Συστήματα Ηλεκτρονικών Πληρωμών: ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ

Φελλά Αντιγόνη
Παπαπαύλου Αργυρή
ΤΜΗΜΑ ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΣΤΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΟΙΚΟΝΟΜΙΑ
Τ.Ε.Ι. ΜΕΣΟΛΟΓΓΙΟΥ

ΠΕΡΙΕΧΟΜΕΝΑ

Κεφάλαιο 3ο

Λειτουργία έξυπνων καρτών

Κεφάλαιο 4ο

Λογισμικό έξυπνων καρτών

Κεφάλαιο 5ο

Αναγνώστες έξυπνων καρτών

Κεφάλαιο 6ο

Βιομετρική

Κεφάλαιο 7ο

Ασφάλεια

Κεφάλαιο 8ο

Κρυπτογραφία

Κεφάλαιο 9ο

Υποκλοπή

Κεφάλαιο 10ο

Συμπεράσματα

ΕΙΣΑΓΩΓΗ

Από την εμφάνιση του ανθρώπινου γένους πάνω στη γη εμφανίστηκε η ανάγκη επικοινωνίας. Οι άνθρωποι άρχισαν να ζουν σε οργανωμένες κοινωνίες. Με το καιρό κατάλαβαν ότι για να επιβιώσουν και να επικοινωνήσουν μέσα σ' αυτές έχει ο ένας την ανάγκη του άλλου.

Με το καιρό διαπίστωσαν ότι η ανταλλαγή αγαθών για την ικανοποίηση των αναγκών τους, δεν ήταν ο πιο δίκαιος τρόπος. Εξαιτίας του προβλήματος αυτού, χρειάστηκε να βρουν ένα κοινά αποδεκτό τρόπο έτσι ώστε οι συναλλαγές αυτές να είναι δίκαιες. Ξεκινώντας, λοιπόν, από την ανταλλαγή των προϊόντων έφτασαν σε σημείο να χρησιμοποιήσουν τα χρήματα, με τη μορφή των κερμάτων και αργότερα των χαρτονομισμάτων. Είναι λογικό, εξαιτίας της έμφυτης ανάγκης του ανθρώπου για εξέλιξη, ο τρόπος αυτός συναλλαγής να εξελιχθεί. Φτάνοντας στη σημερινή εποχή, το χρήμα τείνει να αντικατασταθεί με διάφορα άλλα μέσα, όπως οι πιστωτικές κάρτες, οι τηλεφωνικές κάρτες, οι κάρτες διοδίων κ.τ.λ.

Πλέον, αντί να κρατάμε επάνω μας χαρτονομίσματα, το νέο «πορτοφόλι» θα αποθηκεύει ψηφιακό χρήμα που είναι αδύνατο να παραχαραχθεί. Σήμερα, όταν δίνεται ένα χαρτονόμισμα, μία επιταγή, μία διατακτική δώρου, κ.λ.π. η μεταβίβαση χρήματος αντιπροσωπεύει μεταβίβαση κεφαλαίου. Αλλά το χρήμα δεν είναι απαραίτητο να εκφράζεται σε χαρτί. Μπορεί να εκφραστεί με τη μορφή πιστωτικής κάρτας, τηλεφωνικής κάρτας, κάρτας SIM κ.λ.π., οι οποίες ανήκουν στις πιο συνηθισμένες κατηγορίες έξυπνων καρτών.

Σήμερα, η εξέλιξη των έξυπνων καρτών είναι ραγδαία αφού χρησιμοποιούνται ευρέως σε όλες σχεδόν τις καθημερινές δραστηριότητες. Επίσης, είναι σημαντικό το γεγονός ότι μια έξυπνη κάρτα μπορεί να χρησιμοποιηθεί

για πολλές εφαρμογές ταυτοχρόνως, αφού μπορείτε να ταξιδεύσετε μ' αυτήν, να τη χρησιμοποιείτε ως αποδεικτικό πληρωμής της εισόδου σας στο θέατρο, σε βιβλιοθήκες, σε κτίρια υψηλής ασφαλείας(π.χ. σε στρατιωτικές βάσεις) και ό,τι άλλο μπορείτε να φανταστείτε. Σε λίγα χρόνια, χάρη στο προσωπικό υπολογιστή τσέπης, όλοι θα μπορούν να συναλλάσσονται με ψηφιακό χρήμα. Το ψηφιακό χρήμα θα χρησιμοποιείται και για διαπροσωπικές συναλλαγές.

Καθώς θα καταργούνται σιγά- σιγά τα μετρητά και οι πιστωτικές κάρτες, οι εγκληματίες θα βάζουν στόχο τις έξυπνες κάρτες και επομένως, θα πρέπει να υπάρχει ασφάλεια που θα εμποδίζει να χρησιμοποιηθούν με τον ίδιο τρόπο που μπορεί να χρησιμοποιηθεί σήμερα μία κλεμμένη πιστωτική κάρτα. Μέσα στις κάρτες αυτές θα είναι αποθηκευμένα τα κλειδιά που θα χρησιμοποιείται για να προσδιορίσετε την ταυτότητά σας. Θα μπορείτε εύκολα να ακυρώνετε τα κλειδιά σας και να τα αλλάζετε τακτικά. Την ώρα ορισμένων σημαντικών συναλλαγών θα χρειάζεται, ίσως, να πληκτρολογήσετε ένα συνθηματικό. Οι αυτόματες ταμειακές μηχανές σας ζητούν να δώσετε το προσωπικό κωδικό αριθμό σας, δηλαδή ένα σύντομο συνθηματικό. Άλλη δυνατότητα που θα καταργεί την ανάγκη να θυμάστε κάποιο συνθηματικό, θα είναι η χρήση βιομετρικών μέτρων- όπως η αποτύπωση της φωνής ή το δακτυλικό αποτύπωμα. Τα ατομικά βιομετρικά μέτρα είναι ασφαλέστερα και είναι σχεδόν βέβαιο, ότι θα προστατεύουν τις έξυπνες κάρτες.

Η ασφάλεια των πληροφοριών και των ευαίσθητων προσωπικών δεδομένων διαδραματίζει σημαντικό ρόλο στην εξέλιξη και τη λειτουργία των έξυπνων καρτών. Αυτό είναι ένα θέμα που απασχολεί τη τεχνολογική κοινωνία και απ' ότι φαίνεται θα συνεχίσει να την απασχολεί και για αρκετά χρόνια αργότερα.

ΚΕΦΑΛΑΙΟ 1ο

ΣΥΣΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ

1. Η εμφάνιση της κοινωνίας χωρίς μετρητά

Στο σύγχρονο κόσμο, η διαδεδομένη χρήση των μετρητών υπό μορφή χαρτονομισμάτων και νομισμάτων φαίνεται όλο και περισσότερο να εμποδίζει την αποτελεσματική επέκταση των νέων μορφών εμπορικών συναλλαγών. Είναι απόλυτα σαφές ότι η ηλεκτρονική αποθήκευση και η μεταφορά της αξίας των χρημάτων είναι αναγκαία, ιδιαίτερα όπου οι χαμηλής αξίας πληρωμές απαιτούν να γίνουν διεθνής .

Η εικονική εξάλειψη των μετρητών είναι, επομένως, ιερό ποτήριο των εθνικών κυβερνήσεων, των εμπόρων Διαδικτύου και των χρηματοδοτικών οργανισμών, με ένα πραγματικό ενδιαφέρον για τον έλεγχο και το όφελος από εκείνο το 80% των δαπανών των κεντρικών οδών που γίνονται αυτήν την περίοδο με τα χαρτονομίσματα και τα νομίσματα. Τέτοια ηλεκτρονικά χρήματα μπορούν να λάβουν πολλές μορφές και έχουν χρηματοδοτηθεί με ένα ευρύ και παραπλανητικό λεξιλόγιο, συμπεριλαμβανομένης της αποθηκευμένης αξίας και του ηλεκτρονικού πορτοφολιού. Αυτό έχει οδηγήσει στην ανάπτυξη, από διάφορους οικονομικούς οργανισμούς, προϊόντων βασισμένων στις έξυπνες κάρτες που εκτελούν τις λειτουργίες αποθηκευμένης αξίας.

Μέχρι σήμερα, η ενιαία λειτουργία, γενικά των καρτών που λειτουργούν σαν ηλεκτρονικά πορτοφόλια και εκδίδονται από τους οικονομικούς οργανισμούς στα ποικίλα προγράμματα σε διάφορες χώρες, έχει οδηγήσει στην τεχνική επιτυχία αλλά και στην εμπορική αποτυχία από την άποψη

του ποσοστού χρήσης, Η αξία του προπληρωμένου σώματος είναι ελκυστική στις τηλεπικοινωνίες, στους χειριστές μεταφορικών μέσων και στους λιανοπωλητές, ενώ οι τράπεζες μάχονται τώρα για να υποστηρίξουν αυτή τη νομοθεσία..

Ακόμη και μέσα στη τραπεζική κοινότητα, ασυμβίβαστες και ανταγωνιστικές αρχιτεκτονικές πορτοφολιών πολλαπλασιάζονται με τα ανώνυμα και μη εκτιμημένα προϊόντα, όπως το Mondex (που ανήκει στη Master Card), ενάντια στα πλήρως εκτιμημένα συστήματα στο χώρο της Visa. Οι ευρωπαϊκές πρωτοβουλίες εδραιώνονται κάτω από την Κοινή Προδιαγραφή των Ηλεκτρονικών πορτοφολιών (CEPS). Μέχρι σήμερα, πάνω από 80 εκατομμύρια κάρτες-ηλεκτρονικών πορτοφολιών στην Ευρώπη χρησιμοποιούνται, κατά μέσον όρο, μόνο μία φορά κάθε έξι εβδομάδες. Αυτό είναι μια αντανάκλαση της τρέχουσας εμπορικής αποτυχίας τέτοιων πρωτοβουλιών.

2. Τρέχουσες διαδικασίες ηλεκτρονικής πληρωμής

Δεν είναι δυνατό να υπάρξει ηλεκτρονικό εμπόριο χωρίς έναν τρόπο μεταφοράς χρηματικών πόρων (πληρωμής) μέσω της ψηφιακής υποδομής. Κάθε σύστημα ηλεκτρονικής πληρωμής θα πρέπει να καλύπτει όλα τα χαρακτηριστικά που οι διάφορες πλευρές μιας συναλλαγής θεωρούν ως απαραίτητα ή σημαντικά. Σε μια ηλεκτρονική συναλλαγή εμπλέκονται συνήθως τρία μέρη: ο έμπορος (πωλητής), ο πελάτης (αγοραστής), και αυτός που παρέχει οικονομικές υπηρεσίες (οργανισμός πιστωτικών καρτών).

Έμπορος

Το σημαντικότερο χαρακτηριστικό ενός συστήματος πληρωμής, από την πλευρά του εμπόρου, είναι η ευκολία της χρήσης του από τον πελάτη. Ο πελάτης θα πρέπει να έχει τη δυνατότητα να κάνει παρορμητικές αγορές, χωρίς να εμποδίζεται από δυσκολίες που οφείλονται αποκλειστικά στο σύστημα πληρωμής. Ένας από τους λόγους, που ο έμπορος έχει υιοθετήσει το ηλεκτρονικό εμπόριο είναι ότι μπορεί να διευρύνει τη βάση των πελατών

του. Αν το σύστημα πληρωμής περιορίζει αυτή τη βάση, το κίνητρο αναιρείται. Έτσι, μια από τις προϋποθέσεις ενός συστήματος ηλεκτρονικής πληρωμής είναι η ευρεία αποδοχή του.

Ένα δεύτερο χαρακτηριστικό είναι το κόστος των συναλλαγών. Ο έμπορος επιθυμεί να έχει μικρό κόστος συναλλαγών ώστε να μπορεί να μειώσει τις τιμές των προϊόντων και να αυξήσει την ανταγωνιστικότητά του. Ένα μέρος του κόστους συναλλαγών είναι η αμοιβή του οικονομικού οργανισμού που ενεργεί στις ηλεκτρονικές πληρωμές. Άλλα στοιχεία του κόστους συναλλαγών είναι ο απαιτούμενος χρόνος για την ολοκλήρωση μιας συναλλαγής και ο κίνδυνος επισφαλών συναλλαγών.

Πελάτης

Πολλά από τα παραπάνω χαρακτηριστικά αφορούν εξίσου τον πελάτη. Ο πελάτης θέλει να αισθάνεται ότι είναι ασφαλής και ότι δεν θα πέσει θύμα απατεώνων που θα εκμεταλλευτούν τις πληροφορίες, σχετικά με την ηλεκτρονική πληρωμή του π.χ. αριθμός πιστωτικής κάρτας. Επίσης, θα πρέπει να μπορεί να κάνει ηλεκτρονικές πληρωμές με το ίδιο σύστημα και με την ίδια ευκολία σε πολλούς εμπόρους, όχι μόνο για να έχει τη δυνατότητα επιλογής αλλά και για να αποφεύγει την ταλαιπωρία της εκμάθησης πολλών διαφορετικών μεθόδων πληρωμής. Οι πελάτες δεν μπορούν να ανεχθούν κανένα πρόσθετο κόστος στις συναλλαγές τους, είτε αυτό είναι σε χρήμα είτε σε χρόνο.

Οργανισμός οικονομικών υπηρεσιών

Οι οργανισμοί που υποστηρίζουν ηλεκτρονικές πληρωμές, όπως οι οργανισμοί πιστωτικών καρτών, έχουν ως σκοπό το κέρδος. Έτσι, κάθε συναλλαγή που χρησιμοποιεί ως ενδιάμεσο ένα τέτοιο οργανισμό επιβαρύνεται με την αμοιβή του οργανισμού. Φυσικά, για να κρατούν τις υπηρεσίες τους ελκυστικές, οι οργανισμοί οικονομικών υπηρεσιών κρατούν το κόστος κάθε συναλλαγής αρκετά χαμηλό και προσπαθούν να αυξήσουν τα κέρδη τους με την διεύρυνση της χρήσης των μέσων πληρωμής που προσφέρουν. Ένα πρόβλημα στο σημείο αυτό είναι η δυσπιστία εμπόρων και καταναλω-

τών προς τους οικονομικούς οργανισμούς που μονοπωλούν κάποιο μέσο πληρωμής.

Η λύση είναι η δημιουργία ενός κοινού μέσου πληρωμής που να υποστηρίζεται από πολλούς οργανισμούς, ώστε να εξασφαλίζεται μια ανταγωνιστική αγορά οικονομικών υπηρεσιών. Ο ανταγωνισμός μπορεί να οδηγήσει στη μείωση του κόστους συναλλαγών και στην προσφορά πρόσθετων υπηρεσιών, που είναι προς το κοινό όφελος καταναλωτών και εμπόρων.

Μια από τις υπηρεσίες προστιθέμενης αξίας που αναλαμβάνουν οι οργανισμοί οικονομικών υπηρεσιών, στα πλαίσια του μεταξύ τους ανταγωνισμού, είναι η διαχείριση των κινδύνων συναλλαγής. Στη διάρκεια μιας ηλεκτρονικής συναλλαγής υπάρχουν πολλοί παράγοντες που μπορεί να προκαλέσουν μια αποτυχία. Για παράδειγμα, ο πωλητής μπορεί να μην λάβει την πληρωμή, ο αγοραστής να μην λάβει το προϊόν για το οποίο ήδη έχει πληρώσει, ενώ τα στοιχεία της πληρωμής μπορούν να υποκλαπούν ή να παραποιηθούν για παράνομους σκοπούς. Ο οικονομικός οργανισμός μπορεί να καλύψει όλους αυτούς τους κινδύνους, όπως να εγγυηθεί στον πωλητή την κάλυψη του ποσού πληρωμής, να βεβαιώσει στον αγοραστή την είσπραξη του ποσού από τον πωλητή και να φροντίσει για την απαραίτητη τεχνολογική υποδομή που θα προστατεύσει τις πληροφορίες από υποκλοπή ή παραποίηση. Δυο πολλοί μεγάλοι οργανισμοί που προσφέρουν τέτοιες υπηρεσίες διαχείρισης του κινδύνου είναι οι γνωστοί οργανισμοί πιστωτικών καρτών Visa και MasterCard.

3. Πρότυπα και μέθοδοι ηλεκτρονικής πληρωμής

Όλα τα συστήματα ηλεκτρονικής πληρωμής πρέπει να περιλαμβάνουν την έννοια της χρηματικής αξίας και από την άποψη αυτή οι μέθοδοι που χρησιμοποιούνται πρέπει να είναι ισοδύναμες με τις υπάρχουσες συνθήκες πληρωμής: το «ηλεκτρονικό χρήμα» θα πρέπει να είναι ανταλλάξιμο με κάθε άλλη μορφή χρήματος. Θα πρέπει να είναι δυνατή η αποθήκευση και η ανάκτηση, αλλά όχι η αναπαραγωγή του. Λόγω της φύσης του ηλεκτρονικού χρήματος (ψηφιακές πληροφορίες αποθηκευμένες σε κάποιο

μέσο), οι διαδικασίες ηλεκτρονικής πληρωμής θα πρέπει να προστατεύουν όλες τις συμβαλλόμενες πλευρές από κάθε εξωτερική επέμβαση στις πληροφορίες αυτές.

Εκτός από τις παραπάνω θεμελιώδεις ιδιότητες του χρήματος, ένα σύστημα ηλεκτρονικής πληρωμής πρέπει επίσης να διαθέτει τα εξής χαρακτηριστικά: ασφάλεια, αξιοπιστία, δυνατότητα μαζικής χρήσης, ανωνυμία, αποδοχή, ευρεία βάση πελατών, ευελιξία, μετατρεψιμότητα, αποτελεσματικότητα συναλλαγών, μικρό κόστος και ευκολία χρήσης.

Τα ένδεκα αυτά χαρακτηριστικά μπορούν να χρησιμοποιηθούν ως κριτήρια για την ανάλυση των μεθόδων ηλεκτρονικής πληρωμής, η οποία γίνεται με τη κρυπτογραφημένη μετάδοση στοιχείων συμβατικής πληρωμής που είναι σήμερα σε χρήση : ψηφιακά μετρητά, λογαριασμοί χρέωσης-πίστωσης, ηλεκτρονικές επιταγές, άμεση μεταφορά και υπηρεσίες είσπραξης.

3.1. Κρυπτογραφημένη μετάδοση στοιχείων

Η κρυπτογραφημένη μετάδοση στοιχείων συμβατικής πληρωμής (π.χ. αριθμών πιστωτικών καρτών) είναι η ευρύτερα διαδεδομένη μέθοδος σήμερα, που ονομάζεται επίσης μέθοδος της «ασφαλούς αναπαράστασης». Η κρυπτογραφημένη μετάδοση εξασφαλίζει την ασφάλεια των πληροφοριών, που μπορούν να χρησιμοποιηθούν μόνο από τον έμπορο ή κάποιον ενδιάμεσο οργανισμό.

Το κυριότερο πλεονέκτημα της μεθόδου είναι ότι ο πελάτης και ο έμπορος δεν υποχρεούνται να διατηρούν σχέση με κάποιον ενδιάμεσο οικονομικό οργανισμό προκειμένου να πραγματοποιηθεί μια συναλλαγή. Η διαδικασία της πληρωμής ακολουθεί την συναλλαγή και δεν προϋποθέτει καμιά προεργασία (pull model), ενώ έτσι ευνοούνται οι παρορμητικές αγορές και διευρύνεται η βάση πελατών. Ο κίνδυνος των οικονομικών δεδομένων που μεταδίδονται κρυπτογραφημένα, μέσω του δικτύου, είναι πολύ μικρότερος από τον κίνδυνο μετάδοσης των ίδιων δεδομένων με συμβατικό τρόπο (π.χ. ταχυδρομικά ή τηλεφωνικά).

Το αδύνατο σημείο αυτής της μεθόδου δεν είναι η μετάδοση των οι-

κονομικών πληροφοριών αλλά η αποθήκευσή τους στους ηλεκτρονικούς υπολογιστές του εμπόρου ή του ενδιάμεσου οργανισμού, όπου παραμένουν μετά την ολοκλήρωση της συναλλαγής και μπορούν να υποκλαπούν από κάποιον που μελλοντικά θα διεισδύσει παράνομα στους υπολογιστές αυτούς. Ο κίνδυνος αυτός μπορεί να προληφθεί με την τήρηση αυστηρών μέτρων ασφαλείας από τον έμπορο ή τον ενδιάμεσο οργανισμό. Ένα δεύτερο μειονέκτημα είναι το κόστος της χρήσης ενός ενδιάμεσου οργανισμού για την πραγματοποίηση των πληρωμών. Ειδικά, αν η τιμή των προϊόντων είναι πολύ μικρή, το κόστος μιας συναλλαγής μπορεί να είναι υψηλότερο από το αντίστοιχο της πώλησης.

