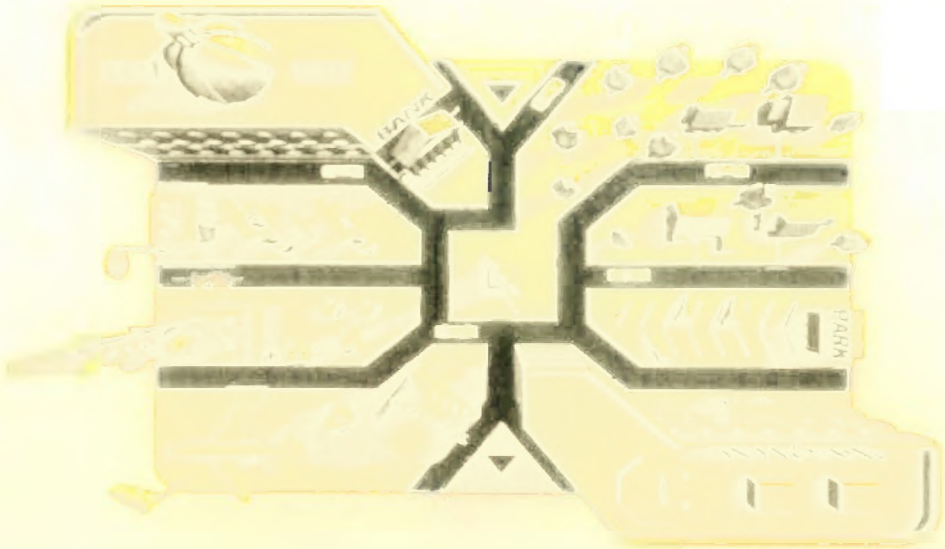
Τ.Ε.Ι. ΜΕΣΟΛΟΓΓΙΟΥ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΣΤΗ ΔΙΟΙΚΗΣΗ & ΟΙΚΟΝΟΜΙΑ

ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ

σε οικονομικά και κοινωνικά συστήματα



ΜΕΣΟΛΟΓΓΙ 2004

Πρόλογος

Η εργασία έχει εκπονηθεί, κατά βάση στο Τεχνολογικό Εκπαιδευτικό Ίδρυμα Μεσολόγγιου, με την χρήση των εγκαταστάσεων του υπολογιστικού κέντρου της Ε.Π.Δ.Ο.

Το σύνολο της εργασίας, είναι κυρίως μία συλλογή δεδομένων και πληροφοριών από το internet. Ο σκοπός αυτής της ενασχόλησης ήταν, το δυνατόν, η συλλογή, η επιλεκτική διαλογή και η επεξεργασία των δεδομένων, με σκοπό την πιο κατανοητή έκθεση γνώσης πάνω στην τεχνολογία των έξυπνων καρτών, μέχρι σήμερα, ώστε ο οποιοσδήποτε να είναι σε θέση να κατανοήσει κάποιες βασικές αρχές και έννοιες των έξυπνων καρτών.

Η αναζήτηση των στοιχείων έγινε από αρκετά μεγάλο αριθμό ιστοσελίδων, δημοσιεύσεων και αρκετών βιβλίων παρόλα αυτά στην εργασία χρησιμοποιήθηκαν πληροφορίες από πολύ λιγότερες ιστοσελίδες και άρθρα.

Ευχαριστίες θα πρέπει να δοθούν στον επιβλέποντα καθηγητή Δρ.Δρόσο Λάμπρο, ο οποίος έδειξε μεγάλο ενδιαφέρον για την πρόοδο και την βέλτιστη τελική μορφή της εργασίας. Επίσης θα πρέπει να δοθούν ιδιαίτερες ευχαριστίες στην κα. Αντωνία Στεφανή, η οποία με το ενδιαφέρον για την εργασία, βοήθησε σημαντικά στον εμπλουτισμό της και την ολοκληρωμένη παρουσίαση της. Βάζοντας τις τελευταίες πινελιές, δίνοντας ιδέες, υλικό και πολύ σημαντικές πληροφορίες για την άρτια ανάλυση, βοήθησαν και οι δύο ώστε η εργασία αυτή να παρουσιαστεί στην τελική της μορφή. Επίσης από τη διπλωματική αυτή εργασία πορέκυψαν αρκετά ερωτήματα και ανοιχτά προβλήματα τα οποία θα πρέπει να επιλυθούν. Αυτό όμως το αφήνουμε για μία μελλοντική ενασχόληση.

Περίληψη

Το περιεχόμενο της εργασίας χωρίζεται σε δύο μέρη. Στο Α' μέρος παρατίθονται κάποια γενικά στοιχεία καθώς και μία ιστορική αναδρομή. Στην συνέχεια ακολουθεί μία σύντομη περιγραφή των τύπων των έξυπνων καρτών και των αναγνωστών έξυπνων καρτών. Για την πλήρη κατανόηση της χρησιμότητας των έξυπνων καρτών, δίνονται κάποια παραδείγματα λειτουργιών, που είτε εφαρμόζονται είτε πρόκειται να εφαρμοστούν και στην χώρα μας.

Στην συνέχεια ακολουθεί μία περιγραφή της κατάστασης, τόσο στον ευρωπαϊκό, όσο και στον ελλαδικό χώρο. Το 4ο κεφάλαιο αναφέρεται αποκλείστηκα στην ασφάλεια των καρτών. Εδώ γίνεται μία ανάλυση των διαφόρων στρωμάτων επικοινωνίας (από το φυσικό, ως το ανώτερο) περιγράφοντας τις πιθανές απειλές και τις πολιτικές ασφάλειας. Σ' αυτό το κεφάλαιο επίσης αναφέρονται και κάποιες μέθοδοι κρυπτογράφησης δεδομένων, όσον αφορά τις έξυπνες κάρτες και την ηλεκτρονική επικοινωνία γενικότερα. Στο τέλος του Α' μέρους υπάρχουν κάποιες προτάσεις προς την πολιτεία, καθώς και κάποια συμπεράσματα, βασισμένα σε διάφορες μελέτες.

Το Β' μέρος, περιέχει την παρουσίαση του Gemplus Card Reader 680, το παράρτημα και τις πηγές στις οποίες βασίστηκε η εργασία.

Περιεχόμενα

ΜΕΡΟΣ Α

Κεφάλαιο 1ο

Κεφάλαιο 2ο

2. *ΈΞΥΠΝΕΣ ΚΑΡΤΕΣ*

Κεφάλαιο 3ο

Κεφάλαιο 4ο

Κεφάλαιο 5ο

ΜΕΡΟΣ Β

Κεφάλαιο 6ο

6. *ΠΑΡΟΥΣΙΑΣΗ ΤΟΥ GCR680*

Κεφάλαιο 7ο

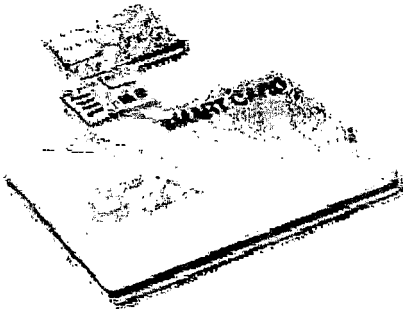
7. *ΠΑΡΑΡΤΗΜΑ*

Κεφάλαιο 8ο

1. Εισαγωγή

1.1. Γενικά

Αρκετοί από εμάς χρησιμοποιούμε ήδη μία ή περισσότερες έξυπνες κάρτες στην καθημερινή μας ζωή. Για παράδειγμα, έξυπνη κάρτα είναι η κάρτα SIM που χρησιμοποιείται στο σύστημα κινητής τηλεφωνίας GSM. Οι έξυπνες κάρτες είναι ουσιαστικά μμικροσκοπικοί υπολογιστές, που έχουν το μέγεθος και τη φόρμα μίας πιστωτικής κάρτας, πάνω στην οποία είναι ενσωματωμένο ένα ολοκληρωμένο κύκλωμα (chip), στην εμπρόσθια αριστερή πλευρά.



Το ολοκληρωμένο κύκλωμα περιέχει τις επαφές εισόδου-εξόδου και μπορεί να περιέχει μόνο μνήμη ή και μικροεπεξεργαστή. Μπορεί να παρέχει επίσης μία ασφαλή δομή πολλαπλών επιπέδων και να επιτρέπει ιεραρχημένη πρόσβαση, καθιστώντας δύσκολη την πρόσβαση στα στοιχεία και την παραποίηση αυτών, να υπολογίζει κρυπτογραφικές συναρτήσεις (cryptographic functions) και να αντιλαμβάνεται άμεσα προσπάθειες πρόσβασης, οι οποίες δεν είναι έγκυρες όπως για παράδειγμα το κλείδωμα της κάρτας SIM σε περίπτωση εισαγωγής λανθασμένου PIN περισσότερες από τρεις -συνήθως- φορές.

Το κύριο γνώρισμα των έξυπνων καρτών είναι η ικανότητα να αποθηκεύουν και να επεξεργάζονται πληροφορίες με ένα ασφαλή τρόπο. Τα πλεονεκτήματα των έξυπνων καρτών είναι η προστασία των δεδομένων που περιέχουν, η φορητότητα και η ευκολία χρήσης.

1.2. Ιστορία Έξυπνων Καρτών

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

Αργότερα, η εκτύπωση του ονόματος γινόταν σε ανάγλυφο (όπως για παράδειγμα σήμερα στις κάρτες ανάληψης χρημάτων από τα ATM των τραπεζών), ώστε να διευκολύνεται η αποτύπωση του ονόματος του κατόχου. Μερικά χρόνια αργότερα οι κάρτες αυτές απέκτησαν μία μαγνητική λωρίδα (magnetic stripe), η οποία επέτρεπε τη μηχανική αποτύπωση των στοιχείων του κατόχου.

Με τον τρόπο αυτό η επεξεργασία των στοιχείων μπορούσε να γίνει ηλεκτρονικά, επιταχύνοντας τις συναλλαγές. Παρέμενε όμως το πρόβλημα της απάτης, καθώς οποιοσδήποτε, έχοντας τον κατάλληλο εξοπλισμό, μπορούσε να δημιουργήσει πλαστές κάρτες.

Θα μπορούσαμε να πούμε ότι οι έξυπνες κάρτες είναι το αποτέλεσμα της ταυτόχρονης βελτίωσης των πλαστικών καρτών και των microchip. Το 1969 παρουσιάστηκε στη Γαλλία, από τον δημοσιογράφο Roland Moreno, μία ιδέα για μία κάρτα με ενσωματωμένο κύκλωμα. Έτσι γεννήθηκε η έξυπνη κάρτα. Οι έξυπνες κάρτες αναπτύχθηκαν ανεξάρτητα στη Γερμανία (1967), στην Ιαπωνία (1970) και στις Η.Π.Α. (1972). Οι έξυπνες κάρτες άνθισαν τη δεκαετία του 1980.

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

Μετά την πετυχημένη δοκιμή, οι Γαλλικές τράπεζες εισήγαγαν τη χρήση των έξυπνων καρτών για τραπεζικές λειτουργίες στο ευρύ κοινό. Η χρήση αυτή είναι το πρώτο παράδειγμα δημόσιας λειτουργίας των έξυπνων καρτών για τραπεζικές λειτουργίες. Παράλληλα, έγινε μία μεγάλη διαφημιστική εκστρατεία, οπότε και καθιερώθηκε ο όρος «έξυπνη κάρτα» (smart card).

Διεθνώς, κατά την τελευταία δεκαετία οι τεχνολογίες των Έξυπνων Καρτών χρησιμοποιούνται για την προσέγγιση και επίλυση προβλημάτων πρόσβασης, διαχείρισης και διακίνησης πληροφορίας σχεδόν σε όλους τους τομείς της οικονομίας και της κοινωνίας. Αυτό γίνεται εκτενώς στα πλαίσια ερευνητικών και πιλοτικών έργων και σε μικρότερη έκταση στα πλαίσια τομεακών έργων τοπικής ή εθνικής κλίμακας, π.χ. κάρτα υγείας, ταυτότητας,

ηλεκτρονικό πορτοφόλι, κάρτα πρόσβασης στις συγκοινωνίες κλπ. Είναι πλέον γενικώς αποδεκτό ότι οι τεχνολογίες των Έξυπνων Καρτών προσφέρουν πολλά επιχειρησιακά πλεονεκτήματα στη υλοποίηση σύγχρονων ηλεκτρονικών υπηρεσιών. Ο ρόλος τους κυρίως εστιάζεται στην διαμόρφωση και διασφάλιση περιβάλλοντος εμπιστοσύνης στις συναλλαγές μεταξύ πολιτών και παροχέων υπηρεσιών σε όλους τους τομείς της σύγχρονης οικονομίας.

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

1. Έλλειψη ενιαίας προσέγγισης, για την χρησιμότητα και λειτουργικότητα των Έξυπνων Καρτών, μεταξύ όλων των εμπλεκομένων μερών, τόσο στην λήψη αποφάσεων όσο και στην υλοποίηση εφαρμογών.
2. Έλλειψη ευρέως αποδεκτών προτύπων, σε όλα τα επίπεδα των τεχνολογιών των Έξυπνων Καρτών (κάρτες, αναγνώστες καρτών, λογισμικό, τυποποίηση πληροφοριών κλπ.) για την διασφάλιση της διαλειτουργικότητας (interoperability) μεταξύ συστημάτων σε τομεακό, διατομεακό και διακρατικό επίπεδο.
3. Το σχετικά υψηλότερο κόστος των έξυπνων καρτών σε σύγκριση με τις μαγνητικές κάρτες. Βέβαια η διαφορά αυτή στο κόστος μεταξύ των δύο τεχνολογιών μειώνεται σημαντικά αν λάβουμε υπόψη τη διαφορά στην αναμενόμενη διάρκεια ζωής της κάρτας, καθώς και την ικανότητα υποστήριξης πολλαπλών εφαρμογών.
4. Ο καταναλωτής πρέπει να είναι τεχνικά πεπειραμένος για να επιλέξει την πιό κατάλληλη κάρτα για την εφαρμογή στόχων.

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

Για την μελέτη των θεμάτων των trail-blazer συγκροτήθηκαν αντίστοιχες ομάδες εργασίας αποτελούμενες από εκπροσώπους κοινωνικών ομάδων και παροχέων υπηρεσιών, της βιομηχανίας και του ακαδημαϊκού και ερευνητικού χώρου.

Οι ομάδες εργασίας που ασχολούνται με τα θέματα των Public Identity, Identification & Authedication, Certification & Protection Profile και Multi-application Smart Cards έχουν αναπτύξει σημαντική δραστηριότητα και έχουν παράγει τα πρώτα αποτελέσματα προς δημόσια διαβούλευση. Η ελληνική συμμετοχή στις εν λόγω ομάδες εργασίας είναι πολύ περιορισμένη. Παράλληλα, στα πλαίσια του Γ'ΚΠΣ συζητούνται ή ανακοινώνονται σχέδια για διάφορες εφαρμογές Έξυπνων Καρτών, όπως: κάρτες υγείας, πρόνοιας, εκπαίδευσης, εργασίας - ασφάλισης, κάρτες χρηματιστηρίου, κάρτες εφορίας, κάρτες διοδίων κτλ. Η κατάσταση στη χώρα μας και η κινητικότητα που έχει δημιουργηθεί σε ευρωπαϊκό και διεθνές επίπεδο για θέματα ανάπτυξης εφαρμογών Έξυπνων Καρτών συνηγορούν στη συγκρότηση διεπιστημονικής ομάδας εργασίας για την αποτίμηση της ελληνικής κατάστασης λαμβάνοντας υπ' όψη ζητήματα που είτε έχουν προκύψει σε άλλες χώρες, ή δεν έχουν αντιμετωπιστεί ακόμη.

1.3. Πλεονεκτήματα Έξυπνων Καρτών

Τα βασικά πλεονεκτήματα της τεχνολογίας των έξυπνων καρτών είναι:

1. Ύπαρξη διεθνών προτύπων, που εξασφαλίζουν τη διάθεση των καρτών από πολλούς προμηθευτές και επομένως περισσότερο ανταγωνιστικές τιμές.
2. Μεγάλη διάρκεια ζωής (οι προμηθευτές εγγυώνται μέχρι 10.000 αναγνώσεις/ εγγραφές της ίδιας κάρτας).
3. Λειτουργικά συστήματα που υποστηρίζουν τις πολλαπλές εφαρμογές και εξασφαλίζουν την ανεξάρτητη αποθήκευση δεδομένων στην ίδια κάρτα.

Ειδικότερα, όσον αφορά την λειτουργικότητα των καρτών:

- Η ικανότητα επεξεργασίας, όχι μόνο αποθήκευσης πληροφορίας.
- Η δυνατότητα επικοινωνίας με άλλα υπολογιστικά συστήματα μέσων ενός smart card reader.
- Η δυνατότητα ενημέρωσης- ανανέωσης των πληροφοριών και εφαρμογών που βρίσκονται αποθηκευμένες στην κάρτα, χωρίς να είναι απαραίτητη η έκδοση νέας κάρτας. Και συνεπώς, η ακρίβεια παροχής πληροφοριών.
- Χαμηλό κόστος ανάπτυξης και χρήσης.

Σε θέματα σφάλειας:

- Η δυνατότητα ασφαλούς, off-line επεξεργασίας, λόγω της ύπαρξης των μικροεπεξεργαστών και των δεδομένων πάνω στην κάρτα.
- Η δυνατότητα προστασίας ανάγνωσης ή εγγραφής των πληροφοριών της κάρτας με χρήση ενός κωδικού PIN
- Η δυνατότητα πραγματοποίησης κρυπτογράφησης

2. Έξυπνες κάρτες

2.1 Είδη και Κατηγορίες Έξυπνων Καρτών

Μια έξυπνη κάρτα είναι δομή μεγέθους αντίστοιχου της πιστωτικής κάρτας, φτιαγμένη από πλαστικό, η οποία διαθέτει μικροεπεξεργαστή (embedded microprocessor chip) και χρησιμοποιείται για την αποθήκευση οικονομικών δεδομένων και προσωπικών πληροφοριών[1]

Στις μέρες μας, οι έξυπνες κάρτες μπορούν να κατηγοριοποιηθούν με δύο βασικά κριτήρια: επεξεργαστική ικανότητα και δυνατότητες εισόδου-εξόδου. Με βάση το πρώτο κριτήριο, διακρίνουμε τρία είδη έξυπνων καρτών:

1. *Κάρτες μνήμης* – κάρτες αποθήκευσης πληροφοριών (memory cards). Οι κάρτες αυτές περιέχουν κάποια μνήμη και λογική σε υλικό (hardware logic), η οποία μπορεί να θέσει ή να διαγράψει τιμές στη μνήμη. Οι κάρτες μνήμης αναφέρονται καταχρηστικά ως έξυπνες κάρτες, καθώς δεν έχουν δυνατότητα επεξεργασίας των δεδομένων.

2. *Έξυπνες κάρτες* (smart cards, IC cards, microprocessor cards). Είναι οι «κλασικές» έξυπνες κάρτες ή κάρτες με μικροεπεξεργαστή. Ο επεξεργαστής τους, πέρα από την αποθήκευση και ασφάλιση πληροφοριών, μπορεί να λαμβάνει αποφάσεις που ορίζονται στις προδιαγραφές του έργου για το οποίο θα χρησιμοποιηθούν.

3. *Έξυπνες κάρτες πολλαπλών εφαρμογών* (multi-application smart cards). Οι έξυπνες κάρτες τελευταίας γενιάς έρχονται με ανοικτά λειτουργικά συστήματα (Java, MULTOS) και μπορούν να εκτελούν περισσότερες από μία εφαρμογές. Παρέχεται επίσης η δυνατότητα στο χρήστη να «φορτώνει» νέες εφαρμογές, ή να διαγράφει άλλες ανάλογα με τις ανάγκες του.

---

[1] Πηγή: Bidgoli Hossein, "*Electronic Commerce, Principles and Practice*", Academic Press, USA, 2002

Οι κάρτες με μικροεπεξεργαστή, εκτός από CPU, διαθέτουν μνήμη ROM για την αποθήκευση του λειτουργικού συστήματος της κάρτας, μνήμη RAM για γρήγορη εκτέλεση υπολογισμών και μνήμη EEPROM για την αποθήκευση εφαρμογών και δεδομένων. Πρόκειται ουσιαστικά για ολοκληρωμένους μικροσκοπικούς Η/Υ, οι οποίοι στερούνται μόνο συσκευών εισόδου/εξόδου. Έτσι προκειμένου να επικοινωνήσουμε με τους υπολογιστές αυτούς χρησιμοποιούμε τις **συσκευές αποδοχής έξυπνων καρτών (card readers).**

Μία δεύτερη κατηγοριοποίηση αφορά τον τρόπο επικοινωνίας των έξυπνων καρτών με το εξωτερικό περιβάλλον. Με βάση αυτό το κριτήριο, διακρίνουμε τις εξής κατηγορίες:

1. ***Έξυπνες κάρτες με επαφές*** (Contact Cards). Οι κάρτες αυτές επικοινωνούν με ηλεκτρικές επαφές και πρέπει να εισαχθούν σε μία συσκευή ανάγνωσης προκειμένου να διαβαστούν ή να εισαχθούν πληροφορίες.

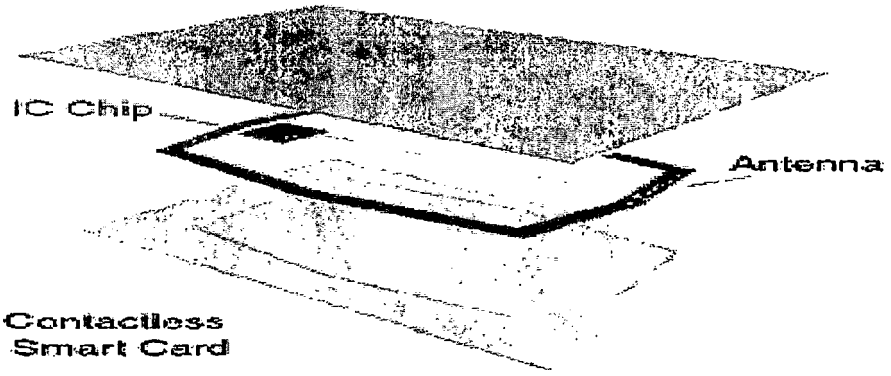
Οι έξυπνες κάρτες επαφών έχουν το μέγεθος μίας συμβατικής πιστωτικής κάρτας με ένα ενιαίο ενσωματωμένο chip κυκλωμάτων που περιέχει είτε μία μνήμη είτε μία μνήμη και ένα μικροεπεξεργαστή.

Τα chip που περιέχουν μόνο μία μνήμη, είναι λειτουργικά παρόμοια με μικρό πλαδαρό δίσκο. Είναι συνήθως, λιγότερο ακριβοί από τα chip μικροεπεξεργαστών, αλλά προσφέρουν επίσης και μικρότερη ασφάλεια, έτσι δεν πρέπει να χρησιμοποιηθούν για να καταχωρίσουν τις ευαίσθητες ή πολύτιμες πληροφορίες.

Τα chip που περιέχουν μία μνήμη και έναν μικροεπεξεργαστή, είναι επίσης παρόμοια με ένα μικρό πλαδαρό δίσκο, εκτός εάν περιέχουν έναν «ευφυή» ελεγκτή (controller) που χρησιμοποιείται για να προσθέσει με ασφάλεια, να διαγράψει, να ενημερώσει τις πληροφορίες που βρίσκονται στη μνήμη. Τα πολυπλοκότερα chip μικροεπεξεργαστών, χτίζουν τα χαρακτηριστικά γνωρίσματα ασφαλείας κατάστασης προόδου (state-of-the-art) ώστε να προστατέψουν το περιεχόμενο της μνήμης από αναρμόδια πρόσβαση.

Οι έξυπνες κάρτες επαφών πρέπει να παρεμβληθούν σε μία συσκευή, αποδέκτη καρτών, όπου τα pins που συνδέονται με τον αναγνώστη, κάνουν «την επαφή» με τα pads στην επιφάνεια της κάρτας, για να διαβάσουν και να αποθηκεύσουν πληροφορίες στο chip. Αυτός ο τύπος κάρτας, χρησιμοποιείται σε μία ευρεία ποικιλία εφαρμογών, συμπεριλαμβανομένης της ασφάλειας δικτύων, της πώλησης, των ηλεκτρονικών μετρητών (electronic cash), κυβερνητικών ή πανεπιστημιακών IDs, του ηλεκτρονικού εμπορίου, των καρτών υγείας και πολλών άλλων εφαρμογών.

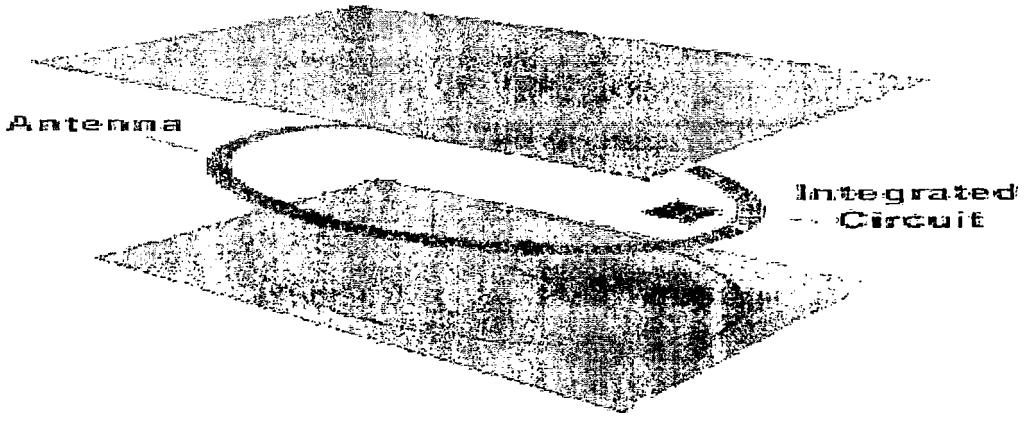
2. *Ασύρματες έξυπνες κάρτες* (Contactless Cards). Οι κάρτες αυτές έχουν ενσωματωμένη εσωτερικά μία μικροσκοπική κεραία και μπορούν να επικοινωνούν με μία κεραία λήψης χωρίς τη φυσική τους επαφή με κάποια συσκευή ανάγνωσης προκειμένου οι πληροφορίες να ανανεωθούν, να αλλάξουν ή να υποβληθούν σε επεξεργασία.



Εκτός από τα χαρακτηριστικά γνωρίσματα και τις λειτουργίες που βρίσκονται στις έξυπνες κάρτες, οι ασύρματες έξυπνες κάρτες περιέχουν μία ενσωματωμένη κεραία αντί των pads επαφών που συνδέονται με το chip για τις πλατφόρμες ανάγνωσης και γραψίματος, που περιλαμβάνονται στη μνήμη του chip. Οι ανέπαφες κάρτες δεν είναι απαραίτητο να παρεμβληθούν σε μία συσκευή αποδέκτη καρτών. Άντ' αυτού, χρειάζεται μόνο να περάσουν από το πεδίο αποδέκτη ραδιοσυχνότητας, για να διαβάσουν και να καταχωρίσουν τις πληροφορίες στο chip. Η αναλογία της λειτουργίας είναι χαρακτηριστικά από περίπου 2,5'' σε 3,9'' (63,5mm 99.06mm) ανάλογα με τον αποδέκτη.

Οι ασύρματες κάρτες χρησιμοποιούνται σε πολλές από τις ίδιες εφαρμογές με αυτές των έξυπνων καρτών επαφής, ειδικά όπου η προστιθέμενη ευκολία και ταχύτητα όταν η κάρτα δεν χρειάζεται να παρεμβληθεί σε κάποια συσκευή, είναι επιθυμητή. Υπάρχει μια αυξανόμενη αποδοχή αυτού του τύπου κάρτας τόσο για τις φυσικές όσο και για τις λογικές εφαρμογές ελέγχου πρόσβασης. Ο προσδιορισμός σπουδαστών, το ηλεκτρονικό διαβατήριο, η πώληση, ο χώρος στάθμευσης και οι φόροι είναι κοινές εφαρμογές για τις ανέπαφες κάρτες.

Proximity Cards

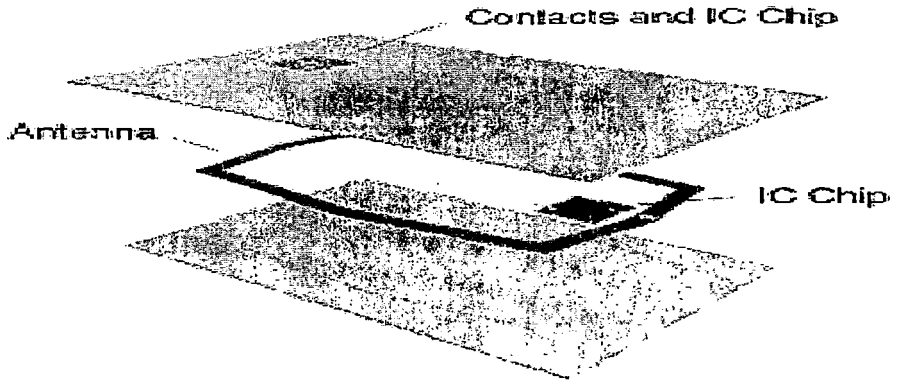


Οι κάρτες εγγύτητας ή απλά "prox cards" επικοινωνούν μέσω μιας κεραίας παρόμοιας με τις ανέπαφες έξυπνες κάρτες εκτός από το ότι είναι read-only συσκευές, οι οποίες έχουν γενικά ένα πολύ μεγαλύτερο εύρος λειτουργιών. Η αναλογία της λειτουργίας για τις κάρτες prox είναι χαρακτηριστικά από 2,5 "σε 20" (63,5mm 508mm) ανάλογα με τον αναγνώστη. Είναι πιθανό να διαβαστεί ένα μικρό ποσό πληροφοριών με τις συγκεκριμένες κάρτες, όπως ένας κώδικας προσδιορισμού, που ελέγχεται συνήθως από έναν απομακρυσμένο υπολογιστή, εντούτοις, είναι απίθανο να γραφτούν οι πληροφορίες πίσω στην κάρτα. Οι Prox cards είναι διαθέσιμες από διάφορες πηγές, κατά το ISO το πάχος της κάρτας κυμαίνεται από 0,027" μέχρι 0,033" (0,6858mm εώς 0,8382mm).

Οι κάρτες Prox συνεχίζουν να αυξάνονται σε δημοτικότητα λόγω της ευκολίας που προσφέρουν στην ασφάλεια, τον προσδιορισμό, και τις εφαρμογές ελέγχου πρόσβασης, ειδικά πρόσβαση πορτών όπου προτιμάται η γρήγορη, με ελεύθερα χέρια λειτουργία.

