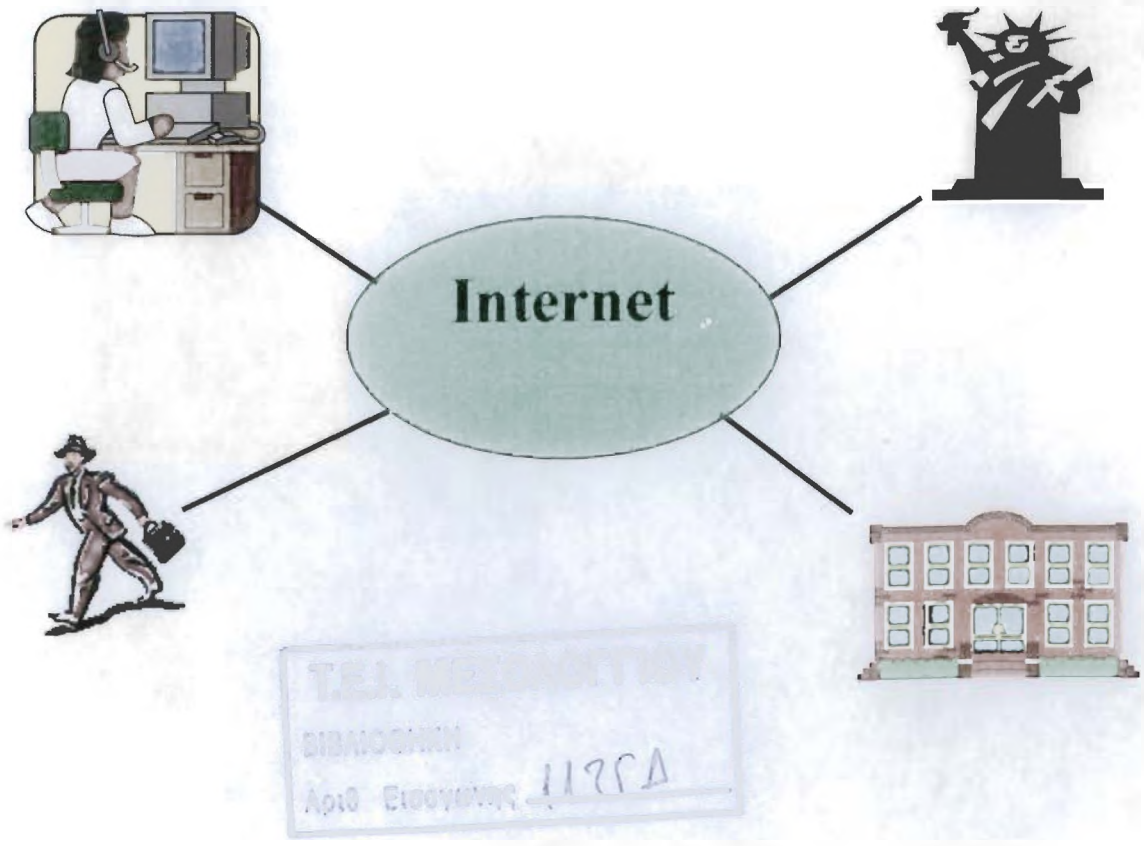
ΑΚΑΔΗΜΑΪΚΟ ΕΤΟΣ:2009-2010

ΣΤΟΙΧΕΙΑ ΦΟΙΤΗΤΗ:
ΜΠΑΡΔΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ του ΒΑΣΙΛΕΙΟΥ
ΑΡΙΘΜΟΣ ΜΗΤΡΩΟΥ:11413

ΣΧΟΛΗ: ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ:ΔΙΟΙΚΗΣΗ ΚΟΙΝΩΝΙΚΩΝ & ΣΥΝΕΤΑΙΡΙΣΤΙΚΩΝ
ΕΠΙΧΕΙΡΗΣΕΩΝ&ΟΡΓΑΝΩΣΕΩΝ ΣΤΟ ΤΕΙ ΜΕΣΟΛΟΓΓΙΟΥ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ:
ΘΕΜΑ: «ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ : ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΛΗΡΩΜΕΣ & ΑΣΦΑΛΕΙΣ ΣΥΝΑΛΛΑΓΕΣ».



ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Η πτυχιακή αυτή εργασία έχει ως κύριο σκοπό, όπως άλλωστε φαίνεται και από τον τίτλο της, την κατανόηση και ανάπτυξη του ηλεκτρονικού εμπορίου μέσα από το παγκόσμιο διαδίκτυο (Internet). Η ραγδαία διάδοση του Διαδικτύου έχει συμβάλλει κατά πολύ στη διαμόρφωση της σύγχρονης κοινωνίας. Τα αποτελέσματα αυτής της διάδοσης τα ζούμε καθημερινά, σε όλους τους τομείς και όχι μόνο σε μια κλειστή ομάδα ανθρώπων που χρησιμοποιούν τους υπολογιστές. Με βάση αυτό ως δεδομένο αναμενόμενο και λογικό ήταν, η εξέλιξη αυτή να επηρεάσει σημαντικά και έναν καθοριστικό τομέα της ζωής μας, που είναι το εμπόριο.

Ηλεκτρονικό εμπόριο είναι η ικανότητα να πραγματοποιούνται συναλλαγές, που σχετίζονται με την ανταλλαγή αγαθών ή υπηρεσιών, μεταξύ δύο ή περισσότερων χρησιμοποιώντας ηλεκτρονικά μέσα, ανεξάρτητα από την γεωγραφική θέση.

Ο στόχος του ηλεκτρονικού εμπορίου είναι να ικανοποιήσει την κοινή επιθυμία των ανθρώπων για καλύτερη ποιότητα αγαθών και υπηρεσιών με στόχο την μεγαλύτερη ταχύτητα εκτέλεσης σε συνδυασμό με το μικρότερο δυνατό κόστος. Συγκεκριμένα η δομή της εργασίας αποτελείται από τρία κεφάλαια.

Στο πρώτο κεφάλαιο θα γίνει μια εισαγωγή στο ηλεκτρονικό εμπόριο, επειδή είναι ένα νέο και εξελίξιμο βήμα στην τεχνολογία των υπολογιστών, ενώ στη συνέχεια θα εξετάσουμε τις αρχές, της κατηγορίες, τα διάφορα προϊόντα που μπορούμε να αγοράσουμε από το διαδίκτυο, τέλος θα αναφέρουμε τα πλεονεκτήματα και τα μειονεκτήματα του.

Στο δεύτερο κεφάλαιο θα μελετήσουμε στους μεθόδους ηλεκτρονικών πληρωμών, ενώ ακολούθως θα εξετάσουμε τον σκοπό της ασφάλειας συναλλαγών, τις απαιτήσεις, της διάφορες τεχνολογίες που χρησιμοποιούνται για να προστατέψουν της συναλλαγές και τα υπολογιστικά συστήματα. Τέλος θα αναφερθούμε σε διάφορα νομικά θέματα του ηλεκτρονικού εμπορίου.

Στο τρίτο κεφάλαιο θα κάνουμε μια αναφορά για την δημιουργία των ηλεκτρονικών καταστημάτων και θα αναφέρουμε μερικούς καταλόγους προϊόντων που μπορούμε να βρούμε στο διαδίκτυο. Τέλος θα κλείσουμε με διάφορες κρατικές πρωτοβουλίες για το ηλεκτρονικό εμπόριο καθώς και μερικά στατιστικά στοιχεία του για την ανάπτυξή του στην Ελλάδα.

Οπότε το κείμενο μας απαντά στην ανάγκη τόσο των ανθρώπων όσο και των επιχειρήσεων να αποδεχτούν την εξέλιξη της τεχνολογίας και να προσπαθούν να την εφαρμόσουν στην καθημερινότητα τους. Κανένας δεν μπορεί να βλέπει με αισιοδοξία τα επιχειρηματικά του σχέδια, αν σε αυτά δεν συμπεριλάβει το ηλεκτρονικό εμπόριο.

ΚΕΦΑΛΑΙΟ 1

ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

1. Ιστορικά στοιχεία

Ιστορικά η ανάπτυξη του ηλεκτρονικού εμπορίου ξεκίνησε τη δεκαετία του 1970 με την εμφάνιση των συστημάτων ηλεκτρονικής μεταφοράς χρηματικών πόρων μεταξύ τραπεζών, που χρησιμοποιούσαν ασφαλή ιδιωτικά δίκτυα, και τα οποία άλλαξαν τη μορφή των χρηματοοικονομικών αγορών.

Στη δεκαετία του 1980 έκαναν την εμφάνισή τους οι τεχνολογίες ηλεκτρονικής επικοινωνίας που βασίζονταν στην αρχιτεκτονική της ανταλλαγής μηνυμάτων (συστήματα EDI και ηλεκτρονικό ταχυδρομείο). Με αυτόν τον τρόπο δραστηριότητες, που παραδοσιακά χρησιμοποιούσαν ως μέσο το χαρτί, μπόρεσαν πλέον να διεκπεραιωθούν ηλεκτρονικά γρηγορότερα και με μικρότερο κόστος.

Στις αρχές της δεκαετίας του 1990 τα δίκτυα ηλεκτρονικής επικοινωνίας και κυρίως το Internet προσφέρουν μια νέα μορφή κοινωνικής επικοινωνίας, με δυνατότητες όπως το ηλεκτρονικό ταχυδρομείο (e-mail), η ηλεκτρονική

συνδιάσκεψη (conferencing), η ηλεκτρονική συνομιλία, οι ομάδες συζήτησης (newsgroups), η ηλεκτρονική μεταφορά αρχείων (FTP), κλπ.

Στη συνέχεια η εμφάνιση του παγκόσμιου ιστού Web, η επικράτηση των προσωπικών ηλεκτρονικών υπολογιστών (PC) και η ευρεία χρήση των λεγόμενων «παραθυρικών» συστημάτων λογισμικού συνετέλεσαν στην ανοδική πορεία του ηλεκτρονικού εμπορίου.

Το ηλεκτρονικό εμπόριο αποτέλεσε έναν φθηνότερο τρόπο για την πραγματοποίηση μεγάλου όγκου συναλλαγών και συγχρόνως επέτρεψε την παράλληλη λειτουργία πολλών διαφορετικών επιχειρηματικών δραστηριοτήτων, επιτρέποντας σε μικρές επιχειρήσεις να ανταγωνιστούν μεγαλύτερες με πολύ ευνοϊκότερες προϋποθέσεις.

Προς το τέλος της δεκαετίας του 1990 η καθιέρωση μεθόδων κρυπτογράφησης του περιεχομένου και εξακρίβωσης της ταυτότητας του αποστολέα ηλεκτρονικών μηνυμάτων, καθώς και η φιλελευθεροποίηση των εθνικών νομοθεσιών σε τομείς εισαγωγών-εξαγωγών και επικοινωνιών, κάνει δυνατή την πραγματοποίηση ασφαλών διεθνών ηλεκτρονικών συναλλαγών.

Οι προβλέψεις για τα επόμενα χρόνια αναφέρουν ότι οι προμήθειες μεταξύ των επιχειρήσεων θα πραγματοποιούνται στο μεγαλύτερο μέρος τους μέσω του Internet και ότι το ηλεκτρονικό εμπόριο λιανικής πώλησης θα αναπτυχθεί ακόμα περισσότερο. Άλλωστε οι εμπορικές συναλλαγές μέσω Internet έφτασαν τα 9 δισεκατομμύρια δολάρια στο τέλος του 2000 και προβλέπεται να πλησιάσουν τα 30 δισεκατομμύρια δολάρια μέχρι το 2005.[1]

1.1 Τι είναι το Ηλεκτρονικό Εμπόριο

Όσον αφορά τον ορισμό του ηλεκτρονικού εμπορίου έχουν δοθεί διαφορετικοί ορισμοί. Ένας ορισμός που έχει δοθεί είναι: «Το ηλεκτρονικό εμπόριο είναι η επικοινωνία και η σύναψη εμπορικών συναλλαγών μεταξύ επιχειρήσεων ή

[1] Συρμακεσης Σ. "Ηλεκτρονικό Εμπόριο", Σελ:

μεταξύ επιχειρήσεων και των πελατών τους, με τη χρήση ηλεκτρονικών μέσων».[1] Ένας αντίστοιχος ορισμός είναι: « Το ηλεκτρονικό εμπόριο καλύπτει οποιαδήποτε μορφή επιχειρηματικής ή διοικητικής συναλλαγής ή ανταλλαγής πληροφοριών, η οποία εκτελείται με τη χρησιμοποίηση οποιασδήποτε τεχνολογίας Πληροφορικής και τηλεπικοινωνιών ».[2]

Όμως αν και ακριβής αυτός ο ορισμός δεν εγκλωβίζει σε καμία περίπτωση το νόημα του ηλεκτρονικού εμπορίου που στην πράξη είναι πιο εύκολα κατανοητό σαν μία από εκείνες τις σπάνιες περιπτώσεις που οι συνεχώς μεταβαλλόμενες ανάγκές μας και οι νέες τεχνολογίες συντάσσονται μαζί για να φέρουν την επανάσταση στον τρόπο με τον οποίο γίνετε το εμπόριο και γενικότερα όλες οι συναλλαγές με απώτερο σκοπό το κέρδος.

Ο τρόπος που γίνονται οι σημερινές εμπορικές διαδικασίες χαρακτηρίζονται από μια συνεχώς αυξανόμενη ικανότητα παροχών, από ένα συνεχώς αυξανόμενο ανταγωνισμό και τέλος από την υπερβολική αύξηση των απαιτήσεων των πελατών. Αποτέλεσμα όλων αυτών είναι οι επιχειρήσεις να αλλάξουν όλη την οργάνωση και τις λειτουργίες τους.

Έτσι καταργούν παλιές ιεραρχικές δομές και εξαλείφουν τους διαχωρισμούς ανάμεσα στα επιμέρους τμήματα τους. Επίσης μειώνουν την απόσταση τους από τους πελάτες και προμηθευτές. Όλες οι διεργασίες σήμερα αναδιαρθρώνονται έτσι ώστε να ξεπερνούν τις παλιές μορφές οργάνωσης. Έτσι βλέπουμε σήμερα πολλές διεργασίες να απλώνονται σε όλα τα τμήματα μίας επιχείρησης, καθώς και διεργασίες που ανήκουν και διεκπεραιώνονται ταυτόχρονα από την εταιρία και τους πελάτες ή προμηθευτές.

1.2 Βασικές αρχές ηλεκτρονικού εμπορίου

[1] Πασχόπουλος Α, Σκαλτσάς Π, "Ηλεκτρονικό Εμπόριο", Σελ.44
[2] Συρμακέσης Σ. . "Ηλεκτρονικό Εμπόριο", Σελ:

Η ανάγκη για Ηλεκτρονικό Εμπόριο προκύπτει από την απαίτηση, των επιχειρήσεων και των κυβερνήσεων, για καλύτερη χρήση της τεχνολογίας των υπολογιστών και των τηλεπικοινωνιών ώστε να βελτιωθούν:

- οι σχέσεις αμφίδρομης επικοινωνίας με τους πελάτες –πολίτες- καταναλωτές,
- οι επιχειρηματικές διεργασίες και η ανταλλαγή πληροφοριών ενδο-επιχειρησιακά.
- η ανταλλαγή πληροφοριών μεταξύ επιχειρήσεων.

Πάντως η ουσιαστική επιδίωξη κάθε επιχείρησης, στον έντονα ανταγωνιστικό επιχειρηματικό στίβο της εποχής μας, είναι η εξασφάλιση στρατηγικού πλεονεκτήματος. Η τεχνολογία και ειδικότερα το Ηλεκτρονικό Εμπόριο παρέχει ευέλικτες και ολοκληρωμένες λύσεις τοποθέτησης των επιχειρήσεων στις επιθυμητές αγορές (target markets), παρεμβαίνοντας ευεργετικά σε κάθε στάδιο της αλυσίδας αξίας τους (value chain).

Το Ηλεκτρονικό Εμπόριο προσφέρει τη δυνατότητα εκτέλεσης πράξεων για την ανταλλαγή προϊόντων ή υπηρεσιών, μεταξύ δυο ή περισσοτέρων μερών, με χρήση ηλεκτρονικών υπολογιστών και δικτύων υπολογιστών. Βασίζεται στην ηλεκτρονική επεξεργασία και μετάδοση δεδομένων, ήχου και εικόνων βίντεο. Η έννοια του Ηλεκτρονικού Εμπορίου περιλαμβάνει πολλές διαφορετικές δραστηριότητες όπως:

- Ηλεκτρονική εμπορία αγαθών και υπηρεσιών.
- Παράδοση ψηφιακού περιεχομένου (άυλων αγαθών).
- Ηλεκτρονική αγοραπωλησία μετοχών.
- Εμπορικές δημοπρασίες.
- Συλλογικές εργασίες σχεδίασης και τεχνικών μελετών.
- Ενημέρωση από πηγές σε απευθείας σύνδεση.
- Κρατικές προμήθειες.
- Πωλήσεις απευθείας στον καταναλωτή και μεταγοραστική εξυπηρέτηση.

Οι εφαρμογές ηλεκτρονικού εμπορίου αφορούν τόσο προϊόντα (π.χ. καταναλωτικά αγαθά) όσο και υπηρεσίες (π.χ. υπηρεσίες πληροφόρησης, χρηματοπιστωτικές και νομικές υπηρεσίες), παραδοσιακές δραστηριότητες (π.χ. ιατρική περίθαλψη, εκπαίδευση) και νέες δραστηριότητες (π.χ. εικονικά πολυκαταστήματα).

Οι τεχνολογίες που χρησιμοποιούνται για τις εφαρμογές του ηλεκτρονικού εμπορίου περιλαμβάνουν όλες τις μορφές ηλεκτρονικών μηνυμάτων, ηλεκτρονικής ανταλλαγής δεδομένων (Electronic Data Interchange, EDI), ηλεκτρονικής μεταφοράς κεφαλαίων (Electronic Funds Transfer, EFT), ηλεκτρονικού ταχυδρομείου (Electronic Mail, E-mail), ηλεκτρονικών καταλόγων, υπηρεσιών ηλεκτρονικού πίνακα ανακοινώσεων (Bulletin Board Services - BBS), κοινών βάσεων δεδομένων και οδηγών, συστημάτων συνεχιζόμενης αγοράς και υποστήριξης για όλο τον κύκλο ζωής των προϊόντων, ηλεκτρονικών ειδήσεων και υπηρεσιών πληροφόρησης, ηλεκτρονικής μισθοδοσίας, ηλεκτρονικών εντύπων, πρόσβασης σε απευθείας σύνδεση σε υπηρεσίες μέσω Internet, καθώς και κάθε άλλη μορφή ηλεκτρονικής μετάδοσης δεδομένων για εμπορικούς σκοπούς. [1]

Το Ηλεκτρονικό Εμπόριο μπορεί να εφαρμοστεί σε μια ευρεία ομάδα επιχειρηματικών λειτουργιών που περιλαμβάνουν:

- **Ανταλλαγή πληροφοριών για προϊόντα και υπηρεσίες** (πριν την πώληση). Η ανταλλαγή πληροφοριών, η διαφήμιση και ενημέρωση για προϊόντα και υπηρεσίες είναι ίσως η πλέον διαδεδομένη χρήση του Ηλεκτρονικού Εμπορίου.
- **Υποστήριξη πελάτη** (πριν και μετά την πώληση).

Πολλές επιχειρήσεις δημιουργούν ομάδες συζητήσεων και επαφών με τους πελάτες τους, οι οποίοι με τον τρόπο αυτό μπορούν να επικοινωνούν όχι μόνο με τον προμηθευτή, αλλά και μεταξύ τους, ανταλλάσσοντας ιδέες, ερωτήσεις, συμβουλές, κ.α.

---

[1] Δουκίδης Γ, Θεμιστοκλέους Μ, Δράκος Β, Παπαζαφειροπούλου Ν, "Ηλεκτρονικό Εμπόριο", Σελ.16,17

- **Δημιουργία ηλεκτρονικών επιχειρήσεων** (virtual enterprises) – **Εμπορικών Κέντρων**.

Το Ηλεκτρονικό Εμπόριο παρέχει τη δυνατότητα δημιουργίας ηλεκτρονικών επιχειρήσεων στο δίκτυο (όπως ηλεκτρονικά καταστήματα, εταιρείες παροχής υπηρεσιών κλπ). Επιπλέον πολλές επιχειρήσεις (κυρίως μικρομεσαίες) δημιουργούν Ηλεκτρονικά Εμπορικά Κέντρα, δηλαδή ομάδες επιχειρήσεων που συνεργάζονται ηλεκτρονικά δημιουργώντας ένα Εμπορικό κέντρο στο Internet. Μια ηλεκτρονική επιχείρηση (virtual enterprise) αποτελείται από δυο ή περισσότερα ηλεκτρονικά καταστήματα και παρέχει τη δυνατότητα στις επιχειρήσεις να δημιουργήσουν ισχυρούς και ανταγωνιστικούς ομίλους εταιρειών.

- **Ηλεκτρονικές Τράπεζες**.

Αρκετές τράπεζες έχουν δημιουργήσει ηλεκτρονικές υπηρεσίες παρέχοντας ένα σύνολο δυνατοτήτων στους πελάτες τους.

- **Ηλεκτρονική διανομή**.

Στα πλαίσια της ηλεκτρονικής διανομής μπορούν να ενταχθούν υπηρεσίες on-line διάχυσης πληροφοριών με μηδαμινό κόστος χρήσης.

- **Ανάπτυξη κοινών επιχειρηματικών διαδικασιών** (shared business processes) μεταξύ επιχειρήσεων.

Τέτοιες διαδικασίες φέρνουν σε στενή επαφή τους συμμετέχοντες στο εμπορικό κύκλωμα, συσφίγγοντας τους επιχειρηματικούς δεσμούς και δυσχεραίνοντας με αυτόν τον τρόπο την αλλαγή συνεργατών (lock-in).

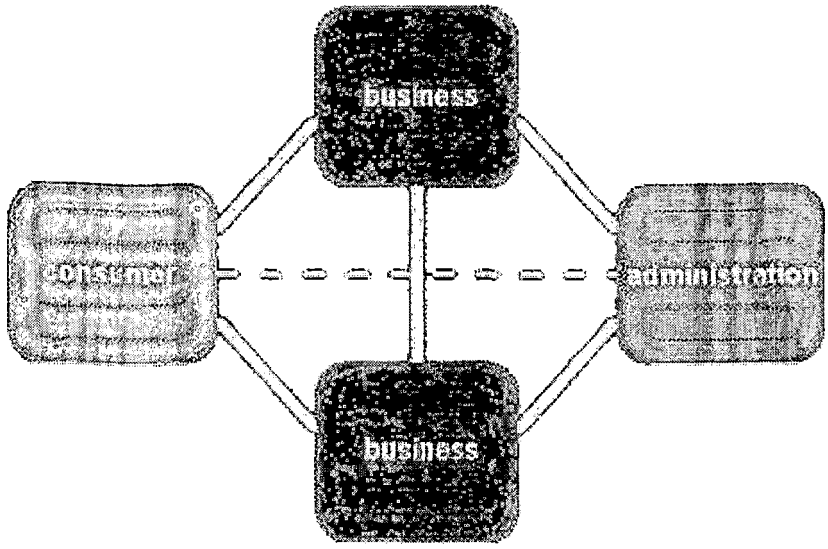
Το κόστος χρήσης ηλεκτρονικής επικοινωνίας δεν είναι το ίδιο για κάθε εφαρμογή και εξαρτάται από μια πληθώρα παραγόντων, όπως η εξοικείωση τ ης επιχείρησης με την πληροφορική, η τυχόν ήδη χρήση δικτύων και ηλεκτρονικών μεθόδων επικοινωνίας, ο αριθμός των συναλλασσομένων εταιρειών, κ.α. Γενικά μια επιχείρηση που χρησιμοποιεί ήδη την πληροφορική σε ικανοποιητικό βαθμό και συναλλάσσεται με άλλους εταίρους που κάνουν το ίδιο, δεν αντιμετωπίζει συνήθως το κόστος επένδυσης για τη χρήση του Ηλεκτρονικού Εμπορίου σαν ανασχετικό παράγοντα. Αντίθετα, μια επιχείρηση που πρέπει να επενδύσει από την αρχή σε όλο τον απαραίτητο εξοπλισμό και τεχνογνωσία και ίσως χρειαστεί να «πριμοδοτήσει» κάποιους μικρούς πελάτες και προμηθευτές να κάνουν το ίδιο, ίσως χρειάζεται να

αντιπαραβάλλει προσεκτικά τα κόστη με τα αναμενόμενα (άμεσα και στρατηγικά) οφέλη.

1.3 Κατηγορίες ηλεκτρονικού εμπορίου

Σε ένα περιβάλλον Ηλεκτρονικού Εμπορίου μπορεί να συμμετάσχουν επιχειρήσεις, δημόσιοι οργανισμοί και καταναλωτές . Στα πλαίσια αυτά οι εφαρμογές του Ηλεκτρονικού Εμπορίου μπορούν να διαχωριστούν στις ακόλουθες τέσσερις κατηγορίες:

- **επιχείρηση - επιχείρηση**
- **επιχείρηση - καταναλωτής**
- **επιχείρηση - δημόσια διοίκηση**
- **καταναλωτής - δημόσια διοίκηση**



Εικόνα 1 Κατηγορίες ηλεκτρονικού εμπορίου

1.3.1 επιχείρηση – επιχείρηση (Business to Business)

Είναι μια επιχείρηση που χρησιμοποιεί ένα δίκτυο για τις παραγγελίες της από προμηθευτές, που λαμβάνει τιμολόγια και κάνει πληρωμές. Απαραίτητη προϋπόθεση για την επιτυχία των εφαρμογών της κατηγορίας αυτής είναι η συνεργασία και ο συντονισμός των επιχειρήσεων . Ένα παράδειγμα εφαρμογής ηλεκτρονικού εμπορίου μεταξύ επιχειρήσεων είναι η χρήση τηλεπικοινωνιακών δικτύων για να διεκπεραιωθούν ηλεκτρονικά καίριες λειτουργίες , όπως η παραγγελία και τιμολόγηση .Αυτή η κατηγορία έχει κατοχυρωθεί αρκετά χρόνια, ειδικά με την χρησιμοποίηση του EDI σε κλειστά ή διεθνή δίκτυα.

1.3.2 επιχείρηση – καταναλωτής(Business to consumer)

Η κατηγορία εφαρμογών επιχείρηση προς καταναλωτή παρουσιάζει αυξανόμενη χρήση σε διεθνές επίπεδο, λόγω της ευρείας χρήσης των δυνατοτήτων του Internet, το οποίο ενδείκνυται για την αποτελεσματική προώθηση προϊόντων και υπηρεσιών σε μεγάλο εύρος πιθανών πελατών.

Οι επιχειρήσεις εκμεταλλευόμενες τα στρατηγικά οφέλη που προσφέρει το ηλεκτρονικό εμπόριο και ειδικότερα η παγκοσμιοποίηση της αγοράς μέσω της οικονομίας του διαδικτύου, δημιουργούν καινοτομικά προϊόντα και υπηρεσίες και τα προωθούν στους καταναλωτές. Έτσι έχει αναπτυχθεί μια ατελείωτη σειρά εφαρμογών που περιλαμβάνει μεταξύ άλλων και τα ακόλουθα:

- Υποστήριξη πελατών
- Ηλεκτρονική δημοσιογραφία (εφημερίδες, περιοδικά)
- Ηλεκτρονική διανομή προϊόντων (πληροφορίες, εφημερίδες, μουσική)
- Διαφήμιση
- Ηλεκτρονικά καταστήματα – ηλεκτρονικές αγορές
- Ηλεκτρονικές πληρωμές
- Ηλεκτρονικές τράπεζες[1]

Οι καταναλωτές ζητούν πάντοτε μεγαλύτερη άνεση και μικρότερες τιμές για τις αγορές τους. Το ηλεκτρονικό εμπόριο προσφέρει αυτή την άνεση με διάφορες μεθόδους, από τη δημοσίευση τιμοκαταλόγων μέχρι την 24-ωρη πρόσβαση σε τραπεζικούς λογαριασμούς, ενώ συγχρόνως εξαλείφει το κόστος της φυσικής παρουσίας για την πραγματοποίηση των ίδιων δραστηριοτήτων με παραδοσιακούς τρόπους. Παράλληλα, το ηλεκτρονικό εμπόριο εξασφαλίζει στους παραγωγούς πολλές διευκολύνσεις, όπως η κατάργηση αρκετών ενδιάμεσων σταδίων στην αλυσίδα παραγωγής, η δυνατότητα συντονισμού των δραστηριοτήτων για τη μείωση του όγκου των αποθεμάτων, και ο περιορισμός του κόστους διανομής, που έμμεσα επιτρέπουν την προσφορά καλύτερων τιμών στους καταναλωτές.

