ΑΝΩΤΑΤΟ
ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ
ΜΕΣΟΛΟΓΓΙΟΥ

Το Α και το Ω της Δικτυακής Ασφάλειας

Μουλίνος Νέστορας
Πλιάκος Βασίλης
ΑΜ:8479-7870

ΕΙΣΗΓΗΤΗΣ:
ΜΠΕΛΙΓΙΑΝΝΗΣ Γ.

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Ιστορική Αναδρομή Ηλεκτρονικού Εμπορίου ... 1

Βασικές Αρχές Ηλεκτρονικού Εμπορίου ... 2

Ηλεκτρονικό Εμπόριο / E-Commerce ... 3

ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΛΗΡΩΜΕΣ

1. Ηλεκτρονικές Πληρωμές ...
   - 1.1. Εισαγωγικά ... 6
   - 1.2. Μέθοδοι Ηλεκτρονικών Πληρωμών ... 7
     - 1.2.1. E-CASH ... 7
     - 1.2.2. Ηλεκτρονικές Επιταγές ... 8
     - 1.2.3. Πιστωτικές Κάρτες ... 11
     - 1.2.4. Internet Banking ...
     - 1.2.5. Γενικά προβλήματα ... 16

2. Συστήματα Ηλεκτρονικών Πληρωμών ...
   - 2.1. Διαδικασίες Ηλεκτρονικής Πληρωμής ... 21
     - 2.1.1. Έμπορος ... 21
     - 2.1.2. Πελάτης ... 21
     - 2.1.3. Οργανισμός Οικονομικών Υπηρεσιών ... 22
   - 2.2. Μέθοδοι και Πρότυπα Ηλεκτρονικής Πληρωμής ... 22
     - 2.2.1. Κρυπτογραφημένη Μετάδοση Στοιχείων ... 23
     - 2.2.2. Ψηφιακά Μετρητά ... 24
     - 2.2.3. Ηλεκτρονική Μεταφορά Κεφαλαίων ... 31
     - 2.2.4. Λογαριασμοί Χρέωσης – Πίστωσης ... 31
     - 2.2.5. Άμεση Μεταφορά ... 32
     - 2.2.6. Υπηρεσίες Είσπραξης ... 32
   - 2.3. Πρότυπα Ηλεκτρονικών Πληρωμών ... 33
   - 2.4. Αξιολόγηση και Επιλογή Μεθόδων Ηλεκτρονικής Πληρωμής ... 35

3. Ηλεκτρονικά Συστήματα Πληρωμής σε Ανοικτό Δίκτυο Υπολογιστών ...
   - 3.1. Εισαγωγικά ... 36
   - 3.2. Σχηματική Ταξινόμηση Ηλεκτρονικών Συστημάτων Πληρωμής ... 37
   - 3.3. Αξιολόγηση Συστημάτων ... 40
   - 3.4. Περιγραφή Συστημάτων ... 41

3.4.1. Digicash ... 41
3.4.1.1. Το πρότυπο E-CASH ... 41
3.4.1.2. Νομίσματα E-CASH ... 43
3.4.1.3. Χαρακτηριστικά γνωρίσματα Digicash ... 44
3.4.2. Millicent ... 45
3.4.2.1. Scrips ... 45
3.4.2.2. Το Millicent ... 46
3.4.2.3. Χαρακτηριστικά γνωρίσματα Millicent ... 47
3.4.3. CAFÉ ... 48
3.4.3.1. Το πρότυπο CAFÉ ... 49
3.4.3.2. Χαρακτηριστικά γνωρίσματα CAFÉ ... 50
3.4.4. Mondex ... 52
3.4.4.1. Χαρακτηριστικά γνωρίσματα Mondex ... 53
3.4.5. NetCash ... 54

4. EBPP ...
4.1. Ηλεκτρονική Παρουσίαση και Πληρωμή Λογαριασμών ... 55
4.1.1. Μπορούμε να έχουμε παντού ηλεκτρονικούς λογαριασμούς; . 55
4.2. Τα επιχειρηματικά μοντέλα του EBPP ... 56
4.2.1. Biller-Direct Model ... 56
4.2.2. Consolidation Model ... 57
4.3. Γιατί EBPP; ... 58
4.3.1. Επιχειρηματικό πλάνο για επιτυχημένο EBPP ... 60
4.3.2. Στρατηγική και στόχοι EBPP ... 60
4.3.3. Ανάλυση Αγοράς ... 61
4.3.4. Οικονομική Ανάλυση ... 62

5. Συλλογή Στοιχείων / Customer Spotting / Επικοινωνία / Προβολή – Προώθηση ...
5.1. Δημιουργία Λίστας Αποστολής Μηνυμάτων (Mailing List) ... 63
5.2. Customer Spotting ... 64
5.3. Επικοινωνία μέσω του Διαδικτύου ... 66
5.4. Προβολή-Προώθηση μέσω του Διαδικτύου ... 66

6. Τραπεζικές Συναλλαγές ...
6.1. Διαδικτυακές Τραπεζικές Συναλλαγές (e-banking). Η σημερινή εφαρμογή τους στην Ελλάδα ... 68
6.1.1. E-Banking και Διαδικτυακό Έγκλημα ... 70
6.2. Τραπεζικές Συναλλαγές μέσω κινητού τηλεφώνου: Η εφαρμογή της υπηρεσίας σήμερα στην Ελλάδα ... 74
6.2.1. Παροχή Υπηρεσιών μέσω κινητού τηλεφώνου ... 74

ΚΡΥΠΤΟΓΡΑΦΗΣΗ – ΑΣΦΑΛΕΙΑ

1. Κρυπτογράφηση – Ασφάλεια
1.1. Εισαγωγικά ... 76
1.2. Κρυπτογράφηση: Το Α και το Ω της Δικτυακής Ασφάλειας ... 77
1.3. Γιατί πρέπει να χρησιμοποιείται ... 78

2. Δημόσιο Κλειδί
2.1. Η Υποδομή Δημόσιου Κλειδιού και η Κρυπτογράφηση στην Πράξη. 79
2.1.1. PGP ... 83
2.1.2. X.509 ... 85

3. Τι είναι η Ηλεκτρονική Υπογραφή
3.1. Δημιουργία και Επαλήθευση Ηλεκτρονικής Υπογραφής ... 86
3.2. Η Ηλεκτρονική Υπογραφή (e-signature) στις Online Συναλλαγές ... 87
3.3. Η Πιστοποίηση της Ψηφιακής Υπογραφής ... 87
3.4. Χρήση Ψηφιακών Υπογραφών με το Office XP της Microsoft ... 88
3.5. Τρόπος διαπίστωσης ότι ένα αρχείο φέρει υπογραφή ... 89
3.6. Υπηρεσίες Παροχών Πιστοποίησης ... 89

4. Η έννοια της Ασφάλειας του Συστήματος
4.1. Πολιτική Ασφάλειας ... 92
4.2. Κόστος Ασφάλειας ... 94
4.3. Μοντέλα Ασφάλειας ... 95
4.3.1. Μοντέλο Bell-La-Padula ... 96
4.3.2. Μοντέλο Biba ... 97
4.3.3. Στρατιωτικό Μοντέλο ... 97
4.4. Απαιτήσεις Ασφάλειας ... 99
4.5. Μηχανισμοί Ασφάλειας ... 100
4.5.1. Συμμετρική Κρυπτογράφηση ... 100
4.5.2. Ασύμμετρη Κρυπτογράφηση ... 100
4.5.3. Κβαντική Κρυπτογράφηση ... 101

5. Proxy και Proxy Chains ... 102

6. Mixnets και Mixnet Reply Blocks ... 102

7. Γνωστοί Αλγόριθμοι Κρυπτογράφησης ... 103

8. Έμπιστες Τρίτες Οντότητες ... 104
8.1. Λειτουργικές Απαιτήσεις της Έμπιστης Τρίτης Οντότητας ... 106
8.2. Ο Ρόλος της Έμπιστης Τρίτης Οντότητας στην Ασφάλεια Δικτύων – Ασφάλεια μέσα από την Έμπιστη Τρίτη Οντότητα ... 107
8.3. Υποδομή των Έμπιστων Τρίτων Οντοτήτων ... 108

8.3.1. Τοπολογία ... 108
8.3.2. Σειριακή Σύνδεση ... 108
8.3.3. Παράλληλη Ενεργή Σύνδεση ... 109
8.3.4. Παράλληλη Ανενεργή Σύνδεση ... 110
8.4. Δομή των Πιστοποιητικών ... 110
8.6. Διασύνδεση Έμπιστων Τρίτων Οντοτήτων ... 111
8.5. Βασικές Λειτουργίες των Έμπιστων Τρίτων Οντοτήτων ... 111
8.7. Απαιτήσεις σε Υπηρεσίες Ασφάλειας στα Δίκτυα ... 113
8.7.1. Εφαρμογές που απαιτούν Ασφάλεια ... 113
8.7.2. Απαιτήσεις Εφαρμογών για Υπηρεσίες Ασφάλειας ... 114

9. Βασικές Πολιτικές Ασφάλειας ... 115
9.1. Ασφάλεια Εκτεταμένων Δικτύων ... 116
9.2. Ασφάλεια Ψηφιακών Δικτύων Ολοκληρωμένων Υπηρεσιών ... 116

10. Πολιτικές Ασφάλειας Δικτύων ... 117
10.1. Πολιτική Ασφάλειας DMZ ... 118
10.2. Πολιτική Ασφάλειας Firewall ... 119
10.3. Πολιτική Ασφάλειας Ασύρματων Δικτύων ... 120
10.4. Πολιτική Ασφάλειας Απομακρυσμένης Πρόσβασης ... 121

11. Πολιτικές Ασφάλειας Προσωπικού ... 122
11.1. Κωδικοί Πρόσβασης ... 122
11.2. Χρήση Internet ... 123
11.3. Χρήση Ηλεκτρονικού Ταχυδρομείου ... 123
11.4. Χρήση Φορητών Η/Υ ... 124

12. Βασικές Υπηρεσίες Ασφάλειας Δικτύων ... 125
12.1. Αυθεντικοποίηση ... 126
12.2. Εμπιστευτικότητα Δεδομένων ... 128
12.3. Ακεραιότητα Δεδομένων ... 128
12.4. Καταλογισμός Ευθύνης ... 129

13. Τεχνικές Υλοποίησης των Υπηρεσιών Ασφάλειας ... 129
13.1. Έλεγχος Προσπέλασης ... 129
13.2. Κρυπτογραφία ... 131
13.3. Ψηφιακή Υπογραφή ... 132

14. Προϋποθέσεις Εφαρμογής ενός Συστήματος Ασφάλειας ... 133

15. Προβλήματα Ασφάλειας Δικτύων ... 134

16. Οδηγός για Ασφαλή Πλοήγηση στο Internet ... 135

17.Firewalls: Αδιαπέραστα Τείχη 137

ΝΟΜΙΚΑ - ΚΟΙΝΩΝΙΚΑ ΘΕΜΑΤΑ

1. Νομικά και Κοινωνικά Θέματα 139
   1.1. Ηλεκτρονικά Έγγραφα 140
   1.2. Προεδρικό Διάταγμα 150 του 2001 για Ηλεκτρονική Υπογραφή 141
   1.3. Ο Ρόλος της ΕΕΤΤ 142
   1.4. Άλλες Διατάξεις 143
   1.5. Προστασία Πνευματικών Δικαιωμάτων 144
   1.6. Προστασία Προσωπικών Δεδομένων 145
   1.7. Η Αναγκαιότητα του Θεσμικού Ελέγχου της Προστασίας των Προσωπικών Πληροφοριών 152

ΒΙΒΛΙΟΓΡΑΦΙΑ 154

ΔΙΑΔΙΚΤΥΟ 155

ΕΙΣΑΓΩΓΗ

Ιστορική Αναδρομή Ηλεκτρονικού Εμπορίου

Η εμφάνιση κατά τη δεκαετία του 1970 της Ηλεκτρονικής Μεταφοράς Κεφαλαίων (EFT) μεταξύ τραπεζών, μέσω ασφαλών ιδιωτικών δικτύων, άλλαξε την εικόνα των χρηματοπιστωτικών αγορών. Η Ηλεκτρονική Μεταφορά Κεφαλαίων βελτιώνει τις ηλεκτρονικές πληρωμές με την αποστολή πληροφοριών με ηλεκτρονικά μέσα. Σήμερα, υπάρχουν πολλές παραλλαγές της EFT, μεταξύ των οποίων οι συνηθέστερες είναι οι χρεωστικές κάρτες και οι άμεσες καταθέσεις στους τραπεζικούς λογαριασμούς των εργαζομένων. Κάθε μέρα περίπου 4 τρις. Δολάρια αλλάζουν χέρια με EFT μέσω δικτύων που συνδέουν τράπεζες, αυτοματοποιημένα γραφεία συμψηφισμού και επιχειρήσεις, Το υπουργείο Οικονομικών των ΗΠΑ εκτιμά ότι το 1995 το 55% του συνόλου των πληρωμών της ομοσπονδιακής κυβέρνησης πραγματοποιήθηκε με EFT.

Στις αρχές της δεκαετίας του 1980, το Ηλεκτρονικό Εμπόριο διαδόθηκε μεταξύ των επιχειρήσεων αρχικά ως τεχνολογία ηλεκτρονικής μετάδοσης μηνυμάτων: Ηλεκτρονική Ανταλλαγή Δεδομένων (EDI) και Ηλεκτρονικό Ταχυδρομείο (E-mail). Με τις τεχνολογίες της Ηλεκτρονικής Ανταλλαγής Δεδομένων εκσυγχρονίστηκαν οι διαδικασίες των επιχειρήσεων καθόσον μειώθηκαν τα έγγραφα σε χαρτί και αυξήθηκε η αυτοματοποίηση. Οι τεχνολογίες EDI εξελίχθηκαν σε αναπόσπαστο τμήμα της ροής της εργασίας ή των συνεργαζομένων συστημάτων υπολογιστών, συνδυάζοντας υπάρχουσες μη ηλεκτρονικές μεθόδους με ηλεκτρονικά μέσα για τη βελτίωση της αποτελεσματικότητας των επιχειρηματικών διαδικασιών. Η Ηλεκτρονική Ανταλλαγή Δεδομένων επιτρέπει στις επιχειρήσεις να στέλνουν και να λαμβάνουν έγγραφα εργασίας (όπως παραγγελίες αγορών) σε τυποποιημένη ηλεκτρονική μορφή με την ελάχιστη ανθρώπινη παρέμβαση.

Με την πάροδο των ετών, η ηλεκτρονική ανταλλαγή δεδομένων εντάχθηκε στα εσωτερικά συστήματα πληροφοριών και στις καθημερινές πρακτικές των επιχειρήσεων και αποδείχθηκε ιδιαίτερα επιτυχείς σε ορισμένους τομείς, όπως στη διαχείριση κατηγοριών προϊόντων (category management) για είδη παντοπωλείου λιανικό εμπόριο.

Η εξέλιξη του διαδικτύου (internet) στα τέλη της δεκαετίας του 1980 έδωσε τη δυνατότητα να αναπτυχθούν ριζικά διαφορετικές μορφές ηλεκτρονικού εμπορίου, όπως υπηρεσίες σε απευθείας σύνδεση, καθώς και νέες μορφές μαζικών κοινωνικών επαφών και διάδοσης γνώσεων. Εκτός από τη διαθεσιμότητα και το χαμηλό κόστος των πληροφοριών σε αυτό το "δίκτυο των δικτύων", βασικός παράγοντας για την προώθηση της ευρείας χρήσης του από τις επιχειρήσεις είναι η ύπαρξη κατάλληλων υποδομών "από άκρη σε άκρη" και εφαρμογών που υποστηρίζουν τις διαδικασίες με ολοκληρωμένο τρόπο.

Ο παγκόσμιος ιστός (world wide web) στη δεκαετία του1990 αντιμετώπισε με αποφασιστικό τρόπο θέματα δημοσίευσης και διάδοσης πληροφοριών. Ο ιστός καθιστά το ηλεκτρονικό εμπόριο ένα φθηνότερο μέσο για την εκτέλεση των επιχειρηματικών δραστηριοτήτων (οικονομίες κλίμακας) και επιτρέπει την μεγαλύτερη διαφοροποίηση των δραστηριοτήτων (οικονομίες φάσματος). Οι περιορισμένες απαιτήσεις εισόδου (ένας προσωπικός υπολογιστής, ένας αποδιαμορφωτής – modem και λογαριασμός internet) επιτρέπουν στις μικρές επιχειρήσεις να εισέλθουν στον τομέα αυτό με τεχνολογικές βάσεις που δεν διαφέρουν από εκείνες των μεγάλων επιχειρήσεων.

Βασικές Αρχές Ηλεκτρονικού Εμπορίου

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 αμφίδρομής επικοινωνίας με τους πελάτες/ πολίτες/ καταναλωτές, οι επιχειρηματικές διεργασίες και η ανταλλαγή πληροφοριών ενδο-επιχειρησιακά, αλλά και κυρίως μεταξύ των 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).

Ένας απλός ορισμός για το Ηλεκτρονικό Εμπόριο είναι ότι αποτελεί κάθε μορφή επιχειρηματικής συναλλαγής και επικοινωνίας που γίνεται με ηλεκτρονικά μέσα. Ένας τέτοιος απλοϊκός ορισμός όμως, παρόλο που τεχνικά μπορεί να είναι ακριβής, δεν μπορεί να συλλάβει το βασικό πνεύμα του Ηλεκτρονικού Εμπορίου που δεν είναι απλώς η χρήση των ηλεκτρονικών μέσων για επικοινωνία, αλλά οι δυνατότητες για επανακαθορισμό του τρόπου με τον οποίο γίνεται το εμπόριο, ο οποίος γίνεται για πρώτη φορά εφικτός με τη χρήση νέων τεχνολογιών από τις σύγχρονες επιχειρήσεις.

Έτσι το Ηλεκτρονικό Εμπόριο θα μπορούσε να οριστεί ως ένα σύνολο επιχειρηματικών στρατηγικών που μπορούν να υποστηρίξουν συγκεκριμένους τομείς επιχειρηματικής δραστηριότητας και συγκεκριμένες επιχειρηματικές πρακτικές οι οποίες επιτρέπουν, μέσω της χρήσης νέων τεχνολογιών, τη διεκπεραίωση εμπορικών διαδικασιών με ηλεκτρονικά μέσα.

Το Ηλεκτρονικό Εμπόριο προσφέρει τη δυνατότητα εκτέλεσης πράξεων για την ανταλλαγή προϊόντων ή υπηρεσιών μεταξύ δύο 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 (άϋλων αγαθών),
- ηλεκτρονική ανταλλαγή μεταφοράς μεταφορών,
- εμπορικές δημοπρασίες,
- συλλογικές εργασίες σχεδίασης και τεχνικών μελετών,
- ενημέρωση από πηγές σε απευθείας σύνδεση,
- ψηφιακές προμήθειες,
- πωλήσεις απευθείας στον καταναλωτή και μεταπωλητική εξυπηρέτηση.

Οι εφαρμογές του 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 συμπεριλαμβάνουν όλες τις μορφές των 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 του Internet, καθώς και κάθε άλλη μορφή ηλεκτρονικής μετάδοσης δεδομένων για εμπορικούς σκοπούς.

Ηλεκτρονικό Εμπόριο/E-commerce

Το τελευταίο και πιο προχωρημένο στάδιο εκμετάλλευσης του διαδικτύου είναι το η-εμπόριο. Αυτό πρακτικά σημαίνει τη δυνατότητα της εμπορίας προϊόντων μέσω Internet. Η ανάπτυξη ενός πλάνου για ηλεκτρονικό εμπόριο μέσω της ιστοσελίδας θα πρέπει να έχει πρθοβλέψει πολλούς παράγοντες.

Αν όλα γίνουν σωστά οι πωλήσεις της επιχείρησης μπορούν να αυξηθούν και να δώσουν μεγάλη ώθηση στα επόμενα σχέδια του επιχειρηματία. Ένα τέτοιο

εγχείρημα δεν είναι δαπανηρό αλλά θα πρέπει να έχει μελετηθεί καλά πριν πραγματοποιηθεί. Στο εκπαιδευτικό υλικό του κόμβου θα βρείτε πολλές χρήσιμες πληροφορίες.

Παρακάτω δίνονται επιγραμματικά μερικές συμβουλές που θα σας βοηθήσουν στην καλύτερη πραγματοποίηση και πιο ρεαλιστική αντιμετώπιση του Ηλεκτρονικού Εμπορίου για την επιχείρησή σας:

- ✓ Ελέγξτε αν οι πιθανοί πελάτες σας είναι σε θέση να επισκεφθούν το δικτυακό σας κατάστημα. Αν η ιστοσελίδα ή τα προϊόντα απευθύνονται σε ηλικιωμένους σαφώς μειονεκτούν έναντι των αντίστοιχων που απευθύνονται στις πιο νεαρές ηλικίες.

- ✓ Μελετήστε τις δυνατότητες ανταπόκρισης σε πιθανή αύξηση της ζήτησης. Δε θα ήταν καθόλου καλό να δημιουργήσετε δυσαρεστημένους πελάτες από αδυναμία ανταπόκρισης στις παραγγελίες.

- ✓ Ελέγξτε τις δυνατότητες και το κόστος του δικτύου διανομής σας. Πολλές εταιρείες δεν είχαν μελετήσει καλά το εύρος και το κόστος της διανομής με αποτέλεσμα να αποτύχουν.

- ✓ Κάνετε σαφές στην ιστοσελίδα σας ποιες περιοχές εξυπηρετείτε και με τι κόστος (επιπλέον ή μη)

- ✓ Κάνετε εύκολη την αγορά μέσω της ιστοσελίδας. Μερικές φορές οι καταναλωτές απογοητεύονται ή κουράζονται από τις χρονοβόρες και δύσκολες διαδικασίες και σταματάνε ή ακυρώνουν τις παραγγελίες τους.

- ✓ Προσπαθήστε να εγγυηθείτε για την ασφάλεια των συναλλαγών. Υπάρχουν εταιρείες που βοηθάνε και πιστοποιούν την ασφάλεια των ιστοσελίδων.

- ✓ Δώστε εναλλακτική λύση εκτός της πιστωτικής κάρτας για πληρωμή. Υπάρχουν πολλοί που δεν είναι διατεθειμένοι να χρησιμοποιήσουν την πιστωτική τους κάρτα για συναλλαγές στο διαδίκτυο.

- ✓ Δείχνετε φωτογραφίες και περιλήψεις των προϊόντων. Δύσκολα κάποιος θα αγοράσει ένα προϊόν που δεν έχει δει και δεν ξέρει τα χαρακτηριστικά του.

- ✓ Βεβαιώστε και κάνετε σαφές ότι κανένα από τα στοιχεία των πελατών σας δε θα βγει εκτός εταιρείας. Υπάρχει μεγάλη φιλυποψία

σχετικά με την εμπιστευτικότητα των στοιχείων που συλλέγουν οι επιχειρήσεις.

- Βεβαιωθείτε ότι μπορείτε να χειρισθείτε σωστά, γρήγορα και αποτελεσματικά τις παραγγελίες τις αιτήσεις, τα σχόλια αλλά και τις ερωτήσεις των πελατών σας.

- Να είστε σαφείς και ειλικρινείς για τις τιμές αλλά και τους χρόνους παράδοσης των προϊόντων.

- Ενημερώνετε πάντα τους πελάτες για τυχόν προβλήματα ή καθυστερήσεις. Έχει πολύ καλύτερα αποτελέσματα από το να φανείτε ασυνεπείς

Το διαδίκτυο είναι ένα εργαλείο που περισσότερο μικραίνει παρά μεγαλώνει την απόσταση μεταξύ των μεγάλων εταιρειών και των μικρομεσαίων επιχειρήσεων. Η εκμετάλλευσή του έχει προχωρήσει πολύ στο εξωτερικό και τώρα αναπτύσσεται και στη Ελλάδα. Συμβουλευτείτε πάντα τους ειδικούς πριν από μια τέτοια κίνηση.

ΚΕΦΑΛΑΙΟ 1ο

ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΛΗΡΩΜΕΣ

Ηλεκτρονικές Πληρωμές

Εισαγωγικά

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 ηλεκτρονικών πληρωμών μέσω των οποίων θα διεκπεραιώνονται ηλεκτρονικά οι οφειλές των εμπλεκομένων μερών. Ήδη έχουν υιοθετηθεί διάφορα συστήματα ηλεκτρονικών πληρωμών (π.χ. πιστωτικές κάρτες, ηλεκτρονικό χρήμα κ.λ.π.) κατάλληλα για την εξυπηρέτηση των συναλλαγών και ειδικότερα σε συστήματα πληρωμών που χρησιμοποιούν πιστωτικές κάρτες, ψηφιακό χρήμα ή ηλεκτρονικές επιταγές.

Η εξάπλωση του διαδικτύου την τελευταία δεκαετία και η χρήση του για εμπορικούς σκοπούς δημιούργησε νέα δεδομένα στο χώρο των επιχειρήσεων. Οι νέες τεχνολογίες μετέβαλλαν ραγδαία τόσο το χώρο δράσης των επιχειρήσεων, την αγορά, όσο και την οργανωτική δομή των οικονομικών μονάδων. Στα πρώτα στάδια ανάπτυξης του ηλεκτρονικού εμπορίου οι πληρωμές γίνονταν εκτός του διαδικτύου με καταβολή των ποσών σε κάποια τράπεζα. Ο αναχρονιστικός όμως αυτός τρόπος χρηματικής εκκαθάρισης των διαδικτυακών συναλλαγών δεν συμβάδιζε με την ταχύτητα και την αξιοπιστία που απαιτούν οι σύγχρονες διαδικτυακές συναλλαγές.

Για την αναβάθμιση του τρόπου εκκαθάρισης των τραπεζικών συναλλαγών προτάθηκαν και εφαρμόστηκαν τρεις κυρίως λύσεις που συνοψίζονται στον όρο ηλεκτρονική πληρωμή. Πρώτος είναι η ηλεκτρονική καταβολή μέσω ηλεκτρονικής μεταφοράς κεφαλαίων (EFT), δεύτερος η χρήση πιστωτικών καρτών για συναλλαγές που γίνονται στο διαδίκτυο τρίτος το ηλεκτρονικό χρήμα.

Μέθοδοι Ηλεκτρονικών Πληρωμών

Το κρισιμότερο σημείο κάθε εμπορικής συναλλαγής είναι η πληρωμή. Εμπόριο χωρίς χρήμα δεν έχει νόημα. Το Internet παρουσιάζει την ιδιομορφία να μην υπάρχει προσωπική επαφή μεταξύ του εμπόρου και του πελάτη, ιδιαίτερα στις λιανικές συναλλαγές. Κατά συνέπεια το θέμα των πληρωμών είναι το σημαντικότερο κομμάτι του ηλεκτρονικού εμπορίου.

Το μεγαλύτερο μέρος της παρακάτω συζήτησης θα αναφέρεται κυρίως στις πληρωμές λιανικών πωλήσεων, οι οποίες έχουν και το σημαντικότερο πρόβλημα καθώς τις περισσότερες φορές η επαφή πελάτη-εμπόρου είναι πολύ σπάνια ή και μοναδική (λ.χ. η αγορά ενός ασφαλιστηρίου συμβολαίου από ένα πράκτορα που διαπραγματεύεται πολλές εταιρίες). Οι πληρωμές του χονδρικού εμπορίου έχουν διαφορετική λογική και άλλα μέσα (λ.χ. εγγυητικές επιστολές, φορτωτικές κλπ) και δεν έχουν τα ίδια προβλήματα. Η ύπαρξη παραστατικών που τα απαιτούν οι αρχές, κάνει δύσκολη τη δημιουργία νέων κόλπων από κακοπληρωτές ή τη διείσδυση νέου τύπου απατεώνων. Αν η κύρια χρήση του δικτυακού τόπου είναι το χονδρεμπόριο τότε λίγα πράγματα θα αλλάξουν από πλευράς πληρωμών. Απλά θα υπάρχει ακόμα ένα κανάλι διανομής στο οποίο η επιχείρηση πρέπει να χρησιμοποιήσει την τακτική της συγκεκριμένης αγοράς.

Δύο πράγματα θα πρέπει πάντως να παρακολουθεί κάποιος. Πρώτον, το θέμα της νομικής υπόστασης της ηλεκτρονικής ανταλλαγής εγγράφων, κατά πόσον δηλαδή είναι δυνατόν να θεωρηθεί κάποιας μορφής ηλεκτρονική ανταλλαγή ως νόμιμο αντίστοιχο λ.χ. του τιμολογίου. Αυτό προσπαθεί να το κάνει η κοινότητα, οπότε μπορεί να θεσμοθετηθεί απότομα.

Το άλλο είναι το γεγονός ότι οι αυτόματες διαδικασίες πολλές φορές είναι δύσκολο να παρακολουθούνται με τους παραδοσιακούς τρόπους γι'αυτό καλό θα ήταν να μελετηθούν προσεκτικά τα πιστωτικά όρια και μετά να αυτοματοποιηθούν.

E-cash

Με αυτή τη μέθοδο υπάρχει μια «τράπεζα» εκδίδει «νόμισμα», στην πραγματικότητα ηλεκτρονικές εγγραφές σε υπολογιστές που λέγονται tokens, και η αγοραπωλησίες γίνονται με ανταλλαγή των tokens. Με άλλα λόγια αγοράζει κάποιος κάτι και μια εγγραφή φεύγει από τον υπολογιστή του και πάει στον υπολογιστή του πωλητή, από όπου μπορεί να φύγει προς ένα τρίτο για μια άλλη συναλλαγή, κ.ο.κ. Ο κεντρικός πυρήνας αυτής της τεχνολογίας είναι η κρυπτογραφία ασύμμετρου κλειδιού. Ουσιαστικά τα tokens είναι ένα είδος λογιστικών εγγραφών που επιβεβαιώνονται από την «εκδοτική αρχή» του «νομίσματος» μέσω της κρυπτογραφικής αυτής μεθόδου.

Αυτό τον καιρό είμαστε στον δεύτερο κύκλο προσπαθειών για δημιουργία e-cash. Ο πρώτος απέτυχε κυρίως για εμπορικούς λόγους, αλλά και λόγω εχθρότητας των κεντρικών τραπεζών.

Μολονότι το e-cash είναι τεχνικά εφικτό, τα διάφορα γενικότερα προβλήματα που δημιουργούνται είναι τεράστια. Είναι η προβληματικότερη μορφή πληρωμών στο διαδίκτυο. Τα προβλήματα, εκτός από τα τεχνικά, είναι και γενικότερης κοινωνικής και πολιτικής φύσεως. Για τους ανθρώπους που ασχολούνται παραγωγικά με το ηλεκτρονικό εμπόριο, το μόνο που ενδιαφέρει είναι να παρακολουθούν τις εξελίξεις, καθώς η γενική εντύπωση είναι ότι μόλις αρχίσει να λειτουργεί θα είναι απαραίτητο.

Ηλεκτρονικές επιταγές

Οι ηλεκτρονικές επιταγές είναι ένα σύστημα ηλεκτρονικών πληρωμών το οποίο χρησιμοποιείται τον τελευταίο καιρό σε χώρες με παράδοσης χρήσης επιταγών. Μία επιταγή έχει μια σειρά από νούμερα τα οποία καθιστούν την κάθε επιταγή μοναδική. Ο αγοραστής εισάγει αυτά τα νούμερα, η τράπεζα ειδοποιείται και ακυρώνει την συγκεκριμένη επιταγή, αν το επιτρέπει το υπόλοιπο του λογαριασμού του. Η μέθοδος είναι αποτελεσματική, αλλά μάλλον ακατάλληλη για την Ελλάδα. Δεδομένης της ανυπαρξίας της λιανικών συναλλαγών με επιταγή η αξία αυτής της διαδικασίας είναι μάλλον ακαδημαϊκή στην Ελλάδα. Αν όμως υπάρχει σημαντικός αριθμός πελατών από Αγγλοσαξονικές κυρίως χώρες, θα πρέπει να μελετηθεί το θέμα προσεκτικά με τελικό στόχο την υλοποίηση.

Μια έντυπη επιταγή είναι ουσιαστικά μια εντολή μεταφοράς κεφαλαίων από ένα λογαριασμό σε έναν άλλο. Η εντολή αυτή αποστέλλεται αρχικά στον αποδέκτη των κεφαλαίων , ο οποίος με τη σειρά του, παρουσιάζει την επιταγή στην τράπεζα προκειμένου να λάβει το αντίστοιχο ποσό.

Μια ηλεκτρονική επιταγή έχει όλα τα χαρακτηριστικά που διαθέτει μια έντυπη επιταγή και χρησιμοποιείται σαν ένα μήνυμα προς την τράπεζα του αποστολέα για την μεταφορά κεφαλαίων από ένα λογαριασμό σε έναν άλλο. Σε αντιστοιχία με την παραδοσιακή διαδικασία, η ηλεκτρονική επιταγή αποστέλλεται αρχικά στον αποδέκτη ο οποίος την υπογράφει και την προωθεί στην τράπεζα προκειμένου να λάβει το αντίστοιχο ποσό.

Από άποψη ασφάλειας, η ηλεκτρονική επιταγή θεωρείται καλύτερη από την έντυπη επιταγή, και αυτό γιατί ο αποστολέας μπορεί να προστατέψει τον εαυτό του από μια απάτη. Αυτό γίνεται με την κωδικοποίηση του αριθμού του λογαριασμού του με το δημόσιο κλειδί της τράπεζας, χωρίς έτσι να αποκαλύπτει τον αριθμό του λογαριασμού του στον έμπορο.

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 πληρωμών το FSTC προσφέρει στους χρήστες διάφορες επιλογές επιταγών ανάλογα με τις ανάγκες του χρήστη. Οι ηλεκτρονικές επιταγές μπορούν να παραδοθούν είτε με άμεση παράδοση μέσω ενός δικτύου ή μέσω ηλεκτρονικού ταχυδρομείου.

Σε κάθε περίπτωση, τα υπάρχοντα τραπεζικά κανάλια μπορούν να εκκαθαρίσουν τις πληρωμές, μέσω των δικτύων τους. Κάτι τέτοιο οδηγεί σε μια ικανοποιητική αναβάθμιση της υπάρχουσας τραπεζικής υποδομής και του Internet.

CheckFree:

Η εταιρεία CheckFree προσφέρει μια μερική λύση για την πραγματοποίηση ηλεκτρονικών πληρωμών. Επικεντρώνεται κυρίως, σε άτομα ή επιχειρήσεις που πληρώνουν μηνιαίους λογαριασμούς και επιθυμούν να αυτοματοποιήσουν τις πληρωμές τους. Βασικά, είναι μια υπηρεσία πληρωμών που επιτρέπει στους πελάτες της να πληρώνουν τους λογαριασμούς τους μέσα από το Internet. Η εταιρεία CheckFree είναι συνδεδεμένη με το δίκτυο ηλεκτρονικών συναλλαγών της Αμερικάνικης Τράπεζας Federal Reserve Bank και με αρκετούς λογαριασμούς πιστωτικών καρτών. Όταν κάποιος γίνεται πελάτης της CheckFree, πρέπει να δώσει τα στοιχεία ενός τραπεζικού λογαριασμού. Όλες οι μελλοντικές πληρωμές θα γίνονται από το λογαριασμό αυτό. Το μόνο που πρέπει πλέον να κάνει ο πελάτης είναι να δηλώσει στην CheckFree, μέσα από το Internet, το ποσό και τον αποδέκτη. Το σύστημα της CheckFree μπορεί στη συνέχεια να βρει τον καταλληλότερο τρόπο για την πληρωμή του αποδέκτη (π.χ. ηλεκτρονικά ή με ταχυδρομική επιταγή) και να πραγματοποιήσει την πληρωμή χρεώνοντας το αντίστοιχο ποσό στο λογαριασμό του πελάτη. Το κύριο πλεονέκτημα του συστήματος CheckFree είναι ότι έχει στενή επικοινωνία με το τραπεζικό σύστημα και είναι εξαιρετικά εύχρηστο. Επίσης, χρησιμοποιεί ένα υψηλό επίπεδο κρυπτογράφησης για την ασφαλή μετάδοση των πληροφοριών. Το πρόβλημα είναι ότι δεν χρησιμοποιεί κοινά αποδεκτά πρότυπα στον τομέα της κρυπτογράφησης και της ασφάλειας. Αυτό αναμένεται να αλλάξει σύντομα, καθώς οι εταιρίες CheckFree και CyberCash έχουν ξεκινήσει από κοινού την ανάπτυξη ενός συμβατού λογισμικού.

On-line CHECK:

Η εταιρεία On-line CHECK Systems χρησιμοποιεί πολύ ισχυρούς αλγόριθμους κρυπτογράφησης (RSA) για την μετάδοση οικονομικών δεδομένων, τα οποία στη συνέχεια παραδίδει σε έντυπη μορφή στις αρμόδιες τράπεζες.

NetCheque:

Ένα πρότυπο πληρωμής ηλεκτρονικών επιταγών, που χρησιμοποιεί ένα μηχανισμό συμμετρικής κρυπτογράφησης (με μυστικό κλειδί) βασισμένο στο σύστημα Kerberos.

NetChex:

Ένα σχήμα ηλεκτρονικών πληρωμών που βασίζεται στις επιταγές αλλά χρησιμοποιεί πιστωτικές κάρτες για την ρύθμιση των οφειλών. Πρόκειται για ένα ιδιωτικό σύστημα για το οποίο δεν υπάρχουν διαθέσιμες πληροφορίες. Γενικά ο μηχανισμός χρησιμοποιεί ένα κοινό μυστικό.

NetBill:

Ένα σύστημα ηλεκτρονικών επιταγών που χρησιμοποιεί συμμετρική κρυπτογράφηση (με μυστικό κλειδί) βασισμένη στο σύστημα Kerberos. Η ομάδα του πανεπιστημίου Carnegie Mellon που αναπτύσσει το σύστημα NetBill ενδιαφέρεται κυρίως για την πώληση πληροφοριών μέσα από το δίκτυο. Ένας κεντρικός κόμβος διατηρεί οικονομικές πληροφορίες (λογαριασμούς) των χρηστών. Όταν ένας χρήστης ενδιαφέρεται να αγοράσει μια πληροφορία στέλνει στον κόμβο μια κρυπτογραφημένη παραγγελία αντίστοιχης αξίας. Μόλις ο κόμβος βεβαιώσει την παραλαβή της παραγγελίας, επιτρέπει την αποκρυπτογράφηση της πληροφορίας.

CheckMaster:

Η εταιρεία CheckMaster χρησιμοποιεί την τεχνολογία ActiveX της Microsoft για την ηλεκτρονική έκδοση και την ψηφιακή υπογραφή επιταγών. Το σύστημα λειτουργεί με το λογισμικό MS Money της Microsoft και Quicken της Intuit. Τα θέματα ασφάλειας δεν έχουν δημοσιευτεί.

Επικύρωση σε Kerberos:

Σε ένα ανοικτό διανεμημένο υπολογιστικό περιβάλλον (DCE), ένας τερματικός σταθμός δε μπορεί να είναι έμπιστος για να προσδιορίσει τους χρήστες του, επειδή ο τερματικός σταθμός δε μπορεί να βρεθεί σε ένα καλά ελεγχόμενο περιβάλλον και μπορεί να είναι μακριά από τον κεντρικό υπολογιστή. Ένας χρήστης μπορεί να είναι ένας εισβολέας που μπορεί να προσπαθήσει να επιτεθεί στο σύστημα ή να προσποιηθεί ότι είναι κάποιος άλλος για να εξάγει πληροφορίες από το σύστημα στο οποίο δεν έχει δικαίωμα.
Προκειμένου να προστατευθεί ένα σύστημα από τους μακρινούς hosts δικτύων, ένα ορισμένο είδος επικύρωσης πρέπει να ληφθεί υπόψιν.

Το Kerberos είναι ένα από τα συστήματα που παρέχει τις έμπιστες τρίτες-υπηρεσίες επικύρωσης, για να επικυρώσει τους χρήστες σε ένα διανεμημένο δικτυακό περιβάλλον. Βασικά, όταν ζητά ένας χρήστης ή ένας πελάτης μια πρόσβαση σε μια ιδιαίτερη υπηρεσία από το κεντρικό υπολογιστή πρέπει να λάβει ένα εισιτήριο ή ένα πιστοποιητικό από τον υπολογιστή πιστοποίησης (AS) Kerberos. Ο χρήστης έπειτα παρουσιάζει το πιστοποιητικό στο κεντρικό υπολογιστή χορήγησης εισιτηρίων (TGS) και λαμβάνει ένα εισιτήριο υπηρεσιών. Ως εκ τούτου, ο χρήστης μπορεί να ζητήσει την υπηρεσία με την υποβολή του εισιτηρίου υπηρεσιών στο επιθυμητό κεντρικό υπολογιστή.

Έχοντας αυτό το πρωτόκολλο, ο κεντρικός υπολογιστής μπορεί να επιβεβαιώσει τις παρεχόμενες υπηρεσίες στο σωστό πελάτη που έχει δικαίωμα πρόσβασης. Αυτό γίνεται, επειδή ο Kerberos υποθέτει ότι μόνο ο σωστός χρήστης μπορεί να χρησιμοποιήσει το πιστοποιητικό, δεδομένου ότι άλλοι δεν έχουν τον κωδικό πρόσβασης για να το αποκρυπτογραφήσουν. Και επίσης λόγω αυτού, ένας χρήστης μπορεί πραγματικά να κάνει αίτηση με το πιστοποιητικό άλλων. Δηλαδή ο χρήστης δεν επικυρώνεται στο αρχικό στάδιο.

Κατά αυτόν τον τρόπο, ένας εισβολέας μπορεί να λάβει το πιστοποιητικό ενός άλλου χρήστη και να εκτελέσει την off-line επίθεση με τη χρησιμοποίηση ενός υποθετικού κωδικού πρόσβασης, καθώς το εισιτήριο σφραγίζεται μόνο από τον κωδικό πρόσβασης.Αυτή η αδυναμία ασφάλειας του Kerberos επισημαίνεται από τον Mark και Gary (1995) σε ένα από τα άρθρα τους για την ενσωμάτωση της έξυπνης κάρτας στα συστήματα επικύρωσης.

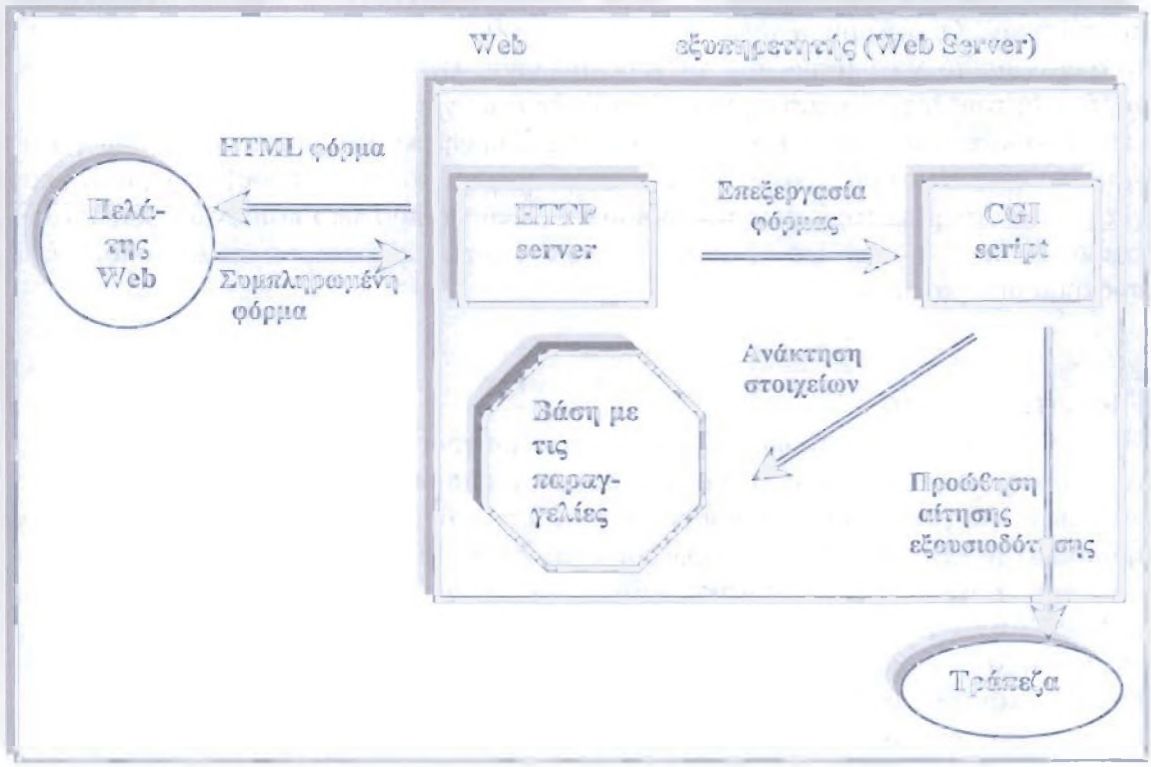
Στην έκθεσή τους, πρότειναν να ενσωματώσουν την έξυπνη κάρτα στο σύστημα Kerberos για να υπερνικήσουν αυτό το πρόβλημα. Έξι διαφορετικά σχέδια προτάθηκαν. Ολόκληρη η ιδέα είναι να ενισχυθεί η ασφάλεια επικύρωσης από το Kerberos με το να επικυρώσει το χρήστη άμεσα και στην αρχή και πριν από την χορήγηση του αρχικού εισιτηρίου , έτσι ώστε ένας χρήστης να μη μπορεί να έχει το εισιτήριο κάποιου άλλου. Και «η χρήση της έξυπνης κάρτας απαιτεί την αναγραφή χρηστών στο σύστημα, όχι μόνο στην ανάκληση του κωδικού πρόσβασης, αλλά και για να είναι στην κατοχή ενός τεκμηρίου». Τελικά, το πρότυπο που αναφέρθηκε εδώ, κατέδειξε πως η τεχνολογία των έξυπνων καρτών μπορεί να εξασφαλίσει ένα σύστημα διαδικαστικά.

Πιστωτικές κάρτες

Ο πλέον διαδεδομένος τρόπος πληρωμής στο Internet βασίζεται στο γεγονός ότι το νούμερο της κάρτας είναι μυστικό και όσοι το χρησιμοποιούν (εστιατόρια, διάφορα μαγαζιά) είναι μέρος του συστήματος ασφαλείας. Δεδομένου ότι είναι ο μόνος τρέχον τρόπος στην Ελλάδα όταν θα αναφερόμαστε στο θέμα της ασφάλειας πληρωμών θα εννοούμε πληρωμές με πιστωτικές κάρτες, εκτός αν γίνετε ρητή αναφορά σε άλλη μέθοδο. Αυτός ο οποίος αναλαμβάνει την διαδικασία της πληρωμής είναι συνήθως μια τράπεζα. Αν για κάποιο λόγο δεν είναι δυνατή η συνεργασία με μία Ελληνική τράπεζα τότε κάποιος θα πρέπει να δοκιμάσει μερικούς ειδικούς οργανισμούς πληρωμών όπως το CCBILL ή το IBILL (και τα δύο στις ΗΠΑ) ή κάτι παρόμοιο. Αυτό ήδη γίνεται από μερικούς τόπους στην Ελλάδα έχει δε κάποια πλεονεκτήματα όπως τις εμπειρίας του οργανισμού, της καλύτερης εξυπηρέτησης λόγω του ανταγωνιστικού διεθνούς περιβάλλοντος αλλά και της διεθνούς εμβέλειας αυτών των εταιριών. Από την άλλη πλευρά, θα χρειαστεί πολύ καλή γνώση αγγλικών, πιθανών συμβόλαια με χώρα επίλυσης διαφορών της ΗΠΑ κλπ. Είναι βέβαια θέμα επιλογής της κάθε εταιρίας, αλλά ένα ψάξιμο στο διαδίκτυο αμέσως πριν την απόφαση και μία έστω αρχική επαφή με κάποιους ξένους οργανισμούς πληρωμών είναι μία καλή τακτική κίνηση, ειδικά αν αναμένονται σκληρές διαπραγματεύσεις με την τράπεζα.

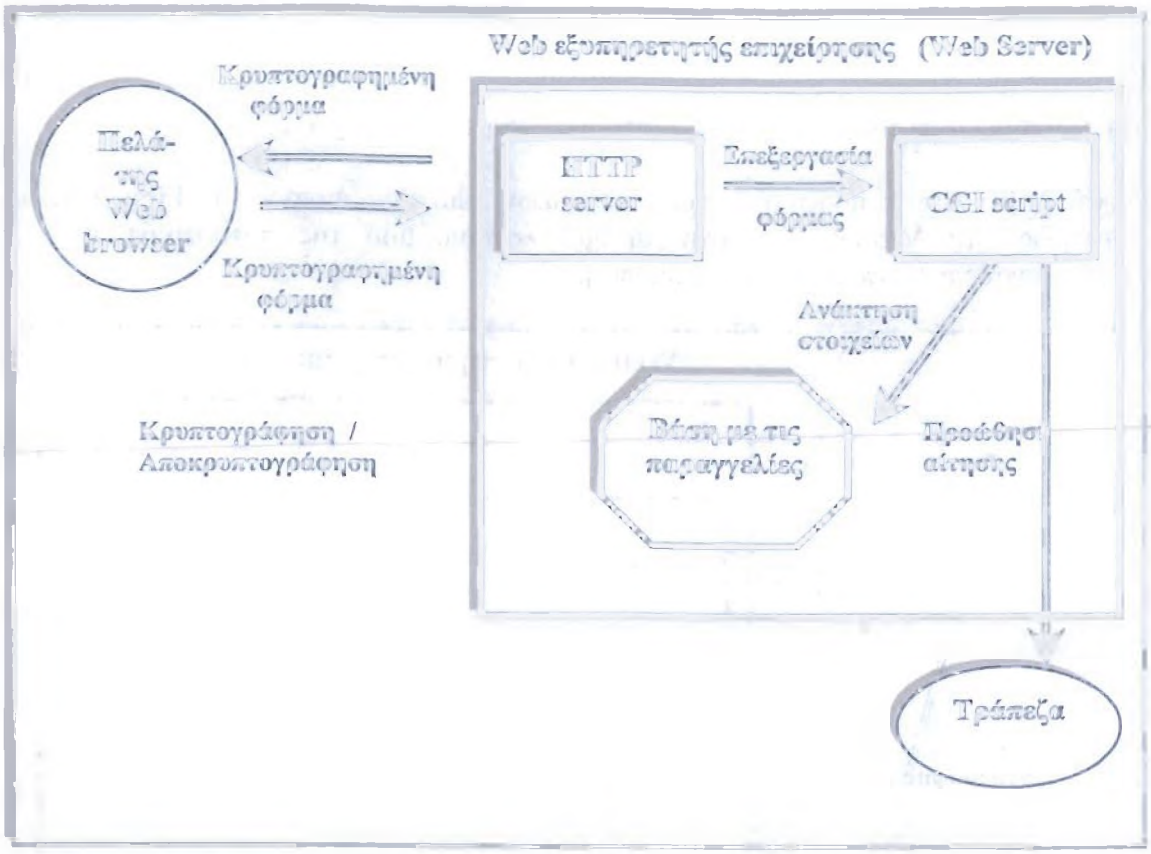
Σε μια παραδοσιακή συναλλαγή με πιστωτική κάρτα, ο προμηθευτής καταγράφει τα στοιχεία της πιστωτικής κάρτας του πελάτη δημιουργώντας ένα έγγραφο συναλλαγής. Το εν λόγω έγγραφο υπογράφεται από τον αγοραστή και προωθείται στη συνέχεια στην τράπεζα για διεκπεραίωση. Στο τέλος η τράπεζα χρεοπιστώνει τους 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 που αναφέρθηκε στην προηγούμενη παράγραφο. Επιπλέον, το σενάριο αυτό εμπλουτίζεται με μηχανισμούς ασφαλείας (π.χ. έλεγχος ταυτότητας πελάτη και εμπόρου). Το γεγονός αυτό έχει οδηγήσει στην ύπαρξη μιας γκάμας συστημάτων ηλεκτρονικών πληρωμών με πιστωτικές κάρτες. Δύο 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 μέρη (αγοραστής, προμηθευτής, τράπεζα).



Σχήμα 1 : Μη Ασφαλής Ανταλλαγή Στοιχείων Πιστωτικής Κάρτας

Κατά τη διάρκεια μιας on-line συναλλαγής, τα στοιχεία της πιστωτικής κάρτας ενός αγοραστή μπορούν να μεταφερθούν με δύο τρόπους. Ο πρώτος τρόπος θεωρείται μη ασφαλής και υποστηρίζει την αποστολή των στοιχείων της ηλεκτρονικής πληρωμής από τον πελάτη στον έμπορο (ή την τράπεζα) σε μη κρυπτογραφημένη μορφή (σχήμα 1). Η μέθοδος αυτή κρίνεται ως μη ασφαλής και υποστηρίζει την αποστολή των στοιχείων της ηλεκτρονικής πληρωμής από τον πελάτη στον έμπορο (ή την τράπεζα) σε μη κρυπτογραφημένη μορφή (σχήμα 1). Η μέθοδος αυτή κρίνεται ως μη ασφαλής γιατί κατά τη μεταβίβαση των στοιχείων μπορεί να παρεισφρήσει 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 την πληρωμή πριν την αποστολή τους στον έμπορο (ή την τράπεζα) μέσω του Internet (σχήμα 2).



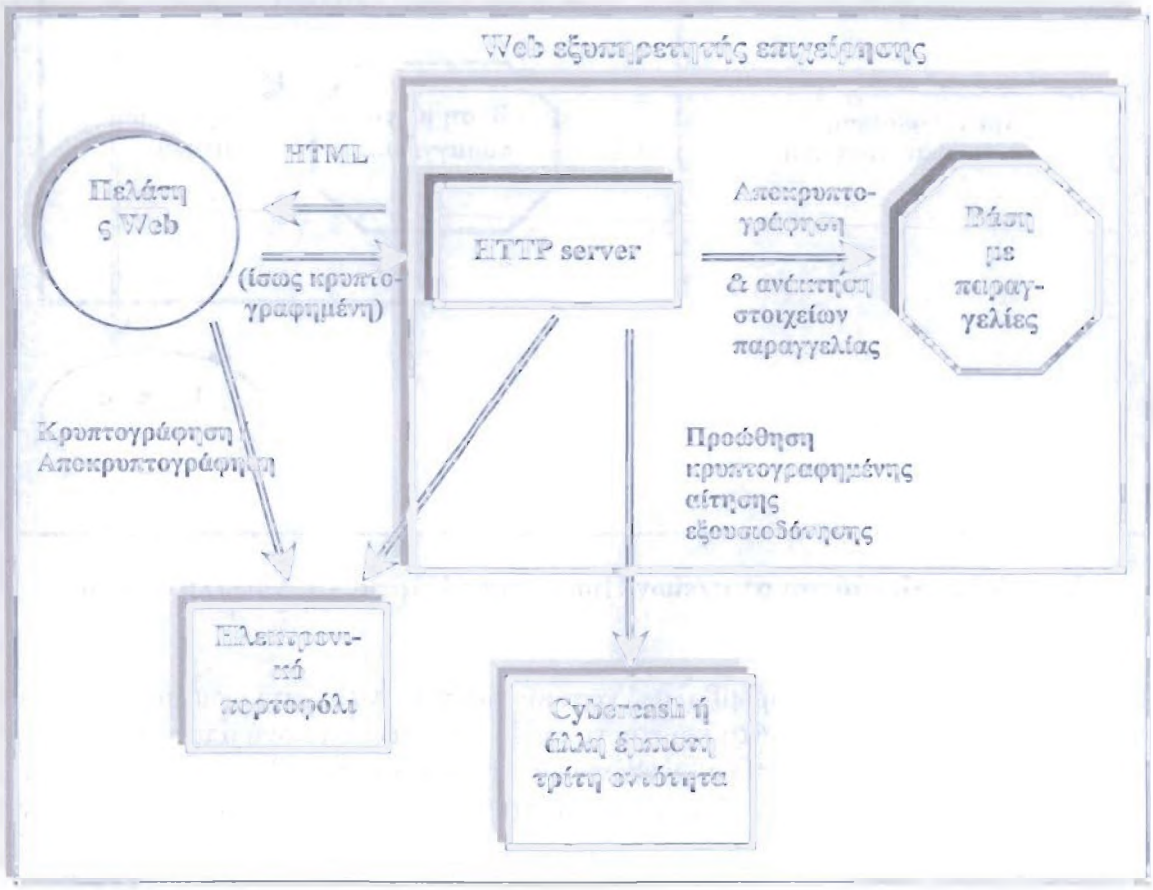
Σχήμα 2 : Μεταβίβαση στοιχείων Πιστωτικής Κάρτας με Ασφαλή Τρόπο

Για την αποφυγή της παρεμβολής κάποιου τρίτου κατά την 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 έμπορο.

Για την αποφυγή εξαπάτησης του πελάτη από τον έμπορο (π.χ. 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 στην όλη διαδικασία αποκρυπτογραφώντας τα στοιχεία της πιστωτικής κάρτας επικυρώνοντας τη συναλλαγή (σχήμα 3).Σε αρκετές περιπτώσεις εταιρίες που παράγουν συστήματα ηλεκτρονικών πληρωμών όπως η Cybercash, η Verifone ή η First Virtual, χρησιμοποιούν μηχανισμούς με τους οποίους παρέχουν υπηρεσίες ΕΤΟ. Όπως φαίνεται και στο (σχήμα 3) η Cybercash και η Verifone χρησιμοποιούν το μηχανισμό των «wallet». Ο μηχανισμός αυτός

μεταφέρει τον κρυπτογραφημένο αριθμό της πιστωτικής κάρτας από τον έμπορο στον δικό τους επεξεργαστή για τον έλεγχο αυθεντικότητας και την έγκριση της συναλλαγής. Η εταιρία First Virtual εκδίδει κάποιο Virtual Pin στον πελάτη που το χρησιμοποιεί αντί του αριθμού της πιστωτικής κάρτας (σχήμα 4).

Αφού λάβει τις πληροφορίες των πωλήσεων από τον έμπορο, η First Virtual μετατρέπει το Virtual Pin στον αριθμό λογαριασμού της πιστωτικής κάρτας προκειμένου να διεκπεραιωθεί η πληρωμή.

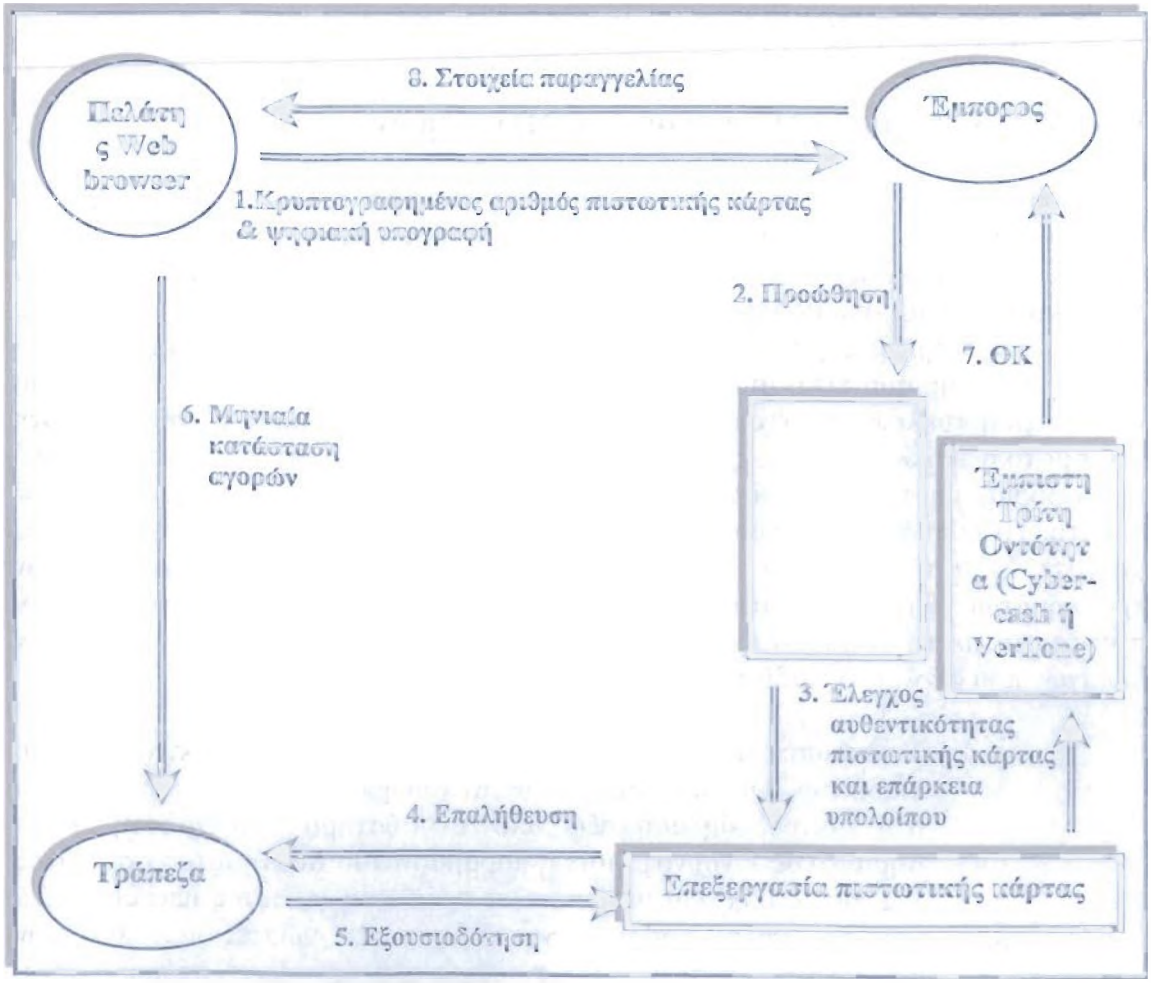


Σχήμα 3 : Χρήση Ηλεκτρονικού Πορτοφολιού & μιας Ενδιάμεσης Έμπιστης Τρίτης Οντότητας

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 Έμπιστης Οντότητας, όπως η Cybercash ή η First Virtual, η επεξεργασία των στοιχείων αυτών δεν γίνεται από τον έμπορο, οπότε και εξαλείφεται ο κίνδυνος απάτης από την πλευρά του τελευταίου.

Στο σημείο αυτό θα πρέπει να σημειωθεί ότι παρά την πρόοδο που έχει σημειωθεί στα συστήματα ηλεκτρονικών πληρωμών με χρήση πιστωτικών καρτών, εξακολουθούν να υπάρχουν ακόμη ορισμένα προβλήματα.

Το σημαντικότερο πρόβλημα που υφίσταται ακόμη είναι η τυποποίηση. Θα πρέπει να υιοθετηθεί μια κοινά αποδεκτή μέθοδος (ή πρότυπο) διεκπεραίωσης των ηλεκτρονικών συναλλαγών στο Internet, που θα επιτρέπει την επικοινωνία μεταξύ των διαφορετικών τύπων λογισμικού των συναλλασσόμενων μερών. Η εξασφάλιση ή όχι αυτής της διαλειτουργικότητας θα καθορίσει και την μελλοντική πορεία των ηλεκτρονικών συστημάτων πληρωμών μέσω πιστωτικής κάρτας.



Σχήμα 4 : Διαχείριση on-line Συναλλαγής με το Σύστημα της Cybercash ή Verifone

Internet Banking

Υπάρχει μια γκάμα πιθανών μεθόδων πληρωμής που χρησιμοποιείται στο Internet. Η πιο συνήθης είναι η χρήση πιστωτικής κάρτας. Δεδομένου ότι αυτή είναι η μόνη ώριμη μέθοδος στην Ελλάδα, θα επικεντρωθούμε σε αυτή. Οι άλλες που υπάρχουν είναι τεχνολογικά ανώριμες ή δεν έχουν φτάσει στην Ελλάδα. Στις τεχνολογικά ανώριμες περιλαμβάνεται το e-cash και σε αυτές που δεν έχουν έρθει στην Ελλάδα περιλαμβάνονται οι ηλεκτρονικές επιταγές.

Τέλος, η ταχύτητα εξελίξεων στο διαδίκτυο είναι τέτοια που πάντα θα πρέπει κάποιος να θεωρεί ότι πάντα θα υπάρχουν μέθοδοι πληρωμών που δεν ξέρει, αλλά θα πρέπει να ψάχνει συνέχεια.

Γενικά Προβλήματα Ηλεκτρονικών Πληρωμών

Τα προβλήματα που μπορεί να παρουσιαστούν στις ηλεκτρονικές πληρωμές είναι ποικίλα και πολλές φορές απρόβλεπτα. Το χαρακτηριστικότερο ίσως πρόβλημα είναι το θέμα της επίδρασης στην νομισματική πολιτική μιας χώρας. Το e-cash μπορεί να δημιουργηθεί από οποιαδήποτε ομάδα και να χρησιμοποιείται από τα μέλη της ομάδας για πληρωμές με βάση κάποιους ιδιωτικούς κανόνες. Αν η ομάδα είναι μεγάλη τότε δημιουργείται μια παράλληλη οικονομία. Η οικονομία αυτή θα έχει μια νομισματική κυκλοφορία, η οποία θα προστεθεί, σε κάποιο σημαντικό ποσοστό, στη νομισματική κυκλοφορία της υπόλοιπης χώρας. Αυτή η επιπλέον νομισματική κυκλοφορία, με την τρέχουσα λογική λειτουργίας μιας κεντρικής τράπεζας είναι αόρατη. Το τελικό αποτέλεσμα είναι η νομισματική πολιτική από δύσκολη να γίνεται αδύνατη. Σε αυτό το στάδιο μια απαρίθμηση (σίγουρα όχι ολοκληρωμένη) μερικών προβλημάτων θα είναι διαφωτιστική, τόσο για τα ίδια τα προβλήματα που σχετίζονται με το δικτυακό εμπόριο και τις πληρωμές του όσο και σαν γεύση των αλλαγών που φέρνει το διαδίκτυο.

