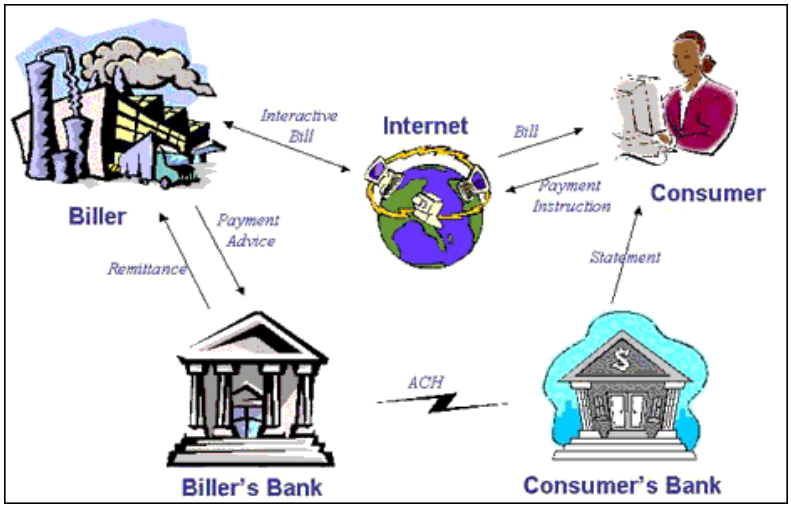
3.1 Τα βασικά μοντέλα του EBPP

Δύο είναι τα επιχειρηματικά μοντέλα του EBPP:

- **biller-direct model** (απευθείας αποστολή του λογαριασμού από τον πάροχο (biller) στον πελάτη)
- **consolidation model** («φιλοξενία» ή «συνένωση» πολλών παρόχων σε ένα κοινό τόπο). Εδώ επίσης μπορούμε να διακρίνουμε δύο υπό-μοντέλα:
    - **biller consolidation model**
    - **consumer consolidation model**

3.1.1 Biller-direct model

Στο μοντέλο **biller-direct**, αρχικά έχουμε την εγγραφή του πελάτη στην υπηρεσία EBPP που προσφέρει ο εκάστοτε πάροχος (biller). Στη συνέχεια ο πάροχος δημιουργεί έναν ηλεκτρονικό φάκελο, στον οποίο καταγράφονται όλες οι πληροφορίες που σχετίζονται με το λογαριασμό του πελάτη. Αφού δημιουργηθεί ο ηλεκτρονικός φάκελος, έπειτα οι λογαριασμοί των πελατών παρουσιάζονται στο δικτυακό τόπο του παρόχου και οι πελάτες καλούνται να παρακολουθούν και να εξοφλούν τους λογαριασμούς τους κατευθείαν από εκεί. Ουσιαστικά, ο πάροχος στέλνει ένα e-mail στους πελάτες ενημερώνοντάς τους για τον καινούριο τους λογαριασμό. Στη συνέχεια οι πελάτες εισέρχονται στο δικτυακό τόπο του παρόχου, μέσω μιας ασφαλούς σύνδεσης, παρακολουθούν τις πληροφορίες που περιλαμβάνει ο λογαριασμός τους και εξοφλούν το αναφερόμενο ποσό απευθείας από το site. Πρέπει να προσθέσουμε επίσης, ότι οι λογαριασμοί παρουσιάζονται στους πελάτες σύμφωνα με τους όρους λειτουργικότητας που θέτει ο πάροχος, ενώ η πληρωμή των λογαριασμών υλοποιείται μέσω τραπεζών της επιλογής του ιδίου.



Σχήμα 3.1 Μοντέλο Biller-direct

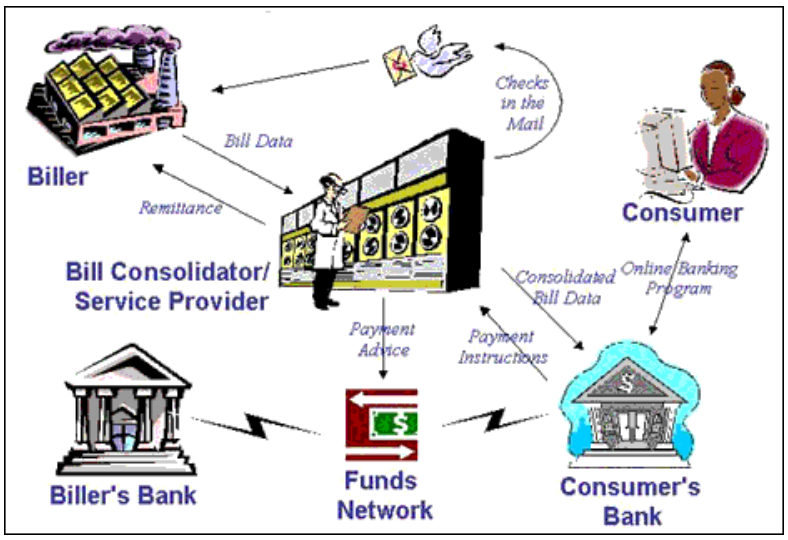
Το μοντέλο biller-direct είναι το πιο απλό και το πιο καλά ορισμένο απ' τα μοντέλα του EBPP που χρησιμοποιούνται την σημερινή εποχή. Ο πάροχος παίζει τον βασικό ρόλο σ' αυτό το μοντέλο, καθώς χειρίζεται τις ευθύνες που έχει ο κάθε πελάτης κατά την εγγραφή του και γενικά σε όλη την υπηρεσία, μορφοποιεί και «μεταφράζει» τα δεδομένα των λογαριασμών των πελατών, καθώς επίσης έχει και την ευθύνη για την παρουσίαση του δικτυακού τόπου.

Το κύριο μειονέκτημα αυτού του μοντέλου είναι ότι ο πελάτης πρέπει να επισκέπτεται κάθε φορά και διαφορετικό site για την πληρωμή του κάθε λογαριασμού. Επίσης πολλοί λογαριασμοί επαναλαμβάνονται σε διάφορες χρονικές στιγμές κατά την διάρκεια του μήνα κάτι που έχει ως αποτέλεσμα οι πελάτες να πρέπει να εισέρχονται πολλές φορές στον λογαριασμό τους για να τον εξοφλήσουν.

3.1.2 Biller Consolidation Model

Το μοντέλο biller consolidation είναι πιο πολύπλοκο, αρχικά λόγω του ότι ένας ή και περισσότεροι εξωτερικοί «συμμέτοχοι» ενεργούν σαν μεσάζοντες για την διεύθυνση των δεδομένων των λογαριασμών. Οι μεσάζοντες αυτοί χωρίζονται σε δύο κατηγορίες: οι πρώτοι καλούνται ***bill***

consolidators και οι δεύτεροι ***biller service providers***. Οι *bill consolidators* λαμβάνουν τα δεδομένα λογαριασμών από πολλαπλούς παρόχους και στη συνέχεια συνενώνουν την πληροφορία σε τόπους διανομής σύμφωνα με το που έχει εγγραφεί κάθε πελάτης. Συνήθως, αυτοί οι τόποι διανομής είναι τράπεζες, αλλά μπορεί επίσης να είναι και μια Διαδικτυακή Πύλη (portal) όπως εν παραδείγματι το AOL, το Quicken.com, το Yahoo! Finance καθώς ακόμα και το United States Postal Service.



Σχήμα 3.2 Μοντέλο Biller Consolidation

Υπάρχουν πολλές «παραλλαγές» του consolidator μοντέλου, οι οποίες κυρίως έχουν ως κριτήριο τον όγκο παροχής υπηρεσιών του consolidator καθώς και το ποσό εμπλοκής του biller service provider στην υπηρεσία. Η κύρια διαφορά όμως σ' αυτές τις «παραλλαγές» έχει να κάνει με το ποσό των δεδομένων που μεταφέρονται για αποθήκευση στον consolidator και το δικαίωμα εισόδου του πελάτη.

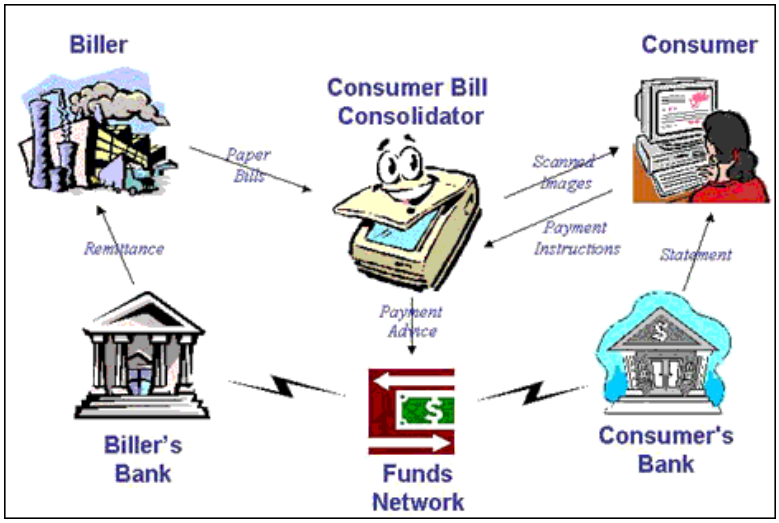
Οι δύο βασικές «παραλλαγές» είναι:

1. Το **thick model**, βάσει του οποίου μία πλήρης αναφορά του λογαριασμού του πελάτη παρέχεται από το διαδικτυακό χώρο του παρόχου υπηρεσιών (Customer Service Provider -- CSP) και

2. το **thin model**, με το οποίο τα συνοπτικά στοιχεία του λογαριασμού του πελάτη παρέχονται από την ιστοσελίδα του παρόχου.

3.1.3 Consumer Consolidation Model

Το μοντέλο consumer consolidator είναι το μόνο που παρέχει τη δυνατότητα στους πελάτες να παρακολουθούν ταυτόχρονα όλους τους λογαριασμούς τους μέσω του δικτύου (web), αν αυτοί το θελήσουν. Αυτό επιτυγχάνεται μέσω μιας προσέγγισης «χαμηλής τεχνολογίας», στην οποία όλοι οι λογαριασμοί (τα χαρτιά) αποστέλλονται σε μία κεντρική υπηρεσία όπου και μετατρέπονται σε αρχεία pdf, τα οποία στη συνέχεια οι πελάτες μπορούν να τα δουν online.



Σχήμα 3.3 Μοντέλο Consumer Consolidation

Γενικά οι πελάτες δεν έχουν ικανότητες αλληλεπίδρασης με τους λογαριασμούς. Όλα τα επιπλέον περιεχόμενα των λογαριασμών καταστρέφονται. Ο διαδικτυακός χώρος του παροχέα υπηρεσιών προσφέρει ένα πολύ βολικό περιβάλλον αλληλεπίδρασης στον χρήστη (user interface) για να μπορεί να οργανώνει και να παρακολουθεί τους λογαριασμούς του καθώς και να συμπληρώνει τις επιλογές για τον τρόπο πληρωμής. Μερικοί επίσης προσφέρουν την δυνατότητα να μπορεί ο πελάτης να αποθηκεύει

παλιούς λογαριασμούς του online ή σε ένα CD. Αφού ο πελάτης ελέγξει τους λογαριασμούς του και στείλει τις οδηγίες πληρωμής στον παροχέα υπηρεσιών, ο δεύτερος μεταφέρει αυτές τις οδηγίες σε μία τράπεζα για να εκπληρωθούν.

3.2 Κατάσταση στην ελληνική αγορά

Ελάχιστες είναι οι ελληνικές εταιρίες που παρέχουν λύσεις ηλεκτρονικής παρουσίασης και πληρωμών λογαριασμών. Ενδεικτικά αναφέρουμε:

- **LYKOS Paperless Solutions (**www.lps.gr**)**: Η εταιρία έχει προσαρμόσει αλλά και αναπτύξει το λογισμικό της αμερικανικής Checkfree Corporation, μιας από τις σημαντικότερες πλατφόρμες ηλεκτρονικής χρέωσης (e-billing) σε παγκόσμιο επίπεδο, με αποτέλεσμα σήμερα η εταιρία να διαθέτει ένα ολοκληρωμένο πακέτο υπηρεσιών EBP προσαρμοσμένο στις ανάγκες της ελληνικής αγοράς. Ο κεντρικός κόμβος (Consolidation Center) μπορεί να υποδεχθεί πολλαπλές εφαρμογές και να υποστηρίξει όλους τους εμπλεκόμενους φορείς (Billers, Τράπεζες, Customer Service Providers). Ταυτόχρονα παρέχει στον κάθε φορέα την ευχέρεια να χτίσει το δικό του ανταγωνιστικό πλεονέκτημα με εξατομικευμένη πληροφορία προς τον τελικό καταναλωτή.
- **Exodus (**www.exodus.gr**)**: Χαρακτηριστική στο χώρο των ηλεκτρονικών πληρωμών είναι η εφαρμογή η e.Payments της εταιρίας Exodus, η οποία έχει υιοθετηθεί από την Τράπεζα Πειραιώς και αφορά στην ηλεκτρονική εκκαθάριση συναλλαγών με πιστωτική κάρτα. Συγκεκριμένα, το σύστημα πληρωμών της εφαρμογής e.Payments υποστηρίζει ασφαλείς ηλεκτρονικές πληρωμές από τον πελάτη με τη χρήση πιστωτικής κάρτας, παρέχοντας στις επιχειρήσεις τη δυνατότητα απάντησης στον πελάτη σε πραγματικό χρόνο, για την έγκριση ή απόρριψη της συναλλαγής. Παράλληλα, ενημερώνει για κάθε συναλλαγή ημέρας ή συγκεκριμένης χρονικής περιόδου με συγκεντρωτικούς και αναλυτικούς πίνακες.

Κεφάλαιο 4ο: Ηλεκτρονικές Συναλλαγές

Εισαγωγή

Στα συστήματα ηλεκτρονικών συναλλαγών εντάσσεται κάθε μέθοδος που χρησιμοποιείται για να εξυπηρετήσει την πραγματοποίηση αγορών μέσω του Internet. Ορίζοντας τις ηλεκτρονικές συναλλαγές με αυτό τον τρόπο, μπορούμε να συμπεριλάβουμε σε αυτές, εκτός από τις αμιγώς ψηφιακές, και κάποιες παραδοσιακές μεθόδους. Έτσι, σύστημα ηλεκτρονικών συναλλαγών θεωρούνται όχι μόνο η χρήση πιστωτικών καρτών, το ψηφιακό χρήμα και οι ηλεκτρονικές επιταγές, αλλά και το έμβασμα, η αντικαταβολή, η μεταφορά χρημάτων σε λογαριασμό κ.ά. Κοινό χαρακτηριστικό των παραπάνω μεθόδων είναι ότι μπορούν να ενσωματωθούν στη λειτουργία ενός online καταστήματος εξυπηρετώντας τις αγοραπωλησίες και το εν γένει ηλεκτρονικό εμπόριο.

Σε μια ηλεκτρονική επικοινωνία, η εμπιστοσύνη μεταξύ των συναλλασσόμενων μερών είναι πολύ σημαντική, γι' αυτό και θα πρέπει να δίνεται ιδιαίτερη έμφαση στο θέμα της ασφάλειας των συναλλαγών. Σήμερα, η τεχνολογία παρέχει προηγμένες λύσεις στο θέμα αυτό. Ένα ηλεκτρονικό κατάστημα που μεριμνά για την ασφάλεια των πελατών του οφείλει να χρησιμοποιεί και να αναφέρει ρητά όλα τα απαραίτητα συστήματα ασφαλείας καθώς και να παρέχει τις απαραίτητες πληροφορίες για την πιστοποίηση της ταυτότητάς του.

Για τις μικρομεσαίες επιχειρήσεις το ηλεκτρονικό εμπόριο είναι περισσότερο ασφαλές από ένα «πραγματικό» κατάστημα, το οποίο μπορεί να λεηλατηθεί, να καεί, να πλημμυρίσει. Η δυσκολία έγκειται στο να κάνουν τους πελάτες να εξοικειωθούν με την ιδέα ότι το ηλεκτρονικό εμπόριο είναι ασφαλές γι' αυτούς.

Μολονότι θεωρείται ότι οι συναλλαγές μέσω πιστωτικής κάρτας στο Internet δεν είναι ασφαλείς, οι ειδικοί υποστηρίζουν ότι το ηλεκτρονικό

εμπόριο και οι online συναλλαγές εν γένει είναι ασφαλέστερες από τις αγορές με πιστωτικές κάρτες σε «φυσικά» καταστήματα. Κάθε φορά που ο πελάτης πληρώνει με πιστωτική κάρτα σε ένα κατάστημα ή εστιατόριο και κάθε φορά που πετά την απόδειξη μιας πιστωτικής κάρτας γίνεται περισσότερο ευάλωτος στην απάτη.

4.1 Έξυπνες Κάρτες (Smart Cards)

Τα τελευταία χρόνια η τρομακτική ανάπτυξη της τεχνολογίας έχει πραγματικά διαμορφώσει μια νέα πραγματικότητα για την ζωή των ανθρώπων. Μάλιστα, παρατηρείται μια διεξοδική εισβολή τεχνικών όρων και ακρωνύμιων, που ο μέσος άνθρωπος αδυνατεί να τα κατανοήσει. Ένας τέτοιος όρος είναι και ο όρος Smart Cards (Έξυπνες Κάρτες). Οι έξυπνες κάρτες είναι ουσιαστικά μικροσκοπικοί υπολογιστές, που έχουν το μέγεθος και τη φόρμα μίας πιστωτικής κάρτας, πάνω στην οποία είναι ενσωματωμένο ένα ολοκληρωμένο κύκλωμα (chip), στην εμπρόσθια αριστερή πλευρά.

Το ολοκληρωμένο κύκλωμα περιέχει τις επαφές εισόδου/εξόδου και μπορεί να περιέχει μόνο μνήμη ή και μικροεπεξεργαστή. Το ολοκληρωμένο κύκλωμα μπορεί να παρέχει μία ασφαλή δομή πολλαπλών επιπέδων και να επιτρέπει ιεραρχημένη πρόσβαση, καθιστώντας δύσκολη την πρόσβαση στα στοιχεία και την παραποίηση αυτών, να υπολογίζει κρυπτογραφικές συναρτήσεις (cryptographic functions) και να αντιλαμβάνεται άμεσα προσπάθειες πρόσβασης, οι οποίες δεν είναι έγκυρες όπως για παράδειγμα το κλείδωμα της κάρτας SIM σε περίπτωση εισαγωγής λανθασμένου PIN περισσότερες από τρεις, συνήθως, φορές.

Οι κάρτες με μικροεπεξεργαστή, εκτός από CPU, διαθέτουν μνήμη ROM για την αποθήκευση του λειτουργικού συστήματος της κάρτας, μνήμη RAM για γρήγορη εκτέλεση υπολογισμών και μνήμη EEPROM για την αποθήκευση εφαρμογών και δεδομένων. Πρόκειται ουσιαστικά για

ολοκληρωμένους μικροσκοπικούς Η/Υ, οι οποίοι στερούνται μόνο συσκευών εισόδου/εξόδου. Έτσι προκειμένου να επικοινωνήσουμε με τους υπολογιστές αυτούς χρησιμοποιούμε τις συσκευές αποδοχής έξυπνων καρτών (*card readers*).

Το κύριο γνώρισμα των έξυπνων καρτών είναι η ικανότητα να αποθηκεύουν και να επεξεργάζονται πληροφορίες με ένα ασφαλή τρόπο. Τα πλεονεκτήματα των έξυπνων καρτών είναι η **προστασία** των δεδομένων που περιέχουν, η **φορητότητα** και η **ευκολία χρήσης**. Προκειμένου το ολοκληρωμένο αυτό κύκλωμα να μπορεί να χρησιμοποιηθεί και σε τερματικά ή αναγνώστες τα οποία δεν έχουν το απαιτούμενο μέγεθος για την εισαγωγή ολόκληρης της κάρτας, είναι δυνατή η παραγωγή των καρτών με εγκοπές γύρω από το κύκλωμα, προκειμένου αυτό να αφαιρείται και να τοποθετείται στην τερματική συσκευή. Κλασσικό παράδειγμα οι κάρτες SIM.

4.1.1 Είδη έξυπνων καρτών

Στις μέρες μας, οι έξυπνες κάρτες μπορούν να κατηγοριοποιηθούν με δύο βασικά κριτήρια:

α) επεξεργαστική ικανότητα και

β) δυνατότητες εισόδου/εξόδου.

Με βάση το **πρώτο** κριτήριο, διακρίνουμε τρεις κατηγορίες έξυπνων καρτών:

1. **Κάρτες μνήμης**, κάρτες αποθήκευσης πληροφοριών (*memory cards*). Οι κάρτες αυτές περιέχουν κάποια μνήμη και λογική σε υλικό (*hardware logic*), η οποία μπορεί να θέσει ή να διαγράψει τιμές στη μνήμη. Οι κάρτες μνήμης αναφέρονται καταχρηστικά ως έξυπνες κάρτες, καθώς δεν έχουν δυνατότητα επεξεργασίας των δεδομένων.
2. **Έξυπνες κάρτες** (*smart cards, IC cards, microprocessor cards*). Είναι οι «κλασικές» έξυπνες κάρτες ή κάρτες με μικροεπεξεργαστή,. Ο επεξεργαστής τους, πέρα από την αποθήκευση και ασφάλιση

πληροφοριών, μπορεί να λαμβάνει αποφάσεις που ορίζονται στις προδιαγραφές του έργου για το οποίο θα χρησιμοποιηθούν.

3. **Έξυπνες κάρτες πολλαπλών εφαρμογών** (multi-application smart cards). Οι έξυπνες κάρτες τελευταίας γενιάς έρχονται με ανοικτά λειτουργικά συστήματα (Java, MULTOS) και μπορούν να εκτελούν περισσότερες από μία εφαρμογές. Παρέχεται επίσης η δυνατότητα στο χρήστη να «φορτώνει» νέες εφαρμογές, ή να διαγράφει άλλες ανάλογα με τις ανάγκες του.

Μία **δεύτερη** κατηγοριοποίηση αφορά τον τρόπο επικοινωνίας των έξυπνων καρτών με το εξωτερικό περιβάλλον. Με βάση αυτό το κριτήριο, διακρίνουμε τις εξής κατηγορίες:

1. **Έξυπνες κάρτες με επαφές** (Contact Cards). Οι κάρτες αυτές επικοινωνούν με ηλεκτρικές επαφές και πρέπει να εισαχθούν σε μία συσκευή ανάγνωσης προκειμένου να διαβαστούν ή να εισαχθούν πληροφορίες.
2. **Ασύρματες έξυπνες κάρτες** (Contactless Cards). Οι κάρτες αυτές έχουν ενσωματωμένη εσωτερικά μία μικροσκοπική κεραία και μπορούν να επικοινωνούν με μία κεραία λήψης χωρίς τη φυσική τους επαφή με κάποια συσκευή ανάγνωσης προκειμένου οι πληροφορίες να ανανεωθούν, να αλλάξουν ή να υποβληθούν σε επεξεργασία.
3. **Υβριδικές κάρτες και συνδυασμένες κάρτες** (Hybrid και Combination Cards). Οι κάρτες αυτές ενσωματώνουν και τους δύο τρόπους μετάδοσης και συνεπώς μπορούν να επικοινωνήσουν κατά περίπτωση είτε με ενσύρματο είτε με ασύρματο τρόπο.

4.1.2 Εφαρμογές των έξυπνων καρτών

Οι έξυπνες κάρτες όπως είναι αναμενόμενο προσφέρονται για πλήθος εφαρμογών. Στην αύξηση των εφαρμογών συμβάλλει και η εξέλιξη των έξυπνων καρτών με την αύξηση της διαθέσιμης υπολογιστικής δύναμης και της μνήμης τους.

Παρουσιάζουμε στη συνέχεια μερικά παραδείγματα όπου χρησιμοποιούνται οι έξυπνες κάρτες για να γίνει πιο κατανοητή η αξία και η χρησιμότητά τους.

Ηλεκτρονικό πορτοφόλι

Η έξυπνη κάρτα μπορεί να αποθηκεύσει νομισματικές μονάδες, διευκολύνοντας σημαντικά τις πληρωμές και αγορές. Παραδείγματα χρήσεων αποτελούν οι ελεγχόμενοι χώροι στάθμευσης, διόδια σε δρόμους, πληρωμή εισιτηρίου σε μέσα μαζικής μεταφοράς (μετρό, τρένο, λεωφορεία), αγορά αναψυκτικών από μηχανήματα που βρίσκονται σε δημόσιους χώρους (venting machines) και αυτόματη πληρωμή φωτοτυπιών σε δημόσιες βιβλιοθήκες αλλά και αγορές καταναλωτικών ειδών σε κάθε είδους κατάστημα. Επιτυχημένα παραδείγματα ηλεκτρονικού πορτοφολιού είναι η κάρτα Mondex και τα αντίστοιχα της Visa.

Χρήση έξυπνων καρτών στις μεταφορές

Οι Μεταφορές αποτελούν την εφαρμογή – κλειδί, γιατί έχουν πολυάριθμο και σταθερό κοινό. Οι εφαρμογές στον τομέα των Μεταφορών που μπορούν να προσφέρουν οι έξυπνες κάρτες είναι οι εξής:

- Πληρωμή εισιτηρίου στις Δημόσιες Συγκοινωνίες.
- Πληρωμή διοδίων.
- Δικαιώματα parking.
- Κρατήσεις αεροπορικών εισιτηρίων, κρατήσεις σε ξενοδοχεία και μεταφορά των αποσκευών.
- Τεκμηρίωση κατόχου, ηλεκτρονικό διαβατήριο.

Έλεγχος πρόσβασης σε κτίρια

Μία έξυπνη κάρτα μπορεί να αποθηκεύσει τα στοιχεία αναγνώρισης ενός ατόμου για τον έλεγχο πρόσβασης σε κτίρια υψηλής και μη ασφάλειας- χώρος εργασίας αλλά και σε πανεπιστήμια, σχολεία, βιβλιοθήκες και

λέσχες. Για ανάγκες υψηλότερης ασφάλειας και πρόσβαση σε συγκεκριμένες υπηρεσίες ή πληροφορίες, μια έξυπνη κάρτα μπορεί να αποτελέσει μια συσκευή για την αποθήκευση πληροφοριών όπως η εικόνα ή άλλα βιομετρικά χαρακτηριστικά (π.χ. τα δακτυλικά αποτυπώματα, ίριδα του ματιού) του χρήστη.

GSM κάρτες και τηλεκάρτες

Οι έξυπνες κάρτες βρήκαν εφαρμογή σε πολλούς τομείς της καθημερινής μας ζωής. Δύο από τις πιο επιτυχημένες εφαρμογές τους είναι στον τομέα τηλεπικοινωνιών και μάλιστα στην πιο απλή τους (προπληρωμένη τηλεκάρτα) και στην πιο σύνθετη (GSM κάρτες) μορφή τους.

Άλλες εφαρμογές

Άλλες εφαρμογές των έξυπνων καρτών είναι η χρήσης τους σε αποκωδικοποιητές, Internet access, πρόσβαση σε ανοικτά ή κλειστά δίκτυα, product tracking, δίπλωμα οδήγησης (ιδανική για αποθήκευση penalty points και άμεση αφαίρεση του διπλώματος), κ.ά.