4. Υβριδικές κάρτες και συνδυασμένες κάρτες (Hybrid και Combination Cards). Οι κάρτες αυτές ενσωματώνουν και τους δύο τρόπους μετάδοσης και συνεπώς μπορούν να επικοινωνήσουν κατά περίπτωση είτε με ενσύρματο είτε με ασύρματο τρόπο. **Συσκευές αποδοχής έξυπνων καρτών (card readers)**

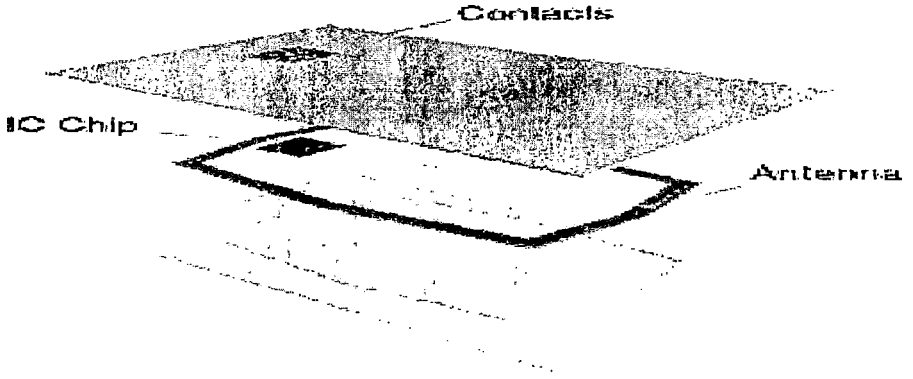
Hybrid Cards



Η υβριδική κάρτα είναι ο όρος που δίνεται στις e-cards που περιέχουν δύο ή περισσότερες ενσωματωμένες τεχνολογίες chip, όπως ένα ανέπαφο έξυπνο chip με την κεραία της, ένα έξυπνο chip επαφών με τα pads επαφών της, ή/ και ένα chip εγγύτητας με την κεραία της -- όλα σε μια ενιαία κάρτα. Το ανέπαφο chip χρησιμοποιείται χαρακτηριστικά για τις εφαρμογές που απαιτούν τους γρήγορους χρόνους συναλλαγής, όπως τη μαζική διέλευση (mass transit). Το chip επαφών μπορεί να χρησιμοποιηθεί στις εφαρμογές που απαιτούν τα υψηλότερα επίπεδα ασφάλειας. Τα μεμονωμένα ηλεκτρονικά συστατικά δεν συνδέονται το ένα με το άλλο ακόμα κι αν μοιράζονται το διάστημα σε μια ενιαία κάρτα.

Οι υβριδικές κάρτες προσφέρουν μια μοναδική λύση για την ενημέρωση του υπάρχοντος badging συστήματος. Αυτή η e-card επιτρέπει την προσαρμογή της υποδομής και της τεχνολογίας καρτών ενός legacy συστήματος, ενώ προσθέτει νέες εφαρμογές και τεχνολογίες e-cards -- όλες σε μια ενιαία κάρτα ταυτότητας.

Combo Cards



Η κάρτα combo -- που είναι γνωστή επίσης ως dual-interface card -- ενσωματώνει το ένα έξυπνο chip στην κάρτα που μπορεί να προσεγγιστεί μέσω είτε των pads επαφών είτε μιας ενσωματωμένης κεραίας. Αυτή η μορφή της έξυπνης κάρτας αυξάνεται στη δημοτικότητα επειδή παρέχει την ease-of-use και υψηλή ασφάλεια σε ένα ενιαίο προϊόν καρτών.

Η μαζική διέλευση (Mass transit) αναμένεται να είναι μια από τις δημοφιλέστερες εφαρμογές για την κάρτα combo. Σε μία εφαρμογή μαζικής διέλευσης, ένας αποδέκτης μπορεί να χρησιμοποιηθεί για να τοποθετήσει μια αξία μετρητών στη μνήμη του chip και η ασύρματη διαπροσωπεία μπορεί να χρησιμοποιηθεί για να αφαιρέσει μια τιμή από την κάρτα.

2.2 Συσκευές επικοινωνίας Έξυπνων Καρτών

Όπως προαναφέρθηκε, προκειμένου να επικοινωνήσουμε με τις έξυπνες κάρτες είναι απαραίτητες οι συσκευές αποδοχής έξυπνων καρτών. Οι συσκευές αυτές χωρίζονται σε δύο βασικές κατηγορίες:

1. **Τερματικές συσκευές**, οι οποίες διαθέτουν όλες τις απαραίτητες συσκευές για την επικοινωνία με την κάρτα π.χ. πληκτρολόγιο, εκτυπωτή, οθόνη, modem, κ.τ.λ. (EFT/POS, κινητά τηλέφωνα, καρτοτηλέφωνα, αυτόματοι πωλητές και αποκωδικοποιητές).

2. **Αναγνώστες - εγγραφείς έξυπνων καρτών**. Στις συσκευές που δε φέρουν κατάλληλο εξοπλισμό για την ανάγνωση έξυπνων καρτών (Η/Υ, info kiosks, controllers κ.α.), συνδέονται εξωτερικοί αναγνώστες, επιλύοντας ετσι το πρόβλημα ανάγνωσης.

Μία βασική υποομάδα αναγνωστών είναι οι ασφαλείς αναγνώστες, οι οποίοι διαθέτουν οθόνη LCD και PIN pad. Άλλες υποομάδες είναι οι αναγνώστες χωρίς καλώδιο, αναγνώστες χωρίς επαφές, οι επιτραπέζιοι, οι ενσωματωμένοι σε άλλες συσκευές (πληκτρολόγιο, CPU) κ.α.

2.3 Πρότυπα και κατευθύνσεις για έξυπνες κάρτες

2.3.1 Διεθνής Οργανισμός Προτύπων – ISO

Τα παγκόσμια πρότυπα διαμορφώνονται από έναν οργανισμό ο οποίος είναι γνωστός ως ISO (International Standards Organisation-Διεθνής Οργανισμός Προτύπων), ο οποίος εδρεύει στη Γενεύη. Ο οργανισμός IEC (International Electrotechnical Commission) ενδιαφέρεται για πρότυπα στο χώρο της ηλεκτρονικής. Σε πολλές περιπτώσεις τα πρότυπα των δύο οργανισμών έχουν συνδυαστεί και αναφέρονται ως ISO/IEC πρότυπα.

Ο ISO/IEC έχει ορίσει την επιτροπή JTC1 (Joint Technical Committee), η οποία παρακολουθεί τα πρότυπα των υπολογιστών. Τμήμα της JTC1 αποτελεί ο SC17, ο οποίος ασχολείται με «κάρτες ταυτότητας». Ο SC17 αποτελείται από 6 ομάδες εργασίας (WG). Η ομάδα WG4 ασχολείται με τα πρότυπα των καρτών με ολοκληρωμένο κύκλωμα και επαφές (Contact Integrated Circuit) ενώ η ομάδα WG8 ασχολείται με τα πρότυπα των ασύρματων έξυπνων καρτών (Contactless Integrated Circuit).

2.3.2 Ευρωπαϊκός Οργανισμός Προτύπων – CEN

Η προτυποποίηση των καρτών καθοδηγείται από την Τεχνική Επιτροπή (Technical Committee 224 – TC224) του Ευρωπαϊκού Οργανισμού Προτύπων και μερικές από τις ομάδες ασχολούνται με τα παρακάτω:

- WG1 – Φυσικά Χαρακτηριστικά Καρτών
- WG5 – Αποδέκτης να αποκτά μηνύματα πληρωμών
- WG6 – Επιφάνεια μηχανής
- ERWG8 – Λεπτές και ευέλικτες κάρτες
- WG9 – Εφαρμογές στον τομέα τηλεπικοινωνιών
- WG10 – Ηλεκτρονικό πορτοφόλι σε διαφόρους τομείς

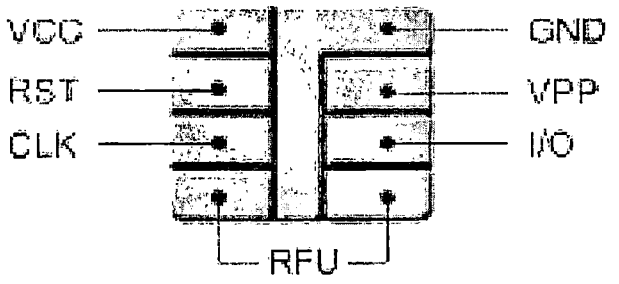
- WG11 – Εφαρμογές στον τομέα των συγκοινωνιών

- WG12 – Εφαρμογές στον τομέα της υγείας

Ο Ευρωπαϊκός Οργανισμός Προτύπων δημοσιεύει τα πρότυπα με το πρόθεμα EN. Πρότυπα που βρίσκονται σε δοκιμαστικό στάδιο, το οποίο μπορεί να διαρκέσει κατά το ανώτατο όριο 3 έτη και χρησιμοποιούνται σε τομείς όπου η τεχνολογία εξελίσσεται ραγδαία φέρουν το πρόθεμα ENV. Όλα τα μέλη της CEN πρέπει να δημοσιεύουν EN πρότυπα σαν δικά τους και να προωθούν αυτά τα πρότυπα ως ISO

2.3.3.Δυο χρήσιμα πρότυπα είναι το EN 726 και το EN1546. Γενικά

Το ολοκληρωμένο κύκλωμα μίας έξυπνης κάρτας χρησιμοποιεί μεταλλικές επαφές, οι οποίες έχουν οριστεί με βάση διεθνή πρότυπα:



- VCC – Power Supply Voltage

- RST – Reset the Microprocessor

- CLK – Clock Signal

- GND – Ground
- VPP – Programming or Write Voltage
- I/O – Serial Input/Output Line
- RFU – Future Use

Από τα παραπάνω μόνο το I/O και το Ground είναι απαραίτητα για την κάρτα και πρέπει να ακολουθούν τα διεθνή πρότυπα, όλα τα υπόλοιπα είναι προαιρετικά.

2.3.4. *Πρότυπα καρτών με επαφές – Contact Card Standards (ISO/IEC 7816)*

ISO/IEC 7816-1:1998 Physical Characteristics of IC cards, physical dimensions

o Βελτίωση 1 (1998): Επανεξέταση έκδοσης Μάρτιος 1998

Καθορίζει τις φυσικές διαστάσεις της κάρτας (πλάτος, μήκος και πάχος), τα οποία είναι ίδια με αυτά μιας κανονικής πιστωτικής κάρτας. Επιπρόσθετα χαρακτηριστικά αναφέρονται στο ISO/IEC 7816 -1 και αυτά αναφέρονται σε ακτίνες X, σημεία επαφής της επιφάνειας, μηχανική ισχύς, ηλεκτρομαγνητικά χαρακτηριστικά και στατικό ηλεκτρισμό

- ISO/IEC 7816-2:1999 Position of Module and Contacts on IC cards

Ορίζει τις διαστάσεις και την περιοχή στην οποία τοποθετούνται οι επαφές

- ISO/IEC 7816-3:1997 Electrical specifications and communication protocols

o Βελτίωση 1 (1992): Πρωτόκολλο T = 1
o Βελτίωση 2 (1994): Επανεξέταση της επιλογής τύπου πρωτοκόλλου
o Βελτίωση 3 (1998): Εισαγωγή 3 Volts ICCs

Ελέγχει τα χαρακτηριστικά των ηλεκτρικών σημάτων και τα πρωτοκόλλων μεταφοράς καθώς και την τυποποίηση της κάρτας «Απάντηση Επαναφοράς»

- ISO/IEC 7816-4:1995 Command set for microprocessor cards

o Βελτίωση 1 (1998): Επανεξέταση Ασφαλούς Αποστολής

Μηνυμάτων (Secure Messaging)

Ελέγχει:

- ✓ τις εντολές μεταξύ διαφορετικών βιομηχανιών,
- ✓ τις προδιαγραφές του APDU,
- ✓ τα ιστορικά χαρακτηριστικά «Answer to Reset»,
- ✓ τις δομές αρχείων,
- ✓ τις μεθόδους πρόσβασης,
- ✓ και την ασφαλή αποστολή μηνυμάτων

- ISO/IEC 7816-5:1994 Application identification

Καταχωρητικό σύστημα το οποίο κατέχει στοιχεία για αναγνώριση
εφαρμογών και επιτρέπει στα διάφορα τερματικά να διαλέξουν αναμφίβολα μια εφαρμογή από την κάρτα

- ISO/IEC 7816-6:1996 Inter-industry data elements

Ορίζει τα στοιχεία δεδομένων που προορίζονται για ανταλλαγή

- ISO/IEC 7816-7:1999 Inter-industry commands for Structured Card Query Language (SCQL)

Ορίζει την SCQL και τις εντολές οι οποίες επιτρέπουν την διαχείριση σχεσιακών βάσεων δεδομένων στην έξυπνη κάρτα

- ISO/IEC DIS 7816-8 Security related inter-industry commands

Ορίζει θέματα ασφάλειας για εντολές που χρησιμοποιούνται μεταξύ βιομηχανιών

• ISO/IEC DIS 7816-9 Additional inter-industry commands and security attributes

Ορίζει επιπρόσθετα θέματα ασφάλειας για εντολές και χαρακτηριστικά που χρησιμοποιούνται μεταξύ βιομηχανιών

• ISO/IEC DIS 7816-10 Electronic signals and answer to reset for synchronous cards

Ορίζει τα ηλεκτρονικά σήματα και την «απάντηση επαναφοράς» για έξυπνες κάρτες που χρησιμοποιούν σύγχρονο τρόπο μετάδοσης δεδομένων.

2.3.5. *Πρότυπα καρτών χωρίς επαφές – Contactless card standards*

Οι κάρτες χωρίς επαφές αναγνωρίζονται από τον οργανισμό ISO (SC17-WG18) ως «κάρτες ταυτότητες». Τα φυσικά χαρακτηριστικά τους είναι σε συμφωνία με ISO 7810 και ISO 7813. Η μόνη τους διαφορά είναι το πάχος της κάρτας μιας και στο παρελθόν η κάρτα χωρίς επαφή ήταν πιο παχιά.

Υπάρχουν 3 τύποι καρτών χωρίς επαφές που αναγνωρίζονται από τον οργανισμό ISO και άλλους σχετικούς οργανισμούς. Υπάρχουν 3 διαφορετικές ομάδες που ασχολούνται με αυτές τις κάρτες

Πρώτη Ομάδα (Task Force 1)

Η ομάδα αυτή ασχολείται με τις κάρτες αυστηρής εγγύτητας (Close Proximity Cards), οι οποίες χρειάζονται να είναι κοντά στον αναγνώστη της κάρτας για λειτουργήσουν σωστά.

• IS 10536 –1 Physical Characteristics

Ελέγχει τα φυσικά χαρακτηριστικά της κάρτας αλλά περιλαμβάνει και άλλα στοιχεία όπως κατατομή της επιφάνειας, ηλεκτρομαγνητικές δυνατότητες, και θερμοκρασία λειτουργίας

• IS 10536 – 2 Dimensions and locations of coupling areas

Θέτει διαφορετικές δυνατότητες

• DIS 10536 - 3 Electronic Signal and mode switching

Βρίσκεται ακόμα στα αρχικά στάδια και περιλαμβάνει πληροφορίες για ηλεκτρονικά σήματα και διαδικασίες επαναφοράς των καρτών στις αρχικές τους συνθήκες

• CD 10536 - 4

Βρίσκεται ακόμα στα αρχικά στάδια και περιλαμβάνει πληροφορίες για πρωτόκολλα, ειδικά για την υλοποίηση full-duplex επικοινωνία

Δεύτερη Ομάδα (Task Force 2)

Η ομάδα αυτή ασχολείται με την κατηγορία "Remote Coupled" των αρτών χωρίς επαφές, και τα ενδιαφέροντα στοιχεία είναι επισήμανση/χειρισμός προβλημάτων όταν μια ή περισσότερες κάρτες υπάρχουν στον «αναγνώστη κάρτας»

• **CD 14443 - 1**

Βρίσκεται ακόμα στα αρχικά στάδια και περιλαμβάνει πληροφορίες για τα φυσικά χαρακτηριστικά

• **14443 - 2**

Βρίσκεται ακόμα στα αρχικά στάδια και θα περιγράφει radio frequency Interface

• **14443 - 3**

Βρίσκεται ακόμα στα αρχικά στάδια και θα περιγράφει πρωτόκολλα μεταφορών

• **14443 - 4**

Βρίσκεται ακόμα στα αρχικά στάδια και θα περιγράφει χαρακτηριστικά ασφαλούς μεταφοράς

Τρίτη Ομάδα (Task Force 3)

Η ομάδα αυτή ασχολείται με κάρτες χωρίς επαφή που λειτουργούν από απόσταση. Η ομάδα αυτή βρίσκεται ακόμα στα αρχικά στάδια και δεν υπάρχουν κάποια αποτελέσματα

2.3.6. *Δοκιμαστικά/Ελεγχος καρτών – Card Testing*

- ISO 10373

Αναφέρεται στις μεθόδους ελέγχου που χρησιμοποιούνται για τον έλεγχο των έξυπνων καρτών, όπως λύγισμα της κάρτας σε οριζόντιο και κάθετο άξονα, έλεγχος σε διαφορετικές θερμοκρασίες και υγρασία κ.τ.λ.

2.3.7. *Πρωτόκολλα Ανταλλαγής Μηνυμάτων – Message Exchange Protocols*

- ISO 8583 Financial transaction card originated messages – interchange message specification

Πρότυπα μηνυμάτων που προέρχονται από κάρτες οικονομικών συναλλαγών – προσδιορισμός και προδιαγραφές ανταλλαγής μηνυμάτων

- ISO 9992 Financial transaction cards - messages between the integrated circuit card and the card accepting device

Πρότυπα καρτών για οικονομικές συναλλαγές – μηνύματα μεταξύ ολοκληρωμένου κυκλώματος καρτών και του αναγνώστη της κάρτας

2.3.8. *Πρότυπα σχετικά με θέματα Ασφάλειας – Security Related Standards*

- ISO 9564 Banking – PIN management and security

Πρότυπα για τραπεζικές λειτουργίες, διαχείριση και ασφάλεια του προσωπικού κωδικού ασφαλείας

- ISO 9796 IT security techniques – digital signatures

Πρότυπα για τεχνικές ασφάλειας – ψηφιακές υπογραφές

- ISO 9797 IT security techniques – data integrity mechanism

Πρότυπα για τεχνικές ασφάλειας – μηχανισμός που ελέγχει την ακρίβεια των καταχωρημένων στοιχείων χρησιμοποιώντας μια κρυπτογραφική λειτουργία

- ISO 9798 IT security techniques – entity authentication

Πρότυπα για τεχνικές ασφάλειας – ταυτοποίηση οντότητας

- ISO 10202 Financial transaction cards – security architecture using IC Cards

Πρότυπα καρτών για οικονομικές συναλλαγές –

- ISO 11568 Banking - key management (retail)

Πρότυπα για τραπεζικές λειτουργίες – λιανική

2.4. Εφαρμογές

Οι έξυπνες κάρτες είναι πρακτικά ένας φορητός υπολογιστής με αυξημένα χαρακτηριστικά ασφάλειας σε φυσικό επίπεδο. Η συνεχής πρόοδος στην τεχνολογία ολοκλήρωσης παρέχει σήμερα χαρακτηριστικά επεξεργασίας στις έξυπνες κάρτες που ήταν διαθέσιμα στους πρώτους προσωπικούς υπολογιστές.

Στη συνέχεια παρουσιάζονται μερικά παραδείγματα όπου χρησιμοποιούνται οι έξυπνες κάρτες για να γίνει πιο κατανοητή η αξία και η χρησιμότητά τους και τα οποία σχηματικά έχουν ως εξής:

Γνωστές και πιθανές εφαρμογές έξυπνων καρτών κατά τομέα και τύπο κάρτας

	Stored Value Cards	Data/Information Files	Identification/ Access/Security	Membership Cards
Τραπεζικός τομέας	• Ηλεκτρονικό πορτοφόλι • Τραπεζικές συναλλαγές • Ηλεκτρονικές πληρωμές • Ασφαλιστική αίτηση		• Πρόσβαση με συγκεκριμένο λογαριασμό • Ασφάλεια χρησιμοποιών τας το internet από το σπίτι	• Πιστωτικές κάρτες • Χρεωστικές κάρτες
Τηλεπικοινωνίες	Προπληρωμένη τηλεκάρτα	Αποθήκευση αριθμού	Κάρτες SIM/GSM	
Δημόσιος Τομέας	• Διαχείρηση λογαριασμών (συντάξεις, επιδόματα κ.τ.λ.) • Προηγμένες ηλεκτρονικές υπογραφές σε ηλεκτρονικά έγγραφα		• Διαβατήριο • Ταυτότητα • Δίπλωμα οδήγησης	
Μεταφορές	• Ηλεκτρονικά εισιτήρια (temporary validity contacts – ημερήσια, μηνιαία ή ετήσια εισιτήρια) • Αυτόματη πληρωμή διοδίων		• Κάρτα επιβίβασης – πάσο δωρεάν επιβίβασης • Κάρτα δικαιώματος πρόσβασης	• Κάρτα τήρησης post payment contact

	• Πληρωμές μεταφορικών μέσων με ηλεκτρονικό πορτοφόλι (λεωφορείο, ταξί, τραίνο κ.τ.λ.)		οχήματος σε ζώνη ελεγχόμενης πρόσβασης	
Υγεία	• Πληρωμές ασφάλειας • Ιατρικές πληρωμές	• Αποθήκευση/ ανάκτηση ιατρικού ιστορικού • Αποθήκευση πληροφοριών δότη		• Κάρτες υγείας
Λοιπά	• Κρατήσεις ξενοδοχείων • Πληρωμές μισθοδοσίας προσωπικού • Πληρωμές μέσω τηλεόρασης • Χρηματική μεταφορά από άτομο σε άτομο • Πρόγραμμα διατηρησιμότητας και εξυπηρέτησης πελατών (π.χ. έπαθλα) • Μικροπληρωμές (π.χ. χώρους στάθμευσης, τηλεφωνήματα κ.τ.λ.)	• Πληροφορίες/ ιστορικό προσωπικού • Ακαδημαϊκές πληροφορίες/ ιστορικό • Αποθήκευση προσωπικής πληροφορίας • Αρχεία ενοικίασης αυτοκινήτων • Προσωπικό προφίλ (π.χ. προτιμήσεις για το πρόγραμμα εξυπηρέτησης πελατών)	• Γρήγορο check in/ out • Κλειδιά δωματίου σε ξενοδοχείο • Πρόσβαση στο διαδίκτυο • Πρόσβαση σε κτήρια • Πρόσβαση σε δίκτυα • Κλειδιά ενοικίασης αυτοκινήτου	Πρόγραμμα Frequent traveler • Κάρτα διατηρησιμότητας & εξυπηρέτησης πελατών (loyalty cards)

2.4.4. *Ηλεκτρονικό Πορτοφόλι*

Η έξυπνη κάρτα μπορεί να αποθηκεύσει νομισματικές μονάδες, διευκολύνοντας σημαντικά τις πληρωμές και αγορές. Παραδείγματα χρήσεων αποτελούν οι ελεγχόμενοι χώροι στάθμευσης, διόδια σε δρόμους, πληρωμή εισιτηρίου σε μέσα μαζικής μεταφοράς (μετρό, τρένο, λεωφορεία), αγορά αναψυκτικών από μηχανήματα που βρίσκονται σε δημόσιους χώρους (venting machines) και αυτόματη πληρωμή φωτοτυπιών σε δημόσιες βιβλιοθήκες αλλά και αγορές καταναλωτικών ειδών σε κάθε είδους κατάστημα.

Με αυτό τον τρόπο διευκολύνεται η άμεση είσπραξη του πληρωτέου ποσού καθώς επίσης και η εκκαθάριση μεταξύ καταστημάτων και τραπεζικών ιδρυμάτων. Επιτυχημένα παραδείγματα ηλεκτρονικού πορτοφολιού είναι η κάρτα Mondex1 και τα αντίστοιχα της Visa2.

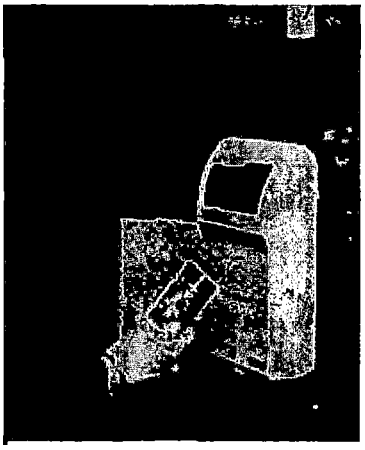
2.4.5. *Πιστωτικές Κάρτες*

Όταν οι πελάτες εισέρχονται σε ένα συμβατικό κατάστημα για να προμηθευτούν ένα προϊόν, ο πιο απλός τρόπος είναι να το πληρώσουν τοις μετρητοίς. Οι δικτυακοί πελάτες δεν έχουν αυτή τη δυνατότητα, γεννώντας έτσι την ανάγκη δημιουργίας μετάβασης των επιχειρήσεων σε ηλεκτρονικά μέσα πληρωμής. Οι πιο δημοφιλείς υπηρεσίες αναφέρονται στη χρήση πιστωτικών καρτών. Πρόκειται για ταχύτατες και ασφαλείς συναλλαγές, με τις οποίες ο χρήστης του Internet είναι εξοικειωμένος από τα πρώτα του βήματα στον κόσμο των δικτυακών αγορών.

Οι δικτυακές πληρωμές με πιστωτικές κάρτες λειτουργούν περίπου όπως και σε περιβάλλον λιανικής πώλησης. Για να γίνονται δεκτές δικτυακές πληρωμές μέσω πιστωτικών καρτών, θα πρέπει να προϋπάρχει συνεργασία με εταιρία εκτέλεσης δικτυακών πληρωμών (Cybercash, PaymentNet, κλπ)

2.4.6. *Χρήση Έξυπνων Καρτών στις Μεταφορές*

Οι Μεταφορές αποτελούν την εφαρμογή - κλειδί, γιατί έχουν πολυάριθμο και σταθερό κοινό. Οι εφαρμογές στον τομέα των Μεταφορών που μπορούν να προσφέρουν οι έξυπνες κάρτες είναι οι εξής:



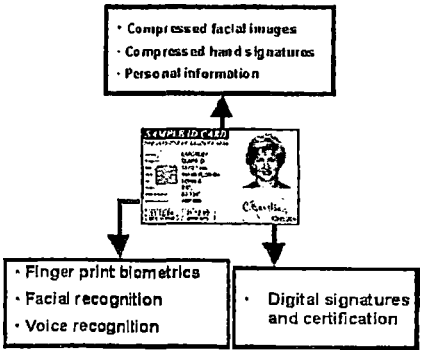
- Πληρωμή εισιτηρίου στις Δημόσιες Συγκοινωνίες
- Πληρωμή διοδίων
- Δικαιώματα parking
- Κρατήσεις αεροπορικών εισιτηρίων,
- Κρατήσεις σε ξενοδοχεία και μεταφορά των αποσκευών
- Τεκμηρίωση κατόχου, ηλεκτρονικό διαβατήριο.

Πηγή: ITS International.

Από τα παραπάνω, η πιο σημαντική εφαρμογή, είναι οι Δημόσιες Συγκοινωνίες, παρόλο που σε μερικά χρόνια μπορεί να θεωρείται εξίσου σημαντική και η εφαρμογή της πληρωμής Διοδίων. Επιπλέον η εφαρμογή για δικαιώματα parking μπορεί να συνδυαστεί αποτελεσματικά με την πληρωμή Διοδίων και /ή τις Δημόσιες Συγκοινωνίες. Ένας τέτοιος συνδυασμός μπορεί να επιτρέπει, οι πληρωμές για parking να πιστώνονται ακόμα και στην περίπτωση που κάποιος παρκάρει το αυτοκίνητό του και συνεχίζει το ταξίδι του με Δημόσια Συγκοινωνία.

Ακόμα η υπηρεσία Κράτησης αεροπορικών εισιτηρίων μπορεί να πραγματοποιηθεί από μία ξεχωριστή κάρτα ή να συμπεριληφθεί σε μία γενική Έξυπνη κάρτα των πολιτών.

2.4.7. Κάρτα Διατηρησιμότητας και Εξυπηρέτησης Πελατών (loyalty cards)



Οι επιχειρήσεις λιανικού εμπορίου έχουν τη δυνατότητα να χρησιμοποιούν τις έξυπνες κάρτες προκειμένου να εξυπηρετούν πιο αποτελεσματικά τους πελάτες τους και να τους κρατούν πιστούς. Για παράδειγμα μπορούν να πριμοδοτούν τους πελάτες τους με κάποιους πόντους σε κάθε τους αγορά και να τους επιβραβεύουν δίνοντας τους δώρα με την εξαργύρωση των πόντων αυτών όταν φτάσουν σε ένα ορισμένο επίπεδο πόντων.

Το γεγονός ότι οι πόντοι αποθηκεύονται στο chip προσφέρει δύο *βασικά πλεονεκτήματα*:

α. Δεν χρειάζεται να υπάρχει δίκτυο μεταξύ των καταστημάτων προκειμένου να ενημερώνεται μία κεντρική βάση με τους πόντους του πελάτη.
β. Ο πελάτης επιβραβεύεται άμεσα με την επίτευξη του ορίου πόντων, δίνοντάς του επιπλέον κίνητρο για αγορές.

Με τον τρόπο αυτό κρατούν πιστούς τους πελάτες τους ενώ ταυτόχρονα παίρνουν πληροφορίες για τις καταναλωτικές τους συνήθειες, στοιχεία πολύτιμα τόσο για την στρατηγική marketing και πωλήσεων όσο και για την αποτελεσματικότερη εξυπηρέτηση των πελατών τους.

2.4.8. Έλεγχος Πρόσβασης σε Κτίρια

Μία έξυπνη κάρτα μπορεί να αποθηκεύσει τα στοιχεία αναγνώρισης ενός ατόμου για τον έλεγχο πρόσβασης σε κτίρια υψηλής και μη ασφάλειας-χώρος εργασίας αλλά και σε πανεπιστήμια, σχολεία, βιβλιοθήκες και λέσχες.

Για ανάγκες υψηλότερης ασφάλειας και πρόσβαση σε συγκεκριμένες υπηρεσίες ή πληροφορίες, μια έξυπνη κάρτα μπορεί να αποτελέσει μια συσκευή για την αποθήκευση πληροφοριών όπως η εικόνα ή άλλα βιομετρικά χαρακτηριστικά (π.χ. τα δακτυλικά αποτυπώματα, ίριδα του ματιού) του χρήστη.

Η ίδια κάρτα μπορεί στη συνέχεια να διατηρεί στοιχεία για την ταυτοποίηση του ατόμου στα υπολογιστικά συστήματα του οργανισμού. Παράδειγμα αποτελεί η κάρτα Mcard, που χρησιμοποιείται από 110.000 μέλη του Πανεπιστημίου του Michigan και σε αυτή υπάρχουν πληροφορίες για την ταυτότητα του κάθε φοιτητή και μπορεί να χρησιμοποιηθεί για χρηματοοικονομικές συναλλαγές, για αγορά φαγητού, βιβλίων, για φωτοαντίγραφα και άλλες χρήσεις.

2.4.9. Πρόσβαση σε Ανοικτά ή Κλειστά Δίκτυα

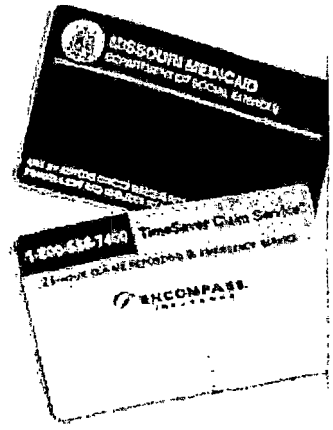
Οι έξυπνες κάρτες μπορούν να αποθηκεύσουν ψηφιακά πιστοποιητικά (digital certificates) και άλλες πληροφορίες για τον έλεγχο του δικαιώματος πρόσβασης του χρήστη, ώστε να μπορεί να χρησιμοποιεί υπολογιστικά και δικτυακά συστήματα με ασφαλή τρόπο.