- **Υποκλοπές και Hacking:** Είναι οι πιο γνωστοί κίνδυνοι στο διαδίκτυο. Οι υποκλοπές γίνονται συνήθως με ειδικά μηχανήματα στο δίκτυο, δηλαδή έξω από το σύστημα του χρήστη. Είναι σημαντικός κίνδυνος διότι η παράβαση του συστήματος ασφάλειας της πιστωτικής κάρτας αποτελεί πρόκληση για τους hackers, αλλά και ένα καλό εισόδημα για διάφορους γνώστες των θεμάτων ασφάλειας δικτύων. Η συμπεριφορά τέτοιων ατόμων είναι απρόβλεπτη και θα πρέπει να παρατηρηθεί ότι υπάρχουν συλλέκτες ενεργών αριθμών Visa, οι οποίοι δεν τους χρησιμοποιούν, παρά μόνο όταν χρειαστεί να αποδείξουν ότι το νούμερο είναι «ζωντανό». Επίσης θα πρέπει να παρατηρηθεί ότι η συλλογή αριθμών Visa δεν είναι παράνομη στην Ελλάδα. Η υποκλοπή γίνεται με μία διαδικασία η οποία μπορεί να θεωρηθεί αντίστοιχη της τηλεφωνικής υποκλοπής. Η αντιμετώπισή της είναι αρμοδιότητα του ηλεκτρονικού καταστήματος και γι' αυτό αναφέρεται εδώ.

- **Πλαστοπροσωπία:** Ένας σοβαρός αλλά όχι ιδιαίτερα γνωστός κίνδυνος. Έγκειται στο να χρησιμοποιήσει κάποιος τη δικτυακή ταυτότητα κάποιου άλλου με κακόβουλο σκοπό. Η λύση είναι περίπλοκη, τόσο τεχνικά όσο και διαδικαστικά/ νομικά. Μία ιδιόμορφη περίπτωση που μοιάζει με πλαστοπροσωπία είναι η χρήση ενός ονόματος ενός δικτυακού τόπου που να διαφέρει μόνο σε ένα γράμμα από ένα άλλο. Αν τα δύο αυτά γράμματα είναι κοντά στο πληκτρολόγιο τότε ένας υποψήφιος πελάτης, κάνοντας ένα συνηθισμένο λάθος, θα βρεθεί σε άλλο δικτυακό τόπο. Αν ο τόπος αυτός μοιάζει με αυτόν που πραγματικά ήθελε ο πελάτης υπάρχει η πιθανότητα να γίνουν συναλλαγές χωρίς να γίνει αντιληπτό το λάθος. Αυτό το κόλπο χρησιμοποιείται με τα ονόματα των εταιρειών με γνωστό όνομα (λ.χ. αντί να ονομάσουμε τον κόμβο) ώστε να «υποκλέπτεται» ένα ποσοστό της πελατείας της γνωστής εταιρείας.

- **Κλασικές απάτες:** Πεδίον δόξης λαμπρό. Λόγω του ότι οι πληρωμές είναι απρόσωπες και χωρίς να είναι γνωστή η γεωγραφική θέση των μερών, είναι εύκολο να χρησιμοποιηθούν κλασικά μοτίβα εξαπάτησης, τα οποία πολλές φορές έχουν καταπολεμηθεί αποτελεσματικά στη φυσική τους μορφή. Παράδειγμα αποτελούν οι διάφορες μορφές χρηματιστηριακής η ασφαλιστικής εξαπάτησης, τα παράνομα στοιχήματα, οι πυραμίδες κ.λ.π.

- **Ξέπλυμα χρήματος:** Πρόκειται για ένα άλλο θέμα που προκαλεί πονοκεφάλους σε διάφορες αστυνομικές δυνάμεις. Πολλά και ποικίλα κόλπα είναι δυνατά, αλλά τα διάφορα ηλεκτρονικά καζίνο φαίνεται να απαριθμούν τον μεγαλύτερο αριθμό υπόπτων. Υπάρχει μία μικρή πιθανότητα να εμπλακούν και άσχετοι τρίτοι σε μερικά τέτοια κόλπα, γι' αυτό οι εταιρείες που διακινούν πολύ χρήμα θα πρέπει να είναι κάπως φιλύποπτες.

- **Φοροδιαφυγή:** Ο μεγαλύτερος πονοκέφαλος πολλών κυβερνήσεων. Ένα μεγάλο μέρος των εσόδων πολλών κυβερνήσεων προέρχεται από τους έμμεσους φόρους. Δεδομένου όμως ότι πολλές από τις συναλλαγές στο Διαδίκτυο είναι διεθνείς, ο φόρος, όταν πληρώνεται, μένει στην χώρα αποστολής, σε αντίθεση με τα σημερινά δεδομένα. Συνήθως, δε, η χώρα αποστολής δεν θέλει να εισπράξει φόρους από εξαγωγή. Στη χώρα εισαγωγής τώρα είναι σχεδόν αδύνατο να συλληφθεί αυτή η φορολογητέα ύλη, καθώς τα προϊόντα αποστέλλονται σε μικρές ποσότητες μέσω ταχυδρομείου. Το αποτέλεσμα είναι μία τεράστια διαρροή εσόδων για όλες τις χώρες. Το πρόβλημα έχει πάρει και διεθνείς πολιτικές διαστάσεις καθώς το μεγαλύτερο μέρος των εμπορικών τόπων είναι στις Η.Π.Α. και οι καταναλωτές είναι πρακτικά σε όλα τα μήκη και τα πλάτη της γης.

Το αποτέλεσμα αυτής της κατάστασης είναι ότι οι Η.Π.Α εισπράττουν τον εμπορικό όγκο και τα υπόλοιπα κράτη χάνουν τα έσοδα.. Αν η αύξηση του όγκου του ηλεκτρονικού εμπορίου διατηρηθεί στα σημερινά επίπεδα, τότε το πρόβλημα της φοροδιαφυγής / φοροαποφυγής θα εξελιχθεί στο υπ'αριθμόν ένα οικονομικό-πολιτικό πρόβλημα της δεκαετίας. Σε αυτό το στάδιο θα πρέπει να αναμένεται ισχυρή επέμβαση των κυβερνήσεων, αλλά δεν είναι καθόλου βέβαιο ότι θα βρεθεί ικανοποιητική λύση. Σε κάθε περίπτωση, θα πρέπει να αναμένονται σημαντικές αλλαγές στο διεθνές φορολογικό κύκλωμα.

- **Νομισματική πολιτική:** Ένα από τα πλέον ύπουλα προβλήματα του ηλεκτρονικού εμπορίου. Αν οι ηλεκτρονικές πληρωμές είναι σε μορφή e-cash το πρόβλημα είναι άμεσο και εμφανές. Κάποιοι έχουν κόψει χρήμα. Αν το χρήμα αυτό είναι αναξιόπιστο, τότε έχουμε την επανεμφάνιση μιας παλιάς μορφής απάτης. Ουσιαστικά, ξαναγυρίζουμε στην παλιά εποχή όπου οι τράπεζες έκοβαν το νόμισμα (εξού και τραπεζογραμμάτιο) με αντίκρισμα το χρυσό που είχαν υπό φύλαξη. Η κλασσική τραπεζική απάτη ήταν να κοπούν γρήγορα πολλά τραπεζογραμμάτια (περισσότερα από το χρυσό) και εν συνεχεία να πτωχεύσει η τράπεζα. Αν το χρήμα είναι καλό, τότε δημιουργείται μια δικτυακή οικονομία που είναι σε κάποιο βαθμό ανεξάρτητη της πραγματικής. Αν μάλιστα οι αγοραπωλησίες είναι αγοραπωλησίες αγαθών που παράγονται και καταναλώνονται δικτυακά (λ.χ. προγράμματα, σχέδια CAD κ.λ.π.), η οικονομία αυτή μπορεί να είναι τελείως ανεξάρτητη. Αυτή η οικονομική δραστηριότητα δεν εμφανίζεται στις συνήθεις μετρήσεις των κεντρικών τραπεζών (λ.χ. διαθέσιμα τραπεζών ή νομισματικός όγκος) αλλά αργά ή γρήγορα θα εμφανισθεί στην πραγματική οικονομία ως υπερβάλλουσα, άρα πληθωριστική ζήτηση. Τα παραδοσιακά εργαλεία νομισματικής πολιτικής βασίζονται στο γεγονός ότι μόνο η κεντρική τράπεζα μπορεί να κόψει χρήμα και κάθε παραχαράκτης θα πρέπει να χρησιμοποιήσει το σύστημα (Τράπεζες κυρίως) σε κάποιο στάδιο. Με την εμφάνιση του e-cash αυτό παύει να ισχύει. Σχεδόν ο καθένας μπορεί να δημιουργήσει ένα κλειστό κύκλωμα πληρωμών με μικρή επαφή με το παραδοσιακό τραπεζικό σύστημα. Σε αυτές τις συνθήκες κάθε νομισματική πολιτική είναι μάταιη. Γι'αυτό το λόγο οι συγγραφείς πιστεύουν ότι το e-cash θα επιτύχει μόνο αν συμμετέχουν οι Κεντρικές Τράπεζες. Το πρόβλημα είναι σοβαρό ακόμα και αν χρησιμοποιήσουμε πιο παραδοσιακούς τρόπους όπως οι πιστωτικές κάρτες.

Το πρόβλημα εδώ είναι ότι η υπερβάλλουσα ζήτηση δημιουργείται από αλλαγές στη συμπεριφορά της διακίνησης του χρήματος. Η νομισματική πολιτική δεν πρέπει να ελέγχει μόνο τον όγκο του

κυκλοφορούντος χρήματος αλλά και την ταχύτητά του. Με κάποιους περίπλοκούς τρόπους λοιπόν τόσο ο όγκος όσο και η ταχύτητα του χρήματος προκαλούν πληθωρισμό, άρα πρέπει να ελέγχονται από την Κεντρική Τράπεζα. Με την χρήση του διαδικτύου πολλές συναλλαγές αλλάζουν μορφή (π.χ. αντί να αγοράζω βιβλία στην Ελλάδα αγοράζω στο Amazon) με αποτέλεσμα να γίνεται ακόμη πιο δύσκολος ο τρόπος υπολογισμού των παραμέτρων της νομισματικής πολιτικής. Βέβαια εδώ τα πράγματα είναι πιο ελέγξιμα από την περίπτωση του e-cash, όμως το πρόβλημα εξακολουθεί να παραμένει καίριο.

- **Έλλειψη κεντρικού εγγυητή των συναλλαγών:** Το πρόβλημα αυτό είναι συναφές με το προηγούμενο. Μία από τις λειτουργίες μιας Κεντρικής Τράπεζας είναι η εγγύηση του συστήματος πληρωμών. Αν π.χ. κάποιος σας δώσει μια τραπεζική επιταγή και η εκδότρια τράπεζα δεν μπορεί να πληρώσει, τότε η εκδότρια τράπεζα κλείνει και η Κεντρική Τράπεζα πληρώνει από το εκδοτικό προνόμιο. Έτσι, αν μια εγγυημένη μορφής πληρωμή μείνει στον αέρα υπάρχει έσχατος εγγυητής με την ισχύ να επέμβει. Στις πληρωμές μέσω διαδικτύου είναι δύσκολο να φτιάξει κανείς τέτοια εγγυητική αρχή. Ο κίνδυνος που υπάρχει είναι να εγγραφεί ένας μεγάλος αριθμών πληρωμών, να μην συμψηφισθεί άμεσα και η πλευρά που χρωστάει τα λεφτά να κηρύξει στάση πληρωμών στο μέσο της διαδικασίας. Σε αυτή την περίπτωση ο έχων λαμβάνειν θα βρεθεί να έχει δώσει τα λεφτά χωρίς να τα πάρει στο τέλος της ημέρας. Δεδομένου ότι το ποσοστό των διεθνών συναλλαγών στο διαδίκτυο είναι μεγάλο, εγγύηση των πληρωμών στην ουσία σημαίνει είτε κάποιας μορφής παγκόσμια Κεντρική Τράπεζα είτε σοβαρή επανασχεδίαση του παγκόσμιου διατραπεζικού συστήματος πληρωμών. Το πρόβλημα αυτό σε διάφορες μορφές είναι γνωστό τουλάχιστον από τις αρχές της δεκαετίας του 1970 με την πτώχευση μιας Γερμανικής τράπεζας, της Herstatt. Παρά το χρονικό περιθώριο των σχεδόν 30 ετών δε μοιάζει να υπάρχει ακόμη κοινά αποδεκτή λύση. Το μέγεθος του πολιτικού αλλά και του καθαρά τεχνικού προβλήματος είναι εμφανές.

- **Παράκαμψη διαφόρων νόμων & κανόνων:** Κάθε χώρα έχει ένα σύνολο εμπορικών κανόνων για την προστασία του εμπορικού συνόλου. Ένα παράδειγμα είναι οι κανόνες για το εμπόριο φαρμάκων. Με τον απρόσωπο χαρακτήρα του διαδικτύου γίνεται πολύ δύσκολο να εντοπισθούν οι διάφοροι παραβάτες. Είναι πολύ εύκολο λ.χ. κάποιος να στήσει ένα ηλεκτρονικό κατάστημα και να πουλάει ληγμένα φάρμακα σε χαμηλές τιμές και με διάφορες δικαιολογίες. Δεδομένου ότι η βάση λειτουργίας μπορεί να είναι οπουδήποτε στον κόσμο, τότε το πρόβλημα είναι εμφανές.

Το σοβαρότερο πρόβλημα μοιάζει να είναι η διακίνηση Viagra. Ένας στους δύο τόπους διαφημίζει πωλήσεις και δεν είναι δυνατόν να είναι όλο νόμιμο. Το τι αγοράζει κανείς σε τέτοια περίπτωση είναι απροσδιόριστης ποιότητας. Οι πληρωμές σε τέτοιες περιπτώσεις είναι εύκολο να περάσουν απαρατήρητες, διότι η τράπεζα που δίνει την Visa, δύσκολα μπορεί να βρει τι πραγματικά γίνεται.
Το πρόβλημα αυτό είναι συναφές με το θέμα της φοροδιαφυγής. Υπάρχουν παρόμοιες παράμετροι και παρόμοιες δυσκολίες στη λύση του. Δύο τέτοιοι τομείς είναι τα φάρμακα και τα πλαστά μουσικά CDs.

- Δημιουργία δύο παγκόσμιων καταναλωτών: Πρόκειται για ένα εν δυνάμει σοβαρό κοινωνικό πρόβλημα. Ειδικά σε κοινωνίες με σημαντικές οικονομικές ανισότητες ο κίνδυνος είναι ότι οι «συνδεδεμένοι»/ «καλωδιωμένοι» θα γίνουν πλουσιότεροι αγοράζοντας στη φτηνή παγκόσμια αγορά του διαδικτύου, ενώ οι φτωχοί θα παγιδευτούν σε μια πρωτόγονη και ακριβή οικονομία.

Συστήματα Ηλεκτρονικών Πληρωμών

Διαδικασίες Ηλεκτρονικής Πληρωμής

Δεν είναι δυνατό να υπάρξει ηλεκτρονικό εμπόριο χωρίς έναν τρόπο μεταφοράς χρηματικών πόρων (πληρωμής) μέσω της ψηφιακής υποδομής. Κάθε σύστημα ηλεκτρονικής πληρωμής θα πρέπει να καλύπτει όλα τα χαρακτηριστικά που οι διάφορες πλευρές μιας συναλλαγής θεωρούν ως απαραίτητα ή σημαντικά. Σε μια ηλεκτρονική συναλλαγή εμπλέκονται συνήθως τρία μέρη: ο έμπορος (πωλητής), ο πελάτης (αγοραστής), και αυτός που παρέχει οικονομικές υπηρεσίες (οργανισμός πιστωτικών καρτών).

Έμπορος

Το σημαντικότερο χαρακτηριστικό ενός συστήματος πληρωμής, από την πλευρά του εμπόρου, είναι η ευκολία της χρήσης του από τον πελάτη. Ο πελάτης θα πρέπει να έχει τη δυνατότητα να κάνει παρορμητικές αγορές, χωρίς να εμποδίζεται από δυσκολίες που οφείλονται αποκλειστικά στο σύστημα πληρωμής. Ένας από τους λόγους, που ο έμπορος έχει υιοθετήσει το ηλεκτρονικό εμπόριο είναι ότι μπορεί να διευρύνει τη βάση των πελατών του. Αν το σύστημα πληρωμής περιορίζει αυτή τη βάση, το κίνητρο αναιρείται. Έτσι, μια από τις προϋποθέσεις ηλεκτρονικής πληρωμής είναι η ευρεία αποδοχή του.

Ένα δεύτερο χαρακτηριστικό είναι το κόστος των συναλλαγών. Ο έμπορος επιθυμεί να έχει μικρό κόστος συναλλαγών ώστε να μπορεί να μειώσει τις τιμές των προϊόντων και να αυξήσει την ανταγωνιστικότητα του. Ένα μέρος του κόστους συναλλαγών είναι αμοιβή του οικονομικού οργανισμού που ενεργεί στις ηλεκτρονικές πληρωμές. Άλλα στοιχεία του κόστους συναλλαγών είναι ο απαιτούμενος χρόνος για την ολοκλήρωση μιας συναλλαγής και ο κίνδυνος επισφαλών συναλλαγών.

Πελάτης

Πολλά από τα παραπάνω χαρακτηριστικά αφορούν εξίσου τον πελάτη. Ο πελάτης θέλει να αισθάνεται ότι είναι ασφαλής και ότι δε θα πέσει θύμα απατεώνων που θα εκμεταλλευτούν τις πληροφορίες, σχετικά με την ηλεκτρονική πληρωμή του π.χ. αριθμός πιστωτικής κάρτας. Επίσης, θα πρέπει να μπορεί να κάνει ηλεκτρονικές πληρωμές με το ίδιο σύστημα και με την ίδια ευκολία σε πολλούς εμπόρους, όχι μόνο για να έχει τη δυνατότητα επιλογής αλλά και για να αποφεύγει την ταλαιπωρία της εκμάθησης πολλών διαφορετικών μεθόδων πληρωμής. Οι πελάτες δεν μπορούν να ανεχθούν κανένα πρόσθετο κόστος στις συναλλαγές τους, είτε αυτό είναι σε χρήμα είτε σε χρόνο.

Οργανισμός οικονομικών υπηρεσιών

Οι οργανισμοί που υποστηρίζουν ηλεκτρονικές πληρωμές, όπως οι οργανισμοί πιστωτικών καρτών, έχουν ως σκοπό το κέρδος. Έτσι, κάθε συναλλαγή που χρησιμοποιεί ως ενδιάμεσο ένα τέτοιο οργανισμό επιβαρύνεται με την αμοιβή του οργανισμού. Φυσικά, για να κρατούν τις υπηρεσίες τους ελκυστικές, οι οργανισμοί οικονομικών υπηρεσιών κρατούν το κόστος κάθε συναλλαγής αρκετά χαμηλό και προσπαθούν να αυξήσουν τα κέρδη τους με τη διεύρυνση της χρήσης των μέσων πληρωμής που προσφέρουν. Ένα πρόβλημα στο σημείο αυτό είναι η δυσπιστία εμπόρων και καταναλωτών προς τους οικονομικούς οργανισμούς που μονοπωλούν κάποιο μέσο πληρωμής. Η λύση είναι η δημιουργία ενός κοινού μέσου πληρωμής που να υποστηρίζεται από πολλούς οργανισμούς, ώστε να εξασφαλίζεται μια ανταγωνιστική αγορά οικονομικών υπηρεσιών. Ο ανταγωνισμός μπορεί να οδηγήσει στη μείωση του κόστους συναλλαγών και στην προσφορά πρόσθετων υπηρεσιών, που είναι προς το κοινό όφελος καταναλωτών και εμπόρων.

Μία από τις υπηρεσίες προστιθέμενης αξίας που αναλαμβάνουν οι οργανισμοί οικονομικών υπηρεσιών, στα πλαίσια του μεταξύ τους ανταγωνισμού, είναι η διαχείριση των κινδύνων συναλλαγής. Στη διάρκεια μιας ηλεκτρονικής συναλλαγής υπάρχουν πολλοί παράγοντες που μπορεί να προκαλέσουν μια αποτυχία. Για παράδειγμα, ο πωλητής μπορεί να μην λάβει την πληρωμή, ο αγοραστής να μη λάβει το προϊόν για το οποίο ήδη έχει πληρώσει, ενώ τα στοιχεία της πληρωμής μπορούν να υποκλαπούν ή να παραποιηθούν για παράνομους σκοπούς. Ο οικονομικός οργανισμός μπορεί να καλύψει όλους αυτούς τους κινδύνους, όπως να εγγυηθεί στον πωλητή την κάλυψη του ποσού πληρωμής, να βεβαιώσει στον αγοραστή την είσπραξη του ποσού από τον πωλητή και να φροντίσει για την απαραίτητη τεχνολογική υποδομή που θα προστατέψει τις πληροφορίες από υποκλοπή ή παραποίηση. Δύο πολλοί μεγάλοι οργανισμοί που προσφέρουν τέτοιες υπηρεσίες διαχείρισης κινδύνου είναι η γνωστοί οργανισμοί πιστωτικών καρτών Visa και MasterCard.

Μέθοδοι και Πρότυπα Ηλεκτρονικής Πληρωμής

Όλα τα συστήματα ηλεκτρονικής πληρωμής πρέπει να περιλαμβάνουν την έννοια της χρηματικής αξίας και από την άποψη αυτή η μέθοδοι που χρησιμοποιούνται πρέπει να είναι ισοδύναμες με τις υπάρχουσες συνθήκες πληρωμής: το «το ηλεκτρονικό χρήμα » θα πρέπει να είναι ανταλλάξιμο με κάθε άλλη μορφή χρήματος. Θα πρέπει να είναι δυνατή η αποθήκευση και η ανάκτηση, αλλά όχι η αναπαραγωγή του. Λόγω της φύσης του ηλεκτρονικού χρήματος (ψηφιακές πληροφορίες αποθηκευμένες σε κάποιο μέσο), οι διαδικασίες ηλεκτρονικής πληρωμής θα πρέπει να προστατεύουν όλες τις συμβαλλόμενες πλευρές από κάθε εξωτερική επέμβαση στις πληροφορίες αυτές.

Ένα σύστημα ηλεκτρονικής πληρωμής πρέπει επίσης να διαθέτει τα εξής χαρακτηριστικά: ασφάλεια, αξιοπιστία, δυνατότητα μαζικής χρήσης, ανωνυμία, αποδοχή, ευρεία βάση πελατών, ευελιξία, μετατρεψιμότητα, αποτελεσματικότητα, μικρό κόστος και ευκολία χρήσης.

Τα έντεκα αυτά χαρακτηριστικά μπορούν να χρησιμοποιηθούν ως κριτήρια για την ανάλυση των μεθόδων ηλεκτρονικής πληρωμής, η οποία γίνεται με την κρυπτογραφημένη μετάδοση στοιχείων συμβατικής πληρωμής που είναι σήμερα σε χρήση: ψηφιακά μετρητά, λογαριασμοί χρέωσης-πίστωσης, ηλεκτρονικές επιταγές, άμεση μεταφορά και υπηρεσίες είσπραξης.

Κρυπτογραφημένη Μετάδοση Στοιχείων

Η κρυπτογραφημένη μετάδοση στοιχείων συμβατικής πληρωμής (π.χ. αριθμός πιστωτικών καρτών) είναι η ευρύτερα διαδεδομένη μέθοδος σήμερα, που ονομάζεται επίσης μέθοδος της «ασφαλούς αναπαράστασης ». Η κρυπτογραφημένη μετάδοση εξασφαλίζει την ασφάλεια των πληροφοριών, που μπορούν να χρησιμοποιηθούν μόνο από τον έμπορο ή κάποιον ενδιάμεσο οργανισμό.

Το κυριότερο πλεονέκτημα της μεθόδου είναι ότι ο πελάτης και ο έμπορος δεν υποχρεούνται να διατηρούν σχέση με κάποιον ενδιάμεσο οικονομικό οργανισμό προκειμένου να πραγματοποιηθεί μια συναλλαγή. Η διαδικασία της πληρωμής ακολουθεί την συναλλαγή και δεν προϋποθέτει καμία προεργασία (pull model), ενώ έτσι ευνοούνται οι παρορμητικές αγορές και διευρύνεται η βάση πελατών. Ο κίνδυνος των οικονομικών δεδομένων που μεταδίδονται κρυπτογραφημένα, μέσω του δικτύου είναι πολύ μικρότερος από τον κίνδυνο μετάδοσης των ίδιων δεδομένων με συμβατικό τρόπο (π.χ. ταχυδρομικά ή τηλεφωνικά).

Το αδύνατο σημείο αυτής της μεθόδου δεν είναι η μετάδοση των οικονομικών πληροφοριών αλλά η αποθήκευσή τους στους ηλεκτρονικούς υπολογιστές του εμπόρου ή του ενδιάμεσου οργανισμού, όπου παραμένουν μετά την ολοκλήρωση της συναλλαγής και μπορούν να υποκλαπούν από κάποιον που μελλοντικά θα διεισδύσει παράνομα στους υπολογιστές αυτούς. Ο κίνδυνος αυτός μπορεί να προληφθεί με την τήρηση αυστηρών μέτρων ασφαλείας από τον έμπορο ή τον ενδιάμεσο οργανισμό.

Ένα δεύτερο μειονέκτημα είναι το κόστος της χρήσης ενός ενδιάμεσου οργανισμού για την πραγματοποίηση των πληρωμών. Ειδικά, αν ή τιμή των προϊόντων είναι πολύ μικρή, το κόστος μιας συναλλαγής μπορεί να είναι υψηλότερο από το αντίστοιχο της πώλησης.

Χώρα	Χαρακτήρας σχεδίου/ όνομα	Θέση-κυκλοφορία
Βέλγιο	Bankpas/proton	Εθνικό roll-out
Κίνα	Τράπεζα της Κίνας	Δοκιμή εν εξελίξει
Χονγκονγκαϊκά	Easy card	Roll-out σε 100 καταστήματα
Δανία	Dankort	Εθνικό roll-out
Φινλανδία	Avant	Εθνικό roll-out
Ολλανδία	Chipper	Roll-out 1997
Ολλανδία	Chip Knip	Πειραματικό εν εξελίξει
Πορτογαλία	SIBS/Multibanco	Εθνικό roll-out
Σιγκαπούρη	Nets/CashCard	Εθνικό roll-out
Ισπανία	SEMP	Εθνικό roll-out
Ελβετία	Swiss PTT/Postcard	Πιλότο roll-out
Ταϊβάν	FISC	Roll-out
Ταϊλάνδη	Ταϊλανδική τράπεζα αγροτών	Δοκιμή πλάνου
U.K	Mondex (master card)	Πιλότοι στη U.K, τον Καναδά & το Hong-Kong
Διεθνή	VisaCash	U.K

Πίνακας 1 : Συστήματα κρυπτογραφημένης μετάδοσης

Ψηφιακά Μετρητά

Τα «ψηφιακά μετρητά» είναι ένα μέσο ηλεκτρονικής πληρωμής ανάλογο με τα κοινά μετρητά, κέρματα και χαρτονομίσματα. Ο πελάτης έχει ένα «ηλεκτρονικό πορτοφόλι» συνήθως με τη μορφή μιας ειδικής ηλεκτρονικής κάρτας που το «φορτώνει» χρήματα από τον τραπεζικό λογαριασμό ή πληρώνοντας τα αντίστοιχα μετρητά στο ταμείο μιας τράπεζας. Η κάρτα είναι ανώνυμη και έχει αποθηκευμένη την αξία των χρημάτων με τα οποία έχει «φορτωθεί». Ένας έμπορος που δέχεται ψηφιακά μετρητά μπορεί να αφαιρέσει ένα ποσό από την κάρτα και να το μεταφέρει σε ένα δικό του ηλεκτρονικό πορτοφόλι. Ο οικονομικός οργανισμός που υποστηρίζει τα ψηφιακά μετρητά μπορεί στη συνέχεια να ανταλλάξει την αξία που είναι αποθηκευμένη στην κάρτα του εμπόρου με κοινά χρήματα.

Τα ψηφιακά μετρητά έχουν δύο πλεονεκτήματα. Το πρώτο που έχει ιδιαίτερη σημασία για τους πελάτες, είναι η ανωνυμία των συναλλαγών. Το δεύτερο είναι η δυνατότητα χρήσης των ψηφιακών μετρητών ως μέσο πληρωμής ακόμη και χωρίς τη μεσολάβηση του οικονομικού οργανισμού που τα υποστηρίζει.

Για παράδειγμα, ένας έμπορος μπορεί να χρησιμοποιήσει απευθείας το ηλεκτρονικό του πορτοφόλι για να πληρώσει τις προμήθειές του, χωρίς να είναι υποχρεωμένος να το ξεφορτώσει στον τραπεζικό του λογαριασμό ή να μετατρέψει το περιεχόμενό του σε άλλο μέσο πληρωμής. Μελλοντικά, η χρησιμοποίηση του ηλεκτρονικού χρήματος προβλέπεται να επιταχθεί και να υποκαταστήσει σε μεγάλο βαθμό το χρήμα στη φυσική του μορφή.

CyberCash:

Ένα σύστημα που χαρακτηρίζεται ως «ηλεκτρονικό πορτοφόλι» και χρησιμοποιεί την τεχνική της κρυπτογράφησης με δημόσιο κλειδί (πάνω σε λογισμικό της RSA Data Security). Το «πορτοφόλι» μπορεί να αποθηκεύσει πληροφορίες για διάφορες πιστωτικές κάρτες και ο κάτοχος μπορεί να επιλέξει ποια θα χρησιμοποιήσει κάθε φορά. Στη συνέχεια, στέλνει τις πληροφορίες της πιστωτικής κάρτας μαζί με πληροφορίες για τη συναλλαγή στην εταιρεία CyberCash, η οποία αποκρυπτογραφεί τα δεδομένα και φροντίζει για την έγκριση της πληρωμής από την αρμόδια τράπεζα. Μετά την έγκριση, τα δεδομένα στέλνονται κρυπτογραφημένα στον πωλητή, που εκδίδει μια ηλεκτρονική απόδειξη και παραδίδει το προϊόν στον αγοραστή.

Το σύστημα CyberCash έχει ήδη ολοκληρωθεί και βρίσκεται σε χρήση από ένα μεγάλο αριθμό επιχειρήσεων κάθε μεγέθους, που δραστηριοποιούνται στο ηλεκτρονικό εμπόριο. Ο κίνδυνος για τους αγοραστές που χρησιμοποιούν το σύστημα CyberCash είναι ελάχιστος και συχνά καλύπτεται από την πολιτική των οργανισμών πιστωτικών καρτών (για παράδειγμα στις ΗΠΑ οι οργανισμοί πιστωτικών καρτών καλύπτουν κάθε απώλεια αξίας πάνω από 50$). Το πλεονέκτημα του συστήματος CyberCash είναι ότι χρησιμοποιεί ισχυρή κρυπτογράφηση και συγχρόνως μπορεί να περνά χωρίς πρόβλημα από φίλτρα πρόσβασης στο Internet. Το κύριο μειονέκτημα είναι ότι δεν προστατεύει την ανωνυμία του αγοραστή, όπως συμβαίνει πάντοτε με την χρήση πιστωτικών καρτών.

SET:

Οι δύο μεγαλύτεροι οργανισμοί πιστωτικών καρτών VISA και MasterCard, σε συνεργασία με έναν αριθμό μεγάλων επιχειρήσεων από τον χώρο της πληροφορικής τεχνολογίας, έχουν αναπτύξει το πρωτόκολλο SET, για την ασφαλή πραγματοποίηση συναλλαγών μέσα από ψηφιακά κέντρα. Οι πληροφορίες που μεταδίδονται σύμφωνα με το πρωτόκολλο SET, προστατεύονται με κρυπτογράφηση με δημόσιο κλειδί. Το πρωτόκολλο SET, απαιτεί την ύπαρξη ειδικού λογισμικού στον υπολογιστή του αγοραστή όπως και στον κόμβο του πωλητή.

Βασικά, το πρωτόκολλο SET, περιλαμβάνει τις ίδιες διαδικασίες που υπάρχουν ήδη για την πληρωμή με πιστωτικές κάρτες: ο πωλητής επικοινωνεί (τηλεφωνικά ή μέσα από ειδική συσκευή) με τον οργανισμό πιστωτικών καρτών, δίνει τον αριθμό της πιστωτικής κάρτας του αγοραστή και την αξία της πώλησης και ζητά έγκριση της συναλλαγής.

Στη συνέχεια ο πωλητής εισπράττει την πληρωμή του από την τράπεζα που έχει εκδώσει την πιστωτική κάρτα και ο αγοραστής πρέπει να καλύψει το υπόλοιπο της πιστωτικής κάρτας σύμφωνα με τους όρους που έχει συμφωνήσει με την τράπεζα. Το πρωτόκολλο SET, ουσιαστικά επιτρέπει την επικοινωνία για την έγκριση της συναλλαγής μέσα από το ψηφιακό δίκτυο.

Το πρωτόκολλο SET, είναι ένα πολύπλοκο και συμπαγές σύστημα που χρησιμοποιεί την ισχυρότερη υπάρχουσα μέθοδο κρυπτογράφησης και ψηφιακά πιστοποιητικά για την προστασία κάθε συναλλαγής. Σε κάθε συναλλαγή συμμετέχουν τέσσερα μέρη: ο αγοραστής, ο πωλητής, η τράπεζα και ο οργανισμός πιστωτικών καρτών. Αυτό σημαίνει ότι για κάθε συναλλαγή πρέπει να δημιουργούνται και να μεταδίδονται πολλά ψηφιακά πιστοποιητικά, κάτι που δεν έχει ακόμα δοκιμαστεί στην πράξη σε μεγάλη κλίμακα.

Visa Cash:

Η Visa έχει αναγγείλει πρόσφατα την κάρτα καταχωρημένης αξίας (SVC) που βασίζεται αρχικά στο Δανικό σύστημα Danmont, το οποίο μπορεί να είναι στη μορφή μιας χρήσης ή επαναφορτώσιμης κάρτας ολοκληρωμένου κυκλώματος. Η μιας χρήσης κάρτες φορτώνονται εκ των προτέρων με ένα καθορισμένο ποσό που οι καταναλωτές μπορούν να ξοδεύουν μέχρι να μηδενιστεί. Η Visa Cash άρχισε την επέκταση με 3.000.000 κάρτες στους Ολυμπιακούς αγώνες του 1996 στην Ατλάντα.

Η επαναφορτώσιμες κάρτες μπορούν να συμπληρωθούν σε ATMs, στις συσκευές φόρτωσης και στα μελλοντικά τηλέφωνα και PCs. Η επαναφορτώσιμη έκδοση μπορεί ακόμα και να "συγκατοικήσει" με άλλες λειτουργίες, όπως η πίστωση ή η χρέωση μέσα σε μια ενιαία κάρτα. στη UK, έξι σημαντικά ιδρύματα τίθενται ως στόχος να τρέξουν μια δοκιμή της Visa Cash το 1997 σε διάφορες σημαντικές πόλεις.

Danmont:

Μια από τις πιο γνωστές διαδικασίες ηλεκτρονικών πορτοφολιών είναι το σχέδιο Danmont που προωθείται στη Δανία το 1992. το Danmont χρησιμοποιεί τις προπληρωμένες κάρτες (τηλεφωνίας) στις διάφορες αξίες. Οι κάρτες χρησιμοποιούνται ατά ένα μεγάλο μέρος στις διαδικασίες χαμηλής αξίας, όπως στους μετρητές στάθμευσης και σε μερικά καταστήματα. Από την ολοκλήρωση της αρχικής τεχνολογικής δοκιμής στο Naestved στην νοτιοδυτική Δανία, το σχέδιο έχει επεκταθεί σε περισσότερες από 20 δανικές πόλεις. Κατά την διάρκεια του 1995, το Danmont εισήγαγε τις επαναφορτώσιμες κάρτες που

μπορούν να φορτωθούν με μετρητά από λογαριασμούς τραπεζών σε ATM. Οι συναλλαγές είναι off-line με μια ασφαλή εφαρμογή που χρησιμοποιείται για να επικυρώσει την κάρτα και να προσδιορίσει μια αναφορά συναλλαγής. Οι λεπτομέρειες καταχωρούνται στα τερματικά για την προς τα εμπρός μεταφορά στο κεντρικό σύστημα, όπου επικυρώνεται και ένα ίχνος ελέγχου διατηρείται έως ότου εξαντληθεί η αξία της κάρτας.

Avant:

Το Φιλανδικό σχέδιο ηλεκτρονικών πορτοφολιών Avant εισήχθη στο τέλος του 1992 για τη χρήση στους κερματοδέκτες και τους μετρητές χώρου στάθμευσης στην περιοχή του Ελσίνκι, το σχέδιο αναπτύχθηκε από το Setec Oy, έναν εκτυπωτή ασφάλειας και ένα υποκατάστημα της τράπεζας της Φιλανδίας. Όπως το Danmont, το σύστημα άρχισε με τις προπληρωμένες, μιας χρήσης κάρτες, αν και υπάρχουν σχέδια για να προωθήσουν τις επαναφορτώσιμες κάρτες για τη χρήση σε ATMs σύντομα. Στα προηγούμενα δύο έτη, το σχέδιο Avant επεκτείνεται αργά και σταθερά με εφαρμογές όπως στο σύστημα σφράγισης στο ταχυδρομείο του Ελσίνκι, τα διόδια, τις μηχανές πώλησης και τις κάρτες πόλεων.

Proton:

Το Βελγικό σχέδιο ηλεκτρονικών πορτοφολιών άρχισε τις δοκιμές στο Leuven και στο Wavre το 1995.το Banksys είναι η Βελγική διατραπεζική λειτουργία, για τις ηλεκτρονικές πληρωμές και την Proton κάρτα, και στοχεύουν στης μικρής αξίας συναλλαγές μέσα στην υπάρχουσα λειτουργία Bancontact/ MasterCash. Ο πιλότος περιλαμβάνει περίπου 50.000 κάρτες αρχίζοντας από τις επαναφορτώσιμες και βαθμιαία την μετανάστευση της τεχνολογίας στις κάρτες πίστωσης και χρέωσης των πελατών, που θα έχουν έτσι μια ενιαία συνδυασμένη λειτουργία ηλεκτρονικών πορτοφολιών.

Το Banksys παρέχει τις λειτουργίες του προμηθευτή πορτοφολιών, του SAM εκδότη, του Load Agent και του αγοραστή. Οι κάρτες εκδίδονται από τις συμμετέχουσες τράπεζες που παρέχουν την εγγύηση των κεφαλαίων. Το σχέδιο είναι ανοικτό σε οποιονδήποτε κρατά μια κάρτα Proton. Η ηλεκτρονική αξία που περιλαμβάνεται στο τερματικό αγορών μπορεί να φορτωθεί από ένα τραπεζικό λογαριασμό μέσω ενός modem. Αυτό είναι πολύ χρήσιμο αφού, παραδείγματος χάριν, ξεφορτώνει τα κεφάλαια από μια off-line μηχανή πώλησης.

Οι αγορές μπορούν να γίνουν σε οποιονδήποτε παροχέα της υπηρεσίας. Οι πολλαπλές χρήσεις επιτρέπονται ενώ παρέχεται και η ευκολία κλειδώματος του κεφαλαίου. το σύστημα σχεδιάστηκε για να είναι ανώνυμο και οι κάρτες είναι επομένως μεταβιβάσιμες μεταξύ των ανθρώπων. Το Proton έχει χορηγήσει την άδεια της τεχνολογίας σε μια ομάδα Ολλανδικών τραπεζών υπό τον τίτλο ChipKnip.

Mondex:

Το Mondex είναι μια πρωτοβουλία πληρωμής που αναπτύσσεται από την Εθνική τράπεζα Westminster (εθνική δύση) στη UK για να διατηρήσει τα χαρακτηριστικά γνωρίσματα του πυρήνα που κάνουν τα μετρητά την κυρίαρχη μέθοδο παγκόσμιας πληρωμής και προσθέτοντας τα σημαντικά οφέλη.

Στην καρδιά του Mondex είναι το ηλεκτρονικό πορτοφόλι (EP), που εφαρμόζεται στις ανθεκτικές στην πλαστογράφηση κάρτες ολοκληρωμένου κυκλώματος, στις οποίες η αξία καταχωρείται. Το Mondex είναι ένα ανοιχτό σύστημα πληρωμής όπου η αξία μπορεί να μεταφερθεί από το ένα πορτοφόλι σε ένα άλλο χωρίς την ανάγκη για οποιαδήποτε έγκριση, καθάρισμα, ή τακτοποίηση μετά από την συναλλαγή.

Είναι ένα σύστημα ψηφιακών μετρητών που βασίζεται σε ειδικές ηλεκτρονικές κάρτες (smart cards) και απαιτεί προεργασία για την χρήση του. Οι ψηφιακές κάρτες εξασφαλίζουν μια φορητότητα και ανεξαρτησία από το είδος του ψηφιακού δικτύου, ανάλογη με αυτήν ενός μεταλλικού νομίσματος. Ουσιαστικά πρόκειται για μια πλαστική κάρτα, που εξωτερικά μοιάζει με μια πιστωτική κάρτα που μπορεί να «φορτωθεί» με ένα χρηματικό ποσό και να χρησιμοποιηθεί σε διαφορετικές συσκευές είσπραξης.

Η ανεξαρτησία των καρτών αυτών είναι το κυριότερο πλεονέκτημα τους. Η αξία τους είναι αποθηκευμένη μέσα σε αυτές και δεν χρειάζονται έγκριση από κανένα κεντρικό οργανισμό. Είναι ένα πραγματικό ψηφιακό χρήμα και όχι απλά μια επέκταση των πιστωτικών καρτών. Οι κίνδυνοι είναι ίδιοι με αυτούς των κοινών μετρητών. Αν ο κάτοχος χάσει την κάρτα του, χάνει το χρηματικό ποσό που υπήρχε φορτωμένο σε αυτήν. Όμοια, αν μια κάρτα κλαπεί, το περιεχόμενο περνά στον κλέφτη.

Ο κάτοχος έχει την ελευθερία να χρησιμοποιήσει την κάρτα χωρίς να αφήνει ίχνη των συναλλαγών του και φυσικά να την δώσει στο παιδί του χωρίς κανένα πρόβλημα.

Η τράπεζα της Σκωτίας ανήγγειλε το 1995 ότι είχε υπογράψει το Mondex.η τράπεζα του Hong Kong και της Σαγκάης έχει αγοράσει τα δικαιώματα προνομίων για την Άπω Ανατολή και είναι αυτήν την περίοδο στο στάδιο της έκδοσης των προνομίων του Mondex στους κατάλληλους συνεργάτες. Το Mondex συνεχίζει να παραμένει το πιο κομψό σχέδιο ηλεκτρονικών πορτοφολιών στον κόσμο. Είναι μια ανεξάρτητη λύση στο παγκόσμιο πρόβλημα των πληρωμών. Η δύναμη του Mondex βρίσκεται στη συλλογική δύναμη των δικαιοδόχων της.

CyberCoin:

Μια τεχνολογία ψηφιακών μετρητών, που μπορεί να χρησιμοποιηθεί για συναλλαγές ελάχιστης αξίας. Στηρίζεται στο «ηλεκτρονικό πορτοφόλι» της CyberCash, που έχει αναφερθεί παραπάνω. Το χρηματικό ποσό με το οποίο «φορτώνεται» το πορτοφόλι δεν μεταφέρεται πραγματικά με το οποίο «φορτώνεται» το πορτοφόλι δεν μεταφέρεται πραγματικά, αλλά δεσμεύεται από την τράπεζα μέχρι ο πελάτης να πληρώσει για μια αγορά-οπότε μεταφέρεται στον λογαριασμό του πωλητή.

Οι συναλλαγές δεν είναι ανώνυμες, ενώ η Cyber Cash αναλαμβάνει την ευθύνη για την παράδοση των προϊόντων. Με τον τρόπο αυτό, το σύστημα μοιάζει πάρα πολύ με τη χρήση υπηρεσιών είσπραξης.

Το κύριο πλεονέκτημα της μεθόδου αυτής είναι η υποστήριξη που βρίσκει στην αγορά. Κορυφαία στελέχη από τον κλάδο της επεξεργασίας συναλλαγών και της κρυπτογράφησης εργάζονται πάνω στ σύστημα CyberCoin. Η κύρια αδυναμία του είναι η έλλειψη ανωνυμίας. Μοιράζεται επίσης, το πρόβλημα όλων των μεθόδων που δεν χρησιμοποιούν τις ειδικές κάρτες smart card, δηλαδή ότι οι πληροφορίες αποθηκεύονται σε ηλεκτρονικούς υπολογιστές και αργά ή γρήγορα μπορεί κάποιος μη εξουσιοδοτημένος να τις αποκρυπτογραφήσει ή να τις χρησιμοποιήσει για παράνομους σκοπούς.

Ηλεκτρονική Μεταφορά Κεφαλαίων

Η ηλεκτρονική μεταφορά πίστωσης είναι πράξη πραγματοποιούμενη με πρωτοβουλία του εντολέα μέσω ιδρύματος ή υποκαταστήματος ιδρύματος, με σκοπό να τεθεί στη διάθεση του δικαιούχου χρηματικό ποσό σε ένα ίδρυμα ή υποκατάστημα ιδρύματος. Ο εντολέας και ο δικαιούχος είναι δυνατόν να είναι ένα και το αυτό πρόσωπο. Η ηλεκτρονική μεταφορά κεφαλαίων είναι δυνατόν να είναι και διασυνοριακή, δηλαδή η μεταφορά να γίνεται όχι μόνο μέσα στο ίδιο κράτος αλλά και μεταξύ κρατών. Στην Ελλάδα τα θέματα των διασυνοριακών μεταφορών πιστώσεων ρυθμίζει το Π.Δ. 33/2003, το οποίο εναρμονίζει την ελληνική νομοθεσία με την Οδηγία 1997/5. Στην Ευρώπη ισχύει ακόμη και ο Κανονισμός 2560/2001

Λογαριασμοί Χρέωσης - Πίστωσης

Το σύστημα των λογαριασμών χρέωσης-πίστωσης προϋποθέτει την υποδομή της τήρησης λογαριασμού τόσο από τον πωλητή όσο και από τον αγοραστή σε κάποιο ενδιάμεσο οικονομικό οργανισμό. Όταν πραγματοποιείται μια συναλλαγή, η αξία της αφαιρείται από τον λογαριασμό του αγοραστή και μεταφέρεται στο λογαριασμό του πωλητή. Στη διάρκεια της διαδικασίας πληρωμής ο ενδιάμεσος οργανισμός έχει την ευθύνη για την πιστοποίηση της ταυτότητας του αγοραστή. Ο λογαριασμός του αγοραστή μπορεί να λειτουργεί με δύο τρόπους: είτε η αξία των αγορών να καλύπτεται προκαταβολικά, είτε να εξοφλείται μετά την πραγματοποίησή τους. Ανάλογα με τον τρόπο λειτουργίας, ο λογαριασμός ονομάζεται χρεωστικός ή πιστωτικός.

Το κύριο πλεονέκτημα αυτής της μεθόδου είναι η ευελιξία. Ο ίδιος μηχανισμός μπορεί να χρησιμοποιηθεί για πολλά είδη συναλλαγών. Αν χρειαστεί, το σύστημα μπορεί επίσης να επιτρέπει ανώνυμες συναλλαγές. Το μειονέκτημα της μεθόδου είναι ότι η προεργασία για την πληρωμή προηγείται της συναλλαγής (push model) και κάθε

πελάτης πρέπει να έχει ανοίξει λογαριασμό πριν πραγματοποιήσει την πρώτη του αγορά. Έτσι, το σύστημα δεν υποστηρίζει παρορμητικές αγορές.

Άμεση Μεταφορά

Αν ο αγοραστής και ο πωλητής διατηρούν λογαριασμό στον ίδιο οικονομικό οργανισμό, ο αγοραστής μπορεί να δώσει ηλεκτρονικά εντολή για τη μεταφορά του ποσού πληρωμής στο λογαριασμό του πωλητή. Μόλις ο πωλητής βεβαιωθεί για την είσπραξη της πληρωμής μπορεί να παραδώσει το προϊόν στον αγοραστή. Η μέθοδος αυτή είναι μια από τις σπανιότερα χρησιμοποιούμενες και έχει τα ίδια πλεονεκτήματα και μειονεκτήματα με τους λογαριασμούς χρέωσης-πίστωσης.

Υπηρεσίες Είσπραξης

Οι υπηρεσίες είσπραξης, που ονομάζονται επίσης εκκαθάρισης συναλλαγών, δεν είναι μία αυτόνομη μέθοδος πληρωμής αλλά ένα μέσο για την πραγματοποίηση των πληρωμών με τις μεθόδους που έχουν αναφερθεί παραπάνω. Οι υπηρεσίες είσπραξης είναι ενδιάμεσοι που αναλαμβάνουν την είσπραξη πληρωμών για λογαριασμό των εμπόρων. Ο αγοραστής λαμβάνει από τον έμπορο τις απαραίτητες πληροφορίες για να πληρώσει στην υπηρεσία είσπραξης, η οποία δέχεται την πληρωμή και επιστρέφει στον πελάτη μία απόδειξη, με την οποία αυτός μπορεί να παραλάβει το προϊόν που έχει αγοράσει. Η διαδικασία της συναλλαγής περιπλέκεται, αλλά ο έμπορος έχει το πλεονέκτημα ότι η υπηρεσία είσπραξης μπορεί να δεχθεί όλες τις μεθόδους ηλεκτρονικής πληρωμής.

First Virtual:

Το σύστημα First Virtual προσφέρει ασφαλείς ηλεκτρονικές συναλλαγές με τη χρήση ενός ειδικού αριθμού αναγνώρισης των πελατών, που ονομάζεται VirtualPIN αντί για αριθμούς πιστωτικών καρτών, οι οποίοι είναι αποθηκευμένοι σε ασφαλείς ηλεκτρονικούς υπολογιστές της First Virtual που δεν είναι συνδεδεμένοι στο Internet. Ο αγοραστής δίνει στον πωλητή τον αριθμό VirtualPIN. Ο πωλητής επικοινωνεί με την First Virtual, η οποία ζητά από τον αγοραστή να επιβεβαιώσει τη συναλλαγή. Τότε μόνο η πιστωτική κάρτα του αγοραστή χρεώνεται με την αξία της αγοράς.

InterCoin:

Η εταιρεία InterCoin προσφέρει υπηρεσίες ηλεκτρονικής πληρωμής σε μηνιαία βάση. Ο πελάτης μπορεί να πραγματοποιεί αγορές αξίας κάτω των 10 δολαρίων, της οποίες εξοφλεί συνολικά στο τέλος του μήνα. Το κόστος των συναλλαγών δε χρεώνεται στον αγοραστή αλλά στον πωλητή. Τα οικονομικά στοιχεία των πελατών αποθηκεύονται σε ασφαλείς ηλεκτρονικούς υπολογιστές που δεν είναι συνδεδεμένοι στο Internet.

TelPayZ:

Ένα σύστημα που επιτρέπει την πληρωμή λογαριασμών από το Internet. Δεν υπάρχουν περαιτέρω πληροφορίες.

Πρότυπα Ηλεκτρονικών Πληρωμών

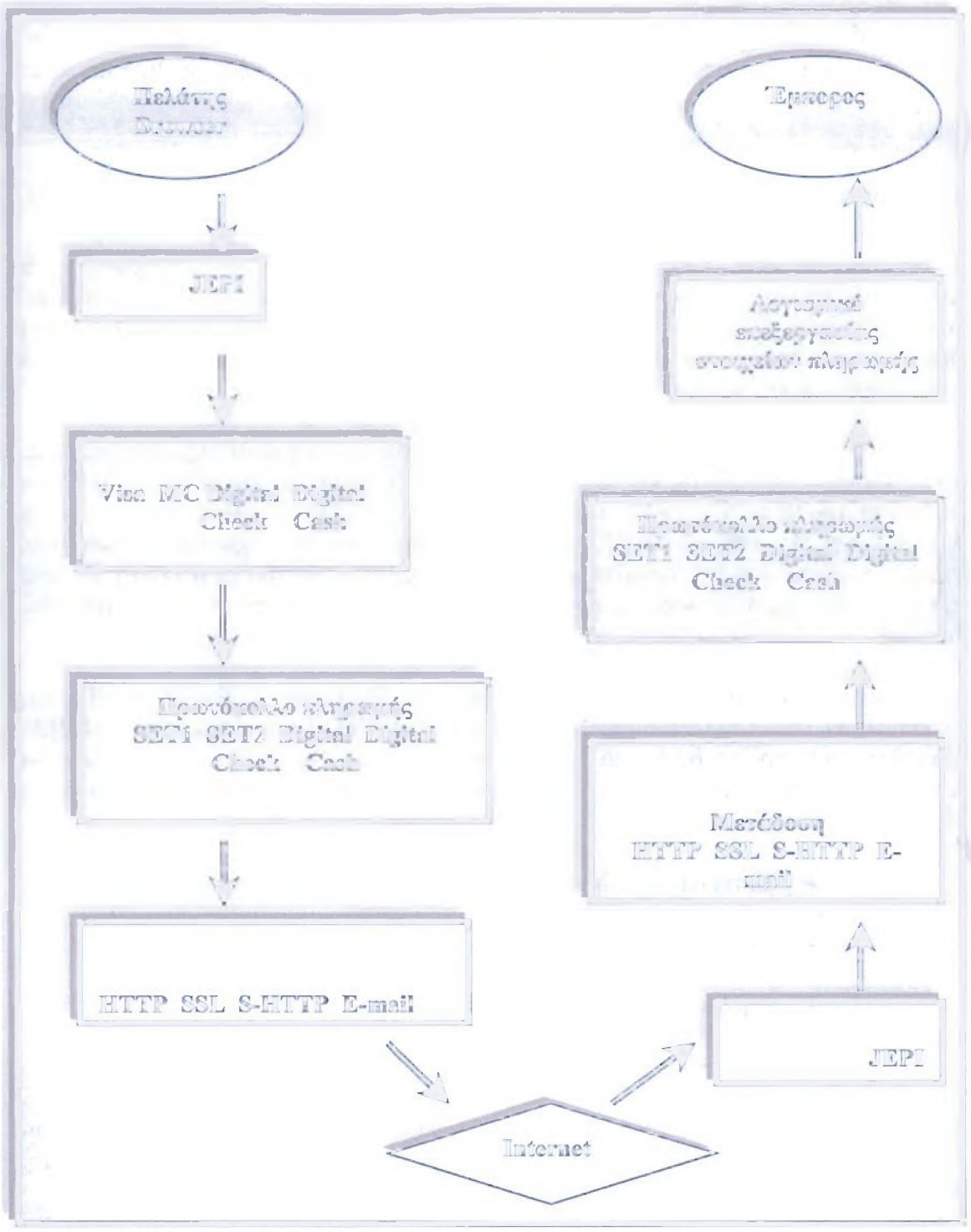
Παρά την ύπαρξη αρκετά ισχυρών συστημάτων ηλεκτρονικών πληρωμών με πιστωτικές κάρτες, θα πρέπει να αναπτυχθεί κάποιο κοινό πρότυπο που να επιτρέπει στα συστήματα πληρωμών να μπορούν να επικοινωνήσουν μεταξύ τους. Η έλλειψη διαλειτουργικότητας που παρατηρείται σήμερα ίσως να ελαττώσει την αποδοχή των συστημάτων ηλεκτρονικών πληρωμών.

Παρόλα αυτά υπάρχουν ήδη, δύο σημαντικά πρότυπα υπό ανάπτυξη, τα οποία θα καταστήσουν την διαλειτουργικότητα αυτών των συστημάτων πιο εύκολη. Το πρώτο από αυτά αφορά 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 σε μια συναλλαγή. Επίσης, κρυπτογραφεί τις πληροφορίες των πιστωτικών καρτών πριν τη μετάδοσή τους στο Internet.

Το δεύτερο πρότυπο αφορά το Joint Electronic Payments Initiative (JEPI), που αναπτύχθηκε από την CommerceNet και το World Wide Web Consortium. Το JEPI αποτελεί μια προσπάθεια για προτυποποίηση των διαφορετικών μηχανισμών πληρωμών, πρωτοκόλλων και μεταφοράς. Τέτοια παραδείγματα μηχανισμών πληρωμών περιλαμβάνουν:

- Πιστωτικές κάρτες,
- Χρεωστικές κάρτες,
- Ψηφιακό χρήμα και
- Ηλεκτρονικές επιταγές.

Τα πρωτόκολλα πληρωμών περιλαμβάνουν το STT και το SEPP. Στην ουσία ορίζουν την μορφή του μηνύματος και την διαδικασία που απαιτείται για την ολοκλήρωση της πληρωμής.
Το JEPI παρέχει τη δυνατότητα στον πελάτη να χρησιμοποιήσει μία μόνο εφαρμογή και μία μόνο διεπαφή χρήστη για την διεκπεραίωση των συναλλαγών του (σχήμα 5). Από την άλλη πλευρά, ο έμπορος μπορεί να υποστηρίξει την ποικιλία των συστημάτων πληρωμών που χρησιμοποιεί ο πελάτης.



Σχήμα 5 : Το Πρωτόκολλο JEPI

Αξιολόγηση και επιλογή μεθόδων ηλεκτρονικής πληρωμής

Ο πίνακας που ακολουθεί απαριθμεί μια σειρά από κριτήρια για την αξιολόγηση συστημάτων ηλεκτρονικής πληρωμής. Η επιλογή της καλύτερης μεθόδου ηλεκτρονικής πληρωμής για το ηλεκτρονικό εμπόριο πρέπει να γίνει μετά από μία συστηματική και ορθολογική διαδικασία λήψης απόφασης. Τα κριτήρια είναι τα εξής:

Ανταλλαξιμότητα
Χαμηλό πάγιο κόστος (για τον έμπορο)
Πιθανοί περιορισμοί
Αμφίδρομες πληρωμές
Απαίτηση για ειδικό λογισμικό
Μεταφερσιμότητα
Ταχύτητα συναλλαγών
Ανάκλητες συναλλαγές
Διακριτικότητα
Διαθεσιμότητα σήμερα
Κόστος συναλλαγών για μεγάλες και μικρές επιχειρήσεις
Απαίτηση κρυπτογράφησης για τον αγοραστή και τον πωλητή
Ανωνυμία για τον αγοραστή και τον πωλητή
Κίνδυνος παραποίησης πλαστογράφησης
Ανεξαρτησία από τον τύπο του υπολογιστή
Έλεγχος της ροής της συναλλαγής από τον αγοραστή
Δυνατότητα μαζικής χρήσης
Οικονομικός κίνδυνος για τον αγοραστή και τον πωλητή
Δυνατότητα άμεσης χρήσης των εσόδων σε ηλεκτρονική μορφή
Δυνατότητα λειτουργίας χωρίς σύνδεση
Φορητότητα
Ανάγκη για ύπαρξη τραπεζικού λογαριασμού
Βαθμός αποδοχής από τους χρήστες
Ασφάλεια από πρόσβαση χωρίς εξουσιοδότηση
Ευκολία πρόσβασης

Πίνακας 2 : Κριτήρια αξιολόγησης συστημάτων ηλεκτρονικής πληρωμής

Η εξέταση και η σύγκριση όλων των δυνατών χαρακτηριστικών κάθε συστήματος ηλεκτρονικής πληρωμής είναι χρονοβόρα και μπορεί να έχει μεγάλο κόστος. Ένας πίνακας των κυριότερων χαρακτηριστικών μπορεί να επιταχύνει σημαντικά την διαδικασία αξιολόγησης και σύγκρισης. Η απόφαση μπορεί να στηριχθεί σε μία ιεράρχηση των κριτηρίων του παραπάνω πίνακα, ώστε να εξεταστούν λεπτομερώς μόνο τα συστήματα εκείνα που ικανοποιούν τα κριτήρια που η επιχείρηση θεωρεί απαραίτητα.

Ο τρόπος αυτός ιεραρχικής επιλογής λειτουργεί όταν υπάρχουν ένα ή περισσότερα συστήματα που καλύπτουν το σύνολο των απαραίτητων κριτηρίων. Αν δεν υπάρχει τέτοιο σύστημα, η επιλογή θα πρέπει να γίνει με βάση ένα υποσύνολο των αρχικών κριτηρίων και η επιχείρηση θα πρέπει να αποφασίσει ποιος από τους υπάρχοντες συνδυασμούς κριτηρίων είναι ο καλύτερος, κάτι που δεν είναι πάντοτε εύκολο. Ένα συνηθισμένο λάθος που γίνεται στο σημείο αυτό, είναι ότι όλα τα κριτήρια θεωρούνται ισοδύναμα μεταξύ τους.

Προς το παρόν δεν υπάρχει ένα σύστημα ηλεκτρονικής πληρωμής που να δείχνει ότι επικρατεί απέναντι στα υπόλοιπα. Από τη στιγμή που το ηλεκτρονικό εμπόριο θα αποκτήσει κρίσιμη μάζα, η επιλογή θα γίνει αυτόματα από τους πελάτες-θα είναι μια αλυσιδωτή αντίδραση, όπου οι νέοι χρήστες θα έχουν την τάση να προτιμούν την μέθοδο που ήδη χρησιμοποιείται περισσότερο. Μέχρι τότε τα διάφορα συστήματα θα βρίσκονται σε ένα αγώνα δρόμου, προσπαθώντας να καθιερωθούν έγκαιρα ως το επικρατέστερο πρότυπο ηλεκτρονικής πληρωμής στην κατηγορία τους.

Ηλεκτρονικά Συστήματα Πληρωμής σε Ανοικτό Δίκτυο Υπολογιστών

Εισαγωγικά

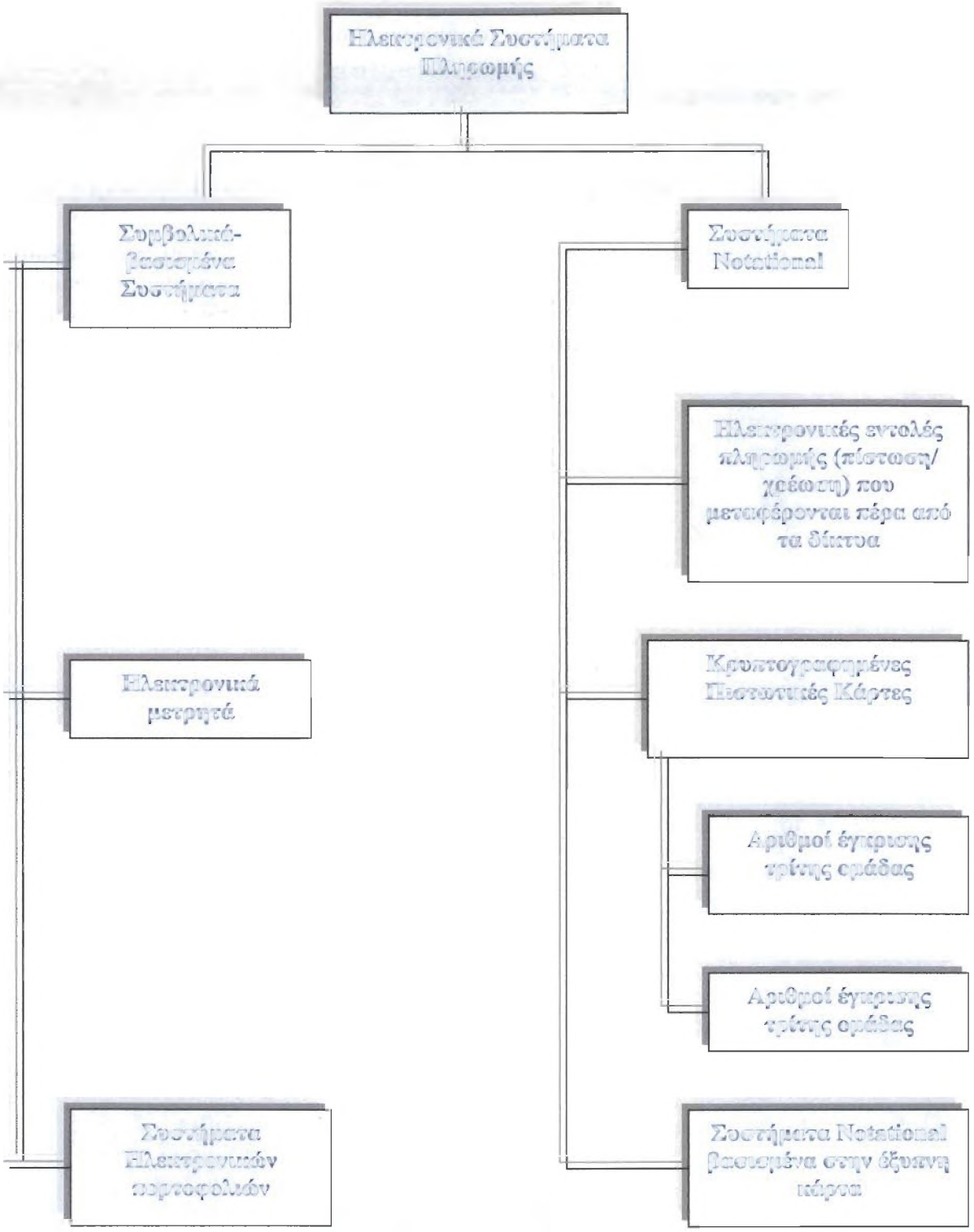
Η εξαιρετική αύξηση των διεθνών διασυνδεδεμένων δικτύων υπολογιστών και η κυρίαρχη τάση της χρησιμοποίησης αυτών των δικτύων ως νέο τομέα για την διεύθυνση των διαδικασιών της επιχείρησης υποκινεί τη ζήτηση για τις νέες μεθόδους πληρωμής. Αυτές οι νέες μέθοδοι πρέπει να επιτυγχάνουν υψηλά επίπεδα ασφάλειας, ταχύτητας, μυστικότητας, διοικητικής αποκέντρωσης και διεθνοποίησης για το ηλεκτρονικό εμπόριο που γίνετε αποδεκτό από τους καταναλωτές και τις επιχειρήσεις. Αυτό το έγγραφο ερευνά την κατάσταση προόδου στις τεχνολογίες πληρωμής και σκιαγραφεί τις αναδυόμενες εξελίξεις.

