Α.Τ.Ε.Ι.
ΜΕΣΟΛΟΓΓΙΟΥ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
Τμήμα Εφαρμογών Πληροφορικής
στη Διοίκηση και την Οικονομία

ΤΕΧΝΟΛΟΓΙΑ ΚΑΙ ΧΡΗΣΗ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ

ΦΟΙΤΗΤΕΣ:

ΚΑΘΗΓΗΤΗΣ:

Η πτυχιακή εργασία έχει ως στόχο την γνωριμία και εξοικείωση με τις λεγόμενες "έξυπνες κάρτες", μία σύγχρονη και νέα σχετικά τεχνολογία που χρησιμοποιείται παγκοσμίως σε όλο και περισσότερες και πιο προηγμένες εφαρμογές. Κάποιες γνωστές εφαρμογές με έξυπνες κάρτες σχετίζονται με τις τηλεκάρτες, τις κάρτες SIM στην κινητή τηλεφωνία, κάρτες πρόσβασης και αναγνώρισης σε προστατευμένους χώρους, το ηλεκτρονικό πορτοφόλι και τις κάρτες διοδίων.

Οι έξυπνες κάρτες χωρίζονται σε συγκεκριμένες κατηγορίες, ανάλογα με το αν περιέχουν μικροεπεξεργαστή ή όχι και με το αν επικοινωνούν με ηλεκτρικές επαφές ή ασύρματα.

Λέξεις Κλειδιά: έξυπνες κάρτες, reader καρτών, COS, API, APDU, MAC, e-purse, Secure Messaging, Secret Key, Secret Code, 3DES, Transaction Proofs.

ΠΕΡΙΕΧΟΜΕΝΑ

1

Εισαγωγή

Ανατρέχοντας στην απώτερη ακόμη ιστορία, βλέπουμε ανθρώπους να υιοθετούν, να φέρουν και να χρησιμοποιούν αντικείμενα που συμβολίζουν ή υποδηλώνουν σημαντικά για τον φέροντα χαρακτηριστικά και στοιχεία. Τα μικρά συνήθως αυτά αντικείμενα, χωρίς ιδιαίτερη αξία αυτά καθ' εαυτά, μέσω της μοναδικότητάς τους αποτύπωναν και μετέφεραν αντιπροσωπευτικά χαρακτηριστικά του κατόχου τους, υποδηλώνοντας τη θέση του, τις ιδιότητες και τα προνόμιά του.

Μία σύγχρονη εκδοχή αυτών των αντικειμένων είναι και οι έξυπνες κάρτες, οι οποίες καλύπτουν τις ίδιες βασικές ανάγκες στηριγμένες σε αξιόπιστη τεχνολογία και ευρύ πεδίο εφαρμογών ενώ προσφέρουν ακόμη ευρύτερες προοπτικές. Μικρές σε μέγεθος και εύχρηστες δεν έχουν αξία αυτές καθ΄εαυτές, αποκτούν όμως μεγάλη αξία αν αναλογιστεί κανείς τις υπηρεσίες που μπορούν να προσφέρουν, τις λειτουργίες που υποστηρίζουν και τα στοιχεία που δίνονται να αποθηκεύουν και να μεταφέρουν.

Στη σύγχρονη κοινωνία όπου η ταχύτητα και η ασφάλεια ανταλλαγής πληροφοριών παίζουν κύριο ρόλο στην επιτυχή διεκπεραίωση καθημερινών και μη λειτουργιών και όπου η τεχνολογία έρχεται να αντικαταστήσει κλασικές και συνήθως χρονοβόρες διαδικασίες στις οποίες κυρίαρχη θέση κατείχε ο ανθρώπινος παράγοντας, οι έξυπνες κάρτες έρχονται να διασφαλίσουν την μετάβαση σε μία πραγματικότητα με μεγάλη λειτουργικότητα ποικίλων διεργασιών.

1.1 Αντικείμενο της Πτυχιακής

Η πτυχιακή αυτή εργασία έχει ως σκοπό να παρουσιάσει την τεχνολογία των έξυπνων καρτών και να δώσει μία εικόνα βασικών λειτουργιών και χαρακτηριστικών τους. Επιπλέον παρουσιάζεται η επικρατούσα κατάσταση στην αγορά της συγκεκριμένης τεχνολογίας και συζητούνται οι προοπτικές των έξυπνων καρτών στον εμπορικό και τον επιστημονικό τομέα.

Κύριος στόχος της εργασίας είναι η γνωριμία και η εξοικείωση με το αντικείμενο αυτό και η απόκτηση βασικής τεχνογνωσίας σε θέματα έξυπνων καρτών, γεγονός που ανοίγει τον δρόμο για ανάπτυξη πραγματικών εφαρμογών και αναζήτηση προηγμένων λύσεων σε υπάρχοντα ή και μελλοντικά τεχνικά, εμπορικά, υπολογιστικά προβλήματα σε ένα ευρύ φάσμα δραστηριοτήτων.

1.2 Οργάνωση του τόμου

Για την καλύτερη κατανόηση του αντικείμενου της παρούσας πτυχιακής και για την ευκολία πρόσβασης στις επιμέρους πληροφορίες, το κείμενο έχει χωριστεί σε κεφάλαια και ενότητες, τα οποία θα αναφερθούν ακολούθως περιληπτικά.

Το πρώτο κεφάλαιο περιέχει την εισαγωγή της πτυχιακής εργασίας, δίνοντας πληροφορίες για το αντικείμενό της και το πλαίσιο στο οποίο εκπονήθηκε καθώς επίσης και μία περιγραφή της οργάνωσης των κεφαλαίων.

Το δεύτερο κεφάλαιο περικλείει εισαγωγικά στοιχεία για τις έξυπνες κάρτες, δίνοντας μία πρώτη περιγραφή της τεχνολογίας αυτής και παρέχοντας μια ιστορική αναδρομή πάνω στην παρουσία των έξυπνων καρτών και την εξέλιξή τους. Επίσης παρατίθενται στατιστικά στοιχεία για την αγορά των έξυπνων καρτών τα τελευταία χρόνια και την αναμενόμενη εξάπλωσή τους ενώ παρουσιάζονται και οι κυριότερες εφαρμογές που συναντάμε στην παγκόσμια αγορά και οι οποίες στηρίζονται στην νέα αυτή τεχνολογία.

Στο τρίτο κεφάλαιο παρέχεται λεπτομερής ανάλυση της τεχνολογίας των έξυπνων καρτών, με ανάλυση βασικών τεχνικών στοιχείων για την καλύτερη κατανόηση της δομής τους, πληροφορίες για τους τύπους των καρτών που υπάρχουν καθώς επίσης και εξέταση κύριων χαρακτηριστικών της τεχνολογίας όπως το λειτουργικό σύστημα των καρτών, και το πρωτόκολλο επικοινωνίας μεταξύ καρτών και reader. Επίσης γίνεται μία εισαγωγή στη τεχνολογία των reader – αναγνωστών καρτών.

Στο τέταρτο κεφάλαιο περιγράφεται η χρήση των έξυπνων καρτών και στο πέμπτο μας κεφάλαιο υπάρχει η ορολογία των έξυπνων καρτών. Τέλος στο τελευταίο μας κεφάλαιο υπάρχει η βιβλιογραφία της πτυχιακής.

2

Εισαγωγή Στις Έξυπνες Κάρτες

Ο όρος και μόνο "έξυπνη κάρτα" εντυπωσιάζει και εξάπτει τη φαντασία τουλάχιστον αυτών που ενδιαφέρονται για τις τεχνολογίες αιχμής, χωρίς να είναι όμως επαρκής για να προσδιορίσει τις ιδιότητες και τις δυνατότητες μίας φαινομενικά απλής πλαστικής κάρτας.

Η έξυπνη κάρτα στην πραγματικότητα ορίζεται ως μία πλαστική κάρτα, συνήθως σε μέγεθος και σχήμα πιστωτικής κάρτας, η οποία όμως περιέχει μνήμη ή/και μικροεπεξεργαστή που της δίνουν τη δυνατότητα αποθήκευσης και επεξεργασίας μεγάλου όγκου δεδομένων και η οποία συμμορφώνεται με διεθνή πρότυπα.

Με απλούς όρους, η έξυπνη κάρτα είναι ένας μικροσκοπικός υπολογιστής με πολύ σημαντικές δυνατότητες και αποτελεί την πιο πρόσφατη εξέλιξη στο χώρο των πλαστικών καρτών, έχοντας ήδη ανοίξει το δρόμο σε σημαντικές και εκτεταμένες εφαρμογές παγκοσμίως. Ο μικροσκοπικός αυτός υπολογιστής, αλλιώς καλούμενος μικροτσίπ, είναι ένα ολοκληρωμένο κύκλωμα με ηλεκτρικές επαφές ή με δυνατότητες ασύρματης επικοινωνίας που συνδυαζόμενος με την κατάλληλη συσκευή υποδοχής καρτών έχει τη δυνατότητα αποθήκευσης και μεταφοράς χιλιάδων bit πληροφορίας καθώς και μεγάλη δύναμη επεξεργασίας αυτών των δεδομένων για την εξυπηρέτηση ποικίλων εφαρμογών.

Κύρια χαρακτηριστικά των έξυπνων καρτών είναι ότι παρέχουν ασφάλεια δεδομένων και συνδιαλλαγών, ταχύτητα και ευκολία χρήσης καθώς επίσης αντοχή στην καταπόνηση και κακή χρήση και μεγάλο διάστημα "ζωής".

Σε αντίθεση με τις γνωστές κάρτες με μαγνητική ταινία, οι έξυπνες κάρτες κατέχουν βασικές και απαραίτητες διεργασίες και πληροφορίες αποθηκευμένες στο σώμα τους προσφέροντας έτσι περισσότερη ασφάλεια καθώς και τη δυνατότητα μεταφοράς σημαντικών δεδομένων χωρίς την ανάγκη σύνδεσης με κεντρικές βάσεις δεδομένων για την άντληση ουσιωδών πληροφοριών. Για αυτό το λόγο η τάση στις σύγχρονες αγορές κυρίως της Ευρώπης, είναι η αντικατάσταση των καρτών μαγνητικής ταινίας από τις έξυπνες κάρτες και η ανάπτυξη όλο και πιο πολύπλοκων εφαρμογών, όλο και πιο αυτοματοποιημένων διαδικασιών.

Για να καταλάβουμε τη σπουδαιότητα της εξέλιξης αυτής, της μετάβασης δηλαδή από τις κάρτες μαγνητικής ταινίας στις έξυπνες κάρτες, είναι προτιμότερο να αναλύσουμε τα χαρακτηριστικά της χρήσης των πρώτων σε διάφορες διαδικασίες.

2.1 Κάρτες Μαγνητικής Ταινίας

Οι κάρτες μαγνητικής ταινίας είναι ευρέως διαδεδομένες και χρησιμοποιούνται από το μεγαλύτερο μέρος του πληθυσμού σε διάφορες καθημερινές και μη συναλλαγές και λειτουργίες.

Σχήμα 2.1 - Δύο όψεις κάρτας μαγνητικής ταινίας

Από τις πιστωτικές κάρτες, στις κάρτες αυτόματης ανάληψης μετρητών και από τις κάρτες προγραμμάτων εμπιστοσύνης πολυκαταστημάτων ή αεροπορικών εταιριών στις κάρτες ελέγχου πρόσβασης σε κτίρια, οι κάρτες μαγνητικής ταινίας χρησιμοποιούνται για να αποθηκεύουν πληροφορίες σε μορφή αναγνώσιμη από μηχανές και έτσι έχουν αυτοματοποιήσει καθημερινές συναλλαγές και διαδικασίες. Η εκτεταμένη τους χρήση έχει σαφώς διευκολύνει τον απλό χρήστη καθώς και διάφορους τραπεζικούς και εμπορικούς φορείς, έχει όμως ταυτόχρονα επιδείξει σημαντικά μειονεκτήματα τα οποία πλέον δεν μπορούν να παρακαμφθούν.

Εξετάζοντας αυτά τα μειονεκτήματα έχουμε να παρατηρήσουμε ότι η κύρια πηγή προβλημάτων έγκειται στο γεγονός ότι τα δεδομένα που αποθηκεύονται στη μαγνητική ταινία μιας κάρτας μπορούν εύκολα να διαβαστούν και να τροποποιηθούν από οποιονδήποτε έχει πρόσβαση στον κατάλληλο εξοπλισμό. Έτσι είναι σαφές ότι εμπιστευτικές και κρίσιμες πληροφορίες όπως ο κωδικός αναγνώρισης του κατόχου, δεν μπορούν να αποθηκεύονται στην ίδια τη κάρτα αλλά αναγκαστικά καταχωρούνται σε κάποια κεντρική βάση δεδομένων.

Αυτό σημαίνει ότι για να εκτελεστεί οποιαδήποτε συναλλαγή πρέπει το τερματικό συναλλαγής (π.χ. ATM) να είναι online συνδεδεμένο με κάποιο κεντρικό υπολογιστή για να γίνει πιστοποίηση αυθεντικότητας, διαδικασία χρονοβόρα και με κόστος.

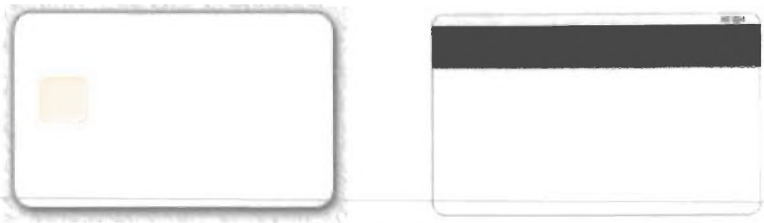
Έτσι, η χρήση των καρτών μαγνητικής ταινίας συνδυάζεται με την ύπαρξη και συντήρηση μεγάλων κεντρικών μονάδων για τη φύλαξη και επεξεργασία των ευαίσθητων δεδομένων, καθώς και με τη συντήρηση κυκλωμάτων για τις απαραίτητες online συνδέσεις μεταξύ κεντρικών βάσεων δεδομένων και σημείων πώλησης - συναλλαγής.

Επιπλέον, οι κάρτες μαγνητικής ταινίας παρουσιάζουν ευαισθησία σε παράγοντες όπως τα μαγνητικά πεδία, οι τυχόν επαφές με αιχμηρά αντικείμενα και η παρατεταμένη χρήση τους, οι οποίοι μπορούν να καταστρέψουν τη μαγνητική ταινία της κάρτας. Επίσης, οι κάρτες αυτές σχεδιάζονται για μία και μόνο εφαρμογή και οποιαδήποτε αλλαγή στα χαρακτηριστικά της εφαρμογής ή στα στοιχεία του κατόχου σημαίνει και αντικατάσταση της ίδιας της κάρτας.

Τα ανωτέρω στοιχεία, με κυριότερο το θέμα της ασφάλειας των δεδομένων και της εγκυρότητας των συναλλαγών, καθιστούν τις κάρτες μαγνητικής ταινίας ένα προϊόν που δεν δύνεται να καλύψει πλήρως τις συνεχώς αυξανόμενες ανάγκες και απαιτήσεις της σύγχρονης αγοράς.

2.2 Σύγκριση Καρτών Μαγν/κής Ταινίας Με Έξυπνες Κάρτες

Οι έξυπνες κάρτες, όπως προαναφέρθηκε, έχουν σημαντικά πλεονεκτήματα σε σχέση με τις ευρέως χρησιμοποιούμενες κάρτες μαγνητικής ταινίας και τείνουν να αποτελέσουν τη κυρίαρχη τάση για ανεπτυγμένες, απλές ή και πιο σύνθετες εφαρμογές σε ποικίλους τομείς.



Σχήμα 2.2 - Έξυπνη κάρτα - Κάρτα μαγνητικής ταινίας

Κύρια χαρακτηριστικά των έξυπνων καρτών είναι οι προηγμένες διαδικασίες ασφάλειας δεδομένων και συνδιαλλαγών, η δυνατότητα μεταφοράς σημαντικών δεδομένων καθώς και η εύκολη και γρήγορη πρόσβαση σε ευαίσθητες πληροφορίες εφόσον αποτελούν ένα κινητό ηλεκτρονικό αρχείο. Επίσης οι έξυπνες κάρτες προσφέρουν ευκολία χρήσης, ανθεκτικότητα, δυνατότητα επικοινωνίας και σύνδεσης με υπολογιστές, ταχύτητα επεξεργασίας και συνήθως υπολογιστική δύναμη.

Συγκρίνοντας τις δύο προαναφερθείσες μορφές πλαστικών καρτών, παρατηρούμε σημαντικές διαφορές σε τομείς που θα αναλυθούν ακολούθως.

• Αποθήκευση Δεδομένων: σε σχέση με τη περιορισμένη δυνατότητα αποθήκευσης πληροφοριών των καρτών μαγνητικής ταινίας (ως 140 byte πληροφορίας), οι έξυπνες κάρτες έχουν μεγάλη χωρητικότητα, με δυνατότητα αποθήκευσης ως και 80 φορές περισσότερων ηλεκτρονικών δεδομένων (από 1Kbyte ως 32Kbytes πληροφορίας).

• Ασφάλεια: ενώ στις κάρτες μαγνητικής ταινίας οι εκάστοτε πληροφορίες μπορούν εύκολα να αλλοιωθούν ή να αναπαραχθούν από μη έγκυρους χρήστες, οι έξυπνες κάρτες παρέχουν αυξημένη ασφάλεια δεδομένων και συναλλαγών, με τη χρήση διαδικασιών όπως κρυπτογράφηση και κωδικοποίηση.

• Αντοχή / Διάρκεια: σε αντίθεση με την ευαισθησία των καρτών μαγνητικής ταινίας που συνίσταται στη πιθανότητα απομαγνητισμού της ταινίας λόγω χρήσης ή λόγω εξωτερικών μαγνητικών πεδίων, οι έξυπνες κάρτες παρουσιάζουν μεγάλη ανθεκτικότητα και έχουν μεγάλη συγκριτικά διάρκεια ζωής και αντοχή σε αλλεπάλληλες εισαγωγές σε μηχανήματα υποδοχής καρτών 100.000 φορές και πάνω.

• Χρήση: η σχεδίαση των καρτών μαγνητικής ταινίας γίνεται για μία εφαρμογή και η χρήση τους περιορίζεται σε απλά και επαναλαμβανόμενα καθήκοντα, ενώ οι έξυπνες κάρτες υποστηρίζουν πολλαπλές και πολύπλοκες εφαρμογές.

• Ευελιξία: τα δεδομένα μίας κάρτας μαγνητικής ταινίας είναι μόνο αναγνώσιμα με αποτέλεσμα οποιαδήποτε σημαντική αλλαγή στοιχείων να καθιστά αναγκαία την έκδοση νέας κάρτας, ενώ σε μία έξυπνη κάρτα διαδικασίες ανάγνωσης, εγγραφής και ανανέωσης δεδομένων γίνονται εύκολα και γρήγορα.

• Σύνδεση: η χρήση καρτών μαγνητικής ταινίας καθιστά αναγκαία την online σύνδεση με κεντρική βάση δεδομένων για κάθε συναλλαγή, γεγονός που συνεπάγεται συνήθως την ύπαρξη μισθωμένης γραμμής. Το κόστος που αντιστοιχεί στη μίσθωση γραμμής είναι ένα επιπλέον κόστος που δεν υπάρχει στην περίπτωση των έξυπνων καρτών, οι οποίες μπορούν να κάνουν offline ασφαλείς και έγκυρες συναλλαγές τα στοιχεία των οποίων θα περνάνε αν χρειάζεται σε κεντρικό σύστημα σε δεδομένη χρονική στιγμή, ανεξάρτητη της στιγμής συναλλαγής.

Το κόστος κατασκευής έξυπνων καρτών είναι μεγαλύτερο από το αντίστοιχο των καρτών μαγνητικής ταινίας, λόγω όμως της ανθεκτικότητάς τους, της χρησιμοποίησής τους σε ποικίλες εφαρμογές, τη μείωση των οικονομικών απατών και τη μείωση του κόστους τηλ/κής σύνδεσης, οι έξυπνες κάρτες είναι τελικά πιο αποδοτικές ως προς το κόστος.

Αν και οι παράγοντες που ευνοούν τη χρήση των έξυπνων καρτών στη θέση των καρτών μαγνητικής ταινίας είναι σημαντικοί, δεν έχουν το ίδιο βάρος σε όλες τις σύγχρονες αγορές με αποτέλεσμα να μην έχουν την ίδια απήχηση παγκοσμίως. Έτσι χρησιμοποιούνται ήδη ευρέως στις αγορές της Ευρώπης, της Ασίας και της Αφρικής, έχοντας γίνει ένα προϊόν εμπορικά επιτυχημένο. Οι εφαρμογές που στηρίζονται σε έξυπνες κάρτες καλύπτουν τομείς όπως η πρόσβαση και η αναγνώριση ταυτότητας σε

διάφορους χώρους, οι ηλεκτρονικές αγορές μέσω του Διαδικτύου και οι τουριστικές επιχειρήσεις, δίνοντας εξελιγμένες δυνατότητες. Υπάρχουν όμως αγορές στις οποίες οι έξυπνες κάρτες, παρότι παρουσιάστηκαν επιτυχώς και ελπιδοφόρα, δεν έχουν καταφέρει ακόμα να καθιερωθούν ως κοινό μέσο συναλλαγών και εφαρμογών. Ένα σημαντικό παράδειγμα είναι η αγορά της Αμερικής στην οποία η τεχνολογία των έξυπνων καρτών είναι ακόμα καινούρια. Το υψηλό κόστος των έξυπνων καρτών σε σχέση με τις κάρτες μαγνητικής ταινίας και η αναγκαιότητα ειδικών συσκευών ανάγνωσης καρτών (card readers) συνεπάγονται μία υψηλή επένδυση για τα Αμερικανικά οικονομικά ιδρύματα τα οποία ήδη έχουν επενδύσει στα συστήματα μαγνητικής ταινίας. Ο χρόνος και το κόστος μίας μεγάλης αλλαγής στη τεχνολογία αυτή αποτέλεσαν μέχρι τώρα ανασταλτικούς παράγοντες για μεγάλες και τολμηρές επενδύσεις. Κύριος όμως ανασταλτικός παράγοντας για την Αμερικανική αγορά αποτελεί το ότι η δομή διεξαγωγής οικονομικών και πληροφοριακών συναλλαγών έχει εξελιχθεί διαφορετικά από ότι στην Ευρώπη. Η Ευρώπη κατάφερε να αναπτύξει την τεχνολογία των έξυπνων καρτών ως ένα αποδοτικό, ως προς το κόστος, τρόπο διεξαγωγής συναλλαγών οι οποίες αποσυνδέθηκαν από τις online διαδικασίες πιστοποίησης που στην Ευρώπη συνεπάγονται μεγάλο τηλεπικοινωνιακό κόστος. Στην Αμερική αντιθέτως το τηλεπικοινωνιακό κόστος είναι χαμηλό και έτσι αποδυναμώνεται ένα σημαντικό προτέρημα της εισαγωγής των έξυπνων καρτών.

2.3 Ιστορική Αναδρομή

Πολλοί θεωρούν ότι οι έξυπνες κάρτες είναι μια πρόσφατη εφεύρεση. Αυτό όμως δε θα μπορούσε να απέχει περισσότερο από την αλήθεια. Στην πραγματικότητα, η ιστορική προέλευση των έξυπνων καρτών μας οδηγεί στη δεκαετία του 70. Η αρχική ιδέα της ενσωμάτωσης μικροτσίπ σε πλαστικές κάρτες γεννήθηκε το 1968 στη Γερμανία από τον Jurgen Dethloff και τον Helmut Grotrupp. Δύο χρόνια αργότερα, το 1970 στην Ιαπωνία, ο εφευρέτης Kunitaka Arimura διατύπωσε μία παρόμοια πατέντα στην ιδέα της έξυπνης κάρτας. Τα πραγματικά θεμέλια όμως για την υλοποίηση της τεχνολογίας των έξυπνων καρτών μπήκαν το 1974 στη Γαλλία από τον ανεξάρτητο εφευρέτη και ερευνητή Roland Moreno. Ο Moreno υλοποίησε πιλοτικά την ένωση πλαστικής κάρτας και μικροτσίπ, το παρουσίασε σε κάποιες τράπεζες στη Γαλλία και τον επόμενο χρόνο το κατοχύρωσε και ως πατέντα.

Η πρώτη έξυπνη κάρτα κατασκευάστηκε τελικά το 1977 από την Motorola και την Bull ενώ συγχρόνως 3 εμπορικοί κατασκευαστές, η Bull, η SGS Thomson και η Schlumberger ξεκίνησαν να αναπτύσσουν εφαρμογές πάνω στη νέα τεχνολογία. Η πρώτη αυτή κάρτα περιείχε δύο μικροτσίπ, δηλαδή ένα μικροελεγκτή και μία ξεχωριστή συσκευή μνήμης. Το 1980 η Motorola παρουσίασε την πρώτη ασφαλή έξυπνη κάρτα με ένα μικροτσίπ, για χρήση στο Γαλλικό τραπεζικό χώρο. Το 1982 έγινε στη Γαλλία το πρώτο εκτεταμένο και πραγματικό τεστ έξυπνων καρτών και συγκεκριμένα τηλεφωνικών καρτών σειριακής μνήμης. Ακολούθως το 1984 έγιναν τα πρώτα τεστ στην παραγωγή των έξυπνων καρτών αυτόματης ανάληψης.

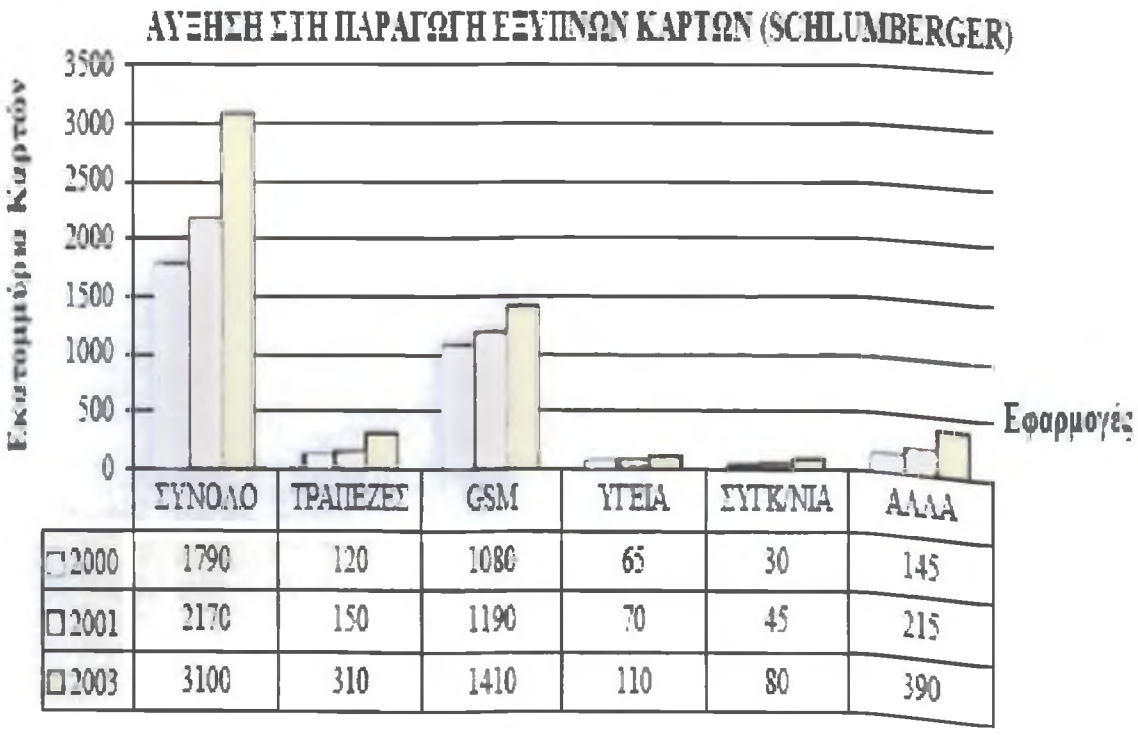
Με την πάροδο των χρόνων, οι έξυπνες κάρτες εξελίσσονταν συνεχώς, και καινούριες εφαρμογές αναπτύσσονταν, κυρίως στην Ευρώπη. Η Γαλλία έχει πρωτοπορήσει όλα αυτά τα χρόνια στο σχεδιασμό και τη χρήση εφαρμογών έξυπνων καρτών και μαζί με τη Γερμανία αποτελούν τις κορυφαίες χώρες σε εισαγωγή ποικίλων εφαρμογών σε έξυπνες κάρτες. Το 1987 εφαρμόστηκε το πρώτο μεγάλης κλίμακας έργο με έξυπνες κάρτες στην Αμερική ενώ το 1993 οι πρώτες εφαρμογές με κάρτες πολλαπλών διεργασιών δοκιμάστηκαν στην Γαλλία. Το ίδιο έτος ολοκληρώθηκε σχεδόν στη Γαλλία η αντικατάσταση των υπάρχουσων τραπεζικών καρτών με έξυπνες κάρτες και η τάση αυτή εξαπλώθηκε σε άλλες Ευρωπαϊκές και Ασιατικές χώρες.