4.2 Ψηφιακό Χρήμα

Το ψηφιακό ή ηλεκτρονικό χρήμα είναι το ηλεκτρονικό ανάλογο του φυσικού χρήματος. Εκδίδεται από τράπεζες και οι πελάτες μπορούν να το χρησιμοποιήσουν για να αγοράσουν αγαθά ή υπηρεσίες από εμπόρους που αποδέχονται αυτήν τη μορφή ηλεκτρονικής πληρωμής. Τρία μέρη εμπλέκονται σε ένα σύστημα ηλεκτρονικού χρήματος: μια τράπεζα, που εκδίδει το ηλεκτρονικό χρήμα, ένας πελάτης και ένας έμπορος.

Γενικά, υπάρχουν δύο ξεχωριστοί τύποι ηλεκτρονικού χρήματος: το ηλεκτρονικό χρήμα που προσδιορίζει την ταυτότητα του ιδιοκτήτη του (identified e-money) και το ανώνυμο ηλεκτρονικό χρήμα (anonymous e-money), γνωστό επίσης και ως ψηφιακά μετρητά. Ο πρώτος τύπος περιλαμβάνει πληροφορίες που γνωστοποιούν την ταυτότητα του

προσώπου που έκανε την ανάληψη χρημάτων από την τράπεζα και βοηθάει την τράπεζα να ανιχνεύσει την διακίνηση του μέσα στην οικονομία, λειτουργεί δηλαδή με τον ίδιο τρόπο με τον οποίο λειτουργούν και οι πιστωτικές κάρτες. Ο δεύτερος τύπος ηλεκτρονικού χρήματος μοιάζει με τα χάρτινα μετρητά που κυκλοφορούν. Το ανώνυμο ηλεκτρονικό χρήμα μπορεί να ξοδευτεί ή και να χαθεί ακόμα, χωρίς όμως η τράπεζα, να γνωρίζει κάτι για την διακίνησή του από την ανάληψη του και μετά.

Τους παραπάνω δύο τύπους ηλεκτρονικού χρήματος μπορούμε να τους συναντήσουμε σε δύο κατηγορίες: on-line και offline. Η πρώτη κατηγορία προϋποθέτει αλληλεπίδραση του πελάτη με την τράπεζα, μέσω διαδικτύου, για να διεξαχθεί η εμπορική πράξη μέσω ενός τρίτου, για παράδειγμα ενός εμπόρου. Με την δεύτερη κατηγορία ηλεκτρονικού χρήματος δεν απαιτείται η απευθείας εμπλοκή της τράπεζας για να διεκπεραιωθεί η οικονομική συναλλαγή. Η συναλλαγή με offline ανώνυμο ηλεκτρονικό χρήμα, το οποίο είναι το πραγματικό ψηφιακό χρήμα, είναι και η περισσότερο περίπλοκη συναλλαγή ηλεκτρονικού χρήματος, αφού η μυστικότητα η οποία προσφέρει, οδηγεί στη δυνατότητα ξεπλύματος παράνομου χρήματος ή στην απόκρυψη χρήματος που προήλθε από παράνομες ενέργειες. Η διαπίστωση αυτή οδήγησε στην ανάπτυξη σχεδόν ανώνυμων συστημάτων ηλεκτρονικού χρήματος, στα οποία η ταυτότητα του πελάτη είναι δυνατόν να αποκαλυφθεί, υπό συγκεκριμένους όρους.

4.2.1 Ιδιότητες ψηφιακού χρήματος

Είναι κοινά αποδεκτό ότι το ανώνυμο ηλεκτρονικό χρήμα πρέπει να έχει ορισμένες ιδιότητες. Έτσι το ηλεκτρονικό χρήμα πρέπει να είναι:

1. **Ανεξάρτητο**. Το ηλεκτρονικό χρήμα πρέπει να είναι ανεξάρτητο, με την έννοια ότι η ύπαρξή του δεν πρέπει να εξαρτάται από συγκεκριμένες πλατφόρμες ή συστήματα.
2. **Ανώνυμο.** Ένα από τα ξεχωριστά χαρακτηριστικά του πραγματικού χρήματος είναι η ανωνυμία του, με την έννοια ότι το χρήμα δεν πρέπει

να παρέχει πληροφορίες που να επιτρέπουν την αναγνώριση των προηγούμενων ιδιοκτητών του. Είναι λογικό, λοιπόν, να απαιτούμε και από το ηλεκτρονικό χρήμα να έχει την ιδιότητα αυτή. Συνεπώς, το ηλεκτρονικό χρήμα πρέπει να μπορεί να μεταφέρεται από άτομο σε άτομο, και μάλιστα με τέτοιον τρόπο ώστε να μην είναι δυνατόν να ανακαλυφθεί ποιος το κατείχε προηγουμένως.

3. **Να χρησιμοποιείται μόνο μία φορά.** Σύμφωνα και με τα παραπάνω καταλήγουμε στο ότι πρέπει να είναι βέβαιο ότι κάθε ηλεκτρονικό νόμισμα χρησιμοποιείται μόνο μία φορά και ότι κάθε απόπειρα διπλής χρήσης είναι ανιχνεύσιμη.
4. **Διαθέσιμο και διαιρετό.** Το ηλεκτρονικό χρήμα πρέπει να είναι διαθέσιμο σε διάφορα ποσά και να είναι διαιρετό, όπως και το πραγματικό.
5. **Ασφαλές.** Τέλος, το ηλεκτρονικό χρήμα πρέπει να είναι δυνατόν να αποθηκευτεί με ασφάλεια σε σκληρό δίσκο ή σε έξυπνη κάρτα.

4.2.2 Συστήματα ψηφιακού χρήματος

Η ιδέα του ανώνυμου ηλεκτρονικού χρήματος, εκτός από το σύστημα ανώνυμου ηλεκτρονικού χρήματος Ecash, έχει εξεταστεί και στα πλαίσια του Ευρωπαϊκού έργου **C**onditional **A**ccess **F**or **E**urope (CAFE). Επίσης ένα άλλο offline σύστημα ανώνυμου ηλεκτρονικού χρήματος με υποστήριξη υλικού είναι το Mondex, το οποίο αναπτύσσεται κυρίως στο Ηνωμένο Βασίλειο. Το NetCash είναι ένα σύστημα ηλεκτρονικού χρήματος που παρέχει αδύναμη ανωνυμία. Ο όρος αυτός σημαίνει ότι, αν ένας πελάτης δώσει το νόμισμα NetCash σ' έναν έμπορο, δεν υπάρχει τρόπος μόνος του ο έμπορος να διαπιστώσει την ταυτότητα του πελάτη. Ωστόσο, αν ο έμπορος συνεργαστεί με την τράπεζα, είναι δυνατόν από κοινού να ανακαλύψουν την ταυτότητα του πελάτη. Τέλος, το CyberCash είναι παράδειγμα συστήματος ηλεκτρονικού χρήματος που δεν ενδιαφέρεται καθόλου για την ανωνυμία του πελάτη.

4.3 Ηλεκτρονικές Επιταγές

Επειδή οι επιταγές αποτελούν ένα αρκετά διαδεδομένο μέσο πληρωμής στον πραγματικό κόσμο, οι ηλεκτρονικές επιταγές μπορούν να αποτελέσουν ένα ενδιαφέρον σχήμα πληρωμής για το ηλεκτρονικό εμπόριο. Ένα σύστημα πληρωμής ηλεκτρονικών επιταγών λειτουργεί συνοπτικά ως εξής: Ο πελάτης εκδίδει μια ηλεκτρονική επιταγή στο όνομα του εμπόρου και ο έμπορος καταθέτει την επιταγή στην τράπεζα προκειμένου να την εξαργυρώσει. Το σύστημα, λοιπόν, αποτελείται από τα εξής μέρη: έναν πελάτη και την τράπεζά του, έναν έμπορο και την τράπεζά του και τέλος ένα διατραπεζικό οργανισμό για την επεξεργασία των επιταγών ανάμεσα στις τράπεζες.

Από τεχνική σκοπιά, οι ηλεκτρονικές επιταγές είναι σχετικά απλές. Μια ηλεκτρονική επιταγή μπορεί απλώς να αποτελείται από ένα έγγραφο που είναι ψηφιακά υπογραμμένο με το ιδιωτικό κλειδί του πελάτη. Ο παραλήπτης (ο έμπορος ή η τράπεζά του) μπορούν να χρησιμοποιήσουν το δημόσιο κλειδί του πελάτη προκειμένου να επιβεβαιώσουν την ψηφιακή υπογραφή. Παραδείγματα συστημάτων ηλεκτρονικών επιταγών αποτελούν τα PayNow και NetCheque.

4.3.1 Πλεονεκτήματα ηλεκτρονικών επιταγών

Σε σύγκριση με τις συμβατικές επιταγές και κάποιες άλλες μορφές συμβατικών πληρωμών, οι ηλεκτρονικές επιταγές έχουν αρκετά πλεονεκτήματα. Αυτά είναι τα εξής:

- Οι ηλεκτρονικές επιταγές μπορούν να εκδοθούν χωρίς να χρειάζεται να συμπληρωθούν, να ταχυδρομηθούν ή να παραδοθούν χαρτιά.
- Ο χρόνος επεξεργασίας τους είναι μικρότερος. Ο έμπορος, όταν έχει να κάνει με συμβατικές επιταγές, συνήθως τις συγκεντρώνει και μετά τις καταθέτει στην τράπεζά του. Αντίθετα, όταν έχει να κάνει με ηλεκτρονικές επιταγές, μπορεί να τις προωθεί μία-μία στην τράπεζά του και να πιστώνει ανάλογα το λογαριασμό του.

- Τα συστήματα ηλεκτρονικών επιταγών μπορούν να σχεδιαστούν έτσι ώστε ο έμπορος να λαμβάνει κατάλληλη εξουσιοδότηση από την τράπεζα του πελάτη πριν αποδεχτεί μια επιταγή. Η δυνατότητα αυτή μοιάζει πολύ με τη λύση των τραπεζικών επιταγών.

4.4 Πιστωτικές Κάρτες

Μέχρι τώρα, οι πιστωτικές ή χρεωστικές κάρτες παρέχουν τον απλούστερο, αν όχι τον ιδανικότερο, τρόπο μεταφοράς αξίας πάνω στο Internet, γι' αυτό και είναι και η ευρύτερα διαδεδομένη και γνωστή στο αγοραστικό κοινό. Υπάρχουν διάφορες απαιτήσεις ασφάλειας που αυτά τα συστήματα πρέπει να πληρούν. Για παράδειγμα, πρέπει να υπάρχει ένας μηχανισμός που θα αυθεντικοποιεί τα διάφορα εμπλεκόμενα μέρη, δηλαδή τους πελάτες, τους εμπόρους και τις συμμετέχουσες τράπεζες. Πρέπει, επίσης, να υπάρχει ένας άλλος μηχανισμός που θα προστατεύει τις πληροφορίες της κάρτας και της πληρωμής καθώς αυτές μεταδίδονται μέσω του Internet. Τέλος, πρέπει να συμφωνηθεί μια διαδικασία επίλυσης διαφορών μεταξύ των εμπλεκόμενων μερών.

Έχουν σχεδιαστεί αρκετά συστήματα ηλεκτρονικών πληρωμών με πιστωτικές κάρτες που αντιμετωπίζουν αυτές τις απαιτήσεις. Τα περισσότερα απ' αυτά έχουν και επιπλέον πλεονεκτήματα. Για παράδειγμα, σε κάποια απ' αυτά τα συστήματα οι πληροφορίες της πιστωτικής κάρτας δεν αποκαλύπτονται στον έμπορο. Το χαρακτηριστικό αυτό δεν υπάρχει στα συμβατικά συστήματα πληρωμής με πιστωτικές κάρτες. Επομένως, ένα ηλεκτρονικό σύστημα πληρωμής με πιστωτικές κάρτες μπορεί να παρέχει μεγαλύτερη ασφάλεια απ' ότι το συμβατικό σύστημα. Επίσης, ένα ηλεκτρονικό σύστημα πληρωμής με πιστωτικές κάρτες μπορεί να σχεδιαστεί έτσι ώστε να κάνει σχεδόν άμεσα την πληρωμή στον έμπορο. Στο συμβατικό σύστημα απαιτείται αρκετός χρόνος μέχρι ο έμπορος να πάει τις αποδείξεις στην τράπεζα και η τράπεζα να εκκαθαρίσει το προς πληρωμή ποσό.

4.4.1 Κατηγορίες συναλλαγών με χρήση Πιστωτικών Καρτών

Οι συναλλαγές στο Διαδίκτυο, με χρήση πιστωτικών καρτών, μπορούν να χωριστούν χάριν ευχρηστίας σε 3 κατηγορίες:

1. Ο πελάτης ταχυδρομεί ηλεκτρονικά στον έμπορο τις λεπτομέρειες της πιστωτικής του κάρτας (ή συμπληρώνει μια σελίδα στον Παγκόσμιο Ιστό), με τον ίδιο τρόπο που κάποιος σήμερα στέλνει μία κοινή πληροφορία με e-mail, σε μη κρυπτογραφημένη μορφή. Με τη μέθοδο αυτή εγκυμονεί ο κίνδυνος να αντιγραφεί η πληροφορία καθ' οδών. Η υπαιτιότητα του πελάτη για απατηλή χρήση σε τέτοιες περιπτώσεις τοποθετείται στο όριο των $50 όπως και σε κάθε άλλη συναλλαγή με πιστωτική κάρτα.
2. Ο πελάτης κρυπτογραφεί τα δεδομένα της πιστωτικής του κάρτας πριν τα αποστείλει π.χ. με PGP ή με SSL πρωτόκολλο. Δεδομένου του περιορισμού ότι ένας αποφασισμένος εισβολέας εξοπλισμένος με πολλούς Η/Υ και χρόνο μπορεί να «σπάσει» πάντα κάποιους από τους βραχύτερους κωδικούς στη χρήση, στην περίπτωσή μας ελαττώνεται ο κίνδυνος να αντιγραφούν οι λεπτομέρειες της πιστωτικής κάρτας από τρίτους. Στους κινδύνους συμπεριλαμβάνεται η περίπτωση ένα σύστημα κρυπτογράφησης να είναι ελαττωματικό, άσχημα υλοποιημένο ή χρησιμοποιούμενο σε ανασφαλή πλατφόρμα π.χ. σε μια που αποθηκεύει τα δεδομένα με αβέβαιο τρόπο.
3. Ο πελάτης έρχεται σε συμφωνία με έναν τρίτο, όπως η First Virtual Holdings, όπου οι λεπτομέρειες της πιστωτικής του κάρτας μεταφέρονται στον τρίτο με άλλο μέσο. Στην περίπτωση της First Visual κάθε συναλλαγή επιβεβαιώνεται με e-mail. Σε άλλες περιπτώσεις μπορούν να διατεθούν στον πελάτη δεδομένα ταυτοποίησης όπως PIN ή ένα ζευγάρι δημόσιου-ιδιωτικού κλειδιού, με το οποίο να υπογράφονται ψηφιακά τα μηνύματα. Και στις δύο περιπτώσεις οι συμμετέχοντες έμποροι ξεκαθαρίζουν τις συναλλαγές

μέσω τρίτων πριν η χρέωση ταχυδρομηθεί στην πιστωτική κάρτα του πελάτη.

4.5 Κατάθεση σε λογαριασμό, έμβασμα και μεταφορά

Τέλος, υπάρχουν και άλλες, παραδοσιακές μέθοδοι διεξαγωγής συναλλαγών, παραδοσιακές με την έννοια ότι απαντώνται στο φυσικό εμπόριο εδώ και αρκετές δεκαετίες, που μπορούν να εξυπηρετήσουν με αρκετή ασφάλεια το ηλεκτρονικό εμπόριο. Η κατάθεση χρημάτων σε λογαριασμό τρίτου, το έμβασμα και η μεταφορά επί πιστώσει σε λογαριασμό τρίτου μέσω της φυσικής ή ηλεκτρονικής τραπεζικής (e-banking) είναι οι πιο γνωστές από αυτές. Για την ενσωμάτωση των τριών αυτών συναλλακτικών μεθόδων στη λειτουργία του ηλεκτρονικού καταστήματος, αρκεί ο έμπορος να ενημερώσει τον πελάτη για τον αριθμό λογαριασμού όπου επιθυμεί να πιστωθούν ή να κατατεθούν τα χρήματα. Προκειμένου να εξυπηρετηθεί ο πελάτης, πρέπει να συμπληρώσει την ηλεκτρονική φόρμα και να καταθέσει (ή να μεταφέρει) τα χρήματα στο λογαριασμό που θα του υποδειχθεί. Για την ολοκλήρωση της παραγγελίας, χρειάζεται η τράπεζα του παρόχου να επιβεβαιώσει την κατάθεση των χρημάτων.

Οι εν λόγω τρόποι συναλλαγής για ηλεκτρονικές αγορές είναι και οι λιγότερο ελκυστικοί τόσο για τους πελάτες όσο και για τους εμπόρους για μια σειρά από λόγους. Καθυστέρηση ολοκλήρωσης συναλλαγής (καθώς απαιτείται επιβεβαίωση από την τράπεζα), δαπάνη χρόνου για τον πελάτη (όταν πρόκειται για καταθέσεις μέσω της φυσικής οδού), οικονομικές επιβαρύνσεις από τις τράπεζες (ειδικά στα εμβάσματα αλλά και στις μεταφορές χρημάτων) είναι ορισμένοι από αυτούς.

4.6 Τεχνικές Απάτης

Από τις περιπτώσεις που έχουν εντοπιστεί μέχρι σήμερα από τις τράπεζες, οι πιο διαδεδομένες μέθοδοι ηλεκτρονικής απάτης είναι οι εξής:

- **«Νιγηριανές απάτες»**. Η συγκεκριμένες τεχνικές διαδόθηκαν μέσω των ταχυδρομείων, αλλά συνεχίζουν να γίνονται μέχρι και τις μέρες μας μέσω e-mail. Στην Αμερική, είναι γνωστές επίσης σαν "Advance Fee fraud" ή "419 fraud" (το 419 έρχεται από το άρθρο 419 του Νιγηριανού Ποινικού Κώδικα, το οποίο απαγορεύει και καθιστά παράνομες τέτοιες απάτες). Στη περίπτωση αυτή κάποιος στέλνει ένα e-mail σε πολλαπλούς αποστολείς, όπου αναπτύσσει μια ολόκληρη ιστορία για μια μεταφορά χρημάτων που δεν μπορεί να την κάνει ο ίδιος. Όποιος απαντήσει στο mail κινδυνεύει να του αποσπάσει τον τραπεζικό λογαριασμό ή τα στοιχεία της κάρτας του.
- **Phishing**. Όπως το ίδιο το όνομά του υπονοεί, παραλλαγή του αγγλικού «fishing» (ψάρεμα), το Phishing αναφέρεται στην προσπάθεια απόσπασης προσωπικών στοιχείων, οικονομικού συνήθως χαρακτήρα που αφορούν τραπεζικούς λογαριασμούς και πιστωτικές κάρτες, χρησιμοποιώντας ως δόλωμα κάποιο ψεύτικο πρόσχημα. Το Phishing επιχειρείται συνήθως με τη αποστολή κάποιου spam e-mail**,** το οποίο ισχυρίζεται, ψευδώς, ότι αποστέλλεται από κάποια υπαρκτή και νόμιμη εταιρεία (τράπεζα, ηλεκτρονικό κατάστημα, υπηρεσία ηλεκτρονικών πληρωμών κλπ.), σε μία προσπάθεια να παραπλανήσει τον παραλήπτη και να του αποσπάσει απόρρητα προσωπικά και οικονομικά δεδομένα. Στη συνέχεια, τα στοιχεία αυτά θα χρησιμοποιηθούν από τους εγκέφαλους της απάτης για την πραγματοποίηση μη εξουσιοδοτημένων/παράνομων οικονομικών συναλλαγών. Τα e-mail αυτά ισχυρίζονται ότι ο παραλήπτης απαιτείται να ενημερώσει ή να επαληθεύσει άμεσα κάποια προσωπικά στοιχεία του για λόγους ασφαλείας, και τον οδηγούν μέσω συνδέσμων σε πλαστά web sites, τα οποία μιμούνται πολύ πειστικά τους διαδικτυακούς τόπους υπαρκτών και αξιόπιστων οργανισμών.
- **Skimming («ξάφρισμα»)**. Αποκαλείται και «σύγχρονη πληγή» των ATM. Τοποθετείται ένας λεπτός μηχανισμός πάχους μερικών χιλιοστών (κάποτε είχε πάχος περίπου 2 εκατοστά) στον

καρταναγνώστη (μέσα στην υποδοχή όπου βάζουμε την κάρτα) του ΑΤΜ. Ο μηχανισμός αυτός δεν διακρίνεται εύκολα από τον πελάτη, ο οποίος βάζει την κάρτα του στο ΑΤΜ και εκτελεί τη συναλλαγή του κανονικά. Ο μηχανισμός, όμως, αυτός αντιγράφει όλα τα στοιχεία της κάρτας. Έτσι, ο επιτήδειος έχει στα χέρια του το 16ψήφιο της κάρτας, αλλά του λείπει το PIN. Αυτό το υποκλέπτει με τους εξής τρόπους: Τοποθετώντας μικροκάμερα πάνω ή δίπλα στο ΑΤΜ, είτε παρατηρώντας ο επιτήδειος την πληκτρολόγηση του PIN από τον κάτοχο της κάρτας. Με τη μέθοδο αυτή ο επιτήδειος μπορεί να υποκλέψει στοιχεία πολλών καρτών σε μια «βάρδια». Τα στοιχεία αυτά είτε αποθηκεύονται στον μηχανισμό, είτε εκπέμπονται με έναν πομπό σε έναν συνεργάτη, ο οποίος αναλαμβάνει την αντιγραφή της κάρτας. Από τη στιγμή που είναι διαθέσιμα ο αριθμός της κάρτας και ο PIN, η καινούρια «πλαστή» κάρτα είναι έτοιμη για αγορές.

- **«Λιβανέζικες θηλιές» ή «Λιβανέζικοι βρόχοι»** . Σε ένα πολύ λεπτό πλαστικό δένεται με θηλιά μια λεπτή κλωστή. Το πλαστικό με την κλωστή τοποθετείται μέσα στην υποδοχή όπου μπαίνει η κάρτα στα ΑΤΜ. Όταν ο κάτοχος της κάρτας τη βάλει στην υποδοχή, αυτή μπλοκάρει. Τότε ένας πολύ ευγενικός κύριος προσπαθούσε να βοηθήσει και μεταξύ άλλων ρωτούσε και το PIN. Τελικά, όμως, δεν γινόταν τίποτα και μόλις ο κάτοχος της κάρτας απομακρυνόταν, ο επιτήδειος έπαιρνε την κάρτα, ενώ γνωρίζει και το PIN. Με τη μέθοδο αυτή μπορούν να κλαπούν 2-4 κάρτες την «βάρδια».
- **Γεννήτριες τυχαίων αριθμών**. Χρησιμοποιούνται συνήθως στις απάτες μέσω Internet. Υπάρχει ειδικό λογισμικό, το οποίο «παράγει» τυχαία 16ψήφιους αριθμούς. Ορισμένοι από αυτούς τυχαίνουν να συμπίπτουν με πραγματικές πιστωτικές κάρτες. Οι κάρτες αυτές χρεώνονται όταν ο επιτήδειος κάνει αγορές μέσω Internet.

Κεφάλαιο 5ο: Κρυπτογραφία

Εισαγωγή

Το Διαδίκτυο ήδη χρησιμοποιείται από εκατομμύρια χρήστες, και επεκτείνεται με εκθετικούς ρυθμούς αύξησης. Μπορεί να θεωρηθεί ένας χώρος επικοινωνίας, εκπαίδευσης και οικονομικής δραστηριότητας με διαρκώς αυξανόμενη δύναμη. Η νέα αυτή ψηφιακή κοινωνία οφείλει να παρέχει μηχανισμούς προστασίας του απαραβίαστου της προσωπικής ζωής των μελών της, το οποίο αποτελεί θεμελιώδες ανθρώπινο δικαίωμα.

Σε νομικό και κοινωνικό επίπεδο, τίθεται ζήτημα προστασίας του απορρήτου της ηλεκτρονικής αλληλογραφίας (e-mail), των συναλλαγών (αριθμός πιστωτικής κάρτας, τραπεζικό απόρρητο), του ιατρικού απορρήτου και γενικότερα το ζήτημα της προστασίας προσωπικών στοιχείων και δεδομένων του κάθε χρήστη του Διαδικτύου, που με διάφορους τρόπους μπορούν να συλλεχθούν από τρίτους και να χρησιμοποιηθούν για οποιονδήποτε σκοπό χωρίς τη συγκατάθεση του.

Σε ακαδημαϊκό επίπεδο, τίθεται θέμα προστασίας αποτελεσμάτων ακαδημαϊκής έρευνας, ευαίσθητων προσωπικών δεδομένων (βαθμολογία φοιτητών), ακαδημαϊκών μελετών και γενικότερα προστασίας των πνευματικών δικαιωμάτων (copyright) των μελών της ακαδημαϊκής κοινότητας.

Σε οικονομικό επίπεδο, η ασφάλεια και προστασία των εμπορικών πλέον δεδομένων, όπως η εξασφάλιση της εγκυρότητας των συναλλαγών μέσω της αποδοχής μίας ηλεκτρονικής υπογραφής και η ασφάλεια των συναλλαγών είναι κρίσιμα ζητήματα, που αποτελούν το υπόβαθρο της ψηφιακής παγκόσμιας αγοράς.

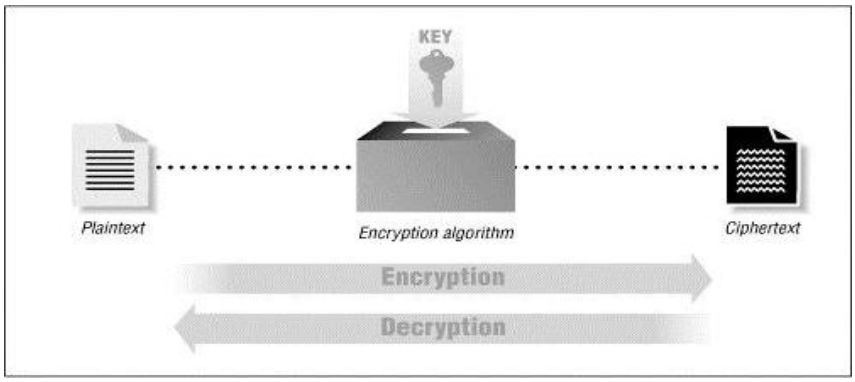
Η Κρυπτογραφία (cryptography) εξασφαλίζει το απόρρητο των προσωπικών πληροφοριών και είναι η τεχνολογική πλευρά της λύσης στα προαναφερθέντα ζητήματα ασφαλείας.

5.1 Τι είναι η κρυπτογραφία

Κρυπτογραφία είναι ο επιστημονικός κλάδος ο οποίος ασχολείται με τη μελέτη και σχεδίαση κρυπτογραφικών τεχνικών και συστημάτων, που βασίζονται σε μαθηματικά προβλήματα δύσκολο να λυθούν. Κρυπτανάλυση (cryptanalysis) είναι ο κλάδος ο οποίος ασχολείται με τη μελέτη τρόπων παραβίασης αυτών, και τέλος κρυπτολογία (cryptology) είναι ο συνδυασμός της κρυπτογραφίας και κρυπτανάλυση σε ένα ενιαίο επιστημονικό κλάδο.

