ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΜΕΣΟΛΟΓΓΙΟΥ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΟΙΚΟΝΟΜΙΑ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Συστήματα ηλεκτρονικών πληρωμών
Έξυπνες κάρτες
(εφαρμογές –ασφάλεια)

Μαριάνθη Π. Μπομπούλα
Α.Μ : 8587

Επιβλέπων καθηγητής : Γρηγόριος Μπεληγιάννης

ΜΕΣΟΛΟΓΓΙ
ΜΑΪΟΣ 2006

ΕΥΧΑΡΙΣΤΙΕΣ

Για αυτή την Πτυχιακή Εργασία θέλω να απευθύνω ένα μεγάλο ευχαριστώ στον εισηγητή καθηγητή μου από το ΤΕΙ Μεσολογγίου κ. Γρηγόριο Μπεληγιάννη, η καθοδήγηση του οποίου υπήρξε όχι απλά σημαντική αλλά καθοριστική για την ολοκλήρωση της συγκεκριμένης εργασίας. Τον ευχαριστώ επίσης θερμά για την εμπιστοσύνη που μου έδειξε, τις επισημάνσεις του και τις συμβουλές του καθ' όλη την διάρκεια του έτους που συνέβαλαν στο μέγιστο στην προσπάθεια εκπόνησης της παρούσας εργασίας.

ΠΕΡΙΕΧΟΜΕΝΑ

ΜΕΡΟΣ Α

ΣΥΣΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ

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 προκείμενου 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 πεντατετία 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 παρακάτω πτυχιακής, 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.

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. Η πτυχιακή αυτή κλείνει με μια σύνοψη αποτελεσμάτων και ένα κατάλογο προτάσεων για την Πολιτεία, τις τράπεζες και τις επιχειρήσεις.

1 ΟΡΙΣΜΟΣ ΚΑΙ ΔΙΑΚΡΙΣΕΙΣ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ [1]

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 ποσών.* Μέσα στις τέσσερις δεκαετίες που μεσολάβησαν από την εμφάνιση τους, έχουν λάβει χώρα σημαντικές τεχνολογικές εξελίξεις που αφενός διεύρυναν 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 των 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 τεχνολογίας.[2] [*Soramäki, K. & Hanssens, B. (2003)*]

Είναι προφανές ότι με βάση τον ορισμό αυτό οι ηλεκτρονικές πληρωμές που θα αποτελέσουν αντικείμενο της παρούσας εργασίας, αφορούν τις πληρωμές εκείνες που γίνονται από τον ίδιο τον πληρωτή είτε είναι καταναλωτής ,είτε επιχείρηση χωρίς την παρέμβαση άλλου φυσικού προσώπου.[3] [*Συρμακέσης, Σ. (2003)*] 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 εμπλεκομένων 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 μια αρχική διάκριση των ηλεκτρονικών πληρωμών σε αυτές που στηρίζονται στη **μεταφορά αξίας** και σε αυτές που στηρίζονται στη **μεταφορά πληροφοριών.**[4] [*Goldfinger, C. (1999).*]

Στην πρώτη κατηγορία, πραγματοποιείται η μεταφορά χρηματικών ποσών μέσω των συστημάτων ηλεκτρονικών πληρωμών. Αντίθετα, στην δεύτερη κατηγορία αυτό που μεταφέρεται μεταξύ των συναλλασσομένων μερών είναι πληροφορίες αφενός για την συναλλαγή και αφετέρου για τους τραπεζικούς λογαριασμούς των εμπλεκομένων. 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.

---

* 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 συμμετέχουν.

Έτσι, οι συναλλαγές μπορούν να πραγματοποιηθούν[5] [*Alpha Bank 2000*] :

❖ **Μέσω τηλεφώνου** Οι πληρωμές μέσω του τηλεφωνικού δικτύου αποτελούν μια 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 με τις πληρωμές 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, διεύρυναν σημαντικά το πεδίο δράσης όλων των επιχειρήσεων με αποτέλεσμα το ηλεκτρονικό, κυρίως, αλλά και το κινητό επιχειρείν να εξελιχθούν σε μια σημαντική παράμετρο της σύγχρονης επιχειρηματικής πρακτικής. Δεδομένου ότι οι επιχειρηματικές δραστηριότητες που κάνουν χρήση των 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 παρούσα εργασία εστιάζει κυρίως στις δύο αυτές κατηγορίες συστημάτων ηλεκτρονικών πληρωμών.

Σκοπός της 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 αυτών των μέσων.

2 ΣΥΣΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ – ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ [6]

Ο διαρκώς αυξανόμενος όγκος συναλλαγών μέσω διαδικτύου την τελευταία δεκαετία έχει καταστήσει απαραίτητη την ανάπτυξη και διάδοση καινοτομικών συστημάτων ηλεκτρονικών πληρωμών. Στόχος των συστημάτων αυτών είναι να μπορούν να υποστηρίξουν τα ιδιαίτερα χαρακτηριστικά των συναλλαγών στο διαδίκτυο όπως ταχύτητα και αμεσότητα χωρίς όμως παράλληλα να θυσιάζουν βασικά πλεονεκτήματα των παραδοσιακών μέσων πληρωμών όπως είναι η ασφάλεια και η ευκολία.

ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΣΥΣΤΗΜΑΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ

Μπορούμε να περιγράψουμε συνοπτικά τα συστήματα ηλεκτρονικών πληρωμών που έχουν αναπτυχθεί με τα εξής χαρακτηριστικά :

Α) ΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑ

- Μηχανισμός πληρωμής: Άμεσος ή Έμμεσος ,πιστωτική κάρτα ,απευθείας κατάθεση ,επιταγή.
- Βαθμός αυτοματοποίησης: πλήρης ή μερική αυτοματοποίηση, συμπεριλαμβανομένης της τιμολόγησης ,της προσκόμισης λογαριασμού ,της ενοποίησης λογαριασμού ,της σύγκρισης τιμολογίων ,της εκκίνησης της διαδικασίας πληρωμής, της μεταφοράς κεφαλαίων.
- Ολοκλήρωση με : επιχειρησιακά συστήματα ,τραπεζικά συστήματα κ.α.
- Μέθοδοι ασφαλείας : με βάση το hardware ή το software ,SSL,SET, smart cards ,πιστοποιητικά.
- Χαρακτηριστικά ελέγχου: (έλεγχος στα πιστωτικά όρια των καρτών αγοράς).
- Υποστήριξη αποφάσεων : (π.χ διαχείριση στοιχείων ενεργητικού με βάση τον άριστο χρόνο και τρόπο πληρωμής.

Όσον αφορά τη λειτουργικότητα ,τα αυτοματοποιημένα συστήματα πληρωμών ποικίλουν συναρτήσει διαφόρων χαρακτηριστικών .Οι διαφορετικές προσεγγίσεις μπορούν να σκιαγραφηθούν από τις απαντήσεις στις παρακάτω ερωτήσεις:

➢ **Ποιοι μηχανισμοί πληρωμών υποστηρίζονται; (έμμεσος ή άμεσος)**

Ο παρακάτω πίνακας παραθέτει τις βασικές διαφορές μεταξύ άμεσων και έμμεσων μεθόδων πληρωμής. Οι άμεσες μέθοδοι συνεπάγονται άμεση αλληλεπίδραση αγοραστή και προμηθευτή. Και τα δύο μέρη ανταλλάσσουν οικονομικά στοιχεία ενεργητικού ,όπως επιταγές και έγγραφα πιστωτικών καρτών.

Η έμμεση πληρωμή σημαίνει ότι και τα δύο μέρη βασίζονται στους αντίστοιχους οικονομικούς οργανισμούς ώστε να διεκπεραιώσουν τη συναλλαγή. Παραδείγματα περιλαμβάνουν την EFT και πληρωμές που διεξάγονται απευθείας από έναν λογαριασμό επιταγών .

Πολλές μέθοδοι πληρωμών μέσω Διαδικτύου χρησιμοποιούν μοντέλα άμεσης πληρωμής συμπεριλαμβανομένων των μηχανισμών ψηφιακών μετρητών ,ηλεκτρονικών επιταγών και πιστωτικών καρτών.

ΑΜΕΣΗ ΠΛΗΡΩΜΗ	ΕΜΜΕΣΗ ΠΛΗΡΩΜΗ
Πληρωμή μετρητών Ο τραπεζικός λογαριασμός του οφειλέτη χρεώνεται πριν την πληρωμή. Η πληρωμή διεξάγεται με τη μεταφορά ψηφιακών νομισμάτων στο λογαριασμό του αποδέκτη . **Πληρωμή με επιταγή** Ο λογαριασμός του οφειλέτη χρεώνεται ταυτόχρονα με την πίστωση του λογαριασμού του αποδέκτη κατά τη διάρκεια ή μετά την πληρωμή. **Πληρωμή με πιστωτική κάρτα** Ο λογαριασμός του αποδέκτη πιστώνεται πριν χρεωθεί ο λογαριασμός του οφειλέτη.	Ο οφειλέτης ή ο αποδέκτης ξεκινά τη διαδικασία πληρωμής χωρίς να υπάρχει ταυτόχρονη αλληλεπίδραση μεταξύ τους. (π.χ Electronic Funds Transfer –EFT)

ΕΙΚΟΝΑ 1 : Διαφορές άμεσης και έμμεσης πληρωμής

- **Η διαδικασία πληρωμής είναι πλήρως ή μερικώς αυτοματοποιημένη;**

Οι μέθοδοι πληρωμής διαφοροποιούνται με βάση το τμήμα της διαδικασίας πληρωμής που καλύπτουν .Τα βήματα περιλαμβάνουν την τιμολόγηση ,την προσκόμιση του λογαριασμού ,την ενοποίηση του λογαριασμού ,τη σύγκριση των τιμολογίων ,την εκκίνηση της διαδικασίας πληρωμής και τη μεταφορά κεφαλαίων. Μερικές αυτοματοποιημένες μέθοδοι πληρωμής υποστηρίζουν την απευθείας πληρωμή και την εξάλειψη μερικών βημάτων όπως η ξεχωριστή τιμολόγηση.

- **Πως ολοκληρώνεται το σύστημα πληρωμών με άλλες εφαρμογές;**

Η διαδικασία πληρωμής συμβαδίζει με μία σειρά από επιχειρηματικές λειτουργίες ,τόσο εσωτερικές όσο και εξωτερικές. Τα ηλεκτρονικά συστήματα πληρωμής αντικατοπτρίζουν αυτό το γεγονός ,παρέχοντας συνδέσμους και επικοινωνία με διαφορετικά επιχειρηματικά συστήματα όπως για παράδειγμα το λογιστήριο ,οι προμήθειες κ.λ.π. Οι εξωτερικές συνδέσεις περιλαμβάνουν επικοινωνία με εμπόρους, τράπεζες κέντρα πωλήσεων ,εταιρείες πιστωτικών καρτών κ.λ.π.

- **Πως επιτυγχάνεται ασφάλεια στις συναλλαγές;**

Μια ποικιλία μηχανισμών έχει αναπτυχθεί προκειμένου να υπάρχουν ασφαλείς συναλλαγές και να διασφαλιστεί η μυστικότητα των δεδομένων που ανταλλάσσονται.

Υπάρχουν συστήματα που βασίζονται σε software χρησιμοποιώντας πρότυπα όπως το SET (Secure electronic transaction) και το SSL (Secure socket layer) ή πιστοποιητικά, ενώ άλλα χρησιμοποιούν smart cards και άλλων ειδών hardware .Συνήθως το δεύτερο είδος τεχνολογιών θεωρείται πιο ασφαλές από το πρώτο.

Μέχρι σήμερα οι παραδοσιακές επιταγές αποτελούν την πιο συχνή μέθοδο πληρωμής μεταξύ των επιχειρήσεων .Τα έμμεσα μοντέλα πληρωμής ,όπως τα

συστήματα βασισμένα σε πιστωτικές κάρτες ,βρίσκονται επί κεφαλής των ηλεκτρονικών μηχανισμών πληρωμής. Τα smart cards τέλος , κερδίζουν ολοένα και περισσότερο έδαφος στην Ευρώπη.

Β) ΑΝΤΙΠΡΟΣΩΠΕΥΤΙΚΑ ΠΑΡΑΔΕΙΓΜΑΤΑ

- Εταιρίες παροχής πιστωτικών καρτών (Visa ,Master Card, American Express) επεκτείνουν τη λειτουργικότητα των προϊόντων τους ώστε να ανταποκρίνονται στις απαιτήσεις των πελατών – επιχειρήσεων ,συμπεριλαμβανομένων αυτομάτων συστημάτων εφοδιασμού.
- Συστήματα στην αγορά επιχείρησης προς καταναλωτή που σχετίζονται με τις διαδικασίες προμηθειών του πεδίου επιχείρησης – προς –επιχείρηση περιλαμβάνουν ηλεκτρονική προσκόμιση και πληρωμή λογαριασμών (electronic bill payment and presentment – EBPP- βλέπε κεφάλαιο 12.1) και μηχανισμούς ηλεκτρονικών πληρωμών , π.χ ηλεκτρονικά μετρητά , συστήματα βασισμένα σε επιταγές , συστήματα βασισμένα σε πιστωτικές κάρτες.
- Προσπάθειες τυποποίησης : Open Training Protocol (OTP) και Open Buying on the Internet. (OBI)

Γ) ΠΕΛΑΤΕΣ ΣΤΟΧΟΣ

- Οι εταιρίες πιστωτικών καρτών στοχεύουν στους ήδη υπάρχοντες πελάτες και παρέχουν επιπρόσθετη αξία ,όπως ο έλεγχος π.χ του πιστωτικού ορίου (κύριος στόχος είναι οι «μικροί» αγοραστές με τα «μικρά» συστήματα ηλεκτρονικών προμηθειών) ή η βελτιωμένη πληροφόρηση στα σημεία πώλησης (point of sale information) με κύριο στόχο τους «μεγάλους» αγοραστές.
- Οι μέθοδοι EBRP είναι περισσότερο ελκυστικές για μεγάλους προμηθευτές με επαναλαμβανόμενους κύκλους πληρωμών ,όπως π.χ οι εταιρίες τηλεπικοινωνιών.
- Οι μέθοδοι τυποποίησης στοχεύουν σε ένα μεγάλο κοινό στην προσπάθεια τους να προσεγγίσουν μεγάλο αριθμό πελατών που θα τις υιοθετήσουν ,των εταιριών παροχής οικονομικών υπηρεσιών και παροχή τεχνολογίας.

Δ) ΕΠΙΧΕΙΡΗΜΑΤΙΚΑ ΜΟΝΤΕΛΑ

- Προσεγγίσεις καθοδηγούμενες από τις προμήθειες : εστίαση στις πηγές εσόδων ,εξειδικευμένες λύσεις, στρατηγικές συμμαχίες με περιορισμένο αριθμό συμμετεχόντων ,γρήγορη είσοδος στην αγορά.
- Προσεγγίσεις καθοδηγούμενες από τους χρήστες και τις βιομηχανικές κοινοπραξίες: λειτουργίες υποστήριξης των επιχειρηματικών διαδικασιών ,έκταση πρωτοβουλιών που εμπλέκουν μεγάλο αριθμό συμμετεχόντων ,αργή πρόοδος εξαιτίας του πολύπλοκου συντονισμού ,χρήση «ανοιχτών» τεχνολογιών.

Ε) ΕΠΙΚΑΛΥΨΗ ΜΕ ΑΛΛΕΣ ΚΑΤΗΓΟΡΙΕΣ

- Παραδοσιακές μέθοδοι αυτόματων πληρωμών ,όπως η EDI και η EFT , μηχανισμοί πληρωμών (ηλεκτρονικό χρήμα ,ηλεκτρονικές επιταγές ,EBRP), συστήματα πληρωμών που αποτελούν μέρος των συστημάτων προμηθειών.

ΣΤ) ΔΥΝΑΜΕΙΣ ΚΑΙ ΑΔΥΝΑΜΙΕΣ

- Πολλά υποσχόμενες προσεγγίσεις σε μεμονωμένους τομείς (συστήματα ηλεκτρονικών πληρωμών ,κάρτες προμηθειών και εργαλεία ασφάλειας) αναβαθμίζουν την αξία των εφαρμογών ηλεκτρονικού εμπορίου και βελτιώνουν τα ανεπαρκή συστήματα πληρωμών.
- Ανώριμη αγορά : Εφαρμογές που συχνά έχουν ανεπαρκείς ενδείξεις βιωσιμότητας στην πράξη ,ανεπαρκής ολοκλήρωση ,έλλειψη ευρέως εφαρμοσμένων προτύπων και επιχειρηματικών μοντέλων.

Ζ) ΑΞΙΟΛΟΓΗΣΗ

- Η ολοκλήρωση των ηλεκτρονικών συστημάτων πληρωμής προϋποθέτει ασφαλείς συνδέσεις μεταξύ των συμμετεχόντων , συμπεριλαμβανομένων των οικονομικών οργανισμών .
- Προσεγγίσεις όπως οι OTP και OBI έχουν υψηλή αξία αν εφαρμοστούν από ικανό αριθμό μελών της αγοράς.

2.1 ΤΑΞΙΝΟΜΗΣΗ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ [7]

Μέχρι σήμερα έχει υπολογιστεί ότι υπάρχουν διεθνώς τουλάχιστον 150 διαφορετικά συστήματα ηλεκτρονικών πληρωμών[8] [*Peirce, M. (2001)*] που υποστηρίζουν συναλλαγές στο διαδίκτυο, ενώ μόνο στην Ευρώπη έχουν καταμετρηθεί ήδη 60 διαφορετικές λύσεις.[9] [*Ensor, B.; Torris, T.; & Martinez, N. (June 2003*].

Ο αριθμός αυτός αυξάνεται δε διαρκώς, ως αποτέλεσμα των νέων τεχνολογικών λύσεων που κατά καιρούς εμφανίζονται αλλά και της προσπάθειας πολλών νέων χρηστών να αποκτήσουν ρόλο μεσολαβητή στο κύκλωμα πληρωμών μέσω διαδικτύου.

Ένα δεύτερο πρόβλημα σε κάθε συστηματική προσπάθεια ταξινόμησης των συστημάτων ηλεκτρονικών πληρωμών μέσω διαδικτύου, είναι η τάση σύνδεσης του συνόλου των ηλεκτρονικών πληρωμών με τις αγοραπωλησίες στο διαδίκτυο. Αν και η ανάπτυξη του διαδικτύου επέτρεψε τη ανάπτυξη συστημάτων όπως το E-cash ή το CyberCash [συστήματα τα οποία θα αναλύσουμε στην ενότητα 4.1] που διεκπεραιώνουν τις ηλεκτρονικές συναλλαγές μέσω του διαδικτύου, το μεγαλύτερο μέρος των συναλλαγών που σχετίζονται με αγορές στο διαδίκτυο δεν διεκπεραιώνεται μέσω αυτού.

Για παράδειγμα, οι πιστωτικές κάρτες που αποτελούν το βασικό μέσο πληρωμής στο διαδίκτυο, χρησιμοποιούν το διαδίκτυο μόνο στα αρχικά στάδια της συναλλαγής όταν ο καταναλωτής αποστέλλει τα στοιχεία του στον έμπορο. Στην συνέχεια η συναλλαγή ολοκληρώνεται μέσω των ιδιόκτητων δικτύων των εταιρειών πιστωτικών καρτών. Επιπλέον υπάρχουν συστήματα ηλεκτρονικών πληρωμών όπως το SWIFT που λειτουργούν πολύ πριν εμφανιστεί το διαδίκτυο. Επομένως, είναι σαφές ότι δεν υπάρχει πλήρης αντιστοιχία μεταξύ των συστημάτων ηλεκτρονικών πληρωμών, εν γένη, και των συστημάτων που χρησιμοποιούν το διαδίκτυο ως βασικό κανάλι διανομής[10] [*Goldfinger, C. (1999)*].

Είναι επομένως εμφανές ότι η όποια προσπάθεια συστηματικής ταξινόμησης των συστημάτων ηλεκτρονικών πληρωμών, πρέπει αφενός να διαθέτει αρκετά γενικές κατηγορίες ώστε να είναι δυνατή η παρουσίαση της πλειοψηφίας των υπαρχουσών λύσεων ενώ να είναι εύκολο να ενταχθούν και μελλοντικές λύσεις. Αφετέρου,

δεδομένης της ταχύτητας των τεχνολογικών εξελίξεων στα συστήματα ηλεκτρονικών πληρωμών και στην μέχρι σήμερα απουσία διεθνώς αποδεκτών λύσεων, η όποια ταξινόμηση δεν μπορεί να στηρίζεται στην τεχνολογία. Για τους λόγους αυτούς, στην παρούσα ανάλυση υιοθετούμε μια ταξινόμηση που αρθρώνεται σε δύο διαφορετικά επίπεδα.

Τα συστήματα ηλεκτρονικών πληρωμών αρχικά ταξινομούνται με βάση:

❖ **1 το είδος της πληροφορίας που ανταλλάσσεται μεταξύ των μερών.**

Έτσι, 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 χρήμα [*Abrazhevich, D. (2001)*].

❖ **2 την καινοτομία 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.

ΣΥΣΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ		ΥΠΟΘΕΜΑ	
		ΓΡΑΜΜΑΤΙΟ	ΛΟΓΑΡΙΑΣΜΟΣ
ΠΑΡΑΔΟΣΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΠΡΟΣΑΡΜΟΣΜΕΝΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ	**Πιστωτικές κάρτες**		**X**
	Μεταφορά ποσών επί πιστώσει		**X**
	Πάγιες εντολές		**X**
	Χρεωστικές κάρτες		**X**
	Ηλεκτρονικές επιταγές		**X**
ΚΑΙΝΟΥΡΙΑ ΣΥΣΤΗΜΑΤΑ ΓΙΑ ΧΡΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ	**Ηλεκτρονικό χρήμα**	**X**	
	Πληρωμές μεταξύ ομότιμων		**X**
	Προπληρωμένες Κάρτες	**X**	

ΕΙΚΟΝΑ 2 : Ταξινόμηση των 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. Αυτό έχει ως αποτέλεσμα να αποκλείονται κοινωνικές ομάδες που για διάφορους λόγους δεν έχουν τραπεζικούς λογαριασμούς, ενώ παράλληλα να μην προφυλάσσεται η ανωνυμία των συναλλαγών.

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.

2.2 ΠΑΡΑΔΟΣΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΠΡΟΣΑΡΜΟΣΜΕΝΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ [12]

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 παραδοσιακά συστήματα είναι:

- **Πιστωτικές κάρτες**
- **Μεταφορά ποσών επί πιστώσει**
- **Πάγιες εντολές**
- **Χρεωστικές κάρτες**
- **Ηλεκτρονικές επιταγές**

Α) ΠΙΣΤΩΤΙΚΕΣ ΚΑΡΤΕΣ [13]

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

Σε ένα μηχανισμό ηλεκτρονικής πληρωμής με χρήση πιστωτικής κάρτας ακολουθείται περίπου το ίδιο σενάριο με αυτό που αναφέρθηκε στην προηγούμενη παράγραφο. Επιπλέον το σενάριο αυτό ,εμπλουτίζεται με μηχανισμούς ασφαλείας (έλεγχος ταυτότητας πελάτη και εμπόρου.) Το γεγονός αυτό έχει οδηγήσει στην ύπαρξη μιας γκάμας συστημάτων ηλεκτρονικών πληρωμών με πιστωτικές κάρτες.

Δύο από αυτά τα χαρακτηριστικά που προσδιορίζουν και διαφοροποιούν τα συστήματα αυτά ,είναι το επίπεδο της ασφάλειας των συναλλαγών και το λογισμικό που απαιτείται από όλα τα εμπλεκόμενα μέρη (αγοραστής ,τράπεζα).

Κατά τη διάρκεια μιας on-line συναλλαγής ,τα στοιχεία της πιστωτικής κάρτας ενός αγοραστή μπορούν να μεταφερθούν με δύο τρόπους .Ο πρώτος τρόπος θεωρείται μη ασφαλής και υποστηρίζει την αποστολή των στοιχείων της

ηλεκτρονικής πληρωμής από τον πελάτη στον έμπορο (ή την τράπεζα) σε μη κρυπτογραφημένη μορφή .Η μέθοδος αυτή κρίνεται ως μη ασφαλής ,γιατί κατά τη μεταβίβαση των στοιχείων μπορεί να παρεισφρήσει κάποιος «εισβολέας» και να τροποποιήσει τα στοιχεία της συναλλαγής ή ακόμα και να τα υποκλέψει. Ο δεύτερος τρόπος θεωρείται πιο ασφαλής και προβλέπει την κρυπτογράφηση όλων των πληροφοριών που σχετίζονται με την πληρωμή πριν την αποστολή τους στον έμπορο(ή την τράπεζα) μέσω Διαδικτύου.

Για την αποφυγή της παρεμβολής κάποιου τρίτου κατά την διεξαγωγή των συναλλαγών μεταξύ του πελάτη και του εμπόρου, μια καλή επιλογή αποτελεί εκείνος ο συνδυασμός web browser και web server που θα υποστηρίξει το πρωτόκολλο Secure Sockets Layer (SSL) .Η χρησιμοποίηση διακομιστή web και web browser που υποστηρίζουν το πρωτόκολλο SSL ,εξασφαλίζει την προστασία των δεδομένων από κάποιο τρίτο .Δεν εγγυάται όμως ότι τα δεδομένα αυτά δεν θα χρησιμοποιηθούν σκόπιμα από τον έμπορο. Το SSL αποτελεί τα αρχικά για το ασφαλές επίπεδο υποδοχής. Ο όρος περιγράφει μια μέθοδο κρυπτογράφησης της ροής δεδομένων μεταξύ ενός προγράμματος πλοήγησης και του διακομιστή Web. Ο κόσμος το χρησιμοποιεί καθημερινά για να ανακτήσει οικονομικές πληροφορίες και για να παραγγείλει μέσω διαδικτύου .

Οι εταιρίες Visa και MasterCard ανέπτυξαν ένα νέο πιο ασφαλές πρωτόκολλο το Secure Electronic Transaction (SET) ,το οποίο θεωρητικά είναι τέλειο. Για την αποφυγή εξαπάτησης του πελάτη από τον έμπορο (για παράδειγμα ,χρήση των στοιχείων της πιστωτικής κάρτας από τον έμπορο για την διεξαγωγή μη εξουσιοδοτημένων αγορών), θα μπορούσε να χρησιμοποιηθεί ένας ανεξάρτητος φορέας διασφάλισης των συναλλαγών γνωστός ως «Έμπιστη Τρίτη Οντότητα (ΕΤΟ)» Μια ΕΤΟ μεσολαβεί ανεξάρτητα στην όλη διαδικασία αποκρυπτογραφώντας τα στοιχεία της πιστωτικής κάρτας και επικυρώνοντας τη συναλλαγή.

Σε αρκετές περιπτώσεις ,εταιρίες που παράγουν συστήματα ηλεκτρονικών πληρωμών ,όπως η Cyber cash , η Verifone ή η First Virtual, χρησιμοποιούν μηχανισμούς με τους οποίους παρέχουν υπηρεσίες ΕΤΟ. Και η Cyber cash ,και η Verifone χρησιμοποιούν τον μηχανισμό των wallet.Ο μηχανισμός αυτός μεταφέρει τον κρυπτογραφημένο αριθμό της πιστωτικής κάρτας από τον έμπορο στον δικό τους επεξεργαστή για τον έλεγχο αυθεντικότητας και την έγκριση της συναλλαγής. Η εταιρεία First Virtual εκδίδει κάποιο Virtual PIN στον πελάτη που το χρησιμοποιεί αντί του αριθμού της πιστωτικής κάρτας .Αφού λάβει τις πληροφορίες των πωλήσεων από τον έμπορο ,η First Virtual μετατρέπει το Virtual PIN στον αριθμό λογαριασμού της πιστωτικής κάρτας ,προκειμένου να διεκπεραιωθεί η πληρωμή.

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

Σε αυτό το σημείο θα πρέπει να σημειωθεί ότι παρά την πρόοδο που έχει σημειωθεί στα συστήματα ηλεκτρονικών πληρωμών με χρήση πιστωτικών καρτών εξακολουθούν να υπάρχουν ακόμη ορισμένα προβλήματα .Το σημαντικότερο πρόβλημα που εξακολουθεί να υφίσταται ακόμη είναι η τυποποίηση. Θα πρέπει να υιοθετηθεί μια κοινά αποδεκτή μέθοδος (ή πρότυπο) διεκπεραίωσης των ηλεκτρονικών συναλλαγών στο διαδίκτυο ,που θα επιτρέπει την επικοινωνία μεταξύ των διαφορετικών τύπων λογισμικού των συναλλασσομένων μερών. Η εξασφάλιση ή

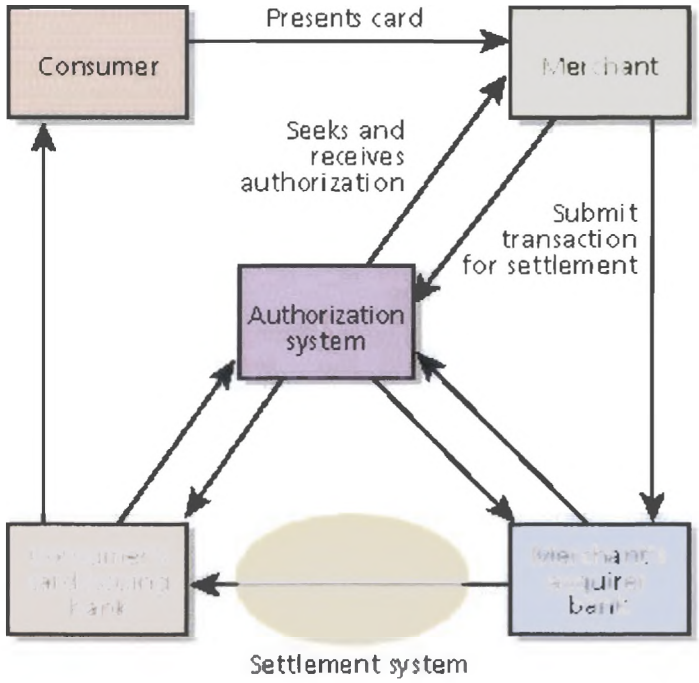
όχι αυτής της δια-λειτουργικότητας θα καθορίσει και την μελλοντική πορεία των ηλεκτρονικών συστημάτων πληρωμών μέσω πιστωτικής κάρτας.

Πιστωτικές Κάρτες και Ιστός [14] [*www2.ellinogermaniki.gr*]

Στις συναλλαγές ηλεκτρονικού εμπορίου, τα συστήματα πιστωτικών καρτών λειτουργούν περίπου με τον ίδιο τρόπο όπως τώρα. Ο πελάτης είναι σε θέση να χρησιμοποιήσει την πιστωτική κάρτα του, εάν το επιθυμεί, για να αγοράσει αντικείμενα απευθείας από τον πωλητή. Η βασική διαφορά είναι ότι οι μεγάλες εταιρείες πιστωτικών καρτών έχουν δημιουργήσει ένα πρότυπο αποκρυπτογράφησης που ονομάζεται "Ασφαλείς Ηλεκτρονικές Συναλλαγές" (SET).

Με το SET ο έμπορος δεν λαμβάνει τον αριθμό της πιστωτικής κάρτας σας. Παίρνει μόνο μια ένδειξη που μεταβαίνει στην τράπεζα, η οποία τη χρησιμοποιεί για να πάρει τον πραγματικό αριθμό, εγκρίνει ή απορρίπτει τη συναλλαγή και στη συνέχεια στέλνει στον έμπορο έναν αριθμό έγκρισης. Ο έμπορος διαβεβαιώνεται ότι η κάρτα είναι εντάξει και ολοκληρώνει τη συναλλαγή.

Όλα αυτά γίνονται με αποκρυπτογράφηση, για να επιβεβαιωθεί η πραγματική ταυτότητα των μερών. Επίσης, με το SET ο καταναλωτής παίρνει μια πιστοποιημένη ψηφιακή απόδειξη για τη συναλλαγή.



ΕΙΚΟΝΑ 3: Διαδικασία πληρωμής με πιστωτική κάρτα

Τα πλεονεκτήματα αυτής της μεθόδου πληρωμής είναι:

- Τα χρήματά σας είναι ασφαλισμένα στην τράπεζα:

Εάν τύχει και χάσετε την κάρτα, ο λογαριασμός είναι ακόμη συνδεδεμένος με το όνομά σας. Έτσι, σε αντίθεση με τα συστήματα μετρητών υπάρχει τρόπος η τράπεζα να επιβεβαιώνει το υπόλοιπο του λογαριασμού και τα χρήματα να μην χάνονται.

- Δεν υπάρχει λόγος να ανοίξετε νέο λογαριασμό:

Σε αντίθεση με τα συστήματα μετρητών που απαιτούν από το χρήστη να ανοίξει νέο λογαριασμό στην τράπεζα που διαχειρίζεται αυτού του είδους τη συναλλαγή, με το σύστημα της πιστωτικής κάρτας ο πελάτης μπορεί να διατηρήσει το λογαριασμό και την κάρτα που ήδη έχει. Αυτός είναι ένας πολύ σημαντικός παράγοντας στα πρώτα στάδια του ηλεκτρονικού εμπορίου.

Το κύριο μειονέκτημα αυτής της μεθόδου πληρωμής είναι:

- Μη διασφάλιση των προσωπικών δεδομένων:

Σε αντίθεση με τις συναλλαγές σε μετρητά που είναι ανώνυμες, οι συναλλαγές με πιστωτικές κάρτες συνδέουν το όνομά σας με το λογαριασμό. Έτσι ο πελάτης δε μπορεί να διατηρήσει την ανωνυμία μιας συναλλαγής σε μετρητά. Διατρέχει επίσης τον κίνδυνο να περάσει το όνομά του σε μια σειρά από ταχυδρομικές λίστες.

Β) ΜΕΤΑΦΟΡΑ ΠΟΣΩΝ ΕΠΙ ΠΙΣΤΩΣΕΙ [15]

Σε αυτό το σύστημα πληρωμών ο καταναλωτής δίνει εντολή στην τράπεζά του να μεταφέρει χρηματικά ποσά ανάλογα της πληρωμής που θέλει να πραγματοποιήσει στον λογαριασμό του εμπόρου.[16] [*European Central Bank, E-payments in Europe*] 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.

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 Τράπεζας [*European Central Bank ,E-payments in Europe*][17], τα εν λόγω συστήματα ηλεκτρονικών πληρωμών λειτουργούν προς το παρόν σε αυστηρά εθνικά πλαίσια με αποτέλεσμα να μην είναι βολικά για διεθνείς συναλλαγές.

Γ) ΠΑΓΙΕΣ ΕΝΤΟΛΕΣ

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 ομοιάζει 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.

Δ) ΧΡΕΩΣΤΙΚΕΣ ΚΑΡΤΕΣ

Το εν λόγω σύστημα ηλεκτρονικών πληρωμών αποτελεί μια παραλλαγή των πάγιων εντολών όπου οι απαιτούμενες για τη συναλλαγή πληροφορίες περιέχονται σε ειδική κάρτα 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 παγίων 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 γεγονός 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 πλεονεκτήματα τους έναντι των πιστωτικών καρτών[18] [*Turban, E.; Electronic commerce*]. 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 τους επιβαρύνουν με προμήθεια. Επιπλέον, στην επιχειρηματικές συναλλαγές μέσω διαδικτύου (B2B) οι χρεωστικές κάρτες μπορεί να αποδειχθούν φθηνότερη λύση ακριβώς για αυτόν το λόγο.

Ε) ΗΛΕΚΤΡΟΝΙΚΕΣ ΕΠΙΤΑΓΕΣ

Οι ηλεκτρονικές επιταγές είναι η φυσιολογική συνέχεια των παραδοσιακών επιταγών. Μια επιταγή είναι μια γραπτή εντολή από τον εκδότη προς τον αποδέκτη που είναι συνήθως μια 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 μορφή.[19] [*European Central Bank ,E-payments in Europe*] Επιπλέον, καθώς ο εκδότης πρέπει να υπογράψει την επιταγή προκειμένου να είναι έγκυρη ,στις ηλεκτρονικές επιταγές χρησιμοποιείται η ψηφιακή υπογραφή προκειμένου να ολοκληρωθεί η διαδικασία.[20] [*Παπαναγιώτου, Ν.: Internet –Επιχείρηση*].

Στην χρήση ηλεκτρονικών υπογραφών εντοπίζονται και τα περισσότερα προβλήματα που συναντά στην διάδοση του το συγκεκριμένο σύστημα πληρωμής. Η χρήση κρυπτογραφικών μεθόδων αλλά και η τεχνολογία που απαιτείται για να υποστηρίξει τις ηλεκτρονικές υπογραφές έχουν μέχρι τώρα δημιουργήσει αρκετά εμπόδια στην χρήση των ηλεκτρονικών επιταγών. Τα θέματα αυτά θα αναλυθούν σε επόμενη ενότητα.

Επιταγές και Ιστός[21] [www2.ellinogermaniki.gr]

Τα συστήματα που μεταφέρουν ηλεκτρονικές επιταγές στον ιστό δεν έχουν αναπτυχθεί τόσο καλά, όπως άλλες μορφές μεταφοράς κεφαλαίων. Οι επιταγές θα μπορούσαν να είναι κάτι τόσο απλό όσο η αποστολή μέσω ηλεκτρονικού ταχυδρομείου ενός μηνύματος σε έναν έμπορο, που θα έδινε έγκριση για ανάληψη χρημάτων από το λογαριασμό σας με ψηφιακές υπογραφές και συνημμένα πιστοποιητικά.

Σε πολλές περιπτώσεις ένα σύστημα επιταγών είναι μια ενδιάμεση λύση μεταξύ των πιστωτικών καρτών και των μετρητών. Οι CheckFree, NetCheque, και NetChex είναι οι μεγαλύτεροι παράγοντες στην αγορά επιταγών.

Τα πλεονεκτήματα αυτού του συστήματος είναι

- Επεξεργασία: Οι ηλεκτρονικές επιταγές μπορούν να επεξεργαστούν όπως οι κανονικές επιταγές μέσω αυτοματοποιημένων μηχανισμών. Μοιάζουν διαφορετικές αλλά δεν παύουν να είναι επιταγές.

- Το ότι δίνει ρέστα: Δεν μπορεί να χρησιμοποιηθεί οποιοδήποτε ποσό ηλεκτρονικών μετρητών. Εάν έχετε μια σειρά 25 δολαρίων από το NetCash και θέλετε να αγοράσετε κάτι για 5 δολάρια, θα πρέπει να στείλετε εντολή πίσω στη Netbank και να ζητήσετε να σας κάνει ψιλά. Μπορούν να σας στείλουν ένα χρηματικό ανάλογο των $5 και ένα των $20. Το σύστημα επιταγών θα επέτρεπε στο χρήστη να καθορίσει το ακριβές ποσό της συναλλαγής.

- Τα χρήματά σας είναι ασφαλή στην τράπεζα: Οι πελάτες δεν χρειάζεται να ανησυχούν μήπως χάσουν κάτι, όπως θα ανησυχούσαν με ένα σύστημα μετρητών.

Το κύριο μειονέκτημα αυτού του είδους του συστήματος είναι:

- Μη διασφάλιση των προσωπικών δεδομένων: Μολονότι αυτό το σύστημα δεν έχει τις ίδιες συνέπειες όπως οι πιστωτικές κάρτες, οι επιταγές αποκαλύπτουν επίσης στοιχεία σχετικά με τον πελάτη.

2.2.1 ΣΥΧΝΕΣ ΕΡΩΤΗΣΕΙΣ ΚΑΙ ΣΧΕΤΙΚΕΣ ΠΛΗΡΟΦΟΡΙΕΣ ΓΙΑ ΤΙΣ ΠΙΣΤΩΤΙΚΕΣ ΚΑΡΤΕΣ [22]

❖ **Πιστωτική κάρτα**

Μορφή του λεγόμενου «πλαστικού χρήματος», σύγχρονου και διαδεδομένου τρόπου συναλλαγών, που παρέχει τη δυνατότητα αγοράς αγαθών ή υπηρεσιών χωρίς άμεση εκταμίευση μετρητών για πληρωμή της αξίας τους. Οι πιστωτικές κάρτες εκδίδονται κυρίως από πιστωτικά ιδρύματα (π.χ. τράπεζες) και μεταξύ άλλων η χρήση τους παρέχει και τα ακόλουθα πλεονεκτήματα :

α) ευκολία στις συναλλαγές σε όσες περιπτώσεις ο κάτοχος της κάρτας δεν έχει ή δεν θέλει να έχει μαζί του μετρητά.
β) ασφάλεια στις συναλλαγές, γιατί ο κάτοχος της κάρτας δεν χρειάζεται να έχει μαζί του μετρητά διακινδυνεύοντας έτσι να τα χάσει.

γ) εξασφάλιση περιόδου χάριτος αρκετών ημερών (π.χ. 25 ή 40 ημέρες) χωρίς τόκο από την ημερομηνία έκδοσης του λογαριασμού έως την ημερομηνία πληρωμής.
δ) (λειτουργώντας ως κάρτες ηλεκτρονικών συναλλαγών) παροχή της δυνατότητας στους κατόχους τους να διενεργούν τραπεζικές πράξεις μέσω των Αυτόματων Ταμειολογιστικών Μηχανών (ATM), όπως αναλήψεις, καταθέσεις, μεταφορά ποσών από λογαριασμό σε λογαριασμό κ.ά.

Τα τελευταία χρόνια η ευρεία διάδοση των πιστωτικών καρτών και ο τραπεζικός ανταγωνισμός έχουν οδηγήσει σε μια συνεχή επέκταση των παρεχόμενων υπηρεσιών, διευρύνοντας έτσι την κλασική λειτουργία της κάρτας ως μέσο πληρωμών.

Έτσι, προστέθηκαν ασφαλιστικές καλύψεις (ταξιδιωτική ασφάλιση, ιατρική και νομική βοήθεια), καταρτίστηκαν ειδικά προγράμματα συνεργασίας τραπεζών με επιχειρήσεις, ώστε να παρέχονται εκπτώσεις για την αγορά αγαθών ή υπηρεσιών, και τελευταία άρχισαν να εφαρμόζονται προγράμματα σύνδεσης πιστωτικών καρτών με οργανισμούς, σωματεία, λέσχες, φιλανθρωπικές ή οικολογικές οργανώσεις κ.ά.

Η προσπάθεια αυτή εμπλουτισμού των πιστωτικών καρτών με στοιχεία που δεν σχετίζονται άμεσα με την κύρια λειτουργία τους αποσκοπεί κυρίως στη διεύρυνση της πελατείας του τραπεζικού φορέα, στην εξυπηρέτηση και ικανοποίηση του πελάτη και στην προβολή του συνεργαζόμενου φορέα (π.χ. ποδοσφαιρικό ή φιλανθρωπικό σωματείο).

❖ **Τι είναι οι πιστωτικές κάρτες**

Είναι σύγχρονος και διαδεδομένος τρόπος συναλλαγών, μορφή του λεγόμενου «πλαστικού χρήματος». Εκδίδονται από πιστωτικούς οργανισμούς με ευρύτατη αποδοχή και αναγνώριση και εξασφαλίζουν στους κατόχους τους τη δυνατότητα αγοράς αγαθών ή υπηρεσιών χωρίς να απαιτείται άμεση καταβολή της αξίας τους.

Η πιστωτική κάρτα έχει τη μορφή μιας πλαστικής κάρτας η οποία φέρει στη μια πλευρά της με ανάγλυφα στοιχεία τον αριθμό μητρώου και το ονοματεπώνυμο του κατόχου της, τη λήξη ισχύος της, καθώς και το πιστωτικό κατάστημα το οποίο τη χορήγησε. Στην άλλη πλευρά συνήθως υπάρχει η μαγνητική ταινία, θέση για την υπογραφή του κατόχου της και ο λογότυπος του οργανισμού που την εξέδωσε.

❖ **Τι δυνατότητες παρέχει στον κάτοχό της η πιστωτική κάρτα;**

Η πιστωτική κάρτα παρέχει στον κάτοχό της τη δυνατότητα να πραγματοποιεί αγορές αγαθών και υπηρεσιών χωρίς άμεση καταβολή της αξίας τους, εντός βέβαια των πιστωτικών ορίων της, από επιχειρήσεις που είναι συμβεβλημένες με τον τραπεζικό οργανισμό που την εξέδωσε. Η δυνατότητα αυτή για ορισμένες κάρτες επεκτείνεται και στο εξωτερικό, ενώ άλλες μπορούν να χρησιμοποιηθούν για απεριόριστο όριο αγορών, με μόνη προϋπόθεση τη μηνιαία εξόφληση του λογαριασμού.

Επίσης, με την πιστωτική κάρτα παρέχεται η δυνατότητα ανάληψης μετρητών 24 ώρες το 24ωρο, ανάλογα βέβαια με το ύψος του πιστωτικού ορίου. Το μηνιαίο όριο ανάληψης μετρητών κλιμακώνεται ανάλογα με το πιστωτικό όριο που έχει ο κάτοχος της κάρτας, π.χ. για πιστωτικό όριο 500.000 δρχ. το μηνιαίο όριο ανάληψης μετρητών ανέρχεται σε 200.000 δρχ.

Ακόμη, η πιστωτική κάρτα ως κάρτα ηλεκτρονικών συναλλαγών παρέχει στον κάτοχό της τη δυνατότητα να διενεργεί τραπεζικές πράξεις μέσω των Αυτόματων

Ταμειολογιστικών Μηχανών (ΑΤΜ) επί συνδεδεμένων τραπεζικών λογαριασμών, προσωπικών του ή κοινών, τους οποίους δήλωσε στην αίτησή του ότι επιθυμεί να κινεί. Δηλαδή μέσω των μηχανών αυτόματης εξυπηρέτησης, τις οποίες διαθέτουν σε ευρύ συνήθως δίκτυο οι τράπεζες, ο κάτοχος της πιστωτικής κάρτας μπορεί να πραγματοποιεί αναλήψεις, καταθέσεις, μεταφορά ποσών από λογαριασμό σε λογαριασμό, εξόφληση της δόσης ή ακόμη να έχει ενημέρωση για το υπόλοιπο των λογαριασμών του ή της πιστωτικής του κάρτας.

Πέρα από αυτές τις κύριες δυνατότητες, παρέχεται και σειρά υπηρεσιών όπως είναι τα πλήρη πακέτα ασφαλιστικών καλύψεων (π.χ. ταξιδιωτική ασφάλιση, ασφάλιση τροχαίου δυστυχήματος κ.ά.), η δυνατότητα λήψης επιπρόσθετου συναλλάγματος για ταξίδια στο εξωτερικό, ευνοϊκά τουριστικά πακέτα με εκπτώσεις στις τιμές των ξενοδοχείων, σε ενοικιάσεις αυτοκινήτων κ.ά.

Επιπλέον, σε πολλές περιπτώσεις οι κάτοχοι πιστωτικών καρτών ενημερώνονται, μέσω ειδικών περιοδικών που τους αποστέλλονται, για προσφορές καταστημάτων κατά τις οποίες η εξόφληση των άμεσων αγορών που πραγματοποιούνται γίνεται ύστερα από την παρέλευση αρκετών μηνών (προγράμματα μεταχρονολογημένων χρεώσεων) ή με πολλές άτοκες μηνιαίες δόσεις (προγράμματα άτοκων δόσεων).

❖ **Ποια είναι η διαδικασία έκδοσης πιστωτικής κάρτας;**

Ο ενδιαφερόμενος υποβάλλει σχετική αίτηση και μετά την έγκριση ανοίγει ένα λογαριασμό στην εκδούσα τράπεζα για την αυτόματη εξόφληση του λογαριασμού της κάρτας. Η αίτηση συνοδεύεται από φωτοτυπία της αστυνομικής ταυτότητας, καθώς και φωτοτυπία του τελευταίου εκκαθαριστικού της εφορίας ή της τρέχουσας μισθοδοσίας.

Προκειμένου να εγκρίνει την αίτηση η τράπεζα συνεκτιμά ένα σύνολο από κριτήρια, όπως το ύψος και η πηγή του εισοδήματος, η σταθερή επαγγελματική κατάσταση, η τυχόν προηγούμενη πελατειακή σχέση με την τράπεζα. Η κάθε πιστωτική κάρτα έχει ορισμένα όρια πίστωσης, υπάρχουν όμως και ορισμένες, οι οποίες χαρακτηρίζονται συνήθως ως «χρυσές», που έχουν ιδιαίτερα υψηλά πιστωτικά όρια και συνοδεύονται από ακόμη μεγαλύτερες παροχές, πιο ισχυρά ασφαλιστικά πακέτα και πολλά ιδιαίτερα προνόμια.

❖ **Τι πλεονεκτήματα παρουσιάζει η πιστωτική κάρτα σε σχέση με τις συναλλαγές με μετρητά;**

Τα κύρια πλεονεκτήματα είναι:

Α) ευκολία στις συναλλαγές σε περίπτωση που ο κάτοχός της δεν έχει ή δεν θέλει να έχει μαζί του μετρητά.

Β) ασφάλεια στις συναλλαγές, γιατί ο κάτοχος της κάρτας δεν απαιτείται να έχει μαζί του μετρητά διακινδυνεύοντας να τα χάσει.

Γ) εξασφάλιση περιόδου χάριτος αρκετών ημερών (π.χ. 25 ή 40 ημέρες) χωρίς τόκο, από την ημερομηνία έκδοσης του λογαριασμού έως την ημερομηνία πληρωμής.

❖ **Ποιες κατηγορίες πιστωτικών καρτών υπάρχουν;**

Σε γενικές γραμμές οι πιστωτικές κάρτες μπορούν να χωριστούν σε τρεις κατηγορίες: στην πρώτη ανήκουν όσες μπορούν να χρησιμοποιηθούν μόνο στο

εσωτερικό της χώρας, στη δεύτερη οι κάρτες που η ισχύ τους επεκτείνεται και στο εξωτερικό, ενώ στην τρίτη κατηγορία ανήκουν οι κάρτες που χαρακτηρίζονται ως «χρυσές», «prestige» κ.ά. και οι οποίες παρέχουν υψηλά πιστωτικά όρια και συνοδεύονται συνήθως από προνόμια και παροχές όπως ισχυρά ασφαλιστικά πακέτα, νομική προστασία κ.ά.

❖ **Τι είναι ο προσωπικός αριθμός αναγνώρισης (P.I.N);**

Ο προσωπικός αριθμός αναγνώρισης ή **P.I.N.** (Personal Identification Number) είναι ο απόρρητος κωδικός αριθμός που ισοδυναμεί με την υπογραφή του κατόχου της κάρτας και ο οποίος είναι απαραίτητος σε συνδυασμό με την κάρτα για την πραγματοποίηση συναλλαγών. Ο αριθμός αυτός είναι και πρέπει να παραμένει αυστηρά προσωπικός. Ο κάτοχος της κάρτας πρέπει να τον φυλάσσει με πολύ μεγάλη προσοχή (το καλύτερο είναι να τον απομνημονεύσει), να μην τον αναγράφει στην κάρτα του ή σε οποιοδήποτε άλλο έγγραφο και να καταστρέφει τα έντυπα στα οποία αυτός αναγράφεται.

❖ **Τι κοστίζει μια πιστωτική κάρτα;**

Οι εκδότες πιστωτικών καρτών χρεώνουν τους κατόχους των καρτών για τις υπηρεσίες που τους παρέχουν με μια ετησία συνδρομή, που κυμαίνεται ανάλογα με το είδος της κάρτας και τον εκδότη. Εκτός από τη δαπάνη αυτή υπάρχει και το ετήσιο συμβατικό επιτόκιο, με το οποίο δανειοδοτείται ο κάτοχος της κάρτας, καθώς και ο Ειδικός Φόρος Τραπεζικών Εργασιών (ΕΦΤΕ), που επιβαρύνει τους τόκους. Εκτός από τις επιβαρύνσεις αυτές, ο κάτοχος βαρύνεται συνήθως και με τα έξοδα αποστολής του μηνιαίου λογαριασμού ή και με άλλα διαχειριστικά έξοδα.

Για να είναι σε θέση ο καταναλωτής να συγκρίνει τη συνολική Ετήσια Πραγματική Επιβάρυνση (ΕΠΕ) από κάρτα σε κάρτα, το Υπουργείο Εμπορίου έχει υποχρεώσει τους οργανισμούς έκδοσης πιστωτικών καρτών να αναγράφουν στη σύμβαση που υπογράφει ο πελάτης, εκτός από τους όρους χορήγησης της κάρτας, και την ετήσια πραγματική επιβάρυνση βάσει ενός υποθετικού παραδείγματος.

❖ **Σε περίπτωση απώλειας ή κλοπής της πιστωτικής κάρτας τι πρέπει να κάνει ο κάτοχός της;**

Πρέπει να ειδοποιήσει αμέσως την εκδούσα τράπεζα ή οργανισμό και να υποβάλει σχετική έγγραφη δήλωση, η οποία συνοδεύεται συνήθως από υπεύθυνη δήλωση του Ν. 1599. Η γνωστοποίηση της απώλειας της κάρτας πρέπει να γίνει το ταχύτερο δυνατό, διότι μέχρι την ημέρα που θα λάβει γνώση η τράπεζα ο κάτοχος εξακολουθεί να είναι υπεύθυνος για τις αποδείξεις πώλησης και τις άλλες τυχόν συναλλαγές που διενεργούνται μέσω της κάρτας του.

❖ **Τι ισχύει σχετικά με τις πιστωτικές κάρτες όσον αφορά τη φορολογία εισοδήματος;**

Τα τελευταία χρόνια έχει καθιερωθεί ως πρόσθετο φορολογικό τεκμήριο η χρήση πιστωτικών καρτών. Το τεκμήριο αυτό συγκρίνεται με τα τεκμήρια δαπανών διαβίωσης και απόκτησης περιουσιακών στοιχείων και αν τα υπερβαίνει, φορολογείται αυτό. Οι οργανισμοί έκδοσης πιστωτικών καρτών χορηγούν στους πελάτες τους στο τέλος κάθε χρόνου βεβαίωση στην οποία αναγράφεται το συνολικό

ποσό που κατέβαλε ο πελάτης τους. Οι βεβαιώσεις αυτές αθροίζονται και αν το σύνολό τους είναι μεγαλύτερο τόσο από το δηλούμενο στην Εφορία εισόδημα όσο και από το ποσό που προκύπτει από τα τεκμήρια δαπανών διαβίωσης και απόκτησης περιουσιακών στοιχείων, τότε αυτό θεωρείται ότι είναι το φορολογητέο εισόδημα του οικονομικού έτους, εκτός και αν αποδειχτεί ανάλωση κεφαλαίου που αποκτήθηκε τα προηγούμενα έτη.

Οι φορολογούμενοι, λοιπόν, θα πρέπει να προσέχουν ώστε οι αγορές που πραγματοποιούν με πιστωτικές κάρτες να μην είναι μεγαλύτερες από το εισόδημα που δηλώνεται στις φορολογικές αρχές

❖ **Τι πρέπει να προσέχει ο καταναλωτής σχετικά με τις πιστωτικές κάρτες;**

Το πρώτο πράγμα που πρέπει να έχει υπόψη του ο καταναλωτής είναι ότι η πιστωτική κάρτα απαιτεί συνετή χρήση. Ένα από τα μεγάλα σύγχρονα κοινωνικά προβλήματα σε χώρες όπου υπάρχει μεγάλη διάδοση των πιστωτικών καρτών, όπως είναι οι ΗΠΑ, ο Καναδάς, η Γαλλία κ.ά., είναι η λεγόμενη «υπερχρέωση των νοικοκυριών». Υπάρχουν δηλαδή νοικοκυριά που χρωστούν μία ή και παραπάνω φορές το ετήσιο εισόδημά τους λόγω υπέρμετρων αγορών μέσω πιστωτικών καρτών.

Σύμφωνα με υποδείξεις της Διεύθυνσης Καταναλωτών του Υπουργείου Εμπορίου, οι καταναλωτές που κάνουν χρήση πιστωτικών καρτών πρέπει να φροντίζουν:

- Να διαβάζουν προσεκτικά τους όρους χρήσης των πιστωτικών καρτών.
- Να έχουν τις κάρτες μαζί τους, αλλά όχι μέσα σε πορτοφόλι ή τσάντα που κινδυνεύουν να κλαπούν ή να ξεχαστούν.
- Να έχουν γραμμένους σε ασφαλές μέρος τους αριθμούς και τους προσωπικούς κωδικούς (PIN) των καρτών.
- Να αποφεύγουν να υπογράφουν κενά (άγραφα) δελτία χρέωσης.
- Πριν από την υπογραφή ενός δελτίου χρέωσης, να διαγράφουν τα τετραγωνίδια που βρίσκονται πάνω από το συνολικό ποσό.
- Να κρατούνται προσεκτικά οι μηνιαίοι λογαριασμοί των πιστωτικών καρτών.
- Να ειδοποιούν αμέσως την τράπεζα που εξέδωσε την κάρτα σε περίπτωση απώλειας ή κλοπής της, καθώς και σε περίπτωση αλλαγής της διεύθυνσης κατοικίας τους.
- Να μη δανείζουν την πιστωτική τους κάρτα.
- Να μη δίνουν τον αριθμό της κάρτας από το τηλέφωνο.

❖ **Τι καινοτομίες δρομολογούνται στον τομέα των πιστωτικών καρτών;**

Το λεγόμενο «πλαστικό χρήμα» εκτιμάται από τους ειδικούς ότι θα αποτελέσει τομέα ιδιαίτερης ανάπτυξης κατά τη μετάβαση στον 21ο αιώνα και αναμένεται ότι ένα σημαντικό μερίδιο του τραπεζικού μάρκετινγκ θα αφορά τη διάδοση και τη γενίκευση της χρήσης των πιστωτικών καρτών και γενικότερα μορφών του πλαστικού χρήματος. Ήδη όλο και περισσότερα μεγάλα καταστήματα στο εξωτερικό εκδίδουν πιστωτικές κάρτες, προσπαθώντας με τον τρόπο αυτόν να διατηρήσουν έναν σημαντικό αριθμό πελατών.

Πρόσφατη καινοτομία είναι η έκδοση πιστωτικών καρτών που είναι συνδεδεμένες με αθλητικά σωματεία (π.χ. Παναθηναϊκός FC-Visa), πολιτιστικούς οργανισμούς (π.χ. Artion Visa σε συνεργασία με τον Οργανισμό Μεγάρου Μουσικής

Αθηνών) κ.ά. Στόχος της είναι η διεύρυνση της πελατείας του τραπεζικού φορέα, η προβολή του συνεργαζόμενου φορέα και η εξυπηρέτηση του πελάτη (π.χ. εκπτώσεις, εξασφάλιση εισιτηρίων, θέσεων σε εκδηλώσεις του φορέα κ.ά.).

Σημαντική αύξηση παρουσιάζουν τα τελευταία χρόνια και οι χρεωστικές τραπεζικές κάρτες, με τις οποίες μπορεί κανείς να πραγματοποιεί αγορές με απευθείας χρέωση του λογαριασμού του χωρίς κανένα όριο ή επιβάρυνση με τόκους. Τέλος, τα επόμενα χρόνια εκτιμάται ότι θα κυκλοφορήσουν και στην Ελλάδα οι λεγόμενες «έξυπνες κάρτες» (smart cards), που θα αποτελέσουν έναν σημαντικό νέο τρόπο συναλλαγών λειτουργώντας ως ηλεκτρονικά πορτοφόλια.

❖ **Τι θα συμβεί αν η ηλεκτρονική πληρωμή με πιστωτική κάρτα δεν γίνει αποδεκτή από τον κάτοχο της κάρτας;**

Οι συμβατικοί κανόνες και οι διαδικασίες που υιοθετούν οι τράπεζες καθιερώνουν για όσους αποδέχονται πληρωμές μέσω πιστωτικής κάρτας την υποχρέωση να λαμβάνουν μία υπογεγραμμένη εντολή πληρωμής και να εξακριβώνουν ότι η υπογραφή ανταποκρίνεται σ΄αυτήν της κάρτας. Είναι όμως φανερό ότι αυτό δεν μπορεί να εφαρμοστεί στην περίπτωση πληρωμής με πιστωτική κάρτα μέσω διαδικτύου.

Επομένως η θέση του πωλητή στη συγκεκριμένη περίπτωση δεν είναι ισχυρή από νομικής πλευράς, αφού ο αγοραστής μπορεί να αρνηθεί την εντολή αγοράς. Χρησιμοποιώντας την διαδικασία Ασφαλούς Ηλεκτρονικής Συναλλαγής (SET-Secure Electronic Transaction),[σύστημα το οποίο θα αναλύσουμε στην ενότητα 9.4] δίνεται η δυνατότητα βελτίωσης της αποδεικτικής ικανότητας.

Αν ο πελάτης αμφισβητεί τη συναλλαγή, η Τράπεζα πρέπει να αποδείξει ότι η εν λόγω συναλλαγή έχει πραγματοποιηθεί και ότι ο πελάτης έχει δώσει την έγκρισή του.

ΠΡΑΓΜΑΤΙΚΟ ΠΕΡΙΣΤΑΤΙΚΟ ΜΕ ΠΙΣΤΩΤΙΚΗ ΚΑΡΤΑ [23]

Η εταιρία Χ είχε την πρώτη της εμπειρία παράνομης χρήσης με πιστωτική κάρτα πριν από ένα μήνα .Κάποιος έκλεψε τον αριθμό πιστωτικής κάρτας και χρησιμοποίησε τον κλεμμένο αριθμό για να αγοράσει ένα προϊόν αξίας 500 ευρώ από την εταιρία. Ο απατεώνας γνώριζε την πραγματική διεύθυνση του κατόχου την οποία και κοινοποίησε στην εταιρεία ,αλλά ζήτησε η παράδοση να γίνει σε διαφορετική διεύθυνση.

Δεδομένου ότι είναι σύνηθες φαινόμενο κάποιοι από τους πελάτες να ζητούν η διεύθυνση παράδοσης να είναι διαφορετική από τη διεύθυνση τιμολόγησης, το αίτημα του συγκεκριμένου πελάτη δεν κίνησε υποψίες.Η πολιτική της εταιρίας είναι να στέλνονται τα τιμολόγια στη διεύθυνση του κατόχου πράγμα που έγινε. Μερικές μέρες αργότερα ,η εταιρία δέχθηκε ένα τηλέφωνημα από τον νόμιμο κάτοχο της κλεμμένης κάρτας που την πληροφόρησε ότι ουδεποτε είχε κάνει αγορά από την εταιρία αυτή.

Ο συγκεκριμένος απατεώνας είχε κάνει χρήση μια δωρεάν υπηρεσίας e-mail και συγκεκριμένα της Juno για να ανοίξει e-mail στο όνομα του κατόχου της κάρτας ,γεγονός που έδωσε στη συναλλαγή έναν νομιμοφανή χαρακτήρα. Η εταιρία ενημέρωσε το τμήμα ασφάλειας της Juno για την διαπραχθείσα απάτη και η Juno έκλεισε το λογαριασμό του απατεώνα .Αν και είχε πάρει κανονικά την απαιτούμενη εξουσιοδότηση και έγκριση από την εταιρία που διαχειρίζεται τον εταιρικό της λογαριασμό πιστωτικών καρτών, πλήρωσε εξ ολοκλήρου τη ζημιά .Επικοινώνησε και

με την τράπεζα και με όλους τους εμπλεκόμενους ακόμα και με την αστυνομία. Κανείς τους δεν φάνηκε διατεθειμένος να τη βοηθήσει ,ίσως επειδή ήταν πολύ απασχολημένοι ή επειδή αισθανόντουσαν ότι το εν λόγω ποσόν των 500 ευρώ δεν ήταν τόσο σημαντικό για να κινήσουν περαιτέρω διαδικασίες.

Μετά από αυτό το πάθημα τους ,αποφάσισαν να κάνουν κάποιες έρευνες και να γνωρίσουν με πιο τρόπο οι άλλες εταιρίες αντιμετωπίζουν αυτό το πρόβλημα. Ανακάλυψαν ότι η απάτη με τις πιστωτικές κάρτες γιγαντώνεται ολοένα και περισσότερο για τις εταιρίες που κάνουν πωλήσεις μέσω διαδικτύου .Τους έκανε εντύπωση πως ένα τόσο μεγάλο πρόβλημα δεν έχει ακόμα λάβει σχετική δημοσιότητα.

Ανακάλυψαν ακόμα ότι αυτού του είδους οι απατεώνες είναι σε θέση πλέον να δημιουργούν φανταστικούς αριθμούς πιστωτικών καρτών (δηλαδή που δεν έχουν εκδοθεί ακόμα) βασιζόμενοι στους εφαρμοζόμενους αλγόριθμους για την παραγωγή των αυθεντικών αριθμών .Όπως είναι αναμενόμενο ,αυτοί οι αριθμοί περνούν άνετα το στάδιο της επαλήθευσης και λαμβάνουν τους απαραίτητους κωδικούς έγκρισης.

Ακόμα υπάρχουν ομάδες δημοσίευσης πληροφοριών (Newsgroups) οι οποίες δημοσιεύουν κλεμμένα στοιχεία πιστωτικών καρτών και έτσι εάν κλαπεί ο αριθμός της πιστωτικής σας κάρτας μπορεί να δημοσιευθεί ανά τον κόσμο μέσα σε λίγα λεπτά.

❖ **<u>Τα προβλήματα (και οι δυνατότητες άμυνας) του καταναλωτή</u>**

Όλοι μας έχουμε ακούσει να μιλούν για τους κινδύνους της χρήσης πιστωτικών καρτών στο διαδίκτυο. Η λαϊκή φαντασία, τροφοδοτούμενη από αμαθείς δημοσιογράφους, υποστηρίζει ότι κάθε φορά που πραγματοποιούμε μια συναλλαγή online και δίνουμε τα στοιχεία της κάρτας μας σε έναν έμπορο, αυτά αποθηκεύονται στη βάση δεδομένων του και βρίσκονται πλέον στο έλεος κάθε αδίστακτου εισβολέα ο οποίος μπορεί να τα αποκτήσει, παραβιάζοντας τα συστήματα ασφαλείας, και στη συνέχεια να σπαταλήσει τεράστια ποσά τα οποία φυσικά θα χρεώσει στη δική μας κάρτα.

Ευτυχώς για τους καταναλωτές όμως τα πράγματα δεν είναι ακριβώς έτσι. Είναι αλήθεια βέβαια ότι, αν κάνω χρήση της πιστωτικής μου κάρτας στο δίκτυο, τα στοιχεία της μπορεί να πέσουν στα χέρια αδίστακτων ανθρώπων. Ωστόσο, για να προστατευτούν οι καταναλωτές από αυτό τον κίνδυνο, υπάρχει ειδική νομοθεσία, τόσο στην Ευρωπαϊκή Ένωση όσο και στις ΗΠΑ, η οποία ορίζει ότι ο κάτοχος της κάρτας μπορεί να αρνηθεί τη χρέωση οποιασδήποτε συναλλαγής έχει πραγματοποιηθεί χωρίς την παρουσίαση του φυσικού σώματος της κάρτας.

Με τον τρόπο αυτό η ευθύνη για την κάρτα μου περιορίζεται μόνο στο υλικό μέρος της και μόνο αν χάσω την ίδια την κάρτα αναλαμβάνω την ευθύνη της ακύρωσής της και βαρύνομαι με όποιες δαπάνες έγιναν πριν δηλώσω την απώλειά της. Επειδή όμως η διακίνηση των στοιχείων της κάρτας δεν ελέγχεται και μπορεί να τα αποκτήσει χωρίς δική μου γνώση ή υπαιτιότητα ο οποιοσδήποτε (π.χ. ο πωλητής του πολυκαταστήματος από το οποίο αγόρασα ένα ζευγάρι κάλτσες), δεν με υποχρεώνει κανείς να αναγνωρίσω όποια συναλλαγή πραγματοποιείται χωρίς την ίδια την κάρτα.

Έτσι, σε περίπτωση online συναλλαγών με κλεμμένα στοιχεία καρτών, ο κάτοχος όταν δει τη χρέωση στο αντίγραφο του λογαριασμού του μπορεί να αρνηθεί την καταβολή του αντιτίμου και η τράπεζα όχι μόνο δεν θα καταβάλει το ποσό αυτό στον πωλητή, αλλά θα χρεώσει και το κατάστημα με τα έξοδα ακύρωσης της συναλλαγής. Φυσικά, για τον κάτοχο της κάρτας η διαδικασία άρνησης χρέωσης και

στη συνέχεια αλλαγής της κάρτας του (προκειμένου να μην επαναληφθεί το ίδιο φαινόμενο) δεν είναι απλή υπόθεση. Ωστόσο, ο «μπελάς» είναι μικρός συγκρινόμενος με τις δυσκολίες που έχει να αντιμετωπίσει όποιο ηλεκτρονικό κατάστημα εμπιστεύθηκε αυτή την κάρτα και παρέδωσε προϊόντα ή προσέφερε υπηρεσίες στον ψεύτικο κάτοχό της.

❖ **Τα προβλήματα (και οι δυνατότητες άμυνας) του ηλεκτρονικού εμπόρου**

Κάθε ηλεκτρονικός επιχειρηματίας έχει φυσικά το δικαίωμα να διώξει δικαστικά τον παραλήπτη των προϊόντων τα οποία ζητήθηκαν με κλεμμένα στοιχεία πιστωτικής κάρτας, ζητώντας αποζημίωση. Δυστυχώς όμως, το δύσκολο έργο της ανακάλυψης του ενόχου και της τιμωρίας του σπάνια έχει αίσιο τέλος. Στην πλειοψηφία των περιπτώσεων μάλιστα αυτό είναι πρακτικώς αδύνατον (π.χ. τα έξοδα δίωξης κατοίκου άλλης χώρας είναι τόσο υψηλά που δεν αξίζει τον κόπο να ασχοληθεί κανείς με το θέμα). Γι' αυτό και τα ηλεκτρονικά καταστήματα προτιμούν την πρόληψη από τη θεραπεία. Η πρώτη γραμμή άμυνάς τους είναι ο έλεγχος της αξιοπιστίας των πιστωτικών καρτών.

Πολλές φορές μια κάρτα μπορεί να είναι έγκυρη (να μην έχει ακυρωθεί ακόμη από την Τράπεζα), αλλά τα στοιχεία της να έχουν κλαπεί και να έχει ήδη χρησιμοποιηθεί στο παρελθόν για αγορές τις οποίες αρνήθηκε να αναγνωρίσει ο κάτοχός της.

Γι' αυτό και τα ηλεκτρονικά καταστήματα μισθώνουν τις υπηρεσίες ειδικών εταιρειών, όπως η Cybersource *[http://www.cybersource.com]*, οι οποίες παρακολουθούν τα περιστατικά αυτά και ενημερώνουν το ηλεκτρονικό κατάστημα αν παρουσιάστηκαν προβλήματα με τη συγκεκριμένη κάρτα στο παρελθόν. Οι υπηρεσίες αυτές βέβαια δεν παρέχονται δωρεάν. Ωστόσο, η χρήση τους είναι υποχρεωτική για όλα τα καταστήματα, καθώς περιορίζουν τις απώλειες από το 20% στο 1% των παραγγελιών. (Δηλαδή χωρίς έλεγχο των καρτών το 20% των παραγγελιών αποδεικνύονται πλαστές και η αξία των προϊόντων δεν εισπράττεται ποτέ!).

Η δεύτερη, και τελευταία, γραμμή άμυνας για κάθε ηλεκτρονικό κατάστημα είναι ο έλεγχος των παραγγελιών για την ανακάλυψη «ύποπτων» αιτημάτων. Ενδεικτικά αναφέρουμε μερικά παραδείγματα παραγγελιών οι οποίες πρέπει να ελέγχονται εξονυχιστικά:

- Μεγάλες παραγγελίες από πελάτες οι οποίοι δεν έχουν αγοράσει τίποτε στο παρελθόν.
- Παραγγελία η οποία πρέπει να παραδοθεί σε ανεξέλεγκτη διεύθυνση όπως κάποια γραμματοθυρίδα ή το post restant.
- Πολλαπλές παραγγελίες για καταναλωτικά είδη τα οποία συνήθως αγοράζονται μια φορά (π.χ. παραγγελία 30 ρακετών του τένις από ένα άτομο).
- Παραγγελία ειδών με περίεργη ακολουθία (π.χ. παραγγελία 2 πουκαμίσων μεγέθους small, συν 2 ίδιου χρώματος και σχεδίασης μεγέθους medium, συν άλλα δύο large, συν άλλα δύο extra large).
- Υποβολή πολλών παραγγελιών με την ίδια κάρτα σε μικρό χρονικό διάστημα.
- Υποβολή πολλών παραγγελιών με την ίδια κάρτα και παράδοση σε διαφορετικές διευθύνσεις.
- Υποβολή πολλών παραγγελιών με διαφορετικές κάρτες και παράδοση στην ίδια διεύθυνση.

❖ **Μελλοντικές λύσεις στο πρόβλημα**

Αναγνωρίζοντας τα προβλήματα που δημιουργεί αυτός ο τρόπος συναλλαγών, οι εταιρείες Visa και Mastercard έχουν προτείνει ένα άλλο σύστημα γνωστό με το όνομα SET (Secure Electronic Transaction). Στο κείμενο αυτό δεν θα επεκταθούμε εδώ πολύ στα τεχνικά χαρακτηριστικά του συστήματος, αλλά αν το επιθυμείτε μπορείτε να πάρετε περισσότερες πληροφορίες γι' αυτό από τη διεύθυνση http://www.setco.org. Συνοπτικά πάντως αναφέρουμε ότι το SET αποτελείται από τρία μέρη:

- Μια «ηλεκτρονική πιστωτική κάρτα» η οποία είναι εγκατεστημένη στον Η/Υ του χρήστη (το ειδικό λογισμικό παρέχεται δωρεάν από το SET).
- Ειδικό λογισμικό εγκατεστημένο στο ηλεκτρονικό κατάστημα.
- Ειδικό λογισμικό εγκατεστημένο σε μια πιστοποιημένη από το SET τράπεζα.

Χάρη στην εφαρμογή αυτή τα στοιχεία της πιστωτικής κάρτας του αγοραστή διαβιβάζονται από το ηλεκτρονικό κατάστημα στην τράπεζα χωρίς ο πωλητής να μαθαίνει ποτέ το παραμικρό για την κάρτα του αγοραστή (δεν γνωρίζει ούτε το όνομα, ούτε τον αριθμό, ούτε την ημερομηνία λήξεως).

Με τον τρόπο αυτό τα στοιχεία της κάρτας του αγοραστή έχουν μηδαμινές πιθανότητες τα υποκλαπούν από τρίτους. Γι' αυτό και οι Visa και Mastercard προσδοκούν ότι το σύστημα αυτό θα υιοθετηθεί τελικά ως η βάση για κάθε συναλλαγή ηλεκτρονικού εμπορίου. Είναι μάλιστα τόσο σίγουρες για την ασφάλειά του που εγγυώνται κάθε συναλλαγή η οποία γίνεται μέσω SET. Δηλαδή με το SET ο online έμπορος δεν διατρέχει κανέναν από τους κινδύνους των παραγγελιών με πλαστά στοιχεία τους οποίους αναφέραμε παραπάνω.

Δυστυχώς, μέχρι σήμερα το SET δεν έχει διαδοθεί ευρέως. Απ' ό,τι φαίνεται, η ευκολία της χρήσης πιστωτικής κάρτας με τον παραδοσιακό τρόπο (SSL) είναι τόσο μεγάλη (ή το λογισμικό του SET είναι τόσο περίπλοκο) που οι καταναλωτές δεν το έχουν ακόμη υιοθετήσει παρά τα προφανή πλεονεκτήματα ασφαλείας τα οποία διαθέτει.

Έτσι, συνήθως η χρήση του SET περιορίζεται μόνο στις επικοινωνίες μεταξύ εμπόρου και τράπεζας, ενώ η επικοινωνία του εμπόρου με τον πελάτη εξακολουθεί να διεξάγεται με SSL. Με τον τρόπο αυτό όμως ο κίνδυνος των πλαστών παραγγελιών παραμένει το ίδιο μεγάλος. Όλες οι ελπίδες λοιπόν έχουν εναποτεθεί στο SET 2 το οποίο θα χρησιμοποιεί έξυπνες κάρτες (ηλεκτρονικά πορτοφόλια) και θα είναι πολύ πιο απλό στη χρήση από τις σημερινές εφαρμογές. Δυστυχώς όμως, ο χρόνος υλοποίησης του SET 2 παραμένει ακόμη άγνωστός (πιθανότητα ένα ή δύο χρόνια).

❖ **Η κατάσταση στην Ελλάδα**

Αν και δεν έχω συγκεκριμένα στοιχεία υπ' όψιν μου, εκτιμώ ότι το πρόβλημα των συναλλαγών με κλεμμένα στοιχεία πιστωτικών καρτών δεν πρέπει να είναι ιδιαίτερα σημαντικό στη χώρα μας για τους ακόλουθους λόγους:

1. **Τα περισσότερα ηλεκτρονικά καταστήματα παρέχουν τις υπηρεσίες τους μόνο στην ελληνική γλώσσα**
   Έτσι, μπορούν να αποτελέσουν στόχο μόνο για όσους μιλούν ελληνικά δηλαδή για τους κατοίκους Ελλάδας και Κύπρου (όπου όμως βρίσκονται και

τα ίδια τα καταστήματα, άρα η δίωξη είναι πιο εύκολη), καθώς και για τους Έλληνες του εξωτερικού (το υψηλό μορφωτικό και οικονομικό επίπεδο των οποίων όμως δεν ευνοεί την ευρεία εμφάνιση ανάλογων μορφών δράσης).

2. **Πολλά καταστήματα πωλούν εξειδικευμένα προϊόντα ελληνικού χαρακτήρα**
(π.χ. www.grproducts.gr) τα οποία σίγουρα δεν ενδιαφέρουν ιδιαίτερα τους διεθνείς «δικτυοαπατεώνες».

3. **Συνήθως, τα ελληνικά ηλεκτρονικά καταστήματα έχουν μικρό μέγεθος και δεν διαχειρίζονται αυτόματα δικτυακές συναλλαγές**
Έτσι, μια ύποπτη παραγγελία θα περάσει αναγκαστικά από τα χέρια ενός ανθρώπου ο οποίος είναι αρκετά πιο πιθανό να αναγνωρίσει ότι υπάρχει κάτι περίεργο σε αυτήν.

❖ **Συμπεράσματα**

Οι απάτες λόγω της χρήσης κλεμμένων στοιχείων πιστωτικών καρτών γίνονται όλο και πιο δημοφιλείς με αποτέλεσμα πολλοί έμποροι να συζητούν πλέον σοβαρά τη διακοπή των πωλήσεων στις περιοχές του πλανήτη όπου παρουσιάζεται μεγάλος αριθμός παρόμοιων περιστατικών (Ρωσία και Βαλκανικές χώρες εκτός Ελλάδος). Μια τέτοια ενέργεια όμως μπορεί να δυσκολέψει, αλλά σίγουρα δεν θα αποθαρρύνει τους οργανωμένους εγκληματίες οι οποίοι θα υποχρεωθούν να μεταφέρουν τις δραστηριότητές τους σε άλλες λιγότερο ύποπτες χώρες. Το business to consumer ηλεκτρονικό εμπόριο λοιπόν θα συνεχίσει να αντιμετωπίζει τα ίδια προβλήματα ως τη στιγμή που η τεχνολογία (SET 2 ή κάτι άλλο) να δώσει την οριστική λύση. Μέχρι τότε όμως το μόνο που μας μένει να κάνουμε είναι υπομονή.

2.3 ΚΑΙΝΟΤΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ [24]

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 άϋλων αγαθών μικρής αξίας κ.α. Μερικά από τα συστήματα αυτά, όπως οι έξυπνες κάρτες, αρχίζουν να χρησιμοποιούνται και στο φυσικό κόσμο ενώ άλλα είναι σχεδιασμένα αποκλειστικά για χρήση στο διαδίκτυο.

Ειδικότερα τα καινοτομικά συστήματα είναι:

❖ **Ηλεκτρονικό χρήμα**
❖ **Πληρωμές μεταξύ ομότιμων**
❖ **Προπληρωμένες κάρτες**

Α) ΣΧΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΧΡΗΜΑΤΟΣ

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

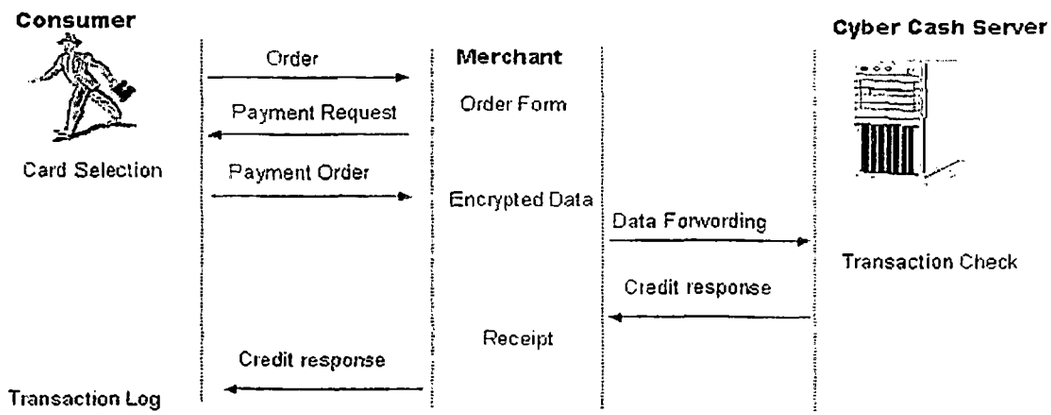
χρήση τραπεζικών λογαριασμών. Το ηλεκτρονικό χρήμα θα λειτουργεί ως προπληρωμένο υπόθεμα, ενώ τα δίκτυα θα είναι είτε ανοικτά δηλαδή θα επιτρέπουν την άμεση μεταφορά χρημάτων μεταξύ υποθεμάτων είτε κλειστά όπου η χρέωση του υποθέματος θα γίνεται από συγκεκριμένο τραπεζικό λογαριασμό αποκλειστικά».[25] [*Turban, E.; Electronic commerce*] 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 λογισμικό*.[26] [*European Central Bank E-payments in Europe*] 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 έχουν μείνει σε πιλοτικό στάδιο.

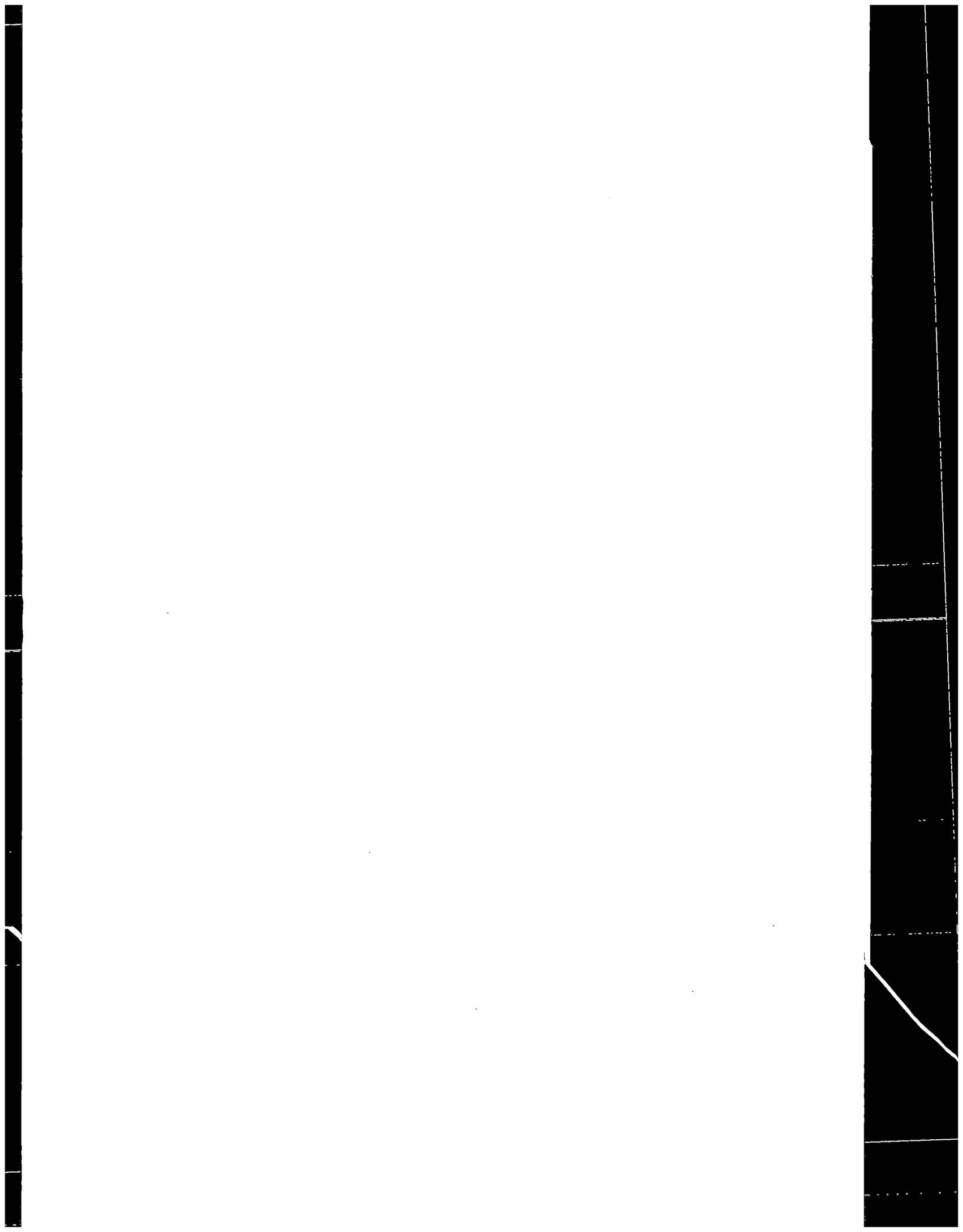
Το βασικό πλεονέκτημα πάντως των σχημάτων ηλεκτρονικών πληρωμών και στις δύο περιπτώσεις είναι ότι διατηρείται η ανωνυμία των συναλλαγών που είναι ιδιαίτερα σημαντική για τους πελάτες. Επιπλέον, ειδικά οι κάρτες αποθηκευμένης αξίας είναι ιδιαίτερα ευέλικτο μέσο πληρωμής που επιτρέπει και διεθνείς συναλλαγές.

Ηλεκτρονικά μετρητά και Ιστός[27] [www2.ellinogermaniki.gr]

Συστήματα όπως τα Digicash και Net Cash επιτρέπουν στον πελάτη να καταθέσει μετρητά σε έναν τραπεζικό λογαριασμό και μετά να χρησιμοποιήσει τα μετρητά για να αγοράσει αντικείμενα από το Διαδίκτυο. Digicash Οι πελάτες λαμβάνουν έναν κωδικοποιημένο αριθμό 64-bit για κάθε νόμισμα των 5 σεντς που μετατρέπουν σε ηλεκτρονικά μετρητά, τα οποία στη συνέχεια μεταφέρονται στο σκληρό δίσκο του χρήστη. Κατόπιν, ο πελάτης μπορεί να μεταφέρει τα μετρητά σε πωλητές στο Διαδίκτυο (αρκεί ο πωλητής να δέχεται αυτή τη μέθοδο πληρωμής). Ο πωλητής μετά επιστρέφει τα ηλεκτρονικά μετρητά στην τράπεζα ανταλλάσσοντάς τα με πραγματικά χρήματα.



ΕΙΚΟΝΑ 4 : Διαδικασία πληρωμής με ηλεκτρονικά μετρητά



Τα πλεονεκτήματα αυτού του συστήματος είναι:

- Ασφάλεια των προσωπικών δεδομένων:

Τα ηλεκτρονικά μετρητά δεν μπορούν να ανιχνευθούν. Η τράπεζα δεν συνδέει τα νούμερα με ένα συγκεκριμένο άτομο κι έτσι είναι αδύνατο να συνδεθεί η πληρωμή με αυτόν που πληρώνει. Ο πελάτης δεν χρειάζεται να ανησυχεί ότι θα προστεθεί σε μια σειρά από ταχυδρομικές λίστες, εκτός εάν έχει παραγγείλει εμπόρευμα το οποίο πρέπει να αποσταλεί στο σπίτι του αντί για πληροφορίες που μπορούν να αποσταλούν μέσω Διαδικτύου.

- Περιορισμένη ευθύνη:

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

Το κύριο μειονέκτημα αυτού του τύπου της συναλλαγής είναι ότι:

- Τα ψηφιακά χρήματα δεν είναι εξασφαλισμένη μέθοδος:

Για παράδειγμα, εάν καταρρεύσει ο σκληρός δίσκος σας, η ηλεκτρονική τράπεζα καταστρέφεται. Επιπλέον, εάν χάκερ αποκωδικοποιήσουν τους αριθμούς σας, δεν υπάρχει τρόπος να ανακτήσετε τα χαμένα σας μετρητά (σαν να πετούσατε ένα χαρτονόμισμα 20 δολαρίων στο δρόμο και το χάνατε). Από τη στιγμή που η τράπεζα δεν συνδέει τα χρήματα με το όνομά σας, δεν υπάρχει τρόπος να σας αποζημιώσει.