Έκτοτε η βιομηχανία των έξυπνων καρτών εξαπλώνεται με πολύ μεγάλο ρυθμό και έχει φτάσει σε βαθμό παραγωγής και αποστολής καρτών σχεδόν ίσο με 1.000.000.000 το χρόνο ενώ πλέον οι έξυπνες κάρτες χρησιμοποιούνται σε διάφορες εφαρμογές σε περισσότερες από 90 χώρες παγκοσμίως. Το μεγαλύτερο μερίδιο της αγοράς των έξυπνων καρτών κατέχουν οι εφαρμογές τηλεφωνίας, οι τραπεζικές εφαρμογές, έργα που αφορούν το τομέα της Υγείας καθώς και άλλα ποικίλα σχέδια που θα αναπτύξουμε παρακάτω.

2.4 Στατιστικά Στοιχεία

Σύμφωνα με αναλύσεις της αγοράς έξυπνων καρτών από οικονομικούς παράγοντες και εταιρίες κατασκευής καρτών, έχουν προκύψει έγκυρες αναφορές της κίνησης της αγοράς των έξυπνων καρτών παγκοσμίως. Οι αναφορές αυτές προσδιορίζουν το μέγεθος της παραγωγής έξυπνων καρτών μέσα στο χρονικό διάστημα των τελευταίων ετών και παρουσιάζουν την εξάπλωση αυτής της τεχνολογίας ανά περιοχή. Συγχρόνως, λεπτομερή μοντέλα πρόβλεψης δείχνουν την πιθανή εικόνα της αγοράς των έξυπνων καρτών στα επόμενα χρόνια δίνοντας έτσι την ευκαιρία κυρίως στις εταιρίες να κατανοήσουν τις οικονομικές και επενδυτικές κινήσεις που μπορούν να ακολουθήσουν στην αγορά αυτή.

Με βάση το Σχήμα 2.4.1 που ακολουθεί (διάγραμμα της παραγωγής έξυπνων καρτών ανά τομέα εφαρμογής), παρατηρούμε ότι το μεγάλο μερίδιο κατέχουν εφαρμογές κινητής τηλεφωνίας (GSM) που χρησιμοποιούν την έξυπνη κάρτα ως κάρτα SIM του κινητού τηλεφώνου. Δεύτερος τομέας σημαντικής χρήσης έξυπνων καρτών είναι ο τραπεζικός και ακολουθούν ο τομέας της Υγείας και των Συγκοινωνιών.

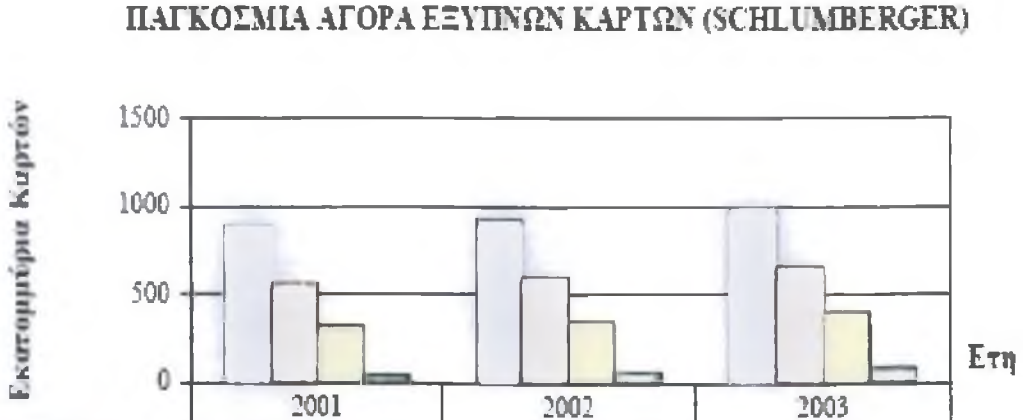


Σχήμα 2.4.1

Το σημαντικό στοιχείο, σύμφωνα και με το ακόλουθο διάγραμμα (η καφέ στήλη αποτελεί πρόβλεψη) είναι ότι κάθε τομέας και κυρίως το σύνολο της παραγωγής παρουσιάζει σταθερά αύξηση από το ένα έτος στο άλλο, δείχνοντας ότι η αγορά των έξυπνων καρτών είναι ακόμα σε ταχεία ανάπτυξη και εξάπλωση.

Σχήμα 2.4.2

Σημαντικά συμπεράσματα βγάζουμε επίσης παρατηρώντας τη μορφή και το μέγεθος της αγοράς των έξυπνων καρτών ανά περιοχή.

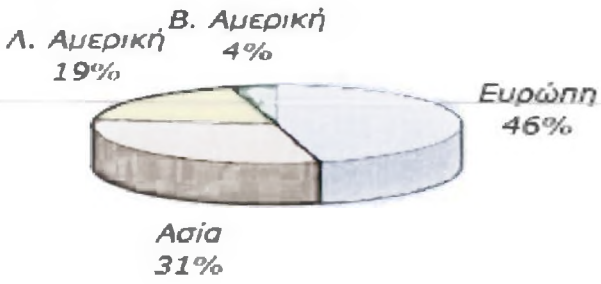


	2001	2002	2003
ΕΥΡΩΠΗ	883	923	974
ΑΣΙΑ	558	597	656
Λ.ΑΜΕΡΙΚΗ	322	346	402
Β.ΑΜΕΡΙΚΗ	38	58	85

Σχήμα 2.4.3

Όπως έχει αναφερθεί και νωρίτερα, οι εφαρμογές έξυπνων καρτών είναι κυρίως διαδεδομένες στην Ευρώπη και την Ασία, με τον Ευρωπαϊκό χώρο να αποτελεί το μεγαλύτερο πεδίο χρήσης της τεχνολογίας αυτής κρατώντας το 46% της αγοράς. Η αγορά της Λατινικής Αμερικής ακολουθεί τρίτη, με μεγέθη κυκλοφορίας έξυπνων καρτών σχετικά κοντά με τα αντίστοιχα της Ασιατικής αγοράς, ενώ η Βόρεια Αμερική βρίσκεται στη τελευταία θέση, παρουσιάζοντας συγκριτικά πολύ μικρά μεγέθη χρήσης εφαρμογών που στηρίζονται σε έξυπνες κάρτες.

Χρήση Έξυπνων Καρτών Ανά Περιοχή

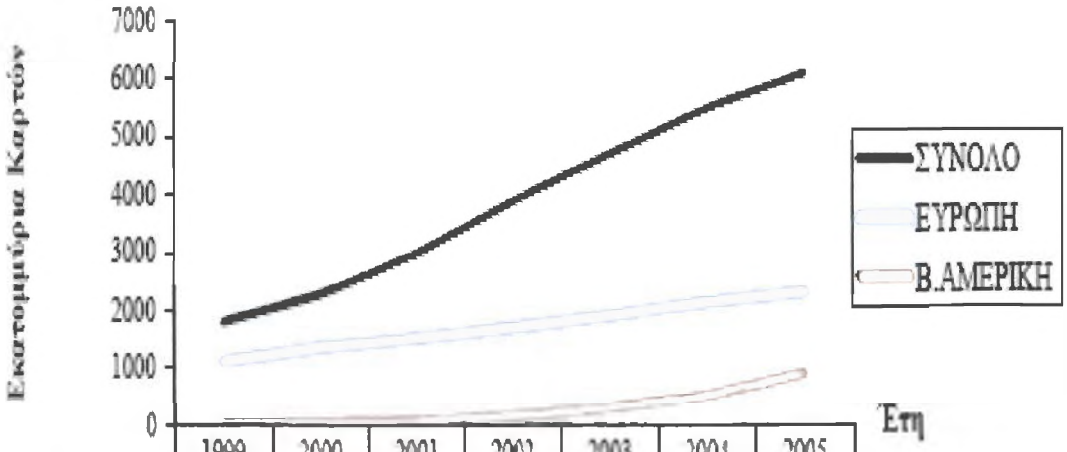


Σχήμα 2.4.4

Όπως παρατηρούμε και από την πίτα καταμερισμού της αγοράς, η Βόρεια Αμερική κατέχει μόνο το 4% της παγκόσμιας αγοράς. Το γεγονός αυτό οφείλεται σε παράγοντες που έχουν ήδη αναλυθεί, είναι όμως ελπιδοφόρο το γεγονός ότι με την πάροδο των ετών ο αριθμός των έξυπνων καρτών που κυκλοφορούν και χρησιμοποιούνται στην αγορά των Ηνωμένων Πολιτειών παρουσιάζει αύξηση. Σε αντίθεση με την Β. Αμερική, η Ευρώπη κατέχει μερίδιο αγοράς σχεδόν ίσο με το 50%. Η Λατινική Αμερική, η Κίνα, η Ιαπωνία και άλλες Ασιατικές χώρες, όπως είδαμε και προηγουμένως πρόκειται να αποτελέσουν δυνατούς διεκδικητές στη μάχη των μεριδίων της αγοράς.

Όπως τέλος παρατηρούμε από το διάγραμμα που ακολουθεί και παρουσιάζει μία πρόβλεψη για τη χρήση έξυπνων καρτών στην Ευρώπη και την Βόρεια Αμερική, μπορεί μεν ο αριθμός των καρτών που κυκλοφορούν ανά έτος στην αγορά να είναι πολύ μεγαλύτερος στον Ευρωπαϊκό χώρο και να προβλέπεται να παραμένει ανώτερος στα επόμενα χρόνια, ο ρυθμός ανάπτυξης όμως της αγοράς στη Βόρεια Αμερική παρουσιάζεται σημαντικά μεγαλύτερος από τον αντίστοιχο ευρωπαϊκό, ιδιαίτερα από το 2002 και έπειτα.

ΠΡΟΒΛΕΨΗ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ ΑΝΑ ΠΕΡΙΟΧΗ (TSI International)



	1999	2000	2001	2002	2003	2004	2005
ΣΥΝΟΛΟ	1800	2300	3000	3900	4700	5500	6100
ΕΥΡΩΠΗ	1124	1371	1535	1720	1926	2157	2318
Β.ΑΜΕΡΙΚΗ	36	50	76	164	310	530	915

Σχήμα 2.4.5

Συγκεκριμένα, σύμφωνα με αναλύσεις, ο ετήσιος ρυθμός ανάπτυξης της αγοράς έξυπνων καρτών στην Βόρεια Αμερική, αγγίζει το 50% στο 2004, γεγονός που δείχνει τη σημαντική δυναμική της τεχνολογίας έξυπνων καρτών στην αγορά αυτή. Σε γενικότερη κλίμακα, παρατηρούμε ότι ο ρυθμός ανάπτυξης της παγκόσμιας αγοράς έξυπνων καρτών είναι έντονα θετικός, παρουσιάζοντας έτσι την εφαρμογή της τεχνολογίας των έξυπνων καρτών ως μία καλπάζουσα τάση που εδραιώνεται όλο και περισσότερο στη σύγχρονη πραγματικότητα, καθώς και στη συνείδηση των καταναλωτών και των επιχειρήσεων.

Ενδεικτικό είναι το γεγονός ότι εκτιμάται πως οι παγκόσμιες πωλήσεις έξυπνων καρτών θα φτάσουν τα 12 δισεκατομμύρια δολάρια το 2010. Υπάρχουν σαφώς αρκετά βήματα τα οποία πρέπει να γίνουν για να υπάρχει ακόμα μεγαλύτερη ανάπτυξη της αγοράς των έξυπνων καρτών, βήματα που έχουν σχέση με τη γνωριμία και εμπιστοσύνη του κοινού με τη νέα αυτή τεχνολογία, καθώς και με την ανάπτυξη κατάλληλης υποδομής σε πολλούς τομείς. Υπάρχει η βεβαιότητα όμως ότι η απόδοση των υπάρχουσων εφαρμογών θα αποτελέσουν τον καλύτερο "πωλητή" των έξυπνων καρτών στην αγορά.

2.5 Εφαρμογές Έξυπνων Καρτών

Οι έξυπνες κάρτες βοηθούν τις επιχειρήσεις να εξελιχθούν και να διευρύνουν τα προϊόντα και τις υπηρεσίες τους σε μία συνεχώς μεταβαλλόμενη παγκόσμια αγορά. Λόγω της επεξεργαστικής δυνατότητας που έχουν μέσω του ενσωματωμένου μικροτσίπ, χρησιμοποιούνται παγκοσμίως για ένα μεγάλο εύρος καθημερινών εργασιών αλλά και προηγμένων εφαρμογών, την πλειονότητα των οποίων θα αναπτύξουμε παρακάτω.

Οι εκάστοτε εταιρίες, σχεδιάζοντας εφαρμογές και προγράμματα, μπορούν να δουν και να χρησιμοποιήσουν τις έξυπνες κάρτες ως:

• Μέσα Πληρωμής: οι έξυπνες κάρτες εξασφαλίζουν ασφαλείς χρεωστικές και πιστωτικές συναλλαγές, με μηχανισμούς που να προστατεύουν από κακόβουλες επιθέσεις. Συγχρόνως, αποτελούν για τις εταιρίες μία νέα καθαρή πηγή εσόδων αφού τις απαλλάσσουν από το πάγιο κόστος συναλλαγής το οποίο συνόδευε κάθε συναλλαγή με τις γνωστές τραπεζικές κάρτες (credit/debit cards) όπως και από τις πιθανές απώλειες εσόδων λόγω χαμένων / κλεμμένων καρτών.

• Εργαλεία Πρόσβασης: οι έξυπνες κάρτες υποστηρίζουν λειτουργίες κρυπτογράφησης, πιστοποίησης, εξουσιοδότησης, επεξεργασίας και αποθήκευσης πληροφοριών οι οποίες καθιστούν δυνατή την ασφαλή διεξαγωγή οικονομικών συναλλαγών και ανταλλαγή πληροφορίας σε on-line/off-line περιβάλλοντα. Έτσι γίνονται ιδανικές για τον έλεγχο πρόσβασης στο Διαδίκτυο και για εφαρμογές όπως το home banking.

• Διαχειριστές Πληροφοριών: λόγω της επεξεργαστικής και αποθηκευτικής τους δύναμης όσο αφορά πληροφορίες, οι έξυπνες κάρτες μπορούν να χρησιμοποιηθούν ως ένα κινητό ηλεκτρονικό αρχείο που μπορεί να μεταφέρει δεδομένα όπως χρήσιμα τηλέφωνα, στοιχεία του λογαριασμού του κατόχου, πόντους προγραμμάτων εμπιστοσύνης λιανικής πώλησης ή ακόμα και τον ιατρικό φάκελο του χρήστη.

• Εργαλεία Προώθησης: οι έξυπνες κάρτες μπορούν να λειτουργήσουν ως προϊόντα προώθησης μίας εταιρίας αφού υπηρεσίες όπως εκπτωτικές προσφορές, προγράμματα εμπιστοσύνης, ηλεκτρονικά κουπόνια και δωροεπιταγές μπορούν κάλλιστα να

αποθηκεύουν και να επεξεργάζονται με ασφάλεια τα εκάστοτε στοιχεία τους στις έξυπνες κάρτες.

• Συστήματα Προσωποποιημένων Υπηρεσιών: με τις δυνατότητες αποθήκευσης, επεξεργασίας και κωδικοποίησης δεδομένων που υποστηρίζουν οι έξυπνες κάρτες, μπορούν να κρατούν σημαντικά στοιχεία για το κάτοχό τους και να χρησιμεύουν για την παροχή προσωποποιημένων υπηρεσιών από διάφορες εταιρίες.

Με μία ή περισσότερες από τις μορφές που αναφέρθηκαν παραπάνω, οι έξυπνες κάρτες έχουν χρησιμοποιηθεί σε ποικίλες εφαρμογές τις οποίες θα παραθέσουμε ακολούθως πιο διεξοδικά.

2.5.1 Τηλεφωνικές Κάρτες

Οι τηλεφωνικές κάρτες προπληρωμένης αξίας αποτελούν μία από τις πρώτες εφαρμογές έξυπνων καρτών. Διαδεδομένη χρήση τους ξεκίνησε το 1986 από τη Γαλλία και έκτοτε επεκτάθηκε ραγδαία και σε άλλες χώρες. Σε περισσότερες από 100 χώρες παγκοσμίως οι τηλεφωνικοί κερματοδέκτες σε δημόσιους και κοινόχρηστους χώρους, έχουν αντικατασταθεί από καρτοτηλέφωνα και τα κέρματα, ως μέσο πληρωμής των τηλεφωνικών υπηρεσιών, από τις τηλεφωνικές έξυπνες κάρτες.

Αγοράζονται από τους καταναλωτές έναντι συγκεκριμένου αντιτίμου (3€, 6€ και 18€ για την Ελληνική αγορά) και περιέχουν συγκεκριμένο αριθμό μονάδων (ανάλογα με το ποσό αγοράς τους), οι οποίες μειώνονται με κάθε κλήση. Οι τηλεκάρτες είναι έξυπνες κάρτες που ανήκουν στην κατηγορία των καρτών μνήμης (memory cards).

Μεγάλης κλίμακας προγράμματα εφαρμόζονται σε χώρες όπως η Γερμανία, η Γαλλία, η Αγγλία, η Βραζιλία, το Μεξικό και η Κίνα, ενώ στην Ελλάδα το δίκτυο καρτοτηλεφωνίας περιλαμβάνει 70.000 καρτοτηλέφωνα σε όλη τη χώρα.

2.5.2 Κινητή Τηλεφωνία (GSM)

Οι έξυπνες κάρτες χρησιμοποιούνται ευρέως ως κάρτες SIM (Security Identity Module) στην κινητή τηλεφωνία GSM (Global System for Mobile communications). Η κάρτα SIM περιέχει πληροφορίες ασφαλείας και συνδρομητικά στοιχεία. Μπορεί είτε να εισάγεται στη συσκευή είτε να βρίσκεται ενσωματωμένη σε αυτή και με την ενεργοποίησή της το τηλέφωνο προσωποποιείται ως προς το χρήστη και φορτώνει στοιχεία όπως το νούμερό του στο δίκτυο, πληροφορίες κοστολόγησης και πρόσφατα κληθέντες αριθμούς. Η κάρτα μπορεί να μεταφέρεται από συσκευή σε συσκευή αφού περιέχει τα στοιχεία του συνδρομητή τα οποία προστατεύονται από ειδικό κωδικό (PIN).

Οι παροχείς κινητής τηλεφωνίας κερδίζουν από τη μείωση των περιπτώσεων απάτης και μη έγκυρης χρήσης λόγω της αυξημένης ασφάλειας που προσφέρουν οι έξυπνες κάρτες. Με την έλευση προηγμένων υπηρεσιών κινητής τηλεφωνίας όπως η πρόσβαση στο Διαδίκτυο (web browsing), το ηλεκτρονικό ταχυδρομείο και άλλες υπηρεσίες πληροφοριών, οι παροχείς βασίζονται στις έξυπνες κάρτες να δράσουν ως μηχανισμοί ασφαλείας για τις υπηρεσίες αυτές.

Στη παγκόσμια αγορά, το 1994 πωλήθηκαν περισσότερες από 9.000.000 έξυπνες κάρτες κινητής τηλεφωνίας ενώ πλέον τα κινητά τηλέφωνα που χρησιμοποιούν τις έξυπνες κάρτες ως κάρτες SIM ξεπερνούν τα 300.000.000.

2.5.3 Συνδρομητική Τηλεόραση

Σχεδόν κάθε μικρό πιάτο δορυφορικής τηλεόρασης στις Ηνωμένες Πολιτείες χρησιμοποιεί μία έξυπνη κάρτα ως αφαιρέσιμο στοιχείο ασφαλείας και πληροφοριών για το συνδρομητή.

Οι έξυπνες κάρτες λειτουργούν ως μία προπληρωμένη εφαρμογή, όπως και οι τηλεκάρτες που αναφέρθηκαν παραπάνω, και περιέχουν πληροφορίες εξουσιοδότησης και κοστολόγησης που αντιστοιχούν στον συνδρομητή-κάτοχο. Κυρίως περιέχουν ειδικά "κλειδιά" (keys) τα οποία χρειάζονται για να μπορεί ο συνδρομητής να δει την κωδικοποιημένη μετάδοση.

Η κάρτα συνδρομητικής τηλεόρασης μπορεί να χρησιμοποιηθεί σε οποιοδήποτε χώρο έχει την κατάλληλη υποδομή και δε συνδέεται αποκλειστικά με τη συσκευή αλλά με το συνδρομητή. Έτσι ένας συνδρομητής μπορεί με την κάρτα του να παρακολουθήσει το πρόγραμμα της συνδρομητικής τηλεόρασης στο σπίτι του αλλά και σε ένα ξενοδοχείο.

Ένα μεγάλο προτέρημα της χρήσης έξυπνων καρτών σε αυτή την εφαρμογή είναι τα στοιχεία προσωποποίησης που περιέχουν και προσδιορίζουν-φιλτράρουν το μέρος της μετάδοσης που θα λαμβάνει ο συνδρομητής. Έτσι οι γονείς μπορούν να παρέχουν στα παιδιά κάρτες συνδρομητικής τηλεόρασης που αποκλείουν την πρόσβαση των παιδιών σε προγράμματα ακατάλληλα.

Στην Αμερική, πάνω από 4.000.000 κάρτες συνδρομητικής τηλεόρασης χρησιμοποιούνται και εκατομμύρια ακόμα διατίθενται στην Ευρώπη και την Ασία.

2.5.4 Συγκοινωνίες

Οι έξυπνες κάρτες χρησιμοποιούνται σε μεγάλο βαθμό ως "εισιτήρια", στα μέσα μαζικής μεταφοράς, στα πάρκινγκ και τα διόδια. Συνήθως χρησιμοποιούνται contactless (χωρίς επαφή) κάρτες, που διευκολύνουν και επιταχύνουν τη διαδικασία. Πωλούνται ως κάρτες προπληρωμένης αξίας, όπως και οι τηλεφωνικές. Σχεδιάζονται για χρήση σε μέσα μαζικής μεταφοράς όπως λεωφορεία και τρένα, όπως επίσης και στα διόδια, κάνοντας τη διαδικασία έκδοσης εισιτηρίων πολύ πιο γρήγορη και εύκολη.

Η αξία του εισιτηρίου, ανάλογα με το πεδίο εφαρμογής, αφαιρείται από το ποσό που είναι αποθηκευμένο στη κάρτα κάθε φορά που ο κάτοχος περνάει από την ειδική συσκευή ανάγνωσης / γραφής και μπορεί να επαναφορτώνεται στο κατάλληλο σημείο πώλησης. Αυτός ο τρόπος παρέχει ευκολία στους καταναλωτές και με τη χρήση ειδικών "επιβραβευτικών" προγραμμάτων στις συγκοινωνίες, αυξάνει τη χρήση των μέσων μαζικής μεταφοράς, προσελκύοντας περισσότερους καταναλωτές.

Ειδικά στην περίπτωση των διοδίων, η χρήση των έξυπνων καρτών συμβάλει πολύ στην εξυπηρέτηση του κοινού αφού επιτρέπει την συλλογή διοδίων χωρίς τη παρεμπόδιση της κυκλοφορίας. Στις περιοχές συλλογής των διοδίων υπάρχουν ειδικές συσκευές ανάγνωσης και πάνω στα διερχόμενα οχήματα υπάρχουν ειδικές συσκευές για τις

έξυπνες κάρτες ούτως ώστε με τη διέλευση του οχήματος από το σημείο συλλογής, η χρέωση να γίνεται αυτόματα χωρίς να χρειάζεται να δημιουργούνται ουρές.

2.5.5 Banking / E-purse

Ο οικονομικός και τραπεζικός χώρος ήταν από τους πρώτους που υιοθέτησαν την τεχνολογία των έξυπνων καρτών σε πολλές χώρες παγκοσμίως. Κάθε Γαλλική χρεωστική κάρτα VISA έχει πλέον μικροτσίπ. Χώρες όπως η Πορτογαλία και η Σιγκαπούρη έχουν εισάγει προγράμματα ηλεκτρονικού πορτοφολιού στα εθνικά τραπεζικά δίκτυά τους.

Οι έξυπνες κάρτες χρησιμοποιούνται από τις τράπεζες είτε ως πιστωτικές είτε ως χρεωστικές, εις αντικατάσταση των υπάρχουσων καρτών μαγνητικής ταινίας. Οι πιστωτικές κάρτες δίνουν πληροφορίες για το πιστωτικό λογαριασμό του κατόχου ο οποίος θα χρεωθεί μετά από μία αγορά και είναι ένας τρόπος να δοθεί μία "πίστωση χρόνου" στον κάτοχό της για την πληρωμή, ένας τρόπος άτοκου (μέχρι ενός ορισμένου χρονικού διαστήματος) δανεισμού. Οι χρεωστικές κάρτες δίνουν πληροφορίες για τον καταθετικό λογαριασμό του κατόχου της κάρτας και η οποιαδήποτε αγορά χρεώνεται κατευθείαν στο λογαριασμό, είναι δηλαδή μία άμεση πληρωμή χωρίς μετρητά.

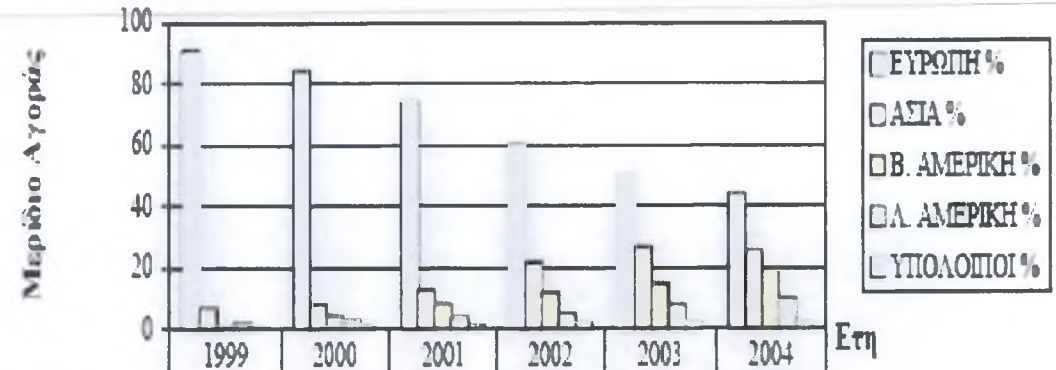
Η πιστοποίηση της ταυτότητας του κατόχου μίας κλασικής πιστωτικής κάρτας γίνεται με παρατήρηση της υπογραφής του και της ταυτότητας του, ενώ στην περίπτωση των συνηθισμένων χρεωστικών καρτών (debit cards) υπάρχει ένας κωδικός (PIN) που επαληθεύεται όμως μόνο on-line. Οι έξυπνες κάρτες έρχονται να αλλάξουν αυτό το τοπίο αφού ο κωδικός του κατόχου είναι αποθηκευμένος στην ίδια την κάρτα και προστατεύεται όπως και επαληθεύεται με ασφαλείς διαδικασίες που παρέχει η κάρτα.

Έτσι οι κάρτες αυτές γίνονται πιο ασφαλείς και για τις καινούριες τραπεζικές υπηρεσίες που παρέχονται στους πελάτες, όπως το web-banking, αυξάνοντας την ποιότητα εξυπηρέτησης των πελατών. Συγχρόνως, μειώνεται το λειτουργικό κόστος των πιστωτικών ιδρυμάτων αφού εργασίες που θα απαιτούσαν καθημερινή ανθρώπινη εργασία γίνονται με ηλεκτρονικό τρόπο.

Η τεχνολογία των έξυπνων καρτών ευνοεί και τους πωλητές λιανικής αφού με την ασφάλεια που παρέχει μειώνει το κόστος από απώλειες λόγω απατών ή λαθών.