Εφαρμογή της κρυπτογραφίας είναι η κρυπτογράφηση. Κρυπτογράφηση είναι μια διεργασία με την οποία ένα μήνυμα (που ονομάζεται **plaintext**) μετατρέπεται σε ένα άλλο μήνυμα (που ονομάζεται **ciphertext**) χρησιμοποιώντας μια μαθηματική συνάρτηση (αλγόριθμος κρυπτογράφησης ή **cipher**) και ένα ειδικό password κρυπτογράφησης, που ονομάζεται **κλειδί**. Σκοπός της κρυπτογράφησης είναι να εξασφαλίσει το απόρρητο των δεδομένων κρατώντας τα κρυφά από όλους όσους έχουν πρόσβαση σε αυτά

Αποκρυπτογράφηση (decryption) είναι η αντίστροφη διεργασία. Το ciphertext μετατρέπεται στο αρχικό κείμενο *(*plaintext*)* χρησιμοποιώντας μια άλλη μαθηματική συνάρτηση και ένα άλλο κλειδί (ή και το ίδιο). Η διεργασία της κρυπτογράφησης και της αποκρυπτογράφησης φαίνεται στην *Σχήμα 5.1*.



Σχήμα 5.1 Κρυπτογράφηση/Αποκρυπτογράφηση απλού κειμένου

Η κρυπτογράφηση και η αποκρυπτογράφηση απαιτούν, όπως είπαμε, την χρήση κάποιας μυστικής πληροφορίας, το κλειδί. Για μερικούς μηχανισμούς χρησιμοποιείται το ίδιο κλειδί και για την κρυπτογράφηση και για την αποκρυπτογράφηση, για άλλους όμως τα κλειδιά που χρησιμοποιούνται διαφέρουν.

Παράδειγμα

Στο σημείο αυτό θα παρουσιάσουμε ένα παράδειγμα plaintext :

“Ο αριθμός της πιστωτικής μου κάρτας είναι 3456344”

Το μήνυμα μπορεί να κρυπτογραφηθεί με έναν αλγόριθμο γνωστό ως Data Encryption Standard (DES) και ένα κλειδί mycard. Το αποτέλεσμα θα είναι το παρακάτω κρυπτογράφημα *(*ciphertext*):*

":"=3094~~!2f9kf09j4krfFgg

Όταν αυτό αποκρυπτογραφηθεί με το κλειδί mycard, θα αναπαραχθεί το αρχικό μήνυμα:

“Ο αριθμός της πιστωτικής μου κάρτας είναι 3456344”

Εάν προσπαθήσεις να αποκρυπτογραφήσεις το μήνυμα με ένα άλλο κλειδί, ίσως πάρεις το εξής :

Kdk$)_!9fk98+||3kf98fu3$#$#

Έτσι ο μόνος τρόπος να αποκρυπτογραφήσεις ένα ciphertext είναι να γνωρίζεις το μυστικό κλειδί mycard. Εάν δεν ξέρεις το μυστικό κλειδί και δεν έχεις πρόσβαση σε έναν πολύ γρήγορο υπολογιστή, δεν μπορείς να το αποκρυπτογραφήσεις. Ακόμα εάν χρησιμοποιήσεις ένα ισχυρό αλγόριθμο κρυπτογράφησης και ένας υπέρ-υπολογιστής δεν θα μπορέσει να σε βοηθήσει.

5.2 Κρυπτογραφικές υπηρεσίες και πρωτόκολλα

Η κρυπτογραφία, σύμφωνα με έναν από τους πολλούς ορισμούς που προτείνονται στη διεθνή βιβλιογραφία, ασχολείται με την επικοινωνία

παρουσία αντιπάλων. Ο λόγος που αποδεχόμαστε έναν τόσο γενικό ορισμό είναι γιατί και οι απειλές στις επικοινωνίες είναι ποικίλες, και η κρυπτογραφία παρέχει τη δυνατότητα αντιμετώπισής των. Οι κρυπτογραφικές υπηρεσίες είναι υπηρεσίες που χρησιμοποιώντας κρυπτογραφία, στοχεύουν στην αντιμετώπιση συγκεκριμένων απειλών. Οι κρυπτογραφικές υπηρεσίες είναι οι ακόλουθες:

- **Εμπιστευτικότητα** (Confidentiality). Είναι η προστασία από τη μη εξουσιοδοτημένη αποκάλυψη της πληροφορίας. Η εμπιστευτικότητα θα πρέπει να προσφέρεται με τέτοιον τρόπο ώστε να είναι αδύνατη η αποκάλυψη και πολλές φορές η ίδια η ύπαρξη της πληροφορίας σε μη εξουσιοδοτημένα άτομα. Για παράδειγμα κατά την κρίση στον Περσικό Κόλπο, η πληροφορία ότι η στρατιωτική ηγεσία των Ηνωμένων Πολιτειών προετοίμαζε επιχειρήσεις, διέρρεε λόγω του αυξημένου αριθμού παραγγελιών σε πιτσαρία γειτονική του Πενταγώνου κατά τις νυκτερινές ώρες.
- **Ακεραιότητα** (Integrity). Είναι η προστασία από τη μη εξουσιοδοτημένη τροποποίηση των δεδομένων. Η ακεραιότητα θα πρέπει να παρέχει στον παραλήπτη και γενικότερα στον κάτοχο ενός μηνύματος τη δυνατότητα να μπορεί να ανιχνεύσει πιθανές αλλαγές στο μήνυμα από μη εξουσιοδοτημένα άτομα. Στον χώρο των τηλεπικοινωνιών και της θεωρίας της πληροφορίας, η ακεραιότητα είναι γνωστή ως ανίχνευση σφαλμάτων, όπου ένα μήνυμα μπορεί να υποστεί τροποποίηση λόγω του θορύβου του καναλιού επικοινωνίας.
- **Αυθεντικοποίηση** (Authentication). Είναι η εξασφάλιση του ότι γνωρίζουμε το χρήστη ή γενικότερα την οντότητα που επικοινωνούμε (user/ entity authentication). Αυθεντικοποίηση δεδομένων (data authentication) είναι η εξασφάλιση ότι ένα μήνυμα προέρχεται πράγματι από τον αποστολέα που πιστεύουμε ότι το έστειλε.
- **Μη-απάρνηση** (non-repudiation). Είναι η υπηρεσία κατά την οποία ο παραλήπτης δεν μπορεί να απαρνηθεί ότι έλαβε το μήνυμα (μη-απάρνηση

προορισμού (non-repudiation of destination)), ή η υπηρεσία κατά την οποία ο αποστολέας δεν μπορεί να απαρνηθεί ότι έστειλε το μήνυμα (μη-απάρνηση προέλευσης (non-repudiation of origin)).

Θα πρέπει να σημειωθεί ότι υπάρχει αλληλεξάρτηση της **ακεραιότητας** και της **αυθεντικοποίησης** ενός μηνύματος. Δεν είναι δυνατό να προσφέρεται με επιτυχία μόνον ακεραιότητα χωρίς να προσφέρεται αυθεντικοποίηση και αντίστροφα. Σε περίπτωση που προσφέρεται αυθεντικοποίηση χωρίς ακεραιότητα, ο αντίπαλος μπορεί να τροποποιήσει την πληροφορία αυθεντικοποίησης, προσδίδοντας διαφορετικό κάτοχο στο μήνυμα. Σε περίπτωση που προσφέρεται ακεραιότητα χωρίς αυθεντικοποίηση, ο αντίπαλος μπορεί ανεξέλεγκτα να τροποποιήσει το μήνυμα και να επαναϋπολογίσει το κρυπτογραφικό άθροισμα ελέγχου που προσδιορίζει την ακεραιότητα του μηνύματος.

Κρυπτογραφικό πρωτόκολλο είναι η πλήρως αποσαφηνισμένη διαδικασία που πρέπει να ακολουθήσουν τα επικοινωνούντα μέλη, προκειμένου να επιτύχουν μια συγκεκριμένη κρυπτογραφική υπηρεσία.

Το βασικό χαρακτηριστικό του κρυπτογραφικού πρωτοκόλλου είναι ότι πρέπει το κάθε μέλος να γνωρίζει σε κάθε χρονική στιγμή (κατά τη διάρκεια εκτέλεσης του πρωτοκόλλου) ποιο βήμα πρέπει να εκτελεστεί και πως πρέπει να εκτελεστεί. Οποιαδήποτε παρέκκλιση από τη διαδικασία που απαιτεί το κρυπτογραφικό πρωτόκολλο έχει ως αποτέλεσμα την κατάρρευση της επικοινωνίας ή της υποκείμενης κρυπτογραφικής υπηρεσίας.

5.3 Οι «ρίζες» της κρυπτογραφίας

Η ιδέα της κρυπτογράφησης δεν είναι νέα υπόθεση. Ακόμη και στην αρχαιότητα Έλληνες και Ρωμαίοι στρατηγοί χρησιμοποιούσαν διάφορες μεθόδους κρυπτογράφησης για να επικοινωνούν με τους επιτελείς τους κατά την διάρκεια των μαχών, με κωδικοποιημένα μηνύματα τα οποία δεν

θα ήταν δυνατόν να τα διαβάσουν οι εχθροί του. Αυτές οι μέθοδοι βασιζόταν κυρίως σε δύο τεχνικές:

α) την **αντικατάσταση** και

β) την **αντιμετάθεση**.

5.3.1 Κώδικες αντικατάστασης

Ο πιο χαρακτηριστικός κώδικας αντικατάστασης (substitution cipher) των αρχαίων χρόνων είναι αυτός του Ιουλίου Καίσαρα. Ο κώδικας αυτός βασιζόταν στην *αντικατάσταση* κάθε γράμματος του αλφαβήτου με κάποιο άλλο, όχι όμως τυχαία επιλεγμένο. Ο κώδικας κρυπτογράφησης είναι η ολίσθηση των γραμμάτων του αλφαβήτου προς τα δεξιά. Κάθε γράμμα αντικαθίσταται από κάποιο άλλο με κάποιο κλειδί π.χ. 3. Δηλαδή, η κρυπτογράφηση ενός μηνύματος γίνεται με αντικατάσταση κάθε γράμματος από το γράμμα που βρίσκεται 3 θέσεις δεξιότερά του στο αλφάβητο. Θα μπορούσε φυσικά το κλειδί να ήταν 6, οπότε το κρυπτογραφημένο κείμενο που θα προέκυπτε θα ήταν διαφορετικό. Έτσι, διατηρώντας τον ίδιο κώδικα κρυπτογράφησης και επιλέγοντας διαφορετικό κλειδί παράγονται διαφορετικά κρυπτογραφημένα μηνύματα.

Η αντιστοίχηση των γραμμάτων με κλειδί 3 φαίνεται στον παρακάτω πίνακα:

Το γράμμα	a	b	c	d	e	f	.	.	.	t	u	v	w	x	y	z
Αντικαθίσταται από το γράμμα	d	e	f	g	h	i	.	.	.	w	x	y	z	a	b	c

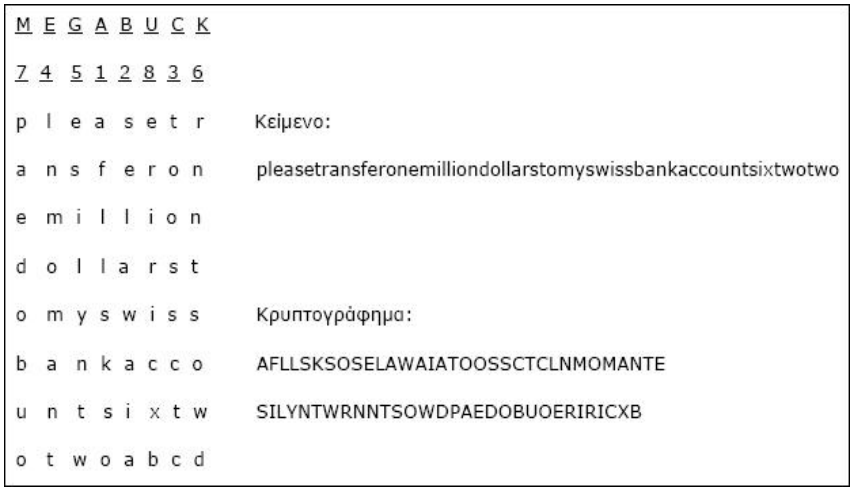
Πίνακας 5.1 Αντιστοίχηση των γραμμάτων με κλειδί 3

Αν, για παράδειγμα, το απλό κείμενο είναι η λέξη “enemy”, θα προκύψει το κρυπτογράφημα “hqhpb”. Για να το αποκρυπτογραφήσει κάποιος θα πρέπει να αντιστρέψει τη διαδικασία κρυπτογράφησης, με άλλα λόγια να αντικαταστήσει κάθε γράμμα με αυτό που βρίσκεται 3 θέσεις αριστερότερά του στο αλφάβητο. Προφανώς, δεν αρκεί να ξέρει ότι ο κατάλληλος

αλγόριθμος αποκρυπτογράφησης είναι η ολίσθηση των γραμμάτων του αλφαβήτου προς τα αριστερά, αλλά πρέπει να γνωρίζει και πόσες θέσεις χρειάζεται να τα ολισθήσει. Πρέπει να γνωρίζει το κλειδί, που σε αυτήν την περίπτωση είναι ο αριθμός 3.

5.3.2 Κώδικες Αντιμετάθεσης

Οι κώδικες αντικατάστασης, όπως είδαμε πιο πριν, διατηρούν τη σειρά των συμβόλων του κειμένου αλλά τα μεταμφιέζουν. Οι κώδικες αντιμετάθεσης (*transposition ciphers*) αντίθετα, αναδιατάσσουν τα σύμβολα αλλά δεν τα μεταμφιέζουν. Κάτι ανάλογο χρησιμοποιούσαν οι αρχαίοι Σπαρτιάτες όταν έγραφαν το κείμενό τους (σε σειρές) σε μια λωρίδα τυλιγμένη σε κύλινδρο, την οποία όταν ξετύλιγαν είχε τα γράμματα ανακατεμένα (σε μία στήλη), και για να διαβαστεί ξανά το μήνυμα από τον παραλήπτη του έπρεπε να χρησιμοποιηθεί κύλινδρος ίδιων διαστάσεων. Το σχήμα 5.2 δείχνει έναν συνήθη κώδικα αντιμετάθεσης, την αντιμετάθεση στηλών. Ο κώδικας έχει για κλειδί μια λέξη ή φράση που δεν περιέχει επαναλαμβανόμενα γράμματα. Στο παράδειγμα αυτό το κλειδί είναι το MEGABUCK. Ο σκοπός του κλειδιού είναι να αριθμήσει τις στήλες, θεωρώντας ως $1^{η}$ στήλη αυτή που βρίσκεται κάτω από το γράμμα του κλειδιού που βρίσκεται πιο κοντά στην αρχή τον αλφάβητου, κοκ. Το κείμενο γράφεται οριζόντια, σε σειρές. Το κρυπτογράφημα διαβάζεται ανά στήλη, με πρώτη τη στήλη της οποίας το γράμμα-κλειδί είναι το μικρότερο.



Σχήμα 5.2 Ένας κώδικας αντιμετάθεσης.

5.3.3 Κρυπτογραφία στο παρόν και στο μέλλον

Σήμερα ο κύριος ρόλος της κρυπτογραφίας είναι να προστατεύσει τις ηλεκτρονικές επικοινωνίες. Αμέσως μετά το γεγονός που ο Samuel Morse δημόσια παρουσίασε τον τηλέγραφο το 1845, οι χρήστες του τηλέγραφου άρχισαν να ανησυχούν για το πόσο εμπιστευτικά ήταν τα μηνύματα που μετέφεραν. Τι θα γινόταν αν κάποιος ηχογραφούσε την γραμμή του τηλέγραφου; Τι θα εμπόδιζε τον ασυνείδητο τηλεγραφητή να κρατήσει ένα αντίγραφο του μηνύματος που θα το αναμετάδιδε και σε άλλους; Η απάντηση ήταν να κωδικοποιήσουν τα μηνύματα με ένα μυστικό κώδικα έτσι ώστε μόνο ο παραλήπτης να μπορούσε να τα αποκωδικοποιήσει.

Η κρυπτογραφία έγινε ακόμα ποιο σημαντική με την εφεύρεση της ραδιοτηλεφωνίας και τη χρήση της στον πόλεμο. Χωρίς κρυπτογραφία, τα μηνύματα που μεταδίδονταν μεταξύ συμμάχων μπορούσαν να υποκλέπτονταν από τον εχθρό.

Οι σημερινές τεχνολογίες κρυπτογράφησης, παρότι παρέχουν μεγάλο ποσοστό ασφάλειας, έχει αποδειχθεί ότι δεν είναι άτρωτες. Η απάντηση στο πρόβλημα είναι η χρήση της κβαντικής Φυσικής. Εν συντομία, το σκεπτικό έχει ως εξής: οποιαδήποτε προσπάθεια παρατήρησης ενός κβαντικού

συστήματος αυτόματα προκαλεί την "αλλοίωσή" του. Κατ' αυτό τον τρόπο, ακόμη και η παραμικρή προσπάθεια υποκλοπής γίνεται αμέσως αντιληπτή. Η κβαντική κρυπτογράφηση βρίσκεται εδώ και μια δεκαετία στο στάδιο των εργαστηριακών δοκιμών, αλλά σύντομα αναμένεται να εφαρμοστεί και εμπορικά.

5.4 Τι μπορούμε να επιτύχουμε με την κρυπτογράφηση

Στις μέρες μας κρυπτογραφία δεν είναι μόνο κρυπτογράφηση και αποκρυπτογράφηση. Εκτός από την διασφάλιση του απόρρητου (*privacy*), η αυθεντικοποίηση (*authentication*) είναι άλλη μία έννοια που έχει γίνει μέρος της ζωής μας. Πιστοποιούμε την ταυτότητα μας καθημερινά και ανεπαίσθητα, για παράδειγμα όταν υπογράφουμε ένα έγγραφο, όταν δείχνουμε την ταυτότητα μας. Καθώς ο κόσμος εξελίσσεται σε ένα περιβάλλον που όλες οι αποφάσεις και οι συναλλαγές θα γίνονται ηλεκτρονικά, χρειαζόμαστε ηλεκτρονικές τεχνικές που θα επιτελούν την πιστοποίηση της ταυτότητας μας.

Η κρυπτογραφία παρέχει μηχανισμούς για τέτοιες διαδικασίες. Η ψηφιακή υπογραφή συνδέει ένα έγγραφο με τον κάτοχο ενός κλειδιού έτσι ώστε όλοι όσοι είναι σε θέση να το αναγνώσουν να είναι σίγουροι για το ποιος το έχει γράψει. Επίσης, μία ψηφιακή χρονοσφραγίδα (*digital timestamp*) συνδέει ένα έγγραφο με την ώρα της δημιουργίας του. Τέτοιοι μηχανισμοί μπορούν να χρησιμοποιηθούν για έλεγχο πρόσβασης σε ένα σκληρό δίσκο, για ασφαλής συναλλαγές μέσω του Διαδικτύου ή ακόμα και για σύνδεση με καλωδιακή τηλεόραση.

Αναφορικά μπορούμε να σημειώσουμε ότι η κρυπτογράφηση μπορεί να παίξει σημαντικό ρόλο στις καθημερινές μας υπολογιστικές και επικοινωνιακές μας ανάγκες με τους εξής τρόπους:

- ✓ Μπορεί να προστατεύσει πληροφορίες αποθηκευμένες στον υπολογιστή μας από πρόσβαση ενός τρίτου, με ή χωρίς άδεια.

- ✓ Μπορεί να προστατεύσει πληροφορίες κατά την διάρκεια της μεταφοράς από ένα υπολογιστικό σύστημα στο άλλο.
- ✓ Μπορεί να χρησιμοποιηθεί για να εμποδίσει και για να εντοπίσει τυχαίες ή σκόπιμες αλλαγές στα δεδομένα μας.
- ✓ Μπορεί να χρησιμοποιηθεί για να επικυρώσει την ταυτότητα του δημιουργού.

Πέρα από αυτά τα πλεονεκτήματα, υπάρχουν και κάποια όρια τα οποία πρέπει να γνωρίζουμε για να αποφεύγουμε τα ανεπιθύμητα αποτελέσματα :

- Η κρυπτογράφηση δεν μπορεί να προφυλάξει τα δεδομένα μας από κάποιον εισβολέα που θέλει να σβήσει τα δεδομένα μας όπως είναι.
- Ένας εισβολέας μπορεί να έχει τροποποιήσει και να εκθέτει ένα πρόγραμμα κρυπτογράφησης από μόνος του, έτσι ώστε να μπορεί να αποκρυπτογραφήσει όλα τα μηνύματα με το δικό του κλειδί. Ή μπορεί να κρατά σε ένα αρχείο όλα τα κλειδιά για να τα χρησιμοποιήσει αργότερα.
- Ένας εισβολέας μπορεί να έχει πρόσβαση στα αρχεία μας πριν τα κρυπτογραφήσουμε και αφού τα αποκρυπτογραφήσουμε.
- Ένας εισβολέας ίσως βρει έναν άγνωστο προηγούμενα και σχετικά εύκολο τρόπο να αποκρυπτογραφεί τα μηνύματα που εμείς κρυπτογραφούμε με κάποιο αλγόριθμο.

Για όλους αυτούς του λόγους, η κρυπτογράφηση θα πρέπει να θεωρείται σαν ένα μέρος της ολικής στρατηγικής ασφαλείας που έχουμε, και όχι σαν υποκατάστατο άλλων μέτρων ασφαλείας που πρέπει να έχουμε, όπως είναι ο κατάλληλος έλεγχος πρόσβασης στον υπολογιστή μας.

5.5 Στοιχεία της κρυπτογράφησης

Υπάρχουν πολλοί και διάφοροι τρόποι με τους οποίους μπορούμε να κρυπτογραφήσουμε και να αποκρυπτογραφήσουμε μια πληροφορία.

Παρόλα αυτά, όλα τα συστήματα κρυπτογράφησης μοιράζονται κάποια κοινά στοιχεία. Αυτά είναι τα εξής:

Απλό ή μη κρυπτογραφημένο κείμενο (plaintext)

Τα δεδομένα όπως χρησιμοποιούνται από τους ανθρώπους ή τις εφαρμογές.

Κρυπτογραφημένο κείμενο (ciphertext)

Τα δεδομένα σε ακατάληπτη για τους ανθρώπους ή τις εφαρμογές μορφή.

Κρυπτογράφηση (encryption)

Ο μετασχηματισμός του απλού κειμένου σε κρυπτογραφημένο κείμενο.

Αποκρυπτογράφηση (decryption)

Ο μετασχηματισμός του κρυπτογραφημένου κειμένου σε απλό.

Αλγόριθμος κρυπτογράφησης (encryption algorithm)

Ο αλγόριθμος κρυπτογράφησης είναι μια συνάρτηση, συνήθως μαθηματικών αρχών, η οποία εκτελεί το έργο της κρυπτογράφησης των δεδομένων μας.

Αλγόριθμος αποκρυπτογράφησης (decryption algorithm)

Ο αλγόριθμος αποκρυπτογράφησης είναι μια συνάρτηση, συνήθως μαθηματικών αρχών, η οποία εκτελεί το έργο της αποκρυπτογράφησης των δεδομένων μας.

Κρυπταλγόριθμος (cipher)

Ο κρυπταλγόριθμος αποτελείται από τον αλγόριθμο κρυπτογράφησης και τον αλγόριθμος αποκρυπτογράφησης.

Κλειδιά κρυπτογράφησης

Τα κλειδιά κρυπτογράφησης χρησιμοποιούνται από τον αλγόριθμο κρυπτογράφησης για να ορίσουν πώς τα δεδομένα είναι κρυπτογραφημένα ή αποκρυπτογραφημένα. Τα κλειδιά είναι παρόμοια με τα password των υπολογιστών. Όταν ένα μέρος μιας πληροφορίας κρυπτογραφείται, πρέπει να έχουμε το σωστό κλειδί για να έχουμε πρόσβαση πάλι σε αυτό. Στη περίπτωση που ένα πρόγραμμα χρησιμοποιεί password για την πρόσβαση

μας σε αυτό, τότε το πρόγραμμα ελέγχει αν το κλειδί που του δίνουμε, για να εισέλθουμε στο πρόγραμμα, ταιριάζει με το κλειδί που αρχικά ορίσαμε για να το κλειδώσουμε, και εάν τα δύο αυτά κλειδιά ταιριάζουν τότε και μόνο μας επιτρέπεται η πρόσβαση στο πρόγραμμα. Αντίθετα ένα πρόγραμμα κρυπτογράφησης χρησιμοποιεί το κλειδί μας για να μετατρέψει το κρυπτογραφημένο μήνυμα (*ciphertext*) στο αρχικό κείμενο (*plaintext*). Εάν δώσουμε το σωστό κλειδί θα πάρουμε το αρχικό μήνυμα. Εάν όμως το κλειδί μας δεν είναι σωστό τότε στη περίπτωση αυτή θα πάρουμε σκουπίδια.

Μήκος κλειδιών

Όπως και με τα password, τα κλειδιά κρυπτογράφησης έχουν ένα προκαθορισμένο μήκος. Τα μεγαλύτερα κλειδιά είναι πιο δύσκολο να τα μαντέψει κάποιος σε σχέση με τα μικρότερα καθώς υπάρχουν περισσότερα πιθανά κλειδιά που πρέπει να δοκιμάσει κάποιος επιτιθέμενος, για να βρει το σωστό. Μερικά συστήματα κρυπτογράφησης μας επιτρέπουν να χρησιμοποιούμε διαφορετικό μήκος κλειδιών και άλλα μεταβλητού μήκους κλειδιών.

5.6 Κρυπτογραφικά εργαλεία

Σ' αυτό το σημείο θα ασχοληθούμε με τους μηχανισμούς με τους οποίους εφαρμόζεται η κρυπτογραφία γενικότερα.

5.6.1 Block Ciphers

Ο **block cipher** είναι ένας τύπος αλγόριθμου συμμετρικής κρυπτογράφησης που μετατρέπει ένα τμήμα (block) μη κρυπτογραφημένου καθορισμένου μήκους κειμένου (plaintext), σε τμήμα κρυπτογραφημένου του ίδιου μήκους κειμένου *(*ciphertext*)*. Αυτός ο μετασχηματισμός πραγματοποιείται με την βοήθεια ενός μυστικού κλειδιού που χορηγείται από τον χρήστη. Η αποκρυπτογράφηση γίνεται με την εφαρμογή του αντίστροφου μετασχηματισμού στο κρυπτογραφημένο κείμενο χρησιμο-

ποιώντας το ίδιο μυστικό κλειδί (ή και διαφορετικό). Το καθορισμένο μήκος καλείται *block size* και για πολλούς αλγορίθμους (ciphers) είναι 64 bits. Στα μελλοντικά χρόνια το μήκος θα αυξηθεί στα 128 bits καθώς οι υπολογιστές γίνονται πιο ικανοί. Κάθε κείμενο δίνει διαφορετικό ciphertext.