Η ασφάλεια εδώ αναφέρεται τόσο στην πιστοποίηση της ταυτότητας του χρήστη, όσο και στη δημιουργία ιδιωτικών εικονικών δικτύων (VPN) για την πρόσβαση εταιρικών συστημάτων από δημόσια δίκτυα, όπως για παράδειγμα το Internet.Τραπεζικές συναλλαγές μεγάλοι τραπεζικοί οργανισμοί, όπως για παράδειγμα η Visa και η American Express θεωρούν ήδη τις έξυπνες κάρτες ως το επόμενο βήμα στις τραπεζικές συναλλαγές, καθώς προσφέρουν σημαντικά πλεονεκτήματα έναντι των καρτών με μαγνητική λωρίδα.

Για το λόγο αυτό έχει συσταθεί η εταιρεία EMVco (EUROPAY-MASTECARD-VISA co) η οποία επεξεργάζεται τις προδιαγραφές EMV τις οποίες θα πρέπει να ακολουθήσουν όλα τα εμπλεκόμενα μέρη (Τράπεζες, κατασκευαστές καρτών και εξοπλισμού, εταιρείες ανάπτυξης λογισμικού τερματικών συσκευών και back office συστημάτων κ.α.) προκειμένου να είναι δυνατή η επίτευξη EMV συναλλαγών. Η νεότερη έκδοση EMV προδιαγραφών είναι τα EMV2000. Οι EMV κάρτες θα αντικαταστήσουν τις πιστωτικές και χρεωστικές κάρτες μαγνητικής ταινίας, ενώ θα μπορούν να υποστηρίζουν και επιπλέον εφαρμογές π.χ. loyalty, ηλεκτρονικό πορτοφόλι κ.α.

Οι EMV κάρτες θα μπορούν να χρησιμοποιηθούν επίσης σε τραπεζικές συναλλαγές εξ αποστάσεως (internet banking, mobile banking), με χρήση ηλεκτρονικών πιστοποιητικών για την πιστοποίηση της ταυτότητας του χρήστη.

2.4.10. *Υγεία και Ασφάλιση*



Η έξυπνη κάρτα μπορεί να χρησιμοποιηθεί για την ασφαλή αποθήκευση στοιχείων ταυτότητας, ασφάλισης και ιατρικών δεδομένων ενός ατόμου ή για την αποθήκευση των σημείων όπου βρίσκονται στοιχεία ιατρικού φακέλου (pointer cards). Με τον τρόπο αυτό οι πληροφορίες είναι έγκαιρα και έγκυρα διαθέσιμες στους ασθενείς και ιατρούς υποστηρίζοντας και διευκολύνοντας σημαντικά την ελεύθερη διακίνηση των ασθενών που μπορούν να ταξιδεύουν στο εσωτερικό καιστο εξωτερικό φέροντας μαζί τους τον ασφαλιστικό και ιατρικό τους φάκελο. Πέραν αυτού, οι έξυπνες κάρτες στο τομέα της υγείας χρησιμοποιούνται σε εφαρμογές ταυτοποίησης του ασθενούς και επαγγελματιών υγείας (ιατρών, νοσηλευτών κλπ), ηλεκτρονικών υπογραφών για την ακεραιότητα και την αυθεντικότητα των ιατρικών δεδομένων, κρυπτογράφησης των δεδομένων για τη διασφάλιση της εμπιστευτικότητας (health professional cards), ασφαλή πρόσβαση σε δίκτυα υγείας κλπ.

2.4.11. *Προηγμένες Ηλεκτρονικές Υπογραφές σε Ηλεκτρονικά Έγγραφα*

Οι έξυπνες κάρτες, με τις δυνατότητες δημιουργίας ζεύγους κλειδιών, και ασφαλούς εναποθήκευσης ιδιωτικών κλειδιών και ηλεκτρονικών πιστοποιητικών που παρέχουν, αποτελούν αξιόπιστο τμήμα των "ασφαλών διατάξεων δημιουργίας υπογραφής" που απαιτεί η Ευρωπαϊκή Οδηγία 93 του 1999 "για τις ηλεκτρονικές υπογραφές" -και το αντίστοιχο ελληνικό Π.Δ. 150/2001-, ώστε οι κάτοχοί τους, που πιστοποιούν την

ταυτότητά τους με "αναγνωρισμένα πιστοποιητικά" (σύμφωνα με το Π.Δ.) από έναν κατάλληλο "Πάροχο Υπηρεσιών

Πιστοποίησης", να μπορούν να υπογράφουν ηλεκτρονικά έγγραφα με δικονομική αξία ίση με αυτήν της ιδιόχειρης υπογραφής τους στα έντυπα έγγραφα".

Κατά την εφαρμογή των παραπάνω εμπλέκονται τρεις (3) διακριτές οντότητες:

1. Πάροχος Υπηρεσιών Πιστοποίησης (Έμπιστη Τρίτη Οντότητα).

2. Τελική οντότητα (αποδέκτης της ηλεκτρονικής υπογραφής και του πιστοποιητικού, ή αλλιώς "βασιζόμενο μέρος") συνήθως παροχέας υπηρεσιών ασφαλούς δικτύου στους πελάτες του (π.χ. Τράπεζα).

3. Τελικός χρήστης-υπογράφων (π.χ. πελάτης Τράπεζας).

2.4.12. Ηλεκτρονικό Εμπόριο

Οι ηλεκτρονικές αγορές έχουν ως σκοπό τη διάθεση των εμπορικών πληροφοριών των εταιρειών-μελών τους σε άλλες εταιρίες ανεξάρτητα από το μέγεθός τους ή τη γεωγραφική τους θέση. Συγκεκριμένα:

- ✓ Αυξάνουν την ενημέρωση σχετικά με τις σύγχρονες τεχνολογίες πληροφορικής.
- ✓ Κάνουν δυνατή την αποτελεσματική χρήση των τεχνολογιών αυτών.
- ✓ Προωθούν τη χρήση της ηλεκτρονικής αγοράς, ώστε να μειώσουν το διαδικασιακό κόστος των εταιρειών που δραστηριοποιούνται στο διεθνές εμπόριο.

Τα έσοδα της ηλεκτρονικής αγοράς είναι οι συνδρομές των εταιρειών-μελών της οι οποίοι διατηρούν την ιστοσελίδα τους μέσα στον δικτυακό τόπο της αγοράς και τα προϊόντα τους προωθούνται μέσω ενός συστήματος BBS (Bulletin Board System).

Οι ηλεκτρονικές αγορές επιτρέπουν στα μέλη τους να δημιουργήσουν την ιστοσελίδα τους η οποία φιλοξενείται στο δικτυακό τόπο της αγοράς, και να συνδέσουν τις λεπτομέρειες των προϊόντων τους μαζί με αντίστοιχες φωτογραφίες στο εμπορικό BBS της αγοράς, παρέχοντας με τον τρόπο αυτό ολοκληρωμένη παρουσία στα προϊόντα ή τις υπηρεσίες τους.

Η χρηστικότητα του BBS έγκειται στο ότι προσομοιώνει τις κλασικές διαδικασίες των επιχειρήσεων εισαγωγών/εξαγωγών και λειτουργεί

παρόμοια με ένα παραδοσιακό εμπορικό περιοδικό ή κατάλογο (περιέχει διαφημίσεις, προϊόντα, περιγραφές, κλπ).

Η ιστοσελίδα κάθε επιχείρησης που φιλοξενείται στην ηλεκτρονική αγορά είναι σχετικά απλή και λειτουργεί κυρίως ως ένας κατάλογος προϊόντων.

2.4.13. *GSM Κάρτες και Τηλεκάρτες*

Οι έξυπνες κάρτες βρήκαν εφαρμογή σε πολλούς τομείς της καθημερινής μας ζωής. Δύο από τις πιο επιτυχημένες εφαρμογές τους είναι στον τομέα τηλεπικοινωνιών και μάλιστα στην πιο απλή τους (προπληρωμένη τηλεκάρτα) και στην πιο σύνθετη μορφή τους (GSM κάρτες).

Αυτή τη στιγμή κυκλοφορούν παγκοσμίως πολλά δισεκατομμύρια τηλεκάρτες και εκατοντάδες εκατομμύρια SIM κάρτες αφού τα GSM τηλέφωνα υπολογίζονται σε 500.000.000.

2.4.14 *Internet Security*

Οι φόβοι των γονέων, σχετικά με την ασφάλεια του Διαδικτύου, για την πρόσβαση των παιδιών τους στις ακατάλληλες περιοχές Ιστού ή για τα καλωδιακά κανάλια, μπορούν να εξεταστούν μέσω των έξυπνων καρτών που σχεδιάζονται για Διαδίκτυο και των καλωδιακών καναλιών.

Όπου το Διαδίκτυο προσεγγίζεται μέσω ενός Intrnet TV Box, η έξυπνη κάρτα παρέχει ένα πλήκτρο για τον γονικό έλεγχο από την αφαίρεση ορισμένων λειτουργιών - όπως η περιοδεία Ιστού ή το ηλεκτρονικό ταχυδρομείο - που μπορούν να θεωρηθούν ακατάλληλα. Μια εναλλακτική προσπέλαση για τους γονείς, είναι να χρησιμοποιηθούν οι έξυπνες κάρτες για να επιτρέψουν στα παιδιά τους να έχουν πρόσβαση σε έναν περιορισμένο αριθμό περιοχών Ιστού που θεωρούνται κατάλληλες από έναν ανήλικο. Αυτές οι περιοχές μπορούν να καταχωρηθούν από το γονέα σε ένα "favorite album" στην κάρτα.[2]

Άλλες εφαρμογές

Άλλες εφαρμογές των έξυπνων καρτών είναι η χρήση τους σε αποκωδικοποιητές, Internet access, product tracking, δίπλωμα οδήγησης

[2] Πηγή: Smart cards: a youthful market

(ιδανική για αποθήκευση penalty points και άμεση αφαίρεση του διπλώματος) κ.α.

3. Αποτύπωση Υφιστάμενης Κατάστασης

3.1. Η Κατάσταση στην Ευρώπη

Για την Ευρωπαϊκή Ένωση, οι Έξυπνες Κάρτες αποτελούν μία από τις προτεραιότητες του Σχεδίου Δράσης του eEurope στα πλαίσια της ανάπτυξης ασφαλών και γρήγορων δικτύων και της ενίσχυσης των ηλεκτρονικών υπηρεσιών και του ηλεκτρονικού επιχειρείν.

Μία πρόσφατη έρευνα, που υλοποιήθηκε από την εταιρεία EDS κατόπιν παραγγελίας και με την συνεργασία του trailblazer 10 του eEurope Smart Card Charter με στόχο την αποτύπωση και την μελέτη των εφαρμογών έξυπνων καρτών στην ηλεκτρονική διακυβέρνηση cards - G2G (government-to-government), G2B (government-to-business), G2C (government-to-citizens) και e-Procurement στη δημόσια διοίκηση, ανέδειξε ότι οι εφαρμογές έξυπνων καρτών που υλοποιούνται στην Ευρώπη αφορούν στις παρακάτω ενότητες:

- Ηλεκτρονική υπογραφή
- Ταυτοποίηση προσωπικού (δημοσίων υπαλλήλων, επαγγελματιών υγείας, κλπ.)
- Ταυτοποίηση εταιρειών από δημόσια διοίκηση και δημόσιους οργανισμούς
- Ηλεκτρονική ταυτότητα πολιτών
- Ηλεκτρονική ταυτότητα ασφαλισμένων
- Υποστήριξη υπηρεσιών σε σχετικά μικρές περιοχές (μαζικές μεταφορές, αναψυχή κλπ.)

Συγκεκριμένα η έρευνα εντόπισε τις παρακάτω εφαρμογές ανά χώρα μέλους της Ευρωπαϊκής Ένωσης.

Χώρα	Ονομασία Έργου	Περιγραφή/ Σχόλια
Austria	citizen card (bürgerkarte)	Common framework social security and other citizen identity cards
Belgium	belpic	BELgian Personal Identity Card for citizens and civil servants
	sis	Social security card
Finland	fineid	Finnish identity cards
	satakunka	Macro-pilot covering health and social security information.
	North karelian hospital district	Management and exchange of health data (FINEID card used for authentication)
France	titre fondateur	Common basis for electronic identity cards, potentially covering: personal identity card, driver licence, other specific cards
	teleprocedures	Tax teleprocedures
	sesam vitale	Identification of insured persons (social security)

Χώρα	Ονομασία Έργου	Περιγραφή/ Σχόλια
	gip cps	Health Professional Cards
	adep	A group of small and mid-sized towns to test usage of e-procedures with the citizen and with the administrations
Germany	media@komm	Initiative for the development of e-procedures in townships and urban districts. The cities of Bremen, Nürnberg and Esslingen are pilots.
	Land of Baden-Württenberg	Multifunctional cards to citizen and public e-procurement
	beschaffungsamt	e-procurement for administrations
Ireland	public services broker	Secure access to public services.
Italy	ieic	Italian Electronic Identity Card
	aes	Advanced Electronic Signature based on IEIC
	msc	Multi Services organisation Card based on IEIC
Netherlands	pki overheid	Government PKI for civil servants
Norway	-	Digital Signature
	-	Health project (under development)
	-	National betting system (under development)
Spain	national PKI	Usage of smart cards in public sector's PKI based applications: identification/authentication + e-sign for civil servants.
Sweden	ID CARD	Multipurpose identity card Internal use within the Administration : National Taxboard, Social Insurance Board
U.K.	e-tendering	System to allow UK departments to exchange tendering information (pilot stage)
	dfee	Connections card: a scheme for 16-19 year olds in education, covering attendance monitoring, access to facilities, credits, etc.
	SMARTCITIES	Local services with the City of Southampton as first pilot

Πηγή: μελέτη EDS – TB 10

Οι βασικές δυσκολίες – προβλήματα που προέκυψαν κατά τον σχεδιασμό και την υλοποίηση των παραπάνω έργων δύναται να συνοψιστούν στα εξής:

- ✓ Στην έλλειψη εξοπλισμού (αναγνωστών καρτών) από πολίτες και μικρές εταιρείες αποτελεί εμπόδιο στην υλοποίηση εφαρμογών G2C
- ✓ Στη συνήθη σύνθεση των θέσεων εργασίας (workstations) που δεν είναι επαρκής και το πλήθος των χρηστών εκτιμούν ότι ο πρόσθετος απαιτούμενος εξοπλισμός είναι σχετικά ακριβός σε σχέση με τα αναμενόμενα αποτελέσματα από την χρήση των έξυπνων καρτών.
- ✓ Στο ότι το πλήθος των χρηστών αισθάνονται ότι η τεχνολογίες έξυπνων καρτών δεν είναι ώριμές και υπάρχει η πιθανότητα να αλλάξουν στο κοντινό μέλλον.
- ✓ Στο ότι μερικές κατηγορίες εργαζομένων - χρηστών θεωρούν ότι η χρήση των έξυπνων καρτών επιφέρουν αλλαγές συνηθειών στην εργασία και υπάρχει φόβος επιβολής πρόσθετων ελέγχων από τις διοικήσεις των με την εφαρμογή έξυπνων καρτών.
- ✓ Στο γενικότερο φόβο, από μεριάς των πελατών, για τις νέες τεχνολογίες, οι οποίοι δύσκολα αλλάζουν συνήθιες. Σ'αυτή την περίπτωση είναι απαραίτητη η ειδική πολιτική marketing, λαμβάνοντας υπόψη, σε μεγάλο βαθμό, τον ψυχολογικό παράγοντα, καθώς και την τεχνολογική μόρφωση του πελάτη.[3]

Όμως, σε όλες τις περιπτώσεις των έργων που μελετήθηκαν, προέκυψε ότι οι έξυπνες κάρτες έγιναν αποδεκτές και χρησιμοποιήθηκαν αποτελεσματικά μετά την περίοδο προσαρμογής.

Αποτελεί γενική εκτίμηση ότι η εξέλιξη και η αποτελεσματικότητα των εφαρμογών έξυπνων καρτών στην Ευρώπη εξαρτάται από τα πρότυπα που υποστηρίζονται, το περιεχόμενο των εφαρμογών και την δυνατότητα χρήσης μίας κάρτας για την εξυπηρέτηση διαφόρων χρήσεων (multi-application usage).

Σχετικά με το θεσμικό πλαίσιο δύο θέματα αναφέρθηκαν:

1. Η προστασία των προσωπικών δεδομένων βάση της εθνικής νομοθεσίας και του European Directive 97/66/EC
2. Η ηλεκτρονική υπογραφή βάση της εθνικής νομοθεσίας και του European Directive 1999/93/EC

Τέλος, οι εφαρμογές έξυπνων καρτών στην ηλεκτρονική διακυβέρνηση θα εστιαστούν κυρίως στις κάρτες υγείας και κοινωνικής ασφάλισης καθώς επίσης και στις κάρτες ταυτοποίησης πολιτών και δημοσίων λειτουργών με δυνατότητες ηλεκτρονικής υπογραφής.

Η συνολική εικόνα για την παρούσα κατάσταση των έξυπνων καρτών στην Ευρώπη δίδεται στη εκτενή μελέτη «Ανοικτή Υποδομή Έξυπνων Καρτών για την

[3] Deborah Fain, Mary Lou Roberts (1997) "Technology vs. Consumer Behavior: the battle for the Financial Servises Customer "

Ευρώπη» που εκπονήθηκε από τις ομάδες εργασίας που εργάστηκαν στα πλαίσια του eEurope Smart Card Charter. Η εν λόγω μελέτη περιλαμβάνει αναλυτική αποτύπωση και αξιολόγηση των έργων που έχουν υλοποιηθεί μέχρι σήμερα στην Ευρώπη, Αμερική και Ιαπωνία καθώς επίσης κατευθύνσεις και πρότυπα για την ανάπτυξη διαλειτουργικών εφαρμογών έξυπνων καρτών ανά τομέα. Η μελέτη «Open Smart Card Infrastructure for Europe", είναι διαθέσιμη στην ηλεκτρονική σελίδα του eEurope Smart Card Charter www.eeuropesmartcards.org.

3.2. Έξυπνες Κάρτες στην Ελλάδα

Οι πρώτες πιλοτικές εφαρμογές Έξυπνων Καρτών εμφανίστηκαν στην χώρα μας το 1988 στο χώρο της υγείας. Έκτοτε ακολούθησαν διάφορες εφαρμογές κυρίως σε ερευνητικό – πιλοτικό περιβάλλον καθώς επίσης και η χρήση των έξυπνων καρτών στις τηλεπικοινωνίες - στην κινητή τηλεφωνία και στα καρτοτηλέφωνα. Οι σημαντικότερες χρήσεις και εφαρμογές έξυπνων καρτών στη χώρα μας είναι:

3.2.1. Κάρτες Τηλεπικοινωνιών

- Εταιρίες κινητής τηλεφωνίας κάρτες SIM - Μερικά εκατομμύρια.
- ΟΤΕ - κάρτες προπληρωμένες (Μνήμης) - Δεκάδες εκατομμύρια.

3.2.2. Τραπεζικές Κάρτες

- Πιστωτικές κάρτες – Ευρεία χρήση, ίσως και εκατομμύρια καρτών.
- Διάφορες Τράπεζες - Έξυπνες κάρτες σαν Security Application Modules - Δεκάδες χιλιάδες.
- Ηλεκτρονικό Πορτοφόλι Εθνικής Τράπεζας - Μερικές εκατοντάδες.
- Ηλεκτρονικό Πορτοφόλι Cafe Εθνική και Εμπορική Τράπεζα - Μερικές εκατοντάδες.
- Εθνική Τράπεζα – Έργο IST Starfish – Μερικές δεκάδες.
- Cash Cards

3.2.3. Κάρτες Υγείας-Κοινωνικής Ασφάλισης

- ΔΗΜΟΣ ΑΜΑΡΟΥΣΙΟΥ (υλοποίηση του Ευρωπαϊκού έργου Cardlink) -
  Μερικές χιλιάδες
- ΕΟΔΕΑΠ (ασφαλιστικός οργανισμός) - Μερικές χιλιάδες
- Ερυθρός Σταυρός - κάρτα διαβητικών - Μερικές εκατοντάδες
- Νοσοκομείο Νίκαιας - κάρτα καρδιοπαθών - Μερικές εκατοντάδες

3.2.4. *Κάρτες Πελατειακής Πιστότητας*

- Εθνοκάρτα - Παρουσίαση (loyalty) - Δεκάδες χιλιάδες
- Καταστήματα VETO (loyalty) - Μερικές χιλιάδες

3.2.5 *Διάφορες Εφαρμογές*

- ΧΑΑ - ΑΣΥΚ (PKI - digital signatures) - Μερικές χιλιάδες
- ΤΕΟ - ΑΤΤΙΚΗ ΟΔΟΣ - ΤΗΛΕΚΑΡΤΕΣ (prepaid) - Δεκάδες χιλιάδες
- Κάρτες πληρωμής διοδίων, δημόσιων συγκοινωνιών και στάθμευσης στην Θεσσαλονίκη (υλοποίηση του Ευρωπαϊκού έργου ADEPT II) – Μερικές Εκατοντάδες.
- Κάρτα πολλαπλών χρήσεων για πληρωμή μεταφορικών υπηρεσιών, υπηρεσίες Υγείας και προσωποποιημένης πρόσβασης σε πληροφορία, στην Θεσσαλονίκη (υλοποίηση του Ευρωπαϊκού έργου DISTINCT) – Μερικές εκατοντάδες.
- Εταιρία διανομής πετραιλοειδών (fleet card) - Δεκάδες χιλιάδες
- Ασφαλής ζύγιση φορτίων ΑΓΕΤ - Μερικές εκατοντάδες

3.3. Θεσμικό Πλαίσιο

3.3.1. Θεσμικό πλαίσιο που διέπει 'άμεσα' τις «έξυπνες κάρτες»

Οι έξυπνες κάρτες, λόγω της πρόσφατης ανάδειξής τους ως μέσο συναλλαγών αλλά και της εμφανιζόμενης πολυμορφίας στον τρόπο χρήσης τους και στις εφαρμογές τους, δεν έχουν αποτελέσει (τουλάχιστον ακόμη), αυτούσιο αντικείμενο κάποιας νομοθετικής ρύθμισης, τόσο σε εθνικό όσο και σε ευρωπαϊκό επίπεδο.Χαρακτηριστικό είναι το γεγονός ότι η φράση 'Έξυπνες Κάρτες' στο εθνικό μας δίκαιο απαντάται μόνο μία φορά (*σύμφωνα με τα δεδομένα της 'Τράπεζας Νομικών Πληροφοριών' του Δικηγορικού Συλλόγου Αθηνών, www.dsanet.gr*) και αυτό στην Υπ. Αποφ. 3227/31-1-2002 (ΦΕΚ Α' 23/13-02-02) του Υπουργείου Εξωτερικών '*περί της δημοσίευσης της απόφασης 1382/2001 του Συμβουλίου Ασφαλείας του ΟΗΕ*' ως προϊόν που εντάσσεται (υπό όρους) στο εμπάργκο (κυρώσεις) κατά του Ιράκ! Βέβαια, οι έξυπνες κάρτες (smart cards) αναφέρονται σε πάρα πολλά προπαρασκευαστικά κείμενα (*δηλαδή κείμενα μη άμεσης υποχρεωτικής εφαρμογής*) της Ευρωπαϊκής Ένωσης, όπως ανακοινώσεις, ψηφίσματα, συστάσεις, γνωμοδοτήσεις κ.λ.π., ιδίως στα πλαίσια των εγκεκριμένων προγραμμάτων δράσης eEurope2002 (και πρόσφατα eEurope2005) στα οποία διαφαίνεται η πρόθεση προώθησης και υιοθέτησης του συγκεκριμένου μέσου ως βασικό συντελεστή για την επίτευξη της πολυπόθητης ασφάλειας στην Κοινωνία της Πληροφορίας.

Επίσης, ο προσδιορισμός τεχνικών προδιαγραφών και οι δημιουργία σχετικών τεχνικών προτύπων από οργανισμούς προτυποποίησης (π.χ. ETSI, CEN, ISO, ITU, κ.λ.π.) ή και από διάφορα ιδιωτικά consortiums (π.χ. EMVCo) -*για συγκεκριμένες χρήσεις τους ή γενικά*- δεν αποτελούν από μόνα τους 'θεσμικό πλαίσιο' στον βαθμό, βέβαια, που δεν υπάρχουν οι σχετικές νομοθετικές, κανονιστικές ή διοικητικές διατάξεις που να παραπέμπουν ή να αναφέρονται σ' αυτά. (*μιας και τα 'πρότυπα', ακόμη και αν έχουν δημοσιευθεί από 'αναγνωρισμένους οργανισμούς', δεν είναι –από μόνα τους- υποχρεωτικά*)

3.3.2. Θεσμικό πλαίσιο που σχετίζεται (έμμεσα) με τις «έξυπνες κάρτες»

Από την άλλη πλευρά, τουλάχιστον σε ευρωπαϊκό επίπεδο (*και στο βαθμό που εναρμονίζεται με αυτό η εθνική νομοθεσία μας, και σε εθνικό επίπεδο*), έχουν θεσπισθεί μια σειρά από διατάξεις (κυρίως Οδηγίες του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου) σχετικά με θέματα που άπτονται συγκεκριμένων εφαρμογών των 'έξυπνων καρτών'. Έτσι, ανάλογα με το είδος της εφαρμογής που χρησιμοποιείται μια έξυπνη κάρτα, μπορούν να αναφερθούν χαρακτηριστικά τα εξής νομοθετήματα:

- **Η Έξυπνη κάρτα ως *'συσκευή για την πρόσβαση υπό όρους'* (σε 'προστατευόμενες υπηρεσίες')**

  - Οδηγία 98/84/ΕΚ «*για τη νομική προστασία των υπηρεσιών που βασίζονται ή συνίστανται στην παροχή πρόσβασης υπό όρους*»

  Με την Οδηγία αυτή λαμβάνονται μέτρα κατά των παράνομων συσκευών που παρέχουν μη επιτρεπόμενη πρόσβαση σε προστατευόμενες υπηρεσίες, ενώ
  παράλληλα προστατεύεται (άρ. 3 §2) *η ελεύθερη κυκλοφορία των συσκευών για την πρόσβαση υπό όρους.*

  Ως '**συσκευή για την πρόσβαση υπό όρους**' δίνεται (άρ. 2, περ. γ') ο εξής ορισμός:

  «*οποιοσδήποτε εξοπλισμός ή λογισμικό που έχει σχεδιαστεί ή προσαρμοστεί έτσι ώστε να καθιστά δυνατή την πρόσβαση σε μια υπηρεσία σε κατανοητή μορφή*» και προφανώς βρίσκει εφαρμογή σε πολλές περιπτώσεις που η έξυπνη κάρτα χρησιμοποιείται ως (μέρος) τέτοιου εξοπλισμού π.χ. για την αποκωδικοποίηση δορυφορικών τηλεοπτικών σημάτων, για την πρόσβαση στο δίκτυο GSM (κινητή τηλεφωνία), ακόμη και για πρόσβαση σε συγκεκριμένες υπηρεσίες τηλεματικής, όπως είναι π.χ. το σύστημα 'HERMES' του Χρηματιστηρίου Αξιών Αθηνών που χρησιμοποιεί έξυπνες κάρτες για ταυτοποίηση των χρηστών του.

- **Η Έξυπνη κάρτα ως *'ασφαλή διάταξη δημιουργίας (ηλεκτρονικής) υπογραφής'***

  - Οδηγία 99/93/ΕΚ «*σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές*»

  Με την Οδηγία αυτή (*η οποία έχει ενσωματωθεί στο εθνικό μας δίκαιο με το π.δ. 150/2001*) , αν και δεν αναφέρεται ονομαστικά στις smart cards, θέτονται οι βασικές προδιαγραφές που πρέπει να τηρούν οι φορείς (και όχι μόνο) των ιδιωτικών κλειδιών ('δεδομένων δημιουργίας υπογραφής') των τελικών χρηστών ώστε να εξασφαλίζεται το απαιτούμενο επίπεδο

ασφάλειας για την δημιουργία (εφόσον συντρέχουν και άλλες προϋποθέσεις, όπως αυτή της έκδοσης 'αναγνωρισμένου πιστοποιητικού') *'αναγνωρισμένης ηλεκτρονικής υπογραφής'* (άρ 5§1 της Οδηγίας ή 3§1 του ελληνικού π.δ.) που χαίρει απόλυτης ισοδυναμίας με την αντίστοιχη ιδιόχειρη υπογραφή.

Αν και ως *'φορείς των δεδομένων δημιουργίας υπογραφής'* μπορούν να χρησιμοποιηθούν και άλλα μέσα (π.χ. USB tokens), η χρήση των 'έξυπνων καρτών (*που θα τηρούν τις τεχνικές προδιαγραφές και τα πρότυπα που εκδίδονται από τους ευρωπαϊκούς οργανισμούς προτυποποίησης και που εξειδικεύουν –κατά παραγγελία της σχετικής επιτροπής- τις διατάξεις της συγκεκριμένης οδηγίας*) ως βασικό ασφαλές μέσον για την εναπόθεση ιδιωτικών κλειδιών και τη δημιουργία αναγνωρισμένων υπογραφών, θεωρείται δεδομένη. (*λόγω και των προαναφερόμενων για το εγκεκριμένο σχέδιο δράσης eEurope2005*).

- **Η Έξυπνη κάρτα ως *'ηλεκτρονικό πορτοφόλι' ή, άλλως, ως 'φορέας πιστωτικών μονάδων'***

Αν και οι συγκεκριμένες εφαρμογές της έξυπνης κάρτας χρησιμοποιούνται ήδη σε πιλοτικά προγράμματα (π.χ. BalcanCard) ή και σε πρακτικές εφαρμογές (π.χ. οι γνωστές 'τηλεκάρτες' με τις προπληρωμένες μονάδες), εντούτοις δεν υπάρχει ακόμη σχετικό θεσμικό πλαίσιο και οι σχετικές αποδεικτικές συμβάσεις διέπονται πλήρως από την αρχή της «ελευθερίας των συμβάσεων» όπου οι χρήστες και οι πάροχοι των σχετικών υπηρεσιών συμφωνούν από μόνοι τους στον αποδεικτικό χαρακτήρα και λειτουργία των μέσων που χρησιμοποιούν!

Στα πλαίσια της **αναμενόμενης Οδηγίας «για την εξ αποστάσεως εμπορία καταναλωτικών χρηματοπιστωτικών υπηρεσιών»** είναι πολύ πιθανό να ρυθμιστούν σχετικά θέματα και να θέτονται κάποια standard ασφαλείας στα μέσα που θα χρησιμοποιούνται για αυτές. Πάντως, είναι δεδομένο ότι στο βαθμό που αρμόζουν, ισχύουν και για τις έξυπνες κάρτες οποιεσδήποτε διατάξεις διέπουν την χρήση και λειτουργία ανάλογων μέσων πληρωμής.