Στο διάγραμμα που ακολουθεί στο Σχήμα 2.5.1 βλέπουμε πώς κινείται η αγορά των έξυπνων τραπεζικών καρτών παγκοσμίως και παρατηρούμε πως το μεγαλύτερο μερίδιο κατέχει σταθερά η Ευρώπη, το μέγεθος όμως του μεριδίου ελαττώνεται με την πάροδο των ετών, καθώς η τεχνολογία αυτή εξαπλώνεται στις άλλες ηπείρους.

ΑΝΑΛΥΣΗ ΜΕΡΙΔΙΩΝ ΑΓΟΡΑΣ ΤΡΑΠΕΖΙΚΩΝ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ



	1999	2000	2001	2002	2003	2004
ΕΥΡΩΠΗ %	90,82	84,09	73,92	59,85	49,49	43,82
ΑΣΙΑ %	6,61	7,78	12,63	21,85	26,46	25,17
Β. ΑΜΕΡΙΚΗ %	0,37	4,59	8,31	11,79	14,64	19,5
Λ. ΑΜΕΡΙΚΗ %	1,84	2,69	3,67	4,79	7,79	9,81
ΥΠΟΛΟΙΠΟΙ %	0,37	0,85	1,47	1,72	1,65	1,7

Σχήμα 2.5.1

Τέλος, το ηλεκτρονικό πορτοφόλι (e-purse/e-wallet) είναι ένας ακόμα τρόπος κατοχής ηλεκτρονικού χρήματος (κάτι αντίστοιχο με τις κάρτες προπληρωμένης αξίας όπως οι τηλεφωνικές κάρτες), με τη διαφορά ότι μπορεί να γίνει και πίστωση και χρέωση στην κάρτα, δίνοντας έτσι μεγαλύτερες δυνατότητες στο κάτοχο. Το ηλεκτρονικό πορτοφόλι προσφέρει στους κατόχους ευκολία χρήσης και ασφάλεια και προτείνεται κυρίως σε εφαρμογές που έχουν σχέση με το Διαδίκτυο.

2.5.6 Προγράμματα Εμπιστοσύνης

Πολλές εταιρίες χρησιμοποιούν έξυπνες κάρτες σε προγράμματα εμπιστοσύνης για να εντοπίζουν και να δίνουν κίνητρα αγοράς στους τακτικούς πελάτες.

Οι κάρτες αυτές είναι συνήθως κάρτες επαφής (contact cards) που μαζεύουν πόντους από αγορά προϊόντων ή υπηρεσιών από συγκεκριμένο πωλητή λιανικής. Οι πόντοι αυτοί ανταλλάσσονται με πιστώσεις, με βραβεία ή και άλλα στοιχεία. Μέσω του συστήματος αυτού, οι εταιρίες λιανικής πώλησης μπορούν για πρώτη φορά να έχουν λεπτομερή στοιχεία για τις προτιμήσεις των πελατών.

Ειδικά για μεγάλες αλυσίδες πωλήσεων που διαχειρίζονται προγράμματα εμπιστοσύνης σε διαφορετικά αντικείμενα (όπως τα πολυκαταστήματα), πληροφορίες για τον πελάτη και τις προτιμήσεις του διαχειρίζονται και αποθηκεύονται κεντρικά σε μία έξυπνη κάρτα που κατέχει όλες τις πληροφορίες και δίνει την δυνατότητα στις εταιρίες λιανικής πώλησης να κάνουν σωστό σχεδιασμό της πολιτικής προσέγγισης των πελατών. Έτσι παρέχεται μεγαλύτερη ποιότητα στην εξυπηρέτηση των πελατών και σαφώς τα έσοδα για τις εταιρίες είναι μεγαλύτερα.

2.5.7 Έλεγχος Πρόσβασης

Σημαντική δραστηριότητα έχει παρουσιαστεί από μεγάλες εταιρίες και οργανισμούς, καθώς και από κυβερνήσεις για την εισαγωγή καινούριων συστημάτων ελέγχου πρόσβασης, τα οποία ελέγχουν την ταυτότητα και τα επίπεδα εξουσιοδότησης κάποιου πριν του δοθεί πρόσβαση φυσική (σε κάποιο κτίριο για παράδειγμα) ή λογική (π.χ. σε εμπιστευτικές πληροφορίες σε δίκτυα).

Όσο περισσότερο οι ανωτέρω φορείς χρησιμοποιούν δίκτυα τοπικά και μη, και το Διαδίκτυο για να αποθηκεύουν και να κοινοποιούν σημαντικές πληροφορίες σε αυτούς που τις χρειάζονται, τόσο περισσότερο επεκτείνεται η χρήση των έξυπνων καρτών σε αυτό το τομέα.

Μεγάλες εμπορικές επιχειρήσεις όπως η Sun και η Microsoft, εφαρμόζουν συστήματα ελέγχου πρόσβασης που βασίζονται στη τεχνολογία των έξυπνων καρτών για να διαχειριστούν καθολικά την πρόσβαση εργαζομένων σε συγκεκριμένες πηγές.

Σε αυτή την κατεύθυνση, οι έξυπνες κάρτες προσφέρουν ταχύτητα πρόσβασης και μειωμένα κόστη συντήρησης (ειδικά στην περίπτωση του ασύρματου ελέγχου πρόσβασης), πολλαπλά επίπεδα ταυτοποίησης και πλήθος μεθόδων κρυπτογράφησης και πιστοποίησης, καθώς και ευελιξία στη χρησιμοποίηση διαφορετικών καρτών λόγω σταθερών προτύπων που ακολουθούνται.

2.5.8 Υγεία

Οι ιατρικές έξυπνες κάρτες χρησιμοποιούνται κατά κόρον σε πολλές χώρες παγκοσμίως. Η τάση των τελευταίων ετών είναι η μεταφορά από συστήματα πληροφοριών ιατρικής φροντίδας που βασίζονται σε χαρτιά και έγγραφα σε ηλεκτρονικά συστήματα τα οποία προστατεύουν τα προσωπικά δεδομένα των κατόχων των καρτών.

Οι έξυπνες ιατρικές κάρτες αποθηκεύουν πολλών ειδών ιατρικές πληροφορίες που αφορούν τον κάτοχο, όπως λεπτομέρειες για αλλεργίες και χρόνιες ασθένειες. Μπορούν να έχουν αποθηκευμένες παλιές, επαναλαμβανόμενες ή και νέες συνταγές ιατρών καθώς και διάφορες θεραπείες στις οποίες ο κάτοχος έχει υποβληθεί. Για τους ασθενείς, αυτός ο τρόπος αυξάνει την ποιότητα της παρεχόμενης ιατρικής φροντίδας, ενώ για τους παροχείς της ιατρικής βοήθειας, μειώνονται τα λειτουργικά κόστη και αυξάνεται η αποτελεσματικότητα της δράσης τους. Το κυριότερο είναι ότι με αυτή τη μέθοδο, σώζονται πραγματικά ζωές, αφού το ηλεκτρονικό ιατρικό ιστορικό του ασθενή είναι εύκολα προσβάσιμο και μπορεί να μεταφέρεται. Πολλές χώρες με εθνικά προγράμματα ιατρικής φροντίδας χρησιμοποιούν συστήματα έξυπνων καρτών, το μεγαλύτερο των οποίων λειτουργεί στη Γερμανία όπου πάνω από 80.000.000 κάρτες έχουν μοιραστεί σε κάθε άτομο στη Γερμανία και την Αυστρία.

2.5.9 Πανεπιστημιακοί χώροι

Πανεπιστήμια και σχολές σε πολλές χώρες χρειάζονται ένα τρόπο αναγνώρισης της ταυτότητας των εργαζομένων και των φοιτητών και χρησιμοποιούν τη τεχνολογία των έξυπνων καρτών για αυτό το σκοπό. Οι περισσότεροι από τους κατόχους αυτών των καρτών έχουν πρόσβαση σε συγκεκριμένες πληροφορίες, εξοπλισμό και τμήματα, ανάλογα με τις συνθήκες και τα χαρακτηριστικά της θέσης τους.

Έξυπνες κάρτες πολλαπλών διεργασιών περιέχουν τα στοιχεία ταυτότητας με χαρακτηριστικά πρόσβασης ενώ επίσης μπορούν να αποθηκεύουν αξία (χρήματα) για χρήση σε διάφορους χώρους εντός των πανεπιστημίων, όπως τα κυλικεία ή κάποια καταστήματα.

Γίνονται έτσι ένα εύκολο εργαλείο για τον εργαζόμενο και τον φοιτητή ο οποίος με μία κάρτα μπορεί να κινηθεί όπου επιθυμεί και να καλύψει τις ανάγκες του στο συγκεκριμένο χώρο.

Για παράδειγμα, το Πανεπιστήμια της Florida, έχει εκδώσει 40.000 κάρτες οι οποίες εξυπηρετούν λειτουργίες προσωπικής ταυτοποίησης, τραπεζικών συναλλαγών και πρόσβασης σε σπουδαστικούς χώρους για τους φοιτητές ενώ ταυτόχρονα λειτουργούν ως κάρτες προπληρωμένης αξίας για υπηρεσίες σίτισης, τηλεφωνίας και μετακίνησης μέσα στο Πανεπιστήμιο.

2.6 Βασικά Στοιχεία και Χαρακτηριστικά Έξυπνων Καρτών

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, 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 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.

- ***Υπολογιστική ισχύς***

Σήμερα χρησιμοποιούνται ελεγκτές σε συνδυασμό με έναν 32bit επεξεργαστή RISC που τρέχει στα 25-32 MHz.

2.7 Πλεονεκτήματα & Αδύνατα Σημεία

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.

2.8 Πλεονεκτήματα των Έξυπνων Καρτών

Τα βασικά πλεονεκτήματα της τεχνολογίας των smart card 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 στη

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.

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

2.9 Εμπόδια κατά την αποδοχή των Έξυπνων Καρτών

Υπάρχουν όμως και κάποιοι παράγοντες που εμποδίζουν την αποδοχή της τεχνολογίας έξυπνων καρτών. Μερικοί από αυτούς είναι:

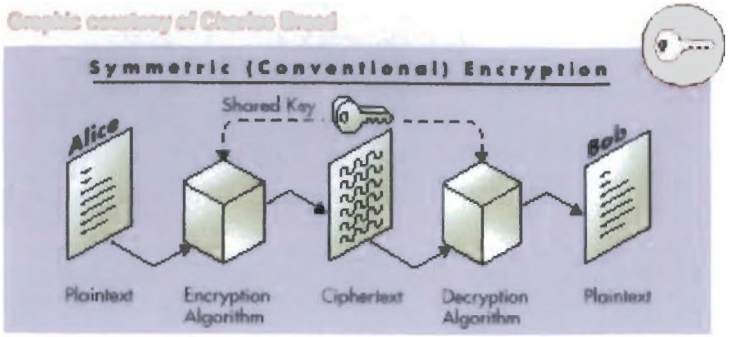
- Το σχετικά υψηλότερο κόστος των έξυπνων καρτών σε σύγκριση με τις μαγνητικές κάρτες. Βέβαια η διαφορά αυτή στο κόστος μεταξύ των δύο τεχνολογιών μειώνεται σημαντικά αν λάβουμε υπόψη τη διαφορά στην αναμενόμενη διάρκεια ζωής της κάρτας, καθώς και την ικανότητα υποστήριξης πολλαπλών εφαρμογών.
- Έλλειψη παρούσας υποδομής για να υποστηρίξει την έξυπνη κάρτα.
- Ο καταναλωτής πρέπει να είναι τεχνικά πεπειραμένος για να επιλέξει την πιό 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.

2.10 Έξυπνες Κάρτες & Ασφάλεια

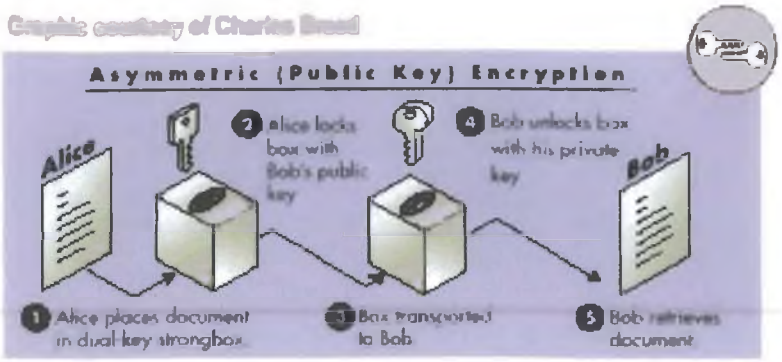
2.10.1 Αλγόριθμοι Κρυπτογράφησης

Υπάρχουν δυο είδη αλγορίθμων κρυπτογράφησης:

1. 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).



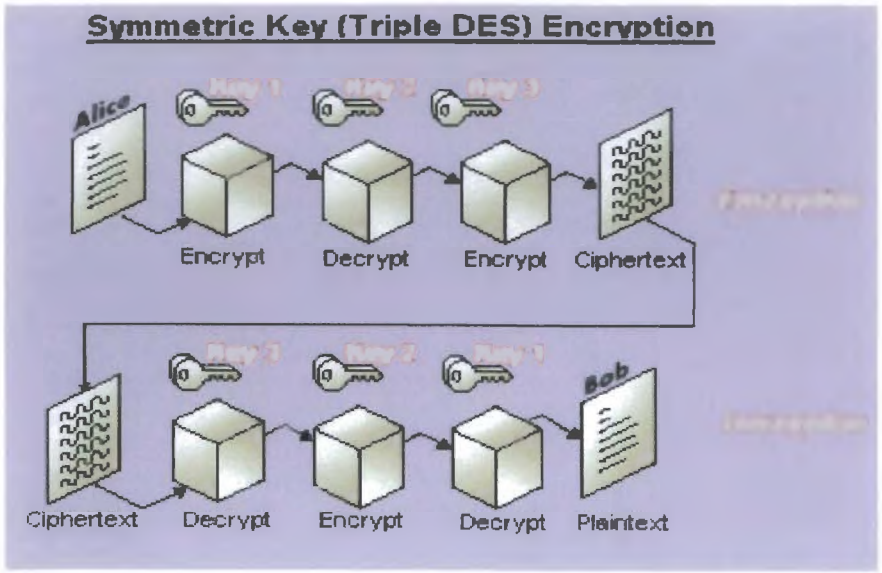
2. οι μη συμμετρικούς. Ο πιο γνωστός μη συμμετρικός αλγόριθμος είναι ο RSA, που πήρε το όνομά του από τους δημιουργούς του (Rivest, Shamir, και Adleman). Ο RSA χρησιμοποιεί δύο κλειδιά, που ονομάζονται **private key**.



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.



2.10.2 Δυνατότητες Κρυπτογράφησης

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 επαν-αρχικοποιήσει 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.

2.10.3 Χρήση Έξυπνων Καρτών για την ασφάλεια των δεδομένων

Υπάρχουν δύο τρόποι χρησιμοποίησης της κάρτας για την ασφάλεια συστημάτων host-based και card-based. Τα ασφαλέστερα συστήματα υιοθετούν και τις δύο μεθοδολογίες.

2.10.3.1 Σύστημα με Host-Based ασφάλεια

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.

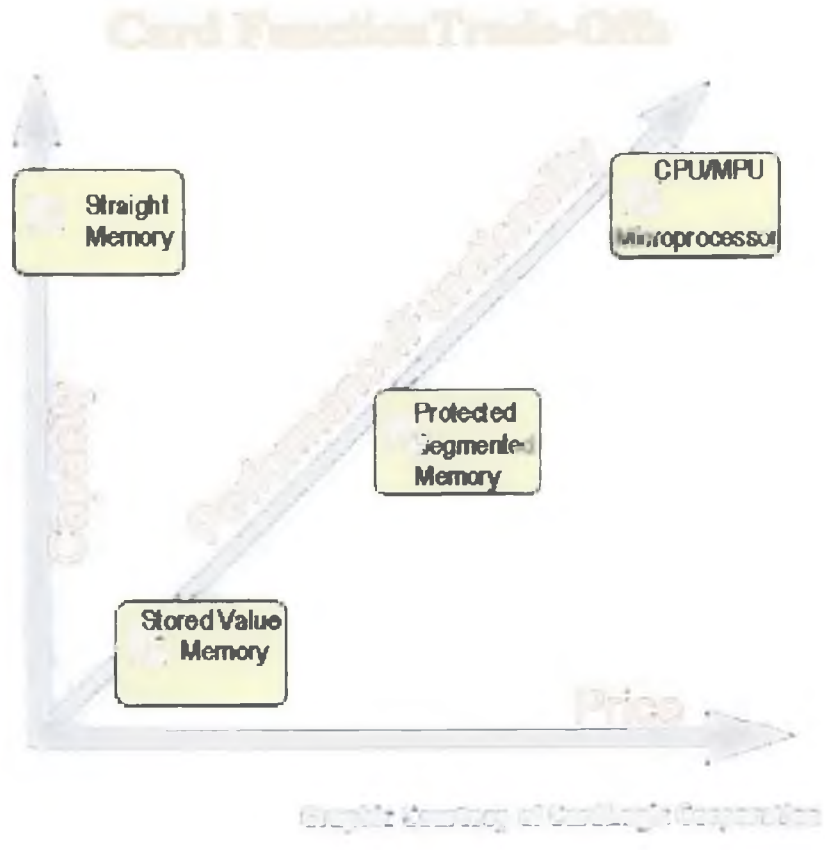
Δυστυχώς οι κωδικοί αυτοί είναι εύκολο να «εξουδετερωθούν». Αυτή η μεθοδολογία χρησιμοποιείται όταν κανείς εργάζεται τακτικά στα στοιχεία της κάρτας και μπορεί να παρακολουθεί τα περιεχόμενά της.

2.10.3.2 Σύστημα με Card -Based ασφάλεια

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.

2.11 Κριτήρια Επιλογής Κάρτας

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.



Αν κανείς πραγματοποιήσει μια έρευνα αγοράς για έξυπνες κάρτες που ικανοποιούν τις ανάγκες μιας εφαρμογής που τον ενδιαφέρει, θα καταλήξει στο συμπέρασμα ότι κυκλοφορούν αρκετά προϊόντα στην αγορά και από διάφορους προμηθευτές. Πιο συγκεκριμένα, ύστερα από μια έρευνα στο Διαδίκτυο σχετικά με τις έξυπνες κάρτες που θα μπορούσαν να χρησιμοποιηθούν σε ένα Πανεπιστήμιο, συντάχθηκε ο παρακάτω πίνακας καρτών μόνο της εταιρείας Gemplus:

Όνομα κάρτας
GemClub-Memo
GemCombi/MPCOS Pro
GemEasy8000
GemSAFE an Entrust Ready solution
GemSAFE Libraries
GemSAFE Logon
GemTwin
GPM2K
GPM8K
MPCOS-EMV

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 στην κάρτα;

Ειδικά όσον αφορά στην Ασφάλεια

- Ποιες είναι οι απαιτήσεις σε ασφάλεια;
- Χρειάζονται όλα τα δεδομένα υψηλό επίπεδο ασφάλειας ή ορισμένα από αυτά;
- 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)

3

Τεχνολογία Έξυπνων Καρτών

Για να κατανοήσουμε τα τεχνικά χαρακτηριστικά των έξυπνων καρτών χρειάζεται να εξηγήσουμε περιληπτικά κάποιες βασικές ηλεκτρονικές έννοιες.

3.1 Βασικές Έννοιες

3.1.1 Μικροτσίπ

Το μικροτσίπ είναι ένα σύνολο πολύπλοκων και πολύ μικρών στοιχείων που μπορούν να αποθηκεύσουν υπολογιστική μνήμη ή να παρέχουν το λογικό κύκλωμα για μικροεπεξεργαστές. Κατασκευάζεται από λεπτά κυκλικά επίπεδα δισκία πυριτίου τα οποία επεξεργάζονται ως προς το μέγεθος και συνδέονται με κυκλώματα και ηλεκτρονικές συσκευές. Οι συσκευές αυτές χρησιμοποιούν τεχνολογία ημιαγωγών μετάλλου-οξειδίου. Το τρέχον στάδιο της ολοκλήρωσης των μικροτσίπ είναι το γνωστό VLSI (Very Large-Scale Integration). Το μικροτσίπ καλείται αλλιώς και ολοκληρωμένο κύκλωμα (IC).

3.1.2 VLSI

VLSI είναι όπως είπαμε, το παρόν επίπεδο "μικρογραφίας" μικροτσίπ υπολογιστών και αναφέρεται σε μικροτσίπ που περιέχουν εκατοντάδες χιλιάδες τρανζίστορ, δίνοντας έτσι τη δυνατότητα να παραχθούν μνήμες (RAM, ROM) ή μονάδες επεξεργασίας (CPU) σε ένα και μόνο τσιπ.

3.1.3 Μνήμη

Μνήμη είναι το ηλεκτρονικό μέρος αποθήκευσης εντολών και πληροφοριών στις οποίες ένας επεξεργαστής μπορεί εύκολα να έχει πρόσβαση. Σε έναν υπολογιστή που βρίσκεται σε κανονική λειτουργία, η μνήμη περιέχει κύρια μέρη του λειτουργικού συστήματος του

υπολογιστή και πολλά ή όλα τα προγράμματα εφαρμογών και τα δεδομένα που αυτά χρησιμοποιούν.

3.1.3.1 RAM

RAM (Random Access Memory - Μνήμη Τυχαίας Προσπέλασης) είναι μνήμη που περιέχεται σε ένα ή περισσότερα μικροτσίπ κοντά στον μικροεπεξεργαστή, έχει μικρό φυσικό μέγεθος και μικρή γενικά χωρητικότητα σε σχέση με άλλα αποθηκευτικά μέσα όπως ο σκληρός δίσκος και το CD-ROM. Είναι όμως πολύ πιο γρήγορη και άμεση η πρόσβαση στα δεδομένα της και οι διαδικασίες ανάγνωσης και εγγραφής γίνονται ταχύτερα (χρόνος πρόσβασης σε τάξη nanoseconds). Τα όποια δεδομένα και στοιχεία συστήματος αποθηκεύονται στη RAM, βρίσκονται εκεί μόνο όσο ο υπολογιστής λειτουργεί και χάνονται όταν το ρεύμα αφαιρεθεί.

Ο όρος "τυχαία προσπέλαση" αναφέρεται στο ότι η πρόσβαση σε αποθηκευμένη πληροφορία δεν γίνεται ακολουθιακά αλλά άμεσα.

3.1.3.2 ROM

Η ROM (Read Only Memory - Μνήμη Μόνο Ανάγνωσης) είναι μνήμη στην οποία δεν μπορούν να γίνουν εγγραφές, αλλά μόνο ανάγνωση. Η ROM περιέχει τα στοιχεία προγραμματισμού που επιτρέπουν σε ένα υπολογιστή να ξεκινήσει και δεν χάνει τα δεδομένα της όταν ο υπολογιστής κλείσει. Όταν η ROM συντηρείται με μπαταρία, αυτή είναι μία μικρή μεγάλης διάρκειας μπαταρία. Υπάρχουν και ROM που "χτίζονται" μία φορά κατά τη κατασκευή τους (firmware). Το κόστος μίας ROM μνήμης είναι μεγαλύτερο από αυτό της RAM.

3.1.3.3 EEPROM

Η EEPROM (Electrically Erasable Programmable Read-Only Memory) είναι μνήμη ROM που μπορεί να μεταβληθεί από τον χρήστη, δηλαδή μπορεί να σβηστεί και να επαναπρογραμματιστεί με την εφαρμογή υψηλότερης από την κανονική τάσης. Το κύριο χαρακτηριστικό της είναι ότι δεν μπορεί να σβηστεί και να προγραμματιστεί σε κομμάτια και αυτό μπορεί να γίνει χωρίς να μετακινηθεί από τον υπολογιστή. Έχει περιορισμένη διάρκεια ζωής αφού επιτρέπει περιορισμένο αριθμό επαναπρογραμματισμών ο οποίος φτάνει σε δεκάδες ή εκατοντάδες χιλιάδες φορές.

3.1.3.4 FLASH

Η μνήμη FLASH είναι ένας τύπος μνήμης EEPROM με τη βασική διαφορά να έγκειται στη ταχύτητα της διαγραφής και επαναπρογραμματισμού του περιεχομένου της. Συγκεκριμένα, ενώ στην EEPROM μπορεί να διαγραφεί ένα byte τη φορά, στη μνήμη FLASH μπορούν να σβηστούν ολόκληρα μπλοκ από byte, αυξάνοντας έτσι την ταχύτητα διαγραφής και προγραμματισμού της μνήμης αυτής.

3.1.4 Επεξεργαστής

Ο επεξεργαστής είναι η λογική κυκλωματική συνδεσμολογία που επεξεργάζεται και ανταποκρίνεται σε βασικές εντολές που οδηγούν ένα υπολογιστή. Ο όρος "επεξεργαστής" έχει γενικά αντικαταστήσει τον όρο Κεντρική Μονάδα Επεξεργασίας (CPU). Ο επεξεργαστής σε ένα προσωπικό υπολογιστή ή ενσωματωμένος σε μικρές συσκευές καλείται συχνά "μικροεπεξεργαστής".

3.1.5 Μικροεπεξεργαστής

Ο μικροεπεξεργαστής είναι ένας επεξεργαστής υπολογιστή σε μικροτσίπ. Μερικές φορές καλείται "λογικό τσιπ". Είναι σχεδιασμένος για να εκτελεί αριθμητικές και λογικές διεργασίες που χρησιμοποιούν μικρές περιοχές καταγραφής αριθμών που καλούνται καταχωρητές. Τυπικές τέτοιες διεργασίες είναι η πρόσθεση, αφαίρεση ή σύγκριση δύο αριθμών ή η μεταφορά αριθμών από μία περιοχή σε άλλη. Αυτές οι διεργασίες είναι αποτέλεσμα ενός συνόλου εντολών που αποτελούν μέρος του σχεδιασμού του μικροεπεξεργαστή.

3.1.6 Εντολές

Μία εντολή είναι μία διαταγή που δίνεται σε ένα επεξεργαστή από ένα υπολογιστικό πρόγραμμα. Στο πιο χαμηλό επίπεδο (επίπεδο μηχανής), κάθε εντολή είναι μία ακολουθία από μηδενικά και άσσους που περιγράφουν μία φυσική διεργασία που θα εκτελέσει ο υπολογιστής ή η ταυτότητα των καταχωρητών που θα χρησιμοποιηθούν για την εντολή. Στη γλώσσα assembly ενός υπολογιστή μία δήλωση αντιστοιχεί σε μία εντολή μικροεπεξεργαστή ενώ σε γλώσσες υψηλότερου επιπέδου, αντιστοιχεί σε σετ εντολών.

3.1.7 Private Key

Ένα private (secret) key είναι μία κλείδα (ένας κωδικός) που χρησιμοποιείται για κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων μέσα στα πλαίσια της επικοινωνίας δύο πλευρών. Το κλειδί αυτό προφανώς είναι κοινώς γνωστό στις δύο πλευρές που επικοινωνούν και συνεπακόλουθα αν μία από τις δύο πλευρές το χάσει ή το κλειδί κλαπεί, η ασφάλεια και η μυστικότητα της επικοινωνίας θα χαθεί.

3.1.8 Public Key

Ένα public key είναι πάλι ένας κωδικός, ο οποίος όμως σε συνδυασμό με ένα private key το οποίο παράγεται από το public key, χρησιμοποιείται για ασφαλή κρυπτογράφηση μηνυμάτων και δημιουργία ψηφιακών υπογραφών. Η συνδυαστική χρήση public και private keys είναι γνωστή ως ασύμμετρη κρυπτογράφηση.

3.2 Τύποι καρτών

Υπάρχουν διάφορες κατηγορίες στις οποίες χωρίζονται οι έξυπνες κάρτες, ανάλογα με το τύπο της διεπαφής τους (interface) με τον έξω κόσμο ή ανάλογα με το τύπο του μικροτσίπ.

3.2.1 Contact Cards

Οι κάρτες με επαφή χρειάζεται να εισαχθούν μέσα σε ένα card reader (αναγνώστη καρτών) ο οποίος θα έχει άμεση επαφή με το λεπτό μεταλλικό πιάτο που βρίσκεται στην επιφάνεια της κάρτας (κάτω από το οποίο βρίσκεται το μικροτσίπ), για να επιτευχθεί η επικοινωνία μεταξύ τους μέσω αυτών των ηλεκτρικών επαφών και για να πάρουν ρεύμα.

Η επικοινωνία συνίσταται στην ανταλλαγή εντολών, δεδομένων και πληροφοριών κατάστασης. Οι επαφές πρέπει να βρίσκονται σε αυστηρά καθορισμένο επίπεδο και να μην υπάρχει μεταξύ τους μη αγώγιμο υλικό.

