Τ*εχνολογικό*
Ε*κπαιδευτικό*
Ί*δρυμα*
Κ*ρήτης*

Τμήμα Ηλεκτρονικής
(Παράρτημα Χανίων**)**

Πτυχιακή Εργασία:

"Τεχνολογία Smart Card"

Επιμέλεια:Βαρούχας Ζαχαρίας

Σεπτέμβριος 2003

Αφιέρωση

Η παρούσα πτυχιακή καθώς και το πτυχίο μου αφιερώνεται στους γονείς μου Έλλη & Μαρίνο Βαρούχα καθώς και σε όλους αυτούς που πίστεψαν σε μένα και πάνω από όλα μου έδωσαν την ευκαιρία-βοήθεια να ολοκληρώσω με επιτυχία αυτόν το στόχο μου.

Ευχαριστίες

Το ότι ο κ$_{ος}$ Αντωνιδάκης είναι ο άνθρωπος που έχει δώσει μια πραγματική-ουσιαστική ανωτατοποίηση στο τμήμα Ηλεκτρονικής είναι ηλίου φαεινότερο. Τόσο το γεγονός αυτό όσο και η πολύτιμη βοήθεια του όλα αυτά τα χρόνια που συνεργαστήκαμε με κάνουν να θέλω, μέσα από την καρδιά μου, να τον ευχαριστήσω για όλα.

Περίληψη

Η χρήση έξυπνων καρτών (smart cards) σε τομείς εφαρμογών όπως έλεγχος πρόσβασης (access control) και πληρωμή χωρίς μετρητά (cashless payment) αυξάνεται ολοένα και περισσότερο. Οι διάφορες κάρτες και κυρίως οι μαγνητικές χρησιμοποιούνται με επιτυχία εδώ και χρόνια στις παραπάνω εφαρμογές, κρατώντας είτε τα στοιχεία των κατόχων τους για ταυτοποίηση (identification), προσφέροντας δηλαδή ένα τρόπο αναγνώρισης ή προσδιορισμού της ταυτότητας του κατόχου, είτε περιέχοντας κάποιο ποσό χρημάτων ή μονάδων για διεκπεραίωση συναλλαγών, αγορών, τηλεφωνίας, κτλ.

Η επιτυχία τους και η πλατιά διάδοσή τους οφείλεται στην ευκολία μεταφοράς και χρήσης τους, στο ότι προσφέρουν ασφάλεια και προστασία των δεδομένων που περιέχουν, στο μικρό κόστος τους, καθώς επίσης και στην μη ανάγκη ύπαρξης προσωπικού υποστήριξης όπου εγκαθίστανται τέτοια συστήματα.

Η πρόοδος της τεχνολογίας, επέτρεψε αρχικά την τοποθέτηση διαφόρων ειδών μνήμης στις κάρτες, με χωρητικότητες που συνεχώς αυξάνουν προσφέροντας έτσι την δυνατότητα αποθήκευσης ολοένα και μεγαλύτερου όγκου δεδομένων, καθώς και την ενσωμάτωση ενός μικροεπεξεργαστή στην κάρτα, δημιουργώντας τις "έξυπνες" κάρτες, και προσφέροντας μεγαλύτερη ασφάλεια, απαραίτητη για σοβαρότερες εφαρμογές.

Οι κυριότεροι τομείς στους οποίους χρησιμοποιούνται σήμερα smart cards είναι η ιδιωτική και δημόσια κινητή και σταθερή τηλεφωνία, ο τραπεζικός τομέας, ο τομέας της υγείας, η προσφορά και χρέωση διαφόρων εξειδικευμένων υπηρεσιών (Pay-TV, NOVA Sat), ο έλεγχος πρόσβασης (access control), ο προσδιορισμός της ταυτότητας του κατόχου (identification) και αρκετές άλλες μείζονος σημασίας. Παράλληλα, η ανάπτυξη του διαδικτύου (internet), δημιούργησε ένα πλήθος καινούριων εφαρμογών, όπως το ηλεκτρονικό εμπόριο (e-commerce), όπου οι smart cards με τις δυνατότητες που προσφέρουν, παίζουν το σημαντικότερο ρόλο για τη διεκπεραίωση συναλλαγών και είναι το κλειδί τόσο για την επιβίωση όσο και για τον πλουτισμό των ηλεκτρονικών επιχειρήσεων.

Στην πτυχιακή αυτή θα δούμε ένα ολοκληρωμένο σύστημα που βασίζεται σε smart cards κατάλληλο για access control, cashless payment applications,user authentication στο web, και e-commerce.

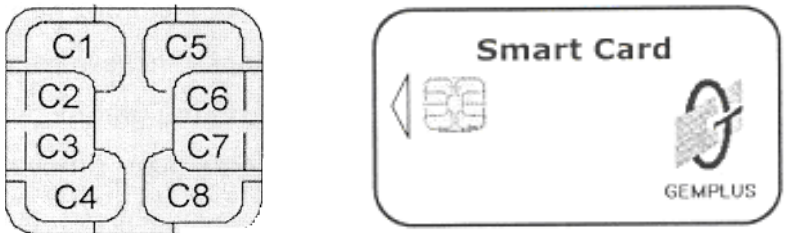
ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ

Στο κεφάλαιο αυτό περιγράφουμε εν συντομία το ρόλο που παίζουν σήμερα οι smart cards, την διάδοση τους και που οφείλεται αυτή, καθώς και τις εφαρμογές που κυρίως χρησιμοποιούνται.

1.1 Τι είναι οι smart cards

Οι smart cards είναι πλαστικές κάρτες στο μέγεθος των γνωστών μας πιστωτικών καρτών με τη διαφορά ότι έχουν ενσωματωμένο ένα chip. Το chip αυτό όπως θα δούμε παρακάτω μπορεί να είναι μόνο μνήμη ή μνήμη μαζί με κάποιον μικροεπεξεργαστή. Σε αυτό φυλάσσονται διάφορες πληροφορίες σε ηλεκτρονική μορφή. Το μέγεθος της κάρτας καθώς και τα υπόλοιπα φυσικά χαρακτηριστικά της, η ανθεκτικότητα της κάρτας στην θερμοκρασία, η ελαστικότητά της, η θέση των ηλεκτρικών επαφών και η λειτουργία τους, ο τρόπος επικοινωνίας του ολοκληρωμένου κυκλώματος με τον έξω κόσμο καθορίζονται από τον Διεθνή Οργανισμό Τυποποίησης (International Organization for Standardization, ISO) με το standard ISO7816.



Πάχος: 0.76 ±0.08,Μήκος: 85.6 ± 0.12,Πλάτος:53.97 ± 0.05

Σχήμα 1.1 Εξωτερική όψη μιας smart card και οι επαφές της

Η ευκολία μεταφοράς και χρήσης τους, η δυνατότητα αποθήκευσης μεγάλου όγκου πληροφοριών, η ασφάλεια των δεδομένων που προσφέρουν, το χαμηλό τους κόστος, είναι μερικά από τα χαρακτηριστικά που κάνουν τις smart cards να χρησιμοποιούνται σε όλο και περισσότερες αλλά και σοβαρότερες εφαρμογές.

1.2 Είδη καρτών

Ο Διεθνής Οργανισμός Τυποποίησης (ISO) χρησιμοποιεί τον όρο Integrated Circuit Card (ICC) για να περιγράψει όλες τις κάρτες που περιέχουν ένα ολοκληρωμένο κύκλωμα. Οι κάρτες αυτές μπορεί να είναι:

- μόνο μνήμης
- μνήμης με λογική ασφάλειας
- μνήμης με μικροεπεξεργαστή

Οι κάρτες μνήμης περιέχουν κάποιο από τα γνωστά είδη μνήμης. Τα συνηθέστερα είδη είναι η μνήμη ROM, η οποία γράφεται από το εργοστάσιο κατά την διάρκεια κατασκευής της κάρτας και η μνήμη EEPROM, η οποία μπορεί να σβηστεί και να ξαναγραφεί ηλεκτρικά, στην οποία γράφονται τα δεδομένα της εφαρμογής.

Οι κάρτες μνήμης με λογική ασφάλειας περιέχουν το ίδιο είδος μνήμης με τις κάρτες μνήμης με την προσθήκη κωδικού πρόσβασης (access code) ο οποίος ελέγχει και επιτρέπει ή όχι την πρόσβαση στα περιεχόμενα της μνήμης.

Οι κάρτες μνήμης με μικροεπεξεργαστή περιέχουν έως 256 bytes Random Access Memory (RAM), έως 16 Kbytes Read Only Memory (ROM), και έως 8 Kbytes Electrically-Erasable Programmable Read Only Memory (EEPROM). Περιέχουν επίσης και ένα 8-bit μικροεπεξεργαστή ο οποίος έχει την δυνατότητα να γράψει ή να διαβάσει την μνήμη, να "πάρει αποφάσεις" και να εκτελέσει πιο πολύπλοκες λειτουργίες. Από αυτές τις κάρτες προέρχεται και ο όρος smart cards.

Και τα τρία είδη καρτών προσφέρουν πολύ μεγαλύτερη ασφάλεια από τις μαγνητικές κάρτες των οποίων η πληροφορία που βρίσκεται σε μια μαγνητική ταινία στο εξωτερικό της κάρτας μπορεί εύκολα να αντιγραφεί. Επιπλέον οι smart cards χάρη στον επεξεργαστή τους μπορούν να προστατεύσουν τα δεδομένα υλοποιώντας πολύπλοκους αλγόριθμους κρυπτογράφησης και ψηφιακές υπογραφές (digital signatures).

Οι smart cards, χωρίζονται επίσης σε contact και contactless. Οι πρώτες πρέπει να εισέλθουν μέσα σε κάποια συσκευή ανάγνωσης (smart card reader), η οποία διαβάζει και γράφει την κάρτα μέσω των ηλεκτρικών επαφών της κάρτας. Οι δεύτερες εκτός από τον μικροεπεξεργαστή και την μνήμη, έχουν ένα σπείρωμα που παίζει το ρόλο κεραίας και μπορούν να

επικοινωνήσουν με την συσκευή ανάγνωσης/εγγραφής από απόσταση. Επίσης υπάρχουν και οι CompiCards που λειτουργούν και ως contact και ως contactless.

Τέλος οι κάρτες χωρίζονται σε disposable και reloadable. Οι πρώτες περιέχουν κάποιο ποσό μονάδων η χρημάτων ανάλογα την εφαρμογή, το οποίο με την χρήση της κάρτας μειώνεται έως ότου εξαντληθεί εντελώς. Η κάρτα δεν μπορεί να ξαναγεμίσει ή να ξαναχρησιμοποιηθεί και ο κάτοχός της την πετάει. Οι δεύτερες έχουν την δυνατότητα να ξαναεγγραφούν και χρησιμοποιούνται σε εφαρμογές που ο κάτοχος ξαναγεμίζει την κάρτα σε συχνή βάση αντί του να αγοράζει κάθε φορά μια καινούρια.

1.3 Εφαρμογές των smart cards

Οι κυριότερες από τις εφαρμογές που χρησιμοποιούνται σήμερα ή πρόκειται να χρησιμοποιηθούν στο εγγύς μέλλον περιγράφονται παρακάτω:

- Τηλεπικοινωνίες. Στην σταθερή τηλεφωνία (καρτοτηλέφωνα), χρησιμοποιούνται χαμηλού κόστους, αναλώσιμες (disposable), προοριζόμενες για μία χρήση κάρτες, με ένα προκαθορισμένο αριθμό μονάδων οι οποίες "καίγονται" μετά από κάθε χρήση. Επίσης στην κινητή τηλεφωνία η κάρτα που μπαίνει μέσα στα κινητά τηλέφωνα περιέχει όλες τις προσωπικές πληροφορίες του χρήστη, απαραίτητες για την χρέωση του λογαριασμού του.

- Ηλεκτρονικές πληρωμές. Οι περισσότεροι σήμερα γνωρίζουμε τις πιστωτικές κάρτες που χρησιμοποιούμε για διάφορες αγορές. Η επόμενη γενιά πιστωτικών καρτών που σχεδιάζεται θα στηρίζεται αποκλειστικά σε smart cards αντί των μαγνητικών, οι οποίες προσφέρουν μεγαλύτερη χωρητικότητα και ασφάλεια. Επίσης οι smart cards θα χρησιμοποιούνται και για πληρωμές αγορών που γίνονται μέσω του internet (e-commerce).

- Υγεία. Εδώ οι smart cards θα χρησιμοποιούνται σαν ένα κινητό ηλεκτρονικό αρχείο με πληροφορίες που αφορούν την υγεία του ασθενή, το ιατρικό ιστορικό του, κτλ.

- Μεταφορές. Εδώ οι smart cards και ιδιαίτερα οι contactless μπορούν να αντικαταστήσουν τα εισιτήρια στα μέσα μαζικής μεταφοράς, στα parking, στα διόδια των εθνικών οδών διευκολύνοντας τις

συναλλαγές και μειώνοντας τον χρόνο διεκπεραίωσης.

- Έλεγχος πρόσβασης. Οι smart cards χρησιμοποιούνται για την πιστοποίηση της ταυτότητας του χρήστη, σε οποιοδήποτε κτίριο, οργανισμό, η άλλο μέρος χρειάζεται έλεγχος πρόσβασης.

- Εκπαίδευση. Σε πολλά πανεπιστήμια οι smart cards δίνονται στους φοιτητές και χρησιμοποιούνται σαν multi-purpose cards για ένα πλήθος δραστηριοτήτων που αφορά την ζωή του πανεπιστημίου, όπως προσδιορισμός της ταυτότητας του φοιτητή (identification), έλεγχος πρόσβασης στις εστίες και σε διάφορα εργαστήρια, αγορά αγαθών από σημεία πώλησης (point of sales), χρήση φωτοτυπικών μηχανημάτων, δανεισμό βιβλίων από την βιβλιοθήκη κτλ. Όλα αυτά γίνονται φυσικά με μία μόνο κάρτα.

- Όργανα μέτρησης. Σε πολλά κράτη οι smart cards χρησιμοποιούνται για την χρέωση της κατανάλωσης των δημοσίων οργανισμών κοινής ωφέλειας όπως τους οργανισμούς ρεύματος και ύδρευσης. Ο χρήστης αγοράζει κάρτες με κάποιο αριθμό μονάδων προπληρώνοντας έτσι την κατανάλωση νερού ή ρεύματος που θα κάνει. Με τον τρόπο αυτό μειώνονται τα λειτουργικά έξοδα της επιχείρησης αφού εξαλείφεται όλος ο μηχανισμός για την καταγραφή με τα κλασικά ρολόγια, έκδοση, αποστολή και πληρωμή του λογαριασμού.

Η τάση της αγοράς και της βιομηχανίας είναι στην χρησιμοποίηση καρτών πολλαπλών εφαρμογών (multi-application cards). Οι κάρτες αυτές έχουν την δυνατότητα να υποστηρίξουν διαφορετικά είδη εφαρμογών έτσι ώστε ο χρήστης να κατέχει μία κάρτα για όλες τις εφαρμογές που χρησιμοποιεί αντί της μιας κάρτας για κάθε ξεχωριστή εφαρμογή όπως συμβαίνει μέχρι σήμερα. Η θέσπιση κοινών standards και μια ανοιχτή αρχιτεκτονική που θα επιτρέπει την προσθήκη εφαρμογών σε μια κάρτα χωρίς να επηρεάζει τις ήδη υπάρχουσες είναι απαραίτητες προϋποθέσεις για να γίνει η multi-application card πραγματικότητα.

1.4 Διάδοση των smart cards

Card Application	1996*	2003*	Average Annual Growth
Pay Phone	605	1,500	29%
GSM	20	45	25%
Health Care	70	120	14%
Banking	40	250	105%
Identity-Access	20	300	280%
Transportation	15	200	247%
Pay TV	15	75	80%
Gaming	5	200	780%
Metering-Vending	10	80	140%
Retail-Loyalty	5	75	280%

* in millions
**Source: Phoenix Planning & Evaluation

Το 1996 κυκλοφόρησαν 805 εκατομμύρια smart cards. Ο αριθμός αυτός αναμένεται να αυξηθεί σε 2.8 δισεκατομμύρια το έτος 2003. Η κατανομή των καρτών στις διάφορες εφαρμογές φαίνεται στον παραπάνω πίνακα:**

Σημαντικό ρόλο στην ευρεία διάδοση των καρτών θα παίξει και αυτό που ονομάζουμε interoperability, η συμβατότητα δηλαδή ανάμεσα στις smart cards, στις συσκευές ανάγνωσης/εγγραφής και στις εφαρμογές. Η βιομηχανία επομένως θα πρέπει να μελετήσει και να θεσπίσει τα standards τα οποία θα εφαρμοστούν παγκοσμίως έτσι ώστε να επιτευχθεί αυτή η συμβατότητα. Ήδη ο Διεθνής Οργανισμός Τυποποίησης (ISO) κινείται προς αυτή την κατεύθυνση.

1.5 World Wide Web και smart cards

Η ανάπτυξη του internet δημιούργησε ένα νέο πεδίο στο οποίο οι smart cards έχουν ένα πολύ σημαντικό ρόλο να παίξουν. Λόγω του μικρού κόστους των συσκευών ανάγνωσης/εγγραφής προβλέπεται ότι πολύ σύντομα οι προσωπικοί υπολογιστές θα εφοδιαστούν και με τέτοιες συσκευές αποκτώντας την δυνατότητα να διαβάζουν smart cards. Ήδη η Microsoft έχει αναγγείλει ότι μεταγενέστερες εκδόσεις των Windows θα υποστηρίζουν την χρήση smart cards. Λόγω της αυξημένης ασφάλειας που προσφέρουν οι smart cards μπορούν να χρησιμοποιηθούν για πιστοποίηση του χρήστη του παγκοσμίου ιστού (web user authentication), πρόσβαση σε

εξειδικευμένες υπηρεσίες, on-line πληρωμές και γενικότερα το ηλεκτρονικό εμπόριο (e-commerce).