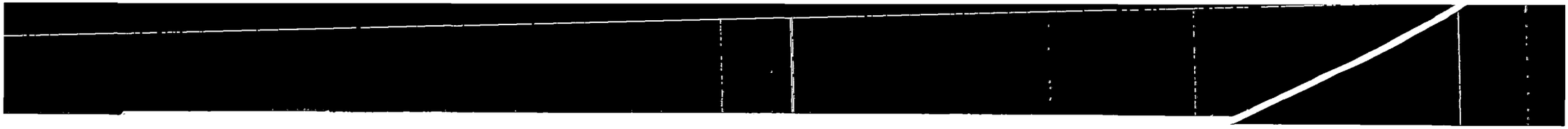
Ωστόσο, τα ηλεκτρονικά μετρητά Digicash μπορούν να ανακτηθούν στην περίπτωση κατάρρευσης του σκληρού δίσκου. Τότε ο πελάτης θα πρέπει να εγκαταλείψει την ανωνυμία του, ώστε η τράπεζα να αντικαταστήσει τα ηλεκτρονικά μετρητά του

Β) ΠΛΗΡΩΜΕΣ ΜΕΤΑΞΥ ΟΜΟΤΙΜΩΝ [28]

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 συναλλαγή. [*European Central Bank E-payments in Europe*][29] Επιπλέον, η απόκτηση λογαριασμού είναι πιο εύκολη απ' ότι 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.

Γ) ΠΡΟΠΛΗΡΩΜΕΝΕΣ ΚΑΡΤΕΣ

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.

Στον πίνακα που ακολουθεί επιχειρείται μια συνοπτική σύγκριση των έξι βασικότερων κατηγοριών συστημάτων ηλεκτρονικών πληρωμών με βάση χαρακτηριστικά που εντοπίστηκαν στην βιβλιογραφία.

Τα συστήματα που παρουσιάζονται είναι :

1) On-line πληρωμή με πιστωτική κάρτα
2) Ηλεκτρονικό χρήμα
3) Ηλεκτρονικές επιταγές
4) Προπληρωμένη κάρτα
5) Πληρωμές μεταξύ ομοτίμων
6) Μεταφορά ποσών

Στόχος αυτής της σύγκρισης είναι η εποπτική παρουσίαση των βασικότερων πλεονεκτημάτων και μειονεκτήματων κάθε συστήματος ηλεκτρονικών πληρωμών

Καθώς η λειτουργία και τα χαρακτηριστικά των χρεστικών καρτών ομοιάζουν με αυτά των πιστωτικών ,δεν περιλήφθηκαν και οι χρεωστικές κάρτες στον πίνακα.

	Εκ των υστέρων πληρωμή	Προπληρωμένα	Εκ των υστέρων πληρωμή	Προπληρωμένα	Πληρωμή τη στιγμή της αγοράς	Εκ των υστέρων πληρωμή
	Το κατάστημα και η τράπεζα ελέγχουν την φερεγγυότητα της πιστωτικής κάρτας	Ελεύθερη μεταφορά. Οι συναλλαγές δεν είναι προσωποπαγείς	Απαιτείται υπογραφή των ηλεκτρονικών επιταγών	Οι έξυπνες κάρτες πραγματοποιούν την μεταφορά πληροφοριών	Ο παροχέας επιβεβαιώνει τα στοιχεία των συναλλασσομένων	Η τράπεζα
	On-line	On-line	Επιτρέπονται offline συναλλαγές	Επιτρέπονται offline συναλλαγές	On-line	On-line
	Χρησιμοποιείται ο λογαριασμός της πιστωτικής κάρτας	Καμία χρήση	Απαιτείται χρήση τραπεζικού λογαριασμού	Χρησιμοποιείται ο λογαριασμός της έξυπνης κάρτας	Απαιτείται χρήση τραπεζικού λογαριασμού	Απαιτείται χρήση τραπεζικού λογαριασμού
	Κάθε κάτοχος πιστωτικής κάρτας	Οποιοδήποτε	Οποιοσδήποτε κάτοχος τραπεζικού λογαριασμού	Οποιοσδήποτε κάτοχος τραπεζικού λογαριασμού	Οποιοσδήποτε κάτοχος τραπεζικού λογαριασμού	Οποιοσδήποτε κάτοχος τραπεζικού λογαριασμού
	Η τράπεζα επωμίζεται το μεγαλύτερο μέρος του κινδύνου ενώ ο καταναλωτής μόνο ένα μέρος του	Ο καταναλωτής κινδυνεύει από κλοπή ή κακή χρήση του ηλεκτρονικού χρήματος	Ο καταναλωτής αναλαμβάνει το μεγαλύτερο μέρος του κινδύνου εντούτοις μπορεί να παγώσει ανά πάσα στιγμή τις πληρωμές	Ο καταναλωτής κινδυνεύει από κλοπή ή κακή χρήση της έξυπνης κάρτας	Ο καταναλωτής αναλαμβάνει το μεγαλύτερο μέρος του κινδύνου εντούτοις μπορεί να παγώσει ανά πάσα στιγμή τις πληρωμές	Ο καταναλωτής αναλαμβάνει το μεγαλύτερο μέρος του κινδύνου εντούτοις μπορεί να παγώσει ανά πάσα στιγμή τις πληρωμές
	Είναι δυνατή η χρήση τους διεθνώς και έτσι είναι πολύ δημοφιλής τρόπος πληρωμών	Όχι ιδιαίτερα δημοφιλής καθώς έχει σημαντικούς περιορισμούς	Μη δημοφιλές μέσο	Η χρήση του διευρύνεται διαρκώς καθώς μπορούν να χρησιμοποιηθούν διεθνώς	Η χρήση του διευρύνεται διαρκώς καθώς μπορούν να χρησιμοποιηθούν διεθνώς	Χρησιμοποιείται για διάφορες πληρωμές και στον πραγματικό κόσμο δεν είναι τόσο διαδεδομένο
	Μερικώς η ολικώς ανώνυμη συναλλαγή	Πλήρης ανωνυμία	Επώνυμη συναλλαγή	Πλήρης ανωνυμία	Επώνυμη συναλλαγή	Επώνυμη συναλλαγή
	Κόστος συναλλαγής υψηλό που δεν ενδείκνυται για ποσά μικρής αξίας	Χαμηλό κόστος συναλλαγών βολικό για ποσά μικρής αξίας	Επιτρέπει στα καταστήματα να συσσωρεύουν ποσά προτού γίνει η πληρωμή	Επιτρέπει στα καταστήματα να συσσωρεύουν ποσά προτού γίνει η πληρωμή	Δεν υπάρχει περιορισμός στο ποσό πληρωμής	Δεν υπάρχει περιορισμός στο ποσό πληρωμής
	Σε κάποιες περιπτώσεις χρησιμοποιείται και στον πραγματικό κόσμο	Χρήση μόνο στον εικονικό κόσμο	Χρήση στον εικονικό κόσμο.Μπορει να εκδίδει κανονικές επιταγές	Αληθινός και εικονικός κόσμος	Χρήση μόνο στον εικονικό κόσμο	Αληθινός και εικονικός κόσμος
	Εξαρτάται από το όριο της πιστωτικής κάρτας	Εξαρτάται από το ποσό που προπληρώθηκε	Κανένας περιορισμός	Εξαρτάται από την ποσότητα χρήματος που έχει αποθηκευτεί	Εξαρτάται από το ποσό που διαθέτει ο τραπεζικός λογαριασμός	Εξαρτάται από το ποσό που διαθέτει ο τραπεζικός λογαριασμός

ΕΙΚΟΝΑ 5 : Σύγκριση συστημάτων ηλεκτρονικών πληρωμών (προσαρμογή από Yu et al .2002)

2.3.1 ΣΥΧΝΕΣ ΕΡΩΤΗΣΕΙΣ ΚΑΙ ΣΧΕΤΙΚΕΣ ΠΛΗΡΟΦΟΡΙΕΣ ΓΙΑ ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΧΡΗΜΑ [30]

❖ **Τι είναι το ηλεκτρονικό χρήμα;**

Με τον όρο ηλεκτρονικό χρήμα περιγράφουμε κάθε μορφή μεταφοράς κεφαλαίου ,μεταξύ δύο ή περισσότερων μερών που γίνεται με ψηφιακό τρόπο και χωρίς την μεσολάβηση υλικού μέσου.

Το ηλεκτρονικό χρήμα βασίζεται στην ανταλλαγή πραγματικού χρήματος σε μια τράπεζα με ηλεκτρονικό τρόπο. Ένα συγκεκριμένο , δηλαδή, ποσό αληθινών χρημάτων ανταλλάσσεται με "κυβερνονομίσματα". Για την ύπαρξη δηλαδή ηλεκτρονικού χρήματος είναι απαραίτητα τρία στοιχεία 1) η νομισματική αξία αντιπροσωπευόμενη από απαίτηση έναντι του εκδότη, να είναι αποθηκευμένη σε ηλεκτρονικό υπόθεμα, 2) να έχει εκδοθεί κατόπιν παραλαβής χρηματικού ποσού τουλάχιστον ίσου με την εκδοθείσα νομισματική αξία, και 3) γίνεται δεκτή ως μέσο πληρωμής από άλλες επιχειρήσεις πέραν της εκδότριας.

❖ **Τα χαρακτηριστικά που πρέπει να έχει το ηλεκτρονικό χρήμα είναι:**

1. Ευρεία αποδοχή.
2. Ικανοποιητικό επίπεδο ασφαλείας.
3. Ανωνυμία.
4. Μεταφερσιμότητα (από μια μορφή σε μια άλλη π.χ. από ηλεκτρονικές μονάδες σε μετρητά).
5. Απεριόριστη διάρκεια (να μην έχει ημερομηνία λήξεως μετά το πέρας της οποίας θα πάψει να έχει αξία).
6. Αμφίδρομη κινητικότητα (κάθε κάτοχος να μπορεί να αποκτήσει και να δώσει χρήμα με την ίδια ευκολία. Δηλαδή να μην υπάρχει μια κυκλική ροή του τύπου: Τράπεζα-Ιδιώτης (αγοραστής)-Επιχείρηση (πωλητής)-Τράπεζα αλλά η δυνατότητα συναλλαγών και κάθε είδους πληρωμών μεταξύ όλων των οικονομικών μονάδων π.χ. μεταφορές χρημάτων από ιδιώτη σε ιδιώτη, από επιχείρηση σε επιχείρηση, από επιχείρηση σε ιδιώτη κτλ.).
7. Διαιρετότητα (να μπορεί να διαιρεθεί σε όσα τμήματα ίσης συνολικής αξίας θέλει ο κάτοχος).
8. Ευχρηστία.
9. Σταθερή αξία (προστασία από πληθωρισμό, υποτίμηση κτλ.).

❖ **Τι είναι το υπογεγραμμένο ηλεκτρονικό χρήμα (identified digital cash) και τι το ανώνυμο ηλεκτρονικό χρήμα (anonymous digital cash) ;**

Το Υπογεγραμμένο χρήμα περιέχει πληροφορίες που αναφέρουν ποιός υπήρξε ο αρχικός δημιουργός του (αυτός που έκανε την ανάληψη χρημάτων από την Τράπεζα) και ποιοί οι μετέπειτα κάτοχοί του. Ετσι, λειτουργεί σχεδόν με τον ίδιο τρόπο που λειτουργούν και οι πιστωτικές κάρτες, επιτρέποντας στην Τράπεζα να ακολουθήσει την πορεία του χρήματος μέσα στην οικονομία από τον ένα παραλήπτη στον άλλο.

Το Ανώνυμο χρήμα λειτουργεί ακριβώς όπως και τα μετρητά. Από την στιγμή που θα γίνει η ανάληψή του από τον τραπεζικό λογαριασμό, μπορεί να χρησιμοποιηθεί χωρίς να μπορεί κανείς να παρακολουθήσει την πορεία του.

Το ανώνυμο χρήμα λειτουργεί με την χρήση αριθμημένων (για έλεγχο) αλλά ανώνυμων τραπεζικών λογαριασμών και με τις λεγόμενες εικονικές υπογραφές (blind signatures). Πρόκειται για ηλεκτρονικές υπογραφές που εγγυώνται την αυθεντικότητά του, αλλά που ανήκουν στην τράπεζα και όχι σε συγκεκριμένα άτομα.

❖ **Τι είναι το ελεγχόμενο (online digital cash) και τι το αυτόνομο (offline digital cash) ηλεκτρονικό χρήμα;**

Στο Ελεγχόμενο ηλεκτρονικό χρήμα σημαίνει πως για την χρήση του πρέπει να υπάρχει επικοινωνία με μια Τράπεζα (μέσω modem ή δικτύου) η οποία ενεργεί ως μεσάζων/ ελεγκτής προκειμένου να πραγματοποιηθεί μια συναλλαγή.

Στο Αυτόνομο ηλεκτρονικό χρήμα αυτή η άμεση μεσολάβηση δεν είναι απαραίτητη. Αυτή η ιδιαιτερότητα κάνει το ανώνυμο χρήμα πιο περίπλοκο στην χρήση του και δημιουργεί το πρόβλημα του παράλληλου χρήματος (double-spending problem). Από την άλλη μεριά το αυτόνομο χρήμα έχει λιγότερες απαιτήσεις σε τηλεπικοινωνιακή υποδομή (αφού δεν χρειάζεται περίπλοκες και άμεσες συνδέσεις και ανταλλαγή μηνυμάτων με την μεσολαβούσα Τράπεζα ή άλλους φορείς).

❖ **Ποιοι μπορούν να εκδίδουν ηλεκτρονικό χρήμα;**

Ηλεκτρονικό χρήμα μπορούν να εκδίδουν μόνο πρόσωπα ή επιχειρήσεις που αποτελούν πιστωτικά ιδρύματα κατά την έννοια της οδηγίας 2000/12/ΕΚ, άρθρο 1, σημείο 1 πρώτο εδάφιο -"πιστωτικό ίδρυμα": επιχείρηση, της οποίας η δραστηριότητα συνίσταται στην αποδοχή καταθέσεων ή άλλων επιστρεπτέων κεφαλαίων από το κοινό και στη χορήγηση πιστώσεων για ίδιο λογαριασμό.

❖ **Τι γίνεται στην περίπτωση που αμφισβητηθεί η ηλεκτρονική πληρωμή με ηλεκτρονικό χρήμα;**

Αυτή η πληρωμή είναι μία τριπλή λειτουργία. Η τράπεζα πιστώνει τον πωλητή ,αφού εξακριβώσει τους κρυφούς κώδικες του ηλεκτρονικού χρήματος, με το ποσό που πληρώθηκε από τον καταναλωτή, του οποίου χρεώθηκε ο τρέχον λογαριασμός. Η τράπεζα επιβεβαιώνει την επιτυχή σύναψη της συναλλαγής και η πληρωμή δεν μπορεί να αμφισβητηθεί από τον πελάτη λόγω δέσμευσής της τράπεζας του να διαφυλάττει τους μυστικούς του κώδικες.

❖ **Ποιες πληροφορίες πρέπει να έχει στη διάθεσή του ο καταναλωτής από τον εκδότη ηλεκτρονικού χρήματος;**

Κατά την υπογραφή της σύμβασης του ηλεκτρονικού μέσου πληρωμής ο εκδότης ανακοινώνει στον κάτοχο τους συμβατικούς όρους που διέπουν την έκδοση και χρησιμοποίηση του ηλεκτρονικού μέσου πληρωμής. Οι όροι γνωστοποιούνται εγγράφως Οι όροι πρέπει να περιλαμβάνουν απαραίτητα :

α) περιγραφή του ηλεκτρονικού μέσου πληρωμής.
β) περιγραφή των αντίστοιχων υποχρεώσεων και ευθυνών του κατόχου και του εκδότη αναφέρονται ιδίως οι βασικές προφυλάξεις που πρέπει να λαμβάνει κάτοχος για να εξασφαλίσει την ασφάλεια του μέσου ηλεκτρονικής πληρωμής καθώς και τα μέσα που του επιτρέπουν να το χρησιμοποιεί (προσωπικός αριθμός αναγνώρισης ταυτότητας ή άλλος κωδικός αριθμός).

γ) κατά περίπτωση την κανονική περίοδο εντός της οποίας χρεώνεται ή πιστώνεται ο λογαριασμός του κατόχου.
δ) τα είδη των τυχόν εξόδων που βαρύνουν τον κάτοχο.
ε) τη χρονική περίοδο εντός της οποίας μια συγκεκριμένη συναλλαγή μπορεί να αμφισβητηθεί από τον κάτοχο και αναφορά των διαδικασιών καταγγελίας.

❖ **Ποιες πληροφορίες πρέπει να παρέχονται στον καταναλωτή μετά τη συναλλαγή;**

Ο εκδότης ηλεκτρονικού χρήματος πρέπει να παρέχει στον κάτοχο πληροφορίες σχετικά με τις συναλλαγές που έχουν γίνει με ηλεκτρονικό μέσο πληρωμής. Οι πληροφορίες αυτές που πρέπει να παρέχονται εγγράφως και περιλαμβάνουν τουλάχιστον τα ακόλουθα:

α) ένδειξη που επιτρέπει στον κάτοχο να εντοπίσει τη συναλλαγή.
β) το ποσό της συναλλαγής που χρεώνεται στον κάτοχο στο νόμισμα τιμολόγησης και κατά περίπτωση το ποσό σε ξένο νόμισμα.
γ) το ποσό τυχόν προμηθειών και εξόδων που εφαρμόζονται σε ορισμένα είδη συναλλαγών.

Ο εκδότης γνωστοποιεί επίσης στον κάτοχο τη συναλλαγματική ισοτιμία βάσει της οποίας γίνονται οι μετατροπές συναλλαγών σε ξένο νόμισμα. Ο εκδότης ενός μέσου ηλεκτρονικού χρήματος παρέχει στον κάτοχο τη δυνατότητα να ελέγχει τις τελευταίες πέντε συναλλαγές που εκτελέστηκαν με το μέσο αυτό και την απομένουσα αποθηκευμένη αξία σ' αυτό.

❖ **Ποιες είναι οι υποχρεώσεις του κατόχου ηλεκτρονικού χρήματος ;**

Ο κάτοχος ηλεκτρονικού χρήματος πρέπει να:

α) χρησιμοποιεί το μέσο ηλεκτρονικής πληρωμής σύμφωνα με τους όρους που διέπουν την έκδοση και χρήση του μέσου πληρωμής και ειδικότερα να λαμβάνει όλα τα απαραίτητα μέτρα για την ασφαλή φύλαξη του μέσου ηλεκτρονικής πληρωμής και των μέσων (προσωπικός αριθμός αναγνώρισης ταυτότητας ή άλλος κωδικός αριθμός) που επιτρέπουν τη χρησιμοποίησή του
β) ειδοποιεί χωρίς καθυστέρηση τον εκδότη μόλις αντιληφθεί:

- την απώλεια ή κλοπή του μέσου ηλεκτρονικής πληρωμής ή των μέσων που επιτρέπουν τη χρησιμοποίησή του
- τον καταλογισμό στο λογαριασμό του οποιασδήποτε συναλλαγής που έγινε παρά τη βούλησή του
- τυχόν σφάλμα ή ανωμαλία στην τήρηση του λογαριασμού του από τον εκδότη

γ) να μην καταγράφει τον προσωπικό του αριθμό αναγνώρισης ταυτότητας ή άλλο κωδικό αριθμό επί του μέσου ηλεκτρονικής πληρωμής ή άλλου αντικειμένου που φυλάσσει ή μεταφέρει μαζί με το μέσο ηλεκτρονικής πληρωμής.
δ) να μην ανακαλεί εντολή που έχει δώσει με το μέσο ηλεκτρονικής πληρωμής εκτός εάν το ποσό της δεν είχε προσδιοριστεί όταν δόθηκε η εντολή πληρωμής.

❖ **Πως και πότε μπορεί ο καταναλωτής να ζητήσει την εξαργύρωση του ηλεκτρονικού χρήματος που κατέχει;**

Ο κάτοχος ηλεκτρονικού χρήματος δικαιούται, κατά την περίοδο ισχύος του χρήματος αυτού, να ζητήσει την εξαργύρωση του στην ονομαστική αξία σε κέρματα και χαρτονομίσματα ή με μεταφορά σε τραπεζικό λογαριασμό χωρίς άλλα τέλη από τα απολύτως αναγκαία για την εκτέλεση της συγκεκριμένης πράξης.

Η σύμβαση μεταξύ του εκδότη και του κομιστή πρέπει να ορίζει σαφώς τους όρους εξαργύρωσης και να προβλέπει ένα ελάχιστο όριο εξαργύρωσης, το οποίο δεν μπορεί να υπερβαίνει τα 10 ευρώ.

❖ **Τι είναι το πρόβλημα του παράλληλου χρήματος (double-spending problem) ;**

Το ηλεκτρονικό χρήμα δεν είναι παρά μια σειρά από ψηφιακά στοιχεία (0 και 1). Για τον λόγο αυτό είναι εύκολο να αντιγραφεί. Επειδή κάθε αντίγραφο θα είναι ακριβώς το ίδιο με το πρωτότυπο, είναι αδύνατον να διακρίνουμε ποιό είναι το πρωτότυπο. Άρα, κάνοντας μερικά αντίγραφα του ηλεκτρονικού χρήματος που διαθέτει κάποιος μπορεί εύκολα, γρήγορα και απλά να γίνει εκατομμυριούχος, στέλνοντάς τα σε παράλληλους δρόμους μέσα στο δίκτυο.

Στα συστήματα ελεγχόμενου ηλεκτρονικού χρήματος (Online digital cash), το πρόβλημα παρακάμπτεται με την ανάγκη επιβεβαίωσης της συναλλαγής από την Τράπεζα πριν την εκτέλεσή της. Ο υπολογιστής της Τράπεζας έχει μια βάση δεδομένων στην οποία καταγράφονται όλες οι συναλλαγές που έχουν πραγματοποιηθεί. Ετσι η Τράπεζα γνωρίζει ανά πάσα στιγμή πόσα χρήματα δεν έχουν χρησιμοποιηθεί ακόμη (το υπόλοιπο του λογαριασμού του συναλλασσόμενου).

Αν οι Η/Υ της Τράπεζας λένε πως όλο το ποσό έχει δαπανηθεί, τότε ο συναλλασσόμενος ενημερώνεται σχετικά και αρνείται την εκτέλεση της συναλλαγής. Με άλλα λόγια, το σύστημα λειτουργεί με τον ίδιο τρόπο που σήμερα οι συναλλασσόμενοι ελέγχουν τις πιστωτικές κάρτες για να βεβαιωθούν ότι έχουν υπόλοιπο πριν γίνει η συναλλαγή.

Στην περίπτωση του αυτόνομου ηλεκτρονικού χρήματος (Offline digital cash) το πρόβλημα του παράλληλου χρήματος έχει διάφορες πιθανές λύσεις. Η μια είναι με την χρήση μια ειδικής "έξυπνης" κάρτας που περιέχει έναν επεξεργαστή για την καταχώρηση των συναλλαγών (σε μερικά συστήματα ο επεξεργαστής αυτός λέγεται "Παρατηρητής" (Observer). Ο Παρατηρητής καταχωρεί σε μια μικρή βάση δεδομένων όλες τις συναλλαγές με τέτοιο τρόπο που να μην είναι δυνατή η διαγραφή ή αλλοίωσή τους. Ετσι, δεν μπορεί να υπάρξει υπερκάλυψη του ποσού που έχει καταχωρηθεί στην κάρτα.

Ο άλλος τρόπος είναι η χρήση ειδικών κρυπτογραφικών πρωτοκόλλων που να κάνουν βέβαιη την εκ των υστέρων αναγνώριση της ταυτόχρονης χρήσης του ιδίου χρήματος (με μεταγενέστερο έλεγχο όλων των συναλλαγών). Το σύστημα αυτό μπορεί να ανακαλύψει τις παράνομες συναλλαγές, αφού όμως έχουν ήδη πραγματοποιηθεί. Η συλλογιστική πίσω από μια τέτοια μέθοδο είναι πως αν ο υποψήφιος παραβάτης ξέρει πως δεν υπάρχει καμία περίπτωση να γλιτώσει δεν θα κάνει την παρανομία. Το πλεονέκτημα αυτή της μεθόδου είναι ότι μπορεί να λειτουργήσει σε κοινούς προσωπικούς Η/Υ και φθηνές έξυπνες κάρτες χωρίς να χρειάζεται ειδικούς (και ακριβούς) επεξεργαστές.

Συστήματα που να χρησιμοποιούν υπογεγραμμένο αυτόνομο χρήμα είναι αρκετά εύκολο να δημιουργηθούν. Κάθε φορά που γίνεται μια καινούρια συναλλαγή,

στην υπογραφή που περιέχεται στο χρήμα αυτό προστίθεται ο τελευταίος συναλλασσόμενος. Ετσι, όταν τελικά το χρήμα κάνει τον κύκλο του και επιστρέψει στην Τράπεζα για κατάθεση, αυτή μπορεί να ελέγξει αν έχει γίνει παράλληλη χρήση του ίδιο ποσού. Στην περίπτωση που έχει συμβεί κάτι τέτοιο, οι υπογραφές μπορούν εύκολα να μας οδηγήσουν στον παραβάτη.

Το ίδιο θα συμβεί και στην περίπτωση του αυτόνομου χρήματος. Και εδώ, με κάθε συναλλαγή, μεγαλώνει η υπογραφή του χρήματος, καταγράφοντας στοιχεία. Στην περίπτωση αυτή, τα στοιχεία που καταγράφονται είναι διαφορετικά, αλλά το αποτέλεσμα το ίδιο. Όταν κάποια στιγμή το χρήμα φθάσει στην Τράπεζα, εκείνη θα μπορέσει να διακρίνει αν έγινε παράλληλη χρήση, και να ανακαλύψει τον δράστη. Η διαφορά έγκειται στο γεγονός πως στο αυτόνομο χρήμα, η Τράπεζα θα μάθει τις ταυτότητες όλων όσων χρησιμοποίησαν αυτό το χρήμα μόνο αν έχει υπάρξει παράλληλη χρήση. Δηλαδή μόνο όταν είναι αναγκαίο. Αν το χρήμα έχει χρησιμοποιηθεί κανονικά, η Τράπεζα δεν μπορεί να μάθει ποιός είναι ο αρχικός αποστολέας του χρήματος, ούτε ποιες συναλλαγές έγιναν με αυτό πριν καταλήξει σε εκείνη.

❖ **Γιατί αναπτύσσονται τόσα πολλά είδη ηλεκτρονικού χρήματος;**

Κατά αρχήν διότι είμαστε ακόμη στο πειραματικό στάδιο και κάθε ενδιαφερόμενος προτείνει την λύση που πιστεύει πως θα ικανοποιήσει καλύτερα τις μελλοντικές ανάγκες. Επίσης, διότι δεν γνωρίζουμε ακριβώς τι είδους ανάγκες θα πρέπει να καλύψει το ηλεκτρονικό χρήμα και για αυτό κάθε πρόταση προβάλλει εκείνες που θεωρεί πιο σημαντικές ή εκείνες που έχει την τεχνογνωσία να καλύψει.

Αυτό άλλωστε είναι και ο λόγος που υπάρχουν τόσα είδη χρήματος και στην "πραγματική" οικονομία (μετρητά, προσωπικές επιταγές, τραπεζικές επιταγές, εμβάσματα, πιστωτικές και χρεωστικές κάρτες, γραμμάτια, συναλλαγματικές κτλ.).

Κάθε ένα από αυτά καλύπτει διαφορετικές ανάγκες (ανωνυμία, αποδοχή από την αγορά, ασφάλεια, κόστος συναλλαγών, δυνατότητα εύκολης διαίρεσης ενός μεγάλου ποσού, ανεξαρτησία από την χρήση μηχανών κτλ.). Αφού υπάρχουν διαφορετικά είδη συναλλαγών και χρήματος στην "πραγματική" οικονομία πρέπει να περιμένουμε το ίδιο να συμβεί και στην οικονομία του δικτύου.

❖ **Μπορεί να γίνει "ξέπλυμα χρημάτων" με το ηλεκτρονικό χρήμα;**

Κατά αρχήν αυτή την στιγμή δεν υπάρχει πραγματικό ηλεκτρονικό χρήμα και κατόπιν τούτου δεν μπορούμε να πούμε με βεβαιότητα πως θα μπορεί να χρησιμοποιηθεί για τέτοιες δραστηριότητες όταν θα υπάρξει. Η συλλογιστική πάντως είναι ότι: Ο Α έμπορος ναρκωτικών βάζει προς πώληση στο Internet ένα άχρηστο αντικείμενο που στη συνέχεια αγοράζει ο ίδιος με άλλο όνομα (το να αποκτήσεις πολλά ονόματα στο Internet είναι πολύ εύκολο). Ετσι, χωρίς να μπορεί να τον ελέγξει κανείς (αφού το ηλεκτρονικό χρήμα δεν αφήνει στοιχεία για την χρήση του) έκανε μια νόμιμη συναλλαγή και έφερε τα χρήματά που κέρδισε παράνομα στην νόμιμη οικονομία.

Εχει γίνει κάποια συζήτηση για το θέμα αυτό αλλά είναι πολύ νωρίς για να φθάσουμε σε συμπεράσματα (π.χ. μπορεί να υπάρξει ένα ανώτατο ποσό ανά συναλλαγή, πάνω από το οποίο να χρειάζεται ειδική δήλωση της ταυτότητας των συμβαλομένων).

❖ **Γιατί πολλοί θεωρούν το Ηλεκτρονικό Χρήμα σαν ένα τρόπο να προστατευτούν οι ατομικές ελευθερίες;**

Διότι κάθε μορφή συναλλαγών που κάνουμε με πλασματικό χρήμα (επιταγές, πιστωτικές κάρτες κτλ.) καταγράφεται στα αρχεία των πιστωτικών ιδρυμάτων που μας χορηγούν τα νέα αυτά μέσα συναλλαγών. Όταν μια Τράπεζα γνωρίζει όλες τις καταναλωτικές μου συνήθειες (αφού γνωρίζει τι αγοράζω καθώς κάθε μήνα εκκαθαρίζει τις συναλλαγές που έκανα με την πιστωτική μου κάρτα) μπορεί να πουλήσει αυτό το υλικό σε διαφημιστές, να το χρησιμοποιήσει για να δημιουργήσει ένα ψυχολογικό πορτραίτο μου, να προβλέψει το κόμμα που ψηφίζω ή το ιδεολογικό προφίλ μου (αν πληρώνω για συνδρομές σε περιοδικά, συλλόγους ή προσφέρω οικονομική ενίσχυση σε κάποιο κόμμα πληρώνοντας με την κάρτα μου) κτλ. Το ηλεκτρονικό χρήμα υπόσχεται ανωνυμία, δεν μπορεί να το παρακολουθήσει κανείς και για τον λόγο αυτό εξασφαλίζει ότι κανένας δεν θα μπορεί να μάθει πως δαπανώ το εισόδημά μου και γιατί.

❖ **Η τεχνολογία για την δημιουργία ηλεκτρονικού χρήματος είναι ήδη διαθέσιμη. Γιατί λοιπόν δεν υπάρχει ακόμη στην πράξη;**

Το πρόβλημα σε τέτοιες περιπτώσεις είναι πάντοτε τα πρότυπα. Ας μην ξεχνούμε ότι όταν λέμε χρήμα, εννοούμε ένα "ευρέως αποδεκτό μέσο συναλλαγών". Το "ευρέως αποδεκτό" είναι που απουσιάζει σήμερα. Πάντως το μέλλον φαίνεται πως ανήκει στο ελεγχόμενο και υπογεγραμμένο χρήμα για τις μεταβιβάσεις σχετικά μεγάλων ποσών, ενώ στο αυτόνομο και ανώνυμο χρήμα για τις συναλλαγές με μικροποσά (με άλλα λόγια, λίγο πολύ ότι γίνεται και στην πραγματική οικονομία μεταξύ πιστωτικών καρτών-επιταγών από την μια μεριά και μετρητών από την άλλη).

Πολύ καλό μέλλον φαίνεται πως έχουν και οι έξυπνες κάρτες, ή ηλεκτρονικά πορτοφόλια όπως αλλιώς λέγονται, διότι υπόσχονται ευχρηστία, απλότητα και υψηλό επίπεδο ασφαλείας.

❖ **Τι είναι οι small-money transfers και ποιές οι εφαρμογές τους;**

Κυριολεκτικά, ο όρος αναφέρεται σε χρηματικές συναλλαγές που αφορούν εξαιρετικά μικρά ποσά (συνήθως μικρότερα από 1 ή 2 δολλάρια). Επειδή όμως κάτι τέτοιο δεν μπορεί να γίνει με τους παραδοσιακούς τρόπους πληρωμής (επιταγές, πιστωτικές κάρτες κτλ.) διότι το σταθερό κόστος είναι μεγάλο, θα εκτελούνται με κάποια μορφή ηλεκτρονικού χρήματος.

Η βασική εφαρμογή που μπορούν να έχουν είναι η αγορά των λεγόμενων information mini-services. Για παράδειγμα, εγώ σαν συγγραφέας χρεώνω 30 δρχ. σε εσάς για την ανάγνωση αυτού του κειμένου. Το ποσό είναι αρκετά μικρό για να δεχθείτε να το πληρώσετε. Αν χίλιοι άνθρωποι δεχθούν να πληρώσουν, η αμοιβή των 30.000 Δρχ. που θα λάβω θα είναι αρκετά ικανοποιητική για τον κόπο μου.

Τεχνικά δεν υπάρχει κανένα πρόβλημα με το είδος αυτό των συναλλαγών. Το μόνο πρόβλημα βρίσκεται στο ότι η αμοιβή μιας τέτοιας υπηρεσίας σήμερα δεν μπορεί να είναι μικρότερη από 1000 δρχ. Ετσι, για καθαρά οικονομικούς λόγους θα πρέπει να περιμένουμε μέχρι η τεχνολογία, ο αυτοματισμός και τα τραπεζικά καρτέλ

να επιτρέψουν στις προμήθειες που εισπράτονται από κάθε συναλλαγή να μειωθούν δραστικά.

❖ **Τι προβλέπεται για την προστασία των προσωπικών δεδομένων και την ασφάλεια των συναλλαγών στη χρήση του ηλεκτρονικού χρήματος**

Η ηλεκτρονική πληρωμή έχει οριστικό χαρακτήρα. Η εντολή που δίνεται μέσω μιας κάρτας πληρωμής είναι ανέκκλητη και δεν επιτρέπει επομένως καμία αντίθετη εντολή.

Τα δεδομένα που διαβιβάζονται, τη στιγμή της πληρωμής, στην τράπεζα του παρέχοντος υπηρεσίες και στη συνέχεια στον εκδότη 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.

Όλα τα προβλήματα που συνδέονται με την προστασία των δεδομένων και την ασφάλεια πρέπει να αναφέρονται ρητά και να επιλύονται σε όλα τα στάδια της σύναψης των συμβάσεων μεταξύ των συμβαλλόμενων μερών.Οι συμβάσεις δεν πρέπει να θέτουν σε κίνδυνο την ελευθερία διαχείρισης των παρεχόντων υπηρεσιών και τον ανταγωνισμό μεταξύ τους.

2.4 ΚΙΝΗΤΕΣ ΠΛΗΡΩΜΕΣ (MOBILE PAYMENTS) [31]

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 των κόσμο το 2002, σύμφωνα με τον παγκόσμιο οργανισμό κινητής τηλεφωνίας (UMTS). Σύμφωνα με έρευνα του διεθνούς οίκου Forester (2001)[32] [*De Lussanet, M., Nordan, M.M., Siepermann, M. & Bedarida, D.E. (May 2001)*]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) [33] [*Tan Cheng-Lin, (2002) Mobile payments in M-Commerce*] συνήθως εμφανίζονται οι παρακάτω συμμετέχοντες στη διαδικασία αγοράς αγαθών και υπηρεσιών μέσω κινητού τηλεφώνου: ο παροχέας περιεχομένου (content provider), ο παροχέας αυθεντικοποίησης του καταναλωτή (authentication provider), ο οργανισμός που εγκρίνει την πληρωμή (payment authorisation), ο διεκπεραιωτής της συναλλαγής (settlement provider), ο παροχέας υπηρεσιών πληρωμών (Payment Service Provider) και τέλος ο καταναλωτής (consumer).

Ο καταναλωτής είναι αυτός που έχει στην κατοχή του τη συσκευή κινητής τηλεφωνίας και προχωρά σε αγορά περιεχομένου ή υπηρεσιών από τον παροχέα περιεχομένου. Ο παροχέας αυθεντικοποίησης της ταυτότητας του καταναλωτή ή αλλιώς Έμπιστη Τρίτη Οντότητα (ΕΤΟ) είναι ένας ανεξάρτητος οργανισμός που φροντίζει για την πιστοποίηση της ταυτότητας του καταναλωτή. Ο διεκπεραιωτής της συναλλαγής θα μπόρουσε να είναι μια τράπεζα, μία εταιρία παροχής κινητής τηλεφωνίας ή ακόμη και ένας εκδότης πιστωτικών καρτών.

Ο παροχέας υπηρεσιών πληρωμών (Payment Service Provider PSP), είναι κεντρική οντότητα για την διαδικασία της πληρωμής μέσω κινητού. Αυτός δέχεται το μήνυμα για αγορά αγαθού και το κατευθύνει στην ΕΤΟ. Το μήνυμα μπορεί να σταλεί με μία πληθώρα τεχνολογιών που υιοθετούνται από τις συσκευές κινητής τηλεφωνίας όπως SMS, WAP, SIM application toolkit (SAT), USSD, IVR, dual slot phones, dual SIM Phones, Bluetooth, Infrared, Bar code readers και contactless chips.

Οι ηλεκτρονικές πληρωμές μέσω κινητού συνήθως περιλαμβάνουν μια εφαρμογή ηλεκτρονικού πορτοφολιού που επιτρέπει στους καταναλωτές να αποθηκεύουν τις πληροφορίες της αγοράς του αγαθού, όπως τον αριθμό της πιστωτικής τους κάρτας και/ ή τη διεύθυνση αποστολής του αγαθού σε έναν ασφαλή διακομηστή (server) του παροχέα υπηρεσιών πληρωμών. Χαρακτηριστικό είναι ότι πίσω από τους ρόλους του Παροχέα Υπηρεσιών Πληρωμών, της Έμπιστης Τρίτης Οντότητας, και του Παροχέα Περιεχομένου συνήθως βρίσκεται μια εταιρία παροχής υπηρεσιών κινητής τηλεφωνίας.

Οι μεταβλητές που προσδίδουν ιδιαίτερα χαρακτηριστικά στις αγορές μέσω κινητού τηλεφώνου είναι συνήθως ο χρόνος διεκπεραίωσης της συναλλαγής, το περιεχόμενο αυτής και το ύψος της αγοράς.

Έτσι έχουμε τα παρακάτω **είδη συναλλαγών μέσω κινητού τηλεφώνου.**

Α) Προπληρωμένες αγορές:

Ο καταναλωτής προπληρώνει στον PSP ένα συγκεκριμένο ποσό για το περιεχόμενο της υπηρεσίας ή των αγαθών που θα αγοράσει, με την μορφή αγοραστικών μονάδων ή μονάδων μιας κάρτας ομιλίας.

Β) Πληρωμές μετά την αγορά:

Ο καταναλωτής αφού προβεί στην αγορά του αγαθού πληρώνει εκ των υστέρων ,συνήθως με χρέωση της πιστωτικής του κάρτας ή με χρέωση του λογαριασμού του κινητού του τηλεφώνου.

Γ) Αγορά σε πραγματικό χρόνο:

Ο καταναλωτής προχωρά στην αγορά ενός αγαθού τη στιγμή που εξερευνά την ηλεκτρονική ιστοσελίδα μιας εταιρίας μέσω της συσκευής του. Για παράδειγμα όταν θέλει να αποθήκευσει στη συσκευή του ένα τραγούδι σε μορφή MP3, απλά το επιλέγει και το αποθηκεύει στο κινητό του. Η χρέωση γίνεται με τις διαδικασίες που ακολουθούνται στο ηλεκτρονικό εμπόριο.

Το είδος των αγαθών που μπορεί να αγοράσει ο καταναλωτής συνήθως χωρίζονται στις παρακάτω κατηγορίες:

- 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 (ψήφος σε ένα τηλεπαιχνίδι)
- Αγορά εισιτηρίων (κινηματογράφου, θεάτρου κλπ.)

Επίσης, αναλόγως του περιεχομένου της αγοράς, οι πληρωμές χωρίζονται σε μίκρο και μάκρο πληρωμές. Συνήθως το διαχωριστικό όριο αξίας του αγαθού είναι το ποσό των 10 Ευρώ.

Η κεντρική τράπεζα της Φινλανδίας σε έκθεση της, το 2003[34] [*Jyrkonen, H. and Paunonen H. (2003)*]κάνει μια αναφορά στα πιο διαδεδομένα συστήματα ηλεκτρονικών πληρωμών ανά την Ευρώπη. Ένα από τα πιο γνωστά συστήματα είναι 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.

3 ΤΡΕΧΟΥΣΕΣ ΔΙΑΔΙΚΑΣΙΕΣ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ [35]

Δεν είναι δυνατό να υπάρξει ηλεκτρονικό εμπόριο χωρίς έναν τρόπο μεταφοράς χρηματικών πόρων (πληρωμής) μέσω της ψηφιακής υποδομής. Κάθε σύστημα ηλεκτρονικής πληρωμής θα πρέπει να καλύπτει όλα τα χαρακτηριστικά που οι διάφορες πλευρές μιας συναλλαγής θεωρούν ως απαραίτητα ή σημαντικά.

Σε μια ηλεκτρονική συναλλαγή εμπλέκονται συνήθως τρία μέρη:

- ο έμπορος (πωλητής),
- ο πελάτης (αγοραστής), και
- ο οργανισμός που παρέχει τις οικονομικές υπηρεσίες (π.χ. οργανισμός πιστωτικών καρτών)

Έμπορος

Το σημαντικότερο χαρακτηριστικό ενός συστήματος πληρωμής, από την πλευρά του εμπόρου, είναι η ευκολία της χρήσης του από τον πελάτη. Ο πελάτης θα πρέπει να έχει τη δυνατότητα να κάνει παρορμητικές αγορές, χωρίς να εμποδίζεται από δυσκολίες που οφείλονται αποκλειστικά στο σύστημα πληρωμής.

Ένας από τους λόγους που ο έμπορος έχει υιοθετήσει το ηλεκτρονικό εμπόριο είναι ότι μπορεί να διευρύνει τη βάση των πελατών του. Αν το σύστημα πληρωμής περιορίζει αυτή τη βάση, το κίνητρο αναιρείται. Έτσι μια από τις προϋποθέσεις ενός συστήματος ηλεκτρονικής πληρωμής είναι η ευρεία αποδοχή του.

Ένα δεύτερο χαρακτηριστικό είναι το κόστος των συναλλαγών. Ο έμπορος επιθυμεί να έχει μικρό κόστος συναλλαγών ώστε να μπορεί να μειώσει τις τιμές των προϊόντων και να αυξήσει την ανταγωνιστικότητά του. Ένα μέρος του κόστους συναλλαγών είναι η αμοιβή του οικονομικού οργανισμού που ενεργεί τις ηλεκτρονικές πληρωμές.

Άλλα στοιχεία του κόστους συναλλαγών είναι ο απαιτούμενος χρόνος για την ολοκλήρωση μιας συναλλαγής, και ο κίνδυνος επισφαλών συναλλαγών (όπως για παράδειγμα πλαστά στοιχεία πληρωμής ή αδυναμία του πελάτη να καλύψει το ποσό της πληρωμής).

Πελάτης

Πολλά από τα παραπάνω χαρακτηριστικά αφορούν εξίσου τον πελάτη. Ο πελάτης θέλει να αισθάνεται ότι είναι ασφαλής και ότι δεν θα πέσει θύμα απατεώνων που θα εκμεταλλευτούν τις πληροφορίες σχετικά με την ηλεκτρονική πληρωμή του (π.χ. τον αριθμό της πιστωτικής κάρτας).

Επίσης θα πρέπει να μπορεί να κάνει ηλεκτρονικές πληρωμές με το ίδιο σύστημα και με την ίδια ευκολία σε πολλούς εμπόρους-όχι μόνο για να έχει τη δυνατότητα επιλογής, αλλά και για να αποφεύγει την ταλαιπωρία της εκμάθησης πολλών διαφορετικών μεθόδων πληρωμής.

Οι πελάτες δεν μπορούν να ανεχθούν κανένα πρόσθετο κόστος στις συναλλαγές τους, είτε αυτό είναι σε χρήμα είτε σε χρόνο. (π.χ για την επανειλημμένη πληκτρολόγηση των προσωπικών τους στοιχείων σε μια οθόνη)

Οργανισμός οικονομικών υπηρεσιών

Οι οργανισμοί που υποστηρίζουν ηλεκτρονικές πληρωμές, όπως οι οργανισμοί πιστωτικών καρτών, έχουν ως σκοπό το κέρδος. Έτσι κάθε συναλλαγή που χρησιμοποιεί ως ενδιάμεσο ένα τέτοιο οργανισμό επιβαρύνεται με την αμοιβή του οργανισμού. Φυσικά για να κρατούν τις υπηρεσίες τους ελκυστικές οι οργανισμοί οικονομικών υπηρεσιών κρατούν το κόστος κάθε συναλλαγής αρκετά χαμηλό και προσπαθούν να αυξήσουν τα κέρδη τους με την διεύρυνση της χρήσης των μέσων πληρωμής που προσφέρουν. Ένα πρόβλημα στο σημείο αυτό είναι η δυσπιστία εμπόρων και καταναλωτών προς οικονομικούς οργανισμούς που μονοπωλούν κάποιο μέσο πληρωμής.

Η λύση είναι η δημιουργία ενός κοινού μέσου πληρωμής που να υποστηρίζεται από πολλούς οργανισμούς, ώστε να εξασφαλίζεται μια ανταγωνιστική αγορά οικονομικών υπηρεσιών. Ο ανταγωνισμός μπορεί να οδηγήσει στη μείωση του κόστους συναλλαγών και στην προσφορά πρόσθετων υπηρεσιών, που είναι προς το κοινό όφελος καταναλωτών και εμπόρων.

Μια από τις υπηρεσίες προστιθέμενης αξίας που αναλαμβάνουν οι οργανισμοί οικονομικών υπηρεσιών, στα πλαίσια του μεταξύ τους ανταγωνισμού, είναι η διαχείριση των κινδύνων συναλλαγής. Στη διάρκεια μιας ηλεκτρονικής συναλλαγής υπάρχουν πολλοί παράγοντες που μπορεί να προκαλέσουν μια αποτυχία. Για παράδειγμα, ο πωλητής μπορεί να μην λάβει την πληρωμή ο αγοραστής να μην λάβει το προϊόν για το οποίο ήδη έχει πληρώσει, και τα στοιχεία της πληρωμής μπορούν να υποκλαπούν ή να παραποιηθούν για παράνομους σκοπούς.

Ο οικονομικός οργανισμός μπορεί να καλύψει όλους αυτούς τους κινδύνους όπως να εγγυηθεί στον πωλητή την κάλυψη του ποσού πληρωμής, να βεβαιώσει στον αγοραστή την είσπραξη του ποσού από τον πωλητή, και να φροντίσει για την απαραίτητη τεχνολογική υποδομή που θα προστατεύσει τις πληροφορίες από υποκλοπή ή παραποίηση. Δυο πολλοί μεγάλοι οργανισμοί που προσφέρουν τέτοιες υπηρεσίες διαχείρισης του κινδύνου είναι οι γνωστοί οργανισμοί πιστωτικών καρτών MasterCard και VISA.

4 ΠΡΟΤΥΠΑ ΚΑΙ ΜΕΘΟΔΟΙ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ [36]

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

Εκτός από τις παραπάνω θεμελιώδεις ιδιότητες του χρήματος, ένα σύστημα ηλεκτρονικής πληρωμής πρέπει επίσης να διαθέτει τα εξής χαρακτηριστικά: ασφάλεια, αξιοπιστία, δυνατότητα μαζικής χρήσης, ανωνυμία, αποδοχή, ευρεία βάση πελατών, ευελιξία, μετατρεψιμότητα, αποτελεσματικότητα συναλλαγών, μικρό κόστος και ευκολία χρήσης.

Τα ένδεκα αυτά χαρακτηριστικά μπορούν να χρησιμοποιηθούν ως κριτήρια για την ανάλυση των μεθόδων ηλεκτρονικής πληρωμής που είναι σήμερα σε χρήση:

- **κρυπτογραφημένη μετάδοση στοιχείων συμβατικής πληρωμής,**
- **ψηφιακά μετρητά,**
- **λογαριασμοί χρέωσης-πίστωσης,**
- **ηλεκτρονικές επιταγές,**
- **άμεση μεταφορά και**
- **υπηρεσίες είσπραξης.**

Α) Κρυπτογραφημένη μετάδοση στοιχείων

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

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

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

Ένα δεύτερο μειονέκτημα είναι το κόστος της χρήσης ενός ενδιάμεσου οργανισμού για την πραγματοποίηση των πληρωμών. Ειδικά αν η τιμή των προϊόντων

είναι πολύ μικρή, το κόστος μιας συναλλαγής μπορεί να είναι υψηλότερο από το αντίστοιχο της πώλησης.

Β) Ψηφιακά μετρητά

Τα «ψηφιακά μετρητά» είναι ένα μέσο ηλεκτρονικής πληρωμής ανάλογο με τα κοινά μετρητά, κέρματα και χαρτονομίσματα. Ο πελάτης έχει ένα «ηλεκτρονικό πορτοφόλι» συνήθως με τη μορφή μιας ειδικής ηλεκτρονικής κάρτας, που το «φορτώνει» χρήματα από τον τραπεζικό λογαριασμό ή πληρώνοντας τα αντίστοιχα μετρητά στο ταμείο μιας τράπεζας. Η κάρτα είναι ανώνυμη και έχει αποθηκευμένη την αξία των χρημάτων με τα οποία έχει «φορτωθεί».

Ένας έμπορος που δέχεται ψηφιακά μετρητά μπορεί να αφαιρέσει ένα ποσό από την κάρτα και να το μεταφέρει σε ένα δικό του ηλεκτρονικό πορτοφόλι. Ο οικονομικός οργανισμός που υποστηρίζει τα ψηφιακά μετρητά μπορεί στη συνέχεια να ανταλλάξει την αξία που είναι αποθηκευμένη στην κάρτα του εμπόρου με κοινά χρήματα.

Τα ψηφιακά μετρητά έχουν δυο πλεονεκτήματα Το πρώτο που έχει ιδιαίτερη σημασία για τους πελάτες, είναι η ανωνυμία των συναλλαγών. Το δεύτερο είναι η δυνατότητα χρήσης των ψηφιακών μετρητών ως μέσο πληρωμής ακόμη και χωρίς την μεσολάβηση του οικονομικού οργανισμού που τα υποστηρίζει: για παράδειγμα ένας έμπορος μπορεί να χρησιμοποιήσει απευθείας το ηλεκτρονικό του πορτοφόλι για να πληρώσει τις προμήθειες του, χωρίς να είναι υποχρεωμένος να το ξεφορτώσει στον τραπεζικό του λογαριασμό ή να μετατρέψει το περιεχόμενό του σε άλλο μέσο πληρωμής.

Γ) Λογαριασμοί χρέωσης-πίστωσης

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

Το κύριο πλεονέκτημα αυτής της μεθόδου είναι η ευελιξία. Ο ίδιος μηχανισμός μπορεί να χρησιμοποιηθεί για πολλά είδη συναλλαγών. Αν χρειαστεί το σύστημα μπορεί επίσης να επιτρέψει ανώνυμες συναλλαγές.

Το μειονέκτημα της μεθόδου είναι ότι η προεργασία για την πληρωμή προηγείται της συναλλαγής (push model) και κάθε πελάτης πρέπει να έχει ανοίξει λογαριασμό πριν πραγματοποιήσει την πρώτη του αγορά. Έτσι το σύστημα δεν υποστηρίζει παρορμητικές αγορές.

Δ) Ηλεκτρονικές επιταγές

Οι ηλεκτρονικές επιταγές είναι η φυσιολογική συνέχεια των παραδοσιακών επιταγών, που τώρα υπογράφονται και μεταβιβάζονται ηλεκτρονικά, και μπορούν να έχουν όλες τις παραλλαγές των κοινών επιταγών, όπως ταξιδιωτικές επιταγές ή πιστοποιημένες επιταγές. Οι ηλεκτρονικές επιταγές χρησιμοποιούν την τεχνολογία των ψηφιακών υπογραφών, και μπορούν να αποτελέσουν το συνδετικό κρίκο που θα

διευκολύνει το πέρασμα από τις υπάρχουσες μεθόδους πληρωμής στις μεθόδους ηλεκτρονικής πληρωμής.

Ε) Άμεση μεταφορά

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

ΣΤ) Υπηρεσίες είσπραξης

Οι υπηρεσίες είσπραξης, που ονομάζονται επίσης εκκαθάρισης συναλλαγών, δεν είναι μια αυτόνομη μέθοδος πληρωμής αλλά ένα μέσο για την πραγματοποίηση των πληρωμών με τις μεθόδους που έχουν αναφερθεί παραπάνω.

Οι υπηρεσίες είσπραξης είναι ενδιάμεσοι που αναλαμβάνουν την είσπραξη πληρωμών για λογαριασμό των εμπόρων. Ο αγοραστής λαμβάνει από τον έμπορο τις απαραίτητες πληροφορίες για να πληρώσει στην υπηρεσία είσπραξης, η οποία δέχεται την πληρωμή και επιστρέφει στον πελάτη μια απόδειξη, με την οποία αυτός μπορεί να παραλάβει το προϊόν που έχει αγοράσει.

Η διαδικασία της συναλλαγής περιπλέκεται, αλλά ο έμπορος έχει το πλεονέκτημα ότι η υπηρεσία είσπραξης μπορεί να δεχθεί όλες τις μεθόδους ηλεκτρονικής πληρωμής.

4.1 ΔΙΑΘΕΣΙΜΑ ΣΥΣΤΗΜΑΤΑ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ ΣΗΜΕΡΑ [37]

Τα σημερινά συστήματα ηλεκτρονικής πληρωμής χωρίζονται σε δυο κατηγορίες-αυτά που βασίζονται σε ειδικό λογισμικό και αυτά που χρησιμοποιούν ειδικές ηλεκτρονικές κάρτες (smart cards). Η τεχνολογία των συστημάτων ηλεκτρονικής πληρωμής βρίσκεται σε μια φάση διαμόρφωσης και είναι ακόμη πολύ ρευστή.

Συστήματα κρυπτογραφημένης μετάδοσης και πιστωτικές κάρτες :

❖ **Cyber Cash [www.cybercash.com]**

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

Το σύστημα CyberCash έχει ήδη ολοκληρωθεί και βρίσκεται σε χρήση από ένα μεγάλο αριθμό επιχειρήσεων κάθε μεγέθους, που δραστηριοποιούνται στο ηλεκτρονικό

εμπόριο. Ο κίνδυνος για τους αγοραστές που χρησιμοποιούν το σύστημα CyberCash είναι ελάχιστος, και συχνά καλύπτεται από την πολιτική των οργανισμών πιστωτικών καρτών (για παράδειγμα στις ΗΠΑ οι οργανισμοί πιστωτικών καρτών καλύπτουν κάθε απώλεια αξίας πάνω από 50 δολάρια).

Το πλεονέκτημα του συστήματος CyberCash είναι ότι χρησιμοποιεί ισχυρή κρυπτογράφηση και συγχρόνως μπορεί να περνά χωρίς πρόβλημα από φίλτρα πρόσβασης στο διαδίκτυο. Το κύριο μειονέκτημα είναι ότι δεν προστατεύει την ανωνυμία του αγοραστή, όπως συμβαίνει πάντοτε με την χρήση πιστωτικών καρτών.

❖ **SET [www.visa.com]** [Αναλυτικά στην ενότητα 9.4]

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

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

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

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

❖ **NetCash. [www.netbank.com] (Software Agents)**

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

Ψηφιακά μετρητά

❖ **Millicent [www.millicent.org]**

Ένα «ελαφρύ» αλλά ασφαλές πρωτόκολλο, που επιτρέπει οικονομικές συναλλαγές με πάρα πολύ μικρά ποσά. Το κόστος κάθε συναλλαγής είναι ένα χιλιοστό του Cent (1/100 του δολαρίου), από όπου το σύστημα έχει πάρει το όνομά του.

Ο αγοραστής έχει αποθηκευμένο στον υπολογιστή του ένα χρηματικό ποσό, με την μορφή ψηφιακών μετρητών, που μπορεί να αναγνωριστεί μόνο από ένα συγκεκριμένο πωλητή. Η μεταφορά και η επιβεβαίωση των πληρωμών γίνεται απευθείας στον κόμβο του εμπόρου.

Η κύρια δύναμη του συστήματος Millicent βρίσκεται στην κατασκευή ψηφιακών υπογραφών πολύ χαμηλού κόστους, που δεν εξαρτώνται από δημόσια κλειδιά που πρέπει να είναι διαθέσιμα σε όλους. Το κόστος της διατήρησης ενός κόμβου στο διαδίκτυο για την «είσπραξη» ψηφιακών μετρητών είναι γενικά πολύ μικρό. Επίσης η κλοπή των ψηφιακών μετρητών αυτού του τύπου δεν έχει νόημα, επειδή η αξία κάθε μονάδας (που ονομάζεται scrip-κλάσμα του δολαρίου) είναι μικρή.

Τα μειονεκτήματα του συστήματος είναι δυο. Πρώτον τα ψηφιακά μετρητά ισχύουν μόνο για ένα πωλητή, με τον οποίο ο πελάτης πρέπει να έχει συχνές συναλλαγές. Αν ένας πελάτης χρειάζεται ψηφιακά μετρητά για πολλούς διαφορετικούς προμηθευτές, η χρήση του συστήματος γίνεται ασύμφορη και μπορεί να επιβαρύνει τον ηλεκτρονικό υπολογιστή του. Δεύτερον υπάρχει κίνδυνος κάποιος να παράγει (πλαστογραφήσει) δικά του ψηφιακά μετρητά.

❖ **CAFÉ [www.digicash.com,conditional access for Europe ww.semper.org/sirene/project/cafe]**

Ένα σύστημα ψηφιακών μετρητών που χρησιμοποιεί ειδικές ηλεκτρονικές κάρτες (smart card), που περιέχουν μικροεπεξεργαστή, και παρέχει ισχυρές εγγυήσεις για την ανωνυμία των χρηστών. Υποστηρίζεται από μια Ευρωπαϊκή κοινοπραξία 13 εταίρων, μεταξύ των οποίων η Digicash.

Το πρόγραμμα CAFE βρίσκεται στη φάση της δοκιμαστικής υλοποίησης και το μέλλον του εξαρτάται από τον βαθμό αποδοχής του από τις τράπεζες και τον πολιτικό κόσμο. Περισσότερες λεπτομέρειες δεν είναι προς το παρόν διαθέσιμες, και αυτό ίσως είναι μια ένδειξη ότι το σύστημα πλησιάζει στην ολοκλήρωσή του.

❖ **Mondex [www.mondexusa.com]**

Ένα σύστημα ψηφιακών μετρητών που βασίζεται σε ειδικές ηλεκτρονικές κάρτες (smart card) και απαιτεί προεργασία για τη χρήση του. Οι ψηφιακές κάρτες εξασφαλίζουν μια φορητότητα και ανεξαρτησία από το είδος του ψηφιακού δικτύου, ανάλογη με αυτήν ενός μεταλλικού νομίσματος.

Ουσιαστικά πρόκειται για μια πλαστική κάρτα, που εξωτερικά μοιάζει με μια πιστωτική κάρτα, μπορεί να «φορτωθεί» με ένα χρηματικό ποσό κα να χρησιμοποιηθεί σε διαφορετικές συσκευές είσπραξης.

Η ανεξαρτησία των καρτών αυτών είναι το κυριότερο πλεονέκτημά τους. Η αξία τους είναι αποθηκευμένη μέσα σε αυτές και δεν χρειάζονται έγκριση από κανένα κεντρικό οργανισμό. Είναι ένα πραγματικό ψηφιακό χρήμα και όχι απλά μια επέκταση των πιστωτικών καρτών.

Οι κίνδυνοι είναι ίδιοι με αυτούς των κοινών μετρητών. Αν ο κάτοχος χάσει την κάρτα του, χάνει το χρηματικό ποσό που υπήρχε φορτωμένο σε αυτήν. Όμοια, αν μια κάρτα κλαπεί, το περιεχόμενο περνά στον κλέφτη. Ο κάτοχος έχει την ελευθερία να χρησιμοποιήσει την κάρτα χωρίς να αφήνει ίχνη των συναλλαγών του, και φυσικά μπορεί να την δώσει στο παιδί του χωρίς κανένα πρόβλημα.

❖ **CyberCoin [www.cybercash.com/cybercash/shoppers/coingenpage.]**

Μια τεχνολογία ψηφιακών μετρητών, που μπορεί να χρησιμοποιηθεί για συναλλαγές ελάχιστης αξίας 0.25 δολαρίων. Στηρίζεται στο «ηλεκτρονικό πορτοφόλι» της CyberCash, που έχει αναφερθεί παραπάνω.

Το χρηματικό ποσό με το οποίο «φορτώνεται» το πορτοφόλι δεν μεταφέρεται πραγματικά, αλλά δεσμεύεται από την τράπεζα μέχρι ο πελάτης να πληρώσει για μια αγορά-οπότε μεταφέρεται στον λογαριασμό του πωλητή. Οι συναλλαγές δεν είναι ανώνυμες, ενώ η Cyber Cash αναλαμβάνει την ευθύνη για την παράδοση των προϊόντων. Με τον τρόπο αυτό, το σύστημα μοιάζει πάρα πολύ με τη χρήση υπηρεσιών είσπραξης.

Το κύριο πλεονέκτημα της μεθόδου αυτής είναι η υποστήριξη που βρίσκει στην αγορά. Κορυφαία στελέχη από τον κλάδο της επεξεργασίας συναλλαγών και της κρυπτογράφησης εργάζονται πάνω στο σύστημα CyberCoin.

Η κύρια αδυναμία του είναι η έλλειψη ανωνυμίας. Μοιράζεται επίσης το πρόβλημα όλων των μεθόδων που δεν χρησιμοποιούν τις ειδικές κάρτες smart card, δηλαδή ότι οι πληροφορίες αποθηκεύονται σε ηλεκτρονικούς υπολογιστές και αργά ή γρήγορα μπορεί κάποιος μη εξουσιοδοτημένος να τις αποκρυπτογραφήσει ή να τις χρησιμοποιήσει για παράνομους σκοπούς.

Ηλεκτρονικές επιταγές :

❖ **CheckFree [www.checkfree.com]**

Η εταιρία Checkfree προσφέρει μια μερική λύση για την πραγματοποίηση ηλεκτρονικών πληρωμών. Επικεντρώνεται κυρίως σε άτομα ή επιχειρήσεις που πληρώνουν μηνιαίους λογαριασμούς και επιθυμούν να αυτοματοποιήσουν τις πληρωμές τους. Βασικά είναι μια υπηρεσία πληρωμών που επιτρέπει στους πελάτες της να πληρώνουν τους λογαριασμούς τους μέσα από το διαδίκτυο. Η εταιρία Checkfree είναι συνδεδεμένη με το δίκτυο ηλεκτρονικών συναλλαγών της Αμερικάνικης τράπεζας Federal Reserve Bank και με αρκετούς οργανισμούς πιστωτικών καρτών.

Όταν κάποιος γίνεται πελάτης της Checkfree, πρέπει να δώσει τα στοιχεία ενός τραπεζικού του λογαριασμού. Όλες οι μελλοντικές πληρωμές θα γίνονται από τον λογαριασμό αυτό. Το μόνο που πρέπει πλέον να κάνει ο πελάτης είναι να δηλώσει στην Checkfree (μέσα από το διαδίκτυο) το ποσό και τον αποδέκτη. Το σύστημα της Checkfree μπορεί στη συνέχεια να βρει τον καταλληλότερο τρόπο για την πληρωμή του αποδέκτη (π.χ. ηλεκτρονικά ή με ταχυδρομική επιταγή) και να πραγματοποιήσει την πληρωμή χρεώνοντας το αντίστοιχο ποσό στον λογαριασμό του πελάτη.

Το κύριο πλεονέκτημα του συστήματος Checkfree είναι ότι έχει στενή επικοινωνία με το τραπεζικό σύστημα και είναι εξαιρετικά εύχρηστο. Επίσης χρησιμοποιεί ένα υψηλό επίπεδο κρυπτογράφησης για την ασφαλή μετάδοση των πληροφοριών.

Το πρόβλημα είναι ότι δεν χρησιμοποιεί κοινά αποδεκτά πρότυπα στον τομέα της κρυπτογράφησης και της ασφάλειας. Αυτό αναμένεται να αλλάξει σύντομα, καθώς οι εταιρίες Checkfree και CyberCash έχουν ξεκινήσει από κοινού την ανάπτυξη ενός συμβατού λογισμικού.

❖ **On-line CHECK [www.on-linecheck.com]**

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

❖ **NetCheque** **[www.nii-server.isi.edu/info/NetCheque]**

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

❖ **NetChex** **[www.netchex.com]**

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

❖ **NetBill** **[www.ini.cmu.edu/netbill Carnegie Mellon Univercity]**

Ένα σύστημα ηλεκτρονικών επιταγών που χρησιμοποιεί συμμετρική κρυπτογράφηση (με μυστικό κλειδί) βασισμένη στο σύστημα Kerberos. Η ομάδα του πανεπιστημίου Carnegie Mellon που αναπτύσσει το σύστημα NetBill ενδιαφέρεται κυρίως για την πώληση πληροφοριών μέσα από το δίκτυο. Ένας κεντρικός κόμβος διατηρεί οικονομικές πληροφορίες (λογαριασμούς) των χρηστών.

Όταν ένας χρήστης ενδιαφέρεται να αγοράσει μια πληροφορία στέλνει στον κόμβο μια κρυπτογραφημένη παραγγελία αντίστοιχης αξίας. Μόλις ο κόμβος βεβαιώσει την παραλαβή της παραγγελίας, επιτρέπει την αποκρυπτογράφηση της πληροφορίας.

❖ **CheckMaster** **[www.checkmaster.com]**

Η εταιρία CheckMaster χρησιμοποιεί τη τεχνολογία ActiveX της Microsoft για την ηλεκτρονική έκδοση και την ψηφιακή υπογραφή επιταγών. Το σύστημα λειτουργεί με το λογισμικό MS Money της Microsoft και Quicken της Intuit.

Υπηρεσίες είσπραξης

❖ **TelPay** **[www.telpay.ca]**

Ένα σύστημα που επιτρέπει την πληρωμή λογαριασμών από το διαδίκτυο. Δεν υπάρχουν διαθέσιμες περισσότερες πληροφορίες.

❖ **First Virtual** **[www.fv.com] (First Virtual Holdings)**

Το σύστημα First Virtual προσφέρει ασφαλείς ηλεκτρονικές συναλλαγές με τη χρήση ενός ειδικού αριθμού αναγνώρισης των πελατών, που ονομάζεται VirtualPIN, αντί για αριθμούς πιστωτικών καρτών, οι οποίοι είναι αποθηκευμένοι σε ασφαλείς ηλεκτρονικούς υπολογιστές της First Virtual που δεν είναι συνδεδεμένοι στο διαδίκτυο.

Ο αγοραστής δίνει στον πωλητή τον αριθμό VirtualPIN. Ο πωλητής επικοινωνεί με την First Virtual, η οποία ζητά από τον αγοραστή να επιβεβαιώσει τη συναλλαγή. Τότε μόνο η πιστωτική κάρτα του αγοραστή χρεώνεται με την αξία της αγοράς.

❖ **InterCoin** **[www.intercoin.com]**

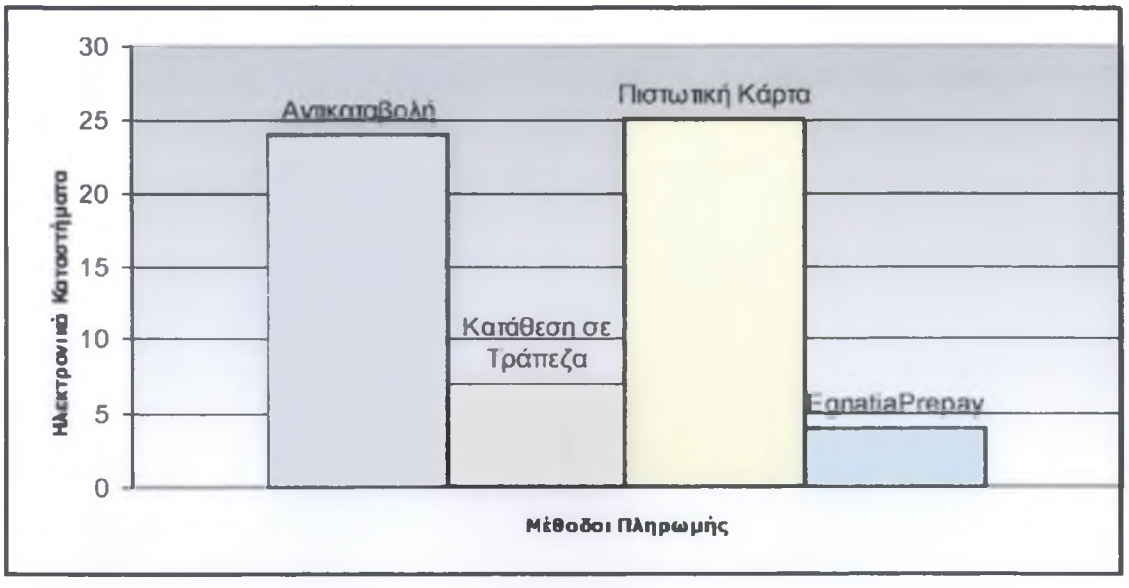
Η εταιρία Intercoin προσφέρει υπηρεσίες ηλεκτρονικής πληρωμής σε μηνιαία βάση. Ο πελάτης μπορεί να πραγματοποιεί αγορές αξίας κάτω των 10 δολαρίων, τις οποίες εξοφλεί συνολικά στο τέλος του μήνα. Το κόστος των συναλλαγών δεν χρεώνεται στον αγοραστή αλλά στον πωλητή. Τα οικονομικά στοιχεία των πελατών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

4.2 ΕΛΛΗΝΙΚΑ ΗΛΕΚΤΡΟΝΙΚΑ ΚΑΤΑΣΤΗΜΑΤΑ ΚΑΙ ΙΣΧΥΟΥΣΕΣ ΜΕΘΟΔΟΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ[38]

Προκειμενου 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 καταστήματα .

Έτσι μετά από πολύχρονες έρευνες όσον αφορά τις επιλογές που προσφέρονταν στους καταναλωτές αναφορικά με τις πληρωμές των προϊόντων και υπηρεσιών που παρέχουν τα διάφορα ηλεκτρονικά καταστήματα μέσω των ιστοσελίδων τους ανακαλύψαμε ότι, 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 των ερευνών ήταν η δημιουργία καλαθιού αγορών προκειμένου να καταστεί εφικτή η πρόσβαση στην ιστοσελίδα όπου προσφέρονταν οι διαθέσιμοι τρόποι πληρωμής.



ΕΙΚΟΝΑ 6 : Διαθέσιμες μέθοδοι πληρωμών στα Ελληνικά ηλεκτρονικά καταστήματα

Όπως φαίνεται και στο παραπάνω σχήμα , που απεικονίζει τα αποτελέσματα των ερευνών, 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 Prepay)

Είναι επίσης προφανές από το σχήμα 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 τονίζεται 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 ότι 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 τα οποία και παρουσιάζονται στην ενότητα. 7

5 ΑΞΙΟΛΟΓΗΣΗ ΚΑΙ ΕΠΙΛΟΓΗ ΤΩΝ ΜΕΘΟΔΩΝ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ [39]

Ο πίνακας που ακολουθεί απαριθμεί μια σειρά από κριτήρια για την αξιολόγηση συστημάτων ηλεκτρονικής πληρωμής (MacKie-Mason & White, 1996). Η επιλογή της καλύτερης μεθόδου ηλεκτρονικής πληρωμής για το ηλεκτρονικό εμπόριο πρέπει να γίνει μετά από μια συστηματική και ορθολογική διαδικασία λήψης απόφασης. Τα κριτήρια είναι τα εξής:

ΕΙΚΟΝΑ 7 : Κριτήρια αξιολόγησης συστημάτων ηλεκτρονικών πληρωμών

Ανταλλαξιμότητα
Χαμηλό πάγιο κόστος (για τον έμπορο)
Πιθανοί περιορισμοί
Αμφίδρομες πληρωμές
Απαίτηση για ειδικό λογισμικό
Μεταφερσιμότητα
Ταχύτητα συναλλαγών
Ανέκκλητες συναλλαγές
Διακριτικότητα
Διαθεσιμότητα σήμερα
Κόστος συναλλαγών για μεγάλες και μικρές επιχειρήσεις
Απαίτηση κρυπτογράφησης για τον αγοραστή και τον πωλητή
Ανωνυμία για τον αγοραστή και τον πωλητή
Κίνδυνος παραποίησης πλαστογράφησης
Ανεξαρτησία από τον τύπο του υπολογιστή
Έλεγχος της ροής της συναλλαγής από τον αγοραστή
Δυνατότητα μαζικής χρήσης
Οικονομικός κίνδυνος για τον αγοραστή και τον πωλητή
Δυνατότητα άμεσης χρήσης των εσόδων σε ηλεκτρονική μορφή

Δυνατότητα λειτουργίας χωρίς σύνδεση
Φορητότητα
Ανάγκη για ύπαρξη τραπεζικού λογαριασμού
Βαθμός αποδοχής από τους χρήστες
Ασφάλεια από πρόσβαση χωρίς εξουσιοδότηση
Ευκολία πρόσβασης
Χρηματική αξία

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

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

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

6 ΣΥΣΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ ΣΤΗΝ ΕΥΡΩΠΑΪΚΗ ΕΝΩΣΗ [40]

Στην Ευρωπαϊκή Ένωση, όπως αναφέρει ο διεθνής ερευνητικός οίκος Forester[41] [*Ensor, B., Torris, T., Fagerström, M. & Martínez, N. (June 2003).*] αναπτύχθηκαν την τελευταία τριετία περίπου 70 συστήματα ηλεκτρονικών πληρωμών. Στην ανάπτυξη και υλοποίηση τους δραστηριοποιήθηκαν κυρίως πιστωτικά ιδρύματα, εταιρίες παροχής υπηρεσιών κινητής τηλεφωνίας και οργανισμοί 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 διαδίκτυο τα τελευταία χρόνια και η διείσδυση του σε ένα πολύ μεγάλο ποσοστό νοικοκυριών, έχει οδηγήσει στη δημιουργία μιας αγοράς 34 εκατομμυρίων καταναλωτών.[42] [*Reitsma, R., Pearce, F. & de Montigny, E. (May 2002*].

- 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 εμπορίου.[43] [*Jennings, R.U., O'Connell, P. & Bradford, N. (September 2001).*]

- 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 τα οποία είναι τα εξής :

- **Έξυπνες κάρτες**
- **Προπληρωμένες κάρτες συναλλαγών**
- **Κινητά πορτοφόλια**
- **Κινητοί λογαριασμοί πληρωμών**
- **Ηλεκτρονικοί λογαριασμοί πληρωμων**

Α) ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ (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 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 μπορεί να γίνεται αυτό, όπως μέσω ATMs ή άλλα τερματικά.

Β) ΠΡΟΠΛΗΡΩΜΕΝΕΣ ΚΑΡΤΕΣ ΣΥΝΑΛΛΑΓΩΝ (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 διακομηστή. 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.

Γ) «ΚΙΝΗΤΑ» ΠΟΡΤΟΦΟΛΙΑ (Mobile wallets)

Τέτοιου είδους συστήματα κινητών πορτοφολιών στην Ευρωπαϊκή αγορά είναι τα Bankpass Mobile και Vodafone's mPay cards τα οποία χρησιμοποιώντας SMS μηνύματα, 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 των 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 της στη χρήση των δικών της συστημάτων. Η Vodafone για παράδειγμα επιτρέπει τη χρήση του συστήματος μόνο στους δικούς της πελάτες.

Δ) «ΚΙΝΗΤΟΙ» ΛΟΓΑΡΙΑΣΜΟΙ ΠΛΗΡΩΜΩΝ (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.

Ε) ΗΛΕΚΤΡΟΝΙΚΟΙ ΛΟΓΑΡΙΑΣΜΟΙ ΠΛΗΡΩΜΩΝ (On line payment accounts)

Τα συστήματα αυτά ανέρχονται σήμερα στα 16 στην Ευρωπαϊκή αγορά και τα πιο διαδομένα 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 στοιχειών 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 τον καταναλωτή για κάθε αγορά του και με προμήθεια 2-3% της αξίας του αγαθού τον 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 παράγοντες[44] [*Ensor, B., Torris, T., Fagerström, M. & Martínez, N. (June 2003).*]

- 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 κα. Ακόμη μόνο το 13% των ευρωπαίων συνδρομητών κινητής τηλεφωνίας υποστήριξε ότι θα ήταν πρόθυμο να προβεί σε αγορές μέσο των κινητών τους τηλεφώνων. Τέλος, πολύ λιγότεροι είναι οι καταναλωτές που χρησιμοποιούν το διαδίκτυο για ηλεκτρονικές αγορές, και συγκεκριμένα στη Βρετανία μόνο το 2% 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 τα μεγέθη από τα οποία αρχίζει η κερδοφορία του. Αυτό συνέβη φυσικά και με τη δημιουργία 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 παρκινγκ των αυτοκινήτων τους σε διάφορους σταθμούς στάθμευσης.

7 ΚΑΙΝΟΤΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ ΣΤΗΝ ΕΛΛΑΔΑ [45]

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 όπως αυτά που αναφέρθηκαν στην ενότητα [3.2] της παρούσας εργασίας. 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 συστήμα πληρωμών μέσω κινητού τηλεφώνου. Ειδικότερα, και με βάση τις πληροφορίες που συλλέχθηκαν αλλά και μέσω έρευνας στον τύπο, τα συστήματα ηλεκτρονικών πληρωμών που υπάρχουν στην Ελλάδα είναι τα ακόλουθα[†].

7.1 EGNATIA PREPAY

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 καταστήματα[46][*www.egnatia.gr]* .

Η πρόσβασή 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 οδηγίες. Για την εγγραφή στη υπηρεσία και την συνεπακόλουθη αγορά της κάρτας απαιτούνται μόνο η εισαγωγή της

[†] 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 είναι η Attica Gift Card VISA που 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.

ηλικίας και του e-mail του ενδιαφερόμενου οπότε διασφαλίζεται η ανωνυμία των συναλλαγών που θα πραγματοποιηθούν μέσω της κάρτας.

Η πληρωμή με χρήση προπληρωμένης 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.

ΕΙΚΟΝΑ 8 : Το πληροφοριακό σύστημα της Εγνατίας Τράπεζας

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.

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.

7.2 ATTICA GIFT CARD VISA

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 δωρηθεί 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 όψή 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 Ελλήνων καταναλωτών έναντι των πληρωμών μέσω διαδικτύου. Η ύπαρξη συγκεκριμένου χρηματικού διαθεσίμου 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 δημοσιεύματα[47] [*Ημερησία, Ένθετο Net Economy, σελ. 155.*] 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.

7.3 ΧΡΥΣΗ ΕΥΚΑΙΡΙΑ-ΑΓΟΡΕΣ ΜΕΣΩ ΚΙΝΗΤΟΥ

Η εφημερίδα αγγελιών Χρυσή Ευκαιρία είναι η πιο δημοφιλής εφημερίδα αγγελιών στην Ελλάδα. Ανήκει σε ένα από τους μεγαλύτερος 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 B2C 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 συγκεκριμενου 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, καλύπτωντας 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 ανεύρευση της κατάλληλης αγγελίας.

Ένα άλλο πρόβλημα που σχετιζόταν με τη χρήση πιστωτικών καρτών ήταν η χρονοβόρα φύση της διαδικασίας πληρωμής καθώς ο αγοραστής θα αναγκαζόνταν 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 υπηρεσίας για τη Χρυσή Αγγελία. Ο μηχανισμός αυτός είναι ειδικά προσαρμοσμένος στο ηλεκτρονικό σύστημα των μικρών αγγελιών και σχετίζεται με την προβολή των στοιχείων επικοινωνίας που πλαισιώνουν κάθε αγγελία [48] [*Presspoint.gr (2002)*]

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.

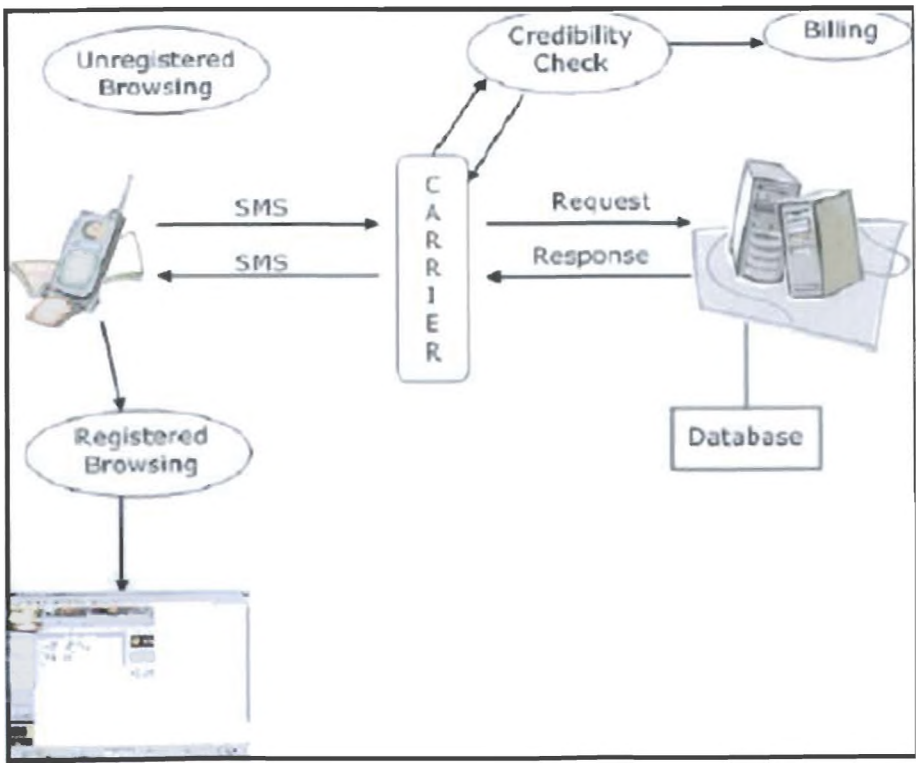
Για να αποκτήσει ο αναγνώστης τον κωδικό αυτό, απαιτείται πληρωμή η οποία όμως δεν ολοκληρώνεται με τη χρήση πιστωτικής κάρτας, αλλά με τη χρήση κινητού τηλεφώνου. Ο χρήστης απλά στέλνει από το κινητό του τηλέφωνο ένα γραπτό μήνυμα SMS με περιεχόμενο ΧΕ στον αριθμό 1450. Στη συνέχεια μόλις το κέντρο μηνυμάτων κάθε εταιρίας παροχής υπηρεσιών κινητής τηλεφωνίας λάβει το μήνυμα του αναγνώστη, 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 .Μέσα σε ένα μήνα απο τη λειτουργία του συστήματος κινητών ηλεκτρονικών πληρωμών, διαπιστώθηκε οτι «αγοράσθηκαν» περίπου 6000 προσωπικοί κωδικοί. Από τους 5.000 ημερίσιους επισκέπτες της ηλεκτρονικής ιστοσελίδας, παρατηρήθηκαν 300 αγορές προσωπικών κωδικών, ποσοστό 6% των ημερίσιων επισκεπτών, για να έχουν πρόσβαση στο προστατευμένο περιεχόμενο.

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



ΕΙΚΟΝΑ 9 : Σύστημα διεξαγωγής πληρωμών EZPay της Χρυσής Ευκαιρίας

8 ΤΟ ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΛΗΡΩΜΕΣ [49]

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 θα 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 διαδικτύου[50] [*www .Ebusiness Forum.*] 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. 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. Σκοπός της ενότητας δεν είναι η εκτενής παρουσίαση και ανάλυση των ισχυουσών νομοθετικών ρυθμίσεων. 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.

8.1 ΕΥΡΩΠΑΪΚΗ ΝΟΜΟΘΕΣΙΑ [51] [http://europa.eu.int]

Η Ευρωπαϊκή Ένωση προχωρά σταδιακά σε μια συντονισμένη προσπάθεια αντιμετώπισης του προβλήματος [52][*www.Ebusiness Forum*] της έλλειψης ξεκάθαρων νομοθετικών ρυθμίσεων που να διέπουν τις ηλεκτρονικές συναλλαγές 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 εμπορίου[53][*European Central Bank (/2002)*].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 on-line 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.

Ακολουθεί συνοπτική παρουσίαση της Ευρωπαϊκής Νομοθεσίας σχετικά με τις ηλεκτρονικές πληρωμές. Στη συνέχεια τα επιμέρους νομοθετήματα παρουσιάζονται και αναλύονται διεξοδικά.

Ευρωπαϊκή Νομοθεσία

- **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 υπηρεσίες 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.

➢ **Κανονισμός (ΕΚ) αριθ. 2560/2001** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 19ης 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 παρόν 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 χρήματος[54] [*Γκόρτσος, Χ. Βλ. (2002)*] 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 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. Στη συγκεκριμένη οδηγία περιλαμβάνονται οι τροποποιήσεις των ορισμών «συνολικό κόστος πίστωσης για τον καταναλωτή» και «συνολικό ετήσιο πραγματικό επιτόκιο».

➢ **Οδηγία 97/5/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου** της 27ης 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 πίστωσης [*Law Net S.A.*] [55] ,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 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 συνολική 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», «νομοθετικώς 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 υπηρεσιών 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 σταστοιχεία 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.

8.2 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.

Τα νομοθετήματα που ρυθμίζουν το νομικό καθεστώς διενέργειας ηλεκτρονικών πληρωμών στην Ελλάδα παρουσιάζονται συνοπτικά στη παράγραφο 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.
- **Πράξη Συμβουλίου Νομισματικής Πολιτικής 52/2003** Τροποποίηση του Κανονισμού Λειτουργίας του Συστήματος Διακανονισμού Εντολών - Πληρωμής σε ευρώ σε Συνεχή Χρόνο ΕΡΜΗΣ ΤΡΑΠΕΖΑ ΤΗΣ ΕΛΛΑΔΟΣ.
- **Πράξη Διοικητή αριθ. 2535/2004** Στατιστική πληροφόρηση της Τράπεζας της Ελλάδος για συναλλαγές μεταξύ κατοίκων Ελλάδος και μη κατοίκων σε ευρώ και σε συνάλλαγμα.
- **Πράξη Διοικητή αριθ. 2536/2004** Προϋποθέσεις παροχής άδειας λειτουργίας και κανόνες εποπτείας από την Τράπεζα της Ελλάδος των εταιρειών διαμεσολάβησης στη μεταφορά κεφαλαίων.
- **Πράξη Διοικητή αριθ. 2527/2003** Κανόνες προληπτικής εποπτείας από την Τράπεζα της Ελλάδος των Ιδρυμάτων Ηλεκτρονικού Χρήματος.
- **Πράξη Διοικητή αριθ. 2526/2003** Σχετικά με τους όρους και προϋποθέσεις παροχής άδειας για ίδρυση πιστωτικού ιδρύματος στην Ελλάδα.
- **Πράξη Διοικητή αριθ. 2495/2002** Τροποποίηση της Μηνιαίας Λογιστικής Κατάστασης που υποβάλλουν τα πιστωτικά ιδρύματα στην Τράπεζα της Ελλάδος (ΠΔ/ΤΕ 2458/1.3.2000).

- **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 σκοπείται 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). Καθώς το περιεχόμενο των Οδηγιών 200/12/ΕΚ και 2000/46/ΕΚ παρουσιάστηκε εκτενώς στην προηγούμενη ενότητα [8.1] δεν θα γίνει περαιτέρωαναφορά στο περιεχόμενο του Νόμου 3148/2003/.

➢ **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". Καθώς το περιεχόμενο της Οδηγίας 97/5/ΕΚ παρουσιάστηκε στην προηγούμενη ενότητα [8.1] δεν θα γίνει περαιτέρω αναφορά στο περιεχόμενο του Π.Δ 33.2000.

➢ **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 μέρους 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 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 ζημίες 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 συναλλασσομένων 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).

➢ **Πράξη Συμβουλίου Νομισματικής Πολιτικής 52/2003** Η παρούσα Πράξη καθορίζει ότι Μέλη του Συστήματος δύνανται να είναι όλα τα νομίμως λειτουργούντα στην Ελλάδα πιστωτικά ιδρύματα, εξαιρουμένων των ιδρυμάτων ηλεκτρονικού χρήματος, είτε εδρεύουν, είτε είναι εγκατεστημένα μέσω υποκαταστήματος στην Ελλάδα ή σε άλλη χώρα του Ευρωπαϊκού.