Σχήμα 3.2.1 - Επαφές κάρτας

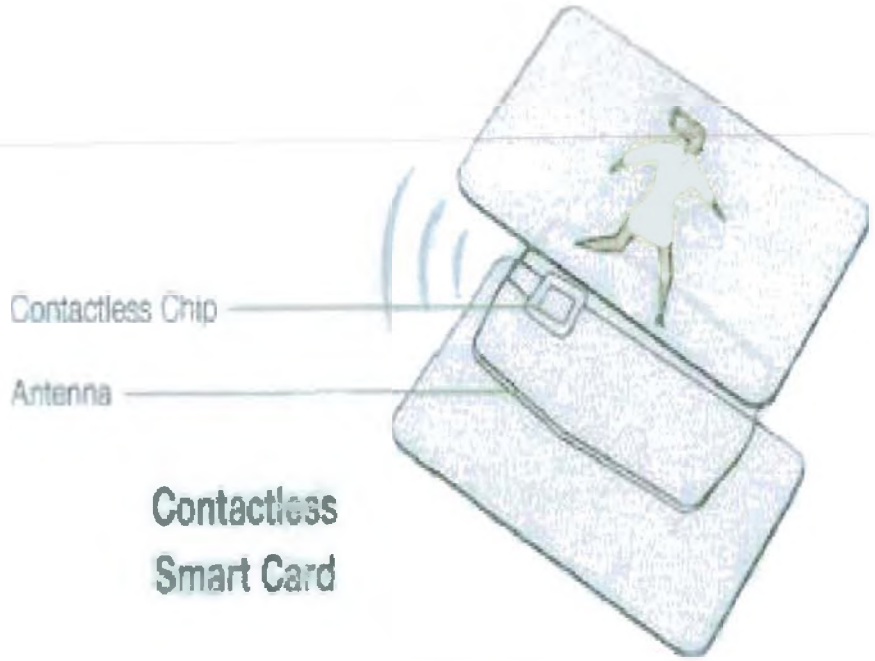
Στο παραπάνω σχήμα φαίνονται οι ηλεκτρικές επαφές στην επιφάνεια της κάρτας, των οποίων η θέση καθορίζεται από παγκόσμια πρότυπα (ISO 7816-1 και ISO 7816-2).

Οι λειτουργίες των επαφών αναλύονται ακολούθως. Η επαφή C1 αντιστοιχεί στη Vcc που είναι η τάση τροφοδοσίας και συνήθως είναι στα 5V. Η επαφή C2 αντιστοιχεί στο Reset που είναι η γραμμή σήματος η οποία χρησιμεύει για να αρχικοποιήσει την κατάσταση του ολοκληρωμένου κυκλώματος μετά τη τροφοδοσία της κάρτας. C3 είναι η επαφή που συνδέεται με το σήμα ρολογιού (Clock) το οποίο οδηγεί την λογική του ολοκληρωμένου και συγχρόνως χρησιμοποιείται ως σημείο αναφοράς για τη σειριακή σύνδεση επικοινωνίας. Οι επαφές C4 και C8 δεν χρησιμοποιούνται. Η επαφή C5 αντιστοιχεί στο GND (γείωση) που είναι σημείο μηδενικού δυναμικού και βάση του οποίου μετριέται η τάση τροφοδοσίας. C6 είναι η επαφή που αντιστοιχεί στη Vpp, στην υψηλή δηλαδή τάση που χρησιμοποιείται για να προγραμματιστεί η EEPROM μνήμη. Τέλος, η επαφή C7 αντιστοιχεί στη σειριακή θύρα εισόδου-εξόδου η οποία χρησιμοποιείται για την ανταλλαγή και τη λήψη εντολών και πληροφοριών από τον εξωτερικό κόσμο.

Οι κάρτες με επαφή μειονεκτούν στο ότι έχουν περιορισμένη διάρκεια ζωής λόγω φθοράς. Τα κυκλώματα στη κάρτα μπορεί να καταστραφούν από παράγοντες όπως οι ηλεκτροστατικές εκκενώσεις ή η κακή χρήση των καρτών από τους κατόχους.

3.2.2 Contactless Cards

Οι ασύρματες κάρτες χρειάζεται μόνο να βρίσκονται κοντά σε ένα reader και δεν απαιτείται φυσική επαφή. Η κάρτα έχει εσωτερικά ενσωματωμένη κεραία όπως και ο reader και επικοινωνούν μέσω αυτού του ασύρματου συνδέσμου. Οι περισσότερες ασύρματες κάρτες παίρνουν και το ρεύμα για τη λειτουργία του τσιπ τους από το ηλεκτρομαγνητικό σήμα μεταξύ κάρτας και reader.



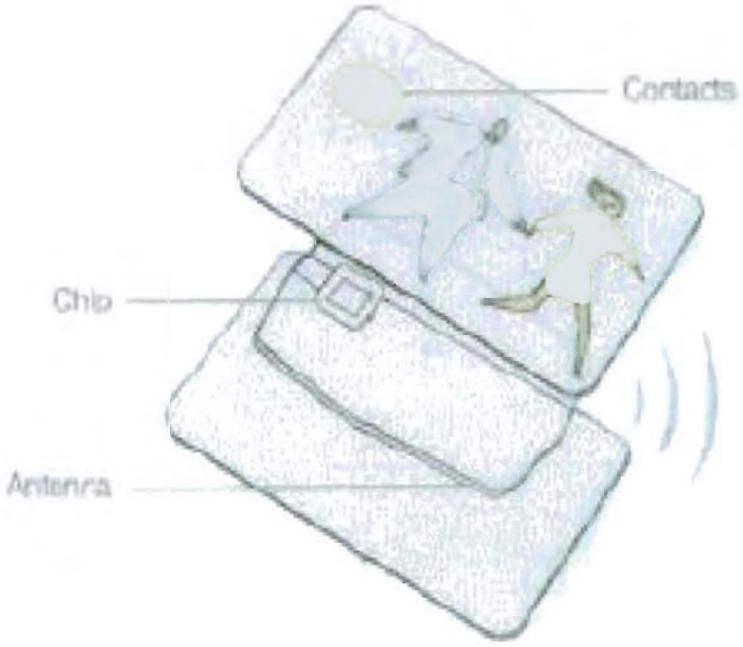
Στη παραπάνω εικόνα φαίνονται τα τρία στρώματα που στοιχειοθετούν μία ασύρματη κάρτα. Το πάνω και το κάτω στρώμα (εξωτερικά στρώματα) κλείνουν εσωτερικά το επίπεδο με την κεραία και το μικροτσίπ. Η κεραία είναι συνήθως 3 - 5 στροφές από πολύ λεπτό σύρμα (ή αγώγιμο μελάνι) που συνδέεται με το μικροτσίπ.

Οι ασύρματες κάρτες χρησιμοποιούνται κυρίως σε εφαρμογές και χώρους όπου οι συναλλαγές πρέπει να γίνονται πολύ γρήγορα, όπως για παράδειγμα στα μέσα συγκοινωνίας και στους σταθμούς διοδίων. Είναι πιο ακριβές από τις κάρτες επαφής αλλά έχουν μεγαλύτερη διάρκεια ζωής και είναι πιο αξιόπιστες.

3.2.3 Combi – Hybrid Cards

Από τις παραπάνω κατηγορίες καρτών που ορίστηκαν ως προς τον τύπο του interface τους, προκύπτουν και δύο ακόμα τύποι, οι Combi και οι Hybrid κάρτες. Οι κάρτες Hybrid, οι οποίες ήδη κυκλοφορούν στην αγορά, έχουν δύο τσιπ, ένα με επαφές και ένα για ασύρματη επικοινωνία. Τα δύο τσιπ δεν επικοινωνούν μεταξύ τους. Υπάρχουν ήδη εφαρμογές στις οποίες αυτός ο τύπος καρτών εξυπηρετεί τους καταναλωτές αλλά και τους παροχείς των καρτών.

Οι κάρτες Combi από την άλλη, ενσωματώνουν και τους δύο τύπους interface σε μία κάρτα με ένα τσιπ. Δηλαδή μπορεί να υπάρχει πρόσβαση στο ίδιο μικροτσίπ και μέσω ηλεκτρικών επαφών στην επιφάνεια της κάρτας και μέσω ασύρματης επικοινωνίας με τη χρήση της κεραίας. Στις κάρτες αυτές το επίπεδο ασφαλείας είναι πολύ υψηλό.



Σχήμα 3.2.3 – Combi Card

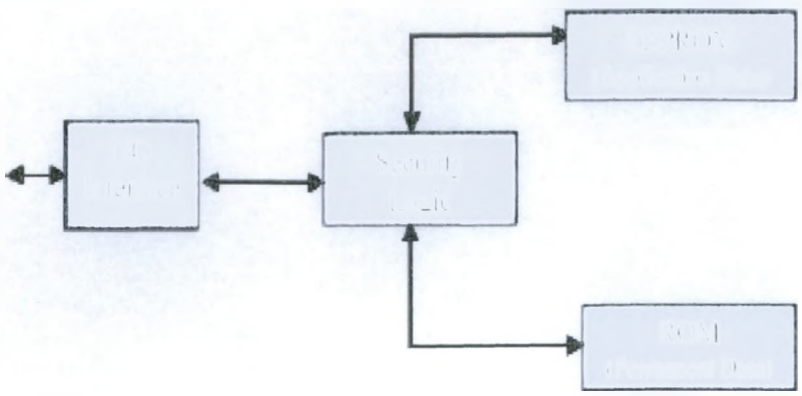
Οπως βλέπουμε και στην παραπάνω εικόνα, στην ίδια κάρτα το μικροτσίπ μπορεί να έχει επικοινωνία με τον εξωτερικό κόσμο μέσω των ηλεκτρικών επαφών στην επιφάνεια της κάρτας και μέσω της κεραίας που το περιβάλλει στο εσωτερικό στρώμα της κάρτας. Το ασύρματο τσιπ χρησιμοποιείται για εφαρμογές που χρειάζονται γρήγορες συναλλαγές και το τσιπ με τις ηλεκτρικές επαφές για εφαρμογές που απαιτούν μεγαλύτερη ασφάλεια.

Οι κάρτες αυτές αναμένεται να έχουν μεγάλη απορρόφηση στο χώρο των μέσων μαζικής μεταφοράς και στο τραπεζικό τομέα.

3.2.4 Memory Cards

Εξετάζοντας τις κάρτες ως προς τον τύπο του μικροτσίπ που περιέχουν, προκύπτουν δύο κατηγορίες καρτών: οι κάρτες μνήμης (memory cards) και οι κάρτες με μικροεπεξεργαστή (microprocessor cards).

Οι κάρτες μνήμης δεν έχουν επεξεργαστική δύναμη και δεν μπορούν να χειριστούν αρχεία δυναμικά. Ένα τσιπ μνήμης μπορεί να θεωρηθεί ως μία δισκέτα με διάφορες χωρητικότητες και με προαιρετική ασφάλεια. Οι κάρτες αυτές επικοινωνούν με το reader με σύγχρονα πρωτόκολλα τα οποία θα εξηγήσουμε παρακάτω. Είναι πιο κοινές και φτηνές από τις microprocessor κάρτες αλλά μειονεκτούν στα θέματα προστασίας και διαχείρισης δεδομένων. Μπορούν να αποθηκεύσουν από μερικές εκατοντάδες bit ως συνήθως 16Kbyte πληροφορίας. Γενικά οι κάρτες μνήμης περιέχουν δύο είδη μνήμης, μνήμη EEPROM και μνήμη ROM. Η μνήμη EEPROM χρησιμοποιείται για την αποθήκευση των δεδομένων της εκάστοτε εφαρμογής και μπορεί να προστατεύεται τμηματικά ή στην ολότητά της από κάποιο κωδικό. Ο κωδικός αυτός μπορεί να παρέχεται από το reader ή από τον κάτοχο της κάρτας κατά τη χρήση της. Η μνήμη ROM χρησιμοποιείται για την αποθήκευση δεδομένων που δεν αλλάζουν στη διάρκεια ζωής της κάρτας, όπως ο αναγνωριστικός αριθμός της κάρτας, τα στοιχεία του κατόχου της κάρτας κ.α.



Σχήμα 3.2.4 – Δομή Κάρτας Μνήμης

Επίσης οι κάρτες μνήμης μπορούν να περιέχουν στη μνήμη τους μία εφαρμογή η οποία δεν εκτελείται από τις ίδιες τις κάρτες που δεν έχουν δύναμη επεξεργασίας, αλλά από τις συσκευές υποδοχής των καρτών με τις οποίες επικοινωνούν.

Αναλύοντας λίγο παραπάνω τη τεχνολογία των καρτών μνήμης, μπορούμε να τις χωρίσουμε σε 3 υποκατηγορίες.

3.2.4.1 Straight Memory Cards

Οι κάρτες αυτές χρησιμεύουν μόνο για την αποθήκευση δεδομένων και δεν μπορούν να προσφέρουν καμία ασφάλεια. Είναι οι πιο φτηνές κάρτες μνήμης. Δεν μπορούν να δηλώσουν τη ταυτότητά τους στο reader, ο οποίος για να έχει επικοινωνία μαζί τους πρέπει εκ των προτέρων να γνωρίζει τι τύπου κάρτες είναι.

3.2.4.2 Protected / Segmented Memory Cards

Αυτές οι κάρτες έχουν ενσωματωμένη λογική για να ελέγχουν την πρόσβαση στη μνήμη. Μπορούν να προγραμματιστούν έτσι ώστε να προστατεύουν κομμάτια ή και ολόκληρη τη μνήμη από διαδικασίες εγγραφής / ανάγνωσης ή και τις δύο. Συνήθως αυτό γίνεται με τη χρήση κάποιου κωδικού ή κλειδιού συστήματος. Οι κάρτες αυτές έχουν τη δυνατότητα να χωριστούν σε λογικές ενότητες με στόχο την χρήση τους σε διαφορετικές ταυτόχρονες εφαρμογές (multi-functionality).

3.2.4.3 Stored Value Memory Cards

Οι κάρτες μνήμης αποθηκευμένης αξίας σχεδιάζονται μόνο για αποθήκευση αξίας ή "αποδείξεων". Μπορούν να είναι και επαναφορτιζόμενες, έχουν δηλαδή τη δυνατότητα με την εξάντληση της αποθηκευμένης αξίας να την ανανεώνουν αποθηκεύοντας καινούρια. Οι περισσότερες από αυτές τις κάρτες συσσωματώνουν στοιχεία ασφαλείας κατά την κατασκευή τους. Οι περιοχές μνήμης σχεδιάζονται και λειτουργούν είτε ως αφαιρέτες είτε ως μετρητές. Ελάχιστη ή καθόλου μνήμη περισσεύει για να χρησιμοποιηθεί σε κάποια άλλη λειτουργία.

3.2.5 Microprocessor Cards

Σε εφαρμογές που η ασφάλεια παίζει σημαντικό ρόλο χρησιμοποιούνται κάρτες με μικροεπεξεργαστή. Αυτές οι κάρτες είναι οι μόνες που μπορούν να χαρακτηριστούν τεχνικά ως έξυπνες κάρτες.

Οι μικροεπεξεργαστές λειτουργούν όπως ένας υπολογιστής με θύρα εισόδου / εξόδου, λειτουργικό σύστημα και σκληρό δίσκο. Μπορούν να αποθηκεύσουν και να επεξεργαστούν δεδομένα, κυρίως όμως ξεχωρίζουν λόγω της δυνατότητάς τους για δυναμική κρυπτογράφηση και για ενημερώσεις στις λογισμικές εφαρμογές τους. Αυτό σημαίνει ότι μπορεί να προσθέσει ή να αφαιρέσει εφαρμογές ή ακόμα να βελτιώσει μία υπάρχουσα εφαρμογή, γεγονός που κάνει τις microprocessor κάρτες πολύ ευέλικτες.

Ο επεξεργαστής μπορεί να υποστηρίξει διαδικασίες εγγραφής, ανάγνωσης και ενημέρωσης πληροφορίας καθώς και κρυπτογράφησης / αποκρυπτογράφησης δεδομένων αποθηκευμένων στην EEPROM. Χειρίζεται την κατανομή της μνήμης και τη πρόσβαση σε αρχεία και οργανώνει την πληροφορία σε συγκεκριμένες δομές αρχείων μέσω ενός λειτουργικού συστήματος της κάρτας (Card Operating System – COS).

Οι κάρτες με μικροεπεξεργαστή αποτελούνται κυρίως από τα ακόλουθα στοιχεία:

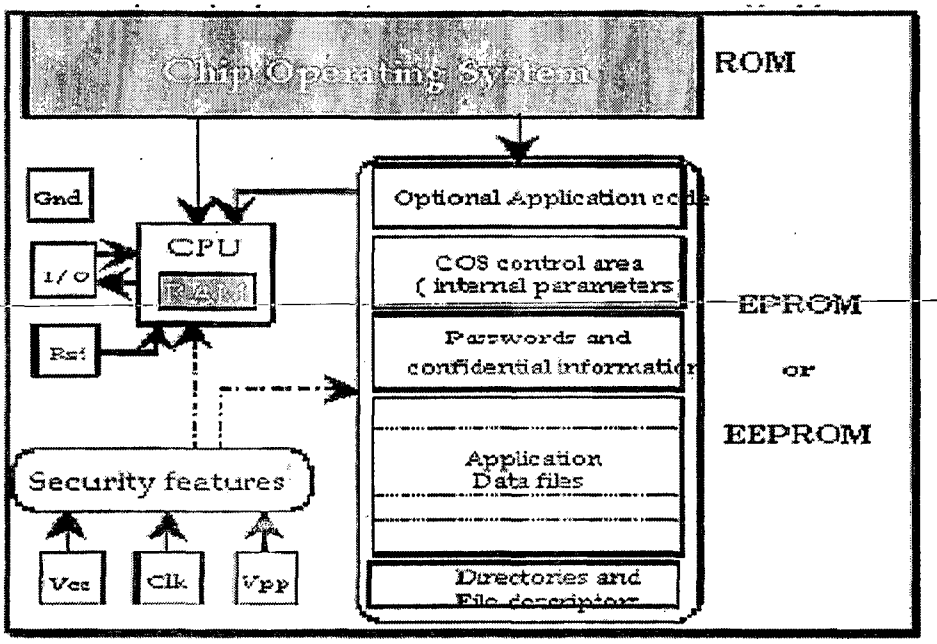
• ROM: η μνήμη ROM περιέχει το λειτουργικό σύστημα της κάρτας και καλείται αλλιώς "μάσκα" (mask) της κάρτας. Οι διάφορες εντολές γράφονται μόνιμα στη μνήμη από τον κατασκευαστή της κάρτας κατά την κατασκευή της. Το μέγεθός της κινείται από μερικά Kbyte μέχρι τα 32Kbyte, ανάλογα με το λειτουργικό σύστημα που χρησιμοποιείται.

• EEPROM: η μνήμη αυτή περιέχει τα προγράμματα εφαρμογών της κάρτας και τα αντίστοιχα δεδομένα των εφαρμογών. Τα περιεχόμενά της δεν είναι μόνιμα, μπορούν δηλαδή να διαγραφούν και να επανεγγραφούν.

• RAM: η μνήμη αυτή χρησιμεύει για την προσωρινή αποθήκευση αποτελεσμάτων από υπολογισμούς ή στοιχείων της επικοινωνίας με τον έξω κόσμο. Τα περιεχόμενά της διαγράφονται όποτε η κάρτα αποσυνδέεται από το ρεύμα.

• CPU: η κεντρική μονάδα επεξεργασίας είναι η καρδιά της microprocessor κάρτας. Η μονάδα επεξεργασίας έχει την ευθύνη της εκτέλεσης διαφόρων εντολών.

Η γενική αρχιτεκτονική του μικροτσίπ φαίνεται στο ακόλουθο διάγραμμα.



Σχήμα 3.2.5 – Αρχιτεκτονική Μικροτσίπ

Όπως αναφέραμε και προηγουμένως, οι κάρτες αυτές έχουν τη δυνατότητα να τρέχουν και να ανανεώνουν τις εφαρμογές τους. Ας αναλύσουμε όμως λίγο τι εννοούμε με τον όρο "εφαρμογή". Στο χώρο των έξυπνων καρτών ο όρος εφαρμογή χρησιμοποιείται για να περιγράψει το λογισμικό ή το πρόγραμμα που η κάρτα εφαρμόζει. Στην πιο απλή περίπτωση, εφαρμογή μπορεί να είναι ένας διαχειριστής αρχείων για την οργάνωση της αποθήκευσης και της ανάκτησης πληροφοριών. Μία τέτοια εφαρμογή μπορεί να σχεδιασθεί και να πραγματοποιηθεί κατευθείαν στη λογική του μικροτσίπ. Αντίστοιχα το τσιπ πρέπει να έχει τη κατάλληλη λογική σχεδίαση για την επίτευξη επικοινωνίας, μέσω της οποίας θα δέχεται εντολές από το reader καθώς και θα λαμβάνει και θα μεταδίδει τα δεδομένα της εφαρμογής.

Οι κάρτες με μικροεπεξεργαστή μπορούν να υποστηρίξουν και πιο προηγμένες εφαρμογές αφού η CPU μπορεί πέρα από την επεξεργασία δεδομένων να πάρει και αποφάσεις πάνω σε θέματα - πράξεις που ανακύπτουν.

3.3 Πρότυπα

3.3.1 Η ανάγκη για πρότυπα

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:
    1. τη δυνατότητα χρησιμοποίησης
    2. την ασφάλεια
    3. την εμπιστοσύνη προς φορείς
    4. το σχεδιασμό με βάση τις ανάγκες όλων των πολιτών

Ακολουθεί παρουσίαση των πιο σημαντικών προτύπων σχετικά με τις έξυπνες κάρτες.

3.3.2 Επίσημα Πρότυπα

3.3.2.1 Πρότυπο ISO- 7816

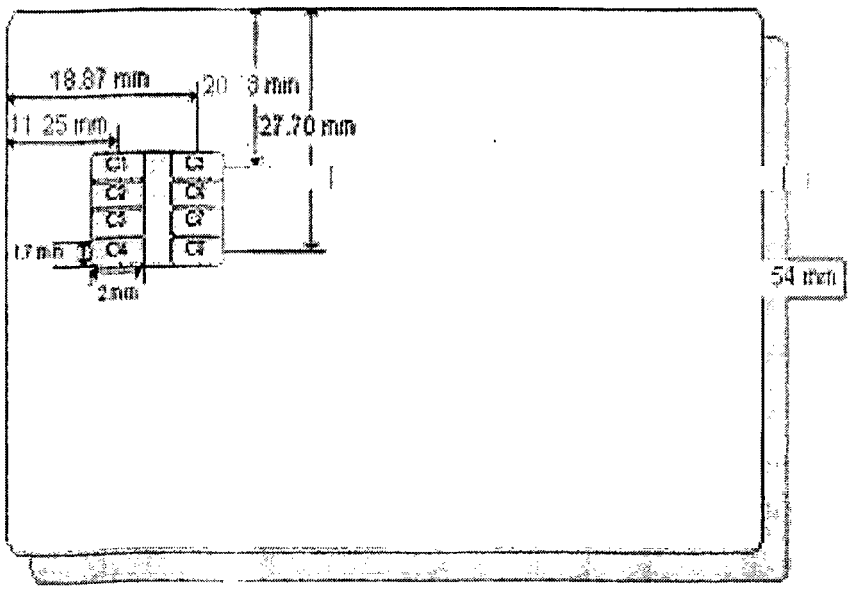
Η τυποποίηση των συστημάτων έξυπνων καρτών είναι μια διαδικασία που συνεχίζεται μέχρι σήμερα. Το πιο σημαντικό πρότυπο που μπορεί να αναφέρει κανείς σχετικά με τις έξυπνες κάρτες είναι η ομάδα προτύπων ISO- 7816. Πρόκειται για πρότυπα που έχουν καθιερωθεί από το Διεθνή Οργανισμό Τυποποίηση (International 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 6 πρώτα από τα οποία παρατίθενται στον ακόλουθο πίνακα:

ISO7816	Περιγραφή
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 αναγνώριση εφαρμογών
ISO 7816-6	Interindustry data elements

3.3.2.1.1 ISO 7816-1: Φυσικά Χαρακτηριστικά των καρτών ολοκληρωμένων Κυκλωμάτων

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



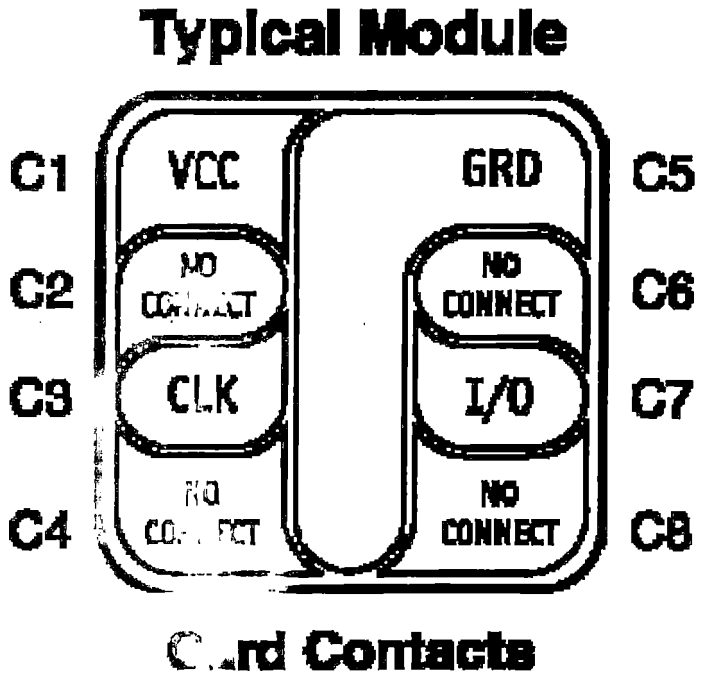
Εικόνα 5 [5]

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.

3.3.2.1.2 ISO 7816-2: Διαστάσεις και θέση των επαφών

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. 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 μέσω της οποίας το IFD μπορεί να 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	Ground line providing common electrical ground between the IFD and the ICC Επίσεια γραμμή που παρέχει το κοινό ηλεκτρικό έδαφος μεταξύ του IFD και του ICC
C6	Vpp	Σύνδεση που χρησιμοποιείται για τον προγραμματισμό της EEPROM
C7	I/O	Γραμμή εισόδου/εξόδου που παρέχει ένα ημι-αμφίδρομο κανάλι επικοινωνίας μεταξύ του αναγνώστη και της έξυπνης κάρτας (Input/Output line)
C8	RFU	Δεσμεύεται για χρήση στο μέλλον (Reserved for Future Use)

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.

3.3.2.1.3 ISO 7816-3: Ηλεκτρονικά Σήματα & Πρωτόκολλα Μετάδοσης

Στο τμήμα αυτό του προτύπου περιγράφονται τα ηλεκτρονικά σήματα και τα πρωτόκολλα μετάδοσης των καρτών ολοκληρωμένων κυκλωμάτων.

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 μικροελεγκτή είτε από τη σειριακή/παράλληλη/USB/PCMCIA θύρα ενός PC. Είναι ιδιαίτερα ενδιαφέρον να δει κανείς τι πληροφορίες μπορεί να πάρει από την ανταπόκριση Answer to Reset (ATR) μιας κάρτας.

ISO7816 3.1 Voltage and current values

ISO7816 3.2 Operating procedure for integrated circuit(s) cards

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:

a. σύνδεση και ενεργοποίηση των επαφών από τη συσκευή
b. reset της κάρτας
c. ανταπόκριση από την κάρτα με το σήμα Answer To Reset
d. ανταλλαγή πληροφοριών μεταξύ κάρτας και συσκευής
e. απενεργοποίηση των επαφών από τη συσκευή (όταν η συναλλαγή έχει πραγματοποιηθεί ή έχει εντοπιστεί απομάκρυνση της κάρτας από τη συσκευή)

ISO7816 3.3 Answer to Reset

Υπάρχουν δυο τρόποι για μετάδοση της απάντησης:

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

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

ISO7816 3.4 Protocol type selection (PTS)

ISO7816 3.5 Protocol type T=0, asynchronous half duplex character

ISO7816 3.5.a - Specific interface parameters: the work waiting time

ISO7816 3.5.b - Structure and processing of commands

Παρατηρήσεις:

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.