3.3.3. Άλλες διατάξεις που σχετίζονται έμμεσα με τις «έξυπνες κάρτες»

Άλλες σημαντικές διατάξεις -που σχετίζονται όμως, **κυρίως με τον τρόπο ανάπτυξης των εφαρμογών που χρησιμοποιούν 'έξυπνες κάρτες'** και όχι άμεσα με αυτές τις ίδιες, είναι πάρα πολλές και ισχύουν κατά περίπτωση. Ενδεικτικά:

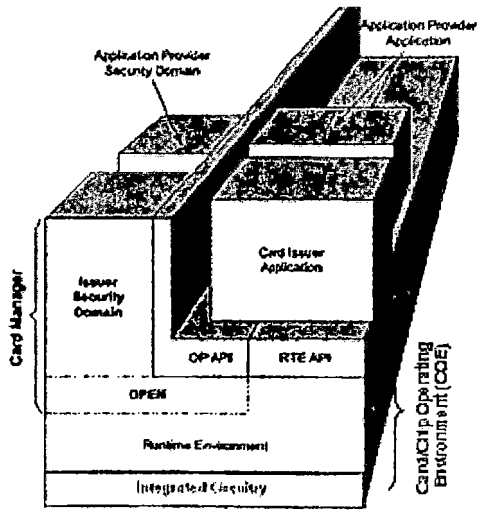
- ✓ Οδηγίες 95/46/ΕΚ και 97/66/ΕΚ για την προστασία δεδομένων προσωπικού χαρακτήρα,

- ✓ Οδηγία 97/7/ΕΚ για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις,
- ✓ Οδηγία 00/31/ΕΚ για το ηλεκτρονικό εμπόριο.

4. Ασφάλεια έξυπνων καρτών

4.1. Εισαγωγή

Οι απαιτήσεις ασφάλειας για τις Open Platform (OP) έξυπνες κάρτες (OP) καθορίζονται από τον GlobalPlatform Card Specification και ανασχηματίζονται με την γλώσσα ISO/IEC 15408 (the "Common Criteria") στο Visa Open Platform Protection Profile. Το GPCS δεν διαμορφώνει στις απαιτήσεις ασφάλειας για το ελλοχεύουν περιβάλλον χρόνου εκτέλεσης (Runtime Environment, RTE) ή τα ενσωματωμένα στοιχεία κυκλώματος (IC).



Εντούτοις, το OP3 μπαίνει σε μία περαιτέρω λεπτομέρεια, με τον προσδιορισμό της ιδιοκτησίας ασφάλειας αυτού που καλεί "Card/Chip Operating Environment" ("λειτουργούν περιβάλλον καρτών/τσιπ", COE, βλέπε το σχήμα

παρακάτω) από την άποψη των στόχων ασφάλειας, των προσδοκώμενων λειτουργιών ασφάλειας και των τύπων απειλής ότι το COE αναμένεται να αντιμετωπίσει. Αυτή η προδιαγραφή οφείλει να είναι ικανοποιητική, αλλά στην πράξη υπάρχουν άλλα σχεδιαγράμματα προστασίας που χρειάζονται να θεωρηθούν.

4.2. Η αρχιτεκτονική ασφάλειας.

Η αρχιτεκτονική ασφάλειας εμφανίζεται στο παρακάτω σχεδιάγραμμα. Αυτή η αρχιτεκτονική μπορεί να θεωρηθεί γενική και εφαρμόσιμη σε όλες τις OP έξυπνες κάρτες. Υπάρχουν 8 ιεραρχικά στρώματα, αποκαλούμενα:

(α) **Στρώμα 1** - φυσική αντίσταση

(β) **Στρώμα 2** - ηλεκτρική διαπροσωπεία

(γ) **Στρώμα 3** - έλεγχος λογισμικού

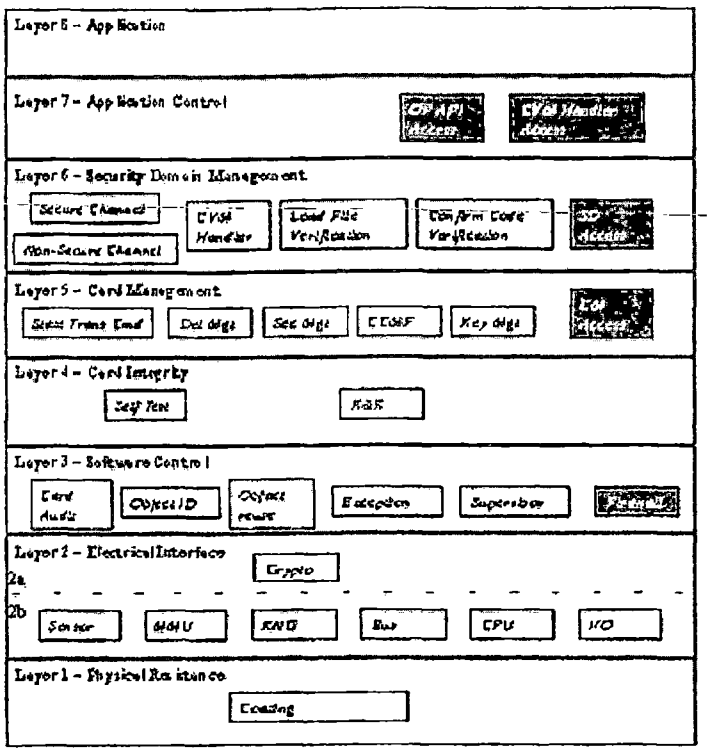
(δ) **Στρώμα 4** - ακεραιότητα καρτών

(ε) **Στρώμα 5** - διαχείριση καρτών

(στ) **Στρώμα 6** - διαχείριση δικτυακών γειτονιών ασφάλειας

(ζ) **Στρώμα 7** - έλεγχος εφαρμογής

(η) **Στρώμα 8** - εφαρμογή.



Υποθέτοντας ότι το TOE είναι εμπιστευτικό, υπάρχουν ακριβώς τρεις τρόποι από τους οποίους ένας επιτιθέμενος μπορεί να προσπαθήσει να αποκτήσει πρόσβαση στα προτερήματα που προστατεύονται από το TOE:

(α) ως εφαρμογή (στρώμα 8), το οποίο σημαίνει ότι ο επιτιθέμενος πρέπει κάπως να εισαγάγει μια εφαρμογή "πρακτόρων" "agent" επάνω στην κάρτα .

(β) ως μακριά οντότητα καρτών μέσω της δυνατότητας εισόδου/εξόδου (I/O) (στρώμα 2), το οποίο είναι η κανονική μέθοδος για μια απομακρυσμένη οντότητα καρτών για να επικοινωνήσει με την κάρτα.

(γ) από μια άμεση επίθεση στην κάρτα.

Σε πρώτο στάδιο, μια τέτοια άμεση επίθεση μπορεί να προσπαθήσει να διαπεράσει τις υπερασπίσεις του πρώτου στρώματος - φυσική αντίσταση. Στη συνέχεια ο επιτιθέμενος πρέπει να αντιμετωπίσει τις υπερασπίσεις του δεύτερου στρώματος - ηλεκτρική διαπροσωπεία. Μια επίθεση που διαπράττεται μέσω μιας απομακρυσμένης οντότητας καρτών μέσω της I/O δυνατότητας εξετάζεται επίσης σε αυτό το στρώμα. Κατά συνέπεια, αυτά τα δύο στρώματα διαμορφώνουν την πρώτη γραμμή υπεράσπισης ενάντια σε μια άμεση επίθεση στην κάρτα.

Στο στρώμα 3 - ο έλεγχος λογισμικού, OP παίρνει τον έλεγχο της ασφάλειας, που εξασφαλίζει ότι τα χαρακτηριστικά γνωρίσματα ασφάλειας OP και του RTE καλούνται πάντα και μπορούν να παρακαμφθούν, να απενεργοποιηθούν, να αλλοιωθούν ή ειδάλλως να παρακαμφθούν. Το στρώμα 3, που χτίζει στα διοικητικά χαρακτηριστικά γνωρίσματα μνήμης που περιλαμβάνονται στο στρώμα 2 και τους μηχανισμούς "firewall" RTE που ενσωματώνονται στο στρώμα 3, παρέχει επίσης το χωρισμό applet. Κατά συνέπεια, μια άλλη υπηρεσία που παρέχεται από το στρώμα 3 στα υψηλότερα στρώματα είναι ότι η μια εφαρμογή, συμπεριλαμβανομένων των SELECT-able OP εφαρμογών (δηλ. διευθυντής καρτών και οι διάφορες δικτυακές γειτονιές ασφάλειας) μπορεί να παρέμβει η μια με την άλλη.

Στο στρώμα 4 - η ακεραιότητα καρτών, οποιαδήποτε προβλήματα ως αποτέλεσμα της πρόωρης απόσυρσης της κάρτας από μια συσκευή ή ένα τερματικό αποδοχής καρτών, ή οποιασδήποτε μορφής της ισχύος επιλύεται.

Στο στρώμα 5 - η διαχείριση καρτών, πρόσβαση στις OP διοικητικές λειτουργίες καρτών κοντά από τις οντότητες καρτών ελέγχεται, η απαραίτητη OP λειτουργία διευθυντών καρτών παρέχεται και οι διάφορες κρατικές μεταβάσεις (π.χ. λήξη καρτών, κλείδωμα εφαρμογής και ξεκλείδωμα) εφαρμόζονται.

Στο στρώμα 6 - η διαχείριση δικτυακών γειτονιών ασφάλειας, πρόσβασης στις OP λειτουργίες δικτυακών γειτονιών ασφάλειας (π.χ. η καθιέρωση ενός ασφαλούς καναλιού) από τις οντότητες από-καρτών ελέγχεται και η σχετική λειτουργία παρέχεται.

Στο στρώμα 7 - ο έλεγχος εφαρμογής, πρόσβαση OP API από τις εφαρμογές ελέγχεται. Οι ιδιαίτερες λειτουργίες ασφάλειας OP που λειτουργούν στο στρώμα 5 αποτρέπουν τη φόρτωση των εφαρμογών, που εκτελούν στο στρώμα 8, το οποίο είναι αναρμόδιο από τον εκδότη .

Οι λειτουργίες ασφάλειας εκτός από τα διάφορα στρώματα, προσδιορίζουν "bundles" SFRs (δέσμες) που έχουν έναν ομοειδή σκοπό. Αυτές αντιπροσωπεύουν τα χαρακτηριστικά γνωρίσματα ασφάλειας της αρχιτεκτονικής, η οποία μπορεί να αναφερθεί καθώς η ασφάλεια TOE λειτουργεί (TSFs).

4.2.1. Τα στρώματα 1 και 2

Τα πρώτα δύο στρώματα μπορούν να θεωρηθούν ευρέως ως αντιπροσωπεύσεις του ολοκληρωμένου κυκλώματος. Εντούτοις, για να εφαρμόσει μια υψηλής ποιότητας τυχαία γεννήτρια αριθμού στο υλικό, η απόφαση, για να χρησιμοποιήσει το υλικό ή το λογισμικό, η κρυπτογράφηση αφήνεται στον κατασκευαστή καρτών. Συνεπώς, το στρώμα 2 είναι χωρισμένο σε 2 υποστρώματα για να επιτρέψει στην αρχιτεκτονική να περιγράψει πιστά τις κάρτες με και χωρίς τη βασισμένη στο υλικό κρυπτογράφηση. "Crypto" TSF παρέχει τις υπηρεσίες κρυπτογράφησης/ αποκρυπτογράφησης σε διάφορα TSFs στα στρώματα

5 και 6, όπως "Del Man" TSF, το οποίο παρέχει την OP εξουσιοδοτημένη διοικητική λειτουργία, η οποία είναι στη συνέχεια βασισμένη στο σύστημα κρυπτογραφία. Συγκεκριμένα, ο εκδότης καρτών μπορεί να επιτρέψει σε έναν προμηθευτή εφαρμογής να διαχειριστεί τη φόρτωση, την εγκατάσταση και τη διαγραφή των αιτήσεών τους, δίνοντας την κατάλληλη προ-έγκριση. Στην περίπτωση της φόρτωσης και της εγκατάστασης ο εκδότης καρτών παρέχει τον προμηθευτή εφαρμογής ένα σημείο που είναι μια λειτουργία της εξουσιοδοτημένης εφαρμογής που υπογράφεται, χρησιμοποιώντας ένα ιδιωτικό πλήκτρο από τον εκδότη καρτών. "Del Man" TSF επιστρέφει επίσης ένα unforgeable σημείο για να επιβεβαιώσει ότι η λειτουργία έχει εκτελεσθεί επιτυχώς.

Το άλλο TSFs στο στρώμα 1 και 2 επάνω στα κύρια συστατικά που καθένας θα ανέμενε να βρεί σε ένα ολοκληρωμένο κύκλωμα, όπως η κεντρική μονάδα επεξεργασίας (CPU), η είσοδος/η έξοδος (I/O), η διοικητική μονάδα μνήμης (MMU) και οι δίαυλοι, καθώς επίσης και μερικοί εκ των οποίων η αρχική λειτουργία είναι η ασφάλεια, όπως και οι αισθητήρες. Ο σκοπός των "αισθητήρων" TSF είναι να ανιχνευθεί πότε οι λειτουργούσες παράμετροι, όπως η θερμοκρασία, η ηλεκτρική τάση και η συχνότητα ρολογιών, πηγαίνουν πέρα από τα ασφαλή λειτουργούντα όριά τους. Το "MMU" TSF ελέγχει την πρόσβαση στη μνήμη, έτσι ώστε το λογισμικό, που έχει περιοριστεί για να χρησιμοποιήσει μια ιδιαίτερη σειρά διευθύνσεων, μπορεί να έχει πρόσβαση σε οποιοδήποτε μέρος της μνήμης έξω από εκείνη την σειρά. Επιπλέον τα μέτρα ασφάλειας που παρέχονται με το " Bus " TSF σχεδιάζονται για να προστατεύσουν την εμπιστευτικότητα των στοιχείων που περνούν κατά μήκος του σε και από την CPU και τα άλλα συστατικά ολοκληρωμένου κυκλώματος.

Το "επίστρωμα" (Coating) TSF έχει το σκοπό να κάνει προφανή οποιαδήποτε προσπάθεια να πειράξει φυσικά την κάρτα και μπορεί ίσως, ανάλογα με τα χαρακτηριστικά του επιστρώματος, να οδηγήσει στην αμετάκλητη ζημία στο ολοκληρωμένο κύκλωμα.

4.2.2. Το στρώμα 3

Το στρώμα 3 παρέχει τα περισσότερα από τα χαρακτηριστικά γνωρίσματα ασφάλειας που απαιτούνται από το RTE, άλλα που παρέχονται στα στρώματα 4 και 5. Η πρόσβαση εφαρμογής ελέγχων "Firewall" TSF σε RTE αντικειμένα, αντιτίθεται και στηρίζεται στην ταυτότητα "TSF" για να τους προσδιορίσει. Ο αρχικός σκοπός του "Firewall" TSF, σε συνδυασμό με το "MMU" TSF, είναι να να αποτρέψει τις εφαρμογές από την επικοινωνία η μια με την άλλη από οποιαδήποτε μέσα εκτός από ένα υποστηριγμένο RTE κανάλι επικοινωνίας διά-εφαρμογής (π.χ. μέσω ενός διαμοιράσιμου αντικειμένου διαπροσωπειών σε JavaCard™) και μόνο σύμφωνα με μια προσδιορισμένη RTE πολιτική

ελέγχου πρόσβασης και μια προσδιορισμένη RTE πολιτική ελέγχου ροής πληροφοριών.

Τα μέσα "εξαίρεσης" TSF χειρίζονται τις εξαιρέσεις RTE (πχ. σύμφωνα με τις προδιαγραφές JavaCard™) αλλά επιπλέον φροντίζουν για OP "εξαιρέσεις", όπως η ανίχνευση των πιθανών παραβιάσεων ασφάλειας. Σε όλες τις περιπτώσεις, η προκύπτουσα ενέργεια πρέπει να είναι σύμφωνη με μια καθορισμένη πολιτική εκδόσης καρτών, η οποία δεν καθορίζεται από το OP3 ή οποιαδήποτε άλλο PPs που μελετάται, αποκαλούμενα ως P.EVENT_ACTIONS. Αυτή η πολιτική καθοδηγεί το διευθυντή καρτών τι να κάνει σε κάθε ιδιαίτερη περίσταση. Οι ενέργειες κυμαίνονται από "do nothing" σε "terminate the card ", και παρέχουν στον εκδότη καρτών την ευελιξία να υιοθετήσει ή να απορροφήσει τις προαιρετικές απαιτήσεις GPCS στις οποίες οι OP3 αναφέρονται ως "Intrusion Detection Package" (συσκευασία ανίχνευσης παρείσφρησης). Ο διευθυντής καρτών είναι ένα OP συστατικό που είναι η αντιπροσωπευτική κάρτα του εκδότη καρτών και είναι ο κεντρικός διοικητής της κάρτας.Αυτή η λειτουργία είναι τυλιγμένη επάνω στο επόπτη TSF, ο οποίος επίσης:

- Από μια προοπτική ασφάλειας, εξασφαλίζει ότι όλα εφαρμοσμένα τα λογισμικό χαρακτηριστικά γνωρίσματα ασφάλειας καλούνται στο σωστό χρόνο και μπορούν να παρακαμφθούν, να απενεργοποιηθούν, να αλλοιωθούν ή ειδάλλως να παρακαμφθούν (FPT_RVM.1).
- Από μια προοπτική JavaCard™, εκτελεί τα applets.

Η επαναχρησιμοποίηση "TSF" αντικειμένου σιγουρεύει, ότι οποιοδήποτε στοιχείο που αφήνεται σε οποιοδήποτε αντικείμενο, καταστρέφεται προτού να επαναχρησιμοποιηθεί εκείνο το αντικείμενο, ή να μπορέσει ειδάλλως να προσεγγιστεί από μια διαφορετική εφαρμογή. Υπάρχουν ποικίλοι τέτοιοι όροι επαναχρησιμοποίησης, που περιλαμβάνουν τα προσωρινά αντικείμενα αποθήκευσης στοιχείων, τους κρυπτογραφικούς προσωρινούς χώρους, τον προσωρινό χώρο APDU και τη μεταβλητή επίμονη μνήμη που πρέπει να εγκαταλειφθούν όταν διαγράφεται μια εφαρμογή. Ο λογιστικός έλεγχος "TSF" καρτών επιτρέπει στην ταυτότητα της κάρτας να αποκαλυφθεί σε μια μακριά οντότητα καρτών μαζί με άλλη, παραδοσιακότερες πληροφορίες λογιστικού ελέγχου υπολογιστών, σύμφωνα με τις πολιτικές του εκδότη καρτών.

4.2.3. *Το στρώμα 4*

Τα SFRs που χαρτογραφούν στο στρώμα 4 διαιρούνται σε δύο ευδιάκριτες κατηγορίες: σε εκείνα που εξετάζουν την κάρτα και εκείνων που επιτρέπουν στην κάρτα να ανακτηθεί σε ένα ασφαλές κράτος, μετά από μερική ατυχία, όπως μια αποτυχία ισχύος. Το Self-testing, μεταξύ άλλων, επιτρέπει στην κάρτα να ανιχνεύσει, εάν έχει πειραχτεί, δεδομένου ότι τροφοδοτήθηκε στο τέλος. Αυτό είναι πολύ σημαντικό, δεδομένου ότι μια κρίσιμη πτυχή της ασφάλειας πληροφοριών, είναι να είναι γνωστό πότε έχειγίνει μία επίθεση. Η ενέργεια που λαμβάνεται σε αυτό το γεγονός θα ήταν σύμφωνη με την πολιτική P.EVENT_ACTIONS αλλά θα μπορούσε να δοποιήσει τον εκδότη και το κλείδωμα καρτών, ή να ολοκληρώσει την κάρτα. Το άλλο TSF (R&R) εξετάζει τη μείωση των τιμών και την αποκατάσταση. Αυτό δεν είναι τόσο απλό όπως πιθανόν να αναμενόταν, από μια προοπτική ασφάλειας, μερικά γεγονότα δεν πρέπει ποτέ να κυληθούν πίσω. Παραδείγματος χάριν, εάν το pin ξαναδοκιμάσει αντίθετα, ο επιτιθέμενος μπορεί να είναι σε θέση να κερδίσει έναν απεριόριστο αριθμό προσπαθειών. Οι πολιτικές που έχονται σχέση προσδιορίζονται από το OP3.

4.2.4. *Το στρώμα 5*

Το στρώμα 5 παρέχει τα χαρακτηριστικά γνωρίσματα διευθυντών καρτών όπως καθορίζονται σε GPCS και τις βασικές κρυπτογραφικές βασικές διοικητικές υπηρεσίες. Τα τελευταία, που εφαρμόζονται από το "βασικό Mgt" TSF, έχουν σχέση την παραγωγή, την διανομή, τη δυνατότητα πρόσβασης και την καταστροφή των κρυπτογραφικών πλήκτρων. Το TSF βρίσκεται στο υψηλότερο επίπεδο, στη βαλμένη σε στρώσεις, ιεραρχία από το "R&R" TSF επειδή υπάρχουν πίσω πολιτικές ρόλων που συνδέονται με ορισμένες βασικές διοικητικές διαδικασίες, όπως η αντικατάσταση ενός πλήκτρου. Τόσο οι OP, όσο και οι βασικές διοικητικές RTE διαδικασίες φροντίζουν, με αυτόν τον τρόπο να επιτρέψουν στις εφαρμογές τη δυνατότητα να καλέσουν τις πρότυπες κρυπτογραφικές λειτουργίες RTE.

Το "State Trans Cmd" TSF, ελέγχει τις μεταβάσεις μεταξύ του διάφορων διευθυντή καρτών, του αρχείου φορτίων και των κρατών κύκλου της ζωής εφαρμογής που καθορίζονται από GPCS. Το OP3, η εφαρμόσιμη πολιτική ελέγχου πρόσβασης, είναι P.STATE_TRANSITION. Από την παραμονή TSFs, "Del Mgt" έχει συζητηθεί προηγουμένως (βλ. τα στρώματα 1 και 2), "τα SEC Mgt" και "CCMF" παρέχουν τις διάφορες λειτουργίες ασφάλειας και διαχείρισης και ικανοποιητικής διαχείρισης

καρτών αντίστοιχα, και τους ελέγχους "πρόσβασης CM" από την πρόσβαση καρτών (δηλ. μέσω των εντολών APDU) στο διευθυντή καρτών. Το OP3, η εφαρμόσιμη πολιτική ελέγχου πρόσβασης, είναι P.CARD_MANAGER. Στις μελλοντικές αναθεωρήσεις της αρχιτεκτονικής, είναι πιθανό ότι το "Del Mgt" και το "CCMF" TSFs θα συνδυαστεί επειδή η εξουσιοδοτημένη GPCS διοικητική λειτουργία είναι ακριβώς μια ειδική περίπτωση του γενικότερου κανόνα ότι όλο το CCMFs (π.χ. η φόρτωση, η εγκατάσταση και η διαγραφή των εφαρμογών) πρέπει μόνο να πραγματοποιηθεί με την προ-έγκριση του εκδότη καρτών. Φυσικά, όταν εκδίδει ο εκδότης καρτών την εντολή, καθένας θα υπέθετε ότι "προ-έχει εγκρίνει" ο ίδιος!

4.2.5. Τα στρώματα 6, 7 και 8

Τα TSFs στο στρώμα 6 αντιπροσωπεύουν τις διάφορες λειτουργίες GPCS σχετικά με τις δικτυακές γειτονιές ασφάλειας. Οι δικτυακές γειτονιές ασφάλειας είναι οι αντιπρόσωποι-καρτών των προμηθευτών εφαρμογής και των αρχών επαλήθευσης (που καλούνται συλλογικά " χρήστες δικτυακών γειτονιών ασφάλειας") και μπορούν να διαχειριστούν τη φόρτωση και την εγκατάσταση των εφαρμογών προ-που εγκρίνονται από τον εκδότη καρτών. Η πολλαπλότητα των δικτυακών γειτονιών ασφάλειας επιτρέπει στα στοιχεία ασφάλειας, κάθε ασφάλειας χρήστη δικτυακών γειτονιών (όπως τα κρυπτογραφικά πλήκτρα) να κρατηθεί χωριστά και ιδιωτικά από αυτόν των άλλων χρηστών δικτυακών γειτονιών ασφάλειας και του εκδότη καρτών. Ο διευθυντής καρτών περιέχει μια δικτυακή γειτονιά ασφάλειας (που αναφέρεται ως δικτυακή γειτονιά ασφάλειας εκδοτών) για τη μόνη χρήση του εκδότη καρτών στο ρόλο του ως προμηθευτή εφαρμογής ή αρχή επαλήθευσης. (στον τραπεζικό κόσμο αυτή η δυαδικότητα του ρόλου είναι ο κανόνας, παρά την εξαίρεση.) Η αρχή επαλήθευσης είναι ένας ρόλος που είναι ουσιαστικός στην περίπτωση JavaCard™, δεδομένου ότι η λειτουργία της είναι να επιβεβαιώσει ότι οι εφαρμογές έχουν περάσει την επαλήθευση κώδικα οκτάδων. Στην περίπτωση όπου ο εκδότης καρτών δεν είναι ο μόνος προμηθευτής εφαρμογής, το OP3 επιμένει ότι η επιβεβαίωση της επιτυχούς επαλήθευσης κώδικα οκτάδων εκτελείται χρησιμοποιώντας τις λειτουργίες επαλήθευσης προτύπων πιστοποίησης ταυτότητας στοιχείων GPCS (DAP), μέσω μιας χωριστής δικτυακής γειτονιάς ασφάλειας που είναι κύριως από την αρχή επαλήθευσης και χρησιμοποιείται μόνο για εκείνο τον σκοπό. Αυτή η λειτουργία παρέχεται από τον TSF "κώδικα επιβεβαίωσης της επαλήθευσης".

Ο αρχικός σκοπός GPCS της επαλήθευσης DAP, είναι να επιτραπεί στους προμηθευτές εφαρμογής την ευκαιρία να ελέγξουν ότι οι εφαρμογές που φορτώνονται από τον εκδότη καρτών, είναι γνήσιοι. Αυτό είναι μια προαιρετική λειτουργία του GPCS, όπως η ανάγκη να

πραγματοποιηθεί αυτή η μορφή της επαλήθευσης εξαρτάται από το επίπεδο κινδύνου που είναι αποδεκτό στα διάφορα συμβαλλόμενα μέρη που έχουν σχέση. Η λειτουργία παρέχεται από τη "επαλήθευση" TSF αρχείων φορτίων και μπορεί να συνδυαστεί σε μια μελλοντική αναθεώρηση της αρχιτεκτονικής με " Confirm Code Verification" TSF κώδικα (επιβεβαίωση του κώδικα επαλήθευσης), όπως οι μηχανικοί των δύο μηχανισμών ασφάλειας, αν και αυτοί χρησιμοποιούνται για δύο εξ ολοκλήρου διαφορετικούς σκοπούς, είναι ίδια.

Το "ασφαλές κανάλι" TSF εφαρμόζει όλο το SFRs σχετικά με το OP ασφαλές πρωτόκολλο καναλιών (SCP). Το SCP παρέχει ποικίλες ασφαλείς υπηρεσίες επικοινωνιών κάρτα-host συμπεριλαμβανομένου:

- Αμοιβαία ή όμοια πιστοποίηση ταυτότητας ανάλογα με το SCP που χρησιμοποιείται (GCPS η έκδοση 2.1 καθορίζει δύο τέτοια πρωτόκολλα)
- Κρυπτογράφηση μηνυμάτων
- Ακεραιότητα μηνυμάτων
- Μια υπεράσπιση ενάντια στην επίθεση "επανάληψης"
- Ασφαλή μέσα για τη βασική διανομή και το φόρτωμα "των αξιών επαλήθευσης κατόχων κάρτας", π.χ. PINs.

Αν και το SCP πρέπει να χρησιμοποιηθεί για τις ιδιαίτερες εντολές APDU, υπάρχουν άλλες επικοινωνίες, παραδείγματος χάριν εκείνοι μεταξύ μιας μακριά οντότητας καρτών και των εφαρμογών, για τις οποίες η χρήση του SCP είναι προαιρετική. Ο σκοπός του "μη-ασφαλούς καναλιού" TSF είναι να εξασφαλιστεί ότι αυτό το "μη-ασφαλές κανάλι" μπορεί να χρησιμοποιηθεί για να συμβιβάσει την ασφάλεια της κάρτας. Αυτός ο μάλλον περίεργος στόχος ενισχύεται στο GPCS, στην έκδοση 2.1, δεδομένου ότι μια περίοδος επικοινωνίας SCP θα ξεκινάει αυτόματα μόλις παραλαμβάνεται μια cryptographically προστατευμένη εντολή APDU, παρά να πρέπει να περιμένει μια INITIALIZE UPDATE που είναι η ρητή εντολή για να αρχίσει μια περίοδο επικοινωνίας SCP.

Ο "CVM χειριστής" TSF παρέχει τα μέσα για τις εφαρμογές για να μοιραστεί μια κοινή μέθοδο επαλήθευσης κατόχων κάρτας (που είναι μια προαιρετική δυνατότητα GPCS), καθώς επίσης και παρέχοντας τα παραδοσιακά μέσα RTE για την πιστοποίηση ταυτότητας κατόχων κάρτας όπως το pin ιδιοκτητών σε JavaCard™. Από την οντότητα καρτών η πρόσβαση σε όλες αυτές τις λειτουργίες ελέγχεται από την πρόσβαση

"TSF" SD (P.SECURITY_ DOMAIN in OP3). Η πρόσβαση σε αυτές τις λειτουργίες, και εκείνες στο στρώμα 5, που είναι προσιτές στις εφαρμογές (δηλ. μέσω OP API) ελέγχονται από το "CVM χειριστή" TSF για την πιστοποίηση ταυτότητας κατόχων κάρτας (P.CVM OP3) και από την "OP API πρόσβαση" TSF για όλες τις άλλες λειτουργίες (P.OP_API OP3). Αυτή την περίοδο κανένα TSFs δεν συνδέεται με το στρώμα εφαρμογής, σε καμία από τις μελετημένες PPs, μέχρι τώρα, εφαρμογές κάλυψης.