➢ **Πράξη Διοικητή 2536/2004** Στην Πράξη αυτή ορίζεται ότι Η Τράπεζα της Ελλάδος παρέχει άδεια λειτουργίας σε ανώνυμες εταιρείες, προκειμένου να δραστηριοποιούνται στην παροχή υπηρεσιών διαμεσολάβησης στη μεταφορά κεφαλαίων, εφόσον πληρούνται οι ακόλουθοι όροι και προϋποθέσεις:

α) διαθέτουν ελάχιστο αρχικό μετοχικό κεφάλαιο 150.000 ευρώ.
β) καθ' όλη τη διάρκεια της λειτουργίας των εν λόγω εταιρειών τα ίδια κεφάλαιά δεν επιτρέπεται να υπολείπονται του ως άνω ελαχίστου ορίου.

Οι μεταφορές κεφαλαίων είναι δυνατόν να διενεργούνται χωριστά ή συμψηφιστικά, ανά τακτά χρονικά διαστήματα, μέσω λογαριασμού που τηρεί η εν λόγω εταιρεία σε πιστωτικό ίδρυμα που λειτουργεί στην Ελλάδα και ο οποίος θα κινείται αποκλειστικά με το προϊόν των σχετικών εντολών.

Για τα προς μεταφορά ποσά θα τηρούνται οι διαδικασίες για τη στατιστική ενημέρωση της Τράπεζας της Ελλάδος, σύμφωνα με τις διατάξεις της Π./ΤΕ 2535/2004.Η διαβίβαση από την εταιρεία της εντολής του πελάτη προς τη συνεργαζόμενη επιχείρηση ή τον πράκτορα για τη διάθεση του ποσού στο δικαιούχο πρέπει να πραγματοποιείται την ίδια ημέρα με τη λήψη του σχετικού ποσού από τον εντολέα. Συνοπτικά η Πράξη αυτή ορίζει :

1 Υπό ποιες προϋποθέσεις παρέχεται άδεια λειτουργίας σε εταιρείες διαμεσολάβησης στη μεταφορά κεφαλαίων.
2 Ποιοι είναι οι κανόνες άσκησης της δραστηριότητας διαμεσολάβησης στη μεταφορά κεφαλαίων και πως ενημερώνονται οι συναλλασσόμενοι.

➢ **Πράξη Διοικητή αριθ. 2535/2004** Κατά τη μεταφορά κεφαλαίων από κατοίκους Ελλάδος προς μη κατοίκους, η αξία των οποίων υπερβαίνει το ισότιμο των 12.500 ευρώ, το πιστωτικό ή χρηματοδοτικό ίδρυμα με τη μεσολάβηση του οποίου διενεργείται η συναλλαγή ζητεί από τον κάτοικο Ελλάδος τη δήλωση των ακόλουθων στοιχείων:

- Στοιχεία αιτούντος (ονοματεπώνυμο, διεύθυνση, αριθμός δελτίου ταυτότητος κλπ.) και αντισυμβαλλομένοι δικαιούχου μη κατοίκου.
- Κατηγορία συναλλαγής.
- Χώρα προορισμού των κεφαλαίων ή κατοικίας του αντισυμβαλλόμενου μη κατοίκου.
- Χώρα προέλευσης των αγαθών σε περίπτωση εισαγωγών.
- Αξία και νόμισμα της συναλλαγής.
- Αρχική διάρκεια (μικρότερη / ίση ή μεγαλύτερη του ενός έτους), σε περίπτωση δανείων.
- Είδος αγαθού ΚΣΟ (Κωδικός Συνδυασμένης Ονοματολογίας) προκειμένου για αγορές /εισαγωγές αγαθών εξαιρουμένων εκείνων που προορίζονται για κάλυψη προσωπικών αναγκών.
- ΑΦΜ, σύμφωνα με τις διατάξεις του Π.Δ. 96/93, όπως τροποποιήθηκε με το Ν. 3148/5.6.2003.

Νομικά πρόσωπα, κάτοικοι Ελλάδος, υποχρεούνται να δηλώνουν απευθείας στην Τράπεζα της Ελλάδος (Διεύθυνση Στατιστικής Τομέας Στατιστικής Ισοζυγίου Πληρωμών), σύμφωνα με το συνημμένο υπόδειγμα και τις εκάστοτε τεχνικές οδηγίες της εν λόγω Διεύθυνσης, τα στατιστικά στοιχεία των πάσης φύσεως συναλλαγών ανεξαρτήτως ποσού, τις οποίες διενήργησαν με μη κατοίκους χωρίς τη μεσολάβηση πιστωτικών ή χρηματοδοτικών ιδρυμάτων που λειτουργούν στην Ελλάδα.

➢ **Πράξη Διοικητή αριθ. 2527/2003** Τα Ιδρύματα Ηλεκτρονικού Χρήματος, όπως ορίζονται στην παρ. 16 του άρθρου 2 του Ν. 2076/1992, όπως ισχυει μετά την τροποποίησή του από τον νόμο 3148/2003, υποχρεούνται πριν την έναρξη λειτουργίας τους να υποβάλουν αίτηση προς την Τράπεζα της Ελλάδος για παροχή άδειας ίδρυσης και λειτουργίας, ακολουθώντας τη διαδικασία που προβλέπεται στο κεφ. Α' της ΠΔ/ΤΕ 2526/8.12.2003.

Επίσης υπάρχουν κανόνες προληπτικής εποπτείας που εφαρμόζονται στα Ιδρύματα Ηλεκτρονικού Χρήματος τα οποία αναλαμβάνουν την κάλυψη των κινδύνων κατά την διενέργεια των επενδύσεων. Επιπλέον τα Ιδρύματα Ηλεκτρονικού Χρήματος υποχρεούνται να διαθέτουν σύστημα εσωτερικού ελέγχου, το οποίο θα

διασφαλίζει την αποτελεσματική και ασφαλή λειτουργία των εφαρμογών ηλεκτρονικού χρήματος, κατά τα προβλεπόμενα στην ΠΔ/ΤΕ 2438/1998.

Για την παροχή άδειας ίδρυσης και λειτουργίας υποκαταστήματος Ιδρύματος Ηλεκτρονικού Χρήματος που εδρεύει σε χώρα εκτός του Ε.Ο.Χ. απαιτείται ελάχιστο αρχικό κεφάλαιο ίσο προς το εκάστοτε απαιτούμενο για την ίδρυση Ιδρύματος Ηλεκτρονικού Χρήματος στην Ελλάδα (σήμερα ευρώ 3.000.000).

- **Πράξη Διοικητή αριθ. 2526/2003** Η εν λόγω πράξη ενημερώνει σχετικά με:

1) Ποια είναι η διαδικασία για την παροχή άδειας ίδρυσης και λειτουργίας στην Ελλάδα πιστωτικού ιδρύματος.
2) Ποια είναι η διαδικασία για την παροχή άδειας ίδρυσης υποκαταστήματος στην Ελλάδα πιστωτικού ιδρύματος που εδρεύει σε χώρα εκτός της Ευρωπαϊκής Ένωσης ή σε χώρα που δεν έχει κυρώσει τη Συμφωνία για τον Ε.Ο.Χ.

8.3 ΝΟΜΟΛΟΓΙΑ

- **Άρειος Πάγος 589.2001** : Προστασία καταναλωτών - Ενωση καταναλωτών - Συλλογική αγωγή - Πιστωτική κάρτα - Τηλεφωνική παραγγελία εμπορευμάτων - Απόδειξη συναλλαγής - Βάρος απόδειξης - Αποδεικτικά μέσα.
- **Απόφαση 2319/1999 Εφετείου Αθήνας** Αποστολή περιοδικών σε καταναλωτές, χωρίς προηγούμενη παραγγελία και χρέωση των πιστωτικών τους καρτών που είχε στην διάθεσή του ο εκδότης, από προηγούμενες συναλλαγές.

- **Άρειος Πάγος 589.2001** Σε περίπτωση προβλεπόμενης στη σύμβαση εκδότη πιστωτικής κάρτας και κατόχου αυτής, δυνατότητας του κατόχου της κάρτας να συναλλαγεί με τρίτη συμβεβλημένη επιχείρηση εξ αποστάσεως μέσω τηλεφωνικής παραγγελίας ή δια του διαδικτύου, η εκδότρια της κάρτας τράπεζα έχει το βάρος αποδείξεως της συναλλαγής αυτής, δηλαδή αυτή υποχρεούται ν' αποδείξει ότι ο κάτοχος της κάρτας παρήγγειλε τηλεφωνικώς και έλαβε εμπορεύματα ή υπηρεσίες από τη συμβεβλημένη επιχείρηση.

Αν κατά τους διέποντες τη σχέση τράπεζας και κατόχου κάρτας Γ.Ο.Σ. θεμέλιο ευθύνης της πρώτης είναι μόνο το υπογεγραμμένο από τον κάτοχο της κάρτας δικαιολογητικό, τότε δεν επιτρέπονται προς απόδειξη της συναλλαγής το εμμάρτυρο μέσο. Αντιθέτως επιτρέπεται η χρήση και άλλων αποδεικτικών μέσων που δεν απαγορεύονται από τη σύμβαση με την τράπεζα ή τους Γ.Ο.Σ. της τελευταίας.

Η περιεχόμενη στη σύμβαση μεταξύ εκδότη της κάρτας και συμβεβλημένης επιχειρήσεως δυνατότητα της δεύτερης να επιχειρεί συναλλαγές με κατόχους της κάρτας μέσω τηλεφώνου ή διαδικτύου δεν παρέχει συγχρόνως ανάλογο δικαίωμα στον εκδότη της κάρτας να χρεώνει την τελευταία με χρηματικά ποσά αφορώντας συναλλαγές πραγματοποιούμενες μέσω τηλεφώνου ή διαδικτύου, αν τέτοια δυνατότητα δεν περιλαμβάνεται στη σύμβαση μεταξύ εκδότη της κάρτας και κατόχου της.

Ανάλογη δυνατότητα έχει και η ένωση καταναλωτών, η οποία ασκώντας κατά της τράπεζας-εκδότριας της κάρτας ως προμηθεύτριας συλλογική αγωγή δικαιούται να προβάλει ότι η εφαρμοζόμενη από την τράπεζα τακτική αυτή έναντι απροσδιορίστου αριθμού καταναλωτών - κατόχων κάρτας, δηλαδή της χωρίς προηγούμενο έλεγχο και απόδειξη χρεώσεως των κατόχων κάρτας με χρηματικά ποσά αφορώντας συναλλαγές

που πραγματοποιήθηκαν εξ αποστάσεως με τον διαληφθέντα τρόπο συνιστά παροχή από υπαιτιότητα ελαττωματικών και συνεπώς παρανόμων υπηρεσιών γιατί προκαλούν διασάλευση της δικαιολογημένα προσδοκώμενης ασφάλειας των συναλλαγών και εκθέτουν σε κίνδυνο τα οικονομικά συμφέροντα των καταναλωτών, αφού με τον τρόπο αυτό δημιουργείται ο κίνδυνος χρεώσεως αυτών με χρηματικά ποσά που αφορούν συναλλαγές που δεν αποδεικνύεται ότι έγιναν και τις οποίες η εκδότρια της κάρτας τράπεζα αποδέχθηκε χωρίς να στηριχθεί προς τούτο σε ασφαλή αποδεικτικά στοιχεία, και έτσι ν' αξιώσει την παύση της τακτικής αυτής.

➢ **Απόφαση 2319/1999 Εφετείου Αθήνας** Στην παρούσα απόφαση ενημερωνόμαστε για την αποστολή περιοδικών σε καταναλωτές, χωρίς προηγούμενη παραγγελία και χρέωση των πιστωτικών τους καρτών που είχε στην διάθεσή του ο εκδότης, από προηγούμενες συναλλαγές.

Επίσης γνωρίζοντας ότι είναι παράνομη η χρέωση των πιστωτικών καρτών, υποχρεούται ο εκδότης και οι τράπεζες για την αποζημίωση των καταναλωτών. Μη εφαρμογή, κατά τον κρίσιμο χρόνο, της οδηγίας 97/7/ΕΚ, με την οποία οι χρηματοοικονομικές υπηρεσίες εξαιρούνται από τις προστατευτικές διατάξεις των συμβάσεων από απόσταση λόγω μη ύπαρξης σχετικού εθνικού κανόνα δικαίου.

9 ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ [56]

Σύμφωνα με έρευνα που πραγματοποιήθηκε από τον ΟΟΣΑ στις Σκανδιναβικές χώρες και την Ιαπωνία το 2002 [*OECD 2002, 150-152.*] [57], απεδείχθει 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. 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.

9.1 ΣΥΝΙΣΤΩΣΕΣ ΑΣΦΑΛΕΙΑΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ

Τα γενικά χαρακτηριστικά που αναφέρονται παρακάτω αποτελούν τα συστατικά στοιχεία ασφαλείας που θα πρέπει να έχει ένα σύστημα Ηλεκτρονικών Πληρωμών και Συναλλαγών: [58] [*European Central Bank, (2002)*]

- **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 τους απαραίτητους μηχανισμους 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 συναλλασσομένου 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 επιβάλει 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 ασφάλειας στις συναλλαγές δεν είναι μόνο θέμα

τεχνολογικό, αλλά εντάσσεται στην ευρύτερη στρατηγική ενός οργανισμού εξασφαλίζοντας την αποδοχή αυτού του τρόπου πληρωμών από τους τελικούς καταναλωτές σε συνδυασμό με το χαμηλό κόστος της συναλλαγής.

9.2 ΑΣΦΑΛΕΙΑ ΣΥΝΑΛΛΑΓΩΝ [59]

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 Διαδίκτυο.

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 (http://nemis.cti.gr/ebusiness/www.netscape.com)
- είτε από αυτό της Microsoft (http://nemis.cti.gr/ebusiness/www.microsoft.com).

9.3 ΤΕΧΝΟΛΟΓΙΕΣ ΠΟΥ ΕΞΑΣΦΑΛΙΖΟΥΝ ΥΨΗΛΑ ΕΠΙΠΕΔΑ ΑΣΦΑΛΕΙΑΣ ΣΤΙΣ ΣΥΝΑΛΛΑΓΕΣ [60]

Οι τεχνολογίες που αναφέρονται στην βιβλιογραφία ως κατάλληλες για την επίτευξη υψηλού επιπέδου ασφάλειας στις ηλεκτρονικές συναλλαγές κατατάσσονται σε δύο γενικές κατηγορίες μεθόδων: συμμετρική και ασύμμετρη κρυπτογράφηση.

Η κωδικοποίηση είναι η μετατροπή πληροφορίας σε μορφή μη κατανοητή ή αναγνώσιμη. Σκοπός της είναι να διασφαλίσει το απόρρητο κρατώντας την πληροφορία "κρυμμένη", ακόμα και αν το κωδικοποιημένο κείμενο διαρρεύσει με κάποιον τρόπο σε μη εξουσιοδοτημένους αναγνώστες. Αποκωδικοποίηση είναι η εξαγωγή της πληροφορίας μέσα από το φαινομενικά ακατανόητο κωδικοποιημένο κείμενο. Για την κωδικοποίηση και την αποκωδικοποίηση μιας πληροφορίας είναι απαραίτητη η χρήση μιας μυστικής πληροφορίας που ονομάζεται "κλειδί" και, ανάλογα με το μηχανισμό κρυπτογράφησης, μπορεί να είναι το ίδιο ή διαφορετικό για τις δυο διεργασίες.

Η καθιέρωση της κρυπτογράφησης, λοιπόν, έδωσε τη λύση σε όλα τα προβλήματα μετάδοσης ευαίσθητων πληροφοριών. Επίσης, εκτός από την κωδικοποίηση-αποκωδικοποίηση της πληροφορίας, η κρυπτογράφηση, εισάγει και τη διαρκή πιστοποίηση (authentication) του δημιουργού αλλά και του τελικού αποδέκτη της πληροφορίας. Αποτέλεσμα είναι απλές, καθημερινές διαδικασίες, όπως η υπογραφή ενός κειμένου ως σημάδι γνησιότητας, μπορούν να μεταφερθούν μέσω της κρυπτογράφησης στο ηλεκτρονικό τους αντίστοιχο και να επικυρώσουν αποφάσεις, συμφωνίες, κτλ.

Στη συνέχεια γίνεται αναφορά στις δύο αυτές μεθόδους με σκοπό όχι την παρουσίαση τεχνικών ζητημάτων αλλά στην πληρέστερη κατανόηση βασικών θεμάτων και χαρακτηριστικών ασφαλείας των συστημάτων ηλεκτρονικών πληρωμών.

9.3.1 ΣΥΜΜΕΤΡΙΚΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ

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 μηνυμάτων.

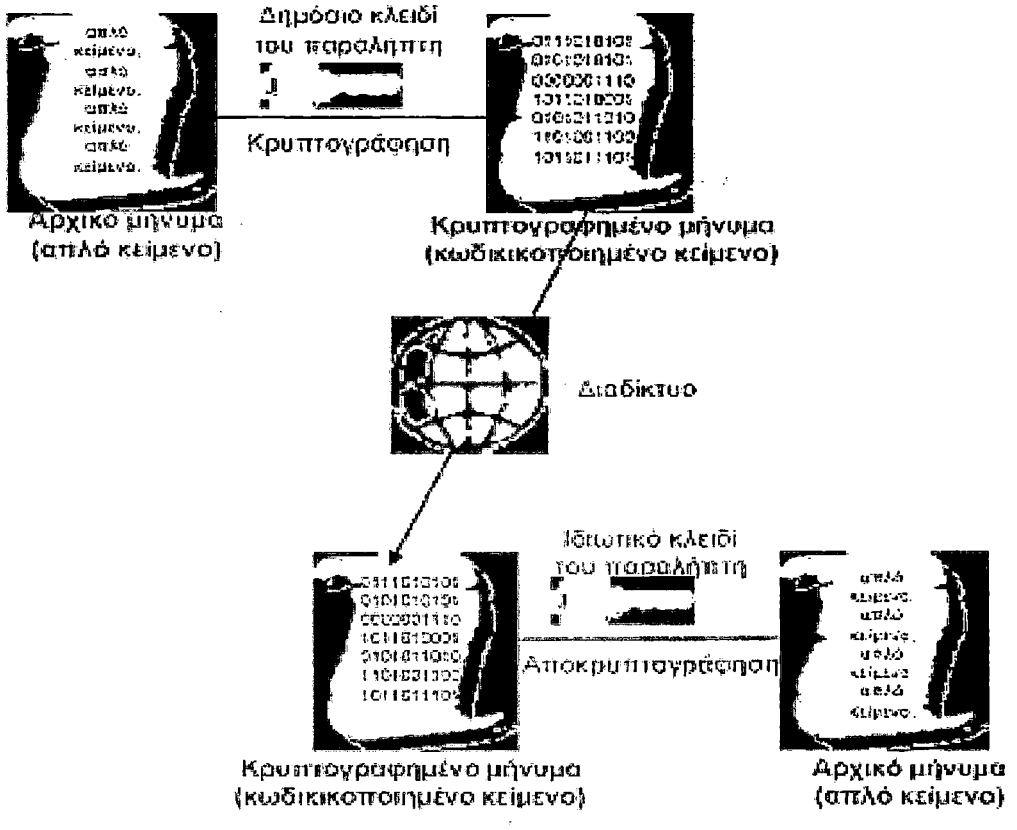
Τα χαρακτηριστικά ασφάλειας, μη αποποίηση ευθύνης, αυθεντικότητα και ακεραιότητα μπορούν να επιτευχθούν με ιδιαίτερη ευκολία μέσω της συμμετρικής κρυπτογράφησης. Τα υπόλοιπα δύο όμως για να επιτευχθούν χρειάζονται την εφαρμογή συμπληρωματικών μεθόδων.

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 ασφάλειας 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.

9.3.2 ΑΣΥΜΜΕΤΡΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ [61]

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 κράτα 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 <u>πλεονέκτημα</u> 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 διαδομένη σε «ανοιχτά» δίκτυα (Open networks).



ΕΙΚΟΝΑ 10 : Κρυπτογράφηση δημοσίου – ιδιωτικού κλειδιού

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 Κρυπτογράφει		Δέκτης Αποκρυπτογράφει	
Ιδιωτικό Κλειδί Αποστολέα	Ακεραιότητα ----------→	**Δημόσιο Κλειδί Αποστολέα**	Ο δέκτης συγκρίνει την περιγραφεί 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	Εμπιστευτικότητα ----------→	Ιδιωτικό Κλειδί Δέκτη	Μόνο ο δέκτης μπορεί να διαβάσει το μήνυμα με το ιδιωτικό του κλειδί

ΕΙΚΟΝΑ 11 : Κρυπτογράφηση Δημοσίου Κλειδιού (Public Key Encryption)

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 εμπιστευτικότητας (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 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 στα 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 ενδιαφερομένου 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).

9.3.3 ΑΣΥΜΜΕΤΡΕΣ ΤΕΧΝΙΚΕΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ [62]

❖ **Secure Socket Layer SSL and Transport Layer Security: TLS**

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 διακομηστή. 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 ασφάλειας , περί της απόδειξης πραγματοποίησης της συναλλαγής (non-repudiation).Η μετεξέλιξη του πρωτοκόλλου επικοινωνίας SSL αναφέρεται να είναι το Transport Layer Security (TLS).

❖ **Συστήματα ασφαλείας που χρησιμοποιούνται για την αγορά μέσω πιστωτικών καρτών:**

Ένα από τα πιο διαδεδομένα συστήματα ασφαλείας στις αγορές μέσω πιστωτικών καρτών αναφέρεται να είναι το SET (Security Electronic Transaction),που βασίζεται στη μέθοδο PKI. Υλοποιήθηκε στις αρχές τις δεκαετίας του 1990 από τις εταιρίες παροχής πιστωτικών καρτών και χρηματοπιστωτικών συναλλαγών VISA και MasterCard. Το SET παρέχει τα ακόλουθα χαρακτηριστικά ασφαλείας: αυθεντικοποιήση, ακεραιότητα, ασφάλεια των δεδομένων από τρίτους και δυνατότητα απόδειξης της συναλλαγής.

Επιπλέον, παρέχει τη 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 ένα 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 διακομηστή της 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 μέσω 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:**

Όπως αναφέρθηκε πιο πάνω, 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, στα οποία σε συνδυασμό με τα ασύρματα δίκτυα επικοινωνίας GPRS και UMTS διευκολύνεται σημαντικά η πραγματοποίηση ηλεκτρονικών πληρωμών.

9.3.4 ΜΕΘΟΔΟΙ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ [63]

Υπάρχουν διάφορες μέθοδοι κρυπτογράφησης, οι οποίες δεν διαφέρουν όσον αφορά στην κεντρική ιδέα αλλά στους αλγορίθμους και τις αρχικές παραδοχές τους.

❖ **DES** (Data Encryption Standrad)

Ο DES ανήκει στην κατηγορία των "Secret Keys", δηλαδή των συμμετρικών αλγορίθμων. Αναπτύχθηκε στις αρχές της δεκαετίας του '70 και καθιερώθηκε επίσημα από την κυβέρνηση των Ηνωμένων Πολιτειών το 1977. Το μέγεθος του κλειδιού του αλγορίθμου είναι 56 bits, κάτι που σημαίνει ότι αν κάποιος θέλει να "σπάσει" την κωδικοποίηση πρέπει να δοκιμάσει 2^{55} διαφορετικά κλειδιά.

Νεότερες τεχνικές που βασίζονται στη διαφορική κρυπτανάλυση δίνουν από υπολογιστικής πλευράς ελαφρώς καλύτερα αποτελέσματα. Την εποχή που καθιερώθηκε ο αλγόριθμος και με βάση τα τότε δεδομένα σε σχέση με τις υπολογιστικές δυνατότητες των υπαρχόντων συστημάτων, ήταν πρακτικά ανέφικτο και

πολυδάπανο να "σπάσει" αυτού του είδους η κρυπτογράφηση σε κάποιο λογικό πλαίσιο χρόνου.

Με τη ραγδαία εξέλιξη των υπολογιστικών συστημάτων κάτι τέτοιο έχει γινει σχετικά εφικτό, ωστόσο εξακολουθεί να είναι πολυέξοδο από την πλευρά της απαιτούμενης υπολογιστικής ισχύος. Μία από τις τελευταίες προσπάθειες "επίθεσης" εναντίον του DES στηρίχτηκε στη "γραμμική κρυπτανάλυση" όπου, κωδικοποιώντας 2^{47} συγκεκριμένες λέξεις, έγινε δυνατό να ανακτηθεί το μυστικό κλειδί ύστερα από υπολογισμούς 50 ημερών σε 12 HP9735, ενώ στις 26 Φεβρουαρίου 1998 παρόμοιο εγχείρημα κατέστη δυνατό μέσα από τη σύνδεση δεκάδων χιλιάδων υπολογιστών μέσω Internet σε 39 ημέρες.

Μια παραλλαγή του DES η οποία χρησιμοποιείται σήμερα είναι ο triple-DES που λογικά είναι πιο αργός, έχοντας όμως μέγεθος κλειδιού 168 bits είναι πρακτικά απίθανο να σπαστεί.

❖ **IDEA** (International Data Encryption Algorithm)

Ο IDEA είναι συμμετρικός αλγόριθμος με μέγεθος κλειδιού 128 bits. Αναπτύχθηκε από τους James L. Massey και Xuejia Lai, ενώ η δημοσίευσή του έγινε το 1990. Από τα θετικά χαρακτηριστικά του είναι ότι "αντιστέκεται" πολύ καλύτερα συγκριτικά με τον DES σε τεχνικές όπως η διαφορική και η γραμμική κρυπτανάλυση.

❖ **RC2**

Το RC2 είναι ένας αλγόριθμος γρηγορότερος από τον DES, ο οποίος έχει σχεδιαστεί ως αντικαταστάτης του. Έχει τη δυνατότητα να χρησιμοποιεί κλειδιά μεταβλητού μεγέθους. Ο αλγόριθμος σχεδιάστηκε από τον Rivest για την RSA Data Security, η δε ονομασία του προέρχεται ή από το "Ron's Code" ή από το "Rivest's Cipher". Η κυβέρνηση των Ηνωμένων Πολιτειών, έπειτα από συμφωνία με την SPA (Software Publishers Association), επιτρέπει την εξαγωγή, μόνο αν το μέγεθος του κλειδιού δεν ξεπερνά τα 40 bits, εκτός από ειδικές περιπτώσεις. Το ίδιο ισχύει και για τον αλγόριθμο RC4

❖ **RSA**

Ο RSA προτάθηκε το 1977 από τους Ron Rivest, Adi Shamir και Leonard Adleman. Είναι από τους πιο δημοφιλείς αλγορίθμους δημοσίου κλειδιού, προσφέροντας τη δυνατότητα κρυπτογράφησης αλλά και πιστοποίησης. Τα δημόσια και τα ιδιωτικά κλειδιά κατασκευάζονται με τη χρήση δύο πολύ μεγάλων πρώτων αριθμών και ο αλγόριθμος στηρίζει τη δύναμή του στη δυσκολία που υπάρχει όσον αφορά στη παραγοντοποίηση.

❖ **DIFFIE – HELLMAN**

Ο Diffie-Hellman αλγόριθμος αναπτύχθηκε περί το 1976 και επιτρέπει σε δύο άτομα να ανταλλάξουν με ασφαλή τρόπο ένα μυστικό κλειδί σε ένα μη ασφαλές μέσο. Ο αλγόριθμος στηρίζεται στο πρόβλημα των διακριτών λογαρίθμων.

Στην αρχική ανάπτυξή του ο αλγόριθμος ήταν ευάλωτος σε αυτό που ονομάστηκε "Επίθεση Ενδιάμεσου Προσώπου" (Middleperson Attack), όπου αν κάποιος είχε τη δυνατότητα να ελέγχει πλήρως τα μηνύματα που ανταλλάσσονται ανάμεσα σε δύο άτομα, μπορούσε να υποκλέψει τα πάντα, εδραιώνοντας δύο

διαφορετικές κωδικοποιημένες κατά τα άλλα επικοινωνίες με τα δύο άκρα. Το 1992 δόθηκε λύση στο πρόβλημα, εισάγοντας ένα αρχικό στάδιο πιστοποίησης πριν από την καθεαυτού διαδικασία, οδηγώντας σε αυτό που ονομάζεται "Authenticated Diffie-Hellman Key Agreement" και χρησιμοποιείται ευρέως σήμερα.

❖ **WORLD WIDE WEB - HTTP**

Έχει ήδη αναφερθεί πως με την άνθηση του ηλεκτρονικού εμπορίου μεγάλο μέρος συναλλαγών γίνεται ηλεκτρονικά. Οι συναλλαγές μπορεί να ποικίλουν από την απλή αγορά ενός προϊόντος μέσω πιστωτικής κάρτας έως εκτενείς τραπεζικές και χρηματιστηριακές συναλλαγές. Οι εκδόσεις των δύο δημοφιλέστερων φυλλομετρητών (webbrowsers) τα τελευταία χρόνια, σε συνδυασμό βέβαια και με το λογισμικό για WebServers, υποστηρίζουν τρόπους κωδικοποίησης των πληροφοριών που ανταλλάσσονται ανάμεσα σε εξυπηρετούμενο (client) και εξυπηρετητή (server).

Το επικρατέστερο πρωτόκολλο είναι το SSL (Secure Socket Layer) και οι διάφορες εκδόσεις του. Το SSL αναπτύχθηκε από την εταιρία Netscape και χρησιμοποιεί τεχνικές δημόσιου κλειδιού στην αρχική επικοινωνία, ώστε να επιτευχθούν οι ακόλουθοι στόχοι:

1 Ο εξυπηρετητής δηλώνει την ταυτότητά του μέσω της ψηφιακής υπογραφής του.

2 Εξυπηρετητής και εξυπηρετούμενος συμφωνούν στη χρήση ενός συγκεκριμένου κλειδιού/ αλγορίθμου, με το οποίο θα κρυπτογραφηθεί το υπόλοιπο της συνομιλίας.

Οι συμμετρικοί αλγόριθμοι κρυπτογράφησης τους οποίους χρησιμοποιεί το SSL είναι συνήθως οι RC2/RC4 για την έκδοση SSL v2, ενώ στην έκδοση SSL v3 υπάρχουν και οι RC4 128bit και Triple DES (όπου αυτοί επιτρέπονται). Η αδυναμία του SSL για τους χρήστες όλων των χωρών εκτός των Ηνωμένων Πολιτειών είναι το μικρό μέγεθος key (40 bits) που χρησιμοποιεί για τη συμμετρική κρυπτογράφηση των δεδομένων. Πέρα από την αντικειμενική ή όχι ανεπάρκεια στη δύναμη της 40-bit κρυπτογράφησης, υπάρχει το δεδομένο ότι για συγκεκριμένες υπηρεσίες υψηλής ασφάλειας και ρίσκου, κυρίως στον τραπεζικό χώρο, δεν γίνονται αποδεκτοί φυλλομετρητές που δεν προσφέρουν 128-bit κωδικοποίηση.

Εκτός του SSL, υπάρχει και η δυνατότητα χρήσης τού πρωτοκόλλου S-HTTP (Secure Hypertext Transfer Protocol), το οποίο αναπτύχθηκε από την Enterprise Integration Technologies (EIT). Οι διαφορές του σε σχέση με το SSL είναι ότι λειτουργεί στο επίπεδο της εφαρμογής αντί για το επίπεδο της μεταφοράς καθώς και το ότι, ενώ στο SSL γίνεται κωδικοποίηση ολόκληρου του διαύλου επικοινωνίας, στο S-HTTP κάθε μήνυμα κωδικοποιείται ξεχωριστά. Το S-HTTP παρέχει τη δυνατότητα καθένα από τα μηνύματα που μεταφέρονται να "υπογράφεται" ψηφιακά και όχι μόνο τα αρχικά μηνύματα κατά τη διάρκεια της πιστοποίησης όπως στο SSL.

❖ **PGP** (Pretty Good Privacy)

Το πρόγραμμα PGP είναι ένα δημοφιλές πακέτο λογισμικού κρυπτογράφησης, που αναπτύχθηκε από την εταιρεία Network Associates και το οποίο συνδυάζει συμμετρική και ασύμμετρη κρυπτογράφηση για να παρέχει μεγαλύτερη ασφάλεια. Επίσης πριν εκκινηθεί η διαδικασία κρυπτογράφησης, τα δεδομένα συμπιέζονται.

Για την κρυπτογράφηση/ αποκρυπτογράφηση χρησιμοποιούνται δυο κλειδιά, ένα κλειδί συνόδου session key και το δημόσιο κλειδί του παραλήπτη. Το κλειδί συνόδου δημιουργείται με τυχαίο τρόπο με βάση την συμπεριφορά του χρήστη. Στη συνέχεια το αρχείο που πρόκειται να αποσταλεί, κρυπτογραφείται με τη μέθοδο της συμμετρικής κρυπτογράφησης με το κλειδί συνόδου και το κλειδί συνόδου είναι αυτό που κρυπτογραφείται με βάση το δημόσιο κλειδί του παραλήπτη. Κατά την αποστολή του μηνύματος αποστέλλεται επίσης και το κρυπτογραφημένο κλειδί συνόδου.

Στον παραλήπτη ακολουθείται η ακριβώς αντίστροφη διαδικασία. Το κλειδί συνόδου αποκρυπτογραφείται με βάση το ιδιωτικό κλειδί του παραλήπτη, το οποίο στη συνέχεια μπορεί να χρησιμοποιηθεί για να αποκρυπτογραφήσει το αρχικό κείμενο.

Συνήθως για την κρυπτογράφηση του κειμένου χρησιμοποιείται το πρότυπο DES ενώ για το κλειδί συνόδου το πρότυπο RSA . Το σύστημα με αυτό τον τρόπο συνδυάζει ευελιξία και ασφάλεια.

Κάποια συνοδευτικά πακέτα του PGP είναι τα:

- **PGPmail :** Για την προστασία των μηνυμάτων ηλεκτρονικού ταχυδρομείου. Συνοδεύεται με plug - in για δημοφιλή προγράμματα ηλεκτρονικού ταχυδρομείου, όπως τα Microsoft Outlook , Netscape Messenger , Eudora
- **PGPdisk :** Για την κρυπτογράφηση αρχείων ή και διαμερίσεων στον σκληρό δίσκο
- **PGPfire :** firewall εφοδιασμένο με την τεχνολογία PGP
- **PGPvpn :** Δημιουργεί εικονικά ιδιωτικά δίκτυα (virtual private networks) με το να επιτρέπει την (κρυπτογραφημένη) ανταλλαγή μηνυμάτων σε συγκεκριμένους παραλήπτες.

9.4 ΣΥΣΤΗΜΑ SET (SECURE ELECTRONIC TRANSACTION)

9.4.1 ΓΕΝΙΚΑ ΓΙΑ ΤΙΣ ΑΣΦΑΛΕΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ ΜΕ ΤΟ ΣΥΣΤΗΜΑ SET [64]

Έως σήμερα αρκετές επιχειρήσεις χρησιμοποιούν συστήματα ηλεκτρονικών συναλλαγών, τα οποία στις περισσότερες περιπτώσεις είναι ασύμβατα μεταξύ τους, ενώ άλλες απέχουν από το ηλεκτρονικό εμπόριο έως ότου σιγουρευτούν ότι υπάρχει ένα ευρύτερα αποδεκτό και εγγυημένα ασφαλές πρότυπο συναλλαγών. Η πιθανότητα για τη δημιουργία ενός τέτοιου προτύπου άρχισε να καθίσταται σημαντική, από το Φεβρουάριο του 1996, όταν η Visa και η Mastercard αποφάσισαν να προβούν στην από κοινού υλοποίησή του. Το SET (Secure Electronics Transaction), όπως ονομάστηκε το νέο πρότυπο, προήλθε από τη συνεργασία κολοσσών στο χώρο της Πληροφορικής, συμπεριλαμβανομένων των GTE, IBM, Microsoft, Netscape και VeriSign. Ορισμένες εξ αυτών είχαν συνεργαστεί με τους δύο μεγάλους χρηματοπιστωτικούς οργανισμούς προτού αυτοί ξεκινήσουν τη μεταξύ τους συνεργασία και, ως εκ τούτου, το SET συγκεντρώνει τα καλύτερα στοιχεία που είχαν προκύψει από τις μέχρι τώρα έρευνες.

Με το SET, δίνεται στο χρήστη ένα ηλεκτρονικό πορτοφόλι (ψηφιακό πιστοποιητικό) και η συναλλαγή διεξάγεται και επαληθεύεται χρησιμοποιώντας ένα συνδυασμό ψηφιακών πιστοποιητικών και ψηφιακών υπογραφών ανάμεσα στον αγοραστή, τον έμπορο και την τράπεζα του αγοραστή με τρόπο που εξασφαλίζει εχεμύθεια και εμπιστευτικότητα. Το SET χρησιμοποιεί το Secure Sockets Layer (SSL - Ασφαλές Επίπεδο Υποδοχής) του Netscape, τη Secure Transaction Technology (STT -

Τεχνολογία Ασφαλών Συναλλαγών) της Microsoft, και το Secure Hypertext Transfer Protocol (S-HTTP - Ασφαλές Πρωτόκολλο Μεταφοράς Υπερκειμένου) του συστήματος Terisa.

Οι στόχοι της ασφάλειας 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.

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.

9.4.2 ΟΡΙΣΜΟΣ ΚΑΙ ΠΡΟΔΙΑΓΡΑΦΕΣ ΣΥΣΤΗΜΑΤΟΣ SET [65]

ΟΡΙΣΜΟΣ

Το SET (Secure Electronic Transaction) είναι ένα πρωτόκολλο εμπορικών συναλλαγών με τη χρήση καρτών σε ανοικτά δίκτυα, το οποίο αναπτύχθηκε από την MasterCard και την Visa σαν μια μέθοδος εξασφάλισης των συναλλαγών με τη χρήση καρτών διαμέσου του διαδικτύου.

Η διαδικασία περιλαμβάνει ένα αριθμό ελέγχων ασφαλείας που πραγματοποιείται με τη χρήση ψηφιακών πιστοποιητικών που χορηγούνται στους εμπλεκόμενους αγοραστές, εμπόρους και τράπεζες.

ΠΡΟΔΙΑΓΡΑΦΕΣ

Το SET έχει δημιουργηθεί βάση συγκεκριμένων προδιαγραφών που προήλθαν από τις απαιτήσεις των επιχειρήσεων και αφορούσαν τις συναλλαγές τους. Αυτές οι προδιαγραφές είναι:

1 Παροχή προστασίας των οικονομικών δεδομένων ή και άλλων που διακινούνται μαζί τους από υποκλοπή.
2 Διασφάλιση της ακεραιότητας των δεδομένων.
3 Παροχή διαδικασιών πιστοποίησης ταυτότητας του κατόχου κάρτας.

4 Παροχή υπηρεσιών πιστοποίησης των εμπόρων που μπορούν να δεχθούν την πληρωμή με τη χρήση τέτοιας μεθόδου, που προκύπτει από τη σχέση τους με κάποιο οικονομικό ίδρυμα παροχής καρτών.

5 Διασφάλιση της χρήσης των καλύτερων τεχνικών ασφάλειας και σχεδίασης συστημάτων για την προστασία όλων των νόμιμα εμπλεκομένων πλευρών.

6 Η δημιουργία ενός πρωτοκόλλου το οποίο να είναι ανεξάρτητο από τους μηχανισμούς ασφάλειας του επιπέδου μεταφοράς χωρίς όμως και να αποτρέπει τη χρήση τους.

7 Να είναι διαλειτουργικό (όλοι οι κύριοι browsers δουλεύουν με όλους τους κύριους servers και οι τελευταίοι με τη σειρά τους δεν θα έχουν πρόβλημα συμβατότητας με τους Payment Gateway Servers).

9.4.3 ΣΥΣΤΑΤΙΚΑ ΣΤΟΙΧΕΙΑ ΣΥΣΤΗΜΑΤΟΣ SET

Τα συστατικά στοιχεία του συστήματος SET είναι τέσσερα και είναι τα παρακάτω:

- **Cardholder Wallet** (Πορτοφόλι Χρήστη Κάρτας)

Είναι ένα προϊόν που χρησιμοποιεί ο καταναλωτής που βρίσκεται on-line και που επιτρέπει την πραγματοποίηση ασφαλών συναλλαγών σε ένα δίκτυο. Το Wallet πρέπει να δημιουργεί μηνύματα που τα αντιλαμβάνονται τα άλλα τρία προϊόντα που απαρτίζουν το SET (Merchant, Payment Gateway, Certificate Authority).

- **Merchant Server** (Server - Έμπορος)

Είναι ένα προϊόν το οποίο τρέχει κάποιος on-line έμπορος για την επεξεργασία των στοιχείων των συναλλαγών και τη διεκπεραίωσή τους. Επικοινωνεί και αυτό με τα άλλα τρία μέρη του SET.

- **Payment Gateway** (Πύλη Πληρωμών)

Είναι το προϊόν που τρέχει κάποιος τρίτος ο οποίος και επεξεργάζεται την πιστοποίηση των εμπόρων και των συναλλαγών (συμπεριλαμβανομένων οδηγιών πληρωμών από κατόχους καρτών). Επιπλέον αλληλεπιδρά και με ιδιωτικά εμπορικά δίκτυα.

- **Certificate Authority** (Υπηρεσία Πιστοποιητικών)

Είναι το τελευταίο από τα συστατικά στοιχεία του SET το οποίο τρέχει μια αρμόδια υπηρεσία έκδοσης και πιστοποίησης ψηφιακών πιστοποιητικών για το σκοπό αυτό και όποτε ζητείται από τα Wallet, Merchant και Payment Gateway πάνω από δημόσια ή ιδιωτικά δίκτυα.

9.4.4 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΣΤΟΙΧΕΙΑ ΣΥΣΤΗΜΑΤΟΣ SET

Το SET σαν πρωτόκολλο έχει ήδη υιοθετηθεί από τράπεζες και οικονομικούς οργανισμούς παγκοσμίως. Παρακάτω παρατίθενται τα χαρακτηριστικά του και μια σύντομη αναφορά στο τι ακριβώς σημαίνουν.

- Ανοιχτές προδιαγραφές

Το SET είναι πρωτόκολλο ανοικτών προδιαγραφών που έχει επιλεγεί παγκοσμίως από μεγάλα χρηματοπιστωτικά ιδρύματα για συναλλαγές με πιστωτικές κάρτες στο διαδίκτυο

- Βιομηχανική Υποστήριξη

Το SET έχει την υποστήριξη των κυριότερων μελών της βιομηχανίας πιστωτικών καρτών όπως οι Visa, MasterCard, American Express και JCB

- Ανεξαρτησία Πλατφόρμας

Το SET έχει σχεδιαστεί να είναι ανεξάρτητο από οποιαδήποτε συγκεκριμένη πλατφόρμα

- Διαλειτουργικότητα

Το SET είναι το μόνο πρωτόκολλο ηλεκτρονικού εμπορίου που σχεδιάστηκε για συνεργασία με πολλαπλά προγράμματα που προέρχονται από διαφορετικούς κατασκευαστές

- Επέκταση της Υπάρχουσας Υποδομής

Το SET επεκτείνει την υπάρχουσα υποδομή πιστωτικών καρτών στο διαδίκτυο

- Δυνατή Ασφάλεια

Το SET χρησιμοποιεί τεχνολογία κρυπτογράφησης για να προστατεύσει ευαίσθητες πληροφορίες από τα αδιάκριτα βλέμματα τρίτων

- Πιστοποίηση

Η τεχνολογία SET πιστοποιεί όλα τα εμπλεκόμενα, σε μια συναλλαγή, μέρη κάνοντας χρήση ψηφιακών πιστοποιητικών

- Περιβάλλον Εμπιστοσύνης

Το SET χρησιμοποιεί ένα ιεραρχικό σχήμα πέντε επιπέδων πιστοποίησης της εγκυρότητας, διασφαλίζοντας ένα περιβάλλον εμπιστοσύνης για το ηλεκτρονικό εμπόριο

- Λύσεις End-to-End

Το SET πιστοποιεί και εγκρίνει όλα τα εμπλεκόμενα μέρη.

9.4.5 ΔΙΑΔΙΚΑΣΙΑ ΣΥΝΑΛΛΑΓΗΣ ΜΕ ΤΟ ΣΥΣΤΗΜΑ SET [66]

Η λειτουργία του SET βασίζεται στην κρυπτογράφηση και τη χρήση ψηφιακών υπογραφών, με σκοπό τη διασφάλιση ότι ένα μήνυμα λαμβάνεται μόνο από τον επιθυμητό παραλήπτη, χωρίς αλλαγές στο περιεχόμενο, ενώ παράλληλα περιέχει στοιχεία που επιτρέπουν την επαλήθευση του αποστολέα του.Το SET χρησιμοποιεί και συμμετρική και ασύμμετρη μέθοδο κρυπτογράφησης, με αποτέλεσμα η διαδικασία της συναλλαγής να γίνεται μεν πιο πολύπλοκη, αλλά και περισσότερο ασφαλής.

Οι εταιρίες Microsoft και Netscape έχουν ήδη ανακοινώσει browsers που θα ενσωματώνουν το πρότυπο SET. Προκειμένου ο χρήστης να πραγματοποιήσει μια ηλεκτρονική συναλλαγή μέσω του WWW, θα χρειάζεται έναν εξ αυτών των browsers και έναν λογαριασμό σε οργανισμό που θα υποστηρίζει το SET. Μέσω του browser ο χρήστης επισκέπτεται το web site που τον ενδιαφέρει, επιλέγει προϊόντα και, με το πάτημα ενός κουμπιού, εκτελείται η παραγγελία του και επαληθεύονται τα στοιχεία που αφορούν στον ίδιο και το λογαριασμό του.

Στο παρασκήνιο, η διαδικασία είναι αρκετά πιο πολύπλοκη και αποτελείται από τα εξής βήματα:

1 Ο πελάτης "ανοίγει" έναν λογαριασμό, ο οποίος μπορεί να είναι τραπεζικός, με πιστωτική κάρτα ή με κάποιο πιο σύγχρονο σύστημα πληρωμών, όπως για παράδειγμα το DigiCash. Το τελευταίο επιτρέπει στο χρήστη να μετατρέψει πραγματικό χρήμα σε άυλο. Ο λογαριασμός θα είναι με κάποιο χρηματοπιστωτικό οργανισμό, όπως η Mastercard και η Visa, ο οποίος θα υποστηρίζει το SET και στο εξής θα αναφέρεται ως Τράπεζα.

2 Ο πελάτης λαμβάνει ένα πιστοποιητικό. Με το άνοιγμα του λογαριασμού στην Τράπεζα, ο πελάτης λαμβάνει ένα ηλεκτρονικό αρχείο, το οποίο θα αναφέρεται ως Πιστοποιητικό και λειτουργεί ως πιστωτική κάρτα για on-line αγορές. Το αρχείο αυτό περιέχει πληροφορίες για τον πελάτη, συμπεριλαμβανομένου του δημόσιου κλειδιού. Το πιστοποιητικό έχει μια ημερομηνία λήξης και μια ηλεκτρονική υπογραφή της τράπεζας η οποία εξασφαλίζει την πιστότητά του.

3 Οι έμποροι έχουν τα δικά τους πιστοποιητικά. Κάθε έμπορος που συναλλάσσεται με την Τράπεζα διαθέτει Πιστοποιητικό, στο οποίο περιλαμβάνεται το δικό του δημόσιο κλειδί και το δημόσιο κλειδί της Τράπεζας. Το κλειδί αυτό διαθέτει επίσης ημερομηνία λήξεως και είναι υπογεγραμμένο ηλεκτρονικά προκειμένου να εξασφαλίζεται η πιστότητά του.

4 Ο πελάτης κάνει μια παραγγελία. Με τη χρήση ηλεκτρονικού ταχυδρομείου ή μέσω μιας web σελίδας, ο έμπορος ενημερώνεται σχετικά με τα προϊόντα ή τις υπηρεσίες που θέλει να αγοράσει ο πελάτης. Από τη στιγμή που θα δοθεί η εντολή αγοράς, συμβαίνουν τα εξής:

α) Ο browser λαμβάνει ένα αντίγραφο του Πιστοποιητικού του εμπόρου, γεγονός που εξασφαλίζει ότι το κατάστημα είναι διαπιστευμένο από την Τράπεζα. Ο πελάτης βλέποντας το πιστοποιητικό, εξασφαλίζεται ότι ο έμπορος είναι αυτός που υποστηρίζει ότι είναι, καθώς και ότι έχει το δικαίωμα να εκτελεί συναλλαγές

β) Ο browser στέλνει στον έμπορο την παραγγελία, η οποία είναι κρυπτογραφημένη με το δημόσιο κλειδί του εμπόρου, ώστε να είναι αναγνώσιμη μόνο

από αυτόν, την πληροφορία που αφορά στην πληρωμή, η οποία είναι κρυπτογραφημένη με το δημόσιο κλειδί της Τράπεζας και επομένως ο έμπορος δεν μπορεί να δει την πληροφορία αυτή, και, τέλος, έναν κωδικό που συνθέτει στοιχεία της παραγγελίας και της πληρωμής, προκειμένου να είναι σίγουρο ότι υπάρχει αντιστοιχία μεταξύ των δύο

5 Ο έμπορος λαμβάνει την παραγγελία και ελέγχει τα προϊόντα που έχει παραγγείλει ο πελάτης και την ηλεκτρονική υπογραφή του.

6 Ο έμπορος επαληθεύει την ταυτότητα του πελάτη, χρησιμοποιώντας την Τράπεζα ή κάποιον τρίτο οργανισμό (VeriSign, Nortel) που έχει πληροφορίες για την αξιοπιστία του. Η διαδικασία αυτή είναι αντίστοιχη με την επαλήθευση της πιστωτικής κάρτας σας σε ένα κατάστημα. Αφού γίνει η επαλήθευση ο έμπορος στέλνει στον πελάτη ένα μήνυμα, προκειμένου να τον ενημερώσει ότι η παραγγελία έχει ληφθεί.

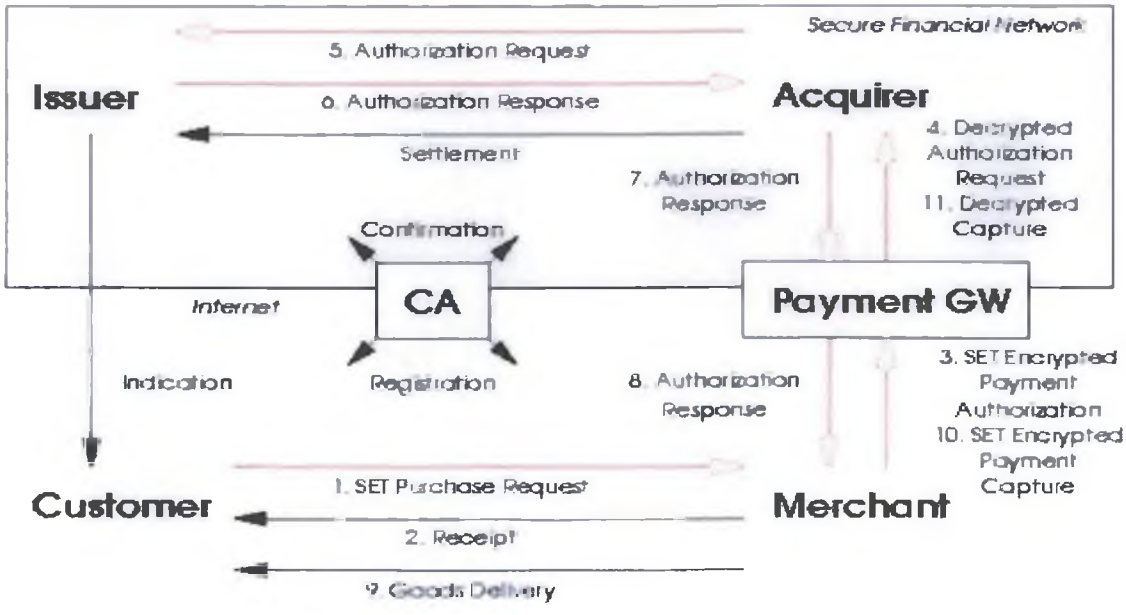
7 Ο έμπορος στέλνει την πληρωμή στην Τράπεζα, χρησιμοποιώντας το δημόσιο κλειδί που έχει στην κατοχή του. Το μήνυμα προς την Τράπεζα εκτός από τις πληροφορίες πληρωμής περιλαμβάνει και το Πιστοποιητικό του εμπόρου.

8 Η Τράπεζα ελέγχει τον έμπορο και το μήνυμα. Το λογισμικό της Τράπεζας ελέγχει πρώτα το αν ο έμπορος είναι εξουσιοδοτημένος και στη συνέχεια, μέσω της ηλεκτρονικής υπογραφής του μηνύματος, ελέγχει την αξιοπιστία του.

9 Η Τράπεζα ελέγχει την πληρωμή και παράλληλα ελέγχει ότι το συγκεκριμένο μήνυμα αφορά στον συγκεκριμένο έμπορο και τη συγκεκριμένη παραγγελία.

10 Η πληρωμή εγκρίνεται από την Τράπεζα και ένα κρυπτογραφημένο μήνυμα αποστέλλεται στον έμπορο, ο οποίος μπορεί πλέον να στείλει τα προϊόντα.

Η διαδικασία των συναλλαγών φαίνεται και στο σχήμα που ακολουθεί :



ΕΙΚΟΝΑ 12 : Διαδικασία συναλλαγής πληρωμής με το SET

9.5 ΣΥΣΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ ΣΤΙΣ ΧΩΡΕΣ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ [67]

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 Regulierungsbehorde fur 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 μίας 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 προσεχτικά 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.

10 ΔΙΑΠΙΣΤΩΣΕΙΣ ΓΙΑ ΤΑ ΣΥΣΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ ΣΤΗΝ ΕΛΛΑΔΑ [68]

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 διάφορων ερευνών 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, όπως αυτή συγκεντρώθηκε κατά την βιβλιογραφική επισκόπηση στις διαβουλεύσεις των διαφόρων ερευνών, καταλήγουμε σε μια σειρά διαπιστώσεων που σκιαγραφούν λεπτομερώς την ελληνική πραγματικότητα και ερμηνεύουν σε μεγάλο βαθμό την περιορισμένη διάδοση των ηλεκτρονικών πληρωμών στην χώρα μας.

- **<u>Απουσία περιεχομένου για πώληση</u>:**

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.

- **<u>Απουσία κρίσιμου μεγέθους που θα προσελκύσει επενδύσεις:</u>**

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 καθώς τόσο η περίοδος αποπληρωμής όσο και το όφελος από μια τέτοια επένδυση 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.

- **<u>Διατήρηση συναλλακτικών ηθών που δεν επιτρέπουν την δημιουργία συστημάτων ηλεκτρονικών αγορών</u>:**

Στα πλαίσια της διαβούλευσης πολλοί εκ των παρευρισκομένων τόνισαν ότι η ύπαρξη επιτυχημένων συστημάτων ηλεκτρονικών πληρωμών για τις συναλλαγές μεταξύ εταιρειών (B2B) θα δημιουργούσε τις απαραίτητες προϋποθέσεις για την περαιτέρω εξάπλωση και υιοθέτηση των συστημάτων αυτών και από τους καταναλωτές. 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.

- **<u>Εκπαίδευση καταναλωτών στη χρήση συστημάτων ηλεκτρονικών πληρωμών:</u>**

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%).

- **<u>Ανάγκη προσέγγισης καταναλωτών νεαρών ηλικιακών ομάδων</u>:**

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 κινητήριο 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.

- **<u>Κατακερματισμός της τραπεζικής αγοράς στην Ελλάδα:</u>**

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. Χαρακτηριστικός είναι ο τρόπος με τον οποίον έχουν οργανωθεί οι ηλεκτρονικές πληρωμές στην Πορτογαλία. Σε αυτή τη χώρα, οι ηλεκτρονικές πληρωμές είναι κεντρικοποιημένες και ελέγχονται από το διατραπεζικό σύστημα της χώρας. Ο πελάτης βλέπει μια κοινή διεπαφή 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 κεντρικοποιημένες 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 εξυπηρέτηση 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.

11 ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΤΑ ΣΥΣΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ [69]

11.1 ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΤΗΝ ΠΟΛΙΤΕΙΑ

Η βασική άποψη που επικρατεί είναι ότι η Πολιτεία έχει να διαδραματίσει ιδιαίτερα σημαντικό ρόλο στην ανάπτυξη και υιοθέτηση συστημάτων ηλεκτρονικών πληρωμών. Για το λόγο αυτό οι ενέργειες στις οποίες οφείλει η Πολιτεία να προβεί εφόσον επιθυμεί να προωθήσει τις ηλεκτρονικές πληρωμές στην Ελλάδα είναι οι εξης:

- **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 των

εκσυγχρονισμό των ηθών στο εμπόριο κατά τρόπο τέτοιο που να μην υπάρχουν εμπόδια στην περαιτέρω ψηφιοποίησης τους.

11.2 ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΤΙΣ ΤΡΑΠΕΖΕΣ ΚΑΙ ΤΙΣ ΕΤΑΙΡΙΕΣ

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, οι προτάσεις για τις τράπεζες και τις εταιρίες είναι οι εξής:

- **<u>Ενημέρωση του καταναλωτικού κοινού</u>:**

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.

- **<u>Προώθηση της ΔΙΑΣ Α.Ε.:</u>**

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 προώθηση 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.

12 ΠΑΡΑΔΕΙΓΜΑΤΑ ΣΥΣΤΗΜΑΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ [70]

12.1 ΠΑΡΑΔΕΙΓΜΑ Α – ΜΟΝΤΕΛΟ EBPP

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

❖ **Ηλεκτρονική παρουσίαση και πληρωμή λογαριασμών**

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

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

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

❖ **Μπορούμε να έχουμε παντού ηλεκτρονικούς λογαριασμούς**

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

Αν πάρουμε, για παράδειγμα, τις τηλεπικοινωνίες, όλες οι εγγραφές που αφορούν στις χρεώσεις των υπηρεσιών γίνονται και τηρούνται ηλεκτρονικά. Κάθε τηλεφώνημα δημιουργεί μία εγγραφή στο σύστημα χρεώσεων της τηλεπικοινωνιακής εταιρίας. Η άθροιση των εγγραφών για ένα τηλεφωνικό αριθμό ή μία ομάδα αριθμών σε συγκεκριμένη χρονική περίοδο δημιουργεί το λογαριασμό τηλεπικοινωνιακών

τελών που μας αποστέλλει η αντίστοιχη εταιρία. Κατά συνέπεια, τα δεδομένα του λογαριασμού υπάρχουν ήδη ηλεκτρονικά, τόσο στην παραπάνω όσο και στη μεγάλη πλειονότητα των συναλλαγών μας. Με τα σύγχρονα συστήματα λογιστηρίου και τα προγράμματα ERP, κάθε συναλλαγή -ηλεκτρονική ή μη- παράγει ηλεκτρονικές εγγραφές, από τις οποίες μπορούμε να εκδώσουμε τόσο έντυπους όσο και ηλεκτρονικούς λογαριασμούς.

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

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

❖ Τα επιχειρηματικά μοντέλα του EBRP

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

❖ Consolidation model

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

Το ρόλο του CSP μπορούν να παίξουν Internet Service Providers (Εταιρίες Παροχής Υπηρεσιών διαδικτύου), portals (δικτυακές πύλες), χρηματοοικονομικά ιδρύματα, e-marketplaces, κ.λπ. Επικρατέστερα πάντως στην ελληνική αγορά για το ρόλο του CSP παρουσιάζονται τα web banking sites των τραπεζών, που διαθέτουν τις

κατάλληλες υποδομές και δημιουργούν τις απαραίτητες συνθήκες για ενσωμάτωση των διαδικασιών πληρωμών.

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

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

❖ **Γιατί να χρησιμοποιήσουμε το EBRP**

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

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

- Κόστη
  Κόστος λογαριασμού €0,018
  Κόστος φακέλου €0,035
  Κόστος εκτύπωσης €0,043
  Κόστος ταχυδρομείου €0,088
  Διαχείριση €0,035
  Αναλώσιμα εκτυπωτή €0,25
  Συντήρηση εκτυπωτή €0,009

Παρόλο που αθροιζόμενα τα παραπάνω κόστη δεν αποτελούν ευκαταφρόνητο ποσό ανά λογαριασμό, οι περιορισμοί της ελληνικής νομοθεσίας που αναφέραμε παραπάνω μειώνουν σημαντικά τα οφέλη, καθώς, όπως και νά 'χει, πρέπει να στείλουμε τουλάχιστον μία έντυπη σελίδα. Ωστόσο δεν καταργούνται τα οφέλη από το EBPP, καθώς μπορούμε να στείλουμε στους πελάτες μας μόνο μία σελίδα και όχι ανάλυση του λογαριασμού (η ανάλυση μπορεί να παρέχεται ηλεκτρονικά), εξοικονομώντας σε χαρτί, εκτύπωση, διαχείριση και ταχυδρομικά.

Είναι χαρακτηριστικό ότι ο τηλεπικοινωνιακός λογαριασμός μιας μεγάλης εταιρίας μπορεί να αποτελείται από δεκάδες σελίδες με ανάλυση των κλήσεων. Η εκτύπωση και αποστολή αυτού του μικρού βιβλίου κοστίζει αρκετά στην τηλεπικοινωνιακή εταιρία, ενώ και ο πελάτης που το λαμβάνει δεν μπορεί ουσιαστικά να το διαχειριστεί, καθώς κανένας συνδρομητής δεν πληκτρολογεί τα δεδομένα για να επαληθεύσει το πληρωτέο ποσό! Επίσης, ο εκδότης του λογαριασμού έχει όφελος και από τη διαδικασία πληρωμής του, αφού με την ηλεκτρονική πληρωμή γίνονται όλα πιο άμεσα και πιο οικονομικά γι' αυτόν.

❖ **Οφέλη για τους πελάτες:**

Ανεξάρτητα από το μοντέλο EBPP, οι πελάτες κερδίζουν ως προς το ότι χρησιμοποιούν ένα μέσο (το διαδίκτυο) για να διαχειρίζονται τους λογαριασμούς τους. Επίσης, οι ηλεκτρονικοί λογαριασμοί τούς προσφέρουν μεγάλη ευελιξία στην επεξεργασία του περιεχομένου τους. Το παράδειγμα του τηλεπικοινωνιακού λογαριασμού που αναφέραμε παραπάνω είναι χαρακτηριστικό: με όλα τα δεδομένα των κλήσεων να είναι διαθέσιμα ηλεκτρονικά, ο πελάτης μπορεί εύκολα να κάνει επεξεργασία και να βγάλει χρήσιμα γι' αυτόν συμπεράσματα σχετικά με τις κλήσεις του.

❖ **Ολοκλήρωση των ηλεκτρονικών συναλλαγών:**

Το EBPP προσφέρει πολλά σε κάθε είδους συναλλαγή, στην περίπτωση όμως των ηλεκτρονικών, αποτελεί αναπόσπαστο μέρος, καθώς θα ήταν τουλάχιστον ανώφελο να γίνεται μία πώληση ηλεκτρονικά και ο λογαριασμός να αποστέλλεται και να εξοφλείται με άλλο, μη ηλεκτρονικό τρόπο. Έτσι, καθώς θα αυξάνονται οι ηλεκτρονικές συναλλαγές, και ιδιαίτερα αυτές που αφορούν το B2B, το EBPP θα χρησιμοποιείται όλο και περισσότερο, αποδεικνύοντας τα αναμφισβήτητα πλεονεκτήματά του.

❖ **Προστιθέμενη αξία προς τον πελάτη:**

Το EBPP προσφέρει στους εκδότες των λογαριασμών τη δυνατότητα να κάνουν πιο εύκολα προωθητικές ενέργειες και ενέργειες marketing προς τους πελάτες τους, ανάλογα με την κατηγορία των τελευταίων. Στους έντυπους λογαριασμούς είναι πολύ δύσκολο να συμπεριλάβουμε πολλά διαφορετικά φυλλάδια και να τα αποστείλουμε σε συγκεκριμένους πελάτες.

Στους ηλεκτρονικούς λογαριασμούς, όμως, μπορούμε να επιτύχουμε ακόμα και προσωπική προσέγγιση στον κάθε πελάτη μας. Επίσης, το EBPP αποτελεί μέρος ενός αποτελεσματικού customer service. Στο χαρτί μπορούμε να συμπεριλάβουμε λίγα στοιχεία ανάλυσης για το λογαριασμό. Αντίθετα, στην ηλεκτρονική του μορφή μπορούμε να έχουμε επαρκέστατη ανάλυση, μειώνοντας τις περιπτώσεις κλήσεων από πελάτες για παροχή διευκρινίσεων και, βέβαια, παρέχοντάς τους ποιοτικότερες υπηρεσίες.

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

❖ **Επιχειρηματικό πλάνο για επιτυχημένο EBRP**

Για κάθε επιχείρηση που θέλει να λέγεται σοβαρή, πριν από την τελική απόφαση για την είσοδο σε μια νέα δραστηριότητα, απαραίτητη θεωρείται η κατάρτιση ενός επιχειρηματικού πλάνου (του γνωστού business plan).

Ένα σωστά σχεδιασμένο, δομημένο και φυσικά ρεαλιστικό επιχειρηματικό πλάνο θα καθορίσει αν μια νέα επιχειρηματική δραστηριότητα είναι κατάλληλη για τη φιλοσοφία της επιχείρησης, εφικτή, επιχειρηματικά αξιοποιήσιμη και, κατ' επέκταση, κερδοφόρα.Το επιχειρηματικό πλάνο ουσιαστικά εκπαιδεύει τη διοίκηση

και αποτελεί ένα εργαλείο που χρησιμοποιείται για την όσο το δυνατόν ρεαλιστικότερη αποτίμηση ενός έργου.

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

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

❖ **Στρατηγική και στόχοι**

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

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

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

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

Σημαντική, στην παρούσα φάση, είναι και η ανάπτυξη μιας ευέλικτης προσέγγισης στο EBPP, ειδικά στα αρχικά στάδια εξέλιξης. Η κατανόηση των αγοραστικών τάσεων θα βοηθήσει στο σχεδιασμό μιας εφαρμογής που θα μπορέσει να ενσωματώσει και να εκμεταλλευθεί τις πρωτοπορίες που υπάρχουν στην αγορά.

Επίσης, σημαντική είναι η κατανόηση των εσωτερικών διαδικασιών και η αξιολόγηση των επιπτώσεων από την εφαρμογή του EBPP. Συγκεκριμένα, θα πρέπει να απαντηθούν τα παρακάτω:

- Η EBPP δραστηριότητα θα τονώσει τη χρηματορροή;

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

❖ **Ανάλυση αγοράς**

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

- Μπορεί το EBPP να βελτιώσει τη "μεταφορά" σχετικών με τα προϊόντα πληροφοριών στους πελάτες;
- Προσφέρει η εγκατάσταση μιας τέτοιας λύσης αυξημένες δυνατότητες παροχής υπηρεσιών σε όσους από αυτούς θεωρούνται καλοί;
- Μπορεί το EBPP να τους προσφέρει μια εύχρηστη λύση αυτοεξυπηρέτησης;
- Μπορούν οι πελάτες: να έχουν πρόσβαση στο ιστορικό των πληρωμών τους, να αμφισβητήσουν ή να καθορίσουν μια πληρωμή, να αλλάξουν διεύθυνση ή τα δεδομένα για μια άμεση πληρωμή;

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

❖ **Οικονομική ανάλυση**

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

Έσοδα

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

Έξοδα

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

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

❖ **Αποτίμηση κινδύνου**

Όταν η επιχείρηση αξιολογεί μια δραστηριότητα που σχετίζεται με την ενσωμάτωση μιας νέας τεχνολογίας, θα πρέπει να είναι σε θέση να αποτιμήσει, όσο το δυνατόν αντικειμενικότερα, και το σχετικό ρίσκο, τόσο για το ενδεχόμενο υιοθέτησης όσο και για το ενδεχόμενο μη υιοθέτησής της.

Κίνδυνοι από την υιοθέτηση

- Ελαττωματική λειτουργική διαδικασία.
- Στροφή της αγοράς σε διαφορετική κατεύθυνση.
- Απόκλιση των εσόδων ή των εξόδων από τις αρχικές εκτιμήσεις.
- Πιθανότητα για αυξημένη απάτη.
- Πιθανότητα μη αποδοχής της λύσης μετά την εγκατάσταση.
- Το κόστος σε χαμένους πελάτες και χρήματα, αν δεν τηρηθούν τα χρονοδιαγράμματα υλοποίησης της λύσης.

Κίνδυνοι από τη μη υιοθέτηση

- Απώλεια πελατών.
- Δημιουργία ανταγωνιστικού μειονεκτήματος.
- Ελάττωση του μεριδίου αγοράς.
- Κλιμάκωση των τρεχόντων εξόδων και συρρίκνωση των περιθωρίων κέρδους.

❖ **Λύσεις στην ελληνική αγορά**

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

- **Lykos Paperless Solutions,** [http://www.lps.gr/]

Η εταιρία έχει προσαρμόσει αλλά και αναπτύξει το λογισμικό της αμερικανικής Checkfree Corporation, μιας από τις σημαντικότερες πλατφόρμες ηλεκτρονικής χρέωσης (e-billing) σε παγκόσμιο επίπεδο, με αποτέλεσμα σήμερα η

εταιρία να διαθέτει ένα ολοκληρωμένο πακέτο υπηρεσιών EBPP προσαρμοσμένο στις ανάγκες της ελληνικής αγοράς.

Ο κεντρικός κόμβος (Consolidation Center) μπορεί να υποδεχθεί πολλαπλές εφαρμογές και να υποστηρίξει όλους τους εμπλεκόμενους φορείς (Billers, Τράπεζες, Customer Service Providers). Ταυτόχρονα παρέχει στον κάθε φορέα την ευχέρεια να χτίσει το δικό του ανταγωνιστικό πλεονέκτημα με εξατομικευμένη πληροφορία προς τον τελικό καταναλωτή.

Ειδικά για τις τράπεζες το EBPP είναι η ευκαιρία να αναδείξουν τον ηγετικό τους ρόλο στις νέες τεχνολογίες και να αποκτήσουν τη θέση που τους αρμόζει στις ηλεκτρονικές πληρωμές λογαριασμών. Είναι ένα σημαντικό εργαλείο για να αναπτύξουν έσοδα και πελάτες.

- **Exodus**, [http://www.exodus.gr/]

Χαρακτηριστική στο χώρο των ηλεκτρονικών πληρωμών είναι η εφαρμογή e.Payments της εταιρίας Exodus, η οποία έχει υιοθετηθεί από την Τράπεζα Πειραιώς και αφορά στην ηλεκτρονική εκκαθάριση συναλλαγών με πιστωτική κάρτα.

Συγκεκριμένα, το σύστημα πληρωμών της εφαρμογής e.Payments υποστηρίζει ασφαλείς ηλεκτρονικές πληρωμές από τον πελάτη με τη χρήση πιστωτικής κάρτας, παρέχοντας στις επιχειρήσεις τη δυνατότητα απάντησης στον πελάτη σε πραγματικό χρόνο, για την έγκριση ή απόρριψη της συναλλαγής. Παράλληλα, ενημερώνει για κάθε συναλλαγή ημέρας ή συγκεκριμένης χρονικής περιόδου με συγκεντρωτικούς και αναλυτικούς πίνακες.

12.2 ΠΑΡΑΔΕΙΓΜΑ Β – ΠΡΑΓΜΑΤΙΚΟ ΠΑΡΑΔΕΙΓΜΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΠΛΗΡΩΜΗΣ [71]

Είναι ευκολότερο να κατανοηθεί η διαδικασία μιας ηλεκτρονικής πληρωμής με τη χρήση ενός παραδείγματος βήμα προς βήμα.

Έστω ότι το ψηφιακό χρήμα πρόκειται να διατεθεί από μια τράπεζα και να χρησιμοποιηθεί σε συναλλαγές πραγματικού χρόνου ανάμεσα στην Alice, μια πελάτισσα και τον Bob, έναν έμπορο. Σε μια συναλλαγή πραγματικού χρόνου η Alice αγοράζει πληροφορία (λογισμικό, νέα, τέχνη, το δικαίωμα να βλέπει μια web σελίδα) on-line. Μπορεί να παρεμβάλλονται δευτερόλεπτα μόνο ανάμεσα στην προσφορά πληρωμής της Alice και στην προσδοκία της να παραδώσει τα αγαθά ο Bob.

Ο Bob πρέπει να επιβεβαιώσει την εγκυρότητα της πληρωμής της Alice αμέσως ή να δεχτεί το ρίσκο ότι μπορεί να κάνει ελάχιστα αν η Alice τον εξαπάτησε. Μια Internet συναλλαγή μπορεί φυσικά να πάρει πολλές άλλες μορφές οι οποίες και αναφέρονται περιστασιακά στα επόμενα. Η συναλλαγή θα μπορούσε να είναι, για παράδειγμα, ένας κατάλογος αγορών στον οποίο η Alice τοποθετεί μια παραγγελία, πληρώνει και ο Bob περιμένει να ξεκαθαρίσει η πληρωμή πριν αποστείλει εμπορεύματα. Σ' αυτό το μοντέλο, το ρίσκο του Bob ότι η πληρωμή θα είναι κακή, είναι σχετικώς χαμηλό αφού το μόνο που χρειάζεται είναι να αστοχήσει στην αποστολή των εμπορευμάτων.

Επειδή το ψηφιακό χρήμα αναπαρίσταται από σειρά bits και υπάρχουν λίγα πράματα σ' αυτή τη ζωή πιο εύκολα αντιγράψιμα από τα bits, η τράπεζα νοιάζεται να σιγουρέψει, ότι οποιαδήποτε αντίγραφα ψηφιακού χρήματος που δημιουργήθηκαν από την Alice ή την Mallet, ένα εχθρικό τρίτο θα είναι μη ξοδέψιμα ή τουλάχιστον θα ανιχνεύονται εύκολα. Η τράπεζα επιθυμεί να εμποδίσει, η τουλάχιστον να ανιχνεύσει,

απόπειρα διπλοξοδέματος ψηφιακού χρήματος προκειμένου να αποφύγει διπλοπληρωμή και στην ιδανικότερη περίπτωση να ξέρει ποιοι είναι οι διπλοξοδευτές ώστε να τους διώξει ποινικά για απάτη. Για παράδειγμα, αν η επικοινωνία της Alice με την τράπεζα δεν είναι κρυπτογραφημένη, η Mallet μπορεί να κρυφακούσει στην τηλεφωνική γραμμή της Alice να καταγράψει το ψηφιακό χρήμα και να προσπαθήσει να το ξοδέψει πριν την Alice. Ακόμη και αν η επικοινωνία με την Alice είναι ασφαλής, η τράπεζα επιθυμεί να σιγουρέψει ότι η ίδια η Alice δεν μπορεί να ξοδέψει ούτε κέρμα πάνω από μια φορά.

Ο Bob, ο έμπορος, επιθυμεί να μπορεί να αποδείξει ότι η Alice εξουσιοδότησε τη συναλλαγή προκειμένου να διασφαλίσει ότι η Alice δεν θα το αρνηθεί αργότερα (μη αποκήρυξη). Ο Bob θέλει επίσης εγγύηση ότι η Alice έχει το κεφάλαιο να πληρώσει για τη συναλλαγή και ότι η τράπεζα θα του χορηγήσει τα χρήματα. Υπό ορισμένες συνθήκες ο Bob ίσως θέλει να αποκρύψει το γεγονός της συναλλαγής.

Εν τω μεταξύ, η Alice επιθυμεί να διασφαλίσει ότι μη εξουσιοδοτημένες πληρωμές είναι αδύνατες, ότι ο Bob δεν μπορεί να αρνηθεί ότι πληρώθηκε, ότι το γεγονός της συναλλαγής είναι ιδιωτικό και ότι υπάρχει αποζημίωση διαθέσιμη αν ο Bob αθετήσει τη συμφωνία ή παραδώσει σκάρτα εμπορεύματα. Σε μερικές περιπτώσεις η Alice θέλει η συναλλαγή να είναι πλήρως ανώνυμη - ούτε καν ο Bob να ξέρει την ταυτότητα της Alice. Σε τέτοιες περιπτώσεις ωστόσο ο Bob θα θελήσει να σιγουρευτεί ότι η Alice αδυνατεί να αποποιηθεί την υποχρέωση να πληρώσει.

Αν η συναλλαγή είναι εξ' ολοκλήρου ηλεκτρονική, καθένα από τα μέρη θα χρειαστεί μηχανισμό να διασφαλίσει ότι τα άλλα μέρη θα πληρώσουν ότι απαιτείται. Σε έναν κόσμο όπου η απάτη είναι πιθανή ή η συναλλαγή έχει μη στιγμιαίες πλευρές (πχ. μια εγγύηση, την δυνατότητα αγωγής για οφειλή προϊόντος, τη δυνατότητα ένα μέρος να επιχειρήσει να αποκηρύξει την πληρωμή) τα μέρη θα ζητήσουν εγγυήσεις ότι οι εταίροι είναι αυτοί που ισχυρίζονται ότι είναι: η τράπεζα, ο Bob και η Alice (η ιδιοκτήτης του ψηφιακού χρήματος). Η αυθεντικότητα της ταυτότητας ωστόσο είναι με διαφορά η ευκολότερη πλευρά της ηλεκτρονικής συναλλαγής, καθώς μπορεί εύκολα να επιτευχθεί με ψηφιακές υπογραφές.

Το ψηφιακό χρήμα μπορεί να αποθηκευτεί σε ένα πλήθος τύπων: στον Η/Υ του οικονομικού φορέα, στους Η/Υ της Alice και του Bob ή σε έξυπνες κάρτες που φέρουν ο πελάτης ή ο έμπορος. Το ψηφιακό χρήμα μπορεί να καλύψει τωρινά ή όχι. Ανάλογα με το χρησιμοποιούμενο σύστημα, αν η Alice και ο Bob κρατούν το ψηφιακό χρήμα, η τράπεζα μπορεί να το εκθέσει σε μορφή ψηφιακών "νομισμάτων" τα οποία πρέπει αθροιζόμενα να ανέλθουν του συνολικού ποσού της αγοράς ή η Alice και ο Bob μπορούν να το κρατούν σε ψηφιακό λογαριασμό πάνω σε έξυπνες κάρτες οι οποίες χρεώνονται ή πιστώνονται όπως χρειάζεται. Το σύστημα ίσως απαιτεί όλες οι συναλλαγές να ρυθμίζονται από τον διατελούντες τη συναλλαγή ή επιτρέπει να ρέουν ελεύθερα κεφάλαια μεταξύ πελατών και εμπόρων.

Ότι ακολουθεί ευελπιστούμε να είναι ένα αντιπροσωπευτικό δείγμα των τύπων ψηφιακού χρήματος υπό ανάπτυξη στις μέρες μας. Λίγα από τα ψηφιακά συστήματα πληρωμών που θα συζητηθούν παρακάτω επιτρέπουν απεριόριστη άμεση μεταφερσιμότητα μεταξύ φορέων ηλεκτρονικών κεφαλαίων:

-με μόνη εξαίρεση το Mondex ψηφιακό ταμειακό μοντέλο, σε όλα τα μοντέλα ψηφιακού νομίσματος ο παραλήπτης ψηφιακής πληρωμής πρέπει πάντα να επιστρέψει στην τράπεζα για ένα νέο νόμισμα πριν καταστεί ικανός να το ξοδέψει, αν και είναι θεωρητικά εφικτό για τους χρήστες να τροποποιούν τουλάχιστον ένα σχήμα πληρωμής ψηφιακού νομίσματος έτσι ώστε να επιτρέπεται τα νομίσματα να μεταφέρονται μέσω τρίτου χωρίς επιστροφή στην τράπεζα.

❖ Το μοντέλο χρεωστικής κάρτας

Το μοντέλο χρεωστικής κάρτας είναι μια απλή καί δαπανηρή στρατηγική ηλεκτρονικής πληρωμής που πληρεί τις ανάγκες ασφαλείας της τράπεζας ενώ διατελείται η συναλλαγή. Η υψίστης ασφαλείας έκδοση αυτού του μοντέλου δεν είναι πραγματικά ψηφιακό χρήμα και τυποποιείται πάνω σε χρεωστικές κάρτες. Η τράπεζα αξιώνει ο Bob, ο έμπορος, να έρχεται σ' επαφή με την τράπεζα on-line τη στιγμή της πληρωμής προκειμένου να μεταφέρει τα κεφάλαια από τον λογαριασμό της Alice στο λογαριασμό του Bob.

Αν η αποταμίευση της Alice δεν επαρκεί τότε η τράπεζα αρνείται να επιτρέψει τη συναλλαγή. Αν ο πελάτης διαθέτει το κεφάλαιο, τότε αυτό μεταφέρεται από τον λογαριασμό πελάτη στον λογαριασμό εμπόρου τη στιγμή της πώλησης. Μια εναλλακτική μορφή του μοντέλου αυτού θέλει την τράπεζα να αντικαθίσταται από μια υπηρεσία διαλεύκανσης η οποία προάγει τις εντολές πληρωμής στις συνήθεις τράπεζες οι οποίες έχουν εκ των προτέρων επιλεγεί από μέλη του σχήματος.

Η ταυτότητα της Alice και του Bob μπορούν να επαληθευτούν με χρήση απαραχάρακτων ψηφιακών υπογραφών, απομακρύνοντας τις πιθανότητες απατηλής ή αποκυρησσόμενης συναλλαγής όσο και τα δύο μέρη προστατεύουν προσεχτικά τις φράσεις κώδικα (αλφαριθμητική, εκδόσεις PIN αριθμών τραπεζικών καρτών) με τις οποίες προσπελαύνουν τους λογαριασμούς τους. Δεν υπάρχει κίνδυνος διπλοπληρωμής ή διπλότυπου ψηφιακού χρήματος διότι το ψηφιακό χρήμα ποτέ δεν αφήνει το τραπεζικό σύστημα.

Ένα μειονέκτημα αυτής της προσέγγισης είναι ότι η on-line επαλήθευση εισάγει καθυστέρηση και έξοδα στη συναλλαγή συγκριτικά με την πεπατημένη των πιστωτικών καρτών. Το κόστος συναλλαγών σε συνδυασμό με το παράδειγμα χρεωστικής κάρτας το κάνουν ακατάλληλο για συναλλαγές χαμηλής αξίας / μεγάλου όγκου. Το βασικό μοντέλο χρεωστικής κάρτας θα δούλευε για την αγορά αυτοκινήτου on-line ή ακόμα και για ένα φανελάκι αλλά όχι για χρέωση 1/10 του cent προς ανάγνωση μιας web σελίδας. Το παράδειγμα χρεωστικής κάρτας επίσης δεν κάνει τίποτα για να προστατέψει τα συμφέροντα ιδιωτικότητας του Bob και της Alice. Η τράπεζα έχει πλήρως καταγεγραμμένη κάθε συναλλαγή. Αυτό διευκολύνει την υπακοή και είναι πολύτιμο για την επιβολή νόμων, αλλά σημαίνει επίσης ότι η ιδωτικότητα τράπεζα είναι χαμηλή και ότι η τράπεζα εύκολα βρίσκει το profile του καταναλωτή.

❖ Το βασικό ψηφιακό νόμισμα

Το βασικό μοντέλο ψηφιακού νομίσματος είναι τελείως απλό. Η τράπεζα αποδίδει στο χρήστη έναν μακρύ πιθανοτικά μοναδικό, τυχαίο αριθμό (τον "σειριακό αριθμό" του νομίσματος) υπογεγραμμένο με το ιδιωτικό κλειδί της τράπεζας. Όταν η Alice θέλει να ξοδέψει ένα νόμισμα, το στέλνει στον Bob, ο οποίος το στρέφει στην τράπεζα είτε on-line είτε μετά το γεγονός. Η τράπεζα ελέγχει το σειριακό αριθμό με βάση τη λίστα εξοδεμένων νομισμάτων και αν το νόμισμα δεν έχει πρωτύτερα ξοδευτεί ή πιστώνει το λογαριασμό του Bob ή του αποδίδει νέο νόμισμα με νέο σειριακό αριθμό. Όσο η τράπεζα είναι ειλικρινής η Alice και ο Bob έχουν και οι δύο τις αποδείξεις που χρειάζονται ότι η συναλλαγή έλαβε χώρα.

Το μοντέλο του νομίσματος είναι επίσης εύκολο να υλοποιηθεί υπολογιστικά. Κάθε νόμισμα απαιτεί μακρύ, μοναδικό τυχαίο αριθμό αλλά η τράπεζα μπορεί να ξαναχρησιμοποιήσει το ίδιο ζευγάρι ιδιωτικού - δημόσιου κλειδιού για να υπογράψει κάθε νόμισμα μιας δεδομένης αξίας. Το βασικό μοντέλο νομίσματος δεν επιτρέπει

ελεύθερη ροή νομισμάτων. Κάθε φορά που η Alice ξοδεύει ένα νόμισμα στο μαγαζί του Bob, ο Bob πρέπει να εξαργυρώσει το νόμισμα στην τράπεζα που το έβγαλε είτε πρόκειται για παραδοσιακό κεφάλαιο είτε για νέο νόμισμα, πριν μπορέσει να το ξοδέψει.

Το μοντέλο βασικού νομίσματος έχει 2 προβλήματα.

Πρώτον αν η συναλλαγή είναι on-line σε πραγματικό χρόνο, αλλά η επαλήθευση είναι off-line (δηλαδή κάποιο χρόνο μετά την ολοκλήρωσή της συναλλαγής), ο Bob δεν θα μπορεί ίσως να ελέγξει αν το νόμισμα που του προσφέρει η Alice δεν έχει προηγουμένως ξοδευτεί πριν να είναι αργά. Ο Bob μπορεί να ελέγξει την ψηφιακή υπογραφή της ισχυριζόμενης αξίας. Αυτό το test θα διακρίνει ένα κάλπικο νόμισμα από ένα πραγματικό. Αλλά χωρίς την on-line επαλήθευση ο Bob δεν μπορεί να πει αν ένα νόμισμα έχει ήδη εξοφληθεί κάπου αλλού την ώρα που η Alice αγοράζει από αυτόν. Η on-line επαλήθευση διασφαλίζει ότι το νόμισμα που προσφέρεται είναι έγκυρο, αλλά αυτή η επαλήθευση προσθέτει κατά πάσα πιθανότητα καθυστέρηση και κόστος.

Δεύτερον, εφόσον ο σειριακός αριθμός του νομίσματος είναι μοναδικός και γνωστός στην τράπεζα, η εξαγορά του νομίσματος από τον Bob συνδέει την Alice με την συναλλαγή και η τράπεζα καταλήγει σε μια βάση δεδομένων που να περιέχει πληροφορία για όλους τους πελάτες της. Όπως και στο μοντέλο πιστωτικής κάρτας οι πελάτες δεν απολαμβάνουν ιδωτικότητα.

Τα βασικά ψηφιακά νομίσματα έχουν το πολύ μικρό αντίκτυπο στα χρηματικά εφόδια. Το αν θα επηρεάζουν ολωσδιόλου εξαρτάται σε μεγάλο ποσοστό από το πως μεταχειρίζονται πελάτες και τράπεζες τα νομίσματα και από το αν χρησιμοποιούν on-line ή off-line συστήματα διευκόλυνσης (ξεκαθαρίσματος). Στο ένα άκρο, οι συναλλαγές ξεκαθαρίζονται on-line και η τράπεζα θέλει την Alice να μην αγοράζει νομίσματα μέχρι τη στιγμή που τα χρειάζεται. Σαν αποτέλεσμα, η Alice κρατάει το κεφάλαιό της σε έναν φορολογήσιμο λογαριασμό μέχρι που να χρειαστεί νόμισμα. Όταν θελήσει να συναλλαγεί με τον Bob επικοινωνεί με την τράπεζα, η τελευταία βγάζει νόμισμα και εκείνη το προσφέρει στον Bob, ο οποίος το εξαργυρώνει μόλις το λάβει από την Alice. Στο σενάριο αυτό οι επιδράσεις του νομίσματος στη διαθέσιμη ποσότητα χρήματος είναι αμελητέες.

Στο άλλο άκρο, οι συναλλαγές ξεκαθαρίζονται off-line και η τράπεζα απαιτεί η Alice να αποκτήσει ψηφιακά νομίσματα πριν τα χρειαστεί, όπως κάποιος αγοράζει ταξιδιωτικά τσεκ σήμερα. Επειδή το on-line ξεκαθάρισμα δεν είναι διαθέσιμο ή είναι πολύ ακριβό, άρα μη πρακτικό, ο Bob ρισκάρει να μην πληρωθεί με προεξοφλημένο νόμισμα τη στιγμή που το δέχεται από την Alice. Η ανάγκη του Bob να συναθροίσει νομίσματα πριν τα εξαργυρώσει από την τράπεζα εισάγει περαιτέρω καθυστέρηση πριν τη συμφωνία. Σ' αυτή την έκδοση τα ψηφιακά νομίσματα λειτουργούν αρκετά, σαν ταξιδιωτικά τσεκ. Εφόσον τα ταξιδιωτικά τσεκ όσο και τα μετρητά είναι μέρη του M1, το στενότερο μέτρο χρημάτων ευρέως χρησιμοποιούμενο από μακροοικονομολόγους, αυτό από μόνο του δε λέει τίποτα. Αν ωστόσο, ο κόσμος διαλέξει να φέρει ψηφιακά νομίσματα αντί για τα συνηθισμένα μετρητά, το περισσότερο από το χρήμα σε κυκλοφορία θα διοχετευτεί στο τραπεζικό σύστημα αυξάνοντας το απόθεμα χρήματος μέσω τμηματικού αποταμιευτικού δανεισμού. Τα ψηφιακά νομίσματα θα μπορούσαν να έχουν επίσης μικρό αντίκτυπο στην κινητικότητα του χρήματος αν προκαλέσουν μεγαλύτερο αριθμό συναλλαγών ετησίως ή αν η ύπαρξη παγκοσμίων 24ωρων κυβερνομονοπατιών ενθαρρύνει τον κόσμο να συναλλάσσεται συχνότερα.

