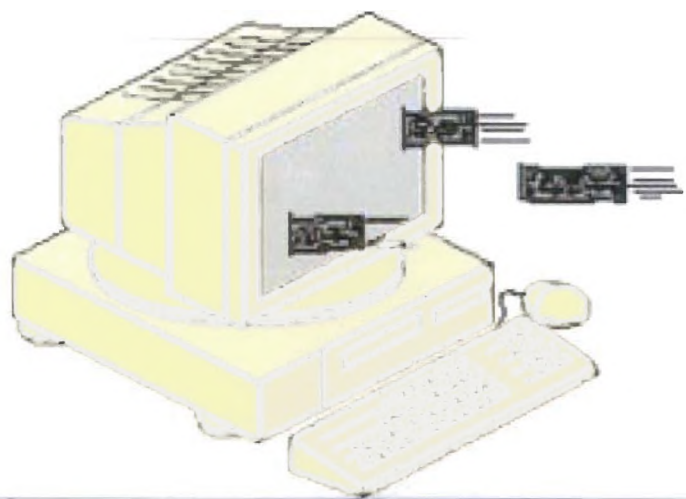




Πτυχιακή Εργασία



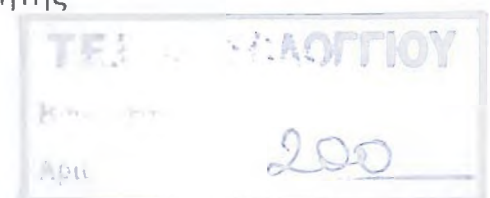
ΣΥΣΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ

ΑΠΟΣΤΟΛΟΠΟΥΛΟΥ ΒΑΣΙΛΙΚΗ

A.M. : 9476

Επιβλέπων **Σπύρος Συρμακέσης**, Επίκουρος Καθηγητής

Σεπτέμβριος 2005



Αφιερωμένο στα
φοιτητικά μου χρόνια

Πίνακας Περιεχομένων

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ	3
ΠΙΝΑΚΑΣ ΣΧΗΜΑΤΩΝ	5
1. ΕΙΣΑΓΩΓΗ	6
2. ΜΕΘΟΔΟΛΟΓΙΚΗ ΠΡΟΣΕΓΓΙΣΗ	8
3. ΟΡΙΣΜΟΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ - ΔΙΑΚΡΙΣΕΙΣ	10
4. ΣΥΣΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ	13
4.1 ΠΑΡΑΔΟΣΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΠΡΟΣΑΡΜΟΣΜΕΝΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ	17
4.2 ΚΑΙΝΟΤΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ ΓΙΑ ΤΟ ΔΙΑΔΙΚΤΥΟ	38
4.3 ΚΙΝΗΤΕΣ ΠΛΗΡΩΜΕΣ (MOBILE PAYMENTS)	48
4.3.1 ΑΠΟ ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΣΤΟ ΚΙΝΗΤΟ ΕΜΠΟΡΙΟ.....	53
4.3.2 ΟΙ ΠΑΙΚΤΕΣ ΤΟΥ ΚΙΝΗΤΟΥ ΕΠΙΧΕΙΡΕΙΝ.....	61
5. ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ	64
5.1 ΣΥΝΙΣΤΩΣΕΣ ΑΣΦΑΛΕΙΑΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ	64
5.1.1 ΜΕΘΟΔΟΙ ΑΣΦΑΛΕΙΑΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΝΑΛΛΑΓΩΝ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΕΣ ΥΠΟΓΡΑΦΕΣ.....	64
5.2 ΤΕΧΝΟΛΟΓΙΕΣ ΠΟΥ ΕΞΑΣΦΑΛΙΖΟΥΝ ΥΨΗΛΑ ΕΠΙΠΕΔΑ ΑΣΦΑΛΕΙΑΣ ΣΤΙΣ ΣΥΝΑΛΛΑΓΕΣ	67
5.2.1 ΠΙΣΤΟΠΟΙΗΣΗ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ (PKI ΚΑΙ PGP).....	67
5.2.1.1 <i>Είδη Ηλεκτρονικών Πιστοποιητικών</i>	68
5.2.1.2 <i>Μορφή και περιεχόμενο των η-Πιστοποιητικών (X.509)</i>	69
5.2.1.3 <i>Ο έλεγχος του κύρους των η-πιστοποιητικών και των η-υπογραφών</i>	69
5.3 ΣΥΜΜΕΤΡΙΚΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ	71
5.3.1 ΑΣΥΜΜΕΤΡΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ.....	71
5.4 ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ	74
5.4.1 ΤΙ ΠΡΟΒΛΕΠΕΙ ΤΟ ΓΣΧΥΟΝ ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΥΠΟΓΡΑΦΕΣ.....	74
5.4.2 ΠΩΣ ΛΕΙΤΟΥΡΓΟΥΝ ΟΙ ΠΡΟΗΓΜΕΝΕΣ ΨΗΦΙΑΚΕΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΥΠΟΓΡΑΦΕΣ.....	76
5.4.3 ΤΙ ΕΞΟΠΛΙΣΜΟΣ ΑΠΑΙΤΕΙΤΑΙ ΓΙΑ ΤΗ ΔΗΜΙΟΥΡΓΙΑ ΚΑΙ ΤΗΝ ΕΠΑΛΗΘΕΥΣΗ ΤΩΝ Η - ΥΠΟΓΡΑΦΩΝ..	78
5.4.4 ΤΙ ΠΡΕΠΕΙ ΝΑ ΠΡΟΣΕΧΕΙ Ο 'ΥΠΟΓΡΑΦΩΝ' ΚΑΙ ΤΙ Ο 'ΑΠΟΔΕΚΤΗΣ' RELYING PARTY ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΓΡΑΦΩΝ.....	79
5.4.5 ΠΟΙΕΣ ΕΙΝΑΙ ΣΗΜΕΡΑ ΟΙ ΣΗΜΑΝΤΙΚΟΤΕΡΕΣ ΕΦΑΡΜΟΓΕΣ ΚΑΙ ΠΟΙΕΣ ΟΙ ΠΡΟΟΠΤΙΚΕΣ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΓΡΑΦΩΝ.....	81
5.5 ΠΑΡΑΔΕΙΓΜΑΤΑ ΑΣΥΜΜΕΤΡΩΝ ΤΕΧΝΙΚΩΝ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ	82
6. ΣΥΣΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ ΣΤΙΣ ΧΩΡΕΣ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ	91
7. ΣΥΣΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ ΣΤΗΝ ΕΥΡΩΠΑΪΚΗ ΕΝΩΣΗ	94

8. ΕΛΛΗΝΙΚΑ ΗΛΕΚΤΡΟΝΙΚΑ ΚΑΤΑΣΤΗΜΑΤΑ: ΙΣΧΥΟΥΣΕΣ ΜΕΘΟΔΟΙ ΠΛΗΡΩΜΗΣ.....	97
9. ΚΑΙΝΟΤΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ ΣΤΗΝ ΕΛΛΑΔΑ ..	99
9.1 ΕΓΝΑΤΙΑΡΕΡΕΡΑΥ	99
9.2 ΑΤΤΙΣΑ GIFT CARD VISA.....	102
9.3 ΧΡΥΣΗ ΕΥΚΑΙΡΙΑ – ΑΓΟΡΕΣ ΑΓΓΕΛΙΩΝ ΜΕΣΩ ΚΙΝΗΤΟΥ	104
10. ΤΟ ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΛΗΡΩΜΕΣ	107
10.1 ΕΥΡΩΠΑΪΚΗ ΝΟΜΟΘΕΣΙΑ.....	108
10.2 ΕΛΛΗΝΙΚΗ ΝΟΜΟΘΕΣΙΑ	114
11. ΔΙΑΠΙΣΤΩΣΕΙΣ	118
12. ΠΡΟΤΑΣΕΙΣ ΕΡΓΑΣΙΑΣ.....	122
12.1 ΠΡΟΣ ΤΗΝ ΠΟΛΙΤΕΙΑ.....	122
12.2 ΠΡΟΣ ΤΙΣ ΤΡΑΠΕΖΕΣ ΚΑΙ ΕΤΑΙΡΕΙΕΣ.....	123
13. ΒΙΒΛΙΟΓΡΑΦΙΑ	124

Πίνακας Σχημάτων

<i>Εικόνα 1: Αίτηση εγγραφής Νομικού Προσώπου</i>	23
<i>Εικόνα 2: Αίτηση εγγραφής Φυσικού προσώπου</i>	25
<i>Εικόνα 3: Εισαγωγή πάγιας εντολής</i>	27
<i>Εικόνα 4: Εισαγωγή στοιχείων</i>	28
<i>Εικόνα 5: Δείγμα εντύπου</i>	28
<i>Εικόνα 6: Προώθηση πάγιας εντολής</i>	29
<i>Εικόνα 7: Όροι ένταξης στο σύστημα E-Banking</i>	29
<i>Εικόνα 8: Εξόφληση Πάγιας εντολής</i>	30
<i>Εικόνα 9: Αναζήτηση εντολών</i>	30
<i>Εικόνα 10: Μεταβολή στοιχείων πάγιας εντολής</i>	31
<i>Εικόνα 11: Καταχωρήσεις</i>	31
<i>Εικόνα 12: Προώθηση Εντολής</i>	32
<i>Εικόνα 13: Καταχώρηση εντολής</i>	32
<i>Εικόνα 14: Επιλογή ανάκλησης πάγιας εντολής</i>	33
<i>Εικόνα 15: Ανάκληση πάγιας εντολής</i>	33
<i>Εικόνα 16: Επιβεβαίωση ανάκλησης</i>	33
<i>Εικόνα 17: Ασφάλεια έξυπνων καρτών για επιχειρήσεις και πελάτες</i>	41
<i>Εικόνα 18: Η κινητή τηλεφωνία σε ευρωπαϊκό επίπεδο</i>	62
<i>Εικόνα 19: Πως λειτουργεί το SET</i>	84

<i>Εικόνα 1: Αίτηση εγγραφής Νομικού Προσώπου</i>	23
<i>Εικόνα 2: Αίτηση εγγραφής Φυσικού προσώπου</i>	25
<i>Εικόνα 3: Εισαγωγή πάγιας εντολής</i>	27
<i>Εικόνα 4: Εισαγωγή στοιχείων</i>	28
<i>Εικόνα 5: Δείγμα εντύπου</i>	28
<i>Εικόνα 6: Προώθηση πάγιας εντολής</i>	29
<i>Εικόνα 7: Όροι ένταξης στο σύστημα E-Banking</i>	29
<i>Εικόνα 8: Εξόφληση Πάγιας εντολής</i>	30
<i>Εικόνα 9: Αναζήτηση εντολών</i>	30
<i>Εικόνα 10: Μεταβολή στοιχείων πάγιας εντολής</i>	31
<i>Εικόνα 11: Καταχωρήσεις</i>	31
<i>Εικόνα 12: Προώθηση Εντολής</i>	32
<i>Εικόνα 13: Καταχώρηση εντολής</i>	32
<i>Εικόνα 14: Επιλογή ανάκλησης πάγιας εντολής</i>	33
<i>Εικόνα 15: Ανάκληση πάγιας εντολής</i>	33
<i>Εικόνα 16: Επιβεβαίωση ανάκλησης</i>	33
<i>Εικόνα 17: Ασφάλεια έξυπνων καρτών για επιχειρήσεις και πελάτες</i>	41
<i>Εικόνα 18: Η κινητή τηλεφωνία σε ευρωπαϊκό επίπεδο</i>	62
<i>Εικόνα 19: Πως λειτουργεί το SET</i>	84

<i>Σχήμα 1: Διαθέσιμες μέθοδοι πληρωμής στα ελληνικά ηλεκτρονικά καταστήματα</i>	98
<i>Σχήμα 2: Το πληροφοριακό σύστημα της Εγνατίας τράπεζας</i>	101
<i>Σχήμα 3: Σύστημα διεξαγωγής πληρωμών EZPay της Χρυσής Ευκαιρίας</i>	105

1. ΕΙΣΑΓΩΓΗ

Η εξάπλωση του Διαδικτύου την τελευταία δεκαετία και η χρήση του για εμπορικούς σκοπούς δημιούργησε νέα δεδομένα στο χώρο των επιχειρήσεων. Οι επιχειρήσεις καλούνται να δημιουργήσουν τις υποδομές εκείνες που θα επιτρέψουν στους καταναλωτές την αγορά προϊόντων και υπηρεσιών στο Διαδίκτυο. Ήδη στις περισσότερες χώρες του κόσμου το Ηλεκτρονικό Εμπόριο αποτελεί μια αδιαμφισβήτητη πραγματικότητα στην οποία οι επιχειρήσεις οφείλουν να προσαρμοστούν προκειμένου να παραμείνουν ανταγωνιστικές εξυπηρετώντας παράλληλα την πελατεία τους.

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 το λόγο αυτό μια σειρά από συστήματα ηλεκτρονικών πληρωμών αναπτύχθηκε σταδιακά. Τα συστήματα αυτά είτε αποτελούσαν μια μεταφορά παραδοσιακών πρακτικών του πραγματικού κόσμου στο Διαδίκτυο όπως είναι η περίπτωση online πληρωμών με πιστωτική κάρτα είτε οι δημιουργοί τους προχώρησαν σε καινοτομικές λύσεις που εκμεταλλεύονταν τα χαρακτηριστικά του Διαδικτύου ή των δικτύων κινητής τηλεφωνίας προκειμένου να προτείνουν πρωτοποριακές λύσεις όπως οι συναλλαγές μεταξύ ομοτίμων.

Στην Ελλάδα, στα πλαίσια ευρύτερων θεσμικών αλλαγών, που δρομολογήθηκαν ήδη από την τελευταία πενταετία της δεκαετίας του 1990, το ηλεκτρονικό εμπόριο έχει αρχίσει σιγά - σιγά να κερδίζει έδαφος στην αγορά υποβοηθούμενο από κατάλληλες δράσεις τόσο του Β΄ όσο και του Γ΄ Κοινοτικού Πλαισίου Στήριξης αλλά και τη δραστηριότητα θυγατρικών μεγάλων πολυεθνικών. Εντούτοις, αν και έχουν γίνει συστηματικές αποτιμήσεις της πορείας και των προοπτικών που υπάρχουν για το ηλεκτρονικό εμπόριο στην Ελλάδα δεν έχει γίνει μέχρι σήμερα μια ενδελεχής αποτίμηση των συστημάτων ηλεκτρονικών πληρωμών στη χώρα μας. Επομένως στόχος της Εργασίας, ήταν η συστηματική εξέταση των υπαρχόντων συστημάτων ηλεκτρονικών πληρωμών στην Ελλάδα και η διερεύνηση εκείνων των παραγόντων που σχετίζονται με την ανάπτυξη και υιοθέτηση τους από τους καταναλωτές αλλά και τις επιχειρήσεις.

Η Εργασία επικεντρώθηκε κυρίως σε εκείνα τα χαρακτηριστικά της ελληνικής αγοράς τα οποία προκαλούν σημαντική δυστοκία στην ανάπτυξη συστημάτων ηλεκτρονικών πληρωμών. Επίσης εξετάστηκε η κατάσταση του ηλεκτρονικού εμπορίου στην χώρα μας ως ένας σημαντικός παράγοντας που επιδρά στην ανάπτυξη συστημάτων ηλεκτρονικών πληρωμών αλλά και η αγοραστική κουλτούρα των ελλήνων καταναλωτών που επιδρά αποφασιστικά στην υιοθέτηση τέτοιων συστημάτων. Ειδική μνεία έγινε για τον κινητήριο ρόλο των πρωτοβουλιών της Δημόσιας Διοίκησης, όπως το Taxis.net, οι οποίες εξοικειώνουν τον πληθυσμό στη χρήση νέων τεχνολογιών ενώ είναι σε θέση να δημιουργήσουν σε πολύ σύντομο χρονικό διάστημα τη κρίσιμη μάζα που απαιτείται για την επιτυχία κάθε πρωτοβουλίας.

Η παρούσα εργασία περιλαμβάνει αρχικά τον εννοιολογικό προσδιορισμό των ηλεκτρονικών πληρωμών. Στην συνέχεια αναλύονται τα υπάρχοντα συστήματα ηλεκτρονικών πληρωμών διεθνώς ενώ ιδιαίτερη έμφαση δίνεται στην κατάσταση στην Ευρώπη και στην Ελλάδα. Εξετάζονται επίσης, τεχνικά, κοινωνικά και νομικά ζητήματα που συνδέονται με τις ηλεκτρονικές πληρωμές. Επιπροσθέτως γίνεται αναφορά στις διαθέσιμες τεχνολογίες και τεχνικές για Ηλεκτρονικές Πληρωμές πρωτόκολλα, συστήματα ασφαλείας και κρυπτογραφίας. Η έκθεση κλείνει με μία σύνοψη των αποτελεσμάτων της διαβούλευσης και ένα κατάλογο προτάσεων για την Πολιτεία, τις τράπεζες και τις επιχειρήσεις.

2. ΜΕΘΟΔΟΛΟΓΙΚΗ ΠΡΟΣΕΓΓΙΣΗ

Η σημασία των ηλεκτρονικών πληρωμών για την επιτυχημένη ανάπτυξη του ηλεκτρονικού και κινητού επιχειρείν αποτέλεσε το έναυσμα για την διερεύνηση του φαινομένου. Η σημαντική άνθηση του ηλεκτρονικού και κινητού επιχειρείν κυρίως στο εξωτερικό αλλά και στην Ελλάδα, δυστυχώς δεν συνοδεύεται από μία ανάλογη εξέλιξη των συστημάτων ηλεκτρονικών πληρωμών. Συνέπεια αυτού του γεγονότος είναι η εμφάνιση σημαντικών προβλημάτων στις συναλλαγές τα οποία αποδυναμώνουν τη δυναμική αυτών των δύο καινοτομικών καναλιών διανομής αγαθών και υπηρεσιών.

Η έρευνα για το ζήτημα των ηλεκτρονικών πληρωμών στην Ελλάδα, ξεκίνησε από αυτή ακριβώς την διαπίστωση και έθεσε ως στόχο την συστηματική ανάλυση του φαινομένου με σκοπό την διαμόρφωση προτάσεων προς όλους του εμπλεκόμενους φορείς. Η διερεύνηση της βιβλιογραφίας διαμόρφωσε ένα αρχικό αριθμό ζητημάτων με βάση είτε την κατάσταση στο εξωτερικό είτε την ελληνική εμπειρία.

Η αρχική αυτή διερεύνηση του φαινομένου κατέδειξε όμως και μία σειρά γενικότερων ζητημάτων για τον χώρο των ηλεκτρονικών πληρωμών. Έτσι, διαπιστώθηκε ότι δεν υπάρχει συμφωνία σε ότι αφορά στις ηλεκτρονικές πληρωμές ούτε στις τεχνολογικές λύσεις που προτείνονται ενώ και η νομοθεσία που αναπτύσσεται σε εθνικό και διεθνές επίπεδο δεν ξεκαθαρίζει άμεσα την κατάσταση. Επιπλέον, κατέστη σαφές ότι ιδιαίτερα σημαντική παράμετρος των ηλεκτρονικών πληρωμών είναι το κόστος που επωμίζονται όλοι οι εμπλεκόμενοι φορείς για την εγκατάσταση και υλοποίηση ενός τέτοιου συστήματος. Τέλος, η αποδοχή των συστημάτων αυτών από το καταναλωτικό κοινό και η ανάπτυξη εμπιστοσύνης στην αποτελεσματικότητά τους είναι ιδιαίτερα σημαντικές για την ανάπτυξη και υιοθέτηση των ηλεκτρονικών πληρωμών. Με στόχο την μελέτη όλων των σημαντικών παραμέτρων των ηλεκτρονικών πληρωμών, η εργασία θα επικεντρωθεί γύρω από τέσσερις κεντρικούς άξονες. Ειδικότερα, οι άξονες αυτοί είναι:

- **Τεχνολογικές εξελίξεις:** στην ενότητα αυτή διερευνήθηκαν οι διαθέσιμες τεχνολογικές λύσεις. Επιπλέον εξετάστηκαν και ζητήματα ασφάλειας, αξιοπιστίας και προστασίας δεδομένων.
- **Οικονομικά δεδομένα:** στην ενότητα αυτή διερευνήθηκαν ζητήματα όπως το κόστος των ηλεκτρονικών συναλλαγών, η δυνατότητα συναλλαγών από ιδιώτες, το εύρος των χρηστών, η δυνατότητα χρήσης επιτυχημένων συστημάτων και από άλλες εταιρείες πέραν αυτών που τα ανέπτυξαν, ο χρηματοοικονομικός κίνδυνος τέτοιων συναλλαγών.
- **Κοινωνικοί προβληματισμοί:** στην εν λόγω ενότητα εξετάστηκε ο βαθμός αποδοχής της ελληνικής κοινωνίας σε θέματα ηλεκτρονικών πληρωμών.

Επιπλέον, εξετάστηκαν τα χαρακτηριστικά που πρέπει να διαθέτει ένα σύστημα προκειμένου να αναπτυχθεί εμπιστοσύνη γύρω αυτό.

- **Νομικό πλαίσιο:** η ενότητα αυτή εξέτασε το νομικό πλαίσιο σε επίπεδο Ευρωπαϊκής Ένωσης αλλά και ελληνικής νομοθεσίας.
-

3. ΟΡΙΣΜΟΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ - ΔΙΑΚΡΙΣΕΙΣ

Συστήματα πληρωμών που χρησιμοποιούν ηλεκτρονικά δίκτυα διανομής αποτελούν διαδεδομένη πρακτική στο χώρο των τραπεζών και των επιχειρήσεων ήδη από την δεκαετία του 1960 ειδικά για την μεταφορά μεγάλων χρηματικών ποσών¹. Μέσα στις τέσσερις δεκαετίες που μεσολάβησαν από την εμφάνισή τους έχουν λάβει χώρα σημαντικές τεχνολογικές εξελίξεις που αφενός διέυρυναν τις δυνατότητες των συστημάτων ηλεκτρονικών πληρωμών και αφετέρου δημιούργησαν καινούριες κοινωνικές πρακτικές που καθιστούν τη χρήση των συστημάτων αυτών αναγκαία. Οι μεταβολές αυτές όπως είναι φυσικό έχουν επηρεάσει και τον ορισμό των ηλεκτρονικών πληρωμών που μετεξελίσσεται ανάλογα με τις ανάγκες κάθε περιόδου.

Στην πιο γενική του μορφή, ο όρος **ηλεκτρονικές πληρωμές (electronic payments)** περιλαμβάνει κάθε πληρωμή προς τις επιχειρήσεις, τις τράπεζες ή τις δημόσιες υπηρεσίες από πολίτες ή επιχειρήσεις οι οποίες εκτελούνται με την μεσολάβηση ενός τηλεπικοινωνιακού ή ηλεκτρονικού δικτύου με χρήση της σύγχρονης τεχνολογίας². Είναι προφανές ότι με βάση τον ορισμό αυτό οι ηλεκτρονικές πληρωμές αφορούν τις πληρωμές εκείνες που γίνονται από τον ίδιο τον πληρωτή είτε είναι καταναλωτής είτε επιχείρηση χωρίς την παρέμβαση άλλου φυσικού προσώπου³. Επίσης, η πληρωμή γίνεται εξ αποστάσεως χωρίς τη φυσική παρουσία του πληρωτή και φυσικά δεν περιλαμβάνει μετρητά. Ορίζοντας τις ηλεκτρονικές πληρωμές κατ' αυτόν τον τρόπο, συμπεριλαμβάνουμε την μεταφορά πληροφοριών σχετικά με τους λογαριασμούς των εμπλεκόμενων μερών στη συναλλαγή καθώς και τα τεχνολογικά μέσα ή κανάλια διανομής μέσω των οποίων πραγματοποιείται η συναλλαγή. Το εύρος του ορισμού έχει ως αποτέλεσμα να είναι εφικτές πολλαπλές ταξινομήσεις του φαινομένου.

Με γνώμονα αυτόν το ορισμό, είναι δυνατόν να πραγματοποιηθεί μία αρχική διάκριση των ηλεκτρονικών πληρωμών σε αυτές που στηρίζονται στην **μεταφορά αξίας** και σε αυτές που στηρίζονται στην **μεταφορά πληροφοριών**⁴. Στην πρώτη κατηγορία, πραγματοποιείται η μεταφορά χρηματικών ποσών μέσω των συστημάτων ηλεκτρονικών πληρωμών. Αντίθετα, στην δεύτερη κατηγορία αυτό που μεταφέρεται μεταξύ των

1 Τέτοια συστήματα είναι το SWIFT που αποτελεί ένα παγκόσμιο δίκτυο που επιτρέπει τη διακίνηση κεφαλαίων μεταξύ Τραπεζών αλλά και τα Εθνικά Διατραπεζικά Συστήματα όπως η ΔΙΑΣ Α.Ε στην Ελλάδα που επιτρέπουν τις διατραπεζικές συναλλαγές των πελατών των Τραπεζών που μετέχουν

2 Sarawak K. & Hansen's B. (2003). E-payments: What are they and what makes them different? Epos Discussion Starter No1. Διαθέσιμο στο www.e-payments.com.

3 Συρμακέζης, Σ. (2003). Όλα όσα θέλατε να μάθετε για τις ηλεκτρονικές πληρωμές και εισπράξεις (και δεν ξέρατε που να ρωτήσετε). Δελτίο ΕΕΤ, Γ' Τριμηνία, σελ. 27-55

4 Goldfinger, C. (1999). Secure electronic payments on the Internet. Διαθέσιμο στο www.goldfinger.com.

συναλλασσόμενων μερών είναι πληροφορίες αφενός για την συναλλαγή και αφετέρου για τους τραπεζικούς λογαριασμούς των εμπλεκόμενων. Η χρηματική συναλλαγή λαμβάνει χώρα είτε off-line είτε με την χρήση ιδιόκτητων ηλεκτρονικών δικτύων χρηματοπιστωτικών ιδρυμάτων ή εταιρειών. Σήμερα, ο κυρίως όγκος ηλεκτρονικών πληρωμών διεκπεραιώνεται μέσω συστημάτων ηλεκτρονικών πληρωμών που στηρίζονται στην μεταφορά πληροφοριών.

Ένας δεύτερος, πιο διαδεδομένος τρόπος ταξινόμησης των ηλεκτρονικών πληρωμών μπορεί να γίνει με βάση τη τεχνολογία που χρησιμοποιεί ένα ηλεκτρονικό δίκτυο διανομής. Έτσι, οι συναλλαγές μπορούν να πραγματοποιηθούν⁵:

- **μέσω τηλεφώνου:** Οι πληρωμές μέσω του τηλεφωνικού δικτύου αποτελούν μία καινούρια μορφή ηλεκτρονικών πληρωμών. Στόχος είναι η εκμετάλλευση της υπάρχουσας τεχνικής υποδομής αλλά και της σημαντικής διείσδυσης που έχει το τηλέφωνο ως τεχνολογία σε όλα τα κοινωνικά στρώματα. Πολλές επιχειρήσεις, τράπεζες αλλά και οι δημόσιες υπηρεσίες επιτρέπουν την εξόφληση λογαριασμών μέσω τηλεφώνου με αποτέλεσμα αυτά τα συστήματα ηλεκτρονικών πληρωμών να κερδίζουν σημαντικά την εμπιστοσύνη του καταναλωτικού κοινού.
- **μέσω Διαδικτύου (Internet):** Πρόκειται για την πιο σύγχρονη μορφή ηλεκτρονικών πληρωμών. Η άνθηση του ηλεκτρονικού επιχειρείν καθιστά ιδιαίτερα σημαντική την ύπαρξη συστημάτων ηλεκτρονικών πληρωμών που χρησιμοποιούν το Διαδίκτυο ως κανάλι διανομής. Επιπλέον, η εύκολη πρόσβαση στο διαδίκτυο από την πλειοψηφία του καταναλωτικού κοινού καθιστούν τα εν λόγω συστήματα ηλεκτρονικών πληρωμών ιδιαίτερα δημοφιλή στις μέρες μας.
- **μέσω κινητής τηλεφωνίας (m-payments):** Η ανάπτυξη τεχνολογιών όπως το WAP επιτρέπουν την εκτέλεση βασικών χρηματικών συναλλαγών από κινητές και ασύρματες συσκευές ανεξαρτήτως χώρου και χρόνου. Πρόκειται για ένα μέσο πιο αυτόνομο ενώ η ευρεία αποδοχή και χρήση του από το καταναλωτικό κοινό το καθιστούν ιδιαίτερα δημοφιλή λύση συχνά ανταγωνιστική των πληρωμών μέσω Διαδικτύου.

Όπως αναφέρθηκε και στην αρχή της ενότητας η χρήση ηλεκτρονικών συστημάτων για την πραγματοποίηση πληρωμών είναι συνηθισμένη πρακτική αρκετές δεκαετίες τώρα. Εντούτοις, την τελευταία πενταετία, ο χώρος των ηλεκτρονικών πληρωμών έχει προκαλέσει ιδιαίτερο ενδιαφέρον τόσο στην επιχειρηματική όσο και στην ακαδημαϊκή κοινότητα. Το αυξημένο αυτό ενδιαφέρον πρέπει να αποδοθεί κυρίως στην ανάπτυξη του Διαδικτύου, αλλά και στην εξάπλωση της κινητής τηλεφωνίας που προσέφεραν νέες δυνατότητες σε όλες τις επιχειρήσεις. Ο οικουμενικός χαρακτήρας και των δύο αυτών μέσων καθώς και η ευκολία πρόσβασης σε αυτά, διέυρναν σημαντικά το πεδίο δράσης όλων των επιχειρήσεων με αποτέλεσμα το ηλεκτρονικό, κυρίως, αλλά και το κινητό επιχειρείν να εξελιχθούν σε μία σημαντική παράμετρο της σύγχρονης επιχειρηματικής πρακτικής. Δεδομένου ότι οι επιχειρηματικές δραστηριότητες που κάνουν χρήση των

5 Βλ. Alpha Bank: "Ηλεκτρονική Τραπεζική: Παρόν και Μέλλον", Οικονομικό Δελτίο, Τεύχος 76, Δεκέμβριος 2000, σελ. 24.

νέων αυτών τεχνολογιών χρειάζονται υποστήριξη από σύγχρονα συστήματα ηλεκτρονικών συναλλαγών η συζήτηση σε ότι αφορά το χώρο επικεντρώνεται κυρίως στα συστήματα πληρωμών μέσω Διαδικτύου και μέσω κινητών συσκευών. Για το λόγο αυτό η εργασία εστιάζει κυρίως στις δύο αυτές κατηγορίες συστημάτων ηλεκτρονικών πληρωμών. Σκοπός της εργασίας είναι να εξεταστούν κυρίως οι μεταβολές που σημειώνονται στον τραπεζικό και επιχειρηματικό χώρο αλλά και στη δημόσια διοίκηση εξαιτίας της χρήσης του Διαδικτύου και της κινητής τηλεφωνίας. Συνεπώς, με τον όρο συστήματα ηλεκτρονικών πληρωμών στο εξής θα νοείται η παροχή προϊόντων και υπηρεσιών -και όχι μόνο πληροφοριών- μέσω αυτού του μέσου και όχι των άλλων που αναφέρθηκαν στην παρούσα ενότητα.

της ταχύτητας των τεχνολογικών εξελίξεων στα συστήματα ηλεκτρονικών πληρωμών και στην απουσία διεθνώς αποδεκτών λύσεων προς το παρόν, η όποια ταξινόμηση δεν μπορεί να στηρίζεται στην τεχνολογία. Για τους λόγους αυτούς στην παρούσα ανάλυση υιοθετείται μία ταξινόμηση που αρθρώνεται σε δύο διαφορετικά επίπεδα. Οι ηλεκτρονικές πληρωμές αρχικά ταξινομούνται με βάση:

1. το είδος της πληροφορίας που ανταλλάσσεται μεταξύ των μερών. Έτσι, μπορούμε να διακρίνουμε τα συστήματα ηλεκτρονικών πληρωμών σε αυτά που απαιτούν την ύπαρξη τραπεζικού λογαριασμού όπως οι χρεωστικές ή οι πιστωτικές κάρτες και σε αυτά που λειτουργούν με την ανταλλαγή γραμματίων ηλεκτρονικής μορφής κατ' αντιστοιχία των τραπεζογραμματίων όπως είναι το ηλεκτρονικό χρήμα⁹.

2. την καινοτομικότητα του συστήματος. Στην περίπτωση αυτή τα συστήματα ηλεκτρονικών πληρωμών διακρίνονται σε αυτά που προϋπήρχαν του ηλεκτρονικού επιχειρείν και απλά προσαρμόστηκαν για τη χρήση τους στο Διαδίκτυο όπως οι πιστωτικές κάρτες και οι ηλεκτρονικές επιταγές. Καθώς και σε αυτά δημιουργήθηκαν προκειμένου να υποστηρίξουν τις συναλλαγές μέσω Διαδικτύου όπως οι «έξυπνες» κάρτες.

Στον πίνακα που ακολουθεί παρουσιάζεται εποπτικά η προτεινόμενη ταξινόμηση των συστημάτων ηλεκτρονικών πληρωμών.

		ΥΠΟΘΕΜΑ	
		ΓΡΑΜΜΑΤΙΟ	ΛΟΓΑΡΙΑΣΜΟΣ
Παραδοσιακά συστήματα πληρωμών (Πιστωτικές Κάρτες)	Πιστωτικές Κάρτες		X
	Μεταφορά ποσών επί πιστώσει		X
	Πάγιες εντολές		X
	Χρεωστικές Κάρτες		X
	Ηλεκτρονικές επιταγές		X
Καινοτομικά συστήματα πληρωμών (Ηλεκτρονικό χρήμα)	Ηλεκτρονικό χρήμα	X	
	Πληρωμές μεταξύ ομότιμων		X
	Προπληρωμένες κάρτες	X	

Πίνακας 1 Ταξινόμηση συστημάτων ηλεκτρονικών πληρωμών

Είναι προφανές ότι τα περισσότερα παραδοσιακά συστήματα πληρωμών όπως οι πιστωτικές κάρτες ή οι ηλεκτρονικές επιταγές απαιτούν την ύπαρξη τραπεζικού λογαριασμού προκειμένου να υποστηρίξουν τις συναλλαγές. Με αποτέλεσμα βέβαια να αποκλείονται κοινωνικές ομάδες που για διάφορους λόγους δεν έχουν τραπεζικούς λογαριασμούς ενώ παράλληλα να μην προφυλάσσεται η ανωνυμία των συναλλαγών.

9 Abravaz., Pernul (Eds.) EC-Web 2001, LNCS 2115 (pp. 81-90). Berlin: Springer – Verlag,hevich, D. (2001). Classification and characteristics of electronic payment systems. In K. Bauknecht, S.K. Madria & G

Αντίθετα, τα πιο πρόσφατα συστήματα ηλεκτρονικών πληρωμών είναι περισσότερο προσαρμοσμένα στις ανάγκες των αγοραπωλησιών στο Διαδίκτυο με αποτέλεσμα να μην απαιτούν την χρήση τραπεζικού λογαριασμού αλλά αντίθετα να έχουν προσομοιώσει την διαδικασία έκδοσης χρήματος στον φυσικό κόσμο.

♦ **Ποιους αφορά; Ποιοι εμπλέκονται σε μια ηλεκτρονική πληρωμή;**

Οι οντότητες (entities) που συμμετέχουν σε μια ηλεκτρονική πληρωμή είναι δύο: ο πληρωτής (payer) και ο πληρωτέος (payee). Καθεμιά από αυτές εμπίπτει σε μία από τις κατηγορίες "πρόσωπο" ("Person", "P") ή "καταναλωτής" ("Consumer", "C") και "επιχείρηση" ("Business", "B"). Ειδικά η δεύτερη οντότητα ("πληρωτέος") περιλαμβάνει και την κατηγορία "πολιτεία" ή "κράτος" ("Government", "G"). Αυτός είναι και ο λόγος που οι ηλεκτρονικές πληρωμές μεταξύ των παραπάνω οντοτήτων (ως συνέχεια των αντίστοιχων εμπορικών συναλλαγών) κωδικοποιούνται στις υποπεριπτώσεις:

Person –To–Person (P2P): Αφορά πληρωμές μεταξύ προσώπων, κανένα από τα οποία δεν συμμετέχει με επιχειρηματικό ρόλο. Παράδειγμα: πληρωμή προσωπικού χρέους.
Consumer–To– Business και Business –To– Consumer (C2B ή B2C): Έχει επικρατήσει το ακρωνύμιο "B2C", εκφράζοντας την πώληση από την επιχείρηση προς τον καταναλωτή, η οποία ολοκληρώνεται με την πληρωμή της πρώτης από το δεύτερο. Παράδειγμα: πώληση/ αγορά αγαθών ή παροχή/ λήψη υπηρεσιών.

Business–To–Business (B2B): Πρόκειται για πληρωμές μεταξύ επιχειρήσεων. Διαφέρουν από τις υπόλοιπες λόγω του πολύ μικρότερου πλήθους τους και των πολύ μεγαλύτερων ποσών που εμπεριέχουν. Παράδειγμα: πληρωμή τιμολογίου.

Person–To–Government (P2G) και Business–To–Government (B2G), συνολικά x2G: Πρόκειται για πληρωμές προς δημόσιες υπηρεσίες (Υπουργεία, Τοπική Αυτοδιοίκηση κ.λπ.) και συνήθως αφορά οφειλές των πολιτών. Παράδειγμα: πληρωμή Φ.Π.Α, πληρωμή τελών κυκλοφορίας. Η αντίστροφη μορφή πληρωμών (G2P, G2B) υφίσταται, αλλά προς το παρόν δεν υλοποιείται με τη μορφή των μεμονωμένων πληρωμών. Παράδειγμα: επιστροφή φόρου μέσω τραπεζών. Οι οντότητες αυτές συμμετέχουν στα δύο "άκρα" μιας ηλεκτρονικής πληρωμής, ανεξάρτητα από το ηλεκτρονικό δίκτυο ή μέσο που αξιοποιούν και άσχετα από το χρηματοοικονομικό εργαλείο που η καθεμιά χρησιμοποιεί.

♦ **Τι κόστος έχουν οι ηλεκτρονικές πληρωμές; Ποιος το υφίσταται;**

Σε όλες τις περιπτώσεις το κόστος επιβαρύνει το δικαιούχο της πληρωμής. Οι παράγοντες κόστους είναι οι εξής:

- Προμήθεια επί του ποσού. Η προμήθεια υπολογίζεται ως ποσοστό επί του ποσού κάθε συναλλαγής. Όταν η πληρωμή γίνεται με πιστωτική κάρτα, το εν λόγω ποσοστό μπορεί να ξεκινά από 1,0%-1,5% και να φτάνει σε πολύ υψηλότερα ποσοστά όταν υπάρχει αυξημένη πιθανότητα αμφισβήτησης των συναλλαγών (π.χ. 10,0%).

- Σταθερή αμοιβή. Για κάθε πληρωμή υπολογίζεται χρέωση ενός σταθερού ποσού ως αμοιβή για τη διεκπεραίωση της συναλλαγής. Αν υπάρχει, το ποσό κυμαίνεται μεταξύ 0,10 και 1,00.
- Συνδρομή στην υπηρεσία. Για την παροχή της δυνατότητας ηλεκτρονικών εισπράξεων, ο δικαιούχος χρεώνεται με μηνιαία ή ετήσια συνδρομή. Συνήθως αυτή η χρέωση συμψηφίζεται με τις παραπάνω χρεώσεις και έχει νόημα μόνον όταν οι συναλλαγές είναι ελάχιστες και δεν αποφέρουν επαρκές έσοδο στην τράπεζα ή την εταιρεία που εξυπηρετεί την πληρωμή.
- Συνδυασμός των παραπάνω με ελάχιστη και μέγιστη χρέωση.
- Επιπλέον χρέωση για διεκπεραίωση αμφισβητούμενης συναλλαγής. Επειδή οι αμφισβητούμενες συναλλαγές δημιουργούν μεγάλο φόρτο στις τράπεζες/acquirers, αυτές οδηγούνται στην επιβολή μιας ειδικής χρέωσης για κάθε τέτοια περίπτωση. Ανάλογα με την περίπτωση, οι χρεώσεις αυτές κυμαίνονται μεταξύ 5 και 40.
- Χρέωση για παροχή ψηφιακού πιστοποιητικού. Αυτή η χρέωση, όταν υπάρχει, ενσωματώνεται στη συνδρομή και αφορά την εξασφάλιση της τράπεζας ή της εταιρείας ότι σε κάθε συναλλαγή έχει να κάνει με το συγκεκριμένο δικαιούχο και όχι με κάποιον που προσποιείται ότι είναι ο δικαιούχος.
- Ημερομηνία αξίας (valuer). Ο δικαιούχος μπορεί να πιστώνεται σε πραγματικό χρόνο, καθημερινά ή σε τακτά χρονικά διαστήματα (π.χ. κάθε εβδομάδα ή κάθε μήνα). Ακόμα, δεδομένου ότι κάθε τέτοια πίστωση δημιουργεί επιπλέον κόστος, πολλές φορές ορίζεται ένα ελάχιστο ποσό (π.χ. 50€) που πρέπει να έχει συγκεντρωθεί πριν γίνει κάποια πληρωμή.

Σε ορισμένες, σπάνιες περιπτώσεις υπάρχει χρέωση και για τον πληρωτή. Αυτό συνήθως συμβαίνει όταν η υπηρεσία πληρωμής παρέχεται με προστιθέμενη αξία στον πληρωτή (π.χ. παρουσίαση και πληρωμή λογαριασμού) ή γίνεται με πρωτοβουλία του (π.χ. αποστολή ποσού με υπηρεσία P2P payment).

Τέλος, όταν οι συναλλαγές απαιτούν την εμπλοκή επιπλέον πόρων (π.χ. τη συμμετοχή ενός τηλεφωνικού αντιπροσώπου, την αποστολή γραπτών μηνυμάτων SMS κ.λπ., όπως αναφέρεται παρακάτω), ενδέχεται να υπάρχει επιπλέον χρέωση, την οποία υφίσταται είτε ο δικαιούχος είτε ο πληρωτής είτε και οι δύο. Η χρέωση αυτή έρχεται να καλύψει το επιπλέον κόστος διεκπεραίωσης της συναλλαγής.

4.1 ΠΑΡΑΔΟΣΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΠΡΟΣΑΡΜΟΣΜΕΝΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Στην κατηγορία αυτή ανήκουν συστήματα πληρωμών τα οποία προϋπήρχαν της εμφάνισης του Διαδικτύου. Η διαδεδομένη χρήση τους αλλά και η σιγουριά που προσέφεραν στους καταναλωτές κατέστησαν τα μέσα αυτά ιδιαίτερα δημοφιλή και στο Διαδίκτυο. Επιπλέον η χρήση τους δεν απαιτούσε ιδιαίτερη επένδυση ούτε από την πλευρά των εταιρειών που δραστηριοποιούνταν στο διαδίκτυο με αποτέλεσμα να κυριαρχήσουν τουλάχιστον στα αρχικά στάδια του ηλεκτρονικού εμπορίου. Τα συστήματα αυτά απαιτούν την ύπαρξη τραπεζικών λογαριασμών από τους καταναλωτές με αποτέλεσμα ένα μέρος των συναλλαγών να πρέπει να εκκαθαριστεί εκτός του Διαδικτύου. Ειδικότερα, τα συστήματα αυτά είναι:

- **Πιστωτικές κάρτες:** Οι πιστωτικές κάρτες επιτρέπουν στους καταναλωτές την πραγματοποίηση συναλλαγών μέχρι ενός προκαθορισμένου ποσού. Το ποσό των συναλλαγών που έχουν πραγματοποιηθεί μέσω της κάρτας εκκαθαρίζεται στο τέλος κάθε ημερολογιακού μήνα είτε πλήρως είτε μερικώς οπότε το υπόλοιπο θεωρείται ως πίστωση του εκδοτικού οργανισμού προς τον κάτοχο.

Οι πιστωτικές κάρτες έχουν τύχει ευρείας χρήσης στο Διαδίκτυο επειδή διαθέτουν σημαντικά πλεονεκτήματα έναντι των εναλλακτικών μεθόδων πληρωμής¹⁰. Κατ' αρχήν είναι διεθνώς γνωστές και αποδεκτές από τους εμπόρους. Η χρήση τους στο Διαδίκτυο δεν διαφέρει σημαντικά από τον τρόπο που χρησιμοποιούνταν μέχρι τώρα στις συναλλαγές στον φυσικό κόσμο¹¹. Επιπλέον, η σημαντική διάδοση των πιστωτικών καρτών και στις παραδοσιακές συναλλαγές έχει συντελέσει στην δημιουργία μιας ιδιαίτερα αποτελεσματικής υποδομής για την εκκαθάριση των πληρωμών η οποία μάλιστα επιτρέπει και την πραγματοποίηση διεθνών συναλλαγών. Αυτό έχει σαν αποτέλεσμα την πραγματοποίηση συναλλαγών στο Διαδίκτυο χωρίς σημαντικές επενδύσεις από την πλευρά των εμπόρων αλλά και χωρίς αλλαγή στην συμπεριφορά των καταναλωτών.

Στα πρώτα στάδια του ηλεκτρονικού εμπορίου, οι καταναλωτές απλά έστελναν τον αριθμό της πιστωτικής τους κάρτας και την ημερομηνία λήξης στους εμπόρους με την μορφή απλού μηνύματος χωρίς κρυπτογράφηση. Σύντομα όμως αυτός ο τρόπος χρήσης της πιστωτικής κάρτας στο Διαδίκτυο εγκαταλείφθηκε καθώς το μήνυμα ήταν πολύ εύκολο να υποκλαπεί με αποτέλεσμα να παρατηρηθούν κρούσματα απάτης με πιστωτικές κάρτες. Προκειμένου να λυθούν τα προβλήματα απάτης οι οργανισμοί πιστωτικών καρτών προχώρησαν στην δημιουργία προτύπων όπως το SET (Secure Electronic Transaction) που ήταν πρωτοβουλία της VISA και της MASTERCARD. Τα πρότυπα αυτά ενίσχυσαν σημαντικά την ασφάλεια των συναλλαγών στο Διαδίκτυο μέσω πιστωτικής κάρτας δεν έτυχαν όμως ευρείας αποδοχής από το καταναλωτικό κοινό.

10 European Central Bank. E-payments in Europe – The euro system's perspective. Issue Paper available at www.ecb.int.

11 Turban, E.; Lee, J.; King, D. & Chung, H. M. (xxx). Electronic commerce: A managerial perspective. International Edition, Upper Saddle River: Prentice Hall, pp.

Ένα από τα πιο δημοφιλή συστήματα που αναπτύχθηκαν για αυτό το λόγο είναι το σύστημα της εταιρίας Cyber Cash. Το σύστημα *Cash Register* δουλεύει συνδεδεμένο με όποιο ιστοχώρο αγοράσει το σύστημα το *CashRegister*. Αυτή η σύνδεση διαχειρίζεται από κώδικα που βρίσκεται στον ιστοχώρο του εμπόρου. Όταν ο πελάτης συμπληρώνει μια φόρμα στον ιστοχώρο του εμπόρου για την αγορά ενός προϊόντος, τα στοιχεία της πιστωτικής κάρτας του στέλνονται με ασφαλή τρόπο στο σύστημα *CashRegister*. Αυτό επιβεβαιώνει τη συναλλαγή, εκτελώντας εργασίες όπως ο έλεγχος του αριθμού της πιστωτικής κάρτας, έλεγχος για τυχόν κλεμμένη κάρτα και επιβεβαίωση ότι το πιστωτικό όριο της κάρτας δεν έχει ξεπεραστεί. Αν η συναλλαγή είναι έγκυρη το σύστημα *CashRegister* θα αφαιρέσει το ποσό από το λογαριασμό του πελάτη, θα το πιστώσει στο λογαριασμό του εμπόρου και θα του στείλει μήνυμα για την ασφαλή αποστολή των αγαθών. Αυτό είναι μόνο ένα παράδειγμα συστήματος πληρωμής με πιστωτική κάρτα, αφού υπάρχουν πολλά άλλα.

Κατά τη χρήση πιστωτικής κάρτας, ο καταναλωτής παρουσιάζει τον αριθμό της κάρτας στον προμηθευτή από όπου θα αγοράσει το προϊόν που τον ενδιαφέρει. Ο προμηθευτής από την άλλη, επιβεβαιώνει την ισχύ του αριθμού της πιστωτικής κάρτας με την τράπεζα και δημιουργεί ένα δελτίο αγοράς για τον καταναλωτή που πρέπει ο τελευταίος να το επικυρώσει. Ο προμηθευτής χρησιμοποιεί αυτό το δελτίο πληρωμής για να παραλάβει το χρηματικό ποσό που αντιστοιχεί στο προϊόν, από την τράπεζα, και στην επόμενη ενημέρωση τραπεζικού λογαριασμού του καταναλωτή περιλαμβάνεται η εξαργύρωση των χρημάτων από το ηλεκτρονικό κατάστημα.

Η χρήση της πιστωτικής κάρτας μέσα στο Διαδίκτυο ακολουθεί ακριβώς την ίδια διαδικασία, μόνο που στο ηλεκτρονικό περιβάλλον ακολουθούνται επιπλέον βήματα για την εξασφάλιση ασφαλούς μεταφοράς συναλλάγματος και αυθεντικότητας προσωπικών δεδομένων του καταναλωτή αλλά και του προμηθευτή.

Δύο είναι οι βασικές διαφορές συναλλαγής στο Διαδίκτυο από ότι στο φυσικό κατάστημα. Η πρώτη αναφέρεται στο επίπεδο ασφάλειας μεταφοράς χρηματικών ποσών και η δεύτερη στο πρόγραμμα λογισμικού που διαθέτουν και οι δύο πλευρές (προμηθευτής-καταναλωτής).

Δύο επίσης είναι και οι τρόποι χρήσης της πιστωτικής κάρτας στο Διαδίκτυο. Στην πρώτη περίπτωση ο καταναλωτής στέλνει φανερά τον αριθμό της κάρτας και στην δεύτερη περίπτωση διαθέτει τα προσωπικά δεδομένα σε κρυπτογραφημένη μορφή. Η δεύτερη περίπτωση είναι και εκείνη που χρησιμοποιείται συχνά αλλά ακολουθείται ιδιαίτερη διαδικασία.

Στη περίπτωση λοιπόν κρυπτογραφημένων στοιχείων, ο προμηθευτής χρειάζεται να αποκρυπτογραφήσει κάποια από τα στοιχεία για να εκτελέσει την παραγγελία. Επιπλέον, για να καθησυχάσει τον καταναλωτή ότι τα στοιχεία της πιστωτικής κάρτας χρησιμοποιούνται μόνο από εξουσιοδοτημένα πρόσωπα αποκλείοντας κάθε περίπτωση κατάχρησής τους, χρησιμοποιείται συνήθως ένας ανεξάρτητος οργανισμός που διασφαλίζει τον σωστό τρόπο χρησιμοποίησης της κάρτας.

Στην περίπτωση τώρα που σε κάποια ιστοσελίδα ζητείται η συμπλήρωση προσωπικών δεδομένων σε απλή φόρμα, η συναλλαγή εγκυμονεί κίνδυνο παραβίασης

της κάρτας από κάποιον τρίτο. Μόνο στις περιπτώσεις που ο εξυπηρετητής (πρόγραμμα λογισμικού) χρησιμοποιεί εφαρμογή **CGI script**, η ασφάλεια είναι δεδομένη. Το CGI script είναι ένα έγγραφο συστήματος σχεδιασμένο να λειτουργεί με ένα πρωτόκολλο αρχείου μεταφοράς πληροφορίας μεταξύ πελάτη και εξυπηρετητή δικτύου και συνήθως η χρήση του γίνεται για την ανταλλαγή πληροφορίας και δεδομένων.

Επίσης, μια άλλη μορφή πιστοποίησης εξασφάλισης δεδομένων, είναι η χρήση συστημάτων ασφαλείας, γνωστών ως **Secure Sockets Layer (SSL)**, τα οποία προστατεύουν τα δεδομένα από τους κατασκόπους του Διαδικτύου. Το συγκεκριμένο σύστημα ασφαλείας SSL, διασφαλίζει την προστασία δεδομένων από τυχόν κατάχρηση τους από τους προμηθευτές, αφού υπεύθυνοι για αυτή την περίπτωση είναι οι οργανισμοί ασφαλείας **CyberCash**, **Verifone** και **First Virtual**. Όταν λοιπόν κάποια ιστοσελίδα υποστηρίζεται από έναν από τους τρεις οργανισμούς ασφαλείας, τότε οι συναλλαγές είναι εγγυημένες.

Στον παρακάτω πίνακα ας δούμε τα βασικά χαρακτηριστικά τους:

Υπέρ
-Αποτελούν την πιο γνωστή και δημοφιλή κατηγορία πλαστικού χρήματος
-Ασφάλεια
-Ύπαρξη «περιόδου χάριτος»
-Παροχή πίστωσης με την μορφή ανακυκλούμενου δανείου
-Δυνατότητα ανάληψης μετρητών (με μηνιαίο όριο)
-Έχουν τοπική ή διεθνή ισχύ. Διεθνείς είναι οι κάρτες που κυκλοφορούν από διάφορες τράπεζες συνεργαζόμενες με τους διεθνείς οργανισμούς VISA ή MASTERCARD
Κατά
-Αυστηρότερα κριτήρια αξιολόγησης
-Ετήσιες συνδρομές
-Τόκοι που επιβαρύνουν τον πελάτη όταν χρησιμοποιεί πίστωση για τις αγορές του

Πίνακας 2:Βασικά χαρακτηριστικά πιστωτικών καρτών

ΠΕΡΙΓΡΑΦΗ –ΜΗΧΑΝΙΣΜΟΣ

Οι κάρτες **VISA** ή **MASTERCARD** ,έχουν διεθνή ισχύ, σε εκατομμύρια συμβεβλημένες επιχειρήσεις, ανεξάρτητα από τις τοπικές τράπεζες ή χρηματοοικονομικούς οργανισμούς που τις εκδίδουν.

Οι πιστωτικές κάρτες δεν απαιτούν, απαραίτητα , την ύπαρξη τραπεζικού λογαριασμού και παρέχουν «**περίοδο χάριτος**» όπως ακριβώς οι χρεωστικές. Το μεγάλο πλεονέκτημα των καρτών αυτών είναι ότι ο κάτοχός τους όταν λαμβάνει την μηνιαία εκκαθάριση του λογαριασμού του έχει δύο επιλογές:

1. Να εξοφλήσει όλο το ποσό που αναγράφεται στο μηνιαίο λογαριασμό
2. Να πληρώσει ένα μέρος του λογαριασμού και να αποπληρώσει το υπόλοιπο έντοκα τους επόμενους μήνες.

Με αυτόν τον τρόπο έχει στην διάθεσή του ένα συνεχές **κυλιόμενο δάνειο** για τις αγορές του σε οποιοδήποτε μέρος του κόσμου. Το υψηλό επίπεδο εξυπηρέτησης συνεπάγεται υψηλά λειτουργικά κόστη και υψηλά επιτόκια. Η απουσία λογαριασμού και η δυνατότητα του κυλιόμενου δανείου έχουν σαν αποτέλεσμα την **ύπαρξη πιστωτικού ορίου**, το οποίο αυξάνει την αγοραστική δύναμη του κατόχου. Το πιστωτικό όριο διαμορφώνεται ανάλογα με τα κριτήρια πιστοληπτικής αξιολόγησης και τον κίνδυνο που επιθυμεί να αναλάβει η τράπεζα. Ο πελάτης έχει επίσης την δυνατότητα ανάληψης μετρητών (μέχρι ενός συγκεκριμένου ποσού κάθε μήνα), τα οποία χρεώνονται έντοκα στο λογαριασμό του.

Οι πιστωτικές κάρτες αποτελούν υπερσύνολο των χρεωστικών καρτών ,με μεγαλύτερη αποδοχή ,γεγονός που τις καθιστά το δημοφιλέστερο και συνεχώς αναπτυσσόμενο είδος πλαστικού χρήματος.

Α)για τον πελάτη

Κατοχή	
Οφέλη	Μειονεκτήματα
-Αναγνωρισιμότητα του πελάτη	-Κόστος συνδρομής
-Δυνατότητα συναλλαγών σε όλο τον κόσμο	-Εξοδα ανάληψης μετρητών
Χρήση	
Οφέλη	Κίνδυνοι
-Αγορές μέσω προγ/των δανείων	-Αλόγιστη χρήση της κάρτας
-Ασφάλεια(προσωπικό & μυστικό PIN)	-Κοινοποίηση του PIN σε τρίτους
-Υποκατάστατα μετρητών	
-Αγορές με πίστωση	
-Εναλλακτικοί τρόποι εξόφλησης της υποχρέωσης	

Β) για την Τράπεζα

Κατοχή	
Οφέλη	Μειονεκτήματα
-Ετήσια συνδρομή	-Δεν υπάρχουν άλλες πηγές εσόδων
-Αύξηση του μεριδίου αγοράς των πιστωτικών καρτών	για την Τράπεζα -Κόστος διαχείρισης προϊόντων
-Διαχείριση του κινδύνου τόσο σε επίπεδο πιστωτικής απόφασης όσο και σε επίπεδο χρήσης ορίων	
Χρήση	
Οφέλη	Κίνδυνοι
-Τόκοι	-Απώλεια
-Είσπραξη προμήθειας από εμπόρους	-Κλοπή
-Αύξηση του μεριδίου αγοράς στις συναλλαγές	-Αντιγραφή της κάρτας

Πίνακας 3: Οφέλη και πλεονεκτήματα από την κατοχή και χρήση των πιστωτικών καρτών

Τέλος μπορούμε να πούμε ότι οι πιστωτικές κάρτες είναι προϊόντα που:

Έχουν περιορισμένο κίνδυνο (η απόφαση και η ευθύνη της έκδοσής τους λαμβάνεται βάση αυτοματοποιημένων μοντέλων στατιστικής αξιολόγησης. Οι κάρτες ελέγχονται αυτόματα κατά τις εξουσιοδοτήσεις συναλλαγών)
Προσφέρονται για μαζικές πωλήσεις

- **Μεταφορά ποσών επί πιστώσει (e-banking)** :Σε αυτό το σύστημα πληρωμών ο καταναλωτής δίνει εντολή στην τράπεζα του να μεταφέρει χρηματικά ποσά ανάλογα της πληρωμής που θέλει να πραγματοποιήσει στον λογαριασμό του εμπόρου¹². Αυτή η μέθοδος πληρωμής υποστηρίζεται σημαντικά από τις τράπεζες στα πλαίσια των εφαρμογών ηλεκτρονικής τραπεζικής που προσφέρουν στους πελάτες τους. Ειδικά για συναλλαγές στο διαδίκτυο οι πελάτες μπορούν να επιλέξουν την μεταφορά ποσών επί πιστώσει ως την επιθυμητή μέθοδο πληρωμής και απλά να αποδεχθούν τον λογαριασμό που θα εμφανιστεί στην οθόνη τους. Εφόσον ο πελάτης αποδέχεται την συναλλαγή μεταφέρεται στον δικτυακό τόπο της τράπεζας όπου ολοκληρώνει την συναλλαγή του και κατόπιν επιστρέφει στο ηλεκτρονικό κατάστημα στο οποίο βρισκόταν.