Πίνακας 1

Συστήματα κρυπτογραφημένης μετάδοσης

Χώρα	**Χειριστής σχεδίου /όνομα**	**Θέση - κατάσταση**
Βέλγιο	Banksys / Proton	Εθνικό roll-out
Κίνα	Τράπεζα της Κίνας	Δοκιμή εν εξελίξει
Τσεχοσλοβακία	Easy card	Roll-out σε 100 καταστήματα
Δανία	Danmont	Εθνικό roll-out
Φινλανδία	Avant	Εθνικό roll-out
Ολλανδία	Chipper	Roll-out το 1997
Ολλανδία	ChipKnip	Πειραματικό εν εξελίξει
Πορτογαλία	SIBS/Multibanco	Εθνικό roll-out
Σιγκαπούρη	Nets / CashCard	Εθνικό roll-out
Ισπανία	SEMP	Εθνικό roll-out
Ελβετία	Swiss PTT / Postcard	Πλάνο Roll-out
Ταϊβάν	FISC	Roll-out
Ταϊλάνδη	Ταϊλανδική τράπεζα αγροτών	Δοκιμή πλάνου
U.K.	Mondex (mastercard)	Πιλότοι στη UK, τον Καναδά & το Χονγκ Κονγκ
Διεθνή	VisaCash	UK,

3.2. Ψηφιακά μετρητά

Τα «ψηφιακά μετρητά» είναι ένα μέσο ηλεκτρονικής πληρωμής ανάλογο με τα κοινά μετρητά, κέρματα και χαρτονομίσματα. Ο πελάτης έχει ένα «ηλεκτρονικό πορτοφόλι» συνήθως με τη μορφή μιας ειδικής ηλεκτρονικής κάρτας, που το «φορτώνει» χρήματα από τον τραπεζικό λογαριασμό ή πληρώνοντας τα αντίστοιχα μετρητά στο ταμείο μιας τράπεζας. Η κάρτα είναι ανώνυμη και έχει αποθηκευμένη την αξία των χρημάτων με τα οποία έχει «φορτωθεί». Ένας έμπορος που δέχεται ψηφιακά μετρητά μπορεί να αφαιρέσει ένα ποσό από την κάρτα και να το μεταφέρει σε ένα δικό του ηλεκτρονικό πορτοφόλι. Ο οικονομικός οργανισμός που υποστηρίζει τα ψηφιακά μετρητά μπορεί στη συνέχεια να ανταλλάξει την αξία που είναι αποθηκευμένη στην κάρτα του εμπόρου με κοινά χρήματα.

Τα ψηφιακά μετρητά έχουν δυο πλεονεκτήματα Το πρώτο που έχει ιδιαίτερη σημασία για τους πελάτες, είναι η ανωνυμία των συναλλαγών. Το δεύτερο είναι η δυνατότητα χρήσης των ψηφιακών μετρητών ως μέσο πληρωμής ακόμη και χωρίς την μεσολάβηση του οικονομικού οργανισμού που τα υποστηρίζει. Για παράδειγμα, ένας έμπορος μπορεί να χρησιμοποιήσει απευθείας το ηλεκτρονικό του πορτοφόλι για να πληρώσει τις προμήθειες του, χωρίς να είναι υποχρεωμένος να το ξεφορτώσει στον τραπεζικό του λογαριασμό ή να μετατρέψει το περιεχόμενό του σε άλλο μέσο πληρωμής. Μελλοντικά, η χρησιμοποίηση του ηλεκτρονικού χρήματος προβλέπεται να επιταχθεί και να υποκαταστήσει σε μεγάλο βαθμό το χρήμα στη φυσική του μορφή.

- **CyberCash.** Ένα σύστημα που χαρακτηρίζεται ως «ηλεκτρονικό πορτοφόλι» και χρησιμοποιεί την τεχνική της κρυπτογράφησης με δημόσιο κλειδί (πάνω σε λογισμικό της RSA Data Security). Το «πορτοφόλι» μπορεί να αποθηκεύσει πληροφορίες για διάφορες πιστωτικές κάρτες και ο κάτοχος μπορεί να επιλέξει ποια θα χρησιμοποιήσει κάθε φορά. Στη συνέχεια, στέλνει τις πληροφορίες της πιστωτικής κάρτας μαζί με πληροφορίες για τη συναλλαγή στην εταιρία CyberCash, η οποία αποκρυπτογραφεί τα δεδομένα και φροντίζει για την

έγκριση της πληρωμής από την αρμόδια τράπεζα. Μετά την έγκριση, τα δεδομένα στέλνονται κρυπτογραφημένα στον πωλητή, που εκδίδει μια ηλεκτρονική απόδειξη και παραδίδει το προϊόν στον αγοραστή.

Το σύστημα CyberCash έχει ήδη ολοκληρωθεί και βρίσκεται σε χρήση από ένα μεγάλο αριθμό επιχειρήσεων κάθε μεγέθους, που δραστηριοποιούνται στο ηλεκτρονικό εμπόριο. Ο κίνδυνος για τους αγοραστές που χρησιμοποιούν το σύστημα CyberCash είναι ελάχιστος και συχνά καλύπτεται από την πολιτική των οργανισμών πιστωτικών καρτών (για παράδειγμα στις ΗΠΑ οι οργανισμοί πιστωτικών καρτών καλύπτουν κάθε απώλεια αξίας πάνω από 50 δολάρια). Το πλεονέκτημα του συστήματος CyberCash είναι ότι χρησιμοποιεί ισχυρή κρυπτογράφηση και συγχρόνως μπορεί να περνά χωρίς πρόβλημα από φίλτρα πρόσβασης στο internet. Το κύριο μειονέκτημα είναι ότι δεν προστατεύει την ανωνυμία του αγοραστή, όπως συμβαίνει πάντοτε με την χρήση πιστωτικών καρτών.

- **SET :** Οι δυο μεγαλύτεροι οργανισμοί πιστωτικών καρτών, VISA και Mastercard, σε συνεργασία με έναν αριθμό μεγάλων επιχειρήσεων από τον χώρο της πληροφορικής τεχνολογίας, έχουν αναπτύξει το πρωτόκολλο SET, για την ασφαλή πραγματοποίηση συναλλαγών μέσα από ψηφιακά κέντρα. Οι πληροφορίες που μεταδίδονται σύμφωνα με το πρωτόκολλο SET, προστατεύονται με κρυπτογράφηση με δημόσιο κλειδί. Το πρωτόκολλο SET, απαιτεί την ύπαρξη ει δικού λογισμικού στον υπολογιστή του αγοραστή όπως και στον κόμβο του πωλητή.

Βασικά το πρωτόκολλο SET, περιλαμβάνει τις ίδιες διαδικασίες που υπάρχουν ήδη για την πληρωμή με πιστωτικές κάρτες: ο πωλητής επικοινωνεί (τηλεφωνικά ή μέσα από ειδική συσκευή) με τον οργανισμό πιστωτικών καρτών, δίνει τον αριθμό της πιστωτικής κάρτας του αγοραστή και την αξία της πώλησης και ζητά έγκριση της συναλλαγής. Στη συνέχεια ο πωλητής εισπράττει την πληρωμή του από την τράπεζα που έχει εκδώσει την πιστωτική κάρτα και ο αγοραστής πρέπει να καλύψει το υπόλοιπο της πιστωτικής κάρτας σύμφωνα με τους όρους που έχει συμφωνήσει με την τράπεζα. Το πρω-

τόκολλο SET, ουσιαστικά επιτρέπει την επικοινωνία για την έγκριση της συναλλαγής μέσα από το ψηφιακό δίκτυο.

Το πρωτόκολλο SET, είναι ένα πολύπλοκο και συμπαγές σύστημα που χρησιμοποιεί την ισχυρότερη υπάρχουσα μέθοδο κρυπτογράφησης και ψηφιακά πιστοποιητικά για την προστασία κάθε συναλλαγής. Σε κάθε συναλλαγή συμμετέχουν τέσσερα μέρη: ο αγοραστής, ο πωλητής, η τράπεζα και ο οργανισμός πιστωτικών καρτών. Αυτό σημαίνει ότι για κάθε συναλλαγή πρέπει να δημιουργούνται και να μεταδίδονται πολλά ψηφιακά πιστοποιητικά, κάτι που δεν έχει ακόμη δοκιμαστεί στην πράξη σε μεγάλη κλίμακα.

- **Visa Cash:** Η Visa έχει αναγγείλει πρόσφατα τη κάρτα καταχωρημένης αξίας (SVC) που βασίζεται αρχικά στο Δανικό σύστημα Danmont, το οποίο μπορεί να είναι στη μορφή μίας χρήσης ή επαναφορτώσιμης κάρτας ολοκληρωμένου κυκλώματος. Οι μίας χρήσης κάρτες φορτώνονται εκ των προτέρων με ένα καθορισμένο ποσό που οι καταναλωτές μπορούν να ξοδεύουν μέχρι να μηδενιστεί. Η Visa Cash άρχισε την επέκταση με 3.000.000 κάρτες στους ολυμπιακούς αγώνες του 1996 στην Ατλάντα.

Οι επαναφορτώσιμες κάρτες μπορούν να συμπληρωθούν σε ATMs, στις συσκευές φόρτωσης και στα μελλοντικά τηλέφωνα και PCs. Η επαναφορτώσιμη έκδοση μπορεί ακόμα και να συγκατοικήσει με άλλες λειτουργίες, όπως η πίστωση ή η χρέωση μέσα σε μια ενιαία κάρτα. Στη UK, έξι σημαντικά ιδρύματα τίθενται ως στόχος να τρέξουν μια δοκιμή της Visa Cash το 1997 σε διάφορες σημαντικές πόλεις.

- **Danmont:** Μια από τις πιο γνωστές διαδικασίες ηλεκτρονικών πορτοφολιών είναι το σχέδιο Danmont που προωθείται στη Δανία το 1992. Το Danmont χρησιμοποιεί τις προπληρωμένες κάρτες (τηλεφωνίας) στις διάφορες αξίες. Οι κάρτες χρησιμοποιούνται κατά ένα μεγάλο μέρος στις διαδικασίες χαμηλής αξίας, όπως στους μετρητές στάθμευσης και σε μερικά καταστήματα. Από την ολοκλήρωση της αρχικής τεχνολογικής δοκιμής στο Naestved - στη νοτιοδυτική Δανία, το σχέδιο έχει επεκταθεί σε περισσότερες από 20 δανικές πόλεις. Κατά τη διάρκεια του 1995, το Danmont εισήγαγε τις επαναφορώσιμες κάρτες που μπορούν να φορτωθούν με μετρητά από λο-

γαριασμούς τραπεζών σε ATM. Οι συναλλαγές είναι off-line με μία ασφαλή εφαρμογή που χρησιμοποιείται για να επικυρώσει την κάρτα και να προσδιορίσει μια αναφορά συναλλαγής. Οι λεπτομέρειες καταχωρούνται στα τερματικά για την προς τα εμπρός μεταφορά στο κεντρικό σύστημα, όπου επικυρώνεται και ένα ίχνος ελέγχου διατηρείται έως ότου εξαντληθεί η αξία της κάρτας.

- **Avant:** Το φινλανδικό σχέδιο ηλεκτρονικών πορτοφολιών Avant εισήχθη στο τέλος του 1992 για τη χρήση στους κερματοδέκτες και τους μετρητές χώρου στάθμευσης στην περιοχή του Ελσίνκι. Το σχέδιο αναπτύχθηκε από το Setec Oy, έναν εκτυπωτή ασφάλειας και ένα υποκατάστημα της τράπεζας της Φινλανδίας. Όπως το Danmont, το σύστημα άρχισε με τις προπληρωμένες, μίας χρήσης κάρτες, αν και υπάρχουν σχέδια για να προωθήσουν τις επαναφορτώσιμες κάρτες για τη χρήση σε ATMs σύντομα. Στα προηγούμενα δύο έτη, το σχέδιο Avant επεκτείνεται αργά και σταθερά με εφαρμογές όπως στο σύστημα σφράγισης στο ταχυδρομείο του Ελσίνκι, τα διόδια, τις μηχανές πώλησης και τις κάρτες πόλεων.

- **Proton**: Το βελγικό σχέδιο ηλεκτρονικών πορτοφολιών άρχισε τις δοκιμές στο Leuven και στο Wavre το 1995. Το Banksys είναι η βελγική διατραπεζική λειτουργία, για τις ηλεκτρονικές πληρωμές και την Proton κάρτα, και στοχεύουν στις μικρής αξίας συναλλαγές μέσα στην υπάρχουσα λειτουργία Bancontact / MasterCash. Ο πιλότος περιλαμβάνει περίπου 50.000 κάρτες αρχίζοντας από τις επαναφορτώσιμες κάρτες και βαθμιαία τη μετανάστευση της τεχνολογίας στις κάρτες πίστωσης και χρέωσης των πελατών, που θα έχουν έτσι μια ενιαία συνδυασμένη λειτουργία ηλεκτρονικών πορτοφολιών.

Το Banksys παρέχει τις λειτουργίες του προμηθευτή πορτοφολιών, του SAM εκδότη, του Load Agent και του αγοραστή. Οι κάρτες εκδίδονται από τις συμμετέχουσες τράπεζες που παρέχουν την εγγύηση των κεφαλαίων. Το σχέδιο είναι ανοικτό σε οποιονδήποτε κρατά μια κάρτα Proton. Η ηλεκτρονική αξία που περιλαμβάνεται στο τερματικό αγορών μπορεί να φορ-

τωθεί από ένα τραπεζικό λογαριασμό μέσω ενός modem. Αυτό είναι πολύ χρήσιμο αφού, παραδείγματος χάριν, ξεφορτώνει τα κεφάλαια από μια off-line μηχανή πώλησης.

Οι αγορές μπορούν να γίνουν σε οποιοδήποτε παροχέα της υπηρεσίας. Οι πολλαπλές χρήσεις επιτρέπονται ενώ παρέχεται και η ευκολία κλειδώματος του κεφαλαίου. Το σύστημα σχεδιάστηκε για να είναι ανώνυμο και οι κάρτες είναι επομένως μεταβιβάσιμες μεταξύ των ανθρώπων. Το Proton έχει χορηγήσει την άδεια της τεχνολογία σε μια ομάδα ολλανδικών τραπεζών υπό τον τίτλο ChipKnip.

- **MEP:** Το πορτογαλικό σχέδιο ηλεκτρονικών πορτοφολιών Multibanco άρχισε τις δοκιμές στη Λισσαβόνα, κατά τη διάρκεια του 1994. Όπως στο Βέλγιο, η πρωτοβουλία έρχεται από μια υπάρχουσα διατραπεζική λειτουργία, κατά ένα μεγάλο μέρος ενδιαφερόμενη για τις ηλεκτρονικές πληρωμές και την αντιπροσώπευση 30 πορτογαλικών τραπεζών που ανήκουν στο δίκτυο Multibanco.

Δύο τύποι καρτών είναι προβλεπόμενοι: μια ανώνυμη κάρτα πορτοφόλι και μια πολλαπλών χρήσεων κάρτα που θα λειτουργεί ως κάρτα πίστωσης /χρέωσης. Και οι δύο θα είναι επαναφορτώσιμες. Η κάρτα πορτοφόλι δεν θα συνδέεται με οποιοδήποτε ιδιαίτερο τραπεζικό λογαριασμό, αν και εκδίδεται κάτω από το εμπορικό σήμα μιας μεμονωμένης τράπεζας. Στο μέλλον, το σχέδιο θα μπορούσε να κινηθεί στο ύφος του Mondex στις κάρτα με κάρτα συναλλαγές.

Κάτω από αυτό το σχέδιο οι πελάτες πληρώνουν για την κάρτα και χρεώνονται για τη φόρτωση αυτής. Μπορούν, επίσης, να πληρώσουν για να εμφανίσουν τις τελευταίες 30 συναλλαγές που καταχωρούνται στην κάρτα και τις τυπώνουν σε οποιοδήποτε ATM.

- **SEMP** :Στα σύνορα στην Ισπανία, οι δοκιμές αρχίζουν επίσης στο σχέδιο ηλεκτρονικών πορτοφολιών που αναπτύσσεται από τη Sociedad Espanola de Medios de Pago (SEMP), μια κοινοπραξία που αντιπροσωπεύει τις σημαντικές τράπεζες της Ισπανίας. Αυτό είναι ένα πολλαπλών χρήσεων πρόγραμμα καρτών, με ένα ανοιχτό ηλεκτρονικό πορτοφόλι για τις διατρα-

πεζικές συναλλαγές και διάφορα κλειστά πορτοφόλια προς χρήση από τις εκδότριες τράπεζες, με διάφορους τρόπους. Το σύστημα είναι ενδεχομένως πολλαπλών νομισμάτων αλλά οι δοκιμές χρησιμοποιούν πορτοφόλια πεσετών μόνο.

➢ **Chipper:** Το chipper είναι μια πολυσύνθετη έννοια καρτών ολοκληρωμένου κυκλώματος που ενσωματώνει ένα επαναφορτώσιμο ηλεκτρονικό πορτοφόλι. Το Chipper είναι η κοινή ολλανδική πρωτοβουλία από τη PTTTelecom και τη Postbank. Είναι βασισμένο σε μια ανοικτή, τυποποιημένη, πολλαπλών χρήσεων κάρτα ολοκληρωμένου κυκλώματος που βασίζεται στα διεθνή πρότυπα ETSI TE9. Η PTT TELECOM άρχισε τις δοκιμές το 1995 και οι περαιτέρω δοκιμές συνεχίστηκαν. 20.000 τηλεφωνικοί θάλαμοι έχουν μετατραπεί ήδη, όχι μόνο για να εφαρμόσουν στις κλήσεις το Chipper αλλά για να ενεργήσουν ως σταθμοί φόρτωσης.

➢ **Pacific Rim**: Μέσα στην Ασία, ένα από τα πιο προηγμένα σχέδια ηλεκτρονικών πορτοφολιών είναι το FISC (οικονομικό κέντρο συστήματος πληροφοριών-Financial Information Systems Center) πρόγραμμα στην Ταϊβάν, το οποίο προωθήθηκε στο τέλος του 1992. Το FISC ιδρύθηκε ως μη κερδοσκοπικό σώμα κάτω από τους οιωνούς του υπουργείου Οικονομικών, ενώ το σχέδιο είναι μια πολύ-τραπεζική λειτουργία που περιλαμβάνει περισσότερες από 30 τράπεζες με τις κάρτες που χρησιμοποιούνται για τις διατραπεζικές συναλλαγές. Πρόσθετες υπηρεσίες προγραμματίζονται για τις κάρτες στο μέλλον. Το σχέδιο της Σιγκαπούρης CashCard έχει αρχίσει επίσης εκτενής δοκιμές με περίπου 40.000 προπληρωμένες κάρτες.

➢ Millicent: ένα «ελαφρύ» αλλά ασφαλές πρωτόκολλο, που επιτρέπει οικονομικές συναλλαγές με πάρα πολύ μικρά ποσά. Το κόστος κάθε συναλλαγής είναι ένα χιλιοστό του Cent (1/100 του δολαρίου), από όπου το σύστημα έχει πάρει το όνομά του. Ο αγοραστής έχει αποθηκευμένο στον υπολογιστή του ένα χρηματικό ποσό, με την μορφή ψηφιακών μετρητών, που μπορεί να αναγνωριστεί μόνο από ένα συγκεκριμένο πωλητή. Η μεταφορά και η επιβεβαίωση των πληρωμών γίνεται απευθείας στον κόμβο του εμπό-

ρου. Η κύρια δύναμη του συστήματος Millicent βρίσκεται στην κατασκευή ψηφιακών υπογραφών πολύ χαμηλού κόστους, που δεν εξαρτώνται από δημόσια κλειδιά που πρέπει να είναι διαθέσιμα σε όλους. Το κόστος της διατήρησης ενός κόμβου στο internet για την «είσπραξη» ψηφιακών μετρητών είναι γενικά πολύ μικρό. Επίσης, η κλοπή των ψηφιακών μετρητών αυτού του τύπου δεν έχει νόημα, λόγω της χαμηλής αξίας κάθε μονάδας (που ονομάζεται scrip-Κλάσμα του δολαρίου). Τα μειονεκτήματα του συστήματος είναι δυο. Πρώτον, τα ψηφιακά μετρητά ισχύουν μόνο για ένα πωλητή, με τον οποίο ο πελάτης πρέπει να έχει συχνές συναλλαγές. Αν ένας πελάτης χρειάζεται ψηφιακά μετρητά για πολλούς διαφορετικούς προμηθευτές, η χρήση του συστήματος γίνεται ασύμφορη και μπορεί να επιβαρύνει τον ηλεκτρονικό υπολογιστή του. Δεύτερον, υπάρχει κίνδυνος κάποιος να παράγει (πλαστογραφήσει) δικά του ψηφιακά μετρητά.

- **CAFE** (Conditional Access for Europe): Ένα σύστημα ψηφιακών μετρητών που χρησιμοποιεί ειδικές ηλεκτρονικές κάρτες (smart card), που περιέχουν μικροεπεξεργαστή και παρέχει ισχυρές εγγυήσεις για την ανωνυμία των χρηστών. Υποστηρίζεται από μια Ευρωπαϊκή κοινοπραξία 13 εταίρων, μεταξύ των οποίων η Digicash. Το πρόγραμμα CAFE βρίσκεται στη φάση της δοκιμαστικής υλοποίησης και το μέλλον του εξαρτάται από τον βαθμό αποδοχής του από τις τράπεζες και τον πολιτικό κόσμο. Περισσότερες λεπτομέρειες δεν είναι προς το παρόν διαθέσιμες και αυτό ίσως είναι μια ένδειξη ότι το σύστημα πλησιάζει στην ολοκλήρωσή του.
- **Mondex.** Το Mondex είναι μια πρωτοβουλία πληρωμής που αναπτύσσεται από την Εθνική τράπεζα Westminster (εθνική δύση) στη UK για να διατηρήσει τα χαρακτηριστικά γνωρίσματα του πυρήνα που κάνουν τα μετρητά τη κυρίαρχη μέθοδο παγκόσμιας πληρωμής και προσθέτοντας τα σημαντικά οφέλη

Στην καρδιά του Mondex είναι το ηλεκτρονικό πορτοφόλι (EP), που εφαρμόζεται στις ανθεκτικές στη πλαστογράφηση κάρτες ολοκληρωμένου κυκλώματος, στις οποίες η αξία καταχωρείται. Το Mondex είναι ένα

ανοικτό σύστημα πληρωμής όπου η αξία μπορεί να μεταφερθεί από το ένα πορτοφόλι σε ένα άλλο χωρίς την ανάγκη για οποιαδήποτε έγκριση, καθάρισμα, ή τακτο-ποίηση μετά από τη συναλλαγή.