❖ Τυφλωμένα νομίσματα

Το βασικό μοντέλο νομίσματος εμπιστεύεται την τράπεζα με τίμημα την on-line επαλήθευση και την ευκαιρία για τις τράπεζες να συσσωρεύσουν χαρακτηριστικά εξόδων των πελατών. Είναι δυνατό, ωστόσο, να κρατήσουμε τα γνωρίσματα εκείνα του βασικού μοντέλου νομίσματος που καθιστούν αδύνατο ή τουλάχιστο πολύ ριψοκίνδυνο για τους ανθρώπους να αντιγράφουν το ψηφιακό τους χρήμα και να το ξοδεύουν εις διπλούν χωρίς να έχει η τράπεζα τη δυνατότητα να δημιουργήσει γιγαντιαία βάση δεδομένων με το ποιος ξόδεψε τι και που. Σ' αυτό το μοντέλο οι πληρώνοντες, αλλά όχι οι πληρωνόμενοι, μπορούν να μείνουν ανώνυμοι.

Χρησιμοποιώντας "τυφλωμένα νομίσματα" η Alice μπορεί να αποκτήσει ψηφιακό χρήμα με μοναδικό σειριακό αριθμό από τράπεζα χωρίς να επιτρέψει στην τράπεζα να δημιουργήσει εγγραφή με το σειριακό αριθμό του νομίσματος. Πέρα από την άγνοια της τράπεζας περί του σειριακού αριθμού, η μοναδικότητα του αριθμού βοηθάει να διασφαλίσουμε ότι η Alice δεν μπορεί να ξοδέψει το νόμισμα δύο φορές.

Οι τεχνικές που το καταφέρνουν αναπτυγμένες και κατοχυρωμένες από τον David Cham και πραγματευόμενες από μια εταιρία που ίδρυσε ονόματι DiyiCash, είναι περίπλοκες. Όπως ένα βασικό ψηφιακό νόμισμα, ένα τυφλωμένο νόμισμα ξεκινά με ένα μακρύ τυχαίο σειριακό αριθμό, αλλά αυτή τη φορά ο σειριακός αριθμός γεννιέται από την Alice, τον πελάτη που σκοπεύει να αποκτήσει νόμισμα από την τράπεζα. Η Alice πολλαπλασιάζει αυτόν τον σειριακό αριθμό με έναν άλλον τυχαίο συντελεστή (τον "τυφλωμένο συντελεστή" και στέλνει το προϊόν (τον "τυφλωμένο αριθμό") στην τράπεζα. Όπως και στη βασική περίπτωση, η τράπεζα υπογράφει τον αριθμό με το μυστικό κλειδί της.

Αντίθετα απ' ότι συμβαίνει στη βασική περίπτωση, ωστόσο, μια τράπεζα που βγάζει ένα τυφλωμένο σύστημα δεν γνωρίζει τον πραγματικό σειριακό αριθμό του νομίσματος τη στιγμή που το διαθέτει τυπώνοντας την ψηφιακή της υπογραφή στον "τυφλωμένο αριθμό". Όλα όσα ξέρει η τράπεζα είναι ότι η Alice αγόρασε νόμισμα δεδομένης αξίας και τον "τυφλωμένο αριθμό" που υπέβαλε η Alice. Απουσία ανωνύμων τραπεζικών λογαριασμών, η τράπεζα γνωρίζει την ταυτότητα της Alice και πόσα νομίσματα από κάθε αξία αγοράζει η Alice. Εφοδιασμένη μ' αυτή την πληροφορία, η τράπεζα θα πρέπει να μπορεί να εναρμονιστεί με κανόνες σχεδιασμένους να ελέγχουν το ξέπλυμα χρήματος και την φοροδιαφυγή όσο και οποιαδήποτε συνηθισμένη τράπεζα. Η ιδιωτικότητα της Alice εξαρτάται από εν μέρει από την ύπαρξη επαρκούς όγκου νομισμάτων σε κυκλοφορία τέτοιου που οι αγορές της Alice και η χρήση των νομισμάτων να μην ξεχωρίζει.

Υπάρχει κι άλλος ένας τρόπος να κρύβουμε και να ανακαλούμε την ταυτότητα της Alice. Σ' αυτή τη διαφοροποίηση η τράπεζα δεν ξέρει ποιος ξόδεψε τα χρήματα ενόσω ξοδεύτηκαν μια φορά, αλλά αυτή η πληροφορία είναι προσβάσιμη από συστημένο οργανισμό ξένο προς την τράπεζα. Οι εφευρέτες αυτού του είδους ψηφιακού χρήματος προτείνουν ο διαπιστευμένος τρίτος ο οποίος θα κρατάει τα μέσα για την αποανωνυμοποίηση του ψηφιακού χρήματος να είναι "οργάνωση για τα δικαιώματα του καταναλωτή". Τίποτα στο πρωτόκολλό τους, ωστόσο, δεν θα εμπόδιζε μια κυβέρνηση από το να απαιτήσει αυτή η οργάνωση να είναι η αστυνομία ή τα δικαστήρια.

Στην πραγματικότητα αυτό το πρωτόκολλο ανοίγει την πόρτα σε πρώτης τάξης ψηφιακό χρήμα. Έτσι η κυβέρνηση θα μπορούσε να επισκοπήσει συναλλαγματικά δεδομένα τα οποία υπόκεινται στους περιορισμούς της τέταρτης τροπολογίας. Είναι δυνατό να τροποποιηθεί το σύστημα ανιχνεύσιμου ανώνυμου χρήματος έτσι ώστε η ταυτότητα του χρήστη να αποκαλύπτεται μόνο όταν διάφορα

μέρη ("διαπιστευμένοι") συμφωνήσουν. Αυτό το σύστημα πολλαπλών διαπιστευμένων μοιάζει με το σύστημα πολλαπλών συντελεστών που επιθυμούν τα κλειδιά του τσιπ κοπής νομισμάτων.

Όλα τα είδη "τυφλωμένων νομισμάτων" δημιουργούνται ως εξής: Όταν επιστραφεί στην Alice το υπογεγραμμένο τυφλωμένο νούμερο από την τράπεζα, αυτή εκτελεί έναν μαθηματικό υπολογισμό που αφαιρεί τον "τυφλωτικό παράγοντα". Το αποτέλεσμα είναι ένα νόμισμα που μοιάζει με το βασικό ψηφιακό νόμισμα, κατέχει τον "πραγματικό" σειριακό αριθμό και φέρει την ψηφιακή υπογραφή της τράπεζας που επιβεβαιώνει την αυθεντικότητα του πραγματικού -όχι του τυφλωμένου- σειριακού αριθμού. Η Alice μπορεί να ξοδέψει τώρα το νόμισμα στο μαγαζί του Bob σαν να ήταν βασικό νόμισμα. Απουσία ανώνυμων τραπεζικών λογαριασμών, ο Bob οφείλει ακόμη να αποκαλύπτει την ταυτότητά του για να εξαργυρώσει το νόμισμα. (Αν για κάποιο λόγο θελήσει η Alice αργότερα να "διακόψει την πληρωμή" στο νόμισμα διότι ο Bob παρέβηκε συμφωνία μπορεί πάντα να αποκαλύπτει τον πραγματικό σειριακό αριθμό στην τράπεζα.

Όπως και το βασικό νόμισμα έτσι και το τυφλωμένο δεν είναι παρά ψηφιοποιημένα δεδομένα. Εφόσον η διαδικασία τύφλωσης σημαίνει ότι η τράπεζα δε μπορεί να οδηγηθεί από τον σειριακό αριθμό στην Alice πρέπει να υπάρξει κάποιος τρόπος που να την πείθει να μην τυπώνει και να μην διπλοτυπώνει νομίσματα. Το να εμποδίσουμε την Alice να ξεγελάσει ένα σύστημα βασισμένο σε off-line ξεκαθάρισμα είναι πιο δύσκολο.

- **<u>Α) Αποτροπή διπλοξοδέματος τυφλωμένων νομισμάτων με on-line ξεκαθάρισμα (DigiCash)</u>**

Όταν η Alice ξοδεύει ένα τυφλωμένο νόμισμα και ο Bob παρουσιάζει το νόμισμα στην τράπεζα για την τακτοποίηση, η τράπεζα δεν μπορεί να συνδέσει το νόμισμα με την Alice διότι δεν έχει εγγραφή με το σειριακό αριθμό του νομίσματος. Χωρίς κάποιο μέσο αποθάρρυνσης του διπλοξοδέματος, ο πειρασμός ίσως υπερκεράσει τους ενδοιασμούς της Alice. Το on-line ξεκαθάρισμα αίρει κάθε πειρασμό.

Εφόσον η τράπεζα ξέρει κάθε εξαργυρωμένο σειριακό αριθμό, μπορεί να ελέγξει το προτεινόμενο νόμισμα του Bob σε σχέση με την κύρια λίστα. Αν το νόμισμα έχει ήδη ξοδευτεί αρνείται την πληρωμή. Καθώς το ξεκαθάρισμα είναι on-line ο Bob μπορεί να πει στην Alice ότι η τράπεζα αρνήθηκε να εξοφλήσει το νόμισμά της, όπως ακριβώς ένας έμπορος θα πει σε πελάτη ότι μια εταιρία πιστωτικών καρτών αρνήθηκε να εξουσιοδοτήσει μια αγορά.

Στις 23 Οκτωβρίου 1995, η Mark Twain Bank of St Louis Missouri, έγινε ο πρώτος παγκοσμίως οργανισμός που πρότεινε τυφλωμένα ψηφιακά νομίσματα χρηματοδοτούμενης αξίας. Η τράπεζα χρησιμοποιεί λογισμικό εξουσιοδοτημένο από την DiyiCash. Το σύστημα βασίζεται στο on-line ξεκαθάρισμα τυφλωμένων νομισμάτων, αλλά οι λεπτομέρειες των τεχνικών προδιαγραφών του συστήματος ήταν περιορισμένες όταν το παρόν άρθρο τυπώθηκε. Αλλοι οικονομικοί οργανισμοί θα προσφέρουν κατά πάσα πιθανότητα παρεμφερής ηλεκτρονικής υπηρεσίας χρήματος στο εγγύς μέλλον. Για παράδειγμα η DigiCash εξουσιοδοτεί το λογισμικό της στο Σουηδικό Post Office, το οποίο υποστηρίζει τη λιανική τραπεζική δραστηριότητα η οποία σχετίζεται με λογαριασμούς υποστηριζόμενους από το 75% των Σουηδικών νοικοκυριών .

➢ **Β) Αποτροπή διπλοξοδέματος τυφλωμένων νομισμάτων με off-line ξεκαθάρισμα**

Το on-line ξεκαθάρισμα είναι ακριβό σε χρόνο και χρήμα. Το off-line ξεκαθάρισμα δίνει την ευκαιρία σε ανέντιμους παράγοντες να ξοδέψουν το ίδιο νόμισμα πολλές φορές εφόσον το παραλαμβάνον μέρος δεν γνωρίζει ότι το νόμισμα έχει ήδη ξοδευτεί μέχρι που είναι πολύ αργά.

Το ρίσκο του Bob ότι το νόμισμα που προσφέρει η Alice θα αποδειχτεί άνευ αξίας αυξάνεται όταν ούτε ο Bob ούτε η τράπεζα ξέρουν ποια είναι η Alice, αφού η Alice πιστεύει εύλογα ότι η ανωνυμία την προστατεύει από τις συνέπειες του διπλοξοδέματος. Ακόμη και αν ο Bob παίρνει σοβαρό ρίσκο αφού το κόστος εξαναγκασμού της Alice να πληρώσει είναι μεγαλύτερο από το ίδιο το χρέος. Αυτό περιλαμβάνει ίσως ευρεία γκάμα συναλλαγών αν το Internet εμπόριο γίνει παγκόσμιο. Παρόλα αυτά αν η Alice ξέρει ότι ο Bob και η τράπεζα γνωρίζουν την ταυτότητά της, φοβάται φυσικά μήπως ο Bob την καταδώσει στις αρμόδιες αρχές, ενδεχομένως με ποινική δίωξη κατά εγκληματία, πράγμα το οποίο θα απαξίωνε τον πειρασμό για διπλοξόδεμα.

Η ουσία του τυφλωμένου νομίσματος είναι ότι η τράπεζα δεν γνωρίζει το σειριακό αριθμό του νομίσματος και έτσι αδυνατεί να συμπεράνει την ταυτότητά του πληρώνοντος όταν το νόμισμα παρουσιάζεται για εξαγορά από τον πληρωμένο. Τόσο στο βασικό μοντέλο όσο και στο τυποποιημένο μοντέλο τυφλωμένου νομίσματος, το νόμισμα δεν φέρει πληροφορία σχετική με την Alice. Είναι δυνατό, ωστόσο, να κωδικοποιήσουμε πληροφορία έτσι ώστε αυτή να παραμείνει κρυπτογραφημένη αν το νόμισμα ξοδευτεί μια μόνο φορά. Αν κάποιος προσπαθήσει να ξοδέψει ένα νόμισμα που έχει ήδη εξαργυρωθεί, το δεύτερο ξόδεμα θα αποκαλύψει την κωδικοποιημένη πάνω στο νόμισμα πληροφορία για το γνήσιο ιδιοκτήτη του. Αυτό το σύστημα δουλεύει ακόμη και αν η Alice ξοδέψει το νόμισμα σε δύο διαφορετικούς εμπόρους.

Το δεύτερο ξόδεμα μπορεί να αποκαλύψει μόνο την όποια πληροφορία προσάρτησε η τράπεζα στο νόμισμα όταν το έδωσε στην Alice. Η τράπεζα είναι υπεύθυνη για την επιλογή κωδικοποίησης επαρκούς πληροφορίας π.χ. έναν μοναδικό αριθμό ταυτοποίησης, ο οποίος να επιτρέπει την προσέγγιση του πελάτη. Η τράπεζα έχει ωστόσο ένα πρόβλημα. Δεν μπορεί να διαβάσει την κρυπτογραφημένη, σχετική με την Alice, πληροφορία, εκτός και αν το τυφλωμένο νόμισμα ξοδεύτηκε δυο φορές.

Μ' άλλα λόγια, η τύφλωση εμποδίζει την τράπεζα να επιθεωρήσει το νόμισμα τη στιγμή της παραγωγής του ώστε να διασφαλίσει ότι η Alice έχει στην πραγματικότητα παραδώσει την απαιτούμενη πληροφορία. Η τράπεζα μπορεί όμως να χρησιμοποιήσει πιθανοτικές μεθόδους που καθιστούν πολύ πιθανό η Alice να κωδικοποιεί την ταυτότητά της στο νόμισμα τη στιγμή που η τράπεζα το παράγει.

Για παράδειγμα, έστω ότι η τράπεζα απαιτεί η Alice να δημιουργήσει εκατό τυφλωμένους αριθμούς και συσχετισμένα πεδία κρυπτογραφημένων δεδομένων. Η τράπεζα θα μπορούσε να απαιτήσει τότε την αποκάλυψη του περιεχομένου των 99 νομισμάτων κατ' επιλογή της τράπεζας. Αν όλα αυτά τα νομίσματα αποδειχτεί ότι περιέχουν τη δέουσα πληροφορία για την Alice, υπάρχουν καλές πιθανότητες και το 100οστό νόμισμα -το μόνο που θα υπογραφεί πραγματικά από την τράπεζα και το μόνο για το οποίο η Alice δεν αποκαλύπτει περιεχόμενα- να περιέχει αυτή την πληροφορία. Αν η Alice προσπαθήσει να εξαπατήσει εισάγοντας ελλιπή ή λανθασμένη πληροφορία έστω και σε ένα από τα 100 νομίσματα., η τράπεζα κατά πάσα πιθανότητα θα το ανιχνεύσει. Κι αν η τράπεζα ανιχνεύσει απόπειρα εξαπάτησης, θα αρνηθεί να ξαναεφοδιάσει την Alice ψηφιακά νομίσματα.

Σε ένα off-line σχήμα ξεκαθαρίσματος, η εξασφάλιση του Bob απέναντι στο διπλοξόδεμα εναπόκειται σε ένα πρωτόκολλο πρόκλησης - απόκρισης το οποίο αποκαλύπτει την ταυτότητα της Alice αν προσπαθήσει να διπλοξοδέψει. Ο Bob αναλαμβάνει έτσι κάποιο ρίσκο να μπλεχτεί με το ψηφιακό ισοδύναμο του sluy σε αυτόματο πωλητή διότι η Alice έχει ίσως ξοδέψει το νόμισμα αλλού πριν αυτός το φέρει στην τράπεζα. Αντίθετα απ' ότι sluy σε αυτόματο πωλητή, το κέρμα μπορεί να περιέχει πληροφορία που γνωστοποιεί την ταυτότητα της Alice στην τράπεζα. Το αν αυτό αρκεί για να βρούμε την Alice και να αναλάβουμε πολιτικά ή εγκληματολογικά ένδικα μέσα εξαρτάται από το αν η πληροφορία στο νόμισμα είναι ακριβής και από τους εμπλεκόμενους αρμόδιους.

Ίσως τα τυφλωμένα νομίσματα δεν μπορούν να παραχθούν ασφαλώς με αξίες σεβαστού μεγέθους απουσία αποδοτικού on-line συστήματος ξεκαθαρίσματος. Η Alice θα μπορούσε να ξοδέψει ακόμη και ένα νόμισμα $1 πολλές φορές μέσα σε λίγα λεπτά και ακολούθως να επιχειρήσει να εξαφανιστεί. Ωστόσο, αν η αξία είναι χαμηλή, ο Bob μπορεί να περιορίσει τον κίνδυνο αν ελέγχει κάθε μικρής αξίας νόμισμα που προσφέρει η Alice έτσι ώστε να σιγουρευτεί ότι δεν είναι διπλότυπο νομίσματος που έχει ο ίδιος δεχτεί στο παρελθόν και να φροντίσει να επικοινωνήσει με την τράπεζα για επαλήθευση οποτεδήποτε δέχεται τόσα νομίσματα όσα θέλει να κρατήσει ρισκάροντας.

- **Γ) Αποτροπή διπλοξοδέματος τυφλωμένων νομισμάτων με ηλεκτρονικά πορτοφόλια.**

Προκειμένου να νιώσουμε πεπεισμένοι σχετικά με την παραγωγή τυφλωμένων νομισμάτων, οι τράπεζες απαιτούν κατά το δυνατό αξιοπρεπή βαθμό διαβεβαίωσης ότι τα νομίσματα δε μπορούν να ξοδευτούν περισσότερες από μία φορά. Οι τράπεζες θέλουν επίσης να ελαχιστοποιήσουν τις πιθανότητες κάποιος τρίτος να ξεπλύνει χρήματα προκειμένου να αποφύγουν μπλεξίματα με τις κρατικές ρυθμιστικές αρχές. Από την πλευρά της τράπεζας είναι ίσως πολυτέλεια να μπορεί να ταυτοποιήσει το πρόσωπο που ξόδεψε ένα νόμισμα ένα εκατομμύριο φορές αν αυτό το πρόσωπο δε μπορεί να βρεθεί.

Το ηλεκτρονικό πορτοφόλι είναι μία έξυπνη κάρτα με μικροεπεξεργαστή. Το πορτοφόλι αλληλεπιδρά με ειδικά σχεδιασμένους αναγνώστες καρτών, κάτι σαν τραπεζικές κάρτες που χρησιμοποιούνται στις Automatic Teller Machines. Εμβαπτίζοντας το νόμισμα ή τουλάχιστον μέρος της αναγκαίας πληροφορίας για χρήση του νομίσματος, σε μια έξυπνη κάρτα με ανεκτικά στην παραχάραξη χαρακτηριστικά έχουμε πρόσθετη ασφάλεια, ιδίως αν το ανεκτικό στην παραχάραξη μέρους της κάρτας είναι προγραμματισμένο να εμποδίζει το διπλοξόδεμα. Τράπεζες, έμποροι, ακόμη και προσωπικοί υπολογιστές θα μπορούσαν να εφοδιαστούν με τους απαραίτητους αναγνώστες έξυπνων καρτών.

Μια προέκταση αυτού του μοντέλου απαιτεί το ανεκτικό στην παραχάραξη μέρους της κάρτας να έχει ηλεκτρονικό παρατηρητή του οποίου η συμμετοχή είναι απαραίτητη για το ξόδεμα ενός νομίσματος. Ο συνδυασμός προστατεύει την ιδιωτικότητα διοχετεύοντας όλες τις επικοινωνίες του παρατηρητή μέσω του Η/Υ της Alice ο οποίος είναι προγραμματισμένος να διασφαλίζει ότι δεν αποκαλύπτονται λεπτομέρειες της συναλλαγής. Αν κάποιος σπάσει την αντοχή στην παραχάραξη και επιχειρήσει να διπλοξοδέψει, το πρωτόκολλο των τυφλωμένων νομισμάτων συνεχίζει να εφαρμόζεται και αποκαλύπτεται η ταυτότητα του αυθεντικού ιδιοκτήτη του νομίσματος.

Το καλύτερο ίσως παράδειγμα είναι η εφαρμογή υπό όρους πρόσβαση για την Ευρώπη (CAFE - Contitional Access For Europe), την οποία πατρονάρει το πρόγραμμα ESPRIT της ευρωπαϊκής ένωσης. Το πρωτόκολλο CAFE υπόσχεται υψηλή ασφάλεια στον πολίτη, πιθανότητα να πάρει πίσω αξόδευτα χρήματα αν χαθεί το πορτοφόλι και η ιδιωτικότητα του πληρώνοντος (όχι του πληρωμένου). Ως τώρα, δεν υπάρχει πραγματικό προϊόν CAFE πέρα απ' τα πρωτότυπα.

❖ **Το μοντέλο της ταξιδιωτικής επιταγής.**

Τα χρηματικά συστήματα που βασίζονται σε ψηφιακά νομίσματα έχουν προβλήματα με το ακριβές αντίτιμο. Τα ψηφιακά νομίσματα δεν είναι δυνατό να διαχωριστούν χωρίς να θυσιαστεί ιδιωτικότητα του πελάτη και επίσης προκαλούν την πολύ μικρή λειτουργικότητα του συστήματος πληρωμής.Τα αδιαχώριστα νομίσματα κανονικά πρέπει να συναθροιστούν για να σχηματίσουν το ποσό που χρειάζεται για μία αγορά, ακριβώς όπως τα δεκάρικα και οι δραχμές θα μπορούσαν να συνδυαστούν για να σχηματίσουν μια κατοχή 23 δραχμών.

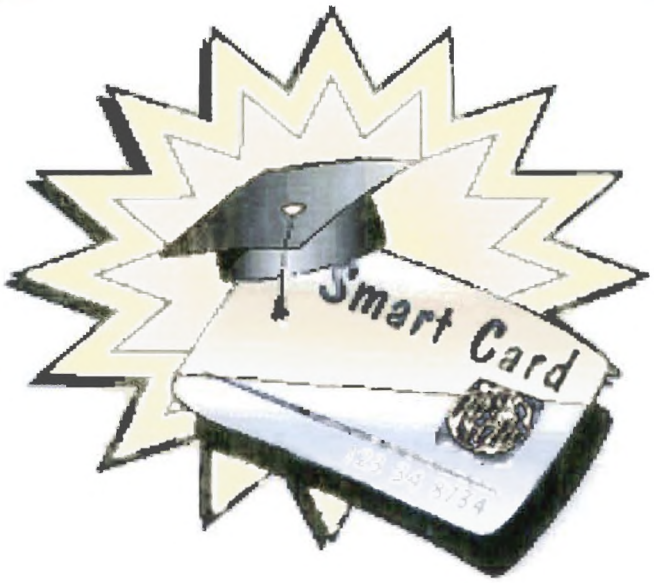
Αν τα νομίσματα είναι σε μικρές υποδιαιρέσεις, ένας μεγάλος αριθμός νομισμάτων απαιτείται για να αγοραστεί ό,τιδήποτε ακόμα και σχετικά φτηνό. Ως ένα σημείο, η διαχείριση ενός αρκετά μεγάλου αριθμού νομισμάτων μπορεί να εισάγει καθυστερήσεις μεταφοράς και κόστος πληροφοριών διαχείρισης. Αν τα νομίσματα πρόκειται να κουβαληθούν μέσω μιας έξυπνης κάρτας, μεγάλοι αριθμοί νομισμάτων απαιτούν μια κάρτα με ακόμη μεγαλύτερη μνήμη, το οποίο αυξάνει την επένδυση που απαιτείται προκειμένου να συμμετάσχει κανείς στο σύστημα.

Οποιαδήποτε είναι η τιμή του αγαθού που αγοράζεται, ο Bob χρειάζεται να παρέχει ρέστα εάν η Alice συμβαίνει να μην έχει τα ακριβή νομίσματα που απαιτούνται. Για αυτό το λόγο ο Bob χρειάζεται να έχει εναπόθεμα νομισμάτων στο χέρι για να πληρώσει την Alice (θυμηθείτε ότι όλα τα νομίσματα πρέπει να επιστρέφονται στην τράπεζα κάθε φορά που ξοδεύονται) και η Alice χρειάζεται να είναι ικανή να καταθέτει νομίσματα στην τράπεζα όπως επίσης και να τα αποσύρει.

Αντιθέτως ένα ηλεκτρονικό σύστημα ταξιδιωτικής επιταγής επιτρέπει στην Alice να ξοδεύει κάθε επιταγή για ποσό μέχρις ενός προκαθορισμένου μεγίστου. Η τράπεζα χρεώνει την Alice για τη μέγιστη τιμή όταν δημιουργείται η επιταγή και αποδίδει στην Alice τη διαφορά μεταξύ του μεγίστου και του ποσού που δαπανήθηκε στην πραγματικότητα.

Αν το σύστημα επιταγών βασίζεται σε "τυφλωμένες" επιταγές συναφείς με τα τυφλωμένα νομίσματα, είναι δυνατό να σχεδιαστεί σύστημα επιστροφής χρημάτων έτσι ώστε όταν η Alice παρουσιάζει το αξόδευτο τμήμα της επιταγής για απόδοση χρημάτων, τίποτα στην αίτησή της (δεν έχει σχέση με το απαιτούμενο ποσό) να μη δίνει στην τράπεζα πληροφορία που θεατής επέτρεπε να συνδέσει την αίτηση απόδοσης χρημάτων με κάποια συγκεκριμένη πληρωμή .Σε αντίθεση με τις ταχυδρομικές επιταγές, ανταγωνιστικές πιέσεις θα μπορούσαν να εξαναγκάσουν τις τράπεζες να πληρώνουν τόκο για τα κεφάλαια που δεσμεύονται για την κάλυψη της επιταγής.

ΜΕΡΟΣ Β



ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ

ΕΙΣΑΓΩΓΗ

Διεθνώς, κατά την τελευταία δεκαετία οι τεχνολογίες των Έξυπνων Καρτών χρησιμοποιούνται για την προσέγγιση και επίλυση προβλημάτων πρόσβασης, διαχείρισης και διακίνησης πληροφορίας σχεδόν σε όλους τους τομείς της οικονομίας και της κοινωνίας. Αυτό γίνεται εκτενώς στα πλαίσια ερευνητικών και πιλοτικών έργων και σε μικρότερη έκταση στα πλαίσια τομεακών έργων τοπικής ή εθνικής κλίμακας, π.χ. κάρτα υγείας, ταυτότητας, ηλεκτρονικό πορτοφόλι, κάρτα πρόσβασης στις συγκοινωνίες κλπ. Είναι πλέον γενικώς αποδεκτό ότι οι τεχνολογίες των Έξυπνων Καρτών προσφέρουν πολλά επιχειρησιακά πλεονεκτήματα στη υλοποίηση σύγχρονων ηλεκτρονικών υπηρεσιών. Ο ρόλος τους κυρίως εστιάζεται στην διαμόρφωση και διασφάλιση περιβάλλοντος εμπιστοσύνης στις συναλλαγές μεταξύ πολιτών και παροχέων υπηρεσιών σε όλους τους τομείς της σύγχρονης οικονομίας.

Τα κύρια ζητήματα, που έχουν λειτουργήσει ανασταλτικά στην προώθηση και την εκτεταμένη αξιοποίηση των Έξυπνων Καρτών αφορούν στα κάτωθι:

1. έλλειψη ενιαίας προσέγγισης για την χρησιμότητα και λειτουργικότητα των Έξυπνων Καρτών μεταξύ όλων των εμπλεκομένων μερών τόσο στην λήψη αποφάσεων όσο και στην υλοποίηση εφαρμογών.
2. έλλειψη ευρέως αποδεκτών προτύπων σε όλα τα επίπεδα των τεχνολογιών των Έξυπνων Καρτών (κάρτες, αναγνώστες καρτών, λογισμικό, τυποποίηση πληροφοριών κλπ.) για την διασφάλιση της διαλειτουργικότητας (interoperability) μεταξύ συστημάτων σε τομεακό, διατομεακό και διακρατικό επίπεδο.

Για την Ευρωπαϊκή Ένωση, οι Έξυπνες Κάρτες αποτελούν μία από τις προτεραιότητες του Σχεδίου Δράσης του eEurope στα πλαίσια της ανάπτυξης ασφαλών και γρήγορων δικτύων και ενίσχυσης του ηλεκτρονικού επιχειρείν. Η Ευρωπαϊκή Επιτροπή προωθεί το θέμα με την οργάνωση Συνόδου Κορυφής για τις Έξυπνες Κάρτες και τον προσδιορισμό των αναγκαίων ενεργειών (trail-blazers) για την επίτευξη των στόχων του eEurope. Τα trail-blazers που αρχικά δημιουργήθηκαν είναι: Public Identity, Identification & Authedication, Certification & Protection Profile, Generalized Card Reader, e-Payments, Contactless Smart Cards, Multi-application Smart Cards. Στην συνέχεια δημιουργήθηκαν συμπληρωματικά τέσσαρα ακόμη trail-blazers, που αφορούν στα: User Interface-Consumer Issues, Public Transport, Healthcare και e-Government. Για την μελέτη των θεμάτων των trail-blazer συγκροτήθηκαν αντίστοιχες ομάδες εργασίας αποτελούμενες από εκπροσώπους κοινωνικών ομάδων και παροχέων υπηρεσιών, της βιομηχανίας και του ακαδημαϊκού και ερευνητικού χώρου.

Η κατάσταση στη χώρα μας και η κινητικότητα που έχει δημιουργηθεί σε ευρωπαϊκό και διεθνές επίπεδο για θέματα ανάπτυξης εφαρμογών Έξυπνων Καρτών όπως: κάρτες υγείας, πρόνοιας, εκπαίδευσης, εργασίας -ασφάλισης, κάρτες χρηματιστηρίου, κάρτες εφορίας, κάρτες διοδίων κτλ συνηγορούν στη συγκρότηση διεπιστημονικής ομάδας εργασίας για την αποτίμηση της ελληνικής κατάστασης λαμβάνοντας υπ' όψη ζητήματα που είτε έχουν προκύψει σε άλλες χώρες, ή δεν έχουν αντιμετωπιστεί ακόμη.

13 ΙΣΤΟΡΙΑ ΤΩΝ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ [72]

Οι πρόγονοι των έξυπνων καρτών θεωρούνται οι πιστωτικές κάρτες που εξέδωσε ο οργανισμός Diners Club τη δεκαετία του 1950 στις Ηνωμένες Πόλιτείες όπου εισήγαγε την πρώτη πλαστική κάρτα για χρήση σε εφαρμογές πληρωμών. Οι κάρτες αυτές είχαν το μέγεθος μίας επαγγελματικής κάρτας (business card) και είχαν τυπωμένο το όνομα του κατόχου της στην εμπρόσθια όψη. Η επίδειξη της ήταν αρκετή, ώστε ο πάροχος της υπηρεσίας (π.χ. ξενοδοχείο ή εστιατόριο) να παράσχει πίστωση στον κάτοχό της. Με τον τρόπο αυτό διευκολύνθηκαν τα επαγγελματικά ταξίδια.

Αργότερα, η εκτύπωση του ονόματος γινόταν σε ανάγλυφο (όπως για παράδειγμα σήμερα στις κάρτες ανάληψης χρημάτων από τα ATM των τραπεζών), ώστε να διευκολύνεται η αποτύπωση του ονόματος του κατόχου.

Μερικά χρόνια αργότερα οι κάρτες αυτές απέκτησαν μία μαγνητική λωρίδα (magnetic stripe), η οποία επέτρεπε τη μηχανική αποτύπωση των στοιχείων του κατόχου. Με τον τρόπο αυτό η επεξεργασία των στοιχείων μπορούσε να γίνει ηλεκτρονικά, επιταχύνοντας τις συναλλαγές. Παρέμενε όμως το πρόβλημα της απάτης, καθώς οποιοσδήποτε, έχοντας τον κατάλληλο εξοπλισμό, μπορούσε να δημιουργήσει πλαστές κάρτες.

Θα μπορούσαμε να πούμε ότι οι έξυπνες κάρτες είναι το αποτέλεσμα της ταυτόχρονης βελτίωσης των πλαστικών καρτών και των microchip αφού οι ευρωπαϊκές χώρες πέτυχαν μια τεράστια βελτίωση πέρα από τη μαγνητική τεχνολογία λωρίδων με την εισαγωγή της κάρτας ολοκληρωμένων κυκλωμάτων (ICC).

Το 1969 παρουσιάστηκε στη Γαλλία, από τον δημοσιογράφο Roland Moreno, μία ιδέα για μία κάρτα με ενσωματωμένο κύκλωμα. Έτσι γεννήθηκε η έξυπνη κάρτα Οι έξυπνες κάρτες αναπτύχθηκαν ανεξάρτητα στην Γερμανία (1967), όπου το 1968, οι Γερμανοί εφευρέτες Jórgen Dethloff και ο Helmut Grftrupp υπέβαλαν αίτηση για τα πρώτα (ICC) σχετικά διπλώματα ευρεσιτεχνίας, στην Ιαπωνία (1970) από τον Kunitaca Arimura που αρχειοθέτησε το πρώτο δίπλωμα ευρασιτεχνίας για την έξυπνη κάρτα και στις Η.Π.Α. (1972).

Οι έξυπνες κάρτες άνθισαν τη δεκαετία του 1980. Στο διάστημα 1982-84 η Cartes Bancaire (Ένωση Τραπεζικών Καρτών της Γαλλίας) έτρεξε το πρώτο πιλοτικό πρόγραμμα για έξυπνες κάρτες. Η Ένωση συνεργάστηκε με τις εταιρείες Bull, Philips και Schlumberger κάνοντας δοκιμές στις Γαλλικές πόλεις Blois, Caen και Lyon. Οι δοκιμές είχαν τεράστια επιτυχία και μόνο ελάσσονα προβλήματα. Μία βελτίωση που προέκυψε από το πιλοτικό πρόγραμμα ήταν η ενσωμάτωση της μαγνητικής λωρίδας, ώστε να διατηρηθεί η συμβατότητα με τα τότε υπάρχοντα συστήματα.

Το 1984, οι γαλλικές ταχυδρομικές και τηλεπικοινωνιακές υπηρεσίες (PTT) επιτυχώς πραγματοποίησαν μια υπαίθρια δοκιμή με τις τηλεφωνικές κάρτες. Μέχρι το 1986, πολλά εκατομμύρια των γαλλικών τηλεφωνικών έξυπνων καρτών ήταν στην κυκλοφορία. Ο αριθμός τους έφθασε σε σχεδόν 60 εκατομμύρια το 1990, και 150 εκατομμύρια προβλήθηκαν το 1996.

Μετά την πολύ πετυχημένη δοκιμή, οι Γαλλικές τράπεζες εισήγαγαν τη χρήση των έξυπνων καρτών για τραπεζικές λειτουργίες στο ευρύ κοινό. Η χρήση αυτή είναι το πρώτο παράδειγμα δημόσιας λειτουργίας των έξυπνων καρτών για τραπεζικές λειτουργίες. Παράλληλα, έγινε μία μεγάλη διαφημιστική εκστρατεία, οπότε και καθιερώθηκε ο όρος «έξυπνη κάρτα» (smart card).Επίσης αξίζει να σημειωθεί ότι το 1993 η Γερμανική αρχή κοινωνικής ασφάλισης και η γνώση γιατρών Ταμείων ασθένειας άρχισαν μια κάρτα υγείας σε κάθε Γερμανό πολίτη (δηλαδή περίπου 79 εκατομμύρια).

13.1 ΟΡΙΣΜΟΣ ΕΞΥΠΝΗΣ ΚΑΡΤΑΣ [73]

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.

ΕΙΚΟΝΑ 13 : Μια έξυπνη κάρτα

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

Ο όρος "έξυπνη κάρτα" γενικά αναφέρεται σε μια πλαστική κάρτα διαστάσεων 85x53mm, η οποία περιέχει ένα ενσωματωμένο module που έχει δημιουργηθεί από ένα chip.

Αυτό το chip ημιαγωγού μπορεί να λειτουργεί ως μνήμη (κάρτα μνήμης), ή/ και ως επεξεργαστής (κάρτα μικροελεγκτή). Αν και οι κάρτες μικροελεγκτή είναι αυτές που πραγματικά αντιπροσωπεύουν τον όρο "έξυπνη κάρτα", στις μέρες μας η έκφραση "έξυπνη κάρτα" χρησιμοποιείται για τις κάρτες μνήμης και τις κάρτες μικροελεγκτών παρομοίως.

❖ Chip [74]

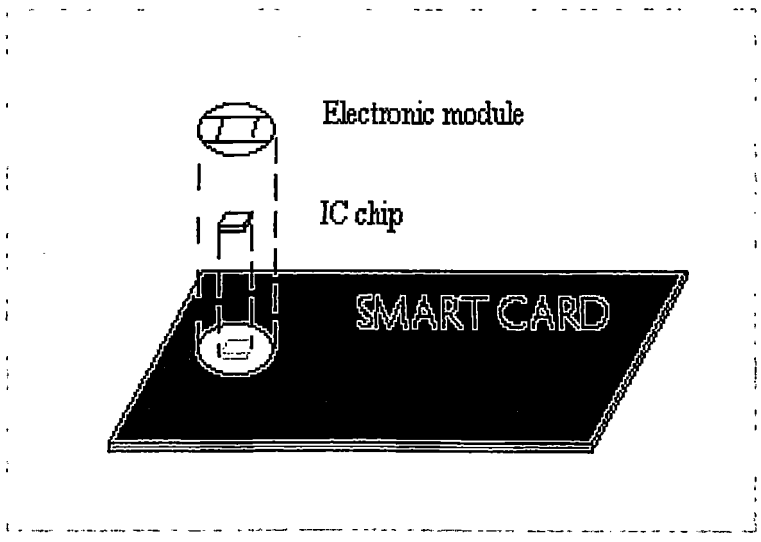
Το chip είναι κρύσταλλος πυριτίου σε μορφή λεπτού ελάσματος που περιέχει ένα ηλεκτρονικό κύκλωμα μονού ημιαγωγού. Στη βιβλιογραφία συχνά χρησιμοποιούνται αρκετές εναλλακτικές εκφράσεις για τα chips όπως: IC (ολοκληρωμένο κύκλωμα), μικροελεγκτής (microcontroller) ή microchip. Το πρώτο chip αναπτύχθηκε το 1950 από τους Jack Kilby (Texas Instruments) και Robert Noyce (Fairchild Semiconductor).

Το βασικό υλικό για την παραγωγή chips είναι άμμος χαλαζία. Αυτή υπόκειται σε διαδικασία επεξεργασίας, ώστε να διαχωριστεί πρώτα από όλα το πυρίτιο. Έπειτα ακολουθεί ο σχηματισμός πολυκρυστάλλων πυριτίου υψηλής καθαρότητας και τέλος το επονομαζόμενο wafer πυριτίου. Το wafer είναι η βάση για την κατασκευή ενός chip. Στην αλληλουχία επεξεργασιών μεγάλης πολυπλοκότητας και συνθετότητας, είναι εφικτή η δημιουργία ενός μεγάλου αριθμού ταυτόσημων ηλεκτρονικών κυκλωμάτων πάνω στο wafer, του οποίου το πλάτος είναι λίγα εκατοστά. Η επιφάνεια ενός chip μπορεί να φτάσει τα 25 τετραγωνικά χιλιοστά και μπορεί να περιέχει εκατομμύρια ηλεκτρονικά στοιχεία (τρανζίστορς).

Τα chips χρησιμοποιούνται σε πολλές εφαρμογές, όπως για παράδειγμα σε στερεοφωνικές συσκευές και συσκευές βίντεο, προϊόντα τηλεπικοινωνιών, αυτοκίνητα και έξυπνες κάρτες.

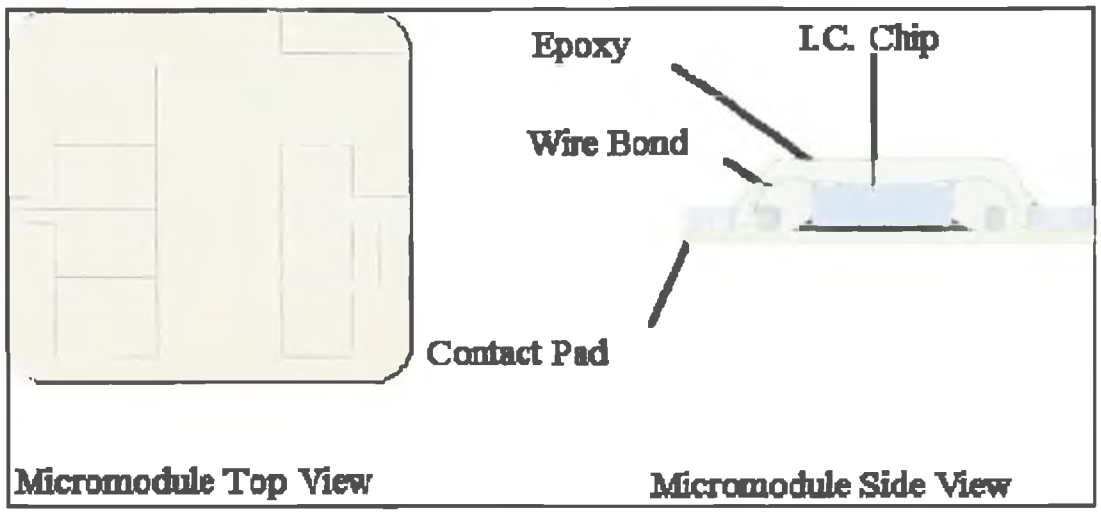
❖ Module

Για να μπορεί ένα chip να συνδεθεί με άλλες ηλεκτρονικές συσκευές, πρέπει πρώτα να συνδεθεί με μια επιφάνεια επαφής. Ένα τέτοιο στοιχείο καλείται chip module. Αυτό σημαίνει ότι το chip module είναι προ-προϊόν, το οποίο έχει άμεση εφαρμογή στη παραγωγική διαδικασία της έξυπνης κάρτας. Τα modules σήμερα, έχουν φυσιολογικά από έξι μέχρι οκτώ επιφάνειες επαφής. Η επιλογή του module εξαρτάται από τις διαστάσεις του χρησιμοποιούμενου chip. Τα modules διαχωρίζονται αναλόγως με τη μορφή τους (TAB module, chip-on-flex module, leadframe, chip-on-surface) και με τη μέθοδο μετάδοσης δεδομένων (chip module επαφής, χωρίς επαφή, διπλής διεπαφής).



ΕΙΚΟΝΑ 14 : Το module και το chip μιας έξυπνης κάρτας.

Όταν μια έξυπνη κάρτα εισάγεται σε μια συσκευή υποδοχής καρτών (reader), οι μεταλλικές επαφές έρχονται σε επαφή με τα αντίστοιχα μεταλλικά σημεία της συσκευής, με αποτέλεσμα να μπορεί να επιτευχθεί επικοινωνία μεταξύ κάρτας και συσκευής. Οι έξυπνες κάρτες πρέπει πάντα να ρυθμίζονται ξανά όταν εισάγονται σε έναν αναγνώστη. Αυτή η ενέργεια αναγκάζει την έξυπνη κάρτα να ανταποκριθεί με την αποστολή ενός μηνύματος «Answer-to-Reset» (ATR),[που θα αναλύσουμε στο κεφάλαιο 15.1.3] που ενημερώνει τη συσκευή σχετικά με τους κανόνες, που καθορίζουν την επικοινωνία με την κάρτα και την επεξεργασία της συναλλαγής.



ΕΙΚΟΝΑ 15 : Οι όψεις του module μιας έξυπνης κάρτας

❖ **ΤΑ ΤΜΗΜΑΤΑ ΤΟΥ MODULE** [75]

Το micromodule στην έξυπνη κάρτα αποτελείται από ορισμένα βασικά συστατικά που της επιτρέπουν να εκτελεί διάφορες εντολές.

- **Microprocessor Unit (MPU)**: εκτελεί τις προγραμματισμένες εντολές. Οι παλαιότερες εκδόσεις έξυπνων καρτών χαρακτηρίζονταν από σχετικά αργούς, οκτάμπιτους ενσωματωμένους ελεγκτές. Κατά τη διάρκεια της δεκαετίας του '90 άρχισαν να χρησιμοποιούνται ελεγκτές με έναν τριανταδυάμπιτο RISC (Reduced Instruction Set Computing) επεξεργαστή που τρέχει στα 25-32 MHz.

- **I/O ελεγκτής (I/O Controller):** διαχειρίζεται τη ροή των στοιχείων μεταξύ της συσκευής αποδοχής καρτών και του μικροεπεξεργαστή.

- **Μνήμη μόνο για ανάγνωση (ROM- Read Only Memory):** είναι η μνήμη στην οποία αποθηκεύονται από τον κατασκευαστή μόνιμα εντολές, οι οποίες αποτελούν τη βάση του Λειτουργικού Συστήματος της κάρτας (Chip Operating System - COS). Παραδείγματα τέτοιων εντολών είναι η ενεργοποίηση της παροχής ηλεκτρικού ρεύματος και του προγράμματος που διαχειρίζεται τον κωδικό πρόσβασης.

- **Μνήμη τυχαίας προσπέλασης (RAM- Random Access Memory):** χρησιμεύει στην προσωρινή αποθήκευση των αποτελεσμάτων από τους υπολογισμούς ή την επικοινωνία εισόδου / εξόδου. Η RAM χάνει τα περιεχόμενά της σε περίπτωση διακοπής της παροχής ηλεκτρικού ρεύματος.

- **Μνήμη Εφαρμογής (Application Memory):** σχεδόν πάντα είναι μια διπλή **EPROM** (Electrically Erasable Programmable Read-Only Memory), της οποία τα περιεχόμενα μπορούν να διαγραφούν/ γραφτούν /ενημερωθούν μόνο ηλεκτρονικά. Σύμφωνα με τα διεθνή πρότυπα, αυτή η μνήμη πρέπει να διατηρήσει τα στοιχεία της μέχρι και 10 έτη και να υποστηρίξει τουλάχιστον 10.000 ενέργειες ανάγνωσης-γραφής κατά τη διάρκεια της ζωής της κάρτας.Για κάθε εφαρμογή που φιλοξενείται στην κάρτα χρησιμοποιείται μέρος της μνήμης εφαρμογής για να καταχωρηθούν οι πληροφορίες που την αφορούν.

13.2 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΩΝ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ [76]

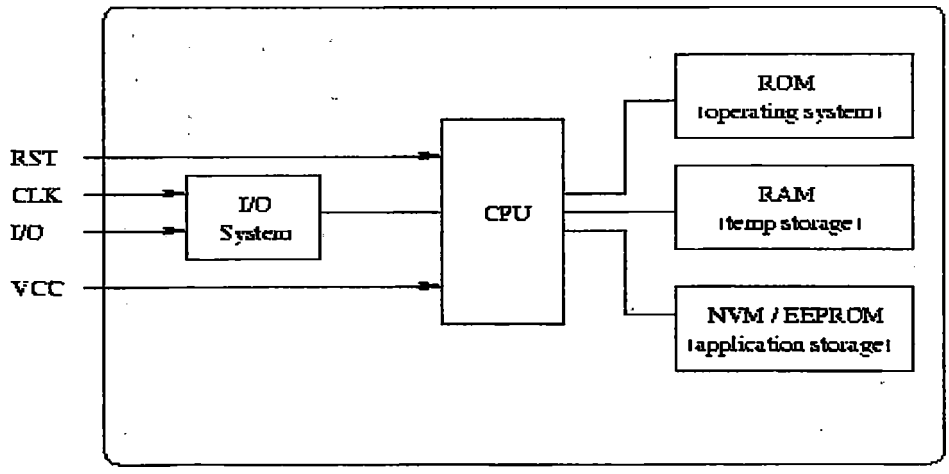
Οι έξυπνες κάρτες λόγω του ενσωματωμένου τσιπ αποτελούν μια πρόκληση όσον αφορά την σχεδίαση της αρχιτεκτονική τους η οποία βασίζεται :

- στη μονάδα επεξεργασίας ,
- στο σύστημα μνήμης ,
- στις συσκευές διεπαφών και
- στη μονάδα εισόδου εξόδου.

➢ ΜΟΝΑΔΑ ΚΕΝΤΡΙΚΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ

Παραδοσιακά η μονάδα κεντρικής επεξεργασίας είναι ένας οκτάμπιτος μικροελεγκτής που χρησιμοποιεί όλοένα και περισσότερο ισχυρότερα τσιπ των 16 και των τριανταδυο bit. Εντούτοις, κανένας δεν έχει τα πολυνηματώδη και άλλα ισχυρά χαρακτηριστικά γνωρίσματα που είναι κοινά στους τυποποιημένους υπολογιστές.

Η μονάδα κεντρικής επεξεργασίας CPU μιας έξυπνης κάρτας εκτελεί τις οδηγίες μηχανών με μια ταχύτητα περίπου 1 MIPS. Ένας συνεπεξεργαστής συμπεριλαμβάνεται συχνά για να βελτιώσει την ταχύτητα των υπολογισμών κρυπτογράφησης.



ΕΙΚΟΝΑ 16 : Αρχιτεκτονική μιας έξυπνης κάρτας

➢ ΣΥΣΤΗΜΑ ΜΝΗΜΗΣ

Υπάρχουν τρεις κύριοι τύποι μνημών στις κάρτες:

- RAM. 1K. Αυτό απαιτείται για γρήγορους υπολογισμούς και όταν χρειάζεται να δωθεί κάποια απάντηση. Μόνο ένα μικροσκοπικό ποσό είναι διαθέσιμο.

- EEPROM (ηλεκτρικά εξαλείψιμο PROM). Μεταξύ 1 και 24K. Αντίθετα από το RAM, το περιεχόμενό του δεν χάνεται όταν χάνεται το ρεύμα. Οι εφαρμογές μπορούν να ανατρέξουν και να το ξαναγράψουν, αλλά είναι πολύ αργό.

- ROM. Μεταξύ 8 και 24K. Εδώ αποθηκεύονται το λειτουργικό σύστημα και άλλα βασικά στοιχεία του λογισμικού όπως οι αλγόριθμοι κρυπτογράφησης.

➢ **ΣΥΣΚΕΥΕΣ ΔΙΕΠΑΦΩΝ (Interface Devices -IFDS)**

Οι έξυπνες κάρτες για να τρέξουν τα προγράμματα, χρειάζονται μία συσκευή ανάγνωσης διεπαφών - συνήθως έναν αναγνώστη έξυπνων καρτών –που έρχεται σε επαφή με την κάρτα. Αυτό προφανώς σημαίνει ότι μια έξυπνη κάρτα δεν είναι τίποτα περισσότερο από μια συσκευή αποθήκευσης.

Ο αναγνώστης είναι αρμόδιος για το άνοιγμα ενός καναλιού επικοινωνίας μεταξύ των προγραμμάτων εφαρμογών του υπολογιστή και του λειτουργικού συστήματος της κάρτας. Σχεδόν όλοι οι αναγνώστες έξυπνων καρτών είναι πραγματικά αναγνώστες/ συγγραφείς, δηλαδή επιτρέπουν σε μια εφαρμογή να γράψει στην κάρτα καθώς επίσης και να διαβάσουν από αυτήν.

Το κανάλι επικοινωνίας σε μια έξυπνη κάρτα είναι ημιαμφίδρομο. Αυτό σημαίνει ότι τα στοιχεία μπορούν είτε να ρεύσουν από το IFD στην κάρτα είτε από την κάρτα στο IFD αλλά τα στοιχεία δεν μπορούν να ρεύσουν και στις δύο κατευθύνσεις συγχρόνως. Ο δέκτης απαιτείται να επιλέξει το σήμα στην τμηματική γραμμή στο ίδιο ποσοστό με αυτό του αποστολέα έτσι ώστε να ληφθούν τα σωστά στοιχεία. Αυτό το ποσοστό είναι γνωστό ως ποσοστό δυαδικών ψηφίων.

➢ **ΕΙΣΟΔΟΣ /ΕΞΟΔΟΣ I/O**

Αυτό γίνεται μέσω μιας ενιαίας θύρας (I/O-Input/Output) εισόδου / εξόδου που ελέγχεται από τον επεξεργαστή για να εξασφαλίσει ότι οι επικοινωνίες είναι τυποποιημένες, υπό μορφή APDUs (μια μονάδα στοιχείων πρωτοκόλλου).

13.3 ΒΑΣΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΩΝ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ [77]

Τα χαρακτηριστικά των καρτών που αξίζει κανείς να σημειώσει είναι τα παρακάτω:

- Κόστος

Το κόστος ανά κάρτα αυξάνεται ανάλογα με τις ικανότητες που διαθέτει το chip της κάρτας και μειώνεται όταν η ποσότητα των καρτών που παραγγέλλονται μεγαλώνει.

- Αξιοπιστία

Οι προμηθευτές εγγυώνται 10.000 ενέργειες ανάγνωσης/ γραφής. Οι κάρτες που ανταποκρίνονται στις προδιαγραφές διεθνών προτύπων (ISO) πρέπει να έχουν ορισμένη συμπεριφορά σε θέματα όπως θερμοκρασία, υγρασία, στατική ηλεκτρική ενέργεια, υπεριώδη ακτίνα, την ακτίνα X, κάμψη και γδάρσιμο.

- Διόρθωση Σφαλμάτων

Τα σύγχρονα λειτουργικά συστήματα καρτών (Chip Operating Systems - COS) πραγματοποιούν έλεγχο σφαλμάτων. Κάθε φορά που δίνεται μια εντολή από το τερματικό στην κάρτα, το λειτουργικό σύστημα του τερματικού πρέπει να ελέγξει τον κωδικό κατάστασης (2 bytes) που επιστρέφει το COS (όπως καθορίζεται από το ISO 7816-4). Σε περίπτωση σφαλμάτων, το τερματικό λαμβάνει τα απαραίτητα διορθωτικά μέτρα.

- Ικανότητα Αποθήκευσης

EEPROM: 8K - 128K. (Σημειώστε 1Kbit = 1.000.000bits). Υπάρχουν σύγχρονες τεχνικές συμπίεσης που επιτρέπουν αποθήκευση στην κάρτα περισσότερων στοιχείων.

- Ευκολία Χρήσης

Οι έξυπνες κάρτες είναι φιλικές προς το χρήστη και χρησιμοποιούνται όπως και οι κάρτες τραπεζών με τις οποίες είναι εξοικειωμένοι οι χρήστες.

- Ασφάλεια

Οι έξυπνες κάρτες είναι ιδιαίτερα ασφαλείς. Επειδή τα δεδομένα είναι καταχωρημένα μέσα στο τσιπ είναι δύσκολο να αναπαραχθούν ή να διαγραφούν. Ο μικροεπεξεργαστής υποστηρίζει τα πρότυπα DES, 3-DES, RSA ή ECC για κρυπτογράφηση, πιστοποίηση ταυτότητας και ψηφιακή υπογραφή.

- Ταχύτητα ανάγνωσης

Το πρότυπο ISO 7816 περιορίζει το ρυθμό μετάδοσης στις κάρτες επαφής σε 9600 baud. Μερικά λειτουργικά συστήματα επιτρέπουν αλλαγή στο baud rate. Μια καλά σχεδιασμένη εφαρμογή μπορεί συχνά να ολοκληρώσει μια συναλλαγή καρτών σε ένα ή δύο δευτερόλεπτα. Η ταχύτητα των έξυπνων καρτών αναγνώρισης είναι γρήγορη και περιορίζεται μόνο από το ISO πρότυπο ταχύτητας I/O.

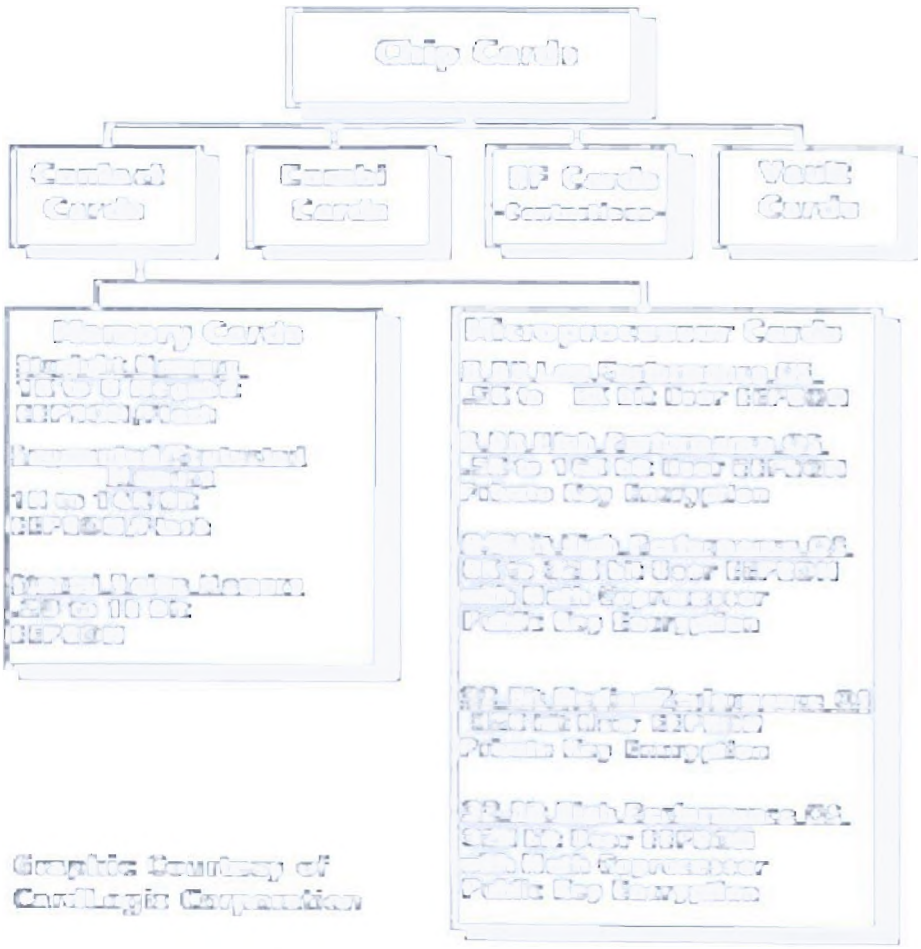
14 ΤΥΠΟΙ ΤΩΝ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ [78]

Σύμφωνα με τις βασικές αρχές της λειτουργίας καρτών ,οι σημερινές έξυπνες κάρτες χρειάζονται την ηλεκτρική δύναμη από έξω και επίσης να υπάρχει ένας τρόπος για τα στοιχεία να διαβάζονται από το τσίπ και μερικές φορές να διαβιβάζονται σε αυτό. Αλληλεπιδρούν με μια " συσκευή αποδοχής", συνήθως γνωστή ως αναγνώστης καρτών, η οποία ανταλλάσσει τα στοιχεία με την κάρτα και περιλαμβάνει συνήθως την ηλεκτρονική μεταφορά των χρημάτων ή των προσωπικών πληροφοριών. Οι πληροφορίες ή η εφαρμογή που αποθηκεύονται στο τσιπ ολοκληρωμένου κυκλώματος μεταφέρονται μέσω ενός ηλεκτρονικού module που διασυνδέεται με ένα τερματικό ή με έναν αναγνώστη καρτών.

Οι έξυπνες κάρτες ανάλογα με τη δυνατότητα εισόδου και εξόδου (ή το είδος διεπαφής του χρήστη) διακρίνονται στις εξής βασικές κατηγορίες :

Α) ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ ΜΕ ΕΠΑΦΗ
Β) ΑΝΕΠΑΦΕΣ ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ
Γ) ΥΒΡΙΔΙΚΕΣ ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ
Δ) ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ COMBI

Οι δύο τελευταίες κατηγορίες προέρχονται από την έξυπνη κάρτα με επαφή και την έξυπνη κάρτα χωρίς επαφή αντιστοίχως.

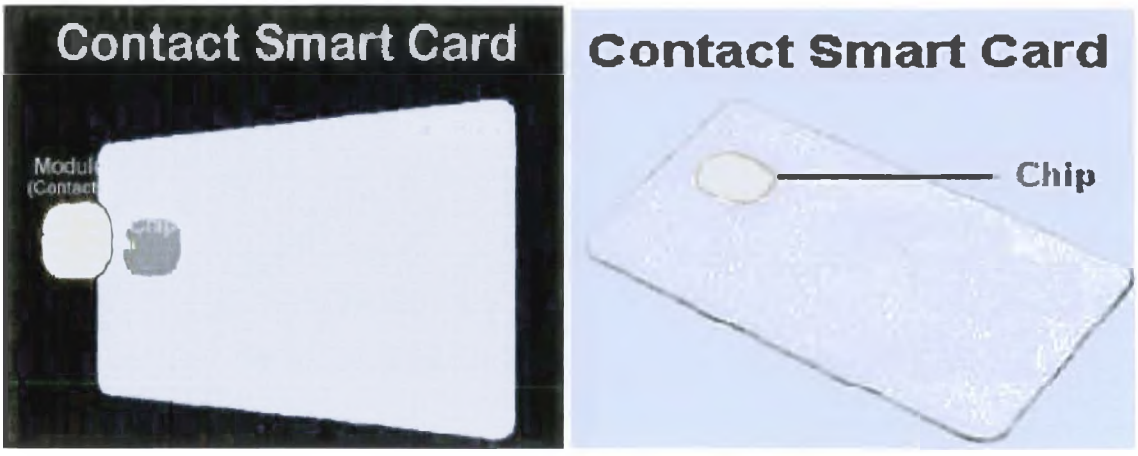


ΕΙΚΟΝΑ 17 : Τύποι των έξυπνων καρτών

14.1 ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ ΜΕ ΕΠΑΦΗ (CONTACT CARDS)[79]

Οι έξυπνες κάρτες επαφής (Contact smart cards) εισάγονται σε μια ειδική συσκευή που ονομάζεται αναγνώστης καρτών (smart card reader) και πραγματοποιείται φυσική σύνδεση μεταξύ κάρτας και συσκευής.

Μια έξυπνη κάρτα επαφών αποτελείται από το πλαστικό σώμα καρτών, το ηλεκτρικό τερματικό (οι χρυσές καλυμμένες επαφές), και ένα τσιπ , όπου το σύνολο των χρυσών καλυμμένων ηλεκτρικών επαφών είναι ενσωματωμένο στην επιφάνεια του πλαστικού σώματος στη μία μεριά .Προκειμένου να μεταφερθούν τα στοιχεία από την έξυπνη κάρτα επαφής πρέπει να παρεμβληθεί από έναν αναγνώστη έξυπνων καρτών.



ΕΙΚΟΝΑ 18 : Έξυπνες κάρτες επαφής

Η έξυπνη κάρτα επαφών χρησιμοποιείται με την εισχώρηση της κάρτας (με το σωστό προσανατολισμό) σε μια αυλάκωση σε έναν αναγνώστη καρτών, ο οποίος έχει ηλεκτρικές επαφές, που συνδέουν με τις επαφές στο πάνω μέρος των καρτών (ή όπως συνήθως λέγεται πρόσωπο καρτών). Με αυτό τα τρόπο εγκαθίσταται μια άμεση σύνδεση με το αγώγιμο micromodule στην επιφάνεια της κάρτας. Αυτή η κάρτα έχει μια επιφάνεια επαφής στο πρόσωπο, η οποία είναι ένα μικρό χρυσό τσιπ με τη μισή διάμετρο στο μπροστινό μέρος, αντί για μιά μαγνητική λωρίδα στην πλάτη όπως μια" πιστωτική κάρτα ".Όταν η κάρτα παρεμβάλλεται / εισέρχεται σε έναν αναγνώστη έξυπνων καρτών , κάνει την επαφή με έναν ηλεκτρικό ανταποκριτή για να διαβάζει και να γράφει από το τσίπ και σε αυτό. Μόνο χάρις αυτών των φυσικών σημείων επαφής η διαβίβαση εντολών και στοιχείων πραγματοποιείται.

❖ **ΧΡΗΣΕΙΣ ΕΞΥΠΝΗΣ ΚΑΡΤΑΣ ΜΕ ΕΠΑΦΗ**

Μια τέτοια κάρτα χρησιμοποιείται παραδοσιακά στη λιανική θέση πώλησης ή στο τραπεζικό περιβάλλον ή ως κάρτα GSM SIM στο «κινητό» τηλέφωνο.

❖ **ΔΙΑΚΡΙΣΕΙΣ ΕΞΥΠΝΗΣ ΚΑΡΤΑΣ ΜΕ ΕΠΑΦΗ**

Υπάρχουν δύο είδη έξυπνων καρτών με επαφή:

Α1) ΚΑΡΤΕΣ ΜΝΗΜΗΣ
Α2) ΚΑΡΤΕΣ ΜΕ ΜΙΚΡΟΕΠΕΞΕΡΓΑΣΤΗ

14.1.1 ΚΑΡΤΑ ΜΝΗΜΗΣ [80]

Μια κάρτα μνήμης περιέχει ένα τσιπ μνήμης με την ικανότητα ανάγνωσης-γραφής και σε μερικές περιπτώσεις, με μερικές λειτουργίες ασφάλειας. Αυτός ο τύπος καρτών μπορεί μόνο να αποθηκεύσει στοιχεία αφού δεν έχει καμία ικανότητα επεξεργασίας.

Περιέχουν την περιορισμένη λογική διευθύνσεων και ασφάλειας, EEPROM και ROM μνήμη. Το ROM καθορίζεται, και το EEPROM είναι για να γράφει/ σβήνει και να διαβάζει ανάλογα με τη θέληση.

Το τσιπ μνήμης που διαθέτουν χαρακτηρίζεται από τη μη- προγραμματίσιμη λογική με χωρητικότητα αποθήκευσης για δεδομένα και με ένα λογικό επίπεδο ενσωματωμένης ασφάλειας. Οι κάρτες μνήμης μπορούν να διατηρήσουν από 1-4 KB σε στοιχεία αλλά δεν έχουν κανένα επεξεργαστή στην κάρτα με τον οποίο να μπορούν να χειριστούν αυτά τα στοιχεία.

Στα απλά σχέδια καρτών, η λογική υπάρχει για να αποτρέψει το γράψιμο και το σβήσιμο των στοιχείων. Τα πιο σύνθετα σχέδια καρτών επιτρέπουν περιορισμένη πρόσβαση στην ανάγνωσης της μνήμης. Οι κάρτες μνήμης είναι λιγότερο ακριβές από τις κάρτες μικροεπεξεργαστών , αλλά είναι επίσης λιγότερο λειτουργικές αφού έχουν αντίστοιχα μειωμένη ικανότητα στη διοικητική ασφάλεια των στοιχείων. Οι κάρτες μνήμης βασίζονται στην ασφάλεια του αναγνώστη καρτών για την επεξεργασία και είναι ιδανικές στις περιπτώσεις όπου οι απαιτήσεις ασφάλειας επιτρέπουν την χρήση καρτών με χαμηλή έως μέση ασφάλεια και για χρήσεις όπου η κάρτα εκτελεί μια σταθερή λειτουργία.

❖ ΔΙΑΚΡΙΣΕΙΣ ΤΩΝ ΚΑΡΤΩΝ ΜΝΗΜΗΣ

Οι κάρτες μνήμης διαφοροποιούνται από το μέγεθος της μνήμης τους, της δομής στην οποία το στοιχείο αποθηκεύεται και του μηχανισμού από τους οποίους αυτή η μνήμη προσεγγίζεται. Υπάρχουν τρεις βασικοί τύποι καρτών μνήμης:

➢ STRAIGHT MEMORY CARDS
(Ευθεία κάρτα μνήμης)

Αυτός ο τύπος κάρτας χρησιμοποιείται απλά για να αποθηκεύσει τις πληροφορίες και δεν έχει καμία απολύτως ικανότητα επεξεργασίας. Δεν παρέχει καμία ασφάλεια και δεν μπορεί ούτε να προσδιοριστεί στον αναγνώστη καρτών, οπότε το σύστημα οικοδεσποτών πρέπει να ξέρει εκ των προτέρων ποιος τύπος κάρτας έχει εισαχθεί. Έχει το όφελος της υψηλής ικανότητας αποθήκευσης στοιχείων ενώ έχει το χαμηλότερο κόστος ανά bit μνήμης όλων των έξυπνων καρτών.

➢ STORED VALUE MEMORY CARDS
(Κάρτα μνήμης αποθηκευμένης αξίας)

Οι κάρτες αυτές σχεδιάστηκαν για να ικανοποιήσουν συγκεκριμένες ανάγκες αποθήκευσης τιμών (value) ή «κουπονιών» (tokens). Υπάρχει η δυνατότητα επαναφόρτωσης τιμής, μπορεί να είναι δηλαδή rechargeable. Στις περισσότερες από αυτές τις κάρτες ορίζονται τα μέτρα της ασφάλειάς τους από τον κατασκευαστή. Τα μέτρα αυτά περιλαμβάνουν κωδικούς (password keys) κάποιου είδους λογική στο chip. Τα περιεχόμενα της μνήμης τους είναι συνήθως ένας μετρητής και δεν υπάρχει ελεύθερος χώρος για καμία άλλη εφαρμογή.

Στην περίπτωση μιας απλής εφαρμογής όπως μια τηλεκάρτα το chip μνήμης θα έχει π.χ. 100 κελιά, ένα για κάθε τηλεφωνική μονάδα. Κάθε κελί «καθαρίζεται» μόλις η τηλεφωνική μονάδα χρησιμοποιηθεί.

Όταν όλες οι μονάδες χρησιμοποιηθούν η κάρτα είναι άχρηστη και δε μπορεί να χρησιμοποιηθεί. Στην περίπτωση όμως μιας rechargeable κάρτας, θα μπορούσε κανείς να την «ξαναγεμίσει» με μονάδες.

➢ **PROTECTED / SEGMENTED MEMORY CARDS**
(Προστατευμένες / τετμημένες κάρτες μνήμης)

Οι προστατευμένες κάρτες διαθέτουν κάποια λογική για να μπορέσουν να ελέγξουν την πρόσβαση στα περιεχόμενά τους. Μπορεί κανείς να ορίσει προστασία κατά την εγγραφή ή την ανάγνωση της κάρτας, ή ακόμη και στις δυο περιπτώσεις. Αυτό γίνεται με τη βοήθεια ενός κωδικού ή ενός κλειδιού συστήματος (system key).

Στην περίπτωση που είναι τετμημένες τότε η μνήμη της κάρτας μπορεί να διαιρεθεί σε λογικά τμήματα, καθένα από τα οποία μπορεί να φιλοξενήσει τα περιεχόμενα διαφορετικών εφαρμογών (multi-functionality).

❖ **ΧΡΗΣΕΙΣ ΚΑΡΤΩΝ ΜΝΗΜΗΣ**

Οι κάρτες μνήμης αντιπροσωπεύουν τον όγκο των έξυπνων καρτών που πωλούνται πρώτιστα για τις εφαρμογές μίας χρήσης προπληρωμένων καρτών όπως οι προπληρωμένες τηλεφωνικές κάρτες. Αυτές είναι δημοφιλείς ως εναλλακτικές λύσεις υψηλής-ασφάλειας στις μαγνητικές κάρτες λωρίδων.

Η επικοινωνία των καρτών μνήμης με τους αναγνώστες γίνεται με πρωτόκολλα σύγχρονης μετάδοσης που θα αναλυθούν στο κεφάλαιο 15.1.3 στη σελίδα 144.

❖ **ΕΙΔΙΚΟΙ ΤΥΠΟΙ ΚΑΡΤΩΝ ΜΝΗΜΗΣ**

1) ΟΠΤΙΚΗ ΚΑΡΤΑ ΜΝΗΜΗΣ

Οι οπτικές κάρτες μνήμης μοιάζουν με μία κάρτα με ένα κομμάτι του cd που κολλιέται στην κορυφή (που κάτι τέτοιο βασικά είναι).Οι οπτικές κάρτες μνήμης μπορούν να αποθηκεύσουν μέχρι 4 MB των στοιχείων. Αλλά μόλις γραφτούν, τα στοιχεία δεν μπορούν να αλλάξουν ή να αφαιρεθούν.

Επειδή οι συσκευές για ανάγνωση και γραφή αυτών των καρτών είναι πολύ ακριβές οι εφαρμογές τους είναι αρκετά περιορισμένες.

❖ **ΧΡΗΣΕΙΣ ΟΠΤΙΚΩΝ ΚΑΡΤΩΝ ΜΝΗΜΗΣ**

Αυτός ο τύπος κάρτας είναι ιδανικός για την τήρηση αρχείων - παραδείγματος χάριν ιατρικά αρχεία, στοιχεία οδήγησης, ή ιστορίες ταξιδιού.

2) ΚΑΡΤΑ ΕΥΦΥΟΥΣ ΜΝΗΜΗΣ

Οι κάρτες ευφυούς μνήμης ή όπως αλλιώς λέγονται «καλωδιομένες κάρτες λογικής» περιέχουν επίσης κάποια ενσωματωμένη λογική που συνήθως χρησιμοποιείται για να ελέγξει την πρόσβαση στη μνήμη της κάρτας.

14.1.2 ΚΑΡΤΕΣ ΜΕ ΜΙΚΡΟΕΠΕΞΕΡΓΑΣΤΗ [81]
(CPU/ MPU MICROOPROCESSOR MULTIFUNCTION CARDS)

Οι κάρτες αυτές διαφέρουν από όλες τις υπόλοιπες, γιατί έχουν δυνατότητες επεξεργασίας στο εσωτερικό τους. Γίνεται κατανομή της μνήμης της κάρτας σε διάφορα ανεξάρτητα τμήματα, καθένα από τα οποία αφιερώνεται σε κάποια συγκεκριμένη εφαρμογή ή λειτουργία.

Στο εσωτερικό της κάρτας υπάρχει ένα chip μικροεπεξεργαστή ή μικρό-ελεγκτή που διαχειρίζεται την κατανομή της μνήμης και τη διαχείριση των αρχείων. Ο τύπος αυτό chip είναι παρόμοιος με αυτούς που συναντά κανείς σε έναν προσωπικό υπολογιστή. Όταν ενσωματώνεται σε μια έξυπνη κάρτα τότε οργανώνει και διαχειρίζεται τα δεδομένα σε δομές αρχείων υπό την καθοδήγηση του Λειτουργικού Συστήματος της κάρτας (Card Operating System - COS).

Το λειτουργικό αυτό σύστημα [που θα αναλυθεί στο κεφάλαιο 16] ελέγχει την πρόσβαση στη μνήμη που υπάρχει στην κάρτα, με αποτέλεσμα να υπάρχει η δυνατότητα αποθήκευσης στην κάρτα πολλών διαφορετικών εφαρμογών, που ανήκουν σε διαφορετικές επιχειρήσεις. Τα χαρακτηριστικά λοιπόν της κάρτας αυτής ευνοούν την ανάπτυξη μιας κάρτας πολλαπλών εφαρμογών που παρέχει πρόσβαση σε πολλαπλές υπηρεσίες.

Μια έξυπνη κάρτα περιέχει μια ΚΜΕ, ένα RAM, ένα EEPROM, και ένα ROM (είναι λειτουργικό σύστημα).Μια έξυπνη κάρτα είναι ένας "υπολογιστής σε ένα τσιπ".

Αυτός ο "υπολογιστής σε ένα τσιπ" επιτρέπει τη μετάδοση, την αποθήκευση και την επεξεργασία των στοιχείων με την υψηλή ασφάλεια. Τα συστήματα λογικής λειτουργίας και ασφάλειας της κάρτας εποπτεύουν τη μετάδοση στοιχείων πέρα από την τμηματική διεπαφή. Αυτές οι λειτουργίες μνήμης του γραψίματος, του σβησίματος, και της ανάγνωσης ελέγχονται.

ROM - μνήμη μόνο για ανάγνωση : αυτός ο τύπος μνήμης μπορεί να γραφτεί μόνο μιά φορά κατά τη διάρκεια της παραγωγής. Το ROM μιας έξυπνης κάρτας περιέχει το μεγαλύτερο μέρος του λειτουργικού συστήματος, καθώς επίσης και τις διαγνωστικές και εξεταστικές λειτουργίες. Το ROM δημιουργεί το "ασφαλές λειτουργικό σύστημα" για τις έξυπνες κάρτες.

EEPROM - ηλεκτρική εξαλείψιμη προγραμματίσιμη μνήμη μόνο για ανάγνωση : αυτός ο τύπος μνήμης χρησιμοποιείται στις έξυπνες κάρτες για όλα τα στοιχεία και τα προγράμματα που πρέπει να τροποποιηθούν ή να διαγραφούν. EEPROM λειτουργεί όπως έναν σκληρό δίσκο σε ένα PC. Τα στοιχεία θα παραμείνουν στη μνήμη ακόμα και όταν δεν υπάρχει ρεύμα.

RAM - τυχαία μνήμη πρόσβασης : αυτό είναι η μνήμη της έξυπνης κάρτας κατά τη διάρκεια μιας συνόδου. Μόλις το ρεύμα χάνεται, το RAM θα καθαριστεί όλων των στοιχείων.

ΚΜΕ - μονάδα κεντρικής επεξεργασίας : αυτό είναι η συσκευή στην έξυπνη κάρτα που ερμηνεύει και εκτελεί τις οδηγίες. Είναι ο εγκέφαλος.

Οι κάρτες μικροεπεξεργαστών (γενικά ονομαζόμενες και ως «κάρτες τσιπ» προσφέρουν μεγαλύτερη αποθήκευση μνήμης και μεγαλύτερη ασφάλεια δεδομένων από μια παραδοσιακή μαγνητική κάρτα λωρίδων. Τα τσιπ αυτών των καρτών μπορούν επίσης να κληθούν ως μικροεπεξεργαστές με την εσωτερική μνήμη που,

εκτός από τη μνήμη, ενσωματώνουν έναν επεξεργαστή που ελέγχονται από ένα λειτουργικό σύστημα καρτών, με τη δυνατότητα να υποβληθούν σε επεξεργασία τα στοιχεία του τσιπ.

❖ ΧΡΗΣΕΙΣ ΚΑΡΤΩΝ ΜΕ ΕΠΕΞΕΡΓΑΣΤΗ

Αυτές οι κάρτες χρησιμοποιούνται για ποικίλες εφαρμογές, ειδικά εκείνες που ενσωματώνουν το σύστημα κρυπτογραφίας, το οποίο απαιτεί το χειρισμό των μεγάλων αριθμών. Πολύ συχνά η δύναμη επεξεργασίας δεδομένων χρησιμοποιείται για να κρυπτογραφήσει/ αποκρυπτογραφεί τα στοιχεία, το οποίο κάνει αυτόν τον τύπο καρτών πολύ μοναδικό για το προσδιορισμού των προσώπων.

Η επεξεργασία δεδομένων επιτρέπει επίσης τη δυναμική διαχείριση αποθήκευσης, η οποία επιτρέπει την πραγματοποίηση της εύκαμπτης πολυσύνθετης κάρτας. Κατά συνέπεια, οι κάρτες τσιπ είναι η κύρια πλατφόρμα για τις κάρτες που κρατούν μια ασφαλή ψηφιακή ταυτότητα. Ως εκ τούτου είναι σε θέση να προσφέρουν τον προηγμένο μηχανισμό ασφάλειας, την τοπική επεξεργασία δεδομένων, το σύνθετο υπολογισμό και άλλες διαλογικές διαδικασίες. Οι περισσότερες κάρτες αποθηκευμένης-αξίας που είναι ενσωματωμένες με ικανότητες προσδιορισμού, ασφάλειας και πληροφόρησης είναι κάρτες επεξεργαστών.

❖ Μερικά παραδείγματα αυτών των καρτών είναι :

- κάρτες που κρατούν τα χρήματα ("αποθηκευμένης κάρτες αξίας").
- κάρτα που κρατά τα αντίτιμα χρημάτων (παραδείγματος χάριν, "κάρτες συγγένειας").
- κάρτες που παρέχουν την ασφαλή πρόσβαση σε ένα δίκτυο κάρτες που εξασφαλίζουν τα κυψελοειδή τηλέφωνα από την απάτη.
- κάρτες που επιτρέπουν στους μετασχηματιστές στις τηλεοράσεις για να παραμείνουν ασφαλείς από την πειρατεία.

❖ ΕΙΔΙΚΟΣ ΤΥΠΟΣ ΚΑΡΤΑΣ ΜΕ ΜΙΚΡΟΕΠΕΞΕΡΓΑΣΤΗ ΚΡΥΠΤΟΓΡΑΦΙΚΗ ΚΑΡΤΑ ΣΥΝΕΠΕΞΕΡΓΑΣΤΩΝ

Αν και τεχνικά αυτός ο τύπος είναι στην κατηγορία καρτών μικροεπεξεργαστών, είναι χωρισμένος εδώ λόγω των διαφορών στο κόστος και τη λειτουργία. Επειδή οι κοινοί συμμετρικοί κρυπτογραφικοί αλγόριθμοι της εποχής μας (όπως ο RSA) απαιτούν πολύ μεγάλους υπολογισμούς ακέραιων αριθμών, ένας μικροεπεξεργαστής 8 μπιτ με πολύ μικρή μνήμη RAM μπορεί να κάνει αρκετά λεπτά να εκτελέσει μια λειτουργία ιδιωτικού κλειδιού.

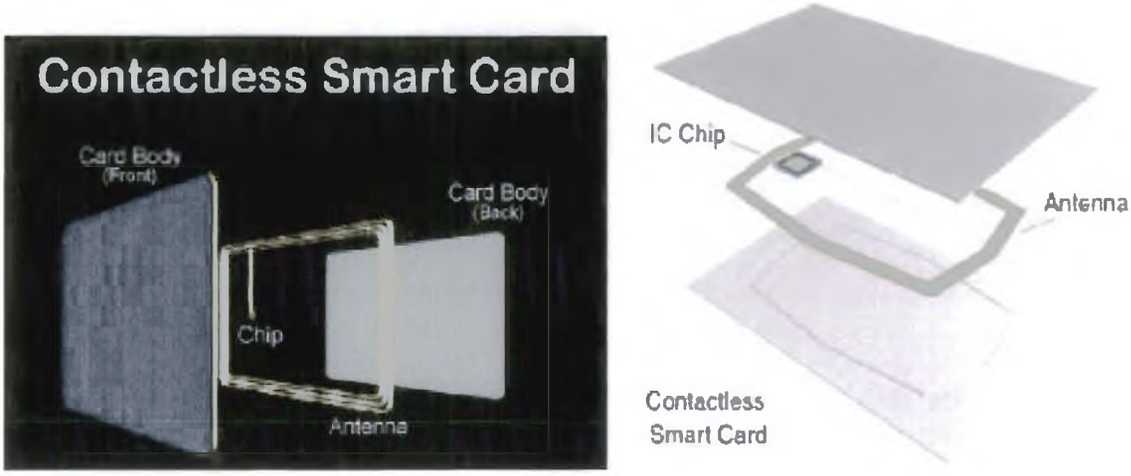
Εντούτοις, εάν ένας κρυπτογραφικός συνεπεξεργαστής προστεθεί στην αρχιτεκτονική, ο χρόνος που απαιτείται για αυτήν την ίδια λειτουργία μειώνεται γύρω σε μερικές εκατοντάδες μικροδευτερόλεπτα. Οι συνεπεξεργαστές περιλαμβάνουν πρόσθετες αριθμητικές μονάδες που αναπτύσσονται συγκεκριμένα για το μεγάλο αριθμό ακεραίων. Υπάρχει ένα μειονέκτημα, εντούτοις, και είναι το κόστος.

Η προσθήκη ενός κρυπτογραφικού συνεπεξεργαστή μπορεί να αυξήσει το κόστος των σημερινών έξυπνων καρτών κατά 50% ως 100%. Αυτές οι αυξήσεις δαπανών θα μικραίνουν πιθανώς καθώς οι συνεπεξεργαστές γίνονται πιο διαδεδομένοι.

14.2 ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ ΧΩΡΙΣ ΕΠΑΦΗ (CONTACT LESS CARDS) [82]

Αν και η αξιοπιστία των έξυπνων καρτών με επαφή έχει βελτιωθεί σε πολύ αποδεκτά επίπεδα, οι επαφές είναι ένα από τα συχνότερα σημεία αποτυχίας σε οποιοδήποτε ηλεκτρομηχανικό σύστημα λόγω ρύπων, ένδυσης, και ούτω καθ'εξής.

Η ανέπαφη κάρτα λύνει αυτό το πρόβλημα και παρέχει επίσης στον εκδότη μια ενδιαφέρουσα σειρά των νέων δυνατοτήτων κατά τη διάρκεια της χρήσης. Οι κάρτες δεν χρειάζονται πλέον να παρεμβληθούν σε έναν αναγνώστη, οι οποίες θα μπορούσαν να βελτιώσουν την αποδοχή τελικών χρηστών.



ΕΙΚΟΝΑ 19 : Ανέπαφες έξυπνες κάρτες

Μια ανέπαφη έξυπνη κάρτα αποτελείται από δύο πλαστικούς οργανισμούς καρτών, ένα τσιπ υπολογιστών, και μια σπείρα κεραιών που ενσωματώνονται μέσα στην κάρτα. Τα στοιχεία μπορούν να μεταφερθούν από την ανέπαφη κάρτα και αντίστοιχα προς την κάρτα ,με την κεραία και τη μονάδα συζευκτήρων χωρίς οποιαδήποτε φυσική επαφή.

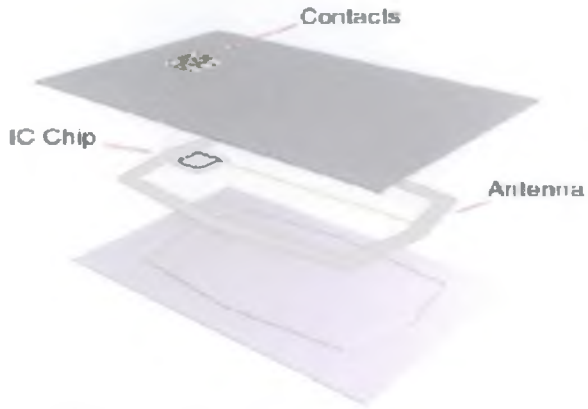
Αυτή η κεραία επιτρέπει στη κάρτα να επικοινωνήσει με μια εξωτερική κεραία στο σημείο συναλλαγής για να μεταφέρει τις πληροφορίες. Η κεραία είναι χαρακτηριστικά 3 - 5 στροφές ενός πολύ λεπτού καλωδίου (ή ενός αγώγιμου μελανιού), που συνδέονται με το ανέπαφο τσιπ. Αυτή η εναέρια σπείρα της κεραίας είναι τοποθετημένη σε στρώματα στην κάρτα και επιτρέπει την επικοινωνία ακόμη και ενώ η κάρτα βρίσκεται μέσα σε ένα πορτοφόλι ή μια τσάντα.

❖ ΧΡΗΣΕΙΣ ΕΞΥΠΝΗΣ ΚΑΡΤΑΣ ΧΩΡΙΣ ΕΠΑΦΗ

Τέτοιες έξυπνες κάρτες χρησιμοποιούνται όταν πρέπει να υποβληθούν σε επεξεργασία γρήγορα οι συναλλαγές, όπως στη συλλογή φόρου μαζικής διέλευσης ή οπουδήποτε ο κάτοχος κάρτας είναι εν κινήση τη στιγμή της συναλλαγής. Η στενή εγγύτητα, χαρακτηριστικά ένα κενό αέρος μέχρι 10cms για τις μη τροφοδοτημένες κάρτες απαιτείται για τέτοιες συναλλαγές, οι οποίες μειώνουν το χρόνο συναλλαγής και η αυξανόμενη ευκολία (αφού και ο αναγνώστης και η κάρτα έχουν κεραία) πραγματοποιούν την επικοινωνία μέσω αυτής της ανέπαφης σύνδεσης. Οι περισσότερες ανέπαφες κάρτες αντλούν επίσης την εσωτερική πηγή ενέργειας τσιπ από αυτό το ηλεκτρομαγνητικό σήμα.

