

Έξυπνες Κάρτες - Smart Cards



- Βασικές Έννοιες
- Εφαρμογές
- Πρότυπα
- Ορολογία



Βασικές Έννοιες Ορισμός έξυπνων καρτών

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 μικροσκοπικοί 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. Το ολοκληρωμένο κύκλωμα μπορεί να παρέχει 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 έναν ασφαλή τρόπο. Τα πλεονεκτήματα των έξυπνων καρτών είναι η προστασία των δεδομένων που περιέχουν, η φορητότητα και η ευκολία χρήσης.

Προκειμένου το ολοκληρωμένο να μπορεί να χρησιμοποιηθεί και σε τερματικά ή αναγνώστες τα οποία δεν έχουν το απαιτούμενο μέγεθος για την εισαγωγή ολόκληρης της κάρτας, είναι δυνατή η παραγωγή των καρτών με εγκοπές γύρω από το ολοκληρωμένο, προκειμένου αυτό να αφαιρείται και να τοποθετείται στην τερματική συσκευή. Κλασσικό παράδειγμα οι κάρτες SIM.

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 πολύ 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).

Είδη έξυπνων καρτών

Στις μέρες μας, οι έξυπνες κάρτες μπορούν να κατηγοριοποιηθούν με δύο βασικά κριτήρια:

- α) επεξεργαστική ικανότητα και
- β) δυνατότητες εισόδου-εξόδου.

Με βάση το πρώτο κριτήριο, διακρίνουμε τρεις κατηγορίες έξυπνων καρτών:

- ❶ 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.
- ❷ 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.
- ❸ 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.

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:

- ❶ 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.



- **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.
- **3. Υβριδικές κάρτες ή συνδυασμένες κάρτες (Hybrid or 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)

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.** Οι συσκευές αυτές δε φέρουν εξοπλισμό και συνδέονται σε τερματικές συσκευές οι οποίες δε διαθέτουν αναγνώστη έξυπνων καρτών (H/Y, info kiosks, controllers κ.α.).

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.

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.

Παρουσιάζουμε στη συνέχεια μερικά παραδείγματα όπου χρησιμοποιούνται οι έξυπνες κάρτες για να γίνει πιο κατανοητή η αξία και η χρησιμότητά τους.

1. 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.

¹ URL: <http://www.mondex.com>
² URL: <http://www.visa.com/pd/ewallet/main.html>

2. Κάρτα διατηρησιμότητας & εξυπηρέτησης πελατών (loyalty cards)

Οι επιχειρήσεις λιανικού εμπορίου έχουν τη δυνατότητα να χρησιμοποιούν τις έξυπνες κάρτες προκειμένου να εξυπηρετούν ποιο 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.



3. 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 Michigan³ 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.

4. 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.

5. 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.

³ URL: <http://www.mcard.umich.edu/>



Οι EMV κάρτες θα αντικαταστήσουν τις πιστωτικές και χρεωστικές κάρτες μαγνητικής πίστας, 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.

6. 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 και στο 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.

7. 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 σε ένα δίκτυο και να μπορούν να υπογράψουν ηλεκτρονικά έγγραφα με δικονομική αξία ίση με αυτήν της ιδιόχειρης υπογραφής τους στα έντυπα έγγραφα.

Για την εφαρμογή των παραπάνω είναι απαραίτητες τρεις διακριτές οντότητες:

- ▶ α. **Πάροχος Υπηρεσιών Πιστοποίησης** (Έμπιστη Τρίτη Οντότητα)
- ▶ β. **Τελική οντότητα**, συνήθως παροχέας υπηρεσιών ασφαλούς δικτύου στους πελάτες του (π.χ. Τράπεζα)
- ▶ γ. **Τελικός χρήστης** (π.χ. πελάτης Τράπεζας)

8. 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 (GSM κάρτες) μορφή τους.

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

9. Άλλες εφαρμογές

Άλλες εφαρμογές των έξυπνων καρτών είναι η χρήσης τους σε αποκωδικοποιητές, Internet access, product tracking, δίπλωμα οδήγησης (ιδανική για αποθήκευση penalty points και άμεση αφαίρεση του διπλώματος), κ.α.