Είναι ένα σύστημα ψηφιακών μετρητών που βασίζεται σε ειδικές ηλεκτρονικές κάρτες (smart card) και απαιτεί προεργασία για τη χρήση του. Οι ψηφιακές κάρτες εξασφαλίζουν μια φορητότητα και ανεξαρτησία από το είδος του ψηφιακού δικτύου, ανάλογη με αυτήν ενός μεταλλικού νομίσματος. Ουσιαστικά πρόκειται για μια πλαστική κάρτα, που εξωτερικά μοιάζει με μια πιστωτική κάρτα που μπορεί να «φορτωθεί» με ένα χρηματικό ποσό και να χρησιμοποιηθεί σε διαφορετικές συσκευές είσπραξης.

Η ανεξαρτησία των καρτών αυτών είναι το κυριότερο πλεονέκτημά τους. Η αξία τους είναι αποθηκευμένη μέσα σε αυτές και δεν χρειάζονται έγκριση από κανένα κεντρικό οργανισμό. Είναι ένα πραγματικό ψηφιακό χρήμα και όχι απλά μια επέκταση των πιστωτικών καρτών. Οι κίνδυνοι είναι ίδιοι με αυτούς των κοινών μετρητών. Αν ο κάτοχος χάσει την κάρτα του, χάνει το χρηματικό ποσό που υπήρχε φορτωμένο σε αυτήν. Όμοια, αν μια κάρτα κλαπεί, το περιεχόμενο περνά στον κλέφτη. Ο κάτοχος έχει την ελευθερία να χρησιμοποιήσει την κάρτα χωρίς να αφήνει ίχνη των συναλλαγών του και φυσικά μπορεί να την δώσει στο παιδί του χωρίς κανένα πρόβλημα.

Η τράπεζα της Σκοτίας ανήγγειλε το 1995 ότι είχε υπογράψει το Mondex. Η τράπεζα του Χονγκ Κονγκ και της Σαγκάης έχει αγοράσει τα δικαιώματα προνομίων για την Άπω Ανατολή και είναι αυτήν την περίοδο στο στάδιο της έκδοσης των προνομίων του Mondex στους κατάλληλους συνεργάτες. Το Mondex συνεχίζει να παραμένει το πιο κομψό σχέδιο ηλεκτρονικών πορτοφολιών στον κόσμο. Είναι μια ανεξάρτητη λύση στο παγκόσμιο πρόβλημα των πληρωμών. Η δύναμη του Mondex βρίσκεται στη συλλογική δύναμη των δικαιοδόχων της.

- **CyberCoin**. Μια τεχνολογία ψηφιακών μετρητών, που μπορεί να χρησιμοποιηθεί για συναλλαγές ελάχιστης αξίας. Στηρίζεται στο «ηλεκτρονικό πορτοφόλι» της CyberCash, που έχει αναφερθεί παραπάνω.

Το χρηματικό ποσό με το οποίο «φορτώνεται» το πορτοφόλι δεν μεταφέρεται πραγματικά, αλλά δεσμεύεται από την τράπεζα μέχρι ο πελάτης να πληρώσει για μια αγορά-οπότε μεταφέρεται στον λογαριασμό του πωλητή. Οι συναλλαγές δεν είναι ανώνυμες, ενώ η Cyber Cash αναλαμβάνει την ευθύνη για την παράδοση των προϊόντων. Με τον τρόπο αυτό, το σύστημα μοιάζει πάρα πολύ με τη χρήση υπηρεσιών είσπραξης.

Το κύριο πλεονέκτημα της μεθόδου αυτής είναι η υποστήριξη που βρίσκει στην αγορά. Κορυφαία στελέχη από τον κλάδο της επεξεργασίας συναλλαγών και της κρυπτογράφησης εργάζονται πάνω στο σύστημα CyberCoin. Η κύρια αδυναμία του είναι η έλλειψη ανωνυμίας. Μοιράζεται, επίσης, το πρόβλημα όλων των μεθόδων που δεν χρησιμοποιούν τις ειδικές κάρτες smart card, δηλαδή ότι οι πληροφορίες αποθηκεύονται σε ηλεκτρονικούς υπολογιστές και αργά ή γρήγορα μπορεί κάποιος μη εξουσιοδοτημένος να τις αποκρυπτογραφήσει ή να τις χρησιμοποιήσει για παράνομους σκοπούς.

3.3. Λογαριασμοί χρέωσης-πίστωσης

Το σύστημα των λογαριασμών χρέωσης-πίστωσης προϋποθέτει την υποδομή της τήρησης λογαριασμού τόσο από τον πωλητή όσο και από τον αγοραστή σε κάποιο ενδιάμεσο οικονομικό οργανισμό. Όταν πραγματοποιείται μια συναλλαγή, η αξία της αφαιρείται από τον λογαριασμό του αγοραστή και μεταφέρεται στον λογαριασμό του πωλητή. Στη διάρκεια της διαδικασίας πληρωμής ο ενδιάμεσος οργανισμός έχει την ευθύνη για την πιστοποίηση της ταυτότητας του αγοραστή. Ο λογαριασμός του αγοραστή μπορεί να λειτουργεί με δυο τρόπους: είτε η αξία των αγορών να καλύπτεται προκαταβολικά, είτε να εξοφλείται μετά την πραγματοποίησή τους. Ανάλογα με τον τρόπο λειτουργίας, ο λογαριασμός ονομάζεται ή χρεωστικός ή πιστωτικός.

Το κύριο πλεονέκτημα αυτής της μεθόδου είναι η ευελιξία. Ο ίδιος μηχανισμός μπορεί να χρησιμοποιηθεί για πολλά είδη συναλλαγών. Αν χρειαστεί, το σύστημα μπορεί επίσης να επιτρέψει ανώνυμες συναλλαγές. Το

μειονέκτημα της μεθόδου είναι ότι η προεργασία για την πληρωμή προηγείται της συναλλαγής (push model) και κάθε πελάτης πρέπει να έχει ανοίξει λογαριασμό πριν πραγματοποιήσει την πρώτη του αγορά. Έτσι, το σύστημα δεν υποστηρίζει παρορμητικές αγορές.

NetCash. Ένα σύστημα ψηφιακών μετρητών, που βασίζεται σε λογαριασμούς χρέωση-πίστωσης αλλά επιτρέπει παρορμητικές αγορές καθώς δεν απαιτεί καμία προεργασία για την πραγματοποίηση μιας πληρωμής. Η μετάδοση δεδομένων κρυπτογραφείται με τη μέθοδο PGP.

3.4. Ηλεκτρονικές επιταγές

Οι ηλεκτρονικές επιταγές είναι η φυσιολογική συνέχεια των παραδοσιακών επιταγών, που τώρα υπογράφονται και μεταβιβάζονται ηλεκτρονικά και μπορούν να έχουν όλες τις παραλλαγές των κοινών επιταγών, όπως ταξιδιωτικές επιταγές ή πιστοποιημένες επιταγές. Οι ηλεκτρονικές επιταγές χρησιμοποιούν την τεχνολογία των ψηφιακών υπογραφών και μπορούν να αποτελέσουν το συνδετικό κρίκο που θα διευκολύνει το πέρασμα από τις υπάρχουσες μεθόδους πληρωμής στις μεθόδους ηλεκτρονικής πληρωμής. Η μέθοδος αυτή χαρακτηρίζεται από υψηλό βαθμό ασφάλειας, διότι χρησιμοποιείται κωδικοποίηση των απαραίτητων στοιχείων που αποστέλλονται στον προμηθευτή, ενώ υπάρχει και δυνατότητα ελέγχου του διαθέσιμου ποσού του καταναλωτή πριν από την ολοκλήρωση της συναλλαγής.

- **CheckFree:** Η εταιρία Checkfree προσφέρει μια μερική λύση για την πραγματοποίηση ηλεκτρονικών πληρωμών. Επικεντρώνεται κυρίως, σε άτομα ή επιχειρήσεις που πληρώνουν μηνιαίους λογαριασμούς και επιθυμούν να αυτοματοποιήσουν τις πληρωμές τους. Βασικά, είναι μια υπηρεσία πληρωμών που επιτρέπει στους πελάτες της να πληρώνουν τους λογαριασμούς τους μέσα από το internet. Η εταιρία CheckFree είναι συνδεδεμένη με το δίκτυο ηλεκτρονικών συναλλαγών της Αμερικάνικης τράπεζας Federal Reserve Bank και με αρκετούς οργανισμούς πιστωτικών καρτών. Όταν κάποιος γίνεται πελάτης της Checkfree, πρέπει να δώσει τα στοιχεία ενός τραπεζικού του λογαριασμού. Όλες οι μελλοντικές πληρωμές

θα γίνονται από τον λογαριασμό αυτό. Το μόνο που πρέπει πλέον να κάνει ο πελάτης είναι να δηλώσει στην Checkfree, μέσα από το internet, το ποσό και τον αποδέκτη. Το σύστημα της Checkfree μπορεί στη συνέχεια να βρει τον καταλληλότερο τρόπο για την πληρωμή του αποδέκτη (π.χ. ηλεκτρονικά ή με ταχυδρομική επιταγή) και να πραγματοποιήσει την πληρωμή χρεώνοντας το αντίστοιχο ποσό στον λογαριασμό του πελάτη. Το κύριο πλεονέκτημα του συστήματος Checkfree είναι ότι έχει στενή επικοινωνία με το τραπεζικό σύστημα και είναι εξαιρετικά εύχρηστο. Επίσης χρησιμοποιεί ένα υψηλό επίπεδο κρυπτογράφησης για την ασφαλή μετάδοση των πληροφοριών. Το πρόβλημα είναι ότι δεν χρησιμοποιεί κοινά αποδεκτά πρότυπα στον τομέα της κρυπτογράφησης και της ασφάλειας. Αυτό αναμένεται να αλλάξει σύντομα, καθώς οι εταιρίες Checkfree και CyberCash έχουν ξεκινήσει από κοινού την ανάπτυξη ενός συμβατού λογισμικού.

- **On-line CHECK**: Η εταιρία On-line CHECK Systems χρησιμοποιεί πολύ ισχυρούς αλγόριθμους κρυπτογράφησης (RSA) για τη μετάδοση οικονομικών δεδομένων, τα οποία στη συνέχεια παραδίδει σε έντυπη μορφή στις αρμόδιες τράπεζες.
- **NetCheque**: Ένα πρότυπο πληρωμής ηλεκτρονικών επιταγών, που χρησιμοποιεί ένα μηχανισμό συμμετρικής κρυπτογράφησης (με μυστικό κλειδί) βασισμένο στο σύστημα Kerberos.
- **NetChex:** Ένα σχήμα ηλεκτρονικών πληρωμών που βασίζεται στις επιταγές αλλά χρησιμοποιεί πιστωτικές κάρτες για τη ρύθμιση των οφειλών. Πρόκειται για ένα ιδιωτικό σύστημα για το οποίο δεν υπάρχουν διαθέσιμες πληροφορίες. Γενικά ο μηχανισμός χρησιμοποιεί ένα κοινό μυστικό.
- **NetBill:** Ένα σύστημα ηλεκτρονικών επιταγών που χρησιμοποιεί συμμετρική κρυπτογράφηση (με μυστικό κλειδί) βασισμένη στο σύστημα **Kerberos****. Η ομάδα του πανεπιστημίου Carnegie MeIIon που αναπτύσσει το σύστημα NetBiII ενδιαφέρεται κυρίως για την πώληση πληροφοριών μέσα από το δίκτυο. Ένας κεντρικός κόμβος διατηρεί οικονομικές πληροφορίες (λογαριασμούς) των χρηστών. Όταν ένας χρήστης

ενδιαφέρεται να αγοράσει μια πληροφορία στέλνει στον κόμβο μια κρυπτογραφημένη παραγγελία αντίστοιχης αξίας. Μόλις ο κόμβος βεβαιώσει την παραλαβή της παραγγελίας, επιτρέπει την αποκρυπτογράφηση της πληροφορίας.

- **CheckMaster:** Η εταιρία CheckMaster χρησιμοποιεί τη τεχνολογία ActiveX της Microsoft για την ηλεκτρονική έκδοση και την ψηφιακή υπογραφή επιταγών. Το σύστημα λειτουργεί με το λογισμικό MS Money της Microsoft και Quicken της Intuit.Τα θέματα ασφάλειας δεν έχουν δημοσιοποιηθεί.

**** Επικύρωση σε Kerberos**

Σε ένα ανοικτό διανεμημένο υπολογιστικό περιβάλλον (DCE), ένας τερματικός σταθμός δεν μπορεί να είναι έμπιστος για να προσδιορίσει τους χρήστες του, επειδή ο τερματικός σταθμός δεν μπορεί να βρεθεί σε ένα καλά ελεγχόμενο περιβάλλον και μπορεί να είναι μακριά από τον κεντρικό υπολογιστή. Ένας χρήστης μπορεί να είναι ένας εισβολέας που μπορεί να προσπαθήσει να επιτεθεί στο σύστημα ή να προσποιηθεί ότι είναι κάποιος άλλος για να εξαγάγει πληροφορίες από το σύστημα, στο οποίο δεν έχει δικαίωμα. Προκειμένου να προστατευθεί ένα σύστημα από τους μακρινούς hosts δικτύων, ένα ορισμένο είδος επικύρωσης πρέπει να ληφθεί υπόψη.

Το Kerberos είναι ένα από τα συστήματα που παρέχει τις έμπιστες τρίτες-υπηρεσίες επικύρωσης, για να επικυρώσει τους χρήστες σε ένα διανεμημένο δικτυακό περιβάλλον. Βασικά, όταν ζητά ένας χρήστης ή ένας πελάτης μια πρόσβαση σε μια ιδιαίτερη υπηρεσία από τον κεντρικό υπολογιστή, πρέπει να λάβει ένα εισιτήριο ή ένα πιστοποιητικό από τον υπολογιστή πιστοποίησης(επικύρωσης) (AS) Kerberos. Ο χρήστης έπειτα παρουσιάζει το πιστοποιητικό στον κεντρικό υπολογιστή χορήγησης εισιτηρίων (TGS) και λαμβάνει ένα εισιτήριο υπηρεσιών. Ως εκ τούτου, ο χρήστης μπορεί να ζητήσει την υπηρεσία με την υποβολή του εισιτηρίου υπηρεσιών στον επιθυμητό κεντρικό υπολογιστή.

Έχοντας αυτό το πρωτόκολλο, ο κεντρικός υπολογιστής μπορεί να επιβεβαιώσει τις παρεχόμενες υπηρεσίες στο σωστό πελάτη που έχει δικαίωμα πρόσβασης. Αυτό γίνεται, επειδή, το Kerberos υποθέτει ότι μόνο ο σωστός χρήστης μπορεί να χρησιμοποιήσει το πιστοποιητικό, δεδομένου ότι άλλοι δεν έχουν τον κωδικό πρόσβασης για να το αποκρυπτογραφήσουν. Και επίσης, λόγω αυτού, ένας χρήστης μπορεί πραγματικά να κάνει αίτηση με το πιστοποιητικό άλλων. Δηλαδή, ο χρήστης δεν επικυρώνεται στο αρχικό στάδιο.

Κατ' αυτό τον τρόπο, ένας εισβολέας μπορεί να λάβει το πιστοποιητικό ενός άλλου χρήστη, και να εκτελέσει την off-line επίθεση με τη χρησιμοποίηση ενός υποθετικού κωδικού πρόσβασης, καθώς το εισιτήριο σφραγίζεται μόνο από τον κωδικό πρόσβασης. Αυτή η αδυναμία ασφάλειας του Kerberos επισημαίνεται από τον Mark και Gary (1995) σε ένα από τα άρθρα τους για την ενσωμάτωση της Έξυπνης κάρτας στα συστήματα επικύρωσης.

Στην έκθεσή τους, πρότειναν να ενσωματώσουν την έξυπνη κάρτα στο σύστημα Kerberos για να υπερνικήσουν αυτό το πρόβλημα. Έξι διαφορετικά σχέδια προτάθηκαν. Ολόκληρη η ιδέα είναι να ενισχυθεί η ασφάλεια επικύρωσης από το Kerberos με το να επικυρώσει το χρήστη άμεσα και στην αρχή και πριν από τη χορήγηση του αρχικού εισιτηρίου, έτσι ώστε ένας χρήστης να μη μπορεί να έχει το εισιτήριο κάποιου άλλου. Και «η χρήση της έξυπνης κάρτας απαιτεί την αναγραφή χρηστών στο σύστημα, όχι μόνο στην ανάκληση του κωδικού πρόσβασης, αλλά και για να είναι στην κατοχή ενός τεκμηρίου». Τελικά, το πρότυπο που αναφέρθηκε εδώ, κατέδειξε πως η τεχνολογία των έξυπνων καρτών μπορεί να εξασφαλίσει ένα σύστημα διαδικαστικά

3.5. Άμεση μεταφορά

Αν αγοραστής και ο πωλητής διατηρούν λογαριασμό στον ίδιο οικονομικό οργανισμό, ο αγοραστής μπορεί να δώσει ηλεκτρονικά εντολή για τη μεταφορά του ποσού πληρωμής στον λογαριασμό του πωλητή. Μόλις ο πωλητής βεβαιωθεί για την είσπραξη της πληρωμής, μπορεί να παραδώσει το

προϊόν στον αγοραστή. Η μέθοδος αυτή είναι μια από τις σπανιότερα χρησιμοποιούμενες και έχει τα ίδια πλεονεκτήματα και μειονεκτήματα με τους λογαριασμούς χρέωσης-πίστωσης.

3.6. Υπηρεσίες είσπραξης

Οι υπηρεσίες είσπραξης, που ονομάζονται επίσης εκκαθάρισης συναλλαγών, δεν είναι μια αυτόνομη μέθοδος πληρωμής αλλά ένα μέσο για την πραγματοποίηση των πληρωμών με τις μεθόδους που έχουν αναφερθεί παραπάνω. Οι υπηρεσίες είσπραξης είναι ενδιάμεσοι που αναλαμβάνουν την είσπραξη πληρωμών για λογαριασμό των εμπόρων. Ο αγοραστής λαμβάνει από τον έμπορο τις απαραίτητες πληροφορίες για να πληρώσει στην υπηρεσία είσπραξης, η οποία δέχεται την πληρωμή και επιστρέφει στον πελάτη μια απόδειξη, με την οποία αυτός μπορεί να παραλάβει το προϊόν που έχει αγοράσει. Η διαδικασία της συναλλαγής περιπλέκεται, αλλά ο έμπορος έχει το πλεονέκτημα ότι η υπηρεσία είσπραξης μπορεί να δεχθεί όλες τις μεθόδους ηλεκτρονικής πληρωμής.

- **First Virtual:** Το σύστημα First Virtual προσφέρει ασφαλείς ηλεκτρονικές συναλλαγές με τη χρήση ενός ειδικού αριθμού αναγνώρισης των πελατών, που ονομάζεται VirtualPIN αντί για αριθμούς πιστωτικών καρτών, οι οποίοι είναι αποθηκευμένοι σε ασφαλείς ηλεκτρονικούς υπολογιστές της First Virtual που δεν είναι συνδεδεμένοι στο internet. Ο αγοραστής δίνει στον πωλητή τον αριθμό VirtualPIN. ο πωλητής επικοινωνεί με την First Virtual, η οποία ζητά από τον αγοραστή να επιβεβαιώσει τη συναλλαγή. Τότε μόνο η πιστωτική κάρτα του αγοραστή χρεώνεται με την αξία της αγοράς.

- **InterCoin:** Η εταιρία Intercoin προσφέρει υπηρεσίες ηλεκτρονικής πληρωμής σε μηνιαία βάση. Ο πελάτης μπορεί να πραγματοποιεί αγορές αξίας κάτω των 10 δολαρίων, τις οποίες εξοφλεί συνολικά στο τέλος του μήνα. Το κόστος των συναλλαγών δεν χρεώνεται στον αγοραστή αλλά στον πωλητή. Τα οικονομικά στοιχεία των πελατών αποθηκεύονται σε ασφαλείς ηλεκτρονικούς υπολογιστές που δεν είναι

συνδεδεμένοι στο internet.

- TelPay. Ένα σύστημα που επιτρέπει την πληρωμή λογαριασμών από το internet. Δεν υπάρχουν διαθέσιμες περισσότερες πληροφορίες.

4. Αξιολόγηση και επιλογή μεθόδων ηλεκτρονικής πληρωμής

Ο πίνακας που ακολουθεί απαριθμεί μια σειρά από κριτήρια για την αξιολόγηση συστημάτων ηλεκτρονικής πληρωμής. Η επιλογή της καλύτερης μεθόδου ηλεκτρονικής πληρωμής για το ηλεκτρονικό εμπόριο πρέπει να γίνει μετά από μια συστηματική και ορθολογική διαδικασία λήψης απόφασης. Τα κριτήρια είναι τα εξής:

Πίνακας 2

Κριτήρια αξιολόγησης συστημάτων ηλεκτρονικής πληρωμής

Ανταλλαξιμότητα
Χαμηλό πάγιο κόστος (για τον έμπορο)
Πιθανοί περιορισμοί
Αμφίδρομες πληρωμές
Απαίτηση για ειδικό λογισμικό
Μεταφερσιμότητα
Ταχύτητα συναλλαγών
Ανέκκλητες συναλλαγές
Διακριτικότητα
Διαθεσιμότητα σήμερα
Κόστος συναλλαγών για μεγάλες και μικρές επιχειρήσεις
Απαίτηση κρυπτογράφησης για τον αγοραστή και τον πωλητή
Ανωνυμία για τον αγοραστή και τον πωλητή
Κίνδυνος παραποίησης πλαστογράφησης
Ανεξαρτησία από τον τύπο του υπολογιστή
Έλεγχος της ροής της συναλλαγής από τον αγοραστή

Δυνατότητα μαζικής χρήσης
Οικονομικός κίνδυνος για τον αγοραστή και τον πωλητή
Δυνατότητα άμεσης χρήσης των εσόδων σε ηλεκτρονική μορφή
Δυνατότητα λειτουργίας χωρίς σύνδεση
Φορητότητα
Ανάγκη για ύπαρξη τραπεζικού λογαριασμού
Βαθμός αποδοχής από τους χρήστες
Ασφάλεια από πρόσβαση χωρίς εξουσιοδότηση
Ευκολία πρόσβασης

Η εξέταση και η σύγκριση όλων των δυνατών χαρακτηριστικών κάθε συστήματος ηλεκτρονικής πληρωμής είναι χρονοβόρα και μπορεί να έχει μεγάλο κόστος. Ένας πίνακας των κυριότερων χαρακτηριστικών μπορεί να επιταχύνει σημαντικά τη διαδικασία αξιολόγησης και σύγκρισης. Η απόφαση μπορεί να στηριχθεί σε μια ιεράρχηση των κριτηρίων του παραπάνω πίνακα, ώστε να εξεταστούν λεπτομερώς μόνο τα συστήματα εκείνα που ικανοποιούν τα κριτήρια που η επιχείρηση θεωρεί απαραίτητα.