ΚΕΦΑΛΑΙΟ 2

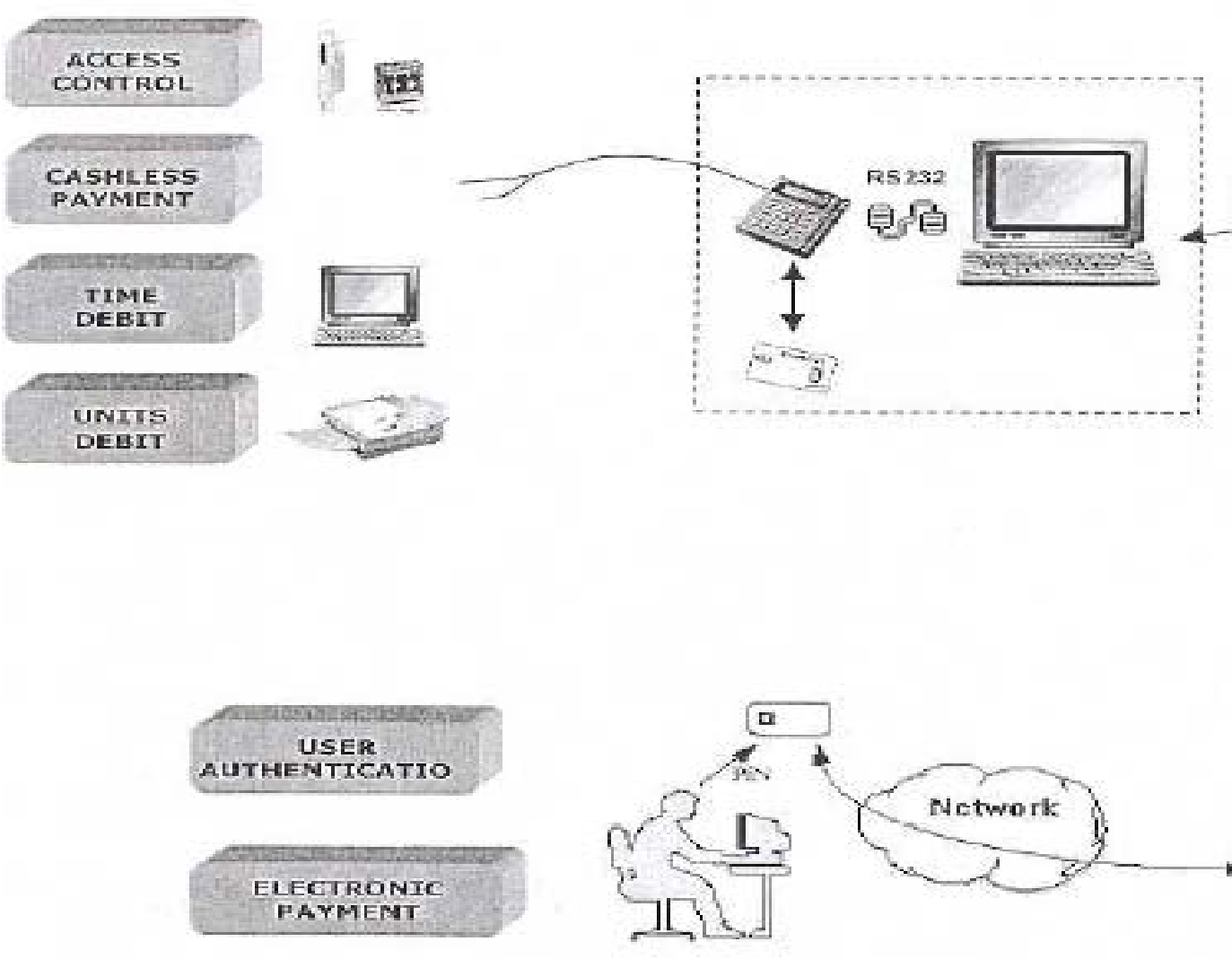
Η ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΟΛΟΚΛΗΡΩΜΕΝΩΝ ΣΥΣΤΗΜΑΤΩΝ ΜΕ SMART CARDS

Στη πτυχιακή αυτή θα αναλύσουμε ένα ολοκληρωμένο σύστημα που θα μπορούσε να καλύψει ένα πλήθος εφαρμογών με smart cards. Οι εφαρμογές αυτού του τύπου είναι:

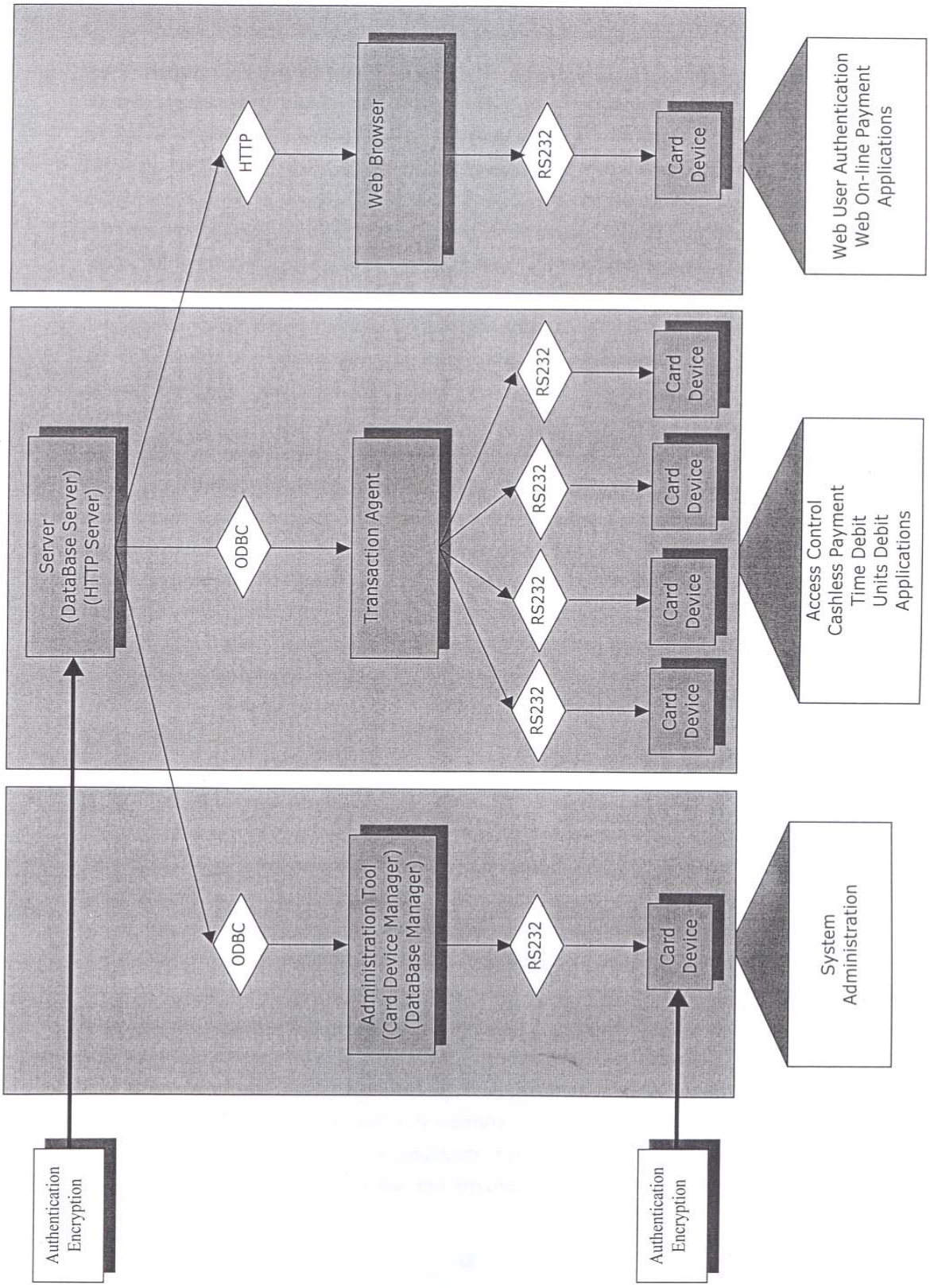
- έλεγχος πρόσβασης (access control)
- χρηματική χρέωση (cashless payment)
- χρονοχρέωση (time debit)
- χρέωση μονάδων (units debit)
- πιστοποίηση χρήστη στον παγκόσμιο ιστό (web user authentication)
- on-line χρέωση στον παγκόσμιο ιστό (web on-line payment)

Τα υπάρχοντα συστήματα δουλεύουν με διαφορετικές συσκευές, κάτι που ανεβάζει το κόστος κατασκευής τους. Η συσκευή ανάγνωσης/εγγραφής καρτών προτείνεται και θα μπορούσε να σχεδιαστεί έτσι ώστε να μπορεί να ανταποκριθεί σε όλες τις παραπάνω εφαρμογές χωρίς καμία αλλαγή σε hardware. Επίσης ο τελικός χρήστης θα μπορούσε να έχει μία μόνο κάρτα για όλες τις εφαρμογές (multi-application card).

Στα παρακάτω σχήματα φαίνεται η γενική άποψη των εφαρμογών του συστήματος και η γενική αρχιτεκτονική.



Σχήμα 2.1 Γενική άποψη των εφαρμογών του συστήματος



Σχήμα 2.2 Γενική άποψη της αρχιτεκτονικής του συστήματος

2.1 Σύστημα εξυπηρετητών

Το σύστημα εξυπηρετητών αποτελείται από δυο εξυπηρετητές. Έναν εξυπηρετητή βάσης δεδομένων (Database Server) και έναν εξυπηρετητή παγκοσμίου ιστού (Web Server). Οι εξυπηρετητές μπορούν να τρέχουν σε έναν υπολογιστή ή σε δυο διαφορετικούς που είναι συνδεδεμένοι στο διαδίκτυο. Οι παραπάνω εξυπηρετούν τις αιτήσεις που προέρχονται από τα τρία υποσυστήματα: διαχείρισης του συστήματος (administration tool), διακομιστή συνδιαλλαγών (transaction agent), και το σύστημα πιστοποίησης χρήστη και ηλεκτρονικής χρέωσης (web user authentication, web on-line payment) που ενσωματώνεται στον φυλλομετρητή (Web Browser) σαν add-in. Τα τρία αυτά υποσυστήματα φαίνονται στο δεύτερο επίπεδο του δέντρου της αρχιτεκτονικής (σχήμα 2.2) πιο αναλυτικά.

2.1.1 Εξυπηρετητής βάσης δεδομένων (Database Server)

Είναι υπεύθυνος για την εξυπηρέτηση αιτήσεων από τις εφαρμογές που αλληλεπιδρούν με την βάση δεδομένων του συστήματος. Ο εξυπηρετητής εκτός από την υλοποίηση της βάσης σύμφωνα με το σχεσιακό μοντέλο παρέχει τους απαραίτητους μηχανισμούς για επεξεργασία και βελτιστοποίηση των ερωτήσεων (queries) που αιτούνται καθώς και τους μηχανισμούς που θα πρέπει να χαρακτηρίζουν ένα διανεμημένο σύστημα όπως Ταυτοχρονισμός (Concurrency), Συνέπεια (Consistency), και υποστήριξη Συνδιαλλαγών (Transactions). Οι εφαρμογές που χρησιμοποιούν τη βάση χρησιμοποιούν το πρωτόκολλο ODBC (Open Data Base Connectivity).

2.1.2 Εξυπηρετητής παγκοσμίου ιστού (Web Server)

Είναι υπεύθυνος για την εξυπηρέτηση των αιτήσεων που προέρχονται από τον Transaction Agent και το υποσύστημα υποστήριξης authentication / on-line payment. Επίσης παρέχει την ίδια την εφαρμογή υποστήριξης authentication / on-line payment στους τελικούς χρήστες του συστήματος αφού αυτή συνίσταται κατά ένα τμήμα της από σελίδες παγκοσμίου ιστού και ενεργοποιείται μέσα σε αυτές, έπειτα από αίτηση του φυλλομετρητή. Οι εφαρμογές επικοινωνούν με τον εξυπηρετητή παγκοσμίου ιστού μέσω

του πρωτοκόλλου HTTP (Hyper Text Transfer Protocol).

2.2 Εφαρμογή διαχείρισης του συστήματος (Administration Tool)

Είναι υπεύθυνη για τη διαχείριση των καρτών, της συσκευής ανάγνωσης/εγγραφής καρτών (Card Device) και για τη διαχείριση της βάσης δεδομένων. Επικοινωνεί με τον εξυπηρετητή της βάσης μέσω του πρωτοκόλλου ODBC και με την συσκευή ανάγνωσης/εγγραφής καρτών μέσω του RS-232 πρωτοκόλλου. Η εφαρμογή διαχείρισης τρέχει στον υπολογιστή, που τρέχει και ο εξυπηρετητής βάσης δεδομένων ή σε υπολογιστή που βρίσκεται σε τοπικό δίκτυο με αυτόν. Επίσης σε σειριακή θύρα του υπολογιστή είναι συνδεδεμένη η συσκευή ανάγνωσης/εγγραφής καρτών. Χωρίζεται σε δύο τμήματα:

2.2.1 Υποσύστημα διαχείρισης καρτών-συσκευής

Παρέχονται μηχανισμοί και user interface για την επισκόπηση, διαγραφή, έκδοση καρτών καθώς και για τη ρύθμιση της συσκευής ανάγνωσης/εγγραφής καρτών. Για παράδειγμα ο διαχειριστής μπορεί να εκδώσει νέα κάρτα με συγκεκριμένο περιεχόμενο χρημάτων, προσωπικό αριθμό αναγνώρισης (PIN), μονάδες χρονοχρέωσης ή να ρυθμίσει την συγκεκριμένη συσκευή για την εφαρμογή ελέγχου πρόσβασης (access control).

2.2.2 Υποσύστημα διαχείρισης βάσης δεδομένων

Παρέχονται μηχανισμοί και user interface για την εισαγωγή, διαγραφή και ενημέρωση των εγγραφών της βάσης δεδομένων όπως και για την παρακολούθηση της δραστηριότητας του συστήματος. Για παράδειγμα ο διαχειριστής μπορεί να κάνει εισαγωγή στο σύστημα ενός νέου χρήστη κάρτας (card owner) αφού έχει εκδώσει κάρτα για αυτόν ή μπορεί να παρακολουθήσει τη δραστηριότητα κάποιας συγκεκριμένης συσκευής. Δηλαδή για πόσο χρόνο και πότε έχει εξυπηρετήσει κάποιον χρήστη ή το συνολικό ποσό των χρημάτων που έχουν καταναλωθεί στη συγκεκριμένη

συσκευή για κάποιο χρονικό διάστημα και από ποιες κάρτες.

2.3 Πράκτορας - διακομιστής συνδιαλλαγών (Transaction Agent)

Είναι υπεύθυνος για την καταχώρηση των συνδιαλλαγών (Iogging) που λαμβάνουν χώρα στις συνδεδεμένες σε αυτόν συσκευές καρτών, στη κεντρική βάση δεδομένων. Η εφαρμογή τρέχει σε υπολογιστή συνδεδεμένο στο διαδίκτυο και συνδέεται επίσης με τις συσκευές καρτών για τις οποίες κρατείται αρχείο συνδιαλλαγών (Iog file) στη βάση δεδομένων. Για παράδειγμα, αν ένας χρήστης χρησιμοποιήσει την κάρτα του σε συσκευή για έλεγχο πρόσβασης (access control), ο Transaction Agent αναλαμβάνει να καταχωρήσει στη βάση δεδομένων την ακριβή ημερομηνία και ώρα που συνέβη η συγκεκριμένη ενέργεια, το αναγνωριστικό του χρήστη, της κάρτας και της συσκευής.

2.4 Υποστήριξη πιστοποίησης χρήστη και ηλεκτρονικής χρέωσης εμπορικών συνδιαλλαγών για τον παγκόσμιο ιστό (web user authentícatíon and web on-line payment).

Ο μηχανισμός user authentication επιτρέπει στον τελικό χρήστη να προσπελάσει συγκεκριμένο πόρο (Web Page) του εξυπηρετητή παγκοσμίου ιστού (Web Server) , μέσω κάποιου φυλλομετρητή (Web Browser) , μόνο αφού χρησιμοποιήσει την προσωπική του κάρτα. Ο εκδότης του πόρου θα πρέπει να κάνει κατάλληλες ρυθμίσεις στην πλευρά του εξυπηρετητή ώστε να απαιτείται η παρουσία κάρτας στη συσκευή ανάγνωσης/εγγραφής καρτών στην πλευρά του υπολογιστή που τρέχει ο φυλλομετρητής. Για παράδειγμα ο εκδότης ενός εξυπηρετητή νέων (σε HTML μορφή), μπορεί να δώσει πρόσβαση με πιστοποίηση, σε επίπεδο συνόδου (session), σε χρήστες που διαθέτουν συγκεκριμένες κάρτες.

Ο μηχανισμός υποστήριξης on-line payment παρέχει στο χρήστη του φυλλομετρητή τη δυνατότητα να χρεωθεί στην προσωπική του κάρτα για υπηρεσίες ή προϊόντα που υποστηρίζουν το συγκεκριμένο σύστημα. Ο τελικός χρήστης έχει τη δυνατότητα να αγοράσει έπειτα από επιλογή τα

προϊόντα που παρουσιάζονται σε σελίδες ή να αποκτήσει πρόσβαση σε κάποιον πόρο χρεώνοντας την προσωπική του κάρτα. Ο εκδότης του συγκεκριμένου πόρου θα πρέπει να χρησιμοποιήσει τις κατάλληλες ρυθμίσεις στην πλευρά του εξυπηρετητή για να υποστηρίξει την on-line χρέωση καθώς και την χρήση συστήματος καταχώρησης και εξυπηρέτησης παραγγελιών προϊόντων.