14.3 ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ COMBI [83]

Η έξυπνη κάρτα combi (επίσης γνωστή ως κάρτα **διπλής-διεπαφής**) είναι μια κάρτα που συνδιάζει και διεπαφή με επαφή και ανέπαφη διεπαφή. Μπορεί να ενσωματώσει δύο τσιπ που δεν επικοινωνούν - ένα για κάθε διεπαφή - αλλά κατά προτίμηση έχει ένα ενιαίο, τσιπ διπλής-διεπαφής που παρέχει τα διάφορα πλεονεκτήματα ενός ενιαίου ηλεκτρονικού πορτοφολιού.



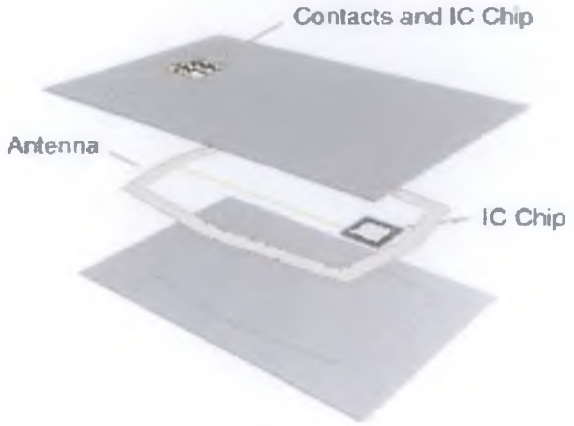
ΕΙΚΟΝΑ 20 : Έξυπνη κάρτα Combi

Η μαζική διέλευση αναμένεται να είναι μια από τις δημοφιλέστερες εφαρμογές για την κάρτα combi στην οποία ,ένας αποδέκτης τύπου επαφής μπορεί να χρησιμοποιηθεί για να τοποθετήσει μια αξία μετρητών στη μνήμη του τσιπ και η ανέπαφη διεπαφή μπορεί να χρησιμοποιηθεί για να αφαιρέσει μια τιμή από την κάρτα

14.4 ΥΒΡΙΔΙΚΕΣ ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ

Μια υβριδική έξυπνη κάρτα έχει δύο τσιπ, (ένα ανέπαφο τσιπ με την κεραία του ή /και ένα τσιπ επαφών με τα μαξιλάρια επαφών του, όλα σε μια ενιαία κάρτα) κάθε ένα με την αντίστοιχη επαφή και ανέπαφη διεπαφή.

Τα δύο τσιπ δεν συνδέονται, αλλά για πολλές εφαρμογές, αυτό το υβρίδιο εξυπηρετεί τις ανάγκες των καταναλωτών και των εκδοτών καρτών. Το ανέπαφο τσιπ χρησιμοποιείται χαρακτηριστικά για τις εφαρμογές που απαιτούν τους γρήγορους χρόνους συναλλαγής, όπως τη μαζική διέλευση. Το τσιπ επαφών μπορεί να χρησιμοποιηθεί στις εφαρμογές που απαιτούν τα πιό υψηλά επίπεδα ασφάλειας.



ΕΙΚΟΝΑ 21 : Υβριδική έξυπνη κάρτα

15 ΠΡΟΤΥΠΑ ΤΩΝ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ [84]

Η ΑΝΑΓΚΗ ΓΙΑ ΠΡΟΤΥΠΑ

Κρίνεται σημαντικό να ακολουθεί κανείς τα υπάρχοντα πρότυπα όταν πρόκειται να προχωρήσει στην υλοποίηση μιας εφαρμογής. Αυτό μας καθιστά ανεξάρτητους από τους κατασκευαστές έξυπνων καρτών ή αναγνωστών.

Πιο συγκεκριμένα, τα πρότυπα είναι απαραίτητα για τους παρακάτω λόγους:

- Προστασία του χρήστη όσον αφορά την λειτουργική συνέπεια και την ασφάλεια ενός συστήματος.
- Παροχή στον κατασκευαστή μιας ενιαίας πλατφόρμας, απαραίτητης για την διασφάλιση της διαλειτουργικότητας.
- Αποφυγή του φαινομένου της πρώιμης απόσυρσης νέων τεχνολογικών μοντέλων μετά από σύντομα χρονικά διαστήματα.
- Αποφυγή της κυριαρχίας των κατασκευαστών στην αγορά.
- Παροχή λειτουργίας σε πανευρωπαϊκό επίπεδο.
- Προστασία και εγγύηση για τον πολίτη αναφορικά με:
  - τη δυνατότητα χρησιμοποίησης.
  - την ασφάλεια.
  - την εμπιστοσύνη προς φορείς.
  - το σχεδιασμό με βάση τις ανάγκες όλων των πολιτών.

Ακολουθεί παρουσίαση των πιο σημαντικών προτύπων σχετικά με τις έξυπνες κάρτες

ΕΠΙΣΗΜΑ ΠΡΟΤΥΠΑ

15.1 ΠΡΟΤΥΠΟ ISO 7816

Η τυποποίηση των συστημάτων έξυπνων καρτών είναι μια διαδικασία που συνεχίζεται μέχρι σήμερα. Το πιο σημαντικό πρότυπο που μπορεί να αναφέρει κανείς σχετικά με τις έξυπνες κάρτες είναι η ομάδα προτύπων ISO- 7816. Πρόκειται για πρότυπα που έχουν καθιερωθεί από το Διεθνή Οργανισμό Τυποποίησης (International Standards Organization - ISO) για να περιγράψουν τις Κάρτες Αναγνώρισης (Identification Cards) - Κάρτες Ολοκληρωμένων Κυκλωμάτων με Επαφή (Integrated Circuit Cards with Contacts). Περιλαμβάνει 10 τμήματα, τα 5 πρώτα από τα οποία παρατίθενται στον ακόλουθο πίνακα:

ISO 7816	ΠΕΡΙΓΡΑΦΗ
ISO 7816-1	Φυσικά χαρακτηριστικά
ISO 7816-2	Διαστάσεις και θέση των επαφών
ISO 7816-3	Ηλεκτρονικά σήματα και πρωτόκολλα μετάδοσης
ISO 7816-4	Εντολές για την μεταφορά δεδομένων από και προς την κάρτα
ISO 7816-5	Αριθμητικό σύστημα και διαδικασίες εγγραφής για την αναγνώριση εφαρμογών

ΕΙΚΟΝΑ 22 : Τα μέρη του προτύπου ISO 7816

15.1.1 ΠΡΟΤΥΠΟ ISO 7816-1 : ΦΥΣΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ [85]

Το τμήμα αυτό του προτύπου περιγράφει τα φυσικά χαρακτηριστικά των καρτών ολοκληρωμένων κυκλωμάτων (έξυπνων καρτών). Καθορίζονται τα όρια έκθεσης σε διάφορα ηλεκτρομαγνητικά φαινόμενα όπως οι ακτίνες X, το υπεριώδες (UV) φως, τα ηλεκτρομαγνητικά πεδία, τα στατικά ηλεκτρικά πεδία, καθώς και η περιβαλλοντική θερμοκρασία της κάρτας.

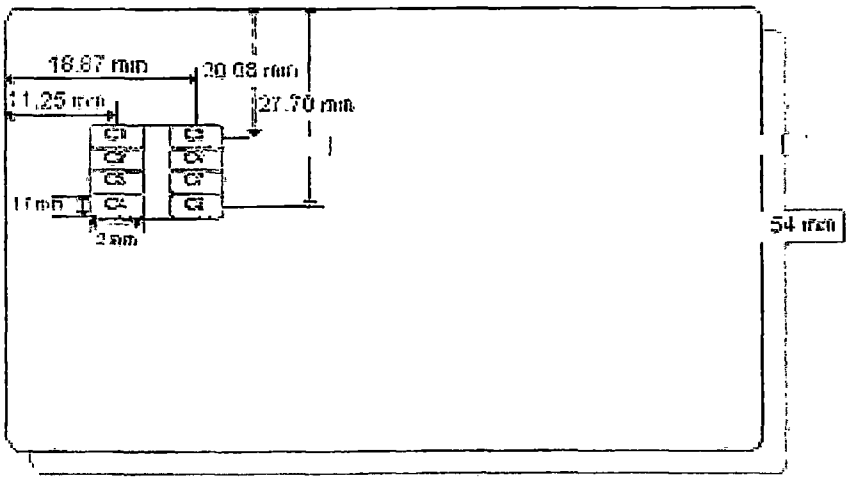
Φαινόμενο	Όριο
Υπεριώδες φως	Περιβαλλοντικό
Ακτίνες X	Δύο φορές η αποδεκτή ετήσια ανθρώπινη δόση
Ηλεκτρομαγνητική διεπαφή (EMI)	Καμία παρέμβαση με τη μαγνητική λωρίδα
Ηλεκτρομαγνητικά πεδία	Λιγότερο από 1.000 Oe
Στατική ηλεκτρική ενέργεια	Απαλλαγή 1.500 βολτ μέσω του αντιστάτη 1,5 Kohm από pF τον πυκνωτή 100
Διασκεδασμός θερμότητας	Λιγότερο από 2,5 Watt θερμοκρασία καρτών λιγότερο από

ΕΙΚΟΝΑ 23 : Όρια έκθεσης για τα φυσικά φαινόμενα

Επιπλέον το ISO7816-1 καθορίζει τα χαρακτηριστικά μιας κάρτας όταν αυτή κάμπτεται. Με τον τρόπο αυτό εξασφαλίζεται ότι οι πλαστικές κάρτες με τα ενσωματωμένα τσιπ κατασκευάζονται με τέτοιο τρόπο που εγγυάται την άψογη λειτουργία κατά τη διάρκεια του αναμενόμενου χρόνου ζωής μιας κάρτας.

Αυτό το μέρος του ISO7816-1 είναι σημαντικό κυρίως για τους κατασκευαστές καρτών, γιατί αυτοί είναι υπεύθυνοι για την επιλογή των υλικών και την καθιέρωση της διαδικασίας που ενσωματώνει το ολοκληρωμένο κύκλωμα στην κάρτα.

Ενδεικτικά αναφέρουμε και τις φυσικές διαστάσεις μιας έξυπνης κάρτας (η οποία ορίζεται ως ταυτότητα-1) οι οποίες περιγράφονται αναλυτικά στον ISO 7810. Διαστάσεις : 85,6 χιλ X 54 χιλ ,Ακτίνα γωνιών : 3.18 χιλ και Πάχος καρτών :76 χιλ.



ΕΙΚΟΝΑ 24 : Φυσικές διαστάσεις μιας έξυπνης κάρτας

15.1.2 ΠΡΟΤΥΠΟ ISO 7816-2 : ΔΙΑΣΤΑΣΕΙΣ ΚΑΙ ΘΕΣΕΙΣ ΤΩΝ ΕΠΑΦΩΝ [86]

Το δεύτερο τμήμα του ISO 7816 καθορίζει τις διαστάσεις και τη θέση των επαφών. Αυτό το μέρος περιλαμβάνει τα πρότυπα για τον αριθμό, τη λειτουργία και τη θέση των ηλεκτρικών επαφών. Η κάρτα ολοκληρωμένων κυκλωμάτων (ICC) έχει 8 ηλεκτρικές επαφές σε μια τυποποιημένη θέση στο μπροστινό μέτωπο της κάρτας.

Αυτές οι ηλεκτρονικές επαφές αναφέρονται ως C1 - C8. Δεν συνδέονται και οι 8 επαφές ηλεκτρικά με το ενσωματωμένο τσιπ μικροεπεξεργαστή και επομένως κάποιες παραμένουν αχρησιμοποίητες.

Ο ακόλουθος πίνακας περιέχει τον καθορισμό επαφών σύμφωνα με το ISO7816-2.

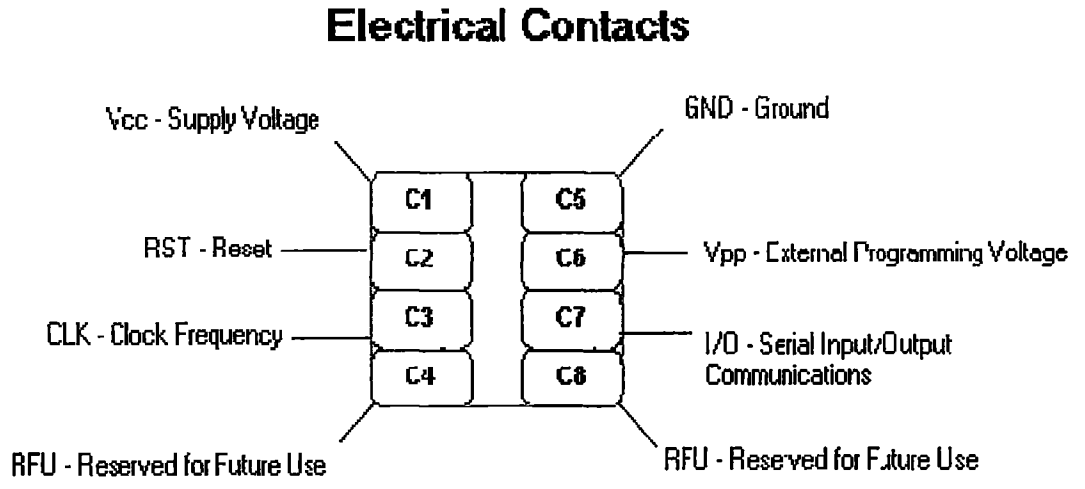
Επαφή	Ονομασία	Χρήση
C1	VCC	Σύνδεση μέσω της οποίας παρέχεται η απαραίτητη δύναμη (ισχύς) για να λειτουργήσει το τσιπ μικροεπεξεργαστή της κάρτας
C2	RST	Γραμμή αναστοιχειοθέτησης μέσω της οποίας το IFD κάνει σήμα στον μικροεπεξεργαστή της έξυπνης κάρτας για να αρχίσει η ακολουθία εντολών reset (Reset line)
C3	CLK	Γραμμή σημάτων ρολογιού που ελέγχει την ταχύτητα λειτουργίας και παρέχει ένα κοινό πλαίσιο για τη μετάδοση στοιχείων μεταξύ του IFD και του ICC (Clock signal line)
C4	RFU	Δεσμεύεται για χρήση στο μέλλον (Reserved for Future Use)
C5	GND	Επίγεια γραμμή που παρέχει το κοινό ηλεκτρικό έδαφος μεταξύ του IFD και του ICC (Ground line providing common electrical ground between the IFD and the ICC)
C6	Vpp	Σύνδεση μέσω της οποίας παρέχεται μια χωριστή πηγή ενέργειας που χρησιμοποιείται για τον προγραμματισμό της EEPROM στο τσίπ.
C7	I/O	Γραμμή εισόδου/ εξόδου που παρέχει ένα ημί-αμφίδρομο κανάλι επικοινωνίας μεταξύ του αναγνώστη και της έξυπνης κάρτας (Input/Output line)
C8	RFU	Δεσμεύεται για χρήση στο μέλλον (Reserved for Future Use)

ΕΙΚΟΝΑ 25 : Ορισμοί των επαφών ενός τσιπ μιας έξυπνης κάρτας

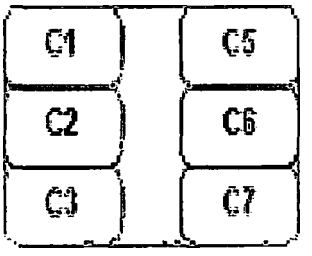
Μόνο οι επαφές I/O και GND είναι απαραίτητο σε μια κάρτα να ανταποκρίνονται στα διεθνή πρότυπα, η συμβατότητα των άλλων είναι προαιρετική.

Παρατήρηση: Μερικές έξυπνες κάρτες που εκδόθηκαν πριν από το 1990 ακολουθούσαν διαφορετικά πρότυπα όσον αφορά τη θέση των επαφών και επομένως δεν μπορούν να χρησιμοποιηθούν στους σημερινούς αναγνώστες έξυπνων καρτών που είναι συμβατοί με το πρότυπο ISO7816- 2.

Οι περισσότερες έξυπνες κάρτες έχουν οκτώ τομείς επαφών στο μπροστινό πρόσωπο, εντούτοις, δύο από αυτές είναι διατηρημένες για τη μελλοντική χρήση έτσι μερικοί κατασκευαστές παράγουν τις κάρτες με μόνο έξι τομείς επαφών, οι οποίες μειώνουν ελαφρώς τις δαπάνες παραγωγής. Οι ηλεκτρικές επαφές είναι χαρακτηριστικά αριθμημένες από C1 μέχρι C8 από το κορυφαίο αριστερό στο κατώτατο δεξιό.



ΕΙΚΟΝΑ 26 : Η θέση των ηλεκτρονικών επαφών για διαμορφώσεις 8 τομέων.



ΕΙΚΟΝΑ 27 : Η θέση των ηλεκτρονικών επαφών για διαμορφώσεις 6 τομέων.

Η επαφή Vpp χρησιμοποιήθηκε αρκετά έτη πριν για να παρέχει την τάση σε EEPROMs για τον προγραμματισμό και το σβήσιμο. Εντούτοις, με την εμφάνιση των αντλιών δαπανών που υπάρχουν στο τσιπ, η επαφή Vpp χρησιμοποιείται σπάνια σήμερα.

Η Vcc τάση ανεφοδιασμού διευκρινίζεται σε 5 βολτ ± 10%, Υπάρχει μια ώθηση της βιομηχανίας για τα πρότυπα έξυπνων καρτών να υποστηρίξουν την τεχνολογία των 3 βολτ επειδή όλα τα κινητά τηλεφωνικά τμήματα είναι διαθέσιμα σε μια διαμόρφωση των 3 βολτ, και οι έξυπνες κάρτες είναι το μόνο συστατικό που έχει απομείνει που απαιτεί ένα κινητό τηλέφωνο για να έχει έναν μετατροπέα δαπανών.

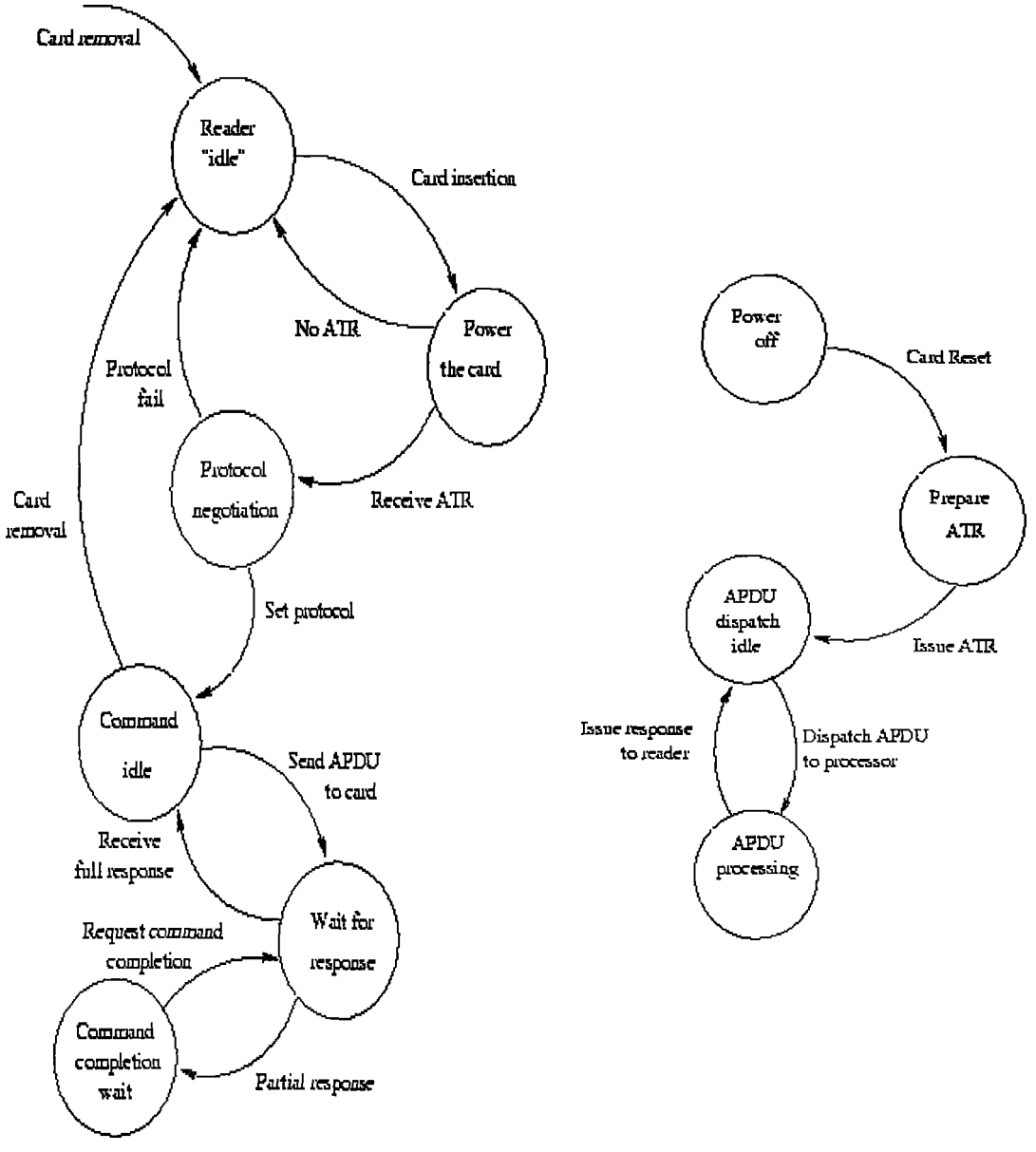
Είναι θεωρητικά δυνατό να αναπτυχθούν οι έξυπνες κάρτες των 3-βολτ, αλλά η διαλειτουργικότητα με τα τρέχοντα 5-volt συστήματα θα ήταν ένα πρόβλημα. Εν τούτοις, μια ευρύτερη σειρά τάσης που χειρίζεται 3 έως 5 βολτ θα γίνει πιθανώς υποχρεωτική στο εγγύς μέλλον.

Βασική λειτουργία αυτών των ηλεκτρονικών επαφών είναι να διαμορφώνουν τη διεπαφή μεταξύ του αναγνώστη και του μικροεπεξεργαστή της κάρτας.

15.1.3 ΠΡΟΤΥΠΟ ISO 7816-3 : ΗΛΕΚΤΡΟΝΙΚΑ ΣΗΜΑΤΑ ΚΑΙ ΠΡΩΤΟΚΟΛΛΑ ΜΕΤΑΔΟΣΗΣ [87]

Το μέρος 3 του ISO 7816 καθορίζει τα ηλεκτρικά σήματα και τα πρωτόκολλα μετάδοσης. Περιγράφει τη σχέση μεταξύ της έξυπνης κάρτας και του αναγνώστη ως μια σχέση μεταξύ σε έναν κύριο (αναγνώστης) και έναν σκλάβο (έξυπνη κάρτα).

Ο αναγνώστης καθιερώνει την επικοινωνία με την επισήμανση της έξυπνης κάρτας μέσω των ηλεκτρικών επαφών σχετικά με την κάρτα. Η έξυπνη κάρτα αποκρίνεται αναλόγως. Έτσι μόλις διανείμει ο αναγνώστης μια εντολή στην έξυπνη κάρτα, αυτή εμποδίζεται έως ότου ο αναγνώστης παραλάβει μια απάντηση. Το παρακάτω σχήμα επεξηγεί την επικοινωνία μεταξύ της έξυπνης κάρτας και του αναγνώστη μέσω μιας σειράς μεταβάσεων.



Διάγραμμα αναγνώστη Διάγραμμα κάρτας

ΕΙΚΟΝΑ 28 : Διαγράμματα μεταβάσεων αναγνωστών και έξυπνων καρτών

Στο τμήμα αυτό του προτύπου όπως προαναφέραμε περιγράφονται τα ηλεκτρονικά σήματα και τα πρωτόκολλα μετάδοσης των καρτών ολοκληρωμένων κυκλωμάτων. Έτσι τα θέματα που θα μελετήσουμε αφορούν την μετάδοση των χαρακτήρων (ασύγχρονη και σύγχρονη), την ανταπόκριση Answer to Reset (ATR) μιας κάρτας και τα δύο πιο συχνά χρησιμοποιούμενα πρωτόκολλα μετάδοσης το t=0 και t=1.

Το μεγαλύτερο μέρος του ISO 7816-3 είναι σημαντικό για τους κατασκευαστές ή τους προγραμματιστές που επιθυμούν να πραγματοποιήσουν επικοινωνία με την έξυπνη κάρτα σε χαμηλό επίπεδο, το επίπεδο των σημάτων. Η επικοινωνία μπορεί να γίνει είτε από έναν μικρό-ελεγκτή είτε από τη σειριακή/ παράλληλη/ USB / PUMICE θύρα ενός PC. Είναι ιδιαίτερα ενδιαφέρον να δει κανείς τι πληροφορίες μπορεί να πάρει από την ανταπόκριση Answer to Reset (ATR) μιας κάρτας.

❖ ΔΙΑΔΙΚΑΣΙΑ ΛΕΙΤΟΥΡΓΙΑΣ ΓΙΑ ΤΙΣ ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ

Η διαδικασία λειτουργίας που περιγράφεται παρακάτω ισχύει για κάθε κάρτα ολοκληρωμένου κυκλώματος με τις επαφές. Ο «διάλογος» μεταξύ συσκευής και κάρτας πραγματοποιείται σε βήματα, που ορίζονται ως εξής:

Α. σύνδεση και ενεργοποίηση των επαφών από τη συσκευή
Β. reset της κάρτας
Γ. ανταπόκριση από την κάρτα με το σήμα Answer To Reset
Δ. ανταλλαγή πληροφοριών μεταξύ κάρτας και συσκευής
Ε. απενεργοποίηση των επαφών από τη συσκευή (όταν η συναλλαγή έχει πραγματοποιηθεί ή έχει εντοπιστεί απομάκρυνση της κάρτας από τη συσκευή).

❖ ΑΝΤΑΠΟΚΡΙΣΗ ΤΗΣ ΚΑΡΤΑΣ ΜΕ ΣΗΜΑ ANSWER TO RESET

Υπάρχουν δυο τρόποι για μετάδοση της απάντησης:

A Ασύγχρονη μετάδοση: όπου μεταδίδονται στην I/O line χαρακτήρες με ασύγχρονο ημι-αμφίδρομο τρόπο. Κάθε χαρακτήρας είναι 8bit.

B Σύγχρονη Μετάδοση: όπου μια σειρά από bits μεταδίδονται στην I/O line με ημι-αμφίδρομο τρόπο και σε συγχρονισμό με το σήμα του ρολογιού CLK.

Α) ΑΣΥΓΧΡΟΝΗ ΜΕΤΑΔΟΣΗ ΣΤΟΙΧΕΙΩΝ

Όλη η επικοινωνία από και προς την έξυπνη κάρτα και τον αναγνώστη και αντιστρόφως, πραγματοποιείται από τη επαφή C7. Νωρίτερα, καθορίσαμε την επαφή C7 ως επαφή εισόδου / εξόδου. Επειδή τα στοιχεία μπορούν είτε να ρεύσουν από τον αναγνώστη στην κάρτα ή από την κάρτα στον αναγνώστη ,αλλά όχι συγχρόνως το κανάλι επικοινωνίας που χρησιμοποιείται καλείται «αμφίδρομο».

Αυτό απλά σημαίνει ότι μόνο ένα συμβαλλόμενο μέρος μπορεί να επικοινωνήσει σε έναν συγκεκριμένο χρόνο, είτε η το τελικό τερματικό (αναγνώστης) είτε η έξυπνη κάρτα. Εάν τα στοιχεία διαβιβαστούν ταυτόχρονα από την έξυπνη κάρτα και τον αναγνώστη τότε θα χαθούν.

Η επικοινωνία αρχίζει πάντα από το τερματικό και η κάρτα αποκρίνεται μόνο στις οδηγίες του τερματικού. Η κάρτα δεν διαβιβάζει ποτέ τα στοιχεία χωρίς να έχει προηγηθεί ένα αίτημα από το τερματικό. Αυτό μιμείται μια σχέση ενός πελάτη και ενός κεντρικού υπολογιστή. Η έξυπνη κάρτα είναι ο πελάτης, και ο κεντρικός υπολογιστής είναι το τερματικό.

➢ **Ροή επικοινωνίας της κάρτας και του τερματικού**

Βήμα 1 : η έξυπνη κάρτα εισάγεται στον αναγνώστη.

Βήμα 2 : οι επαφές της έξυπνης κάρτας ενεργοποιούνται ηλεκτρικά.

Βήμα 3: η έξυπνη κάρτα εκτελεί μια εντολή power- on – reset και στέλνει μια απάντηση answer-to-reset (ATR) στο τερματικό.

Βήμα 4: το τερματικό αξιολογεί τον ATR και επισημαίνει τις διαφορετικές παραμέτρους καρτών. Σε αυτό το σημείο, ανάλογα με την κάρτα, το τερματικό μπορεί να στείλει μια οδηγία PTS στην κάρτα.

Το **PTS** είναι επιλογή τύπων πρωτοκόλλου. Αυτή η οδηγία χρησιμοποιείται από το τερματικό για να θέσει τις διάφορες παραμέτρους μετάδοσης σχετικά με το πρωτόκολλο της κάρτας. Τα πρωτόκολλα μετάδοσης θα τα μελετήσουμε στην επόμενη ενότητα .

Βήμα 5: εάν η οδηγία PTS εστάλη στην έξυπνη κάρτα, η έξυπνη κάρτα αποκρίνεται με μια απάντηση.

Βήμα 6 - η αμφίδρομη επικοινωνία συνεχίζεται. Το τερματικό στέλνει μια οδηγία, η έξυπνη κάρτα κατόπιν στέλνει μια απάντηση. Αυτή η διαδικασία συνεχίζεται έως ότου απενεργοποιηθεί η κάρτα (να την βγάλουμε από τον αναγνώστη).

Η επικοινωνία μεταξύ μιας έξυπνης κάρτας και του τερματικού είναι τμηματική. Αυτό σημαίνει ότι όλα τα στοιχεία επεξεργασμένα μετατρέπονται σε τμηματικά κομμάτια πληροφοριών. (Ένα byte είναι χωρισμένο σε οκτώ μεμονωμένα bit). Σε αυτά τα bit στέλνονται οι πληροφορίες σε πακέτα το ένα μετά από το άλλο).

Στις έξυπνες κάρτες, η μετάδοση στοιχείων είναι ασύγχρονη. Αυτό σημαίνει ότι σε κάθε byte (8 μπιτ) πρέπει να παρέχεται με τα πρόσθετα bit. Ένα από τα πρόσθετα bit καλείται bit έναρξης. Το bit έναρξης επισημαίνει την αρχή μιας ακολουθίας αποστολής (δηλαδή ενημερώνει τον αποδέκτη ότι θα λάβει κάποια bit).

Μετά από την ακολουθία των byte, υπάρχει ένα bit ισότητας για ανίχνευση λάθους και ένα ή δύο bit στάσεων. Τα bit στάσεων δίνουν στον αποδέκτη και στον αποστολέα χρόνο να προετοιμαστούν για την επόμενη αποστολή. Ένα πλεονέκτημα της ασύγχρονης μετάδοσης είναι ότι δεν απαιτεί ένα ρολόι. Ο συγχρονισμός παράγεται από τον συγχρονισμό μεταξύ των bit παρά ένα ρολόι.

❖ ΠΡΩΤΟΚΟΛΛΑ ΜΕΤΑΔΟΣΗΣ

Ένα πρωτόκολλο είναι ένα σύνολο κανόνων και διαδικασιών που κυβερνούν την ανταλλαγή των πληροφοριών μεταξύ μιας έξυπνης κάρτας και του τερματικού. Το πρωτόκολλο είναι η ολόκληρη δομή της επικοινωνίας.

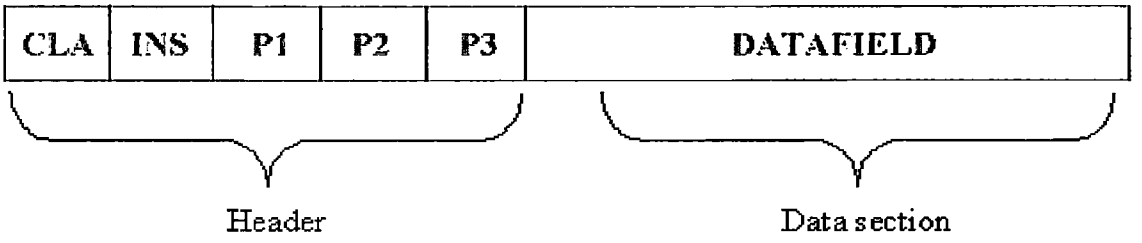
❖ ΤΥΠΟΣ ΠΡΩΤΟΚΟΛΛΟΥ Τ

Τ=0 πρωτόκολλο ασύγχρονης ημι-αμφίδρομης μετάδοσης χαρακτήρων.
Τ=1 πρωτόκολλο ασύγχρονης ημι-αμφίδρομης μετάδοσης με φραγμένο προορισμό
Τ=2 δεσμεύεται για μελλοντική χρήση και αμφίδρομη μετάδοση.
Τ=3 δεσμεύεται για μελλοντική χρήση και αμφίδρομη μετάδοση.
Τ=4 δεσμεύονται για μελλοντική ασύγχρονη ημι-αμφίδρομη μετάδοση χαρακτήρων.
Τ=5 έως Τ=13 δεσμεύονται για μελλοντική χρήση.
Τ=14 δεσμεύονται για πρωτόκολλα κατά ISO.
Τ=15 δεσμεύονται για μελλοντική χρήση.

Τα πρωτόκολλα Τ=0, και Τ=1 είναι τα συνηθέστερα χρησιμοποιημένα πρωτόκολλα παγκοσμίως.

❖ ΠΡΩΤΟΚΟΛΛΟ ΜΕΤΑΔΟΣΗΣ Τ=0

Η μικρότερη μονάδα που υποβάλλεται σε επεξεργασία από το πρωτόκολλο Τ=0 είναι ένα ενιαίο byte. Λόγω του προσανατολισμού των byte αυτού του πρωτοκόλλου, εάν ένα λάθος μετάδοσης ανιχνευτεί, το byte πρέπει να ζητηθεί πάλι. Η ανίχνευση αυτών των λαθών είναι δυνατή επειδή κάθε byte διαθέτει ένα bit ισότητας. Είναι ευκολότερο να γίνει κατανοητό πώς κάθε ψηφιολέξη διαβιβάζεται με το Τ=0 πρωτόκολλο με το ακόλουθο διάγραμμα:



ΕΙΚΟΝΑ 29 : Πρωτόκολλο μετάδοσης Τ=0

Η κύρια λειτουργία της φρουράς των χρονικών bit είναι να χωριστούν τα μεμονωμένα byte κατά τη διάρκεια της μετάδοσης. Αυτό δίνει στον αποστολέα και στο δέκτη περισσότερο χρόνο να πραγματοποιήσουν τις λειτουργίες του πρωτοκόλλου μετάδοσης. Εάν ένα λάθος ανιχνευτεί κατά τη διάρκεια αυτής της μετάδοσης byte, η φρουρά των χρονικών bit τα μετατρέπει σε μήνυμα λάθους που λέει στην κάρτα να στείλει εκ νέου τα byte στον αναγνώστη.

❖ ΠΡΩΤΟΚΟΛΛΟ ΜΕΤΑΔΟΣΗΣ Τ=1

Το Τ=1 πρωτόκολλο είναι ένα πρωτόκολλο φραγμών. Ο φραγμός είναι η μικρότερη μονάδα στοιχείων που μπορεί να διαβιβαστεί μεταξύ της κάρτας και του τερματικού. Οι φραγμοί είναι ομάδες bytes.

Υπάρχουν τρεις τύποι φραγμών:

- Φραγμοί πληροφοριών - χρησιμοποιούνται για τη διαφανή ανταλλαγή των στοιχείων στρώματος εφαρμογής.
- Φραγμός αναγνώρισης υποδοχής - δεν περιέχει ποτέ έναν τομέα πληροφοριών και εξυπηρετεί για την υποδοχή επιβεβαίωσης.
- Φραγμοί συστημάτων - που χρησιμοποιείται για τον έλεγχο στοιχείων που αφορούν το ίδιο το πρωτόκολλο.

Protogue Field			Information Field	Epilogue Field
Note Address NAD	Protocol Control Byte PCB	Length NEN	APDU	EDC
1 Byte	1 Byte	1 Byte	1 - 254 Bytes	1 - 2 Bytes

ΕΙΚΟΝΑ 30 : Δομή πρωτοκόλλου T=1 φραγμών μετάδοσης

Οι φραγμοί αποτελούνται από έναν τομέα προλόγου, τον τομέα πληροφοριών, και τον τομέα επιλόγου. Οι τομείς προλόγου και επιλόγου είναι υποχρεωτικοί.

- **Τομέας προλόγου** : διαβιβάζεται στην αρχή ενός φραγμού και αποτελείται από το NAD, το PCB, και το LEN.

NAD (node address) : διεύθυνση κόμβων - περιέχει τις διευθύνσεις στόχων και προέλευσης φραγμών.

PCB (protocol control byte) : πρωτόκολλο ελέγχου byte – ελέγχει και εποπτεύει το πρωτόκολλο μετάδοσης.

LEN (length) : μήκος - δείχνει το μήκος του τομέα πληροφοριών.

- **Τομέας πληροφοριών** σε ένα φραγμό πληροφοριών είναι τα στοιχεία του στρώματος εφαρμογής. Το περιεχόμενο αυτού του τομέα διαβιβάζεται διαφανώς. Αυτό σημαίνει απλά ότι αυτές οι πληροφορίες διαβιβάζονται από το πρωτόκολλο μετάδοσης χωρίς την ανάλυση ή αξιολόγηση.

- **Τομέας πληροφοριών** σε ένα φραγμό συστήματος είναι τα στοιχεία που διαβιβάζονται.

APDU (Application Protocol Data Unit) : μονάδα στοιχείων πρωτοκόλλου εφαρμογής,
εντολή ADPU - αντιπροσωπεύει τις οδηγίες στην κάρτα,
απάντηση ADPU - απαντήσεις από την κάρτα.

- **Τομέας επιλόγου** - που διαβιβάζεται στο τέλος ενός φραγμού περιέχει τον κώδικα ανίχνευσης λάθους (EDC - error detection code).

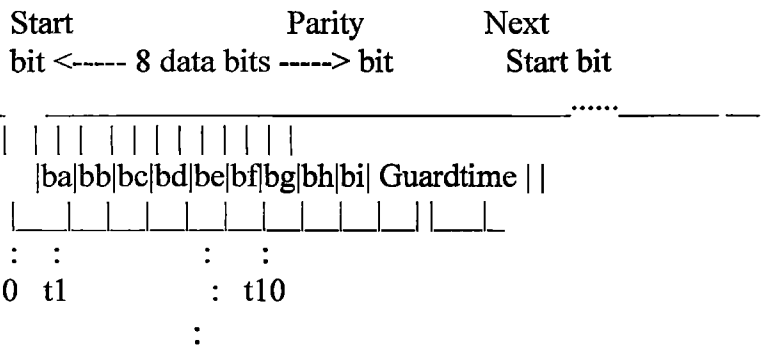
ΠΑΡΑΤΗΡΗΣΕΙΣ

❖ **Reset της κάρτας**

1 . Θεωρείται ότι η εσωτερική κατάσταση της κάρτας δεν είναι γνωστή πριν από το reset.
2 . Για να είναι εφικτή οποιαδήποτε επικοινωνία της συσκευής με την κάρτα θα πρέπει να οριστεί το RST σε μια κατάσταση που να δηλώνει ότι υπάρχει απάντηση στη γραμμή I/O.
3 . Το RESET αρχίζει από τη συσκευή. Μέχρι το τέλος της ενεργοποίησης των επαφών, η κάρτα είναι έτοιμη για reset. Αφού ρυθμιστεί το σήμα του ρολογιού CLK και η I/O line, η κάρτα ύστερα από κάποιο χρονικό διάστημα (κύκλους του ρολογιού) πρέπει να επιστρέψει την απάντηση ATR. Αν μέσα στο προβλεπόμενο χρονικό διάστημα η κάρτα δεν επιστρέψει απάντηση τότε απενεργοποιούνται οι επαφές από τη συσκευή.

❖ **Answer to Reset σε ασύγχρονη μετάδοση**

Ένας χαρακτήρας κατά την ασύγχρονη μετάδοση αποτελείται από τα εξής 10 bits: ένα bit εκκίνησης, οχτώ bits πληροφορίας (ba, bb, bc ...bh) ,ένα (δέκατο) bit bi που χρησιμοποιείται για τον έλεγχο άρτιας ισοτιμίας.
Σημειώνεται ότι η ισοτιμία είναι σωστή όταν το πλήθος των μονάδων είναι άρτιος αριθμός.



Αν το I/O είναι σε κατάσταση Z, τότε η μετάδοση έγινε σωστά.
Αν το I/O είναι σε κατάσταση A, τότε η μετάδοση δεν πραγματοποιήθηκε σωστά και πρέπει να επαναληφθεί μετά από κάποιο χρονικό διάστημα.

Β) ΣΥΓΧΡΟΝΗ ΜΕΤΑΔΟΣΗ ΣΤΟΙΧΕΙΩΝ

Η σύγχρονη μετάδοση είναι μια τμηματική μετάδοση που απαιτεί ένα σήμα ρολογιών για να παρέχει το συγχρονισμό και να ελέγξει την παραγωγή των στοιχείων. Σχεδιάστηκε με μεγάλη απλότητα. Η σύγχρονη μετάδοση στις κάρτες μνήμης επιτρέπει στην εφαρμογή του τερματικού να προσεγγίσει τις διευθύνσεις μνήμης του τσιπ άμεσα. Απαιτείται λίγη λογική στην κάρτα μνήμης κάτι (που τις καθιστά λιγότερο ακριβές). Το τερματικό αναλαμβάνει εντελώς τη φυσική εξέταση της μνήμης. Η ίδια η κάρτα μπορεί μόνο να εμποδίσει ορισμένες περιοχές ενάντια στο σβήσιμο.

Τα πρωτόκολλα μετάδοσης που χρησιμοποιούνται για τις κάρτες μνήμης είναι S=8, S=9, S=10.

15.1.4 ΠΡΟΤΥΠΟ ISO 7816-4 :ΕΝΤΟΛΕΣ ΓΙΑ ΤΗΝ ΜΕΤΑΦΟΡΑ ΔΕΔΟΜΕΝΩΝ ΑΠΟ ΚΑΙ ΠΡΟΣ ΤΗΝ ΚΑΡΤΑ [88]

Αυτό το μέρος του ISO/ IEC 7816 προτύπου έξυπνων καρτών προσδιορίζει :

- το περιεχόμενο των μηνυμάτων, εντολών και απαντήσεων, που διαβιβάζονται από τη συσκευή στην κάρτα και αντίστροφα.
- τη δομή και το περιεχόμενο των ιστορικών bytes που στέλνονται από την κάρτα κατά τη διάρκεια της απάντησης ATR.
- τη δομή των αρχείων και των δεδομένων.
- τις μεθόδους προσπέλασης στα αρχεία και δεδομένα της κάρτας.
- τις μεθόδους για την ασφαλή μετάδοση μηνυμάτων.
- τις μεθόδους προσπέλασης στους αλγορίθμους που υποβάλλονται προς επεξεργασία στην κάρτα, χωρίς να περιγράφει τους ίδιους τους αλγορίθμους.

Οι εντολές μπορούν να ταξινομηθούν ανάλογα με τη λειτουργία τους ως εξής:

- Επιλογή Αρχείου.
- Ανάγνωση / εγγραφή αρχείου.
- Αναζήτηση αρχείου.
- Διαχείριση Αρχείων.
- Αναγνώριση.
- Πιστοποίηση.
- Εντολές Κρυπτογράφησης.
- Εντολές για ηλεκτρονικά πορτοφόλια.
- Εντολές ειδικές για κάθε εφαρμογή.

ΒΙΟΜΗΧΑΝΙΚΑ ΠΡΟΤΥΠΑ

15.2 ΠΡΟΤΥΠΟ EMV [89]

EMV είναι ένα ακρωνύμιο που προκύπτει από τα αρχικά των λέξεων Europay, MasterCard και Visa. Οι τρεις αυτοί οργανισμοί έχουν συμφωνήσει στη σύνταξη ορισμένων προδιαγραφών γνωστές με το όνομα "EMV card specification".

Οι προδιαγραφές αυτές περιγράφουν τον τρόπο με τον οποίο οι κάρτες που εκδίδονται από οποιονδήποτε από τους τρεις οργανισμούς θα λειτουργεί σε ένα τερματικό μηχάνημα ή ένα Automated Teller Machine (ATM).

Υπάρχουν δύο κυρίως λόγοι για τη στροφή που παρατηρήθηκε προς έξυπνες κάρτες χρέωσης/ πίστωσης:

1. η ανάγκη για μείωση των κρουσμάτων απάτης που παρατηρήθηκαν με τις μαγνητικές κάρτες.

2. η ανάγκη για πραγματοποίηση συναλλαγών χρέωσης /πίστωσης στις συσκευές POS (point of sale) offline με σκοπό να επιτύχουμε μεγαλύτερο επίπεδο ασφάλειας.

Η κάρτα EMV μπορεί να θεωρηθεί ως μια σειρά από επίπεδα. Η διαδικασία της προσωποποίησης γεμίζει την κάρτα με τα δεδομένα του κατόχου και ενεργοποιεί την εφαρμογή να επικοινωνεί με το chip μέσω του λειτουργικού συστήματος. Διαφορετικά λειτουργικά συστήματα απαιτούν η EMV εφαρμογή να είναι προσωποποιημένη με έναν συγκεκριμένο τρόπο.

ΕΙΚΟΝΑ 31 : Επίπεδα μιας κάρτας EMV

Το τέταρτο επίπεδο είναι η περιοχή όπου αποθηκεύονται τα δεδομένα του κατόχου και τα κλειδιά (Secret Keys).

Το τρίτο επίπεδο αφορά στην EMV εφαρμογή, που μπορεί να είναι από τη Europay, τη MasterCard ή τη Visa. Σε κάθε περίπτωση όμως η εφαρμογή θα πρέπει να έχει γραφτεί σύμφωνα με τις προδιαγραφές EMV.

Το δεύτερο επίπεδο είναι το λειτουργικό σύστημα που τροποποιείται για να είναι συμβατό με τον μικροεπεξεργαστή. Υπάρχουν τουλάχιστον 7 διαφορετικοί κατασκευαστές λειτουργικών συστημάτων καρτών.

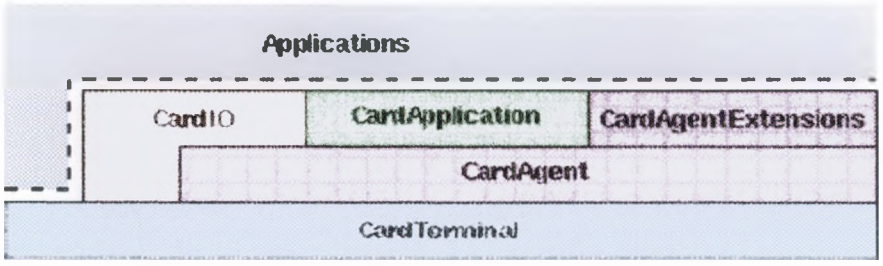
Στο χαμηλότερο επίπεδο βρίσκεται ο μικροεπεξεργαστής, για τον οποίο υπάρχουν τουλάχιστον τέσσερις διαφορετικοί κατασκευαστές.

15.3 ΠΡΟΤΥΠΟ OPEN CARD [90]

Το πρότυπο OpenCard αφορά την υλοποίηση διαλειτουργικών εφαρμογών έξυπνων καρτών σε διαφορετικές πλατφόρμες και διαφορετικό εξοπλισμό. Πρόκειται για ένα ανοικτό πρότυπο, το οποίο παρέχει την αρχιτεκτονική και ένα σύνολο από APIs που επιτρέπουν στους προγραμματιστές να αναπτύξουν εφαρμογές έξυπνων καρτών σε Java. Διαφέρει από το PC/ SC στο γεγονός ότι παρέχει μια ενιαία διεπαφή για την ανάπτυξη εφαρμογών έξυπνων καρτών σε όλες τις νέες πλατφόρμες, όπως δίκτυα υπολογιστών, τηλέφωνα, TAM, Unix workstations κ.α.

➢ **ΑΡΧΙΤΕΚΤΟΝΙΚΗ OPEN CARD**

Το πρότυπο OpenCard παρέχει ένα API (application programming interface), που επιτρέπει την έκδοση καρτών, τον εντοπισμό κάρτας στον reader ή ακόμη και να ενεργοποιούνται Java agents όταν εισάγεται μια κάρτα στον reader. Η αρχιτεκτονική αυτή φαίνεται στο παρακάτω σχήμα.



ΕΙΚΟΝΑ 32 : Αρχιτεκτονική OpenCard Framework

Το OpenCard αποτελείται από 4 Java packages με το πρόθεμα opencard:

1. application
2. io
3. agent
4. terminal

Τα packages opencard.application και opencard.io παρέχουν το API υψηλού επιπέδου που χρησιμοποιείται από τον προγραμματιστή. Οι λειτουργίες που χρειάζεται το API αυτό υλοποιούνται από κλάσεις στα opencard.agent και opencard.terminal packages. Το opencard.agent package αναφέρεται στις λειτουργίες της έξυπνης κάρτας μέσω του CardAgent, το package opencard.terminal αναφέρεται στις λειτουργίες του τερματικού (readers).

➢ **Στόχοι του προτύπου OpenCard**:

- ανεξαρτησία από προμηθευτές τερματικών καρτών,
- ανεξαρτησία από προμηθευτές λειτουργικών συστημάτων καρτών,
- ανεξαρτησία από εκδότες καρτών.

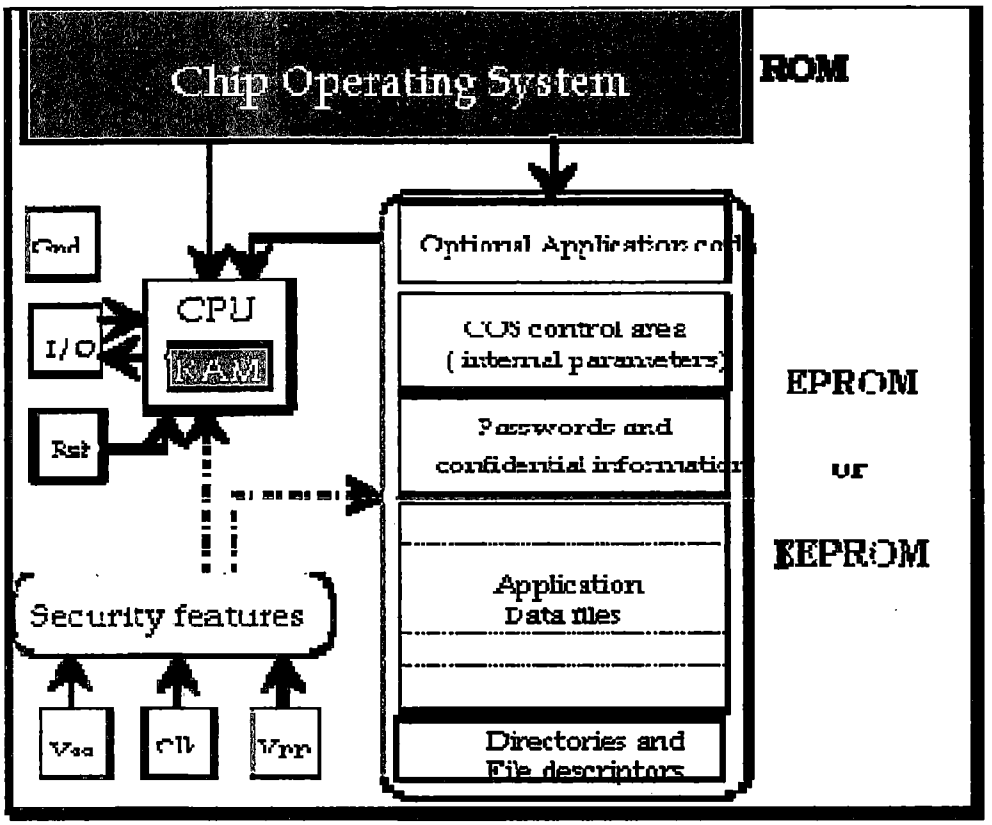
15.4 PC / SC [91]

Πρόκειται για την ανοιχτή πλατφόρμα της Microsoft με σκοπό την συνεργασία ανάμεσα σε έξυπνες κάρτες και ηλεκτρονικούς υπολογιστές. Το PC/SC ουσιαστικά βασίζεται στα επιτεύγματα των ISO 7816 & EMV.

Στην διαμόρφωση του προτύπου έχουν εμπλακεί οι μεγαλύτεροι κατασκευαστές Η/Υ και έξυπνων καρτών. Χαρακτηριστικά αναφέρονται οι εταιρίες Bull, Gemplus, Hewlett-Packard, IBM, Schlumberger, Siemens, Sun και άλλοι. Σκοπός της προσπάθειας είναι η επίτευξη της διαλειτουργικότητας των καρτών 'σε χαμηλό επίπεδο', με την χρήση καταλλήλων και συμβατών interfaces (API – Application Program Interface) ανάμεσα στην κάρτα και τον αναγνώστη ώστε να αποδεσμευτεί ο χρήστης από επιλογή συγκεκριμένων μηχανημάτων, κυρίως αναγνωστών.

16 ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ ΤΩΝ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ [92]

Κάθε έξυπνη κάρτα με μικροεπεξεργαστή έχει ένα λειτουργικό σύστημα, το οποίο ονομάζουμε Λειτουργικό Σύστημα Κάρτας (Card Operation System ή Chip Operation System). Παρέχει τη δυνατότητα εκτέλεσης βασικών λειτουργιών όπως ασφαλή πρόσβαση και αποθήκευση δεδομένων στην κάρτα, πιστοποίηση ταυτότητας και κρυπτογράφηση.



ΕΙΚΟΝΑ 33 : Το λειτουργικό σύστημα ενός τσίπ

16.1 ΤΙ ΑΚΡΙΒΩΣ ΕΙΝΑΙ ΤΟ COS

Το Chip Operating System της έξυπνης κάρτας είναι μια ακολουθία εντολών, ενσωματωμένη μόνιμα στη ROM της έξυπνης κάρτας. Όπως το DOS ή το λειτουργικό σύστημα Windows, οι εντολές του COS δεν εξαρτώνται από οποιαδήποτε ιδιαίτερη εφαρμογή, αλλά χρησιμοποιούνται συχνά από τις περισσότερες εφαρμογές.

Τα λειτουργικά συστήματα COS διαιρούνται σε δύο κατηγορίες:

- <u>τα COS γενικού σκοπού</u> (general purpose COS) που καλύπτουν τις περισσότερες εφαρμογές. Η πρώτη αυτή προσέγγιση ,αντιμετωπίζει την κάρτα ως ασφαλή συσκευή υπολογισμού και αποθήκευσης. Τα αρχεία και η άδεια πρόσβασης σε αυτά ορίζονται από τον εκδότη της κάρτας. Η μόνη πρόσβαση στις κάρτες γίνεται μέσω του λειτουργικού συστήματος. Δεν γίνεται τροποποίηση της δομής των αρχείων στην κάρτα. Τα περιεχόμενα της κάρτας

διαβάζονται ή ενημερώνονται σύμφωνα με τις άδειες που έχουν ορίσει οι εκδότες. Το λειτουργικό σύστημα εκτελεί ενέργειες όπως πιστοποίηση ταυτότητας και κρυπτογράφηση μέσω των εντολών που στέλνονται στην κάρτα.

- **το «αφιερωμένο» COS** (dedicated COS) με εντολές που σχεδιάζονται για τις συγκεκριμένες εφαρμογές και που μπορούν ακόμη και να περιέχουν την ίδια την εφαρμογή. Ένα παράδειγμα θα ήταν μια κάρτα με σκοπό να υποστηρίξει μια συγκεκριμένη ηλεκτρονική εφαρμογή πορτοφολιών.

Σύμφωνα με τη δεύτερη μεθοδολογία, η κάρτα διαθέτει ένα διαχειριστή της μνήμης της που μας επιτρέπει να φορτώσει επάνω στην κάρτα κάποια συγκεκριμένη εφαρμογή και κάποια αρχεία. Το λειτουργικό αυτό σύστημα είναι κατάλληλο για κάρτες που προβλέπεται να έχουν μεγάλη διάρκεια ζωής.

Παραδείγματα τέτοιων COS είναι το Java Cards και το COS Windows της Microsoft. Σε αυτή την περίπτωση όμως, αυξάνονται τα προβλήματα ασφάλειας και υπάρχει και ο κίνδυνος να εισαχθεί στην κάρτα κάποιος ιός.

Οι **βασικές λειτουργίες** ενός COS που είναι κοινές σε όλα τα προϊόντα έξυπνων καρτών περιλαμβάνουν:

- Διαχείριση της ανταλλαγής δεδομένων μεταξύ της κάρτας και του εξωτερικού κόσμου, κυρίως από την άποψη του χρησιμοποιούμενου πρωτοκόλλου.
- Διαχείριση των αρχείων και των δεδομένων που φυλάσσονται στη μνήμη
- Έλεγχος πρόσβασης σε πληροφορίες και λειτουργίες (παραδείγματος χάριν select file, read, write, update data).
- Διαχείριση της ασφάλειας καρτών και των κρυπτογραφικών αλγορίθμων.
- Διατήρηση της αξιοπιστίας, ιδιαίτερα από την άποψη της συνέπειας στοιχείων, της διαχείρισης των interrupts και την επαναφορά από ένα σφάλμα.
- Διαχείριση των διάφορων φάσεων του κύκλου ζωής της κάρτας (δηλαδή επεξεργασία, εξατομίκευση, ενεργός ζωή και τέλος της ζωής).

Για την ανάπτυξη των προγραμμάτων που τρέχουν μέσα στο ασφαλές περιβάλλον των έξυπνων καρτών, προτείνονται λειτουργικά συστήματα που έχουν τη μεγαλύτερη απήχηση στην αγορά όπως JavaCard OS, MultOS και πρόσφατα Windows for smart cards.

16.2 MULTOS APPLICATION CARD OPERATING SYSTEMS (MACOS)

Μέχρι την εμφάνιση των έξυπνων καρτών πολλαπλών εφαρμογών, κάθε εφαρμογή λογισμικού που αντιπροσωπεύει ένα προϊόν ή μια υπηρεσία σε μια κάρτα γράφτηκε για ένα συγκεκριμένο λειτουργικό σύστημα.

Τα λειτουργικά συστήματα πολλαπλών εφαρμογών επιτρέπουν την ανάπτυξη των πολλαπλών εφαρμογών που τρέχουν σε μια κάρτα. Στην ιδανική περίπτωση οι εφαρμογές που φιλοξενούνται στην ίδια κάρτα δεν μπορούν να παρεμποδίζουν η μια την άλλη και προστατεύονται από ένα firewall. Αυτήν την περίοδο υπάρχουν τρία σημαντικά λειτουργικά συστήματα πολλαπλών εφαρμογών στην αγορά:

- Java Card για όσους θέλουν να προγραμματίσουν σε Java.

- MultOS είναι το πρώτο λειτουργικό σύστημα πολλαπλών εφαρμογών (multiapplication) για έξυπνες κάρτες που προσφέρει υψηλό επίπεδο ασφάλειας. Το MultOS επιτρέπει τη φόρτωση, την ενημέρωση ή τη διαγραφή οποιασδήποτε εφαρμογής κατά τη διάρκεια της ζωής της κάρτας.

- Windows for Smart Cards Microsoft licenses Windows® for Smart Cards Toolkit

16.3 MULTOS

16.3.1 OVERVIEW

Το MULTOS είναι ένα λειτουργικό σύστημα πολλαπλών εφαρμογών για έξυπνες κάρτες με υψηλότερες ανάγκες ασφάλειας. Το πλεονέκτημα αυτού του συστήματος είναι ότι τα διαφορετικά συμβαλλόμενα μέρη μπορούν να αναπτύξουν εφαρμογές που τρέχουν στην ίδια κάρτα και συνυπάρχουν ανεξάρτητα. Με τον τρόπο αυτό εφαρμογές από διάφορους προμηθευτές μπορούν να συνδυαστούν σε μια κάρτα.

Η ανοικτή φύση της πλατφόρμας MULTOS επιτρέπει στον καθένα να εκδόσει κάρτες, να γράψει εφαρμογές, να εφαρμόσει το λειτουργικό σύστημα σε ένα συγκεκριμένο τσιπ ή να κατασκευάσει έξυπνες κάρτες.

16.3.2 SECURE MULTI-APPLICATION SMART CARD OPERATING SYSTEM

Οι εφαρμογές είναι απομονωμένες η μια από την άλλη. Ένα σύστημα από firewalls εξασφαλίζει ότι τα στοιχεία δεν μπορούν να προσπελασθούν χωρίς κατάλληλη έγκριση. Αυτό έχει ως αποτέλεσμα, να μην είναι απαραίτητο οι προμηθευτές των εφαρμογών να εμπιστεύονται ο ένας τον άλλον, ούτε καν να έχουν οποιαδήποτε σχέση.

16.3.3 APPLICATION LOAD & UNLOAD

Το MULTOS επιτρέπει φόρτωση των εφαρμογών «on-the-fly» . Αυτό σημαίνει ότι μια κάρτα με το λειτουργικό σύστημα MULTOS μπορεί να αλλάξει τα χαρακτηριστικά της γνωρίσματα κατά τη διάρκεια ζωής της. Παραδείγματος χάριν ένας σπουδαστής για τον οποίο έχει εκδοθεί μια έξυπνη κάρτα με MULTOS, μπορεί να φορτώσει εφαρμογές μέσω του διαδικτύου, αφού βέβαια είχε την απαραίτητη πιστοποίηση - έγκριση.

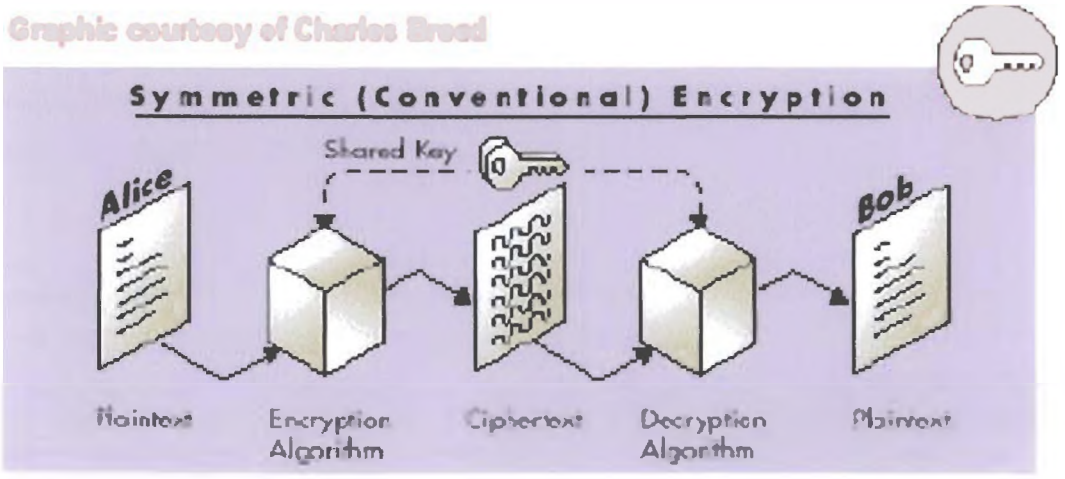
Με τον τρόπο αυτό ο σπουδαστής μπορεί να αλλάξει το σύνολο διαθέσιμων εφαρμογών της κάρτας του κατά τη διάρκεια ζωής της. Έτσι τη μια μέρα μπορεί η κάρτα του να περιέχει μια εφαρμογή ηλεκτρονικού πορτοφολιού και μια εφαρμογή πληρωμής του μετρό, ενώ την επόμενη να προσθέσει ένα ηλεκτρονικό κλειδί για να έχει πρόσβαση στο πανεπιστημιακό δίκτυο. Η δυνατότητα αυτή είναι σημαντική όχι μόνο για τον κάτοχο, αλλά και για τον εκδότη των καρτών.

17 ΑΣΦΑΛΕΙΑ ΤΩΝ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ

17.1 ΑΛΓΟΡΙΘΜΟΙ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ [93]

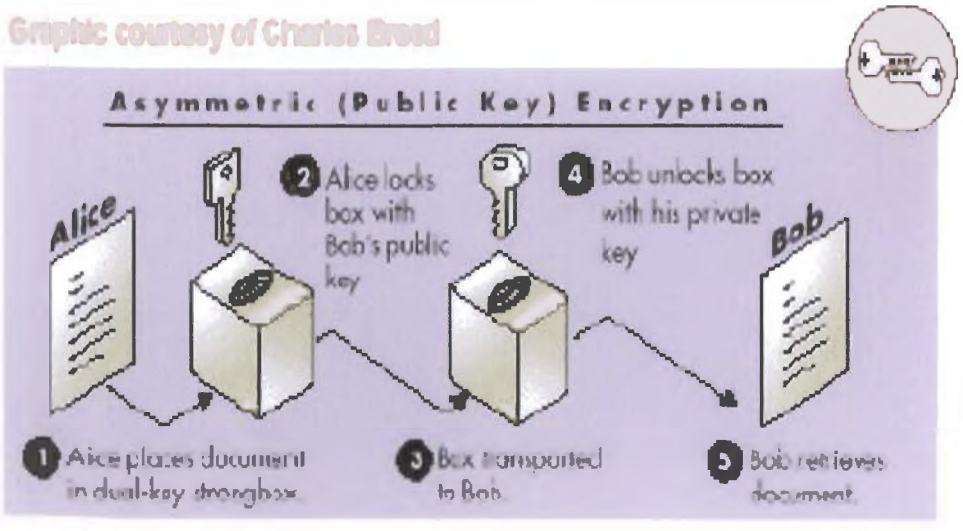
Υπάρχουν δυο είδη αλγορίθμων κρυπτογράφησης:

➢ **οι συμμετρικοί**, όπου το ίδιο κλειδί (secret key) χρησιμοποιείται για την κρυπτογράφηση και την αποκρυπτογράφηση. Ο πιο γνωστός συμμετρικός αλγόριθμος είναι ο DES (Data Encryption Standard).



ΕΙΚΟΝΑ 34 : Συμμετρική κρυπτογράφηση

➢ **οι μη συμμετρικοί**. Ο πιο γνωστός μη συμμετρικός αλγόριθμος είναι ο RSA, που πήρε το όνομά του από τους δημιουργούς του (Rivest, Shamir, και Adleman). Ο RSA χρησιμοποιεί δύο κλειδιά, που ονομάζονται private key.

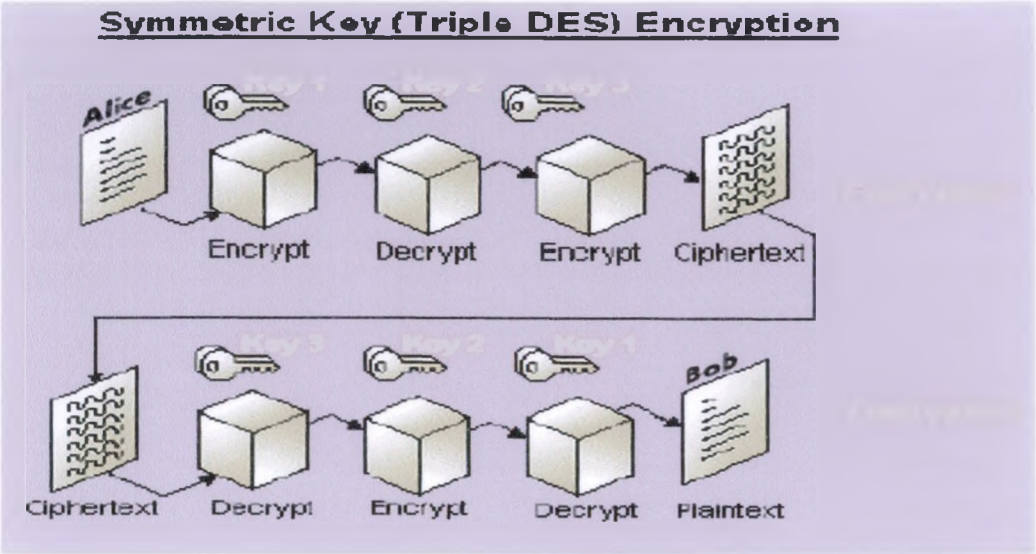


ΕΙΚΟΝΑ 35 : Ασύμμετρη κρυπτογράφηση

DES - Triple-DES Ο αλγόριθμος DES δημιουργήθηκε από την IBM Corporation τη δεκαετία του 1970. Έχει μελετηθεί από πολλούς για περίπου 20 χρόνια, αλλά δεν έχει

βρεθεί κάποιος τρόπος παραβίασής του. Ο αλγόριθμος DES έχει ένα κλειδί 56-bit, δηλαδή 256 πιθανές τιμές.

Ο Triple-DES είναι ένας αλγόριθμος που προσφέρει μεγαλύτερη ασφάλεια. Μπορεί να υλοποιηθεί με δύο ή τρία κλειδιά. Το παρακάτω διάγραμμα δείχνει την πορεία της κρυπτογράφησης σύμφωνα με τον αλγόριθμο Triple-DES με τρία κλειδιά.



ΕΙΚΟΝΑ 36 : Αλγόριθμος DES

17.2 ΔΥΝΑΤΟΤΗΤΕΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ [94]

Οι έξυπνες κάρτες που κυκλοφορούν στην αγορά σήμερα έχουν ικανοποιητικές ικανότητες κρυπτογράφησης, ώστε να υποστηρίζουν τις πιο δημοφιλείς εφαρμογές και πρωτόκολλα ασφάλειας.

Υπογραφές RSA και επαληθεύσεις υποστηρίζονται με κλειδιά (keys) μήκους 512, 768, ή 1024 bit. Οι αλγόριθμοι χρησιμοποιούν χαρακτηριστικά το θεώρημα Chinese Remainder Theorem (CRT) προκειμένου να επιταχυνθεί η επεξεργασία. Ακόμη και στην περίπτωση κλειδιού μήκους 1024 bit, ο χρόνος που απαιτείται για μια υπογραφή είναι χαρακτηριστικά κάτω από ένα δευτερόλεπτο. Συνήθως ο σχεδιασμός είναι τέτοιος ώστε το ευαίσθητο βασικό υλικό δεν φεύγει ποτέ από το τσιπ. Ούτε ο κάτοχος καρτών δεν μπορεί να έχει πρόσβαση στο βασικό υλικό σε αυτήν την περίπτωση. Η χρήση του private key προστατεύεται από το PIN του χρήστη, έτσι ώστε η κατοχή της κάρτας να μην συνεπάγεται τη δυνατότητα να υπογράψει ο χρήστης με την κάρτα.

Ο ψηφιακός αλγόριθμος υπογραφών (Digital Signature Algorithm - DSA) εφαρμόζεται λιγότερο από τη RSA και συνήθως με μήκος κλειδιού 512 bit. Οι έξυπνες κάρτες υποστηρίζουν τη δυνατότητα πολλαπλών PINs που μπορεί να εξυπηρετούν διαφορετικούς σκοπούς. Χρησιμοποιούνται PINs που διαχειρίζονται τα PIN των χρηστών, με σκοπό την επίτευξη μεγαλύτερου επιπέδου ασφαλείας (π.χ. μπορεί να μπλοκάρει την κάρτα ύστερα από έναν καθορισμένο αριθμό αποτυχημένων προσπαθειών εισαγωγής PIN ή να αρχικοποιήσει ξανά την κάρτα). Χρησιμοποιούνται επίσης PINs για να ελέγξουν την πρόσβαση στα ευαίσθητα αρχεία ή τη διαχείριση ηλεκτρονικού πορτοφολιού.

Στις πιο σύγχρονες έξυπνες κάρτες χρησιμοποιούνται οι μέθοδοι κρυπτογράφησης DES και triple DES. Είναι δυνατό να χρησιμοποιηθούν σε μια

λειτουργία Message Authentication Code (MAC). Βέβαια, επειδή ο σειριακός τρόπος επικοινωνίας με την έξυπνη κάρτα έχει χαμηλό εύρος ζώνης, η συμμετρική κρυπτογράφηση είναι πολύ αργή.

Προκειμένου να αποφευχθεί η αντιγραφή καρτών, ένας σταθερός (αμετάβλητος) σειριακός αριθμός (serial number) αποθηκεύεται συχνά στη μνήμη. Οι κάρτες σχεδιάζονται για να επαναρυθμίζονται αυτόματα μόνες τους μόλις ανιχνεύσουν μεταβολές στην τάση ή τη θερμοκρασία. Οι διαδικασίες ανάγνωσης ή εγγραφής της ROM είναι συνήθως απενεργοποιημένη.

Στις έξυπνες κάρτες συνήθως φιλοξενούνται και εφαρμογές ηλεκτρονικού πορτοφολιού, οι οποίες είναι βασισμένες σε συμμετρικές τεχνολογίες όπως DES και triple DES. Κατά συνέπεια, ένα μυστικό κλειδί (key) ευνοεί την ασφάλεια σε πολλές από αυτές τις εφαρμογές. Τα πρωτόκολλα επικοινωνιών των έξυπνων καρτών σε επίπεδο εντολών πολλές φορές ενσωματώνουν και πρωτόκολλο ασφάλειας. Αυτά είναι συνήθως βασισμένα σε συμμετρικές τεχνολογίες και επιτρέπουν στην ίδια την έξυπνη κάρτα να πιστοποιεί το τερματικό ανάγνωσης/ εγγραφής και αντίστροφα.

17.3 ΧΡΗΣΗ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΔΕΔΟΜΕΝΩΝ [95]

Υπάρχουν δύο τρόποι χρησιμοποίησης της κάρτας για την ασφάλεια συστημάτων host based και card-based. Τα ασφαλέστερα συστήματα υιοθετούν και τις δύο μεθοδολογίες.

17.3.1 ΣΥΣΤΗΜΑ ΜΕ HOST-BASED ΑΣΦΑΛΕΙΑ

Ένα τέτοιο σύστημα αντιμετωπίζει την κάρτα ως ένα απλό μέσο μεταφοράς στοιχείων. Η ασφάλεια παρέχεται από τον host υπολογιστή. Τα δεδομένα της κάρτας μπορεί να είναι κρυπτογραφημένα, αλλά υπάρχει σημαντικός κίνδυνος κατά τη μεταφορά τους στον υπολογιστή.

Η ασφάλεια σε αυτές τις περιπτώσεις μπορεί να αυξηθεί με τη χρήση έξυπνων καρτών που χρησιμοποιούν μηχανισμούς κωδικών πρόσβασης για να αποτρέψουν την ανάγνωση των στοιχείων της κάρτας από άτομα που δεν έχουν το δικαίωμα αυτό. Δυστυχώς οι κωδικοί αυτοί είναι εύκολο να «εξουδετερωθούν». Αυτή η μεθοδολογία χρησιμοποιείται όταν κανείς εργάζεται τακτικά στα στοιχεία της κάρτας και μπορεί να παρακολουθεί τα περιεχόμενά της.

17.3.2 ΣΥΣΤΗΜΑ ΜΕ CARD-BASED ΑΣΦΑΛΕΙΑ

Στα συστήματα αυτά χρησιμοποιούνται έξυπνες κάρτες με μικροεπεξεργαστή. Το σύστημα αντιμετωπίζει την κάρτα ως συσκευή επεξεργασίας και η εξουσιοδότηση παρέχεται από το σύστημα ύστερα από αλληλεπίδραση μεταξύ host υπολογιστή και κάρτας. Κατά τη διαδικασία αυτή εξετάζεται αν η κάρτα μπορεί να παρέχει τα απαραίτητα πιστοποιητικά στο σύστημα, ώστε να μπορέσει να συνεχιστεί η συναλλαγή.

Από την άλλη πλευρά και η ίδια η κάρτα μπορεί να ζητήσει την ίδια επιβεβαίωση από το host υπολογιστή. Έτσι λοιπόν η πρόσβαση σε πληροφορίες της κάρτας ελέγχεται από α) το Λειτουργικό Σύστημα που υπάρχει στο εσωτερικό της κάρτας, αλλά και β) τις άδειες που έχει ορίσει ο εκδότης της κάρτας.

17.4 ΠΡΟΤΥΠΑ ΠΟΥ ΣΧΕΤΙΖΟΝΤΑΙ ΜΕ ΤΗΝ ΑΣΦΑΛΕΙΑ [96]

Πολλά από την πρότυπα που έχουν προαναφερθεί εστιάζουν στις λεπτομέρειες των τερματικών ανάγνωσης –γραφής μιας έξυπνης κάρτας και στα χαμηλά επίπεδα των στρωμάτων λογισμικού. Μια άλλη σημαντική κατηγορία προτύπων εστιάζει στον τρόπο με τον οποίο οι έξυπνες κάρτες είναι ενσωματωμένες στις εφαρμογές οι οποίες παρέχουν ασφάλεια στους υπολογιστές και στα δίκτυα. Αυτή η ενότητα συζητά τις αρχές αυτών των προτύπων, των προεξεχόντων προτύπων, όπως επίσης και των φορέων που τα καθορίζουν και τα χρησιμοποιούν.

❖ ΑΡΧΕΣ ΤΩΝ ΠΡΟΤΥΠΩΝ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ

Οποιαδήποτε πρότυπο που έχει σχεδιαστεί με σκοπό να διευκολύνει την ένταξη των έξυπνων καρτών στα συστήματα ασφάλειας υπολογιστών πρέπει να ακολουθεί ορισμένες αρχές προκειμένου να είναι χρήσιμο και να κερδίσει αποδοχή. Μερικά παραδείγματα αυτών των αρχών είναι τα εξής :

- **Multi-platform (Πολύ-πλατφόρμα)**

Τα πρότυπα πρέπει να ισχύσουν στα πολυάριθμα σύγχρονα λειτουργικά συστήματα και διαφορετικές αρχιτεκτονικές υπολογιστών όπως τα Windows, Unix, MAC, x86, Sparc και ούτω καθ'εξής.

- **Open participation (Ανοιχτή συμμετοχή)**

Τα πρότυπα πρέπει να δεχτούν την εισαγωγή και την αναθεώρηση από τα μέλη της βιομηχανίας, του ακαδημαϊκού κόσμου, και της κυβέρνησης.

- **Interoperability (Διαλειτουργικότητα)**

Τα πρότυπα πρέπει να είναι διαλειτουργικά με άλλα κύρια πρότυπα και πρωτόκολλα.

- **Functional (Λειτουργικότητα)**

Τα πρότυπα πρέπει να ισχύσουν για τα πραγματικά παγκόσμια προβλήματα και αγορές και επίσης πρέπει να εξεταστούν επαρκώς οι απαιτήσεις τους.

- **Experience, Products (Εμπειρία, προιόντα)**

Τα πρότυπα πρέπει να δημιουργηθούν από μια ομάδα ανθρώπων με την εμπειρία στα σχετικά με την ασφάλεια προϊόντα και πρότυπα.

- **Extensibility (Επεκτασιμότητα)**

Τα πρότυπα πρέπει να διευκολύνουν την επέκταση στις νέες εφαρμογές, τα πρωτόκολλα, και τις ικανότητες έξυπνων καρτών που δεν υπήρχαν όταν τα πρότυπα δημιουργήθηκαν.

❖ ΠΡΟΔΙΑΓΡΑΦΕΣ ΚΑΙ ΠΡΟΤΥΠΑ ΤΩΝ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ

Τα εξής προκύπτουν ως σημαντικά πρότυπα όσον αφορά την ένταξη των έξυπνων καρτών στις εφαρμογές ασφάλειας υπολογιστών και δικτύων:

- **PKCS # 11 : Κρυπτογραφικά συμβολικά πρότυπα διεπαφών**

Αυτό το πρότυπο διευκρινίζει μια εφαρμογή διεπαφής προγραμματισμού (API), που καλείται «Cryptoki», στις συσκευές που φυλάσσουν τις κρυπτογραφικές πληροφορίες και εκτελούν τις κρυπτογραφικές λειτουργίες. Το Cryptoki, προφέρεται «crypto-key» και αποτελεί σύντμηση για τον όρο της κρυπτογραφικής συμβολικής διεπαφής, ακολουθεί μια απλή βασισμένη σε αντικείμενα προσέγγιση, εξετάζοντας τους στόχους της ανεξαρτησίας της τεχνολογίας (οποιοδήποτε είδος συσκευής) και της διανομής των πόρων (πολλαπλάσιες εφαρμογές που έχουν πρόσβαση στις πολλαπλάσιες συσκευές).

Το PKCS#11 παρουσιάζει στις εφαρμογές μια κοινή, λογική άποψη της συσκευής αποκαλούμενης «cryptographic token». Τα πρότυπα δημιουργήθηκαν το 1994 από τον αλγόριθμο RSA με την εισαγωγή από τη βιομηχανία, τον ακαδημαϊκό κόσμο, και την κυβέρνηση.

- **PC/SC**

Η ομάδα εργασίας PC/SC διαμορφώθηκε τον Μάιο του 1997. Δημιουργήθηκε για να διευθύνει τα κρίσιμα τεχνικά ζητήματα σχετικά με την ολοκλήρωση και ενσωμάτωση των έξυπνων καρτών στους υπολογιστές (PC).Τα μέλη της ομάδας εργασίας PC/SC περιλαμβάνουν τις εξής εταιρίες : τα προσωπικά συστήματα συναλλαγής Bull, Gemplus, την Hewlett-Packard, την IBM, την εταιρία της Microsoft, Schlumberger, Siemens-Nixdorf Inc., Sun Microsystems, την εταιρία Toshiba, και VeriFone.

Η προδιαγραφή εξετάζει τους περιορισμούς στα υπάρχοντα πρότυπα που περιπλέκουν την ολοκλήρωση ICC συσκευών(συσκευών έξυπνων καρτών) με τον υπολογιστή (PC) και αποτυγχάνουν να εξετάσουν επαρκώς τη διαλειτουργικότητα, από μια προοπτική εφαρμογής PC, μεταξύ των προϊόντων από τους πολλαπλάσιους προμηθευτές. Παρέχει τυποποίηση για τις διεπαφές για να διασυνδέσει τις συσκευές (IFDs) και την προδιαγραφή των κοινών διεπαφών προγραμματισμού PC και των μηχανισμών ελέγχου. Η έκδοση 1.0 κυκλοφόρησε το Δεκέμβριο του 1997.

- **OpenCard**

Το OpenCard είναι ένα τυποποιημένο πλαίσιο που αναγγέλλεται από τη διεθνή εταιρία μηχανών γραφείου, την A.E., Netscape, το NCI, και Sun Microsystems Inc., που επιτρέπει τις διαλειτουργικές λύσεις έξυπνων καρτών σε πολλές πλατφόρμες υλικού και λογισμικού. Το πλαίσιο OpenCard είναι ανοικτό πρότυπο που παρέχει μια αρχιτεκτονική και ένα σύνολο των APIs που επιτρέπει στους υπεύθυνους την ανάπτυξη εφαρμογών και τους φορείς παροχής υπηρεσιών να χτίσουν και να επεκτείνουν τις ενήμερες λύσεις έξυπνων καρτών σε οποιοδήποτε OpenCard περιβάλλον. Αναγγέλθηκε αρχικά τον Μάρτιο, του 1997.

- **JavaCard**

Το JavaCard API είναι μια προδιαγραφή που επιτρέπει μιά φορά την εγγραφή, την ικανότητα να μπορεί να τρέξει το πρόγραμμα της Java σε όλες τις έξυπνες κάρτες και σε άλλες συσκευές με περιορισμένη μνήμη. Το JavaCard API αναπτύχθηκε από κοινού από διευθύνοντα μέλη της βιομηχανίας έξυπνων καρτών και έχει υιοθετηθεί από πάνω από 95% των κατασκευαστών έξυπνων καρτών, συμπεριλαμβανομένου του Bull/CP8, , de La rue, Geisecke & Devrient, Gemplus, Inside Technologies, Motorola, Oberthur, Schlumberger, και Toshiba.

➢ **Κοινή αρχιτεκτονική για την ασφάλεια των στοιχείων**

Αναπτυγμένη από την Intel, η κοινή αρχιτεκτονική ασφάλειας στοιχείων (CDSA) παρέχει ένα πλαίσιο ανοικτού, διαλειτουργικού λογισμικού που καθιστά τις πλατφόρμες υπολογιστών ασφαλέστερες για όλες τις εφαρμογές συμπεριλαμβανομένου του ηλεκτρονικού εμπορίου, των επικοινωνιών, και του ψηφιακού περιεχομένου. Οι προδιαγραφές CDSA 2,0 υιοθετήθηκαν από το Open group τον Δεκέμβριο του 1997.

➢ **Microsoft κρυπτογραφικό API**

Το Microsoft® κρυπτογραφικό API (CryptoAPI) παρέχει τις υπηρεσίες που επιτρέπουν στους υπεύθυνους για την ανάπτυξη εφαρμογών για να προσθέσουν το σύστημα κρυπτογραφία και τη λειτουργία για διοίκηση πιστοποιητικών στις αιτήσεις για Win32® . Οι εφαρμογές μπορούν να χρησιμοποιήσουν τις λειτουργίες σε CryptoAPI χωρίς καμία γνώση για την ελλοχεύουσα εφαρμογή, με τον ίδιο σχεδόν τρόπο πού μια εφαρμογή μπορεί να χρησιμοποιήσει μια βιβλιοθήκη γραφικών παραστάσεων χωρίς καμία γνώση για την συγκεκριμένη διαμόρφωση υλικού γραφικών παραστάσεων.

17.5 ΣΗΜΑΣΙΑ ΤΩΝ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ [97]

❖ **Σημασία των έξυπνων καρτών ως μηχανισμός σχεδίασης για τα δίκτυα υπολογιστών**

Αυτό το τμήμα δίνει έμφαση στις θεμελιώδεις προκλήσεις ασφάλειας που μας αντιμετωπίζουν σε αυτόν τον όλο και περισσότερο προσανατολισμένο προς το δίκτυο κόσμο υπολογιστών, και πώς οι έξυπνες κάρτες μπορούν να παρέχουν τα βασικά πλεονεκτήματα όσον αφορά την ασφάλεια.

❖ **Θεμελιώδεις προκλήσεις ασφάλειας**

Επειδή οι υπολογιστές και τα δίκτυα γίνονται το επίκεντρο στις ζωές μας σε αυτήν την ψηφιακή εποχή, πολλές νέες προκλήσεις ασφάλειας προκύπτουν. Αυτό είναι η εποχή της πλήρους συνδετικότητας, και ηλεκτρονικά και φυσικά. Οι έξυπνες κάρτες μπορούν να διευκολύνουν αυτήν την συνδετικότητα και άλλες ικανότητες προστιθέμενης αξίας, ενώ παράλληλα παρέχουν τις απαραίτητες διαβεβαιώσεις ασφάλειας που δεν είναι διαθέσιμες μέσω άλλων μέσων.

Στο διαδίκτυο, οι έξυπνες κάρτες αυξάνουν την ασφάλεια της επικύρωσης, της έγκρισης, της ιδιωτικότητας και της ακεραιότητας, των δομικών μονάδων. Πρώτιστα, αυτό είναι επειδή το ιδιωτικό κλειδί υπογραφής δεν αφήνει ποτέ την έξυπνη κάρτα έτσι είναι πολύ δύσκολο να αποκτηθεί η γνώση του ιδιωτικού κλειδιού μέσω ενός συμβιβασμού του συστήματος οικοδεσποτών υπολογιστών (host computer system).

Σε ένα σύστημα εταιρικής επιχείρησης, τα πολλαπλά χωρισμένα συστήματα συχνά απαρτίζονται από συστήματα ασφαλείας τα οποία βασίζονται σε διαφορετικές τεχνολογίες. Οι έξυπνες κάρτες μπορούν να τα συγκεντρώσουν μαζί με την αποθήκευση των πολλαπλών πιστοποιητικών και των κωδικών πρόσβασης στην ίδια κάρτα. Ασφαλές ηλεκτρονικό ταχυδρομείο ,πρόσβαση ενδοδικτύου, τηλεφωνική

πρόσβαση στο δίκτυο, κρυπτογραφημένα αρχεία, ψηφιακά υπογεγραμμένες μορφές διαδικτύου , όλα βελτιώνονται μέσα από την έξυπνη κάρτα.

Σε μια κατάσταση, όπου μια επιχείρηση θα επιθυμούσε να χορηγήσει την ασφάλεια στους επιχειρησιακούς συνεργάτες και τους προμηθευτές, οι έξυπνες κάρτες μπορούν να διανεμηθούν έτσι ώστε να επιτρέπουν την πρόσβαση σε ορισμένους εταιρικούς πόρους. Η σημασία της έξυπνης κάρτας σε αυτήν την κατάσταση είναι εμφανής λόγω της ανάγκης για την ισχυρότερη πιθανή ασφάλεια. Κατά τη διανομή των πιστοποιητικών από την έξυπνη κάρτα, μια επιχείρηση μπορεί να έχει μια υψηλότερη διαβεβαίωση ότι εκείνα τα πιστοποιητικά δεν μπορούν να μοιραστούν, να αντιγραφούν, ή ειδάλλως να συμβιβαστούν.

