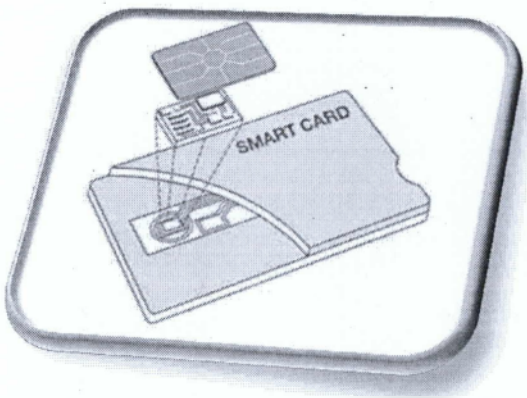
Τ.Ε.Ι ΠΕΛΟΠΟΝΗΣΣΟΥ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ (ΕΔΡΑ: ΣΠΑΡΤΗ)

Έξυπνες Κάρτες & Η Ασφάλεια Τους



ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

της

ΜΑΡΙΑΣ ΠΑΥΛΑΚΟΥ

Επιβλέπων Καθηγητής: Κουτσούκου Ελένη

Σπάρτη, Μάρτιος 15

Τ.Ε.Ι ΠΕΛΟΠΟΝΗΣΣΟΥ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ (ΕΔΡΑ: ΣΠΑΡΤΗ)

Έξυπνες Κάρτες & Η Ασφάλεια Τους

Επιβλέπων Καθηγητής: Κουτσούκου Ελένη

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την Κυριακή, 22 Μαρτίου 2015

....

Σπάρτη, Μάρτιος 15

Ευχαριστίες

Θέλω να ευχαριστήσω θερμά την καθηγήτρια μου και επιβλέποντα της πτυχιακής μου κ. Ελένη Κουτσούκου για τη διαρκή καθοδήγηση μου και την πολύτιμη βοήθειά της.

Θέλω να ευχαριστήσω θερμά την μητέρα μου την Κυριακή για την οικονομική και ηθική υποστήριξη όλα αυτά τα χρόνια. Επίσης θέλω να ευχαριστήσω τους στενούς μου φίλους, την Εύα, την Αρχοντούλα, την Παρασκευή, και τον Αντρέα που με στήριξαν και ηθικά αλλά και πνευματικά όλα αυτά τα χρόνια.

Μαρία Παυλάκου,

Μάρτιος 15

Περίληψη

Σκοπός της παρούσας πτυχιακής μου εργασίας είναι η παρουσία των έξυπνων καρτών. Στην πτυχιακή περιλαμβάνονται έξι κεφάλαια. Στο πρώτο κεφάλαιο γίνεται μια αναφορά στις έξυπνες κάρτες, στον ιστορικό και στις κάρτες μαγνητικής ταινίας. Στο δεύτερο κεφαλαίο, περιγράφεται η αρχιτεκτονική και το υλικό των έξυπνων καρτών. Επίσης, στο τρίτο κεφάλαιο αναφέρεται στην καθημερινή χρήση εφαρμογών με έξυπνες κάρτες αλλά και ποια είναι τα πλεονεκτήματα. Ενώ, στο κεφάλαιο 4 και 5 εξετάζονται η τεχνολογία Java Card και το λογισμικό των έξυπνων καρτών. Τέλος , στο κεφάλαιο 6 γίνεται αναφορά στην ασφάλεια των έξυπνων καρτών.

Λέξεις κλειδιά: Έξυπνες κάρτες, Java Card, E-wallet, GSM, JCRE, JCAPI, APDU, COS, ISO

Abstract

My purpose this thesis is the presence of smart cards. In the thesis includes six chapters. The first chapter is a reference to smart cards, in the historical and magnetic stripe cards. The second chapter describes the architecture and hardware of smart cards. Also, in the third chapter refers to the everyday use applications with smart cards and what are the advantages. While, in Chapter 4 and 5 examined the Java Card technology and software of smart cards. Finally, Chapter 6 refers to the security of smarts cards.

Key Words: Smart Cards, Java Card, E-wallet, GSM, JCRE, JCAPI, APDU, COS, ISO

Περιεχόμενα

Περιεχόμενα: Εικόνες

Περιεχόμενα: Πίνακες

Περιεχόμενα: Διαγράμματα

ΚΕΦΑΛΑΙΟ 1 ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ (SMART CARDS)

1.1 Εισαγωγή έξυπνης κάρτας

Η έξυπνη κάρτα (smart card) προσδιορίζεται από μία πλαστική κάρτα η οποία έχει την μορφή μιας πιστωτικής κάρτας. Αυτή περιλαμβάνει μια μνήμη και ένα μικροεπεξεργαστή όπου προσφέρουν τη δυνατότητα αποθήκευσης και επεξεργασίας ενός τεράστιου όγκου δεδομένων και αρχείων . Η καθορισμένη δυνατότητα συνδυάζεται με τον προσδιορισμό των παγκόσμιων προτύπων.

Η smart card είναι , στην ουσία, ένας μικροσκοπικός υπολογιστής όπου εμπεριέχεις πολύ σημαντικές και βασικές λειτουργίες. Αποτελεί την πιο πρόσφατη εξέλιξη στο χώρο των πλαστικών καρτών. Ο μικροσκοπικός υπολογιστής λέγεται διαφορετικά και ως μικροτσίπ (μικροεπεξεργαστή). Το μικροτσίπ αποτελείται από ένα ολοκληρωμένο κύκλωμα με ηλεκτρικές επαφές και μπορεί να περιλαμβάνει και μια λειτουργία ασύρματης επικοινωνίας με συνδυασμό με μία συσκευή αποδοχής καρτών όπου μέσα σ' αυτήν θα αποθηκεύονται και θα μεταφέρονται χιλιάδες bit δεδομένων αλλά παράλληλα, θα επεξεργάζεται ένα τεράστιο όγκο πληροφοριών για να μπορεί να πραγματοποιείται εξυπηρέτηση διάφορων εφαρμογών. Κύρια γνωρίσματα μιας έξυπνης κάρτας είναι η ασφάλεια δεδομένων και συμβιβασμοί , η ταχύτητα και η ευχέρεια χρήσης και ανθεκτικότητα στην εξάντληση και στην κακή διαχείριση. Το κόστος της είναι μικρό και εξαρτάται από το μέγεθος της μνήμης και το λογισμικό. Το λογισμικό λειτουργεί στην κάρτα (on board software) και ανάλογα με το τύπο της κάρτας μπορεί ένα λειτουργικό σύστημα να φτάσει έως σε ένα περίπλοκο περιβάλλον το οποίο να περιβάλλεται από ένα υψηλό επίπεδο γλωσσών ώστε να μπορεί να εφαρμοστεί η προσθήκη νέων εφαρμογών. Επιπροσθέτως, η Κεντρική μονάδα επεξεργασίας της (ΚΜΕ) αποτελείται από ένα 8-bit μικροεπεξεργαστή αλλά τελευταία γίνεται χρήση και ενός 32-bit μικροεπεξεργαστή

Η μια διαφορά που έχουν οι έξυπνες κάρτες με τις μαγνητικές (ταινίες) κάρτες είναι ότι οι πρώτες έχουν τις απαραίτητες διεργασίες και πληροφορίες αποθηκευμένες στο σώμα τους λαμβάνοντας περισσότερη ασφάλεια και μεταφορά των απαραίτητων δεδομένων χωρίς να χρειάζεται να υπάρχει σύνδεση με τα κεντρικά συστήματα των δεδομένων για την απόκτηση πληροφοριών.

Περαιτέρω, γίνεται μια λεπτομερής αναφορά σχετικά με τις μαγνητικές ταινίες , ποια είναι η διαφορά τους με τις έξυπνες κάρτες και ποιο είναι το ιστορικό των έξυπνων καρτών.

1.1.1 Ιστορικό

Η δημιουργία των πλαστικών καρτών για την εξυπηρέτηση των καθημερινών αναγκών πραγματοποιήθηκε στις αρχές της δεκαετία του 50 στην Αμερική. Οι πρώτες κάρτες που σχηματίστηκαν εμπεριείχαν τρία χαρακτηριστικά:

- Το όνομα της εταιρίας που εκδόθηκε.
- Τα προσωπικά στοιχεία του ιδιοκτήτη.
- Ένα αριθμό που τις προσδιόριζε.

Η ανάγκη για περισσότερη ασφάλεια ως προς τις συναλλαγές οδηγήθηκε στον σχηματισμό των καρτών μαγνητικής ταινίας γνωστές και ως πιστωτικές κάρτες. Οι πιστωτικές κάρτες χρησιμοποιούνται από τους παροχείς της κάρτας για κατάθεση χρημάτων για ανάληψη χρημάτων και οποιαδήποτε άλλη ενέργεια που συνδέεται με την συναλλαγή των χαρτονομισμάτων. Η σταδιακή εξέλιξη στην τεχνολογία της μικροηλεκτρονικής καθοδήγησε σε αυτό που λέμε σήμερα έξυπνη κάρτα.

Η έξυπνη κάρτα εφευρέθηκε από τον Γάλλο εκδότη Roy Bright το 1980 αλλά η έμπνευση για μια κάρτα ολοκληρωμένου κυκλώματος είχε εκφραστεί από δύο γερμανούς μηχανικούς, τον Jurgen Dethloff τον Helmut Grotrupp, το 1968. Το 1970, η ίδια αντίληψη παρουσιάστηκε στην Ιαπωνία από τον Kunitaka Arimura. Όμως με τον Roland Moreno το 1974 στην Γαλλία, μέσω της βιομηχανίας των ημιαγωγών , σχηματίστηκαν τα ολοκληρωμένα κυκλώματα σε αποδεκτές τιμές . Το 1979, δημιουργήθηκε, και πάλι στην Γαλλία, η πρώτη έξυπνη κάρτα από την εταιρία Motorola , ενώ το 1984 υλοποιήθηκε με επιτυχία ένα μεγάλο πιλοτικό πρόγραμμα με έξυπνες τηλεφωνικές κάρτες (τηλεκάρτες).

Τα ολοκληρωμένα κυκλώματα που μεταχειρίζονται σε μια τηλεκάρτα είναι μικρά και φτηνά ολοκληρωμένα κυκλώματα μνήμης, τα οποία έχουν σχηματιστεί σύμφωνα με το διαθέσιμο χρηματικό υπόλοιπο της κάρτας που μειώνεται ανάλογα με την χρήση της. Εντωμεταξύ, τα ολοκληρωμένα κυκλώματα που περιέχουν μικροεπεξεργαστή είναι μεγαλύτερα αλλά πολύπλοκα και χρησιμοποιήθηκαν για πρώτη φορά σε εταιρείες κινητής τηλεπικοινωνίας. Καινοτόμος στο φορέα αυτό ήταν το Γερμανικό Ταχυδρομείο το οποίο χρησιμοποίησε το 1988 μία κάρτα με μικροεπεξεργαστή που πρόσφερε εξουσιοδοτημένη πρόσβαση στο αναλογικό δίκτυο κινητής τηλεφωνίας C-Netz. Αυτή είναι η αιτία που μετά από λίγο χρονικά διάστημα οδήγησε την χρήση των έξυπνων καρτών σε GSM δίκτυα κινητής τηλεφωνίας. Στον φορέα των τραπεζικών καρτών, η πρόοδος ήταν μικρή εξαιτίας της μεγάλης δυσκολίας σε αναλογία με τις τηλεφωνικές κάρτες. Οι γαλλικές τράπεζες εισήγαγαν την συγκεκριμένη τεχνολογία το 1984 δηλαδή τον σχηματισμό καρτών τραπεζών εμπεριέχοντας ένα μικροεπεξεργαστή. Ενώ , την εποχή του 1997, όλες οι γερμανικές εταιρίες έκαναν χρήση των έξυπνων καρτών για τις συναλλαγές.

Η τεχνολογία των έξυπνων καρτών δεν είχε την ίδια ανταπόκριση τόσο στην Αμερική όσο και στην Ευρώπη. Έτσι την εποχή των ολυμπιακών αγώνων στην Ατλάντα το 1996, η Visa εκτύπωσε περίπου ενάμιση εκατομμύριο έξυπνες κάρτες VisaCASH. Την ίδια τεχνολογία , η Visa και η Master Card, έκαναν έρευνες για την επίλυση του προβλήματος συμβατότητας των καρτών με περιβάλλοντα προγραμματισμού. Η επίλυση του συγκεκριμένου προβλήματος ήταν η δημιουργία της Java Card που υποστηρίχθηκε από τη Visa, την Master Card καθώς και από το λειτουργικό σύστημα MultOs (Multi – Operating System).

Στην σημερινή εποχή, οι έξυπνες κάρτες υπάρχουν σε διάφορους φορείς όπως είναι οι τηλεπικοινωνίες , οι υπηρεσίες υγείας καθώς και σε εφαρμογές κρυπτογράφησης παραδείγματος χάριν η ψηφιακή υπογραφή.

1.2 Εισαγωγή Κάρτα Μαγνητικής Ταινίας

Η χρήση των μαγνητικών ταινιών καρτών είναι να αποθηκεύουν πληροφορίες σε μορφή αναγνωρίσιμη από μηχανές και έτσι έχουν αυτοματοποιήσει καθημερινές συναλλαγές και λειτουργίες. Όμως , η αυξημένη χρήση τους βοήθησε σε διάφορους χρήστες (απλοί, τραπεζικοί ή εμπορικοί). Αλλά στην πορεία προέκυψαν αρκετά και σημαντικά μειονεκτήματα.

Ένα βασικό μειονέκτημα πηγάσετε από το συμβάν ότι τα δεδομένα που αποθηκεύονται στην μαγνητική ταινία της κάρτας αποτελεί την ευχέρεια να διαβαστούν και να επεξεργαστούν από οποιονδήποτε χρήστη που έχει πρόσβαση στον κατάλληλο εξοπλισμό. Οι εμπιστευτικές πληροφορίες όπως είναι δηλαδή ο κωδικός ανάγνωσης του κατόχου να μην έχουν τη δυνατότητα να αποθηκεύονται στην ίδια κάρτα, οπότε αναγκάζονται να καταγραφούν σε μια άλλη κεντρική βάση δεδομένων. Επομένως , για να εφαρμοστούν οποιαδήποτε δοσοληψία χρειάζεται να υπάρχει τότε μία συσκευή συναλλαγής με τον ενδεχόμενο ότι βρίσκεται σε online σύνδεση με τον κεντρικό υπολογιστή ώστε να πραγματοποιηθεί η πιστοποίηση αυθεντικότητας . Άρα, όλη αυτή η διαδικασία είναι χρονοβόρα σε χρόνο αλλά και το κόστος αρκετό υψηλό.

Συμπεραίνουμε ότι οι μαγνητικές ταινίες διαχειρίζονται με συνδυασμό την ύπαρξη μεγάλων κεντρικών μονάδων με σκοπό τη φύλαξη και την κατεργασία των ευαίσθητων δεδομένων και τη συντήρηση κυκλωμάτων για τις σημαντικές online συνδέσεις ανάμεσα στην κεντρική βάση δεδομένων και στο σημείο συναλλαγής. Επιπροσθέτως, επειδή εμφανίζουν κάποια ευαισθησία σε συντελεστές π.χ. τα μαγνητικά παιδία και οι επαφές που περιλαμβάνουν αιχμηρά αντικείμενα και εκτεταμένη διαχείριση τους, αυτό μπορεί να έχει σαν συνέπεια την καταστροφή της μαγνητικής κάρτας ταινίας. Τέλος, οι καθορισμένες κάρτες έχουν σχεδιαστεί ώστε να εμπεριέχουν μια αποκλειστική εφαρμογή και στον ενδεχόμενο μιας αλλαγή στα χαρακτηριστικά είτε της εφαρμογής είτε στα προσωπικά στοιχεία του κατόχου απευθείας γίνεται η αντικατάσταση.

1.3 Παραλληλισμός της έξυπνης κάρτας & κάρτα μαγνητικής ταινίας

Στις παραπάνω ενότητες έγινε μια αναφορά στο τι είναι έξυπνες κάρτες και μαγνητικές ταινίες, ποια είναι τα βασικά χαρακτηριστικά, ποια είναι η λειτουργία τους και ποια τα πλεονεκτήματα και μειονεκτήματα. Σ' αυτή την ενότητα θα αναφερθούν και θα περιγραφούν οι διαφορές ανάμεσα στις δύο συγκεκριμένες κάρτες. Οι διαφορές είναι οι ακόλουθες:

- **Αποθήκευση δεδομένων:** Οι κάρτες της μαγνητικής ταινίας περιέχουν περιορισμένη δυνατότητα αποθήκευσης δηλαδή από 1byte έως 140 bytes. Ενώ οι έξυπνες κάρτες περιλαμβάνουν τεράστια χωρητικότητα με δυνατότητα αποθήκευσης από 1Kbyte έως 32Kbytes πληροφορίας)
- **Ασφάλεια:** Στις κάρτες μαγνητικής ταινίας τα στοιχεία μπορούν με ευχέρεια να τροποποιηθούν ή να παραχθούν από μη νόμιμους χρήστες. Ενώ στις έξυπνες κάρτες μέσω της κρυπτογράφησης κατέχει μια αυξημένη προστασία στα δεδομένα και στη δοσοληψία .
- **Αντίσταση:** Οι κάρτες της μαγνητικής ταινίας θεωρούνται εύθικτες κάρτες επειδή δέχονται είτε απομαγνητισμό είτε από εξωτερικούς συντελεστές μαγνητικών πεδίων. Ενώ οι έξυπνες κάρτες φανερώνουν την ανθεκτικότητα και επίσης αποτελούν κάρτες με μεγάλη διάρκεια ζωής.
- **Χρησιμοποίηση:** Οι κάρτες μαγνητικής ταινίας έχουν προγραμματιστεί έτσι ώστε να συμπεριλάβουνε αποκλειστικά μόνο μία εφαρμογή καθώς και να επαναλαμβάνουνε τα ίδια καθήκοντα. Ενώ στις έξυπνες κάρτες μπορούν να ενισχυθούν από περίπλοκες πολλαπλές εφαρμογές.
- **Ευελιξία:** Στις κάρτες μαγνητικής ταινίας , τα δεδομένα αποτελούν μόνο αναγνώσιμα και αυτό έχει σαν συνέπεια όταν είναι αναγκαία η αλλαγή στοιχείων τότε πρέπει να εκτυπωθεί μια καινούρια κάρτα. Ενώ στις έξυπνες κάρτες . πραγματοποιούνται με ευχέρεια και ταχύς οι λειτουργίες ανάγνωσης , εγγραφής και ανανέωσης των δεδομένων.
- **Σύζευξη:** Στις κάρτες μαγνητικής ταινίας απαιτείται online σύνδεση με την κεντρική βάση δεδομένων για κάθε δοσοληψία όπου επιφέρεται η ύπαρξη της μισθωμένης γραμμής. Ενώ στις έξυπνες κάρτες υλοποιούν offline συνδέσεις με έγκυρες δοσοληψίες.
- **Κόστος:** Αν και η δημιουργία μιας έξυπνης κάρτας περιλαμβάνει υψηλό κόστος εξαιτίας της ανθεκτικότητας, τη χρήση πολλαπλών εφαρμογών, τη μείωσης οικονομικών απατών και τηλεπικοινωνιακής σύνδεσης παρέχει ένα αποδοτικό κόστος σε σύγκριση με τις μαγνητικές ταινίες καρτών.

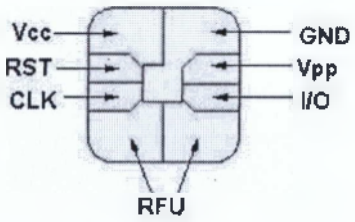
ΚΕΦΑΛΑΙΟ 2 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΚΑΙ ΥΛΙΚΟ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ

2.1 Περιγραφή υλικού έξυπνων καρτών

Σχετικά με την τεχνολογία των έξυπνων καρτών (smart cards) , υπάρχουν κάποια τεχνικά γνωρίσματα. Για να υπάρξει σαφές η κατανόηση των γνωρισμάτων μιας έξυπνης κάρτας , είναι αναγκαία να διευκρινίσουμε κάποιες σημαντικές ηλεκτρονικές έννοιες στο κομμάτι του υλικού των έξυπνων καρτών και στη συνέχεια να προχωρήσουμε στο κομμάτι της αρχιτεκτονικής των έξυπνων καρτών

2.1.1 Σημεία επαφής μιας έξυπνης κάρτας

Μια έξυπνη κάρτα αποτελείται από οχτώ σημεία επαφής. Τα οχτώ σημεία επαφής εφαρμόζονται για τρεις βασικές ενέργειες δηλαδή για τροφοδοσία , για παλμούς ρολογιού και για μετάδοση δεδομένων. Οι επαφές εφαρμόζονται σύμφωνα με το πρότυπο του ISO7816-2 το οποίο προσδιορίζει τη θέση, το ελάχιστο μέγεθος και την λειτουργία τους. Παρακάτω υπάρχει μια εικόνα όπου απεικονίζει την δομή των επαφών μιας έξυπνης κάρτας.



Εικόνα 1: Σημεία επαφής έξυπνης κάρτα

Vcc: Τροφοδοτεί με τάση το κύκλωμα. Η τάση κυμαίνεται από 4.5V έως 5.5V **RST:** Αποστολή σήματος reset στον chip, μέθοδος warm reset ή Αφαίρεση και επαναφορά τροφοδοσίας, μέθοδος cold reset. **CLK:** Τροφοδοσία του επεξεργαστή με παλμούς ρολογιού – clock signal **GND:** Γείωση του κυκλώματος **Vpp:** Χρήση υψηλής τάσης. Είναι απαραίτητο για τον προγραμματισμό μνήμης EEPROM. **I/O**: Μεταφορά δεδομένων από και προς την κάρτα. Χρήση μεθόδους half duplex δηλαδή τα δεδομένα μεταδίδονται σε μία κατεύθυνση στη συγκεκριμένη χρονική στιγμή. **RFU**: Μελλοντική χρήση

Πίνακας 1: Επεξήγηση ορολογίας

2.1.2 Μικροτσίπ ή Ολοκληρωμένο Κύκλωμα

Το μικροτσίπ είναι γνωστό και ως ολοκληρωμένο κύκλωμα. Αποτελείται από ένα σύνολο πολύπλοκων και πολύ μικρών στοιχείων που έχουν τη δυνατότητα να αποθηκεύονται σε κάποια μνήμη του υπολογιστή ή να χορηγούν ένα λογικό κύκλωμα για μικροεπεξεργαστές. Το μικροτσίπ κατασκευάζεται πάνω σε φύλλα ημιαγωγών και πιο συγκεκριμένα από κυκλικά επίπεδα δισκίου πυριτίου τα οποία εξετάζονται ως προς το μέγεθος και συνδέονται με κυκλώματα και ηλεκτρονικές συσκευές. Σήμερα, τα ολοκληρωμένα κυκλώματα χρησιμοποιούνται σε κάθε στοιχείο ηλεκτρονικού εξοπλισμού.

Ανάλογα με τον αριθμό των λογικών πυλών από τα οποία αποτελούνται τα μικροτσίπ διακρίνονται σε τέσσερις κατηγορίες: (1) SSI , (2) MSI, (3) LSI και (4) VLSI.

- ***SSI:*** Στα ελληνικά σημαίνει η μικρή κλίμακας ολοκλήρωσης. Είναι ολοκληρωμένα κυκλώματα που εμπεριέχουν είκοσι λογικές πύλες. Περιλαμβάνουν μεμονωμένες λογικές πύλες που μπορεί να χρειάζεται ένα απλό κύκλωμα.
- ***MSI:*** Στα ελληνικά δηλώνει τη μεσαία κλίμακα ολοκλήρωσης. Είναι ολοκληρωμένα κυκλώματα που εμπεριέχουν διακόσες λογικές πύλες. Περιλαμβάνουν λογικές δομικές μονάδες ολοκληρωμένων κυκλωμάτων
- ***LSI:*** Στα ελληνικά εκφράζει τη μεγάλη κλίμακα οργάνωσης. Είναι ολοκληρωμένα κυκλώματα που εμπεριέχουν διακόσες με διακόσες χιλιάδες λογικές πύλες.
- ***VLSI:*** Στα ελληνικά σημαίνει τη πολύ μεγάλη κλίμακα ολοκλήρωσης. Είναι τα ολοκληρωμένα κυκλώματα που εμπεριέχουν πολλές λογικές πύλες. Δίνουν τη δυνατότητα να δημιουργούνται μνήμες όπως είναι RAM ή ROM ή μονάδες επεξεργασίας CPU σε ένα και μόνο τσιπ.

2.1.3 Μνήμη

Η μνήμη είναι ένα ηλεκτρικό μέσο αποθήκευσης που αποθηκεύονται διάφορες εντολές και πληροφορίες παίρνοντας ψηφιακή μορφή. Ο επεξεργαστής μπορεί με ευχέρεια να έχει πρόσβαση στα δεδομένα . Όταν ένας υπολογιστής λειτουργεί τότε η μνήμη περιλαμβάνει τα κύρια μέρη του λειτουργικού συστήματος του υπολογιστή ή όλες τις εφαρμογές και δεδομένα που αυτά διαχειρίζονται. Υπάρχουν τέσσερις μνήμες οι οποίες είναι: RAM, ROM, EEPROM, FLASH τις οποίες αναλύονται ακριβώς παρακάτω.

2.1.3.1 Μνήμη RAM

Η μνήμα RAM προέρχεται από τις αγγλικές λέξεις Random Access Memory και σημαίνουν Μνήμη Τυχαίας Προσπέλασης. Αναφέρεται στην κεντρική μνήμη του υπολογιστή όπου αποθηκεύονται προγράμματα και δεδομένα ώστε να μπορούν να εκτελούν εφαρμογές και να υφίστανται επεξεργασία αντίστοιχα. Επιπλέον, έχει μικρή χωρητικότητα σε σύγκριση με άλλα αποθηκευτικά μέσα όπως είναι ο σκληρός δίσκος. Όταν ο υπολογιστής βρίσκεται εκτός λειτουργίας τότε όλα τα δεδομένα και προγράμματα που έχουν αποθηκευτεί στη μνήμη RAM θα χαθούν. Η έννοια "Τυχαία Προσπέλαση" εκφράζεται στο ότι η πρόσβαση σε αποθηκευμένη πληροφορία δεν προκύπτετε ακολουθιακά αλλά άμεσα.

2.1.3.2 Μνήμη ROM

Η μνήμη ROM προέρχεται από τις αγγλικές λέξεις Read Only Memory και σημαίνουν Μνήμη Μόνο Ανάγνωσης. Όπως η μνήμη RAM έτσι και η μνήμη ROM είναι μια μορφή ηλεκτρονικής μνήμης η οποία δεν έχει την δυνατότητα να κάνει εγγραφές, αλλά μόνο ανάγνωση. Επιπλέον , αυτή η μνήμη είναι και μη πτητική ,δηλαδή δε χάνει δεδομένα της με τη διακοπή της τροφοδοσίας του ρεύματος, που χρησιμοποιείται σε ηλεκτρονικές συσκευές όπως είναι ο ηλεκτρονικός υπολογιστής. Επίσης γράφεται μόνο μία φορά από το εργοστάσιο που την κατασκευάζει. Τέλος, το κόστος της Μνήμης Μόνο Ανάγνωσης (ROM) είναι εξέχων υψηλός από αυτό της Μνήμης Τυχαίας Προσπέλασης (RAM).

2.1.3.3 Μνήμη EEPROM

Η μνήμη EEPROM προέρχεται από τις αγγλικές λέξεις Electrically Erasable Programmable Read – Only Memory που σημαίνουν Ηλεκτρικά Διαγραφόμενη Προγραμματιζόμενη Ανάγνωση Μόνο Μνήμη. Είναι η μεταγενέστερη έκδοση της Μνήμης Μόνο Ανάγνωσης (ROM). Ένα χαρακτηριστικό που έχει αυτή η μνήμη είναι ότι διατηρούν τα περιεχόμενα τους μετά τη διακοπή της τροφοδοσίας τους με ηλεκτρική ισχύ. Αλλά όμως μπορούν να ακυρώνουν και να ξανά προγραμματίζουν με νέα δεδομένα με ηλεκτρικό τρόπο ακόμα και όταν βρίσκονται πάνω στο κύκλωμα. Η διάρκεια ζωής της μνήμης είναι μειωμένη επειδή εγκρίνει ένα συγκεκριμένο αριθμό επαναπρογραμματισμών που απλώνεται σε δεκάδες ή εκατοντάδες χιλιάδες.

2.1.3.4 Μνήμη FLASH

Η μνήμη FLASH αντιστοιχεί με το είδος της μνήμης EEPROM. Αυτό που κάνει τη διαφορά μεταξύ των δύο τύπων μνήμης είναι στη ταχύτητα της διαγραφής και του επαναπρογραμματισμού του περιεχομένου της. Δηλαδή, η μνήμη EEPROM διαγράφει ένα byte τη φορά ενώ η μνήμη FLASH ακυρώνει ολόκληρα μπολ από byte, πολλαπλασιάζοντας με αυτό τον τρόπο την ταχύτητα διαγραφής και προγραμματισμού της μνήμης αυτής. Επιπροσθέτως , υπάρχουν δύο βασικά είδη μνήμης η NAND και NOR γνωστές ως πύλες λογικής. Τα κύρια γνωρίσματα της μνήμης FLASH εμφανίζονται παρόμοια με τα χαρακτηριστικά των αντίστοιχων πυλών. Η NAND ή NOR μνήμη FLASH εφαρμόζεται για την αποθήκευση δεδομένων διαμόρφωσης σε πολλά ψηφιακά προϊόντα. Τέλος, το μειονέκτημα που έχει η συγκεκριμένη μνήμη είναι το καθορισμένο ποσό των κύκλων εγγραφής σε ένα συγκεκριμένο μπλοκ.