4.2.6. Μια παρατήρηση

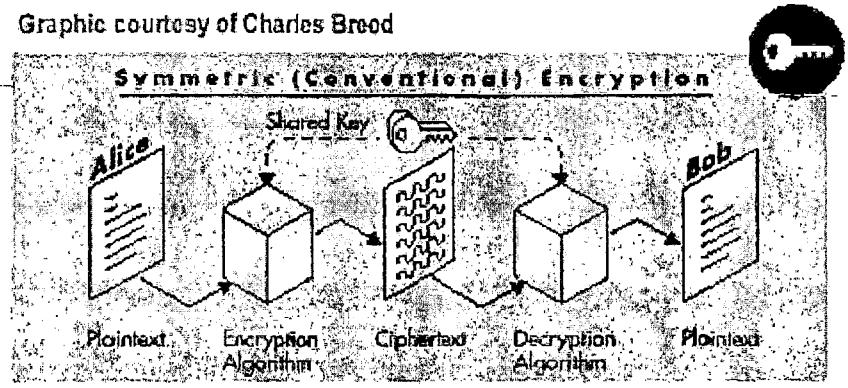
Κατά τη διάρκεια της κατανομής SFRs στο στρώμα 2 TSFs έγινε εμφανής ότι:

1. Υπήρξε απώλεια SFRs. Παραδείγματος χάριν, μία από τις λειτουργίες του "RNG" TSF είναι να παράγει τυχαίες καταστάσεις αναμονής, αλλά εκεί δεν υπάρχει κάποιο αντίστοιχο SFR, σε κανένα από τα PPs, οποιοσδήποτε ο PPs που να καθοδηγεί τον εκτιμητή να κοιτάξει τι κάνει το κύκλωμα με αυτο.
2. Η σχέση μεταξύ των SFRs διαδραματίζει έναν σημαντικό ρόλο στον προσδιορισμό των σεναρίων επίθεσης ενάντια στα οποία το ολοκληρωμένο κύκλωμα πρέπει να υπερασπίσει το ίδιο. Οποιαδήποτε μέθοδος χρησιμοποιείται για να προστατεύσει τα στοιχεία που περνάνε κατά μήκος των buses προς κοινοποίηση, μπορεί να ανακαλυφθεί μόλις τα στοιχεία περάσουν από το IC, μέσω της I/O θύρας, του ολοκληρωμένου κυκλώματος δίνοντας στο μηχανισμό προστασίας, κατά ένα μεγάλο μέρος, απόβλητα του χρόνου Παραδείγματος χάριν, μόλις τροφοδοτηθεί η κάρτα, θα στείλει μια "απάντηση στην αναστοιχειοθέτηση" από την κάρτα. Αυτό είναι ανάλογο με μια σαφή επίθεση κειμένων στο σύστηματης κρυπτογραφίας.

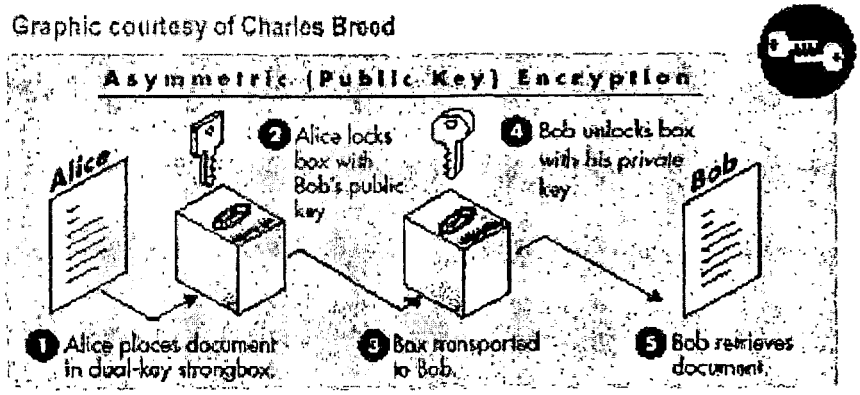
4.3. Αλγόριθμοι Κρυπτογράφησης

Υπάρχουν δυο είδη αλγορίθμων κρυπτογράφησης:

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



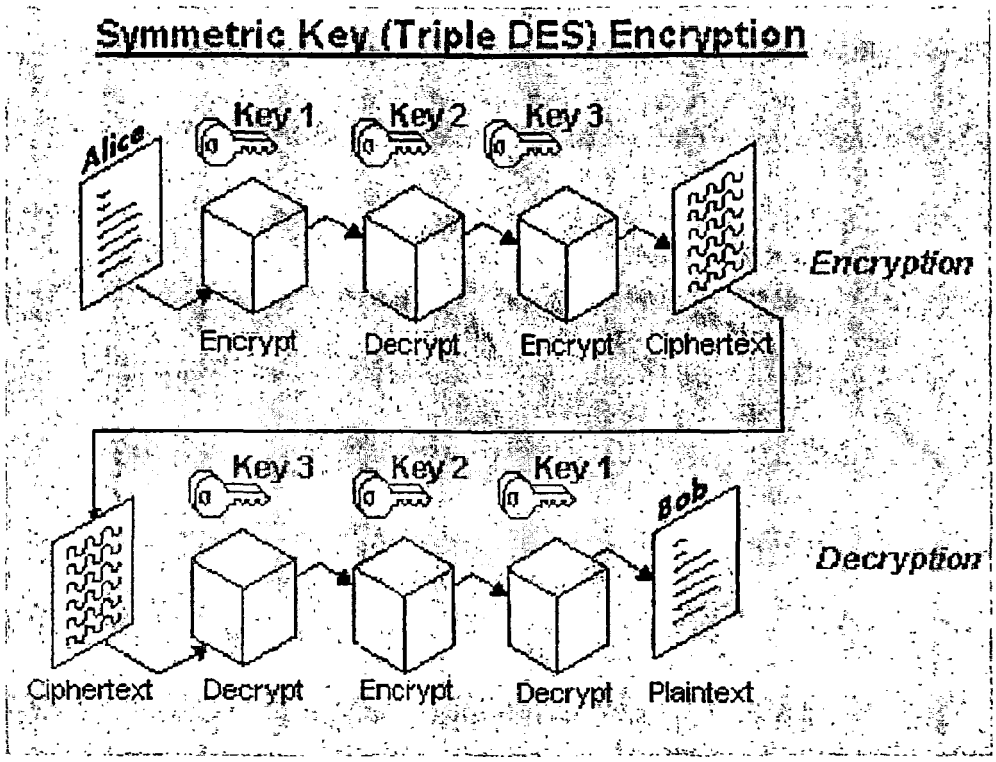
2. *Οι μη συμμετρικοί.* Ο πιο γνωστός μη συμμετρικός αλγόριθμος είναι ο RSA, που πήρε το όνομά του από τους δημιουργούς του (Rivest, Shamir, και Adleman). Ο RSA χρησιμοποιεί δύο κλειδιά, που ονομάζονται **private key**.



DES - Triple-DES

Ο αλγόριθμος DES δημιουργήθηκε από την IBM Corporation τη δεκαετία του 1970. Έχει μελετηθεί από πολλούς για περίπου 20 χρόνια, αλλά δεν έχει βρεθεί κάποιος τρόπος παραβίασής του. Ο αλγόριθμος DES έχει ένα κλειδί 56-bit, δηλαδή 256 πιθανές τιμές.

Ο Triple-DES είναι ένας αλγόριθμος που προσφέρει μεγαλύτερη ασφάλεια. Μπορεί να υλοποιηθεί με δύο ή τρία κλειδιά. Το παρακάτω διάγραμμα δείχνει την πορεία της κρυπτογράφησης σύμφωνα με τον αλγόριθμο Triple-DES με τρία κλειδιά.



4.4. Δυνατότητες Κρυπτογράφησης

Οι έξυπνες κάρτες που κυκλοφορούν στην αγορά σήμερα έχουν ικανοποιητικές ικανότητες κρυπτογράφησης, ώστε να υποστηρίζουν τις πιο δημοφιλείς εφαρμογές και πρωτόκολλα ασφάλειας.

Υπογραφές RSA και επαληθεύσεις υποστηρίζονται με κλειδιά (keys) μήκους 512, 768, ή 1024 bit. Οι αλγόριθμοι χρησιμοποιούν χαρακτηριστικά το θεώρημα Chinese Remainder Theorem (CRT) προκειμένου να επιταχυνθεί η επεξεργασία. Ακόμη και στην περίπτωση κλειδιού μήκους 1024 bit, ο χρόνος που απαιτείται για μια υπογραφή είναι χαρακτηριστικά κάτω από ένα δευτερόλεπτο. Συνήθως ο σχεδιασμός είναι τέτοιος ώστε το ευαίσθητο βασικό υλικό δεν φεύγει ποτέ από το chip. Ούτε ο κάτοχος καρτών δεν μπορεί να έχει πρόσβαση στο βασικό υλικό σε αυτήν την περίπτωση. Η χρήση του private key προστατεύεται από το PIN του χρήστη, έτσι ώστε η κατοχή της κάρτας να μην συνεπάγεται τη δυνατότητα να υπογράψει ο χρήστης με την κάρτα.

Ο ψηφιακός αλγόριθμος υπογραφών (Digital Signature Algorithm - DSA) εφαρμόζεται λιγότερο από τη RSA και συνήθως με μήκος κλειδιού 512 bit. Οι έξυπνες κάρτες υποστηρίζουν τη δυνατότητα πολλαπλών PINs που μπορεί να εξυπηρετούν διαφορετικούς σκοπούς. Χρησιμοποιούνται PINs που διαχειρίζονται τα PIN των χρηστών, με σκοπό την επίτευξη μεγαλύτερου επιπέδου ασφαλείας (π.χ. μπορεί να μπλοκάρει την κάρτα ύστερα από έναν καθορισμένο αριθμό αποτυχημένων προσπαθειών εισαγωγής PIN ή να επαν-αρχικοποιήσει την κάρτα). Χρησιμοποιούνται επίσης PINs για να ελέγξουν την πρόσβαση στα ευαίσθητα αρχεία ή τη διαχείριση ηλεκτρονικού πορτοφολιού.

Στις πιο σύγχρονες έξυπνες κάρτες χρησιμοποιούνται οι μέθοδοι κρυπτογράφησης DES και triple DES. Είναι δυνατό να χρησιμοποιηθούν σε μια λειτουργία Message Authentication Code (MAC). Βέβαια, επειδή ο σειριακός τρόπος επικοινωνίας με την έξυπνη κάρτα έχει χαμηλό εύρος ζώνης, η συμμετρική κρυπτογράφηση είναι πολύ αργή.

Προκειμένου να αποφευχθεί η αντιγραφή καρτών, ένας σταθερός (αμετάβλητος) σειριακός αριθμός (serial number) αποθηκεύεται συχνά στη μνήμη. Οι κάρτες σχεδιάζονται για να επαναρυθμίζονται αυτόματα μόνες τους μόλις ανιχνεύσουν μεταβολές στην τάση ή τη θερμοκρασία. Οι διαδικασίες ανάγνωσης ή εγγραφής της ROM είναι συνήθως απενεργοποιημένη.

Στις έξυπνες κάρτες συνήθως φιλοξενούνται και εφαρμογές ηλεκτρονικού πορτοφολιού, οι οποίες είναι βασισμένες σε συμμετρικές τεχνολογίες όπως DES και triple DES. Κατά συνέπεια, ένα μυστικό κλειδί (key) ευνοεί την ασφάλεια σε πολλές από αυτές τις εφαρμογές. Τα πρωτόκολλα επικοινωνιών των έξυπνων καρτών σε επίπεδο εντολών πολλές φορές ενσωματώνουν και πρωτόκολλο ασφάλειας. Αυτά είναι συνήθως βασισμένα σε συμμετρικές τεχνολογίες και επιτρέπουν στην ίδια την έξυπνη κάρτα να πιστοποιεί το τερματικό ανάγνωσης/ εγγραφής και αντίστροφα.

4.5 Χρήση Έξυπνων Καρτών για την ασφάλεια των δεδομένων

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

4.5.1. Σύστημα με Host-Based ασφάλεια

Ένα τέτοιο σύστημα αντιμετωπίζει την κάρτα ως ένα απλό μέσο μεταφοράς στοιχείων. Η ασφάλεια παρέχεται από τον host υπολογιστή. Τα δεδομένα της κάρτας μπορεί να είναι κρυπτογραφημένα, αλλά υπάρχει σημαντικός κίνδυνος κατά τη μεταφορά τους στον υπολογιστή. Η ασφάλεια σε αυτές τις περιπτώσεις μπορεί να αυξηθεί με τη χρήση έξυπνων καρτών που χρησιμοποιούν μηχανισμούς κωδικών πρόσβασης

για να αποτρέψουν την ανάγνωση των στοιχείων της κάρτας από άτομα που δεν έχουν το δικαίωμα αυτό. Δυστυχώς οι κωδικοί αυτοί είναι εύκολο να «εξουδετερωθούν». Αυτή η μεθοδολογία χρησιμοποιείται όταν κανείς εργάζεται τακτικά στα στοιχεία της κάρτας και μπορεί να παρακολουθεί τα περιεχόμενά της.

4.5.2. Σύστημα με Card -Based ασφάλεια

Στα συστήματα αυτά χρησιμοποιούνται έξυπνες κάρτες με μικροεπεξεργαστή. Το σύστημα αντιμετωπίζει την κάρτα ως συσκευή επεξεργασίας και η εξουσιοδότηση παρέχεται από το σύστημα ύστερα από αλληλεπίδραση μεταξύ host υπολογιστή και κάρτας. Κατά τη διαδικασία αυτή εξετάζεται αν η κάρτα μπορεί να παρέχει τα απαραίτητα πιστοποιητικά στο σύστημα, ώστε να μπορέσει να συνεχιστεί η συναλλαγή. Από την άλλη πλευρά και η ίδια η κάρτα μπορεί να ζητήσει την ίδια επιβεβαίωση από το host υπολογιστή. Έτσι λοιπόν η πρόσβαση σε πληροφορίες της κάρτας ελέγχεται α) από το Λειτουργικό Σύστημα που υπάρχει στο εσωτερικό της κάρτας, αλλά και β) τις άδειες που έχει ορίσει ο εκδότης της κάρτας.

5. Συμπεράσματα και Προτάσεις Στρατηγικής

5.1. Γενικοί άξονες (Προτάσεις προς την πολιτεία)

Οι έξυπνες κάρτες επιλέγονται διεθνώς σαν ένα ασφαλές μέρος των υποδομών ασφάλειας των πληροφοριακών συστημάτων και ιδιαίτερα σαν μέσο πρόσβασης σε ανοικτά δίκτυα. Οι κλάδοι των Τραπεζών και της Κινητής Τηλεφωνίας έχουν επενδύσει και επενδύουν δισεκατομμύρια ευρώ ενώ οι νέοι χρήστες είναι οι Οργανισμοί Μαζικών Συγκοινωνιών και ο Δημόσιος Τομέας για μια σειρά εφαρμογών.

Στην Ευρώπη αλλά και στις ΗΠΑ και την Ιαπωνία, οι αρμόδιοι κυβερνητικοί φορείς υλοποιούν μεγάλης κλίμακας έργα με έξυπνες κάρτες και προωθούν την έρευνα και ανάπτυξη σε παρεμφερείς συμπληρωματικές τεχνολογίες όπως την βιομετρική.

Στην Ελλάδα εκτός από τους Τηλεπικοινωνιακούς φορείς δεν έχουν γίνει μαζικές επενδύσεις. Μάλιστα η μεγάλη επιτυχία των τηλεκαρτών στην Ελλάδα κατά την τελευταία δεκαετία οδήγησε στην κατασκευή τριών εργοστασίων τα οποία προσβλέπουν σε αναδυόμενες αγορές.

Η Ομάδα Εργασίας του e-business forum, του Υπουργείου Ανάπτυξης, κατόρθωσε να συγκεντρώσει για πρώτη φορά όλους τους άμεσα ενδιαφερόμενους χρήστες, ερευνητές και προμηθευτές έξυπνων καρτών στο πλαίσιο της ενημέρωσης και ανταλλαγής απόψεων.Η Ομάδα Εργασίας προτείνει ομόφωνα να συνεχιστεί η προσπάθεια αυτή μέσα από:

1. Την δημιουργία μιας μη-κερδοσκοπικής εταιρίας Έξυπνων Καρτών που θα συγχρηματοδοτείται από τον ιδιωτικό και Δημόσιο Τομέα. Ο σκοπός αυτής της ομάδας είναι να επεξεργαστεί ζητήματα που αφορούν:

- ✓ Την εκπαίδευση προσωπικού σε αυτές τις τεχνολογίες σε συνεργασία με Ακαδημαϊκά Ιδρύματα
- ✓ Την προώθηση της έρευνας και ανάπτυξης
- ✓ Την εξασφάλιση του νομικού και θεσμικού πλαισίου που εναρμονίζεται με το Ευρωπαϊκό

- ✓ Την εξασφάλιση διαλειτουργικότητας των υποδομών των διαφόρων κλάδων
- ✓ Την διερεύνηση κοινών επενδύσεων διαφόρων κλάδων
- ✓ Την ευθυγράμμιση με τις Ευρωπαϊκές πρωτοβουλίες όπως έχουν εξελιχθεί μετά την δημοσίευση της Ανοικτής Υποδομής Έξυπνων Καρτών για την Ευρώπη στα πλαίσια της πρωτοβουλίας e-Europe.
- ✓ Την προσπάθεια προώθησης λύσεων σε γειτονικές χώρες

2. Την διοργάνωση **Ελληνικού Συνεδρίου (πιθανόν και έκθεσης προϊόντων και εφαρμογών) smart cards** που θα επαναλαμβάνεται σε ετήσια βάση.

3. Την προετοιμασία **πρότασης Ελληνικού Roadmapping Ερευνητικού Project,** πιθανόν στο πλαίσιο του επερχόμενου προγράμματος e-business της ΓΓΕΤ. Το έργο πρέπει να περιλαμβάνει όλους τους «παίκτες» της Ελληνικής αγοράς (Ακαδημαϊκά & Ερευνητικά Ιδρύματα, Βιομηχανίες καρτών και readers, εταιρείες ανάπτυξης λογισμικού, consultants). Στόχοι του έργου θα πρέπει να είναι :

- ✓ Smart cards technology foresight για την επόμενη 5-ετία
- ✓ Smart cards business development foresight για την επόμενη 5-ετία
- ✓ Αναγνώριση αναγκών σε έρευνα για την ανάπτυξη της Ελληνικής βιομηχανίας έξυπνων καρτών
- ✓ Αναγνώριση αναγκών σε υποδομές και δομές για την υποστήριξη της επιχειρηματικότητας της Ελληνικής βιομηχανίας έξυπνων καρτών
- ✓ Καθορισμός μέτρων για την κάλυψη των παραπάνω αναγκών.
- ✓ Πιλοτικές προσπάθειες ανάπτυξης Τεχνολογίας και εφαρμογών για την επικύρωση των παραπάνω αποτελεσμάτων

5.2. Προτάσεις για τον Δημόσιο Τομέα

Στην πρώτη συνάντηση της Ομάδας Εργασίας που αφορούσε στον Δημόσιο Τομέα πήραν μέρος εκπρόσωποι από 8 Υπουργεία και Οργανισμούς. Υπάρχει ενδιαφέρον για την τεχνολογία αυτή και ελλείψει εξοικείωσης των χρηστών αλλά και των τεχνολόγων υπάρχει κίνδυνος σπατάλης πόρων για μελέτη και ανάπτυξη ξεχωριστών συστημάτων μη συνεργάσιμων ή για επικαλύψεις. Είναι χαρακτηριστικό ότι οι κάρτες διοδίων της Αττικής Οδού και του Ταμείου Εθνικής Οδοποιίας δεν συνεργάζονται.

Η πρόταση για την δημιουργία ενός οργάνου που θα συντονίζει την ανάπτυξη των υποδομών και την έκδοση των καρτών μπορεί να αποτρέψει τέτοιου είδους περιττές σπατάλες. Ταυτόχρονα μπορεί να δημιουργηθεί για τον σκοπό αυτό - στα πλαίσια του οργάνου αυτού - μια επιτροπή για τις ανάγκες αποκλειστικά του δημοσίου τομέα.

Ήδη σε Ευρωπαϊκό επίπεδο - και με υπό ένταξη κράτη - υπάρχει ικανοποιητικός συντονισμός ανάλογων πρωτοβουλιών: Η Ομάδα Porvoo που συγκεντρώνει 15 χώρες και έχει σκοπό την διευρωπαϊκή Ηλεκτρονική Ταυτότητα, το επιδοτούμενο από την Ευρωπαϊκή Επιτροπή έργο eEpoch, η πρωτοβουλία eEurope Smart Cards και άλλες που ασχολούνται με ιδιαίτερες εφαρμογές όπως την κάρτα E-111 κτλ.

Το προτεινόμενο όργανο θα μεριμνά ώστε να υπάρχει Ελληνική συμμετοχή και δραστηριοποίηση σε όλες τις σχετικές πρωτοβουλίες και παράλληλος συντονισμός μεταξύ των πρωτοβουλιών αυτών. Ιδιαίτερα να υπάρχει συμμετοχή με αυτοχρηματοδότηση του Ελληνικού Υπουργείου Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης στο έργο eEpoch.

Ένα ιδιαίτερα σημαντικό θέμα είναι η μεταφορά της τεχνογνωσίας που έχει αναπτυχθεί διεθνώς στην δημόσια διοίκηση. Αυτό μπορεί να επιτευχθεί μέσα από μιασειρά σεμιναρίων, ημερίδων κτλ αλλά, και ιδιαίτερα, μέσα από ορισμένα πιλοτικά προγράμματα που πρέπει να υλοποιηθούν σε τοπικό επίπεδο ώστε να αποκτηθεί ιδία εμπειρία.

5.3. Ενημέρωση και Ευαισθητοποίηση

Τα πορίσματα της Ομάδας Έξυπνων Καρτών, μαζί και τα παραδοτέα του eEuropev Smart Cards, μπορούν και πρέπει να προωθηθούν σε όλους του ενδιαφερόμενους. Αποτελούν την καταγραφή των πιο έγκυρων πληροφοριών, Λευκών Βίβλων, προτάσεων και προδιαγραφών στην Ελλάδα και την Ευρώπη. Η προώθηση και προβολή πρέπει να είναι από τα πρώτα μελήματα του προτεινόμενου οργάνου.

Τεχνικά Θέματα - Πρότυπα

Στο παραδοτέο για την Ανοικτή Υποδομή Έξυπνων Καρτών για την Ευρώπη που εκπονήθηκε στα πλαίσια της πρωτοβουλίας e-Europe, υπάρχει αναλυτική αναφορά τόσο στα βασικά Τεχνικά Θέματα όσο και στα Πρότυπα, και τις νέες ανάγκες προτυποποίησης. Στην πρωτοβουλία συμμετείχαν και συμμετέχουν ενεργητικά τα βασικά Κέντρα Προτυποποίησης όπως: το CEN/ISSS και ETSI, ενώ πολλοί ειδικοί συμμετέχουν σε επιτροπές ISO. Δεδομένου ότι η συμμετοχή της χώρας μας είναι περιορισμένη - μόνο δύο άτομα συμμετέχουν στις επιτροπές του eEurope Smart Card Charter και ο Ελληνικός Οργανισμός Τυποποίησης δεν συμμετέχει στις επιτροπές προτύπων έξυπνων καρτών, θα πρέπει να προωθηθεί η σχετική πληροφόρηση στους εμπλεκόμενους φορείς.

6. Παρουσίαση του GCR680

6.1. Εισαγωγή

Πολλές μεγάλες εταιρείες, ανάμεσα τοθς και αρκετές ελληνικές, έχουν αναπτύξει τεχνολογία έξυπνων καρτών, ώστε να ικανοποιηθούν οι ανάγκες των πελατών τους. Σ' αυτό το κεφάλαιο, γίνεται η παρουσίαση του GCR680 της GEMPLUS, για να γίνει πιο κατανοητή η φιλοσοφία της ανάγνωσης καρτών. Παρόλα αυτά υπάρχουν επιπλέον και αρκέτες σημαντικές επιχειρήσεις με παρόμοια ή και πιο εξελιγμένα μηχανήματα ανάγνωσης καρτών.

Ο GEMPLUS CARD READER 680 (GCR680) είναι ένας αναγνώστης καρτών για τις GEMPLUS contactless κάρτες GCR680. Ο GCR680 δεν συμπεριλαμβάνει όλα τα χαρακτηριστικά του GCI400 hardware, παρόλα αυτά το firmwire του, περιλαμβάνει OROS εντολές και το GCR680 -συγκεκριμένο ROS680 που υποστηρίζει τις σχετικές GCR680 εντολές.

Όταν λειτουργήσει το GCR680, είναι σε θέση να διερμηνεύσει είτε OROS εντολές, οι οποίες περιγράφονται στο GCI400 reference guide είτε τις ROS608εντολές που αρμόζουν στην χρήση των GCL8K καρτών.

6.2. Διαμορφώνοντας τον GCR680

Στον GCR680 είναι προκαθορισμένη η ακόλουθη διαμόρφωση (το ακόλουθο configuration):

- 8-bits
- no parity
- 9600 Baund
- ROS680 εντολές σε ισχύ

Μπορεί να γίνει τροποποίηση σε κάθε μία από αυτές τις τιμές, κάνοντας χρήση Cofigure SIO Line εντολής (περισσότερα στη σελ.)

6.3. Πρωτόκολλα GCR680

Όλες οι μεταδόσεις με τον GCR680 γίνονται με βάση τρία επίπεδα πρωτοκόλλων:

- Το επίπεδο εντολών
- Το επίπεδο μετάδοσης
- Το φυσικό επίπεδο

Το *επίπεδο εντολών,* χειρίζεται τις διερμηνείες των εντολών GCR680. αυτές μπορεί να είναι είτε ROS680 είτε OROS εντολές. Περιέχει τον κώδικα εντολών, δεδομένα και παραμέτρους.

Το *επίπεδο μεταφοράς,* χειρίζεται την διευθυνσιοδότηση των μηνυμάτων, συγκεκριμενοποιεί τον τύπο της μεταφοράς και αξιολογεί (validates) κάθε μεταφορά.

Το *φυσικό επίπεδο,* χειρίζεται την ίδια την μετάδοση δεδομένων. Το GCR680φυσικό επίπεδο, χρησιμοποιεί και το RS-232 πρωτόκολλο.

Οι επόμενες παράγραφοι περιγράφουν με μεγαλύτερη λεπτομέρεια τα επίπεδα εντολών.

6.4. Command layer

Το επίπεδο εντολών χειρίζεται και διερμηνεύει τις εντολές. Αυτέςμπορεί να είναι είτε ROS680 είτε OROS εντολές. Αποτελείται από τον κώδικα εντολών, τα δεδομένα και τις παραμέτρους.

Οι εντολές μπορούν να σταλθούν στο GCR680 με την ακόλουθη μορφή (format):

|CommCode | Parameters | Data|

όπου:
CommCode → κώδικας εντολών

Parameters → οι παράμετροι που στέλνονται με τις εντολές
Data → τα δεδομένα που ακολουθούν την εντολή, όπου χρειάζεται.

Το τμήμα του GCR680 interface εντολών, ξεκινάει με την σελίδα **"Error! Bookmark not defined"**, περιγράφει το CommCode, τις παραμέτρους και το Data field Values για κάθε εντολή.

Ο GCR680 απαντάει σε κάθε εντολή που λαμβάνει, με ένα status code, το οποίο έχει την ακόλουθη μορφή:

|S | Data|

όπου:
S → status code identifier
Data → τα δεδομένα που επιστρέφονται με το status code, όπου αυτό χρειάζεται.

Στο παράρτημα 7.4. υπάρχει λίστα με τα status code και τις παραμέτρους τους

6.5. Transport layer

Το επίπεδο μεταφοράς χειρίζεται την διευθυνσιοδότης των μηνυμάτων, συγκεκριμενοποιεί τον τύπο μεταφοράς και αξιολογεί (validates) κάθε μεταφορά. Το TLP224 επίπεδο μεταφοράς χρησιμοποιεί είτε το TLP224 ή το GEMPLUS Block protocol.

6.5.1. TLP224

Η διαδικασία του TLP224 πρωτοκόλλου περιλαμβάνει δύο βήματα:

Το πρώτο βήμα είναι η δόμηση του μηνύματος που πρόκειται να μεταδοθεί. Κ άτω από το TLP224, το GCR680 και το σύστημα του host, ανταλλάσσουν πληροφορίες (tranmissions) με την ακόλουθη μορφή:

Για την μετάδοση μηνυμάτων χωρίς λάθη:

<ACK> <LN> <MESSAGE> <LRC>

όπου:

ACK → 60h, υποδεικνύει ότι η προηγούμενη εντολή ή το status code μεταδόθηκε χωρίς λάθος.

LN → μέγεθος μηνύματος (εντολής ή status code)

MESSAGE → εντολή ή status code

LRC → το αποτέλεσμα από ένα EXCLUSIVE OR (XOR) ανάμεσα στους χαρακτήρες ACK, LN, και MESSAGE.

Όταν εμφανίζεται ένα λάθος στη μετάδοση:

<NACK> <LN> <LRC>

όπου:

NACK → E0h, υποδεικνύοντας ότι υπήρχε λάθος.

LN → 00

LRC → E0

Κατά τη διάρκεια του δεύτερου βήματος η πηγή ακολουθεί την εξής διαδικασία:

- Αντιστρέφει (converts) κάθε byte που πρόκειται να μεταδοθεί σε δύο ASCII χαρακτήρες. Για παράδειγμα, για να μεταδοθεί

ένα byte 3Ah και 41h. αυτό αποτρέπει άλλον εξοπλισμό να επέμβει στους χ

α	ACK	LEN	Message	CRC	EOT
Command	60	01	4D	2C	
TLP πρωτόκολλο μεταφορά τ ή ρ ες ελέγχου.	36 30	30 31	34 44	32 43	03

➢ Προσθέτει ένα End Of Transmission (EOT) byte κατά το τέλος της μετάδοσης. Αυτή είναι η τιμή 03h.

Για παράδειγμα, για την μετάδοση της εντολής κλεισίματος (power down) κάτω από το TLP224 πρωτόκολλο, το οποίο έχει τον κώδικα εντολής 4Dh και καθόλου παραμέτρους, η ακόλουθη συχνότητα, θα πρέπει να μεταδοθεί:

Το time out ανάμεσα σε κάθε χαρακτήρα, είναι 100ms.

6.5.2. *GEMPLUS Block Protocol*

Το GEMPLUS Block Protocol (GBP) είναι μια απλοποιημένη έκδοση του T=1 card protocol. Κάτω από το GBP τα δεδομένα μεταδίδονται, ανάμεσα στην πηγή και τον προορισμό σε blocks.

Υπάρχουν τρεις τύποι block:

- I-Blocks. (Information blocks). Τα I-Blocks κρατούν τα δεδομένα που πρόκειται να ανταλλαχθούν ανάμεσα στην πηγή και τον προορισμό.

- R-Blocks (Receive Ready Block), τα οποία συγχρονίζουν τις μεταδόσεις ανάμεσα στην πηγή και τον προορισμό.

- S-Blocks (Supervisory Block). Τα block εποπτείας συγχρονίζουν τις μεταδόσεις ανάμεσα στη πηγή και τον προορισμό.

  Το GCR680 και ο host ανταλλάσσουν GBP blocks σύμφωνα με την ακόλουθη μορφή:

NAD	PCB	LEN	DAT	EDC

όπου:

NAD → είναι ο identifier της πηγής κα του προορισμού σε ένα byte με την ακόλουθη μορφή:

7	6	5	4	3	2	1	0

7-4 → destination identifier (πηγής)
3-0 → source identifier (προορισμού)

Ο GCR680 identifierείναι το 4, ενώ ο identifier του συστήματος του host είναι το 2.

