



Πανεπιστήμιο Μακεδονίας
ΠΜΣ Πληροφοριακά Συστήματα

Μάθημα: “Πληροφοριακά Συστήματα για Μάρκετινγκ και Δημοσκοπήσεις”

Καθηγητής: Αναστάσιος Οικονομίδης

Smart Cards

Καγκάνη Αικατερίνη
MIS-Μάιος 2002

ΠΕΡΙΛΗΨΗ

Στο πλαίσιο της εργασίας αυτής γίνεται αναφορά στην ιστορία των έξυπνων καρτών, περιγραφή των τύπων έξυπνων καρτών και των χαρακτηριστικών τους. Επίσης επιχειρείται μια σύντομη παρουσίαση των προτύπων που έχουν υιοθετηθεί μέχρι σήμερα, επισημαίνοντας τον τρόπο με τον οποίο αυτά επηρέασαν την ασφάλεια των υπολογιστικών συστημάτων.

Οι έξυπνες κάρτες είναι στην πραγματικότητα μικροί υπολογιστές. Το γεγονός αυτό σημαίνει ότι μπορούν να βρίσκουν εφαρμογή σε πάρα πολλούς τομείς δραστηριότητας και ότι είναι πολύ πιθανό να έχουν την ίδια ραγδαία ανάπτυξη που ακολούθησαν και οι υπολογιστές.

Διακρίνονται σε δυο γενικές κατηγορίες, τις κάρτες μνήμης και τις κάρτες με μικροεπεξεργαστή. Μπορούμε όμως να τις διακρίνουμε και σε contact και contactless, ανάλογα με τον τρόπο που επικοινωνούν με τον reader. Σε κάθε κάρτα εκτός από τα δεδομένα μιας ή περισσότερων εφαρμογών υπάρχει και το Λειτουργικό Σύστημα (COS), το οποίο παρέχει τη δυνατότητα εκτέλεσης βασικών λειτουργιών, όπως ασφαλή πρόσβαση και αποθήκευση δεδομένων στην κάρτα, πιστοποίηση ταυτότητας και κρυπτογράφηση κ.α. Όσον αφορά στην ασφάλεια των έξυπνων καρτών, οι πιο γνωστοί αλγόριθμοι κρυπτογράφησης που χρησιμοποιούν είναι DES και Triple-DES.

Οι έξυπνες κάρτες αποτελούν ένα μέσο συναλλαγής, εξασφάλισης εξουσιοδότησης και αναγνώρισης ενός χρήστη. Οι δυνατότητές τους αυξάνουν με πολύ γρήγορους ρυθμούς και προβλέπεται ότι σύντομα θα αντικαταστήσουν ό,τι υπάρχει στο πορτοφόλι μας, δηλαδή πιστωτικές κάρτες, μετρητά, άδειες, φωτογραφίες κ.α. Τέλος αξίζει να σημειωθεί και η είσοδος στην αγορά των καρτών πολλαπλών εφαρμογών, οι οποίες προσφέρουν ενοποιημένες υπηρεσίες στον κάτοχό της.

SUMMARY

In this paper we will describe the history of smartcards, the different types of smart cards, their low-level properties, the standards that affect their adoption in market, and how they relate to today's computer security systems.

Smart cards are actually small computers. This means that they can be used find application in many sectors and that it is very likely they have the same rapid growth as the computers.

They are distinguished in two general categories, the memory cards and the microprocessor cards. We can however distinguish them also in contact and contactless, depending on the way that they communicates with the reader. In each card exists, apart from data, the Functional System (COS), which provides the possibility of implementing the basic operations, in order to secure access and storage of data in the card, certification of identity and encryption. With regard to the safety, smartcards use the encryption algorithms DES and Triple-DES.

Smart cards constitute a means of transaction, guarantee of authorisation and recognition of user. Their functions fast and it is forecasted that shortly they will replace what exists in our wallet, that is to say credit cards, cash, authorisations, photographs.

ΠΕΡΙΛΗΨΗ.....	0
1 Η Τεχνολογία των Έξυπνων Καρτών.....	4
1.1 Τι είναι η έξυπνη κάρτα;	4
1.2 Βασικά Στοιχεία και Χαρακτηριστικά Έξυπνων Καρτών	4
1.3 Τύποι έξυπνων καρτών	5
1.3.1 Κάρτες Μνήμης (Memory) – Κάρτες Μικροεπεξεργαστή (Microprocessor).....	5
1.3.2 Κάρτες Επαφής (Contact) – Κάρτες χωρίς Επαφή (contactless).....	5
1.3.3 Κατηγορίες Έξυπνων Καρτών.....	5
1.3.4 Memory Cards – Κάρτες Μνήμης.....	6
1.3.5 Contactless Cards	7
1.3.6 Hybrid Cards	8
1.3.7 Combi Cards	8
1.4 Το Chip Contact Καρτών	8
1.4.1 Micromodule	8
1.4.2 Τμήματα του Micromodule	9
2 Πεδία Εφαρμογής των Έξυπνων Καρτών	9
2.1.1 Τεχνολογία Πληροφοριών - Information Technology	9
2.1.2 Κινητές Τηλεπικοινωνίες - Mobile Telecommunications	10
2.1.3 Εμπορικές εφαρμογές - Commercial Applications	10
2.1.4 Παραδείγματα Εφαρμογών.....	10
3 Πλεονεκτήματα & Αδύνατα Σημεία	11
3.1 Πλεονεκτήματα των Έξυπνων Καρτών.....	12
3.2 Εμπόδια κατά την αποδοχή των Έξυπνων Καρτών	12
4 Πρότυπα.....	13
4.1 Η ανάγκη για πρότυπα	13
4.2 Επίσημα Πρότυπα	13
4.2.1 Πρότυπο ISO- 7816.....	13
4.2.2 Draft ISO 14443	19
4.2.3 Draft ISO 15693	19
4.3 Βιομηχανικά Πρότυπα.....	19
4.3.1 Πρότυπο EMV	19
4.3.2 Open Card.....	20
4.3.3 PC/SC.....	21
5 Λειτουργικό Σύστημα Έξυπνων Καρτών (COS)	21
5.1 Τι ακριβώς είναι το COS;.....	22
5.2 Multi Application Card Operating Systems (MACOS).....	23
5.3 MULTOS.....	23
5.3.1 Overview	23
5.3.2 Secure Multi-Application Smart Card Operating System.....	23
5.3.3 Application Load & Unload	23
6 Έξυπνες Κάρτες & Ασφάλεια.....	24
6.1 Αλγόριθμοι Κρυπτογράφησης.....	24
6.2 Δυνατότητες Κρυπτογράφησης	25
6.3 Χρήση Έξυπνων Καρτών για την ασφάλεια των δεδομένων.....	26
6.3.1 Σύστημα με Host-Based ασφάλεια	26
6.3.2 Σύστημα με Card -Based ασφάλεια.....	26

7	Κριτήρια Επιλογής Κάρτας.....	26
8	Βιβλιογραφία	29

1 Η Τεχνολογία των Έξυπνων Καρτών

1.1 Τι είναι η έξυπνη κάρτα;