[1] Δουκίδης Γ, Θεμιστοκλέους Μ, Δράκος Β, Παπαζαφειροπούλου Ν, "Ηλεκτρονικό Εμπόριο", Σελ:21

1.3.3 Δημόσιος φορέας - επιχείρηση

Η κατηγορία αυτή καλύπτει όλες τις συναλλαγές μεταξύ επιχειρήσεων και δημόσιων οργανισμών, τόσο τη διεκπεραίωση φορολογικών ή άλλων υποχρεώσεων , όσο και για την αυτοματοποίηση της διαδικασίας των δημοσίων προμηθειών . Οι συναλλαγές των επιχειρήσεων με τους δημόσιους φορείς αφορούν συνήθως τέσσερις περιπτώσεις :

- Φορολογία
- Εισαγωγές – εξαγωγές μέσω τελωνείων
- Δημόσιες προμήθειες
- Προηγμένες ηλεκτρονικές υπηρεσίες (π .χ ηλεκτρονική πληροφόρηση, έκδοση βεβαιώσεων – πιστοποιητικών κ.λ.π)

Σε προηγμένες χώρες όπως οι ΗΠΑ, ο Καναδάς , η Σιγκαπούρη κ.τ.λ. έχει αναπτυχθεί πληθώρα εφαρμογών της μορφής αυτής, επιτυγχάνοντας μείωση των λειτουργικών εξόδων, καλύτερες υπηρεσίες, αποτελεσματικότερο έλεγχο των εσόδων και διαφανή δημόσια διοίκηση. Σύντομα θα τεθούν σε λειτουργία και στη χώρα μας παρόμοιες εφαρμογές όπως για παράδειγμα η ηλεκτρονική υποβολή και διεκπεραίωση των δηλώσεων του ΦΠΑ και δηλώσεων εισοδήματος.

1.3.4 Δημόσιος φορέας προς πολίτες – καταναλωτές

Στις περισσότερες εφαρμογές της μορφής αυτής, οι πολίτες – φορολογούμενοι συναλλάσσονται με τους δημόσιους οργανισμούς χρησιμοποιώντας εφαρμογές ηλεκτρονικού εμπορίου είτε για να ολοκληρώσουν τις φορολογικές τους υποχρεώσεις

, είτε για να προμηθευτούν με τα απαραίτητα πιστοποιητικά ή βεβαιώσεις είτε ακόμη για να εξασφαλίσουν τις απαραίτητες πληροφορίες που χρειάζονται .[1]

1.4 Ηλεκτρονικά Προϊόντα στο Internet

Το *"Internet"* ξεκίνησε σαν ένα διαπανεπιστημιακό δίκτυο υπολογιστικών δικτύων, και εξελίχτηκε σε ένα απαραίτητο εργαλείο της επιστήμης, της επικοινωνίας και των συναλλαγών. Ειδικά μετά τη δημιουργία της γλώσσας *HTML (HyperText Markup Language)* το 1991 και του πρωτοκόλλου *HTTP (HyperText Transfer Protocol)* που επέτρεπε τη διασύνδεση των σελίδων, το *Internet* άλλαξε ριζικά, αφού δημιουργήθηκε το *World Wide Web*, διανθίζοντας τις σελίδες με γραφικά.

Τότε άρχισαν διάφορες εταιρίες να προβάλλουν τις σελίδες τους στο *Internet*, παρουσιάζοντας ένα γενικότερο προφίλ των δραστηριοτήτων τους και τοποθετώντας λίστες με τα προϊόντα τους, τα οποία μπορούσε ο κάθε ενδιαφερόμενος να παραγγείλει. Έτσι γεννήθηκαν αρχικά τα ηλεκτρονικά καταστήματα και κατ' επέκταση το ηλεκτρονικό εμπόριο.

Τα ηλεκτρονικά καταστήματα δεν είναι κατ' ανάγκη υπαρκτά καταστήματα, με την έννοια ότι θα πρέπει να έχουν αποθηκευτικούς χώρους, βιτρίνα και εμπόρευμα. Ένα τέτοιο «εικονικό» κατάστημα είναι δυνατόν να αποτελείται από έναν δικτυωμένο υπολογιστή που περιέχει μια βάση δεδομένων με πληροφορίες για τα προϊόντα που «πουλάει», έτσι ώστε ο κάθε επισκέπτης να μπορεί να βρει κάποιο προϊόν που τον ενδιαφέρει και να το παραγγείλει. Από τη στιγμή που θα γίνει η παραγγελία, αναλαμβάνουν οι διαχειριστές του υπολογιστή να την διεκπεραιώσουν.

Οφείλουμε να σημειώσουμε, ότι στην Ελλάδα οι εφαρμογές του ηλεκτρονικού εμπορίου βρίσκονται σε αρκετά χαμηλότερο επίπεδο από τις αντίστοιχες στις ανεπτυγμένες Ευρωπαϊκές χώρες, ενώ απέχουν ακόμα περισσότερο από αυτές των ΗΠΑ.

---

[1] Δουκίδης Γ, Θεμιστοκλέους Μ, Δράκος Β, Παπαζαφειροπούλου Ν, "Ηλεκτρονικό Εμπόριο", Σελ:20

Κατατάσσουμε τις ηλεκτρονικές συναλλαγές στις παρακάτω κατηγορίες:

1. **Πώληση ηλεκτρονικών προϊόντων, όπου συμπεριλαμβάνονται:**

   - Αντικείμενα εύκολα στη μεταφορά τους, όπως βιβλία, CDs, γυαλιά, υπολογιστές και οτιδήποτε άλλο που κατασκευάζεται.

   - Προϊόντα των οποίων η αποστολή είναι δυνατό να γίνει ηλεκτρονικά, όπως προγράμματα και διάφορα προϊόντα λογισμικού.

2. **Υπηρεσίες με την ευρύτερη εκδοχή της έννοιας, όπως:**

   - παροχή πληροφοριών μέσω συνδρομής,
   - αγορές αεροπορικών εισιτηρίων,
   - κρατήσεις ξενοδοχειακών κλινών,
   - ενοικίαση αυτοκινήτων,
   - άλλες ανάλογες υπηρεσίες.

1.5 Στοιχεία που περιλαμβάνει το Ηλεκτρονικό Εμπόριο

Το ηλεκτρονικό εμπόριο, σαν έννοια, δεν περιλαμβάνει μόνο τη διεξαγωγή ηλεκτρονικών αγορών, αλλά χαρακτηρίζεται από μια ποικιλία λειτουργιών που προσφέρει. Αυτές αναφέρονται παρακάτω:

- Εγκαθίδρυση μιας αρχικής επαφής, π.χ. μεταξύ του πελάτη και του καταστήματος

- Ανταλλαγή πληροφοριών και εγγράφων με ασφάλεια με τη χρήση π.χ. του EDI

- Υποστήριξη του πελάτη πριν και μετά τις πωλήσεις, όπως:
  - Προβολή των προϊόντων μέσα από ηλεκτρονικούς καταλόγους
  - Πληροφορίες για τα προϊόντα ή τις υπηρεσίες
  - Τεχνική υποστήριξη για τη χρήση των προϊόντων
  - Απαντήσεις σε ερωτήσεις των καταναλωτών

- Πωλήσεις

- Ηλεκτρονικές πληρωμές

- Διανομές, οι οποίες περιλαμβάνουν:
  - Τη συνεργασία με μεταφορικές εταιρίες για την αποστολή προϊόντων
  - Την ηλεκτρονική αποστολή αγαθών που μπορούν να σταλούν μέσω δικτύου

1.6 Πλεονεκτήματα – Μειονεκτήματα ηλεκτρονικού εμπορίου

Το ηλεκτρονικό εμπόριο λειτουργεί θετικά τόσο για τις επιχειρήσεις όσο και για τους καταναλωτές στους οποίους προσφέρει μεγάλες ευκολίες.

Τα βασικά πλεονεκτήματα είναι:

- **Διευρυμένη αγορά**

Τα όρια του ηλεκτρονικού εμπορίου δεν περιορίζονται από τα αντίστοιχα γεωγραφικά ή εθνικά όρια, που στην πραγματικότητα περιορίζουν την εμβέλεια των επιχειρήσεων. Έτσι επιτρέπεται ακόμα και στις μικρότερες επιχειρήσεις να πετύχουν μια σφαιρική παρουσίαση των προϊόντων τους, να συναγωνιστούν «επί ίσοις όροις» άλλες επιχειρήσεις άσχετα με το μέγεθός τους και να εδραιωθούν σε παγκόσμιο επίπεδο, αποκτώντας ένα αγοραστικό κοινό οποιασδήποτε εθνικότητας. Είναι

προφανές ότι η ηλεκτρονική προβολή των καταστημάτων αποτελεί τον καλύτερο ίσως τρόπο διαφήμισής τους.

Το αντίστοιχο όφελος του καταναλωτή είναι ότι μπορεί να διαλέξει αυτό που τον ενδιαφέρει από διάφορους προμηθευτές, χωρίς να τον απασχολεί η γεωγραφική θέση της επιχείρησης. Η παγκόσμια αγορά συνδέεται ηλεκτρονικά και δημιουργείται με τον τρόπο αυτό μια κατάσταση πολυπωλίου, με αποτέλεσμα να μπορεί ο χρήστης να βρει μια πολύ συμφέρουσα προσφορά σε ελάχιστο χρόνο.

Λόγω του πολυπωλίου που δημιουργείται, κάθε επιχείρηση, μικρή ή μεγάλη, πρέπει να ακολουθήσει τις νέες εξελίξεις, αυτές που ορίζουν οι ηλεκτρονικές συναλλαγές, προκειμένου να παραμείνει ανταγωνιστική.

- **Αυξημένος ανταγωνισμός**

Λόγω της κατάστασης παντοπωλείου ο ανταγωνισμός αυξάνεται και η κάθε επιχείρηση προσπαθεί να κερδίσει τους πελάτες, βελτιώνοντας όχι μόνο την ποιότητα των προϊόντων, αλλά και έναν αριθμό άλλων πραγμάτων που προσελκύουν τον καταναλωτή. Έτσι, δίνεται έμφαση στην παρουσίαση των προϊόντων, στις πληροφορίες που παρέχονται γι' αυτά, στις οδηγίες χρήσης, στην ικανοποίηση των απαιτήσεων του πελάτη και στην καλύτερη και γρηγορότερη εξυπηρέτησή του.

Συμπερασματικά, αν μια εταιρία επιθυμεί να διατηρήσει και να αυξήσει το αγοραστικό της κοινό πρέπει να προσέξει έτσι ώστε η προβολή των προϊόντων της να γίνεται μέσα από ένα εύχρηστο, ευχάριστο, έμπιστο και λειτουργικό περιβάλλον.

- **Μείωση κόστους προϊόντων – Μείωση τιμών**

Ένα από τα μεγαλύτερα οφέλη του ηλεκτρονικού εμπορίου είναι η μείωση του κόστους συναλλαγής. Η μείωση των τιμών είναι ένα έμμεσο αποτέλεσμα του χαμηλότερου κόστους συναλλαγής. Σύμφωνα με τη θεωρία του κόστους συναλλαγών, για κάθε δραστηριότητα της αλυσίδας αξιών μια επιχείρηση πρέπει να αποφασίσει αν θα την αναθέσει σε εξωτερικό προμηθευτή ή αν θα την εκτελέσει η ίδια. Το κριτήριο της απόφασης αυτής είναι το σχετικό κόστος των δυο επιλογών. Το ηλεκτρονικό

εμπόριο επιτρέπει την απλοποίηση και την αυτοματοποίηση πολλών δραστηριοτήτων, ιδίως αυτών που αφορούν την επικοινωνία με πελάτες ή προμηθευτές. Έτσι, ο συνολικός κύκλος από τη σχεδίαση του προϊόντος ως την παράδοση στον τελικό καταναλωτή απλοποιείται, πολλά στάδια που περιλάμβαναν τη χρήση ενδιαμέσων καταργούνται ή ενοποιούνται, και το κόστος παραγωγής και διάθεσης των προϊόντων μειώνεται.[1]

- **Μείωση προμηθευτικών αλυσίδων – Ταχύτατη ανταπόκριση στον πελάτη**

Το ηλεκτρονικό εμπόριο προκαλεί τη μείωση έως και τον εκμηδενισμό των προμηθευτικών αλυσίδων, αφού σε αρκετές περιπτώσεις τα προϊόντα στέλνονται κατευθείαν από τον παραγωγό στον καταναλωτή, προσπερνώντας τα παραδοσιακά «στάδια» από τα οποία περνάει κάποιο προϊόν μέχρι να παραδοθεί στον παραλήπτη. Ειδικά στα προϊόντα που παραδίδονται ηλεκτρονικά, η αλυσίδα εκμηδενίζεται. Ο πελάτης επωφελείται από το ότι βρίσκει αυτό που θέλει, σε λίγο χρόνο, απ' ευθείας από τον προμηθευτή, χωρίς να περιορίζεται στα προϊόντα των τοπικών καταστημάτων που βρίσκονται σε stock.

- **Δημιουργία προφίλ καταναλωτών, Μαζική παραγωγή προϊόντων - Προϊόντα και υπηρεσίες προσωπικής επιλογής για τους καταναλωτές**

Μέσω της ηλεκτρονικής επικοινωνίας είναι δυνατό τα καταστήματα να συγκεντρώσουν πληροφορίες για τις ιδιαίτερες ανάγκες και επιθυμίες μεμονωμένα κάθε πελάτη πάνω σε ορισμένα προϊόντα. Δημιουργούν έτσι το προφίλ του κάθε καταναλωτή χωριστά και μπορούν κατ' επέκταση να προσαρμόζουν τις ιστοσελίδες τους ανάλογα με τις ιδιαίτερες «προτιμήσεις» του πελάτη. Με τον τρόπο αυτό, καταργείται το «απρόσωπο» των συναλλαγών που χαρακτηρίζει το ηλεκτρονικό εμπόριο και δημιουργείται για τον καταναλωτή ένα περιβάλλον οικείο, στο οποίο αισθάνεται την άνεση και την ασφάλεια για να διεκπεραιώσει τις συναλλαγές του.

---

[1] Συρμακέσης Σ. . "Ηλεκτρονικό Εμπόριο", Σελ:

Επιπλέον, το κάθε κατάστημα, συγκεντρώνοντας τις ιδιαίτερες προτιμήσεις των καταναλωτών, μπορεί να καταλήξει σε κάποια συμπεράσματα, που αφορούν σε ένα σύνολο αναγκών τους, οι οποίες δεν καλύπτονται από την αγορά. Αυτό θα έχει σαν αποτέλεσμα τη μαζική παραγωγή ειδικών προϊόντων που θα καλύπτουν τις ανάγκες του καταναλωτικού κοινού και που θα προσφέρονται σε μαζικές τιμές αγοράς, χωρίς δηλαδή κάποια επιπλέον επιβάρυνση.

Τα βασικά μειονεκτήματα είναι:

- **Προβλήματα ασφαλείας**

Το διαδίκτυο είναι ένα μέσο που δεν παρέχει το επιθυμητό επίπεδο ασφάλειας στις συναλλαγές, με αποτέλεσμα και οι συναλλαγές να μην ασφαλείς. Βέβαια σε αυτόν τον τομέα γίνεται εκτεταμένη έρευνα έτσι ώστε οι συναλλαγές να γίνονται με όσο το δυνατόν μεγαλύτερη ασφάλεια. Βέβαια για να μην είμαστε υπερβολικοί, τα ηλεκτρονικά συστήματα πληρωμών που εφαρμόζονται, έχουν λύσει τα μεγαλύτερα προβλήματα ασφάλειας και μπορεί κανείς να πει ότι είναι εξίσου, αν όχι περισσότερο, ασφαλή και ευέλικτα από τις παραδοσιακές μεθόδους πληρωμών.

- **Έλλειψη επαφής πωλητή – πελάτη**

Το φαινόμενο αυτό δημιουργεί δυσπιστία στον καταναλωτή αφού δεν βλέπει το προϊόν και τον πωλητή. Δεν είναι σίγουρος αν αυτό που βλέπει στην οθόνη είναι όντως αυτό που θα παραλάβει, ή αν αυτά που ισχυρίζεται η εταιρία για το προϊόν είναι όντως αληθινά.

- **Δυσκολία της χρήσης πολύπλοκων ηλεκτρονικών συστημάτων πληροφορικής**

Η εκθετική αύξηση της ποσότητας των πληροφοριών που είναι διαθέσιμες μέσα από τη ψηφιακή υποδομή, κάνει διαρκώς δυσκολότερο το διαχωρισμό και την ανεύρεση συγκεκριμένων πληροφοριών. Οι χρήστες επιθυμούν να μπορούν να βρουν

πληροφορίες με την ελάχιστη δυνατή προσπάθεια, αλλά συχνά δεν διαθέτουν τα εργαλεία και τις γνώσεις που απαιτούνται για μια αποτελεσματική αναζήτηση. Οι επιχειρήσεις που επιθυμούν να στηρίξουν τις δραστηριότητές τους πάνω στη ψηφιακή υποδομή αντιμετωπίζουν δυσκολίες στην επιλογή του κατάλληλου εξοπλισμού Η/Υ και λογισμικού, κάτι που όχι σπάνια οφείλεται στην απουσία ή στη συνεχή αλλαγή των προδιαγραφών.

- **Δυσκολία εκτίμησης των πλεονεκτημάτων έναντι του κόστους των νέων εφαρμογών**

Πολλές επιχειρήσεις εμφανίζονται αρνητικές ή διστακτικές όταν εξετάζουν τις δυνατότητες επέκτασής τους, και λαμβάνουν υπόψη μόνο το άμεσο κόστος και τα άμεσα πλεονεκτήματα, αποτυγχάνοντας να δουν τα μακροπρόθεσμα οφέλη. Το κόστος της απαιτούμενης επένδυσης είναι γενικά ευδιάκριτο, αλλά τα πλεονεκτήματα μπορεί να απαιτούν ένα πιο μακροπρόθεσμο ορίζοντα. Έτσι είναι δυσκολότερο να εκτιμηθούν, και κατά συνέπεια είναι δύσκολο να δικαιολογηθεί η αρχική επένδυση.[1]

[1] Συρμακέσης Σ. . "Ηλεκτρονικό Εμπόριο", Σελ:

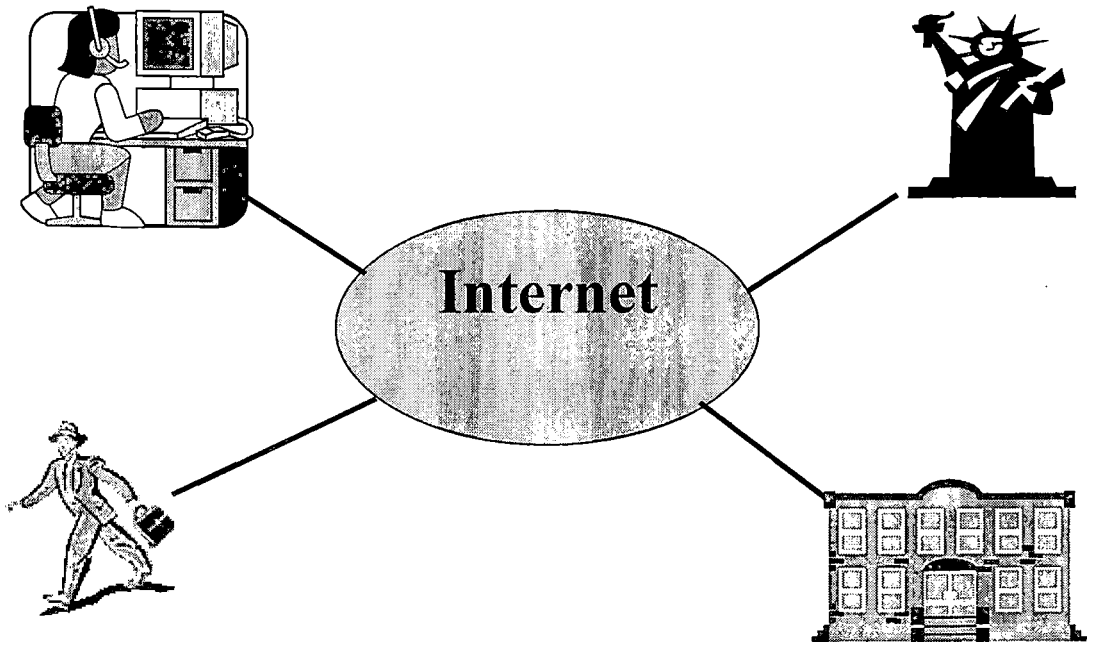
ΚΕΦΑΛΑΙΟ 2

ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΛΗΡΩΜΕΣ ΚΑΙ ΑΣΦΑΛΕΙΑ ΣΥΝΑΛΛΑΓΩΝ

2.1 Μέθοδοι πληρωμής

Η συνεχώς αυξανόμενη εμπορευματοποίηση του Internet, και η χρήση του WEB έχουν ωθήσει τις επιχειρήσεις στην εύρεση μεθόδων και συστημάτων πληρωμών για την υποστήριξη του Ηλεκτρονικού Εμπορίου. Η πρακτική εφαρμογή του Ηλεκτρονικού Εμπορίου στο σύγχρονο επιχειρηματικό περιβάλλον απαιτεί την ύπαρξη συστημάτων πληρωμών μέσω των οποίων θα διεκπεραιώνονται ηλεκτρονικά οι οφειλές των εμπλεκομένων μερών. Ήδη έχουν υιοθετηθεί διάφορα συστήματα ηλεκτρονικών πληρωμών. Οι κυριότεροι είναι οι εξής:

- Πιστωτικές κάρτες, κάρτες χρέωσης, κάρτες αγορών.
- Ηλεκτρονικές επιταγές.
- ψηφιακά μετρητά.



2.1.1 Πιστωτικές κάρτες

Σε μια παραδοσιακή συναλλαγή με πιστωτική κάρτα ο προμηθευτής καταγράφει τα στοιχεία της πιστωτικής κάρτας του πελάτη δημιουργώντας ένα έγγραφο συναλλαγής. Το εν λόγω έγγραφο υπογράφεται από τον αγοραστή και προωθείται στη συνέχεια στη τράπεζα για διεκπεραίωση. Στο τέλος η τράπεζα χρεοπιστώνει τους αντίστοιχους λογαριασμούς ενημερώνοντας τα εμπλεκόμενα μέρη για τη συναλλαγή που έγινε.

Σε ένα μηχανισμό ηλεκτρονικής πληρωμής με χρήση πιστωτικής κάρτας, ακολουθείται περίπου το ίδιο σενάριο με αυτό της προηγούμενης

παραγράφου. Επιπλέον το σενάριο εμπλουτίζεται με μηχανισμούς ασφαλείας, όπως έλεγχος ταυτότητας πελάτη και εμπόρου. Το γεγονός αυτό έχει δημιουργήσει μια ποικιλία συστημάτων ηλεκτρονικών πληρωμών με πιστωτικές κάρτες. Δυο από τα χαρακτηριστικά που προσδιορίζουν και διαφοροποιούν τα συστήματα αυτά, είναι το επίπεδο της ασφάλειας των συναλλαγών, και το λογισμικό που απαιτείται από όλα τα εμπλεκόμενα μέλη, αγοραστής, προμηθευτής, τράπεζα.

Κατά τη διάρκεια μιας συναλλαγής τα στοιχεία της πιστωτικής κάρτας ενός αγοραστή μπορούν να μεταφερθούν με δυο τρόπους. Ο πρώτος τρόπος θεωρείται μη ασφαλής και υποστηρίζει την αποστολή των στοιχείων της ηλεκτρονικής πληρωμής από τον πελάτη στον έμπορο σε μη κρυπτογραφημένη μορφή. Η μέθοδος αυτή κρίνεται ως μη ασφαλής διότι κατά την μεταβίβαση των στοιχείων μπορεί να παρέμβει κάποιος εισβολέας και να τροποποιήσει τα στοιχεία της συναλλαγής ή ακόμη και να τα υποκλέψει. Ο δεύτερος τρόπος θεωρείται πιο ασφαλής και προβλέπει την κρυπτογράφηση όλων των πληροφοριών που σχετίζονται με τη πληρωμή πριν την αποστολή τους στον έμπορο ή στην τράπεζα μέσω του Internet. Για την αποφυγή της παρεμβολής κάποιου τρίτου κατά τη διεξαγωγή των συναλλαγών μεταξύ του πελάτη και του εμπόρου, μια καλή επιλογή αποτελεί εκείνος ο συνδυασμός web browser και web server που θα υποστηρίζει το πρωτόκολλο, Secure Sockets Layer (SSL).

Η χρησιμοποίηση web servers και web browsers που υποστηρίζουν το πρωτόκολλο SSL, εξασφαλίζει την προστασία των δεδομένων από κάποιο τρίτο. Δεν εγγυάται όμως ότι τα δεδομένα αυτά δεν θα χρησιμοποιηθούν σκόπιμα από τον ίδιο τον έμπορο. Για την αποφυγή εξαπάτησης του πελάτη από τον έμπορο (χρήση των στοιχείων της πιστωτικής κάρτας από τον έμπορο για την διεξαγωγή μη εξουσιοδοτημένων αγορών), θα μπορούσε να χρησιμοποιηθεί ένας ανεξάρτητος φορέας διασφάλισης των συναλλαγών γνωστός ως Έμπιστη Τρίτη Οντότητα (ΕΤΟ). Μια ΕΤΟ μεσολαβεί ανεξάρτητα στη όλη διαδικασία αποκρυπτογραφώντας τα στοιχεία της πιστωτικής κάρτας επικυρώνοντας τη συναλλαγή.

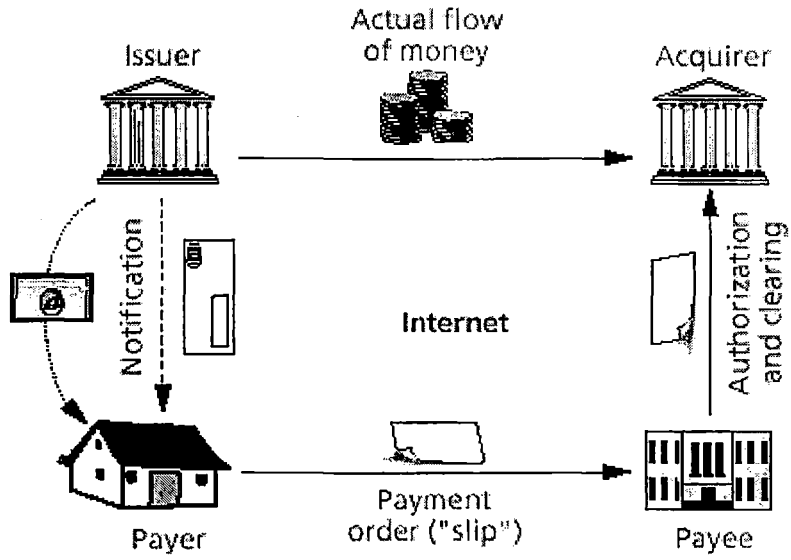
Σε αρκετές περιπτώσεις εταιρείες που παράγουν συστήματα ηλεκτρονικών πληρωμών όπως η Microsoft – VISA και Nestcape – Verifone χρησιμοποιούν μηχανισμούς με τους οποίους παρέχουν υπηρεσίες ΕΤΟ. Οι μηχανισμοί αυτοί

μεταφέρουν τον κρυπτογραφημένο αριθμό της πιστωτικής κάρτας από τον έμπορο στον δικό τους επεξεργαστή για τον έλεγχο της αυθεντικότητας και την έγκριση της συναλλαγής.

Σε αυτή την περίπτωση η ηλεκτρονική ολοκλήρωση των συναλλαγών παρουσιάζει το εξής πλεονέκτημα έναντι του παραδοσιακού τρόπου πληρωμής με πιστωτική κάρτα. Κρυπτογραφώντας τα στοιχεία της πιστωτικής κάρτας και με την μεσολάβηση μιας Τρίτης Εμπιστευτικής Οντότητας, όπως η επεξεργασία των στοιχείων αυτών δεν γίνεται από τον έμπορο, οπότε και εξαλείφεται ο κίνδυνος απάτης από την πλευρά του τελευταίου.

Θα πρέπει να σημειωθεί ότι παρά την πρόοδο που έχει σημειωθεί στα συστήματα πληρωμών με χρήση πιστωτικών καρτών, εξακολουθούν να υπάρχουν ακόμη ορισμένα προβλήματα. Το σημαντικότερο πρόβλημα που εξακολουθεί να υφίσταται ακόμη είναι η τυποποίηση. Θα πρέπει να υιοθετηθεί ένα κοινά αποδεκτό πρότυπο διεκπεραίωσης των ηλεκτρονικών συναλλαγών στο Internet, που θα επιτρέπει την επικοινωνία μεταξύ των διαφορετικών τύπων λογισμικού των συναλλασσομένων μερών. Η εξασφάλιση ή όχι της διαλειτουργικότητας θα καθορίσει και την μελλοντική πορεία των ηλεκτρονικών συστημάτων πληρωμών μέσω πιστωτικής κάρτας.[1]

[1] Δουκίδης Γ, Θεμιστοκλέους Μ, Δράκος Β, Παπαζαφειροπούλου Ν, "Ηλεκτρονικό Εμπόριο",Σελ.198



Η ροή στο Check-like σύστημα

2.1.2 Ηλεκτρονικές επιταγές

Οι ηλεκτρονικές επιταγές είναι ουσιαστικά μια εντολή μεταφοράς κεφαλαίων από ένα λογαριασμό σε ένα άλλο. Η εντολή αποστέλνεται αρχικά στον αποδέκτη των κεφαλαίων, ο οποίος την υπογράφει με τη σειρά του και την προωθεί στη τράπεζα προκειμένου να λάβει το αντίστοιχο ποσό.

Οι ηλεκτρονικές επιταγές έχουν πολλές ομοιότητες με τις συμβατές επιταγές, ενώ χρησιμοποιούν ψηφιακές υπογραφές για την έκδοση ή την οπισθογράφηση, και απαιτούν ψηφιακά πιστοποιητικά για την ταυτότητα του πληρωτή, της τράπεζας και του τραπεζικού λογαριασμού.