Το PDB αναγνωρίζει τον τύπο του block. Η μορφή του, εξαρτάται από τον τύπο block, όπως περιγράφεται παρακάτω:

Το I-Block PCBs έχει την ακόλουθη μορφή:

Bit

7	6	5	4	3	2	1	0
0	S	0					

4-0→ δεν χρησιμοποιούνται
S → Bit συχνότητας

Το Bit συχνότητας μηδενίζεται στο σύστημα του host ή "GCR680 power up". Η πηγή στέλνει το πρώτο I-Block το οποίο μεταδίδει με το bit της συχνότητας ρυθμισμένο στο 0. Αυξάνει το bit της συχνότητας κατά 1 κάθε φορά που στέλνει ένα block πληροφοριών ο GCR680 και το σύστημα του host, παράγουν τιμές για τα bit συχνότητας ανεξάρτητα.

Το R-Block PCBs έχει την ακόλουθη μορφή:

Bit

7	6	5	4	3	2	1	0
1	0	0	S	0	0	E	V

S → 1= έχει εξακριβωθεί λάθος από το EDC
E→ 1= ένα λάθος εντοπίστηκε
V→ 1=ο αριθμός της συχνότητας που εντοπίστηκε το λάθος

Το S-Block ζητάει τον προορισμό για να μηδενίσει τα bit των συχνοτήτων και να επιστρέψει μία απάντηση στην πηγή που υποδεικνύει ότι η απάντηση έχει ολοκληρωθεί.

Τα S-Block PCBs έχουν την ακόλουθη μορφή:

Bit

7	6	5	4	3	2	1	0
1	1	0	0	0	0	0	0

Resynch αίτηση

Bit

7	6	5	4	3	2	1	0
1	1	0	0	0	0	0	0

Resynch επικόλληση

Το LEN συγκεκριμενοποιεί, σε ένα Byte τον αριθμό των Bytes στο INF πεδίο.

Το DAT κρατάει τα δεδομένα που μεταδίδονται.

Το EDC είναι το αποτέλεσμα του αποκλειστικού OR που παρουσιάζεται στα NDA, PCB, LEN και DAT bytes.

6.6. Phisical Layer : {φυσικό επίπεδο}

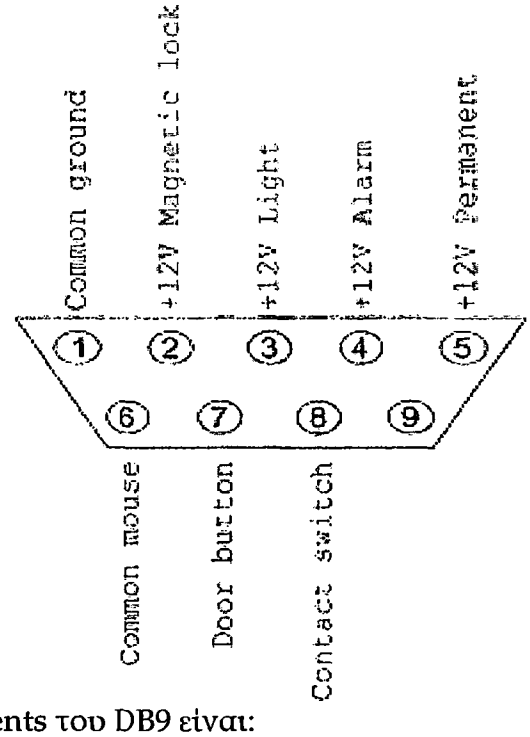
Το φυσικό επίπεδο διαχειρίζεται την ίδια την μετάδοση δεδομένων. Το φυσικό επίπεδο του GCR680 χρησιμοποιεί το RS-232 πρωτόκολλο.

RS-232 πρωτόκολλο

Το RS-232 μπορεί να στέλνεται απευθείας στον σειριακό DB9 αρσενικό σύνδεσμο του GCR680.

Τα bytes στέλνονται πάνω σε μία γραμμή με ένα UART του οποίου τα χαρακτηριστικά μετάδοσης (τόσο η ταχύτητα όσο και το parity είναι determined από το configuration του GCR680.

Το ακόλουθο διάγραμμα δείχνει το pin configuration του DB9 connector –a.



Τα pin assignments του DB9 είναι:

PX- pin3

Tx – pin2

GRD – pin5

Τα υπόλοιπα pins είναι για μελλοντική χρήση και δεν τα συνδέουμε.

6.7. GCR680 εντολές interface

Αυτό το κεφάλαιο παρέχει κάποιες πληροφορίες υποβάθρου για τις λειτουργίες ελέγχου του GCR680 και περιγράφει τις GCR680 εντολές. Για κάθε εντολή περιγράφει:

- Τις λειτουργίες που κάνει.
- Την σύνταξη του.
- Τα δεδομένα που επιστρέφει.

Οι εντολές GCR680είναι συμβατές με τις Open Reader Operating System (OROS – σύστημα λειτουργίας open reader) εντολές.

6.7.1. Εισαγωγή στις εντολές ελέγχου GCL8K

Μία από τις δυνατότητες του κλειδιού του GCL8K είναι η ικανότητα του reader να χειρίζεται μεταδόσεις (transactions), όταν πολλαπλές μεταδόσεις είναι στον χώρο της κεραίας.

Η αρχή της λειτουργίας των πολλαπλών καρτών βασίζεται στην ικανότητα του GCR680, να προσδιορίσει και να επιλέξει μία επιστρέφοντας τον σειριακό της αριθμό. Η εφαρμογή μπορεί μετά να κάνει έλεγχο της κάρτας χρησιμοποιώντας συγκεκριμένες εντολές και ενδεχομένως να μεταβεί σε άλλη κάρτα εκτελώντας μία άλλη "pick up" συχνότητα.

Η λειτουργία διαχείρισης της πολλαπλής κάρτας GCR680, είναι προσβάσιμη είτε με ένα υψηλό επίπεδο εντολών ελέγχου της κάρτας ή με χαμηλό επίπεδο εντολών, σχετιζόμενες απευθείας με το ASIC interface που ελέγχει την επικοινωνία ανάμεσα στον reader και των καρτών.

Οι εντολές υψηλού επιπέδου είναι:

- Reset
- Get Card
- Get First Card

Οι εντολές χαμηλού επιπέδου είναι:

- Request
- Request All
- Anticollision
- Select
- Request All & Select
- Halt

Οι εφαρμογές πρόσβασης στην μνήμη του GCR680 χρησιμοποιούν την εντολή Exchange APDU. Αυτή η εντολή μεταγλωττίζει (compiles) μαζί με το ISO7816-3-4 πρωτόκολλο.

Είναι δυνατή η ανάπτυξη εφαρμογών, χρησιμοποιώντας είτε υψηλού είτε χαμηλού επιπέδου εντολών ελέγχου της κάρτας. Οι υψηλού επιπέδου εντολές, είναι πιο απλές στον χειρισμό (implement) και συμβατές με τις υπάρχουσες GEMPLUS εφαρμογές επικοινωνίας καρτών.

6.7.2. *Κάνοντας χρήση των εντολών υψηλού επιπέδου*

Οι υψηλού επιπέδου, ελέγχου της κάρτας, εντολές GCL8K είναι:

- Reset
- Get Card
- Get First Card

Η εντολή Reset, κάνει reset τις περισσότερες μεταβλητές που είναι αποθηκευμένες στον GCR680 και επιστρέφει σε ένα γνωστό state (κατάσταση), με σεβαστές επικοινωνίες ανάμεσα στον GCR680 και τις GCL8K κάρτες. Η εντολή Reset επίσης κάνει reset σε όλες τις κάρτες GCL8K, οι οποίες είναι στο πεδίο της κεραίας (κάνοντας reset στις κάρτες τις επιστρέφει σε κατάσταση "Home State"), μετά το reset ο GCR680 δεν αναγνωρίζει τις GCL8K κάρτες που βρίσκονται στο πεδίο της κεραίας.

Η εντολή Get Card εμφανιζόμενη μετά την Reset, επιλέγει την πρώτη GCL8K που εντοπίζει στο πεδίο. Οι ακόλουθες Get Card εντολές επιλέγουν τις άλλες κάρτες που παρουσιάζονται στο πεδίο, μία προς μία, μέχρι να μην υπάρχουν άλλες διαθέσιμες κάρτες και όλες τους να είναι "scanned" από την συχνότητα των εντολών Get Card .

Όπως μία αναλογία με την ISO7816-3-4 κάρτα ελέγχου, το multiple Get Card μπορεί να θεωρηθεί σαν μία σειρά από συχνότητες Warm Reset μέσα στο ίδιο session πιάνοντας διαφορετικά λειτουργικά modes από μία μοναδική κάρτα, σε περίπτωση των καρτών επικοινωνίας. Οι GCR680/GCL8K Get Card εντολές, επιλέγουν άλλες κάρτες, σαν αναλογία σε άλλα modes.

Ανά πάσα στιγμή η διαδικασία σκαναρίσματος GCL8K, μπορεί να γίνει reset εκτελώντας μία εντολή Reset. Όλες οι κάρτες είναι Reset και μια Get Card συχνότητα, μπορεί να ενεργοποιήσει την εφαρμογή για να γίνει re-scan σε όλες τις GCL8K που βρίσκονται στο πεδίο της κεραίας.

Όταν γίνεται ανάπτυξη των GCL8K εφαρμογών, θα πρέπει να συνυπολογίζονται οι ακόλουθοι κανόνες:

- Η εντολή Reset, θα πρέπει να εκτελεστεί ακόμα και όταν δεν έχουν σκαναριστεί όλες οι κάρτες.

- Η σειρά επιλογής των καρτών, μπορεί να διαφέρει στις διαφορετικές συχνότητες σαρώματος.
- Μία κάρτα, μπορεί να εμφανιστεί δύο φορές κατά τη διάρκεια του σαρώματος. Αυτό σημαίνει ότι έχει γίνει reset στη κάρτα επειδή έγινε έξοδος και επανείσοδος της κάρτας στην περιοχή της κεραίας.
- Όταν δεν θα μπορούν να επιλέγουν άλλες κάρτες στην συχνότητα του σαρώματος, η εντολή Get Card επιστρέφει ένα συγκεκριμένο κώδικα. Σ' αυτή την περίπτωση, η Get Cardεντολή μπορεί να εκτελεστεί περιστασιακά και μετά να προσδιοριστεί και να επιλέξει ό,τι καινούριες κάρτες έχουν εισέλθει στο πεδίο της κεραίας ή όποια κάρτα στην οποία έχει γίνειreset, εξαιτίας της εξόδου και επανεισόδου της, στο πεδίο της κεραίας.

Για να γίνει πιο απλή η συχνότητα του σαρώματος, μία Get First Card εντολή περιλαμβάνεται στις εντολές ROS680. αυτή η εντολή, είναι παρόμοια με μια εντολή Reset, ύστερα από μία Get Card εντολή. Όλοι οι παραπάνω κανόνες εφαρμόζονται όταν γίνεται χρήση της Get Card εντολής, αφού κάνει reset στην GCL8K, στην διαδικασία σαρώματος και ταυτόχρονα προσδιορίζει και επιλέγει την "First Card".μια συχνότητα σαρώματος, παρόλα αυτά, αποτελείται από μια Get First Card εντολή, ακολουθούμενη από πολλαπλές Get Card εντολές.

6.7.3. Διάκριση της δομής των εντολών

Διάκριση της δομής των GCR680 εντολών:

- Configure SIO Line
- Read OROS Firmware Version
- Read ROS680 Firmware Version

Παρακάτω παρουσιάζονται αναλυτικά αυτές οι εντολές.

Configure SIO Line

Αυτή η εντολή θέτει τι SIO line parity, Baud rate, and number of bits per character.

Μετά το άνοιγμα, "power up" the line defaults to no parity, 8 bits per character and 9600 Baud.

Σημείωση: Η γραμμή ανασυντάσσεται μόλις η εντολή εκτελεστεί, γι' αυτό το γεγονός ότι το GCR680 χρησιμοποιεί το καινούργιο configuration (την καινούρια διαμόρφωση) υποδεικνύει ότι η εντολή ήταν επιτυχημένη.

Read OROS Firmware Version

Επιστρέφει το version από το OROS Firmware που έχει εγκατασταθεί στο GCR680.

FORMAT
22h 05h 3fh f0h 10h

RESULT
S Version

Όπου: Version → το εγκατεστημένο OROS Version σε ASCII.

Read ROS680 Firmware Version

Επιστρέφει το το version από το ROS680 Firmware που έχει εγκατασταθεί στο GCR680.

FORMAT
E1h FFh

RESULT
S Version

Όπου: Version → το εγκατεστημένο ROS680 Version σε ASCII.

6.7.4. GCR680 Interface Εντολών

Υψηλού Επιπέδου Εντολές Ελέγχου GCR680:

- Reset
- Get Card
- Get First Card

Χαμηλού Επιπέδου Εντολές Ελέγχου GCR680:

- Request
- Request All
- Anticollision

- Select
- Request All & Select
- Halt

GCR680 Εντολές Πρόσβασης στη μνήμη:

- Exchange APDU

Security Module ASIC Command (εντολές ασφάλειας του Module ASIC)

- Exchange APDU
- Load Key

Έλεγχος Λειτουργίας GCR680

- RF On
- RF Off

Οι επόμενοι παράγραφοι περιγράφουν αυτές τις εντολές.

Reset

Κάνει Reset σε όλες τις κάρτες που είναι στην περιοχή της κεραίας, επιστρέφοντας αυτές σε"home state" και κάνει Reset στον GCR680. αυτή η εντολή δίνει την δυνατότητα για restart του πολλαπλού GCL8K scanning sequence που περιέχει διαδοχικές Get Card εντολές.

FORMAT
E1h

RESULT
S
Η εντολή Reset εκτελείται πάντα χωρίς λάθη.

Get Card

Την πρώτη φορά που εκτελείται μια εντολή Get Card, μετά από ένα Reset, ο GCR680 κάνει reset σε όλες τις κάρτες, μέσα στην περιοχή της κεραίας και επιλέγει την πρώτη κάρτα που εντοπίζει. Είναι πανομοιότυπο με το ακόλουθο sequence των, χαμηλού επιπέδου, εντολών:

- Request All
- Anticollision
- Select

Όλες οι ακόλουθες Get Card εντολές (έχοντας υπόψη ότι η Reset εντολή δεν εκτελείται ανάμεσα σ' αυτές), βάζουν την επιλεγμένη κάρτα σε κατάσταση sleep mode, σαρώνει όλες τις κάρτες στο πεδίο της κεραίας και ύστερα επιλέγει μία νέα κάρτα. Σ' αυτή την περίπτωση, ο GCR680 εκτελεί το ακόλουθο sequence του χαμηλού επιπέδου εντολών:

- Halt
- Request
- Anticollision
- Select

Αυτή η εντολή επιστρέφει τον τύπο της κάρτας και ένα σειριακό αριθμό από το block0 του sector1 της κάρτας που είναι επιλεγμένη στο standard ISO 7816-3 ATR format:

FORMAT

E2h [00 tt]

Όπου:

tt= ζητά ένα non-response timeout σε hundreds of ms. Η τιμή 0 καθορίζει μία 25.6 δεύτερη timeout περίοδο. Ο GCR680 εκτελεί τη εντολή Request All, μέχρι είτε να βρει μια κάρτα είτε το non-response timeout λήξει.

RESULT

S <card response>

Όπου:

<card response> → |TS| T0 | TD |Historical characters|

όπου:

TS → 3Bh

T0 → 87

TD → 01

Historical Characters → 04 00 sn sn sn sn 08

04 00, είναι ο Tag Type (0004)

sn sn sn sn, είναι ένας σειριακός αριθμός των 4-byte

08, είναι το μέγεθος του chip.

Get First Card

Κάνει reset στον GCR680, εκτελεί το anticollision sequence, επιλέγει την πρώτη κάρτα μέσα στο πεδίο της κεραίας που αποκρίνεται.

Επιστρέφει τον τύπο της κάρτας και έναν σειριακό αριθμό από το block0 του sector1 της κάρτας που είναι επιλεγμένη στο standard ISO 7816-3 ATR format. Αυτό το sequence εντολής, είναι το ίδιο με την εκτέλεση του ακόλουθου sequence του χαμηλού επιπέδου εντολών:

- Request
- Request All
- Anticollision
- Select

Ή του υψηλού επιπέδου εντολών του ακόλουθου sequence :

- Reset
- Get Card

FORMAT

E2h [00 tt]

Όπου:

tt= ζητά ένα non-response timeout σε hundreds of ms. Ο GCR680 εκτελεί τη εντολή Request All, μέχρι είτε να βρει μια κάρτα είτε το non-response timeout λήξει.

RESULT

S <card response>

Όπου:

<card response> → |TS| T0 | TD |Historical characters|

όπου:

TS → 3Bh

T0 → 87

TD → 01

Historical Characters → 04 00 sn sn sn sn 08

04 00, είναι ο Tag Type (0004)

sn sn sn sn, είναι ένας σειριακός αριθμός των 4-byte

08, είναι το μέγεθος του chip.

REQUEST

Υπαγορεύει τις κάρτες που είναι στο πεδίο της κεραίας και δεν βρίσκονται σε sleep mode και επιστρέφει τον τύπο τους.

FORMAT

E2h 10h

RESULT

S 00 04

REQUEST ALL

Υπαγορεύει τις κάρτες που είναι στο πεδίο της κεραίας και επιστρέφει τον τύπο τους.

FORMAT
E2h 10h

RESULT
S 00 04

ANTICOLLISON

Ανακτά τον σειριακό αριθμό μιας κάρτας από αυτές που είναι στο πεδίο της κεραίας.

FORMAT
E2h 12h

RESULT
S <card response>
Όπου:
<card response> → |TS| T0 | TD |Historical characters|
όπου:
TS → 3Bh
T0 → 87
TD → 01
Historical Characters → 04 00 sn sn sn sn 08
04 00, είναι ο Tag Type (0004)
sn sn sn sn, είναι ένας σειριακός αριθμός των 4-byte
08, είναι το μέγεθος του chip.

SELECT

Επιλέγει την κάρτα στην οποία στέλνονται οι διαδικαστικές εντολές. Θα πρέπει να εκτελεστεί τα διάβασμα ή το γράψιμο στην κάρτα. Η επιλεγμένη κάρτα επιστρέφει το μέγεθος της μνήμης της .

FORMAT

E2h 13h xx xx xx xx

Όπου: xx xx xx xx, είναι ο σειριακός αριθμός της κάρτας που έχει επιλεχθεί.

RESULT

S 08

Request All & Select

Υπαγορεύει κάρτες μέσα στο πεδίο της κεραίας για να επιστρέψει τον τύπο του αναγνωριστικού αριθμού της κάρτας και επιλέγει την συγκεκριμένη κάρτα. Αυτή η εντολή μπορεί είτε να επιδράσει σε όλες τις κάρτες είτε μόνο σε όσες δεν βρίσκονται σε κατάσταση sleep mode. Όλες οι κάρτες σε sleep mode, επιστρέφουν σε sleep mode αφού επιστρέψει τον τύπο του identifier τους. Με αυτή την εντολή είναι δυνατό να γίνει απευθείας επιλογή μιας κάρτας η οποία βρίσκεται στο πεδίο της κεραίας, χωρίς να πρέπει να εκτελέσει ένα Get Card scanning sequence.

FORMAT

E2h 14h xx xx xx xx

Όπου: xx xx xx xx, είναι ο σειριακός αριθμός της κάρτας που έχει επιλεχθεί.

RESULT

S zz

Όπου: zz, είναι το μέγεθος της μνήμης της κάρτας (08) για το GCL8K.

HALT

Θέτει την πρόσφατα επιλεγμένη κάρτα σε sleep mode.

FORMAT

E2h 14h

RESULT

S

EXCHANGE APDU

Στέλνει μία εντολή interface GCL8K σε μία GCL8K κάρτα και ανακτά την απάντηση.

Η συγκεκριμένη εντολή έχει σαν σκοπό τις συναλλαγές με την κάρτα και μεταφέρονται στον GCR680 με ένα Application Protocol Data Unit (APDU) format. Καιη απόκριση της κάρτας επιστρέφεται από τον GCR680 με το ίδιο APDU format.

FORMAT

E2h APDU

Όπου: APDU, είναι η εντολή APDU

RESULT

R Response APDU

Όπου: Response APDU, είναι η απάντηση APDU στην εντολή.

APDU FORMAT

Το APDU format καθορίζεται από το ISO 7816-3 standard.

Το GCR680 υποστηρίζει το ακόλουθο case:

CASE 4-5 hort format: εντολή δεδομένων ανάμεσα σε 1 και 255 bytes, απάντηση δεδομένων ανάμεσα σε 1 και 256 bytes.

COMMAND FORMAT

Ο GCR680 δέχεται εντολές με το ακόλουθο format:

HEADER	BODY		
CLA INS P_1 P_2	Lc	Parameters/Data	Le

Τα πεδία περιγράφονται παρακάτω:

HEADER FIELDS

Τα headers fields, είναι υποχρεωτικά, όπως παρακάτω:

Field Name	**Length**	**Description**
CLA	1	Instruction class.
INS	1	Instruction Code.δίνεται με τις περιγραφές των εντολών.
P_1	1	Parameter1.

P_2	1	Parameter 2.

Body Fields

Το σώμα της εντολής είναι προαιρετικό. περιλαμβάνει τα ακόλουθα πεδία:

Field Name	Length	Description
Lc	1	Data length
Data		Commands parameters of Data
Le	1	Expected length of data to be returned

Response format

Ο GCR680 δέχεται αποκρίσεις στις εντολές με το ακόλουθο format:

Body	Trailer
Data	SW1, SW2

Το Body είναι προαιρετικό και κρατάει τα επιστρεφόμενα δεδομένα μέσω της κάρτας.

Το Trailer περιλαμβάνει τα ακόλουθα δύο υποχρεωτικά bytes:

SW1: Status byte 1, που επιστρέφει το processing status (θέση επεξεργασίας)

SW2: Status byte 2, που επιστρέφει το processing qualification (προσόντα επεξεργασίας) της εντολής.

6.7.5. Security module ASIC Interface Command Set

Ο GCR680 περιέχει ένα module ασφάλειας ASIC, που ελέγχεται απευθείας από τον microprocessor. Το security module ASIC χειρίζεται:

- RF έλεγχος επικοινωνίας
- Low Level Security Features
-

Ο GCR680, αποθηκεύει τα ίδια κρυφά κλειδιά που χρησιμοποιούνται για cross authentication (διασταύρωση πιστοποίησης ταυτότητας), όπως οι GCL8K κάρτες. Τα κρυφά κλειδιά αποθηκεύονται στο GCR680 ASIC, το οποίο είναι, non-volatile (αμετάβλητη) Write Only Memory (WOM) module. ASIC interface command Exchange APDU μπορεί να στείλει την εντολή Load Key στο GCR680 ASIC.

EXCHANGE APDU

Στέλνει μία εντολή Load Key στο ASIC και ανακτά την απόκριση.

FORMAT

EDh APDU

Όπου: APDU, είναι η εντολή APDU

RESULT

R Response APDU

Όπου: Response APDU, είναι η απάντηση APDU στην εντολή.

LOAD_KEY

Κάνει load, σε ένα κρυφό κλειδί, στη WOM μνήμη του GCR680 ASIC.

FORMAT

CLA INS P1 P2	Lc	Parameters/ Data	Le
0x80 0xD8 P1 P2	0x0D	S Data	-

Όπου:

P1 P2, είναι η διεύθυνση του block που προστατεύεται από το κλειδί που γίνεται Loaded.

S, είναι το Authentication Mode Control byte.

Data, είναι το κλειδί που πρόκειται να φορτωθεί(6 bytes) και το σχετικό του transport key (6bytes).

RESPONSE

	SW1, SW2

Υπόψη ότι μπορεί να εκτελεστεί μια παρόμοια εντολή, χρησιμοποιώντας την GCL8K Exchange APDU εντολή : E2h

Σ' αυτήν την περίπτωση στέλνεται ο κώδικας:

CLA INS P1 P2	Lc	Parameters/ Data	Le
0x80 0xD8 P1 P2	0x0D	S Data	-

Η πρόσβαση στο ASIC, χρησιμοποιώντας την E2h εντολή, μπορεί να μην υποστηρίζεται στο μέλλον, σαν αποτέλεσμα της εξέλιξης των λειτουργιών πρόσβασης στην μνήμη του ASIC. Παρόλα αυτά όμως, όσο η πρόσβαση σ' αυτές τις λειτουργίες είναι περιορισμένη, σε ένα non-ciphered Load Key, αυτή η απλοποιημένη μέθοδος πρόσβασης μπορεί να χρησιμοποιηθεί στην ανάπτυξη αφαρμωγών.

RF On

Ενεργοποιεί το RF σήμα, αν είναι απενεργοποιημένο, και κάνει reset την Get Card flag, έτσι ώστε η νέα Get Card εντολή που εκτελείται, θα δράσει σαν να είναι η πρώτη που θα εκτελεστεί μετά το Reset.

FORMAT
E1h 10h

RESULT
S

RF Off

Απενεργοποιεί το RF σήμα.

FORMAT
E1h 11h

RESULT
S

6.8. GCL8K Interface Commands

Οι GCL8K εντολές interface, ομαδοποιούνται σε δύο sets: το elementary command set και το combined command set. Οι elementary commands, εκτελούν τις λειτουργίες τους χωρίς να αυθεντικοποιούν τον target sector, όπου οι combined εντολές, μπορούν προαιρετικά να αυθεντικοποιήσουν τον target sector, πριν την εκτέλεση των λειτουργιών τους. Στέλνονται GCL8K εντολές στον GCR680 χρησιμοποιώντας την εντολή Exchange APDU.

Για την εκτέλεση Read ή Write λειτουργιών, χρησιμοποιούνται οι C_Card και C_Write εντολές με συγκεκριμένες παραμέτρους.

6.8.1. Elementary Command Set

Οι GCL8K elementary εντολές, είναι:

- Authenticate
- Transfer
- Restore
- Subtract Vakue
- Add Value

Authenticate

Επιλέγει ένα κλειδί, το οποίο είναι αποθηκευμένο και το προκαλεί προς ένα αποκρινόμενο κλειδί, στο sector που περιέχει το block, διευθυνσηδούμενο από τα P1 και P2. Αν η πρόκληση είναι επιτυχημένη, η πρόσβαση χορηγείται στον sector που κρατάει το challenged key για τις λειτουργίες οι οποίες καθορίζονται από τις συνθήκες πρόσβασης.

FORMAT

CLA INS P1 P2	Lc	Parameters/ Data	Le
0x84 0x28 P2	01	S	00

Όπου:

P2, καθορίζει την διεύθυνση του block που αυθεντικοποιείται, από 0εως 63..

S, είναι το Authentication Mode Control byte.Ο ακόλουθος πίνακας περιγράφει την μορφή του S byte.

V	SE	A	M	S1	AB	K1	K0

Όπου:

V 0: χωρίς επαλήθευση

1: μετά την εκτέλεση της εντολής Write Block οι ROS680, εκτελούν την εντολή Read Block, για να επιβεβαιώσουν ότι η εντολή Write Block εκτελέστηκε με επιτυχία.

SE 0: default

A 0: χωρίς αυθεντικοποίηση

1: η αυθεντικοποίηση πρέπει να εκτελεστεί σύμφωνα με την αξία των άλλων bits.

M 0: τα SE, S1, AB, K1 και K0 bits θα πρέπει να ερμηνευτούν

1: RFU

S1 0

1: RFU

AB 0: Key A

1: Key B

K1,K0 0,0: ASIC Keyset 0

0,1: ASIC Keyset 1

1,0: ASIC Keyset 2

1,1: RFU

RESPONSE

	SW1, SW2

TRANSFER

Μπορεί να εκτελεστεί μόνο σε value blocks.

Η εντολή αυτή θα πρέπει να εκτελείται μετά από κάθε Add Value ή Subtract Value εντολή. Μεταφέρει το αποτέλεσμα από μία προσθήκη ή αφαίρεση στο value block που είναι διευθυνσηοδοτημένο από τα P1 και P2.

FORMAT

CLA INS P1 P2	Lc	Parameters/ Data	Le
0x84	01	00	-

0xD4 P1 P2			

Όπου:

P1 P2, καθορίζουν target value block.

RESPONSE

	SW1, SW2

RESTORE

Μπορεί να εκτελεστεί μόνο σε value blocks.

Αντιγράφει την αποθηκευμένη αξία στο value block που είναι διευθυνσηοδοτημένο από τα P1 και P2, στο GCL8K buffer register (κατάλογο προσωρινών χώρων).

FORMAT

CLA INS P1 P2	Lc	Parameters/ Data	Le
0x84 0xB4 P1 P2	01	00	-

Όπου:

P1 P2, καθορίζουν την πηγή του value block.

RESPONSE

	SW1, SW2

SUBTRACT VALUE

Μπορεί να εκτελεστεί μόνο σε value blocks.

Αφαιρεί μία συγκεκριμένη αξία από το value block που καθορίζεται από το P1 και P2. Αυτή η εντολή μπορεί να εκτελεστεί, αν το κατάλληλο κλειδί για την χορήγηση πρόσβασης στο subtract value

(καθώς καθορίζεται από τις συνθήκες πρόσβασης του sector target), έχει προκληθεί χρησιμοποιώντας την εντολή αυθεντικοποίησης Authenticate. Το αποτέλεσμα της αφαίρεσης είναι αποθηκευμένο σε ένα buffer register, μέχρι να εκτελεστεί η επόμενη εντολή. Η διαχείριση του Back up θα πρέπει να ελέγχεται από την εφαρμογή.

FORMAT

CLA INS P1 P2	Lc	Parameters/ Data		Le
0x84 0x34 P1 P2	5	00	Count	-

Όπου:
P1 P2, καθορίζουν την διεύθυνση του target value block.
Count , καθορίζει την αξία που θα αφαιρεθεί

RESPONSE

	SW1, SW2

ADD VALUE

Μπορεί να εκτελεστεί μόνο σε value blocks.

Προσθέτει μία συγκεκριμένη αξία στο block που καθορίζεται από το P1 και P2. Αυτή η εντολή μπορεί να εκτελεστεί, αν το κατάλληλο κλειδί για την χορήγηση πρόσβασης στο add value (καθώς καθορίζεται από τις συνθήκες πρόσβασης του sector target), έχει προκληθεί χρησιμοποιώντας την εντολή αυθεντικοποίησης Authenticate. Το αποτέλεσμα της αφαίρεσης είναι αποθηκευμένο σε ένα buffer register, μέχρι να εκτελεστεί η επόμενη εντολή. Η διαχείριση του Back up θα πρέπει να ελέγχεται από την εφαρμογή.

FORMAT

CLA INS P1	Lc	Parameters/ Data	Le

P2				
0x84 0x36 P1 P2	5	00	Count	-

Όπου:

P1 P2, καθορίζουν την διεύθυνση του target value block.

Count , καθορίζει την αξία που θα προστεθεί.

RESPONSE

	SW1, SW2

6.9. Συνδυασμένα set εντολών

Οι combined εντολές απλοποιούν την ανάπτυξη των GCL8K εφαρμογών. Κάθε συνδυασμένη εντολή ανταποκρίνεται απευθείας σε μία εφαρμογή λειτουργίας. Χρησιμοποιώντας τις combined εντολές, μπορούμε να αυξήσουμε σημαντικά την ταχύτητα μετάδοσης. Οι combined εντολές είναι:

- C_Read
- C_Write
- C_Read Value
- C_Subtract Value
- C_Add Value
- C_Copy Value
- C_Load Key

6.9.1. Authentication Mode Control Byte

Όλες οι combined εντολές περιέχουν το Authentication Mode Control Byte. Αυτό καθορίζει πότε θα εκτελεστεί η αυθεντικοποίηση και πώς. Το ακόλουθο παράδειγμα περιγράφει το format του S byte.