Οι νέες ηλεκτρονικές τεχνολογίες συνδυάζουν μία σφαιρικά αναπτυσσόμενη οικονομία πληροφοριών στο διαδίκτυο για να αλλάξουν τον τρόπο με τον οποίο εργαζόμαστε. Στο κέντρο αυτών των εξελίξεων είναι οι ηλεκτρονική μηχανισμοί πληρωμής που παρέχουν την οικονομική υποδομή με την οποία πρέπει να ανοίξει η ηλεκτρονική αγορά. Αυτό το έγγραφο δίνει μια επισκόπηση των νέων μηχανισμών πληρωμής με περιγραφή και αξιολόγηση μερικών εκ των οποίων υπάρχουν αυτήν την

περίοδο ή αναπτύσσονται. Αυτές οι αναθεωρήσεις και οι αξιολογήσεις είναι απαραιτήτως δοκιμαστικές, επειδή τα διάφορα συστήματα είναι σε διαφορετικά στάδια ανάπτυξης και οι διάφορες επιχειρήσεις λειτουργούν σε διαφορετικά επίπεδα δημόσιας κοινοποίησης.

Σχηματική Ταξινόμηση Ηλεκτρονικών Συστημάτων Πληρωμής

Αυτή την στιγμή, υπάρχουν πολλές διαφορετικές επιχειρήσεις που προσπαθούν να τοποθετήσουν τα προϊόντα τους σαν κυρίαρχο τρόπο να μεταφερθούν τα χρήματα σε ολόκληρο το διαδίκτυο. Σε αυτή την ενότητα ταξινομούμε τα ηλεκτρονικά συστήματα πληρωμής σύμφωνα με το ακόλουθο σχήμα (επεξηγημένο επίσης γραφικά στο σχήμα 6):



Σχήμα 6 : Το σχήμα ταξινόμησης

Συγκεκριμένα:

Συμβολικά – βασισμένα συστήματα: αυτά τα συστήματα χρησιμοποιούν τα σημεία, αντικείμενα τα οποία γενικά συμφωνούν στο να φέρουν αξία τα ίδια. Η αξία που φέρεται από τα σημεία είναι συμβατική, ένα θέμα συναίνεσης. Αυτά τα συστήματα είναι βασισμένα "στη προκαταβολή πληρωμής", δηλαδή επισύροντας τη προσοχή μέσα στον τραπεζικό λογαριασμό κάποιου για να πάρει στην κατοχή του όργανα πληρωμής, συμβολικά χρήματα, που χρησιμοποιούνται για μετέπειτα συναλλαγές. Έχουμε δύο υποκατηγορίες συμβολικά-βασισμένων συστημάτων:

Ηλεκτρονικά μετρητά: προσπαθούν να αντικαταστήσουν τα μετρητά (χαρτονομίσματα) ως κύριο μέσο πληρωμής, ανάμεσα σε απευθείας πληρωμές μέσω διαδικτύου.

Συστήματα ηλεκτρονικών πορτοφολιών: είναι βασισμένα στις έξυπνες κάρτες, αποκαλούμενες επίσης και αποθηκευμένες valuecards, το οποίο χρησιμοποιεί ένα ολοκληρωμένο κύκλωμα για να αποθηκεύσει τα ηλεκτρονικά χρήματα.

Σημειογραφικά συστήματα: σε αυτά τα συστήματα η συναλλαγή είναι άμεσα ή έμμεσα συνδεδεμένοι με το να εκτιμά και να αποθηκεύει αλλού. Οι τρεις υποκατηγορίες που μπορούμε να διακρίνουμε εδώ είναι οι εξής:

Ηλεκτρονικές εντολές πληρωμής (πίστωσης / χρέωσης) που επεξεργάζονται πέρα από το δίκτυο: η συναλλαγή είναι άμεσα συνδεδεμένη με την αξία που αποθηκεύεται αλλού (συνήθως μέσα σε ένα τραπεζικό λογαριασμό). Αυτά τα συστήματα καλούνται επίσης "pay now" (πλήρωσε τώρα) επειδή μεταφέρουν την κατάθεση χρημάτων αμέσως μετά από την έναρξη μιας εντολής πληρωμής. Παράδειγμα αυτών των συστημάτων είναι οι χρεωστικές κάρτες, οι λογαριασμοί και οι πιστωτικές μεταφορές.

Συναλλαγές Πιστωτικών Καρτών πέρα από το δίκτυο: η συναλλαγή είναι άμεσα συνδεδεμένη με την αξία σε αυτή, όταν το χρησιμοποιείς αναλαμβάνεις να γίνεις υπεύθυνος για το ποσό της συναλλαγής. Αυτά τα συστήματα καλούνται επίσης "pay later" (πλήρωσε αργότερα) και είναι βασισμένα στον καταναλωτή, στην πίστωση ή /και στην καθυστερημένη χρέωση του τρέχοντος απολογισμού του πληρωτή. Μπορούν να εφαρμοστούν με δύο τρόπους: με κρυπτογραφημένες πιστωτικές κάρτες ή με έγκριση τρίτων αριθμών.

Κρυπτογραφημένες Πιστωτικές Κάρτες: σε αυτά τα συστήματα, οι λεπτομέρειες των πιστωτικών καρτών κρυπτογραφούνται πριν αποσταλούν πέρα από τα ανοικτά δίκτυα υπολογιστών.

Αριθμοί έγκρισης τρίτου: μια λύση στην ασφάλεια και επαλήθευση των προβλημάτων κατά την διάρκεια των οικονομικών συναλλαγών είναι η εισαγωγή ενός τρίτου για να συλλέγει και να εγκρίνει τις πληρωμές από τον ένα πελάτη στον άλλο.

Έξυπνες πόρτες-βασισμένες στα σημειογραφικά συστήματα: αυτά τα συστήματα χρησιμοποιούν την τεχνολογία έξυπνων καρτών για να αποθηκεύουν ειδικές πληροφορίες πελάτη σε μια προσπάθεια να προσφέρουν υψηλότερα επίπεδα προστασίας από ότι μόνο το λογισμικό των σημειογραφικών συστημάτων.

Πρέπει να σημειώσουμε εδώ ότι μερικά συστήματα μπορούν να περιλάβουν και την αποθηκευμένη αξία και μια κατάθεση ικανότητας μεταφοράς ισορροπίας, ενσωματώνοντας κατά συνέπεια και τις δύο κατηγορίες συστημάτων πληρωμής.

Αξιολόγηση Συστημάτων

Η αξιολόγηση των ηλεκτρονικών συστημάτων πληρωμής είναι αρκετά δύσκολη, επειδή δοκιμάζουμε απότομα από τα σαφή και καθορισμένα κριτήρια για την εκτίμηση της λειτουργίας και της ποιότητας τέτοιων συστημάτων. Παρακάτω παρουσιάζουμε τις παραμέτρους που χρησιμοποιούνται για την αξιολόγηση των συστημάτων.

Το κόστος συναλλαγής: η διεύθυνση μιας συναλλαγής δεν πρέπει να είναι ακριβή. Πρέπει να σημειωθεί ότι η οικονομία μιας συναλλαγής είναι μια σχετική ιδιοκτησία. Παραδείγματος χάριν, εάν μια συναλλαγή αξίας 1000 € τα ενδιαφερόμενα μέλη κόστισαν 1€ για να διαχειριστούν, αυτό θα ήταν οικονομικό, εντούτοις, αν μια συναλλαγή των 5€ κοστίζει 10€ για να διαχειριστεί, αυτό δεν θα ήταν οικονομικό.

Ασφάλεια: οι υπηρεσίες που παρέχονται σήμερα από το διαδίκτυο στα δίκτυα που είναι σχετικά ανοικτά και η υποδομή που υποστηρίζει το ηλεκτρονικό εμπόριο πρέπει να είναι ανθεκτικά στις επιθέσεις από το περιβάλλον όπου το να κρυφακούσουν και να τροποποιήσουν μηνύματα είναι εύκολο. Αυτό σημαίνει ότι τα συστήματα πληρωμής απαιτούν την εμμονή σε μερικές θεμελιώδεις αρχές ασφάλειας εκείνων των συστημάτων που ενισχύουν πολύ την κρυπτογραφία. Αυτές οι αρχές είναι η επικύρωση, η ακεραιότητα πληρωμής, τα διπλά έξοδα πρόληψης, η απώλεια ανοχής και η μη αποποίηση ευθύνης.

Επικύρωση: απαιτείται για να μας βοηθήσει να σιγουρευτούμε ότι τα πρόσωπα που κάνουν μια συναλλαγή είναι αυτά που ισχυρίζονται.

Ακεραιότητα μηνυμάτων: απαιτείται για να εξασφαλίσει ότι οι πληροφορίες δεν έχουν αλλάξει από τότε που υπογράφηκε το στοιχείο.

Απώλεια ανοχής: αν το δίκτυο αποτύχει ή συντριβεί ο υπολογιστής κατά την διάρκεια μιας πληρωμής τα χρήματα της συναλλαγής μπορεί να χαθούν. Προκειμένου να λυθεί αυτό το πρόβλημα, ένας μηχανισμός πρέπει να είναι διαθέσιμος για να ανακτήσει την αξία αυτών των χαμένων χρημάτων. Ισχύει μόνο σε συμβολικά βασισμένα συστήματα.

Μη αποποίηση ευθύνης: απαιτείται για να αποτρέψει τον υπογράφοντα ενός εγγράφου από την άρνηση, την υποβολή, την παράδοση, ή την ακεραιότητα του περιεχομένου του. Αυτή η παράμετρος ισχύει μόνο σε σημειογραφικά συστήματα.

Μυστικότητα: απαιτείται να σιγουρευτεί ότι οι πληροφορίες δεν αποκαλύπτονται στους αναρμόδιους ανθρώπους. Το σύστημα κρυπτογραφίας μπορεί να χρησιμοποιηθεί για να ενισχύσει την μυστικότητα κατά την διάρκεια των ψηφιακών επικοινωνιών. Με αυτή την τεχνολογία, οι πληροφορίες μπορούν να υπολογιστούν έτσι ώστε το αναρμόδιο προσωπικό να μην μπορεί να τις καταλάβει. Μόνο με τον κατάλληλο κωδικό μπορούν οι πληροφορίες να αποκρυπτογραφηθούν εύκολα και να γίνουν κατανοητές.

Συμβάσεις σε απευθείας σύνδεση: ηλεκτρονικά συστήματα πληρωμής που χρειάζονται τη βοήθεια ενός απομακρυσμένου υπολογιστή σε όλη τη διάρκεια της συναλλαγής λέγονται συστήματα ανοιχτής γραμμής. Από την άλλη μεριά , σε πληρωμές μη απευθείας σύνδεσης δεν περιλαμβάνεται καμία επαφή με κάποιον τρίτο κατά τη διάρκεια της πληρωμής η συναλλαγή περιλαμβάνει μόνο τον πληρωτή και τον αποδέκτη πληρωμής.

Τα συστήματα ανοιχτής γραμμής απαιτούν προφανώς περισσότερη επικοινωνία, αλλά επίσης θεωρούνται ασφαλέστερα από τα μη απευθείας σύνδεσης συστήματα δεδομένου ότι αποτρέπουν τα προβλήματα των διπλών εξόδων και των ανέντιμων συναλλαγών. Στα μη απευθείας σύνδεσης συστήματα πληρωμής, αυτά τα προβλήματα θα μπορούσαν να λυθούν από τα ασφαλή τμήματα υλικού όπως οι έξυπνες κάρτες. να πρόβλημα είναι ότι δεν υπάρχουν αληθινά σε μη απευθείας σύνδεση μετρητά που να μπορούν να κυκλοφορούν στο εμπόριο για πάντα χωρίς κάποιος τρίτος να ενεργήσει ως μεσάζοντας. Τα χαρτονομίσματα ή τα χρυσά νομίσματα μπορούν να κυκλοφορήσουν στο εμπόριο για χρόνια χωρίς να κατατεθούν σε τράπεζα, αλλά αυτό γίνεται επειδή δεν μπορούν να πλαστογραφηθούν. Οι ψηφιακές σημειώσεις είναι εύκολο να αντιγραφούν. Οι κρυπτογραφικοί αλγόριθμοι μπορούν να πιάσουν τους παραχαράκτες, αλλά μόνο όταν τα χρήματα υποβάλλονται σε επεξεργασία μέσα σε τράπεζα.Αυτό σημαίνει ότι ακόμη και τα μη απευθείας σύνδεσης μετρητά είναι ακόμα, από μία άποψη, on-line. Αυτό σημαίνει ότι στην αλληλεπίδραση με ένα τρίτο, η συναλλαγή, μπορεί να πραγματοποιηθεί με ένα πιο ήρεμο ρυθμό. Έτσι η διάκριση μεταξύ on-line και off-line είναι ασαφής. Είναι πραγματικά μια διάκριση ανάμεσα στο τώρα και στο αργότερα.

Δυνατότητα αλλαγής εμπορεύσιμου: σε μερικά συστήματα ο έμπορος μπορεί να δώσει αλλαγή στον αγοραστή. Αυτή η παράμετρος ισχύει μόνο στα συμβολικά-βασισμένα συστήματα.

Δυνατότητα παραλήπτης: ο παραλήπτης ενός τεκμηρίου μπορεί να ξοδέψει αυτό το τεκμήριο χωρίς να χρειάζεται να έρθει σε επαφή με κάποιον εκδότη. Αυτό βελτιώνει την ανωνυμία και μειώνει το ποσό κυκλοφορίας δικτύων, αλλά περιπλέκει τα ζητήματα ασφαλείας. Έχει μόνο νόημα να ρωτηθεί αν ένα σύστημα υποστηρίζει τη δυνατότητα μεταβίβασης και αν είναι ένα συμβολικά-βασισμένο σύστημα.

Μεταφορά από πορτοφόλι σε πορτοφόλι: μερικά συστήματα υποστηρίζουν τις συναλλαγές από πορτοφόλι σε πορτοφόλι (purse-to-purse) που μιμούνται τις λειτουργίες του συμβατικού χρήματος. Αυτή η παράμετρος ισχύει μόνο στα συμβολικά-βασισμένα συστήματα.

Περιγραφή Συστημάτων

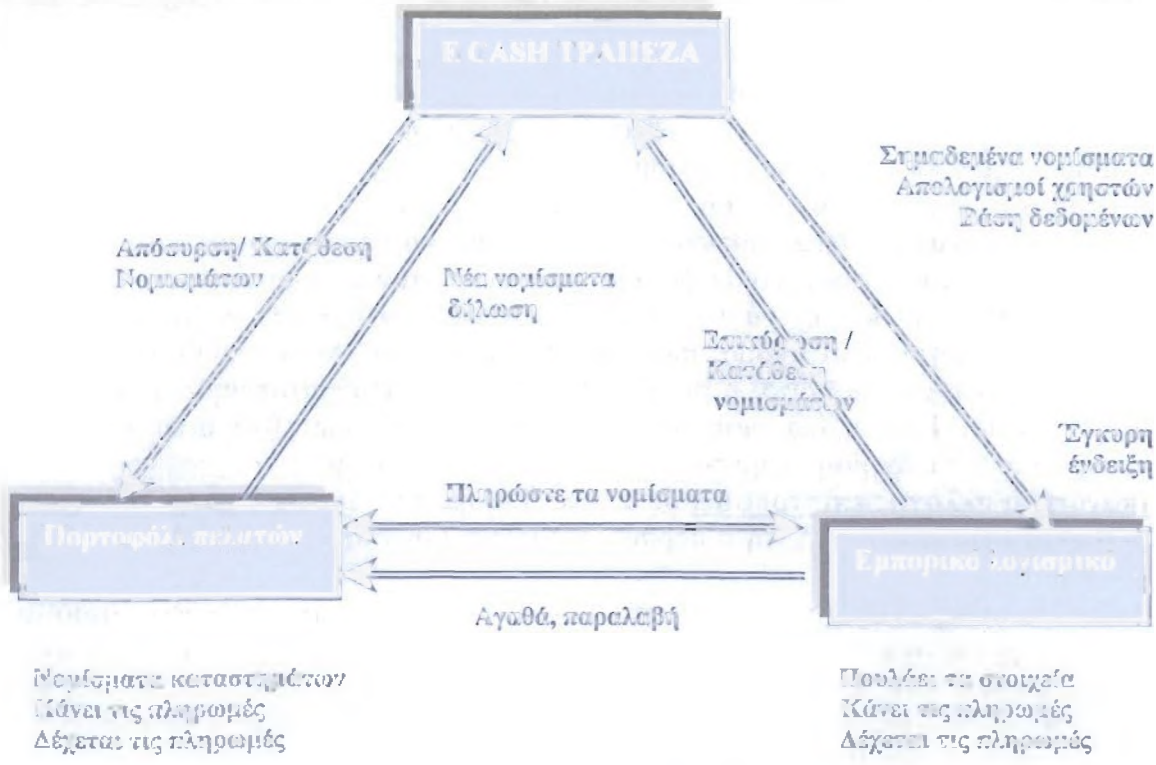
Digicash

Βασισμένο στις Κάτω Χώρες και τις ΗΠΑ, ο προμηθευτής τεχνολογίας Digicash συνεργάζεται με την αμερικανική τράπεζα Mark Twain σε έναν πιλότο του "ecash ", ένα σύστημα βασισμένο σε ένα "λογισμικό πορτοφόλι "και" ηλεκτρονικά νομίσματα" που μπορούν να φορτωθούν επάνω στο σκληρό δίσκο κάποιου υπολογιστή.

Το πρότυπο ecash

Αυτοί που δρουν μέσα στο σύστημα είναι οι πελάτες, οι έμποροι κα οι ecash τράπεζες, όπως φαίνεται στο σχήμα 7. Οι πελάτες και οι έμποροι έχουν τους απολογισμούς σε μια τράπεζα ecash. Το λογισμικό πορτοφολιών ecash καλείται cyber wallet. Αποθηκεύει και διαχειρίζεται τα χρήματα ενός πελάτη, διατηρεί τα αρχεία

όλων των συναλλαγών και κάνει το πρωτόκολλο να εμφανιστεί όσο το δυνατόν πιο προφανές στο πελάτη.



Σχήμα 7 : Οι οντότητες και οι λειτουργίες τους μέσα στο σύστημα ecash

Η ροή των αλληλεπιδράσεων στο πρότυπο DigiCash αποτελείται από τέσσερα μέρη:

Απόσυρση των νομισμάτων

- Το λογισμικό cyber wallet του πελάτη παράγει τους τυχαίους αύξοντες αριθμούς για τα νομίσματα ecash. Οι αύξοντες αριθμοί έπειτα αποκρύπτονται. Τα κρυμμένα νομίσματα στέλνονται στην τράπεζα ecash.
- Η τράπεζα ελέγχει την υπογραφή και χρεώνει τον απολογισμό σε αυτόν που υπέγραψε.
- Η τράπεζα επικυρώνει τα χρήματα και τα επιστρέφει στον πελάτη.
- Ο πελάτης διευκρινίζει τα νομίσματα.

Σημειώνεται εδώ ότι πολλά νομίσματα διαφορετικών μετονομασιών, που διευκρινίζονται από τον πελάτη, μπορούν να αποκτηθούν σε ένα ενιαίο αίτημα απόσυρσης.

Εκδίδοντας χρήματα

- Ο πελάτης στέλνει ένα αίτημα αγοράς στον έμπορο.
- Ο έμπορος στέλνει ένα αίτημα πίσω στο λογισμικό cyber wallet για να στείλει τα χρήματα.
- Ο πελάτης επιβεβαιώνει τη συναλλαγή και το λογισμικό μεταφέρει το ακριβές ποσό των χρημάτων.

Εξαργυρώνοντας χρήματα

- Ο έμπορος πρέπει να ελέγξει την ισχύ των νομισμάτων. Τα στέλνει στην τράπεζα που εξέδωσε τα νομίσματα για να εξασφαλίσει ότι δεν έχουν ξοδευτεί ήδη.
- Η τράπεζα ελέγχει τον αύξοντα αριθμό για τα διπλά έξοδα. Αν τα νομίσματα ισχύουν, τότε καταστρέφει τα νομίσματα, προσθέτει τον αριθμό στη βάση δεδομένων των νομισμάτων που έχουν ξοδευτεί και μεταφέρει το ποσό στο λογαριασμό του εμπόρου.

Δίξη της συναλλαγής

Αφότου έχουν επικυρωθεί τα νομίσματα, οι έμποροι στέλνουν τα αγορασμένα αγαθά και την απόδειξη στον πελάτη και η οικονομική συναλλαγή τελειώνει. Ένας έμπορος μπορεί επίσης να κάνει τις πληρωμές σε ένα πελάτη χρησιμοποιώντας την ίδια διαδικασία.

Νομίσματα E-cash

Τα ηλεκτρονικά νομίσματα που χρησιμοποιούνται μέσα στο σύστημα e-cash είναι μοναδικά δεδομένου ότι βγαίνουν από τον πελάτη πριν υπογραφούν από την τράπεζα. Κάθε νόμισμα έχει έναν αύξοντα αριθμό που παράγεται από το λογισμικό του cyber wallet πελάτη. Οι αύξοντες αριθμοί επιλέγονται τυχαία και είναι αρκετά μεγάλοι, έτσι υπάρχει πολύ μικρή πιθανότητα κάποιος άλλος να παράγει τους ίδιους αύξοντες αριθμούς.Ο αύξοντας αριθμός αποκρύπτεται και στέλνεται στην τράπεζα να υπογραφεί. Αυτό γίνεται χρησιμοποιώντας το απόκρυφο πρωτόκολλο υπογραφών. Η τράπεζα δεν μπορεί να δει τον αύξοντα αριθμό στο νόμισμα που υπογράφει. Η μέθοδος μπορεί να θεωρηθεί παρόμοια με την

τοποθέτηση του νομίσματος και ενός καρμπόν μέσα σε ένα φάκελο. Ο φάκελος στέλνεται στην τράπεζα όπου υπογράφεται και επιστρέφεται στον πελάτη. Ο πελάτης ανοίγει τον φάκελο και παίρνει το νόμισμα (το αποκαλύπτει).Το νόμισμα τώρα έχει υπογραφεί. Το καρμπόν εξασφάλισε ότι η υπογραφή της τράπεζας μπήκε μέσα στον φάκελο. Η υπογραφή στο νόμισμα εμφανίζεται ίδια με οποιαδήποτε άλλη κανονική ψηφιακή υπογραφή. Δεν υπάρχει κανένας τρόπος για να πει ότι το νόμισμα υπογράφηκε χρησιμοποιώντας το απόκρυφο πρωτόκολλο υπογραφών.

Εντούτοις, υπάρχει ένα πρόβλημα με αυτή τη μέθοδο. Δεδομένου ότι η τράπεζα δεν μπορεί να δει την υπογραφή, πώς μπορεί να οριστεί η αξία του νομίσματος; Η αξία δεν μπορεί να συμπεριληφθεί με τον αύξοντα αριθμό στους τομείς του νομίσματος επειδή η τράπεζα δεν μπορεί να τον δει. Ο πελάτης μπορεί να ορίσει μια πολύ υψηλή αξία και να πει στην τράπεζα ότι είναι μόνο ένα νόμισμα μικρής αξίας.

Το πρόβλημα μπορεί να λυθεί από την τράπεζα χρησιμοποιώντας ένα διαφορετικό κλειδί υπογραφών για κάθε νόμισμα που μετονομάζεται. Ο πελάτης ενημερώνει την τράπεζα για την αξία που θέλει να αξίζει το απόκρυφο νόμισμα. Κατόπιν η τράπεζα υπογράφει το νόμισμα με το κλειδί υπογραφών που αντιπροσωπεύει αυτή την μετονομασία και αφαιρεί εκείνο το ποσό από το λογαριασμό του πελάτη.

Χαρακτηριστικά γνωρίσματα DigiCash

Χαμηλό κόστος συναλλαγής

Πρόληψη διπλών εξόδων: το DigiCash υποστηρίζει την πρόληψη διπλών εξόδων. Για να εξασφαλίσει ότι ένας αύξοντας αριθμός δεν ξοδεύεται δύο φορές, η νομισματική τράπεζα πρέπει να καταγράφει κάθε νόμισμα που κατατίθεται πίσω σε εκείνη. Μια πολύ μεγάλη βάση δεδομένων όλων των αυξόντων αριθμών που έχουν δοθεί αναπτύσσεται σύντομα. Όταν ένα έγκυρο νόμισμα γίνεται αποδεκτό, αυτό κατόπιν θεωρείται πως έχει δοθεί και ο αύξοντας αριθμός του εισάγεται στη βάση δεδομένων. Με τη χρησιμοποίηση των ημερομηνιών λήξης για τα νομίσματα, οι αύξοντες αριθμοί μπορούν να αφαιρεθούν από την ημερομηνία λήξης. Κατά αυτόν τον τρόπο μειώνουμε τους αύξοντες αριθμούς που πρέπει να κρατηθούν στη βάση δεδομένων. Το λογισμικό πορτοφολιών μπορεί αυτόματα να εξασφαλίσει ότι τα νομίσματα επιστρέφονται στην τράπεζα προτού να λήξουν.

Απώλεια ανωνυμίας: αν το δίκτυο αποτύχει ή συντριβούν οι υπολογιστές κατά τη διάρκεια μιας συναλλαγής ή πληρωμής, τα νομίσματα χάνονται. Υπάρχει, ωστόσο ένας μηχανισμός για να ανακτήσει την αξία αυτών των χαμένων νομισμάτων.

Εμπιστευτικότητα πληρωμής και επεξαιτέρω μηνυμάτων: όλη η επικοινωνία στο σύστημα DigiCash υπογράφεται ψηφιακά και κρυπτογραφείται κατευθείαν κάνοντας εκτενή χρήση του συμμετρικού και του μη συμμετρικού συστήματος κρυπτογραφίας.

Ανωνυμία πληρωτών: το τρέχον σύστημα DigiCash περιλαμβάνει τις κρυπτογραφημένες ψηφιακές υπογραφές για την προστασία της ανωνυμίας από τους αγοραστές. Όπως το σύστημα CAFÉ, τα νομίσματα μπορούν να υπογραφούν για να ανιχνεύσουν τον αγοραστή που

τα ξοδεύει δύο φορές. Αυτή η μερική ανωνυμία αναφέρεται ως αποτρεπτικός παράγοντας στην εγκληματική χρήση του συστήματος.

Μη σύνολη παρακολούθηση πληρωτών: στο σύστημα DigiCash ο αποστολέας είναι σε θέση να αποδειχθεί ότι έστειλε τα χρήματα, εντούτοις ο παραλήπτης (ή κάποιος που ρωτά αργότερα το σύστημα) δεν μπορεί να δει ποιος έστειλε τα χρήματα.

Διαιρετότητα: ο πελάτης ενημερώνει την τράπεζα για το πόσο θέλει να αξίζει το απόκρυφο νόμισμα. Η τράπεζα έπειτα υπογράφει το νόμισμα με το κλειδί υπογραφών που αντιπροσωπεύει αυτή την μετονομασία. Για παράδειγμα, η τράπεζα μπορεί να έχει μία υπογραφή του 1 cent, μία υπογραφή των 5 cents, μία υπογραφή των 10 cents κτλ.

Ικανότητα αλλαγής-επιστροφής: το σύστημα δεν έχει καμία ικανότητα αλλαγής-επιστροφής. Κατά συνέπεια, ο πελάτης πρέπει πάντα να παρέχει τον ακριβή αριθμό νομισμάτων που απαιτούνται για την αγορά. Αυτό γίνεται επειδή η αποδεκτή αλλαγή θα μπορούσε να εκθέσει σε κίνδυνο την ανωνυμία του χρήστη (ο έμπορος θα μπορούσε να καταγράψει την παρουσίαση σε συνεχείς αριθμούς για να αλλάζουν και να συνεργούν με την τράπεζα ώστε να αποκαλύψουν την ταυτότητα του χρήστη). Το cyber wallet θα συγκεντρώσει αυτόματα το σωστό ποσό και μπορεί να αποσύρει τα νέα νομίσματα από την τράπεζα αν απαιτούνται περισσότερες μετονομασίες.

Μεταφορά από πορτοφόλι σε πορτοφόλι (purse-to-purse): η μεταφορά από πορτοφόλι σε πορτοφόλι (purse-to-purse) του ecash είναι δυνατή, αν το ποσό που μεταφέρεται πρέπει να είναι διαβιβασμένο στην τράπεζα για επαλήθευση. Τα νομίσματα διαβιβάζονται μέσο του δικαιούχου πληρωμής στην τράπεζα όπου κατατίθενται. Η αξία των νέων νομισμάτων πρέπει να είναι του ίδιου ποσού και να επιστρέφονται έπειτα στο δικαιούχο της πληρωμής. Όλα αυτά γίνονται φανερά από το λογισμικό έτσι ώστε να φαίνεται ότι τα νέα νομίσματα τα είχε λάβει άμεσα ο πληρωτής. Αυτή την εποχή, όπως και με τις εμπορικές πληρωμές, και οι δύο χρήστες πρέπει να έχουν λογαριασμούς στην ίδια τράπεζα ecash προκειμένου να εκτελεστεί μία μεταφορά από πορτοφόλι σε πορτοφόλι (purse-to-purse).

Millicent

Το Millicent στοχεύει στη μερίδα micropayment του εμπορίου του διαδικτύου, όπου οι συναλλαγές θα μπορούσαν να περιλάβουν τα μέρη 1 cent και να γίνονται πολύ πιο γρήγορα. Λαμβάνοντας υπόψη αυτούς τους περιορισμούς, οι τεχνικές micropayment πρέπει να είναι και ανέξοδες και γρήγορες. επιτυγχάνοντας και τα δύο απαιτούνται ορισμένοι συμβιβασμοί, όπως η σχετικά ελαφριά ασφάλεια.

Scrips

Το σύστημα Millicent χρησιμοποιεί scrips, μία μορφή σημείων που ισχύουν μόνο για έναν ιδιαίτερο προμηθευτή, για μια περιορισμένη χρονική περίοδο, και για τους μεσίτες, οι οποίοι ενεργούν ως μεσάζοντες ανάμεσα στους προμηθευτές και στους πελάτες. Προκειμένου να αποφευχθεί οι πελάτες να πρέπει να διατηρήσουν χωριστούς λογαριασμούς με τους προμηθευτές, με τους οποίους μπορούν μόνο να

έχουν μια πολύ σύντομη σχέση, οι μεσίτες ενεργούν όπως οι μεσάζοντες. Οι μακροπρόθεσμες σχέσεις είναι μεταξύ των μεσιτών και των πελατών. Ένα scrip μπορεί να θεωρηθεί ως "απολογισμός" μεταξύ του πελάτη και του εμπόρου ο οποίος ιδρύεται, χρησιμοποιημένος και κλειστός. Το scrip περιέχει μια αξία και όταν κάνει ένας πελάτης μια αγορά με αυτό, το ποσό της πληρωμής αφαιρείται από την αξία των scrip και το scrip στέλνεται πίσω στον πελάτη ως ανταλλαγή.

Ένα scrip δεν μπορεί να χρησιμοποιηθεί περισσότερο από μία φορά, μπορεί μόνο να ξοδευτεί από τον αρχικό ιδιοκτήτη του σε έναν συγκεκριμένο έμπορο, έχει μια ημερομηνία λήξης (ημερομηνία στην οποία το scrip ακυρώνεται, χρησιμοποιείται για να περιορίσει το scrip'IDs που πρέπει να αναφερθεί από ένα προμηθευτή για να αποτρέψει το διπλάσιο) και μπορεί να αναπαραχθεί μέχρι την λήξη.

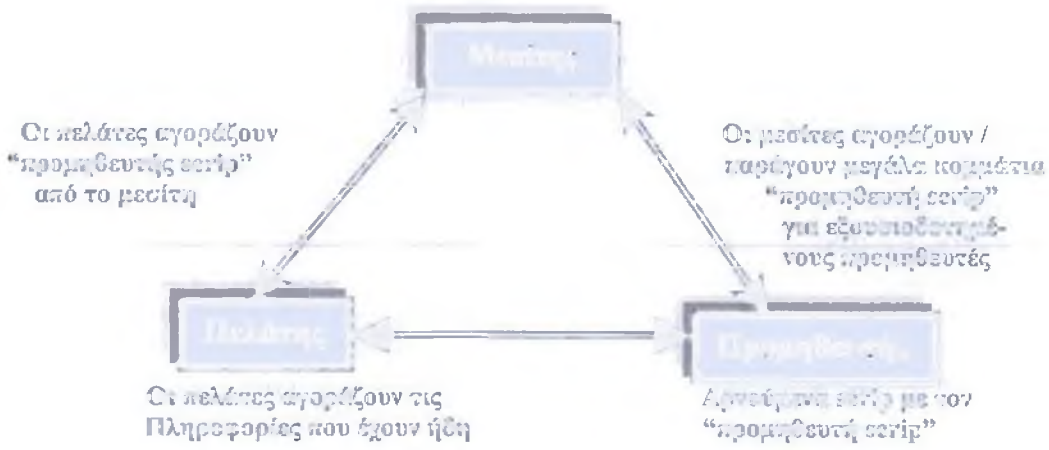
Το Millicent

Η βασική ακολουθία αλληλεπιδράσεων στο πρότυπο Millicent είναι η ακόλουθη (σχήμα 8):

- Ο πελάτης αγοράζει μια ποσότητα μεσίτη scrips χρησιμοποιώντας ένα από τα σχέδια macropayment.
- Όταν ένας πελάτης αντιμετωπίζει αρχικά έναν νέο προμηθευτή, πρέπει να αγοράσει τον προμηθευτή scrip από τον μεσίτη για να ξοδέψει επί του τόπου του προμηθευτή. Επομένως τοποθετεί ένα αίτημα από τον προμηθευτή scrip για το μεσίτη.
- Ο μεσίτης λαμβάνει τον απαραίτητο προμηθευτή scrip από τον προμηθευτή.
- Ο μεσίτης πουλάει τον προμηθευτή scrip στον πελάτη. Π.χ., ο πελάτης μπορεί να αγοράσει 20 cents του προμηθευτή scrip χρησιμοποιώντας τα $5 του μεσίτη scrip που αγοράστηκε νωρίτερα (βήμα 1), και ο νέος προμηθευτής scrip και η αλλαγή στον μεσίτη scrip επιστρέφονται στον πελάτη.
- Ο προμηθευτής scrip στέλνεται στον έμπορο με αίτημα αγορών.
- Ο προμηθευτής δίνει την αλλαγή στον προμηθευτή scrip μαζί με το αγορασμένο περιεχόμενο.

Τα βήματα 1 και 3 δεν χρειάζεται να συμβούν σε κάθε συναλλαγή που ο πελάτης θα αγόραζε ικανοποιητικό scrip από το μεσίτη του για να ικανοποιήσει τις ανάγκες του για μια χρονική περίοδο, ομοίως ο μεσίτης θα είχε αρκετό προμηθευτή scrip για να συντηρήσει διάφορα αιτήματα των πελατών, ή θα είχε την άδεια από τον προμηθευτή να κόψει νομίσματα ο συγκεκριμένος scrip άμεσα.

Αν και θα φαινόταν ότι υπάρχει μεγάλη κυκλοφορία σε αυτό το πρωτόκολλο, δεν υπάρχει κανένα εμπόδιο στη σύνδεση έκδοσης ενός ενιαίου νομίσματος για κάθε συναλλαγή ειδικά στα βήματα 1 και 3 αναλύονται σε παράγοντες.



Σχήμα 8 : Σχέσεις μεσίτη – πελάτη & προμηθευτή

Χαρακτηριστικά γνωρίσματα Millicent

Ασφάλεια και μυστικότητα: τα πρωτόκολλα Millicent προσφέρουν διάφορα επίπεδα ασφάλειας και μυστικότητας. Δηλαδή, scrip μέσα στις σαφείς προσφορές δεν προσφέρει καμία ασφάλεια και μυστικότητα. Εδώ το scrip μεταφέρεται μεταξύ του πελάτη και του προμηθευτή χωρίς οποιαδήποτε κρυπτογράφηση ή προστασία. Αυτό θα επέτρεπε σε κάποιον που κάνει υποκλοπή στη σύνδεση για να πάρει ένα αντίγραφό του scrip να το επιστρέψει ως αλλαγή και να το ξοδέψει μόνος του. Το ιδιωτικό και ασφαλές πρωτόκολλο χρησιμοποιεί ένα κοινό μυστικό κλειδί μεταξύ των δύο συμβαλλόμενων μερών για να καθιερώσει ένα ασφαλές κανάλι επικοινωνίας (κρυπτογραφήστε και το scrip και ζητά την αγορά). Και η ασφαλής χωρίς πρωτόκολλο κρυπτογράφηση κάνει το ίδιο πράγμα χωρίς την πτυχή της μυστικότητας προκειμένου να επιτευχθεί η καλύτερη απόδοση.

- Πρόληψη διπλών εξόδων σε όλα τα πρωτόκολλα Millicent τα διπλά έξοδα θα ανιχνευθούν τοπικά από τον προμηθευτή στο χώρο της αγοράς.

- Ανωνυμία πληρωτών: αν και το πρωτόκολλο Millicent περιλαμβάνει ένα τομέα στο scrip για να φέρει στον πελάτη πληροφορίες, αυτός ο τομέας δεν χρησιμοποιείται πάντα. Η ομάδα Millicent προτείνει ότι μια καλή χρήση αυτού του τομέα θα ήταν να μεταφερθεί η ηλικία και οι πληροφορίες κατοικιών για φορολογικούς λόγους και

οποιεσδήποτε πληροφορίες που απαιτούνται για τις εκπτώσεις, όπως η θέση σπουδαστών. Ωστόσο μερικοί που περιορίζουν την ανωνυμία θα μπορούσαν να διατηρηθούν αγοράζοντας από τον μεσίτη scrip χρησιμοποιώντας ένα ανώνυμο σύστημα macropayment.

- Μη εύκολη παρακολούθηση πληρωτών: ένα scrip έχει τους ορατούς αύξοντες αριθμούς που θα μπορούσαν να καταγραφούν και να επισημανθούν.

Σε απευθείας σύνδεση συναλλαγών: το σύστημα Millicent είναι σε μη απευθείας σύνδεση μέχρι το σημείο που δεν απαιτείται καμία σύνδεση με έναν κεντρικό υπολογιστή. Το γεγονός ότι οποιοσδήποτε ιδιαίτερος τύπος scrip ισχύει μόνο σε έναν ιδιαίτερο προμηθευτή σημαίνει ότι ο προμηθευτής δε πρέπει να συνδεθεί με έναν χωριστό εκδότη για να επικυρώσει το σημείο, με αυτόν τον τρόπο μειώνει την κυκλοφορία των δικτύων και εξαλείφει το συνοδευτικό κόστος μιας τέτοιας επικύρωσης.
Διαμεσολάβηση: το scrip μπορεί να αντιπροσωπεύσει οποιαδήποτε μετονομασία του νομίσματος. Αναμενόμενη σειρά τιμών από το 1/10 του cent μέχρι περίπου $5, αν και δεν υπάρχει κανένα καθορισμένο ανώτερο ή χαμηλότερο συνδεδεμένο όριο.

CAFE

Το CAFE είναι ένα σχέδιο μετρητών με την εγγύηση της ανωνυμίας για τους χρήστες. Περιλαμβάνει ένα ηλεκτρονικό πορτοφόλι που χρησιμοποιείται ως πανευρωπαϊκός μηχανισμός για τις καταναλωτικές πληρωμές, πρόσβαση στις υπηρεσίες και αν είναι απαραίτητο προσδιορισμός πληροφοριών. Υπάρχουν δύο είδη ανθεκτικών ασφαλών ηλεκτρονικών συσκευών πλαστογραφήσεων που χρησιμοποιούνται στο σύστημα CAFE: έξυπνες κάρτες και πορτοφόλια. Αυτές οι συσκευές χρησιμοποιούνται για να αποθηκεύσουν τα ηλεκτρονικά χρήματα, να εκτελέσουν κρυπτογραφικές διαδικασίες και να κάνουν τις πληρωμές στους εμπόρους.
Έξυπνες κάρτες: αυτό είναι το απλούστερο πρωτόκολλο των συσκευών που χρησιμοποιούνται. Είναι παρόμοιο με μια πιστωτική κάρτα και τροφοδοτεί έναν ενσωματωμένο μικροεπεξεργαστή από μια εξωτερική πηγή. Όλες οι πληροφορίες είναι αποθηκευμένες στο chip, το οποίο εκτελεί επίσης τους κρυπτογραφικούς υπολογισμούς.
Χαρτοφυλάκιο: ένα χαρτοφυλάκιο αποτελείται από δύο μέρη που λειτουργούν από κοινού το ένα με το άλλο. Το ένα μέρος είναι γνωστό ως παρατηρητής και προστατεύει τα τραπεζικά επιτόκια και το άλλο είναι γνωστό ως πορτοφόλι και προστατεύει τα συμφέροντα του χρήστη.
Το CAFE υποστηρίζει επίσης τις ανέπαφες συναλλαγές μέσω των υπέρυθρων πορτοφολιών.

Το πρότυπο CAFE

Απόσυρση: συνήθως μόνο ένας πληρωτής πρέπει να επικοινωνήσει με την τράπεζα μέσω μιας συνόδου απόσυρσης, η οποία οδηγεί σε διάφορες κενές ηλεκτρονικές ολισθήσεις πληρωμής που φορτώνονται στη δική του έξυπνη κάρτα. Η τράπεζα παρακολουθεί την ισορροπία της κάρτας με τη βοήθεια ενός μετρητή που είναι μέρος των παρατηρητών της έξυπνης κάρτας. Η ισορροπία ενημερώνεται κατά τη διάρκεια ενός αιτήματος απόσυρσης και το αντίστοιχο ποσό αφαιρείται από τον τραπεζικό λογαριασμό του χρήστη. Μία σύνοδος απόσυρσης αποτελείται από τα ακόλουθα βήματα:

- Η έξυπνη κάρτα του χρήστη στέλνει την ταυτότητα της τράπεζας, τις πληροφορίες και το δημόσιο βασικό πιστοποιητικό για την τράπεζα στο τερματικό. Αυτό επιτρέπει στο τερματικό να τον συνδέσει με τη σωστή τράπεζα και ελέγχει/ ενημερώνει το δημόσιο βασικό πιστοποιητικό της τράπεζας πουαποθηκεύεται στην έξυπνη κάρτα.

- Η κάρτα και η τράπεζα έπειτα αμοιβαία επικυρώνουν η μία την άλλη μέσω του τερματικού.

- Ο χρήστης παράγει μία ολίσθηση πληρωμής και διαβιβάζει hash από αυτήν στην τράπεζα. Η τράπεζα δημιουργεί μια ψηφιακή υπογραφή διαβιβασμένου hash και στέλνει το αποτέλεσμα στην κάρτα του χρήστη. Ο χρήστης πρέπει να αποθηκεύσει μόνο την υπογραφή της τράπεζας στην κάρτα όπως όλες τις άλλες τιμές που πρέπει να αποτελέσουν την ολίσθηση πληρωμής (όπως τα one-time δημόσια κλειδιά) μπορούν να αναπαραχθούν από την κάρτα χρήστη στο βήμα 2 του σταδίου πληρωμής.

Πληρωμή: η συναλλαγή πληρωμής αποτελείται από τον χρήστη που συμπληρώνει ένα ποσό σε μία κενή ολίσθηση πληρωμής μαζί με το όνομα του δικαιούχου πληρωμής, που υπογράφεται με το μυστικό κλειδί του χρήστη. Τα βήματα που συμπεριλαμβάνονται στην πληρωμή μιας συναλλαγής είναι τα ακόλουθα:

- Ένας πελάτης εισάγει την κάρτα του στο τερματικό πληρωμής ενός εμπόρου. Το τερματικό εμφανίζει την κάρτα, την ταυτότητα του δικαιούχου πληρωμής, την ημερομηνία και του ποσού που αφαιρούνται από το μετρητή μέσα στο μέρος των παρατηρητών της έξυπνης κάρτας.

- Η κάρτα αναπαράγει την επόμενη ολίσθηση πληρωμής που χρησιμοποιείται. Αυτό αποτελείται από την παραγωγή κρυπτογραφικών κλειδιών

- Η κάρτα στέλνει την κενή ολίσθηση πληρωμής στον έμπορο, που αποτελείται από την υπογραφή της τράπεζας και τα δημόσια κλειδιά πρέπει να χρησιμοποιηθούν για την ολίσθηση.

- Το τερματικό ελέγχει την υπογραφή της τράπεζας στην ολίσθηση πληρωμής.
- Οι πληροφορίες που δίνονται από το τερματικό σε πρώτη φάση κωδικοποιούνται από την κάρτα ολίσθησης πληρωμής (Μ).
- Όταν η πληρωμή οριστικοποιηθεί, το τερματικό στέλνει μια αναγνώριση.

Κατάθεση: στην αποδοχή μιας ολίσθησης πληρωμής, ο δικαιούχος πληρωμής το διαβιβάζει στον αγοραστή (σε μια μεταγενέστερη ημερομηνία) ο οποίος το καθαρίζει στη συνέχεια μέσω του υπάρχοντος οικονομικού συστήματος καθαρίσματος. Ο αγοραστής:

- Ελέγχει το περιεχόμενο της ολίσθησης πληρωμής και επικυρώνει την υπογραφή της τράπεζας.
- Ελέγχει ότι η ολίσθηση πληρωμής δεν έχει κατατεθεί προηγουμένως.
- Κοιτάζει στη βάση δεδομένου του για να ελέγξει ότι το αντίστοιχο μέρος της ολίσθησης πληρωμής δεν έχει ξοδευτεί προηγουμένως.

Εάν οι δύο πρώτοι όροι τηρούνται, ο δικαιούχος πληρωμής έχει το δικαίωμα να πιστωθεί για το ποσό της πληρωμής. Ένας δικαιούχος πληρωμής είναι αρμόδιος για τον έλεγχο όλων των λαμβανόμενων ολισθήσεων πληρωμής σε σχέση με τα τοπικά αντίγραφά του της μαύρης λίστας (βάση δεδομένων που περιέχει το IDs ολισθήσεων πληρωμής που έχουν ξοδευτεί) κατά τη διάρκεια της φάσης πληρωμής. Αν μια ολίσθηση βαλμένη στη μαύρη λίστα ανιχνεύεται, ο δικαιούχος πληρωμής αποβάλει τη συναλλαγή. Αν ένας δικαιούχος πληρωμής αποτύχει να ελέγξει τις λαμβανόμενες ολισθήσεις πληρωμής σε σχέση με τη μαύρη λίστα, κατόπιν θα πρέπει να δεχτεί την ευθύνη για αυτούς ως κέντρο καθαρίσματος που θα τους απορρίψει. Όταν το κέντρο καθαρίσματος ανιχνεύει τα διπλά έξοδα, η ολίσθηση πληρωμής θα προστεθεί αμέσως στη μαύρη λίστα.

Χαρακτηριστικά γνωρίσματα CAFE

Επικύρωση: τα πορτοφόλια του CAFE μπορούν να διαμορφωθούν για να χρησιμοποιηθούν με ένα PIN. Σε αυτή την περίπτωση ο αγοραστής υποτίθεται πάντα ότι είναι ο νόμιμος χρήστης της συσκευής. Κατά τη διάρκεια της φάσης απόσυρσης, η κάρτα και η τράπεζα επικυρώνουν αμοιβαία η μία την άλλη μέσω του τερματικού. Οι παρόμοιες διαδικασίες επικύρωσης πραγματοποιούνται μεταξύ του πληρωτή και του δικαιούχου πληρωμής καθώς επίσης και μεταξύ του δικαιούχου πληρωμής και της τράπεζας κατά τη διάρκεια της πληρωμής και των φάσεων κατάθεσης αντίστοιχα.

Ακεραιότητα μηνυμάτων: το μέρος των παρατηρητών της έξυπνης κάρτας εξασφαλίζει την ακρίβεια όλων των συναλλαγών που έχουν εκτελεστεί κοντά στο χρήστη. Ένας χρήστης δε θα είναι σε θέση να ολοκληρώσει επιτυχώς μια συναλλαγή πληρωμής χωρίς τη συνεργασία του παρατηρητή.

Πρόληψη διπλών εξόδων: η προστασία ενάντια στα διπλά έξοδα είναι εγγυημένη εφόσον η αντίσταση πλαστογραφήσεων δεν είναι συμβιβασμένη. Όσο αυτό ισχύει το CAFE προσφέρει δύο επίπεδα ανίχνευσης διπλών εξόδων. Αρχικά, ένας δικαιούχος πληρωμής είναι αρμόδιος για τον έλεγχο όλων των λαμβανόμενων ολισθήσεων πληρωμής για τα διπλά έξοδα. Εάν αποτύχει να το κάνει , τότε το CAFE έχει έναν κρυπτογραφικό μηχανισμό επιφύλαξης που επιτρέπει τα οικονομικά ιδρύματα να ανιχνεύσουν τα διπλά έξοδα του ηλεκτρονικού νομίσματος (αφότου έχουν ξοδευτεί) και να βάλουν στη μαύρη λίστα τις αντίστοιχες ολισθήσεις πληρωμών. Οι τράπεζες διανέμουν αυτούς τους καταλόγους σε όλους τους εμπόρους του συστήματος. Αυτή η ανίχνευση επιτυγχάνεται με κόστος μια βάση δεδομένων που έχει πρόσφατα ξοδέψει ολισθήσεις πληρωμής από τους χρηματοδοτικούς οργανισμούς.

Ασφάλεια ενεργός: εάν ο χρήστης χάσει το πορτοφόλι του, η τράπεζα μπορεί να ανακτήσει τα χρήματα από μία εφεδρεία και την κατάθεση αντιγράφων. Αυτό γίνεται από τα κανονικά εφεδρεία κατά τη διάρκεια μιας συναλλαγής απόσυρσης. Εάν ένας χρήστης θέλει να ανακτήσει τα χαμένα χρήματα, αποκαλύπτει την ταυτότητα των ολισθήσεων πληρωμής που αποθηκεύονται μετά από την τελευταία απόσυρση. Αυτό επιτρέπει στην τράπεζα να ακολουθήσει αυτές τις ολισθήσεις πληρωμής.

Ενημερευνησιμότητα πληρωμής: το πορτοφόλι θα αποκρύψει/εξουδετερώσει οποιεσδήποτε επικοινωνίες που μπορούν να αποκαλύψουν τις μυστικές πληροφορίες για τον χρήστη στον εξωτερικό κόσμο. Επιπλέον, όλες οι επικοινωνίες μεταξύ του πορτοφολιού και του εξωτερικού κόσμου γίνονται αποκλειστικά μέσω του πορτοφολιού, και εγγυώνται ότι ο παρατηρητής δεν μπορεί να αποκαλύψει οποιεσδήποτε μυστικές πληροφορίες στην τράπεζα χωρίς τη γνώση του χρήστη.

Ανωνυμία πληρωτών: το πορτοφόλι επικυρώνει κάθε πληρωμή δίνοντας μια κρυπτογραφική υπογραφή. Σαν επιφυλακτικό μηχανισμό, τα χρήματα τα οποία χρησιμοποιεί το πορτοφόλι είναι ένα κρυπτογραφημένο σχήμα όπου η ταυτότητα του πληρωτή κωδικοποιείται με τον αριθμό του νομίσματος. Αυτό γίνεται με τέτοιο τρόπο ώστε η ταυτότητα του πληρωτή να μπορεί να ανακτηθεί μόνο αν το νόμισμα έχει ξοδευτεί δύο φορές.

Μη εύκολη παρακολούθηση πληρωτών: υπό κανονικές συνθήκες, οι πληρωμές δεν μπορούν να συνδεθούν με έναν χρήστη ακόμα και αν υπάρχει συνεργασία μεταξύ των εμπόρων και των τραπεζών.

Σε απευθείας σύνδεση επαλήθευση: το σύστημα είναι σε θέση να εκτελεί τις συναλλαγές σε μη απευθείας σύνδεση, εξαλείφοντας κατά συνέπεια την ανάγκη να συνδέσει τους κεντρικούς υπολογιστές. Πρέπει να σημειωθεί ότι οι συναλλαγές είναι μόνο σε μη απευθείας σύνδεση κατά τη διάρκεια της αγοράς, αποσύρσεις από τα ηλεκτρονικά χρήματα στο πορτοφόλι είναι, αναπόφευκτα, συναλλαγές σε απευθείας σύνδεση. Επίσης μπορεί να αποφασιστεί ότι οι πληρωμές πέρα από ένα ορισμένο κατώτατο όριο πρέπει να επιβεβαιωθούν on-line.

Ικανότητα αλλαγής-επισυναφής: το τερματικό του εμπόρου λέει στην κάρτα το ποσό που πρέπει να καταβάλλει και έπειτα αυτές οι πληροφορίες κωδικοποιούνται

από την κάρτα σε μια ολίσθηση πληρωμής. Έτσι ο πληρωτής πληρώνει το ακριβές ποσό που απαιτείται για την αγορά, το οποίο σημαίνει ότι η ικανότητα αλλαγής της επιστροφής δεν περιέχεται σε αυτό το σύστημα.

Πολλαπλάσια νομίσματα: τα πορτοφόλια του CAFE έχουν διάφορες τσέπες για τα διαφορετικά νομίσματα. Όπως τα μετρητά οι χρήστες μπορούν είτε να τα ανταλλάξουν είτε να τα κυκλοφορήσουν στην τράπεζα (που χαμηλώνει το κόστος σε μια τσέπη και που αυξάνεται σε μια άλλη) ή να [πληρώσουν σε μη τοπικό νόμισμα αν ο έμπορος το δέχεται.

Δυνατότητα μεταβίβασης: η συσκευή λαμβάνει τα νομίσματά της με την απόσυρσή τους από ένα τραπεζικό λογαριασμό μέσω αυτοματοποιημένης μηχανής ταμείων τράπεζας (ATM). Έτσι "προπληρώνεται" και τα νομίσματα στη μηχανή δεν υπάρχουν όπως τα νομίσματα οπουδήποτε αλλού. Όταν ο χρήστης ξοδεύει τα χρήματα η συσκευή διαβιβάζει ένα ή περισσότερα νομίσματα στη συσκευή του πωλητή και τα στοιχεία τους όπως ξοδεύονται μέσα στη συσκευή. Ο πωλητής έχει τώρα την αξία αυτών των νομισμάτων. Ωστόσο, πρέπει να κατατεθούν σε έναν εκδότη για την αξία που πραγματοποιείται. Κατά συνέπεια, η αρχική ροή του συστήματος CAFE είναι αυτή της αποσυρόμενης- αμοιβής- κατάθεσης και τα μεμονωμένα νομίσματα δεν παραμένουν στην κυκλοφορία με τον ίδιο τρόπο όπως κάνουν τα πραγματικά σημεία μετρητών. Κατά συνέπεια, η δυνατότητα μεταβίβασής δεν ισχύει για αυτό το σύστημα.

Mondex

Η έννοια της κάρτας Mondex αναπτύχθηκε στο NatWest, σε σημαντικές Βρετανικές τραπεζικές εργασίες οργάνωσης, το 1990. Η τεχνολογία αναπτύχθηκε με διάφορους κατασκευαστές που περιέχονταν στην παραγωγή του ασφαλούς υλικού, συμπεριλαμβανομένης της εταιρίας Hitachi. Τον Ιούλιο του 1996 μια ξεχωριστή επιχείρηση, Mondex διεθνώς διαμορφώθηκε για να προωθήσει την τεχνολογία μέσω μιας σειράς δοκιμών σε πολλές διαφορετικές τοποθεσίες σε ολόκληρο τον κόσμο.

Το πρότυπο Mondex

Η κάρτα φορτώνεται αρχικά με το να έρχεται σε επαφή με την χρησιμοποίηση τραπεζών είτε με μια Mondex Αυτοματοποιημένη Μηχανή Ταμείων τραπεζών (ATM) είτε με τη χρησιμοποίηση ενός ειδικά προσαρμοσμένου τηλεφώνου. Αυτές οι συσκευές πρόσβασης δεν χρειάζεται να γνωρίζουν πως λειτουργεί το πρωτόκολλο chip-to-chip, αλλά μάλλον ενσωματώνουν μια Συσκευή Διεπαφών (IFD) η οποία περιέχει έναν επεξεργαστή ελέγχου που μεσολαβεί στο διάλογο μεταξύ της κάρτας και της τράπεζας. Στην τράπεζα, μια μορφή χρηματοκιβωτίου αποκαλούμενη Παράθυρο Τιμών Mondex εγκαθίστανται. Αυτή είναι μια συσκευή υλικού που μπορεί να κρατήσει τους μεγάλους αριθμούς καρτών Mondex και εκτελείται σαν μια αποθήκευση των τιμών για διάλογοι με τις κάρτες του πληθυσμού που έχουν εκδοθεί. Οι μεταφορές από και προς το Παράθυρο Τιμών είναι ελεγχόμενες από ένα σύστημα λογισμικού καλούμενο ως Έλεγχος και Διαχείρισης Συστημάτων Αξίας, και οι μετακινήσεις θα απεικονιστούν έπειτα στους τραπεζικούς λογαριασμούς των κατόχων της κάρτας.

Μια κάρτα Mondex παρεμβάλλεται σε ATM (ή σε προσαρμοσμένο τηλέφωνο) όπου πραγματοποιούνται οι διάλογοι chip-to-chip μεταξύ του IFD και της κάρτας που είναι υπό τον έλεγχο της συσκευής του ATM. Το Mondex IFD καθιερώνει έπειτα ένα διάλογο με την τράπεζα. Μόλις καθιερωθεί ο αριθμός λογαριασμού του κατόχου κάρτας, και η ελεγχόμενη ταυτότητα καρτών, η αξία μεταφέρεται από τις κάρτες στο Παράθυρο Τιμών της τράπεζας από το πρωτόκολλο chip-to-chip στο chip προορισμού που υπάρχει στην κάρτα. Το Σύστημα Ελέγχου και Διαχείρισης Αξίας ενημερώνει τα συστήματα λογιστικής της τράπεζας να χρεώσουν το ποσό στον τραπεζικό λογαριασμό του κατόχου της κάρτας.

Το να ξοδεύεις είναι μια παρόμοια διαδικασία, όπου οι έμποροι λιανικής πώλησης είναι εξοπλισμένοι με μια συσκευή η οποία αποκαλείται Τερματικό Μεταφοράς Αξίας. Άλλη μια φορά, αυτό περιέχει μια συσκευή IFD που διευκολύνει τη μεταφορά από την κάρτα πελατών στην κάρτα εμπόρων λιανικής πώλησης. Δεν υπάρχει καμία ανάγκη για έναν διάλογο σε απευθείας σύνδεση με την τράπεζα για να ελεγχθεί η μεταφορά. Σε ένα μεταγενέστερο στάδιο, ο έμπορος λιανικής πώλησης μπορεί να έρθει σε επαφή με την τράπεζα, να μεταφέρει την αξία του Παράθυρου Τιμών της τράπεζας, και ταυτόχρονα να πιστώνει το ποσό του λογαριασμού του.

Η συναλλαγή Mondex στο διαδίκτυο τρέχει ως εξής:

- Με την ολοκλήρωση της επιλογής προϊόντων του και την επιβεβαίωσή του στον προμηθευτή, ο πελάτης θα κλιθεί να παρεμβάλει την κάρτα Mondex του σε έναν αναγνώστη καρτών που συνδέεται με τον υπολογιστή του.

- Στην επιβεβαίωση ότι μια άλλη έγκυρη συσκευή υπάρχει στο τέλος της σύνδεσης, η αξία μεταφέρεται από την κάρτα του πελάτη στην κάρτα του προμηθευτή.

- Ο πελάτης λαμβάνει τις πληροφορίες (γραφικά, κείμενο, κομμάτια ήχου ή βίντεο) που ταξινόμησε.

Τα φυσικά αγαθά μπορούν επίσης να διαταχθούν και να πληρωθούν με τον ίδιο τρόπο.

Χαρακτηριστικά γνωρίσματα Mondex

Ασφάλεια: το θέμα της ασφάλειας βασίζεται πάνω σε μία ψηφιακή υπογραφή η οποία παράγεται από ένα chip της κάρτας. Η ψηφιακή υπογραφή μπορεί μόνο να αναγνωριστεί από άλλους ικανούς χρήστες του Mondex σε μια συναλλαγή.
Επειδή το Mondex μεταχειρίζεται μια κατάσταση της τεχνολογίας των υπολογιστών η οποία θα είναι απαραίτητη για να πολυγραφηθεί σε κάθε προσπάθεια για πλαστογράφηση είναι βέβαιο ότι τέτοιου είδους εξαπάτηση θα είναι μη κερδοφόρα.

Επίσης το Mondex σχεδιάζει να πραγματοποιήσει κανονικές και "σποραδικές" αναβαθμίσεις στα chips έτσι ώστε κάθε επιτυχημένη πλαστογράφησης να αποτυγχάνει ραγδαία. Ακόμα το Mondex σχεδιάζει να χρησιμοποιήσει διεξαγωγή δειγματοληψίας για να διατηρήσει μια εικόνα της ροής της αξίας και να χρησιμοποιήσει αυτή για να αναγνωρίσει τη δόλια και παράνομη χρήση της αξίας του Mondex σε κάθε πρώιμο στάδιο. Φυσικά για να είναι κάτι τέτοιο πιθανό το σύστημα Mondex δεν μπορεί να είναι ανώνυμο. Επιπλέον, τα Mondex chips έχουν σχεδιαστεί για να αντιστέκονται σε κάθε φυσική συνθήκη του κρύου, της ζέστης, της υγρασίας ή ηλεκτρικής παρέμβασης.

Double-spending prevention: σε κάθε Mondex συναλλαγή τα μηνύματα διαπερνούν διαμέσου της κάρτας συμπεριλαμβάνοντας δεδομένα τα οποία είναι μοναδικά για πάντα και δεν μπορούν να επαναληφθούν. Αυτή η ιδιαιτερότητα εμποδίζει μια πιθανή απάτη χρησιμοποιώντας οποιοδήποτε λαμβανόμενο μήνυμα για να "επαναλάβει" μια συναλλαγή και να στείλει $5 σε δύο ξεχωριστούς ανθρώπους ξεχωριστά.

Απώλεια-Ανευθυνότητα: αν η κάρτα χαθεί, η αξία σε χρήματα που υπάρχει μέσα στην κάρτα δεν είναι δυνατόν να αποκαλυφθεί. Όμως το Mondex επιτρέπει στους χρήστες καρτών να "κλειδώνουν" την αξία στις κάρτες τους εμποδίζοντας άλλους ανθρώπους να στείλουν χρήματα στην κάρτα. Αυτή η ευκολία δίνει την δυνατότητα στις τράπεζες να διαχειρίζονται ένα σύστημα επιστροφής και ανταμοιβής, και να υποστηρίζει την επιστροφή των καρτών στους σωστούς κατόχους τους (όπου αναγνωρίζονται), κάτι που δεν μπορεί ποτέ να συμβεί με την απώλεια 10 pounds ή εκατοντάδων φράγκων.

Ανωνυμία πληρωμή και μη αναγνώριση: η κάρτα διαφυλάττει ένα χαρτάκι που υπενθυμίζει τις τελευταίες 10 συναλλαγές που πραγματοποιήθηκαν με την κάρτα και το εσωτερικό του συστήματος, κρατά στη μνήμη του τις τελευταίες 300 συναλλαγές. Αυτό περιορίζει την ανωνυμία και αυξάνει την αναγνώριση του συστήματος.

Μεταφορά purse-to-purse: το Mondex επιτρέπει τις purse-to-purse πληρωμές. Χρησιμοποιώντας ένα Mondex χαρτοφυλάκιο δύο χρήστες καρτών μπορούν να μεταφέρουν μετρητά στις μεταξύ τους κάρτες. Με ένα Mondex τηλέφωνο οι purse-to-purse πληρωμές γίνονται ανά τον κόσμο.

Κατάσταση: το σχέδιο Mondex είναι σε ένα πιο ανεπτυγμένο στάδιο από ότι το πρότυπο CAFE συμπεριλαμβανομένου τους κατασκευαστές που φτιάχνουν και διακινούν τον απαραίτητο εξοπλισμό για να αναλάβουν τις Mondex διαχειρίσεις και έναν αριθμό επιτυχημένων μελετών.

NetCash

Ένα σύστημα ψηφιακών μετρητών, που βασίζεται σε λογαριασμούς χρέωσης-πίστωσης αλλά επιτρέπει παρορμητικές αγορές καθώς δεν απαιτεί καμία προεργασία για την πραγματοποίηση μιας πληρωμής. Η μετάδοση δεδομένων κρυπτογραφείται με την μέθοδο PGP.