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 χρησιμοποιώντας το internet από το σπίτι	- Πιστωτικές κάρτες - Χρεωστικές κάρτες		
Τηλεπικοινωνίες	Προπληρωμένη τηλεκάρτα		Αποθήκευση αριθμού		Κάρτες SIM/GSM			
Δημόσιος Τομέας	- Διαχείριση λογαριασμών (συντάξεις, επιδόματα, κ.τ.λ) - Προηγμένες ηλεκτρονικές υπογραφές σε ηλεκτρονικά έγγραφα				- Διαβατήριο - Ταυτότητα - Διπλώμα οδήγησης			
Μεταφορές	- Ηλεκτρονικά εισιτήρια - Αυτόματη πληρωμή διόδων - Πληρωμές μεταφορικών μέσων (λεωφορείο, ταξί, τρένο, κ.τ.λ)				Κάρτα επιβίβασης			
Υγεία	- Πληρωμές ασφαλείας - Ιατρικές πληρωμές		- Αποθήκευση/ανάκτηση ιατρικού ιστορικού - Αποθήκευση πληροφοριών δότη			Κάρτα 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. χάρους 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 - Πρόσβαση σίθουσα λέσχης αεροδρομίου (lounge)/ σίθουσα αναχώρησης - Κλεδιά δωματίου σε ξενοδοχείο - Πρόσβαση στο διαδίκτυο - Πρόσβαση σε κτίρια - Πρόσβαση σε δίκτυα - Κλεδιά ενοικίασης αυτοκινήτου	- Πρόγραμμα Frequent traveler - Κάρτα διατηρησιμότητας & εξυπηρέτησης πελατών (loyalty cards)				



Ασφάλεια και Πλεονεκτήματα

Επιχειρήσεις

- Περριρισμός οικονομικού εγκλήματος
- Αποδοτικότητα και αποτελεσματικότητα πωλήσεων

Πελάτες

- Προσφέρουν μεγαλύτερη ασφάλεια
- Μια έξυπνη κάρτα πολλοπλών εφαρμογών προσφέρει ευκολία
- Επιτρέπει την συμμετοχή σε προγράμματα rewards και loyalty
- Επιτρέπει αποθήκευση και πρόσβαση σε απαραίτητη πληροφορία

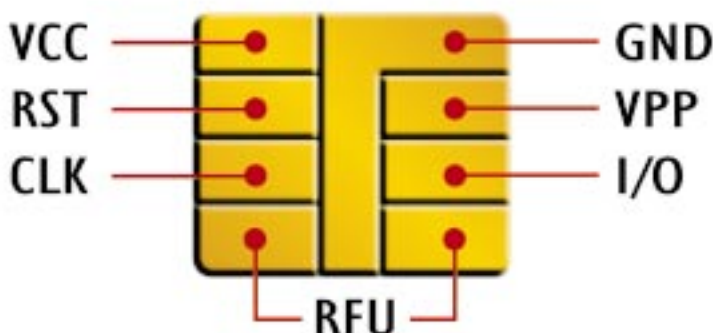
- Χαρακτηριστικό ανοχής σε κακόβουλους χειρισμούς (tamper-resistant)
- Μπορούν να ανιχνεύσουν και να αντιδράσουν σε κακόβουλους χειρισμούς (tamper-proof)
- Ενσωματώνουν τις ραγδαίες εξελίξεις στην τεχνολογία ημιαγωγών, επιτρέποντας τη συνεχή βελτίωση των χαρακτηριστικών τους
- Ως επί το πλείστον είναι επαναπρογραμματιζόμενες
- Διαθέτουν δυνατότητες υπολογισμού και πράξεων (computing & calculating)
- Διαθέτουν κυκλώματα λογικής και μνήμης
- Επεξεργάζονται δεδομένα και αποθηκεύουν πληροφορίες
- Μπορούν να συγκρίνουν και να διαχειρίζονται σύνθετες πληροφορίες
- Συνήθως χρησιμοποιούνται για εφαρμογές μεγάλης ασφάλειας (high security)
- Επιτρέπουν off-line εξακριβωση των στοιχείων, σε αντίθεση με μία κάρτα με μαγνητική λωρίδα
- Δίνουν δυνατότητα επιλογής στο ποια στοιχεία της κάρτας είναι πρόσβαση από διαφορετικές εφαρμογές
- Επιτρέπουν μεγάλη ασφάλεια, και αυτό οφείλεται στις πολύπλοκες κρυπτογραφικές τεχνικές που χρησιμοποιούνται για να κωδικοποιούν και αποκωδικοποιούν την "κυκλοφορία" της πληροφορίας μεταξύ έξυπνων καρτών και άλλων συσκευών
- Προσφέρουν μεγάλη χωρητικότητα αποθήκευσης πληροφοριών
- Είναι συμβατές με φορητές ηλεκτρονικές συσκευές

Παράρτημα Α

Πρότυπα και κατευθύνσεις για έξυπνες κάρτες

1. Γενικά

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



Από τις παραπάνω επαφές, μόνο η I/O και η Ground είναι απαραίτητες για την κάρτα και πρέπει να ακολουθούν τα διεθνή πρότυπα, όλες οι υπόλοιπες είναι προαιρετικές.