2.1.4 Επεξεργαστής – Κεντρική Μονάδα Επεξεργασίας

Ο επεξεργαστής παρουσιάζεται ως Κεντρική Μονάδα Επεξεργασίας ή CPU (από τις αγγλικές λέξεις Central Processing UNIT). Η ιδιότητα του επεξεργαστή είναι να ασκεί έλεγχο στη λειτουργία του υπολογιστή και να εφαρμόζει τις λειτουργίες επεξεργασίας δεδομένων. Όταν είναι ενσωματωμένος ο επεξεργαστής σε ένα προσωπικό υπολογιστή ή σε μικρές συσκευές λέγεται μικροεπεξεργαστής (microprocessor) ή μικροελεγκτής (microcontroller). Άρα CPU είναι ενσωματωμένη σε κάθε είδους συσκευής στην οποία είναι ανάγκη να υπάρχει υπολογιστική ικανότητα.

2.1.5 Μικροεπεξεργαστής – Microprocessor

Ο μικροεπεξεργαστής αποτελείται από ένα επεξεργαστή του υπολογιστή που έχει την μορφή ενός μικροτσίπ. Η ιδιότητα του μικροεπεξεργαστή είναι να επιτελεί αριθμητικές και λογικές πράξεις που χρησιμοποιούνται σε μικρές περιοχές μέτρησης αριθμών τα οποία λέγονται καταχωρητές. Τέτοιες πράξεις είναι η πρόσθεση, αφαίρεση, σύγκριση δύο αριθμών, και η μεταφορά αριθμών από μια περιοχή σε άλλη. Η συνέπεια αυτών των διεργασιών είναι το άθροισμα των εντολών που απαρτίζεται μέρος του πλάνου του μικροεπεξεργαστή (microprocessor). Επίσης, αυτό απαρτίζεται από τρία βασικά μέρη, τα οποία συμπράττουν αρμονικά μεταξύ τους και είναι τα εξής:

- Αριθμητική και λογική μονάδα (Arithmetic and Logic Unit, ALU)
- Μονάδα ελέγχου (Control Unit, CU)
- Καταχωρητές (Registers)

2.1.6 Εντολές

Είναι οι διαταγές που δέχεται ο επεξεργαστής του υπολογιστικού συστήματος. Αυτές οι εντολές έχουν την μορφή μίας ακολουθίας από μηδενικά και άσσους ψηφία. Τα συγκεκριμένα ψηφία απεικονίζουν μία φυσική διεργασία που επιτελεί ο υπολογιστής ή ταυτότητα των καταχωριστών που θα μεταχειριστούν για την εντολή.

2.1.7 Δημόσιο Κλειδί – Public Key

Κρυπτογραφία δημόσιου κλειδιού ή ασύμμετρη κρυπτογραφία έχει σαν βασικό χαρακτηριστικό την χρήση δύο διαφορετικά αλλά μαθηματικά συσχετιζόμενα κλειδιά. Το δημόσιο κλειδί μπορεί να καταχωρηθεί σε όποιον θέλει να κάνει μια συναλλαγή με την οντότητα όπως που διαχειρίζεται το ιδιωτικό κλειδί. Δηλαδή, σε περίπτωση που χρειάζεται να κρυπτογραφηθούν κάποια στοιχεία τότε εφαρμόζεται η μεταχείριση του δημόσιου κλειδιού ενώ το ιδιωτικό κλειδί εφαρμόζεται στην διαδικασία της αποκρυπτογράφησης. Επιπλέον, το public key εφαρμόζεται στη δημιουργία μη παραποιούμενων ψηφιακών υπογραφών βασισμένου στο private key του χρήστη. Τέλος, ένα πολύ σημαντικό μειονέκτημα που έχει είναι η αύξηση του υπολογιστικού κόστους του.

2.1.8 Ιδιωτικό Κλειδί – Private Key

Το ιδιωτικό κλειδί αποτελεί ένα κρυπτογραφικό κλειδί που δεν είναι αποθηκευμένο σε ένα μέσο συνδεδεμένο στο δίκτυο. Βασικό γνώρισμα του είναι η χρήση του πάνω στην αποκρυπτογράφηση κάποιων δεδομένων και στην δημιουργία αντιγράφων ασφαλείας δεδομένων. Αν σε περίπτωση το κλειδί χαθεί τότε η ασφάλεια και η μυστικότητα της επικοινωνίας θα χαθεί.

2.2 Δημιουργία σχηματισμού μιας έξυπνης κάρτας

Η δημιουργία μιας έξυπνης κάρτας είναι μια περίπλοκη διαδικασία. Σ' αυτή την ενότητα θα αναφερθούν τα στάδια που πρέπει να ακολουθηθούν ώστε να σχηματιστεί μία έξυπνη κάρτα. Τα βήματα που πρέπει να εκτελεστούν είναι τα ακόλουθα.

- **1ο στάδιο:** Η δημιουργία ολοκληρωμένου: Εφαρμόζονται οι ενέργειες για την κατασκευή ενός κυκλώματος.
- **2ο στάδιο:** Η δημιουργία ολόκληρου τμήματος των επαφών: Για να δημιουργηθεί ο σχηματισμός ενός ολόκληρου τμήματος των επαφών πρέπει το κύκλωμα να συσσωματωθεί με την περιοχή των επαφών.
- **3ο στάδιο:** Η δημιουργία πλαστικής κάρτας: Εδώ πρέπει να χρησιμοποιηθεί το PVC ως ένα υλικό της κάρτας. Επίσης, εκδίδεται και η κάρτα.
- **4ο στάδιο**: Διορισμός (τοποθέτηση) του τμήματος των επαφών: Σχηματίζεται μια τρύπα ώστε να εισαχθεί το κομμάτι του ολοκληρώματος των επαφών.
- **5ο στάδιο:** Εφαρμογή της αρχικοποίησης: Στο συγκεκριμένο στάδιο τα δεδομένα και οι εφαρμογές εισάγονται στην μνήμη EEPROM.

- **6ο στάδιο:** Ενέργεια της προσωποποίησης: Σ' αυτό το βήμα δηλαδή θα τοποθετηθούν δεδομένα που θα αφορά τον χρήστη όπως είναι το όνομα του.

2.2.1 Προσχεδιασμός μικροεπεξεργαστή (chip)

Η επιλογή για την ενσωμάτωση ενός μικροεπεξεργαστή μέσα σε μια κάρτα εξαρτάται από ορισμένους συντελεστές. Οι πιο σημαντικοί συντελεστές είναι οι ακόλουθες:

- Η επιλογή τύπου μικροεπεξεργαστή.
- Ποιο θα είναι το μέγεθος της μνήμης RAM.
- Ποιο θα είναι το μέγεθος της μνήμης ROM.
- Επιλογή τύπου μιας ευμετάβλητης μνήμης.
- Ποιο θα είναι το μέγεθος της ευμετάβλητης μνήμης.
- Ποια θα είναι η ταχύτητα του ρολογιού.
- Ποιοι θα είναι οι ηλεκτρονικοί παράμετροι.
- Ποιοι θα είναι οι παράμετροι επικοινωνίας.
- Η χρήση του μηχανισμού RESET
- Η χρήση του SLEEP MODE

2.2.2 Προσχεδιασμός της κάρτας

Οι συντελεστές που συμβάλλουν στον προσχεδιασμό μιας κάρτας είναι κοινές με αρκετές εφαρμογές που εφαρμόζονται πάνω στο πρότυπο ISO ID1. Περαιτέρω γίνεται μια αναφορά αυτών των συντελεστών.

- Εξαρτάται από τις διαστάσεις της κάρτας
- Εξαρτάται από τη θέση του μικροεπεξεργαστή
- Εξαρτάται από τη χρήση του υλικού της κάρτας
- Από τις απαιτήσεις εκτύπωσης
- Από την μαγνητική ταινία και από τα διάφορα σχέδια αλλά δεν εξαρτώνται σε τόσο μεγάλο βαθμό σε σύγκριση με τους άλλους συντελεστές.
- Εξαρτάται από τους παραμέτρους που σχετίζονται με το περιβάλλον εκτέλεσης

2.2.3 Προσχεδιασμός μνήμης μάσκας Rom

Η μάσκα ROM είναι μια μορφή της μνήμης μόνο για ανάγνωση των οποίων τε δεδομένα έχουν προγραμματιστεί από το ολοκληρωμένο κύκλωμα του κατασκευαστή. Ο όρος μάσκα (mask) πηγάζετε από την ανάπτυξη ολοκληρωμένων κυκλωμάτων. Ασχολούνται με την αντιμετώπιση των δεδομένων αλλά έχουν την δυνατότητα να ασχοληθούν με άλλες ενέργειες όπως είναι κρυπτογραφικοί αλγόριθμοι. Συνδέο-

νται με το πρότυπο ISO 7816-4. Τέλος , ο κώδικας χορηγείται στον προμηθευτή ώστε να ενσωματώσει τα δεδομένα σαν μέρος της διαδικασίας κατασκευής της κάρτας.

2.2.4 Προσχεδιασμός λογισμικού εφαρμογών

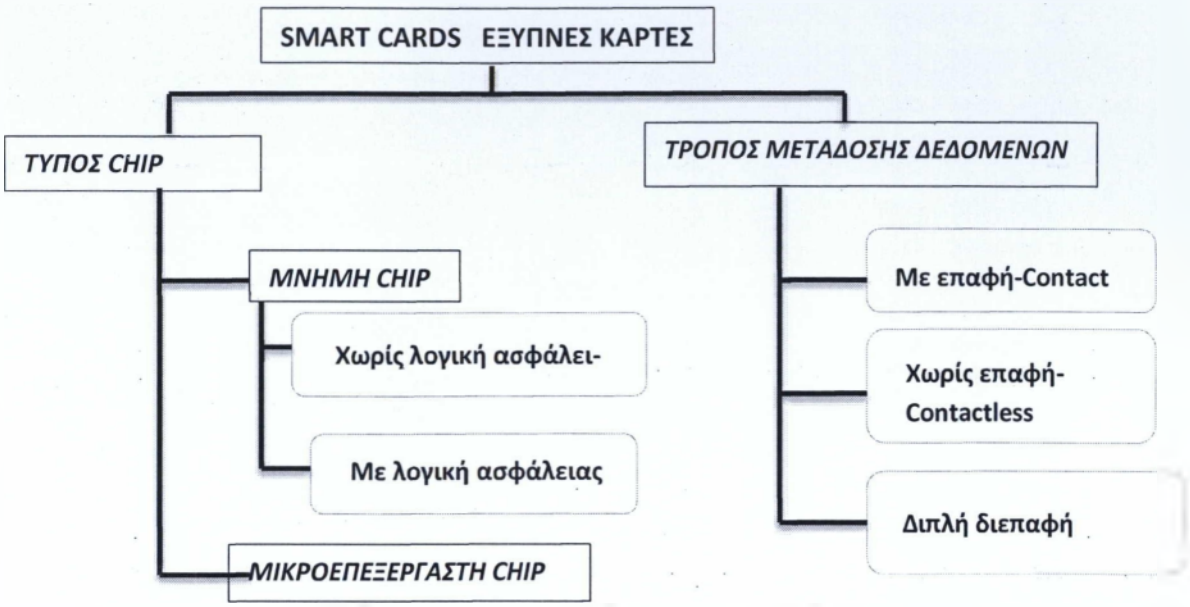
Ο προσχεδιασμός λογισμικού εφαρμογών εξαρτάται από την φύση της εφαρμογής. Ο κώδικα της κάποτε σχεδιαζόταν σαν μέρος στην μάσκα ROM αλλά τώρα σχεδιάζεται σαν μέρος της μνήμης EEPROM επειδή μπορεί η εφαρμογή να φορτωθεί στον μικροεπεξεργαστή πιο εύκολα αλλά και να μεταφέρει τον κώδικα σε αναπτυξιακό περιβάλλον. Ο κώδικας της εφαρμογής κατορθώνει να φορτωθεί στη μνήμη EEPROM μέσα σε λίγα λεπτά.

2.2.5 Ενέργειες δημιουργίας μικροεπεξεργαστή (chip)

Η πρώτη ενέργεια για την δημιουργία ενός μικροεπεξεργαστή είναι η κατασκευή ενός υποστρώματος το οποίο περιέχει και το chip. Γι' αυτή την ενέργεια υπάρχουν τρεις ελεύθερες τεχνολογίες δηλαδή την wire bonding, την flip chip processing, και την tape automated bonding. Σε κάθε βήμα ο δίσκος πυριτίου διαιρείται σε μικρά chips. Η τεχνική που εφαρμόζεται για την δημιουργία των έξυπνων καρτών είναι η wire bonding. Αυτή η τεχνολογία κάνει χρήση υπερηχητικών κύματα ή θερμοσυμπίεση και ένα χρυσό ή αλουμινένιο καλωδίων με διάσταση 25mm που συνδέει το chip με το υπόστρωμα. Στην περίπτωση της θερμικής συμπίεσης επιζητεί την διατήρηση του υποστρώματος σε θερμοκρασία ανάμεσα στους 150^{o} και στους 2000^{o}C . Κατά τη διάρκεια της διασύνδεσης φτάνει περίπου στους 350^{o}C. Για την επίλυση των προβλημάτων υπάρχει η μέθοδος της ηχητικής συγκόλλησης. Είναι ο συνδυασμός των δύο παραπάνω διαδικασιών και εφαρμόζεται σε χαμηλές θερμοκρασίες.

2.3 Τύποι καρτών

Οι έξυπνες κάρτες έχουν την ευχέρεια να αρχειοθετούνται μα βάση δύο κριτήρια: πρώτον, ο τρόπος με τον οποίο τα δεδομένα διαβάζονται από αυτές και γράφονται σε αυτές και δεύτερον, ο τύπος και οι δυνατότητες του ολοκληρωμένου κυκλώματος που περιλαμβάνονται. Στο παρακάτω σχήμα, παρουσιάζεται ένα διάγραμμα με τον οποίο οι έξυπνες κάρτες ταξινομούνται ανάλογα με τον τύπο του ολοκληρωμένου κυκλώματος που μεταχειρίζεται και ανάλογα με τη μέθοδο μετάδοσης δεδομένων.



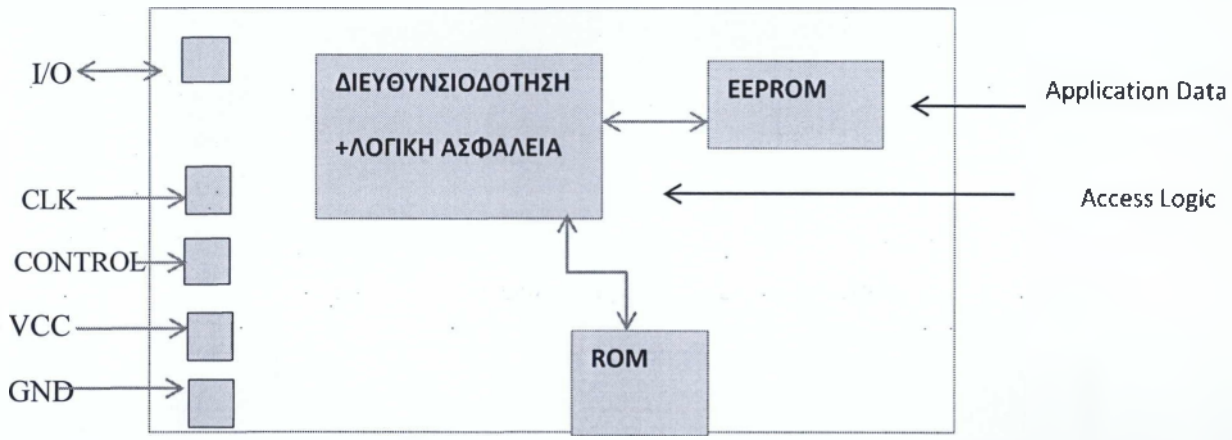
Διάγραμμα 1: Κατάταξη των έξυπνων καρτών συμφώνα με το τύπο και τον τρόπο μετάδοση δεδομένων

2.3.1 Κάρτες Μνήμης - Memory Cards

Οι κάρτες μνήμης συγκαταλέγουν ένα κύκλωμα μνήμης και προγραμματίζονται μια φορά από την κατασκευάστρια εταιρία. Αυτές δεν εμπεριέχουν ένα ενσωματωμένο μικροεπεξεργαστή και μπορούν να μεταχειριστούν μόνο για την αποθήκευση δεδομένων. Συγκαταλέγουν ένα κύκλωμα μνήμης, που λέγεται EEPROM και τα αρχικά τους προέκυψαν από τις αγγλικές λέξεις Electrically Erasable Programmable Read Only Memory, και μια μη προγραμματιζόμενη λογική. Ένα μειονέκτημα που συνθέτουν τις κάρτες μνήμης είναι ότι δεν ξανά-προγραμματίζονται άρα δεν ξαναχρησιμοποιούνται

Λόγω της ένδειας του μικροεπεξεργαστή, η προσπέλαση της μνήμης τελείται μέσω ενός μηχανισμού που προσδιορίζεται στο τρίτο μέρος του προτύπου ISO 7816. Το κανάλι επικοινωνίας μεταξύ του χρήστη και της κάρτας συνίσταται από τον έλεγχο της συσκευής ανάγνωσης (reader card) και το κύκλωμα της κάρτας που εισακούεται με ένα σύγχρονο τρόπο στις χαμηλού επιπέδου εντολές της reader card για την αναζήτηση συγκεκριμένων περιοχών μνήμης και για ανάγνωση από ή εγγραφή σε αυτές. Τα δεδομένα μεταφέρονται στην κάρτα και από την κάρτα μέσω της θύρας εισόδου-εξόδου. Επιπλέον, η πρόσβαση στη μνήμη εξετάζεται από μια μονάδα ελέγχου

ασφαλείας, security logic unit, η οποία απαρτίζεται από προστασία εγγραφής ή διαγραφής για όλη ή για συγκεκριμένες περιοχές της μνήμης. Όμως, υπάρχουν κάποια άλλα κυκλώματα που συμπεριλαμβάνουν πολύπλοκες δομές ασφαλείας και τα οποία επιτελούν απλές κρυπτογραφικές λειτουργίες. Παρακάτω παρουσιάζεται ένας πίνακας και ένα διάγραμμα που απεικονίζει την αρχιτεκτονική της κάρτας μνήμης:



Διάγραμμα 2: Αρχιτεκτονική έξυπνης κάρτας

I/O: Μεταφορά δεδομένων ανάμεσα σε αναγνώστη και κάρτα με τρόπο μονής κατεύθυνσης. **Vcc:** Παροχή τάσης στο Ολοκληρωμένο. Η τάση κυμαίνεται μεταξύ 4.5V και 5.5V **CLK:** Εφαρμογή εξωτερικού ρολογιού **Control:** Μεταφορά εξωτερικού ρολογιού **GND:** Σύνδεση με τη γη

Πίνακας 2: Επεξήγηση των ορολογιών

Επιπροσθέτως, οι κάρτες μνήμης περιλαμβάνουν μια εφαρμογή η οποία εκτελείται μέσω των συσκευών υποδοχών των καρτών με τις οποίες επικοινωνούν. Αυτές μπορούν να ταξινομηθούν σε τρεις υποκατηγορίες.

2.3.1.1 Straight Memory Cards - Ευθεία Κάρτες Μνήμης

Οι Straight Memory Cards είναι κάρτες που ωφελούν μόνο για την αποθήκευση δεδομένων. Το μειονέκτημα τους είναι ότι δεν έχουν την δυνατότητα να επεξεργάζονται τα δεδομένα και δεν μπορούν να παρέχουν καμία ασφάλεια. Είναι οι πιο φτηνές κάρτες μνήμης. Υλοποιούνται με I2C ή με σειριακή ημιαγωγών φλας. Επιπλέον , αυτές δεν μπορούν να ταυτίζονται με τον reader-αναγνώστη, ο οποίος για να έχει επικοινωνία μαζί τους πρέπει εκ προτέρων να αναγνωρίζει τι τύπου κάρτες είναι.

2.2.3.2 Protected ή Segment Memory Cards - Προστατευόμενες ή Κατάτμηση Κάρτες Μνήμης

Οι Protected ή Segment Memory Cards είναι κάρτες που εμπεριέχουν μία ενσωματωμένη λογική για να εξακριβώνουν την πρόσβαση στη μνήμη. Αυτές μπορούν να ρυθμιστούν με κύριο στόχο να ορίσουν την προστασία εγγραφής μερικών κομματιών ή το σύνολο της διάταξης της μνήμης .Κατά κανόνα αυτό πραγματοποιείται με τη χρήση κάποιου κωδικού πρόσβασης συστήματος. Επιπλέον, χωρίζονται σε λογικές ενότητες ώστε να μπορούν να χρησιμοποιηθούν σε διαφορετικές ταυτόχρονες εφαρμογές.

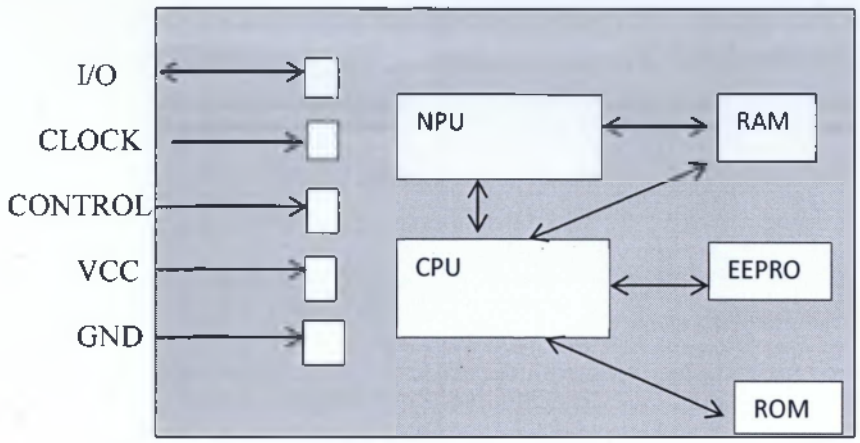
2.2.3.3 Stored Value Memory Cards - Αποθηκευμένες Αξίες Κάρτες Μνήμης

Οι Stored Value Memory Cards είναι εκείνες οι κάρτες μνήμης που μπορούν να είναι μίας χρήσης ή και επαναφορτιζόμενες δηλαδή όταν θα εξανεμίζονται οι αποθηκευμένες αξίες τότε θα γίνεται μια ανανέωση ώστε να αποθηκεύονται καινούριες. Πολλές από αυτές τις κάρτες ενσωματώνουν μόνιμα μέτρα ασφαλείας στο σημείο της κατασκευής. Τα μέτρα ασφαλείας περιλαμβάνουν κλειδιά κωδικού πρόσβασης και λογική που έχουν κρυπτογραφηθεί στο τσιπ κατά την κατασκευή τους . Οι συστοιχίες μνήμης σχεδιάζονται και λειτουργούν είτε ως αφαιρέτες είτε ως μετρητές. Ελάχιστη ή καθόλου μνήμη περισσεύει για να μεταχειριστεί σε κάποια άλλη λειτουργία.

2.3.2 Κάρτες Με Μικροεπεξεργαστή - Microprocessor Cards

Οι κάρτες με μικροεπεξεργαστή είναι "γνωστές" ως έξυπνες κάρτες. Περιλαμβάνουν έναν μικροεπεξεργαστή. Ο μικροεπεξεργαστής διαχειρίζεται την επεξεργασία δεδομένων , την αποθήκευση και την αυξημένη ασφάλιση των δεδομένων καθώς και συνάμα υποστηρίξει πολλές διαφορετικές λειτουργίες. Η επεξεργασία υλοποιείται με τον κώδικα που εμπεριέχεται στην κάρτα, τον οποίο έχουμε την δυνατότητα να το επαναφορτίσουμε, διαγράψουμε, προσθέσουμε μεταβάλλοντας ως ακολούθως τη λειτουργία της κάρτας. Περαιτέρω παρέχουν έναν υψηλό επίπεδο ασφάλειας και γι' αυτό το λόγο χρησιμοποιούνται για την μεταφορά χρημάτων, τον έλεγχο πρόσβασης και γενικότερα όπου η ασφάλεια των δεδομένων και διαφύλαξη προσωπικών δεδομένων αποτελούν προτεραιότητα. Προτέρημα τους είναι η δυναμική κρυπτογράφηση και οι ενημερώσεις στις λογισμικές εφαρμογές. Επιπροσθέτως,, επικοι-

νωνεί με τις διαθέσιμες μνήμες τύπου ROM,RAM, EEPROM και από μια θύρα εισόδου και εξόδου. Παρακάτω παρουσιάζεται το διάγραμμα που περιγράφει την αρχιτεκτονική των καρτών με μικροεπεξεργαστή.



Διάγραμμα 3: Αρχιτεκτονική των καρτών με μικροεπεξεργαστή

Στη μνήμη ROM υπάρχει ένα λειτουργικό σύστημα της κάρτας που μετατρέπεται σε burned in κατά την συσκευή του κυκλώματος. Οι διάφορες εντολές καταγράφονται στη μνήμη από τον κατασκευαστή της κάρτας κατά την κατασκευή της. Το μέγεθος της κινεί από μερικά Kbyte μέχρι τα 32Kbyte, και αυτό εξαρτάται κυρίως από το λειτουργικό σύστημα που διαχειρίζεται.. Στην ουσία, η μνήμη ROM χρειάζεται για την αποθήκευση του λειτουργικού συστήματος. Στη μνήμη RAM είναι μια μνήμη εργασίας του μικροεπεξεργαστή. Δηλαδή, είναι μια βοηθητική μνήμη που περιλαμβάνει προσωρινά δεδομένα ήτοι όταν η κάρτα βρεθεί εκτός λειτουργίας τα δεδομένα αυτά χάνονται. Μέσω της θύρας εισόδου και εξόδου που αποτελείται από ένα καταχωρητή, δια μέσω του οποίου τα δεδομένα μεταφέρονται με ένα δυαδικό ψηφίο την φορά. Αν σε περίπτωση αυτές χρησιμοποιηθούν για μεγάλους αριθμητικούς υπολογισμούς τότε απαιτείται ένας βοηθητικός μικροεπεξεργαστής NPU, Numeric Processor Unit. Ενώ η μνήμη EEPROM είναι διαρκής , non volatile μνήμη. Δηλαδή, η μνήμη αυτή περιέχει τα προγράμματα εφαρμογών της κάρτας και τα αντίστοιχα δεδομένα των εφαρμογών. Τα περιεχόμενα της δεν είναι μόνιμα, μπορούν δηλαδή να διαγραφούν και να ξαναγραφτούν.

2.3.3 Έξυπνες κάρτες πολλαπλών εφαρμογών – Multi-Application Smart Cards

" Οι έξυπνες κάρτες τελευταίας γενιάς έρχονται με ανοικτά λειτουργικά συστήματα όπως είναι η JAVA, MULTOS και μπορούν να εκτελούν περισσότερες από

μία εφαρμογές. Επιπλέον, παρέχεται η δυνατότητα στο χρήστη να «φορτώνει» νέες εφαρμογές, ή για να διαγράφει άλλες ανάλογα με τις ανάγκες του."[1]

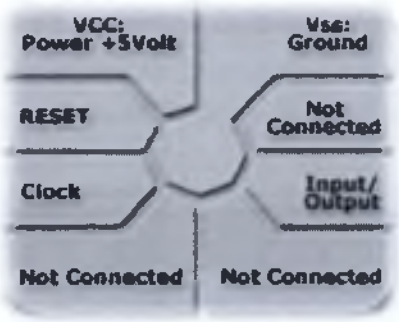
2.3.4 Έξυπνες Κάρτες Με Επαφές - Contact Cards

Προϋπόθεση για την λειτουργία των έξυπνων καρτών με επαφές είναι να εισαχθούν μέσα σε ένα card reader δηλαδή σε ένα αναγνώστη καρτών. Ο αναγνώστης θα έχει απευθείας επαφή με ένα μεταλλικό πιάτο το οποίο είναι τοποθετημένο στην επιφάνεια της κάρτας δηλονότι κάτω το οποίο βρίσκεται το μικροτσίπ, ώστε κατορθωθεί η μέθεξη ανάμεσα τους μέσω αυτών των ηλεκτρικών επαφών και για να πάρουν ρεύμα. Η επικοινωνία συνίσταται από τρία μέρη:

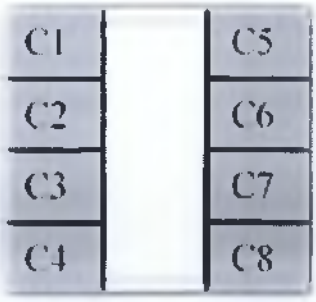
- **Ανταλλαγή δεδομένων κατάστασης**
- **Ανταλλαγή εντολών κατάστασης**
- **Ανταλλαγή πληροφοριών κατάστασης**

Ένα μειονέκτημα που έχουν οι έξυπνες κάρτες με επαφές είναι ότι έχουν περιορισμένη διάρκεια ζωής λόγω φθοράς. Τα κυκλώματα που εμπεριέχονται στην κάρτα έχουν την ευχέρεια να καταστραφούν από κάποιους παράγοντες όπως είναι οι ηλεκτροστατικές εκκενώσεις και η κακή χρήση καρτών από τους κατόχους.

Στις δύο παρακάτω εικόνες παρατηρούμε τις ηλεκτρικές επαφές οι οποίες είναι τοποθετημένες στην επιφάνεια της κάρτας. Η θέση τους προσδιορίζεται από τα διεθνή πρότυπα ISO 7816-1 και ISO 7816-2. Περαιτέρω αναλύονται οι λειτουργίες των ηλεκτρονικών επαφών.