Ηλεκτρονική Παρουσίαση και Πληρωμή Λογαριασμών

"Κάθε φορά που μια εταιρία συναλλάσσεται με τους πελάτες της, δημιουργεί λογαριασμούς για τα προϊόντα και τις υπηρεσίες που παρέχει. Το Internet μπορεί να διαδραματίσει σημαντικότατο ρόλο στη διαχείριση των λογαριασμών, στην παρουσίασή τους στους πελάτες και, φυσικά, στην πληρωμή τους από τους τελευταίους. "

Ο όρος Electronic Bill Presentment and Payment (EBPP) αναφέρεται στη χρήση του Διαδικτύου προκειμένου να παρουσιαστεί ο λογαριασμός στον πελάτη και, εν συνεχεία, όπου είναι απαραίτητο, να εξοφληθεί online. Θα πρέπει να γίνει σαφές ότι, ενώ το EBPP ανήκει σε αυτό που γενικά χαρακτηρίζουμε "ηλεκτρονικό εμπόριο", εντούτοις δεν περιορίζεται μόνο στα προϊόντα και τις υπηρεσίες που παρέχονται μέσο Internet.

Χαρακτηριστικό παράδειγμα, για να κατανοήσουμε αυτή την παρατήρηση, είναι οι τηλεπικοινωνιακές υπηρεσίες που παρέχονται από τα δίκτυα σταθερής ή κινητής τηλεφωνίας. Μπορεί, λοιπόν, οι υπηρεσίες να παρέχονται από ένα μέσο και με μία συγκεκριμένη διαδικασία, ωστόσο η παρουσίαση και πληρωμή του λογαριασμού μπορεί να γίνουν διαδικτυακά. Φυσικά, το EBPP μπορεί κάλλιστα να εφαρμοστεί και στις περιπτώσεις κατά τις οποίες ολόκληρη η συναλλαγή γίνεται μέσω Internet, για παράδειγμα όταν αγοράζουμε ένα ηλεκτρονικό βιβλίο (e-book) από το http://www.amazon.com./

Μπορούμε να έχουμε παντού ηλεκτρονικούς λογαριασμούς;

Στις συναλλαγές που γίνονται εξολοκλήρου -ή έστω σε μεγάλο βαθμό- online, το EBPP μοιάζει ως λογική συνέχεια της συναλλαγής και κατά συνέπεια χρησιμοποιείται. Πώς μπορούμε όμως να εντάξουμε το EBPP σε συναλλαγές που δεν πραγματοποιούνται μέσω Internet; Την απάντηση στο ερώτημα αυτό μπορούμε να τη δώσουμε εύκολα, εάν αναλογιστούμε ότι στη συντριπτική πλειονότητα των συναλλαγών, τα στοιχεία δημιουργούνται ή/ και τηρούνται με ηλεκτρονικό τρόπο.

Αν πάρουμε, για παράδειγμα, τις τηλεπικοινωνίες, όλες οι εγγραφές που αφορούν στις χρεώσεις των υπηρεσιών γίνονται και τηρούνται ηλεκτρονικά. Κάθε τηλεφώνημα δημιουργεί μία εγγραφή στο σύστημα χρεώσεων της τηλεπικοινωνιακής εταιρίας. Η άθροιση των εγγραφών για ένα τηλεφωνικό αριθμό ή μία ομάδα αριθμών σε συγκεκριμένη χρονική περίοδο δημιουργεί το λογαριασμό τηλεπικοινωνιακών τελών που μας αποστέλλει η αντίστοιχη εταιρία. Κατά συνέπεια, τα δεδομένα του λογαριασμού υπάρχουν ήδη ηλεκτρονικά, τόσο στην παραπάνω όσο και στη μεγάλη πλειονότητα των συναλλαγών μας. Με τα σύγχρονα συστήματα λογιστηρίου και τα προγράμματα ERP, κάθε συναλλαγή -ηλεκτρονική ή μη- παράγει ηλεκτρονικές εγγραφές, από τις οποίες μπορούμε να εκδώσουμε τόσο έντυπους όσο και ηλεκτρονικούς λογαριασμούς.

Από τη στιγμή που το κομμάτι που αφορά στα στοιχεία των λογαριασμών επιτρέπει την ηλεκτρονική διαχείριση, μπορούμε να κάνουμε εύκολα ηλεκτρονικά και το presentment, δηλαδή την παρουσίαση του λογαριασμού προς τον πελάτη μέσω Internet, αλλά και το payment, δηλαδή την ηλεκτρονική εξόφλησή του.

Εδώ αξίζει να αναφέρουμε ότι, μολονότι μελετάμε τη διαδικασία presentment και payment από κοινού, εντούτοις δεν είναι υποχρεωτικό να τις υλοποιήσουμε και τις δύο ηλεκτρονικά. Το πώς θα υλοποιηθεί το EBPP από μία εταιρία αλλά και το ποια στοιχεία του θα συμπεριλάβει στην υλοποίησή του είναι κάτι που εξαρτάται αποκλειστικά από τη στρατηγική της επιχείρησης. Επίσης, δεν πρέπει να ξεχνάμε και τους νομικούς περιορισμούς, οι οποίοι προς το παρόν επιβάλλουν την έκδοση έντυπων παραστατικών για τις συναλλαγές. Έτσι, μπορεί για παράδειγμα μία εταιρία να εφαρμόζει πρακτικές EBPP, πρέπει όμως να αποστείλει στους πελάτες της έντυπους λογαριασμούς ή τιμολόγια, ώστε να τα χρησιμοποιήσουν στην τήρηση των βιβλίων τους. Ωστόσο, παρά το γεγονός ότι και με το EBPP εκδίδονται έντυπα παραστατικά, δεν καταργούνται τα ουσιώδη πλεονεκτήματά του, ούτε τα οικονομικά ούτε όσα σχετίζονται με την εξυπηρέτηση του πελάτη.

Τα επιχειρηματικά μοντέλα του EBPP

Τα δύο βασικά μοντέλα του EBPP είναι το biller-direct και το consolidation ή aggregation model. Ως biller-direct νοείται το μοντέλο εκείνο που περιλαμβάνει την απευθείας αποστολή του λογαριασμού από τον πάροχο (biller) στον πελάτη, ενώ το consolidation model αφορά στη "φιλοξενία" ή "συνένωση" πολλών παρόχων σε ένα κοινό τόπο. Στο δεύτερο μοντέλο συναντάμε δύο κυρίως παραλλαγές, το thick και το thin model, τα οποία θα εξηγήσουμε αναλυτικότερα στη συνέχεια.

Biller-Direct Model

Το μοντέλο λειτουργίας biller-direct αφορά στην παροχή υπηρεσιών EBPP για ένα συγκεκριμένο πάροχο μέσω του δικού του δικτυακού τόπου. Οι λογαριασμοί παρουσιάζονται στους πελάτες (εταιρίες και ιδιώτες) σύμφωνα με τους όρους λειτουργικότητας που θέτει ο πάροχος, ενώ η πληρωμή των λογαριασμών υλοποιείται μέσω τραπεζών της επιλογής του ιδίου.

Στο μοντέλο αυτό, από τη στιγμή που ο πελάτης εγγραφεί στις υπηρεσίες EBPP, ο πάροχος δημιουργεί έναν ηλεκτρονικό φάκελο, στον οποίο καταγράφονται όλες οι πληροφορίες που σχετίζονται με το λογαριασμό του. Σε ορισμένες περιπτώσεις, ο πάροχος μπορεί να επιλέξει τη μέθοδο του outsourcing, αναθέτοντας δηλαδή την παραπάνω διαδικασία σε έναν BSP (Bill Service

Provider), ο οποίος αναλαμβάνει την παροχή υπηρεσιών όπως μετάφραση και τυποποίηση των ηλεκτρονικών
λογαριασμών, ανάλυση των δεδομένων και, μερικές φορές φιλοξενία (hosting) του site του παρόχου.

Το επόμενο βήμα, μετά τη δημιουργία του ηλεκτρονικού φακέλου, αφορά στην ειδοποίηση του πελάτη. Συγκεκριμένα, ο πάροχος ειδοποιεί τον πελάτη για έναν εκκρεμή λογαριασμό, συνήθως μέσω email, και ο πελάτης "κατευθύνεται" στο δικτυακό τόπο του παρόχου (ή του BSP) όπου βλέπει την κατάσταση του λογαριασμού του σε ηλεκτρονική μορφή. Στη συνέχεια, ο πελάτης μπορεί να προχωρήσει σε πληρωμή του λογαριασμού του απευθείας από το site.

Όπως βλέπουμε, η λέξη-κλειδί στο συγκεκριμένο μοντέλο είναι η απευθείας επικοινωνία. Από τη στιγμή της εγγραφής του πελάτη μέχρι και την πληρωμή δεν παρεμβαίνει κανείς πλην του παρόχου και του πελάτη. Για το λόγο αυτό, ο πάροχος είναι υπεύθυνος για την επικοινωνία με τον πελάτη σε όλη τη διάρκεια της διαδικασίας.

Consolidation Model

Το συγκεκριμένο μοντέλο αναπτύχθηκε για να ικανοποιήσει τις επιθυμίες των πελατών ως προς την ύπαρξη κοινού τόπου, όπου θα διεκπεραιώνουν τις πληρωμές τους, προσφέροντας παράλληλα μειωμένο κόστος ανάπτυξης μιας EBPP λύσης στους παρόχους. Στο μοντέλο αυτό, ο πάροχος αποστέλλει τις πληροφορίες του λογαριασμού του πελάτη σε έναν τρίτο, ο οποίος καλείται bill consolidator. Αυτός, λειτουργώντας προς όφελος του πελάτη, συνδυάζει τα δεδομένα από πολλαπλούς παρόχους και συνενώνει την πληροφορία σε έναν κοινό τόπο. Μολονότι κάποιοι consolidators παρουσιάζουν τους λογαριασμούς στα δικά τους websites, το μοντέλο αυτό λειτουργεί πιο ευέλικτα με την ύπαρξη Customer Service Providers (CSP), στους δικτυακούς τόπους των οποίων παρουσιάζονται με ενοποιημένο τρόπο οι λογαριασμοί πολλαπλών billers

Το ρόλο του CSP μπορούν να παίξουν Internet Service Providers (Εταιρίες Παροχής Υπηρεσιών Internet), portals (δικτυακές πύλες), χρηματοοικονομικά ιδρύματα, e-marketplaces, κ.λ.π. Επικρατέστερα πάντως στην ελληνική αγορά για το ρόλο του CSP παρουσιάζονται τα web banking sites των τραπεζών, που διαθέτουν τις κατάλληλες υποδομές και δημιουργούν τις απαραίτητες συνθήκες για ενσωμάτωση των διαδικασιών πληρωμών.

Το consolidation μοντέλο περιλαμβάνει δύο επιμέρους "παραλλαγές", το thick model, βάσει του οποίου όλα τα στοιχεία του λογαριασμού παρέχονται από συγκεκριμένο CSP site, και το thin model, με το οποίο τα αναλυτικά στοιχεία του λογαριασμού παρέχονται από την ιστοσελίδα του παρόχου.

Ολοκληρώνοντας την αναφορά μας στα μοντέλα του EBPP, θα πρέπει να σημειώσουμε ότι το consolidation model είναι το εκείνο που εμφανίζει τις μεγαλύτερες πιθανότητες να επικρατήσει στο χώρο του EBPP, καθώς προσφέρει ταυτόχρονη παρακολούθηση όλων των λογαριασμών και ενιαίο σχεδιασμό λογαριασμών (one-stop billing). Η ανάπτυξή του στην Ελλάδα εξαρτάται σε σημαντικό βαθμό από την αντίληψη των τραπεζών, οι οποίες περιμένουν... ποια θα κάνει την αρχή, για να ακολουθήσουν και οι υπόλοιπες, κατάσταση δηλαδή παρόμοια με εκείνη του web banking.

Γιατί EBPP;

Ανάλογα με τον τρόπο και την εφαρμογή, το EBPP προσφέρει σημαντικά πλεονεκτήματα τόσο σε αυτούς που εκδίδουν τους λογαριασμούς όσο και στους πελάτες τους.

- Οφέλη για τους εκδότες των λογαριασμών: Με τη χρήση του EBPP μειώνεται ή περιορίζεται σημαντικά η ανάγκη για αποστολή έντυπων λογαριασμών προς τους πελάτες. Σύμφωνα με έρευνα της εταιρίας Linkata, το κόστος για κάθε έντυπο λογαριασμό είναι:

- Κόστος λογαριασμού €0,018

    - Κόστος φακέλου €0,035
    - Κόστος εκτύπωσης €0,043
    - Κόστος ταχυδρομείου €0.088
    - Διαχείριση €0,035
    - Αναλώσιμα εκτυπωτή €0,25
    - Συντήρηση εκτυπωτή €0,009

Παρόλο που αθροιζόμενα τα παραπάνω κόστη δεν αποτελούν ευκαταφρόνητο ποσό ανά λογαριασμό, οι περιορισμοί της ελληνικής νομοθεσίας που αναφέραμε παραπάνω μειώνουν σημαντικά τα οφέλη, καθώς, όπως και να έχει, πρέπει να στείλουμε τουλάχιστον μία έντυπη σελίδα. Ωστόσο δεν καταργούνται τα οφέλη από το EBPP, καθώς μπορούμε να στείλουμε στους πελάτες μας μόνο μία σελίδα και όχι ανάλυση του λογαριασμού (η ανάλυση μπορεί να παρέχεται ηλεκτρονικά), εξοικονομώντας σε χαρτί, εκτύπωση, διαχείριση και ταχυδρομικά. Είναι χαρακτηριστικό ότι ο τηλεπικοινωνιακός λογαριασμός μιας μεγάλης εταιρίας μπορεί να αποτελείται από δεκάδες σελίδες με ανάλυση των κλήσεων. Η εκτύπωση και αποστολή αυτού του μικρού... βιβλίου κοστίζει αρκετά στην τηλεπικοινωνιακή εταιρία, ενώ και ο πελάτης που το λαμβάνει δεν μπορεί ουσιαστικά να το διαχειριστεί, καθώς κανένας συνδρομητής δεν πληκτρολογεί τα δεδομένα για να επαληθεύσει το πληρωτέο ποσό! Επίσης, ο

εκδότης του λογαριασμού έχει όφελος και από τη διαδικασία πληρωμής του, αφού με την ηλεκτρονική πληρωμή γίνονται όλα πιο άμεσα και πιο οικονομικά γι' αυτόν.
Οφέλη για τους πελάτες: Ανεξάρτητα από το μοντέλο EBPP, οι πελάτες κερδίζουν ως προς το ότι χρησιμοποιούν ένα μέσο (το Internet) για να διαχειρίζονται τους λογαριασμούς τους. Επίσης, οι ηλεκτρονικοί λογαριασμοί τούς προσφέρουν μεγάλη ευελιξία στην επεξεργασία του περιεχομένου τους. Το παράδειγμα του τηλεπικοινωνιακού λογαριασμού που αναφέραμε παραπάνω είναι χαρακτηριστικό: με όλα τα δεδομένα των κλήσεων να είναι διαθέσιμα ηλεκτρονικά, ο πελάτης μπορεί εύκολα να κάνει επεξεργασία και να βγάλει χρήσιμα γι' αυτόν συμπεράσματα σχετικά με τις κλήσεις του.

- Ολοκλήρωση των ηλεκτρονικών συναλλαγών: Το EBPP προσφέρει πολλά σε κάθε είδους συναλλαγή, στην περίπτωση όμως των ηλεκτρονικών, αποτελεί αναπόσπαστο μέρος, καθώς θα ήταν τουλάχιστον ανώφελο να γίνεται μία πώληση ηλεκτρονικά και ο λογαριασμός να αποστέλλεται και να εξοφλείται με άλλο, μη ηλεκτρονικό τρόπο. Έτσι, καθώς θα αυξάνονται οι ηλεκτρονικές συναλλαγές, και ιδιαίτερα αυτές που αφορούν το B2B, το EBPP θα χρησιμοποιείται όλο και περισσότερο, αποδεικνύοντας τα αναμφισβήτητα πλεονεκτήματά του. Προστιθέμενη αξία προς τον πελάτη: Το EBPP προσφέρει στους εκδότες των λογαριασμών τη δυνατότητα να κάνουν πιο εύκολα προωθητικές ενέργειες και ενέργειες marketing προς τους πελάτες τους, ανάλογα με την κατηγορία των τελευταίων. Στους έντυπους λογαριασμούς είναι πολύ δύσκολο να συμπεριλάβουμε πολλά διαφορετικά φυλλάδια και να τα αποστείλουμε σε συγκεκριμένους πελάτες. Στους ηλεκτρονικούς λογαριασμούς, όμως, μπορούμε να επιτύχουμε ακόμα και προσωπική προσέγγιση στον κάθε πελάτη μας. Επίσης, το EBPP αποτελεί μέρος ενός αποτελεσματικού customer service. Στο χαρτί μπορούμε να συμπεριλάβουμε λίγα στοιχεία ανάλυσης για το λογαριασμό. Αντίθετα, στην ηλεκτρονική του μορφή μπορούμε να έχουμε επαρκέστατη ανάλυση, μειώνοντας τις περιπτώσεις κλήσεων

  από πελάτες για παροχή διευκρινίσεων και, βέβαια, παρέχοντάς τους ποιοτικότερες υπηρεσίες.

Είναι γεγονός ότι, αν και στις περισσότερες περιπτώσεις το EBPP υιοθετείται για τον περιορισμό των εξόδων έκδοσης και διαχείρισης λογαριασμών, εντούτοις γρήγορα οι εταιρίες αντιλαμβάνονται ότι απολαμβάνουν επιπλέον οφέλη, τα οποία πηγάζουν από τη δημιουργία καλύτερων σχέσεων με τους καταναλωτές.

Επιχειρηματικό πλάνο για επιτυχημένο EBPP

Για κάθε επιχείρηση που θέλει να λέγεται σοβαρή, πριν από την τελική απόφαση για την είσοδο σε μια νέα δραστηριότητα, απαραίτητη θεωρείται η κατάρτιση ενός επιχειρηματικού πλάνου (του γνωστού business plan). Ένα σωστά σχεδιασμένο, δομημένο και φυσικά ρεαλιστικό επιχειρηματικό πλάνο θα καθορίσει αν μια νέα επιχειρηματική δραστηριότητα είναι κατάλληλη για τη φιλοσοφία της επιχείρησης, εφικτή, επιχειρηματικά αξιοποιήσιμη και, κατ' επέκταση, κερδοφόρα. Το επιχειρηματικό πλάνο ουσιαστικά εκπαιδεύει τη διοίκηση και αποτελεί ένα εργαλείο που χρησιμοποιείται για την όσο το δυνατόν ρεαλιστικότερη αποτίμηση ενός έργου.

Στην περίπτωση του EBPP, η ανάπτυξη επιχειρηματικού πλάνου ακολουθεί τις βασικές αρχές, προσαρμοσμένες φυσικά στη συγκεκριμένη αγορά. Θεωρούμε ότι η παράθεση των βασικών σταδίων στην ανάπτυξη business plan είναι εξαιρετικά σημαντική για τις εταιρίες εκείνες που επιθυμούν να δραστηριοποιηθούν στο συγκεκριμένο χώρο, ο οποίος, σύμφωνα με τις διεθνείς τάσεις, θα γνωρίσει μεγάλη εξάπλωση τα προσεχή χρόνια. Τα βασικά, συνεπώς, στάδια ενός EBPP επιχειρηματικού πλάνου περιλαμβάνουν:

- Τη στρατηγική και τους στόχους της επιχείρησης,
- Την ανάλυση της τρέχουσας κατάστασης της αγοράς αλλά και των μελλοντικών τάσεων,
- Την οικονομική ανάλυση της επιχείρησης, που θα καθορίζει τα απαιτούμενα έσοδα αλλά και τα πάσης,
- Τη δημιουργία ενός πλάνου αποτίμησης κινδύνου τόσο για την υιοθέτηση όσο και για τη μη υιοθέτηση της δραστηριότητας.

Στρατηγική και στόχοι EBPP

Καθώς η επιχείρηση εξετάζει το EBPP project και τις επιπτώσεις του, είναι σημαντική η εξασφάλιση της "ευθυγράμμισής" του με τη συνολική της φιλοσοφία. Έτσι, αρχικά θα πρέπει να δοθεί απάντηση στο ερώτημα:

- Διαθέτει η επιχείρηση εμπειρία στο χώρο του ηλεκτρονικού εμπορίου; Υπάρχουν συγκεκριμένοι στόχοι για την αύξηση της ηλεκτρονικής δραστηριότητας και τη μείωση του χαρτιού;

Στη συνέχεια, η αναζήτηση θα πρέπει να στραφεί εσωτερικά, έτσι ώστε να καθοριστούν σαφώς τα "δυνατά χαρτιά" της επιχείρησης. Απαντήσεις ζητούν τα παρακάτω ερωτήματα:

- Υπάρχουν στελέχη με εμπειρία στο EBPP;
- Θα πρέπει να προσληφθούν άτομα με σχετική εμπειρία
- Θα πρέπει να χρησιμοποιηθούν σύμβουλοι;
- Πέραν των στελεχών που θα απασχοληθούν, μπορεί να χρησιμοποιηθεί η υπάρχουσα υποδομή;
- Υπάρχει πληρότητα στις λειτουργίες της επιχείρησης, ώστε να "στηριχτεί" η νέα υπηρεσία;

Σημαντική, στην παρούσα φάση, είναι και η ανάπτυξη μιας ευέλικτης προσέγγισης στο EBPP, ειδικά στα αρχικά στάδια εξέλιξης. Η κατανόηση των αγοραστικών τάσεων θα βοηθήσει στο σχεδιασμό μιας εφαρμογής που θα μπορέσει να ενσωματώσει και να εκμεταλλευθεί τις πρωτοπορίες που υπάρχουν στην αγορά. Επίσης, σημαντική είναι η κατανόηση των εσωτερικών διαδικασιών και η αξιολόγηση των επιπτώσεων από την εφαρμογή του EBPP. Συγκεκριμένα, θα πρέπει να απαντηθούν τα παρακάτω:

- Η EBPP δραστηριότητα θα τονώσει τη χρηματορροή;
- Η υιοθέτηση του EBPP θα εξαφανίσει/ μειώσει την παραδοσιακή επεξεργασία των λογαριασμών και των πληρωμών;
- Θα υπάρξει αύξηση της πίεσης στο web site και, αν ναι, μπορεί η υπάρχουσα υποδομή να διαχειριστεί τον αυξημένο όγκο;
- Ποιες είναι οι επιπτώσεις του EBPP στα υπάρχοντα επίπεδα προσωπικού; (π.χ. θα υπάρχει αποσυμφόρηση στο τηλεφωνικό κέντρο;)
- Ποια υποδομή θα χρειαστεί για κάλυψη 24x7x365, η οποία είναι δεδομένη από τη στιγμή που η υπηρεσία παρέχεται μέσω Internet;

Ανάλυση Αγοράς

Προτού προβεί στην ανάλυση της τρέχουσας αγοραστικής κατάστασης, η επιχείρηση θα πρέπει να κοιτάξει τους υπάρχοντες πελάτες της.

- Μπορεί το EBPP να βελτιώσει τη "μεταφορά" σχετικών με τα προϊόντα πληροφοριών στους πελάτες;

Από τη στιγμή που έχει ληφθεί η απόφαση για την τελική υλοποίηση μιας EBPP λύσης, η διοίκηση οφείλει να αξιολογήσει τις δυνατότητες της επιχείρησης να ολοκληρώσει το προϊόν. Έτσι, η επιχείρηση θα πρέπει να συνειδητοποιήσει ότι το EBPP θα της δώσει τη δυνατότητα να στοχεύσει σε συγκεκριμένους πελάτες και, μάλιστα, σε βάση "1 προς 1". Αυτό επιτυγχάνεται από τη στιγμή που αυτή έχει πλέον τη δυνατότητα να μάθει περισσότερα για τις αγοραστικές συνήθειες του κάθε πελάτη ξεχωριστά ή και συγκεκριμένων ομάδων πελατών με τις ίδιες συνήθειες, και να "στοχεύσει" ανάλογα. Επιπλέον, το EBPP προσφέρει στην επιχείρηση τον "αέρα" της πρωτοπορίας, αυξάνει τη δυνατότητα εδραίωσης της επωνυμίας της και μπορεί να αποτελέσει το πρώτο βήμα για πρόσθετες δραστηριότητες στο χώρο του

Από τη στιγμή που έχει περατωθεί η έρευνα της αγοράς και έχει διαπιστωθεί ότι η επιχείρηση διαθέτει τις τεχνικές δυνατότητες για την υλοποίηση μιας EBPP λύσης, το επόμενο βήμα αφορά στα οικονομικά αποτελέσματα του εγχειρήματος στον οργανισμό.

- Μπορεί η εγκατάσταση του EBPP να αυξήσει τα έσοδα από διασταυρούμενες πωλήσεις;
- Θα δημιουργήσει το EBPP νέα διαφημιστικά έσοδα;
- Μπορεί η υιοθέτηση μιας EBPP λύσης να βοηθήσει στη διατήρηση των, υψηλής - για την επιχείρηση- αξίας, νοικοκυριών ή/ και πελατών;

Έξοδα

Με την υλοποίηση του EBPP, η επιχείρηση μπορεί να εξοικονομήσει σημαντικά κόστη από την παροχή ηλεκτρονικών λογαριασμών σε σχέση με την παραδοσιακή έντυπη μέθοδο. Τα διεθνή στοιχεία αναφέρουν μια μέση μείωση του κόστους που κυμαίνεται από 1 έως και 5 δολάρια ανά λογαριασμό.

- Η επιχείρηση θα πρέπει να έχει κατά νου ότι η εγκατάσταση οποιασδήποτε νέας τεχνολογικής υποδομής που θα στηρίξει την EBPP λύση μπορεί να επιφέρει αύξηση στα κόστη.
- Τα ηλεκτρονικά προϊόντα έχουν από τη φύση τους μια ισχυρή δυναμική μείωσης του κόστους, που προέρχεται από τα σχετικά με τα ανθρώπινα λάθη έξοδα επεξεργασίας. Το EBPP μπορεί να μειώσει τα έξοδα που προέρχονται από την επεξεργασία των πληρωμών.

Συλλογή Στοιχείων / Customer Spotting / Επικοινωνία / Προβολή - Προώθηση

Το διαδίκτυο μπορεί να φανεί ένα πολύ χρήσιμο εργαλείο όσον αφορά στη συλλογή στοιχείων για τους υπάρχοντες πελάτες σας αλλά και τους εν δυνάμει πελάτες σας. Μέσα από την ιστοσελίδα σας μπορείτε να συλλέξετε στοιχεία που θα σας φανούν πολύ χρήσιμα για την κατανόηση των χαρακτηριστικών της "ομάδας στόχος" (target group).

Η μετέπειτα επεξεργασία των στοιχείων που θα συγκεντρώσετε θα σας βοηθήσει να κατανοήσετε τις ανάγκες των πελατών σας, να βελτιώσετε το επίπεδο των προϊόντων και των υπηρεσιών που προσφέρετε όπως επίσης και να μπορέσετε να έχετε πιο προσωποποιημένη επικοινωνία με τους πιθανούς πελάτες σας.
Πιο αναλυτικά μπορείτε να κάνετε τα παρακάτω:

Δημιουργία λίστας αποστολής μηνυμάτων (Mailing List)

Συγκεντρώνοντας τα e-mail των πελατών σας μπορείτε να αναπτύξετε μαζί τους μια μόνιμη επικοινωνία η οποία θα είναι επωφελής για την εικόνα, τις σχέσεις με τους πελάτες και τις πωλήσεις της επιχείρησης. Ένας καλός τρόπος για την συγκέντρωση των Ηλεκτρονικών Διευθύνσεων των εν δυνάμει πελατών σας είναι να τους ζητάτε, μέσω της ιστοσελίδας, να δηλώσουν ενδιαφέρον για την παραλαβή ενός περιοδικού ενημερωτικού Newsletter.

Σε κάποιες περιπτώσεις καλύτερο θα ήταν να δίνατε τη δυνατότητα επιλογής για το περιεχόμενο των e-mail ή των Newsletter ώστε να μην βομβαρδίζονται από αδιάφορα προς αυτούς μηνύματα.

Σε αυτό το σημείο θα πρέπει να τονίσουμε ότι οι περισσότεροι χρηστές Ηλεκτρονικού Ταχυδρομείου θεωρούν "ιερό" των φάκελο εισερχομένων, γι' αυτό το λόγο θα πρέπει να είσαστε προσεκτικοί στα παρακάτω:

- Να μη στέλνετε συνεχώς e-mail. Θα πρέπει να υπάρχει κάποια περιοδικότητα η οποία δε θα εκνευρίσει τον αναγνώστη.
- Τα e-mail που στέλνετε δε θα πρέπει να είναι εκτός θέματος και πέρα από αυτό που έχουν ζητήσει οι πελάτες ή οι ενδιαφερόμενοι.
- Θα πρέπει να εγγυηθείτε ότι δεν θα κοινοποιήσετε τη λίστα σας αλλού και για άλλους σκοπούς από αυτούς για τους οποίους σας ζητήθηκε.
- Θα πρέπει να είσαστε προσεκτικοί στις διατυπώσεις σας για την αποφυγή παρεξηγήσεων.

Στην Ελληνική αγορά υπάρχουν πολλές εξειδικευμένες εταιρείες οι οποίες θα μπορέσουν να σας δώσουν ιδέες και λύσεις για την καλύτερη δημιουργία και διαχείριση της λίστας αποστολής μηνυμάτων (mailing list).

Customer Spotting

Η συλλογή στοιχείων των πελατών και η χρήση τους για την καταγραφή των αναγκών τους, της συμπεριφορά τους και τελικά για επικοινωνία ονομάζεται Customer Spotting.
Μέσω της ιστοσελίδας σας ή και κατά την ώρα της πώλησης μπορείτε να συμπληρώσετε τα στοιχεία πελατών και ενδιαφερομένων για τα προϊόντα ή τις υπηρεσίες σας. Αργότερα προσθέτοντας αυτά τα στοιχεία σε μια βάση δεδομένων μπορείτε να βγάλετε συμπεράσματα όπως:

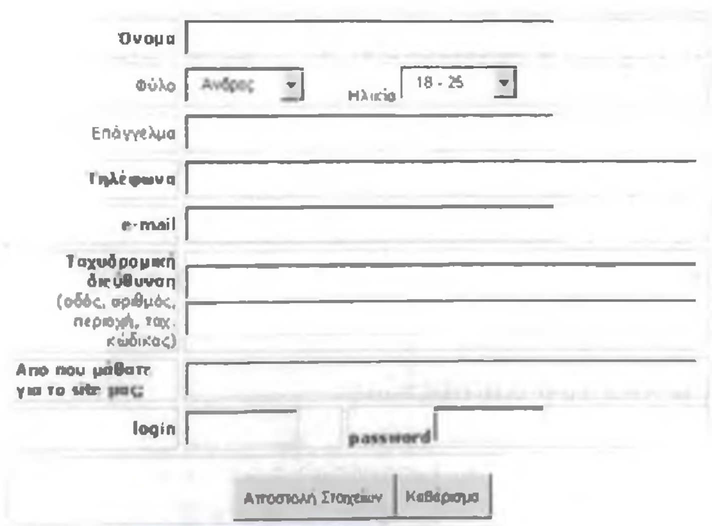
- Τι ηλικία έχει η πλειονότητα των πελατών σας,
- Επίπεδο μόρφωσης ή επάγγελμα,
- Ποια περίοδο του χρόνου συνήθως υπάρχει αύξηση και σε ποιο προϊόν

Επίσης μπορείτε να συνδυάσετε στοιχεία όπως:

- Ηλικία, φύλο, επάγγελμα ανά προϊόν (π.χ. οι νέοι μπορεί να αγοράζουν περισσότερο κινητά που αλλάζουν πρόσοψη, ενώ σε
- πιο μεγάλες ηλικίες ενδιαφέρονται πιο πολύ για ένα εύχρηστο κινητό),
- Ποσό που ξοδεύτηκε ανά κατηγορία πελάτη κ.λ.π.

Γενικά, επιλέγετε τι θέλετε να παρατηρήσετε και ανάλογα διαμορφώνετε τη φόρμα. Ιδιαίτερη προσοχή πρέπει να δοθεί στο να μη γίνονται αδιάκριτες ερωτήσεις και να μην ζητούνται πολλά και ευαίσθητα δεδομένα ώστε να μειωθούν οι πιθανότητες μη απάντησης.

Παρακάτω παρουσιάζεται ένα παράδειγμα φόρμας στην οποία συλλέγονται δημογραφικά στοιχεία (e-mail, φύλο, ηλικία, επάγγελμα) και άλλα στοιχεία. Σε αυτήν εδώ τη φόρμα ο ενδιαφερόμενος μπορεί να γίνει και μέλος κάποιου club που έχει δημιουργήσει η εταιρεία. Η συγκεκριμένη φόρμα θα πρέπει να μπορεί να χρησιμοποιηθεί για την αποστολή κάποιου καταλόγου για την άμεση επικοινωνία μέσω e-mail ή για τη μαζική αποστολή Newsletter κ.λ.π.



Υπάρχουν πολλά απλά και εύχρηστα προγράμματα στην αγορά που μπορούν να καλύψουν τις ανάγκες σας. Επίσης μπορείτε να συμβουλευτείτε εταιρείες λογισμικού για τη δημιουργία ενός προγράμματος κομμένου και ραμμένου στα μέτρα σας.

Επικοινωνία μέσω του διαδικτύου

Η επικοινωνία μέσω του διαδικτύου με οποιονδήποτε ενδιαφερόμενο (πελάτες, συνεργάτες, προμηθευτές κ.λ.π.) προσφέρει στην επιχείρηση πολλά πλεονεκτήματα. Μερικά από αυτά αναφέρονται παρακάτω:

- Εξοικονόμηση χρημάτων από τα τηλεφωνήματα,
- Δυνατότητα αποστολής εγγράφων, φωτογραφιών και αρχείων video με σχεδόν μηδενικό κόστος,
- Άμεση απάντηση και καταγραφή ερωτημάτων, παρατηρήσεων και σχολίων των πελατών,
- Ανάπτυξη πιο καλών και συχνών σχέσεων με τους πελάτες,
- Δυνατότητα πιο προσωποποιημένης επικοινωνίας με χαμηλότερο κόστος

Η επικοινωνία και η ανάπτυξη σχέσεων μειώνει κατά πολύ τις επιλογές των πελατών και δημιουργεί πιστούς πελάτες. Αυτό έχει πολλαπλά οφέλη αφού το κόστος της επίσκεψης ενός νέου πελάτη είναι περισσότερο από το πενταπλάσιο από το αντίστοιχο κόστος ενός παλιού.

Επίσης η ανάπτυξη σχέσεων βοηθάει στη δημιουργία μιας σταθερής πελατειακής βάσης, η οποία συνήθως είναι το πιο ισχυρό χαρτί για την επιβίωση αλλά και την ανάπτυξη της ΜΜΕ. Επίσης δεν πρέπει να υποτιμάται η χρήση της επικοινωνίας ως μέσου προώθησης η σημασία της οποίας εξετάζεται στην επόμενη ενότητα.

Προβολή-Προώθηση μέσω του Διαδικτύου

Στις μέρες μας ο μέσος καταναλωτής δέχεται καταιγισμό πιέσεων και μηνυμάτων από πάρα πολλές μεγάλες εταιρείες οι οποίες έχουν την δυνατότητα να κάνουν συνδυασμένες διαφημιστικές καμπάνιες χρησιμοποιώντας όλα τα δυνατά μέσα (τηλεόραση, ραδιόφωνο, εφημερίδες, Διαδίκτυο κ.α.). Αυτό δημιουργεί ιδιαίτερα προβλήματα στις μικρότερες επιχειρήσεις οι οποίες στην πλειονότητά τους ως μόνο μέσο προβολής έχουν το ίδιο το κατάστημα ή τα γραφεία τους.

Κάτω από αυτές τις συνθήκες οι μικρότερες επιχειρήσεις πρέπει να βρουν έναν οικονομικό τρόπο να προβάλουν τον εαυτό τους αλλά και τα πλεονεκτήματά τους έναντι των μεγαλύτερων ανταγωνιστών τους. Το διαδίκτυο προσφέρει μια καλή και οικονομική λύση προβολής της επιχείρησης και των προϊόντων της.

Μέσω του διαδικτύου μπορεί να ανοίξει ένα "υποκατάστημα σας σε κάθε σπίτι" αφού ο ενδιαφερόμενος θα μπορεί να δει την επιχείρηση και τα προϊόντα της από το σπίτι του. Θα μπορεί να μάθει περισσότερα στοιχεία να δει φωτογραφίες, τιμές αλλά και να επικοινωνήσει με την επιχείρηση για οποιονδήποτε λόγο επιθυμεί (Τα πολλαπλά οφέλη της επικοινωνίας αναλύθηκαν στην προηγούμενη ενότητα).

Η σημασία της προβολής και της προώθησης είναι μεγάλη και δεν είναι τυχαίο ότι υπάρχουν επιχειρήσεις που δαπανούν ετησίως τεράστια ποσά για την προβολή τους. Τα κύρια θετικά αποτελέσματά της αναφέρονται επιγραμματικά παρακάτω:

- **Εξοικείωση του καταναλωτή με την εταιρεία το προϊόν ή τη φίρμα:**

Έχει αποδειχτεί ότι πιο εύκολα εμπιστευόμαστε μία εταιρεία που την έχουμε ξαναδεί, έστω και αν δεν έχουμε αγοράσει ποτέ από αυτή, παρά μια που ποτέ δεν την έχουμε ξαναδεί).

- **Απόκτηση μεγαλύτερης αξιοπιστίας και κύρους:**
  Η δημιουργία μίας καλαίσθητης ιστοσελίδας μπορεί να προσδώσει πολλά στην εικόνα της επιχείρησης και αυτό είναι κάτι που έχει μεγάλη σημασία για τον καταναλωτή

- **Πληροφόρηση:**
  Ο καταναλωτής μπορεί να μάθει για τις τιμές και τα χαρακτηριστικά των προϊόντων από την ιστοσελίδα.

- **Ικανοποίηση:**
  Ο καταναλωτής πάντα εκτιμά την προσπάθεια να ενημερώνεται και να εξυπηρετείται.

Πριν αποφασίσετε να προχωρήσετε στην κατασκευή μιας ιστοσελίδας θα πρέπει να έχετε απαντήσει στα παρακάτω ερωτήματα:

- **Τι θέλω να πετύχω μέσω της ιστοσελίδας;**
- **Σε ποιους απευθύνεται;**
- **Τι θέλουν οι ενδιαφερόμενοι να δουν;**
- **Πώς θα κάνω πιο γνωστή την ιστοσελίδα μου;**
- **Θα έχει αποτελέσματα η δαπάνη μου;**

Η δημιουργία μιας σωστής ιστοσελίδας για την εξυπηρέτηση των σκοπών της επιχείρησης θα πρέπει να γίνεται σε συνεργασία με εταιρείες που είναι εξειδικευμένες σε αυτόν τον τομέα (παροχή υπηρεσιών Internet- Internet Service Providers-ISPs ή άλλοι προμηθευτές.

Επίσης είναι σε θέση να σας αναλύσουν και να σας δώσουν ολοκληρωμένες λύσεις και προτάσεις για τους στόχους και τη μορφή της ιστοσελίδας σας. Στην ιστοσελίδα του "Δικτυωθείτε" μπορείτε να δείτε αρκετά παραδείγματα επιτυχημένων ιστοσελίδων που έκαναν και χρήση του προγράμματος.

Παρόλα αυτά μπορείτε και μόνοι σας να φτιάξετε μια αξιόλογη ιστοσελίδα με πολύ καλά αποτελέσματα. Ενδιαφέρον παρουσιάζει το αφιέρωμα που υπάρχει στον κόμβο σχετικά με τις λύσεις πακέτων για αυτόματη δημιουργία ιστοσελίδων.
Περισσότερες πληροφορίες για την προώθηση και την προβολή μέσω του διαδικτύου στο αφιέρωμα "Το Internet ως μέσο για προωθητικές ενέργειες".

Τραπεζικές Συναλλαγές

Διαδικτυακές Τραπεζικές Συναλλαγές (e-banking). Η σημερινή εφαρμογή τους στην Ελλάδα

"Το e-banking (ή Internet banking) υπόσχεται την επανάσταση στις τραπεζικές συναλλαγές. "Μεταφέρει" την ίδια την τράπεζα στην οθόνη του υπολογιστή μέσω Διαδικτύου, με άμεση πρόσβαση στους τραπεζικούς λογαριασμούς, παρέχοντας τη δυνατότητα διεκπεραίωσης συναλλαγών, παρακολούθησης της πορείας χαρτοφυλακίων, εξόφλησης λογαριασμών ΔΕΚΟ και πιστωτικών καρτών, καθώς και πλήθος άλλων υπηρεσιών. Οι πελάτες (ιδιώτες και επιχειρήσεις) ωφελούνται σημαντικά από τη χρήση των υπηρεσιών e-banking, καθώς τους παρέχεται η δυνατότητα να διεκπεραιώνουν ένα μεγάλο μέρος των συναλλαγών τους με την τράπεζα εύκολα, γρήγορα και με ασφάλεια 24 ώρες το 24ωρο, 365 μέρες το χρόνο. Για τις ΜΜΕ το όφελος είναι ακόμη μεγαλύτερο, καθώς περιορίζεται το κόστος λειτουργίας τους όσον αφορά σε λειτουργικά έξοδα, προμήθειες και κινδύνους απώλειας χρήματος, ενώ παράλληλα εξοικονομείται πολύτιμος χρόνος.

Με το e-banking οι τραπεζικές υπηρεσίες προσφέρονται ανά πάσα στιγμή, ο δε καταναλωτής μπορεί να ενημερωθεί για κάθε προϊόν ή υπηρεσία ανέξοδα και χωρίς χρόνους αναμονής. Συχνό είναι και το φαινόμενο των προσφορών ή της εφαρμογής ευνοϊκότερων όρων στην παροχή προϊόντων μέσω Internet, γεγονός που από μόνο του είναι ικανό να προσελκύσει σημαντική μερίδα καταναλωτών που αναζητούν προσφορές.

Οι βασικότερες υπηρεσίες που παρέχουν μέσω Internet οι ελληνικές τράπεζες είναι οι εξής:

- **Πληροφορίες υπολοίπων για τους τηρούμενους λογαριασμούς,**
- **Μεταφορές ποσών μεταξύ των τηρούμενων λογαριασμών του ιδίου νομίσματος,**
- **Πληροφορίες σχετικά με τις πρόσφατες κινήσεις των τηρούμενων λογαριασμών,**
- **Δυνατότητα έκδοσης και αποστολής παλαιότερων κινήσεων των τηρούμενων λογαριασμών,**
- **Παραγγελία μπλοκ επιταγών,**
- **Δυνατότητα υποβολής αίτησης για ανάκληση επιταγών ή ολόκληρου του μπλοκ επιταγών,**
- **Εντολές αγοραπωλησίας μετοχών,**
- **Ενημέρωση για την κίνηση των προσωπικών αμοιβαίων κεφαλαίων,**
- **Δυνατότητα υποβολής αιτήσεων εμβασμάτων,**
- **Αλλαγή του απορρήτου κωδικού PIN,**
- **Προσωπικά μηνύματα.**

Σε πολλές ευρωπαϊκές χώρες, όπου τα συστήματα πληρωμών είναι περισσότερο ανεπτυγμένα και τυποποιημένα, ο προσανατολισμός των τραπεζών στρέφεται σταδιακά στην παροχή πρόσθετων υπηρεσιών προς τις επιχειρήσεις (corporate sites), πεδίο στο οποίο η γκάμα των επιλογών είναι ιδιαίτερα διευρυμένη.

Σύμφωνα με έρευνες, όλο και περισσότεροι ιδιώτες αλλά και επιχειρήσεις στην Ελλάδα προτιμούν να διεκπεραιώνουν τις τραπεζικές τους συναλλαγές μέσω Διαδικτύου. Τα αποτελέσματα της Εθνικής Έρευνας για τις Νέες Τεχνολογίες και την Κοινωνία της Πληροφορίας δείχνουν ότι το 2001 περίπου 150.000 πελάτες (1%-1,5% του πληθυσμού) πραγματοποίησαν τραπεζικές συναλλαγές ηλεκτρονικά. Το 2002 ο αριθμός αυτός ξεπέρασε τους 250.000 (2,5% του συνολικού πληθυσμού). Σύμφωνα με εκτιμήσεις τραπεζών, το 2001 ο τζίρος

από online τραπεζικές συναλλαγές έφθασε
τα 2 δισ. ευρώ. Το 2002 το ποσό αυτό εκτιμάται ότι αυξήθηκε σε 10 δισ. ευρώ, ενώ για φέτος αναμένεται ναυπερβεί τα 12 δισεκατομμύρια.

Σύμφωνα με στοιχεία της Τράπεζας Πειραιώς, οι συναλλαγές μέσω Winbank Internet παρουσιάζουν ραγδαία ανάπτυξη: το 2003 οι εγχρήματες συναλλαγές αυξάνονται με ρυθμό της τάξεως του 150% έναντι του 2002. Επίσης, το 50% όλων των πληρωμών ΙΚΑ πραγματοποιείται online, ενώ οι ηλεκτρονικές χρηματιστηριακές συναλλαγές υπερβαίνουν το 15% επί του συνόλου.

Η εξάπλωση του e-banking είναι ραγδαία σε όλο τον κόσμο. Ειδικοί εκτιμούν ότι στο οι σύγχρονες τράπεζες θα δραστηριοποιούνται αποκλειστικά μέσω των νέων τεχνολογιών. Ενδεικτικά, στη Γερμανία το 42% του πληθυσμού χρησιμοποιεί τις υπηρεσίες e-banking, στη Σουηδία το 28%, στη Βρετανία το 7%.

E-banking και Διαδικτυακό Έγκλημα

Παρά τις εξελιγμένες μεθόδους για τη διασφάλιση των τραπεζικών συναλλαγών, η συχνότητα των ηλεκτρονικών επιθέσεων αυξάνεται τα τελευταία χρόνια. Η αύξηση αυτή προκαλεί ανησυχία στους ειδικούς, καθώς διακυβεύονται τεράστια ποσά, ειδικά στις περιπτώσεις κατά τις οποίες θύματα απάτης γίνονται επιχειρήσεις.

Οι επίδοξοι εισβολείς έχουν πολλούς τρόπους για να επιτύχουν τους σκοπούς τους. Οι μεγαλύτεροι κίνδυνοι δεν προέρχονται από ατέλειες των συστημάτων ασφαλείας και κρυπτογράφησης αλλά από τον ανθρώπινο παράγοντα. Έρευνες ειδικών σε θέματα ασφάλειας αποδεικνύουν ότι στις περισσότερες περιπτώσεις επιθέσεων, οι εισβολείς είτε είχαν την ακούσια -συνήθως- βοήθεια και κάποιου που εργαζόταν στην τράπεζα, είτε υπέκλεψαν κωδικούς χρηστών. Οι επιχειρήσεις-πελάτες είναι συνήθως προσεκτικές και χρησιμοποιούν συστήματα ασφαλείας στα δίκτυά τους. Την ίδια "σοφία" ή προσοχή δεν δείχνουν και οι ιδιώτες πελάτες, οι περισσότεροι από τους οποίους δεν χρησιμοποιούν λογισμικό για ασφάλεια. Οι απλοί χρήστες γίνονται εύκολα θύματα προγραμμάτων που στην πραγματικότητα ανοίγουν "τρύπες" ασφάλειας στο σύστημα επιτρέποντας σε επιτήδειους να έχουν πρόσβαση σε αυτό. Ωστόσο και οι επιχειρήσεις δεν είναι πάντοτε ασφαλείς. Σε ορισμένες περιπτώσεις, εταιρίες συνεργάζονται με τράπεζες προκειμένου να διαχειριστούν τις πληρωμές των λογαριασμών και τις συναλλαγές με εταιρικούς πελάτες. Οι τράπεζες ενίοτε επιτρέπουν στις εταιρίες αυτές να διαχειρίζονται ολόκληρο το δίκτυό τους. Σε αυτήν την περίπτωση, οι επιτήδειοι μελετούν τον τρόπο με τον οποίο οι επιχειρήσεις επεξεργάζονται τις πληρωμές και μεταφέρουν τα χρήματα. Μόλις βρεθεί μια αδυναμία, μεταφέρουν με λίγες απλές κινήσεις ολόκληρους εταιρικούς λογαριασμούς στις προσωπικές τους θυρίδες. Να σημειωθεί, πάντως, πως η πρακτική αυτή, η διαχείριση δηλαδή τραπεζικού δικτύου από εταιρικό πελάτη, δεν συνηθίζεται στην Ελλάδα. Εξάλλου μέχρι σήμερα δεν έχουν δει το φως της δημοσιότητας περιπτώσεις απάτης στον τομέα του ελληνικού e-banking.

Εθνική Τράπεζα

Η Εθνική Τράπεζα παρέχει στους πελάτες της (φυσικά ή νομικά πρόσωπα) υπηρεσίες e-banking, καλύπτοντας τραπεζικές και χρηματιστηριακές συναλλαγές μέσω Διαδικτύου από το σπίτι ή το γραφείο, με ταχύτητα και ασφάλεια, με στόχο την εξοικονόμηση πολύτιμου προσωπικού χρόνου.
Το Internet Banking της Εθνικής Τράπεζας παρέχει τη δυνατότητα ενημέρωσης για το υπόλοιπο και την κίνηση των λογαριασμών (ημερήσια - μηνιαία ανάλυση).

Τράπεζα Εγνατίας

Η Εγνατία Τράπεζα παρέχει στους πελάτες της επτά υπηρεσίες e-banking. Πρόκειται για:

- Την Egnatia Payment, η οποία προσφέρει τη δυνατότητα σε εταιρίες να διεκπεραιώνουν αυτόματα τη μισθοδοσία του προσωπικού τους ή να εκτελούν οποιαδήποτε άλλη εντολή πληρωμής προς τρίτους μέσω Διαδικτύου,

- Την υπηρεσία egnatiaTeller, η οποία απευθύνεται σε ιδιώτες και επιχειρήσεις, παρέχοντάς τους τη δυνατότητα διενέργειας τραπεζικών συναλλαγών μέσω Internet,

- Την υπηρεσία egnatiaTrader, η οποία απευθύνεται σε ιδιώτες και εταιρίες δίνοντας τους την δυνατότητα εκτέλεσης χρηματιστηριακών συναλλαγών και χρηματιστηριακής ενημέρωσης μέσω Internet,

- Την υπηρεσία webFunds, η οποία προσφέρει την δυνατότητα σε εταιρίες και ιδιώτες, διάθεσης και εξαγοράς Α/Κ μέσω του Διαδικτύου,

- Τις υπηρεσίες WebShop και egnatia Prepay, οι οποίες απευθύνονται σε εταιρίες που προσφέρουν προϊόντα και υπηρεσίες στους πελάτες τους μέσω Internet, και

- Την υπηρεσία webticket, που δίνει την δυνατότητα σε εταιρίες που δραστηριοποιούνται στον χώρο του θεάματος γενικότερα, να διαθέτουν εισιτήρια για εκδηλώσεις και παραστάσεις τους μέσω του Διαδικτύου.

Winbank, Τράπεζα Πειραιώς

Η Winbank εφαρμόζει δύο προγράμματα e-banking, αυτό που προορίζεται για ιδιώτες (Winbank Internet Personal) και αυτό που αφορά στις επιχειρήσεις (Winbank Internet Business).

Citibank-Online

Μέσω της υπηρεσίας Citibank Online, οι πελάτες μπορούν να ελέγξουν το υπόλοιπο και τις πρόσφατες κινήσεις στους λογαριασμούς τους, να εκτελέσουν μεταφορές μεταξύ των λογαριασμών τους αλλά και καταθέσεις σε λογαριασμούς άλλων πελατών της Citibank στην Ελλάδα ή και το εξωτερικό, καθώς και να πληρώσουν τις κάρτες τους Citibank Visa και Diners Club.

Η διαδικασία ενεργοποίησης της Citibank Online γίνεται μέσω μιας απλής αίτησης που διατίθεται στο Διαδίκτυο και στα καταστήματα της Citibank. Μόλις η αίτηση γίνει δεκτή, η πρόσβαση στην υπηρεσία Citibank Online γίνεται με τον αριθμό της κάρτας Citibank Card και τον κωδικό του ATM, απαλλάσσοντας έτσι το χρήστη από την απομνημόνευση πολλών κωδικών.

Alpha Web Banking

Η Alpha Bank προσφέρει τη δυνατότητα στους πελάτες της να εκτελούν, εντελώς δωρεάν, τραπεζικές συναλλαγές μέσω Internet 24 ώρες το 24ωρο. Ο συνδρομητής μπορεί να παρακολουθεί τα υπόλοιπα των καταθετικών λογαριασμών, των στεγαστικών δανείων, των ανοικτών προσωπικών δανείων και των πιστωτικών καρτών, να πραγματοποιεί μεταφορές κεφαλαίων και πληρωμές οφειλών σε τρίτους, να πληροφορείται για τιμές συναλλάγματος και μετοχών κ.λ.π. μέσω του Alpha Web Banking.

Eurobank

Η EFG Eurobank, μέσω της εταιρίας του ομίλου EFG e-Solutions, έχει αρχίσει από το 2001 να δραστηριοποιείται στον τομέα των ηλεκτρονικών εφαρμογών υψηλής τεχνολογίας για εναλλακτικά δίκτυα διανομής (e-banking, m-banking).

Πέρα από τις υπηρεσίες για τους ιδιώτες πελάτες της, η Eurobank παρέχει στους εταιρικούς πελάτες τη δυνατότητα πλήρους απεικόνισης των φυσικών διαδικασιών κάθε εταιρίας στον ηλεκτρονικό κόσμο. Κάθε επιχείρηση μπορεί να ορίσει απεριόριστο αριθμό χρηστών που έχουν το δικαίωμα να εκτελούν συναλλαγές, με πολλαπλά επίπεδα έγκρισης και διαφορετικά δικαιώματα ανά χρήστη.

Η Eurobank δημιούργησε έναν πλήρη δικτυακό τόπο, από όπου μπορεί κανείς να πραγματοποιήσει πληθώρα συναλλαγών, αλλά και να συμμετέχει ενεργά στο Χρηματιστήριο με online αγοραπωλησίες. Αξίζει να σημειωθεί ότι η Eurobank δεν υποχρεώνει τον πελάτη να επισκεφθεί κάποιο υποκατάστημα για να υποβάλει τη σχετική αίτηση.

NovaWeb της NovaBank

Η NovaBank δημιούργησε το NovaWeb, το δίκτυο εξυπηρέτησης μέσω του οποίου μπορεί να πραγματοποιηθεί κάθε συναλλαγή ηλεκτρονικά. Ειδικότερα οι συναλλαγές του e-banking που προσφέρει η NovaBank χωρίζονται σε δύο κατηγορίες, στο NovaBanker και το NovaInvestor.

Internet Banking από την Τράπεζα Κύπρου

Η χρήση του Internet Banking εξασφαλίζει στους πελάτες της Τράπεζας Κύπρου ταχύτητα και ευκολία στις καθημερινές τους συναλλαγές. Επεκτείνει, επίσης, τα χρονικά όρια συναλλαγών, καθώς οι πελάτες έχουν πρόσβαση στους λογαριασμούς τους όλο το 24ωρο. Καλύπτει μια γεωγραφικά ευρύτερη περιοχή, τόσο της Ελλάδας όσο και του εξωτερικού, και προσφέρεται χωρίς επιπρόσθετη χρέωση.

Emporiki e. Banking

Η Εμπορική Τράπεζα, μέσω της υπηρεσίας Emporiki e.Banking, καθιστά δυνατή την πραγματοποίηση συναλλαγών όλο το 24ωρο, 7 ημέρες την εβδομάδα, εύκολα και χωρίς πρόσθετο κόστος συναλλαγής. Η τράπεζα εγγυάται την ασφάλεια των συναλλαγών χρησιμοποιώντας την πιστοποίηση της VeriSign. Η εφαρμογή Emporiki e.Banking καλύπτει ένα ευρύ φάσμα αναγκών των ιδιωτών, των επαγγελματιών και των επιχειρήσεων. Ιδιαίτερα για τις επιχειρήσεις, προσφέρεται η δυνατότητα πρόσβασης σε πολλαπλούς εκπροσώπους με διαφορετικά δικαιώματα πρόσβασης και διαχείρισης.

Τραπεζικές Συναλλαγές μέσω κινητού τηλεφώνου: Η εφαρμογή της υπηρεσίας σήμερα στην Ελλάδα

"Το m-banking, σύντμηση του mobile banking, επιτρέπει τη διαχείριση τραπεζικών λογαριασμών από το κινητό τηλέφωνο. Παρέχει τη δυνατότητα για άμεση πληροφόρηση για την κίνηση ενός λογαριασμού, 24 ώρες το 24ωρο και, ανάλογα με τον τρόπο που έχει σχεδιάσει η τράπεζα την υπηρεσία της, την άμεση διενέργεια συναλλαγών."
Με τη συγκεκριμένη υπηρεσία μπορούν να πραγματοποιηθούν τραπεζικές αλλά και χρηματιστηριακές συναλλαγές μέσω κινητού τηλεφώνου, από όπου και αν βρίσκεται ο πελάτης. Οι τράπεζες που προσφέρουν την εν λόγω υπηρεσία συνεργάζονται με συγκεκριμένους παροχής τηλεπικοινωνιακών υπηρεσιών. Σημειώνεται ότι η υπηρεσία δεν προσφέρεται δωρεάν, καθώς χρεώνεται ο λογαριασμός του κινητού τηλεφώνου για κάθε συναλλαγή που πραγματοποιείται. Όλες οι συναλλαγές γίνονται μέσω γραπτών μηνυμάτων (SMS). Η αποδεικτική αξία των ηλεκτρονικών εντολών είναι ίδια με αυτή των εγγράφων και οι συναλλαγές γίνονται μόνο απότο προσωπικό κινητό τηλέφωνο του χρήστη.

Η ασφάλεια των συναλλαγών μέσω της υπηρεσίας m-banking εξασφαλίζεται χάρη στα συστήματα ασφάλειας και κρυπτογράφησης που χρησιμοποιούνται από τον τηλεπικοινωνιακό οργανισμό κινητής τηλεφωνίας που έχει επιλέξει ο χρήστης.

Παροχή Υπηρεσιών μέσω κινητού τηλεφώνου

Οι υπηρεσίες στις οποίες έχουν πρόσβαση οι πελάτες μέσω κινητού τηλεφώνου είναι:

- Κατάσταση λογαριασμού,
- Υπόλοιπα και μεταφορές χρημάτων μεταξύ λογαριασμών της ίδιας τράπεζας,
- Παραγγελία για πλήρη statements,
- Αγορά και πώληση μετοχών,
- Ενημέρωση εντός ολίγων λεπτών για εκτέλεση εντολής,
- Ενημέρωση σε πραγματικό χρόνο (real time) για την τιμή της μετοχής προς αγορά ή πώληση,
- Παρακολούθηση και αποτίμηση χαρτοφυλακίου,

- Αναλυτική πληροφόρηση για πραγματοποιούμενες κινήσεις στο χαρτοφυλάκιο,
- Πληροφορίες και διαφημιστικά μηνύματα για υπηρεσίες, προϊόντα και προσφορές της τράπεζας,
- Αλλαγή του απόρρητου κωδικού PIN,
- Προσωπικά μηνύματα,
- Αναφορά για απώλεια κάρτας

Παρά τα πλεονεκτήματα, τις ευκολίες και την ευχρηστία του, το m-banking δεν έχει καταφέρει ακόμη να πείσει το ελληνικό καταναλωτικό κοινό. Αυτό οφείλεται ενδεχομένως στη χρήση του κινητού ως κατεξοχήν μέσου επικοινωνίας, συνεπώς η αποδοχή της αξιοπιστίας του ως μέσου διεξαγωγής χρηματοοικονομικών συναλλαγών δεν είναι εύκολη. Οι Έλληνες χρήστες και οι επιχειρήσεις δείχνουν να εμπιστεύονται περισσότερο το Internet, γεγονός που εξηγεί τα μεγαλύτερα ποσοστά διείσδυσης του e-banking έναντι του m-banking.

Ωστόσο, με αργούς αλλά σταθερούς ρυθμούς τα πράγματα αλλάζουν. Οι επιχειρήσεις, και ειδικότερα οι μικρομεσαίες, αλλά και οι ιδιώτες έχουν αρχίσει να αντιλαμβάνονται ότι οι υπηρεσίες mobile banking αποφέρουν κέρδος σε πολύτιμο χρόνο και, κατά συνέπεια, χρήμα.

Από έρευνες που έχουν πραγματοποιηθεί για λογαριασμό τραπεζών υπολογίζεται ότι το 7% των πελατών τους κάνει σήμερα χρήση του τηλεφώνου για τραπεζικές συναλλαγές. Τα τελευταία στοιχεία που έχουν στη διάθεσή τους οι τράπεζες δείχνουν ότι το 2001 πραγματοποιήθηκαν 100.000 εγχρήματες συναλλαγές μέσω κινητού τηλεφώνου, ενώ ο τζίρος ανήλθε σε 4 δισ. ευρώ. Φέτος οι συναλλαγές αναμένεται να αυξηθούν σε 120.000 και ο τζίρος σε 10 δις. Ευρώ.

Να σημειώσουμε ότι στο δικτυακό τόπο του Lawnet.gr (www.lawnet.gr) παρέχονται συμβουλές νομικής φύσεως στους χρήστες mobile banking.

ΚΕΦΑΛΑΙΟ 2ο

ΚΡΥΠΤΟΓΡΑΦΗΣΗ-ΑΣΦΑΛΕΙΑ

Ασφάλεια Πληροφοριακών Συστημάτων

Εισαγωγικά

Η χρήση των ηλεκτρονικών υπολογιστών (Η/Υ) και η εισαγωγή τους στην καθημερινή εργασία τα τελευταία χρόνια έχει αυξηθεί κατακόρυφα και σε συνδυασμό με τις τεχνολογικές εξελίξεις οι χρήστες απολαμβάνουν την συνεχώς αυξανόμενη υπολογιστική ισχύ που τους παρέχεται τόσο στο σπίτι όσο και στους χώρους εργασίας. Δεν αυξάνεται όμως μόνο η υπολογιστική ισχύ των υπολογιστών αλλά ταυτόχρονα βελτιώνονται και οι υπηρεσίες που παρέχονται μέσω αυτών και κυρίως αυτές που αφορούν την ανταλλαγή πληροφοριών μέσω δικτύων.

Για το σκοπό αυτό έχουν δημιουργηθεί μεγάλα δίκτυα με στόχο την σύνδεση υπολογιστικών συστημάτων. Οι Η/Υ που διασυνδέονται στα δίκτυα αυτά συνήθως ανήκουν είτε σε απλούς ιδιώτες είτε σε εταιρείες ή οργανισμούς που ο καθένας έχει διαφορετική αντίληψη για τα θέματα «Ασφάλειας»των πληροφοριών που διακινούνται. Από την άλλη πλευρά υπάρχουν και διαφορετικές απαιτήσεις σχετικά με την ασφάλεια των υπολογιστών και των πληροφοριακών συστημάτων και κατά συνέπεια είναι πολύ δύσκολο να διατυπωθεί με ακρίβεια η έννοια του «Ασφαλούς Συστήματος».Μια συναφής έννοια με αυτή της ασφάλειας είναι και αυτή της «Αξιοπιστίας». Οι Η/Υ αξιοποιούνται με την εγκατάσταση σε αυτούς και τη χρήση διάφορων εφαρμογών για τη λειτουργία των οποίων απαιτείται υψηλή αξιοπιστία.

Η ασφάλεια των συστημάτων Η/Υ αντιμετωπιζόταν παραδοσιακά μέχρι σήμερα σαν ένα ανεξάρτητο αντικείμενο χωρίς να έχει κάποια κοινή βάση με τα θέματα αξιοπιστίας, ενώ από την άλλη πλευρά η αξιοπιστία των πληροφοριακών συστημάτων αντιμετωπιζόταν χωρίς να δίνεται η απαραίτητη προσοχή σε θέματα ασφάλειας. Οι δύο αυτές περιοχές που αφορούν τα πληροφοριακά συστήματα πρέπει να αποτελούν ένα ολοκληρωμένο συνδυασμό ο οποίος με τη σειρά του πρέπει να συμπεριλαμβάνεται στο σχεδιασμό των σύγχρονων συστημάτων. Η ορθή προσέγγιση των θεμάτων ασφάλειας για ένα πληροφοριακό σύστημα ενδυναμώνει τη λειτουργικότητά του και ενισχύει στους χρήστες του το αίσθημα της εμπιστοσύνης.

Η ενασχόληση με θέματα ασφάλειας πληροφοριακών συστημάτων και μεθόδους εφαρμογής κατάλληλων κανόνων προϋποθέτει μια κοινή οπτική και από τις δύο πλευρές (του μελετητή και του φορέα). Για το λόγο αυτό απαιτείται στην παρούσα φάση η ταξινόμηση των εννοιών που χρειάζεται να γνωρίζει κάποιος σε συνδυασμό

με την ορολογία για να εκτιμήσει την ανάλυση και σχεδίαση ενός ασφαλούς συστήματος.

Κρυπτογράφηση: Το Α και το Ω της Δικτυακής Ασφάλειας

"Οι σύγχρονες επιχειρηματικές ανάγκες απαιτούν συχνά τη μετάδοση εμπιστευτικών δεδομένων μέσω του Διαδικτύου. Η νέα ψηφιακή κοινωνία οφείλει να παρέχει μηχανισμούς προστασίας του απαραβίαστου του επαγγελματικού απορρήτου. Βασική τεχνολογία στον τομέα της ασφάλειας στο Internet είναι η κρυπτογράφηση."