Από άποψη ασφάλειας η ηλεκτρονική επιταγή θεωρείται καλύτερη από την έντυπη επιταγή. Ο αποστολέας μπορεί να προστατεύσει τον εαυτό του από απάτη. Αυτό επιτυγχάνεται με την κωδικοποίηση του αριθμού του λογαριασμού του με το

δημόσιο κλειδί της τράπεζας και με αυτόν τον τρόπο δεν αποκαλύπτει τον αριθμό του λογαριασμού του στον έμπορο.

Μια ηλεκτρονική επιταγή μπορεί να παραδοθεί είτε με άμεση παράδοση μέσω ενός δικτύου ή μέσω ηλεκτρονικού ταχυδρομείου. Οι ηλεκτρονικές γίνονται δεκτές από τράπεζες και εξοφλούνται μέσα από υπάρχοντες τραπεζικούς μηχανισμούς.

Το FSTC αποτελεί μια συνεργασία τραπεζών και πιστωτικών οργανισμών, που έχουν υλοποιήσει μια ηλεκτρονική επιταγή. Στηριγμένη στην παραδοσιακή επιταγή η επιταγή του FSTC επιτρέπει την ψηφιακή υπογραφή του αποδέκτη. Για την προσθήκη μεγαλύτερης ευελιξίας σε αυτό το σύστημα των πληρωμών, το FSTC προσφέρει στους χρήστες διάφορες επιλογές επιταγών ανάλογα με τις ανάγκες του χρήστη. Η σύνδεση της υπάρχουσας τραπεζικής υποδομής με τα δημόσια δίκτυα θα διευκολύνει τη συνεργασία τραπεζών, επιχειρήσεων και πελατών και θα κάνει πιο δυνατή την εξάπλωση της χρήσης ηλεκτρικών επιταγών.[1]

Οι υποστηρικτές του συστήματος των ηλεκτρονικών επιταγών πιστεύουν ότι θα ευνοήσει την ανάπτυξη των ηλεκτρονικών συναλλαγών για τους εξής λόγους:

- Θα επιτρέψει την αμφίδρομή επικοινωνία, π.χ. ο αποδέκτης θα μπορεί να επικοινωνήσει με την τράπεζα του εκδότη και να επιβεβαιώσει την κάλυψη της επιταγής.
- Θα βελτιώσει την ασφάλεια σε όλα τα βήματα της συναλλαγής, μέσα από τον έλεγχο της ηλεκτρονικής υπογραφής των δύο μερών και της τράπεζας.
- Θα διευκολύνει τη σύνδεση των πληρωμών με τα ήδη χρησιμοποιούμενα συστήματα EDI.

[1] Δουκίδης Γ, Θεμιστοκλέους Μ, Δράκος Β, Παπαζαφειροπούλου Ν, "Ηλεκτρονικό Εμπόριο", Σελ,200

2.1.3 Έξυπνες κάρτες (Smarts Cards)

Με τις έξυπνες κάρτες έγινε το πραγματικό πέρασμα από το πλαστικό χρήμα στο ηλεκτρονικό χρήμα. Οι έξυπνες κάρτες (smart cards) είναι οι κάρτες που μοιάζουν αρκετά με τις πιστωτικές και ως προς την εμφάνιση και ως προς τον τρόπο χρήσης τους. Γενικά η Έξυπνη κάρτα είναι μια πλαστική κάρτα που έχει ενσωματωμένο ένα μικροτσίπ το οποίο περιέχει πληροφορίες όπως προσωπικά στοιχεία, αριθμούς πιστωτικών καρτών, κλειδιά κρυπτογράφησης, οικονομικά στοιχεία κ.α. Μπορεί να αποθηκεύσει πάνω από 100 φορές μεγαλύτερο όγκο πληροφοριών από ότι μια πιστωτική κάρτα, παρέχοντας παράλληλα μεγαλύτερη ασφάλεια. Για παράδειγμα, σε μια συνηθισμένη πιστωτική κάρτα φαίνεται καθαρά ο αριθμός με το μάτι. Σε μια έξυπνή κάρτα απαιτείται ένας κωδικός για το ξεκλείδωμα των κρυπτογραφημένων πληροφοριών που παρέχει και δεν υπάρχει κανένας εμφανίσιμος αριθμός, ούτε κάποια υπογραφή του κατόχου την οποία μπορεί να πλαστογραφήσει κάποιος απατεώνας.

Υπάρχουν δυο κατηγορίες έξυπνων καρτών:

1. Στην έξυπνη κάρτα με επαφή

Για να γίνει η ανάγνωση και ενημέρωση των πληροφοριών στο ενσωματωμένο μικροτσίπ, απαιτείται η τοποθέτηση της σε ένα ειδικό μηχάνημα ανάγνωσης. Για παράδειγμα μπορεί να χρησιμοποιηθεί σε ειδικά τερματικά φια την πληρωμή των τηλεφωνικών λογαριασμών.

2. Στην κάρτα χωρίς επαφή

Υπάρχει επιπλέον μια ενσωματωμένη σπειροειδής κεραία που δίνει τη δυνατότητα απομακρυσμένης μετάδοσης των πληροφοριών. Για παράδειγμα μπορεί να χρησιμοποιηθεί όταν ένας οδηγός περνάει από τα διόδια. Έτσι δεν απαιτείται η στάση και η πιθανή καθυστέρηση του οδηγού εκεί, καθώς η χρέωση γίνεται αυτόματα.[1]

Η Εθνική Τράπεζα έχει θέσει σε πιλοτική εφαρμογή τις Έξυπνες κάρτες ,σε δυο υπηρεσίες της. Στα κεντρικά γραφεία της Εθνοκάρτας στην Αθήνα και στην περιφερειακή διοίκηση Θεσσαλονίκης, οι εργαζόμενοι μπορούν να πληρώνουν στα κυλικεία των υπηρεσιών αυτών με τον τρόπο αυτόν. Οι Έξυπνες Κάρτες αποτελούν ένα νέο τομέα αγοράς για τις τράπεζες, σε σημεία που δεν έχει πρόσβαση η πιστωτική κάρτα, είτε επειδή αυτό είναι τεχνικά αδύνατο, είτε είναι οικονομικά ασύμφορο , αφού το κόστος των καρτών δεν δικαιολογεί τόσο μικρές συναλλαγές (από 0,05€)

Όμως για να γίνουν πραγματικότητα οι Έξυπνες Κάρτες, πρέπει να γίνουνε δυο απαραίτητα βήματα:

- Απαιτούνται επενδύσεις αρκετών χιλιάδων ευρώ, ώστε να δημιουργηθούν σημεία συναλλαγής. Αυτό πρακτικά σημαίνει ότι πρέπει ένα πλήθος επιχειρήσεων, από περίπτερα μέχρι βενζινάδικα, να εφοδιαστούν με μηχανήματα EFT/POS ώστε να μπορούν να πραγματοποιούνται οι συναλλαγές. Σύμφωνα με τα όσα ισχύουν τώρα, οι συναλλαγές θα

[1] Πομπόρτσης Α., Τσούλφας Α, "Εισαγωγή στο Ηλεκτρονικό Εμπόριο", Σελ:192

πραγματοποιούνται με τον ίδιο τρόπο, δηλαδή ο περιπτεράς δεν θα εκδίδει ταυτόχρονα και απόδειξη ,απλά θα πληρώνει με ηλεκτρονικό τρόπο.

- Το προϊόν να γίνει κερδοφόρο για τις τράπεζες γεγονός που απαιτεί σωστό σχεδιασμό, ώστε να είναι ελκυστικό για τους καταναλωτές, τις επιχειρήσεις και παράλληλα προσοδοφόρο για τις τράπεζες.

Οι τελευταίες μέσα από τις smart cards θα κερδίσουν μικρή προμήθεια από την συναλλαγή και φυσικά από την εκμετάλλευση της προείσπραξης. Αυτός ο τόπος πληρωμής είναι ήδη διαδεδομένος στις υπόλοιπες χώρες τις Ευρωπαϊκής Ένωσης. Για να μπουν στην τσέπη μας οι Έξυπνες Κάρτες , χρειάζεται να περάσουν σε δύο στάδια:

- Να παραχθούν οι Έξυπνες Κάρτες (των οποίων το κόστος είναι μεγαλύτερο από αυτό των μαγνητικών πιστωτικών καρτών) και τα τερματικά , που θα τις δέχονται. Υιοθέτηση της τεχνολογικής πλατφόρμας στην τεχνολογία Έξυπνων Καρτών, που θα είναι ενιαία για όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης και η οποία θα εφαρμόζεται από τις τράπεζες και τις επιχειρήσεις.

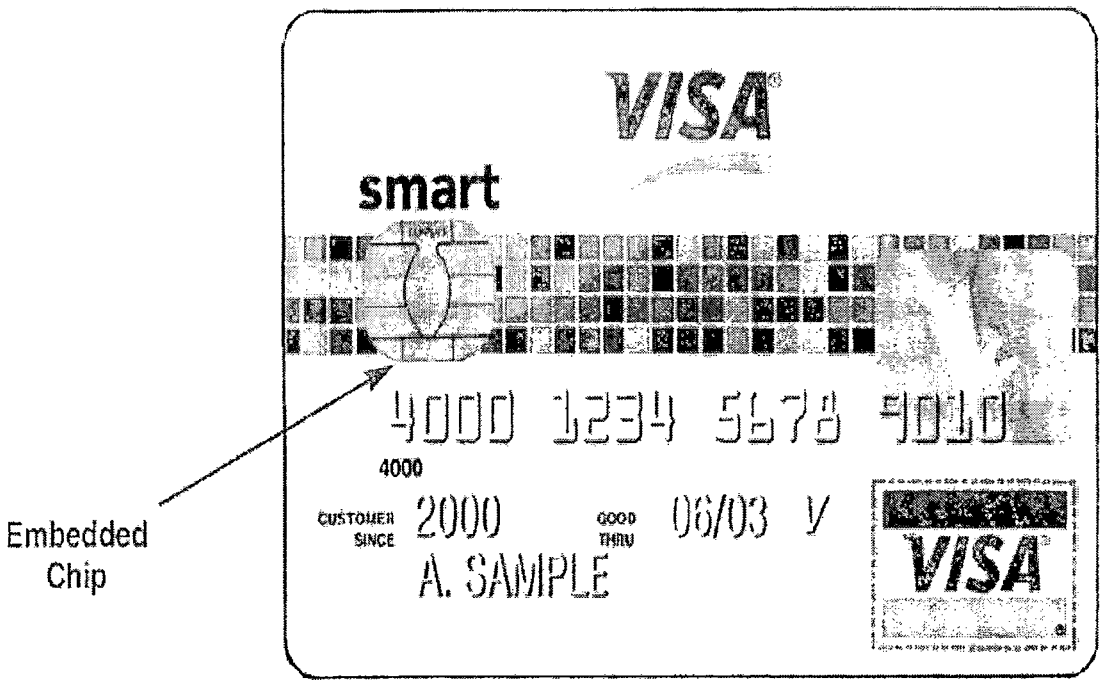
- Οι επιχειρήσεις θα εφοδιαστούν με μηχανάκια και θα συνάψουν τις συμβάσεις με τις τράπεζες για να μπορούν οι καταναλωτές να χρησιμοποιούν τις Έξυπνες Κάρτες. Τα μηχανάκια θα έχουν διπλή οθόνη. Ο καταναλωτής θα περνάει την κάρτα στην ειδική υποδοχή του μηχανήματος και θα έχει μπροστά του δύο πλήκτρα με τις ενδείξεις ΝΑΙ και ΟΧΙ. Ο έμπορος θα πληκτρολογεί το ποσό, το οποίο θα βλέπει και ο συναλλασσόμενο. Για να ολοκληρωθεί η συναλλαγή, θα πρέπει να πατήσει το πλήκτρο ΝΑΙ.

Σύμφωνα με τις προδιαγραφές της αγοράς, ο χρόνος συναλλαγής δεν θα ξεπερνά τα 3΄΄ και αυτός είναι ο λόγος που τα τερματικά έχουν διπλή οθόνη. Σε περίπτωση κλοπής η απώλειας, ο καταναλωτής χάνει το ποσό που υπάρχει μέσα στη

Κάρτα. Το πόσο αυτό, αν για την συναλλαγή απαιτείται PIN δεν μπορεί να το καρπωθεί τρίτος.

Η κάρτα θα γεμίζει από την τράπεζα και είναι απαραίτητη η ύπαρξη ενός τραπεζικού λογαριασμού. Ο καταναλωτής θα παίρνει ένα ποσό από το τραπεζικό του λογαριασμό από 30 Ευρώ και πάνω και το πιστώνει στη συνέχεια στην Έξυπνη Κάρτα.

Exhibit 13.4 Smart Card Image



Source: Courtesy of Visa USA, Inc..

Τα πλεονεκτήματα από την υιοθέτηση της νέας τεχνολογίας:

- Για τις εκδότριες τράπεζες:

  - Μείωση του κόστους και μεγαλύτερη ασφάλεια.
  - Προοπτική νέων εσόδων.
  - Κέρδη από την αξιοποίηση του αχρησιμοποίητου ποσού που βρίσκεται μέσα στην κάρτα.
  - Μείωση της απάτης.

- Για τους εμπόρους:

    - Μείωση μετρητών προς φύλαξη, λιγότερος κίνδυνος κλοπής .
    - Μεγαλύτερη ταχύτητα εξυπηρέτησης.
    - Προοπτική αύξησης των πωλήσεων.
    - Σημαντική μείωση του κόστους τηλεπικοινωνιών.

- Για τους καταναλωτές:

    - Άνεση και ευκολία στις συναλλαγές τους.
    - Εξάλειψη της ανάγκης μετρητών
    - Καλύτερος έλεγχος προϋπολογισμού.
    - Μεγαλύτερη ταχύτητα εξυπηρέτησης.
    - Επιπλέον, μπορούν όλοι, ανεξαρτήτως ηλικίας ή οικονομικής κατάστασης να αποκτήσουν την κάρτα, χωρίς χρονοβόρες διαδικασίες. Η εύκολη απόκτηση και από αλλοδαπούς τουρίστες για όσο διάστημα θα βρίσκονται στη χώρα μας.

- Τέλος, η κάρτα αυτή δεν θα λειτουργεί ανταγωνιστικά ως προς τις άλλες κάρτες, αλλά θα αποτελεί συμπλήρωμα τους.

Οι έξυπνες κάρτες διευκολύνουν στη μεταφορά των στοιχείων του κατόχου τους, ώστε να μπορούν να χρησιμοποιούνται και από άλλους υπολογιστές στο σπίτι, στο γραφείο ή σε άλλους χώρους που είναι συνδεδεμένοι με το Διαδύκτιο. Είναι μια τεχνολογία που δείχνει να έχει μεγάλη προοπτική εξέλιξης.

2.1.4 Ψηφιακό χρήμα (digital cash ή e-cash)

Το ψηφιακό χρήμα είναι ένας μηχανισμός εξοφλήσεις μικροποσών μέσω του Internet. Σε ένα σύστημα ψηφιακού χρήματος, το νόμισμα δεν είναι τίποτα άλλο παρά μια σειρά από ψηφία. Συστήματα όπως τα Digicash και Net Cash επιτρέπουν στο πελάτη να καταθέσει μετρητά σε έναν τραπεζικό λογαριασμό και μετά να χρησιμοποιήσει τα μετρητά για να αγοράσει αντικείμενα στο Διαδίκτυο. Οι πελάτες λαμβάνουν έναν κωδικοποιημένο αριθμό 64-bit για κάθε νόμισμα των 5 σεντς που μετατρέπουν σε ηλεκτρονικά μετρητά, τα οποία στη συνέχεια μεταφέρονται στο σκληρό δίσκο του χρήστη. Κατόπιν , ο πελάτης μπορεί να μεταφέρει τα μετρητά σε πωλητές στο Διαδίκτυο (αρκεί ο πωλητής να δέχεται αυτή τη μέθοδο πληρωμής). Ο πωλητής μετά επιστρέφει τα ηλεκτρονικά μετρητά στην τράπεζα ανταλλάσσοντας τα με πραγματικά χρήματα.

Η τράπεζα για να διασφαλίσει ότι μια χρηματο-ροή (token) χρησιμοποιείται μόνο μια φορά, καταγράφει τον σειριακό αριθμό κάθε token που ξοδεύεται. Αν ο σειριακός αριθμός του token υπάρχει ήδη στη βάση δεδομένων, τότε η τράπεζα έχει εντοπίσει κάποιον που προσπάθησε να χρησιμοποιήσει το περισσότερες από μια φορές το token και θα ενημερώσει τον έμπορο ότι αυτή η χρηματική μονάδα είναι άκυρη.

Μια εναλλακτική λύση που προτάθηκε από την DigiCash επιτρέπει στους χρήστες να διατηρήσουν την ανωνυμία τους. Αυτός ο μηχανισμός ονομάζεται blind signature και επιτρέπει στον αγοραστή να λάβει ηλεκτρονικό χρήμα από μια τράπεζα χωρίς η τράπεζα να μπορεί να συσχετίσει το όνομα του αγοραστή με τα tokens που του διανέμει. Η τράπεζα πρέπει να εκτιμήσει το token που λαμβάνει από τον έμπορο, μέσω της ψηφιακής στάμπας που έχει αρχικά τοποθετήσει στα tokens του χρήστη αλλά δεν μπορεί να καταλάβει ποιος έκανε την πληρωμή.[1]

[1] Δουκίδης Γ, Θεμιστοκλέους Μ, Δράκος Β, Παπαζαφειροπούλου Ν, "Ηλεκτρονικό Εμπόριο", Σελ. 201

Από τεχνική άποψη, τα ψηφιακά μετρητά βασίζονται στις ψηφιακές υπογραφές. Μια τράπεζα διανέμει σε όλους τους πελάτες της (εμπόρους και καταναλωτές) το δημόσιο κλειδί της, ώστε να μπορούν να αποκωδικοποιήσουν οποιαδήποτε ψηφιακή πληροφορία έχει κρυπτογραφηθεί με το μυστικό κλειδί της τράπεζας. Έτσι, η δυνατότητα αποκρυπτογράφησης αποτελεί αναμφισβήτητη απόδειξη της γνησιότητας των πληροφοριών(της προέλευσης τους απευθείας από την τράπεζα). Τις δυο τελευταίες δεκαετίες η τεχνολογία των ψηφιακών υπογραφών έχει γίνει απόλυτα ασφαλής, όσον αφορά της μαθηματικές βάσεις των αλγόριθμών που χρησιμοποιούνται , και στην πράξη έχει αποδειχθεί ότι είναι πολύ ευκολότερο να πλαστικοποιηθούν χειρόγραφες υπογραφές ή ακόμη και χαρτονομίσματα, παρά ψηφιακές υπογραφές. Τα ψηφιακά μετρητά μπορούν να αποθηκεύονται σε μια μαγνητική κάρτα. Η διαδικασία θα είναι παρόμοια με την ανάληψη μετρητών από μια αυτόματη ταμειακή μηχανή, μόνο που αντί να δίνει μετρητά η μηχανή θα αποθηκεύει το ποσό με ηλεκτρονικό τρόπο πάνω στην ίδια την κάρτα. Αν ο καταναλωτής δεν έχει τραπεζικό λογαριασμό θα μπορεί να ΄΄φορτώσει΄΄ την κάρτα του πληρώνοντας στο ταμείο της τράπεζας συμβατά μετρητά, που αμέσως θα μεταφέρονται σε ψηφιακή μορφή στην κάρτα του.

Στη συσκευή είσπραξής του πωλητή, θα υπάρχει λογισμικό που θα μπορεί να αφαιρεί το ποσό της πληρωμής από την κάρτα του πελάτη και να το αποθηκεύσει σε μια αντίστοιχη κάρτα του καταστήματος. Κάθε κάρτα μετρητών θα μπορεί να χρησιμοποιηθεί ανώνυμα χωρίς την ανάγκη μετάδοσης αριθμών πιστωτικών καρτών ή έγκρισης από οποιοδήποτε οργανισμό. Ο κάτοχος θα μπορεί να χρησιμοποιήσει τα ψηφιακά μετρητά σε κάθε κατάστημα, εισάγοντας απλά την κάρτα στη συσκευή είσπραξης του καταστήματος.

Πλεονεκτήματα του συστήματος:

- Ασφάλεια των προσωπικών δεδομένων:

Τα ηλεκτρονικά μετρητά δεν μπορούν να ανιχνευθούν. Η τράπεζα δεν συνδέει τα νούμερα με ένα συγκεκριμένο άτομο κι έτσι είναι αδύνατο να συνδεθεί η πληρωμή με αυτόν που πληρώνει. Ο πελάτης δεν χρειάζεται να ανησυχεί ότι θα προστεθεί σε

μια σειρά από ταχυδρομικές λίστες, εκτός εάν έχει παραγγείλει εμπόρευμα το οποίο πρέπει να αποσταλεί στο σπίτι του αντί για πληροφορίες που μπορούν να αποσταλούν μέσω διαδικτύου.

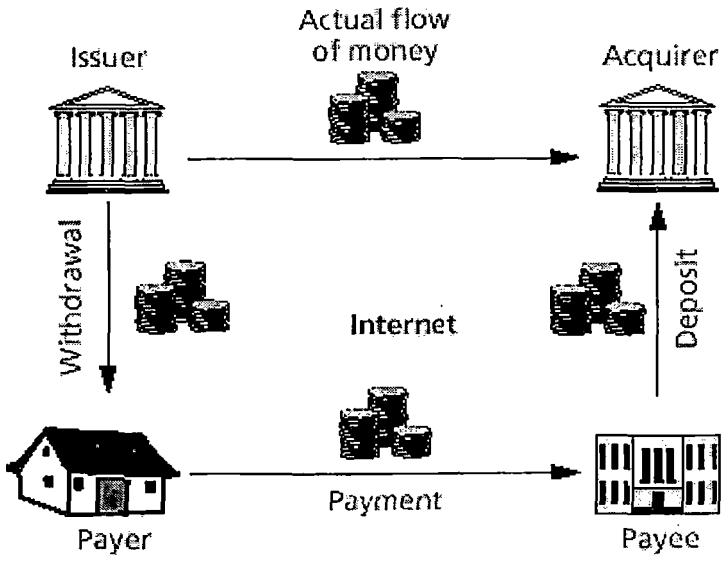
- Περιορισμένη ευθύνη:

Ο πελάτης μπορεί να χάσει μόνο όσα χρήματα μεταφέρει. Ο κόσμος προτιμά περισσότερο να χειρίζεται ηλεκτρονικά μετρητά και να διακινδυνεύει τα 20 δολάρια στο ΄΄ηλεκτρονικό πορτοφόλι΄΄ παρά να διακινδυνεύει των 5.000 δολαρίων αριθμό της χρυσής κάρτας του στο δίκτυο.

Μειονεκτήματα του συστήματος:

- Τα ψηφιακά χρήματα δεν είναι απόλυτα εξασφαλισμένη μέθοδος:

Εάν καταρρεύσει ρεύσει ο σκληρός δίσκός του Η/Υ, η ηλεκτρονική τράπεζα καταστρέφεται. Επιπλέον, εάν χάκερ αποκωδικοποιήσουν τους αριθμούς των ψηφιακών μετρητών, δεν υπάρχει τρόπος να ανακτηθούν τα χαμένα μετρητά (σαν να πετούσατε ένα χαρτονόμισμα στο δρόμο και να το χάνατε).
Από τη στιγμή που η τράπεζα δεν συνδέει τα χρήματα με το όνομα του πελάτη, δεν υπάρχει τρόπος να τον αποζημιώσει. Ωστόσο, τα ηλεκτρονικά μετρητά Digicash μπορούν να ανακτηθούν στην περίπτωση κατάρρευσης του σκληρού δίσκου. Τότε ο πελάτης θα πρέπει να εγκαταλείψει την ανωνυμία του, ώστε η τράπεζα να αντικαταστήσει τα ηλεκτρονικά μετρητά του.



Η ροή του χρήματος στο e-cash σύστημα

2.1.5 Κυβερνοπληρωμές (cyber-payment ή on-line payments)

Στις μέρες μας πλέον έχουμε φτάσει στο σημείο να είναι διαδεδομένες και οι **κυβερνοπληρωμές**. Αυτού του είδους οι συναλλαγές επιτυγχάνονται πάλι με τη χρήση πιστωτικών καρτών, αλλά εμπλέκουν, πέρα από τον έμπορο, τον πελάτη και την τράπεζα του εμπόρου και το δίκτυο επεξεργασίας της κάρτας.

Η διαδικασία έχει ως εξής. Ο έμπορος ανοίγει έναν επιχειρηματικό λογαριασμό σε κάποια τράπεζα (Acquiring Bank) από τον οποίο θα εξαρτηθεί και το ποιες κάρτες θα γίνονται δεκτές στις συναλλαγές του. Ο πελάτης χρησιμοποιεί την κάρτα του για την αγορά που ενδιαφέρεται να κάνει και δίνει τα στοιχεία της στον έμπορο με κρυπτογραφημένη αποστολή μέσω του Internet. Ο έμπορος, αφού λάβει τα στοιχεία της κάρτας του πελάτη μέσω του δικτύου επεξεργασίας καρτών (Card Processing Network), επιβεβαιώνει την πιστοληπτική ικανότητα του πελάτη από την τράπεζα που έχει εκδώσει την κάρτα (Issuing Bank), και στη συνέχεια εκτελεί την παραγγελία. Το δίκτυο επεξεργασίας καρτών ολοκληρώνει τη συναλλαγή μεταξύ της

τράπεζας του πελάτη (Issuing Bank) και της τράπεζας του εμπόρου (Acquiring Bank). Αυτού του είδους οι συναλλαγές μπορούν να είναι άμεσες ή ομαδικές. Στην πρώτη περίπτωση, ο server που λαμβάνει την πληροφορία της πιστωτικής κάρτας του πελάτη και την παραγγελία του, προωθεί άμεσα την πληροφορία αυτή στο δίκτυο επεξεργασίας καρτών το οποίο με τη σειρά του ζητεί και παίρνει επιβεβαίωση από την τράπεζα του πελάτη το αργότερο μέσα σε είκοσι τέσσερις ώρες. Ο τελικός διακανονισμός μεταξύ της τράπεζας του πελάτη και του εμπόρου γίνεται σε επόμενο χρόνο. Στη δεύτερη περίπτωση, ο server του εμπόρου λειτουργεί ως βάση καταγραφής παραγγελιών και στοιχείων πιστωτικών καρτών, που σε επόμενο στάδιο επεξεργάζονται ομαδικά μέσω των τραπεζών των πελατών. Για αυτή την ομαδική εξέταση μπορεί να μην χρησιμοποιηθεί δίκτυο επεξεργασίας καρτών, μπορεί να γίνει και με τον παραδοσιακό τρόπο από πλευράς εμπόρου.[1]

2.1.6 Με μεσολάβηση τρίτου φορέα

Μία εναλλακτική λύση, κυρίως ως προς τα προβλήματα που εμφανίζονται στη χρήση πιστωτικών καρτών στο Διαδίκτυο, αποτελεί η ύπαρξη ενός μεσολαβητή. Πρόκειται για εταιρίες που σκοπό έχουν την πιστοποίηση των ηλεκτρονικών στοιχείων τόσο του πελάτη όσο και του καταστήματος. Με τον τρόπο αυτό μπορούν να εγγυηθούν την αξιοπιστία των εμπλεκόμενων στη συναλλαγή μερών, απαλλάσσοντας έτσι αμφότερους από την επίπονη διαδικασία πιστοποίησης της αυθεντικότητας της συναλλαγής. Οι εταιρίες αυτές αμείβονται με ένα ποσοστό επί των πωλήσεων του ηλεκτρονικού καταστήματος. Η πιστοποίηση της αυθεντικότητας επιτυγχάνεται με τη χρήση ειδικού λογισμικού, το οποίο ως επί το πλείστον παρέχεται δωρεάν.

Παρά τη ύπαρξη αρκετά ισχυρών συστημάτων πληρωμών με πιστωτικές κάρτες, θα πρέπει να αναπτυχθεί κάποιο κοινό πρότυπο που να επιτρέπει στα συστήματα

[1] WWW.Google.gr

πληρωμών να μπορούν να επικοινωνήσουν μεταξύ τους. Η έλλειψη διαλειτουργικότητας που παρατηρείται σήμερα ίσως να ελαττώσει την αποδοχή των συστημάτων ηλεκτρονικών πληρωμών.