Η υποστήριξη των παραπάνω λειτουργιών γίνεται εφικτή με την ενσωμάτωση του κατάλληλου λογισμικού , στην πλευρά του εξυπηρετητή παγκοσμίου ιστού. Μέρος του λογισμικού ενεργοποιείται στον φυλλομετρητή έπειτα από αίτηση του χρήστη στη συγκεκριμένη τοποθεσία παγκοσμίου ιστού (Web Site). Στην πλευρά του υπολογιστή του φυλλομετρητή θα πρέπει να υπάρχει φυσικά συνδεδεμένη και μια συσκευή ανάγνωσης/εγγραφής καρτών.

Το λογισμικό στην μεριά του φυλλομετρητή τρέχει στην ίδια διεργασία (process) με αυτόν, επικοινωνεί με την συσκευή ανάγνωσης/εγγραφής καρτών με RS232 πρωτόκολλο και με τον εξυπηρετητή παγκοσμίου ιστού με HTTP πρωτόκολλο χρησιμοποιώντας τους μηχανισμούς που παρέχονται από τον ίδιο τον φυλλομετρητή. Στις δύο παραπάνω επικοινωνίες πρέπει να υπάρχει ένα επίπεδο κρυπτογράφησης (Cryptography), και πιστοποίησης (authentication), για να διασφαλισθούν τόσο η ακεραιότητα των μεταφερομένων δεδομένων και η ασφάλεια της συναλλαγής όσο και η πιστοποίηση των μερών που συναλλάσσονται.

2.5 Η συσκευή ανάγνωσης/εγγραφής καρτών

Χρησιμοποιείται για την ανάγνωση και εγγραφή των καρτών τόσο από τον διαχειριστή του συστήματος όσο και από τους τελικούς χρήστες. Ο διαχειριστής του συστήματος χρησιμοποιεί την συσκευή ανάγνωσης/εγγραφής καρτών για την έκδοση των καρτών. Συνδέεται στην σειριακή θύρα του υπολογιστή ο οποίος τρέχει την εφαρμογή διαχείρισης καρτών-συσκευής και επικοινωνεί με αυτόν μέσω του RS-232 πρωτοκόλλου. Αφού προγραμματιστεί κατάλληλα, τοποθετείται στα σημεία όπου εγκαθίσταται το σύστημα και υλοποιεί μία από τις παρακάτω εφαρμογές:

- Έλεγχος πρόσβασης. Στην εφαρμογή αυτή η συσκευή συνδέεται με ηλεκτρονική κλειδαριά και η κάρτα χρησιμοποιείται για έλεγχο πρόσβασης. Ο προσφέρων την υπηρεσία επιτρέπει την πρόσβαση του τελικού χρήστη μόνο μετά την εισαγωγή από αυτόν της κάρτας του και του προσωπικού του PIN.

- Χρηματική χρέωση. Στην εφαρμογή αυτή η συσκευή χρησιμοποιείται σαν ένα είδος ταμειακής μηχανής. Ο προσφέρων την υπηρεσία αφαιρεί από την κάρτα του τελικού χρήστη το χρηματικό ποσό που εισάγει μέσω του πληκτρολογίου της συσκευής.

- Χρονοχρέωση. Στην εφαρμογή αυτή η συσκευή ανάγνωσης/εγγραφής καρτών συνδέεται με κάποια άλλη ηλεκτρονική συσκευή (π.χ. ηλεκτρονικός υπολογιστής) μέσω relay. Ο προσφέρων την υπηρεσία χρεώνει τους τελικούς χρήστες ανάλογα με το χρόνο χρήσης αυτής της συσκευής. Με την εισαγωγή της κάρτας επιτρέπεται η χρήση της ηλεκτρονικής συσκευής ενώ από την κάρτα του χρήστη αφαιρείται χρόνος.

- Χρέωση μονάδων. Στην εφαρμογή αυτή η συσκευή ανάγνωσης/ εγγραφής καρτών συνδέεται με κάποια άλλη ηλεκτρονική συσκευή (π.χ. φωτοτυπικό μηχάνημα) μέσω relay. Ο προσφέρων την υπηρεσία χρεώνει τους τελικούς χρήστες για την χρήση αυτής της συσκευής μέσω μονάδων. Με την εισαγωγή της κάρτας επιτρέπεται η χρήση της ηλεκτρονικής συσκευής ενώ από την κάρτα του χρήστη αφαιρείται μία μονάδα κάθε φορά που η συσκευή ανάγνωσης/εγγραφής καρτών δεχτεί το απαραίτητο σήμα.

- Πιστοποίηση χρήστη στον παγκόσμιο ιστό. Στην εφαρμογή αυτή η συσκευή ανάγνωσης/εγγραφής καρτών συνδέεται με ηλεκτρονικό υπολογιστή ο οποίος είναι συνδεδεμένος στο διαδίκτυο. Ο προσφέρων την υπηρεσία επιτρέπει την πρόσβαση του τελικού χρήστη σε συγκεκριμένο πόρο, μόνο μετά την απαραίτητη πιστοποίηση.

- On-line χρέωση στον παγκόσμιο ιστό. Στην εφαρμογή αυτή η συσκευή ανάγνωσης/εγγραφής καρτών συνδέεται με ηλεκτρονικό υπολογιστή ο οποίος είναι συνδεδεμένος στο διαδίκτυο. Ο προσφέρων την υπηρεσία αφαιρεί από την κάρτα του τελικού χρήστη κάποιο ποσό χρημάτων με κάθε επίσκεψη του δεύτερου σε συγκεκριμένο πόρο που εκδίδει ο πρώτος.

Στις τέσσερις πρώτες εφαρμογές η συσκευή ανάγνωσης/εγγραφής καρτών μπορεί να συνδεθεί μέσω σειριακής θύρας με ηλεκτρονικό υπολογιστή ο οποίος τρέχει την εφαρμογή πράκτορα - διακομιστή συνδιαλλαγών (Transaction Agent) για την καταχώρηση των συνδιαλλαγών στη κεντρική βάση δεδομένων ή μπορεί να λειτουργήσει ανεξάρτητα (stand alone).

ΚΕΦΑΛΑΙΟ 3

Η ΧΡΗΣΗ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ

Στο κεφάλαιο αυτό περιγράφουμε την χρήση του συστήματος τόσο από την πλευρά του χρήστη όσο και από την πλευρά του διαχειριστή.

3.1 Εφαρμογή διαχείρισης καρτών-συσκευής.

Οι λειτουργίες που προσφέρονται χωρίζονται σε δύο γενικές κατηγορίες, αυτές που αναφέρονται στην κάρτα και αυτές που αναφέρονται στη συσκευή ανάγνωσης/εγγραφής καρτών. Για την κάρτα προσφέρονται ανάγνωση, εγγραφή και διαγραφή των τιμών που υπάρχουν σε κάθε κάρτα.

Συγκεκριμένα:

ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΑΡΤΑΣ		
ΠΕΔΙΟ	**ΠΕΡΙΓΡΑΦΗ**	**ΣΗΜΑΣΙΑ**
Group Id	**Αναγνωριστικός αριθμός ομάδας συσκευών**	**Η κάρτα χρησιμοποιείται μόνο από τις συσκευές που ανήκουν στη συγκεκριμένη ομάδα. Υποστηρίζονται 65 ομάδες συσκευών από 1000 συσκευές η κάθε μία. Κάθε συσκευή ανήκει σε μια ομάδα σύμφωνα με τη χιλιάδα του αναγνωριστικού της (Device Id).**
Card Id	**Αναγνωριστικός αριθμός κάρτας**	**Χαρακτηρίζει μοναδικά κάθε κάρτα**
Card PIN	**Προσωπικός αριθμός αναγνώρισης χρήστη**	**Προσωπικός αριθμός που πρέπει να γνωρίζει κάθε χρήστης για να χρησιμοποιεί την κάρτα του για εφαρμογές πρόσβασης (access control, web user authentication)**
Money	**Συνοπτικό ποσό χρημάτων**	**Χρησιμοποιείται για τις εφαρμογές cashless payment, web on-line payment**
Time	**Συνολικός χρόνος**	**Χρησιμοποιείται για την εφαρμογή χρονοχρέωσης (time debit)**
Units	**Μονάδες**	**Χρησιμοποιείται για την εφαρμογή χρέωσης με μονάδες (units debit)**

Για τη συσκευή προσφέρονται οι λειτουργίες:

- Σύνδεσης/Αποσύνδεσης (Connect/Disconnect) κατά την οποία μέσω της σειριακής θύρας η εφαρμογή συνδέεται/αποσυνδέεται με τη συσκευή ώστε να λάβει χώρα μια σύνοδος (session) διαχείρισης ή αντίστοιχα ο τερματισμός αυτής.

- Ανάκτησης κατάστασης συσκευής (Device Status).

- Προγραμματισμού συσκευής (Programming Device).

Στις δύο τελευταίες ανακτώνται/ρυθμίζονται τα χαρακτηριστικά της συσκευής που επεξηγούνται παρακάτω:

ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΣΥΣΚΕΥΗΣ		
ΠΕΔΙΟ	**ΠΕΡΙΓΡΑΦΗ**	**ΣΗΜΑΣΙΑ**
Application Id	**Αναγνωριστικό εφαρμογής που ανατίθεται στην συσκευή.**	**Εφαρμογή της συσκευής PIN-Access control Money- Money debit Time-Time debit Units-Units debit**
Device Id	**Αναγνωριστικός αριθμός συσκευής.**	**Η συσκευή χρησιμοποιεί κάρτες που έχουν καταχωρημένη την ομάδα που ανήκει η συσκευή. Η ομάδα των συσκευών καθορίζεται από το συγκεκριμένο πεδίο.**
PC Communication Critical	**Η σύνδεση με υπολογιστή είναι κρίσιμη ή όχι.**	**Αναφέρεται στο αν η συσκευή συνδέεται σε υπολογιστή για την καταχώρηση των συναλλαγών. Έτσι μπλοκάρεται κάποια εφαρμογή αν υπάρξει πρόβλημα στην επικοινωνία με την βάση δεδομένων**

Οι τιμές των χαρακτηριστικών πεδίων τόσο της κάρτας όσο και της συσκευής μπορούν να αποθηκευτούν και να ανακτηθούν από αρχείο.

Επίσης γίνεται έλεγχος μεγίστων, ελαχίστων και επιτρεπόμενων τιμών εισαγωγής καθώς και εμφάνιση μηνυμάτων για όλες τις καταστάσεις της δυάδας εφαρμογής-συσκευής και τα σφάλματα επικοινωνίας που μπορούν να συμβούν (π.χ. «Card Not Present. Please Insert Card»).

3.2 Διαχείριση της βάσης δεδομένων του συστήματος

Οι λειτουργίες που προσφέρονται είναι οι εξής:

- Εισαγωγή, ενημέρωση, διαγραφή εγγραφών για κάθε κατάλογο.

- Επίβλεψη της δραστηριότητας του συστήματος. Ο διαχειριστής αφού έχει επιλέξει κάποιον κατάλογο κάνοντας διπλό κλικ στο όνομα του καταλόγου που θέλει να επιβλέψει εμφανίζονται οι εγγραφές του καταλόγου.

3.3 Πράκτορας-διακομιστής συνδιαλλαγών (Transaction Agent)

Ο Transaction Agent συνδέεται με τις συσκευές ανάγνωσης/εγγραφής καρτών μέσω των σειριακών θυρών του υπολογιστή στον οποίο τρέχει. Αναλαμβάνει την καταγραφή των συνδιαλλαγών που γίνονται στις συνδεδεμένες σε αυτόν συσκευές στη κεντρική βάση δεδομένων δεχόμενος αιτήσεις για καταχώρηση από την κάθε μια συσκευή. Οι συσκευές είναι ρυθμισμένες η κάθε μια σε κάποια από τις τέσσερις εφαρμογές που αναφέρθηκαν. Η μεταφορά των δεδομένων του log γίνεται με τη χρήση ODBC ή HTTP πρωτοκόλλου. Για να συνδεθεί ο Transaction Agent με τη βάση δεδομένων θα πρέπει να εισαχθεί το κατάλληλο login name και password. Επίσης επιλέγεται το πρωτόκολλο σύνδεσης με τη βάση (ODBC Connection ή HTTP Connection). Η βάση μπορεί να βρίσκεται στον ίδιο υπολογιστή ή να είναι απομακρυσμένη.

3.4 Υποστήριξη πιστοποίησης χρήστη και ηλεκτρονικής χρέωσης για τον παγκόσμιο ιστό (web user authentication και web on-line payment).

3.4.1 Πιστοποίηση χρήστη (web user authentication)

Η κάρτα χρησιμοποιείται στην πιστοποίηση κάποιου χρήστη για να επιτραπεί η πρόσβαση του σε κάποιο πόρο συγκεκριμένης τοποθεσίας του παγκοσμίου ιστού (web site resource). Ο εκδότης (web master) του συγκεκριμένου πόρου διατηρεί τους πόρους σε καταλόγους, και για κάθε κατάλογο (directory) περιγράφει τον τύπο της πιστοποίησης που επιθυμεί για τον συγκεκριμένο κατάλογο. Πιο συγκεκριμένα οι τύποι πιστοποίησης που υποστηρίζονται είναι:

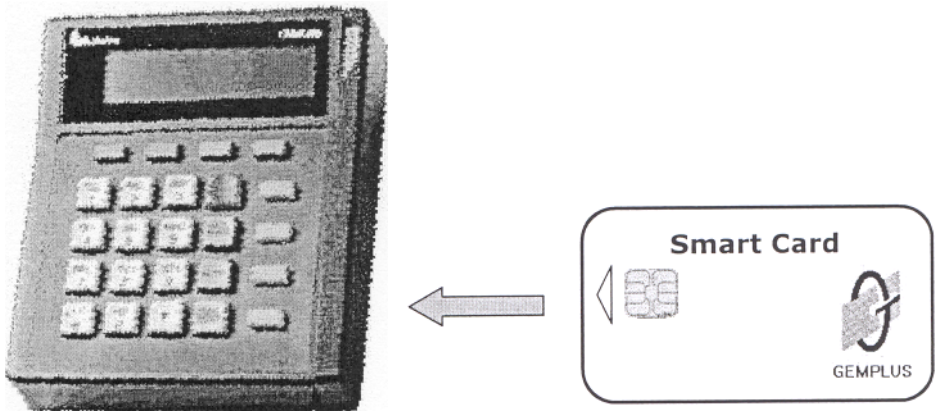
- Απλή χρήση κάρτας. Ο τελικός χρήστης έχει πρόσβαση στη σελίδα απλά με τη εισαγωγή της κάρτας στη συσκευή ανάγνωσης/εγγραφής καρτών.

- Χρήση κάρτας και εισαγωγή προσωπικού κωδικού. Ο τελικός χρήστης καλείται να εισάγει τον προσωπικό του κωδικό (PIN) για να αποκτήσει πρόσβαση στη σελίδα.

3.4.2 Ηλεκτρονική χρέωση για τον παγκόσμιο ιστό (web on-line payment)

Ο χρήστης έχει τη δυνατότητα να επισκεφτεί μια σελίδα αφού πρώτα χρεώσει την προσωπική του κάρτα ή να αγοράσει κάποιο προϊόν και να το χρεωθεί στην προσωπική του κάρτα. Ο εκδότης θα πρέπει για το ηλεκτρονικό εμπόριο, να υποστηρίζει και σύστημα καταχώρησης και εκτέλεσης παραγγελιών εκτός του να παρουσιάζει τα προϊόντα του στις σελίδες. Με την κατάλληλη εφαρμογή υποστήριξης επιτυγχάνεται η ολοκληρωμένη λειτουργία της αγοράς προϊόντων μέσω του διαδικτύου.

3.5 Συσκευή ανάγνωσης/εγγραφής καρτών



Σχήμα 3.5 Συσκευή ανάγνωσης/εγγραφής καρτών

Μία συσκευή ανάγνωσης/εγγραφής καρτών φαίνεται στο παραπάνω σχήμα. Μετά τον προγραμματισμό της συσκευής με την εφαρμογή διαχείρισης καρτών-συσκευής η συσκευή είναι έτοιμη να λειτουργήσει. Ο τελικός χρήστης καθοδηγείται με τα κατάλληλα μηνύματα τα οποία είναι ανάλογα με την εφαρμογή για την οποία έχει προγραμματιστεί η συσκευή.

Στην εφαρμογή ελέγχου πρόσβασης ζητείται η εισαγωγή του PIN και επιτρέπεται ή όχι η πρόσβαση ανάλογα με το αν το PIN που εισάγεται είναι αυτό που περιέχεται στην κάρτα.

Στην εφαρμογή χρηματικής χρέωσης εμφανίζεται στην οθόνη το ποσό χρημάτων και αφαιρείται από την κάρτα το ποσό που εισάγεται μέσω του πληκτρολογίου.

Στην εφαρμογή χρονοχρέωσης εμφανίζεται ο χρόνος που απομένει στην κάρτα, επιτρέπεται η χρήση της ηλεκτρονικής συσκευής με την οποία είναι συνδεδεμένη η συσκευή ανάγνωσης/εγγραφής καρτών και αρχίζει να αφαιρείται χρόνος.

Στην εφαρμογή χρέωσης μονάδων εμφανίζεται στην οθόνη το ποσό των μονάδων που περιέχει η κάρτα, επιτρέπεται η χρήση της ηλεκτρονικής συσκευής με την οποία είναι συνδεδεμένη η συσκευή ανάγνωσης /

εγγραφής καρτών και αφαιρείται μία μονάδα από την κάρτα κάθε φορά που η συσκευή ανάγνωσης/εγγραφής καρτών δεχτεί το απαραίτητο σήμα.