Οι block ciphers λειτουργούν επαναληπτικά, κρυπτογραφώντας ένα τμήμα διαδοχικά αρκετές φορές. Σε κάθε επανάληψη, ο ίδιος μετασχηματισμός εφαρμόζεται στα δεδομένα χρησιμοποιώντας ένα *subkey*. Το σύνολο των subkeys προέρχεται από το μυστικό κλειδί που χορήγησε ο χρήστης, με ειδική συνάρτηση. Το σύνολο των subkeys καλείται *key schedule*.
Ο αριθμός των επαναλήψεων του επαναληπτικού αλγορίθμου (cipher) εξαρτάται από το επίπεδο της επιθυμητής ασφάλειας και την απόδοση του συστήματος. Στις περισσότερες περιπτώσεις, ο αυξημένος αριθμός επαναλήψεων βελτιώνει την προσφερόμενη ασφάλεια, αλλά για μερικούς αλγόριθμους ο αριθμός των επαναλήψεων για να επιτευχθεί ικανοποιητική ασφάλεια θα είναι πολύ μεγάλος για να πραγματοποιηθεί.

5.6.2 Steam Ciphers

Ο **Stream cipher** είναι ένας τύπος αλγόριθμου συμμετρικής κρυπτογράφησης. Είναι εξαιρετικά ταχύτατοι αλγόριθμοι, κατά πολύ ταχύτεροι από τους block ciphers. Σε αντίθεση με τους block ciphers που λειτουργούν με μεγάλα τμήματα δεδομένων *(blocks)*, οι stream ciphers τυπικά λειτουργούν με μικρότερες μονάδες απλού κειμένου, συνήθως με bits. Η κρυπτογράφηση ενός συγκεκριμένου κειμένου με έναν block cipher θα καταλήγει πάντα στο ίδιο αποτέλεσμα όταν χρησιμοποιείται το ίδιο κλειδί. Με έναν stream cipher, ο μετασχηματισμός των μικρότερων αυτών μονάδων θα ποικίλει, ανάλογα με το πότε αντιμετωπίζονται κατά την διάρκεια της κρυπτογράφησης.

Ένας stream cipher παράγει μια ακολουθία από bits που χρησιμοποιείται σαν κλειδί και καλείται keystream. Η κρυπτογράφηση επιτυγχάνεται με τον

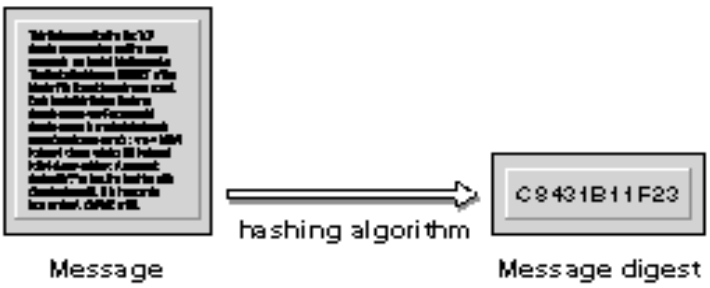
συνδυασμό του keystream με το plaintext, συνήθως μέσω μιας X-OR πράξης. Η παραγωγή του keystream μπορεί να είναι ανεξάρτητη του plaintext και του ciphertext *(synchronous stream cipher)* ή μπορεί να εξαρτάται από αυτά *(self-synchronizing stream cipher)*. Οι περισσότεροι stream ciphers είναι synchronous.

5.6.3 Hash Functions

Ο όρος *hash function* υποδηλώνει ένα μετασχηματισμό ο οποίος παίρνει σαν είσοδο ένα μήνυμα m οποιουδήποτε μήκους και επιστρέφει στην έξοδο μία ακολουθία χαρακτήρων h περιορισμένου μήκους που καλείται *hash value*, δηλαδή είναι *h=H(m)*. Οι hash functions είναι συναρτήσεις της μορφής *H(x)=y*, με τις εξής ιδιότητες:

1. η είσοδος είναι οποιουδήποτε μήκους,
2. η έξοδος έχει περιορισμένο μήκος,
3. δεδομένου του *x*, ο υπολογισμός του *y* είναι εύκολος,
4. η *H(x)* είναι μη αντιστρέψιμη,
5. η *H(x)* είναι αμφιμονοσήμαντη (ένα προς ένα συνάρτηση).

Η hash value παρουσιάζει συνοπτικά το μεγαλύτερο μήνυμα ή έγγραφο, γι' αυτό καλείται και σύνοψη μηνύματος (*message digest*), *Σχήμα 5.3*. Μπορούμε να φανταστούμε την σύνοψη του μηνύματος σαν "ψηφιακό αποτύπωμα" *("digital fingerprint")* του εγγράφου. Παραδείγματα γνωστών hash functions είναι οι MD2, MD5 και SHA.



Σχήμα 5.3 Hash function

Επειδή οι hash functions είναι πιο γρήγορες από τους αλγόριθμους κρυπτογράφησης και ψηφιακών υπογραφών, συνηθίζεται να παράγεται η υπογραφή των μηνυμάτων με την εφαρμογή κρυπτογραφικών διαδικασιών στο message digest, το οποίο είναι πιο μικρό και εύκολο στην διαχείριση. Επιπλέον ένα message digest μπορεί να δημοσιοποιηθεί χωρίς να αποκαλύπτει τα περιεχόμενα του αυθεντικού κειμένου.

5.7 Είδη Κρυπτογραφίας

Υπάρχουν δύο βασικά είδη κρυπτογραφικών αλγόριθμων σε χρήση σήμερα:

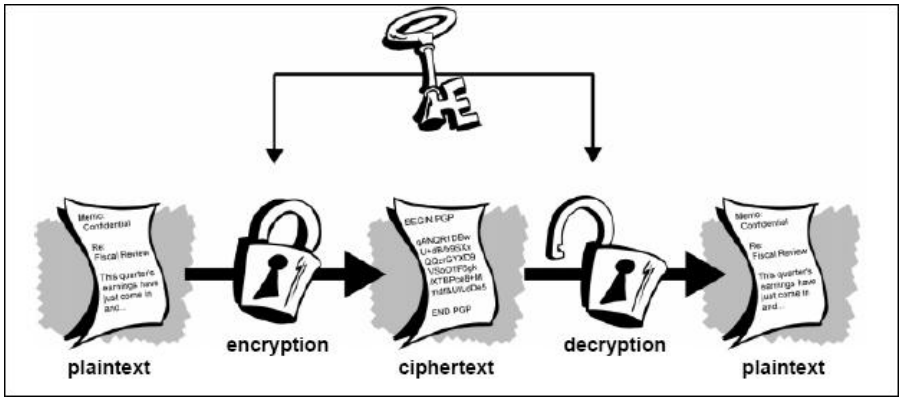
- **Συμμετρική Κρυπτογραφία** (*symmetric-key cryptography*), η οποία χρησιμοποιεί το ίδιο κλειδί για να κρυπτογραφήσει και να αποκρυπτογραφήσει το μήνυμα. Αυτός ο τύπος είναι επίσης γνωστός σαν κρυπτογραφία προσωπικού κλειδιού (*private-key cryptography*) ή και μυστικού κλειδιού (*secret-key cryptography*).
- **Ασύμμετρη Κρυπτογραφία** (*asymmetric-key cryptography*), η οποία χρησιμοποιεί ένα δημόσιο κλειδί (public key) για να κρυπτογραφήσει το μήνυμα, και ένα προσωπικό κλειδί (private key) για να το αποκρυπτογραφήσει. Το όνομα "δημόσιο κλειδί" οφείλεται στο γεγονός ότι μπορούμε να κάνουμε το κλειδί αυτό δημοσίως γνωστό χωρίς να διακινδυνεύσουμε την μυστικότητα του μηνύματος ή του κλειδιού αποκρυπτογράφησης. Τα συστήματα ασύμμετρου κλειδιού είναι επίσης γνωστά σαν κρυπτογραφία δημόσιου κλειδιού (*public-key cryptography*).

5.7.1 Συμμετρική Κρυπτογραφία (Symmetric-Key Cryptography)

Η μοντέρνα κρυπτογραφία χρησιμοποιεί τις ίδιες βασικές ιδέες με την παραδοσιακή κρυπτογραφία, δηλαδή την αντιμετάθεση και την αντικατάσταση, αλλά με διαφορετική έμφαση. Παραδοσιακά οι

κρυπτογράφοι χρησιμοποιούσαν απλούς αλγόριθμους και στήριζαν την ασφάλεια σε μεγάλα κλειδιά. Σήμερα ισχύει το αντίστροφο: ο στόχος είναι να γίνει ο αλγόριθμος τόσο περίπλοκος, ώστε ακόμα και αν ο κρυπταναλυτής αποκτήσει τεράστιες ποσότητες κρυπτογραφημάτων της δικής του επιλογής, να μην είναι σε θέση να βγάλει κανένα απολύτως νόημα.

Η βασική ιδέα των αλγορίθμων συμμετρικού κλειδιού (ή αλλιώς μυστικού κλειδιού) φαίνεται στο *Σχήμα 5.4*. Το ίδιο κλειδί που χρησιμοποιείται για την κρυπτογράφηση, χρησιμοποιείται και για την αποκρυπτογράφηση.



Σχήμα 5.4 Συμμετρική Κρυπτογραφία

Στη συμμετρική κρυπτογραφία υπάρχουν αρκετοί αλγόριθμοι, εκ των οποίων ο πιο γνωστός είναι ο Data Encryption Standard (**DES**). Εκτός του DES, όμως, υπάρχει ένας μεγάλος αριθμός κρυπτογραφικών αλγορίθμων, κάθε ένας από τους οποίους έχει τα δικά του χαρακτηριστικά, πλεονεκτήματα και μειονεκτήματα. Οι πιο ευρέως χρησιμοποιούμενοι, συμπεριλαμβανομένου και του DES, είναι οι ακόλουθοι:

- **DES** (*Data Encryption Standard*), αρχικά αναπτύχθηκε από την IBM το 1977, ενώ σημαντικό ρόλο στην ανάπτυξη του έπαιξε η NSA (*National Security Agency*) και το NIST (*National Institute of Standards and Technology*). Είναι ο πιο γνωστός και παγκόσμια

χρησιμοποιούμενος συμμετρικός αλγόριθμος. Ο DES κρυπτογραφεί ανά τμήματα (blocks) των 64 bits (8 bytes) με 16 επαναλήψεις για κάθε τμήμα, χρησιμοποιώντας ένα κλειδί των 56 bits. Όταν χρησιμοποιείται για την επικοινωνία, αποστολέας και παραλήπτης μοιράζονται το ίδιο κλειδί. Επίσης, μπορεί να χρησιμοποιηθεί για κρυπτογράφηση αρχείων αποθηκευμένα σε σκληρό δίσκο σε περιβάλλοντα ενός χρήστη.

- **Triple-DES** είναι μια παραλλαγή του DES, και κρυπτογραφεί τρεις φορές το ίδιο κείμενο με τον αλγόριθμο DES, αλλά χρησιμοποιώντας διαφορετικό κλειδί για κάθε κρυπτογράφηση.
- **DESX** είναι μια άλλη παραλλαγή του DES. Η διαφορά του DES και του DESX είναι ότι η είσοδος, καθώς και η έξοδος της κρυπτογράφησης, στο DESX, περνάει από μια X-OR πράξη με ένα επιπλέον κλειδί 64 bits. Η αιτία ανάπτυξης του DESX είναι η δραματική μείωση της «αντοχής» του DES σε γνωστές επιθέσεις.
- **IDEA** (*International Data Encryption Algorithm*), είναι ένας block cipher που αναπτύχθηκε από τους Lai και Massey το 1990 και είναι δομημένος όπως το DES. Κρυπτογραφεί τμήματα (blocks) των 64 bits χρησιμοποιώντας ένα κλειδί μήκους 128 bits. Η διαδικασία της κρυπτογράφησης απαιτεί 8 σύνθετες επαναλήψεις για κάθε τμήμα. Η αποκρυπτογράφηση γίνεται με τον ίδιο τρόπο που γίνεται και η κρυπτογράφηση. Έχει σχεδιαστεί να είναι εύκολα εφαρμόσιμος τόσο σε hardware όσο και σε software. Μερικές, όμως, αριθμητικές διεργασίες που χρησιμοποιεί ο IDEA καθιστούν τις λογισμικές εφαρμογές αργές, παρόμοιες σε ταχύτητα με τον DES. Ο IDEA αποτελεί ένα πολύ δυνατό αλγόριθμο που είναι απρόσβλητος από τα περισσότερα είδη επιθέσεων.
- **RC2** είναι ένας block cipher με κλειδί μεταβλητού μήκους που σχεδιάστηκε από τον Ron Rivest για την RSA Inc. Τα αρχικά σημαίνουν "Ron's Code" ή "Rivest's Cipher". Είναι γρηγορότερος

από τον DES και στόχος της σχεδίασης ήταν να λειτουργήσει για αντικατάσταση του DES. Μπορεί να γίνει περισσότερο ή λιγότερο ασφαλής από τον DES, ανάλογα με το μήκος του κλειδιού. Έχει μέγεθος block ίσο με 64 bits και είναι έως και τρεις φορές ταχύτερος από τον DES.

- **RC4** είναι ένας stream cipher που σχεδιάστηκε πάλι από την Ron Rivest για λογαριασμό της RSA Inc. Έχει μεταβλητό μήκος κλειδιού και λειτουργεί στο επίπεδο του byte. Θεωρείται εξαιρετικά ασφαλής και οι υλοποιήσεις του σε λογισμικό τρέχουν πολύ γρήγορα. Χρησιμοποιείται για κρυπτογράφηση τοπικά αποθηκευμένων αρχείων και για την διασφάλιση της επικοινωνίας μεταξύ δύο απομακρυσμένων σημείων μέσω του πρωτοκόλλου SSL.
- **RC5** είναι ένας γρήγορος block cipher από τον Ron Rivest για λογαριασμό της RSA Inc το 1994. Έχει πολλές παραμέτρους: μεταβλητό μήκος κλειδιού, μεταβλητό μέγεθος block και μεταβλητό αριθμό επαναλήψεων. Τυπικές επιλογές για το μέγεθος του block είναι 32 bits (για πειραματικές εφαρμογές), 64 bits (για αντικατάσταση του DES) και 128 bits. Ο αριθμός των επαναλήψεων μπορεί να είναι από 0 έως και 255. Ο RC5 είναι πολύ απλός στην λειτουργία, πράγμα που τον κάνει εύκολο στην ανάλυση.
- **Blowfish**, είναι ένας block cipher που κατασκευάστηκε από τον Schneier. Κρυπτογραφεί τμήματα (blocks) των 64 bits και έχει μεταβλητό μήκος κλειδιού, με μέγιστο μήκος 448 bits. Όλες οι διεργασίες βασίζονται σε X-OR πράξεις και προσθέσεις λέξεων των 32 bits. Από το κλειδί παράγεται πίνακας με τα subkeys που χρησιμοποιούνται σε κάθε γύρο επανάληψης της κρυπτογράφησης. Έχει σχεδιασθεί για 32-bit μηχανές και είναι αρκετά ταχύτερος από τον DES. Παρ’ όλες τις αδυναμίες που έχουν ανακαλυφθεί καθ' όλη την διάρκεια της ύπαρξης του, θεωρείται ακόμα ασφαλής αλγόριθμος.

5.7.2 Ασύμμετρη Κρυπτογραφία (Asymmetric-Key Cryptography)

Από ιστορικής πλευράς, το πρόβλημα της διανομής των κλειδιών ήταν πάντα ο αδύναμος κρίκος των περισσότερων κρυπτοσυστημάτων. Άσχετα με το πόσο δυνατό ήταν το κρυπτοσύστημα, εάν ένας παρείσακτος μπορούσε να κλέψει το κλειδί το σύστημα ήταν άχρηστο. Εφόσον όλοι οι κρυπτολόγοι θεωρούσαν δεδομένο ότι τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης ήταν τα ίδια (ή θα προέκυπταν εύκολα το ένα από το άλλο) και το κλειδί έπρεπε να διανεμηθεί σ' όλους τους χρήστες του συστήματος, φαινόταν σαν να υπήρχε ένα εγγενές πρόβλημα: τα κλειδιά έπρεπε να προφυλαχθούν από κλοπή, αλλά έπρεπε επίσης και να διανεμηθούν, επομένως δεν μπορούσαν να κλειδωθούν στο θησαυροφυλάκιο μιας τράπεζας.

Το 1976 δύο ερευνητές στο Stanford University, οι Diffie και Hellman, πρότειναν έναν ριζικά καινούργιο τύπο κρυπτοσυστήματος, όπου τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης ήταν διαφορετικά και το κλειδί αποκρυπτογράφησης δεν μπορούσε να προκύψει από το κλειδί κρυπτογράφησης (υπάρχουν τώρα αποδείξεις ότι επιστήμονες της Βρετανικής Υπηρεσίας Πληροφοριών το είχαν ανακαλύψει μερικά χρόνια πριν, αλλά κρατήθηκε στρατιωτικό μυστικό και δεν αξιοποιήθηκε περαιτέρω). Στην πρότασή τους, ο (με κλειδί) αλγόριθμος κρυπτογράφησης **E** και ο (με κλειδί) αλγόριθμος αποκρυπτογράφησης **D**, έπρεπε να ικανοποιούν τις ακόλουθες τρεις απαιτήσεις. Αυτές οι απαιτήσεις μπορούν να διατυπωθούν με απλό τρόπο ως εξής:

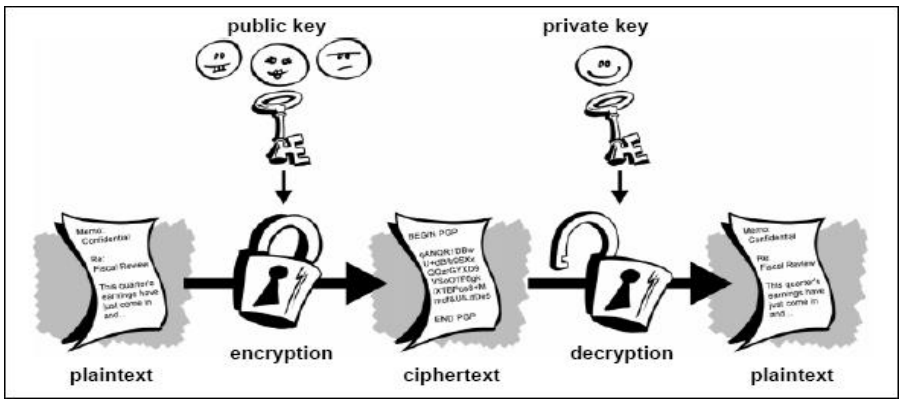
1) D(E(P)) = P.

2) Είναι υπερβολικά δύσκολη η παραγωγή του D από το E.

3) Ο αλγόριθμος E δεν μπορεί να σπάσει με επίθεση επιλεγμένου κειμένου.

Η πρώτη απαίτηση λέει ότι εάν εφαρμόσουμε τον αλγόριθμο D σε κρυπτογράφημα, το E(P), θα ξαναπάρουμε το πρωτότυπο κείμενο

(*plaintext*), P. Η δεύτερη απαίτηση μιλά από μόνη της. Η τρίτη απαίτηση χρειάζεται επειδή, όπως θα δούμε αμέσως, οι επιτιθέμενοι μπορεί να πειραματίζονται με τον αλγόριθμο όσο τραβά η ψυχή τους. Κάτω απ' αυτές τις συνθήκες δεν υπάρχει λόγος να μην δημοσιοποιηθεί το κλειδί κρυπτογράφησης. Γι' αυτόν το λόγο ονομάστηκε κρυπτογραφία δημόσιου κλειδιού (άλλη ονομασία που έχει είναι ασύμμετρη κρυπτογραφία). Το παρακάτω σχήμα δείχνει πώς λειτουργεί αυτή η μέθοδος.



Σχήμα 5.5 Ασύμμετρη Κρυπτογραφία

Το κλειδί κρυπτογράφησης δημοσιεύεται στο ευρύ κοινό, ενώ αυτό της αποκρυπτογράφησης κρατείται μυστικό (ιδιωτικό κλειδί). Οποιοσδήποτε διαθέτει το δημόσιο κλειδί μπορεί να κρυπτογραφήσει το κείμενο αλλά όχι και να το αποκρυπτογραφήσει.

Το βασικό προτέρημα αυτού του είδους της κρυπτογραφίας (και ο λόγος που αρχικά «πολεμήθηκε» η διανομή του) είναι ότι επιτρέπει στο ευρύ κοινό να ανταλλάσει μηνύματα με ασφαλή τρόπο. Μέχρι τώρα αυτό ήταν προνόμιο μόνο των κυβερνήσεων και των μεγάλων οργανισμών που είχαν την οικονομική ευχέρεια να αναπτύξουν ασφαλή δίκτυα διανομής των μυστικών κλειδιών τους.

Μερικά παραδείγματα αλγορίθμων ζεύγους κλειδιών είναι ο Diffie-Hellman, ο RSA, ο Elgamal και ο DSS, οι οποίοι περιγράφονται συνοπτικά παρακάτω.

- **Diffie-Hellman key exchange,** είναι ένα σύστημα για ανταλλαγή κρυπτο-γραφικών κλειδιών ανάμεσα σε ενεργά μέρη. Ο Diffie-Hellman δεν είναι ακριβώς μια μέθοδος κρυπτογράφησης και αποκρυπτογράφησης, αλλά μια μέθοδος ανάπτυξης και ανταλλαγής ενός μοιρασμένου μυστικού κλειδιού σε ένα δημόσιο κανάλι επικοινωνίας. Στην πραγματικότητα, τα δύο μέρη συμφωνούν σε μερικές κοινές αριθμητικές τιμές, και τότε το κάθε μέρος δημιουργεί ένα κλειδί. Οι μαθηματικοί μετασχηματισμοί των κλειδιών ανταλλάσσονται. Κάθε μέρος μπορεί τότε να υπολογίσει ένα τρίτο κλειδί συνόδου (*session key*) το οποίο δεν μπορεί εύκολα να παραχθεί από έναν επιτιθέμενο που γνωρίζει και τον δύο τις αριθμητικές τιμές.
- **RSA.** Ο RSA είναι ένα πολύ γνωστό κρυπτογραφικό σύστημα αναπτυγμένο από καθηγητές του MIT, τους Ronald Rivest, Adi Shamir και Leonard Adleman. Ο RSA μπορεί να χρησιμοποιηθεί και για να κρυπτογραφεί πληροφορίες αλλά και σαν βάση του συστήματος ψηφιακών υπογραφών. Οι ψηφιακές υπογραφές μπορούν να χρησιμοποιηθούν για να αποδείξουν την πατρότητα και γνησιότητα της ψηφιακής πληροφορίας. Το κλειδί μπορεί να είναι οποιουδήποτε μήκους, ανάλογα με την εφαρμογή που χρησιμοποιείται.
- **Elgamal.** Ο δημιουργός αυτού του αλγόριθμου είναι ο Taher Elgamal, είναι ένα κρυπτογραφικό σύστημα δημόσιου κλειδιού που είναι βασισμένο στο πρωτόκολλο ανταλλαγής κλειδιών των Diffie-Hellman. Ο ELGamal χρησιμο-ποιείται για κρυπτογράφηση και για ψηφιακές υπογραφές με τον ίδιο τρόπο όπως ο RSA.
- **DSS** (Digital Signature Standard). Αναπτύχθηκε από την National Security Agency (NSA) και εφαρμόστηκε σαν ομοσπονδιακό πρότυπο επεξεργασίας πληροφοριών FIPS (Federal Information Processing

Standard) από την NIST (National Institute for Standards and Technology). Ο DSS είναι βασισμένος στον αλγόριθμο ψηφιακών υπογραφών (DSA). Αν και ο DSA επιτρέπει κλειδιά οποιουδήποτε μήκους, στον DSS επιτρέπονται μόνο κλειδιά ανάμεσα σε 512 και 1024 bits. Όπως αναφέρθηκε, ο DSS μπορεί να χρησιμοποιηθεί μόνο για ψηφιακές υπογραφές, αν και είναι πιθανό να χρησιμοποιήσει DSA εφαρμογές για την κρυπτογράφηση επίσης.

5.8 Συμμετρικοί έναντι ασύμμετρων αλγορίθμων

Οι συμμετρικοί αλγόριθμοι μπορούν να υλοποιηθούν ιδιαίτερα αποτελεσματικά, υπάρχει όμως το πρόβλημα ότι πρέπει να υπάρχει ένα *διαμοιραζόμενο μυστικό*. Δύο μέλη που λαμβάνουν μέρος σε επικοινωνία με συμμετρική κρυπτογράφηση πρέπει να έχουν το ίδιο μυστικό κλειδί. Για το λόγο αυτό, η συμμετρική κρυπτογραφία είναι ακατάλληλη για να αποδεικνύεται η ταυτότητα του κάθε μέρους σε τρίτους, καθώς τουλάχιστον δύο μέλη μοιράζονται το ίδιο κλειδί, και έτσι το κλειδί δεν είναι μονοσήμαντος σύνδεσμος προς συγκεκριμένο χρήστη. Ένα ακόμη πρόβλημα είναι η αναγκαιότητα μετάδοσης του κλειδιού διαμέσου του δικτύου αν τα μέλη της επικοινωνίας βρίσκονται σε διαφορετικές τοποθεσίες. Η συμμετρική κρυπτογραφία μπορεί να χρησιμοποιηθεί για επίτευξη της αυθεντικότητας, σε συνδυασμό με έναν κεντρικό εξυπηρέτη αυθεντικοποίησης, ο οποίος φυλάσσει τα μυστικά για όλα τα μέλη.

Το πρόβλημα του κοινού μυστικού δεν υφίσταται στην ασύμμετρη κρυπτογραφία. Κάθε μέλος κατέχει ένα μοναδικό *ζεύγος κλειδιών*. Ένα από αυτά δημοσιοποιείται, ενώ το άλλο παραμένει στην αποκλειστική κατοχή και χρήση της οντότητας, πιθανώς αποθηκευμένο σε κάποια έξυπνη κάρτα. Με το ιδιωτικό κλειδί παράγονται ψηφιακές υπογραφές, οι οποίες είναι δυνατόν να επαληθευτούν με το δημόσιο κλειδί, επιτυγχάνοντας έτσι την αυθεντικότητα. Χρησιμοποιώντας αντιστρέψιμους αλγόριθμους είναι δυνατόν να επιτευχθεί και η εμπιστευτικότητα, καθώς ακόμη και αν

υποκλαπεί η επικοινωνία, μόνο ο κάτοχος του μυστικού κλειδιού μπορεί να αποκρυπτογραφήσει το περιεχόμενό της.

Η εφαρμογή ωστόσο της ασύμμετρης κρυπτογραφίας οδηγεί σε ένα σύνολο πρακτικών ζητημάτων. Ένα από αυτά είναι ότι βασίζονται σε περίπλοκες μαθηματικές θεωρίες και περιλαμβάνουν τη χρήση μεγάλων αριθμών, με αποτέλεσμα να είναι πιο αργοί από τους συμμετρικούς και συνήθως ακατάλληλοι για κρυπτογράφηση δεδομένων μεγάλου όγκου. Μια γενικώς παραδεκτή λύση είναι να κρυπτογραφούνται τα δεδομένα με συμμετρικούς αλγόριθμους και να ανταλλάσσονται τα σχετικά κλειδιά με ασύμμετρους.