Ο τρόπος αυτός ιεραρχικής επιλογής λειτουργεί όταν υπάρχουν ένα ή περισσότερα συστήματα που καλύπτουν το σύνολο των απαραίτητων κριτηρίων. Αν δεν υπάρχει τέτοιο σύστημα, η επιλογή θα πρέπει να γίνει με βάση ένα υποσύνολο των αρχικών κριτηρίων και η επιχείρηση θα πρέπει να αποφασίσει ποιος από τους υπάρχοντες συνδυασμούς κριτηρίων είναι ο καλύτερος, κάτι που δεν είναι πάντοτε εύκολο. Ένα συνηθισμένο λάθος που γίνεται στο σημείο αυτό, είναι ότι όλα τα κριτήρια θεωρούνται ισοδύναμα μεταξύ τους.

Προς το παρόν δεν υπάρχει ένα σύστημα ηλεκτρονικής πληρωμής που να δείχνει ότι επικρατεί απέναντι στα υπόλοιπα. Από τη στιγμή που το ηλεκτρονικό εμπόριο θα αποκτήσει κρίσιμη μάζα, η επιλογή θα γίνει αυτόματα από τους πελάτες-θα είναι μια αλυσιδωτή αντίδραση, όπου οι νέοι χρήστες θα έχουν την τάση να προτιμούν τη μέθοδο που ήδη χρησιμοποιεί-

ται περισσότερο. Μέχρι τότε τα διάφορα συστήματα θα βρίσκονται σε έναν αγώνα δρόμου, προσπαθώντας να καθιερωθούν έγκαιρα ως το επικρατέστερο πρότυπο ηλεκτρονικής πληρωμής στην κατηγορία τους.

5. Το μέλλον του «εικονικού χρήματος»

Το εικονικό χρήμα (virtual money) αποτελεί ήδη μια πρόκληση, με αποτέλεσμα οι τράπεζες, ως διαχειριστές της πληροφόρησης, να είναι αντιμέτωπες με τους ιδιοκτήτες των δικτύων που τη μεταφέρουν. Πιθανές συνεργασίες των τραπεζών με εταιρείες του χώρου ή ακόμη και ανάπτυξη εσωτερικών δικτύων από τις ίδιες τις τράπεζες αποτελούν κινήσεις που ενδέχεται να εμφανιστούν ως «απάντηση» στην επερχόμενη απειλή.

Στις μέρες μας, καθώς η διάθεση προϊόντων μέσα από το internet γενικεύεται, είναι λίγες οι τράπεζες που δεν έχουν παρουσία στο Διαδίκτυο. Με την ανάπτυξη των νέων τρόπων διάθεσης των προϊόντων τους, οι τράπεζες αναπτύσσουν τις στρατηγικές τους κινούμενες γύρω από δύο άξονες, α) αυτόν της Ορθολογικοποίησης των καταστημάτων του δικτύου και β) αυτόν της διαφοροποίησης της δομής των συστημάτων διάθεσης προϊόντων με την εισαγωγή νέων καναλιών.

Παρά την ενσωμάτωση των νέων τρόπων διάθεσης των προϊόντων τους, οι τράπεζες που διατηρούν ευρύ δίκτυο καταστημάτων, βρίσκονται σε δυσχερή θέση. Από τη μια πλευρά, είναι υποχρεωμένες να επενδύουν στη νέα τεχνολογία και να επιχειρούν να στρέψουν ολοένα ευρύτερες κατηγορίες της πελατείας τους προς τη χρήση των εναλλακτικών καναλιών διανομής, ώστε να διατηρούν την πελατειακή βάση τους ενώ παράλληλα να περιορίζουν το κόστος τους. Από την άλλη όμως πλευρά, επιδιώκοντας να εκμεταλλευτούν το πλεονέκτημα της προσωπικής σχέσης με τον πελάτη, με την προοπτική προσφοράς όσο το δυνατόν πιο μεγάλου εύρους προϊόντων και υπηρεσιών, διατηρούν το δίκτυο καταστημάτων τους, αποδεχόμενες έτσι και το υψηλό κόστος διαχείρισης του.

Με τα σημερινά δεδομένα, η επεξεργασία, η μεταφορά και η αποθήκευση όλων των απαραίτητων στοιχείων για την κίνηση του χρήματος

πραγματοποιούνται με πολύ χαμηλότερο κόστος για μια τράπεζα απ' ό,τι στο παρελθόν. Σε μερικά χρόνια, ένα πολύ μεγάλο μέρος των τρεχουσών δαπανών των καταναλωτών θα καλύπτεται χωρίς τη μεσολάβηση του χρήματος, με την εξάπλωση του «ηλεκτρονικού πορτοφολιού», γεγονός που μπορεί να πλήξει θανάσιμα τη δραστηριότητα των τραπεζών ως «μέσο πληρωμής». Χαρακτηριστικό είναι το παράδειγμα της τηλεφωνικής κάρτας, η οποία, αν και αναπτύχθηκε τελείως έξω από τον τραπεζικό χώρο και αρχικά τουλάχιστον τον θορύβησε, στη συνέχεια ενσωματώθηκε στις τραπεζικές κάρτες, με αποτέλεσμα οι τελευταίες να εκμεταλλευτούν τα οφέλη παροχής μιας ανάλογης υπηρεσίας.

ΚΕΦΑΛΑΙΟ 2ο

ΟΡΙΣΜΟΣ, ΧΡΗΣΗ ΚΑΙ ΕΦΑΡΜΟΓΕΣ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ

1. Εισαγωγικά στοιχεία

Μια έξυπνη κάρτα μοιάζει με μια πιστωτική κάρτα στο μέγεθος και τη μορφή, αλλά εσωτερικά είναι εντελώς διαφορετική. Η διαχείριση των πληροφοριών γίνεται με ασφαλή τρόπο ενώ υπάρχουν πολλαπλές δυνατότητες χρήσης των καρτών. Καταρχήν, μια κανονική πιστωτική κάρτα είναι ένα απλό κομμάτι πλαστικού. Το εσωτερικό της, συνήθως, περιέχει έναν ενσωματωμένο οκτάμπιτο μικροεπεξεργαστή.

Σκεφτείτε, το μικροεπεξεργαστή ως τον αντικαταστάτη της συνηθισμένης μαγνητικής λωρίδας μιας πιστωτικής ή χρεωστικής κάρτας. Σήμερα, οι έξυπνες κάρτες χρησιμοποιούνται σε πολλούς τομείς της καθημερινής μας ζωής. Στις δημόσιες τηλεφωνικές συσκευές, οι Ε.Κ. χρησιμοποιούνται αντί των νομισμάτων. Στον τομέα της υγείας, δίνουν τη δυνατότητα στον ασθενή να έχει, όπου και αν βρίσκεται, όλο το ιατρικό ιστορικό του αποθηκευμένο σε μια Ε.Κ. Επίσης, οι Ε.Κ. μπορούν να περιέχουν ένα χρηματικό ποσό για τις καθημερινές χρηματικές μας συναλλαγές. Όλες αυτές οι διαφορετικές και ανεξάρτητες εφαρμογές μπορούν να συνυπάρχουν σε μια Ε.Κ. κάνοντάς την ένα απαραίτητο εξάρτημα της καθημερινής μας ζωής.

Ο μικροεπεξεργαστής στην έξυπνη κάρτα βρίσκεται εκεί για την ασφάλεια. Ο κεντρικός υπολογιστής δικτύου και ο αναγνώστης καρτών, στη πραγματικότητα, "μιλούν" στο μικροεπεξεργαστή. Ο μικροεπεξεργαστής επιβάλλει την πρόσβαση στα στοιχεία που βρίσκονται στην κάρτα. Εάν ο

κεντρικός υπολογιστής διάβαζε και έγραφε στην μνήμη άμεσης προσπέλασης της έξυπνης κάρτας (RAM), δεν θα υπήρχε καμία διαφορά απ' ότι σε μια δισκέτα.

Οι έξυπνες κάρτες μπορούν να έχουν RAM μεγαλύτερη του 1 kilobyte, 24 kilobyte ROM, 16 kilobyte προγραμματιζόμενης ROM και ένα οκτάμπιτο μικροεπεξεργαστή που τρέχει στα 5 MHz. Η έξυπνη κάρτα χρησιμοποιεί μια σειριακή διεπαφή και λαμβάνει την ισχύ της από εξωτερικές πηγές, όπως έναν αναγνώστη καρτών. Ο επεξεργαστής χρησιμοποιεί ένα περιορισμένο ρεπερτόριο εντολών για εφαρμογές όπως το σύστημα κρυπτογραφίας.

Αυτό που καθιστά την κάρτα "έξυπνη", συγκρίνοντας τη με μια κάρτα μνήμης ή μια μαγνητική κάρτα, είναι η επιβολή των κανόνων ελέγχου πρόσβασης στη μνήμη: για παράδειγμα μερικές περιοχές (όπως το όνομα του κατόχου της κάρτας) μπορούν να γίνουν μόνο αναγνώσιμες, αφού γίνει η πρώτη εγγραφή (που κρατά την αξία της κάρτας).Μπορεί να γίνει εγγραφή μόνο με έναν τρόπο, που επιτρέπει στην αξία της κάρτας να μειωθεί, όχι να αυξηθεί. Αυτός ο έλεγχος πρόσβασης μπορεί να εκτελεσθεί από έναν οκτάμπιτο μικροελεγκτή όμοιο με ένα Motorola 6805 ή ένα Intel 8051.

Μέσα σ' αυτές, υπάρχουν τα προστατευμένα PIN που τις καταστούν παρόμοιες στη φύση με τις κάρτες του ATM που χρησιμοποιούμε. Και, γι' αυτό το θέμα, ακόμα και διεθνώς η αγορά των PC πρέπει να αγκαλιάσει πλήρως τις έξυπνες κάρτες. Ο λόγος είναι η έλλειψη ενός ενσωματωμένου αναγνώστη. Εφαρμογές και συστήματα που χτίζονται συγκεκριμένα για την εργασία χρήσης των έξυπνων καρτών (όπως οι κερματοδέκτες) δουλεύουν εξαιρετικά καλά. Αλλά για την αποδοχή της αγοράς των PC από τους καταναλωτές απαιτείται μια καταλληλότερη λύση. Εκτός από τους προβλέψιμους εφιάλτες της νέας τεχνολογίας, για την επέκταση των αναγνωστών των έξυπνων καρτών, υπάρχει και το ζήτημα του κόστους. Αντίθετα με τους αναγνώστες, οι έξυπνες κάρτες είναι σχετικά οικονομικές.

Έχει ειπωθεί ότι οι έξυπνες κάρτες μια ημέρα θα είναι τόσο σημαντικές όσο είναι οι υπολογιστές σήμερα. Αυτή η δήλωση είναι λίγο λανθασμένη

επειδή υπονοεί ότι οι έξυπνες κάρτες δεν είναι υπολογιστές, όταν στην πραγματικότητα, είναι. Επειδή, οι έξυπνες κάρτες είναι στην πραγματικότητα μικροσκοπικοί υπολογιστές, είναι δύσκολο να προβλεφθεί η ποικιλία των εφαρμογών που θα είναι δυνατή μ' αυτές στο μέλλον. Είναι δυνατόν, οι έξυπνες κάρτες να ακολουθήσουν την ίδια τάση της ραγδαίας αύξησης στη δύναμη της επεξεργασίας που έχουν οι υπολογιστές, διπλασιάζοντας την απόδοση και μειώνοντας το κόστος.

Οι έξυπνες κάρτες εφευρέθηκαν ανεξάρτητα στη Γερμανία (1967), την Ιαπωνία (1970), τις Ηνωμένες Πολιτείες (1972), και τη Γαλλία (1974) Το 1980, όταν η Γαλλία άρχισε μια σημαντική εκστρατεία για να εξάγει την τεχνολογία, ο Roy Bright της κυβερνητικής εμπορικής οργάνωσης, Intelmatique, επινόησε τη φράση "έξυπνη κάρτα" για να περιγράψει την τεχνολογία.

Οι έξυπνες κάρτες είναι δημοφιλέστερες στην Ευρώπη απ' ότι στις Ηνωμένες Πολιτείες. Στην Ευρώπη, η ασφάλεια υγείας και οι τραπεζικές βιομηχανίες χρησιμοποιούν εκτενώς τις έξυπνες κάρτες. Κάθε γερμανός πολίτης έχει μια έξυπνη κάρτα για την ασφάλεια υγείας του. Η τεχνολογία της μαγνητικής λωρίδας παραμένει σε ευρεία χρήση στις Ηνωμένες Πολιτείες. Εντούτοις, τα δεδομένα στη λωρίδα μπορούν εύκολα να διαβαστούν, να γραφτούν, να διαγραφούν ή να αλλάξουν με τη χρήση κάποιου παράνομου εξοπλισμού. Επομένως, η λωρίδα δεν είναι το πραγματικά καλύτερο μέρος για να καταχωρηθούν ευαίσθητες πληροφορίες. Για την προστασία του καταναλωτή, οι επιχειρήσεις στις ΗΠΑ έχουν επενδύσει σε μια απευθείας σύνδεση που βασίζεται στα δίκτυα υπολογιστών μεγάλης ισχύος για την επαλήθευση και την επεξεργασία. Στην Ευρώπη, δεν έχει αναπτυχθεί μια τέτοια υποδομή .

Οι έξυπνες κάρτες έχουν αποδειχθεί αρκετά χρήσιμες ως μέσο συναλλαγής, εξουσιοδότησης και αναγνώρισης στις ευρωπαϊκές χώρες. Όπως αυξάνονται οι ικανότητές τους, θα μπορούσαν να αντικαταστήσουν τελικά όλα τα πράγματα που μεταφέρουμε στα πορτοφόλια μας, συμπεριλαμβανομένου των πιστωτικών καρτών, των αδειών, των μετρητών, ακόμη και των οικογενειακών μας φωτογραφιών. (Οι φωτογραφίες μπορούν να αντιμετωπισθούν

ή/ και να ανταλλαγούν μέσω των ικανών τερματικών ή των προσωπικών υπολογιστών.) Με τον περιορισμό των διάφορων πιστοποιητικών αναγνώρισης, οι έξυπνες κάρτες μπορούν να χρησιμοποιηθούν για να προσδιορίσουν εθελοντικά τις ιδιότητές μας οπουδήποτε και αν βρισκόμαστε ή με οποίο δίκτυο υπολογιστών είμαστε συνδεμένοι. Δεν θα προσπαθήσουμε να προβλέψουμε το μέλλον των δυνατοτήτων της εφαρμογής των έξυπνων καρτών, ούτε τον αντίκτυπό τους στην κοινωνία, αλλά αντί αυτού στρεφόμαστε στη κατάσταση προόδου των έξυπνων καρτών και της χρήσης τους στα συστήματα ασφάλειας υπολογιστών και δικτύων. Οι κάρτες δεν είναι επιστημονικά περιεκτικές σχετικά με κάθε λεπτομέρεια του ολοκληρωμένου κυκλώματος, αλλά αντίθετα προσπαθούν να βρουν μια μέση λύση μεταξύ της ακρίβειας και της δυνατότητας κατανόησης.

Οι ρίζες των διαδεδομένων σήμερα έξυπνων καρτών χαράχτηκαν από τις ΗΠΑ στις αρχές της δεκαετίας του '50, όταν το Dinners Club παρήγαγε την πρώτη πλαστική κάρτα για να χρησιμοποιηθεί για εφαρμογές πληρωμής. Το συνθετικό υλικό PVC που χρησιμοποιήθηκε, επέτρεψε κάρτες μεγαλύτερης διάρκειας απ' ότι οι προηγούμενες συμβατικές κάρτες που βασίζονταν στα έγγραφα(χαρτί). Σε αυτό το σύστημα, μόνο το γεγονός ότι εκδώσατε μια Dinner Club κάρτα, σας επιτρέπει να πληρώνετε με το "καλό σας όνομά" παρά με μετρητά. Στην πραγματικότητα, η κάρτα σας αναγνωρίζει ως μέλος μιας επίλεκτης ομάδας και γίνεστε αποδεκτός από ορισμένα εστιατόρια και ξενοδοχεία που αναγνωρίζουν αυτήν την ομάδα. Η VISA και η MasterCard μπήκαν αργότερα στην αγορά αλλά τελικά με το κόστος της απάτης, τον εμπορικό χειρισμό και το κόστος των τραπεζών κατέστησαν απαραίτητη μια κάρτα που είναι αναγνώσιμη από μια μηχανή.

Η μαγνητική λωρίδα που εισήχθη, επέτρεψε σε περαιτέρω μεταλλαγμένα στοιχεία να αποθηκεύονται στις κάρτες σε ένα αναγνώσιμο από τη μηχανή σχήμα. Αυτός ο τύπος κάρτας, αποτυπωμένος σε ανάγλυφο με μια μαγνητική λωρίδα είναι η πιο συνηθισμένη μέθοδος πληρωμής. Η τεχνολογία των μαγνητικών λωρίδων πάσχει από μια κρίσιμη αδυναμία, αφού ο οποιοσδήποτε με πρόσβαση στην κατάλληλη συσκευή μπορεί να διαβάσει,

να αντιγράψει ή να διαγράψει τα δεδομένα. Κατά συνέπεια, μια κάρτα με μαγνητική λωρίδα είναι ακατάλληλη για τη διαφύλαξη ευαίσθητων στοιχείων. Υπό αυτήν τη μορφή, απαιτείται μια εκτενής απευθείας σύνδεση, συγκεντρωμένη στο πίσω μέρος της υποδομής για την επαλήθευση και επεξεργασία. Αυτός ο τύπος της υποδομής διατέθηκε στις ΗΠΑ αλλά δεν ήταν εύκολα διαθέσιμος στις Ευρωπαϊκές χώρες. Όπως σε οποιαδήποτε αρχιτεκτονική client/server, μια λύση στην αδυναμία επεξεργασίας του πίσω μέρους είναι να προστεθεί ισχύς στο πίσω μέρος της πλευράς του κεντρικού υπολογιστή. Μια άλλη λύση είναι να καταστήσει το κομμάτι του client ισχυρότερο, ανακουφίζοντας, κατά συνέπεια, μερικά από τα καθήκοντα του πίσω μέρους. Οι ευρωπαϊκές χώρες φαίνονται να έχουν προτίμηση στη δεύτερη προσέγγιση και να κάνουν μια τεράστια βελτίωση, πέρα από τη τεχνολογία των μαγνητικών λωρίδων, με την εισαγωγή της κάρτας του ολοκληρωμένου κυκλώματος (ICC).

Το 1968, οι γερμανοί εφευρέτες Jörgen Dethloff και ο Helmut Grötrupp υπέβαλαν αίτηση σχετικά με τα πρώτα ICC διπλώματα ευρεσιτεχνίας. Παρόμοιες εφαρμογές ακολούθησαν η Ιαπωνία το 1970 και η Γαλλία το 1974. Το 1984, το γαλλικό PTT (ταχυδρομικές και τηλεπικοινωνιακές υπηρεσίες) πραγματοποίησε επιτυχώς μια υπαίθρια δοκιμή με τις τηλεφωνικές κάρτες. Μέχρι το 1986, πολλά εκατομμύρια γαλλικές τηλεφωνικές έξυπνες κάρτες βρίσκονταν σε κυκλοφορία. Ο αριθμός τους έφθασε σχεδόν τα 60 εκατομμύρια το 1990 και 150 εκατομμύρια προβλήθηκαν το 1996.

Μεγάλη πρόοδο σημείωσαν το σύστημα κρυπτογραφίας τη δεκαετία του '60 και οι μηχανισμοί ασφάλειας. Οπότε, οι έξυπνες κάρτες αποδεδειγμένα μπορούν να είναι ένα ιδανικό μέσο για τη δημιουργία ακίνδυνων κρυπτογραφικών κλειδιών και αλγορίθμων. Οι γαλλικές τράπεζες ήταν ο πρώτος τομέας που εισήγαγε αυτού του τύπού κάρτες, με μια τραπεζική κάρτα με ενσωματωμένο τσιπ το 1984. Οι γερμανικές τράπεζες άρχισαν να την παρουσιάζουν περίπου το 1997. Άλλη μια εφαρμογή που τοποθετήθηκε στη Γερμανία περιλάμβανε την έκδοση άνω των 70 εκατομμυρίων έξυπνων καρτών, οι οποίες έφεραν πληροφορίες για την ασφάλεια υγείας.