Η έξυπνη κάρτα είναι μια από τις τεχνολογίες που εμφανίστηκαν πρόσφατα στον κόσμο της Τεχνολογίας της Πληροφορίας. Μοιάζει πολύ σε μέγεθος με τις πλαστικές κάρτες που χρησιμοποιούνται για πληρωμές, με τη διαφορά ότι διαθέτει έναν μικροεπεξεργαστή ή ένα chip μνήμης. Σε συνδυασμό με έναν καρταναγνώστη (smart card reader) έχει τη δυνατότητα να εξυπηρετήσει πολλές διαφορετικές εφαρμογές με την υπολογιστική της δύναμη. Μπορεί να χρησιμοποιηθεί ως συσκευή ελέγχου πρόσβασης και να επιτρέψει την προσπέλαση δεδομένων μόνο στους κατάλληλους χρήστες. Μπορεί ακόμη να χρησιμοποιηθεί για την πραγματοποίηση αγορών. Γενικά μπορούμε να πούμε ότι η έξυπνη κάρτα προσφέρει δυνατότητες μεταφοράς δεδομένων, ασφάλεια και ευκολία. [4]

1.2 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, υπερϊώδη ακτίνα, την ακτίνα Χ, κάμψη, γδάρισμα.

- 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 αναπαράχθούν 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.

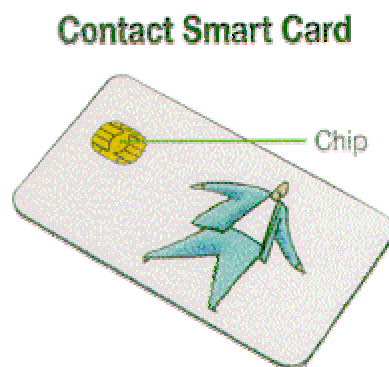
- Υπολογιστική ισχύς

Σήμερα χρησιμοποιούνται ελεγκτές σε συνδυασμό με έναν 32-μπιτο επεξεργαστή RISC που τρέχει στα 25-32 MHz. [1]

1.3 Τύποι έξυπνων καρτών

1.3.1 Κάρτες Μνήμης (Memory) – Κάρτες Μικροεπεξεργαστή (Microprocessor)

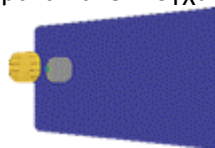
Υπάρχουν δύο είδη έξυπνων καρτών: κάρτες μνήμης και κάρτες με μικροεπεξεργαστή. Η κάρτα μνήμης απλά αποθηκεύει δεδομένα. Θα μπορούσε κανείς να τη θεωρήσει ως μικρή δισκέτα, με τη διαφορά όμως ότι προσφέρουν σημαντικά υψηλότερο επίπεδο ασφάλειας. Από την άλλη πλευρά σε μια κάρτα με μικροεπεξεργαστή υπάρχει η δυνατότητα να προσθέσουμε, να διαγράψουμε και να διαχειριστούμε τις πληροφορίες της. Θα μπορούσε κανείς να τις θεωρήσει ως έναν μικρό υπολογιστή. [4]



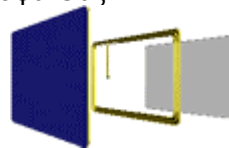
Εικόνα 1 [4]

1.3.2 Κάρτες Επαφής (Contact) – Κάρτες χωρίς Επαφή (contactless)

Οι έξυπνες κάρτες προσφέρουν δύο είδη διεπαφής χρήστη: με επαφή και χωρίς επαφή. Οι έξυπνες κάρτες επαφής (Contact smart cards) εισάγονται σε μια ειδική συσκευή που ονομάζεται καρταναγνώστης (smart card reader) και πραγματοποιείται φυσική σύνδεση μεταξύ κάρτας και συσκευής. Οι έξυπνες κάρτες χωρίς επαφή (Contactless smart cards) διαθέτουν ενσωματωμένη στο πλαστικό σώμα του μια κεραία που επιτρέπει την επικοινωνία με τον καρταναγνώστη χωρίς να πραγματοποιείται φυσική επαφή της κάρτας με τη συσκευή. Υπάρχουν βέβαια και κάρτες που συνδυάζουν τα δυο παραπάνω interfaces. Πρόκειται για τις combi κάρτες που πραγματοποιούν επικοινωνία με τη συσκευή με φυσική σύνδεση και με ραδιοκύματα και επιτυγχάνουν πολύ υψηλό επίπεδο ασφάλειας. [4]



Contact smart cards [4]



Contactless smart cards [4]

Εικόνα 2

1.3.3 Κατηγορίες Έξυπνων Καρτών

Οι έξυπνες κάρτες διακρίνονται σε κατηγορίες ανάλογα με τον τύπο του chip που βρίσκεται μέσα στην κάρτα και τις δυνατότητές του. Στο σχήμα 1 φαίνονται όλα τα είδη έξυπνων καρτών. [2]

1.3.4 Memory Cards – Κάρτες Μνήμης

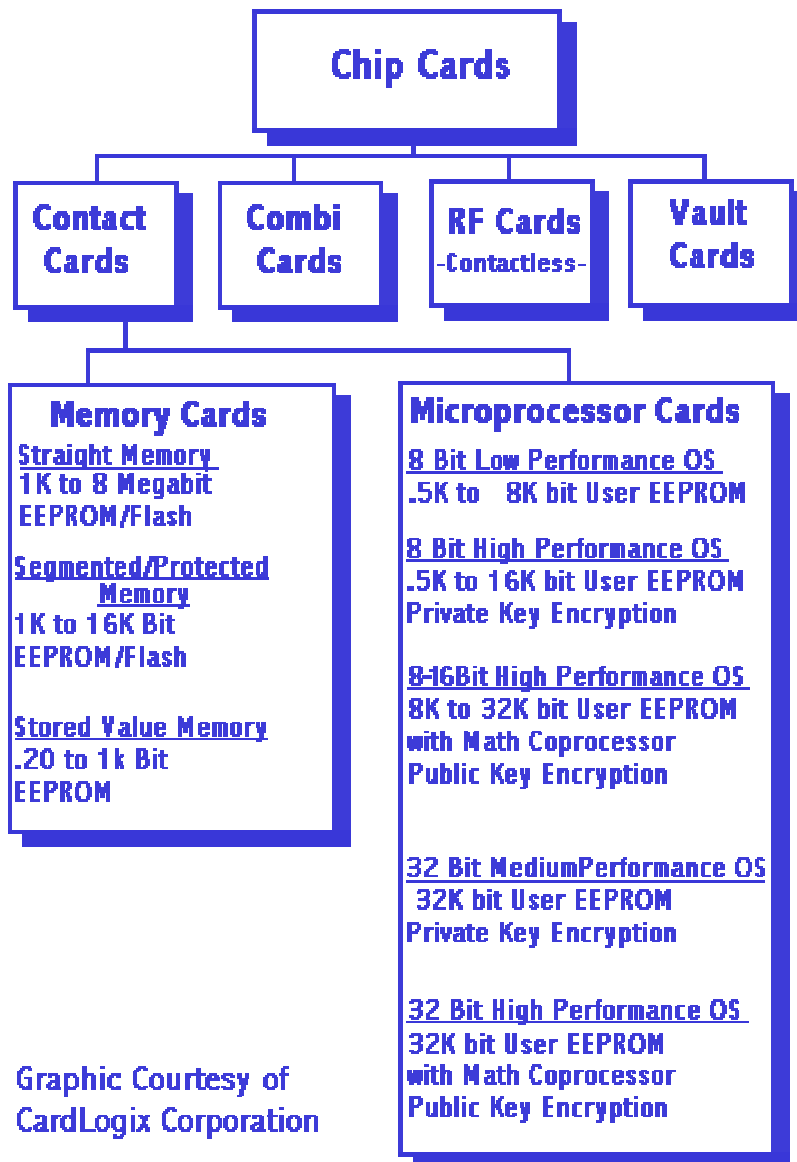
Κάρτες που διαθέτουν μνήμη, δεν έχουν ιδιαίτερη υπολογιστική ικανότητα και δε μπορούν να διαχειριστούν αρχεία δυναμικά. Η επικοινωνία με του αναγνώστες γίνεται με πρωτόκολλα σύγχρονης μετάδοσης. Διακρίνονται σε τρεις τύπους:

1.3.4.1 Straight Memory Cards

Στις κάρτες αυτές αποθηκεύονται απλώς δεδομένα, χωρίς να υπάρχει δυνατότητα επεξεργασίας. Έχουν το χαμηλότερο κόστος ανά bit μνήμης και μπορεί κανείς να πει ότι μοιάζουν με δισκέτες διαφόρων μεγεθών.

1.3.4.2 Protected / Segmented Memory Cards

Οι Protected κάρτες διαθέτουν κάποια λογική για να μπορέσουν να ελέγξουν την πρόσβαση στα περιεχόμενά τους. Μπορεί κανείς να ορίσει προστασία κατά την εγγραφή ή την ανάγνωση της κάρτας, ή ακόμη και στις δυο περιπτώσεις. Αυτό γίνεται με τη βοήθεια ενός κωδικού ή ενός κλειδιού συστήματος (system key). Στην περίπτωση που είναι Segmented τότε η μνήμη της κάρτας μπορεί να διαιρεθεί σε λογικά τμήματα, καθένα από τα οποία μπορεί να φιλοξενήσει τα περιεχόμενα διαφορετικών εφαρμογών (multi-functionality).



Σχήμα 1 [2]

1.3.4.3 Stored Value Memory Cards

Οι κάρτες αυτές σχεδιάστηκαν για να ικανοποιήσουν συγκεκριμένες ανάγκες αποθήκευσης τιμών (value) ή «κουπονιών» (tokens). Υπάρχει η δυνατότητα επαναφόρτωσης τιμής, μπορεί να είναι δηλαδή rechargeable. Στις περισσότερες από αυτές τις κάρτες ορίζονται τα μέτρα της ασφάλειάς τους από τον κατασκευαστή. Τα μέτρα αυτά περιλαμβάνουν κωδικούς (password keys) κάποιου είδους λογική στο chip. Τα περιεχόμενα της μνήμης τους είναι συνήθως ένας μετρητής και δεν υπάρχει ελεύθερος χώρος για καμία άλλη εφαρμογή. Στην περίπτωση μιας απλής εφαρμογής όπως μια τηλεκάρτα το chip μνήμης θα έχει π.χ. 100 κελιά, ένα για κάθε τηλεφωνική μονάδα. Κάθε κελί «καθαρίζεται» μόλις η τηλεφωνική μονάδα χρησιμοποιηθεί. Όταν όλες οι μονάδες χρησιμοποιηθούν η κάρτα είναι άχρηστη και δε μπορεί να χρησιμοποιηθεί. Στην περίπτωση όμως μιας rechargeable κάρτας, θα μπορούσε κανείς να την «ξαναγεμίσει» με μονάδες.

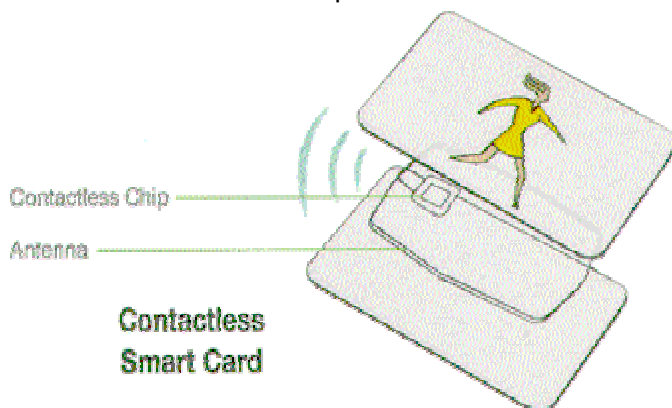
1.3.4.4 CPU/MPU Microprocessor Multifunction Cards

Οι κάρτες αυτές διαφέρουν από όλες τις υπόλοιπες, γιατί έχουν δυνατότητες επεξεργασίας στο εσωτερικό τους. Γίνεται κατανομή της μνήμης της κάρτας σε διάφορα ανεξάρτητα τμήματα, καθένα από τα οποία αφιερώνεται σε κάποια συγκεκριμένη εφαρμογή ή λειτουργία. Στο εσωτερικό της κάρτας υπάρχει ένα chip μικροεπεξεργαστή ή μικροελεγκτή που διαχειρίζεται την κατανομή της μνήμης και τη διαχείριση των αρχείων. Ο τύπος αυτό chip είναι παρόμοιος με αυτούς που συναντά κανείς σε έναν προσωπικό υπολογιστή. Όταν ενσωματώνεται σε μια έξυπνη κάρτα τότε οργανώνει και διαχειρίζεται τα δεδομένα σε δομές αρχείων υπό την καθοδήγηση του Λειτουργικού Συστήματος της κάρτας (Card Operating System - COS). Το λειτουργικό αυτό σύστημα ελέγχει την πρόσβαση στη μνήμη που υπάρχει στην κάρτα, με αποτέλεσμα να υπάρχει η δυνατότητα αποθήκευσης στην κάρτα πολλών διαφορετικών εφαρμογών, που ανήκουν σε διαφορετικές επιχειρήσεις. Τα χαρακτηριστικά λοιπόν της κάρτας αυτής ευνοούν την ανάπτυξη μιας κάρτας πολλαπλών εφαρμογών που παρέχει πρόσβαση σε πολλαπλές υπηρεσίες.

Θα μπορούσε κανείς να αναφέρει ως παράδειγμα μια πιστωτική κάρτα, η οποία εκτός από τη συνηθισμένη χρήση της, επιτρέπει στο κάτοχο - φοιτητή την είσοδό του στο χώρο του Πανεπιστημίου. Επίσης η τεχνολογία αυτή επιτρέπει την ενημέρωση και αντικατάσταση των περιεχομένων της κάρτας, γεγονός που μειώνει τα κόστη. Από την πλευρά του χρήστη, μια τέτοια κάρτα συνεπάγεται μεγαλύτερη ευκολία στη χρήση, μεγαλύτερη ασφάλεια.