5.9 Πιστοποίηση Ταυτότητας και Υπογραφές

5.9.1 Ψηφιακή υπογραφή (*Digital Signature*)

Η ψηφιακή υπογραφή είναι μία ακολουθία χαρακτήρων άμεσα συσχετισμένη με το περιεχόμενο του μηνύματος και την ταυτότητα αυτού που το υπογράφει. Αποστέλλεται μαζί με το μήνυμα και ο παραλήπτης μπορεί, ελέγχοντας την υπογραφή, να βεβαιωθεί ότι το περιεχόμενο του μηνύματος δεν έχει παραποιηθεί και ότι ο αποστολέας του είναι όντως αυτός που ισχυρίζεται ότι είναι.

5.9.2 Δημιουργία ψηφιακής υπογραφής

Η ψηφιακή υπογραφή είναι ένα εργαλείο που παρέχει αυθεντικοποίηση (authentication). Η έννοια αυθεντικοποίηση περιλαμβάνει όλες εκείνες τις διαδικασίες που είναι απαραίτητες για την επαλήθευση συγκεκριμένων ευαίσθητων πληροφοριών, όπως την ταυτότητα του αποστολέα ενός μηνύματος, την αυθεντικότητα ενός εγγράφου, ακεραιότητα δεδομένων και την ταυτότητα ενός υπολογιστή.

Η χρήση της ηλεκτρονικής υπογραφής περιλαμβάνει δύο διαδικασίες: α) τη δημιουργία της υπογραφής και β) την επαλήθευσή της. Κατά τη δημιουργία μιας ψηφιακής υπογραφής δεν κρυπτογραφούνται τα προς υπογραφήν

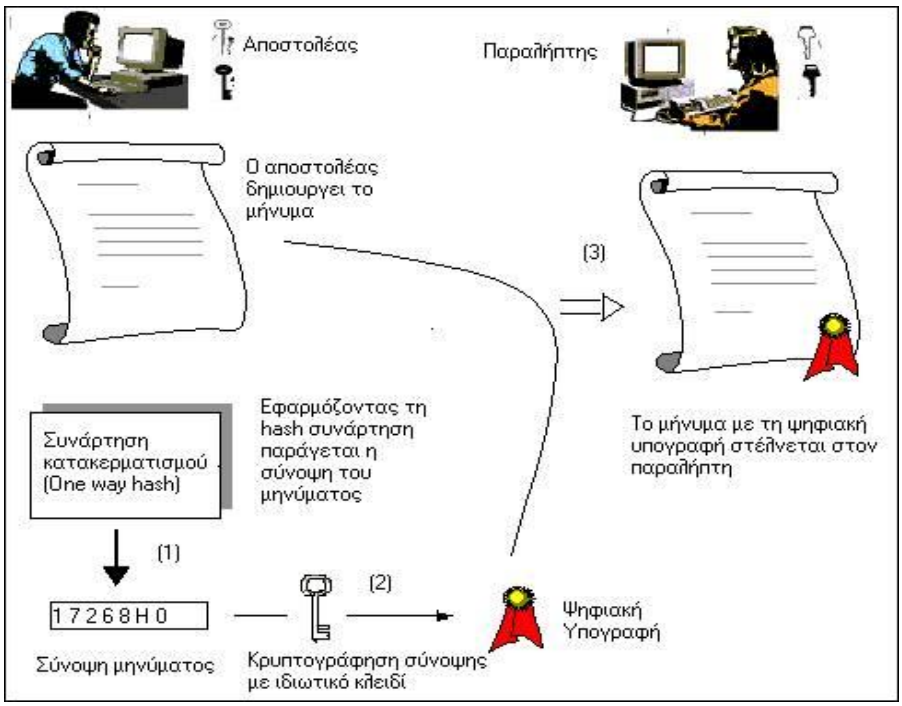
δεδομένα, αλλά μία μικρή μαθηματική «σύνοψή» τους (message digest), η οποία παράγεται μέσω μιας hash function και του ιδιωτικού κλειδιού του αποστολέα. Ο όρος hash function υποδηλώνει ένα μετασχηματισμό που παίρνει σαν είσοδο ένα μήνυμα m οποιουδήποτε μήκους και επιστρέφει στην έξοδο μία ακολουθία χαρακτήρων h περιορισμένου μήκους που καλείται hash value, δηλαδή είναι $h = H(m)$ (δες παράγραφο 5.6.3). Για κάθε μήνυμα λοιπόν, και ανεξαρτήτως του μεγέθους του, δημιουργείται μια σύνοψή του, που είναι μια σειρά από bits με συγκεκριμένο πλήθος.

Η σύνοψη του μηνύματος (message digest) αποτελεί την ψηφιακή αναπαράσταση του μηνύματος και είναι μοναδική για το μήνυμα που αντιπροσωπεύει. Αν αλλάξουμε έστω και μια τελεία στο μήνυμα, θα αλλάξει και η σύνοψή του, ενώ είναι πρακτικά αδύνατο δύο διαφορετικά μηνύματα να δώσουν την ίδια σύνοψη. Η μεγάλη αυτή ευαισθησία στα δεδομένα εισόδου αποτελεί μια από τις πολυτιμότερες ιδιότητες (δυνατότητες) των συναρτήσεων hash. Είναι επίσης πρακτικά αδύνατο να ανακτήσουμε το αρχικό μήνυμα ακόμη και αν γνωρίζουμε τη σύνοψή του.
Αυτή η σύνοψη των δεδομένων, κρυπτογραφείται με το ιδιωτικό κλειδί του υπογράφοντα και επισυνάπτεται (πιθανώς μαζί και με άλλες χρήσιμες σχετικές πληροφορίες, π.χ. χρησιμοποιούμενοι αλγόριθμοι, εφαρμοζόμενη πολιτική υπογραφής κ.ά.) στα αρχικά δεδομένα, αποτελώντας την προηγμένη ψηφιακή υπογραφή. Παρακάτω περιγράφονται οι ενέργειες του αποστολέα και του παραλήπτη, ώστε να γίνει κατανοητός ο μηχανισμός της δημιουργίας και επαλήθευσης της υπογραφής (*Σχήμα 5.6*):

1. Ο *αποστολέας* δημιουργεί τη σύνοψη του μηνύματος (message digest) που θέλει να στείλει χρησιμοποιώντας κάποιον αλγόριθμο κατακερματισμού (one way hash). Ανεξάρτητα από το μέγεθος του μηνύματος, αυτό που θα παραχθεί θα είναι μία συγκεκριμένου μήκους σειρά ψηφίων.
2. Στη συνέχεια κρυπτογραφεί τη σύνοψη με τη χρήση του ιδιωτικού του κλειδιού. Αυτό που παράγεται είναι η ψηφιακή υπογραφή. Η

υπογραφή είναι ουσιαστικά μία σειρά ψηφίων συγκεκριμένου πλήθους.

3. Τέλος η κρυπτογραφημένη σύνοψη (ψηφιακή υπογραφή) προσαρτάται στο κείμενο και το μήνυμα με τη ψηφιακή υπογραφή μεταδίδονται μέσω του δικτύου (σημειώνεται ότι ο αποστολέας αν επιθυμεί μπορεί να κρυπτογραφήσει το μήνυμά του με το δημόσιο κλειδί του παραλήπτη).



Σχήμα 5.6 Διαδικασία δημιουργίας ψηφιακής υπογραφής

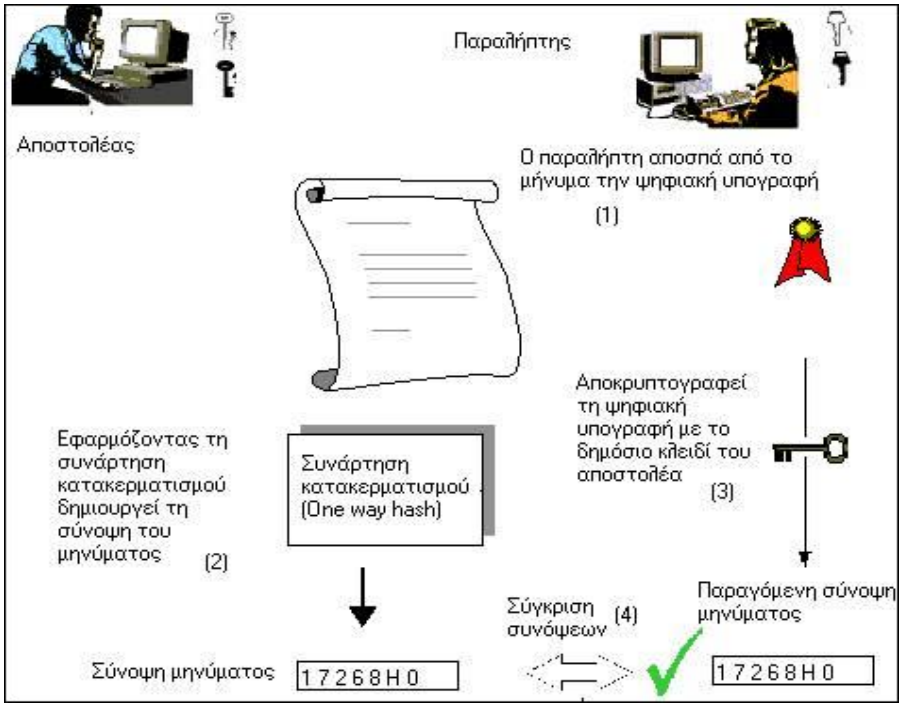
Για να έχει αποτέλεσμα η παραπάνω μέθοδος, πρέπει να τηρούνται δύο προϋποθέσεις: (α) η hash function πρέπει να είναι όσο το δυνατόν περισσότερο μη αντιστρέψιμη και (β) τα ζεύγη δημόσιου/ιδιωτικού κλειδιού να είναι συσχετισμένα με τους νόμιμους κατόχους τους. Για την εξασφάλιση της δεύτερης προϋπόθεσης υπάρχουν ψηφιακά έγγραφα που καλούνται πιστοποιητικά (*certificates*) και συνδέουν ένα άτομο με ένα συγκεκριμένο δημόσιο κλειδί.

5.9.3 Επαλήθευση ψηφιακής υπογραφής

Κατά τη διαδικασία της επαλήθευσης (*verification*) μιας ψηφιακής υπογραφής, εφαρμόζεται στο κανονικό κείμενο ο ίδιος αλγόριθμος κατακερματισμού που χρησιμοποιήθηκε κατά την υπογραφή του και δημιουργείται κατά αυτόν τον τρόπο μια νέα σύνοψη. Κατόπιν, αποκρυπτογραφείται με το δημόσιο κλειδί του αποστολέα η κρυπτογραφημένη σύνοψη του μηνύματος. Έτσι, η νέα σύνοψη που παράγεται, συγκρίνεται με την αντίστοιχη σύνοψη που προέρχεται από την αποκρυπτογράφηση της ψηφιακής υπογραφής. Εάν ταυτίζονται οι δύο συνόψεις, τότε η υπογραφή επαληθεύεται και επιβεβαιώνεται αφενός μεν ότι τα δεδομένα υπογράφηκαν από τον κάτοχο του σχετικού ιδιωτικού κλειδιού, αφετέρου δε ότι τα αρχικά δεδομένα δεν έχουν αλλοιωθεί.

Συνοπτικά τα βήματα που περιλαμβάνονται στη διαδικασία επαλήθευσης της ψηφιακής υπογραφής είναι (*Σχήμα 5.7*):

1. Ο *παραλήπτης* αποσπά από το μήνυμα την ψηφιακή υπογραφή (κρυπτογραφημένη, με το ιδιωτικό κλειδί του αποστολέα, σύνοψη).
2. Εφαρμόζοντας στο μήνυμα που έλαβε τον ίδιο αλγόριθμο κατακερματισμού, ο παραλήπτης δημιουργεί τη σύνοψη του μηνύματος.
3. Στη συνέχεια, αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα, την κρυπτογραφημένη σύνοψη του μηνύματος (ψηφιακή υπογραφή).
4. Τέλος συγκρίνονται οι δύο συνόψεις και αν βρεθούν ίδιες, αυτό σημαίνει ότι το μήνυμα που έλαβε ο παραλήπτης είναι ακέραιο. Αν το μήνυμα έχει μεταβληθεί, η σύνοψη που θα παράγει ο παραλήπτης θα είναι διαφορετική από την σύνοψη που έχει κρυπτογραφηθεί.



Σχήμα 5.7 Διαδικασία επαλήθευσης ψηφιακής υπογραφής

5.9.4 Πιστοποίηση ψηφιακής υπογραφής (Digital Certificate)

Με τη λήψη ενός μηνύματος με ψηφιακή υπογραφή, ο παραλήπτης επαληθεύοντάς την βεβαιώνεται ότι το μήνυμα είναι ακέραιο. Ο παραλήπτης, όμως, πρέπει να είναι βέβαιος ότι ο αποστολέας του μηνύματος είναι όντως αυτός που ισχυρίζεται ότι είναι. Απαιτείται δηλαδή να διασφαλιστεί ότι ο δικαιούχος του ιδιωτικού κλειδιού, και μόνον αυτός, δημιούργησε την υπογραφή και ότι το δημόσιο κλειδί του αποστολέα που χρησιμοποιεί ο παραλήπτης για την επαλήθευση της υπογραφής είναι όντως του αποστολέα. Απαιτείται δηλαδή, η ύπαρξη ενός μηχανισμού τέτοιου, ώστε ο παραλήπτης να μπορεί να είναι σίγουρος για την ταυτότητα του προσώπου που κατέχει το δημόσιο κλειδί.

Η Αρχή Πιστοποίησης (*Certification Authority (CA)*) είναι ένας «οργανισμός», ο οποίος παρέχει μεταξύ άλλων την υπηρεσία εκείνη με την

οποία πιστοποιείται η σχέση ενός προσώπου με το δημόσιο κλειδί του. Ο τρόπος με τον οποίο γίνεται αυτό, είναι με την έκδοση ενός πιστοποιητικού (ηλεκτρονικό αρχείο), στο οποίο η Αρχή Πιστοποίησης πιστοποιεί την ταυτότητα του προσώπου και το δημόσιο κλειδί του. Η υποδομή με την οποία μία Αρχή Πιστοποίησης εκδίδει, υπογράφει, δημοσιεύει και υποστηρίζει τυποποιημένες ηλεκτρονικές βεβαιώσεις (πιστοποιητικά) για τα κρυπτογραφικά κλειδιά των συνδρομητών του ονομάζεται Υποδομή Δημοσίου Κλειδιού (*Public Key Infrastructure -- PKI*) την οποία αναλύουμε περαιτέρω στην παράγραφο 5.11.

Λόγω της διαρκούς τεχνολογικής εξέλιξης, θεωρείται δεδομένη η εξασθένηση της ασφάλειας των χρησιμοποιούμενων κρυπτογραφικών κλειδιών στο πέρασμα του χρόνου. Έτσι, τα πιστοποιητικά δημοσίου κλειδιού, εκδίδονται με περιορισμένη διάρκεια ισχύος (συνήθως 1 έως 3 έτη). Εκτός όμως από την προγραμματισμένη λήξη, η ισχύς ενός πιστοποιητικού μπορεί οποτεδήποτε να ανακληθεί οριστικά (revocation) ή να ανασταλεί προσωρινά (suspension), ύστερα από αίτημα του ίδιου του τελικού χρήστη (π.χ. επειδή έχασε τον φορέα των κρυπτογραφικών κλειδιών του) ή/και από σχετική απόφαση του Εκδότη τους (π.χ. λόγω λάθους στην αναγραφή στοιχείων). Η ανάκληση και η αναστολή ενός πιστοποιητικού πραγματοποιείται με την εγγραφή του σειριακού αριθμού του πιστοποιητικού (*certificate's serial number*) σε μια «Λίστα Ανακληθέντων Πιστοποιητικών» (*Certificate Revocation List -- CRL*) η οποία υπογράφεται και δημοσιεύεται σε τακτά χρονικά διαστήματα από τον ίδιο τον Εκδότη των πιστοποιητικών.

Τις εταιρείες που παρέχουν υπηρεσίες πιστοποίησης αλλά και βεβαιώσεις για την ασφάλεια της ψηφιακής υπογραφής ελέγχει στην Ελλάδα, η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ), η οποία διαπιστώνει εάν οι συγκεκριμένες εταιρείες είναι σε θέση να παρέχουν υπηρεσίες πιστοποίησης.

5.10 Τύποι κλειδιών

Τα κλειδιά ταξινομούνται ανάλογα με τον τύπο του κρυπταλγόριθμου και ανάλογα με τη χρήση για την οποία προορίζονται.

Ανάλογα με τον τύπο του κρυπταλγόριθμου, τα κλειδιά χωρίζονται σε τρεις κατηγορίες:

- **μυστικό κλειδί**, το οποίο ορίζεται σε συμμετρικό κρυπτοσύστημα. Το μυστικό κλειδί θα πρέπει να βρίσκεται στην κατοχή όλων των μελών που επικοινωνούν χρησιμοποιώντας συμμετρική κρυπτογραφία.
- **δημόσιο κλειδί**, το οποίο ορίζεται σε ασύμμετρο κρυπτοσύστημα. Το δημόσιο κλειδί είναι το κλειδί εκείνο το οποίο αναφέρεται σε κάποιο μέλος με το οποίο είναι επιθυμητή η επικοινωνία. Το δημόσιο κλειδί είναι γνωστό σε όλους.
- **ιδιωτικό κλειδί**, το οποίο ορίζεται σε ασύμμετρο κρυπτοσύστημα. Το ιδιωτικό κλειδί συνδέεται κρυπτογραφικά με το δημόσιο κλειδί και είναι γνωστό σε ένα μόνο μέλος.

Ανάλογα με τη χρήση για την οποία προορίζονται τα παραπάνω κλειδιά, διακρίνουμε τους ακόλουθους τύπους:

- **κλειδί συνόδου** (*session key*), το οποίο χρησιμοποιείται για την κρυπτογράφηση για μόνο μία περίοδο επικοινωνίας. Μετά το τέλος της επικοινωνίας, το κλειδί καταστρέφεται. Σε επόμενη περίοδο επικοινωνίας, δημιουργείται νέο κλειδί συνόδου.
- **κλειδί τερματικού** (*terminal key*). Στην περίπτωση που το κλειδί συνόδου δεν καταστρέφεται, αλλά χρησιμοποιείται για περισσότερες από μία επικοινωνίες ενός μέλους, τότε το κλειδί αυτό ονομάζεται κλειδί τερματικού.
- **κύριο κλειδί** (*master key*). Συνήθως ένα μέλος στην πράξη κατέχει πολλά κλειδιά συνόδου και κλειδιά τερματικού. Προκειμένου να απλουστευθεί η διαχείριση των κλειδιών, χρησιμοποιείται το κύριο

κλειδί. Έτσι κατά την αποθήκευση των κλειδιών, αυτά κρυπτογραφούνται με το κύριο κλειδί, οπότε ο έλεγχος της ασφαλούς αποθήκευσης εξαρτάται από μία και μόνον ποσότητα, το κύριο κλειδί. Επίσης, το κύριο κλειδί μπορεί να χρησιμοποιηθεί για τη δημιουργία κλειδιού τερματικού, ή κλειδιού συνόδου.

Οι παραπάνω τύποι κλειδιών έχουν διαφορετικές κρυπτοπεριόδους, όπου κρυπτοπερίοδος καλείται ο χρόνος ο οποίος περιλαμβάνει τη δημιουργία, διανομή και χρήση ενός κλειδιού. Το κλειδί συνόδου ονομάζεται και βραχυπρόθεσμο κλειδί (*short term key*) και έχει τη μικρότερη κρυπτοπερίοδο από τους τρεις τύπους κλειδιών. Αντίθετα, το τερματικό κλειδί και το κύριο κλειδί είναι μακροπρόθεσμα κλειδιά (*long term keys*), με μεγαλύτερες κρυπτοπεριόδους. Μεταξύ των δύο αυτών κλειδιών, το κύριο κλειδί έχει μεγαλύτερη κρυπτοπερίοδο, αφού χρειάζεται για την αποθήκευση των υπολοίπων κλειδιών.

Η ύπαρξη των διαφορετικών τύπων κλειδιών με βάση τον προορισμό χρήσης τους, οφείλεται σε πρακτικούς λόγους. Είναι πλέον σαφές ότι η κρυπτογραφία δε λύνει τα προβλήματα, αλλά τα μετασχηματίζει σε μορφές όπου η διαχείριση του προβλήματος είναι αποτελεσματικότερη και ευκολότερη. Είδαμε ότι προστατεύοντας μια συγκριτικά μικρή ποσότητα πληροφορίας που ονομάζουμε «κλειδί», μπορούμε με τη χρήση της κρυπτογραφίας να προστατεύσουμε μια κατά πολύ μεγαλύτερη σε μέγεθος πληροφορία, το «απλό κείμενο». Αντίστοιχα, με τη διαχείριση των κλειδιών, χρησιμοποιούμε κλειδιά για να προστατεύσουμε άλλα κλειδιά. Η ανάγκη αυτή δημιουργήθηκε λόγω της ύπαρξης πολλών κλειδιών σε ένα σύστημα επικοινωνίας.

5.11 Υποδομές δημόσιου κλειδιού

Οι υποδομές δημόσιου κλειδιού (public key infrastructures, PKIs), όπως αναφέραμε και πιο πάνω, είναι μοντέλα τα οποία αναπτύχθηκαν με κύριο σκοπό την πιστοποίηση των οντοτήτων που συμμετέχουν σε ένα σύστημα

επικοινωνίας. Έτσι, η ασφάλεια και η αξιοπιστία της διαδικασίας αυθεντικοποίησης των μελών που γίνεται με τη χρήση ενός PKI, συνδέεται με την κρυπτογραφική ισχύ των κρυπταλγόριθμων που υποστηρίζει το PKI. Ωστόσο, η συνολική ασφάλεια της διαδικασίας πιστοποίησης δεν εξαρτάται μόνον από την ισχύ του κρυπταλγόριθμου. Όπως θα δούμε στη συνέχεια, ένα PKI αποτελείται από διάφορες οντότητες, όπου η κάθε οντότητα έχει συγκεκριμένους ρόλους. Έτσι, η συνολική ασφάλεια εξαρτάται από την εκτέλεση των ρόλων από τις οντότητες, θα διαπιστώσουμε ότι η κρυπτογραφία μετασχηματίζει προβλήματα ασφάλειας σε μορφές που επιτρέπουν αποτελεσματικότερη διαχείριση, χωρίς όμως να λύνει τα προβλήματα αυτά.

Η διαδικασία αυθεντικοποίησης ενός μέλους ή γενικότερα μιας οντότητας χαρακτηρίζεται ισχυρή, αν η πιθανότητα απάτης είναι ικανοποιητικά μικρή. Η απάτη αφορά την προσπάθεια του αντιπάλου να προσποιηθεί άλλη ταυτότητα.

Η αυθεντικοποίηση ενός μέλους στην ασύμμετρη κρυπτογραφία γίνεται με τη χρήση του δημόσιου κλειδιού του μέλους, αυτό έχει ως αποτέλεσμα η όλη διαδικασία αυθεντικοποίησης να εξαρτάται από την αυθεντικότητα του δημόσιου κλειδιού. Αν κατά την αυθεντικοποίηση ενός μέλους δεν υπάρχει τρόπος να ελεγχθεί η αυθεντικότητα του δημόσιου κλειδιού του μέλους αυτού, τότε ο αντίπαλος θα μπορεί να αντικαταστήσει το δικό του δημόσιο κλειδί χωρίς αυτό να γίνει αντιληπτό.

Χωρίς τη συμμετοχή μιας έμπιστης τρίτης οντότητας, η λύση στο πρόβλημα της αυθεντικότητας των κλειδιών θα ήταν το κάθε μέλος να έχει στην κατοχή του τα δημόσια κλειδιά όλων των μελών, τα οποία τα έχει παραλάβει μέσω ενός καναλιού που προσφέρει υψηλή ακεραιότητα. Ας σημειωθεί ότι το κανάλι δεν απαιτείται να προσφέρει εμπιστευτικότητα, αφού τα κλειδιά είναι δημόσια. Η ακεραιότητα όμως απαιτείται να είναι υψηλή, ώστε ο αντίπαλος να μην έχει τη δυνατότητα να αντικαταστήσει τα δημόσια κλειδιά με τα δικά του. Εναλλακτικά, το κάθε μέλος θα μπορούσε

να παραλάβει μόνον εκείνα τα δημόσια κλειδιά τα οποία θα χρειασθεί προκειμένου να επικοινωνήσει με τα αντίστοιχα μέλη. Ένα τέτοιο μοντέλο διανομής δημόσιων κλειδιών δεν είναι πρακτικό, αφού δεν μπορεί να κλιμακωθεί με ευκολία και απαιτεί διαρκώς ασφαλές κανάλι με υψηλή ακεραιότητα.

Η συμμετοχή μιας έμπιστης τρίτης οντότητας μπορεί να απλοποιήσει το παραπάνω πρόβλημα αποτελεσματικά. Αντί να απαιτείται η ασφαλής μεταφορά όλων των δημόσιων κλειδιών, αρκεί να διανεμηθεί με υψηλή ακεραιότητα το δημόσιο κλειδί της έμπιστης τρίτης οντότητας και να χρησιμοποιηθεί αυτό για να πιστοποιήσει τα δημόσια κλειδιά των υπολοίπων. Αυτό σε γενικές γραμμές είναι μια υποδομή δημόσιου κλειδιού, ή ένα PKI για συντομία, που θα εξετάσουμε στη συνέχεια.

5.11.1 Συστατικά ενός PKI

Ένα PKI αποτελείται από τα εξής συστατικά:

- **Αρχή Πιστοποίησης** (*Certification Authority*). Η Αρχή Πιστοποίησης είναι το κεντρικό συστατικό ενός PKI. Αποτελεί την έμπιστη τρίτη οντότητα η οποία είναι υπεύθυνη για την πιστοποίηση των δημόσιων κλειδιών των μελών. Η ακεραιότητα όλης της υποδομής συγκεντρώνεται στην Αρχή Πιστοποίησης.
- **Αρχή Εγγραφής** (*Registration Authority*). Η Αρχή Εγγραφής είναι προαιρετική. Εμφανίσθηκε κυρίως για εμπορικούς λόγους και στην περίπτωση απουσίας αυτής, τα καθήκοντα της αναλαμβάνει η Αρχή Πιστοποίησης. Η Αρχή Εγγραφής είναι υπεύθυνη για την αρχική εξακρίβωση των στοιχείων του μέλους, προτού πιστοποιηθεί το δημόσιο του κλειδί.
- **Εντολέας** (*Principal*). Είναι η οντότητα η οποία πιστοποιείται από την Αρχή Πιστοποίησης. Οι οντότητες με τις οποίες έχουμε ασχοληθεί είναι τα επικοινωνούντα μέλη, τα οποία είναι φυσικά

πρόσωπα, αλλά μπορούν να είναι και υπολογιστές που βρίσκονται σε δίκτυο, μηχανές ATM των τραπεζών, κτλ.