Σε νομικό και κοινωνικό επίπεδο, τίθεται ζήτημα προστασίας του απορρήτου σε όλες τις εκδοχές δικτυακής συναλλαγής (email, εμπορικές συναλλαγές, τραπεζικό και ιατρικό απόρρητο) και γενικότερα ζήτημα **προστασίας προσωπικών δεδομένων** του κάθε χρήστη του Internet.

Η κρυπτογράφηση έρχεται να εξασφαλίσει το απόρρητο των προσωπικών πληροφοριών. Πρόκειται για μια επιστήμη που βασίζεται στα μαθηματικά για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων. Οι μέθοδοι κρυπτογράφησης καθιστούν τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο από όσους είναι κατάλληλα εξουσιοδοτημένοι. Εξασφαλίζουν έτσι το απόρρητο στις ψηφιακές επικοινωνίες αλλά και στην αποθήκευση ευαίσθητων πληροφοριών. Το αρχικό μήνυμα ονομάζεται απλό κείμενο (plaintext), ενώ το ακατάληπτο μήνυμα που προκύπτει από την κρυπτογράφηση του απλού κειμένου ονομάζεται κρυπτογράφημα (ciphertext).

Αποκρυπτογράφηση είναι η ανάκτηση του απλού κειμένου από το κρυπτογράφημα με την εφαρμογή αντίστροφου αλγορίθμου. Η κρυπτογραφημένη επικοινωνία είναι αποτελεσματική, όταν μόνο τα άτομα που συμμετέχουν σε αυτήν μπορούν να ανακτήσουν το περιεχόμενο του αρχικού μηνύματος. Η κρυπτογραφία δεν πρέπει να συγχέεται με την κρυπτανάλυση, που ορίζεται ως η επιστήμη για την ανάλυση και αποκωδικοποίηση κωδικοποιημένων πληροφοριών χωρίς τη χρήση του αντίστροφου αλγορίθμου κρυπτογράφησης.

Ο αλγόριθμος κρυπτογράφησης είναι μια μαθηματική συνάρτηση που χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση πληροφοριών. Όσο αυξάνεται ο βαθμός πολυπλοκότητας του αλγορίθμου, τόσο μειώνεται η πιθανότητα να τον προσπελάσει κάποιος. Ο αλγόριθμος κρυπτογράφησης λειτουργεί σε συνδυασμό με ένα κλειδί (key), για την κρυπτογράφηση του απλού κειμένου. Το ίδιο απλό κείμενο κωδικοποιείται σε διαφορετικά κρυπτογραφήματα όταν χρησιμοποιούνται διαφορετικά κλειδιά.

Η ανάγκη για εμπιστευτικότητα στις ηλεκτρονικές συναλλαγές ικανοποιείται με την **κρυπτογράφηση**. Ο αποστολέας, χρησιμοποιώντας συγκεκριμένη μαθηματική συνάρτηση, μετατρέπει το αρχικό κείμενο σε μορφή μη κατανοητή για οποιονδήποτε τρίτο (κρυπτογραφημένο κείμενο). Ο παραλήπτης, έχοντας γνώση του τρόπου κρυπτογράφησης, αποκρυπτογραφεί το κείμενο στην αρχική του μορφή. Το μήνυμα παραμένει εμπιστευτικό, ωσότου αποκρυπτογραφηθεί.

Οι διάφορες μέθοδοι κρυπτογράφησης βασίζονται στη χρήση ενός "κλειδιού", ενός μαθηματικού δηλαδή κώδικα - αλγόριθμου, ο οποίος διασφαλίζει το μη "αναγνώσιμο" από τρίτους, και χρησιμοποιείται στην κρυπτογράφηση και την αποκρυπτογράφηση. Κάθε αλγόριθμος παίρνει την ονομασία του από τον αριθμό που μεταλλάσσεται και πρέπει να βρεθεί με μία σειρά μαθηματικών πράξεων.

Αρχικά το κλειδί κρυπτογράφησης ήταν το ίδιο με το κλειδί αποκρυπτογράφησης, δηλαδή αποστολέας και παραλήπτης χρησιμοποιούσαν το ίδιο συμμετρικό κρυπτογραφικό σύστημα (symmetric cryptosystem). Το σύστημα αυτό χρησιμοποιήθηκε κυρίως σε κλειστά συστήματα και εφαρμόστηκε τη δεκαετία του '80 για τη μεταφορά τραπεζικών δεδομένων. Αργότερα η εξέλιξη οδήγησε στη χρησιμοποίηση δύο κλειδιών, ενός ιδιωτικού και ενός δημόσιου (ασύμμετρο κρυπτογραφικό σύστημα - asymmetric or public key cryptosystem). Το ιδιωτικό κλειδί (private key) χρησιμοποιείται για το σφράγισμα του ηλεκτρονικού μηνύματος και είναι απόρρητο, ενώ το δημόσιο κλειδί (public key) αντιστοιχεί στο πρώτο, χρησιμοποιείται για την αποσφράγιση του μηνύματος και δεν είναι απόρρητο. Συνεπώς, το πρώτο κλειδί το γνωρίζει μόνο ο αποστολέας και μόνο με αυτό μπορεί κανείς να επέμβει στο κείμενο, ενώ το δεύτερο το γνωστοποιεί σε κάθε συναλλασσόμενο του για να μπορεί να αποκρυπτογραφεί/ διαβάζει τα μηνύματα του πρώτου.

Γιατί πρέπει να χρησιμοποιείται

Δεν είναι λίγοι αυτοί που πιστεύουν ότι η χρήση κρυπτογραφικών εργαλείων αφορά μόνο... κατασκόπους ή μανιώδεις χρήστες υπολογιστών. Στην πραγματικότητα, όταν κάποιος αποστέλλει ένα προσωπικό e-mail ή ανταλλάσσει εμπιστευτικές εμπορικές πληροφορίες για ένα έργο μέσω του ηλεκτρονικού ταχυδρομείου, οφείλει να γνωρίζει ότι, εάν δεν έχει κρυπτογραφηθεί, είναι σαν να το στέλνει με card-postal: μπορεί να το διαβάσει σχεδόν οποιοσδήποτε.

Ένα e-mail, εκτός από τον αποστολέα και τον παραλήπτη, μπορεί να διαβαστεί εύκολα και από τους εργαζόμενους στον ISP (εταιρία παροχής Internet) του αποστολέα, τους εργαζόμενους στον ISP του παραλήπτη, από οποιονδήποτε ελέγχει τους routers από τους οποίους θα περάσουν τα "πακέτα" του μηνύματος και από στην

οποιονδήποτε έχει πρόσβαση στον εξοπλισμό τηλεφωνίας τηλεφωνική εταιρία.
Αν το μήνυμα αποστέλλεται ή παραλαμβάνεται από κινητό τηλέφωνο με σύνδεση στο Διαδίκτυο, τότε μπορεί να υποκλαπεί από άτομα με ειδικές συσκευές υποκλοπής συνομιλιών και μηνυμάτων κινητής τηλεφωνίας. Επιπλέον, είναι πολύ απλό να πλαστογραφηθεί η διεύθυνση αποστολής, ακόμα και με ένα τυπικό πρόγραμμα e-mail. Με λίγο περισσότερη δουλειά, κάποιος επιτήδειος μπορεί να αποκρύψει και άλλα σημάδια που δείχνουν από πού πραγματικά προέρχεται ένα μήνυμα.

Λύση στα παραπάνω προβλήματα δίνουν οι τεχνολογίες κρυπτογράφησης. Οι τεχνολογίες αυτές εξασφαλίζουν ότι το μήνυμα θα μπορεί να το διαβάσει μόνο ο παραλήπτης του, καθώς στα ενδιάμεσα στάδια το μήνυμα εμφανίζεται με ακατάληπτους χαρακτήρες, είναι δηλαδή μη αναγνώσιμο. Εκτός από την κρυπτογράφηση, μια άλλη τεχνολογία που παρέχει τέτοιου είδους ασφάλεια είναι η ηλεκτρονική υπογραφή, τομέας με τον οποίο έχουμε ήδη ασχοληθεί.

Αξίζει, πάντως, να σημειώσουμε ότι είναι δυνατόν ένα μήνυμα να κρυπτογραφηθεί και ταυτόχρονα να υπογραφεί ηλεκτρονικά. Έτσι εξασφαλίζονται εξίσου η ασφάλεια στην επικοινωνία και η πιστοποίηση περιεχομένου και ταυτότητας αποστολέα.

Δημόσιο Κλειδί

Στην ηλεκτρονική υπογραφή ακολουθείται το σύστημα της ασύμμετρης κρυπτογράφησης (δημόσιο κλειδί). Ακόμα κι αν γνωρίζει κάποιος το ένα κλειδί, είναι πρακτικά αδύνατον να υπολογίσει το άλλο. Το ένα κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το άλλο για την επαλήθευσή της. Η διαφοροποίηση από την κρυπτογράφηση έγκειται στο ότι για τη δημιουργία της ηλεκτρονικής υπογραφής ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα.

Στη διαδικασία της δημιουργίας και επαλήθευσης της υπογραφής υπεισέρχεται και η έννοια της συνάρτησης κατακερματισμού (ή κατατεμαχισμού - one way hash). Με την εφαρμογή της συνάρτησης κατακερματισμού, από κάθε μήνυμα -ανεξαρτήτως μεγέθους- παράγεται μια "σύνοψη", η οποία είναι μία σειρά από bits συγκεκριμένου μεγέθους (π.χ. 128 ή 160 bits). Η σύνοψη του μηνύματος (fingerprint ή message digest) αποτελεί ψηφιακή αναπαράσταση του μηνύματος και είναι μοναδική για το μήνυμα που αντιπροσωπεύει.

Η υποδομή Δημόσιου Κλειδιού και η Κρυπτογράφηση στην Πράξη

Η Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure - PKI) αποτελεί ένα συνδυασμό λογισμικού, τεχνολογιών κρυπτογραφίας και υπηρεσιών, ο οποίος πιστοποιεί την εγκυρότητα του κάθε φυσικού προσώπου που εμπλέκεται σε μια συναλλαγή στο Διαδίκτυο, και παράλληλα προστατεύει την ασφάλεια της συναλλαγής.

Το PKI ενσωματώνει ψηφιακά πιστοποιητικά, κρυπτογραφία δημόσιου κλειδιού και αρχές πιστοποίησης σε ένα ασφαλές αρχιτεκτονικό σχήμα. Μια τυπική υλοποίηση του PKI περιλαμβάνει την παροχή ψηφιακών πιστοποιητικών σε χρήστες, εξυπηρετητές (servers) και λογισμικό χρηστών. Παράλληλα προσφέρει σειρά εργαλείων για τη διαχείριση, ανανέωση και ανάκληση των πιστοποιητικών.

Οι βασικές λειτουργίες / υπηρεσίες των Υποδομών Δημόσιου Κλειδιού είναι οι εξής:

Εμπιστευτικότητα (Confidentiality): Πρόκειται για την προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη πρόσβαση ή γνωστοποίησή τους. Η υπηρεσία αυτή υλοποιείται μέσω μηχανισμών ελέγχου πρόσβασης στην περίπτωση αποθήκευσης δεδομένων και μέσω κωδικοποίησης κατά την αποστολή τους. Η Υποδομή Δημόσιου Κλειδιού παρέχει κωδικοποίηση, αφού οι μηχανισμοί ελέγχου πρόσβασης υλοποιούνται κατά βάση από το συνδυασμό μεθόδων πιστοποίησης (authentication) και εξουσιοδότησης (authorization).

Ακεραιότητα (Integrity): Είναι η προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη τροποποίηση ή αντικατάστασή τους. Παρέχεται από μηχανισμούς κρυπτογραφίας όπως οι ηλεκτρονικές υπογραφές Μη Άρνηση Αποδοχής (Non-Repudiation): Η Μη Άρνηση Αποδοχής συνδυάζει τις υπηρεσίες της Πιστοποίησης και της Ακεραιότητας. Ο αποστολέας δεδομένων δεν μπορεί να αρνηθεί ότι δημιούργησε και απέστειλε το μήνυμα. Η ασύμμετρη κρυπτογραφία παρέχει ηλεκτρονικές υπογραφές, κατά συνέπεια μόνο ο αποστολέας του μηνύματος θα μπορούσε να κατέχει τη συγκεκριμένη υπογραφή. Με αυτόν τον τρόπο, ο οποιοσδήποτε, και φυσικά ο παραλήπτης του μηνύματος, μπορεί να επιβεβαιώσει την ηλεκτρονική υπογραφή του αποστολέα. Πιστοποίηση (Authentication): Πρόκειται για την επιβεβαίωση της ταυτότητας ενός ατόμου ή της πηγής αποστολής των πληροφοριών. Κάθε χρήστης που επιθυμεί να επιβεβαιώσει την ταυτότητα ενός άλλου προσώπου ή εξυπηρετητή με τον οποίο επικοινωνεί, βασίζεται στην πιστοποίηση. Οι παραδοσιακές μέθοδοι πιστοποίησης είναι οι εξής:

⇒Με κάποιον κωδικό που γνωρίζουμε, όπως το PIN μιας τραπεζικής κάρτας ή το password ενός λογαριασμού,

⇒Με κάποιο αντικείμενο που έχουμε στην κυριότητά μας, λόγου χάρη το κλειδί μιας πόρτας ή μια τραπεζική κάρτα,

⇒Με βιομετρικά αποτυπώματα, φωνή κ.λπ.

Το πιστοποιητικό (certificate) είναι ο τρόπος με τον οποίο η Υποδομή Δημόσιου Κλειδιού μεταδίδει τις τιμές των δημόσιων κλειδιών ή πληροφορίες που σχετίζονται με αυτά, ή και τα δύο. Η εκδότρια αρχή των πιστοποιητικών ονομάζεται Αρχή Πιστοποίησης (Certificate Authority - CA). Οι Αρχές Πιστοποίησης διασφαλίζουν τη δημοσίευση και τη διανομή των δημόσιων κλειδιών και λαμβάνουν το δημόσιο κλειδί του ενδιαφερόμενου χρήστη. Εάν ο χρήστης ενεργεί στη συγκεκριμένη περίπτωση ως

ιδιώτης, θα πρέπει να παραχωρήσει όλα τα απαραίτητα στοιχεία που αποδεικνύουν την ταυτότητά του. Σε αντίθετη περίπτωση, ο χρήστης θεωρείται ότι ενεργεί εκ μέρους κάποιας επιχείρησης, οπότε οφείλει να παραχωρήσει όλες τις νομικές πληροφορίες που απαιτούνται για την αξιοπιστία και τη νόμιμη λειτουργία της.

Ουσιαστικά ένα ψηφιακό πιστοποιητικό αποτελεί μια ψηφιακά υπογεγραμμένη δήλωση από μια αρχή πιστοποίησης, η οποία:

⇒Προσδιορίζει την αρχή πιστοποίησης που το εξέδωσε,

⇒Περιέχει το όνομα και κάποιες άλλες πληροφορίες του εγγεγραμμένου,

⇒Περιέχει το δημόσιο κλειδί του εγγεγραμμένου, το οποίο είναι ψηφιακά υπογεγραμμένο από την αρχή πιστοποίησης που το εξέδωσε

Για την πιστοποίηση της ταυτότητας των συναλλασσομένων χρησιμοποιούνται τα πιστοποιητικά ασφαλείας, που επιπλέον εγγυώνται και την ασφάλεια ενός δικτυακού τόπου. Υπάρχουν δύο είδη πιστοποιητικών

⇒**Τα προσωπικά πιστοποιητικά:** τα οποία αποτελούν ένα είδος εγγύησης ότι ο χρήστης είναι αυτός που δηλώνει ότι είναι. Σε αυτά καταχωρούνται προσωπικές πληροφορίες, όπως όνομα χρήστη και κωδικός πρόσβασης. Στη συνέχεια, οι πληροφορίες αυτές αποθηκεύονται σε ένα πιστοποιητικό, το οποίο χρησιμοποιείται όταν στέλνονται προσωπικές πληροφορίες σε ένα διακομιστή ελέγχου ταυτότητας που απαιτεί πιστοποιητικό. Επίσης, ένα προσωπικό πιστοποιητικό επιτρέπει στο χρήστη να λαμβάνει κρυπτογραφημένα μηνύματα από τους υπόλοιπους χρήστες.

⇒**Τα πιστοποιητικά δικτυακών τόπων:** τα οποία περιέχουν πληροφορίες που πιστοποιούν ότι η συγκεκριμένη ιστοσελίδα είναι γνήσια και ασφαλής. Αυτό διασφαλίζει ότι κανένα άλλο site δεν μπορεί να παρουσιαστεί με την ταυτότητα της γνήσιας, ασφαλούς τοποθεσίας. Επίσης, τα πιστοποιητικά δικτυακών τόπων χρονολογούνται κατά την έκδοσή τους. Όταν προσπαθείτε να συνδεθείτε με το website ενός οργανισμού, το πρόγραμμα ανάγνωσης επαληθεύει τη διεύθυνση Internet που είναι αποθηκευμένη στο πιστοποιητικό και ελέγχει την ημερομηνία λήξης του. Εάν οι πληροφορίες αυτές δεν είναι έγκυρες ή εάν έχει παρέλθει η ημερομηνία λήξης, εμφανίζεται προειδοποιητικό μήνυμα (Warning).

Έχουν αναπτυχθεί ή βρίσκονται υπό κατασκευή διάφορα πρωτόκολλα ασφαλείας που κάνουν χρήση των παραπάνω τεχνικών, όπως το SSL (Secure Sockets Layer), της Netscape, και το SET (Secure Electronic Transactions), που αναπτύχθηκε από τη Visa και τη MasterCard. Από αυτά σήμερα χρησιμοποιείται το SSL. Αρκετές ιστοσελίδες είναι εξοπλισμένες με προγράμματα που χρησιμοποιούν το πρωτόκολλο αυτό, αποτρέποντας έτσι τα μη εξουσιοδοτημένα πρόσωπα από την πρόσβασή τους σε δεδομένα που αποστέλλονται από και προς αυτές τις ιστοσελίδες. Τέτοια sites ονομάζονται "ασφαλή".

Οι πιο γνωστοί φυλλομετρητές ιστοσελίδων (browsers) υποστηρίζουν το πρωτόκολλο SSL και την κρυπτογράφηση που προσφέρει, ενώ ενημερώνουν το χρήστη ότι βρίσκεται σε ασφαλή τοποθεσία και μπορεί να στέλνει πληροφορίες ακίνδυνα. Με το πρωτόκολλο αυτό οι επικοινωνίες πραγματοποιούνται σε κωδικοποιημένη μορφή και επιπλέον γίνεται έλεγχος της αυθεντικότητας της ιστοσελίδας.

Η διαδικασία μιας ασφαλούς επικοινωνίας έχει ως εξής:

⇒Ο φυλλομετρητής συνδέεται με τον ασφαλή διικτυακό τόπο.

⇒Ο διικτυακός τόπος δηλώνει την ταυτότητά του, η οποία ελέγχεται με τα πιστοποιητικά που εκδίδονται από υπηρεσίες πιστοποίησης.

⇒Η ασφαλής ιστοσελίδα και ο browser συμφωνούν στη χρήση συγκεκριμένου κλειδιού/ αλγορίθμου που χρησιμοποιείται για την κρυπτογράφηση της υπόλοιπης επικοινωνίας.

⇒Τα δεδομένα που διακινούνται είναι κρυπτογραφημένα με το κλειδί/ αλγόριθμο που συμφωνήθηκε στο προηγούμενο βήμα.

Η κρυπτογράφηση γίνεται με χρήση αλγορίθμου 40bit ή 128bit. Εάν έχει χρησιμοποιηθεί κρυπτογράφηση 40bit, τότε για να αποκρυπτογραφήσει κανείς τα δεδομένα που ανταλλάχθηκαν, θα πρέπει να δοκιμάσει περίπου 240 διαφορετικά κλειδιά, ενώ, εάν έχει χρησιμοποιηθεί κρυπτογράφηση 128bit, τότε θα πρέπει να δοκιμάσει περίπου 2.128 διαφορετικά κλειδιά. Με τη χρήση μεγάλης υπολογιστικής ισχύος, η αποκρυπτογράφηση του κλειδιού των 40bit μπορεί να επιτευχθεί σε μερικές ημέρες, ενώ η αποκρυπτογράφηση του κλειδιού των 128bit, με τα σημερινά δεδομένα, είναι πρακτικά αδύνατη. Θα πρέπει να σημειωθεί ότι απαγορεύεται από τη νομοθεσία των ΗΠΑ η εξαγωγή και χρήση προγραμμάτων που υποστηρίζουν κωδικοποίηση 128bit εκτός των Ηνωμένων Πολιτειών και του Καναδά.

Στο πλαίσιο των προσπαθειών που καταβάλλονται για την ανάπτυξη των ηλεκτρονικών συναλλαγών, έχει επιτραπεί η χρήση της τεχνολογίας SGC (Server

Gated Cryptography) ή International Step-Up Encryption, που αποτελεί επέκταση του πρωτοκόλλου SSL, από πιστωτικά ιδρύματα και άλλων χωρών. Η επέκταση αυτή επιτρέπει στα πιστωτικά ιδρύματα, εφόσον διαθέτουν το κατάλληλο πιστοποιητικό, να επικοινωνούν με τους πελάτες τους με κωδικοποίηση 128bit.

PGP (Pretty Good Privacy)

Στην αγορά κυκλοφορούν αρκετά προγράμματα λογισμικού κρυπτογράφησης. Είναι πολύ σημαντικό να γίνεται σωστή επιλογή του προϊόντος που θα χρησιμοποιηθεί. Υπάρχουν προγράμματα που είτε δεν χρησιμοποιούν αρκετά ασφαλείς αλγόριθμους είτε δημιουργούν σφάλματα (bugs) στην υλοποίηση της κρυπτογράφησης. Επίσης, θα πρέπει η τεχνική κρυπτογράφησης να ελέγχεται από ειδικούς, ενώ οι μέθοδοι πρέπει να είναι γνωστές και το λογισμικό που τις υλοποιεί υψηλής ποιότητας.

Για την κρυπτογράφηση ηλεκτρονικού ταχυδρομείου και αρχείων, δημοφιλέστερο πρόγραμμα είναι το PGP (Pretty Good Privacy). Οι αλγόριθμοι του PGP είναι γνωστοί και ασφαλείς. Ο πηγαίος κώδικάς του είναι διαθέσιμος στο κοινό, γεγονός που επέτρεψε σε ειδικούς επιστήμονες των κλάδων της πληροφορικής και της κρυπτογραφίας να το εξετάσουν και να αναζητήσουν σφάλματα ή "κερκόπορτες" (back doors). Χρησιμοποιείται εδώ και αρκετά χρόνια, και οι ειδικοί της κρυπτογραφίας το θεωρούν σε μεγάλο βαθμό αξιόπιστο.

Το PGP αποτελεί ένα κρυπτοσύστημα που δημιουργήθηκε από τον καθηγητή Philip Zimmerman του MIT και χρησιμοποιεί τους αλγόριθμους για την κρυπτογράφηση και υπογραφή μηνυμάτων ηλεκτρονικού ταχυδρομείου. Όταν κυκλοφόρησε για πρώτη φορά, η αμερικανική κυβέρνηση προσπάθησε να απαγορεύσει τη διανομή του, με τη δικαιολογία ότι η υψηλής ποιότητας κρυπτογράφηση συμπεριλαμβάνεται στα όπλα, και η κυβέρνηση έχει δικαίωμα να περιορίσει την χρήση της.

Πρόκειται βέβαια για εμπορικό πρόγραμμα, μπορεί ωστόσο να χρησιμοποιηθεί χωρίς χρέωση για μη επαγγελματική χρήση. Επίσης υπάρχουν και εκδόσεις open source/free software (λογισμικό ανοιχτού/ ελεύθερου κώδικα και δωρεάν διανομής), όπως το gnup gp. Το PGP ήταν αρχικά διαθέσιμο από την PGP Inc. Η εταιρία εξαγοράστηκε από τη Network Associates, η οποία ανέλαβε την εξέλιξη και τις αναβαθμίσεις του προγράμματος. Στις αρχές του 2002 η Network Associates ανακοίνωσε ότι θα σταματήσει την πώληση και υποστήριξη του PGP. Αργότερα, όμως, αποφασίσθηκε η επανασύσταση της PGP Corporation, η οποία αναπτύσσει τη νέα έκδοση (8.0) του προγράμματος και θα αναλάβει την υποστήριξή του.

Ο χρήστης προγραμμάτων τύπου PGP πρέπει αρχικά να δημιουργήσει ένα ζευγάρι κλειδιών (key pair), δημόσιο και ιδιωτικό. Παρέχει το δημόσιο κλειδί σε όλους τους παραλήπτες είτε με e-mail είτε δημοσιεύοντάς το στο Internet. Το ιδιωτικό κλειδί παραμένει κρυφό, στο σταθμό εργασίας του χρήστη, και δεν θα πρέπει να διαρρεύσει, καθώς εξασφαλίζει την αποτελεσματικότητα της κρυπτογράφησης.

Ο αποστολέας κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί. Αυτή είναι μια μονόδρομη διαδικασία: αφού κρυπτογραφηθεί το μήνυμα, δεν μπορεί να αποκρυπτογραφηθεί παρά μόνο με το ιδιωτικό κλειδί. Για το λόγο αυτό, είναι σημαντικό να μη διαρρεύσει. Επειδή και το ιδιωτικό και το δημόσιο κλειδί μπορεί να αποτελούν αρκετά μεγάλα σε όγκο αρχεία, το πρόγραμμα PGP αποθηκεύει το ιδιωτικό κλειδί στο δίσκο κρυπτογραφημένο. Κάθε φορά που ο χρήστης θέλει να το χρησιμοποιήσει, πρέπει να εισάγει την "pass phrase", κωδικό που δεν αποθηκεύεται πουθενά αλλά έχει ο ίδιος απομνημονεύσει.

Κάθε χρήστης του PGP διατηρεί λίστα με τα δημόσια κλειδιά των χρηστών με τους οποίους επικοινωνεί (keyring). Για την προστασία της λίστας, την υπογράφει ο ίδιος με το ιδιωτικό του κλειδί. Κάθε κλειδί που προστίθεται στη λίστα είναι δυνατόν να φέρει έναν από τους παρακάτω χαρακτηρισμούς

⇒Απολύτως Έμπιστο (Completely Trusted)

⇒Μερικώς Έμπιστο (Marginally Trusted)

⇒Μη Έμπιστο (Untrusted)

⇒Άγνωστο (Unknown)

Πάντως, αν και το PGP είναι σε μεγάλο βαθμό αξιόπιστο για εφαρμογές απλής ταυτοποίησης που εκτελούνται από απλούς χρήστες, δεν θεωρείται κατάλληλο για εφαρμογές ηλεκτρονικού εμπορίου και για όσες απαιτούν ισχυρή ταυτοποίηση.

Τα πιστοποιητικά του PGP δεν είναι επεκτάσιμα και περιέχουν μόνο μία διεύθυνση ηλεκτρονικής αλληλογραφίας, την τιμή ενός δημόσιου κλειδιού και ένα χαρακτηρισμό βαθμού εμπιστοσύνης.

Καθώς η διεύθυνση ηλεκτρονικής αλληλογραφίας δεν μπορεί να αποτελέσει ασφαλές μέσο προσδιορισμού της ταυτότητας ενός χρήστη, το PGP δεν μπορεί να παράσχει ισχυρή ταυτοποίηση (strong authentication). Η έλλειψη επεκτασιμότητας των πιστοποιητικών του PGP τα καθιστά ακατάλληλα για άλλες εφαρμογές εκτός της ηλεκτρονικής αλληλογραφίας. Επίσης, το συγκεκριμένο πρόγραμμα δεν υποστηρίζει μεθόδους επαλήθευσης και ανάκλησης των πιστοποιητικών. Οι διαδικασίες αυτές διεξάγονται αποκλειστικά με άμεση επικοινωνία των χρηστών. Επιπλέον, δεν παρέχει την επιλογή της ανωνυμίας, καθώς η χρήση μιας διεύθυνσης e-mail που δεν περιέχει κάποια ένδειξη για την ταυτότητα του χρήστη καθιστά αδύνατη την επικοινωνία μεταξύ των χρηστών για την επαλήθευση και ανάκληση των πιστοποιητικών.

X.509

Το X.509 είναι ένα πρότυπο κρυπτογράφησης το οποίο σχεδιάστηκε για να παρέχει την υποδομή πιστοποίησης στις υπηρεσίες καταλόγου X.500 (LDAP). Το πρωτόκολλο X.500 αποτελεί μια ιεραρχική μέθοδο οργάνωσης ευρετηρίων (καταλόγων), η οποία σχεδιάστηκε από το Διεθνή Οργανισμό Τυποποίησης (International Standards Organization - ISO) και ενσωματώθηκε στο διαδικτυακό πρωτόκολλο LDAP (Lightweight Directory Access Protocol).

Η πρώτη έκδοση του X.509 δημοσιεύθηκε το 1988, καθιστώντας το την παλαιότερη πρόταση για μια παγκόσμια Υποδομή Δημόσιου Κλειδιού. Το γεγονός αυτό, σε συνδυασμό με την υποστήριξη του προτύπου από τον ISO και τη Διεθνή Ένωση Τηλεπικοινωνιών (International Telecommunications Union - ITU), έχουν οδηγήσει στην υιοθέτηση του X.509 από μεγάλο αριθμό οργανισμών και κατασκευαστών. Αρκετά χρηματοπιστωτικά ιδρύματα χρησιμοποιούν το X.509 για το πρότυπο ασφαλών συναλλαγών SET (Secure Electronic Transactions). Χρησιμοποιείται επίσης σε φυλλομετρητές ιστοσελίδων (browsers), εξυπηρετητές (servers) και προγράμματα λογισμικού, για τη διαχείριση του ηλεκτρονικού ταχυδρομείου (mail server/clients) κτλ., από πολλές γνωστές εταιρίες ανάπτυξης λογισμικού.

Τι είναι η Ηλεκτρονική Υπογραφή

Ως ηλεκτρονική υπογραφή, λοιπόν, νοείται κάθε "κλειδωμένη" σύντμηση ηλεκτρονικού κειμένου, η οποία παρέχει εγγύηση της αυθεντικότητας και της μη αλλοίωσής του. Έχει επιβεβαιωτική λειτουργία (ο παραλήπτης είναι βέβαιος ότι το μήνυμα που παραλαμβάνει ανήκει στον αποστολέα χωρίς αλλοιώσεις) και εμπιστευτική λειτουργία (μόνο ο παραλήπτης μπορεί να διαβάσει το μήνυμα).

Το ελληνικό Δίκαιο με ειδική πρόβλεψη (**Ν. 2672/1999**) προτείνει τον όρο "ψηφιακή υπογραφή" αντί για "ηλεκτρονική", και δίνει τον ορισμό της: "Η ψηφιακής μορφής υπογραφή σε δεδομένα ή λογικά συνεχιζόμενη με αυτά, που χρησιμοποιείται από τον υπογράφοντα ως ένδειξη υπογραφής του περιεχομένου των δεδομένων αυτών, εφόσον η εν λόγω υπογραφή α) συνδέεται μονοσήμαντα με τον υπογράφοντα, β) ταυτοποιεί τον υπογράφοντα, γ) δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον έλεγχό του και δ) συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο ώστε να μπορεί να αποκαλυφθεί οποιαδήποτε αλλοίωση των εν λόγω δεδομένων". Παρά τον ορισμό αυτό, ο εν λόγω νόμος δεν εξομοιώνει νομικά τη ψηφιακή υπογραφή με την ιδιόχειρη, κενό το οποίο ήρθε να καλύψει το **Προεδρικό Διάταγμα 150/2001**.

Δημιουργία και Επαλήθευση Ηλεκτρονικής Υπογραφής.

Όπως ειπώθηκε παραπάνω, η χρήση της ηλεκτρονικής υπογραφής περιλαμβάνει δύο στάδια: τη δημιουργία/ μετάδοση και την επαλήθευσή της. Παρακάτω περιγράφονται οι ενέργειες του αποστολέα και του παραλήπτη, ώστε να γίνει κατανοητός ο μηχανισμός της δημιουργίας και επαλήθευσης της ψηφιακής υπογραφής:

Αποστολέας

⇒ Δημιουργεί τη σύνοψη του μηνύματος (message digest) που θέλει να στείλει χρησιμοποιώντας κάποιον αλγόριθμο κατακερματισμού (one way hash). Ανεξάρτητα από το μέγεθος του μηνύματος, αυτό που θα παραχθεί θα είναι μία συγκεκριμένου μήκους σειρά ψηφίων.

⇒ Με το ιδιωτικό του κλειδί κρυπτογραφεί τη σύνοψη. Αυτό που παράγεται είναι η ψηφιακή υπογραφή. Η υπογραφή είναι ουσιαστικά μία σειρά ψηφίων συγκεκριμένου πλήθους.

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

Παραλήπτης

⇒ Ο παραλήπτης αποσπά από το μήνυμα την ψηφιακή υπογραφή (κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα).

⇒ Εφαρμόζοντας στο μήνυμα που έλαβε τον ίδιο αλγόριθμο κατακερματισμού, ο παραλήπτης δημιουργεί τη σύνοψη του μηνύματος.

⇒ Στη συνέχεια, αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα, την κρυπτογραφημένη σύνοψη του μηνύματος (ψηφιακή υπογραφή).

⇒ Συγκρίνονται οι δύο συνόψεις και, αν βρεθούν ίδιες, το μήνυμα που έλαβε ο παραλήπτης είναι ακέραιο. Αν το μήνυμα έχει μεταβληθεί, η σύνοψη που θα παράγει ο παραλήπτης θα είναι διαφορετική από τη σύνοψη που έχει κρυπτογραφηθεί.

Η Ηλεκτρονική Υπογραφή (e-signature) στις Online Συναλλαγές

"Η "νομιμοποίηση" ενός εγγράφου ισοδυναμούσε ανέκαθεν με την υπογραφή που έφερε. Καθώς τα ηλεκτρονικά έγγραφα κάθε είδους τείνουν να αντικαταστήσουν τα "παραδοσιακά" χειρόγραφα, αντίστοιχα και η υπογραφή του συντάκτη γίνεται "εικονική", ηλεκτρονική."

Η ανάπτυξη του Διαδικτύου, το **ηλεκτρονικό εμπόριο** και οι συναλλαγές μέσω ανοιχτών δικτύων καθιστούν επιτακτική την ανάγκη ασφάλειας, η οποία εξαρτάται σε μεγάλο βαθμό από την υπογραφή, την ταυτότητα δηλαδή των συναλλασσομένων. Ο χρήστης που συναλλάσσεται ηλεκτρονικά απαιτεί τα δεδομένα (μήνυμα ή κείμενο) που στέλνει να μην μπορούν να αποκαλυφθούν ή να διατεθούν σε μη εξουσιοδοτημένα άτομα (**εμπιστευτικότητα**). Τα δεδομένα απαγορεύεται να αλλοιωθούν κατά τη μετάδοσή τους. Ο παραλήπτης θα πρέπει να λάβει τα δεδομένα που του στάλθηκαν, χωρίς αυτά να έχουν τροποποιηθεί στο ελάχιστο (**ακεραιότητα**). Σε μια τέτοια συναλλαγή, ο παραλήπτης πρέπει να είναι βέβαιος για την ταυτότητα του αποστολέα (**αυθεντικότητα**). Η συμμετοχή σε μία ηλεκτρονική συναλλαγή προϋποθέτει ότι τα εμπλεκόμενα μέρη δεν έχουν νόμιμο δικαίωμα να αρνηθούν εκ των υστέρων τη συμμετοχή τους στη συναλλαγή αυτή (**μη αποποίηση ευθύνης**).

Η Πιστοποίηση της Ψηφιακής Υπογραφής (Certification)

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

Ο Πάροχος Υπηρεσιών Πιστοποίησης (ΠΥΠ) είναι ο "οργανισμός" που βεβαιώνει με ακρίβεια τη σχέση ενός φυσικού προσώπου με το δημόσιο κλειδί του, με την έκδοση ενός ηλεκτρονικού πιστοποιητικού, στο οποίο ο ΠΥΠ πιστοποιεί την ταυτότητα του προσώπου και το δημόσιο κλειδί του.

Κύριος τύπος ψηφιακών πιστοποιητικών είναι τα πιστοποιητικά δημοσίου κλειδιού (public key certificates). Το πιστοποιητικό αναφέρει το δημόσιο κλειδί και επιβεβαιώνει ότι το συγκεκριμένο πρόσωπο είναι ο δικαιούχος του αντίστοιχου ιδιωτικού κλειδιού. Έτσι ο παραλήπτης που λαμβάνει ένα μήνυμα με ψηφιακή υπογραφή, μπορεί να είναι σίγουρος ότι το μήνυμα έχει σταλεί από το πρόσωπο που το υπογράφει. Το ψηφιακό πιστοποιητικό είναι εν ολίγης ένα διαβατήριο. Η συσχέτιση ενός δημόσιου κλειδιού με τον δικαιούχο του γίνεται με χρήση της ψηφιακής υπογραφής του ΠΥΠ, ο οποίος υπογράφει το πιστοποιητικό του δικαιούχου. Η κατοχή του ψηφιακού πιστοποιητικού διασφαλίζεται από την αποκλειστική κατοχή συγκεκριμένων ψηφιακών δεδομένων (ιδιωτικό κλειδί) από το φυσικό πρόσωπο. Ο ΠΥΠ δημοσιεύει ψηφιακά δεδομένα σχετικά με την επαλήθευση της κατοχής του πιστοποιητικού (δημόσιο κλειδί) και εγγυάται για τα στοιχεί του φυσικού προσώπου.

Η ηλεκτρονική υπογραφή δημιουργείται με βάση τα δεδομένα αποκλειστικής κατοχής (ιδιωτικό κλειδί) και τα προς υπογραφή δεδομένα, και αποτελεί την ψηφιακή τους "ετικέτα". Βασικοί στόχοι είναι:

⇒ Η ταυτοποίηση του υπογράφοντος, δηλαδή η σύνδεση της ηλεκτρονικής συναλλαγής με το φυσικό πρόσωπο που υπογράφει,

⇒ Η εγγύηση της γνησιότητας των ψηφιακών δεδομένων και

⇒ Η δέσμευση του υπογράφοντος ως προς την ηλεκτρονική συναλλαγή, δηλαδή ο υπογράφων δεν μπορεί να αρνηθεί τη συμμετοχή του στην εν λόγω συναλλαγή

Σε αντιδιαστολή με την ιδιόχειρη υπογραφή, το ακριβές περιεχόμενο της ηλεκτρονικής υπογραφής διαφοροποιείται ανάλογα με τα προς υπογραφή δεδομένα, αφού προκύπτει και βάσει αυτών.

Χρήση Ψηφιακών Υπογραφών με το Office XP της Microsoft

Η συγγραφή, η αποθήκευση και κυρίως η διανομή ενός ηλεκτρονικού εγγράφου μέσα από το Microsoft Office XP είναι μια απλή και συνηθισμένη υπόθεση. Ο χρήστης μπορεί να αποστείλει ένα έγγραφο συνημμένο σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου, να αποθηκεύσει ένα έγγραφο σε μια κοινόχρηστη θέση, ή να διανείμει ένα έγγραφο με δισκέτα. Κατ' αυτόν τον τρόπο, όμως, αυξάνεται ο κίνδυνος αλλοίωσης των δεδομένων ή μόλυνσή τους με ιούς από άλλους χρήστες.

Ένας τρόπος ελαχιστοποίησης αυτού του κινδύνου, με παράλληλη λήψη περισσότερων πληροφοριών για την εγκυρότητα του εγγράφου, είναι η χρήση ψηφιακών υπογραφών. Ο χρήστης μπορεί να χρησιμοποιεί ψηφιακές υπογραφές μέσα

στην εταιρεία όπου εργάζεται κατά τη διανομή ή δημοσίευση εγγράφων. Η υπογραφή σε ένα έγγραφο υποδηλώνει στους συναδέλφους ότι βλέπουν την τελική, μη τροποποιημένη έκδοση του εγγράφου. Επειδή σε ένα έγγραφο μπορούν να επισυναφθούν πολλές υπογραφές, μπορούν επίσης να χρησιμοποιηθούν υπογραφές, για να υποδηλωθεί ότι ο χρήστης και κάποιος συνάδελφός του συμφωνεί όσον αφορά το τελικό περιεχόμενο ενός εγγράφου. Για παράδειγμα, υπάλληλος και διευθυντής μπορούν να χρησιμοποιούν ψηφιακές υπογραφές, για να υπογράφουν την αναθεώρηση επιδόσεων.

Τρόπος διαπίστωσης ότι ένα αρχείο φέρει υπογραφή

Στα προγράμματα του Office τα οποία υποστηρίζουν ψηφιακές υπογραφές, υπάρχουν δύο βασικοί τύποι υπογεγραμμένων αρχείων: υπογεγραμμένα αρχεία όπως έγγραφα, παρουσιάσεις ή φύλλα εργασίας και υπογεγραμμένες μακροεντολές. Ο τρόπος με τον οποίο υπογράφεται κάθε τύπος αρχείου και τα πλεονεκτήματα της υπογραφής κάθε τύπου διαφέρουν ελαφρώς. Γενικά, υπογράφεται ένα έγγραφο για να επικυρωθεί το περιεχόμενό του. Υπογράφεται μια μακροεντολή για την παροχή κάποιας διαβεβαίωσης ότι δεν περιέχει ιό.

Ένα έγγραφο παραμένει υπογεγραμμένο μέχρι να τροποποιηθεί. Συνεπώς, η επισύναψη της υπογραφής πρέπει να είναι η τελευταία ενέργεια πριν από τη διανομή του. Οποιεσδήποτε αλλαγές πραγματοποιηθούν μετά την υπογραφή του εγγράφου καταργούν την εγκυρότητα της υπογραφής.

Υπάρχουν δύο τρόποι για να διαπιστώσει κανείς εάν ένα έγγραφο είναι υπογεγραμμένο. Πρώτον, εξετάζεται η γραμμή κατάστασης. Ένα υπογεγραμμένο έγγραφο περιέχει τη σφραγίδα υπογραφής στη γραμμή κατάστασης. Επίσης εξετάζεται η γραμμή τίτλου του παραθύρου του εγγράφου. Ένα υπογεγραμμένο έγγραφο φέρει την ένδειξη (Υπογεγραμμένο) αμέσως μετά τον τίτλο του εγγράφου.

Για τη λήψη πληροφοριών σχετικά με το ψηφιακό πιστοποιητικό το οποίο χρησιμοποιήθηκε για την υπογραφή, ο χρήστης μπορεί να επιλέξει την εντολή Επιλογές στο μενού Εργαλεία και από εκεί την καρτέλα Ασφάλεια και την επιλογή Ψηφιακές Υπογραφές.

Υπηρεσίες Παροχών Πιστοποίησης

Οι ΠΥΠ εκδίδουν τα πιστοποιητικά με στόχο τη συσχέτιση του δημόσιου κλειδιού με τον δικαιούχο του, προβαίνοντας παράλληλα και στην οργάνωση μιας αξιόπιστης "Υποδομής Δημόσιου Κλειδιού", (PKI Public Key Infrastructure) για την έκδοση, διάθεση και διαχείριση των σχετικών πιστοποιητικών.

Κατά συνέπεια, οι ΠΥΠ επιβάλλεται να προσφέρουν μια σειρά από υπηρεσίες, που δεν περιορίζονται στην έκδοση του πιστοποιητικού, αλλά αφορούν τον "κύκλο ζωής" του. Οι υπηρεσίες αυτές διασφαλίζονται μέσα στα πλαίσια του ΠΥΠ από τις εξής υπηρεσίες:

⇒ Υπηρεσία Εγγραφής (Registration Authority)

Παραλαμβάνει τις αιτήσεις και τα δικαιολογητικά για την έκδοση του πιστοποιητικού και είναι υπεύθυνη για τη συλλογή των πληροφοριών που αποτελούν το απαραίτητο περιεχόμενο του πιστοποιητικού. Τις πληροφορίες αυτές, που είναι απαραίτητες για την ταυτοποίηση του κατόχου των δεδομένων δημιουργίας με τον αιτούντα το πιστοποιητικό, τις μεταβιβάζει στη συνέχεια στην Υπηρεσία Έκδοσης των πιστοποιητικών.

⇒ Υπηρεσία Έκδοσης Πιστοποιητικών (Certification Authority)

Εκδίδει το πιστοποιητικό σύμφωνα με τη "Δήλωση Πρακτικής Πιστοποίησης".

⇒ Υπηρεσία Δημοσίευσης και Διανομής (Dissemination Service)

Δημοσιεύει τον κατάλογο με τα εκδοθέντα πιστοποιητικά, τους ιδιαίτερους όρους χρήσης του κάθε είδους πιστοποιητικού (Πολιτικές Πιστοποιητικών) καθώς και τη Δήλωση Πρακτικής Πιστοποίησης, με τρόπο που να τις καθιστά προσβάσιμες σε κάθε ενδιαφερόμενο.

⇒ Υπηρεσία Διαχείρισης και Δημοσίευσης Ανάκλησης (Revocation Management and Status Service)

Διαχειρίζεται τον κατάλογο με τα υπό έκδοση ή εκδοθέντα πιστοποιητικά. Δέχεται και ελέγχει αιτήματα ανάκλησης ή παύσης των πιστοποιητικών και προβαίνει στην έγκαιρη ενημέρωση της "Λίστας Ανακληθέντων Πιστοποιητικών ".

Προαιρετικά, ένας ΠΥΠ μπορεί να παρέχει και τις εξής υπηρεσίες

⇒ Υπηρεσίες Χρονοσήμανσης (Time Stamping Authority) των εγγράφων, όπως και από αίτηση των συνδρομητών.

⇒ Υπηρεσίες Προμήθειας Συσκευών Δημιουργίας Υπογραφής (Device Provision Service)

Υπηρεσίες οι οποίες παρέχουν στο συνδρομητή το ιδιωτικό του κλειδί, συνήθως υπό τη μορφή μιας "έξυπνης κάρτας". Στην περίπτωση που ο ΠΥΠ παρέχει υπηρεσίες προμήθειας συσκευών δημιουργίας υπογραφής και εκδίδει αναγνωρισμένα πιστοποιητικά, οφείλει να εγγυηθεί ότι τα δεδομένα δημιουργίας και επαλήθευσης υπογραφής μπορούν να χρησιμοποιηθούν συμπληρωματικά.

Οι παραπάνω υπηρεσίες μπορούν να παρέχονται άμεσα από τον ίδιο τον εκδότη των πιστοποιητικών ή από εξουσιοδοτημένους συνεργάτες του.

Η Έννοια της Ασφάλειας Συστήματος

Η ασφάλεια (security) μπορεί να οριστεί σαν την δυνατότητα παροχής προστασίας σε «αντικείμενα» (objects) ενός συστήματος, σε σχέση με την ακεραιότητά τους και το βαθμό εμπιστευτικότητας που τα διακρίνει. Ως «αντικείμενο» ορίζεται κάθε παθητικό τμήμα σε ένα σύστημα το οποίο αποτελείται από πληροφορίες και πόρους του συστήματος όπως κεντρικές μονάδες επεξεργασίας (CPUS), δίσκοι και προγράμματα. Ως «οντότητα» (entity) (ή υποκείμενο) ορίζεται κάθε ενεργητικό τμήμα ενός συστήματος που προκαλεί τη ροή πληροφοριών μεταξύ των αντικειμένων ή προκαλεί αλλαγές στην κατάσταση ενός συστήματος, όπως για παράδειγμα οι χρήστες, οι διαδικασίες που διενεργούνται ή και διάφορες συσκευές.

Επίσης, η ασφάλεια σχετίζεται με την ικανότητα του συστήματος να παρέχει ορθές και αξιόπιστες πληροφορίες, οι οποίες είναι διαθέσιμες στους εξουσιοδοτημένους χρήστες κάθε φορά που τις αναζητούν. Ο ορισμός που δόθηκε για την ασφάλεια είναι αρκετά γενικότερος από τον ορισμό που την περιορίζει στα πλαίσια της ασφάλειας των πληροφοριών και μόνο. Συμπεριλαμβάνει δε και την προστασία των πόρων ενός συστήματος όπως για παράδειγμα την προστασία έναντι της παράνομης χρήσης χρόνου επεξεργασίας, δίσκων και δικτύου. Η παροχή της ασφάλειας συστημάτων είναι στενά συνδεδεμένη με τη λήψη μέτρων τα οποία διασφαλίζουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, καθώς επίσης και την αδιάκοπη λειτουργία του συστήματος και άρα των υπηρεσιών που προσφέρει.

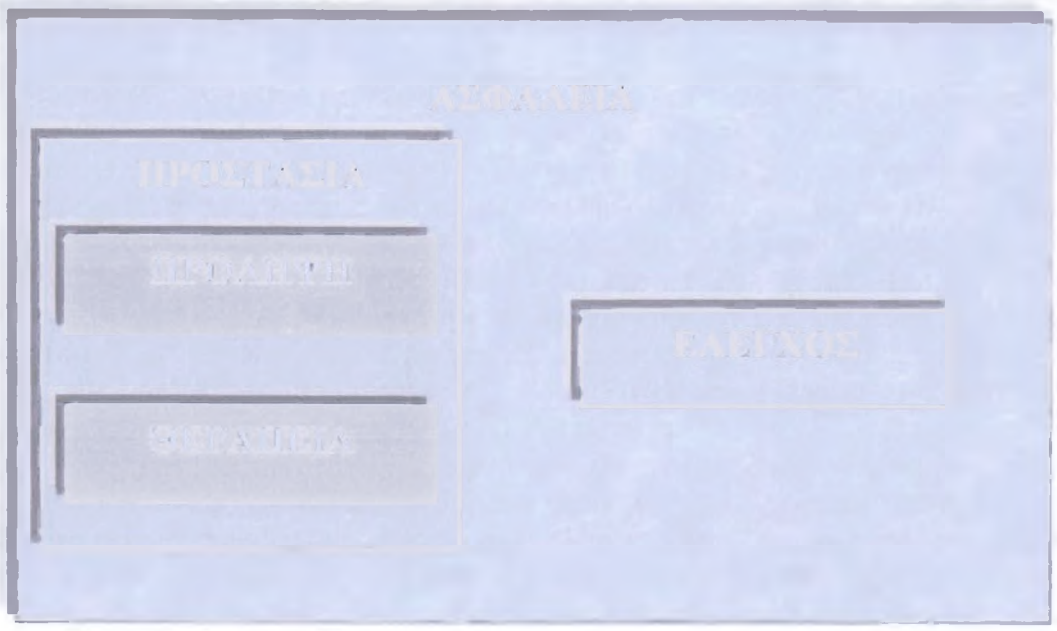
Η ασφάλεια αποτελεί παράγοντα εξαιρετικού ενδιαφέροντος ειδικά για τα συστήματα εκείνα τα οποία πρέπει να προστατεύονται από απειλές που υφίστανται στο περιβάλλον λειτουργίας τους. Άρα λοιπόν η ασφάλεια έχει να κάνει με την πρόληψη και την ανίχνευση μη εξουσιοδοτημένων ενεργειών των χρηστών ενός υπολογιστικού συστήματος καθώς και με τη λήψη μέτρων και αντίμετρων σε περίπτωση που υπάρξει περιστατικό παραβίασής της. Για το λόγο αυτό η ασφάλεια σχετίζεται με τις παρακάτω έννοιες:

⇒ **Πρόληψη:** είναι η λήψη μέτρων για να εμποδιστεί η δημιουργία φθορών που συνιστούν παραβίαση της ασφάλειας ενός υπολογιστικού συστήματος.

⇒ **Ανίχνευση:** είναι η λήψη μέτρων για την ανίχνευση μιας παραβίασης της ασφάλειας σε σχέση με το χρόνο, τον τρόπο και από ποιον έγινε αυτή.

⇒ **Αντίδραση:** είναι η λήψη μέτρων για την αποκατάσταση ή την ανάκτηση των
συστατικών ενός υπολογιστικού συστήματος

Η ασφάλεια μπορεί να θεωρηθεί ότι αποτελείται από κύριες συνιστώσες, την προστασία και τον έλεγχο, από τις οποίες η προστασία αναλύεται στην πρόληψη και την θεραπεία (σχήμα 1).



Σχήμα 1 : Οι βασικές συνιστώσες της ασφάλειας

Η έννοια της ασφάλειας ενός πληροφοριακού συστήματος είναι συνυφασμένη με δύο κύριες παραμέτρους:

⇒ Την πολιτική ασφάλειας

⇒ Το κόστος υλοποίησης

Πολιτική Ασφάλειας

Πολιτική ασφάλειας είναι ένα σύνολο κανόνων μέσα από τους οποίους πρέπει να διακρίνεται σαφώς τι επιτρέπεται και τι δεν επιτρέπεται να γίνεται σε ένα σύστημα κατά τη διάρκεια κανονικής λειτουργίας του. Πρέπει να είναι διατυπωμένη με γενικούς όρους και να περιγράφει τις απαιτήσεις ασφάλειας για το πληροφοριακό σύστημα.

Μέσα από αυτή ορίζεται το κανονιστικό πλαίσιο σύμφωνα με το οποίο προδιαγράφεται ο τρόπος πρόσβασης των οντοτήτων ενός συστήματος στα αντικείμενά του. Επίσης, πρέπει μέσα από αυτή να περιγράφεται η μέθοδος προστασίας του συστήματος εκτιμώντας οικονομικά ισορροπημένες και υλοποιήσιμες λύσεις και να περιλαμβάνονται στο σχεδιασμό όλες οι οντότητες και τα αντικείμενα του συστήματος.

Η Ανάλυση Απειλών (Threat Analysis) παρέχει σημαντικές πληροφορίες για τον καθορισμό πολιτικής ασφάλειας και αποτελεί τη διαδικασία μέσω της οποίας αναγνωρίζονται όλες οι πιθανές απειλές στις οποίες είναι εκτεθειμένο ένα σύστημα. Αποτέλεσμα της ανάλυσης αυτής είναι η δημιουργία μιας λίστας απειλών που υφίστανται και του βαθμού επικινδυνότητας που τις χαρακτηρίζει. Η λίστα αυτή μπορεί να αποτελέσει τη βάση για τον περαιτέρω καθορισμό πολιτικής. Αφού καθοριστεί η πολιτική ασφάλειας, μπορεί στη συνέχεια να χρησιμοποιηθεί στη λήψη αποφάσεων για την επιλογή Μηχανισμών Ασφάλειας ή αντίμετρων. Μηχανισμοί Ασφάλειας είναι οι μηχανισμοί που υλοποιούν μέτρα ασφαλείας σε ένα σύστημα, όπως για παράδειγμα οι μηχανισμοί ελέγχου πρόσβασης μέσω των οποίων αποφασίζεται ποιες οντότητες επιτρέπεται να έχουν πρόσβαση σε ένα αντικείμενο.

Σχήμα 2 : Ο ρόλος της πολιτικής ασφάλειας

Κατά τη διαδικασία καθορισμού πολιτικής ασφάλειας είναι σημαντικό να γίνει αντιληπτό ότι οι κανόνες που θα προταθούν επηρεάζουν την επιλογή μηχανισμών. Άρα είναι σημαντικό να προσεγγίζεται το θέμα της πολιτικής με τέτοιο τρόπο ώστε να οδηγεί σε εφικτές από την άποψη του σχεδιασμού λύσεις με στόχο την ορθή αλλά και πρακτική χρήση τους. Ένα ορθά σχεδιασμένο σύστημα ασφάλειας μπορεί να παρομοιαστεί με την είσοδο ενός κτιρίου. Αν η πόρτα και η κλειδαριά είναι αρκετά καλές οι περισσότεροι εισβολείς αποτρέπονται εξαρχής και δεν προσπαθούν να την παραβιάσουν. Βέβαια αν ένας εισβολέας θέλει πραγματικά να μπει στο κτίριο δεν θα τον εμποδίσει καμία πόρτα όσο καλή και αν είναι απλά θα ανέβει το επίπεδο δυσκολίας για αυτόν. Αν όμως η κλειδαριά δεν είναι εύκολη στη χρήση γρήγορα θα παρατηρηθεί η τάση να μην χρησιμοποιείται από το προσωπικό δημιουργώντας προϋποθέσεις για ευκολότερη παραβίαση.

Οι ίδιοι κανόνες εφαρμόζονται και στην ασφάλεια των πληροφοριακών συστημάτων. Τα εργαλεία που θα χρησιμοποιηθούν για να ενισχύσουν την ασφάλεια πρέπει να είναι καλά σχεδιασμένα αλλά και εύκολα στη χρήση ώστε να γίνουν αποδεκτά και να χρησιμοποιούνται από τους χρήστες του συστήματος.

Οποιαδήποτε ενέργεια σκόπιμη ή μη σκόπιμη, που παραβιάζει τους καθορισμένους κανόνες ασφάλειας θεωρείται σαν Παραβίαση Ασφάλειας (Security Violation).

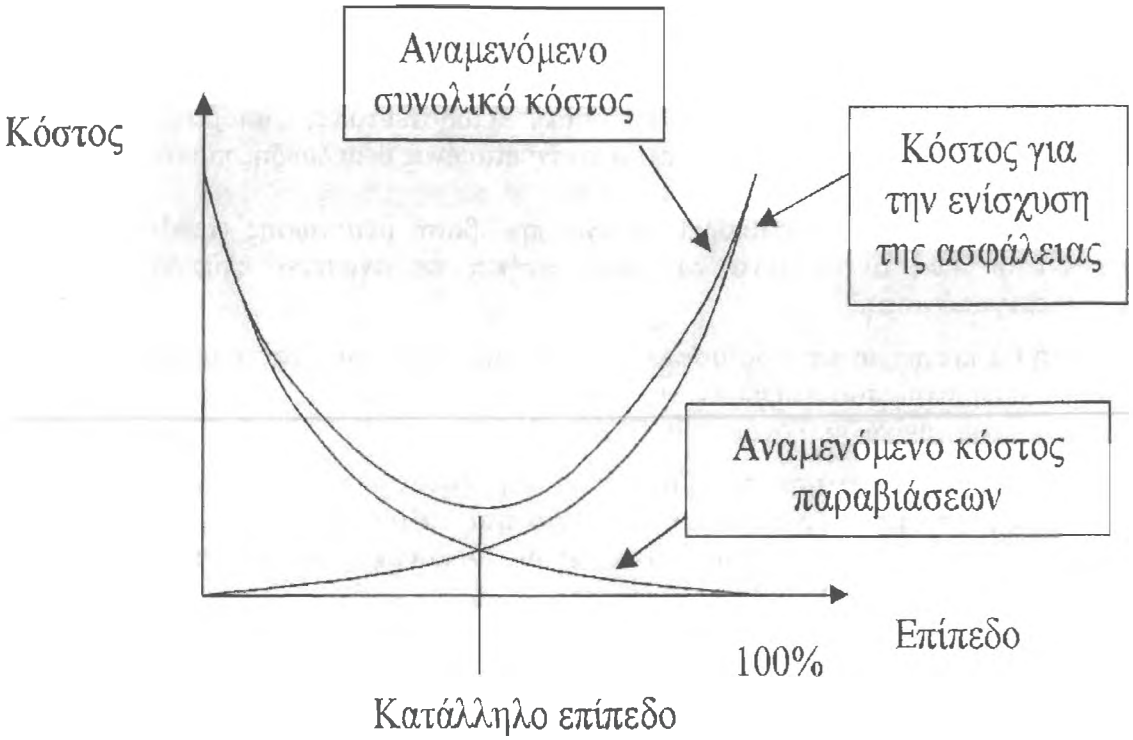
Κόστος Ασφάλειας

Οι απαιτήσεις και τα επίπεδα ασφάλειας ενός υπολογιστικού συστήματος διαφέρουν ανάλογα με τις εφαρμογές για τις οποίες χρησιμοποιείται, π.χ.: οικονομικές συναλλαγές, συστήματα κράτησης θέσεων ή συστήματα ελέγχου, όλα έχουν διαφορετικές απαιτήσεις. Επίσης, ποικίλει και το χρηματικό πόσο που διαθέτουν οι ιδιοκτήτες των συστημάτων για την υλοποίηση κανόνων και τεχνικών ασφάλειας. Πρέπει βέβαια να επισημανθεί ότι 'δεν υπάρχουν πλήρως ασφαλή και αξιόπιστα συστήματα. Αντιθέτως μάλιστα υπάρχει η έννοια του συνεχούς, κατά τη μετάβαση από ένα ανασφαλές σύστημα σε ένα συνολικά ασφαλές.

"Ασφαλές σύστημα νοείται αυτό στο οποίο ένας υποψήφιος εισβολέας χρειάζεται να σπαταλήσει ένα μεγάλο και μη αποδεκτό χρονικό διάστημα ή χρηματικό ποσό για να διεισδύσει σε αυτό. Επίσης ο κίνδυνος να αποκαλυφθεί ο ίδιος πρέπει να βρίσκεται σε υψηλά ποσοστά."

Αυξημένη ασφάλεια συχνά σημαίνει και αυξανόμενο κόστος. Το κόστος αυτό συνήθως συνδυάζει πολλούς παράγοντες, όχι μόνο καθαρά οικονομικούς, όπως για παράδειγμα τη μείωση της απόδοσης του συστήματος ή την αύξηση της πολυπλοκότητας του. τη μείωση χρήσης του και την αύξηση κόστους λειτουργίας και συντήρησης. Πολλοί τέτοιοι παράγοντες υπεισέρχονται στη εκτίμηση κόστους με αρκετά πολύπλοκο τρόπο. Για παράδειγμα) μπορεί να επιτευχθεί υψηλό επίπεδο ασφάλειας με την απομάκρυνση των περισσότερων ή και όλων των υπηρεσιών που παρέχονται από ένα σύστημα αλλά αυτό θα έχει σαν αποτέλεσμα την αχρήστευση του με τη μείωση της χρήσης του από τους χρήστες.

Σε τελική ανάλυση για όλα σχεδόν τα συστήματα έχει εκτιμηθεί ότι το κόστος για την διασφάλιση των κανόνων ασφαλείας αυξάνεται εκθετικά όσο πλησιάζουμε το 100% του επιπέδου ασφάλειας. Κρίνεται λοιπόν αναγκαίο να περιοριστεί η εφαρμογή των κανόνων ασφάλειας στους πόρους εκείνους του συστήματος που πρέπει να προστατευθούν εκτιμώντας την αξία τους. Πρέπει επομένως να υπάρχει μια εξισορροπημένη αναλογία ανάμεσα στην αυξανόμενη ασφάλεια ενός συστήματος και στο κόστος που αυτή συνεπάγεται.



Σχήμα 3 : Η συνάρτηση κόστους ασφάλειας

Από την άλλη πλευρά το συνολικό κόστος από την παραβίαση της ασφάλειας ενός συστήματος πρέπει να υπολογίζεται σαν το κόστος από την απώλεια που συνεπάγεται μια μεμονωμένη παραβίαση επί τη συχνότητα επανάληψης της παραβίασης αυτής, το οποίο επίσης αποτελεί μια ιδιαίτερα δύσκολη εκτίμηση.

Μοντέλα Ασφάλειας

Μέσω ενός τυπικού μοντέλου ασφάλειας καθορίζεται με ακρίβεια ο τρόπος με τον οποίο επιτρέπεται η πρόσβαση σε αντικείμενα. Σαν αποτέλεσμα προκύπτει ότι με την μοντελοποίηση μπορεί να περιγραφεί η ροή των πληροφοριών σε ένα σύστημα και έτσι αποδεικνύεται η διατήρηση της ακεραιότητας ή/ και της εμπιστευτικότητας των αντικειμένων.

Δύο σημαντικά μοντέλα περιγράφονται παρακάτω: Το μοντέλο Bell-La Padula που ενισχύει την εμπιστευτικότητα των αντικειμένων και το μοντέλο Biba που ενισχύει την ακεραιότητά τους. Και τα δύο μοντέλα βασίζονται στη θεωρία συνόλων και μέσω αυτής ορίζονται ασφαλείς καταστάσεις και μεταβάσεις σε ένα σύστημα.

Το Μοντέλο Bell-La-Padula

Σύμφωνα με το μοντέλο αυτό όλες οι οντότητες διακρίνονται σε ταξινομημένα επίπεδα ασφάλειας (π.χ. Μη-απόρρητες, εμπιστευτικές, απόρρητες, άκρως απόρρητες). Μέσω αυτού του μοντέλου ενισχύεται ένας θεμελιώδης κανόνας:

"Καμία οντότητα δεν θα μπορεί να έχει πρόσβαση ανάγνωσης (read-access) σε ένα αντικείμενο το οποίο ανήκει σε ανώτερο επίπεδο ασφάλειας από αυτή."

Δηλαδή θα πρέπει το επίπεδο ασφάλειας μιας οντότητας να είναι ανώτερο από αυτό του αντικειμένου που επιχειρεί να αναγνώσει. Αυτός είναι ένας απλός κανόνας ασφάλειας με την κωδική ονομασία «No Read-up».

Για να έχει μια οντότητα πρόσβαση εγγραφής (write access) σε ένα αντικείμενο σύμφωνα με το μοντέλο αυτό αρκεί η οντότητα να ανήκει σε επίπεδο ασφάλειας μικρότερο ή ίσο με αυτό του αντικειμένου. Ο κανόνας αυτός έχει την κωδική ονομασία «No write-down».

Και οι δύο αυτοί κανόνες αποδίδονται από τις ακόλουθες σχέσεις:

Ανάγνωση (read): SL (Entity) >= SL (Obj)

Εγγραφή (write): SL (Entity) <= SL (Obj)

Όπου με SL συμβολίζεται το επίπεδο ασφάλειας (Security Level) για μια οντότητα (Entity) ή ένα αντικείμενο(Object).