Στις εφαρμογές πιστοποίησης χρήστη και on-line χρέωσης στον παγκόσμιο ιστό ο έλεγχος περνάει στην εφαρμογή που τρέχει στον υπολογιστή του χρήστη.

Στις τέσσερις πρώτες εφαρμογές, και αν η συσκευή ανάγνωσης/εγγραφής καρτών έχει προγραμματιστεί ώστε η επικοινωνία με υπολογιστή να είναι κρίσιμη για την καταχώρηση των συνδιαλλαγών, κάθε φορά που εισάγεται μία κάρτα επιχειρείται η επικοινωνία με τον υπολογιστή μέσω της σειριακής θύρας. Αν αυτή αποτύχει εμφανίζεται κάποιο μήνυμα σφάλματος και ο χρήστης δεν μπορεί να συνεχίσει.

Σε όλες τις παραπάνω εφαρμογές πλην της χρονοχρέωσης ο χρήστης επιτρέπεται να βγάλει την κάρτα του οποιαδήποτε στιγμή. Στην περίπτωση της χρονοχρέωσης και επειδή ο χρήστης δεν θα έπρεπε να βγάζει την κάρτα του πριν αφαιρεθεί από αυτήν ο χρόνος που κατανάλωσε, η κάρτα σβήνεται αμέσως μόλις εισαχθεί και διαβαστεί. Τα δεδομένα της κρατούνται στην μνήμη της συσκευής, ο χρόνος χρήσης αφαιρείται από τα δεδομένα αυτά και η κάρτα ξαναγράφεται όταν ο χρήστης πατήσει το κουμπί ESC. Αν ο χρήστης τραβήξει την κάρτα οποιαδήποτε στιγμή εμφανίζεται ένα μήνυμα λάθους που τον προειδοποιεί να ξαναεισάγει την κάρτα του, διαφορετικά τα δεδομένα της κάρτας θα χαθούν.

Αυτός ο τρόπος λειτουργίας επιλέγεται για την προστασία αυτού που προσφέρει την εφαρμογή έτσι ώστε να μην υπάρχει περίπτωση χρήσης της ηλεκτρονικής συσκευής, χωρίς την αντίστοιχη χρέωση. Για την προστασία του χρήστη και για την περίπτωση που υπάρξει πρόβλημα στην λειτουργία της συσκευής ανάγνωσης/εγγραφής καρτών, όπως π.χ. διακοπή της τροφοδοσίας, τα δεδομένα κρατούνται εκτός από την μνήμη της συσκευής και σε nonvolatile μνήμη. Μια πιθανή διακοπή της τροφοδοσίας ανιχνεύεται και όταν η συσκευή τροφοδοτηθεί ξανά, διαβάζει τα δεδομένα από την nonvolatile μνήμη, εμφανίζει στην οθόνη το ανάλογο μήνυμα και ζητά από τον χρήστη να εισάγει την κάρτα του ώστε να επανεγγραφούν τα δεδομένα.

ΚΕΦΑΛΑΙΟ 4

Η SMART CARD GPM896

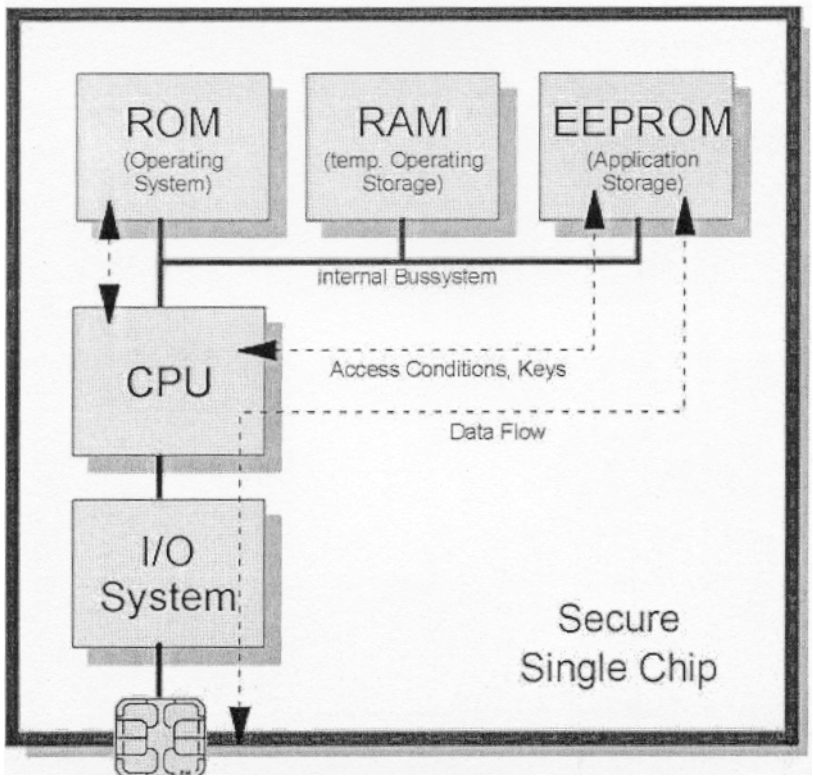
Στο κεφάλαιο αυτό περιγράφουμε και αναλύουμε τα τεχνικά χαρακτηριστικά και τις δυνατότητες που προσφέρει το μοντέλο μιας κάρτας που μπορεί να πραγματοποιήσει όλες τις εφαρμογές που αναφέρθηκαν στα προηγούμενα κεφάλαια.

4.1 Γενικά

Όπως είδαμε στην εισαγωγή της πτυχιακής, στην αγορά υπάρχει ένα πλήθος καρτών με διαφορετικά χαρακτηριστικά και η επιλογή μιας κάρτας γίνεται με βάση τις απαιτήσεις της εφαρμογής σε χωρητικότητα, ασφάλεια των δεδομένων, τρόπο ανάγνωσης/εγγραφής και φυσικά το κόστος. Θυμίζουμε ότι οι κάρτες χωρίζονται σε contact, contactless, όσον αφορά τον τρόπο ανάγνωσης/εγγραφής τους και σε μνήμης, μνήμης με λογική ασφάλειας και μνήμης με μικροεπεξεργαστή όσον αφορά το ολοκληρωμένο που περιέχουν. Στην συγκεκριμένη πτυχιακή θα αναλύσουμε μια κάρτα τύπου contact, με μνήμη με λογική ασφάλειας. Η λογική ασφάλειας προσφέρει μια πολύ καλή εξασφάλιση των δεδομένων έναντι κάποιας προσπάθειας ανάγνωσης/εγγραφής της κάρτας χωρίς φυσικά να φτάνει το επίπεδο ασφάλειας που προσφέρουν οι κάρτες μνήμης με μικροεπεξεργαστή. Η ασφάλεια του συστήματος μπορεί φυσικά να ενισχυθεί, με την κρυπτογράφηση των δεδομένων. Η κάρτα πρέπει να είναι επανεγγράψιμη (reloadable) και όχι, για παράδειγμα, κάποια από αυτές που χρησιμοποιούνται στην τηλεφωνία όπου οι μονάδες που περιέχουν "καίγονται" με την χρήση και στη συνέχεια η κάρτα είναι άχρηστη.

Μια σημαντική διαφορά των καρτών μνήμης με λογική ασφαλείας και αυτών με μικροεπεξεργαστή είναι ότι οι κάρτες με μικροεπεξεργαστή έχουν την δυνατότητα να πιστοποιήσουν την γνησιότητά τους στην συσκευή ανάγνωσης/εγγραφής. Αυτό γίνεται ως εξής: η συσκευή ανάγνωσης/εγγραφής και η κάρτα περιέχουν κατ' αρχήν το ίδιο κλειδί K. Η συσκευή ανάγνωσης/εγγραφής παράγει ένα τυχαίο αριθμό R και τον κωδικοποιεί χρησιμοποιώντας το κλειδί K. Το αποτέλεσμα της κωδικοποίησης R' στέλνεται στην κάρτα. Η κάρτα αποκωδικοποιεί το R', χρησιμοποιώντας το ίδιο κλειδί K, παράγοντας έτσι τον αριθμό X τον οποίο στέλνει στην συσκευή ανάγνωσης/εγγραφής. Αυτή συγκρίνει το X με τον αρχικό αριθμό R συμπεραίνοντας έτσι την γνησιότητα της κάρτας.

Επειδή τα R' και X αλλάζουν σε κάθε νέα επικοινωνία κάρτας και συσκευής η υποκλοπή τους δεν βοηθάει στην παραβίαση του συστήματος. Στο παρακάτω σχήμα βλέπουμε την εσωτερική αρχιτεκτονική μίας κάρτας με μικροεπεξεργαστή



Σχήμα 4.1 Η εσωτερική αρχιτεκτονική μίας κάρτας με μικροεπεξεργαστή

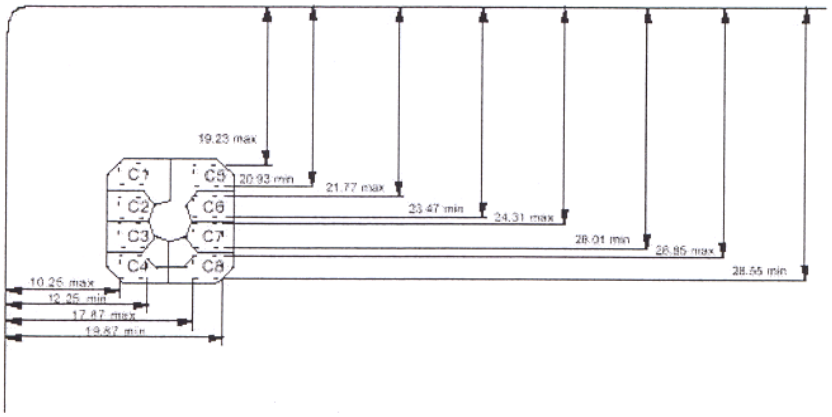
Στις κάρτες μνήμης το παραπάνω σχήμα πιστοποίησης είναι αδύνατο, λόγω του ότι η κάρτα δεν μπορεί να εκτελέσει καμία λειτουργία. Οι εντολές που δέχονται οι κάρτες μνήμης και ο τρόπος που αποκρίνονται σε αυτές είναι συγκεκριμένος. Οι εντολές αυτές περιγράφονται σε επόμενη παράγραφο.

4.2 Τεχνικά χαρακτηριστικά

Η κάρτα που θα δούμε είναι η GPM896 της Gemplus. Είναι μία χαμηλού κόστους, σύγχρονης επικοινωνίας smart card η οποία έχει 896-bit Electronically Erasable Programmable Read Only Memory (EEPROM). Τα γενικά χαρακτηριστικά της είναι τα ακόλουθα:

- συμβατή με ISO 7816
- εσωτερικά παραγόμενη τάση προγραμματισμού
- χρόνος πρόσβασης σε επίπεδο bit κατά την ανάγνωση 2 micro seconds
- απαίτηση μιας εξωτερικής τάσης 5Volt για όλες τις λειτουργίες
- 10000 κύκλους ανάγνωσης/εγγραφής
- διατήρηση δεδομένων για 10 χρόνια

Οι επαφές και η θέση τους φαίνεται στο παρακάτω σχήμα:

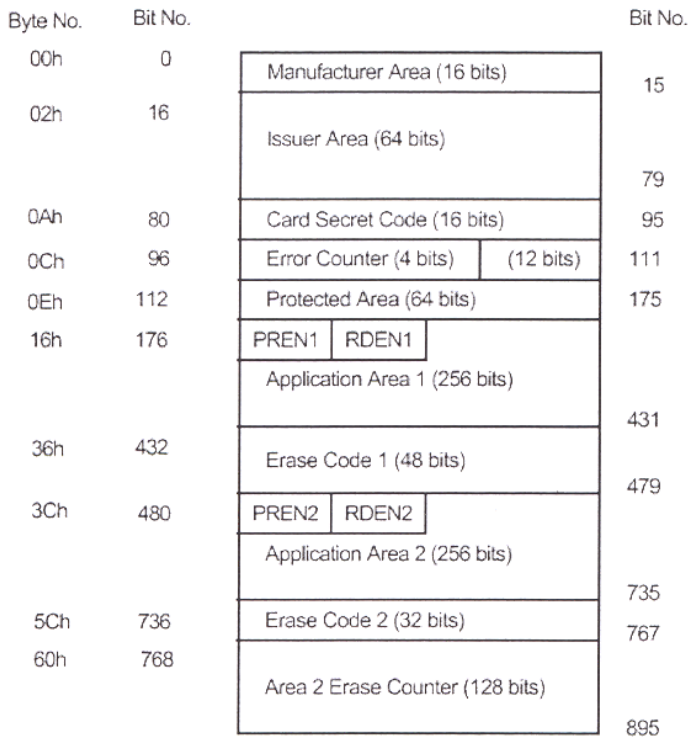


C1 = Vcc	C5 = Vss
C2 = RST	C6 = NC (Not connected)
C3 = CLK	C7 = I/O
C4 = FUSE	C8 = PROG

Σχήμα 4.2.1 Οι επαφές της GPM896

ΕΠΑΦΗ	ΛΕΙΤΟΥΡΓΙΑ
Vcc	**Τροφοδοσία της κάρτας (5Volt)**
RST	**Reset. Χρησιμοποιείται στην αρχή κάθε επικοινωνίας με την κάρτα.**
CLK	**Clock. Το ρολόι για την σύγχρονη επικοινωνία.**
FUSE	**Ηλεκτρική ασφάλεια μετά το κάψιμο της οποίας μεταβάλλονται οι συνθήκες πρόσβασης στη μνήμη.**
Vss	**Γείωση.**
NC	**Δεν χρησιμοποιείται.**
I/O	**Το Input/Output μέσω του οποίου η κάρτα επικοινωνεί με την συσκευή ανάγνωσης/εγγραφής.**
PROG	**Program. Χρησιμοποιείται για το γράψιμο και το σβήσιμο της κάρτας.**

Στο παρακάτω σχήμα φαίνεται η δομή της μνήμης της κάρτας



Σχήμα 4.2.2 Η δομή της μνήμης της κάρτας

Οι διάφορες περιοχές αναλύονται παρακάτω:

ΠΕΡΙΟΧΗ	ΣΗΜΑΣΙΑ
Manufacturer Area	**Τα περιεχόμενα αυτής της περιοχής γράφονται κατά την διάρκεια κατασκευής της κάρτας και δεν μπορούν να αλλαχθούν.**
Issuer Area	**Τα περιεχόμενα αυτής της περιοχής γράφονται κατά την διάρκεια προσωποποίησης της κάρτας και δεν μπορούν να αλλαχθούν.**
Card Secret Code	**Κωδικός ο οποίος πρέπει να παρουσιαστεί για να είναι δυνατή η πρόσβαση στις υπόλοιπες περιοχές της κάρτας.**
Error Counter Area	**Μετρητής ο οποίος μετράει τις λανθασμένες παρουσιάσεις του Card Secret Code. Μηδενίζεται μετά από κάθε σωστή παρουσίαση και μπλοκάρει την κάρτα μετά από ένα συγκεκριμένο αριθμό συνεχόμενων λανθασμένων παρουσιάσεων του Card Secret Code.**
Protected Area	**Περιοχή η οποία μπορεί να διαβαστεί ελεύθερα. Για το γράψιμο και την διαγραφή της απαιτείται η παρουσίαση του Card Secret Code.**
Application Area 1	**Περιέχει τα δεδομένα της εφαρμογής. Το γράψιμο και το διάβασμα τις καθορίζονται από τις τιμές των bits PREN1 και RDEN1 αντίστοιχα. Τα περιεχόμενα αυτής της περιοχής δεν μπορούν να διαγραφούν επιλεκτικά. Ολόκληρη η περιοχή διαγράφεται μετά από την παρουσίαση του Erase Code 1. Ο αριθμός των φορών που μπορεί να διαγραφεί είναι απεριόριστος.**
Erase Code 1	**Κωδικός ο οποίος πρέπει να παρουσιαστεί για να είναι δυνατή η διαγραφή της Application Area 1.**
Application Area 2	**Περιέχει τα δεδομένα της εφαρμογής . Το γράψιμο και το διάβασμα της καθορίζονται από τις τιμές των bits PREN2 RDEN2 αντίστοιχα. Τα περιεχόμενα αυτής της περιοχής δεν μπορούν να διαγραφούν επιλεκτικά. Ολόκληρη η περιοχή διαγράφεται μετά από την παρουσίαση του Erase Code 2. Ο αριθμός των φορών που μπορεί να διαγραφεί περιορίζεται στις 128.**
Erase Code 2	**Κωδικός ο οποίος πρέπει να παρουσιαστεί για να είναι δυνατή η διαγραφή της Application Area 2.**
Erase Counter	**Μετρητής ο οποίος μετράει τον αριθμό των διαγραφών της Application Area 2.**

Στο παρακάτω σχήμα φαίνονται οι συνθήκες πρόσβασης της μνήμης:

MEMORY AREA	READ	ERASE	WRITE
Manufacturer Area	**Enabled**	**Disabled**	**Disabled**
Issuer Area	**Enabled**	**Disabled**	**Disabled**
Card Secret Code	**Disabled**	**Enabled if CSC = 1**	**Enabled if CSC = 1**
Error Counter Area	**Enabled**	**Enabled if CSC = 1**	**Enabled**
Protected Area	**Enabled**	**Enabled if CSC = 1**	**Enabled if CSC = 1**
Application Area 1	**Enabled if RDEN1 = 1 or CSC = 1**	**Enabled if CSC = 1 and ESC1 = 1**	**Enabled if PREN1 = 1 and CSC = 1**
Erase Code 1	**Disabled**	**Disabled**	**Disabled**
Application Area 2	**Enabled if RDEN2 = 1 or CSC = 1**	**Enabled if CSC = 1 and ESC2 = 1 and EC = 1**	**Enabled if PREN2 = 1 and CSC = 1**
Erase Code 2	**Disabled**	**Disabled**	**Disabled**
Erase Counter	**Enabled**	**Disabled**	**Enabled**

Σχήμα 4.2.3 Οι συνθήκες πρόσβασης της μνήμης

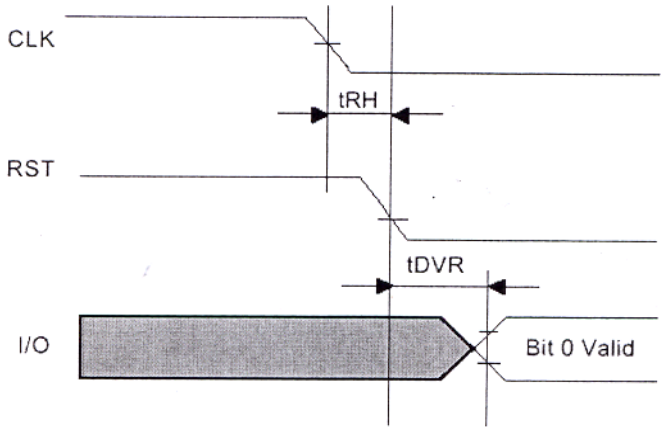
όπου CSC=1 μετά από επιτυχή παρουσίαση του Card Secret Code

4.3 Οι εντολές της κάρτας

Για την επικοινωνία με την κάρτα υπάρχουν πέντε εντολές οι οποίες καθορίζονται από τα control σήματα RST, CLK, PROG καθώς και από την θέση του εσωτερικού address counter.