17.6 ΤΟ ΠΛΕΟΝΕΚΤΗΜΑ ΑΣΦΑΛΕΙΑΣ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ [98]

Μερικοί λόγοι για τους οποίους οι έξυπνες κάρτες μπορούν να ενισχύσουν την ασφάλεια των σύγχρονων συστημάτων είναι:

Α) PKI είναι καλύτερο από τους κωδικούς πρόσβασης –Οι έξυπνες κάρτες ενισχύουν PKI

Τα συστήματα υποδομής δημοσίου κλειδιού είναι ασφαλέστερα από τα συστήματα που είναι βασισμένα στον κωδικό πρόσβασης επειδή δεν υπάρχει καμία κοινή γνώση του μυστικού. Το ιδιωτικό κλειδί χρειάζεται να είναι γνωστό μόνο σε μια θέση, παρά δύο ή περισσότερες.

Εάν η μια θέση είναι σε μια έξυπνη κάρτα, και το ιδιωτικό κλειδί δεν αφήνει ποτέ την έξυπνη κάρτα, το κρίσιμο μυστικό για το σύστημα δεν είναι ποτέ σε μια κατάσταση όπου συμβιβάζεται εύκολα. Μια έξυπνη κάρτα επιτρέπει στο ιδιωτικό κλειδί να είναι χρησιμοποιήσιμο και όμως δεν εμφανίζεται ποτέ σε ένα δίκτυο ή στο σύστημα οικοδεσποτών υπολογιστών.

- **Οι έξυπνες κάρτες αυξάνουν την ασφάλεια των συστημάτων που είναι βασισμένα στον κωδικό πρόσβασης**

Αν και οι έξυπνες κάρτες έχουν τα προφανή πλεονεκτήματα για τα συστήματα PKI, μπορούν επίσης να αυξήσουν την ασφάλεια των συστημάτων που είναι βασισμένα στον κωδικό πρόσβασης. Ένα από τα μεγαλύτερα προβλήματα στα χαρακτηριστικά συστήματα κωδικού πρόσβασης είναι ότι οι χρήστες γράφουν τον κωδικό πρόσβασής τους και τον συνδέουν με την οθόνη ελέγχου ή το πληκτρολόγιό τους. Τείνουν επίσης να επιλέξουν τους αδύνατους κωδικούς πρόσβασης και να μοιραστούν τους κωδικούς πρόσβασής τους με άλλους ανθρώπους.

Εάν μια έξυπνη κάρτα χρησιμοποιείται για να αποθηκεύσει τους πολλαπλούς κωδικούς πρόσβασης ενός χρήστη, χρειάζονται μόνο να θυμηθούν το pin (προσωπικό αριθμό αναγνώρισης) στην έξυπνη κάρτα για να έχουν πρόσβαση σε όλους τους κωδικούς πρόσβασης. Επιπλέον, εάν ένας ανώτερος υπάλληλος ασφάλειας μονογράφει την έξυπνη κάρτα, οι πολύ ισχυροί κωδικοί πρόσβασης μπορούν να επιλεχτούν και να αποθηκευτούν στην έξυπνη κάρτα.

Β) Επικύρωση δύο και περισσοτέρων παραγόντων

Τα συστήματα ασφάλειας ωφελούνται από την επικύρωση πολλαπλών παραγόντων. Οι παράγοντες που συνήθως χρησιμοποιούνται είναι: «Κάτι που εσείς

ξέρετε», «κάτι εσείς έχετε», «κάτι που είστε», και «κάτι που κάνετε».Τα συστήματα που είναι βασισμένα στον κωδικό πρόσβασης χρησιμοποιούν χαρακτηριστικά μόνο τον πρώτο παράγοντα, «κάτι που εσείς ξέρετε». Οι έξυπνες κάρτες προσθέτουν έναν πρόσθετο παράγοντα, «κάτι που εσείς έχετε».

Η επικύρωση δύο παραγόντων έχει αποδειχθεί αποτελεσματικότερη από την ενιαία επειδή το "κάτι που εσείς ξέρετε " είναι ένας παράγοντας που πολύ εύκολα συμβιβάζεται ή μοιράζεται. Οι έξυπνες κάρτες μπορούν επίσης να ενισχυθούν για να περιλάβουν τα υπόλοιπα δύο χαρακτηριστικά γνωρίσματα. Τα πρωτότυπα σχέδια είναι διαθέσιμα να δέχονται ένα δακτυλικό αποτύπωμα στην επιφάνεια της κάρτας εκτός από το pin προκειμένου να ξεκλειδωθούν οι υπηρεσίες της κάρτας.

Εναλλακτικά, ένα πρότυπο με δακτυλικό αποτύπωμα ,ή το πρότυπο αμφιβληστροειδών, ή άλλες βιομετρικές πληροφορίες μπορούν να αποθηκευτούν στην κάρτα, για να ελεγχθούν μόνο σε σχέση με τα στοιχεία που λαμβάνονται από μια χωριστή βιομετρική συσκευή εισαγωγής.

Ομοίως, ο παράγοντας «κάτι που εσείς κάνετε» όπως η δακτυλογράφηση των σχεδίων, χειρόγραφα χαρακτηριστικά υπογραφών, ή τα πρότυπα κάμψης φωνής μπορούν να αποθηκευτούν στην κάρτα και να αντιστοιχηθούν με τα στοιχεία που γίνονται αποδεκτά από τις εξωτερικές συσκευές εισαγωγής.

Γ) Φορητοτητα των κλειδιών και των πιστοποιητικών

Τα δημόσια κλειδιά και τα ιδιωτικά κλειδιά των πιστοποιητικών μπορούν να χρησιμοποιηθούν από τους ξεφυλλιστές Ιστού (web browsers) και άλλα δημοφιλή πακέτα λογισμικού και υπό κάποια έννοια προσδιορίζουν τον τερματικό σταθμό παρά το χρήστη. Το κλειδί και το στοιχείο πιστοποιητικών αποθηκεύονται σε μια ιδιόκτητη περιοχή αποθήκευσης του ξεφυλλισθή και πρέπει να είναι εξαγόμενος /εισαγόμενος προκειμένου να κινηθούν από έναν τερματικό σταθμό προς άλλο.

Με τις έξυπνες κάρτες το πιστοποιητικό και το ιδιωτικό κλειδί είναι φορητά, και μπορούν να χρησιμοποιηθούν στους πολλαπλάσιους τερματικούς σταθμούς, είτε είναι στην εργασία, στο σπίτι, ή στο δρόμο. Εάν τα χαμηλότερα στρώματα λογισμικού επιπέδων το υποστηρίζουν, μπορούν να χρησιμοποιηθούν από τα διαφορετικά προγράμματα λογισμικού από τους διαφορετικούς προμηθευτές, για τις διαφορετικές πλατφόρμες, όπως τα Windows, Unix, και MAC.

Δ) Να θέσει αυτόματα εκτός λειτουργίας τα pin εναντίον των επιθέσεων των λεξικών

Εάν ένα ιδιωτικό κλειδί αποθηκεύεται σε ένα αρχείο αποθήκευσης του ξεφυλλισθή σε έναν σκληρό δίσκο, προστατεύεται χαρακτηριστικά από έναν κωδικό πρόσβασης. Αυτό το αρχείο μπορεί να δεχτεί μια «επίθεση λεξικού» όπου οι συνήθως χρησιμοποιημένοι κωδικοί πρόσβασης προσπαθούνται με έναν τρόπο ωμής βίας να αποκαλύψουν τα στοιχεία του ιδιωτικού κλειδιού.

Αφ' ετέρου, μια έξυπνη κάρτα θα κλειδωθεί αυτόματα μετά από κάποιο χαμηλό αριθμό διαδοχικών κακών προσπαθειών εισαγωγής PIN , παραδείγματος χάριν 10. Κατά συνέπεια, η επίθεση λεξικών δεν είναι πλέον ένας εφικτός τρόπος να προσεγγιστεί το ιδιωτικό κλειδί εάν αυτό έχει αποθηκευτεί ασφαλώς σε μια έξυπνη κάρτα.

Ε) Μη αποκήρυξη

Η δυνατότητα να αρνηθεί, μετά από το γεγονός, ότι το ιδιωτικό κλειδί σας εκτέλεσε μια ψηφιακή υπογραφή καλείται αποκήρυξη. Εάν, εντούτοις, το ιδιωτικό κλειδί υπογραφής σας υπάρχει μόνο σε μια ενιαία έξυπνη κάρτα και εσείς μόνο ξέρετε το PIN σε εκείνη την έξυπνη κάρτα, είναι πολύ δύσκολο για άλλους να μιμηθούν τη ψηφιακή υπογραφή σας με τη χρησιμοποίηση του ιδιωτικού κλειδιού σας. Πολλά ψηφιακά συστήματα υπογραφών απαιτούν "την μη αποκήρυξη δύναμης υλικού", σημαίνοντας ότι το ιδιωτικό κλειδί προστατεύεται πάντα μέσα στην περίμετρο ασφάλειας ενός σημείου υλικού και δεν μπορεί να χρησιμοποιηθεί χωρίς τη γνώση του κατάλληλου PIN. Οι έξυπνες κάρτες μπορούν να παρέχουν την μη αποκήρυξη δύναμης υλικού.

ΣΤ) Υπολογισμός του αριθμού χρήσεων του ιδιωτικού κλειδιού

Πολλά από τα σημαντικά πράγματα στις ζωές μας εγκρίνονται από τη χειρόγραφη υπογραφή μας. Η έξυπνη κάρτα χρησιμοποίησε τις ψηφιακές υπογραφές έτσι ώστε να παρέχουν περισσότερα οφέλη από τις χειρόγραφες υπογραφές επειδή είναι δυσκολότερο να αντιγραφούν και μπορούν να επιβάλουν την ακεραιότητα του εγγράφου μέσω των τεχνολογιών όπως « hashing».

Επίσης, επειδή η υπογραφή είναι βασισμένη σε μια συσκευή που είναι πραγματικά ένας υπολογιστής, μπορούν να συλληφθούν πολλά νέα οφέλη. Παραδείγματος χάριν, μια έξυπνη κάρτα θα μπορούσε να μετρήσει τον αριθμό χρόνων που το ιδιωτικό κλειδί σας χρησιμοποιήθηκε, δίνοντας κατά συνέπεια σας ένα ακριβές μέτρο πόσων φορών χρησιμοποιήσατε την ψηφιακή υπογραφή σας κατά τη διάρκεια μιας δεδομένης χρονικής περιόδου.

17.7 ΕΠΙΘΕΣΕΙΣ ΣΤΙΣ ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ [99]

Οι επιθέσεις των έξυπνων καρτών διακρίνονται σε τέσσερις κατηγορίες :

1) **ΛΟΓΙΚΕΣ ΕΠΙΘΕΣΕΙΣ**

Οι λογικές επιθέσεις εμφανίζονται όταν λειτουργεί μια έξυπνη κάρτα υπό τις κανονικές φυσικές καταστάσεις, αλλά οι ευαίσθητες πληροφορίες λαμβάνονται με την εξέταση των bytes που μεταφέρονται από και προς την έξυπνη κάρτα. Ένα παράδειγμα είναι η αποκαλούμενη "επίθεση συγχρονισμού" που περιγράφεται από τον Paul Kocher. Σε αυτήν την επίθεση, τα διάφορα σχέδια bytes στέλνονται στην κάρτα που υπογράφεται από το ιδιωτικό κλειδί. Υπάρχουν λογικά αντίμετρα σε αυτήν την επίθεση αλλά δεν τα έχουν εφαρμόσει όλοι οι κατασκευαστές έξυπνων καρτών. Αυτή η επίθεση απαιτεί ότι το pin της κάρτας είναι γνωστό ,ώστε να μπορούν να εκτελεσθούν πολλές διαδικασίες ιδιωτικού κλειδιού.

2) **ΦΥΣΙΚΕΣ ΕΠΙΘΕΣΕΙΣ**

Οι φυσικές επιθέσεις εμφανίζονται όταν αλλάζουν οι κανονικές φυσικές καταστάσεις, όπως η θερμοκρασία, η συχνότητα ρολογιών, η τάση, και ούτω καθεξής προκειμένου να αποκτήσουν πρόσβαση στις ευαίσθητες πληροφορίες για την έξυπνη κάρτα. Τα περισσότερα λειτουργικά συστήματα έξυπνων καρτών γράφουν τα ευαίσθητα στοιχεία στην περιοχή EEPROM κατά τρόπο ιδιόκτητο και κρυπτογραφημένο έτσι ώστε είναι δύσκολο να ληφθούν τα κλειδιά με άμεση εισβολή στην EEPROM. Άλλες φυσικές επιθέσεις που έχουν αποδειχθεί επιτυχείς

περιλαμβάνουν μια έντονη φυσική διακύμανση στον ακριβή χρόνο και τη θέση όπου πραγματοποιείται η επαλήθευση pin. Κατά συνέπεια, οι ευαίσθητες λειτουργίες καρτών μπορούν να εκτελεσθούν ακόμα και αν το pin είναι άγνωστο. Αυτός ο τύπος επίθεσης μπορεί να συνδυαστεί με τη προαναφερθείσα λογική επίθεση προκειμένου να αποκτηθεί η γνώση του ιδιωτικού κλειδιού. Οι περισσότερες φυσικές επιθέσεις απαιτούν ειδικό εξοπλισμό.

3) ΕΠΙΘΕΣΕΙΣ ΔΟΥΡΕΙΟΥ ΙΠΠΟΥ

Αυτή η επίθεση περιλαμβάνει έναν απατεώνα, μια εφαρμογή δούρειου ίππου που έχει φυτευτεί στον τερματικό σταθμό ενός ανυποψίαστου χρήστη. Ο δούρειος ίππος περιμένει έως ότου υποβάλλει ο χρήστης ένα έγκυρο PIN από μια εμπιστευμένη εφαρμογή, επιτρέποντας κατά συνέπεια τη χρήση του ιδιωτικού κλειδιού, και ζητά έπειτα από την έξυπνη κάρτα για να υπογράψει ψηφιακά μερικά στοιχεία απατεώνων. Η λειτουργία ολοκληρώνεται αλλά ο χρήστης δεν ξέρει ποτέ ότι το ιδιωτικό κλειδί τους μόλις χρησιμοποιήθηκε ενάντια στη θέλησή τους.

Το αντίμετρο για να αποτρέψει αυτήν την επίθεση είναι να χρησιμοποιηθεί μια αρχιτεκτονική "οδηγών συσκευών ενιαίας-πρόσβασης". Με αυτόν τον τύπο αρχιτεκτονικής, το λειτουργικό σύστημα επιβάλλει ότι μόνο μια εφαρμογή μπορεί να έχει πρόσβαση στην τμηματική συσκευή (και έτσι την έξυπνη κάρτα) οποιαδήποτε στιγμή. Αυτό αποτρέπει την επίθεση αλλά και ελαττώνει την ευκολία της έξυπνης κάρτας επειδή οι πολλαπλές εφαρμογές δεν μπορούν να χρησιμοποιήσουν τις υπηρεσίες της κάρτας συγχρόνως. Ένας άλλος τρόπος να αποτραπεί η επίθεση είναι με τη χρησιμοποίηση μιας έξυπνης κάρτας που επιβάλλει ένα πρότυπο πολιτικής κατά το οποίο "κατά τη χρήση ενός ιδιωτικού κλειδιού να αντιστοιχεί μία μόνο εισαγωγή pin ". Σε αυτό το πρότυπο, ο χρήστης πρέπει να εισαγάγει το pin του κάθε φορά που το ιδιωτικό κλειδί πρόκειται να χρησιμοποιηθεί και επομένως ο δούρειος ίππος δεν θα είχε πρόσβαση στο κλειδί.

4) ΚΟΙΝΩΝΙΚΕΣ ΕΠΙΘΕΣΕΙΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΜΗΧΑΝΙΚΗΣ

Στα συστήματα ασφάλειας υπολογιστών, αυτός ο τύπος επίθεσης είναι συνήθως ο επιτυχέστερος, ειδικά όταν εφαρμόζεται κατάλληλα και μετασχηματίζεται η τεχνολογία ασφάλειας. Συνήθως, αυτές οι επιθέσεις στηρίζονται στα ελαττώματα των ανθρώπινων όντων. Ένα παράδειγμα μιας κοινωνικής επίθεσης εφαρμοσμένης μηχανικής είναι ένας «χάκερ» που μιμείται έναν τεχνικό υπηρεσιών δικτύων και πλησιάζει έναν χαμηλού επιπέδου υπάλληλο και ζητά τον κωδικό πρόσβασής τους με σκοπό τη συντήρηση του δικτύου. Με τις έξυπνες κάρτες, αυτός ο τύπος επίθεσης είναι δυσκολότερος. Οι περισσότεροι άνθρωποι δεν θα εμπιστεύονταν έναν μιμητή που επιθυμεί την έξυπνη κάρτα και το pin τους για λόγους υπηρεσιών.

Οποιοδήποτε σύστημα ασφάλειας, συμπεριλαμβανομένων των έξυπνων καρτών, είναι εύθραυστο. Εντούτοις, υπάρχει μια εκτίμηση για το κόστος που απαιτείται για να σπάσει το σύστημα, το οποίο πρέπει να είναι πολύ μεγαλύτερο από την αξία της προστασίας των στοιχείων από το σύστημα. Υπάρχουν ανεξάρτητα εργαστήρια που κάνουν δοκιμές ασφαλείας και επιτίθενται σε έξυπνες κάρτες και μπορούν συνήθως να παρέχουν μια εκτίμηση του κόστους για τον εξοπλισμό και την αιτούμενη πείρα για να σπάσει μια έξυπνη κάρτα. Έτσι κατά τη διάρκεια επιλογής μιας έξυπνης κάρτας, μπορούμε να ρωτήσουμε τον κατασκευαστή για τις αναφορές στα ανεξάρτητα εργαστήρια στα οποία έχουν κάνει τη δοκιμή ασφάλειας.

18 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΑΔΥΝΑΜΙΕΣ ΤΩΝ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ [100]

Το τμήμα αυτό περιγράφει τους λόγους για τους οποίους θα έπρεπε οι διάφοροι οργανισμοί και επιχειρήσεις να εξετάσουν τη χρήση των έξυπνων καρτών. Γίνεται επεξήγηση των βασικών πλεονεκτημάτων της τεχνολογίας των έξυπνων καρτών και επισημαίνονται τα εμπόδια που υπάρχουν στην αποδοχή των έξυπνων καρτών.

Οι έξυπνες κάρτες συντελούν στην προσπάθεια μιας εταιρείας για εξέλιξη και επέκτασή της σε μια διαρκώς μεταβαλλόμενη παγκόσμια αγορά. Το πεδίο χρήσεων μιας έξυπνης κάρτας γίνεται με το χρόνο ευρύτερο ώστε να συμπεριλάβει εφαρμογές που απευθύνονται σε διάφορα τμήματα της αγοράς.

Θα μπορούσαμε να πούμε ότι οι επιχειρήσεις και οι οργανισμοί στις οποίες συμβαίνουν τα εξής:

- είναι απαραίτητη η ύπαρξη ενός φορητού αρχείου μιας ή περισσότερων εφαρμογών,
- τα αρχεία είναι πιθανό να απαιτούν ενημέρωση κατά τη διάρκεια του χρόνου,
- τα αρχεία θα διασυνδέονται με περισσότερα από ένα αυτοματοποιημένα συστήματα,
- η ασφάλεια και η εμπιστευτικότητα των αρχείων είναι σημαντικές, θα έπρεπε να ενσωματώσουν την τεχνολογία των έξυπνων καρτών στη λειτουργία τους. Η έξυπνη κάρτα είναι μια εφικτή λύση αυτοματοποίησης για να καταστήσει την επεξεργασία και τη μεταφορά δεδομένων αποδοτικότερη και ασφαλέστερη.

18.1 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΤΩΝ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ

Τα βασικά πλεονεκτήματα της τεχνολογίας των smart cards είναι:

- Ύπαρξη διεθνών προτύπων, που εξασφαλίζουν τη διάθεση των καρτών από πολλούς προμηθευτές και επομένως περισσότερο ανταγωνιστικές τιμές.
- Μεγάλη διάρκεια ζωής (οι προμηθευτές εγγυώνται μέχρι 10.000 αναγνώσεις/ εγγραφές της ίδιας κάρτας).
- Λειτουργικά συστήματα που υποστηρίζουν τις πολλαπλές εφαρμογές και εξασφαλίζουν την ανεξάρτητη αποθήκευση δεδομένων στην ίδια κάρτα.

Ειδικότερα, όσον αφορά την **Λειτουργικότητα:**

- ικανότητα επεξεργασίας, όχι μόνο αποθήκευσης πληροφορίας.
- δυνατότητα επικοινωνίας με άλλα υπολογιστικά συστήματα μέσων ενός smart card reader.
- δυνατότητα ενημέρωσης- ανανέωσης των πληροφοριών και εφαρμογών που βρίσκονται αποθηκευμένες στην κάρτα, χωρίς να είναι απαραίτητη η έκδοση νέας κάρτας.

Ειδικότερα, όσον αφορά την **Ασφάλεια:**

- δυνατότητα ασφαλούς, off-line επεξεργασίας, λόγω της ύπαρξης των μικροεπεξεργαστών και των δεδομένων πάνω στην κάρτα.
- δυνατότητα προστασίας ανάγνωσης ή εγγραφής των πληροφοριών της κάρτας με χρήση ενός κωδικού PIN.
- δυνατότητα πραγματοποίησης κρυπτογράφησης.

18.2 ΕΜΠΟΔΙΑ ΚΑΤΑ ΤΗΝ ΑΠΟΔΟΧΗ ΤΩΝ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ

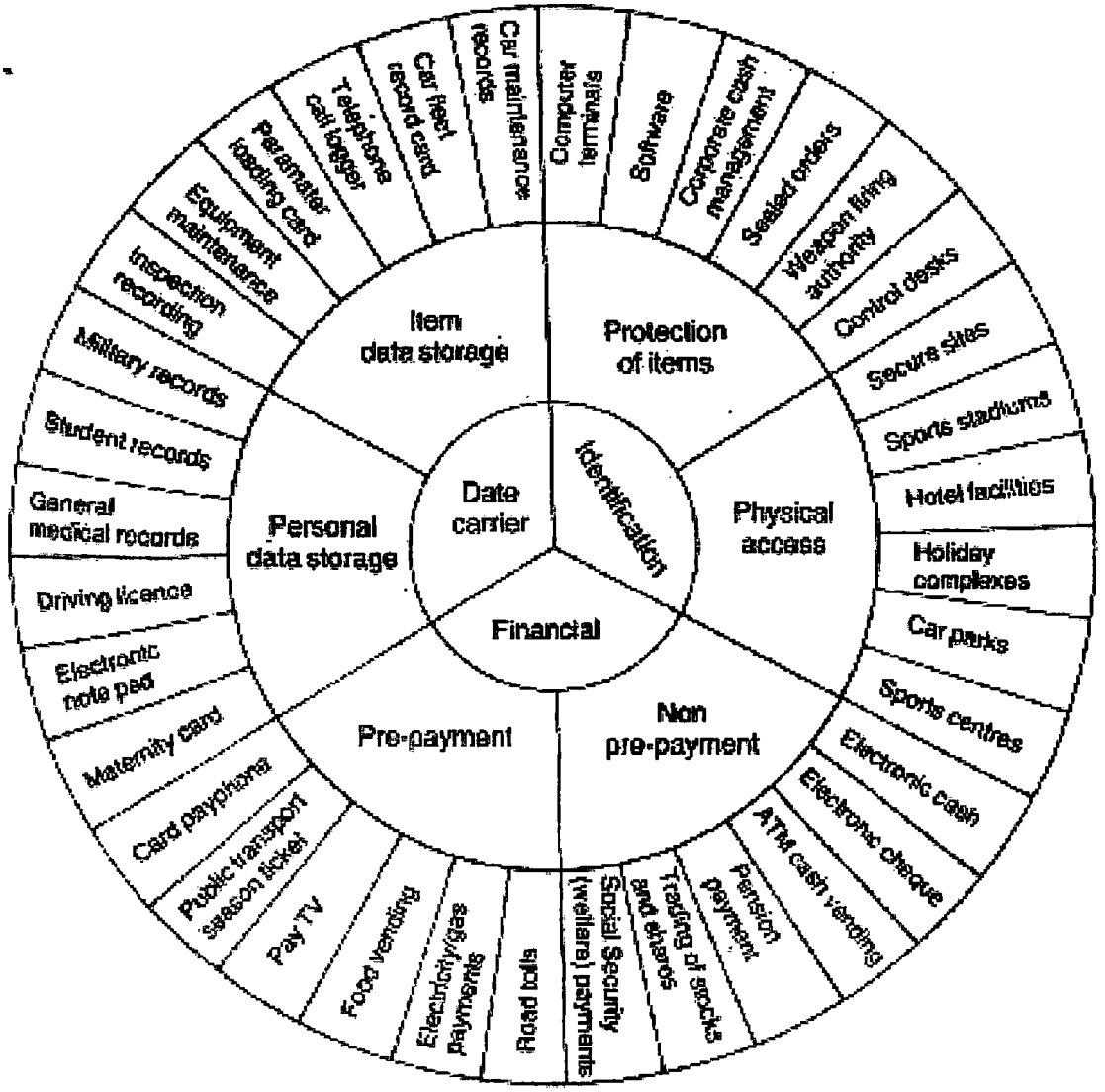
Υπάρχουν όμως και κάποιοι παράγοντες που εμποδίζουν την αποδοχή της τεχνολογίας έξυπνων καρτών. Μερικοί από αυτούς είναι:

- Το σχετικά υψηλότερο κόστος των έξυπνων καρτών σε σύγκριση με τις μαγνητικές κάρτες. Βέβαια η διαφορά αυτή στο κόστος μεταξύ των δύο τεχνολογιών μειώνεται σημαντικά αν λάβουμε υπόψη τη διαφορά στην αναμενόμενη διάρκεια ζωής της κάρτας, καθώς και την ικανότητα υποστήριξης πολλαπλών εφαρμογών.
- Έλλειψη παρούσας υποδομής για να υποστηρίξει την έξυπνη κάρτα.
- Ο καταναλωτής πρέπει να είναι τεχνικά πεπειραμένος για να επιλέξει την πιο κατάλληλη κάρτα για την εφαρμογή στόχων.
- Έλλειψη προτύπων για την εξασφάλιση διαλειτουργικότητας των προγραμμάτων μεταξύ των ποικίλων έξυπνων καρτών.
- Εκκρεμή νομικά και ζητήματα πολιτικής, όπως νόμοι προστασίας καταναλωτών ή προστασίας των ιδιωτικών δεδομένων.

19 ΕΦΑΡΜΟΓΕΣ ΤΩΝ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ [101]

Σε αυτό το κεφάλαιο θα εξετάσουμε μερικές από τις εφαρμογές στις οποίες χρησιμοποιείται η έξυπνη κάρτα. Δεδομένου ότι οι εφαρμογές για την έξυπνη κάρτα είναι ατελείωτες και αρκετά εκτενείς, αυτό το κεφάλαιο προορίζεται να δώσει μια επισκόπηση σε αυτές τις εφαρμογές.

Οι πρακτικές εφαρμογές μιας έξυπνης κάρτας μπορούν να ταξινομηθούν ευρέως σε 3 κύριες κατηγορίες όπως φαίνεται στο παρακάτω σχήμα :



ΕΙΚΟΝΑ 37 : Μερικές από τις πολλές εφαρμογές των έξυπνων καρτών

Οι πρώτες τσιπ κάρτες ήταν απλές προπληρωμένες τηλεφωνικές κάρτες που εφαρμόστηκαν στην Ευρώπη στα μέσα της δεκαετίας του '80 (κάρτες μνήμης). Σήμερα, οι σημαντικότεροι τομείς εφαρμογής για τις βασισμένες σε μικροεπεξεργαστή έξυπνες κάρτες είναι: οικονομικός, επικοινωνίες, κυβερνητικά προγράμματα, ασφάλεια πληροφοριών, φυσική ασφάλεια πρόσβασης, μεταφορά, λιανική πώληση και πίστη (loyalty), υγειονομική περίθαλψη, και university identification.

Στις ενότητες που ακολουθούν θα αναφερθούμε στις σημαντικότερες εφαρμογές των έξυπνων καρτών.

19.1 ΧΡΗΣΗ ΤΩΝ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ ΣΤΙΣ ΜΕΤΑΦΟΡΕΣ [102]

Η Έξυπνη κάρτα και συγκεκριμένα η έξυπνη κάρτα χωρίς επαφή παρέχει τη μέγιστη ταχύτητα πρόσβασης σε υπηρεσίες εισιτηρίων και διοδίων για την χρήση μέσων μαζικής μεταφοράς και οδικών δικτύων αντίστοιχα , χωρίς περιορισμούς στον τομέα της ασφάλειας της οικονομικής συναλλαγής .Πρόσθετα ,παρέχει δυνατότητες και προϋποθέσεις για την δημιουργία διαλειτουργικών υπηρεσιών για όλα τα μέσα μαζικής μεταφοράς και οδικά δίκτυα, προσφέροντας στον πολίτη ένα σύνολο εξυπηρετήσεων που οι συμβατικές τεχνολογίες δύσκολα θα υποστήριζαν.

Συμπερασματικά οι εφαρμογές στον τομέα των Μεταφορών που μπορούν να προσφέρουν οι έξυπνες κάρτες είναι οι εξής:

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

Από τα παραπάνω, η πιο σημαντική εφαρμογή, σύμφωνη με την ανάλυση που γίνεται σε αυτό το έγγραφο, είναι οι δημόσιες συγκοινωνίες, παρόλο που σε μερικά χρόνια μπορεί να θεωρείται εξίσου σημαντική και η εφαρμογή της πληρωμής διοδίων. Επιπλέον η εφαρμογή για δικαιώματα parking μπορεί να συνδυαστεί αποτελεσματικά με τη πληρωμή διοδίων και /ή τις δημόσιες συγκοινωνίες.

Ένας τέτοιος συνδυασμός μπορεί να επιτρέπει, οι πληρωμές για parking να πιστώνονται ακόμα και στην περίπτωση που κάποιος παρκάρει το αυτοκίνητό του και συνεχίζει το ταξίδι του με δημόσια συγκοινωνία. Επίσης η υπηρεσία κράτησης αεροπορικών εισιτηρίων μπορεί να πραγματοποιηθεί από μία ξεχωριστή κάρτα ή να συμπεριληφθεί σε μία γενική Έξυπνη κάρτα των πολιτών.

Μερικά από τα πολυάριθμα παραδείγματα των έξυπνων καρτών στη μεταφορά είναι:

➢ **<u>Δημόσιες συγκοινωνίες</u>**

Η χρησιμοποίηση των ανέπαφων έξυπνων καρτών επιτρέπει σε έναν επιβάτη να επιβιβαστεί σε διάφορα λεωφορεία και τραίνα κατά τη διάρκεια της καθημερινής του διαδρομής από και προς το χώρο εργασίας του χωρίς να ανησυχεί για το αν έχει πάνω του κέρματα ή εισιτήρια.

Στο Λονδίνο, τα λεωφορεία χρησιμοποιούν τις ανέπαφες έξυπνες κάρτες για να συλλέξουν τις τιμές. Κάθε φορά που μπαίνουν οι επιβάτες σε ένα λεωφορείο, περνούν την κάρτα τους μπροστά από έναν αναγνώστη που αφαιρεί την τιμή από την πίστωση που αποθηκεύεται στην κάρτα. Επίσης προγραμματίζουν να επεκτείνουν αυτήν την μορφή πληρωμής στο χώρο στάθμευσης υπόγειων και αυτοκινήτων σταθμών.

➢ **<u>Αστικός χώρος στάθμευσης</u>**

Δεν χρειάζεται πλέον να κουβαλάτε το απαραίτητο ποσό κερμάτων .Αρκεί να έχετε μαζί σας μια έξυπνη κάρτα προπληρωμένης αξίας.

➢ **Ηλεκτρονική συλλογή φόρου**

Όπως οδηγείτε μέσω της πύλης διοδίων μιας γέφυρας ,μια έξυπνη κάρτα που παρεμβάλλεται σε έναν αναμεταδότη μέσα στο αυτοκίνητο σας ολοκληρώνει τη συναλλαγή πληρώνοντας ηλεκτρονικά το φόρο διοδίων .

Το σύστημα ηλεκτρονικής οδικής τιμολόγησης αποτελείται από τρία κύρια συστατικά : 1) τον ατσάλινο σκελετό 2)την μονάδα IU (In vehicle unit) που είναι μια ηλεκτρονική συσκευή που εγκαθίσταται στο όχημα που δέχεται μια έξυπνη κάρτα αποθηκευμένης αξίας και 3) το συγκρότημα κεντρικών ηλεκτρονικών υπολογιστών.

Το IU αφαιρεί τις κατάλληλες δαπάνες από την έξυπνη κάρτα κάθε φορά που περνά το όχημα μέσω του ατσάλινου σκελετού ERP. Σε περίπτωση που κάποιος κάνει παράνομη καταχώρηση όπως εκείνοι που περνάνε χωρίς μια μονάδα IU ,ή χωρίς κάρτα με αποθηκευμένη αξία ή ακόμα και με κάρτα με ανεπαρκές υπόλοιπο ,θα φωτογραφηθούν από τις ειδικές φωτογραφικές μηχανές που είναι ενσωματωμένοι στους ατσάλινους σκελετούς για μελλοντική παρακράτηση του αντίστοιχου ποσού.

19.2 ΟΙ ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ ΣΤΟ ΧΩΡΟ ΤΗΣ ΥΓΕΙΑΣ [103]

Στο χώρο της υγείας η προστασία των ευαίσθητων προσωπικών δεδομένων (η διασφάλιση του ιατρικού απορρήτου), είτε αυτά αποτελούν αποσπάσματα του ιατρικού φακέλου, είτε απλώς δείκτες σε συγκεκριμένους δικτυακούς τόπους που υποστηρίζουν εφαρμογές παροχής ιατρικής φροντίδας /πληροφορίας, αποτελεί ζήτημα μείζονος σημασίας . Οι έξυπνες κάρτες από πλευράς τεχνολογίας είναι το ασφαλέστερο μέσο ,τόσο για την ασφαλή πρόσβαση σε ειδική και γενική ιατρική πληροφορία όσο και για την αποθήκευση δεδομένων υγείας .Στο χώρο της ασφάλισης οι έξυπνες κάρτες μπορούν να αντικαταστήσουν τα παραδοσιακά χάρτινα βιβλιάρια, με σκοπό να προσφέρουν ταχύτητα συναλλαγής ασφάλεια συναλλαγής και ευκολία πρόσβασης σε νέες ηλεκτρονικές υπηρεσίες.

Η έξυπνη κάρτα μπορεί να χρησιμοποιηθεί για την ασφαλή αποθήκευση στοιχείων ταυτότητας, ασφάλισης και ιατρικών δεδομένων ενός ατόμου ή για την αποθήκευση των σημείων όπου βρίσκονται στοιχεία ιατρικού φακέλου (pointer cards). Με τον τρόπο αυτό οι πληροφορίες είναι έγκαιρα και έγκυρα διαθέσιμες στους ασθενείς και ιατρούς υποστηρίζοντας και διευκολύνοντας σημαντικά την ελεύθερη διακίνηση των ασθενών που μπορούν να ταξιδεύουν στο εσωτερικό και στο εξωτερικό φέροντας μαζί τους τον ασφαλιστικό και ιατρικό τους φάκελο.

Πέραν αυτού, οι έξυπνες κάρτες στο τομέα της υγείας χρησιμοποιούνται σε εφαρμογές ταυτοποίησης του ασθενούς και επαγγελματιών υγείας (ιατρών, νοσηλευτών κλπ), ηλεκτρονικών υπογραφών για την ακεραιότητα και την αυθεντικότητα των ιατρικών δεδομένων, κρυπτογράφησης των δεδομένων για τη διασφάλιση της εμπιστευτικότητας (health professional cards), ασφαλή πρόσβαση σε δίκτυα υγείας κλπ.

Στην υγειονομική περίθαλψη, οι έξυπνες κάρτες μπορούν να χρησιμοποιηθούν σαν ιατρικές κάρτες σαν κάρτα ασφάλειας υγείας ή ιατρική κάρτα πρόσβασης αρχείων.

Αυτό έχει τα ακόλουθα πλεονεκτήματα

- μειώνει τη στερεότυπη γραφική εργασία.
- εξαλείφει τα λάθη και την απάτη.

- επιταχύνει τις διαδικασίες πληρωμής.
- οργάνωση εξοπλισμού χωρίς πολλά έξοδα.
- το ιστορικό και τα ιατρικά στοιχεία του ασθενή μπορούν να αποθηκευτούν και διατίθενται εύκολα χρησιμοποιώντας έναν αναγνώστη καρτών.
- ο ασθενής ελέγχει τη πρόσβαση των γιατρών στις πληροφορίες.
- ο φαρμακοποιός έχει πρόσβαση στις πληροφορίες συνταγών μόνο.

ΕΙΚΟΝΑ 38 : Μια έξυπνη κάρτα υγειονομικής περίθαλψης

19.3 ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ [104]

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

➢ **Προπληρωμένες τηλεφωνικές κάρτες**

Τα οφέλη των προπληρωμένων καρτών μπορούν να βρεθούν σε πολλές άλλες εφαρμογές όπου οι μηχανές που λειτουργούν με κέρματα πάσχουν από τις αυξανόμενες δαπάνες και την απώλεια υπηρεσιών από το βανδαλισμό, συλλογή νομισμάτων, και χαμηλή αξιοπιστία. Οι έξυπνες κάρτες χρησιμοποιούνται ήδη σαν αντικατάσταση μετρητών για :

- θάλαμοι φόρου.
- μέρη χώρων στάθμευσης.
- βενζινάδικα.
- μηχανές πώλησης.

➢ **Εξασφάλιση των κινητών τηλεφώνων**

Το σύστημα ράδιο τηλεφώνων GSM (παγκόσμιο σύστημα για την κινητή επικοινωνία), που δημιουργήθηκε στην Ευρώπη όχι μόνο επιτρέπει σε κάθε εθνικό

χειριστή να κρατήσει τον έλεγχο των πτυχών ασφάλειας και πληρωμής, αλλά συγχρόνως διευκολύνει τη διασυνοριακή χρήση των κινητών τηλεφώνων.

Το GSM χρησιμοποιεί μια έξυπνη κάρτα που αποθηκεύει όλες τις προσωπικές πληροφορίες του συνδρομητή. Η έξυπνη κάρτα παρεμβάλλεται σε οποιοδήποτε τηλέφωνο GSM για την κατάλληλη λειτουργία. Οι κλήσεις στον κινητό αριθμό των συνδρομητών θα κατευθυνθούν αναλόγως και οι λογαριασμοί θα χρεωθούν στον προσωπικό απολογισμό του συνδρομητή. Όσον αφορά την εξασφάλιση των στοιχείων σχετικά με τη συνδρομή GSM αυτά φυλάσσονται στην έξυπνη κάρτα και όχι στο τηλέφωνο.

Ένας μυστικός κώδικας, γνωστός ως PIN (προσωπικός αριθμός αναγνώρισης), ενσωματώνεται επίσης για να προστατεύει τον συνδρομητή από την κακή χρήση και την απάτη Με την έξυπνη κάρτα, το κινητό τηλέφωνο μπορεί επίσης να ανακατώσει τις κλήσεις για να εξασφαλίσει εμπιστευτικότητα. Τα πρότυπα GSM και τα υποσύνολά του χρησιμοποιούνται σε πάνω από 90 χώρες παγκοσμίως (Gemplus).

Αυτή τη στιγμή κυκλοφορούν παγκοσμίως πολλά δισεκατομμύρια τηλεκάρτες και εκατοντάδες εκατομμύρια SIM κάρτες αφού τα GSM τηλέφωνα υπολογίζονται σε 500.000.000.

19.4 ΠΡΟΣΩΠΙΚΟΣ ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΚΑΙ ΠΡΟΣΒΑΣΗ [105]

Διάφορες χώρες συμπεριλαμβανομένης της Ισπανίας και της Νότιας Κορέας έχουν αρχίσει τις δοκιμές με τις έξυπνες κάρτες που παρέχουν τον προσδιορισμό για τους πολίτες της. Στην Ισπανία, η κάρτα ταυτότητας κοινωνικής ασφάλισης έχει διανεμηθεί σε 500.000 πολίτες που παρέχει την πρόσβαση στα ιατρικά οφέλη.

Επτά εκατομμύρια εκδόθηκαν μέχρι το 1997, και 40 εκατομμύρια έχουν προγραμματιστεί από το έτος 2001 και ύστερα. Ο έλεγχος των στοιχείων γίνεται με αποθηκευμένα δακτυλικά αποτυπώματα. Ένα πιλοτικό έργο είναι σε λειτουργία στη Νότια Κορέα που περιλαμβάνει τον προσωπικό προσδιορισμό στοιχείων, την άδεια του οδηγού και την ιατρική ασφάλεια .

- **<u>Έλεγχος πρόσβασης στα κτίρια</u>**

Μία έξυπνη κάρτα μπορεί να αποθηκεύσει τα στοιχεία αναγνώρισης ενός ατόμου για τον έλεγχο πρόσβασης σε κτίρια υψηλής και μη ασφάλειας κα χώρους εργασίας αλλά και σε πανεπιστήμια, σχολεία, βιβλιοθήκες και λέσχες. Για ανάγκες υψηλότερης ασφάλειας και πρόσβαση σε συγκεκριμένες υπηρεσίες ή πληροφορίες, μια έξυπνη κάρτα μπορεί να αποτελέσει μια συσκευή για την αποθήκευση πληροφοριών όπως η εικόνα ή άλλα βιομετρικά χαρακτηριστικά (π.χ. τα δακτυλικά αποτυπώματα, ίριδα του ματιού) του χρήστη.

Η ίδια κάρτα μπορεί στη συνέχεια να διατηρεί στοιχεία για την ταυτοποίηση του ατόμου στα υπολογιστικά συστήματα του οργανισμού. Παράδειγμα αποτελεί η κάρτα Mcard, που χρησιμοποιείται από 110.000 μέλη του Πανεπιστημίου του Michigan [URL :http//www.mcard.umich.edu/] και σε αυτή υπάρχουν πληροφορίες για την ταυτότητα του κάθε φοιτητή και μπορεί να χρησιμοποιηθεί για χρηματοοικονομικές συναλλαγές, για αγορά φαγητού, βιβλίων, για φωτοαντίγραφα και άλλες χρήσεις.

- **<u>Πρόσβαση σε ανοιχτά ή κλειστά δίκτυα</u>**

Οι έξυπνες κάρτες μπορούν να αποθηκεύσουν ψηφιακά πιστοποιητικά (digital certificates) και άλλες πληροφορίες για τον έλεγχο του δικαιώματος πρόσβασης του χρήστη, ώστε να μπορεί να χρησιμοποιεί υπολογιστικά και δικτυακά συστήματα με ασφαλή τρόπο.

Η ασφάλεια εδώ αναφέρεται τόσο στην πιστοποίηση της ταυτότητας του χρήστη, όσο και στη δημιουργία ιδιωτικών εικονικών δικτύων (VPN) για την πρόσβαση εταιρικών συστημάτων από δημόσια δίκτυα, όπως για παράδειγμα το Internet.

19.5 ΗΛΕΚΤΡΟΝΙΚΟ ΠΟΡΤΟΦΟΛΙ [106]

Η Έξυπνη κάρτα σταδιακά αντικαθιστά την τεχνολογία της μαγνητικής λωρίδας στις πιστωτικές/ χρεωστικές κάρτες βοηθώντας στην καταπολέμηση της διευρυνόμενης απάτης σε διεθνή κλίμακα .Παράλληλα μπορεί να διευκολύνει τις αγορές μέσω διαδικτύου , δικτύων κινητής τηλεφωνίας, άλλων συμβατικών δικτύων (π.χ κοινόχρηστη τηλεφωνία) ή και νέων εφαρμογών όπως η πλατφόρμα ψηφιακής τηλεόρασης κλπ. Η μεγάλη αυτή τεχνολογική μετάπτωση γίνεται με βάση τις προδιαγραφές EMV.Τέλος μικρά ποσά θα μπορούν να αποθηκεύονται σε κάρτες (ηλεκτρονικό πορτοφόλι) για να διευκολύνουν τις καθημερινές συναλλαγές μικρής αξίας και να μειώσουν την ανάγκη χρήσης κερμάτων ιδιαίτερα σε αυτόματους πωλητές.

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

Με αυτό τον τρόπο διευκολύνεται η άμεση είσπραξη του πληρωτέου ποσού καθώς επίσης και η εκκαθάριση μεταξύ καταστημάτων και τραπεζικών ιδρυμάτων. Επιτυχημένα παραδείγματα ηλεκτρονικού πορτοφολιού είναι η κάρτα Mondex [URL: http://www.mondex.com] και τα αντίστοιχα της Visa [URL: http://www.visa.com /pd/ewallet/main.html].

19.6 ΤΡΑΠΕΖΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ [107]

Μεγάλοι τραπεζικοί οργανισμοί, όπως για παράδειγμα η Visa και η American Express θεωρούν ήδη τις έξυπνες κάρτες ως το επόμενο βήμα στις τραπεζικές συναλλαγές, καθώς προσφέρουν σημαντικά πλεονεκτήματα έναντι των καρτών με μαγνητική λωρίδα.

Για το λόγο αυτό έχει συσταθεί η εταιρεία **EMVco** (EUROPAY-MASTECARD-VISA corporation) η οποία επεξεργάζεται τις προδιαγραφές EMV τις οποίες θα πρέπει να ακολουθήσουν όλα τα εμπλεκόμενα μέρη (Τράπεζες, κατασκευαστές καρτών και εξοπλισμού, εταιρείες ανάπτυξης λογισμικού τερματικών συσκευών κ.α.) προκειμένου να είναι δυνατή η επίτευξη EMV συναλλαγών.

Η νεότερη έκδοση EMV προδιαγραφών είναι τα EMV2000. Οι EMV κάρτες θα αντικαταστήσουν τις πιστωτικές και χρεωστικές κάρτες μαγνητικής πίστας, ενώ θα μπορούν να υποστηρίζουν και επιπλέον εφαρμογές π.χ. κάρτες πελατειακής πίστης (loyalty), ηλεκτρονικό πορτοφόλι κ.α.

Τέλος οι EMV κάρτες θα μπορούν να χρησιμοποιηθούν επίσης σε τραπεζικές συναλλαγές εξ αποστάσεως (internet banking, mobile banking), με τη χρήση ηλεκτρονικών πιστοποιητικών για την πιστοποίηση της ταυτότητας του χρήστη.

19.7 ΚΑΡΤΑ ΔΙΑΤΗΡΗΣΙΜΟΤΗΤΑΣ ΚΑΙ ΕΞΥΠΗΡΕΤΗΣΗΣ ΠΕΛΑΤΩΝ (LOYALTY CARDS) [108]

Οι επιχειρήσεις λιανικού εμπορίου έχουν τη δυνατότητα να χρησιμοποιούν τις έξυπνες κάρτες προκειμένου να εξυπηρετούν πιο αποτελεσματικά τους πελάτες τους και να τους κρατούν πιστούς. Για παράδειγμα μπορούν να πριμοδοτούν τους πελάτες τους με κάποιους πόντους σε κάθε τους αγορά και να τους επιβραβεύουν δίνοντας τους δώρα με την εξαργύρωση των πόντων αυτών όταν φτάσουν σε ένα ορισμένο επίπεδο πόντων.

Το γεγονός ότι οι πόντοι αποθηκεύονται στο chip προσφέρει δύο βασικά πλεονεκτήματα:

Α Δεν χρειάζεται να υπάρχει δίκτυο μεταξύ των καταστημάτων προκειμένου να ενημερώνεται μία κεντρική βάση με τους πόντους του πελάτη.
Β Ο πελάτης επιβραβεύεται άμεσα με την επίτευξη του ορίου πόντων, δίνοντάς του επιπλέον κίνητρο για αγορές. Με τον τρόπο αυτό κρατούν πιστούς τους πελάτες τους ενώ ταυτόχρονα παίρνουν πληροφορίες για τις καταναλωτικές τους συνήθειες, στοιχεία πολύτιμα τόσο για την στρατηγική marketing και πωλήσεων όσο και για την αποτελεσματικότερη εξυπηρέτηση των πελατών τους.

19.8 ΠΡΟΗΓΜΕΝΕΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΥΠΟΓΡΑΦΕΣ ΣΕ ΗΛΕΚΤΡΟΝΙΚΑ ΕΓΓΡΑΦΑ [109]

Οι έξυπνες κάρτες, με τις δυνατότητες δημιουργίας ζεύγους κλειδιών, και ασφαλούς εναποθήκευσης ιδιωτικών κλειδιών και ηλεκτρονικών πιστοποιητικών που παρέχουν, αποτελούν αξιόπιστο τμήμα των "ασφαλών διατάξεων δημιουργίας υπογραφής" που απαιτεί η Ευρωπαϊκή Οδηγία 93 του 1999 "για τις ηλεκτρονικές υπογραφές" και το αντίστοιχο ελληνικό Π.Δ 150/2001, ώστε οι κάτοχοί τους, που πιστοποιούν την ταυτότητά τους με "αναγνωρισμένα πιστοποιητικά" από έναν κατάλληλο "Πάροχο Υπηρεσιών Πιστοποίησης", να μπορούν να υπογράφουν ηλεκτρονικά έγγραφα με δικονομική αξία ίση με αυτήν της ιδιόχειρης υπογραφής τους στα έντυπα έγγραφα".

Κατά την εφαρμογή των παραπάνω εμπλέκονται τρεις (3) οντότητες:

1 Πάροχος Υπηρεσιών Πιστοποίησης (Έμπιστη Τρίτη Οντότητα).

2 Τελική οντότητα (αποδέκτης της ηλεκτρονικής υπογραφής και του πιστοποιητικού, ή αλλιώς "βασιζόμενο μέρος"), συνήθως παροχέας υπηρεσιών ασφαλούς δικτύου στους πελάτες του (π.χ. Τράπεζα).

3 Τελικός χρήστης-υπογράφων (π.χ. πελάτης Τράπεζας).

19.9 ΓΝΩΣΤΕΣ ΕΦΑΡΜΟΓΕΣ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ ΚΑΤΑ ΤΟΜΕΑ ΚΑΙ ΤΥΠΟ ΚΑΡΤΑΣ [110]

	Stored Value Cards	Data Information Files	Identification / Access Security	Membership Cards
Τραπεζικός Τομέας	• Ηλεκτρονικό πορτοφόλι • Τραπεζικές συναλλαγές • Ηλεκτρονικές πληρωμές • Ασφαλιστική αίτηση		• Πρόσβαση με συγκεκριμένο λογαριασμό • Ασφάλεια με χρήση διαδικτύου στο σπίτι	• Πιστωτικές Κάρτες • Χρεωστικές κάρτες
Τηλεπικοινωνίες	• Προπληρωμένη τηλεκάρτα	• Αποθήκευση αριθμού	• Κάρτες SIM /GSM	
Δημόσιος Τομέας	• Διαχείριση λογαριασμών • (συντάξεις, επιδόματα κτλ) • Προηγμένες ηλεκτρονικές Υπογραφές σε ηλεκτρονικά έγγραφα.		• Διαβατήριο • Ταυτότητα • Δίπλωμα Οδήγησης	
Μεταφορές	• Ηλεκτρονικά εισιτήρια • (ημερήσια ,μηνιαία ή ετήσια εισιτήρια) • Αυτόματη πληρωμή διοδίων • Πληρωμές μεταφορικών μέσων με ηλεκτρονικό πορτοφόλι (τρένο, ταξί, λεωφορείο κ.τ.λ)		• Κάρτα επιβίβασης – πάσο δωρεάν επιβίβασης • Κάρτα πρόσβασης Οχήματος 4 σε ζώνη ελεγχόμενης πρόσβασης	• Κάρτα τήρησης post payment contract
Υγεία	• Πληρωμές ασφάλειας • Ιατρικές πληρωμές	• Αποθήκευση / Ανάκτηση ιατρικού ιστορικού • Αποθήκευση πληροφοριών δότη		• Κάρτα υγείας

ΕΙΚΟΝΑ 39 : Γνωστές εφαρμογές έξυπνων καρτών κατά τομέα και τύπο κάρτας

	Stored Value Cards	Data / Information Files	Identification Access / Security	Membership Cards
Λοιπά	• Κρατήσεις ξενοδοχείων • Πληρωμές μισθοδοσίας προσωπικού • Πληρωμές μέσω τηλεόρασης • Χρηματική μεταφορά από άτομο σε άτομο • Πρόγραμμα διατηρησιμότητας και εξυπηρέτησης πελατών (π.χ έπαθλα) • Μικροπληρωμές (π.χ χώρους στάθμευσης τηλεφωνήματα κτλ)	• Πληροφορίες / Ιστορικό προσωπικού • Ακαδημαϊκές πληροφορίες / ιστορικό • Αποθήκευση Προσωπικής πληροφορίας • Αρχεία ενοικίασης αυτοκινήτων • Προσωπικό προφίλ (π.χ προτιμήσεις για το πρόγραμμα εξυπηρέτησης πελατών	• Γρήγορο check in/out • Πρόσβαση σε αίθουσα λέσχης αεροδρομίου και σε αίθουσα αναχώρησης • Κλειδιά δωματίου σε ξενοδοχείο • Πρόσβαση στο διαδίκτυο , σε κτίρια κ σε δίκτυα. • Κλειδιά ενοικίασης αυτοκινήτων	• Πρόγραμμα Frequent Traveler • Κάρτα διατηρησιμότητας και εξυπηρέτησης πελατών (loyalty cards)

ΕΙΚΟΝΑ 39 : Γνωστές εφαρμογές έξυπνων καρτών κατά τομέα και τύπο κάρτας

19.10 ΑΛΛΕΣ ΕΦΑΡΜΟΓΕΣ ΈΞΥΠΝΩΝ ΚΑΡΤΩΝ [111]

Άλλες εφαρμογές των έξυπνων καρτών είναι η χρήση τους σε αποκωδικοποιητές, Internet access, product tracking, δίπλωμα οδήγησης (ιδανική για αποθήκευση penalty points και άμεση αφαίρεση του διπλώματος), κ.α.

Τέλος πρέπει να αναφέρουμε την εφαρμογή των έξυπνων καρτών στην ηλεκτρονική διακυβέρνηση όπου η εξυπηρέτηση και συναλλαγή του πολίτη με το κράτος βασίζεται σε συγκεκριμένους αριθμούς π.χ Αριθμός Δελτίου Αστυνομικής Ταυτότητας ,Αριθμος Φορολογικού μητρώου ,αριθμός εκλογέα κλπ. Η ανάπτυξη ηλεκτρονικών υπηρεσιών βασίζεται στην δυνατότητα αυτοματοποίησης αναγνώρισης και πολίτη. Τα στοιχεία ταυτοποίησης αποθήκευονται σε μια έξυπνη κάρτα και ανακαλούνται ανά περίπτωση με τον πλέον ασφαλή τρόπο.

Οι δυνατότητες που προσφέρουν οι έξυπνες κάρτες χαρακτηρίζονται από

- Ταχύτητα συναλλαγής.
- Ασφάλεια συναλλαγής.
- Ευκολία πρόσβασης.

Η χρήση των Έξυπνων καρτών ως μέσο ασφαλούς πρόσβασης σε νέες υπηρεσίες προϋποθέτει την εναρμόνιση με την Ευρωπαϊκή Πολιτική σε θέματα προστασίας προσωπικών δεδομένων (υποδομή δημοσίου κλειδιού κλειδιού).

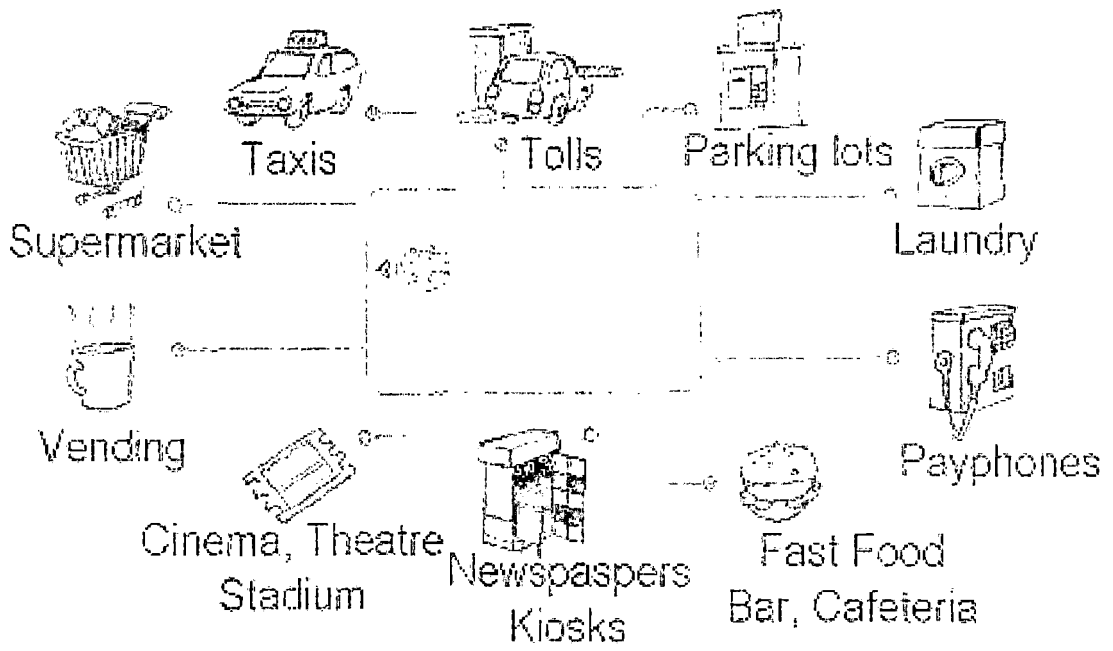
19.11 ΕΞΥΠΝΗ ΚΑΡΤΑ ΠΟΛΥΕΦΑΡΜΟΓΩΝ [112]

Τα περισσότερα από τα συστήματα έξυπνων καρτών που είναι σε χρήση σήμερα ,εξυπηρετούν έναν σκοπό και συσχετίζονται με μόνο μια διαδικασία. Παραδείγματος χάριν, η έξυπνη τηλεφωνική κάρτα που καθιστά τα δημόσια τηλέφωνα κατάλληλα και η ιατρική κάρτα που αποθηκεύει τις πληροφορίες ιατρικού ιστορικού και ασφάλειας. Όλες αυτές οι εφαρμογές αποθηκεύονται σε διαφορετικά συστήματα έξυπνων καρτών ξεχωριστά, και οδηγούν στην ίδια κατάσταση και στα ίδια προβλήματα με το παραδοσιακό σύστημα μαγνητικών καρτών λωρίδων που απαιτούν από τους χρήστες να φέρουν τις πολλαπλές κάρτες για τις πολλαπλές εφαρμογές.

Στην πραγματικότητα, η έξυπνη κάρτα έχει την ικανότητα να ενσωματώσει εκείνες τις εφαρμογές μαζί για να διαμορφωθεί μαζί μια κάρτα πολλαπλής εφαρμογής με τη χρησιμοποίηση των ενσωματωμένων χώρων αποθήκευσης των μικροεπεξεργαστών και της μνήμης. Εντούτοις, αυτό το είδος ενσωμάτωσης περιορίζεται πάντα από μερικά από τα εξωτερικά λογικά στοιχεία παρά από τα τεχνικά ζητήματα. Παραδείγματος χάριν, στην ενιαία εφαρμογή ενός συστήματος καρτών, το στοιχείο που αποθηκεύεται στην κάρτα ή ακόμα και η ίδια η κάρτα ανήκει πάντα στον εκδότη καρτών. Στην περίπτωση που υπάρχουν περισσότερες από μια εφαρμογές σε μια ενιαία κάρτα, αυτό γίνεται μη πρακτικό.

Αυτή την περίοδο, τα πρότυπα 7816 είναι ελλιπή σε όλα τα επίπεδα. Στο επίπεδο καρτών δεν έχουμε μια πλήρως διευκρινισμένη διεπαφή λειτουργικών συστημάτων, δεν έχουμε μια κατάλληλα διευκρινισμένη δομή καταλόγου και οι ονομασίες για τα πρότυπα εφαρμογής είναι ελλιπείς και οι δομές δεδομένων επιπέδων καρτών δεν διευκρινίζονται πλήρως. Στο επίπεδο εφαρμογής, τα πρότυπα επιπέδων εφαρμογής είναι ελλιπή, και σε μερικές περιπτώσεις, δεν έχουν ακόμα ξεκινήσει.

Ως εκ τούτου υπάρχει ακόμα η ανάγκη να ληφθεί κάποιος χρόνος ,έτι ώστε να οριστικοποιηθούν τα πρότυπα πριν εφαρμοστεί η ιδέα μιας κάρτας πολυεφαρμογών.



ΕΙΚΟΝΑ 40 : Μια έξυπνη κάρτα πολυεφαρμογής (πηγή Gemplus)

20 ΑΝΑΓΝΩΣΤΕΣ ΤΩΝ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ [113]

Όπως προαναφέρθηκε, προκειμένου να επικοινωνήσουμε με τις έξυπνες κάρτες είναι απαραίτητες οι συσκευές αποδοχής έξυπνων καρτών.

Οι συσκευές αποδοχής έξυπνων καρτών χωρίζονται σε δύο βασικές κατηγορίες:

1. **Τερματικές συσκευές**, οι οποίες διαθέτουν όλες τις απαραίτητες συσκευές για την επικοινωνία με την κάρτα π.χ. πληκτρολόγιο, εκτυπωτή, οθόνη, modem, κ.τ.λ. (EFT/POS, κινητά τηλέφωνα, καρτοτηλέφωνα, αυτόματοι πωλητές και αποκωδικοποιητές).
2. **Αναγνώστες – εγγραφείς έξυπνων καρτών**. Οι συσκευές αυτές δε φέρουν εξοπλισμό και συνδέονται σε τερματικές συσκευές οι οποίες δε διαθέτουν αναγνώστη έξυπνων καρτών (H/Y, info kiosks, controllers κ.α.).

Μία βασική υποομάδα αναγνωστών είναι οι ασφαλείς αναγνώστες, οι οποίοι διαθέτουν οθόνη LCD και PIN pad. Άλλες υποομάδες είναι οι αναγνώστες χωρίς καλώδιο, αναγνώστες χωρίς με επαφές, οι επιτραπέζιοι, οι ενσωματωμένοι σε άλλες συσκευές (πληκτρολόγιο, CPU) κ.α.

Εν τούτοις συνήθως με τον όρο "αναγνώστες έξυπνων καρτών", αναφερόμαστε σε όλα τα τερματικά των έξυπνων καρτών , τα οποία εξ ορισμού, έχουν τη δυνατότητα να διαβάσουν και να γράψουν εφ' όσον το υποστηρίζει η έξυπνη κάρτα και έχουν τηρηθεί οι κατάλληλοι όροι πρόσβασης.

Ένας αναγνώστης έξυπνων καρτών αναφέρεται επίσης στο τομέα της βιομηχανίας με τον όρο :

- IFD interface device (συσκευή διεπαφών),
- CAD chip accepting device (συσκευή που δέχεται το chip),
- CCR chip card reader (αναγνώστης καρτών με τσιπ).

Σε αντίθεση με τις έξυπνες κάρτες, που όλες έχουν σχεδόν παρόμοια κατασκευή, οι αναγνώστες έξυπνων καρτών διαθέτουν μια ποικιλία στην μορφή ανάλογα με τα επίπεδα μηχανικής και λογικής εκλέπτυνσης.

Οι αναγνώστες μπορούν να είναι στάσιμοι, απομακρυσμένοι, να μπορούν να λειτουργήσουν off-line,ή σε απευθείας σύνδεση (on-line), να διαθέτουν μπαταρία ως πηγή τροφοδότησης ή να χρησιμοποιούν ηλεκτρικό ρεύμα από ένα συνδεόμενο σύστημα.

Μερικά παραδείγματα περιλαμβάνουν:

- αναγνώστη που ενσωματώνεται σε μια μηχανή πώλησης,
- φορητό αναγνώστη με λειτουργία συσσωρευτή με μια μικρή οθόνη LCD,
- αναγνώστη που ενσωματώνεται σε ένα GSM κινητό τηλέφωνο,
- και αναγνώστη που συνδέεται με έναν προσωπικό υπολογιστή.

Μηχανικά, οι αναγνώστες έχουν διάφορες επιλογές συμπεριλαμβανομένων των εξής:

- εάν ο χρήστης πρέπει να παρεμβάλλει/ αφαιρέσει την κάρτα του σε αντίθεση με τον αυτοματοποιημένο μηχανισμό εισαγωγής/ εκτίναξης.
- εάν πρέπει να χρησιμοποιούνται επαφές που ολισθαίνουν σε αντίθεση με τις επαφές που προσγειώνονται.

- ποικιλία για τις παροχές για τις επιδείξεις και την είσοδο πληκτρολόγησης.

Όσον αφορά το ηλεκτρικό τμήμα ο αναγνώστης πρέπει να προσαρμοστεί στα πρότυπα του ISO 7816-3.

Οι επιλογές για τους αναγνώστες είναι πολυάριθμες. Αυτό το τμήμα θα εστιάσει στους αναγνώστες που συνδέονται με τα συστήματα προσωπικών ηλεκτρονικών υπολογιστών (PC), επειδή εκείνοι ασκούν μεγαλύτερη επίδραση στην ασφάλεια υπολογιστών και δικτύων.

20.1 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΤΩΝ ΑΝΑΓΝΩΣΤΩΝ [114]

ΦΥΣΙΚΗ ΣΥΝΔΕΣΗ	ΠΛΕΟΝΕΚΤΗΜΑΤΑ	ΜΕΙΟΝΕΚΤΗΜΑΤΑ
Τμηματικός λιμένας	Πολύ συνηθισμένος και ανέξοδος. Προσφέρει διαγώνια υποστήριξη πλατφορμών για τα Windows, MAC, και Unix.	Πολλοί υπολογιστές γραφείου δεν έχουν κανέναν ελεύθερο τμηματικό λιμένα. Απαιτεί την δύναμη εξωτερικής μπαταρίας.
PCMCIA	Άριστος για τους διακινούμενους χρήστες με τους υπολογιστές lap-top	Μπορέστε να είναι ελαφρώς ακριβότερος. Πολλά υπολογιστικά συστήματα γραφείου δεν έχουν τις αυλακώσεις PCMCIA.
PS/2 λιμένας πληκτρολογίων	Εύκολος να εγκαταστηθεί. Προσφέρει προστασία στη πορεία του .	Πιο αργές ταχύτητες επικοινωνίας.
Floppy	Πολύ εύκολος για εγκατάσταση	Απαιτεί μια μπαταρία. Η ταχύτητα επικοινωνιών μπορεί να είναι ένα πρόβλημα .
USB	Πολύ υψηλές ταχύτητες μεταφοράς στοιχείων.	Όχι ακόμα ευρέως διαθέσιμος.
Ενσωματωμένος	Καμία ανάγκη για την εγκατάσταση υλικού ή λογισμικού.	Όχι ακόμα ευρέως διαθέσιμος.

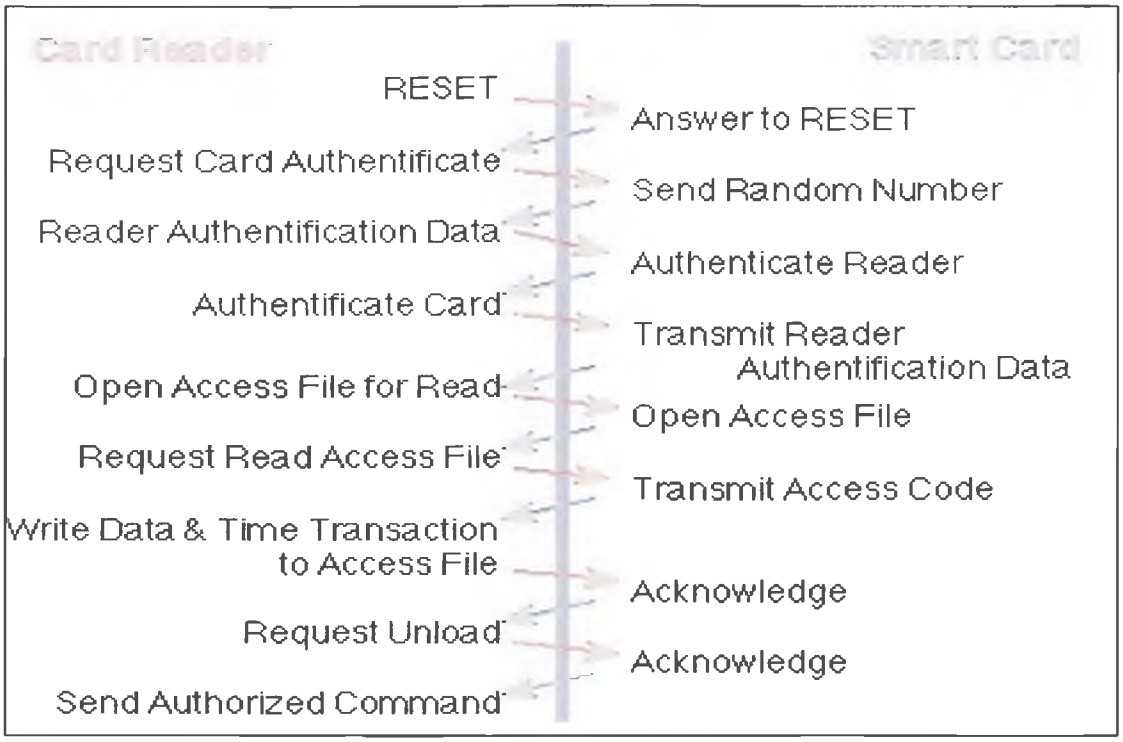
ΕΙΚΟΝΑ 41 : Πλεονεκτήματα και μειονεκτήματα διαφόρων αναγνωστών

20.2 ΕΠΙΚΟΙΝΩΝΙΑ ΜΕ ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ [115]

Όπως έχουμε προαναφέρει η σχέση μεταξύ ενός αναγνώστη έξυπνων καρτών και μιας έξυπνης κάρτας είναι μια σχέση «κυρίου – σκλάβου» .

Ο αναγνώστης στέλνει μια εντολή στην έξυπνη κάρτα , η κάρτα εκτελεί την εντολή και επιστρέφει το αποτέλεσμα στον αναγνώστη και περιμένει μια καινούρια εντολή.

Η παρακάτω εικόνα δείχνει ένα αντιπροσωπευτικό παράδειγμα πρωτοκόλλου επικοινωνίας των έξυπνων καρτών με τους αναγνώστες.



ΕΙΚΟΝΑ 42 : Πρωτόκολλο επικοινωνίας αναγνωστών και έξυπνων καρτών

20.3 ΕΓΚΑΤΑΣΤΑΣΗ ΤΩΝ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ [116]

Μπορείτε να εγκαταστήσετε μια έξυπνη κάρτα στον υπολογιστή ενώ ο υπολογιστής τρέχει. Ο υπολογιστής ανιχνεύει αυτόματα την κάρτα.

Για να εγκαταστήσει μια έξυπνη κάρτα:

1. Αφαιρέστε το κενό έξυπνων καρτών από την αυλάκωση έξυπνων καρτών.
2. Κρατήστε το πρόσωπο καρτών επάνω με το χρυσό μαξιλάρι επαφών στην κορυφαία επιφάνεια και να δείξει προς την αυλάκωση των έξυπνων καρτών.

ΕΙΚΟΝΑ 43 : Η πάνω πλευρά μιας έξυπνης κάρτας

1. χρυσό μαξιλάρι επαφών
2. έξυπνη κάρτα (κορυφή)

3. Γλιστρήστε την έξυπνη κάρτα στην αυλάκωση έξυπνων καρτών έως ότου η κάρτα είναι εντελώς καθισμένη στο συνδετήρα της. Η έξυπνη κάρτα προεξέχει περίπου 1,27 εκατ. (0,5 ίντσα) από την αυλάκωση. Η αυλάκωση έξυπνων καρτών βρίσκεται κάτω από την αυλάκωση καρτών PC.

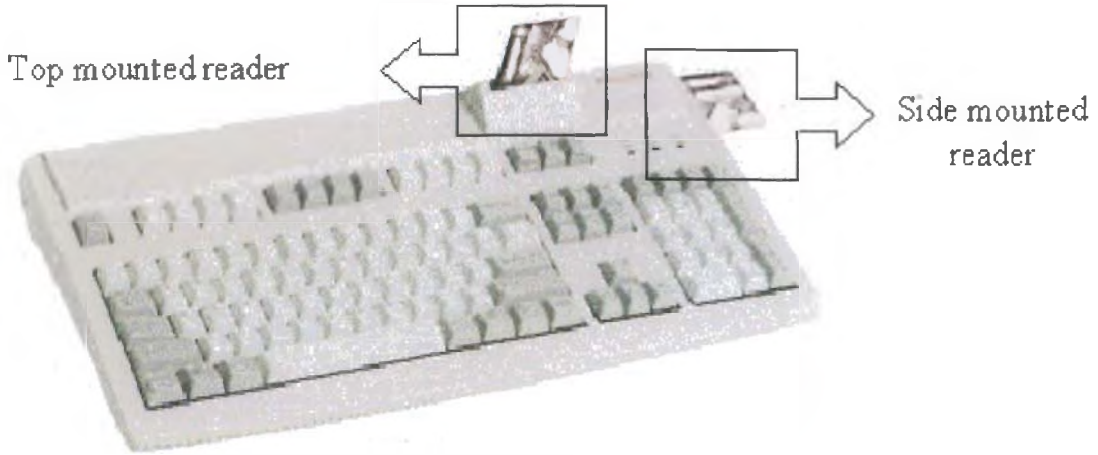
Εάν αντιμετωπίζετε πάρα πολλή αντίσταση, μην αναγκάστε την κάρτα. Ελέγξτε τον προσανατολισμό καρτών και προσπαθήστε πάλι.

ΕΙΚΟΝΑ 44 : Εγκατάσταση μιας έξυπνης κάρτας

1. Αυλάκωση καρτών PC.
2. Αυλάκωση έξυπνων καρτών.
3. Έξυπνη κάρτα.

20.4 ΤΕΧΝΟΛΟΓΙΑ ΑΝΑΓΝΩΣΤΩΝ [117]

Οι αναγνώστες καρτών παρέχουν τη φυσική σύνδεση μεταξύ της έξυπνης κάρτας και του κεντρικού υπολογιστή (που αναφέρεται ως host) .Η παρακάτω εικόνα δείχνει ένα συνδυασμό πληκτρολογίου και αναγνώστη καρτών.



ΕΙΚΟΝΑ 45 : Αναγνώστης έξυπνων καρτών

Ο κεντρικός υπολογιστής host μπορεί να είναι ένα PC ή μια αυτόνομη συσκευή. Ο αναγνώστης απελευθερώνει ισχύ, αρχικοποιεί την κάρτα και ενεργεί ως μεσολαβητής μεταξύ του κεντρικού υπολογιστή (host) και της έξυπνης κάρτας. Η ισχύς διανέμεται στην έξυπνη κάρτα μέσω μιας επαφής στο micro module της επαφής των έξυπνων καρτών ή με την πρόκληση ρεύματος μέσω της κεραίας των ανέπαφων σχεδίων.

Η αρχικοποίηση είναι ένα καθορισμένο πρωτόκολλο που πρέπει να εκτελούν όλες οι κάρτες. Όλοι οι αναγνώστες έξυπνων καρτών υποστηρίζουν την αρχικοποίηση οποιασδήποτε έξυπνης κάρτας ,αλλά μπορούν να σταματήσουν να υποστηρίζουν την κάρτα με την διακοπή του ηλεκτρικού ρεύματος.

❖ **Ενημερότητα της κάρτας**

Η όψη ενός αναγνώστη μιας έξυπνης κάρτας καλείται ενημερότητα κάρτας. Οι περισσότεροι αναγνώστες καρτών υποστηρίζουν και τις δύο επιλεγμένες όψεις :

- Οι ενήμεροι αναγνώστες εμφανίζουν τη φυσική δομή καρτών και δρουν ως μεταφραστές μεταξύ του κεντρικού υπολογιστή (host) και της κάρτας. Οι κάρτες μνήμης απαιτούν την ενήμερη όψη ,επειδή οι αναγνώστες πρέπει να ξέρουν την ακριβή διεύθυνση για τα δεδομένα.

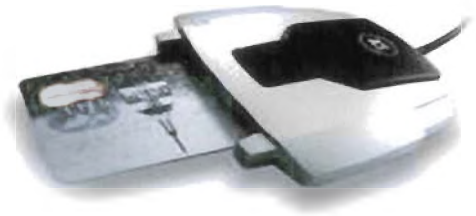
- Οι γενικοί αναγνώστες γνωρίζουν τη λογική δομή της κάρτας και περνούν τις εντολές από τον host κατευθείαν στην κάρτα ,χωρίς να αλλάζουν την εντολή. Οι κάρτες των μικροεπεξεργαστών χρησιμοποιούν τη γενική όψη ,επειδή οι κάρτες έχουν δικό τους λειτουργικό σύστημα και λογική για να ερμηνεύουν τις εντολές.

20.5 ΠΑΡΑΔΕΙΓΜΑΤΑ ΑΝΑΓΝΩΣΤΩΝ [118]

ΕΙΚΟΝΑ 46 : Μερικοί τύποι αναγνωστών έξυπνων καρτών

❖ ΣΥΣΚΕΥΕΣ ΑΝΑΓΝΩΣΗΣ ΠΟΥ ΣΥΝΔΕΟΝΤΑΙ ΜΕ PC

➢ Συσκευή ανάγνωσης ACR38U



ΕΙΚΟΝΑ 47 : Συσκευή ανάγνωσης ACR38U

Με τη συνεχόμενη εξέλιξη των προτύπων των προσωπικών υπολογιστών, ο αναγνώστης έξυπνων καρτών ACR38 είναι μια USB 2,0 πλήρης συσκευή ταχύτητας που σχεδιάζεται για χρήση στο περιβάλλον PC.

Η πιο πρόσφατη ενσάρκωση της σειράς αναγνωστών συνδυάζει ένα σύγχρονο σχέδιο με την πιο πρόσφατη τεχνολογία και το καθιστά κατάλληλη λύση για τις απαιτήσεις των περιβαλλόντων. Το ACR38 είναι ιδανικό για χρήση σε εφαρμογές στην ασφάλεια δικτύων και στα ηλεκτρονικά συστήματα πληρωμής καθώς επίσης και σε άλλες προηγμένες εφαρμογές έξυπνων καρτών.

➢ Συσκευή ανάγνωσης ACR38K

ΕΙΚΟΝΑ 48 : Συσκευή ανάγνωσης ACR38K

Το πληκτρολόγιο πολυμέσων ACR38K σας προσφέρει με την εξειδικευμένη ρύθμιση πληκτρολογίων, να έχετε πρόσβαση σε κάθε λειτουργία με μόνο μια πληκτρολόγηση, συν έναν εκπληκτικό ελεγκτή πολυμέσων.

Αυτή η συσκευασία έρχεται επίσης με έναν αναγνώστη καρτών που σας επιτρέπει να εφαρμόσετε εύκολα τα συστήματα που είναι βασισμένα σε έξυπνες κάρτες. Οι αναγνώστες έξυπνων καρτών ACS χρησιμοποιούν την πιο πρόσφατη πρόοδο της τεχνολογίας μικροτσίπ, η οποία σας προσφέρει υψηλή ασφάλεια για τα εμπιστευτικά αρχεία σας ,έτσι ώστε να μεταφέρετε εύκολα την έξυπνη κάρτα μικροτσίπ.

Οι οδηγοί και τα εργαλεία λογισμικού σε αυτό το πακέτο θα σας επιτρέψουν να γράψετε αρχεία στην έξυπνη κάρτα σας και να διαβάσετε τα περιεχόμενα τους.

➢ **Συσκευή ανάγνωσης ACR38T**

ΕΙΚΟΝΑ 49 : Συσκευή ανάγνωσης ACR38T

Ο αναγνώστης /συγγραφέας ACR38T είναι μια συσκευή USB υψηλών ταχυτήτων που αποτελεί την διεπαφή για την επικοινωνία μεταξύ του υπολογιστή και της έξυπνης κάρτας και για αυτό και σχεδιάζεται για περιβάλλον PC.

➢ **Συσκευή ανάγνωσης ACR38DT**

ΕΙΚΟΝΑ 50 : Συσκευή ανάγνωσης ACR38DT

Η συσκευή ανάγνωσης ACR38DT προσφέρει και τις 2 λύσεις βασισμένη στην έξυπνη κάρτα combi (χωρίς επαφή κάρτα και με επαφή) μεγέθους SIM .Έχει τις πλήρεις λειτουργίες ACR38T με το χαρακτηριστικό γνώρισμα της ανέπαφης προστιθέμενης αξίας.

➢ **Συσκευή ανάγνωσης ACR30**

ΕΙΚΟΝΑ 51 : Συσκευή ανάγνωσης ACR30

Το ACR30 είναι ένας συμπαγής ,πολύ αποδοτικός οικονομικά, ενιαίου τσιπ αναγνώστης έξυπνων καρτών που υποστηρίζει όλες τις έξυπνες κάρτες βασισμένες

στα T=0 ή T=1 πρωτόκολλα καθώς επίσης και τις δημοφιλείς κάρτες μνήμης στην αγορά. Υποστηρίζει όλες τις σημαντικές πλατφόρμες των Η/Υ συμπεριλαμβανομένου του DOS των Windows και Linux. Ο συγκεκριμένος αναγνώστης είναι μια από τις πιο οικονομικώς αποδοτικές λύσεις για το ηλεκτρονικό εμπόριο, την ασφάλεια πληροφοριών ,τον έλεγχο πρόσβασης ,την ταυτοποίηση και άλλες γνωστές εφαρμογές των έξυπνων καρτών.

- **Συσκευή ανάγνωσης ACK30S**

ΕΙΚΟΝΑ 52 : Συσκευή ανάγνωσης ACK30S

Ο συγκεκριμένος αναγνώστης είναι μια ενσωματωμένη λύση για τις εφαρμογές PC/SC.Ο αναγνώστης έξυπνων καρτών είναι ενσωματωμένος ηλεκτρονικά και μηχανικά σε ένα πληκτρολόγιο που παρέχει μια τέλεια λύση για τις υψηλές εφαρμογές ασφαλείας.

Αυτή η συσκευή είναι ιδανική για τις εφαρμογές συμπεριλαμβανομένων των εξής : τραπεζικές εργασίες διαδικτύου, απευθείας σύνδεση με το χρηματιστήριο ,επιχειρήσεις που κάνουν εμπόριο μέσω διαδικτύου, αγορές μέσω διαδικτύου(on-line), ψυχαγωγία σε απευθείας σύνδεση όπως ο κινηματογράφος ,χαρτοπαικτικές λέσχες και άλλα παιχνίδια και εφαρμογές.

- **Συσκευή ανάγνωσης ACR38F**

ΕΙΚΟΝΑ 53 : Συσκευή ανάγνωσης ACR38F

Αυτός ο αναγνώστης είναι η ιδανική λύση για την εύκολη ενσωμάτωση ενός αναγνώστη έξυπνων καρτών στο περιβάλλον των υπολογιστών γραφείου. Χρησιμοποιεί το ίδιο ηλεκτρονικό κύκλωμα με τους αναγνώστες ACR38 Χρησιμοποιώντας την διεπαφή USB ,χρησιμοποιεί την εσωτερική παροχή ηλεκτρικού ρεύματος του υπολογιστή και μπορεί να διαμορφωθεί με διάφορους τρόπους για να ταιριάζει στις απαιτήσεις των πελατών.

❖ ΣΥΣΚΕΥΕΣ ΑΝΑΓΝΩΣΗΣ ΙΣΟΡΡΟΠΙΑΣ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ

➢ Αναγνώστης ισορροπίας

ΕΙΚΟΝΑ 54 : Αναγνώστης ισορροπίας

Η ACS παρέχει ένα ευρύ φάσμα αναγνωστών ισορροπίας (ελεγκτές αξίας) για να μπορούν να διαμορφωθούν έτσι ώστε να χρησιμοποιούνται σε διαφορετικές εφαρμογές όπως ο έλεγχος ισορροπίας, η επιλογή νομίσματος , τα αρχεία συναλλαγής εξέτασης , η επαλήθευση ταυτότητας ,το αρχείο βιβλιοθηκών και άλλα.

➢ Αναγνώστης δυναμικής γεννήτριας κωδικού πρόσβασης

ΕΙΚΟΝΑ 55 : Αναγνώστης κωδικού πρόσβασης

Αυτή η δυναμική γεννήτρια είναι συμπαγής και χρησιμοποιείται με μια έξυπνη κάρτα μεγέθους SIM. Μπορεί να χρησιμοποιηθεί με τον κωδικό πρόσβασης ενός χρήστη για την επικύρωση και επομένως είναι κατάλληλο για τη χρήση στην εφαρμογή ασφάλειας.

❖ ΣΥΣΚΕΥΕΣ ΑΝΑΓΝΩΣΗΣ ΔΑΚΤΥΛΙΚΩΝ ΑΠΟΤΥΠΩΜΑΤΩΝ

➢ Συσκευή ανάγνωσης ADT60 BioSIMKey

ΕΙΚΟΝΑ 56 : Συσκευή ανάγνωσης ADT60 BioSIMKey

Το BioSIMKey είναι μια εξαιρετικά συμπαγής συσκευή που ενσωματώνει έναν ανιχνευτή δακτυλικών αποτυπωμάτων και έναν αναγνώστη έξυπνων καρτών. Είναι η πιο πρόσφατη καινοτομία στη βιομετρική τεχνολογία των έξυπνων καρτών.

➢ **Συσκευή ανάγνωσης AET60 Bio CARDKey**

ΕΙΚΟΝΑ 57 : Συσκευή ανάγνωσης AET60 Bio CARDKey

Η συσκευή AET60 Bio CARDKey συνδυάζει τον ιδιαίτερα επιτυχημένο αναγνώστη έξυπνων καρτών που χρησιμοποιεί αισθητήρες δακτυλικών αποτυπωμάτων πυριτίου και χρησιμοποιεί την ίδια τεχνολογία όπως η συσκευή ADT60 BioSIMKey και έτσι εξασφαλίζει τις υψηλότερες ποιοτικές εικόνες που χρησιμοποιούνται με έξυπνες κάρτες full-size. Η συγκεκριμένη συσκευή ανάγνωσης βελτιώνει την ασφάλεια και την αποδοτικότητα της πρόσβασης στο δίκτυο, του ηλεκτρονικού εμπορίου και των εγχώριων τραπεζικών εργασιών.

➢ **Συσκευή ανάγνωσης AET60 Bio TRUSTKey**

ΕΙΚΟΝΑ 58 : Συσκευή ανάγνωσης AET60 Bio TRUSTKey

Το AET60 Bio TRUSTKey συνδυάζει τον ιδιαίτερα επιτυχημένο αναγνώστη έξυπνων καρτών που χρησιμοποιεί αισθητήρες δακτυλικών αποτυπωμάτων πυριτίου για να επιτύχει την εξαιρετικά ασφαλή επικύρωση. Είναι πλήρως ενσωματωμένο στο βιομετρικό υποσύστημα που βασίζεται στα αποτυπώματα, συνδυάζοντας την ανίχνευση δακτυλικών αποτυπωμάτων και την επεξεργασία αλγορίθμου σε μια ενιαία, συμπαγή συσκευή.

Όλη η βιομετρική επεξεργασία αλγορίθμου πραγματοποιείται σε ένα τσιπ που ενσωματώνεται στο πίσω μέρος του αισθητήρα δακτυλικών αποτυπωμάτων πυριτίου.

❖ ΣΥΣΚΕΥΕΣ ΑΝΑΓΝΩΣΗΣ ΜΕ ΠΛΗΚΤΡΟΛΟΓΙΟ ΕΙΣΑΓΩΓΗΣ PIN

➢ Συσκευή ανάγνωσης ACR80

ΕΙΚΟΝΑ 59 : Συσκευή ανάγνωσης ACR80

Το ACR80 είναι ένα ασφαλές τερματικό έξυπνων καρτών. Περιλαμβάνει ένα βασικό αριθμητικό πληκτρολόγιο με 16 αυλακώσεις 4 κλειδιά λειτουργίας και 2 έξυπνες κάρτες με αυλάκωση.

❖ ΣΥΣΚΕΥΕΣ ΑΝΑΓΝΩΣΗΣ ΓΙΑ ΑΝΕΠΑΦΕΣ ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ

➢ Συσκευή ανάγνωσης ACR120 Contact less Reader

ΕΙΚΟΝΑ 60 : Συσκευή ανάγνωσης ACR120 Contact less Reader

Οι συσκευές ACR120 είναι συμπαγείς και οικονομικώς αποδοτικοί ανέπαφοι αναγνώστες και συγγραφείς. Σχεδιάζεται για τη γρήγορη ένταξη στα διαφορετικά συστήματα. Μπορεί να ενσωματωθεί εύκολα στις υπάρχουσες εφαρμογές συλλογής δεδομένων όπως τα φορητά τερματικά ,η επικόλληση ετικέτας ,η μηχανή πώλησης ή ο έλεγχος πρόσβασης.