Εικόνα 2: Condact Cards



Εικόνα 3: Condact Cards

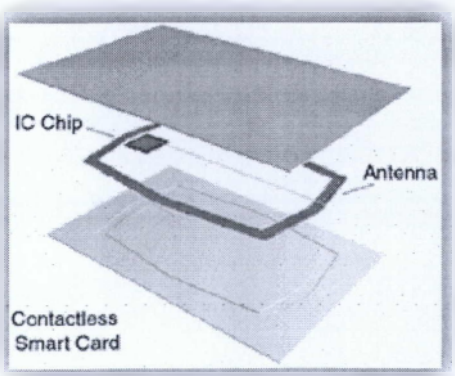
[1] http://www.ebusinessforum.gr/old/content/ downloads/smart_all.pdf

Η επαφή C1 ισοδυναμεί στη Vcc. Η Vcc ενέχει την τάση τροφοδοσίας που κατά κανόνα είναι 5V. Η επαφή C2 ισοδυναμεί στο Reset. Αυτό αποτελεί την γραμμή σήματος που ωφελεί ώστε να προετοιμάσει την κατάσταση του ολοκληρωμένου κυκλώματος έπειτα από την τροφοδοσία της κάρτας. Η επαφή C3 συσσωματώνεται με το clock– σήμα ρολογιού. Το σήμα του ρολογιού υποδεικνύει τη λογική του ολοκληρωμένου και παράλληλα διαχειρίζεται ως σημείο αναφοράς για τη σειριακή σύνδεση επικοινωνίας. Οι αντίστοιχες επαφές C4 και C8 είναι εκτός λειτουργίας. Η επαφή C5 ισοδυναμεί στη γείωση GND το οποίο ορίζεται ως σημείου μηδενικού και είναι η αφετηρία για την μέτρηση της ροπής τροφοδοσίας. Ενώ, η επαφή C6 ισοδυναμεί με την Vpp. Το Vpp χρησιμεύει στην υψηλή τάση που είναι αναγκαία για να προγραμματιστεί η μνήμη EEPROM. Και η τελευταία επαφή C7 ισοδυναμεί με τη σειριακή θύρα I/O. Αυτή η θύρα διαχειρίζεται για την ανταλλαγή και τη λήψη εντολών και πληροφοριών από την εξωτερική επιφάνεια.

2.3.5 Ασύρματες Έξυπνες Κάρτες - Contactless Cards

Οι ασύρματες έξυπνες κάρτες είναι κάρτες χωρίς ηλεκτρονικές επαφές και είναι τοποθετημένες κοντά σε ένα αναγνώστη-reader. Οι συγκεκριμένες κάρτες και ο reader έχουν εσωτερικά ενσωματωμένη μια κεραία ώστε να έρχονται σε επαφή μέσω αυτού του ασύρματου συνδέσμου. Η ενέργεια που προϋποθέτεται για τη λειτουργία του chip μπορεί να μεταφέρεται μέσω μικροκυματικών συχνοτήτων από την συσκευή ανάγνωσης- card reader στην κάρτα. Ανάλογα με τι συχνότητα εκπέμπονται τα ηλεκτρομαγνητικά κύματα, η απόσταση ανάμεσα στην κάρτα και στον reader μπορεί να αυξομειωθεί από μερικά εκατοστά όταν πρόκειται για μετάδοση σε υψηλές συχνότητες έως ένα μέτρο όταν αφορά για μετάδοση σε χαμηλές συχνότητες. Αυτές οι κάρτες ενεργοποιούνται κυρίως σε εφαρμογές και χώρους όπου οι συναλλαγές επιβάλλεται να εκτελούνται γρήγορα, π.χ. τα μέσα συγκοινωνίας, τους σταθμούς διοδίων κ.α. Σε αντίθεση με τις έξυπνες κάρτες των ηλεκτρονικών επαφών , οι ασύρματες κάρτες είναι πιο ακριβές αλλά έχουν μεγαλύτερη διάρκεια ζωής και είναι πιο αξιόπιστες.

Στην παρακάτω εικόνα παρουσιάζεται η δομή της έξυπνης κάρτας χωρίς ηλεκτρονικές επαφές. Παρατηρούμε ότι υπάρχουν τρία στρώματα που στοιχειοθετούν μία ασύρματη κάρτα. Τα εξωτερικά στρώματα, το πάνω και το κάτω στρώμα, κλείνουν εσωτερικά το επίπεδο με την κεραία και το μικροτσίπ. Η κεραία είναι κατά κανόνα τρεις με πέντε στροφές από πολύ λεπτό σύρμα ή αγώγιμο μελάνι που συνδέεται με το μικροτσίπ.

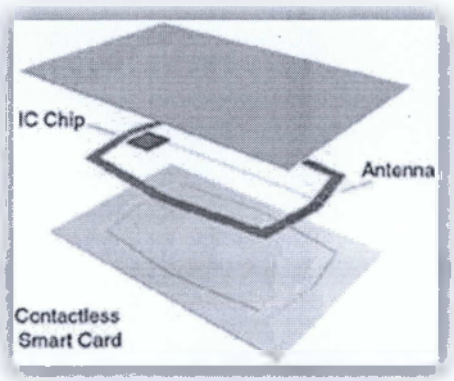


Εικόνα 4: Η δομή της ασύρματης κάρτας

2.3.6 Υβριδικές & Συνδυασμένες κάρτες- Hybrid & Combination Cards

Σύμφωνα από τις προηγούμενες κατηγορίες καρτών που καθορίστηκαν ως προς τον τύπο του interface τους , προέκυψαν δύο επιπρόσθετοι τύποι. Ο πρώτος τύπος είναι οι υβριδικές κάρτες- hybrid cards και ο δεύτερος τύπος είναι οι συνδυασμένες κάρτες-combination cards. Έτσι, οι κάρτες αυτές εμπεριέχουν και τους δύο τρόπους μετάδοσης και επομένως, μπορούν να επικοινωνήσουν είτε με ενσύρματο τρόπο είτε με ασύρματο τρόπο.

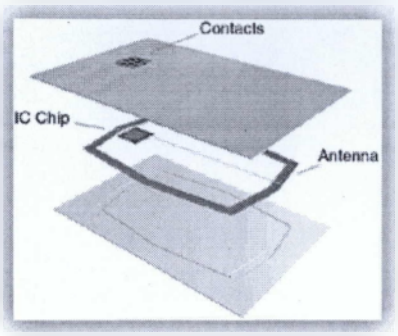
Οι υβριδικές κάρτες έχουν δύο chip, ένα με επαφές και ένα για ασύρματη επικοινωνία. Τα δύο αυτά κυκλώματα συνήθως δεν επικοινωνούν μεταξύ τους. Υφίστανται σε πολλές εφαρμογές και ο συγκεκριμένος τύπος καρτών διευκολύνει την εξυπηρέτηση τόσο στους καταναλωτές όσο και σε αυτούς που κατέχουν την κάρτα. Παρακάτω παρουσιάζεται τα μέρη που συνίσταται μία υβριδική κάρτα.



Εικόνα 5: Υβριδική Κάρτα

Από την άλλη πλευρά, οι συνδυαστικές κάρτες έχουν ενσωματωμένο ένα ολοκληρωμένο κύκλωμα. Ήτοι, μπορεί να υπάρχει πρόσβαση στο ίδιο μικροτσίπ μέσω 4ηλεκτρικών επαφών (επιφάνεια κάρτας) αλλά και μέσω ασύρματης επικοινωνίας (χρήση κεραίας). Με αυτό τον τρόπο μπορεί να καθιστάει δυνατή τη χρήση της σε μια υπεραφθονία εφαρμογών διαφορετικού τύπου. Επιπλέον, αυτές παρέχουν ένα υψηλό επίπεδο ασφαλείας .Οι συνδυαστικές σε αντίθεση με τις υβριδικές κάρτες είναι πιο

φτηνές. Παρακάτω παρουσιάζεται τα μέρη που συγκροτούνται μια συνδυαστική κάρτα.

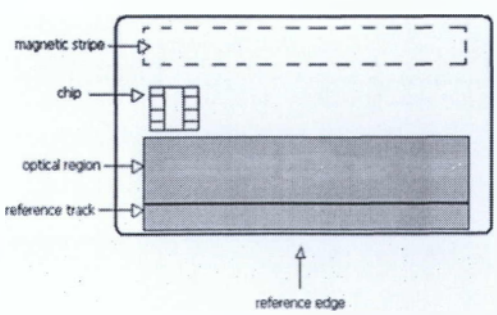


Εικόνα 6: Συνδυαστική κάρτα

2.3.7 Οπτικές Έξυπνες Κάρτες Μνήμης – Optical Smart Cards

Οι οπτικές έξυπνες κάρτες χρησιμοποιούνται για εγγραφή και ανάγνωση δεδομένων με οπτικές μεθόδους .Όμως οι εγγραφές γίνονται μία φορά και δεν μπορούν να διαγράφουν. Η μνήμη των συγκεκριμένων καρτών είναι αρκετή ώστε να αποθηκεύει ένα μεγάλο ποσό από megabytes δεδομένα. Εκτός από την έλλειψη δυνατότητας επανεγγραφής στην οπτική περιοχή, μείον θεωρείται επίσης το υψηλό κόστος.

"Το πρότυπο ISO/IEC 11 693-94 καθορίζει τις διαστάσεις και τα φυσικά χαρακτηριστικά των οπτικών καρτών, καθώς και την τεχνική εγγραφής δεδομένων. Ο συνδυασμός της υψηλής αποθηκευτικής ικανότητας των οπτικών καρτών με την ευφυΐα των έξυπνων καρτών έχει ως αποτέλεσμα νέα ενδιαφέροντα χαρακτηριστικά." Στην παρακάτω εικόνα βλέπουμε την δομή μιας οπτικής έξυπνης κάρτας.[2]



[2] nefeli.lib.teicrete.gr/browse2/stef/thl/2004/Kapetanakis/attached-document/2004Kapetanakis.pdf

Εικόνα 7: Οπτική έξυπνη κάρτα

2.3.8 Έξυπνες Κάρτες Υποδομής Δημόσιου Κλειδιού (PKI Cards)

Οι έξυπνες κάρτες υποδομής δημόσιου κλειδιού (PKI cards) παρέχουν έναν μικροεπεξεργαστή. Επιπλέον, αυτές συγκαταλέγουν και ένα συνεπεξεργαστή ώστε να υλοποιούνται οι κρυπτογραφικές λειτουργίες. Στις κρυπτογραφικές λειτουργίες περικλείονται τα εξής:

- **Δημιουργία ζεύγους RSA κλειδιών** (μήκος: 512-1024 bit)
- **Δημιουργία και επαλήθευση ψηφιακών υπογραφών**
- **Κρυπτογράφηση και αποκρυπτογράφηση**
- **Καθορισμός πολιτικής χρήσης ζεύγους κλειδιών**

2.4 Συσκευές αποδοχής έξυπνων καρτών

Για να επικοινωνήσει ένας χρήστης με τις έξυπνες κάρτες είναι απαραίτητο να υπάρχουν οι συσκευές αποδοχής των έξυπνων καρτών οι οποίες ονομάζονται CADs από τις λέξεις Card Acceptance Devices . Οι συσκευές αυτές είναι ταξινομημένες σε δύο βασικά κριτήρια: τερματικές συσκευές και Αναγνώστες-εγγραφείς έξυπνων καρτών.

Οι τερματικές συσκευές έχουν όλες τις απαραίτητες συσκευές για την επικοινωνία με την κάρτα όπως είναι το πληκτρολόγιο, εκτυπωτή, οθόνη , κτλ. (EFT/POS, κινητά τηλέφωνα, καρτοτηλέφωνα, αυτόματοι πωλητές και αποκωδικοποιητές). Ομού, οι αναγνώστες- εγγραφείς έξυπνων καρτών είναι οι συσκευές που συνδέονται απευθείας σε τερματικές συσκευές που δεν έχουν αναγνώστη έξυπνων καρτών (Η/Υ, info kiosks, controllers). Με άλλα λόγια οι εγγραφείς των έξυπνων καρτών εμπεριέχουν διάφορες ποικιλίες σχετικά με τον μηχανισμό εισαγωγής / εξαγωγής της κάρτας, το είδος των επαφών καθώς και την παρουσία οθόνων και πληκτρολογίων για εισαγωγή κωδικών. Οι λειτουργίες των αναγνωστών ορίζονται από το ISO/IEC 7816-3.

2.5 Τεχνικά χαρακτηριστικά έξυπνων καρτών

2.5.1 Διαστάσεις

Οι διαστάσεις των έξυπνων καρτών έχουν προσδιοριστεί σύμφωνα με το πρότυπο ISO 7810. Έχουν τυποποιηθεί σε τρεις διαφορετικές μορφές οι οποίες είναι οι εξής: 1) ID-1 , 2) ID-000 , 3) ID-00

ID-1:

Οι διαστάσεις της συγκεκριμένης κάρτας έχει τα εξής χαρακτηριστικά:

- Μήκος: 85,6 mm
- Πλάτος: 54 mm
- Πάχος: 0,76 mm με απόκλιση 0,08 mm
- Γωνιακή ακτίνα: 3,18 mm με απόκλιση 0,30 mm

ID-000:

Η συγκεκριμένη κάρτα έχει τη μορφή της κάρτας SIM και χρησιμοποιείται για τηλεφωνικές συσκευές. Οι διαστάσεις της έχει τα εξής χαρακτηριστικά:

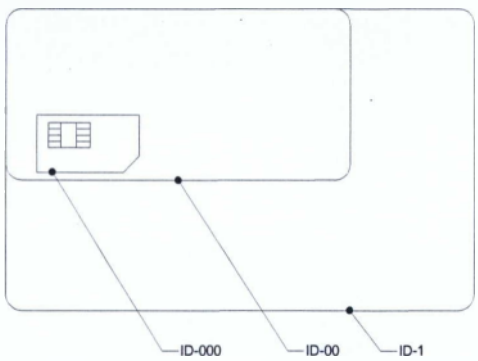
- Μήκος: 25 mm
- Πλάτος 15 mm
- Πάχος: 0,76 mm με απόκλιση 0,08 mm
- Γωνιακή ακτίνα: 3mm με απόκλιση 0,03 mm

ID-00:

Οι διαστάσεις της έχει τα εξής γνωρίσματα:

- Μήκος: 66 mm
- Πλάτος: 33 mm
- Πάχος: 0,76 mm με απόκλιση 0,08 mm
- Γωνιακή Ακτίνα: 3,18 mm με απόκλιση 0,03 mm

Στο παρακάτω σχήμα επιδεικνύονται τα μεγέθη κάθε κάρτας.



Εικόνα 8: Μεγέθη κάθε κάρτας

2.5.2 Τύποι ηλεκτρονικών επαφών

Οι ηλεκτρονικές επαφές βρίσκονται στο σημείο το οποίο περιβάλλεται από μέταλλο και εντοπίζεται στην επιφάνεια. Αυτές θεωρούνται το μέσο επικοινωνίας του

μικροεπεξεργαστή της κάρτας με τη συσκευή ανάγνωσης. Το μεταλλικό εξωτερικό περίβλημα μπορεί να εμπεριέχει έξι ή οχτώ επαφές αλλά αυτό εξαρτάται κυρίως από το μέγεθος του ολοκληρωμένου κυκλώματος που μεταχειρίζεται. Δηλαδή αν τα κυκλώματα έχουν μέγεθος μέχρι 5mm2 τότε επιτρέπεται να χρησιμοποιηθούν οι μεταλλικές πλάκες των έξι επαφών, διαφορετικά χρησιμοποιούνται οι μεταλλικές πλάκες των όχτων επαφών.

Η λειτουργία κάθε ηλεκτρικής επαφής καθορίζεται από τα πρότυπα ISO/IEC 7816-2 , ISO/IEC 7816-3 και GSM 1111. Με το ISO/IEC 7816-2, οι έξυπνες κάρτες περιέχουν οχτώ ηλεκτρικές επαφές. Οι οχτώ ηλεκτρικές επαφές καλούνται C1, C2, C3,…,C8 πλην τις C4 και C8 οι οποίες θα ανεξαρτητοποιηθούν στο μέλλον. Στη συνέχεια αναλύεται σε πίνακα η διευκρίνιση της ιδιότητας κάθε επαφής.

	Περιγραφή	
C1	Vcc	**Τροφοδοσία , συνήθως με τιμή 5 ± 0,5 Volt**
C2	RST	**Είσοδος επαναφοράς (Reset input)**
C3	CLK	**Είσοδος ρολογιού (Clock input)**
C4	RFU	**Δεσμευμένη για μελλοντική χρήση**
C5	GND	**Γείωση (Ground)**
C6	Vpp	**Τάση προγραμματισμού (δεν χρησιμοποιείται πια). Σε παλαιότερες κάρτες χρησιμοποιούνταν για να σβήνει και να προγραμματίζει τη μνήμη EEPROM.**
C7	I/O	**Σειριακή είσοδος/ έξοδος**
C8	RFU	**Δεσμευμένη για μελλοντική χρήση**

Πίνακας 3: Οι ιδιότητες των επαφών

2.5.2.1 API-Application Programming Interface

Το API είναι η συντομογραφία των λέξεων Application Programming Interface (API) και δηλώνει τη Διεπαφή ή τη Διασύνδεση Προγραμματισμού εφαρμογών. Η ιδιότητα του είναι ένα πρόγραμμα λογισμικού που διερμηνεύει τις εντολές και τις λειτουργίες μίας εφαρμογής σε ειδική γλώσσα την οποία συλλαμβάνει μια έξυπνη κάρτα ή cards reader (αναγνώστης καρτών). Παράλληλα, στοχεύει και στην επικοινωνία ανάμεσα σε μια συσκευή ανάγνωσης-υποδοχής καρτών και σε διάφορες μορφές καρτών. Αυτό ευνοεί τις μεγάλες εφαρμογές που συνεργάζονται με διάφορους εκδότες έξυπνων καρτών και είναι αναγκαίο μία κοινή βάση επικοινωνίας. Τέλος, δεν έχει σχεδιαστεί για να καθορίζει την επικοινωνία μίας εφαρμογής με όλα τα είδη καρτών αλλά μπορεί να παρέχει μια συμβατότητα της εφαρμογής με αρκετά διαφορετικά COS καρτών.

ΚΕΦΑΛΑΙΟ 3 ΚΑΘΗΜΕΡΙΝΗ ΧΡΗΣΗ ΕΦΑΡΜΟΓΩΝ

3.1 Εισαγωγή

Οι έξυπνες κάρτες είναι πρακτικά ένας φορητός υπολογιστής με αυξημένα χαρακτηριστικά ασφάλειας σε φυσικό επίπεδο. Η ραγδαία ανάπτυξη της τεχνολογίας τα τελευταία χρόνια έχει ως αποτέλεσμα να παρέχει χαρακτηριστικά επεξεργασίας στις έξυπνες κάρτες που ήταν διαθέσιμα στους πρώτους προσωπικούς υπολογιστές. Παρακάτω αναφέρουμε μερικές εφαρμογές όπου μεταχειρίζονται οι έξυπνες κάρτες για να γίνει πιο κατανοητή αξία και η χρησιμότητα τους.

3.1.1 Ηλεκτρονικό πορτοφόλι ή E-Wallet

Καθημερινά κάνουμε διάφορες συναλλαγές μέσω των μετρητών ή τραπεζικών καρτών ή επιταγών ή ακόμη μέσω του ηλεκτρονικού πορτοφόλι. Το ηλεκτρονικό πορτοφόλι ή ewallet είναι μία «έξυπνη» κάρτα που αντικαθιστά τα μετρητά και χρησιμοποιείται για συναλλαγές μικρού ύψους χρημάτων στο διαδίκτυο. Για να λειτουργήσει ένα ηλεκτρονικό πορτοφόλι πρέπει ο κάτοχος του να μεταφέρει ένα ποσό από κάποια πιστωτική κάρτα στο ηλεκτρονικό πορτοφόλι και έτσι να αρχίζει να πραγματοποιεί συναλλαγές χωρίς να είναι απαραίτητη χρήση κωδικού-PINβ π.χ. στα μέσα μαζικής μεταφοράς , σε χώρους στάθμευσης. Όταν εξαντληθούν τα χρήματα από την κάρτα , επαναλαμβάνει την ίδια διαδικασία. Ομού, μπορεί να ενσωματωθεί στην τραπεζική κάρτα του κατόχου και να συνδεθεί απευθείας με τον τραπεζικό λογαριασμό. Η πρώτη τροφοδότηση του ηλεκτρονικού πορτοφολιού γίνεται από την τράπεζα και το ποσό που μεταφέρεται στην κάρτα μειώνεται από τον τραπεζικό λογαριασμό.

Υπάρχουν κάποιοι ορισμένους τύπους καρτών ηλεκτρονικού πορτοφόλι. Αυτοί οι τύποι είναι:

1) **Πρότυπο κάρτα** (Primary Card Standard Card): Εκδόθηκε απροσδιόριστα, χωρίς ισορροπία και ο αριθμός Sri elementary (0000) δεν είναι έγκυρη για οποιαδήποτε εφαρμογή , εκτός αν έχει αλλάξει από το σημείο πώλησης ή από το ATM.

2) **Ασημένια κάρτα** (Silver Card): Ζητάει από την τράπεζα προς όφελος ενός συγκεκριμένου προορισμού με βάση την αποστολή να αποκαλύψει τα ονόματα των πελατών τους που θέλουν να εκδίδουν κάρτες και οι κάρτες που έχουν εκδοθεί για τη διασφάλιση του θεσμού. Παράλληλα, εκδίδεται με εξατομικευμένο όνομα του πελάτη και ο πρώτος αριθμός είναι η σειρά 0000 που είναι υποχρεωμένη να το αλλάξει ο ιδιοκτήτης της κάρτας πριν κάνει οποιαδήποτε

συναλλαγή. Η κάρτα χρησιμοποιείται για να πληρώσει τους μισθούς, την υποστήριξη των φοιτητών, η καταβολή των ασφαλίστρων μικρό- χρηματοδοτήσεων και άλλα πολλά.

3) **Χρυσή κάρτα (Gold Card):** Η κάρτα εκδίδεται και εξατομικευμένο με το όνομα του πελάτη και ο πρώτος αριθμός είναι η σειρά 000 και είναι υποχρεωμένη να το αλλάξει ο ιδιοκτήτης πριν κάνει οποιαδήποτε συναλλαγή. Η οροφή της κάρτας είναι ανοιχτό. Η οροφή της απόσυρσης των 1000C σε ένα χρόνο, το ανώτατο όριο της οροφής εφιστά 10000C ανά ημέρα

3.1.2 Τηλεπικοινωνίες : το σύστημα GSM

Ο όρος GSM προέρχεται από τις Αγγλικές λέξεις Global System for Mobile communications που μεταφράζεται στα Ελληνικά ως Παγκόσμιο Σύστημα Κινητών Επικοινωνιών. Το 1982, το Ευρωπαϊκό Τηλεπικοινωνιακό Συμβούλιο ξεκίνησε την μελέτη για την δημιουργία ενός ψηφιακού συστήματος κινητής τηλεφωνία δεύτερης γενιάς 2G ή GSM από Group Special Mobile. Το σύστημα GSM είναι ένα κυψελοειδές ψηφιακό σύστημα κινητής τηλεφωνίας δεύτερης γενιάς 2G ,το οποίο περιλαμβάνει ηλεκτρομαγνητικά σήματα και την τεχνική πολλαπλής πρόσβασης με διαχωρισμό του διαθέσιμου φάσματος συχνοτήτων σε ένα αριθμό καναλιών και την διαίρεση αυτών σε χρονοθυρίδες για την μετάδοση σημάτων.

Το 1989 , το Ευρωπαϊκό Τηλεπικοινωνιακό Ινστιτούτο Προτύπων ETSI ανέλαβε την ευθύνη για την δημιουργία του συγκεκριμένου συστήματος και το 1990, γνωστοποιούν το πρότυπο και τα χαρακτηριστικά του 2G. Ενώ το 1991, εμφανίστηκε στην Ευρωπαϊκή αγορά και αντίστοιχα στην Ελλάδα χρησιμοποιήθηκε το 1993 από την εταιρία WIND Hellas.

Στην κινητή τηλεφωνία GSM περιλαμβάνονται οι έξυπνες κάρτες οι οποίες είναι γνωστές ως κάρτες SIM. Οι κάρτες SIM προέρχονται από τις αγγλικές λέξεις Security Identity Module και συγκαταλέγει πληροφορίες ασφάλειας και συνδρομητικά στοιχεία. Εισάγεται στη συσκευή ή βρίσκεται ενσωματωμένη σε αυτή. Από τη στιγμή που θα ενεργοποιηθεί η κάρτα SIM , το τηλέφωνο προσωποποιείται ως προς το χρήστη και φορτώνει στοιχεία όπως το νούμερο του στο δίκτυο, πληροφορίες κοστολόγησης , πρόσφατους κληθέντες αριθμούς. Επίσης, η συγκεκριμένη κάρτα μπορεί να μεταφέρεται σε διαφορετική συσκευή αφού περιλαμβάνει τα στοιχεία του συνδρομητή και παράλληλα, προστατεύονται από ένα ειδικό κωδικό γνωστό ως PIN.

3.1.3 Κάρτες διατηρησιμότητας & εξυπηρέτησης πελατών- loyalty cards

Μέσα από διάφορες επιχειρήσεις του λιανικού εμπορίου πραγματοποιείται η χρήση των έξυπνων καρτών ή πιο συγκεκριμένα από τις κάρτες διατηρησιμότητας και εξυπηρέτησης πελατών ή Loyalty cards με κύριο σκοπό να εξυπηρετούν αποτελεσματικά τους καταναλωτές τους και να τους κρατούν πιστούς. Για παράδειγμα , οι πελάτες , έχοντας δείξει την κάρτα. κερδίζουν κάποιους βαθμούς με την αγορά κάποια αγαθών ή υπηρεσιών. Φτάνοντας σε ένα συγκεκριμένο όριο πόντων, οι πελάτες επιβραβεύονται με διάφορα δώρα εξαργυρώνοντας έτσι τους πόντους τους. Έτσι, με την χρήση των έξυπνων καρτών που οι πόντοι αποθηκεύονται μέσα στο chip , παρέχουν δυο βασικά πλεονεκτήματα:

- Δεν απαιτείται να υπάρχει δίκτυο μεταξύ των καταστημάτων για να ενημερώνεται η κεντρική βάση με τους πόντους του καταναλωτή. Επί πρόσθετα, επικροτείται άμεσα με την επίτευξη ορίου πόντων και έτσι του χορηγείται το κίνητρο στον πελάτη να κάνει περισσότερες αγορές
- Οι επιχειρήσεις μπορούν να υλοποιήσουν προγράμματα Loyalty πάνω από το διαδίκτυο με την προϋπόθεση ότι η έξυπνη κάρτα θα είναι το κεντρικό ασφαλές μέσο για την αποθήκευση των μονάδων παροχών.

Άρα, με τη χρήση των καρτών διατηρησιμότητας και εξυπηρέτησης πελατών κρατούν πιστούς τους καταναλωτές αλλά παράλληλα ενημερώνονται για τις καταναλωτικές τους συνήθεις λόγω της στρατηγικής marketing και πωλήσεων που ακολουθούν αλλά και την αποτελεσματικότερη εξυπηρέτηση πελατών.

3.1.4 Έλεγχος φυσικής και λογικής πρόσβασης

3.1.4.1 Έλεγχος πρόσβασης σε κτίρια

Μια έξυπνη κάρτα μπορεί να χρησιμοποιηθεί για τον έλεγχο πρόσβασης κτιρίων. Πιο αναλυτικά, η συγκεκριμένη κάρτα καταγράφει τα στοιχεία αναγνώρισης ενός ατόμου για τον έλεγχο πρόσβασης σε κτίρια υψηλής και μη ασφάλειας όπως είναι για παράδειγμα τα πανεπιστήμια ή οι βιβλιοθήκες.

Σε περιπτώσεις , που είναι αναγκαία η υψηλή ασφάλεια και πρόσβαση σε συγκεκριμένες υπηρεσίες ή πληροφορίες τότε η έξυπνη κάρτα μπορεί να λειτουργήσει ως μια συσκευή που αποθηκεύει πληροφορίες όπως η εικόνα ή τα βιομετρικά χαρακτηριστικά του χρήστη δηλαδή τα δακτυλικά αποτυπώματα. Στην συνέχεια διαφυλάσσει τα δεδομένα ώστε να πραγματοποιηθεί η ταυτοποίηση του ατόμου μέσα από τα υπολογιστικά συστήματα του οργανισμού.

"Παράδειγμα αποτελεί η Mcard , που χρησιμοποιείται από 110.000 μέλη του πανεπιστημίου του Michigan και σε αυτή υπάρχουν πληροφορίες για την ταυτότητα του κάθε φοιτητή και μπορεί να χρησιμοποιηθεί για χρηματοοικονομικές συναλλαγές , για αγορά φαγητού ή βιβλίων, για φωτοαντίγραφα, και άλλες συναλλαγές".[3]

3.1.4.2 Βιομετρικές κάρτες:

Νέα μέθοδος ταυτοποίησης με βιομετρικά στοιχεία και χαρακτηριστικά τα οποία θα είναι αποθηκευμένα σ' ένα είδος κάρτας. Η βιομετρική κάρτα θα περιλαμβάνει όλα τα βασικά χαρακτηριστικά ενός ατόμου και θα χρησιμοποιείται ως ηλεκτρονική ταυτότητα .