Υπάρχουν ήδη δυο σημαντικά πρότυπα υπό ανάπτυξη, τα οποία θα καταστήσουν τη διαλειτουργικότητα αυτών των συστημάτων πιο εύκολη. Το πρώτο είναι το Secure Electronic Transactions (SET), που αναπτύχθηκε από την Visa και την Mastercard. Το SET χρησιμοποιεί τα λεγόμενα ψηφιακά πιστοποιητικά για την πιστοποίηση της ταυτότητας των συμμετεχόντων στη συναλλαγή. Επίσης, κρυπτογραφεί τις πληροφορίες των πιστωτικών καρτών πριν την μετάδοσή τους στο Internet. Το δεύτερο πρότυπο αφορά το Joint Payments Initiative (JEPI), που αναπτύχθηκε από την CommerceNet και το World Wide Web Consortium. Το JEPI αποτελεί μια προσπάθεια για τυποποίηση των διαφορετικών μηχανισμών πληρωμών, πρωτοκόλλων και μεταφοράς. Τέτοια παραδείγματα μηχανισμών περιλαμβάνουν:

- Πιστωτικές κάρτες
- Χρεωστικές κάρτες
- Ψηφιακό χρήμα και
- Ηλεκτρονικές επιταγές.[1]

2.1.7 Παραδοσιακοί τρόποι συναλλαγών

Τα συστήματα ηλεκτρονικών πληρωμών βρίσκονται, όπως αναφέρθηκε, σε πρώιμο στάδιο, με αποτέλεσμα οι πελάτες να εμφανίζονται δύσπιστοι απέναντί τους. Για το λόγο αυτό, πολλά ηλεκτρονικά καταστήματα παρέχουν στους πελάτες τους δυνατότητα εξόφλησης των αγορών τους και με παραδοσιακούς τρόπους, θέλοντας παράλληλα να προσελκύσουν και κοινό που δεν είναι κάτοχοι πιστωτικών καρτών. Έτσι, στους τρόπους διεκπεραίωσης συναλλαγών που

[1] Δουκίδης Γ, Θεμιστοκλέους Μ, Δράκος Β, Παπαζαφειροπούλου Ν, "Ηλεκτρονικό Εμπόριο", Σελ. 201

συναντάμε στο ηλεκτρονικό εμπόριο, μπορούμε να προσθέσουμε και τους παρακάτω:

α) Με αντικαταβολή. Η εταιρία στέλνει το προϊόν με το ταχυδρομείο ή με κούριερ και ο πελάτης καλείται να εξοφλήσει με την παράδοση.

β) Με ταχυδρομική επιταγή. Ο πελάτης καλείται να αποστείλει ταχυδρομική επιταγή κατάλληλου ποσού προκειμένου να εξοφλήσει την αγορά.

γ) Με κατάθεση στον τραπεζικό λογαριασμό του καταστήματος. Ο πελάτης καταθέτει το αντίστοιχο ποσό στο λογαριασμό της επιχείρησης και επιδεικνύει την απόδειξη κατάθεσης.

δ) Παραπομπή στο πλησιέστερο κατάστημα. Ο πελάτης πρέπει να πάει σε κάποιο υποκατάστημα της επιχείρησης προκειμένου να επικυρώσει και να ολοκληρώσει την αγορά.

2.2 Ασφάλεια συναλλαγών

2.2.1 Ο σκοπός της ασφάλειας

Η ραγδαία διάδοση του Διαδικτύου (Internet) προσέφερε στις επιχειρήσεις αλλά και στους καταναλωτές μια μοναδική ευκαιρία επικοινωνίας τόσο σε εθνικό όσο και σε παγκόσμιο επίπεδο. Το χαμηλό κόστος, η εύκολη πρόσβαση, η γρήγορη και συνεχής ενημέρωση, είναι μόνο μερικοί από τους παράγοντες που βοήθησαν στην ανάπτυξη του ηλεκτρονικού εμπορίου. Ωστόσο, από πολύ νωρίς φάνηκαν και τα προβλήματα τα οποία συνδέονται με το ηλεκτρονικό εμπόριο και τα οποία πρέπει να αντιμετωπισθούν αποτελεσματικά για την περαιτέρω εξέλιξή του. Ο πιο σημαντικός φραγμός για την υιοθέτηση του ηλεκτρονικού εμπορίου είναι η ασφάλεια των συναλλαγών.

Ο δισταγμός των περισσότερων επιχειρήσεων αλλά και των καταναλωτών οφείλεται κυρίως στην ανησυχία για την ασφάλεια του δικτύου αλλά και των συναλλαγών που πραγματοποιούνται μέσα σε αυτό. Υπάρχουν πολλές περιπτώσεις καταστροφής δεδομένων, εξαπάτησης ή κλοπής χρημάτων, παραποίησης εγγράφων, υποκλοπής προσωπικών ή οικονομικών πληροφοριών (π.χ. αριθμοί πιστωτικών καρτών), κλπ.

Με απλά λόγια ασφάλεια στο ηλεκτρονικό εμπόριο σημαίνει να μπορεί για παράδειγμα ο καταναλωτής να δώσει άφοβα τα στοιχεία της πιστωτικής του κάρτας σε μια συναλλαγή στο διαδίκτυο, χωρίς να υποκλαπούν ή να στείλει ένα e-mail χωρίς να μετατραπούν τα περιεχόμενά του μέχρι να φτάσει στον τελικό προορισμό του. Επίσης να ξέρει ότι μια συγκεκριμένη ιστοσελίδα που επισκέπτεται ανήκει στη συγκεκριμένη εταιρεία και ότι τα προσωπικά στοιχεία που δίνει σε μια συναλλαγή δεν θα δημοσιευτούν στο Διαδίκτυο.

Οι κυριότερες απειλές και επιθέσεις στις οποίες οι εμπορικές δραστηριότητες σε δικτυωμένα περιβάλλοντα μπορεί να είναι ευάλωτες φαίνονται στην ακόλουθη λίστα:

- Πρόσβαση χωρίς εξουσιοδότηση σε δικτυακούς πόρους.
- Καταστροφή πληροφοριών και δικτυακών πόρων.
- Μεταβολή, είσοδος και μετατροπή πληροφοριών.
- Αποκάλυψη πληροφοριών σε μη εξουσιοδοτημένα άτομα.
- Πρόκληση διάρρηξης και διακοπής δικτυακών υπηρεσιών.
- Κλοπή πληροφοριών και δικτυακών πόρων.
- Άρνηση λήψης υπηρεσιών και άρνηση αποστολής ή λήψης πληροφοριών.
- Ισχυρισμός κατοχής υπηρεσιών χωρίς άδεια.
- Αποκάλυψη προς τρίτους κατά τη διάρκεια της συναλλαγής εμπιστευτικών στοιχείων (όπως ο αριθμός της πιστωτικής κάρτας στην οποία χρεώνεται μία συναλλαγή, το πλήθος των αντικειμένων που παραγγέλλονται, κλπ.).

Για τους παραπάνω λόγους η ασφάλεια ενός συστήματος ηλεκτρονικού εμπορίου αποτελεί πρωταρχική προϋπόθεση για την επιτυχή λειτουργία του, αφού τα δεδομένα που ανταλλάσσονται στις διάφορες επιχειρηματικές δραστηριότητες είναι ιδιαίτερα ευαίσθητα (π.χ. οικονομικές συναλλαγές).

Οι εφαρμογές και οι τεχνολογίες ηλεκτρονικού εμπορίου πρέπει να αντιμετωπίζουν με επιτυχία αυτά τα θέματα. Είναι σημαντικό να κατανοούνται οι κίνδυνοι αυτοί στα σημερινά περιβάλλοντα υπολογιστών. Η κατανόηση αυτή βοηθά τον διαχειριστή (manager) ασφαλείας μιας επιχείρησης στο να επιλέξει κατάλληλα και με καλό λόγο κόστους- απόδοσης συστήματα που ελέγχουν και προστατεύουν τις πληροφορίες μιας επιχείρησης.

Οι βασικότερες μέθοδοι προστασίας συστημάτων που εφαρμόζονται σήμερα είναι οι εξής:

- Ασφάλεια βασισμένη στην εμπιστοσύνη.
- Ασφάλεια μέσω απόκρυψης.
- Σύστημα Password.

Η εγγυημένη ασφάλεια είναι απαραίτητη συνιστώσα των παραγόντων που θα επιτρέψουν την ευρεία διάδοση, χρήση και αποδοχή του εμπορίου πάνω από ανοικτά συστήματα. Η δημιουργία ασφαλούς περιβάλλοντος ηλεκτρονικού εμπορίου σημαίνει προστασία των δικτυακών πόρων από ενδεχόμενες απειλές και εγγύηση τουλάχιστον του ίδιου επιπέδου ασφαλείας με το συμβατικό εμπόριο. Συνεπώς το μέλλον του ηλεκτρονικού εμπορίου συνδέεται άμεσα με την ικανοποιητική λύση του προβλήματος της ασφάλειας.[1]

[1,2] Συρμακέσης Σ. "Ηλεκτρονικό Εμπόριο", Σελ.

2.2.2 Απαιτήσεις ασφαλείας συστημάτων ηλεκτρονικού εμπορίου

Υπάρχουν διάφορες απαιτήσεις για τη δημιουργία ασφαλούς περιβάλλοντος ηλεκτρονικού εμπορίου. Οι απαιτούμενες υπηρεσίες που συνθέτουν ένα γενικό ασφαλές πλαίσιο εργασίας μπορούν να χωριστούν στα εξής θέματα:

1. Έλεγχος αυθεντικότητας (Authentication).
2. Εξουσιοδότηση (Authorization).
3. Εμπιστευτικότητα (Confidentiality).
4. Ακεραιότητα (Integrity).
5. Μη αποποίηση ευθύνης (Non-repudation).

Οι αρχές ασφαλείας του ηλεκτρονικού εμπορίου βασίζονται σ' αυτές τις πέντε βασικές απαιτήσεις οι οποίες εξαρτώνται άμεσα η μία από την άλλη. Οι απαιτήσεις αυτές πρέπει να συμβαδίζουν και με την πολιτική ασφαλείας που έχει επιλεγεί για το σύστημα.[1]

2.2.3 Έλεγχος αυθεντικότητας (Authentication)

Η διαδικασία αυτή έχει στόχο την εξακρίβωση της ταυτότητας του χρήστη.

Όλα τα μέρη που εμπλέκονται στη συναλλαγή πρέπει να αισθάνονται σίγουρα ότι επικοινωνούν με άλλα μέλη που συνεργάζονται και όχι με κάποιον που ισχυρίζεται ότι είναι κάποιος άλλος. Ο έλεγχος αυτός πραγματοποιείται πριν την έναρξη οποιασδήποτε ηλεκτρονικής συναλλαγής και υλοποιείται με τη χρήση διαφόρων τεχνολογιών. Συγκεκριμένα, ο χρήστης παρέχει πληροφορίες για τη ταυτότητά του και συγκρίνονται με αυτές που το σύστημα ήδη γνωρίζει για το χρήστη. Αν το σύστημα λάβει από το χρήστη τις σωστές πληροφορίες (δηλαδή, ταυτίζονται με αυτές

που έχει καταχωρημένες), τότε αναγνωρίζει το χρήστη και τον πιστοποιεί σαν το μέλος του συστήματος με τα συγκεκριμένα στοιχεία.

Οι μέθοδοι αυθεντικοποίησης βασίζονται στους ακόλουθους παράγοντες:

1. Παρουσίαση της γνώσης κάποιου τύπου ιδιοκτησιακών πληροφοριών, όπως είναι τα passwords.
2. Κατοχή κάποιου τύπου ιδιοκτησιακής πληροφορίας όπως ένα κλειδί ή μια κάρτα.
3. Παρουσίαση κάποιου τύπου βιομετρικών χαρακτηριστικών, όπως είναι έναδακτυλικό αποτύπωμα.
4. Απόδειξη ότι ένα έμπιστο τρίτο μέλος έχει ήδη εγκαταστήσει πιστοποίηση για αυτόν που τη διεκδικεί.

Για να εξακριβωθεί η ταυτότητα ενός χρήστη, αυτοί οι παράγοντες πρέπει να ληφθούν υπόψη σε συνδυασμό μεταξύ τους παρά ξεχωριστά. Μερικές κοινές μέθοδοι για συστήματα ασφάλειας δικτύων που χρησιμοποιούνται για να επιτύχουν αυθεντικότητα των χρηστών, περιλαμβάνουν passwords, προσωπικούς αριθμούς αναγνώρισης , ψηφιακές υπογραφές και πιστοποιητικά.[1]

2.2.4 Εξουσιοδότηση (Authorization)

Η εξουσιοδότηση περιλαμβάνει τον έλεγχο πρόσβασης σε συγκεκριμένες πληροφορίες και υπηρεσίες όταν η ταυτότητα του χρήστη εξακριβωθεί. Δηλαδή εξουσιοδότηση σημαίνει παραχώρηση δικαιωμάτων από τον ιδιοκτήτη στο χρήστη. Για παράδειγμα, ο πελάτης εξουσιοδοτεί τον έμπορο ώστε ο τελευταίος να ελέγξει αν ο αριθμός της πιστωτικής κάρτας είναι έγκυρος και αν τα χρήματα στο λογαριασμό μπορούν να καλύψουν το ποσό των συναλλαγών.

[1] Συρμακέσης Σ. "Ηλεκτρονικό Εμπόριο", Σελ.

2.2.5 Εμπιστευτικότητα (Confidentiality)

Η εμπιστευτικότητα είναι συνυφασμένη με την αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας, παρέχεται μέσω κρυπτογράφησης και είναι απαραίτητο στοιχείο της ιδιωτικότητας του χρήστη. Για το ηλεκτρονικό εμπόριο, η εμπιστευτικότητα αποτελεί ύψιστης σημασίας συστατικό στην προστασία των οικονομικών δεδομένων ενός οργανισμού ή μιας εταιρείας, των πληροφοριών ανάπτυξης προϊόντων, των οργανωτικών δομών, και διαφόρων άλλων τύπων προσωπικών πληροφοριών από μη εξουσιοδοτημένη πρόσβαση. Σε ένα περιβάλλον ηλεκτρονικού εμπορίου, πληροφορίες εξαρτώμενες από το χρόνο μπορεί να είναι επίσης ένα κρίσιμο θέμα των εμπιστευτικών υπηρεσιών. Μια λίστα τιμών ή μια αναφορά μπορεί να είναι πολύ εμπιστευτικές για κάποιο συγκεκριμένο χρονικό διάστημα, και ελεύθερα διαθέσιμες αμέσως μετά. Για να συμβιβαστούν αυτές οι ανάγκες, πολιτικές ελέγχου της ροής της πληροφορίας πρέπει να περιλαμβάνονται στην εμπιστευτικότητα καθώς και στον έλεγχο αυθεντικότητας. Οι πολιτικές αυτές καθορίζουν όχι μόνο πότε ένα αντικείμενο θα ανακοινωθεί, αλλά ποια τιμή θα καθοριστεί και ποιος θα το χρεωθεί. Σε επιχειρήσεις με οικονομία βασισμένη σε πληροφορίες, οι συνέπειες ενός κενού στην εμπιστευτικότητα μπορεί να είναι καταστροφικές.

Η εμπιστευτικότητα πρέπει να εξασφαλίζει ότι:

- Η πληροφορία δεν μπορεί να διαβαστεί, αντιγραφεί, μετατραπεί ή αποκαλυφθεί χωρίς την απαραίτητη εξουσιοδότηση.
- Οι επικοινωνίες μέσω των δικτύων δεν μπορούν να διακοπούν. Τεχνικές κρυπτογράφησης και κωδικοποίησης έχουν σχεδιαστεί για να ικανοποιούν αυτές τις απαιτήσεις.[1]

[1] Συρμακέσης Σ. "Ηλεκτρονικό Εμπόριο", Σελ.

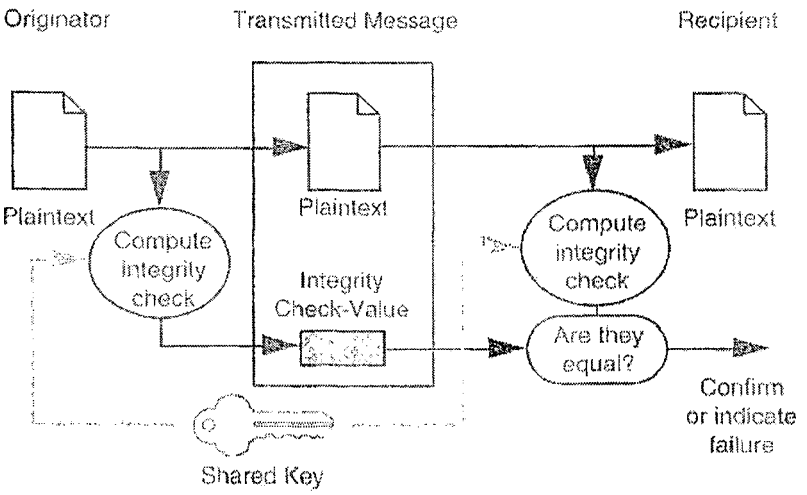
2.2.6 Ακεραιότητα (Integrity)

Ακεραιότητα σημαίνει αποφυγή μη εξουσιοδοτημένης τροποποίησης των δεδομένων κατά τη μεταφορά τους στο δίκτυο.

Υπάρχουν μέθοδοι (ψηφιακές υπογραφές) που ελέγχουν αν ένα μήνυμα έχει μεταβληθεί τη στιγμή της μεταφοράς. Τα συστήματα ηλεκτρονικού εμπορίου πρέπει να χρησιμοποιούν τέτοιες μεθόδους ώστε να μπορούν να διασφαλίσουν ότι τα δεδομένα φτάνουν στον προορισμό τους όπως ακριβώς στάλθηκαν. Οι υπηρεσίες ακεραιότητας θα πρέπει να προστατεύουν από μετατροπές στα δεδομένα αλλά επίσης και προσθέσεις, αφαιρέσεις και αναδιατάξεις μερών των δεδομένων.

Έστω ότι ο αποστολέας στέλνει ένα μήνυμα στον παραλήπτη χωρίς την απαίτηση της μυστικότητας. Παρόλα αυτά το μήνυμα δεν πρέπει να παραποιηθεί στη διαδρομή. Ο έλεγχος αυτός μπορεί να επιτευχθεί χρησιμοποιώντας ένα integrity check-value, το οποίο είναι μια ποσότητα πληροφορίας που παράγεται από τον αποστολέα και συνοδεύει το μήνυμα στον παραλήπτη. Η τιμή του integrity check-value εξαρτάται από όλα τα bits του μηνύματος. Έστω ένα bit να αλλάξει, παράγεται διαφορετικό integrity check-value και ο παραλήπτης καταλαβαίνει ότι το μήνυμα έχει παραποιηθεί.[1]

[1] WWW.E-COMMERCE.GR



Όπως φαίνεται και στο παραπάνω σχήμα η διαδικασία του integrity check-value χρησιμοποιεί ένα κρυφό κλειδί. Αυτό γίνεται για να μη μπορεί ο οποιοσδήποτε να δημιουργήσει το integrity check-value και να το επικολλήσει στο μήνυμα.

Ένας σημαντικός μηχανισμός ελέγχου ακεραιότητας με το όνομα Message Authentication Code (MAC) έγινε standard από τη βιομηχανία το 1986 και χρησιμοποιείται ευρέως από τότε. Ο μηχανισμός αυτός χρησιμοποιεί ένα συμμετρικό block cipher, όπως το DES.

2.2.7 Μη αποποίηση ευθύνης (Non-repudiation)

Μη αποποίηση ευθύνης σημαίνει ότι κανένας από τους συναλλασσόμενους δεν πρέπει να έχει τη δυνατότητα να αρνηθεί τη συμμετοχή του σε μια συναλλαγή. Οι υπηρεσίες μη αποποίησης ευθύνης πρέπει, αν ερωτηθούν από ένα τρίτο μέλος, να μπορούν να αποδείξουν την προέλευση, μεταφορά, παράδοση και μετάδοση των δεδομένων. Η ανάγκη για τέτοιες υπηρεσίες αντικατοπτρίζει τις ατέλειες σε κάθε περιβάλλον επικοινωνίας, είτε είναι δικτυωμένο είτε όχι, και φανερώνει το γεγονός

ότι απαιτούνται κατάλληλοι μηχανισμοί ασφαλείας για την πραγματοποίηση κρίσιμων και ζωτικής σημασίας συναλλαγών και επικοινωνιών.[1]

2.3 Τεχνολογίες Ασφάλειας Συναλλαγών

Η ασφάλεια είναι σημαντικός και καθοριστικός παράγοντας στα χρηματοοικονομικά συστήματα, ανεξάρτητα από το αν είναι βασισμένα σε φυσικές ή ηλεκτρονικές συναλλαγές. Στον κόσμο των διασυνδεδεμένων υπολογιστών συναντάμε πλήθος απειλών για την ασφάλεια των ηλεκτρονικών συναλλαγών.

Το πρόβλημα υπάρχει λόγω της έλλειψης υπηρεσιών ασφάλειας στην υποδομή του Διαδικτύου. Αυτή η έλλειψη ασφάλειας μπορεί να οδηγήσει και να καθορίσει συγκεκριμένα, σοβαρά προβλήματα όπως:

- Υποκλοπή αριθμών πιστωτικών καρτών την στιγμή μετάδοσής τους από στο Διαδίκτυο.
- Υποκλοπή κωδικών που χρησιμεύουν για την προστασία διαφόρων συστημάτων.
- Κλοπή χρημάτων τροποποιώντας το ποσό μιας συναλλαγής.
- Συλλογή ποσών με απάτη, αν ο επίδοξος παραβάτης προσποιηθεί κάποιον άλλο.
- Μέτοχος σε συναλλαγή, ενδέχεται αργότερα να αρνηθεί την πράξη του.

Ένα από τα πλέον σοβαρότερα προβλήματα στο Διαδίκτυο, σχετίζεται με το γεγονός ότι η ομάδα των TCP/IP πρωτοκόλλων είναι ανασφαλής. Δεν παρέχεται υπηρεσία αυθεντικοποίησης. Οι χρήστες μπορούν να παριστάνουν άλλους, αλλάζοντας διεύθυνση στα πακέτα καθώς και να τροποποιούν πακέταπου προέρχονται από άλλους χρήστες.

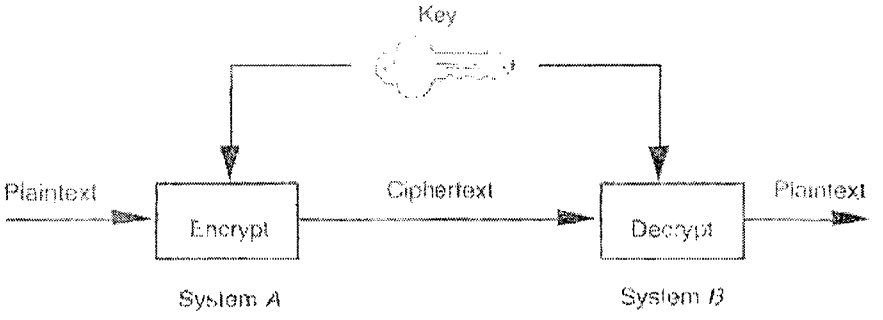
---

[1] Συρμακέσης Σ. "Ηλεκτρονικό Εμπόριο", Σελ.

Σήμερα είναι έντονη η προσπάθεια ανάπτυξης standard που θα καταστίσουν το Διαδίκτυο ένα αξιόπιστο χώρο διεξαγωγής εμπορίου. Καταβάλλεται προσπάθεια ώστε να υπάρχει μια αποδεκτή ταχύτητα λειτουργίας και να εκμηδενισθεί η πιθανότητα επιτυχημένης επίθεσης στο σύστημα.

2.3.1 Συμμετρική κρυπτογραφία και κρυπτογραφία δημοσίου κλειδιού

Τα συμμετρικά κρυπτοσυστήματα χρησιμοποιούνται σε εμπορικές εφαρμογές από τη δεκαετία του 70 και έχουν το χαρακτηριστικό ότι το ίδιο κλειδί χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση.



Κρυπτοσύστημα συμμετρικού κλειδιού

Στην συμμετρική παραδοσιακή κρυπτογραφία ο αποστολέας και ο παραλήπτης ενός μηνύματος χρησιμοποιούν το ίδιο μυστικό κλειδί. Αυτή η μέθοδος είναι γνωστή σαν συμμετρική κρυπτογραφία. Η ακαταλληλότητα της μεθόδου έγκειται στο ότι αδυνατεί να προσφέρει πρακτικά ασφαλή διαχείριση κλειδιών σε δημόσια δίκτυα με πληθώρα χρηστών. Συγκεκριμένα, έστω ότι δυο μέρη συμφωνούν πάνω σε ένα διαμοιραζόμενο ιδιωτικό κλειδί. Η σχέση με Ν ανταποκριτές επιβάλει την αποθήκευση Ν ιδιωτικών κλειδιών, ένα για κάθε ανταποκριτή. Ένα τέτοιο σχήμα στερείται στοιχειώδους ευελιξίας. Αν χρησιμοποιηθούν κοινά κλειδιά για δύο

ανταποκριτές, τότε καταλήγουμε στην ανεπιθύμητη κατάσταση να μπορεί ο ένας να διαβάσει τα μηνύματα που απευθύνονται στον άλλον. Το σχήμα συμμετρικής κρυπτογραφίας αντιμετωπίζει πρόβλημα στο θέμα της αυθεντικοποίησης, μιας και είναι αδύνατο να αποδειχθεί η ταυτότητα του αποστολέα και παραλήπτη του μηνύματος. Εφόσον τόσο ο ανταποκριτής Α όσο και ο Β μοιράζονται το ίδιο κλειδί, μπορούν προφανώς να στείλουν κρυπτογραφημένο μήνυμα και να ισχυριστούν ότι το έστειλε ο άλλος. Αυτή η έμφυτη ασάφεια πάνω στο ποιος δημιούργησε το μήνυμα αδυνατεί να ικανοποιήσει την απαίτηση για μη αποποίηση ευθύνης.[1]

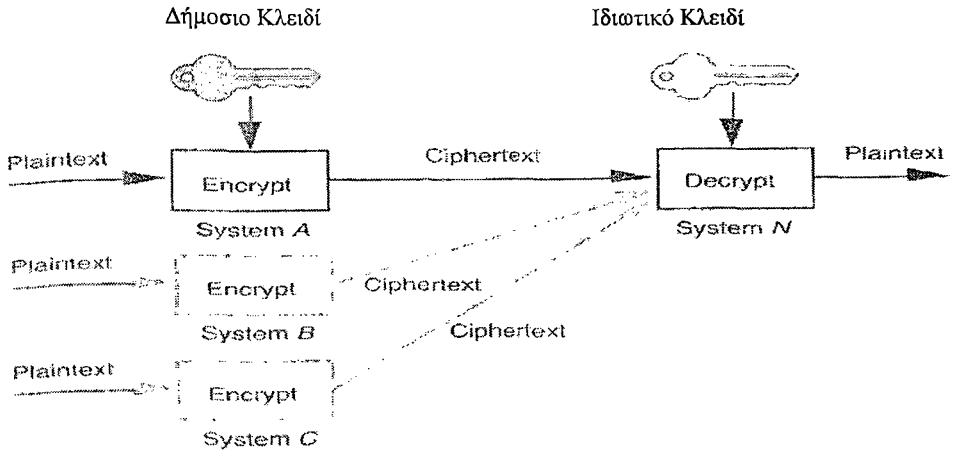
Τη λύση έρχεται να δώσει η ασύμμετρη κρυπτογραφία ή κρυπτογραφία δημόσιου κλειδιού. Σε αντίθεση με τα συμμετρικά κρυπτοσυστήματα, αυτά του δημοσίου κλειδιού χρησιμοποιούν ένα ζεύγος κλειδιών, ένα κλειδί για κρυπτογράφηση και ένα άλλο για αποκρυπτογράφηση. Το ζεύγος των κλειδιών είναι συσχετισμένο με ένα από τα συστήματα που συμμετέχουν στην επικοινωνία. Το ένα κλειδί, γνωστό και ως ιδιωτικό κλειδί (private key), είναι γνωστό μόνο στο συγκεκριμένο σύστημα, ενώ το άλλο, το δημόσιο κλειδί (public key), μπορεί να γίνει γνωστό σε όλα τα συστήματα. Το κρυπτοσύστημα πρέπει να έχει το χαρακτηριστικό ότι δοθέντος του δημοσίου κλειδιού να μην είναι δυνατό να υπολογιστεί το ιδιωτικό κλειδί.

Το δημόσιο κλειδί δημοσιεύεται (π.χ. με e-mail, σε κάποιον εξυπηρετητή ή μέσω υπηρεσιών καταλόγου δημοσίων κλειδιών τις οποίες προσφέρουν οι Αρχές Πιστοποίησης) ενώ το ιδιωτικό παραμένει μυστικό.

Η ανάγκη για τον παραλήπτη και τον αποστολέα να διαμοιραστούν απόρρητη πληροφορία περιορίζεται πλέον.

Υπάρχουν δύο βασικοί τρόποι λειτουργίας του κρυπτοσυστήματος δημοσίου κλειδιού, που διαφέρουν στη χρήση του δημοσίου κλειδιού στην κρυπτογράφηση ή αποκρυπτογράφηση. Παρακάτω φαίνεται η χρήση του δημοσίου κλειδιού στην κρυπτογράφηση των μηνυμάτων.

[1] Συρμακέσης Σ."Ηλεκτρονικό Εμπορίο", Σελ.