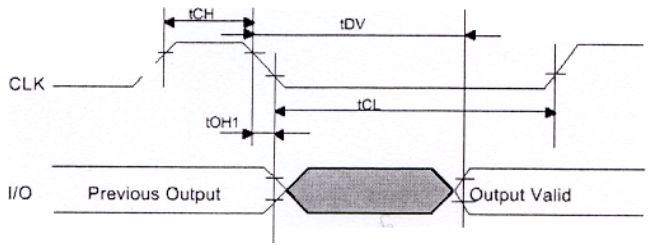
RESET

Μηδενίζει τον address counter στο 0. Τα δεδομένα του bit 0 στέλνονται στην Input/Output επαφή μόλις τα CLK και RST τεθούν στο 0. Τα δεδομένα είναι διαθέσιμα στην Input/Output επαφή μέχρι την επόμενη πτωτική ακμή του CLK.



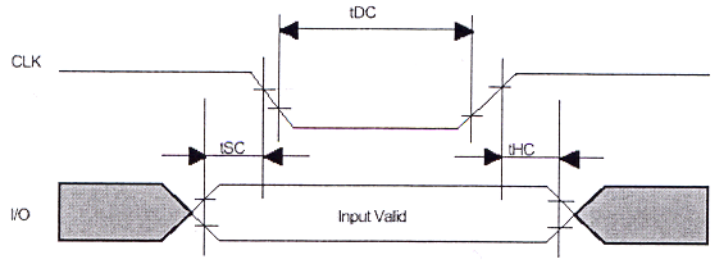
INCREMENT/READ

Ο address counter αυξάνεται κατά ένα σε κάθε ανοδική ακμή του CLK και ενώ τα PROG και RST είναι στο 0. Τα δεδομένα του addressed bit στέλνονται στην Input/Output επαφή σε κάθε πτωτική ακμή του CLK



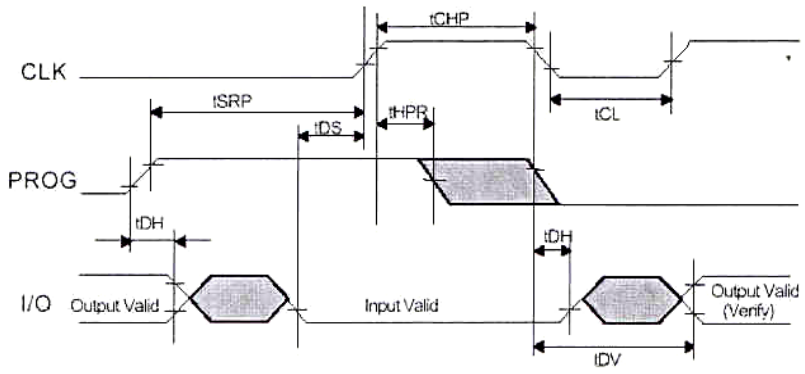
CMP

Συγκρίνει την τιμή στην Input/Output επαφή με αυτή του addressed bit. Χρησιμοποιείται για την παρουσίαση του Card Secret Code και του Erase Code. Για να εκτελέσουμε αυτή την εντολή κάνουμε τα εξής: θέτουμε τα RST και PROG στο 0,θέτουμε το CLK στο 1, τοποθετούμε την τιμή που θα συγκρίνουμε στην Input/Output επαφή και θέτουμε το CLK στο 0. Αυξάνουμε τον address counter με ανοδική ακμή του CLK. Επαναλαμβάνουμε το βήμα 2 έως ότου συγκρίνουμε όλα τα bits που θέλουμε.



WRITE

Το addressed bit γράφεται, δηλαδή τίθεται στο 0, ως εξής: θέτουμε την Input/Output επαφή στο 0 ενώ τα CLK και RST είναι 0 και το PROG είναι 1 και θέτουμε το CLK στο 1 για τουλάχιστον 5ms. Το bit που γράφτηκε τίθεται στην Input/Output επαφή κατά την πτωτική ακμή του CLK.



ERASE

Η λέξη (16 bits) που περιέχει το addressed bit διαγράφεται, δηλαδή τίθεται στο 1, ως εξής: θέτουμε την Input/Output επαφή στο 1 ενώ τα CLK και RST είναι 0 και το PROG είναι 1 και θέτουμε το CLK στο 1 για τουλάχιστον 5ms.

Οι χρόνοι που φαίνονται στα παραπάνω σχήματα έχουν ως εξής:

Parameter	Symbol	Min.	Max.	Unit
Clock frequency	fCLK	-	300	kHz
PROG setup time	tSRP	0.2	-	μs
PROG hold time	tHPR	0.2	tCHP	μs
Low level pulse width for CLK	tCL	0.2	-	μs
High level pulse width for CLK	tCH	0.2	-	μs
CLK programming pulse width	tCHP	5.0	-	ms
Input data setup time	tDS	0.2	-	μs
Input data hold time	tDH	0.0	-	μs
Output data hold time	tOH1	-	0.2	μs
Low level pulse width for CLK during code presentation	tDC	2.0	-	μs
Input data setup time for Erase Code presentation	tSC	0.0	-	μs
Input data hold time for code validation	tHC	0.2	-	μs
RST hold time (high level)	tRH	0.2	-	μs
Delay time for data validation	tDV	-	2.0	μs
Output delay to I/O high Z	tOH2	0.2	-	μs
Delay time for data validation after RESET	tDVR	-	2.0	μs

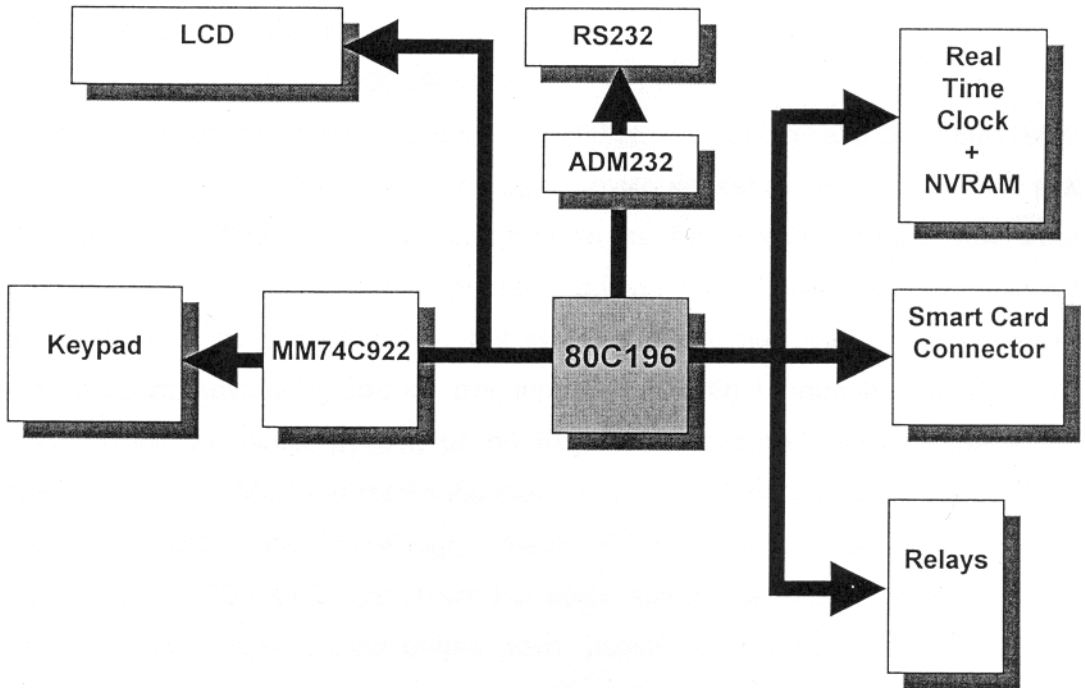
Η συχνότητα του ρολογιού μπορεί να είναι μέχρι 300KHz.

ΚΕΦΑΛΑΙΟ 5

Η ΣΥΣΚΕΥΗ ΑΝΑΓΝΩΣΗΣ/ΕΓΓΡΑΦΗΣ ΚΑΡΤΩΝ

5.1 Γενικά χαρακτηριστικά

Η συσκευή ανάγνωσης/εγγραφής καρτών είναι το βασικό μηχάνημα που χρησιμοποιείται για να διαβάζει και να γράφει κάρτες. Συνδέεται με relay στην συσκευή την οποία θέλουμε να ελέγξουμε ή να δώσουμε πρόσβαση μέσω της κάρτας, όπως για παράδειγμα σε πόρτα με ηλεκτρονική κλειδαριά, σε προσωπικό υπολογιστή, σε φωτοτυπικό μηχάνημα, κτλ. Αποτελείται από ένα μικροεπεξεργαστή στον οποίο συνδέουμε μονάδα απεικόνισης (LCD), πληκτρολόγιο (keypad), σειριακή θύρα RS232 για σύνδεση με προσωπικό υπολογιστή, ολοκληρωμένο με real time clock και nonvolatile RAM, smart card connector και 3 relays. Το block διάγραμμα μιας τέτοιας συσκευής φαίνεται στο παρακάτω σχήμα:



Σχήμα 5.1 Block διάγραμμα της συσκευής ανάγνωσης/εγγραφής καρτών

Τα τεχνικά χαρακτηριστικά της συσκευής ανάγνωσης/εγγραφής φαίνονται στον παρακάτω πίνακα:

ΤΕΧΝΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ	
Power Supply	**9 Volt DC**
Display	**2x16 LCD Alphanumeric**
Keypad	**16 Keys**
Card Type	**ISO 7816 Synchronous Memory Card**
Communication Speed with Card	**250 KHz**
Interface	**RS232 port**
RS232 Communication Speed	**56700 bps**
Memory	**242 bytes NVRAM**
Memory Backup	**Min 10 years. Lithium Battery**
Weight	**0.7 Kg approx.**
Dimensions (mm)	**220 (W) x 145 (D) x 55 (H)**

5.2 Υλοποίηση του hardware

5.2.1 Ο μικροεπεξεργαστής 80C196KC

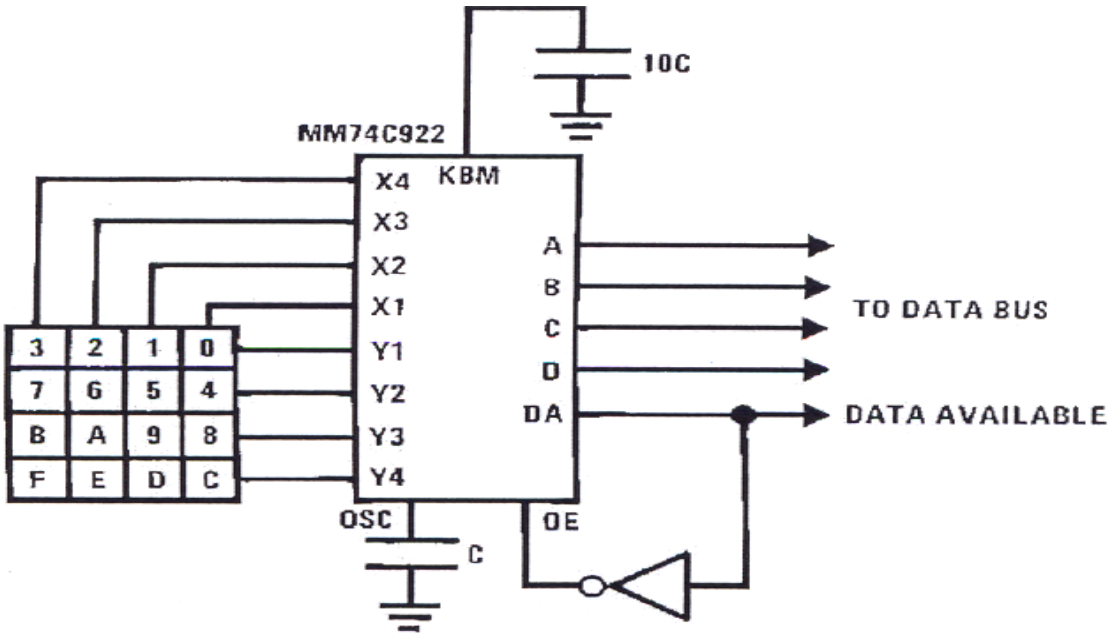
Για την υλοποίηση της συσκευής μπορεί να χρησιμοποιηθεί ο μικροεπεξεργαστής 80C196KC της Intel, ο οποίος μοιράζεται την ίδια αρχιτεκτονική και set εντολών με τα άλλα μέλη της οικογένειας MCS-96, και χρησιμοποιείται σε ένα πλήθος εφαρμογών όπως modems, motor-control systems, printers, engine-control systems, photocopiers, anti-lock brakes, air conditioner, control systems, λόγω της υψηλής του ταχύτητας τόσο στους υπολογισμούς όσο και στις input/output (I/O) λειτουργίες του. Πρόκειται για ένα 16-bit μικροεπεξεργαστή με 64 Kbytes addressable memory space, 512bytes εσωτερική RAM (συμπεριλαμβανομένων και των Special Function Registers, SFRs), 16 Kbytes One-Time-Programmable ROM και 16MHZ μέγιστη συχνότητα λειτουργίας. Ο 80C196KC έχει πέντε I/O ports των 8-bits, μερικές από τις οποίες είναι input μόνο, μερικές είναι output μόνο, μερικές είναι διπλής κατεύθυνσης και μερικές

υποστηρίζουν πολλαπλές λειτουργίες. Έχει επίσης σειριακή I/O θύρα η οποία είναι μία σύγχρονη/ασύγχρονη θύρα και περιλαμβάνει Universal Asynchronous Receiver and Transmitter (UART) με ένα σύγχρονο και τρία ασύγχρονα modes λειτουργίας. Έχει ακόμη δύο timers, High-Speed Input/Output (HSIO) Unit η οποία μπορεί να καταγράψει τους χρόνους εξωτερικών γεγονότων ή να προκαλέσει γεγονότα σε προκαθορισμένους χρόνους βασιζόμενη στους Timer 1 ή Timer 2 ,Analog-to-Digital Converter, Pulse Width Modulator (PWM) και Watchdog Timer.

5.2.2 Τα περιφερειακά και οι συνδέσεις τους με τον μικροεπεξεργαστή

Το LCD, μοντέλο M1632 της Seiko, συνδέεται στο port του μικροεπεξεργαστή. Για την εξοικονόμηση των output pins μπορούμε να χρησιμοποιήσουμε 4-bits για την μεταφορά των δεδομένων, αντί των 8-bits, κάτι που υποστηρίζεται από το συγκεκριμένο LCD. Επίσης τα σήματα ελέγχου του LCD, E,R/W και RS συνδέονται στα port pins του μικροεπεξεργαστή.

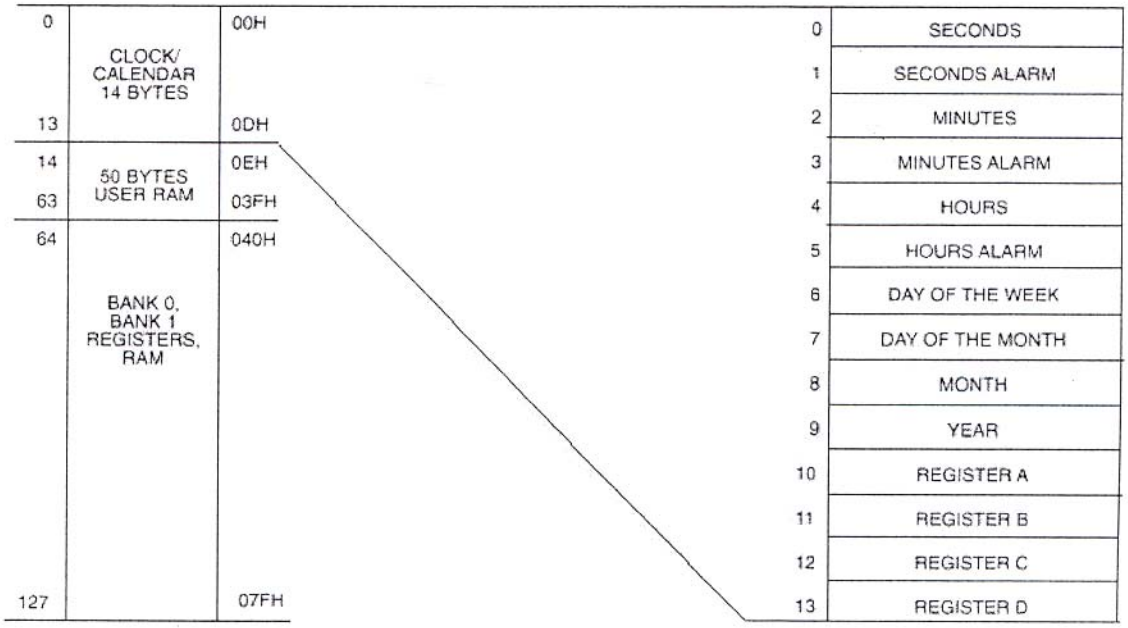
Το keypad συνδέεται μέσω ενός chip, π.χ. του MM74C922 της National Semiconductor. Το MM74C922 είναι ένας 16-key Encoder κατάλληλος για την σύνδεση ενός keypad με ένα μικροεπεξεργαστή με εύκολο έλεγχο του scan rate και του key debounce period μέσω πυκνωτών. Στο παρακάτω σχήμα φαίνεται η σύνδεση του MM74C922 με το keypad. Τα A, B, C, D συνδέονται στα P0.0-P0.3 του μικροεπεξεργαστή και το Data Available δίνει το interrupt στο P0.7 (EXTINT).