- **Πιστοποιητικό δημόσιου κλειδιού** (*Public Key Certificate*). Το πιστοποιητικό δημόσιου κλειδιού είναι μια δομή δεδομένων η οποία αποτελείται από ένα σύνολο στοιχείων που περιλαμβάνει δύο μέρη. Το πρώτο μέρος αποτελείται από την περιγραφή του εντολέα και το δημόσιο κλειδί του. Το δεύτερο μέρος του πιστοποιητικού αποτελείται από την ψηφιακή υπογραφή της Αρχής Πιστοποίησης επάνω στα στοιχεία του πρώτου μέρους.
- **Αποθήκη πιστοποιητικών** (*Certificate Repository*). Αποτελεί τον χώρο αποθήκευσης των πιστοποιητικών ενός PKI. Στην πράξη αυτό υλοποιείται από υπηρεσία καταλόγου (*directory service*) στο οποίο μπορούν να απευθυνθούν τα μέλη προκειμένου να παραλάβουν το δημόσιο κλειδί του μέλους με το οποίο επιθυμούν να επικοινωνήσουν.
- **Υπηρεσία ανάκλησης πιστοποιητικού** (*certificate revocation service*). Η υπηρεσία ανάκλησης πιστοποιητικού συμμετέχει στη διαδικασία εξακρίβωσης της εγκυρότητας του πιστοποιητικού και παρέχει πληροφορίες σχετικά με την ανάκληση αυτού.
- **Δήλωση Χρήσης Πιστοποιητικού** (*Certificate Practice Statement*). Είναι ένα είδος συμφωνητικού το οποίο περιγράφει τους ρόλους, τις διαδικασίες, τα δικαιώματα και τις υποχρεώσεις καθενός από τα μέλη. Για παράδειγμα, περιγράφει τα δικαιολογητικά τα οποία θα πρέπει να κατατεθούν από τον εντολέα προκειμένου να του εκδοθεί το πιστοποιητικό.

Από την παραπάνω περιγραφή των συστατικών μπορεί να γίνει αντιληπτή η καίρια θέση της Αρχής Πιστοποίησης και η εξάρτηση της ασφάλειας του PKI από αυτήν. Η δύναμη που έχει η Αρχή Πιστοποίησης στο να δημιουργεί πιστοποιητικά για τα μέλη είναι και η συνέπεια της απαίτησης

εμπιστοσύνης, η οποία καθιστά την Αρχή Πιστοποίησης ως Έμπιστη Τρίτη Οντότητα.

5.11.2 Πιστοποιητικά

Το πιστοποιητικό δημοσίου κλειδιού (*public key certificate*) είναι από τους σημαντικότερους τύπους ψηφιακών πιστοποιητικών. Ο στόχος του πιστοποιητικού δημοσίου κλειδιού είναι η δημιουργία μιας σχέσης ταυτοποίησης μεταξύ του δημοσίου κλειδιού και του δικαιούχου του. Το πιστοποιητικό αναφέρει το δημόσιο κλειδί (το οποίο και είναι το αντικείμενο του πιστοποιητικού) και επιβεβαιώνει ότι το συγκεκριμένο πρόσωπο που αναφέρεται στο πιστοποιητικό είναι ο δικαιούχος του αντίστοιχου ιδιωτικού κλειδιού. Έτσι ο παραλήπτης που λαμβάνει ένα μήνυμα με ψηφιακή υπογραφή, μπορεί να είναι σίγουρος ότι το μήνυμα έχει σταλεί από το πρόσωπο που το υπογράφει.

Ένα ψηφιακό πιστοποιητικό αποτελείται από τρία στοιχεία, που βοηθούν τους άλλους να επαληθεύσουν εάν το κλειδί είναι αυθεντικό και αν ισχύει ακόμα. Αυτά είναι:

1. Ένα δημόσιο κλειδί.
2. Πληροφορίες του πιστοποιητικού (Συνήθως πληροφορίες σχετικά με την ταυτότητα του χρήστη, όπως όνομα, userID, κλπ. Επίσης μπορεί να περιέχονται πληροφορίες σχετικά με τα δικαιώματα του κατόχου του, όπως δικαιώματα για πρόσβαση σε αρχεία (file permissions κτλ.).
3. Μία ή περισσότερες ψηφιακές υπογραφές.

Ο σκοπός της ψηφιακής υπογραφής σε ένα πιστοποιητικό είναι για να επικυρώσει ότι τα στοιχεία που περιλαμβάνει πηγαίνουν μαζί με το συμπεριλαμβανόμενο δημόσιο κλειδί. Έτσι ένα πιστοποιητικό είναι στην ουσία ένα δημόσιο κλειδί μαζί με επισυναπτόμενα στοιχεία του ιδιοκτήτη του και μια σφραγίδα μιας έμπιστης οντότητας που επικυρώνει αυτή τη σύνδεση.

Πιστοποιητικό X.509

Υπάρχουν διάφορες μορφές που μπορούν να έχουν τα πιστοποιητικά (PGP, X.509). Εδώ θα αναπτύξουμε αυτά της μορφής X.509, μιας που είναι τα πιο συνηθισμένα.

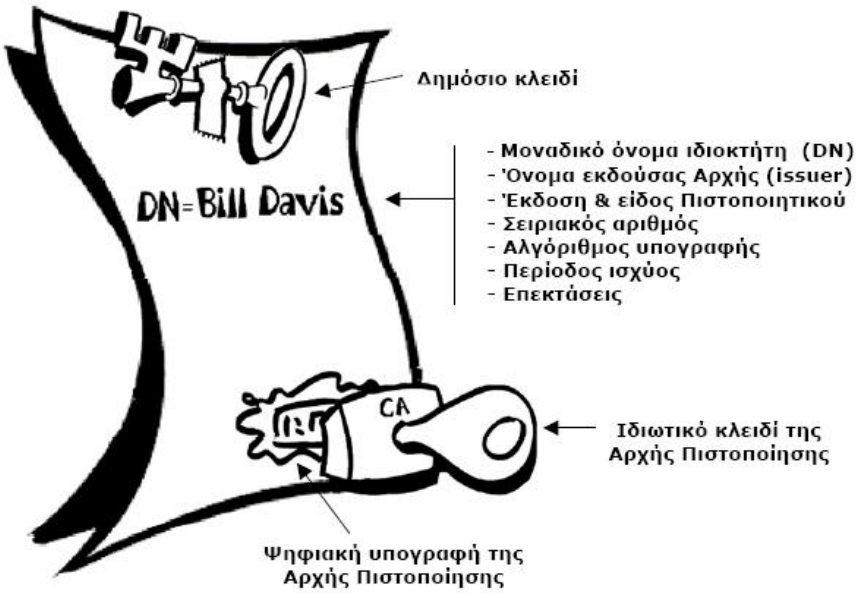
Όλα τα πιστοποιητικά της μορφής X.509 συνάδουν με το διεθνές πρότυπο ITU-T X.509, έτσι ώστε (θεωρητικά τουλάχιστον) τα πιστοποιητικά αυτού του είδους που δημιουργήθηκαν για μια εφαρμογή να μπορούν να χρησιμοποιηθούν από μια άλλη εφαρμογή συμβατή με αυτό το πρότυπο. Στην πραγματικότητα όμως, πολλές εταιρίες έχουν δημιουργήσει δικές τους εκδόσεις πιστοποιητικών X.509 οι οποίες δεν είναι όλες συμβατές μεταξύ τους.

Σε άλλα είδη Πιστοποιητικών (όπως αυτά του κρυπτοσυστήματος PGP – Pretty Good Privacy) οποιοσδήποτε μπορεί να παίξει τον ρόλο αυτού που επικυρώνει τη σύνδεση του δημοσίου κλειδιού με τα στοιχεία του κατόχου του. Στο X.509 όμως αυτό μπορεί να το κάνει μόνο μια CA ή κάποιος που έχει επικυρωθεί από μια CA.

Ένα πιστοποιητικό X.509 είναι μια συλλογή από συγκεκριμένα πεδία που περιέχουν πληροφορίες σχετικά με έναν χρήστη ή μια συσκευή, καθώς και το δημόσιο κλειδί που τους αντιστοιχεί (*Πίνακας 5.1*). Το πρότυπο X.509 ορίζει το τι θα γραφεί στο πιστοποιητικό και το πώς θα γραφεί, δηλαδή τη μορφοποίησή του.

Σε αντίθεση με άλλα είδη πιστοποιητικών το X.509 υποστηρίζει ένα και μοναδικό όνομα και πληροφορίες για τον ιδιοκτήτη του κλειδιού, και επίσης μία και μοναδική ψηφιακή υπογραφή που να το επικυρώνει.
Για να αποκτήσεις ένα πιστοποιητικό X.509 πρέπει να απευθυνθείς σε μία Αρχή Πιστοποίησης για να σου το εκδώσει. Της παρέχεις το δημόσιό σου κλειδί, αποδείξεις ότι κατέχεις το αντίστοιχο ιδιωτικό κλειδί, και μερικές συγκεκριμένες πληροφορίες για σένα. Μετά υπογράφεις ψηφιακά όλες αυτές τις πληροφορίες και στέλνεις όλο το πακέτο (δηλαδή την αίτηση

πιστοποιητικού) στην CA. Εκεί γίνεται ένας ενδελεχής έλεγχος της αυθεντικότητας των στοιχείων και αν είναι επιτυχής, παράγεται το πιστοποιητικό και αποστέλλεται στον ιδιοκτήτη του. Το πιστοποιητικό αυτό θα έχει τη μορφή που παρουσιάζεται στο επόμενο σχήμα.

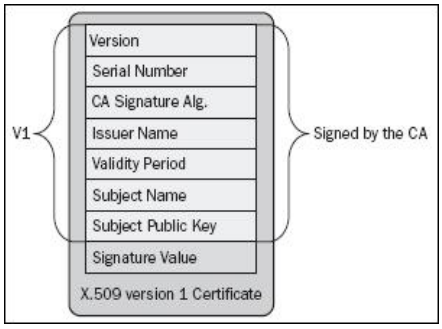


Σχήμα 5.8 Πιστοποιητικό X.509

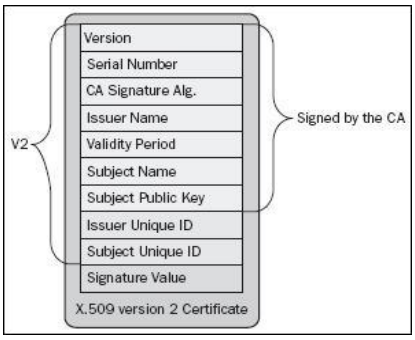
Ο παρακάτω πίνακας μας παρουσιάζει τα πεδία του προτύπου X.509 περιγράφοντας μας το καθένα απ' αυτά, ενώ οι εικόνες 5.9, 5.10 και 5.11 δείχνουν τις διαφορές στις 3 εκδόσεις του πιστοποιητικού X.509.

Όνομα πεδίου	Χρήση
version	Η έκδοση του προτύπου X.509. Ορίζονται 3 εκδόσεις του X.509. Η έκδοση 1 δεν περιέχει τα πεδία *issuer unique id, subject unique id* τα οποία προστέθηκαν στην έκδοση 2, καθώς και το πεδίο *extensions* το οποίο προστέθηκε στην έκδοση 3.
serial number	Ένας μοναδικός ακέραιος που καθορίζεται από την Αρχή Πιστοποίησης για να αναγνωρίσει το πιστοποιητικό.
signature algorithm identifier	Το πεδίο αυτό αποτελείται στην ουσία από 2 πεδία. Από τα ονόματα των κρυπτογραφικών συναρτήσεων που συμμετέχουν και από τις σχετικές παραμέτρους αυτών.
issuer name	Το όνομα της Αρχής Πιστοποίησης.
validity period	Αποτελείται από δύο ημερομηνίες, από την ημερομηνία ενεργοποίησης του πιστοποιητικού και από την ημερομηνία λήξης του πιστοποιητικού.
subject name	Το όνομα της οντότητας που πιστοποιείται.
public key	Το δημόσιο κλειδί της οντότητας που αναγνωρίζεται από το πεδίο subject name. Η οντότητα αυτή κατέχει το ιδιωτικό κλειδί.
issuer unique id	Ο αριθμός αυτός χρησιμοποιείται σε συνδυασμό με το όνομα της Αρχής Πιστοποίησης για να ενισχύσει την αναγνώριση αυτής.
subject unique id	Ο αριθμός αυτός χρησιμοποιείται σε συνδυασμό με το όνομα της οντότητας για να προσδώσει μοναδικότητα στο πιστοποιητικό, σε περίπτωση που το όνομα της οντότητας χρησιμοποιείται για άλλο πιστοποιητικό.
extensions	Εδώ μπορούν να προστεθούν επιπλέον στοιχεία για να υποστηρίξουν ειδικές απαιτήσεις της εφαρμογής.
signature value	Η ψηφιακή υπογραφή με το ιδιωτικό κλειδί της Αρχής Πιστοποίησης επάνω σε όλες τις προαναφερθείσες πληροφορίες.

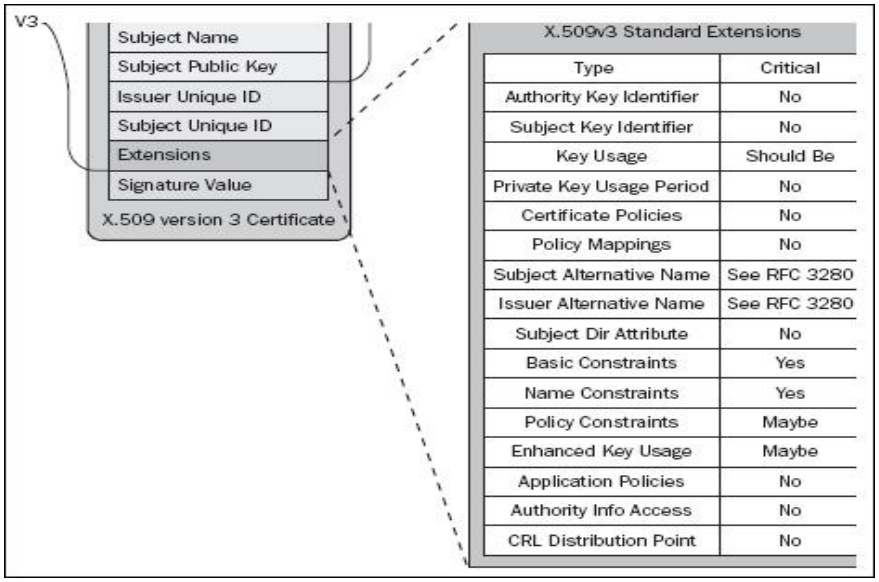
Πίνακας 5.2 Πεδία του πιστοποιητικού X.509



Εικόνα 5.9 X.509 Έκδοση 1



Εικόνα 5.10 X.509 Έκδοση 2



Εικόνα 5.11 X.509 Έκδοση 3

Διαδικασία δημιουργίας και δημοσίευσης του πιστοποιητικού του χρήστη

Ο σκοπός του πιστοποιητικού, όπως έχουμε αναφέρει αρκετές φορές, είναι η σύνδεση ενός ονόματος με ένα δημόσιο κλειδί. Έτσι, απαραίτητη προϋπόθεση είναι η δημιουργία ενός ζεύγους δημόσιου και ιδιωτικού κλειδιού. Το δημόσιο κλειδί θα κατατεθεί στην Αρχή Εγγραφής μαζί με τα στοιχεία του χρήστη. Υπάρχουν δύο εναλλακτικές όπου μπορεί να δημιουργηθεί το ζεύγος του κλειδιού:

α) **Στο περιβάλλον του χρήστη**. Στην περίπτωση αυτή το ρίσκο να αποκαλυφθεί το ιδιωτικό κλειδί είναι ελάχιστο, αφού ο μόνος γνώστης του κλειδιού είναι ο χρήστης. Ωστόσο, αν το κλειδί χρησιμοποιείται για κρυπτογράφηση μηνυμάτων και όχι για αυθεντικοποίηση, η απώλεια του κλειδιού θα καταστήσει αδύνατη την αποκρυπτογράφηση των μηνυμάτων που έχουν κρυπτογραφηθεί με το αντίστοιχο δημόσιο κλειδί.

β) **Στο περιβάλλον της Αρχής Εγγραφής ή Πιστοποίησης**. Η δημιουργία του ζεύγους κλειδιών σε τοποθεσία διαφορετική από τον νόμιμο κάτοχο του ιδιωτικού κλειδιού έχει επίπτωση στην αυξημένη πολυπλοκότητα του μοντέλου επικοινωνίας. Αρχικά θα πρέπει να υπάρχει ένα ασφαλές κανάλι από το οποίο θα μεταφερθεί το ιδιωτικό κλειδί στον χρήστη. Επίσης, ο βαθμός εμπιστοσύνης και οι απαιτήσεις ασφάλειας της Αρχής Εγγραφής θα είναι πολύ μεγαλύτερες, γιατί σε περίπτωση επιτυχούς επίθεσης εκτίθενται τα ιδιωτικά κλειδιά των χρηστών. Το πλεονέκτημα της δημιουργίας του ζεύγους κλειδιών στην Αρχή Εγγραφής ή Πιστοποίησης επιτρέπει την ασφαλή αποθήκευση του ιδιωτικού κλειδιού και την ανάκτηση του αν ο χρήστης χάσει το κλειδί.

Σε ένα ανοικτό Διαδικτυακό περιβάλλον τα κλειδιά δημιουργούνται στο περιβάλλον του χρήστη, ενώ σε εταιρικά περιβάλλοντα υπάρχει συνήθως μια υπηρεσία η οποία δημιουργεί και παρέχει τα κλειδιά στους χρήστες.

Όποια εναλλακτική και να ακολουθηθεί, το ιδιωτικό κλειδί καταλήγει στο Ασφαλές Προσωπικό Περιβάλλον του χρήστη (*Personal Security Environment*) το οποίο μπορεί να είναι είτε ένας σκληρός δίσκος, ή ένας αποσπώμενος δίσκος ή ακόμα μία έξυπνη κάρτα. Από τα τρία, η ασφαλέστερη αποθήκευση είναι η έξυπνη κάρτα, η οποία θεωρείται ανθεκτική σε εξωτερικές επεμβάσεις (*tamper proof*) και έχει τη δυνατότητα να δημιουργεί τις ψηφιακές υπογραφές χωρίς να απαιτείται το ιδιωτικό

κλειδί να μεταφερθεί σε λιγότερο ασφαλές περιβάλλον, όπως ο προσωπικός υπολογιστής του χρήστη.

Όταν η Αρχή Πιστοποίησης υπογράψει τα στοιχεία του χρήστη μαζί με το δημόσιο του κλειδί, το πιστοποιητικό που προκύπτει μεταφέρεται στον χρήστη είτε άμεσα, είτε μέσω της υπηρεσίας καταλόγου. Στη δεύτερη περίπτωση, η Αρχή Πιστοποίησης δημοσιεύει το πιστοποιητικό σε κάποιο κατάλογο ο οποίος διατίθεται δημόσια. Από το δημόσιο κατάλογο όλα τα μέλη έχουν πρόσβαση όπου επιτρέπεται μόνον η ανάγνωση. Αντίθετα, η Αρχή Πιστοποίησης έχει δυνατότητα πρόσβασης ανάγνωσης και εγγραφής. Οι απαιτήσεις ασφάλειας του καταλόγου είναι σχετικά μικρές, αφού η αυθαίρετη τροποποίηση ενός ή περισσοτέρων πιστοποιητικών μπορεί να ανιχνευθεί. Ο αντίπαλος που θα επιχειρήσει να μεταβάλλει το πιστοποιητικό κάποιου χρήστη θα πρέπει να γνωρίζει το ιδιωτικό κλειδί της Αρχής Πιστοποίησης.

Διαδικασία ελέγχου του πιστοποιητικού

Θεωρούμε τη διαδικασία όπου ένας χρήστης επιθυμεί να επικοινωνήσει με έναν άλλον. Επίσης θεωρούμε ότι η ασφαλής επικοινωνία απαιτεί αμοιβαία αυθεντικοποίηση των δύο χρηστών και καθορισμό κλειδιού συνόδου. Σ' αυτό το σημείο θα περιγράψουμε τη διαδικασία αυθεντικοποίησης των μελών από τα ψηφιακά χαρακτηριστικά.

Αρχικά, ο χρήστης Α επικοινωνεί με τον χρήστη Β ή με τον κατάλογο, προκειμένου να προσκομίσει το δημόσιο κλειδί του χρήστη Β. Στη συνέχεια, εκτελεί τις ακόλουθες δύο ενέργειες ελέγχου:

1. **Έλεγχος των στοιχείων του πιστοποιητικού**. Κατά τον έλεγχο αυτό, ο Α εξετάζει τα στοιχεία του πιστοποιητικού που περιγράφουν τον Β, καθώς και την επικαιρότητα του πιστοποιητικού. Το πιστοποιητικό θεωρείται επίκαιρο, αν η ημερομηνία λήξης είναι μεγαλύτερη από την τρέχουσα ημερομηνία.

2. **Έλεγχος ανάκλησης του πιστοποιητικού**. Πολλές φορές, λόγω κακής χρήσης του πιστοποιητικού ή λόγω υποψίας διαρροής του ιδιωτικού κλειδιού, το πιστοποιητικό μπορεί να λήξει πριν από την αναγραφόμενη ημερομηνία λήξης. Η τεχνητή αυτή λήξη ονομάζεται ανάκληση του πιστοποιητικού. Υπάρχουν δύο τεχνολογίες ανάκλησης του πιστοποιητικού: οι **λίστες ανακληθέντων πιστοποιητικών** (*certificate revocation lists*) και το **πρωτόκολλο κατάστασης πιστοποιητικού** (*online certificate status protocol*). Οι λίστες ανακληθέντων πιστοποιητικών είναι πιστοποιητικά ειδικού τύπου τα οποία υπογράφει και εκδίδει η Αρχή Πιστοποίησης, όπου φαίνονται όλα τα πιστοποιητικά τα οποία έχουν ανακληθεί. Το πρωτόκολλο κατάστασης πιστοποιητικού προϋποθέτει σύνδεση με την αντίστοιχη υπηρεσία της Αρχής Πιστοποίησης η οποία παρέχει πληροφορίες σχετικά με την ανάκληση ενός συγκεκριμένου πιστοποιητικού.

Μετά την επιτυχή ολοκλήρωση των δύο παραπάνω ελέγχων και από τις δύο πλευρές, ακολουθεί πρωτόκολλο αυθεντικοποίησης το οποίο βασίζεται σε ασύμμετρη κρυπτογραφία.

Διαδικασία ανάκλησης του πιστοποιητικού

Η ανάκληση του πιστοποιητικού γίνεται σε δύο περιπτώσεις:

- Στην περίπτωση που ο χρήστης υποψιασθεί ότι το ιδιωτικό του κλειδί έχει εκτεθεί και έχει γίνει γνωστό σε τρίτους.
- Στην περίπτωση που γίνει κακή χρήση του πιστοποιητικού από τον χρήστη. Κακή χρήση ορίζεται η οποιαδήποτε χρήση του πιστοποιητικού πέραν της προβλεπόμενης.

Ο προορισμός χρήσης των πιστοποιητικών καθορίζεται από την Αρχή Πιστοποίησης. Ένα πιστοποιητικό μπορεί να χρησιμοποιηθεί για αυθεντικοποίηση, για εμπιστευτικότητα, ή και για τις δύο υπηρεσίες. Λόγω των νομικών περιορισμών, ή για καθαρά πρακτικούς λόγους, η χρήση των

πιστοποιητικών είναι συγκεκριμένη. Για την κρυπτογράφηση μηνυμάτων για παράδειγμα, υπάρχουν νομικοί περιορισμοί που διαφέρουν από χώρα σε χώρα. Οι νομικοί περιορισμοί επικεντρώνονται στο μέγεθος του ιδιωτικού κλειδιού. Αντίθετα, στην περίπτωση της αυθεντικοποίησης με τη χρήση της ψηφιακής υπογραφής, δεν υπάρχει ουσιαστικός περιορισμός. Έτσι, η κρυπτογράφηση με ένα κλειδί το οποίο χρησιμοποιείται για αυθεντικοποίηση ενδεχομένως μπορεί να αποτελέσει αδίκημα.

Ο διαχωρισμός της χρήσης των πιστοποιητικών για αυθεντικοποίηση και εμπιστευτικότητα, συμβάλλει στην καλύτερη διαχείριση των κλειδιών. Στην περίπτωση των πιστοποιητικών αυθεντικοποίησης δεν απαιτείται εφεδρική αποθήκευση του ιδιωτικού κλειδιού, διότι εάν ο χρήστης χάσει το κλειδί του, μπορεί να ζητήσει νέο πιστοποιητικό χωρίς να υπάρξουν πρακτικές συνέπειες. Στην περίπτωση όμως που ο χρήστης χάσει το ιδιωτικό κλειδί του πιστοποιητικού που χρησιμοποιεί για εμπιστευτικότητα, τότε αν δεν υπάρχει εφεδρική αποθήκευση του ιδιωτικού κλειδιού, δεν θα είναι σε θέση να αποκρυπτογραφήσει όλα τα κρυπτοκείμενα που κρυπτογραφήθηκαν με το αντίστοιχο δημόσιο κλειδί. Συνεπώς, η εφεδρική αποθήκευση του ιδιωτικού κλειδιού ενός πιστοποιητικού εμπιστευτικότητας είναι επιθυμητή, αφού συμβάλει στη μείωση του ρίσκου άρνησης υπηρεσίας.

Όταν η Αρχή Πιστοποίησης κρίνει ότι απαιτείται ανάκληση του πιστοποιητικού ενός χρήστη, ανανεώνει τη λίστα ανακληθέντων πιστοποιητικών και τη δημοσιεύει στον κατάλογο που χρησιμοποιεί για τα πιστοποιητικά. Έτσι κατά τον έλεγχο ανάκλησης, ο χρήστης μπορεί να παραλάβει τη λίστα από τον κατάλογο. Σε κρίσιμες εφαρμογές, η Αρχή Πιστοποίησης (ή η υπηρεσία ανάκλησης, αν αυτή είναι διαφορετική από την Αρχή Πιστοποίησης) αναλαμβάνει τη μετάδοση της λίστας απευθείας στους χρήστες, όποτε γίνεται ανανέωση του περιεχομένου της.

Εναλλακτικά, ο χρήστης μπορεί να επικοινωνήσει με την υπηρεσία ανάκλησης για να πληροφορηθεί σχετικά με την εγκυρότητα ενός

πιστοποιητικού, μέσω κάποιου πρωτοκόλλου ανάκλησης, όπως το πρωτόκολλο ανάκλησης πιστοποιητικού, OCSP.