Τα πλεονεκτήματα της υπηρεσίας αυτής (e-banking) είναι σημαντικά τόσο για τους πελάτες, αφού δεν θα χρειάζεται να προσέρχονται στα τραπεζικά καταστήματα, όσο και για τις τράπεζες αφού περιορίζεται σημαντικά το κόστος συναλλαγών.

Διαδικασία ένταξης πελατών

Ο πελάτης για να ενταχθεί στο Internet Banking πρέπει να συμπληρώσει αίτηση εγγραφής :

- Είτε ηλεκτρονικά μέσω του Διαδικτύου
- Είτε προσερχόμενος σε κάποιο Κατάστημα

Παρακάτω εμφανίζονται δύο παραδείγματα αιτήσεων εγγραφής Νομικού και Φυσικού προσώπου για e-Banking ,σύμφωνα με την Εμπορική Τράπεζα.

12 European Central Bank E-payments in Europe-The euro system's perspective .Issue paper available at www.ecb.int

Eurobank e.Banking

ΠΡΟΣΦΕΡΟΜΕΝΟΣ ΝΟΜΙΜΟΝ ΤΥΠΟΣ

Παρακαλούμε συμπληρώστε με ΚΕΦΑΛΑΙΑ ΓΡΑΜΜΑΤΑ αυτή τη φόρμα.
(Τα πεδία με αστερίσκο [*] είναι υποχρεωτικά)

ΣΤΟΙΧΕΙΑ ΠΡΟΣΩΠΟΥ

ΠΑΤΡΗΣ ΕΠΩΝΥΜΙΑ*	<input type="text"/>		
A.Φ.Μ.†	<input type="text"/>	ΑΡΜΟΔΙΑ Δ.Ο.Υ*	<input type="text"/>

ΣΤΟΙΧΕΙΑ ΕΠΙΧΕΙΡΗΣΗΣ / ΠΡΟΣΦΕΡΟΜΕΝΟΝ ΤΥΠΟΝ

για κάθε εκπρόσωπο πρέπει να συμπληρωθεί ανεξάρτητα αίτηση

ΕΠΩΝΥΜΟ 1*	<input type="text"/>	ΟΝΟΜΑ*	<input type="text"/>
ΕΠΩΝΥΜΟ 2	<input type="text"/>	ΟΝΟΜΑ ΠΑΤΕΡΑ*	<input type="text"/>
ΕΙΔΟΣ ΤΑΥΤΟΤΗΤΑΣ*	(επιλέξτε) <input type="text"/>	ΑΡΙΘΜΟΣ*	<input type="text"/>
ΗΜ/ΝΙΑ ΕΚΔΟΣΗΣ*	<input type="text"/> / <input type="text"/> / <input type="text"/>	ΕΚΔΟΤΡΙΑ ΑΡΧΗ*	<input type="text"/>
ΗΜ/ΝΙΑ ΓΕΝΝΗΣΗΣ*	<input type="text"/> / <input type="text"/> / <input type="text"/>	ΕΠΑΓΓΕΛΜΑ	(επιλέξτε) <input type="text"/>
A.Φ.Μ.*	<input type="text"/>	ΑΡΜΟΔΙΑ Δ.Ο.Υ*	<input type="text"/>
ΟΙΚΟΓΕΝΕΙΑΚΗ ΚΑΤΑΣΤΑΣΗ†	(επιλέξτε) <input type="text"/>	ΑΡ. ΠΑΙΔΙΩΝ	<input type="text"/>

ΣΤΟΙΧΕΙΑ ΜΕΛΟΥΣ ΣΕ ΤΙΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

ΟΔΟΣ*	<input type="text"/>	ΑΡΙΘΜΟΣ*	<input type="text"/>
T.K.*	<input type="text"/>	ΠΟΛΗ*	<input type="text"/>
ΝΟΜΟΣ*	<input type="text"/>	E-MAIL*	<input type="text"/>
ΤΗΛΕΦΩΝΑ*	<input type="text"/>	FAX	<input type="text"/>

ΣΥΝΔΕΣΜΟΙ ΣΕ ΛΟΓΑΡΙΑΣΜΟΥΣ

Συμπληρώστε τους αριθμούς των τραπεζικών σας λογαριασμών, των καρτών σας, καθώς και των λογαριασμών τρίτων για τους οποίους θέλετε να έχετε πρόσβαση μέσω της "Υπηρεσίας Emproribi e.Banking".
Μπορείτε να δηλώσετε μέχρι 15 λογαριασμούς.

ΛΟΓΑΡΙΑΣΜΟΣ 1:	<input type="text"/>	<input type="text"/>	<input type="text"/>		ΛΟΓΑΡΙΑΣΜΟΣ 2:	<input type="text"/>	<input type="text"/>	<input type="text"/>	
ΛΟΓΑΡΙΑΣΜΟΣ 3:	<input type="text"/>	<input type="text"/>	<input type="text"/>		ΛΟΓΑΡΙΑΣΜΟΣ 4:	<input type="text"/>	<input type="text"/>	<input type="text"/>	
ΛΟΓΑΡΙΑΣΜΟΣ 5:	<input type="text"/>	<input type="text"/>	<input type="text"/>		ΛΟΓΑΡΙΑΣΜΟΣ 6:	<input type="text"/>	<input type="text"/>	<input type="text"/>	
ΛΟΓΑΡΙΑΣΜΟΣ 7:	<input type="text"/>	<input type="text"/>	<input type="text"/>		ΛΟΓΑΡΙΑΣΜΟΣ 8:	<input type="text"/>	<input type="text"/>	<input type="text"/>	
ΛΟΓΑΡΙΑΣΜΟΣ 9:	<input type="text"/>	<input type="text"/>	<input type="text"/>		ΛΟΓΑΡΙΑΣΜΟΣ 10:	<input type="text"/>	<input type="text"/>	<input type="text"/>	
ΛΟΓΑΡΙΑΣΜΟΣ 11:	<input type="text"/>	<input type="text"/>	<input type="text"/>		ΛΟΓΑΡΙΑΣΜΟΣ 12:	<input type="text"/>	<input type="text"/>	<input type="text"/>	

ΛΟΓΑΡΙΑΣΜΟΣ 13: ▼

ΛΟΓΑΡΙΑΣΜΟΣ 14: ▼

ΛΟΓΑΡΙΑΣΜΟΣ 15: ▼

ΙΔ - ΛΟΓΑΡΙΑΣΜΟΣ ΤΟΥ ΠΕΛΑΤΗ
ΤΡ - ΛΟΓΑΡΙΑΣΜΟΣ ΤΡΙΤΩΝ

ΕΠΙΘΥΜΩ ΤΗ ΔΥΝΑΤΟΤΗΤΑ ΜΕΤΑΦΟΡΑΣ ΚΡΕΔΩΝΤΩΝ ΚΑΙ ΠΑΡΩΜΩΝ*

ΟΧΙ ΝΑΙ

ΠΡΟΣ ΛΟΓΑΡΙΑΣΜΟΥΣ ΙΔΙΟΥ

ΑΝΕΥ ΟΡΙΟΥ ΠΟΣΟΥ

ΠΡΟΣ ΛΟΓΑΡΙΑΣΜΟΥΣ ΤΡΙΤΩΝ

ΕΩΣ ΗΜΕΡΗΣΙΟΥ ΠΟΣΟΥ

(επιλέξτε) ▼

ΕΤΩ

ΣΥΝΕΡΓΑΣΙΑ ΜΕ ΑΛΛΗ ΤΡΑΠΕΖΑ

ΟΧΙ ΝΑΙ

ΤΡΑΠΕΖΑ

ΚΑΤΑΣΤΗΜΑ ΕΞΥΠΗΡΕΤΗΣΗΣ
"Υπηρεσίες Εμπορική e.Banking"*

(επιλέξτε) ▼

Καθαρισμός

Αποστολή

Εικόνα 1: Αίτηση εγγραφής Νομικού Προσώπου

Εμπορική e.Banking

ΑΡΧΗ ΜΕΛΕΤΗΣ ΚΑΙ ΣΥΜΦΩΝΗΤΗΣΗΣ

Παρακαλούμε συμπληρώστε με ΚΕΦΑΛΑΙΑ ΓΡΑΜΜΑΤΑ αυτή τη φόρμα.
(Τα πεδία με αστέριко [*] είναι υποχρεωτικά)

ΑΝΤΙΚΑΤΑΧΕΥΣΗ

ΕΠΩΝΥΜΟ 1* <input style="width: 100%;" type="text"/> ΕΠΩΝΥΜΟ 2 <input style="width: 100%;" type="text"/> ΕΙΔΟΣ ΤΑΥΤΟΤΗΤΑΣ* <input style="width: 100%;" type="text" value="(Επιλέξτε)"/> ΗΜ/ΝΙΑ ΕΚΔΟΣΗΣ* <input style="width: 100%;" type="text"/> / <input style="width: 100%;" type="text"/> / <input style="width: 100%;" type="text"/> ΗΜ/ΝΙΑ ΓΕΝΝΗΣΗΣ* <input style="width: 100%;" type="text"/> / <input style="width: 100%;" type="text"/> / <input style="width: 100%;" type="text"/> Α.Φ.Μ.* <input style="width: 100%;" type="text"/> ΟΙΚΟΓΕΝΕΙΑΚΗ ΚΑΤΑΣΤΑΣΗ* <input style="width: 100%;" type="text" value="(Επιλέξτε)"/>	ΟΝΟΜΑ* <input style="width: 100%;" type="text"/> ΟΝΟΜΑ ΠΑΤΕΡΑ* <input style="width: 100%;" type="text"/> ΑΡΙΘΜΟΣ* <input style="width: 100%;" type="text"/> ΕΚΔΟΤΡΙΑ ΑΡΧΗ* <input style="width: 100%;" type="text"/> ΕΠΑΓΓΕΛΜΑ <input style="width: 100%;" type="text" value="(Επιλέξτε)"/> ΑΡΜΟΔΙΑ Δ.Ο.Υ* <input style="width: 100%;" type="text"/> ΑΡ. ΠΑΙΔΙΩΝ <input style="width: 100%;" type="text"/>
---	--

ΣΤΑΘΕΡΑ ΔΙΕΥΣΗ

ΟΔΟΣ* <input style="width: 100%;" type="text"/> Τ.Κ.* <input style="width: 100%;" type="text"/> ΝΟΜΟΣ* <input style="width: 100%;" type="text"/> ΤΗΛΕΦΩΝΑ* <input style="width: 100%;" type="text"/>	ΑΡΙΘΜΟΣ* <input style="width: 100%;" type="text"/> ΠΟΛΗ* <input style="width: 100%;" type="text"/> Ε-MAIL* <input style="width: 100%;" type="text"/> FAX <input style="width: 100%;" type="text"/>
---	---

ΣΥΝΕΧΕΙΣ ΛΟΓΑΡΙΑΣΜΟΙ

Συμπληρώστε τους αριθμούς των τραπεζικών σας λογαριασμών, των καρτών σας, καθώς και των λογαριασμών τρίτων για τους οποίους θέλετε να έχετε πρόσβαση μέσω της "Υπηρεσίας Εμπορική e.Banking".
Μπορείτε να δηλώσετε μέχρι 15 λογαριασμούς.

ΛΟΓΑΡΙΑΣΜΟΣ 1: <input style="width: 100%;" type="text"/> <input style="width: 100%;" type="text"/> ΛΟΓΑΡΙΑΣΜΟΣ 3: <input style="width: 100%;" type="text"/> <input style="width: 100%;" type="text"/> ΛΟΓΑΡΙΑΣΜΟΣ 5: <input style="width: 100%;" type="text"/> <input style="width: 100%;" type="text"/> ΛΟΓΑΡΙΑΣΜΟΣ 7: <input style="width: 100%;" type="text"/> <input style="width: 100%;" type="text"/> ΛΟΓΑΡΙΑΣΜΟΣ 9: <input style="width: 100%;" type="text"/> <input style="width: 100%;" type="text"/> ΛΟΓΑΡΙΑΣΜΟΣ 11: <input style="width: 100%;" type="text"/> <input style="width: 100%;" type="text"/> ΛΟΓΑΡΙΑΣΜΟΣ 13: <input style="width: 100%;" type="text"/> <input style="width: 100%;" type="text"/> ΛΟΓΑΡΙΑΣΜΟΣ 15: <input style="width: 100%;" type="text"/> <input style="width: 100%;" type="text"/>	ΛΟΓΑΡΙΑΣΜΟΣ 2: <input style="width: 100%;" type="text"/> <input style="width: 100%;" type="text"/> ΛΟΓΑΡΙΑΣΜΟΣ 4: <input style="width: 100%;" type="text"/> <input style="width: 100%;" type="text"/> ΛΟΓΑΡΙΑΣΜΟΣ 6: <input style="width: 100%;" type="text"/> <input style="width: 100%;" type="text"/> ΛΟΓΑΡΙΑΣΜΟΣ 8: <input style="width: 100%;" type="text"/> <input style="width: 100%;" type="text"/> ΛΟΓΑΡΙΑΣΜΟΣ 10: <input style="width: 100%;" type="text"/> <input style="width: 100%;" type="text"/> ΛΟΓΑΡΙΑΣΜΟΣ 12: <input style="width: 100%;" type="text"/> <input style="width: 100%;" type="text"/> ΛΟΓΑΡΙΑΣΜΟΣ 14: <input style="width: 100%;" type="text"/> <input style="width: 100%;" type="text"/>
---	---

IA - ΛΟΓΑΡΙΑΣΜΟΣ ΙΔΙΟΥ
TP - ΛΟΓΑΡΙΑΣΜΟΣ ΤΡΙΤΩΝ

ΕΠΙΘΥΜΩ ΤΗ ΔΥΝΑΤΟΤΗΤΑ ΜΕΤΑΦΟΡΑΣ ΧΡΗΜΑΤΩΝ ΚΑΙ ΠΛΗΡΩΜΩΝ *
ΠΡΟΣ ΛΟΓΑΡΙΑΣΜΟΥΣ ΙΔΙΟΥ ΑΝΕΥ ΟΡΙΟΥ ΠΟΣΟΥ

ΟΧΙ ΝΑΙ

Εικόνα 2: Αίτηση εγγραφής Φυσικού προσώπου

Το συγκεκριμένο σύστημα πληρωμών προϋποθέτει την ύπαρξη συμφωνίας μεταξύ της τράπεζας και του εμπόρου. Επιπλέον ο πελάτης πρέπει να χρησιμοποιεί τις υπηρεσίες ηλεκτρονικής τραπεζικής που του προσφέρει η τράπεζα του. Σύμφωνα με μελέτη της Ευρωπαϊκής Κεντρικής Τράπεζας¹³, τα εν λόγω συστήματα ηλεκτρονικών πληρωμών λειτουργούν προς το παρόν σε αυστηρά εθνικά πλαίσια με αποτέλεσμα να μην είναι βολικά για διεθνείς συναλλαγές.

Απλή περίπτωση: Μεταφορά μεταξύ λογαριασμών

Ο απλούστερος τρόπος για τη διεκπεραίωση πληρωμής μέσω internet banking είναι η μεταφορά του ποσού από το λογαριασμό του πληρωτή στο λογαριασμό του δικαιούχου. Ο πληρωτής πρέπει απλά να περιγράψει ως "αιτιολογία" τα στοιχεία που χρειάζεται ο δικαιούχος για να αναγνωρίσει την πληρωμή. Είναι προφανές ότι, από τη μια πλευρά ο συγκεκριμένος τρόπος δεν χρειάζεται ιδιαίτερη υλοποίηση, από την άλλη όμως ελλοχεύουν πολλά λάθη (ποσό, αιτιολογία). Ο συγκεκριμένος τρόπος είσπραξης χρησιμοποιείται από φορείς που δεν έχουν σταθερούς πελάτες ή / και δέχονται περιστασιακές πληρωμές. Αφορά δε όλες τις κατηγορίες (P2P, B2C, B2B, x2G).

Ο εν λόγω τρόπος συναλλαγής για ηλεκτρονικές αγορές είναι και ο λιγότερος ελκυστικός τόσο για τους καταναλωτές όσο και για τους εμπόρους για μια σειρά από λόγους. Καθυστέρηση ολοκλήρωσης συναλλαγής (καθώς απαιτείται επιβεβαίωση από την τράπεζα), δαπάνη χρόνου για τον καταναλωτή (όταν πρόκειται για καταθέσεις μέσω της φυσικής οδού), οικονομικές επιβαρύνσεις από τις τράπεζες (ειδικά στα εμβάσματα αλλά και στις μεταφορές χρημάτων) είναι ορισμένοι από αυτούς. Εντούτοις, οι παραπάνω μέθοδοι μπορούν να φανούν αρκετά εξυπηρετικές όταν το προϊόν είναι άυλο και αφορά στην παροχή υπηρεσιών. Για παράδειγμα, η κράτηση ενός δωματίου από τον πελάτη στο δικτυακό τόπο ενός ξενοδοχείου ή, άλλο παράδειγμα, η δυνατότητα απόκτησης δικαιώματος πρόσβασης σε κάποιο συνδρομητικό site, μπορεί να

13 European Central Bank. E-payments in Europe – The euro system's perspective. Issue Paper available at www.ecb.int,

πραγματοποιηθεί εύκολα με τη συμπλήρωση της σχετικής φόρμας ενδιαφέροντος και είτε με τη χρήση πιστωτικής κάρτας είτε με κατάθεση χρημάτων για την ολοκλήρωσή της.

- **Πάγιες εντολές (e-banking)** :πρόκειται για προεγκριμένα χρεωστικά ποσά από τον τραπεζικό λογαριασμό του πελάτη που εκχωρούνται στον δικαιούχο. Οι πάγιες εντολές χρησιμοποιούνται συνήθως για επαναλαμβανόμενες πληρωμές όπως αυτές για λογαριασμούς ΔΕΚΟ ή για εφάπαξ πληρωμές όταν δεν υπάρχει άμεση επαφή μεταξύ εμπόρου και αγοραστή. Στις πάγιες εντολές, ο δικαιούχος αποστέλλει στον οφειλέτη ένα ειδικό έντυπο το οποίο ο τελευταίος συμπληρώνει αναγνωρίζοντας κατ' αυτό τον τρόπο την οφειλή του δικαιούχου. Στην συνέχεια ο τελευταίος προωθεί το ειδικό έντυπο στην συμβεβλημένη τράπεζα για την ολοκλήρωση της συναλλαγής.

Οι πάγιες εντολές χρησιμοποιούνται και για πληρωμές στο Διαδίκτυο. Στην περίπτωση αυτή όλη η ανωτέρω διαδικασία γίνεται ηλεκτρονικά και μοιάζει αρκετά στις πληρωμές στο Διαδίκτυο με τη χρήση πιστωτικής κάρτας. Η βασική διαφορά έγκειται στο γεγονός ότι ο οφειλέτης αποστέλλει το νούμερο του τραπεζικού του λογαριασμού και όχι αυτό της πιστωτικής του κάρτας.

Ειδικές περιπτώσεις: Εξειδικευμένη σελίδα πληρωμής

Για να διευκολύνουν τους συμμετέχοντες και να αποφεύγονται τα λάθη, οι τράπεζες δημιουργούν εξειδικευμένες σελίδες ("φόρμες") πληρωμής για κάθε δικαιούχο. Στις φόρμες αυτές ο δικαιούχος ζητά από τον πληρωτή συγκεκριμένα στοιχεία. Μάλιστα μερικά από τα στοιχεία αυτά μπορούν να ελεγχθούν για την ορθότητά τους, π.χ. με ψηφίο ελέγχου (check digit). Για να δημιουργήσουν τις εν λόγω σελίδες πληρωμής, οι τράπεζες πρέπει να θεωρήσουν ότι οι συγκεκριμένες συναλλαγές θα έχουν αρκετή χρήση, τόσο ώστε να τεκμηριώνεται τουλάχιστον το κόστος υλοποίησης. Αυτός είναι και ο λόγος που οι περισσότερες πληρωμές αφορούν μεγάλους φορείς με πολυπληθείς πελατειακές βάσεις, με αποτέλεσμα οι διαθέσιμες πληρωμές να είναι αρκετά περιορισμένες

Παράδειγμα 1:

Πληρωμή λογαριασμού ΔΕΗ. Ο πληρωτής/ συνδρομητής της ΔΕΗ περιγράφει το λογαριασμό, καταχωρίζοντας τον κωδικό ηλεκτρονικής πληρωμής, όπως αυτός περιγράφεται στο λογαριασμό της ΔΕΗ και καταχωρίζει και το ποσό πληρωμής. Το internet banking ελέγχει την ακρίβεια του κωδικού, με βάση το ψηφίο ελέγχου και χρησιμοποιώντας τον αλγόριθμο της ΔΕΗ. Το σύνολο των πληρωμών δημιουργεί αρχείο που αποστέλλεται στη ΔΕΗ και ο λογαριασμός της πιστώνεται στο συμφωνημένο χρόνο.

Παράδειγμα 2:

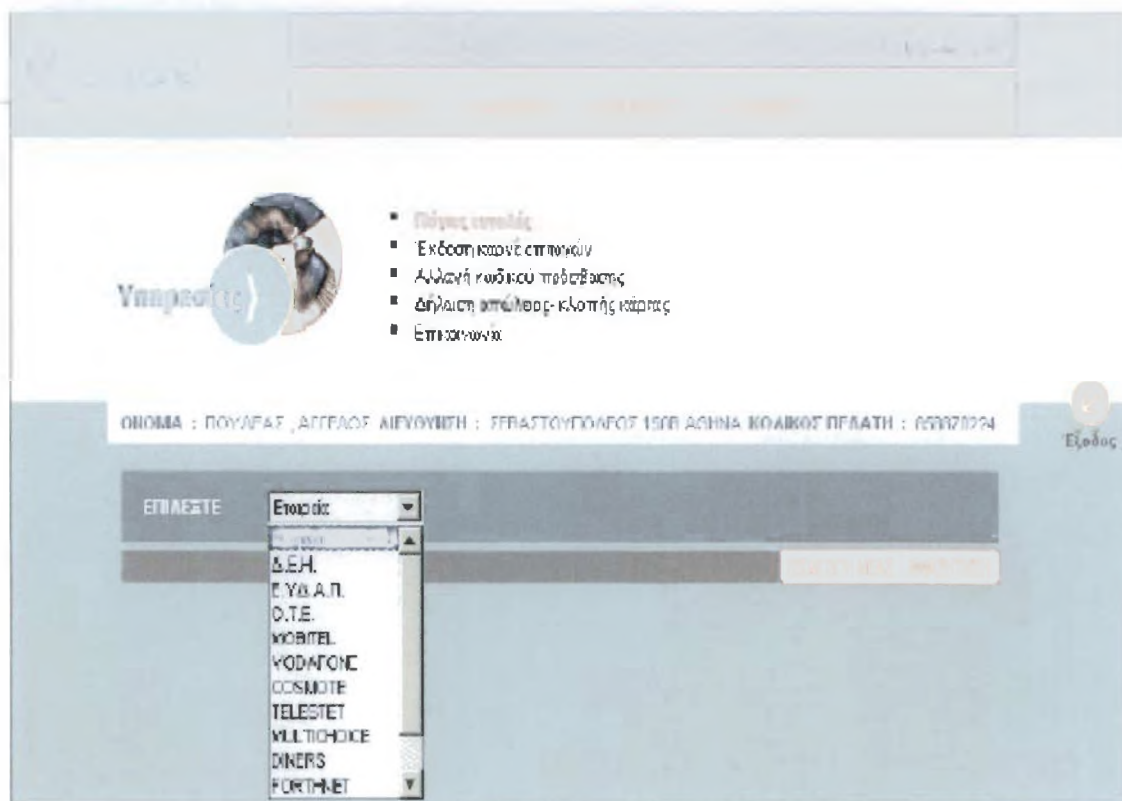
Πληρωμή Φ.Π.Α. Ο πληρωτής/ λογιστής καταχωρίζει το Α.Φ.Μ του πελάτη του, γράφει και την αντίστοιχη επωνυμία και δηλώνει το ποσό και το λογαριασμό που θα χρεωθεί. Το internet banking ελέγχει την ορθότητα (ύπαρξη) του Α.Φ.Μ, χρεώνει το λογαριασμό και ενημερώνει το αρχείο πληρωμών Φ.Π.Α Στην καθορισμένη ημερομηνία, το αρχείο αποστέλλεται στη ΔΙΑΣ, η οποία συγκεντρωτικά στέλνει ένα αρχείο στη ΓΓΠΣ του Υπ. Οικονομίας.

Ας δούμε τον τρόπο που με τον οποίο πραγματοποιούνται οι πληρωμές αυτές στην Εμπορική Τράπεζα:

Επιλέγοντας 'Πάγιας εντολές' από το μενού ΥΠΗΡΕΣΙΕΣ, εμφανίζεται μενού πολλαπλών επιλογών με όλες τις διαθέσιμες εταιρείες, τους λογαριασμούς των οποίων μπορείτε να εξοφλείτε με πάγια εντολή (Δ.Ε.Η , Ε.Υ.Δ.Α.Π., Ο.Τ.Ε., MOBITEL, VODAFONE, COSMOTE, TELESTET, MULTICHOICE, DINERS, FORTHNET , TELEPASSPORT, T.E.B.E).

Εισαγωγή πάγιας εντολής

Για να εισάγετε μία νέα πάγια εντολή επιλέξτε με κλικ του ποντικιού την εταιρεία που επιθυμείτε και το πλήκτρο **ΕΙΣΑΓΩΓΗ ΝΕΑΣ**




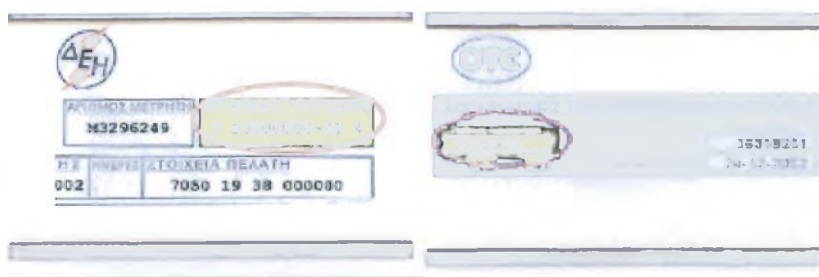
Εικόνα 3:Εισαγωγή πάγιας εντολής

Αμέσως εμφανίζεται η ακόλουθη οθόνη η οποία σας ζητάει να επιλέξετε το λογαριασμό που θα χρεώνεται και να συμπληρώσετε το ονοματεπώνυμο του συνδρομητή , το ανώτατο ποσό χρέωσης και τα στοιχεία λογαριασμού της εταιρείας που απαιτούνται



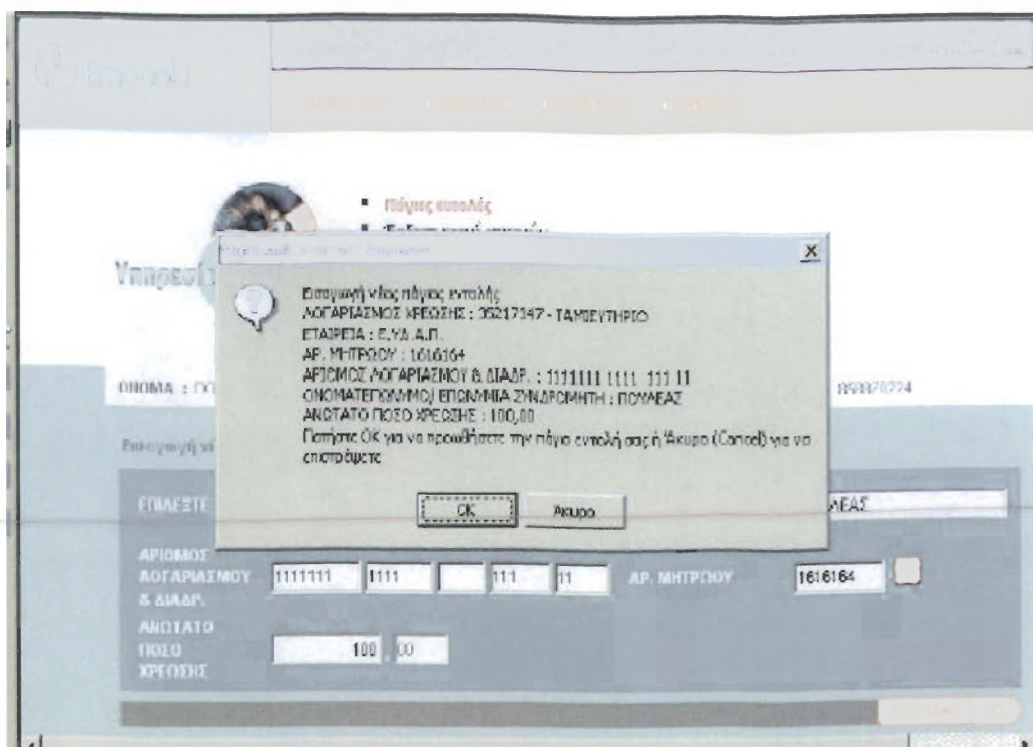
Εικόνα 4:Εισαγωγή στοιχείων

Για την διευκόλυνσή σας στη συμπλήρωση των απαραίτητων πεδίων μπορείτε να δείτε το δείγμα εντύπου όπου αναφέρονται με διακριτό τρόπο τα στοιχεία του λογαριασμού κάνοντας κλικ στο . Για παράδειγμα:



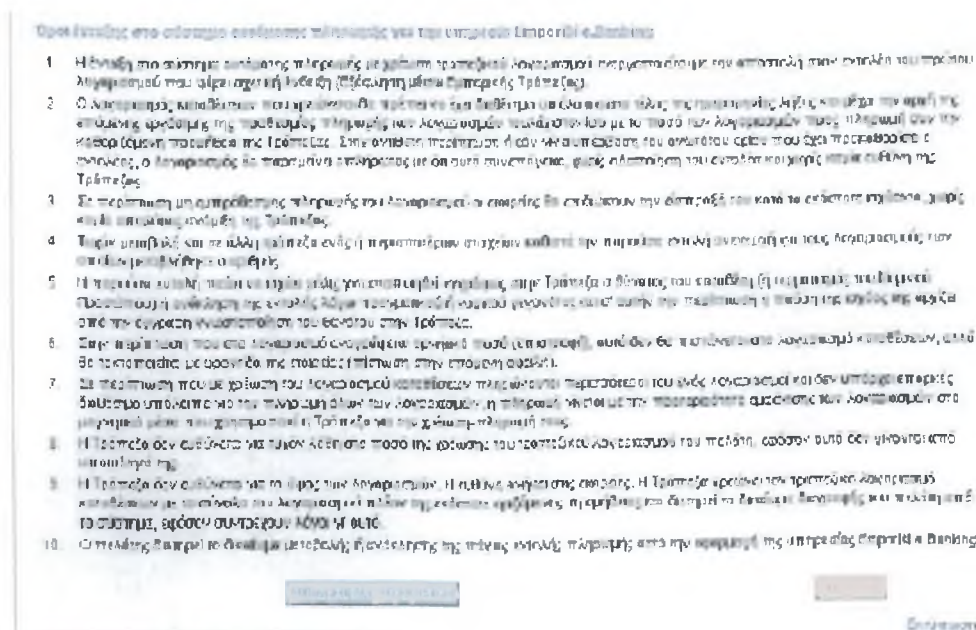
Εικόνα 5:Δείγμα εντύπου

Κάνοντας κλικ στο κουμπί **OK** εμφανίζεται το παρακάτω μήνυμα που σας ενημερώνει για τις επιλογές σας και σας προτρέπει να αποδεχθείτε ή όχι την προώθηση της πάγιας εντολής



Εικόνα 6: Προώθηση πάγιας εντολής

Τέλος, για την ολοκλήρωση και προώθηση της εντολής σας θα πρέπει να διαβάσετε και αποδεχθείτε τους όρους ένταξης στο σύστημα αυτόματης πληρωμής της υπηρεσίας e-Banking.



Εικόνα 7: Όροι ένταξης στο σύστημα E-Banking

Προσοχή: Η εντολή σας θα ενεργοποιηθεί από την εταιρεία και θα ισχύει μόνο για τους Λογαριασμούς στο αντίγραφο των οποίων θα υπάρχει σχετική αναφορά «Εξόφληση μέσω Εμπορική Bank» Αναζήτηση

ΟΝΟΜΑ : ΠΟΥΛΙΑΣ , ΑΓΓΕΛΟΣ ΔΙΕΥΘΥΝΣΗ : ΣΙΒΙΑΤΕΙΟΝ ΠΟΡΕΙΣ 1509 ΑΘΗΝΑ ΚΡΑΘΟΣ ΠΕΛΑΤΗ : 88880224

Η εντολή πάγιας πληρωμής που αποβάλλει καταχωρήθηκε. Η πάγια εντολή θα ενεργοποιηθεί από την εταιρεία και θα ισχύει μόνο για τους λογαριασμούς στο αντίγραφο των οποίων θα υπάρχει σχετική αναφορά "Εξόφληση μέσω Εμπορική Bank"

ΛΟΓΑΡΙΑΣΜΟΣ ΚΡΕΤΗΣΗΣ	36217347
ΕΤΑΙΡΕΙΑ	Ε.Υ.Α.Π.
ΣΤΟΙΧΕΙΑ ΛΟΓΑΡΙΑΣΜΟΥ	1616164 1111111111111111
ΟΝΟΜΑΤΕΠΩΝΥΜΟ/ΕΠΩΝΥΜΙΑ ΣΥΜΠΡΟΣΩΠΟΥ	ΠΟΥΛΙΑΣ
ΠΡΟΫΠΟΛΟΓΙΣΜΟΣ	02072003
ΑΜΟΙΒΑΤΟ ΠΟΣΟΣ ΚΡΕΤΗΣΗΣ	100,00

Εικόνα 8: Εξόφληση Πάγιας εντολής

Αναζήτηση εντολών

Μπορείτε να δείτε συγκεντρωτικά όλες τις πάγιες εντολές που έχετε δηλώσει επιλέγοντας από την οθόνη των πάγιων εντολών ΑΝΑΖΗΤΗΣΗ. Οι εντολές σας εμφανίζονται ανά λογαριασμό.

ΟΝΟΜΑ : ΠΟΥΛΙΑΣ , ΑΓΓΕΛΟΣ ΔΙΕΥΘΥΝΣΗ : ΣΙΒΙΑΤΕΙΟΝ ΠΟΡΕΙΣ 1509 ΑΘΗΝΑ ΚΡΑΘΟΣ ΠΕΛΑΤΗ : 88880224

ΕΤΡΑΧΕΤΕ:

ΛΟΓΑΡΙΑΣΜΟΣ ΚΡΕΤΗΣΗΣ	ΕΤΑΙΡΕΙΑ	ΣΤΟΙΧΕΙΑ ΛΟΓΑΡΙΑΣΜΟΥ	ΟΝΟΜΑΤΕΠΩΝΥΜΟ/ΕΠΩΝΥΜΙΑ ΣΥΜΠΡΟΣΩΠΟΥ	ΑΜΟΙΒΑΤΟ ΠΟΣΟΣ ΚΡΕΤΗΣΗΣ
36217347	Ε.Υ.Α.Π.	4404994 1111111111111111	ΠΟΥΛΙΑΣ , ΑΓΓΕΛΟΣ	2,00
36217347	Ε.Υ.Α.Π.	2088756	ΠΑΡΙΑ	30,00
36217347	Ε.Υ.Α.Π.	0410995	ΚΑΛΙΦΑΣ	100,00
36217347	ΚΟΥΡΦΕΡΗΣ	6400200 0541123456	ΠΟΥΛΙΑΣ , ΑΓΓΕΛΟΣ	2,00
36217347	ΤΕΛΕΡΕΤΡΥ	610040 600020318	ΠΟΥΛΙΑΣ , ΑΓΓΕΛΟΣ	100,00
36217347	ΤΕΛΕΡΑΦΟΡΤ	04004052704	ΠΟΥΛΙΑΣ , ΑΓΓΕΛΟΣ	€ 433.000,00
31017235	Δ.Ε.Ρ.	1 01234567890	ΠΟΥΛΙΑΣ , ΑΓΓΕΛΟΣ	10,00
31017235	Ε.Υ.Α.Π.	1111111 1111111111111111	ΠΟΥΛΙΑΣ , ΑΓΓΕΛΟΣ	1,00
31017235	ΚΟΥΡΦΕΡΗΣ	6400200 0541123456	ΠΟΥΛΙΑΣ , ΑΓΓΕΛΟΣ	4,00
31017235	ΟΔΗΓΩΤΕ	10049940	ΚΟΥΡΦΕΡΗΣ ΔΗΜΗΤΡΗΣ	1,00
31017235	ΟΔΗΓΩΤΕ	11234567890	ΠΟΥΛΙΑΣ , ΑΓΓΕΛΟΣ	2,00

Εικόνα 9: Αναζήτηση εντολών

Μπορείτε επίσης να δείτε τις εντολές που έχετε δώσει για μία μόνο εταιρεία, επιλέγοντας τη συγκεκριμένη εταιρεία και το πλήκτρο **ΑΝΑΖΗΤΗΣΗ**. Από τη λίστα των εντολών σας μπορείτε επίσης να πάρετε περισσότερες πληροφορίες για την κάθε εντολή, κάνοντας κλικ στο κουμπί με το **βελάκι**

στο δεξί μέρος κάθε εντολής.

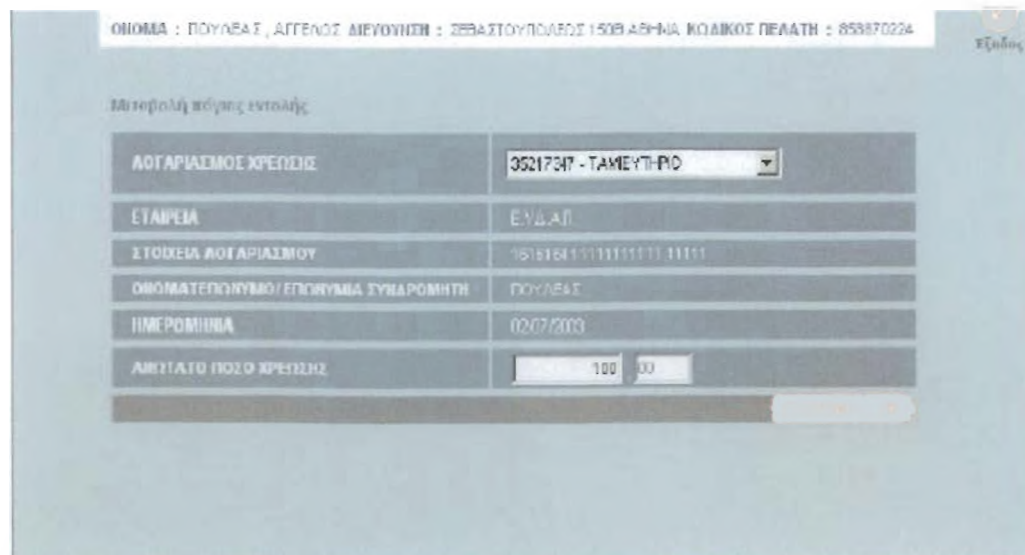
Μεταβολή στοιχείων πάγιας εντολής

Μπορείτε οποιαδήποτε στιγμή να μεταβάλλετε το λογαριασμό χρέωσης της εντολής σας αλλά και το ανώτατο ποσό χρέωσης του λογαριασμού σας ,επιλέγοντας το κουμπί



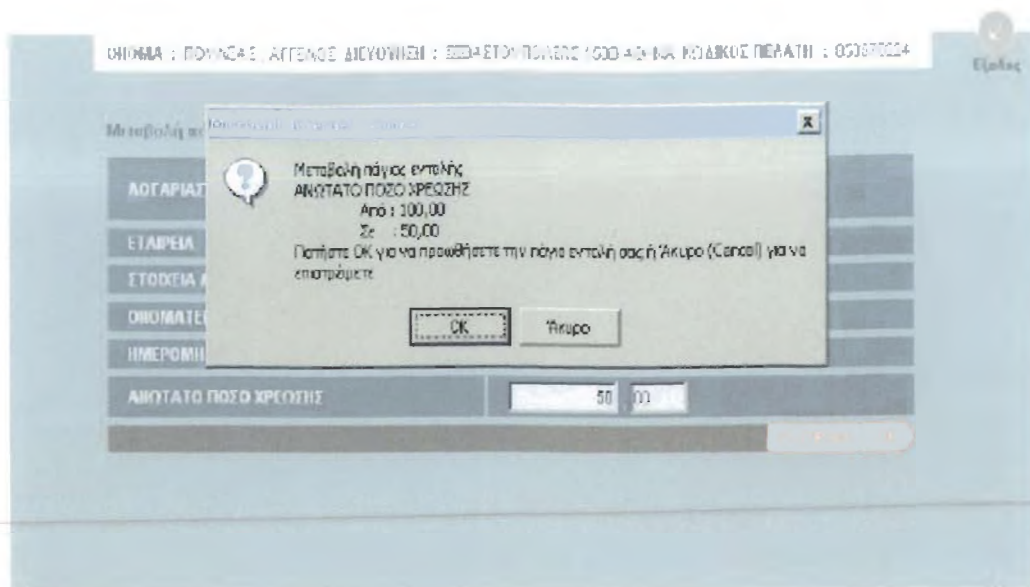
Εικόνα 10:Μεταβολή στοιχείων πάγιας εντολής

Εμφανίζεται η ακόλουθη οθόνη στην οποία μπορείτε να καταχωρήσετε τις τροποποιήσεις σας.



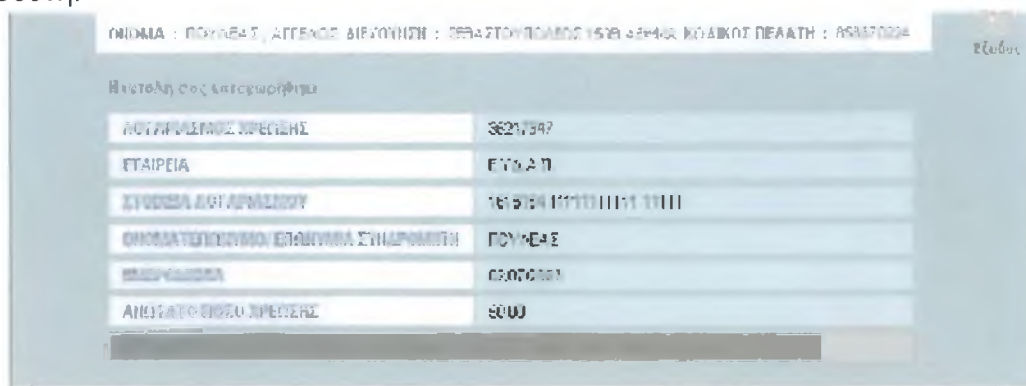
Εικόνα 11:Καταχωρήσεις

Πατώντας **OK** η υπηρεσία σας ενημερώνει για τις επιλογές σας και σας προτρέπει να προωθήσετε ή όχι την εντολή σας.



Εικόνα 12:Πρώθηση Εντολής

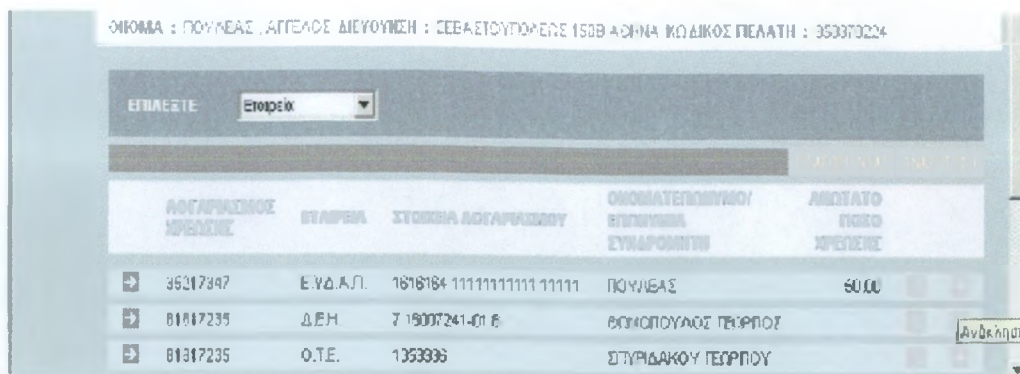
Κάνοντας κλικ στο πλήκτρο OK οι αλλαγές σας καταχωρούνται. Μήνυμα **επιτυχούς καταχώρησης** της πάγιας εντολής σας εμφανίζεται στην οθόνη.



Εικόνα 13:Καταχώρηση εντολής

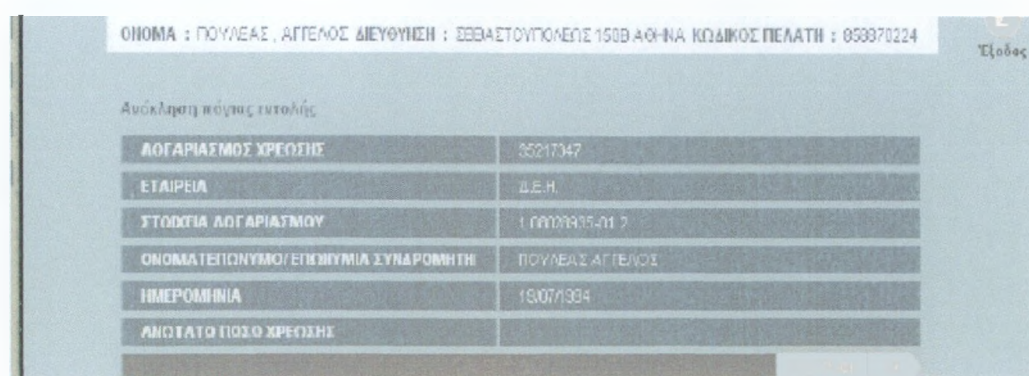
Ανάκληση πάγιας εντολής
Μπορείτε ακόμα οποιαδήποτε στιγμή επιθυμείτε να ανακαλέσετε την πάγια εντολή

σας, επιλέγοντας το κουμπί  στο δεξιό μέρος της εντολής σας.



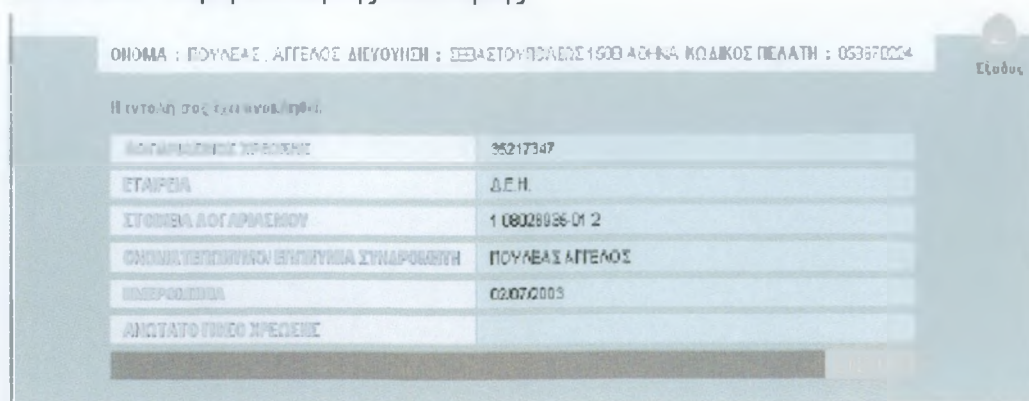
Εικόνα 14:Επιλογή ανάκλησης πάγιας εντολής

Εμφανίζεται η παρακάτω οθόνη η οποία σας ενημερώνει για τα στοιχεία της πάγιας εντολής που θέλετε να ανακληθεί. Κάνοντας κλικ στο πλήκτρο OK η εντολή σας θα ανακληθεί,



Εικόνα 15:Ανάκληση πάγιας εντολής

και θα δείτε επιβεβαίωση της ανάκλησης.



Εικόνα 16:Επιβεβαίωση ανάκλησης

- **Χρεωστικές κάρτες:** το εν λόγω σύστημα ηλεκτρονικών πληρωμών αποτελεί μία παραλλαγή των πάγιων εντολών όπου οι απαιτούμενες για τη συναλλαγή πληροφορίες περιέχονται σε ειδικές κάρτες με μαγνητική ταινία ή μικροεπεξεργαστή. Για την πραγματοποίηση συναλλαγών απαιτείται η ύπαρξη ειδικού τερματικού το οποίο θα επαληθεύει την εγκυρότητα των πληροφοριών που είναι αποθηκευμένες στην κάρτα και θα ελέγχει αν αυτή βρίσκεται σε ισχύ. Η διαδικασία πληρωμής είναι ακριβώς ίδια με αυτή των πάγιων εντολών με τη διαφορά ότι οι απαιτούμενες πληροφορίες είναι αποθηκευμένες στην κάρτα με αποτέλεσμα η συναλλαγή να είναι ασφαλέστερη. Ο κάτοχος της κάρτας πρέπει να διαθέτει ειδικό μηχάνημα υποδοχής συνδεδεμένο με τον υπολογιστή του που σημαίνει βέβαια ότι απαιτείται επιπλέον εξοπλισμός για τη χρήση της. Εντούτοις, το ειδικό αυτό μηχάνημα συχνά εκχωρείται στον πελάτη από την ίδια την τράπεζα.

Το βασικό μειονέκτημα των χρεωστικών καρτών είναι ότι από την σκοπιά του πελάτη ~~δεν είναι σαφή τα πλεονεκτήματά τους έναντι των πιστωτικών καρτών¹⁴~~. Ειδικά στις συναλλαγές στο Διαδίκτυο, οι χρεωστικές κάρτες προσφέρουν μικρότερη προστασία έναντι των πιστωτικών σε περιπτώσεις που τα αντικείμενα που αγοράστηκαν δεν παραδίδονται ή είναι ελαττωματικά. Από την πλευρά των εμπόρων πάντως οι χρεωστικές κάρτες είναι προτιμότερες καθώς δεν επιβαρύνουν με προμήθεια των εμπόρων. Επιπλέον, στην επιχειρηματικές συναλλαγές μέσω Διαδικτύου (B2B) οι χρεωστικές κάρτες μπορεί να αποδειχθούν φθηνότερη λύση ακριβώς για τον ίδιο λόγο.

Ας δούμε στον παρακάτω πίνακα τα βασικά χαρακτηριστικά των καρτών αυτών:

Υπέρ
Ασφάλεια
Δυνατότητα ανάληψης χρημάτων (όριο ανά μήνα)
Περίοδος χάριτος
Δυνατότητα προκαθορισμένων δόσεων (υπό προϋποθέσεις)
Αγορές «χωρίς όριο» (αρκεί να εξοφληθούν με την λήξη της περιόδου χάριτος)
Δεν απαιτείται τραπεζικός λογαριασμός
Κατά
Αυστηρότερα κριτήρια αξιολόγησης
Ακριβές συνδρομές
Υποχρεωτική εξόφληση του συνόλου του λογαριασμού κάθε μήνα
Υψηλοί τόκοι σε περίπτωση καθυστέρησης της εξόφλησης του λογαριασμού

ΠΕΡΙΓΡΑΦΗ-ΜΗΧΑΝΙΣΜΟΣ

Οι κάρτες αυτές δεν συνδέονται απαραίτητα με τραπεζικό λογαριασμό ενώ εκδίδονται

14 Turban, E.; Lee, J.; King, D. & Chung, H. M. (2003). Electronic commerce: A managerial perspective. International Edition, Upper Saddle River: Prentice Hall, pp. 289

για χρήστες με σχετικά υψηλά εισοδήματα ,έχουν δε υψηλές συνδρομές. Οι κάρτες αυτές δεν παρέχουν πίστωση στον χρήστη παρά **μόνο** « περίοδο χάριτος » ,ένα χρονικό διάστημα δηλαδή 20-30 ημερών ,που μεσολαβεί από την συναλλαγή έως την **εξ' ολοκλήρου εξόφληση** του αντιτίμου.

Ο κάτοχος της κάρτας πρέπει κάθε μήνα να εξοφλεί **ολόκληρο** το ποσό ,το οποίο αναγράφεται στον λογαριασμό του. Στην αντίθετη περίπτωση οι τόκοι είναι πολύ υψηλοί γιατί έχουν **χαρακτήρα** τόκων υπερημερίας (πρόστιμο δηλαδή για καθυστέρηση πληρωμής) και **όχι** τόκων πιστωτικού δανείου. Οι κάρτες προωθούνται στο καταναλωτικό κοινό ως κάρτες χωρίς πιστωτικό όριο, στην πραγματικότητα όμως πιστωτικό όριο υπάρχει για κάθε πελάτη. Σε ειδικές περιπτώσεις και μετά από συμφωνία με εμπόρους προσφέρονται διευκολύνσεις με προγράμματα άτοκων δόσεων, για τους κατόχους τέτοιων καρτών.

Οι κάρτες αυτές (η Diners παλαιότερα, American Express) έχουν σχετικά χαμηλή αποδοχή ,που φαίνεται από την μικρή εξάπλωσή τους ,τον σχετικά χαμηλό αριθμό συμβεβλημένων επιχειρήσεων και το μικρό μερίδιο αγοράς τους, επί του συνόλου των καρτών στην Ελλάδα. Τα έσοδα των καρτών αυτών προέρχονται από τις ετήσιες συνδρομές και από τις προμήθειες των εμπόρων.

Πώς γίνεται η πληρωμή με πιστωτική και χρεωστική κάρτα; Υπάρχει Point Of Sales (POS);

Όπως και στο “φυσικό κόσμο”, στο τέλος της διαδικασίας ο πελάτης πηγαίνει στο ταμείο για να πληρώσει. Δεδομένου ότι στο Internet ο πελάτης δεν μπορεί να πληρώσει με μετρητά, το προσφορότερο μέσο πληρωμής είναι η κάρτα, χρεωστική και πιστωτική. Στις περισσότερες περιπτώσεις η διεκπεραίωση της χρέωσης της κάρτας του πελάτη γίνεται από μια τράπεζα.

Η κάρτα είναι το καταλληλότερο μέσο για αυτές τις πληρωμές, λόγω της “παγκοσμιοότητας” που τη χαρακτηρίζει. Κάθε εμπορικό κατάστημα, τόσο στο φυσικό κόσμο όσο και στο Internet, μπορεί να συνεργαστεί με μία ή περισσότερες τράπεζες και να αποκτήσει τη δυνατότητα να κάνει τις εισπράξεις του, χρεώνοντας οποιαδήποτε πιστωτική κάρτα φέρει το σήμα ενός από τους διεθνείς οργανισμούς καρτών (Visa, MasterCard, Diners, American Express κ.λπ.) και ανεξάρτητα από τη χώρα και την τράπεζα που έχει εκδώσει την κάρτα.

Στο φυσικό κόσμο υπάρχει το τερματικό EFT /POS (Electronic Funds Transfer/Point Of Sales), που ανήκει στην τράπεζα με την οποία συνεργάζεται το εμπορικό κατάστημα (στον κόσμο των καρτών, η τράπεζα αυτή λέγεται “acquiring bank” ή “acquirer”). Η διαδικασία πληρωμής είναι ως εξής:

1. Ο πελάτης δίνει στον ταμιά την κάρτα του (πιστωτική και ενίοτε χρεωστική) και αυτός την εισάγει στο POS και πληκτρολογεί το ποσό.
2. Το POS δημιουργεί τη συναλλαγή πληρωμής και τη στέλνει στην τράπεζα / acquirer.

3. Ο acquirer στέλνει τη συναλλαγή στον οργανισμό, το σήμα του οποίου φέρει η κάρτα.
4. Ο οργανισμός την προωθεί στην τράπεζα που έχει εκδώσει τη συγκεκριμένη κάρτα (η τράπεζα αυτή λέγεται "issuing bank" ή "issuer").
5. Ο issuer εγκρίνει (οπότε χρεώνει τον πελάτη) ή απορρίπτει τη συναλλαγή.
6. Η απάντηση, μέσω του ίδιου οργανισμού, επιστρέφει στον acquirer και, από εκεί, στο POS.
7. Αν η συναλλαγή/ χρέωση είναι επιτυχής, ο πελάτης παραλαμβάνει τα αγαθά ή τις υπηρεσίες.

Στο Internet, όπως και στο φυσικό κόσμο, υπάρχει ένα ιδεατό POS (virtual POS ή electronic POS), αντίστοιχο με αυτό του εμπορικού καταστήματος. Όταν ο πελάτης έχει ολοκληρώσει τις επιλογές του (προϊόντα ή / και υπηρεσίες), του παρουσιάζεται η σελίδα που υλοποιεί το μηχανισμό του POS. Η διαδικασία είναι πανομοιότυπη με αυτή του φυσικού κόσμου. Υπάρχουν όμως μερικές ουσιώδεις διαφορές, οι κυριότερες από τις οποίες είναι οι εξής:

- Ο πελάτης (ως φυσική παρουσία) είναι απών.
- Η φυσική κάρτα (πλαστικό) δεν είναι παρούσα.
- Η εισαγωγή των στοιχείων της κάρτας (στο αντίστοιχο βήμα 1 παραπάνω) γίνεται από τον πελάτη. Τα στοιχεία που εισάγει ο πελάτης είναι ο αριθμός της κάρτας (συνήθως 16 ψηφία), η ημερομηνία λήξης (μήνας/ έτος) και ο τριψήφιος κωδικός ασφαλείας Card Security Code: η Visa τον ονομάζει CVV2 (Card Verification Value 2) και η MasterCard τον ονομάζει CVC2 (Card Verification Code 2) και είναι γραμμένος στο πίσω μέρος του πλαστικού, πάνω στη χάρτινη ταινία όπου μπαίνει η υπογραφή του κατόχου της κάρτας.
(Τα παραπάνω έχουν άμεση επίπτωση στην ασφάλεια της συναλλαγής).