Σχήμα 5.2.2.1 Η σύνδεση του MM74C922 με το keypad

Για την υλοποίηση της σειριακής επικοινωνίας μπορούμε να χρησιμοποιήσουμε το ολοκληρωμένο ADM232A της Analog Devices το οποίο μετατρέπει τα TTL σήματα του μικροεπεξεργαστή σε σήματα συμβατά με την τάση που χρησιμοποιεί το RS-232 πρωτόκολλο και το αντίστροφο. Το DS1687 είναι ένα ολοκληρωμένο της Dallas Semiconductor που έχει Real Time Clock καθώς και 242 bytes nonvolatile RAM (NVRAM). Χρησιμοποιείται για την παραγωγή ενός interrupt κάθε 1 sec, και για αποθήκευση δεδομένων στη μνήμη.

Συνδέεται στο data bus (port 3) του μικροεπεξεργαστή. Η δομή της μνήμης του DS1687 φαίνεται στο παρακάτω σχήμα:



Σχήμα 5.2.2.2 Η δομή της μνήμης του DS1687

Το interrupt που δίνει στο pin P2.2 (EXTINT1) ανά ένα sec το Real Time Clock χρησιμοποιείται στην εφαρμογή χρονοχρέωσης για την μέτρηση του χρόνου. Στην nonvolatile μνήμη του DS1687 αποθηκεύονται κάποια δεδομένα απαραίτητα για την λειτουργία της συσκευής ανάγνωσης/εγγραφής, όπως το mode λειτουργίας της, καθώς και τα δεδομένα της κάρτας για την περίπτωση που υπάρξει διακοπή της τροφοδοσίας στην εφαρμογή χρονοχρέωσης ή ο χρήστης τραβήξει την κάρτα του χωρίς να πατήσει το πλήκτρο ESC (Όπως είπαμε και στο κεφάλαιο 3, στην εφαρμογή χρονοχρέωσης η κάρτα διαγράφεται αμέσως μόλις εισαχθεί και διαβαστεί).

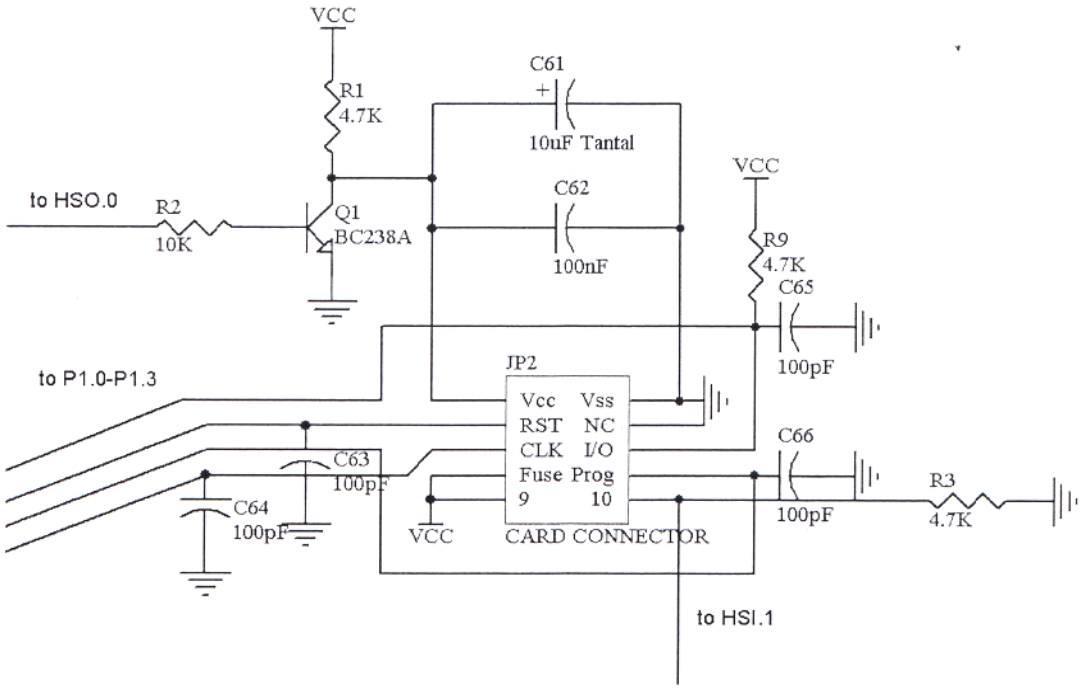
Συγκεκριμένα τα δεδομένα που αποθηκεύονται στην nonvolatile RAM φαίνονται στον παρακάτω πίνακα:

ΘΕΣΗ ΜΝΗΜΗΣ (Hex)	ΜΕΤΑΒΛΗΤΗ	ΠΕΡΙΓΡΑΦΗ
OE	**Power down**	**Δηλώνει αν υπήρξε ή δεν υπήρξε διακοπή τροφοδοσίας.**
OF	**Application Id**	**Εφαρμογή της συσκευής PIN-Access control Money- Money debit Time-Time debit Units-Units debit**
10	**PC Communication Critical**	**Αναφέρεται στον αν η συσκευή συνδέεται σε υπολογιστή για την καταχώρηση των συνδιαλλαγών.**
11-12	**Device Id**	**Αναγνωριστικό της συσκευής.**
13-21	**Card_buf**	**Δεδομένα της κάρτας.**

Τα Application Id, Device Id και PC Communication Critical αποθηκεύονται κάθε φορά που ο διαχειριστής του συστήματος προγραμματίζει την συσκευή ανάγνωσης/εγγραφής και διαβάζονται κάθε φορά που αυτή τροφοδοτείται.

Ο smart card connector και τα σήματα που χρειάζεται η κάρτα, I/O, RST, PROG και CLK συνδέονται στο port 1 του 80C196 και συγκεκριμένα στα P1.0-P1.3 .Για την σύλληψη της εισόδου και εξόδου της κάρτας χρησιμοποιείται το interrupt στο HSI.1 pin. Για την τροφοδοσία της κάρτας πρέπει να χρησιμοποιηθεί κατάλληλο κύκλωμα με transistor σε συνδεσμολογία κοινού εκπομπού το οποίο οδηγείται από το HSO.0 pin έτσι ώστε να είναι δυνατή η διακοπή της τροφοδοσίας σε περίπτωση που ο χρήστης τραβήξει την κάρτα. Για την προστασία της κάρτας και των δεδομένων της ο χρόνος που πρέπει να διακοπεί η τροφοδοσία σε μια τέτοια περίπτωση είναι μικρότερος του 1 ms.

Στο παρακάτω σχήμα φαίνονται οι συνδέσεις του smart card connector:



Σχήμα 5.2.2.3 Οι συνδέσεις του smart card connector

Τα relays συνδέονται στα port pins.Το πλήκτρο ESC δίνει ένα interrupt. Για την αφαίρεση μιας μονάδας στην εφαρμογή χρέωσης μονάδων απαιτείται ένα interrupt.Η τροφοδοσία της συσκευής γίνεται με 9Volt DC. Τα relays τροφοδοτούνται απευθείας με 9Volt, ενώ για την τροφοδοσία των ολοκληρωμένων που λειτουργούν με 5Volt χρησιμοποιείται ο ρυθμιστής τάσης LM7805C της National Semiconductor.

ΚΕΦΑΛΑΙΟ 6

Η ΑΣΦΑΛΕΙΑ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ

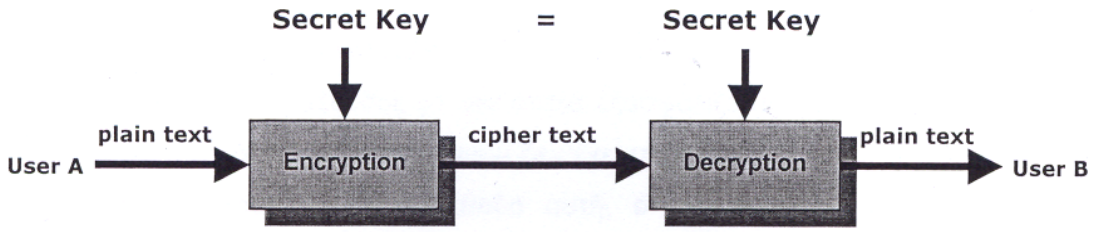
6.1 Γενικά

Για την ασφάλεια των δεδομένων που διακινούνται στο σύστημα είναι απαραίτητο να εισαχθούν μηχανισμοί που να εγγυούνται τόσο την ακεραιότητα τους όσο και την πιστοποίηση των μερών που συναλλάσσονται. Αυτό επιτυγχάνεται με τη δημιουργία ασφαλών καναλιών επικοινωνίας μεταξύ της συσκευής ανάγνωσης/εγγραφής και των εξυπηρετητών του συστήματος. Η επικοινωνία γίνεται ασφαλής με την χρησιμοποίηση πρωτοκόλλου ανταλλαγής κλειδιών και αλγορίθμων κρυπτογράφησης και πιστοποίησης.

6.1.1 Κρυπτογράφηση (Cryptography)

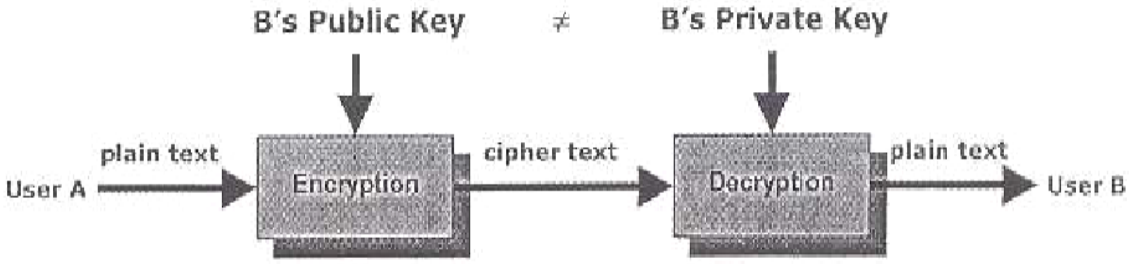
Ο βασικός σκοπός της κρυπτογράφησης είναι να δώσει την δυνατότητα σε δύο μέρη, να επικοινωνήσουν μέσω ενός απροστάτευτου καναλιού με τέτοιο τρόπο ώστε ένας αντίπαλος, να μην μπορεί να καταλάβει τι μεταδόθηκε. Η πληροφορία που το πρώτο μέρος θέλει να στείλει, την οποία αποκαλούμε plaintext μπορεί να είναι κείμενο, αριθμητικά δεδομένα ή οτιδήποτε άλλο. Ο αποστολέας κωδικοποιεί το plaintext χρησιμοποιώντας ένα προκαθορισμένο κλειδί και στέλνει το αποτέλεσμα, που ονομάζεται ciphertext, μέσω του καναλιού. Ο αντίπαλος μπορεί να υποκλέψει το ciphertext, παρακολουθώντας το κανάλι, αλλά δεν μπορεί να καταλάβει τι ήταν το αρχικό plaintext. Ο παραλήπτης όμως ο οποίος γνωρίζει το κλειδί, μπορεί να αποκωδικοποιήσει το ciphertext κατασκευάζοντας έτσι το αρχικό plaintext.

Η κρυπτογράφηση διακρίνεται σε συμμετρική (symmetric) και ασύμμετρη (asymmetric). Στην συμμετρική κρυπτογράφηση που αναφέρεται και σαν conventional cryptography υπάρχει ένα μοναδικό κλειδί (secret key) το οποίο γνωρίζουν και τα δύο μέρη που θέλουν να επικοινωνήσουν και χρησιμοποιείται και για την κρυπτογράφηση και για την αποκρυπτογράφηση.



Σχήμα 6.1.1.1 Συμμετρική κρυπτογράφηση

Στην ασύμμετρη κρυπτογράφηση που αναφέρεται και σαν public key cryptography ο αλγόριθμος κρυπτογράφησης είναι κατασκευασμένος έτσι ώστε το μήνυμα να κωδικοποιείται με ένα κλειδί και να αποκωδικοποιείται με ένα άλλο. Κάθε μέρος που συμμετέχει στην επικοινωνία έχει ένα δημόσια γνωστό κλειδί (public key) και ένα ιδιωτικό κλειδί (private key) το οποίο γνωρίζει μόνο αυτό. Ο αποστολέας ενός μηνύματος κωδικοποιεί το μήνυμα με το public key του παραλήπτη. Μόνο ο συγκεκριμένος παραλήπτης μπορεί να αποκωδικοποιήσει το μήνυμα χρησιμοποιώντας το δικό του private key.



Σχήμα 6.1.1.2 Ασύμμετρη κρυπτογράφηση

Η ασφάλεια ενός συστήματος κρυπτογράφησης περιγράφεται με δυο τρόπους. Ο πρώτος μετράει την ασφάλεια ενός συστήματος με βάση την υπολογιστική προσπάθεια που απαιτείται για να υποκλαπεί το σύστημα (computational security). Ορίζεται δηλαδή ότι ένα σύστημα κρυπτογράφησης είναι computationally secure, αν ο καλύτερος αλγόριθμος για να υποκλαπεί το σύστημα απαιτεί τουλάχιστον N πράξεις, όπου N είναι κάποιος καθορισμένος πολύ μεγάλος αριθμός. Ο δεύτερος τρόπος μετράει την ασφάλεια ενός συστήματος όταν δεν υπάρχει όριο στην υπολογιστική προσπάθεια που απαιτείται για να υποκλαπεί το σύστημα (unconditional security). Ορίζεται δηλαδή ότι ένα σύστημα κρυπτογράφησης είναι unconditional secure, αν δεν μπορεί να υποκλαπεί, ακόμη και με άπειρο

αριθμό πράξεων. Το εργαλείο με το οποίο μελετάται η ασφάλεια αυτών των συστημάτων (unconditional secure) είναι η θεωρία πιθανοτήτων.

6.1.2 Πιστοποίηση (Authentication)

Authentication είναι η μέθοδος με την οποία εξασφαλίζεται η ακεραιότητα (integrity) ενός μηνύματος, ότι δηλαδή το μήνυμα δεν έχει παραποιηθεί και ότι προέρχεται από τον "νόμιμο" αποστολέα. Στη μέθοδο αυτή, ο αποστολέας και ο παραλήπτης μοιράζονται το ίδιο κλειδί (secret key). Ο αποστολέας χρησιμοποιεί αυτό το κλειδί για να υπολογίσει μία σταθερού μήκους ετικέτα (authentication tag) μέσω κάποιας συνάρτησης που παίρνει σαν είσοδο το μήνυμα που θέλει να στείλει. Η ετικέτα αυτή στέλνεται στον παραλήπτη μαζί με το μήνυμα, ο οποίος χρησιμοποιώντας την ίδια συνάρτηση και το ίδιο κλειδί επαληθεύει την ακεραιότητα του μηνύματος. Σε κάθε νέα επικοινωνία το κλειδί αλλάζει. Έτσι η ασφάλεια του συστήματος είναι απόλυτη (unconditional security).

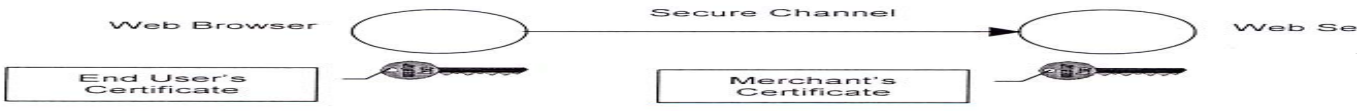
6.2 Οι μηχανισμοί ασφάλειας στο internet

Τα δύο πιο διαδεδομένα πρωτόκολλα για ασφάλεια στον παγκόσμιο ιστό είναι το SSL και το S-HTTP.