Το μοντέλο αυτό ενισχύει την εμπιστευτικότητα των αντικειμένων, αφού καμία οντότητα δεν μπορεί να αναγνώσει αντικείμενα που ανήκουν σε υψηλότερο επίπεδο ασφάλειας από αυτό στο οποίο ανήκει αύτή. Εντούτοις, επειδή παρέχει την δυνατότητα εγγραφής σε αντικείμενα με υψηλότερο δείκτη ασφάλειας παραβιάζεται η ακεραιότητα των αντικειμένων.

Η εφαρμογή των κανόνων αυτού του μοντέλου μπορεί να δημιουργήσει διάφορα προβλήματα. Π.χ. κατά την επικοινωνία μιας οντότητας με μια άλλη θα πρέπει επίσης να τηρούνται οι κανόνες που προαναφέρθηκαν. Το γεγονός αυτό έχει ως αποτέλεσμα να μην είναι εφικτή η αποστολή μηνύματος σε οντότητα με υψηλότερο δείκτη ασφάλειας διότι ο παραλήπτης δεν επιτρέπεται να απαντήσει στο μήνυμα και ούτε καν να στείλει ACK στον αποστολέα. Σε ορισμένες περιπτώσεις λύση σε τέτοια προβλήματα δίνεται με τη χρήση εμπιστευτικού ενδιάμεσου.

Γενικά παρατηρείται στο μοντέλο αυτό η τάση ροής της πληροφορίας από τα κατώτερα προς τα ανώτερα επίπεδα ασφάλειας.

Το Μοντέλο Biba

Αποτελεί ένα επίσης τυπικό μοντέλο συμπληρωματικό προς το προηγούμενο. Σύμφωνα με τους κανόνες που εφαρμόζονται σε αυτό ενισχύεται η ακεραιότητα των αντικειμένων αντί της εμπιστευτικότητας διασφαλίζοντας ότι μια οντότητα μπορεί να έχει πρόσβαση εγγραφής (write Access) μόνο σε αντικείμενα που είναι ταξινομημένα σε χαμηλότερο επίπεδο ασφάλειας από αυτό στο οποίο ανήκει αυτή.

Με αυτό τον τρόπο εμποδίζεται η σκόπιμη τροποποίηση αντικειμένων με υψηλό δείκτη ασφάλειας από επισφαλείς οντότητες κάτι το οποίο αντιθέτως επιτρέπεται στο προηγούμενο μοντέλο που παρουσιάστηκε. Επίσης, μια οντότητα μπορεί να αναγνώσει πληροφορίες από αντικείμενα τα οποία έχουν υψηλότερο δείκτη ασφάλειας από την ίδια.

Και οι δύο αυτοί κανόνες αποδίδονται από τις ακόλουθες σχέσεις:

Εγγραφή (write): **IL (Entity) >= IL (Obj)**

Ανάγνωση (read): **IL (Entity) <= IL (Obj)**

Όπου με IL συμβολίζεται το επίπεδο ακεραιότητας οντότητα(Entity) ή ένα αντικείμενο(Object).

Σύμφωνα με τους ανωτέρω κανόνες επιτρέπεται σε μια οντότητα να αποκαλύψει τα περιεχόμενα αντικειμένων που χαρακτηρίζονται από υψηλότερο επίπεδο ασφάλειας σε σχέση με αυτό στο οποίο ανήκει αυτή.

Τα δύο αυτά μοντέλα μπορούν να συνδυαστούν και να αποτελέσουν ένα ενιαίο σύστημα, η περιγραφή της υλοποίησης του οποίου ξεφεύγει από τους στόχους αυτής της εισαγωγικής προσέγγισης στα θέματα ασφάλειας.

Το Στρατιωτικό Μοντέλο Ασφάλειας

Συναντάται και με την ονομασία δικτυωτό και χρησιμοποιείται από το στρατό των Ηνωμένων Πολιτειών και την κυβέρνηση τους. Αποτελεί ένα καλό παράδειγμα υλοποίησης υποχρεωτικής εφαρμογής πολιτικής ελέγχου πρόσβασης. Στο παράδειγμα που παρουσιάζεται στο ακόλουθο σχήμα διακρίνονται 9 μη-ιεραρχημένα επίπεδα ασφάλειας (A-I) τα οποία καλούνται τμήματα και 4 ιεραρχημένα επίπεδα ασφάλειας (μη-απόρρητο, εμπιστευτικό, απόρρητο και άκρως απόρρητο) που περιγράφουν ταξινομημένα την ασφάλεια αντικειμένων. Στο σχήμα περιέχονται τρία αντικείμενα και για παράδειγμα το αντικείμενο 2 ανήκει στα τμήματα F, G και H και έχει ταξινομηθεί ως απόρρητο αντικείμενο. Πρακτικά αυτό σημαίνει ότι όλα τα αντικείμενα έχουν για παράδειγμα μια ετικέτα που δείχνει το επίπεδο ασφάλειας στο οποίο ανήκουν και το τμήμα

Τα τμήματα στα οποία ανήκει ένα αντικείμενο καθώς και το επίπεδο ασφάλειας που το χαρακτηρίζει ελέγχονται μέσω της υποχρεωτικής πολιτικής πρόσβασης. Για να έχει πρόσβαση μια οντότητα σε ένα αντικείμενο πρέπει να είναι μέλος όλων των τμημάτων στα οποία ανήκει το αντικείμενο. Για παράδειγμα για να προσπελαστεί από μια οντότητα το αντικείμενο 2 τότε αυτή πρέπει τουλάχιστον να είναι μέλος των F, G και H. Ουσιαστικά δηλαδή η πρόσβαση περιορίζεται μόνο στις οντότητες που απαιτείται/ χρειάζεται να γνωρίζουν και μόνο σε αυτές. Επίσης, μια οντότητα μπορεί να αναγνώσει πληροφορίες από αντικείμενα τα οποία έχουν υψηλότερο δείκτη ασφάλειας από την ίδια.

Και οι δύο αυτοί κανόνες αποδίδονται από τις ακόλουθες σχέσεις:

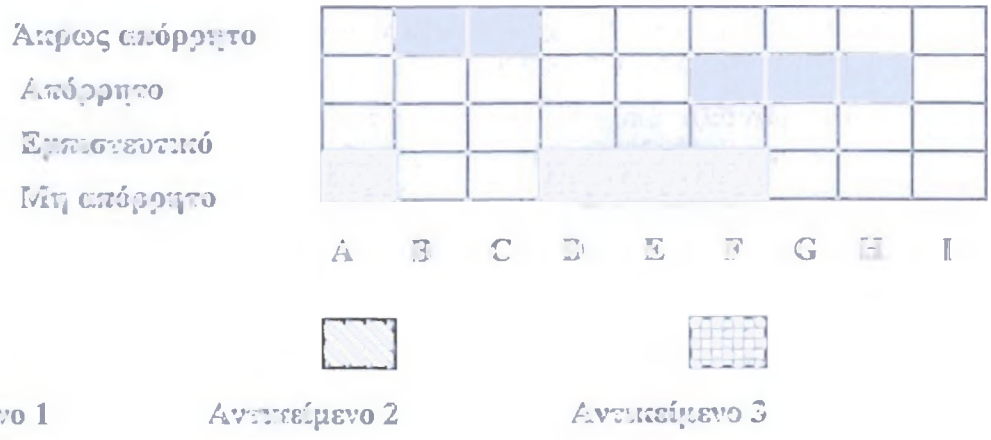
Εγγραφή (write): IL (Entity) >= IL (Obj)

Ανάγνωση (read): IL (Entity) <= IL (Obj)

Όπου με IL συμβολίζεται το επίπεδο ακεραιότητας οντότητα(Entity) ή ένα αντικείμενο(Object).

Σύμφωνα με τους ανωτέρω κανόνες επιτρέπεται σε μια οντότητα να αποκαλύψει τα περιεχόμενα αντικειμένων που χαρακτηρίζονται από υψηλότερο επίπεδο ασφάλειας σε σχέση με αυτό στο οποίο ανήκει αυτή.

Τα δύο αυτά μοντέλα μπορούν να συνδυαστούν και να αποτελέσουν ένα ενιαίο σύστημα, η περιγραφή της υλοποίησης του οποίου ξεφεύγει από τους στόχους αυτής της εισαγωγικής προσέγγισης στα θέματα ασφάλειας.



Σχήμα 4 : Συνδυαστικό μοντέλο ασφάλειας με υποχρεωτικούς ελέγχους πρόσβασης

Επίσης, η πολιτική υποχρεωτικών ελέγχων πρόσβασης διασφαλίζει ότι καμία οντότητα δεν μπορεί να τροποποιήσει το τμήμα ή το επίπεδο ασφάλειας στο οποίο ανήκει ένα αντικείμενο.

Απαιτήσεις Ασφάλειας

Εισαγωγικά

Ένα από τα πιο σημαντικά ζητήματα που σχετίζονται άμεσα με τη χρήση και τη διάδοση του ηλεκτρονικού εμπορίου αφορά το επίπεδο ασφάλειας των ηλεκτρονικών συναλλαγών. Στη συνέχεια παρατίθενται μια συνοπτική αναφορά στις απαιτήσεις και στους μηχανισμούς ασφάλειας, στα ψηφιακά πιστοποιητικά, καθώς και στους πιο γνωστούς αλγόριθμους κρυπτογράφησης.

Οι απαιτήσεις ασφάλειας είναι οι ακόλουθες:

Εμπιστευτικότητα (Confidentiality): η εμπιστευτικότητα είναι απαραίτητο στοιχείο της ιδιωτικότητας του χρήστη (user privacy) καθώς και της προστασίας των μυστικών πληροφοριών. Η εμπιστευτικότητα είναι συνυφασμένη με την αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας και παρέχεται μέσω κρυπτογράφησης. Σε ένα ηλεκτρονικό περιβάλλον θα πρέπει να υπάρχει η βεβαιότητα ότι το περιεχόμενο των μηνυμάτων που ανταλλάσσονται παραμένει αναλλοίωτο.

Ακεραιότητα (Integrity): ακεραιότητα σημαίνει αποφυγή μη εξουσιοδοτημένης τροποποίησης των πληροφοριών που ανταλλάσσονται και παρέχεται μέσω ψηφιακής υπογραφής. Τα δεδομένα που αποστέλλονται ως μέρος της συναλλαγής πρέπει να είναι μη τροποποιήσιμα κατά τη διάρκεια της μεταφοράς και αποθήκευσής τους στο δίκτυο.

Έλεγχος Αυθεντικότητας (Authentication): η διαδικασία επαλήθευσης της ορθότητας του ισχυρισμού ενός χρήστη ότι κατέχει μια συγκεκριμένη ταυτότητα, αλλά και η βεβαιότητα ότι το περιεχόμενο του μηνύματος παρέμεινε αναλλοίωτο κατά την μεταφορά, οριοθετούν την έννοια του ελέγχου αυθεντικότητας. Σύμφωνα με τον παραπάνω ορισμό, η πιστοποίηση της ταυτότητας των επιχειρήσεων που συμμετέχουν σε μια συναλλαγή είναι απαραίτητη ‘ώστε κάθε συναλλασσόμενο μέρος να μπορεί να πεισθεί για την ταυτότητα του άλλου. Ο έλεγχος αυθεντικότητας παρέχεται μέσω ψηφιακής υπογραφής.

Εξουσιοδότηση (Autherization): η εξουσιοδότηση αφορά την παραχώρηση δικαιωμάτων από τον ιδιοκτήτη στο χρήστη. Για παράδειγμα, ο πελάτης εξουσιοδοτεί τον έμπορο ώστε ο τελευταίος να ελέγχει αν ο αριθμός της πιστωτικής κάρτας είναι έγκυρος και αν τα χρήματα στο λογαριασμό μπορούν να καλύψουν το ποσό των συναλλαγών.

Εξασφάλιση (Assurance): η εμπιστοσύνη ότι κάποιος αντικειμενικός σκοπός ή απαίτηση επιτυγχάνονται. Για παράδειγμα, μια από τις απαιτήσεις του πελάτη είναι η βεβαιότητα ότι ο έμπορος με τον οποίο συναλλάσσεται είναι νόμιμος και έμπιστος.

Μη αποποίηση ευθύνης (Non-repudiation): κανένα από τα συναλλασσόμενα μέρη δεν πρέπει να έχει τη δυνατότητα να αρνηθεί τη συμμετοχή του σε μια συναλλαγή.

Απόδοση ευθυνών (accountability): η ανάθεση ευθυνών σε χρήστες του συστήματος όταν συμβεί παραβίαση της ασφάλειάς του. Για το λόγο αυτό πρέπει να υπάρχει ασφαλής αναγνώριση των και διατήρηση εγγραφών ελέγχου της δραστηριότητας στο σύστημα.

Αξιοπιστία (reliability) και σιγουριά (safety): η ασφάλεια σχετίζεται με την αξιοπιστία και τη σιγουριά καθώς έχει να κάνει με συστήματα που πρέπει να λειτουργούν κανονικά σε αντίξοες συνθήκες.

Μηχανισμοί Ασφάλειας

Προκειμένου να επιτευχθεί εμπιστευτικότητα των πληροφοριών των ηλεκτρονικών συναλλαγών χρησιμοποιείται κρυπτογράφηση, δημόσιου ή ιδιωτικού κλειδιού.

Συμμετρική κρυπτογράφηση (Symmetric key encryption):

Η κρυπτογράφηση ιδιωτικού κλειδιού ή συμμετρική κρυπτογράφηση βασίζεται σε ένα κοινό κλειδί το οποίο διαμοιράζεται μεταξύ των συναλλασσόμενων μερών. Το κλειδί αυτό χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση των μηνυμάτων. Ο Kerberos και το Data Encryption Standard είναι οι πλέον παραδοσιακές τεχνολογίες ιδιωτικού κλειδιού. Το βασικό πρόβλημα της κρυπτογράφησης του τύπου αυτού αφορά τη δημιουργία, την αποθήκευση και τη μετάδοση του μυστικού κλειδιού (Key management). Συγκεκριμένα:

⇒ Και τα δύο συναλλασσόμενα μέρη θα πρέπει να συμφωνήσουν για ένα κοινό μυστικό κλειδί.

⇒ Κάθε χρήστης θα πρέπει να έχει τόσα μυστικά κλειδιά όσα και τα μέλη με τα οποία συναλλάσσεται.

⇒ Δεν ικανοποιείται η απαίτηση για αυθεντικότητα, γιατί δε μπορεί να αποδειχτεί η ταυτότητα των συναλλασσόμενων μερών. Από τη στιγμή που δύο άτομα κατέχουν το ίδιο κλειδί, τότε και οι δύο μπορούν να κρυπτογραφήσουν κάποιο μήνυμα και να ισχυριστούν ότι το έστειλε το άλλο άτομο. Κατά συνέπεια, η μη αποποίηση της ευθύνης (non-repudiation) για την αποστολή ενός μηνύματος καθίσταται και αυτή αδύνατη. Το πρόβλημα αυτό επιλύεται με την κρυπτογράφηση δημόσιου κλειδιού ή ασύμμετρη κρυπτογράφηση.

Ασύμμετρη κρυπτογράφηση (Asymmetric key encryption):

Η κρυπτογράφηση δημόσιου κλειδιού βασίζεται σε ένα ζεύγος κλειδιών εκ των οποίων το ένα είναι δημόσια γνωστό ενώ το άλλο είναι ιδιωτικό. Στην κρυπτογράφηση δημόσιου κλειδιού οτιδήποτε κρυπτογραφείται με το ένα κλειδί μπορεί να αποκρυπτογραφηθεί χρησιμοποιώντας μόνο το άλλο κλειδί.

Το κύριο πλεονέκτημα που προσφέρει η κρυπτογράφηση δημόσιου κλειδιού είναι η αυξημένη ασφάλεια που παρέχει. Η κρυπτογράφηση δημόσιου κλειδιού θεωρείται κατάλληλη για το Ηλεκτρονικό Εμπόριο για τους εξής λόγους:

⇒ Εξασφαλίζει την εμπιστευτικότητα του μηνύματος,

⇒ Παρέχει πιο ευέλικτα μέσα αυθεντικοποίησης των χρηστών,

⇒ Υποστηρίζει ψηφιακές υπογραφές (ακεραιότητα μηνύματος).

Τα δύο αυτά κλειδιά μπορούν να χρησιμοποιηθούν με δύο διαφορετικούς τρόπους για να εξασφαλίσουν την εμπιστευτικότητα του μηνύματος και να αποδείξουν την αυθεντικότητα του δημιουργού του.

⇒ Στην πρώτη περίπτωση για την παραγωγή ενός εμπιστευτικού μηνύματος, ο αποστολέας χρησιμοποιεί το δημόσιο κλειδί του παραλήπτη για να κρυπτογραφήσει το μήνυμα, έτσι ώστε να παραμείνει απόρρητο ως ότου αποκρυπτογραφηθεί από το ιδιωτικό κλειδί του παραλήπτη.

⇒ Στη δεύτερη περίπτωση, ο αποστολέας κωδικοποιεί ένα μήνυμα με το ιδιωτικό του κλειδί, το οποίο είναι απόρρητο. Το ιδιωτικό κλειδί αποδεικνύει την ταυτότητα του χρήστη (αυθεντικοποίηση). Δηλαδή, η χρήση ιδιωτικού κλειδιού για την κρυπτογράφηση ενός μηνύματος είναι αντίστοιχη με την προσθήκη της υπογραφής του αποστολέα σε κάποιο έγγραφο. Έτσι λοιπόν οποιοσδήποτε χρησιμοποιήσει το δημόσιο κλειδί του αποστολέα για να αποκρυπτογραφήσει το μήνυμα θα είναι σίγουρος για την ταυτότητα του πρώτου.

Επίσης υπάρχει και μια άλλη μέθοδος κρυπτογράφησης:

Το μέλλον:
Κβαντική κρυπτογράφηση:

Οι σημερινές τεχνολογίες κρυπτογράφησης, παρότι παρέχουν μεγάλο ποσοστό ασφάλειας, έχει αποδειχθεί ότι δεν είναι άτρωτες. Η απάντηση στο πρόβλημα είναι η χρήση της κβαντικής Φυσικής, όπως υποστηρίζει ο Νικολά Ζισίν, πρωτοπόρος της συγκεκριμένης τεχνολογίας στο Πανεπιστήμιο της Γενεύης. Εν συντομία, το σκεπτικό έχει ως εξής: οποιαδήποτε προσπάθεια παρατήρησης ενός κβαντικού συστήματος αυτόματα προκαλεί την "αλλοίωσή" του. Κατ' αυτό τον τρόπο, ακόμη και η παραμικρή προσπάθεια υποκλοπής γίνεται αμέσως αντιληπτή. Η κβαντική κρυπτογράφηση βρίσκεται εδώ και μια δεκαετία στο στάδιο των εργαστηριακών δοκιμών, αλλά σύντομα αναμένεται να εφαρμοστεί και εμπορικά.

Proxy και Proxy Chains

Η αρχαιότερη τεχνολογία και η βάση όλων των ανώνυμων επικοινωνιών στο Διαδίκτυο είναι ο proxy.Ο proxy είναι ένας υπολογιστής στο δίκτυο, ο οποίος αναλαμβάνει να προωθήσει ένα "μήνυμα" που αποστέλλει ένας υπολογιστής Α σε ένα

υπολογιστή Β, φροντίζοντας έτσι ώστε να μην αποκαλυφθεί ποτέ η πηγή του μηνύματος.

Ένας τέτοιος proxy, δηλαδή ένας proxy που κατορθώνει επιτυχώς να αποκρύψει την ταυτότητα του αποστολέα του μηνύματος καλείται "anonymizer".
Οι "anonymizer" προέκυψαν ως απομιμήσεις τις καθημερινής ζωής... π.χ. στην συχνή περίπτωση που ένας δημοσιογράφος μεταφέρει μια είδηση αρχίζοντας με την φράση

"Σύμφωνα με πηγές" και άλλα τετριμμένα χωρίς ωστόσο να κατονομαστεί η πηγή του μηνύματος έχουμε να κάνουμε με ένα "anonymizer".

Όταν ένα μήνυμα περνάει από μια αλυσίδα anonymizers, περνάει μέσα από ένα σύστημα υπολογιστών που καλείται proxy chains (αλυσίδα από proxies) Πιο αποτελεσματικοί proxy chains είναι αυτοί που υποστηρίζουν ισχυρή κρυπτογράφηση δεδομένων.

Mixnets και Mixnet Reply Blocks

Τα Mixnets πρωτοεμφανίστηκαν αν το 1981 από τον David Chaum.Βασική έννοια στα Mixnets είναι ο MIX, ένας proxy που αποδέχεται τα κρυπτογραφημένα μηνύματα με το Public key (μέθοδος πιστοποίησης ταυτότητας που λειτουργεί ως κλειδί για την αποκρυπτογράφηση της πληροφορίας), τα αποκωδικοποιεί, τα ταξινομεί και τα προωθεί στον τελικό τους αποδέκτη, διαγράφοντας όλες τις πληροφορίες για την πηγή τους.

Επιπλέον, ο Chaum, καθόρισε τον τρόπο με το οποίο η χρήση αλυσίδων από Mix μπορεί να οδηγήσει στην τελική διαγραφή όλων των στοιχείων που αποδεικνύουν την ταυτότητα του αποστολέα. Ένα mixnet τώρα συνιστά ένα κόμβο υπολογιστών, καθένας από τους οποίους έχουν ένα ζεύγος pubic/secret keys.

Το μήνυμα φθάνει κρυπτογραφημένο στο πρώτο MIX, αποκρυπτογραφείται, κρυπτογραφείται και στην συνέχεια περνάει στο επόμενο MIX όπου ακολουθείται πάλι η ίδια διαδικασία μέχρι να φθάσει στον τελικό MIX και να ανακατευθυνθεί στον τελικό αποδέκτη. Όσο πιο μεγάλη είναι η αλυσίδα των MIX τόσο πιο δύσκολο είναι για κάποιον να εντοπίσει την πηγή του μηνύματος.

Η πολυπλοκότητα των MIXnets καθώς επίσης και η δεδομένη καθυστέρηση που παρατηρείται στην αποστολή του μηνύματος, τα καθιστούν μη πρακτικά για χρήσεις

όπως Web browsing ή και συμμετοχή σε chat rooms και σε άλλα μέρη όπου υπάρχει απαίτηση για συνεχή διάδοση.

Τα MIXnets Reply Blocks, καθορίζουν πέρα από την αποστολή του μηνύματος και τη διαδρομή της απάντησης σε αυτό, αναγκάζουν, δηλαδή, τον αποδέκτη του μηνύματος να απαντήσει χρησιμοποιώντας την ίδια ή παρεμφερή ασφαλή διαδικασία.

Γνωστοί Αλγόριθμοι Κρυπτογράφησης

Στην ενότητα αυτή παρατίθενται συνοπτικά οι πιο γνωστοί αλγόριθμοι κρυπτογράφησης:

DES-DATA Encryption Standard:
Είναι ένα σώμα κρυπτογραφικών εντολών που δημιουργήθηκε από την IBM και πήρε έγκριση από την Αμερικάνικη κυβέρνηση το 1977. Χρησιμοποιεί ένα 56-bit κλειδί και χρησιμοποιεί μία ομάδα από 64 bits. Είναι σχετικά γρήγορος αλγόριθμος και χρησιμοποιείται για την κρυπτογράφηση μεγάλου όγκου δεδομένων, ταυτόχρονα.

Triple DES:
Βασίζεται στον DES αλγόριθμο. Κρυπτογραφεί μία ομάδα δεδομένων τρεις φορές, με τρία διαφορετικά κλειδιά. Έχει προταθεί σαν εναλλακτική λύση αντί του DES, γιατί υποστηρίζεται ότι τον τελευταίο καιρό έχει γίνει πιο εύκολο και πιο γρήγορο το "σπάσιμο" του DES αλγόριθμου.

RC2 και RC4:
Σχεδιάστηκαν από τον Ron Rivest (από εκεί προέρχεται το R στην RSA Data Security Inc.). Παρέχουν ποικιλία ως προς το μέγεθος του κλειδιού κρυπτογράφησης, για πολύ γρήγορη και μεγάλου όγκου κρυπτογράφηση. Οι δύο αυτοί αλγόριθμοι θεωρούνται λίγο πιο γρήγοροι από τον DES και μπορούν να γίνουν ακόμα πιο ασφαλείς αν επιλέξουμε μεγαλύτερο μήκος κλειδιού. Ο αλγόριθμος RC2 αποτελεί μία ομάδα (block) κρυπτογράφησης και μπορεί να χρησιμοποιηθεί στην θέση του DES. Ο RC4 είναι ένα "ρεύμα" (stream) ψηφιών κρυπτογράφησης και θεωρείται περίπου 10 φορές πιο γρήγορος από τον DES.

IDEA:
Ο International Data Encryption Algorithm δημιουργήθηκε το 1991 και σχεδιάστηκε να είναι ικανός για την πραγματοποίηση υπολογισμών στο λογισμικό. Προσφέρει πολύ δυνατή κρυπτογράφηση χρησιμοποιώντας ένα 128-bit κλειδί.

RSA:
Ονομάστηκε έτσι από τους σχεδιαστές του, Rivet, Shamir και Adelman. Είναι ένας αλγόριθμος "δημόσιου κλειδιού" (public-key) ο οποίος υποστηρίζει μια ποικιλία μήκους κλειδιών, καθώς επίσης ποικιλία όσον αφορά το μέγεθος του σώματος του κειμένου προς κρυπτογράφηση το απλό block κειμένου πρέπει να είναι μικρότερο από το μήκος του κλειδιού. Το συνηθισμένο μήκος κλειδιού είναι 512 bits.

Diffie-Hellman:
Αποτελεί το παλιότερο "δημόσιου κλειδιού" σύστημα κρυπτογράφησης, που ακόμα χρησιμοποιείται. Δεν υποστηρίζει κρυπτογράφηση ή ψηφιακές υπογραφές. Το σύστημα έχει σχεδιαστεί για να επιτρέπει στις δύο πλευρές να συμφωνούν με την χρήση ενός κατανεμημένου κλειδιού (shared key), ακόμα και αν το μόνο που κάνουν είναι να ανταλλάσσουν μηνύματα δημοσίως.

DSA:
Ο Digital Signature Algorithm σχεδιάστηκε από την NIST, στηρίχθηκε πάνω σε αυτό που αποκαλείται EL Gamal αλγόριθμος. Το σχήμα των υπογραφών χρησιμοποιεί το ίδιο είδος κλειδιών που χρησιμοποιεί και ο Diffie-Hellman αλγόριθμος και μπορεί να δημιουργήσει υπογραφές πιο γρήγορα από τον RSA. Έχοντας προωθηθεί από την NIST ως την DSS σύστημα, το Digital Signature standard, παρ΄όλη την αποδοχή του, απέχει ακόμα πολύ από το να παρέχει σιγουριά.

Έμπιστες Τρίτες Οντότητες (ΕΤΟ)

Εισαγωγικά
Η ραγδαία εξέλιξη της τεχνολογίας των πληροφοριών και η εύκολη πλέον πρόσβαση στις λεωφόρους των πληροφοριών, οδήγησε στην αύξηση των συναλλαγών μέσω του διαδικτύου. Απόρροια αυτών των εξελίξεων αποτέλεσε και η επιτακτική ανάγκη για διασφάλιση της ακεραιότητας των δεδομένων και προστασίας των πληροφοριών που διακινούνται στο δίκτυο. Για το σκοπό αυτό αναπτύχθηκαν τα τελευταία χρόνια μηχανισμοί ασφάλειας με μικρό κόστος για τον τελικό χρήστη και δυνατότητα υλοποίησης ασφαλών πλέον ηλεκτρονικών συναλλαγών. Θεωρείται λοιπόν απαραίτητη η ύπαρξη μιας αρχής που θα εξασφαλίζει την εμπιστευτικότητα και αυθεντικότητα των συναλλαγών και θα προσφέρει υπηρεσίες Έμπιστης Τρίτης Οντότητας.

Μία Έμπιστη Τρίτη Οντότητα, θα μπορούσε να οριστεί μία αρχή ασφαλείας ή μία υπηρεσία την οποία εμπιστεύονται άλλες οντότητες για την διασφάλιση των συναλλαγών τους, καθώς επίσης και για τις λειτουργίες-υπηρεσίες ασφαλείας που παρέχει.

Μία Έμπιστη Τρίτη Οντότητα παρέχει τους μηχανισμούς εκείνους μέσω των οποίων εξασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα και η αυθεντικότητα των ηλεκτρονικών συναλλαγών και των πληροφοριών που διακινούνται στο διαδίκτυο.
Μια ΕΤΟ προσδιορίζεται ως μια αρχή που εξυπηρετεί άλλες οντότητες. Οι οντότητες που πιστοποιούνται από μια ΕΤΟ μπορεί να περιλαμβάνουν τα άτομα που χρησιμοποιούν τις υπηρεσίες ενός οργανισμού, ή τους servers (εξυπηρετητές) του οργανισμού που προσφέρουν τις συγκεκριμένες υπηρεσίες.

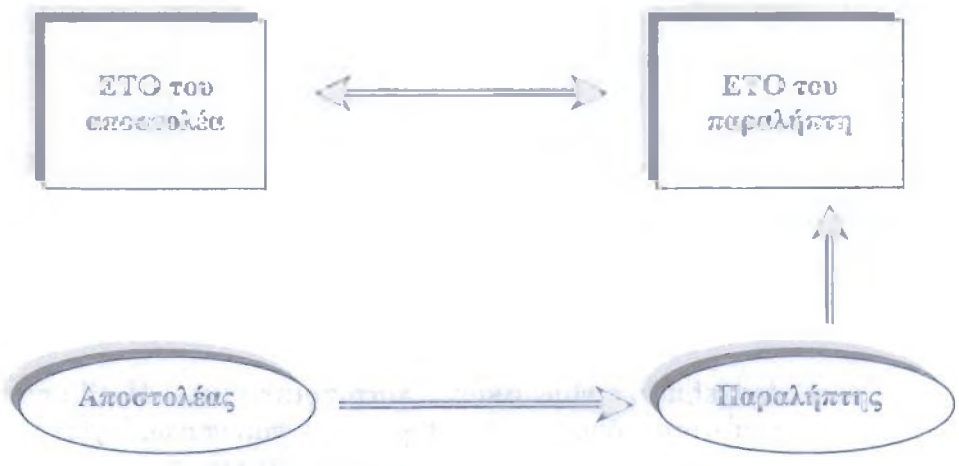
Μια Έμπιστη Τρίτη Οντότητα παρέχει ενεργεί είτε ως:

⇒ Αρχή Πιστοποίησης (certification Authority) είτε ως

⇒ Υπηρεσία καταλόγου (Registration), στην οποία καταγράφονται οι χρήστες και πελάτες της ΕΤΟ.

Ένα κλασσικό σενάριο λειτουργίας μιας ΕΤΟ είναι το ακόλουθο: Ο τελικός χρήστης είναι συνδεδεμένος στο web και μπορεί να επικοινωνήσει άμεσα με την Αρχή Πιστοποίησης, για να κάνει αίτηση ή να λάβει ένα νέο πιστοποιητικό.

Ουσιαστικά το πιστοποιητικό αυθεντικοποιεί την ταυτότητα του χρήστη στους servers άλλων οργανισμών. Η λειτουργία της αυθεντικοποίησης πραγματοποιείται ως εξής: όταν ένας χρήστης πρόκειται να επικοινωνήσει με servers άλλων οργανισμών για να πραγματοποιήσει κάποια ηλεκτρονική συναλλαγή ή απλώς να πάρει κάποιες πληροφορίες, αποστέλλει το πιστοποιητικό του στους servers αυτούς. Στη συνέχεια οι servers (παραλήπτες), ελέγχουν την ορθότητα του πιστοποιητικού και αν εξακριβώσουν την αυθεντικότητα αυτού, τότε παραχωρούν στο χρήστη τα ανάλογα δικαιώματα πρόσβασης στο server. Η εξακρίβωση της αυθεντικότητας του πιστοποιητικού πραγματοποιείται με τον έλεγχο της ψηφιακής υπογραφής η οποία είναι ενσωματωμένη στο πιστοποιητικό και ανήκει στην Αρχή Πιστοποίησης (σχήμα 5).



Σχήμα 5 : Σενάριο λειτουργίας ΕΤΟ

Τα χαρακτηριστικά που πρέπει να διαθέτει μια Έμπιστη Τρίτη Οντότητα έτσι ώστε αυτή να θεωρείται αποτελεσματική και με σαφής, περιεκτική λειτουργία, μπορούν να συνοψισθούν στα ακόλουθα: Η ΕΤΟ θα πρέπει:

⇒ Να λειτουργεί με ασφάλεια,

⇒ Να λειτουργεί μέσα σε συγκεκριμένο νομικό πλαίσιο,

⇒ Να μπορεί να προσφέρει μεγάλο πλήθος διαφορετικών υπηρεσιών,

⇒ Να διαθέτει ένα πορτφόλιο υποχρεωτικών υπηρεσιών που θα παρέχονται σ' όλους τους πελάτες,

⇒ Να ακολουθεί τα Ευρωπαϊκά ή τα διεθνή πρότυπα,

⇒ Να είναι σε θέση να παίζει τον ρόλο του διαμεσολαβητή (διαμεσολαβητή)

Λειτουργικές Απαιτήσεις της Έμπιστης Τρίτης Οντότητας

Οι λειτουργικές απαιτήσεις μιας Έμπιστης Τρίτης Οντότητας είναι οι ακόλουθες:

⇒ **Αποθήκευση και Αντιστοίχηση Ονόματος.** Η Έμπιστη Τρίτη Οντότητα χρησιμοποιεί την λειτουργία του Καταλόγου για να αποθηκεύσει τις πληροφορίες που αφορούν τους χρήστες. Οι πληροφορίες αυτές αποθηκεύονται με τέτοιο τρόπο έτσι ώστε να είναι προσβάσιμες από διάφορες υπηρεσίες και εφαρμογές σύμφωνα με κοινά αποδεκτά πρότυπα. Αρκετές φορές κρίνεται η δυνατότητα επέκτασης του καταλόγου ή η διασύνδεσή του με άλλους καταλόγους, προκειμένου να υπάρχει πρόσβαση σε πληροφορίες για οντότητες και από άλλα δίκτυα ή υπηρεσίες. Συνήθως, παρέχεται η δυνατότητα στους χρήστες και πελάτες μιας ΕΤΟ να έχουν πρόσβαση σε μια λίστα που περιέχει όλους τους χρήστες της ΕΤΟ, έτσι ώστε να είναι δυνατή η επικοινωνία μεταξύ των χρηστών.

⇒ **Διαχείριση ψηφιακών πιστοποιητικών.** Η Έμπιστη Τρίτη Οντότητα, όπως αναφέρθηκε και παραπάνω, έχει το δικαίωμα έκδοσης πιστοποιητικών. Συνεπώς έχει και την υποχρέωση σωστής διαχείρισης αυτών. Κάτι τέτοιο συνεπάγεται την υποστήριξη από την ΕΤΟ ασφαλούς επικοινωνίας. Η πρόσβαση μιας οντότητας στον server της ΕΤΟ με σκοπό την απόκτηση ή τον έλεγχο αυθεντικότητας ενός πιστοποιητικού, απαιτεί την ασφαλή αποθήκευση και επεξεργασία των δεδομένων του server. Με άλλα λόγια, κρίνεται απαραίτητη η κρυπτογραφημένη μεταφορά των δεδομένων που ανταλλάσσουν οι οντότητες-πελάτες της ΕΤΟ.

⇒ **Υπηρεσίες Ασφάλειας**. Οι υπηρεσίες ασφάλειας που παρέχονται από την ΕΤΟ στοχεύουν κυρίως στην εξασφάλιση της αυθεντικότητας του πιστοποιητικού που διαθέτει ο χρήστης, έτσι ώστε να αποδοθούν σε αυτόν τα ανάλογα δικαιώματα ή να αποκλειστεί η πρόσβασή του στο σύστημα πληροφοριών. Η διαδικασία της αυθεντικοποίησης αποσκοπεί στην εξακρίβωση της ταυτότητας την οποία ισχυρίζεται ότι ένα χρήστης έχει.

⇒ **Υπηρεσίες Ελέγχου και Εποπτείας**. Οι Έμπιστες Τρίτες Οντότητες πρέπει να διαθέτουν ένα μηχανισμό για την παρακολούθηση των συναλλαγών που λαμβάνουν μέρος στον server της επιχείρησης. Για το σκοπό αυτό, συνήθως χρησιμοποιούνται
αρχεία στα οποία αποθηκεύονται όλες οι ενέργειες που πραγματοποιούνται στα πλαίσια του οργανισμού. Η χρήση αρχείων για την αποθήκευση των στοιχείων των συναλλαγών προσφέρει τη δυνατότητα παραγωγής στατιστικών αναφορών που αφορούν τη λειτουργία της ΕΤΟ και τις πιστοποιημένες σε αυτή οντότητες.

Παράλληλα, υπάρχει πλέον ευκολία στην πραγματοποίηση ελέγχου για την ανίχνευση τυχόν σφαλμάτων ή παράνομών ενεργειών.
Ο έλεγχος της αυθεντικότητας του χρήστη γίνεται πριν την έναρξη οποιασδήποτε ηλεκτρονικής συναλλαγής και υλοποιείται με τη χρήση των πιστοποιητικών τα οποία έχουν χορηγηθεί στους χρήστες από την ΕΤΟ και φέρουν την ψηφιακή υπογραφή της. Ο έλεγχος αυτός πραγματοποιείται από τον server στον οποίο επιχειρεί να συνδεθεί ο χρήστης και η λειτουργία που ουσιαστικά συντελείτε είναι η αναζήτηση στους καταλόγους της ΕΤΟ με σκοπό να βρεθεί ο χρήστης που ζητά πρόσβαση στις υπηρεσίες του οργανισμού και να του αποδοθούν τα κατάλληλα δικαιώματα. Πρέπει να σημειώσουμε ότι το πιστοποιητικό που παραχωρείται στον χρήστη έχει κάποια ημερομηνία λήξης. Όταν το πιστοποιητικό πλέον δεν έχει ισχύ ανακαλείται και διαγράφεται από τον κατάλογο της ΕΤΟ.

Ο Ρόλος της Έμπιστης Τρίτης Οντότητας στην Ασφάλεια Δικτύων - Ασφάλεια μέσα από την Έμπιστη Τρίτη Οντότητα

Κατά την ανταλλαγή δεδομένων μεταξύ οντοτήτων σε ένα περιβάλλον κατανεμημένης επεξεργασίας, πέραν από τις κλασσικές απαιτήσεις σε υπηρεσίες ασφαλείας, υπάρχουν και απαιτήσεις ασφαλείας που σχετίζονται με τις ιδιότητες που αφορούν στις συναλλαγές (transactions) μεταξύ των εμπλεκόμενων οντοτήτων, όπως για παράδειγμα ύπαρξη εμπιστοσύνης στην ακεραιότητα των συναλλασσόμενων δεδομένων και προστασία έναντι των επιπτώσεων της μη συμμόρφωσης των συναλλασσομένων με τους υπάρχοντες κανόνες. Μεταξύ δύο συναλλαγών, ασφαλής θεωρείται εκείνη για την οποία εγγυάται το Πληροφοριακό Σύστημα (ΙΤ). Για να έχει τη δυνατότητα το Πληροφοριακό Σύστημα να εγγυηθεί την ασφάλεια των

συναλλαγών που ενεργούνται σε αυτό χρειάζεται να καταφύγει πολλές φορές στις υπηρεσίες μιας Έμπιστης Τρίτης Οντότητας που προστίθεται στο κατανεμημένο πληροφοριακό περιβάλλον και εγγυάται αυτή την ασφάλεια.

Η Έμπιστη Τρίτη Οντότητα (TTP), όπως δείχνει και το όνομα, αναμιγνύεται στην διαδικασία της συναλλαγής μεταξύ δύο οντοτήτων. Ανάλογα με τις παροχές των υπηρεσιών ασφαλείας, η TTP μπορεί να αποτελεί ξεχωριστή οντότητα, οπότε το όλο Κατανεμημένο Πληροφοριακό Σύστημα διαχωρίζεται στο μη ασφαλές του μέρος και στο ασφαλές του, που είναι η Τρίτη Οντότητα. Υπάρχουν όμως και περιπτώσεις παροχής υπηρεσιών ασφαλείας, όπου δεν υπάρχει ξεχωριστή Τρίτη Οντότητα. Σε αυτή την περίπτωση, σαν Έμπιστη Τρίτη Οντότητα θεωρείται ολόκληρο το Κατανεμημένο Πληροφοριακό Σύστημα . Η ανάμειξη της TTP στην διαδικασία συναλλαγής δημιουργεί άμεσες ή έμμεσες τροποποιήσεις σε αυτή την διαδικασία, που ανάγονται μεταξύ άλλων σε μετατροπές υπαρχόντων μηνυμάτων, παρεμβολές νέων μηνυμάτων, προσθήκες διαφόρων παραμέτρων, κλπ. Η TTP παρατηρεί ή και επιβάλλει την πολιτική ασφάλειας που ισχύει στο Πληροφοριακό Σύστημα και η εμπιστοσύνη που εμπεριέχεται σε αυτή δεν μπορεί να αλλοιωθεί από τα συναλλασσόμενα μέρη.

Ένας σημαντικός λόγος για την χρησιμοποίηση TTP είναι ότι είναι μια "τρίτη" οντότητα, γεγονός που της δίνει τη δυνατότητα να εμφανίζεται στα συναλλασσόμενα μέρη σαν μια ανεξάρτητη, αδιαφιλονίκητη οντότητα. Παίζει λοιπόν σημαντικό ρόλο για την εξασφάλιση αυτής της ανεξάρτητης, αδιαφιλονίκητης ιδιότητας, εκτός από το τεχνικό μέρος, και το νομικό πλαίσιο που θα επιτρέψει την σωστή επιλογή του φορέα που θα χειρίζεται και θα καθορίζει τις διαδικασίες λειτουργίας και ελέγχου, που θα χρησιμοποιούνται. Η δημιουργία ενός κοινά αποδεκτού νομικοτεχνικού πλαισίου λειτουργίας μιας TTP και γενικότερα ενός δικτύου TTPs παρέχει εχέγγυα για την οικοδόμηση της απαραίτητης εμπιστοσύνης που απαιτείται για την χρήση των TTPs από τους συναλλασσομένους.

Η αποκατάσταση αδιαμφισβήτητης εμπιστοσύνης στα TTPs για την εξασφάλιση υπηρεσιών ασφαλείας, θεωρείται μεγαλύτερη από την ίδια την εξασφάλιση των υπηρεσιών ασφαλείας.

Υπηρεσία των Έμπιστων Τρίτων Οντοτήτων

Τοπολογία

Μια Έμπιστη Τρίτη Οντότητα μπορεί να παρέχει τις υπηρεσίες της σ' ένα πληροφοριακό περιβάλλον τοπολογικά με τρεις διαφορετικούς τρόπους.

Σειριακή σύνδεση

Στη σειριακή σύνδεση (in-line TTP), όπως φαίνεται στο σχήμα η TTP υπεισέρχεται στον επικοινωνιακό δρόμο μεταξύ των συναλλασσομένων οντοτήτων. Η τοπολογία

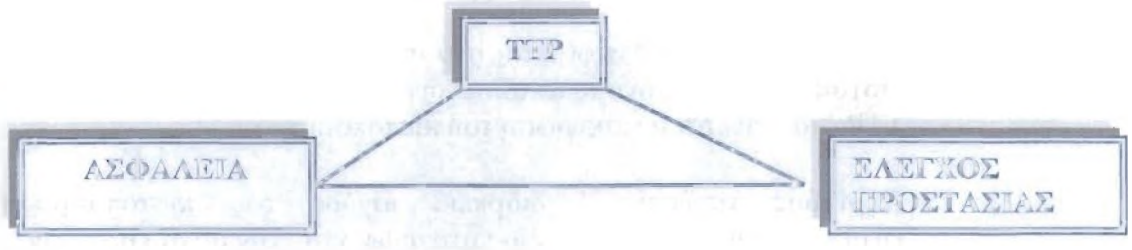
αυτή χρησιμοποιείται κυρίως λόγο της άμεσης ανάμειξης της Έμπιστης Τρίτης Οντότητας κατά την διάρκεια των συναλλαγών μεταξύ των συναλλασσομένων μερών. Η χρησιμοποίηση της TTP σε αυτού του είδους την τοπολογία είναι αναγκαστική.

Συνήθως σε τέτοιου είδους τοπολογία η TTP έχει την δυνατότητα να παρέχει όλες τις πιθανές υπηρεσίες ασφάλειας που μία Έμπιστη Τρίτη Οντότητα μπορεί να υποστηρίξει. Ενδεικτικά αναφέρονται ηλεκτρονικές υπηρεσίες σχετικές με τη συμβολαιογραφία, δημιουργία και διάθεση κρυπτογραφικών κλειδιών, πιστοποίηση κλειδιών, κλπ.

Σχήμα 6 : Τοπολογία σειριακής σύνδεσης

Παράλληλη ενεργή σύνδεση

Η παράλληλη ενεργή σύνδεση (on-line TTP) έχει την τοπολογία του σχήματος παρακάτω. Σε αυτή την περίπτωση η Έμπιστη Τρίτη Οντότητα βρίσκεται σε συνεχή επαφή με τις συναλλασσόμενες οντότητες, αλλά δεν είναι προφανές ότι συμμετέχει σε κάθε συναλλαγή τους. Η TTP δύναται να παρέχει όλες τις υπηρεσίες ασφάλειας που παρέχονται και στην προηγούμενη περίπτωση της σειριακής σύνδεσης.



Σχήμα 7 : Τοπολογία παράλληλης ενεργής σύνδεσης

αλλά επαφίεται στα συναλλασσόμενα μέρη να τις ζητήσουν και να τις χρησιμοποιήσουν. Όταν ζητηθεί η μεσολάβησή της, τότε αναμειγνύεται κατά τη διάρκεια της συναλλαγής όπως κατά τη σειριακή σύνδεση.

Παράλληλη ανενεργή σύνδεση

Η παράλληλη ανενεργή σύνδεση (off-line TTP), όπως φαίνεται και στο σχήμα παρακάτω, έχει τοπολογικά την ίδια σύνδεση με την προηγούμενη, αλλά διαφέρει ως προς την λειτουργία και τις δυνατότητες Έμπιστης Τρίτης Οντότητας. Οι υπηρεσίες ασφάλειας παρέχονται πριν ή μετά την συναλλαγή και ποτέ κατά την διάρκεια περιορίζοντας με αυτό τον τρόπο την γκάμα των υπηρεσιών αυτών. Παραδείγματα υπηρεσιών τέτοιου είδους είναι η ονοματοδοσία, η δημιουργία και πιστοποίηση των μυστικών κλειδιών, κλπ.

Δομή των Πιστοποιητικών

Ένας από τους πιο σημαντικούς ρόλους της TTP είναι η έκδοση και η επικύρωση/ επαλήθευση πιστοποιητικών (certificates). Για τον λόγο αυτό παρατίθεται ενδεικτικά η δομή ενός πιστοποιητικού που δείχνει τα στοιχεία που μπορεί να περιέχει.

Ενδεικτική δομή πιστοποιητικού

⇒ **Αριθμός έκδοσης:** Αναφέρεται στη συγκεκριμένη έκδοση της δομής του πιστοποιητικού. Κάθε φορά που θα αλλάζει η δομή του πιστοποιητικού σύμφωνα με τα διεθνή πρότυπα θα αλλάζει και ο αριθμός για να αντανακλά το χρησιμοποιούμενο πρότυπο.

⇒ **Σειριακός αριθμός:** δείχνει τον σειριακό αριθμό του συγκεκριμένου πιστοποιητικού που εκδίδεται από την TTP και είναι μοναδικός για κάθε πιστοποιητικό.

⇒ **Υπογραφή:** Σ' αυτό το πεδίο καθορίζεται ο αλγόριθμος ποτ χρησιμοποιείται από την TTP για να υπογράψει το πιστοποιητικό.

⇒ **Όνομα της TTP:** Αναφέρεται στο όνομα της TTP που εξέδωσε το πιστοποιητικό. Το όνομα αυτό συνδυάζεται με το δημόσιο κλειδί της TTP όταν γίνεται η επικύρωση του πιστοποιητικού.

⇒ **Περίοδος ισχύος:** Η διάρκεια ισχύος του πιστοποιητικού καταχωρείται σ' αυτό το πεδίο καταγράφοντας την αρχή και το τέλος αυτού του διαστήματος. Όσο μεγαλύτερο είναι αυτό το διάστημα τόσο μεγαλύτερη είναι η πιθανότητα διακύβευσης της ασφάλειας.

⇒ **Όνομα του κατόχου:** Σ' αυτό το πεδίο περιέχεται το όνομα του κατόχου του πιστοποιητικού που αντιστοιχεί σε κάποιο σύστημα καταλόγου.

⇒ **Δημόσιο κλειδί κατόχου:** Το πεδίο αυτό περιέχει το δημόσιο κλειδί του κατόχου του πιστοποιητικού και οποιαδήποτε άλλη σχετική πληροφορία.

Τα ονόματα που αναφέρθηκαν παραπάνω ενδείκνυται να στηρίζονται σε κάποιο ευρέως αποδεκτό πρότυπο συστήματος ονοματοδοσίας όπως για παράδειγμα το X.500 και X.509, ώστε να γίνεται πλήρης αξιοποίηση και εναρμόνιση των πρακτικών των διεθνών δικτύων.

Τα πιστοποιητικά αυτά συνδυάζονται με την χρήση έξυπνων καρτών που χρησιμοποιούν ηλεκτρονικές υπογραφές έτσι ώστε οι διάφορες εφαρμογές που αναφέρθηκαν προηγουμένως να λειτουργούν αυτόματα με πλήρη ασφάλεια και πίστη.

Διασύνδεση Έμπιστων Τρίτων Οντοτήτων

Οι Έμπιστες Τρίτες Οντότητες υπάρχουν και λειτουργούν συνήθως στα πλαίσια δικτύων, που πολλές φορές είναι διασυνδεδεμένα και υπερβαίνουν τα εθνικά όρια μιας χώρας. Όταν συμβαίνει αυτό θα πρέπει να ορίζεται ξεκάθαρα η περιοχή ευθύνης (domain) της κάθε TTP καθώς και οι διαδικασίες συνεργασίας μεταξύ τους. Ένας τρόπος συνεργασίας είναι η ιεράρχηση των περιοχών ευθύνης των TTPs καθορίζοντας έτσι την ιεράρχηση των ίδιων των TTPs. Με αυτόν τον τρόπο ορίζονται διεθνώς κοινά αποδεκτά επίπεδα TTPs και υπάρχει μια υψηλότερη ιεραρχικά TTP που είναι υπεύθυνη για την έκδοση πιστοποιητικών για τις αμέσως χαμηλότερα ιεραρχικά TTPs και καθεμία από αυτές για τις αμέσως χαμηλότερες.

Έτσι για παράδειγμα μπορεί να υπάρχει μια ύψιστη TTP ανά χώρα και όλες μαζί να αναφέρονται σε μια TTP ανά ήπειρο κοκ. Υπάρχει πάντα η δυνατότητα της εναλλακτικής λύσης της ύπαρξης διασύνδεσης TTPs στο ίδιο επίπεδο ακόμη και στο ύψιστο. Σε αυτή την περίπτωση απαιτούνται πρωτόκολλα επικοινωνίας μεταξύ των TTPs του ίδιου επιπέδου για την ανταλλαγή των σχετικών δεδομένων για την εξασφάλιση της σωστής παροχής των υπηρεσιών ασφαλείας. Η διασύνδεση αυτή των TTPs επιτρέπει την απεριόριστη χρήση των ηλεκτρονικών καρτών για ποικίλες εφαρμογές.

Βασικές Λειτουργίες Έμπιστων Τρίτων Οντοτήτων

Για να αντεπεξέλθει μια Έμπιστη Τρίτη Οντότητα στο ρόλο της, προβαίνει σε κάποιες βασικές λειτουργίες που στηρίζονται σε αυτοματοποιημένες ή μη διαδικασίες. Οι λειτουργίες αυτές απορρέουν από την υπάρχουσα πολιτική σε θέματα ασφάλειας. Χωρίζονται δε σε μη αυτοματοποιημένες, ή ημιαυτοματοποιημένες και αυτοματοποιημένες. Ένας ενδεικτικός κατάλογος τέτοιων βασικών λειτουργιών ακολουθεί.

Μη αυτοματοποιημένες λειτουργίες

⇒ **Ρυθμιστικού τύπου:** Τέτοιου είδους λειτουργίες αναφέρονται στη δημιουργία κανόνων, οδηγιών διοίκησης, αρχών λειτουργίας, κλπ που εφάπτονται της λειτουργίας των TTPs και συνήθως καθορίζονται διεθνώς από μεγάλους φορείς κοινών συμφερόντων.

⇒ **Επιτηρητικές:** Η ίδια η TTP έχει ανάγκη αναγνώρισης ότι τηρεί τα διεθνή πρότυπα και πρακτικές. Περιοδικά, λοιπόν, πρέπει να προβλέπονται διαδικασίες επικύρωσης της σωστής λειτουργίας των TTPs.

⇒ **Υλοποίησης υπηρεσιών:** Οι λειτουργίες αυτές εξασφαλίζουν την ορθή υλοποίηση διαφόρων υπηρεσιών που παρέχονται από μια TTP, συμπεριλαμβανομένων και των τεχνικών λεπτομερειών.

⇒ **Ελέγχου μιας TTP:** Τέτοιου είδους λειτουργίες αναφέρονται στον περιοδικό έλεγχο μιας TTP για την εξασφάλιση της τήρησης των κανόνων λειτουργίας της

Ημιαυτοματοποιημένες λειτουργίες

⇒ **Ασφάλειας συναλλαγής:** Με αυτή τη λειτουργία εξασφαλίζεται ο περιορισμός τυχόν ζημιών από τη μη ορθή εκτέλεση μιας συναλλαγής, λόγο αποτυχίας μερικής ή ολικής της λειτουργίας της TTP.

⇒ **Εγκατάστασης παραμέτρων:** Για κάθε προσφερόμενη υπηρεσία υπάρχουν αναγκαίες διαδικασίες που αφορούν στην καταχώρηση διαφόρων παραμέτρων στην TTP που είναι σχετικές με την συγκεκριμένη υπηρεσία.

⇒ **Αλλαγής, Διεύρυνσης, Απεγγραφής παραμέτρων:** Όλες αυτές οι λειτουργίες έχουν να κάνουν με τις παραμέτρους για τις προσφερόμενες υπηρεσίες που αναφέρθηκαν παραπάνω στη λειτουργία της εγκατάστασης.

Αυτοματοποιημένες λειτουργίες

⇒ **Παραγωγής Εμπιστευτικών Δεδομένων:** Με αυτές τις λειτουργίες παράγονται ή ενημερώνονται εμπιστευτικά δεδομένα υπηρεσιών ασφάλειας σχετικών με τις συναλλαγές. Τέτοιου είδους δεδομένα έχουν να κάνουν με την παρακολούθηση της ροής των πληροφοριών, με στοιχεία ελέγχου, κλπ.

⇒ **Επιβεβαίωσης Εμπιστευτικών Δεδομένων:** Οι λειτουργίες αυτές εξασφαλίζουν την πιστοποίηση διαφόρων δεδομένων που χρησιμοποιούνται από τις υπηρεσίες ασφάλειας.

⇒ **Εφοδιασμού Εμπιστευτικών Δεδομένων, Ελεγκτικών ιχνών, Αποδεικτικών στοιχείων:** Πρόκειται για παρεμφερείς λειτουργίες, που αφορούν στον εφοδιασμό και παραχώρηση στοιχείων σχετικών με τις υπηρεσίες ασφάλειας που παρέχονται από την TTP. Η παραχώρηση τέτοιων στοιχείων υπόκεινται στους περιορισμούς της υπάρχουσας στην TTP πολιτικής σε θέματα ασφαλείας.

⇒ **Εγκαθίδρυσης διαλειτουργικής πολιτικής ασφάλειας:** Η αυτοματοποιημένες αυτές λειτουργίες έχουν να κάνουν με την υποστήριξη των διαλειτουργιών μεταξύ TTPs που επιτυγχάνεται με την ανταλλαγή σχετικών παραμέτρων μεταξύ τους.

Όλες οι προαναφερθείσες λειτουργίες είναι ενδεικτικές και εξαρτάται από την κάθε TTP αν θα υλοποιηθούν όλες ή αν θα προστεθούν και άλλες. Ο βαθμός αξιοπιστίας της κάθε TTP εξαρτάται από τον αριθμό, τον τρόπο υλοποίησης και την βαρύτητα των λειτουργιών που έχει στο ρεπερτόριό της.

Απαιτήσεις σε Υπηρεσίες Ασφάλειας στα Δίκτυα

Εφαρμογές που απαιτούν Ασφάλεια

Η υποδομή που αναφέρθηκε στην προηγούμενη ενότητα καθίσταται αναγκαία λόγο των αυξανόμενων απαιτήσεων για ηλεκτρονικές συναλλαγές με την χρήση δικτύων υπολογιστών, που αναδύει προβλήματα που σχετίζονται με την εξασφάλιση της εγκυρότητας και της εμπιστοσύνης. Η επιτυχής αντιμετώπιση αυτών των προβλημάτων θα οδηγήσει τον κόσμο πιο κοντά στη εγκατάλειψη της χρήσης χαρτιού.

Η συναλλαγές που, εκ πρώτης όψης είναι ιδανικές για την χρήση της τεχνολογίας της Έμπιστης Τρίτης Οντότητας σχετίζονται με εφαρμογές στις περιοχές της υγείας, της οικονομίας, του εμπορίου με ηλεκτρονικά μέσα, των μεταφορών και γενικότερα υπηρεσιών που παρέχονται μέσα από τα τηλεπικοινωνιακά δίκτυα και τα δίκτυα υπολογιστών και απαιτούν νομικές συμφωνίες και κοστολογήσεις καθώς και χρεώσεις αυτών των υπηρεσιών. Οι συναλλαγές αυτές απαιτούν σήμερα την χρησιμοποίηση μεγάλου αριθμού ανθρώπινων πόρων και τη χρήση τεράστιων ποσοτήτων χαρτιού, η δε σωστή διαχείρισή τους καθίσταται εξαιρετικά δυσχερής.

Απαιτήσεις των εφαρμογών για υπηρεσίες ασφάλειας

Η επιτυχής χρήση των TTPs, πέραν από τη σωστή τεχνική λειτουργία τους, σχετίζεται σε πολλές περιπτώσεις με την συμπληρωματική στενή χρησιμοποίηση των ηλεκτρονικών υπογραφών που υλοποιούνται μέσα από την χρήση έξυπνων ηλεκτρονικών καρτών. Ο κύριος ρόλος των ηλεκτρονικών καρτών είναι η δημιουργία ασφαλών ηλεκτρονικών υπογραφών, δηλαδή υπογραφών που να μην επιδέχονται παραχάραξη. Η Έμπιστες Τρίτες Οντότητες είναι υπεύθυνες για την πιστοποίηση της εγκυρότητας αυτών των υπογραφών καθώς και για την έκδοση ηλεκτρονικών πιστοποιητικών εγκυρότητας.

Η χρησιμοποίηση ηλεκτρονικών συναλλαγών απαιτεί κατ' αρχή, την αναγνώριση και την πιστοποίηση της αυθεντικότητας των συναλλασσομένων μερών. Η χρήση διεθνών δικτύων απαιτεί την προσεκτική, σωστή και μονοσήμαντη, σε διεθνές επίπεδο, ονοματοδότηση των κοινά αποδεκτών αναγνωρισμένων μερών. Η διεθνής αυτή ονοματοδοσία των μερών θα πρέπει να συνοδεύεται από σωστές και ακριβείς διαδικασίες εγγραφής, αναθέσεις αρμοδιοτήτων και ευθυνών καθώς και από διαδικασίες ελέγχου των μερών και των οργανισμών στους οποίους αυτά ανήκουν. Η σωστή οργάνωση και ο έλεγχος των εμπλεκομένων μερών μέσα από τις διαδικασίες ονοματοδοσίας αποτελεί την βάση για την ορθή δημιουργία της υποδομής που απαιτείται και την εύκολη σχετικά εξασφάλιση της πιστοποίησης της αυθεντικότητας των συναλλασσομένων οντοτήτων.

Μετά την αναγνώριση και της ονοματοδοσίας των εμπλεκομένων οντοτήτων και της πιστοποίησης της αυθεντικότητάς τους, οι επόμενες απαιτήσεις των εφαρμογών σε υπηρεσίες ασφάλειας έχουν να κάνουν με την προστασία των συναλλαγών. Η προστασία αυτή σε περιβάλλον που χρησιμοποιεί την τεχνολογία των ηλεκτρονικών υπογραφών και των TTPs, έγκειται στην εξασφάλιση της ακεραιότητας και της εμπιστευτικότητας των δεδομένων των συναλλαγών ενάντια σε παράνομες ή κατά τύχη μεταποιήσεις ή αποκαλύψεις δεδομένων. Το προαναφερθέν περιβάλλον επιτρέπει την διαχείριση των μυστικών κλειδιών στα συστήματα κρυπτογραφίας που ενδείκνυται να χρησιμοποιούνται για την υποστήριξη αυτής της προστασίας.

Εκτός από τις παραπάνω υπηρεσίες ασφάλειας κατά την συναλλαγή, απαιτείται και η πιστοποίηση της ταυτότητας των συναλλασσομένων οντοτήτων με τέτοιο τρόπο ώστε να μην υπάρχει περίπτωση αμφισβήτησής τους και των ενεργειών τους αργότερα (non repudiation). Η ύπαρξη και οι ιδιότητες της Έμπιστης Τρίτης Οντότητας εξασφαλίζουν αυτήν την μία άρνηση της ταυτότητας και των ενεργειών που πηγάζουν από αυτή, γεγονός που έχει σοβαρές νομικές επεκτάσεις.

Πέραν από τις υπηρεσίες ασφάλειας που παρέχονται από το περιβάλλον που προαναφέρθηκε και του κύριου ρόλου του ως κέντρου πιστοποίησης, οι Έμπιστες Τρίτες Οντότητες παρέχουν διάφορες υπηρεσίες σχετικές με την κρυπτογραφία, όπως η αποθήκευση των μυστικών κλειδιών και κάποιων ευαίσθητων δεδομένων, η δημιουργία και πιστοποίηση ηλεκτρονικών υπογραφών, κλπ. Επίσης παίζουν

πρωταρχικό ρόλο στη διαχείριση των αρχείων εγγραφής και ονοματοδοσίας των οντοτήτων καθώς και στην διαχείριση της έκδοσης των πιστοποιητικών και των αρχείων που χρησιμοποιούνται γι' αυτά.

Η λειτουργία των Έμπιστων Τρίτων Οντοτήτων μέσα στα διεθνή δίκτυα υποδεικνύει την ανάγκη για την διασύνδεσή τους και για την εξασφάλιση της διεθνούς αναγνώρισής τους ως κέντρο εμπιστοσύνης. Θα πρέπει, λοιπόν, να υπάρχει ένα ελάχιστο κοινό όριο διαδικασιών και λειτουργιών καθώς και ένα επαρκές νομικό πλαίσιο λειτουργίας που να προσδίδει αυτή την εμπιστοσύνη.

Βασικές Πολιτικές Ασφάλειας

Ενδεικτικά, μερικές από τις πολιτικές ασφάλειας περιλαμβάνουν:

⇒ Γενική εταιρική πολιτική ασφάλειας

Κάθε τμήμα είναι υπεύθυνο για τον προσδιορισμό της δικής του πολιτικής ασφάλειας, που θα καθορίζει τους κανόνες προστασίας των συστημάτων, εφαρμογών, δεδομένων και διαδικασιών, ανάλογα με τις απειλές/ κινδύνους που έχουν προκύψει έπειτα από ανάλυση και πάντα με γνώμονα την αξία αυτών των πόρων. Όλα τα δεδομένα θα πρέπει να κατηγοριοποιούνται σύμφωνα με το σύστημα διαβάθμισης της εταιρίας.

⇒ Πολιτική ασφάλειας δεδομένων

Όλα τα σημαντικά δεδομένα και πληροφορίες ανήκουν σε συγκεκριμένο μέλος της επιχείρησης. Ο "κάτοχος" οφείλει να κατηγοριοποιεί τα δεδομένα σύμφωνα με το σύστημα διαβάθμισης της εταιρίας και είναι υπεύθυνος για την προστασία τους. Επίσης δηλώνει ποιοι έχουν πρόσβαση σε αυτά.

⇒ Διαβάθμιση της πληροφορίας

Σύστημα διαβάθμισης των δεδομένων, το οποίο κατηγοριοποιεί τις πληροφορίες σύμφωνα με το βαθμό σπουδαιότητάς τους (π.χ. μη εμπιστευτική πληροφορία, δεδομένα για εσωτερική χρήση, εμπιστευτική πληροφορία, πολύ ευαίσθητη εμπιστευτική πληροφορία), με στόχο την ανάλογη μεταχείριση από τους εξουσιοδοτημένους χρήστες.

Ασφάλεια Εκτεταμένων Δικτύων

Από τα προηγούμενα προκύπτει ότι η ασφάλεια των δικτύων, ιδιαίτερα των τοπικών (LAN), μπορεί να εξασφαλιστεί με ένα σωστό διαχειριστικό έλεγχο, ο οποίος με κατάλληλες διαδικασίες μπορεί να προστατεύσει τους χρήστες και το ίδιο το τοπικό δίκτυο ως ολότητα. Δεν είμαστε όμως σε θέση να ισχυριστούμε το ίδιο και για την περίπτωση των εκτεταμένων δικτύων (WAN). Και αυτό διότι στις περιπτώσεις αυτές η μετάδοση πληροφοριών γίνεται μεταξύ απομακρυσμένων φορέων ή οργανισμών που συνδέονται μεταξύ τους με δημόσια δίκτυα τα οποία δεν είναι ασφαλή.