1.3.5 Contactless Cards

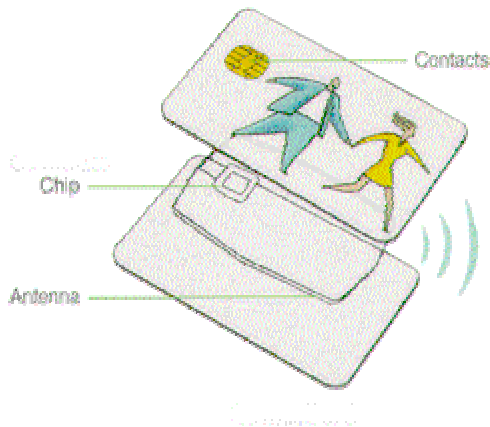
Για μια contactless κάρτα σημασία έχει να βρίσκεται σε κοντινή απόσταση από τον καρταναγνώστη. Τόσο η κάρτα όσο και ο καρταναγνώστης περιέχουν μια κεραία μέσω της οποίας πραγματοποιείται η επικοινωνία. Η κεραία είναι συνήθως ένα πολύ λεπτό καλώδιο που συνδέεται στο contactless chip. [3]



Εικόνα 3 [4]

1.3.6 Hybrid Cards

Μια υβριδική κάρτα διαθέτει 2 chips, καθένα από τα οποία διαθέτει contact και contactless interface. Τα κυκλώματα αυτά δεν συνδέονται, αλλά λειτουργεί ανεξάρτητα το contact από το contactless μέρος ικανοποιώντας τις ανάγκες διαφορετικών εφαρμογών. [3]



Εικόνα 4 [4]

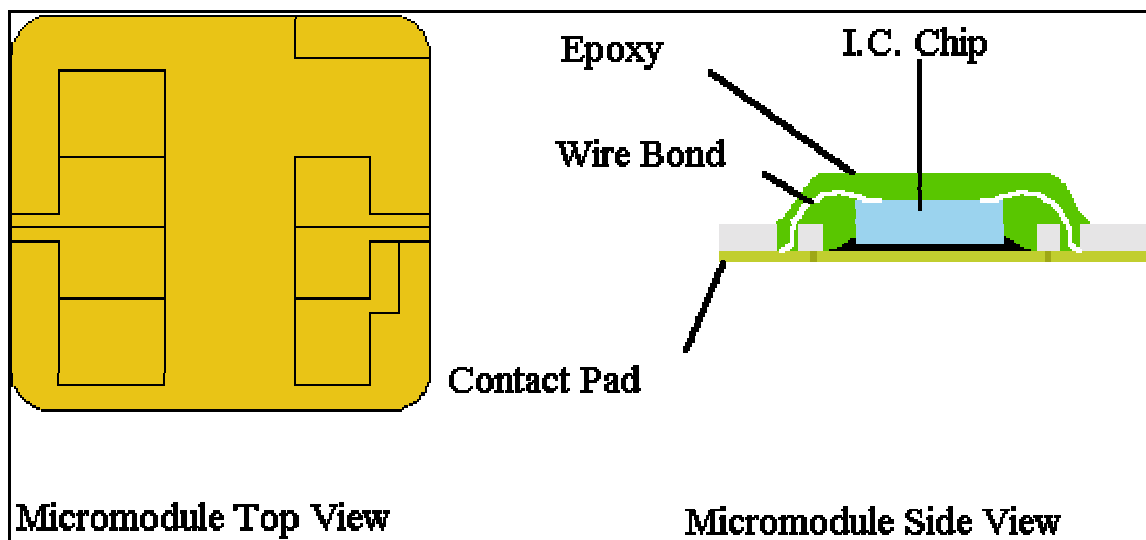
1.3.7 Combi Cards

Μια τέτοια κάρτα διαθέτει μόνο ένα chip το οποίο έχει και contact και contactless interface. Μπορεί δηλαδή κανείς να έχει πρόσβαση στο ίδιο chip είτε με contact είτε με contactless τρόπο και μάλιστα με πολύ υψηλό επίπεδο ασφάλειας. Αναμένεται να χρησιμοποιηθούν ιδιαίτερα από τους κλάδους των μεταφορών και των τραπεζών. [3]

1.4 To Chip Contact Καρτών

1.4.1 Micromodule

Οι έξυπνες κάρτες επαφής είναι φιαγμένες από εύκαμπτο πλαστικό υλικό (πολυβινυλικό χλωρίδιο ή PVC) και έχουν ενσωματωμένο ένα micromodule, το οποίο διαθέτει ένα ολοκληρωμένο κύκλωμα με μνήμη και μικροεπεξεργαστή. Το micromodule έχει οκτώ μεταλλικές επαφές στην επιφάνειά του, η λειτουργία των οποίων καθορίζεται από συγκεκριμένα διεθνή πρότυπα (βλ. Ενότητα 5).



Σχήμα 2 [3]

Όταν μια έξυπνη κάρτα εισάγεται σε μια συσκευή υποδοχής καρτών (reader), οι μεταλλικές επαφές έρχονται σε επαφή με τα αντίστοιχα μεταλλικά σημεία της συσκευής, με αποτέλεσμα να μπορεί να επιτευχθεί επικοινωνία μεταξύ κάρτας και συσκευής. Οι έξυπνες κάρτες πρέπει πάντα να επαναρυθμίζονται όταν εισάγονται σε ένα reader. Αυτή η ενέργεια αναγκάζει την έξυπνη κάρτα να ανταποκριθεί με την αποστολή ενός μηνύματος " Answer-to-Reset " (ATR), που ενημερώνει τη συσκευή σχετικά με τους κανόνες, που καθορίζουν την επικοινωνία με την κάρτα και την επεξεργασία της συναλλαγής. [1]

1.4.2 Τμήματα του Micromodule

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

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

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

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

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

Μνήμη Εφαρμογής (Application Memory): σχεδόν πάντα είναι μια διπλή EPROM (Electrically Erasable Programmable Read-Only Memory), της οποίας τα περιεχόμενα μπορούν να διαγραφούν/γραφτούν/ενημερωθούν μόνο ηλεκτρονικά. Σύμφωνα με τα διεθνή πρότυπα, αυτή η μνήμη πρέπει να διατηρήσει τα στοιχεία της μέχρι και 10 έτη και να υποστηρίξει τουλάχιστον 10.000 ενέργειες ανάγνωσης-γραφής κατά τη διάρκεια της ζωής της κάρτας. Για κάθε εφαρμογή που φιλοξενείται στην κάρτα χρησιμοποιείται μέρος της μνήμης εφαρμογής για να καταχωρηθούν οι πληροφορίες που την αφορούν. [1]

2 Πεδία Εφαρμογής των Έξυπνων Καρτών

Οι πρώτες τσιπ κάρτες ήταν απλές προπληρωμένες τηλεφωνικές κάρτες που εφαρμόστηκαν στην Ευρώπη στα μέσα της δεκαετίας του '80 (κάρτες μνήμης). Σήμερα, οι σημαντικότεροι τομείς εφαρμογής για τις βασισμένες σε μικροεπεξεργαστή έξυπνες κάρτες είναι: οικονομικός, επικοινωνίες, κυβερνητικά προγράμματα, ασφάλεια πληροφοριών, φυσική ασφάλεια πρόσβασης, μεταφορά, λιανική πώληση και πίστη (loyalty), υγειονομική περίθαλψη, και university identification. Πρόκειται για τομείς που επικαλύπτονται, αφού μια έξυπνη κάρτα μπορεί να «φιλοξενεί» εφαρμογές που ανήκουν σε διάφορους τομείς. [1]