Η σελίδα που αντιστοιχεί στο POS μπορεί να ανήκει:

Στο ίδιο το web site. Στην περίπτωση αυτή τα στοιχεία που εισάγει ο πελάτης συλλέγονται από το web site και, μαζί με τα άλλα στοιχεία της συναλλαγής (ποσό, κωδικός εμπόρου κ.λπ.), στέλνονται στην τράπεζα με την οποία συνεργάζεται το web site. Στη συνέχεια η τράπεζα δημιουργεί τη συναλλαγή χρέωσης της κάρτας και εφαρμόζει τα υπόλοιπα βήματα που περιγράφηκαν παραπάνω. Θεωρητικά και για λόγους ασφάλειας, το web site δεν πρέπει να αποθηκεύει τα στοιχεία των καρτών. Στο web site της τράπεζας / acquirer. Ο πελάτης "μεταφέρεται" διαφανώς στο web site της τράπεζας, όπου του παρουσιάζεται μια σελίδα εισαγωγής των στοιχείων της κάρτας. Τα στοιχεία γίνονται γνωστά μόνο στην τράπεζα, η οποία εφαρμόζει τα υπόλοιπα βήματα της παραπάνω διαδικασίας, στο τέλος της οποίας "μεταφέρει" τον πελάτη στο αρχικό web site όπου ενημερώνεται για το αποτέλεσμα της συναλλαγής (έγκριση/ απόρριψη). Στο web site παρόχου υπηρεσιών πληρωμής. Λόγω της ιδιαιτερότητας του Internet, έχει εμφανιστεί το μοντέλο Internet Payment Service Provider (IPSP). Οι IPSP είναι εταιρείες που αναλαμβάνουν τη διεκπεραίωση της πληρωμής συνεργαζόμενες με μία ή περισσότερες τράπεζες. Ο ιδιοκτήτης του web site είναι πελάτης του IPSP και όχι της τράπεζας. Ο IPSP συγκεντρώνει όλα τα στοιχεία των συναλλαγών και προωθεί τις συναλλαγές σε μία από τις τράπεζες, με την οποία συνεργάζεται. Η είσπραξη των ποσών γίνεται από τον IPSP, ο οποίος κατανέμει τα ποσά στους πελάτες του στα συμφωνημένα χρονικά διαστήματα και αφού παρακρατήσει τη συμφωνημένη προμήθεια.

- **Ηλεκτρονικές επιταγές:** Οι ηλεκτρονικές επιταγές είναι η φυσιολογική συνέχεια των παραδοσιακών επιταγών. Μια επιταγή είναι μία γραπτή εντολή από τον εκδότη προς τον αποδέκτη που είναι συνήθως τράπεζα με την οποία ο εκδότης απαιτεί από τον αποδέκτη την καταβολή ενός συγκεκριμένου ποσού είτε στον εκδότη είτε σε τρίτο πρόσωπο που ορίζεται από αυτόν. Οι ηλεκτρονικές επιταγές ακολουθούν κατά βάση τον ίδιο κανόνα με τη διαφορά ότι η επιταγή είναι σε ηλεκτρονική μορφή¹⁵. Επιπλέον, καθώς ο εκδότης πρέπει να υπογράψει την επιταγή προκειμένου να είναι έγκυρη στις ηλεκτρονικές επιταγές χρησιμοποιείται η ψηφιακή υπογραφή προκειμένου να ολοκληρωθεί η διαδικασία¹⁶. Λειτουργικά οι ηλεκτρονικές επιταγές έχουν πολλές ομοιότητες με τις συμβατικές επιταγές, ενώ χρησιμοποιούν ψηφιακές υπογραφές για την έκδοση ή την οπισθογράφιση, και απαιτούν ψηφιακά πιστοποιητικά για την ταυτότητα του πληρωτή, της τράπεζας και του τραπεζικού λογαριασμού. Το σύστημα ασφάλειας-πιστοποίησης υποστηρίζεται από ψηφιακές υπογραφές που χρησιμοποιούν κρυπτογράφιση με δημόσιο κλειδί.

Μια ηλεκτρονική επιταγή μπορεί να μεταβιβαστεί είτε με απευθείας (κλειστή) σύνδεση δυο ηλεκτρονικών υπολογιστών, με τη χρήση MODEM και τηλεφωνικών γραμμών, είτε μέσα από δημόσια δίκτυα, όπως το INTERNET. Οι ηλεκτρονικές επιταγές γίνονται δεκτές από τράπεζες και εξοφλούνται μέσα από υπάρχοντες τραπεζικούς μηχανισμούς (όπως το δίκτυο BACS στη Βρετανία). Η σύνδεση της υπάρχουσας τραπεζικής υποδομής με τα δημόσια δίκτυα θα διευκολύνει τη συνεργασία τραπεζών, επιχειρήσεων και πελατών, και θα κάνει δυνατή την εξάπλωση της χρήσης ηλεκτρονικών επιταγών.

Οι υποστηρικτές του συστήματος των ηλεκτρονικών επιταγών πιστεύουν ότι θα ευνοήσει την ανάπτυξη των ηλεκτρονικών συναλλαγών για τους εξής λόγους: (α) θα επιτρέψει την αμφίδρομη επικοινωνία, π.χ. ο αποδέκτης θα μπορεί να επικοινωνήσει με την τράπεζα του εκδότη και να επιβεβαιώσει την κάλυψη της επιταγής, (β) θα βελτιώσει την ασφάλεια σε όλα τα βήματα της συναλλαγής, μέσα από τον έλεγχο της ηλεκτρονικής υπογραφής των δυο μερών και της τράπεζας, και (γ) θα διευκολύνει τη σύνδεση των πληρωμών με τα ήδη χρησιμοποιούμενα συστήματα EDI.

Η χρήση ηλεκτρονικών επιταγών δείχνει να είναι ένα μάλλον Αμερικανικό φαινόμενο - κάτι αναμενόμενο, αφού επιχειρήσεις και καταναλωτές στις Η.Π.Α μένουν προσκολλημένοι στη χρήση επιταγών και δεν υιοθετούν τις πιστωτικές κάρτες, που γνωρίζουν μεγάλη επιτυχία στον υπόλοιπο κόσμο. Στην Ευρώπη υπάρχει ένα πολύ μεγαλύτερο ενδιαφέρον των επιχειρήσεων για πιστωτικές κάρτες και ψηφιακά μετρητά

15 European Central Bank. E-payments in Europe – The eurosystem's perspective. Issue Paper available at www.ecb.int

16 Παπαναγιώτου, Ν.: Internet – Επιχείρηση. Διαθέσιμο στο http://users.ciionet.gr/~pap_n@ciionet.htm.

4.2 ΚΑΙΝΟΤΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ ΓΙΑ ΤΟ ΔΙΑΔΙΚΤΥΟ

Στην κατηγορία αυτή υπάρχουν συστήματα πληρωμών τα οποία κάνουν χρήση καινοτομικών τεχνολογιών που μέχρι πρόσφατα δεν ήταν διαθέσιμες για την διεξαγωγή πληρωμών. Επιπλέον, πολλά από τα συστήματα αυτά είναι προσαρμοσμένα στις τρέχουσες τάσεις του ηλεκτρονικού επιχειρείν και προσπαθούν να ικανοποιήσουν τις καταναλωτικές τάσεις που φαίνεται να διαμορφώνονται στο διαδίκτυο όπως η αγορά άυλων αγαθών μικρής αξίας κ.α. Μερικά από τα συστήματα αυτά όπως οι έξυπνες κάρτες αρχίζουν να χρησιμοποιούνται και στον φυσικό κόσμο ενώ άλλα είναι σχεδιασμένα αποκλειστικά για χρήση στο διαδίκτυο.

Ειδικότερα τα συστήματα αυτά είναι:

Σχήματα ηλεκτρονικού χρήματος

Ως **ηλεκτρονικό χρήμα**, η Ευρωπαϊκή Κεντρική Τράπεζα ορίζει «την αποθήκευση χρηματικής αξίας σε ψηφιακή μορφή μέσω μιας συσκευής που μπορεί να χρησιμοποιηθεί ευρέως για την πραγματοποίηση πληρωμών σε δίκτυα χωρίς την χρήση τραπεζικών λογαριασμών». Το ηλεκτρονικό χρήμα θα λειτουργεί ως προπληρωμένο υπόθεμα. Ενώ τα δίκτυα θα είναι είτε ανοικτά δηλαδή θα επιτρέπουν την άμεση μεταφορά χρημάτων μεταξύ υποθεμάτων είτε κλειστά όπου η χρέωση του υποθέματος θα γίνεται από συγκεκριμένο τραπεζικό λογαριασμό αποκλειστικά¹⁷. Είναι επομένως εμφανές ότι το ηλεκτρονικό χρήμα έχει ανάλογες ιδιότητες με τα κοινά τραπεζογραμμάτια.

Μέχρι τώρα τα ισχύοντα σχήματα ηλεκτρονικού χρήματος στηρίζονται είτε σε κάρτες αποθηκευμένης αξίας είτε σε ειδικό λογισμικό¹⁸. Στην πρώτη περίπτωση η κάρτα περιέχει ένα χρηματικό ποσό ανάλογο με αυτό που έχει προπληρώσει ο κάτοχος της. Η κάρτα μπορεί δε να είναι είτε ανώνυμη είτε ονομαστική. Ο κάτοχος της μπορεί να τη φορτίζει κάθε φορά με το ποσό που επιθυμεί. Για λόγους ασφαλείας, η κάρτα προστατεύεται από τετραψήφιο κωδικό.

Στα σχήματα ηλεκτρονικού χρήματος μέσω λογισμικού πραγματοποιείται έκδοση ηλεκτρονικών νομισμάτων από έναν παροχέα υπηρεσιών πληρωμών. Τα ηλεκτρονικά αυτά νομίσματα είναι αποθηκευμένα σε ένα ηλεκτρονικό πορτοφόλι στον υπολογιστή του χρήστη ο οποίος μπορεί να τα χρησιμοποιήσει για αγορές μέσω Διαδικτύου. Μέχρι τώρα οι περισσότερες πρωτοβουλίες με σχήματα ηλεκτρονικού χρήματος μέσω ειδικού λογισμικού δεν έτυχαν ευρείας αποδοχής καθώς δεν είναι ιδιαίτερα ευέλικτα. Οι όποιες προσπάθειες έμειναν σε πιλοτικό στάδιο.

17 Turban, E.; Lee, J.; King, D. & Chung, H. M. (2003). Electronic commerce: A managerial perspective. International Edition, Upper Saddle River: Prentice Hall, pp. 289.

18 European Central Bank E-payments in Europe – The eurosystem's perspective. Issue Paper available at www.ecb.int

Το βασικό πλεονέκτημα πάντως των σχημάτων ηλεκτρονικών πληρωμών και στις δύο περιπτώσεις είναι ότι διατηρείται η ανωνυμία των συναλλαγών που είναι ιδιαίτερα σημαντική για τους πελάτες. Επιπλέον, ειδικά οι κάρτες αποθηκευμένης αξίας είναι ιδιαίτερα ευέλικτο μέσο πληρωμής που επιτρέπει και διεθνείς συναλλαγές.

Τα σχήματα ηλεκτρονικού χρήματος στηρίζονται:

- Σε Προπληρωμένες Κάρτες αποθηκευμένης αξίας (prepaid stored-value cards)

Οι Κάρτες αποθηκευμένης αξίας χρησιμοποιούνται περισσότερο από το e-cash ως εναλλακτική για τις πιστωτικές κάρτες. Όταν χρησιμοποιούνται για να αποθηκεύσουν μετρητά από μία τράπεζα ή ένα λογαριασμό πιστωτικής κάρτας, οι έξυπνες κάρτες μπορούν να χρησιμοποιηθούν για την αγορά αντικειμένων με αξία από λίγα έως πολλά Ευρώ. Διάφοροι τύποι προμηθευτών αποδέχονται κάρτες αποθηκευμένης αξίας:

Fast-food εστιατόρια, φαρμακεία, αυτόματες μηχανές πώλησης, βενζινάδικα κ.ά. Visa cash - Mondex -Κάρτα αποθηκευμένης αξίας που έχει σχεδιαστεί για μικρές αγορές ή μικροπληρωμές.

- Έξυπνες Κάρτες (μικρό-τσιπ & μνήμη) ή κάρτες μαγνητικής ταινίας

Αρκετοί από εμάς χρησιμοποιούμε ήδη μία ή περισσότερες έξυπνες κάρτες στην καθημερινή μας ζωή. Για παράδειγμα, έξυπνη κάρτα είναι η κάρτα SIM που χρησιμοποιείται στο σύστημα κινητής τηλεφωνίας GSM. Οι έξυπνες κάρτες είναι ουσιαστικά μικροσκοπικοί υπολογιστές, που έχουν το μέγεθος και τη φόρμα μίας πιστωτικής κάρτας, πάνω στην οποία είναι ενσωματωμένο ένα ολοκληρωμένο κύκλωμα (chip), στην εμπρόσθια αριστερή πλευρά.



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

Το κύριο γνώρισμα των έξυπνων καρτών είναι η ικανότητα να αποθηκεύουν και να

επεξεργάζονται πληροφορίες με ένα ασφαλή τρόπο. Τα πλεονεκτήματα των έξυπνων καρτών είναι η προστασία των δεδομένων που περιέχουν, η φορητότητα και η ευκολία χρήσης.

Προκειμένου το ολοκληρωμένο να μπορεί να χρησιμοποιηθεί και σε τερματικά ή αναγνώστες τα οποία δεν έχουν το απαιτούμενο μέγεθος για την εισαγωγή ολόκληρης της κάρτας, είναι δυνατή η παραγωγή των καρτών με εγκοπές γύρω από το ολοκληρωμένο, προκειμένου αυτό να αφαιρείται και να τοποθετείται στην τερματική συσκευή. Κλασικό παράδειγμα οι κάρτες SIM

Τομέας	Υπάρχοντα	Πιθανές	Προβλεπόμενα	Μειονεκτήματα
Τραπεζικός Τομέας	Κάρτες πληρωμής (MasterCard, Visa, American Express, Eurocard, etc.)	Κάρτες πιστώσεων (American Express, Visa Signature, etc.)	Κάρτες με ενσωματωμένο chip (Smart Cards)	Απαιτείται υποδομή για ανάγνωση
Τηλεπικοινωνίες Δημόσιος Τομέας	Κάρτες SIM (Subscriber Identity Module)	Κάρτες με ενσωματωμένο chip (Smart Cards)	Κάρτες με ενσωματωμένο chip (Smart Cards)	Απαιτείται υποδομή για ανάγνωση
Μεταφορές	Κάρτες πληρωμής (MasterCard, Visa, American Express, Eurocard, etc.)	Κάρτες πιστώσεων (American Express, Visa Signature, etc.)	Κάρτες με ενσωματωμένο chip (Smart Cards)	Απαιτείται υποδομή για ανάγνωση
Υγεία	Κάρτες πληρωμής (MasterCard, Visa, American Express, Eurocard, etc.)	Κάρτες πιστώσεων (American Express, Visa Signature, etc.)	Κάρτες με ενσωματωμένο chip (Smart Cards)	Απαιτείται υποδομή για ανάγνωση
Λοιπά	Κάρτες πληρωμής (MasterCard, Visa, American Express, Eurocard, etc.)	Κάρτες πιστώσεων (American Express, Visa Signature, etc.)	Κάρτες με ενσωματωμένο chip (Smart Cards)	Απαιτείται υποδομή για ανάγνωση

Πίνακας 4: Γνωστές και πιθανές εφαρμογές έξυπνων καρτών κατά τομέα και τύπο κάρτας

ΠΛΕΟΝΕΚΤΗΜΑΤΑ

-Χαρακτηριστικό ανοχής σε κακόβουλους χειρισμούς (tamper-resistant)
-Μπορούν να ανιχνεύσουν και να αντιδράσουν σε κακόβουλους χειρισμούς (tamper-proof)
-Ενσωματώνουν, τις ραγδαίες εξελίξεις στην τεχνολογία ημιαγωγών, επιτρέποντας τη συνεχή βελτίωση των χαρακτηριστικών τους
-Ως επί το πλείστον είναι επαναπρογραμματιζόμενες
-Διαθέτουν δυνατότητες υπολογισμού και πράξεων (computing & calculating)
-Διαθέτουν κυκλώματα λογικής και μνήμης
-Επεξεργάζονται δεδομένα και αποθηκεύουν πληροφορίες
-Μπορούν να συγκρίνουν και να διαχειρίζονται σύνθετες πληροφορίες
-Συνήθως χρησιμοποιούνται για εφαρμογές μεγάλης ασφάλειας (high security)
-Επιτρέπουν off-line εξακρίβωση των στοιχείων, σε αντίθεση με μία κάρτα με μαγνητική λωρίδα
-Δίνουν δυνατότητα επιλογής στο ποια στοιχεία της κάρτας είναι προσβάσιμα από διαφορετικές εφαρμογές
-Επιτρέπουν μεγάλη ασφάλεια, και αυτό οφείλεται στις πολύπλοκες κρυπτογραφικές τεχνικές που χρησιμοποιούνται για να αποκωδικοποιούν την «κυκλοφορία» της πληροφορίας μεταξύ έξυπνων καρτών και άλλων συσκευών
-Προσφέρουν μεγάλη χωρητικότητα αποθήκευσης πληροφοριών
-Είναι συμβατές με φορητές ηλεκτρονικές συσκευές

Πίνακας 5:Πλεονεκτήματα έξυπνων καρτών

ΑΣΦΑΛΕΙΑ

ΕΠΙΧΕΙΡΗΣΕΙΣ

1. Περιορισμός οικονομικού εγκλήματος
2. Αποδοτικότητα και αποτελεσματικότητα πωλήσεων

ΠΕΛΑΤΗ

1. Προσφέρουν μεγαλύτερη ασφάλεια
2. Μια έξυπνη κάρτα πολλαπλών εφαρμογών προσφέρει ευκολία
3. Επιτρέπει την συμμετοχή σε προγράμματα rewards και loyalty
4. Επιτρέπει αποθήκευση και πρόσβαση σε απαραίτητη πληροφορία

Εικόνα 17:Ασφάλεια έξυπνων καρτών για επιχειρήσεις και πελάτες

- Στη μνήμη Ηλ. Υπολογιστή (ή άλλης φορητής συσκευής) με τη μορφή Λογισμικού e - wallet

E-WALLET

Ένα ηλεκτρονικό πορτοφόλι (e-wallet) είναι μια επέκταση της ιδέας της πιστωτικής κάρτας. Τέτοια πορτοφόλια κρατούν αρχείο των πληρωμών σας με πιστωτική κάρτα, διαχειρίζονται τη χρήση περισσότερων πιστωτικών καρτών και αυτοματοποιούν την αγορά αγαθών στο διαδίκτυο. Για παράδειγμα, δε χρειάζεται να τυπώνεται συνεχώς τις λεπτομέρειες των πιστωτικών σας καρτών. Οι περισσότερες καινοτομίες στον τομέα αυτό έχουν γίνει από εταιρίες όπως Mastercard και Visa που έδωσαν άδεια για τη συγκεκριμένη τεχνολογία στις τράπεζες. Η τεχνολογία που χρησιμοποιείται επισταμένως είναι η SSL.

Χωρίζονται σε δύο κατηγορίες:

- Τα ηλεκτρονικά πορτοφόλια από την πλευρά του εξυπηρετητή αποθηκεύουν τις πληροφορίες των πελατών στον απομακρυσμένο εξυπηρετητή του εμπόρου ή ακόμα καλύτερα στον εκδότη του ηλ. πορτοφολιού. Βασικό τους μειονέκτημα είναι ότι εάν γίνει κάποια υποκλοπή, θα αποκαλυφθούν προσωπικές πληροφορίες μεγάλου αριθμού χρηστών. Γι' αυτό το λόγο διαθέτουν ένα πολύ ισχυρό σύστημα ασφαλείας.
- Τα ηλεκτρονικά πορτοφόλια από την πλευρά του χρήστη αποθηκεύουν τις πληροφορίες στους υπολογιστές των πελατών. Έτσι δεν υπάρχει το μειονέκτημα στο βαθμό που αναφέραμε προηγουμένως. Τα περισσότερα ηλ. Πορτοφόλια είναι αυτού του τύπου, δίνοντας την δυνατότητα ασφαλέστερων αγορών μέσω του Διαδικτύου. Βασικό τους μειονέκτημα είναι ότι δεν είναι μεταφέριμα, δηλαδή είναι διαθέσιμα μόνο στον υπολογιστή που έχουν εγκατασταθεί. Αυτό έχει ως αποτέλεσμα οι πελάτες να μην έχουν την δυνατότητα χρήσης τους από έναν άλλο υπολογιστή.

Ηλεκτρονικά νομίσματα (e-coins) ή Ηλεκτρονικά μετρητά (e-cash)

ΨΗΦΙΑΚΟ ΧΡΗΜΑ

Παρά το γεγονός πως ένα ψηφιακό ισότιμο των μετρητών μπορεί να φαίνεται άμεσο σύστημα, τα ψηφιακά μετρητά, ή e-cash όπως συνηθίζονται να λέγονται, παρουσίασαν κάποια σημαντικά ρυθμιστικά ζητήματα που σχετίζονται κυρίως με την ασφάλεια και την μυστικότητα. Αποτελούν επίσης ένα σύστημα που ταιριάζει περισσότερο σε συναλλαγές που αφορούν μικρά ποσά διακινούμενων χρημάτων σε πραγματικό χρόνο στο διαδίκτυο, το οποίο πολλοί αντιμετωπίζουν ως το νέο κύμα εφαρμογών στο χώρο του ηλεκτρονικού εμπορίου.

Σε ένα σύστημα ψηφιακών μετρητών το συνάλλαγμα δεν είναι παρά μόνο μια ακολουθία ψηφίων. Η τράπεζα μπορεί να διανείμει αυτές τις ακολουθίες ψηφίων και να χρεώσει το λογαριασμό του αγοραστή με μια ανάληψη ίση με την αξία του συναλλάγματος που έχει εκδοθεί (κουπόνι – token). Η τράπεζα επικυρώνει το κάθε κουπόνι με την ψηφιακή της σφραγίδα πριν από την μετάδοση στον υπολογιστή του καταναλωτή. Όταν λοιπόν θέλετε να ξοδέψετε κάποια e-cash, πρέπει μόνο να μεταδώσετε το κατάλληλο ποσό κουπονιών στον έμπορο, ο οποίος με τη σειρά του τα

αναμεταδίδει στην τράπεζα για επικύρωση και εξαργύρωση. Για να διασφαλιστεί πως το κάθε κουπόνι χρησιμοποιείται μια μόνο φορά, η τράπεζα καταγράφει τον αύξοντα αριθμό του κάθε κουπονιού καθώς αυτό ξοδεύεται. Αν ο αύξοντας αριθμός του κουπονιού είναι ήδη καταγεγραμμένος στην βάση δεδομένων, η τράπεζα διαπιστώνει προσπάθεια εξαπάτησης, ενημερώνει τον έμπορο και ακυρώνει το κουπόνι.

Για εκείνους που επιθυμούν να διατηρήσουν την ανωνυμία τους υπάρχει η μέθοδος των «τυφλών υπογραφών» η οποία χρησιμοποιείται στο σύστημα που αναπτύχθηκε από την Digicash. Αυτή η μέθοδος επιτρέπει στον αγοραστή να προμηθευτεί e-cash από την τράπεζα χωρίς εκείνη να είναι σε θέση να συσχετίσει το όνομα του αγοραστή με τα κουπόνια που εκδίδει. Αυτό μοιάζει περισσότερο με τα κανονικά μετρητά, όπου σε κάθε νόμισμα που λαμβάνουμε από την τράπεζα δεν αναγράφεται το όνομα μας. Η τράπεζα πρέπει να αναγνωρίσει το κουπόνι μόλις το λάβει από τον έμπορο από την σφραγίδα πιστοποίησης που είναι συνυφασμένη με τα κουπόνια του αγοραστή, χωρίς όμως να μπορεί να αναγνωρίσει ποιος έκανε την πληρωμή.

Το κύριο ζήτημα γι' αυτά τα συστήματα είναι η ασφάλεια. Όμως το ερώτημα που τίθεται είναι αν είναι όντως απαραίτητη η ασφάλεια για κάθε κουπόνι που εκδίδεται ή μήπως το ποσό και η αξία αυτών των κουπονιών είναι τόσο μικρή που τα καθιστά ανάξια να τραβήξουν την προσοχή κάποιου επιτήδειου; Εντούτοις, πιο ισχυρές μέθοδοι κρυπτογραφίας μπορούν να διασφαλίσουν τις διαδικασίες του συστήματος.

Ένα άλλο σημαντικό πρόβλημα που αντιμετωπίζουν τα συστήματα αυτά σχετίζεται με την υποδομή καθώς κάθε τράπεζα εκδίδει τα δικά της κουπόνια που πιθανά δεν είναι συμβατά με τα συστήματα που χρησιμοποιούν κάποιες άλλες τράπεζες. Το γεγονός αυτό επηρεάζει κυρίως τις business-to-consumer εφαρμογές μιας για business-to-business εφαρμογές προτιμούνται τα EDI συστήματα.

Τα πρότυπα για την πραγματοποίηση χρηματικών συναλλαγών βρίσκονται ακόμα σε εξέλιξη, οπότε σε αυτό το στάδιο οι επιχειρήσεις μπορούν να επιλέξουν είτε να ακολουθήσουν τις μεθόδους των πρωτοπόρων στον τομέα αυτό, είτε να υποστηρίξουν περισσότερα του ενός συστημάτων πληρωμής.

Τα ψηφιακά μετρητά συνδυάζουν την άνεση των ηλεκτρονικών συναλλαγών με την ασφάλεια και την ανωνυμία που εξασφαλίζει η χρήση κοινών χαρτονομισμάτων. Η ευελιξία των ψηφιακών μετρητών μπορεί να ανοίξει τον δρόμο για ένα μεγάλο αριθμό νέων αγορών και νέων εφαρμογών. Τα ψηφιακά μετρητά σκοπεύουν να αντικαταστήσουν τα συμβατικά μετρητά ως το κύριο μέσο πληρωμής ηλεκτρονικών συναλλαγών. Όσο και αν φαίνεται παράξενο, μετά από τριάντα χρόνια εξέλιξης των συστημάτων ηλεκτρονικής πληρωμής, τα μετρητά εξακολουθούν να είναι το μέσο πληρωμής που προτιμά η συντριπτική πλειοψηφία των καταναλωτών. Αυτό συμβαίνει για τρεις λόγους: (α) έλλειψη εμπιστοσύνης των καταναλωτών στο τραπεζικό σύστημα, (β) ασύμφοροι διακανονισμοί πληρωμής με άλλα μέσα εκτός από μετρητά, και (γ) πολύ χαμηλά επιτόκια καταθέσεων.

Οι τρεις αυτοί λόγοι για την προτίμηση των καταναλωτών στα μετρητά ως μέσο πληρωμής, φανερώνουν μια ανάγκη αναθεώρησης του τρόπου πραγματοποίησης συναλλαγών. Για να αντικατασταθούν τα μετρητά, τα συστήματα ηλεκτρονικών πληρωμών θα πρέπει να αποκτήσουν μερικές από τις θετικές ιδιότητες των μετρητών, που δεν έχουν σήμερα οι πιστωτικές και άλλες πλαστικές κάρτες. Για παράδειγμα, τα

μετρητά είναι μεταβιβάσιμα και μπορούν να χρησιμοποιηθούν ανεξάρτητα από το πρόσωπο του κατόχου τους. Τα μετρητά αποτελούν επίσημη αξία, δηλαδή ο πωλητής είναι υποχρεωμένος να τα δεχθεί ως μέσο πληρωμής. Τα μετρητά είναι απρόσωπα, δηλαδή ο κομιστής αναγνωρίζεται αυτόματα ως κάτοχος. Τα μετρητά δεν προϋποθέτουν την ύπαρξη τραπεζικού λογαριασμού για τη χρήση τους. Τέλος, τα μετρητά απαλλάσσουν τον αποδέκτη από κάθε κίνδυνο: η πληρωμή ολοκληρώνεται τη στιγμή της ανταλλαγής.

Οι πιστωτικές και άλλες κάρτες έχουν σημαντικούς περιορισμούς σε σύγκριση με τη χρήση μετρητών. Πρώτον, δεν μεταβιβάζονται, καθώς αποτελούν μέσο αναγνώρισης, παραμένουν στην ιδιοκτησία του πιστωτικού ιδρύματος (π.χ. τράπεζα) που τις έχει εκδώσει και μπορούν να χρησιμοποιηθούν μόνο από ένα πρόσωπο. Δεύτερον, δεν αποτελούν επίσημη αξία (χρήμα), και ο πωλητής έχει δικαίωμα να μην τις δεχθεί ως μέσο πληρωμής. Τρίτον, για τη χρήση τους απαιτείται η ύπαρξη τραπεζικού λογαριασμού ή / και η έγκριση της συναλλαγής από το πιστωτικό ίδρυμα. Από την άλλη πλευρά, η χρήση επιταγών προϋποθέτει την προσωπική γνώριμια αυτού που πληρώνει, ή τη μεσολάβηση ενός οργανισμού που εγγυάται την κάλυψη των επιταγών. Για να πετύχει ένα νέο σύστημα ηλεκτρονικών πληρωμών θα πρέπει να προσφέρει κάτι περισσότερο από την ευκολία της χρήσης πιστωτικών καρτών. Τα ψηφιακά μετρητά θα πρέπει να έχουν μερικές από τις ιδιότητες των συμβατικών μετρητών.

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

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

- **Πληρωμές μεταξύ ομοτίμων:** η μεγάλη επιτυχία των ηλεκτρονικών δημοπρασιών στο διαδίκτυο οδήγησε και στην δημιουργία συστημάτων πληρωμών προσαρμοσμένων στις ανάγκες των συμμετεχόντων. Ειδικότερα, αναπτύχθηκαν συστήματα που στόχο είχαν να παρέχουν την δυνατότητα σε χρήστες του Διαδικτύου να πραγματοποιούν απευθείας συναλλαγές χωρίς την μεσολάβηση κάποιου χρηματοπιστωτικού οργανισμού. Τα συστήματα πληρωμών μεταξύ ομοτίμων λειτουργούν κατά βάση όπως οι τράπεζες καθώς οι πελάτες ανοίγουν λογαριασμούς σε παροχείς υπηρεσιών πληρωμών όπου καταθέτουν χρηματικά ποσά. Η βασική καινοτομία προέρχεται από το γεγονός ότι τα συστήματα αυτά χρησιμοποιούν τις ηλεκτρονικές διευθύνσεις των δικαιούχων καθώς και τον δικτυακό τόπο της εταιρείας υπηρεσιών πληρωμών προκειμένου να συνεννοηθούν τα μέρη για την συναλλαγή¹⁹. Επιπλέον, η απόκτηση λογαριασμού είναι πιο εύκολη απ' ό,τι στον πραγματικό κόσμο.

Ειδικότερα, ένας οποιοσδήποτε χρήστης του Διαδικτύου μπορεί να προβεί σε απευθείας πληρωμές εφόσον εγγραφεί στο σύστημα του παροχέα που προσφέρει την υποδομή για τις συναλλαγές αυτές. Η εταιρεία ζητά συνήθως από τους πελάτες της να πραγματοποιήσουν κατάθεση σε τραπεζικό λογαριασμό της εταιρείας χρησιμοποιώντας κάποιο παραδοσιακό μέσο πληρωμής όπως η πιστωτική κάρτα ή η επιταγή. Με την πραγματοποίηση της κατάθεσης ο πελάτης αποκτά ηλεκτρονικό λογαριασμό στην εταιρεία ο οποίος είναι πιστωμένος με το ποσό που κατέθεσε. Όταν θέλει να πραγματοποιήσει την πληρωμή ο κάτοχος του λογαριασμού συνδέεται με το σύστημα του παροχέα ηλεκτρονικών πληρωμών και δίνει εντολή μεταφοράς χρημάτων. Ο παροχέας απλά μεταφέρει τα ποσά από τον ένα λογαριασμό στον άλλο. Το σύστημα χρησιμοποιεί τις ηλεκτρονικές διευθύνσεις των δικαιούχων για την πιστοποίηση τους ενώ τα στοιχεία της συναλλαγής αποστέλλονται στους δικαιούχους μέσω ηλεκτρονικού ταχυδρομείου.

Το βασικό πλεονέκτημα αυτού του συστήματος πληρωμών είναι ότι υποστηρίζει διεθνείς συναλλαγές ενώ δεν απαιτείται ειδικός εξοπλισμός όπως κάρτες ή τερματικά για την χρήση του. Επιπλέον δεν παρακρατείται προμήθεια από τον παροχέα με αποτέλεσμα να είναι φθηνότερη λύση για τους καταναλωτές.

- **Προπληρωμένες κάρτες:** πρόκειται για κάρτες που είναι δυνατόν να αγοραστούν από περίπτερα ή καταστήματα και περιέχουν μονάδες ανάλογα με την τιμή αγοράς τους. Η κάρτα περιέχει ένα κωδικό που αποκαλύπτεται αφού αφαιρεθεί η ειδική επίστρωση από τον κάτοχο της. Οι λογαριασμοί με τα προπληρωμένα ποσά είναι αποθηκευμένοι σε ένα ειδικό διακομιστή και έτσι δεν απαιτείται αποθήκευση του ποσού στον υπολογιστή του χρήστη ή σε έξυπνη κάρτα.

Οι προπληρωμένες κάρτες χρησιμοποιούνται κυρίως για την διεκπεραίωση συναλλαγών μικρής αξίας στο διαδίκτυο. Επιπλέον έχουν το πλεονέκτημα ότι προστατεύουν την ανωνυμία του κατόχου καθώς δεν απαιτείται προεγγραφή σε κάποιο τρίτο μέρος ή χρήση τραπεζικού λογαριασμού.

¹⁹ European Central Bank E-payments in Europe – The eurosystem's perspective. Issue Paper available at www.ecb.int.

Οι προπληρωμένες πιστωτικές κάρτες αποτελούν ένα καινούργιο προϊόν των χρηματοπιστωτικών ιδρυμάτων, που αποσκοπεί στην ενθάρρυνση των οικονομικών συναλλαγών μέσω Διαδικτύου. Η φιλοσοφία των εν λόγω καρτών συνοψίζεται στο ότι ο χρήστης που θέλει να πραγματοποιήσει online αγορές προμηθεύεται από κάποιο τραπεζικό κατάστημα την κάρτα προκαταβάλλοντας την αξία της. "Αγοράζει" δηλαδή κάποιο ποσό, το οποίο και μπορεί να χρησιμοποιήσει για ηλεκτρονικές αγορές με την κάρτα, χωρίς διατυπώσεις και χωρίς την ύπαρξη τραπεζικού λογαριασμού. Η διαδικασία απόκτησης και χρήσης αυτού του είδους καρτών είναι παρόμοια με τη διαδικασία απόκτησης και χρήσης μιας τηλεφωνικής κάρτας (τηλεκάρτας, χρονοκάρτας κ.λπ.) και έτσι ακόμη και ένας ανήλικος μπορεί να τις αποκτήσει και να τις χρησιμοποιήσει.

Μέχρι στιγμής, οι προπληρωμένες κάρτες που διατίθενται στην ελληνική αγορά είναι δύο: Η egnatiaPrepay, από την Εγνατία Τράπεζα, και η Attica Gift Card Visa, από την Τράπεζα Αττικής, χωρίς να αποκλείεται σύντομα και άλλες τράπεζες να παρουσιάσουν κάποιο αντίστοιχο προϊόν. Ειδικότερα, η egnatiaPrepay κοστίζει 100 € και επιτρέπει στον κάτοχό της να προβεί σε συνολικές αγορές ισόποσης αξίας, στα περίπου 20 ελληνικά ηλεκτρονικά καταστήματα, που κάνουν δεκτό (μέχρι τώρα) το συγκεκριμένο τρόπο πληρωμής. Εννοείται ότι ο ενδιαφερόμενος, για να ικανοποιήσει τις ανάγκες του, μπορεί να αγοράσει περισσότερες από μία κάρτες. Το κόστος της Attica Gift Card Visa ξεκινά από τα 50 € και φθάνει μέχρι και τα 3.000 € (πλέον μικρής τραπεζικής προμήθειας που βαρύνει τον αγοραστή της κάρτας) και επιτρέπει στον κάτοχό της την πραγματοποίηση αγορών ισόποσης αξίας σε όλα τα e-shop της Ελλάδας και του εξωτερικού που δέχονται πιστωτικές κάρτες τύπου Visa. Ουσιαστικά πρόκειται για μία πιστωτική Visa, με προκαθορισμένο από τον πελάτη χρηματικό απόθεμα.

Οι κάρτες αυτές καλύπτουν ένα σημαντικό κενό στο χώρο των ηλεκτρονικών συναλλαγών, γιατί επιτρέπουν στον Έλληνα χρήστη να απολαύσει όλα τα θετικά που συνοδεύουν τη χρήση πιστωτικών καρτών, επιλέγοντας εκείνος το χρηματικό ποσό που θα κεφαλαιοποιήσει στην κάρτα του και χωρίς καμία τραπεζική δέσμευση. Πολύ περισσότερο, ακόμα και αν η κάρτα χαθεί ή υποκλαπούν τα στοιχεία της, το μόνο που μπορεί να απολέσει ο κάτοχος είναι το ποσό της κάρτας. Αν, έστω χάσει κανείς την egnatiaPrepay, δεν πρόκειται να ζημιωθεί περισσότερο από την ονομαστική αξία (100 €).

Τα μειονεκτήματα του πρακτικού αυτού τρόπου πληρωμής είναι ελάχιστα. Για την κάρτα της Τράπεζας Εγνατία, το πρόβλημα εστιάζεται κυρίως στο ότι ο πελάτης μπορεί να πραγματοποιήσει τις αγορές του μόνο στα περίπου 20 εγχώρια ηλεκτρονικά καταστήματα που κάνουν αποδεκτή τη συγκεκριμένη κάρτα. Το γεγονός αυτό περιορίζει κάπως τους χρήστες και ενδεχομένως να λειτουργεί αποτρεπτικά. Πάντως, αφενός τα e-shops που αποδέχονται την egnatiaPrepay καλύπτουν μεγάλη προϊοντική γκάμα, αφετέρου αυξάνονται συνεχώς. Για την κάρτα της Τράπεζας Αττικής, το μόνο αρνητικό εστιάζεται στην προμήθεια που παρακρατά η τράπεζα (περίπου 1,5%) για την παροχή της κάρτας, καθώς και στα διαχειριστικά έξοδα που θα χρεωθεί ο κάτοχος εάν επιστρέψει την κάρτα χωρίς να έχει εξαντλήσει το πιστωτικό υπόλοιπο.

Στον πίνακα που ακολουθεί επιχειρείται μία συνοπτική σύγκριση των έξι βασικότερων κατηγοριών συστημάτων ηλεκτρονικών πληρωμών με βάση χαρακτηριστικά που εντοπίστηκαν στην βιβλιογραφία. Στόχος αυτής της σύγκρισης είναι η εποπτική παρουσίαση των βασικότερων πλεονεκτημάτων και μειονεκτημάτων κάθε συστήματος ηλεκτρονικών πληρωμών.

Κριτήριο	Πιστωτική κάρτα	Πιστωτική κάρτα	Πιστωτική κάρτα	Πιστωτική κάρτα	Πιστωτική κάρτα	Πιστωτική κάρτα
Πραγματικός χρόνος πληρωμής	Εξ των υστέρων πληρωμή	Γραπτόγραμμα	Εξ των υστέρων πληρωμή	Γραπτόγραμμα	Πίνακας τη στιγμή της αγοράς	Εξ των υστέρων πληρωμή
Μεθόδωση πληροφορίας για την συναλλαγή	Το κατάστημα και η τράπεζα ελέγχουν την ακεραιότητα της πιστωτικής κάρτας	Ελεύθερη απόσπασή. Οι συναλλαγές δει είναι τραπεζοαποδοτικές	Απαιτείται υπογραφή των πληρωστών στοιχείων	Ο έμπορος κάρτας και των δύο μερών πραγματοποιούν την μεσοσάση πληρωσάση	Ο πωστήρας επιδεικνύει το στοιχεία των συναλλαγών	Η τράπεζα
Online / offline συναλλαγές	Online	Online	Επιτόκισμα offline συναλλαγές	Επιτόκισμα offline συναλλαγές	Online	Online
Χρήση τραπεζικού λογαριασμού	Χρησιμοποιείται ο λογαριασμός της πιστωτικής κάρτας	Καμία χρήση	Απαιτείται χρήση τραπεζικού λογαριασμού	Χρησιμοποιείται ο λογαριασμός της έμπορος κάρτας	Απαιτείται χρήση τραπεζικού λογαριασμού	Απαιτείται χρήση τραπεζικού λογαριασμού
Χρήστες	Κάθε έμπορος πιστωτικής κάρτας	Οποσδήποτε	Οποσδήποτε έμπορος τραπεζικού λογαριασμού	Οποσδήποτε έμπορος τραπεζικού λογαριασμού ή πιστωτικής κάρτας	Οποσδήποτε έμπορος τραπεζικού λογαριασμού	Οποσδήποτε έμπορος τραπεζικού λογαριασμού
Κίνδυνος για τον καταναλωτή	Η τράπεζα επιβάλλει το μεγαλύτερο μέρος του κινδύνου. Ο καταναλωτής αναλαμβάνει μόνο ένα μέρος του κινδύνου	Ο καταναλωτής αναλαμβάνει το κίνδυνο από κλοπή, απώλεια ή κακή χρήση του ηλεκτρονικού χρήματος	Ο καταναλωτής αναλαμβάνει το μεγαλύτερο μέρος του κινδύνου ενόσω μπορεί να «κλείσει» τις πληρωμές οποσδήποτε στιγμή	Ο καταναλωτής αναλαμβάνει το κίνδυνο από κλοπή, απώλεια ή κακή χρήση της έμπορος κάρτας	Ο καταναλωτής αναλαμβάνει το μεγαλύτερο μέρος του κινδύνου ενόσω μπορεί να «κλείσει» τις πληρωμές οποσδήποτε στιγμή	Ο καταναλωτής αναλαμβάνει το μεγαλύτερο μέρος του κινδύνου ενόσω μπορεί να «κλείσει» τις πληρωμές οποσδήποτε στιγμή
Δημοσιότητα	Είναι δυνατή η χρήση τους άθελά να στα είναι πολύ δημοφιλής τσέκας πληρωμής	Όχι άθελά δημοφιλής τσέκας ένα σημαντικό μέρος περιορισμούς στη χρήση τους	Μη δημοφιλής μέσο	Η χρήση του θεωρείται άθελά να στα είναι πολύ δημοφιλής τσέκας πληρωμής	Η χρήση τους θεωρείται άθελά να στα είναι πολύ δημοφιλής τσέκας πληρωμής	Χρησιμοποιείται για διάφορα πληρωμές και στην πιστωτική κάρτα δεν είναι τόσο δημοφιλής στην αμερική
Ανωνυμία	Μερικές ή ολικής ανώνυμη συναλλαγή	Πλήρης ανωνυμία	Επιτόκισμα συναλλαγή	Πλήρης ανωνυμία επιτόκισμα ή Κεντρική τράπεζα επιτόκισμα μπορεί να θητήρα από το καταστήματα πληροφορίας για τον καταναλωτή	Επιτόκισμα συναλλαγή	Επιτόκισμα συναλλαγή
Ποσά μικρής αξίας	Το κόστος της συναλλαγής είναι υψηλό και δεν ενθαρρύνεται να ποσά μικρής αξίας	Χαμηλό κόστος συναλλαγών, βολικό για ποσά μικρής αξίας	Επιτόκισμα στα πιστωτικά να αυσκουρύνει ποσά μικρά ένα όρα προτού γίνει η πληρωμή. Κατάλληλο για ποσά μικρής αξίας	Επιτόκισμα στα πιστωτικά να αυσκουρύνει ποσά μικρά ένα όρα προτού γίνει η πληρωμή. Κατάλληλο για ποσά μικρής αξίας	Δεν υπάρχει περιορισμός στο ποσά της πληρωμής	Δεν υπάρχει περιορισμός στο ποσά της πληρωμής
Αληθινός / εικονικός κόσμος	Σε ορισμένες πιστωτικές χρησιμοποιείται να στην πιστωτική κάρτα	Χρήση μόνο στον εικονικό κόσμο	Χρήση στον εικονικό κόσμο, ο λογαριασμός ένας μέρος να σάββα και κανονικές απεικονίσεις	Αληθινός και εικονικός κόσμος	Χρήση μόνο στον εικονικό κόσμο	Αληθινός και εικονικός κόσμος
Περιορισμοί στη μεταφορά χρηματικών ποσών	Εξαρτάται από το όρα της πιστωτικής κάρτας	Εξαρτάται από το ποσά που προληφθεί	Κανόνες περιορισμός	Εξαρτάται από την ποσότητα χρήματος που έχει αποθηκευθεί	Εξαρτάται από το ποσά που διαθέτει ο τραπεζικός λογαριασμός	Εξαρτάται από το ποσά που διαθέτει ο τραπεζικός λογαριασμός
Κινητικότητα	Ναι	Όχι	Όχι	Ναι		

Πίνακας 6: Σύγκριση συστημάτων ηλεκτρονικών πληρωμών (Προσαρμογή από Yu et al 2002)

20 Καθώς η λειτουργία και τα χαρακτηριστικά των χρεωστικών καρτών μοιάζουν με αυτά των πιστωτικών δεν περιλήφθηκαν και οι χρεωστικές κάρτες στον πίνακα.

4.3 ΚΙΝΗΤΕΣ ΠΛΗΡΩΜΕΣ (MOBILE PAYMENTS)

"Στο κινητό ηλεκτρονικό εμπόριο (M-commerce) γίνεται χρήση ασύρματων συναλλαγών για την παροχή υπηρεσιών που στηρίζονται στην εκάστοτε θέση καθώς και στο συγκεκριμένο προφίλ χρηστών κινητών συσκευών υψηλής ταχύτητας και ασύρματων δικτύων ανά τον κόσμο. Η πραγματοποίηση συναλλαγών όπως κρατήσεις ξενοδοχείων, εισιτηρίων, αγορές προϊόντων με χρήση κινητού τηλεφώνου ή άλλης συσκευής θα αποτελέσει τον κυρίαρχο τρόπο για την ολοκλήρωση όμοιων ενεργειών στην 3G εποχή"

Πριν αναφερθεί η σχέση της κινητής τεχνολογίας με το ηλεκτρονικό εμπόριο ίσως θα έπρεπε να δοθεί ένας ορισμός, επεξήγηση του όρου ηλεκτρονικό εμπόριο:

"Ως Ηλεκτρονικό εμπόριο (E-commerce) ορίζεται η διεκπεραίωση οικονομικών συναλλαγών με χρήση ηλεκτρονικών μέσων. Λόγω της ραγδαίας ανάπτυξης του εμπορίου στο Internet, το ηλεκτρονικό εμπόριο συχνά αναφέρεται σε αγορές από on-line καταστήματα του Διαδικτύου, που είναι γνωστά ως δικτυακοί τόποι ηλεκτρονικού εμπορίου, εικονικά καταστήματα, ή καταστήματα του κυβερνοχώρου". (http://www.straight-on.com/ecommerce_definition.html)

Παρ' όλα αυτά ο όρος ηλεκτρονικό εμπόριο δεν θα έπρεπε να συνδεθεί αποκλειστικά με την ύπαρξη μιας ιστοσελίδας όπου είναι δυνατή η πραγματοποίηση αγορών. Περιλαμβάνει κάθε είδος ηλεκτρονική επικοινωνία μέσω της οποίας μπορεί ο πελάτης να αναζητήσει κάποιο προϊόν που τον ενδιαφέρει και να πραγματοποιήσει μια συναλλαγή. Επιπλέον λόγω της ταχύτητας ανάπτυξης της τεχνολογίας και των καλύτερων και αποδοτικότερων συστημάτων έγινε δυνατή η ασύρματη επικοινωνία πελατών που βρίσκονται σε κίνηση με τους δικτυακούς τόπους ακόμα και μέσω συσκευών που καταλαμβάνουν ελάχιστο χώρο και δεν αποτελούν βάρος για τον πελάτη όπως είναι οι συσκευές κινητής τηλεφωνίας.

Με την εμφάνιση και ραγδαία διάδοση της κινητής τηλεφωνίας εμφανίστηκε ένας σημαντικός αριθμός πρωτοβουλιών για πληρωμές μέσω κινητού τηλεφώνου. Στην ανάληψη τέτοιων πρωτοβουλιών συνέβαλε φυσικά και η απότομη πτώση των εταιρειών ηλεκτρονικού εμπορίου στις αρχές του 2000 που οδήγησε πολλούς οργανισμούς να στραφούν προς την εκμετάλλευση της υπάρχουσας τεχνολογίας, σε άλλους χώρους ώστε να αυξήσουν την κερδοφορία τους. Στην προσπάθειά τους αυτή δεν θα μπορούσαν να αγνοήσουν τους περίπου ένα δισεκατομμύριο χρήστες κινητών τηλεφώνων ανά τον κόσμο το 2002, σύμφωνα με τον παγκόσμιο οργανισμό κινητής τηλεφωνίας (UMTS). Σύμφωνα με έρευνα του διεθνούς οίκου Forester (2001)²¹, το 2005 υπολογίζεται ότι οι κινητές ηλεκτρονικές πληρωμές στην Ευρώπη θα φτάσουν στο μέγεθος των 26 δισεκατομμυρίων Ευρώ.

Σύμφωνα με το επιχειρηματικό μοντέλο που αναπτύσσει η Ernst & Young (2002)²² συνήθως αναγνωρίζονται οι παρακάτω συμμετέχοντες στην αγορά αγαθών και υπηρεσιών μέσω κινητού: ο παροχέας περιεχομένου (content provider), ο παροχέας

21 De Lussanet, M., Nordan, M.M., Siepermann, M. & Bedarida, D.E. (May 2001). Mobile payments slow start. Techstrategy Report. Διαθέσιμο στο

22 Buchanan, D. Cheong, Y. C. and Tan Cheng-Lin, (2002) Mobile payments in M-Commerce, Gap Gemini Ernst & Young

- Ψηφιακά αγαθά (MP3, ringtones, ή πληροφορία επιπλέον αξίας, όπως παρακολούθηση των τιμών των μετοχών στο χρηματιστήριο κ.α.)
- Παραδοσιακά αγαθά (αγορά τηλεόρασης, DVD κλπ.)
- Ψηφοφορίες (ψηφός σε ένα τηλεπαιχνίδι)
- Αγορά εισιτηρίων (κινηματογράφου, θεάτρου κλπ.)

Επίσης αναλόγως του περιεχομένου της αγοράς χωρίζονται σε μικρο και μεγάλο πληρωμές. Συνήθως το διαχωριστικό όριο αξίας του αγαθού είναι το ποσό των 10 Ευρώ. Η κεντρική τράπεζα της Φινλανδίας σε έκθεση της, το 2003²³, κάνει μία αναφορά στα πιο διαδεδομένα συστήματα το PAYBOX (<http://www.paybox.net>) το οποίο εφαρμόστηκε αρχικά στη Γερμανία και αργότερα υιοθετήθηκε από την Αυστρία, την Ισπανία, τη Σουηδία και το Ηνωμένο Βασίλειο. Η υπηρεσία αυτή επιτρέπει στους καταναλωτές να προβούν στην αγορά αγαθών και υπηρεσιών μέσω του κινητού τους τηλεφώνου και στην μεταφορά χρημάτων μέσω τραπεζικών λογαριασμών.

Μία άλλη εφαρμογή αρκετά διαδεδομένη στην Ισπανία αναφέρεται να είναι το MOBIPAY (<http://www.mobipay.com>). Το σύστημα αυτό χρησιμοποιείται για αγορές αγαθών και υπηρεσιών, αλλά ακόμη και για πληρωμή υπηρεσιών μεταξύ φυσικών προσώπων, αλλά και για εξόφληση λογαριασμών. Τέλος το σύστημα Payex (<http://www.payex.no>) είναι αρκετά διαδεδομένο στη Νορβηγία. Οι καταναλωτές ανοίγουν ένα λογαριασμό στο σύστημα Payex και μετά βάζουν χρήματα σε αυτόν ώστε να προβούν στην αγορά αγαθών και υπηρεσιών μέσω της συσκευής τους

Είναι εμφανές ότι είναι πλέον δύσκολος ο διαχωρισμός και η κατηγοριοποίηση των υπηρεσιών που προσφέρονται για αγορές μέσω του Διαδικτύου και για αγορές μέσω ενός κινητού τηλεφώνου. Στην πραγματικότητα χρησιμοποιούνται παραδοσιακές υπηρεσίες μέσω καινούριων μέσων, συσκευών. Για παράδειγμα οι πιστωτικές κάρτες και πολλές τραπεζικές υπηρεσίες χρησιμοποιούνται για αγορές είτε μέσω του Διαδικτύου, είτε μέσω συσκευών κινητής τηλεφωνίας παράλληλα με τον παραδοσιακό τρόπο. Άρα στην ουσία μιλάμε για νέα κανάλια παροχής υπηρεσιών. Ενδιαφέρον θα είναι να παρακολουθήσουμε όμως ποιο από τα εναλλακτικά αυτά κανάλια θα χρησιμοποιηθεί ευρέως από τους καταναλωτές. Θα υπερτερήσουν τελικά τα νέα τεχνολογικά κανάλια πραγματοποίησης συναλλαγών έναντι των παραδοσιακών; Το ερώτημα για το αν έχουν αποδώσει κέρδη όλες αυτές οι επενδύσεις στην τεχνολογία, όπως για παράδειγμα στην τεχνολογική υποδομή που χρειάζεται για να υποστηρίξει κινητά τηλέφωνα τρίτης γενιάς, θα παραμείνει αναπάντητο, τουλάχιστον για το πρώτο μισό της δεκαετίας που διανύουμε.

23 Jyrkonen, H. and Paunonen H. (2003). Card Internet and Mobile Payments. Bank of Finland Discussion Papers No 8-2003. Central Bank of Finland.

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

Πίνακας 7:Παροχή υπηρεσιών μέσω κινητού τηλεφώνου

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.

Ξεκινώντας από την Ιαπωνία μετά το 1998 η ιδέα της χρήσης των κινητών τηλεφώνων για λειτουργίες πέρα της απλής επικοινωνίας επεκτάθηκε μέσα στο 2000 στις Η.Π.Α. και κατόπιν κερδίζει συνεχώς έδαφος σε όλο τον κόσμο.

Όμως, η επιτυχία των υπηρεσιών αυτών θα εξαρτηθεί από το πόσο ικανές θα αποδειχθούν οι εταιρίες στο να δημιουργήσουν εθιστικό περιεχόμενο, στον τομέα της ψυχαγωγίας, των υπηρεσιών ή της πληροφόρησης που θα ωθεί τους χρήστες να χρησιμοποιούν συχνά τις συσκευές τους.

Παραδείγματα αποτελούν τα on-line παιχνίδια μεταξύ χρηστών, οι διαγωνισμοί και ψηφοφορίες και οι δημοπρασίες.

Καθώς η αγορά θα ωριμάζει, τράπεζες, έμποροι και παροχείς υπηρεσιών θα μπορέσουν να διακρίνουν ποιες υπηρεσίες και προϊόντα είναι πιο δημοφιλή με τους πελάτες χωρίς βέβαια αυτό να σημαίνει πως θα υπάρχει αρχικά αξιόλογο κέρδος από τις συναλλαγές κινητού ηλεκτρονικού εμπορίου.

Οι επιχειρήσεις θα έχουν διαφορετικές απόψεις για το αν μπορούν να πείσουν τους χρήστες να πληρώσουν για κάποια υπηρεσία και η διαφορά αυτή θα εντείνεται από μια χώρα σε άλλη με ανάλογο πολιτισμικό και κοινωνικό υπόβαθρο. Οι εφαρμογές που θα εξοικονομούν χρήματα και χρόνο για τον χρήστη θα είναι αυτές που θα μπορέσουν να ανταγωνιστούν τις υπάρχουσες πρακτικές.

Παρά το γεγονός ότι ένας αριθμός από αυτές έχουν ήδη σημειώσει επιτυχία σε άλλους τομείς τίποτα δεν βεβαιώνει ότι θα μπορούν να λειτουργήσουν εξίσου καλά στο περιβάλλον του κινητού ηλεκτρονικού εμπορίου.

Για παράδειγμα η πιλοτική εφαρμογή το 1999 των Barclaycard και BT Cellnet για μηχανές ηλεκτρονικού χρήματος που επέτρεπε στους χρήστες να "κατεβάσουν" ηλεκτρονικό χρήμα (e-cash) εισάγοντας την πιστωτική τους κάρτα Barclaycard σε ένα ειδικά σχεδιασμένο κινητό τηλέφωνο, απέτυχε να ικανοποιήσει σημαντικά κριτήρια επιτυχίας. Η υπηρεσία ήταν πολύπλοκη, χρονοβόρα και χωρίς το απαραίτητο επίπεδο ασφάλειας.

Σύμφωνα με μια άποψη λίγοι προμηθευτές θα καταφέρουν να κερδίσουν χρήματα από το κινητό ηλεκτρονικό εμπόριο, τουλάχιστον τον πρώτο καιρό. Οι καταναλωτές θα απογοητευτούν διαπιστώνοντας ότι οι αγαπημένες τους δικτυακές εφαρμογές δεν μπορούν να συμπιεστούν ώστε να λειτουργούν εξίσου καλά στα μικρά τερματικά που χρησιμοποιούνται στην κινητή τεχνολογία.

Δεδομένης όμως της τεράστιας διάδοσης της κινητής τηλεφωνίας και των δυνατοτήτων που δημιουργούνται για ανάπτυξη και εμπόριο βεβαιώνεται η ανάγκη για επένδυση στον συγκεκριμένο τομέα διακίνησης προϊόντων. Πρέπει όμως να προσφερθούν ανταγωνιστικές λύσεις με ορατό πλεονέκτημα έναντι των ήδη καθιερωμένων εναλλακτικών και να προωθηθούν στους πιθανούς χρήστες.