2. Χρήσεις

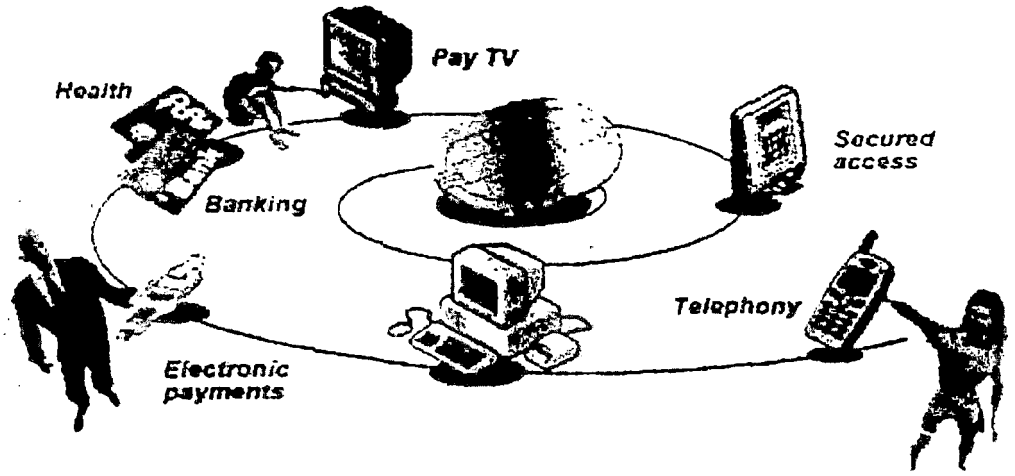
- Η χρήση των έξυπνων καρτών εμφανίζεται σε γενικές κατηγορίες εφαρμογών. Οι έξυπνες κάρτες μπορούν να χρησιμοποιηθούν ως:
- **Χρηματοπιστωτικό μέσο (πιστωτική κάρτα - κάρτα χρέωσης):** διευκολύνουν τις πιστωτικές και χρεωστικές συναλλαγές με ασφαλέστερο τρόπο και περιορίζονται στο ελάχιστο οι πιθανότητες ύπαρξης οποιασδήποτε οικονομικής απάτης..
- **Κλειδιά πρόσβασης:** διευκολύνουν την αυθεντικοποίηση και ταυτοποίηση του κατόχου της και την επεξεργασία δεδομένων, παρέχοντας έτσι ένα ασφαλέστερο περιβάλλον για τη μεταφορά, αποθήκευση και ανταλλαγή πληροφοριών. Οι δυνατότητες των καρτών αυτών τις καθιστούν ιδανικές για εφαρμογές Διαδικτύου (Internet), υπηρεσίες Home-banking ή ακόμα και ως κάρτες μέλους οργανισμών (loyalty cards). Πρόκειται συνήθως για κάρτες τύπου contact, οι οποίες χρησιμοποιούνται για την προμήθεια αγαθών ή υπηρεσιών από συγκεκριμένο έμπορο. Μέσω του κατάλληλου συστήματος, ο έμπορος είναι σε θέση να λάβει λεπτομερείς πληροφορίες για τον πελάτη έχοντας ως αποτέλεσμα τη βελτίωση των υπηρεσιών προς αυτόν.
- **Μέσω Web Browsers:** οι μηχανισμοί αναζήτησης χρησιμοποιούν τεχνολογίες, όπως Secure Sockets Layer(SSL) ή Transport Layer Security(TLS) προκειμένου να προσδώσουν μεγαλύτερη ασφάλεια στο Διαδίκτυο. Οι τεχνολογίες αυτές μπορούν να πραγματοποιήσουν αυθεντικοποίηση του πελάτη-χρήστη και του διακομιστή, παρέχοντας ειδικά κανάλια επικοινωνίας και μεταφοράς μηνυμάτων. Η εισαγωγή της έξυπνης κάρτας εστιάζεται κυρίως στη μεταφορά ειδικού κλειδιού αποκρυπτογράφησης, ώστε να αποφεύγεται οποιαδήποτε προσπάθεια αντιγραφής των σχετικών κλειδιών.
- **Secure E-mail:** όπως και με τις παραπάνω τεχνολογίες και σε αυτήν την εφαρμογή η έξυπνη κάρτα μπορεί να χρησιμοποιηθεί κατά παρόμοιο τρόπο.

- **Kiosk computer:** πολλές εφαρμογές προϋποθέτουν την ύπαρξη κατάλληλου κεντρικού σταθμού (kiosk), που συνδέεται με πολλούς υπολογιστές συγχρόνως (τερματικά). Η ύπαρξη κατάλληλης μνήμης και του μικροεπεξεργαστή παρέχει στο χρήστη τη μεταφορά οικονομικών δεδομένων, δημογραφικών δεδομένων, καθώς και οποιωνδήποτε πληροφοριών θεωρεί αυτός ότι είναι χρήσιμες μέσω μιας φορητής κάρτας
- **Ηλεκτρονικό πορτοφόλι (e-purse):** Προσαρμοσμένες αγοραπωλησίες με τη βοήθεια βάσεων δεδομένων, ηλεκτρονικά κουπόνια, προγράμματα αξιοπιστίας ή ακόμα και πιστοποιητικά δώρων μπορούν να διαχειρισθούν επιτυχώς με τη χρήση έξυπνων καρτών. Το ηλεκτρονικό χρήμα ομοιάζει με την περίπτωση προπληρωμένων τηλεφωνικών καρτών, καθώς η τιμή που περιλαμβάνει η κάρτα είναι προκαθορισμένη και σε οποιαδήποτε χρήση της αφαιρείται το αντίστοιχο ποσό. Χαρακτηριστικό παράδειγμα αυτής της εφαρμογής αποτελούν οι ηλεκτρονικές διατάξεις ανάγνωσης καρτών Automatic Teller Machine (ATM), όπου ο χρήστης με τη βοήθεια κατάλληλου προσωπικού αριθμού αναγνώρισης (PIN) αποκτά πρόσβαση σε κάποιο τραπεζικό δίκτυο, εκτελώντας τραπεζικές συναλλαγές, όπως κατάθεση ή ανάληψη χρημάτων. Οπωσδήποτε και σ' αυτήν την εφαρμογή παρέχεται ένα ασφαλέστερο περιβάλλον με ταυτόχρονη μείωση του κόστους επεξεργασίας των δεδομένων. Η χρήση τους σ' αυτόν τον τομέα εξυπηρετεί κυρίως εφαρμογές προώθησης υπηρεσιών και προϊόντων .
- **Κρυπτογράφηση αρχείων**
- **Ανάληψη ηλεκτρονικού χρήματος**

3. Εφαρμογές

Οι έξυπνες κάρτες επεκτείνονται στους περισσότερους τομείς της δημόσιας και ιδιωτικής αγοράς. Οι κάρτες ενιαίας λειτουργίας χρησιμοποιούνται για την καρτοτηλεφωνία, την ψηφιακή κινητή τηλεφωνία (αυτές οι κάρτες από μία άποψη δε προσαρμόζονται στο βασικό ορισμό μίας έξυπνης

κάρτας), τις λειτουργίες πίστωσης και χρέωσης των οικονομικών οργανισμών, τα συνεταιρικά συστήματα προσωπικού, τις λειτουργίες της συνδρομητικής τηλεόρασης και πολλά άλλα. Με την εμφάνιση των καρτών-πολυεφαρμογών, ικανών να μεταφέρουν δεδομένα που σχετίζονται με διάφορες λειτουργίες, τα πιο σύνθετα σχέδια αναπτύσσονται ιδιαίτερα, από τις πόλεις για τους πολίτες και από κεντρικές κυβερνήσεις για τους κατοίκους τους. Στα περισσότερα από αυτά σχέδια ,οι απλές δομές δεδομένων κρατιούνται και ενημερώνονται μέσα στις κάρτες, συμπεριλαμβάνοντας τις προσωπικές πληροφορίες για τον κάτοχο της κάρτας και τη σχέση του λογαριασμού του, ή της κάρτας και του εκδότη της εφαρμογής μαζί με τα διεξαγόμενα δεδομένα. Τα κεντρικά συστήματα των διαδικασιών συχνά καθρεφτίζουν αυτά τα δεδομένα, έχοντας συλλέξει αυτά μέσω ενός μηχανισμού συγκέντρωσης από τα τερματικά, τα οποία δέχονται οι ειδικές κάρτες και τους επιτρέπουν να συμμετάσχουν στις σχετικές συναλλαγές.



ΣΧΗΜΑ 1: Χαρακτηριστικές εφαρμογές

Η πρώτη εισαγωγή των έξυπνων καρτών έγινε, ως εργαλείο καταχωρημένης αξίας, στην προπληρωμένη τηλεφωνία(pay phones), για να μειωθούν οι κλοπές. Όπως στις έξυπνες κάρτες και άλλες αναβαθμισμένες κάρτες που βασίζονταν στα τσιπ, οι άνθρωποι βρήκαν νέους τρόπους να τις χρησιμοποιούν. Οι καταναλωτές χρησιμοποιούν τις κάρτες τσιπ για τα πάντα, από την επίσκεψη τους σε βιβλιοθήκες μέχρι την αγορά ταινιών από βιντεο-

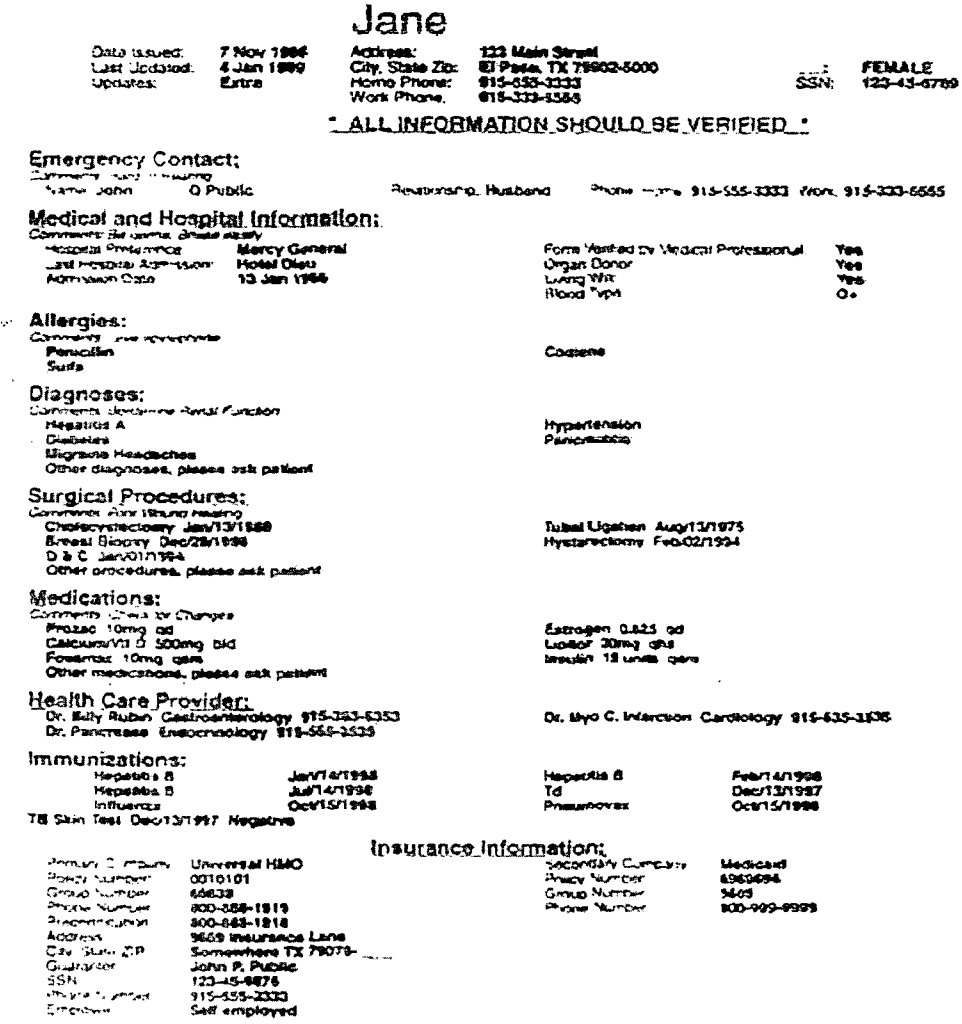
κλάμπ και εγκαθίστανται σταθερά στη καθημερινή μας ζωή. Διάφορα κράτη έχουν προγράμματα καρτών τσιπ υπό εξέλιξη στις κυβερνητικές τους εφαρμογές που παρατάσσονται από το τμήμα οχημάτων μέχρι την ηλεκτρονική μεταφορά οφελών (EBT). Πολλές βιομηχανίες έχουν εφαρμόσει τις δυνατότητες των έξυπνων καρτών στα προϊόντα τους, όπως τα νέα ψηφιακά κυψελοειδή τηλέφωνα GSM και τους αποκωδικοποιητές της δορυφορικής TV.

Οι πιο κοινές εφαρμογές των έξυπνων καρτών είναι:

- **Τηλεφωνικές κάρτες:** Προπληρωμένες τηλεφωνικές κάρτες (είτε κάρτες μνήμης είτε κάρτες με μικροεπεξεργαστή) συγκεκριμένων ποσών παρέχονται στους χρήστες προς εξυπηρέτηση τους σε δημόσια τηλέφωνα, τα οποία είναι εξοπλισμένα με τις αντίστοιχες ηλεκτρονικές διατάξεις ανάγνωσης. Η χρήση τους έγινε για πρώτη φορά το 1986 στη Γαλλία, με στόχο τη μείωση της ζημίας λόγω απατής η βανδαλισμών, του κόστους λειτουργίας που συνδέεται με τη συγκέντρωση των νομισμάτων και τη συντήρηση των τηλεφώνων, καθώς και την αποτελεσματικότερη εξυπηρέτηση του κοινού. Το 1995, οι πωλήσεις των καρτών σε αυτόν τον τομέα υπολογίζεται ότι ξεπέρασαν τα 400 εκατομμύρια σε περισσότερες από 70 χώρες.

- **Κάρτες υγείας**: Οι κάρτες αυτές έχουν τη δυνατότητα αποθήκευσης διαφορετικών ειδών ιατρικής πληροφορίας του κατόχου τους, όπως παραδείγματος χάρη τρέχουσες συνταγές φαρμάκων, αλλεργίες, χρόνια προβλήματα του ασθενούς κ.λ,π. Επιπρόσθετα, πραγματοποιείται αναγνώριση ταυτότητας του κατόχου-ασθενούς για επιβεβαίωση κάλυψης εξόδων από ασφαλιστικές εταιρείες, νοσοκομεία, ταμεία ασφαλίσεων. Η κάρτα αυτή θεωρείται δυναμική, αφού μπορεί να αποθηκεύσει νέα δεδομένα, όταν η κατάσταση υγείας του κατόχου αλλάξει. Αποτέλεσμα της χρήσης της από ασθενείς είναι η βελτίωση της ποιότητας της ιατρικής αγωγής, η μείωση του διοικητικού κόστους και η εύκολη πρόσβαση σε πληροφορίες άμεσης ανάγκης (σχήμα 2), Τέλος, περιορίζεται η πιθανότητα πρόσβασης ατόμων μη σχετικών με τη θεραπεία ή την εφαρμογή, δηλαδή εκτός γιατρών, νοσηλευτών ή τεχνολόγων υγείας, τα οποία ενδέχεται να αλλοιώσουν τις ιατρικές πληρο-

φορίες, θέτοντας σε κίνδυνο την υγεία του ασθενούς. Υπολογίζεται, ότι στη Γαλλία περίπου 500 χιλιάδες ασθενών χρησιμοποιούν ευρύτατα τις κάρτες υγείας.


Jane

Data Issued: 7 Nov 1994 Address: 123 Main Street
Last Updated: 4 Jan 1999 City, State Zip: El Paso, TX 79902-5000 FEMALE
Updates: Extra Home Phone: 915-653-3333 SSN: 123-45-6789
Work Phone: 915-333-5555

* ALL INFORMATION SHOULD BE VERIFIED *

Emergency Contact:
Name: John Q Public Relationship: Husband Phone: 915-555-3333 Work: 915-333-5555

Medical and Hospital Information:
Hospital Preference: Mercy General
Last Hospital Admission: Hotel Dieu
Admission Date: 13 Jan 1994
Form Verified by Medical Professional: Yes
Organ Donor: Yes
Living Will: Yes
Blood Type: O+

Allergies:
Penicillin
Sulfa
Codeine

Diagnoses:
Hepatitis A
Diabetes
Migraine Headaches
Other diagnoses, please ask patient
Hypertension
Pancreatitis

Surgical Procedures:
Cholecystectomy Jan/13/1988
Breast Biopsy Dec/28/1996
D & C Jan/01/1984
Other procedures, please ask patient
Tubal Ligation Aug/13/1975
Hysterectomy Feb/02/1994

Medications:
Prozac 10mg qd
Calcium/Vit D 500mg bid
Fosamax 10mg qam
Other medications, please ask patient
Estrogen 0.625 qd
Lipitor 20mg qhs
Insulin 18 units qam

Health Care Provider:
Dr. Billy Rubin Gastroenterology 915-333-5353
Dr. Pancrease Endocrinology 915-555-3535
Dr. Myo C. Infarction Cardiology 915-635-3535

Immunizations:
Hepatitis B Jan/14/1994
Hepatitis B Jul/14/1994
Influenza Oct/15/1994
Hepatitis B Feb/14/1996
Td Dec/13/1997
Pneumovax Oct/15/1996
TB Skin Test Dec/13/1997 Negative

Insurance Information:
Primary Company: Universal HMO
Policy Number: 0016101
Group Number: 66633
Phone Number: 800-555-1515
Precertification: 800-555-1516
Address: 9669 Insurance Lane
City, State, ZIP: Somewhere TX 79078-
Guarantor: John P. Public
SSN: 123-45-6676
Phone Number: 915-555-3333
Employer: Self employed
Secondary Company: Medicaid
Policy Number: 6969696
Group Number: 5405
Phone Number: 800-999-9999

ΣΧΗΜΑ 2: Ιατρική εφαρμογή έξυπνης κάρτας

Τραπεζικές κάρτες: Οι γαλλικές τράπεζες αποτέλεσαν τους πρωτοπόρους στον τομέα αυτό στοχεύοντας με την ύπαρξη κατάλληλων συστημάτων, στη μείωση της ζημίας λόγω κλοπών ή απάτης, στην ελαχιστοποίηση οποιωνδήποτε λαθών και στη βελτίωση των παρεχόμενων υπηρεσιών από αυτές.

Υπάρχουν τρεις βασικοί τύποι πιστωτικών καρτών:

- ❖ τραπεζικές κάρτες, που εκδίδονται από τις τράπεζες (παραδείγματος χάριν, η Visa, MasterCard και Discover card)
- ❖ κάρτες ταξιδιού και ψυχαγωγίας (T&E), όπως American Express και Dinners Card
- ❖ κάρτες σπιτιού που είναι καλές μόνο σε μια αλυσίδα καταστημάτων (Sears είναι η μεγαλύτερη από αυτές, και ακολουθείται από τις επιχειρήσεις πετρελαίου, τις τηλεφωνικές επιχειρήσεις και τα τοπικά τμήματα καταστημάτων).

Μπορείτε επίσης να εξοικειωθείτε με τις γνωστές κάρτες συγγένειας. Αυτή η κάρτα -- χαρακτηριστικά η MasterCard ή η Visa -- φέρει και το λογότυπο ενός οργανισμού εκτός από το έμβλημα του δανειστή. Συνήθως, αυτοί οι κάτοχοι καρτών αποκομίζουν κάποιο όφελος χρησιμοποιώντας τη κάρτα -- ίσως τα μίλια συχνών πτήσεων ή οι πόντοι σχετικά με τα εμπορεύματα. Οι οργανισμοί δελεάζουν τα μέλη τους για να πάρουν τις κάρτες, με την ιδέα να κρατηθεί το όνομα του ομίλου μπροστά από τον κάτοχο της κάρτας. Εκτός από την καθιέρωση των εμπορικών σημάτων, ο οργανισμός λαμβάνει κάποια οικονομικά κίνητρα (ένα μέρος της ετήσιας αμοιβής ή των εξόδων χρηματοδότησης ή κάποιο μικρό ποσό ανά συναλλαγή ή ένας συνδυασμός απ' αυτά) από την επιχείρηση πιστωτικών καρτών.

- **Κάρτες Pay TV**: Οι κάρτες αυτές προϋποθέτουν την εγγραφή του συνδρομητή-κατόχου σε καλωδιακού δικτύου τηλεόραση. Η κάρτα, στην περίπτωση αυτή, λειτουργεί ως προπληρωμή της εφαρμογής που απαιτεί ο συνδρομητής και περιλαμβάνει τα στοιχεία λογαριασμού και της αναγνώρισης του κατόχου της. Ο χρήστης είναι σε θέση να χρησιμοποιήσει την κάρτα οπουδήποτε (από το σπίτι του ή από ένα Ξενοδοχείο), αποκτώντας πρόσβαση στις εφαρμογές του δικτύου. Η χρήση τους, όμως, δεν περιορίζεται μόνο στην καλωδιακή τηλεόραση αλλά και στις υπηρεσίες δορυφορικής τηλεόρασης, με τη διαδικασία πρόσβασης να είναι απολύτως όμοια. Υπολογίζεται ότι περίπου 10 εκατομμύρια κάρτες αυτού του τύπου χρησιμοποιήθηκαν σε ολόκληρο τον κόσμο το έτος 1994.