Η συγκεκριμένη μέθοδος υλοποιείται σε διάφορες εφαρμογές που σχετίζονται με :

1. "Έλεγχο πρόσβασης σε φυσικούς χώρους
2. Ασφάλεια χρήσης λογισμικών, ταυτοποίηση χρηστών
3. Συνοριακό έλεγχο. Έκδοση βιομετρικών διαβατηρίων
4. Καταγραφή χρόνου εργασίας προσωπικού εταιριών
5. Μηχανές αναζήτησης που επιβεβαιώνουν αντικείμενα από φωτογραφίες
6. Εγκληματολογία για τον εντοπισμό δραστών
7. Εφαρμογές διαδικτύου όπως η ηλεκτρονική τράπεζα"[4]

Η βιομετρική κάρτα έχει την δυνατότητα να αποθηκεύει μια βιομετρική φόρμα δηλαδή την ψηφιακή αναπαράσταση ενός ανθρώπινου βιομετρικού χαρακτηριστικού εφόσον ή μνήμη της κάρτας φτάνει στα 32K. Περιλαμβάνει ένα βιομετρικό αποτύπωμα του χρήστη σε κωδικοποιημένη μορφή στη μνήμη. Η σύγκριση ανάμεσα στο αποτύπωμα του ατόμου και στο αποτύπωμα που περικλείει η κάρτα πραγματοποιείται σε ολοκληρωμένες συσκευές που συγκαταλέγουν σαρωτή και αναγνώστη κάρτας . Έτσι, ευδοκιμεί τον ασφαλέστερο τρόπο ώστε να μην υπάρξει κίνδυνος να υποκλαπεί το βιομετρικό αποτύπωμα.

3.1.4.3 Πρόσβαση σε δίκτυα υπολογιστών και εφαρμογές

Οι έξυπνες κάρτες μπορούν να χρησιμοποιηθούν σε οποιοδήποτε τύπο δικτύου ανταλλαγής ηλεκτρονικών δεδομένων. Έχουν τη δυνατότητα να αποθηκεύουν ψη-

[3] http://www.ebusinessforum.gr/old/content/downloads/smart_all.pdf
[4] http://www.dpa.gr/portal/page?_pageid=33,131221&_schema=PORTAL

φιακά πιστοποιητικά γνωστά ως digital certificates και άλλες πληροφορίες με κύριο σκοπό τον έλεγχο του δικαιώματος πρόσβασης του χρήστη. Με αυτό τον τρόπο, ο χρήστης θα μεταχειρίζεται τα υπολογιστικά και δικτυακά συστήματα μ' έναν ασφαλή τρόπο. Η ασφάλεια εδώ εκθέτεται τόσο στην πιστοποίηση της ταυτότητας του χρήστη όσο και στη δημιουργία ιδιωτικών εικονικών δικτύων VPN ώστε να υπάρξει πρόσβαση εταιρικών συστημάτων μέσα από τα δημόσια δίκτυα όπως είναι διαδίκτυο-Internet.

3.1.5 Υγεία και ασφάλιση

Ένας άλλος τομέας που μπορούν να εφαρμοστούν οι έξυπνες κάρτες είναι η υγεία και ασφάλιση. Οι ιατρικές έξυπνες κάρτες προσφέρουν μια νέα οπτική στις εφαρμογές υγείας. , Αυτές μπορούν να διαχειριστούν για την ασφαλή αποθήκευση στοιχείων ταυτότητας, ασφάλισης και ιατρικών δεδομένων του ασθενούς και για την αποθήκευση των σημείων όπου βρίσκονται στοιχεία ιατρικού φακέλου pointer cards. Αυτό έχει ως αποτέλεσμα, οι πληροφορίες να είναι διαθέσιμες έγκυρες και έγκαιρες στους ασθενείς και στους γιατρούς και διευκολύνεται η ελεύθερη διακίνηση των ασθενών που μπορούν να ταξιδεύουν στο εσωτερικό και στο εξωτερικό έχοντας μαζί τους τον ασφαλιστικό και ιατρικό τους φάκελο.

Υπάρχουν επιπλέον χρήσεις των έξυπνων καρτών στον τομέα της υγείας οι οποίες είναι:

- Ταυτοποίηση ασθενούς και επαγγελματιών υγείας
- Ηλεκτρονικές υπογραφές για την ακεραιότητα και την αυθεντικότητα ιατρικών δεδομένων
- Κρυπτογράφηση δεδομένων
- Ασφαλή πρόσβαση σε δίκτυα υγείας

3.1.6 Τραπεζικές συναλλαγές

Οι έξυπνες κάρτες χρησιμοποιούνται στις τραπεζικές συναλλαγές καθώς έχουν σημαντικά πλεονεκτήματα έναντι των καρτών με μαγνητική λωρίδα.

OI FMV κάρτες θα υποκαταστήσουν τις πιστωτικές και χρεωστικές κάρτες με μαγνητική λωρίδα, ενώ θα μπορούν να υποστηρίζουν και επιπλέον εφαρμογές. Επί πρόσθετα , έχουν την δυνατότητα να πραγματοποιούν συναλλαγές εξ' αποστάσεως με τη χρήση ηλεκτρονικών πιστοποιητικών για την πιστοποίηση της ταυτότητας του χρήστη.

3.1.7 Άλλες εφαρμογές

Οι έξυπνες κάρτες μπορούν να χρησιμοποιηθούν και σε άλλες εφαρμογές όπως είναι :

- Χρήση σε αποκωδικοποιητές
- Πρόσβαση στο διαδίκτυο – Internet Access
- Product tracking
- Δίπλωμα οδήγησης

Παρακάτω βλέπουμε ένα συνοπτικό πίνακα με γνωστές και πιθανές εφαρμογές έξυπνων καρτών ταξινομημένα κατά τομέα και τύπο κάρτας:

	Κάρτα προπληρωμένης αξίας	**Κάρτα αποθήκευσης αρχείων και πληροφοριών**	**Κάρτα ελέγχου πρόσβασης & ασφάλειας**	**Κάρτα μέλους**
Τραπεζικός τομέας	• Ηλεκτρονικό πορτοφόλι • Τραπεζικές συναλλαγές • Ηλεκτρονικές πληρωμές • Ασφαλιστική αίτηση		• Πρόσβαση σε συγκεκριμένο λογαριασμό • Ασφάλεια χρησιμοποιώντας το Διαδίκτυο από το σπίτι	• Πιστωτικές κάρτες • Χρεωστικές κάρτες
Τηλεπικοινωνίες	• Προπληρωμένη τηλεκάρτα		• Κάρτες SIM	
Δημόσιος τομέας	• Διαχείριση λογαριασμών (συντάξεις, επιδόματα κλπ)		• Διαβατήριο • Ταυτότητα • Δίπλωμα οδήγησης	
Μεταφορές	• Ηλεκτρονικά εισιτήρια • Αυτόματη πληρωμή διοδίων		• Κάρτα επιβίβασης	• Κάρτες υγείας
Υγεία	• Πληρωμές ασφαλείας • Ιατρικές πληρωμές	• Αποθήκευση/ ανάκτηση ιατρικού ιστορικού • Αποθήκευση πληροφοριών δότη		
Λοιπά	• Κρατήσεις ξενοδοχείων • Πληρωμές μισθοδοσίας προσωπικού	• Πληροφορίες /ιστορικό Προσωπικού • Ακαδημαϊκές πληροφορίες • Αποθήκευση προσωπικής πληροφορίας • Αρχεία ενοικίασης αυτοκινήτων	• Πρόσβαση σε αίθουσες αναχώρησης αεροδρομίου • Κλειδιά δωματίων σε ξενοδοχείο • Πρόσβαση σε κτίρια • Πρόσβαση σε δίκτυα	• Προγράμματα και εξυπηρέτησης πελατών

		• Προσωπικό προφίλ (π.χ. προτιμήσεις για το πρόγραμμα εξυπηρέτησης πελατών)	• Κλειδιά ενοικίασης αυτοκινήτου	

Πίνακας 4: Πλεονεκτήματα Εφαρμογών

3.1.8 Πλεονεκτήματα εφαρμογών

Βασικό γνώρισμα που προσδιορίζουν τις έξυπνες κάρτες είναι η ασφάλεια. Έτσι, δίνεται η δυνατότητα να πραγματοποιηθούν πολλές εφαρμογές παρέχοντας μια αλληλουχία προτερημάτων τόσο στις επιχειρήσεις όσο και στους πελάτες της επιχείρησης. Δηλαδή στις επιχειρήσεις παρέχεται ο περιορισμός οικονομικού εγκλήματος και αποδοτικότητα και αποτελεσματικότητα πωλήσεων , ενώ στον πελάτη του προσφέρουν μεγαλύτερη ασφάλεια , η χρήση μιας έξυπνης κάρτας πολλαπλών εφαρμογών του προσφέρει ευκολία, του επιτρέπει την συμμετοχή σε προγράμματα rewards και loyalty και του επιτρέπει αποθήκευση και πρόσβαση σε απαραίτητες πληροφορίες,

Οι κάρτες μνήμης έχουν τρία βασικά προτερήματα τα οποία είναι τα εξής: (α) έχουν χαμηλό κόστος, (β) δεν προγραμματίζονται και (γ) έχουν συνήθως προπληρωμένη αξία ή περιορισμένη δυνατότητα προσθαφαίρεσης πόντων. Ενώ οι έξυπνες κάρτες είναι πιο ακριβές αλλά:

- Αντέχουν σε κακόβουλους λογισμικούς (ηλεκτρονικοί ιοί)
- Εντοπίζουν και αντιμετωπίζουν τους κακόβουλους λογισμικούς
- Επαναλαμβάνουν τον προγραμματισμό
- Κάνουν υπολογισμούς και πράξεις
- Εμπεριέχουν κυκλώματα λογικής και μνήμης
- Έχουν τη δυνατότητα να επεξεργάζονται δεδομένα και να αποθηκεύουν πληροφορίες
- Έχουν την ευχέρεια να συγκρίνουν και να διαχειρίζονται σύνθετα δεδομένα
- Ενεργοποιούνται για εφαρμογές μεγάλης ασφάλειας
- Εγκρίνουν off- line επαλήθευση των στοιχείων
- Επιλέγουν ποια στοιχεία της κάρτας είναι αποδεκτές από τις εφαρμογές
- Παρέχουν υψηλή ασφάλεια εξαιτίας των πολύπλοκων κρυπτογραφικών τεχνικών που εφαρμόζονται για να γίνει η κωδικοποίηση και η αποκωδικοποίηση
- Χορηγούν τεράστιο χώρο αποθήκευσης πληροφοριών
- Είναι συμβατές με φορητές ηλεκτρονικές συσκευές

ΚΕΦΑΛΑΙΟ 4 ΤΕΧΝΟΛΟΓΙΑ JAVA CARD

4.1 Εισαγωγή στην τεχνολογία java card

Η τεχνολογία Java Card κατασκευάστηκε από τη Sun Microsystems και η ιδιότητα της είναι να παρέχει ένα ασφαλές περιβάλλον για εφαρμογές οι οποίες τρέχουν σε έξυπνες κάρτες ή σε άλλες τερματικές συσκευές που έχουν μια καθορισμένη μνήμη και καθορισμένες δυνατότητες επεξεργασίας. Επιπλέον, δίνει τη δυνατότητα σε εφαρμογές που είναι γραμμένες σε γλώσσα Java να λειτουργούν πάνω στις έξυπνες κάρτες.

Ένα από τα πλεονεκτήματα που προσφέρει η τεχνολογία Java Card είναι η διαλειτουργικότητα (Interoperability) δηλαδή οι εφαρμογές που δημιουργούνται σύμφωνα με την συγκεκριμένη τεχνολογία μπορούν να λειτουργούν σε κάρτες που περιλαμβάνουν τη Java Card χωρίς να εξαρτάται από τον κατασκευαστή. Επίσης, ο προγραμματιστής δεν είναι υποχρεωμένος να είναι ενημερωμένος για τα πρωτόκολλα επικοινωνίας και τις τεχνικές διαχείρισης μνήμης που περιλαμβάνει το λειτουργικό σύστημα της κάρτας. Παρακάτω, αναφέρονται συνοπτικά και άλλα προνόμια που έχει η τεχνολογία Java Card τα οποία είναι τα ακόλουθα:

- **Ασφάλεια:** Περιλαμβάνει ένα πολύ ασφαλές περιβάλλον εκτέλεσης και αυτό οφείλεται στη Java.
- **Συμβίωση πολλαπλών εφαρμογών:** Η Java Card εγκρίνει σε μια έξυπνη κάρτα να υπάρχουν διάφορες εφαρμογές. Με αυτή τη διαδικασία μπορεί επίσης να κάνει ένα ορθό έλεγχο ώστε να σταθεροποιηθεί η χρήση της ασφάλειας.
- **Εγκατάσταση εφαρμογών:** Με την εγκατάσταση των εφαρμογών στην κάρτα, η εταιρεία έχει τη δυνατότητα να εγκαθιστά καινούρια Applets ή να εφαρμόζει αντικατάσταση των ήδη υπαρχόντων ανάλογα με τις ανάγκες του χρήστη,
- **Συμβατότητα με τα πρότυπα των έξυπνων καρτών:** Είναι συμβατό με τα διεθνή πρότυπα ISO 7816 , EMV, ETSI και Global Platform
- **Αντικειμενοστραφής Προγραμματισμός:** Δεν είναι ανάγκη ο προγραμματιστής να εξετάζει με διαδικασίες το συγκεκριμένο υλικό όπως η διαχείριση μνήμης. Αυτό έχει ως αποτέλεσμα την μείωση του χρόνου παραγωγής αλλά συνάμα την αύξηση αξιοπιστίας των εφαρμογών.
- **Ανεξαρτησία:** Αυτή δεν είναι εξαρτημένη από την αρχιτεκτονική της κάρτας και του λειτουργικού συστήματος που εφαρμόζονται σε αυτή. Παράλληλα, εγκρίνει τους προγραμματιστές να συντάσσουν κώδικα όπου η γλώσσα με την οποία συνθέτουν πρέπει να είναι υψηλού επιπέδου ώστε να έχει τη δυνατότητα να λειτουργεί σε διάφορες τεχνολογίες έξυπνων καρτών.

Ένα μεγάλο πρόβλημα που υπήρξε για την ανάπτυξη της τεχνολογίας Java Card ήταν η προσαρμογή της τεχνολογίας Java Card στο περιορισμένο υλικό γιατί έπρεπε να έχει κατοχυρωθεί χώρο και για τις εφαρμογές. Η επίλυση του προβλήματος ήταν να περιέχει ένα συγκεκριμένο κομμάτι της γλώσσας Java και ένα μοντέλο εικονικής μηχανής το οποίο έπρεπε να διασπαστεί.

Στη συνέχεια αναφέρονται τα χαρακτηριστικά της Java που υποστηρίζονται από την Java Card αλλά και τα χαρακτηριστικά που δεν υποστηρίζονται από την Java Card. Τα χαρακτηριστικά που υποστηρίζονται είναι τα εξής:

- Μικροί τύποι δεδομένων: Boolean, Byte, Short
- Πίνακες μίας διάστασης
- Πακέτα της Java, κλάσεις, διεπαφές και εξαιρέσεις
- Αντικειμενοστραφή χαρακτηριστικά της Java: virtual methods, overloading και dynamic object creation, access scope και binding rules.
- Η υποστήριξη της λέξης κλειδί int καθώς και η υποστήριξη τύπου integer είναι προαιρετικές

Ενώ, τα χαρακτηριστικά τα οποία δεν υποστηρίζονται είναι τα εξής:

- Μεγάλοι τύποι δεδομένων: long, double, float
- Χαρακτήρες και συμβολοσειρές
- Πολυδιάστατοι πίνακες
- Δυναμικό φόρτωμα κλάσεων
- Security manager
- Garbage collection and finalization
- Threads
- Object serializing
- Object cloning

4.2 Αρχιτεκτονική java card

Η έξυπνη κάρτα είναι μία από τις πιο μικρές υπολογιστικές πλατφόρμες που κυκλοφορούν στην σημερινή εποχή. Ο χώρος της έξυπνης κάρτας περιλαμβάνει μνήμη RAM 1k, μνήμη EEPROM 16k και μνήμη ROM 24k. Το μεγάλο πρόβλημα που δημιουργήθηκε για την ανάπτυξη της τεχνολογίας Java Card ήταν η προσαρμογή της στο περιορισμένο υλικό εξασφαλίζοντας συνάμα και χώρο για τις εφαρμογές. Ο τρόπος με τον οποίο διαχειρίστηκε αυτή η δυσκολία ήταν να εμπεριέχει ένα τμήμα της γλώσσας Java και ένα μοντέλο εικονικής μηχανής που έπρεπε να διασπαστεί.

Μια ιδιότητα που περιλαμβάνει η συγκεκριμένη τεχνολογία είναι ο προσδιορισμός ενός περιβάλλοντος εκτέλεσης-Java Card Runtime Environment (JCRE) ενισχύοντας το σύστημα μνήμης της έξυπνης κάρτας, την επικοινωνία, την ασφάλεια και

το μοντέλο εκτέλεσης εφαρμογών. Το περιβάλλον εκτέλεσης απαρτίζεται από το Java Card Framework &APIs και το Java Card Virtual Machine.

Το Java Card Framework & APIs συγκαταλέγουν κλάσεις και πακέτα που είναι σημαντικά για τον προγραμματισμό μιας έξυπνης κάρτας. Θεωρείται το υψηλότερο επίπεδο και έρχεται σε επαφή με τα Applets. Και στέλνει τις εντολές στην εικονική μηχανή. Ενώ, το Java Card Virtual Machine προσδιορίζει το υποσύνολο της γλώσσας Java, Java card , και της γλώσσας Java Virtual Machine , Java Card Virtual Machine. Απαρτίζεται σε δύο τμήματα. Το πρώτο τμήμα είναι αυτό που λειτουργεί πάνω στην κάρτα on card και το δεύτερο τμήμα είναι εκείνο που λειτουργεί εκτός κάρτας off card. Το φόρτωμα των κλάσεων, ο έλεγχος του κώδικα , η βελτιστοποίηση είναι μία από τις πολλές διαδικασίες που εφαρμόζονται από την εικονική μνήμη της εκτός κάρτας.

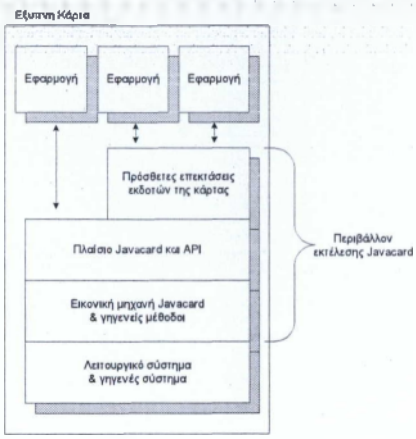
Η πιο σημαντική λειτουργία του είναι ένα σαφές διαχωρισμός ανάμεσα στο λειτουργικό σύστημα της έξυπνης κάρτας και στις εφαρμογές. Δηλαδή, η εικονική μνήμη στο κομμάτι του λειτουργικού συστήματος διαχειρίζεται την πολυπλοκότητα και τις λεπτομέρειες του συστήματος της κάρτας. Ενώ στις εφαρμογές απαιτούνται υπηρεσίες και πόρους συστήματος μέσα από ένα υψηλό επίπεδο διεπαφής.

Σύμφωνα με την πλατφόρμα Java Card, οι εφαρμογές που είναι διατυπωμένες σε γλώσσα Java , μπορούν να εφαρμοστούν είτε στις έξυπνες κάρτες είτε σε άλλες συσκευές αλλά με την προϋπόθεση ότι η μνήμη έχει περιορισμένες δυνατότητες. Η πλατφόρμα διαιρείται σε τρία ακόλουθα μέρη και το καθένα από αυτά ορίζεται σε ένα φύλλο προδιαγραφών:

1. **Εικονική Μηχανή (JCVM):** Προσδιορίζεται το υποσύνολο της Java η οποία περιλαμβάνει την Java Card και μια εικονική μηχανή κατάλληλη για εφαρμογές Java Card.

2. **Περιβάλλον Εκτέλεσης (JCRE):** Αναλύεται η συμπεριφορά του περιβάλλοντος εκτέλεσης και συνυπολογίζεται μέσα σ' αυτόν η διαχείριση μνήμης , η διαχείριση εφαρμογών και άλλα πολλά χαρακτηριστικά του περιβάλλοντος εκτέλεσης.

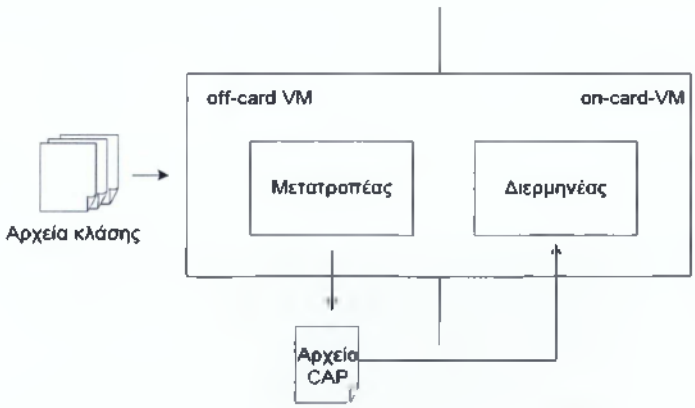
3. **Java Card Applications Programming Interface (JC API):** Αναλύονται τα πακέτα και οι κλάσεις της Java Card για τη δημιουργία εφαρμογών Java Card.



Διάγραμμα 4: Η δομή των έξυπνων καρτών

4.2.1 Java card virtual machine – η εικονική μηχανή java card

Η κύρια διαφορά που κάνει την εικονική μηχανή Java Card να ξεχωρίζει από την εικονική μηχανή Java είναι ότι η πρώτη εφαρμόζεται σε δύο ξεχωριστά τμήματα. Ο ένας κλάδος της JVCM που εντοπίζεται πάνω στην κάρτα (on card) περιλαμβάνει ένα διερμηνέα (Interpreter) που επιτελεί εντολές με μορφή Byte-Code , επαληθεύει τη δέσμευση μνήμης αλλά και τη δημιουργία αντικειμένων. Επίσης, αποτελεί σημαντική βοήθεια για την ασφάλεια για το διάστημα που πραγματοποιείται η εκτέλεση. Και ο άλλος κλάδος της JVCM που εντοπίζεται εκτός κάρτας (off card) είναι ο μετατροπέας (Converter) ο οποίος λειτουργεί στο τερματικό και η ιδιότητα του είναι η επεξεργασία των αρχείων των κλάσεων ώστε να μετατραπούν σε αρχεία CAP (Converted Applet) .Ύστερα, αποθηκεύονται στη έξυπνη κάρτα και εκτελείται από τον διερμηνέα. Παράλληλα ο μετατροπέας συνθέτει ένα αρχείο εξαγωγής όπου συμπεριλαμβάνει τα APIs του τροποποιημένου πακέτου .



Διάγραμμα 5: Η δομή της εικονικής μηχανής

4.2.1.1 Αρχεία converted applet & exports files

Ένα αρχείο CAP περικλείει πληροφορίες για τις κλάσεις της εφαρμογής , για το εκτελέσιμο δυαδικό κώδικα αλλά και πληροφορίες σύνδεσης και επιβεβαίωσης της λειτουργίας. Η ιδιότητα του είναι να κάνει χρήση των συμπιεσμένων δομών δεδομένων και να καθορίζονται τα είδη του δυαδικού κώδικα ώστε να είναι κατάλληλα σχεδιασμένα για τις δυνατότητες της Java Card. Επιπλέον, η μορφή CAP είναι εκείνη η μορφή όπου το λογισμικό φορτώνεται σε μια έξυπνη κάρτα η οποία ενισχύει της πλατφόρμα της Java Card όμως επιτρέπει και την εισαγωγή εφαρμογών της ανεξάρτητα αν είναι πριν ή μετά τη δημιουργία της κάρτας.

Αντίθετα, τα αρχεία εξαγωγής δεν έχουν τη δυνατότητα να φορτώνονται στις έξυπνες κάρτες γι' αυτό το λόγο δεν καθίσταται δυνατή η άμεση χρήση του διερμηνέα. Αυτό που παρέχουν είναι η δημιουργία και η επεξεργασία από τον μετατροπέα για λόγους εξακρίβωσης και σύνδεσης. Επίσης, έχουν τη δυνατότητα να συμπεριλάβουν πληροφορίες που συνδέονται με τις μεθόδους ενός ολόκληρου πακέτου κλάσεων .Πιο συγκεκριμένα , καθορίζουν τα ονόματα των κλάσεων, των μεθόδων και των πεδίων. Αλλά επιπλέον, μπορούν να περιέχουν πληροφορίες για τη σύνδεση πακέτων κλάσεων μέσα στην κάρτα. Τέλος, δεν περιλαμβάνουν γενικά εκτελέσιμο κώδικα και έτσι διανέμεται ελεύθερα από τους προγραμματιστές στους χρήστες της εφαρμογής χωρίς να φανερώνονται οι λεπτομέρειες για την εσωτερική πραγμάτωση της εφαρμογής.

4.2.1.1 Ο μετατροπέας (converter) java card

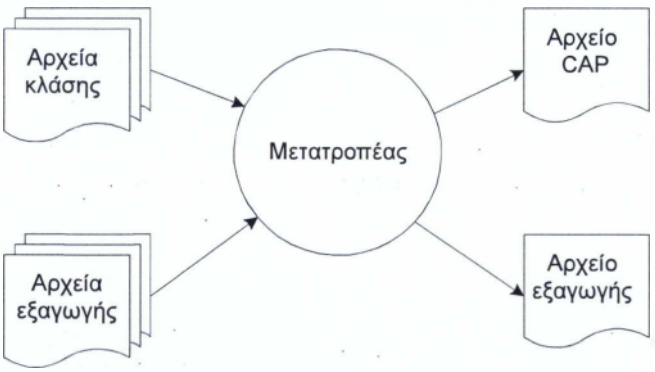
Καταρχάς, για να αρχίσει η εγκατάσταση μιας εφαρμογής πρέπει να μεταγλωττιστεί ο κώδικας λαμβάνοντας σαν έξοδο τα class αρχεία. Ύστερα, ο μετατροπέας επεξεργάζεται όλα τα αρχεία κλάσεων που ανήκουν στο ίδιο πακέτο μετατρέποντας σε ένα αρχείο CAP και μετά το πρόγραμμα της συγκεκριμένης μορφής φορτώνεται στην Java Card.

Στο διάστημα που υλοποιείται η διαδικασία της μετατροπής, ο converter εφαρμόζει τις εξής διεργασίες:

- Εξακριβώνει ότι οι κλάσεις είναι σωστά μορφοποιημένες .
- Ασκεί έλεγχο για παραβίαση του υποσύνολου της γλώσσας Java που χρησιμοποιείται στην Java Card.
- Αρχικοποιεί τις στατικές μεταβλητές.
- Προσδιορίζει με αδιάσπαστη μορφή τις κλάσεις, τις μεθόδους και τα πεδία ώστε να είναι πιο εύκολη η διαχείριση πάνω στην κάρτα.
- Βελτιστοποιεί τον δυαδικό κώδικα.

- Δεσμεύει ένα αποθηκευτικό χώρο και συνθέτει τις δομές δεδομένων της εικονικής μηχανής ώστε να αναπαριστούν οι κλάσεις.

Ο μετατροπέας δέχεται ως είσοδο ένα ή και περισσότερα αρχεία εξαγωγής. Στην έξοδο του δημιουργεί και ένα αρχείο εξαγωγής εκτός από το αρχείο Cap για το πακέτο που μετατρέπεται εκείνη τη στιγμή. Με άλλα λόγια, ο μετατροπέας φορτώνει όλα τα αρχεία των κλάσεων σε ένα πακέτο και αν κάποια κλάση του συγκεκριμένου πακέτου καθιερώσει μια άλλη κλάση ενός άλλου πακέτου τότε ο μετατροπέας παίρνει μια επιπλέον είσοδο και το αρχείο εξαγωγής του πακέτου περιλαμβάνει την εισαγόμενη κλάση.



Διάγραμμα 6: Διαδικασία μετατροπής ενός πακέτου

4.2.1.2 Ο διερμηνέας (interpreter) JAVA CARD

Ο διερμηνέας απαρτίζεται σε ένα τμήμα της εικονικής μηχανής πάνω στην κάρτα. Εξασφαλίζει την ανεξαρτησία του κώδικα της εφαρμογής από το υλικό περιβάλλον της κάρτας. Οι λειτουργίες που εφαρμόζει είναι οι ακόλουθες:

- Υλοποιεί το δυαδικό κώδικα
- Ασκεί έλεγχο στην δεσμευμένη μνήμη και το σχηματισμό αντικειμένων,
- Δίνει ιδιαίτερη προσοχή στην ασφάλεια της μνήμης κατά το διάστημα της υλοποίησης στην κάρτα.