4.3.1 Από το ηλεκτρονικό στο κινητό εμπόριο

Ποιες όμως είναι οι διαφορές μεταξύ του ηλεκτρονικού και του κινητού εμπορίου; Ρωτώντας το διαφορετικά, ποια είναι τα ιδιαίτερα στοιχεία και πλεονεκτήματα του κινητού εμπορίου τα οποία οδηγούν ολοένα και περισσότερες εταιρείες στην υιοθέτησή του;

ΚΙΝΗΤΟ ΕΜΠΟΡΙΟ	ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ	ΟΦΕΛΟΣ
Ενεργητική προσέγγιση: τα μηνύματα καταλήγουν στον κάτοχο της συσκευής ο οποίος ειδοποιείται τις περισσότερες φορές πρακτικά και άμεσα	Τα μηνύματα καταλήγουν στον e-mail server και -ανάλογα με τη χρήση του διαδικτύου και την προσβασιμότητα σε Η/Υ - ο παραλήπτης μπορεί να τα λάβει ακόμη και μετά την πάροδο εβδομάδων	Άμεση «παραλαβή» του μηνύματος και αύξηση πιθανότητας επιθυμητής ενέργειας (π.χ. αγοράς ενός προϊόντος)
Ο πάροχος κινητής τηλεφωνίας γνωρίζει ανά πάσα στιγμή τη γεωγραφική θέση ενός μοναδικού και αναγνωρίσιμου προσώπου	Η τοποθεσία του χρήστη δεν μπορεί να είναι γνωστή και επιπλέον πολλοί χρήστες του διαδικτύου δίνουν ανακριβή ή και μη αληθή στοιχεία	Καλύτερη στόχευση στο επιθυμητό κοινό με γεωγραφικά ΚΑΙ δημογραφικά κριτήρια
Το κινητό τηλέφωνο στην Ελλάδα είναι μαζικό μέσο επικοινωνίας ¹	Η πρόσβαση στο διαδίκτυο, αν και με αυξητικές τάσεις, δεν καλύπτει ακόμη την πλειονότητα του πληθυσμού	Μεγαλύτερο κοινό
Η κατοχή του κινητού τηλεφώνου εκτείνεται στο μεγαλύτερο μέρος του 24ώρου	Ο χρήστης έχει επαφή με τον υπολογιστή λιγότερες ώρες μέσα στην ημέρα	Μεγαλύτερο χρονικό πεδίο για αποστολή μηνυμάτων

Πίνακας 8: Σύγκριση Κινητού-Ηλεκτρονικού Εμπορίου

Μερικές ακόμη μοναδικές ιδιότητες της κινητής τηλεφωνίας σαν μέσο επικοινωνίας και προώθησης είναι οι παρακάτω:

- Το 94% των εισερχομένων μηνυμάτων διαβάζονται και το 23% προωθείται σε φίλους (Enpocket Insight Report 2003)
 - Το μέσο ποσοστό ανταπόκρισης είναι 13% έναντι του 3.5% των άλλων μεθόδων άμεσου marketing
 - Μπορεί να χρησιμοποιηθεί ως αυτοτελές μέσο αλλά και σαν βοηθητικό εργαλείο στα παραδοσιακά μέσα προώθησης
 - Έχει χαμηλό κόστος
 - Τα αποτελέσματα είναι μετρήσιμα σε πραγματικό χρόνο και δίνουν τη δυνατότητα άμεσων αλλαγών για τη βελτίωση της κάθε ενέργειας προώθησης
- Όπως και με το ηλεκτρονικό εμπόριο, τα μηνύματα που αποστέλλονται μπορούν να έχουν εικόνα, ήχο stereo, και κίνηση

Στόχοι του Κινητού Εμπορίου

Οι στόχοι του Κινητού Εμπορίου είναι οι παρακάτω:

1. Χτίσιμο & ανάπτυξη πωλήσεων

α. Δοκιμή προϊόντος β. Αύξηση της συχνότητας αγοράς του προϊόντος γ. Αύξηση των πιστών πελατών

2. «Χτίσιμο» ονόματος (branding)
3. Υποστήριξη πελατών
4. Δημιουργία βάσης δεδομένων
5. Έρευνα αγοράς

Κινητό Εμπόριο και διαφήμιση

Εργαλεία προώθησης μέσω κινητού

Ας δούμε τώρα τα εργαλεία που χρησιμοποιεί το κινητό εμπόριο για να προωθήσει προϊόντα, υπηρεσίες και ιδέες για να πετύχει τους στόχους του:

1. **Υπηρεσίες με βάση τη γεωγραφική θέση του χρήστη.** Οι εφαρμογές με βάση τη γεωγραφική θέση του χρήστη έχουν να κάνουν

α. με προώθηση προϊόντων και υπηρεσιών που βρίσκονται κοντά στο χρήστη με μήνυμα που στέλνει ο πάροχος (με την έγκριση του χρήστη). Τα μηνύματα μπορεί να είναι του τύπου «προσφορά στα κινητά ΧΨΖ στο κατάστημα ΑΒΓ». Εξυπακούεται ότι το κατάστημα είναι πολύ κοντά στη θέση που βρίσκεται ο χρήστης. Μια πιο προχωρημένη εφαρμογή θα ήταν ο χρήστης να έχει δηλώσει κατηγορίες προϊόντων και υπηρεσιών για τις οποίες ενδιαφέρεται να λαμβάνει μηνύματα τη συγκεκριμένη χρονική περίοδο (π.χ. για κινητά τηλέφωνα)

β. με υπηρεσίες που προσφέρονται στο χρήστη ώστε αυτός να μπορεί να βρίσκει το κοντινότερο προϊόν ή υπηρεσία βάσει του που βρίσκεται (π.χ. το κοντινότερο φαρμακείο ή βενζινάδικο)

2. **Διαγωνισμοί.** Οι διαγωνισμοί συνήθως ζητούν τη σωστή απάντηση σε μια εύκολη ερώτηση ώστε να προσελκύσουν αρκετούς χρήστες, άρα και χρήματα μέσω των χρεώσεων των μηνυμάτων. Οι χρήστες μπορούν να λάβουν μέρος μία ή περισσότερες φορές και οι νικητές μπαίνουν σε κλήρωση για κάποιο έπαθλο. Αν η συμμετοχή στο διαγωνισμό προϋποθέτει αγορά κάποιου προϊόντος, πάνω στο οποίο ο καταναλωτής βρίσκει έναν αριθμό τον οποίο στέλνει με το κινητό του, τότε η ενέργεια ονομάζεται «on-pack» - επάνω δηλαδή στη συσκευασία.

3. **Κληρώσεις.** Η διαφορά τους από τους διαγωνισμούς είναι ότι δεν χρειάζεται να απαντηθεί κάποια ερώτηση. Ο χρήστης απλά στέλνει συνήθως όσες φορές θέλει το μήνυμα που του ζητά ο διαφημιζόμενος και έτσι αυξάνει τις πιθανότητές του να κληρωθεί για κάποιο έπαθλο. Και εδώ το μήνυμα μπορεί να είναι on-pack

4. **Κουπόνια.** Είναι ηλεκτρονικά κουπόνια – διαθέτουν ηλεκτρονικό bar-code- τα οποία προσφέρονται από εταιρείες που θέλουν να αυξήσουν τις πωλήσεις τους με προσφορές, και εξαργυρώνονται σε σημεία πώλησης όπως super markets, καταστήματα ηλεκτρικών ειδών, βιβλιοπωλεία κ.ά.

5. **Ειδοποιήσεις.** Ο χρήστης δίνει τη συγκατάθεσή του να δέχεται μηνύματα ειδοποίησης αφού δώσει μέσω κινητού ή σε κάποιο site συγκεκριμένες ημερομηνίες

κατά τις οποίες θέλει να τον ειδοποιούν. Τα συχνότερα παραδείγματα είναι αυτά για ειδοποιήσεις εορτών. Οι εταιρείες που μπορεί να χορηγούν αυτά τα μηνύματα είναι συνήθως ανθοπωλεία, βιβλιοπωλεία, ζαχαροπλαστεία, δισκοπωλεία, εταιρείες διοργάνωσης μουσικών και άλλων εκδηλώσεων κ.ά. Τα κινητά τρίτης γενιάς, τα οποία δίνουν τη δυνατότητα στους παρόχους να ξέρουν τη συγκεκριμένη τοποθεσία στην οποία βρίσκεται ο χρήστης, δίνουν τη δυνατότητα στους χρήστες να δέχονται ειδοποιήσεις ανάλογα με το που βρίσκονται (βλέπε και 1β: Υπηρεσίες με βάση τη γεωγραφική θέση του χρήστη). Για παράδειγμα, κάποιος χρήστης μπορεί να θέλει να λαμβάνει υπενθυμίσεις όταν βρίσκεται σε κάποιο συγκεκριμένο μέρος της Ελλάδας ή της Αττικής για να αγοράσει κάποιο τοπικό προϊόν

6. Υπηρεσίες. Υπηρεσίες σε μορφή ειδοποιήσεων μπορεί να περιλαμβάνουν μηνύματα σχετικά με πληροφόρηση (π.χ. άρθρα σχετικά με κάποιο θέμα, χρηματιστηριακές ειδοποιήσεις) αποτελέσματα αγώνων διασκέδαση / προσωπικά (ωροσκόπιο, εύρεση συντρόφου, προσφορές για κρατήσεις σε clubs, εστιατόρια, κ.ά)

7. Χορηγίες. Είναι ο ιδεώδης τρόπος ώστε μια εταιρεία να δημιουργήσει και να «τρέξει» μια εκστρατεία μέσω κινητού, έχοντας μια άλλη εταιρεία να αναλαμβάνει το λογαριασμό της εκστρατείας, ή ακόμη και των μηνυμάτων. Σε αντάλλαγμα, ο χορηγός βάζει τον λογότυπό του ή και μια πρόταση στο τέλος του μηνύματος που χορηγεί. Για παράδειγμα, ένα βιβλιοπωλείο μπορεί να χορηγεί μηνύματα σχετικά με νέες εκδόσεις βιβλίων, έχοντας το λογότυπό του και την ηλεκτρονική του διεύθυνση στο τέλος του μηνύματος.

8. Banners. Τα γνωστά banners του Διαδικτύου αλλά σε μέγεθος οθόνης κινητού, τα οποία μπορεί να ενεργοποιήσει ο χρήστης και να μεταβεί στην ειδικά διαμορφωμένη για κινητά σελίδα του διαφημιζόμενου.

9. Interstitials. Διαφήμιση η οποία εμφανίζεται σε όλη την οθόνη για μερικά δευτερόλεπτα ενώ ο χρήστης ψάχνει σε υπηρεσίες περιεχομένου. Οι τρόποι πληρωμής για τις χορηγίες, τα banners και τα interstitials είναι τρεις:

- Πάγιο τέλος ανά μήνα
- Τέλος βασισμένο στον αριθμό των εμφανίσεων των διαφημιστικών μηνυμάτων
- Τέλος βασισμένο στον αριθμό ενεργειών που θα κάνει ο χρήστης του κινητού (πόσοι χρήστες δηλαδή θα ακολουθήσουν το μήνυμα, θα μεταβούν στο site του διαφημιζόμενου, θα εξαργυρώσουν ένα κουπόνι, θα λάβουν μέρος σε διαγωνισμό, ή θα αγοράσουν το προϊόν)

10. Δημοσκοπήσεις. Μίνι ερωτηματολόγια για δημοσκοπήσεις οι οποίες συνήθως απσκοπούν στη συλλογή δημογραφικών στοιχείων

Παγίδες και κίνδυνοι του Κινητού Εμπορίου

Ας δούμε τώρα κάποιες παγίδες και κινδύνους τους οποίους μπορεί να κρύβει η προώθηση μέσω κινητών τηλεφώνων:

- Υπερβολικές χρεώσεις στον τελικό καταναλωτή, ειδικά αν οι χρεώσεις δεν είναι ξεκάθαρες σ' αυτόν
- Αποστολή μηνυμάτων χωρίς τη συγκατάθεση του χρήστη (spamming)

- Αποστολή μεγάλου αριθμού μηνυμάτων μέσα σε μία χρονική περίοδο
- Έλλειψη δημιουργικότητας και στερεότυπα μηνύματα
- Αυτοχρηματοδότηση εκστρατείας (ο καταναλωτής πληρώνει το μήνυμα που στέλνει ή / και αγοράζει κάποιο προϊόν για να στείλει σαν μήνυμα έναν αριθμό που βρίσκει μέσα στο πακέτο) χωρίς μια ελάχιστη προσφορά στον καταναλωτή
- Κακή χρονική στιγμή αποστολής μηνυμάτων
- Προσπάθεια εκμείευσης δημογραφικών στοιχείων (όνομα, διεύθυνση, εισόδημα
- Χρήση μηνυμάτων ή ενεργειών μόνο για αύξηση πωλήσεων

Όλα τα παραπάνω έχουν σαν αποτέλεσμα τον εκνευρισμό του αποδέκτη των μηνυμάτων, ο οποίος βέβαια δημιουργεί άσχημη εικόνα για την εταιρεία και την μάρκα. Εδώ πρέπει να σημειώσουμε πως ο εκνευρισμός μπορεί να προέλθει από την εταιρεία Α και να έχει επιπτώσεις και στην εταιρεία Β: αν η εταιρεία Α έχει κάνει κακή χρήση της δυνατότητάς της να προσεγγίσει τον χρήστη και τον έχει βομβαρδίσει σε διάστημα λίγων εβδομάδων με μηνύματα, ο καταναλωτής μπορεί να καταλήξει να μην επιθυμεί μηνύματα από καμιά εταιρεία στο κινητό του.

Υπηρεσίες προς τους πελάτες μέσω Κινητού Εμπορίου

1. Πληροφορίες. Οι χρήστες της κινητής τηλεφωνίας μπορούν να έχουν στο κινητό τους εκατοντάδες πληροφορίες σε δεκάδες θέματα, είτε δίνοντας μία «πάγια» εντολή του τύπου «ημερήσια ενημέρωση για τον καιρό στην Αθήνα» μέσω των δικτυακών πυλών για κινητά, είτε στέλνοντας ένα SMS ζητώντας μια συγκεκριμένη πληροφορία (π.χ. «ταινίες τρόμου»). Είναι σημαντικό να σημειώσουμε πως συνήθως οι χρήστες χρεώνονται για τις υπηρεσίες αυτές με κάποια πάγια χρέωση ανά μήνα βάσει του αριθμού των πληροφοριών που αναζητούν ή με χρέωση ανά μήνυμα (SMS / MMS).

2. Πληροφορίες καταλόγου. Εδώ μιλάμε για ένα χρυσό οδηγό στο κινητό του χρήστη, ο οποίος μπορεί να αναζητήσει προϊόντα και υπηρεσίες με βάση τον τόπο που βρίσκεται, το τι επιθυμεί ή τον συνδυασμό αυτών. Αν, για παράδειγμα, ο χρήστης βρίσκεται σε μια πόλη, μπορεί να εισάγει τον ταχυδρομικό κωδικό της περιοχής και να αναζητήσει εστιατόρια, βενζινάδικα, γιατρούς, τραπεζικά καταστήματα κλπ. Οι συνηθέστερες κατηγορίες είναι: ενημέρωση, καιρός, χρηματιστήριο, ταξίδια, αγορές, γνωριμίες, αθλητικά, χάρτες, διασκέδαση κ.ά. Ένα τέτοιο οδηγό μπορεί να βρει κανείς στη διεύθυνση <http://www.gps2.com>

3. Δικτυακές πύλες κινητών. Η όλη ιδέα γύρω απ' αυτές τις πύλες είναι ο χρήστης να «αποθηκεύσει» αλλά και να ανανεώνει τις προσωπικές του πληροφορίες και προτιμήσεις στην ιστοσελίδα της πύλης (κάτι όχι εύκολο, χρονοβόρο και με υψηλό κόστος για να γίνει μέσω του κινητού του). Οι πύλες αυτές δίνουν στους χρήστες λύσεις όπως e-mail, αποστολή και λήψη μηνυμάτων, έρευνα αγοράς, και διαχείριση προσωπικών πληροφοριών (ημερολόγιο, βιβλίο διευθύνσεων κλπ). Τα προσωπικά δεδομένα (ονοματεπώνυμο και διεύθυνση, ημερομηνία γέννησης, φύλο) και οι προτιμήσεις που καταχωρούν οι χρήστες (ενδιαφέροντα, επιθυμία να λαμβάνουν διαφημιστικά μηνύματα και για ποια προϊόντα, αριθμό μηνυμάτων ανά ημέρα ή εβδομάδα που θέλουν να δέχονται) βοηθούν τις εταιρείες που θέλουν να διαφημιστούν μέσα απ' αυτές τις πύλες ή και μέσω SMS & MMS να στοχεύσουν τα μηνύματά τους σε συγκεκριμένο κοινό με δηλωμένα ενδιαφέροντα.

4. Φωνητικές πύλες. Οι φωνητικές πύλες δίνουν ακόμη μεγαλύτερη ευελιξία στους χρήστες να χειριστούν το κινητό τους και να δώσουν εντολές αγοράς ή να κάνουν αναζητήσεις, ακόμη και όταν οδηγούν, όταν χειρίζονται τον ηλεκτρονικό υπολογιστή και γενικότερα όταν προσπαθούν να χρησιμοποιήσουν το κινητό τους κάνοντας ταυτόχρονα κάτι άλλο. Με τις φωνητικές πύλες, οι χρήστες μπορούν να δώσουν εντολές ώστε ν' ακούσουν το ωροσκόπιο τους, να δώσουν χρηματιστηριακές ή τραπεζικές εντολές, ν' ακούσουν το e-mail τους, ή πληροφορίες για τον καιρό ή την κυκλοφοριακή κατάσταση σε συγκεκριμένους δρόμους, ακόμη και για ν' αγοράσουν προϊόντα. Παραδείγματα λειτουργίας και πληροφορίες για φωνητικές πύλες μπορεί κανείς να βρει στις διευθύνσεις

5. Τραπεζικές εργασίες μέσω κινητού. Οι τράπεζες «ανακάλυψαν» το κινητό τηλέφωνο σαν μέσο επικοινωνίας με τους πελάτες τους για να δώσουν μια παραπάνω ευκολία στους πελάτες τους οι οποίοι μπορούν να εκτελέσουν πολλές τραπεζικές τους εργασίες απ' όπου κι αν βρίσκονται, οποιαδήποτε ώρα της ημέρας, και για να μειώσουν τα λειτουργικά τους κόστη, αφού ο πελάτης-χρήστης αυτοεξυπηρετείται χωρίς τη διαμεσολάβηση υπάλληλου και χωρίς τη χρήση εντύπων. Οι χρήστες μπορούν να δουν το υπόλοιπο του λογαριασμού τους, να κάνουν μεταφορά χρημάτων από ένα τραπεζικό λογαριασμό σε έναν άλλο, να δώσουν εντολή αγοράς ή πώλησης μετοχών, ή να λάβουν ηλεκτρονική απόδειξη κατάθεσης του μισθού τους. Πρόσφατα (2002) η τράπεζα Nordea (με πάνω από 2 εκατομμύρια χρήστες στην Φινλανδία, Σουηδία, Δανία και Νορβηγία) συνέπραξε με τη Nokia και τη Visa International ώστε να πραγματοποιήσουν πληρωμές μέσω κινητών τηλεφώνων. Η διαδικασία είναι απλή – ο χρήστης πληρώνει μέσω Διαδικτύου ή και επί τόπου σε κάποιο κατάστημα χρησιμοποιώντας το κινητό του αντί πιστωτικής κάρτας - και βασίζεται σε μία έξυπνη κάρτα (χρεωστική ή πιστωτική) η οποία ενσωματώνεται στο κινητό του (το οποίο πρακτικά αποκτά λειτουργίες πορτοφολιού).

6. Αγορές μέσω κινητού. Όπως και στο διαδίκτυο, τα προϊόντα για τα οποία θα υπάρξει κρίσιμη μάζα καταναλωτών οι οποίοι θα αγοράσουν μέσω κινητού είναι τα ταξιδιωτικά εισιτήρια, η ενοίκιαση αυτοκινήτων και δωματίων ξενοδοχείων, εισιτήρια για συναυλίες, θέατρο, κινηματογράφο, και αγορές δώρων όπως λουλούδια, γλυκά, βιβλία και CD's

7. Διασκέδαση. Μία σημαντική υπηρεσία για τους χρήστες δεδομένου ότι από το 2000 ακόμη την χρησιμοποιούσε το 30% των εγγεγραμμένων στην υπηρεσία i-mode. Οι μορφές αυτής της υπηρεσίας είναι πολλές:

- α. Παιχνίδια
- β. Κατέβασμα μουσικής / video
- γ. Κατέβασμα ringtones
- ε. Ηλεκτρονικές ευχετήριες και άλλες κάρτες
- στ. Υπηρεσίες γνωριμιών
- ζ. Τζόγος (είναι νόμιμος μόνο σε μερικές χώρες)

Εκτός όμως από τα κλασσικά αυτά προϊόντα, έρευνες για τη συμπεριφορά του καταναλωτή σχετικά με τη χρήση του κινητού του για αγορές, έχουν γίνει και για προϊόντα όπως η Coca Cola: στο αεροδρόμιο του Helsinki λειτούργησε πειραματικά ένα μηχάνημα το οποίο αντί για κέρματα δεχόταν κλήση ενός συγκεκριμένου αριθμού από κινητό τηλέφωνο. Η χρέωση γινόταν στο λογαριασμό τηλεφώνου του κατόχου του κινητού.

Σε κάποιες χώρες της Ευρώπης και στην Ιαπωνία και με τη σύμπραξη εταιρειών λιανεμπορίου, τραπεζών και κατασκευαστών κινητών τηλεφώνων λειτουργούν πιλοτικά πληρωμές σε σημεία λιανικής πώλησης μέσω κινητών που περιέχουν τσιπάκια έξυπνων πιστωτικών ή χρεωστικών καρτών

Ακολουθεί λίστα με τις τραπεζικές εργασίες που ήδη προσφέρονται από ελληνικές τράπεζες στους πελάτες τους και τις οποίες μπορούν να εκτελέσουν μέσω του κινητού τους τηλεφώνου

ΔΙΑΧΕΙΡΙΣΗ ΛΟΓΑΡΙΑΣΜΩΝ

-Υπόλοιπα και Κινήσεις λογαριασμών
-Ανάλυση Υπολοίπου
-Αναλυτικά Στοιχεία λογαριασμού
-Παραγγελία Βιβλιαρίου Επιταγών
-Ανάκληση Βιβλιαρίου Επιταγών ή Επιταγής

ΔΙΑΧΕΙΡΙΣΗ ΚΑΡΤΩΝ

-Υπόλοιπα και Κινήσεις πιστωτικών καρτών
-Αναλυτικά Στοιχεία πιστωτικών καρτών
-Πληρωμή άμεσα ή σε μελλοντική ημερομηνία

ΔΙΑΧΕΙΡΙΣΗ ΔΑΝΕΙΩΝ

-Συνολική απεικόνιση των δανείων
-Αναλυτικά Στοιχεία δανείων

ΠΛΗΡΩΜΕΣ-ΜΕΤΑΦΟΡΕΣ

-Μεταφορά σε λογαριασμό του πελάτη
-Μεταφορά σε λογαριασμούς τρίτων
-Εντολές Πληρωμής τρίτων σε μελλοντική ημερομηνία
-Εντολές Εμβασμάτων
-Καθορισμός Περιοδικών πληρωμών
-Αποθήκευση τακτικών πληρωμών για άμεση επανάληψη
-Αλλαγή λεπτομερειών αποθηκευμένων εντολών πληρωμών
-Αναβολή ή Ακύρωση αποθηκευμένων εντολών πληρωμών
-Αιτιολογία πληρωμών προς ενημέρωση του αποδέκτη
-Μεμονωμένες Εντολές πληρωμής Δ.Ε.Κ.Ο, Ο.Τ.Ε, ΔΕΗ)
-Μεμονωμένες Εντολές πληρωμής (Ι.Κ.Α, Φ.Π.Α, Τ.Ε.Β.Ε)
-Ιστορικό όλων των Πληρωμών

ΧΡΗΜΑΤΙΣΤΗΡΙΑΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

-Παρακολούθηση on-line σε πραγματικό χρόνο, του χαρτοφυλακίου σας και των τιμών των μετοχών
-Εντολές Αγοράς με χρέωση του λογαριασμού
-Εντολές Πώλησης με πίστωση του λογαριασμού
-Ενημέρωση για την εκτέλεση των εντολών
-Εντολές Ημέρας
-Συμμετοχή σε Δημόσιες Εγγραφές

ΠΡΟΣΩΠΙΚΕΣ ΥΠΗΡΕΣΙΕΣ ΠΕΛΑΤΗ

-Επιλογή & Αλλαγή προσωπικού κωδικού εισόδου
-Επιλογή & Αλλαγή κωδικού ασφαλείας
-Επιλογή Γλώσσας Επικοινωνίας (Ελληνικά/Αγγλικά)
-Προσωπικά Μηνύματα από την Τράπεζα
-"Ιστορικό" Κινήσεων / Συναλλαγών
-Φόρμα Επικοινωνίας με την Τράπεζα
-Ευρετήριο Καταστημάτων & ATM
-Διαχείριση Αιτήσεων

Ένα παράδειγμα που αφορά την Υπηρεσία m-banking της Alpha Bank



Η Alpha Bank προσφέρει τη δυνατότητα στους πελάτες της να εκτελούν δωρεάν τραπεζικές συναλλαγές μέσω κινητού τηλεφώνου 24 ώρες το 24ωρο. Ο συνδρομητής της υπηρεσίας m-banking μπορεί να παρακολουθεί τα υπόλοιπα των καταθετικών λογαριασμών, των στεγαστικών δανείων, των ανοιχτών προσωπικών δανείων Alpha 700 και των πιστωτικών καρτών, να πραγματοποιεί μεταφορές κεφαλαίων και πληρωμές οφειλών σε τρίτους, να πληροφορείται για τιμές συναλλάγματος και μετοχών κ.λπ. Ιδιώτες πελάτες αλλά και επιχειρήσεις μπορούν να εκτελούν τραπεζικές συναλλαγές μέσω κινητού τηλεφώνου που διαθέτει υποστήριξη υπηρεσιών WAP. Αναλυτικά ο χρήστης μπορεί:

- Να έχει πρόσβαση στα υπόλοιπα και τις τελευταίες πέντε κινήσεις των τραπεζικών λογαριασμών που πραγματοποιήθηκαν μέχρι τις 23:00 (24 ώρες το 24ωρο).
- Να πληροφορείται για την οφειλή και το διαθέσιμο υπόλοιπο αγορών στις πιστωτικές κάρτες (07:30 - 23:00)

- Να πληροφορείται για την οφειλή και το διαθέσιμο υπόλοιπο του δανείου Alpha 700 (07:30 - 23:00)
- Να πληροφορείται για την κατάσταση των επιταγών των καρτέ (24 ώρες το 24ωρο)
- Να μεταφέρει άμεσα χρήματα (Ευρώ) από ένα λογαριασμό σε άλλον (07:30 - 23:00)
- Να μεταφέρει χρήματα (Ευρώ) σε λογαριασμούς τρίτων (07:30 - 23:00)
- Να πληρώνει οφειλές σε πιστωτικές κάρτες εκδόσεως Alpha Bank ή σε προσωπικό δάνειο (24 ώρες το 24ωρο)
- Να πληρώνει τους λογαριασμούς Ε.Υ.Δ.Α.Π (24 ώρες το 24ωρο)

Σχετικός σύνδεσμος: <http://www.alpha.gr/>

4.3.2 Οι παίκτες του κινητού επιχειρείν

Το κινητό ηλεκτρονικό επιχειρείν σήμερα κυριαρχείται από τις εταιρείες κινητής τηλεφωνίας οι οποίες ελέγχουν πλήρως την αγορά, όσο αυτή είναι ακόμα σχετικά μικρή και η ανάπτυξη νέων υπηρεσιών περιλαμβάνει σημαντικό ρίσκο. Σταδιακά όμως παρατηρούμε σε ορισμένες αγορές την ανάπτυξη τρίτων παροχέων υπηρεσιών και περιεχομένου. Ένα από τα γνωστότερα παραδείγματα είναι η Paybox η οποία παρέχει στη Γερμανία και την Αγγλία υπηρεσίες πληρωμών μέσω του κινητού τηλεφώνου. Το ερώτημα είναι πως θα διαμορφωθεί ο χάρτης του κινητού επιχειρείν όταν η αγορά μεγαλώσει και αρχίσει να ωριμάζει; Ξεχωρίζουμε 17 δυνητικούς παίκτες και τους ταξινομούμε σε 6 κατηγορίες, ως ακολούθως. Κάποιες εταιρείες μπορεί να παίξουν περισσότερους από έναν από τους παρακάτω ρόλους .

1. Τεχνική υποδομή

- 1.1. Κατασκευαστές υποδομών δικτύων
 - 1.2. Παροχείς δικτυακών υπηρεσιών
 - 1.3. Εταιρείες ανάπτυξης εφαρμογών
-

2. Εμπορική υποδομή

- 2.1. Χρηματοδότες
- 2.2. Έμπιστη Τρίτα Μέρη
- 2.3. Σύμβουλοι και εταιρικές υπηρεσίες

3. Ευρύτερο περιβάλλον

- 3.1. Ρυθμιστικά όργανα (π.χ. ΕΕΤΤ)
- 3.2. Οργανισμοί προτυποποίησης
- 3.3. Μη κρατικοί φορείς ανάπτυξης και προώθησης της τεχνολογίας

4. Παροχείς υπηρεσιών

- 4.1. Παροχείς υπηρεσιών ασύρματων εφαρμογών
- 4.2. Παροχείς πληροφοριών και περιεχομένου
- 4.3. Εταιρείες συγκέντρωσης και ολοκλήρωσης (παροχής πακέτων) υπηρεσιών

5. Μαζική παραγωγή και κατανάλωση

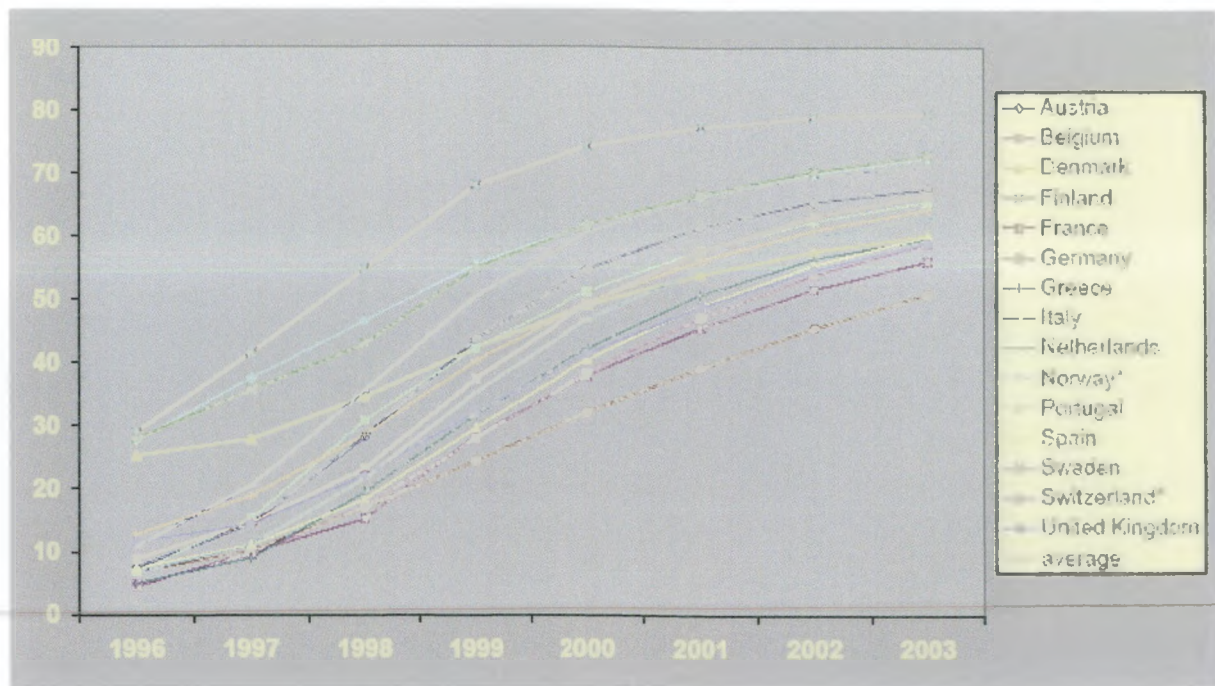
- 5.1. Κατασκευαστές κινητών τηλεφώνων και συσκευών
- 5.2. Δίκτυα λιανικού εμπορίου

6. Πελάτες

- 6.1. Καταναλωτές
- 6.2. Εταιρικοί πελάτες
- 6.3. Δημόσιος τομέας

Διείσδυση της κινητής τηλεφωνίας στην Ευρώπη

Το σχήμα που ακολουθεί μας δίνει μια συνολική εικόνα της διείσδυσα κινητής τηλεφωνίας σε ευρωπαϊκό επίπεδο. Πάντως και ενώ η διείσδυση της κινητής τηλεφωνίας παρουσιάζεται συνεχώς αυξανόμενη, τείνει να φτάσει σε ανώτατα δυνατά επίπεδα (π.χ. στην Ελλάδα βρίσκεται πια στα επίπεδα του 70%), γεγονός που καθιστά επιτακτική την ανάγκη για ανάπτυξη υπηρεσιών προστιθέμενης αξίας τα επόμενα χρόνια ανοίγοντας το δρόμο για την ανάπτυξη του ΚΗΕ.



Εικόνα 18: Η κινητή τηλεφωνία σε ευρωπαϊκό επίπεδο

Συμπεράσματα & Προτάσεις

Συνολικά, η Ευρωπαϊκή αγορά Κ.Η.Ε παρά την παγκόσμια οικονομική ύφεση βρίσκεται σε πλεονεκτική θέση μιας και παρουσιάζει μια συνεχή ανάπτυξη στο χώρο της κινητής τεχνολογίας ενώ η εμπειρία που προέρχεται από την εξέλιξη του Ηλεκτρονικού Εμπορίου στις Η.Π.Α. αποτελεί ένα χρήσιμο οδηγό. Αποφασιστικής σημασίας είναι : α) η διαμόρφωση ενός αποτελεσματικού ρυθμιστικού πλαισίου β) η ασφάλεια των συναλλαγών, γ) και η παροχή πλούσιου και ενδιαφέροντος περιεχομένου προς τον τελικό χρήστη.

Τα σημαντικότερα συμπεράσματα μπορούν να συνοψιστούν ως εξής :

- Οι ευρυζωνικές τεχνολογίες είναι ακόμα σε χαμηλό επίπεδο ανάπτυξης σε σχέση με της Η.Π.Α. αλλά αναμένεται ταχύρυθμη ανάπτυξη τα επόμενα χρόνια.
- Η απελευθέρωση του τηλ/κού τομέα θα ενδυναμώσει τον ανταγωνισμό προς όφελος του τελικού καταναλωτή

Στην παρούσα φάση η Μέση Απόδοση ανά Καταναλωτή (**ARPU, average return per user**) τείνει να φτάσει στα ανώτερα δυνατά επίπεδα. Αυτό οδηγεί στην ανάγκη ανάπτυξης υπηρεσιών προστιθέμενης αξίας για τον πελάτη. Σε αυτό το πλαίσιο, οι εφαρμογές ΚΗΕ θα γνωρίζουν ταχύρυθμη ανάπτυξη αντίστοιχη με αυτή των αγορών Ηλεκτρονικού Εμπορίου, δίνοντας προστιθέμενη αξία στην αγορά κινητής τηλεφωνίας. Οι χρηματοοικονομικές συναλλαγές και οι υπηρεσίες ψυχαγωγίας αναμένεται να αποτελέσουν τις σημαντικότερες εφαρμογές του ΚΗΕ στην Ευρώπη.

Κρίσιμος θα είναι ο ρόλος των κατασκευαστών κινητών τηλεφώνων. Στην παρούσα φάση οι τεχνολογικοί περιορισμοί αποτελούν κρίσιμο παράγοντα ανάσχεσης. Ωστόσο, αυτό δεν μπορεί να αποτελέσει δικαιολογία για τους παίκτες που δραστηριοποιούνται στο χώρο. Κρίσιμος παράγοντας επιτυχίας είναι η «κοινωνικοποίηση» των νέων εφαρμογών ΚΗΕ και όχι η προσαρμογή των

καταναλωτών σε ένα στείρο τεχνο-οικονομικό μοντέλο. Ιδιαίτερη αξία θα έχουν οι επενδύσεις στις νεαρές ηλικίες (12-25). Παρά την ανάπτυξη παγκοσμιοποιημένων στρατηγικών, υπάρχει ολοένα και μεγαλύτερη ανάγκη για ανάπτυξη υπηρεσιών τοπικού ενδιαφέροντος (Global strategy, local services)

5. ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ

Σύμφωνα με έρευνα που πραγματοποιήθηκε από τον ΟΟΣΑ στις Σκανδιναβικές χώρες και την Ιαπωνία το 2002 ²⁴, απεδείχθη ότι η ασφάλεια και η αβεβαιότητα των χρηστών αναφορικά με την εκτέλεση ηλεκτρονικών αγορών, αποτελούν ίσως τους σημαντικότερους περιοριστικούς λόγους εξάπλωσης του ηλεκτρονικού εμπορίου. Αυτή η ενότητα εστιάζει στους τρόπους που εξασφαλίζεται η ασφάλεια των ηλεκτρονικών πληρωμών, μέσω της συμμετρικής και ασύμμετρης μεθόδου κρυπτογράφησης και άλλων τρόπων. Ακόμη, γίνεται αναφορά στην πιο διαδεδομένη τεχνολογία κρυπτογράφησης την PKI (Public Key Infrastructure), και η ενότητα ολοκληρώνεται συζητώντας διάφορα θέματα ασφαλείας που προκύπτουν σχετικά με τις ηλεκτρονικές πληρωμές.

5.1 ΣΥΝΙΣΤΩΣΕΣ ΑΣΦΑΛΕΙΑΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ

5.1.1 Μέθοδοι ασφάλειας ηλεκτρονικών συναλλαγών και ηλεκτρονικές υπογραφές

Στις καθημερινές **συμβατικές συναλλαγές** έχουν καθιερωθεί –είτε εθιμικά είτε νομοθετικά- η χρήση διαφόρων μεθόδων για την εξακρίβωση της ταυτότητας των συναλλασσόμενων και την συγκέντρωση και διατήρηση αποδείξεων για την πραγματοποίηση μιας συναλλαγής, που βασίζονται κυρίως σε **πρωτότυπα ενυπόγραφα έγγραφα** που αρχειοθετούνται για όσο και επιδεικνύονται όποτε χρειάζεται.

Αντιθέτως, **στις ηλεκτρονικές συναλλαγές**, τα χρησιμοποιούμενα ψηφιακά δεδομένα, λόγω της μη ενσωμάτωσής τους σε ένα μοναδικό υλικό φορέα, είναι δύσκολο να προστατευθούν από αλλοίωση ή / και αντιγραφή, ενώ και η απόδειξη της προέλευσής τους καθίσταται, επίσης, ιδιαίτερα προβληματική.

Οι βασικές σήμερα μέθοδοι ηλεκτρονικής **‘ταυτοποίησης των συναλλασσόμενων’** (π.χ. **‘κωδικός χρήστη / ‘κωδικός πρόσβασης)** και **‘διαφύλαξης της ακεραιότητας των δεδομένων’** (π.χ. **συμμετρική κρυπτογράφηση**), λειτουργούν με την χρήση κοινών **‘κλειδιών’** ή **‘κωδικών’** από τους συναλλασσόμενους, με συνέπεια **να μην μπορούν** να υποστηρίξουν εφαρμογές που απαιτούν **ασφαλή, αξιόπιστη και εγγυημένη** πιστοποίηση της ταυτότητας (**‘ταυτοποίηση’**) των χρηστών

24 OECD Information Technology Outlook 2002, 150-152

αυτών των κλειδιών έναντι κάθε τρίτου, **ούτε και να** εξασφαλίσουν την πιστοποίηση της προέλευσης ('αυθεντικότητα'), την 'ακεραιότητα' και την 'εμπιστευτικότητα' των διακινούμενων ή / και αρχειοθετούμενων 'ηλεκτρονικών δεδομένων'. Σχετική με την παραπάνω ανεπάρκεια των χρησιμοποιούμενων μεθόδων, αποτελεί και η διαπίστωση πρόσφατης μεγάλης έρευνας²⁵, σύμφωνα με την οποία, η «έλλειψη ασφάλειας στις ηλεκτρονικές συναλλαγές» αποτελεί τον πρώτο (με ποσοστό 77%!) αρνητικό λόγο που δικαιολογούν οι επιχειρήσεις την απροθυμία τους να ενασχοληθούν με το «ηλεκτρονικό εμπόριο» ταυτοτήτων, σφραγισμένοι φάκελοι, θεωρημένα τιμολόγια, κ.λπ.) εξακολουθούν να αποτελούν σήμερα τα κύρια αποδεικτικά στοιχεία μιας συναλλαγής.

Πιο συγκεκριμένα τα κριτήρια ασφαλείας των Συστημάτων Ηλεκτρονικών Πληρωμών ομαδοποιούνται ως εξής:

- **Διαθεσιμότητα (Availability):** Το σύστημα θα πρέπει να προσφέρει αποτελεσματική ασφάλεια και στιγμιαία χρονική απόκριση, ακόμη θα πρέπει να έχει ταχύτατη ανάκτηση δεδομένων στην περίπτωση διακοπής της λειτουργίας του.
- **Αυθεντικότητα και έγκριση συναλλαγής (Authenticity and authorisation):** Το σύστημα θα πρέπει να διαθέτει τις απαραίτητες μετρικές ώστε να ελέγχει τη γνησιότητα της ταυτότητας αυτού που συναλλάσσεται χρησιμοποιώντας μία υπηρεσία, και να εξασφαλίζει τη νομιμότητα της συναλλαγής.
- **Ακεραιότητα (Integrity):** Το σύστημα θα πρέπει να διασφαλίζει την προστασία των προσωπικών δεδομένων των συναλλασσομένων. Αυτό σημαίνει ότι τα προσωπικά δεδομένα των συναλλασσομένων δεν θα είναι διαθέσιμα σε οποιονδήποτε και για οποιονδήποτε σκοπό, χωρίς την προσωπική έγκρισή τους.
- **Μη αποποίηση ευθύνης (Non-Repudiation):** Το σύστημα θα πρέπει να εφαρμόζει κατάλληλες μεθόδους συναλλαγής ώστε από τη στιγμή που θα διαπιστωθεί η γνησιότητα της ταυτότητας του προσώπου το οποίο συναλλάσσεται, να εξασφαλίζεται με αποδεικτικά μέσα και η γνησιότητα της συναλλαγής. Αυτό πιστοποιείται από το μήνυμα που ζητάει την άδεια του συναλλασσόμενου για την αποδοχή και τη συνέχιση διεκπεραίωσης της συναλλαγής.
- **Εμπιστευτικότητα (Confidentiality):** Το σύστημα θα πρέπει να διασφαλίζει την προστασία των δεδομένων της συναλλαγής από τρίτους. Η επίτευξη αυτών των χαρακτηριστικών ασφαλείας επιβάλλει τον συνδυασμό διαφόρων τεχνικών κρυπτογράφησης οι οποίες πρέπει να συνδυαστούν με τις σχετικές επιχειρησιακές διαδικασίες ενός οργανισμού. Τέλος είναι πολύ σημαντικό όλα αυτά τα χαρακτηριστικά να συνδυαστούν με την απαραίτητη αξιοπιστία, ώστε να κερδίσουν την εμπιστοσύνη του τελικού καταναλωτή. Χαρακτηριστικό είναι ότι η επίτευξη ενός υψηλού επιπέδου ασφαλείας στις συναλλαγές δεν είναι μόνο θέμα τεχνολογικό, αλλά εντάσσεται στην ευρύτερη

²⁵ που πραγματοποιήθηκε στα πλαίσια του έργου 'La Mer' (9/2003) με την συμπλήρωση σχετικού ερωτηματολογίου από πολλές συμμετέχουσες ΜΜΕ

στρατηγική ενός οργανισμού εξασφαλίζοντας την αποδοχή αυτού του τρόπου πληρωμών από τους τελικούς καταναλωτές σε συνδυασμό με το χαμηλό κόστος της συναλλαγής.

Έτσι τα 'έντυπα μέσα' που χρησιμοποιούνται για την καταγραφή και την απόδειξη μιας συναλλαγής (π.χ. ενυπόγραφα ιδιωτικά έγγραφα, επικυρωμένα φωτοαντίγραφα) η πλήρης αντικατάστασή τους με αντίστοιχα 'ψηφιακά δεδομένα' επιτρέπουν ολοκληρωμένες ηλεκτρονικές συναλλαγές) –ιδίως σε περιπτώσεις 'σημαντικών' συναλλαγών- , προϋποθέτει την χρήση ασφαλών και τεχνικώς αξιόπιστων μεθόδων πιστοποίησης της 'προέλευσης' και της 'ακεραιότητας' των δεδομένων και κυρίως την παροχή αποδείξεων για την 'μη αποκλήρυξη' της συναλλαγής, κάτι που, με τις υπάρχουσες σήμερα τεχνολογικές δυνατότητες, μπορεί να παράσχει άμεσα μόνο η χρήση **'προηγμένων ηλεκτρονικών υπογραφών'** και σχετικών **'ηλεκτρονικών πιστοποιητικών ταυτοποίησης'**.

5.2 ΤΕΧΝΟΛΟΓΙΕΣ ΠΟΥ ΕΞΑΣΦΑΛΙΖΟΥΝ ΥΨΗΛΑ ΕΠΙΠΕΔΑ ΑΣΦΑΛΕΙΑΣ ΣΤΙΣ ΣΥΝΑΛΛΑΓΕΣ

Οι τεχνολογίες που αναφέρονται ως κατάλληλες για την επίτευξη υψηλού επιπέδου ασφάλειας στις ηλεκτρονικές συναλλαγές κατατάσσονται σε τέσσερις γενικές κατηγορίες μεθόδων. Στη συνέχεια γίνεται αναφορά στις μεθόδους αυτές με σκοπό όχι την παρουσίαση τεχνικών ζητημάτων αλλά στην πληρέστερη κατανόηση βασικών θεμάτων και χαρακτηριστικών ασφάλειας των συστημάτων ηλεκτρονικών πληρωμών.

Δημόσια υποδομή
Συμμετρική και Ασύμμετρη Κρυπτογράφηση
Ψηφιακές υπογραφές
Πρότυπα για Ηλεκτρονικές πληρωμές

Η δημόσια υποδομή *public key infrastructure* είναι ένας τρόπος διασφάλισης των ηλεκτρονικών πληρωμών με χρήση απόκρυψης με δημόσιο κλειδί, ψηφιακές υπογραφές και ψηφιακά πιστοποιητικά με μια δικτυακή εφαρμογή.

5.2.1 Πιστοποίηση Δημόσιου Κλειδιού (PKI και PGP)

Κρυπτογράφηση

Οι ευαίσθητες πληροφορίες που κυκλοφορούν σε δημόσια δίκτυα μπορούν να προστατευθούν με την κρυπτογράφησή τους, δηλαδή με τη γραφή τους σε κάποιο σύστημα συμβόλων ακατανόητο για οποιονδήποτε να τις υποκλέψει. Η κρυπτογράφηση ψηφιακών πληροφοριών γίνεται με την εφαρμογή κάποιων πολύπλοκων μαθηματικών πράξεων στο ψηφιακό περιεχόμενό τους. Στις πράξεις αυτές χρησιμοποιείται ένα "κλειδί", που είναι ένας πάρα πολύ μεγάλος αριθμός (αποθηκευμένος επίσης ψηφιακά). Η αντιστροφή της κρυπτογράφησης, δηλαδή η αποκρυπτογράφηση, γίνεται με κάποιες άλλες μαθηματικές πράξεις, στις οποίες πρέπει να χρησιμοποιηθεί το ίδιο ή κάποιο συμπληρωματικό "κλειδί". Σήμερα υπάρχουν δυο κύριες μέθοδοι κρυπτογράφησης. Η παλιότερη χρησιμοποιεί για κρυπτογράφηση και αποκρυπτογράφηση το ίδιο κλειδί, που πρέπει να διατηρείται μυστικό. Η νεότερη χρησιμοποιεί ένα ζευγάρι από συμπληρωματικά κλειδιά, από τα οποία το ένα είναι μυστικό ενώ το άλλο είναι δημόσιο.

Παρόλα αυτά διατηρείται ακέραια η **ανάγκη**, *-ιδίως σε 'ανοικτές εφαρμογές' με πολλαπλούς ή ακόμη και άγνωστους αποδέκτες-*, για την ύπαρξη μιας **«Έμπιστης Τρίτης Οντότητας»** που ονομάζεται **«Πάροχος Υπηρεσιών Πιστοποίησης»** (ΠΥΠ) η οποία, επιπλέον, πιστοποιεί προς οποιοδήποτε τρίτο-αποδέκτη μιας ψηφιακής υπογραφής:

- την καταγραφή (registration) της πραγματικής ταυτότητας του κατόχου του ιδιωτικού κλειδιού που αντιστοιχεί στο χρησιμοποιούμενο δημόσιο κλειδί, και
- τη σύνδεση του σχετικού ιδιωτικού κλειδιού με τον κάτοχο του πιστοποιητικού (proof of possession).

Η παραπάνω πιστοποίηση (προς χρήση από τους αποδέκτες της ηλεκτρονικής υπογραφής) γίνεται με την έκδοση **«ψηφιακών πιστοποιητικών»** τα οποία υπογράφονται ηλεκτρονικά από τον ΠΥΠ και τα οποία περιέχουν τα στοιχεία

ταυτοποίησης του κατόχου του ιδιωτικού κλειδιού, καθώς και το σχετικό δημόσιο κλειδί του.

Η υποδομή με την οποία ένας ΠΥΠ εκδίδει, δημοσιεύει και υποστηρίζει 'τυποποιημένες ηλεκτρονικές βεβαιώσεις' (πιστοποιητικά) για τους συνδρομητές του (υποκείμενα πιστοποίησης) ονομάζεται '**Υποδομή Δημοσίων Κλειδιού**' (Public Key Infrastructure – 'PKI').

Μια άλλη εναλλακτική μέθοδος πιστοποίησης των δημοσίων κλειδιών ενός χρήστη βασίζεται στα «αυτό-υπογραφόμενα πιστοποιητικά» που εκδίδονται από το ίδιο τον (τελικό) χρήστη (κάτοχο του συγκεκριμένου ζεύγους κρυπτογραφικών κλειδιών), ο οποίος λειτουργεί παράλληλα και ως 'αποδέκτης'. Τα πιστοποιητικά αυτά δημοσιεύονται από τον εκδότη τους σε έναν ή περισσότερους δημόσιους 'εξυπηρετητές κλειδιών' (key servers), απ' όπου λαμβάνονται, αξιολογούνται και πιθανώς υπογράφονται και από άλλους χρήστες, οι οποίοι, μέσω διαπροσωπικής επικοινωνίας τους με το υποκείμενο-κάτοχό τους, αλληλο-επιβεβαιώνουν και πιστοποιούν την συγκεκριμένη συσχέτιση. Ένα πολύ διαδεδομένο τέτοιο σύστημα (αλληλο-)πιστοποίησης είναι το '**Pretty Good Privacy**' (PGP) και βασίζεται στην δημιουργία ενός (αποκεντρωμένου) '**δικτύου εμπιστοσύνης**' ('web of trust') που αναπτύσσεται με την μεταβίβαση της εμπιστοσύνης μεταξύ των χρηστών της.

5.2.1.1 Είδη Ηλεκτρονικών Πιστοποιητικών

Τα 'πιστοποιητικά δημοσίου κλειδιού' μπορούν να διακριθούν σε '**επώνυμα**' και σε '**ψευδώνυμα**' πιστοποιητικά, ανάλογα με τη δημοσιοποίηση του πραγματικού ονόματος του υποκειμένου στο οποίο αναφέρονται. Είναι ακόμη δυνατόν να εκδοθούν και '**ανώνυμα**' πιστοποιητικά, στα οποία συνήθως πιστοποιείται -μέσω απομακρυσμένης on-line επικοινωνίας- μόνο η χρήση ενός συγκεκριμένου λογαριασμού ηλεκτρονικού ταχυδρομείου (*e-mail address*) από το υποκείμενο.

Εκτός από στοιχεία ταυτοποίησης του υποκειμένου τους, τα πιστοποιητικά δημοσίου κλειδιού μπορούν να περιλαμβάνουν και αναφορά σε συγκεκριμένες (πιστοποιημένες ή μη) **ιδιότητες** του υποκειμένου (*π.χ. επάγγελμα κ.λ.π.*). Μια άλλη σχετική δυνατότητα είναι η χρήση άλλων (πρόσθετων) ειδικών '**πιστοποιητικών ιδιοτήτων**' (attribute certificates) τα οποία χρησιμοποιούνται παράλληλα με τα '**βασικά πιστοποιητικά δημοσίου κλειδιού**', και τα οποία μπορούν να εκδίδονται από μια 'Αρχή Πιστοποίησης Ιδιοτήτων' (Attribute Authority – 'AA').

Πέρα των πιστοποιητικών για φυσικά πρόσωπα, μια **άλλη κατηγορία πιστοποιητικών** δημοσίων κλειδιών αποτελεί αυτή που εκδίδεται με 'υποκείμενο' τηλεπικοινωνιακά ή πληροφορικά συστήματα και συσκευές (*web servers, routers, client devices, κ.λ.π.*). Η χρήση των κρυπτογραφικών κλειδιών που σχετίζονται με τα συγκεκριμένα πιστοποιητικά, γίνεται συνήθως με αυτόματο τρόπο από τους servers αυτών (*server authentication*) και, **β)** σε «κρυπτογράφηση άλλων συμμετρικών κλειδιών» τα οποία χρησιμοποιούνται για την περαιτέρω κρυπτογράφηση των διακινούμενων δεδομένων. Χαρακτηριστική εφαρμογή είναι η '**πιστοποίηση προέλευσης ιστοσελίδων**' όπου, στην πράξη, πιστοποιείται η νόμιμη εξυπηρέτηση μιας 'διεύθυνσης διαδικτύου' (URL) από έναν συγκεκριμένο 'εξυπηρετητή Διαδικτύου' (web server) -στον οποίον έχουν εγκατασταθεί τα σχετικά κρυπτογραφικά κλειδιά- επιτρέποντας παράλληλα και την 'κρυπτογράφηση παροδικών συμμετρικών

κλειδιών' (*session keys*) για την επίτευξη ασφαλούς (εμπιστευτικής) επικοινωνίας τύπου «SSL» ή «TSL».

Τέλος, μια άλλη κατηγορία ηλεκτρονικών πιστοποιητικών, αποτελούν τα 'πιστοποιητικά χρονοσήμανσης' τα οποία, εκδίδονται ad hoc σε συγκεκριμένα ηλεκτρονικά έγγραφα, μετά από αίτημα του υπογράφοντα ή / και του αποδέκτη τους. Στα περιεχόμενά τους, εκτός των στοιχείων του εκδότη τους (και πιθανώς και του αιτούντα), περιλαμβάνουν την 'σύνοψη' του συγκεκριμένου εγγράφου στο οποίο αναφέρονται και την ακριβή χρονική στιγμή έκδοσής τους (η οποία βασίζεται σε αξιόπιστη πηγή χρονολόγησης που διαθέτει ο εκδότης τους). Η χρήση των πιστοποιητικών χρονοσήμανσης **εξασφαλίζει αποδείξεις** για την ύπαρξη μιας ηλεκτρονικής υπογραφής σε μια συγκεκριμένη χρονική στιγμή, αποκλείοντας έτσι την δυνατότητα μελλοντικής 'αποποίησης' της από τον υπογράφοντα με τον ισχυρισμό ότι αυτή δημιουργήθηκε μετά την λήξη ή την ανάκληση του σχετικού 'πιστοποιητικού δημοσίου κλειδιού' (π.χ. λόγω έκθεσης του συγκεκριμένου κρυπτογραφικού κλειδιού σε τρίτους).

5.2.1.2 Μορφή και περιεχόμενο των η-Πιστοποιητικών (X.509)

Τα ηλεκτρονικά 'Πιστοποιητικά Δημοσίου Κλειδιού' ('Public Key Certificates' ή 'PKC') είναι τυποποιημένα ηλεκτρονικά έγγραφα τα οποία εκδίδονται και υπογράφονται από έναν ΠΥΠ (που μπορεί να είναι και 'φυσικό πρόσωπο') με σκοπό να πιστοποιήσουν την κατοχή συγκεκριμένου ζεύγους (ασύμμετρων) κρυπτογραφικών κλειδιών από ένα 'υποκείμενο' (*Proof of Possession*) και να περιγράψουν 'στοιχεία ταυτοποίησης' (*Identification*) του 'υποκειμένου' αυτού.

Το πιο διαδεδομένο (διεθνώς) πρότυπο για την σύνταξη ενός 'πιστοποιητικού δημοσίου κλειδιού' είναι το 'X.509' το οποίο αποτελεί 'Σύσταση' (*Recommendation*) της Διεθνούς Ένωσης Τηλεπικοινωνιών (ITU). Το πρότυπο X.509 διαθέτει αρκετά προκαθορισμένα πεδία για την αναγραφή των απαραίτητων πληροφοριών (αριθμός ταυτοποίησης του πιστοποιητικού, εκδότης, υποκείμενο-θέμα, δημόσιο κλειδί υποκειμένου, υπογραφή εκδότη, διάρκεια ισχύος, χρήσεις κλειδιού, πολιτική πιστοποιητικού, διευθύνσεις πληροφοριών ανάκλησης, κ.ά.), καθώς και τη δυνατότητα να συμπεριλάβει και επιπλέον εκτεταμένα πεδία (*extensions*) που καθορίζονται από τον Εκδότη των πιστοποιητικών.

5.2.1.3 Ο έλεγχος του κύρους των η-πιστοποιητικών και των η-υπογραφών

Λόγω της διαρκούς τεχνολογικής εξέλιξης, θεωρείται δεδομένη η εξασθένιση της ασφάλειας των χρησιμοποιούμενων κρυπτογραφικών κλειδιών στο πέρασμα του χρόνου. Έτσι, τα πιστοποιητικά δημοσίου κλειδιού, που αναφέρονται σε -αλλά και που υπογράφονται από- τέτοια κρυπτογραφικά κλειδιά, εκδίδονται με **περιορισμένη διάρκεια ισχύος (συνήθως 1 έως 3 έτη)**, η οποία και αναγράφεται μέσα στα προκαθορισμένα για τον σκοπό αυτό πεδία τους.