2.1.1 Τεχνολογία Πληροφοριών - Information Technology

Στις μέρες μας ολοένα και περισσότερες επιχειρήσεις και οργανισμοί, όπως η κυβέρνηση, οι οργανισμοί υγειονομικής περίθαλψης, καταχωρούν και δημοσιεύουν πληροφορίες μέσω δικτύων, Intranets, extranets και του Διαδικτύου. Με σκοπό να καταστήσουν διαθέσιμες τις πληροφορίες αυτές, δηλαδή εύκολα προσπελάσιμες από αυτούς που τις χρειάζονται, αλλά και να τις προστατεύσουν από ανεπιθύμητες παρεισφρήσεις, οι οργανισμοί αυτοί στρέφονται προς τις έξυπνες κάρτες. Στο επίπεδο αυτό οι έξυπνες κάρτες επιτρέπουν:

- Ασφαλής σύνδεση και πιστοποίηση ταυτότητας χρήστη σε PCs και δίκτυα

- Ασφαλές B2B και B2C ηλεκτρονικό εμπόριο
- Αποθήκευση ψηφιακών υπογραφών, ψηφιακών πιστοποιητικών και κωδικών πρόσβασης
- Κρυπτογράφηση ευαίσθητων δεδομένων [4]

2.1.2 Κινητές Τηλεπικοινωνίες - Mobile Telecommunications

Οι άνθρωποι που χρησιμοποιούν το πρότυπο Global System for Mobile communications (GSM) για τα κινητά τηλέφωνα στην πραγματικότητα χρησιμοποιούν την τεχνολογία έξυπνων καρτών. Η έξυπνη κάρτα εισάγεται ή ενσωματώνεται στη συσκευή του κινητού μικροτηλεφώνου. Στην κάρτα βρίσκονται αποθηκευμένες διάφορες προσωπικές πληροφορίες και προτιμήσεις συνδρομητών που μπορεί να προστατεύονται από έναν κωδικό PIN και μπορούν να μεταφέρονται από τηλέφωνο σε τηλέφωνο. Οι έξυπνες κάρτες επιτρέπουν:

- Ασφαλή πιστοποίηση του συνδρομητή
- Χρήση πολλών δικτύων (Roaming)
- Ασφαλείς υπηρεσίες προστιθέμενης αξίας [4]

2.1.3 Εμπορικές εφαρμογές - Commercial Applications

Η μεταφερσιμότητα και η δυνατότητα ενημέρωσης των περιεχομένων μιας έξυπνης κάρτας την καθιστούν κατάλληλη για την υλοποίηση διαφόρων εφαρμογών. Σε αυτές καταχωρούνται πληροφορίες, χρήματα, ή/και εφαρμογές που μπορούν να χρησιμοποιηθούν για:

- Τραπεζικές συναλλαγές (Banking) / πληρωμές (Payment)
- Loyalty και προώθηση
- Έλεγχο πρόσβασης (Access control)
- Αποθήκευση αξίας (Stored value)
- Αναγνώριση χρήστη (Identification)
- Ticketing
- Πληρωμή πάρκινγκ και διοδίων (Parking - toll collection) [4]

2.1.4 Παραδείγματα Εφαρμογών

Στη συνέχεια παρουσιάζονται κάποια παραδείγματα εφαρμογών έξυπνων καρτών. [1]

Οικονομικές Εφαρμογές (Financial Applications)

- Ηλεκτρονικό Πορτοφόλι (Electronic Purse), για να αντικαταστήσει τα νομίσματα για τις μικρές αγορές.
- Λογαριασμοί Πίστωσης ή/και Χρέωσης (Credit and/or Debit Accounts), με υψηλότερο επίπεδο ασφάλειας.
- Ασφάλεια πληρωμής στο Διαδίκτυο (ως τμήμα του ηλεκτρονικού εμπορίου).

Εφαρμογές επικοινωνιών (Communications Applications)

- Η ασφαλής πραγματοποίηση κλήσεων και ο προσδιορισμός αυτού που καλεί (για λόγους τιμολόγησης) σε οποιοδήποτε τηλέφωνο GSM (Global System for Mobile Communications).
- Ενεργοποίηση συνδρομητών στην καλωδιακή τηλεόραση.
- Τηλεκάρτες
- SIM κάρτες (chip κάρτες που χρησιμοποιούνται στην κινητή τηλεφωνία)
- Σύνδεση και Πρόσβαση μέσα σε δίκτυο
- Κάρτα πρόσβασης σε ψηφιακή τηλεόραση

Κυβερνητικά προγράμματα (Government Programs)

Ασφάλεια πληροφοριών (Information Security)

- Κάρτα πρόσβασης υπαλλήλων με κωδικούς και δυνατότητα να υιοθετηθεί η βιομετρική για να προστατευθεί την πρόσβαση στα συγκροτήματα ηλεκτρονικών υπολογιστών.

Φυσική πρόσβαση (Physical Access)

- Κάρτα πρόσβασης υπαλλήλων με ID και δυνατότητα να υιοθετηθεί η βιομετρική για να προστατευθεί η φυσική πρόσβαση σε εγκαταστάσεις.

Μεταφορές (Transportation)

- Άδειες οδήγησης
- Ηλεκτρονικά συστήματα πληρωμής διοδίων (Electronic Toll Collection Systems)
- Πληρωμή εισιτηρίου στις Δημόσιες Συγκοινωνίες
- Πληρωμή διοδίων
- Δικαιώματα parking
- Κρατήσεις αεροπορικών εισιτηρίων
- Τεκμηρίωση κατόχου, ηλεκτρονικό διαβατήριο.

Λιανική Πώληση και Loyalty (Retail and Loyalty)

- Ανταμοιβή Χρήσης

Κάρτα Υγείας (Health Card)

- Κάρτα υγείας που περιέχει πληροφορίες για την ασφάλεια που έχει επιλέξει ο ασθενής και διάφορα ιατρικά στοιχεία έκτακτης ανάγκης.

Αναγνώριση Φοιτητή σε Πανεπιστήμια (University Identification)

- Κάρτα ID σπουδαστών που περιέχει ποικίλες εφαρμογές όπως ηλεκτρονικό πορτοφόλι (για τις μηχανές πώλησης και πλυντηρίων μέσα στο campus του πανεπιστημίου), κάρτα βιβλιοθηκών και κάρτα γεύματος.

3 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. [1]

3.1 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. [1]

Ειδικότερα, όσον αφορά στη

Λειτουργικότητα:

- ικανότητα επεξεργασίας, όχι μόνο αποθήκευσης πληροφορίας.
- δυνατότητα επικοινωνίας με άλλα υπολογιστικά συστήματα μέσω ενός smart card reader.
- δυνατότητα ενημέρωσης- ανανέωσης των πληροφοριών και εφαρμογών που βρίσκονται αποθηκευμένες στην κάρτα, χωρίς να είναι απαραίτητη η έκδοση νέας κάρτας. [4]

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 [4]

3.2 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 πιο κατάλληλη κάρτα για την εφαρμογή στόχων.
- Έλλειψη προτύπων για την εξασφάλιση διαλειτουργικότητας των προγραμμάτων μεταξύ των ποικίλων έξυπνων καρτών.
- Εκκρεμή νομικά και ζητήματα πολιτικής, όπως νόμοι προστασίας καταναλωτών ή προστασίας των ιδιωτικών δεδομένων. [1]

4 Πρότυπα

4.1 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 αναγνώστών.