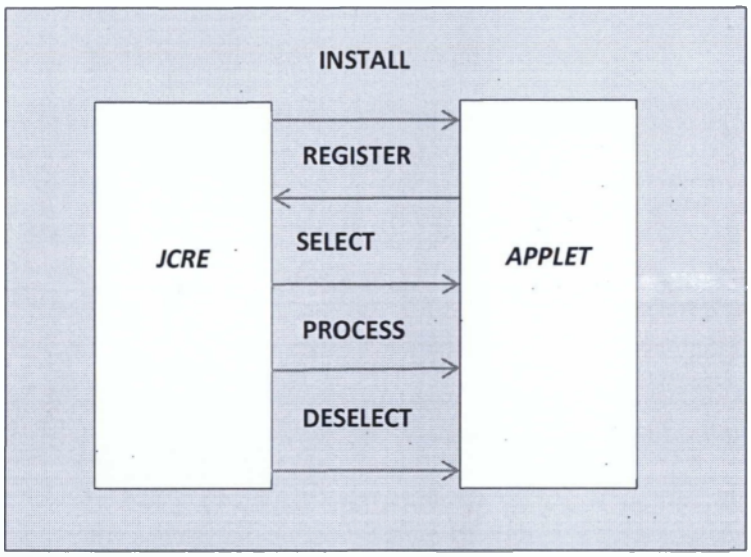
]

4.2.2 Περιβάλλον εκτέλεσης εφαρμογών Java Card (JCRE)

Παραπάνω (Αρχιτεκτονική Java Card) είχαμε παρουσιάσει την ιδιότητα της Java Card Runtime Environmentη οποία είναι η ανάλυση της συμπεριφοράς του περιβάλλοντος εκτέλεσης και η ενίσχυση στο σύστημα της έξυπνης κάρτας , στην επι-

κοινωνία , στην ασφάλεια και στο μοντέλο εκτέλεσης εφαρμογών. Επίσης, είχαμε γνωστοποιήσει και αναλύσει τα μέρη που απαρτίζεται δηλαδή από τη Java Card Framework &APIs και από Java Card Virtual Machine.\

Εδώ αναφερόμαστε στην επικοινωνία μεταξύ της Applet και της Java Card Runtime Environment η οποία συνδέεται με τις πέντε βασικές λειτουργίες. Από αυτές ανακαλύπτονται ορισμένα σημεία εισόδου (multiple entry points) σε ένα Applet. Στην ουσία, είναι οι τρόποι επικοινωνίας αυτού με τον έξω κόσμο. Παρακάτω περιγράφονται οι τρόποι επικοινωνίας αλλά και ποιος έχει το δικαίωμα κλήσης της κάθε μεθόδου.



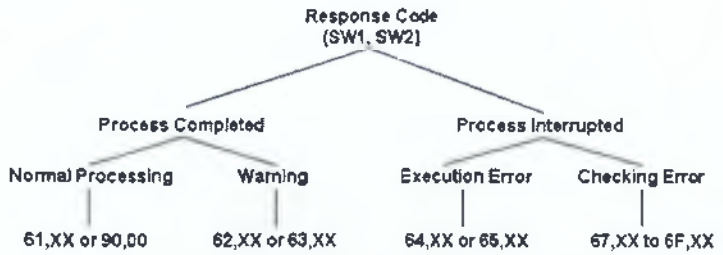
Διάγραμμα 7: Σύνδεση επικοινωνίας μεταξύ JCRE-APPLET

1. **Μεθοδολογία Install:** Η ιδιότητα της είναι η εγκατάσταση αντικειμένου. Εφαρμόζεται μία φορά στη διάρκεια ζωής του Applet αρκετές φορές εμφανίζει κάποια ορίσματα αρχικοποίησης. Η βασική της λειτουργία περιλαμβάνει την δημιουργία ενός στιγμιότυπου, την κλάση του Applet και η δέσμευση στο JVRE. Η δέσμευση πραγματοποιείται με την κλήση της μεθόδου register. Η register είναι απαραίτητη να υπάρχει σε κάθε εγκατάσταση (install) αλλιώς η εγκατάσταση δε θα ευδοκιμήσει. Αυτή προστάζεται από το JCRE αλλά το σώμα πραγματοποιείται στο Applet.
2. **Μεθοδολογία Register:** Η ιδιότητα της είναι η καταχώρηση στιγμιότυπου. Προτρέπεται από το Applet για να μπορέσει να καταχωρηθεί στο JVCR. Το διάστημα που εφαρμόζεται η install σχηματίζεται ένα στιγμιότυπο της κλάσης του Applet. Το συγκεκριμένο στιγμιότυπο αποθηκεύεται στο JCRE. Τέλος, το κάλεσμα της μεθόδου πραγματοποιείται από το σώμα της μεθόδου install και προστάζεται από το Applet.
3. **Μεθοδολογία Select:** Η ιδιότητα της είναι η επιλογή της εφαρμογής. Η επιλογή της εφαρμογής είναι πολύ σημαντική όταν το Applet εφαρμόζει μία λειτουργία. Στην πραγματικότητα , πρώτα πραγματοποιείται η επιλογή και αυτό

διότι το JCRE πρέπει να καταλάβει σε ποιο Applet γίνεται η αναφορά. Αφού γίνει η επιλογή , πέμπεται ένα μήνυμα το οποίο εμπεριέχει το AID του Applet. Αν το το AID είναι καταχωρημένο στα στιγμιότυπα τότε η εγκατάσταση του Applet είναι επιτυχής και έτσι καλείται η select ώστε να επιλεχθεί αυτό. Αυτό εφαρμόζει μόνο λειτουργίες που υποστηρίζει και είναι επιλεγμένο μία φορά.

4. **Μεθοδολογία Process:** Η ιδιότητα της είναι η εκτέλεση εντολής εντός εφαρμογής. Με τη βοήθεια του Applet εφαρμόζεται η εκτέλεση εντολής εντός εφαρμογής. Αφού έχει γίνει η εγκατάσταση του Applet με επιτυχία , τότε αποστέλλεται το μήνυμα στην κάρτα και εκείνη τη στιγμή εφαρμόζεται η process με τα απαραίτητα ορίσματα του μηνύματος.
5. **Μεθοδολογία Deselect:** Η ιδιότητα της συνδέεται με την εγκατάλειψη εφαρμογής. Υλοποιείται μέσω του JCRE από τη στιγμή που έχει ληφθεί το μήνυμα με το AID Applet που είναι επιλεγμένο. Διαφορετικά αποδίδει με ένα μήνυμα λάθους. Η χρήση της πραγματοποιείται σε περιπτώσεις εγκατάλειψης ενός Applet ή για επιλογή κάποιου άλλου Applet.

Αφού ολοκληρωθεί η αποστολή του μηνύματος στην κάρτα και η επεξεργασία από τον περιβάλλον εκτέλεσης εφαρμογών, ύστερα, στέλνεται ένα μήνυμα προς τους χρήστες για να πληροφορηθούν αν είναι λανθασμένη ή επιτυχημένη η εκτέλεση εντολής. Δηλαδή, αν ο χρήστης στείλει ένα μήνυμα επιλογής Applet που περιλαμβάνεται το AID στο περιβάλλον εκτέλεσης και λειτουργήσει η επιλογή τότε ο χρήστης θα λάβει σαν απάντηση τον αριθμό 90,00 που δηλώνει ότι υλοποιήθηκε η εκτέλεση ενέργειας. Αλλά στην περίπτωση που η ενέργεια είναι αποτυχημένη τότε στέλνεται ένα μήνυμα λάθους το οποίο θα περιλαμβάνει μια απάντηση που συνδέεται με την κατηγορία που ανήκει το συγκεκριμένο λάθος.



Διάγραμμα 8: Η δομή των μηνυμάτων απάντησης

4.2.3 Java Card Applications Programming Interface (JC API)

Η Java Card API είναι ένα σύνολο κανόνων το οποίο προσδιορίζει τις απαραίτητες κλάσεις για την εφαρμογή των έξυπνων καρτών σύμφωνα με το πρότυπο ISO

7818. Περιλαμβάνει τρία πακέτα και ένα πακέτο επέκτασης τα οποία είναι τα ακόλουθα:

1. **Java .lang:** Είναι ένα πακέτο που υποδηλώνει το υποσύνολο του πακέτου java. lang της Java. Οι υποστηριζόμενες κλάσεις είναι οι Object, Throw able και Exception . Η κλάση Object προσδιορίζει τη ρίζα της σειράς των κλάσεων Java, ενώ η κλάση Throw able , ορίζει ένα κοινό πρόγονο από τον οποίον κληρονθομούν όλες οι κλάσεις των εξαιρέσεων.
2. **Java-card. Framework:** Είναι ένα πακέτο που προσφέρει τις κλάσεις και διεπαφές για τη λειτουργία μιας Java Card εφαρμογής. Σημαντική κλάση που προσδιορίζεται σε αυτό το πακέτο είναι η Applet, το οποίο είναι ο συνδετικός κρίκος για την επικοινωνία ανάμεσα στο περιβάλλον εκτέλεσης και στις εφαρμογές. Η κλάση μίας εφαρμογής επιβάλλεται να κληρονομεί από την κλάση Applet και να παραβλέπει τις τις μεθόδους της. Μια άλλη κλάση είναι η APDU. Έχει προσδιοριστεί με έναν τρόπο ώστε να είναι ανεξάρτητη από τα πρωτόκολλα μεταφοράς και αυτό δίνεται η δυνατότητα στους δημιουργούς να διαχειρίζονται με ευχέρεια τα μηνύματα APDU. Γενικά, εμπεριέχουν κλάσεις με μεθόδους οι οποίες ασκούν έλεγχο στην εκτέλεση μίας εφαρμογής, στη διαχείριση πόρων και στην εισαγωγή ενός κωδικού PIN.
3. **Java card. security:** Είναι ένα πακέτο που παρέχει ένα πλαίσιο για τις κρυπτογραφικές λειτουργίες που ενισχύονται από την Java Card. Προσδιορίζεται η κλάση Key Builder και διάφορες διεπαφές για τον σχηματισμό κρυπτογραφικών κλειδιών με τη χρήση συμμετρικών και ασύμμετρων αλγορίθμων. Αλλά και οι κλάσεις Random, Data, Sigruture και Message Digest οι οποίες εφαρμόζονται για τον σχηματισμό των δεδομένων και για την παραγωγή σύνοψης μηνυμάτων και ψηφιακών υπογραφών.
4. **Java cardx. Crypto**: Είναι ένα πακέτο επέκτασης. Συμπεριλαμβάνει κρυπτογραφικές κλάσεις και διεπαφές. Σημαντική κλάση του συγκεκριμένου πακέτου είναι η Cipher η οποία υποστηρίζει κρυπτογραφικές και αποκρυπτογραφείς λειτουργίες.

4.3 Εφαρμογές java cart ή java cart applets

Τα προγράμματα Java Card είναι εφαρμογές των Java οι οποίες υφίστανται κάποιους περιορισμούς για να μπορούν να εφαρμοστούν στο περιβάλλον εκτέλεσης της Java Card. Δηλαδή, μία Java Card Applet μπορεί να φορτωθεί στην κάρτα ακόμα και μετά την κατάσταση της. Αυτή ταξινομείται σε δύο μεθοδολογίες ώστε να μπορέσει να υλοποιηθεί. Η πρώτη μέθοδος είναι σύμφωνα με τη λογική του μοντέλου αιτήσεων – απαντήσεων (όπως είναι Client-Server) δηλαδή μία client εφαρμογή πέμπει αιτήματα και δέχεται αποκρίσεις από την κάρτα. Ενώ η δεύτερη μέθοδος εφαρμόζει τη κλήση απομακρυσμένων μεθόδων (RMI: Remote Method Invocation). Η RMI εείναι μια μεθοδολογία που εγκρίνει στους χρήστες να υλοποιούν απομακρυσμένες κλήσεις, μεταξύ διαφορετικών προγραμμάτων. Επίσης, οι κάρτες οι οποίες είναι σχεδιασμένες για Java Card έχουν τη δυνατότητα να ενισχύουν τις πολλαπλές εφαρμογές

που περιλαμβάνονται στην ίδια κάρτα. Δηλαδή οι εφαρμογές των δύο μεθοδολογιών μπορούν να συνυπάρχουν και να αλληλεπιδρούν συνάμα με ασφάλεια.

Οι εφαρμογές της κάρτας, επίσης , έχουν τη δυνατότητα να επικοινωνούν με προγράμματα που βρίσκονται είτε εκτός κάρτας είτε στο τερματικό είτε στο υπολογιστή αναλόγως τι CAD θα χρησιμοποιήσει ο χρήστης. Για παράδειγμα στο APDU, το ρόλο του server το έχουν applets δηλαδή απαντάνε σε αιτήσεις του client , και στην συγκεκριμένη περίπτωση είναι οι εφαρμογές του τερματικού. Ενώ, με την μέθοδος RMI , οι εφαρμογές εντός και εκτός κάρτας επικοινωνούν ανάμεσά τους με κλήσεις συναρτήσεων.

4.4 Επικοινωνία εφαρμογών έξυπνων καρτών

Στην ενότητα επικοινωνία εφαρμογών έξυπνων καρτών διευκρινίζεται η μέθοδος με την οποία υλοποιείται η ανταλλαγή των πληροφοριών των εφαρμογών που εφαρμόζονται είτε μέσα στην κάρτα είτε εκτός κάρτας. Η μέθοδος αυτή συνδέεται άμεσα με την τεχνολογία υλοποίησης. Παρακάτω, αποσαφηνίζονται οι διαφορές και τα βήματα που συσχετίζονται με την ολοκλήρωση επικοινωνίας και ύστερα διεξάγεται μια αναφορά στη διαδικασία ανάπτυξης εφαρμογών.

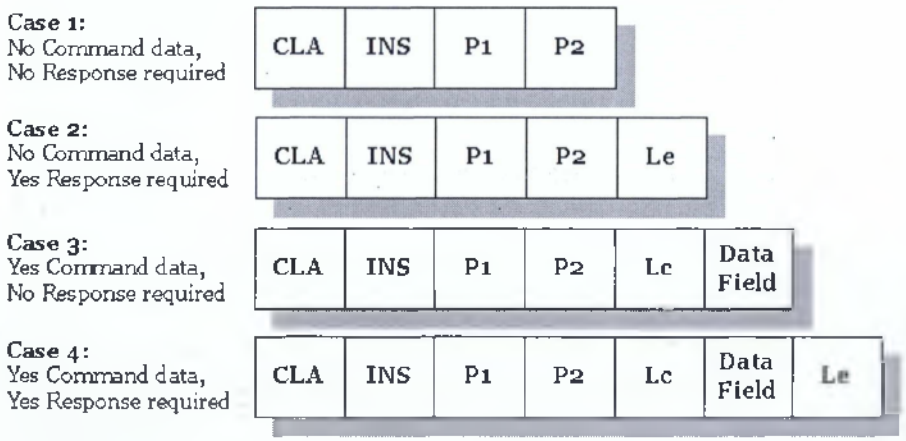
4.4.1 Επικοινωνία μέσω APDUS

Το APDUs είναι μια εφαρμογή πρωτοκόλλου και χρησιμοποιείται για την επικοινωνία ενός αναγνώστη έξυπνων καρτών (card reader) και μια έξυπνη κάρτα (smart card). Επιπλέον, το APDUs των έξυπνων καρτών είναι τοποθετημένο πάνω από το στρώμα μεταφοράς και μεταφορά δεδομένων υλοποιείται με μηνύματα TPDU. Η δομή του καθορίζεται από το πρότυπο από το ISO 7816-4. Η δομή του περιλαμβάνει δύο μορφές APDUs δηλαδή το APDUs command και το Response APDUs. Τα APDUs εντολές πέμπονται από τον host στην εφαρμογή μέσα στην κάρτα. Ενώ, τα APDUS απαντήσεις πέμπονται ως απάντηση από την έξυπνη κάρτα.

Η εντολή APDUs περιλαμβάνει από μία κεφαλίδα και ένα σώμα. Η κεφαλίδα (Header) κατανέμεται σε τέσσερις τομείς και αναπαριστούν ένα byte το καθένα. Ο πρώτος τομέας εκφράζει την εντολή κλάσης (CLA) και αναπαριστά την κλάση που επιθυμεί ο χρήστης να αναφερθεί. Ο δεύτερος τομέας προσδιορίζει μια συγκεκριμένη εντολή (INS) που συνδέεται με την κλάση που διαλέχτηκε. Οι άλλοι δύο τομείς εφαρμόζονται σαν ορίσματα ώστε να καθορίζονται σαφέστατα την εργασία που ορίζουν τα αρχικά δύο bytes. Το μήκος του σώματος μπορεί να μην είναι σταθερό ή μπορεί να μην περιέχεται στο πεδίο δεδομένων. Υπάρχουν κάποια χαρακτηριστικά που εμπεριέχονται στις εντολές APDUs και είναι τα ακόλουθα:

- "Ένα class byte (CLY). Καθορίζει την κλάση της εντολής.
- Ένα instruction byte (INS). Καθορίζει την συγκεκριμένη εντολή.

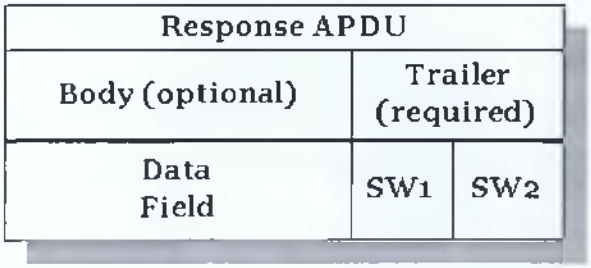
- Δύο παράμετροι bytes P1 και P2. Αυτά χρησιμοποιούνται για διοχέτευση παραμέτρων στην εντολή.
- Ένα byte μήκους Lc ("length command") . Καθορίζει το μήκος των προαιρετικών δεδομένων που στέλνονται με το APDU,
- Προαιρετικά Δεδομένα (Optional Data).
- Ένα byte μήκους Le ("length expected"). Καθορίζει το αναμενόμενο μήκος των δεδομένων που θα σταλούν στο αμέσως επόμενο APDU απάντησης (response APDU). Αν το Le είναι τότε ο host περιμένει η κάρτα να στείλει όλα τα δεδομένα που είναι διαθέσιμα στην απάντηση αυτής της εντολής."[5]



Διάγραμμα 9: Πιθανές εντολές APDU command

Ενώ οι απαντήσεις APDUs δεν είναι αναγκαίο να περιέχει ένα σώμα αλλά είναι υποχρεωτικό να συμπεριλαμβάνει την ουρά .Το JCRE στέλνει πάντοτε απάντηση για να γνωρίζει ο χρήστης την έκβαση μιας εντολής που έστειλε. Τα ακόλουθα πεδία που εμπεριέχονται στα APDUS απαντήσεις είναι τα ακόλουθα:

- Προαιρετικά δεδομένα.
- Δύο λέξεις καταστάσεων SW1 και SW2 οι οποίες περιέχουν πληροφορίες κατάστασης.



[5] artemis-new.cslab.ece.ntua.gr:8080/jspui/bitstream/123456789/5827/1/PD2006-0003

Διάγραμμα 10: Η δομή της απάντησης APDU

4.4.2 Διαφορές APDU – RMI

Στο διάστημα που πρέπει να αναπτυχθεί η κάρτα Java, πρέπει να έχει επιλεχθεί η χρήση του εξοπλισμού όπου επιβάλλει και την τεχνολογία υλοποίησης. Και αυτό συμβαίνει επειδή το APDU ενισχύει όλους τους τύπους έξυπνων καρτών σε αντίθεση με το RMI που υποστηρίζεται από την έκδοση 2.2 της Java card και μετά. Παρακάτω αναφέρονται οι πιο σημαντικές διαφορές μεταξύ APDU και RMI.

- Η πρώτη διαφορά ανάμεσα στο APDU και RMI είναι ότι πρώτο έχει πλήρης έλεγχο των APDU μηνυμάτων, ενώ το δεύτερο υπάρχει απόκρυψη των APDU μηνυμάτων.
- Η δεύτερη διαφορά είναι ότι στο ένα περιλαμβάνει έκδοση ή δημιουργία εντολών ενώ το δεύτερο περιλαμβάνει μια κλήση μεθόδων.
- Μια άλλη διαφορά είναι ότι το μεν APDU περιέχει μια απλότητα Applet εφαρμογής ενώ ο δεν RMI έχει περίπλοκη εφαρμογή Applet.
- Στο APDU περιλαμβάνει μια επικοινωνία των Applet μέσω διαμοιραζόμενης διασύνδεσης ενώ στο RMI είναι αδύνατη η υλοποίηση διαμοιραζόμενης διασύνδεσης.

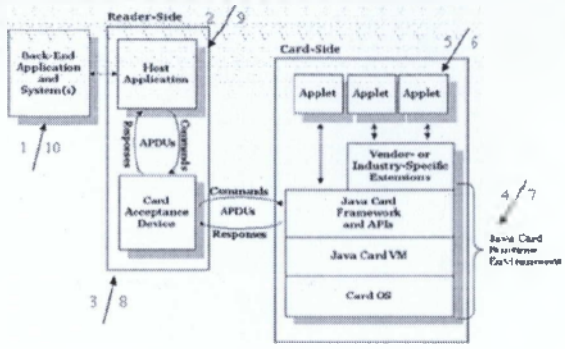
4.4.3 Επικοινωνία μεταξύ κάρτας και πελάτη

Σε μια APDU εφαρμογή, είναι αναγκαία να υπάρχει μια αλλεπάλληλη επικοινωνία προγραμμάτων. Στην ουσία, κάποια προγράμματα είναι έτοιμα ενώ κάποια άλλα πρέπει να εφαρμοστούν. Υφίστανται τρεις μορφές προγραμμάτων εκτός κάρτας και είναι οι ακόλουθες:

- Back End (service – client)
- Host (πληρεξούσια εφαρμογή)
- Card Acceptance Devices (CAD)

Η Back-End και η Host ανήκουν στις εφαρμογές που πρέπει να εφαρμοστούν ενώ η Host είναι μία ολοκληρωμένη εφαρμογή και εκτελεί τη φυσική διασύνδεση μεταξύ της Host και την εντός κάρτας προγραμμάτων.

Στον ενδεχόμενο ενός RMI, οι τρεις συγκεκριμένες μορφές περιπλέκονται σε τέτοιο σημείο ώσπου δεν γίνεται σαφής επεξήγηση των μορφών. Για παράδειγμα, σε μια APDU τεχνολογία ο πελάτης επικοινωνεί με την πληρεξούσια εφαρμογή. Αυτή πέμπει ένα μήνυμα στην CAD εφαρμογή με τελικό προορισμό την κάρτα.



Διάγραμμα 11: Επικοινωνία πελάτη-κάρτα

Σύμφωνα με την εικόνα παρατηρούμαι ότι ενέργεια αρχίζει από το πεδίο 1 και καταλήγει στο 11 . Απαρτίζεται από δύο μέρη. Το πρώτο μέρος εκκινεί από την εφαρμογή χρήστη και φτάνει στην κάρτα όπου δείχνει την κατεύθυνση της εντολής command UPDU προς την κάρτα.. Το δεύτερο μέρος κάνει εκκίνηση στο σημείο 6 ώστε να καταλήξει στο 11, όπου πραγματοποιείται η response APDU προς το πελάτη. Δηλαδή ο χρήστης ξεκινάει μια διεργασία από το γραφικό περιβάλλοντος του χρήστη ώστε να θέσει τα δεδομένα και στη συνέχεια ο client τα αποστέλλει ως όρισμα στην Host. Έπειτα, η πληρεξούσια εφαρμογή μετατρέπει τα δεδομένα σε bytes και αφού ολοκληρώσει τα πεδία σε μία εντολή APDU τα θέτει εντός αυτής και πέμπει την εντολή στη CAD. Η CAD παίρνει τον έλεγχο της εντολής και με την βοήθεια του card reader πέμπει την εντολή στην κάρτα. Στην συνέχεια μαζί με την JCRE τροποποιούν τα δεδομένα και ωθούν το κατάλληλο APPLET το οποίο εντοπίζει την εντολή και υλοποιεί της κατάλληλες ενέργειες.

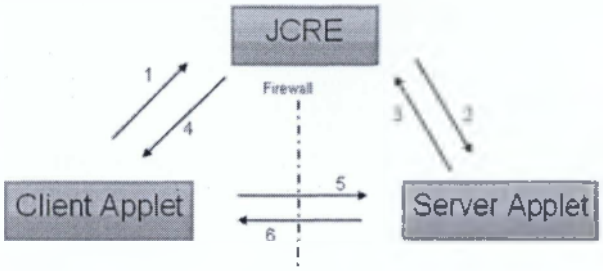
Τώρα αρχίζει η διαδικασία της αποστολής της απάντησης. Το Applet πέμπει την απάντηση στο JVCR και αυτό το στέλνει πίσω στην CAD. Αυτή πέμπει το μήνυμα της απάντησης στην HOST όπου θα λάβει τα δεδομένα , θα τα τροποποιήσει και θα επιστρέψει στην απαραίτητη μορφή στον πελάτη. Και ύστερα ο client θα ενημερώσει το χρήστη για τα αποτελέσματα που συνεπάγεσαι η εντολή που είχε παραχωρήσει ο χρήστης. Αν υπάρξει το ενδεχόμενο ότι το συγκεκριμένο Applet δεν υπάρχει στην κάρτα τότε παραλείπονται τα βήματα 5και 9 γιατί το περιβάλλον εκτέλεσης έχει την εύθηνη για τη δημιουργία και την αποστολή CAD.

4.4.3 Επικοινωνία εφαρμογών μέσα στην κάρτα

Η επικοινωνία των εφαρμογών μέσα στην κάρτα ελέγχεται από τον μηχανισμό του λογισμικού της κάρτας JCRE, firewall. Οι εφαρμογές στην κάρτα τάσσονται σε πακέτα. Όταν επικοινωνούν δύο εφαρμογές του ίδιου πακέτου τότε δεν τους επηρεάζει το firewall. Αντίθετα, όταν είναι σε διαφορετικά πακέτα το firewall μπλοκάρει την επικοινωνία προγραμμάτων επειδή η μία από τις δύο εφαρμογές μπορεί να είναι κα-

κόβουλη και μη εξουσιοδοτημένη για να μπορέσει να έχει πρόσβαση σε ευαίσθητα δεδομένα.

Με την τεχνική διαμοιραζόμενης διασύνδεσης (Shareable Interface) μπορεί να αποφύγει το firewall. Το κύριο γνώρισμα της είναι ότι έχει τη δυνατότητα να δώσει την έγκριση σε μια εφαρμογή της κάρτας να δηλώσει ποια δεδομένα σκοπεύει μα επιμερίσει με άλλα προγράμματα.



Διάγραμμα 12: Η δομή της Sharable Interface

• Στάδιο 1: **Αίτηση διαμοιραζόμενης διασύνδεσης από το JCRE**
• Στάδιο 2: **Αίτηση διαμοιραζόμενης διασύνδεσης από το Applet**
• Στάδιο 3: **Επιστροφή διαμοιραζόμενης διασύνδεσης από το Applet**
• Στάδιο 4: **Επιστροφή διασύνδεσης από το JCRE**
• Στάδιο 5: **Χρήση της διασύνδεσης**
• Στάδιο 6: **Επιστροφή αποτελεσμάτων**

Πίνακας 5: Sharable Interface

Το πρώτο βήμα είναι ο προγραμματιστής να σχηματίσει μια επιμέρους διασύνδεση στο server applet ώστε να γνωστοποιήσει μία εφαρμογή όπου θα αναφέρονται οι μεθοδολογίες που στοχεύουν να επιμερίσουν. Ύστερα, η εφαρμογή εκτελεί τη διασύνδεση και τις μεθοδολογίες που έχουν καθοριστεί σ' αυτήν και έπειτα να τις διανέμει. Αφετέρου, αν υπάρχει μια εφαρμογή που προτίθεται να κάνει χρήση τις επιμέρους μεθοδολογίες μιας άλλης εφαρμογής δηλαδή το client applet τότε φτιάχνει μια αίτηση στο JCRE αναφέροντας το AID της εφαρμογής που θέλει να επικοινωνήσει. Στη συνέχεια, το JVRE επικοινωνεί με την εφαρμογή που έχει καθορισμένο το AID επιζητώντας από αυτήν την επικύρωση για τη διαμοίραση των δεδομένων της. Εφόσον δεν έχει εμφανιστεί κάποιο σφάλμα τότε γυρίζει στην εφαρμογή που έκανε την αίτηση. Έπειτα, ο πελάτης (client) applet εκμεταλλεύεται τη διασύνδεση ώστε να επιζητήσει τα δεδομένα που είναι αναγκαία ενώ ο εξυπηρετητής (server) applet γυρίζει τα αποτελέσματα στο applet.

Σύμφωνα με αυτή τη μεθοδολογία μια APDU εφαρμογή διανέμει με ευχέρεια και ασφάλεια τα στοιχεία , ενώ μια RMI εφαρμογή της καθιστά αδύνατο εξαιτίας της δομής της αλλά όμως μπορεί να εφαρμοστεί για την διαμοιραζόμενη διασύνδεση μιας APDU εφαρμογής σε ένα υβριδικό μοντέλο.

ΚΕΦΑΛΑΙΟ 5 ΛΟΓΙΣΜΚΟ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ

5.1 Εισαγωγή

Σ' αυτό το κεφάλαιο αναλύουμε τα λειτουργικά συστήματα, των είδος των λειτουργικών συστημάτων που εγκρίνουν την ανάπτυξη εφαρμογών από τον ίδιο τον κάτοχο της κάρτας, την μεταφορά των δεδομένων και το πρωτόκολλό τους, για το κεντρικό σύστημα έξυπνων καρτών, για το πρότυπο ISO7816 και για τις καρτ-εφαρμογές και τις τελικές εφαρμογές.

5.2 Διαδικασία ανάπτυξης εφαρμογών σε μια έξυπνη κάρτα

Οι εφαρμογές των έξυπνων καρτών είναι ταξινομημένες σε δύο βασικές κατηγορίες οι οποίες είναι οι ακόλουθες. Το πρώτο μέρος είναι οι καρτ-εφαρμογές που είναι τοποθετημένες πάνω στην έξυπνη κάρτα και εφαρμόζονται πάνω σε αυτές. Ενώ το δεύτερο μέρος θα συμπεριλαμβάνει τις τελικές εφαρμογές ή εφαρμογές των χρηστών οι οποίες θα εντοπίζονται και θα ασκούνται στο τερματικό.