- **Κάρτες GSM**: Για υπηρεσίες κινητής τηλεφωνίας GSM, χρησιμοποιούνται έξυπνες κάρτες τύπου contact, όπου ο προσδιορισμός ταυτότητας του χρήστη στο τηλεφωνικό σύστημα πραγματοποιείται με το Security Identity Module. Η κάρτα μπορεί να χρησιμοποιηθεί σε οποιοδήποτε κινητό GSM τηλέφωνο, ενώ η χρέωση του λογαριασμού αποστέλλεται στον ιδιοκτήτη της κάρτας. Το 1994, υπολογίζεται ότι πωλήθηκαν περισσότερες από 9 εκατομμύρια κάρτες σε αυτόν τον τομέα, ενώ η ευρεία χρήση των κινητών τηλεφώνων τα τελευταία χρόνια έχει αυξήσει ραγδαία τον αριθμό των πωλήσεων

- **Εισιτήρια μεταφοράς**: Πρόκειται, συνήθως, για κάρτες τύπου contactless, οι οποίες διατίθονται σε προκαθορισμένες τιμές. Η τιμή της κάρτας αφαιρείται κάθε φορά που χρησιμοποιείται από τον κάτοχο της για κάποια μεταφορά. Η χρήση τους θεωρείται αποδοτική στα μέσα μαζικής μεταφοράς, όπου διευκολύνεται το κοινό, ενώ ταυτόχρονα μειώνεται το διοικητικό κόστος.

- **Ηλεκτρονικές ταυτότητες**: Στην εφαρμογή αυτή κυρίως ανήκουν κυβερνητικά προγράμματα και πανεπιστήμια, όπου απλά παραδείγματα είναι η πρόσβαση των φοιτητών σε βιβλιοθήκες ή άλλες ευκολίες που παρέχει το πανεπιστήμιο, η απόκτηση πρόσβασης σε στρατιωτικές υπηρεσίες ή κτίρια. Η χρήση των καρτών σ' αυτού του είδους τις εφαρμογές παρέχει στα άτομα κατευθείαν και γρηγορότερη πρόσβαση σε συνδυασμό με μεγαλύτερη ασφάλεια και ευκολία. Επιπροσθέτως, εμφανίζονται και άλλα πλεονεκτήματα, όπως μείωση ζημιών, αυτοματοποιημένη διαχείριση των εγγράφων και μείωση οποιουδήποτε κόστους λειτουργίας.

- **Κάρτες διοδίων**: Οι εταιρίες κατασκευής γεφυρών, διοδίων και σηράγγων εισήγαγαν τη χρήση των έξυπνων καρτών, προκειμένου να διευκολύνουν τους πελάτες και να μειώσουν το κόστος λειτουργίας, με τη βοήθεια κατάλληλων συστημάτων, που ονομάζονται Electronic Toll and Management Systems (ETTM). Επίσης, επιτρέπουν τη συλλογή του χρηματικού αντίτιμου χωρίς την παρεμπόδιση της κυκλοφορίας, αφού η αντίστοιχη τιμή αφαιρείται κάθε φορά που πραγματοποιείται διέλευση του κατόχου

από ηλεκτρονικά διόδια, από το ποσό που περιέχει η κάρτα. Τέλος, εξαλείφεται κάθε κίνδυνος ζημίας από απάτη ή ληστεία.

- **Κάρτες στάθμευσης**: Ομοιάζουν στις αντίστοιχες προπληρωμένες τηλεφωνικές κάρτες με τη διαφορά ότι χρησιμεύουν για τη στάθμευση οχημάτων με την τιμή να αφαιρείται σε κάθε χρήση της κάρτας. Με αυτόν τον τρόπο, μειώνονται τα κόστη συντήρησης και επιδιόρθωσης των απαραίτητων μηχανημάτων, καθώς και τα αντίστοιχα συλλογής των κερμάτων, ενώ παράλληλα περιορίζονται οι πιθανότητες ζημίας λόγω κλοπών ή απάτης.

- **Κάρτες επιβάτη:** Μεγάλες αεροπορικές εταιρείες, όπως οι Lufthansa, Delta και American Airlines προχώρησαν στη χρήση έξυπνων καρτών, όπου περιέχονται δυο επεξεργαστές: ένας τύπου contact και άλλος ένας τύπου contactless. Ο επεξεργαστής τύπου contact παρέχει στο χρήστη την ευχέρεια αυτόματης αγοράς αεροπορικών εισιτηρίων, πιστωτικής πρόσβασης, προπληρωμής τηλεφωνικών συνδιαλλαγών και αποθήκευσης αριθμών πτήσεων. Από την άλλη μεριά, ο επεξεργαστής τύπου contactless επιτρέπει την επιβίβαση του επιβάτη στο αεροπλάνο μέσα σε σύντομο χρονικό διάστημα. Τα πλεονεκτήματα της παραπάνω εφαρμογής είναι όμοια με τις προαναφερόμενες περιπτώσεις, ενώ επιπλέον μειώνεται ο όγκος των απαραίτητων εγγράφων και πραγματοποιείται σημαντική εξοικονόμηση χρόνου. Στατιστικά, η χρήση τέτοιων καρτών προτιμάται κατά 85% από τους ερωτηθέντες επιβάτες σε σύγκριση με το τυπικό αεροπορικό εισιτήριο.

- **Κάρτες πρόσβασης:** Η βιομηχανία ξενοδοχειακών εγκαταστάσεων έχει πραγματοποιήσει πληθώρα πειραμάτων προς διευκόλυνση του ελέγχου εισόδου, της πληρωμής των παρεχόμενων υπηρεσιών και των διαδικασιών ελέγχου αναχώρησης των πελατών. Η χρήση των καρτών σε αυτόν τον τομέα θεωρείται απαραίτητη λόγω της υψηλής ζημίας των ξενοδοχείων από υπηρεσίες, οι οποίες δεν έχουν συμπεριληφθεί στον τελικό λογαριασμό λόγω ανθρωπίνου λάθους. Επιπλέον, διευκολύνονται οι πελάτες, ενώ παρέχεται ασφάλεια και αξιοπιστία στις πραγματοποιούμενες συναλλαγές.

Αναμφίβολα, είναι αδύνατο να καλύψουμε κάθε χρήση και εφαρμογή των έξυπνων καρτών, εφόσον η χρήση τους θεωρείται απεριόριστη και

η μελλοντική τους εξέλιξη ραγδαία σε όλους τους τομείς ακόμα και μέρα με τη μέρα. Γεγονός είναι, ότι ταυτόχρονα με την ανάπτυξη της τεχνολογίας θα συμβαδίζει και η εισαγωγή των καρτών σε ποικίλους τομείς, με στόχο πάντοτε τη μείωση του κόστους, τη διευκόλυνση των χρηστών και την παροχή ασφάλειας σε οποιαδήποτε ενέργεια.

4. Παραδείγματα εφαρμογών και πιλοτικά προγράμματα

Ιατρικά αρχεία:

Χαρακτηριστικότερο παράδειγμα της εισαγωγής των έξυπνων καρτών στο χώρο της ιατρικής, αποτελεί η χρήση τους για την αποθήκευση των ιατρικών αρχείων των ασθενών, εφαρμογή που κρίνεται ιδιαίτερα σημαντική για την απλοποίηση ιατρικών διαδικασιών.

Τα ιατρικά αρχεία, αναμφισβήτητα, αθροίζονται σε υπερβολικά μεγάλο όγκο δεδομένων, αφού τα αρχεία ενός ασθενούς κατά τη διάρκεια της ζωής του μπορούν να ποικίλλουν από μερικά kilobytes ως και megabytes, όταν παρουσιάζονται χρόνιες παθήσεις. Οπωσδήποτε, η αποθήκευση αυτών των μεγεθών στην κάρτα κρίνεται μη εφικτή με την παρούσα τεχνολογία έξυπνων καρτών, με αποτέλεσμα να θεωρείται αναγκαία η προσέγγιση εναλλακτικών μεθόδων, όπως::

- Η διαχείριση των δεδομένων σε online πληροφοριακό σύστημα, ενώ η κάρτα ιατρικής πληροφορίας αποτελεί μέσο ελέγχου της πρόσβασης του χρήστη (αυθεντικοποίηση) στα αρχεία.
- Η διατήρηση βασικών ιατρικών πληροφοριών στην κάρτα με αναφορές στα αντίστοιχα τηρούμενα λεπτομερέστερα αρχεία που βρίσκονται στο online σύστημα.
- Η χρήση της κάρτας για συγκεκριμένες εφαρμογές ή υπό συγκεκριμένες συνθήκες (π.χ. νοσοκομειακή περίθαλψη ή μόνο παιδιατρική κάρτα).
- Περιορισμός της χρήσης της κάρτας σαν μέσου επικοινωνίας μεταξύ των επαγγελματιών υγείας σε πολύ συγκεκριμένες εφαρμογές (π.χ. συνταγές η εξετάσεις).

- Η χρήση της κάρτας σε συνδυασμό με άλλη κάρτα ή σύστημα, το οποίο να έχει αποθηκευμένες ας απαραίτητες πληροφορίες.

Η πρώτη επιλογή (full online storage) θεωρείται και ως η πιο εφικτή σε συστήματα, όπου οι ασθενείς χρησιμοποιούν πολλαπλές υπηρεσίες υγείας ή διαφορετικούς παροχείς υπηρεσιών υγείας. Το πλεονέκτημα της μεθόδου αυτής είναι η χρήση της κάρτας από τον κάτοχο της. οποτεδήποτε του παρέχεται κάποια υπηρεσία, αποθηκεύοντας συγχρόνως οποιαδήποτε ιατρική πληροφορία στο αρχείο του.

Η δεύτερη από τις παραπάνω λύσεις (αποθήκευση του ελαχίστου των πληροφοριών στην κάρτα) χρησιμοποιείται ευρέως σήμερα, ενημερώνοντας τον θεράποντα ιατρό για ειδικές συνθήκες ή εξετάσεις που θα επιφέρουν αποτελεσματικότερη θεραπευτική αγωγή του ασθενούς. Κάθε μία από τις υπόλοιπες επιλογές έχει εφαρμοστεί και θεωρείται ότι υπολείπονται σε πλεονεκτήματα έναντι των προαναφερόμενων μεθόδων.

Χαρακτηριστικό παράδειγμα στις κάρτες ασφάλισης ασθενών αποτελεί το πρόγραμμα Versichertenkarte στη Γερμανία, οπού η κάρτα παρέχεται σε κάθε ασφαλιζόμενο (περίπου 70 εκατομμύρια κάρτες). Την κύρια διάταξη ασφαλείας των καρτών αυτών αποτελεί η γενική χρήση μνήμης write-protected, όπου η κάρτα μπορεί να "διαβαστεί" σε οποιοδήποτε νοσοκομείο η κλινική που είναι εξουσιοδοτημένη ,αλλά τα δεδομένα μπορούν να αποσταλούν στην κάρτα μονό από τον ασφαλιστή. Επιπλέον, οι κάρτες περιέχουν μια περιοχή εξουσιοδότησης που επιτρέπει στον κάθε ασφαλιστή να αναγνωρίζει τις κάρτες που είναι στη δικαιοδοσία του.

Τα τελευταία χρόνιο έχουν προταθεί πλήθος τεχνολογιών σχετικά με ιατρικές κάρτες, όπως για παράδειγμα στην Ιαπωνία και την Κίνα, όπου υπάρχουν ήδη σε μεγάλη κλίμακα συστήματα, που χρησιμοποιούν οπτικές κάρτες. Η μεγάλη χωρητικότητα και η δυνατότητα εγγραφής γίνεται μόνο μία φορά, ενώ η ανάγνωση της κάρτας μπορεί να πραγματοποιηθεί πολλές φορές. Αυτά, αποτελούν στοιχεία που καθιστούν την τεχνολογία αυτή ιδανική για χρήση σε εφαρμογές ιατρικών αρχείων.

Η Ευρωπαϊκή ένωση έχει ήδη θέσει σε εφαρμογή δυο προγράμματα ιατρικών αρχείων. τα οποία χρησιμοποιούν έξυπνες κάρτες:

Cardlink: έχουν μοιραστεί έξυπνες κάρτες σε περίπου 250.000 ασθενείς διαφόρων ευρωπαϊκών κρατών. Σκοπός του προγράμματος είναι η δοκιμή των συστημάτων κωδικοποίησης και της ευκολίας χρήσης, όπως και της ασφαλείας και των μελλοντικών απαιτήσεων.

Diabcard: οι κάρτες αυτές θα προσφερθούν σε περίπου 1.000 ασθενείς με χρόνιες παθήσεις, αφού σ' αυτό το στάδιο οι διεργασίες έχουν καθαρά αναγνωριστικό χαρακτήρα.

Παράδειγμα εφαρμογής παρόμοιων προγραμμάτων αποτελεί η προσπάθεια της Γαλλίας μέσω των καρτών Santal ,οι οποίες είναι κάρτες μνήμης (memory cards) με καταχωρημένα κάποια δεδομένα. Τα δεδομένα αυτά μπορούν να ανακτηθούν μόνο από τους ιατρικούς επαγγελματίες, με χρήση της αντίστοιχης επαγγελματικής κάρτας που διαθέτουν .

Ενδιαφέρον παρουσιάζει και η λειτουργία ενός παρόμοιου προγράμματος στο νησί του Σαν Μαρίνο, 25.000 κατοίκων, όπου η τοπική τράπεζα παρέχει σε όλους τους κατοίκους μία έξυπνη κάρτα, για χρήση σε τερματικά τραπεζικών συνδιαλλαγών (ATM) και σαν πιστωτική κάρτα. Όμως, η κάρτα περιλαμβάνει μία ξεχωριστή ιατρική ζώνη, η οποία μπορεί να «διαβαστεί» από τα τοπικά νοσοκομεία, κλινικές και από φαρμακοποιούς ή ιατρικούς θεραπευτές.

Ομοίως, στην πόλη του Λεβερκούζεν στη Γερμανία, λαμβάνει χώρα ένα άλλο πιλοτικό πρόγραμμα (ένα υβριδικό opto-smart card πρόγραμμα). Η παραπάνω κάρτα περιέχει μια οπτική περιοχή μνήμης και ένα μικροεπεξεργαστή πολυεφαρμογών, σύμφωνα με τα πρότυπα ISO. Οι διοικητικές πληροφορίες των αρχείων αποθηκεύονται στον μικροεπεξεργαστή, όμως η πλειοψηφία των ιατρικών δεδομένων αποθηκεύονται στην οπτική μνήμη, αλλά σε κωδικοποιημένη μορφή. Ως επακόλουθο, ο αριθμός των οπτικών συστημάτων ανάγνωσης περιορίζεται αισθητά για τους εξής λόγους::

ΚΕΦΑΛΑΙΟ 3ο

ΛΕΙΤΟΥΡΓΙΑ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ

1. Η φυσική δομή των έξυπνων καρτών

Αυτό το τμήμα συζητά τη φυσική δομή μιας έξυπνης κάρτας και εξετάζει τα συστατικά της. Επίσης, αναφέρεται σε όλες τις φάσεις του κύκλου ζωής μιας κάρτας και ερευνά πώς το microchip χειρίζεται και μεταφέρει τα δεδομένα ασφαλή από τον κατασκευαστή της κάρτας στον προμηθευτή της εφαρμογής και έπειτα στο φορέα. Κατά συνέπεια, να προσδιορίσουμε πώς τα δεδομένα ή οι πληροφορίες που αποθηκεύονται στη κάρτα μπορούν να προστατευθούν.

Φυσική δομή

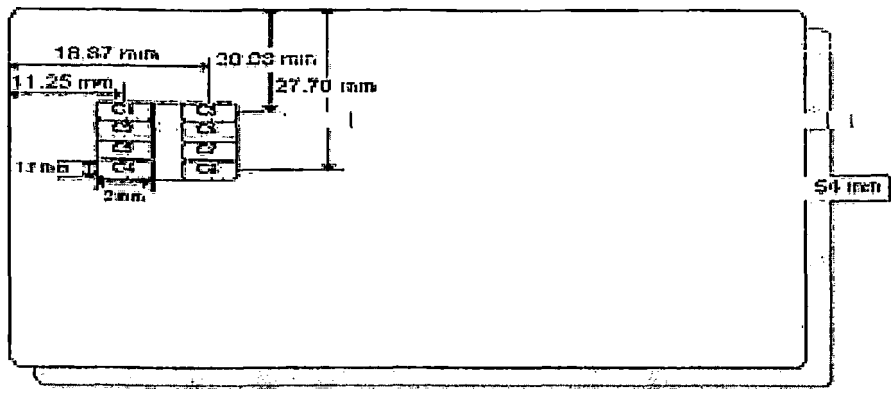
Η φυσική δομή μιας έξυπνης κάρτας προσδιορίζεται από την οργάνωση διεθνών προτύπων (ISO) 7810, το 7816/1 και 7816/2.

Προσδιορίζονται δύο φυσικές διαστάσεις για τις έξυπνες κάρτες. Η δημοφιλέστερη μορφή είναι περίπου στο μέγεθος μιας πιστωτικής κάρτας. Η πλαστική κάρτα είναι το πιο βασικό και έχει διαστάσεις 85.60mm X 53.98mm X 0.80mm. Η κάρτα είναι αρκετά μικρή για να είναι εύκολα φορητή, αλλά από την άλλη πλευρά είναι αρκετά μεγάλη για να παρουσιάσει γραφικά και διαφημίσεις.

Το δεύτερο, μικρότερο μέγεθος έξυπνων καρτών, προσδιορίζεται από το ευρωπαϊκό ινστιτούτο προτύπων τηλεπικοινωνιών (ETSI) και χρησιμοποιείται συγκεκριμένα από το παγκόσμιο σύστημα επικοινωνίας της κινητής

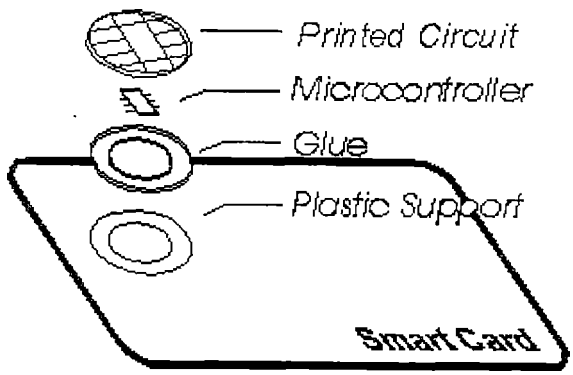
τηλεφωνίας (GSM), το κυρίαρχο κυψελοειδές σύστημα τηλεφωνικής τεχνολογίας στην Ευρώπη.

Figure 17-1: Smartcard Physical Dimensions



ΣΧΗΜΑ 3: Φυσικές διαστάσεις έξυπνης κάρτα

Ένα τυπωμένο κύκλωμα και ένα τσιπ ολοκληρωμένων κυκλωμάτων ενσωματώνονται στην κάρτα. Το σχήμα 4 παρουσιάζει τη φυσική δομή μιας έξυπνης κάρτας.



Σχήμα 4: Φυσική δομή μιας έξυπνης κάρτας (πηγή: της Philips DX εγχειρίδιο αναφοράς έξυπνων καρτών, 1995)

Το τυπωμένο κύκλωμα προσαρμόζεται στα πρότυπα του ISO 7816/3, που παρέχουν πέντε σημεία σύνδεσης για τη ισχύ και τα δεδομένα. Το καθο-

ρίζει ερμητικά στην εσοχή που υπάρχει στην κάρτα και καίγεται επάνω στο τσιπ κυκλωμάτων, γεμίζει με ένα αγώγιμο υλικό και σφραγίζεται με τη σύνδεση των προεξοχών. Το τυπωμένο κύκλωμα προστατεύει το τσιπ κυκλωμάτων από τη μηχανική πίεση και τη στατική ηλεκτρική ενέργεια. Η επικοινωνία με το τσιπ ολοκληρώνεται μέσω των επαφών που επιστρώνουν το τυπωμένο κύκλωμα.

Η ικανότητα μιας έξυπνης κάρτας καθορίζεται από το τσιπ ολοκληρωμένων κυκλωμάτων της. Χαρακτηριστικά, ένα τσιπ ολοκληρωμένων κυκλωμάτων αποτελείται από έναν μικροεπεξεργαστή, μια μνήμη μόνο για ανάγνωση (ROM), μια μη στατική μνήμη τυχαίας προσπέλασης (RAM) και μία ηλεκτρικά εξαλείψιμη προγραμματίσιμη μνήμη μόνο για ανάγνωση (EEPROM), που θα διατηρήσει τη κατάστασή του όταν αφαιρείται η ισχύς. Το τρέχον τσιπ κυκλωμάτων γίνεται από πυρίτιο που δεν είναι εύκαμπτο και ιδιαίτερα εύκολο να σπάσει. Επομένως, προκειμένου να αποφευχθεί η θραύση όταν κάμπτεται η κάρτα, το τσιπ είναι περιορισμένο μόνο σε μερικά χιλιοστά.

Επιπλέον, η φυσική διεπαφή, που επιτρέπει την ανταλλαγή δεδομένων μεταξύ του τσιπ ολοκληρωμένων κυκλωμάτων και της συσκευής αποδέκτη καρτών (CAD), περιορίζεται σε 9600 μπιτ ανά δευτερόλεπτο. Η γραμμή επικοινωνίας είναι μια αμφίδρομη γραμμή τμηματικής μετάδοσης που προσαρμόζεται στα πρότυπα του ISO 7816/3. Όλες οι ανταλλαγές δεδομένων είναι υπό τον έλεγχο της κεντρικής μονάδας επεξεργασίας στο τσιπ ολοκληρωμένων κυκλωμάτων. Η κάρτα διατάζει και τα δεδομένα εισόδου στέλνονται στο τσιπ που απαντάει με λέξεις θέσης και δεδομένα εξόδου, κατά τη παραλαβή αυτών των εντολών και των δεδομένων. Οι πληροφορίες στέλνονται κατά τέτοιο τρόπο, ώστε η μετάδοση των δεδομένων να γίνεται προς μια κατεύθυνση τη φορά. . Αυτό το πρωτόκολλο μαζί με τον περιορισμό του ποσοστού των bit αποτρέπει τη μαζική επίθεση δεδομένων στην κάρτα.