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

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

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

4.2 Επίσημα Πρότυπα

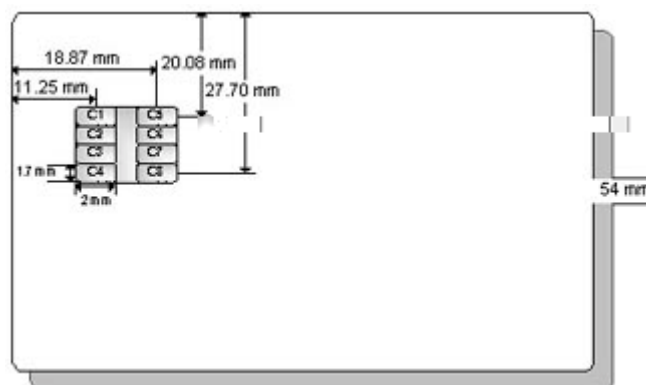
4.2.1 Πρότυπο ISO- 7816

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
<u>ISO 7816-1</u>	Φυσικά χαρακτηριστικά
<u>ISO 7816-2</u>	Διαστάσεις και θέση των επαφών
<u>ISO 7816-3</u>	Ηλεκτρονικά σήματα και πρωτόκολλα μετάδοσης
<u>ISO 7816-4</u>	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

4.2.1.1 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]

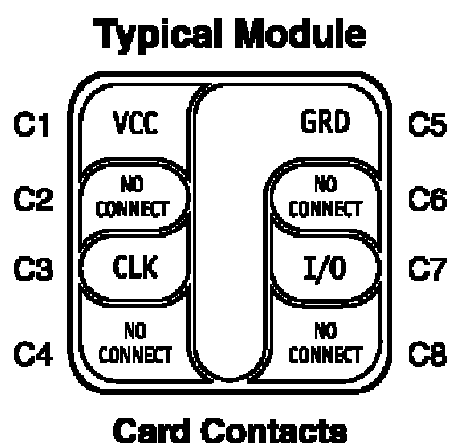
Επιπλέον το ISO7816-1 καθορίζει τα χαρακτηριστικά μιας κάρτας όταν αυτή κάμπτεται. Με τον τρόπο αυτό εξασφαλίζεται ότι οι πλαστικές κάρτες με τα ενσωματωμένα τσιπ κατασκευάζονται με τέτοιο τρόπο που εγγυάται την άψογη λειτουργία κατά τη διάρκεια του αναμενόμενου χρόνου ζωής μιας κάρτας.

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.

4.2.1.2 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 Επίσης 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.

4.2.1.3 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

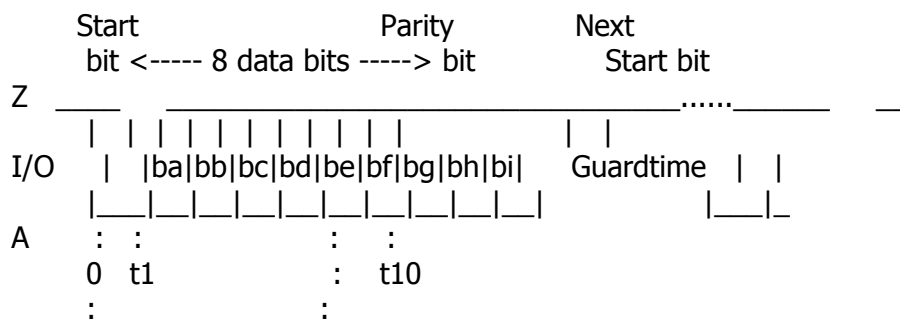
- 1 – Θεωρείται ότι η εσωτερική κατάσταση της κάρτας δεν είναι γνωστή πριν από το reset.
- 2 – Για να είναι εφικτή οποιαδήποτε επικοινωνία της συσκευής με την κάρτα θα πρέπει να οριστεί το RST σε μια κατάσταση που να δηλώνει ότι υπάρχει απάντηση στη γραμμή I/O.
- 3 - Το RESET αρχίζει από τη συσκευή. 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

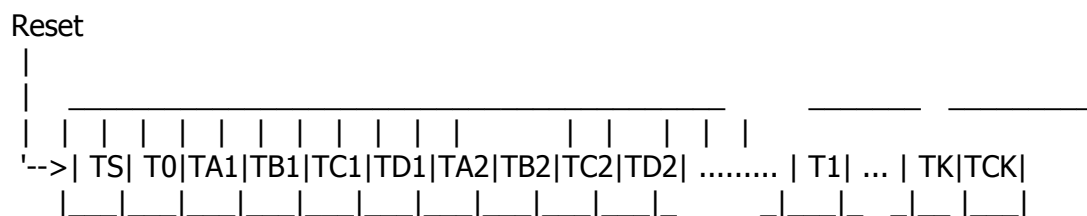
Αν το I/O είναι σε κατάσταση Z, τότε η μετάδοση έγινε σωστά

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

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)
- T_{Ai}, T_{Bi}, T_{CI}, T_{Di} ... Interface characters (Optional)
- T1, T2, ... ,TK Historical characters (Optional)
- TCK Check character (Conditional)

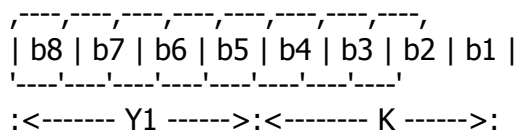


TS : Initial character
 T0 : Format character
 T_{Ai} : Interface character [codes FI,DI]
 T_{Bi} : Interface character [codes II,PI1]
 T_{CI} : Interface character [codes N]
 T_{Di} : Interface character [codes Y_{i+1}, T]
 T1, ... , TK : Historical characters (max,15)
 TCK : Check character

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 historical 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.

4.2.1.4 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: [5]

- Επιλογή Αρχείου
- Ανάγνωση / εγγραφή αρχείου
- Αναζήτηση αρχείου
- Διαχείριση Αρχείων
- Identification
- Authentication
- Εντολές Κρυπτογράφησης
- Εντολές για ηλεκτρονικά πορτοφόλια
- Εντολές ειδικές για κάθε εφαρμογή

4.2.2 Draft ISO 14443

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

Αποτελείται από 4 μέρη ως εξής:

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

4.2.3 Draft ISO 15693

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

Αποτελείται από 4 μέρη ως εξής:

- Φυσικά χαρακτηριστικά
- Ισχύς ραδιο-συχνότητας και αλληλεπίδραση σημάτων
- Αλγόριθμος anti – collision και πρωτόκολλα επικοινωνίας
- Εκτεταμένη σειρά εντολών και χαρακτηριστικά ασφαλείας

4.3 Βιομηχανικά Πρότυπα

4.3.1 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.