Για να ξεκινήσει η επικοινωνία χρειάζεται να δοθούν εντολές APDU μεταξύ του αναγνώστη της κάρτας και ενός μοντέλου. Η λειτουργία μοιάζει πανομοιότυπα με εκείνη του μοντέλου client-server. Απλά κάνουμε μια αντικατάσταση τον εξυπηρετητή με την έξυπνη κάρτα που εμπεριέχει τις εφαρμογές και τα δεδομένα και τον πελάτη με την εφαρμογή τελικών χρηστών.

Η ανάπτυξη των υπηρεσιών μιας έξυπνης κάρτας εξετάζεται σε δύο μέρη δηλαδή από την πλευρά του εξυπηρετητή και από την πλευρά του πελάτη. Από τη μία όψη ο εξυπηρετητής μπορεί να σχηματίσει ένα καθορισμένο σύνολο δομών των οποίων θα φιλοξενούνται τα δεδομένα και οι εφαρμογές πάνω στην κάρτα. Το έργο των καρτ-εφαρμογών ,σε κάρτες που περιλαμβάνουν ένα σύστημα αρχείων, θα απαρτίζεται με το άθροισμα των αρχείων που θα είναι ενωμένα μεταξύ τους αλλά και με το άθροισμα κανόνων που σχετίζονται με την πρόσβαση των δεδομένων των αρχείων αυτών. Όλες οι λειτουργίες της κάρτας ,ήτοι η ανάγνωση, η εγγραφή, οι κρυπτογραφικές λειτουργίες και ο έλεγχος πρόσβασης, θα καθορίζεται από το λειτουργικό σύστημα της κάρτας. Από την άλλη όψη, ο πελάτης θα σχετίζεται με την ανάπτυξη των προγραμμάτων διασύνδεσης της κάρτας , του αναγνώστη, των εφαρμογών των τελικών χρηστών και της κατάλληλης γραφικής διαπροσωπείας.

5.3 Μεταφορά δεδομένων στις έξυπνες κάρτες

Η επικοινωνία ανάμεσα στην έξυπνη κάρτα και στο τερματικό συσκευής υλοποιείται μέσω της επαφής εισόδου και εξόδου δηλαδή στη αποκλειστική επαφή C7.

Αυτός ο περιορισμός είναι η αιτία που υφίσταται half-duplex. Το half-duplex είναι η διαδικασία με την οποία η μια πλευρά διαβιβάζει δεδομένα ενώ από την άλλη πλευρά δηλαδή ο παραλήπτης περιμένει τη σειρά του για μετάδοση. Η εκκίνηση της επικοινωνίας εφαρμόζεται από την στιγμή που θα υπάρξει μία αίτηση από το τερματικό και η κάρτα θα απαντά στις αιτήσεις του τερματικού.

Από τη στιγμή που η κάρτα θα έχει πρόσβαση στη συσκευή ανάγνωσης τότε οι επαφές της θα εισαχθούν με τις αντίστοιχες επαφές της συσκευής ανάγνωσης (card reader). Όταν η κάρτα λοιπόν φορτώσει, τότε εκτελεί την εντολή Power – On Reset. Έπειτα, πέμπει ένα Answer to Reset (ATR) σήμα στη συσκευή ανάγνωσης . Το ATR είναι μία αλληλουχία δεδομένων σε μορφή bytes όπου επιστρέφεται από την κάρτα στο τερματικό και έτσι καθορίζεται η επίτευξη της Power up διαδικασία. Επίσης χρησιμοποιείται και ως πρωτόκολλο μετάδοσης. Επιπροσθέτως, το μέγιστο μήκος που μπορεί να υφίσταται αυτό είναι 33 bytes αλλά όμως απαρτίζεται συνήθως από μερικά μόνο bytes. Το τερματικό αφού έχει επεξεργαστεί τις παραμέτρους που περιέχει το σήμα ATR, πέμπει την πρώτη εντολή στην κάρτα. Εφόσον, η κάρτα έχει δεκτή την εντολή τότε στέλνει μία απάντηση στο τερματικό.

Για την υλοποίηση της μεταφοράς δεδομένων απαιτείται να υπάρχει μια αλληλουχία από διάφορα πρωτόκολλα. Κύριο χαρακτηριστικό αυτών των πρωτοκόλλων είναι το σύμβολο «T=» το οποίο περιλαμβάνεται μαζί με έναν αριθμό από το 0 έως 15. Περαιτέρω, γίνεται μια σύντομη αναφορά για το ποια είναι τα πρωτόκολλα και ποια είναι η λειτουργία τους.

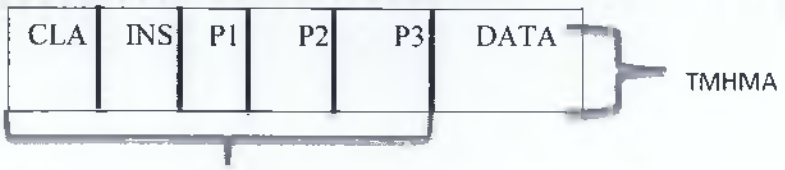
- Πρωτόκολλο T=0:Είναι ασύγχρονη, half-duplex και ανά byte επικοινωνία
- Πρωτόκολλο T=1:Είναι ασύγχρονη, half-duplex και ανά block επικοινωνία
- Πρωτόκολλο T=2:Είναι ασύγχρονη, full-duplex και ανά block επικοινωνία
- Πρωτόκολλο T=3:Είναι full-duplex αλλά είναι μη υποστηριζόμενη
- Πρωτόκολλο T=4:Είναι ασύγχρονη, half-duplex και ανά byte επικοινωνία. Είναι η επέκταση του T=0.
- Πρωτόκολλο T=5:Είναι δεσμευμένο για μελλοντική χρήση
- Πρωτόκολλο T=6:Είναι δεσμευμένο για μελλοντική χρήση
- Πρωτόκολλο T=7:Είναι δεσμευμένο για μελλοντική χρήση
- Πρωτόκολλο T=8:Είναι δεσμευμένο για μελλοντική χρήση
- Πρωτόκολλο T=9:Είναι δεσμευμένο για μελλοντική χρήση
- Πρωτόκολλο T=10:Είναι δεσμευμένο για μελλοντική χρήση
- Πρωτόκολλο T=11:Είναι δεσμευμένο για μελλοντική χρήση
- Πρωτόκολλο T=12:Είναι δεσμευμένο για μελλοντική χρήση
- Πρωτόκολλο T=13:Είναι δεσμευμένο για μελλοντική χρήση
- Πρωτόκολλο T=14: Για εθνικές λειτουργίες και δεν υποστηρίζεται από το ISO
- Πρωτόκολλο T=15:Είναι δεσμευμένο για μελλοντική χρήση

5.3.1 Πρωτόκολλο μεταφοράς δεδομένων

Ένα από τα πιο δημοφιλές πρωτόκολλα που εφαρμόζονται συχνά είναι το πρωτόκολλο μεταφοράς T=0 και το T=1. Πρωτόκολλο T=0 προσδιορίζεται σύμφωνα με το πρότυπο ISO 7816-3 και θεωρείται ασύγχρονο. Αυτό φανερώνει ότι δεν υπάρχει αυστηρή χρονική συνοχή ανάμεσα σε μία εντολή που στέλνεται από τη συσκευή ανάγνωσης στην κάρτα αλλά ούτε στην εντολή που πέμπεται από την κάρτα στην συσκευή ανάγνωσης. Από τη στιγμή που η κάρτα παραλάβει την εντολή από την συσκευή ανάγνωσης τότε υλοποιεί τις επιζητούμενες εντολές και στη συνέχεια πέμπει ένα μήνυμα απάντησης. Αφού έχουν εκτελεσθεί οι προηγούμενες διαδικασίες, τότε η συσκευή ανάγνωσης είναι ελεύθερη να στείλει την επόμενη εντολή στην κάρτα.

Η υλοποίηση ενός πρωτοκόλλου T=0 ξεκινά με την μετατροπή των δεδομένων σε bytes . Αυτή η διαδικασία γίνεται μέσω ενός καναλιού μεταξύ της κάρτας και της συσκευής ανάγνωσης. Μετά, πραγματοποιείται ένας έλεγχος λαθών μέσω του parity bit δηλαδή έλεγχος bit. Στην περίπτωση που το parity bit είναι διαφορετικό από το parity bit των δεδομένων που αποστέλλονται τότε πρόκειται για σφάλμα και έτσι το μήνυμα αναμεταδίδεται. Η επικοινωνία ενδιάμεσα της κάρτας και της συσκευής ανάγνωσης εφαρμόζεται μέσω μίας μορφή δομής δεδομένων το Transmission Protocol Data Units (TPDUs). Στην περίπτωση του συγκεκριμένου πρωτοκόλλου το TPDUs απαρτίζεται από την εντολή - command TPDU όπου πέμπεται από τη συσκευή ανάγνωσης στην κάρτα. Και από την απάντηση – response TPDU το οποίο πέμπεται από την κάρτα στη συσκευή ανάγνωσης.

Η εντολή TPDU περιέχει μια επικεφαλίδα η οποία απαρτίζεται από πέντε τμήματα και το καθένα έχει μήκος ένα byte. Το πρώτο τμήμα είναι CLA και προσδιορίζει μια συγκεκριμένη κλάση εντολών. Το δεύτερο τμήμα είναι INS και καθορίζει την εντολή TPDU που θα εφαρμοστεί μέσα από την κλάση εντολών. Το τρίτο και τέταρτο τμήμα είναι η P1 και η P2 αντίστοιχα όπου θεσπίζουν τις παραμέτρους της εντολής. Ενώ το πέμπτο τμήμα είναι η P3 και ορίζει τον αριθμό των bytes των δεδομένων που θα μεταφερθούν. Κάθε φορά που στέλνεται η εντολή TPDU από την συσκευή ανάγνωσης ,η κάρτα θα απαντάει με ένα TPDU απόκριση. Το response TPDU απαρτίζεται από τρία αναγκαστικά μέρη και ένα θεληματικό τα οποία περιλαμβάνον μήκος 1 byte. Τα τρία υποχρεωτικά πεδία είναι το ACK όπου υποδεικνύει ότι η κάρτα έχει λάβει την εντολή, το NULL χρησιμοποιείται για τον έλεγχο ροής στο κανάλι εισόδου και εξόδου της κάρτας και το SW1 που περιέχει η απάντηση της κάρτας στην συγκεκριμένη εντολή. Ενώ το προαιρετικό πεδίο είναι το SW2 που περιλαμβάνει την απάντηση της κάρτας στην συγκεκριμένη εντολή.



Διάγραμμα 13: TPDU command

5.4 Λειτουργικά συστήματα

Το λειτουργικό σύστημα (Operating System – OS) είναι το λογισμικό του υπολογιστή που είναι ο υπόλογος για τη διαχείριση και τον συντονισμό των εργασιών καθώς και την κατανομή των διαθέσιμων πόρων. Παρέχει ένα ενδιάμεσο επίπεδο λογικής διασύνδεσης ανάμεσα στο λογισμικό και τον υλικό, διαμέσου του οποίου οι εφαρμογές αντιλαμβάνονται εμμέσως τον υπολογιστή. Η κεντρική του λειτουργία είναι η διαχείριση του υλικού, απαλλάσσοντας έτσι το λογισμικό του χρήστη από τον άμεσο και επίπονο χειρισμό του υπολογιστή και καθιστώντας ευκολότερο τον προγραμματισμό τους.

5.4.1 Λειτουργικό σύστημα έξυπνων καρτών (cos)

Το λειτουργικό σύστημα που περικλείει τις έξυπνες κάρτες είναι το Chip Operating System δηλαδή Επεξεργαστή Ανοιχτού συστήματος αλλά είναι αναγνωρισμένο ως COS .Αυτό περιλαμβάνει μια αλληλουχία από εντολές οι οποίες έχουν εισαχθεί μόνιμα στη μνήμη ROM. Οι εντολές του καθορισμένου συστήματος δεν εξαρτώνται από κάποια συγκεκριμένη εφαρμογή αλλά έχουν τη δυνατότητα να χρησιμοποιούνται σε περισσότερες εφαρμογές, όπως είναι για παράδειγμα το λειτουργικό σύστημα των Windows ή το DOS. Το Chip Operating System ταξινομείται σε δύο κατηγορίες οι οποίες είναι τα εξής:

- **General Purpose COS – Γενικός Σκοπός Λειτουργικού Συστήματος Έξυπνων Καρτών:** Είναι ένα σύνολο που παρέχει κάποιες καθολικές εντολές οι οποίες έχουν διαφορετικές ακολουθίες και έτσι, με αυτό τον τρόπο συγκαλύπτουν τις περισσότερες εφαρμογές. Δηλαδή, καταφέρνει να κάνει τη κάρτα ως εκ τούτου μία ασφαλή συσκευή υπολογισμού. Συνάμα, τα αρχεία και η άδεια πρόσβασης προσδιορίζονται κατά κανόνα από τον εκδότη της κάρτας. Πιο συγκεκριμένα, τα δεδομένα, της κάρτας διαβάζονται ή ενημερώνονται ανάλογα με τις άδειες που έχουν προσδιορίσει οι εκδότες. Τέλος, η πιστοποίηση ταυτότητας και η κρυπτογράφηση είναι δύο σημαντικές ενέργειες που

εφαρμόζει το συγκεκριμένο λειτουργικό μέσω των εντολών που πέμπονται στη κάρτα.

- **Dedicated COS – Αφιερωμένο Λειτουργικό Σύστημα Έξυπνων Καρτών**: Περιλαμβάνει έναν αριθμό εντολών που είναι σχεδιασμένες για προσδιορισμένες εφαρμογές αλλά εμπεριέχει και την ίδια την εφαρμογή. Με άλλα λόγια ,υπάρχει ένας διαχειριστής για τη μνήμη που δίνει τη δυνατότητα να φορτώνει επάνω στην κάρτα κάποια καθορισμένη εφαρμογή και κάποια δεδομένα .Αυτό το λειτουργικό σύστημα αρμόζει για κάρτες που φέρουν μεγάλη διάρκεια ζωής π.χ. οι Java Cards. Ένα μειονέκτημα που μπορεί να θεωρηθεί είναι η αύξηση των προβλημάτων των ασφαλειών καθώς και η απειλή που μπορεί να εισαχθεί στην κάρτας ένας ιός.

Περαιτέρω, διατυπώνονται οι πιο σημαντικές και ισοδύναμες λειτουργίες του λειτουργικού συστήματος COS:

- Η χρήση των ανταλλαγών μεταξύ του εξωτερικού κόσμου και της κάρτας.
- Η χρήση των αρχείων και πληροφοριών που προστατεύονται από τη μνήμη.
- Παροχή σταθερής αξιοπιστίας ,και συγκεκριμένα μέσα στα πλαίσια της αλληλουχίας των δεδομένων, των διακοπών μιας σειράς αλλά και της ανάκτησης λειτουργίας σε περίπτωση λάθους.
- Η χρήση της ασφάλειας καρτών και και των κρυπτογραφικών αλγορίθμων
- Παρέχει έλεγχο πρόσβασης σε πληροφορίες και λειτουργίες δηλαδή στην ανάγνωση και εγγραφή , στην ενημέρωση δεδομένων αλλά και στην επιλογή αρχείου.
- Η χρήση διάφορων καταστάσεων στη διάρκεια ζωής μιας κάρτας , όπως είναι η κατασκευή και η προσωποποίηση μιας κάρτας , η ενεργός ζωή ή ο τερματισμός ζωής της κάρτας

5.4.1.1 Multos – multi application operating

Το MULTOS είναι ένα λειτουργικό σύστημα που ανήκει στην κατηγορία των πολλαπλών εφαρμογών. Η ιδιότητα του είναι να ικανοποιεί τις απαιτήσεις των συστημάτων ηλεκτρονικής πληρωμής. Διαμορφώθηκε και ενισχύθηκε από την Master Card και την Mondex. Οι απαιτήσεις αυτών των συστημάτων είναι οι ακόλουθες:

- Ο εκδότης της κάρτας θα είναι σε θέση να αυξάνει και να μειώνει εφαρμογές. Με αυτό τον τρόπο , προστατεύεται η καλή λειτουργία της κάρτας.
- Μέσω το δημόσιων και μη προστατευόμενων δικτύων θα υλοποιείται η μεταφορά των δεδομένων χωρίς να είναι σίγουρο ότι εξασφαλίζεται η ασφάλεια.
- Θα ενισχύονται με πολλαπλοί προμηθευτές εφαρμογών χωρίς το στοιχείο αυτό να απαιτείται η δημοσίευση μυστικών κλειδιών ή του κώδικα των

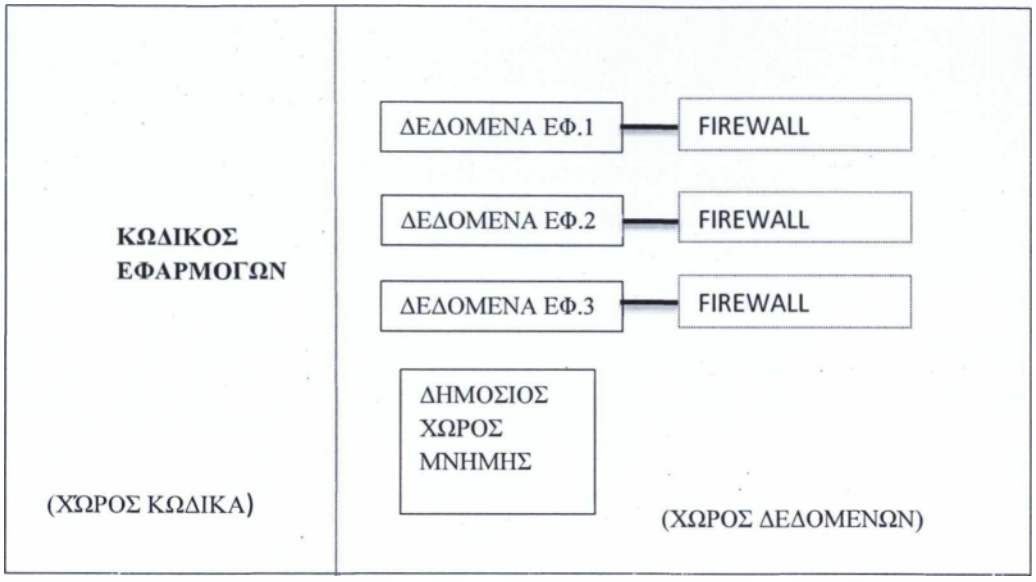
εφαρμογών ανάμεσα των προμηθευτών εφαρμογών και των εκδοτών καρτών.

Επιπλέον, η βάση του Multos αποτελείται από ένα μεταγλωττιστή ο οποίος εγκρίνει τη δημιουργία εφαρμογών ανεξάρτητα από την κάρτα την οποία τρέχουν. Αυτό έχει ως αποτέλεσμα , οι εφαρμογές του Multos να λειτουργούν σε οποιαδήποτε κάρτα που να ενισχύεται από το λειτουργικό σύστημα. Επίσης, υποστηρίζονται από τις πολλαπλές εφαρμογές με απεριόριστη ασφάλεια εξαιτίας της χρήσης των τοίχων προστασίας.

Αυτό περιλαμβάνει ένα σύστημα αρχείων το οποίο αντιστοιχεί τόσο στο πρότυπο ISO όσο και σε ένα περιβάλλον εκτέλεσης για εφαρμογές. Οι προγραμματιστές έχουν τη δυνατότητα να βελτιώνουν τις εφαρμογές κάνοντας χρήσης μιας γλώσσας που καλείται Multos-Executable Language/MEL ή σε γλώσσα C όπου στη συνέχεια απαιτείται να μεταγλωττιστεί σε MEL. Το λειτουργικό σύστημα χρειάζεται 32k μνήμη ROM και για τις εφαρμογές περίπου 16k μνήμης EEPROM.Επίσης, οι συναρτήσεις του Multos περιλαμβάνουν κρυπτογράφηση και αποκρυπτογράφηση (DES, RSA κ.α.) , γεννήτρια τυχαίων αριθμών κ.α. Μέσω της κρυπτογραφίας του δημόσιου κλειδιού υλοποιείται η διαδικασία φόρτωσης και διαγραφής εφαρμογών σε μια έξυπνη κάρτα Multos. Αυτή η μέθοδος εξασφαλίζει την ασφάλεια και τη διατήρηση ελέγχου.

Επιπροσθέτως, εντοπίζεται ανάμεσα του μικροεπεξεργαστή της έξυπνης κάρτας και των προγραμμάτων που λειτουργούν σε αυτή. Το Multos έχει ένα κοινό λειτουργικό σύστημα με ένα API, το Application Abstract Machine (AMM). Αυτό στοχεύει κατόπιν το σχηματισμό μιας καινούριας εφαρμογής για Multos , αυτή θα είναι σε θέση να φορτώνεται σε κάθε κάρτα που υποστηρίζει Multos. Επίσης, το Application Programming Interface καθορίζεται από ένα σύνολο εντολών και συναρτήσεων βιβλιοθήκης γνωστές ως primitives. Το Application Abstract Machine βρίσκεται στη κορυφή του συστήματος και δεν εξαρτάται από το hardware. Επίσης, αυτό αναλύει την εφαρμογή που έχει γραφτεί στη γλώσσα MEL και την μεταφράζει σε εντολές προς το λειτουργικό και έπειτα υλοποιείται.

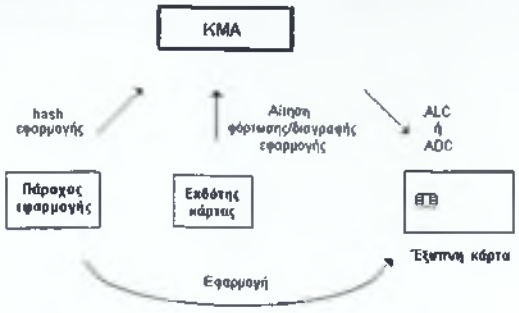
Η μνήμη της ιδεατής μηχανής του Multos (AMM) απαρτίζεται από δύο μέρη τα οποία είναι ανεξάρτητα μαζί τους. Το ένα τμήμα συνδέεται με τον κώδικα (Code space) όπου σ' αυτό το μέρος υλοποιούνται οι εφαρμογές και το άλλο τμήμα συσχετίζεται με τα δεδομένα (Data space). Στο πεδίο των δεδομένων υπάρχουν ένα καθορισμένο αριθμό δεδομένων τα οποία είναι ελεύθερα για τις εφαρμογές. Μάλιστα, οι εφαρμογές έχουν το δικό τους προσωπικό χώρο μνήμης με τη χρήση των firewalls και αυτό δεν συνδέεται με τις υπόλοιπες εφαρμογές. Επιπροσθέτως, στο τμήμα των δεδομένων απαρτίζεται και ο δημόσιος χώρος μνήμης που είναι προσπελάσιμος από τις εφαρμογές.



Διάγραμμα 14: Η δομή της μνήμης AMM

Η οντότητα Multos κατέχει ένα Κλειδί Διαχειριστικής Αρχής (Key Management Authority – KMA) και το κύριο χαρακτηριστικό αυτού του κλειδιού είναι να συντάσσει ψηφιακά πιστοποιητικά τον Application Load Certificates (ALC) και τον Application Delete Certificate (ADC). Το πιστοποιητικό ALC εφαρμόζεται για τη φόρτωση εφαρμογών, ενώ το πιστοποιητικό ADC χρησιμοποιείται για την διαγραφή εφαρμογών. Κάθε Multo έξυπνης κάρτας κατέχει ένα αποκλειστικό αριθμό εκδότη , ένα δημόσιο κλειδί KMA και ένα αποκλειστικό κλειδί ζεύγους δημοσίου και ιδιωτικού. Κάνοντας χρήση το δημόσιο κλειδί η KMA έχει την δυνατότητα να στείλει κρυπτογραφημένα μηνύματα τα οποία εμπεριέχουν κρυφά δεδομένα ή εφαρμογές όπου αυτά δεν μπορούν να εφαρμοστούν σε κάποια άλλη κάρτα.

Όταν πραγματοποιείται μια διαδικασία είτε φόρτωσης είτε διαγραφής ενός προγράμματος απαιτείται να υπάρχει μια πιστοποίηση του ALC ή του ADC. Μέσω της κάρτας εξακριβώνεται η ισχύς του πιστοποιητικού όπου μαζί με το δημόσιο κλειδί της KMA γίνεται μια σύγκριση με τον αριθμό εκδότη κάρτας. Αφού η κάρτα επιβεβαιώσει ότι ο εκδότης θέλει να φορτώσει ή να διαγράψει μια εφαρμογή τότε ο πάροχος της εφαρμογής μπορεί να προχωρήσει στην υποβολή ενός hash εφαρμογής στην KMA,ύστερα η KMA συγκαταλέγει στο πιστοποιητικό ALC. Υπολογίζοντας και συγκρίνοντας μεταξύ του hash της εφαρμογής και του hash του ALC, η κάρτα εξακριβώνει την ακεραιότητα του κώδικα της εφαρμογής. Ξέχωρα, ο πάροχος είναι υποχρεωμένος να υπογράψει ψηφιακό τον κώδικα της εφαρμογής έχοντας το ιδιωτικό κλειδί. Μετά πέμπει το δημόσιο κλειδί στην KMA για να προστεθεί στο πιστοποιητικό ALC. Τέλος, η κάρτα έχει τη δυνατότητα να εξακριβώσει την αυθεντικότητα της κάρτας μέσω της επαλήθευσης της ψηφιακής υπογραφής του παρόχου με χρήση του δημόσιου κλειδιού.



Εικόνα 9 : Η λειτουργία Multus

5.4.1.2 Java card

Είναι προϊόν της Sun Microsystem. Αναφέρεται σε μια τεχνολογία λογισμικού που επιτρέπει σε μικρές εφαρμογές βασισμένες στην Java οι οποίες καλούνται Java Card applets για να τρέξει με ασφάλεια στις έξυπνες κάρτες ή σε άλλες συσκευές οι οποίες περιέχουν μικρό περιβάλλον μνήμης και μικρής ισχύς. Οι δυνατότητες που μπορεί να περιλαμβάνει είναι μεταξύ της δυναμικής φόρτωσης κλάσεων και της κλάσης Security Manager. Ενώ, δεν υποστηρίζονται από τους πίνακες , τους τύπους δεδομένων χαρακτήρων, τη κινητή υποδιαστολή και τους ακέραιους μεγάλου μεγέθους. Η Java card απαρτίζεται από την εικονική μηχανή Java Card , το περιβάλλον εκτέλεσης Java Card και το Java Card Application Programming Interface.

5.4.1.3 Linux

Το Linux αποτελεί ένα λειτουργικό σύστημα το οποίο απαρτίζεται από ένα ελεύθερο λογισμικό με ανοιχτού κώδικα. Μπορεί να εγκαθιστά και να λειτουργεί στα περισσότερα είδη του υπολογιστικού συστήματος δηλαδή από μικρές συσκευές π.χ. κινητά έως στους μικροεπεξεργαστές. Ένα από τα σημαντικά χαρακτηριστικά είναι οι άπειρες επιλογές που προσφέρει στους χρήστες του. Περιβάλλεται από εφαρμογές και προγράμματα. . Για να εισαχθεί στους μικροεπεξεργαστές είναι απαραίτητο οι μικροεπεξεργαστές να διαθέτουν 32bit και πολλά Kbytes μνήμης ROM και RAM.

5.4.1.4 Smart card for windows

Είναι η συνένωση μεταξύ του λειτουργικού συστήματος συμβατού ISO-4 και μιας πλατφόρμας ανάπτυξης εφαρμογών μέσα σε μια έξυπνη κάρτα. Η βάση του λειτουργικού συστήματος προσφέρει ένα σύστημα αρχείων, έναν έλεγχο πρόσβασης, μεταφορά δεδομένων I/O, κάποιες κρυπτογραφικές υπηρεσίες , ένα API και μια συλλογή από εντολές ISO. Κύριο γνώρισμα του είναι ότι εγκρίνει σε άλλες εταιρείες να

εφαρμόσουν ένα δικό τους λειτουργικό σύστημα χρησιμοποιώντας ένα βασισμένο σε Windows και ένα σύνολο εργαλείων σε Visual Basic.

5.5 Σύστημα αρχείων έξυπνων καρτών (smart card system file)

Οι έξυπνες κάρτες περιλαμβάνουν ένα ολοκληρωμένο σύστημα σωστής χρήσης των αρχείων το οποίο είναι σχεδιασμένο κατάλληλα γι αυτές. Το Σύστημα Αρχείων Έξυπνων Καρτών – Smart Card System File είναι καθορισμένο σύμφωνα με το πρότυπο ISO 7816-4 και υλοποιείται κυρίως στη μνήμη EEPROM της κάρτας. Αυτό το σύστημα καθορίζεται σε τρία δομικά στοιχεία τα οποία είναι τα ακόλουθα, το βασικά αρχείο-master file (MF) ,το αρχείο καταλόγου-dedicated file (DF) και το αρχείο δεδομένων-elementary file (EF). Στη συνέχεια, αναλύεται ο κάθε τύπος των αρχείων.

Βασικό Αρχείο / Master File (MF): Το σύστημα αρχείων έξυπνων καρτών περιλαμβάνει μονάχα ένα βασικό αρχείο. Το Master File συνίσταται ως η αφετηρία της ιεραρχικής δομής του συστήματος. Αυτό μπορεί να εμπεριέχει και αρχεία καταλόγου (DF) αλλά και αρχεία δεδομένων (EF). Μάλιστα, τα αρχεία δεδομένων εντοπίζονται κάτω από το βασικό αρχείο και κατά κανόνα, η χρήση τους είναι κυρίως για την αποθήκευση κλειδιών και δεδομένων τα οποία είναι κοινά σε άλλες εφαρμογές της κάρτας. Σχετικά με το πρότυπο ISO 7816-4, σε κάθε συμβατή κάρτα το αναγνωριστικό του βασικού αρχείου (MF) είναι 0χ3F00 σε δέκα-εξαδική τιμή.