❖ ΣΥΣΚΕΥΕΣ ΑΝΑΓΝΩΣΗΣ ΓΙΑ ΚΛΕΙΔΑΡΙΕΣ

➢ Κλειδαριές έξυπνων καρτών με επαφή

ΕΙΚΟΝΑ 61 : Κλειδαριές έξυπνων καρτών με επαφή

Η ACS προσφέρει μια μεγάλη ποικιλία από κλειδαριές έξυπνων καρτών με επαφή μαζί με το σύστημα διαχείρισης των κλειδαριών για ξενοδοχεία. Οι κλειδαριές αυτές χρησιμοποιούνται επίσης σε γραφεία και σε σπίτια και έχουν αρχίσει και αναπτύσσονται πολύ στο εμπόριο.

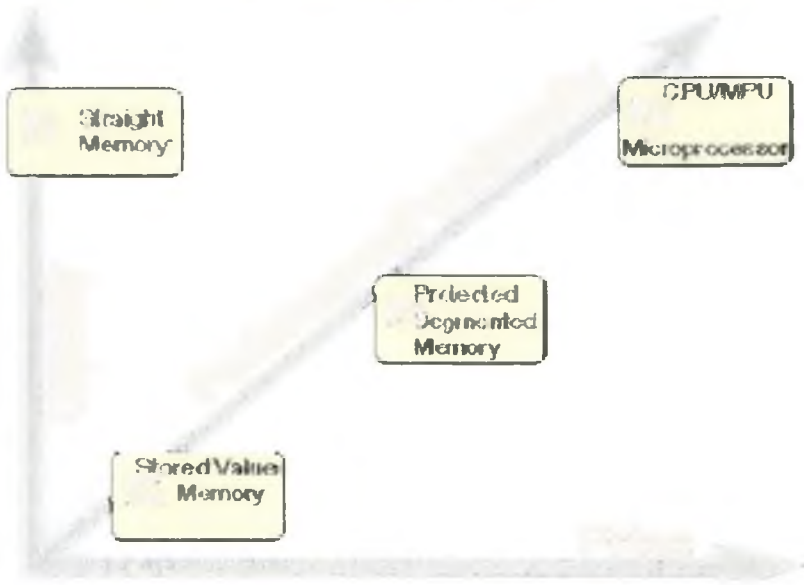
- **Κλειδαριές έξυπνων καρτών χωρίς επαφή**

ΕΙΚΟΝΑ 62 : Κλειδαριές έξυπνων καρτών χωρίς επαφή

Η ACS προσφέρει μια μεγάλη ποικιλία από κλειδαριές έξυπνων καρτών χωρίς επαφή μαζί με το σύστημα διαχείρισης των κλειδαριών για ξενοδοχεία.

21 ΚΡΙΤΗΡΙΑ ΕΠΙΛΟΓΗΣ ΤΩΝ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ [119]

Όσο αυξάνεται η υπολογιστική ισχύς και η μνήμη της κάρτας τόσο αυξάνεται και το κόστος της. Για να μπορέσει κανείς να επιλέξει την κατάλληλη κάρτα για την εφαρμογή που τον ενδιαφέρει, δεν έχει παρά να εκτιμήσει το κόστος σε σχέση με τη λειτουργικότητα και να ορίσει το επίπεδο ασφάλειας που τον ενδιαφέρει. Το παρακάτω διάγραμμα δείχνει τους γενικούς αυτούς κανόνες επιλογής της κατάλληλης λύσης.



ΕΙΚΟΝΑ 63 : Κριτήρια για την σωστή επιλογή μιας έξυπνης κάρτας

Η επιλογή της κάρτας που κατά περίπτωση είναι κατάλληλη, είναι μια διαδικασία δύσκολη και πρέπει να γίνεται προσεκτικά γιατί επηρεάζει το σχεδιασμό ολόκληρου του συστήματος. Κρίνεται λοιπόν σκόπιμο, προτού προχωρήσουμε στην επιλογή μιας κάρτας να θέσουμε ερωτήματα, όπως τα παρακάτω:

- Πόσες εφαρμογές θέλουμε να αποθηκεύσουμε στην κάρτα;
- Τι είδους πληροφορία θα αποθηκεύσω στις κάρτες;
- Πόση μνήμη είναι απαραίτητη για κάθε εφαρμογή;
- Πόσες κάρτες θα αγοραστούν;
- Μας ενδιαφέρει η ταχύτητα της συναλλαγής;
- Το ποσό της κάρτας θα μπορεί να ανανεώνεται; Πρόκειται δηλαδή για reloadable ή disposable κάρτα;
- Ποια είναι η μέγιστη και η ελάχιστη τιμή που μπορεί να αποθηκευτεί;

Ειδικά όσον αφορά την ασφάλεια

- Ποιες είναι οι απαιτήσεις σε ασφάλεια;
- Ποιος έχει δικαίωμα πρόσβασης στις πληροφορίες;
- Ποιος έχει δικαίωμα τροποποίησης των δεδομένων;
- Ποια λύση θεωρείται καλύτερη για την ασφάλεια των δεδομένων; (κρυπτογράφηση, κωδικοί πρόσβασης, PINs ή συνδυασμός όλων).

22 ΑΠΟΤΥΠΩΣΗ ΤΗΣ ΥΦΙΣΤΑΜΕΝΗΣ ΚΑΤΑΣΤΑΣΗΣ [120]

22.1 Η ΚΑΤΑΣΤΑΣΗ ΤΗΝ ΕΥΡΩΠΗ

Για την Ευρωπαϊκή Ένωση, οι Έξυπνες Κάρτες αποτελούν μία από τις προτεραιότητες του Σχεδίου Δράσης του eEurope στα πλαίσια της ανάπτυξης ασφαλών και γρήγορων δικτύων και της ενίσχυσης των ηλεκτρονικών υπηρεσιών και του ηλεκτρονικού επιχειρείν.

Μία πρόσφατη έρευνα, που υλοποιήθηκε από την εταιρεία EDS κατόπιν παραγγελίας και με την συνεργασία του trailblazer 10 του eEurope Smart Card Charter με στόχο την αποτύπωση και την μελέτη των εφαρμογών έξυπνων καρτών στην ηλεκτρονική διακυβέρνηση cards - G2G (government-to-government), G2B (government-tobusiness), G2C (government-to-citizens) και e-Procurement στη δημόσια διοίκηση, ανέδειξε ότι οι εφαρμογές έξυπνων καρτών που υλοποιούνται στην Ευρώπη αφορούν στις παρακάτω ενότητες:

- Ηλεκτρονική υπογραφή.
- Ταυτοποίηση προσωπικού (δημοσίων υπαλλήλων, επαγγελματιών υγείας, κλπ.).
- Ταυτοποίηση εταιρειών από δημόσια διοίκηση και δημόσιους οργανισμούς.
- Ηλεκτρονική ταυτότητα πολιτών.
- Ηλεκτρονική ταυτότητα ασφαλισμένων.
- Υποστήριξη υπηρεσιών σε σχετικά μικρές περιοχές (μαζικές μεταφορές, αναψυχή κλπ.).

Συγκεκριμένα η έρευνα εντόπισε τις παρακάτω εφαρμογές ανά χώρα μέλους της Ευρωπαϊκής Ένωσης:

ΧΩΡΑ	ΟΝΟΜΑΣΙΑ ΕΡΓΟΥ	ΠΕΡΙΓΡΑΦΗ / ΣΧΟΛΙΑ
Austria	citizen card (bürgerkarte)	Common framework social security and other citizen identity card
Belgium	belpic	BELgian Personal Identity Card for citizens and civil servants
	sis	Social security card
Finland	fineid	Finnish identity cards
	satakunka	Macro-pilot covering health and social security information.
	North karelian hospital district	Management and exchange of health data (FINEID card used for authentication)
France	titre fondateur	Common basis for electronic identity cards, potentially covering: personal identity card, driver licence, other specific cards
	teleprocedures	Tax teleprocedures
	sesam vitale	Identification of insured persons (social security)
	gip cps	Health Professional Cards

	adep	A group of small and mid-sized towns to test usage of eprocedures with the citizen and with the administrations
Germany	media@komm	Initiative for the development of e-procedures in townships and urban districts. The cities of Bremen, Nürnberg and Esslingen are pilots.
	Land of Baden-Württenberg	Multifunctional cards to citizen and public e-procurement
	beschaffungsamt	e-procurement for administrations
Ireland	public services broker	Secure access to public services
Italy	ieic	Italian Electronic Identity Card
	aes	Advanced Electronic Signature based on IEIC
	msc	Multi Services organisation Card based on IEIC
Netherlands	pki overheid	Government PKI for civil servants
Norway	-	Digital Signature
	-	Health project (under development)
	-	National betting system (under development)
Spain	national PKI	Usage of smart cards in public sector's PKI based applications: identification/authentication + e-sign for civil servants.
Sweden	ID CARD	Multipurpose identity card Internal use within the Administration : National Taxboard, Social Insurance Board
U.K.	e-tendering	System to allow UK departments to exchange tendering information (pilot stage)
	dfee	Connections card: a scheme for 16-19 year olds in education, covering attendance monitoring, access to facilities, credits, etc.
	SMARTCITIES	Local services with the City of Southampton as

ΕΙΚΟΝΑ 64 : Εφαρμογές ανά χώρα μέλους της Ευρωπαϊκής Ένωσης

Πηγή : μελέτη EDS –TB 10

Η εν λόγω μελέτη αναφέρει ότι οι βασικές δυσκολίες - προβλήματα που προέκυψαν κατά τον σχεδιασμό και την υλοποίηση των παραπάνω έργων δύναται να συνοψιστούν στα εξής:

- στην έλλειψη εξοπλισμού (αναγνωστών καρτών) από πολίτες και μικρές εταιρείες αποτελεί εμπόδιο στην υλοποίηση εφαρμογών G2C
- στη συνήθη σύνθεση των θέσεων εργασίας (workstations) που δεν είναι επαρκής και το πλήθος των χρηστών εκτιμούν ότι ο πρόσθετος απαιτούμενός

εξοπλισμός είναι σχετικά ακριβός σε σχέση με τα αναμενόμενα αποτελέσματα από την χρήση των έξυπνων καρτών.

- στο ότι το πλήθος των χρηστών αισθάνονται ότι οι τεχνολογίες έξυπνων καρτών δεν είναι ώριμες και υπάρχει η πιθανότητα να αλλάξουν στο μέλλον.
- στο ότι μερικές κατηγορίες εργαζομένων - χρηστών θεωρούν ότι η χρήση των έξυπνων καρτών επιφέρουν αλλαγές συνηθειών στην εργασία και υπάρχει φόβος επιβολής πρόσθετων ελέγχων με την εφαρμογή έξυπνων καρτών.

Όμως, σε όλες τις περιπτώσεις των έργων που μελετήθηκαν, προέκυψε ότι οι έξυπνες κάρτες έγιναν αποδεκτές και χρησιμοποιήθηκαν αποτελεσματικά μετά την περίοδο προσαρμογής. Αποτελεί γενική εκτίμηση ότι η εξέλιξη και η αποτελεσματικότητα των εφαρμογών έξυπνων καρτών στην Ευρώπη εξαρτάται από τα πρότυπα που υποστηρίζονται, το περιεχόμενο των εφαρμογών και την δυνατότητα χρήσης μία κάρτας για την εξυπηρέτηση διαφόρων χρήσεων (multi-application usage).

Τέλος, από την μελέτη προκύπτει ότι εφαρμογές έξυπνων καρτών στην ηλεκτρονική διακυβέρνηση θα εστιαστούν κυρίως στις κάρτες υγείας και κοινωνικής ασφάλισης καθώς επίσης και στις κάρτες ταυτοποίησης πολιτών και δημοσίων λειτουργών με δυνατότητες ηλεκτρονικής υπογραφής.

22.2 ΟΙ ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ ΣΤΗΝ ΕΛΛΑΔΑ

Οι πρώτες πιλοτικές εφαρμογές Έξυπνων Καρτών εμφανίστηκαν στην χώρα μας το 1988 στο χώρο της υγείας. Έκτοτε ακολούθησαν διάφορες εφαρμογές κυρίως σε ερευνητικό – πιλοτικό περιβάλλον καθώς επίσης και η χρήση των έξυπνων καρτών στις τηλεπικοινωνίες - στην κινητή τηλεφωνία και στα καρτοτηλέφωνα. Οι σημαντικότερες χρήσεις και εφαρμογές έξυπνων καρτών στη χώρα μας είναι:

Κάρτες Τηλεπικοινωνιών **i)** Εταιρίες κινητής τηλεφωνίας κάρτες SIM - Μερικά εκατομμύρια **ii)** ΟΤΕ - κάρτες προπληρωμένες (Μνήμης) - δεκάδες εκατομμύρια.

Τραπεζικές κάρτες **i)** διάφορες Τράπεζες - Έξυπνες κάρτες σαν Security Application Modules -δεκάδες χιλιάδες **ii)** Ηλεκτρονικό Πορτοφόλι Εθνικής Τράπεζας - Μερικές εκατοντάδες **iii)** Ηλεκτρονικό Πορτοφόλι Cafe Εθνική και Εμπορική Τράπεζα – Μερικές εκατοντάδες **iv)** Εθνική Τράπεζα – Έργο IST Starfish – Μερικές δεκάδες.

Κάρτες Υγείας-Κοινωνικής Ασφάλισης **i)** Δήμος Αμαρουσίου (υλοποίηση του Ευρωπαϊκού έργου Cardlink) - Μερικές χιλιάδες **ii)** ΕΟΔΕΑΠ (ασφαλιστικός οργανισμός) - Μερικές χιλιάδες **iii)** Ερυθρός Σταυρός - κάρτα διαβητικών - Μερικές εκατοντάδες **iv)** Νοσοκομείο Νίκαιας - κάρτα καρδιοπαθών - Μερικές εκατοντάδες.

Κάρτες Πελατειακής Πιστότητας **i)** Εθνοκάρτα - Παρουσίαση (loyalty) - Δεκάδες χιλιάδες **ii)** Καταστήματα VETO (loyalty) - Μερικές χιλιάδες.

Διάφορες εφαρμογές π.χ Αττική οδός - Τηλεκάρτες (prepaid) Κάρτα πληρωμής διοδίων, δημόσιων συγκοινωνιών και στάθμευσης στην Θεσσαλονίκη.

23 ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ [121]

23.1 ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ ΠΟΥ ΔΙΕΠΕΙ ΑΜΕΣΑ ΤΙΣ ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ

Οι έξυπνες κάρτες, λόγω της πρόσφατης ανάδειξής τους ως 'μέσο συναλλαγών' αλλά και της εμφανιζόμενης πολυμορφίας στον τρόπο χρήσης τους και στις εφαρμογές τους, δεν έχουν αποτελέσει (τουλάχιστον ακόμη), 'αυτούσιο αντικείμενο' κάποιας νομοθετικής ρύθμισης, τόσο σε εθνικό όσο και σε ευρωπαϊκό επίπεδο.

Χαρακτηριστικό είναι το γεγονός ότι η φράση 'Έξυπνες Κάρτες' στο εθνικό μας δίκαιο απαντάται μόνο μία φορά (σύμφωνα με τα δεδομένα της 'Τράπεζας Νομικών Πληροφοριών' του δικηγορικού Συλλόγου Αθηνών, [www.dsanet.gr])και αυτό στην Υπ. Αποφ. 3227/31-1-2002 (ΦΕΚ Α΄ 23/13-02-02) του Υπουργείου Εξωτερικών 'περί της δημοσίευσης της απόφασης 1382/2001 του Συμβουλίου Ασφαλείας του ΟΗΕ' ως προϊόν που εντάσσεται (υπό όρους) στο εμπάργκο (κυρώσεις) κατά του Ιράκ!

Βέβαια, οι έξυπνες κάρτες (smart cards) αναφέρονται σε πάρα πολλά 'προπαρασκευαστικά κείμενα' (δηλαδή κείμενα μη άμεσης υποχρεωτικής εφαρμογής) της Ευρωπαϊκής Ένωσης, όπως ανακοινώσεις, ψηφίσματα, συστάσεις, γνωμοδοτήσεις κ.λ.π., ιδίως στα πλαίσια των εγκεκριμένων προγραμμάτων δράσης eEurope2002 (και, πρόσφατα, eEurope2005) στα οποία διαφαίνεται η πρόθεση προώθησης και υιοθέτησης του συγκεκριμένου μέσου ως βασικό συντελεστή για την επίτευξη της πολυπόθητης ασφάλειας στην 'Κοινωνία της Πληροφορίας'.

Επίσης, ο προσδιορισμός 'τεχνικών προδιαγραφών' και η δημιουργία σχετικών 'τεχνικών προτύπων' από οργανισμούς προτυποποίησης (π.χ. ETSI, CEN, ISO, ITU, κ.λ.π.) ή και από διάφορα ιδιωτικά consortiums (π.χ. EMVCo) -για συγκεκριμένες χρήσεις τους ή γενικά- δεν αποτελούν από μόνα τους 'θεσμικό πλαίσιο' στον βαθμό, βέβαια, που δεν υπάρχουν οι σχετικές νομοθετικές, κανονιστικές ή διοικητικές διατάξεις που να παραπέμπουν ή να αναφέρονται σ' αυτά! (μιας και τα 'πρότυπα', ακόμη και αν ,έχουν δημοσιευθεί από 'αναγνωρισμένους οργανισμούς', δεν είναι –από μόνα τους- υποχρεωτικά!).

23.2 ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ ΠΟΥ ΣΧΕΤΙΖΕΤΑΙ ΑΜΕΣΑ ΜΕ ΤΙΣ ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ

Από την άλλη πλευρά, τουλάχιστον σε ευρωπαϊκό επίπεδο (και στο βαθμό που εναρμονίζεται με αυτό η εθνική νομοθεσία μας, και σε εθνικό επίπεδο), έχουν θεσπισθεί μια σειρά από διατάξεις (κυρίως Οδηγίες του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου) σχετικά με θέματα που άπτονται συγκεκριμένων εφαρμογών των 'έξυπνων καρτών'. Έτσι, ανάλογα με το είδος της εφαρμογής που χρησιμοποιείται μια έξυπνη κάρτα, μπορούν να αναφερθούν χαρακτηριστικά τα εξής νομοθετήματα:

Η Έξυπνη κάρτα ως '**συσκευή για την πρόσβαση υπό όρους**' (σε 'προστατευόμενες υπηρεσίες')

- **Οδηγία 98/84/ΕΚ «για τη νομική προστασία των υπηρεσιών που βασίζονται ή συνίστανται στην παροχή πρόσβασης υπό όρους»**

Με την Οδηγία αυτή λαμβάνονται μέτρα κατά των παράνομων συσκευών που παρέχουν μη επιτρεπόμενη πρόσβαση σε προστατευόμενες υπηρεσίες, ενώ παράλληλα προστατεύεται (άρ. 3 §2) 'η ελεύθερη κυκλοφορία των συσκευών για την πρόσβαση υπό όρους'.

Ως 'συσκευή για την πρόσβαση υπό όρους' δίνεται (άρ. 2, περ. γ') ο εξής ορισμός: «οποιοσδήποτε εξοπλισμός ή λογισμικό που έχει σχεδιαστεί ή προσαρμοστεί έτσι ώστε να καθιστά δυνατή την πρόσβαση σε μια υπηρεσία σε κατανοητή μορφή» και προφανώς βρίσκει εφαρμογή σε πολλές περιπτώσεις που η έξυπνη κάρτα χρησιμοποιείται ως (μέρος) τέτοιου εξοπλισμού π.χ. για την αποκωδικοποίηση δορυφορικών τηλεοπτικών σημάτων, για την πρόσβαση στο δίκτυο GSM (κινητή τηλεφωνία), ακόμη και για πρόσβαση σε συγκεκριμένες υπηρεσίες τηλεματικής, όπως είναι π.χ. το σύστημα 'HERMES' του Χρηματιστηρίου Αξιών Αθηνών που χρησιμοποιεί έξυπνες κάρτες για ταυτοποίηση των χρηστών του!

Η Έξυπνη κάρτα ως (μέρος της) **'ασφαλή διάταξη δημιουργίας (ηλεκτρονικής) υπογραφής'**

- **Οδηγία 99/93/ΕΚ «σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές»**

Με την Οδηγία αυτή (η οποία έχει ενσωματωθεί στο εθνικό μας δίκαιο με το π.δ. 150/2001) , αν και δεν αναφέρεται ονομαστικά στις 'smart cards', θέτονται οι βασικές προδιαγραφές που πρέπει να τηρούν οι φορείς (και όχι μόνο) των ιδιωτικών κλειδιών ('δεδομένων δημιουργίας υπογραφής') των τελικών χρηστών ώστε να εξασφαλίζεται το απαιτούμενο επίπεδο ασφάλειας για την δημιουργία (εφόσον συντρέχουν και άλλες προϋποθέσεις, όπως αυτή της έκδοσης 'αναγνωρισμένου πιστοποιητικού') 'αναγνωρισμένης ηλεκτρονικής υπογραφής' (άρ 5§1 της Οδηγίας ή 3§1 του ελληνικού π.δ.) που χαίρει απόλυτης ισοδυναμίας με την αντίστοιχη ιδιόχειρη υπογραφή.

Αν και ως 'φορείς των δεδομένων δημιουργίας υπογραφής' μπορούν να χρησιμοποιηθούν και άλλα μέσα (π.χ. USB tokens), η χρήση των 'έξυπνων καρτών' (που θα τηρούν τις 'τεχνικές προδιαγραφές' και τα 'πρότυπα' που εκδίδονται από τους ευρωπαϊκούς οργανισμούς προτυποποίησης και που εξειδικεύουν –κατά παραγγελία της σχετικής 'επιτροπής'- τις διατάξεις της συγκεκριμένης οδηγίας) ως βασικό ασφαλές μέσον για την εναπόθεση ιδιωτικών κλειδιών και τη δημιουργία 'αναγνωρισμένων υπογραφών', θεωρείται δεδομένη! (λόγω και των προαναφερόμενων για το εγκεκριμένο σχέδιο δράσης 'eEurope2005').

Η Έξυπνη κάρτα ως **'ηλεκτρονικό πορτοφόλι'** ή, άλλως, ως **'φορέας πιστωτικών μονάδων'**

Αν και οι συγκεκριμένες εφαρμογές της έξυπνης κάρτας χρησιμοποιούνται ήδη σε πιλοτικά προγράμματα (π.χ. BalcanCard) ή και σε πρακτικές εφαρμογές (π.χ. οι γνωστές 'τηλεκάρτες' με τις προπληρωμένες μονάδες), εντούτοις δεν υπάρχει ακόμη σχετικό θεσμικό πλαίσιο και οι σχετικές (αποδεικτικές) συμβάσεις διέπονται πλήρως από την αρχή της «ελευθερίας των συμβάσεων» όπου οι χρήστες και οι πάροχοι των σχετικών υπηρεσιών συμφωνούν από μόνοι τους στον αποδεικτικό χαρακτήρα και λειτουργία των μέσων που χρησιμοποιούν!

Στα πλαίσια της αναμενόμενης Οδηγίας «για την εξ αποστάσεως εμπορία καταναλωτικών χρηματοπιστωτικών υπηρεσιών» (βλ. προοίμιο αρ. 11 της Οδηγίας

'για το ηλεκτρονικό εμπόριο') είναι πολύ πιθανό να ρυθμιστούν σχετικά θέματα και να θέτονται κάποια 'στάνταρτ ασφαλείας' στα 'μέσα' που θα χρησιμοποιούνται για αυτές. Πάντως, είναι δεδομένο ότι στο βαθμό που αρμόζουν, ισχύουν και για τις 'έξυπνες κάρτες' οποιεσδήποτε διατάξεις διέπουν την χρήση και λειτουργία ανάλογων 'μέσων πληρωμής' (όπως π.χ. η «Απόφαση-πλαίσιο του Συμβουλίου της 28-5-2001 για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών» -ΕΕ L 149 της 2.6.2001, σελ. 1) .

23.3 ΑΛΛΕΣ ΔΙΑΤΑΞΕΙΣ ΠΟΥ ΣΧΕΤΙΖΟΝΤΑΙ ΕΜΜΕΣΑ ΜΕ ΤΙΣ ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ

Άλλες σημαντικές διατάξεις -που σχετίζονται, όμως, **κυρίως με τον τρόπο ανάπτυξης των εφαρμογών που χρησιμοποιούν 'έξυπνες κάρτες'** και όχι άμεσα με αυτές τις ίδιες, είναι πάρα πολλές και ισχύουν κατά περίπτωση. Ενδεικτικά:

- Οδηγίες 95/46/ΕΚ και 97/66/ΕΚ για την προστασία δεδομένων προσωπικού χαρακτήρα,
- Οδηγία 97/7/ΕΚ για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις,
- Οδηγία 00/31/ΕΚ για το ηλεκτρονικό εμπόριο.

24 ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΠΡΟΤΑΣΕΙΣ ΣΤΡΑΤΗΓΙΚΗΣ ΓΙΑ ΤΙΣ ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ [122]

24.1 ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΤΗΝ ΠΟΛΙΤΕΙΑ

Οι έξυπνες κάρτες επιλέγονται διεθνώς σαν ένα ασφαλές μέρος των υποδομών ασφάλειας των πληροφοριακών συστημάτων και ιδιαίτερα σαν μέσο πρόσβασης σε ανοικτά δίκτυα. Οι κλάδοι των Τραπεζών και της Κινητής Τηλεφωνίας έχουν επενδύσει και επενδύουν δισεκατομμύρια ευρώ ενώ οι νέοι χρήστες για μια σειρά εφαρμογών είναι οι Οργανισμοί Μαζικών Συγκοινωνιών και ο δημόσιος Τομέας.

Στην Ευρώπη αλλά και στις ΗΠΑ και την Ιαπωνία, οι αρμόδιοι κυβερνητικοί φορείς υλοποιούν μεγάλης κλίμακας έργα με έξυπνες κάρτες και προωθούν την έρευνα και ανάπτυξη σε παρεμφερείς συμπληρωματικές τεχνολογίες όπως την βιομετρική. Στην Ελλάδα εκτός από τους Τηλεπικοινωνιακούς φορείς δεν έχουν γίνει μαζικές επενδύσεις. Μάλιστα η μεγάλη επιτυχία των τηλεκαρτών στην Ελλάδα κατά την τελευταία δεκαετία οδήγησε στην κατασκευή τριών εργοστασίων τα οποία προσβλέπουν σε αναδυόμενες αγορές.

Επιλεγμένη ομάδα εργασίας του Υπουργείου Ανάπτυξης, κατόρθωσε να συγκεντρώσει για πρώτη φορά όλους τους άμεσα ενδιαφερόμενους χρήστες, ερευνητές και προμηθευτές έξυπνων καρτών στο πλαίσιο της ενημέρωσης και ανταλλαγής απόψεων και έχουν να κάνουν τις εξής προτάσεις:

1) **Την δημιουργία μιας μη-κερδοσκοπικής εταιρίας Έξυπνων Καρτών που θα συγχρηματοδοτείται από τον ιδιωτικό και δημόσιο Τομέα.**

Ο σκοπός αυτής της ομάδας είναι να επεξεργαστεί ζητήματα που αφορούν:

- Την εκπαίδευση προσωπικού σε αυτές τις τεχνολογίες σε συνεργασία με Ακαδημαϊκά Ιδρύματα
- Την προώθηση της έρευνας και ανάπτυξης
- Την εξασφάλιση του νομικού και θεσμικού πλαισίου που εναρμονίζεται με το Ευρωπαϊκό
- Την εξασφάλιση διαλειτουργικότητας των υποδομών των διαφόρων κλάδων
- Την διερεύνηση κοινών επενδύσεων διαφόρων κλάδων
- Την ευθυγράμμιση με τις Ευρωπαϊκές πρωτοβουλίες όπως έχουν εξελιχθεί μετά την δημοσίευση της Ανοικτής Υποδομής Έξυπνων Καρτών για την Ευρώπη στα πλαίσια της πρωτοβουλίας e-Europe.
- Την προσπάθεια προώθησης λύσεων σε γειτονικές χώρες

2) **Την διοργάνωση Ελληνικού Συνεδρίου (πιθανόν και έκθεσης προϊόντων και εφαρμογών) smart cards** που θα επαναλαμβάνεται σε ετήσια βάση.

3) **Την προετοιμασία πρότασης Ελληνικού Roadmapping Ερευνητικού Project.** Το έργο πρέπει να περιλαμβάνει όλους τους «παίκτες» της Ελληνικής αγοράς (Ακαδημαϊκά & Ερευνητικά Ιδρύματα, Βιομηχανίες καρτών και readers, εταιρείες ανάπτυξης λογισμικού, consultants). Στόχοι του έργου θα πρέπει να είναι :

- Smart cards technology foresight για την επόμενη 5-ετία

- Smart cards business development foresight για την επόμενη 5-ετία
- Αναγνώριση αναγκών σε έρευνα για την ανάπτυξη της Ελληνική βιομηχανίας έξυπνων καρτών
- Αναγνώριση αναγκών σε υποδομές και δομές για την υποστήριξη της επιχειρηματικότητας της Ελληνικής βιομηχανίας έξυπνων καρτών
- Καθορισμός μέτρων για την κάλυψη των παραπάνω αναγκών.
- Πιλοτικές προσπάθειες ανάπτυξης Τεχνολογίας και εφαρμογών για την επικύρωση των παραπάνω αποτελεσμάτων

24.2 ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΤΟ ΔΗΜΟΣΙΟ ΤΟΜΕΑ

Στον δημόσιο τομέα που συμπεριελαμβάνονται διάφορα Υπουργεία και Οργανισμοί αν και υπάρχει το ενδιαφέρον για την τεχνολογία των έξυπνων καρτών παρόλα αυτά έχει παρατηρηθεί έλλειψη εξοικείωσης των χρηστών αλλά και των τεχνολόγων. Αυτό σημαίνει ότι υπάρχει κίνδυνος σπατάλης πόρων για μελέτη και ανάπτυξη ξεχωριστών συστημάτων μη συνεργάσιμων ή για επικαλύψεις.

Είναι χαρακτηριστικό ότι οι κάρτες διοδίων της Αττικής Οδού και του Ταμείου Εθνικής Οδοποιίας δεν συνεργάζονται. Η πρόταση για την δημιουργία ενός οργάνου που θα συντονίζει την ανάπτυξη των υποδομών και την έκδοση των καρτών μπορεί να αποτρέψει τέτοιου είδους περιττές σπατάλες. Ταυτόχρονα μπορεί να δημιουργηθεί για τον σκοπό αυτό - στα πλαίσια του οργάνου αυτού - μια επιτροπή για τις ανάγκες αποκλειστικά του δημοσίου τομέα. Ήδη σε Ευρωπαϊκό επίπεδο - και με υπό ένταξη κράτη - υπάρχει ικανοποιητικός συντονισμός ανάλογων πρωτοβουλιών:

Η Ομάδα Porvoo που συγκεντρώνει 15 χώρες και έχει σκοπό την διευρωπαϊκή Ηλεκτρονική Ταυτότητα, το επιδοτούμενο από την Ευρωπαϊκή Επιτροπή έργο eEpoch, η πρωτοβουλία eEurope Smart Cards και άλλες που ασχολούνται με ιδιαίτερες εφαρμογές όπως την κάρτα E-111 κτλ.

Το προτεινόμενο όργανο θα μεριμνά ώστε να υπάρχει Ελληνική συμμετοχή και δραστηριοποίηση σε όλες τις σχετικές πρωτοβουλίες και παράλληλος συντονισμός μεταξύ των πρωτοβουλιών αυτών. Ιδιαίτερα να υπάρχει συμμετοχή με αυτοχρηματοδότηση του Ελληνικού Υπουργείου Εσωτερικών, δημόσιας διοίκησης και Αποκέντρωσης στο έργο eEpoch.

Ένα ιδιαίτερα σημαντικό θέμα είναι η μεταφορά της τεχνογνωσίας που έχει αναπτυχθεί διεθνώς στην δημόσια διοίκηση. Αυτό μπορεί να επιτευχθεί μέσα από μια σειρά σεμιναρίων, ημερίδων κτλ αλλά, και ιδιαίτερα, μέσα από ορισμένα πιλοτικά που πρέπει να υλοποιηθούν σε τοπικό επίπεδο ώστε να αποκτηθεί ιδία εμπειρία

25 ΠΑΡΑΔΕΙΓΜΑΤΑ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ

25.1 ΠΑΡΑΔΕΙΓΜΑ Α - ΜΟΝΤΕΛΟ SMART READER 4000 [123]

Η συσκευή ανάγνωσης δέχεται 'έξυπνες κάρτες' τύπου SLE4442 (Siemens). Οι κάρτες αυτές διαθέτουν ηλεκτρονικό κωδικό ασφαλείας τον οποίο χειρίζονται ειδικοί κρυπτογραφικοί αλγόριθμοι ώστε να εξασφαλιστεί σε απόλυτο βαθμό η ασφάλεια και η άριστη λειτουργία. Έτσι, είναι πρακτικά αδύνατον να δημιουργηθούν αντίγραφα (κάρτες - κλώνοι) από μη εξουσιοδοτημένα άτομα.

Κάθε κάρτα χαρακτηρίζεται από την ημέρα – ώρα έκδοσης της. Κατά την εγγραφή της από τη συσκευή προγραμματισμού λαμβάνει ένα μυστικό κωδικό ο οποίος προκύπτει από την τρέχουσα ημ/νία – ώρα. Κάθε φορά που τοποθετούμε την κάρτα στην συσκευή ανάγνωσης γίνεται έλεγχος του κωδικού αυτού. Η συσκευή ανάγνωσης εξετάζει αν ο κωδικός είναι ίδιος ή διαφορετικός με αυτόν που είχε κάρτα στο προηγούμενο πέρασμα της. Αν είναι ίδιος της επιτρέπει την πρόσβαση. Αν όχι, τότε εφόσον αυτός είναι μεγαλύτερος από τον προηγούμενο (κάρτα με νεώτερη έκδοση) της επιτρέπει την πρόσβαση σημειώνοντας στη μνήμη του τον νέο αριθμό. Αν είναι μικρότερος της απαγορεύει την πρόσβαση.

Πρακτικά αυτό σημαίνει ότι <u>κάθε νέα κάρτα που εκδίδεται ακυρώνει την προηγούμενη</u>. Έτσι, αν χάσετε (ή σας κλέψουν) την κάρτα σας η νέα που θα εκδοθεί θα ακυρώσει την προηγούμενη. Ωστόσο, αυτός ο μηχανισμός μπορεί να δημιουργήσει ένα σημαντικό πρόβλημα.

Αν υποθέσουμε ότι έχουμε εγκαταστήσει αναγνώστες πρόσβασης στα δωμάτια ενός ξενοδοχείου, κάθε νέος πελάτης θα λαμβάνει από τη reseption κάρτα με νέα έκδοση. Όμως, στα δωμάτια καθημερινά πρέπει να μπαίνουν και υπάλληλοι του ξενοδοχείου (π.χ. καμαριέρα). Αφού λοιπόν ο πελάτης έχει νεώτερη έκδοση καταργεί την παλιά άρα η κάρτα του υπάλληλου χάνει την πρόσβαση. Για να ξεπεραστεί το πρόβλημα αυτό <u>κάθε αναγνώστης διαθέτει τέσσερις ζώνες πρόσβασης</u> οι οποίες λειτουργούν ανεξάρτητα. Έτσι, στο προηγούμενο παράδειγμα ο πελάτης θα έχει πρόσβαση στη ζώνη 'Α' ενώ ο υπάλληλος στη ζώνη 'Β'.

❖ **<u>Η εγκατάσταση των συσκευών ανάγνωσης.</u>**

Κάθε συσκευή ανάγνωσης διαθέτει ένα μοναδικό κωδικό ο οποίος αποτελείται από 6 γράμματα. Αυτός είναι ο κωδικός - κλειδί τον οποίο πρέπει να περιέχει η κάρτα ώστε να έχει πρόσβαση στον συγκεκριμένο αναγνώστη. Ο τεχνικός πριν βιδώσει στον τοίχο την συσκευή πρέπει να σημειώσει σε ένα τετράδιο τον κωδικό αυτό (θα τον βρει στο κάτω μέρος της συσκευής). δίπλα στον κωδικό πρέπει να σημειώσει ένα όνομα που περιγράφει το σημείο εγκατάστασης.

Για παράδειγμα, αν η συσκευή με τον κωδικό '84D53F' πρόκειται να τοποθετηθεί στο δωμάτιο 120 του ξενοδοχείου στο τετράδιο ο τεχνικός θα σημειώσει:

84D53F : Δωμάτιο 120

Αυτό θα πρέπει να επαναλάβει σε κάθε συσκευή που τοποθετεί. Αφού τελειώσει την εγκατάσταση καταχωρεί τους κωδικούς αυτούς με τα αντίστοιχα ονόματα στο πρόγραμμα που δημιουργεί τις κάρτες (παρουσιάζεται στη συνέχεια).

❖ **Ο χειρισμός των αναγνωστών.**

Η συσκευή ανάγνωσης πρέπει να βρίσκεται συνεχώς σε λειτουργία. Αν υπάρχει αστάθεια στο ηλεκτρικό δίκτυο (διακοπές τάσεως) θα πρέπει να τοποθετηθεί ένα UPS το οποίο θα τροφοδοτεί με τάση 220V τη συσκευή όποτε υπάρχει διακοπή.

Ο αναγνώστης περιμένει την εισαγωγή της κάρτας. Όταν ο χρήστης τοποθετήσει την κάρτα ο αναγνώστης εξετάζει τα στοιχεία της και αν είναι αποδεκτά ενεργοποιεί το relay. Στην περίπτωση αυτή ανάβει με πράσινο χρώμα το ενδεικτικό LED και σβήνει όταν το relay απενεργοποιηθεί. Αν η κάρτα δεν έχει πρόσβαση ανάβει με κόκκινο χρώμα το LED και παραμένει αναμμένο έως ότου βγάλουμε την κάρτα.

❖ **Ο προγραμματισμός των έξυπνων καρτών- Η συσκευή προγραμματισμού.**

Η κάρτα SLE4442 περιέχει τσιπάκι ηλεκτρονικής μνήμης με χωρητικότητα 256 bytes. Στη μνήμη αυτή σημειώνονται τα στοιχεία του χρήστη και οι κωδικοί πρόσβασης. Η εγγραφή της κάρτας γίνεται από μία ειδική συσκευή η οποία ονομάζεται 'προγραμματιστής'. Η συσκευή αυτή διατίθεται από την εταιρία SmartControl. Συνδέεται σε υπολογιστή τύπου PC στην θύρα RS232. Χρησιμοποιεί λογισμικό το οποίο τρέχει σε περιβάλλον Windows 98 η ανώτερο.

Η εγκατάσταση του λογισμικού γίνεται τρέχοντας το αρχείο Setup.exe της δισκέτας (παρέχεται μαζί με την συσκευή προγραμματισμού). Η εγκατάσταση σας επιτρέπει να επιλέξετε τον φάκελο όπου θα τοποθετηθούν τα αρχεία. Αφού τελειώσει μπορείτε να τρέξετε την εφαρμογή. Κάνοντας διπλό κλικ στο εικονίδιο της εφαρμογής θα εμφανιστεί η εξής φόρμα.

ΕΙΚΟΝΑ 65 : Φόρμα προγραμματισμού έξυπνων καρτών

❖ **Καθορισμός των στοιχείων.**

Στο πρώτο πεδίο της φόρμας σημειώνουμε το ονοματεπώνυμο του χρήστη. Αν υπάρχουν και άλλα στοιχεία αυτά μπορούμε να τα σημειώσουμε στη φόρμα των σημειώσεων η οποία εμφανίζεται όταν κάνουμε κλικ στο πλήκτρο 'σημειώσεις'. Τα στοιχεία χρήστη είναι προαιρετικά. Αν δεν μας ενδιαφέρουν μπορούμε να τα παραλείψουμε.

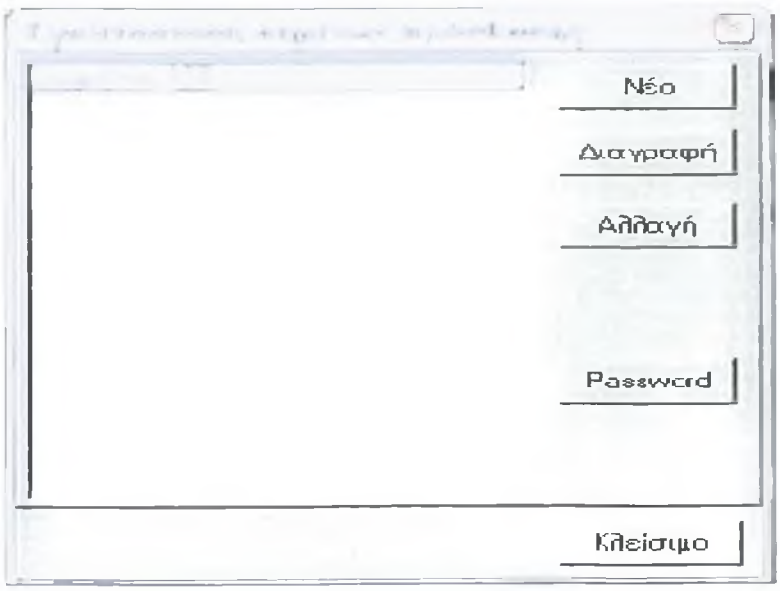
Το τρίτο πεδίο καθορίζει τη διάρκεια πρόσβασης της κάρτας. Η δυνατότητα αυτή είναι προαιρετική και ενεργοποιείται με κλικ στο αριστερό κουτάκι (θα γίνει 'Χ') . Κατόπιν στα πεδία 'Ημέρες' – 'Ώρες' σημειώνουμε το πλήθος των ημερών – ωρών που θα ισχύει η κάρτα. Αν σημειώσουμε μηδέν και στα δύο πεδία η κάρτα θα έχει απεριόριστη διάρκεια πρόσβασης. Η διάρκεια ξεκινά να μετρά από την ώρα που η κάρτα θα μπει για πρώτη φορά στην συσκευή ανάγνωσης. Όταν παρέλθει ο χρόνος που καθορίσαμε η κάρτα παύει να έχει πρόσβαση. Στην περίπτωση αυτή η κάρτα μπορεί να προγραμματιστεί ξανά με νέο χρόνο.

Η 'ζώνη' είναι ένα σημαντικό πεδίο το οποίο δηλώνεται υποχρεωτικά. Καθορίζει την ζώνη στην οποία θα έχει πρόσβαση η κάρτα (κάθε συσκευή ανάγνωσης διαθέτει τέσσερις ζώνες).

Τα 'σημεία πρόσβασης' καθορίζουν τις συσκευές ανάγνωσης στις οποίες θα έχει πρόσβαση η κάρτα. Παρατηρούμε δύο λίστες. Στην αριστερή λίστα παρουσιάζονται όλα τα σημεία που υπάρχουν εγκατεστημένοι αναγνώστες. Στη δεξιά λίστα σημειώνονται τα σημεία που θα έχει πρόσβαση η κάρτα. Στην αριστερή λίστα με τα πλήκτρα του κέρσορα ή με το ποντίκι επιλέγουμε το σημείο που θέλουμε να έχει πρόσβαση η κάρτα και πατώντας το πλήκτρο '_' το προσθέτουμε στη δεξιά λίστα. Μπορούμε να επιλέξουμε όσα σημεία θέλουμε. Με το πλήκτρο '_' αφαιρούμε κάποιο από τη λίστα.

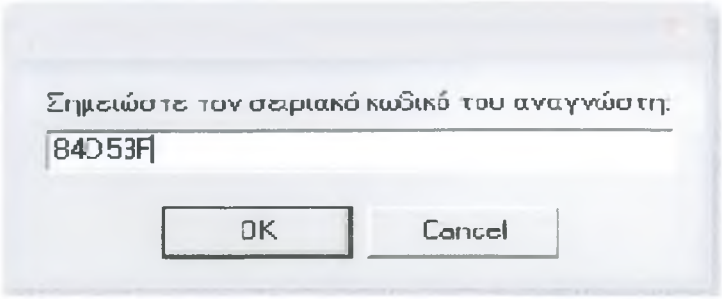
❖ **Καθορισμός των σημείων πρόσβασης.**

Το πλήκτρο '...' αφορά τον τεχνικό που εγκατέστησε τις συσκευές ανάγνωσης. Πατώντας το εμφανίζεται η εξής φόρμα:



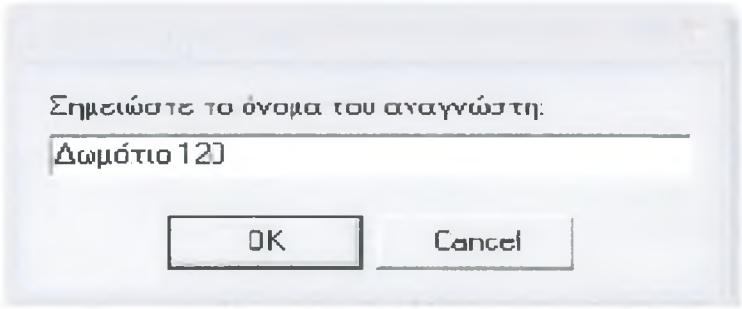
ΕΙΚΟΝΑ 66 : Φόρμα καθορισμού στοιχείων πρόσβασης

Ο τεχνικός, αφού έχει ολοκληρώσει την εγκατάσταση των συσκευών ανάγνωσης επιλέγει αυτή τη φόρμα. Για κάθε κωδικό που έχει σημειώσει στο τετράδιο του κάνει κλικ στο πλήκτρο 'Νέο'. Εμφανίζεται το εξής πλαίσιο:



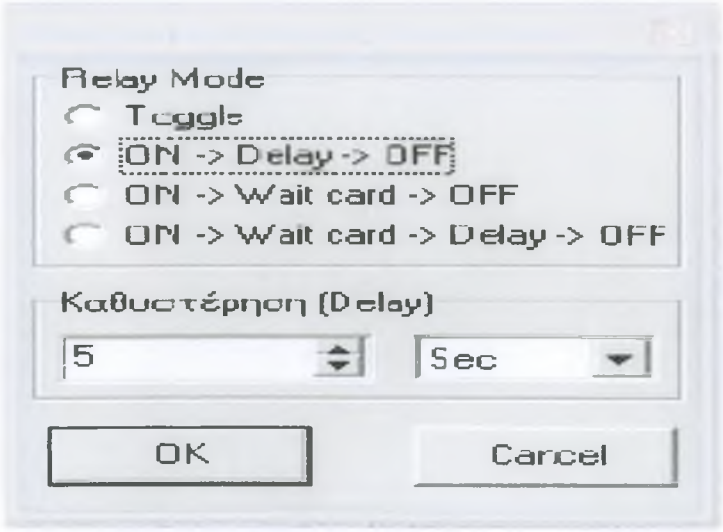
ΕΙΚΟΝΑ 67 : Φόρμα συμπλήρωσης κωδικού του αναγνώστη

Στο πλαίσιο αυτό σημειώνει τον κωδικό της συσκευής και πατά 'OK'. Τότε εμφανίζεται το εξής πλαίσιο:



ΕΙΚΟΝΑ 68 : Φόρμα συμπλήρωσης ονόματος του αναγνώστη

Στο πλαίσιο αυτό σημειώνει το περιγραφικό όνομα του σημείου όπου τοποθετήθηκε η συσκευή ανάγνωσης και πατά 'OK' οπότε εμφανίζεται η φόρμα:



ΕΙΚΟΝΑ 69 : Φόρμα προγραμματισμού του RELAY

Στη φόρμα αυτή ο τεχνικός πρέπει να καθορίσει τον τρόπο συμπεριφοράς του relay που διαθέτει η συσκευή ανάγνωσης. Υπάρχουν τέσσερις επιλογές:

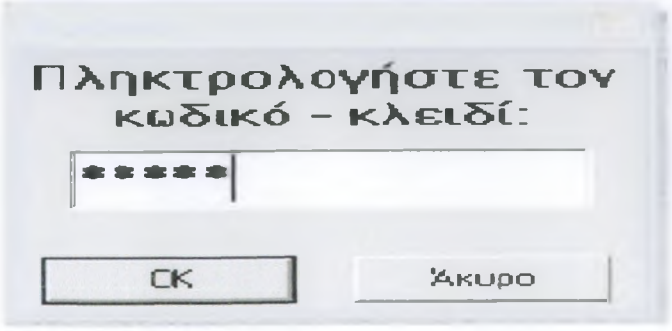
Toggle	Το relay αλλάζει κατάσταση κάθε φορά που περνά η κάρτα.
ON->Delay->OFF	Όταν τοποθετηθεί η κάρτα ενεργοποιείται το relay, παραμένει ενεργό για όσο χρόνο δηλώνει η Delay και κατόπιν απενεργοποιείται.
ON->WaitCard->OFF	Όταν τοποθετηθεί η κάρτα ενεργοποιείται το relay και παραμένει ενεργό για όσο χρόνο η κάρτα είναι εντός της συσκευής. Όταν βγάλουμε την κάρτα το relay απενεργοποιείται.
ON->WaitCard->Delay ->OFF	Ίδιο με την προηγούμενη επιλογή μόνο που όταν η κάρτα βγει υπάρχει μία χρονοκαθυστέρηση για όσο χρόνο δηλώνει η Delay και κατόπιν το relay απενεργοποιείται.

ΕΙΚΟΝΑ 70 : Επιλογές για τον προγραμματισμό του RELAY του αναγνώστη

Ο χρόνος Delay δηλώνεται στο επόμενο πλαίσιο. Αυτός μπορεί να είναι 1...127 δευτερόλεπτα (Sec) ή 1...127 λεπτά (Min).Με την επιλογή 'Διαγραφή' αφαιρούμε μία καταχώρηση ενώ με την επιλογή 'Αλλαγή' αλλάζουμε τα στοιχεία της (όνομα και relay mode).

Το πρόγραμμα δημιουργεί το αρχείο 'Readers.dat' στο οποίο καταχωρεί τα στοιχεία των αναγνωστών που δηλώσαμε. Το αρχείο αυτό θα το βρείτε στον φάκελο όπου έχει εγκατασταθεί η εφαρμογή. Είναι σημαντικό αρχείο και θα πρέπει να διατηρείτε αντίγραφο του σε δισκέτα (BackUp Disk). Αν καταστραφεί ή αν κάνετε εκ νέου την εγκατάσταση του προγράμματος απλώς αντιγράψτε το αρχείο αυτό από τη δισκέτα στον κατάλογο του προγράμματος ώστε να μη χρειαστεί να επαναλάβετε την διαδικασία καταχώρησης.

ΠΡΟΣΟΧΗ! Αν κάποιος κλέψει το αρχείο αυτό μπορεί να φτιάχνει κάρτες οι οποίες θα έχουν πλήρη πρόσβαση. Για να αποτραπεί αυτό μπορείτε να κωδικοποιήσετε τα δεδομένα του αρχείου καθορίζοντας ένα κωδικό ασφαλείας. Αυτό γίνεται από την επιλογή 'Password'. Επιλέγοντας την θα εμφανιστεί η εξής φόρμα:



ΕΙΚΟΝΑ 71 : Φόρμα συμπλήρωσης κωδικού πρόσβασης

Ο κωδικός που ορίζετε αποτελείται από 1…8 ψηφία. Κάθε φορά που θα τρέχετε την εφαρμογή θα σας ζητείται ο κωδικός αυτός. Μόνο αν τον εισάγετε σωστά θα μπορείτε φτιάχνετε κάρτες. Με τον τρόπο αυτό αποτρέπετε τις παρεμβάσεις από μη εξουσιοδοτημένα άτομα.

❖ **Ο προγραμματισμός της κάρτας.**

Αφού καθορίσετε τα στοιχεία τοποθετείστε την κάρτα στη συσκευή προγραμματισμού και κάντε κλικ στο πλήκτρο 'Εγγραφή'. Στο κάτω μέρος της φόρμας παρουσιάζεται η διαδικασία της εγγραφής. Αν η κάρτα δεν είναι συμβατή θα εμφανιστεί λάθος. Ακόμη, αν η κάρτα έχει κλειδώσει θα εμφανιστεί μήνυμα λάθους.

Συνήθως, οι κάρτες κλειδώνουν όταν δημιουργήθηκαν από μη εξουσιοδοτημένη αντιγραφή. Αφού τελειώσει η εγγραφή η κάρτα είναι έτοιμη προς χρήση. Αν χρειάζεστε περισσότερες από μία κάρτες απλώς επαναλάβατε την διαδικασία της εγγραφής για κάθε μία από αυτές. Προσοχή όμως, μην επιλέξετε «Νέα έκδοση» διότι τότε θα δημιουργηθούν κάρτες οι οποίες θα ακυρώνουν τις προηγούμενες.

❖ **Ανάγνωση των στοιχείων της κάρτας.**

Τοποθετήστε την κάρτα στην συσκευή προγραμματισμού και κάντε κλικ στην επιλογή 'Ανάγνωση'. Τα στοιχεία της κάρτας θα εμφανιστούν στην φόρμα. Στην περίπτωση αυτή το πλήκτρο 'Εγγραφή' έχει απενεργοποιηθεί ώστε να αποτραπεί η δημιουργία αντιγράφων.

25.2 ΠΑΡΑΔΕΙΓΜΑ Β - ΜΟΝΤΕΛΟ SMART CONTROL 4000 [124]

Ο αναγνώστης καρτών Smart Control 4000 συνδυάζοντας ασφάλεια και αξιοπιστία, προσφέρει πάμπολλες διαφορετικές εφαρμογές, είναι δηλαδή μία συσκευή με πολλές διαφορετικές χρήσεις :

- Άνοιγμα πόρτας
- Μεγάλη ασφάλεια δωματίων & γραφείων
- Επιτήρηση από απόσταση
- Εξοικονόμηση ενέργειας με χρονοκαθυστέρηση
- Αχρήματες συναλλαγές
- Εύκολος προγραμματισμός Καρτών
- Πιστοποίηση CE
- Εκτύπωση καρτών κατόπιν Παραγγελίας

❖ Περιγραφή

Το προϊόν βασίζεται σε έναν επίτοιχο αναγνώστη καρτών ο οποίος δέχεται πλαστικές έξυπνες κάρτες (που περιέχουν τσιπάκι παρόμοιο με τις τηλεκάρτες).

Όταν τοποθετηθεί από την εξωτερική πλευρά του δωματίου λειτουργεί ως καρτοκλειδαριά, ο ένοικος απλά εισαγάγει την κάρτα του στη σχισμή και ή ηλεκτρική κλειδαριά (κυπρί) ανοίγει με ασφάλεια. Έχει προβλεφθεί εσωτερική μπαταρία στον αναγνώστη καρτών για τις διακοπές ρεύματος. Η διάρκεια ισχύος της τηλεκάρτας εξαρτάται από τον χρονικό προγραμματισμό που θα της γίνει από τη reception.

Η ασφάλεια του αναγνώστη καρτών είναι πολύ υψηλή διότι διαθέτει ένα απαραβίαστο πρόγραμμα με 27 εκατομμύρια κωδικούς που όταν επιχειρηθεί προσπάθεια εισβολής με άλλη μη εξουσιοδοτημένη ή ληγμένη κάρτα να την αγνοεί.

Με τον αναγνώστη καρτών Smart Control 4000 ως καρτοκλειδαριά, μπορείτε να διατηρήσετε την παλιά σας πόρτα με την γνωστή μηχανική κλειδαριά και χωρίς πολλά μερεμέτια να προσθέσετε ένα ηλεκτρικό κυπρί στο σταθερό μέρος της κάσας. Η μόνη απαίτηση είναι η τοποθέτηση ενός ψιλού καλωδίου 0.50mm μέχρι το ηλεκτρικό κυπρί.

Για τον προγραμματισμό της έξυπνης κάρτας χρειάζεται ένα απλό PC και ο ειδικός προγραμματιστής, όπου το πρόγραμμα προγραμματισμού δίδεται δωρεάν.

Υπάρχουν τρία επίπεδα ασφαλείας α) master, β) προσωπικό και γ) πελάτης. Ο πελάτης έχει περιορισμένη χρονική πρόσβαση πχ. 5 ημέρες ή κάποιες ώρες, το προσωπικό πχ. ένα έτος και το master απεριόριστη πρόσβαση.

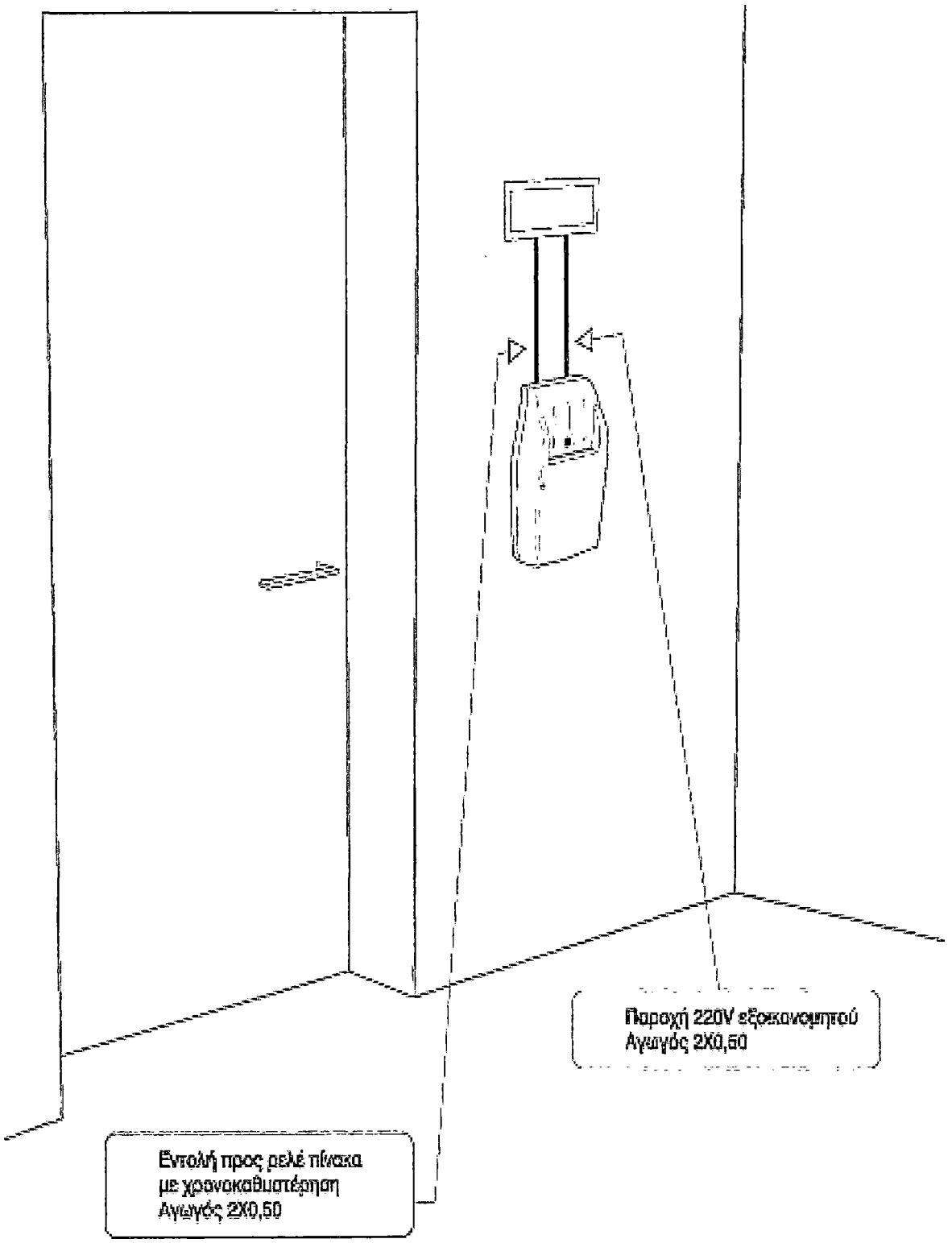
Ο αναγνώστης καρτών Smart Control 4000 όταν τοποθετείται στο εσωτερικό του δωματίου λειτουργεί ως εξοικονομητής (με διαφορετικό λογισμικό).Για τον έλεγχο των φορτίων πχ. 2Kw, 5 ή 10 KW σε studio ή δίχωρα δωμάτια με κουζίνα και θερμοσίφωνα χρειάζεται απαραιτήτως ρελέ ισχύος στον πίνακα του ηλεκτρικού. Η λειτουργία του είναι απλή. Όταν ο ένοικος εισέρχεται στο δωμάτιο βάζει την Smartcard (έξυπνη κάρτα) στον αναγνώστη καρτών και μόνο τότε έχει φώς-ρεύμα το δωμάτιο (εννοείται ότι η γραμμή του ψυγείου έχει εξαιρεθεί από την σύνδεση με τον εξοικονομητή). Όταν ο ένοικος αποχωρεί από το δωμάτιο τραβά την Smartcard από τον αναγνώστη καρτών και το ρεύμα κλείνει μετά από 1 λεπτό, διευκολύνοντας έτσι την αποχώρηση.

Αν προμηθευτείτε τον αναγνώστη καρτών μόνο ως εξοικονομητή, μπορείτε εύκολα να ενσωματώσετε την κάρτα μαζί με το κλειδί του δωματίου με ένα ισχυρό κρίκο όπως το γνωστό μαγνητικό μπρελόκ.

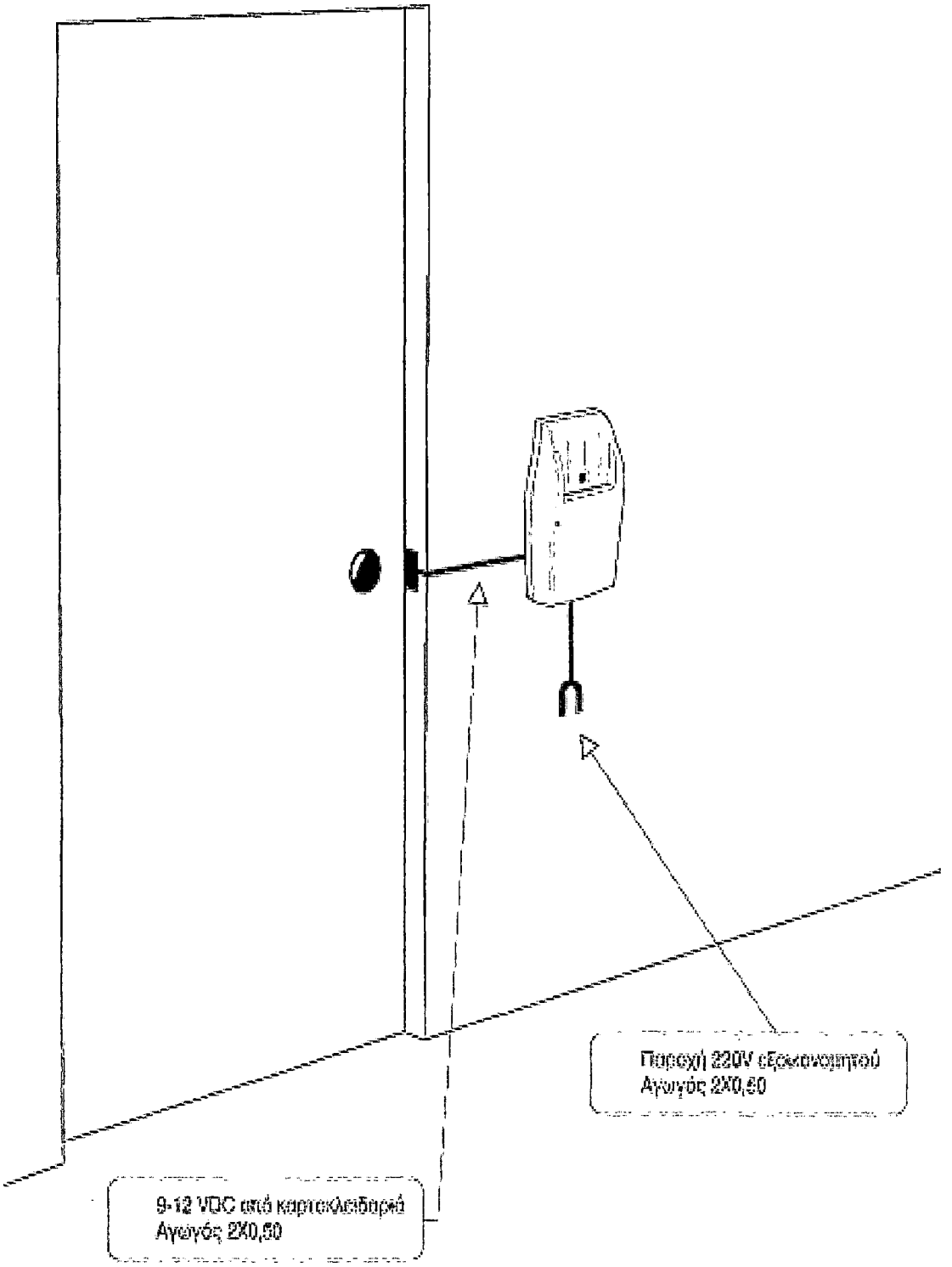
❖ Σύνδεση –Εγκατάσταση

Για τη σύνδεση του Smart Control 4000 χρειάζεται μόνο ένα διπολικό καλώδιο 0,50mm για την ηλεκτρική παροχή της συσκευής και επίσης ένα διπολικό καλώδιο ιδίας διατομής που μεταφέρει την εντολή προς το ρελέ ισχύος ή προς το ηλεκτρικό κυπρί προκειμένου να λειτουργήσει ως καρτοκλειδαριά.

Η μεγάλη ασφάλεια και η αξιοπιστία του αναγνώστη καρτών Smart Control 4000 δίνει την ευχέρεια για πολλές και χρήσιμες εφαρμογές, όπως η τοποθέτηση έξω από κάποιους ειδικούς χώρους ώστε να ελέγχουμε την πρόσβαση πχ. γήπεδα τένις, γυμναστήρια, πισίνες, σάουνα, μπόουλινγκ, γκαράζ, αποθήκες, με τον Smart Control 4000 μπορούμε να ενοικιάζουμε τη χρήση συσκευών - μηχανημάτων κλιματιστικών ή να πραγματοποιούμε αχρήματες συναλλαγές στα διάφορα τμήματα!



ΕΙΚΟΝΑ 72 : Συσκευή ανάγνωσης έξυπνων καρτών για άνοιγμα πόρτας



ΕΙΚΟΝΑ 73 : Συσκευή ανάγνωσης έξυπνων καρτών για άνοιγμα πόρτας

25.3 ΠΑΡΑΔΕΙΓΜΑ Γ – ΕΞΥΠΝΗ ΚΑΡΤΑ ΥΓΕΙΑΣ [125]

Η Σλοβενία είναι πρωτοπόρος χώρα στην εφαρμογή συστημάτων πληροφορικής και τηλεπικοινωνιών, με έμφαση σε εφαρμογές που βασίζονται σε «έξυπνες κάρτες». Το 1992 η Σλοβένικη κυβέρνηση αποφάσισε να αναδιαρθρώσει το εθνικό σύστημα υγείας, στα πλαίσια μιας γενικότερης κοινωνικοοικονομικής μεταρρύθμισης.

Στη Σλοβενία ίσχυε το σύστημα υποχρεωτικής ασφάλισης υγείας όλου του πληθυσμού στο μη-κερδοσκοπικό Ίδρυμα Ασφαλίσεων Υγείας, ενώ ο πληθυσμός δεν μπορούσε να έχει συμπληρωματική ασφάλιση για να καλύπτει περαιτέρω έξοδα υγείας ή να διαλέξει ιατρούς που δεν άνηκαν στο δημόσιο πρόγραμμα υγείας. Στα πλαίσια της μεταρρύθμισης, δόθηκε η δυνατότητα στους ασφαλισμένους να επιλέγουν τον ιατρό τους, στον δημόσιο ή ιδιωτικό τομέα που άρχισε να ανθίζει, αλλά και να επιλέγουν συμπληρωματικά πακέτα ασφάλισης είτε μέσω του κρατικού Ιδρύματος Ασφαλίσεων ή ιδιωτικών ασφαλιστικών οργανισμών.

Οι αλλαγές στο σύστημα υγείας, ήτοι ενθάρρυνση της ιδιωτικής πρωτοβουλίας στον τομέα της υγείας και προώθηση νέων προγραμμάτων ασφάλισης έδωσαν το έναυσμα για τον εκσυγχρονισμό των διαδικασιών του τομέα της υγείας. Το πρώτο βήμα ήταν η υιοθέτηση ενός ηλεκτρονικού εργαλείου διασύνδεσης των σημείων παροχής υπηρεσιών υγείας με τις τυποποιημένες βάσεις δεδομένων του Ιδρύματος Ασφαλίσεων, με απώτερο στόχο την πρόσβαση στην ιατρική πληροφορία του κάθε ασφαλισμένου από οποιοδήποτε σημείο της χώρας.

Το μέσο που επιλέχθηκε για την πλήρωση των στόχων αυτών ήταν οι έξυπνες κάρτες υγείας. Οι κάρτες αντικατέστησαν τα έντυπα βιβλιάρια υγείας. Αξίζει να σημειωθεί ότι το βιβλιάριο υγείας περιείχε γενικές και ιατρικές πληροφορίες για τον κάθε ασφαλιζόμενο και έπρεπε να ανανεώνεται σε μηνιαία βάση από τον εργοδότη ή το κράτος, για τις περιπτώσεις ελεύθερων επαγγελματιών.

Επιπλέον, οι ιατρικές πληροφορίες έπρεπε να συμπληρώνονται μετά από κάθε επίσκεψη στον ιατρό. Ωστόσο, η διαδικασία ενημέρωσης των βιβλιαρίων με την εισαγωγή των νέων στοιχείων ήταν εξαιρετικά χρονοβόρα για όλους τους εμπλεκόμενους (ασθενείς, ιατρούς, εργοδότες) κι έτσι τις περισσότερες φορές τα βιβλιάρια περιείχαν αποσπασματικές και ανεπαρκείς πληροφορίες, καθυστερώντας ακόμα περισσότερο της διαδικασίες αποπληρωμής των ιατρικών υπηρεσιών.

Το Σεπτέμβριο του 1995 το Ίδρυμα Ασφαλίσεων Υγείας της Σλοβενίας έθεσε σε ισχύ το πιλοτικό πρόγραμμα «Κάρτα Ασφάλισης», το οποίο και ήταν βασισμένο σε τεχνολογία έξυπνων καρτών.

Ήδη από την 1η Οκτωβρίου του 2000 η Σλοβενία εφάρμοσε το πλήρες σύστημα προσωπικής ηλεκτρονικής κάρτας υγείας στα σχεδόν 2 εκατομμύρια πληθυσμού της χώρας. Η εν λόγω κάρτα καταργεί τα έντυπα υγείας (ατομικό βιβλιάριο ασφάλισης) και αποτελεί το μοναδικό ηλεκτρονικό μέσο το οποίο και χρειάζεται ο ασθενής προκειμένου να επισκεφτεί τον προσωπικό του ιατρό ή/ και το νοσοκομείο.

25.3.1 ΛΕΙΤΟΥΡΓΙΑ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ

Ο κάθε ασφαλιζόμενος είναι εφοδιασμένος με την έξυπνη κάρτα υγείας, η οποία αντικαθιστά το βιβλιάριο υγείας. Η κάρτα περιέχει έναν μικροεπεξεργαστή και έχει μνήμη 16kB.

Πάνω στην κάθε κάρτα βρίσκονται τυπωμένες οι εξής πληροφορίες, όπως φαίνεται και στην εικόνα που ακολουθεί:

α) το λογότυπο του Ιδρύματος Ασφαλίσεων.
β) ο αριθμός της αρχής που εξέδωσε την κάρτα.
γ) ο αριθμός μητρώου του ασφαλισμένου.
δ) το ονοματεπώνυμο του ασφαλισμένου.
ε) και η ημερομηνία γέννησης του ασφαλισμένου.

ΕΙΚΟΝΑ 74 : Έξυπνη κάρτα υγείας

Για τους ασφαλισμένους που ανήκουν σε εθνικές μειονότητες, δηλαδή Ούγγροι και Ιταλοί, οι πληροφορίες τυπώνονται και στις δύο επίσημες γλώσσες αντίστοιχα. Επίσης, η κάρτα έχει τυπωμένο ειδικό ανάγλυφο σημάδι για τους τυφλούς χρήστες.

Στο τσιπ της κάρτας υγείας αποθηκεύονται οι ακόλουθες πληροφορίες ηλεκτρονικά:

α) **Στοιχεία του κατόχου της κάρτας**
(ονοματεπώνυμο, διεύθυνση, φύλο, ημερομηνία γέννησης)

β) **Στοιχεία του φορέα παροχής ασφαλιστικής κάλυψης**
(αριθμός μητρώου, όνομα φορά, διεύθυνση)

γ) **Στοιχεία υποχρεωτικής ασφάλισης**
(ημερομηνία ανανέωσης, ισχύς της ασφάλισης)

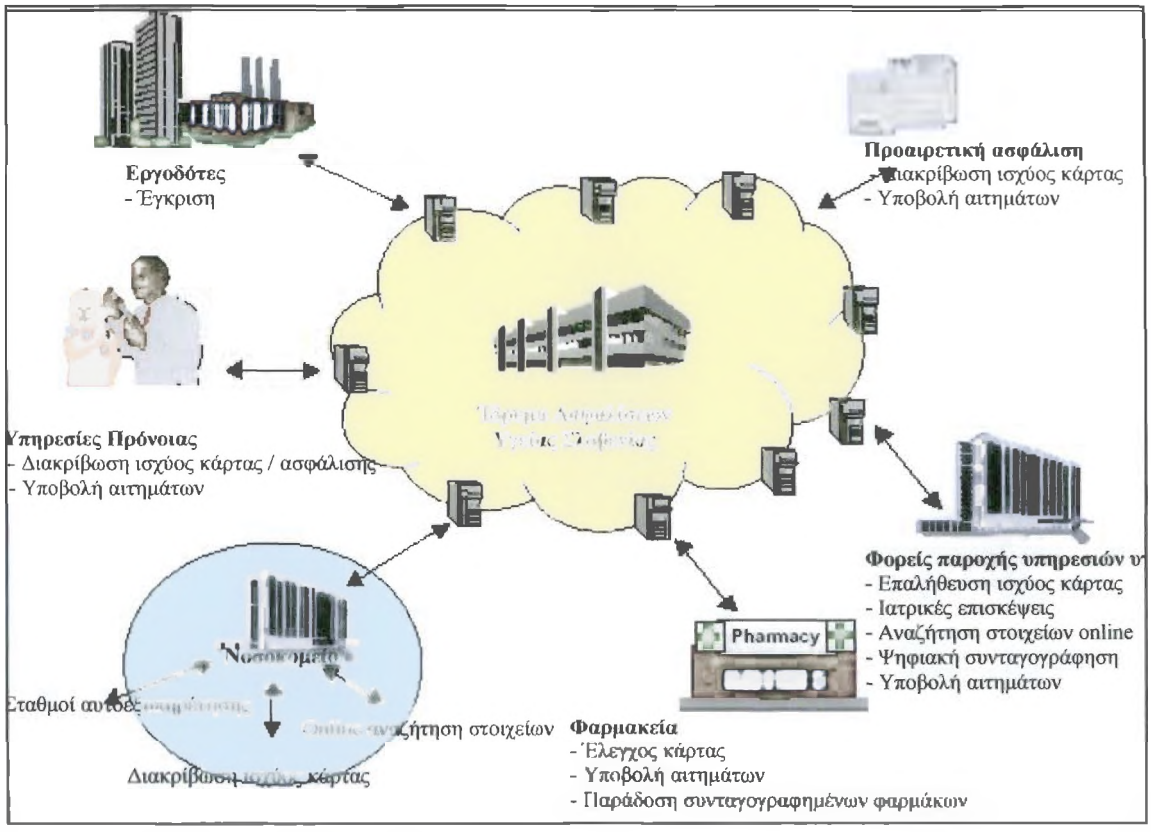
δ) **Στοιχεία προαιρετικής ασφάλισης**
(τύπος ασφάλισης, ισχύς)

ε) **Στοιχεία επιλεγμένων ιατρών**
(παθολόγος, παιδίατρος, οδοντίατρος, γυναικολόγος)

στ) **Ιατρικά βοηθήματα που δόθηκαν στα πλαίσια της ασφάλισης**

Ουσιαστικά, στην κάρτα αποθηκεύονται οι πληροφορίες που βρίσκονται επίσης αποθηκευμένες στην κεντρική βάση δεδομένων του συστήματος υγείας της Σλοβενίας. Η κάρτα δεν αποτελεί ένα «φορητό» ηλεκτρονικό ιατρικό φάκελο, παρά εμπεριέχει μόνο επιλεγμένες ιατρικές πληροφορίες, οι οποίες δεν αλλάζουν συχνά και είναι ουσιαστικές για την παροχή πρώτων βοηθειών (π.χ. αλλεργίες σε συγκεκριμένα σκευάσματα, χορήγηση ινσουλίνης, κτλ).

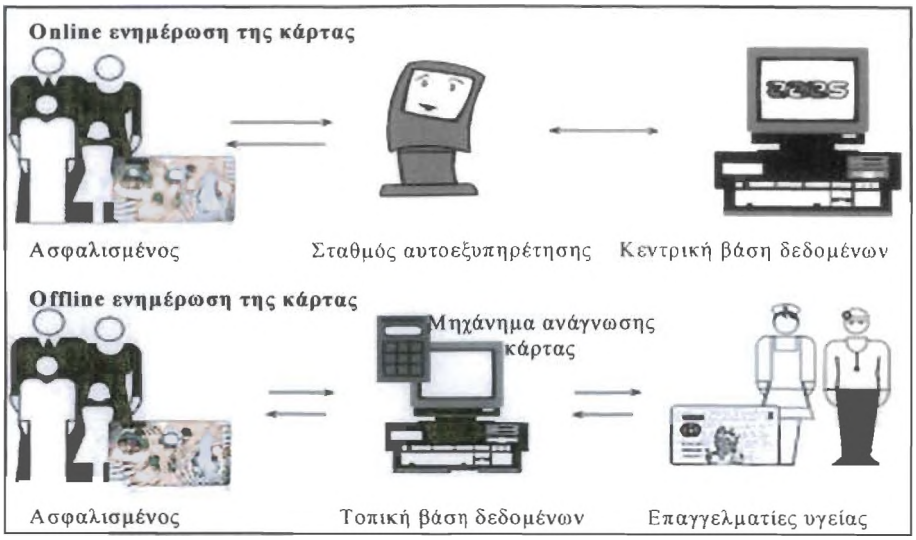
Ωστόσο, μόλις ολοκληρωθεί η ένταξη όλων των φορέων παροχής υπηρεσιών υγείας σε ένα κοινό δίκτυο πληροφοριών η κάρτα μπορεί κάλλιστα να έχει και το ρόλο κλειδιού μέσω του οποίου θα παρέχεται πρόσβαση σε εξουσιοδοτημένους χρήστες στον ιατρικό φάκελο του ασθενούς. Για να υλοποιηθεί όμως αυτό το στάδιο απαιτείται επιπλέον σχεδιασμός λογισμικού καθώς και επένδυση σε υλικοτεχνική υποδομή, ώστε να συνδυαστεί η εγγραφή ευαίσθητης ιατρικής πληροφορίας στην κάρτα με τη διασφάλιση που προσφέρουν οι ηλεκτρονικές υπογραφές.



ΕΙΚΟΝΑ 75 : Ανταλλαγή πληροφορίας στα πλαίσια του συστήματος έξυπνης κάρτας στη Σλοβενία

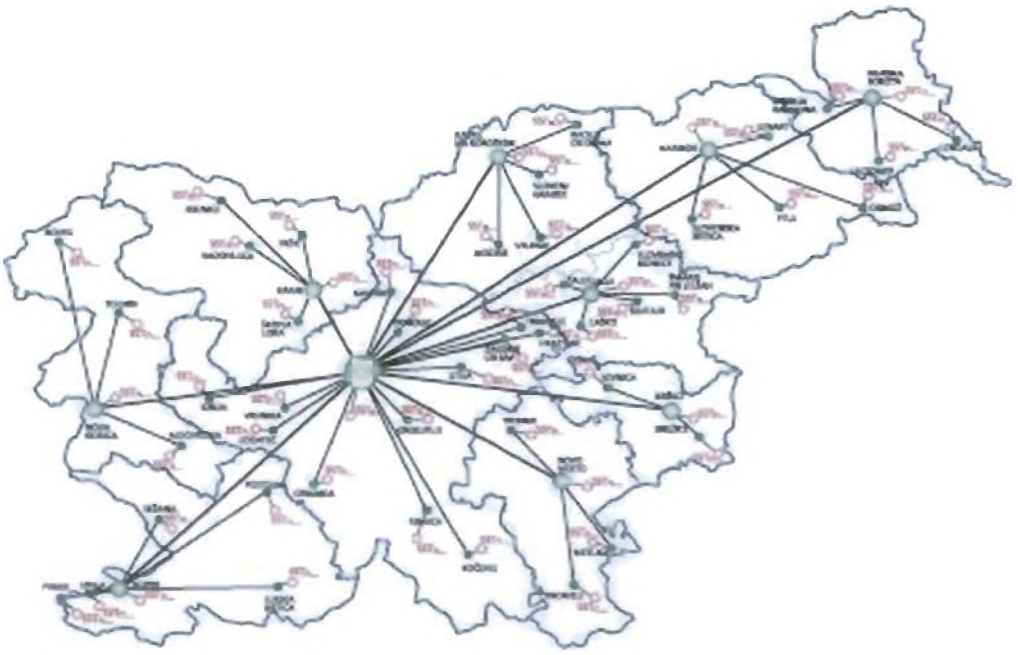
Η ενημέρωση της κάρτας γίνεται από τον ίδιο τον κάτοχο της κάρτας κάθε φορά που επισκέπτεται το νοσοκομείο, όπου και υπάρχουν εγκατεστημένοι τοπικοί σταθμοί αυτοεξυπηρέτησης πελατών.

Στους τοπικούς αυτούς σταθμούς εξακριβώνεται η ισχύς της ασφαλιστικής κάλυψης και άρα και της κάρτας ενώ γίνεται και ανανέωση / αυτόματη ενημέρωση της πληροφορίας που αποθηκεύεται στην κάρτα ηλεκτρονικά από την κεντρική βάση δεδομένων. Ο ασφαλισμένος μπορεί επίσης μέσω τον τοπικών σταθμών να αποστείλει αίτημα και να λάβει κατόπιν (εντός τριών εργάσιμων ημερών) τις ειδικές συμβάσεις, μέσω των οποίων δίδεται η δυνατότητα πρόσβασης σε υπηρεσίες υγειονομικής περίθαλψης κατά τη διάρκεια προσωρινών διαμονών στο εξωτερικό.



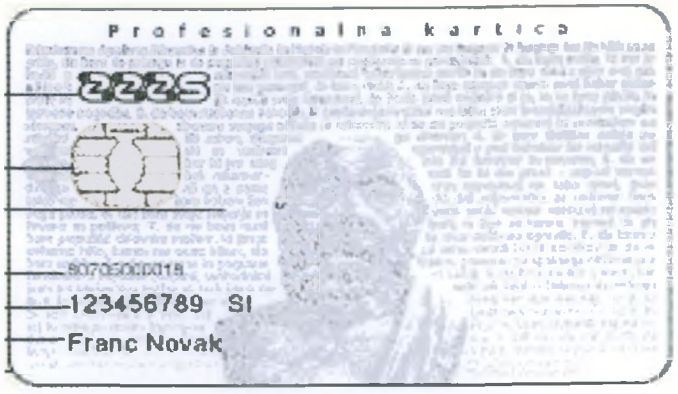
ΕΙΚΟΝΑ 76 : Σχηματική αναπαράσταση ενημέρωσης κάρτας

Υπάρχουν στη Σλοβενία σήμερα 295 τοπικοί σταθμοί αυτοεξυπηρέτησης, εγκατεστημένοι σε βασικά σημεία στη χώρα, κυρίως στις εγκαταστάσεις δημόσιων φορέων παροχής υπηρεσιών υγείας και κοινωφελών ινστιτούτων. Όλοι οι περιφερειακοί σταθμοί συνδέονται με την κεντρική βάση στη Λουμπλιάνα.



ΕΙΚΟΝΑ 77 : Δίκτυο τοπικών σταθμών αυτοεξυπηρέτησης ασφαλισμένων

Σε κάθε άλλη περίπτωση, η πρόσβαση στα στοιχεία της κάρτας γίνεται μόνο με την παρουσία εξουσιοδοτημένου επαγγελματία. Ο τελευταίος έχει στα χέρια του την επαγγελματική κάρτα υγείας. Στην επαγγελματική κάρτα αναγράφεται το ονοματεπώνυμο του κατόχου, ενώ στο πίσω μέρος υπάρχει χώρος υπογραφής. Η κάρτα περιέχει έναν μικροεπεξεργαστή και έχει μνήμη 8kB. Η επαγγελματική κάρτα είναι διακοσμημένη με το πορτρέτο του Ιπποκράτη, ενώ στο φόντο υπάρχει το κείμενο του όρκου του Ιπποκράτη.



ΕΙΚΟΝΑ 78 : Επαγγελματική κάρτα υγείας

Στον επεξεργαστή (μικροτσίπ) της κάρτας αποθηκεύονται ηλεκτρονικά οι εξής πληροφορίες:

α) **Ο μοναδικός αριθμός μητρώου** του κάτοχου της κάρτας στο Ίδρυμα Ασφαλίσεων Υγείας
β) **Το ονοματεπώνυμο του χρήστη**
γ) **Το επάγγελμα**
δ) **Ο κωδικός της χώρας**
ε) **Ο κωδικός του Ινστιτούτου Δημόσιας Υγείας**
στ) **Η ειδικότητα** του κατόχου της κάρτας
ζ) **Το είδος της πρόσβασης** που επιτρέπεται για τον συγκεκριμένο χρήστη

Η επαγγελματική κάρτα υγείας δίδεται σε ιατρούς, νοσοκόμες, το διοικητικό προσωπικό στους χώρους υποδοχής των φορέων παροχής υπηρεσιών υγείας, σε φαρμακοποιούς, φυσιοθεραπευτές και λοιπούς εξουσιοδοτημένους επαγγελματίες της υγείας καθώς και το εξουσιοδοτημένο προσωπικό των ασφαλιστικών οργανισμών.

Η επαγγελματική κάρτα υγείας αποτελεί το κλειδί πρόσβασης στα δεδομένα των καρτών υγείας των ασφαλισμένων. Η προσπέλαση των στοιχείων της κάρτας ενός ασφαλισμένου γίνεται μόνο με την παρουσία ενός κατόχου επαγγελματικής κάρτας (δηλαδή ενός εξουσιοδοτημένου ατόμου) ως εξής: ο εξουσιοδοτημένος χρήστης εισάγει τον μοναδικό προσωπικό του κωδικό αναγνώρισης (PIN) στο μηχάνημα ανάγνωσης καρτών (card reader). Εφόσον αναγνωριστεί ως εξουσιοδοτημένος χρήστης επιτυχώς, μπορεί πλέον να «διαβάσει» τα δεδομένα που βρίσκονται αποθηκευμένα στην κάρτα υγείας του ασφαλισμένου και επίσης να εισάγει νέες πληροφορίες.

ΕΙΚΟΝΑ 79 : Αναγνώστης καρτών, συνδεδεμένος με Η/Υ

ΕΙΚΟΝΑ 80 : Φορητός αναγνώστης καρτών

25.3.2 ΟΦΕΛΗ ΤΩΝ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ ΥΓΕΙΑΣ

Το σύστημα έξυπνων καρτών υγείας της Σλοβενίας την καθιστά μία πρωτοπόρο χώρα σε αυτό τον τομέα. Το σύστημα έχει αναπτυχθεί σε συνάφεια με την ισχύουσα νομοθεσία ενώ είναι εφικτό να ολοκληρωθεί με την Ευρωπαϊκή Κάρτα Υγείας.

Η Σλοβενία θα είναι από τις πρώτες χώρες που θα υιοθετήσουν την Ευρωπαϊκή Κάρτα από την 1η Ιουνίου του 2004. Το 82,9% του πληθυσμού που χρησιμοποιεί την κάρτα αξιολογεί θετικά και είναι ικανοποιημένο από το σύστημα κάρτας υγείας.

Τα οφέλη από την υιοθέτηση του συστήματος έξυπνων καρτών είναι πολλαπλά:

- **Βελτίωση της ποιότητας των παρεχόμενων υπηρεσιών υγείας και απλοποίηση των διαδικασιών**

Η χρήση έξυπνων καρτών επιτρέπει την άμεση και έγκυρη διακίνηση της πληροφορίας μεταξύ των επαγγελματιών της υγείας. Με αυτόν τον τρόπο, αποφεύγεται η άσκοπη επανάληψη διαγνωστικών εξετάσεων και προλαμβάνεται η συνταγογράφηση μη συμβατών φαρμάκων και θεραπευτικών πλάνων.

Η αποθήκευση και έγκαιρη ενημέρωση της ιατρικής πληροφορίας για τον κάθε ασθενή αυξάνει τον όγκο και την ποιότητα της διαθέσιμης πληροφορίας και έτσι ο κάθε ασφαλισμένος / χρήστης της κάρτας απολαμβάνει ποιοτικότερες, ασθενοκεντρικές υπηρεσίες υγείας.

Παράλληλα όμως, η ευαίσθητη ιατρική πληροφορία και κατά επέκταση τα προσωπικά δεδομένα του κάθε ασφαλισμένου προστατεύονται, διότι είναι προσβάσιμα αποκλειστικά από εξουσιοδοτημένους χρήστες.