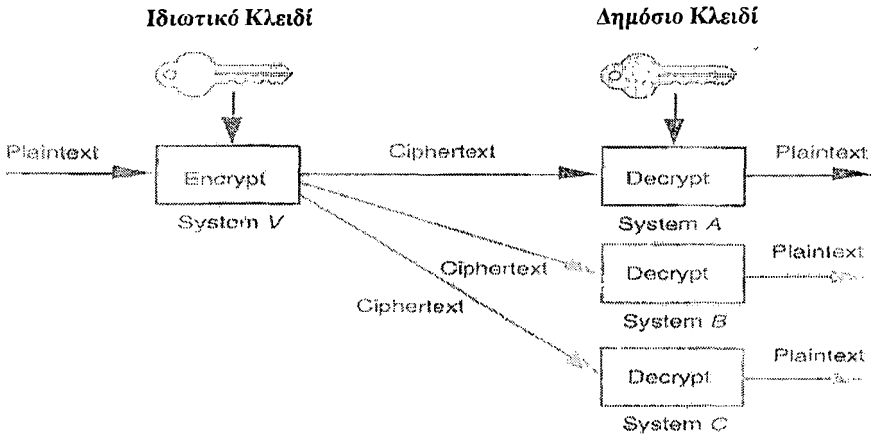


Κρυπτοσύστημα Δημοσίου Κλειδιού

Στην περίπτωση αυτή το ζεύγος δημόσιου – ιδιωτικού κλειδιού ανήκει στο σύστημα N. Το ιδιωτικό είναι αποθηκευμένο με ασφάλεια στο σύστημα N. Το δημόσιο κλειδί έχει γίνει γνωστό με κάποιο τρόπο στα συστήματα A, B, C. Όταν ένα από τα συστήματα αυτά θελήσει να στείλει ένα εμπιστευτικό μήνυμα στο N, θα χρησιμοποιήσει το αντίστοιχο δημόσιο κλειδί για να το κρυπτογραφήσει. Μόνο το σύστημα N θα έχει τη δυνατότητα να αποκρυπτογραφήσει το μήνυμα, διότι μόνο αυτό έχει το κατάλληλο ιδιωτικό κλειδί.

Η δεύτερη χρήση του κρυπτοσυστήματος δημοσίου κλειδιού είναι για την εξασφάλιση της ακεραιότητας και αυθεντικότητας. Το παρακάτω σχήμα περιγράφει αυτή τη διαδικασία. Το σύστημα V έχει συσχετιστεί με ένα ζεύγος κλειδιών. Το ιδιωτικό κλειδί είναι αποθηκευμένο με ασφάλεια στο σύστημα. Το δημόσιο κλειδί είναι γνωστό στα συστήματα A, B, C. Το σύστημα V χρησιμοποιώντας το ιδιωτικό κλειδί του, κρυπτογραφεί το μήνυμα και το στέλνει στους παραλήπτες A, B, C, οι οποίοι χρησιμοποιώντας το δημόσιο κλειδί το αποκρυπτογραφούν. Σ' αυτή την περίπτωση δεν έχουμε κερδίσει τη μυστικότητα του μηνύματος, αφού ο οποιοσδήποτε μπορεί να βρει το δημόσιο κλειδί και να αποκρυπτογραφήσει το μήνυμα. Αυτό που κερδίσαμε είναι η αυθεντικότητα. Τα συστήματα A, B, C είναι σίγουρα ότι το μήνυμα το έστειλε το V, γιατί κατάφεραν να το αποκρυπτογραφήσουν χρησιμοποιώντας το δημόσιο κλειδί του συστήματος V. Επίσης ξέρουμε ότι το

μήνυμα δεν παραποιήθηκε στην πορεία αφού το ιδιωτικό κλειδί που χρησιμοποιείται στην κρυπτογράφηση είναι γνωστό μόνο στο V. Άρα έχουμε κερδίσει και την ακεραιότητα του μηνύματος. Αυτός ο τρόπος λειτουργίας αποτελεί τη βάση για το σχεδιασμό συστημάτων ψηφιακών υπογραφών.



Κρυπτοσύστημα Δημοσίου Κλειδιού – Λειτουργία Αυθεντικότητας

Γενικά τα κρυπτοσυστήματα δημοσίου κλειδιού έχουν χαρακτηριστικά που τα κάνουν ισχυρότερα από τα συμμετρικά. Παρόλα αυτά τα κρυπτοσυστήματα δημοσίου κλειδιού αποτελούν μεγαλύτερη πρόκληση, αφού η πληροφορία του δημοσίου κλειδιού μπορεί να χρησιμοποιηθεί για την παραβίαση του κρυπτοσυστήματος. Μέχρι τώρα τα κρυπτοσυστήματα δημοσίου κλειδιού βασίζονται στο γεγονός ότι το συγκεκριμένο μαθηματικό πρόβλημα είναι υπολογιστικά δύσκολο να λυθεί.[1]

[1] WWW. E-COMMERCE. GR

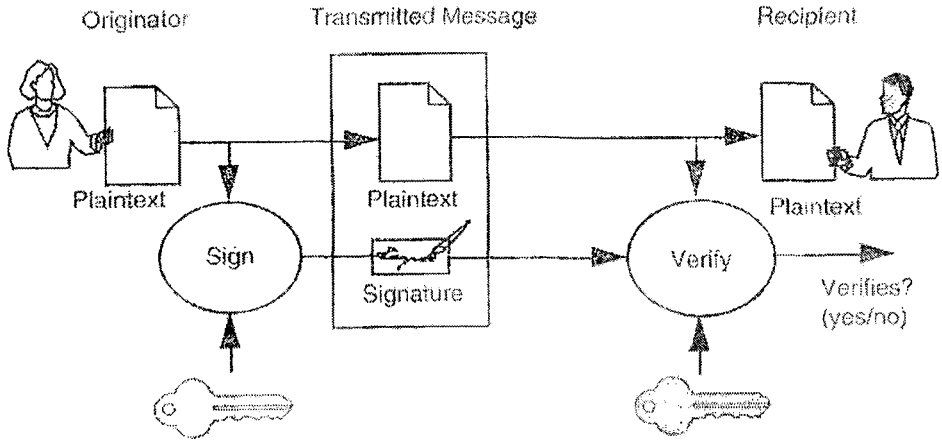
2.3.2 Ψηφιακές υπογραφές

Οι ασύμμετροι αλγόριθμοι είναι υπολογιστικά αργοί για την κρυπτογράφηση ενός ολόκληρου μηνύματος. Έστω λοιπόν ότι ο Α επιθυμεί να στείλει υπογεγραμμένο έγγραφο ή μήνυμα στον Β. Το πρώτο βήμα είναι γενικά να εφαρμόσει μια hash συνάρτηση στο μήνυμα και να δημιουργήσει ένα message digest. Το message digest είναι συνήθως αισθητά μικρότερο από το πρωτότυπο μήνυμα. Ουσιαστικά η δουλειά της hash συνάρτησης είναι να πάρει ένα μήνυμα οποιουδήποτε μεγέθους και να το συρρικνώσει σε προκαθορισμένο μέγεθος. Για να δημιουργήσει κανείς μια ψηφιακή υπογραφή κρυπτογραφεί συνήθως το message digest και όχι το ίδιο το μήνυμα (μ' άλλα λόγια το κρυπτογραφημένο message digest είναι η ψηφιακή υπογραφή του αποστολέα). Ο Α στέλνει στον Β το κρυπτογραφημένο message digest και το μήνυμα κρυπτογραφημένο ή όχι. Προκειμένου ο Β να αυθεντικοποιήσει την υπογραφή κάνει τα εξής:

- Εφαρμόζει, πρώτα απ' όλα, την ίδια hash συνάρτηση με τον Α στο μήνυμα που παρέλαβε (το οποίο επαναλαμβάνουμε είναι κρυπτογραφημένο ή απλό κείμενο). Δημιουργεί έτσι τη δική του εκδοχή για το ορθό message digest.
- Στη συνέχεια αποκρυπτογραφεί τη ψηφιακή υπογραφή την οποία παρέλαβε συνημμένη με το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί του Α. Η διαδικασία αυτή οδηγεί στην αναπαραγωγή του message digest το οποίο δημιούργησε ο Α.

Ο Β έχει τώρα στη διάθεση του δύο message digests. Τα συγκρίνει και αν ταιριάζουν, αυθεντικοποίησε επιτυχώς τη ψηφιακή υπογραφή του Α. Αν όχι, υπάρχουν λίγες πιθανές εξηγήσεις. Είτε κάποιος προσποιείται τον Α, ή το μήνυμα μεταβλήθηκε από τη στιγμή που το υπέγραψε ο Α, ή υπήρξε λάθος στη μετάδοση.[1]

[1] Συρμακέσης Σ."Ηλεκτρονικό Εμπορίο", Σελ.



Ψηφιακή Υπογραφή

2.4 Ψηφιακά πιστοποιητικά και αρχές πιστοποίησης

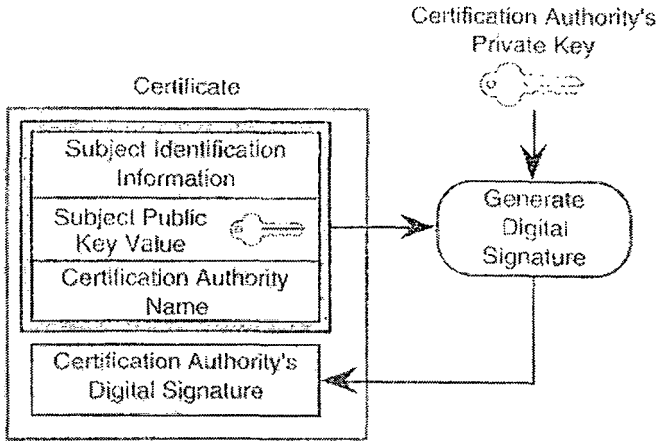
Το πρόβλημα στο μοντέλο δημόσιου κλειδιού είναι η σύνδεση οντότητας (χρήστη, εμπόρου, επιχείρησης.) με το δημόσιο κλειδί της. Έστω ότι ο Α προσποιείται ότι είναι ο Β και υπογράφει έγγραφα με ένα ζευγάρι κλειδιών που ισχυρίζεται ότι είναι του Β. Μένει λοιπόν, να απαντηθεί το ερώτημα, πως πιστοποιεί κανείς, ότι είναι αυτός που ισχυρίζεται ότι είναι και συνεπώς το κλειδί που εκδίδει είναι έγκυρο.

Τη λύση δίνουν ψηφιακά έγγραφα τα οποία καλούνται ψηφιακά πιστοποιητικά και τα οποία συσχετίζουν μια οντότητα με ένα συγκεκριμένο δημόσιο κλειδί. Τα ψηφιακά πιστοποιητικά χρησιμοποιούνται τυπικά, για να δημιουργήσουν αίσθημα εμπιστοσύνης στη νομιμότητα ενός δημόσιου κλειδιού. Είναι ουσιαστικά ψηφιακές υπογραφές που προστατεύουν τα δημόσια κλειδιά από παραχάραξη, λανθασμένη αναπαράσταση ή μετατροπή. Η επαλήθευση μιας ψηφιακής υπογραφής λοιπόν, μεταφράζεται σαν έλεγχος εγκυρότητας του πιστοποιητικού για το εμπλεκόμενο δημόσιο κλειδί.

Από τη στιγμή που δημιουργεί κάποιος το ζευγάρι δημόσιου και ιδιωτικού κλειδιού του, επιφορτίζεται με την προστασία του ιδιωτικού κλειδιού του. Μένει να αποφασίσει με ποιον τρόπο θα διανείμει το δημόσιο κλειδί του στους ανταποκριτές του. Η λύση «ηλεκτρονικό ταχυδρομείο» κρίνεται απαγορευτική μιας και ενέχει τον κίνδυνο να ξεχαστεί κάποιος εκτός λίστας διευθύνσεων, ενώ αδυνατεί να επιτρέψει σε νέους χρήστες να γίνουν ανταποκριτές με δική τους πρωτοβουλία. Άλλο σημαντικό μειονέκτημα της λύσης αυτής είναι ο μικρός βαθμός αξιοπιστίας που προσφέρει όσον αφορά στην αυθεντικοποίηση. Για παράδειγμα, μπορεί ο Β να προσποιηθεί τον Α, να δημιουργήσει ένα ζευγάρι κλειδιών, να στείλει το δημόσιο κλειδί σε ανταποκριτές υποστηρίζοντας ότι προέρχεται από τον Α και να πλαστογραφεί αβίαστα μηνύματα στο όνομα του Α.

Ένας καλύτερος, αξιόπιστος τρόπος διανομής δημόσιων κλειδιών είναι η χρήση μιας Αρχής Πιστοποίησης. Μία κοινώς αποδεκτή αρχή εκδίδει τα πιστοποιητικά για τα ζεύγη δημόσιου – ιδιωτικού κλειδιού. Κάθε πιστοποιητικό περιέχει το δημόσιο κλειδί και πληροφορία που χαρακτηρίζει τον ιδιοκτήτη του, ο οποίος είναι ο κάτοχος του αντίστοιχου ιδιωτικού κλειδιού. Στο τέλος το ψηφιακό πιστοποιητικό υπογράφεται από την εκδίδουσα αρχή χρησιμοποιώντας το ιδιωτικό κλειδί της.

Όταν κάποιος θέλει να χρησιμοποιήσει το δημόσιο κλειδί, πχ για να στείλει ένα εμπιστευτικό μήνυμα στον κάτοχό του, αρκεί να προμηθευτεί ένα αντίγραφο του αντίστοιχου πιστοποιητικού. Χρησιμοποιώντας το δημόσιο κλειδί της εκδίδουσας αρχής (θεωρούμε ότι με κάποιο ασφαλή τρόπο το έχει προμηθευτεί και ότι εμπιστεύεται τη συγκεκριμένη αρχή για την έκδοση των πιστοποιητικών) επαληθεύει τη γνησιότητά του και παίρνει το δημόσιο κλειδί.



Κατασκευή Ψηφιακού Πιστοποιητικού

Για να είναι παγκοσμίως αποδεκτά αυτά τα ψηφιακά πιστοποιητικά πρέπει να εκδίδονται από μια ουδέτερη αρχή και να βρίσκονται σε συμφωνία με τα διεθνή πρότυπα. Φορείς που εκδίδουν ψηφιακά πιστοποιητικά (Αρχές Πιστοποίησης - Certification Authorities) είναι οι Verisign, Cybertrust, Nortel, Globalsign κ.α.

Το στάνταρτ πρότυπο πιστοποιητικών δημοσίου κλειδιού είναι το X.509 το οποίο αποτελείται από:

- Το διακεκριμένο όνομα του κατόχου του.
- Το δημόσιο κλειδί του.
- Την ταυτότητα του χορηγού του πιστοποιητικού και τη ψηφιακή υπογραφή του.
- Ένα κωδικό (serial number) που δίνεται από το χορηγό.
- Μια χρονική περίοδο εγκυρότητας του πιστοποιητικού.

Ένα ψηφιακό πιστοποιητικό μπορεί να εκδοθεί σε μία από τις 4 ορισμένες κλάσεις, οι οποίες υποδεικνύουν σε τι βαθμό έχει διασταυρωθεί η ταυτότητα του χρήστη. Η κλάση 1 είναι η ευκολότερη να αποκτηθεί διότι προϋποθέτει τους λιγότερους ελέγχους στο ποιόν του χρήστη. Μόνο το όνομα και η e-mail διεύθυνση επαληθεύονται. Για τα πιστοποιητικά κλάσης 2, η εκδίδουσα αρχή ελέγχει την άδεια οδήγησης, τον αριθμό κοινωνικής ασφάλισης και την ημερομηνία γέννησης. Οι

χρήστες που αιτούνται πιστοποιητικό κλάσης 3 θα πρέπει να περιμένουν τη διενέργεια πιστωτικού ελέγχου συν τα απαιτούμενα στην κλάση 2. Το πιστοποιητικό κλάσης 4 περιλαμβάνει πληροφορία σχετικά με τη θέση του ιδιώτη μέσα σε έναν οργανισμό. Ωστόσο, οι απαιτήσεις επαλήθευσης για αυτή την κλάση δεν έχουν ως τώρα παγιωθεί.

Οι αρχές πιστοποίησης είναι απαραίτητο να λειτουργούν συνετά. Να σιγουρεύουν ότι οι συσχετισμοί προσώπων είναι εξαντλητικά ελεγμένοι και άρα αντανακλούν την πραγματικότητα (π.χ. έλεγχος ταυτότητας, διαβατηρίου κατά τη φυσική παρουσία των ενδιαφερομένων).

Ας σημειωθεί ότι η έκδοση ψηφιακού πιστοποιητικού από τις αρχές πιστοποίησης δεν είναι δωρεάν. Η τιμή αυξάνει όσο μεγαλύτερη είναι η κλάση του πιστοποιητικού.

Οι αρχές πιστοποίησης φέρουν επίσης την ευθύνη συντήρησης και διάθεσης μιας Λίστας Απόσυρσης Πιστοποιητικών, από την οποία ενημερώνονται οι χρήστες για το ποια πιστοποιητικά δεν είναι πλέον έγκυρα. Οι λίστες απόσυρσης πιστοποιητικών δεν περιέχουν ληγμένα πιστοποιητικά διότι τα τελευταία έχουν ενσωματωμένο μηχανισμό λήξης. Περιέχουν, ωστόσο πιστοποιητικά που χάθηκαν, κλάπηκαν ή παύουν να ισχύουν γενικά.

Εκτός από τις εμπορικές αρχές πιστοποίησης (όπως οι Verisign, Cybertrust, Nortel και Globalsign) υπάρχει η δυνατότητα όσες εταιρείες το επιθυμούν να γίνουν οι ίδιες αρχές πιστοποίησης αγοράζοντας έναν εξυπηρετητή πιστοποιητικών (Certificate Server) από πωλητή πιστοποιημένο από κάποια αρχή πιστοποίησης. Τέτοιου είδους συμφωνίες είναι χρήσιμες όταν μια εταιρεία χρειάζεται να εκδώσει ψηφιακά πιστοποιητικά για να καλύψει ανάγκες των υπαλλήλων της.

Η ασφαλέστερη χρήση αυθεντικοποίησης προϋποθέτει την προσάρτηση ενός ή περισσότερων πιστοποιητικών σε κάθε υπογεγραμμένο μήνυμα. Ο παραλήπτης επαληθεύει το πιστοποιητικό με τη βοήθεια του δημοσίου κλειδιού της πιστοποιούσας αρχής. Σίγουρος πλέον για το δημόσιο κλειδί προχωρά στον έλεγχο της υπογραφής του μηνύματος. Ενδεχομένως υπάρχουν δύο ή περισσότερα πιστοποιητικά προσαρτημένα στο μήνυμα, δημιουργώντας έτσι μια ιεραρχημένη αλυσίδα πιστοποιητικών. Σ' αυτή, το κάθε πιστοποιητικό μαρτυρά την αυθεντικότητα του προηγούμενου. Στην κορυφή της ιεραρχίας υπάρχει μια ηγετική αρχή

πιστοποίησης, η οποία χαίρει άκρας εμπιστοσύνης. Το δημόσιο κλειδί της οφείλει να είναι ευρέως διαδεδομένο.

Όσο πιο οικείος είναι ο αποστολέας στον παραλήπτη, τόσο μικρότερη ανάγκη υπάρχει να προσαρτούμε και να επαληθεύουμε πιστοποιητικά. Ένας αποστολέας του οποίου η εταιρεία είναι γνωστή στον παραλήπτη επισυνάπτει ένα μόνο πιστοποιητικό Δεν συμβαίνει το ίδιο με τον αποστολέα που ανήκει σε εταιρεία άγνωστη στον παραλήπτη.[1]

2.5 Διαχείριση κλειδιών

Διαχείριση κλειδιών ονομάζουμε τη δημιουργία, μεταφορά, αποθήκευση και διαγραφή των κλειδιών. Προφανώς ο αριθμός των πιθανών κλειδιών για κάθε δεδομένη εφαρμογή πρέπει να είναι εξαιρετικά μεγάλος. Διαφορετικά, ένας εισβολέας θα μπορούσε να σπάσει το σύστημα δοκιμάζοντας όλα τα πιθανά κλειδιά. Έστω, ότι ο αριθμός των πιθανών κλειδιών είναι πράγματι εξαιρετικά μεγάλος αλλά κάποια από αυτά τα κλειδιά φέρουν μεγαλύτερη πιθανότητα να παραχθούν από κάποια άλλα. Μια τέτοια κατάσταση αποτελεί πρόβλημα. Συνεπώς πρέπει να χρησιμοποιηθεί μια γεννήτρια τυχαίων ή ψευδοτυχαίων αριθμών για τη δημιουργία κλειδιών.

Τα συμμετρικά κλειδιά που πρόκειται να χρησιμοποιηθούν για μικρές χρονικές περιόδους μπορούν να κρυπτογραφηθούν από συμμετρικά κλειδιά που ισχύουν για μεγάλες χρονικές περιόδους και να ανταλλαχθούν κρυπτογραφημένα. Τα κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση των κλειδιών μπορούν να διανεμηθούν χειρονακτικά ή μπορούν με τη σειρά τους να κρυπτογραφηθούν από άλλα χειρονακτικά διανεμημένα συμμετρικά κλειδιά.

[1] Συρμακέσης Σ."Ηλεκτρονικό Εμπορίο", Σελ.

Τα συμμετρικά κλειδιά μπορούν να κατανεμηθούν επίσης χρησιμοποιώντας κρυπτοσυστήματα δημοσίου κλειδιού. Μια άλλη μέθοδος, η Diffie-Hellman (εκθετική ανταλλαγή κλειδιών), επιτρέπει στους χρήστες να εγκαθιστούν κοινό ιδιωτικό κλειδί χωρίς να απαιτείται κάποια κοινή μυστική πληροφορία και χωρίς να είναι απαραίτητο ασφαλές κανάλι επικοινωνίας. Άλλοι διαδεδομένοι αλγόριθμοι κρυπτογράφησης είναι οι DES, Tripple DES, RC2, RC4, IDEA, RSA, και DSA.[1]

2.6 Αλγόριθμοι Κρυπτογράφησης

Ο DES (Data Encryption Standard) ανήκει στην κατηγορία των συμμετρικών αλγορίθμων. Αναπτύχθηκε στις αρχές της δεκαετίας του 70 και καθιερώθηκε επίσημα από την κυβέρνηση των ΗΠΑ το 1977. Ο DES έχει ερευνηθεί και μελετηθεί τα τελευταία 20 χρόνια και είναι σίγουρα ο πιο γνωστός και ευρύτατα χρησιμοποιημένος αλγόριθμος στον κόσμο. Οι λειτουργίες του είναι σχετικά γρήγορες και δουλεύουν καλά ακόμα και για μεγάλα έγγραφα.

Μια παραλλαγή του DES η οποία χρησιμοποιείται σήμερα είναι ο Triple-DES που λογικά είναι πιο αργός, έχοντας όμως μέγεθος κλειδιού 168 bits είναι πολύ δύσκολο να «σπαστεί».

Ο Triple-DES κρυπτογραφεί κάθε μήνυμα χρησιμοποιώντας τρία διαφορετικά κλειδιά και άρα απαιτεί τρεις φορές περισσότερο χρόνο από τον DES.

Ο RC2 είναι ένας αλγόριθμος γρηγορότερος από τον DES, ο οποίος έχει σχεδιαστεί ως αντικαταστάτης του. Έχει τη δυνατότητα να είναι περισσότερο ή λιγότερο ασφαλής από τον DES σε εξαντλητικές αναζητήσεις κλειδιού χρησιμοποιώντας κατάλληλα κλειδιά μεταβλητού μεγέθους.

Ο RC4 σχεδιάστηκε από τον Ron Rivest και χρησιμοποιεί και αυτός κλειδιά μεταβλητού μεγέθους.

[1] Συρμακέσης Σ."Ηλεκτρονικό Εμπορίο", Σελ

Ανεξάρτητοι αναλυτές εξέτασαν αναλυτικά τον αλγόριθμο και τον θεώρησαν ασφαλή. Χρησιμοποιείται για ασφαλείς επικοινωνίες όπως στην κρυπτογράφηση της πληροφορίας κατά την επικοινωνία με ασφαλή web site (πρωτόκολλο SSL).

Ο IDEA δημιουργήθηκε το 1991 και σχεδιάστηκε με σκοπό την αποδοτικότητα σε επίπεδο λογισμικού. Προσφέρει πολύ δυνατή κρυπτογράφηση κάνοντας χρήση κλειδιού 128 bits.

Η ασφάλεια του RSA βασίζεται στο γεγονός ότι τα δημόσια και ιδιωτικά κλειδιά κατασκευάζονται με τη χρήση δύο πολύ μεγάλων πρώτων αριθμών (μεγαλύτερους από 2^512) και στη δυσκολία που υπάρχει όσον αφορά στο να παραγοντοποιηθούν πολύ μεγάλοι αριθμοί.

Ο RSA είναι σημαντικός γιατί επιτρέπει ψηφιακές υπογραφές που χρησιμοποιούνται για να πιστοποιήσουν ηλεκτρονικά έγγραφα με τον ίδιο ακριβώς τρόπο που οι ιδιόχειρες υπογραφές χρησιμοποιούνται για να πιστοποιήσουν έντυπα έγγραφα. Είναι ενσωματωμένος σε διάφορους φυλλομετρητές (browsers) παγκοσμίου ιστού όπως ο NetScape. Στον τομέα του υλικού ο RSA απαντάται σε ασφαλή τηλέφωνα, σε Ethernet κάρτες δικτύου και σε έξυπνες κάρτες (smartcards).

Ο Diffie-Hellman αλγόριθμος αναπτύχθηκε περί το 1976 από τους Diffie και Hellman και επιτρέπει σε δύο άτομα να ανταλλάξουν με ασφαλή τρόπο ένα μυστικό κλειδί σε ένα μη ασφαλές μέσο.[1]

2.7 Ασφάλεια για Εφαρμογές Ηλεκτρονικού Εμπορίου

Προκειμένου να υλοποιηθεί μια εφαρμογή ηλεκτρονικού εμπορίου μέσω του διαδικτύου είναι απαραίτητο να υπάρχει ένα ασφαλές κανάλι επικοινωνίας μεταξύ τους προκειμένου να γίνεται η ασφαλής ανταλλαγή των δεδομένων. Για το σκοπό αυτό έχουν αναπτυχθεί ειδικά πρωτόκολλα. Τα περισσότερο διαδεδομένα είναι το Secure Sockets Layer (SSL) και το Secure HTTP (S-HTTP). Επίσης για τις

[1] Συρμακέσης Σ."Ηλεκτρονικό Εμποριο", Σελ

συναλλαγές μέσω πιστωτικών καρτών έχει αναπτυχθεί το πρωτόκολλο Secure Electronic Transaction (SET).

2.7.1 Secure Sockets Layer (SSL)

Το SSL αναπτύχθηκε από τη Netscape και μπορεί να προσθέσει ασφάλεια σε μια πληθώρα εφαρμογών. Το SSL είναι ένα νέο επίπεδο που λειτουργεί πάνω από το TCP. Όλες οι εφαρμογές που χρησιμοποιούν το TCP, όπως το HTTP, FTP, TELNET μπορούν να το χρησιμοποιήσουν για να πετύχουν ασφαλή επικοινωνία. Η περισσότερο διαδεδομένη χρήση του είναι η προστασία του HTTP. Όταν το URL ξεκινά με "https://..." υποδηλώνει το γεγονός αυτό.

Οι υπηρεσίες που παρέχει το SSL είναι:

- *Αυθεντικότητα του server*: Ο server αυθεντικοποιείται στον client επιδεικνύοντας το πιστοποιητικό του.
- *Αυθεντικότητα του client*: Ο πελάτης αυθεντικοποιείται στον server επιδεικνύοντας το πιστοποιητικό του. Η υπηρεσία αυτή είναι προαιρετική στις ηλεκτρονικές αγορές (internet shopping) διότι δεν έχουν όλοι οι πελάτες ψηφιακά πιστοποιητικά. Περισσότερο χρησιμοποιείται σε περιπτώσεις internet banking όπου παίζει πολύ σημαντικό ρόλο.
- *Ακεραιότητα των δεδομένων*: Τα δεδομένα που μεταδίδονται προστατεύονται ώστε οποιαδήποτε προσπάθεια αλλοίωσης τους να γίνει αντιληπτή.

Το SSL αποτελείται από δύο υπο-πρωτόκολλα, το SSL Record Protocol και το SSL Hand shake Protocol. Το SSL Record P rotocol ορίζει το βασικό format των δεδομένων που ανταλλάσσονται σε κάθε session. Επίσης είναι αυτό που κάνει τη συμπίεση των δεδομένων, κάνει τον έλεγχο ακεραιότητας και κρυπτογραφεί τα δεδομένα. Προκειμένου το SSL Record Protocol να κάνει την κρυπτογράφηση, να υπολογίσει την τιμή του ελέγχου ακεραιότητας, πρέπει και ο client και ο server να

γνωρίζουν τα κρυπτογραφικά κλειδιά. Το πρωτόκολλο υποστηρίζει την αλλαγή των αλγορίθμων κρυπτογράφησης και των κλειδιών οποιαδήποτε στιγμή.

Το SSL Handshake Protocol χρησιμοποιείται για τη διαπραγμάτευση του αλγορίθμου κρυπτογράφησης που θα χρησιμοποιηθεί, την ανταλλαγή των πιστοποιητικών και την ανταλλαγή των κλειδιών που θα χρησιμοποιηθούν στο session.

Μπορούν να χρησιμοποιηθούν διάφοροι αλγόριθμοι κρυπτογράφησης στο SSL Handshake Protocol όπως ο RSA, ο DES, ο Diffie-Hellman. Το πρωτόκολλο SSL είναι σχεδιασμένο ώστε να μπορεί να χρησιμοποιείται και στις Η.Π.Α. και σε άλλες χώρες. Και οι δύο υλοποιήσεις χρησιμοποιούν τον ίδιο αλγόριθμο κρυπτογράφησης με μήκος κλειδιού 128 bits. Η διαφορά στις δύο υλοποιήσεις βρίσκεται στο SSL Handshake Protocol. Το μήκος κλειδιού στις εκδόσεις που προορίζονται για χρήση στις Η.Π.Α. είναι 128 bits, διαφορετικά το μήκος του κλειδιού είναι 40 bits.