2. Πρότυπα

Η αυξανόμενη χρήση των έξυπνων καρτών και η διείσδυσή τους σε διάφορες εφαρμογές και επιχειρηματικά μοντέλα, έχει οδηγήσει έγκυρους οργανισμούς στον ορισμό ανοικτών προτύπων σχετικά με τις έξυπνες κάρτες. Τα ανοικτά πρότυπα εγγυώνται τη διαλειτουργικότητα των σχετικών προϊόντων σε όλα τα επίπεδα, εντείνοντας την ανταγωνιστικότητα και τη συμβατότητα μεταξύ διαφορετικών κατασκευαστών. Τα σχετικά πρότυπα δημιουργούνται τόσο από οργανισμούς, όπως για παράδειγμα οι ISO, CEN και ETSI, όσο και από συνασπισμούς εταιρειών με κοινό πεδίο εφαρμογών, όπως για παράδειγμα τα EMV, SET, PC/SC, OCF, και PKCS.

Τα πρότυπα αυτά εγγυώνται τη διαλειτουργικότητα σε όλο το φάσμα των εφαρμογών που χρησιμοποιούνται οι έξυπνες κάρτες, από το επίπεδο των φυσικών χαρακτηριστικών (διαστάσεις, τάση λειτουργίας, κτλ) έως και τα πρωτόκολλα και αρχιτεκτονικές για την ανταλλαγή δεδομένων εφαρμογών (π.χ. οικονομικές συναλλαγές και ιατρικά δεδομένα). Ο ενδιαφερόμενος αναγνώστης παραπέμπεται στο URL:

http://www.ebusinessforum.gr/omades_new/intro.php?group=8

για μία εκτενή συλλογή όλων των σχετικών προτύπων που αναφέρονται σε έξυπνες κάρτες.



Παράρτημα Β

Ευρετήριο ορολογίας Έξυπνων Καρτών

ABS

(Acrylonitrile Butadiene Styrene) Ακρυλονιτρικό Βουτανιδικό Στυρένιο. Το πλαστικό που χρησιμοποιείται για την έγχυση των σκελετών των καρτών για διάφορες κάρτες

Acceptor

Αποδοέας. 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 “επιστημοποίηση” 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 περισσότερων 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 κατάχου

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 σχετική 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 κάτοχος 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 τέτοιο τρόπο, ώστε να συμπεριλαμβάνει και τις κάρτες μνήμης, οι οποίες δεν έχουν “έξυπνάδα”

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 πλαστική 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 κυψελαιοδούς 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 κλειδίων και την (εσωτερική) εκτέλεση κρυπτογραφικών λειτουργιών, καθοδηγούμενη από έναν υπολογιστή

Hybrid Card

Υβριδική Κάρτα. Τύπος έξυπνης κάρτας που χρησιμοποιεί δύο διαφορετικά μέσα επικοινωνίας. Πβ. Dual Interface Card

ID-I card

Έξυπνη Κάρτα με προτυποποιημένες κατά ISO διαστάσεις.

IFD

(Interface Device) Άλλη ονομασία του αναγνώστη έξυπνης κάρτας

Initialization

Το πρώτο στάδιο της διαδικασίας έκδοσης καρτών. Ο σκοπός αυτής της διαδικασίας είναι το φόρτωμα των δεδομένων από την εφαρμογή στις έξυπνες κάρτες

Intelligent memory card

Ευφυής κάρτα μνήμης. Κάρτα μνήμης με συμπληρωματικό λεπτομερές λογικό σχέδιο κυκλώματος που επιτρέπει/παρέχει επιπρόσθετες λειτουργίες ασφαλείας που καταγράφουν τη χρήση της μνήμης

Integrity

Ακεραιότητα. Αναφέρεται στις μεθόδους και διαδικασίες που διασφαλίζουν ότι οι πληροφορίες έχουν τροποποιηθεί μόνο από τις οντότητες που έχουν την αντίστοιχη εξουσιοδότηση

Interoperability

Διαλειτουργικότητα. Η δυνατότητα συστημάτων διαφορετικών κατασκευαστών να αλληλεπιδρούν μεταξύ τους.