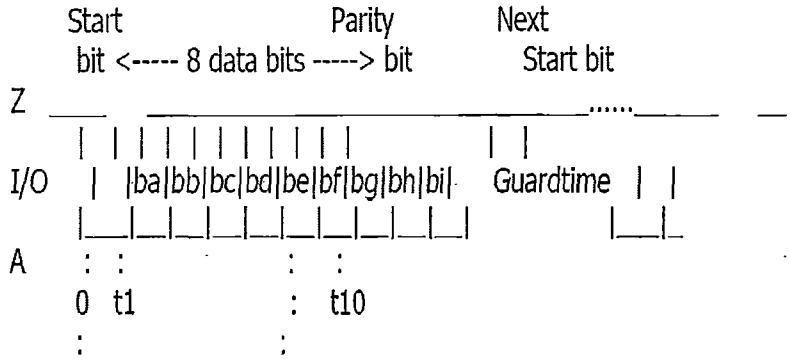
3 - Το RESET αρχίζει από τη συσκευή. Μέχρι το τέλος της ενεργοποίησης των επαφών, η κάρτα είναι έτοιμη για reset. Αφού ρυθμιστεί το σήμα του ρολογιού CLK και η I/O line, η κάρτα ύστερα από κάποιο χρονικό διάστημα (κύκλους του ρολογιού) πρέπει να επιστρέψει την απάντηση ATR. Αν μέσα στο προβλεπόμενο χρονικό 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 παρακάτω 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.



Σχήμα 3: Πλαίσιο Χαρακτήρα

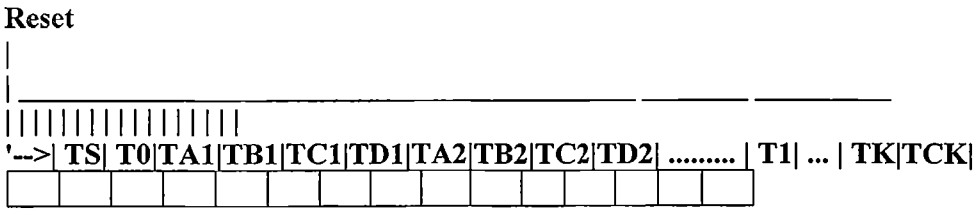
Εντοπισμός λαθών και επανάληψη χαρακτήρα

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

Δομή και περιεχόμενο ATR

Η απάντηση ATR της κάρτας αποτελείται από έναν αρχικό χαρακτήρα TS, ο οποίος ακολουθείται από τουλάχιστον 32 χαρακτήρες με την παρακάτω σειρά:

- T0 ..... Format character (Mandatory)
- **TAi, TBi, TCi, TDi ... Interface characters (Optional)**
- T1, T2, ... ,TK ..... Historical characters (Optional)
- TCK ..... Check character (Conditional)



TS : Initial character

TO : Format character

TAi : Interface character [codes FI,DI]

TBi : Interface character [codes II,PI1]

TCi : Interface character [codes N]

TDi : Interface character [codes Yi+1, T]

T1, ... , TK : Historical characters (max,15)

TCK : Check character

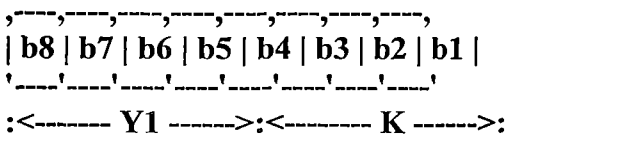
Σχήμα 4 : Γενική Μορφή του «Answer to Reset»

Initial character: χαρακτήρας συγχρονισμού (ISO1177).

Format character: Αποτελείται από δυο τμήματα

Το Y1 που καθορίζει την ύπαρξη των Interface characters

Το K που καθορίζει την ύπαρξη των Historical characters.



Y1 : indicator for the presence of the interface characters

TA1 is transmitted when b5=1

TB1 is transmitted when b6=1

TC1 is transmitted when b7=1

TD1 is transmitted when b8=1

K : number of hitorical characters

Σχήμα 5

Interface characters: ορίζουν φυσικές παραμέτρους του ολοκληρωμένου κυκλώματος της κάρτας, καθώς και λογικά χαρακτηριστικά του πρωτοκόλλου μετάδοσης.

Historical characters: φέρουν γενικές πληροφορίες, όπως για παράδειγμα, τον κατασκευαστή της κάρτας, το είδος του chip, το μέγεθος της ROM στο chip, την κατάσταση της κάρτας όσον αφορά το χρόνο ζωής της.

Check character: η ύπαρξή του εξαρτάται από το πρωτόκολλο που χρησιμοποιείται.

Τύπος Πρωτοκόλλου T

T=0 πρωτόκολλο ασύγχρονης ημι-αμφίδρομης μετάδοσης χαρακτήρων.

T=1 πρωτόκολλο ασύγχρονης ημι-αμφίδρομης μετάδοσης block.

T=2 και T=3 δεσμεύονται για μελλοντική χρήση και αμφίδρομη μετάδοση.

T=4 δεσμεύονται για μελλοντική ασύγχρονη ημι-αμφίδρομης μετάδοσης χαρακτήρων.

T=5 έως T=13 δεσμεύονται για μελλοντική χρήση.

T=14 δεσμεύονται για πρωτόκολλα κατά ISO.

T=15 δεσμεύονται για μελλοντική χρήση.

Answer to Reset σε ασύγχρονη μετάδοση

Δομή του Answer to Reset

Το ATR ξεκινά με την αποστολή μιας κεφαλίδας (header) που έχει σταθερό μήκος 32bits και περιλαμβάνει δυο υποχρεωτικά πεδία των 8bits, H1 και H2.

Η κεφαλίδα περιέχει πληροφορίες για το αν η κάρτα και η συσκευή είναι συμβατά. Αν δεν είναι απενεργοποιούνται οι επαφές. Το πρώτο μέρος H1 καθορίζει τον τύπο του πρωτοκόλλου. Το δεύτερο μέρος περιλαμβάνει παραμέτρους για το ν τύπο του πρωτοκόλλου που ορίστηκε στο H1.

3.3.2.1.4 ISO 7816-4: Interindustry Command for Interchange,

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 κάρτα
- 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:

1. Επιλογή Αρχείου
2. Ανάγνωση / εγγραφή αρχείου
3. Αναζήτηση αρχείου
4. Διαχείριση Αρχείων

5. Identification
6. Authentication
7. Εντολές Κρυπτογράφησης
8. Εντολές για ηλεκτρονικά πορτοφόλια
9. Εντολές ειδικές για κάθε εφαρμογή

3.3.2.2 Draft ISO 14443

Κάρτες αναγνώρισης - Contactless Chip – κάρτες πραγματοποίησης ανταλλαγής δεδομένων από μικρή απόσταση (proximity).

Αποτελείται από 4 μέρη ως εξής:

1. Φυσικά χαρακτηριστικά
2. Ισχύς ραδιο-συχνότητας και αλληλεπίδραση σημάτων
3. Αρχικοποίηση και αλγόριθμοι anti – collision (αποφυγή συγκρούσεων μεταξύ καρτών στο ίδιο πεδίο)
4. Πρωτόκολλα μεταφοράς δεδομένων

3.3.2.3 Draft ISO 15693

Κάρτες αναγνώρισης - Contactless Chip – κάρτες απομακρυσμένης πραγματοποίησης ανταλλαγής δεδομένων (vicinity).

Αποτελείται από 4 μέρη ως εξής:

1. Φυσικά χαρακτηριστικά
2. Ισχύς ραδιο-συχνότητας και αλληλεπίδραση σημάτων
3. Αλγόριθμος anti – collision και πρωτόκολλα επικοινωνίας
4. Εκτεταμένη σειρά εντολών και χαρακτηριστικά ασφαλείας

3.3.3 Βιομηχανικά Πρότυπα

3.3.3.1 Πρότυπο EMV

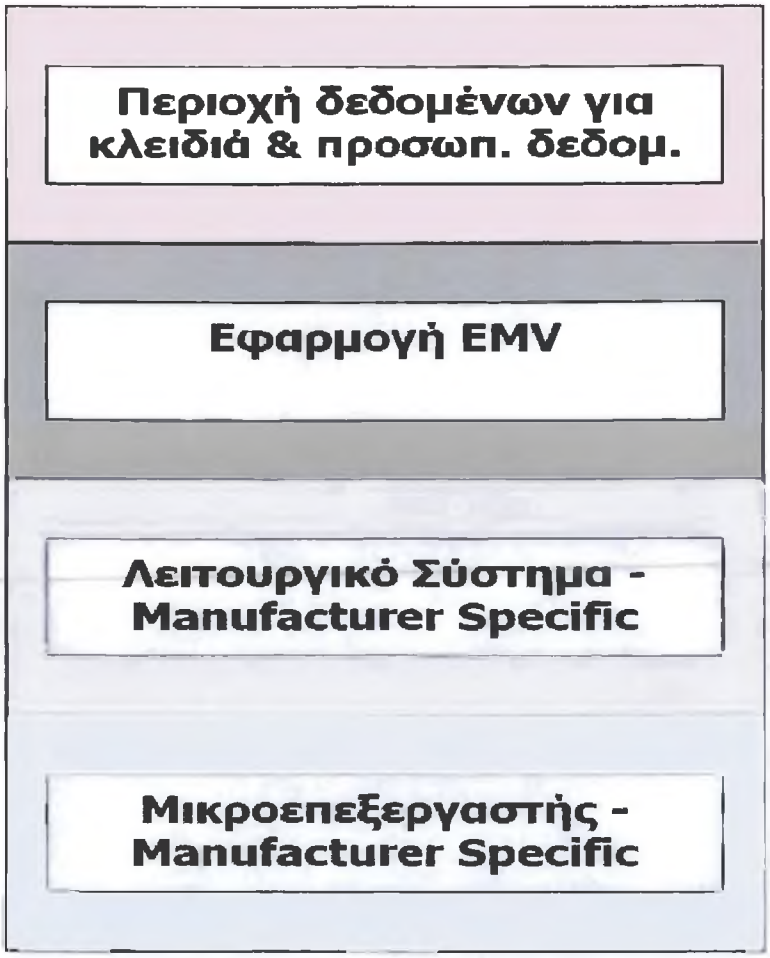
EMV είναι ένα ακρωνύμιο που προκύπτει από τα αρχικά των λέξεων Europay, MasterCard και Visa. Οι τρεις αυτοί οργανισμοί έχουν συμφωνήσει στη σύνταξη ορισμένων προδιαγραφών γνωστές με το όνομα "EMV card specification". Οι προδιαγραφές αυτές περιγράφουν τον τρόπο με τον οποίο οι κάρτες που εκδίδονται από οποιονδήποτε από τους τρεις οργανισμούς θα λειτουργεί σε ένα τερματικό μηχάνημα ή ένα Automated Teller Machine (ATM).

Υπάρχουν τρεις 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.

3. 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.



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.

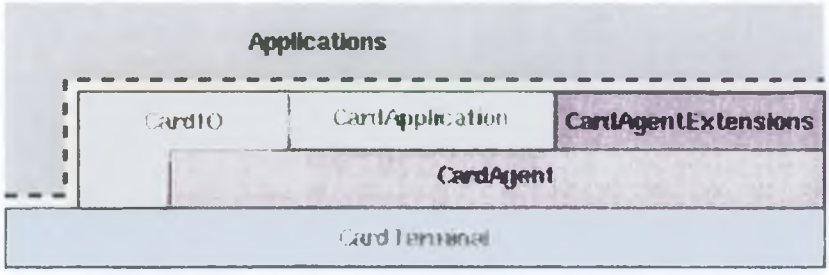
Στο χαμηλότερο επίπεδο βρίσκεται ο μικροεπεξεργαστής, για τον οποίο υπάρχουν τουλάχιστον τέσσερις διαφορετικοί κατασκευαστές.

3.3.3.2 Open Card

Το πρότυπο OpenCard αφορά στη 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 ένα ενιαίο interface για την ανάπτυξη εφαρμογών έξυπνων καρτών σε όλες τις νέες πλατφόρμες, όπως δίκτυα υπολογιστών, τηλέφωνα, ATM, Unix workstations κ.α.

OpenCard architecture

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.



Σχήμα 6. Αρχιτεκτονική OpenCard Framework [7]

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:

1. ανεξαρτησία από προμηθευτές τερματικών καρτών,
2. ανεξαρτησία από προμηθευτές λειτουργικών συστημάτων καρτών,
3. ανεξαρτησία από εκδότες καρτών.

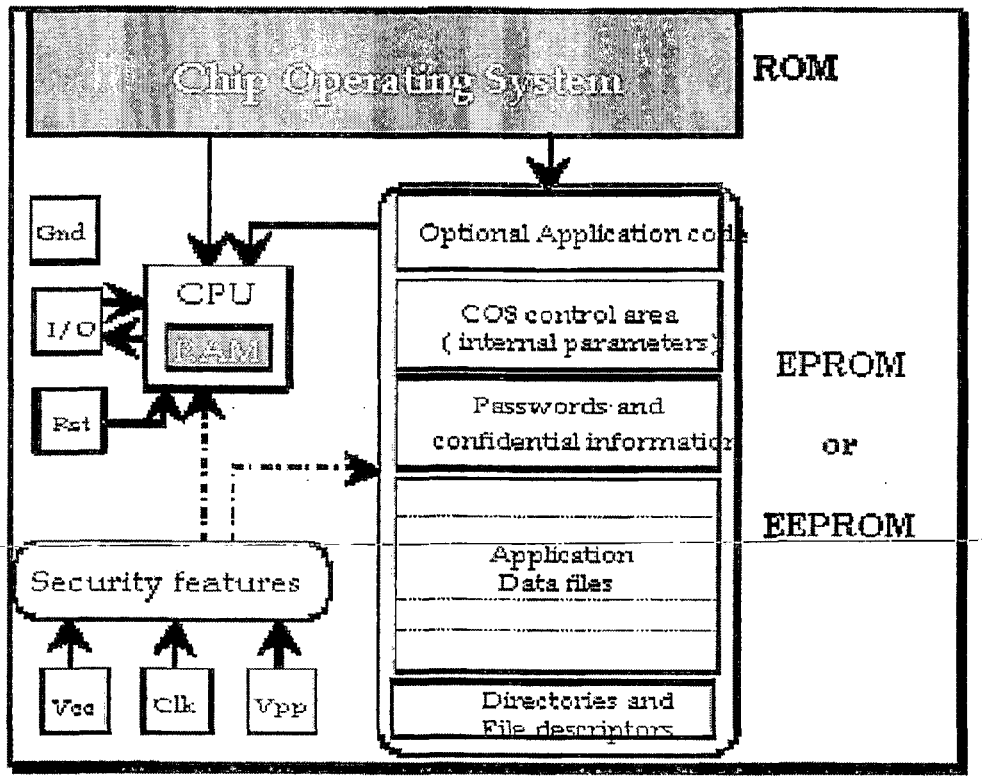
Επιπλέον είναι εύκολο στη χρήση και έχει αρκετές δυνατότητες επέκτασης.

3.3.3.3 PC/SC

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 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.

3.4 Λειτουργικό Σύστημα Έξυπνων Καρτών (COS)

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.



Σχήμα 7 [3]

3.4.1 Τι ακριβώς είναι 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:

- Τα COS γενικού σκοπού (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 προβλέπεται να έχουν μεγάλη διάρκεια ζωής. Παραδείγματα τέτοιων OS είναι το Java Cards και το OS Windows της Microsoft. Στη περίπτωση όμως αυτοί 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:

1. Διαχείριση της ανταλλαγής δεδομένων μεταξύ της κάρτας και του εξωτερικού κόσμου, κυρίως από την άποψη του χρησιμοποιούμενου πρωτοκόλλου.
2. Διαχείριση των αρχείων και των δεδομένων που φυλάσσονται στη μνήμη
3. Έλεγχος πρόσβασης σε πληροφορίες και λειτουργίες (παραδείγματος χάριν select file, read, write, update data).
4. Διαχείριση της ασφάλειας καρτών και των κρυπτογραφικών αλγορίθμων.
5. Διατήρηση της αξιοπιστίας, ιδιαίτερα από την άποψη της συνέπειας στοιχείων, της διαχείρισης των interrupts και την επαναφορά από ένα σφάλμα.
6. 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.

3.4.2 Multi Application Card Operating Systems (MACOS)

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

Τα λειτουργικά συστήματα πολλλαπλών εφαρμογών επιτρέπουν την ανάπτυξη των πολλλαπλών 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:

1. Java Card για όσους θέλουν να προγραμματίσουν σε Java.
2. MultOS είναι το πρώτο λειτουργικό σύστημα πολλαπλών εφαρμογών (multiapplication) για έξυπνες κάρτες που προσφέρει υψηλό επίπεδο ασφάλειας. Το Multos επιτρέπει τη φορτώση, την ενημέρωση ή τη διαγραφή οποιασδήποτε εφαρμογής κατά τη διάρκεια της ζωής της κάρτας.
3. Windows for Smart Cards Microsoft licenses Windows® for Smart Cards Toolkit

3.5 MULTOS

3.5.1 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 εκδώσει κάρτες, να γράψει εφαρμογές, να εφαρμόσει το λειτουργικό σύστημα σε ένα συγκεκριμένο τσιπ ή να κατασκευάσει έξυπνες κάρτες.

3.5.2 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.

3.5.3 Application Load & Unload

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.

4

Χρήση Των Έξυπνων Καρτών

4.1. Έξυπνες κάρτες και υποδομές δημοσίου κλειδιού

Οι έξυπνες κάρτες διευκολύνουν την εφαρμογή των υποδομών δημοσίου κλειδιού (public key infrastructure), οι οποίες χρησιμοποιούνται ευρέως στο ηλεκτρονικό εμπόριο. Οι υποδομές δημοσίου κλειδιού μπορούν να εξασφαλίσουν υψηλό επίπεδο εμπιστοσύνης στις ηλεκτρονικές συναλλαγές.

Επιπλέον παρέχουν ακεραιότητα δεδομένων, ασφάλεια και ιδιωτικότητα. Σ' αυτό το σημείο θα αναφερθούμε στις υποδομές δημοσίου κλειδιού και τη σχέση τους με τις έξυπνες κάρτες, αλλά χωρίς να επεκταθούμε ιδιαίτερα. Στις υποδομές δημοσίου κλειδιού συναντάμε δύο είδη κλειδιών.

Ένα δημόσιο (public key) κι ένα ιδιωτικό κλειδί (private key). Ορισμένοι συνδυασμοί των κλειδιών αυτών χρησιμοποιούνται στην κρυπτογράφηση / αποκρυπτογράφηση δεδομένων, στα ψηφιακά πιστοποιητικά και τις ψηφιακές υπογραφές. Το ιδιωτικό κλειδί, όπως υποδηλώνει το όνομά του, πρέπει να φυλάσσεται καλά από τον κάτοχό του και να παραμένει κρυφό σε αντίθεση με το δημόσιο το οποίο είναι προσβάσιμο από όλους. Η δημιουργία και διάθεση των ιδιωτικών κλειδιών γίνεται από αρχές κοινά αποδεκτές. Για να γίνουν κατανοητά τα παραπάνω παραθέτουμε το εξής παράδειγμα: η ασφάλεια μιας ηλεκτρονικής πληρωμής όπου απαιτείται αριθμός πιστωτικής κάρτας μπορεί να εξασφαλιστεί με τις υποδομές δημοσίου κλειδιού. Μια από τις υποδομές αυτές ορίζει ότι ο συναλλασσόμενος πρέπει να έχει στην κατοχή του μια ψηφιακή υπογραφή, η οποία προκύπτει από την εφαρμογή μιας συνάρτησης στο ιδιωτικό του κλειδί.

Πριν σταλεί ο αριθμός της πιστωτικής του κάρτας στον έμπορο, πρέπει να υπογραφεί με την ψηφιακή του υπογραφή ώστε να εξασφαλιστεί ότι ήταν αυτός που έκανε την ηλεκτρονική πληρωμή. Το δημόσιο κλειδί του συναλλασσόμενου χρησιμοποιείται σ' αυτή την περίπτωση για την επικύρωση της ψηφιακής υπογραφής.

Οι έξυπνες κάρτες μπορούν να προστατεύσουν τα ιδιωτικά κλειδιά στο εσωτερικό των μικροτσίπ που διαθέτουν. Σε αντίθετη περίπτωση τα ιδιωτικά κλειδιά αποθηκεύονται στους υπολογιστές των κατόχων τους, όπου είναι τρωτά σε επιθέσεις εισβολέων με σκοπό την απόκτησή τους. Η μεταφορά του ιδιωτικού κλειδιού μέσα στην έξυπνη κάρτα διευκολύνει ιδιαίτερα τις ηλεκτρονικές συναλλαγές.

4.2. Ο ρόλος των έξυπνων καρτών στις ηλεκτρονικές συναλλαγές

Όπως είναι γνωστό για να γίνει μια ηλεκτρονική συναλλαγή απαιτείται η ανταλλαγή ευαίσθητων προσωπικών δεδομένων μεταξύ των συναλλασσόμενων πλευρών. Οι έξυπνες κάρτες αποτελούν ένα άριστο μέσο για τη μεταφορά ευαίσθητων προσωπικών δεδομένων όπως για παράδειγμα αριθμούς πιστωτικών καρτών, δίπλωμα και ασφάλεια αυτοκινήτου, ιατρικούς φακέλους, συνθηματικά για πρόσβαση σε ιστοσελίδες, κλειδιά κρυπτογράφησης / αποκρυπτογράφησης ή ακόμη και πλαστικό χρήμα. Μ 'αυτόν τον τρόπο μια απλή κάρτα μπορεί να αντικαταστήσει πολλές από τις κάρτες και τα χαρτιά που χρησιμοποιεί σε καθημερινή βάση ένας άνθρωπος σήμερα. Οι έξυπνες κάρτες μπορούν επιπλέον να αντικαταστήσουν κάρτες όπως οι τηλεκάρτες, οι πιστωτικές κάρτες, οι κάρτες ανάληψης μετρητών και άλλες παρόμοιες κάρτες.

Μια τέτοια κάρτα πολλαπλών εφαρμογών που χρησιμοποιείται στις ηλεκτρονικές συναλλαγές είναι η Java Card.

4.3 Το ζήτημα των πληρωμών

Με την εμφάνιση του ηλεκτρονικού εμπορίου, οι ανάγκες για την ευκολότερη ροή του χρήματος πολλαπλασιάστηκαν. Οι συμβατικές μέθοδοι πληρωμών και εισπράξεων δεν επαρκούν για τον νέο τρόπο συναλλαγών, αγορών και πωλήσεων. Οι πραγματικές ηλεκτρονικές συναλλαγές άρχισαν με την εμφάνιση του λεγόμενου «πλαστικού χρήματος», των πιστωτικών καρτών. Οι «πελάτες» και κάτοχοι των πιστωτικών καρτών δεν είχαν παρά να ενημερώσουν τον «έμπορο» για τον αριθμό της κάρτας τους και η χρέωσή τους γίνονταν χειροκίνητα, ημιαυτόματα ή αυτόματα. Μια τέτοια όμως πρακτική εμπεριείχε και κινδύνους. Το χρήμα γίνονταν ανώνυμο και ο καθένας πλέον, γνωρίζοντας απλώς τον αριθμό της πιστωτικής κάρτας κάποιου άλλου, μπορούσε να κάνει συναλλαγές, χρεώνοντας τον λογαριασμό του ανυποψίαστου κατόχου της κάρτας. Αυτό

και μόνο οδήγησε τους υποψήφιους «ηλεκτρονικούς πελάτες» στο να αντιμετωπίσουν με αρκετή καχυποψία τον νέο τρόπο συναλλαγών και τους επίδοξους «ηλεκτρονικούς εμπόρους» να αναζητούν λύσεις, για να εκμηδενίσουν τον κίνδυνο και να πείσουν τους πελάτες τους για την ασφάλεια και την αξιοπιστία του τρόπου συναλλαγής που πρότειναν.

Στην αρχή κατέφυγαν σε πρακτικές λύσεις : Ζητούσαν από τους πελάτες να στείλουν τον αριθμό της πιστωτικής τους κάρτας με fax ή με e-mail, σε δύο ή παραπάνω διαφορετικά μηνύματα που το καθένα περιείχε ένα μέρος του αριθμού. Ο έμπορος έπρεπε να λάβει όλα τα μηνύματα από τον ίδιο πελάτη, να ενώσει τα μέρη των αριθμών και έτσι να έχει όλη την εικόνα σχηματισμένη. Οι λύσεις αυτές παρείχαν στους πελάτες την ασφάλεια που επιθυμούσαν και βέβαια την ευκολία να ολοκληρώνουν τις συναλλαγές τους, χωρίς να απομακρύνονται από το τερματικό τους. Από την άλλη πλευρά όμως, δημιουργούσαν έναν όγκο εργασίας για τους εμπόρους, οι οποίοι θα έπρεπε, πριν εκτελέσουν την παραγγελία, να απευθυνθούν στις τράπεζες που είχαν εκδώσει τις κάρτες, για να επιβεβαιώσουν τα στοιχεία των πελατών και την πιστοληπτική αξιοπιστία των καρτών τους. Η διαδικασία ήταν χρονοβόρα, επιβάρυνε την επιχείρηση και φυσικά δεν έλειπαν οι περιπτώσεις που δημιουργούνταν αντιδικίες μεταξύ του πελάτη, του εμπόρου και των τραπεζών.

Ένας άλλος τρόπος είναι η έγκριση της κάρτας on-line οπότε ο πελάτης θα πρέπει να περιμένει ένα μικρό χρονικό διάστημα, για να γίνει η επικοινωνία με την αρχή έκδοσης της κάρτας. Στην Ελλάδα πιο συγκεκριμένα, η Εγνατία τράπεζα καθώς και οι ηλεκτρονικές τράπεζες (Win Bank και Nova Bank) είναι οι μόνες τράπεζες σύμφωνα με στοιχεία του περιοδικού RAM (Μάρτιος 2001) ήταν οι μόνες που είχαν μέχρι εκείνη την χρονική στιγμή την δυνατότητα να δώσουν έγκριση για κάρτα τύπου Visa on-line μέσω Internet.

Όμως με τις «έξυπνες κάρτες» έγινε πραγματικά το πέρασμα από το «πλαστικό χρήμα» στο «ηλεκτρονικό χρήμα». Αν και οι έξυπνες κάρτες μοιάζουν πολύ με τις πιστωτικές κάρτες ως προς την εμφάνιση και τον τρόπο χρήσης τους, η αντικατάσταση της μαγνητικής ταινίας των τελευταίων από ένα ολοκληρωμένο κύκλωμα με microchip κάνουν την διαφορά. Στην ουσία, ενώ οι πιστωτικές κάρτες αντικατοπτρίζουν την πιστοληπτική ικανότητα του κατόχου τους, οι έξυπνες κάρτες μπορούν να

ενσωματώνουν χρηματικές μονάδες που μεταβιβάζονται από τον λογαριασμό του κατόχου στο χρηματοπιστωτικό ίδρυμα που την έχει εκδώσει, στον μικροεπεξεργαστή της κάρτας. Όταν ο κάτοχος χρησιμοποιεί την κάρτα για αγορές του, οι χρηματικές μονάδες αφαιρούνται από τον μικροεπεξεργαστή της κάρτας και χρεώνονται στον λογαριασμό του εμπόρου. Η χρήση τέτοιων καρτών προϋποθέτει φυσικά την ύπαρξη ειδικών συσκευών που πρέπει να είναι συνδεδεμένη με το τερματικό του πελάτη καθώς και την ανάλογη υποδομή διαχείρισης έξυπνων καρτών από την πλευρά του εμπόρου. Οι έξυπνες κάρτες ακόμα διευκολύνουν στη μεταφορά των στοιχείων του κατόχου τους, ώστε να μπορούν να χρησιμοποιούνται και σε συναλλαγές που εκτελούνται και από άλλους υπολογιστές στο σπίτι, στο γραφείο ή σε άλλους χώρους που είναι συνδεδεμένοι στο διαδίκτυο. Είναι μια τεχνολογία που δείχνει να έχει μεγάλη προοπτική εξέλιξης. Εταιρίες που κάνουν χρήση των καρτών αυτών και της τεχνολογίας κρυπτογράφησης PKI, για να αντιμετωπίσουν προβλήματα ασφάλειας από εμπορικές συναλλαγές, διαφαίνεται ότι τελικά θα κερδίσουν την εμπιστοσύνη των αγοραστών.