Γενικά, το μέγεθος, το πάχος και οι απαιτήσεις κάμψης για τις έξυπνες κάρτες έχουν ως σκοπό να προστατεύσουν την κάρτα από φυσικές καταστροφές. Εντούτοις, αυτό περιορίζει τους πόρους μνήμης και επεξεργασίας

που μπορούν να τοποθετηθούν στην κάρτα. Κατά συνέπεια, οι έξυπνες κάρτες πρέπει πάντα να ενσωματώνουν άλλες εξωτερικές περιφερειακές μονάδες για να λειτουργήσουν. Παραδείγματος χάριν, μπορεί να απαιτήσει μια συσκευή για να παρέχει την εισαγωγή και την έξοδο των χρηστών, πληροφορίες χρόνου, ημερομηνίας, δύναμη και τα λοιπά. Αυτοί οι περιορισμοί μπορούν να υποβιβάσουν την ασφάλεια μιας έξυπνης κάρτας σε μερικές περιστάσεις, δεδομένου ότι τα εξωτερικά στοιχεία είναι αμφίβολα και αβέβαια.

2. Κύκλος ζωής μιας έξυπνης κάρτας

Η έξυπνη κάρτα, ένα ευφυές σημείο, είναι μια πλαστική κάρτα στο μέγεθος της πιστωτικής που ενσωματώνει ένα τσιπ ολοκληρωμένων κυκλωμάτων. Παρέχει όχι μόνο την ικανότητα της μνήμης, αλλά και την υπολογιστική ικανότητα, επίσης. Ο αυτοπεριορισμός της έξυπνης κάρτας την καθιστά ανθεκτική στην επίθεση, δεδομένου ότι δεν πρέπει να εξαρτηθεί από ενδεχόμενες εξωτερικές πηγές. Λόγω αυτών των χαρακτηριστικών, οι έξυπνες κάρτες χρησιμοποιούνται συχνά σε διαφορετικές εφαρμογές που απαιτούν ισχυρή προστασία και επικύρωση ασφάλειας.

Για παράδειγμα, μία έξυπνη κάρτα μπορεί να ενεργήσει ως κάρτα ταυτοποίησης η οποία χρησιμοποιείται για να αποδείξει την ταυτότητα του κατόχου της κάρτας. Μπορεί, επίσης, να είναι μια ιατρική κάρτα που αποθηκεύει το ιατρικό ιστορικό ενός προσώπου. Επιπλέον, η έξυπνη κάρτα μπορεί να χρησιμοποιηθεί ως τραπεζική κάρτα πίστωσης / χρέωσης που επιτρέπει τις εκτός σύνδεσης συναλλαγές. Όλες αυτές οι εφαρμογές απαιτούν να αποθηκευτούν στην κάρτα, όπως οι πληροφορίες βιομετρικής του ιδιοκτήτη της κάρτας, των κρυπτογραφικών κλειδιών για την επικύρωση, κ.λ.π.

Στο εγγύς μέλλον, η παραδοσιακή μαγνητική κάρτα θα αντικατασταθεί και θα ενσωματωθεί σε μια ενιαία κάρτα με τη χρησιμοποίηση της έξυπνης κάρτας πολυεφαρμογής, η οποία είναι γνωστή ως ηλεκτρονικό πορτοφόλι. Η έξυπνη κάρτα γίνεται όλο και περισσότερο σημαντική και θα διαδραματίσει έναν σημαντικό ρόλο στην καθημερινή ζωή μας. Θα χρησιμοποιηθεί για να φέρει πολλά ευαίσθητα και κρίσιμα δεδομένα για τους κατα-

ναλωτές, περισσότερο από πριν, σε σύγκριση με τη μαγνητική κάρτα. Επομένως, υπάρχουν πολλές διαμάχες και συζητήσεις για το εάν οι έξυπνες κάρτες είναι ή όχι αρκετά ασφαλής, για να αποθηκεύσει εκείνες τις πληροφορίες. Αυτό είναι πάντα μια πηγή διαμάχης.

Υπάρχει ένα λειτουργικό σύστημα μέσα σε κάθε έξυπνη κάρτα που μπορεί να περιέχει έναν αριθμό αναγνώρισης κατασκευαστή (ID), ένα τύπο συστατικού(εξαρτήματος, σύνθεσης), μία σειρά αριθμών(serial number), πληροφορίες για το profile, κ.α. Ακόμη πιο σημαντική είναι η περιοχή του συστήματος που μπορεί να περιέχει διαφορετικά κλειδιά ασφάλειας, όπως το κλειδί κατασκευαστή ή το κλειδί επεξεργασίας (KF) και το κλειδί εξατομίκευσης(KP). Όλες αυτές οι πληροφορίες πρέπει να κρατηθούν μυστικές και να μην αποκαλυφθούν από άλλους.

Ως εκ τούτου, από τον κατασκευαστή στον προμηθευτή της εφαρμογής, και έπειτα στον κάτοχο της κάρτας, η παραγωγή μιας έξυπνης κάρτας διαιρείται σε διαφορετικές φάσεις. Ο περιορισμός στη μεταφορά και την πρόσβαση των στοιχείων είναι αυξητικός στις διαφορετικές φάσεις, προκειμένου να προστατευθούν οι διαφορετικές περιοχές στην έξυπνη κάρτα. Υπάρχουν πέντε κύριες φάσεις για έναν τυπικό κύκλο ζωής έξυπνων καρτών. Θα συζητήσουμε κάθε ένα πιο κάτω.

I. *Φάση επεξεργασίας*

Αυτή η φάση πραγματοποιείται από τους κατασκευαστές των τσιπ. Τα τσιπ πυριτίου ολοκληρωμένων κυκλωμάτων δημιουργούνται και εξετάζονται σε αυτήν την φάση. Ένα κλειδί επεξεργασίας(KF) προστίθεται για να προστατεύσει το τσιπ από την ψευδή τροποποίηση, έως ότου συναρμολογηθεί στην υποστήριξη της πλαστικής κάρτας. Το KF κάθε τσιπ είναι μοναδικό και προέρχεται από ένα κύριο κλειδί κατασκευαστών. Άλλα δεδομένα επεξεργασίας θα γραφτούν στο τσιπ κυκλωμάτων στο τέλος αυτής της φάσης. Κατόπιν το τσιπ είναι έτοιμο να παραδοθεί στον κατασκευαστή καρτών με την προστασία του κλειδιού KF.

II. Φάση προ-εξατομίκευσης

Αυτή η φάση πραγματοποιείται από τους προμηθευτές καρτών. Σε αυτήν την φάση, το τσιπ θα τοποθετηθεί στην πλαστική κάρτα που μπορεί να έχει το λογότυπο του προμηθευτή εφαρμογής τυπωμένο σε αυτό. Η σύνδεση μεταξύ του τσιπ και του τυπωμένου κυκλώματος θα γίνει και ολόκληρη η μονάδα μπορεί να δοκιμαστεί. Για προστιθέμενη ασφάλεια και για να επιτραπεί η ασφαλή παράδοση της κάρτας στον εκδότη της κάρτας, το κλειδί επεξεργασίας θα αντικατασταθεί από ένα κλειδί εξατομίκευσης(KP). Μετά από αυτό, μια κλειδαριά εξατομίκευσης VPER θα γραφτεί για να αποτρέψει την περαιτέρω τροποποίηση της KP. Επιπλέον, οι οδηγίες για την πρόσβαση στη φυσική μνήμη θα τεθούν εκτός λειτουργίας. Η πρόσβαση της κάρτας μπορεί να γίνει μόνο με τη χρησιμοποίηση της λογικής διευθυνσιοδότησης της μνήμης. Αυτό προστατεύει τις περιοχές συστήματος και επεξεργασίας που προσπελάζονται ή τροποποιούνται.

III. Φάση εξατομίκευσης

Αυτή η φάση διεξάγεται από τους εκδότες καρτών. Ολοκληρώνει τη δημιουργία των λογικών δομών δεδομένων. Το περιεχόμενο των αρχείων δεδομένων και των δεδομένων εφαρμογής γράφονται στην κάρτα. Οι πληροφορίες της ταυτότητας του κατόχου της κάρτας, PIN, και το ξεμπλοκάρισμα του PIN θα αποθηκευτούν, επίσης. Στο τέλος, μια κλειδαριά Vper χρησιμοποίησης θα καταγραφτεί για να δείξει ότι η κάρτα είναι στη φάση χρησιμοποίησης.

IV. Φάση χρησιμοποίησης

Αυτή είναι η φάση για την κανονική χρήση της κάρτας από τον κάτοχο. Το σύστημα εφαρμογής, οι έλεγχοι της λογικής πρόσβασης των αρχείων και άλλοι ενεργοποιούνται. Η πρόσβαση των πληροφοριών για την κάρτα θα περιοριστεί από τις πολιτικές ασφάλειας που τίθενται από την εφαρμογή. Αυτό θα συζητηθεί λεπτομερώς στο επόμενο τμήμα.

V. Η Φάση του τέλους ζωής (φάση ακύρωσης)

Υπάρχουν δύο τρόποι να κινηθεί η κάρτα σε αυτήν την φάση. Η μία αρχίζει από την εφαρμογή που γράφει την κλειδαριά ακύρωσης σε ένα μεμονωμένο αρχείο ή στο κύριο αρχείο. Όλες οι διαδικασίες, συμπεριλαμβανομένου του γραψίματος και της ενημέρωσης θα τεθούν εκτός λειτουργίας από το λειτουργικό σύστημα. Οι οδηγίες μόνο για ανάγνωση μπορούν να παραμείνουν ενεργές για λόγους ανάλυσης. Ο άλλος τρόπος να τεθεί η κάρτα σε αυτήν την φάση είναι αυτός, όταν το σύστημα ελέγχου εμποδίζει αμετάκλητα την πρόσβαση, επειδή και το PIN και η απελευθέρωση του PIN εμποδίζονται. Κατόπιν, όλες οι διαδικασίες θα μπλοκαριστούν συμπεριλαμβανομένου και της ανάγνωσης.

Τέλος, ο πίνακας 4 συνοψίζει τους όρους και τη πρόσβαση μνήμης μιας έξυπνης κάρτας κατά τη διάρκεια των διάφορων φάσεων που αναφέρονται ανωτέρω.

Περιοχές / φάσεις	Επεξεργασία	Προ-εξατομίκευση	Εξατομίκευση	Χρησιμοποίηση	Τέλος-ΖΩΗΣ
Τρόπος πρόσβασης	Φυσική εξέταση		Φυσική εξέταση		
Σύστημα	Μη προσβάσιμος				
Επεξεργασία (κλειδιά)	Γράψε KF	Γράψε KP	Μη προσβάσιμος		
Επεξεργασία (δεδομένα)	Διάβασε, γράψε, σβήσε	Διάβασε	Διάβασε		
Κατάλογος	Διάβασε, Γράψε, Σβήσε		Σύμφωνα με τις προϋποθέσεις της λογικής πρόσβασης των αρχείων		
Δεδομένα	Διάβασε, Γράψε, Σβήσε		Σύμφωνα με τις προϋποθέσεις της λογικής πρόσβασης των αρχείων		
Προαιρετικός κώδικας	Διάβασε, Γράψε, Σβήσε		Μη προσβάσιμος		

Πίνακας 4: Φάσεις και δικαιώματα πρόσβασης του κύκλου ζωής της Ε.Κ.

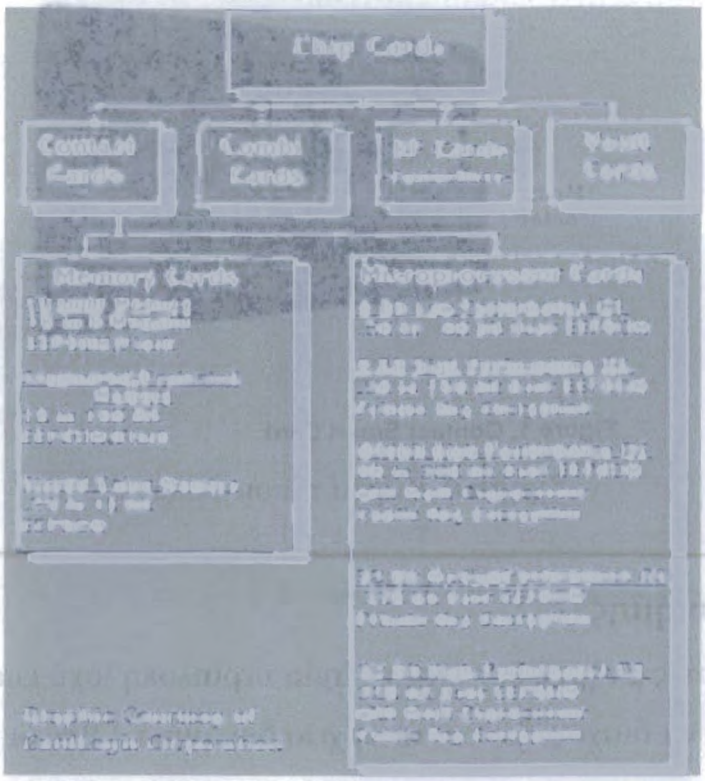
3. Βασικές αρχές και τύποι καρτών

Οι σημερινές έξυπνες κάρτες χρειάζονται την ηλεκτρική δύναμη συν έναν τρόπο για την μετάδοση των δεδομένων που διαβάζονται από το τσιπ. Οι κάρτες χρειάζονται ένα σήμα συγχρονισμού (το ρολόι), για να συγχρονίσουν τη μετάδοση των δεδομένων (έτσι ώστε η συσκευή αποστολής δεδομένων και ο δέκτης να τρέχουν με την ίδια ταχύτητα) ενώ πολλοί μικροεπεξεργαστές βασισμένοι στις κάρτες χρησιμοποιούν, επίσης, εκείνο το σήμα συγχρονισμού για να οδηγήσουν το μικροεπεξεργαστή. Επίσης, πολλές κάρτες (ιδιαίτερα κάρτες επαφής) έχουν μια γραμμή επανατοποθέτησης (ακριβώς όπως το κουμπί reset σε ένα PC, μόνο για να χρησιμοποιηθεί κάτω από ορισμένες ελεγχόμενες περιστάσεις, εάν το πρόβλημα πρόκειται να αποφευχθεί).

Ένα τσιπ έξυπνων καρτών επικοινωνεί με έναν αναγνώστη με άμεση φυσική επαφή ή με το σήμα μιας ραδιοσυχνότητας (RF), ανάλογα με το σχέδιο του συστήματος. Τρία σχέδια έξυπνων καρτών για τις επικοινωνίες μεταξύ του τσιπ και των αναγνωστών είναι:

- Οι κάρτες επαφής(contact)
- Οι ανέπαφες κάρτες(contactless)
- Υβριδικές ή κάρτες διπλής διεπαφής
- Κάρτες Combi

Ο τύπος των έξυπνων καρτών καθορίζεται σύμφωνα με τον τύπο τσιπ που εμφυτεύεται σ' αυτές και τις δυνατότητες κάλυψης του. Υπάρχει μια ευρεία σειρά επιλογών για να γίνει η επιλογή κατά το σχεδιασμό του συστήματος.



Σχήμα 5: Τύποι καρτών με ενσωματωμένο τσιπ

- ***Έξυπνες κάρτες επαφής (contact)***

Παραδοσιακά, για τη χρήση στη λιανική πώληση ή στο τραπεζικό περιβάλλον ή ως κάρτα GSM SIM στο κινητό τηλέφωνο, η κάρτα έχει επικαλυμμένες τις ηλεκτρικές επαφές που ενσωματώνονται στην επιφάνεια του πλαστικού, στη μια πλευρά. Αυτή η τεχνολογία επαφής των καρτών χρησιμοποιείται με την παρεμβολή της κάρτας (στο σωστό προσανατολισμό) στη σχισμή μίας συσκευής ανάγνωσης καρτών, η οποία έχει τις ηλεκτρικές επαφές που συνδέονται με τις επαφές στην όψη της κάρτας.

Οι έξυπνες κάρτες contact είναι το δημοφιλέστερο σχέδιο διασύνδεσης καρτών και χρησιμοποιούνται για τα δυο τους στοιχεία: το μέγεθος των καρτών και το τσιπ. Το σχήμα 6 απεικονίζει μια κάρτα τύπου contact.

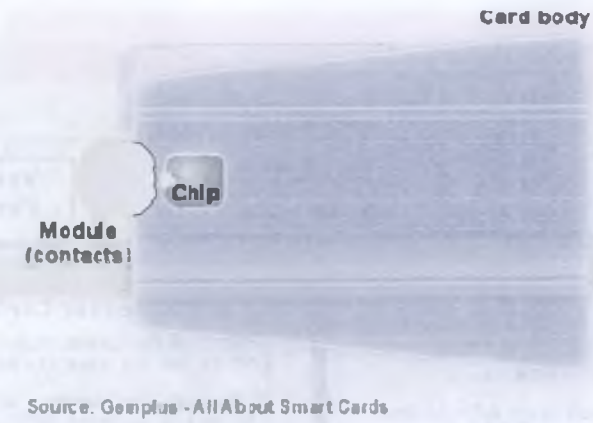


Figure 1. Contact Smart Card

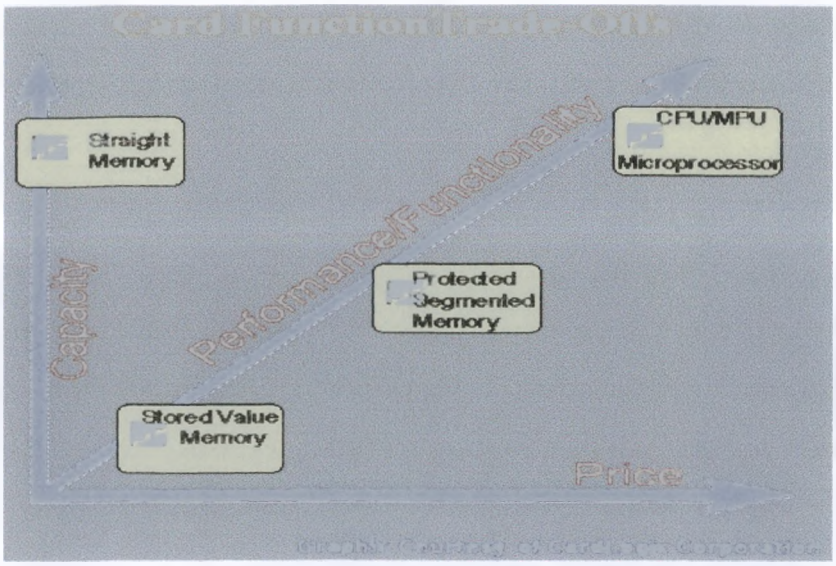
Σχήμα 6: Κάρτα τύπου Contact

4. Κάρτες μνήμης

Οι κάρτες μνήμης δεν έχουν καμία περίπλοκη ισχύ επεξεργασίας και δεν μπορούν να διαχειρίζονται τα αρχεία δυναμικά. Όλες οι μνήμες επικοινωνούν με τους αναγνώστες μέσω σύγχρονων πρωτοκόλλων. Το πυρίτιο σε αυτές τις κάρτες αποτελείται από τη μνήμη με μερική λογική ασφάλεια, που αποτρέπει την πρόσβαση εκτός αν το PIN ή ένας κωδικός πρόσβασης παρουσιαστεί. Οι περισσότερες τηλεφωνικές κάρτες είναι αυτού του τύπου.

Τα αυξημένα επίπεδα επεξεργασίας της ισχύος, της ευελιξίας και της μνήμης προσθέτουν κόστος. Οι ενιαίες λειτουργικές κάρτες είναι, συνήθως, η πιο οικονομική και αποδοτική λύση. Επιλέξτε το κατάλληλο τύπο έξυπνης κάρτας για την εφαρμογή σας αξιολογώντας το κόστος κατά τη λειτουργικότητα και καθορίζοντας το απαιτούμενο επίπεδο ασφάλειάς σας.

Το ακόλουθο διάγραμμα επιδεικνύει τους γενικούς κανόνες .



Υπάρχουν τρεις βασικοί τύποι καρτών μνήμης:

4.1. Άμεσες κάρτες μνήμης

Αυτές οι κάρτες απλά καταχωρούν τα στοιχεία και δεν έχουν καμία δυνατότητα επεξεργασίας των στοιχείων. Αυτές οι κάρτες αποτελούν το χαμηλότερο κόστος ανά δυαδικό ψηφίο για τη μνήμη του χρήστη. Θα πρέπει να θεωρηθούν ως δισκέτες μεταβλητού μεγέθους χωρίς το μηχανισμό κλειδώματος. Αυτές οι κάρτες δεν μπορούν να προσδιορίσουν το είδος τους στον αναγνώστη, ώστε να ξέρει το κεντρικό σύστημα ποιος τύπος κάρτας εισάγεται σε έναν αναγνώστη.

4.2. Προστατευμένες/ τμηματικές κάρτες μνήμης

Αυτές οι κάρτες έχουν την ενσωματωμένη λογική για να ελέγχουν την πρόσβαση στη μνήμη της κάρτας. Μερικές φορές αναφέρονται σαν ευφυής κάρτες μνήμης αυτές οι συσκευές που μπορούν να τεθούν σε προστασία εγγραφής κάποιων στοιχείων ή όλου του πίνακα μνήμης.

Μερικές από αυτές τις κάρτες μπορούν να διαμορφωθούν για να περιορίσουν την πρόσβαση της ανάγνωσης και της εγγραφής. Αυτό, συνήθως, γίνεται μέσω ενός κωδικού πρόσβασης ή ενός κλειδιού του συστήματος. Οι

τμηματικές κάρτες μνήμης μπορούν να διαιρεθούν σε λογικά τμήματα για να προγραμματιστούν για πολύ-λειτουργικότητα.