V	SE	A	M	S1	AB	K1	K0

Όπου:

V 0: χωρίς επαλήθευση

1: μετά την εκτέλεση της εντολής οι ROS680, εκτελούν την εντολή Read Block, για να επιβεβαιώσουν ότι η εντολή εκτελέστηκε με επιτυχία.

SE 0: default

A 0: χωρίς αυθεντικοποίηση

1: η αυθεντικοποίηση πρέπει να εκτελεστεί σύμφωνα με την αξία των άλλων bits.

M 0: τα SE, S1, AB, K1 και K0 bits θα πρέπει να ερμηνευτούν

1: RFU

S1 0

1: RFU

AB 0: Key A

1: Key B

K1,K0 0,0: ASIC Keyset 0

0,1: ASIC Keyset 1

1,0: ASIC Keyset 2

1,1: RFU

Data είναι τα δεδομένα που πρέπει να γραφτούν.

C_READ

Διαβάζει από το 1 έως το 4 block, μέσα σε ένα sector. Αυτή η εντολή μπορεί μόνο να εκτελεστεί, αν το κατάλληλο κλειδί για την χορήγηση πρόσβασης για ανάγνωση (καθώς καθορίζεται από τις συνθήκες πρόσβασης του sector target), έχει προκληθεί χρησιμοποιώντας την εντολή αυθεντικοποίησης Authenticate. Αν πολλαπλά blocks, έχουν πρόσβαση, η εντολή είναι επιτυχημένη μόνο αν οι συνθήκες πρόσβασης επιτρέπουν την πρόσβαση για ανάγνωση σε όλα τα blocks.

FORMAT

CLA INS P1 P2	Lc	Parameters/ Data	Le
0x80 0xB8 P1 P2	01	S	Le

Όπου:

P1 P2, καθορίζει την διεύθυνση (ότι αυτός είναι ο αριθμός) του πρώτου block που θα διαβαστεί, από το 3 εώς το 63.

S, είναι το Authentication Mode Control byte.

Le, είναι ο αριθμός των bytes που πρόκειται να διαβαστούν (α'πο το 0 εώς το 64).

RESPONSE

	SW1, SW2

Data είναι τὰ δεδομένα που πρέπει να γραφτούν.

C_WRITE

Γράφει μέχρι και σε 4 blocks σε ένα sector. Αυτή η εντολή μπορεί μόνο να εκτελεστεί, αν το κατάλληλο κλειδί για την χορήγηση πρόσβασης για εγγραφή (καθώς καθορίζεται από τις συνθήκες πρόσβασης του sector target), έχει προκληθεί χρησιμοποιώντας την εντολή αυθεντικοποίησης Authenticate. Αν πολλαπλά blocks, έχουν πρόσβαση, η

εντολή είναι επιτυχημένη μόνο αν οι συνθήκες πρόσβασης επιτρέπουν την πρόσβαση για εγγραφή σε όλα τα blocks.

FORMAT

CLA INS P1 P2	Lc	Parameters/ Data	Le
0x80 0xD8 P1 P2	Lc	S Data	-

Όπου:

Lc είναι ο αριθμός τωνbytes που πρόκειται να γραφτούν (θα πρέπει να υπάρχει ένα πολλαπλό μέγεθος block, για παράδειγμα 16, 32, 48, 64) +1

P1 P2, καθορίζει την διεύθυνση του πρώτου block που θα γραφτεί.

S, είναι το Authentication Mode Control byte.

Data είναι τα δεδομένα που πρέπει να γραφτούν.

RESPONSE

	SW1, SW2

C_READ VALUE

Μπορεί να εκτελεστεί μόνο σε value blocks.

Διαβάζει το value από το value block και την διεύθυνση του.

Οι ROS680 διαβάζουν το block και ελέγχουν την ακεραιότητα του value block πριν την επιστροφή των read values. Τα Value blocks έχουν μία συγκεκριμένη δομή η οποία περιέχει δεδομένα checksum και redundancy.

FORMAT

CLA INS P1 P2	Lc	Parameters/ Data	Le
0x80 0x32	01	S	4

P1 P2			

Όπου:

P1 P2, καθορίζει την διεύθυνση του πρώτου block που θα διαβαστεί.

S, είναι το Authentication Mode Control byte.

Data είναι τα δεδομένα που πρέπει να γραφτούν.

RESPONSE

	SW1, SW2

Data είναι τα δεδομένα που πρέπει να γραφτούν.

C_ SUBTRACT VALUE

Μπορεί να εκτελεστεί μόνο σε value blocks.

Αφαιρεί μία συγκεκριμένη αξία από το value block που καθορίζεται από το P1 και P2, με την προϋπόθεση ότι οι συνθήκες πρόσβασης επιτρέπουν την Subtract Value να εκτελεστεί. Το αποτέλεσμα της αφαίρεσης δεν γράφεται στο target value block. Είναι αποθηκευμένο σε ένα buffer register μέχρι να εκτελεστεί η επόμενη εντολή. Η διαχείριση του Back up θα πρέπει να ελέγχεται από την εφαρμογή.

FORMAT

CLA INS P1 P2	Lc	Parameters/ Data	Le
0x80 0x34 P1 P2	7	S Count @A1 @A2	-

Όπου:

P1 P2, καθορίζει την διεύθυνση του πρώτου block που θα αφαιρεθεί.

S, είναι το Authentication Mode Control byte.

Count , καθορίζει την αξία που θα αφαιρεθεί.

@A1, @A2, είναι η διεύθυνση του value block στο οποίο γράφεται το αποτέλεσμα.

RESPONSE

	SW1, SW2

C_Add Value

Μπορεί να εκτελεστεί μόνο σε value blocks.

Προσθέτει μία συγκεκριμένη αξία από το value block που καθορίζεται από το P1 και P2, με την προϋπόθεση ότι οι συνθήκες πρόσβασης επιτρέπουν την Add Value να εκτελεστεί. Το αποτέλεσμα της πρόσθεσης δεν γράφεται στο target value block. Είναι αποθηκευμένο σε ένα buffer register μέχρι να εκτελεστεί η επόμενη εντολή. Η διαχείριση του Back up θα πρέπει να ελέγχεται από την εφαρμογή.

FORMAT

CLA INS P1 P2	Lc	Parameters/ Data	Le
0x80 0x36 P1 P2	7	S Count @A1 @A2	-

Όπου:

P1 P2, καθορίζει την διεύθυνση του value block που το προσδιορισμένο value έχει αφαιρεθεί.

S, είναι το Authentication Mode Control byte.

Count , καθορίζει την αξία που θα προστεθεί.

@A1, @A2, είναι η διεύθυνση του value block στο οποίο γράφεται το αποτέλεσμα.

RESPONSE

	SW1, SW2

C_Copy Value

Μπορεί να εκτελεστεί μόνο σε value blocks.

Αντιγράφει τα περιεχόμενα από το source block στο target block.

FORMAT

CLA INS P1 P2	Lc	Parameters/ Data	Le
0x80 0x38 P1 P2	3	S @A1 @A2	-

Όπου:

P1 P2, καθορίζει την διεύθυνση του source block

S, είναι το Authentication Mode Control byte.

@A1, @A2, καθορίζουν τη διεύθυνση του target block.

RESPONSE

	SW1, SW2

7. Παράρτημα

7.1. Η Εφαρμογή

Για να γίνει πιο κατανοητή η χρησιμότητα των έξυπνων καρτών, παρακάτω παραθέτεται μία σημαντική έξυπνη εφαρμογή καρτών. Στο μέλλον, όταν πληρώνουμε μια επίσκεψη στο γιατρό και προτείνει παίρνουμε ένα ιδιαίτερο φάρμακο, να είμαστε φορείς στο ακόλουθο σενάριο:

- Ο γιατρός σας ρωτά για την κάρτα συνταγών σας.
- Η κάρτα παρεμβάλλεται στον αναγνώστη, και ο γιατρός κοιτάζει στην ιστορία συνταγών σας. (Για κάποιους από εμάς τις σύνθετες ιατρικές/ιστορίες φαρμάκων, ένα ειδικό σύστημα μπορεί να είναι απαραίτητο.)
- Ο γιατρός παρατηρεί ότι ένας άλλος γιατρός σας έχει χορηγήσει αυτήν την περίοδο ένα φάρμακο που μπορεί να αντιδράσει με το φάρμακο που σκεφτόταν να χορηγήσει ο ίδιος. Έτσι ο γιατρός επιλέγει ένα διαφορετικό φάρμακο και εισάγει τη νέα συνταγή στην έξυπνη κάρτα συνταγών σας. (Ιδανικά, σε αυτό το σημείο, η κάρτα μπόρεσε να διαβιβάσει την κατάταξη στο φαρμακείο.)
- Παίρνετε την κάρτα σας στο φαρμακείο και την παρεμβάλλετε στον αναγνώστη του φαρμακείου.
- Ο φαρμακοποιός κοιτάζει στην ιστορία συνταγών σας και παίρνει τη νέα συνταγή.
- Υποθέστε ότι τα φαρμακεία έχουν καλύτερα στοιχεία για τα φάρμακα από τους γιατρούς, και αυτός ο ιδιαίτερος φαρμακοποιός σκέφτεται ότι γιατρός πρέπει να επανεξετάσει το ορισμένο φάρμακο. Ο φαρμακοποιός καλεί το γιατρό, ο οποίος τηλεφωνικός αριθμός είναι συμπεριλαμβανόμενος στην έξυπνη κάρτα συνταγών. Μετά από μια συνοπτική συζήτηση, οι δύο αποφασίζουν σχετικά με ένα εναλλάσσομενο φάρμακο και ενημερώνουν την κάρτα.
- Ο φαρμακοποιός γεμίζει τη συνταγή σας, παίρνει τις πληροφορίες σχεδίων προμηθευτών από την κάρτα, και επικοινωνεί με τον προμηθευτή σχεδίων χρησιμοποιώντας ένα κρυπτογραφημένο πρωτόκολλο.

- Ο ιατρικός προμηθευτής ελέγχει ότι είστε πραγματικά μέλος σχεδίων, ελέγχει ότι η συνταγή προέρχεται από έναν εξουσιοδοτημένο γιατρό, και παίρνει την ευκαιρία να ενημερώσει μερικά στοιχεία στην κάρτα σας.
- Ο φαρμακοποιός σας ρωτά για πέντε δολάρια.

Το σύστημα αυτό είναι σαφώς ασφαλέστερο από την γνώριμη σε όλους μας διαδικασία γραψίματος συνταγών σε χαρτί στο οποίο παρεμβάλλονται οι άνθρωποι αντί των συστημάτων υπολογιστών. Στην πραγματικότητα, στη Γερμανία, οι ιατρικές έξυπνες κάρτες χρησημοποιούνται ήδη.

Τα πλεονεκτήματα της έξυπνης κάρτας συνταγών

Η αξία που οι έξυπνες κάρτες προσθέτουν στο παραδοσιακό σχέδιο "καρτών" συνταγών είναι:

- Πρόσβαση στα στοιχεία καρτών όταν αλλάζετε τα καταστήματα, ταξιδεύετε, ή εξετάζετε τις νέες αντιπροσωπείες.
- Στιγμιαία πρόσβαση στο ιατρικό ιστορικό και την ιστορία φαρμάκων για το νοσοκομειακό ή το προσωπικό των επειγόντων περιστατικών.
- Αναλυτικά αρχεία που εμφανίζουν τι έχει χορηγηθεί ήδη -- συμπεριλαμβάνων το που, πότε και πόσο.
- Τα στοιχεία ενημερώνουν στους εγκεκριμένους παραλήπτες.

Προκειμένου να παρασχεθεί η υποστήριξη για την ανωτέρω διαδικασία, χρειαζόμαστε να αναπτύξουμε μια εφαρμογή που μας αφήνει να διαβάσουμε και να γράψουμε τα αρχεία στην κάρτα με έναν ασφαλή τρόπο. Η εφαρμογή ανωτέρω απλά δίνει στο χρήστη τη δυνατότητα να εισαγάγει τα στοιχεία επάνω στην κάρτα. Παραδείγματος χάριν, ο γιατρός μπορεί να προσθέσει μία συνταγή στην κάρτα.

Ανάπτυξη της εφαρμογής

Σε αυτό το τμήμα παίρνουμε τον κώδικα που χρειαζόμαστε να γράψετε τα στοιχεία σε μια έξυπνη κάρτα και να τα διαβάσουμε πίσω. Η πρώτη ενέργεια στο πρόγραμμα που προσπαθεί να διαβάσει ή να γράψει τα στοιχεία σε μια κάρτα μνήμης είναι να αποκτηθεί μια αναφορά σε μια συσκευή που υποστηρίζει μια έξυπνη κάρτα. Μόλις έχουμε τη συσκευή, πρέπει να γράψουμε ή να διαβάσουμε την επιθυμητή συμβολοσειρά. Αυτό επιτυγχάνεται με το να καλέσει τις μεθόδους που παρεχόμενες από το CardStrings.java. Οι παρεχόμενες κλάσεις πρωτοτύπων διευκολύνουν τον προγραμματισμό των έξυπνων καρτών. Έχουμε προσθέσει επίσης έναν χειριστή γεγονότος για την ενημέρωση έξυπνων γεγονότων καρτών όπως η εισαγωγή μιας κάρτας. Το τμήμα του κώδικα που παρατήθεται παρακάτω διευκολύνει στην κατανόηση της λειτουργείας την εφαρμογής:

```
import java.commerce.smartcards.*; Packages form JECF to support smart cards
import java.commerce.gemplus.*;
import java.commerce.DeviceManager.*;
import java.awt.event.*;
/**
* Read and write Gemplus Memory cards. The following cards
* are supported:
* GFM 4k
*/
public class RWString {

    public static void main( String args[]) {
        WriteString ws = new WriteString(args);
    }

}

class WriteString  implements ActionListener {

    ISOCardReader   isoReader = null;
    int                    portNumber;
    String              deviceName;

    public WriteString(String args[]) {

        ////////////////////////////////////
        //     Process the arguments
        ////////////////////////////////////
        for(int i = 0; i < args.length; i++) {
            if ( args[i].equals("-port") ){
                portNumber = 0;
            } else if ( args[i].equals("-device") ) {
                deviceName = new String ( args[++i] );
            } else if ( args[i].equals("-help") ) {
                System.out.println("Usage: string -port # -device COM1 or /dev/ttya"
);
                System.exit(0);
            }
        }

        SmartCardDetector scDetector = new SmartCardDetector(1000);
        scDetector.addActionListener(this);
        scDetector.startDetection();
    }
    public void actionPerformed(ActionEvent actionEvent) {
```

```
            System.out.println("Action Performed: " + actionEvent );
            try {
                // Open the requested port number
                SmartCardReader scr = new SmartCardReader();
                isoReader =  scr.getDefault();
                isoReader.beginCardSession(GemplusSerialReader.GFM);
                CardStrings.writeGFMString("01234567" , isoReader );
                System.out.println(CardStrings.readGFMString(isoReader ) );
                isoReader.endCardSession();
            } catch(Exception e) {
                System.out.println( "Exception " + e);
                e.printStackTrace();
            } finally {
                try {
                    isoReader.endCardSession();
                } catch(Exception eFinally) {
                    System.out.println("Could not power Down card perform manual
reset");
                }
            }
        }
}
```

Η κλάση CardStrings παρέχει μερικές μεθόδους βοηθήματος για να διαβάσει και να γράψει τις συμβολοσειρές στην κάρτα. Οι συμβολοσειρές καταχωρούνται στην κάρτα με ένα πεδίο μήκους δύο οκτάδων, που ακολουθείται έξι κενές οκτάδες, που ακολουθούνται από από τα στοιχεία συμβολοσειράς. Εάν γράφουμε τα αντικείμενα της java μπορούμε να σώσουμε τα στοιχεία χωρίς την ανησυχία για τη μορφή της. Η αρχή γίνεται καταχωρώντας μερικά στοιχεία συμβολοσειράς σε μια κάρτα.

Η εφαρμογή είναι ένα πλήρες παράδειγμα για τα στοιχεία ανάγνωσης και γραψίματος σε μια κάρτα GemPlus GFM που χρησιμοποιεί έναν τμηματικό αναγνώστη GCR400. Με λίγη εργασία άλλοι αναγνώστες μπορούν να υποστηριχθούν.

7.2. ROS680 STATUS CODES

Οι ROS680 επιστρέφουν ένα status code S, μετά από την εκτέλεση μιας εντολής. Η παρακάτω λίστα των status codes, περιγράφει τα status codes που οι ROS680 μπορούν να επιστρέψουν.

Status Code	Sourse OS	Description
03h	OROS ή ROS680	Λάθος παράμετρος. Στέλνοντας μία λάθος παράμετρο σε μία εντολή APDU, θα έχει
		σαν αποτέλεσμα, στο E7h status code, να επιστραφεί αποκρινόμενο στο SW1 ≠90
15h	OROS ή ROS680	Δεν έχει επιλεγεί κάρτα
A2h	OROS ή ROS680	Έχει λήξει η περίοδος Time out
A3h	ROS680	CRG ή λάθος ισότητας σε ένα RF κανάλι το οποίο έχει προσδιοριστεί από το ASIC
AAh	ROS680	Το ASICδεν είναι συνδεμένο ή έχει κρεμάσει
E7h	OROS ή ROS680	SW1 ≠90
FBh	OROS ή ROS680	Η εντολή GET (NEXT) CARD εκτελέστηκε αλλά δεν έχει βρεθεί κάρτα

7.3. "GCL8K STATUS WORDS"

Οι status words που επιστρέφονται από τις εντολές GCR680, αλλά παίρνοντας υπόψη την συμπεριφορά της κάρτας, μπορούμε να τις ομαδοποιήσουμε στην παρακάτω λίστα.

SW1, SW2	Σημασία
67 00	Το μέγεθος του byte δεν είναι σωστό
6A 80	Data field error: το S δεν είναι σωστό
6B 00	P1, P2 δεν είναι σωστά
6C xx	Λάθος η Le παράμετρος. Le θα έπρεπε να είναι xx
6E 00	Το CLASS byte δεν είναι σωστό
6D 00	INS byte δεν είναι σωστό
90 00	Η εντολή έχει εκτελεστεί σωστά
92 02	Αποτυχία μνήμης (μετά από ένα Write_Block με επαλήθευση)
94 04	Λάθος κατά τη διάρκεια λειτουργίας ενός Value Block (εκτός από υπερχείλιση)
94 05	Υπερχείλιση κατά τη διάρκεια λειτουργίας ενός Value Block
98 04	Δεν έχουν εκπληρωθεί οι απαιτούμενες συνθήκες πρόσβασης
98 20	Σφάλμα αυθεντικοποίησης (το κλειδί δεν είναι σωστό)

7.4. Ευρετήριο ορολογίας Έξυπνων Καρτών

ABS	(Acrylonitrile Butadiene Styrene) Ακρυλονιτρικό Βουτανιεδικό Στυρένιο. Το πλαστικό που χρησιμοποιείται για την έγχυση των σκελετών των καρτών για διάφορες κάρτες
Acceptor	Αποδοχέας. Ο οργανισμός (συνήθως ένας έμπορος), ο οποίος δέχεται μία κάρτα (για παράδειγμα για μία πληρωμή).
Acquirer	Μεσολαβητής συναλλαγών. Η Τράπεζα, η οποία επεξεργάζεται τις συναλλαγές ενός εμπόρου και τις προωθεί στο σύστημα εκκαθάρισης (πχ clearing system). Μπορεί να είναι και ένας οργανισμός ο οποίος διαχειρίζεται την ανταλλαγή πληροφοριών και δεδομένων μεταξύ του διαχειριστή ενός συστήματος πληρωμών και του ατόμου το οποίο παρέχει τις διάφορες υπηρεσίες.
AID	Application Identifier. Αναγνωριστικό εφαρμογής. Το AID αναγνωρίζει μία εφαρμογή σε μία έξυπνη κάρτα. Ορίζεται στο πρότυπο ISO/IEC 7816-5. Ένα μέρος του AID μπορεί να κατοχυρώνεται σε εθνικό ή παγκόσμιο επίπεδο. Σε αυτήν την περίπτωση, η εφαρμογή στην οποία αναφέρεται είναι μοναδικά αναγνωρίσιμη. Το AID αποτελείται από δύο τμήματα: το RID (Registered Identifier) και το PIX (Proprietary Identifier).
ALD	(Application Load Certificate) Χρησιμοποιείται από τη προδιαγραφή Multos και παρόμοια συστήματα για την «επισημοποίηση» μιας εφαρμογής που φορτώνεται σε μία κάρτα πολλαπλών εφαρμογών
Algorithm	Αλγόριθμος. Μία μαθηματική διαδικασία που χρησιμοποιείται για να γίνουν υπολογισμοί (στην κρυπτογραφία: αλγόριθμος κρυπτογράφησης)
Analog	Αναλογικός. Χρησιμοποιείται σε αντιδιαστολή με το «Ψηφιακός»
Anti-collision	Αποφυγή σύγκρουσης. Ένας αλγόριθμος που χρησιμοποιείται για την αναγνώριση δύο ή περισσοτέρων ασύρματων έξυπνων καρτών, όταν λειτουργούν ταυτόχρονα.
Anti-tearing	Ένα χαρακτηριστικό της κάρτας, το οποίο προστατεύει τα δεδομένα της μνήμης στην περίπτωση που η κάρτα απομακρυνθεί πριν την ολοκλήρωση μίας συναλλαγής.
APDU (Application Protocol Data Unit)	Μονάδα Δεδομένων Πρωτοκόλλου Εφαρμογής. Είναι ένα «κουτί» δεδομένων λογισμικού, το οποίο χρησιμοποιείται για την ενθυλάκωση των δεδομένων, έτσι ώστε να μπορούν να ανταλλάσσονται ανάμεσα σε μία έξυπνη κάρτα και σε ένα τερματικό.
ASIC	(Application-Specific Integrated Circuit) Ολοκληρωμένα

	Κυκλώματα Ειδικού σκοπού Εφαρμογής. Τα κυκλώματα αυτά ελαχιστοποιούν το κόστος παραγωγής με την υλοποίηση κυκλωμάτων που έχουν όλα τα χαρακτηριστικά της υψηλής τεχνολογίας
Asymmetric Cryptography	Ασυμμετρική ή ασύμμετρη κρυπτογραφία (επίσης «κρυπτογραφία δημόσιου κλειδιού». Αναφέρεται στη μέθοδο κρυπτογράφησης όπου υπάρχουν δύο κλειδιά κρυπτογράφησης. Το ένα χρησιμοποιείται για την κρυπτογράφηση του κειμένου και το άλλο για την αποκρυπτογράφηση.
ATC	(Application Transaction Counter) Μετρητής ο οποίος υπάρχει μέσα στην κάρτα και αυξάνεται κατά μια μονάδα κάθε φορά που πραγματοποιείται μια συναλλαγή
ATM	(Automated Teller Machine) Ειδικό τερματικό, το οποίο τοποθετείται σε δημόσιους χώρους και επιτρέπει την εκτέλεση οικονομικών συναλλαγών.
ATR	(Answer To Reset) Είναι μία ακολουθία από byte, η οποία στέλνεται από μία έξυπνη κάρτα μετά από (hardware) επαναφορά. Μεταξύ άλλων περιέχει διάφορες παραμέτρους σχετικά με το πρωτόκολλο μετάδοσης της κάρτας
Authentication	Ταυτοποίηση. Η διαδικασία αποδείξεως της γνησιότητας μίας οντότητας (π.χ. έξυπνη κάρτα ή μέσω αυτής του κατόχου της), χρησιμοποιώντας κρυπτογραφικές μεθόδους
External Authentication	Εξωτερική Ταυτοποίηση. Η διαδικασία που χρησιμοποιείται για την ταυτοποίηση του «έξω» κόσμου (π.χ. ένα τερματικό) από την έξυπνη κάρτα.
Internal Authentication	Εσωτερική Ταυτοποίηση. Η διαδικασία που χρησιμοποιείται για να αποδείξει μία έξυπνη κάρτα ότι είναι γνήσια.
BIP	(Bearer Independent Protocol) Πρωτόκολλο το οποίο επιτρέπει σε μια κάρτα SIM να επικοινωνεί απευθείας με απομακρυσμένους εξυπηρετητές
Black list	Μαύρη λίστα. Η λίστα, συνήθως σε μία βάση δεδομένων, η οποία περιέχει όλες τις κάρτες που δεν επιτρέπεται πλέον η χρήση τους σε ένα σύστημα
CA	(Certification Authority) Αρχή Πιστοποίησης. Ο οργανισμός που εκδίδει πιστοποιητικά και είναι υπόλογος για τις ευθύνες που προκύπτουν από την εγκυρότητα των στοιχείων του κατόχου
CAM	(Card Authentication Method) Μέθοδος αυθεντικοποίησης κάρτας. Αυτή η μέθοδος χρησιμοποιείται για να εξακριβωθεί εάν η κάρτα προέρχεται από έγκυρο εκδότη
Card accepter	Αποδοχέας καρτών. Οντότητα στην οποία μπορούν να χρησιμοποιηθούν έξυπνες κάρτες για μια συγκεκριμένη

	εφαρμογή
Card body	Σώμα κάρτας. Πλαστική κάρτα, το ενδιάμεσο προϊόν στην κατασκευή της Έξυπνης Κάρτας. Σε επόμενο βήμα της κατασκευής, ενσωματώνεται το ολοκληρωμένο κύκλωμα
Card issuer	Εκδότης κάρτας. Οντότητα, υπεύθυνη για την έκδοση έξυπνων καρτών. Συνήθως, ο πάροχος της εφαρμογής και ο εκδότης της κάρτας ταυτίζονται για τις έξυπνες κάρτες μίας εφαρμογής.
Card manufacturer	Κατασκευαστής κάρτας. Η οντότητα, που κατασκευάζει σώματα καρτών , ενσωματώνει το ολοκληρωμένο κύκλωμα και ανά εφαρμογή το προγραμματίζει (π.χ. κάρτες μνήμης) ή απλώς το προετοιμάζει για να προγραμματιστεί από άλλη οντότητα.
Card owner	Ιδιοκτήτης κάρτας. Είναι η φυσική ή νομική οντότητα που έχει το νόμιμο έλεγχο της κάρτας. Στην περίπτωση των καρτών χρέωσης ή πιστωτικών καρτών, ο ιδιοκτήτης της κάρτας είναι συνήθως η Τράπεζα που εκδίδει την κάρτα. Οι πελάτες που χρησιμοποιούν την κάρτα είναι συνήθως μόνο «κάτοχοι κάρτας» (πβ. Cardholder).
Card possessor	Κύριος κάρτας. Η οντότητα που έχει στην κυριότητά της μία κάρτα
Card reader	Συσκευή με σχετικά απλή ηλεκτρική και μηχανική κατασκευή που μπορεί να δεχτεί έξυπνες κάρτες και να αλληλεπιδράσει μαζί τους
Card user	Το άτομο που χρησιμοποιεί την κάρτα. Δεν είναι υποχρεωτικά ο νόμιμος κάτοχός της
Cardholder	Κάτοχος κάρτας. Αναφέρεται στην οντότητα, η οποία έχει το πραγματικό δικαίωμα κατοχής και χρήσης της κάρτας. Ο κάτοχος της κάρτας δεν είναι αναγκαίο ότι είναι και ο ιδιοκτήτης της κάρτας
Certificate	Πιστοποιητικό. Αρχείο ψηφιακά υπογεγραμμένο από μία Αρχή Πιστοποίησης
CEN	(Centre European pour la Normalisation – European Standards Centre) Ο ευρωπαϊκός οργανισμός προτύπων CEN βρίσκεται στις Βρυξέλλες. Αποτελείται από όλους τους (ευρωπαϊκούς) εθνικούς οργανισμούς προτύπων και είναι ο επίσημος οργανισμός της Ευρωπαϊκής Ένωσης για τα ευρωπαϊκά πρότυπα
Challenge-response	Μέθοδος ταυτοποίησης, όπου το σύστημα που απαιτεί ταυτοποίηση στέλνει μία τυχαία «πρόκληση». Το υπό ταυτοποίηση αντικείμενο (π.χ. μία έξυπνη κάρτα) υπολογίζει την «απάντηση» στην «πρόκληση». Το σύστημα μπορεί να επιβεβαιώσει τη γνησιότητα του αντικειμένου με βάση αυτή την «απάντηση».