Αξίζει να σημειωθεί, ότι τα συγκεντρωμένα ιατρικά δεδομένα μπορούν να χρησιμοποιηθούν ανώνυμα για ιατρικούς ερευνητικούς σκοπούς, συγκριτικές μελέτες, στατιστικά ανάλυση και έρευνα, συμβάλλοντας στην ανάπτυξη βελτιωμένων μηχανισμών προληπτικής ιατρικής και δημόσιας υγείας.

- **Βελτίωση της επικοινωνίας μεταξύ των φορέων παροχής υπηρεσιών υγείας**

Η έξυπνη κάρτα συμβάλλει στην ανταλλαγή της πληροφορίας μεταξύ των φορέων παροχής ιατρικής φροντίδας, των ασφαλιστικών οργανισμών, των φαρμακείων και των ιατρών ανεξαρτήτως γεωγραφικών περιορισμών. Ο πολίτης μπορεί να λαμβάνει πλέον ποιοτικές υπηρεσίες υγείας σε όποιο σημείο της χώρας κι αν βρίσκεται χωρίς ανώφελες καθυστερήσεις που οφείλονται σε χρονοβόρες γραφειοκρατικές διαδικασίες.

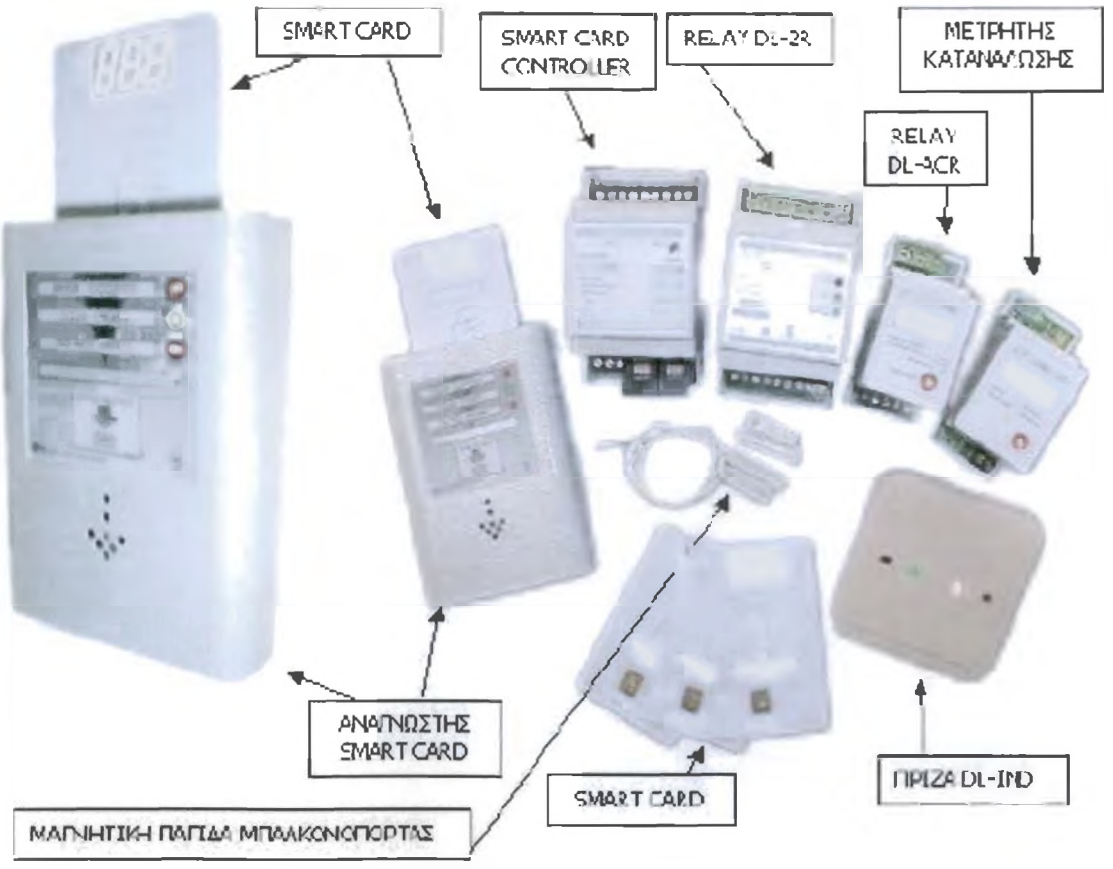
- **Βελτιωμένοι μηχανισμοί ασφάλειας και εμπιστευτικότητας**

Η κάρτα του κάθε ασθενούς ελέγχεται και ενημερώνεται από τον ίδιο ή με την παρουσία εξουσιοδοτημένου χρήστη. Η έξυπνη κάρτα διασφαλίζει την ελεγχόμενη διάθεση της πληροφορίας.

❖ **Μείωση της γραφειοκρατίας - Βελτίωση της λειτουργικής αποδοτικότητας των ασφαλιστικών οργανισμών και των φορέων παροχής υπηρεσιών υγείας**

Η ηλεκτρονική διάθεση και επεξεργασία της πληροφορίας συμβάλλει δραματικά στη μείωση του κόστους διεκπεραίωσης αιτημάτων και συνεπώς, οι εσωτερικές διαδικασίες του εκάστοτε φορέα παροχής υπηρεσιών υγείας γίνονται πιο αποτελεσματικές. Η ηλεκτρονική υποβολή αιτημάτων συμβάλλει στη μείωση του χρόνου που απαιτείται για την ολοκλήρωση των διοικητικών διεργασιών, ενώ και ταυτόχρονα μειώνεται το ενδεχόμενο λαθών από τη χειρόγραφη εισαγωγή στοιχείων. Ως εκ τούτου, μειώνεται το κόστος προσωπικού και επιτυγχάνεται αποτελεσματικότερη και αποδοτικότερη διαχείριση πόρων στα πλαίσια του κάθε φορέα.

25.4 ΠΑΡΑΔΕΙΓΜΑ Δ - ΣΥΣΤΗΜΑΤΑ ΕΛΕΓΧΟΥ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ ΡΕΥΜΑΤΟΣ ΔΩΜΑΤΙΩΝ ΞΕΝΟΔΟΧΕΙΟΥ ΜΕ ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ [126]



ΕΙΚΟΝΑ 81 : Σύστημα ελέγχου και οικονομίας ρεύματος δωματίου ξενοδοχείου με έξυπνη κάρτα

Αποτελείται (ανά δωμάτιο):

- **SCC-3R.** Controller κεντρικού ελέγχου δωματίου, σε κιτίο ηλεκτρολογικού πίνακα (χρειάζεται χώρο 3ων αυτομάτων).Ο κοντρόλερ συνεργάζεται και με

οποιοδήποτε τύπο ηλεκτρολογικών Relay άλλων εταιριών, μέσω των ψυχρών επαφών που διαθέτει (3 mini Relay 1A, για έλεγχο φώτων – κλιματισμού - άνοιγμα πόρτας).

- **DL-2r.** Relay 30A για τον έλεγχο φώτων και άλλων φορτίων και 16A για ξεχωριστό έλεγχο του Air condition (συνδέεται με το SCC-3R).
- **SM-C.** Πρίζες αναγνώστες έξυπνων καρτών (2 τεμάχια) τοποθετημένα ένα εκτός δωματίου για το άνοιγμα της πόρτας και ένα εντός του δωματίου για την συγκράτηση των ηλεκτρικών φορτίων σε λειτουργία.
- Μία έξυπνη κάρτα προγραμματισμένη.
- Μαγνητική επαφή μπαλκονόπορτας.

Επιπλέον ανά ξενοδοχείο δίνονται:

- Έξυπνη κάρτα Master και Reset για προγραμματισμό νέων καρτών από το χρήστη.

❖ ΛΕΙΤΟΥΡΓΙΕΣ :

- **Άνοιγμα πόρτας.**

Ο controller με την εισδοχή αποδεκτής κάρτας στην εξωτερική πρίζα, ενεργοποιεί την τροφοδοσία της ηλεκτρικής κλειδαριάς πόρτας για συγκεκριμένο χρόνο, ενώ ταυτόχρονα ανάβει η πράσινη λυχνία καθοδηγώντας τον πελάτη να σπρώξει την πόρτα. Ταυτόχρονα ο controller ενεργοποιεί το relay φωτισμού και το relay κλιματισμού για χρονικό διάστημα 30sec.

- **Συγκράτηση λειτουργίας.**

Ο πελάτης με την είσοδό του στο δωμάτιο τοποθετεί την έξυπνη κάρτα στην εσωτερική πρίζα για τη μόνιμη λειτουργία των ηλεκτρικών φορτίων του δωματίου. Ενεργοποιείται η πράσινη λυχνία της εσωτερικής πρίζας .Στην εξωτερική πρίζα, ανάβει η κόκκινη λυχνία ενημερώνοντας έτσι τις καμαριέρες ότι το δωμάτιο είναι κατειλημμένο.

- **Έλεγχος κλιματισμού.**

Ο πελάτης έχει δικαίωμα αν ο κλιματισμός είναι ανοικτός, να ανοίξει την μπαλκονόπορτα για χρόνο 5 λεπτών χωρίς να διακοπεί η λειτουργία του. Αν η μπαλκονόπορτα παραμείνει ανοικτή για περισσότερο χρόνο, η λειτουργία του κλιματισμού διακόπτεται.

- **Ταυτόχρονη είσοδος στο δωμάτιο.**

Ο ξενοδόχος μπορεί να διαθέσει και $2^{η}$ κάρτα στους πελάτες του, έτσι ώστε αν κάποιος από τους πελάτες κοιμάται στο δωμάτιο (δωμάτιο κατειλημμένο), ο συγκάτοικός του να μπορεί να ενεργοποιήσει και αυτός το άνοιγμα της πόρτας, με τη δική του κάρτα.

- **Καθυστέρηση στο σβήσιμο.**

Με την αφαίρεση της κάρτας από την εσωτερική πρίζα, (έξοδος πελάτη) ο φωτισμός και το air-condition σβήνουν μετά από 30sec δίνοντας χρόνο στον πελάτη ή να ξαναβάλει την κάρτα ή να απομακρυνθεί με ασφάλεια. Η καθυστέρηση εξασφαλίζει επίσης την μη πρόκληση βλαβών στις ηλεκτρονικές συσκευές από στιγμιαίο σβήσιμο- άναμμα.

- **Ιδιότητα ' Μην ενοχλείτε '.**

Ο πελάτης του δωματίου βγάζοντας και βάζοντας την κάρτα του στήν εσωτερική πρίζα , ενεργοποιεί και απενεργοποιεί αντίστοιχα την λειτουργία '' μην ενοχλείτε '' ανάβοντας την ειδική λυχνία DO NOT DISTURB στην εξωτερική και εσωτερική πρίζα του δωματίου. Όταν το δωμάτιο βρίσκεται σε αυτή την κατάσταση, ο μηχανισμός πόρτας δεν ενεργοποιείται πλέον από άλλες κάρτες του ιδίου δωματίου.(Με ειδικό διαφορετικό χειρισμό προβλέπεται η υπερπήδηση της παραπάνω ιδιότητας, για καταστάσεις ανάγκης).

- **Αναγνώριση πολλών καρτών ανά δωμάτιο.**

Ο controller του δωματίου είναι σε θέση να αναγνωρίζει μέχρι 5 διαφορετικούς κωδικούς καρτών. Έτσι έχουμε τη δυνατότητα π.χ για δυο διαφορετικούς κωδικούς πελατών (κάρτες) και τέσσερις διαφορετικούς κωδικούς (κάρτες) pass-partout , οι οποίες μπορούν να δοθούν σε διαφορετικά συνεργεία (άλλες στις καθαρίστριες, άλλες στους συντηρητές κτλ).

- **Προγραμματισμός και από τον ξενοδόχο.**

Το σύστημα παραδίδεται με προγραμματισμένες κάρτες. Δίνονται όμως στον ξενοδόχο και κάρτες Master και Reset, με την βοήθεια των οποίων μπορεί να προγραμματίσει μια νέα κάρτα (π.χ την $2^{η}$ κάρτα χρήστη ή την πρώτη κάρτα Pass-partout), ώστε να γίνει αποδεκτή από οποιαδήποτε πρίζα. Μπορεί επίσης να ακυρώσει κάποιους ή όλους τους κωδικούς από κάποια ή όλες τις πρίζες, εάν το θέλει, για λόγους ασφαλείας.

Ο προγραμματισμός γίνεται τοπικά, σε οποιαδήποτε πρίζα. Δεν απαιτείται η χρήση κεντρικού Η/Υ. Οι 2 κόκκινες και η πράσινη λυχνία της πρίζας, καθοδηγούν τον ξενοδόχο και διευκολύνουν την διαδικασία προγραμματισμού.

25.5 ΠΑΡΑΔΕΙΓΜΑ Ε – ΕΛΕΓΧΟΣ ΚΑΤΑΝΑΛΩΣΗΣ AIR CONDITION ΜΕ ΜΙΑ ΕΞΥΠΝΗ ΚΑΡΤΑ [127]

❖ **Περιγραφή συστήματος**

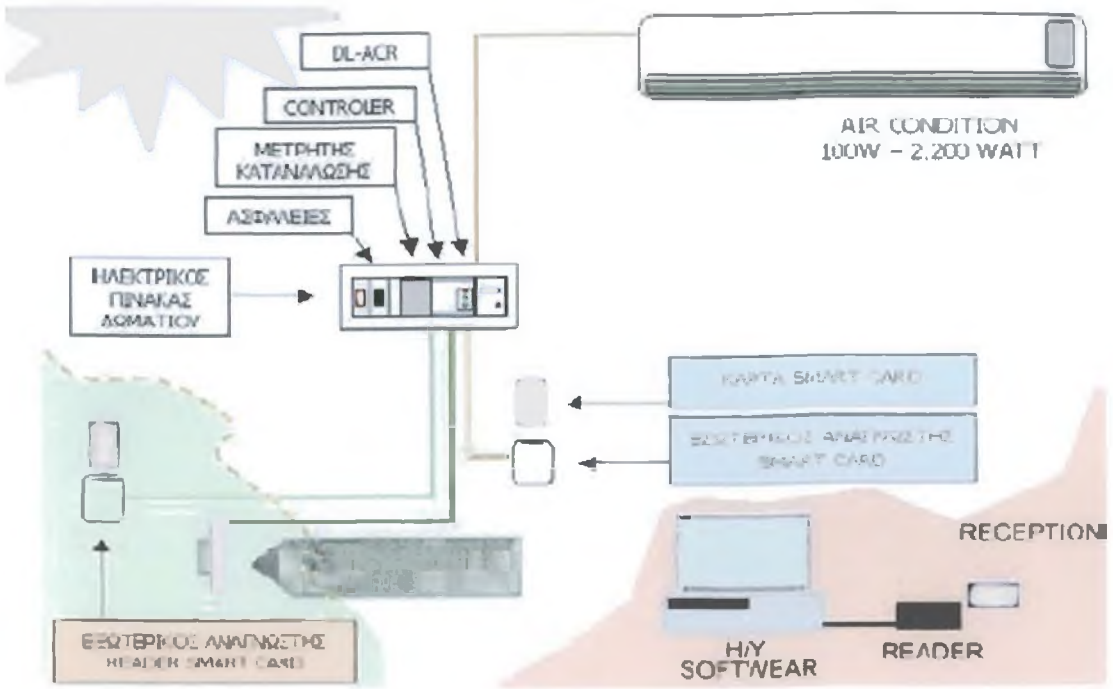
- **ΣΥΣΤΗΜΑ 1 – Έλεγχος air-condition**

Το ΣΥΣΤΗΜΑ1, θέτει σε κατάσταση ετοιμότητας (STAND-BY) το κλιματιστικό, με την είσοδο της έξυπνης κάρτας, στον εσωτερικό αναγνώστη. Μετά από αυτό, μπορεί ο πελάτης με την χρήση του χειριστηρίου, να θέσει σε λειτουργία τον κλιματισμό. Από την στιγμή που ο πελάτης θέσει σε λειτουργία τον κλιματισμό, αρχίζει η καταγραφή του χρόνου στην έξυπνη κάρτα.

Όταν η έξυπνη κάρτα, βγεί από τον αναγνώστη, το κλιματιστικό, δεν είναι δυνατόν να ενεργοποιηθεί. Όταν ο πελάτης κάνει CHECK-OUT, θα παραδώσει την έξυπνη κάρτα, στην Reception του ξενοδοχείου, όπου θα διαβαστεί ο συνολικός χρόνος λειτουργίας του κλιματιστικού και θα χρεωθεί ανάλογα.

Το ΣΥΣΤΗΜΑ1 αποτελείται από

- Αναγνώστη SMART CARD **ΤΕΜ. 1**
- Controller SMART CARD **ΤΕΜ. 1** – (χώρος 3ων ασφαλειών πίνακα)
- RELAY DL-ACR **ΤΕΜ. 1** – (χώρος 2 ασφαλειών πίνακα)
- Μετρητής κατανάλωσης **ΤΕΜ. 1** - (χώρος 2 ασφαλειών πίνακα)



ΕΙΚΟΝΑ 82 : Έλεγχος κατανάλωσης air condition με μια έξυπνη κάρτα

- **<u>ΣΥΣΤΗΜΑ 2 – Energy saver & έλεγχος κλιματιστικού</u>**

Εάν εκτός από τον έλεγχο του κλιματιστικού, θέλουμε να έχουμε και τον έλεγχο των καταναλώσεων του δωματίου, μπορούμε στο σύστημα ελέγχου του κλιματιστικού (**ΣΥΣΤΗΜΑ 1**), να αντικαταστήσουμε το Relay DL-ACR, με το Relay DL-2R.

Το ΣΥΣΤΗΜΑ1 αποτελείται από

- Αναγνώστη SMART CARD **ΤΕΜ. 1**
- Controller SMART CARD **ΤΕΜ. 1** – (χώρος 3ων ασφαλειών πίνακα)
- RELAY DL-2R **ΤΕΜ. 1** – (χώρος 3ων ασφαλειών πίνακα)
- Μετρητής κατανάλωσης **ΤΕΜ. 1** – (χώρος 2 ασφαλειών πίνακα)

- **<u>ΣΥΣΤΗΜΑ 3 – Άνοιγμα πόρτας, energy saver & έλεγχος κλιματιστικού</u>**

Εάν εκτός από τον έλεγχο του κλιματιστικού και των καταναλώσεων του δωματίου, θέλουμε να μπορούμε να ανοίγουμε και την πόρτα του δωματίου (χωρίς κλειδί), μπορούμε στο **ΣΥΣΤΗΜΑ2**, να προσθέσουμε ένα επιπλέον αναγνώστη έξυπνων καρτών , ο οποίος θα τοποθετηθεί εξωτερικά και θα συνεργαστεί με την γλωσσίδα της πόρτας 12V (πχ DOMUS,.. κλπ).

Το ΣΥΣΤΗΜΑ1 αποτελείται από

- Αναγνώστη SMART CARD **ΤΕΜ. 1**
- Controller SMART CARD **ΤΕΜ. 1** – (χώρος 3ων ασφαλειών πίνακα)
- RELAY DL-2R **ΤΕΜ. 1** – (χώρος 3ων ασφαλειών πίνακα)
- Μετρητής κατανάλωσης **ΤΕΜ. 1** – (χώρος 2 ασφαλειών πίνακα)

25.6 ΠΑΡΑΔΕΙΓΜΑ ΣΤ - ΔΙΑΦΟΡΑ ΕΙΔΗ ΚΑΡΤΩΝ [128]

❖ ΕΞΥΠΝΗ ΚΑΡΤΑ ΕΠΙΚΥΡΩΣΗΣ

Η συγκεκριμένη έξυπνη κάρτα επικύρωσης ,διευκολύνει την ασφάλεια των οικονομικών συναλλαγών σε περιβάλλον απευθείας σύνδεσης. Οι πιστωτικές κάρτες του μέλλοντος με ικανότητα επίδειξης, θα παρέχουν στους εκδότες καρτών ένα οικονομικώς αποδοτικό μέσο για να προσφέρουν ισχυρά εργαλεία επικύρωσης σε μια ευρεία καταναλωτική βάση.

Οι επιδείξεις καρτών της εταιρίας Aveso, που ενσωματώνονται στις πιστωτικές κάρτες, θα επιδείξουν έναν μοναδικό κώδικα πιστοποίησης ή κωδικό πιστοποίησης (one time password –OTP) μίας χρήσης για κάθε συναλλαγή, που καθιστά έναν στατικό αριθμό πιστωτικών καρτών άχρηστο.

ΕΙΚΟΝΑ 83 : Έξυπνη κάρτα επικύρωσης

➢ Λειτουργία έξυπνης κάρτας επικύρωσης

1 Ο χρήστης εισάγει το PIN σε ένα αριθμητικό πληκτρολόγιο στην κάρτα.
2 Η είσοδος PIN ενεργοποιεί την παραγωγή του κωδικού πρόσβασης μιάς χρήσης (OTP) που παρουσιάζεται στην επίδειξη της κάρτας Aveso.
3 Ο χρήστης εισάγει τον κωδικό πρόσβασης μίας χρήσης (OTP) μαζί με το όνομα και τον αριθμό κάρτας για να ολοκληρώσει την ασφαλή συναλλαγή.

❖ ΕΞΥΠΝΗ ΚΑΡΤΑ ΥΓΕΙΟΝΟΜΙΚΗΣ ΠΕΡΙΘΑΛΨΗΣ

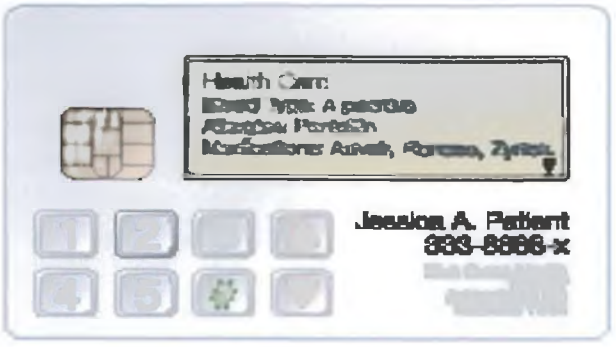
Η συγκεκριμένη έξυπνη κάρτα υγειονομικής περίθαλψης χρησιμοποιείται για την αποθήκευση και πρόσβαση των κρίσιμων ιατρικών πληροφοριών.

Οι έξυπνες κάρτες θεωρούνται ως η τεχνολογία που μπορεί να βοηθήσει τις οργανώσεις να καλύψουν τις απαιτήσεις μυστικότητας και ασφάλειας ενώ παράλληλα μπορούν να βοηθήσουν τις οργανώσεις υγειονομικής περίθαλψης να βελτιώσουν την αποδοτικότητα τους και να έχουν χαμηλότερα διοικητικά έξοδα και να βελτιώσουν την πρόσβαση των ασθενών στην ιατρική φροντίδα. Οι έξυπνες κάρτες αντιπροσωπεύουν επίσης έναν βολικό τρόπο να μεταφερθούν τα στοιχεία μεταξύ των συστημάτων ή στις περιοχές χωρίς συστήματα.

Οι έξυπνες κάρτες υγειονομικής περίθαλψης του μέλλοντος που επιτρέπονται από τις τυπωμένες ηλεκτρονικές επιδείξεις της Aveso θα επιτρέψουν στο χρήστη να

παράγει και να δει τις κρίσιμες πληροφορίες άμεσα από την ίδια την κάρτα η οποία περιλαμβάνει :

- κωδικούς πρόσβασης για την πρόσβαση στα ιατρικά αρχεία.
- ασφάλεια και πληροφορίες οφελών.
- βασικές προσωπικές πληροφορίες.
- ιατρικές πληροφορίες και ιστορικό.



ΕΙΚΟΝΑ 84 : Έξυπνη κάρτα υγειονομικής περίθαλψης

➢ **<u>Λειτουργία έξυπνης κάρτας υγειονομικής περίθαλψης</u>**

1 Ο χρήστης εισάγει την PIN σε ένα αριθμητικό πληκτρολόγιο στην κάρτα.
2 Το PIN επιτρέπει πρόσβαση για να κλειδώσει τις πληροφορίες χρηστών.

❖ **<u>ΕΞΥΠΝΗ ΚΑΡΤΑ ΑΠΟΘΗΚΕΥΜΕΝΗΣ ΑΞΙΑΣ</u>**

Οι κάρτες με αποθηκευμένη αξία του μέλλοντος θα επιτρέψουν στους εκδότες καρτών να προσφέρουν ένα νέο επίπεδο ευκολίας στους πελάτες τους. Οι χρήστες θα είναι σε θέση να δουν τις πληροφορίες όπως τις ισορροπίες καρτών δώρων-καρτών αποθηκευμένης αξίας . Οι κάρτες επίσης παρέχουν στους λιανοπωλητές μέσα για να ενημερώνονται για τις εξατομικευμένες πληροφορίες ή ακόμα και ημερομηνίες λήξης.

Αυτή η νέα γενιά των αποθηκευμένων καρτών δώρων αξίας ,που επιτρέπεται από τις τυπωμένες ηλεκτρονικές επιδείξεις της εταιρίας Aveso θα ενισχύσει το εισόδημα λιανοπωλητών ενώ παράλληλη θα συνεισφέρει και στην καταναλωτική πίστη των πελατών.

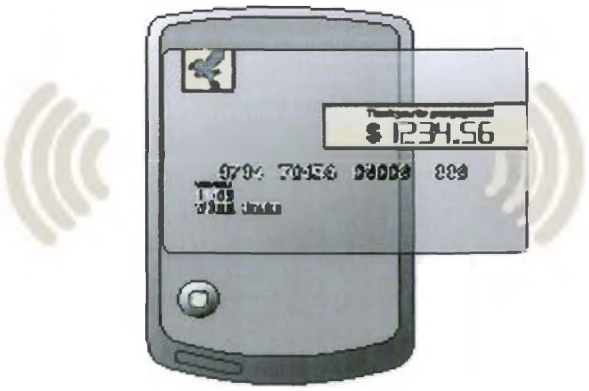
ΕΙΚΟΝΑ 85 : Έξυπνη κάρτα αποθηκευμένης αξίας

➢ **Λειτουργία έξυπνης κάρτας αποθηκευμένης αξίας**

1 Ο χρήστης εισάγει το PIN σε ένα αριθμητικό πληκτρολόγιο στην κάρτα.
2 Η είσοδος PIN ενεργοποιεί την κάρτα ,που επιδεικνύει τις πληροφορίες όπως την αποθηκευμένη ποσά αγορών ισορροπίας ή παρελθόντος.

❖ **ΑΝΕΠΑΦΗ ΕΞΥΠΝΗ ΚΑΡΤΑ ΠΛΗΡΩΜΗΣ**

Η συγκεκριμένη ανέπαφη έξυπνη κάρτα ενισχύει την εμπιστοσύνη των χρηστών μέσω της οπτικής ανατροφοδότησης. Η ανέπαφη πληρωμή αναπτύσσεται γρήγορα ως ευνοημένη νέα πλατφόρμα πληρωμής, ειδικά σε εκείνα τα τμήματα όπου η ταχύτητα και η ευκολία της πληρωμής είναι ουσιαστικές .Ένω οι ανέπαφες κάρτες πληρωμής παρέχουν τα ίδια οφέλη στους πωλητές και τους καταναλωτές, οι ανησυχίες μεταξύ των καταναλωτών σχετικά με τη μυστικότητα και την οικονομική ασφάλεια μπορεί τελικά να περιορίσουν την υιοθέτηση αυτής της βολικής πλατφόρμας.



ΕΙΚΟΝΑ 86 : Ανέπαφη έξυπνη κάρτα πληρωμής

Η επίδειξη της Aveso , σε μια ανέπαφη κάρτα θα επιτρέψει στο χρήστη να δεί την πληρωμή υπό εξέλιξη ή άλλες πληροφορίες συναλλαγής άμεσα για την ίδια την κάρτα που ενισχύει την εμπιστοσύνη στην ευρεία υιοθέτηση των πλατφορμών.

➢ **Λειτουργία ανέπαφης έξυπνης κάρτας πληρωμής**

1 Ο χρήστης «περνάει» την κάρτα μπροστά από τον αναγνώστη καρτών.
2 Ο χρήστης λαμβάνει την άμεση οπτική ανατροφοδότηση στην κάρτα όπως πιστοποίηση της διαδικασίας της συναλλαγής .

26 ΕΥΡΕΤΗΡΙΟ ΟΡΟΛΟΓΙΑΣ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ [129]

ABS (Acrylonitrile Butadiene Styrene) Ακρυλονιτρικό Βουτανιεδικό Στυρένιο. Το πλαστικό που χρησιμοποιείται για την έγχυση των σκελετών των καρτών για διάφορες κάρτες

Acceptor Αποδοχέας. Ο οργανισμός (συνήθως ένας έμπορος), ο οποίος δέχεται μία κάρτα (για παράδειγμα για μία πληρωμή).

Acquirer Μεσολαβητής συναλλαγών. Η Τράπεζα, η οποία επεξεργάζεται τις συναλλαγές ενός εμπόρου και τις προωθεί στο σύστημα εκκαθάρισης (πχ clearing system). Μπορεί να είναι και ένας οργανισμός ο οποίος διαχειρίζεται την ανταλλαγή πληροφοριών και δεδομένων μεταξύ του διαχειριστή ενός συστήματος πληρωμών και του ατόμου το οποίο παρέχει τις διάφορες υπηρεσίες.

AID Application Identifier. Αναγνωριστικό εφαρμογής. Το AID αναγνωρίζει μία εφαρμογή σε μία έξυπνη κάρτα. Ορίζεται στο πρότυπο ISO/IEC 7816-5. Ένα μέρος του AID μπορεί να κατοχυρώνεται σε εθνικό ή παγκόσμιο επίπεδο. Σε αυτήν την περίπτωση, η εφαρμογή στην οποία αναφέρεται είναι μοναδικά αναγνωρίσιμη.
Το AID αποτελείται από δύο τμήματα: το RID (Registered Identifier) και το PIX (Proprietary Identifier).

ALD (Application Load Certificate) Χρησιμοποιείται από τη προδιαγραφή Multos και παρόμοια συστήματα για την «επισημοποίηση» μιας εφαρμογής που φορτώνεται σε μία κάρτα πολλαπλών εφαρμογών

Algorithm Αλγόριθμος. Μία μαθηματική διαδικασία που χρησιμοποιείται για να γίνουν υπολογισμοί (στην κρυπτογραφία: αλγόριθμος κρυπτογράφησης)

Analog Αναλογικός. Χρησιμοποιείται σε αντιδιαστολή με το «Ψηφιακός»

Anti-collision Αποφυγή σύγκρουσης. Ένας αλγόριθμος που χρησιμοποιείται για την αναγνώριση δύο ή περισσοτέρων ασύρματων έξυπνων καρτών, όταν λειτουργούν ταυτόχρονα.

Anti-tearing Ένα χαρακτηριστικό της κάρτας, το οποίο προστατεύει τα δεδομένα της μνήμης στην περίπτωση που η κάρτα απομακρυνθεί πριν την ολοκλήρωση μίας συναλλαγής.

APDU (Application Protocol Data Unit) Μονάδα δεδομένων Πρωτοκόλλου Εφαρμογής. Είναι ένα «κουτί» δεδομένων λογισμικού, το οποίο χρησιμοποιείται για την ενθυλάκωση των δεδομένων, έτσι ώστε να μπορούν να ανταλλάσσονται ανάμεσα σε μία έξυπνη κάρτα και σε ένα τερματικό.

ASIC (Application-Specific Integrated Circuit) Ολοκληρωμένα Κυκλώματα Ειδικού σκοπού Εφαρμογής. Τα κυκλώματα αυτά ελαχιστοποιούν το κόστος παραγωγής με την υλοποίηση κυκλωμάτων που έχουν όλα τα χαρακτηριστικά της υψηλής τεχνολογίας

Asymmetric Cryptography Ασυμμετρική ή ασύμμετρη κρυπτογραφία (επίσης «κρυπτογραφία δημόσιου κλειδιού». Αναφέρεται στη μέθοδο κρυπτογράφησης όπου υπάρχουν δύο κλειδιά κρυπτογράφησης. Το ένα χρησιμοποιείται για την κρυπτογράφηση του κειμένου και το άλλο για την αποκρυπτογράφηση.

ATC (Application Transaction Counter) Μετρητής ο οποίος υπάρχει μέσα στην κάρτα και αυξάνεται κατά μια μονάδα κάθε φορά που πραγματοποιείται μια συναλλαγή

ATM (Automated Teller Machine) Ειδικό τερματικό, το οποίο τοποθετείται σε δημόσιους χώρους και επιτρέπει την εκτέλεση οικονομικών συναλλαγών.

ATR (Answer To Reset) Είναι μία ακολουθία από byte, η οποία στέλνεται από μία έξυπνη κάρτα μετά από (hardware) επαναφορά. Μεταξύ άλλων περιέχει διάφορες παραμέτρους σχετικά με το πρωτόκολλο μετάδοσης της κάρτας

Authentication Ταυτοποίηση. Η διαδικασία αποδείξεως της γνησιότητας μίας οντότητας (π.χ. έξυπνη κάρτα ή μέσω αυτής του κατόχου της), χρησιμοποιώντας κρυπτογραφικές μεθόδους

External Authentication Εξωτερική Ταυτοποίηση. Η διαδικασία που χρησιμοποιείται για την ταυτοποίηση του «έξω» κόσμου (π.χ. ένα τερματικό) από την έξυπνη κάρτα.

Internal Authentication Εσωτερική Ταυτοποίηση. Η διαδικασία που χρησιμοποιείται για να αποδείξει μία έξυπνη κάρτα ότι είναι γνήσια.

BIP (Bearer Independent Protocol) Πρωτόκολλο το οποίο επιτρέπει σε μια κάρτα SIM να επικοινωνεί απευθείας με απομακρυσμένους εξυπηρετητές

Black list Μαύρη λίστα. Η λίστα, συνήθως σε μία βάση δεδομένων, η οποία περιέχει όλες τις κάρτες που δεν επιτρέπεται πλέον η χρήση τους σε ένα σύστημα

CA (Certification Authority) Αρχή Πιστοποίησης. Ο οργανισμός που εκδίδει πιστοποιητικά και είναι υπόλογος για τις ευθύνες που προκύπτουν από την εγκυρότητα των στοιχείων του κατόχου

CAM (Card Authentication Method) Μέθοδος αυθεντικοποίησης κάρτας. Αυτή η μέθοδος χρησιμοποιείται για να εξακριβωθεί εάν η κάρτα προέρχεται από έγκυρο εκδότη

Card accepter Αποδοχέας καρτών. Οντότητα στην οποία μπορούν να χρησιμοποιηθούν έξυπνες κάρτες για μια συγκεκριμένη εφαρμογή

Card body Σώμα κάρτας. Πλαστική κάρτα, το ενδιάμεσο προϊόν στην κατασκευή της Έξυπνης Κάρτας. Σε επόμενο βήμα της κατασκευής, ενσωματώνεται το ολοκληρωμένο κύκλωμα

Card issuer Εκδότης κάρτας. Οντότητα, υπεύθυνη για την έκδοση έξυπνων καρτών. Συνήθως, ο πάροχος της εφαρμογής και ο εκδότης της κάρτας ταυτίζονται για τις έξυπνες κάρτες μίας εφαρμογής.

Card manufacturer Κατασκευαστής κάρτας. Η οντότητα, που κατασκευάζει σώματα καρτών, ενσωματώνει το ολοκληρωμένο κύκλωμα και ανά εφαρμογή το προγραμματίζει (π.χ. κάρτες μνήμης) ή απλώς το προετοιμάζει για να προγραμματιστεί από άλλη οντότητα.

Card owner Ιδιοκτήτης κάρτας. Είναι η φυσική ή νομική οντότητα που έχει το νόμιμο έλεγχο της κάρτας. Στην περίπτωση των καρτών χρέωσης ή πιστωτικών καρτών, ο ιδιοκτήτης της κάρτας είναι συνήθως η Τράπεζα που εκδίδει την κάρτα. Οι πελάτες που χρησιμοποιούν την κάρτα είναι συνήθως μόνο «κάτοχοι κάρτας» (βλέπε Cardholder).

Card possessor Κύριος κάρτας. Η οντότητα που έχει στην κυριότητά της μία κάρτα

Card reader Συσκευή με σχετικά απλή ηλεκτρική και μηχανική κατασκευή που μπορεί να δεχτεί έξυπνες κάρτες και να αλληλεπιδράσει μαζί τους

Card user Το άτομο που χρησιμοποιεί την κάρτα. Δεν είναι υποχρεωτικά ο νόμιμος κάτοχός της

Cardholder Κάτοχος κάρτας. Αναφέρεται στην οντότητα, η οποία έχει το πραγματικό δικαίωμα κατοχής και χρήσης της κάρτας. Ο κάτοχος της κάρτας δεν είναι αναγκαίο ότι είναι και ο ιδιοκτήτης της κάρτας

Certificate Πιστοποιητικό. Αρχείο ψηφιακά υπογεγραμμένο από μία Αρχή Πιστοποίησης

CEN (Centre European pour la Normalisation – European Standards Centre) Ο ευρωπαϊκός οργανισμός προτύπων CEN αποτελείται από όλους τους (ευρωπαϊκούς) εθνικούς οργανισμούς προτύπων και είναι ο επίσημος οργανισμός της Ευρωπαϊκής Ένωσης για τα ευρωπαϊκά πρότυπα

Challengeresponse, Μέθοδος ταυτοποίησης όπου το σύστημα που απαιτεί ταυτοποίηση στέλνει μία τυχαία «πρόκληση». Το υπό ταυτοποίηση αντικείμενο (π.χ. μία έξυπνη κάρτα) υπολογίζει την «απάντηση» στην «πρόκληση». Το σύστημα μπορεί να επιβεβαιώσει τη γνησιότητα του αντικειμένου με βάση αυτή την «απάντηση».

Chip card Κάρτα με ενσωματωμένο ολοκληρωμένο κύκλωμα. Αναφέρεται επίσης ως «έξυπνη κάρτα», αλλά συχνά χρησιμοποιείται με τέτοιον τρόπο, ώστε να συμπεριλαμβάνει και τις κάρτες μνήμης, οι οποίες δεν έχουν «εξυπνάδα»

Clearing/ Clearance Η διαδικασία διαβίβασης, εναρμόνισης και επιβεβαίωσης εντολών χρηματοπιστωτικών ιδρυμάτων

Clearing system Πληροφοριακό Σύστημα, το οποίο εκτελεί σε κεντρική εφαρμογή διακανονισμούς συναλλαγών μεταξύ χρηματοπιστωτικών ιδρυμάτων ή χρηματοπιστωτικών ιδρυμάτων και τρίτων

Cloning Κλωνοποίηση. Προσπάθεια «επίθεσης» σε σύστημα έξυπνων καρτών, με την αντιγραφή της μνήμης ROM και EEPROM μίας γνήσιας σε μία πλαστή κάρτα

CMS (Card Management System) Εργαλεία και διαδικασίες που χρησιμοποιούνται για την ανάπτυξη και διαχείριση εφαρμογών έξυπνων καρτών. Το CMS χρησιμοποιείται κυρίως για την διαχείριση του κύκλου ζωής των καρτών και των εφαρμογών τους

COS (Chip Operating System/Mask) Ακολουθία ενσωματωμένων εντολών, στη μνήμη ROM της έξυπνης κάρτας

Confidentiality Εμπιστευτικότητα. Αναφέρεται στις μεθόδους και διαδικασίες, που διασφαλίζουν ότι οι πληροφορίες είναι προσβάσιμες μόνο από τις οντότητες στις οποίες επιτρέπεται να έχουν πρόσβαση

Combination Card Συνδυασμένη Κάρτα. Έξυπνη κάρτα, η οποία συνδυάζει και τις δύο τεχνολογίες (με επαφές και ασύρματη)

Contact Smart Card Έξυπνη Κάρτα με Επαφές. Έξυπνη κάρτα, η οποία απαιτεί τη φυσική επαφή με τη συσκευή ανάγνωσης, ώστε να ανταλλάξουν δεδομένα

Contactless Smart Card Χωρίς επαφές ή Ασύρματη Έξυπνη Κάρτα. Αναφέρεται σε έξυπνες κάρτες, οι οποίες μεταδίδουν και λαμβάνουν δεδομένα χρησιμοποιώντας ραδιοσυχνότητες

Coupler Ηλεκτρονικό σύστημα - εφαρμογή που χρησιμοποιείται για να μπορεί να διαβάζει την συνήθως ασύρματη έξυπνη κάρτα

CQL (Card Query Language) Υποσύνολο της SQL (Structured Query Language) που έχει υλοποιηθεί πάνω σε έξυπνη κάρτα

CRC (Cyclic Redundancy Check) Μέθοδος ορθής μεταφοράς των δεδομένων

Cryptography Κρυπτογραφία. Η επιστήμη και η τέχνη της μετατροπής συμβολοσειρών (π.χ. κειμένων, αριθμοσειρών κλπ) σε ακατανόητες μορφές, για όσους δεν έχουν τον κατάλληλο μηχανισμό επαναφοράς στην αρχική μορφή (κλειδί)

CVM (Cardholder Verification Method) Μέθοδος Επιβεβαίωσης Κατόχου Κάρτας

DDA (Dynamic Data Authentication) Μέθοδος πιστοποίησης της κάρτας χρησιμοποιώντας μηχανισμό ανταπόκρισης

DF (Dedicated File) Οργάνωση της μνήμης για τις κάρτες με μικροεπεξεργαστή. Ένα DF είναι μία λογική οντότητα, η οποία αποτελείται από EF (elementary file)

Diffie- Hellman Οι εφευρέτες της κρυπτογραφίας δημόσιου κλειδιού

Digital Cash (e- Cash) Είναι ψηφιακό χρήμα που μπορεί να αποθηκεύεται σε τραπεζικό λογαριασμό, προσωπικό υπολογιστή ή έξυπνη κάρτα

Dual Slot Διπλή Θυρίδα. Αναγνώστης έξυπνων καρτών που μπορεί να χρησιμοποιήσει 2 έξυπνες κάρτες ταυτόχρονα. Χρησιμοποιείται σε συστήματα πληρωμών, για την ταυτοποίηση στην Τράπεζα τόσο του εμπόρου όσο και του πελάτη

Dual Interface Card (Combicard) Έξυπνη Κάρτα, η οποία έχει δύο μέσα επικοινωνίας: ενσύρματη, μέσω ηλεκτρομηχανικών επαφών και ασύρματη επικοινωνία, μέσω κατάλληλης κεραίας

Duplication (Cloning) Μεταφορά πρωτότυπων δεδομένων σε μία δεύτερη κάρτα με σκοπό την δημιουργία μιας πανομοιότυπης κάρτας

e-Cash Ψηφιακό /Ηλεκτρονικό Χρήμα, που μπορεί να αποθηκεύεται σε τραπεζικό λογαριασμό, προσωπικό υπολογιστή ή έξυπνη κάρτα

ECC Error Correction Code.Ένας Κώδικας Διόρθωσης Λαθών εντοπίζει σφάλματα στα δεδομένα, τα οποία σε πολλές περιπτώσεις μπορεί να διορθώσει

EEPROM (Electrically Erasable Programmable Read-Only Memory) Τύπος μνήμης ROM που μπορεί να επαναπρογραμματιστεί με την εφαρμογή κατάλληλου ηλεκτρικού πεδίου

EF (Elementary File) Στοιχειώδες Αρχείο. Μέρος της λογικής οργάνωσης της μνήμης μίας κάρτας με μικροεπεξεργαστή, το ανάλογο ενός αρχείου δεδομένων

Embedding Ενσωμάτωση. Η διαδικασία ενσωμάτωσης ενός ολοκληρωμένου κυκλώματος στο σώμα μίας έξυπνης κάρτας.

EMV (Europay – Mastercard – Visa) Μία σειρά από διεθνή πρότυπα για πληρωμές βασισμένες σε έξυπνες κάρτες, τα οποία αναπτύχθηκαν από τους οργανισμούς Europay, Mastercard και Visa

Encryption Κρυπτογράφηση. Η διαδικασία μετασχηματισμού συμβολοσειράς σε ακατάληπτη μορφή, χρησιμοποιώντας ένα κατάλληλο κλειδί

ETU (Elementary Time Unit) Βασική Μονάδα Χρόνου. Η βασική μονάδα χρόνου της έξυπνης κάρτας, στην οποία βασίζονται όλοι οι χρονισμοί επικοινωνίας της κάρτας. Ορίζεται ως ο χρόνος μεταφοράς ενός bit δεδομένων από μία έξυπνη κάρτα

Fabrication Η διαδικασία κατασκευής του ολοκληρωμένου κυκλώματος της έξυπνης κάρτας

Filtered Φιλτραρισμένος. Χαρακτηρισμός για δεδομένα ή λειτουργίες τα οποία έχουν φορτωθεί στην μνήμη της έξυπνης κάρτας

Flash Memory Μνήμη στην οποία μπορεί να γίνει εγγραφή μία φορά αλλά για να γίνει διαγραφή της, θα πρέπει να γίνει διαγραφή του αντίστοιχου block

FRR (False Reject Rate) Μονάδα μέτρησης εσφαλμένης απόρριψης μίας οντότητας σε ένα σύστημα. Χρησιμοποιείται κύρια στα συστήματα βιομετρικής

GSM (Global System for Mobile communications, Group Speciale de Mobile) Σύστημα κυψελοειδούς τηλεφωνίας με ευρεία διάδοση στην Ευρώπη

Garbage Collection Λειτουργία έξυπνης κάρτας τύπου Java Card, η οποία συλλέγει τη μνήμη που δε χρησιμοποιείται πλέον από μία εφαρμογή και τη μετατρέπει σε ελεύθερη μνήμη προς χρήση από άλλες εφαρμογές

Hard Mask Σε μία έξυπνη κάρτα με hard mask το μεγαλύτερο κομμάτι του κώδικα του προγράμματος υλοποιείται στη μνήμη ROM

HSM (Host Security Module) Συσκευή, η οποία χρησιμοποιείται για την ασφαλή αποθήκευση κλειδιών και την (εσωτερική) εκτέλεση κρυπτογραφικών λειτουργιών, καθοδηγούμενη από έναν υπολογιστή

Hybrid Card Υβριδική Κάρτα. Τύπος έξυπνης κάρτας που χρησιμοποιεί δύο διαφορετικά μέσα επικοινωνίας. βλέπε **Dual Interface Card**

ID-I card Έξυπνη Κάρτα με προτυποποιημένες κατά ISO διαστάσεις.

IFD (Interface Device) Άλλη ονομασία του αναγνώστη έξυπνης κάρτας

Initialization Το πρώτο στάδιο της διαδικασίας έκδοσης καρτών. Ο σκοπός αυτής της διαδικασίας είναι το φόρτωμα των δεδομένων από την εφαρμογή στις έξυπνες κάρτες

Intelligent memory card Ευφυής κάρτα μνήμης. Κάρτα μνήμης με συμπληρωματικό λεπτομερές λογικό σχέδιο κυκλώματος που επιτρέπει/ παρέχει επιπρόσθετες λειτουργίες ασφαλείας που καταγράφουν τη χρήση της μνήμης

Integrity Ακεραιότητα. Αναφέρεται στις μεθόδους και διαδικασίες που διασφαλίζουν ότι οι πληροφορίες έχουν τροποποιηθεί μόνο από τις οντότητες που έχουν την αντίστοιχη εξουσιοδότηση

Interoperability Διαλειτουργικότητα. Η δυνατότητα συστημάτων διαφορετικών κατασκευαστών να αλληλεπιδρούν μεταξύ τους.

ISO (International Standards Organization) Ο οργανισμός ISO μεταξύ άλλων εργάζεται στην περιοχή των έξυπνων καρτών, με σκοπό να εξασφαλίσει, μέσω των προτύπων που ορίζει, ότι οι κατασκευαστές των ολοκληρωμένων κυκλωμάτων, οι προγραμματιστές και οι εταιρείες έξυπνων καρτών ακολουθούν τις ίδιες προδιαγραφές

ITSO (Integrated Transport Smart Card Organisation) Οργανισμός ο οποίος ιδρύθηκε στο Ηνωμένο Βασίλειο για να βοηθήσει την εξάπλωση των συστημάτων έξυπνων καρτών στα μέσα μαζικής μεταφοράς.

ITU (International Telecommunications Union) Οργανισμός που συντονίζει, προτυποποιεί και δημιουργεί παγκοσμίως τηλεπικοινωνιακές υπηρεσίες

Java Card Μία προδιαγραφή για την εκτέλεση ενός υποσυνόλου της γλώσσας Java σε μία έξυπνη κάρτα

JCRE (Java Card Runtime Environment) Το περιβάλλον εκτέλεσης στο οποίο εκτελείται η Java Card. Το JCRE είναι υπεύθυνο για όλες τις διαχειριστικές ενέργειες, όπως η φόρτωση και η αρχικοποίηση των εφαρμογών

Key management Διαχείριση κλειδιών. Όλες οι διαχειριστικές λειτουργίες που σχετίζονται με την δημιουργία, διανομή, αποθήκευση, ενημέρωση των κρυπτογραφικών κλειδιών

Key escrow Η μέθοδος κατάθεσης του ιδιωτικού κλειδιού σε τρίτον, συνήθως για τη διασφάλιση της ανάκτησης των δεδομένων τα οποία έχουν κρυπτογραφηθεί ή υπογραφεί με το ιδιωτικό κλειδί. Η κατάθεση του ιδιωτικού κλειδιού, ειδικά στην περίπτωση της χρήσης για ηλεκτρονικές υπογραφές, απαγορεύεται στις περισσότερες έννομες τάξεις.

Lifecycle Κύκλος ζωής. Αναφέρεται στα στάδια επεξεργασίας και λειτουργίας μίας έξυπνης κάρτας, από τη στιγμή της κατασκευής του ολοκληρωμένου κυκλώματος της, έως την απόσυρση από τη χρήση και καταστροφή της

MAC (Message Authentication Code)Κώδικας ταυτοποίησης μηνύματος-Διαδικασία, συνήθως με τη χρήση αλγόριθμων κρυπτογράφησης, η οποία εγγυάται ότι το μήνυμα προέρχεται από τον πρωτότυπο παραλήπτη του και δεν έχει αλλαχθεί στην πορεία

Magnetic Strip Card Κάρτα με μαγνητική λωρίδα, πάνω στην οποία δεδομένα μπορεί να καταχωρηθούν και να διαβαστούν

Memory card Κάρτα μνήμης. Αναφέρεται σε κάρτες που περιέχουν μόνο μνήμη και επιλεκτικά και λογική ενσωματωμένη στο υλικό (hardwired logic). Χρησιμοποιείται σε αντιδιαστολή με τον όρο chip card ή smart card, όπου υποδηλώνεται η ικανότητα επεξεργασίας

MF (Master File) Αποτελεί το βασικό κατάλογο του δένδρου αρχείων που υλοποιεί τη λογική οργάνωση της μνήμης μίας έξυπνης κάρτας. Το Κύριο Αρχείο επιλέγεται αυτόματα κάθε φορά που εκκινεί η έξυπνη κάρτα

Microprocessor Card Κάρτα με μικροεπεξεργαστή. Κάρτα η οποία περιλαμβάνει: επεξεργαστή (CPU), μνήμης (RAM, ROM, EEPROM) και επιλεκτικά αριθμητικό συνεπεξεργαστή (NPU, numerical coprocessor), κάτι που επιτρέπει την άμεση εκτέλεση των αλγορίθμων. Χρησιμοποιείται σε αντιδιαστολή με τον όρο «Κάρτα Μνήμης» (Memory Card).

Mono-application smart card Έξυπνη κάρτα μοναδικής εφαρμογής. Κάρτα που έχει τη δυνατότητα να εκτελέσει μία μόνο εφαρμογή, συνήθως προεγκατεστημένη σε αυτή

Mono-functional smart card Έξυπνη κάρτα μοναδικής λειτουργίας. Κάρτα της οποίας το λειτουργικό σύστημα υποστηρίζει μόνο μια συγκεκριμένη εφαρμογή

Multi-application smart card Έξυπνη κάρτα πολλαπλών εφαρμογών.Αναφέρεται σε έξυπνες κάρτες νεότερης γενιάς , οι οποίες έχουν τη δυνατότητα να εκτελούν πολλαπλές εφαρμογές, από διαφορετικούς κατασκευαστές, σε αντίθεση με τις προηγούμενες, οι οποίες εκτελούσαν εφαρμογές ενός μόνο κατασκευαστή

Multi-functional smart card Κάρτα της οποίας το λειτουργικό σύστημα υποστηρίζει παραπάνω από μια εφαρμογές και περιέχει κατάλληλες λειτουργίες διαχείρισης για την εγγραφή και διαγραφή εφαρμογών και αρχείων

μP card Διαφορετική ονομασία για την κάρτα με μικροεξεργαστή. Βλέπε. Microprocessor card

Non-Volatile Memory Ευσταθής μνήμη. Αναφέρεται σε μνήμες, οι οποίες διατηρούν τα δεδομένα τους, όταν διακοπεί η τροφοδοσία τους (όπως για παράδειγμα τα δεδομένα που είναι αποθηκευμένα στη μνήμη μίας έξυπνης κάρτας)

Numbering Αρίθμηση. Είναι η διαδικασία χάραξης αριθμών πάνω στις έξυπνες κάρτες

OCF (OpenCard Framework) Αρχιτεκτονική για κάρτες και τερματικά που έχει σκοπό την τυποποίηση των τερματικών εφαρμογών

Open application Εφαρμογή μέσα στην έξυπνη κάρτα που την κάνει διαθέσιμη σε ποικίλους παρόχους υπηρεσιών, χωρίς να είναι απαραίτητη η αμοιβαία νομική σχέση μεταξύ τους

Optical memory card Οπτική κάρτα μνήμης. Κάρτα, στην οποία οι πληροφορίες έχουν εγγραφεί σε μία ανακλαστική επιφάνεια με οπτικό τρόπο, παρόμοια με τη λειτουργία των CD.

OSI (Open Systems Interconnection) Μοντέλο του οργανισμού ISO για τις επικοινωνίες

PAC (PIN Authentication Code) Κωδικός Πιστοποίησης Προσωπικού Μυστικού Κωδικού

Padding Μία μέθοδος, σύμφωνα με την οποία ένα ή περισσότερα bit προστίθενται σε ένα μήνυμα, ώστε να αποκτήσει το απαιτούμενο μέγεθος

Passivation layer Στρώμα αδρανοποίησης. Ένα υλικό που καλύπτει το ολοκληρωμένο κύκλωμα της κάρτας, ώστε να είναι ανθεκτικότερη στις επιδράσεις του εξωτερικού περιβάλλοντος

PCC (Proof-carrying code) Κώδικας ο οποίος περιλαμβάνει την απόδειξη συμβατότητας με δεδομένη πολιτική ασφάλειας

PC/SC Αρχιτεκτονική επικοινωνίας τερματικών και έξυπνων καρτών. Το PC/SC προτάθηκε από την εταιρεία Microsoft και άλλους κατασκευαστές έξυπνων καρτών και προσωπικών υπολογιστών με σκοπό την προτυποποίηση των διεπαφών υλικού και λογισμικού των έξυπνων καρτών για την επικοινωνία με προσωπικούς υπολογιστές

PKCS (Public-Key Cryptography Standards) Ανεπίσημα πρότυπα που αφορούν στην κρυπτογραφία δημόσιου κλειδιού. Έχουν δημοσιευθεί από την εταιρεία RSA Inc

PKI (Public Key Infrastructure) Υποδομή Δημόσιου Κλειδιού. Εφαρμόζεται στην περίπτωση της ασύμμετρης κρυπτογράφησης και αναφέρεται στην ύπαρξη ενός ζευγαριού κλειδιών, του δημόσιου και ιδιωτικού) για την ασφάλεια των δεδομένων. Αποτελείται από κατάλληλο λογισμικό και υλικό.

Plug-In Έξυπνη κάρτα με μικρό σχήμα και διάταξη που χρησιμοποιείται κυρίως για τα κινητά τηλέφωνα

Processor card Βλέπε Microprocessor card

PVC (Polyvinyl Chloride) Χλωριούχο Πολυβινύλιο. Το πλαστικό από το οποίο κατασκευάζεται το σώμα της έξυπνης κάρτας

RAM (Random Access Memory) Μνήμη Τυχαίας Προσπέλασης

RISC (Reduced Instruction Set Computer) Μία αρχιτεκτονική σχεδίασης υπολογιστών

Retry Counter Μετρητής Προσπαθειών. Μετρητής, ο οποίος συγκεντρώνει αρνητικές προσπάθειες/ αποτελέσματα και αποφασίζει αν κάποιο κλειδί θα συνεχίσει να χρησιμοποιείται ή όχι. Αν ο καταμετρητής φτάσει στον μέγιστο αριθμό ανεπιτυχών προσπαθειών τότε το κλειδί απενεργοποιείται και δεν μπορεί πλέον να χρησιμοποιηθεί

ROM (Read Only Memory) Μνήμη Ανάγνωσης Μόνο. Ένας τύπος μνήμης, όπου τα δεδομένα που αρχικά έχουν εγγραφεί μπορούν μόνο να προσπελαστούν

RSA (Rivest-Shamir-Adleman) Αλγόριθμος κρυπτογράφησης δημόσιου κλειδιού, ο οποίος πήρε το όνομά του από τους τρεις εφευρέτες του, τους Rivest, Shamir και Adleman

SAM (Security Access Module) Άρθρωμα, το οποίο χρησιμοποιείται σαν τμήμα ενός τερματικού για την ασφαλή αποθήκευση κλειδιών και αλγορίθμων

SDA (Static Data Authentication) Η μέθοδος ταυτοποίησης μίας κάρτας μέσω της ψηφιακής υπογραφής ενός αντιγράφου από επιλεγμένα δεδομένα της κάρτας

Secret Key Μυστικό κλειδί. 1. Το κλειδί στην κρυπτογράφηση δημόσιου κλειδιού που πρέπει να παραμείνει μυστικό. 2. Το κλειδί στην κρυπτογράφηση συμμετρικού κλειδιού. Και σε αυτήν την περίπτωση, το κλειδί πρέπει να παραμείνει μυστικό

Session Συνεδρία. Αναφέρεται στο χρόνο μεταξύ δύο reset μίας κάρτας ή στο χρόνο μεταξύ της τροφοδότησης (power up) και της διακοπής τροφοδοσίας (power down)

SET (Secure Electronic Transaction) Ασφαλής Ηλεκτρονική Συναλλαγή. Πρωτόκολλο που αναπτύχθηκε από τη MasterCard και τη Visa για την κρυπτογραφημένη αποστολή αριθμών πιστωτικών καρτών μέσω του Διαδικτύου (Internet). Σύμφωνα με το SET, ο έμπορος δε μαθαίνει ποτέ τον αριθμό της πιστωτικής κάρτας, περιορίζοντας έτσι τον κίνδυνο της απάτης

SHA-1 (Secure Hash Algorithm 1) Πρότυπο του οργανισμού NIST των Η.Π.Α., το οποίο αναφέρεται στη δημιουργία κρυπτογραφικά ασφαλών κερμάτων (μικρών δεδομένων) από μεγαλύτερο σύνολο δεδομένων

Signed Applets Υπογεγραμμένες Εφαρμογές. Αναφέρεται σε εφαρμογές Java ή Java Card, οι οποίες συνοδεύονται από ψηφιακή υπογραφή. Η υπογραφή αυτή αποδεικνύει την ταυτότητα του κατασκευαστή της εφαρμογής ή του διανομέα της

SIM (Subscriber Authentication Module) Άρθρωμα Ταυτοποίησης Συνδρομητή

SMG9 (Special Mobile Group 9) Ομάδα ειδικών που καθορίζει τις προδιαγραφές των αλληλεπιδράσεων μεταξύ έξυπνων καρτών και κινητών τηλεφώνων

Super Smart Card Υποδηλώνει μία έξυπνη κάρτα με ενσωματωμένα πολύπλοκα στοιχεία, όπως για παράδειγμα οθόνη απεικόνισης και αριθμητικό πληκτρολόγιο

SVC (Stored-Value-Cards) Όρος που χρησιμοποιείται για τις προπληρωμένες κάρτες που έχουν προκαθορισμένη αξία και χρησιμοποιούνται μέχρι εξάντλησης της αξίας αυτής

TASI (Terminal Application Services Interface) Ο τρόπος με τον οποίο μια εφαρμογή διασυνδέεται με τον «έξω κόσμο»

TC (Transaction Certificate) Πιστοποιητικό Συναλλαγής

TTP (Trusted Third Party) Έμπιστη Τρίτη Οντότητα

Transfer Κάρτα μετακίνησης. Είναι μία έξυπνη κάρτα, η οποία χρησιμοποιείται ως μέσο μεταφοράς δεδομένων μεταξύ δύο οντοτήτων. Συνήθως περιέχει μία μεγάλη μνήμη δεδομένων για αυτό το σκοπό και τυπικά περιέχει κλειδιά για την ταυτοποίηση των οντοτήτων και των ενεργειών τους (ανάγνωση/ εγγραφή δεδομένων)

Transmission Protocol Πρωτόκολλο Μετάδοσης. Το σύνολο των κανόνων μετάδοσης που χρησιμοποιούνται για την μεταφορά δεδομένων μεταξύ τερματικού και έξυπνων καρτών

Verifier Εφαρμογή η οποία επεξεργάζεται τον εισερχόμενο κώδικα και διασφαλίζει την συμβατότητά του με τις προβλεπόμενες προδιαγραφές ασφάλειας

Virgin Card Κάρτα στην οποία δεν υπάρχει ακόμα ο μικροεπεξεργαστής και δεν έχει ακόμα προσωποποιηθεί

Volatile Memory Ασταθής μνήμη. Αναφέρεται σε μνήμες, οι οποίες χάνουν τα δεδομένα τους, όταν διακοπεί η τροφοδοσία τους (όπως η μνήμη RAM ενός προσωπικού υπολογιστή)

VOP (Visa Open Platforms) Πολυσήμαντο σύστημα αρχιτεκτονικής το οποίο επιτρέπει την ταχεία ανάπτυξη παγκόσμιων πρακτικών συστημάτων έξυπνων καρτών

White List Λευκή λίστα. Η λίστα, συνήθως σε βάση δεδομένων, η οποία περιέχει όλες τις κάρτες που επιτρέπεται η χρήση τους σε ένα συγκεκριμένο σύστημα

WORM (Write Once Read Many) Αναφέρεται στην μνήμη των έξυπνων καρτών που μπορεί να γίνει εγγραφή στην κάρτα μόνο μία φορά και να διαβαστεί πολλές

27 ΣΧΕΤΙΚΟΙ ΣΥΝΔΕΣΜΟΙ ΓΙΑ ΤΑ ΣΥΣΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ ΚΑΙ ΤΙΣ ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ [130]

27.1 ΣΧΕΤΙΚΟΙ ΣΥΝΔΕΣΜΟΙ ΓΙΑ ΤΑ ΣΥΣΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ

- **Πιστωτικές κάρτες**

American Express
Europay
MasterCard
VISA

- **Ψηφιακά πιστοποιητικά**

Baltimore Technologies
CyberTrust
Digital Signature Trust Company
EuTrust
ICE-TEL
NetDox
Pisces
Ubisecure
VeriSign

- **Ηλεκτρονικά μετρητά**

Chipper
Cybercash
DigiCash
MilliCent (Digital)
MONDEX
OKI Labs
Proton World
VISA Cash

- **Συστήματα πληρωμής Διαδικτύου**

GlobeSet
eConnect
Trintech

- **Εξασφαλίστε τα περιβάλλοντα**

Cylink
Secure Solutions Experts
Security First Technologies
Ubisecure Software

Virtual Open Network Environment (V-ONE)

- **Πρότυπα**

ELAN (Emulated Local Area Network)
IEEE Group Bandwidth Quantum LLC
Open Transport Protocol

27.2 ΣΧΕΤΙΚΟΙ ΣΥΝΔΕΣΜΟΙ ΓΙΑ ΤΙΣ ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ

- **Κατασκευαστές ολοκληρωμένου κυκλώματος**

Advanced Logic Corporation
Atmel
Dallas Semiconductor
Hewlett Packard (HP), Hewlett (Brand)
Intel Corporation
Microchip
Motorola
OKI Semiconductor
Philips
Siemens Electronics
Siemens Semiconductor
STMicroelectronics
Xilinx (Reseller : Siemens)

- **Κατασκευαστές έξυπνων καρτών**

AMD (American Microdevice Manufacturing Inc.)
Bull CP8
Card Logix
Dirl Card
Gemplus
Giesecke & Devrient
IBM Smart Cards
Ink Technologies
Microchip
Motorola
NEC Technologies Inc.
Siemens Card Systems
Sony
Orga
Panasonic Electronics
Schlumberger
Toshiba

- **Κατασκευαστές τερματικών**

Advanced Card Systems
Amphenol Tuchel Electronics

- **Ολοκληρωτής έξυπνων καρτών**

NEC Technologies Inc.
MUSCLE (Movement for the Use of Smart Cards in a Linux Environment)
Orga
Racom Systems
SmartMove
Spyrus
Treviso Citycard
Utimaco
Vasco Data Security
VeriFone
ZeitControl Cardsystems

➢ **Λογισμικό έξυπνων καρτών (OS, εφαρμογές, πρόσβαση)**

3GI
Advanced Card Systems
Aladdin Smartcard Environment (ASE)
Amdahl SmartCard Group
AMMI (American Microdevice Manufacturing, Inc.)
Basic Card
CrypTEC
Dong Sung Inforcomm (DSI)
ELEA CardWare
EximSoft
Helwett-Packard
ICC Solutions
Integri
Litronic
Microsoft
Motorola
SCM Microsystems
The Card Explorer

➢ **Οργανώσεις**

Card Europe
Global Chipcard Alliance
International Card Manufacturers Association
JavaCard Forum
SmartCard Developers Association
Smart Card Industry Association
The Smart Card Club
The SmartCard Forum

➢ **Πρότυπα**

Multos
EMV (Europay-Mastercard-Visa) Specifications
JavaCard
OpenCard

[1] Διαθέσιμο στο [ΣΕΛ.: 9-10]
Έ Κύκλος Εργασιών : Ομάδα εργασίας Ε3 – Ηλεκτρονικές πληρωμές : προβλήματα και προοπτικές
Αρχείο : OE3_TelikoParadoteo 2004.

[2] Διαθέσιμο στο Soramäki, K. & Hanssens, B. (2003). E-payments: What are they and what makes them different?. ePSO Discussion Starterl No1

[3] Συρμακέσης, Σ. (2003). Όλα όσα θέλατε να μάθετε για τις ηλεκτρονικές πληρωμές και εισπράξεις Δελτίο ΕΕΤ, Γ΄ Τριμηνία, σελ. 27-55.

[4] Διαθέσιμο στο .
Goldfinger, C. (1999). Secure electronic payments on the Internet

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

[6] Διαθέσιμο στο
[ΣΕΛ.: 11-14]
Αρχειο 143: Ηλεκτρονικό Εμπόριο και Ηλεκτρονική Τραπεζική, Χριστίνα Καλεμικεράκη

[7] Διαθέσιμο στο [ΣΕΛ.:14-16]
Έ Κύκλος Εργασιών : Ομάδα εργασίας Ε3 – Ηλεκτρονικές πληρωμές : προβλήματα και προοπτικές
Αρχείο : OE3_TelikoParadoteo 2004.

[8] Διαθέσιμο στο
Peirce, M. (2001). Payment mechanisms designed for the Internet. .

[9] Διαθέσιμο στο .
Ensor, B.; Torris, T.; Fagerström, M. & Martinez, N. (June 2003). New payment systems' survival guide. TeckStrategy Report, Forrester

[10] Διαθέσιμο στο
Goldfinger, C. (1999). Secure electronic payments on the Internet

[11] 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.

[12] Διαθέσιμο στο [ΣΕΛ.: 16]
Έ Κύκλος Εργασιών : Ομάδα εργασίας Ε3 – Ηλεκτρονικές πληρωμές : προβλήματα και προοπτικές
Αρχείο : OE3_TelikoParadoteo 2004.

[13] Διαθέσιμο στο Αρχείο : DT2004-0034.pdf [ΣΕΛ.: 16-17]

[14] Διαθέσιμο στο Αρχείο : Teachers training e-commerce [ΣΕΛ. : 18-19]

[15] Διαθέσιμο στο [ΣΕΛ.: 19-20]
Έ Κύκλος Εργασιών : Ομάδα εργασίας Ε3 – Ηλεκτρονικές πληρωμές : προβλήματα και προοπτικές
Αρχείο : OE3_TelikoParadoteo 2004.

[16]Διαθέσιμο στο
European Central Bank (16/10/2002). E-payments in Europe – The eurosystem's perspective

[17] Διαθέσιμο στο
European Central Bank (16/10/2002). E-payments in Europe – The eurosystem's perspective

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

[19] Διαθέσιμο στο
European Central Bank (16/10/2002). E-payments in Europe – The eurosystem's perspective

[20] Διαθέσιμο στο
Παπαναγιώτου, Ν.: Internet – Επιχείρηση.

[21] Διαθέσιμο στο Αρχείο : Teachers training e-commerce [ΣΕΛ. : 21]

[22] για περαιτέρω πληροφορίες της ενότητας 2.2.1 [ΣΕΛ. : 21-30] θα βρείτε στοιχεία στο Αρχείο : η επιχειρειν ηλεκτρονικές πληρωμές συχνές ερωταποκρίσεις και στο Αρχείο : τα πραγματικα προβλήματα από τη χρήση των πιστωτικών καρτών στο διαδίκτυο και στο πληροφορίες για τις πιστωτικές κάρτες

[23] Διαθέσιμο στο Αρχείο : DT2004-0034.pdf [ΣΕΛ.: 26-27]

[24] Διαθέσιμο στο [ΣΕΛ.: 30-31]
Έ Κύκλος Εργασιών : Ομάδα εργασίας Ε3 – Ηλεκτρονικές πληρωμές : προβλήματα και προοπτικές
Αρχείιο : OE3_TelikoParadoteo 2004.

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

[26] Διαθέσιμο στο
European Central Bank (16/10/2002). E-payments in Europe – The eurosystem's perspective

[27] Διαθέσιμο στο Αρχείο : Teachers training e-commerce [ΣΕΛ.: 31-32]

[28] Διαθέσιμο στο [ΣΕΛ.: 32-34]
Έ Κύκλος Εργασιών : Ομάδα εργασίας Ε3 – Ηλεκτρονικές πληρωμές : προβλήματα και προοπτικές
Αρχείιο : OE3_TelikoParadoteo 2004.

[29] Διαθέσιμο στο
European Central Bank (16/10/2002). E-payments in Europe – The eurosystem's perspective

[30] για περαιτέρω πληροφορίες της ενότητας 2.3.1 [ΣΕΛ. : 35-41] θα βρείτε στοιχεία στο Αρχείο : Ερωτήσεις και απαντήσεις για τη επιχειρηματική χρήση Ιντερνετ και στο Αρχείο : η επιχειρειν ηλεκτρονικές πληρωμές συχνές ερωταποκρίσεις

[31] Διαθέσιμο στο [ΣΕΛ.: 41-43]
Έ Κύκλος Εργασιών : Ομάδα εργασίας Ε3 – Ηλεκτρονικές πληρωμές : προβλήματα και προοπτικές
Αρχείιο : OE3_TelikoParadoteo 2004.

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

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

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

[35] Διαθέσιμο στο # 3.7 [ΣΕΛ. : 44-45]

[36] Διαθέσιμο στο # 3.8 [ΣΕΛ. : 46-48]

[37] Διαθέσιμο στο # 3.9 [ΣΕΛ. : 48-53]

[38] Διαθέσιμο στο [ΣΕΛ.: 53-54]
Έ Κύκλος Εργασιών : Ομάδα εργασίας Ε3 – Ηλεκτρονικές πληρωμές : προβλήματα και προοπτικές
Αρχείο : OE3_TelikoParadoteo 2004

[39] Διαθέσιμο στο [ΣΕΛ. : 55-56]

[40] Διαθέσιμο στο [ΣΕΛ.: 57-59]
Έ Κύκλος Εργασιών : Ομάδα εργασίας Ε3 – Ηλεκτρονικές πληρωμές : προβλήματα και προοπτικές
Αρχείο : OE3_TelikoParadoteo 2004.

[41] Διαθέσιμο στο
Ensor, B., Torris, T., Fagerström, M. & Martínez, N. (June 2003). New Payment Systems' Survival Guide. Techstrategy Report.

[42] Διαθέσιμο στο
Reitsma, R., Pearce, F. & de Montigny, E. (May 2002). Seeing Beyond Credit Card Payment Online. Brief

[43] Διαθέσιμο στο
Jennings, R.U., O'Connell, P. & Bradford, N. (September 2001). Making Content Pay. Techstrategy Report

[44] Ensor, B., Torris, T., Fagerström, M. & Martínez, N. (June 2003). New Payment Systems' Survival Guide. Techstrategy Report.

[45] Διαθέσιμο στο [ΣΕΛ.: 60-65]
Έ Κύκλος Εργασιών : Ομάδα εργασίας Ε3 – Ηλεκτρονικές πληρωμές : προβλήματα και προοπτικές
Αρχείο : OE3_TelikoParadoteo 2004.

[46] Πληροφορίες για το συγκεκριμένο προϊόν αντλήθηκαν από την ιστοσελίδα της Εγνατίας Τράπεζας, , καθώς και από δημοσιεύματα στο τύπο.

[47] Ημερησία (31/12/2003-4/1/2004). Τράπεζες: Ηλεκτρονικό εμπόριο α λα καρτ. Ένθετο Net Economy, σελ. 155.

[48] 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. .Δαθέσιμο στο

[49] Η ευρωπαϊκή και ελληνική νομοθεσία σε θέματα ηλεκτρονικών πληρωμών είναι επίσης διαθέσιμη σε ηλεκτρονική μορφή στην ιστοσελίδα του προγράμματος «Δικτυωθείτε» του Υπουργείου Ανάπτυξης, , . [ΣΕΛ.: 66-79]
Περαιτέρω πληροφορίες θα βρείτε επίσης στο ( ). Και στο
Έ Κύκλος Εργασιών : Ομάδα εργασίας Ε3 – Ηλεκτρονικές πληρωμές : προβλήματα και προοπτικές
Αρχείο : OE3_TelikoParadoteo 2004

[50] Ενδεικτικός κατάλογος νομοθεσίας για τις ηλεκτρονικές συναλλαγές. Ebusiness Forum, σελ 1.

[51] Το πλήρες κείμενο των ευρωπαϊκών νομοθετημάτων που παρουσιάζονται σε αυτή την ενότητα μπορεί να βρεθεί στην ιστοσελίδα της Ευρωπαϊκής Ένωσης ( ).
Η ευρωπαϊκή και ελληνική νομοθεσία σε θέματα ηλεκτρονικών πληρωμών είναι επίσης διαθέσιμη σε ηλεκτρονική μορφή στην ιστοσελίδα του προγράμματος «Δικτυωθείτε» του Υπουργείου Ανάπτυξης, , και στην ιστοσελίδα του Εμπορικού και Βιομηχανικού Επιμελητηρίου Αθηνών, .

[52]Ενδεικτικός κατάλογος νομοθεσίας για τις ηλεκτρονικές συναλλαγές. Ebusiness Forum, σελ 2.

[53] European Central Bank (16/09/2002). E-Payments in Europe: The Eurosystem's Perspective.

---

[54]Γκόρτσος, Χ. Βλ. (2002). Ο Κανονισμός 2560/2001 σχετικά με τις διασυνοριακές πληρωμές σε ευρώ .Δελτίο ΕΕΤ, Α΄ Τριμηνία, σελ. 40-49.

[55] Law Net S.A.

[56] Διαθέσιμο στο [ΣΕΛ.: 80]
Έ Κύκλος Εργασιών : Ομάδα εργασίας Ε3 – Ηλεκτρονικές πληρωμές : προβλήματα και προοπτικές
Αρχείο : OE3_TelikoParadoteo 2004.

[57] OECD Information Technology Outlook 2002, 150-152.

[58] European Central Bank, (2002), E-payments in Europe: The Eurosystem Perspective

[59] Διαθέσιμο στο Αρχείο : Distance course [ΣΕΛ. : 81]

[60] Διαθέσιμο στο [ΣΕΛ.: 82]
Έ Κύκλος Εργασιών : Ομάδα εργασίας Ε3 – Ηλεκτρονικές πληρωμές : προβλήματα και προοπτικές
Αρχείο : OE3_TelikoParadoteo 2004.

[61] Διαθέσιμο στο [ΣΕΛ.: 83-84]
Έ Κύκλος Εργασιών : Ομάδα εργασίας Ε3 – Ηλεκτρονικές πληρωμές : προβλήματα και προοπτικές
Αρχείο : OE3_TelikoParadoteo 2004. και στο Αρχείο : Distance course

[62] Διαθέσιμο στο [ΣΕΛ.: 85-86]
Έ Κύκλος Εργασιών : Ομάδα εργασίας Ε3 – Ηλεκτρονικές πληρωμές : προβλήματα και προοπτικές
Αρχείο : OE3_TelikoParadoteo 2004.

[63] Διαθέσιμο στο Αρχείο : Distance course [ΣΕΛ. : 86-89]

[64] Διαθέσιμο στο Αρχείο : Distance course [ΣΕΛ. : 89-90] και στο
Αρχείο : Teachers training e-commerce και στο
Αρχείο : Υποστήριξη συστημάτων ηλ.πληρωμών

[65] Διαθέσιμο στο [ΣΕΛ. : 90-92] και περαιτέρω πληροφορίες βρίσκονται στα
, και στο

[66] Διαθέσιμο στο Αρχείο : Distance course [ΣΕΛ. : 93-94] και στο
Αρχείο : Teachers training e-commerce

[67] Διαθέσιμο στο [ΣΕΛ.: 95-96]
Έ Κύκλος Εργασιών : Ομάδα εργασίας Ε3 – Ηλεκτρονικές πληρωμές : προβλήματα και προοπτικές
Αρχείο : OE3_TelikoParadoteo 2004.

[68] Διαθέσιμο στο [ΣΕΛ.: 97-100]
Έ Κύκλος Εργασιών : Ομάδα εργασίας Ε3 – Ηλεκτρονικές πληρωμές : προβλήματα και προοπτικές
Αρχείο : OE3_TelikoParadoteo 2004.

[69] Διαθέσιμο στο [ΣΕΛ.: 101-102]
Έ Κύκλος Εργασιών : Ομάδα εργασίας Ε3 – Ηλεκτρονικές πληρωμές : προβλήματα και προοπτικές
Αρχείο : OE3_TelikoParadoteo 2004.

[70] Διαθέσιμο στο [ΣΕΛ. : 103-110] η επιχειρείν : ηλεκτρονικές πληρωμές Αρχείο
Electronic bill presentment and payment

[71] Διαθέσιμο στο [ΣΕΛ. : 110-118] Αρχείο : Έλεγχος Καταιγισμού
στον Ωκεανό της Πληροφορίας: Ζώντας με την Ανωνυμία, το Ψηφιακό Χρήμα και τις Κατανεμημένες

Βάσεις Δεδομένων ,A.Michael Froomkin ,Δημοσιευμένο στην 15 U. Pittsburg Journal of Law and Commerce 395 (1996)

[72] Διαθέσιμο στο [ΣΕΛ.: 121]
Γ Κύκλος Εργασιών : Ομάδα εργασίας Γ3 –Έξυπνες κάρτες Αρχείο : G3V4_TelikoParadoteo 2004.
Και στο
Και στο

[73]Διαθέσιμο στο [ΣΕΛ.: 122]
Γ Κύκλος Εργασιών : Ομάδα εργασίας Γ3 –Έξυπνες κάρτες Αρχείο : G3V4_TelikoParadoteo 2004.
Και στο Αρχείο :Τι είναι οι έξυπνες κάρτες.

[74] Διαθέσιμο στο Αρχείο :Τι είναι οι έξυπνες κάρτες. [ΣΕΛ. : 123]

[75] Διαθέσιμο στο [ΣΕΛ. : 124-125] και στο

[76] Διαθέσιμο στο Αρχείο : Στοιχεία της αρχιτεκτονικής των έξυπνων καρτών [ΣΕΛ. : 125-126]

[77] Διαθέσιμο στο [ΣΕΛ. : 126-127] και στο

[78] Διαθέσιμο στο , [ΣΕΛ.:128] και στο
και στο

[79] Διαθέσιμο στο , [ΣΕΛ.: 129] και στο
και στο
Και στο

[80] Διαθέσιμο στο , [ΣΕΛ.:130-131] και στο
και στο
Και στο και στο

[81] Διαθέσιμο στο [ΣΕΛ.:132-133] και στο
Και στο

[82] Διαθέσιμο στο [ΣΕΛ.: 134] και στο
Και στο

[83] Διαθέσιμο στο [ΣΕΛ.: 135] και στο

[84] Διαθέσιμο στο
[ΣΕΛ. :136]

[85]Διαθέσιμο στο [ΣΕΛ. :137] και στο
και στο
Αρχείο : «an introduction to smart cards by Steve Petri »

[86] Διαθέσιμο στο [ΣΕΛ.: 138-139] και στο

[87] Διαθέσιμο στο [ΣΕΛ. :140 -145] και στο

[88] Διαθέσιμο στο Αρχείο : «an introduction to smart cards by Steve Petri » [ΣΕΛ. :146] και στο

[89]Διαθέσιμο στο Αρχείο «the transition from magnetic stripe to EMV chip cards. [ΣΕΛ. :146-147]

[90] Διαθέσιμο στο [ΣΕΛ. :147-148]

[91] Διαθέσιμο στο [ΣΕΛ.148]

[92]Διαθέσιμο στο [ΣΕΛ. : 149-151] και στο και στο

[93] Διαθέσιμο στο Αρχείο : «an introduction to smart cards by Steve Petri » [ΣΕΛ. : 152-153]

[94] Διαθέσιμο στο Αρχείο : «an introduction to smart cards by Steve Petri » [ΣΕΛ. : 153-154] και στο

[95] Διαθέσιμο στο , [ΣΕΛ.:154] και στο

[96] Διαθέσιμο στο Αρχείο : «an introduction to smart cards by Steve Petri » [ΣΕΛ. : 155-157] και στο

[97] Διαθέσιμο στο
[ΣΕΛ. : 157-158] και στο
Αρχείο : «an introduction to smart cards by Steve Petri »

[98] Διαθέσιμο στο Αρχείο : «an introduction to smart cards by Steve Petri » [ΣΕΛ. : 158-160] και στο

[99] Διαθέσιμο στο
[ΣΕΛ. : 160-161] και στο
Αρχείο : «an introduction to smart cards by Steve Petri »

[100] Διαθέσιμο στο [ΣΕΛ. : 162-163] και στο
και στο και στο

---

[101]Διαθέσιμο στο www.javacard.org/others/sc_applications.htm [ΣΕΛ. :164]

[102] Διαθέσιμο στο www.ebusinessforum.gr [ΣΕΛ.: 165-166]
Γ Κύκλος Εργασιών : Ομάδα εργασίας Γ3 –Έξυπνες κάρτες Αρχείο : G3V4_TelikoParadoteo 2004
και στο www.ewh.ieee.org/r10/bombay/news5/SmartCards.htm και στο
www.javacard.org/others/sc_applications.htm

[103] Διαθέσιμο στο www.ebusinessforum.gr [ΣΕΛ.: 166-167]
Γ Κύκλος Εργασιών : Ομάδα εργασίας Γ3 –Έξυπνες κάρτες Αρχείο : G3V4_TelikoParadoteo 2004
και στο www.ewh.ieee.org/r10/bombay/news5/SmartCards.htm

[104] Διαθέσιμο στο www.ebusinessforum.gr [ΣΕΛ.: 167-168]
Γ Κύκλος Εργασιών : Ομάδα εργασίας Γ3 –Έξυπνες κάρτες Αρχείο : G3V4_TelikoParadoteo 2004
και στο www.javacard.org/others/sc_applications.htm] και στο
www.ewh.ieee.org/r10/bombay/news5/SmartCards.htm

[105]Διαθέσιμο στο www.ebusinessforum.gr [ΣΕΛ.: 168-169]
Γ Κύκλος Εργασιών : Ομάδα εργασίας Γ3 –Έξυπνες κάρτες Αρχείο : G3V4_TelikoParadoteo 2004
και στο www.javacard.org/others/sc_applications.htm

[106] Διαθέσιμο στο www.ebusinessforum.gr [ΣΕΛ.: 169]
Γ Κύκλος Εργασιών : Ομάδα εργασίας Γ3 –Έξυπνες κάρτες Αρχείο : G3V4_TelikoParadoteo 2004

[107] Διαθέσιμο στο www.ebusinessforum.gr [ΣΕΛ.: 169]
Γ Κύκλος Εργασιών : Ομάδα εργασίας Γ3 –Έξυπνες κάρτες Αρχείο : G3V4_TelikoParadoteo 2004

[108] Διαθέσιμο στο www.ebusinessforum.gr [ΣΕΛ.: 170]
Γ Κύκλος Εργασιών : Ομάδα εργασίας Γ3 –Έξυπνες κάρτες Αρχείο : G3V4_TelikoParadoteo 2004

[109] Διαθέσιμο στο www.ebusinessforum.gr [ΣΕΛ.: 170]
Γ Κύκλος Εργασιών : Ομάδα εργασίας Γ3 –Έξυπνες κάρτες Αρχείο : G3V4_TelikoParadoteo 2004

[110]Διαθέσιμο στο www.ebusinessforum.gr [ΣΕΛ.: 171-172]
Γ Κύκλος Εργασιών : Ομάδα εργασίας Γ3 –Έξυπνες κάρτες Αρχείο : G3V4_TelikoParadoteo 2004

[111] Διαθέσιμο στο www.ebusinessforum.gr [ΣΕΛ.: 172]
Γ Κύκλος Εργασιών : Ομάδα εργασίας Γ3 –Έξυπνες κάρτες Αρχείο : G3V4_TelikoParadoteo 2004

[112] Διαθέσιμο στο www.javacard.org/others/sc_applications.htm [ΣΕΛ. : 173]

[113]Διαθέσιμο στο www.ebusinessforum.gr [ΣΕΛ.: 174]
Γ Κύκλος Εργασιών : Ομάδα εργασίας Γ3 –Έξυπνες κάρτες Αρχείο : G3V4_TelikoParadoteo 2004
και στο http://www.opengroup.org/comm/the_message/magazine/mmv5n5/SmartCards.htm και στο
http://support.cherry.de/english/new_faqib.asp?faqibid=219

[114]Διαθέσιμο στο http://www.opengroup.org/comm/the_message/magazine/mmv5n5/SmartCards.htm
[ΣΕΛ. :175]

[115] Διαθέσιμο στο http://www.ee.umanitoba.ca/~kinsner/projects/tutorials/tu1999/smcards.html
[ΣΕΛ. :175-176]

[116] Διαθέσιμο στο http://www.cs.utexas.edu [ΣΕΛ.: 176-177]

[117] Διαθέσιμο στο http://support.cherry.de/english/new_faqib.asp?faqibid=219 [ΣΕΛ.: 177-178]

[118] Διαθέσιμο στο www.scs.com.hk [ΣΕΛ. :178-185]

[119] Διαθέσιμο στο [illegible], [ΣΕΛ.:186] και στο [illegible]

[120] Διαθέσιμο στο [illegible] [ΣΕΛ.: 187-189]
Γ Κύκλος Εργασιών : Ομάδα εργασίας Γ3 –Έξυπνες κάρτες Αρχείο : G3V4_TelikoParadoteo 2004

[121]Διαθέσιμο στο [illegible] [ΣΕΛ.: 190-192]
Γ Κύκλος Εργασιών : Ομάδα εργασίας Γ3 –Έξυπνες κάρτες Αρχείο : G3V4_TelikoParadoteo 2004

[122] Διαθέσιμο στο [illegible] [ΣΕΛ.: 193-194]
Γ Κύκλος Εργασιών : Ομάδα εργασίας Γ3 –Έξυπνες κάρτες Αρχείο : G3V4_TelikoParadoteo 2004

[123] Διαθέσιμο στο [illegible] [ΣΕΛ. :195-200]

[124] Διαθέσιμο στο [illegible] [ΣΕΛ. :200-203]

[125]Διαθέσιμο στο [illegible] [ΣΕΛ.:204-210] Αρχείο: Πρακτικός οδηγός χρήσης δικτυακών υπηρεσιών για διοικητές νοσοκομείων

[126] Διαθέσιμο στο [illegible] [ΣΕΛ. :210-212] Αρχείο : Συστηματα ελέγχου και οικονομίας ρεύματος δωματίων ξενοδοχείου με έξυπνες κάρτες

[127] Διαθέσιμο στο [illegible] [ΣΕΛ. : 212-213] Αρχείο Συστήματα οικονομίας ρεύματος - ENERGY SAVERS

[128] Διαθέσιμο στο [illegible] [ΣΕΛ.: 214-216]

[129] Διαθέσιμο στο [illegible] [ΣΕΛ.: 217-227]
Γ Κύκλος Εργασιών : Ομάδα εργασίας Γ3 –Έξυπνες κάρτες Αρχείο : G3V4_TelikoParadoteo 2004.

[130] Διαθέσιμο στο [illegible] [ΣΕΛ.: 228-231]