Εκτός όμως από την προγραμματισμένη λήξη, η ισχύς ενός πιστοποιητικού **μπορεί οποτεδήποτε να ανακληθεί** οριστικά (*revocation*) ή να ανασταλεί (*suspension*), ύστερα από αίτημα του τελικού χρήστη (π.χ. επειδή έχασε τον φορέα των κρυπτογραφικών κλειδιών του) ή / και από σχετική απόφαση του Εκδότη τους (π.χ. λόγω λάθους στην αναγραφή στοιχείων). Η 'ανάκληση' και η 'αναστολή' ενός πιστοποιητικού πραγματοποιείται με την εγγραφή του 'αριθμού ταυτοποίησης του

πιστοποιητικού' (certificate's serial number) σε μια **Λίστα Ανακληθέντων Πιστοποιητικών** (*Certificate Revocation List* ή *CRL*) η οποία υπογράφεται και δημοσιεύεται σε τακτά χρονικά διαστήματα από τον ίδιο τον Εκδότη των πιστοποιητικών²⁶.

Επίσης, επειδή τα **πιστοποιητικά δημοσίων κλειδιών** (*public key certificates – PKC*) που εκδίδει ένας ΠΥΠ προς τις ενδιαφερόμενους τελικούς χρήστες ή 'τελικές οντότητες', είναι και αυτά μια μορφή **ηλεκτρονικών εγγράφων**, επιβάλλεται να φέρουν και αυτά την 'ψηφιακή υπογραφή' του εκδότη τους. Αυτό προϋποθέτει ότι και ο ίδιος ο Εκδότης-ΠΥΠ διαθέτει το δικό του ζεύγος κρυπτογραφικών κλειδιών υπογραφής, το οποίο πρέπει εξίσου να υποστηρίζεται από σχετικό πιστοποιητικό δημοσίου κλειδιού -που κι αυτό, με την σειρά του, πρέπει να είναι υπογεγραμμένο ψηφιακά. Η σχηματιζόμενη αλληλουχία (αλυσίδα) πιστοποιητικών τερματίζεται με ένα τελικό και αξιόπιστο δημοσιευμένο **αυτοϋπογραφόμενο πιστοποιητικό** (*self-signed certificate*) που εκδίδεται από τον **Θεμελιώδη Εκδότη Πιστοποιητικών** (*Root Certification Authority* ή *'Root CA'*) του ΠΥΠ και το οποίο αποτελεί την «κορυφή της πυραμίδας» μιας υποδομής 'PKI'.

Έτσι, για να ελέγξει κάποιος την εγκυρότητα μιας προηγμένης ηλεκτρονικής υπογραφής, θα πρέπει να ελέγξει το κύρος του συγκεκριμένου πιστοποιητικού που την υποστηρίζει, και συγκεκριμένα θα πρέπει να ελέγξει:

- Ότι το συγκεκριμένο πιστοποιητικό του υπογράφοντα είναι **"αυθεντικό"**, με την έννοια ότι υπάρχει τουλάχιστον μία αλληλουχία πιστοποιητικών με όλους τους μεσολαβούντες (υπό-)εκδότες η οποία να καταλήγει σε μια αξιόπιστη -γι' αυτόν- **'ρίζα εμπιστοσύνης'** (συνήθως το αυτό-υπογραφόμενο πιστοποιητικό 'Root CA' ενός γνωστού ΠΥΠ).
- Ότι το συγκεκριμένο πιστοποιητικό είναι **"έγκυρο"**, δηλαδή ότι δεν έχει λήξει ή ανακληθεί η ισχύς του. Αυτό σημαίνει ότι ο αποδέκτης θα πρέπει να ελέγξει, όχι μόνο την διάρκεια ισχύος που αναγράφεται μέσα στο ίδιο το εξεταζόμενο πιστοποιητικό, αλλά και τις σχετικές **Λίστες Ανακληθέντων Πιστοποιητικών** που δημοσιεύει ο ίδιος ο εκδότης του. Ο έλεγχος αυτός μπορεί να γίνει είτε μέσω ειδικών αυτοματοποιημένων εφαρμογών που εμπιστεύεται ο χρήστης, είτε μέσω σχετικής απ' ευθείας υπηρεσίας (*'Online Certificate Status Protocol' - 'OCSP'*) που πιθανώς να παρέχει ο ΠΥΠ.
- Ότι το συγκεκριμένο πιστοποιητικό του υπογράφοντα είναι **"κατάλληλο"** για την συναλλαγή ή την χρήση στην οποία ο αποδέκτης του πρόκειται να προβεί. Για να θεωρηθεί "κατάλληλο" ένα πιστοποιητικό θα πρέπει η προτιθέμενη χρήση του να μην απαγορεύεται από την ισχύουσα **«Πολιτική Πιστοποιητικού»**. Επίσης, εάν από τον τύπο της επιχειρούμενης συναλλαγής έχει καθοριστεί ή / και πρέπει να ακολουθηθεί μια συγκεκριμένη **«Πολιτική (ηλεκτρονικής) Υπογραφής»**, τότε η χρήση του συγκεκριμένου πιστοποιητικού θα πρέπει να προβλέπεται ή, έστω, να επιτρέπεται από την εφαρμοζόμενη Πολιτική Υπογραφής.

²⁶ Βέβαια, τελευταία, έχει αρχίσει να χρησιμοποιείται ευρέως η τεχνολογία / υπηρεσία της «Άμεσης Επιβεβαίωσης της Κατάστασης του Πιστοποιητικού» (*'Online Certificate Status Provision' ή 'OCSP'*) η οποία έχει ως σημαντικό πλεονέκτημα τον άμεσο έλεγχο της πραγματικής κατάστασης ενός πιστοποιητικού, ακόμη και ελάχιστες στιγμές μετά την οριστική αποδοχή του 'αιτήματος ανάκλησης' από τον ΠΥΠ

5.3 Συμμετρική Κρυπτογράφηση

Στη συμμετρική κρυπτογράφηση (secret Key cryptography), ένα κοινό «κλειδί» ασφαλείας χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση. Οι συμμετρικοί κρυπτογραφημένοι αλγόριθμοι είναι εξαιρετικά ταχείς μιας και βασίζονται σε απλές μαθηματικές σχέσεις που βοηθούν την γρήγορη αποκρυπτογράφηση μεγάλου αριθμού κρυπτογραφημένων. Τα χαρακτηριστικά ασφαλείας, μη αποποίηση ευθύνης, αυθεντικότητα και ακεραιότητα μπορούν να επιτευχθούν με ιδιαίτερη ευκολία μέσω της συμμετρικής κρυπτογράφησης. Τα υπόλοιπα δύο όμως για να επιτευχθούν χρειάζονται την εφαρμογή συμπληρωματικών μεθόδων.

Παρόλα αυτά, η εκπλήρωση των παραπάνω απαιτήσεων εξαρτώνται από το στήσιμο της τεχνολογικής πλατφόρμας πάνω στην οποία θα μοιράζονται τα κοινά κλειδιά ασφαλείας στα ενδιαφερόμενα μέρη. Χαρακτηριστικό είναι ότι το κάθε μέλος που εξυπηρετείται από το σύστημα διαθέτει προσωπικό κλειδί ασφαλείας. Αυτό προϋποθέτει ότι το σύστημα πρέπει να παράγει μοναδικά για κάθε χρήστη κλειδιά ασφαλείας.

Το πρωτόκολλα ασφαλείας DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm) και AES (Advanced Encryption Standards) χρησιμοποιούνται σήμερα περισσότερο από οποιαδήποτε άλλα. Τα μειονεκτήματα της συμμετρικής κρυπτογράφησης εντοπίζονται κυρίως στην ανταλλαγή των κλειδιών ασφαλείας. Η συμμετρική κρυπτογράφηση αποδεικνύεται όχι και τόσο ασφαλής μέθοδος όταν πρέπει να γίνει ανταλλαγή πληροφοριών μεταξύ ενός μεγάλου όγκου χρηστών. Γι' αυτό πολλοί ειδικοί σε θέματα ασφαλείας στρέφονται στην ασύμμετρη μέθοδο κρυπτογράφησης.

5.3.1 Ασύμμετρη Κρυπτογράφηση

Η μέθοδος της ασύμμετρης κρυπτογράφησης PKC (Public Key Cryptography), μειώνει το πρόβλημα ανταλλαγής πολλών κλειδιών ασφαλείας μεταξύ ενός μεγάλου αριθμού χρηστών, με το να διαχωρίζει με μαθηματικό τρόπο τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης σε ένα μοναδικό ζευγάρι κλειδιών, εκ των οποίων το ένα παραμένει δημόσια διαθέσιμο (public) και το άλλο προσωπικό (private). Ο κάτοχος αυτών των κλειδιών πρέπει να κρατά μυστικό το ιδιωτικό κλειδί ασφαλείας ενώ το δημόσια διαθέσιμο, που του αντιστοιχεί διανέμεται ελεύθερα. Στην ασύμμετρη κρυπτογράφηση, τα κρυπτογραφημένα δεδομένα του δημοσίου κλειδιού μπορούν να αποκρυπτογραφηθούν μόνο στην περίπτωση που ο χρήστης γνωρίζει τον κωδικό του ιδιωτικού κλειδιού και αντίστροφα. Το μεγάλο πλεονέκτημα της μεθόδου της ασύμμετρης κρυπτογράφησης είναι ότι χρειάζονται λιγότερα κλειδιά ασφαλείας να ανταλλαχθούν για την διεκπεραίωση μιας συναλλαγής, μιας και τα ιδιωτικά κλειδιά ασφαλείας δεν χρειάζεται να μοιράζονται και στις δύο πλευρές αλλά μόνο να μεταδίδονται. Γι' αυτό το λόγο η ασύμμετρη κρυπτογράφηση είναι περισσότερο διαδεδομένη σε «ανοιχτά» δίκτυα (Open networks).

Πιο συγκεκριμένα η κρυπτογράφηση με δημόσιο κλειδί λειτουργεί ως εξής:

- ◆ Πριν από την έναρξη της επικοινωνίας κάθε πλευρά δίνει στην άλλη το δημόσιο κλειδί της.
- ◆ Η πρώτη επιχείρηση κρυπτογραφεί το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί της δεύτερης επιχείρησης. Το μήνυμα μετατρέπεται σε μια σειρά από ακατανόητα σύμβολα.

- ◆ Το μήνυμα μεταδίδεται κανονικά στη δεύτερη επιχείρηση. Ακόμη και αν κάποιος το υποκλέψει δεν θα μπορέσει να το διαβάσει (παρά μόνο αν γνωρίζει το μυστικό κλειδί της δεύτερης επιχείρησης).
- ◆ Η δεύτερη επιχείρηση λαμβάνει το μήνυμα και το αποκρυπτογραφεί χρησιμοποιώντας το μυστικό της κλειδί. Το κλειδί αυτό είναι γνωστό μόνο στην ίδια (δεν υπάρχει ανάγκη να δοθεί σε κανέναν άλλο) και έτσι μόνο η δεύτερη επιχείρηση (παραλήπτης) μπορεί να αποκρυπτογραφήσει οποιοδήποτε μήνυμα που έχει κρυπτογραφηθεί με το δημόσιο κλειδί της.

Όπως και με την συμμετρική μέθοδο κρυπτογράφησης, τα χαρακτηριστικά ασφαλείας που περιγράφονται στην παραπάνω ενότητα, μπορούν επίσης να επιτευχθούν και με την κρυπτογράφηση δημοσίου κλειδιού, όπως δείχνει και ο παρακάτω πίνακας.

Αποστολέας / Κρυπτογραφεί		Δέκτης / Αποκρυπτογραφεί	
Ιδιωτικό κλειδί Αποστολέα	Ακεραιότητα ----->	Δημόσιο κλειδί Αποστολέα	Ο δέκτης συγκρίνει την περιγραφή του μηνύματος με το γνήσιο μήνυμα
Ιδιωτικό κλειδί Αποστολέα	Πιστοποίηση της ταυτότητας του αποστολέα ----->	Δημόσιο κλειδί Αποστολέα	Υποθέτουμε ότι ο πραγματικός αποστολέας έχει στην κατοχή του το ιδιωτικό κλειδί
Δημόσιο κλειδί Δέκτη	Εμπιστευσιμότητα ----->	Ιδιωτικό κλειδί Δέκτη	Μόνο ο δέκτης μπορεί να διαβάσει το μήνυμα με το ιδιωτικό του κλειδί

Πίνακας 9:Κρυπτογράφηση Δημοσίου κλειδιού

Η κρυπτογράφηση Δημοσίου Κλειδιού επιτρέπει, στις περιπτώσεις που χρησιμοποιούνται ηλεκτρονικές υπογραφές για την διεκπεραίωση της συναλλαγής, να επιβεβαιωθεί η ακεραιότητα του μηνύματος που αποστέλλεται και να πιστοποιηθεί η ταυτότητα του αποστολέα. Η απόδειξη πραγματοποίησης της συναλλαγής (non-repudiation) εξαρτάται αφενός από το νομοθετικό πλαίσιο και αφετέρου από την εμπιστοσύνη που έχουμε στον κάτοχο του ιδιωτικού κλειδιού. Το χαρακτηριστικό της εμπιστευσιμότητας (confidentiality) της διακινηθείσας πληροφορίας μέσω της κρυπτογράφησης του μηνύματος από το δημόσιο κλειδί του δέκτη, συνήθως εξασφαλίζεται μέσω της χρήσης συμμετρικών τεχνικών. Η ασύμμετρη μέθοδος δεν ενδείκνυται για την εκπλήρωση αυτού του χαρακτηριστικού εξαιτίας των πολύπλοκων μαθηματικών σχέσεων που χρησιμοποιεί.

Για να επιτευχθούν όμως τα παραπάνω χαρακτηριστικά ασφαλείας χρειάζεται όμως και η συμβολή ενός έμπιστου οργανισμού που ειδικεύεται σε θέματα ασφαλείας. Η εισαγωγή και εφαρμογή ενός συστήματος PKI, προϋποθέτει ότι το δημόσιο κλειδί θα πρέπει να είναι συμβατό με όλες της διαδικασίες από πλευράς οργανισμού που σχετίζονται με την αγορά ενός αγαθού. Συνεπώς η εισαγωγή ενός συστήματος PKI απαιτεί και τον συνδυασμό ενός συστήματος PKC, τα οποία θα εγκατασταθούν στην κατάλληλη τεχνολογική υποδομή του οργανισμού που θα μπορεί να εξυπηρετήσει και αυτές τις υπηρεσίες ασφαλείας.

Σε γενικές γραμμές, η τεχνολογική υποδομή ασύμμετρης κρυπτογράφησης θα πρέπει να στηρίζεται όπως τονίζεται και στις οδηγίες της Ευρωπαϊκής Κεντρικής Τράπεζας, στις παρακάτω λειτουργίες και σε πιστοποιητικά ασφαλείας:

- **Registration Authority (RA).** Ο ρόλος της Αρχής Εγγραφής είναι να ανιχνεύει την ταυτότητα του προσώπου ή του οργανισμού που διενεργεί την συναλλαγή πριν την έκδοση του ζευγαριού των κλειδιών.
 - **Certification Authority (CA).** Το ζεύγος κλειδιών ασφαλείας εκδίδεται από την Αρχή Πιστοποίησης αφού πρώτα έχουν καταγραφεί τα στοιχεία του ενδιαφερόμενου στην Αρχή Εγγραφής (RA). Αναλόγως του επιθυμητού επιπέδου ασφαλείας, το ιδιωτικό κλειδί αποθηκεύεται σε μια έξυπνη κάρτα (smart card), ή σε μία κάρτα SIM ή στον σκληρό δίσκο ενός υπολογιστή. Το δημόσιο κλειδί ασφαλείας αποθηκεύεται στις Υπηρεσίες Καταλόγου.
 - **Directory Services.** Στις υπηρεσίες καταλόγου γίνεται η αποθήκευση των δημοσίων κλειδιών ασφαλείας καθώς και η ανάκτηση τους. Οι παραπάνω υπηρεσίες προσφέρονται συνήθως από εταιρείες παροχής τέτοιων πιστοποιητικών (Certification Service Providers).
-

5.4 ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

Οι 'προηγμένες ηλεκτρονικές (ή ψηφιακές) υπογραφές' και τα 'ψηφιακά πιστοποιητικά ταυτοποίησης', που στηρίζονται στην σύγχρονη τεχνολογία της 'ασύμμετρης κρυπτογραφίας' ικανοποιούν τις παραπάνω απαιτήσεις, αφού μπορούν να εξασφαλίσουν την 'αυθεντικότητα' (authentication) και την 'ακεραιότητα' (integrity) των σχετικών δεδομένων, την 'ταυτοποίηση' (identification) των συναλλασσόμενων και -κάτω από προϋποθέσεις- τη 'νομική δέσμευση' του υπογράφοντα ή αλλιώς την 'μη αποκρήρυξη' (non repudiation) της συναλλαγής ενώ, παράλληλα, μπορούν να προσφέρουν αξιόπιστη λύση και στο ζήτημα της 'εμπιστευτικότητας' (confidentiality) των δεδομένων κατά την διακίνηση ή / και την αρχειοθέτησή τους.

5.4.1 Τι προβλέπει το ισχύον θεσμικό πλαίσιο για τις ηλεκτρονικές υπογραφές

Η 'νομική αναγνώριση' των ηλεκτρονικών υπογραφών σε **διεθνές επίπεδο**, ξεκίνησε από τα μέσα της προηγούμενης δεκαετίας με την θέσπιση σχετικών νόμων σε διάφορα κράτη. Μπορούμε να διακρίνουμε δύο διαφορετικές νομικές προσεγγίσεις:

- Τη '**μινιμαλιστική προσέγγιση**' (minimalist approach), όπου «κάθε αξιόπιστη τεχνολογική μέθοδος απόδειξης της προέλευσης και της αυθεντικότητας των ψηφιακών δεδομένων πρέπει να γίνεται νομικώς αποδεκτή», και
- Την '**αναλυτική προσέγγιση**' (prescriptive approach), σύμφωνα με την οποία «μόνο συγκεκριμένες τεχνολογικές μέθοδοι, οι οποίες ικανοποιούν συγκεκριμένα κριτήρια ασφάλειας και αξιοπιστίας, αναγνωρίζονται 'άμεσα' ως νομικά ισότιμες με τις ιδιόχειρες υπογραφές»

Η **Ευρωπαϊκή Ένωση**, με την Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 1999 'Σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές'(EEL 13/19.1.2000) (εφεξής '**Οδηγία**') ακολούθησε μία μικτή προσέγγιση δύο επιπέδων (*two-tier approach*), η οποία συνδυάζει και τις δύο παραπάνω κατευθύνσεις.

Έτσι, η Ευρωπαϊκή Οδηγία αναγνωρίζει γενικά ως '**ηλεκτρονικές υπογραφές**' -οι οποίες μπορούν να χρησιμοποιηθούν ως 'αποδεικτικά στοιχεία' σε νομικές διαδικασίες, όλα τα: «**δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε, ή λογικά συσχετιζόμενα με, άλλα ηλεκτρονικά δεδομένα και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας**» (ά. 2§1 της Οδηγίας). Ο ορισμός αυτός καλύπτει κάθε ηλεκτρονική μέθοδο απόδειξης της προέλευσης των δεδομένων, από τις πιο 'απλές' (π.χ. απλή αναγραφή του ονόματος του συντάξαντα στο τέλος μιας ηλεκτρονικής επιστολής, αυτόματη σύναψη της ηλεκτρονικής διεύθυνσης αποστολής σε ένα e-mail ή του αριθμού του τηλεφώνου αποστολής σε ένα SMS μήνυμα, κλπ), ως την πιο 'σύνθετες' (π.χ. προηγμένες μέθοδοι κρυπτογράφησης δεδομένων, χρήση βιομετρικών στοιχείων, κλπ), ανεξάρτητα, δηλαδή, από τον βαθμό τεχνικής ασφάλειας που παρέχουν.

Από την κανονιστική πλευρά, η Οδηγία διακρίνει ποιοτικά μία συγκεκριμένη κατηγορία ηλεκτρονικών υπογραφών -αποκαλούμενες συχνά ως **‘αναγνωρισμένες ηλεκτρονικές υπογραφές’**- στην οποία κατηγορία αποδίδει πλήρη και άμεση νομική ισοδυναμία με τις ‘ιδιόχειρες υπογραφές’, σύμφωνα με το ισχύον δίκαιο του κάθε κράτους μέλους. Σε αυτήν την κατηγορία ανήκουν όλες οι: **‘προηγμένες ηλεκτρονικές υπογραφές’** που, επιπλέον, βασίζονται σε **‘αναγνωρισμένο πιστοποιητικό’** και δημιουργούνται από **‘ασφαλή διάταξη δημιουργίας υπογραφής’**.

Ως **‘προηγμένες ηλεκτρονικές υπογραφές’** (οι οποίες στο εθνικό μας δίκαιο –Π.Δ 150/2001-αποκαλούνται και **‘ψηφιακές υπογραφές’**), η Οδηγία προσδιορίζει τις ηλεκτρονικές υπογραφές που ικανοποιούν τις εξής απαιτήσεις: **α)** συνδέονται μονοσήμαντα με τον υπογράφοντα, **β)** είναι ικανές να ταυτοποιήσουν τον υπογράφοντα, **γ)** δημιουργούνται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο, και **δ)** συνδέονται με τα δεδομένα στα οποία αναφέρονται κατά τρόπο ώστε να μπορεί να εντοπιστεί οποιαδήποτε αλλοίωση στα εν λόγω δεδομένα. Οι συγκεκριμένες απαιτήσεις μπορούν να ικανοποιηθούν σήμερα μόνο με την χρήση της τεχνολογίας της **‘ασύμμετρης κρυπτογραφίας’** η οποία κάνει χρήση **ιδιωτικών** (‘δεδομένα δημιουργίας υπογραφής’) και **δημοσίων** (‘δεδομένα επαλήθευσης υπογραφής’) κρυπτογραφικών κλειδιών που χρησιμοποιούνται συμπληρωματικά το ένα προς το άλλο για την παραγωγή και την επαλήθευση της ηλεκτρονικής υπογραφής.

Ως **‘αναγνωρισμένο πιστοποιητικό’** ορίζεται από την Οδηγία η ‘ηλεκτρονική βεβαίωση’ που εκδίδεται από κάποιον ‘Πάροχο Υπηρεσιών Πιστοποίησης’ και η οποία συνδέει μονοσήμαντα τα ‘δεδομένα επαλήθευσης μιας υπογραφής’ (ή ‘δημόσιο κλειδί’) με ένα συγκεκριμένο φυσικό πρόσωπο, τηρώντας κάποιους **βασικούς όρους**.

Τέλος, ως **‘ασφαλής διάταξη δημιουργίας υπογραφής’** ορίζεται το διατεταγμένο υλικό ή / και λογισμικό που χρησιμοποιείται για την εφαρμογή του **‘ιδιωτικού κλειδιού’** (ή, των **‘δεδομένων δημιουργίας υπογραφής’**) από τον υπογράφοντα και το οποίο διασφαλίζει την αξιοπιστία της δημιουργίας της υπογραφής βάσει συγκεκριμένων απαιτήσεων.

Η Οδηγία προβλέπει την ελεύθερη παροχή υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής, **απαγορεύοντας** οποιοδήποτε σύστημα αδειοδότησης της λειτουργίας των Παρόχων Υπηρεσιών Πιστοποίησης (εφεξής, ΠΥΠ), προσδιορίζοντας, όμως τις προϋποθέσεις λειτουργίας και την ευθύνη των ΠΥΠ που εκδίδουν **‘αναγνωρισμένα πιστοποιητικά προς το κοινό’**. Παράλληλα προβλέπει την δυνατότητα **‘Εθελοντικής Διαπίστευσης’** των ΠΥΠ, καθώς και διαδικασία **‘Διαπίστωσης’** της συμμόρφωσης των **‘προϊόντων ηλεκτρονικών υπογραφών’** με τις απαιτήσεις ασφάλειας και αξιοπιστίας της Οδηγίας (βάσει σχετικών ‘γενικώς αναγνωρισμένων προτύπων’) από σχετικούς αρμόδιους φορείς.

Στην Ελλάδα, η πρώτη νομοθετική πρόβλεψη για **‘ψηφιακές υπογραφές’** (οι οποίες ταυτίζονται εννοιολογικά με τις **‘προηγμένες ηλεκτρονικές υπογραφές’** της Οδηγίας) γίνεται ήδη από το **άρθρο 14 του ν. 2672/98** όπου παρέχεται μια αρχική, αλλά περιορισμένη αναγνώρισή τους σε διαδικασίες του δημόσιου τομέα.

Ακολούθησε το **Π.Δ. 150/2001** (ΦΕΚ Α/125 25-6-2001) το οποίο εναρμόνισε το εθνικό μας δίκαιο με την παραπάνω Οδηγία και καθόρισε την **‘Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων’** (ΕΕΤΤ) ως αρμόδια αρχή για την εποπτεία των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης ηλεκτρονικής υπογραφής, καθώς και για την λειτουργία μηχανισμών **‘Εθελοντικής Διαπίστευσης’**

των ΠΥΠ και 'Διαπίστωσης' της συμμόρφωσης των 'προϊόντων ηλεκτρονικής υπογραφής'. Τον Οκτώβριο του 2002, εκδόθηκε το Π.Δ 342/02 το οποίο προσδιορίζει περαιτέρω κάποιους όρους για τη διακίνηση ψηφιακά υπογεγραμμένων 'μηνυμάτων ηλεκτρονικού ταχυδρομείου' στις επικοινωνίες του δημόσιου τομέα.

Τέλος, στο πλαίσιο άσκησης των σχετικών αρμοδιοτήτων της, η ΕΕΤΤ έχει εκδώσει έναν γενικό 'Κανονισμό Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής', καθώς και τρεις Κανονισμούς σχετικά με την 'Εθελοντική Διαπίστευση' των ΠΥΠ, την 'Διαπίστωση' (της συμμόρφωσης με τις απαιτήσεις της Οδηγίας) βασικών 'προϊόντων ηλεκτρονικής υπογραφής' (-βλέπε σχετικά και απάντηση 5), και τον ορισμό των 'Φορέων' που θα προβαίνουν σε σχετικούς ελέγχους και διαπιστεύσεις για λογαριασμό της ΕΕΤΤ.

5.4.2 Πώς λειτουργούν οι προηγμένες ψηφιακές ηλεκτρονικές υπογραφές

Η τεχνολογία της 'ασύμμετρης κρυπτογραφίας, βάσει συγκεκριμένων 'μαθηματικών αλγορίθμων' (π.χ. RSA, DSA, κ.ά.), παράγει τυχαία ζεύγη κρυπτογραφικών 'κλειδιών' (ψηφιακά δεδομένα) τα οποία χαρακτηρίζονται από δύο σημαντικές ιδιότητες:

- το καθένα κλειδί κρυπτογραφεί ψηφιακά δεδομένα τα οποία μπορούν να αποκρυπτογραφηθούν μόνο από το άλλο (συμπληρωματικό του) κλειδί, και
- δεν είναι δυνατό, με τις παρούσες δυνατότητες της τεχνολογίας, να συμπεράνει κανείς ή να αναδημιουργήσει το ένα κλειδί όταν γνωρίζει το άλλο.

Με την τεχνολογία της ασύμμετρης κρυπτογραφίας διατηρώντας μυστικό το ένα κλειδί ως 'ιδιωτικό' ('δεδομένα δημιουργίας υπογραφής') και διανέμοντας ελεύθερα το άλλο κλειδί ως 'δημόσιο' ('δεδομένα επαλήθευσης υπογραφής'), εξασφαλίζουμε ότι όλοι όσοι γνωρίζουν ένα δημόσιο κλειδί μπορούν να 'επαληθεύσουν' μια ψηφιακή υπογραφή που δημιουργείται από τον κάτοχο του αντίστοιχου ιδιωτικού κλειδιού.

Πρέπει να σημειωθεί ότι κατά την 'δημιουργία' μιας 'ψηφιακής υπογραφής' δεν κρυπτογραφούνται τα 'προς υπογραφήν' δεδομένα, αλλά μία μικρή μαθηματική 'σύνοψη' ('digest') τους, η οποία παράγεται από την χρήση 'μονόδρομων αλγορίθμων κατακερματισμού δεδομένων' ('one-way hashing algorithms' -π.χ. MD5, SHA-1 κ.ά.). Αυτή η 'σύνοψη' των δεδομένων, κρυπτογραφείται με το ιδιωτικό κλειδί του υπογράφοντα και επισυνάπτεται (πιθανώς μαζί και με άλλες χρήσιμες σχετικές πληροφορίες, π.χ. χρησιμοποιούμενοι αλγόριθμοι, εφαρμοζόμενη 'πολιτική υπογραφής', κ.ά.), στα αρχικά δεδομένα, αποτελώντας την 'προηγμένη ηλεκτρονική υπογραφή' τους.

Κατά την αντίστροφη διαδικασία της 'επαλήθευσης' (verification) μιας ψηφιακής υπογραφής, εφαρμόζεται στα υπό εξέταση δεδομένα ο ίδιος 'αλγόριθμος κατακερματισμού' που χρησιμοποιήθηκε κατά την 'υπογραφή' τους. Έτσι, η νέα 'σύνοψη' που παράγεται, συγκρίνεται με την αντίστοιχη 'σύνοψη' που προέρχεται από την αποκρυπτογράφηση της 'προηγμένης ηλεκτρονικής υπογραφής' με το υποδεικνυόμενο δημόσιο κλειδί του υπογράφοντα εάν ταυτίζονται οι δύο σνότητες τότε η υπογραφή 'επαληθεύεται' και επιβεβαιώνεται ότι:

1. τα δεδομένα υπογράφηκαν από τον κάτοχο του σχετικού ιδιωτικού κλειδιού

2. τα αρχικά δεδομένα δεν έχουν αλλοιωθεί.

Παρόλα αυτά διατηρείται ακέραια η **ανάγκη**, -ιδίως σε ανοικτές εφαρμογές με πολλαπλούς ή ακόμη και άγνωστους αποδέκτες-, για την ύπαρξη μιας **“Έμπιστης Τρίτης Οντότητας”** που ονομάζεται **‘Πάροχος Υπηρεσιών Πιστοποίησης’** (ΠΥΠ) η οποία, επιπλέον, πιστοποιεί προς οποιοδήποτε τρίτο αποδέκτη μιας ψηφιακής υπογραφής:

3. την καταγραφή (registration) της ταυτότητας του κατόχου του ιδιωτικού κλειδιού που αντιστοιχεί στο συγκεκριμένο δημόσιο κλειδί, και

4. τη πραγματική κατοχή του σχετικού ιδιωτικού κλειδιού από τον πιστοποιούμενο (*proof of possession*).

Η παραπάνω πιστοποίηση (προς χρήση από τους αποδέκτες της ηλεκτρονικής υπογραφής) γίνεται με την έκδοση **‘ψηφιακών πιστοποιητικών’** τα οποία περιέχουν το δημόσιο κλειδί και τα στοιχεία ταυτοποίησης του κατόχου του πιστοποιητικού, και τα οποία υπογράφονται ψηφιακά από τον ‘εκδότη’ τους. Η υποδομή με την οποία ένας ΠΥΠ εκδίδει, υπογράφει, δημοσιεύει και υποστηρίζει ‘τυποποιημένες ηλεκτρονικές βεβαιώσεις’ (πιστοποιητικά) για τα κρυπτογραφικά κλειδιά των συνδρομητών του (υποκειμένων πιστοποίησης) ονομάζεται **‘Υποδομή Δημοσίου Κλειδιού’** (*Public Key Infrastructure – ‘PKI’*).

Επειδή τα **‘πιστοποιητικά δημοσίων κλειδιών’** (*public key certificates*) που εκδίδει ένας ΠΥΠ προς τις ενδιαφερόμενους τελικούς χρήστες ή τελικές ‘οντότητες’, είναι και αυτά μια μορφή **‘ηλεκτρονικών εγγράφων’**, επιβάλλεται να φέρουν και αυτά την ‘ψηφιακή υπογραφή’ του εκδότη τους. Αυτό προϋποθέτει ότι και ο ίδιος ο Εκδότης-ΠΥΠ διαθέτει το δικό του ζεύγος κρυπτογραφικών κλειδιών υπογραφής, το οποίο πρέπει εξίσου να υποστηρίζεται από σχετικό πιστοποιητικό δημοσίου κλειδιού -που κι αυτό, με την σειρά του, πρέπει να είναι υπογεγραμμένο ψηφιακά. Η σχηματιζόμενη αλληλουχία (αλυσίδα) πιστοποιητικών. τερματίζεται με ένα τελικό και αξιόπιστο δημοσιευμένο **‘αυτοϋπογραφόμενο πιστοποιητικό’** (*self-signed certificate*) που εκδίδεται από τον **‘Θεμελιώδη Εκδότη Πιστοποιητικών’** (*Root Certification Authority* ή *‘Root CA’*) του ΠΥΠ και το οποίο αποτελεί την ‘κορυφή της πυραμίδας’ μιας υποδομής ‘PKI’.

Η ιεραρχική πιστοποίηση δημόσιων κλειδιών των συναλλασσόμενων-τελικών οντοτήτων από μια τεκμηριωμένη υποδομή ‘PKI’ ενός (ή περισσότερων) ΠΥΠ, θεωρείται ιδανική για την έκδοση **‘αναγνωρισμένων πιστοποιητικών’**, τα οποία παρέχουν ικανοποιητικές εγγυήσεις στις συναλλαγές -ακόμη και μεταξύ αγνώστων.

Άλλη ευρείας χρήσης εναλλακτική τεχνολογία ‘προηγμένης ηλεκτρονικής υπογραφής’ βασίζεται στα ‘αυτό-ϋπογραφόμενα’ πιστοποιητικά που εκδίδονται από το ίδιο τον (τελικό) χρήστη-κάτοχο ζεύγους κρυπτογραφικών κλειδιών, ο οποίος λειτουργεί και ως αποδέκτης αντίστοιχων πιστοποιητικών. Τα πιστοποιητικά αυτά δημοσιεύονται από τον εκδότη τους σε έναν ή περισσότερους δημόσιους **‘εξυπηρετητές κλειδιών’** (*key servers*) όπου αξιολογούνται και υπογράφονται και από άλλους χρήστες, οι οποίοι, μέσω διαπροσωπικής επικοινωνίας τους με το υποκείμενο-κάτοχό τους, αλληλο-επιβεβαιώνουν και πιστοποιούν την συγκεκριμένη συσχέτιση. Αυτή η μέθοδος πιστοποίησης, η οποία είναι ήδη **πολύ διαδεδομένη διεθνώς** -ιδίως σε κλειστές ομάδες προγραμματιστών Η/Υ και γενικότερα σε κοινότητες με κοινές δραστηριότητες, π.χ. σωματεία, σύλλογοι κ.λπ.- αποκαλείται **‘Pretty Good Privacy’** (PGP) και βασίζεται στην δημιουργία ενός (αποκεντρωμένου).

‘δικτύου εμπιστοσύνης’ (*‘web of trust’*) που αναπτύσσεται με την μεταβίβαση της εμπιστοσύνης μεταξύ των χρηστών της.

Η μέθοδος PGP και οι παραλλαγές της (*GPG, OpenPGP, κ.λ.π.*) δημιουργούν μεν **‘ψηφιακές υπογραφές’** (δηλαδή υπογραφές που ικανοποιούν τους όρους της νομοθεσίας για **‘προηγμένες’** ηλεκτρονικές υπογραφές), **όμως δεν μπορούν να παράξουν ‘αναγνωρισμένες’ ηλεκτρονικές υπογραφές** -εφόσον δεν υποστηρίζονται από ένα **‘αναγνωρισμένο πιστοποιητικό’**. Επειδή κανένας από τους πιστοποιούντες δεν αναλαμβάνει ιδιαίτερη ευθύνη και υποχρεώσεις έναντι των τρίτων, η μέθοδος αυτή **δεν πληροί** προϋποθέσεις ασφάλειας για διενέργεια **‘σημαντικών συναλλαγών’** μεταξύ αγνώστων, εφόσον δεν εξασφαλίζει **‘επαρκείς αποδείξεις’** και δεν παρέχει εγγυήσεις ως προς την πραγματική ταυτότητα των συναλλασσομένων.

5.4.3 Τι εξοπλισμός απαιτείται για τη δημιουργία και την επαλήθευση των η - υπογραφών

Για την δημιουργία μιας ψηφιακής υπογραφής πάνω σε συγκεκριμένα ηλεκτρονικά δεδομένα, θα πρέπει κάποιος, -εκτός από τα απαραίτητα κρυπτογραφικά κλειδιά και το αντίστοιχο έγκυρο πιστοποιητικό-, να διαθέτει και μια ολοκληρωμένη **‘διάταξη δημιουργίας υπογραφής’** η οποία να απαρτίζεται από κατάλληλη σύνθεση υλισμικού (*hardware*) και λογισμικού (*software*). Στην διάταξη αυτή περιλαμβάνονται ο **‘φορέας’** των κρυπτογραφικών κλειδιών (π.χ. σκληρός δίσκος υπολογιστή, έξυπνη κάρτα, USB token, κ.λπ.), ο τυχόν απαραίτητος **‘αναγνώστης του φορέα’** αυτού (π.χ. αναγνώστης έξυπνης κάρτας, θύρα USB, κ.λπ.), το **‘τερματικό επικοινωνίας’** του χρήστη (π.χ. PC, pda, smart phone, κ.λπ.), τα **‘λειτουργικά συστήματα’** και οι **‘οδηγοί’** (*drivers*) των συσκευών αυτών, καθώς και το **‘λογισμικό επικοινωνίας’** (*interface*) του χρήστη που χρησιμοποιείται για τη δημιουργία της ηλεκτρονικής υπογραφής.

Ιδίως για την δημιουργία **‘αναγνωρισμένης’** ηλεκτρονικής υπογραφής, η νομοθεσία απαιτεί την χρήση **‘ασφαλούς διάταξης δημιουργίας υπογραφής’** (α.δ.δ.υ.). Ως τέτοια προσδιορίζεται (*Οδηγίας και Π.Δ 150/2001*) η **‘διάταξη’** η οποία, **-μέσω ενδεδειγμένων τεχνικών και διαδικαστικών μέσων-**, διασφαλίζει τουλάχιστον ότι τα **‘δεδομένα δημιουργίας υπογραφής’** (*ιδιωτικά κλειδιά*) που χρησιμοποιούνται για την παραγωγή υπογραφών’:

α) **«απαντούν, κατ’ ουσίαν, μόνο μια φορά και ότι το απόρρητο είναι διασφαλισμένο»** -το οποίο σημαίνει ότι τα σχετικά κρυπτογραφικά κλειδιά πρέπει να δημιουργούνται με τους κατάλληλους αλγόριθμους δημιουργίας τυχαίων κωδικών, είτε απευθείας μέσα σε συσκευή του χρήστη, είτε από κατάλληλες κρυπτογραφικές μονάδες του ΠΥΠ οι οποίες μεταφέρουν άμεσα τα δημιουργηθέντα ιδιωτικά κλειδιά σε προσωπικές συσκευές του χρήστη για τον οποίο προορίζονται, χωρίς να τα εκθέτουν ή να διατηρούν αντίγραφα τους.

β) **«δεν μπορούν, με εύλογη βεβαιότητα, να αντληθούν από αλλού και ότι η υπογραφή προστατεύεται από πλαστογραφία με τα μέσα της σύγχρονης τεχνολογίας»** -όρος που, εκτός από την απαγόρευση της διατήρησης με οποιονδήποτε τρόπο αντιγράφου του ιδιωτικού κλειδιού, στην ουσία του επιβάλλει την χρήση της τεχνολογίας ασύμμετρης κρυπτογραφίας.

γ) **«μπορούν να προστατεύονται αποτελεσματικά από τον νόμιμο υπογράφοντα κατά της χρησιμοποίησης από τρίτους»** -που σημαίνει ότι τα ιδιωτικά κλειδιά δεν πρέπει να μπορούν να εξαχθούν ή / και να αντιγραφούν από τον φορέα τους, ούτε να

ενεργοποιηθούν χωρίς την προηγούμενη χρήση μιας επιπλέον 'μεθόδου επιβεβαίωσης της ταυτότητας' του χρήστη (π.χ. χρήση μυστικού κωδικού αναγνώρισης (PIN) ή / και ανάγνωση βιομετρικών δεδομένων του δικαιούχου).

Παράλληλα, η νομοθεσία ορίζει ότι οι 'α.δ.δ.υ.' δεν πρέπει να μεταβάλλουν τα προς υπογραφή δεδομένα, ούτε να εμποδίζουν την εμφάνιση των δεδομένων αυτών στον υπογράφοντα πριν από τη διαδικασία υπογραφής (επιβάλλεται δηλαδή η αρχή '**What You See Is What You Sign**' ή '**WYSIWYS**').

Η έως σήμερα **προτυποποίηση** για την εξειδίκευση των απαιτήσεων για 'ασφαλείς διατάξεις δημιουργίας υπογραφής' έχει δώσει ιδιαίτερη έμφαση στην ασφάλεια των 'συσκευών δημιουργίας κρυπτογραφικών κλειδιών' (*key generation systems*) καθώς και των 'τελικών φορέων' τους, που συνήθως είναι μια 'έξυπνη κάρτα' (*smart card*) ή άλλη αντίστοιχη συσκευή (π.χ. *USB Token*).

Αντίστοιχα, για την επαλήθευση (*verification*) των ψηφιακών υπογραφών και τον **έλεγχο της εγκυρότητας** (*validation*) των σχετικών πιστοποιητικών, απαιτείται μια ανάλογη διάταξη, η οποία, εκτός του 'τερματικού επικοινωνίας' του χρήστη και του κατάλληλου 'λογισμικού', θα πρέπει, επιπλέον, να διαθέτει και την δυνατότητα πρόσβασης –*είτε με 'on line' σύνδεση, είτε και με συχνές 'off-line' ενημερώσεις*- σε επικαιροποιημένες πληροφορίες εγκυρότητας ή / και ανάκλησης πιστοποιητικών τις οποίες δημοσιεύει ο εκάστοτε εκδότης (ΠΥΠ) τους. Για τις '**διατάξεις επαλήθευσης υπογραφής**' η Οδηγία 99/93/EK '*συστήνει*' προς τα κράτη-μέλη την συνεργασία τους για την ανάπτυξη συστημάτων τα οποία θα πρέπει να διασφαλίζουν τόσο την αξιοπιστία τους, όσο και την ορθή πληροφόρηση του επαληθεύοντα ως προς τα στοιχεία και τα αποτελέσματα της επαλήθευσης (Παράρτημα IV).

5.4.4 Τι πρέπει να προσέχει ο 'υπογράφων' και τι ο 'αποδέκτης' relying party των ηλεκτρονικών υπογραφών

Τόσο ο **υπογράφων** όσο και ο **αποδέκτης** μιας ηλεκτρονικής υπογραφής, πρέπει, κατ' αρχήν, να κατανοούν τον τρόπο χρήσης και λειτουργίας των ηλεκτρονικών υπογραφών που χρησιμοποιούν. Πρέπει, επίσης, να λάβουν γνώση όλων των σχετικών όρων στα κείμενα που τους παρέχει ο ΠΥΠ (π.χ. *Σύμβαση Συνδρομητή με τον ΠΥΠ, Πολιτική Πιστοποιητικού κ.λπ.*) διότι εκεί αναγράφονται όλοι οι όροι χρήσης και οι περιορισμοί του πιστοποιητικού που υποστηρίζει την συγκεκριμένη ψηφιακή υπογραφή.

Ειδικότερα ο '**υπογράφων**' ('*κάτοχος*' των κρυπτογραφικών κλειδιών και '*υποκείμενο*' του σχετικού πιστοποιητικού τους) θα πρέπει να συμμορφώνεται πλήρως με τους όρους της '**συνδρομητικής σύμβασης**' που σύναψε με τον ΠΥΠ για την απόκτηση του σχετικού πιστοποιητικού του, διότι, σε αντίθετη περίπτωση, είναι πιθανόν να επωμισθεί ο ίδιος την ευθύνη για την οποιαδήποτε τυχόν 'πλημμέλεια' των συναλλαγών που θα πραγματοποιηθούν με την χρήση της σχετικής ηλεκτρονικής υπογραφής του. Οι **βασικότερες υποχρεώσεις** του υπογράφοντα οι οποίες περιλαμβάνονται, συνήθως, σε όλες τις τυποποιημένες σχετικές '**Συνδρομητικές Συμβάσεις**' που συντάσσουν οι ΠΥΠ, είναι οι εξής:

Να δηλώνει πραγματικά και ενημερωμένα στοιχεία της ταυτότητάς του κατά την αίτησή του για την έκδοση του σχετικού πιστοποιητικού ηλεκτρονικής υπογραφής του

στην 'Υπηρεσία Εγγραφής' του ΠΥΠ και να ελέγχει την ορθή μεταφορά τους στο πιστοποιητικό, πριν το χρησιμοποιήσει.

- Να τηρεί με επιμέλεια την μυστικότητα και την αποκλειστική χρήση των σχετικών ιδιωτικών κλειδιών του ('μη έκθεση σε τρίτους'),
- Να ζητά από τον ΠΥΠ την ανάκληση (ή την αναστολή) του σχετικού πιστοποιητικού του εάν βεβαιωθεί για (ή υποψιασθεί) οποιαδήποτε έκθεση των ιδιωτικών κλειδιών του σε τρίτους, καθώς και στην περίπτωση που απολέσει τον φορέα ή / και τον έλεγχο των ιδιωτικών κλειδιών του.
- Να χρησιμοποιεί τα συγκεκριμένα κρυπτογραφικά κλειδιά του μόνο στις επιτρεπόμενες για το σχετικό πιστοποιητικό τους χρήσεις και να μην υπερβαίνει στις σχετικές συναλλαγές του τα τυχόν 'όρια' που προβλέπονται από την σύμβαση και την εφαρμοζόμενη Πολιτική του συγκεκριμένου πιστοποιητικού.

Από την άλλη πλευρά, ο **'αποδέκτης'** μιας ηλεκτρονικής υπογραφής (*relying party*), πριν βασισθεί στα περιεχόμενα του σχετικού πιστοποιητικού (*ώστε να διαμορφώσει συγκεκριμένη πεποίθηση για ένα γεγονός ή να προβεί σε μια σε μια σχετική πράξη*), θα πρέπει να ελέγξει και να αποδεχτεί τους 'όρους χρήσης' του πιστοποιητικού, οι οποίοι, συνήθως, αναφέρονται συνοπτικά σε μια τυποποιημένη και δημοσιευμένη από τον ΠΥΠ **'Σύμβαση Αποδέκτη'** (*Relying Party Agreement*) ή / και ενσωματώνονται (μαζί με άλλους όρους) στην προσδιοριζόμενη **'Πολιτική Πιστοποιητικού'** (*Certificate Policy*). Για να στηριχθεί **'εύλογα'** στην ηλεκτρονική υπογραφή κάποιου τρίτου, ένας αποδέκτης της **θα πρέπει, πρώτα, να εξασφαλίσει ότι το συγκεκριμένο πιστοποιητικό του υπογράφοντα** (που επαληθεύει την υπογραφή):

- είναι **"αυθεντικό"**, με την έννοια ότι υπάρχει τουλάχιστον μία αλληλουχία πιστοποιητικών (με όλους τους μεσολαβούντες υπό-εκδότες) η οποία να καταλήγει σε μια αξιόπιστη -γι' αυτόν- 'ρίζα εμπιστοσύνης' (*συνήθως το αυτό-υπογραφόμενο πιστοποιητικό 'Root CA' ενός γνωστού ΠΥΠ*).
- είναι **"έγκυρο"**, δηλαδή ότι δεν έχει λήξει ή ανακληθεί η ισχύς του. Αυτό σημαίνει ότι ο αποδέκτης θα πρέπει να ελέγξει, όχι μόνο την 'διάρκεια ισχύος' ('ημερομηνία λήξης') που αναγράφεται μέσα στο ίδιο το εξεταζόμενο πιστοποιητικό, αλλά και τις σχετικές *'Λίστες Ανακληθέντων Πιστοποιητικών'* που δημοσιεύει ο ίδιος ο εκδότης του. Ο έλεγχος αυτός μπορεί να γίνει *είτε* μέσω ειδικών αυτοματοποιημένων εφαρμογών που εμπιστεύεται ο χρήστης, *είτε* μέσω σχετικής *'Απ' ευθείας Υπηρεσίας Ενημέρωσης Ανάκλησης Πιστοποιητικών'* (*'Online Certificate Status Protocol' - 'OCSP'*) που πιθανώς να παρέχει ο ΠΥΠ ή τρίτος.
- είναι **"κατάλληλο"** για την συναλλαγή ή την χρήση στην οποία ο αποδέκτης του πρόκειται να προβεί. Για να θεωρηθεί "κατάλληλο" ένα πιστοποιητικό θα πρέπει η προτιθέμενη χρήση του να μην απαγορεύεται από την σχετική *'Πολιτική Πιστοποιητικού'*. Επίσης, εάν από τον τύπο της επιχειρούμενης συναλλαγής έχει καθοριστεί ή / και πρέπει να ακολουθηθεί μια συγκεκριμένη *'Πολιτική (ηλεκτρονικής) Υπογραφής'*, τότε η χρήση του συγκεκριμένου πιστοποιητικού θα πρέπει να προβλέπεται ή, έστω, να επιτρέπεται από την εφαρμοζόμενη *'Πολιτική Υπογραφής'*.

Η 'Πολιτική Υπογραφής' (Signature Policy) είναι ένα συγκεκριμένο (και ταυτοποιημένο με μοναδικό κωδικό 'OID') κείμενο το οποίο αναφέρει διεξοδικά όλους τους απαραίτητους όρους για την 'έγκυρη' εναπόθεση ή / και επαλήθευση μιας ηλεκτρονικής υπογραφής, οι οποίοι εφαρμόζονται σε έναν καθορισμένο κύκλο συναλλαγών. Η 'Πολιτική Υπογραφής' επιλέγεται με συμφωνία των μερών ή, συνηθέστερα, επιβάλλεται από την πλευρά του 'αποδέκτη' των υπογραφών ως 'γενικός όρος συναλλαγών'. Αποτελώντας, μάλιστα, και αντικείμενο πρόσφατης προτυποποίησης από τους αρμόδιους ευρωπαϊκούς οργανισμούς προτυποποίησης, η 'Πολιτική Υπογραφής' μπορεί να προσδιορίζει, -εκτός από τα αποδεκτά είδη / πολιτικές πιστοποιητικών-, τις τυχόν 'απαραίτητες ιδιότητες' του υπογράφοντα, την πιθανή υποχρέωση για εναπόθεση 'αξιόπιστης χρονοσήμανσης' στην δημιουργηθείσα υπογραφή, την ανάγκη για 'επανέλεγχο της ανάκλησης' του πιστοποιητικού πριν την οριστική αποδοχή της υπογραφής, κάποιες συγκεκριμένες 'ρίζες εμπιστοσύνης' που απαιτείται να χρησιμοποιηθούν για την επαλήθευση των πιστοποιητικών, κ.ά.

5.4.5 Ποιες είναι σήμερα οι σημαντικότερες εφαρμογές και ποιες οι προοπτικές των ηλεκτρονικών υπογραφών

Σε διεθνές επίπεδο, η χρήση των ηλεκτρονικών υπογραφών και των ηλεκτρονικών πιστοποιητικών ήδη πλαισιώνει και παρέχει υψηλότερα επίπεδα ασφάλειας σε συναλλαγές διαφόρων τύπων όπως:

- Τυποποιημένες εφαρμογές ηλεκτρονικών συναλλαγών, όπως η ηλεκτρονική ανταλλαγή δεδομένων (*Electronic Data Interchange -EDI*)
- Ηλεκτρονικά τιμολόγια που συντάσσονται σε μορφή άλλη από EDI
- Ηλεκτρονικές δημόσιες προμήθειες
- Ηλεκτρονική ψηφοφορία
- Συστήματα ηλεκτρονικών πληρωμών (π.χ. πιστωτικές κάρτες EuroPay, MasterCard & VISA μέσω του κοινού πρωτοκόλλου τους 'EMV')
- Ηλεκτρονικά 'διαβατήρια' και ηλεκτρονικές 'ταυτότητες' (γενικής ή ειδικής χρήσης -π.χ. 'ναυτικές διεθνείς ταυτότητες') που συνήθως φέρουν ενσωματωμένα και κάποια 'βιομετρικά στοιχεία' (φωτογραφία, δακτυλικά αποτυπώματα, κ.λ.π.) του κατόχου τους
- Υπηρεσίες ασφαλούς ηλεκτρονικού ταχυδρομείου (*S/MIME*)
- Συστήματα 'υπογραφής αυθεντικότητας' διακινούμενου λογισμικού (π.χ. *Microsoft Authenticode*)
- Κλειστές υποδομές 'PKI' για εφαρμογές ασφαλείας μεγάλων οργανισμών (π.χ. *NATO*)
- Πιστοποίηση της ταυτότητας 'εξυπηρετητών Διαδικτύου' (*web servers*), κ.ά.

Στην Ευρωπαϊκή Ένωση, εκτός από πλήθος άτυπων εφαρμογών στις τηλεπικοινωνίες, τραπεζικές εφαρμογές, εμπόριο κλπ, έχουν θεσμοθετηθεί και βρίσκονται ήδη σε λειτουργία 'τυπικές εφαρμογές' των η-υπογραφών, οι προϋποθέσεις των οποίων πηγάζουν από το νόμο. Τα '**ηλεκτρονικά δελτία ταυτότητας**' σε χώρες όπως το Βέλγιο, Φινλανδία Ιταλία, Εσθονία και αλλού, τα οποία χρησιμοποιούν την τεχνολογία PKI σε συνδυασμό με 'έξυπνες κάρτες', αποτελούν ένα παράδειγμα τέτοιων τυπικών εφαρμογών.

Ένας άλλος τομέας εφαρμογής ηλεκτρονικών υπογραφών στην ΕΕ είναι τα '**ηλεκτρονικά τιμολόγια**', τα οποία σύμφωνα και με την Ευρωπαϊκή Οδηγία

01/115/EK, εφόσον φέρουν ηλεκτρονική υπογραφή μπορούν να γίνονται αποδεκτά από τις αρμόδιες αρχές των κρατών μελών.

Άλλη εφαρμογή αποτελούν οι **‘ηλεκτρονικές δημόσιες προμήθειες’** στο πλαίσιο των σχετικών σχεδίων Οδηγιών της ΕΕ. Επίσης, θεσμικά όργανα της Ευρωπαϊκής Ένωσης, όπως η **‘Υπηρεσία Επίσημων Δημοσιεύσεων’**, σχεδιάζουν την χρήση των ηλεκτρονικών υπογραφών για τα έγγραφα που εκδίδουν σε ηλεκτρονική μορφή (π.χ. την *Εφημερίδα των Ευρωπαϊκών Κοινοτήτων, τα περιεχόμενα των νομικών βάσεων δεδομένων CELEX, EUR-Lex & OEIL, τη δημοσίευση προκηρύξεων, κ.λπ.*).

Στην **Ελλάδα**, μια από τις πρώτες εφαρμογές νομικά έγκυρης ηλεκτρονικής υπογραφής επίσημων εγγράφων, η οποία λειτουργεί ήδη από το 2002, είναι το σύστημα ασφαλούς ηλεκτρονικής επικοινωνίας του **Χρηματιστηρίου Αθηνών (ΧΑ)** με τις εισηγμένες σ’ αυτό εταιρίες. Το σύστημα αυτό ονομάζεται **“ΕΡΜΗΣ”** (ή **‘H.E.R.M.E.S.’ -Hellenic Exchanges Remote MEssaging Services**) και βασίζεται στις ψηφιακές υπογραφές εξουσιοδοτημένων φυσικών προσώπων (‘εκπροσώπων’ των εισηγμένων), στα οποία παρέχονται δύο διαφορετικά ζεύγη κλειδιών και πιστοποιητικών (ένα για την ταυτοποίησή τους στο σύστημα και ένα για την ‘αναγνωρισμένη ηλεκτρονική υπογραφή’ τους στις υποβαλλόμενες ηλεκτρονικά δηλώσεις τους) εναποθετημένα σε μια προσωποποιημένη ‘έξυπνη κάρτα’.

Παράλληλα, η υποστήριξη και η χρήση ηλεκτρονικών υπογραφών και πιστοποιητικών προβλέπεται στις προδιαγραφές των περισσότερων έργων που προκηρύχθηκαν ή προκηρύσσονται στα πλαίσια του προγράμματος για την **‘Κοινωνία της Πληροφορίας’** και των σχετικών **‘Επιχειρησιακών Προγραμμάτων’** των φορέων του ευρύτερου Δημόσιου Τομέα. Χαρακτηριστικά παραδείγματα αποτελούν τα έργα ψηφιοποίησης του **Ποινικού Μητρώου** του Υπουργείου Δικαιοσύνης, οι σχεδιαζόμενες εφαρμογές για την ηλεκτρονική κατάθεση **Εμπορικών Σημάτων** καθώς και το σύστημα ηλεκτρονικών **Δημόσιων Προκηρύξεων & Προμηθειών** στο Υπουργείο Ανάπτυξης (Γ.Γ. Εμπορίου), τα σχέδια για ηλεκτρονικές υπογραφές των ηλεκτρονικών **Φύλλων της Εφημερίδας της Κυβερνήσεως (ΦΕΚ)** του Εθνικού Τυπογραφείου, η πλήρης ηλεκτρονική λειτουργία των ΚΕΠ (**e-ΚΕΠ**), κ.ά. Σημαντικότερη εξέλιξη προς την γενικευμένη χρήση ηλεκτρονικών υπογραφών στην Ελληνική Δημόσια Διοίκηση θα αποτελέσει ιδίως η υλοποίηση και η ολοκλήρωση του **‘Υποέργου 9’** του -*ήδη σε εξέλιξη*- συνολικού έργου **‘Σύζευξις’**, όπου προβλέπεται η χρήση **‘Υποδομής Δημοσίου Κλειδιού’ (PKI)** και η πιστοποίηση ψηφιακών υπογραφών για έναν μεγάλο αριθμό (50.000) δημοσίων υπαλλήλων, οι οποίοι θα μπορούν να εκδίδουν, να υπογράφουν και να διακινούν ‘επίσημα’ ηλεκτρονικά δημόσια έγγραφα.