2.7.2 Secure HTTP (S-HTTP)

Το S-HTTP παρέχει περίπου τις ίδιες υπηρεσίες με το SSL αλλά με τελείως διαφορετικό τρόπο. Το S-HTTP σχεδιάστηκε ως μία επέκταση του HTTP το οποίο είναι ένα πρωτόκολλο ερώτησης-απάντησης (request-response transaction protocol). Αυτό το κάνει να διαφέρει ριζικά από το SSL το οποίο είναι πρωτόκολλο προστασίας του session. Ο κύριος ρόλος του S-HTTP είναι να προστατεύει τα requests και τα responses του πρωτοκόλλου.

Οι υπηρεσίες που παρέχονται είναι περίπου ίδιες με το SSL. Επιπλέον παρέχεται και η δυνατότητα χρήσης ηλεκτρονικής υπογραφής, χαρακτηριστικό που συμβάλλει σε περισσότερη ασφάλεια και μη απαρνησιμότητα.

Τα URLs που χρησιμοποιούν το S-HTTP ξεκινούν με "shttp://...".

2.7.3 Secure Electronic Transaction (SET)

Το SET δημιουργήθηκε από τους οργανισμούς Visa και Mastercard και αποτελείται από ένα πρωτόκολλο και προδιαγραφές υλικής υποδομής για την υποστήριξη πληρωμών μέσω πιστωτικών καρτών ως τμήμα των σχετικών υπηρεσιών που χρησιμοποιούν ως μέσο το διαδίκτυο.

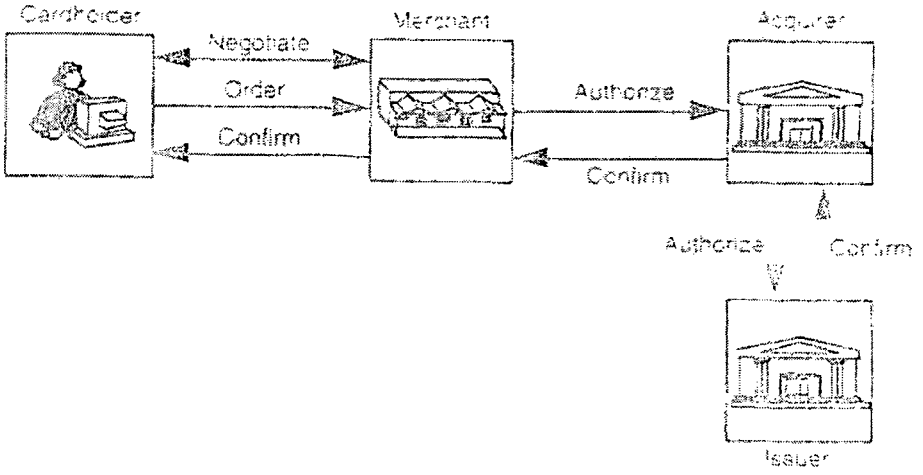
Οι κύριοι συμμετέχοντες στο περιβάλλον του SET είναι:

1. *Ο εκδότης (Issuer):* Είναι ένας οικονομικός οργανισμός που εκδίδει πιστωτικές ή χρεωστικές κάρτες, τυπικά φέρει το όνομα μιας μάρκας (Visa, Mastercard).
2. *Ο κάτοχος(Cardholder):* Είναι ο κάτοχος μιας κάρτας (πιστωτικής ή χρεωστικής), ο οποίος είναι εξουσιοδοτημένος από την τράπεζα να τη χρησιμοποιεί για συναλλαγές.
3. *Ο έμπορος (Merchant):* Είναι ο πωλητής αγαθών, υπηρεσιών ή πληροφοριών που αποδέχεται ηλεκτρονικές πληρωμές.
4. *Ο μεσάζων (Acquirer):* Είναι ένας οικονομικός οργανισμός που υποστηρίζει τους εμπόρους παρέχοντας τις υπηρεσίες για ηλεκτρονικές πληρωμές μέσω πιστωτικών καρτών.

Δευτερεύοντες συμμετέχοντες στην δομή του SET είναι:

5. *Πύλη Πληρωμών (Payment Gateway):* Είναι ένα σύστημα που παρέχει online υπηρεσίες ηλεκτρονικού εμπορίου σε εμπόρους. Τέτοια συστήματα λειτουργούνται είτε από κάποιο μεσάζοντα είτε από κάποιον άλλο που υποστηρίζει κάποιον μεσάζοντα.
6. *Αρχές Πιστοποίησης (Certification Authorities):* Είναι τμήματα της υποδομής που πιστοποιούν τα δημόσια κλειδιά των κατόχων, των εμπόρων, των μεσάζοντων και των πυλών πληρωμών τους.

Εκτελώντας μία ηλεκτρονική συναλλαγή οι πρωτεύοντες συμμετέχοντες αλληλεπιδρούν όπως φαίνεται παρακάτω:



SET: Ηλεκτρονική Συναλλαγή

Όπως φαίνεται, αφού ο κάτοχος της κάρτας συμφωνήσει να κάνει μια αγορά στέλνει μία εντολή πληρωμής στον έμπορο. Ο έμπορος επικοινωνεί online με τον μεσάζοντα διαμέσου της πύλης πληρωμών, συνήθως προωθώντας όλη ή μέρος της εντολής πληρωμής του κατόχου, για να εγκρίνει και επικυρώσει τη συναλλαγή. Η

επικύρωση γίνεται από το μεσάζοντα. Η έγκριση μπορεί να χρειάζεται μία ερώτηση στον εκδότη η οποία γίνεται χρησιμοποιώντας ιδιωτικά δίκτυα και όχι το διαδίκτυο.

Στο περιβάλλον αυτό χρησιμοποιείται τεχνολογία δημοσίου κλειδιού για την υποστήριξη διαφόρων λειτουργιών:

- Κρυπτογράφηση των εντολών πληρωμής με τρόπο που εξασφαλίζει ότι δεν θα διαρρεύσει ο αριθμός της πιστωτικής κάρτας στο διαδίκτυο ούτε εκτίθεται στα συστήματα του έμπορου.
- Αυθεντικοποίηση των κάτοχων στους εμπόρους και μεσάζοντες για την αποφυγή χρήσης κλεμμένων πιστωτικών καρτών.
- Αυθεντικοποίηση των εμπόρων στους κατόχους και τους μεσάζοντες για την αποφυγή περιπτώσεων εικονικών ηλεκτρονικών καταστημάτων που αντικαθιστούν τα πραγματικά και πραγματοποιούν ψευδείς συναλλαγές.
- Αυθεντικότητα των μεσαζόντων στους κατόχους και τους εμπόρους για την αποφυγή περιπτώσεων που κάποιος παριστάνει το μεσάζοντα και έχει

τη δυνατότητα να αποκρυπτογραφήσει την εντολή της ηλεκτρονικής πληρωμής.

- Ακεραιότητα της πληροφορίας συναλλαγής.[1]

2.8 Ασφάλεια Υπολογιστικών Συστημάτων

Όλες οι παραπάνω μέθοδοι προστατεύουν την πληροφορία κατά την μετάδοση της μέσω του διαδικτύου. Η πληροφορία αυτή τελικά αποθηκεύεται σε κάποιο υπολογιστικό σύστημα. Η επίθεση ενός hacker σε ένα τέτοιο σύστημα μπορεί να έχει ως συνέπεια την παραβίασή του και τη γνωστοποίηση ευαίσθητων πληροφοριών στο κοινό. Ακόμα και αν δεν επιτευχθεί αυτό, το σύστημα μπορεί να παύσει να λειτουργεί. Και στις δύο περιπτώσεις η εταιρεία χάνει σημαντικά κέρδη. Είναι προφανές ότι το σύστημα αυτό πρέπει να είναι όσο γίνεται περισσότερο ασφαλές και διαθέσιμο πάντοτε. Παρακάτω παρατίθενται κάποιοι γενικοί κανόνες που ισχύουν σε όλες τις περιπτώσεις που επιδιώκουμε ασφάλεια του υπολογιστικού συστήματος:

- *Φυσική Ασφάλεια:* Ο εξοπλισμός θα πρέπει να είναι σε ξεχωριστούς χώρους που αποκλείουν την είσοδο των μη εξουσιοδοτημένων ατόμων. Ο έλεγχος των ατόμων που έχουν πρόσβαση σε αυτόν θα πρέπει να είναι αυστηρός. Επίσης οι καλωδιώσεις θα πρέπει να είναι προστατευμένες ώστε να προληφθεί η περίπτωση της εγκατάστασης συσκευών υποκλοπής.
- *Ασφάλεια Δικτύου:* Το δίκτυο θα πρέπει να προστατεύεται ώστε να εμποδίζεται η πρόσβαση σε τμήματα και πόρους του υπολογιστικού συστήματος. Ένας τρόπος προστασίας του δικτύου είναι η χρήση firewalls.
- *Έλεγχος Πρόσβασης:* Κάθε εργαζόμενος θα πρέπει να έχει πρόσβαση στην πληροφορία και τους πόρους του συστήματος που χρειάζεται για την

[1] WWW.E-COMMERCE.GR

εργασία του. Αυτό διευκολύνει σημαντικά τους διαχειριστές του υπολογιστικού συστήματος στην ανίχνευση των παραβιάσεων.

- *Κρυπτογράφηση:* Η κρυπτογράφηση εξασφαλίζει την ακεραιότητα και μυστικότητα της πληροφορίας. Αυτό είναι ιδιαίτερα σημαντικό όταν αυτή μεταφέρεται. Όμως και στο περιβάλλον μιας επιχείρησης έχει σημασία όταν πχ η πληροφορία κλαπεί ή η αποτροπή της ανάγνωσης της από μη εξουσιοδοτημένα άτομα.
- *Διαχείριση των κωδικών πρόσβασης:* Οι κωδικοί πρόσβασης που χρησιμοποιούν οι υπάλληλοι μιας επιχείρησης για να αποκτούν πρόσβαση στα υπολογιστικά συστήματά της πρέπει να έχουν ορισμένα χαρακτηριστικά. Πρώτα απ' όλα, πρέπει να επιλέγονται κωδικοί που είναι δύσκολο να τους μαντέψει κάποιος. Τυπικά πρέπει να επιλέγονται λέξεις που δεν υπάρχουν στα λεξικά και έχουν κάποια ιδιαίτερη σημασία για το άτομο που τις χρησιμοποιεί. Επίσης πρέπει να καθορίζεται το ελάχιστο μήκος του κωδικού καθώς και κάθε πότε πρέπει να αλλάζει.
- *Πολιτική Ασφαλείας:* Η πολιτική ασφαλείας είναι ένα έντυπο που συντάσσεται από τους υπεύθυνους πληροφορικής της εκάστοτε επιχείρησης και μοιράζεται σε όλους τους εργαζόμενους. Σε αυτό είναι διατυπωμένο το αμυντικό δόγμα της επιχείρησης. Καθορίζονται τα δικαιώματα, οι υποχρεώσεις και οι περιορισμοί κάθε επιπέδου χρηστών. Προσδιορίζεται η «ορθή» και η «εσφαλμένη» συμπεριφορά. Επίσης αναφέρονται και οι ποινές που θα υπόκειται οποιοσδήποτε παραβιάσει την πολιτική. Ως κείμενο, το έντυπο αυτό θα πρέπει να είναι σύντομο, περιεκτικό και να μπορεί να διαβαστεί από όλους τους υπαλλήλους. Η πολιτική ασφαλείας θα πρέπει να ανανεώνεται τακτικά ώστε να εξασφαλίζεται η απαιτούμενη ασφάλεια.
- *Ασφάλεια Λογισμικού:* Το λογισμικό που χρησιμοποιείται από την επιχείρηση θα πρέπει να είναι δοκιμασμένο για την ασφάλεια που παρέχει. Επίσης θα πρέπει να υπάρχουν περιορισμοί στο λογισμικό που επιτρέπεται ένας χρήστης να εγκαταστήσει στον υπολογιστή του.

- *Σχέδια Αντιμετώπισης Κρίσεων:* Είναι απαραίτητη η σύσταση μιας μικρής ομάδος από ειδικούς η οποία θα αναλάβει να καθορίσει τις πράξεις που πρέπει να γίνουν σε περιπτώσεις φυσικής καταστροφής ή παραβίασης των υπολογιστικών συστημάτων. Πρέπει να περιλαμβάνονται μέτρα ασφαλείας για τα αρχεία εφεδρείας, πότε πρέπει να παίρνονται, από ποιον και που πρέπει να φυλάσσονται. Επίσης πρέπει να προσδιορίζονται και τα άτομα που θα χειριστούν μία τέτοια κρίση.

2.9 Πρακτικά θέματα ηλεκτρονικού εμπορίου

Συνυφασμένα με το ηλεκτρονικό εμπόριο είναι και ζητήματα πρακτικής φύσης, τα οποία ο υποψήφιος ηλεκτρονικός έμπορος θα πρέπει να γνωρίζει προτού περάσει στον κόσμο αυτό. Τα σημαντικότερα παραθέτουμε παρακάτω και αναφέρονται κυρίως σε ζητήματα υποδομής, νομικής φύσης και marketing.

2.9.1 Προϋποθέσεις επιχειρήσεων για εισαγωγή στο χώρο του ηλεκτρονικού εμπορίου

Μία επιχείρηση η οποία θέλει να επεκταθεί στο χώρο του ηλεκτρονικού εμπορίου, οφείλει να κάνει διαρθρωτικές αλλαγές στον τρόπο οργάνωσής της, προκειμένου να αποκομίσει εμφανή οφέλη, οι κυριότερες των οποίων συνίστανται:

1. Διαχείριση και αποθήκευση της κρίσιμης πληροφορίας με ηλεκτρονικά μέσα (πλήρης μηχανοργάνωση - μηχανογράφηση).

2. Ενιαία οργάνωση των βάσεων δεδομένων (ιδιαίτερα σημαντικό για την περίπτωση προμηθευτικών αλυσίδων).
3. Επανασχεδιασμός και τυποποίηση των διαδικασιών της επιχείρησης, λαμβάνοντας υπόψη τις απαιτήσεις του ηλεκτρονικού εμπορίου.

Επιπλέον, προκειμένου να ελέγχονται οι πληρωμές, είναι απαραίτητη η εγκατάσταση αυτοματοποιημένου συστήματος πληρωμών. Για τον σκοπό αυτό, η επιχείρηση πρέπει:

1. Να έρθει σε συμφωνία με χρηματοπιστωτικό οργανισμό (τράπεζα) ή εξειδικευμένο εξωτερικό φορέα.
2. Να ολοκληρώσει το σύστημα λογιστικής / οικονομικής διαχείρισής της

Ως προς τον εξοπλισμό που απαιτείται για τη διεκπεραίωση των διαδικασιών του ηλεκτρονικού εμπορίου, μπορούμε να διακρίνουμε δύο περιπτώσεις:

1. Η εταιρία αναθέτει την συντήρηση του δικτύου εξ ολοκλήρου σε κατάλληλη εταιρία φιλοξενίας δικτυακών τόπων. Η μέθοδος αυτή έχει το πλεονέκτημα ότι η επιχείρηση δεν ανησυχεί για τεχνικά θέματα ούτε για την προμήθεια εξοπλισμού. Πληρώνοντας μία συνδρομή, το ύψος της οποίας ποικίλλει ανάλογα με τις υπηρεσίες, μπορεί να περάσει άμεσα στο χώρο του ηλεκτρονικού εμπορίου. Ωστόσο, μειονέκτημα μπορεί να θεωρηθεί η εξάρτηση από τρίτους για τη λειτουργία του ηλεκτρονικού καταστήματος.

3. Η εταιρία αποφασίζει να προμηθευτεί τον κατάλληλο εξοπλισμό και την τεχνογνωσία. Στην περίπτωση αυτή, μπορούμε να αναφέρουμε τα πιο σημαντικά σημεία όπου πρέπει να εστιαστεί:

Για τον κόμβο World Wide Web:

α) Σχεδίαση του Κέντρου Διαχείρισης Δικτύου (Network Operations Center, NOC) με έμφαση στην ασφάλεια (χρήση firewall), στην αξιοπιστία, στην συντήρηση και στην απόδοση.

β) Ενοικίαση σύνδεσης με το Internet επαρκούς χωρητικότητας, μέσω αξιόπιστου συνδρομητή.

γ) Ενοικίαση πιστοποιητικού εξυπηρετητή (X.509) από παγκοσμίως αναγνωρισμένο Certificate Authority (π.χ. VeriSign), για τις υπηρεσίες που απαιτούν μηχανισμό κρυπτογράφησης δεδομένων (π.χ. SSL ή SET)

2.10 Νομικά θέματα ηλεκτρονικού εμπορίου.

Το εμπόριο γενικά διέπεται από μία πληθώρα νόμων και διατάξεων, προκειμένου να εξασφαλιστεί η ομαλή διεξαγωγή των συναλλαγών. Στην περίπτωση του ηλεκτρονικού εμπορίου, η ταχύτατη εξάπλωσή του σε συνδυασμό με την παγκόσμια εμβέλεια των επιχειρήσεων που δρουν στον τομέα αυτό, έχει φέρει σε αμηχανία τους νομοθέτες πολλών χωρών.

Η Ελλάδα δείχνει να ακολουθεί σωστή πορεία στο θέμα αυτό, καθώς έχει σπεύσει να συμπεριλάβει στην νομοθεσία της αρκετές ρυθμίσεις ώστε να καλύπτονται τα νομικά ζητήματα του ηλεκτρονικού εμπορίου, ωστόσο υπάρχει ακόμα πολύς δρόμος και οι δικαστικοί αγώνες που ενδεχομένως θα διεξαχθούν θα καθορίσουν σε μεγάλο βαθμό τη μελλοντική νομοθεσία.

Αξίζει να σημειωθεί ότι σε πολλές περιπτώσεις η νομοθεσία που εφαρμόζεται για το ηλεκτρονικό εμπόριο αποτελεί αυτούσια ή σχεδόν αυτούσια μεταφορά των νομοθετημάτων που ισχύουν και για το παραδοσιακό εμπόριο. Υπάρχουν ωστόσο και περιπτώσεις όπου νέες, καινοτόμες ιδέες έχουν υιοθετηθεί.

Τα κυριότερα σημεία στα οποία εστιάζεται η συζήτηση για τη νομοθεσία που πρέπει να διέπει το ηλεκτρονικό εμπόριο είναι τα εξής:

1. Δικαιοδοσία, αρμοδιότητα δικαστηρίων
2. Επεξεργασία δεδομένων προσωπικού χαρακτήρα.
3. Πνευματική ιδιοκτησία.
4. Ηλεκτρονική απάτη και πλαστογραφία
5. Διαφήμιση στο Διαδίκτυο.
6. Ονόματα πεδίου (domain names)
7. Φορολογική πολιτική.

Είναι ενδιαφέρον να δούμε καταρχήν μία περίληψη των κυριότερων οδηγιών και ανακοινώσεων της Ευρωπαϊκής ένωσης που αφορούν το ηλεκτρονικό εμπόριο, ειδικότερα τα νομικά θέματα που θίγονται. Με δεδομένα τα παραπάνω θα επιχειρήσουμε να εξάγουμε συμπεράσματα για τα παραπάνω νομικά θέματα που αφορούν το ηλεκτρονικό εμπόριο.

[1]Η Ευρωπαϊκή Ένωση έχει εκδώσει οδηγία «για ορισμένες πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά». Η οδηγία αυτή σκοπό έχει την ομαλή διεξαγωγή του ηλεκτρονικού εμπορίου, μέσα από τη θεσμοθέτηση ενός ενιαίου και σταθερού νομοθετικού πλαισίου σε όλες τις χώρες-μέλη της ΕΕ. Παρακάτω αναφερόμαστε στα άρθρα τα οποία έχουν άμεσο αντίκτυπο στη διεξαγωγή του ηλεκτρονικού εμπορίου. Αξίζει να σημειωθεί ότι καταληκτική ημερομηνία για την ενσωμάτωση της οδηγίας στις εθνικές νομοθεσίες των κρατών μελών είναι η 17η Ιανουαρίου 2002.

Άρθρο 4: *Αρχή της μη αναγκαίας προηγούμενης άδειας.* Η Ευρωπαϊκή ένωση ορίζει ότι η άσκηση επαγγέλματος παροχής υπηρεσιών της κοινωνίας της πληροφορίας δεν απαιτεί και κατά κανέναν τρόπο δεν θα έπρεπε να απαιτεί έκδοση άδειας. Εξαίρεση αποτελούν οι περιπτώσεις που δεν αφορούν αποκλειστικά και μόνο υπηρεσίες της κοινωνίας της πληροφορίας.

[1] http://www.fhilosophe.com/e-commerce.gr

Άρθρο 5: *Γενικές πληροφορίες που πρέπει να παρέχονται.* Η Ευρωπαϊκή Ένωση ορίζει ότι ο φορέας υπηρεσιών της κοινωνίας της πληροφορίας οφείλει να παρέχει άμεση και συνεχή πρόσβαση σε πληροφορίες όπως:

- Επωνυμία του φορέα
- Γεωγραφική διεύθυνση όπου είναι εγκατεστημένος
- Στοιχεία που επιτρέπουν την άμεση επικοινωνία με το φορέα, συμπεριλαμβανομένης της ηλεκτρονικής του διεύθυνσης
- Το εμπορικό ή άλλο δημόσιο μητρώο του φορέα, εφόσον αυτός είναι εγγεγραμμένος σε τέτοιο
- Τα στοιχεία της εποπτικής αρχής, εάν η δραστηριότητα υπόκειται σε τέτοιου είδους έλεγχο

Όσον αφορά τα νομικώς κατοχυρωμένα επαγγέλματα:

- Επαγγελματική ένωση ή παρόμοιο όργανο όπου είναι εγγεγραμμένος ο φορέας,
- Επαγγελματικό τίτλο και τι κράτος μέλος όπου έχει χορηγηθεί,
- Μνεία των επαγγελματικών κανόνων που ισχύουν στο κράτος μέλος εγκατάστασης, καθώς και του τρόπου πρόσβασης σε αυτούς,

- Εάν η δραστηριότητα υπόκειται σε ΦΠΑ, τον αριθμό αναγνώρισης.

Άρθρο 9: *Μεταχείριση ηλεκτρονικών συμβάσεων.* Τα κράτη μέλη πρέπει να έχουν μεριμνήσει ώστε οι συμβάσεις που συνάπτονται με ηλεκτρονικά μέσα να μην θεωρούνται νομικά υποδεέστερες από τις συμβάσεις που συνάπτονται με τον παραδοσιακό τρόπο. Ωστόσο, εξαίρεση προβλέπεται για ειδικές περιπτώσεις συμβάσεων, όπως η μεταβίβαση ακίνητης περιουσίας, οι συμβάσεις που απαιτούν εκ νόμου προσφυγή σε δημόσιες αρχές ή δικαστήρια, συμβάσεις που εμπίπτουν στο

οικογενειακό ή κληρονομικό δίκαιο. Τα κράτη μέλη οφείλουν να ανακοινώνουν τις κατηγορίες συμβάσεων που δεν θεωρούνται έγκυρες ηλεκτρονικά.

Άρθρο 11: *Παραγγελία.* Όταν ένας αποδέκτης υπηρεσίας αναθέτει παραγγελία με ηλεκτρονικά μέσα και εφόσον δεν έχει συμφωνηθεί από τα συμβαλλόμενα μέρη διαφορετικά, ισχύουν οι ακόλουθες αρχές:

- Ο φορέας παροχής των υπηρεσιών οφείλει να αποστέλλει αποδεικτικό της παραλαβής της παραγγελίας του αποδέκτη άμεσα και με ηλεκτρονικά μέσα.
- Η παραγγελία και το αποδεικτικό παραλαβής θεωρείται ότι έχουν παραληφθεί όταν τα μέρη στα οποία απευθύνονται έχουν πρόσβαση σε αυτά.

Ένα σημαντικό κεφάλαιο στη νομοθεσία που αφορά το ηλεκτρονικό εμπόριο και τις ηλεκτρονικές συναλλαγές εν γένει είναι η προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Η φύση του ηλεκτρονικού εμπορίου επιτρέπει την εύκολη συλλογή προσωπικών στοιχείων των καταναλωτών και την ακόμα πιο εύκολη διάδοσή τους. Παρακάτω αναφέρουμε τα κύρια σημεία της ελληνικής και κοινοτικής νομοθεσία σχετικά με το θέμα αυτό.

Ο νόμος 2472/1997 του ελληνικού δικαίου για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα οριοθετεί τη λήψη και επεξεργασία προσωπικών δεδομένων. Ο νόμος έχει συνταχθεί σε συμφωνία με τις οδηγίες 95/46/ΕΚ και 97/66/ΕΚ του Ευρωπαϊκού κοινοβουλίου σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας προσωπικών δεδομένων.

Ο νόμος ορίζει ότι, για να τύχουν νόμιμης επεξεργασίας, τα δεδομένα προσωπικού χαρακτήρα πρέπει:

- Να συλλέγονται κατά τρόπο θεμιτό και νόμιμο για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία εν όψει των σκοπών αυτών.
- Να είναι συναφή, πρόσφορα και όχι περισσότερα από όσα κάθε φορά απαιτείται εν όψει των σκοπών της επεξεργασίας.

- Να είναι ακριβή και, εφόσον χρειάζεται, να υποβάλλονται σε ενημέρωση.
- Να διατηρούνται σε μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων τους μόνο κατά τη διάρκεια της περιόδου που απαιτείται, κατά την κρίση της Αρχής.

Όσον αφορά τις προϋποθέσεις επεξεργασίας τέτοιων δεδομένων, ο νόμος ορίζει ρητά ότι επιτρέπεται όταν το υποκείμενο των δεδομένων έχει δώσει την συγκατάθεσή του. Εξαίρεση αποτελούν ορισμένες ειδικές περιπτώσεις, όπως για παράδειγμα αν ο υποκείμενος τελεί σε φυσική αδυναμία να δώσει τη συγκατάθεση του και η τελευταία είναι απολύτως απαραίτητη.

Πρέπει επίσης να σημειωθεί ότι σύμφωνα με τον ίδιο νόμο ο υπεύθυνος επεξεργασίας υποχρεούται να γνωστοποιήσει εγγράφως στην Αρχή τη σύσταση και λειτουργία αρχείου ή την έναρξη της επεξεργασίας, γνωστοποιώντας τα στοιχεία της επιχείρησης.

Η συλλογή και η επεξεργασία ευαίσθητων δεδομένων απαγορεύεται από το νόμο. Επιτρέπεται μόνο κατ' εξαίρεση και ύστερα από ειδική άδεια της Αρχής, για ορισμένες ειδικές περιπτώσεις. Για να γίνει αυτό πρέπει να εκδοθεί ειδική άδεια από την Αρχή, ορισμένου χρόνου.

Η διαβίβαση δεδομένων προς χώρα της Ευρωπαϊκής Ένωσης είναι ελεύθερη. Το ίδιο ισχύει, έπειτα από έκδοση άδειας, και για χώρες για τις οποίες θεωρείται ότι διατηρείται ένα υψηλό επίπεδο ασφαλείας. Για τις υπόλοιπες χώρες δεν επιτρέπεται η εξαγωγή προσωπικών δεδομένων, εκτός και αν συντρέχουν ιδιαίτεροι λόγοι, όπως η συγκατάθεση του υποκειμένου.

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι απόρρητη και διεξάγεται αποκλειστικά από τον υπεύθυνο επεξεργασίας και από κατάλληλα καταρτισμένα πρόσωπα που τελούν υπό τις εντολές του. Ο υπεύθυνος επεξεργασίας πρέπει να διαφυλάσσει τα δεδομένα από τυχόν απώλεια, κλοπή ή καταστροφή. Αν η επεξεργασία διεξάγεται από πρόσωπο διορισμένο από τον υπεύθυνο επεξεργασίας, πρέπει η ανάθεση να έχει γίνει εγγράφως

Τέλος, μπορούμε να αναφέρουμε τα άρθρα 370Β, 370Γ και 386^{A} του ποινικού κώδικα που αναφέρονται στο ηλεκτρονικό έγκλημα.

Το άρθρο 370Β ορίζει ότι:

Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημόσιου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους, από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους.

Το άρθρο 370Γ αναφέρεται στα εξής:

1. Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι μήνες και χρηματικό πρόστιμο εκατό χιλιάδων έως δύο εκατομμυρίων δραχμών.
2. Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με σήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον δέκα χιλιάδων δραχμών.

Το άρθρο 386Α:

Αφορά την απάτη με υπολογιστή και αναφέρεται ότι όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή, είτε με μη ορθή διαμόρφωση του προγράμματος, είτε με επέμβαση κατά την εφαρμογή του, είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων, είτε με οποιονδήποτε άλλον τρόπο, τιμωρείται με τις ποινές του προηγούμενου άρθρου. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημιάς είναι αδιάφορο αν παθόντες είναι ένα ή περισσότερα άτομα.