Πρέπει να πούμε ότι οι έξυπνες κάρτες αλλά και γενικότερα όλα αυτά τα τελευταίας τεχνολογίας κουπόνια (συμπεριλαμβανομένων και των μαγνητικών καρτών) είναι ο παράγοντας που έδωσε μια ξεχωριστή και υπέρμετρη ώθηση στον τομέα των συναλλαγών.

Χάρις σε αυτόν, πολλά πράγματα και παράγοντες πάνω στις διάφορες συναλλαγές, απλοποιήθηκαν, ενώ πολλά προβλήματα και ζητήματα βρήκαν τις λύσεις τους. Ειδικά για τις έξυπνες κάρτες, ο τομέας της ασφάλειας έχει περάσει σε μια άλλη, νέα διάσταση. Τώρα πλέον, η μεταφορά μετρητών δεν είναι αναγκαία και κίνδυνοι κλοπής έχουν εντελώς εξαφανιστεί.

Άλλωστε, κανένας σήμερα δεν μπορεί να χρησιμοποιήσει μια κλεμμένη έξυπνη κάρτα (χωρίς βέβαια να βάζουμε και το χέρι μας στο τάφο) ενώ σε περίπτωση κλοπής της, η ακύρωσή της καθώς και η έκδοση μιας καινούργιας είναι πλέον μια διαδικασία-ρουτίνα.

4.4 Τεχνικές λεπτομέρειες

Οι διάτρητες κάρτες αποτελούσαν στην πραγματικότητα μια εξαιρετικά καινοτομική και ριζοσπαστικά ανατρεπτική ιδέα. Εμφανίστηκαν λίγα χρόνια μετά την εμφάνιση των ηλεκτρονικών υπολογιστών και αποτέλεσαν το κύριο αποθηκευτικό μέσο του λογισμικού αυτών. Ωστόσο σήμερα μας είναι γνωστό ότι κατά την διάρκεια του δευτέρου παγκοσμίου πολέμου, οι Γερμανοί συνήθιζαν να καταγράφουν έναν - έναν όλους τους Εβραίους παρέχοντας τους από μία μαγνητική κάρτα στον καθένα. Οι μαγνητικές κάρτες βοήθησαν στην επεξεργασία ενός τεράστιου αριθμού δεδομένων αλλά και η εξακρίβωση κάποιας τυχούσας συγγένειας μεταξύ Γερμανών πολιτών και Εβραίων. Οι διάτρητες κάρτες αποτελούνταν από ένα κομμάτι χοντρού σε πάχος χαρτιού (το πλαστικό εφευρέθηκε μια δεκαετία αργότερα) όπου πάνω, μέσω ενός ειδικού μηχανήματος, εφαρμόζονταν τρύπες σε καθορισμένα σημεία με τέτοιο τρόπο που η θέση των τελευταίων ήταν διαφορετική από κάρτα σε κάρτα. Με την ανάπτυξη όμως των υπολογιστικών συστημάτων αλλά και την ανακάλυψη του πλαστικού που ήταν ένα ποιο ανθεκτικό υλικό από το χαρτί, γρήγορα εγκαταλείφτηκαν και οι μαγνητικές κάρτες πήραν την θέση τους στον τομέα της αυθεντικοποίησης (αν και συνέχισαν να χρησιμοποιούνται για αρκετό χρονικό διάστημα στον τομέα των βάσεων δεδομένων με ηλεκτρονικούς υπολογιστές).

Οι μαγνητικές κάρτες είναι ουσιαστικά ένα κομμάτι πλαστικού που στο πίσω μέρος του περιλαμβάνει μια μαγνητική ταινία όπου και αποθηκεύονται δεδομένα. Η διαστάσεις και η μορφή των μαγνητικών καρτών καθορίζεται από το πρότυπο ISO 7810. Τυπικά, πάνω στην μαγνητική ταινία στο πίσω μέρος της κάρτας αποθηκεύεται η πληροφορία αναγνώρισης του ατόμου-κατόχου της (για παράδειγμα μπορεί να είναι ο αριθμός του τραπεζικού του λογαριασμού). Από αρχή της εμφάνιση τέτοιων καρτών, οι τελευταίες συνήθως χρησιμοποιούνται σε συνδυασμό με κάποιον αριθμό PIN (Personal Identification Number ή Προσωπικός Αριθμός Αναγνώρισης) για την επιβεβαίωση της ταυτότητας του νόμιμου χρήστη. Σε συστήματα off-line η πληροφορία αυθεντικοποίησης του PIN αριθμού αποθηκεύεται στην κάρτα. Αυτό σημαίνει ότι είτε το PIN φυλάγεται σε κρυπτογραφημένη μορφή στην κάρτα ή ότι είναι γραμμένο εκεί το αποτέλεσμα μιας μονόδρομης συνάρτησης στο PIN. Σε κάθε περίπτωση, το PIN θα πρέπει να συνδυάζεται με μια πληροφορία που εξαρτάται από τον κάθε χρήστη (όπως ο αριθμός της ταυτότητάς του) πριν την κρυπτογράφησή του ώστε να αποτρέπονται οι επιτιθέμενοι από το να

συγκρίνουν λίστες κρυπτογραφημένων PIN. Αντίθετα με τα παραπάνω, σε συστήματα on-line (όπως είναι για παράδειγμα τα συστήματα ATM), τα PIN των χρηστών επιβεβαιώνονται κεντρικά και γι' αυτό δεν χρειάζεται να γραφούν πάνω στην κάρτα. Ανάλογα λοιπόν με το σύστημα όπου εφαρμόζονται οι μαγνητικές περιπτώσεις, αποθηκεύονται πληροφορίες στην μαγνητική κάρτα.

Περνώντας στις έξυπνες κάρτες στα μέσα τις δεκαετίας του 1980, βλέπουμε ότι έχουν περισσότερες ομοιότητες με την μαγνητικές, παρά με τις διάτρητες κάρτες. Όμως έχουν και τεράστιες διαφορές με τις πρώτες. Καταρχήν, διαθέτουν μικροεπεξεργαστή (IC ή Integrated Circuit) και μνήμη (είτε είναι RAM ή ROM τύπου). Συνήθως έχουν πολύ μεγαλύτερη μνήμη από τις μαγνητικές κάρτες (κατά μέσο όρο σήμερα οι μαγνητικές κάρτες έχουν μνήμη 250 bytes ενώ οι έξυπνες κάρτες φτάνουν τα 35 Kbytes). Βέβαια, τα τελευταία χρόνια άρχισαν να εμφανίζονται και έξυπνες κάρτες που υλοποιούνται με την χρήση μνήμης τύπου Flash (το συγκεκριμένο είδος μνήμης διατηρεί τα δεδομένα του για όσο χρόνο υπάρχει τροφοδοσία ρεύματος στην κάρτα, αντίθετα με την μνήμη ROM που περιέχει δεδομένα χωρίς την χρήση τροφοδοσίας αλλά και με τον περιορισμό της μη αλλαγής αυτών – read only). Υπάρχει όμως και μια ειδική κατηγορία έξυπνων καρτών που δεν περιέχουν καθόλου μνήμη αλλά μόνο το απαραίτητο λογισμικό για την επικοινωνία με ένα κεντρικό πληροφοριακό σύστημα όπου αποθηκεύονται όλες οι πληροφορίες κάθε κατόχου τέτοιου είδους κάρτας. Πρωτοπόρα σε αυτή την εξέλιξη είναι η Chip Net η οποία σήμερα είναι κυρίαρχη εταιρία στον χώρο της. Επιπλέον, οι έξυπνες κάρτες έχουν το ισχυρό πλεονέκτημα της ενσωματωμένης υπολογιστικής ισχύος. Στην ουσία όμως, το κύριο πλεονέκτημά τους είναι ότι παρέχουν φυσική προστασία των αποθηκευμένων δεδομένων. Οι επαφές με το εσωτερικό κύκλωμα υπάρχουν ως επιχρυσωμένες περιοχές στην επιφάνεια της κάρτας, περιλαμβανομένων των επαφών για την τροφοδοσία από εξωτερική πηγή. Η τοποθέτηση αυτών των επαφών, το μέγεθος της κάρτας και τα πρωτόκολλα που χρησιμοποιούνται στην επικοινωνία μεταξύ έξυπνης κάρτας και συσκευής αναγνώρισης καθορίζονται από το πρότυπο ISO/IEC 7816. Ουσιαστικά λοιπόν αποτελούν φορητούς υπολογιστές από τους οποίους λείπει το σύστημα τροφοδοσίας. Το τελευταίο υλοποιείται κατά την χρήση της κάρτας αφού η συσκευή ανάγνωσής της παρέχει ρεύμα στην κάρτα ώστε να λειτουργήσει ο μικροεπεξεργαστής. Συνήθως απαιτείται ρεύμα 10 milliamp καθώς και τάση ρεύματος 5 Vdc +/- 10%. Προχωρώντας πιο πέρα, ο μέσος όρος τέτοιων καρτών είναι εξαιρετικά ανθεκτικές αφού μπορούν να λειτουργούν σε θερμοκρασίες από –40 ο C έως 125 ο C.

Μια από τις πλέον ενδιαφέρουσες ιδιότητες των έξυπνων καρτών είναι ότι είναι εξαιρετικά δύσκολο να αντιγραφούν. Στην πραγματικότητα, οι κατασκευαστές κρατούν καλά κρυμμένες τις λεπτομέρειες της εσωτερικής σχεδίασης προκειμένου να δυσκολέψουν ακόμα περισσότερο την αντιγραφή και την αναπαραγωγή αυτών από επίδοξους απατεώνες.

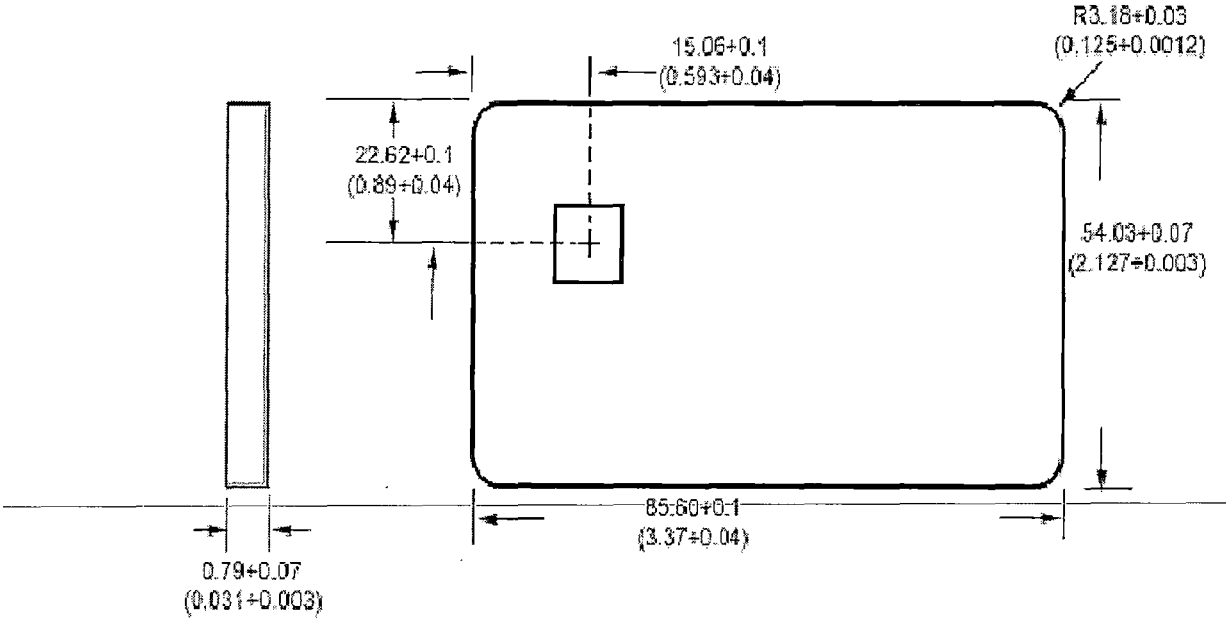
Τα τελευταία χρόνια, εμφανίστηκε και η δεύτερη γενιά έξυπνων καρτών που ουσιαστικά είναι η αναβαθμισμένη έκδοση της πρώτης και αρχικής γενιάς. Η δεύτερη γενιά καρτών περιέχει πιο δυνατούς επεξεργαστές (η πρώτη γενιά χρησιμοποιούσε απλούς επεξεργαστές των 8-bit), περισσότερη μνήμη (η πρώτη γενιά είχε περιορισμένη μνήμη των 8 Kbytes) και μια ποικιλία κρυπτογραφικών λειτουργιών (στην πρώτη γενιά, λίγες ήταν οι κάρτες που πετύχαιναν κρυπτογράφηση των δεδομένων). Μερικά από τα τελευταίας τεχνολογίας μοντέλα μπορούν μάλιστα να εκτελούν υπολογισμούς ψηφιακών υπογραφών σε κλάσματα δευτερολέπτου. Όσον αφορά την ενσωματωμένη κρυπτογραφική επεξεργασία, κρίνεται ιδιαίτερα χρήσιμη καθώς, συνδυαζόμενη με την φυσική ασφάλεια που παρέχεται στα αποθηκευμένα μυστικά δεδομένα, επιτρέπει την χρησιμοποίησή τους σε αλληλεπιδραστικές συσκευές αναγνώρισης. Ειδικότερα, αν το μυστικό σύνθημα P του χρήστη (αντίστοιχο με το PIN των μαγνητικών καρτών μόνο που μπορεί να έχει μεγαλύτερη έκταση και όχι μόνο αριθμούς – κάτι που παρέχουν μεγαλύτερη ασφάλεια από το σπάσιμο των κωδικών) αποθηκευτεί στην κάρτα, τότε και η τελευταία μπορεί να χρησιμοποιηθεί σε ένα σχήμα αναγνώρισης του χρήστη με την μέθοδο της πρόκλησης- απόκλισης υπολογίζοντας την επιλεγμένη μονόδρομης συνάρτηση. Μια βελτιωμένη έκδοση ενός τέτοιου σχήματος απαιτεί από τον χρήστη να εισάγει το συνθηματικό P (μέσω τερματικού εξοπλισμού ή άλλης συσκευής ανάγνωσης της έξυπνης κάρτας) πριν η κάρτα εκτελέσει την λειτουργία της, σαν ένα είδος προστασίας στην περίπτωση που η κάρτα κλαπεί από τον νόμιμο χρήστη της. Επιπλέον, πολλές νέου τύπου κάρτες όπως η SignaSURE της Data Key μπορούν και εμπεριέχουν σύγχρονου τύπου αλγορίθμους κωδικοποίησης τύπου public key που καθιστούν το σπάσιμο των κωδικών εξαιρετικά δύσκολο έως και πρακτικά απίθανο.

Η κατασκευή των έξυπνων καρτών είναι μια εξαιρετικά πολύπλοκη αλλά και επίπονη διαδικασία αφού στην ουσία συναρμολογείτε πάνω στην κάρτα ένα ολόκληρο υπολογιστικό σύστημα. Όμως με τα σύγχρονα μέσα που διαθέτουμε αλλά και την ξέφρενη πορεία που εμφανίζει η κατασκευή επεξεργαστών, ολοκληρωμένων

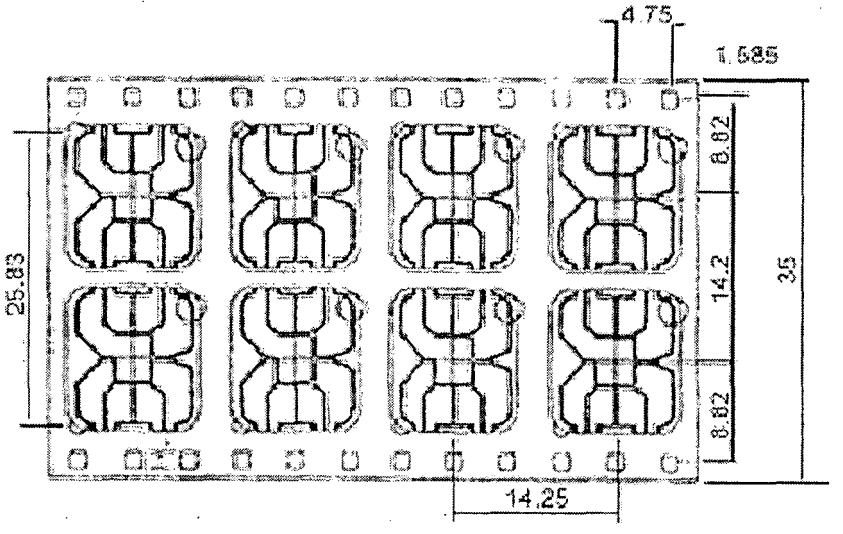
κυκλωμάτων και ψηφιακών σχεδίων, η όλη διαδικασία απλοποιείται σημαντικά με την χρήση ειδικών ρομπότ για όλη αυτή την διαδικασία. Μετά από αυτό, η όλη παραγωγική διαδικασία γίνεται απλή ρουτίνα και μπαίνει στο πλαίσιο της βιομηχανικής μαζικής παραγωγής. Έτσι τόσο το κόστος κατασκευής όσο και ο χρόνος ολοκλήρωσης της διαδικασίας μειώνονται δραματικά. Στην φωτογραφία δίπλα μπορούμε να δούμε ένα είδος ρομπότ που αναφέραμε κατά την κατασκευή του chip (ολοκληρωμένου κυκλώματος) που τοποθετείται στην έξυπνη κάρτα.

Το κύκλωμα καταρχήν δημιουργείται από εξειδικευμένα βιομηχανικά ρομπότ και στην συνέχεια αφού φορτιστεί με τις κατάλληλες πληροφορίες και λογισμικό, τοποθετείται στο πλαστικό περίβλημα της έξυπνης κάρτας. Φυσικά, οι κάρτες μετά από αυτή την διαδικασία μπορούν να υποστούν και περαιτέρω επεξεργασία ανάλογα με τις ανάγκες μας, όπως για παράδειγμα εισαγωγή barcode (όπως οι αμερικάνικες ταυτότητες σε διάφορες υπηρεσίες), ψηφιακής ή φυσικής υπογραφής (όπως οι πιστωτικές κάρτες των τραπεζών), ανάγλυφα για τα άτομα με προβλήματα όρασης αλλά και σαν μέσο ασφάλειας από πλαστά αντίγραφα, φωτογραφία του κατόχου, αόρατα από το ανθρώπινο μάτι υδατογραφήματα για ασφάλεια όπως στα χαρτονομίσματα και πάρα πολλά άλλα.

Όπως αναφέραμε και πιο πάνω, οι περισσότερες από τις έξυπνες κάρτες βασίζονται πάνω στο πρότυπο ISO/IEC 7816. Παρακάτω υπάρχει αναλυτικά η εξήγηση αυτού του προτύπου καθώς παρέχονται και τεχνικές λεπτομέρειες πάνω στην κατασκευή των καρτών. Στην παρακάτω φωτογραφία υπάρχει το τυπικό μέγεθος όλων των έξυπνων καρτών καθώς και η τοποθέτηση του κύριου ολοκληρωμένου κυκλώματος πάνω στην κάρτα, όπως ακριβώς αναφέραμε στην διαδικασία κατασκευής.



Αυτό είναι και το τυπικό μέγεθος. Υπάρχουν βέβαια και έξυπνες κάρτες με διαφορετικό μέγεθος, αλλά ο αριθμός αυτών είναι πολύ μικρός καθώς σπάνια καθορίζονται από ένα πρότυπο ISO. Γι' αυτό και εδώ δεν θα ασχοληθούμε με τέτοια εξαιρετικά ειδικευμένα μοντέλα και κάρτες. Παρακάτω υπάρχει άλλη μια κάτοψη του πρότυπου. Χαρακτηριστικό είναι ο μαύρος «θόλος» που υπάρχει στο πάνω μέρος της κάρτας. Αυτό είναι το ολοκληρωμένο κύκλωμα που όπως είπαμε και πιο πριν τοποθετείται πάνω στην κάρτα κατά την διαδικασία της υλοποίησης.



Αυτό είναι και το μέρος που επικοινωνεί με εξωτερικές συσκευές, και όχι το υπόλοιπο της κάρτας. Μέσα στο chip υπάρχει το COS (Chip Operating System ή πιο απλά Λειτουργικό Σύστημα του Τσιπ) το οποίο με την εκκίνησή του κατά την αρχή της επαφής, εκτελεί τις διάφορες λειτουργίες. Προχωρώντας πιο εσωτερικά στην δομή, χαρακτηριστική είναι και η επόμενη εικόνα. Εδώ υπάρχει η τυπική μορφή ενός ολοκληρωμένου κυκλώματος, όπως καθορίζεται από το πρότυπο ISO.

Φυσικά, από εκεί και πέρα, η λειτουργία της μονάδας αυτής είναι απόλυτα θέμα λογισμικού που εισάγεται σε αυτό ή ρυθμίζεται κατά την κατασκευή του. Κύριο υλικό για την κατασκευή είναι το πυρίτιο και η σιλικόνη. Η κάθε λειτουργική μονάδα περιέχει εκτός από επεξεργαστή και μνήμη, διάφορους επιμέρους επεξεργαστές για διάφορες άλλες λειτουργίες (όπως είναι για παράδειγμα η κρυπτογράφηση των αποθηκευμένων δεδομένων ή ο μικροεπεξεργαστής που ασχολείται με το πρωτόκολλο επικοινωνίας με τον έξω κόσμο) καθώς και διάφορες διασυνδέσεις (bus) μεταξύ των επιμέρους μερών. Ο προγραμματισμός και η σχεδίαση του λογισμικού που περιέχει η κάρτα αναπτύσσεται από ειδικευμένες ομάδες προγραμματιστών που ειδικεύονται στον μικρό-προγραμματισμό, μια νέα τεχνολογία που αναπτύσσεται εξαιρετικά τα τελευταία χρόνια. Ο μικρό-προγραμματισμός ασχολείται ακριβώς με την ανάπτυξη εφαρμογών και διεργασιών για τέτοιου είδους συσκευές. Συνήθη εργαλεία για αυτό αποτελεί η γλώσσα μηχανής (assembly) που συνδέεται απόλυτα με την τεχνολογία του κεντρικού επεξεργαστή ή με άλλες ανάλογες γλώσσες, όπως είναι η micro-Java.

Όσον αφορά την κρυπτογράφηση των δεδομένων, εδώ τα πράγματα είναι περισσότερο πολύπλοκα. Η επικρατέστερη τεχνολογία κρυπτογράφησης είναι η PKI (Public Key Infrastructure encryption) που χρησιμοποιείται και για την ασφαλή ανταλλαγή δεδομένων μέσω του διαδικτύου. Σύμφωνα με αυτή την νέα τεχνολογία μια απλή πλαστική κάρτα μπορεί να αντικατασταθεί από ένα ψηφιακό πιστοποιητικό. Η έννοια των πιστοποιητικών έρχεται απευθείας από το διαδίκτυο όπου και χρησιμοποιείται ευρέως είναι για να πιστοποιηθεί η ταυτότητα κάποιου χρήστη ή για να πιστοποιηθεί η ταυτότητα κάποιου αρχείου καθώς και η καταγωγή του. Επιστρέφοντας πάλι στο θέμα μας, σύμφωνα με αυτή την μέθοδο, οι τράπεζες συνεχίζουν να ελέγχουν και να διασφαλίζουν το επιτυχές των συναλλαγών, ο φυσικός τρόπος πληρωμής δεν είναι

απαραίτητα μια τραπεζική κάρτα, δημιουργούνται νέα μοντέλα επιχειρήσεων αλλά και συναλλαγών και τέλος εμφανίζονται νέου είδους εμπορικές σχέσεις.

Ο τομέας της μνήμης που εμπεριέχεται στην κάρτα είναι ακόμα ένα σημαντικό ζήτημα. Οι περισσότερες κάρτες χρησιμοποιούν μνήμες τύπου flash, δηλαδή αλληλουχίες από flip flop που αποθηκεύουν πληροφορίες. Για να διατηρηθεί βέβαια η μνήμη στην κατάσταση που θέλουμε (δηλαδή να έχει τα στοιχεία που αποθηκεύσαμε), απαιτείται η τακτική τροφοδοσία της με ηλεκτρικό ρεύμα, αντίθετα με τις μαγνητικές κάρτες που αποθηκεύουν οτιδήποτε πάνω σε μια μαγνητική ταινία (και η κατάσταση των δεδομένων εξαρτάται μόνο από το αν η κάρτα έρθει σε επαφή με κάποιο μαγνητικό πεδίο – δεν απαιτείται η ύπαρξη ρεύματος για την διατήρηση των δεδομένων, ακριβώς όπως και στις αναλογικές κασέτες ήχου). Μόλις ο χρήστης εισάγει την έξυπνη κάρτα στο ειδικό μηχάνημα ανάγνωσης / εγγραφής (το είδος του μηχανήματος εξαρτάται από το είδος της χρήσης της κάρτας), η κάρτα τροφοδοτείται με ρεύμα και ειδικοί πυκνωτές και τρανζίστορ στο ολοκληρωμένο κύκλωμά της τροφοδοτούνται και αποθηκεύουν κάποια ποσότητα. Αυτό βέβαια δεν είναι αναγκαίο για την μερίδα έξυπνων καρτών που χρησιμοποιούν μνήμη τύπου EEPROM η οποία δεν χρειάζεται καθόλου ρεύμα για την διατήρηση των δεδομένων αλλά είναι σαφώς πιο αργές στην ανάγνωση και την εγγραφή από τις κάρτες με μνήμη τύπου flash.

Αφού έχουμε αναλύσει πλήρως το βασικά μέρη των έξυπνων καρτών, πολλοί που ασχολούνται με αυτές κατηγοριοποιούν αυτές τις κάρτες με βάση τις δυνατότητες του ολοκληρωμένου κυκλώματος που βρίσκεται όπως είδαμε πάνω της. Έτσι λοιπόν, μπορούμε να έχουμε τις εξής κατηγορίες :

Memory Cards ή κάρτες μνήμης. Αυτές οι κάρτες μπορούν να αποθηκεύουν πληροφορίες και δεδομένα, ενώ παράλληλα δεν έχουν καμιά δυνατότητα επεξεργασίας αυτών ακριβώς των δεδομένων. Περιέχουν απλώς κυκλώματα μνήμης (σε μορφή προσωρινής μνήμη, κάτι που σημαίνει ότι η μη χρήση τους για αρκετό καιρό ή η παρενέργεια από μαγνητικά μέσα μπορούν να καταστρέψουν την κάρτα).

Wired Logic aka Intelligent Memory Cards ή κάρτες μνήμης ολοκληρωμένης λογικής. Αυτή η κατηγορία καρτών περιέχει κάποιου είδους λογική ενσωματωμένη, η οποία

4.5 Έξυπνες κάρτες & Ψηφιακό χρήμα

Η έννοια του ψηφιακού χρήματος είναι στενά συνδεδεμένη με τις κάρτες και τα ηλεκτρονικά κουπόνια γενικότερα, από την αρχή της εμφάνισης των δύο όρων αυτών. Ιδιαίτερα τα τελευταία χρόνια, με την εμφάνιση των τελευταίων μελών της οικογένειας των ηλεκτρονικών κουπονιών, των έξυπνων καρτών, η έννοια του ηλεκτρονική /ψηφιακού χρήματος διευρύνθηκε εξαιρετικά και μπήκε σε μια άλλη καινούργια διάσταση, εντελώς διαφορετική από όσα είχαμε συνηθίσει, δει και ζήσει μέχρι και σήμερα, ανοίγοντάς μας μπροστά στα μάτια μας έναν γενναίο νέο κόσμο.

Αν προσπαθήσουμε να εισχωρήσουμε στην ουσία του όρο, εδώ θα παρατηρήσουμε ότι σημασία έχει το χρήμα και όχι το μέσο. Συνεπώς, όλα τα ηλεκτρονικά / ψηφιακά κουπόνια αποτελούν απλώς και μόνο το αναγκαίο όχημα του ηλεκτρονικού / ψηφιακού χρήματος (ή e-cash όπως έχει επικρατήσει τα τελευταία χρόνια να ονομάζεται) ώστε αυτό να κινηθεί.

Χωρίς το ψηφιακό χρήμα κανένα κουπόνι που αφορά ηλεκτρονικές συναλλαγές δεν έχει αντικειμενική αξία αλλά και αντιστρόφως ανάλογα, χωρίς το ψηφιακό χρήμα, κανένα κουπόνι δεν έχει νόημα ύπαρξης. Η ανάλυση της έννοιας του ψηφιακού χρήματος, είναι σίγουρα εκτός θέματος και δεν θα ασχοληθούμε σε αυτό το σημείο με αυτό το θέμα. Εμείς θα ασχοληθούμε παρακάτω με τον φορέα του, τα ηλεκτρονικά κουπόνια και ειδικότερα το τελειότερο μέλος αυτής της ομάδας, τις έξυπνες κάρτες.