5.5 ΠΑΡΑΔΕΙΓΜΑΤΑ ΑΣΥΜΜΕΤΡΩΝ ΤΕΧΝΙΚΩΝ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

ΤΑ ΠΡΟΤΥΠΑ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΟΥΝΤΑΙ ΓΙΑ ΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΛΗΡΩΜΕΣ

- a) **Secure Socket Layer (ssl)**
- b) **Transport Layer Security (tls)**
- c) **Secure Electronic Transaction (set)**

Secure Socket Layer and Transport Layer Security: Η τεχνολογία τύπου SSL, είναι ένα από τα πιο γνωστά πρωτόκολλα επικοινωνίας που εξυπηρετούν μεθόδους ασύμμετρης κρυπτογράφησης. Συγκεκριμένα χρησιμοποιείται για να εξασφαλίσει

ασφαλή σύνδεση μεταξύ του χρήστη και του κεντρικού διακομιστή. Το πρωτόκολλο SSL παρέχει ακεραιότητα και ασφάλεια στα δεδομένα που διακινούνται, μεταξύ του καταναλωτή και του εμπόρου. Πρώτα υλοποιήθηκε από την εταιρία Netscape αργότερα υιοθετήθηκε από την Internet Engineering Task Force (IETF) σαν γενικό πρωτόκολλο ασφαλείας. Χρησιμοποιείται επίσης ευρέως και σε πολλά συστήματα ηλεκτρονικής τραπεζικής (Internet Banking). Εικονικά θα μπορούσαμε να πούμε ότι τα περισσότερα προγράμματα προβολής ιστοσελίδων (Web Browsers), χρησιμοποιούν την τεχνολογία SSL για να αυθεντικοποιούν και να κρυπτογραφούν τα δεδομένα που διακινούνται. Τέλος πρέπει να τονίσουμε ότι η τεχνολογία SSL, δεν παρέχει το χαρακτηριστικό συνολικής ασφαλείας, περί της απόδειξης πραγματοποίησης της συναλλαγής (non-repudiation). Η μετεξέλιξη του πρωτοκόλλου επικοινωνίας SSL αναφέρεται να είναι το Transport Layer Security (TLS).

Το SSL είναι ένα ευέλικτο, γενικού σκοπού σύστημα κρυπτογράφησης για την προστασία της επικοινωνίας μέσω WEB και παρέχει:

- **Πιστοποίηση (Authentication):** Γίνεται επαλήθευση ότι ένας Δικτυακός τόπος ανήκει στον πραγματικό κάτοχο και όχι σε κάποιον τρίτο.
- **Ακεραιότητα μηνυμάτων (Message integrity):** Κατά την διάρκεια αποστολής ενός μηνύματος, οι υπολογιστές του αποστολέα και του παραλήπτη δημιουργούν ένα κωδικό βασισμένο στο περιεχόμενο του μηνύματος. Εάν έστω και ένα μικρό μέρος του μηνύματος παραποιηθεί κατά την διάρκεια μετάδοσής του ο κωδικός του υπολογιστή –παραλήπτη θα είναι διαφορετικός με αποτέλεσμα το μήνυμα να απορριφθεί.
- **Απόκρυψη δεδομένων (Data Encryption):** Το πρωτόκολλο SSL κρυπτογραφεί όλες τις πληροφορίες που μεταδίδονται μεταξύ ενός web server και των web browsers των πελατών.

Πρωτόκολλο ασφαλών συναλλαγών (SET): Το πρωτόκολλο SET ρυθμίζει τη μετάδοση κρυπτογραφημένων πληροφοριών για πληρωμές από πιστωτικές κάρτες μέσω του δικτύου. Το πρωτόκολλο, που ανακοινώθηκε τον Φεβρουάριο του 1996 από τους δυο μεγαλύτερους οργανισμούς πιστωτικών καρτών, VISA και Mastercard, περιλαμβάνει μια σειρά από απλές τεχνικές προδιαγραφές για την προστασία πληρωμών με πιστωτικές κάρτες μέσα από το INTERNET και άλλα ανοικτά δίκτυα. Στην κοινοπραξία των επιχειρήσεων που ανέπτυξαν και στηρίζουν το πρωτόκολλο SET ανήκουν ονόματα όπως Microsoft, Netscape, GTE, IBM, SAIC, Terisa Systems και Verisign. Το πρωτόκολλο SET βασίζεται σε κρυπτογράφηση με δημόσιο κλειδί και τεχνολογία πιστοποίησης της εταιρίας RSA Data Security. Οι στόχοι της ασφαλείας πληρωμών είναι οι εξής: πιστοποίηση της ταυτότητας εμπόρων και πελατών, εξασφάλιση του απορρήτου των πληρωμών, προστασία των δεδομένων από παραποίηση ή πλαστογράφηση, και ακριβής ορισμός των αλγορίθμων και πρωτοκόλλων που θα χρησιμοποιούνται για αυτές τις υπηρεσίες ασφαλείας.

Ένα από τα πλεονεκτήματα του INTERNET είναι ότι επιτρέπει στους χρήστες να βρίσκουν πληροφορίες όλο το 24-ωρο και ανεξάρτητα από τη γεωγραφική απόσταση, το αντίτιμο όμως είναι ο αυξημένος κίνδυνος υποκλοπής και απάτης. Όταν ο "άλλος" με τον οποίο γίνεται μια συναλλαγή δεν είναι παρά ένα όνομα στην οθόνη του υπολογιστή, είναι πολύ δύσκολο να ελεγχθεί αν ο αριθμός λογαριασμού που δίνει είναι γνήσιος ή έγκυρος. Πώς μπορεί ένας έμπορος να αισθάνεται άνετα όταν πρέπει να δεχθεί έναν αριθμό πιστωτικής κάρτας χωρίς καμία άλλη

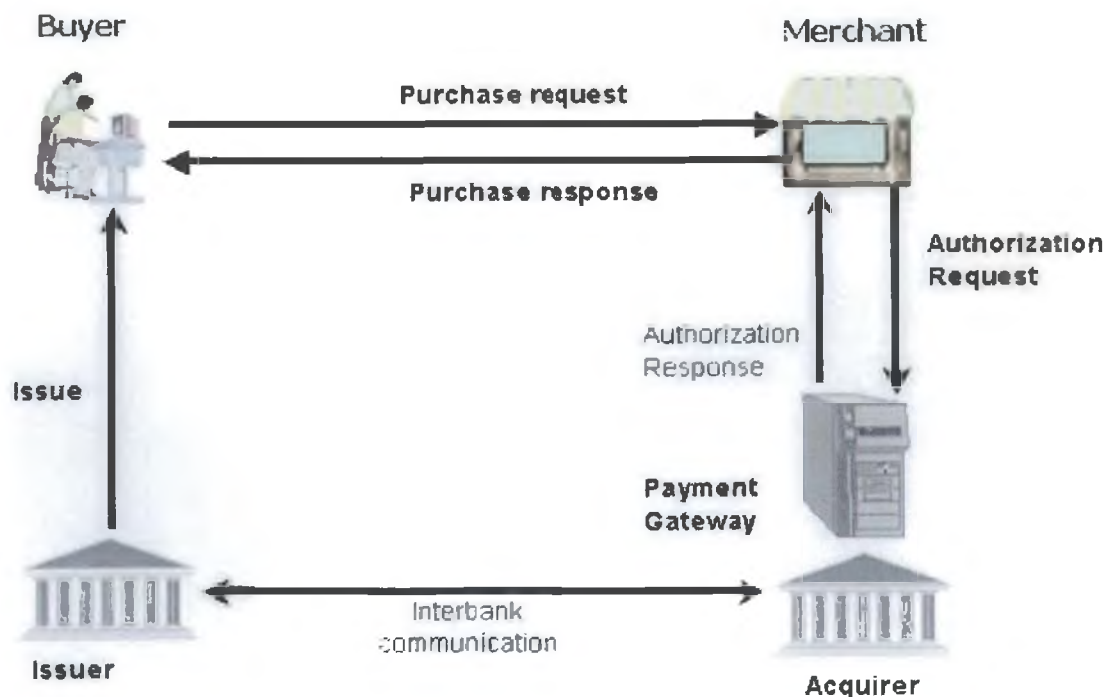
επιβεβαίωση της ταυτότητας του αγοραστή; Όμοια, πώς μπορεί ο πελάτης να εμπιστευτεί έναν έμπορο που ποτέ στη ζωή του δεν έχει συναντήσει;

Ένας τρόπος για την αύξηση της ασφάλειας και της αμοιβαίας εμπιστοσύνης των δυο συναλλασσόμενων πλευρών είναι η πιστοποίηση της ταυτότητας αυτών που συναλλάσσονται. Πολλές επιχειρήσεις που δραστηριοποιούνται στον τομέα της υποστήριξης του ηλεκτρονικού εμπορίου προσπαθούν να υλοποιήσουν μεθόδους πιστοποίησης της ταυτότητας των χρηστών, που να είναι εύχρηστες, ασφαλείς, αξιόπιστες και να μπορούν να λειτουργήσουν με μεγάλο αριθμό χρηστών. Στο περιβάλλον ενός δημόσιου δικτύου πρέπει να υπάρχουν οργανισμοί πιστοποίησης, που να εγγυώνται την ταυτότητα των χρηστών που είναι εγγεγραμμένοι σε αυτούς. Η δυνατότητα πιστοποίησης της ταυτότητας παίζει κεντρικό ρόλο για την ασφάλεια των ηλεκτρονικών συναλλαγών.

Το πρωτόκολλο SET περιέχει ρυθμίσεις που καλύπτουν όλες τις ανάγκες ασφάλειας του ηλεκτρονικού εμπορίου:

- Απόρρητο των πληροφοριών.
- Ακεραιότητα των δεδομένων.
- Πιστοποίηση της ταυτότητας των πελατών.
- Πιστοποίηση της ταυτότητας του εμπόρου.
- Συμβατότητα.

Συνοπτικά, το πρωτόκολλο SET είναι ένα ενιαίο σύνολο όλων των απαραίτητων χαρακτηριστικών για την αύξηση του ενδιαφέροντος και της εμπιστοσύνης των επιχειρήσεων στο ηλεκτρονικό εμπόριο, ενώ υποστηρίζεται από τους μεγαλύτερους οικονομικούς και τεχνικούς οργανισμούς που συνδέονται με το ηλεκτρονικό εμπόριο.



Εικόνα 19: Πως λειτουργεί το SET

Ας υποθέσουμε ότι ο πελάτης διαθέτει ένα πρόγραμμα προβολής ιστοσελίδων που ενεργοποιεί το SET, όπως το Netscape ή ο Internet Explorer της Microsoft και ότι ο παροχέας της συναλλαγής (τράπεζα, κατάστημα κ.λπ.) έχει έναν διακομιστή που ενεργοποιεί επίσης το SET.

1. Ο πελάτης ανοίγει έναν τραπεζικό λογαριασμό MasterCard ή Visa. Κάθε εκδότης πιστωτικής κάρτας είναι ένα είδος τράπεζας.

2. Ο πελάτης λαμβάνει ένα ψηφιακό πιστοποιητικό. Αυτό το ηλεκτρονικό αρχείο λειτουργεί σαν πιστωτική κάρτα για ηλεκτρονικές αγορές ή άλλες συναλλαγές. Περιέχει έναν κωδικό με ημερομηνία λήξης. Είναι ψηφιακά υπογεγραμμένο από την τράπεζα για να εξασφαλιστεί η εγκυρότητά του.

3. Οι έμποροι λαμβάνουν επίσης πιστοποιητικά από την τράπεζα. Αυτά τα πιστοποιητικά περιέχουν τον κωδικό του εμπόρου και της τράπεζας.

4. Ο πελάτης δίνει μια παραγγελία μέσω μιας δικτυακής σελίδας, τηλεφωνικά ή με κάποιο άλλο τρόπο.

5. Το πρόγραμμα προβολής ιστοσελίδων του πελάτη λαμβάνει και επιβεβαιώνει από το πιστοποιητικό του εμπόρου ότι ο έμπορος είναι έγκυρος.

6. Το πρόγραμμα προβολής ιστοσελίδων αποστέλλει την παραγγελία. Αυτό το μήνυμα είναι αποκρυπτογραφημένο με το δημόσιο κλειδί του εμπόρου, με τα στοιχεία της πληρωμής, που είναι αποκρυπτογραφημένα με το δημόσιο κλειδί της τράπεζας (το οποίο δεν μπορεί να διαβάσει ο έμπορος), και στοιχεία που διασφαλίζουν ότι η πληρωμή θα πραγματοποιηθεί μόνο για τη συγκεκριμένη παραγγελία.

7. Ο έμπορος επαληθεύει τον πελάτη ελέγχοντας την ψηφιακή υπογραφή στο πιστοποιητικό του πελάτη. Αυτό μπορεί να γίνει με παραπομπή του πιστοποιητικού στην τράπεζα ή από κάποιον τρίτο φορέα επικύρωσης.

8. Ο έμπορος στέλνει το μήνυμα παραγγελίας στην τράπεζα. Αυτό περιέχει το δημόσιο κλειδί της τράπεζας, τα στοιχεία πληρωμής του πελάτη (τα οποία ο έμπορος δεν μπορεί να αποκωδικοποιήσει) και το πιστοποιητικό του εμπόρου.

9. Η Τράπεζα επαληθεύει τον έμπορο και το μήνυμα. Η τράπεζα χρησιμοποιεί την ψηφιακή υπογραφή στο πιστοποιητικό με το μήνυμα και επιβεβαιώνει το τμήμα πληρωμής του μηνύματος.

10. Η Τράπεζα υπογράφει ψηφιακά και στέλνει έγκριση στον έμπορο, ο οποίος έπειτα μπορεί να συμπληρώσει την παραγγελία.

Πιστοποίηση (Verification)

Στο σύστημα SET, μπορούν και οι δύο συναλλασσόμενες πλευρές να επιβεβαιώσουν, αφενός οι έμποροι ότι οι πελάτες τους είναι κάτοχοι ισχύουσας

πιστωτικής κάρτας και αφετέρου οι πελάτες ότι ο έμπορος είναι φερέγγυος για την πραγματοποίηση συναλλαγών. Σε ένα μεγάλο βαθμό, η φερεγγυότητα του εμπόρου συμβαδίζει με την επωνυμία του.

Πλέον της επωνυμίας όμως, υπάρχουν μια σειρά από ανεξάρτητες εγγυήτριες αρχές, οι οποίες πιστοποιούν ότι ο έμπορος που διατηρεί το συγκεκριμένο ηλεκτρονικό κατάστημα είναι αυτός που υποδηλώνει η επιχείρησή του και δεν πρόκειται για κάποιον ο οποίος τυχαίνει να έχει υποκλέψει την επωνυμία του με δόλια μέσα. Επιπλέον οι εγγυήτριες αυτές αρχές, επιβεβαιώνουν ότι ο συγκεκριμένος έμπορος έχει τη δυνατότητα να προβαίνει σε ηλεκτρονικές δοσοληψίες. Τέτοιες εταιρείες είναι η VeriSign, η GlobalSign, η Nortel κ.α.

Ένα από τα πρώτα βήματα λοιπόν που πρέπει να κάνει μια επιχείρηση που προτίθεται να δραστηριοποιηθεί εμπορικά στο διαδίκτυο είναι να αποταθεί προς μια από τις εγγυήτριες αρχές και να πιστοποιηθεί η δυνατότητά του για πραγματοποίηση ~~δοσοληψιών.~~ Έναντι-πληρωμής παρέχεται στον ενδιαφερόμενο έμπορο, πιστοποιητικό που περιέχει στοιχεία που καθορίζονται από το πρότυπο X.509, τα σημαντικότερα από τα οποία είναι η επωνυμία του, το δημόσιο κλειδί του και η περίοδος εγκυρότητας του πιστοποιητικού.

Για να μπορέσει ο πελάτης να επιβεβαιώσει την ταυτότητα του εμπόρου πριν την ολοκλήρωση της συναλλαγής, μπορεί από τη στιγμή που θα λάβει το δημόσιο κλειδί του να απευθυνθεί στην αρμόδια αρχή πιστοποίησης και με βάση το δημόσιο κλειδί να αποκτήσει πρόσβαση στις πληροφορίες που αναγράφονται στο πιστοποιητικό του εμπόρου. Στη συνέχεια έχοντας εξακριβώσει τη δυνατότητα του εμπόρου να διεξάγει ή όχι συναλλαγές, μπορεί να προχωρήσει ή να διακόψει τη συναλλαγή.

Για να υπάρχει ασφάλεια στις συναλλαγές, απαιτείται η παρουσία ενός ασφαλούς webserver. Ο ασφαλής web server χρησιμοποιείται για την απόκρυψη δεδομένων μεταξύ ενός server και ενός browser. Τα δεδομένα κρυπτογραφούνται και προς τις δύο κατευθύνσεις, έτσι ώστε να μην μπορεί κάποιος να τα παρακολουθήσει κατά τη μεταφορά τους στο Internet.

Η πρόσβαση μέσω ενός ασφαλούς server είναι σαφώς πιο αργή σε σύγκριση με τη σύνδεση μέσω ενός κοινού server, και αυτό οφείλεται στην κρυπτογράφηση / αποκρυπτογράφηση η οποία χρειάζεται να γίνει στα δεδομένα. Εξαιτίας αυτού του επιπλέον φόρτου στον web server, η επιλογή της χρήσης του ασφαλούς web server πρέπει να γίνεται μόνο όταν πρόκειται για την προστασία ευαίσθητων δεδομένων. Πριν τη λειτουργία ενός ηλεκτρονικού καταστήματος, θα πρέπει να γίνουν έλεγχοι έτσι ώστε να είναι βέβαιο πως ο αριθμός της πιστωτικής κάρτας του πελάτη ή οποιαδήποτε άλλα ευαίσθητα δεδομένα, είναι επαρκώς προστατευμένα κατά τη μεταφορά τους από τον browser του πελάτη στον server του καταστήματος ή οποιοδήποτε άλλο server με τον οποίο συνεργάζεται το κατάστημα.

Τα απαραίτητα στοιχεία για να υλοποιηθούν τα παραπάνω είναι τα εξής:

- ♦ Ο web server θα πρέπει να είναι ένας ασφαλής server, ο οποίος προστατεύει τα δεδομένα που στέλνονται από τον web browser του πελάτη (π.χ. μέσω μιας Web φόρμας) στον κεντρικό server κωδικοποιώντας τα. Το URL ενός ασφαλούς server, μοιάζει με τα μέχρι τώρα χρησιμοποιούμενα, αλλά αντί για "HTTP" χαρακτηρίζεται ως "HTTPS" (HTTPSecure).
- ♦ Ο πελάτης χρειάζεται να έχει έναν από τους δύο μεγάλους browsers της αγοράς, είτε τον Netscape Navigator είτε τον Microsoft Internet Explorer, έτσι ώστε να εξασφαλίζεται η μεταβίβαση των δεδομένων από τον πελάτη προς τον server με ασφαλή τρόπο. Η εμφάνιση των web σελίδων, είναι πανομοιότυπη με αυτή κάθε άλλου web server αλλά με δύο διαφορές: υπάρχει μια μπλε γραμμή κατά μήκος του άνω μέρους του παραθύρου του browser, ενώ το κλειδί (στο Netscape Navigator) ή το λουκέτο (στον Microsoft Internet Explorer) στην κάτω αριστερή γωνία του παραθύρου είναι ενεργοποιημένο. Αυτές οι διαφορές κάνουν φανερό ότι εμφανίζεται μια ασφαλής (secure) σελίδα.
- ♦ Πρέπει να σημειωθεί εδώ ότι άλλοι browsers, όπως το Mosaic, δεν έχουν πρόσβαση σε URL που έχουν HTTPS. Έτσι, οι πελάτες που επιθυμούν να κάνουν αγορές αγαθών και υπηρεσιών από διάφορα sites τα οποία χρησιμοποιούν ασφαλείς servers, θα πρέπει να προμηθευτούν τους browsers είτε από το site της Netscape (www.netscape.com) είτε από αυτό της Microsoft (www.microsoft.com).

Συστήματα ασφαλείας που χρησιμοποιούνται για την αγορά μέσω πιστωτικών καρτών:

Παρά το γεγονός ότι οι κάρτες είναι ο πλέον προφανής και εύκολος τρόπος για τη διεκπεραίωση των πληρωμών, δεν είναι και ο ασφαλέστερος – κάθε άλλο. Η μόνη διασφάλιση του δικαιούχου είναι ότι η κάρτα μπορεί να χρεωθεί, δηλαδή δεν είναι κλεμμένη ή χαμένη, έχει επαρκές όριο χρέωσης και η εκδότρια τράπεζα επιτρέπει στον κάτοχό της να τη χρησιμοποιεί.

Ένα από τα πιο διαδεδομένα συστήματα ασφαλείας στις αγορές μέσω πιστωτικών καρτών αναφέρεται να είναι το SET (Security Electronic Transaction), βασίζεται στη μέθοδο PKI. Υλοποιήθηκε στις αρχές της δεκαετίας του 1990 από τις εταιρίες παροχής πιστωτικών καρτών και χρηματοπιστωτικών συναλλαγών VISA και MasterCard. Το SET παρέχει τα ακόλουθα χαρακτηριστικά ασφαλείας: αυθεντικοποίηση, ακεραιότητα, ασφάλεια των δεδομένων από τρίτους και δυνατότητα απόδειξης της συναλλαγής. Επιπλέον, παρέχει την δυνατότητα κρυπτογράφησης των δεδομένων που διακινούνται μέσω του Διαδικτύου αλλά και φύλαξης ευαίσθητων πληροφοριών που περιέχονται πάνω στην πιστωτική κάρτα, όπως η ημερομηνία έκδοσής της, από τρίτα μέρη όπως ο έμπορος. Το πρωτόκολλο SET βασίζεται σε μια ιεραρχική διαδικασία αυθεντικοποίησης (trust chaining). Παρόλα αυτά το SET, είναι ένα ακριβό σύστημα και η διαδικασία εισαγωγής του σε έναν οργανισμό αρκετά περίπλοκη.

Έτσι, το 2001 μεγάλες εταιρίες έκδοσης πιστωτικών καρτών προχώρησαν στην υλοποίηση νέων συστημάτων αυθεντικοποίησης, για την ασφάλεια Διαδικτυακών συναλλαγών. Η VISA για παράδειγμα εισήγαγε ένα νέο σύστημα με την επωνυμία 3-D Secure ή αλλιώς είναι ευρέως γνωστό ως "Verified by VISA", και αντίστοιχα η Mastercard εισήγαγε το SPA (Secure Payment Application). Και τα δύο αυτά συστήματα χρησιμοποιούν τεχνολογία SSL για να εξασφαλίσουν τα προαναφερθέντα χαρακτηριστικά ασφάλειας στις συναλλαγές. Το 3-D Secure χρειάζεται αποθηκευμένο όνομα χρήστη (Username) και έναν προσωπικό κωδικό πρόσβασης (Password), από τον πελάτη που θέλει να προχωρήσει σε μία αγορά και επαληθεύει τα στοιχεία του με τον κεντρικό διακομιστή τη VISA. Τα πιστοποιητικά ασφαλείας PKI χρησιμοποιούνται μόνο για το μέρος της συναλλαγής μεταξύ του εμπόρου και της τράπεζας που έχει εκδώσει την κάρτα VISA. Το Mastercard SPA παρέχει διάφορους τρόπους αυθεντικοποίησης της ταυτότητας του πελάτη, για παράδειγμα μέσω του αποθηκευμένου ονόματος χρήστη (Username) και προσωπικού κωδικού πρόσβασης (Password), μέσω μίας έξυπνης κάρτας (Smartcard), μέσω ψηφιακών πιστοποιητικών ή ακόμα και βιομετρικών μεθόδων. Ο χρήστης είναι αυτός που προσδιορίζει τον τρόπο που θα έχει πρόσβαση στον λογαριασμό του.

- **CEPS – Common Electronic Purse Specification:** Το CEPS είναι ένα πρωτόκολλο διαχείρισης ηλεκτρονικού χρήματος που χρησιμοποιεί ως μέσο συναλλαγής τις πλαστικές κάρτες. Σχεδιάστηκε για να εξυπηρετεί τη διακίνηση χρήματος ηλεκτρονικά και κυρίως εξυπηρετεί όταν πρόκειται για μεταφορά νομισμάτων διαφορετικών εθνικοτήτων. Το σύστημα αυτό παρέχει υψηλά επίπεδα ασφάλειας χρησιμοποιώντας τεχνολογία τύπου PKI.
- **Συστήματα PKI σε δίκτυα κινητής τηλεφωνίας:** Τα δίκτυα κινητής τηλεφωνίας παρουσιάζουν σημαντικές ευκαιρίες ανάπτυξης ηλεκτρονικών πληρωμών. Το κινητό τηλέφωνο έχει τη δυνατότητα να χρησιμοποιηθεί ως μία τερματική συσκευή διεκπεραίωσης ηλεκτρονικών πληρωμών. Τα τελευταία χρόνια γίνεται εκτενής έρευνα σχετικά με τη συμβατότητα του πρωτοκόλλου PKI και τις συσκευές κινητών τηλεφώνων. Τα αποτελέσματα αυτά τα βλέπουμε πλέον στα κινητά τηλέφωνα τρίτης γενιάς.

Οι κυριότεροι κίνδυνοι που υπάρχουν κατά τη χρήση πιστωτικών καρτών είναι οι εξής:

➤ **ΚΛΟΠΗ ΤΑΥΤΟΤΗΤΑΣ (IDENTITY THEFT)**

Είναι η πλέον συνηθισμένη απάτη στο Internet και συνίσταται στην προσποίηση από το χρήστη ότι πρόκειται για άλλο άτομο. Στην περίπτωση αυτή ο δικαιούχος της πληρωμής δείχνει "τυφλή" εμπιστοσύνη στον υποτιθέμενο κάτοχο της κάρτας – καθώς δεν μπορεί να κάνει διαφορετικά – και παρέχει την υπηρεσία ή αποστέλλει τα προϊόντα. Προσωρινά πιστώνεται με το ποσό που πληρώθηκε από τον πελάτη. Αν όμως η κάρτα δεν ανήκε πράγματι στον πληρωτή, η συναλλαγή θα αμφισβητηθεί από τον πραγματικό κάτοχο της κάρτας και ο δικαιούχος θα αναγκαστεί να επιστρέψει το ποσό, προκειμένου αυτό να πιστωθεί στην κάρτα του πραγματικού κατόχου. Είναι σαφές ότι αυτός που αντιμετωπίζει το πρόβλημα δεν είναι ο καταναλωτής/ κάτοχος της κάρτας αλλά ο δικαιούχος που κινδυνεύει να μην πληρωθεί ποτέ, ενώ στο μεταξύ έχει στείλει τα προϊόντα ή, το συνηθέστερο, έχει ήδη παράσχει την υπηρεσία.

Card Security Code

Ο μόνος τρόπος που έχουν όλες οι τράπεζες για να περιορίσουν το πρόβλημα είναι η χρήση του κωδικού ασφαλείας (Card Security Code), που βρίσκεται στο πίσω μέρος της κάρτας. Ο μόνος τρόπος για να πέσει αυτός ο κωδικός στην αντίληψη τρίτου προσώπου είναι το πρόσωπο αυτό να αποκτήσει πρόσβαση στο πλαστικό και να τον συγκρατήσει/ καταγράψει.

Address Verification Service

Στις Η.Π.Α εφαρμόζεται η μέθοδος AVS. Η διεύθυνση αποστολής των προϊόντων και εν γένει η ταχυδρομική διεύθυνση που δηλώνει ο χρήστης πρέπει να είναι ακριβώς ίδια με αυτή που ο κάτοχος της κάρτας έχει δηλώσει στην τράπεζα που την έχει εκδώσει.

SET

Παλιότερα οι οργανισμοί Visa και MasterCard είχαν επινοήσει και υλοποιήσει το πρότυπο SET (Secure Electronic Transaction), που στηριζόταν στην τεχνολογία PKI (Public Key Infrastructure). Με το SET, η τράπεζα που έχει εκδώσει την κάρτα έδινε στον πελάτη της ένα ψηφιακό πιστοποιητικό, καθώς και μια ειδική εφαρμογή, με τα οποία ο πελάτης μπορούσε να αποδείξει στην τράπεζά του ότι είναι ο πραγματικός κάτοχος της κάρτας. Το πρότυπο SET απέτυχε, καθώς οι δυσκολίες στη χρήση του απέτρεψαν τόσο τους εμπόρους όσο και τους κατόχους καρτών από την αξιοποίησή του.

3D-Secure

Πρόσφατα οι οργανισμοί Visa και MasterCard (και αναμένεται να ακολουθήσουν και οι υπόλοιποι) σχεδίασαν και υιοθέτησαν το νέο πρότυπο 3D-Secure. Η υλοποίηση της Visa ονομάζεται Verified by Visa (VbV) και η αντίστοιχη της MasterCard λέγεται SecureCode.

- Με το 3D-Secure, κατά τη διάρκεια της πληρωμής και αμέσως μόλις ο χρήστης συμπληρώσει τα στοιχεία της κάρτας του, η τράπεζα/acquirer (εφόσον έχει υλοποιήσει το πρότυπο) προσπαθεί να ζητήσει από την τράπεζα/issuer να πιστοποιήσει την ταυτότητα του κατόχου της κάρτας.
- Αν η τράπεζα/issuer έχει κι αυτή υλοποιήσει το 3D-Secure, ζητά από τον κάτοχο της κάρτας να εισάγει τον προσωπικό κωδικό που έχει επιλέξει για το σκοπό αυτό. Αυτό γίνεται σε ένα νέο παράθυρο της εφαρμογής πλοήγησης στο Internet (pop-up window στον browser), το οποίο παρουσιάζεται στον κάτοχο της κάρτας.
- Η τράπεζα/issuer πιστοποιεί την ταυτότητα του κατόχου της κάρτας και απαντά αντίστοιχα στην τράπεζα/acquirer. Εννοείται ότι η όλη επικοινωνία γίνεται μέσω του αντίστοιχου οργανισμού (Visa/MasterCard) και με τη χρήση ειδικής τεχνολογίας που υλοποιεί το πρότυπο.
- Αν η τράπεζα/issuer δεν έχει υλοποιήσει το 3D-Secure, η διαδικασία πιστοποίησης δεν προχωρά.
- Μετά την πιστοποίηση της ταυτότητας του κατόχου της κάρτας, η διαδικασία συνεχίζεται με τη λήψη έγκρισης για τη χρέωση της κάρτας, σύμφωνα με τον κλασικό τρόπο που περιγράφηκε παραπάνω.

Το σημαντικό στοιχείο του 3D-Secure είναι ότι, είτε η τράπεζα/issuer έχει υλοποιήσει το πρότυπο (οπότε μπορεί να πιστοποιήσει τον κάτοχο) είτε όχι, αν η τράπεζα/acquirer προσπαθήσει να εφαρμόσει το πρότυπο, τότε η ευθύνη σε περίπτωση αμφισβήτησης της συναλλαγής (λόγω πλαστοπροσωπίας) μετατίθεται στην τράπεζα/issuer. Αυτή η τακτική (liability shift) αναμένεται να λειτουργήσει ως κίνητρο για την εφαρμογή του προτύπου, τόσο από τους acquirers (που απαλλάσσονται από αυτή την κατηγορία αμφισβητήσεων που είναι η συχνότερη), όσο και από τους issuers (που θα προσπαθήσουν να αποφύγουν την "τυφλή" ανάληψη της ευθύνης). Παράλληλα οι συναλλαγές με 3D-Secure δημιουργούν

μικρότερη οικονομική επιβάρυνση στους acquirers, πράγμα που λειτουργεί ως επιπλέον κίνητρο για την εφαρμογή του προτύπου. Το 3D-Secure έχει ήδη εφαρμοστεί σε πολλούς acquirers της Ευρώπης, καθώς και σε λιγότερους issuers, ενώ αναμένεται να εφαρμοστεί και στις Η.Π.Α.

➤ “ΥΠΟΠΤΑ” WEB SITES

Προκειμένου να υποκλέψουν στοιχεία καρτών, πολλά sites ευαγγελίζονται εξαιρετικά δελεαστικές παροχές μόνο και μόνο για να εξωθήσουν τους επισκέπτες να καταχωρίσουν τα στοιχεία των καρτών τους. Στη συνέχεια χρησιμοποιούν τα στοιχεία αυτά για να χρεώσουν τις κάρτες των ανυποψίαστων κατόχων σε άλλα web sites.

Ο μόνος τρόπος για να αποφευχθεί αυτό το πρόβλημα είναι η δέουσα προσοχή εκ μέρους των κατόχων καρτών, οι οποίοι πρέπει να αντιμετωπίζουν τα web sites με τον ίδιο τρόπο που αντιμετωπίζουν και τα φυσικά καταστήματα.

➤ ΜΑΖΙΚΗ ΥΠΟΚΛΟΠΗ ΣΤΟΙΧΕΙΩΝ ΚΑΡΤΩΝ

Αν το web site στο οποίο καταχωρίζονται τα στοιχεία των πιστωτικών καρτών τα αποθηκεύει, υπάρχει ο κίνδυνος υποκλοπής του συνόλου των στοιχείων. Αυτός είναι και ο λόγος που, είτε δεν πρέπει να αποθηκεύονται τα εν λόγω στοιχεία είτε πρέπει να τηρούνται αυστηρότατα μέτρα για την ασφαλή διατήρησή τους. Αν η υποκλοπή γίνει γνωστή, τότε οι οργανισμοί καρτών ενημερώνουν τις εκδότριες τράπεζες, ώστε αυτές, με τη σειρά τους, να ενημερώσουν τους κατόχους καρτών, να ακυρώσουν τις κάρτες τους και να εκδώσουν νέες στη θέση τους.

➤ ΕΠΙΒΕΒΑΙΩΣΗ ΜΕ ΕΙΔΙΚΟ ΚΩΔΙΚΟ

Την ώρα της συναλλαγής και αφού ο πελάτης έχει δώσει τα στοιχεία της πληρωμής, εισάγει και τον αριθμό του κινητού του. Το web site του αποστέλλει έναν κωδικό μιας χρήσης, τον οποίο ο πελάτης πρέπει να εισαγάγει στο site, προκειμένου να πιστοποιηθεί. Η περίπτωση αυτή βρίσκει εφαρμογή σε χρήστες/ κατόχους κινητών τηλεφώνων που έχουν προηγουμένως εγγραφεί στην τράπεζά τους προκειμένου να έχουν αυτή τη δυνατότητα.

6. ΣΥΣΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ ΣΤΙΣ ΧΩΡΕΣ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ

Πολλά συστήματα PKI χρησιμοποιούνται στην Ευρώπη τα τελευταία χρόνια, παρακάτω αναφέρονται τα σημαντικότερα από αυτά.

Στο Βέλγιο, οι μεγαλύτερες τράπεζες μαζί με τον κεντρικό οργανισμό χρεωστικών καρτών (Banksys), το κεντρικό διατραπεζικό σύστημα (ISABEL), και το Βελγικό οργανισμό ταχυδρομείων ίδρυσαν μία εταιρία που παρέχει ψηφιακά πιστοποιητικά αυθεντικοποίησης, την ECERTIO. Οι πελάτες των παραπάνω οργανισμών χρησιμοποιούν αυτά τα πιστοποιητικά για να εκτελέσουν ηλεκτρονικές συναλλαγές, με τις τράπεζες τους, την κυβέρνηση και για να πραγματοποιήσουν επίσης ηλεκτρονικές αγορές.

Στη Φινλανδία, αρκετά συστήματα που χρησιμοποιούν τεχνολογία τύπου PKI έχουν υλοποιηθεί επίσης. Ο οργανισμός καταμέτρησης πληθυσμού έχει προχωρήσει στην έκδοση ηλεκτρονικών καρτών αναγνώρισης προσώπων. Οι χρήστες μπορούν μέσω αυτών των καρτών να συναλλαγούν ηλεκτρονικά με κρατικές υπηρεσίες. Επίσης έχουν υλοποιηθεί αρκετά συστήματα που βασίζονται σε τεχνολογίες τύπου SET, EMV (Europay, Mastercard, Visa) και SIM. Ο οργανισμός Certall είναι το αποτέλεσμα μια κοινής προσπάθειας μεταξύ των χρηματοπιστωτικών ιδρυμάτων και των φινλανδικών ταχυδρομείων, στη δημιουργία ενός κοινού προτύπου PKI το οποίο θα υιοθετηθεί από τους παραπάνω φορείς.

Στην Γαλλία, συστήματα που χρησιμοποιούν τεχνολογία τύπου PKI χρησιμοποιούνται για την ηλεκτρονική εκκαθάριση φόρων, αλλά επίσης έχουν γίνει και πολλές προσπάθειες στο χώρο της υγείας, όπου οι ασθενείς μπορούν να πληρώνουν ηλεκτρονικά της υπηρεσίες που δέχονται (SESAME/VITALE).

Στην Γερμανία, πολλά παραδείγματα χρησιμοποίησης τεχνολογιών τύπου PKI έχουν καταγραφεί στον χώρο της υγείας, των συναλλαγών με το δημόσιο τομέα, στο εμπόριο, στη βιομηχανία και τέλος και στον τραπεζικό τομέα. Ακολουθώντας την Ευρωπαϊκή οδηγία σχετικά με τις ηλεκτρονικές υπογραφές που εκδόθηκε στις 16 Μαΐου 2001 η Γερμανική κυβέρνηση προχώρησε στην ίδρυση του οργανισμού Regulierungsbehörde für Post und Telekommunikation, που λειτουργεί ως ρυθμιστικό όργανο στην τηλεπικοινωνιακή αγορά και στις ταχυδρομικές υπηρεσίες. Στον χώρο της ηλεκτρονικής διακυβέρνησης, η Γερμανική κυβέρνηση προχώρησε στην πρωτοβουλία υλοποίησης του συστήματος «Bund Online», το οποίο είναι ένα σύστημα που βασίζεται σε τεχνολογία τύπου PKI και εξυπηρετεί τις ηλεκτρονικές συναλλαγές του πολίτη με το κράτος.

Στην Ιταλία ο βαθμός συνεργασίας μεταξύ δημοσίων και ιδιωτικών φορέων κρίνεται ικανοποιητικός, αν και ακολουθείται μία παραδοσιακή ιεραρχική μορφή συνεργασίας. Η κεντρική τράπεζα της Ιταλίας (Banca d'Italia), το κράτος και αρκετοί ιδιωτικοί οργανισμοί έκδοσης ψηφιακών πιστοποιητικών έχουν προχωρήσει σε συνεργασία για να σχεδιάσουν ένα κοινό πλαίσιο συνεργασίας σε εθνικό επίπεδο, σχετικά με την υλοποίηση μιας κοινής τεχνολογικής υποδομής που θα βασίζεται σε τεχνολογία τύπου PKI.

Στη Νορβηγία, έχει δημιουργηθεί μια ενιαία τεχνολογική πλατφόρμα, βασιζόμενη σε τεχνολογία τύπου PKI η οποία λειτουργεί σε εθνικό επίπεδο επιτρέποντας την αναγνώριση φυσικών προσώπων μέσω της χρήσης έξυπνων καρτών. Τα πλεονεκτήματα της εφαρμογής μιας κοινής τεχνολογικής πλατφόρμας σε εθνικό επίπεδο είναι αρκετά και τα σημαντικότερα από αυτά είναι: α) μεγαλύτερη εμπιστοσύνη των καταναλωτών, β) χαμηλότερα κόστη συναλλαγών, γ) απλοποίηση διαδικασιών και ε) περισσότερες και ενοποιημένες υπηρεσίες.

Στην Ισπανία, έχουν καταγραφεί αρκετές πρωτοβουλίες σχετικά με την υιοθέτηση ψηφιακών υπογραφών, επιτρέποντας την αποτελεσματική διεξαγωγή ηλεκτρονικών συναλλαγών σε ιδιωτικό αλλά και σε δημόσιο τομέα. Τα πιστοποιητικά έκδοσης ψηφιακών συναλλαγών βασίζονται κυρίως στο πρωτόκολλο X.509 ή σε τεχνολογίες τύπου SET.

Οι προβληματισμοί που ακολουθούν σχετικά με την υιοθέτηση μιας δημόσιας πλατφόρμας διεξαγωγής ηλεκτρονικών πληρωμών χωρίζεται σε θέματα που αφορούν τη νομοθεσία, τεχνικά και οργανωσιακά θέματα και τέλος σε ζητήματα συμβατότητας και συνεργασίας με άλλα συστήματα.

Η υιοθέτηση ενός PKI συστήματος απαιτεί ακριβείς κανόνες εφαρμογής και υλοποίησης ώστε να εγγυηθούν την ορθή χρήση των ψηφιακών πιστοποιητικών, αλλά και την γνησιότητα τους. Τα θέματα που προκύπτουν λοιπόν είναι:

- Πώς μπορεί να διασφαλιστεί η εμπιστοσύνη στους οργανισμούς που παρέχουν τα δημόσια κλειδιά πιστοποίησης (CA certificates);
- Πόσο προσεκτικά θα γίνεται ο έλεγχος δημοσίων κλειδιών πιστοποίησης; Πώς θα προστατεύονται τα ιδιωτικά κλειδιά ασφαλείας από κλοπές και που θα διαφυλάσσονται; Ποιος οργανισμός θα αναλάβει τη φύλαξή τους;
- Πώς θα εξασφαλίζεται η ακεραιότητα των ψηφιακών πιστοποιητικών και υπογραφών, και ποιοι οργανισμοί θα έχουν δικαίωμα έκδοσης αυτών;

Μέχρι σήμερα η υλοποίηση συστημάτων βασιζόμενα σε τεχνολογία PKI επικεντρώνεται στην κάλυψη ενός μεγάλου αριθμού χρηστών σε συγκεκριμένα οργανωσιακά περιβάλλοντα. Αυτά τα συστήματα υλοποιούνται από μεγάλα επιχειρησιακά σχήματα με σκοπό να καλύψουν τις επιχειρησιακές τους ανάγκες (όπως χρηματοοικονομικές υπηρεσίες). Για να επιτύχουν όμως τον μέγιστο βαθμό ασφαλείας σε επίπεδο οργανισμού, και όχι μόνο κάλυψης των ηλεκτρονικών συναλλαγών, αναγκάζονται να στραφούν σε άλλες τεχνολογικές πλατφόρμες, που βασίζονται επίσης σε εργαλεία κρυπτογράφησης και σε τεχνολογία τύπου PKI, αλλά κρατούν την πληροφορία σε ένα άλλο επίπεδο, ενδο-οργανωσιακό. Έχει παρατηρηθεί όμως ότι πολλές φορές είναι δύσκολο ή προκύπτει χρονική καθυστέρηση για τον συγχρονισμό της πληροφορίας σε αυτά τα δύο επίπεδα.

Ακόμη, πολλές φορές η διαχείριση των ηλεκτρονικών πιστοποιητικών και πληροφοριών των πελατών γίνεται από ανεξάρτητες εταιρίες. Πολλές φορές όμως επειδή οι πληροφορίες που διαχειρίζονται είναι ιδιαίτερα ευαίσθητες και πολύτιμες, οι

εταιρίες αυτές συνήθως εξαγοράζονται από μεγάλους τραπεζικούς ομίλους που αποκτούν πρόσβαση στα μητρώα πελατών μικρότερων χρηματοπιστωτικών ιδρυμάτων. Έτσι λοιπόν προκύπτει ένα μεγάλο θέμα σχετικά με τη διαχείριση αυτών των πληροφοριών καθώς οι μικρότερες τράπεζες υποστηρίζουν ότι πέφτουν θύματα αθέμιτου ανταγωνισμού.

7. ΣΥΣΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ ΣΤΗΝ ΕΥΡΩΠΑΪΚΗ ΕΝΩΣΗ

Στην Ευρωπαϊκή Ένωση, όπως αναφέρει ο διεθνής ερευνητικός οίκος Forester²⁷, αναπτύχθηκαν την τελευταία τριετία περίπου 70 συστήματα ηλεκτρονικών πληρωμών. Στην ανάπτυξη και υλοποίηση τους δραστηριοποιήθηκαν κυρίως πιστωτικά ιδρύματα, εταιρίες παροχής υπηρεσιών κινητής τηλεφωνίας και οργανισμούς που ανήκουν στον κλάδο του εμπορίου. Οι βασικές ανάγκες που οδήγησαν τους οργανισμούς στην ανάπτυξη συστημάτων ηλεκτρονικών πληρωμών είναι οι εξής:

- Η ραγδαία ανάπτυξη που γνώρισε το Internet τα τελευταία χρόνια και η διείσδυση του σε ένα πολύ μεγάλο ποσοστό νοικοκυριών, οδηγεί στη δημιουργία μιας αγοράς 34 εκατομμυρίων καταναλωτών²⁸
- Οι εταιρίες παροχής κινητής τηλεφωνίας προχώρησαν σε τεράστιες επενδύσεις κεφαλαίων για την ανάπτυξη υποδομών που υποστηρίζουν την παροχή υπηρεσιών τρίτης γενιάς. Επίσης τα κινητά τηλέφωνα τρίτης γενιάς υποστηρίζουν την ανάπτυξη μιας νέας μορφής εμπορίου, αυτή του κινητού εμπορίου. Τέλος, προσβλέπουν στην μείωση κόστους κατά 40% σχετικά με τις κάρτες προπληρωμένου χρόνου, αν ο χρόνος ομιλίας αγοράζεται μέσω του Διαδικτύου ή χρησιμοποιώντας εφαρμογές κινητού εμπορίου²⁹
- Χρηματοπιστωτικά ιδρύματα και μεγάλοι τραπεζικοί όμιλοι μέσω των συστημάτων ηλεκτρονικών πληρωμών προσβλέπουν στη δραματική μείωση του κόστους κυκλοφορίας χρήματος, προσφέροντας σε πολλές περιπτώσεις μειώσεις ή και μηδενικά κόστη συναλλαγών.

Παρακάτω προχωρούμε στην ανάλυση των τεχνολογιών που χρησιμοποιούν τα πιο δημοφιλή και πετυχημένα συστήματα ηλεκτρονικών πληρωμών στην Ευρωπαϊκή αγορά.

- **Έξυπνες κάρτες (Smart Cards).** Ένα από τα τελευταία συστήματα ηλεκτρονικών πληρωμών μέσω της χρήσης έξυπνων καρτών είναι το Interpay's Chipknip. Στόχος του είναι η αντικατάσταση του φυσικού χρήματος με ηλεκτρονικό από τις αγορές των supermarket μέχρι και τις υπηρεσίες

27 Ensor, B., Torris, T., Fagerström, M. & Martínez, N. (June 2003). New Payment Systems' Survival Guide. Techstrategy Report. Διαθέσιμο στο www.techstrategy.com.

28 Reitsma, R., Pearce, F. & de Montigny, E. (May 2002). Seeing Beyond Credit Card Payment Online. Brief. Διαθέσιμο στο www.techstrategy.com.

29 Jennings, R.U., O'Connell, P. & Bradford, N. (September 2001). Making Content Pay. Techstrategy Report. Διαθέσιμο στο www.techstrategy.com.

πάρκινγκ αυτοκινήτων. Στην πραγματικότητα οι καταναλωτές μπορούν να αποθηκεύουν αγοραστικές μονάδες αξίας 250 Ευρώ σε ένα microchip το οποίο τοποθετείται στις κανονικές πιστωτικές ή χρεωστικές κάρτες και να προβούν σε αγορές αγαθών από τα διάφορα σημεία πώλησης που υποστηρίζουν τη χρήση της έξυπνης κάρτας. Οι έμποροι πληρώνουν μία προμήθεια της τάξης του 0,3% στην αξία του αγαθού η οποία όμως είναι κατά πολύ μικρότερη από την προμήθεια που παρακρατείται για αγορές μέσω πιστωτικών καρτών. Οι καταναλωτές πληρώνουν μια ετήσια συνδρομή της τάξης των 6 Ευρώ το χρόνο για να μπορούν να ξαναγεμίζουν τις κάρτες τους με αγοραστικές μονάδες από τα σημεία που θα μπορεί γίνεται αυτό, όπως μέσω ATMs ή άλλα τερματικά.

- **Προπληρωμένες κάρτες συναλλαγών (Prepaid card – based accounts).** Οι προπληρωμένες κάρτες συναλλαγών όπως οι Paysafecard και Splash Plastic προσφέρουν τη δυνατότητα κυρίως σε νέους καταναλωτές που δεν δικαιούνται την έκδοση πιστωτικής κάρτας και σε 19 εκατομμύρια Ευρωπαίους καταναλωτές που χρησιμοποιούν το διαδίκτυο. Σε αντίθεση με τα ηλεκτρονικά πορτοφόλια οι κάρτες αυτές αποτελούν απλώς ένα αποδεικτικό μέσο της ταυτότητας του χρήστη, καθώς το χρηματικό υπόλοιπο για αγορές βρίσκεται αποθηκευμένο σε έναν κεντρικό διακομιστή. Οι καταναλωτές μπορούν να αγοράσουν τις κάρτες αυτές από πολλά σημεία πώλησης όπως περίπτερα, mini markets κ.α. και χρησιμοποιούν τον αναγραφόμενο αριθμό λογαριασμού για να προβούν στις αγορές τους.
- **“Κινητά” πορτοφόλια (Mobile wallets).** Τέτοιου είδους συστήματα κινητών πορτοφολιών στην Ευρωπαϊκή αγορά είναι τα Bankpass Mobile και Vodafone’s mPay cards τα οποία μέσω SMS μηνυμάτων επιτρέπουν τις αγορές αγαθών μέσω της μεταφοράς χρημάτων από πιστωτικές κάρτες και τραπεζικούς λογαριασμούς. Προμήθεια παρακρατείται από τους διαχειριστές των κινητών δικτύων που χρησιμοποιούνται για τις πληρωμές αγαθών, η οποία και προστίθεται αυτομάτως στο ποσό της αγοράς που χρεώνεται είτε στην πιστωτική κάρτα είτε στον αριθμό του τραπεζικού λογαριασμού του καταναλωτή. Το βασικό πρόβλημα αυτών των μέσων διεξαγωγής ηλεκτρονικών πληρωμών εντοπίζεται κυρίως στις ασυμβατότητες των πολλών συστημάτων που χρησιμοποιούνται από τις εταιρίες παροχής κινητών υπηρεσιών καθώς η κάθε μία από αυτές προσπαθεί να περιορίσει τους πελάτες τις στη χρήση των δικών της συστημάτων. Η Vodafone για παράδειγμα επιτρέπει τη χρήση του συστήματος μόνο στους δικούς τις πελάτες.
- **“Κινητοί” λογαριασμοί πληρωμών (Mobile payment accounts).** Στην ευρωπαϊκή αγορά υπάρχουν περίπου 10 τέτοιου είδους συστήματα και τα πιο διαδεδομένα είναι τα Paybox και Telenor’s SmartCash, τα οποία και χρησιμοποιούν SMS μηνύματα για τη διεξαγωγή των συναλλαγών, χρεώνοντας τους λογαριασμούς των πιστωτικών καρτών και τραπεζικών λογαριασμών των καταναλωτών. Τα συστήματα αυτά χρεώνουν μία προμήθεια της τάξης του 2-3% ενώ η εταιρία παροχής κινητών υπηρεσιών επωφελείται από τη διακίνηση και χρέωση των SMS μηνυμάτων. Τα συστήματα αυτά χρησιμοποιούνται σήμερα για ηλεκτρονικές αγορές αγαθών.
- **Ηλεκτρονικοί λογαριασμοί πληρωμών (Online payment accounts).** Τα συστήματα αυτά ανέρχονται σήμερα στα 16 στην Ευρωπαϊκή αγορά και τα πιο διαδεδομένα είναι τα PayPal και το epagado.com. Οι καταναλωτές μέσω της χρήσης ενός προσωπικού λογαριασμού προχωρούν στην αγορά αγαθών στέλνοντας στην ηλεκτρονική διεύθυνση του πωλητή τα στοιχεία χρέωσης

του λογαριασμού τους. Όταν ο πωλητής πιστοποιήσει την γνησιότητα των στοιχείων αυτών προχωρά προς τη διεκπεραίωση της συναλλαγής. Μια ακόμη εταιρεία που παρέχει αυτήν την υπηρεσία είναι και η FastPay's twenty pence, η οποία και χρεώνει με 0,20 λεπτά του Ευρώ τον καταναλωτή για κάθε αγορά του και με προμήθεια 2-3% της αξίας του αγαθού των πωλητή. Οι καταναλωτές χρησιμοποιούν αυτά τα συστήματα για αγορές αγαθών μικρής αξίας ως εναλλακτική των πιστωτικών καρτών και επίσης για τη διασφάλιση της ανωνυμίας τους. Αυτά τα συστήματα χρησιμοποιούνται ευρέως στις ηλεκτρονικές δημοπρασίες, όπου πολλοί αγοραστές και πωλητές θέλουν να εξασφαλίσουν την ανωνυμία τους.

Σε μια εποχή που συνδυάζει έντονα φαινόμενα ανταγωνισμού σε παγκόσμιο επίπεδο και οικονομική ύφεση, τα συστήματα ηλεκτρονικών πληρωμών ανά την Ευρώπη έχουν ένα αρκετά δύσκολο μέλλον. Πολλά συστήματα έχουν είδη αποτύχει σε διάφορες Ευρωπαϊκές χώρες όπως το Σουηδικό GISMO, τα Γαλλικά MinutePay και Paiement CB sur mobile, το Γερμανικό Click&Pay net 900 και το Γερμανό-Αγγλικό Paybox. Οι αιτίες τις αποτυχίας τους εντοπίζονται κυρίως στους εξής παράγοντες³⁰:

- Το ενδιαφέρον για ηλεκτρονικές συναλλαγές είναι αρκετά περιορισμένο. Χαρακτηριστικά μόνο το ένα τρίτο των χρηστών του Διαδικτύου στην Βρετανία ήταν ενήμερο για συστήματα ηλεκτρονικών πληρωμών παρά το γεγονός ότι τέτοιου είδους υπηρεσίες παρέχονται από μεγάλους ομίλους όπως η εταιρία παροχής κινητής τηλεφωνίας Vodafone, η τράπεζα NatWest κ.α. Ακόμη μόνο το 13% των ευρωπαίων συνδρομητών κινητής τηλεφωνίας υποστήριξε ότι θα ήταν πρόθυμο να προβεί σε αγορές μέσω των κινητών τους τηλεφώνων. Τέλος, πολύ λιγότεροι είναι οι καταναλωτές που χρησιμοποιούν το διαδίκτυο για ηλεκτρονικές αγορές, και συγκεκριμένα στη Βρετανία μόνο το 2% του συνόλου των χρηστών του Διαδικτύου προχωρά σε ηλεκτρονικές πληρωμές.
- Τα περισσότερα συστήματα ηλεκτρονικών πληρωμών συνήθως αντιμετωπίζουν προβλήματα από την έλλειψη ενός κοινού νομοθετικού πλαισίου ανάμεσα στα κράτη μέλη, που δεν επιτρέπει την ελεύθερη διακίνηση πολλών κατηγοριών αγαθών.

Η μη επίτευξη κρίσιμης μάζας καταναλωτών, οι επενδύσεις που απαιτούνται για την ανάπτυξη της κατάλληλης τεχνολογικής υποδομής και ο μεγάλος χρόνος που απαιτείται για την αποδοχή του συστήματος από τους καταναλωτές οδηγεί πολλές φορές σε αποτυχία. Είναι χαρακτηριστικό ότι ο Βελγικός όμιλος Banksys σημείωνε οικονομικές απώλειες 7 ολόκληρα χρόνια μέχρι το σύστημα Proton να φτάσει τους 5 εκατομμύρια χρήστες και τα 100 χιλιάδες σημεία πώλησης, που είναι και τα μεγέθη αυτά από τα οποία αρχίζει η κερδοφορία του. Παράλληλα αυτό συνέβη και με τη βοήθεια στρατηγικών συμμαχιών της Banksys με τις εταιρίες Belgacom και Interparking, οι οποίες επέτρεψαν στους Βέλγους καταναλωτές να χρησιμοποιούν το Proton ως μέσο πληρωμών λογαριασμών σταθερής και κινητής τηλεφωνίας καθώς επίσης για το πάρκινγκ των αυτοκινήτων τους σε διάφορους σταθμούς στάθμευσης

30 Ensor, B., Torris, T., Fagerström, M. & Martínez, N. (June 2003). New Payment Systems' Survival Guide. Techstrategy Report. Διαθέσιμο στο www.forrester.com

8. ΕΛΛΗΝΙΚΑ ΗΛΕΚΤΡΟΝΙΚΑ ΚΑΤΑΣΤΗΜΑΤΑ: ΙΣΧΥΟΥΣΕΣ ΜΕΘΟΔΟΙ ΠΛΗΡΩΜΗΣ

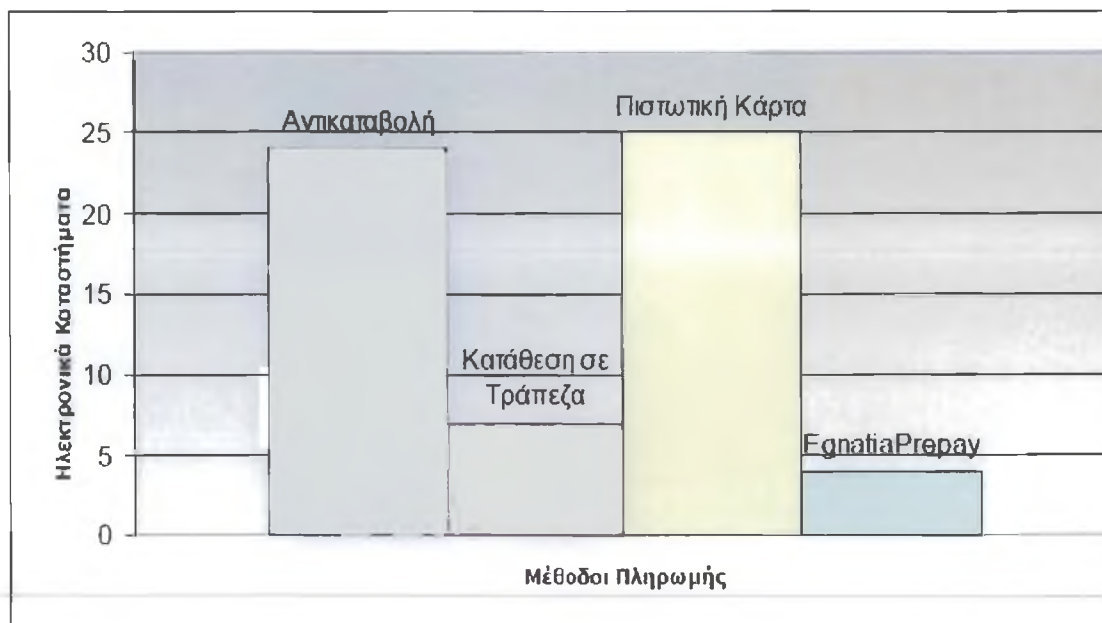
Στα πλαίσια της διαβούλευσης και προκειμένου να γίνει μια συστηματικότερη αποτύπωση της χρήσης και υιοθέτησης συστημάτων ηλεκτρονικών πληρωμών στην Ελλάδα κρίθηκε απαραίτητη η διερεύνηση των μεθόδων πληρωμών που προσφέρονται από τα ελληνικά ηλεκτρονικά καταστήματα³¹.