5.12 Κρυπτογραφικά συστήματα που χρησιμοποιούνται σήμερα

Τα τελευταία χρόνια έχουν αναπτυχθεί και χρησιμοποιηθεί αρκετά κρυπτογραφικά συστήματα για το Internet. Μπορούμε να τα χωρίσουμε σε δύο κατηγορίες. Η πρώτη είναι προγράμματα και πρωτόκολλα που χρησιμοποιούνται για την κρυπτογράφηση μηνυμάτων του ηλεκτρονικού ταχυδρομείου (e-mail). Τα ποιο δημοφιλή είναι τα παρακάτω:

- **PGP**
- **S/MIME**

Η δεύτερη κατηγορία είναι πρωτόκολλα δικτύου που χρησιμοποιούνται για να παρέχουν εμπιστευτικότητα, ακεραιότητα, αυθεντικοποίηση σε περιβάλλον δικτύου. Αυτά τα συστήματα χρειάζονται αλληλεπίδραση πραγματικού χρόνου ανάμεσα στον πελάτη (client) και στον διακομιστή (server) για να λειτουργήσουν σωστά. Τα ποιο δημοφιλή είναι τα παρακάτω:

- **SSL**
- **PCT**
- **S-HTTP**
- **SET and CyberCash**
- **DNSSEC**
- **IPsec and IPv6**
- **Kerberos**
- **SSH**

Όλα τα συστήματα περιγράφονται και συγκρίνονται στον Πίνακα 5.2 που ακολουθεί στην επόμενη σελίδα.

ΣΥΣΤΗΜΑ	ΤΙ ΕΙΝΑΙ;	ΑΛΓΟΡΙΘΜΟΙ	ΤΙ ΠΑΡΕΧΕΙ;
PGP	Εφαρμογή κρυπτογράφησης για πρόγραμμα ηλ. ταχυδρομείου	IDEA, RSA, MD5	Εμπιστευτικότητα, Ακεραιότητα, Αυθεντικοποίηση, Μη-απάρνηση
S/MIME	Format για κρυπτογράφηση ηλεκτρονικού ταχυδρομείου	Καθορίζεται από τον χρήστη	Εμπιστευτικότητα, Ακεραιότητα, Αυθεντικοποίηση, Μη-απάρνηση
SSL	Πρωτόκολλο για να κρυπτογραφεί τις TCP/IP μεταδόσεις	RSA, RCZ, RC4, MD5 κ.ά.	Εμπιστευτικότητα, Ακεραιότητα, Αυθεντικοποίηση, Μη-απάρνηση
PCT	Πρωτόκολλο για να κρυπτογραφεί τις TCP/IP μεταδόσεις	RSA, MD5, RCZ, RC4 κ.ά.	Εμπιστευτικότητα, Ακεραιότητα, Αυθεντικοποίηση, Μη-απάρνηση
S-HTTP	Πρωτόκολλο για να κρυπτογραφεί τις HTTP αιτήσεις και απαντήσεις	RSA, DES κ.ά.	Εμπιστευτικότητα, Ακεραιότητα, Αυθεντικοποίηση, Μη-απάρνηση
SET and CyberCash	Πρωτόκολλα για αποστολή ασφαλών εντολών πληρωμής μέσω του Internet	RSA, MD5, RC2	Εμπιστευτικότητα, Ακεραιότητα, Αυθεντικοποίηση, Μη-απάρνηση
DNSSEC	Secure Domain Name System	RSA, MD5	Ακεραιότητα, Αυθεντικοποίηση
IPsec and IPv6	Χαμηλού επιπέδου πρωτόκολλο για κρυπτογράφηση IP πακέτων	Diffie-Hellman κ.ά.	Εμπιστευτικότητα (προαιρετικά), Ακεραιότητα, Αυθεντικοποίηση
Kerberos	Υπηρεσία ασφάλειας δικτύου για ασφάλιση εφαρμογών υψηλού επιπέδου	DES	Εμπιστευτικότητα Αυθεντικοποίηση
SSH	Κρυπτογράφηση απομακρυσμένου τερματικού (Secure Shell)	RSA, Diffie-Helman, DES, Triple-DES, Blowfish κ.ά.	Εμπιστευτικότητα Αυθεντικοποίηση

Πίνακας 5.3 Σύγκριση κρυπτογραφικών συστημάτων του Internet

5.12.1 PGP (*Pretty Good Privacy*)

Το PGP είναι το πρώτο πρόγραμμα κρυπτογράφησης δημόσιου κλειδιού, γραμμένο από τον Phil Zimmerman που κυκλοφόρησε στο Internet τον Ιούνιο του 1991. Το PGP είναι ένα ολοκληρωμένο σύστημα που προσφέρει κρυπτογραφική προστασία των e-mails και των αρχείων γενικότερα. Το PGP επίσης είναι ένα σύνολο από πρότυπα (standards) που περιγράφουν τις μορφές (formats) των κρυπτογραφημένων μηνυμάτων, των κλειδιών και των ψηφιακών υπογραφών.

Το PGP είναι ένα κρυπτογραφικό σύστημα διασταύρωσης που χρησιμοποιεί τον RSA, αλγόριθμο κρυπτογράφησης δημόσιου κλειδιού, για την διαχείριση των κλειδιών και τον IDEA, συμμετρικό αλγόριθμο, για την κύρια κρυπτογράφηση των δεδομένων.

Το PGP προσφέρει εμπιστευτικότητα, εξαιτίας του ότι ο κρυπτογραφικός αλγόριθμος που χρησιμοποιεί είναι ο IDEA. Προσφέρει ακεραιότητα, εξαιτίας του ότι η συνάρτηση αποσύνθεσης (hash function) που χρησιμοποιεί είναι η MD5. Προσφέρει αυθεντικοποίηση με την χρήση των πιστοποιητικών δημοσίου κλειδιού και προσφέρει και απαγόρευση απάρνησης λόγω των κρυπτογραφικά υπογεγραμμένων μηνυμάτων.

Το PGP είναι διαθέσιμο με δυο τρόπους, σαν μια μεμονωμένη εφαρμογή και σαν ένα ολοκληρωμένο πρόγραμμα ηλεκτρονικού ταχυδρομείου διαθέσιμο από την PGP Inc. Το μεμονωμένο πρόγραμμα "τρέχει" σε πολύ περισσότερα συστήματα από ότι το ολοκληρωμένο πρόγραμμα, αλλά είναι περισσότερο δύσχρηστο. Ένα τέτοιο παράδειγμα που ήταν πολύ διαδεδομένο είναι η εκδόσεις του PGP για περιβάλλον DOS. Επίσης η PGP Inc. αναπτύσσει διάφορα πρόσθετα προγράμματα (plug-ins) για δημοφιλή προγράμματα ηλεκτρονικού ταχυδρομείου για να επιτρέψει σε αυτά να στέλνουν και να λαμβάνουν κρυπτογραφημένα μηνύματα με το PGP.

Ένα πρόβλημα με το PGP είναι η διαχείριση και πιστοποίηση των δημόσιων κλειδιών. Τα κλειδιά που χρησιμοποιεί το PGP δεν έχουν

ημερομηνία λήξης, αντί αυτού, όταν τα κλειδιά εκτεθούν, εξαρτάται από τον ιδιοκτήτη εάν αυτός θέλει να διανέμει, στα μέλη με τα οποία είχε επικοινωνία, μια ειδική PGP πιστοποίηση ακύρωσης του κλειδιού. Οι ανταποκριτές, που δεν μαθαίνουν το γεγονός αυτό και χρησιμοποιούν το εκτεθειμένο κλειδί για εβδομάδες, μήνες ή ακόμα και χρόνια αργότερα, το να στείλουν κρυπτογραφημένα μηνύματα το κάνουν με δική τους ευθύνη, ρισκάροντας την ασφάλεια των μηνυμάτων. Αυτό έχει σαν αποτέλεσμα, εάν δημιουργήσουμε και διανέμουμε ένα PGP δημόσιο κλειδί, πρέπει να διατηρήσουμε το κλειδί μυστικό για πάντα, επειδή το κλειδί αυτό δεν λήγει ποτέ.

5.12.2 S/MIME (*Multipurpose Internet Mail Extensions*)

Το MIME είναι ένα πρότυπο για αποστολή μηνυμάτων με επισυναπτόμενα δυαδικά αρχεία μέσω του Internet. Το Secure/MIME είναι μια επέκταση του προτύπου MIME για την αναγνώριση των κρυπτογραφημένων e-mail. Αντίθετα από το PGP, το S/MIME δεν εφαρμόσθηκε σαν ένα αυτόνομο πρόγραμμα, αλλά σαν ένα εργαλείο που σχεδιάστηκε για να προστίθεται σε διάφορα πακέτα ηλεκτρονικού ταχυδρομείου. Επειδή αυτό το εργαλείο προέρχεται από την RSA Data Security και περιλαμβάνει άδειες για όλους τους απαιτούμενους αλγόριθμους και όλες τις πατέντες, και επειδή οι μεγαλύτερες εταιρίες που πουλούν συστήματα e-mail ήδη έχουν επιχειρηματική σχέση με την RSA Data Security, είναι πιθανό το S/MIME θα υιοθετηθεί περισσότερο απ' ότι το PGP, απ' τις εταιρίες παροχής ηλεκτρονικού ταχυδρομείου.

Το S/MIME προσφέρει εμπιστευτικότητα, εξαιτίας του ότι ο κρυπτογραφικός αλγόριθμος καθορίζεται από τον χρήστη. Προσφέρει ακεραιότητα, εξαιτίας του ότι η συνάρτηση αποσύνθεσης (hash function) καθορίζεται από τον χρήστη. Προσφέρει αυθεντικοποίηση με την χρήση των πιστοποιητικών δημοσίου κλειδιού X.509 v3 και προσφέρει και απαγόρευση απάρνησης λόγω των κρυπτογραφικά υπογεγραμμένων

μηνυμάτων. Το σύστημα μπορεί να χρησιμοποιηθεί με δυνατή ή αδύνατη κρυπτογράφηση.

Για να στείλουμε κρυπτογραφημένα μηνύματα σε κάποιον με το S/MIME, πρέπει να έχουμε ένα αντίγραφο του δημόσιου κλειδιού του. Αναμένεται ότι, τα περισσότερα προγράμματα, που χρησιμοποιούν το S/MIME, θα χρησιμοποιούν πιστοποιητικά υποδομής δημόσιου κλειδιού, όπως το X.509 v3, σαν αυτά που δημιουργούνται από την VeriSign και από άλλες αρχές πιστοποίησης.

5.12.3 SSL (*Secure Socket Layer*)

Το SSL είναι ένα κρυπτογραφικό πρωτόκολλο για ασφαλή κανάλια επικοινωνίας διπλής κατεύθυνσης. Το SSL χρησιμοποιείται συχνά με το TCP/IP πρωτόκολλο του Internet. Το SSL είναι το κρυπτογραφικό σύστημα που χρησιμοποιείται από τους web browsers όπως είναι ο Netscape Navigator και ο Microsoft Internet Explorer, αλλά μπορεί να χρησιμοποιηθεί σε οποιοδήποτε υπηρεσία TCP/IP.

Οι SSL συνδέσεις συχνά ξεκινούν από την πλευρά του web browser εξαιτίας της χρήσης ενός ειδικού προθέματος στην URL διεύθυνση. Για παράδειγμα το πρόθεμα “https://” χρησιμοποιείται για να υποδείξει μια SSL-κρυπτογραφημένη HTTP σύνδεση, ενώ “snews://” χρησιμοποιείται για να υποδείξει μια SSL-κρυπτογραφημένη NNTP σύνδεση.

Το SSL προσφέρει εμπιστευτικότητα, εξαιτίας του ότι ο κρυπτογραφικός αλγόριθμος καθορίζεται από τον χρήστη. Προσφέρει ακεραιότητα, εξαιτίας του ότι η συνάρτηση αποσύνθεσης καθορίζεται από τον χρήστη. Προσφέρει αυθεντικοποίηση με την χρήση των πιστοποιητικών δημοσίου κλειδιού X.509 v3 και προσφέρει και απαγόρευση απάρνησης λόγω των κρυπτογραφικά υπογεγραμμένων μηνυμάτων.

5.12.4 PCT (*Private Communications Technology*)

Το PCT είναι ένα ασφαλές πρωτόκολλο επιπέδου μεταφοράς, παρόμοιο με το SSL, το οποίο αναπτύχθηκε από την Microsoft. Το PCT αναπτύχθηκε σαν απάντηση στα προβλήματα που παρουσίασε το SSL 2.0, αλλά και στο SSL 3.0.

Αν και η Microsoft υποστηρίζει το SSL 3.0 και το TLS, το καινούργιο Transport Layer Security μοντέλο, σκοπεύει να συνεχίσει να υποστηρίζει το PCT γιατί χρησιμοποιείται από πολλούς μεγάλους πελάτες της στα εταιρικά τους ενδοδίκτυα (corporate intranets).

5.12.5 S-HTTP

Το S-HTTP είναι ένα σύστημα για την υπογραφή και κρυπτογράφηση πληροφοριών που στέλνονται μέσω του HTTP πρωτοκόλλου. Το S-HTTP σχεδιάστηκε πριν κυκλοφορήσει δημόσια το SSL. Περιλαμβάνει μερικά κομψά χαρακτηριστικά, όπως είναι η ικανότητα να έχει προϋπογράψει κείμενα που βρίσκονται σε έναν web server. Αλλά το S-HTTP είναι κυρίως ένα «νεκρό» πρωτόκολλο επειδή η Netscape και η Microsoft έχουν αποτύχει να το εφαρμόσουν στους browsers.

5.12.6 SET

Το SET είναι ένα κρυπτογραφικό πρωτόκολλο σχεδιασμένο για την αποστολή κρυπτογραφημένων αριθμών πιστωτικών καρτών μέσω του Internet. Το πρωτόκολλο αυτό είναι ακόμα υπό ανάπτυξη.

Υπάρχουν τρία μέρη που αποτελούν το SET: ένα «ηλεκτρονικό πορτοφόλι» που υπάρχει στον υπολογιστή του χρήστη, ένας διακομιστής (server) που τρέχει στους εμπορικούς δικτυακούς τόπους, και ο SET server πληρωμής (SET Payment Server) που «τρέχει» στη τράπεζα του εμπόρου.

Για να χρησιμοποιήσουμε το σύστημα SET, πρέπει να εισάγουμε πρώτα τον αριθμό της πιστωτικής μας κάρτας στο πρόγραμμα του «ηλεκτρονικού

πορτοφολιού». Οι περισσότερες εφαρμογές αποθηκεύουν τον αριθμό της πιστωτικής κάρτας σε ένα κρυπτογραφημένο αρχείο στον σκληρό μας δίσκο ή σε μια κάρτα (*smart card*). Το πρόγραμμα επίσης δημιουργεί ένα δημόσιο και ένα μυστικό κλειδί για την κρυπτογράφηση διάφορων οικονομικών πληροφοριών μας που θα σταλούν μέσω του Internet.

Όταν εμείς θελήσουμε να αγοράσουμε κάτι, ο αριθμός της πιστωτικής μας κάρτας κρυπτογραφείται και στέλνεται στον έμπορο. Το πρόγραμμα του έμπορου υπογράφει ψηφιακά το μήνυμα πληρωμής και το προωθεί στην τράπεζα όπου το επεξεργάζεται. Εκεί ο SET server πληρωμής αποκρυπτογραφεί όλες τις πληροφορίες και χρεώνει την πιστωτική κάρτα. Στο τέλος, μια απόδειξη είσπραξης στέλνεται πίσω και σε εμάς, τους πελάτες, αλλά και στον έμπορο.

Οι Τράπεζες που επεξεργάζονται τις πιστωτικές κάρτες είναι ενθουσιασμένες για το SET επειδή αυτές κρατούν τους αριθμούς των πιστωτικών καρτών μακριά από τα χέρια των εμπόρων. Αυτό θα περιόριζε σημαντικά τις απάτες που γίνονται, γιατί οι έμποροι, και όχι νεαροί hackers, είναι αυτοί που είναι υπεύθυνοι για τις απάτες των πιστωτικών καρτών σήμερα.

Το SET προσφέρει εμπιστευτικότητα για τους αριθμούς των πιστωτικών καρτών, καθώς κρυπτογραφούνται χρησιμοποιώντας τον RSA αλγόριθμο. Αλλά δεν προσφέρει εμπιστευτικότητα (και κατά συνέπεια μυστικότητα) για τα υπόλοιπα στοιχεία της συναλλαγής του χρήστη. Αυτή ήταν μια αναγκαία συμβιβαστική λύση για να κερδιθεί η έγκριση για την εξαγωγή SET λογισμικού χωρίς περιορισμούς. Το SET παρέχει ακεραιότητα, αυθεντικοποίηση και απαγόρευση απάρνησης χρησιμοποιώντας συναρτήσεις αποσύνθεσης μηνύματος και ψηφιακές υπογραφές.

5.12.7 CyberCash

Το CyberCash είναι ένα πρωτόκολλο ηλεκτρονικής πληρωμής παρόμοιο στο σκοπό με το SET. Στην πραγματικότητα μέρη του SET ήταν μοντέλα ανάπτυξης στο CyberCash. Είναι θα λέγαμε μια παραλλαγή προϊόντος.

5.12.8 DNSSEC (*Domain Name System Security*)

Το πρότυπο Domain Name System Security είναι ένα σύστημα που σχεδιάστηκε για να φέρει ασφάλεια στο Σύστημα Ονοματοδοσίας Διαδικτύου (Domain Name System (DNS)). Το DNSSEC δημιουργεί μία παράλληλη υποδομή δημόσιου κλειδίου «χτισμένη» πάνω στο DNS σύστημα. Κάθε DNS τομέας καθορίζεται από ένα δημόσιο κλειδί. Ένα δημόσιο κλειδί τομέα μπορούμε να το αποκτήσουμε με έναν έμπιστο τρόπο από τον γονικό τομέα (parent domain) ή αυτό μπορεί να φορτωθεί από πριν μέσα σε ένα DNS διακομιστή χρησιμοποιώντας το αρχείο "boot" του server.

Το DNSSEC αναγνωρίζεται για τις ασφαλής ανανεώσεις πληροφοριών στους DNS διακομιστές, κάνοντάς το ιδανικό για απομακρυσμένη διαχείριση. Εφαρμογές που δουλεύουν είναι διαθέσιμες για λήψη από την Trust Information System (http://www.tis.com) και από την CyberCash (http://www.cybercash.com).

5.12.9 IPsec και IPv6

Το IPsec είναι ένα κρυπτογραφικό πρωτόκολλο σχεδιασμένο από η IETF (*Internet Engineering Task Force*) για να την παροχή εμπιστευτικότητας από άκρο προς άκρο, για τα πακέτα που διακινούνται μέσω του Internet. Το IPsec δουλεύει με το IPv4, την πρότυπη έκδοση του IP που χρησιμοποιείται σήμερα στο Internet. Το IPv6, το οποίο είναι η "επόμενη γενιά" για το IP, περιλαμβάνει και αυτό το IPsec.

Το IPsec δεν προσφέρεται για την ακεραιότητα, την αυθεντικοποίηση, ή την απαγόρευση απάρνησης, αλλά αφήνει αυτά τα χαρακτηριστικά για άλλα πρωτόκολλα. Η κύρια χρήση του IPsec φαίνεται να είναι ως πρωτόκολλο για την δημιουργία εικονικών ιδιωτικών δικτύων (*Virtual Private Networks -VPNs*) στο Internet. Αλλά το IPsec έχει την ικανότητα να παρέχει αυθεντικοποίηση, ακεραιότητα, και προαιρετικά την εμπιστοσύνη των δεδομένων για όλες τις επικοινωνίες που παίρνουν μέρος στο Internet, υπό την προϋπόθεση ότι οι εταιρίες παροχής υπηρεσιών θα εφαρμόζουν ευρέως το πρωτόκολλο αυτό και ότι επίσης οι κυβερνήσεις θα επιτρέψουν την χρήση του.

5.12.10 Kerberos

Το Kerberos είναι ένα σύστημα ασφάλειας δικτύου που αναπτύχθηκε από το MIT και χρησιμοποιήθηκε απ' άκρου εις άκρον στις Ηνωμένες Πολιτείες. Αντίθετα με τα άλλα συστήματα που αναφέρθηκαν σ' αυτό το κεφάλαιο, το Kerberos δεν χρησιμοποιεί τεχνολογία δημόσιου κλειδιού. Αντί αυτού, το Kerberos είναι βασισμένο σε συμμετρικούς κρυπταλγόριθμους που μοιράζονται μεταξύ του διακομιστή του Kerberos και κάθε ξεχωριστού χρήστη. Κάθε χρήστης έχει το δικό του κωδικό, και ο διακομιστής του Kerberos χρησιμοποιεί αυτόν το κωδικό για να κρυπτογραφήσει μηνύματα που στέλνονται σε αυτόν τον χρήστη έτσι ώστε να μην μπορούν να διαβαστούν από κανέναν άλλο.

Υποστήριξη για το Kerberos πρέπει να προστίθεται σε κάθε πρόγραμμα που χρειάζεται προστασία. Μέχρι στιγμής, υπάρχουν προς χρήση διάφορες "Kerberized" εκδόσεις πρωτοκόλλων όπως το Telnet, FTP, POP, και Sun RPC. Ένα σύστημα που χρησιμοποιούσε το Kerberos για να παρέχει εμπιστευτικότητα στο πρωτόκολλο HTTP αναπτύχθηκε αλλά δεν βγήκε ποτέ από το εργαστήριο.

Το Kerberos είναι ένα δύσκολο σύστημα στο να διαμορφωθεί και να διαχειριστεί. Για να λειτουργήσει ένα τέτοιο σύστημα θα πρέπει κάθε

δικτυακός τόπος (site) να έχει ένα διακομιστή του Kerberos που θα είναι φυσικά ασφαλής. Ο διακομιστής του Kerberos διατηρεί ένα αντίγραφο του κωδικού κάθε χρήστη. Σε περίπτωση που ο διακομιστής του Kerberos εκτεθεί, ο κωδικός κάθε χρήστη πρέπει να αλλαχθεί.

5.12.11 SSH (*Secure Shell*)

Το SSH είναι το ασφαλές κέλυφος (*Secure Shell*). Παρέχει προστασία με τη χρήση κρυπτογραφίας σε εικονικά τερματικά (*Telnet*) και λειτουργίες μεταφοράς αρχείων (*rcp*). Μη εμπορικές εκδόσεις του SSH είναι διαθέσιμες για πολλές εκδόσεις UNIX συστημάτων. Το SSH είναι διαθέσιμο για συστήματα UNIX, Windows, και Macintosh συστήματα από την εταιρία Data Fellows (http://www.datafellows.com).

Κεφάλαιο 6ο: SSL (Secure Socket Layer)

Εισαγωγή

Το SSL (*Secure Socket Layer*), είναι ένα γενικού σκοπού πρωτόκολλο για την αποστολή κρυπτογραφημένης πληροφορίας μέσω του Internet. Αναπτύχθηκε από την Netscape και έγινε προσιτό από το πλατύ κοινό από τον web browser και τον server της Netscape. Η ιδέα ήταν να αυξήσουν τις πωλήσεις των κρυπτογραφικά ενεργοποιημένων web server μιας εταιρίας, διανέμοντας έναν ελεύθερο πελάτη (free client) ο οποίος εφάρμοζε τα ίδια κρυπτογραφικά πρωτόκολλα.

Από τότε το SSL έχει ενσωματωθεί μέσα σε πολλούς άλλους web servers και browsers, με αποτέλεσμα η υποστήριξη του SSL να μην είναι ένα ανταγωνιστικό πλεονέκτημα αλλά μια. αναγκαιότητα. Το SSL χρησιμοποιείται και για μη δικτυακές εφαρμογές όπως για παράδειγμα για το secure Telnet. Το SSL είναι τώρα ένα από τα ποιο δημοφιλή πρωτόκολλα κρυπτογράφησης στο Internet.

Η Internet Engineering Task Force (IETF) είναι τώρα στην διαδικασία της δημιουργίας ενός Transport Layer Security (TLS) πρωτοκόλλου. Αυτό το πρωτόκολλο είναι βασισμένο στο SSL 3.0, με μικρές αλλαγές στις επιλογή των αλγόριθμων αυθεντικοποίησης και στην μορφή των μηνυμάτων.

6.1 Τι είναι το SSL

Το SSL είναι ένα επίπεδο που τοποθετείται μεταξύ του TCP/IP πρωτοκόλλου και του επιπέδου εφαρμογών. Ενώ το TCP/IP πρωτόκολλο απλά στέλνει ένα ανώνυμο και χωρίς λάθη (error-free) ρεύμα πληροφοριών ανάμεσα στους δύο υπολογιστές (ή ανάμεσα σε δύο διεργασίες οι οποίες λειτουργούν στον ίδιο υπολογιστή), το SSL προσθέτει πολυάριθμες λειτουργίες σε αυτό το ρεύμα, περιλαμβάνοντας:

- Αυθεντικοποίηση και απαγόρευση απάρνησης του διακομιστή

(server), χρησιμοποιώντας ψηφιακές υπογραφές.

- Αυθεντικοποίηση και απαγόρευση απάρνησης του πελάτη (client), χρησιμοποιώντας ψηφιακές υπογραφές.
- Εμπιστοσύνη δεδομένων μέσω της χρήσης της κρυπτογραφίας.
- Ακεραιότητα δεδομένων μέσω της χρήσης κωδικών για την αυθεντικοποίηση των μηνυμάτων.

Η κρυπτογραφία είναι ένας γρήγορα αναπτυσσόμενος τομέας, και τα κρυπτογραφικά πρωτόκολλα δεν λειτουργούν αν τα δυο μέρη της επικοινωνίας δεν χρησιμοποιούν τους ίδιους αλγόριθμους. Για το λόγο αυτό το SSL είναι επεκτάσιμο και ένα πρωτόκολλο που μπορεί να προσαρμοστεί εύκολα. Όταν ένα πρόγραμμα που χρησιμοποιεί SSL προσπαθεί να επικοινωνήσει με ένα άλλο, τότε τα δύο προγράμματα ηλεκτρονικά συγκρίνουν κάποια στοιχεία και καθορίζουν ποιο είναι το πιο ισχυρό κρυπτογραφικό πρωτόκολλο που διαθέτουν από κοινού. Αυτή η συναλλαγή ονομάζεται *SSL Hello.*

Το SSL σχεδιάστηκε για χρήση σε παγκόσμιο επίπεδο, αλλά αναπτύχθηκε στις Ηνωμένες Πολιτείες και συμπεριλαμβάνεται μέσα στα προγράμματα που πωλούνται από εταιρίες των Ηνωμένων Πολιτειών για χρήση στο εξωτερικό. Για το λόγο αυτό, το SSL περιέχει πολλές λειτουργίες σχεδιασμένες έτσι ώστε να μπορεί να συμμορφώνεται με τις κυβερνητικές περιοριστικές πολιτικές σε θέματα εξαγωγής κρυπτογραφικών συστημάτων των Ηνωμένων Πολιτειών.

6.2 Εκδόσεις του SSL

Το SSL πρωτόκολλο σχεδιάστηκε από την Netscape για χρήση με τον Netscape Navigator. Η έκδοση 1.0 του πρωτοκόλλου χρησιμοποιήθηκε μέσα στο Netscape. Η έκδοση 2.0 συμπεριλήφθηκε με το Netscape Navigator 1 και 2. Αφού το SSL 2.0 δημοσιεύτηκε, η Microsoft δημιούργησε ένα παρόμοιο πρωτόκολλο ασφαλούς σύνδεσης, ονομαζόμενο PCT, το οποίο ξεπέρασε μερικές αδυναμίες του SSL 2.0. Τα πλεονεκτή-

ματα του PCT ενσωματώθηκαν στο SSL 3.0. Το πρωτόκολλο SSL 3.0 χρησιμοποιήθηκε σαν την βάση για το Transport Layer Security (*TLS*) πρωτόκολλο το οποίο αναπτύχθηκε από την IETF.