Το SSL (Secure Sockets Layer), αρχικά αναπτύχθηκε από τη Netscape. Η έκδοση που επιτρέπεται να εξαχθεί από τις Η.Π.Α. περιορίζεται σε κλειδιά μήκους 40 bits τα οποία μπορούν να βρεθούν από οποιονδήποτε με λογική υπολογιστική ισχύ ενώ η Netscape αναφέρει ότι χρειάζονται 64MIPS-years. Το SSL συνιστά ένα επίπεδο ασφαλείας ανάμεσα σε πρωτόκολλα εφαρμογών (HTTP, telnet, FTP) και το TCP/IP πρωτόκολλο. Προσφέρει κρυπτογράφηση δεδομένων, πιστοποίηση του εξυπηρετητή, ακεραιότητα μηνύματος, και επιλεκτικά πιστοποίηση πελάτη (client authentication) για μια σύνδεση με TCP/IP. Χρησιμοποιεί RSA encryption με τον RC4 αλγόριθμο για κρυπτογράφηση των δεδομένων, ενώ η τυποποίηση που ακολουθείται για τα πιστοποιητικά (certificates) είναι σύμφωνα με το πρότυπο X.509 .Τα πιστοποιητικά χρησιμοποιούνται για το authentication

του εξυπηρετητή ή του φυλλομετρητή και λαμβάνονται έπειτα από αίτηση του ενδιαφερόμενου χρήστη σε μια αναγνωρισμένη Certificate Authority (CA) στο διαδίκτυο όπως είναι η Verisign. Η λειτουργία της CA είναι να παρέχει certificate που προσφέρει υψηλή διαβεβαίωση για την ταυτότητα ενός συγκεκριμένου χρήστη, αφού επαληθεύσει την ταυτότητά του μέσω κάποιου νομικού εγγράφου όπως είναι η συμβατική του ταυτότητα και το δίπλωμα οδήγησής του. Το SSL χρησιμοποιείται από τις Mastercard και Visa Card.

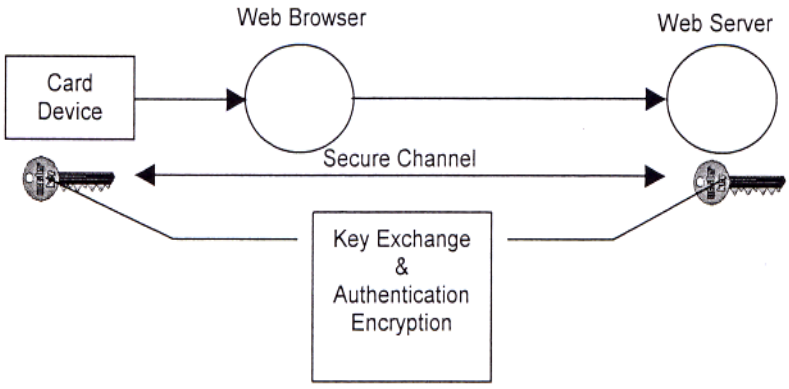
Το S-HTTP (Secure HyperText Transfer Protocol), έχει αναπτυχθεί από το Commerce Net Consortium. Προσφέρει τεχνικές security και encryption που στηρίζονται στις μεθόδους του Kerberos Security System και στην RSA public key cryptography αντίστοιχα. Η εταιρεία που επιθυμεί να το χρησιμοποιήσει διαθέτει δύο κλειδιά, εκδίδει το ένα και διατηρεί το άλλο, όπως περιγράφεται και παραπάνω με τη χρήση certificates. Χαρακτηρίζεται πιο ευέλικτο από το SSL που λόγω ακριβώς της θέσης της Netscape στην αγορά είναι πιο διαδεδομένο. Χαρακτηριστικό του και βασική διαφορά του είναι ότι ενώ το SSL εγκαθιστά μια ασφαλή σύνδεση ανάμεσα σε δύο υπολογιστές, το S-HTTP είναι σχεδιασμένο για να στέλνει ασφαλισμένα ατομικά μηνύματα σε επίπεδο εφαρμογής, και αποτελεί επέκταση του HTTP. Τα παραπάνω συγκλίνουν σε ένα κοινό standard που θα στεγάζει και τα δύο. Όπως φαίνεται, τα παραπάνω προσφέρουν ασφάλεια όσον αφορά τα στοιχεία που εισάγει ο τελικός χρήστης για κάποια ηλεκτρονική συνδιαλλαγή. Όπως credit card numbers.



Σχήμα 6.2.2.1 Μηχανισμός ασφάλειας σύμφωνα με τα SSL και S-HTTP

Το συγκεκριμένο πλάνο φαίνεται στο σχήμα. Το πρόβλημα που καλείται να λυθεί είναι η ασφάλεια όχι μόνο των δεδομένων που εισάγονται από

τον τελικό χρήστη αλλά και η ασφάλεια των δεδομένων που προέρχονται από τη συσκευή ανάγνωσης/εγγραφής καρτών. Έτσι για τα δεδομένα που προέρχονται από τη συσκευή δεν μπορούν να χρησιμοποιηθούν οι μηχανισμοί που προσφέρονται από τα παραπάνω πρωτόκολλα καθώς ένας επιδέξιος προγραμματιστικά τελικός χρήστης θα μπορούσε να εξαπατήσει τον εξυπηρετητή παγκοσμίου ιστού, κωδικοποιώντας τα δεδομένα της συσκευής με τη χρήση των μηχανισμών των συγκεκριμένων πρωτοκόλλων. Έτσι είναι απαραίτητο να υπάρξει ένα πρωτόκολλο ασφαλείας ανάμεσα στην συσκευή ανάγνωσης/εγγραφής καρτών και τον εξυπηρετητή, χρησιμοποιώντας τον υπολογιστή στον οποίο ο τελικός χρήστης τρέχει τον φυλλομετρητή σαν ενδιάμεσο κόμβο. Αυτό το πρωτόκολλο υλοποιείται με τους μηχανισμούς ανταλλαγής κλειδιών, κρυπτογράφησης και πιστοποίησης (key exchange, cryptography, authentication) που αναλύονται παρακάτω. Στο παρακάτω σχήμα φαίνεται το συγκεκριμένο πλάνο:



Σχήμα 6.2.2.2 Ο μηχανισμός ασφάλειας που υλοποιείται

6.3 Οι μηχανισμοί ασφάλειας των smart cards

Οι μηχανισμοί ασφάλειας που χρησιμοποιούνται για την προστασία των δεδομένων των καρτών είναι είτε hardware είτε software. Στους hardware μηχανισμούς τα εργοστάσια κατασκευής προσπαθούν να εξασφαλίσουν τα δεδομένα από μία ενδεχόμενη φυσική παραβίαση με κάποιο ηλεκτρονικό όργανο, κάτι που επιτυγχάνεται σε μεγάλο βαθμό αφού ο

μικροεπεξεργαστής και η μνήμη βρίσκονται σε ένα μόνο ολοκληρωμένο χωρίς να υπάρχει φυσική έκθεση των address, data ή control buses.

Παρ' όλα αυτά η προστασία των δεδομένων από μια ενδεχόμενη hardware παραβίαση είναι ένα θέμα ανοιχτό και υπό συζήτηση. Αν και οι κατασκευάστριες εταιρείες ισχυρίζονται ότι οι κάρτες είναι απόλυτα ασφαλείς, πρόσφατα δύο επιστήμονες που ασχολούνται με την κρυπτογράφηση έδειξαν ότι μπορούν να εξάγουν το μήκους 168-bits κλειδί κρυπτογράφησης του αλγόριθμου 3DES που χρησιμοποιείται στις smart cards. Η μέθοδος που χρησιμοποίησαν ήταν να εφαρμόσουν μικρά ποσά θερμότητας και ακτινοβολίας αλλάζοντας έτσι την δομή του κλειδιού. Στη συνέχεια χρησιμοποιώντας μια τεχνική που ονομάζεται Differential Fault Analysis, συνέκριναν τα κωδικοποιημένα outputs από κατεστραμμένες και κανονικές κάρτες βρίσκοντας το κλειδί.

Στους software μηχανισμούς χρησιμοποιείται κάποια από τις γνωστές τεχνικές κρυπτογράφησης. Στην συμμετρική κρυπτογράφηση η πιο διαδεδομένη μέθοδος είναι το Data Encryption Standard (DES). Το authentication δηλαδή η απόδειξη γνησιότητας της κάρτας από την συσκευή ανάγνωσης (reader) γίνεται ως εξής: Ο reader και η κάρτα περιέχουν κατ' αρχήν το ίδιο κλειδί K. Ο reader παράγει ένα τυχαίο αριθμό R και τον κωδικοποιεί χρησιμοποιώντας το κλειδί K. Το αποτέλεσμα της κωδικοποίησης R' στέλνεται στην κάρτα. Η κάρτα αποκωδικοποιεί το R', χρησιμοποιώντας το ίδιο κλειδί K, παράγοντας έτσι τον αριθμό X τον οποίο στέλνει στον reader. Αυτός συγκρίνει το X με τον αρχικό αριθμό R συμπεραίνοντας έτσι την γνησιότητα της κάρτας. Επειδή τα R' και X αλλάζουν σε κάθε νέα επικοινωνία κάρτας και reader η υποκλοπή τους δεν βοηθάει στην παραβίαση του συστήματος.

Στην ασύμμετρη κρυπτογράφηση οι δύο πιο διαδεδομένοι μέθοδοι είναι το Rivest - Shamir - Adleman (RSA) και το Digital Signature Standard (DSS). Στις μεθόδους αυτές κάθε κάρτα περιέχει ένα private κλειδί, ενώ ένα public κλειδί εκχωρείται για κάθε κάρτα. Όταν η κάρτα εισάγεται στον reader αυτός παράγει ένα τυχαίο αριθμό R και τον στέλνει στην κάρτα. Η κάρτα κωδικοποιεί αυτόν τον αριθμό με κάποια από τις παραπάνω μεθόδους (RSA ή DSS) χρησιμοποιώντας το private κλειδί της και στέλνει το κωδικοποιημένο αποτέλεσμα R' στον reader. Στέλνει επίσης στον reader και το public κλειδί της με τη μορφή ενός certificate το οποίο είναι ένα είδος digital signature. Το certificate αυτό είναι το public κλειδί της κάρτας κωδικοποιημένο με το private κλειδί μιας Certificate Authority (CA). Η CA εμποδίζει την χρήση ψεύτικων public κλειδιών βεβαιώνοντας ότι το

public κλειδί ανήκει σε αυτόν που ισχυρίζεται κάτι τέτοιο. Όταν ο reader πάρει το certificate της κάρτας το αποκωδικοποιεί χρησιμοποιώντας το public κλειδί της CA υπολογίζοντας έτσι το public κλειδί της κάρτας. Στην συνέχεια χρησιμοποιεί αυτό το κλειδί για να αποκωδικοποιήσει τον αριθμό R' που του έστειλε η κάρτα. Αν το αποτέλεσμα είναι ίδιο με τον αρχικό αριθμό R που παρήγαγε ο reader τότε η κάρτα είναι γνήσια. Και πάλι η υποκλοπή των R και R' δεν αρκεί για την παραβίαση της ασφάλειας του συστήματος αφού αυτά αλλάζουν σε κάθε νέα επικοινωνία κάρτας και reader.

Σε σύγκριση, η συμμετρική κρυπτογράφηση (DES) απαιτεί λιγότερη υπολογιστική ισχύ και λιγότερη μνήμη για την υλοποίησή της από την ασύμμετρη (RSA και DSS) γι' αυτό και η πλειοψηφία των σημερινών καρτών την χρησιμοποιούν. Το πρόβλημα με την συμμετρική κρυπτογράφηση είναι ότι η ασφάλεια μειώνεται από την ανάγκη χρησιμοποίησης του ίδιου κλειδιού. Για την χρησιμοποίηση της κάρτας σε πολλές εφαρμογές θα πρέπει ο παρέχων την κάθε εφαρμογή να γνωρίζει το κλειδί αυτό και ενδεχόμενη παραβίαση του κλειδιού θα σήμαινε και την αποκωδικοποίηση όλης της κάρτας και όλων των εφαρμογών. Αντίθετα χρησιμοποιώντας ασύμμετρη κρυπτογράφηση η παραβίαση του private κλειδιού της κάρτας δεν σημαίνει και παραβίαση του συστήματος αφού ο υποκλοπέας θα πρέπει να γνωρίζει και το private κλειδί της CA.

Οι κάρτες που χρησιμοποιούν RSA περιέχουν ένα επεξεργαστή, εκτός από τον κανονικό, ο οποίος είναι αφιερωμένος και βελτιστοποιημένος ώστε να εκτελεί τους υπολογισμούς που απαιτεί το RSA σε λογικό χρόνο, και ο οποίος καταλαμβάνει χώρο στο chip στη θέση όπου κανονικά θα χρησιμοποιούνταν για μνήμη. Η EEPROM μνήμη των καρτών περιορίζεται σε 8 Kbytes (οι κάρτες που χρησιμοποιούν DES φτάνουν τα 8 Kbytes) και το κόστος της κάρτας αυξάνει. Στο μέλλον πάντως, με την ανάπτυξη της τεχνολογίας και την μείωση του κόστους, όλες οι smart cards προβλέπεται ότι θα χρησιμοποιούν ασύμμετρη κρυπτογράφηση αντί της συμμετρικής.

Οι παραπάνω μηχανισμοί παρά το ότι παρέχουν υψηλού επιπέδου ασφάλεια δεν πρέπει να παραβλέψουμε το γεγονός ότι όσο η τεχνολογία

προοδεύει και η επιστημονική κοινότητα ‘γεννάει’ δυνατά και με υπομονή ‘μυαλά’ αυτοί θα παραβιάζονται ξανά και ξανά. Είναι καθαρά θέμα χρόνου για κάποιον με γνώσεις, να κατανοήσει πως δουλεύει το σύστημα και μετά να το ‘οδηγήσει’ όπως αυτός επιθυμεί. Ίσως, αυτός ο φόβος της μη απόλυτης ασφάλειας να κάνει όλες αυτές τις εταιρίες να δαπανάνε εκατομμύρια στην έρευνα για το συγκεκριμένο θέμα και αυτό μόνο καλό κάνει εντέλει, αφού δεν υπάρχει εφησυχασμός κι η τεχνολογία προχωρά όχι μόνο συνέχεια αλλά και με πολύ γρήγορους ρυθμούς προσφέροντας ότι καλύτερο στον καταναλωτή αλλά και στις εταιρίες για την προστασία των προϊόντων τους.

6.4 Μαθηματική τεκμηρίωση

Στις επόμενες τρεις παραγράφους περιγράφουμε τους μηχανισμούς κρυπτογράφησης, πιστοποίησης και ανταλλαγής κλειδιού. Ο αλγόριθμος κρυπτογράφησης Affine Cipher μπορεί να εφαρμοστεί στα δεδομένα της κάρτας και στο πακέτο επικοινωνίας μεταξύ συσκευής ανάγνωσης/εγγραφής και του εξυπηρετητή παγκοσμίου ιστού (Web Server), ενώ η πιστοποίηση και η ανταλλαγή κλειδιού γίνεται μεταξύ της συσκευής ανάγνωσης/εγγραφής και του εξυπηρετητή παγκοσμίου ιστού. Για την ανταλλαγή κλειδιού χρησιμοποιείται το πρωτόκολλο Diffie-Hellman.

6.4.1 Cryptography

Διατυπώνοντας τα γενικά περί κρυπτογράφησης με ένα αυστηρά μαθηματικό τρόπο έχουμε ότι ένα σύστημα κρυπτογράφησης ορίζεται σαν μια πεντάδα (P,C,K,E,D)

Όπου:

1. P είναι ένα πεπερασμένο σύνολο πιθανών plaintexts
2. C είναι ένα πεπερασμένο σύνολο πιθανών ciphertexts

3. *K* είναι ένα πεπερασμένο σύνολο πιθανών κλειδιών

4. Για κάθε Κϵ*K* υπάρχει ένας κανόνας κρυπτογράφησης $e_κ$ ϵ *E* και ένας αντίστοιχος κανόνας αποκρυπτογράφησης $d_κ$ ϵ *D*. Κάθε: $e_κ$:*P*→ *C* και $d_κ$:*C*→*P* είναι τέτοιες συναρτήσεις ώστε $d_κ$ ($e_κ$ (x))= x για κάθε plaintext x ϵ *P*

Η κύρια ιδιότητα είναι η ιδιότητα 4, σύμφωνα με την οποία αν ένα plaintext x κωδικοποιηθεί χρησιμοποιώντας την συνάρτηση $e_κ$ και το παραγόμενο ciphertext αποκωδικοποιηθεί χρησιμοποιώντας την συνάρτηση $d_κ$ τότε το αποτέλεσμα είναι το αρχικό plaintext x.

Είναι φανερό επίσης ότι η συνάρτηση κρυπτογράφησης $e_κ$ πρέπει να είναι ένα προς ένα, διαφορετικά η αποκρυπτογράφηση θα είναι αδύνατη. Αν για παράδειγμα y= $e_κ(x_1)$= $e_κ(x_2)$, όπου x_1 , x_2 είναι plaintexts και y είναι ciphertext με $x_1 \neq x_2$ τότε είναι αδύνατο να διαπιστωθεί αν το ciphertext y αποκρυπτογραφείται στο plaintext x_1ή στο x_2.

Για την κρυπτογράφηση των δεδομένων της κάρτας όπως είπαμε μπορεί να χρησιμοποιηθεί ο αλγόριθμος Affine Cipher ο οποίος ορίζεται ως εξής:

Έστω *P*=*C*=Z_{256} και *K*={(a,b) ϵ Z_{256} x Z_{256}:gcd(a,256) =1}.

Για K=(a,b) ε *K* ,ορίζουμε $e_κ$(x)=ax + b mod256 και
$d_κ$(y)=a^{-1}(y-b) mod256, (x,y ϵ Z_{256}), όπου a^{-1} είναι το multiplicative inverse του a και ορίζεται ως εξής:

Έστω a ϵ *Zm*. Το multiplicative inverse του a είναι ένα στοιχείο a^{-1} τέτοιο ώστε $aa^{-1}≡a^{-1}a≡1(mod m)$. Μπορεί εύκολα να δειχθεί ότι το a έχει ένα multiplicative inverse modulo m αν και μόνο αν gcd(a,*m*) =1.
Επίσης ότι αν το multiplicative inverse υπάρχει, τότε είναι μοναδικό.
Ο αριθμός των κλειδιών του συγκεκριμένου αλγορίθμου είναι axb με το a να υπόκειται στον περιορισμό gcd(a,256) =1.