Η επιλογή των ηλεκτρονικών καταστημάτων έγινε είτε με βάση δημοσιεύματα στον τύπο όπου και ανακοινωνόταν η έναρξη της λειτουργίας είτε κυρίως μέσω των συνδέσμων που βρίσκονταν στις βασικές δικτυακές πύλες της Ελλάδας. Συνολικά επισκεφθήκαμε περί τα 30 ηλεκτρονικά καταστήματα. Τα προϊόντα που προσφέρονταν μέσω αυτών των καταστημάτων κάλυπταν μια ευρεία γκάμα με κυριότερα τα βιβλία και τα είδη γραφικής ύλης, τα είδη υπολογιστών, τις ηλεκτρικές συσκευές, τα άνθη, τα cd/DVD αλλά και άλλες κατηγορίες όπως βρεφικά είδη, είδη ένδυσης, είδη δώρων κ.α.

Στα πλαίσια της έρευνας, επισκεφθήκαμε την ιστοσελίδα κάθε καταστήματος και διερευνήσαμε τις επιλογές που προσφέρονταν στους καταναλωτές σε ότι αφορά στις πληρωμές των προϊόντων και υπηρεσιών που παρέχονταν. Στα περισσότερα ηλεκτρονικά καταστήματα, αυτή η πληροφορία ήταν διαθέσιμη προς τους επισκέπτες της ιστοσελίδας στην ενότητα που αφορούσε στους όρους χρήσης της ιστοσελίδας. Στα καταστήματα εκείνα που η πληροφορία αυτή δεν ήταν άμεσα διαθέσιμη η πρακτική που ακολουθήθηκε στα πλαίσια της έρευνας ήταν η δημιουργία καλαθιού αγορών προκειμένου να καταστεί εφικτή η πρόσβαση στην ιστοσελίδα όπου προσφέρονταν οι διαθέσιμοι τρόποι πληρωμής.

³¹ Στα πλαίσια της έρευνας επισκεφθήκαμε τα ακόλουθα ηλεκτρονικά καταστήματα:

www.wineshop.gr, www.dvdclub.gr, www.creatashop.gr, www.myshops.gr, www.heliosagora.com, www.oops.gr, www.books.gr, www.protoporia.gr, www.kastaniotis.gr, www.plaisio.gr, www.bookmarket.gr, www.e-shop.gr, www.applestore.gr, www.cosmodata.gr, www.1OneWay.gr, www.infoshop.gr, www.pc-shop.gr, www.greekbooks.gr, www.mad.gr, www.cdbase.gr, www.ianos.gr, www.cdnow.com, www.shop21.gr, www.dvdcool.gr, www.greekshops.com, www.female-shop.gr, www.interflora.gr, www.red-rose.gr, www.familyshop.gr, www.mystyle.gr, www.homenet.gr



Σχήμα 1: Διαθέσιμες μέθοδοι πληρωμής στα ελληνικά ηλεκτρονικά καταστήματα

Όπως φαίνεται και στο σχήμα 1, που απεικονίζει τα αποτελέσματα της έρευνας, οι βασικές μέθοδοι πληρωμής που προσφέρονται στους Έλληνες καταναλωτές αυτή τη στιγμή είναι τέσσερις:

- Πληρωμή με αντικαταβολή, ειδικά για κατοίκους Αθηνών και μεγάλων αστικών κέντρων γενικότερα
- Πληρωμή με πιστωτική κάρτα
- Κατάθεση σε τράπεζα
- Προπληρωμένες κάρτες (Egnatia Prepay³²)

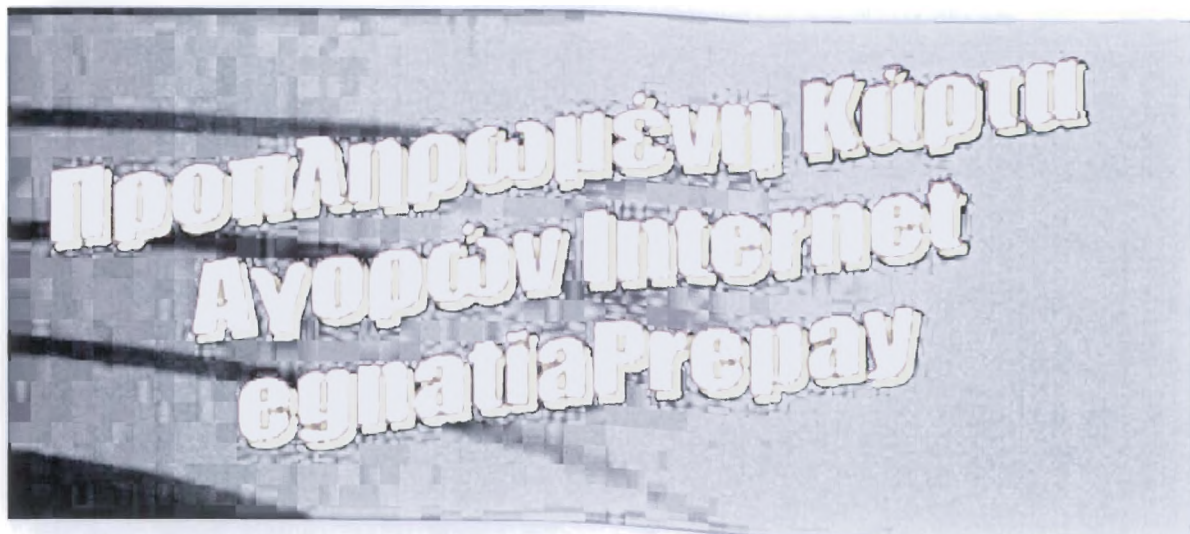
Είναι επίσης προφανές από το σχήμα 1 ότι από αυτές τις τέσσερις μεθόδους πληρωμών, τα ηλεκτρονικά καταστήματα προκρίνουν κυρίως τις πληρωμές με αντικαταβολή ή πιστωτική κάρτα και δευτερευόντως τις πληρωμές με κατάθεση του ποσού σε τραπεζικό λογαριασμό. Ακόμα πιο περιορισμένη είναι η δυνατότητα πληρωμής με σύγχρονα μέσα πληρωμών όπως οι προπληρωμένες κάρτες. Είναι δε χαρακτηριστικό ότι στα περισσότερα ηλεκτρονικά καταστήματα, τονιζόταν ιδιαίτερα η δυνατότητα πληρωμής χωρίς τη χρήση πιστωτικής κάρτας προκειμένου οι επισκέπτες της ιστοσελίδας να πραγματοποιήσουν αγορές. Το γεγονός αυτό καταδεικνύει την γενικότερη δυσπιστία και έλλειψη εμπιστοσύνης που χαρακτηρίζει το ελληνικό καταναλωτικό κοινό σε ό,τι αφορά στα συστήματα ηλεκτρονικών πληρωμών. Τα αποτελέσματα της έρευνας αυτής καταδεικνύουν περαιτέρω και την διστακτικότητα των ελληνικών τραπεζών ή άλλων εταιρειών να προβούν στη δημιουργία καινοτομικών προϊόντων που θα στηρίζονται σε σύγχρονα μέσα πληρωμών δεδομένου ότι η αποδοχή τους αναμένεται να είναι περιορισμένη και να μην δικαιολογεί το ύψος της απαιτούμενης επένδυσης. Για το λόγο αυτό και μέχρι σήμερα στην Ελλάδα υπάρχουν μόνο τρία καινοτομικά συστήματα ηλεκτρονικών πληρωμών.

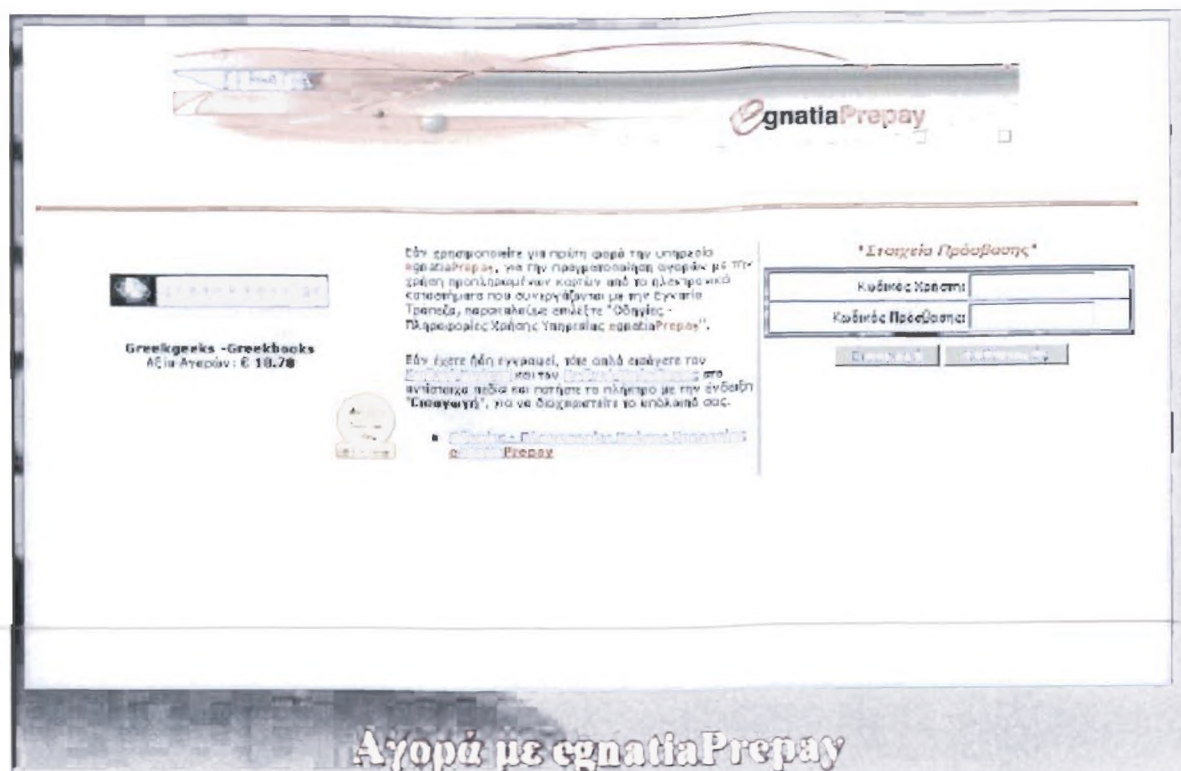
³² Η Εγνατία Τράπεζα συνεργάζεται με επιλεγμένα καταστήματα τα οποία και προσφέρουν την επιλογή πληρωμής των αγορών με χρήση της κάρτας egnatiaPrepay. Η άλλη προπληρωμένη κάρτα που παρουσιάζεται στην επόμενη ενότητα του παραδοτέου η Attica Gift Card VISA δημιουργήθηκε πρόσφατα και ακόμα δεν είναι δυνατή η αποτίμηση του εύρους χρήσης της. Επίσης, η Τράπεζα Αττικής ακολουθεί διαφορετική στρατηγική προώθησης της κάρτας που δεν στηρίζεται στην συνεργασία με συγκεκριμένα καταστήματα ούτε στην αποκλειστική χρήση στο Διαδίκτυο αλλά στην ελεύθερη χρήση της τόσο στο φυσικό όσο και στον εικονικό κόσμο. Επομένως η μεθοδολογία της έρευνας δεν επιτρέπει την αποτίμηση της χρήσης της Attica Gift Card VISA.

9. ΚΑΙΝΟΤΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ ΣΤΗΝ ΕΛΛΑΔΑ

Η περιορισμένη διάδοση του ηλεκτρονικού εμπορίου στην Ελλάδα αλλά και η δυσπιστία του έλληνα καταναλωτή έναντι των on-line αγορών έχει αποτρέψει την εμφάνιση σημαντικών πρωτοβουλιών στο τομέα των συστημάτων ηλεκτρονικών αγορών. Οι περισσότερες τράπεζες, που κατά κύριο λόγο αναλαμβάνουν πρωτοβουλίες στο χώρο, δεν θεωρούν ότι υπάρχει βιώσιμη αγορά με αποτέλεσμα να μην προβαίνουν στη δημιουργία νέων προϊόντων που θα βασίζονταν σε καινοτομικά συστήματα πληρωμών. Επιπλέον, στην χώρα μας δεν δραστηριοποιούνται ούτε άλλοι οργανισμοί στο χώρο όπως συμβαίνει στο εξωτερικό. Μέχρι στιγμής υπάρχουν δύο συστήματα που στηρίζονται στη χρήση προπληρωμένων καρτών ενώ λειτουργεί και ένα σύστημα πληρωμών μέσω κινητού τηλεφώνου. Ειδικότερα, τα συστήματα ηλεκτρονικών πληρωμών που υπάρχουν στην Ελλάδα είναι τα ακόλουθα:

9.1 ΕΓΝΑΤΙΑPREPAY





Η Εγνατία Τράπεζα εισήγαγε πρώτη στην ελληνική αγορά προπληρωμένες κάρτες που επιτρέπουν την αγορά on-line προϊόντων και υπηρεσιών μέσω του Διαδικτύου. Η δημιουργία της egnatiaPrepay είναι ουσιαστικά η πρώτη προσπάθεια δημιουργίας εναλλακτικών συστημάτων πληρωμών στην ελληνική αγορά τα οποία δεν θα απαιτούν τη χρήση των παραδοσιακών πιστωτικών καρτών. Το βασικό κίνητρο για την δημιουργία της egnatiaPrepay από την τράπεζα είναι η έντονη δυσπιστία που χαρακτηρίζει τους Έλληνες καταναλωτές σε ότι αφορά στις πληρωμές μέσω Διαδικτύου και η επιθυμία ανωνυμίας που διακρίνει την ελληνική καταναλωτική κουλτούρα όπως αυτή εκφράζεται από την προτίμηση σε πληρωμές τοις μετρητοίς.

Η προπληρωμένη κάρτα egnatiaPrepay απευθύνεται κατά βάση σε καταναλωτές, οι οποίοι είναι χρήστες του Διαδικτύου αλλά δεν έχουν πιστωτική κάρτα για την πραγματοποίηση αγορών από ηλεκτρονικά καταστήματα, καταναλωτές οι οποίοι είναι χρήστες του Διαδικτύου αλλά είναι επιφυλακτικοί στη χρήση των πιστωτικών καρτών τους για αγορές από ηλεκτρονικά καταστήματα, καθώς και σε καταναλωτές οι οποίοι είναι χρήστες του Διαδικτύου και επιθυμούν την ανωνυμία κατά την πραγματοποίηση των αγορών τους από ηλεκτρονικά καταστήματα³³. Η πρόσβαση στην υπηρεσία egnatiaPrepay γίνεται από τον ηλεκτρονικό υπολογιστή του κατόχου στον οποίο «φορτώνει» το λογισμικό της τράπεζας απευθείας από την ιστοσελίδα της ακολουθώντας μια σειρά οδηγιές. Για την εγγραφή στη υπηρεσία και την συνεπακόλουθη αγορά της κάρτας απαιτούνται μόνο η εισαγωγή της ηλικίας και του E-mail του ενδιαφερόμενου οπότε διασφαλίζεται η ανωνυμία των συναλλαγών που θα πραγματοποιηθούν μέσω της κάρτας. Η πληρωμή με χρήση προπληρωμένης

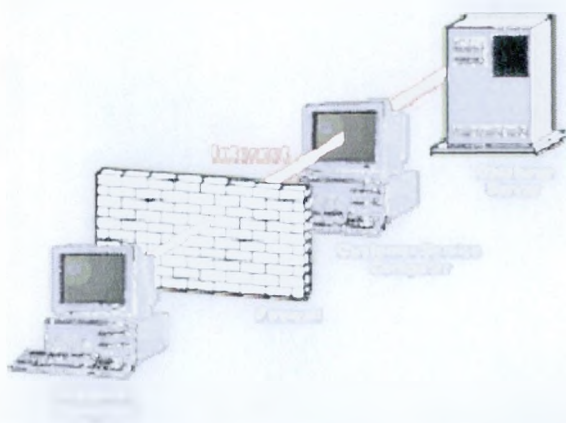
33 Πληροφορίες για το συγκεκριμένο προϊόν αντλήθηκαν από την ιστοσελίδα της Εγνατίας Τράπεζας, www.egnatia.gr, καθώς και από δημοσιεύματα στον τύπο

κάρτας είναι ιδιαίτερα εύκολη, αφού απαιτεί μόνο την εισαγωγή κωδικού χρήστη και κωδικού πρόσβασης στην υπηρεσία egnatiaPrepay, στοιχεία τα οποία διαμορφώνονται από τον ίδιο τον χρήστη. Σε περίπτωση που ο χρήστης ξεχάσει τους κωδικούς του, προβλέπεται η ύπαρξη λέξης / φράσης υπενθύμισης κωδικού, η οποία επιτρέπει την υπενθύμιση των προσωπικών στοιχείων εισόδου.

Σε ότι αφορά την διασφάλιση των πραγματοποιούμενων συναλλαγών αλλά και του χρηματικού υπόλοιπου της κάρτας η τράπεζα χρησιμοποιεί εξελιγμένα συστήματα κρυπτογράφησης που διαφυλάττουν τις μεταδιδόμενες πληροφορίες. Ειδικότερα, για την ασφάλεια των μεταδιδόμενων πληροφοριών μέσω του Διαδικτύου προβλέπεται κρυπτογράφηση SSL 128-bit, η οποία προστατεύει πλήρως τα στοιχεία της συναλλαγής καθώς και εισαγωγή κωδικού χρήστη και κωδικού πρόσβασης στην υπηρεσία. Στο σχήμα που ακολουθεί φαίνεται πώς είναι δομημένα τα συστήματα της Τράπεζας έτσι ώστε να εξασφαλίζεται το απόρρητο των συναλλαγών.

Οι ιστοσελίδες της εφαρμογής είναι εγκατεστημένες σε έναν Web Server. Σε αυτόν εγκαθίσταται Πιστοποιητικό Αυθεντικότητας το οποίο παρέχεται από συγκεκριμένες εξουσιοδοτημένες για το σκοπό αυτό εταιρίες (π.χ. Verisign). Έτσι εξασφαλίζεται στον πελάτη ότι κανείς άλλος δεν μπορεί να προσποιηθεί ότι είναι η Τράπεζα και με τον τρόπο αυτό να υποκλέψει πολύτιμες πληροφορίες (π.χ. το PIN του πελάτη).

Επιπλέον, για την πρόσβαση από τον «έξω κόσμο» ένα Firewall εγκαθίσταται πριν τον Web Server για να φιλτράρει την πρόσβαση. Με αυτό το φιλτράρισμα προστατεύονται όλα τα σημεία του εσωτερικού δικτύου στα οποία ο εξωτερικός χρήστης δεν πρέπει να έχει πρόσβαση.



Σχήμα 2: Το πληροφοριακό σύστημα της Εγνατίας τράπεζας

Ταυτόχρονα στα συστήματα της Τράπεζας εφαρμόζονται και άλλα μέτρα ασφαλείας όπως ο αλγόριθμος IDEA 128 bits που χρησιμοποιείται για την κρυπτογράφηση μηνυμάτων που αφορούν τραπεζικές συναλλαγές όταν ταξιδεύουν στο Internet. Σύμφωνα με τη Netscape, η κρυπτογράφηση με τον αλγόριθμο IDEA 128 bits είναι 309.485.009.821.345.068.724.781.056 φορές ισχυρότερη από την αντίστοιχη των 40bits. Ο χρόνος που θα απαιτούνταν από ένα σύγχρονο υπολογιστικό σύστημα για να "σπάσει" ένας τέτοιος αλγόριθμος και να διαβαστούν τα κρυπτογραφημένα δεδομένα έχει υπολογισθεί σε αρκετά δισεκατομμύρια έτη. Επιπλέον, αν η εφαρμογή δεν χρησιμοποιηθεί για χρονικό διάστημα 15 λεπτών τότε τερματίζεται αυτόματα. Έτσι, αφενός δε μπορεί να χρησιμοποιηθεί από άλλο χρήστη στην απουσία του εξουσιοδοτημένου χρήστη, αφετέρου δίνει ελάχιστο χρόνο για την προσπάθεια αποκρυπτογράφησης του μηνύματος καθώς στην επόμενη ανταλλαγή μηνύματος το κλειδί θα είναι διαφορετικό. Όσο για τα στοιχεία των συναλλαγών που

φυλάσσονται στα αρχεία της Τράπεζας, και αυτά είναι απόλυτα προστατευμένα αφού πρόσβαση σε αυτά έχουν μόνο οι αρμόδιοι υπάλληλοι της Τράπεζας (σύμφωνα με το Νόμο «περί τήρησης αρχείου»).

Βασικός περιορισμός στη χρήση της κάρτας είναι ότι ο κάτοχος μπορεί να πραγματοποιήσει συναλλαγές μόνο με τα συνεργαζόμενα ηλεκτρονικά καταστήματα ενώ η διάθεση της πραγματοποιείται αποκλειστικά από τα υποκαταστήματα της τράπεζας αν και πρόσφατα κατέστη δυνατή και η αγορά της Διαδικτυακά μέσω της ιστοσελίδας της τράπεζας.

9.2 ATTICA GIFT CARD VISA

ATTICA GIFT CARD VISA

Η ΚΑΡΤΑ ΤΗΣ ΝΕΑΣ ΓΕΝΙΑΣ ΓΙΑ
ΑΣΦΑΛΕΣ ΣΥΝΑΛΛΑΓΕΣ ΣΤΟ
ΔΙΑΔΙΚΤΥΟ
ΑΠΟ ΤΗΝ ΤΡΑΠΕΖΑ ΑΤΤΙΚΗΣ

ΤΡΑΠΕΖΑ ΑΤΤΙΚΗΣ

Η Attica Gift CARD VISA είναι μια προπληρωμένη κάρτα που εκδόθηκε πρόσφατα από την Τράπεζα Αττικής. Η ιδιαιτερότητα της συγκεκριμένης κάρτας είναι ότι πρόκειται για κάρτα δώρου την οποία ο αγοραστής της μπορεί να δωρίσει στα αγαπημένα του πρόσωπα, στους φίλους και συγγενείς επ' αφορμή διαφόρων περιστάσεων όπως ονομαστικές εορτές, γενέθλια, γάμοι. Επομένως δεν πρόκειται για κάρτα που δημιουργήθηκε με γνώμονα την αποκλειστική της χρήση για πληρωμές στο διαδίκτυο όπως η egnatiaPrepay. Η ίδια η τράπεζα προτείνει εναλλακτικά τη χρήση της Attica Gift CARD VISA και στο διαδίκτυο ως έναν ασφαλέστερο τρόπο πληρωμής αντί της χρήσης πιστωτικών καρτών καθώς η κάρτα είναι συνδεδεμένη με ονομαστικό τραπεζικό λογαριασμό με κλειστό πιστωτικό υπόλοιπο. Βέβαια, ανεξάρτητα από τον τρόπο προώθησης της στην ελληνική αγορά, η εν λόγω κάρτα είναι ένα καινοτομικό τραπεζικό προϊόν και μια από τις ελάχιστες πρωτοβουλίες για δημιουργία εναλλακτικών συστημάτων πληρωμών στο διαδίκτυο.

Η Attica Gift CARD VISA διατίθεται σε όλα τα καταστήματα της Τράπεζας Αττικής με την απλή συμπλήρωση μιας αίτησης. Μπορεί να χρησιμοποιηθεί σε όλες τις επιχειρήσεις που φέρουν τα σήματα της Visa, στην Ελλάδα και το εξωτερικό καθώς και σε όλες τις αγορές μέσω τηλεφώνου ή internet. Το ποσό που μπορεί να δωριθεί κυμαίνεται από 50 έως 3.000 Ευρώ. Το αρχικό διαθέσιμο ποσό για αγορές τυπώνεται πάνω στην κάρτα, κάτω από το όνομα του κατόχου. Η κάρτα έχει ημερομηνία λήξεως που αναγράφεται στην όψη της κάτω από τον αριθμό της. Η κάρτα ισχύει μέχρι την

τελευταία ημέρα του μήνα που αναγράφεται. Εφόσον εξαντληθεί το διαθέσιμο υπόλοιπο της κάρτας για αγορές πριν τη λήξη της, είναι δυνατή η προμήθεια νέας κάρτας ανάλογα με την ανάγκες του κατόχου. Σε περίπτωση που η κάρτα κατά τη λήξη της έχει διαθέσιμο χρηματικό υπόλοιπο, αυτό επιστρέφεται στον κάτοχο αφού αφαιρεθούν τα λειτουργικά κόστη της τράπεζας. Κάτοχοι της κάρτας μπορεί να είναι και άτομα κάτω των 14 ετών (σύμφωνα με το Νόμο, ο ανήλικος από 14 χρόνων και πάνω μπορεί να διαθέτει ελεύθερα κάθε τι που του δόθηκε για να το χρησιμοποιεί). Εφόσον υπάρχουν αγορές, ο κάτοχος της κάρτας ενημερώνεται με λογαριασμό, ο οποίος αποστέλλεται στη διεύθυνση που έχει δηλώσει.

Για αγορές στο διαδίκτυο, η Attica Gift CARD VISA χρησιμοποιείται όπως μια πιστωτική κάρτα υπό την έννοια ότι ο κάτοχος δεν συνδέεται με τα συστήματα της τράπεζας προκειμένου να γίνει αναγνώριση του μέσω κωδικού χρήστη. Αντίθετα, ο κάτοχος αποστέλλει στα στοιχεία του στον έμπορο όπως συμβαίνει και με τις πιστωτικές κάρτες. Η αυξημένη ασφάλεια που προσφέρει η Attica Gift CARD VISA έγκειται στο γεγονός ότι η κάρτα δεν επιτρέπει συναλλαγές που να ξεπερνούν το διαθέσιμο υπόλοιπο με αποτέλεσμα να μην είναι δυνατή η υπερχρέωση του λογαριασμού από κάποιον που θα υποκλέψει τα στοιχεία της κάρτας.

Στην Attica Gift CARD VISA, δεδομένου ότι δεν έχει σχεδιαστεί για αποκλειστική χρήση στο Internet, κάποιες υπηρεσίες δεν είναι ψηφιακές. Για παράδειγμα, η ερώτηση υπολοίπου γίνεται μέσω τηλεφώνου υποχρεωτικά καθώς δεν υπάρχει εναλλακτικός τρόπος ενημέρωσης του κατόχου για το διαθέσιμο υπόλοιπο της κάρτας. Επίσης η αγορά της είναι δυνατή, όπως προαναφέρθηκε, μόνο από τα υποκαταστήματα της Τράπεζας Αττικής. Εντούτοις, ένα βασικό της πλεονέκτημα είναι ότι μπορεί να χρησιμοποιηθεί σε ένα μεγάλο εύρος καταστημάτων είτε φυσικών είτε ηλεκτρονικών, στην Ελλάδα και στο εξωτερικό, λόγω της συνεργασίας με την VISA. Έτσι, οι κάτοχοι της έχουν περισσότερες επιλογές και μεγαλύτερες δυνατότητες σε ότι αφορά στις αγορές τους. Επιπλέον, το ποσό με το οποίο «φορτώνεται» η κάρτα είναι ευέλικτο και καθορίζεται από τον ίδιο τον αγοραστή με αποτέλεσμα να επιτρέπει την προσαρμογή του προϊόντος στις απαιτήσεις και ανάγκες του. Έτσι, συνολικά η Attica Gift CARD VISA επιτρέπει σημαντική ευελιξία στις αγορές στο διαδίκτυο ακόμα και αν δεν σχεδιάστηκε με γνώμονα αποκλειστικά αυτές.

Όπως φαίνεται από την παρουσίαση των προπληρωμένων καρτών που διατίθενται αυτή τη στιγμή στην ελληνική αγορά, τα βασικά κίνητρα για τη δημιουργία τους σχετίζονται κυρίως με την δυσπιστία των καταναλωτών προς τις πληρωμές στο Internet και την ανάγκη προσέγγισης μικρών ηλικιακά ομάδων του πληθυσμού. Τόσο η egnatiaPrepay όσο και η Attica Gift CARD VISA δημιουργήθηκαν για να διασκεδάσουν τη δυσπιστία των ελληνικών καταναλωτών έναντι των πληρωμών μέσω Διαδικτύου. Η ύπαρξη συγκεκριμένου χρηματικού διαθέσιμου που είτε είναι περιορισμένης αξίας (100 Ευρώ στην egnatiaPrepay) είτε ορίζεται από τον κάτοχο της κάρτας (Attica gift CARD VISA) άρει ως ένα βαθμό την αίσθηση ανασφάλειας που έχουν πολλοί καταναλωτές όταν χρησιμοποιούν τις πιστωτικές τους κάρτες για αγορές στο διαδίκτυο και ενισχύει την σταδιακή εξοικείωση τους με τις αγορές σε ηλεκτρονικά καταστήματα. Επιπλέον, καθώς επιτρέπεται η απόκτηση τους από ανήλικους (από 14 ετών και άνω) οι τράπεζες προσεγγίζουν εκείνες τις ηλικιακές βαθμίδες που είναι περισσότερο εξοικειωμένες με τη χρήση του Διαδικτύου και που μέχρι τώρα δεν είχαν δυνατότητα να πραγματοποιήσουν αγορές με τα διαθέσιμα συστήματα ηλεκτρονικών πληρωμών στην Ελλάδα. Βέβαια, ένα βασικό πρόβλημα που αντιμετωπίζουν οι τράπεζες κατά την δημιουργία προϊόντων για πληρωμές αποκλειστικά στο διαδίκτυο είναι η περιορισμένη ανάπτυξη του ηλεκτρονικού εμπορίου στην Ελλάδα και η μικρή επιλογή σε επίπεδο εμπορευμάτων που είναι δυνατόν να αγοραστούν ηλεκτρονικά. Αυτό έχει σαν αποτέλεσμα να μην δραστηριοποιούνται πολλές τράπεζες στο χώρο των ηλεκτρονικών πληρωμών.

Εκείνες δε οι τράπεζες που προσφέρουν προϊόντα που στηρίζονται σε καινοτομικά συστήματα ηλεκτρονικών πληρωμών φροντίζουν να ενσωματώνουν εναλλακτικές χρήσεις στα προϊόντα αυτά, όπως έκανε η Τράπεζα Αττικής που δημιούργησε ένα υβριδικό προϊόν που χρησιμοποιείται τόσο on-line όσο και off-line.

Συμπερασματικά στην Ελλάδα, οι κάρτες προπληρωμένης αξίας, έχουν μικρό μερίδιο αγοράς έναντι των παραδοσιακών πιστωτικών καρτών. Αυτό οφείλεται αφενός στο γεγονός ότι αυτή τη στιγμή κυκλοφορούν μόλις δύο κάρτες ενώ και το ηλεκτρονικό εμπόριο δεν είναι ιδιαίτερα διαδεδομένο. Εντούτοις, με βάση δημοσιεύματα³⁴, αρκετές τράπεζες εξετάζουν την δραστηριοποίηση τους στο χώρο ορισμένες μάλιστα με συγκεκριμένα χρονοδιαγράμματα όπως η Τράπεζα Πειραιώς που σκοπεύει να εκδώσει προπληρωμένες κάρτες Visa ή Mastercard μέσα στο πρώτο εξάμηνο του 2004.

9.3 ΧΡΥΣΗ ΕΥΚΑΙΡΙΑ – ΑΓΟΡΕΣ ΑΓΓΕΛΙΩΝ ΜΕΣΩ ΚΙΝΗΤΟΥ

Η εφημερίδα αγγελιών Χρυσή Ευκαιρία είναι η πιο δημοφιλής εφημερίδα αγγελιών στην Ελλάδα. Ανήκει σε ένα από τους μεγαλύτερους εκδοτικούς οίκους στην Ελλάδα, τις Χ.Κ. Εκδόσεις Τεγόπουλος Α.Ε., ο οποίος διανείμει περίπου 60.000 φύλλα ημερησίως, με περισσότερες από 40.000 αγγελίες για κάθε φύλλο. Η Χρυσή Ευκαιρία (<http://www.x-e.gr/>) εισήγαγε μία Β2C εφαρμογή η οποία επιτρέπει στους επισκέπτες της ιστοσελίδας της να αναζητούν ηλεκτρονικά τις αγγελίες που φιλοξενούνται στην έντυπη έκδοσή της.

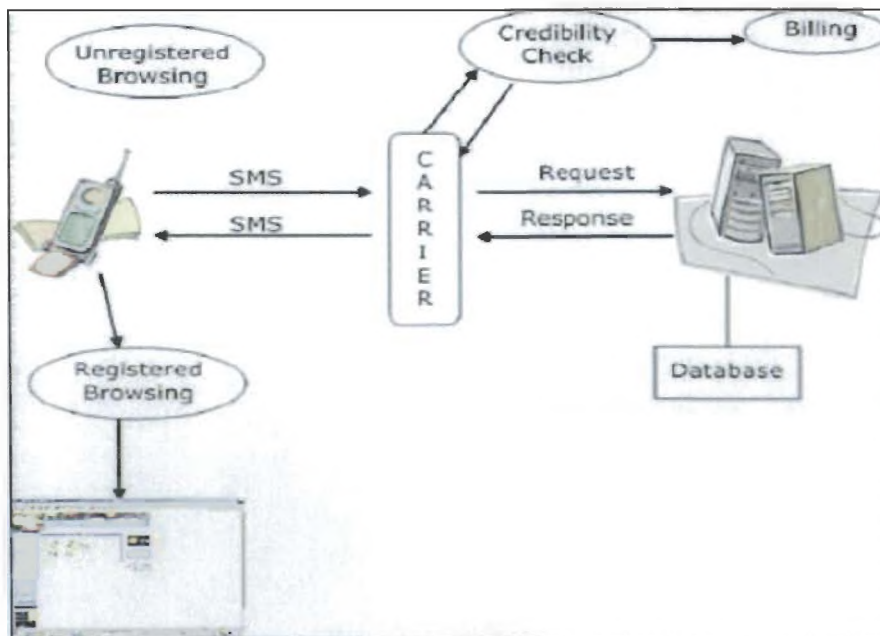
Ο Όμιλος «Χ.Κ. Τεγόπουλος Εκδόσεις Α.Ε.» συνειδητοποιώντας την ανάγκη των αναγνωστών του εντύπου της «Χρυσής Ευκαιρίας» για άμεση και ακόμη πιο γρήγορη ενημέρωση αλλά και αναζήτηση μικρών αγγελιών, ανεξαρτήτου ημέρας και ώρας, μετέφερε την εφημερίδα μικρών αγγελιών «Χρυσή Ευκαιρία» στο Internet. Η φιλοσοφία υλοποίησης του συγκεκριμένου συστήματος μικρών αγγελιών της «Χρυσής Ευκαιρίας» ήταν η ακριβής μεταφορά του εντύπου στο Internet, παρέχοντας στον αναγνώστη περισσότερες ευκολίες σχετικά με την αναζήτηση πληροφοριών που τον ενδιαφέρουν, καλύπτοντας όλη την γκάμα θεμάτων που εμπεριέχονται στο αντίστοιχο έντυπο. Το βασικό ζήτημα που έπρεπε να λυθεί κατά την υλοποίηση της νέας υπηρεσίας ήταν ο τρόπος πληρωμής της κάθε αγγελίας καθώς το κόστος αγγελίας ήταν αρκετά μικρό για να δικαιολογήσει την πληρωμή μέσω πιστωτικής κάρτας ενώ το ενδεχόμενο εβδομαδιαίας ή μηνιαίας συνδρομής στην υπηρεσία θα απέτρεπε πολλούς καταναλωτές καθώς απαιτείται πολύ μικρότερο διάστημα για την ανεύρεση της κατάλληλης αγγελίας. Ένα άλλο πρόβλημα που σχετιζόταν με τη χρήση πιστωτικών καρτών ήταν η χρονοβόρα φύση της διαδικασίας πληρωμής καθώς ο αγοραστής θα αναγκαζόταν να συμπληρώσει διάφορες φόρμες, που θα εξασφάλιζαν την πιστοποίηση των στοιχείων του. Επιπλέον, πολλοί καταναλωτές στην Ελλάδα διακρίνονται για τη δυσπιστία τους σε θέματα ασφάλειας κατά τη χρήση πιστωτικών καρτών. Ιδιαίτερα σημαντικό και για τον ίδιο τον όμιλο ήταν το γεγονός ότι το λειτουργικό κόστος δημιουργίας ενός ασφαλούς συστήματος ηλεκτρονικών πληρωμών με τη χρήση πιστωτικών καρτών είναι αρκετά υψηλό.

Τη λύση σε αυτά τα προβλήματα έδωσε ένας εξελιγμένος μηχανισμός, το Ezpay - παγκόσμια πατέντα της Information Systems Impact που ανέλαβε την υλοποίηση της

³⁴ Ημερησία (31/12/2003-4/1/2004). Τράπεζες: Ηλεκτρονικό εμπόριο a la cart Ένθετο Net Economy, σελ. 155.

στο ηλεκτρονικό σύστημα των μικρών αγγελιών και σχετίζεται με την προβολή των στοιχείων επικοινωνίας που πλαισιώνουν κάθε αγγελία³⁵. Πιο συγκεκριμένα ενώ μέχρι στιγμής στην έντυπη «Χρυσή Ευκαιρία» το κείμενο κάθε αγγελίας συνοδεύεται από τα στοιχεία επικοινωνίας, στην ηλεκτρονική έκδοση της εφημερίδας, ο αναγνώστης για να δει τα στοιχεία αυτά πρέπει να καταχωρήσει ένα κωδικό πρόσβασης στο σύστημα. Για να αποκτήσει ο αναγνώστης τον κωδικό αυτό, απαιτείται πληρωμή η οποία όμως δεν ολοκληρώνεται με τη χρήση πιστωτικής κάρτας, αλλά με τη χρήση κινητού τηλεφώνου. Ο χρήστης απλά στέλνει από το κινητό του τηλέφωνο ένα γραπτό μήνυμα SMS με περιεχόμενο ΧΕ στον αριθμό 1450. Στη συνέχεια μόλις το κέντρο μηνυμάτων, αποστέλλει στο κινητό του αναγνώστη μέσα σε μερικά δευτερόλεπτα ένα νέο μήνυμα SMS, το οποίο περιλαμβάνει τον κωδικό πρόσβασης στο σύστημα. Από τη στιγμή που ο αναγνώστης καταχωρήσει αυτόν τον κωδικό πρόσβασης στο σύστημα της ηλεκτρονικής «Χρυσής Ευκαιρίας» έχει πρόσβαση στο σύνολο της πληροφορίας κάθε μικρής αγγελίας συμπεριλαμβανομένων και των στοιχείων επικοινωνίας (όνομα, τηλέφωνο, κτλ) . Για την υπηρεσία αυτή, κατόπιν καταχώρησης του κωδικού στο σύστημα, χρεώνεται αυτόματα ο λογαριασμός του κινητού τηλεφώνου του χρήστη ή η προπληρωμένη κάρτα του (σε περίπτωση που πρόκειται για καρτοκινητό τηλέφωνο) με το ποσό των 1,7 Ευρώ και η συνδρομή ισχύει για 24 ώρες ή για 1 εβδομάδα ή μήνα ανάλογα με το πακέτο χρέωσης που έχει επιλέξει ο αναγνώστης. Αξίζει να αναφερθεί το γεγονός ότι η Information Systems Impact θέλοντας να καλύψει το ιδιαίτερα αυξημένο αριθμό ελλήνων συνδρομητών υπηρεσιών κινητής τηλεφωνίας, αλλά και ταυτόχρονα το πλήθος των αναγνωστών της «Χρυσής Ευκαιρίας», συνεργάστηκε με όλες τις εταιρίες παροχής υπηρεσιών κινητής τηλεφωνίας (Vodafone, TELESTET, COSMOTE) που λειτουργούν στην Ελλάδα.

Το παρακάτω σχήμα απεικονίζει την λειτουργία του συστήματος διεξαγωγής πληρωμών Ezpay της Impact Information Systems



Σχήμα 3: Σύστημα διεξαγωγής πληρωμών Ezpay της Χρυσής Ευκαιρίας

35 Presspoint.gr (14/03/2002). Αγορές στο Internet εύκολα, γρήγορα και με ασφάλεια; Η INFORMATION SYSTEMS impact και η Χρυσή Ευκαιρία αλλάζουν τα δεδομένα στο χώρο του Internet. Διαθέσιμο στο www.impact.gr/articles

Μέσα σε ένα μήνα από τη λειτουργία του συστήματος κινητών ηλεκτρονικών πληρωμών, διαπιστώθηκε ότι «αγοράσθηκαν» περίπου 6000 προσωπικοί κωδικοί. Από τους 5.000 ημερήσιους επισκέπτες της ηλεκτρονικής ιστοσελίδας, παρατηρήθηκαν 300 αγορές προσωπικών κωδικών, ποσοστό 6% των ημερήσιων επισκεπτών, για να έχουν πρόσβαση στο προστατευμένο περιεχόμενο.

10. ΤΟ ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΛΗΡΩΜΕΣ

Τα συστήματα ηλεκτρονικών πληρωμών πέραν των ζητημάτων τεχνολογικής υφής που τα διέπουν πρέπει επίσης να εναρμονίζονται με την νομοθεσία των χωρών στις οποίες και λειτουργούν. Με την εμφάνιση του Διαδικτύου και την πραγματοποίηση εμπορικών συναλλαγών μέσω αυτού ανέκυψε μια σειρά από νομικά ζητήματα που απασχόλησαν τόσο την ευρωπαϊκή ένωση όσο και τα επιμέρους κράτη - μέλη. Το βασικό πρόβλημα σε επίπεδο νομοθεσίας που αντιμετώπισαν οι περισσότερες εφαρμογές ηλεκτρονικών πληρωμών που αναπτύχθηκαν με την εμφάνιση του Διαδικτύου ήταν η έλλειψη ξεκάθαρων νομοθετικών ρυθμίσεων που να διέπουν τις ηλεκτρονικές συναλλαγές. Η ταχύτητα των τεχνολογικών εξελίξεων δεν επέτρεψε την άμεση ανταπόκριση της νομοθεσίας σε παγκόσμιο επίπεδο η οποία όχι μόνο δεν ήταν προετοιμασμένη για τις καινοτομικές μεθόδους πληρωμών που εμφανίστηκαν αλλά αδυνατούσε και να προσαρμοστεί άμεσα στις νέες εξελίξεις.

Τα βασικά ζητήματα που δυσχεραίνουν σε μεγάλο βαθμό την ρύθμιση των ηλεκτρονικών συναλλαγών εν γένη και των πληρωμών ειδικότερα, σχετίζονται κυρίως με την ίδια την φύση του διαδικτύου³⁶. Ειδικότερα, η φύση του Διαδικτύου που αναιρεί τα εθνικά σύνορα των κρατών έρχεται σε αντίθεση με την εδαφικότητα των νομοθετικών ρυθμίσεων. Επιπλέον, η ψηφιοποίηση των αντικειμένων που αποτελούν το αντικείμενο της συναλλαγής αναιρεί την παραδοσιακή έννοια του πράγματος που ίσχυε μέχρι τώρα. Ενώ οι εμπορικές πρακτικές στο διαδίκτυο είναι σε αρκετές περιπτώσεις διαφορετικές από τις παραδοσιακές με αποτέλεσμα να δημιουργούνται καινούρια συναλλακτικά ήθη για τα οποία απαιτούνται ιδιαίτερες κανονιστικές ρυθμίσεις.

Στην παρούσα ενότητα θα εξεταστεί η νομοθεσία που ρυθμίζει τις ηλεκτρονικές πληρωμές σε ευρωπαϊκό και εθνικό επίπεδο. Η παρούσα ενότητα αποσκοπεί κυρίως στην συνοπτική και επικαιροποιημένη παρουσίαση των νομοθετικών ρυθμίσεων που διέπουν τις ηλεκτρονικές πληρωμές στην Ευρωπαϊκή Ένωση και στην Ελλάδα προκειμένου να καταγράψει την πρόοδο που έχει γίνει και να εντοπίσει ενδεχόμενα προβλήματα που χρήζουν περαιτέρω ρυθμίσεων.

³⁶ Ενδεικτικός κατάλογος νομοθεσίας για τις ηλεκτρονικές συναλλαγές. Ebusiness Forum, σελ 1.

10.1 ΕΥΡΩΠΑΪΚΗ ΝΟΜΟΘΕΣΙΑ³⁷

Δεδομένων των προβλημάτων που δημιουργεί η ίδια η φύση του Διαδικτύου στις όποιες προσπάθειες νομοθετικής ρύθμισης των εμπορικών πράξεων που μετέρχονται ηλεκτρονικών μέσων προκειμένου να υλοποιηθούν. Η Ευρωπαϊκή Ένωση προχωρά σταδιακά σε μια συντονισμένη προσπάθεια αντιμετώπισης του προβλήματος³⁸ με την σταδιακή δημιουργία ενός νομικού πλαισίου που θα θέσει τις βάσεις για μια ολοκληρωμένη ρύθμιση των ηλεκτρονικών συναλλαγών σε κάθε επίπεδο αλλά και για τη σταδιακή αποδοχή του από το καταναλωτικό κοινό.

Στο επίκεντρο των προσπαθειών της Ευρωπαϊκής Ένωσης για τη νομοθετική ρύθμιση των ηλεκτρονικών συναλλαγών βρίσκεται η Οδηγία για το Ηλεκτρονικό Εμπόριο (2000/31/ΕΚ) που θέτει τις βάσεις για την ανάπτυξη του ηλεκτρονικού εμπορίου³⁹. Πρόκειται για μια οριζόντια οδηγία η οποία δεν αποσκοπεί στη ρύθμιση συγκεκριμένου κλάδου. Η οδηγία αυτή συνεπικουρείται από δύο κάθετες οδηγίες που καλύπτουν την έκδοση χρήματος και την νομική ισχύ των ηλεκτρονικών υπογραφών. Με τον τρόπο αυτό δημιουργείται ένα νομικό πλαίσιο για το ηλεκτρονικό εμπόριο το οποίο αποσκοπεί στην διευθέτηση των προβλημάτων που ανακύπτουν από τις online εμπορικές πράξεις και τις ηλεκτρονικές πληρωμές μεταξύ χωρών με διαφορετική νομική, συμβατική και δικονομική παράδοση. Το νομικό αυτό πλαίσιο συμπληρώνουν μια σειρά από οδηγίες, συστάσεις, και κανονισμοί που είτε συστάθηκαν προκειμένου να ρυθμίσουν ηλεκτρονικές μορφές συναλλαγών είτε είναι σχετικές χωρίς βέβαια να αναφέρονται ρητά στις ηλεκτρονικές συναλλαγές. Στον πίνακα που ακολουθεί παρουσιάζεται συνοπτικά η Ευρωπαϊκή Νομοθεσία σχετικά με τις ηλεκτρονικές πληρωμές. Στη συνέχεια τα επιμέρους νομοθετήματα παρουσιάζονται και αναλύονται διεξοδικά.

37 Το πλήρες κείμενο των ευρωπαϊκών νομοθετημάτων που παρουσιάζονται σε αυτή την ενότητα μπορεί να βρεθεί στην ιστοσελίδα της Ευρωπαϊκής Ένωσης (<http://europa.eu.int>). Η ευρωπαϊκή και ελληνική νομοθεσία σε θέματα ηλεκτρονικών πληρωμών είναι επίσης διαθέσιμη σε ηλεκτρονική μορφή στην ιστοσελίδα του προγράμματος «Δικτυωθείτε» του Υπουργείου Ανάπτυξης, www.eso-online.gr, και στην ιστοσελίδα του Εμπορικού και Βιομηχανικού Επιμελητηρίου Αθηνών, www.acci.gr/ecommerce/legal.

38 Ενδεικτικός κατάλογος νομοθεσίας για τις ηλεκτρονικές συναλλαγές. E-Business Forum, σελ 2.

39 European Central Bank . E-Payments in Europe: The Eurosystem's Perspective. Issues Paper.

Νομοθεσία Ευρώπης

Κανονισμός (ΕΚ) 2560/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 19ης Δεκεμβρίου 2001 σχετικά με τις διασυνοριακές πληρωμές σε Ευρώ
Οδηγία 87/102/ΕΟΚ του Συμβουλίου της 22ας Δεκεμβρίου 1986 για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη
Οδηγία 90/88/ΕΟΚ του Συμβουλίου της 22ας Φεβρουαρίου 1990 για την τροποποίηση της οδηγίας 87/102/ΕΟΚ για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη
Οδηγία 97/5/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Ιανουαρίου 1997 για τις διασυνοριακές μεταφορές πιστώσεων
Οδηγία 97/7/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ής Μαΐου 1997 για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις
Οδηγία 2000/12/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ής Μαρτίου 2000 σχετικά με την ανάληψη και την άσκηση δραστηριότητας πιστωτικών ιδρυμάτων
Οδηγία 2000/28/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 18ης Σεπτεμβρίου 2000 για τροποποίηση της οδηγίας 2000/12/ΕΚ σχετικά με την ανάληψη και την άσκηση δραστηριότητας πιστωτικών ιδρυμάτων
Οδηγία 2000/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 18ης Σεπτεμβρίου 2000 για την ανάληψη, την άσκηση και την προληπτική εποπτεία της δραστηριότητας ιδρύματος ηλεκτρονικού χρήματος
Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην Εσωτερική Αγορά («Οδηγία για το ηλεκτρονικό εμπόριο»)
Σύσταση της Επιτροπής 87/598/ΕΟΚ της 8ης Δεκεμβρίου 1987 για ευρωπαϊκό κώδικα δεοντολογίας σε θέματα ηλεκτρονικών πληρωμών (Σχέσεις μεταξύ χρηματοπιστωτικών οργανισμών, εμπόρων ή άλλων παρεχόντων υπηρεσιών και καταναλωτών)
Σύσταση της Επιτροπής 88/590/ΕΟΚ της 17ης Νοεμβρίου 1988 που αφορά τα συστήματα πληρωμών και ιδίως τις σχέσεις μεταξύ κατόχου και εκδότη κάρτας
Σύσταση 97/489/ΕΚ καλύπτει τις συναλλαγές που διενεργούνται με ηλεκτρονικά μέσα πληρωμής. Τα μέσα αυτά περιλαμβάνουν εκείνα που επιτρέπουν την (εξ αποστάσεως) πρόσβαση στο λογαριασμό ενός πελάτη ιδίως τις κάρτες πληρωμής και τις μέσω τηλεφώνου ή κατ' οίκον τραπεζικές εργασίες

Πίνακας 10: Ευρωπαϊκή νομοθεσία για την ρύθμιση των ηλεκτρονικών πληρωμών (με χρονολογική κατάταξη)

Κανονισμός (ΕΚ) αριθ. 2560/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 19^{ης} Δεκεμβρίου 2001 σχετικά με τις διασυνοριακές πληρωμές σε Ευρώ. Ο παρών κανονισμός θεσπίζει κανόνες σχετικά με τις διασυνοριακές πληρωμές σε Ευρώ προκειμένου να εξασφαλιστεί ότι το κόστος για τις πληρωμές αυτές είναι ίδιο με το κόστος των πληρωμών σε Ευρώ που πραγματοποιούνται στο εσωτερικό κράτους μέλους. Ως διασυνοριακές πληρωμές ο παρών ορισμός θεωρεί τις διασυνοριακές μεταφορές πίστωσης, τις διασυνοριακές επιταγές και τις διασυνοριακές πράξεις ηλεκτρονικής πληρωμής. Ειδικότερα, οι διασυνοριακές πράξεις ηλεκτρονικής πληρωμής στις οποίες και επικεντρώνεται η παρούσα ανάλυση ορίζονται ως:

- οι διασυνοριακές μεταφορές χρηματικών ποσών με μέσο ηλεκτρονικής πληρωμής, εκτός από εκείνες τις οποίες εντέλλονται και εκτελούνται από ιδρύματα, και
- οι διασυνοριακές αναλήψεις μετρητών με μέσο ηλεκτρονικής πληρωμής καθώς και η φόρτιση (και αποφόρτιση) υποθέματος ηλεκτρονικού χρήματος σε μηχανήματα αυτόματης ανάληψης και σε αυτόματες ταμειολογιστικές μηχανές στα καταστήματα του εκδότη ή ενός ιδρύματος που έχει συμβατική υποχρέωση να αποδέχεται το μέσο πληρωμής,

Είναι επομένως προφανές ότι οι διατάξεις του συγκεκριμένου κανονισμού δεν αφορούν μόνο στα τραπεζικά ιδρύματα αλλά και σε άλλες ατομικές ή εταιρικές επιχειρήσεις που εκτελούν διασυνοριακές πληρωμές καθώς με βάση την Οδηγία 200/46/ΕΚ, που αναλύουμε στη συνέχεια, στην έννοια του πιστωτικού ιδρύματος εμπίπτουν και τα ιδρύματα ηλεκτρονικού χρήματος⁴⁰. Ο Κανονισμός ορίζει τα έξοδα που επιβάλλονται από τα πιστωτικά ιδρύματα κατά την πραγματοποίηση διασυνοριακών πληρωμών ενώ ορίζονται και οι πληροφορίες που πρέπει να παρέχονται στους καταναλωτές. Έτσι, κάθε ίδρυμα παρέχει εκ των προτέρων στους πελάτες του, με άμεσα κατανοητή μορφή, γραπτώς, καθώς και κατά περίπτωση, βάσει των εθνικών κανόνων, με ηλεκτρονικά μέσα, πληροφορίες σχετικά με τα έξοδα που επιβάλλει για διασυνοριακές πληρωμές και για πληρωμές στο εσωτερικό του κράτους μέλους στο οποίο είναι εγκατεστημένο.

Οδηγία 87/102/ΕΟΚ του Συμβουλίου για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη. Στην οδηγία αυτή περιλαμβάνονται οι ορισμοί των εννοιών «καταναλωτής», «πιστωτικός φορέας», «σύμβαση πίστωσης», «συνολικό κόστος πίστωσης για τον καταναλωτή» και «συνολικό ετήσιο πραγματικό επιτόκιο». Ειδικότερα, η Οδηγία ρυθμίζει τι πρέπει να αναφέρει κάθε διαφήμιση για χορήγηση πίστωσης ή μεσολάβησης για σύναψη συμβάσεων που εκτίθεται σε εμπορικά καταστήματα. Επίσης, ρυθμίζεται και ο τρόπος που καταρτίζονται οι συμβάσεις πίστωσης και τι πρέπει να αναφέρεται απαραίτητα μέσα σε αυτές. Τέλος, αναφέρονται οι υποχρεώσεις και τα δικαιώματα του καταναλωτή σχετικά με τις υπηρεσίες και τις συμβάσεις πίστωσης.

Οδηγία 90/88/ΕΟΚ του Συμβουλίου της 22^{ης} Φεβρουαρίου 1990 για την τροποποίηση της οδηγίας 87/102/ΕΟΚ για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη. Στη συγκεκριμένη οδηγία περιλαμβάνονται οι τροποποιήσεις των ορισμών «συνολικό κόστος πίστωσης για τον καταναλωτή» και «συνολικό ετήσιο πραγματικό επιτόκιο».

⁴⁰ Γκόρτσος, Χ. Βλ. (2002). Ο Κανονισμός. 2560/2001 σχετικά με τις διασυνοριακές πληρωμές σε Ευρώ. Δελτίο ΕΕΤ, Α' Τριμηνία, σελ. 40-49.

Οδηγία 97/5/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27^{ης} Ιανουαρίου 1997 για τις διασυνοριακές μεταφορές πιστώσεων. Οι διατάξεις της παρούσας οδηγίας εφαρμόζονται επί των διασυνοριακών μεταφορών πιστώσεων που διεξάγονται στα νομίσματα των κρατών μελών και σε Ecu και δεν υπερβαίνουν το ισοδύναμο ποσό των 50 000 Ecu. Επιπλέον, στην Οδηγία 97/5/ΕΚ περιλαμβάνονται οι ορισμοί των εννοιών Πιστωτικό ίδρυμα, Χρηματοπιστωτικό ίδρυμα, Διασυνοριακή μεταφορά πίστωσης, Εντολή διασυνοριακής μεταφοράς πίστωσης, Εντολέας, κ.α. Προσδιορίζονται επίσης τα στοιχεία που πρέπει να έχουν τα πιστωτικά ιδρύματα πριν από την εντολή εκτέλεσης διασυνοριακής μεταφοράς πίστωσης⁴¹. Αλλά και ποιες πληροφορίες οφείλουν να παρέχουν στους πελάτες τους μετά την εκτέλεση ή την άφιξη διασυνοριακής μεταφοράς πίστωσης. Πιο συγκεκριμένα, τα στοιχεία αυτά είναι:

- Στοιχεία που θα επιτρέπουν στον πελάτη να εξακριβώσει τη διασυνοριακή μεταφορά πίστωσης.
- Το αρχικό ποσό της διασυνοριακής μεταφοράς πίστωσης.
- Το ποσό των κάθε είδους εξόδων και προμηθειών που βαρύνουν τον πελάτη.
- Την τυχόν υπάρχουσα ημερομηνία αξίας την οποία εφαρμόζει το ίδρυμα.

Επιπλέον σε ότι αφορά τις ελάχιστες υποχρεώσεις των ιδρυμάτων σχετικά με τις διασυνοριακές μεταφορές πιστώσεων αναφέρεται ρητά ότι το ίδρυμα υποχρεούται, εφόσον το ζητήσει ο πελάτης, σε σχέση με διασυνοριακή μεταφορά πίστωσης επακριβώς περιγραφόμενη, να δεσμευθεί ως προς την προθεσμία εκτέλεσης αυτής της μεταφοράς πίστωσης και ως προς τις προμήθειες και τα έξοδα που απορρέουν από αυτήν. Το ίδρυμα του εντολέα υποχρεούται να εκτελέσει τη διασυνοριακή μεταφορά πίστωσης εντός της προθεσμίας που έχει συμφωνήσει με τον εντολέα.

Οδηγία 97/7/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ής Μαΐου 1997 για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις. Η παρούσα οδηγία έχει ως αντικείμενο την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών, οι οποίες αφορούν τις εξ αποστάσεως συμβάσεις μεταξύ καταναλωτών και προμηθευτών.