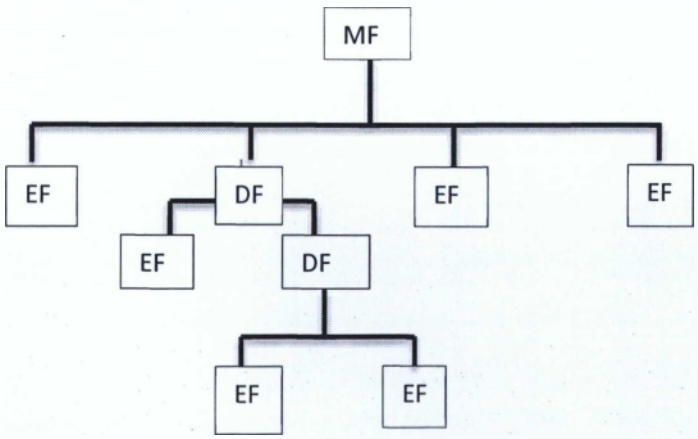
Αρχείο Καταλόγου/ Dedicated File (DF): Τα αρχείο καταλόγων βρίσκονται κυρίως σε συστήματα UNIX ή PC. Το Dedicated File(DF) σχηματίζει ένα υποκατάλογο κάτω από τη ρίζα της ιεραρχίας που είναι το βασικό αρχείο (MF). Επιπλέον, έχει τη δυνατότητα να εμπεριέχει από ένα έως πολλά αρχεία δεδομένων (EF) ή αρχεία καταλόγου (DF). Η χρήση αυτών των αρχείων υλοποιείται κυρίως για τον διαχωρισμό των δεδομένων των διαφορετικών εφαρμογών. Ενώ υφίσταται η δυνατότητα να δημιουργήσουμε δεντρικές δομές των αρχείων όπως γίνεται και στο UNIX.

Αρχείο Δεδομένων / Elementary File (EF): Το συγκεκριμένο αρχείο βρίσκεται στο τελευταία βαθμίδα της ιεραρχίας ενός συστήματος αρχείων έξυπνης κάρτας. Όμως είναι το μόνο αρχείο συγκριτικά με τα προηγούμενα που περιλαμβάνει μονάχα δεδομένα. Επιπλέον, αυτό εμπερικλείει δύο μορφές οι οποίες είναι πρώτον το Internal EF που η ιδιότητα του είναι να χρησιμοποιείται από τις εφαρμογές πάνω στην κάρτα και δεύτερον το Working EF που η αρμοδιότητα του είναι να χρησιμοποιείται για την αποθήκευση πληροφοριών που πηγάζουν από εφαρμογές εκτός κάρτας. Τα αρχεία δεδομένων κατηγοριοποιούνται σε τέσσερις μορφές οι οποίες είναι τα εξής:

1. ***Δυαδική (Transparent):*** Τα αρχεία αυτά αποθηκεύουν μια συγκεκριμένη σειρά από bytes. Όπως στις περιοχές μνήμης έτσι και στα αρχεία δεδομένων με μορφή δυαδική υλοποιείται η ανάγνωση και η εγγραφή. Από τη στιγμή που θα δοθεί μία εντολή ανάγνωσης και εγγραφής με τύπο αρχείου δυαδικού

τότε είναι απαραίτητο να παραχωρηθεί μια τιμή Offset και το αντίστοιχο μήκος length των δεδομένων σε bytes που θα διαβαστούν.

2. ***Γραμμικά σταθερά αρχεία (Fixed Record):*** Είναι ταξινομημένα αρχεία που καθορίζονται σε εγγραφές-records αλλά με τη διαδοχικότητα με τις οποίες αυτές δημιουργήθηκαν. Το μήκος των αρχείων σε μορφή bytes είναι σταθερό. Δηλαδή, η κάθε εγγραφή μπορεί να περιλαμβάνει από 1 έως 254 bytes.Τέλος, η πρόσβαση στα δεδομένα υλοποιείται μέσα από τον καθορισμό του αναγνωριστικού του αρχείου και του αύξοντα αριθμού της εγγραφής.
3. ***Γραμμική μεταβλητού μήκους (Linear variable-length*)**: Είναι ταξινομημένα αρχεία που καθορίζονται σε εγγραφές αλλά το μήκος των εγγραφών είναι μεταβλητό και μπορεί να κυμαίνεται από 1 έως 54 bytes. Η ιδιότητα των γραμμικών μεταβλητών αρχείων επιτρέπει την καλύτερη διαχείριση της διαθέσιμης μνήμης αφού πρώτα έχει δεσμευθεί με ένα ποσοστό χώρου όταν χρειάζεται. Όμως, τα αρχεία χρησιμοποιούν επιπρόσθετο χώρο για την καταγραφή του μήκους κάθε εγγραφής. Η πρόσβαση στα δεδομένα υλοποιείται μέσα από τον καθορισμό του αναγνωριστικού του αρχείου και τον αύξοντα αριθμού της εγγραφής, όπως και στην περίπτωση των αρχείων γραμμικής σταθερού μήκους. Εντωμεταξύ, τα αρχεία με γραμμική μεταβλητού μήκους προσδιορίζονται από εξαιρετικά μικρό χρόνο ανάγνωσης και εγγραφής και εξοικονομούν χώρο στη μνήμη.
4. ***Κυκλικά αρχεία (Cyclic Record):***Είναι ταξινομημένα αρχεία που καθορίζονται σε εγγραφές με δομή δακτυλιδιού. Κύριο γνώρισμα της δομής είναι η εμφάνιση ενός δείκτη που κατευθύνει πάντα στην εγγραφή με την οποία τροποποιήθηκε τελευταία. Μια πράξη εγγραφής εφαρμόζεται πάντα στην επόμενη θέση, ενώ μια πράξη ανάγνωσης διαβάζει πάντα το περιεχόμενο της τελευταίας εγγραφής. Αν ολόκληρη μνήμη που έχει δεσμευτεί για το κυκλικό αρχείο έχει συμπληρωθεί, τότε η επόμενη εγγραφή θα σβήσει την πρώτη εγγραφή που έχει πραγματοποιηθεί. Αυτά τα αρχεία εφαρμόζονται αρκετά συχνά σε εφαρμογές που σχετίζονται με την καταγραφή λειτουργίας.



Διάγραμμα 15: Ταξινόμηση των μορφών συστημάτων αρχείων έξυπνων καρτών

5.5.1 Εντολές διαχείρισης συστημάτων αρχείων έξυπνων καρτών

Σύμφωνα με το πρότυπο του ISO 7816-4 προσδιορίζεται ένα άθροισμα εντολών για ενέργειες όπως είναι η επιλογή, η ανάγνωση και η εγγραφή ενός αρχείου. Στη συνέχεια αναφέρονται και αναλύονται οι εντολές αυτές. Οι εντολές είναι οι ακόλουθες:

- **Select file:** η εντολή αυτή προβάλλει ένα δείκτη σε ένα καθορισμένο αρχείο μέσα στο σύστημα αρχείων της κάρτας. Όταν επιλεχτεί το αρχείο χρησιμοποιώντας την εντολή τότε η εγγραφή και ανάγνωση πραγματοποιείται στο αρχείο που υποδηλώνεται από αυτόν τον δείκτη.
- **Read Binary:** Σχετίζεται με τα δυαδικά αρχεία. Χρησιμοποιείται από μία εφαρμογή ώστε να διαβάσει ένα καθορισμένο κομμάτι του αρχείου. Όμως η συγκεκριμένη εντολή περιλαμβάνει την παράμετρο της τιμής offset που ισοδυναμεί με το πρώτο byte που θα αρχίσει η ανάγνωση και ο αριθμός των bytes που θα διαβαστεί και θα επιστραφεί σαν παρεπόμενο στη εφαρμογή ανάγνωσης.
- **Update Binary:** Συνδέεται με τα δυαδικά αρχεία. Η χρήση της σε μια εφαρμογή επιδιώκει την άμεση διαγραφή και αποθήκευση πληροφοριών σε ένα καθορισμένο κομμάτι του αρχείου EF. Υπάρχουν εσωτερικοί παράμετροι της εντολής που παρέχουν μία offset τιμή με την οποία θα εκκινήσει η εφαρμογή της εντολής και ένα μετρητή byte με το πλήθος των byte που θα εγγραφούν.
- **Write Binary**: Είναι μια ακόμη εντολή που συνδέεται με τα δυαδικά αρχεία. Αυτή η εντολή διαχειρίζεται από μία εφαρμογή ώστε να εγγραφούν δεδομένα σε ένα καθορισμένο κομμάτι του αρχείου EF. Αυτό σχετίζεται με τις απαιτήσεις της εφαρμογής με την οποία εντολή έχει τη δυνατότητα να εισάγει στα επιθυμητά bytes είτε την τιμή 1 είτε την τιμή 0 είτε να συντάσσει μια αλληλουχία από bytes μέσα στο transparent αρχείο.
- **Erase Binary**: Και αυτή η εντολή χρησιμοποιείται σε δυαδικά αρχεία. Η χρήση της σε μια εφαρμογή στοχεύει στη διαγραφή μιας διαδοχικότητας byte. Στην ουσία , τα byte να έχουν σαν τιμή το 0 σε ένα καθορισμένο κομμάτι του αρχείου EF. Οι παράμετροι της εντολής Erase Binary περικλείουν την τιμή offset που ισοδυναμεί με το πρώτο byte που θα κάνει εκκίνηση η διαγραφή και ένα μετρητή byte με το πλήθος των byte που θα διαγραφούν.
- **Read Record**: Η εντολή περιλαμβάνεται κυρίως σε γραμμικά αρχεία. Η χρήση του σε μια εφαρμογή αποσκοπεί στην ανάγνωση και την επιστροφή μίας ή περισσότερων εγγραφών ενός αρχείου EF. Για να διαβαστεί και να επιστραφεί μία εγγραφή δηλαδή μέρος των εγγράφων ή όλες οι εγγραφές ενός αρχείου εξαρτάται από τις παραμέτρους της εντολής.
- **Write Record**: Η εντολή πέμπεται από μία εφαρμογή με στόχο την εγγραφή μίας εγγραφής σε ένα EF αρχείο. Η εντολή υλοποιείται σε γραμμικά αρχεία.

- **Append Record**: Η χρήση της εντολής σε μια εφαρμογή είναι να προσθέτει μια νέα εγγραφή στο τέλος ενός σταθερού αρχείου (γραμμικό) είτε για την εγγραφή της πρώτης εγγραφής ενός μεταβλητού αρχείου (κυκλικό).
- **Update Record:** Είναι εκείνη η εντολή που στοχεύει την άμεση διαγραφή μίας εγγραφής από ένα γραμμικό αρχείο και την εγγραφή μια νέας, αλλά το περιεχόμενο της εξαρτάται από το σώμα της εντολής.

5.5.2 Ολοκληρωμένα συστήματα έξυπνων καρτών

Τα ολοκληρωμένα συστήματα έξυπνων καρτών διαιρούνται σε δύο κατηγορίες, η μία είναι το σύστημα της κάρτας (card system) και η άλλη είναι το κεντρικό σύστημα (host system). Παρακάτω διευκρινίζονται οι δυο αυτές έννοιες.

1) **Card System:** Η κάρτα του συστήματος εμπεριέχει τρία βασικά μέρη δηλαδή το λογισμικό του συστήματος, τα δεδομένα και οι εφαρμογές τα οποία εντοπίζονται πάνω στην έξυπνη κάρτα και είναι αποθηκευμένα στη μνήμη του ολοκληρωμένου συστήματος.
2) **Host System:** Το κεντρικό σύστημα απαρτίζεται από δύο τμήματα, το ένα είναι το λογισμικό του συστήματος και το άλλο είναι οι εφαρμογές που είναι αποθηκευμένες και υλοποιούνται μέσω του ηλεκτρονικού υπολογιστή ή μέσω μιας αυτόνομης συσκευής η οποία θα επικοινωνεί με την κάρτα.

Για να ξεκινήσει η επικοινωνία ανάμεσα στον ηλεκτρονικό υπολογιστή και στην έξυπνη κάρτα πρέπει να υπάρχει card reader (αναγνώστης κάρτας). Ο αναγνώστης της κάρτας μπορεί να απαρτίζεται από ένα αυτόνομο τερματικό που συνδέεται με έναν ηλεκτρονικό υπολογιστή ή μπορεί να είναι ενσωματωμένος σε κάποια τερματική συσκευή. Η επικοινωνία αυτή συμβαδίζετε με εκείνη του μοντέλου client-server, ενώ η ανταλλαγή εντολών και δεδομένων πραγματοποιούνται με το πρωτόκολλο APDU από και προς την κάρτα.

5.6 Συνθήκες πρόσβασης – Access Conditions

Η ιδιότητα των συνθηκών πρόσβασης είναι να ελέγχει τη ροή πρόσβασης στα αρχεία των πληροφοριών. Συνίσταται ως το ιδανικό μέσο για υλοποίηση ασφαλών υποδομών. Κατά τη διάρκεια του σχηματισμού των δομών όπου θα αποθηκεύονται τα δεδομένα υφίσταται η δυνατότητα επισήμανσης λεπτομερειών και συγκεκριμένων επιπέδων πρόσβασης για λειτουργίες πάνω στην κάρτα και για οποιαδήποτε αποθηκευμένη πληροφορία. Επομένως, όταν μια εξωτερική εφαρμογή ζητήσει πρόσβαση στα αρχεία της κάρτας για την υλοποίηση κάποιας λειτουργίας θα πρέπει αρχικά να

πληροί τις συνθήκες πρόσβασης τις οποίες σχετίζονται με το καθορισμένο προϊόν. Οι συνθήκες αυτές εξωτερικεύονται συνήθως με τη διαχείριση κωδικών-passwords γνωστά ως PIN-Personal Identification Numbers.

5.7 Το Κεντρικό σύστημα των έξυπνων καρτών

Το σύστημα της έξυπνης κάρτας διαχωρίζεται σε δύο τμήματα του λογισμικού τα οποία είναι αποθηκευμένες πάνω στην έξυπνη κάρτα δηλαδή στη μνήμη του ολοκληρωμένου κυκλώματος αλλά συνάμα υλοποιούνται. Τα δύο τμήματα είναι το λογισμικό του συστήματος και το λογισμικό των εφαρμογών. Παρακάτω , δίνεται η ακριβής διασάφηση αυτών των λογισμικών.

5.7.1 Λογισμικό συστήματος

Το λογισμικό σύστημα απαρτίζεται από το λειτουργικό σύστημα-Card Operating System και τα βοηθητικά προγράμματα- Utilities. Η αρμοδιότητα τους είναι να ασκούν έλεγχο στη διαχείριση μνήμης , στην αποστολή και λήψη δεδομένων, στην ακεραιότητα και την ασφάλεια των δεδομένων, να ενισχύουν το σύστημα αρχείων ISO και να δίνουν υποστήριξη σε εφαρμογές που είναι συμπεριλαμβανόμενες στην κάρτα. Το καθορισμένο λογισμικό προμηθεύεται από τους σχεδιαστές του ολοκληρωμένου κυκλώματος της και εγκαθίστανται στη μνήμη ROM με τη μέθοδο masking. Επιπλέον, τα δεδομένα που συνδέονται με τον έλεγχο της λειτουργίας της κάρτας δεν είναι προσβάσεως από εξωτερικές εφαρμογές εξαιτίας των μέτρων ασφαλείας. Επίσης, σύμφωνα με το πρότυπο ISO 7816-4 μπορούν να εφαρμοστούν μία αλληλουχία συναρτήσεων που θα ενισχύουν το σύστημα αρχείων και θα υλοποιούνται σε συγκεκριμένες διαδικασίες. Συνάμα, μία ομάδα εντολών μπορεί να παρέχει και βοηθητικές συναρτήσεις χρήσιμες για περίπλοκες εφαρμογές.

5.7.2 Λογισμικό Εφαρμογών

Το λογισμικό απαρτίζεται από δύο μέρη: τα δεδομένα και τις συναρτήσεις που εφαρμόζονται πάνω σ' αυτόν. Υλοποιείται με τη χρήση της συμβολικής γλώσσας του μικροεπεξεργαστή της κάρτας ή με τη χρήση υψηλού επιπέδου γλώσσας η οποία αναλύεται από τον μικροεπεξεργαστή . Άρα, είτε με τον ένα τρόπο είτε με το άλλον είναι απαραίτητο να υπάρχει η προμήθεια ειδικών εργαλείων ανάπτυξης από το δημιουργό του λειτουργικού συστήματος.

5.8 Οι καρτ-εφαρμογές

Σχετίζονται με τη βασική δομή των αρχείων που θα υποδέχονται τα δεδομένα στη μνήμη της κάρτας. Για να εφαρμοστεί αυτό, απαιτείται εξειδικευμένα εργαλεία λογισμικού τα οποία προμηθεύει ο σχεδιαστής της κάρτας. Σε όλη αυτή την λειτουργία απαιτείται να υπάρχει ένας σχηματισμός αλληλουχίας των αρχείων, ο καθορισμός των συνθηκών πρόσβασης σε κάθε στάδιο της διαδοχικότητας και ο σχηματισμός των απαραίτητων αρχείων των οποίων συμπεριλαμβάνονται και οι κωδικοί-PIN. Οι προσωπικοί κωδικοί θα φορτώνουν κατά τη διαδικασία της τελικής προσωποποίησης.

Η καθορισμένη διαδικασία προβάλλει δύο βασικά στοιχεία τα οποία είναι τα ακόλουθα:

- Οι εργαλειοθήκες. Οι απαραίτητες εργαλειοθήκες εξελίσσονται από τους δημιουργούς των λειτουργικών συστημάτων. Συνδέονται σε ειδικές συμβουλές γλώσσες και προσομοιωτές πηγάζοντας από τις κατασκευές ολοκληρωμάτων. Δεν διατίθενται ελεύθερα στους προγραμματιστές εφαρμογών και περιλαμβάνουν ένα υψηλό κόστος.
- Τα λειτουργικά συστήματα. Αυτά εμφανίζουν ξέχωρα χαρακτηριστικά κυρίως στις εσωτερικές τους λειτουργίες όπως είναι οι συνθήκες πρόσβασης. Άρα, η ύπαρξη της ανάπτυξης της δομής των αρχείων απαιτείται ένα προγραμματιστή ο οποίος είναι εξειδικευμένος με τη γνώση των λεπτομερειών της καθορισμένης κάρτας.

5.8.1 Τελικές εφαρμογές

5.8.1.1 Ανάπτυξη προγραμμάτων διασύνδεσης (interface)

Μετά το στάδιο του σχηματισμού της απαραίτητης δομής των αρχείων πάνω στην κάρτα, το επόμενο βήμα είναι η ανάπτυξη των προγραμμάτων διασύνδεσης και επικοινωνίας με τον υπολογιστή μέσω του επιλεγμένου αναγνώστη καρτών (card reader) δηλαδή η χρήση των module κωδικοποίησης και αποκωδικοποίησης. Εξαιτίας της έλλειψης προσωποποιημένων υψηλού επιπέδου προγραμματιστών διεπαφών APIs, οι προγραμματιστές επεξεργάζονται εντολές , πρωτόκολλα επικοινωνίας και άλλες υπηρεσίες , που σχετίζονται με τον δημιουργό του ολοκληρωμένου αλλά και με το λειτουργικό σύστημα που έχει η κάρτα, σε χαμηλό βαθμό. Άρα η κάρτα είναι αναγκαία να περιλαμβάνει ένα συγκεκριμένο τμήμα module ώστε να μπορεί να διαχειριστεί τις εντολές χαμηλού επιπέδου οι οποίες είναι σε μορφή bytes καθώς με αυτό τον τρόπο εφαρμόζεται ένα υψηλό επίπεδο με τις εντολές αλληλεπίδρασης του αναγνώστη και της κάρτας,

Είναι απαραίτητο πρώτον ,η σωστή γνώση των λειτουργιών του αναγνώστη (card reader) που θα χρησιμοποιηθεί και δεύτερον, η χρήση των βιβλιοθηκών που θα διαθέτει ο δημιουργός ώστε να εφαρμοστεί η δρομολόγηση των πακέτων APDU από και προς την κάρτα. Οι βιβλιοθήκες εμπεριέχουν μεθόδους και συναρτήσεις πρόσβασης στον αναγνώστη στις οποίες αποτελούν μέρος των drivers. Οι βασικές συναρτήσεις πρέπει να εφαρμόζονται τα ακόλουθα :

- Συναρτήσεις επιβεβαίωσης πρόσβασης στην κάρτα. Η ιδιότητα αυτών των συναρτήσεων είναι να κάνουν έλεγχο μέσω των κωδικών PIN .
- Συναρτήσεις εγγραφής & ανάγνωσης. Η ιδιότητα των συγκεκριμένων συναρτήσεων είναι να διαβάσουν ή να γράψουν ενός μέρους ή το συνόλου της μνήμης της κάρτας
- Συναρτήσεις πληροφοριών κάρτας. Ο αναγνώστης πέμπει πληροφορίες οι οποίες συνδέονται με τον τύπο της κάρτας που υπάρχει στον αναγνώστη και το πρωτόκολλο επικοινωνίας που εφαρμόζεται.

5.8.1.2 Ανάπτυξη εφαρμογών των τελικών χρηστών

Οι εφαρμογές των τελικών χρηστών είναι το δεύτερο μέρος της διαδικασίας ανάπτυξης προγραμμάτων. Αυτές διακρίνονται σε δύο κατηγορίες.

Η πρώτη κατηγορία συνδέεται με την ανάπτυξη του επιπέδου που εμπεριέχει το σύνολο της εφαρμογής Application Logic όπως είναι οι κανόνες ελέγχου και η ροή των δεδομένων. Ύστερα, η επικοινωνία με την κάρτα υλοποιείται μέσω της API διασύνδεσης. Το επακόλουθο της καθορισμένης διαδικασίας είναι ο σχηματισμός ενός module λειτουργικότητας που εφαρμόζει ολοκληρωμένες εργασίες σε αντίθεση με τις καρτ-εφαρμογές. Ενώ η δεύτερη κατηγορία σχετίζεται με την ανάπτυξη του γραφικού περιβάλλοντος όπου ο τελικός χρήστης ασκεί επιρροή μαζί με το σύστημα είτε παίρνοντας δεδομένα είτε βάζοντας δεδομένα και εντολές προς την κάρτα.

5.9 Πρότυπα έξυπνων καρτών

Μια έξυπνη κάρτα περιβάλλεται από ένα μεγαλύτερο και περίπλοκο σύστημα . Δηλαδή ανάμεσα στην έξυπνη κάρτα και στο υπόλοιπο σύστημα είναι καθορισμένο από ένα σύνολο προδιαγραφών και προτύπων ώστε οι έξυπνες κάρτες, οι συσκευές αποδοχής κάρτας και εφαρμογές να λειτουργούν συνάμα. Άρα, ένα πρότυπο αποτελείται από ένα σύνολο κανόνων εξασφαλίζοντας τη διαλειτουργικότητα και αυτή απαρτίζεται σε τέσσερα στάδια:

1. **Ύπαρξη της κάρτας**
2. **Ύπαρξη συσκευής ανάγνωσης της κάρτας**
3. **Ύπαρξη δικτύου**
4. **Να υπάρχει σύστημα εκδότη της κάρτας**

Περαιτέρω, αναλύονται οι μονάδες που ενισχύουν την τεχνολογία των έξυπνων καρτών και τα σημαντικότερα πρότυπα για την ανάπτυξη συστημάτων αυτών των καρτων.

5.9.1 Διεθνής Οργανισμός Προτυποποίησης (ISO)

Ο διεθνής οργανισμός προτυποποίησης γνωστό ως ISO (International Standard Organization) είναι ένα πρότυπο το οποίο ορίζει τα απαραίτητα χαρακτηριστικά των καρτών με ολοκληρωμένο κύκλωμα καθώς και των ηλεκτρικών επαφών. Το πρότυπο ISO 7816 διαιρείται σε 7 τμήματα και είναι τα ακόλουθα:

- **Τμήμα 1: Φυσικά χαρακτηριστικά**

Ορίζει τις φυσικές διαστάσεις μιας έξυπνης κάρτας με επαφή καθώς και την αντοχή της στο στατικό ηλεκτρισμό, την ηλεκτρομαγνητική ακτινοβολία, και την μηχανική εξασθένιση. Επιπροσθέτως, αναλύει τη φυσική θέση της μαγνητικής ταινίας και του ολοκληρωμένου κυκλώματος όταν η κάρτα συσχετίζεται και με τις δύο τεχνολογίες.

- **Τμήμα 2: Κάρτες με επαφές : Διαστάσεις και θέσεις επαφών**

Προσδιορίζει τη θέση, το μέγεθος αλλά και τα ηλεκτρικά χαρακτηριστικά των μεταλλικών επαφών μιας έξυπνης κάρτας αλλά συνάμα αναλύει τη μέθοδο που θα χρησιμοποιηθεί ώστε να γίνει η καταμέτρηση των αποστάσεων των επαφών της κάρτας.

- **Τμήμα 3: Κάρτες με επαφές: Ηλεκτρική διεπαφή και πρωτόκολλα μετάδοσης**

Καθορίζει τα βασικά ηλεκτρικά χαρακτηριστικά (πχ. Τάση τροφοδοσίας) , το σταμάτημα του ρολογιού και το σήμα μηδενικού (Reset signal). Το μεγαλύτερο μέρος του ISO 7816-3 σχετίζεται με το μέσο μεταφοράς δεδομένων στο φυσικό στρώμα προσδιορίζοντας πρωτόκολλα μεταφοράς T=0 και T=1. Και επίσης θεωρείται ένα πολύ σημαντικό πρότυπο για τα ηλεκτρικά ορίσματα του chip μιας έξυπνης κάρτας

- **Τμήμα 4: Οργάνωση, ασφάλεια και εντολές για την ανταλλαγή**

Προσδιορίζει ένα αριθμό εντολών για την κεντρική μονάδα επεξεργασίας της κάρτας όπου δίνουν την πρόσβαση, την ασφάλεια, και την μετάδοση των δεδομένων από και προς την κάρτα. Σ' αυτό το τμήμα αναλύονται οι απαραίτητοι μηχανισμοί για την χρησιμοποίηση έξυπνων καρτών σε βιομηχανικές εφαρμογές.

- **Τμήμα 5: Εγγραφή παρόχους εφαρμογών**

Καθορίζει το αριθμητικό σύστημα το οποίο μέσω από την χρήση του προσδιορίζονται οι εφαρμογές που υλοποιούνται σε μια έξυπνη κάρτα. Το σύστημα λέγεται AID και απαρτίζεται από το Registered Application Provider Identifier (RID) όπου έχει μήκος από 5 bytes και ορίζει το δημιουργό της εφαρμογής και από το Proprietary Identifier Extension (PIX) το οποίο έχει μήκος μεταξύ του 0 έως 11 bytes και όριζει την εφαρμογή.

- **Τμήμα 6: Διακλαδικά στοιχεία δεδομένων για ανταλλαγή**

Καθορίζει τα στοιχεία δεδομένων (DES) που χρησιμοποιούνται για την ανταλλαγή διακλαδικής βάσης και για τις ενσωματωμένες κάρτες κυκλωμάτων (ICCs) είτε με τις επαφές είτε χωρίς επαφές. Επίσης, παραχωρεί το αναγνωριστικό , το όνομα , την περιγραφή, τη μορφή, την κωδικοποίηση και τη διάταξη και προσδιορίζει τα μέσα απόκτησης από την κάρτα.

- **Τμήμα 7:Διακλαδικές εντολές μέσω SQL**

5.9.2 Πρότυπο FIPS

Το πρότυπο FIPS (Federal Information Processing Standards) δημιουργήθηκε με στόχο την προστασία των ομοσπονδιακών πόρων, συμπεριλαμβάνοντας τα υπολογιστικά και τηλεπικοινωνιακά συστήματα. Περιλαμβάνει κατευθυντήριες επεξηγήσεις οι οποίες έχουν τυπωθεί από το National Institute of Standards and Technology (NIST) Μία έκδοση του FIPS είναι το πρότυπο FIPS-140 όπου παρακάτω δίνεται μια λεπτομερή ανάλυση.

5.9.2.1 FIPS 140

Το πρότυπο FIPS 140 (1-3) περιέχει απαιτήσεις οι οποίες αναφέρονται πάνω σε τμήματα που συνοδεύονται με τη δημιουργία ασφαλείας και μιας μεθόδου κρυπτογράφησης. Στην ουσία, περιγράφουν την φυσική ασφάλεια, τα λειτουργικά συστήματα, τη διαχείριση κλειδιών κρυπτογράφησης, την ηλεκτρομαγνητική αποδοχή, την εγγύηση δημιουργίας καθώς και την μείωση των επιθέσεων. Άρα, η ουσία του προτύπου είναι η αναφορά των λεπτομερειών στο κομμάτι των τεχνητών εφαρμογών.