ISO

(International Standards Organization) Ο οργανισμός ISO μεταξύ άλλων εργάζεται στην περιοχή των έξυπνων καρτών, με σκοπό να εξασφαλίσει, μέσω των προτύπων που ορίζει, ότι οι κατασκευαστές των ολοκληρωμένων, οι προγραμματιστές και οι εταιρείες έξυπνων καρτών ακολουθούν τις ίδιες προδιαγραφές

ITSO

(Integrated Transport Smart Card Organisation) Οργανισμός ο οποίος ιδρύθηκε στο Ηνωμένο Βασίλειο για να βοηθήσει την εξάπλωση των συστημάτων έξυπνων καρτών στα μέσα μαζικής μεταφοράς

ITU

(International Telecommunications Union) Οργανισμός που συντονίζει, προτυποποιεί και δημιουργεί παγκοσμίως τηλεπικοινωνιακές υπηρεσίες



Java Card

Μία προδιαγραφή για την εκτέλεση ενός υποσυνόλου της γλώσσας Java σε μία έξυπνη κάρτα

JCRE

(Java Card Runtime Environment) Το περιβάλλον εκτέλεσης στο οποίο εκτελείται η Java Card. Το JCRE είναι υπεύθυνο για όλες τις διαχειριστικές ενέργειες, όπως η φόρτωση και η αρχικοποίηση των εφαρμογών

Key management

Διαχείριση κλειδιών. Όλες οι διαχειριστικές λειτουργίες που σχετίζονται με την δημιουργία, διανομή, αποθήκευση, ενημέρωση των κρυπτογραφικών κλειδιών

Key escrow

Η μέθοδος κατάθεσης του ιδιωτικού κλειδιού σε τρίτον, συνήθως για τη διασφάλιση της ανάκτησης των δεδομένων τα οποία έχουν κρυπτογραφηθεί ή υπογραφεί με το ιδιωτικό κλειδί. Η κατάθεση του ιδιωτικού κλειδιού, ειδικά στην περίπτωση της χρήσης για ηλεκτρονικές υπογραφές, απαγορεύεται στις περισσότερες έννομες τάξεις.

Lifecycle

Κύκλος ζωής. Αναφέρεται στα στάδια επεξεργασίας και λειτουργίας μίας έξυπνης κάρτας, από τη στιγμή της κατασκευής του ολοκληρωμένου της, έως την απόσυρση από τη χρήση και καταστροφή της

MAC

(Message Authentication Code) Κώδικας Ταυτοποίησης Μηνύματος. Διαδικασία, συνήθως με τη χρήση αλγόριθμων κρυπτογράφησης, η οποία εγγυάται ότι το μήνυμα προέρχεται από τον πρωτότυπο παραλήπτη του και δεν έχει αλλαχθεί στην πορεία

Magnetic Strip Card

Κάρτα με μαγνητική λωρίδα, πάνω στην οποία δεδομένα μπορεί να καταχωρηθούν και να διαβαστούν

Memory card

Κάρτα μνήμης. Αναφέρεται σε κάρτες που περιέχουν μόνο μνήμη και επιλεκτικά και λογική ενσωματωμένη στο υλικό (hardwired logic). Χρησιμοποιείται σε αντιδιαστολή με τον όρο chip card ή smart card, όπου υποδηλώνεται η ικανότητα επεξεργασίας

MF

(Master File) Αποτελεί το βασικό κατάλογο του δένδρου αρχείων που υλοποιεί τη λογική οργάνωση της μνήμης μίας έξυπνης κάρτας. Το Κύριο Αρχείο επιλέγεται αυτόματα κάθε φορά που εκκινεί η έξυπνη κάρτα

Microprocessor Card

Κάρτα με μικροεπεξεργαστή. Κάρτα η οποία περιλαμβάνει: επεξεργαστή (CPU), μνήμης (RAM, ROM, EEPROM) και επιλεκτικά αριθμητικό συνεπεξεργαστή (NPU, numerical coprocessor), κάτι που επιτρέπει την άμεση εκτέλεση των αλγορίθμων. Χρησιμοποιείται σε αντιδιαστολή με τον όρο "Κάρτα Μνήμης" (Memory Card).

Mono-application smart card

Έξυπνη κάρτα μοναδικής εφαρμογής. Κάρτα που έχει τη δυνατότητα να εκτελέσει μία μόνο εφαρμογή, συνήθως προεγκατεστημένη σε αυτή

Mono-functional smart card

Έξυπνη κάρτα μοναδικής λειτουργίας. Κάρτα της οποίας το λειτουργικό σύστημα υποστηρίζει μόνο μια συγκεκριμένη εφαρμογή

Multi-application smart card

Έξυπνη Κάρτα Πολλαπλών Εφαρμογών. Αναφέρεται σε έξυπνες κάρτες νεότερης γενιάς, οι οποίες έχουν τη δυνατότητα να εκτελούν πολλές 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 μικροεπεξεργαστή. 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 αδρανποίησης. 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) Διάρθρωμα, 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