Βλέπουμε λοιπόν ότι υπάρχει άμεση εξάρτηση μεταξύ του ψηφιακού χρήματος και δει των έξυπνων καρτών. Με βάση αυτήν την μοναδική σχέση, αλλά και λαμβάνοντας υπ' όψιν το γενικότερο κοινωνικό, πολιτικό, οικονομικό και διαπροσωπικό περιβάλλον μπορούμε να εξάγουμε πραγματικά ενδιαφέροντα αποτελέσματα.

Σε γενικές αλλά όχι και τόσο σπάνιες περιπτώσεις, το ψηφιακό χρήμα φτάνει στο σημείο να ταυτίζεται με τις έξυπνες κάρτες. Αυτό είναι καθαρά θέμα ανθρώπινης ψυχολογίας, που απλώς δεν μπορεί να κατανοήσει μέχρι ένα βαθμό, το ότι το ψηφιακό χρήμα είναι εντελώς αυλό, χωρίς καμιά φυσική απόσταση και χωρίς αρχή και τέλος.

συνήθως ασχολείται με την πρόσβαση στην μνήμη της κάρτας και τίποτα άλλο ιδιαίτερο. Οι περισσότερες κάρτες του είδους χρησιμοποιούν μνήμη τύπου EEPROM .

Processor Cards ή κάρτες με επεξεργαστή. Αυτού του είδους οι κάρτες περιέχουν μνήμη αλλά και επεξεργαστή και γι' αυτό και έχουν αξιοθαύμαστες δυνατότητες επεξεργασίας. Πολύ συχνά, αυτή η δύναμη επεξεργασίας δεδομένων χρησιμοποιείται με την κωδικοποίηση και αποκωδικοποίηση των πληροφοριών και δεδομένων της μνήμης. Γι' αυτό τον λόγο αυτή η κατηγορία κατέχει ένα πολύ ξεχωριστό χαρακτηριστικό, που αντιστοιχεί στον ιδιοκτήτη της και μόνο σε αυτόν. Βέβαια, η επεξεργασία των δεδομένων επιτρέπει την δυναμική αποθήκευση και διαχείριση δεδομένων, κάτι το οποίο καθιστά αυτού του είδους τις κάρτες ένα πολύτιμο και εξαιρετικά εύχρηστο εργαλείο. Οι περισσότερες κάρτες της κατηγορίας χρησιμοποιούν μνήμη τύπου flash που ενδείκνυται για την μεγάλη ταχύτητά της στην ανάγνωση και εγγραφή.

Φυσικά, όλα τα παραπάνω τα αναφέραμε στην γενική μορφολογία της κάρτας και τώρα μπορούμε να τα κατανοήσουμε πολύ πιο εύκολα. Σημειώνουμε ότι οι μαγνητικές κάρτες ανήκουν στην πρώτη κατηγορία ενώ οι έξυπνες κάρτες στην τρίτη. Η δεύτερη κατηγορία απαρτίζεται από μερικές εξελιγμένες μαγνητικές κάρτες αλλά και αρκετές «πρώιμα» σχεδιαστικά έξυπνες κάρτας, κυρίως την περίοδο της πρώτο εμφάνισής αυτών. Η σειρά που παρουσιάζουμε τις παραπάνω κατηγορίες είναι ουσιαστικά χρονολογική και δείχνει την μετάβαση από ένα είδος στο άλλο, τα οποία αναλύσαμε και πιο πάνω. Συνεπώς, οι έξυπνες κάρτες που είναι και οι μεταγενέστερες, είναι και οι πιο προηγμένες τεχνολογικά από όλες τις άλλες.

Παράλληλα βέβαια με την ασφάλεια της κάρτας, σημείο αναφοράς θα πρέπει να είναι η ασφάλεια του δικτύου όπου θα μεταφέρονται ή θα εισέρχονται δεδομένα από την κάρτα στον έξω κόσμο, όπου η χρήση ενός πρωτοκόλλου ασφαλείας (SSL ή Secure Socket Layer) θεωρείται επιβεβλημένη. Παράλληλα, ειδική έρευνα θα πρέπει να υπάρξει και στο κατά πόσο το λογισμικό που θα χρησιμοποιηθεί κατά την επικοινωνία είναι ασφαλές (π.χ. κατά πόσο τα προγράμματα «shopping cart» και «wallet» που χρησιμοποιούνται κυρίως σε συναλλαγές μέσω internet είναι ασφαλή για την χρήση τους με την έξυπνη κάρτα.

4.6 Χρήση και λειτουργία

Οι έξυπνες κάρτες σχεδιάστηκαν καταρχήν με απώτερο σκοπό να αποτελέσουν το πιο εύχρηστό και ασφαλές τύπο κουπονιών. Αυτό συνεπάγεται ότι κύρια κατεύθυνση κατά την κατασκευή τους είναι η ευχρηστία από την πλευρά και του πελάτη (που θα μπορεί να την χρησιμοποιεί πολύ εύκολα μέσα σε μικρό χρονικό διάστημα) αλλά και η ασφάλεια του τελευταίου (όπως αναφέραμε και πιο πάνω το θέμα ασφάλεια είναι το κυριότερο πρόβλημα όλων των ειδών των κουπονιών). Φυσικά, η χρήση κάθε έξυπνης κάρτας εξαρτάται από τον λόγο που θα την χρησιμοποιήσουμε. Συνεπώς άλλες μπορούμε να χρησιμοποιούμε για τραπεζικές ανάληψης από ATM μηχανήματα και άλλες για απλή αυθεντικοποίησης. Τα τελευταία χρόνια, κύρια κατεύθυνση των προσπαθειών που γίνονται από πολλές εταιρίες στον κόσμο με πρωτοπόρα την IBM είναι η δημιουργία έξυπνων καρτών που θα έχουν πολλαπλές λύσεις. Αν και αυτό παραπέμπει στο μακρινό μέλλον, τα πρώτα δείγματα είναι κάτι παραπάνω από ενθαρρυντικά. Κύριο πρόβλημα στην ολοκλήρωση αυτού του σχεδίου είναι η τεχνολογία καθότι το ολοκληρωμένο κύκλωμα της κάρτας θα πρέπει να είναι εξαιρετικά πολύπλοκο για τις διάφορες εφαρμογές, κάτι που σήμερα είναι δύσκολο να κατασκευαστεί. Όμως με τον ρυθμό ανάπτυξής της, σίγουρα το μέλλον ανήκει σε αυτές τις έξυπνες κάρτες πολλαπλών εφαρμογών.

Με την αύξηση της διαθέσιμης υπολογιστικής δύναμης και της μνήμης, μεγαλώνει και ο αριθμός των εφαρμογών όπου χρησιμοποιούνται οι έξυπνες κάρτες. Αν και στην Ελλάδα μας η κατάσταση δεν είναι ίδια όπως και στο εξωτερικό, δειλά-δειλά έχουν αρχίσει να κάνουν την εμφάνισή τους. Έτσι λοιπόν, στα παραδείγματα των ολοένα αυξανόμενων εφαρμογών των έξυπνων καρτών περιλαμβάνονται τα εξής :

Σε πολλές χώρες οι έξυπνες κάρτες αντικαθιστούν τις μαγνητικές κάρτες για πιστωτικές ή χρεωστικές εφαρμογές. Σε αυτό βοήθησε και η τεράστια ανάπτυξη των τηλεπικοινωνιών. Με την χρήση ειδικευμένων μηχανημάτων ικανών να διαβάζουν έξυπνες κάρτες, η πληρωμή είναι πλέον θέμα χρόνου καθώς όλα αυτά τα μηχανήματα βρίσκεται συνεχώς συνδεδεμένα με βασικά τραπεζικά δίκτυα που επαληθεύουν οποιαδήποτε πληροφορία και εκτελούν οποιαδήποτε εντολή από και προς κάποιον τραπεζικό λογαριασμό. Μάλιστα, τα τελευταία χρόνια εμφανίστηκαν και τέτοιες σπιτικές

συσκευές που μπορούμε να χρησιμοποιήσουμε για να κάνουμε αγορές μέσω του Internet χωρίς βέβαια να χρειάζεται να γνωρίζουμε τον αριθμό της πιστωτικής μας κάρτας.

Όπως είδαμε πιο πάνω, οι έξυπνες κάρτες διευκολύνουν απεριόριστα τις συναλλαγές μας μέσω του διαδικτύου. Αυτό είναι ένα μεγάλο ατού αυτού του είδους των καρτών καθότι είναι πολύ γνωστά σε όλους μας τα πλεονεκτήματα που έχει η διεκπεραίωση εμπορικών συναλλαγών μέσω διαδικτύου : Τα πάντα γίνονται πολύ πιο εύκολα, πολύ πιο γρήγορα και σύντομα θα είναι και πολύ πιο αξιόπιστα.

Και επειδή το μέλλον φαίνεται ότι ανήκει στο διαδίκτυο, το ίδιο συμβαίνει και με τις έξυπνες κάρτες. Μέσω του διαδικτύου, ο χρήστης συνδέει την έξυπνη κάρτα του και έτσι γίνεται ο κόμβος ανάμεσα στο προϊόν που επιθυμεί να αγοράσει και την τράπεζά του. Η μεταφορά των χρημάτων είναι επίσης αυτόματη από την τράπεζα στον προορισμό που επιθυμεί ο χρήστης. Σημειώνουμε ότι η ασφάλεια είναι ιδιαίτερα αυξημένη. Άλλωστε, κανένας τραπεζικός οργανισμός δεν θα ήθελε να αμαυρώσει την φήμη του σε ιδιαίτερα τεχνολογικούς τομείς όπως οι έξυπνες κάρτες. Και αυτό γιατί επειδή είναι μια νέα προοπτική την οποία δεν την γνωρίζει ένα μεγάλο μέρος του πληθυσμού, η αγορά για τις τράπεζες είναι ανοικτή και όλες προσπαθούν να κατακτήσουν το μεγαλύτερο κομμάτι της.

Τα κινητά τηλέφωνα (τόσο τα GSM όσο και τα DCS καθώς και τα αμερικάνικα) απαιτούν την εισαγωγή μιας κάρτας SIM (Subscriber Identity Module ή Κλάση Αναγνώρισης Ταυτότητας) για να λειτουργήσουν. Αυτές οι κάρτες είναι έξυπνες κάρτες στις οποίες αποθηκεύεται η πληροφορία για την ταυτότητα και το μυστικό κλειδί του χρήστη (παρόλο που δεν σχετίζονται με κάποιον συγκεκριμένο χρήστη).

Παρατηρούμε ότι αν και η SIM κάρτα είναι σχετικά μικρή σε μέγεθος και δεν ανταποκρίνεται στο πρότυπο ISO που αναφέραμε, στην πραγματικότητα αυτό δεν είναι αλήθεια αφού όταν αγοράζουμε μια τέτοια κάρτα, πρέπει να σπάσουμε το μικρότερο κομμάτι που τοποθετούμε στο κινητό από μια μεγαλύτερη κάρτα που ανταποκρίνεται στο πρότυπο (αν και σήμερα κάποια κινητά τηλέφωνα δέχονται αυτή την αρχική κάρτα ολόκληρη χωρίς άλλη διαδικασία).

Μια άλλη κατηγορία όπου χρησιμοποιούνται ευρέως οι έξυπνες κάρτες είναι και ο τομέας της αυθεντικοποίησης, όπως είδαμε και πιο πάνω. Οι έξυπνες κάρτες μπορούν να χρησιμοποιηθούν πολύ πιο εύκολα από τις κοινές ταυτότητες καθώς μπορούν να περιέχουν μεγαλύτερο αριθμό στοιχείων και προσωπικών δεδομένων, ενώ ο έλεγχος της ταυτοπροσωπίας μετατρέπεται σε μια απλή ρουτίνα που κρατά μερικά δευτερόλεπτα. Αυτή η μέθοδος χρησιμοποιείται πολύ στην Αμερική αλλά και στο Χόλυγουντ. Σημειώνουμε ότι οι κάρτες που χρησιμοποιούνται στο πανεπιστήμιο Μακεδονίας για την είσοδο σε κάποια ειδικά εργαστήρια (όπως π.χ. τα εργαστήρια του πρώτου και του πέμπτου ορόφου στον πύργο της πληροφορικής) είναι μαγνητικές και όχι έξυπνες κάρτες.

Οι έξυπνες κάρτες ήδη χρησιμοποιούνται για την υποστήριξη εφαρμογών ηλεκτρονικού χρήματος. Έτσι σε πολλές περιπτώσεις αντικαθιστούν τις παλιές κοινές μαγνητικές πιστωτικές κάρτες και με την χρήση διαφόρων συσκευών, μπορούμε να ολοκληρώσουμε οποιαδήποτε εφαρμογή ηλεκτρονικού χρήματος θέλουμε.

Υπάρχουν ακόμα έξυπνες κάρτες που παράγουν γρήγορα ψηφιακές υπογραφές. Η έννοια των ψηφιακών υπογραφών μπήκε στην ζωή μας τα τελευταία πέντε χρόνια με την τεράστια ανάπτυξη του Internet. Και εφόσον οι ψηφιακές υπογραφές θεωρούνται σαν ένα από τα βασικά πλέον χαρακτηριστικά ασφάλειας, δεν θα μπορούσαν να λείπουν και οι έξυπνες κάρτες αφού η αυθεντικοποίησης κυρίως λογισμικού ή ατόμων συνδέεται άμεσα με την τεχνολογία των ψηφιακών υπογραφών. Φυσικά, μόνο οι έξυπνες κάρτες είναι ικανές για παραγωγή ψηφιακών υπογραφών, λόγω και τα ικανότητας λογισμικού που διαθέτουν.

Τα τελευταία χρόνια οι έξυπνες κάρτες έχουν εισβάλλει και στον τομέα των τηλεπικοινωνιών με την παραγωγή τηλεκαρτών και χρονοκαρτών που όλοι γνωρίζουμε. Χαρακτηριστικά είναι τα προϊόντα του ΟΤΕ στην Ελλάδα που με την έλλειψη κάποιου σοβαρού μέσου προστασίας, οδήγησε στην κυκλοφορία διάφορων «παράνομων» οδηγών (κυρίως στο Internet) που περιέχουν βήμα προς βήμα της διαδικασία cracking (σπάσιμο) των κωδικών τέτοιων καρτών και αλλαγή των δεδομένων (π.χ. πρόσθεση μονάδων σε μια τηλεκάρτα που έχει εξαντλήσει τις μονάδες που αρχικά είχε)! Οι τελευταίου είδους κάρτες που κυκλοφορούν, είναι έξυπνες κάρτες. Πριν από μερικά χρόνια, πολλοί θυμούνται την αντικατάσταση όλων των καρτών αλλά και των τηλεφώνων του ΟΤΕ που τις χρησιμοποιούσαν.

Αυτή η περίπτωση ήταν ουσιαστικά η αντικατάσταση των παλιότερων μαγνητικών καρτών με καινούργιες έξυπνες κάρτες, όπως και των μηχανημάτων ανάγνωσης και εγγραφής αυτών.

Πολλές φορές χρησιμοποιούνται έξυπνες κάρτες από διάφορες υπηρεσίες για την πρόσβαση του προσωπικού στις εγκαταστάσεις αλλά και σαν είδος ηλεκτρονικής ταυτότητας. Χαρακτηριστική είναι η σειρά X-FILES όπου το μόνο που βλέπουμε είναι ομοσπονδιακοί πράκτορες να κόβουν βόλτες σε στρατιωτικές ή κρατικές εγκαταστάσεις και να ανοίγουν ή να κλείνουν πόρτες με την χρήση έξυπνων καρτών (αν παρατηρήσουμε τους τίτλους αρχής και ιδιαίτερα την ταυτότητα του Fox Mulder μπορούμε να διακρίνουμε άνετα ότι στην πραγματικότητα είναι μια έξυπνη κάρτα αφού το ολοκληρωμένο σύστημα αλλά και το σύστημα barcode βρίσκονται σε εμφανή θέση πάνω του).

Όλα τα παραπάνω είναι ένα μικρό μα αντιπροσωπευτικό δείγμα για το πού χρησιμοποιούνται σήμερα οι έξυπνες κάρτες. Φυσικά και η λίστα θα μπορούσε να συμπληρωθεί και με πολλά άλλα παραδείγματα. Μεγάλο όμως ενδιαφέρον έχει η χρήση τους πάνω στο ηλεκτρονικό εμπόριο. Και αυτό γιατί από την μία είναι ιδανικά εργαλεία για την επίτευξη συναλλαγών και από την άλλη, κατά την αρχική κατασκευή τέτοιων καρτών, η προσοχή όλων ήταν στραμμένη στην εύρεση μιας λύσης πάνω στις ηλεκτρονικές συναλλαγές. Με την εμφάνιση των έξυπνων καρτών η ιδέα του ηλεκτρονικού χρήματος πήρε μια νέα πνοή και νέοι ορίζοντες ανοίχτηκαν στον τομέα των ηλεκτρονικών συναλλαγών.

Όπως αναφέραμε, οι έξυπνες κάρτες αποτελούν μια εξέλιξη των φυσικών κουπονιών που χρησιμοποιούμε. Έτσι, αποκτούν κάποια από τα πλεονεκτήματα αλλά και τα μειονεκτήματα αυτής της οικογένειας εργαλείων αυθεντικοποίησης που ανήκουν. Αυτό είναι και απόλυτα φυσικό με βάση την κατηγοριοποίησή τους που είδαμε πιο πάνω. Οι έξυπνες κάρτες είναι απλά ένα μέλος της οικογένειας των φυσικών κουπονιών. Αυτό και μόνο τις δεσμεύει πάνω σε κάποια θέματα και θέτει περιορισμούς πάνω σε άλλα, τα οποία θα αναλύσουμε πιο κάτω.

Παρακάτω υπάρχουν τα κύρια πλεονεκτήματα στην χρήση των έξυπνων καρτών, σε σύγκριση πάντα με παλιότερες τακτικές διεκπεραίωσης των διαδικασιών εμπορικών συναλλαγών που αναφέραμε και πιο πάνω στην εισαγωγή αυτής της μελέτης :

Η κρυπτογράφηση που μετασχηματίζει τα δεδομένα που είναι αποθηκευμένα, έτσι ώστε αυτά να είναι ακατάληπτα από τον εξωτερικό παρατηρητή. Συνεπώς μέσω αυτής, η αξία των υποκλοπών και η πιθανότητα για τροποποιήσεις εκμηδενίζεται. Επιπλέον η ικανότητα παραγωγής ψηφιακών πιστοποιητικών καθιστά κάθε κάρτα μοναδική. Με αυτό τον τρόπο η τυχών παραποίηση ανιχνεύεται εξαιρετικά εύκολα αλλά επίσης και η μη εξουσιοδοτημένη χρήση αποκλείεται με έναν απλό και μόνο έλεγχο.

Όσον αφορά τις παλιότερες μαγνητικές κάρτες, για να ολοκληρωθεί μια συναλλαγή απαιτούνταν από τον πωλητή να γνωρίζει τον αριθμό της πιστωτικής κάρτας, ενώ η συναλλαγή ολοκληρώνονταν αφού ο πωλητής ενημέρωνε την τράπεζα για αυτήν καθώς και για τον αριθμό της πιστωτικής κάρτας. Συνεπώς η χρέωση εξαρτιόταν μόνο από τον πωλητή ο οποίος θα μπορούσε πολύ εύκολα να χρεώσει την κάρτα με ένα διαφορετικό ποσό, από όσο έπρεπε. Αυτή η συναλλαγή «κοινής συναίνεσης» πολλές φορές αποδεικνύονταν ότι ήταν επικίνδυνη. Ο πελάτης χρεώνονταν με ποσά τα οποία δεν είχε ποτέ ξοδέψει από τους πωλητές. Και το χειρότερο ήταν ότι δεν μπορούσε να αποδείξει τίποτα, εφόσον δεν υπάρχει αντίστοιχος έλεγχος πάνω σε αυτόν τον τομέα. Η κάρτα δεν γνωρίζει αν την κρατά ο νόμιμος ιδιοκτήτης της ή όχι. Αυτό το σημαντικό πρόβλημα λύθηκε οριστικά με την εμφάνιση των έξυπνων καρτών στο προσκήνιο. Οι έξυπνες κάρτες όπως αναφέραμε διαθέτουν προηγμένες (σε σύγκριση πάντα με τις προγενέστερες κάρτες που είναι οι μαγνητικές) δυνατότητες κρυπτογράφησης. Εφόσον ο νόμιμος κάτοχος κρατάει μυστικό το προσωπικό του συνθηματικό που ενεργοποιεί την έξυπνη κάρτα του, κανείς δεν μπορεί να την χρησιμοποιήσει άντ' αυτού. Έτσι λοιπόν η χρήση γίνεται αυστηρά προσωπική και η χρέωση ενός ποσού στην κάρτα απαιτεί την ύπαρξη του νόμιμου κατόχου. Βλέπουμε λοιπόν ότι με εύκολο τρόπο λύνεται αυτός ο κίνδυνος της μη εξουσιοδοτημένης χρήσης μιας κάρτας.

Τα μέτρα προστασίας λογισμικού ώστε τα προγράμματα που εμπεριέχονται να είναι αρκετά ασφαλή και αξιόπιστα. Κύριος στόχος είναι η αποτροπή εξωτερικών επιθέσεων. Σε αυτά θα μπορούσαμε να συμπεριλάβουμε τα μέτρα ανάπτυξης που αποτελούν πρότυπα (standards) σύμφωνα με τα οποία σχεδιάζονται, κωδικοποιούνται, ελέγχονται

και συντηρούνται τα προγράμματα. Οι εταιρίες παραγωγής έξυπνων καρτών κρατάνε καλά κρυμμένα τα μυστικά του προγραμματισμού αυτών. Άλλωστε μια τυχών διαρροή πληροφοριών θα έπληττε ανεπανόρθωτα τις ίδιες, αφού ο τομέας της ασφάλειας είναι το κυριότερο κίνητρο για την επιλογή μια έξυπνης κάρτας. Σαφώς και οι τεχνικές λεπτομέρειες είναι ελεύθερες στην χρήση ή ανάγνωση από τον καθένα, ο μικρό προγραμματισμός όμως που είναι η κινητήρια δύναμη, είναι ένα καλά κρυμμένο μυστικό.

Τα μέτρα προστασίας υλικού που έχουν προβλεφτεί για να βοηθούν στην ασφάλεια. Αυτά ποικίλλουν από την υλοποίηση της κρυπτογράφησης με υλικό μέχρι και τα κυκλώματα για επιβεβαίωση της ταυτότητας χρηστών. Επίσης, σε αυτά μπορούμε επίσης να συμπεριλάβουμε χρωματισμούς και εικόνες πάνω στο φυσικό μέσο, αόρατα στο ανθρώπινο μάτι σχέδια ή ανάγλυφα αλλά και πολλά άλλα.

Το εξαιρετικά μικρό κόστος κατασκευής των έξυπνων καρτών αφού το πλαστικό αλλά και τα ολοκληρωμένα συστήματα πάνω σε σιλικόνη είναι σήμερα πάμφθηνα σε κόστος με την μεγάλη εξέλιξη που γνωρίζει η βιομηχανία τεχνολογικών προϊόντων. Μάλιστα, βασιζόμενοι στον τεράστιο βαθμό αυτοματοποίησης που γνωρίζει σήμερα η βιομηχανία τεχνολογικών προϊόντων, μπορούμε να πούμε με σιγουριά ότι η κατασκευή έξυπνων καρτών μπορεί να πλησιάσει το ρυθμός κατασκευής CD (Compact Disk) αλλά και το εξαιρετικό χαμηλό κόστος αυτών.

Αυτά είναι και τα σημαντικότερα πλεονεκτήματα της χρήσης των έξυπνων καρτών. Φυσικά αυτά δεν είναι και τα μόνο αλλά τα πιο σημαντικά. Ο καθένας μας θα μπορούσε να απαριθμήσει πολλά ακόμα πάνω στο θέμα. Πέρα όμως από τα όσο πλεονεκτήματα υπάρχουν, υπάρχουν και μειονεκτήματα τα οποία δεν μπορούμε να προσπεράσουμε.

Σίγουρα οι έξυπνες κάρτες αποτελούν την καλύτερη λύση, αλλά όπως συνήθως συμβαίνει δεν αποτελούν και την βέλτιστη. Παρακάτω παραθέτουμε τα κυριότερα προβλήματα χρήσης αλλά και γενικότερα μειονεκτήματα που αντιμετωπίζουν σήμερα, μετά από ένα σχετικά καλό χρονικό διάστημα από την πρώτο εμφάνισή τους (που μπορεί να χαρακτηριστεί από πολλούς ως δοκιμαστικό διάστημα στις πραγματικές συνθήκες, κάτι που συμβαίνει αρκετά συχνά και την δημιουργία μέχρι και την παραγωγή κάποιου προϊόντος.).

Οι έξυπνες κάρτες είναι απλά αντικείμενα και όπως όλη η οικογένεια των φυσικών κουπονιών, υπόκεινται στον ίδιο κίνδυνο. Η περίπτωση να χαθούν, να κλαπούν, να αντιγραφούν ή ακόμα και να παραποιηθούν. Ας μην ξεχνάμε ότι η τεχνολογία τις περισσότερες φορές δεν χρησιμοποιείται για καλούς σκοπούς υπέρ της ανθρωπότητας, αλλά και για άλλους σκοπούς όπως η υπηρεσία προσωπικών συμφερόντων. Με την κατάσταση που επικρατεί σήμερα, είναι απλά θέμα χρόνου να καταρριφθεί η ασφάλεια των έξυπνων καρτών. Ίσως αυτό δεν συμβεί την άλλη μέρα και χρειαστεί να πάρει χρόνο, όμως το σίγουρο είναι ότι θα συμβεί. Πέρα από την αντιγραφή ή την παραποίηση όπου απαιτούνται ειδικές τεχνολογικές γνώσεις, οι περιπτώσεις απώλειας ή κλοπής είναι εξίσου σημαντικές και πρέπει να μας απασχολούν.

Η αποκλειστική αντικατάσταση παραδοσιακών τρόπων διεκπεραίωσης εμπορικών συναλλαγών από τις έξυπνες κάρτες, εγκυμονεί σίγουρα και νέους πρωτοεμφανιζόμενους κινδύνους. Όταν ο άνθρωπος εξαρτάται από την μηχανή ποτέ δεν μπορεί να είναι σίγουρος. Και αυτό για ένα μικρό λάθος στον προγραμματισμό μπορεί να κοστίσει αρκετά στο όλο σύστημα αλλά και τον ίδιο τον άνθρωπο. Αυτό βέβαια βαραίνει περισσότερο τις εταιρίες που εκδίδουν τις κάρτες αλλά τις εταιρίες που κατασκευάζουν τα ειδικά μηχανήματα ανάγνωσης και εγγραφής. Οι τράπεζες άλλωστε ασφαλίζονται με υπερμεγέθη ποσά για τέτοιες περιπτώσεις απέναντι στις εταιρίες που κατασκευάζουν αυτόν τον τεχνολογικό εξοπλισμό που χρησιμοποιούν.