5.9.3 EMV

Το πρότυπο EMVπροέρχεται από τις λέξεις την Europay ,την Master Card και τη VISA. Είναι ένα διεθνές πρότυπο το οποίο εξασφαλίζει την ασφάλεια και τη διαλειτουργικότητα των μικροεπεξεργαστών που σχετίζονται σε κάρτες χρηματικών δοσοληψιών . Το περιεχόμενο εντολών EMV συσχετίζονται με το πρότυπο ISO 7816 και περιέχει τις ακόλουθες εντολές:

- Μπλοκ αίτησης
- Άρση αποκλεισμού εφαρμογής
- Μπλοκ κάρτα
- Εξωτερική πιστοποίηση της αυθεντικότητας (ISO: 7816-4)
- Εκβάλλουν μια εφαρμογή κρυπτογραφήματος
- Παραλαβή δεδομένων (ISO:7816-4)
- Παραλαβή επιλογής επεξεργασίας
- Εσωτερική ταυτότητα (ISO: 7816-4)
- Αλλαγή PIN& Ξεμπλοκάρισμα

- Επιλογή (ISO: 7816-4)
- Επαλήθευση (ISO: 7816-4)

5.9.4 Personal Computer/ Smart Card (PC/SC)

Το πρότυπο Προσωπικός Υπολογιστής/ Έξυπνης Κάρτας (Personal Computer/Smart Card) εφαρμόζεται σε υπολογιστές με λειτουργικό σύστημα Windows. Επίσης, επιτρέπει στις κάρτες να λειτουργούν οποιαδήποτε εφαρμογή ανεξάρτητα τι είδους γλώσσα προγραμματισμού είναι., να έχει ασφαλή αποθήκευση, να υπάρχουν διεπαφές προγραμματισμού για έξυπνες συσκευές ανάγνωσης καρτών και υπολογιστών, να υπάρχει μια υψηλού επιπέδου διεπαφής της εφαρμογής για την ανάπτυξη εφαρμογών. Ο προσχεδιασμός του συγκεκριμένου προτύπου συσχετίζεται με το πρότυπο ISO/IEC 7816 και υποστηρίζει EMV και GSM εφαρμογές προτύπων.Όμως αυτό που είναι αναγκαίο είναι η ύπαρξη ενός κατάλληλου οδηγού για το τερματικό αλλά και κάρτα να είναι αντίστοιχη με το PC/SM.

5.9.5 OCF (Open Card Framework)

Παρέχει ένα Java API για την πρόσβαση τόσο στους αναγνώστες έξυπνων καρτών όσο και για τις απαιτήσεις ενσωματωμένο στις έξυπνες κάρτες. Ο σκοπός της δημιουργίας του ήταν η δημιουργία μίας διεπαφής μεταξύ της έξυπνης κάρτα και του υπολογιστή ανεξάρτητα τι είδους λειτουργικού συστήματος είχε ο υπολογιστής. Διαιρείται σε δύο τμήματα. Η μία είναι η συσκευή ανάγνωσης έξυπνων καρτών και η άλλη μια διεπαφή υψηλού επιπέδου για εφαρμογές που συνδέονται με το ISO 7816 -3 και ISO 7816-4.

5.9.5 Open Platform

Open Platform που σημαίνει Ανοικτή Πλατφόρμα απεικονίζει ένα λειτουργικό σύστημα που συνδέεται με τα ανοιχτά πρότυπα τα οποία στηρίζονται στις διασυνδέσεις προγραμματισμού εφαρμογών (API). Αυτές οι διασυνδέσεις εγκρίνουν τη χρήση λογισμικού ώστε να εφαρμοστεί με άλλες μεθόδους από τον προγραμματιστή που προορίζεται χωρίς να χρειαστεί να τροποποιηθεί ο κώδικας. Το Open Platform υποστηρίζει πολλαπλές εφαρμογές των APIs. Επίσης, δίνει την δυνατότητα στον προγραμματιστή να τροποποιήσει την λειτουργικότητα , αφού οι προδιαγραφές είναι διαθέσιμα στα ανοικτά πρότυπα.

Στην περίπτωση των έξυπνων καρτών προσδιορίζει ένα ολοκληρωμένο περιβάλλον για την ανάπτυξη και λειτουργία συστημάτων έξυπνων καρτών με δυνατότητα υποστήριξης εφαρμογών. Επίσης ορίζει πρότυπα για την κάρτα και το τερματικό. Παράλληλα, προσδιορίζει την εκτός κάρτα επικοινωνίας με το τερματικό και τη διαχείριση της εφαρμογής εντός κάρτας.

ΚΕΦΑΛΑΙΟ 6 Η ΑΣΦΑΛΕΙΑ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ

6.1 Εισαγωγή στην ασφάλεια

Η ασφάλεια των πληροφοριακών συστημάτων βασίζεται στην προστασία των δεδομένων από τυχόν αλλοιώσεις και καταστροφές καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Η ασφάλεια σχετίζεται με την εμπιστευτικότητα, τον έλεγχο ακεραιότητας, με τη μη αποκήρυξη και την πιστοποίηση αυθεντικότητας. Περαιτέρω γίνεται μια σαφές διευκρίνιση αυτών των παραπόνων όρων.

1. "Εμπιστευτικότητα: αφορά στο να κρατούνται οι πληροφορίες ιδιωτικές και μυστικές έτσι ώστε μόνο ο εξουσιοδοτημένος παραλήπτης να μπορεί να τις καταλαβαίνει. Για παράδειγμα, αν ο χρήστης Α στείλει ένα μήνυμα στο χρήστη Β τότε θα πρέπει ο Β (αποκλειστικά από το Β) να είναι σε θέση να διαβάσει και να καταλάβει την πληροφορία.
2. Πιστοποίηση αυθεντικότητας: αφορά στην απόδειξη της ταυτότητας του αποστολέα στον παραλήπτη, έτσι ώστε ο παραλήπτης να μπορεί να είναι σίγουρος ότι ο αποστολέας είναι πράγματι αυτός που ισχυρίζεται ότι είναι. Για παράδειγμα , αν ο χρήστης Β λάβει ένα μήνυμα από το χρήστη Α, θα πρέπει να είναι σε θέση να πιστοποιήσει την ταυτότητα του Α, και να ξέρει ότι το μήνυμα που έλαβε είναι πράγματι από αυτόν.
3. Έλεγχος ακεραιότητας: αφορά στο να διασφαλίσει ότι η πληροφορία του μηνύματος δε έχει αλλοιωθεί κατά τη διάρκεια της μεταφοράς της ή της αποθήκευσης της στο δίκτυο. Οποιοδήποτε μη εξουσιοδοτημένο άτομο δε θα πρέπει να είναι σε θέση να αλλάξει την πληροφορία κατά τη μεταφορά της .Για παράδειγμα , αν ο χρήστης Α στείλει ένα μήνυμα στο χρήστη Β, το περιεχόμενο θα πρέπει να μην αλλαχθεί και να μείνει ίδιο με αυτό που έστειλε ο Α.
4. Μη αποκήρυξη: Αφορά στο να διασφαλίσει ότι ο αποστολέας του μηνύματος δε θα αρνηθεί ότι πράγματι έστειλε την πληροφορία. Για παράδειγμα, αν ο χρήστης Α στείλει ένα μήνυμα στο χρήστη Β τότε ο Α δε θα μπορεί να αρνηθεί αργότερα ότι έστειλε μήνυμα" [6]

6.2 Κρυπτογραφία

Η κρυπτογραφία είναι ένας τομέας που διερευνά τη μελέτη, την ανάπτυξη και τη χρήση των μεθόδων κρυπτογράφησης και αποκρυπτογράφησης με στόχο την απόκρυψη των δεδομένων ενός μηνύματος. Συγκεκριμένα, εφαρμόζονται σε δεδομένα ή μηνύματα που διανέμονται ανάμεσα στις οντότητες ώστε να ικανοποιηθούν οι απαιτήσεις ακεραιότητας και εμπιστευτικότητας. Για παράδειγμα η κρυπτογραφία

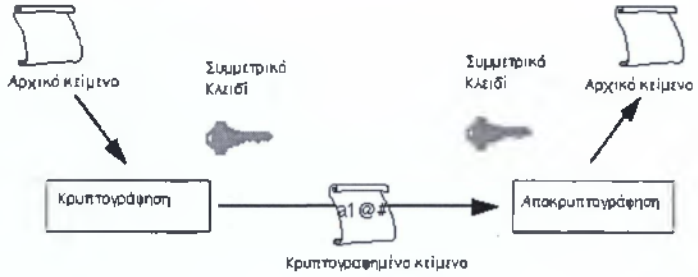
[6] https://dspace.lib.uom.gr/bitstream/2159/14273/1/TsigenopoulouVeraMsc2011.pdf

μπορεί να εφαρμοστεί όταν γίνει η μεταφορά των δεδομένων πάνω σε ανοιχτά δίκτυα ώστε να αποφευχθεί η υποκλοπή.

- Κρυπτογράφηση είναι η μετατροπή των δεδομένων σε μορφή των bit. Η αλληλουχία των bit καλείται κλειδί (key) και συνοδεύεται με κάποιον αλγόριθμο ή συνάρτηση. Ενώ η αντίστροφη διαδικασία λέγεται αποκρυπτογράφηση και είναι απαραίτητο να υπάρχει κλειδί είτε είναι ίδιο είτε διαφορετικό.

6.2.1 Συμμετρική Κρυπτογράφηση

Παρέχει κρυπτογραφικούς αλγορίθμους οι οποίοι εφαρμόζουν το ίδιο κλειδί και για την κρυπτογράφηση και για την αποκρυπτογράφηση δεδομένων. Αυτό το κλειδί ονομάζεται μυστικό κλειδί (secret key) και είναι γνωστό μόνο στον αποστολέα και στον παραλήπτη. Ο τύπος του κλειδιού είναι συμμετρικός επειδή οι δύο οντότητες που θέλουν να επικοινωνήσουν χρησιμοποιούν το ίδιο κλειδί για να την εφαρμόσουν. Παρακάτω υπάρχει η εικόνα που υλοποιείται η συμμετρική κρυπτογράφηση.



Εικόνα 10: Συμμετρική κρυπτογράφηση

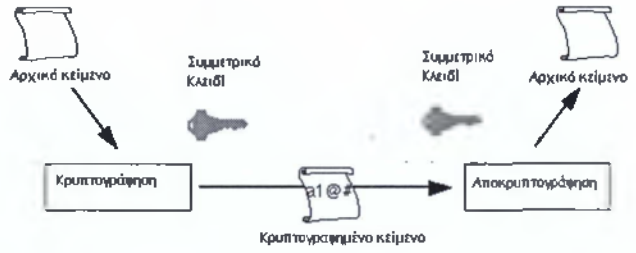
Υπάρχει ένα μήνυμα και κατευθύνεται προς την κρυπτογράφηση. Αφού κρυπτογραφηθεί μέσω του μυστικού κλειδιού κατευθύνεται στην έξοδο όπου το μήνυμα καταλήγει να είναι σε ακατανόητη μορφή, δηλαδή είναι ένα κρυπτογραφημένο μήνυμα.

Η συμμετρική κρυπτογραφία αποτελείται από δύο βασικά μειονεκτήματα . Το πρώτο είναι, όσο μεγαλώνει ο αριθμός των οντοτήτων , η διαχείριση των κλειδιών γίνεται όλο και πιο δύσκολο. Το δεύτερο μειονέκτημα είναι ότι επειδή και οι δυο οντότητες χρησιμοποιούν το ίδιο κλειδί , δεν μπορεί να αποδείξει κάποιος από ξεκίνησε το κρυπτογραφημένο μήνυμα. Το DES (Data Encryption System) και το DESX αποτελούν δύο παραδείγματα αλγορίθμων συμμετρικής κρυπτογραφίας.

6.2.2 Ασύμμετρη κρυπτογράφηση

Η ασύμμετρη κρυπτογραφία λέγεται και ως κρυπτογραφία δημόσιου κλειδιού. Εφαρμόζει δύο διαφορετικά αλλά μαθηματικά συσχετιζόμενα κλειδιά. Το ένα μπορεί να χρησιμοποιηθεί χωρίς να είναι δυνατή η εύρεση του άλλου. Το δημόσιο κλειδί μπορεί να ανακοινώσει σε οποιονδήποτε θέλει να κάνει μια δοσοληψία με την οντότητα που κρατάει το ιδιωτικό κλειδί. Το ιδιωτικό κλειδί πρέπει να είναι κρυφό και μπορεί να το διαχειριστεί ο ιδιοκτήτης του. Ένας γνωστός αλγόριθμος της ασύμμετρης κρυπτογράφησης είναι ο RSA.

Για να κρυπτογραφηθούν κάποια δεδομένα , γίνεται χρήση μόνο του δημοσίου κλειδιού, ενώ το ιδιωτικό κλειδί εφαρμόζεται για την αποκρυπτογράφηση τους . Οποιαδήποτε από τις οντότητες που γνωρίζουν το δημόσιο κλειδί μπορεί να κρυπτογραφήσει δεδομένα με παραλήπτη το ένα και αποκλειστικό κάτοχο του ιδιωτικού κλειδιού. Επιπλέον, η κρυπτογραφία δημοσίου κλειδιού χρησιμοποιείται για την δημιουργία ψηφιακών υπογραφών βασισμένο στο ιδιωτικό κλειδί κάποιου χρήστη.



Εικόνα 11: Ασύμμετρη κρυπτογράφηση

Το μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι το αυξημένο υπολογιστικό κόστος. Γι αυτό το λόγο οι αλγόριθμοι κρυπτογραφίας δημοσίου κλειδιού εφαρμόζονται μόνο για την κρυπτογράφηση περιορισμένου μεγέθους πληροφορίας. Προκειμένου να εφαρμόζεται σωστά η κρυπτογραφία δημοσίου κλειδιού, τα ιδιωτικά κλειδιά πρέπει να προστατεύονται. Άρα, συνοψίζοντας τα βασικά χαρακτηριστικά του ιδιωτικού και δημόσιου κλειδιού είναι τα ακόλουθα:

- Αποτελούν από ένα δυαδικό αλφαριθμητικό (byte)
- Δημιουργούνται συνάμα από ένα ειδικό πρόγραμμα λογισμικού
- Χαρακτηρίζονται μοναδικά κλειδιά ώστε να μπορούν να εφαρμοστούν η κρυπτογράφηση και αποκρυπτογράφηση δεδομένων.
- Τα κλειδιά που ανήκουν σε ένα ζεύγος χαρακτηρίζονται συμπληρωματικά. Τα δεδομένα που κρυπτογραφούνται με το ένα κλειδί μπορούν να αποκρυπτογραφηθούν μόνο με το άλλο και αντίστροφα.

- Η οντότητα που βρίσκεται σε ένα σύστημα επικοινωνίας δημόσιου κλειδιού περιέχει το δικός της ζεύγος κλειδιών (δημόσιο & ιδιωτικό κλειδί)
- Το ιδιωτικό κλειδί περιλαμβάνει προστασία από τον ιδιοκτήτη και χρησιμοποιείται για την δημιουργία ψηφιακής υπογραφή μηνυμάτων.
- Το δημόσιο κλειδί μοιράζεται ελεύθερα, χρησιμοποιείται για την πιστοποίηση ψηφιακών υπογραφών αλλά και την κρυπτογράφηση μηνυμάτων.

6.3 Οι τεχνικές ασφάλειας των έξυπνων καρτών

Κύριο χαρακτηριστικό των έξυπνων καρτών είναι ότι μπορούν να αποθηκεύουν δεδομένα με ένα τρόπο που να προστατεύονται από οποιαδήποτε μη εξουσιοδοτημένη πρόσβαση. Για την επίτευξη αυτού του επίπεδου ασφαλείας πρέπει να αποδοθεί η βελτιστοποίηση της τεχνολογίας του ολοκληρωμένου κυκλώματος από την πλευρά του υλικού και από πλευράς λογισμικού. Οι τεχνικές ασφαλείας απαρτίζονται από τα εξής μέρη, πρώτο μέρος είναι η ασφάλεια των έξυπνων καρτών και το δεύτερο μέρος είναι η κατηγοριοποίηση επιθέσεων και η κατηγοριοποίηση επιτιθέμενων. Παρακάτω γίνεται μια λεπτομερή επεξήγηση αυτών των τεχνικών ασφαλείας.

6.3.1 Ασφάλεια έξυπνων καρτών

Ο πιο σημαντικός συντελεστής για την διατήρηση της εμπιστευτικότητας και της μυστικότητας των δεδομένων μιας έξυπνης κάρτας εναντίον της μη εξουσιοδοτημένης πρόσβασης είναι η ασφάλεια. Πιο συγκεκριμένα , η ύπαρξη της ασφάλειας μέσα σε μια έξυπνη κάρτα προϋποθέτει την υλοποίηση των εφαρμογών ασκώντας έλεγχο αλλά και κάνοντας μια πιστοποίηση ταυτότητας του χρήστη εκεί που επιζητεί να αποκτήσει πρόσβαση στα δεδομένα. Οι δύο εναλλακτικές εφαρμογές που συνδέονται με την προστασία είναι οι ακόλουθες:

- **Ο κωδικός PIN (Personal Identification Number)**
- **Ο έλεγχος βιομετρικών γνωρισμάτων**

Ο κωδικός PIN αποτελείται από τέσσερα ψηφία και είναι αποθηκευμένα στην έξυπνη κάρτα. Όταν ο χρήστης θέλει να έχει πρόσβαση στα δεδομένα της κάρτας πρέπει να εισάγει ένα τετραψήφιο αριθμό. Αφού εισάγεται ο αριθμός πραγματοποιείται μια σύγκριση αυτού του αριθμού με τον αριθμό που είναι αποθηκευμένο στην κάρτα. Αν είναι έγκυρος , ο χρήστης αποκτά πρόσβαση, στο ενδεχόμενο που δεν είναι έγκυρο ξανά-πληκτρολογεί το PIN. Στη περίπτωση που ξεπεράσει τον όριο των προσπαθειών η κάρτα μπλοκάρεται.

Ένα μειονέκτημα όλης αυτής της διαδικασίας είναι ότι αν η κάρτα χρησιμοποιηθεί από τρίτο πρόσωπο και γνωρίζει ,φυσικά τον κωδικό, τότε η ασφάλεια παραβιάζεται και η συσκευή δεν μπορεί να αντιληφθεί ποιος είναι ο κάτοχος της κάρτας. Ένα ακόμη μειονέκτημα αποτελεί και το ενδεχόμενο ένας χρήστης μπορεί να κατέχει

πολλές κάρτες και αυτό να τον οδηγήσει στην πιθανότητα να ξεχάσει τους κωδικούς. Συμπεραίνοντας, η συγκεκριμένη εφαρμογή δεν περιλαμβάνει πολύπλοκες μεθόδους κρυπτογράφησης που συνδέονται με την ασφάλεια.

Μια άλλη εφαρμογή είναι η μέθοδος βιομετρικής τεχνολογίας. Είναι μια ασφαλή μέθοδος ταυτοποίησης και σχετίζεται με τα φυσικά χαρακτηριστικά του ανθρώπινου σώματος ως αποδεικτικά στοιχεία για την αναγνωσιμότητα μιας οντότητας . Δακτυλικά αποτυπώματα , ίριδα ματιού , χροιά φωνής , γεωμετρία χεριού αποτελούν στοιχεία για την διαδικασία αυθεντικοποίησης.

Τα βιομετρικά συστήματα εφαρμόζουν αυτοματοποιημένες μεθόδους για την μέτρηση ενός ανθρώπινου φυσικού χαρακτηριστικού ή συγκεκριμένης ανθρώπινης συμπεριφοράς. Κατά την εγγραφή του ανθρώπινου γνωρίσματος σε ένα βιομετρικό σύστημα , το χαρακτηριστικό αποθηκεύεται με εφαρμογή ειδικών τεχνικών μετρήσεων. Οι τεχνικές διαιρούνται σε δύο μετρήσεις:

1. **Τεχνική μέτρηση ανθρώπινων φυσικών χαρακτηριστικών**. Στην κατηγορία αυτή περιλαμβάνονται δακτυλικά αποτυπώματα, ανάλυση ίριδας ματιού, γεωμετρία χεριού, αναγνώριση αυτιού, ανάλυση δείγματος DNA, ανάλυση ιδρώτα .
2. **Τεχνική μέτρηση συμπεριφοράς:** Εμπεριέχει την αναγνώριση της υπογραφής, την ανάλυση της υπογραφής και η ανάλυση ομιλίας.

Η ανοχή στο σφάλμα και η μέθοδος αποθήκευσης των προτύπων ανάλυσης είναι δυο ορολογίες της τεχνολογίας μέτρησης βιομετρικών χαρακτηριστικών. Η πρώτη αφορά την ρύθμιση του βαθμού σφάλματος σε αυτά τα συστήματα είναι κρίσιμη που επηρεάζει τη ρυθμοαπόδοση του συστήματος. Ενώ, η δεύτερη αφορά στο πρότυπο (αποτύπωση βιομετρικής μέτρησης γνωρίσματος χρήστη) που μπορεί να αποθηκευτεί σε διάφορα μέσα ανάλογα με τις δυνατότητες της τεχνολογίας και τια απαιτήσεις της ασφαλείας της εφαρμογής.

6.3.2 Κατηγοριοποίηση επιθέσεων

Οι επιθέσεις των έξυπνων καρτών αναλύονται σε τρία διαφορετικού τύπου επίπεδα. Τα οποία είναι τα ακόλουθα:

- **Κοινωνικό στρώμα:** Σχετίζονται με επιθέσεις εναντίον των ατόμων που διαχειρίζονται με έξυπνες κάρτες. Συνήθως είναι άτομα που είναι από το κύκλο του λογισμικού ή από τον κύκλο κατασκευής ημιαγωγών. Οι επιθέσεις αντιμετωπίζονται νε τεχνικά και οργανωτικά μέτρα. Π.χ. Η αποκάλυψη του μυστικού πληκτρολόγησης του PIN μπορεί να γίνει με τη χρήση εικονικών οθονών αριστερά και δεξιά από το πληκτρολόγιο εισαγωγής. (τεχνικό μέτρο) . Ενώ με την η δημοσιοποίηση των διαδικασιών εναντίον των προγραμματιστών έξυπνων καρτών θεωρείται οργανωτικό μέτρο.

- **Φυσικό στρώμα:** Απαιτούν τεχνικό εξοπλισμό. Οι επιθέσεις αυτού του στρώματος απαρτίζονται από τις στατικές δηλαδή ο μικροεπεξεργαστής δεν έχει παροχή ρεύματος και από τις δυναμικές δηλαδή ο μικροεπεξεργαστής θέτεται σε λειτουργία. Η διαφορά ανάμεσα στη δυναμική και στην στατική είναι ότι στη πρώτη ο επιτιθέμενος πρέπει να έχει ένα γρήγορο εξοπλισμό ώστε να αποσπάσει τις πληροφορίες μέσα από τη κάρτα μέσα σε λίγο χρόνο ενώ οι δεύτερες δεν δέχονται τέτοιο χρονικό περιορισμό.
- **Λογικό επίπεδο:** Οι πιο δημοφιλές και επιτυχημένες επιθέσεις. Εμπεριέχει κρυπτανάλυση και επιθέσεις «κενά – λάθη» στα λειτουργικά συστήματα των έξυπνων καρτών και στο εκτελέσιμο κώδικα «Δούρειους ίππους»

6.3.3 Κατηγοριοποίηση των επιτιθέμενων

Αν οι επιτιθέμενοι κατηγορηθούν σχετικά με την ιδιότητά τους τότε προσάπτονται 6 μορφές επιτιθέμενων. Οι μορφές είναι οι εξής:

- **Hackers (εισβολείς):** Είναι τα άτομα που εισβάλλουν σε υπολογιστικά συστήματα. Διαθέτουν κατάλληλες γνώσεις και ικανότητες ώστε να μπορούν να διαχειριστούν τα υπολογιστικά συστήματα. Συνήθως είναι προγραμματιστές ή σχεδιαστές συστημάτων.
- **Insider:** Είναι τα άτομα που έχουν άριστη γνώση του συστήματος και μπορούν να έχουν πρόσβαση με τον κατάλληλο μηχανισμό. Δεν θεωρούνται ανώνυμοι οπότε η επίθεση μπορεί να αναγνωριστεί.
- **Εγκληματίες:** Δεν κατέχουν ιδιαίτερες τεχνικές γνώσεις πάνω στο σύστημα. Είναι επικίνδυνοι γιατί μπορούν να αποκτήσουν ζήλο όταν αφορά για προσωπικά οφέλη.
- **Ακαδημαϊκά ιδρύματα:** Οι σπουδαστές και οι καθηγητές μπορεί να είναι αυτοί που κάνουν την επίθεση/ Δεν είναι αναγκαίο να υπάρχουν ειδικές γνώσεις πάνω στους μικροεπεξεργαστές των έξυπνων καρτών . Αντίθετα, ένα εύρος από χρήσιμες πληροφορίες. Επιπλέον με ευχέρεια μπορούν να μεταχειριστούν ανθρώπινους πόρους και κατάλληλο τεχνολογικό εξοπλισμό.
- **Ανταγωνιστές:** Είναι εκείνοι που κατέχουν τεχνικές γνώσεις και περιλαμβάνουν ένα άριστο εξοπλισμό.
- **Οργανωμένο έγκλημα:** Είναι εκείνο το επίπεδο που κατέχει οικονομικούς πόρους ώστε να παραλάβει όλη την τεχνογνωσία και τα εργαλεία που είναι αναγκαία για μια επιτυχημένη επίθεση. Δεν εξαρτάται αν είναι νόμιμα ή μη νόμιμα μέσα.

Βιβλιογραφικές Αναφορές

1. Βιβλίο: Ασφάλεια Πληροφοριακών Συστημάτων – Επιστημονική Επιμέλεια Σωκράτης Κάτσικας- Δημήτρης Γκρίτζαλης – Στέφανος Γκρίτζαλης – Εκδόσεις Νέων Τεχνολογιών
2. http://nefeli.lib.teicrete.gr/browse2/stef/thl/2004/Kapetanakis/attached-document/2004Kapetanakis.pdf
3. http://artemis.cslab.ntua.gr/el_thesis/artemis.ntua.ece/DT2004-0013/DT2004-0013.pdf
4. http://nemertes.lis.upatras.gr/jspui/bitstream/10889/1307/6/Nimertis_Antonopoulos.pdf
5. http://artemis-new.cslab.ece.ntua.gr:8080/jspui/bitstream/123456789/5827/1/PD2006-0003.pdf
6. http://www.ebusinessforum.gr/old/content/downloads/smart_all.pdf
7. http://conta.uom.gr/conta/ekpaideysh/metaptyxiaka/e_commerce/ergasies/2002/Kagkani/SmartCards.pdf
8. http://delab.csd.auth.gr/~katsaros/ThesisVAlmaliotis.pdf
9. https://dspace.lib.uom.gr/bitstream/2159/14273/1/TsigenopoulouVeraMsc2011.pdf
10. https://www.google.gr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB8QFjAA&url=http%3A%2F%2Fartemis.cslab.ntua.gr%2Fel_thesis%2Fartemis.ntua.ece%2FDT2005-0158%2FDT2005-0158.doc&ei=0-YJVfXqHcrWPLib-gZgB&usg=AFQjCNGKfJMEjVJUyQ21_NeFfvwwXyBEfg&sig2=oK7gDl6lWUoYdW2_Eksyww&bvm=bv.88528373,d.ZWU
11. https://www.google.gr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCIQFjAA&url=http%3A%2F%2Fartemis.cslab.ntua.gr%2Fel_thesis%2Fartemis.ntua.ece%2FDT2006-0217%2FDT2006-0217.doc&ei=HOcJVbKNBsK5OJjYgLAE&usg=AFQjCNG3VUdL6Ti9AFXJ30pcE2H-AiYxnw&sig2=FG56KkpLvMWhVfxYtmZv0A&bvm=bv.88528373,d.ZWU
12. http://foxcasino.gr/t%CE%B9-einai-ta-hlektronika-portofolia/
13. http://www.moneypedia.gr/%CF%87%CF%81%CE%B7%CE%BC%CE%B1-%CE%BA%CE%B1%CE%B9-%CE%BD%CE%B5%CE%BF%CE%B9/%CF%87%CF%81%CE%B7%CE%BC%CE%B1-%CE%BA%CE%B1%CE%B9-%CE%BD%CE%B5%CE%BF%CE%B9/%CF%84%CE%B9-%CF%80%CF%81%CE%B5%CF%80%CE%B5%CE%B9-%CE%BD%CE%B1-%CE%BE%CE%B5%CF%81%CF%89-%CE%B3%CE%B9%CE%B1-%CF%84%CE%B9%CF%82-%CE%BA%CE%B1%CF%81%CF%84%CE%B5%CF%82/%CE%B5%CE%BE%CF%85%CF%80%CE%BD%CE%B7-%CE%BA%CE%B1%CF%81%CF%84%CE%B1-%28smart-card%29/%CF%80%CE%B5%CF%81%CE%B9%CF%80%CF%84%CF%89%CF%83%CE%B7--%CF%84%CE%BF-%CE%B7%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CE%BF-

%CF%80%CE%BF%CF%81%CF%84%CE%BF%CF%86%CE%BF%CE%BB%CE%B9-%28e-wallet%29.aspx
14. http://users.teilam.gr/~klimn/mobile/Lec3.pdf
15. http://www.fcbsudan.com/electronic-services/e-purse.html
16. di.ionio.gr/~emagos/security/3/Simeioseis-Kryptografia.pdf

Πίνακας Παραπομπών

[1] http://www.ebusinessforum.gr/old/content/ downloads/smart_all.pdf
[2] nefeli.lib.teicrete.gr/browse2/stef/thl/2004/Kapetanakis/attached-document/2004Kapetanakis.pdf
[3] http://www.ebusinessforum.gr/old/content/downloads/smart_all.pdf
[4]http://www.dpa.gr/portal/page?_pageid=33,131221&_schema=PORTAL
[5] artemis-new.cslab.ece.ntua.gr:8080/ispui/bitstream/123456789/5827/1/PD2006-0003
[6] https://dspace.lib.uom.gr/bitstream/2159/14273/1/TsigenopoulouVeraMsc2011.pdf