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.



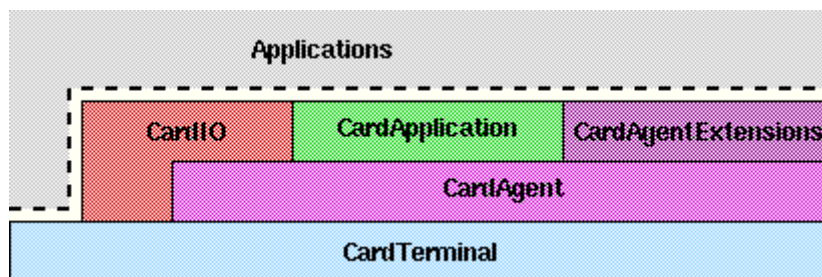
Στο χαμηλότερο επίπεδο βρίσκεται ο μικροεπεξεργαστής, για τον οποίο υπάρχουν τουλάχιστον τέσσερις διαφορετικοί κατασκευαστές. [6]

4.3.2 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:

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

Επιπλέον είναι εύκολο στη χρήση και έχει αρκετές δυνατότητες επέκτασης. [7]

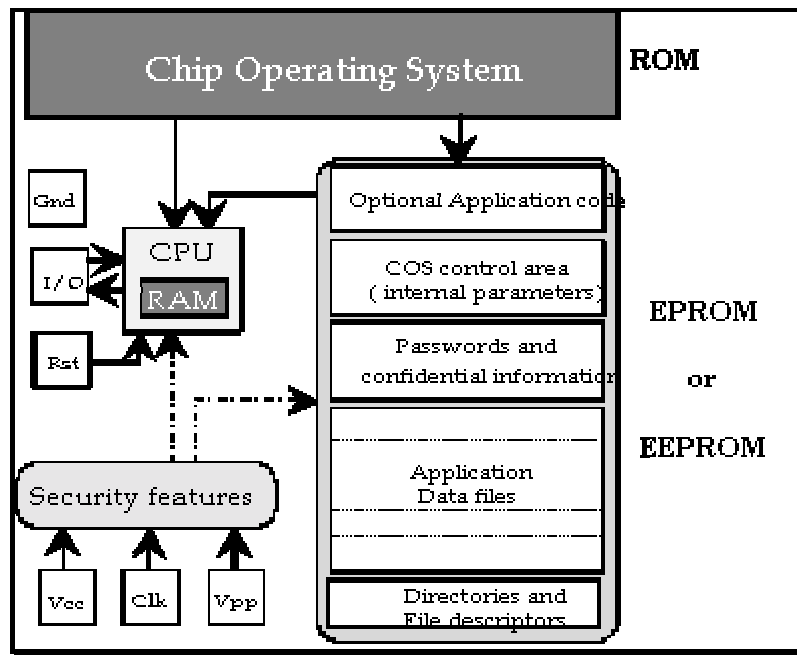
4.3.3 PC/SC

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 αποδευστεί ο χρήστης από επιλογή συγκεκριμένων μηχανημάτων, κυρίως αναγνώστων. [9]

5 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 ασφαλής πρόσβαση και αποθήκευση δεδομένων στην κάρτα, πιστοποίηση ταυτότητας και κρυπτογράφηση.

[1]



Σχήμα 7 [3]

5.1 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. [2]
- 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. [2]

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

- Διαχείριση της ανταλλαγής δεδομένων μεταξύ της κάρτας και του εξωτερικού κόσμου, κυρίως από την άποψη του χρησιμοποιούμενου πρωτοκόλλου.
- Διαχείριση των αρχείων και των δεδομένων που φυλάσσονται στη μνήμη

- Έλεγχος πρόσβασης σε πληροφορίες και λειτουργίες (παραδείγματος χάριν select file, read, write, update data).
- Διαχείριση της ασφάλειας καρτών και των κρυπτογραφικών αλγορίθμων.
- Διατήρηση της αξιοπιστίας, ιδιαίτερα από την άποψη της συνέπειας στοιχείων, της διαχείρισης των interrupts και την επαναφορά από ένα σφάλμα.
- Διαχείριση των διάφορων φάσεων του κύκλου ζωής της κάρτας (δηλαδή επεξεργασία, εξατομίκευση, ενεργός ζωή και τέλος της ζωής).

Για την ανάπτυξη των προγραμμάτων που τρέχουν μέσα στο ασφαλές περιβάλλον των έξυπνων καρτών, προτείνονται λειτουργικά συστήματα που έχουν τη μεγαλύτερη απήχηση στην αγορά όπως JavaCard OS, MultOS και πρόσφατα Windows for smart cards. [1]

5.2 Multi Application Card Operating Systems (MACOS)

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

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

- Java Card για όσους θέλουν να προγραμματίσουν σε Java.
- MultOS είναι το πρώτο λειτουργικό σύστημα πολλαπλών εφαρμογών (multi-application) 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.
- Windows for Smart Cards Microsoft licenses Windows® for Smart Cards Toolkit [1]

5.3 MULTOS

5.3.1 Overview

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

Η ανοικτή φύση της πλατφόρμας MULTOS επιτρέπει στον καθένα να εκδώσει κάρτες, να γράψει εφαρμογές, να εφαρμόσει το λειτουργικό σύστημα σε ένα συγκεκριμένο τσιπ ή να κατασκευάσει έξυπνες κάρτες. [1]

5.3.2 Secure Multi-Application Smart Card Operating System

Οι εφαρμογές είναι απομονωμένες η μια από την άλλη. Ένα σύστημα από firewalls εξασφαλίζει ότι τα στοιχεία δεν μπορούν να προσπελασθούν χωρίς κατάλληλη έγκριση. Αυτό έχει ως αποτέλεσμα, να μην είναι απαραίτητο οι προμηθευτές των εφαρμογών να εμπιστεύονται ο ένας τον άλλον, ούτε καν να έχουν οποιαδήποτε σχέση. [1]

5.3.3 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 γνώρισμα 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 μετρώ, 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. [1]

6 Έξυπνες Κάρτες & Ασφάλεια

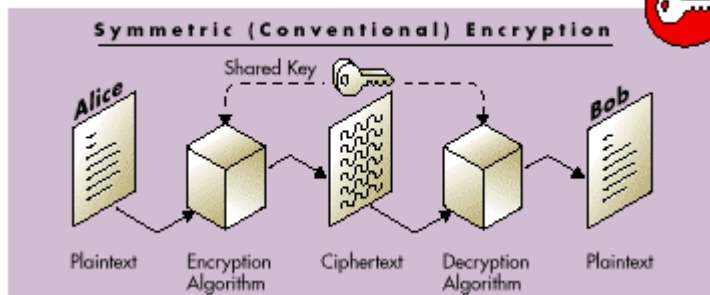
6.1 Αλγόριθμοι Κρυπτογράφησης

Υπάρχουν δυο είδη αλγορίθμων κρυπτογράφησης:

[5]

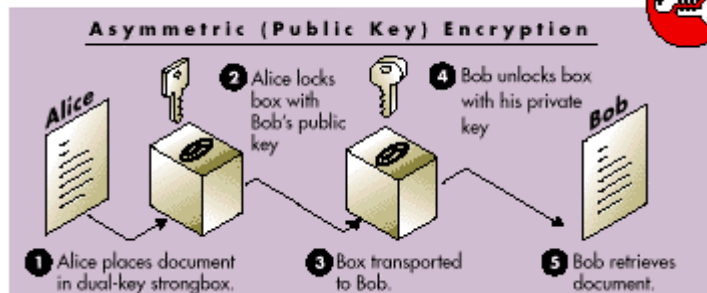
- οι συμμετρικοί, όπου το ίδιο κλειδί (**secret key**) χρησιμοποιείται για την κρυπτογράφηση και την αποκρυπτογράφηση. Ο πιο γνωστός συμμετρικός αλγόριθμος είναι ο DES (Data Encryption Standard).