Τα παραπάνω άρθρα της ελληνικής νομοθεσίας είναι ενδεικτικά του τι έχει γίνει και του τι δεν έχει ακόμα γίνει για την καταπολέμηση του ηλεκτρονικού εγκλήματος. Είναι ωστόσο δικαιολογημένο να αναμένουμε ραγδαίες εξελίξεις,

κάτι που είναι εμφανές από την κινητικότητα και ευαισθησία που δείχνει η Ευρωπαϊκή Ένωση στον τομέα της νομικής κατοχύρωσης του ηλεκτρονικού εμπορίου και της κοινωνίας της πληροφορίας.

Στο σημείο αυτό και έχοντας κάνει μία ανασκόπηση στην κοινοτική και ελληνική νομοθεσία, είναι χρήσιμο να σχολιάσουμε τα θέματα που θίχτηκαν στην αρχή της παραγράφου, λαμβάνοντας υπόψη και άλλες πηγές.

1. *Δικαιοδοσία, αρμοδιότητα δικαστηρίων.* Το ζήτημα του ποιο δικαστήριο είναι αρμόδιο για την εκδίκαση διακρατικών αντιδικιών που αφορούν το ηλεκτρονικό εμπόριο είναι ευαίσθητο. Η Ευρωπαϊκή Επιτροπή προτείνει την εκδίκαση των υποθέσεων από δικαστήριο της χώρας όπου εδρεύει η εταιρία παροχής ηλεκτρονικών υπηρεσιών που εμπλέκεται στην αντιδικία και όχι στον τόπο όπου έλαβε χώρα το έγκλημα. Αυτή είναι μία γνώμη που φαίνεται να συμμερίζονται και τα αμερικανικά δικαστήρια, όπου το πρόβλημα είναι πιο έντονο λόγω των ανά πολιτεία διαφορετικών νόμων.

2. *Επεξεργασία δεδομένων προσωπικού χαρακτήρα.* Η Ευρωπαϊκή νομοθεσία επιδεικνύει ιδιαίτερη ευαισθησία στον τομέα αυτό, με αποτέλεσμα την έκδοση αρκετών οδηγιών και ανακοινώσεων. Μπορούμε λοιπόν να πούμε ότι το πλαίσιο στο οποίο μπορεί να κινηθεί μία επιχείρηση ηλεκτρονικού εμπορίου σχετικά με τη συλλογή και επεξεργασία στοιχείων των πελατών της είναι αυστηρά καθορισμένο, κάτι που βέβαια την προφυλάσσει από περιττές αντιδικίες.

3. *Πνευματική ιδιοκτησία.* Το γεγονός ότι οι νομοθεσίες ανά τον κόσμο περιέχουν σαφής και δοκιμασμένες διατάξεις που αφορούν την πνευματική ιδιοκτησία, καθιστά εύκολη την τροποποίησή τους ώστε να περιλαμβάνουν και θέματα ηλεκτρονικής πνευματικής ιδιοκτησίας.

4. *Ηλεκτρονική απάτη και πλαστογραφία.* Στον τομέα αυτό οι εθνικές και η κοινοτική νομοθεσία βρίσκονται σε πρώιμο στάδιο. Αιτία είναι οι νέες

μορφές εγκλήματος που αφορούν το ηλεκτρονικό εμπόριο, όπως πλαστογραφία της ψηφιακής υπογραφής, υποκλοπή αριθμών πιστωτικής κάρτας και κωδικών πρόσβασης (passwords) κ.α. Ωστόσο υπάρχει αρκετή κινητικότητα στο χώρο, ώστε να αναμένουμε την αποσαφήνιση των ποινικών ευθυνών των εγκληματιών και την επιβολή κοινής νομοθεσίας από τα κράτη-μέλη της Ευρωπαϊκής Ένωσης.

5. *Διαφήμιση στο Διαδίκτυο.* Αυτό είναι ένα θέμα με το οποίο λίγο έχουν ασχοληθεί οι νομοθεσίες των κρατών, κυρίως γιατί προς το παρόν τα προβλήματα είναι περιορισμένης έκτασης, κάτι που αναμένεται να αλλάξει στο μέλλον. Αναφερόμαστε στην περίπτωση της παραπλανητικής, αθέμιτης και συγκριτικής διαφήμισης. Η τάση που φαίνεται να επικρατεί είναι η επέκταση των νόμων που ισχύουν για τις περιπτώσεις αυτές της συμβατικής διαφήμισης και στην ηλεκτρονική. Να σημειωθεί ότι η χώρα μας είναι η μόνη ευρωπαϊκή χώρα που επιτρέπει τη συγκριτική διαφήμιση. Θα πρέπει επίσης να προβλεφθούν διατάξεις και για την περίπτωση της ανεπιθύμητης διαφημιστικής ηλεκτρονικής αλληλογραφίας (junk email, spam email).

6. *Ονόματα πεδίου.* Η αυξανόμενη εμπορική χρήση του Διαδικτύου έχει οδηγήσει σε ένα φαινόμενο κατάχρησης ονομάτων πεδίου (domain names). Συγκεκριμένα, μία επιχείρηση της οποίας τα διακριτικά στοιχεία και η επωνυμία είναι ήδη γνωστά στον εμπορικό κόσμο και τι καταναλωτικό κοινό, συχνά όταν επιχειρεί να περάσει στο χώρο του ηλεκτρονικού εμπορίου ανακαλύπτει ότι το αντίστοιχο όνομα είναι κατειλημμένο. Ο κάτοχος του ονόματος ζητάει τότε υπέρογκα ποσά για να το παραχωρήσει.

7. *Φορολογία.* Τέλος, πολύ συζήτηση έχει γίνει για το θέμα της φορολογίας στο ηλεκτρονικό εμπόριο. Η άποψη που επικρατεί υποστηρίζει την μη προνομιακή μεταχείριση του ηλεκτρονικού εμπορίου σε σχέση με το συμβατικό και το αντίθετο. Να επισημάνουμε ότι η παροχή υπηρεσιών μέσω του Διαδικτύου στο χώρο της Ευρωπαϊκής Ένωσης προς το παρόν δεν

φορολογείται, δεν υπόκειται δηλαδή στο ΦΠΑ, ούτε χρειάζεται η έκδοση ειδικής άδειας.

Ως ειδική περίπτωση ηλεκτρονικού εμπορίου θα μπορούσαμε να θεωρήσουμε και την τηλεϊατρική, όπου πλέον ως τέτοιο θεωρούμε την παροχή ιατρικών υπηρεσιών με ηλεκτρονικό μέσο. Το νομικό τοπίο στον τομέα της τηλεϊατρικής είναι ακόμα πιο περίπλοκο και θολό. Ενδεικτικά θα πούμε ότι ακόμα και χώρες όπως οι Η.Π.Α., όπου το Διαδίκτυο χρησιμοποιείται ευρύτατα ως εμπορικό μέσο, οι νομοθεσία ελάχιστα προβλέπει για την περίπτωση της τηλεϊατρικής. Πιο σημαντικά σημεία σύγχυσης είναι το ζήτημα αρμοδιότητας δικαστηρίων για την εκδίκαση υποθέσεων, το ζήτημα έκδοσης άδειας και το ζήτημα του τι θεωρείται και τι όχι άσκηση τηλεϊατρικής. Αναφερόμενοι στα αμερικανικά δεδομένα, όπου έχουν γίνει και τα περισσότερα βήματα, μπορούμε να υπογραμμίσουμε τα εξής:

- Αρμόδιο δικαστήριο για την εκδίκαση υποθέσεων τηλεϊατρικής είναι το δικαστήριο που βρίσκεται στην πολιτεία όπου εδρεύει ο κατηγορούμενος ιατρός.
- Το ζήτημα της έκδοσης άδειας είναι ακόμη ρευστό. Δηλαδή, ένας γιατρός που έχει εκδώσει άδεια σε μία πολιτεία μπορεί να εξασκεί το επάγγελμά του και σε άλλη πολιτεία; Και αν ναι, υπό τι καθεστώς; Το ζήτημα αυτό είναι υπό συζήτηση και αναμένουμε να δούμε τις εξελίξεις.
- Μέχρι πρότινος ένας γιατρός ζητούσε τη βοήθεια ενός συναδέλφου του μέσω του τηλεφώνου ή του φαξ, χωρίς κανείς να δώσει σημασία. Σήμερα, αν το ίδιο σενάριο επαναληφθεί με χρήση του Διαδικτύου, τότε είναι πολύ πιθανό να θεωρηθεί ότι έχουμε εξάσκηση τηλεϊατρικής και επομένως η συμβουλή αυτή εμπίπτει στη νομοθεσία και τις ευθύνες που διέπουν αυτή.

Τα ζητήματα αυτά είναι πολύ ευαίσθητα και με τον καιρό θα καθοριστεί σε παγκόσμιο επίπεδο τη νομοθεσία που θα τα διέπει.[1]

[1] http://www.go-online.gr/files/document/e-ELLADA.pdf

ΚΕΦΑΛΑΙΟ 3

ΔΗΜΙΟΥΡΓΙΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΚΑΤΑΣΤΗΜΑΤΟΣ ΕΛΛΑΔΑ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

3.1 Σχεδίαση ηλεκτρονικού καταστήματος

Η περίπτωση του ηλεκτρονικού καταστήματος είναι μια ιδιαίτερη περίπτωση δικτυακού τόπου. Αποτελεί τη «βιτρίνα» της εταιρείας που ανήκει αφού μέσω αυτού προωθούνται τα προϊόντα προς πώληση. Επίσης απευθύνεται σε ένα ευρύ κοινό που κατά μέσο όρο δεν έχει εξοικείωση με τους ηλεκτρονικούς υπολογιστές και την πληροφορική. Για τους λόγους αυτούς ο σχεδιασμός του είναι ιδιαίτερα σημαντικός αφού από την επιτυχία του εξαρτάται πολλές φορές και η βιωσιμότητα της επιχείρησης. Τα λάθη δεν συγχωρούνται αφού αυτό μεταφράζεται σε απώλεια πελατών, άρα και κερδών.

Παρακάτω θα παρουσιάσουμε μία γενική μεθοδολογία στο συνολικό σχεδιασμό του ηλεκτρονικού καταστήματος. Επίσης παρουσιάζονται ορισμένοι γενικοί κανόνες σχεδίασης ενός ηλεκτρονικού καταστήματος από την πλευρά της ευχρηστίας και της φιλικότητας προς το χρήστη.

3.1.1 Γενική Μεθοδολογία

Χρήσιμες συμβουλές για την γραφική σχεδίαση ιστοσελίδων

• Τοποθετήστε τα πιο σημαντικά στοιχεία στην κορυφή της σελίδας, όπως είναι ο τίτλος, ο σκοπός της σελίδας και η ημερομηνία

• Καθορίστε μια αισθητική ιεραρχία

• Κατευθύνετε το μάτι

• Περιορίστε το γραφικό περισπασμό

• Κρατήστε μια σταθερή δομή

• Γράφετε καθαρά και συνοπτικά

• Κάντε τα κείμενά σας να διαβάζονται «με μια ματιά». Χρησιμοποιήστε τίτλους και θεματικές λίστες

• Σχεδιάστε προσεκτικά την πλοήγηση

• Αποφύγετε κείμενα και γραφικά που αναβοσβήνουν

• Παρέχετε διεύθυνση e-mail για άμεση επικοινωνία σε μορφή hypertext

• Δώστε πρόσβαση σε όσους περισσότερους χρήστες μπορείτε, συμπεριλαμβανομένων και εκείνων με αργές συνδέσεις ή browsers κειμένου.

➢ Η αισθητική ιεραρχία

Η βασική δουλειά κατά το σχεδιασμό της δομής των ιστοσελίδων σας είναι η δημιουργία μιας σταθερής ιεραρχίας, όπου θα δίνεται έμφαση στα βασικά στοιχεία και το περιεχόμενο θα οργανώνεται λογικά με προβλεπόμενο τρόπο. Ο τρόπος που θα παρεμβάλλονται οι πληροφορίες θα πρέπει να οδηγεί το μάτι του αναγνώστη μέσα στη σελίδα και να το κατευθύνει στο περιεχόμενο.

Αυτό που χρειάζεστε είναι μια ισορροπία, η οποία προσελκύει το μάτι και δημιουργεί μια οπτική αντίθεση.

Οι αναλογίες και η καταλληλότητα είναι τα κλειδιά στον επιτυχημένο σχεδιασμό, που όμως εξαρτάται άμεσα από τους στόχους που θέλετε να επιτύχετε, από το κοινό στο οποίο απευθύνεστε και από τη φύση του περιεχομένου σας.

➢ Κατευθύνοντας το μάτι

Ο τρόπος με τον οποίο διαβάζει το μάτι, τουλάχιστον στο δυτικό κόσμο, είναι αριστερά προς τα δεξιά. Για το λόγο αυτό, ο οπτικός άξονας που δημιουργεί ο τρόπος ανάγνωσης χρησιμοποιείται ως βάση για το γραφικό σχεδιασμό των γραπτών εκδόσεων. Το πάνω μέρος της σελίδας είναι το πιο κυρίαρχο κομμάτι και ιδιαίτερα στην περίπτωση των ιστοσελίδων, μια και το πάνω μέρος μιας ιστοσελίδας είναι το κομμάτι που βλέπουν αμέσως και περισσότερο οι χρήστες μέσα από τις οθόνες τους.

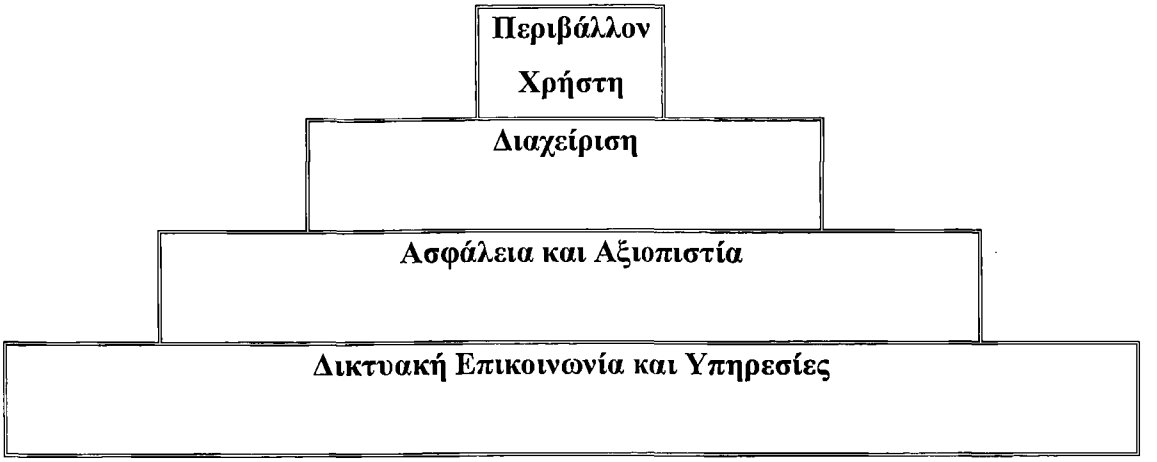
➢ Ο γραφικός περισπασμός

Χρησιμοποιήστε οριζόντιες γραμμές,εικονίδια και άλλα οπτικά σύμβολα, κατάλληλα και με φειδώ. Διαφορετικά, η συχνή αυτή χρήση αυτών των στοιχείων θα υπερφορτώσει τη σελίδα και θα επιφέρει σύγχυση στην κατανόηση του περιεχομένου.

➢ Κρατείστε σταθερή δομή

Δημιουργήστε και διατηρήστε ένα πλάνο της δομής, με το οποίο θα χειρίζεστε κείμενο και γραφικά. Επίσης, επιλέξτε το ύφος που θέλετε να χαρακτηρίζει τις σελίδες σας, αλλά και ένα κατάλληλο θεματικό κανόνα. Στη συνέχεια ακολουθήστε τη δομή πιστά. Μην ανησυχείτε μήπως η επανάληψη θα είναι βαρετή. Αντιθέτως θα δώσει στις σελίδες σας ένα προσωπικό χαρακτήρα και οι επισκέπτες σας θα θυμούνται το κατάστημά σας πιο εύκολα.

Παρακάτω φαίνεται σχηματικά η στρατηγική δημιουργίας ενός ηλεκτρονικού καταστήματος.



- *1ο Επίπεδο:*

Δικτυακή Επικοινωνία και Υπηρεσίες: Στόχος του σταδίου αυτού είναι η απόκτηση του εξοπλισμού που θα εξασφαλίζει ποιότητα, συνέπεια και αξιοπιστία των υπηρεσιών, καθώς επίσης και υψηλή διαθεσιμότητα του συστήματος.

- *2ο Επίπεδο:*

Ασφάλεια και αξιοπιστία: Στόχος του σταδίου αυτού είναι η προστασία και η εξασφάλιση του απορρήτου των συναλλαγών και των δεδομένων. Στο επίπεδο αυτό ανήκουν οι ενέργειες για πιστοποίηση του ηλεκτρονικού καταστήματος, η προμήθεια των συστημάτων κρυπτογράφησης και ασφαλών συναλλαγών.

- *3ο Επίπεδο:*

Διαχείριση: Στόχος είναι η διαμόρφωση του συστήματος και των παρεχόμενων υπηρεσιών, συντήρηση, έλεγχος, αναβάθμιση του εξοπλισμού.

- *4ο Επίπεδο:*

Περιβάλλον χρήστη: Το στάδιο αυτό περιλαμβάνει τη δημιουργία του περιβάλλοντος αλληλεπίδρασης του συστήματος με το χρήστη. Σ' αυτό το στάδιο μεταξύ των άλλων περιλαμβάνονται οι εφαρμογές υποβολής των παραγγελιών, έκδοσης αποδείξεων και η παροχή βοήθειας.

Το σημαντικότερο τμήμα από τα παραπάνω είναι το 4°. Είναι αυτό που φαίνεται προς τον «έξω κόσμο» και βλέπει ο πελάτης. Βέβαια και τα άλλα τμήματα δεν είναι ασήμαντα, αποτελούν τη βάση για την ορθή λειτουργία του ηλεκτρονικού καταστήματος και είναι απαραίτητα. Για το λόγο αυτό αναλύεται περαιτέρω το 4° επίπεδο κυρίως από την πλευρά της φιλικότητας και ευχρηστίας προς τον πελάτη.

3.1.2 Ευχρηστία και Φιλικότητα

Έχει παρατηρηθεί ότι αν ένας πελάτης δυσαρεστηθεί από ένα κατάστημα πολύ δύσκολα θα το επισκεφτεί ξανά. Το ίδιο ισχύει και για τα ηλεκτρονικά καταστήματα. Όπως ο πελάτης πρέπει να νιώθει άνετα και να έχει εμπιστοσύνη στο κατάστημα που εκτελεί τις αγορές του, έτσι πρέπει να νιώθει και στο ηλεκτρονικό.

Υπάρχουν ορισμένες παράμετροι που συμβάλλουν στην δημιουργία του κλίματος αυτού που θα ωθήσει τον πελάτη να πραγματοποιήσει τις αγορές του από το Χ κατάστημα και να απορρίψει τα υπόλοιπα. Αυτές είναι:

1. *Υποστήριξη πελατών:* Το ηλεκτρονικό κατάστημα πρέπει να παρέχει τις ανάλογες υπηρεσίες που θα παρείχε και ένα συμβατικό κατάστημα.
    - Θα πρέπει να δίνεται η δυνατότητα στους πελάτες να διατυπώνουν τις απορίες τους και να παίρνουν απάντηση είτε μέσω E-mail, είτε τηλεφωνικά..
    - Πρέπει να προβλεφθεί η περίπτωση κάποιος πελάτης να έχει ξεχάσει τον κωδικό πρόσβασης. Με κάποιο τρόπο το πρόβλημα πρέπει να λύνεται, είτε με αποστολή του κωδικού μέσω e-mail, είτε τηλεφωνικά.
    - Τα μηνύματα που εμφανίζονται πρέπει να είναι απλά, κατανοητά και να μην περιέχουν τεχνικούς όρους που θα μπορούσαν να προκαλέσουν σύγχυση στον πελάτη.

- Παροχή βοήθειας σχετικά με τις διαδικασίες επιλογής, παραγγελίας, πληρωμής και αποστολής των προϊόντων.

2. *Εμπιστοσύνη:* Το ηλεκτρονικό κατάστημα πρέπει να δίνει στον πιθανό πελάτη το αίσθημα της ασφάλειας και ότι η παραγγελία του θα διεκπεραιωθεί χωρίς απρόοπτα.
   - Είναι απαραίτητο να αναφέρονται ιστορικά στοιχεία του καταστήματος και το έμψυχο υλικό του. Επίσης αν έχει και φυσική υπόσταση, δηλαδή υπάρχει και ως συμβατικό κατάστημα θα πρέπει να αναφέρεται η διεύθυνσή του και ο τρόπος επαφής, όπως τηλέφωνα και e-mails.
   - Ενημέρωση των χρηστών για τον εξοπλισμό ασφάλειας που χρησιμοποιείται για τις χρηματικές συναλλαγές. Πρέπει επίσης να αναφέρεται και η πιστοποίηση του καταστήματος από διεθνείς οργανισμούς.
   - Πρέπει να υπάρχει σαφής θέση του καταστήματος για τη χρήση των προσωπικών δεδομένων. Ερωτήματα σχετικά με τη διάθεση των στοιχείων σε τρίτους θα πρέπει να απαντώνται με σαφήνεια.

3. *Αποτελεσματική Πλοήγηση:* Η πλοήγηση στο ηλεκτρονικό κατάστημα θα πρέπει να είναι απλή, ώστε να απευθύνεται και σε άπειρους χρήστες, αλλά και αποτελεσματική ώστε η εύρεση των προϊόντων να επιτυγχάνεται σύντομα. Ο πελάτης δεν θα πρέπει να έχει την αίσθηση ότι χρονοτριβεί κάνοντας τις αγορές του ηλεκτρονικά.
   - Σημαντικότατο ρόλο παίζει η ευκολία πρόσβασης στο ηλεκτρονικό κατάστημα. Το URL του θα πρέπει να είναι απλό, σχετικό με τα προϊόντα που πωλούνται, ώστε να είναι εύκολο από τους πελάτες να το θυμούνται. Τις περισσότερες φορές η καλύτερη λύση είναι το URL να περιλαμβάνει την επωνυμία της επιχείρησης, πχ www.plaisio.gr

- Σωστή αρχιτεκτονική του καταστήματος και κατηγοριοποίηση των προϊόντων. Η κατηγοριοποίηση των προϊόντων θα πρέπει να γίνεται με λογικό τρόπο, όπως περίπου θα γινόταν και σε ένα συμβατικό κατάστημα.
- Ένα πολύ χρήσιμο εργαλείο σε ένα ηλεκτρονικό κατάστημα είναι μία μηχανή αναζήτησης. Αυτό επιτρέπει στους πελάτες να βρουν πολύ γρήγορα αυτό που ψάχνουν. Η παρουσίαση των αποτελεσμάτων θα πρέπει να γίνεται όπως επιθυμεί ο χρήστης, πχ ανάλογα με την τιμή, την επωνυμία κλπ. Η επιλογή της χρήσης της μηχανής αναζήτησης θα πρέπει να είναι σε εμφανές σημείο του ηλεκτρονικού καταστήματος.
- Ο σχεδιασμός του ηλεκτρονικού καταστήματος θα πρέπει να είναι καλαίσθητος χωρίς υπερβολικά έντονα χρώματα. Οι γραμματοσειρές που χρησιμοποιούνται θα πρέπει να είναι ευδιάγνωστες. Τέλος η υλοποίηση του ηλεκτρονικού καταστήματος θα πρέπει να είναι συμβατή και με τον Internet Explorer και τον Netscape Navigator.

4. *Πληροφορίες Προϊόντων:* Πρέπει να παρέχονται όλες οι πληροφορίες που αφορούν το προϊόν, ώστε να πείθεται ο πελάτης ότι είναι αυτό που επιθυμεί πραγματικά.
   - Είναι αναγκαίο να υπάρχει μια συνοπτική περιγραφή του προϊόντος που να αναφέρει τα κύρια χαρακτηριστικά του και σε ποια σημεία πλεονεκτεί έναντι των άλλων. Αν ένας χρήστης χρειάζεται λεπτομερέστερες πληροφορίες πρέπει να παρέχονται και αυτές. Τα στοιχεία αυτά πρέπει να είναι ακριβή.
   - Σημαντικό είναι να υπάρχει και μια φωτογραφία, ώστε ο πελάτης να βλέπει τι αγοράζει. Η φωτογραφία δεν πρέπει να είναι υπερβολικά μεγάλη, ώστε να είναι χρονοβόρα η φόρτωσή της.

- Το κόστος του προϊόντος θα πρέπει να βρίσκεται σε εμφανές σημείο και να είναι ξεκάθαρο σε τι νόμισμα βρίσκεται και αν συμπεριλαμβάνονται στην τιμή και τα έξοδα αποστολής.
- Η διαθεσιμότητα του προϊόντος πρέπει να γίνεται γνωστή στον πελάτη. Είναι σημαντικό να κρατούνται οι συμφωνίες που γίνονται.
- Χρήσιμο είναι επίσης να προτείνονται στον πελάτη και εναλλακτικά προϊόντα ή προϊόντα που πιθανόν να τον ενδιαφέρουν και να του δίνεται η δυνατότητα να τα συγκρίνει. Αυτό πρέπει να γίνεται με τέτοιο τρόπο που να μην ενοχλείται, αν δε το επιθυμεί.

5. *Πραγματοποίηση της αγοράς:* Το σημαντικότερο τμήμα της συναλλαγής που μόνο ένα μικρό ποσοστό των πελατών φτάνει σε αυτό.
   - Ο πελάτης πριν επικυρώσει την παραγγελία του πρέπει να είναι σίγουρος για το τελικό κόστος, τον τρόπο παράδοσης και το χρονικό διάστημα που θα γίνει αυτό.
   - Θα πρέπει να υπάρχουν δύο τρόποι επιβεβαίωσης της παραγγελίας. Ο ένας είναι μέσω των ιστοσελίδων του ηλεκτρονικού καταστήματος και ο δεύτερος είναι μέσω ενός e-mail που θα περιέχει τα προϊόντα που παραγγέλθηκαν και τον κωδικό επιβεβαίωσης.
   - Χρήσιμο είναι να υποστηρίζεται η παρακολούθηση της πορείας της παραγγελίας. Πολλά ηλεκτρονικά καταστήματα συνάπτουν συμφωνίες με εταιρείες courier και παρέχουν τη δυνατότητα στους πελάτες τους να παρακολουθούν την πορεία του πακέτου τους.

3.2 Κατάλογοι προϊόντων On-Line

Ένας κατάλογος σε περίοπτη θέση επιτρέπει στους πελάτες να δουν ποια αγαθά ή υπηρεσίες μπορούν να διαλέξουν. Επιτρέπει επίσης διαδραστική επαφή, καθώς ο πελάτης μπορεί να αναζητήσει τα χαρακτηριστικά των προϊόντων που τον ενδιαφέρουν για την ενημέρωσή του.

Ο κατάλογος αντί να παραμένει αυτόνομος μπορεί να συνδεθεί και με άλλες υπηρεσίες του καταστήματος, ώστε να υπάρχει επικοινωνία μεταξύ των απαραίτητων πληροφοριών.

Υπάρχουν προγράμματα λογισμικού, τα οποία συλλέγουν αναλυτικές πληροφορίες σχετικά με την κίνηση των πελατών μέσα σε ένα κατάστημα, δηλαδή τις σελίδες που επισκέπτονται, τις ακριβείς διαδρομές που διαγράφουν και τον χρόνο που παραμένουν σε καθεμιά από τις σελίδες αυτές.

Έτσι, μπορούμε να χρησιμοποιήσουμε αυτές τις πληροφορίες, για να προσδιορίσουμε και να βελτιώσουμε τις γνώσεις μας σχετικά με τους πελάτες και να δημιουργήσουμε κατηγορίες προφίλ των πελατών. Κατ' επέκταση, γνωρίζοντας τις συνήθεις διαδρομές που διανύουν οι επισκέπτες, μπορούμε να βελτιώσουμε και την πλοήγησή τους μέσα στο κατάστημα, ώστε να τους επιτρέπεται να βρίσκουν πιο εύκολα αυτό που επιθυμούν και να κάνουν αγορές με λιγότερο κόπο.

Οι επιχειρήσεις πρέπει να αποφεύγουν τις άσκοπες ή αδιάκριτες ερωτήσεις που κουράζουν ή ενοχλούν τους πελάτες τους.

3.3 Ελλάδα και ηλεκτρονικό εμπόριο

3.3.1 Παραδείγματα ελληνικών δικτυακών τόπων για ηλεκτρονικό εμπόριο

Σήμερα παρατηρείται μια αυξημένη κινητικότητα στο συγκεκριμένο χώρο. Συνεχώς δημιουργούνται καινούρια ηλεκτρονικά καταστήματα για κάθε κατηγορία προϊόντων. Ορισμένα από αυτά αποτελούν χαρακτηριστικά παραδείγματα λόγω της πρωτοπορίας τους, της πληρότητας και της ποιότητας υπηρεσιών που προσφέρουν.

3.3.2 Πλαίσιο Α.Ε.