Η διείσδυση σε ένα εκτεταμένο δίκτυο μπορεί να επιτευχθεί με κάποιο είδος "τηλεφωνικής κλήσης" και στη συνέχεια με τη χρήση της ταυτότητας (ID) και του συνθηματικού (password) ενός χρήστη να πραγματοποιηθεί η προσπέλαση σε κάποιο υπολογιστικό σύστημα. Επειδή η τεχνική των συνθηματικών δεν παρέχει αρκετή ασφάλεια πρέπει να δίνεται ιδιαίτερη έμφαση στη σωστή τους διαχείριση και την περιοδική τους αλλαγή. Επιπλέον, η επιλογή τους πρέπει να γίνεται κατά τρόπο που να καθιστά δυσκολότερη την αποκάλυψη τους κάτι όμως που δεν παρατηρείται συχνά στην πράξη καθώς οι χρήστες έχουν την τάση να επιλέγουν απλά συνθηματικά έτσι ώστε να τα ενθυμούνται εύκολα. Ένας άλλος τρόπος ασφαλούς σύνδεσης είναι η χρησιμοποίηση ειδικά προγραμματισμένων modems με ειδικό προεπιλεγμένο αριθμό κλήσης για κάθε χρήστη. Έτσι, ο χρήστης εισάγει την ταυτότητα και στη συνέχεια το modem αυτόματα καλεί τον καταχωρημένο αριθμό για να επιτευχθεί η σύνδεση στο σύστημα.

Όμως ασφαλέστερη σύνδεση, μπορεί να επιτευχθεί με τη χρήση έξυπνων καρτών και τεχνικών κρυπτογράφησης. Σε μια έξυπνη κάρτα μπορούμε να καταχωρήσουμε κάποιο μυστικό κλειδί για την ταυτοποίηση και αυθεντικοποίηση του χρήστη και την κρυπτογράφηση του συνθηματικού ή του μηνύματος πριν την μετάδοσή του στο υπολογιστικό σύστημα στο οποίο επιθυμεί να συνδεθεί. Η εμπιστευτικότητα των διακινούμενων πληροφοριών στα εκτεταμένα δίκτυα εξασφαλίζεται κυρίως με κρυπτογραφικές τεχνικές.

Ασφάλεια Ψηφιακών Δικτύων Ολοκληρωμένων Υπηρεσιών

Το ψηφιακό δίκτυο ολοκληρωμένων υπηρεσιών (Integrated Services Digital Network – ISDN) προήλθε από ένα τηλεφωνικό ολοκληρωμένο ψηφιακό δίκτυο, έτσι ώστε να παρέχει end-to-end ψηφιακές συνδέσεις και να υποστηρίζει διάφορες μορφές πληροφοριών (π.χ. ήχο), τις οποίες οι χρήστες μπορούν να προσπελάσουν με την βοήθεια των προτύπων πολλαπλού σκοπού μέσω επικοινωνίας χρηστών. Ο βασικός σκοπός του ISDN είναι η παροχή μιας ολοκληρωμένης επικοινωνίας με το λιγότερο δυνατό κόστος στο χώρο που χρησιμοποιείται.

Το ISDN έχει τρεις τύπους και χρησιμοποιείται από πολλούς κατασκευαστές που έχουν δημιουργήσει διάφορες εκδόσεις του. Τα κύρια πλεονεκτήματα του είναι το μικρό κόστος και η ευελιξία που παρέχει σε κάθε χρήστη. Όμως, η αδυναμία ορισμένων χρηστών να κατανοήσουν το βασικό σκοπό του ISDN οδήγησε στην άποψη ότι δεν παρέχει σημαντικές υπηρεσίες. Παρόλα αυτά, η αξιοπιστία, τα προβλήματα λογισμικού (software bugs), η συνδετικότητα (connectivity) και η ασφάλεια είναι τα μελλοντικά και αναγκαία σημεία βελτίωσής του.

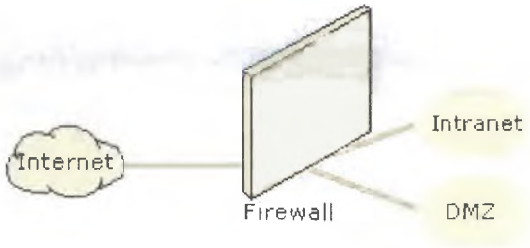
Το βασικότερο πρόβλημα ασφάλειας είναι η αναγνώριση της ταυτότητας του αποστολέα μιας τηλεφωνικής γραμμής (Calling Line Identity). Ο παραλήπτης μπορεί να γνωρίζει κάθε φορά από πού προέρχεται το τηλεφώνημα και να το αποδέχεται ή να το απορρίπτει. Όμως, αν η δυνατότητα αυτή είναι σταθερή και όχι επιλογή του χρήστη τότε υπάρχει παραβίαση των προσωπικών δικαιωμάτων του. Άλλο πρόβλημα ασφάλειας είναι τα μέσα σύνδεσης που χρησιμοποιεί το ISDN και που μπορεί να αντιμετωπισθεί με την κρυπτογραφία, τις ψηφιακές υπογραφές και την ανταλλαγή κλειδιών.

Συμπεραίνεται ότι, το ISDN, όπως και άλλες παρόμοιες μορφές δικτύων (πρότυπα), μπορούν να αποτελέσουν μια ικανοποιητική λύση στο πρόβλημα της ασφάλειας δικτύων, αρκεί να αντιμετωπισθούν τα διάφορα προβλήματα που παρουσιάζουν.

Πολιτικές Ασφάλειας Δικτύων

Το Internet έχει επιφέρει πραγματική επανάσταση στον τρόπο με τον οποίο λειτουργούν οι επιχειρήσεις, "πιέζοντάς" τις είτε να εδραιώσουν την παρουσία τους στον πολλά υποσχόμενο κόσμο του ηλεκτρονικού επιχειρείν, είτε να ρισκάρουν το μέλλον τους μένοντας ενδεχομένως και εκτός αγοράς. Δυστυχώς, η πίεση αυτή οδηγεί συχνά τις εταιρίες να μπαίνουν βιαστικά στο "παιχνίδι", προκειμένου να μη χάσουν το ανταγωνιστικό τους πλεονέκτημα, παραβλέποντας έτσι ή αναβάλλοντας την υλοποίηση πολιτικών και μηχανισμών για τη δημιουργία ενός ασφαλούς ηλεκτρονικού περιβάλλοντος. Αναμφισβήτητα οι απειλές είναι πλέον πάρα πολλές (ιοί, κακόβουλες επιθέσεις σε εταιρικές βάσεις δεδομένων, λογαριασμοί και στοιχεία πελατών που εκτίθενται σε κοινή χρήση, κ.λ.π.) και αυξάνονται ραγδαία. Θα πρέπει λοιπόν η κάθε επιχείρηση που δραστηριοποιείται στο δικτυωμένο περιβάλλον να δίνει ιδιαίτερη βαρύτητα στην αξιοπιστία και την ασφάλεια των ηλεκτρονικών συναλλαγών.

Πολιτική ασφάλειας DMZ



Στην DMZ (Demilitarized Zone - "αποστρατικοποιημένη ζώνη") αναλύονται οι επιχειρηματικές ανάγκες και η στρατηγική της επιχείρησης όσον αφορά στο Internet και τοποθετούνται συστήματα που παρέχουν υπηρεσίες προσβάσιμες από οποιονδήποτε μέσω του Διαδικτύου. Όλες λοιπόν οι μηχανές, συμπεριλαμβανομένων και των δρομολογητών, switches και υπολογιστών, καθώς και το ανάλογο λογισμικό θα πρέπει να ακολουθούν την πολιτική αυτή.

Συγκεκριμένα, θα πρέπει να λαμβάνονται υπόψη τα παρακάτω:

⇒ Θα πρέπει κατ' αρχάς να είναι ξεκάθαρο ποιοι είναι οι υπεύθυνοι για τη διαχείριση των συστημάτων στην DMZ. Στη συνέχεια, όλος ο εξοπλισμός, οι εφαρμογές και οι κωδικοί πρόσβασης που τοποθετούνται σε αυτή τη ζώνη θα πρέπει να εγκρίνονται από το Τμήμα Ασφάλειας και να είναι καταγεγραμμένοι με λεπτομέρεια. Αλλαγές στον υπάρχοντα εξοπλισμό ή προσθήκη νέου θα πρέπει να γίνονται στο πλαίσιο της αντίστοιχης πολιτικής.

⇒ Θα πρέπει να γίνεται λεπτομερής καταγραφή της κίνησης αλλά και αποτελεσματικός έλεγχος της καταγραφής με αυτοματοποιημένο τρόπο από τους υπεύθυνους του συστήματος. Ειδικότερα, πρέπει να καταγράφονται οι αποτυχημένες προσπάθειες πρόσβασης, παράκαμψης δικαιωμάτων καθώς και η μη τήρηση της πολιτικής πρόσβασης σε αυτά.

⇒ Ποτέ δεν θα πρέπει να χρησιμοποιείται λογαριασμός συστήματος (admin-root) για κάτι το οποίο μπορεί να γίνει με απλό λογαριασμό που έχει λιγότερα δικαιώματα.

⇒ Όλα τα συστήματα θα πρέπει να είναι ενημερωμένα με τα τελευταία patches/hot fixes (προγράμματα διόρθωσης κάποιου προβλήματος ασφαλείας) των κατασκευαστών τους, ακόμη και για τις υπηρεσίες που δεν είναι ενεργοποιημένες.

⇒ Οι υπεύθυνοι των συστημάτων οφείλουν να είναι εκπαιδευμένοι και ενημερωμένοι για αυτά.

⇒ Εφαρμογές και υπηρεσίες που δεν χρησιμοποιούνται θα πρέπει να απενεργοποιούνται, ενώ όσες δεν είναι διαθέσιμες σε όλους να προστατεύονται με έλεγχο πρόσβασης και ταυτοποίηση υψηλής ασφάλειας.

⇒ Σε τακτά χρονικά διαστήματα θα πρέπει να γίνεται καταγραφή των συστημάτων από το Τμήμα Ασφάλειας της εταιρίας αλλά και από τρίτους για περισσότερη αντικειμενικότητα.

Πολιτική ασφάλειας Firewall

Firewall αποκαλείται το λογισμικό που ελέγχει ή και απαγορεύει την απομακρυσμένη πρόσβαση σε ένα υπολογιστή, ασκώντας παράλληλο έλεγχο στα εισερχόμενα / εξερχόμενα δεδομένα από και προς αυτόν. Το Firewall μπορεί να εγκατασταθεί ως μέρος μιας ολοκληρωμένης "σουίτας" προγραμμάτων ασφαλείας (Norton & McAfee Internet Security κλπ) ή ακόμη και ως ενσωματωμένο χαρακτηριστικό ενός λειτουργικού συστήματος (Linux).Οι λειτουργίες ελέγχου της εξερχόμενης κυκλοφορίας (traffic) θα πρέπει να είναι ένα από τα πιο σημαντικά κριτήρια επιλογής Internet firewall αφού είναι αυτές που ρυθμίζουν τις επιλογές αποδοχής ή απόρριψης (πρόσκαιρης ή μόνιμης) της αποστολής των packets που επιχειρεί να στείλει μια εφαρμογή

Η πολιτική ασφάλειας δικτύου με τη χρήση firewall θα πρέπει γενικά να ακολουθεί τα εξής:

⇒ Όλες οι συνδέσεις από το δίκτυο της εταιρίας προς το Internet θα πρέπει να γίνονται μέσω του Firewall (software ή hardware που αποτρέπει τις "επιθέσεις" σε κάποιο προσωπικό υπολογιστή ή σε ένα δίκτυο).

⇒ Θα πρέπει να είναι ξεκάθαρο ποιοι είναι οι υπεύθυνοι για τα firewalls, οι οποίοι και τα διαχειρίζονται.

⇒ Τα firewalls θα πρέπει να παρακολουθούνται και να ελέγχονται σε τακτά χρονικά διαστήματα (audits).

⇒ Εισερχόμενες συνδέσεις από το Internet θα πρέπει να χρησιμοποιούν προηγμένους μηχανισμούς ταυτοποίησης/ αναγνώρισης, π.χ. με κωδικούς μιας χρήσης. Το ίδιο ισχύει και για τους λογαριασμούς των διαχειριστών.

⇒ Όλες οι υπηρεσίες/ εφαρμογές που δεν χρειάζονται θα πρέπει να είναι απενεργοποιημένες.

⇒ Όλα τα λειτουργικά θα πρέπει να είναι ενημερωμένα με τα τελευταία patches/hot fixes των κατασκευαστών τους, ακόμη και για τις υπηρεσίες που δεν είναι ενεργοποιημένες.

⇒ Οι υπεύθυνοι των συστημάτων θα πρέπει να είναι εκπαιδευμένοι και ενημερωμένοι για αυτά.

⇒ Το firewall θα πρέπει να είναι διαθέσιμο όλο το εικοσιτετράωρο.

⇒ Όλες οι αλλαγές και οι αναβαθμίσεις θα πρέπει να καταγράφονται και να ακολουθούν την αντίστοιχη πολιτική.

⇒ Θα πρέπει να υπάρχει γρήγορη και αποτελεσματική ενημέρωση σε περίπτωση που κάποιο service δεν λειτουργεί.

Πολιτική ασφάλειας ασύρματων δικτύων

Η χρήση των ασύρματων δικτύων προσφέρει πολλά πλεονεκτήματα, όπως ευελιξία, γρήγορη υλοποίηση και χαμηλό κόστος χρήσης. Το πρόβλημα έγκειται στο ότι ο ασύρματος εξοπλισμός όλων σχεδόν των κατασκευαστών φθάνει στις εταιρίες με τις λειτουργίες ασφάλειας απενεργοποιημένες, καθώς δίνεται έμφαση στην εύκολη και απλή χρήση του. Η πολιτική ασφάλειας ασύρματων δικτύων θα πρέπει να καλύπτει όλο τον ασύρματο εξοπλισμό, όπως σημεία πρόσβασης (access points), υπολογιστές με ασύρματες κάρτες, υπολογιστές παλάμης κ.λ.π. που συνδέονται στο εταιρικό δίκτυο.

Συγκεκριμένα:

⇒ Όλα τα σημεία πρόσβασης (access points), σταθμοί βάσης (base stations), και ασύρματες κάρτες θα πρέπει να εγκρίνονται και να καταγράφονται από το Τμήμα Ασφάλειας της εταιρίας και να προέρχονται από κατασκευαστές που εγκρίνει το παραπάνω τμήμα.

⇒ Η σχεδίαση και υλοποίηση του δικτύου θα πρέπει να γίνεται προσεκτικά, έτσι ώστε να παρέχεται κάλυψη μόνο σε σημεία/ περιοχές όπου χρειάζεται.

⇒ Όλες οι ασύρματες συσκευές θα πρέπει να λειτουργούν μέσω ενός VPN (Ιδεατό Ιδιωτικό Δίκτυο) για κρυπτογράφηση με προηγμένους μηχανισμούς ταυτοποίησης/ αναγνωρισιμότητας.

Πολιτική ασφάλειας απομακρυσμένης πρόσβασης

Σε πολλές περιπτώσεις είναι απαραίτητη η απομακρυσμένη πρόσβαση κάποιου χρήστη στο εταιρικό δίκτυο. Μερικές φορές είναι αναγκαίο η δυνατότητα αυτή να δίνεται ακόμη και σε εξωτερικούς συνεργάτες, προμηθευτές ή και πελάτες. Οι απομακρυσμένες συνδέσεις επιτυγχάνονται με διάφορους τρόπους, όπως με dial-in modems, frame relay, DSL, VPN, κλπ.

Οι κανόνες που ορίζουν το γενικό πλαίσιο χρήσης της απομακρυσμένης πρόσβασης συνοψίζονται στα παρακάτω:

⇒ Οι χρήστες είναι υποχρεωμένοι να μην παρακάμπτουν τα δικαιώματα πρόσβασης που έχουν με τη σύνδεση αυτή.

⇒ Δεν θα πρέπει να κάνουν χρήση της σύνδεσης αυτής για προσωπικούς λόγους, π.χ. Internet, παρά μόνο για σκοπούς που έχουν άμεση σχέση με την εργασία τους.

⇒ Όταν μεταφέρουν αρχεία μέσω αυτής της σύνδεσης, οφείλουν να τηρούν την πολιτική ασφάλειας που ισχύει για τις διαβαθμισμένες πληροφορίες (κρυπτογράφηση, ταυτοποίηση). Επίσης θα πρέπει να τηρούν τις αντίστοιχες πολιτικές χρήσης Διαδικτύου και ηλεκτρονικού ταχυδρομείου.

⇒ Είναι απαραίτητο να υπάρχουν οι κατάλληλοι μηχανισμοί που να ελέγχουν την απομακρυσμένη σύνδεση και να διαχειρίζονται από το Τμήμα Ασφάλειας της εταιρίας.

⇒ Ο έλεγχος πρόσβασης θα πρέπει να γίνεται με προηγμένους μηχανισμούς ταυτοποίησης, π.χ. κωδικοί μιας χρήσης, PKI/δημόσια και ιδιωτικά κλειδιά.

⇒ Οι υπολογιστές που είναι συνδεδεμένοι με το εταιρικό δίκτυο δεν θα είναι συνδεδεμένοι και με άλλο δίκτυο ταυτόχρονα.

⇒ Ο εξοπλισμός που χρησιμοποιείται για τις απομακρυσμένες συνδέσεις θα πρέπει να εγκρίνεται από το Τμήμα Ασφάλειας και να προβλέπει μηχανισμούς ταυτοποίησης/ αναγνώρισης.

⇒ Όλοι οι υπολογιστές που χρησιμοποιούνται θα πρέπει να διαθέτουν ενημερωμένο λογισμικό καταπολέμησης ιών (anti-virus).

Οι πολιτικές ασφάλειας δικτύων που περιγράφονται παραπάνω αποτελούν πραγματική ανάγκη για τις σύγχρονες επιχειρήσεις που βασίζονται στην προστασία και ασφαλή ανταλλαγή ευαίσθητων πληροφοριών, τόσο των ίδιων των εταιριών όσο

και των πελατών τους. Ωστόσο, όλο το ανθρώπινο δυναμικό των επιχειρήσεων οφείλει να είναι σωστά εκπαιδευμένο και πάντοτε ενημερωμένο για τους υφιστάμενους κινδύνους σε ένα δικτυωμένο περιβάλλον, προκειμένου να τηρούνται όλες οι πολιτικές ασφάλειας και να ελαχιστοποιείται το ρίσκο απώλειας ή διαρροής διαβαθμισμένου υλικού.

Πολιτικές Ασφάλειας Προσωπικού

Κωδικοί πρόσβασης

Στα περισσότερα συστήματα οι κωδικοί πρόσβασης αποτελούν την πρώτη δικλείδα ασφαλείας, γι' αυτό και είναι σημαντικό η χρήση τους να είναι προσεκτική και αξιόπιστη. Οι χρήστες δεν πρέπει να μοιράζονται τους λογαριασμούς και τους κωδικούς τους με φίλους, γνωστούς ή συγγενείς, ούτε να δίνουν τις παραπάνω πληροφορίες μέσω τηλεφώνου ή ηλεκτρονικού ταχυδρομείου.

Οι κωδικοί πρόσβασης θα πρέπει να αλλάζουν κάθε τρεις μήνες, ενώ οι χρήστες των οποίων οι λογαριασμοί ανήκουν σε ομάδες με περισσότερα δικαιώματα, π.χ. διαχειριστές συστημάτων ή εφαρμογών, θα πρέπει να έχουν ξεχωριστούς κωδικούς για όλους τους υπόλοιπους λογαριασμούς τους.

Οι χρήστες δεν θα πρέπει να γράφουν τους κωδικούς τους σε χαρτί και να το αφήνουν στο γραφείο τους. Ποτέ επίσης δεν θα πρέπει να αποθηκεύονται οι κωδικοί ηλεκτρονικά σε υπολογιστή ή κινητό χωρίς κρυπτογράφηση.

Οι υπεύθυνοι ασφαλείας της εταιρίας οφείλουν σε τακτά χρονικά διαστήματα να τρέχουν προγράμματα τα οποία "σπάνε" τους κωδικούς, προκειμένου να εντοπίζουν τυχόν αδυναμίες του συστήματος και να αλλάζουν αμέσως τους κωδικούς που προσπέλασαν. Επίσης, οι χρήστες θα πρέπει να είναι ενημερωμένοι για τις δυνατότητες αυτών των προγραμμάτων, τον τρόπο λειτουργίας τους και το βαθμό επιτυχίας τους.

Τέλος, κάθε σύστημα θα πρέπει να ελέγχει το περιεχόμενο του κωδικού ώστε να τον απορρίπτει εφόσον δεν πληρεί τους όρους του συστήματος.

Χρήση Internet

Στις περισσότερες εταιρίες η χρήση του Διαδικτύου αποτελεί ένα από τα κυριότερα εργαλεία για τη διεκπεραίωση καθημερινών, βασικών λειτουργιών. Οι κίνδυνοι όμως είναι αρκετοί. Για παράδειγμα, οι πληροφορίες που αποστέλλονται μέσω Internet χωρίς τη λήψη ειδικών μέτρων, μπορούν να διαβαστούν ή και να αλλαχθούν. Το εσωτερικό δίκτυο μιας εταιρίας μπορεί να γίνει στόχος κακόβουλων ενεργειών και να καταστεί αδύνατη η πρόσβαση από τους εξουσιοδοτημένους χρήστες, με αποτέλεσμα να καταργούνται οι όροι που αναφέρθηκαν παραπάνω, όπως "εμπιστευτικότητα", "ακεραιότητα" και "διαθεσιμότητα".

Για τους λόγους αυτούς, μεγάλη προσοχή θα πρέπει να δοθεί στη χρήση του Διαδικτύου. Οι χρήστες θα πρέπει να είναι ενημερωμένοι για τους ενδεχόμενους κινδύνους και η αντίστοιχη πολιτική πρόσβασης και χρήσης του να είναι γνωστή σε όλους.

Συγκεκριμένα:

⇒ Οι χρήστες θα πρέπει να χρησιμοποιούν το Internet μόνο για σκοπούς που εξυπηρετούν και έχουν άμεση σχέση με την εργασία τους.

⇒ Η πρόσβαση στο Διαδίκτυο θα πρέπει να γίνεται μόνο μέσα από συγκεκριμένες εξόδους (gateways) που τηρούν τους μηχανισμούς ελέγχου και την πολιτική ασφάλειας της εταιρίας.

⇒ Οι servers (εξυπηρετητές) που περιέχουν διαβαθμισμένες πληροφορίες δεν πρέπει να είναι προσβάσιμοι από το Διαδίκτυο με απλό λογισμικό πλοήγησης.

⇒ Θα πρέπει να υπάρχει καθορισμός του περιεχομένου που θα μπορούν να επισκέπτονται οι χρήστες (μη πορνογραφικό, ρατσιστικό κ.λ.π.), συγκεκριμένων ωρών για χρήση του Internet που δεν έχει σχέση με την εργασία, του είδους αρχείων που απαγορεύεται να "κατεβάζουν" οι χρήστες, όπως μη πιστοποιημένο λογισμικό, λογισμικό χωρίς άδεια χρήσης, μουσικά αρχεία κ.λ.π. και καθορισμός όσων έχουν δικαίωμα χρήσης e-mail.

Χρήση ηλεκτρονικού ταχυδρομείου

Το ηλεκτρονικό ταχυδρομείο είναι η πιο διαδεδομένη εφαρμογή επικοινωνίας σήμερα, καθώς είναι αποτελεσματικό, εύκολο στη χρήση του και το κόστος του χαμηλό. Ταυτόχρονα όμως, και αυτό εγκυμονεί κινδύνους, ειδικά όταν

ανταλλάσσονται ευαίσθητες και εμπιστευτικές πληροφορίες, μιας και οι υπάρχοντες μηχανισμοί ελέγχου δεν το καθιστούν απόλυτα ασφαλές μέσο.

Η αντίστοιχη πολιτική θα πρέπει να προσδιορίζει τα ακόλουθα:

⇒ Το ηλεκτρονικό ταχυδρομείο είναι εταιρικός πόρος και όχι προσωπικός.

⇒ Οι χρήστες θα πρέπει να ενημερώνονται και να εκπαιδεύονται για τους σχετικούς κινδύνους.

⇒ Σε καμία περίπτωση δεν θα πρέπει να ανοίγουν μηνύματα και να τρέχουν προγράμματα από αποστολείς άγνωστης ταυτότητας.

⇒ Δεν θα πρέπει να στέλνουν ή να ανοίγουν μηνύματα και αρχεία με περιεχόμενο ρατσιστικό, πορνογραφικό κ.λ.π.

Όταν είναι αναγκαίο να σταλούν μέσω ηλεκτρονικού ταχυδρομείου εμπιστευτικά αρχεία, αυτά πάντοτε θα στέλνονται κρυπτογραφημένα με αλγορίθμους υψηλής ασφάλειας. Επίσης θα πρέπει να γίνεται χρήση υποδομών δημόσιων κλειδιών, PKI, έτσι ώστε να υπάρχει η δυνατότητα ψηφιακής υπογραφής/ πιστοποίησης.

Χρήση φορητών Η/Υ

Η χρήση φορητών υπολογιστών (laptops) προσφέρει πολλά πλεονεκτήματα, όπως ευελιξία και παραγωγικότητα, ακόμη και όταν δεν είμαστε στο γραφείο. Ταυτόχρονα, η μείωση του κόστους αγοράς τους με την ολοένα αυξανόμενη ισχύ τους τα καθιστά προσιτά σε όλους. Γι' αυτό είναι απαραίτητη και η κατάρτιση αντίστοιχης πολιτικής ασφάλειας, που να καλύπτει τη χρήση τους:

⇒ Οι χρήστες θα πρέπει να είναι ενημερωμένοι για τους κινδύνους που απορρέουν από τη χρήση φορητών υπολογιστών.

⇒ Οι κάτοχοι είναι υπεύθυνοι για την ασφάλειά τους εντός και εκτός εταιρίας. Όταν βρίσκονται μέσα στην εταιρία θα πρέπει να είναι κλειδωμένοι σε ασφαλές μέρος για την αποφυγή κλοπής.

⇒ Όλοι οι φορητοί υπολογιστές θα πρέπει να είναι ενεργοποιημένοι από το Τμήμα Πληροφορικής, με λειτουργικά που δεν επιτρέπουν σε απλούς χρήστες να έχουν καθολική πρόσβαση στο σύστημα (Unix, NT).

⇒ Όλοι οι φορητοί υπολογιστές που περιέχουν διαβαθμισμένη πληροφορία θα πρέπει να διαθέτουν κρυπτογράφηση στο δίσκο, έτσι ώστε ακόμη και αν κλαπούν, να είναι δύσκολη η πρόσβαση.

⇒ Η χρήση κωδικών κατά την εκκίνηση του υπολογιστή προσφέρει κάποια προστασία.

⇒ Οι χρήστες δεν θα πρέπει να αποθηκεύουν αρχεία με κωδικούς που δίνουν πρόσβαση στο δίκτυο της εταιρίας, παρά μόνο αν είναι κρυπτογραφημένα.

⇒ Επίσης δεν θα πρέπει να στέλνουν διαβαθμισμένα αρχεία από τους φορητούς Η/Υ μέσω Internet ή δικτύου κινητής τηλεφωνίας, παρά μόνο όταν αυτά κρυπτογραφούνται.

⇒ Όταν χρησιμοποιούν το modem για σύνδεση με το εταιρικό δίκτυο θα πρέπει να ακολουθείται η αντίστοιχη πολιτική πρόσβασης δικτύου.

Οι πολιτικές ασφάλειας θα πρέπει να περιγράφουν το πλαίσιο χρήσης των πόρων της εταιρίας. Θα πρέπει να είναι απλές, κατανοητές, να μη χρειάζονται συχνές αλλαγές και να ανταποκρίνονται πάντοτε στις ανάγκες λειτουργίας της επιχείρησης. Οι πολιτικές αυτές προσδιορίζουν και τις διαδικασίες/ μηχανισμούς που θα χρησιμοποιηθούν για να τις ενεργοποιήσουν. Θα πρέπει επίσης να προβλέπουν τα μέτρα που θα λαμβάνονται εναντίον αυτών που τις παραβαίνουν. Η διοίκηση της εταιρίας είναι υπεύθυνη για την υλοποίησή τους, και χωρίς τη δική της υποστήριξη κανένα μέτρο ασφαλείας δεν μπορεί να πετύχει και να δουλέψει σωστά.

Βασικές Υπηρεσίες Ασφάλειας Δικτύου

Η υπηρεσία ασφάλειας είναι μια δραστηριότητα η οποία ενισχύει την ασφάλεια ενός πληροφοριακού συστήματος και του δικτύου υπολογιστών μέσω του οποίου υλοποιείται. Από τεχνική άποψη, η παροχή των υπηρεσιών ασφάλειας σε περιβάλλοντα δικτύων υπολογιστών είναι περιπλοκότερη από ότι σε απομονωμένα συγκεντρωτικά συστήματα. Επίσης, η ενσωμάτωση διαφόρων τεχνικών μπορεί να έχει αρνητική επίπτωση στην αποδοτικότητα του δικτύου καθώς απαιτείται η κατανάλωση υπολογιστικών πόρων από το σύστημα διαχείρισης των υπηρεσιών ασφάλειας. Για αυτόν τον λόγο η εισαγωγή υπηρεσιών ασφάλειας σε ένα δίκτυο πρέπει να γίνεται κατά τρόπο ώστε η επίπτωσή τους στη συνολική του αποδοτικότητα να είναι η ελάχιστη δυνατή.

Οι υπηρεσίες ασφάλειας, που ορίζονται στα πλαίσια του μοντέλου αναφοράς (Open Systems Interconnection-OSI) για τη διασύνδεση ανοικτών συστημάτων είναι: η αυθεντικοποίηση (authentication), ο έλεγχος προσπέλασης (access control), η εμπιστευτικότητα (confidentiality), η ακεραιότητα (integrity) και ο καταλογισμός ευθύνης (non-repudiation). Αν και πολλές από τις υπηρεσίες αυτές μπορούν να παρέχονται στα περισσότερα από τα επτά επίπεδα του μοντέλου αναφοράς OSI, (πίνακας 1) τελευταία υποστηρίζεται ότι οι υπηρεσίες αυτές είναι καλύτερο να παρέχονται στο επίπεδο εφαρμογής.

Επίπεδο Δικτύου	Υπηρεσία
7. Εφαρμογής (Application)	Αυθεντικοποίηση Έλεγχος Προσπέλασης Ακεραιότητα Δεδομένων Εμπιστευτικότητα Δεδομένων Καταλογισμός Ευθύνης
6. Παρουσίασης (Presentation)	Εμπιστευτικότητα Δεδομένων
5. Συνόδου (Session)	----------
4. Μεταφοράς (Transport)	Αυθεντικοποίηση Προσπέλαση Ελέγχου Ακεραιότητα Δεδομένων Εμπιστευτικότητα Δεδομένων
3. Δικτύου (Network)	Αυθεντικοποίηση Προσπέλαση Ελέγχου Ακεραιότητα Δεδομένων Εμπιστευτικότητα Δεδομένων
2. Σύνδεσης Δεδομένων (Data Link)	Αυθεντικοποίηση Προσπέλαση Ελέγχου Ακεραιότητα Δεδομένων Εμπιστευτικότητα Δεδομένων
1. Φυσικό (Physical)	Εμπιστευτικότητα Δεδομένων

Πίνακας 1 : Σχέση υπηρεσιών ασφάλειας και των επιπέδων του OSI

Αυθεντικοποίηση

Η αυθεντικοποίηση έχει ως στόχο την απόδειξη της γνησιότητας μιας οντότητας (χρήστη ή υπολογιστή) έτσι ώστε να παρεμποδίζεται η εμφάνιση μιας οντότητας ως μια άλλη (impersonation). Επιπλέον, με τη διαδικασία της αυθεντικοποίησης μπορεί να εξασφαλιστεί η γνησιότητα ενός μηνύματος.

Γενικά, η αυθεντικοποίηση είναι η βασικότερη υπηρεσία ασφαλείας που μπορεί να προσφέρει ένα δίκτυο υπολογιστών καθώς αυτή παρέχει προστασία έναντι μη εξουσιοδοτημένων δοσοληψιών εξασφαλίζοντας τη γνησιότητα ενός μηνύματος, τη νομιμότητα ενός χρήστη ή αποστολέα και την εγκυρότητα ενός τερματικό ή υπολογιστή.

Η απλούστερη μορφή αυθεντικοποίησης βασίζεται στην τεχνική των συνθηματικών (passwords). Η τεχνική αυτή χαρακτηρίζεται από πλήθος προβλημάτων όπως η διαδικασία πληκτρολόγησης του συνθηματικού το οποίο εκτίθεται στους παρευρισκόμενους, η καταχώρησή του στον υπολογιστή, η επιλογή και διαφύλαξή του από τον ίδιο το χρήστη.

Επιπλέον, σε περιβάλλον κατανεμημένης επεξεργασίας όπου ένας χρήστης συνδέεται αρχικά σε έναν υπολογιστή και στη συνέχεια μπορεί να ζητήσει κάποια υπηρεσία από άλλο υπολογιστή, η υποκλοπή του συνθηματικού από έναν παρεμβολέα είναι αρκετά δύσκολη.

Οι ισχυρές τεχνικές αυθεντικοποίησης βασίζονται σε κρυπτογραφικά συστήματα και διακρίνονται στην απλή αυθεντικοποίηση (one way) και την αμοιβαία αυθεντικοποίηση (two ways). Σύμφωνα με την απλή αυθεντικοποίηση ένας χρήστης δικτύου πρέπει να γνωστοποιήσει την ταυτότητά του στον υπολογιστή που θέλει να χρησιμοποιήσει, έτσι ώστε να του επιτραπεί η προσπέλαση σε αυτόν. Αντίθετα, σύμφωνα με την αμοιβαία αυθεντικοποίηση και οι δύο (χρήστης και υπολογιστής, χρήστης και χρήστης), πρέπει να γνωστοποιήσουν ο ένας στον άλλο τις ταυτότητές τους.

Η αυθεντικοποίηση σε ένα περιβάλλον δικτύων υπολογιστών όπου εμπλέκεται ένας μεγάλος αριθμός χρηστών από διαφορετικούς οργανισμούς, είναι μια αρκετά χρονοβόρα και περίπλοκη διαδικασία.

Έτσι, η δημιουργία ενός κέντρου ελέγχου (κέντρου αυθεντικοποίησης) διευκολύνει τη διαδικασία της αυθεντικοποίησης με την παροχή των αναγκαίων πληροφοριών σε κάθε εμπλεκόμενο χρήστη. Ειδικότερα, κάθε χρήστης που επιθυμεί να επικοινωνήσει με οποιαδήποτε οντότητα του δικτύου, εξασφαλίζει τις αναγκαίες πληροφορίες από το κέντρο ελέγχου, το οποίο έχει την υπευθυνότητα της διαχείρισής τους.

Απαραίτητη προϋπόθεση για την ύπαρξη ενός τέτοιου κέντρου είναι η αποδοχή του από όλα τα εμπλεκόμενα μέρη, καθώς το κέντρο κατέχει και διαχειρίζεται πληροφορίες, η αποκάλυψη ή τροποποίηση των οποίων συνεπάγεται την υπονόμευση του συστήματος ασφαλείας.

Επειδή στη λειτουργία του κέντρου αυθεντικοποίησης εμπλέκεται και ο ανθρώπινος παράγοντας, ο οποίος μπορεί να συντελέσει στην εξασθένιση της ασφάλειας του συστήματος, προτάθηκε τελευταία μερικές από τις αρμοδιότητες του κέντρου να μεταφερθούν στους χρήστες. Η υλοποίηση ενός τέτοιου συστήματος μπορεί να επιτευχθεί με τη βοήθεια των έξυπνων καρτών (smart cards) στις οποίες καταχωρούνται μυστικά κλειδιά, αλγόριθμοι και χαρακτηριστικά των χρηστών.

Επιπλέον, η μεταφορά αρμοδιοτήτων από το κέντρο προς τους χρήστες συντελεί στην αποσυμφόρηση της επικοινωνίας χρηστών-κέντρου ελέγχου, καθώς τους παρέχει τη δυνατότητα σε πολλές περιπτώσεις να έρθουν σε επικοινωνία απευθείας.

Έλεγχος προσπέλασης

Ο έλεγχος προσπέλασης δικτύων υπολογιστών περιλαμβάνει όλους τους τυπικούς μηχανισμούς ελέγχου που διατίθενται από τα λειτουργικά συστήματα και τα συστήματα βάσεων δεδομένων καθώς και τις επεκτάσεις των ελέγχων αυτών για την προστασία των συνδέσεων μεταξύ των κόμβων ενός δικτύου και των δεδομένων που διακινούνται μέσω αυτών.

Οι έλεγχοι προσπέλασης στα δεδομένα και τους υπολογιστικούς πόρους του δικτύου πρέπει να περιλαμβάνουν κάποια διαδικασία αυθεντικοποίησης του χρήστη (είτε απλή, είτε ισχυρή) που καθορίζεται από το επιθυμητό επίπεδο ασφάλειας.

Εμπιστευτικότητα δεδομένων

Η υπηρεσία εμπιστευτικότητας εγγυάται ότι οι πληροφορίες δεν είναι διαθέσιμες ούτε αποκαλύπτονται στους μη εξουσιοδοτημένους χρήστες και παρέχει μηχανισμούς οι οποίοι προστατεύουν τα μεταδιδόμενα δεδομένα από τους μη ενεργούς παρεμβολείς. Η έννοια της εμπιστευτικότητας μπορεί να εφαρμοστεί είτε σε ολόκληρο το μήνυμα είτε σε ένα τμήμα του.

Για την εξασφάλιση της εμπιστευτικότητας των δεδομένων μπορεί ανάλογα με την περίπτωση, να χρησιμοποιηθεί κρυπτογράφηση των δεδομένων με τους ακόλουθους τρόπους: end to end και link to link. Κατά την πρώτη μέθοδο, τα δεδομένα αποστέλλονται κρυπτογραφημένα και αποκρυπτογραφούνται όταν παραληφθούν από τον χρήστη για τον οποίο προορίζονται. Έτσι, τα δεδομένα δεν είναι αναγνώσιμα από τους ενδιάμεσους κόμβους του δικτύου στο βαθμό που η χρησιμοποιούμενη κρυπτογραφική τεχνική είναι ασφαλής.

Κατά τη δεύτερη μέθοδο, τα δεδομένα αποστέλλονται κρυπτογραφημένα και αποκρυπτογραφούνται όχι μόνο από τον τελικό τους προορισμό αλλά και σε κάθε ενδιάμεσο κόμβο του δικτύου. Έτσι, είναι δυνατή η αποστολή κρυπτογραφημένων δεδομένων από ένα κόμβο του δικτύου σε έναν άλλο και η ταυτόχρονη κοινοποίηση τους σε όλους τους ενδιάμεσους κόμβους. Εφόσον είναι επιθυμητή κάποια επιλογή των ενδιάμεσων κόμβων του δικτύου στους οποίους θα κοινοποιηθούν τα δεδομένα, μπορεί να χρησιμοποιηθεί ένας συνδυασμός των δύο μεθόδων.

Ακεραιότητα δεδομένων

Η υπηρεσία ακεραιότητας των δεδομένων εξασφαλίζει ότι τα δεδομένα δεν έχουν αλλαχθεί ή καταστραφεί από μη εξουσιοδοτημένους χρήστες και είναι συναφής με την αυθεντικοποίηση των δεδομένων. Ειδικότερα, οι υπηρεσίες ακεραιότητας και αυθεντικοποίησης των δεδομένων είναι συνήθως απαραίτητες και οι δύο στο πλαίσιο της ασφάλειας δικτύων και χρησιμοποιούν τους ίδιους μηχανισμούς οι οποίοι βασίζονται σε κρυπτογραφικές τεχνικές. Επίσης, η

ακεραιότητα των δεδομένων μπορεί να εφαρμοστεί είτε σε ολόκληρο το μήνυμα είτε σε επιλεγμένα τμήματά του.

Καταλογισμός ευθύνης

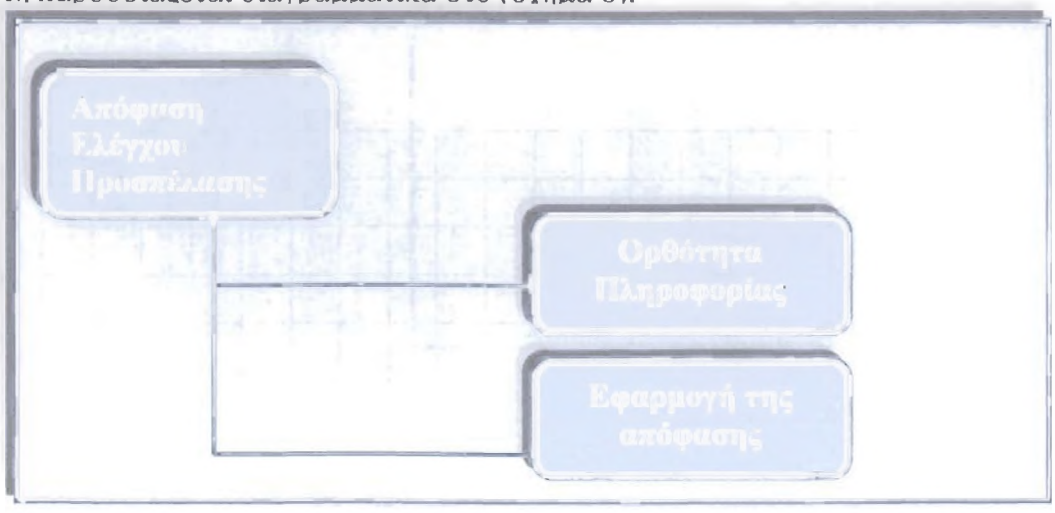
Επιπλέον της αυθεντικοποίησης ενός χρήστη και της ακεραιότητας των δεδομένων που διακινούνται σε ένα δίκτυο υπολογιστών συχνά απαιτείται ο καταλογισμός της ευθύνης για την αποστολή ή την παραλαβή ενός μηνύματος. Δηλαδή, σε ορισμένες περιπτώσεις είναι απαραίτητο ο αποστολέας (παραλήπτης) ενός μηνύματος να μη μπορεί να απαρνηθεί την ευθύνη αποστολής (παραλαβής) του συγκεκριμένου μηνύματος. Ένας μηχανισμός αντιμετώπισης του προβλήματος αυτού του είδους είναι με τη χρήση ψηφιακής υπογραφής (digital signature) που υλοποιείται με τη βοήθεια κρυπτογραφικών συστημάτων. Ένας άλλος μηχανισμός για τον καταλογισμό ευθύνης είναι η ύπαρξη ενός έμπιστου κέντρου ελέγχου (trusted third party).

Τεχνικές Υλοποίησης των Υπηρεσιών Ασφάλειας

Οι τεχνικές υλοποίησης των υπηρεσιών ασφάλειας σε ένα δίκτυο υπολογιστών είναι ο έλεγχος προσπέλασης, η κρυπτογραφία και η ψηφιακή υπογραφή.

Έλεγχος προσπέλασης

Ο έλεγχος προσπέλασης (Access Control) ορίζεται ως η παρεμπόδιση της χρήσης ενός υπολογιστικού πόρου ή δεδομένων, με μη επιτρεπτό τρόπο από τις οντότητες του συστήματος. Ο έλεγχος προσπέλασης σχετίζεται άμεσα με τις υπηρεσίες της αυθεντικοποίησης, ακεραιότητας και εμπιστευτικότητας του μηνύματος. Η σχέση αυτή παρουσιάζεται διαγραμματικά στο (σγήμα 8).

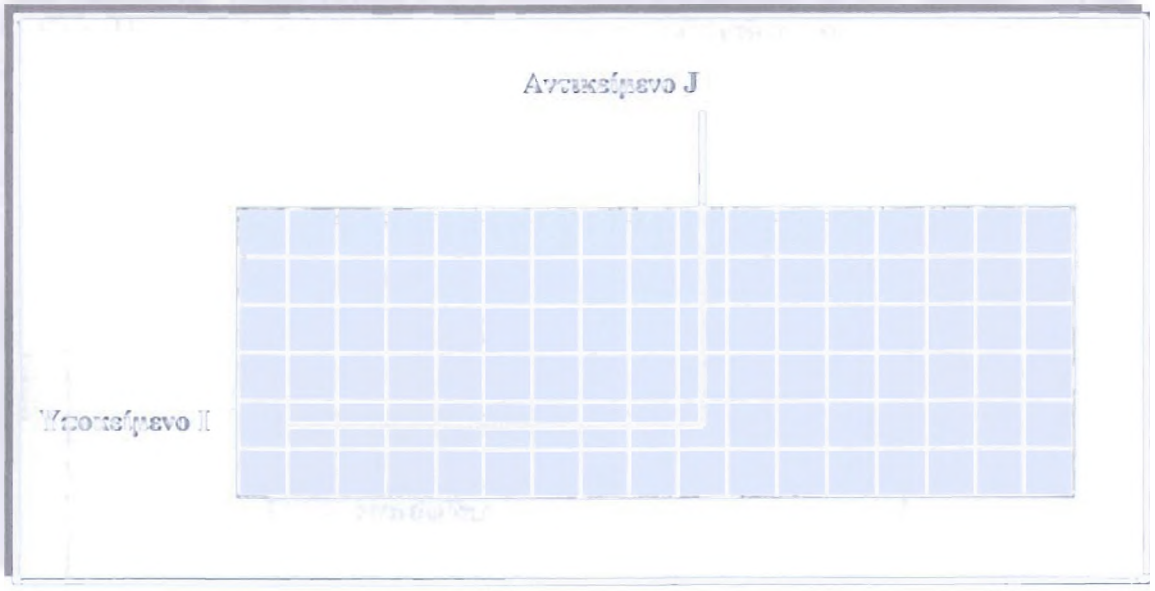


Σχήμα 8 : Σχέση ελέγχου προσπέλασης με τις υπηρεσίας ασφάλειας

Ο έλεγχος προσπέλασης είναι αποτελεσματικός όταν αναφέρεται σε ορθή πληροφορία και μπορεί να εφαρμοστεί. Η εφαρμογή του γίνεται με τη βοήθεια των υπηρεσιών αυθεντικοποίησης, ακεραιότητας και εμπιστευτικότητας του μηνύματος. Η αυθεντικοποίηση και η ακεραιότητα της πληροφορίας εξασφαλίζουν την ορθότητα της πληροφορίας στην οποία ασκείται ο έλεγχος προσπέλασης ενώ η αυθεντικοποίηση και η εμπιστευτικότητα του μηνύματος την εφαρμογή του ελέγχου.

Για παράδειγμα, έστω σε ένα δίκτυο ο χρήστης Α επιθυμεί να στείλει ένα μήνυμα στον χρήστη Β χωρίς να μπορεί να επέμβει ο χρήστης Γ. Η εφαρμογή της απόφασης του ελέγχου προσπέλασης σημαίνει ότι ο χρήστης Γ δεν μπορεί να ενημερωθεί για το μήνυμα που ο χρήστης Α στέλνει στον Β. Η εφαρμογή της απόφασης αυτής μπορεί να γίνει με την δημιουργία ενός ασφαλούς διαύλου μεταξύ των χρηστών Α και Β ώστε οι χρήστες που επικοινωνούν να είναι πράγματι αυτοί (αυθεντικοποίηση) και οι μόνοι που γνωρίζουν το μήνυμα (εμπιστευτικότητα του μηνύματος). Όταν ο χρήστης Β παραλάβει το μήνυμα τότε πραγματοποιείται πάλι έλεγχος προσπέλασης σχετικά με το αν ο χρήστης Β μπορεί να είναι ο παραλήπτης. Στην περίπτωση αυτή θα πρέπει να επαληθευτεί η ταυτότητα των χρηστών (αυθεντικοποίηση) και αν το μήνυμα δεν έχει μορφοποιηθεί (ακεραιότητα του μηνύματος)

Ο έλεγχος προσπέλασης υλοποιείται με τη βοήθεια ενός πίνακα (λίστα) που κάθε στήλη του αφορά το αντικείμενο του ελέγχου και κάθε γραμμή το υποκείμενο του ελέγχου. Αντικείμενο ελέγχου προσπέλασης ορίζεται κάθε αρχείο, τερματικό, εφαρμογή και κάθε υπολογιστικός πόρος του συστήματος να προσπελάσει. Υποκείμενο του ελέγχου προσπέλασης ορίζεται η κάθε οντότητα (χρήστης, υπολογιστής, εφαρμογή) που έχει τη δυνατότητα πρόσβασης. Στο (σχήμα 9) παρουσιάζεται διαγραμματικά ο πίνακας ελέγχου προσπελάσεων (λίστα προσπελάσεων – access list).



Σχήμα 9 : Λίστα προσπελάσεων

Κάθε στοιχείο (I,J) της λίστας περιγράφει το είδος της προσπέλασης που έχει το υποκείμενο I στο αντικείμενο J καθώς και άλλες σχετικές πληροφορίες. Για παράδειγμα, ένα στοιχείο περιγράφει αν ο χρήστης έχει τη δυνατότητα διαβάσματος, ενημέρωσης ή μορφοποίησης ενός αρχείου, εκτέλεσης μιας εφαρμογής, σύνδεσης με ένα άλλο υπολογιστή ενώ ως σχετικές πληροφορίες μπορεί να είναι η δυνατότητα αλλαγής του είδους προσπέλασης που έχει.

Επίσης, ο έλεγχος προσπέλασης χωρίζεται σε ελεύθερης βούλησης (discretionary) και υποχρεωτικός (mandatory). Ελεύθερης βούλησης έλεγχος είναι η παροχή των δικαιωμάτων προσπέλασης (access rights) των αντικειμένων του υποκειμένου, σε άλλα υποκείμενα. Αντίθετα, υποχρεωτικός έλεγχος είναι όταν δεν έχει τη δυνατότητα παροχής των δικαιωμάτων του σε τρίτους.

Μια άλλη μορφή ελέγχου πρόσβασης είναι οι ετικέτες ασφάλειας (security labels). Κάθε υποκείμενο και αντικείμενο του συστήματος έχει ετικέτα ασφάλειας που εκφράζει:

⇒ Η ετικέτα αντικειμένου, τη σημαντικότητα του αντικειμένου μέσα στο σύστημα.

⇒ Η ετικέτα υποκειμένου, την αξιοπιστία του υποκειμένου μέσα στο σύστημα.

Συνεπώς ένα υποκείμενο για να έχει πρόσβαση σε ένα αντικείμενο θα πρέπει ο βαθμός αξιοπιστίας του υποκειμένου να ικανοποιεί τη σημαντικότητα του αντικειμένου.

Κρυπτογραφία

Η κρυπτογραφία σχετίζεται με την τροποποίηση ενός κειμένου από την αρχική μορφή του σε κωδικοποιημένη και την επαναφορά του από κωδικοποιημένη μορφή στην αρχική, έτσι ώστε να μπορεί να μεταφερθεί χωρίς να υπάρχει τρόπος να μορφοποιηθεί. Η κρυπτογραφία χρησιμοποιείται σε πολλούς τομείς και αποτελεί βασικό μηχανισμό για την ανάπτυξη ενός αποτελεσματικού συστήματος ασφάλειας. Σε αντίθεση με την κρυπτογραφία, κρυπτανάλυση ονομάζεται η τεχνική της εύρεσης του αλγορίθμου που χρησιμοποιείται σε ένα κρυπτογραφικό σύστημα για να κωδικοποιεί και αποκωδικοποιεί τα δεδομένα.

Σε ένα κρυπτογραφικό σύστημα ο τρόπος με το οποίο επιτυγχάνεται ο σκοπός του δεν είναι πάντα ο ίδιος. Ορισμένα συστήματα χαρακτηρίζονται επιτυχημένα επειδή ο χρόνος που χρειάζεται ένας μη εξουσιοδοτημένος χρήστης για να ανακαλύψει την λειτουργία είναι μεγάλος. Τα συστήματα αυτά ονομάζονται **υπολογιστικά ασφαλή κρυπτογραφικά συστήματα (computationally secure syetems).**

Υπάρχουν όμως και συστήματα που είναι ανεξάρτητα του χρόνου που έχει στην διάθεση του ο μη εξουσιοδοτημένος χρήστης και ονομάζονται ασφαλή κρυπτογραφικά συστήματα χωρίς χρονικά όρια (unconditionally secure systems).

Ένα άλλο χαρακτηριστικό είναι ο τρόπος κωδικοποίησης και αποκωδικοποίησης του μηνύματος . Μερικά χωρίζουν το μήνυμα σε πολύ μικρά μέρη τα οποία κωδικοποιούν ένα προς ένα, ενώ άλλα σε μεγαλύτερα. Το μέγεθος του τμήματος, αν είναι δηλαδή μικρό ή μεγάλο, είναι σημαντικό καθώς μια απρόσμενη αλλαγή σε ένα από αυτά δεν επιφέρει μεγάλη αλλαγή στο αποτέλεσμα αν το μέγεθος είναι μικρό ενώ όταν είναι μεγάλο το τελικό αποτέλεσμα μπορεί να είναι διαφορετικό.

Μέχρι το 1976 τα συστήματα κρυπτογράφησης χρησιμοποιούσαν ένα κλειδί για την κωδικοποίηση και αποκωδικοποίηση του μηνύματος το οποίο ήταν γνωστό μόνο στις δύο οντότητες που ήθελαν να επικοινωνήσουν. Το κύριο χαρακτηριστικό του κλειδιού, το οποίο ονομάζονταν μυστικό κλειδί (secret key),ήταν η μικρή πιθανότητα εύρεσής του από τρίτη οντότητα καθώς περιλάμβανε μεγάλο πλήθος ψηφίων. Το 1976 οι Diffie και Hellman όρισαν ένα νέο σύστημα κρυπτογράφησης το οποίο είχε δύο κλειδιά, το ένα για την κωδικοποίηση και το άλλο για την αποκωδικοποίηση, τα οποία συσχετίζονταν με μια μαθηματική συνάρτηση. Έτσι δημιουργήθηκαν δύο μεγάλες και βασικές κατηγορίες κρυπτογραφικών συστημάτων:

⇒ Τα συμμετρικά συστήματα (symmetric) ή συστήματα μυστικού κλειδιού (secret key) και

⇒ Τα μη συμμετρικά συστήματα (asymmetric) ή συστήματα δημόσιου κλειδιού

Ψηφιακή υπογραφή

Η ψηφιακή υπογραφή (Digital Signature), θεωρείται ως το ηλεκτρονικό ισοδύναμο της συμβατικής υπογραφής και είναι μια συμβολοσειρά που προκύπτει από το συνδυασμό των δυαδικών ψηφίων ενός μηνύματος και αυτών ενός μυστικού κλειδιού.

Η ψηφιακή υπογραφή πρέπει να δημιουργείται και να επαληθεύεται εύκολα, ενώ η πλαστογράφησή της να πραγματοποιείται με μεγάλη δυσκολία. Η χρησιμοποίηση της ψηφιακής υπογραφής σε ένα σύστημα ασφάλειας ενός δικτύου είναι απαραίτητη καθώς παρέχει αυθεντικοποίηση του αποστολέα, εμπιστευτικότητα και ακεραιότητα του μηνύματος. Ο Merkle έχει περιγράψει δύο εφαρμογές που με τη βοήθεια των ψηφιακών υπογραφών παρέχουν προστασία λογισμικού.

Στην περίπτωση που χρησιμοποιείται συμμετρικό κρυπτογραφικό πρωτόκολλο τότε απαιτείται η συμμετοχή ενός τρίτου έμπιστου χρήστη (trusted third party) και δεν παρέχεται αυθεντικοποίηση του αποστολέα.. Τα προβλήματα και οι κίνδυνοι είναι

πολλοί όταν η ψηφιακή υπογραφή χαθεί ή κλαπεί. Από τα παραπάνω συμπεραίνεται ότι η ψηφιακή υπογραφή και τα κρυπτογραφικά πρωτόκολλα έχουν μεγάλη σχέση μεταξύ τους.

Προϋποθέσεις Εφαρμογής ενός Συστήματος Ασφάλειας

Στην επιτυχημένη εφαρμογή ενός συστήματος ασφάλειας σε ένα δίκτυο θα πρέπει να λαμβάνονται υπόψη οι ακόλουθες προϋποθέσεις:

⇒ Ορισμένοι από τους χρήστες του συστήματος να είναι εξουσιοδοτημένοι. Δηλαδή, το σύστημα να τους θεωρεί αξιόπιστους.

⇒ Ορισμένοι σημαντικοί πόροι του δικτύου να θεωρούνται, επίσης, αξιόπιστοι.

⇒ Να υπάρχουν χάρτες μέσα στο δίκτυο που οι μη εξουσιοδοτημένοι χρήστες να μην μπορούν να επέμβουν.

Οι παραπάνω προϋποθέσεις είναι απαραίτητες για να μπορούν οι κατασκευαστές του συστήματος ασφάλειας να καθορίσουν ποια είναι τα σημεία του δικτύου που μπορεί να υπάρχει επέμβαση, από ποιον και με ποια μορφή.
Για την υλοποίηση ενός συστήματος ασφάλειας σε ένα δίκτυο υπολογιστικών συστημάτων θα πρέπει να ληφθούν υπόψη τα ακόλουθα (trade offs):

⇒ Η υψηλή απόδοση του συστήματος σε σχέση με την απλότητα της αρχιτεκτονικής του συστήματος.

⇒ Η προσαρμοστικότητα του πρωτοκόλλου σε σχέση με την επιβάρυνση απόδοσης του μοντέλου αναφοράς OSI.

⇒ Το απαιτούμενο συνολικό κόστος σε σχέση με το ρόλο της ασφάλειας που παρέχεται από το σύστημα.

⇒ Οι περιορισμοί στη μεταβίβαση των δεδομένων σε σχέση με την εχεμύθεια διαχείρισης και υποστήριξης του συστήματος.

⇒ Ο περιορισμός των δυνατοτήτων σύνδεσης των χρηστών στο δίκτυο σε σχέση με το βαθμό ασφάλειας του δικτύου.

Προβλήματα Ασφάλειας Δικτύων

Κάθε ενέργεια η οποία εκθέτει σε κίνδυνο την ασφάλεια των πληροφοριών ενός οργανισμού ή φυσικού προσώπου συνιστά μια απειλή ασφάλειας (security threat). Σε ένα περιβάλλον δικτύου υπολογιστών οι απειλές μπορεί να προέρχονται είτε από ενεργούς (active) παρεμβολείς είτε από μη ενεργούς (passive) παρεμβολείς και μπορούν να διακριθούν σε εσκεμμένες και τυχαίες με σημαντικότερες τις πρώτες. Οι πιο γνωστές εσκεμμένες απειλές που μπορούν να διαταράξουν την ασφάλεια ενός δικτύου είναι οι ακόλουθες :

⇒ **Μη εξουσιοδοτημένη χρήση ή μεταμφίεση (masquerade):** κατά την οποία επιχειρείται προσπέλαση στα δεδομένα ή στις προσφερόμενες υπηρεσίες του δικτύου από μη εξουσιοδοτημένους χρήστες. Για την μεταμφίεση του εξουσιοδοτημένου χρήστη ο υποκλοπέας (hacker) προσπαθεί να αποκτήσει με αθέμιτα μέσα κάποιο έγκυρο συνθηματικό (password) για να επιτύχει ταυτοποίηση και συνεπώς πρόσβαση στο δίκτυο.

⇒ **Μη ενεργώς παρακολούθηση (passive tapping):** κατά την οποία απειλείτε η εμπιστευτικότητα των ανταλλασομένων μηνυμάτων στο δίκτυο από μη ενεργούς παρεμβολείς ή ωτακουστές της διεξαγόμενης επικοινωνίας. Ο βαθμός της απειλής εξαρτάται και από το μέσο επικοινωνίας που χρησιμοποιείται. Δηλαδή, στα δίκτυα οπτικής ίνας, η παρεμβολή χωρίς εντοπισμό είναι δυσκολότερη από ότι στα δίκτυα ομοαξονικού καλωδίου. Ο κίνδυνος μπορεί να ελαχιστοποιηθεί με τη χρήση κρυπτογραφικών τεχνικών.

⇒ **Ενεργός παρακολούθηση (active tapping):** κατά την οποία επιχειρείται τροποποίηση ή εξαγωγή των ανταλασσόμενων μηνυμάτων στο δίκτυο. Αν και ο ενεργός παρεμβολέας μπορεί να εντοπιστεί ευκολότερα από ένα μη ενεργό θεωρείται πιο επικίνδυνος καθώς μπορεί να προκαλέσει μεγαλύτερη ζημία στο δίκτυο. Επιπλέον, ένας ενεργός παρεμβολέας μπορεί να εισάγει δικά του δεδομένα στο δίκτυο ή να ανακατευθύνει τα μηνύματα σύμφωνα με τις δικές του επιθυμίες.

⇒ **Καταλογισμός ευθύνης (repudiation):** όπου ένας εξουσιοδοτημένος χρήστης μπορεί να απαρνηθεί την ευθύνη αποστολής ή παραλαβής ενός συγκεκριμένου μηνύματος ή ακόμη να κατασκευάσει ένα μη έγκυρο μήνυμα. Η κατάσταση αυτή παρατηρείται συνήθως όταν η επικοινωνία διεξάγεται μεταξύ δύο οργανισμών (π.χ. ηλεκτρονική μετάδοση δεδομένων EDI).

- **Άρνηση εξυπηρέτησης (denial of service):** κατά την οποία το δίκτυο δεν ανταποκρίνεται στο απαιτούμενο επίπεδο εξυπηρέτησης και / ή λειτουργικότητας. Η απειλή μπορεί να προκαλέσει την απώλεια μηνυμάτων, καθυστερήσεις και γενικότερα την ομαλή λειτουργία του οργανισμού. Η πρόκληση ενός τέτοιου κινδύνου μπορεί να είναι είτε από εσκεμμένες είτε από τυχαίες ενέργειες. Φυσικά, μικρές διακοπές της λειτουργίας ενός δικτύου είναι δυνατό να επιτρέπονται, όμως διακοπές μεγάλης διάρκειας επιτρέπονται μόνο εάν είναι εκ των προτέρων προγραμματισμένες.

⇒ **Επανάληψης (replay):** όπου ένας εξουσιοδοτημένος χρήστης προβαίνει στην επανάληψη ενός μηνύματος με στόχο να θεωρηθεί από τον αποδέκτη του ως πρωτότυπο. Οι επαναλήψεις των μηνυμάτων μπορούν να πραγματοποιηθούν είτε από ελαττωματικό λογισμικό είτε από εσκεμμένες προσπάθειες για παραποίηση των μεταδιδόμενων πληροφοριών. Η επίπτωση μιας τέτοιας απειλής στο τραπεζικό περιβάλλον, κατά την ηλεκτρονική μεταβίβαση χρημάτων (Electronic Fund Transfer / EFT), είναι τεράστια.

⇒ **Ανάλυση επικοινωνίας (traffic analysis):** κατά την οποία παρακολουθείται η μετάδοση των μηνυμάτων στο δίκτυο όχι απαραίτητα για την αποκάλυψη του περιεχομένου τους, καθώς αυτά μπορεί να έχουν κρυπτογραφηθεί, αλλά για τον εντοπισμό της προέλευσής τους ή / και της αποστολής τους. Επιπλέον, πολλές φορές κατά την ανάλυση της επικοινωνίας επιδιώκεται από τον παρεμβολέα ο καθορισμός της συχνότητας επικοινωνίας των εμπλεκόμενων χρηστών.

⇒ **Ιοί (viruses):** είναι λογισμικό που σχεδιάζεται για να προκαλέσει προβλήματα στην ομαλή λειτουργία του συστήματος . Οι ιοί μπορούν είτε να καταστρέψουν τα δεδομένα ή να παραποιήσουν την ακεραιότητά τους (Time Bomb, True Viruses, Login Bomb, Trojan Horse) είτε να προκαλέσουν μικρότερα σε μέγεθος προβλήματα (Worms). Ο τρόπος λειτουργίας τους είναι η επαναλαμβανόμενη αντιγραφή τους σε σημεία που ήδη βρίσκονται καταχωρημένα άλλα δεδομένα. Επιπλέον θα πρέπει να ληφθεί υπόψη η φυσική ασφάλεια ενός δικτύου υπολογιστικών συστημάτων που αναφέρεται στην ασφάλεια των δεδομένων και των υπολογιστικών πόρων του συστήματος από φυσικές καταστροφές που θέτουν, έστω και προσωρινά, εκτός λειτουργίας το δίκτυο ή επιμέρους τμήματά του.

Οδηγός για Ασφαλή Πλοήγηση στο Internet

Λίγα είναι αυτά που δεν έχουν ειπωθεί-γραφτεί για την ασφάλεια προσωπικών δεδομένων και υπολογιστικών συστημάτων. Λίγα, όμως, είναι κι αυτά που έχουν γραφτεί ή ειπωθεί πάνω στα ίδια θέματα, που αποφεύγουν την υπερβολή και τον εντυπωσιασμό, παρουσιάζοντας παράλληλα πρακτική αξία και υψηλή χρηστικότητα για τον καθημερινό χρήστη.

Σε ευαίσθητα και ταυτόχρονα "καυτά" θέματα όπως η ασφάλεια των δεδομένων, η προστασία της ανωνυμίας και η προάσπιση του ιδιωτικού απορρήτου, οι όποιες κινήσεις μας απαιτούν προσεκτικό σχεδιασμό και μεθοδικότητα.