Chip card	Κάρτα με ενσωματωμένο ολοκληρωμένο κύκλωμα. Αναφέρεται επίσης ως «έξυπνη κάρτα», αλλά συχνά χρησιμοποιείται με τέτοιον τρόπο, ώστε να συμπεριλαμβάνει και τις κάρτες μνήμης, οι οποίες δεν έχουν «εξυπνάδα»
Clearing/Clearance	Η διαδικασία διαβίβασης, εναρμόνισης και επιβεβαίωσης εντολών χρηματοπιστωτικών ιδρυμάτων
Clearing system	Πληροφοριακό Σύστημα, το οποίο εκτελεί σε κεντρική εφαρμογή διακανονισμούς συναλλαγών μεταξύ χρηματοπιστωτικών ιδρυμάτων ή χρηματοπιστωτικών ιδρυμάτων και τρίτων
Cloning	Κλωνοποίηση. Προσπάθεια «επίθεσης» σε σύστημα έξυπνων καρτών, με την αντιγραφή της μνήμης ROM και EEPROM μίας γνήσιας σε μία πλαστή κάρτα
CMS	(Card Management System) Εργαλεία και διαδικασίες που χρησιμοποιούνται για την ανάπτυξη και διαχείριση εφαρμογών έξυπνων καρτών. Το CMS χρησιμοποιείται κυρίως για την διαχείριση του κύκλου ζωής των καρτών και των εφαρμογών τους
COS	(Chip Operating System/Mask) Ακολουθία ενσωματωμένων εντολών, στη μνήμη ROM της έξυπνης κάρτας
Confidentiality	Εμπιστευτικότητα. Αναφέρεται στις μεθόδους και διαδικασίες, που διασφαλίζουν ότι οι πληροφορίες είναι προσβάσιμες μόνο από τις οντότητες στις οποίες επιτρέπεται να έχουν πρόσβαση
Combination Card	Συνδυασμένη Κάρτα. Έξυπνη κάρτα, η οποία συνδυάζει και τις δύο τεχνολογίες (με επαφές και ασύρματη)
Contact Smart Card	Έξυπνη Κάρτα με Επαφές. Έξυπνη κάρτα, η οποία απαιτεί τη φυσική επαφή με τη συσκευή ανάγνωσης, ώστε να ανταλλάξουν δεδομένα
Contactless Smart Card	Χωρίς επαφές ή Ασύρματη Έξυπνη Κάρτα. Αναφέρεται σε έξυπνες κάρτες, οι οποίες μεταδίδουν και λαμβάνουν δεδομένα χρησιμοποιώντας ραδιοσυχνότητες
Coupler	Ηλεκτρονικό σύστημα - εφαρμογή που χρησιμοποιείται για να μπορεί να διαβάζει την συνήθως ασύρματη έξυπνη κάρτα
CQL	(Card Query Language) Υποσύνολο της SQL (Structured Query Language) που έχει υλοποιηθεί πάνω σε έξυπνη κάρτα
CRC	(Cyclic Redundancy Check) Μέθοδος ορθής μεταφοράς των δεδομένων
Cryptography	Κρυπτογραφία. Η επιστήμη και η τέχνη της μετατροπής συμβολοσειρών (π.χ. κειμένων, αριθμοσειρών κλπ) σε ακατανόητες μορφές, για όσους δεν έχουν τον κατάλληλο μηχανισμό επαναφοράς στην αρχική μορφή (κλειδί)

CVM	(Cardholder Verification Method) Μέθοδος Επιβεβαίωσης Κατόχου Κάρτας
DDA	(Dynamic Data Authentication) Μέθοδος πιστοποίησης της κάρτας χρησιμοποιώντας μηχανισμό ανταπόκρισης
DF	(Dedicated File) Οργάνωση της μνήμης για τις κάρτες με μικροεπεξεργαστή. Ένα DF είναι μία λογική οντότητα, η οποία αποτελείται από EF (elementary file)
Diffie- Hellman	Οι εφευρέτες της κρυπτογραφίας δημόσιου κλειδιού
Digital Cash (e-Cash)	Ψηφιακό Χρήμα, που μπορεί να αποθηκεύεται σε τραπεζικό λογαριασμό, προσωπικό υπολογιστή ή έξυπνη κάρτα
Dual Slot	Διπλή Θυρίδα. Αναγνώστης έξυπνων καρτών που μπορεί να χρησιμοποιήσει 2 έξυπνες κάρτες ταυτόχρονα. Χρησιμοποιείται σε συστήματα πληρωμών, για την ταυτοποίηση στην Τράπεζα τόσο του εμπόρου όσο και του πελάτη
Dual Interface Card (Combicard)	Έξυπνη Κάρτα, η οποία έχει δύο μέσα επικοινωνίας: ενσύρματη, μέσω ηλεκτρομηχανικών επαφών και ασύρματη επικοινωνία, μέσω κατάλληλης κεραίας
Duplication (Cloning)	Μεταφορά πρωτότυπων δεδομένων σε μία δεύτερη κάρτα με σκοπό την δημιουργία μιας πανομοιότυπης κάρτας
e-Cash	Ψηφιακό /Ηλεκτρονικό Χρήμα, που μπορεί να αποθηκεύεται σε τραπεζικό λογαριασμό, προσωπικό υπολογιστή ή έξυπνη κάρτα
ECC	Error Correction Code.Ένας Κώδικας Διόρθωσης Λαθών εντοπίζει σφάλματα στα δεδομένα, τα οποία σε πολλές περιπτώσεις μπορεί να διορθώσει
EEPROM	(Electrically Erasable Programmable Read-Only Memory) Τύπος μνήμης ROM που μπορεί να επαναπρογραμματιστεί με την εφαρμογή κατάλληλου ηλεκτρικού πεδίου
EF	(Elementary File) Στοιχειώδες Αρχείο. Μέρος της λογικής οργάνωσης της μνήμης μίας κάρτας με μικροεπεξεργαστή, το ανάλογο ενός αρχείου δεδομένων
Embedding	Ενσωμάτωση. Η διαδικασία ενσωμάτωσης ενός ολοκληρωμένου κυκλώματος στο σώμα μίας έξυπνης κάρτας.
EMV	(Europay – Mastercard – Visa) Μία σειρά από διεθνή πρότυπα για πληρωμές βασισμένες σε έξυπνες κάρτες, τα οποία αναπτύχθηκαν από τους οργανισμούς Europay, Mastercard και Visa
Encryption	Κρυπτογράφηση. Η διαδικασία μετασχηματισμού συμβολοσειράς σε ακατάληπτη μορφή, χρησιμοποιώντας ένα κατάλληλο κλειδί
ETU	(Elementary Time Unit) Βασική Μονάδα Χρόνου. Η βασική

	μονάδα χρόνου της έξυπνης κάρτας, στην οποία βασίζονται όλοι οι χρονισμοί επικοινωνίας της κάρτας. Ορίζεται ως ο χρόνος μεταφοράς ενός bit δεδομένων από μία έξυπνη κάρτα
Fabrication	Η διαδικασία κατασκευής του ολοκληρωμένου κυκλώματος της έξυπνης κάρτας
Filtered	Φιλτραρισμένος. Χαρακτηρισμός για δεδομένα ή λειτουργίες τα οποία έχουν φορτωθεί στην μνήμη της έξυπνης κάρτας
Flash Memory	Μνήμη στην οποία μπορεί να γίνει εγγραφή μία φορά αλλά για να γίνει διαγραφή της, θα πρέπει να γίνει διαγραφή του αντίστοιχου block
FRR	(False Reject Rate) Μονάδα μέτρησης εσφαλμένης απόρριψης μίας οντότητας σε ένα σύστημα. Χρησιμοποιείται κύρια στα συστήματα βιομετρικής
GSM	(Global System for Mobile communications, Group Speciale de Mobile) Σύστημα κυψελοειδούς τηλεφωνίας με ευρεία διάδοση στην Ευρώπη
Garbage Collection	Λειτουργία έξυπνης κάρτας τύπου Java Card, η οποία συλλέγει τη μνήμη που δε χρησιμοποιείται πλέον από μία εφαρμογή και τη μετατρέπει σε ελεύθερη μνήμη προς χρήση από άλλες εφαρμογές
Hard Mask	Σε μία έξυπνη κάρτα με hard mask το μεγαλύτερο κομμάτι του κώδικα του προγράμματος υλοποιείται στη μνήμη ROM
HSM	(Host Security Module) Συσκευή, η οποία χρησιμοποιείται για την ασφαλή αποθήκευση κλειδιών και την (εσωτερική) εκτέλεση κρυπτογραφικών λειτουργιών, καθοδηγούμενη από έναν υπολογιστή
Hybrid Card	Υβριδική Κάρτα. Τύπος έξυπνης κάρτας που χρησιμοποιεί δύο διαφορετικά μέσα επικοινωνίας. Πβ. Dual Interface Card
ID-1 card	Έξυπνη Κάρτα με προτυποποιημένες κατά ISO διαστάσεις.
IFD	(Interface Device) Άλλη ονομασία του αναγνώστη έξυπνης κάρτας
Initialization	Το πρώτο στάδιο της διαδικασίας έκδοσης καρτών. Ο σκοπός αυτής της διαδικασίας είναι το φόρτωμα των δεδομένων από την εφαρμογή στις έξυπνες κάρτες
Intelligent memory card	Ευφυής κάρτα μνήμης. Κάρτα μνήμης με συμπληρωματικό λεπτομερές λογικό σχέδιο κυκλώματος που επιτρέπει/παρέχει επιπρόσθετες λειτουργίες ασφαλείας που καταγράφουν τη χρήση της μνήμης
Integrity	Ακεραιότητα. Αναφέρεται στις μεθόδους και διαδικασίες που

	διασφαλίζουν ότι οι πληροφορίες έχουν τροποποιηθεί μόνο από τις οντότητες που έχουν την αντίστοιχη εξουσιοδότηση
Interoperability	Διαλειτουργικότητα. Η δυνατότητα συστημάτων διαφορετικών κατασκευαστών να αλληλεπιδρούν μεταξύ τους.
ISO	(International Standards Organization) Ο οργανισμός ISO μεταξύ άλλων εργάζεται στην περιοχή των έξυπνων καρτών, με σκοπό να εξασφαλίσει, μέσω των προτύπων που ορίζει, ότι οι κατασκευαστές των ολοκληρωμένων, οι προγραμματιστές και οι εταιρείες έξυπνων καρτών ακολουθούν τις ίδιες προδιαγραφές
ITSO	(Integrated Transport Smart Card Organisation) Οργανισμός ο οποίος ιδρύθηκε στο Ηνωμένο Βασίλειο για να βοηθήσει την εξάπλωση των συστημάτων έξυπνων καρτών στα μέσα μαζικής μεταφοράς
ITU	(International Telecommunications Union) Οργανισμός που συντονίζει, προτυποποιεί και δημιουργεί παγκοσμίως τηλεπικοινωνιακές υπηρεσίες
Java Card	Μία προδιαγραφή για την εκτέλεση ενός υποσυνόλου της γλώσσας Java σε μία έξυπνη κάρτα
JCRE	(Java Card Runtime Environment) Το περιβάλλον εκτέλεσης στο οποίο εκτελείται η Java Card. Το JCRE είναι υπεύθυνο για όλες τις διαχειριστικές ενέργειες, όπως η φόρτωση και η αρχικοποίηση των εφαρμογών
Key management	Διαχείριση κλειδιών. Όλες οι διαχειριστικές λειτουργίες που σχετίζονται με την δημιουργία, διανομή, αποθήκευση, ενημέρωση των κρυπτογραφικών κλειδιών
Key escrow	Η μέθοδος κατάθεσης του ιδιωτικού κλειδιού σε τρίτον, συνήθως για τη διασφάλιση της ανάκτησης των δεδομένων τα οποία έχουν κρυπτογραφηθεί ή υπογραφεί με το ιδιωτικό κλειδί. Η κατάθεση του ιδιωτικού κλειδιού, ειδικά στην περίπτωση της χρήσης για ηλεκτρονικές υπογραφές, απαγορεύεται στις περισσότερες έννομες τάξεις.
Lifecycle	Κύκλος ζωής. Αναφέρεται στα στάδια επεξεργασίας και λειτουργίας μίας έξυπνης κάρτας, από τη στιγμή της κατασκευής του ολοκληρωμένου της, έως την απόσυρση από τη χρήση και καταστροφή της
MAC	(Message Authentication Code) Κώδικας Ταυτοποίησης Μηνύματος. Διαδικασία, συνήθως με τη χρήση αλγόριθμων κρυπτογράφησης, η οποία εγγυάται ότι το μήνυμα προέρχεται από τον πρωτότυπο παραλήπτη του και δεν έχει αλλαχθεί στην πορεία
Magnetic Strip Card	Κάρτα με μαγνητική λωρίδα, πάνω στην οποία δεδομένα μπορεί να καταχωρηθούν και να διαβαστούν

Memory card	Κάρτα μνήμης. Αναφέρεται σε κάρτες που περιέχουν μόνο μνήμη και επιλεκτικά και λογική ενσωματωμένη στο υλικό (hardwired logic). Χρησιμοποιείται σε αντιδιαστολή με τον όρο chip card ή smart card, όπου υποδηλώνεται η ικανότητα επεξεργασίας
MF	(Master File) Αποτελεί το βασικό κατάλογο του δένδρου αρχείων που υλοποιεί τη λογική οργάνωση της μνήμης μίας έξυπνης κάρτας. Το Κύριο Αρχείο επιλέγεται αυτόματα κάθε φορά που εκκινεί η έξυπνη κάρτα
Microprocessor Card	Κάρτα με μικροεπεξεργαστή. Κάρτα η οποία περιλαμβάνει: επεξεργαστή (CPU), μνήμης (RAM, ROM, EEPROM) και επιλεκτικά αριθμητικό συνεπεξεργαστή (NPU, numerical coprocessor), κάτι που επιτρέπει την άμεση εκτέλεση των αλγορίθμων. Χρησιμοποιείται σε αντιδιαστολή με τον όρο «Κάρτα Μνήμης» (Memory Card).
Mono-application smart card	Έξυπνη κάρτα μοναδικής εφαρμογής. Κάρτα που έχει τη δυνατότητα να εκτελέσει μία μόνο εφαρμογή, συνήθως προεγκατεστημένη σε αυτή
Mono-functional smart card	Έξυπνη κάρτα μοναδικής λειτουργίας. Κάρτα της οποίας το λειτουργικό σύστημα υποστηρίζει μόνο μια συγκεκριμένη εφαρμογή
Multi-application smart card	Έξυπνη Κάρτα Πολλαπλών Εφαρμογών. Αναφέρεται σε έξυπνες κάρτες νεότερης γενιάς, οι οποίες έχουν τη δυνατότητα να εκτελούν πολλαπλές εφαρμογές, από διαφορετικούς κατασκευαστές, σε αντίθεση με τις προηγούμενες, οι οποίες εκτελούσαν εφαρμογές ενός μόνο κατασκευαστή
Multi-functional smart card	Κάρτα της οποίας το λειτουργικό σύστημα υποστηρίζει παραπάνω από μια εφαρμογές και περιέχει κατάλληλες λειτουργίες διαχείρισης για την εγγραφή και διαγραφή εφαρμογών και αρχείων
μP card	Διαφορετική ονομασία για την κάρτα με μικροεξεργαστή. Πβ. Microprocessor card
Non-Volatile Memory	Ευσταθής μνήμη. Αναφέρεται σε μνήμες, οι οποίες διατηρούν τα δεδομένα τους, όταν διακοπεί η τροφοδοσία τους (όπως για παράδειγμα τα δεδομένα που είναι αποθηκευμένα στη μνήμη μίας έξυπνης κάρτας)
Numbering	Αρίθμηση. Είναι η διαδικασία χάραξης αριθμών πάνω στις έξυπνες κάρτες
OCF	(OpenCard Framework) Αρχιτεκτονική για κάρτες και τερματικά που έχει σκοπό την τυποποίηση των τερματικών εφαρμογών
Open application	Εφαρμογή μέσα στην έξυπνη κάρτα που την κάνει διαθέσιμη σε

	ποικίλους παρόχους υπηρεσιών, χωρίς να είναι απαραίτητη η αμοιβαία νομική σχέση μεταξύ τους
Optical memory card	Οπτική κάρτα μνήμης. Κάρτα, στην οποία οι πληροφορίες έχουν εγγραφεί σε μία ανακλαστική επιφάνεια με οπτικό τρόπο, παρόμοια με τη λειτουργία των CD.
OSI	(Open Systems Interconnection) Μοντέλο του οργανισμού ISO για τις επικοινωνίες
PAC	(PIN Authentication Code) Κωδικός Πιστοποίησης Προσωπικού Μυστικού Κωδικού
Padding	Μία μέθοδος, σύμφωνα με την οποία ένα ή περισσότερα bit προστίθενται σε ένα μήνυμα, ώστε να αποκτήσει το απαιτούμενο μέγεθος
Passivation layer	Στρώμα αδρανοποίησης. Ένα υλικό που καλύπτει το ολοκληρωμένο κύκλωμα της κάρτας, ώστε να είναι ανθεκτικότερη στις επιδράσεις του εξωτερικού περιβάλλοντος
PCC	(Proof-carrying code) Κώδικας ο οποίος περιλαμβάνει την απόδειξη συμβατότητας με δεδομένη πολιτική ασφάλειας
PC/SC	Αρχιτεκτονική επικοινωνίας τερματικών και έξυπνων καρτών. Το PC/SC προτάθηκε από την εταιρεία Microsoft και άλλους κατασκευαστές έξυπνων καρτών και προσωπικών υπολογιστών με σκοπό την προτυποποίηση των διεπαφών υλικού και λογισμικού των έξυπνων καρτών για την επικοινωνία με προσωπικούς υπολογιστές
PKCS	(Public-Key Cryptography Standards) Ανεπίσημα πρότυπα που αφορούν στην κρυπτογραφία δημόσιου κλειδιού.Έχουν δημοσιευθεί από την εταιρεία RSA Inc
PKI	(Public Key Infrastructure) Υποδομή Δημόσιου Κλειδιού. Εφαρμόζεται στην περίπτωση της ασύμμετρης κρυπτογράφησης και αναφέρεται στην ύπαρξη ενός ζευγαριού κλειδιών, του δημόσιου και ιδιωτικού) για την ασφάλεια των δεδομένων. Αποτελείται από κατάλληλο λογισμικό και υλικό.
Plug-In	Έξυπνη κάρτα με μικρό σχήμα και διάταξη που χρησιμοποιείται κυρίως για τα κινητά τηλέφωνα
Processor card	Πβ. Microprocessor card
PVC	(Polyvinyl Chloride) Χλωριούχο Πολυβινύλιο. Το πλαστικό από το οποίο κατασκευάζεται το σώμα της έξυπνης κάρτας
RAM	(Random Access Memory) Μνήμη Τυχαίας Προσπέλασης
RISC	(Reduced Instruction Set Computer) Μία αρχιτεκτονική σχεδίασης υπολογιστών
Retry Counter	Μετρητής Προσπαθειών. Μετρητής, ο οποίος συγκεντρώνει

	αρνητικές προσπάθειες/ αποτελέσματα και αποφασίζει αν κάποιο κλειδί θα συνεχίσει να χρησιμοποιείται ή όχι. Αν ο καταμετρητής φτάσει στον μέγιστο αριθμό ανεπιτυχών προσπαθειών τότε το κλειδί απενεργοποιείται και δεν μπορεί πλέον να χρησιμοποιηθεί
ROM	(Read Only Memory) Μνήμη Ανάγνωσης Μόνο. Ένας τύπος μνήμης, όπου τα δεδομένα που αρχικά έχουν εγγραφεί μπορούν μόνο να προσπελαστούν
RSA	(Rivest-Shamir-Adleman) Αλγόριθμος κρυπτογράφησης δημόσιου κλειδιού, ο οποίος πήρε το όνομά του από τους τρεις εφευρέτες του, τους Rivest, Shamir και Adleman
SAM	(Security Access Module) Άρθρωμα, το οποίο χρησιμοποιείται σαν τμήμα ενός τερματικού για την ασφαλή αποθήκευση κλειδιών και αλγορίθμων
SDA	(Static Data Authentication) Η μέθοδος ταυτοποίησης μίας κάρτας μέσω της ψηφιακής υπογραφής ενός αντιγράφου από επιλεγμένα δεδομένα της κάρτας
Secret Key	Μυστικό κλειδί. 1. Το κλειδί στην κρυπτογράφηση δημόσιου κλειδιού που πρέπει να παραμείνει μυστικό. 2. Το κλειδί στην κρυπτογράφηση συμμετρικού κλειδιού. Και σε αυτήν την περίπτωση, το κλειδί πρέπει να παραμείνει μυστικό
Session	Συνεδρία. Αναφέρεται στο χρόνο μεταξύ δύο reset μίας κάρτας ή στο χρόνο μεταξύ της τροφοδότησης (power up) και της διακοπής τροφοδοσίας (power down)
SET	(Secure Electronic Transaction) Ασφαλής Ηλεκτρονική Συναλλαγή. Πρωτόκολλο που αναπτύχθηκε από τη MasterCard και τη Visa για την κρυπτογραφημένη αποστολή αριθμών πιστωτικών καρτών μέσω του Διαδικτύου (Internet). Σύμφωνα με το SET, ο έμπορος δε μαθαίνει ποτέ τον αριθμό της πιστωτικής κάρτας, περιορίζοντας έτσι τον κίνδυνο της απάτης
SHA-1	(Secure Hash Algorithm 1) Πρότυπο του οργανισμού NIST των Η.Π.Α., το οποίο αναφέρεται στη δημιουργία κρυπτογραφικά ασφαλών κερμάτων (μικρών δεδομένων) από μεγαλύτερο σύνολο δεδομένων
Signed Applets	Υπογεγραμμένες Εφαρμογές. Αναφέρεται σε εφαρμογές Java ή Java Card, οι οποίες συνοδεύονται από ψηφιακή υπογραφή. Η υπογραφή αυτή αποδεικνύει την ταυτότητα του κατασκευαστή της εφαρμογής ή του διανομέα της
SIM	(Subscriber Authentication Module) Άρθρωμα Ταυτοποίησης Συνδρομητή
SMG9	(Special Mobile Group 9) Ομάδα ειδικών που καθορίζει τις προδιαγραφές των αλληλεπιδράσεων μεταξύ έξυπνων καρτών

	και κινητών τηλεφώνων
Super Smart Card	Υποδηλώνει μία έξυπνη κάρτα με ενσωματωμένα πολύπλοκα στοιχεία, όπως για παράδειγμα οθόνη απεικόνισης και αριθμητικό πληκτρολόγιο
SVC	(Stored-Value-Cards) Όρος που χρησιμοποιείται για τις προπληρωμένες κάρτες που έχουν προκαθορισμένη αξία και χρησιμοποιούνται μέχρι εξάντλησης της αξίας αυτής
TASI	(Terminal Application Services Interface) Ο τρόπος με τον οποίο μια εφαρμογή διασυνδέεται με τον «έξω κόσμο»
TC	(Transaction Certificate) Πιστοποιητικό Συναλλαγής
TTP	(Trusted Third Party) Έμπιστη Τρίτη Οντότητα
Transfer	Κάρτα μετακίνησης. Είναι μία έξυπνη κάρτα, η οποία χρησιμοποιείται ως μέσο μεταφοράς δεδομένων μεταξύ δύο οντοτήτων. Συνήθως περιέχει μία μεγάλη μνήμη δεδομένων για αυτό το σκοπό και τυπικά περιέχει κλειδιά για την ταυτοποίηση των οντοτήτων και των ενεργειών τους (ανάγνωση/εγγραφή δεδομένων)
Transmission Protocol	Πρωτόκολλο Μετάδοσης. Το σύνολο των κανόνων μετάδοσης που χρησιμοποιούνται για την μεταφορά δεδομένων μεταξύ τερματικού και έξυπνων καρτών
Verifier	Εφαρμογή η οποία επεξεργάζεται τον εισερχόμενο κώδικα και διασφαλίζει την συμβατότητά του με τις προβλεπόμενες προδιαγραφές ασφάλειας
Virgin Card	Κάρτα στην οποία δεν υπάρχει ακόμα ο μικροεπεξεργαστής και δεν έχει ακόμα προσωποποιηθεί
Volatile Memory	Ασταθής μνήμη. Αναφέρεται σε μνήμες, οι οποίες χάνουν τα δεδομένα τους, όταν διακοπεί η τροφοδοσία τους (όπως η μνήμη RAM ενός προσωπικού υπολογιστή)
VOP	(Visa Open Platforms) Πολυσήμαντο σύστημα αρχιτεκτονικής το οποίο επιτρέπει την ταχεία ανάπτυξη παγκόσμιων πρακτικών συστημάτων έξυπνων καρτών
White List	Λευκή λίστα. Η λίστα, συνήθως σε βάση δεδομένων, η οποία περιέχει όλες τις κάρτες που επιτρέπεται η χρήση τους σε ένα συγκεκριμένο σύστημα
WORM	(Write Once Read Many) Αναφέρεται στην μνήμη των έξυπνων καρτών που μπορεί να γίνει εγγραφή στην κάρτα μόνο μία φορά και να διαβαστεί πολλές

7.5. Παραπομπές για Έξυπνες Κάρτες και Συστήματα Ηλεκτρονικών πληρωμων

7.5.1. Smart Cards

IC Manufacturers

www.advancel.com
www.atmel.com/atmel/products/prod11.htm
www.dalsemi.com/Prod_info/Micros/Soft/index.html
www.halsp.hitachi.com/smartcard/ ,
www.hitachi-eu.com/hel/ecg/products/smartcard/index.htm
www.insidefr.com
www.microchip.com/10/Lit/Security/sCards/index.htm
www.mot-sps.com/csic/smartcard/
www.onsemi.com
www.semiconstructors.philips.com/identification/
www.sec-samsung.com/smartcard/
www.w2.siemens.de/semiconductor/products/ics/40/index.htm
www.st.com/stoneline/prodpres/
www.xicor.com/products/MemProd.htm
www.emosyn.com/emosyn2/home.nsf/Pages/sciron

Smart Cards Manufacturers

www.ammismartcards.com
www.cp8.bull.nte/
www.cardlogix .com/
www.digicard.co.at
www.gemplus.com
www.gdm.de/
www.chipcard.ibm.com
www.iris-card.com.my/
www.micromodule .com
www.mot.com/LMPS//RNSG/smartcard/
www.nbstech.com.
www.oberthursc.com
www.orga.com
www.oti.co.it
www.sec-samsung.com/smartcard/
www.slb.com/smatrdards/
www.wtx.com

Terminals Manufacturers

www.acs.com.hk/
www.amphenol-tuchel.com/
www.and.nl/id
www.cp8.bull.net/
www.delarue.com
www.eleacard.com/us_acc.htm
www.eletek .co.uk
www.fisc.com
www.gemplus.com
www.gis.co.uk
www.gdm.de/
www.hp.com/vectra500/ecommerce.html
www.hypercom .com
www.chipcard.ibm.com
www.ingenico .fr
www.innovonics .com
www.keycorp.com.au/products/eps/index.htm
www.litronic.com
www.muehlbauer.de/
www.nbstech.com/.
www.nric.co.kr/
www.orga .com
www.protekila.co.tr/
www.sec-samsung.com/smartcard/
www.slb.com/ms/let/
wwwscmmicro.com
www.smartmove.co.nz
www.trintech .com
www.tritheim .com
www.utimaco de/
www.verifone.com/

Smart Cards Integrator

www.3gi.com/
www.amdahl.com/smartcard/
www.and.nl/id/
www.card.co.uk/
www.autostar.com.sg/
www.bgs.at/
www.cr8.bull.net/
www.cardbase.com
www.cybermark.com/

www.delarue.com/
www.eps.no/
www.eximsoft .com/
www.gdm.de/
www.chopcard.ibm.com/
www.icone.com/
www.id-data.co.uk
wwwleapfrog-smart.com/
www.gpt.co.uk/
www.nbst.com/
www.linuxnet.com/
www.orga.com/
www.racom.com/
www.smartmove.co.nz/
www.spyrus.com/
www.transmo.demon.co.uk/
www.utimaco.de/
www.vasco.com/
www.verifone.com/
www.basiccard.com/

Smart Cards Software (OS, applications, access)

www.3gi.com/
www.acs.com.hk/
www.aks.com/ase.htm
www.amdahl.com/smartcard/
www.ammismartcards.com
www.basiccard.com/
www.cryptec.com/
www.epo.com/dsi/dsi.html
www.elea.com/us_acc.htm
www.eximsoft.com/
www.hp.com/vectra500/ecommerce.html
www.iccsolutions.com/
www.integri.be/
www.litronic.com/
www.microsoft.com/smartcard/
www.mot.com/sisc/smartcard/
www.scmmicro.com/
wwwthoic.com/keyblitz/html/tkp_card_explorer.html

Organisations

www.Card Europe
www.Global Chipcard Alliance
www.International Card Manufacturers Association
www.JavaCard Forum
www.SmartCard Developers Association
www.Smart Card Industry Association
www.The Smart Card Club
www.The SmartCard Forum

Standards

www.Multos
www.EMV (Europay-Mastercard-Visa) Specifications
www.JavaCard
www.OpenCard
www.PC/SC Workgroup
www.Standards Committees and Standards Related to Smart Cards

Λοιπά

www.home.hkstar.com/~alanchan/papers/smartCardSecurity/
www.geocities.comReaserchTriangle/Lab/1578/Smart.htm
www.cardtech.faulknergay.com/
www.datacard.com/
www.xxlink.nl/qcc/home/htm
www.smart-card.com/
www.sjbresearch.com/
www.smartcardcentral.com/
www.cardshow.com/
www.smartcard .co.uk/
www.ebooktech.com/english/
www.smartcardsearch.com/
www.insight-corp.com/beyond.html A market research report (μόνο η περίληψη είναι διαθέσιμη στο net)

7.5.2. Συστήματα Ηλεκτρονικών Πληρωμών

Credits Cards

www.americanexpress.com/
www.europay.com/
www.mastercard.com/

www.visa.com/

Digital Certificates

www.baltimore.ie/
www.bbn.com/products/security/cytrust/
www.digditrust.com/
www.entrust.com/
www.darmstadt.gmd/de/ice-tel/
www.netdox.com/
www.phaos.com/
www.utimaco.de/
www.verisign.com/

Electronic Cash

www.chipper.com/
www.cybercash.com/
www.digicash.com/
www.millicent .digital.com/
www.mondex.com/
www.okilab.com/
www.protonworld.cpm/
www.visa.com/visacash/

Internet Payment Systems

www.globeset.com/
www.econnectholdings.com/
www.trintech.com/

Secure Environments

www.cylink.com/
www.sse.ie/
www.s1.com/
www.utimaco.com/
www.v-one.com/

Standards

www.visa.com/cgi-bin/vee/nt/chip/download.html
www.setco.org/
www.opt.org/

Others

www.ehecks.org/
www.fv.com/ (Payment over the Internet)
www.ibutton.com/ (Dallas Semiconductor)

Γενικές Πληροφορίες

www.tis.com/research/crypto/crypt_surv.htm(TIS Research)
www.ctst.com/
www.fstc.org/
http://forum on risks to the public in computers and related systems
www.(acm)/(ACM)
http://catless.ncl.ac.uk/Risks/4.32.html
http://catless.ncl.ac.uk/Risks/15.56.html
http://catless.ncl.ac.uk/Risks/16.26.html
www. tc68.org/tc68/
http://ganges.cs/tcd.ie/mepeirce//project.html
http://payment www.mechanisms designed for the internet/
www.brp.com/
www.w3.org/pub//WWW/payments
www.x0.org/

Links

http://home.att.net/~s-prasad/ecsc.htm
http://cfec.vub.ac.be/cfec/purses.htm
http://www.bell-labs.com/www-buyinfo/
www.yahoo.com/Business_and_Economy/Electronic_Commerce/

Άλλες ενδιαφέρουσες σελίδες

www.dise.ucl.ac.be/crypto/cascade/index.html.
www.dise.ucl.ac.be/crypto/SCLAPS/sclaps.html. .
www.dise.ucl.ac.be/crypto/security.html.

8. Πηγές - Βιβλιογραφία

Η ανάπτυξη της εφαρμογής, έγινε με βάση το άρθρο που βρίσκεται στην ακόλουθη διεύθυνση:
http://www.javaworld.com/javaworld/jw-12-1997/jw-12-javadev.html

Το κεφάλαιο της ασφάλειας καρτών, βασίστηκε στις έξης διευθύνσεις:
http://www.gammassl.co.uk/topics/smart%20cards/esmart2002.html
http://www.conta.uom.gr/conta/ekpaideysh/metaptyxiaka/e_commerce/ergasies/2002/Kagkani/SmartCards.pdf

Οι παραπομπές έχουν βασιστεί σε:
http://www.dice.ucl.ac.be/crypto/card.html

Μεγάλο μέρος της εργασίας στηρίχθηκε σε πληροφορίες που πάρθηκαν από δημοσιεύσεις που βρίσκονται στην σελίδα του e-business forum:
http://www.ebusinessforum.gr/index.php?op=modload&modname=Calendar

Επιμέρους πληροφορίες πάρθηκαν και από τις παρακάτω διευθύνσεις (καθώς επίσης και από διάφορες άλλες οι οποίες δεν αναφέρονται στην παρούσα βιβλιογραφία):

www.gemplus.com
www. Hackersrussia.ru/Cards/
www.smartcards.net/
www.smartcard.co.uk/
www.citi.umich.edu/projects/smartcard/
www.eeurope-smartcards.org/
www.smartcardalliance.org/
www.go-online.gr/
www.citi.umich.edu
www.design-engine.com
www.digitalsima.gr
java.sun.com

- Smart cards: a youthful market
- Deborah Fain, Mary Lou Roberts (1997) "Technology vs. Consumer Behavior: the battle for the Financial Servises Customer GCR680 Reference Manual"
- GCL8K Technical Specifications
- CL8K Evaluation Kit
- Bidgoli Hossein, "*Electronic Commerce, Principles and Practice*", Academic Press, USA, 2002