Γενικά ο αριθμός των a που ικανοποιούν το gcd(a,*m*)=1 ορίζεται σαν φ(*m*) και βρίσκεται με την Euler phi- function που ορίζεται ως εξής:

Κάθε ακέραιος m >1 μπορεί να παραγοντοποιηθεί σαν γινόμενο δυνάμεων πρώτων αριθμών με μοναδικό τρόπο.

Αν $m = \prod_{i=1}^{n} p_i^{e_i}$ όπου P_i πρώτοι αριθμοί και $e_i > 0$, $1 \leq \boldsymbol{i} \leq$n τότε:

$$\phi(m) = \prod_{i=1}^{n} \left(p_i^{e_i} - p_i^{e_i - 1} \right)$$

Π.χ.: $256=2^8$ και $\varphi(256)=2^8-2^7 =128$. Άρα ο αριθμός των κλειδιών είναι 128 x 256 = 32768 (μήκος κλειδιού = 15 bits).

6.4.2 Authentication

Ομοίως για το authentication έχουμε ότι ο authentication code ορίζεται σαν μια τετράδα (*S,A,K,E*) όπου:

1. *S* είναι ένα πεπερασμένο σύνολο πιθανών source states

2. *A* είναι ένα πεπερασμένο σύνολο πιθανών authentication tags

3. K είναι ένα πεπερασμένο σύνολο πιθανών κλειδιών

4. Για κάθε K ϵ *K*, υπάρχει ένας authentication κανόνας $e_κ$: $S \rightarrow A$

Το μήνυμα ορίζεται ως: M = S x A

Σημειώνουμε ότι source state είναι το ανάλογο του plaintext. Ένα μήνυμα αποτελείται από το plaintext μαζί με ένα προσαρτώμενο authentication tag.

Για να επικοινωνήσουν λοιπόν δύο μέρη ακολουθούν το εξής πρωτόκολλο: Πρώτα διαλέγουν ένα τυχαίο κλειδί K ϵ *K*. Στην συνέχεια υποθέτοντας ότι

ο αποστολέας θέλει να στείλει το source state s ϵ *S* υπολογίζει το authentication tag a = $e_\kappa(s)$ και στέλνει το μήνυμα (s,a). Ο παραλήπτης λαμβάνει το (s,a) και υπολογίζει το a' = $e_\kappa(s)$. Αν a' = a τότε δέχεται το μήνυμα αλλιώς το απορρίπτει.

Αν για παράδειγμα το πακέτο αποτελείται από 20 bytes από τα οποία τα 19 είναι πληροφορία και το τελευταίο είναι το authentication tag και θεωρώντας σαν s το άθροισμα των 19 bytes έχουμε $S=Z_{4846}$. Ο authentication κανόνας είναι $e_\kappa(s)$=ks mod256 με $K=A=Z_{256}$

Η deception probabiIity, δηλαδή η πιθανότητα να εξαπατήσει κάποιος το σύστημα, στέλνοντας το μήνυμα (s,a) και αυτό να γίνει δεκτό είναι 1/256. Στο παραπάνω σχήμα τα δύο συστήματα που εκτελούν την επικοινωνία χρησιμοποιούν το ίδιο κλειδί K για να υπολογίσουν το authentication tag. Το κλειδί αυτό δεν θα πρέπει να είναι το ίδιο σε κάθε επικοινωνία διότι, επειδή ανήκει στο διάστημα [0,255] , θα αρκούσαν κατά μέσω όρο 128 προσπάθειες για να βρεθεί. Για αυτόν τον λόγο το κλειδί πρέπει να αλλάζει σε κάθε επικοινωνία.

6.4.3 Ανταλλαγή κλειδιού (key exchange)

Για την επιλογή του ίδιου κλειδιού από τα δύο μέρη που εκτελούν την επικοινωνία υπάρχουν οι μέθοδοι key distribution και key agreement. Στην πρώτη μέθοδο το ένα μέρος διαλέγει ένα κλειδί και το στέλνει στο άλλο. Στην δεύτερη τα δύο μέρη υπολογίζουν μέσω κάποιας συνάρτησης το ίδιο κλειδί χρησιμοποιώντας σαν input κάποια δεδομένα που στέλνει το ένα στο άλλο. Ακόμη και αν κάποιος παρακολουθεί το κανάλι επικοινωνίας και παρακολουθεί αυτά τα δεδομένα δεν μπορεί να υπολογίσει το κλειδί. Για την επιλογή του κλειδιού χρησιμοποιείται η μέθοδος key agreement και μπορεί να επιλεχθεί το Diffie-Hellman πρωτόκολλο το οποίο περιγράφεται παρακάτω:

Έστω U, V, τα δύο μέρη που θέλουν να επικοινωνήσουν.

Έστω ακόμη ένας πρώτος αριθμός P και ένας a ϵ Zp^* .

Ο U διαλέγει ένα τυχαίο αριθμό a_u , $0 \leq a_u \leq p$-2 , υπολογίζει το $b_u = a^{au} \bmod p$ και το στέλνει στον V.

Ο V διαλέγει ένα τυχαίο αριθμό a_v, $0 \leq a_v \leq p$- 2 , υπολογίζει το $b_v = a^{av} \bmod p$ και το στέλνει στον U.

Στην συνέχεια υπολογίζει το $K_{u,v} = b_u^{av} = (a^{au})^{av} \bmod p$.

Ο U υπολογίζει το $K_{u,v} = b_v^{au} = (a^{av})^{au} \bmod p$.

Στο τέλος της επικοινωνίας και οι δύο έχουν υπολογίσει το κοινό κλειδί $K_{u,v} = a^{av*au} \bmod p$.

ΣΥΜΠΕΡΑΣΜΑΤΑ - ΜΕΛΛΟΝΤΙΚΕΣ ΕΠΕΚΤΑΣΕΙΣ

7.1 Συμπεράσματα

Όπως είδαμε στην πτυχιακή αυτή αναλύθηκε ένα ολοκληρωμένο σύστημα για την κάλυψη μιας πληθώρας εφαρμογών με smart cards. Ας θυμηθούμε τις εφαρμογές:

- έλεγχος πρόσβασης (access control)
- χρηματική χρέωση (cashless payment)
- χρονοχρέωση (time debit)
- χρέωση μονάδων (units debit)
- πιστοποίηση χρήστη στον παγκόσμιο ιστό (web user authentication)
- on-line χρέωση στον παγκόσμιο ιστό (web on-line payment)

Οι παραπάνω εφαρμογές καθώς κι άλλες που προτείνονται παρακάτω, θα μπορούσαν να υλοποιούνται μέσω της ίδιας συσκευής ανάγνωσης/εγγραφής και της ίδιας κάρτας (muIti-appIication card). Μεγάλη έμφαση στον σχεδιασμό τέτοιων συστημάτων πρέπει να δίνεται στην ασφάλεια του συστήματος. Η υλοποίηση μηχανισμών κρυπτογράφησης και πιστοποίησης εγγυάται την ασφάλεια αυτή και είναι το σημαντικότερό μέρος του όλου σχεδιασμού αφού ότι πολύ-εφαρμογές και αν πράττει, παρέχει μια smart card εάν δεν είναι ασφαλή τότε είναι όχι μόνο άχρηστη αλλά κι επιβλαβής για τον χρήστη. Στην πτυχιακή αυτή παρουσιάστηκαν όλα τα απαραίτητα εργαλεία για την διαχείριση και παρακολούθηση του συστήματος. Τα υπάρχοντα διαθέσιμα στην αγορά συστήματα δουλεύουν με διαφορετικές συσκευές και κάρτες λόγω του ότι προσφέρονται από διαφορετικές εταιρείες. Επίσης η υπηρεσία πιστοποίησης χρήστη στον παγκόσμιο ιστό (web user authentication) προσφέρεται από μία μόνο εταιρεία, την Imagine Card AIIiance (Gemplus, HewIett-Packard, Informix), ενώ η υπηρεσία on-line χρέωσης στον παγκόσμιο ιστό είναι μια καινοτομία.

7.2 Μελλοντικές επεκτάσεις

Εκτός από την παραδοσιακή χρήση των καρτών για τηλεφωνία, πιστωτικές

κάρτες, ταυτοποίησης ταυτότητας και έλεγχος πρόσβασης σε συγκεκριμένους χώρους υπάρχουν πολλές εφαρμογές ακόμα που μπορούν να κάνουν τις ήδη έξυπνες κάρτες, εξυπνότερες, πάντα προς όφελος του χρήστη φυσικά.

Για παράδειγμα, μια κάρτα η οποία θα πρόσφερε τη δυνατότητα δανεισμού βιβλίων από οποιαδήποτε βιβλιοθήκη θα ήταν μια υπηρεσία ιδιαίτερα χρήσιμη ιδίως για τους μαθητές-σπουδαστές οι οποίοι είναι αναγκασμένοι να περιμένουν ώρες σε ουρές για τον συγκεκριμένο σκοπό. Αυτό φυσικά θα διευκόλυνε και τα ιδρύματα, τα οποία πρέπει να απασχολούν πολυάριθμο προσωπικό ιδίως τις μέρες των εγγραφών. Το ίδιο σύστημα θα μπορούσε να χρησιμοποιηθεί και για την χρήση του φωτοτυπικού ή και γενικότερα για οποιοδήποτε μηχάνημα εξυπηρέτησης ή παροχής υπηρεσιών τέτοιου τύπου.

Οι έξυπνες κάρτες (smart cards) με μικροεπεξεργαστή μπορούν να υποστηρίζουν παράλληλα διαφορετικές εφαρμογές, όπως την αποθήκευση ιατρικών δεδομένων όπου ακόμα και αν ο ασθενής δεν δύναται να πληροφορήσει για το ιστορικό του λόγω της κατάστασης του, αυτό πλέον θα είναι εύκολο με την εισαγωγή της κάρτας του σε κάποιο τερματικό.

Με τον ίδιο τρόπο ένα μεγάλο μέρος της γραφειοκρατίας και πολλοί τόνοι χαρτιού μπορούν να εξαλειφθούν αφού για οποιαδήποτε συναλλαγή του με οργανισμούς όπως το Ι.Κ.Α. , Τ.Ε.Β.Ε. , Ο.Γ.Α. κτλ, δεν θα απαιτείται κανένα έγγραφο για την πληρωμή ενσήμων ή ασφάλιστρων αφού αυτό μπορεί να γίνεται on-line από οποιοδήποτε τερματικό (ΑΤΜ) των ιδίων οργανισμών ή ακόμα και τραπεζών.

Τέλος μια πρωτοποριακή πρόταση, η οποία εκτός από εξοικονόμηση χρόνου και αποφυγή της ταλαιπωρίας που λέγεται "Πληρωμή λογαριασμών σε ταμεία" για τους καταναλωτές μπορεί να δώσει τεράστια οικονομική πνοή τόσο στο δημόσιο όσο και στις ιδιωτικές επιχειρήσεις οι οποίες έχουν ένα ολόκληρο "στόλο" για την είσπραξη λογαριασμών. Τοποθετώντας ένα τερματικό στο σπίτι , θα δίνεται η δυνατότητα μέσω του αριθμού του λογαριασμού που θέλουμε να πληρώσουμε και την είσοδο στο τερματικό μιας smart card η οποία είναι συνδεδεμένη με ένα δικό μας λογαριασμό τραπέζης να πληρώσουμε γρήγορα και άμεσα χωρίς καμία αναμονή σε ουρές, χωρίς χρήση μεταφορικού μέσου για να πάμε στη

τράπεζα (οικονομικό και οικολογικό ιδίως για τα μεγάλα αστικά κέντρα όπου οι θέσεις Parking είναι ελάχιστες και η μόλυνση του περιβάλλοντος τεράστια), και πάνω από όλα χωρίς καμία επιβάρυνση για το "οικιακό" τερματικό μια και θα το προσφέρουν δωρεάν οι εμπλεκόμενες

επιχειρήσεις αφού είναι σίγουρο ότι το οικονομικό όφελος για αυτές θα είναι τεράστιο αφού εκτός από την σημαντική μείωση του προσωπικού στα ταμεία που θα υπάρξει, στο συγκεκριμένο σύστημα δεν υπάρχει κανένα όριο στο είδος συναλλαγών. Κοινώς οποιαδήποτε συναλλαγή (η οποία θα έχει ένα συγκεκριμένο κωδικό-αριθμό) με οποιαδήποτε επιχείρηση θα είναι εφικτή 24 ώρες το 24ωρο με οποιοδήποτε καταναλωτή (ο οποίος επίσης θα έχει ένα μοναδιαίο κωδικό-αριθμό), και μάλιστα από τον ίδιο τον καταναλωτή.

Όλες οι παραπάνω εφαρμογές καθώς κι οι ήδη υπάρχουσες θα μπορούσαν να γίνονται από μία μόνο smart card αφού όπως είδαμε στην πτυχιακή αυτή, χάρη στον μικροεπεξεργαστή τους παρέχουν μεγάλη χωρητικότητα για αποθήκευση πληροφοριών αλλά και πάνω από όλα μέγιστη ασφάλεια. Η κάρτα δεν χρειάζεται να έχει όλα τα δεδομένα, όλων των εφαρμογών, αποθηκευμένα μέσα στην μνήμη της αλλά μόνο τις διευθύνσεις των server που συνδέονται με τις εφαρμογές αυτές. Έτσι ο χρήστης επιλέγοντας αυτή που θέλει, θα συνδέεται άμεσα με αυτή και η διαδικασία που θα ακολουθείται (κρυπτογράφηση, έλεγχος πρόσβασης, χρηματική χρέωση, χρέωση μονάδων ,χρονοχρέωση, πιστοποίηση χρήστη στον παγκόσμιο ιστό, on-line χρέωση στον παγκόσμιο ιστό, κτλ.), θα είναι ίδια με την ήδη υπάρχουσα. Επιπλέον με αυτή τη μέθοδο δεν αντιμετωπίζουμε κανένα πρόβλημα χωρητικότητας της μνήμης της smart cart. Η ανάγκη για κάτι τέτοιο προβάλει επιτακτική στις μέρες μας αφού από την μία οι καταναλωτές θέλουν προϊόντα πολύ-λειτουργικά αλλά και συνάμα απλά στην χρήση τους, κι από την άλλη οι επιχειρήσεις θέλουν να ικανοποιούν πρώτον, τους καταναλωτές και δεύτερον, τον χρυσό κανόνα της αγοράς ο οποίος αν και παλιός παραμένει ο No1 για την κερδοφορία των επιχειρήσεων: ***Ο χρόνος είναι χρήμα***, δηλαδή όσο πιο γρήγορα γίνονται οι συναλλαγές τόσο πιο πολλές θα γίνονται άρα και τόσο περισσότερα έσοδα θα έχουν.

Ως τα τέλη του 2005 όλοι οι τραπεζικοί οργανισμοί στην Ελλάδα που δραστηριοποιούνται στον χώρο εκκαθάρισης συναλλαγών πιστωτικών καρτών (acquiring) υποχρεούνται από τους οργανισμούς MasterCard και Visa σταδιακά να αναβαθμίσουν ή να αντικαταστήσουν τα ηλεκτρονικά POS παλαιότερης τεχνολογίας που διαθέτουν στις συμβεβλημένες επιχειρήσεις τους, ώστε να δέχονται συναλλαγές με κάρτες με μικροεπεξεργαστή. Για κάποιο διάστημα θα υπάρχει και μαγνητική ταινία σε αυτές για να μην αποκλειστούν επιχειρήσεις που δεν διαθέτουν τον

ανάλογο εξοπλισμό αλλά όπως επισήμανε κι ο κ$_{ος}$ Γ. Χαντζανδρέου (Διευθυντής Marketing της Εθνοκάρτας) η έκδοση και χρησιμοποίηση έξυπνων καρτών (με μικροεπεξεργαστή) αποτελεί πλέον

μονόδρομο για όλες τις επιχειρήσεις προκειμένου να ισχυροποιήσουν τη θέση τους εξασφαλίζοντας μέγιστη ασφάλεια, γρήγορη κι εύκολη διεκπεραίωση συναλλαγών αλλά και ανταγωνιστικά προνόμια για τους κατόχους τους.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Douglas R. Stinson, "Cryptography Theory and Practice", CRC Press, 1995

C.J.Date, "An Introduction to Database Systems", Addison-Wesley Publishing Company, Inc., 1995.

Daniel Mínolí & Emma Mínolí, "Web Commerce Technology Handbook", McGraw-Hill, 1997

GPM896 Technical Specifications Version 2.0, Gemplus, 1998

Jean Walrand, "Communication Networks", Richard D. Irwin, Inc. and Aksen Associates, Inc., 1991

"On lnternet Security", Netscape Communications Corporation, 2001

Ed Tittel, Mark Gaithel, Sebastian Hassinger & Mike Erwin, "Foundations of World Wide Web Programming with HTML & CGI", IDG Books World Wide, 1995

Raman Khana, "Integrating Personal Computers in a Distributed Client-Server Environment", Chap 19, Prentice Hall, 1995

Bruce Elbert & Bobby Martyna, "Client/Server Computing, Architecture, Applications, and Distributed Systems Management", Artech House, Inc. 1994

Andrew S. Athenaeum, "Modern Operating Systems", Prentice Hall, 1992

Internet Client Software Development Kit Documentation, Microsoft Corporation, 2000

Active Server Pages Documentation, Microsoft Corporation, 1997

Visual Basic 5.0 Documentation (Books on line), Microsoft Corporation, 2003

Γ.Χαντζανδρέου , Διευθυντής Marketing της Εθνοκάρτας, ‘‘Νέα γενιά

έξυπνων καρτών’’ , 2002

David Marsh, ’’Get SMART’’, EDN EUROPE, 2003

ΠΕΡΙΕΧΟΜΕΝΑ