Ως εξ αποστάσεων σύμβαση ορίζεται κάθε σύμβαση μεταξύ ενός προμηθευτή και ενός καταναλωτή που αφορά αγαθά ή υπηρεσίες, η οποία συνάπτεται στα πλαίσια ενός συστήματος πωλήσεων ή παροχής υπηρεσιών εξ αποστάσεως, που οργανώνεται από τον προμηθευτή, ο οποίος, με τη σύμβαση αυτή, χρησιμοποιεί αποκλειστικά ένα ή περισσότερα μέσα επικοινωνίας εξ αποστάσεως έως τη σύναψη της συμβάσεως, συμπεριλαμβανομένης και αυτής καθεαυτής της σύναψης της συμβάσεως.

Τα κίνητρα για τη ρύθμιση των εξ αποστάσεων συμβάσεων εντοπίζονται στο γεγονός ότι η διασυνοριακή πώληση εξ αποστάσεως μπορεί να είναι μια από τις κυριότερες εκδηλώσεις της ολοκλήρωσης της εσωτερικής αγοράς για τους καταναλωτές καθώς και στο γεγονός ότι η καθιέρωση νέων τεχνολογιών συνεπάγεται πολλαπλασιασμό των μέσων που τίθενται στη διάθεση των καταναλωτών για να γνωρίσουν τις προσφορές που γίνονται σε ολόκληρη την Κοινότητα. Δεδομένου ότι ορισμένα κράτη μέλη έχουν ήδη λάβει διαφορετικά ή αποκλίνοντα μέτρα προστασίας των καταναλωτών στον τομέα της πώλησης εξ αποστάσεως με αρνητικές συνέπειες

41 Law Net S.A

για τον ανταγωνισμό ,μεταξύ των επιχειρήσεων στην ενιαία αγορά κρίθηκε αναγκαίο να θεσπιστεί ελάχιστο σύνολο κοινών κανόνων σε κοινοτικό επίπεδο στον τομέα αυτόν. Η Οδηγία 97/7/ΕΚ ρυθμίζει τις πληροφορίες που πρέπει να παρέχονται πριν και μετά τη σύναψη της σύμβασης καθώς και τους τρόπους με τους οποίους μπορεί να προστατευθεί ο καταναλωτής όταν έχει πληρώσει με τη πιστωτική του κάρτα ή όταν του παρέχονται υπηρεσίες και αγαθά που δεν έχει ζητήσει.

Οδηγία 2000/12/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ής Μαρτίου 2000 σχετικά με την ανάληψη και την άσκηση δραστηριότητας πιστωτικών ιδρυμάτων. Στην οδηγία αυτή αναλύονται όλα τα θέματα που αφορούν στη δραστηριότητα των πιστωτικών ιδρυμάτων.

Οδηγία 2000/28/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 18ης Σεπτεμβρίου 2000. Η Οδηγία 2000/28/ΕΚ τροποποιεί την οδηγία 2000/12/ΕΚ σχετικά με την ανάληψη και την άσκηση δραστηριότητας πιστωτικών ιδρυμάτων προσθέτοντας διατάξεις σχετικά με το ηλεκτρονικό χρήμα. Ειδικότερα στον ορισμό «Πιστωτικό-ίδρυμα» αναφέρει ότι είναι:

- επιχείρηση της οποίας η δραστηριότητα συνίσταται στην αποδοχή από το κοινό καταθέσεων ή άλλων επιστρεπτέων κεφαλαίων και στη χορήγηση πιστώσεων για ίδιο λογαριασμό, ή
- ίδρυμα ηλεκτρονικού χρήματος κατά την έννοια της οδηγίας 2000/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Σεπτεμβρίου 2000, για την ανάληψη, την άσκηση και την προληπτική εποπτεία της δραστηριότητας ιδρύματος ηλεκτρονικού χρήματος.

Οδηγία 2000/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 18ης Σεπτεμβρίου 2000 για την ανάληψη, την άσκηση και την προληπτική εποπτεία της δραστηριότητας ιδρύματος ηλεκτρονικού χρήματος. Η Οδηγία ορίζει ως «ίδρυμα ηλεκτρονικού χρήματος» μια επιχείρηση ή άλλου τύπου νομικό πρόσωπο εκτός του πιστωτικού ιδρύματος κατά την έννοια του άρθρου 1, σημείο 1, πρώτο εδάφιο στοιχείο α) της οδηγίας 2000/12/ΕΚ, η οποία εκδίδει μέσα πληρωμής υπό μορφή ηλεκτρονικού χρήματος. Επίσης, η Οδηγία αυτή ορίζει και την έννοια του ηλεκτρονικού χρήματος ως νομισματική αξία, η οποία αντιστοιχεί σε απαίτηση έναντι του εκδότη και:

- α) είναι αποθηκευμένη σε ηλεκτρονικό υπόθεμα,
- β) έχει εκδοθεί κατόπιν παραλαβής χρηματικού ποσού και
- γ) γίνεται δεκτή ως μέσο πληρωμής από επιχειρήσεις άλλες, πέραν της εκδότριας.»

Επίσης, με βάση την συγκεκριμένη Οδηγία ρυθμίζεται πότε και πώς μπορεί ο κομιστής ηλεκτρονικού χρήματος να ζητήσει την εξαργύρωση του στην ονομαστική αξία σε κέρματα και χαρτονομίσματα ή με μεταφορά σε τραπεζικό λογαριασμό. Ρυθμίζονται οι περιορισμοί στην έκδοση ηλεκτρονικού χρήματος καθώς και οι κυρώσεις που συνεπάγεται η παραβίαση του Νόμου. Ενώ ρυθμίζονται και οι όροι και προϋποθέσεις ίδρυσης και λειτουργίας ιδρυμάτων ηλεκτρονικού χρήματος.

Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην Εσωτερική Αγορά («Οδηγία για το ηλεκτρονικό εμπόριο»). Ο στόχος της Οδηγίας είναι η τόνωση της οικονομικής ανάπτυξης, της ανταγωνιστικότητας και των επενδύσεων, αίροντας τα πολυάριθμα εμπόδια στην εσωτερική αγορά, στον τομέα της παροχής υπηρεσιών ηλεκτρονικού εμπορίου. Για το σκοπό αυτό, όπως προαναφέρθηκε, η οδηγία είναι οριζόντια

δηλαδή δεν ρυθμίζει νομοθετικά κάποιο συγκεκριμένο τομέα αλλά θέτει τις βάσεις για τη δημιουργία ενός νομικού πλαισίου για τη συνολικότερη ρύθμιση των ηλεκτρονικών πληρωμών. Βασικό κίνητρο για την ψήφιση της συγκεκριμένης οδηγίας υπήρξε το γεγονός ότι το νομικό πλαίσιο στα κράτη μέλη δεν είναι σαφές, λόγω των διαφορών ορισμένων νομοθεσιών εφαρμοστέων στις υπηρεσίες της κοινωνίας της πληροφορίας. Το γεγονός αυτό δημιουργεί νομική ανασφάλεια ενώ η διαφορετική αντιμετώπιση των κρατών μελών στα διάφορα ζητήματα που ανακύπτουν σχετικά με τις υπηρεσίες της κοινωνίας της πληροφορίας ενδέχεται να οδηγήσουν στον κατακερματισμό της εσωτερικής αγοράς. Για το σκοπό αυτό η οδηγία θέτει συγκεκριμένους εναρμονισμένους ορισμούς για της έννοιες «υπηρεσία της κοινωνίας των πληροφοριών», «φορέας παροχής υπηρεσιών», «εγκατεστημένος φορέας παροχής υπηρεσιών», «αποδέκτης της υπηρεσίας», «καταναλωτής», «εμπορικές επικοινωνίες», «νομοθετικός κατοχυρωμένο επάγγελμα » και «συντονισμένος τομέας».

Στο επίκεντρο της οδηγίας βρίσκεται η έννοια του κράτους εγκατάστασης με βάση το οποίο ρυθμίζεται το νομικό καθεστώς παροχής ηλεκτρονικών υπηρεσιών. Η οδηγία θέτει επίσης μέτρα διαφάνειας για την εμπορική επικοινωνία και ορίζει περιπτώσεις στις οποίες εξαιρούνται οι παροχείς τεχνολογικών λύσεων από νομικές υποχρεώσεις.

Σύσταση της Επιτροπής 87/598/ΕΟΚ της 8ης Δεκεμβρίου 1987 για ευρωπαϊκό κώδικα δεοντολογίας σε θέματα ηλεκτρονικών πληρωμών.(Σχέσεις μεταξύ χρηματοπιστωτικών οργανισμών, εμπόρων ή άλλων παρεχόντων υπηρεσίες και καταναλωτών). Ο κώδικας συνοψίζει τους όρους που πρέπει να πληρούνται για να καταστεί δυνατή η ανάπτυξη των νέων μέσων ηλεκτρονικής πληρωμής προς όφελος των οικονομικών εταίρων, να εξασφαλιστεί ασφάλεια και ευκολία χρήσης στους καταναλωτές, μεγαλύτερη παραγωγικότητα και αυξημένη ασφάλεια στους παρέχοντες υπηρεσίες και τους εκδότες των καρτών πληρωμής. Οι βασικές αρχές του κώδικα σχετίζονται με:

- τους όρους των συμβάσεων που καταρτίζονται μεταξύ εκδοτών και καταναλωτών,
- τη διαλειτουργικότητα του συστήματος προκειμένου οι κάρτες που εκδίδονται σε ένα κράτος να μπορούν να χρησιμοποιηθούν σε άλλα,
- τον εξοπλισμό που απαιτείται από τους παροχείς υπηρεσιών ηλεκτρονικών πληρωμών,
- Την προστασία των δεδομένων τα οποία διαβιβάζονται, τη στιγμή της πληρωμής, στην τράπεζα του παρέχοντος υπηρεσίες και στη συνέχεια στον εκδότη. Τα δεδομένα αυτά δεν πρέπει σε καμία περίπτωση να θέσουν σε κίνδυνο την προστασία της ιδιωτικής ζωής και περιορίζονται αυστηρά στα στοιχεία που προβλέπονται συνήθως για τις επιταγές και τις μεταφορές ποσών από λογαριασμό σε λογαριασμό.
- Τη δίκαιη πρόσβαση στο σύστημα ηλεκτρονικών πληρωμών σε όσους παρέχονται υπηρεσίες, όποια και αν είναι η οικονομική τους σημασία. Ο αποκλεισμός από την πρόσβαση δεν είναι δυνατός παρά μόνο για νομικούς λόγους.

Σύσταση της Επιτροπής 88/590/ΕΟΚ της 17ης Νοεμβρίου 1988 που αφορά τα συστήματα πληρωμών και ιδίως τις σχέσεις μεταξύ κατόχου και εκδότη κάρτας. Η

Σύσταση αυτή προβλέπει ότι στον καταναλωτή πρέπει να παρέχονται οι κατάλληλες πληροφορίες για τους συμβατικούς όρους, κυρίως σχετικά με τη συνδρομή και τα άλλα πιθανά έξοδα που πρέπει να καταβάλει, καθώς και τα δικαιώματα που απορρέουν από τη σύμβαση.

Σύσταση 97/489/ΕΚ. Η συγκεκριμένη σύσταση καλύπτει τις συναλλαγές που διενεργούνται με ηλεκτρονικά μέσα πληρωμής. Πρόκειται για επικαιροποίηση της Σύστασης 88/590/ΕΟΚ προκειμένου να περιληφθούν και οι ηλεκτρονικές πληρωμές. Στόχος της είναι η προώθηση της εμπιστοσύνης των πελατών στα μέσα αυτά και η αποδοχή τους από τον τομέα του λιανικού εμπορίου. Η σύσταση αφορά συναλλαγές των ακόλουθων κατηγοριών:

- Μεταφορές χρηματικών ποσών εκτός των εντελλόμενων και εκτελούμενων από χρηματοπιστωτικά ιδρύματα που γίνονται με μέσο ηλεκτρονικής πληρωμής
- αναλήψεις μετρητών με μέσο ηλεκτρονικής πληρωμής και φόρτιση (και αποφόρτιση) μέσου ηλεκτρονικού χρήματος σε μηχανήματα αυτόματης ανάληψης και σε αυτόματες ταμειολογιστικές μηχανές ή στα καταστήματα του εκδότη ή ενός ιδρύματος που έχει συμβατική υποχρέωση να αποδέχεται το μέσο πληρωμής.

Στα πλαίσια της Σύστασης 97/489/ΕΚ ορίζονται οι έννοιες «μέσο ηλεκτρονικής πληρωμής», «μέσο πληρωμής με πρόσβαση εξ αποστάσεως», «μέσο ηλεκτρονικού χρήματος», «χρηματοπιστωτικό ίδρυμα» «εκδότης» και «κάτοχος». Επίσης προσδιορίζονται οι ελάχιστες πληροφορίες που πρέπει να περιέχονται στους όρους και τις προϋποθέσεις που διέπουν την έκδοση και χρησιμοποίηση ηλεκτρονικού μέσου πληρωμής καθώς και οι πληροφορίες που πρέπει να παρέχονται μετά τη συναλλαγή στον καταναλωτή. Τέλος, καθορίζονται οι υποχρεώσεις και οι ευθύνες των μερών δηλαδή του κατόχου και του εκδότη μέσου ηλεκτρονικής πληρωμής, ενώ αναφέρεται και η υποχρέωση του εκδότη να προσφέρει στον καταναλωτή τα απαραίτητα μέσα γνωστοποίησης π.χ. για κλοπή της κάρτας.

10.2 ΕΛΛΗΝΙΚΗ ΝΟΜΟΘΕΣΙΑ

Στην Ελλάδα, οι αρμόδιες αρχές έχουν περιοριστεί στην συμμόρφωση του εσωτερικού δικαίου προς τα ευρωπαϊκά νομοθετήματα που ήδη ισχύουν. Πέραν δε της νομολογίας που έχει ρυθμίσει ειδικότερα πρακτικά ζητήματα δεν υπάρχουν νομοθετήματα προσαρμοσμένα στις ιδιαιτερότητες της ελληνικής αγοράς. Βέβαια, παρά τα όποια προβλήματα διαφαίνεται η σταδιακή δημιουργία ενός νομοθετικού πλαισίου που θα αποτελέσει την βάση για την ρύθμιση του ηλεκτρονικού εμπορίου εν γένη και των ηλεκτρονικών πληρωμών ειδικότερα. Αυτό που χρειάζεται σε επίπεδο ελληνικής νομοθεσίας είναι η έκδοση εξειδικευμένων κανονισμών από τις αρμόδιες αρχές προκειμένου να δοθεί η απαραίτητη ώθηση στο ηλεκτρονικό εμπόριο στην χώρα μας.

Τα νομοθετήματα που ρυθμίζουν το νομικό καθεστώς διενέργειας ηλεκτρονικών πληρωμών στην Ελλάδα παρουσιάζονται συνοπτικά στον πίνακα που ακολουθεί ενώ στη συνέχεια το περιεχόμενο τους παρουσιάζεται και αναλύεται εκτενώς.

Ελληνική Νομοθεσία

Νόμος Υπ' Αριθ 3148/2003 Επιτροπή Λογιστικής Τυποποίησης και Ελέγχων: Επιτροπή Λογιστικής Τυποποίησης και Ελέγχων, αντικατάσταση και συμπλήρωση των διατάξεων για τα ιδρύματα ηλεκτρονικού χρήματος και άλλες διατάξεις
Προεδρικό Διάταγμα 33.2000: Προσαρμογή της Ελληνικής νομοθεσίας προς την Οδηγία 97/5/ΕΚ της 27.1.1997 για τις διασυνοριακές μεταφορές πιστώσεων
Υπουργική Απόφαση Ζ1-178/2001: Συναλλαγές που γίνονται με κάρτες - Εναρμόνιση με τις διατάξεις της Σύστασης 97/489/ΕΚ της Επιτροπής . Καταναλωτική πίστη - Προσαρμογή της Κοινής Υπουργικής Απόφασης Φ1-983/91 προς τις διατάξεις της Οδηγίας 98/7/ΕΚ του Ευρωπαϊκού Κοινοβουλίου
Πράξη Συμβουλίου Νομισματικής Πολιτικής Αριθ. 50/31.7.2002: Καθορισμός πλαισίου επίβλεψης συστημάτων πληρωμών
Πράξη Διοικητή Αριθμ. 2501/31.10.2002: Ενημέρωση των συναλλασσομένων με τα πιστωτικά ιδρύματα για τους όρους που διέπουν τις συναλλαγές τους

Πίνακας 11:Ελληνική νομοθεσία για την ρύθμιση των ηλεκτρονικών πληρωμών

Νόμος 3148/2003: Ο νόμος αυτός ρυθμίζει τη σύσταση και τις αρμοδιότητες της Επιτροπής Λογιστικής Τυποποίησης και Ελέγχων (Ε.Λ.Τ.Ε.). Επίσης έχει γίνει προσθήκη ειδικού κεφαλαίου στον νόμο για τα ιδρύματα ηλεκτρονικού χρήματος. Ειδικότερα, σε ότι αφορά στα ιδρύματα ηλεκτρονικού χρήματος με το Νόμο 3148/2003 σκοπεύει η ενσωμάτωση στην ελληνική τραπεζική νομοθεσία των διατάξεων της 2000/12/ΕΚ Οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου «σχετικά με την ανάληψη και την άσκηση δραστηριότητας πιστωτικών ιδρυμάτων» (L 126/ 26.5.2000), των διατάξεων της 2000/46/ ΕΚ Οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου «για την ανάληψη, άσκηση και προληπτική εποπτεία δραστηριότητας ιδρύματος ηλεκτρονικού χρήματος» (L 275/27.10.2000).

Προεδρικό Διάταγμα 33.2000: Το παρόν Διάταγμα έχει σαν σκοπό τη προσαρμογή της Ελληνικής Νομοθεσίας προς τις διατάξεις της Οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου 97/5/ΕΚ της 27ης Ιανουαρίου 1997 "για τις διασυνοριακές μεταφορές πιστώσεων

Υπουργική Απόφαση Ζ1-178/2001: Σκοπός αυτής της απόφασης είναι η εναρμόνιση προς τις διατάξεις της Σύστασης 97/489/ΕΚ της Επιτροπής της 30ης Ιουλίου 1997 "σχετικά με τις συναλλαγές που γίνονται με μέσα ηλεκτρονικής πληρωμής και ιδίως όσον αφορά τις σχέσεις μεταξύ του εκδότη και του κατόχου" και η προσαρμογή της Κοινής Υπουργικής Απόφασης Φ1-983/91 για την καταναλωτική πίστη (ΦΕΚ Β' 172), όπως ισχύει, προς τις διατάξεις της Οδηγίας 98/7/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 16ης Φεβρουαρίου 1998 "σχετικά με την τροποποίηση της οδηγίας 87/102/ΕΟΚ.

Πράξη Συμβουλίου Νομισματικής Πολιτικής 50/31.7.2002: Η παρούσα Πράξη καθορίζει το πλαίσιο επίβλεψης των συστημάτων πληρωμών. Ειδικότερα περιλαμβάνονται οι ορισμοί των εννοιών ηλεκτρονική πληρωμή, ηλεκτρονικό χρήμα,

πιστωτικός κίνδυνος, διαχειριστής συστημάτων πληρωμών καθώς και άλλες βασικές έννοιες. Στην Πράξη αυτή ορίζεται το σύστημα πληρωμών ως σύστημα που συνίσταται σε σύνολο μέσων και τραπεζικών διαδικασιών που χρησιμοποιούνται, με βάση συμβάσεις και σύμφωνα με τους σχετικούς κανονισμούς λειτουργίας, από ομάδα προσώπων και οργανισμών για να εξυπηρετηθεί, διευκολυνθεί και διασφαλισθεί η ομαλή μεταφορά κεφαλαίων και κυκλοφορία του χρήματος σε μία περιοχή, συνήθως σε μία χώρα. Υπό την έννοια αυτή το σύστημα πληρωμών περιλαμβάνει: (i) τα πιστωτικά ιδρύματα και τους χρηματοδοτικούς οργανισμούς, (ii) τα μη πιστωτικά ιδρύματα που παρέχουν υπηρεσίες για τη διενέργεια πληρωμών, (iii) την τεχνική υποδομή, (iv) το δίκτυο διασύνδεσης των φορέων που μεσολαβούν στις πληρωμές, (v) τις διαδικασίες εκκαθάρισης, συμψηφισμού και διακανονισμού των πληρωμών και (vi) τους κανόνες που διέπουν τα μέσα πληρωμής και την εν γένει λειτουργία του συστήματος.

Επιπλέον, η Πράξη Αριθ. 50/31.7.2002 προσδιορίζει τις γενικές αρχές λειτουργίας των συστημάτων ηλεκτρονικού χρήματος καθώς και την σκοπιμότητα της άσκησης εποπτείας από μέρος της Τράπεζας της Ελλάδος. Τέλος, η Πράξη προσδιορίζει τα στοιχεία που πρέπει να υποβάλλονται από τους διαχειριστές συστημάτων πληρωμών και ηλεκτρονικού χρήματος στην Τράπεζα της Ελλάδος, Διεύθυνση Νομισματικής Πολιτικής και Τραπεζικών Εργασιών, Γραφείο Επίβλεψης Συστημάτων Πληρωμών πριν από την έναρξη λειτουργίας τους, σε εξαμηνιαία βάση, σε ετήσια βάση, και σε περιπτώσεις έκτακτων περιστατικών.

Ειδικότερα, σε ότι αφορά στα συστήματα πληρωμών, πριν από την έναρξη λειτουργίας του συστήματος υποβάλλονται τα παρακάτω στοιχεία:

1. Νομικό πλαίσιο λειτουργίας του συστήματος όπως αυτό εκφράζεται από το καταστατικό του ή / και οποιοδήποτε άλλο σχετικό νομοθέτημα ή συμφωνητικό που περιγράφει τα δικαιώματα και τις υποχρεώσεις του διαχειριστή και των μελών του συστήματος.
2. Οργανωτικό σχήμα και τρόπος διοίκησης του συστήματος.
3. Κανονισμός λειτουργίας του συστήματος, καθώς και οποιοδήποτε άλλο έγγραφο περιγράφει τις προϋποθέσεις συμμετοχής στο σύστημα, την τιμολογιακή πολιτική, τον τρόπο διακανονισμού των πληρωμών, τη χρονική στιγμή, κατά την οποία ο διακανονισμός καθίσταται αμετάκλητος, τις διαδικασίες διαχείρισης των πιστωτικών κινδύνων και των κινδύνων ρευστότητας.
4. Κατάλογος μελών στο σύστημα (για όσα λειτουργούν).
5. Τεχνική υποδομή του συστήματος με αναφορά στις ακολουθούμενες διαδικασίες διασφάλισης της λειτουργικής αξιοπιστίας και ασφάλειάς του.
6. Κόστος ανάπτυξης του συστήματος (για νέα συστήματα πληρωμών).
7. Ενδεχόμενη αξιολόγηση από εσωτερικούς ή εξωτερικούς φορείς.

Σε μηνιαία βάση, υποβάλλονται στοιχεία για κάθε μέσο πληρωμής (π.χ. εντολή μεταφοράς, επιταγή), συγκεντρωτικά και ανά μέλος του συστήματος. Σε ετήσια βάση, υποβάλλονται στοιχεία που αφορούν στο κόστος βελτιώσεων και συντήρησης του συστήματος καθώς και στο λειτουργικό κόστος. Σε περιπτώσεις έκτακτων περιστατικών, υποβάλλονται, εντός 24 ωρών από τη διαπίστωση του προβλήματος, στοιχεία όπως χρόνος, περιγραφή και αίτια του προβλήματος, ενδεχόμενες ζημιές των μελών του συστήματος και μέτρα που λήφθηκαν ή πρόκειται να ληφθούν για την αποκατάσταση του προβλήματος.

Αντίστοιχα, για τα συστήματα ηλεκτρονικού χρήματος υποβάλλονται τα ακόλουθα στοιχεία πριν από την έναρξη λειτουργίας τους:

1. Στοιχεία ταυτότητας του διαχειριστή (επιχειρηματικό σχέδιο, ίδια κεφάλαια, οργανωτικό σχήμα, προσωπικό, τεχνική υποδομή).
 2. Κανονισμός λειτουργίας του συστήματος.
 3. Τρόποι και προϋποθέσεις συμμετοχής στο σύστημα (για τον εκδότη, έμπορο, κάτοχο ηλεκτρονικού χρήματος).
 4. Δικαιώματα και υποχρεώσεις συμμετεχόντων (του εκδότη, εμπόρου, κατόχου ηλεκτρονικού χρήματος).
 5. Χαρακτηριστικά συστήματος (χρήσεις ηλεκτρονικού χρήματος, γεωγραφική κάλυψη, τρόποι έκδοσής του, όριο χρηματικής αξίας, δυνατότητα εξαργύρωσης, δυνατότητα μεταφοράς χρηματικής αξίας μεταξύ πελατών, διαδικασία πληρωμής εμπόρων).
 6. Κόστος ανάπτυξης του συστήματος.
-
7. Προβλεπόμενα μέτρα ασφάλειας για την πρόληψη περιστατικών πλαστογραφίας, απάτης και νομιμοποίησης χρημάτων από εγκληματικές δραστηριότητες.
 8. Προβλεπόμενη διαδικασία αποζημίωσης συμμετεχόντων σε περίπτωση πτώχευσης του εκδότη.
 9. Ενδεχόμενη αξιολόγηση από εσωτερικούς ή εξωτερικούς φορείς.

Σε εξαμηνιαία βάση, υποβάλλονται στοιχεία που αφορούν στον αριθμό συμβεβλημένων εμπορικών επιχειρήσεων, στον αριθμό τερματικών που αποδέχονται τις κάρτες (για τα συστήματα ηλεκτρονικού χρήματος που βασίζονται σε κάρτα). Ενώ σε ετήσια βάση, υποβάλλονται στοιχεία που αφορούν στο κόστος ανάπτυξης και λειτουργίας του συστήματος και στα έσοδα του συστήματος. Τέλος σε περιπτώσεις έκτατων περιστατικών κοινοποιούνται στην αρμόδια αρχή τα ίδια στοιχεία με τα συστήματα πληρωμών.

Πράξη Διοικητή 2501/31.10.2002. Η εν λόγω πράξη ρυθμίζει την ενημέρωση των συναλλασσόμενων με τα πιστωτικά ιδρύματα για τους όρους που διέπουν τις συναλλαγές τους. Στην πράξη αυτή γίνεται ειδική μνεία για τις διενεργούμενες μέσω του Διαδικτύου τραπεζικές συναλλαγές και ρυθμίζεται η πληροφορία που παρέχεται από τα τραπεζικά ιδρύματα προκειμένου να συμμορφώνεται με τις απαιτήσεις της πράξης. Αυτό, σύμφωνα με την πράξη, επιτυγχάνεται είτε με την άμεση γνωστοποίηση στο Διαδίκτυο των σχετικών στοιχείων είτε με παραπομπή σε εναλλακτικό τρόπο παροχής της σχετικής πληροφόρησης (αρμόδιος υπάλληλος, διεύθυνση, αριθμός τηλ.) σε επίπεδο καταστήματος. Επιπλέον, προβλέπεται να παρέχονται από τα τραπεζικά ιδρύματα στις ιστοσελίδες τους: α) στοιχεία της ταυτότητας του πιστωτικού ιδρύματος και ειδικότερα της άδειας της Τράπεζας της Ελλάδος ή της λειτουργίας του μέσω του κοινοτικού διαβατηρίου σύμφωνα με το Ν. 2076/92 και τη δεύτερη συντονιστική τραπεζική Οδηγία 89/646/ΕΟΚ/15.12.89, β) πληροφορίες σχετικά με την ασφαλή διεξαγωγή των συναλλαγών μέσω του Διαδικτύου (μορφή και βαθμός της παρεχόμενης ασφάλειας).

11. ΔΙΑΠΙΣΤΩΣΕΙΣ

Η διεθνής εμπειρία και πρακτική αλλά και η ελληνική πραγματικότητα όπως σκιαγραφείται από τις μέχρι τώρα προσπάθειες δημιουργίας συστημάτων ηλεκτρονικών πληρωμών καταδεικνύουν ότι η απουσία ολοκληρωμένων προτάσεων δεν οφείλεται σε ελλείψεις τεχνολογικής υποδομής. Αντιθέτως, στα πλαίσια των διαβουλεύσεων έγινε σαφές ότι σε επίπεδο τεχνολογικής υποδομής η Ελλάδα δεν υπολείπεται κατά κανένα τρόπο από τις υπόλοιπες ευρωπαϊκές χώρες ενώ σε ορισμένα ζητήματα είναι σαφώς πιο προηγμένη από αρκετές χώρες της Ευρωπαϊκής Ένωσης. Η περιορισμένη ανάπτυξη και χρήση συστημάτων ηλεκτρονικών πληρωμών στην χώρα οφείλεται κυρίως σε διαρθρωτικά προβλήματα της τραπεζικής αγοράς, στην περιορισμένη διείσδυση του Διαδικτύου στις επιχειρήσεις, ιδιαίτερα μικρού και μεσαίου μεγέθους, και στην γενικότερη καταναλωτική κουλτούρα που επιδρά αρνητικά στην χρήση τέτοιων συστημάτων.

Ειδικότερα, με βάση τη διεθνή εμπειρία καταλήξαμε σε μια σειρά διαπιστώσεων που σκιαγραφούν λεπτομερώς την ελληνική πραγματικότητα και ερμηνεύουν σε μεγάλο βαθμό την περιορισμένη διάδοση των ηλεκτρονικών πληρωμών στην χώρα μας.

- **Απουσία περιεχομένου για πώληση:** ένας από τους βασικότερους λόγους για τους οποίους δεν έχουν ακόμα αναπτυχθεί σε μεγάλο βαθμό τα συστήματα ηλεκτρονικών πληρωμών στην Ελλάδα είναι η απουσία περιεχομένου προς πώληση. Μέχρι στιγμής στην Ελλάδα, επιτυχημένα μοντέλα ηλεκτρονικών καταστημάτων εντοπίζονται σε ελάχιστα καταναλωτικά είδη και κυρίως στα βιβλία, τα λουλούδια και τα CD. Αν και υπάρχουν ηλεκτρονικά καταστήματα που διαθέτουν προς πώληση μια πλειάδα ειδών όπως ηλεκτρονικές συσκευές ή ακόμα και είδη για το σπίτι ο αριθμός τους δεν είναι ιδιαίτερα σημαντικός ενώ δεν έχουν την ίδια επιτυχημένη πορεία με τα είδη που προαναφέραμε. Σε γενικές γραμμές, αυτή τη στιγμή και παρά τις όποιες μεμονωμένες προσπάθειες, οι Έλληνες καταναλωτές δεν διαθέτουν μια ευρεία γκάμα προϊόντων τα οποία μπορούν να αγοράσουν ηλεκτρονικά. Ενώ και για τα είδη που είναι διαθέσιμα μέσω του Διαδικτύου δεν υπάρχουν πολλά ηλεκτρονικά καταστήματα που να τα προσφέρουν ώστε να υπάρχει δυνατότητα σύγκρισης όπως υπάρχει στον φυσικό κόσμο.
- **Απουσία κρίσιμου μεγέθους που θα προσελκύσει επενδύσεις:** έως τώρα στην Ελλάδα, έχουν υλοποιηθεί εφαρμογές ηλεκτρονικών πληρωμών που απευθύνονται κυρίως σε καταναλωτές (B2C). Η πλειοψηφία των υλοποιήσεων αυτών δεν μπορεί να θεωρηθεί ιδιαίτερα επιτυχημένη καθώς δεν έχει καταφέρει να συγκεντρώσει κρίσιμη μάζα πελατών που θα διασφαλίσουν την οικονομική βιωσιμότητα των υλοποιήσεων. Η πιο συνηθισμένη πρακτική μεταξύ των εταιριών που προσφέρουν νεωτερικά συστήματα ηλεκτρονικών πληρωμών είναι να συνεργαστούν με κάποια από τις τράπεζες που προσφέρουν ηλεκτρονικές πλατφόρμες όπως η Τράπεζα Πειραιώς, η Εγνατία Τράπεζα και η Eurobank. Παρά όμως την καινοτομικότητα των λύσεων που προσφέρουν και την ασφάλεια που

εγγυάται η παρουσία μιας μεγάλης τράπεζας που λειτουργεί το σύστημα ηλεκτρονικών πληρωμών, το μεγαλύτερο μέρος των εγχειρημάτων αυτών δεν στέφθηκε με ιδιαίτερη επιτυχία καθώς δεν κατόρθωσαν να δημιουργήσουν αγορές.

Αυτό έχει σαν αποτέλεσμα οι περισσότερες ελληνικές τράπεζες να μην έχουν στα άμεσα σχέδια τους την πραγματοποίηση επενδύσεων για την δημιουργία συστημάτων ηλεκτρονικών πληρωμών δεν είναι ορατά. Επιπλέον, υπάρχει και το προηγούμενο της ηλεκτρονικής τραπεζικής όπου οι τράπεζες προέβησαν σε σημαντικές επενδύσεις οι οποίες δεν έδωσαν τα αναμενόμενα αποτελέσματα καθώς από το 1999 η ζήτηση για υπηρεσίες Internet Banking έχει μειωθεί σημαντικά.

- **Διατήρηση συναλλακτικών ηθών που δεν επιτρέπουν την δημιουργία συστημάτων ηλεκτρονικών αγορών:** Αυτή τη στιγμή στην Ελλάδα λειτουργούν τέσσερις μεγάλες ηλεκτρονικές αγορές (e-marketplaces) στις οποίες συμμετέχουν μεγάλοι όμιλοι εταιρειών. Εντούτοις, σε καμία από τις αγορές αυτές, αν και είναι εφικτό από τεχνολογική άποψη, δεν προσφέρεται η δυνατότητα πραγματοποίησης πληρωμών ηλεκτρονικά. Ο βασικός λόγος για τον οποίο δεν έχει ζητηθεί από τους μετέχοντες στην ηλεκτρονική αγορά η ενεργοποίηση των συστημάτων ηλεκτρονικών πληρωμών είναι κυρίως η πρακτική που ακολουθείται μεταξύ των συναλλασσομένων εταιρειών σε όλη την Ελλάδα. Η ύπαρξη συστημάτων ηλεκτρονικών πληρωμών σημαίνει ότι οι επιχειρήσεις θα πρέπει να εγκαταλείψουν την πρακτική των μεταχρονολογημένων επιταγών που αποτελεί τον συνηθέστερο τρόπο εξόφλησης οφειλών στον εμπορικό κόσμο. Όπως είναι φυσικό μια τέτοια αλλαγή δεν είναι δυνατόν να επέλθει άμεσα και φυσικά δεν είναι δυνατόν να προκληθεί μέσω της μεταφοράς των αγορών σε ηλεκτρονικά συστήματα. Αυτό που απαιτείται κυρίως είναι η εξομάλυνση των υπαρχόντων συναλλακτικών ηθών στον φυσικό κόσμο και στη συνέχεια η μεταφορά των νέων πρακτικών στο διαδίκτυο.
- **Εκπαίδευση καταναλωτών στη χρήση συστημάτων ηλεκτρονικών πληρωμών:** οι Έλληνες καταναλωτές δεν έχουν ακόμα κατανοήσει τις δυνατότητες που τους προσφέρουν οι ηλεκτρονικές πληρωμές. Αυτό οφείλεται κυρίως στο γεγονός ότι οι εταιρείες δεν έχουν επενδύσει πόρους και χρόνο ώστε να πείσουν τους Έλληνες καταναλωτές ότι οι νέες εξελίξεις είναι προς το συμφέρον τους. Επιπλέον, το μεγαλύτερο μέρος των καταναλωτών σε ότι αφορά στις συναλλαγές τους χρησιμοποιεί ως επί το πλείστον μετρητά με αποτέλεσμα να μην είναι σε μεγάλο βαθμό εξοικειωμένοι με εναλλακτικές μεθόδους πληρωμής όπως οι πιστωτικές κάρτες ούτε στο φυσικό κόσμο.

Πέρα όμως από ζητήματα καταναλωτικής κουλτούρας, ιδιαίτερη επίδραση στην υιοθέτηση και διάδοση συστημάτων ηλεκτρονικών πληρωμών διαδραματίζει και η εμπιστοσύνη που αποδίδουν στη χρήση τους οι καταναλωτές. Με βάση πρόσφατη έρευνα που πραγματοποιήθηκε από την Ευρωπαϊκή Ένωση φαίνεται ότι οι Έλληνες είναι επιφυλακτικοί για τις ηλεκτρονικές μορφές πληρωμών. Πιο συγκεκριμένα, οι Έλληνες και οι Πορτογάλοι επιδεικνύουν μεταξύ των Ευρωπαίων πολιτών τη μικρότερη εμπιστοσύνη στη χρήση ηλεκτρονικών πληρωμών. Με βάση ένα «δείκτη εμπιστοσύνης που θέσπισε η Επιτροπή, προκύπτει ότι οι Έλληνες εμπιστεύονται κατά 25,83% λιγότερο από το μέσο κοινοτικό όρο τις πληρωμές μέσω πιστωτικής κάρτας ή του Internet. Ακολουθούν οι Πορτογάλοι με 22,16%. Περισσότερη εμπιστοσύνη στις ηλεκτρονικές πληρωμές έχουν οι Φιλανδοί (κατά 18,81% πάνω από το μέσο κοινοτικό όρο), οι Ολλανδοί (11,75%) και οι Σουηδοί (10,05%).

- **Ανάγκη προσέγγισης καταναλωτών νεαρών ηλικιακών ομάδων:** οι ηλικιακές ομάδες που είναι περισσότερο εξοικειωμένες με τη χρήση των νέων τεχνολογιών είναι οι έφηβοι και οι νέοι μέχρι 25 ετών. Το βασικό πρόβλημα με αυτές τις ομάδες του πληθυσμού είναι ότι παρόλο που διάκεινται περισσότερο θετικά από οποιαδήποτε άλλη ηλικιακή ομάδα στις αγορές μέσω Διαδικτύου δεν διαθέτουν τα απαραίτητα κεφάλαια προκειμένου να χρησιμοποιήσουν ένα από τα υπάρχοντα συστήματα ηλεκτρονικών πληρωμών τα περισσότερα εκ των οποίων σχετίζονται με την κατοχή πιστωτικής κάρτας ή τραπεζικού λογαριασμού. Για το λόγο αυτό, οι ελληνικές τράπεζες, που αποτελούν και τη βασική κινητήρια δύναμη πίσω από την ανάπτυξη συστημάτων ηλεκτρονικών πληρωμών, δημιουργούν σταδιακά συστήματα ηλεκτρονικών πληρωμών τα οποία θα είναι εύκολα προσβάσιμα και στις νεαρές ηλικίες. Στόχος αυτής της στρατηγικής είναι η παροχή της δυνατότητας αγορών σε εκείνες τις πληθυσμιακές ομάδες που είναι περισσότερο διατεθειμένες να πραγματοποιήσουν αγορές μέσω Διαδικτύου και η σταδιακή δημιουργία κρίσιμου μεγέθους που θα μπορέσει να δικαιολογήσει περαιτέρω επενδύσεις σε τέτοια συστήματα.
- **Κατακερματισμός της τραπεζικής αγοράς στην Ελλάδα:** μέχρι τώρα στην Ελλάδα δεν υπάρχει κοινή υποδομή σε επίπεδο συστημάτων μεταξύ των εταιρειών. Κάθε τράπεζα αναπτύσσει τα δικά της συστήματα με αποτέλεσμα η αγορά να είναι πλήρως κατακερματισμένη. Χαρακτηριστικά ο τρόπος με τον οποίον έχουν οργανωθεί οι ηλεκτρονικές πληρωμές στην Πορτογαλία είναι: οι ηλεκτρονικές πληρωμές είναι κεντροποιημένες και ελέγχονται από το διατραπεζικό σύστημα της χώρας. Ο πελάτης βλέπει ένα κοινό interface κατά τις συναλλαγές του, το οποίο παρέχεται από την VISA, ενώ η εκκαθάριση των συναλλαγών γίνεται κεντρικά από το διατραπεζικό σύστημα. Τα πλεονεκτήματα ενός τέτοιου τρόπου οργάνωσης εντοπίζονται στο γεγονός ότι δημιουργούνται οικονομίες κλίμακας, συγκεντρώνεται εύκολα κρίσιμος όγκος πελατών ενώ η ανάπτυξη εμπιστοσύνης είναι σαφώς ευκολότερη. Παρόμοιο τρόπο οργάνωσης έχει και η Ισπανία με την διαφορά ότι υπάρχουν πλέον του ενός διατραπεζικά συστήματα. Επίσης και στην Γαλλία ο τρόπος οργάνωσης είναι αρκετά όμοιος. Ενδιαφέρον, παρουσιάζει και η περίπτωση της Βουλγαρίας όπου υπάρχει ανεπτυγμένο ένα ιδιαίτερα εξελιγμένο διατραπεζικό σύστημα που θα μπορούσε να υποστηρίξει κεντροποιημένες ηλεκτρονικές συναλλαγές. Εντούτοις, η εξόρμηση των Ελληνικών Τραπεζών στα Βαλκάνια και η μεταφορά της ελληνικής νοοτροπίας αυτούσιας σε αυτές τις χώρες οδηγεί στον σταδιακό κατακερματισμό του διατραπεζικού συστήματος της Βουλγαρίας. Αυτό οφείλεται στο γεγονός ότι κάθε τράπεζα ακολουθώντας το ελληνικό μοντέλο αναπτύσσει η ίδια τις τεχνολογικές λύσεις που επιθυμεί.

Εν κατακλείδι, στην παρούσα φάση στην Ελλάδα οι όποιες προσπάθειες γίνονται για ηλεκτρονικές συναλλαγές και πληρωμές εκκινούνται κυρίως από τις τράπεζες που ενισχύουν έτσι την γκάμα προϊόντων ηλεκτρονικής τραπεζικής που είναι σε θέση να προσφέρουν αλλά και από μεγάλους επιχειρηματικούς ομίλους, μέσω της σύστασης ηλεκτρονικών επιχειρηματικών αγορών, που στοχεύουν κυρίως στην εξυπηρέτησή τους. Το σύνολο των ενεργειών αν και σημαντικό δεν είναι συντονισμένο και δεν αποσκοπεί σε κάποιο συνολικό αποτέλεσμα αλλά κυρίως στην κατάκτηση μεριδίου αγοράς από τον κάθε εμπλεκόμενο. Δυστυχώς όμως η πρακτική αυτή προκαλεί σημαντικά προβλήματα στην αγορά καθώς:

- δεν δημιουργούνται υποδομές μέσω των οποίων θα μπορούσαν να δραστηριοποιηθούν και οι μικρομεσαίες επιχειρήσεις και έτσι να δημιουργηθεί ευκολότερα κρίσιμο μέγεθος χρηστών
- διάφοροι σημαντικοί παίκτες αποκλείονται από τις εξελίξεις με αποτέλεσμα τελικά να μην επωφελούνται οι ίδιοι οι καταναλωτές
- ο κατακερματισμός της αγοράς δεν μπορεί να ξεπεραστεί και διαιωνίζεται μια κατάσταση η οποία είναι επιζήμια για την πρόοδο της χώρας

Αποτέλεσμα αυτής της κατάστασης είναι μέχρι τώρα οι Έλληνες να έχουν δυνατότητα χρήσης συστημάτων ηλεκτρονικών πληρωμών σε ένα μικρό εύρος υπηρεσιών όπως στις συναλλαγές τους με το Δημόσιο Τομέα, στον Τουρισμό, στην έκδοση εισιτηρίων και σε ένα περιορισμένο εύρος καταναλωτικών αγαθών.

12. ΠΡΟΤΑΣΕΙΣ ΕΡΓΑΣΙΑΣ

Με βάση τα συμπεράσματα που προέκυψαν οι προτάσεις της εργασίας είναι οι ακόλουθες:

12.1 ΠΡΟΣ ΤΗΝ ΠΟΛΙΤΕΙΑ

Η βασική άποψη που επικράτησε κατά τη διάρκεια των διαβουλεύσεων ήταν ότι η Πολιτεία έχει να διαδραματίσει ιδιαίτερα σημαντικό ρόλο στην ανάπτυξη και υιοθέτηση συστημάτων ηλεκτρονικών πληρωμών. Για το λόγο αυτό ο όγκος των προτάσεων της εργασίας αφορά κυρίως την Πολιτεία και τις ενέργειες στις οποίες οφείλει να προβεί εφόσον επιθυμεί να προωθήσει τις ηλεκτρονικές πληρωμές στην Ελλάδα.

- **Διεκπεραίωση των συναλλαγών με το δημόσιο μέσω ηλεκτρονικών συστημάτων.** Με την εφαρμογή του Taxis η Πολιτεία έδειξε ότι διαθέτει και την τεχνογνωσία αλλά κυρίως την βούληση να μεταφέρει ένα σημαντικό όγκο συναλλαγών με τους πολίτες στο διαδίκτυο όπου και διεκπεραιώνονται ταχύτερα. Η συστηματική μεταφορά των πληρωμών προς το Δημόσιο σε ηλεκτρονικά συστήματα θα δημιουργήσει αφενός ένα κρίσιμο όγκο χρηστών που σταδιακά θα επεκτείνει τη χρήση των συστημάτων αυτών και για αγορές καταναλωτικών αγαθών και αφετέρου θα άρει τους φόβους και την δυσπιστία των χρηστών σχετικά με τα συστήματα αυτά.
- **Ενημέρωση και εκπαίδευση των καταναλωτών.** Ένα σημαντικό πρόβλημα στην υιοθέτηση των συστημάτων ηλεκτρονικών πληρωμών κυρίως από καταναλωτές είναι η μεγάλη δυσπιστία που επιδεικνύουν σε ότι αφορά στην ασφάλεια των συναλλαγών. Είναι απαραίτητη η συστηματική ενημέρωση των καταναλωτών για τα πλεονεκτήματα των ηλεκτρονικών πληρωμών. Ιδιαίτερα σημαντική είναι επίσης και η ενημέρωση σε θέματα ασφαλείας αλλά και η εκπαίδευση των καταναλωτών στην χρήση των συστημάτων αυτών και στην τήρηση των κανόνων ασφαλείας προκειμένου να διασφαλίζεται η ακεραιότητα των συναλλαγών.
- **Ταχύτερη υιοθέτηση νομοθετημάτων.** Αν και τα βασικότερα ευρωπαϊκά νομοθετήματα σε θέματα ηλεκτρονικών πληρωμών έχουν υιοθετηθεί από το ελληνικό κράτος, είναι απαραίτητο να επιταχυνθεί ο ρυθμός υιοθέτησης ώστε να διαμορφωθεί σχετικά σύντομα ένα νομοθετικό πλαίσιο που θα ρυθμίζει στο σύνολο τους τις ηλεκτρονικές πληρωμές. Επίσης είναι ιδιαίτερα σημαντικό η έκδοση εξειδικευμένων κανονισμών από τις αρμόδιες αρχές προκειμένου να δοθεί η απαραίτητη ώθηση τόσο στο ηλεκτρονικό εμπόριο όσο και στις ηλεκτρονικές πληρωμές στην χώρα μας

- **Ομαλοποίηση και εκσυγχρονισμός των συναλλακτικών ηθών:** Ένα σημαντικό εμπόδιο ιδιαίτερα στην υιοθέτηση συστημάτων ηλεκτρονικών πληρωμών στις συναλλαγές μεταξύ επιχειρήσεων είναι η ύπαρξη συναλλακτικών ηθών που δεν είναι δυνατόν να μεταφερθούν αυτούσια στον εικονικό κόσμο. Η Πολιτεία οφείλει να καλέσει τους αρμόδιους φορείς (Επιμελητήρια, Τράπεζες, Συλλόγους) σε διαβούλευση προκειμένου να χαραχθεί μια σταδιακή πορεία προς τον εκσυγχρονισμό των συναλλακτικών ηθών στο εμπόριο κατά τρόπο τέτοιο που να μην υπάρχουν εμπόδια στην περαιτέρω ψηφιοποίησή τους.

12.2 ΠΡΟΣ ΤΙΣ ΤΡΑΠΕΖΕΣ ΚΑΙ ΕΤΑΙΡΕΙΕΣ

Τόσο ο τραπεζικός όσο και ο επιχειρηματικός κόσμος μπορούν να διαδραματίσουν σημαντικό ρόλο στην ανάπτυξη και υιοθέτηση καινοτομικών συστημάτων ηλεκτρονικών πληρωμών. Ήδη η τραπεζική αγορά παρουσιάζει ιδιαίτερη κινητικότητα σε ότι αφορά στην δημιουργία προϊόντων που βασίζονται σε προπληρωμένες κάρτες. Όπως είδαμε ήδη υπάρχουν δύο τέτοια προϊόντα που κυκλοφορούν ευρέως ενώ αρκετές τράπεζες ετοιμάζονται να παρουσιάσουν τα δικά τους αντίστοιχα προϊόντα. Εντούτοις, παρά τις όποιες πρωτοβουλίες υπάρχουν σημαντικές ενέργειες που πρέπει να γίνουν προκειμένου οι καταναλωτές να αποκτήσουν εμπιστοσύνη στα συστήματα ηλεκτρονικών πληρωμών. Έτσι,

- **Ενημέρωση του καταναλωτικού κοινού:** Τόσο οι επιχειρήσεις μέσω του Εμπορικού και Βιομηχανικού Επιμελητηρίου αλλά κυρίως οι τράπεζες πρέπει να ενημερώσουν το κοινό για τα πλεονεκτήματα των συστημάτων ηλεκτρονικών πληρωμών. Επίσης πρέπει να εκπαιδεύσουν κατάλληλα το προσωπικό τους ώστε να είναι σε θέση να καθοδηγήσει επαρκώς τους ενδιαφερόμενους στη χρήση συστημάτων ηλεκτρονικών πληρωμών. Ιδιαίτερη έμφαση πρέπει να δοθεί από τις τράπεζες στα μέτρα ασφάλειας που λαμβάνουν προκειμένου να αρθεί η δυσπιστία του καταναλωτικού κοινού που αποτελεί και το βασικό ψυχολογικό εμπόδιο που αποτρέπει την ευρεία υιοθέτηση των ηλεκτρονικών πληρωμών.
- **Πρώθηση της ΔΙΑΣ Α.Ε.:** η ενίσχυση του ρόλου της ΔΙΑΣ Α.Ε. στην ανάπτυξη και διάδοση συστημάτων ηλεκτρονικών πληρωμών θα βοηθήσει σημαντικά στην ταχεία επίτευξη του κρίσιμου εκείνου μεγέθους που θα προσελκύσει νέες επενδύσεις στα συστήματα ηλεκτρονικών πληρωμών και θα ενεργοποιήσει την αγορά. Επιπλέον, θα δοθεί η ευκαιρία σε μικρότερες τράπεζες να συμμετέχουν ενισχύοντας την διάδοση των συστημάτων ηλεκτρονικών πληρωμών.

Συνολικά, τόσο η Πολιτεία όσο και ο τραπεζικός και επιχειρηματικός τομέας πρέπει με συντονισμένες κινήσεις να ενημερώσουν το κοινό για τα πλεονεκτήματα των ηλεκτρονικών πληρωμών. Παράλληλα, όλοι οι εμπλεκόμενοι φορείς πρέπει να δημιουργήσουν εκείνες τις υποδομές στην ελληνική αγορά που θα επιτρέψουν την επίτευξη κρίσιμου μεγέθους προκειμένου τα συστήματα ηλεκτρονικών πληρωμών να γίνουν μια οικονομικά επικερδής δραστηριότητα για τις τράπεζες και τις επιχειρήσεις. Τέλος, ιδιαίτερο ρόλο στην πρώθηση των συστημάτων ηλεκτρονικών πληρωμών θα διαδραματίσει και το κατάλληλο νομοθετικό πλαίσιο που θα επιτρέψει την ορθή λειτουργία αυτών ενώ θα δημιουργήσει και ένα αίσθημα ασφάλειας τόσο στους καταναλωτές όσο και στις επιχειρήσεις.

13. ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Abrazhevich, D. (2001). Classification and characteristics of electronic payment systems. In K. Bauknecht, S.K. Madria & G. Pernul (Eds.) EC-Web 2001, LNCS 2115 (pp. 81-90). Berlin: Springer – Verlag.
2. Alpha Bank: “Ηλεκτρονική Τραπεζική: Παρόν και Μέλλον”, Οικονομικό Δελτίο, Τεύχος 76, Δεκέμβριος 2000. Böhle, K. & Krueger, M. (August 2001). Payment culture matters: A comparative EU-U.S perspective on Internet payments. Background Paper No 4, Electronic Systems Observatory (ePSO). Διαθέσιμο στο www.e-pso.info.
3. Böhle, K. (April 2002). Integration of electronic payment systems into B2C Internet-commerce: Problems and perspectives. Background Paper No 8, Electronic Systems Observatory (ePSO). Διαθέσιμο στο www.epso.info.
4. Böhle, K. (July 2001). The potential of server-based Internet payment systems: An attempt to assess the future of Internet payments. Background Paper No 3, Electronic Systems Observatory (ePSO). Διαθέσιμο στο www.e-pso.info.
5. Böhle, K., Krueger, M., Herrmann, C., Carat, G. & Maghiros, I. (December, 2000). Electronic payment systems: Strategic and technical issues. Background Paper No 1, Electronic Systems Observatory (ePSO). Διαθέσιμο στο www.e-pso.info.
6. Buhan, D., Cheong, Y. C. & Cheng-Lin, T. (2002). Mobile payments in M-Commerce, Gap Gemini Ernst & Young
7. Centeno, C. (April 2002). Building security and consumer trust in Internet payments: The potential of “soft” measures. Background Paper No 7, Electronic Systems Observatory (ePSO). Διαθέσιμο στο www.e-pso.info.
8. Centeno, C. (January 2002). Securing Internet payments: The potential of public key cryptography, public key infrastructure and digital signatures. Background Paper No 6, Electronic Systems Observatory (ePSO). Διαθέσιμο στο www.e-pso.info.
9. De Lussanet, M., Nordan, M.M., Siepermann, M. & Bedarida, D.E. (May 2001). Mobile payments slow start. Techstrategy Report. Διαθέσιμο στο www.forrester.com.

10. Ensor, B., Torris, T., Fagerström, M. & Martínez, N. (June 2003). New Payment Systems' Survival Guide. Techstrategy Report. Διαθέσιμο στο www.forrester.com.
11. European Central Bank (16/09/2002). E-Payments in Europe: The Eurosystem's Perspective. Issues Paper.
12. European Central Bank (16/10/2002). E-payments in Europe – The eurosystem's perspective. Issue Paper available at www.ecb.int
13. Goldfinger, C. (1999). Secure electronic payments on the Internet. Διαθέσιμο στο www.gefma.com.
14. Jennings, R.U., O'Connell, P. & Bradford, N. (September 2001). Making Content Pay. Techstrategy Report. Διαθέσιμο στο www.forrester.com.

15. Jyrkonen, H. & Paunonen H. (2003). Card, Internet and Mobile Payments. Bank of Finland Discussion Papers No 8-2003. Central Bank of Finland.
16. Krueger, M. (August 2001). The future of M-Payments: Business options and policy issues. Background Paper No 2, Electronic Systems Observatory (ePSO). Διαθέσιμο στο www.e-pso.info.
17. Krueger, M. (January 2002). Innovation and regulation: The case of e-money regulation in the EU. Background Paper No 5, Electronic Systems Observatory (ePSO). Διαθέσιμο στο www.e-pso.info.
18. OECD Information Technology Outlook 2002, 150-152.
19. Peirce, M. (2001). Payment mechanisms designed for the Internet. Διαθέσιμο στο <http://ganges.cse.tcd.ie/meperice>.
20. Presspoint.gr (14/03/2002). Αγορές στο Internet εύκολα, γρήγορα και με ασφάλεια; Η INFORMATION SYSTEMS IMPACT και η Χρυσή Ευκαιρία αλλάζουν τα δεδομένα στο χώρο του Internet. Διαθέσιμο στο www.impact.gr./Articles.
21. Reitsma, R., Pearce, F. & de Montigny, E. (May 2002). Seeing Beyond Credit Card Payment Online. Brief. Διαθέσιμο στο www.forrester.com.
22. Sarawak, K. & Hansen's, B. (2003). E-payments: What are they and what makes them different? EPSO Discussion Starter No1. Διαθέσιμο στο www.e-pso.info.
23. Turban, E.; Lee, J.; King, D. & Chung, H. M. (2003). Electronic Commerce: A managerial perspective. International Edition, Upper Saddle River, New Jersey: Prentice Hall.

24. Yu, H.C., Hsi, K. H., Kuo, P.J. (2002). Electronic payment systems: an analysis and comparison of types. *Technology in Society* 24, pp. 331-347.
25. Γιαννόπουλος, Γ. Ν. (2003). Internet Banking: Νομικά ζητήματα από τη διεξαγωγή τραπεζικών συναλλαγών στο Διαδίκτυο. Δελτίο Ε.Ε.Τ., Γ' Τριμηνία, Αφιέρωμα: Internet Banking.
26. Γκόρτσος, Χ. Βλ. & Τασάκος, Κ. Γ. (2003). Το ευρωπαϊκό κοινοτικό δίκαιο για την ηλεκτρονική τραπεζική. Δελτίο Ε.Ε.Τ., Γ' Τριμηνία, Αφιέρωμα: Internet Banking.
27. Γκόρτσος, Χ. Βλ. (2002). Ο Κανονισμός 2560/2001 σχετικά με τις διασυνοριακές πληρωμές σε Ευρώ. Δελτίο ΕΕΤ, Α' Τριμηνία.
28. Ζούλοβιτς, Μ. (2003). Θεσμικό πλαίσιο και ηλεκτρονικό επιχειρείν στην Ελλάδα – Άλληλεπίδραση και προοπτικές. Ομάδα Εργασίας Δ1. Ebusiness Forum – Δ' Κύκλος Εργασιών. Διαθέσιμο στο www.ebusinessforum.gr.
29. Συρμακέζης, Σ. (2003). Όλα όσα θέλατε να μάθετε για τις ηλεκτρονικές πληρωμές και εισπράξεις (και δεν ξέρατε που να ρωτήσετε). Δελτίο ΕΕΤ, Γ' Τριμηνία.
30. Η Ομάδα εργασίας E-3: Ηλεκτρονικές πληρωμές: Προβλήματα και προοπτικές, ebusiness forum, 2004, <http://www.ebusinessforum.gr/index.php?op=modload&modname=Teams&action=teamsviewnewwall&pageid=35>
31. <http://www.Emporiki.gr>
32. <http://www.go-online.gr>
33. <http://www2.ellinogermaniki.gr/ep/agroweb/htmls/lessons/commerce1gr>
34. Α. Πομπόρτσος - Α. Τσουλάφας « Εισαγωγή Στο Ηλεκτρονικό Εμπόριο», Θεσσαλονίκη , 2002