Εκτός από τα παραπάνω, οι έξυπνες κάρτες και ιδιαίτερα η μορφή του ψηφιακού χρήματος που αντιπροσωπεύουν μπορεί να αποτελέσει ένα μεγάλο κίνδυνο για την οικονομία. Με την χρήση ψηφιακού χρήματος, υπάρχει πάντα η πιθανότητα για εμφάνιση ενός ασταθούς ποσοστού εισαγωγών και πληθωρισμού. Αυτό οφείλεται κατά ένα βαθμό στο ότι ο άνθρωπος χάνει πλέον την επαφή που είχε με το φυσικό χρήμα και κατά κάποιο τρόπο σταματά να διακρίνει πόσα ξοδεύει σε σχέση με το παρελθόν. Αυτό μπορεί να οδηγήσει σε διατάραξη των εθνικών χρηματικών αποθεμάτων οδηγώντας σε χειρότερες καταστάσεις, αν πάρει αρκετά μεγάλη μορφή. Σε τελική ανάλυση, η πιθανότητα μιας οικονομικής κρίσης δεν είναι μακριά, όπως υποστηρίζει και ο Tatsuo Tanaka, καθηγητής του τμήματος τηλεπικοινωνιών στο Εθνικό Πανεπιστήμιο Ιαπωνίας, στο έργο του «Πιθανές Οικονομικές Επιπτώσεις του Ψηφιακού Χρήματος» που υπάρχει σε ελεύθερη μορφή-διανομή και στην διεύθυνση στο διαδίκτυο :

(http://www.virtualschool.edu/mon/ElectronicProperty/EconomicConseqDigiCash.html)

Τα τελευταία χρόνια η φρενίτιδα (ειδικά στην χώρα μας) για την συνθήκη του Σέγκεν, έχει κατακλύσει πολλούς πολίτες. Φυσικά, όλη αυτή η κατάσταση δεν θα άφηνε από έξω και τις έξυπνες κάρτες. Έτσι, πολλοί τις αποφεύγουν θεωρώντας ότι έχουν πάνω τους το ίδιο το χάραγμα του θηρίου, τον αριθμό 666. Άλλοι υποστηρίζουν ότι είναι το πρώτο βήμα για την σφράγιση των ανθρώπων με μικροτσίπ και την υποδούλωσή τους στον Σατανά. Αυτό το πανηγύρι συνεχίζεται με πολλές ακόμα απόψεις που αν και είναι ενδιαφέρουσες για το περιβάλλον της παρέας και του «χαβαλέ», σίγουρα δεν ανήκουν εδώ. Βέβαια, η εμφύτευση θα έλυνε το παραπάνω μειονέκτημα (ειδικά στο δεξί χέρι ή στο μέτωπο).

Είδαμε λοιπόν τα σημαντικότερα χαρακτηριστικά των έξυπνων καρτών αλλά πολλές χρήσεις τους μέσα στην μικρή μας κοινωνία. Είδαμε τα τεχνικά τους χαρακτηριστικά αλλά και τα πλεονεκτήματα και μειονεκτήματα που έχουν απέναντι σε άλλους εναλλακτικούς τρόπους που αναφέραμε. Σίγουρα, αυτό το κείμενο αποτελεί μια ελάχιστη μελέτη πάνω σε αυτό το ζήτημα αλλά ελπίζουμε πως είναι πλήρης και αρκετά κατατοπιστική σαν εισαγωγή στις έξυπνες κάρτες.

Κάτι όμως που συνήθως περνά απαρατήρητο από όλους, είναι ότι η χρήση των έξυπνων καρτών δημιουργεί ουσιαστικά ένα ρεύμα για την χρήση ηλεκτρονικού χρήματος. Εκ πρώτης όψεως αυτό δεν φαίνεται να είναι και τόσο σημαντικό. Όμως στην πραγματικότητα είναι. Οι έξυπνες κάρτες δημιουργήθηκαν χωρίς να υπάρχει η έννοια του ηλεκτρονικού χρήματος, απλά σαν ένα μέσο για πιο γρήγορες και ασφαλείς συναλλαγές. Φυσικά, κανένας από αυτούς που την επινόησαν δεν είχαν στο μυαλό τους την έννοια του ηλεκτρονικού χρήματος και έτσι, ούτε την επιδίωκαν. Αυτό όμως εμφανίστηκε μετά από λίγο καιρό σαν απρόβλεπτο αποτέλεσμα της αλλαγής που έφεραν οι έξυπνες κάρτες στην κοινωνία μας. Σήμερα αυτό γίνεται όλο και πιο αισθητό παντού. Και όπως πολύ υποστηρίζουν, αυτή θα είναι και η ταφόπλακα της έξυπνης κάρτας!

Ίσως η παραπάνω ιδέα να φαίνεται τρομερά εξωπραγματική και ακραία αλλά έχει σταθερές βάσεις. Ο άνθρωπος γνώρισε τα οφέλη των έξυπνων καρτών, αλλά και τα μειονεκτήματά τους. Λογικό επόμενο βήμα θα ήταν να επινοήσει τον διάδοχο των έξυπνων καρτών, που θα έχει όλα τα προτερήματά τους ή περισσότερα, και κανένα από

τα μειονεκτήματά τους. Αυτό το βήμα ανταποκρίνεται απόλυτα στο ηλεκτρονικό χρήμα και γι' αυτό πολλοί υποστηρίζουν ότι θα αποτελέσει την εικονική συνέχεια του φυσικού πλαστικού χρήματος. Μόνο ο χρόνος θα δείξει αν αυτή η πρόβλεψη, που πρώτος από όλους συμμερίστηκε ο Άλβιν Τόφλερ στο έργο του «Το τρίτο κύμα» θα βγει στο μέλλον αληθινή ή όχι. Το μόνο σίγουρο είναι το ηλεκτρονικό χρήμα και οι έξυπνες κάρτες συνδέονται πολύ στενά και η εξέλιξή τους για αρκετό καιρό ακόμα θα είναι αναλογική, η μία προς την άλλη.

4.7 Και με την Ελλάδα ... τι γίνεται;

Σε αυτό το σημείο νομίζουμε ότι αξίζει να ρίξουμε και μια ματιά στην χώρα μας και την κατάσταση που επικρατεί. Αξίζει επίσης να δούμε τον συνολικό βαθμό χρήσης των έξυπνων καρτών, καθώς επίσης και την γενικότερη αντιμετώπιση αυτών από τον σύγχρονο Έλληνα. Και αυτό γιατί ενώ όπως αναφέραμε πιο πάνω, η κατάσταση στο εξωτερικό είναι περισσότερο από ενθαρρυντική για τις έξυπνες κάρτες, η κατάσταση στην Ελλάδα, τόσο λόγω τεχνολογικής και οικονομικής ανάπτυξης, όσο και από τα ίδια χαρακτηριστικά του έθνους μας, είναι εντελώς διαφορετική από όσα συμβαίνουν στο εξωτερικό.

Πριν από μερικά χρόνια στην Ελλάδα επικρατούσαν μαύρα μεσάνυχτα για το συγκεκριμένο θέμα, όπως και για πολλά άλλα θέματα άλλωστε. Ο ίδιος ο όρος «Smart Cards» ήταν εντελώς άγνωστος στους περισσότερους. Όμως πριν από μερικά χρόνια είδαμε μια τρομακτική ανάπτυξη πάνω στην χρήση τους. Σε αυτό βέβαια συνέβαλλε ένας κυρίως παράγοντας. Τα κινητά τηλέφωνα. Όπως είπαμε τα κινητά τηλέφωνα χρησιμοποιούν έξυπνες κάρτες για να λειτουργήσουν. Αυτό το μεγαλύτερο μέρος των χρηστών δεν το γνωρίζουν. Η αλήθεια όμως είναι αυτή. Και σήμερα, με βάση διάφορες στατιστικές μελέτες, μικρό είναι το ποσοστό που δεν χρησιμοποιεί κινητό τηλέφωνο (περίπου εννέα εκατομμύρια συνδρομητές υπάρχουν σήμερα στον τόπο μας). Αν μάλιστα συμπεριλάβουμε και τις τηλεκάρτες αλλά και τις πιστωτικές κάρτες μερικών τραπεζικών οργανισμών που αποφάσισαν να χρησιμοποιήσουν αυτό το πρότυπο για το κοινό, το ποσοστό σήμερα που χρησιμοποιεί καθημερινά έξυπνες κάρτες είναι πραγματικά αρκετά μεγάλο.

Βέβαια, όπως είπαμε το μεγαλύτερο μέρος του πληθυσμού δεν γνωρίζει τίποτα για τις έξυπνες κάρτες. Παράλληλα, πολλοί τομείς για τους οποίους χρησιμοποιούνται στο εξωτερικό, στην Ελλάδα δεν υπάρχουν. Σύμφωνα με έρευνες, οι Έλληνες είναι εξαιρετικά συντηρητικοί πάνω στην χρήση νέων τεχνολογιών αλλά και στις αγορές μέσω του διαδικτύου. Αυτή η εξέλιξη επιβραδύνει την περαιτέρω διάδοση αυτών των ψηφιακών κουπονιών. Ο μόνος που γνωρίζει ποια θα είναι η εξελικτική τους πορεία είναι ο χρόνος, αν και πολλοί προβλέπουν ότι θα ενσωματωθούν πλήρως στην Ελληνική οικονομία κυρίως λόγω της Ευρωπαϊκής Ένωσης. Οι υπόλοιπες χώρες έχουν σαφώς μεγαλύτερο ποσοστό χρήστης από τον πληθυσμό και σίγουρα οι τραπεζικοί οργανισμοί (που είναι οι κύριοι ρυθμιστές όλων των οικονομικών συναλλαγών) θα επιδιώξουν αυτήν την προσέγγιση.

Ήδη βέβαια έχουν κάνει την εμφάνισή τους τραπεζικά πρότυπα βασισμένα σε εισαγόμενες ψηφιακές τεχνολογίες. Χαρακτηριστικό παράδειγμα είναι η Nova Bank και η Win Bank που είναι οι πρώτες που εμφανίστηκαν. Οι πρώτες ενδείξεις είναι ενθαρρυντικές ενώ η εξοικείωση των Νεοελλήνων με τέτοια πρότυπα είναι μεν αργή αλλά σταθερή. Οι ηλεκτρονικές – ψηφιακές αυτές τράπεζες σίγουρα στο μέλλον θα δώσουν τρομερή ώθηση στις έξυπνες κάρτες. Και αυτό γιατί οι έξυπνες κάρτες είναι το κλειδί για την χρήση των υπηρεσιών τέτοιου είδους υπηρεσιών. Οι συναλλαγές ολοκληρώνονται μόνο μέσω αυτών ενώ είναι ουσιαστικά το κλειδί για τον προσωπικό λογαριασμού κάποιου.

Βέβαια υπάρχουν και κάποιοι παράγοντες που εμποδίζουν αυτή την εξέλιξη, ενώ συνδέονται άμεσα με την Ελλάδα. Πρώτος από αυτούς είναι η προμήθεια. Η τελευταία στην Ελλάδα είναι ιδιαίτερα υψηλή σε σχέση με άλλες χώρες. Αναφέρουμε χαρακτηριστικά ότι είναι υπερδιπλάσια σε σχέση με τον μέσο όρο στην Ευρωπαϊκή Ένωση.

Αυτό και μόνο καθιστά ιδιαίτερα δαπανηρή την κατοχή πολλών ειδών καρτών – και από ότι γνωρίζουμε σήμερα υπάρχουν πάρα πολλά είδη. Η προμήθεια των πλαστικών καρτών βέβαια επηρεάζεται από πολλούς και διάφορους παράγοντες, οι περισσότεροι από τους οποίους είναι βασικοί παράγοντες της οικονομίας. Η εξέλιξη της τελευταίας και μόνο θα μπορούσε ίσως να δώσει λύση στο θέμα.

Άλλος ένας παράγοντας που φέρεται να εμποδίζει την εξάπλωση της χρήσης έξυπνων καρτών μέσα στην νεοελληνική κοινωνία είναι η γενικότερη δυσπιστία που δείχνει ο Έλληνας απέναντι σε κάθε τι καινούργιο. Ιδιαίτερα, ότι αφορά την τσέπη του και τα χρήματα που έχει, η στάση τις περισσότερες φορές είναι εντελώς αρνητική. Ίσως είναι ψυχολογικό το θέμα, ίσως ιστορικά κατάλοιπα στην μνήμη του λαού μας. Η αλήθεια είναι όμως ότι θα χρειαστεί πολύς και μεγάλος κόπος έτσι ώστε να πειστεί ο νεοέλληνας να εγκαταλείψει το φυσικό χρήμα για μία μικρή πλάκα πλαστικού. Αν αναφερθούμε και στην συνθήκη του Σέγκεν όπως είδαμε παραπάνω, η όλη κατάσταση παίρνει μια καινούργια εντελώς ανατρεπτική τροπή.

Σίγουρα λοιπόν το μέλλων των έξυπνων καρτών προδιαγράφεται λαμπρό, παρόλα τα προβλήματα. Και αυτό γιατί το μέλλον των έξυπνων καρτών έχει ήδη προδιαγραφεί στο εξωτερικό, όπου χρησιμοποιούνται κατά κόρον και με μεγάλη επιτυχία αλλά και ασφάλεια.

Η μικρή Ελλάδα μας συνεπώς δεν μπορεί παρά να ακολουθήσει τις εξελίξεις. Σίγουρα η εξοικείωση με αυτό τον νέο τρόπο συναλλαγών δεν είναι ότι πιο εύκολο για τον μέσο Έλληνα, όμως από την άλλη όταν αναφερόμαστε στα χρήματα κάποιου, δεν χωράει τίποτα περισσότερο. Χαρακτηριστικό παράδειγμα είναι και η κυκλοφορία του Euro στην Ελλάδα.

Αν και στην αρχή οι Έλληνες το αντιμετώπιζαν διστακτικά, μόλις κατανόησαν ότι θα γίνει οριστική αντικατάσταση της δραχμής με αυτό, σε ελάχιστο χρονικό διάστημα μπόρεσαν και εξοικειώθηκαν με αυτό!

4.8 Οργανισμοί και πρότυπα

Σε αυτό το σημείο καλό είναι να αναφέρουμε τους κύριους κατασκευαστές έξυπνων καρτών αλλά και την χρήση των προϊόντων τους. Σημειώνουμε ότι η παρακάτω λίστα περιλαμβάνει τους πιο αντιπροσωπευτικούς εκπροσώπους του χώρου, αλλά και εταιρίες που έδωσαν στην δημοσιότητα διάφορα πρωτοποριακά προϊόντα. Παράλληλα, όπου βέβαια είναι δυνατόν, αναφέρονται και διευθύνσεις με παραπομπές στο διαδίκτυο όπου μπορείτε να βρείτε περισσότερες πληροφορίες πάνω στο θέμα μας.

Data Key Smart Cards (http://www.datakey.com) που χρησιμοποιούνται είτε σαν συμβατικές έξυπνες κάρτες είτε σαν αποθηκευτικά μέσα για διάφορες λειτουργίες. Η συγκεκριμένη εταιρία κατάφερε να περάσει μέσα από ένα σκληρό ανταγωνισμό σώα, και δίκαια σήμερα θεωρείται ως μια από τις μεγαλύτερες εταιρίες κατασκευής έξυπνων καρτών.

Carte Bancaire ονομάζεται η εκδοχή της έξυπνης κάρτας για την ομώνυμη τράπεζα στην Γαλλία. Η επιτυχία που έχει είναι τεράστια αλλά και πρωτοφανής. Σύμφωνα με πρόχειρους υπολογισμούς ο αριθμός τέτοιου είδους έξυπνων καρτών που κυκλοφορούν σήμερα στην Γαλλία ξεπερνάει τα είκοσι δύο εκατομμύρια! Η συγκεκριμένη κάρτα τραπεζικών συναλλαγών αντικατέστησε τις πρόσφατες μαγνητικές κάρτες, που χρησιμοποιούνταν μέχρι και πριν από μερικά χρόνια, με μεγάλη επιτυχία. Μάλιστα, πρόκειται για την έξυπνη κάρτα τραπεζικών συναλλαγών που έχει εκδοθεί στον μεγαλύτερο αριθμό αντιτύπων.

Η επίσης γαλλική Telecarte του αντίστοιχου εθνικού οργανισμού τηλεπικοινωνιών. Εύκολα μπορούμε να μαντέψουμε ότι πρόκειται για... τηλεκάρτες! Η Γαλλία ήταν η πρώτη χώρα όπου εμφανίστηκαν και σήμερα έχει και την μεγαλύτερη εξάπλωση σε σχέση πάντα με τον συνολικό πληθυσμό. Χαρακτηριστικό είναι ότι το τσιπ της κάρτας περιέχει μόνο μνήμη εκτός βέβαια και από το λογισμικό. Αντίθετα με την παραπάνω κάρτα, αυτό το είδος τηλεκάρτες μπορεί να κυκλοφορεί και να τυπώνεται σε πολύ μεγαλύτερους αριθμούς αντιτύπων, αλλά όπως είπαμε υπολείπεται της πλήρους υπολογιστικής ισχύς της πρώτης. Γι' αυτό τον λόγο πολλοί δεν την κατατάσσουν στον χώρο των έξυπνων καρτών αλλά την θεωρούν υβρίδιο ανάμεσα στις παλιές μαγνητικές κάρτες και τις νεότερες έξυπνες κάρτες.

Εμείς, βασιζόμενοι στην κοινή αρχιτεκτονική έξυπνων καρτών και τηλεκαρτών, θα τις κατατάξουμε στην ίδια κατηγορία.

Ο εθνικός οργανισμός υγείας στην Γερμανία αποφάσισε πριν από μια δεκαετία να χρησιμοποιήσει έξυπνες κάρτες για κάθε ασφαλιζόμενο. Αυτό το γιγαντιαίο πρόγραμμα σήμερα έχει ολοκληρωθεί βάζοντας την Γερμανία στην τρίτη θέση του πίνακα με τις χώρες όπου χρησιμοποιείται περισσότερο η έξυπνη κάρτα (μετά τις Ηνωμένες Πολιτείες Αμερικής και την Γαλλία). Μάλιστα, η Γερμανία είναι η πρώτη χώρα στον κόσμο που

καταφέρνει έναν τέτοιο άθλο, που όμως θα την ωφελήσει αρκετά. Τώρα πια, ο κάθε ασθενής θα μπορεί να κουβαλά μαζί του όλες τις εξετάσεις που έχει κάνει, ολόκληρο το ιστορικό του αλλά και τα προσωπικά του στοιχεία.

Chip Net Smart Cards
(http://www.chipnet.com) που χρησιμοποιούνται σαν συμβατικές έξυπνες κάρτες κυρίως για τοπικά δίκτυα εταιριών ή άλλα τοπικά δίκτυα στα οποία οι απαραίτητες πληροφορίες αποθηκεύονται σε ένα κεντρικό υπολογιστικό σύστημα (συνήθως mainframe).

Smart Media Memory Cards
(http://www.flashmemory.com.au/shop/shopdisplayproducts.asp?id=11&cat=SmartMedia+Memory+Cards) που χρησιμοποιούνται ευρέως σε μηχανήματα αναπαραγωγής MP3, ψηφιακές φωτογραφικές μηχανές, ηλεκτρονικά παιχνίδια και palmtops. Για την εγγραφή και χρήση χρησιμοποιούνται ειδικά Smart Media.

Readers/Writers μηχανήματα από την ίδια εταιρία
(http://www.flashmemory.com.au/shop/shopdisplayproducts.asp?id=12&cat=SmartMedia+Reader%2FWriters). Η εταιρία λοιπόν σε γενικές γραμμές αξιοποιεί έξυπνες κάρτες και σε άλλους τομείς πέρα απ τους καθιερωμένους που έχουμε συνηθίσει μέχρι τώρα, όπως στην αποθήκευση και μεταφορά δεδομένων.

Verisign (http://www.verisign.com) Φυσικά τίποτε δεν θα ήταν ολοκληρωμένο χωρίς να αναφερθούμε στην μεγαλύτερη εταιρία παγκοσμίως στην παραγωγή κρυπτογραφικών αλγορίθμων και προϊόντων, αλλά και τον μεγαλύτερο εκδότη ψηφιακών πιστοποιητικών. Η εταιρία αυτή βρίσκεται πραγματικά πίσω από όλα και το όνομά της αποτελεί πολύτιμη εγγύηση και σημαντικό ατού για τις εταιρίες που χρησιμοποιούν έξυπνες κάρτες. Δεν είναι τυχαίο που ακόμα και η αναγραφή του ονόματος της εταιρίας αποτελεί ουσιαστική, πλήρης και ικανοποιητικότατη εγγύηση για κάποιο προϊόν.

Υπάρχουν βέβαια πολλές ακόμα εταιρίες που δραστηριοποιούνται γύρω από τον χώρο των έξυπνων καρτών αλλά μπορούμε να πούμε με σιγουριά ότι η παραπάνω λίστα είναι σίγουρα και η πιο αντιπροσωπευτική. Η αναφορά στα παραπάνω παραδείγματα γίνεται μόνο και μόνο για τον ίδιο τον αναγνώστη να πάρει μια μικρή ιδέα της τεχνολογίας που εφαρμόζεται (είναι από τις λίγες εταιρίες στο διαδίκτυο που προσφέρουν μέσω των

ιστοσελίδων τους ακριβή τεχνολογικά χαρακτηριστικά και ολοκληρωμένες πληροφορίες πάνω στην κατασκευή και χρήση έξυπνων καρτών). Συνολικά, υπολογίζεται ότι υπάρχουν περίπου σαράντα ξεχωριστά είδη έξυπνων καρτών που όλες κάνουν την ίδια όμως δουλεία: την συναλλαγή!

5

Ευρετήριο Ορολογίας Έξυπνων Καρτών

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 «επισημιοποίηση» 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» (πβ. 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 βρίσκεται στις Βρυξέλλες. Αποτελείται από όλους τους (ευρωπαϊκούς) εθνικούς οργανισμούς προτύπων και είναι ο επίσημος οργανισμός της Ευρωπαϊκής Ένωσης για τα ευρωπαϊκά πρότυπα
Challenge-response	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)	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. Πβ. 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, 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 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. Πβ. 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	Πβ. 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

6 *Συμπέρασμα*

Συμπερασματικά, σε αυτή την πτυχιακή εργασία γνωρίσαμε τις έξυπνες κάρτες και πιο συγκεκριμένα τη χρήση και τη τεχνολογία τους. Οι έξυπνες κάρτες αποτελούν πλέον μέρος της καθημερινότητας μας, μπορούμε να τις χρησιμοποιούμε παντού και κάνουν τις καθημερινές μας δραστηριότητες πιο εύκολες. Βέβαια, ο κόσμος και ειδικότερα ο Έλληνας δεν είναι ενημερωμένος για το τι ακριβώς είναι έξυπνη κάρτα και πολλοί τη παρομοιάζουν με τη πιστωτική κάρτα. Όμως σίγουρα έχει δει μία από αυτές, όπως η τηλεκάρτα, και σύντομα αντί για το δίπλωμα αυτοκινήτου ή το διαβατήριό του θα κρατάει στα χέρια του μια έξυπνη κάρτα. Είδαμε τη διαφορά που έχουν οι έξυπνες κάρτες από της κάρτες μαγνητικής ταινίας. Αναλύσαμε το ότι χωρίζονται σε διάφορες κατηγορίες και κάθε μία από αυτές έχουν διαφορετική χρήση. Ενδιαφέρον αποτελούσε και η εφαρμογή αυτών στη κινητή τηλεφωνία, στη συνδρομητική τηλεόραση, στις συγκοινωνίες όπως επίσης και στους πανεπιστημια- κούς χώρους και σε πολλούς άλλους τομείς της καθημερινής μας ζωής.Η χρήση των έξυπνων καρτών έχει πολλά πλεονεκτήματα σε σχέση με τις μαγνητικές αλλά ένα απο τα πιο σημαντικά αντιμετωπίσημα μειονεκτήματα είναι η έλλειψη υποδομών για την υποστήριξή της. Η τεχνολογία τους, δίνει τη δυνατότητα να μιλάμε για ασφαλείς συναλλαγές ευαίσθητων προσωπικών δεδομένων μεταξύ των συναλλασόμενων. Είδαμε ότι η ασφάλειά τους στηρίζεται σε αλγόριθμους κρυπτογράφησης πράγμα το οποίο κάνει την έξυπνη κάρτα να μπορεί δύσκολα να χρησιμοποιηθεί από μη εξουσιοδοτημένο πρόσωπο.Άξιο ανάλυσης ήταν τα μέρη απο τα οποία αποτελείται μια έξυπνη κάρτα, πράγμα απαραίτητο για να κατανοήσουμε τα τεχνικά της χαρακτηριστικά. Στη συνέχεια είδαμε τους τύπους καρτών και τα πρότυπα συμφωνα με τα οποία πρέπει να λειτουργούν.Η έξυπνες κάρτες αποτελλούν έναν από τους πιο «έξυπνους» τρόπους για να συναλλάσεται κάποιος και λέμε έξυπνος γιατί μιλάμε για άνεση, ευκολία μεταφοράς, ευκολία στη χρήση, ασφάλεια στη συναλλαγή, ευκολία στη παραγωγή και άλλα πολλά πλεονεκτήματα που αναλύσαμε παραπάνω. Στην Ελλάδα οι έξυπνες κάρτες δέν έχουν φτάσει ακόμα στο ζενίθ των δυνατοτήτων τους και είναι πολλοί ακόμη οι τομείς οι οποίοι επρόκειτο να χρησιμοποιηθούν. Ο κύριος λόγος είναι η έλλειψη υποδομών αλλά ένας ακόμα σημαντικός λόγος είναι το ότι το Ελληνικό κοινό είναι δύσκολο στο να πιστεί για κάτι καινούριο και πόσο μάλιστα άμα αφορά τη τσέπη του.

7

Βιβλιογραφία

URLs:

1.

Smart card software development and consulting Services

Card Printers - Great for smart card personalization

2.

Πρόκειται για ένα site που δημιουργήθηκε ύστερα από τη συνεργασία και προσπάθεια μιας ομάδας εταιρειών που δρουν επιχειρηματικά στη βιομηχανία έξυπνων καρτών. Κίνητρο αποτέλεσε η πεποίθησή τους ότι ενημερωμένοι χρήστες κάνουν καλύτερες επιλογές. Όπως μπορεί κανείς να καταλάβει και από τον τίτλο του «Smart Card Basics» περιέχει πληροφοριακό υλικό σχετικά με τις έξυπνες κάρτες και στόχος του είναι να φέρει τους επισκέπτες πιο κοντά στην νέα αυτή τεχνολογία και τα πλεονεκτήματά της.

3.

4.

5.

Παγκόσμια εμπορική επιχείρηση Smart Card Industry Association.
Το συγκεκριμένο website παρέχει πληροφορίες σχετικά με την Τεχνολογία Έξυπνων Καρτών, Εφαρμογές της τεχνολογίας αυτής, Νέα από τη βιομηχανία Έξυπνων Καρτών, Συνδέσμους προς άλλα ενδιαφέροντα σχετικά sites και φυσικά ενημέρωση για τα μέλη, τα προϊόντα και γενικά τον οργανισμό της SCIA.

6.

Είναι το site της εταιρείας Gemplus, η οποία είναι μια εταιρεία, ίσως η μόνη, που ασχολείται αποκλειστικά με την τεχνολογία των έξυπνων καρτών. Λειτουργεί σε 37 χώρες, έχει τη μεγαλύτερη ικανότητα παραγωγής στον τομέα της.

7.

Έγγραφο με τίτλο «An Introduction to Smart Cards», Steve Petri.

8.

Datacard Group, "The Transition from Magnetic Stripe to EMV Chip (Smart) Cards", White
Paper, Version 1.0, November 2001.

9.

"Smart cards and the OpenCard Framework», Learn how to implement a card terminal and use a standard API for interfacing to smart cards from your browser, Rinaldo Di Giorgio.

10.

OpenCard Framework, General Information Web Document, Second Edition, October, 1998

11. [illegible]

Interoperability Specification for ICCs and Personal Computer Systems, Part 1. Introduction and Architecture Overview, Revision 1.0, December 1997.

12. *www.ePaynews.com*

13. *www.cardwerk.com*

14. *www.smartcardbasics.com*

15. *www.gemplus.com*

16. *www.weethet.nl*

17. *www.scan.co.id*

18. *www.smartcardgroup.com*

19. *www.smartcardalliance.org*

20. *www.estrategy.gov*

21. *www.smartcardclub.co.uk*

22. ***www.idpdigital.com***

23. ***www.whatis.techtarget.com***

24. ***www.paceintegration.com***

25. ***www.javaworld.com***

26. ***www.infosyssec.org***

27. ***www.citi.umich.edu***

28. ***www.cardshow.com***

BOOKS:

29.

[ACB+97] Allen, Catherine a., William J. Barr, Ron Schultz. *Smart Cards: seizing strategic business opportunities*, 1997

30.

[Eve02] Dr. David B Everett, *Smart Card Technology: Introduction To Smart Cards*, available at www.smartcardclub.co.uk, Smart Card News Ltd., 2002

[Fin03] Klaus Finkenzeller; translated by Rachel Waddington, *RFID handbook: Fundamentals and applications in contactless smart cards and identification*, 2nd edition, 2003

[Haw02] Peter Hawkes, *Opinion: "Why Is No One Trying to Sell Me An Electronic Wallet?"*, available at www.smartcardclub.co.uk, Smart Card News Ltd., 2002

[RE00] W. Rankl, W. Effing; translated by Kermeth Cox. *Smart Card Handbook*, 2nd edition, 2000

[ZM94] Jose Luis Zoreda, Jose Manuel Oton. *Smart Cards*, 1994