6.3 Χαρακτηριστικά του SSL

Το SSL 3.0 προσφέρει πολλά χαρακτηριστικά θεωρητικού αλλά και πρακτικού ενδιαφέροντος.

6.3.1 Διαχωρισμός των καθηκόντων

Το SSL χρησιμοποιεί ξεχωριστούς αλγόριθμους για την κρυπτογράφηση, την αυθεντικοποίηση και την ακεραιότητα των δεδομένων με διαφορετικά κλειδιά (που ονομάζονται "μυστικά", secrets) για κάθε λειτουργία. Το βασικό πλεονέκτημα αυτού του διαχωρισμού των καθηκόντων είναι ότι τα μεγαλύτερα κλειδιά μπορούν να χρησιμοποιηθούν για την αυθεντικοποίηση και για την ακεραιότητα των δεδομένων, ενώ τα μικρότερα κλειδιά να χρησιμοποιούνται για την μυστικότητα. Αυτό είναι χρήσιμο για τα προϊόντα που σχεδιάζονται με σκοπό την εξαγωγή τους από τις Ηνωμένες Πολιτείες, καθώς οι ομοσπονδιακοί κανόνες θέτουν περιορισμούς στο θέμα του μήκους των κλειδιών που χρησιμοποιούνται για την εμπιστευτικότητα ενώ δεν υπάρχουν περιορισμοί για την περίπτωση της ακεραιότητας των δεδομένων και της αυθεντικοποίησης.

Το SSLv3 παρέχεται για τις συνδέσεις που δεν κρυπτογραφούνται αλλά αποδεικνύεται η γνησιότητα τους και προστατεύονται εναντίον προμελετημένων αλλοιώσεων από κάποιον επιτηδευμένο εισβολέα. Αυτό ίσως είναι χρήσιμο σε περίπτωση που η κρυπτογράφηση είναι απαγορευμένη από το νόμο, όπως συμβαίνει στην Γαλλία.

Η επιλογή των αλγόριθμων και του μήκους των κλειδιών καθορίζεται από τον SSL διακομιστή, αλλά περιορίζεται και από τον διακομιστή και από τον πελάτη.

6.3.2 Αποδοτικότητα

Η κρυπτογράφηση και αποκρυπτογράφηση δημόσιου κλειδιού είναι μια χρονοβόρα διαδικασία. Πόσο μάλλον όταν επαναλαμβάνεται αυτή η επεξεργασία για κάθε επικοινωνία ανάμεσα στον πελάτη και σε έναν διακομιστή. Οι SSL εφαρμογές μπορούν να αποθηκεύουν κρυφά (cache) ένα κύριο μυστικό (master secret) που διατηρείται αναλλοίωτο μεταξύ των SSL συνδέσεων. Αυτό επιτρέπει στις καινούργιες SSL συνδέσεις να ξεκινήσουν αμέσως την ασφαλή επικοινωνία, χωρίς να χρειάζεται να εκτελεστούν περισσότερες λειτουργίες δημόσιου κλειδιού.

6.3.3 Πιστοποιητικό βασισμένο στην απόδειξη γνησιότητας

Το SSL παρέχεται για την αυθεντικοποίηση του πελάτη καθώς και του διακομιστή, μέσω της χρήσης των ψηφιακών πιστοποιητικών και των ψηφιακά υπογεγραμμένων αιτήσεων ταυτότητας.

Το SSLv3 χρησιμοποιεί τα X.509 v3 πιστοποιητικά, μολονότι η IETF τυποποίηση του SSL (πιθανώς ονομάζεται TLS) ίσως χρησιμοποιεί διαφορετικά είδη πιστοποιητικών καθώς είναι τυποποιημένα. Η αυθεντικοποίηση είναι ένα προαιρετικό μέρος του πρωτοκόλλου, μολονότι τα πιστοποιητικά του διακομιστή είναι αποτελεσματικά εξουσιοδοτημένα από τις σημερινές SSL εφαρμογές.

6.3.4 Αγνωστικό πρωτόκολλο (Protocol Agnostic)

Παρόλο που το SSL σχεδιάστηκε για να λειτουργεί στην κορυφή του TCP/IP πρωτοκόλλου, στην πραγματικότητα όμως μπορεί να λειτουργήσει στην κορυφή κάθε αξιόπιστου connection-oriented πρωτοκόλλου, όπως είναι το X.25 ή το OSI. Το SSL πρωτόκολλο δεν μπορεί να λειτουργήσει στην κορυφή ενός μη αξιόπιστου πρωτοκόλλου όπως είναι το IP User Datagram Protocol (UDP).

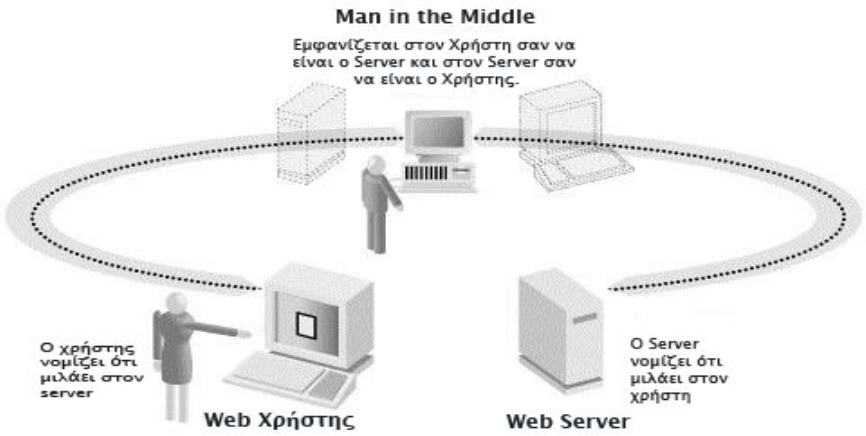
Όλη η SSL επικοινωνία λαμβάνει χώρα διαμέσου ενός μονού αμφίδρομου καναλιού. Στην περίπτωση του TCP/IP, οι πόρτες που χρησιμοποιούνται συνήθως είναι αυτές του παρακάτω πίνακα.

Keyword	Δεκαδική Πόρτα	Σκοπός
https	443/tcp	SSL-protected **HTTP**
ssmtp	465/tcp	SSL-protected **SMTP** (αποστολή e-mail)
snews	563/tcp	SSL-protected **Usenet News**
ssl-ldap	636/tcp	SSL-protected **LDAP**
spop3	995/tcp	SSL-protected **POP3** (λήψη e-mail)

Πίνακας 6.1 Πόρτες TCP/IP που χρησιμοποιούνται από τα πρωτόκολλα SSL

6.3.5 Προστασία ενάντια στις man-in-the-middle και replay επιθέσεις

Το SSL πρωτόκολλο είναι ειδικά σχεδιασμένο για την προστασία ενάντια στις man-in-the-middle και replay επιθέσεις. Σε μια man-in-the-middle επίθεση, ο επιτιθέμενος παρεμβάλλεται και υποκλέπτει όλες τις επικοινωνίες ανάμεσα στα δύο μέρη, κάνοντας τον καθένα να νομίζει ότι συνεχίζει να επικοινωνεί ακόμα με τον άλλον. Η όλη διαδικασία παρουσιάζεται στο *Σχήμα 6.1*.

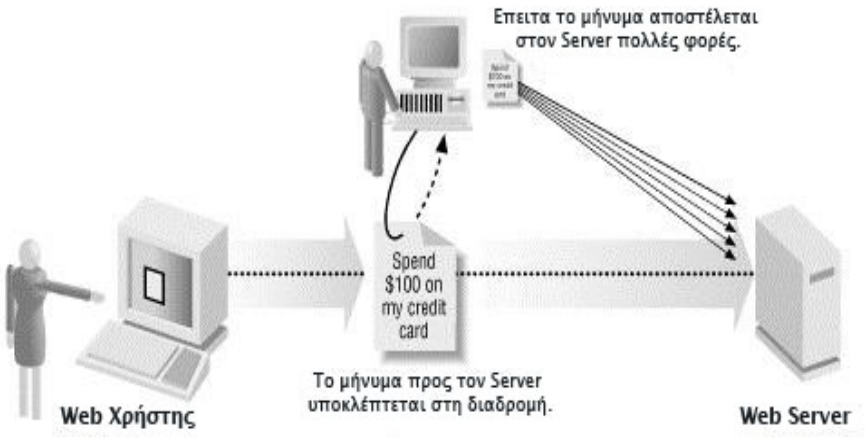


Σχήμα 6.1 Man-in-the-middle επίθεση

Το SSL παρέχει προστασία ενάντια στις "man-in-the-middle" επιθέσεις κάνοντας χρήση ψηφιακών πιστοποιητικών έτσι ώστε να επιτρέψει στον χρήστη του διαδικτύου να μάθει το επικυρωμένο όνομα του διαδικτυακού τόπου. Δυστυχώς, ο Netscape Navigator υποκρύπτει αυτή την πληροφορία, κάνοντας την προσιτή μόνο στους χρήστες που επιλέγουν την εντολή "View Document Info" ("Εμφάνισε τις Πληροφορίες του Αρχείου"). Ένα βελτιωμένο περιβάλλον χρήστη θα εμφάνιζε το επικυρωμένο όνομα του διαδικτυακού τόπου στην "μπάρα τίτλων" (title bar) του web browser, ή σε κάποιο άλλο εμφανή σημείο. Επίσης θα πρέπει να σημειώσουμε ότι το πρωτόκολλο SSL δεν προστατεύει ενάντια στην man-in-the-middle επίθεση όταν χρησιμοποιείται σε κατάσταση "encrypt-only" με κάθε SSL_DH_anon πακέτο κρυπτογράφησης. Αυτό συμβαίνει επειδή σε αυτή τη κατάσταση δεν επιτρέπεται, ούτε στον διακομιστή (server) αλλά ούτε και στον πελάτη (client), να αποδείξουν την γνησιότητα τους ο ένας στον άλλον.

Σε μια replay επίθεση, ο επιτιθέμενος καταγράφει τις επικοινωνίες ανάμεσα στα δύο μέρη και επαναλαμβάνει τα μηνύματα. Για παράδειγμα, ένας επιτιθέμενος ίσως καταγράψει ένα μήνυμα ανάμεσα σε ένα χρήστη και ένα οικονομικό ίδρυμα (τράπεζα) όπου ο πρώτος δίνει την εντολή να πραγματοποιηθεί μια ηλεκτρονική πληρωμή. Επαναλαμβάνοντας αυτό το

μήνυμα, ο επιτιθέμενος μπορεί να προκαλέσει πολλές άλλες ηλεκτρονικές πληρωμές (*Σχήμα 6.2*).



Σχήμα 6.2 Replay επίθεση

6.3.6 Υποστήριξη για συμπίεση

Επειδή τα κρυπτογραφημένα δεδομένα δεν μπορούν να συμπιεστούν, το πρωτόκολλο SSL παρέχει την δυνατότητα της συμπίεσης των δεδομένων του χρήστη πριν αυτά κρυπτογραφηθούν. Το SSL υποστηρίζει πολλούς αλγόριθμους συμπίεσης. Ωστόσο δεν υπάρχει σήμερα κάποια SSL εφαρμογή που να ενσωματώνει την συμπίεση.

ΣΗΜΕΙΩΣΗ

Τα κρυπτογραφημένα δεδομένα δεν μπορούν να συμπιεστούν επειδή μία καλή κρυπτογράφηση αφαιρεί αποτελεσματικά κάθε επανάληψη ή ομοιότητα η οποία έχει αποκομισθεί κατά την διάρκεια της συμπίεσης. Εάν τα κρυπτογραφημένα δεδομένα μπορούν να συμπιεστούν, τότε η κρυπτογράφηση δεν είναι και πολύ καλή.

6.3.7 Συμβατότητα με το SSL 2.0

Οι SSLv3.0 διακομιστές μπορούν να δέχονται συνδέσεις από πελάτες που χρησιμοποιούν SSLv2.0 και να χειρίζονται το μήνυμα αυτόματα χωρίς να υπάρχει ανάγκη να επανασυνδεθεί ο πελάτης.

6.4 Ψηφιακά Πιστοποιητικά

Το SSL κάνει εκτεταμένη χρήση των πιστοποιητικών δημοσίου κλειδιού για την αυθεντικοποίηση τόσο του πελάτη όσο και του διακομιστή στις SSL συναλλαγές. Το SSL κάνει χρήση των X.509 v3 πιστοποιητικών για τον έλεγχο των ζευγών κλειδιού RSA, και ένα τροποποιημένο X.509 πιστοποιητικό για τον έλεγχο δημόσιων κλειδιών που χρησιμοποιούνται από το Fortezza/DMS πρωτόκολλο ανταλλαγής κλειδιών του Υπουργείου Εθνικής Αμύνης των Ηνωμένων Πολιτειών. Τα ψηφιακά πιστοποιητικά εξηγούνται με μεγαλύτερη λεπτομέρεια στις παραγράφους 5.9.4 και 5.11.2.

Το SSL υποστηρίζει τα παρακάτω είδη πιστοποιητικών:

- RSA πιστοποιητικά δημόσιου κλειδιού με δημόσια κλειδιά αυθαίρετου μήκους.
- RSA πιστοποιητικά δημόσιου κλειδιού που περιορίζονται στα 512 bits, για χρήση στα κρυπτογραφικά λογισμικά που πρόκειται να εξαχθούν.
- RSA πιστοποιητικά μόνο για υπογραφή, τα οποία περιέχουν RSA δημόσια κλειδιά που χρησιμοποιούνται μόνο για την υπογραφή δεδομένων, και όχι για κρυπτογράφηση.
- DSS πιστοποιητικά.
- Diffie-Hellman πιστοποιητικά.

Η χρήση των πιστοποιητικών είναι προαιρετική. Το SSL απαιτεί πιστοποιητικά server εκτός αν οι SSL εφαρμογές και του client και του server χρησιμοποιούν το Diffie-Hellman πρωτόκολλο ανταλλαγής κλειδιών. Σήμερα, τα προϊόντα της Netscape δεν εφαρμόζουν τους αλγόριθμους του Diffie-Hellman.

6.5 SSL Εφαρμογές

Το SSL σχεδιάστηκε αρχικά τον Ιούλιο του 1994 και ήταν ένα από τα βασικά επιχειρηματικά πλάνα για την Netscape. Η Netscape σχεδίαζε να δημιουργήσει έναν browser που θα επέτρεπε στον χρήστη να εκτελεί κρυπτογραφημένες επικοινωνίες με τους διακομιστές της Netscape χρησιμοποιώντας ένα πρωτόκολλο δικής της ιδιοκτησίας.

SSL Netscape

Η πρώτη εφαρμογή του SSL ήταν στους browsers και servers της Netscape, που ποτέ δεν πουλήθηκαν ξεχωριστά.

SSLRef

Μετά τον σχηματισμό του Netscape Navigator, η Netscape δημιούργησε μια βοηθητική SSL εφαρμογή η οποία θα διανεμόταν στις Ηνωμένες Πολιτείες. Αυτό το πρόγραμμα γραμμένο σε γλώσσα C, ονομάζεται SSLRef. Η $2^{η}$ έκδοση της βοηθητικής αυτής εφαρμογής δημοσιεύτηκε τον Απρίλιο του 1995.

Ο πηγαίος κώδικας της SSLRef διανέμεται ελεύθερα μέσα στις Ηνωμένες Πολιτείες με μη εμπορικό προσανατολισμό. Όποιος ενδιαφερόταν να χρησιμοποιήσει το SSLRef σε εμπορικές εφαρμογές θα έπρεπε να έρθει σε επαφή με τη Netscape ή τη Consensus.

Η SSLRef εφαρμογή δεν περιέχει κανέναν από τους RC2 και RC4 κρυπτογραφικούς αλγόριθμους. Δυστυχώς, πολλά προγράμματα που χρησιμοποιούν το SSL, όπως είναι ο Netscape Navigator, περιέχουν μόνο τους RC2 και RC4. Κατά συνέπεια, για να συνδυάσεις ένα πρόγραμμα βασισμένο στην SSLRef με ένα πρόγραμμα όπως είναι ο Netscape Navigator, είναι απαραίτητο να χορηγηθούν ξεχωριστές άδειες για τους RC2 και RC4 από την RSA Data Security. Οι αλγόριθμοι αυτοί κατέχουν μία καθιερωμένη θέση στην εργαλειοθήκη του RSA BSAFE.

Η SSLRef εφαρμόζει επίσης τον κρυπτογραφικό αλγόριθμο RSA, ο οποίος πρέπει να έχει άμεσα ή έμμεσα άδεια χρήσης από την RSA Data Security για τις Ηνωμένες Πολιτείες.

SSLeay

Το SSLeay είναι μια ανεξάρτητη εφαρμογή του SSL 3.0 που αναπτύχθηκε από τον Eric Young, έναν προγραμματιστή από την Αυστραλία. Είναι ελεύθερα διαθέσιμη σε όλο τον κόσμο μέσα από έναν μεγάλο αριθμό ανώνυμων FTP ιστοτόπων.

Το SSLeay χρησιμοποιεί εφαρμογές των RC2 και RC4, βασισμένες σε αλγόριθμους που δημοσιεύτηκαν ανώνυμα στο Usenet sci.crypt newsgroup το Σεπτέμβριο του 1994 (RC4) και τον Φεβρουάριο του 1996 (RC2).

Εκτός από τους RC2 και RC4, το SSLeay περιλαμβάνει τους IDEA, DES, και Triple DES κρυπτογραφικούς αλγόριθμους. Ο Eric Young προτείνει ότι οι προγραμματιστές θα πρέπει να χρησιμοποιούν τον Trible DES όταν έχουν τη δυνατότητα να το κάνουν. Επίσης θεωρεί ότι, αντίθετα με τους αλγορίθμους IDEA, RC2 και RC4, ο Triple DES είναι ευρέως αποδεκτός για την ασφάλεια που παρέχει καθώς έχει μελετηθεί για περισσότερα από 20 χρόνια. Τέλος, ισχυρίζεται ότι μπορεί να κρυπτογραφεί με ρυθμούς 410k/sec σε έναν Pentium 100, και 940k/sec σε έναν P6/200, που είναι μια λογική απόδοση. Ο απλός DES μετριέται στα 1160k/sec και 2467k/sec αντίστοιχα και είναι πράγματι αρκετά γρήγορος (56-bit κλειδί).

SSL Java

Υπάρχουν επίσης εφαρμογές του SSL και στην Java. Μερικές από αυτές είναι οι παρακάτω:

- Η **J/SSL** από την Baltimore Technologies είναι μια εφαρμογή κρυπτογραφίας στην Java. Περισσότερα στην διεύθυνση http://www.baltimore.ie/jssl.

- Η **Phaos** έχει αναπτύξει δύο εφαρμογές, την SSLava Toolkit και την JSAFE. Περισσότερα στην διεύθυνση http://phaos.com.

6.6 Επίδοση εκτέλεσης

Το SSL εμφανώς μειώνει την ταχύτητα μετάδοσης της πληροφορίας μέσω του Internet. Η επίδοση της επιβράδυνσης είναι κυρίως αποτέλεσμα της κρυπτογράφησης και αποκρυπτογράφησης δημόσιου κλειδιού που απαιτείται για να αρχικοποιηθεί η πρώτη SSL σύνδεση. Σε σύγκριση με αυτό, η επιπλέον επιβάρυνση που προκαλεί η κρυπτογράφηση και η αποκρυπτογράφηση δεδομένων με τους RC2, RC4, ή τον DES είναι πρακτικά ασήμαντες.

Χρήστες αναφέρουν ότι η απόδοση μειώνεται έως και 50% με την παρουσία του SSL, συγκρινόμενη με την αποστολή πληροφορίας χωρίς την χρήση SSL. Χρήστες υπολογιστών SPARCStation S10 έχουν αναφέρει ότι η κρυπτογράφηση και αποκρυπτογράφηση δημόσιου κλειδιού απαιτεί περίπου τρία CPU δευτερόλεπτα ανά χρήστη με ένα κλειδί των 1024 bits.

Αυτό σημαίνει ότι θα υπάρχει μια παύση τριών δευτερολέπτων ανάμεσα στην έναρξη της σύνδεσης με έναν SSL διακομιστή και στην απόκτηση μιας HTML σελίδας από τον διακομιστή. Επειδή το SSL μπορεί να αποθηκεύει κρυφά το κύριο μυστικό κλειδί (master secret) μεταξύ των δραστηριοτήτων, οι οποίες λαμβάνουν χώρα κατά την αποκατάσταση, διατήρηση και απόλυση μιας σύνδεσης, αυτή η καθυστέρηση επιδρά μόνο στην πρώτη SSL συναλλαγή μεταξύ του πελάτη και του διακομιστή.

Εάν έχουμε έναν γρήγορο υπολογιστή και μια σχετικά αργή σύνδεση στο δίκτυο, η επιβάρυνση του SSL μπορεί να είναι ασήμαντη, ειδικά εάν στέλνουμε μεγάλες ποσότητες πληροφοριών μέσω μιας απλής SSL δραστηριότητας ή μέσω πολλαπλών SSL δραστηριοτήτων που χρησιμοποιούν ένα κοινό κύριο μυστικό κλειδί (master secret).

Από την άλλη πλευρά, εάν απαιτούμε να διενεργήσουμε μεγάλο μέγεθος SSL HTTP αιτήσεων μέσα σε ένα λεπτό, πρέπει να αποφασίσουμε είτε την αγορά ενός εξαιρετικά γρήγορου υπολογιστή είτε την hardware βοήθεια για τις λειτουργίες δημόσιου κλειδιού.

Για να μειώσουν την επίδραση του SSL, πολλοί οργανισμοί μεταδίδουν τις πληροφορίες τους χωρίς να τις κρυπτογραφούν, και χρησιμοποιούν το SSL μόνο για κρυπτογράφηση των ευαίσθητων δεδομένων. Δυστυχώς αυτό περιέχει μια μεγάλη πιθανότητα επίθεσης προς τον χρήστη, επειδή τα μη-κρυπτογραφημένα HTML αρχεία μπορούν να τροποποιηθούν κατά την μετάδοση, καθώς αυτά στέλνονται από τον πελάτη στον διακομιστή, με ένα εξεζητημένο πρόγραμμα φιλτραρίσματος πακέτων και εισαγωγής νέων στοιχείων. (Πτυχιούχοι φοιτητές στο πανεπιστήμιο Berkeley της California έχουν αποδείξει πως ένα πρόγραμμα μπορεί να τροποποιήσει ένα εκτελέσιμο πρόγραμμα το οποίο παραδίδεται άμεσα μέσω ενός δικτύου).

Για παράδειγμα, θα μπορούσε να αλλαχθεί η ετικέτα ενέργειας (action tag) σε μια HTML φόρμα, έτσι ώστε αντί να καταχωρείται ο αριθμός της πιστωτικής κάρτας στο σύστημα επεξεργασίας της συναλλαγής, αντιθέτως, αυτός να καταχωρείται σε έναν πειρατικό υπολογιστή στην Νότια Αμερική. Αν υποθέσουμε ότι ο χειριστής του πειρατικού συστήματος μπορεί να λάβει ένα ψηφιακά υπογεγραμμένο ID για τον δικό του SSL διακομιστή, τότε ίσως είναι πολύ δύσκολο για έναν χρήστη, που εξαπατήθηκε με αυτό το τέχνασμα, να ανακαλύψει ότι ήταν θύμα μιας επίθεσης.

6.7 TLS

Το 1995, η IETF έκανε την πρώτη σκέψη για την υιοθεσία του SSL σαν μέρος ενός νέου προτύπου για τον Internet, το Transport Layer Security (TLS). Ένα προσχέδιο του πρωτοκόλλου δημοσιεύτηκε στης 6 Μαρτίου 1997 από τους Tim Dierks και Christopher Allen στο Consensus Development.

Το TLS είναι πολύ παρόμοιο με το SSL 3.0, με λίγες σημαντικές αλλαγές. Αντί της χρήσης του MD5, το TLS χρησιμοποιεί την HMAC συνάρτηση αποσύνθεσης μηνύματος ασφαλούς κλειδιού. Το TLS επίσης έχει λίγο διαφορετικό τρόπο κρυπτογράφησης από το SSL 3.0.

Βιβλιογραφία

1. Πολλαλής Γιάννης Α., Γιαννακόπουλος Δυνούσης Ι., Παπουτσής Ιωάννης, "Πληροφοριακά Συστήματα Επιχειρήσεων Ι, Εισαγωγή στην Τεχνολογία & Στρατηγική", 2004.
2. Ι. Βασιλείου, "Εισαγωγή στο Ηλεκτρονικό Εμπόριο/Επιχειρείν" (Εθνικό Μετσόβιο Πολυτεχνείο, www.netmode.ntua.gr), 2005.
3. Pete Loshin and John Vacca, “Electronic Commerce, Fourth Edition”, 2004.
4. Μιχάλης Σαλαμπάσης, Χρήστος Γεωργιάδης, Δημήτρης Τεκτονίδης, "ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ μία τεχνολογική προσέγγιση, Τεύχος Α' ", 2005.
5. Σωκράτης Κατσικας, "ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ, Τόμος Β' ", 2001.
6. Froomkin, A. Michael. “Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases“, 2008.
7. Chris Connolly, "Smart Cards: Big Brother's Little Helpers", 1995.
8. Ivona Bezakova, Oleg Pashko, Dinoj Surendran, “Smartcards Survey”, 2000.
9. Wolfgang Rankl & Wolfgang Effing, "Smart Card Handbook, Third Edition", 2002.
10. Information Security Committee, Section of Science & Technology, American Bar Association, "Digital Signature Guidelines", 1996.
11. Simson Garfinkel & Eugene H. Spafford, "Web Security & Commerce, First Edition", 1997.
12. Κ. Βασιλάκης, Σημειώσεις Μαθήματος "ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ", Ακαδημαϊκό έτος 2004-2005.

13. Andrew S. Tanenbaum, “Computer Networks, Fourth Edition”, 2003.
14. Β.Α Κάτος, Γ.Χ. Στεφανίδης, “Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης”, 2003.
15. Microsoft windows server 2003 PKI and Certificate Security 2004.
16. Simson Garfinkel & Eugene H. Spafford, "Web Security & Commerce, First Edition", 1997.

Αναφορές στον Ιστό

1.Πανεπιστημιο Θεσσαλιας

http://www.uth.gr/main/help/help-desk/helpdeskF.html

2. «Εκπαιδευτική Στήριξη του Δικτυωθείτε»

http://www.go-online.gr

3. The University of Texas at Austin

http://misbridge.mccombs.utexas.edu/knowledge/topics/crm/

4. Tech FAQ

http://www.tech-faq.com/ylang/el/erp.shtml

5. Treasury Resourses

http://www.phoenixhecht.com/TreasuryResources/EBPP.html

6. TCMnet, The World's Largest Communications and Technology Community.

www.tmcnet.com/tmcnet/articles/adc0400.htm

7. UC Berkeley School of Information Management and Systems, http://www2.sims.berkeley.edu/courses/is204/f97/GroupE/onepage.html

8. http://en.wikipedia.org

9. http://www.forthnet.gr

10. Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ)

http://www.eett.gr/

11. x5 cryptography FAQ.

http://www.x5.net/faqs/crypto/index.html