Graphic courtesy of Charles Breed



- 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**.

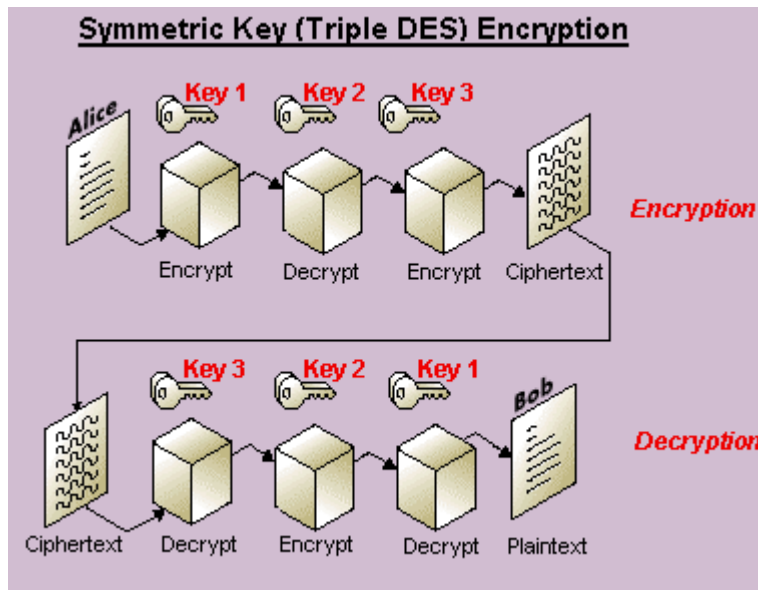
Graphic courtesy of Charles Breed



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 2^{56} 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.



6.2 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 μόλις 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. [5]

6.3 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]

6.3.1 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.

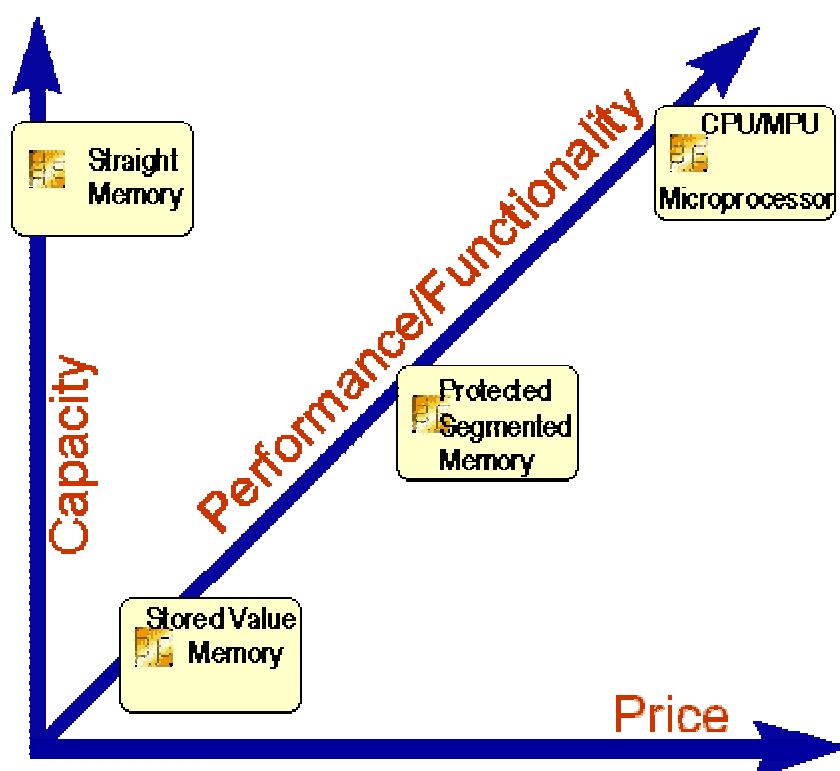
6.3.2 Σύστημα με Card -Based ασφάλεια

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.

7 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. [2]

Card Function Trade-Offs



Graphic Courtesy of CardLogix Corporation

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: [2]

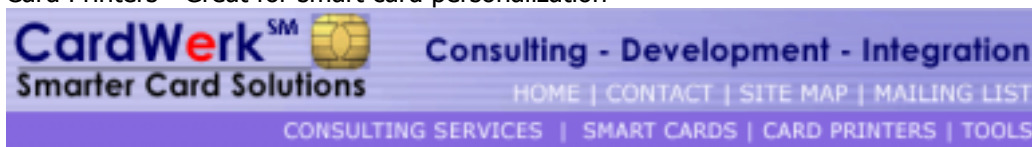
- Πόσες εφαρμογές θέλουμε να αποθηκεύσουμε στην κάρτα;
- Τι είδους πληροφορία θα αποθηκεύσω στις κάρτες;
- Πόση μνήμη είναι απαραίτητη για κάθε εφαρμογή;
- Πόσες κάρτες θα αγορασθούν;
- Μας ενδιαφέρει η ταχύτητα της συναλλαγής;
- Το ποσό της κάρτας θα μπορεί να ανανεώνεται; Πρόκειται δηλαδή για reloadable 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)

8 Βιβλιογραφία

1. http://www.cardwerk.com/smartcards/smartcard_overview.aspx
Smart card software development and consulting Services
Card Printers - Great for smart card personalization



2. <http://www.smartcardbasics.com/>
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. <http://www.scia.org/knowledgebase/aboutSmartCards/primer.htm>
<http://www.scia.org/knowledgebase/aboutSmartCards/stand.html>
<http://www.scia.org/knowledgebase/aboutSmartCards/scapps.html>
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.
4. <http://www.gemplus.com/basics/index.html>
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.
5. http://www.sspsolutions.com/solutions/whitepapers/introduction_to_smartcards/ Έγγραφο με τίτλο «An Introduction to Smart Cards», Steve Petri.
6. www.datacard.com
Datacard Group, "The Transition from Magnetic Stripe to EMV Chip (Smart) Cards", White Paper, Version 1.0, November 2001.
7. www.opencard.org
"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.
<http://www.opencard.org/docs/gim/ocfgim.html#HDRINTRODUCTION>
OpenCard Framework, General Information Web Document, Second Edition, October, 1998



8. <http://www.pcscworkgroup.com/>
Interoperability Specification for ICCs and Personal Computer Systems, Part 1.
Introduction and Architecture Overview, Revision 1.0, December 1997.