Η συχνή παρομοίωση ενός υπολογιστή συνδεδεμένου στο Internet με ένα αυτοκίνητο με ορθάνοιχτες πόρτες και την μηχανή αναμμένη μπορεί να φαντάζει στα αυτιά ενός μέσου ή αν θέλετε ακόμα κι έμπειρου χρήστη με υπερβολή, ωστόσο δεν απέχει σημαντικά από την πραγματικότητα.

Ο μόνος τρόπος για να είστε πραγματικά σίγουροι για την ασφάλεια του υπολογιστή σας δεν είναι ο χρονικός περιορισμός της σύνδεσης στο Διαδίκτυο στο απολύτως απαραίτητο, αλλά η απόλυτη αποχή από αυτό.

Το ζητούμενο, λοιπόν, δεν είναι η πλήρης διασφάλιση του απορρήτου των προσωπικών σας δεδομένων (απλά και μόνο γιατί κάτι τέτοιο αποτελεί ουτοπία) αλλά η προσπάθεια για την επίτευξη υψηλών ποσοστών ασφαλείας – γιατί όχι και του 99%!

Τα "κλειδιά" για την ασφάλεια του ηλεκτρονικού υπολογιστή σας ή του δικτύου υπολογιστών σας στο σπίτι ή στο γραφείο δεν είναι άλλα από τα ειδικά προϊόντα ασφαλείας που καλύπτουν ένα ευρύ φάσμα αναγκών τόσο σε επίπεδο hardware όσο και σε επίπεδο λογισμικού (software).

Ένας άλλος παράγοντας που καθορίζει το βαθμό επικινδυνότητας που παρουσιάζει ο (οι) υπολογιστής(-ές) σας είναι αυτός της διαθεσιμότητάς του. και ειδικότερα της ποιότητας και της ποσότητας αυτής.

Με απλά λόγια, το επισφαλές ενός υπολογιστή καθορίζεται όχι μόνο από το εάν αυτός είναι συνδεδεμένος σε ένα δίκτυο, αλλά και από το διάστημα που είναι συνδεδεμένος όπως επίσης και από την ταχύτητα της σύνδεσής του.

Χωρίς να προχωρήσουμε (τουλάχιστον σε αυτό το σημείο σε τεχνικές λεπτομέρειες) σε γενικές γραμμές οι συνδέσεις που γίνονται με σταθερές IP διευθύνσεις (static IP ISDN, μισθωμένη γραμμή κ.λ.π.) παρουσιάζουν μεγαλύτερη επικινδυνότητα από ότι οι συνήθειςPSTN dial up συνδέσεις.

Για να αντιληφθείτε του λόγου του αληθές, απλά σκεφθείτε πως εάν έχετε σταθερή IP address και ένας hacker ή ένα script kiddie σας εντοπίσει (μια φορά) θα είναι σαν να γνωρίζει τη διεύθυνση του σπιτιού σας - ενώ το αντικλείδι κατά πάσα πιθανότητα θα το έχει ήδη στην διάθεσή του.

Η χρήση personal firewalls, antivirus προγραμμάτων (δύο τουλάχιστον), εξειδικευμένων προγραμμάτων anti-trojan (ανάλογα με το ποιος trojan είναι σε "έξαρση" κάθε περίοδο) και λογισμικού προστασίας προσωπικών δεδομένων είναι επιβεβλημένη.

Αξίζει να σημειωθεί πως η καταπολέμηση των κινδύνων δεν τελειώνει με την εγκατάσταση δύο ή και περισσοτέρων προγραμμάτων ασφαλείας, αντιθέτως μόλις αρχίζει! Εκτός από την εγκατάσταση των προγραμμάτων απαιτείται διαρκής ενημέρωση και σωστή ρύθμιση, αλλιώς η ίδια η γραμμή προστασίας που επιχειρούμε να δημιουργήσουμε στο (και για το) PC μας, μπορεί να στραφεί εναντίον μας.

Κάτι άλλο που πρέπει να έχετε υπόψη όσον αφορά στο θέμα "Ασφάλεια στον Η/Υ" είναι ότι, ως επί το πλείστον οι ψηφιακές επιθέσεις είναι απρόσωπες - δεν έχουν προσωπικό χαρακτήρα (με προφανή εξαίρεση τις επιθέσεις σε ιστοσελίδες).

Οι hackers δεν έχουν κάτι εναντίον σας κι ούτε θέλουν το κακό σας, το μόνο που ζητούν είναι πρόσβαση στο υπολογιστή σας για διαφορετικούς λόγους ο καθένας (ψυχαγωγικούς ή εκπαιδευτικούς).

Πέρα από τις χρήσιμες και πρακτικές συμβουλές που θα έχετε την ευκαιρία να διαβάσετε στο αφιέρωμα, να έχετε πάντα κατά νου ότι όποια μέτρα προστασίας και αν λάβετε το μόνο που κατορθώνεται είναι να δυσκολεύεται το έργο του επίδοξου hacker.

Αν είναι αληθινά επιδέξιος στον τομέα των ψηφιακών επιθέσεων, αργά ή γρήγορα, θα αποκτήσει πρόσβαση στον υπολογιστή ή το δίκτυο σας. Πολλές φορές δεν θα το καταλάβετε καν ή θα το αντιληφθείτε μόνο όταν θα είναι πολύ αργά.

Firewalls: Αδιαπέραστα Τείχη

Πρώτη φροντίδα για την προστασία των ψηφιακών σας δεδομένων απέναντι στους κινδύνους που εγκυμονεί το Διαδίκτυο δεν είναι άλλη από την επιλογή και την χρήση ενός personal firewall προγράμματος. Ενός firewall που μπορεί να διατίθεται ως μέρος μιας ολοκληρωμένης σουίτας προγραμμάτων ασφαλείας (Norton & McAfee Internet Security) ή ακόμη και ως γηγενές χαρακτηριστικό του πυρήνα ενός λειτουργικού συστήματος (Linux).

Ένα από τα πιο σημαντικά κριτήρια επιλογής Internet firewall θα πρέπει να είναι οι λεγόμενες λειτουργίες ελέγχου της εξερχόμενης κυκλοφορίας (traffic), δίνοντάς σας επιλογές αποδοχής, απόρριψης (πρόσκαιρης ή μόνιμης) της αποστολής των packets που επιχειρεί να στείλει μια εφαρμογή.

Ωστόσο για να είναι πραγματικά αποτελεσματική και χρήσιμη μια τέτοια λειτουργία θα πρέπει και εσείς να διαθέτετε ιδιαίτερες γνώσεις ή τουλάχιστον την όρεξη για να τις αποκτήσετε, ώστε να είστε σε θέση να κρίνετε ποια packets είναι καλό να φύγουν από το σύστημά σας και ποια όχι.

Καθώς βασιζόμαστε ολοένα και περισσότερο στους υπολογιστές, αυξάνονται οι πιθανότητες πρόκλησης ζημιάς (υλικής ή άλλης) από τους hackers, αφού πλέον οι τελευταίοι είναι σε θέση να αποκτήσουν πρόσβαση και να χρησιμοποιήσουν με όχι αποδεκτό τρόπο σχεδόν να προσωπικά και εταιρικά δεδομένα.

Τα εργαλεία που χρησιμοποιούν στις μέρες μας οι hackers είναι πιο εξελιγμένα, παρουσιάζουν μεγαλύτερη αυτοματοποίηση ενώ ο εντοπισμός τους είναι σε γενικές γραμμές αρκετά πιο δύσκολος.

Επιπλέον οι συνδέσεις υψηλών ταχυτήτων (που για τη χώρα μας παραμένουν... υπόσχεση) μας έκαναν και πιο φθαρτούς στους crackers, κυρίως λόγω των στατικών ή περιοδικά μεταβαλλόμενων IP διευθύνσεων (η διευθυνσιοδότηση που χρησιμοποιείται στα δίκτυα και στο Internet).

ΚΕΦΑΛΑΙΟ 3ο

ΝΟΜΙΚΑ-ΚΟΙΝΩΝΙΚΑ ΘΕΜΑΤΑ

Νομικά και Κοινωνικά Θέματα

Εισαγωγικά

Η ανοδική τάση που παρατηρείται στη χρήση ηλεκτρονικών μέσων επικοινωνίας τα τελευταία χρόνια οφείλεται στα τεράστια πλεονεκτήματα που προσφέρουν. Εντούτοις, τα πλεονεκτήματα αυτά τότε μόνο μπορούν να αξιοποιηθούν πλήρως, όταν αφενός υπάρχει ευρύτερη νομική αναγνώριση της ηλεκτρονικής επικοινωνίας και αφετέρου η γνησιότητα των μηνυμάτων είναι εξασφαλισμένη. Οι δύο αυτές προϋποθέσεις, η μία νομική και η άλλη τεχνική, είναι απαραίτητες για την εδραίωση του ηλεκτρονικού εμπορίου.

Αρκετά ζητήματα που ανακύπτουν από τη χρησιμοποίηση των νέων μέσων μπορούν, με κατάλληλη ερμηνεία των παραδοσιακών κανόνων δικαίου που βασίζονται στον έγγραφο τύπο, να επιλυθούν χωρίς νομοθετική παρέμβαση. Ουσιαστικές δυσκολίες μπορούν να υπάρξουν από πλευράς φορολογικού δικαίου, η γραφειοκρατική παρέμβαση του οποίου στις συναλλαγές είναι εντονότατη.Το ίδιο ισχύει και με την επιβολή χαρτοσήμανσης.

Γενικότερα η νέα τεχνολογία δεν μεταβάλλει στο συναλλακτικό πεδίο την ουσία των κανόνων του εμπορικού δικαίου. Απλώς καταργεί σε μεγάλο βαθμό τις προσωπικές σχέσεις μεταξύ των συναλλασσομένων και εισάγει και στο εμπορικό δίκαιο το απρόσωπο στοιχείο, ίδιο των καιρών μας, αλλά και τη "βιομηχανοποίηση" της πληροφόρησης και της επικοινωνίας.

Η συνεχώς αυξανόμενη χρήση του Διαδικτύου για τη σύναψη εμπορικών συμβάσεων, το ηλεκτρονικό εμπόριο, και οι ανυπολόγιστες επιδράσεις του στην οικονομία, δραστηριοποίησαν διεθνείς οργανισμούς, την Επιτροπή Ευρωπαϊκών Κοινοτήτων καθώς και κυβερνήσεις διαφόρων χωρών, προκειμένου να ορίσουν το νομικό πλαίσιο των ηλεκτρονικών συναλλαγών.

Σε διεθνές επίπεδο, η Επιτροπή Διεθνούς Εμπορικού Δικαίου των Ηνωμένων Εθνών (UNCITRAL) συνέταξε το 1996 τον Πρότυπο Νόμο για το ηλεκτρονικό εμπόριο, ρυθμίζοντας ζητήματα όπως η εξομοίωση των ηλεκτρονικών πληροφοριών με έγγραφα υλικής υπόστασης, η νομική ισχύς της ηλεκτρονικής υπογραφής, η αποδεικτική δύναμη των ηλεκτρονικών κειμένων, ο τόπος, χρόνος και απόδειξη παραλαβής του ηλεκτρονικού μηνύματος.

Η Ευρωπαϊκή Ένωση, αναγνωρίζοντας την ανάγκη νομικής ρύθμισης των ηλεκτρονικών εμπορικών συναλλαγών, εξέδωσε Οδηγία για το ηλεκτρονικό εμπόριο. Συγκεκριμένα, το Ευρωπαϊκό Κοινοβούλιο προέβη το 1999 στην έκδοση της υπ' αριθμό. 2000/31/ΕΚ Οδηγίας, η οποία τέθηκε σε ισχύ στις 17/07/2000. Με την Οδηγία αυτή καθιερώθηκε η αρχή της ελευθερίας σύναψης ηλεκτρονικών συμβάσεων, η αρχή της χώρας προέλευσης, που σήμαινε ότι το Δίκαιο που διέπει τις συναλλαγές με ηλεκτρονικά μέσα είναι το Δίκαιο της χώρας μόνιμης εγκατάστασης του φορέα παροχής υπηρεσιών, και ο εξωδικαστικός διακανονισμός των διαφόρων που θα προκύψουν.

Το Ευρωκοινοβούλιο, προκειμένου να διασφαλίσει τη γνησιότητα της ηλεκτρονικής υπογραφής, προέβλεψε την έκδοση αναγνωρισμένου Πιστοποιητικού Ηλεκτρονικής Υπογραφής, μιας ηλεκτρονικής βεβαίωσης, η οποία συνδέει δεδομένα επαλήθευσης της υπογραφής με ένα φυσικό πρόσωπο, επιβεβαιώνοντας έτσι την ταυτότητά του.

Η Ελλάδα, με την έκδοση του υπ' αριθμό. 150/2001 Π.Δ. εναρμονίστηκε με την Οδηγία αυτή και προέβη σε σημαντικά βήματα προς τη θέσπιση ενός "Δικαίου του Internet".Χαρακτηριστικό παράδειγμα αποτελεί ο Ν. 2672/1999 για τις ηλεκτρονικές υπογραφές καθώς και ο Ν. 2251/1994 για την προστασία των καταναλωτών.

Ηλεκτρονικά Έγγραφα

Σύμφωνα με την απόφαση υπ' αρ. 1327/2001 του Μονομελούς Πρωτοδικείου Αθηνών, ηλεκτρονικό έγγραφο είναι το σύνολο των έγγραφων δεδομένων στο μαγνητικό δίσκο ενός ηλεκτρονικού υπολογιστή. Τα δεδομένα αυτά λογίζονται ως έγγραφα με βάση το Νόμο, όταν, αφού γίνουν αντικείμενο επεξεργασίας από την κεντρική μονάδα επεξεργασίας, αποτυπώνονται με βάση τις εντολές του software κατά τρόπο που να μπορεί να τα διαβάσει ο άνθρωπος.

Η χρησιμοποίηση της ηλεκτρονικής υπογραφής (έτσι όπως αυτή ρητά περιγράφεται στο (Π.Δ.150/2001) μέσω του δημόσιου κλειδιού σε συνδυασμό με το παρεχόμενο πιστοποιητικό, θα αποτελεί την τεχνολογικά και νομικά προτεινόμενη λύση για την εξασφάλιση της αποδειξιμότητας της εμπιστευτικότητας, της αυθεντικότητας και της ακεραιότητας μιας υπογραφής. Αρμόδια αρχή για την πιστοποίηση είναι η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ).

Η πλειονότητα των ηλεκτρονικών εγγράφων διακινείται μέσω ανοιχτών δικτύων χωρίς ηλεκτρονική υπογραφή. Η Οδηγία 2002/31/ΕΚ για το ηλεκτρονικό εμπόριο επισημαίνει στο άρθρο 9 την υποχρέωση των κρατών - μελών να μεριμνούν ώστε το νομικό τους σύστημα να επιτρέπει την σύναψη συμβάσεων με ηλεκτρονικά μέσα.

Η απόφαση υπ' αριθμό. 1327/2001 ΜΠρ.Αθ. έκρινε ότι ο μοναδικός κωδικός πρόσβασης στο Διαδίκτυο μέσω του ISP που έχει ο χρήστης του email τον συνδέει τόσο στενά με το ηλεκτρονικό μήνυμα, ώστε η απεικόνιση της ηλεκτρονικής διεύθυνσής του να τον καθιστά απολύτως συγκεκριμένο για τον παραλήπτη.

Άρα: password ISP + ηλεκτρονική διεύθυνση = μαχητό τεκμήριο ταυτότητας.

Επιπλέον το δικαστήριο δέχτηκε ότι ο αποστολέας συνδέεται άρρηκτα με το περιεχόμενο του ηλεκτρονικού εγγράφου. Επομένως καθιερώνει τόσο μαχητό τεκμήριο αποδοχής του περιεχομένου όσο και μαχητό τεκμήριο γνησιότητας, οπότε έχουμε και πάλι αντιστροφή του βάρους απόδειξης από τον παραλήπτη του εγγράφου στον αποστολέα.

Η ίδια απόφαση δέχεται ότι η ηλεκτρονική διεύθυνση έχει το χαρακτήρα ιδιόχειρης υπογραφής. Ρητά καθορίζεται ότι το επικυρωμένο κατά το Νόμο αντίγραφο του απεσταλμένου ηλεκτρονικού μηνύματος που περιέχεται στο σκληρό δίσκο του παραλήπτη αποτελεί πλήρη απόδειξη ότι η περιλαμβανόμενη σε αυτό δήλωση προέρχεται από τον εκδότη. Ήδη οι νομοθετικές ρυθμίσεις που αφορούν στα έγγραφα της Δημόσιας Διοίκησης έχουν κάνει σαφή διαχωρισμό της δυνατότητας χρήσης και της αποδεικτικής δύναμης των ηλεκτρονικών εγγράφων, ανάλογα με το αν περιλαμβάνουν ηλεκτρονική υπογραφή ή όχι.

Ο Ν. 2672/1998 (άρθρο 14) για τη διακίνηση εγγράφων ηλεκτρονικά, αναφορικά με τη Δημόσια Διοίκηση και τις εσωτερικές σχέσεις της αλλά και τις σχέσεις της με τα φυσικά ή νομικά πρόσωπα ιδιωτικού δικαίου, καθώς και το Π.Δ. 342/2002 καθιστούν το email νόμιμο μέσο συναλλαγής και πληροφόρησης. Τα σχετικά νομοθετικά κείμενα θεωρούν όμως ότι κάθε πράξη μέσω του ηλεκτρονικού ταχυδρομείου μπορεί να συνδέεται με την παραγωγή έννομων αποτελεσμάτων ή με την άσκηση δικαιώματος μόνον όταν φέρει και ψηφιακή υπογραφή. Διαφορετικά τα έγγραφα που διακινούνται πρέπει να περιορίζονται σε απλές πληροφορίες, οδηγίες και εγκυκλίους.

Το Προεδρικό Διάταγμα 150 του 2001 για την Ηλεκτρονική Υπογραφή

Η e-signature, η πλέον αξιόπιστη μέθοδος πιστοποίησης ταυτότητας στο Internet, έχει ήδη υιοθετηθεί και από την Ελλάδα.

Με το Προεδρικό Διάταγμα 150 του 2001 που υπεγράφη από τους υπουργούς Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης, Εθνικής Οικονομίας, Δικαιοσύνης και Μεταφορών και Επικοινωνιών, η Ελλάδα προσαρμόστηκε στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου σχετικά με τις ηλεκτρονικές υπογραφές.

Σύμφωνα με το Προεδρικό Διάταγμα, η ηλεκτρονική υπογραφή εξομοιώνεται με την ιδιόχειρη κάτω από αυστηρές προϋποθέσεις που θα διασφαλίζουν την ταυτοπροσωπία αλλά και τη μοναδικότητα του φορέα της ηλεκτρονικής υπογραφής.

Κάθε συναλλασσόμενος με πρόσβαση σε ηλεκτρονικό υπολογιστή με σύνδεση στο Internet αποκτά τη δική του "ηλεκτρονική υπογραφή" μέσω διαπιστευμένων-εξουσιοδοτημένων για τον σκοπό αυτό φορέων ή εταιρειών.

Οι συγκεκριμένες εταιρείες εφοδιάζουν τον συναλλασσόμενο με ένα ειδικό software που περιέχει έναν ψηφιακό αλγόριθμο συνδυασμό "κλειδιών", καθώς και έναν προσωπικό μυστικό κωδικό αριθμό (PIN). Ο ψηφιακός αλγόριθμος παίζει το ρόλο ηλεκτρονικής υπογραφής και είναι μοναδικός για κάθε χρήστη, ενώ είναι πολύ δύσκολη η αναπαραγωγή, η παραχάραξη ή η υποκλοπή του, εκτός και αν κάποιος γνωρίζει τον μυστικό κωδικό αριθμό (PIN) ο οποίος είναι απαραίτητος για την πρόσβαση στην ηλεκτρονική υπογραφή.

Το software με την ηλεκτρονική υπογραφή εγκαθίσταται στον προσωπικό υπολογιστή του συναλλασσόμενου, έτσι ώστε κάθε φορά που χρειάζεται να κάνει αγορές-συναλλαγές μέσω του Internet να μπορεί "να βάζει την υπογραφή του", δίνοντας έτσι τη συγκατάθεσή του για την ολοκλήρωση της αγοράς ή της συναλλαγής.

Το ίδιο software ο ενδιαφερόμενος θα μπορεί να το έχει συνεχώς μαζί του (μέσω μιας "έξυπνης" κάρτας) ώστε να το χρησιμοποιεί και από άλλους ηλεκτρονικούς υπολογιστές εκτός του προσωπικού ή εργασιακού χώρου του. Στην πλήρη ανάπτυξη του συστήματος, με την "έξυπνη" αυτή κάρτα που θα υποκαθιστά την υπογραφή του θα μπορεί να προμηθεύεται ακόμα και μέσω των αυτόματων μηχανημάτων συναλλαγών (ATM) των τραπεζών... πιστοποιητικό ποινικού μητρώου, φορολογικής ενημερότητας ή γέννησης.

Ο ρόλος της ΕΕΤΤ

Τις εταιρείες που παρέχουν υπηρεσίες πιστοποίησης αλλά και βεβαιώσεις για την ασφάλεια της ηλεκτρονικής υπογραφής ελέγχει η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ), η οποία διαπιστώνει εάν οι συγκεκριμένες εταιρείες λειτουργούν με τέτοια υποδομή και κανόνες ώστε να είναι σε θέση να παρέχουν υπηρεσίες πιστοποίησης της ηλεκτρονικής υπογραφής. Σε μια τέτοια περίπτωση η ΕΕΤΤ μπορεί να τους παρέχει τη δυνατότητα να αναθέτουν και σε τρίτους το έργο αυτό.

Οι αρμοδιότητες της ΕΕΤΤ όπως απορρέουν από το Π.Δ. είναι επιγραμματικά οι εξής:

- Η παροχή Εθελοντικής Διαπίστευσης, ύστερα από έγγραφη αίτηση του ενδιαφερόμενου Παροχή Υπηρεσιών Πιστοποίησης, προκειμένου να επιτευχθεί βελτιωμένο επίπεδο παροχής υπηρεσιών πιστοποίησης. (άρθρο 4 παρ. 5 εδ.α) ή η ανάθεση σε δημόσιους ή ιδιωτικούς φορείς του έργου αυτού. Με την Εθελοντική Διαπίστευση απονέμονται δικαιώματα και επιβάλλονται υποχρεώσεις, συμπεριλαμβανομένων τελών, στον Πάροχο Υπηρεσιών Πιστοποίησης.

- Η εποπτεία και ο έλεγχος των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης, καθώς και των φορέων διαπίστευσης και ελέγχου της συμμόρφωσης των υπογραφών προς το Παράρτημα ΙΙΙ του πδ. 150/2001 (εφόσον η ΕΕΤΤ αναθέσει τέτοια καθήκοντα σε άλλους φορείς) (άρθρο 4 παρ. 8).

- Η διαπίστωση της συμμόρφωσης των διατάξεων δημιουργίας υπογραφής (υλικού ή λογισμικού που χρησιμοποιείται για την εφαρμογή του ιδιωτικού κλειδιού για τη δημιουργία της ηλεκτρονικής υπογραφής) προς το Παράρτημα ΙΙΙ του Προεδρικού Διατάγματος 150/2001 (άρθρο 4 παρ. 2, εδ.α) ή ανάθεση σε δημόσιους ή ιδιωτικούς φορείς του έργου αυτού.

- Η επιβολή προστίμων σε Παρόχους Υπηρεσιών Πιστοποίησης, οι οποίοι ενεργούν ως διαπιστευμένοι, χωρίς να είναι (άρθρο 4 παρ.9).

- Η ενημέρωση της Ευρωπαϊκής Επιτροπής για τις επωνυμίες και τις διευθύνσεις όλων των διαπιστευμένων εθνικών Παρόχων Υπηρεσιών Πιστοποίησης, καθώς και για τυχόν αλλαγές στις παραπάνω πληροφορίες (άρθρα 8 παρ. 2 και 3).

Η ΕΕΤΤ με την υπ. αρ. 248/71 Απόφασή της "Κανονισμός Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής" (ΦΕΚ 603/Β'/16-5-2002) ρυθμίζει ζητήματα των αναγνωρισμένων πιστοποιητικών και θέτει το θεσμικό πλαίσιο για την εποπτεία και τον έλεγχο των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης.

Άλλες Διατάξεις

Οι διατάξεις του Προεδρικού Διατάγματος 150 του 2001 δεν θίγουν διατάξεις που επιβάλλουν τη χρήση ορισμένου τύπου, ούτε διατάξεις για την αποδεικτική ή άλλη χρήση εγγράφων ή διατάξεις με τις οποίες απαγορεύεται να διακινούνται και να καθίστανται γνωστά έγγραφα.

Επίσης, το διάταγμα περιέχει ορισμούς των εννοιών ηλεκτρονική υπογραφή, προηγμένη ηλεκτρονική υπογραφή, ψηφιακή υπογραφή, υπογράφων, δεδομένα δημιουργίας υπογραφής, διάταξη δημιουργίας υπογραφής και άλλων. Ορίζει τις έννομες συνέπειες των ηλεκτρονικών υπογραφών δηλαδή ότι η ηλεκτρονική υπογραφή ενέχει θέση ιδιόχειρης υπογραφής τόσο στο ουσιαστικό όσο και στο δικονομικά δίκαιο.

Στο διάταγμα αναφέρεται ποια νομοθεσία δεσμεύει τα φυσικά ή νομικά πρόσωπα που εκδίδουν πιστοποιητικά ηλεκτρονικών υπογραφών στην Ελλάδα και στο εξωτερικό αλλά και τις ευθύνες με τις οποίες βαρύνονται οι πάροχοι υπηρεσιών πιστοποίησης. Περιέχει διατάξεις για την προστασία των προσωπικών δεδομένων στην διαδικασία έκδοσης πιστοποιητικών.

Το άρθρο 3 του Π.Δ. αναγνωρίζει ότι "η προηγμένη ηλεκτρονική υπογραφή που βασίζεται σε αναγνωρισμένο πιστοποιητικό και δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής ενέχει θέση ιδιόχειρης υπογραφής τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο". Το άρθρο 7 αναφέρεται στους παροχείς υπηρεσιών πιστοποίησης οι οποίοι υπόκεινται στις διατάξεις του ν. 2472/1997 και του ν. 2774/1999 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Η ηλεκτρονική υπογραφή αποτελεί την "ψηφιοποίηση" της κανονικής υπογραφής και την επικόλλησή της σε ένα έγγραφο. Με αυτόν τον τρόπο δεν πιστοποιείται μόνο η ταυτότητα του χρήστη αλλά και η εγκυρότητα του εγγράφου, καθώς η οποιαδήποτε εκ των υστέρων αλλοίωσή του είναι δυνατόν να εντοπιστεί.

Στα παραρτήματα αναφέρονται ποια στοιχεία πρέπει απαραίτητα να περιλαμβάνονται στα αναγνωρισμένα πιστοποιητικά και τι πρέπει να διασφαλίζουν οι διαδικασίες δημιουργίας ηλεκτρονικής υπογραφής.

Προστασία των Πνευματικών Δικαιωμάτων

Το εμπόριο στο internet θα περιλαμβάνει συχνά την πώληση και τη χορήγηση αδειών πνευματικής ιδιοκτησίας. Για την προώθηση του εμπορίου αυτού, οι πωλητές πρέπει να γνωρίζουν ότι η πνευματική τους ιδιοκτησία δεν θα κλαπεί και οι αγοραστές πρέπει να γνωρίζουν ότι αποκτούν αυθεντικά προϊόντα.

Κατά συνέπεια, είναι αναγκαίες διεθνείς συμφωνίες για τη σαφή και αποτελεσματική προστασία των δικαιωμάτων του δημιουργού, των διπλωμάτων ευρεσιτεχνίας και των εμπορικών σημάτων ώστε να αποτραπεί η πειρατεία και η απάτη. Παρόλο που η τεχνολογία μπορεί να συμβάλει στην καταπολέμηση της πειρατείας στο διαδίκτυο, χρειάζεται ένα κατάλληλο και αποτελεσματικό νομικό πλαίσιο για την αποτροπή της απάτης και της κλοπής της πνευματικής ιδιοκτησίας και για την παροχή αποτελεσματικών νομικών προσφυγών σε περίπτωση τέλεσης των αδικημάτων αυτών.

Από άποψη δικαιωμάτων πνευματικής ιδιοκτησίας, οι επιχειρήσεις πρέπει αφενός να προστατεύσουν τα δικά τους δικαιώματα πνευματικής ιδιοκτησίας και, αφετέρου, να αποφύγουν παραβάσεις. Το θέμα αυτό χρειάζεται να αντιμετωπισθεί από 4-διαφορετικές προοπτικές:

- Επαρκής νομοθετική κατοχύρωση των δικαιωμάτων πνευματικής ιδιοκτησίας,
- Καθιέρωση κατάλληλων ρυθμίσεων για τη χορήγηση αδειών,
- Εφαρμογή διαδικασιών διαχείρισης (π.χ. τήρηση μητρώων και λογιστικός έλεγχος)
- Χρήση τεχνικών μηχανισμών προστασίας (π.χ. κρυπτογράφηση).Η προστασία της πνευματικής ιδιοκτησίας πρέπει σίγουρα να καλύπτει τα ακόλουθα σημεία:
    - Δικαιώματα δημιουργού,
    - Δικαιώματα ευρεσιτεχνίας,
    - Εμπορικά σήματα και ονομασίες περιοχών.

Προστασία των Προσωπικών Δεδομένων

Είναι γνωστό, και ισχύει ιδιαίτερα για τη χώρα μας, ότι η αξία του νόμου φαίνεται κυρίως στην εφαρμογή του. Ως προς αυτό το κριτήριο, οι νέες τεχνολογίες της πληροφορίας βάζουν σε δοκιμασία μεγάλα τμήματα της παραδοσιακής νομοθεσίας. Η ποινική νομοθεσία στα προηγμένα κράτη διευρύνεται ώστε να περιλάβει νέου τύπου αδικήματα, αλλά για την αποτελεσματική εφαρμογή της χρειάζεται ακόμη κατάλληλη εκπαίδευση αστυνομικών και δικαστικών αρχών, των ίδιων των χρηστών των νέων τεχνολογιών, παράλληλη εισαγωγή τεχνικών και οργανωτικών μέτρων ασφάλειας και μέτρα για την επιτάχυνση της διεθνούς συνεργασίας.

Η νομοθεσία για την προστασία της πνευματικής ιδιοκτησίας εξελίσσεται για να καλύψει νέες ηλεκτρονικές μορφές πνευματικών έργων, αλλά για την αποτελεσματική εφαρμογή της χρειάζεται ακόμη εκπαίδευση, τόσο των δημιουργών όσο και των χρηστών των ηλεκτρονικών έργων, διαδικασίες επικοινωνίας των δύο αυτών πλευρών, τεχνικά μέσα για την παρακολούθηση της χρήσης των έργων, νέοι ευέλικτοι τρόποι για την καταβολή και διανομή του αντιτίμου των πνευματικών δικαιωμάτων. Σε αμφότερες τις περιπτώσεις η αποτελεσματικότητα τόσο της νομοθεσίας όσο και των συμπληρωματικών μέτρων θα παραμείνει αμφίβολη όσο το πεδίο εφαρμογής τους είναι μεμονωμένα ανεπτυγμένα κράτη ή και το σύνολο της Ευρωπαϊκής Ένωσης. Οι σύγχρονες τεχνολογικές εξελίξεις απαιτούν μέτρα με παγκόσμια εμβέλεια.

Αλλά και τα νεότερα αντικείμενα της νομοθεσίας, όπως η προστασία των προσωπικών δεδομένων, αν και προϊόντα των νέων τεχνολογιών, βρίσκονται διαρκώς σε δοκιμασία καθώς οι τεχνολογικές εξελίξεις δημιουργούν διαρκώς νέα προβλήματα. Τα ψηφιακά και, μελλοντικά, τα ευρυζωνικά δίκτυα θα συνδέσουν το

σύνολο της υδρογείου όπως συμβαίνει σήμερα με τις γραμμές του τηλεφώνου. Στην Ευρωπαϊκή Ένωση η δημιουργία της κοινωνίας της Πληροφορίας αποτελεί έναν από τους πρωταρχικούς στόχους του Λευκού Βιβλίου για την ανάπτυξη, την ανταγωνιστικότητα και την απασχόληση, ενώ ανάλογες επιδιώξεις έχει και η Εθνική Υποδομή Πληροφοριών (NATIONAL INFORMATION INFRASTRUCTURE) των ΗΠΑ. Με την εισαγωγή της ψηφιακής τεχνολογίας και των ηλεκτρονικών υπολογιστών σε κάθε σπίτι και σε κάθε τομέα της κοινωνικής ζωής (οικονομία , υγεία, πολιτική, περιβάλλον, μεταφορές, ψυχαγωγία, κλπ) προσωπικά δεδομένα θα μεταφέρονται μέσω ηλεκτρονικών δικτύων και θα γίνονται αντικείμενο επεξεργασίας για ποικίλους σκοπούς σε πρωτοφανή κλίμακα. Αυστηρές νομοθεσίες για την προστασία των προσωπικών δεδομένων είναι απαραίτητες ώστε να εξασφαλιστεί η συναίνεση και συμμετοχή των πολιτών στην εισαγωγή των νέων τεχνολογιών. Οι βασικές αρχές των νομοθεσιών αυτών είναι ήδη γνωστές. Περιέχονται σε όλες τις ισχύουσες Ευρωπαϊκές νομοθεσίες, στην Σύμβαση 108 του Συμβουλίου της Ευρώπης και την πρόταση Οδηγίας της Ευρωπαϊκής Ένωσης. Είναι όμως βέβαιο ότι η νομοθεσία γενικού περιεχομένου, όπως οι προαναφερθείσες, είναι μεν απαραίτητη αλλά δεν είναι αρκετή για να εξασφαλίσει τον επιδιωκόμενο στόχο, δηλαδή την προστασία του πολίτη. Θα χρειαστεί και μια σειρά από συμπληρωματικά μέτρα, για την ανάπτυξη καθενός από τα οποία θα χρειαζόταν χωριστή μελέτη. Η απαρίθμηση που ακολουθεί αποτελεί απλή διατύπωση ορισμένων εισαγωγικών σκέψεων, βασισμένων σε εμπειρίες από το διεθνή χώρο.

- Η όποια γενική νομοθεσία πρέπει να συνοδεύεται από νομοθετήματα τομεακού χαρακτήρα. Η ραγδαία εξάπλωση των νέων τεχνολογιών σε όλους τους τομείς της κοινωνικής και οικονομικής ζωής, δημιουργεί ειδικές, χωριστές ανάγκες για την προστασία των προσωπικών δεδομένων ανάλογα με τις ιδιαιτερότητες του κάθε τομέα. Από το 1981 μέχρι σήμερα το Συμβούλιο της Ευρώπης έχει υιοθετήσει μια σειρά από Συστάσεις (RECOMMENDATIONS) που καλύπτουν τις ιατρικές βάσεις δεδομένων, την κοινωνική ασφάλιση, το μάρκετινγκ, τα δεδομένα για τους εργαζόμενους, την εμπορευματοποίηση των δεδομένων του δημοσίου τομέα, τα δεδομένα της αστυνομίας, τα δεδομένα της έρευνας και της στατιστικής τις τηλεπικοινωνίες. Πρόταση τομεακής Οδηγίας για τα ψηφιακά τηλεπικοινωνιακά δίκτυα έχει ήδη υποβληθεί από την Ευρωπαϊκή Επιτροπή.

  Παράλληλα γενικού χαρακτήρα η πρόταση Οδηγίας της Ευρωπαϊκής Ένωσης ζητάει από τα Κράτη Μέλη να ενθαρρύνουν τις επαγγελματικές οργανώσεις, ώστε να υιοθετήσουν τομεακούς κώδικες δεοντολογίας, ενώ αφήνει ανοιχτό το ενδεχόμενο νέων τομεακών νομοθετικών προτάσεων. Τα νομοθετήματα και οι κώδικες δεοντολογίας τομεακού χαρακτήρα, έχουν ένα κοινό χαρακτηριστικό, ότι στον βαθμό που εκπονούνται σε στενή συνεργασία με (ή από τους ίδιους τους) ενδιαφερομένους φορείς, συμβάλουν αποφασιστικά στην ευαισθητοποίηση των χρηστών των

προσωπικών δεδομένων σε κάθε τομέα. Έχουν όμως και μία θεμελιώδη διαφορά, ότι τα πρώτα έχουν νομική ισχύ δημοσίου δικαίου (που αποκτά ιδιαίτερη σημασία εφόσον προβλέπονται αυστηρές κιρρώσεις)ενώ οι δεύτεροι επαφίενται στη "μονιμοφροσύνη " των μελών ων επαγγελματικών οργανώσεων (δεν είναι βέβαιο ότι δεσμεύουν και τα μη μέλη του συγκεκριμένου τομέα) και στην αποφασιστικότητα εθελοντικών διαχειριστικών οργάνων όσο αναφορά την επιβολή κυρώσεων. Και αν σε ορισμένα κράτη μέλη της Ευρωπαϊκής Ένωσης όπως η Βρετανία, η Ιρλανδία και η Ολλανδία, υπάρχει μακρά και σχετικά επιτυχής παράδοση τέτοιων μορφών αυτοδιαχείρισης, η αποτελεσματικότητά τους στις χώρες τις νότιας Ευρώπης και ειδικά στην Ελλάδα, όπου και οι ίδιοι οι νόμοι συχνά δεν εφαρμόζονται, είναι εξαιρετικά αμφίβολη. Χρειάζεται νομοθετική παρέμβαση με τη μεγαλύτερη δυνατή συμμετοχή των ενδιαφερομένων φορέων, τόσο για την πληρότητα του νομοθετήματος όσο και για την ενημέρωση των χρηστών των προσωπικών δεδομένων. Κεφαλαιώδους σημασίας είναι ο ρόλος της υπηρεσίας ελέγχου που προβλέπεται από όλες τις ευρωπαϊκές νομοθεσίες και από την πρόταση Οδηγίας της Ευρωπαϊκής Ένωσης. Η υπηρεσία αυτή ελέγχει κατά κανόνα τόσο τον ιδιωτικό όσο και τον δημόσιο τομέα, επομένως πρέπει να είναι ουσιαστικά ανεξάρτητοι από την κυβέρνηση. Σε περίπτωση αμφισβητήσεων, των τελευταίο ρόλο έχει η δικαστική εξουσία και όχι ο Υπουργός Δικαιοσύνης ή το Υπουργικό Συμβούλιο. Η υπηρεσία ελέγχου πρέπει να έχει εξουσίες τόσο κατασταλτικές (άσκηση ελέγχου, απαγόρευση παράνομης επεξεργασίας δεδομένων, προσφυγή στην δικαιοσύνη), όσο και προληπτικές (έκδοση ερμηνευτικών εγκυκλίων, οργάνωση εκπαιδευτικών σεμιναρίων, θεσμοθετημένο διάλογο με τις ομάδες των χρηστών, συμβολή στην σύνταξη κωδικών δεοντολογίας). Υπάρχουν θαυμάσιες συγκριτικές μελέτες για ορισμένες ευρωπαϊκές χώρες, από τις οποίες μπορούν να αντληθούν χρήσιμα συμπεράσματα. Πρέπει ακόμα να έχει στην διάθεσή της επαρκή μέσα ώστε να ασκήσει επιτυχώς τα καθήκοντά της. Είναι διαφωτιστική η περίπτωση του σκανδάλου της εμπορευματοποίησης προσωπικών δεδομένων του δημοσίου στην Νότια Ουαλλία της Αυστραλίας, που αποκαλύφθηκε το 1990-1992, από την αρμόδια υπηρεσία ελέγχου, που είχε πενιχρά μέσα (π.χ. συνολικό προσωπικό 6 ατόμων), αλλά από την Ανεξάρτητη Επιτροπή εναντίον τις Διαφθοράς που έχει ετήσιο προϋπολογισμό άνω των 100 εκατομ. δολαρίων. Πρέπει επίσης η υπηρεσία ελέγχου να έχει πρόσβαση στην δημοσιότητα και κυρίως στα μέσα μαζικής ενημέρωσης και στο Κοινοβούλιο. Σε μια συνειδητοποιημένη κοινωνία-όπως αναπτύσσεται στην επόμενη παράγραφο-ο φόβος της αρνητικής δημοσιότητας λειτουργεί ως αποτρεπτικός παράγων για παράνομες πράξεις. Πρέπει τέλος στις αρμοδιότητες (αλλά και στις δυνατότητες) της υπηρεσίας ελέγχου να περιλαμβάνεται και η

συνεργασία με τις αντίστοιχες υπηρεσίες άλλων κρατών. Αυτό γίνεται ολοένα περισσότερο αναγκαίο όσο τα τηλεπικοινωνιακά δίκτυα και η πρόοδος της τεχνολογίας διευκολύνουν τη μεταφορά και επεξεργασία προσωπικών δεδομένων σε οποιαδήποτε χώρα της υδρογείου.

- Στις υπηρεσίες ελέγχου ανήκουν οι σημαντικές εξουσίες που προαναφέρθηκαν. Τελικώς κριτής της εφαρμογής του νομού και αρμόδιες για την επιβολή κυρώσεων είναι ο δικαστής. Και αν οι υπηρεσίες ελέγχου διαθέτουν στο στελεχιακό τους δυναμικό τόσο νομομαθείς όσο και ειδικούς της πληροφορικής, που εξειδικεύονται στην εφαρμογή του νόμου με την πείρα που αποκτούν, οι δικαστές σπάνια διαθέτουν ειδικές γνώσεις είτε του δικαίου τις πληροφορικής είτε των εφαρμογών της πληροφορικής σε όλες τις πτυχές της κοινωνικής και οικονομικής ζωής. Για την διαπίστωση της νομιμότητας συγκεκριμένης επεξεργασίας δεδομένων ο νόμος δεν περιέχει πάντοτε ρητές προϋποθέσεις, αλλά παραπέμπει στη συγκριτική εκτίμηση των συμφερόντων τόσο των προσώπων που αφορά η επεξεργασία όσο και των χρηστών που προβαίνουν στην επεξεργασία. Είναι βέβαιο ότι από την γενική φύση τους και τουλάχιστον μέχρι να υπάρχουν πολυάριθμα τομεακά νομοθετήματα για την προστασία των προσωπικών δεδομένων θα αφήσουν μεγάλο πεδίο ερμηνείας και εξειδίκευσης στην νομολογία. Αυτό δεν αφορά βεβαίως μόνο στην προστασία των προσωπικών δεδομένων, αλλά στο σύνολο του δικαίου που επηρεάζεται ή και δημιουργείται από την πληροφορική. Κάποια επιμόρφωση (και μάλιστα διαρκής) των δικαστών θα ήταν επομένως εξαιρετικά χρήσιμη. Με την εξάπλωση της χρήσης των νέων τεχνολογιών της πληροφορίας σε παγκόσμιο επίπεδο και των δυνατοτήτων κατάχρησης προσωπικών δεδομένων, ιδιαίτερα σε χώρες όπου η νομοθεσία είναι από ανεπαρκής έως ανύπαρκτη ή ο νόμος παραβιάζεται από ισχυρά συμφέροντα (είτε του δημοσίου είτε του ιδιωτικού τομέα), το πλέον αποτελεσματικό όπλο για την προστασία των προσωπικών δεδομένων είναι η συμμετοχή της κοινωνίας. Ο πολίτης πρέπει να μάθει, με σαφήνεια και χωρίς υπερβολές, ποια είναι τα οφέλη καθώς και ποια είναι τα σχετικά δικαιώματά του και ποιοι οι κίνδυνοι από την επεξεργασία των προσωπικών του δεδομένων. Παράλληλα, οι χρήστες πρέπει να ενημερωθούν για τις υποχρεώσεις που επιβάλλει η νομοθεσία. Το ζητούμενο είναι να βρεθούμε στην πορεία που σήμερα ακολουθεί, τουλάχιστον στις ανεπτυγμένες χώρες η προστασία του περιβάλλοντος που περιλαμβάνεται ήδη στον σχεδιασμό παραγωγής και στην εκστρατεία μάρκετινγκ πολλών προϊόντων. Να φτάσουμε δηλαδή στο σημείο όπου σε συνθήκες ελεύθερου ανταγωνισμού ο πολίτης θα προτιμά εκείνες τις υπηρεσίες (τηλεπικοινωνιών, πιστωτικών καρτών, πωλήσεων από απόσταση, ιατρικής

περίθαλψης, κλπ) που θα σέβονται και θα προστατεύουν τα προσωπικά του δεδομένα. Από τις ευρωπαϊκές χώρες ο υψηλότερος βαθμός ενδιαφέροντος των πωλητών, παρατηρείται στη Γερμανία και αυτό έχει συμβάλλει στη θέσπιση αυστηρής, γενικής και τομεακής, νομοθεσίας και σε νομολογία όπως η περίφημη απόφαση του συνταγματικού δικαστηρίου της Καρλσρούης που αναγνωρίζει στον πολίτη δικαίωμα "πληροφοριακής αυτοδιάθεσης". Είναι ενδιαφέρουσα η διαφορά ανάμεσα στο πνεύμα της Γερμανικής νομοθεσίας που στηρίζει την νομιμότητα της επεξεργασίας προσωπικών δεδομένων κυρίως στην συναίνεση του πολίτη και της Γαλλικής νομοθεσίας, όπου η νομιμότητα στηρίζεται στην έγκριση της υπηρεσίας ελέγχου. Για να είναι σε θέση να εκτιμήσει τις περιστάσεις και να συναινέσει, ο πολίτης πρέπει να είναι ενημερωμένος, και αυτό είναι φυσικά υποχρέωση του κράτους.

- Η εξέλιξη των νέων τεχνολογιών πληροφορίας και τηλεπικοινωνιών, καθιστά ολοένα και δυσκολότερο τον έλεγχο της επεξεργασίας των προσωπικών δεδομένων με "παραδοσιακούς" τρόπους καθώς η ποσότητα των δεδομένων που γίνονται αντικείμενο επεξεργασίας, ο συνολικός αριθμός των χρηστών τέτοιων δεδομένων και η ταχύτητα μεταφοράς των δεδομένων μέσω τηλεπικοινωνιών δικτύων αυξάνονται ραγδαίως. Η λύση του προβλήματος αυτού βρίσκεται σε μεγάλο βαθμό στην ίδια την τεχνολογία. Είναι τεχνικά δυνατό στο σχεδιασμό του λογισμικού που χρησιμοποιείται για την επεξεργασία των προσωπικών δεδομένων, για σκοπούς π.χ. εργασιακούς, ιατρικής περίθαλψης, κοινωνικών ασφαλίσεων, εμπορικών συναλλαγών, έρευνας αγοράς, κλπ, να περιλαμβάνονται κανόνες για την αποτελεσματική προστασία των προσωπικών δεδομένων, που θα επιτρέπουν δηλαδή επεξεργασία προσωπικών δεδομένων στο βαθμό που είναι απολύτως αναγκαίος για τους συγκεκριμένους σκοπούς, που θα σβήνουν ή "παγώνουν" τα δεδομένα όταν δεν απαιτούνται πλέον για τους σκοπούς αυτούς, που θα επιτρέπουν την πρόσβαση μόνο σε εξουσιοδοτημένα πρόσωπα, που θα διευκολύνουν την παρακολούθηση της πορείας των δεδομένων προς τους διάφορους αποδέκτες-χρήστες. Ειδικό λογισμικό είναι δυνατόν να κατασκευαστεί και για τις ανάγκες των υπηρεσιών ελέγχου, έτσι ώστε να διευκολύνεται και να επιταχύνεται ο έλεγχος των δηλώσεων επεξεργασίας που υποβάλλουν οι χρήστες και τις οποίες επιβάλλουν οι περισσότερες ευρωπαϊκές νομοθεσίες και η πρόταση Οδηγίας της Ε.Ε. Είναι προφανές ότι η βιομηχανία λογισμικού θα προχωρήσει προς αυτή την κατεύθυνση όταν υπάρξει σχετική ζήτηση από την αγορά. Και η ζήτηση θα υπάρξει όταν, όπως προαναφέρθηκε, η προστασία των προσωπικών δεδομένων θα είναι μέρος του κοινωνικού προβληματισμού και μέρος της εμπορικής πολιτικής και επιχειρήσεων.

Σε ένα άλλο κλάδο του δικαίου, εκείνο της προστασίας της πνευματικής ιδιοκτησίας, όπου τα οικονομικά συμφέροντα για την προστασία των ηλεκτρονικών πνευματικών έργων (βάσεων δεδομένων, υπηρεσιών ψυχαγωγίας, MULTIMEDIA) είναι ήδη ισχυρά, έχουν γίνει σημαντικά βήματα από την ίδια την τεχνολογία. Χάρις στο υποπρόγραμμα CITED που συγχρηματοδοτήθηκε από την Ε.Ε. στα πλαίσια του προγράμματος ESPRIT, η παραγωγή τέτοιων έργων έχουν σήμερα την τεχνολογική δυνατότητα να ελέγχουν πλήρως την χρήση των έργων τους από κάθε κατηγορία χρηστών και να εισπράττουν αυτομάτως το αντίτιμο των δικαιωμάτων τους, ανάλογα με τη συγκεκριμένη χρήση και κατηγορία χρήστη. Για την προστασία των προσωπικών δεδομένων κάποιες μελέτες τεχνολογικού χαρακτήρα έχουν προγραμματιστεί στα πλαίσια του προγράμματος της Ε.Ε. για την ασφάλεια των πληροφοριών, που έχει ως στόχο την επίτευξη του τρίπτυχου "εμπιστευτικότητα, πληρότητα, διαθεσιμότητα" (confidentiality, integrity, availability) για τις ηλεκτρονικές πληροφορίες. Μέτρα για την ασφάλεια των προσωπικών δεδομένων απαιτούνται βέβαια από την κάθε ευρωπαϊκή νομοθεσία και από την πρόταση Οδηγίας της Ε.Ε. Αλλά τα μέτρα αυτά είναι ένα μικρό μέρος της πιθανής συμβολής της τεχνολογίας στην αποτελεσματική προστασία των προσωπικών δεδομένων.

- Αν οι νέες τεχνολογίες πληροφοριών αφορούν ένα διαρκώς αυξανόμενο αριθμό ανθρωπίνων δραστηριοτήτων και αν η προστασία των προσωπικών δεδομένων είναι ένα από τα θεμελιώδη δικαιώματα του ανθρώπου, τότε οι ανθρώπινες δραστηριότητες που περιλαμβάνουν επεξεργασία δεδομένων-ή τουλάχιστον ορισμένες από αυτές που θα θεωρηθούν εν δυνάμει περισσότερο επιβλαβής- θα πρέπει να συνοδεύονται από έκθεση των επιπτώσεων της συγκεκριμένης επεξεργασίας για τα προσωπικά δεδομένα. Αυτό ήδη συμβαίνει με την προστασία του περιβάλλοντος. Σύμφωνα με το άρθρο 130 παράγραφος 2 της Ενιαίας Πράξης, όπως έχει ενσωματωθεί στην Συνθήκη για την Ε.Ε., "η ανάγκες στον τομέα της προστασίας του περιβάλλοντος πρέπει να λαμβάνονται υπόψη στον καθορισμό και την εφαρμογή των άλλων πολιτικών της Κοινότητας ". Κάτι ανάλογο θα χρειαστεί και για τα προσωπικά δεδομένα και θα συμβάλλει θετικά στο έργο των υπηρεσιών ελέγχου, στην άσκηση των δικαιωμάτων τους από τους ίδιους τους πολίτες και στη συνειδητοποίηση των χρηστών.

- Όλα όσα αναφέρθηκαν στις προηγούμενες παραγράφους, δηλαδή η θέσπιση τομεακών νομοθετημάτων, η κατάλληλη υποστήριξη των υπηρεσιών ελέγχου, η επιμόρφωση των δικαστών, η συνειδητοποίηση των πολιτών, η παραγωγή κατάλληλου λογισμικού, η έκθεση για της επιπτώσεις της επεξεργασίας των προσωπικών

δεδομένων, θα έχουν μικρή αποτελεσματικότητα αν είναι δυνατή η ανεξέλεγκτη επεξεργασία προσωπικών δεδομένων σε κάποιες τρίτες χώρες. Τεχνικά αυτό είναι εξαιρετικά εύκολο, ενώ ο πλήρης προληπτικός έλεγχος της εξαγωγής δεδομένων είναι αδύνατος. Δειγματοληπτικός έλεγχος ή κυρώσεις για παράνομη εξαγωγή που αποκαλύπτεται εκ των υστέρων έχουν βέβαια και κάποια προληπτική επίδραση, αλά πιθανότατα αφορούν μόνο την κορυφή του παγόβουνου. Η Ευρώπη-κυρίως η διευρυμένη Ε.Ε. με εξαίρεση την Ελλάδα και την Ιταλία- προηγείται σημαντικά, σε ότι αφορά την νομοθεσία προστασίας των προσωπικών δεδομένων, όλων ανεξαιρέτως των τρίτων κρατών, συμπεριλαμβανομένων των κυρίων ανταγωνιστών της στον τομέα των νέων τεχνολογιών πληροφόρησης, των ΗΠΑ, της Ιαπωνίας και των ταχέως αναπτυσσόμενων κρατών της Άπω Ανατολής. Αν η κατάσταση αυτή παραμείνει- και μέχρι να σημειωθούν οι εξελίξεις που πιθανολογούνται στην παράγραφο 4- τότε θα κινδυνεύσουν σοβαρά όχι μόνο ιδιωτική ζωή και τα δικαιώματα των Ευρωπαίων πολιτών αλλά και η ανταγωνιστικότητα των Ευρωπαϊκών εταιριών που επεξεργάζονται προσωπικά δεδομένα και που αφενός υποχρεώνονται να λάβουν μέτρα προστασίας που έχουν οικονομικό κόστος και αφετέρου δεν έχουν το δικαίωμα να κάνουν χρήση προσωπικών δεδομένων με την ευχέρεια των ανταγωνιστών τους στις τρίτες χώρες. Θα πρέπει λοιπόν οι διατάξεις των άρθρων 26 και 27 της πρότασης Οδηγίας της Ε.Ε. να τηρηθούν με αυστηρότητα, έτσι ώστε να θεσπιστεί επαρκείς σχετική νομοθεσία και στις χώρες αυτές. Ήδη παρατηρούνται θετικές εξελίξεις σε ορισμένες τρίτες χώρες, που είναι αποτέλεσμα και της πρότασης Οδηγίας. Στο QUEBEC το πεδίο εφαρμογής του νόμου διευρύνθηκε και περιλαμβάνει τώρα και τον ιδιωτικό τομέα. Η θέσπιση νομοθεσίας στη Νέα Ζηλανδία επιταχύνθηκε από την πρόταση Οδηγίας. Νομοθεσία πολύ παραπλήσια με την πρόταση Οδηγίας εξετάζεται στο HONG-KONG. Στις ΗΠΑ, σε συνδυασμό και με πρωτοβουλίες για την Εθνική Υποδομή Πληροφοριών (NII) το ζήτημα της προστασίας της ιδιωτικής ζωής έρχεται σιγά-σιγά στο προσκήνιο. Θα πρέπει, τέλος, να επισημανθεί ότι για την παρακολούθηση της πρακτικής των τρίτων χωρών στο ζήτημα της επεξεργασίας των προσωπικών δεδομένων, ιδιαίτερα χρήσιμοι είναι η σχετική εργασία κάποιων ιδιωτικών φορέων από τους οποίους ο περισσότερο γνωστός ονομάζεται PRIVACY INTERNATIONAL (προφανώς κατά το πρότυπο της AMNESTY INTERNATIONAL) και καλύπτει ευρύτατο αριθμό κρατών.

- Όλες οι προηγούμενες παράγραφοι έχουν ως αφετηρία το πραγματικό γεγονός της διαρκώς αυξανόμενης επεξεργασίας και μεταφοράς προσωπικών δεδομένων. Αλλά δεν υπάρχει αμφιβολία ότι απολύτως αποτελεσματική για των πολίτη είναι η προστασία

όταν τα προσωπικά του δεδομένα δεν γίνονται αντικείμενα επεξεργασίας. Ο πολίτης θα πρέπει να έχει, όταν αυτό είναι δυνατό, δικαίωμα επιλογής ανάμεσα σε λύσεις που περιλαμβάνουν και σε λύσεις που δεν περιλαμβάνουν επεξεργασία προσωπικών δεδομένων (π.χ. ανάμεσα σε πληρωμή με πιστωτική κάρτα και τοις μετρητοίς). Από την πλευρά των χρηστών θα πρέπει να αποφεύγεται η επεξεργασία προσωπικών δεδομένων χωρίς σοβαρό λόγο (και, φυσικά, να ακολουθούνται οι επιταγές του νόμου, εφόσον γίνεται τέτοια επεξεργασία). Οι δυνατότητες των νέων τεχνολογιών δεν αποτελούν επαρκή λόγο για την επεξεργασία προσωπικών δεδομένων, αλλά εργαλείο που θα πρέπει να χρησιμοποιείται όταν τέτοια επεξεργασία είναι απαραίτητη. Στις περισσότερες χώρες του κόσμου και, δυστυχώς, στη χώρα μας η προστασία των προσωπικών δεδομένων δε έχει βρεθεί μέχρι τώρα στο επίκεντρο της επικαιρότητας και του δημόσιου ενδιαφέροντος. Η ευκαιρία δίνεται τώρα ,στους επόμενους μήνες, όταν τα προγράμματα εργασίας της Ε.Ε., για την κοινωνία της πληροφορίας και των ΗΠΑ για την Εθνική Υποδομή Πληροφοριών, θα πάρουν συγκεκριμένη μορφή. Αμφότερα περιλαμβάνουν, στο σημερινό προκαταρκτικό στάδιο, διακηρύξεις υπέρ της προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής. Αν μείνουν στα λόγια μαζί με τις "λεωφόρους της πληροφορίας" θα ανοίξει ο δρόμος για καταχρήσεις προσωπικών δεδομένων που θα υπονομεύσουν την κοινωνική αποδοχή και την βιωσιμότητά τους. Αν προετοιμαστούν, με σοβαρότητα θα ανοίξουν αναμφίβολα νέους δρόμους για την ανθρωπότητα.

Η Αναγκαιότητα του Θεσμικού Ελέγχου της Προστασίας των Προσωπικών Πληροφοριών

Η ανάγκη προστασίας του πολίτη από τους κινδύνους, που προκύπτουν από τη συλλογή, επεξεργασία και γενικότερα αξιοποίηση προσωπικών πληροφοριών ανάγεται σε εποχές προγενέστερες των ηλεκτρονικών υπολογιστών, ήταν ωστόσο η ανάπτυξη των νέων τεχνολογιών αυτή που την κατέστησε επιτακτική. Δεν είναι τυχαίο ότι ο νομοθέτης τεχνολογικά ανεπτυγμένων κρατών αντέδρασε πρώτος στην ανάγκη αυτή θεσπίζοντας διατάξεις, οι οποίες έθεταν το θεσμικό πλαίσιο της νομικής επεξεργασίας και χρήσης των πληροφοριών προσωπικού χαρακτήρα. Παρά τις διαφορετικές προσεγγίσεις των επιμέρους προβλημάτων νομοθέτες και επιστημονική κοινότητα συνέκλιναν ευθύς εξαρχής στην παραδοχή ότι οι ουσιαστικές ρυθμίσεις μπορούν να αποδειχτούν κενές περιεχομένου και στερούμενες ρυθμιστικής ικανότητας , εάν δεν συνοδεύονται από διατάξεις και διαδικασίες που διασφαλίζουν τη διαφάνεια των πληροφοριακών ροών και την άσκηση ελέγχου.

- Το δικαίωμα πρόσβασης του πολίτη: αναγκαίος αλλά μη επαρκής όρος της αποτελεσματικής προστασίας

Πολλοί – αν και από διαφορετικές οπτικές γωνίες – Θεωρούν την άσκηση ελέγχου πρωτίστως δικαίωμα και καθήκον του ατόμου. Όλες οι εθνικές νομοθεσίες κατοχυρώνουν το "δικαίωμα πρόσβασης" του ιδιώτη/ πολίτη, δηλαδή το δικαίωμά του να μαθαίνει, ποιες προσωπικές του πληροφορίες αποτελούν αντικείμενο συλλογής, επεξεργασίας και μετάδοσης σε τρίτους. Ο ιδιώτης μπορεί μάλιστα να επέμβει στην διαμόρφωση των πληροφοριών αυτών στο βαθμό που δικαιούται να ζητήσει την διόρθωση, συμπλήρωση, τροποποίηση, διευκρίνιση ή διαγραφή των ανακριβών, ασαφών ή αναληθών πληροφοριών που αφορούν το πρόσωπό του.

- Η ανάγκη ύπαρξης ενός ειδικού και ανεξάρτητου ελεγκτικού μηχανισμού

Το βασικό μειονέκτημα του ατομικού ελέγχου εντοπίζεται ακριβώς στο γεγονός ότι αφορά μια ατομική περίπτωση. Μόνο μια συνολική θεώρηση και επιθεώρηση της διαδικασίας επεξεργασίας των προσωπικών πληροφοριών αλλά και της οργάνωσης της διοικητικής αρχής ή επιχείρησης, που προβαίνει σε αυτή, επιτρέπει τη συναγωγή – σχετικά – ασφαλών συμπερασμάτων αναφορικά με την νομιμότητα της όλης διαδικασίας. Το δικαίωμα πρόσβασης, έστω και σε κατάσταση αδράνειας, αναπτύσσει βέβαια μια προληπτική – αποτρεπτική ενέργεια, η αποτελεσματική εφαρμογή της νομοθεσίας όμως προϋποθέτει τη θέσπιση του θεσμικού ελέγχου της προστασίας προσωπικών πληροφοριών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Βλαχοπούλου Μάρω: «e-Marketing Διαδικτυακό Μάρκετινγκ», εκδόσεις Rosili, 2003.

[2] Γεωργακόπουλος Νικόλαος: « Ηλεκτρονικό Επιχειρείν», εκδόσεις Μπένου, 2001.

[3] Δουκίδης Γεώργιος: «Ηλεκτρονικό Εμπόριο», εκδόσεις Νέων Τεχνολογιών, 2001.

[4] Πασχόπουλος Αρσένης: «Ηλεκτρονικό Εμπόριο», εκδόσεις Κλειδάριθμος, 2001.

[5] Σαμαράς Ιωάννης: «Το Marketing στο Internet», εκδόσεις Γκιούρδας, 2001.

[6] Γκρίτζαλης Δ.: «Ασφάλεια Πληροφοριακών Συστημάτων», έκδοση ΕΠΥ., Αθήνα 2001.

[7] Γκρίτζαλης Δ., « Ασφάλεια Πληροφοριακών Συστημάτων σε Περιβάλλοντα υψηλής Ευπάθειας», Διδακτορική διατριβή, Πανεπιστήμιο Αιγαίου (Μαθηματικό Τμήμα), Μάρτιος 1994.

[8] Τραπεζάνογλου Β., «Προσωπικές Πληροφορίες και Υπολογιστές», Νέα Οικολογία, Μάιος 1985.

[9] Πασιάς Α., «Πληροφορική και Δίκαιο», Δοκίμια Ελληνικής Εταιρείας Νομικής Πληροφορικής, Θεσσαλονίκη 1987.

[10] Γ. Δουκίδης, Γ. Γιαγλής, Γ. Παππάς, Β. Ζαρογιάννη, Β. Περγιουδάκης, «Ηλεκτρονικό Εμπόριο και Ηλεκτρονική Ανταλλαγή Δεδομένων», 1996.

[11] Εκδόσεις Νέων Τεχνολογιών, «Ασφάλεια Πληροφοριών», Αθήνα 1995.

[12] Minker J., "Scientific freedom and human rights of computer professionals", in Com. Of the ACM, Vol.32, no 8, pp.957-974, August 1989.

[13] Ravi Kalakota, Andrew Whinston "Managing Electronic Commerce".

[14] Ravi Kalakota, Andrew Whinston "Frontiers of Electronic Commerce", Adison Weslay 1996.

[15] Rossiter, J.R and Percy, "L Advertising & Promotion Management", McGrawHill, New York, 1987.

ΔΙΑΔΙΚΤΥΟ

[1] http://www.go-online.gr/ebusiness/specials/article.html?article_id=408

[2] http://www.go-online.gr/ebusiness/specials/article.html?article_id=536

[3] http://www.go-online.gr/ebusiness/specials/article.html?article_id=561

[4] http://www.go-online.gr/ebusiness/specials/article.html?article_id=562

[5] http://www.go-online.gr/ebusiness/specials/article.html?article_id=563

[6] http://www.go-online.gr/ebusiness/specials/article.html?article_id=564

[7] http://www.go-online.gr/ebusiness/specials/article.html?article_id=566

[8] http://www.go-online.gr/ebusiness/specials/article.html?article_id=618

[9] http://www.go-online.gr/ebusiness/specials/article.html?article_id=673

[10] http://www.go-online.gr/ebusiness/specials/article.html?article_id=681

[11] http://www.go-online.gr/ebusiness/specials/article.html?article_id=682

[12] http://www.go-online.gr/ebusiness/specials/article.html?article_id=683

[13] http://www.go-online.gr/ebusiness/specials/article.html?article_id=684

[14] http://www.go-online.gr/ebusiness/specials/article.html?article_id=710

[15] http://www.go-online.gr/ebusiness/specials/article.html?article_id=712

[16] http://www.researchintl.com

[17] http://www.icap.gr

[18] http://www.focus.gr

[19] http://www.gartner.com

[20] http://www.mediametrix.com

[21] http://www.business.com

[22] http://www.bancamerica.com

[23] http://www.nua.ie