Ένα από τα πρώτα ηλεκτρονικά καταστήματα είναι αυτό της εταιρίας Πλαίσιο Α.Ε που εμπορεύεται είδη γραφείου και Η/Υ. Επίσης είναι και ένα από τα πιο πλήρη. Στο ηλεκτρονικό κατάστημα βρίσκονται σχεδόν όλα τα είδη που υπάρχουν και στο συμβατικό κατάστημα. Επίσης είναι σύμφωνο με αρκετούς από τους κανόνες ευχρηστίας και φιλικότητας που αναφέρθηκαν στην παράγραφο 3.1.2 Η πλοήγηση στο κατάστημα είναι εύκολη, ο χρήστης μπορεί να βρει γρήγορα αυτό που θέλει, δίνεται ιδιαίτερη σημασία στην τεχνική υποστήριξη των πελατών και αναφέρεται η πιστοποίηση από τη Verisign. Για τα περισσότερα προϊόντα παρέχεται φωτογραφία, ενώ υπάρχει και η δυνατότητα σύγκρισης αυτών.[1]

[1] http://www.plaisio.gr

3.3.3 Παπασωτηρίου Α.Ε

Και αυτό το κατάστημα είναι από τα πρώτα που δημιουργήθηκαν. Το περιεχόμενό του είναι πλήρες, αφού όλα τα βιβλία είναι διαθέσιμα μέσω του ηλεκτρονικού καταστήματος. Ακολουθεί και αυτό τους κανόνες ευχρηστίας και φιλικότητας. Αξίζει να αναφερθεί ότι στις ηλεκτρονικές αγορές προσφέρεται έκπτωση 15% και η αποστολή είναι δωρεάν εντός της Ελλάδος.[1]

3.3.4 Oops

Και αυτό είναι ένα πολυκατάστημα που δημιουργήθηκε πρόσφατα από την εταιρία multirama Γερμανός. Μέσω αυτού μπορεί κανείς να κάνει τις αγορές του από γνωστά καταστήματα που περιέχουν προϊόντα όλων των κατηγοριών.κ.α[2]

3.4 Κρατικές πρωτοβουλίες για το ηλεκτρονικό εμπόριο

Πρόσφατα το κράτος ανέλαβε πρωτοβουλίες για το ηλεκτρονικό εμπόριο. Το σημαντικότερο βήμα είναι η σύσταση της *Εθνικής Επιτροπής Ηλεκτρονικού Εμπορίου* από το Υπουργείο Ανάπτυξης.

Στόχοι και σκοποί της επιτροπής είναι:

1. Ο σχεδιασμός της εθνικής στρατηγικής σε θέματα Ηλεκτρονικού Εμπορίου, η κατάρτιση του αναγκαίου θεσμικού πλαισίου και η διατύπωση συγκεκριμένων προτάσεων προς την Ελληνική

[1] http://www.papasotiriou.gr
[2] http://www.oops.gr

κυβέρνηση, όλους τους εμπλεκόμενους φορείς και τα αρμόδια Υπουργεία.

2. Η παρακολούθηση όλων των εθνικών πρωτοβουλιών και προγραμμάτων χρηματοδότησης, ερευνητικών, κλπ. που σχετίζονται με θέματα Ηλεκτρονικού Εμπορίου.

3. Η γνωμοδότηση επί της σκοπιμότητας έργων υποδομής Ηλεκτρονικού Εμπορίου.

4. Η προώθηση (σε συνεργασία με άλλους φορείς) του Ηλεκτρονικού Εμπορίου στο ελληνικό περιβάλλον και στην προετοιμασία και επεξεργασία του αναγκαίου θεσμικού πλαισίου για την χρήση του.

5. Η προώθηση της χρήσης εφαρμογών Ηλεκτρονικού Εμπορίου στο Ελληνικό Δημόσιο, στον συντονισμό και την υποστήριξη της εκπροσώπησης της χώρα μας σε διεθνείς οργανισμούς και διεθνείς πρωτοβουλίες, που αφορούν θέματα Ηλεκτρονικού Εμπορίου καθώς και ανάλογες εθνικές πρωτοβουλίες άλλων κυβερνήσεων.
6. Η συμμετοχή σε όλα τα κυβερνητικά όργανα και επιτροπές που χειρίζονται θέματα Ηλεκτρονικού Εμπορίου (θεσμικά, υποδομής κλπ).

Άλλη μια κρατική προσπάθεια που αξίζει αναφοράς είναι το πρόγραμμα «ΔΙΚΤΥΩΘΕΙΤΕ» του Υπουργείου Ανάπτυξης. Έχει σκοπό την εξοικείωση 50.000 μικρομεσαίων επιχειρήσεων με την ψηφιακή οικονομία, την αξιοποίηση των δυνατοτήτων και των ευκαιριών που προσφέρει το Διαδίκτυο και γενικότερα, την παρακίνηση των επιχειρηματιών για την αξιοποίηση των νέων τεχνολογιών. Το Πρόγραμμα καλύπτει όλη τη χώρα, δηλαδή και τις 13 περιφέρειες, υλοποιείται την περίοδο 2000-2003 και έχει συνολικό προϋπολογισμό 40 δις δρχ. Ο σχετικός δικτυακός τόπος είναι το: www.go-online.gr

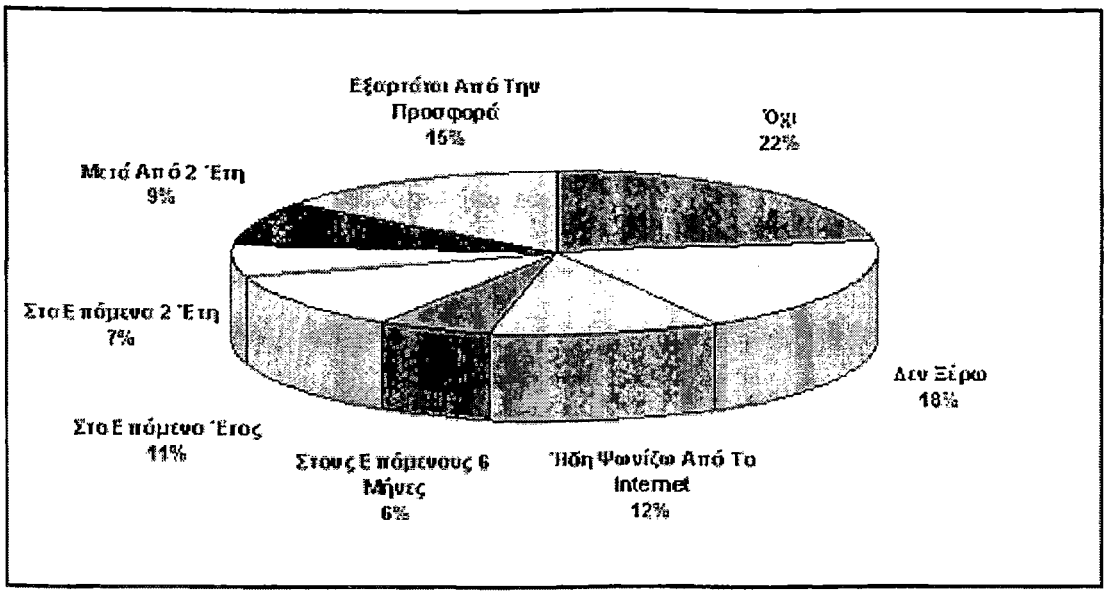
3.5 Στατιστικά στοιχεία της χρήσης του ηλεκτρονικού εμπορίου στην Ελλάδα

Χρήσιμο είναι να εξεταστεί ποιοι είναι αυτοί που χρησιμοποιούν το internet και πραγματοποιούν αγορές μέσω αυτού. Αυτό βοηθάει στον καλύτερο σχεδιασμό των ηλεκτρονικών καταστημάτων με περισσότερα προϊόντα, αναβαθμισμένες υπηρεσίες και προσαρμοσμένο περιβάλλον χρήσης. Με αυτό το σκοπό παρατίθεται η παρακάτω μελέτη από το Οικονομικό Πανεπιστήμιο Αθηνών.

3.5.1 Ο Έλληνας Internet καταναλωτής

Σύμφωνα με τα αποτελέσματα της έρευνας του ΟΠΑ, οι υπάρχοντες Internet καταναλωτές αντιστοιχούν στο 20% των συνολικών χρηστών Internet στην Ελλάδα. Για το 2001 αναμένεται ότι ο αριθμός αυτός θα διπλασιαστεί, οπότε θα υπάρχουν περισσότεροι από 500.000 Έλληνες που χρησιμοποιούν το Internet για αγορές.

Το προφίλ των καταναλωτών που ήδη χρησιμοποιούν το Internet για τις αγορές τους είναι σε μεγάλο βαθμό αναμενόμενο. Πρόκειται για άτομα από 25 έως 44 ετών, με την μεγαλύτερη συγκέντρωση στο ηλικιακό γκρουπ 25 με 34. Επιπλέον, είναι άτομα με υψηλή μόρφωση (δηλαδή τουλάχιστο ένα πανεπιστημιακό πτυχίο). Οι υπάρχοντες Internet καταναλωτές έχουν πρόσβαση στο διαδίκτυο τόσο στην δουλειά όσο και στο σπίτι και έχουν τις αγορές από ηλεκτρονικά καταστήματα σαν πρωταρχικό λόγο χρήσης του Internet. Πρόκειται για άτομα με μεσαία έως και υψηλά εισοδήματα, με την μεγαλύτερη συγκέντρωση στα άτομα με μηνιαία εισοδήματα μεγαλύτερα των 1.500€. Τέλος, η οικογενειακή κατάσταση δεν παρουσιάζεται να επηρεάζει ιδιαίτερα την επιλογή του Internet σαν κανάλι αγορών, παρά το γεγονός ότι οι έγγαμοι καταναλωτές δείχνουν μία ελαφρώς μεγαλύτερη τάση.

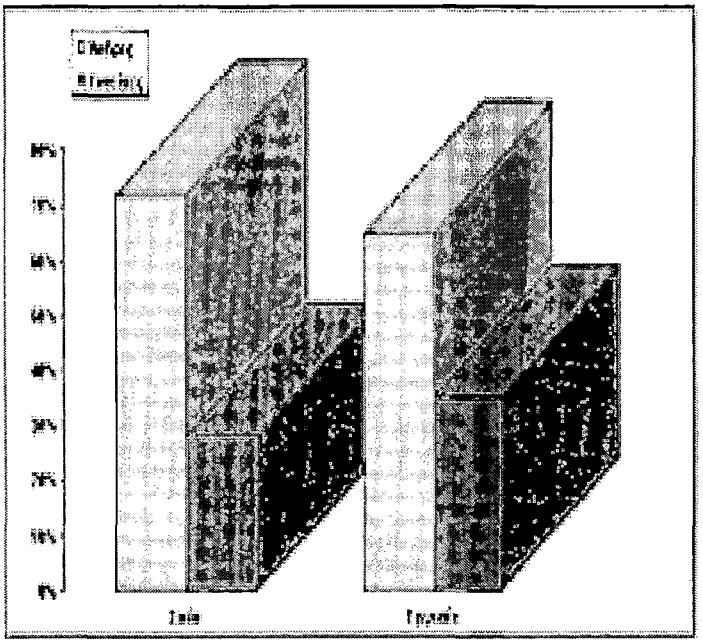


3.5.2 Οι καταναλωτές της νέας δεκαετίας.

Οι καταναλωτές που ήδη αγοράζουν από το διαδίκτυο αποτελούν, όπως αναφέρθηκε προηγουμένως, μόλις το 20% των συνολικών χρηστών Internet στην Ελλάδα. Από τα αποτελέσματα της έρευνας προκύπτει ότι περίπου 17% των υπαρχόντων χρηστών Internet θα αρχίσουν να χρησιμοποιούν το μέσο αυτό για αγορές. Οι νέοι αυτοί Internet καταναλωτές παρουσιάζουν κάποιες διαφορές με τους ήδη υπάρχοντες. Πρώτα απ' όλα, η μέση ηλικία των νέων αυτών καταναλωτών είναι χαμηλότερη, καθώς ένας σημαντικός αριθμός αυτών προέρχεται από το ηλικιακό γκρουπ 18 έως 24 ετών. Η επίδραση που θα έχει η είσοδος νεαρών σε ηλικία ατόμων στην ομάδα Internet καταναλωτών είναι φανερή και σε άλλους τομείς, καθώς η πλειοψηφία των νέων καταναλωτών θα είναι άγαμοι με μηνιαίο εισόδημα μικρότερο των 1000€

Γράφημα 1

Πρόσβαση Στο Internet Ανά Φύλλο



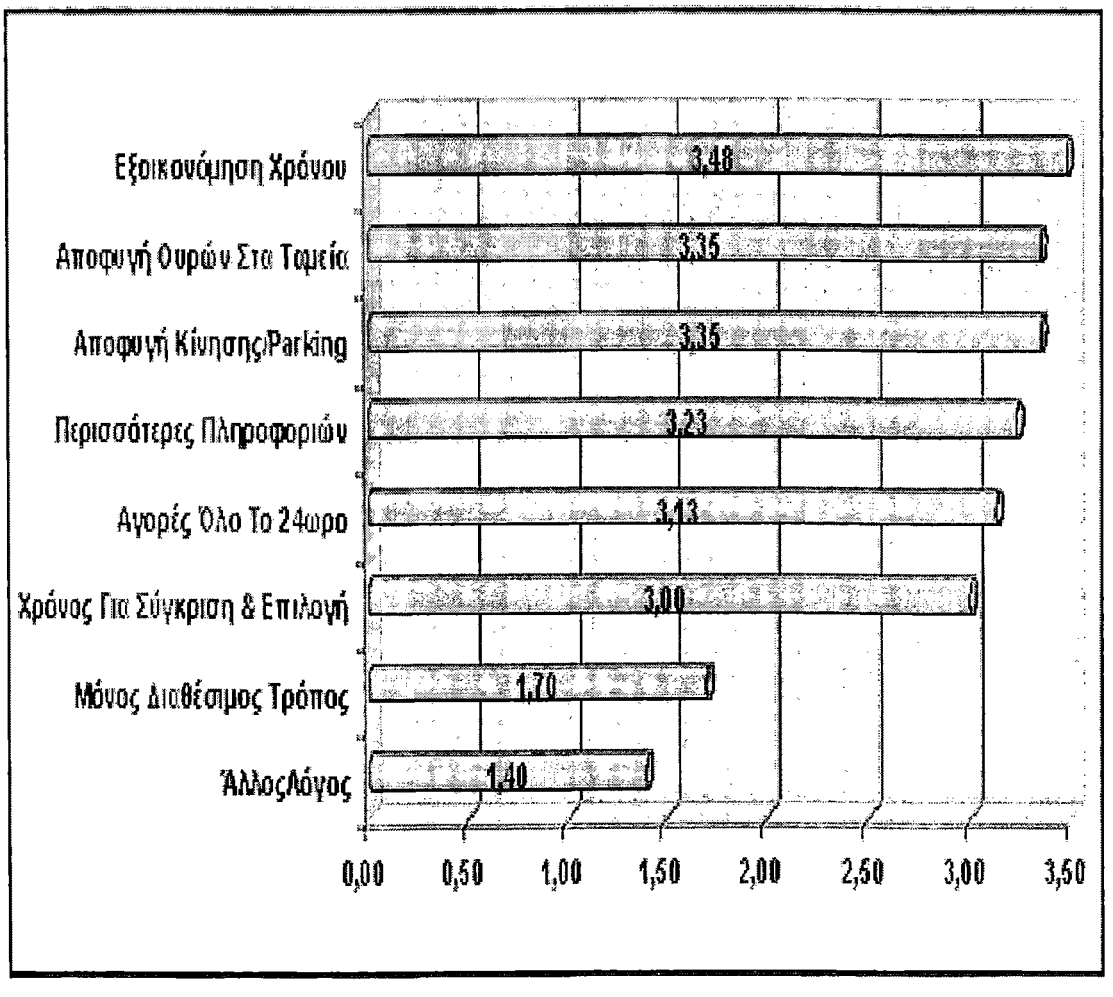
Οι σημαντικότεροι λόγοι, που ένας τόσο σημαντικός αριθμός καταναλωτών θα στραφεί στο Internet, αλλά και τα άλλα δίκτυα αγορών από απόσταση, έχουν κυρίως να κάνουν με τα βασικά χαρακτηριστικά των μέσων αυτών. Πιο συγκεκριμένα, ο σημαντικότερος λόγος είναι η εξοικονόμηση χρόνου. Η επιθυμία αυτή συμπίπτει με τις άλλες προτεραιότητες των Internet καταναλωτών, δηλαδή την προσπάθεια αποφυγής ουρών στα ταμεία, την δυνατότητα αγορών όλο το 24ωρο, την αποφυγή της κίνησης καθώς και την μεγαλύτερη ευχέρεια χρόνου για συγκρίσεις και επιλογές προϊόντων. Εξίσου σημαντικός λόγος αποτελεί και η πληθώρα πληροφοριών που βρίσκονται στην διάθεση των καταναλωτών.

Η ίδια έρευνα επιβεβαίωσε το γεγονός ότι το Internet είναι σε μεγάλο βαθμό αρσενική απασχόληση. Η πρόσβαση στο Internet παρουσιάζει σημαντικές διαφορές ανάμεσα σε άντρες και γυναίκες. Η διαφορά αυτή μεγιστοποιείται στο σπίτι, όπου μόλις 28% όλων των χρηστών Internet που έχουν πρόσβαση από το σπίτι είναι γυναίκες σε αντίθεση με τους άντρες που κατέχουν το υπόλοιπο 72%. Στην εργασία η κατάσταση βελτιώνεται σημαντικά, καθώς από όλους τους χρήστες που έχουν πρόσβαση στο Internet από την δουλειά τους το 35% είναι γυναίκες. Η επικράτηση των ανδρών στην πρόσβαση στο Internet δεν αποτελεί έκπληξη. Η επικράτηση αυτή όμως δεν οφείλεται σε κάποια έμφυτη τάση των αντρών προς το μέσο αυτό, αλλά στη κακή σχέση των γυναικών με το βασικό μέσο πρόσβασης στο Internet, δηλαδή τους

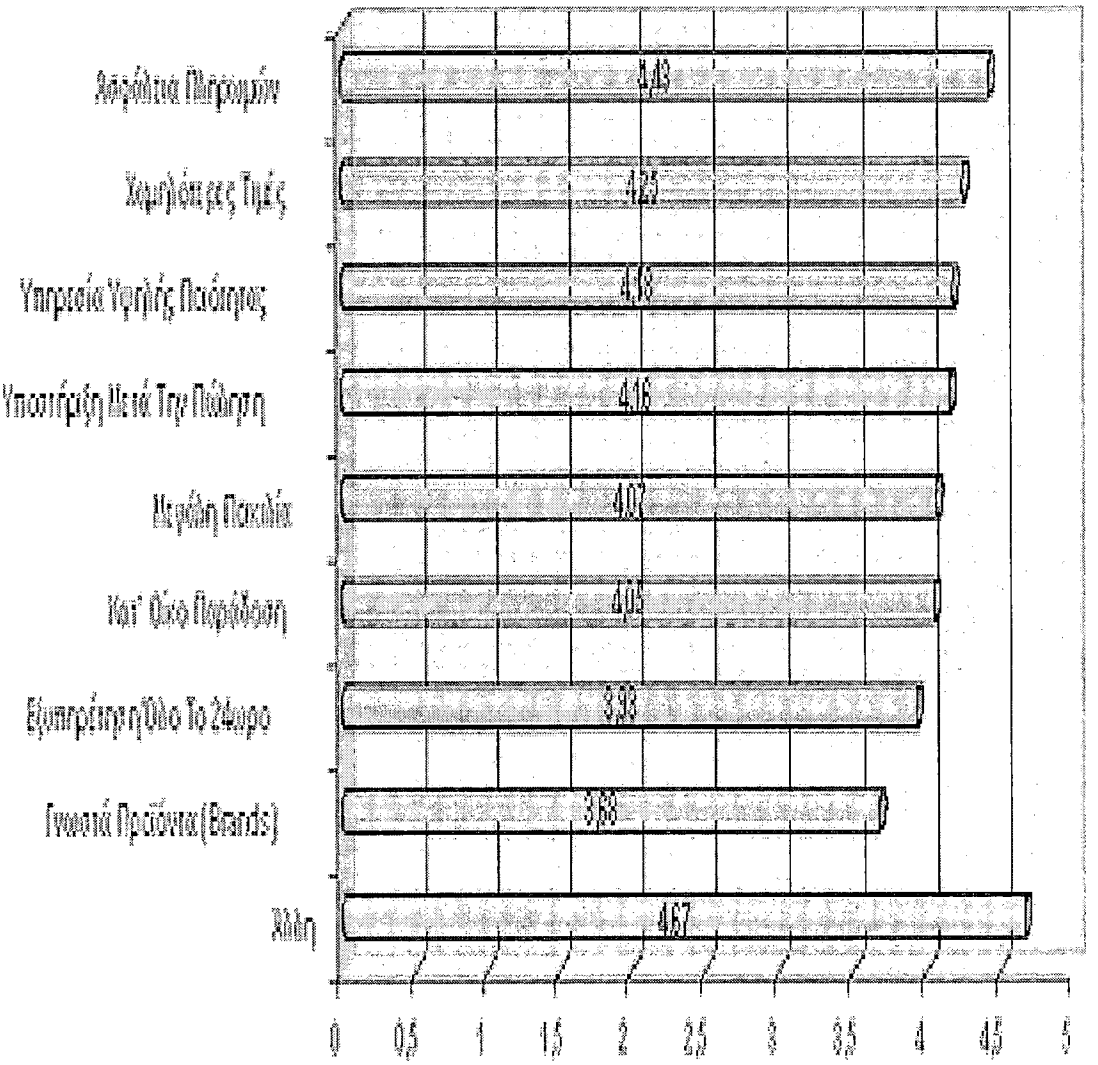
προσωπικούς υπολογιστές (δηλαδή δεν υπάρχουν περισσότεροι από το αναμενόμενο άνδρες χρήστες, αλλά λιγότερες από το αναμενόμενο γυναίκες).

Η αποχή των γυναικών από τις on-line αγορές έχει σημαντικές επιπτώσεις στην εξέλιξη του νέου αυτού καναλιού. Πρώτα απ' όλα η έλλειψη γυναικών μειώνει το μέγεθος της δυνητικής αγοράς κατά το ήμισυ. Επιπλέον, οι γυναίκες είναι πιο ανοιχτές στις επιλογές τους και ψωνίζουν πιο τακτικά από τους άντρες. Σίγουρα λοιπόν αξίζει τα on-line καταστήματα να κάνουν μία προσπάθεια προσέλκυσης γυναικών στο νέο αυτό μέσο αγορών.

Γράφημα 2



Γράφημα 3



Κλίμακα 1 - 5, όπου 5 το πιο σημαντικό και 1 το πιο ασήμαντο.

Πηγή: Οικονομικό Πανεπιστήμιο Αθηνών, 2000

ΕΠΙΛΟΓΟΣ

Είναι σημαντικό και χρήσιμό, όλοι οι άνθρωποι κάθε ηλικίας, στις μέρες μας να αποδέχονται την εξέλιξη της τεχνολογίας και να προσπαθούν να την εφαρμόσουν στην καθημερινότητα τους. Γιατί είναι παγκοσμίως γνωστό ότι ο ρυθμός ανάπτυξης και η εξέλιξη της τεχνολογίας έχει μεγαλώσει και έχει ως απώτερο σκοπό να κάνει τη ζωή μας πιο εύκολη.

Οι Έλληνες καταναλωτές για να πραγματοποιήσουν τις αγορές τους έχουν μία τάση προς την προσωπική επαφή τους με το κατάστημα. Αυτή η προτίμηση θέτει εμπόδια στην διεξαγωγή των ηλεκτρονικών αγορών, επίσης οι καταναλωτές πρέπει να εμπιστευτούν ένα site που πιθανόν δεν γνωρίζουν. Η προσφορά γνωστών καταστημάτων στο διαδίκτυο, η παροχή εγγυήσεων από το κατάστημα και η χρήση των προηγμένων τεχνικών ασφαλείας, σίγουρα βοηθάει στην δημιουργία μίας οικειότητας του χρήστη με το περιβάλλον.

Δεν πρέπει να υπάρχει ασφάλεια μόνο στις συναλλαγές αλλά και στα προσωπικά δεδομένα των καταναλωτών. Οι καταναλωτές απαιτούν αυτή την ασφάλεια, και δεν είναι υπερβολική γιατί στο Internet είναι εύκολο για μία επιχείρηση να συλλέξει προσωπικές πληροφορίες εκατομμυρίων ανθρώπων, οι οποίες μπορούν μετά να μεταπωληθούν σε άγνωστους τρίτους. Αν και υπάρχει σχετική νομοθεσία περί προστασίας δεδομένων που καλύπτει τις απαιτήσεις των καταναλωτών.

Σημαντικός παράγοντας για την εξέλιξη της τεχνολογίας ώστε να πείσουμε τους καταναλωτές να την αποδεχθούν και να την ακολουθήσουν είναι η εξασφάλιση της ασφάλειας των συναλλαγών .

Η γνώση για Ηλεκτρονικό Εμπόριο προκύπτει από την ανάγκη των επιχειρήσεων και των κυβερνήσεων να αναζητούν για δικό τους όφελος την καλύτερη χρήση της τεχνολογίας των υπολογιστών και των τηλεπικοινωνιών έτσι ώστε να επιτευχθούν σταδιακά οι στόχοι τους και σε αυτόν τον τομέα, της τεχνολογίας.

Το Ηλεκτρονικό Εμπόριο προσφέρει τη δυνατότητα εκτέλεσης πράξεων για την ανταλλαγή προϊόντων ή υπηρεσιών, μεταξύ δυο ή περισσοτέρων μερών, με χρήση ηλεκτρονικών υπολογιστών και δικτύων υπολογιστών. Σίγουρα είναι μειονέκτημα η απουσία του ανθρώπινου παράγοντα σε τέτοιου είδους ενέργειες.

Η δημιουργία ασφαλούς περιβάλλοντος ηλεκτρονικού εμπορίου σημαίνει προστασία των δικτυακών πόρων από ενδεχόμενες απειλές και εγγύηση τουλάχιστον του ίδιου επιπέδου ασφαλείας με το συμβατικό εμπόριο. Η Ελλάδα ωστόσο δείχνει να ακολουθεί σωστή πορεία στο θέμα αυτό, καθώς έχει σπεύσει να συμπεριλάβει στην νομοθεσία της αρκετές ρυθμίσεις ώστε να καλύπτονται τα νομικά ζητήματα του ηλεκτρονικού εμπορίου, ωστόσο υπάρχει ακόμα πολύς δρόμος και οι δικαστικοί αγώνες που ενδεχομένως θα διεξαχθούν θα καθορίσουν σε μεγάλο βαθμό τη μελλοντική νομοθεσία.

Συνεπώς το μέλλον του ηλεκτρονικού εμπορίου συνδέεται άμεσα το πόσο χρήσιμο είναι στην καθημερινή πρακτική και κατά πόσο μπορούν οι ειδικοί να εξαλείψουν τα μειονεκτήματα του. Η διευρυμένη αγορά, ο αυξανόμενος ανταγωνισμός, η μείωση του κόστους των προϊόντων, η μείωση των προμηθευτικών αλλαγών και η ταχύτητα ανταπόκρισης στον πελάτη είναι μερικά από τα θετικά αποτελέσματα του ηλεκτρονικού εμπορίου. Τα προβλήματα που θα πρέπει να αντιμετωπίσουν οι ειδικοί είναι η ασφάλεια, η έλλειψη επαφής του πωλητή με τον πελάτη, η δύσκολη χρήση των πολύπλοκων ηλεκτρονικών συστημάτων και τέλος η δυσκολία στην εκτίμηση του κόστους στις νέες τεχνολογίες.

Συμπερασματικά μπορούμε να πούμε πως η Ελλάδα είναι σε ένα ικανοποιητικό επίπεδο σχετικά με την ανάπτυξη του ηλεκτρονικού εμπορίου. Το θέμα είναι αν τελικά θα μπορεί να ανταπεξέλθει στο μεγάλο στοίχημα που είναι οι ανάπτυξη των νέων τεχνολογιών.

Είναι δύσκολο να προβλέψει κάποιος το μέλλον του ηλεκτρονικού εμπορίου που είναι ήδη σε εξέλιξη. Νέες τεχνολογίες δοκιμάζονται και εφαρμόζονται πειραματικά συνεχώς. Πρέπει όμως να εστιάσουμε το ενδιαφέρον μας στο πως θα συνδυαστεί στην αγορά ο ανθρώπινος παράγοντας με την εφαρμογή των καινούριων τεχνολογιών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Δουκίδης Γ., Θεμιστοκλέους Μ., Δράκος Β., Παπαζαφειροπύλου Ν., Ηλεκτρονικό Εμπόριο, Εκδόσεις: Οικονομικό Πανεπιστήμιο Αθήνων, 1998.

Πασχόπουλος Α., Σκαλτσάς Π., Ηλεκτρονικό Εμπόριο, Εκδόσεις: Κλειδάριθμος, 2001.

Πομπόρτσης Α., Τσούλφας Α., Εισαγωγή στο Ηλεκτρονικό Εμπόριο, Εκδόσεις: Τζιόλα, 2002.

Συρμακέσης Σ., Ηλεκτρονικό Εμπόριο, Εκδόσεις:

Http://www.philosophe.gr/e-commerce.html

http://www.echeck.org/library/presentations/index.html

http://www.go-online.gr/files/document/14-10-2002/e-ELLADA.pdf

http://www.microsoft.com

www.eurobank.gr

www.in.gr