4.3. Αποθηκευτική αξία των καρτών μνήμης.

Αυτές οι κάρτες έχουν σχεδιαστεί για το συγκεκριμένο σκοπό της αποθήκευσης της αξίας ή των σημείων. Οι κάρτες είναι είτε μίας χρήσης είτε επαναχρησιμοποιήσιμες (πολλών χρήσεων). Οι περισσότερες κάρτες αυτού του τύπου ενσωματώνουν μόνιμα μέτρα ασφάλειας κατά το στάδιο κατασκευής τους. Αυτά τα μέτρα μπορούν να περιλάβουν κώδικούς κλειδιών πρόσβασης και λογικούς κωδικούς πρόσβασης, που είναι αυστηρά κωδικοποιημένοι στο τσιπ από τον κατασκευαστή. Οι πίνακες μνήμης είναι εγκατεστημένοι σε αυτές τις συσκευές σαν ποσοστά μείωσης ή μετρητές.

Για απλές εφαρμογές όπως μια τηλεφωνική κάρτα, το τσιπ έχει 60 ή 12 κελιά μνήμης, ένα για κάθε τηλεφωνική μονάδα. Ένα κελί μνήμης καθαρίζεται κάθε φορά που χρησιμοποιείται μια τηλεφωνική μονάδα. Μόλις χρησιμοποιηθούν όλες οι μονάδες μνήμης, η κάρτα γίνεται άχρηστη και πετάγεται. Αυτή η διαδικασία μπορεί να αντιστραφεί στην περίπτωση των επαναχρησιμοποιήσιμων καρτών.

5. Κάρτες μικροεπεξεργαστών

Αυτές οι κάρτες είναι σε θέση να τρέξουν τους συμμετρικούς (κοινά κλειδιά μεταξύ του αποστολέα και του παραλήπτη) κρυπτογραφικούς αλγορίθμους, όπως ο DES και να επικυρώσει έτσι την επικοινωνία τους με οποιαδήποτε συσκευή που μοιράζεται τα ίδια κλειδιά.

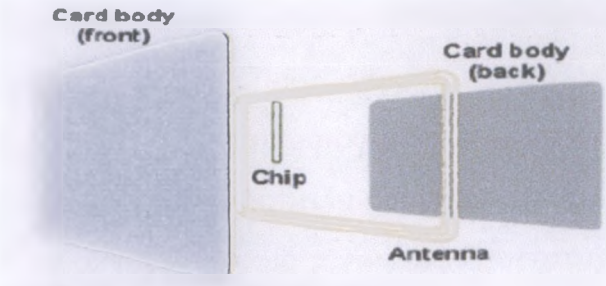
5.1. Κάρτες διπλών επεξεργαστών.

Αυτές οι κάρτες περιέχουν, επίσης, έναν μικροεπεξεργαστή στο πυρίτιό τους αλλά επιπρόσθετα περιλαμβάνουν έναν αφοσιωμένο συνεπεξεργαστή, ικανό να υλοποιήσει τους ασύμμετρους (δημόσιο κλειδί) αλγορίθμους και να παραχθούν έτσι οι ψηφιακές υπογραφές.

Η ασφάλεια και το κόστος πρέπει να είναι τα θεμελιώδη κριτήρια για την εξέταση των σχετικών αξιών των διαφορετικών τύπων προπληρωμένων καρτών, αλλά η επιλογή πρέπει να είναι κατάλληλη στην εφαρμογή. Η ασφάλεια, κατάλληλη για ένα εσωτερικό σχέδιο των καρτών μιας επιχείρησης, παραδείγματος χάριν, μπορεί να είναι πλήρως ακατάλληλη για ένα εθνικό ή διεθνές σχέδιο, όπου οι προμηθευτές υπηρεσίας μπορούν να απαιτήσουν προστασία του ενός από τον άλλο. Οι κάτοχοι κάρτας απαιτούν προστασία των προσωπικών τους δεδομένων. Η δαπάνη για τις κάρτες δεν πρέπει ποτέ να είναι μεμονωμένη, δεδομένου ότι το γενικό κόστος του συστήματος μπορεί να μειωθεί από την επιλογή μιας ακριβότερης (υψηλής λειτουργίας) κάρτας.

- **Οι ανέπαφες έξυπνες κάρτες(contactless)**

Οι ανέπαφες έξυπνες κάρτες, όπως φαίνεται στο σχήμα, χρησιμοποιούν μια κεραία με εμβέλεια περίπου 10 cm για να επικοινωνήσουν με τον αναγνώστη. Αυτές οι συσκευές μνήμης (τσιπ) μεγέθους μιας πιστωτικής κάρτας αντλούν την ισχύ τους από ένα πεδίο RF που παράγεται από τον αναγνώστη καρτών. Το πεδίο RF μεταφέρει, επίσης, τις πληροφορίες από και προς την κάρτα και τον αναγνώστη καρτών. Τα διακριτικά εμβλήματα αναγνώρισης των υπαλλήλων που εκδίδονται από μεγάλες επιχειρήσεις για την οικοδόμηση της πρόσβασης τους είναι χαρακτηριστικά ανέπαφων έξυπνων καρτών (contactless).



Source: Gemplus - All About Smart Cards

Figure 3. Contactless Smart Card

Σχήμα 7: Κάρτες τύπου Contactless

Η τεχνολογία αυτή θεωρείται η πιο συνηθισμένη, ειδικά στην Αμερική, όπου αρχικά χρησιμοποιήθηκε για έλεγχο ασφαλούς πρόσβασης σε κτίρια. Ο τύπος αυτός ενεργοποιείται κατά την τοποθέτηση της κάρτας σε κατάλληλο ηλεκτρομαγνητικό πεδίο, όπου κατόπιν η κάρτα μεταβιβάζει την περιεχόμενη πληροφορία. Η ικανότητα ενεργοποίησης της κάρτας χωρίς επαφή με τη διάταξη ανάγνωσης, καθιστά τον τύπο αυτό ανώτερο σε σύγκριση με την αρχιτεκτονική contact, όταν απαιτείται επάρκεια και αυθεντικοποίηση. Επιπρόσθετα της αυθεντικοποίησης, οι κάρτες αυτές έχουν τη δυνατότητα και άλλων μορφών δεδομένων (όπως ηλεκτρονικού χρήματος) καθιστώντας τη χρήσιμη σε εφαρμογές εισιτηρίων και μέσων μεταφοράς.

Οι κάρτες contactless με τη σειρά τους χωρίζονται σε δυο υποκατηγορίες: τις ενεργές (active) και ης παθητικές κάρτες (passive cards). Οι πρώτες χρησιμοποιούν μπαταρία συνήθως λιθίου, προκειμένου να παρέχουν την απαραίτητη ενέργεια στο σύστημα. Το πλεονέκτημα της παραπάνω χρήσης εστιάζεται στην απουσία επιρροής εξωτερικών πηγών, εφόσον το σύστημα αυτοεξυπηρετείται. Από την άλλη μεριά. όμως, παρουσιάζουν τα εξής μειονεκτήματα: πιθανότητα διαρροής ρεύματος και υψηλό κόστος.

Οι κάρτες passive παράγουν την απαραίτητη ενέργεια, μετατρέποντας την αποστολή ραδιοκυμάτων σε ηλεκτρική ενέργεια. Μάλιστα, συνήθως χρησιμοποιούνται δυο συχνότητες εκπομπής, μία για την παροχή ενέργειας και η άλλη για την αποστολή δεδομένων.

Η απουσία επιφανειακών επαφών και η επικοινωνία μέσω ραδιοσυχνοτήτων καθιστά εύκολη τη χρήση των καρτών αυτών. Το μέγεθος τους είναι λίγο μεγαλύτερο από μία τυπική κάρτα, ενώ η ανάγνωση της πληροφορίας που περιέχουν-ανάλογα με τον τύπο- είναι δυνατή ακόμα και από απόσταση από την απαραίτητη ηλεκτρονική διάταξη. Γι' αυτό και χρησιμοποιούνται ευρύτατα σε εφαρμογές διοδίων, συγκοινωνιών και μέσων μεταφοράς.

Για τη χρήση σε ένα περιβάλλον μαζικής διέλευσης , ή όταν ο κάτοχος της κάρτας βρίσκεται σε κίνηση τη στιγμή της συναλλαγής, η τεχνολογία των ραδιοσυχνοτήτων χρησιμοποιείται για να μεταδώσει την ισχύ από τη

συσκευή ανάγνωσης στην κάρτα ενώ τα δεδομένα μεταδίδονται ομοίως από το κενό αέρος μέχρι 10cms. Αυτή η ανέπαφη τεχνολογία καρτών χρησιμοποιεί μια εναέρια σπείρα που τοποθετείται σε στρώματα στην κάρτα και επιτρέπει την επικοινωνία ακόμη και αν η κάρτα διατηρείται μέσα σε ένα πορτοφόλι ή μια τσάντα. Όταν λοιπόν δεν υπάρχει καμία ηλεκτρική επαφή μιλάμε για ανέπαφη τεχνολογία.

Υβριδικές ή κάρτες διπλής διεπαφής

Ο συνδυασμός έξυπνων καρτών πολλαπλού σκοπού είναι ένα υβριδικό μίγμα σχεδίων επαφών(contact) και ανέπαφων (contactless). Περιλαμβάνουν την επαφή οκτώ pin για την επικοινωνία με έναν αναγνώστη τύπου επαφής(contact) και περιλαμβάνουν επίσης μια κεραία για την επικοινωνία με έναν αναγνώστη τύπου Ραδιοσυχνότητας(RF).

Κάρτες Combi

Ομοίως, ο τύπος combi μοιάζει στην κατηγορία hybrid , με τη διαφορά ότι οι δυο διεπαφές περιέχονται στο ίδιο chip. Πλεονέκτημα και των δυο τεχνολογιών είναι η ευελιξία που παρέχουν στο χρήστη ανάλογα με την εφαρμογή.

Κάρτες τύπου Java

Τέλος, μία ακόμη τεχνολογία καρτών, η οποία δεν είναι τόσο διαδεδομένη, αλλά είναι υπό συνεχή ανάπτυξη, είναι οι κάρτες τύπου Java. Η δυναμικότητα και η ευελιξία της τεχνολογίας Java επιτρέπουν στο χρήστη να εκμεταλλευτεί μία πληθώρα εφαρμογών(Java applets), εξασφαλίζοντας συγχρόνως μεγαλύτερη ασφάλεια και ικανότητα αποθήκευσης δεδομένων (περισσότερο από 4 MB δεδομένων). Επιπλέον, διατηρούνται όλα τα στοιχεία της τεχνολογίας Java, όπως προγραμματισ-τικότητα, δυνατότητα επαναχρησιμοποίησης, πολυλειτουργικότητα και ικανότητα εύκολης μεταφοράς δεδομένων. Η τεχνολογία, όμως αυτή των καρτών έχει ένα ακόμα πλεονέκτημα, καθώς χρησιμοποιούνται στοιχεία, όπως για παράδειγμα το κλειδί (key), δηλαδή ένας μεγάλος αριθμός που χρησιμοποιείται για απόκρυψη

μηνυμάτων, με αποτέλεσμα τη διασφάλιση της αποστολής των δεδομένων μέσω δικτύων (data integrity).

Η αποστολή των δεδομένων στις παραπάνω κάρτες γίνεται ως εξής: Κάθε είδους επικοινωνίας από και προς την έξυπνη κάρτα εκτελείται μέσω της επαφής C7. Έτσι, είναι μονόδρομη η επικοινωνία κάθε φορά, είτε από την κάρτα προς το τερματικό είτε αντίστροφα (λειτουργία half-duplex) Η επικοινωνία αρχικοποιείται από το τερματικό, το οποίο κάνει αίτηση για σχέση πελάτη- διακομιστή μέσω κάρτας-τερματικού.

Αφού η κάρτα έχει εισαχθεί στη συσκευή ανάγνωσης, πραγματοποιείται επανέναρξη των ρυθμίσεων (reset) και αποστέλλεται η σχετική απάντηση επανέναρξης (Answer to Reset) από την κάρτα. Κατά τη διεργασία επανέναρξης, κάποιο μέρος των παραμέτρων απενεργοποιείται και μετά το τερματικό στέλνει κάποιες βασικές οδηγίες προς την κάρτα, η οποία με τη σειρά της παράγει κατάλληλη απάντηση προς το τερματικό. Η διαδικασία αυτή συνεχίζεται έως ότου η κάρτα απομακρυνθεί από τη συσκευή (τέλος χρήσης), οπότε τερματίζεται και η σχέση πελάτη-διακομιστή .

Η ανέπαφη και διπλής διεπαφής αρχιτεκτονική καρτών έχει πολλά πλεονεκτήματα, αλλά είναι πολλά τα χρόνια που θα χρειαστούν οι κύριες και παραδοσιακές- βασισμένες στα σχέδια της τεχνολογίας της επαφής – κάρτες να μεταναστεύσουν σε αυτή τη τεχνολογία.

6. Οι παραλλαγές των έξυπνων καρτών

Οι έξυπνες κάρτες αποτελούνται από ένα ολοκληρωμένο κύκλωμα, μια διεπαφή μεταξύ του ολοκληρωμένου κυκλώματος και του αναγνώστη καρτών, και ενός σώματος. Οι έξυπνες κάρτες διαφοροποιούνται από τον τύπο του ολοκληρωμένου κυκλώματος, το μέγεθος, και τη μέθοδο επικοινωνίας τους με τον αναγνώστη.

Ολοκληρωμένα Κυκλώματα

Τα ενσωματωμένα κυκλώματα των έξυπνων καρτών παρέχουν τη λογική για τις συγκεκριμένες εφαρμογές καρτών. Τα ενσωματωμένα κυκλώματα ICs είναι τσιπ μνήμης ή τσιπ μικροεπεξεργαστών.

Τα τσιπ μνήμης

Τα τσιπ μνήμης των έξυπνων καρτών χρησιμοποιούνται για την αποθήκευση των δεδομένων και την αναγνώριση-προσδιορισμό των εφαρμογών. Τα δεδομένα μπορούν να αποτελούνται από οποιεσδήποτε πληροφορίες που απαιτούνται, για τη διαβίβαση τους σε μια συγκεκριμένη εφαρμογή. Η κύρια χρήση της μνήμης των έξυπνων καρτών είναι να αποθηκεύουν τα κλειδιά και τα πιστοποιητικά για το σύστημα της κρυπτογραφίας. Η λειτουργία των κλειδιών όπως και των κωδικών πρόσβασης είναι η εξασφάλιση του περιβάλλοντος και των πιστοποιητικών που ελέγχουν την αυθεντικότητα των κλειδιών. Η μνήμη των έξυπνων καρτών χτίζεται με βάση τη διαγράψιμη μνήμη που προγραμματίζεται μόνο να διαβάζει(EPROM) ή με ένα ηλεκτρικό τσιπ EPROM (EEPROM). Το EPROM, το οποίο μπορεί μόνο να αλλαχτεί μόνο μια φορά, χρησιμοποιείται συχνά στις υπηρεσίες προπληρωμένων καρτών όπως το τηλέφωνο που καλεί τις κάρτες για να μετρήσουν μέχρι το όριο των λεπτών που χρησιμοποιούνται και έπειτα να απορριφθούν. Το EEPROM, που μπορεί να αλλαχτεί μέχρι και 100.000 φορές, περιλαμβάνει ενσωματωμένη λογική που μπορεί να χρησιμοποιηθεί για να ενημερώσει έναν μετρητή στην υπηρεσία προπληρωμένων καρτών. Η αρχιτεκτονική της μνήμης ενός τσιπ (συνεπώς ,το κόστος) ποικίλλει, ανάλογα με την εφαρμογή. Εντούτοις, η ταυτότητα των κατασκευαστών(ID) και τα πεδία της ταυτότητας της εφαρμογής στην αρχιτεκτονική είναι τα ίδια για όλα τα τσιπ καρτών μνήμης. Ο αναγνώστης των έξυπνων καρτών χρησιμοποιεί αυτά τα πεδία για να επικοινωνήσει με την κάρτα. Η ταυτότητα της εφαρμογής περιλαμβάνει:

- τον εκδότη των καρτών
- τον αριθμό σειράς των καρτών

- άλλες πληροφορίες για το χρήστη(ανάλογα με την εφαρμογή των καρτών) .

Ο σειριακός αριθμός (serial number) είναι μοναδικός για κάθε κάρτα. Τα επιλεγμένα πεδία που βρίσκονται στη μνήμη του τσιπ περιλαμβάνουν τα δεδομένα του μετρητή και μυστικούς κωδικούς ή κλειδιά. Οι υπεύθυνοι ανάπτυξης των εφαρμογών έχουν τις επιλογές, για διάφορες δομές της μνήμης των καρτών για να ανταποκριθούν στις απαιτήσεις του σχεδιασμού.

Τα τσιπ του μικροεπεξεργαστή

Τα τσιπ του μικροεπεξεργαστή των έξυπνων καρτών είναι μικρότερα, πιο αργής έκδοσης από τις κεντρικές μονάδες επεξεργασίας (CPUs) που χρησιμοποιούνται στα PCs.

Η δυνατότητα προγραμματισμού τους παρέχεται για πολλές χρήσεις. Μπορούν ακόμα να συνδυαστούν σε μια ενιαία κάρτα διαφορετικές εφαρμογές. Οι έξυπνες κάρτες μικροεπεξεργαστών απαιτούνται για εφαρμογές που χειρίζονται ή συγκρίνουν δεδομένα, όπως η κρυπτογράφηση δεδομένων με την υποδομή του δημόσιου κλειδιού (PKI), τα applets της Java, και τα ηλεκτρονικά πορτοφόλια. Κάθε έξυπνη κάρτα μικροεπεξεργαστών έχει ένα OS στο τσιπ για να διευθύνει τις εσωτερικές λειτουργίες της εφαρμογής. Το OS φορτώνει με τη μνήμη μόνο ανάγνωσης(ROM), σαν ένα βασικό σύστημα εισόδου/ εξόδου (BIOS) σε ένα σύγχρονο PC. Η αρχική λειτουργία της κάρτας OS είναι ότι καθιστά δυνατή τη πρόσβαση στη μνήμη. Το OS διαχειρίζεται επίσης τις λειτουργίες ασφάλειας που εκτελούν χαρακτηριστικά αυτές οι κάρτες. Μια κάρτα μικροεπεξεργαστών, που χρησιμοποιεί ένα OS, έχει μια προκαθορισμένη συμπεριφορά που επιτρέπει στην κάρτα και την εφαρμογή να επικοινωνεί χρησιμοποιώντας προκαθορισμένες εντολές. Οι μικροεπεξεργαστές έξυπνων καρτών χρησιμοποιούν είτε ανοικτά OS είτε προγράμματα παρόμοια με τα OS. Οι εφαρμογές ανοικτών- OS είναι ευκολότερες για την εγγραφή επειδή οι υπεύθυνοι ανάπτυξης του λογισμικού χρησιμοποιούν διεπαφές προγραμματισμού που ήδη αυτοί γνωρίζουν. Ο κώδικας ανάπτυ-

ξης είναι ίδιος με το κώδικα που χρησιμοποιείται για να γραφτεί ένα πρόγραμμα για μια μηχανή Intel ή ένα PowerPC.

ΚΕΦΑΛΑΙΟ 4ο

ΛΟΓΙΣΜΙΚΟ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ

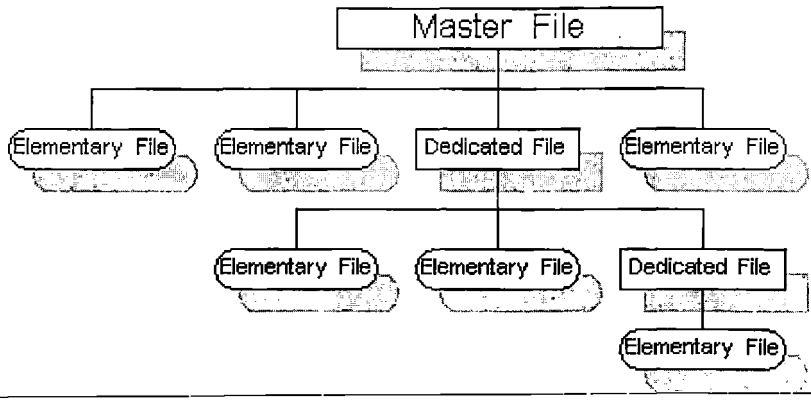
1. Λογική δομή και έλεγχοι πρόσβασης

Αφότου διανέμεται μια έξυπνη κάρτα στον καταναλωτή από τον προμηθευτή εφαρμογής, η προστασία της κάρτας θα ελεγχθεί κυρίως από το λειτουργικό σύστημα της εφαρμογής. Ο φυσικός τρόπος εξέτασης της πρόσβασης στα δεδομένων δεν είναι πλέον διαθέσιμος. Η πρόσβαση στα δεδομένα πρέπει να γίνει μέσω της λογικής δομής των αρχείων στην κάρτα. Αυτό το τμήμα θα συζητήσει πώς το λειτουργικό σύστημα θα ολοκληρώσει την προστασία της ασφάλειας των δεδομένων που αποθηκεύονται στην κάρτα, με την εξέταση της λογικής δομής των αρχείων και των αντίστοιχων ελέγχων πρόσβασης μιας έξυπνης κάρτας.

Λογική δομή αρχείων

Γενικά, από την άποψη της αποθήκευσης στοιχείων, μια έξυπνη κάρτα μπορεί να αντιμετωπισθεί ως δίσκος όπου τα αρχεία οργανώνονται σε μια ιεραρχική μορφή μέσω των καταλόγων. Παρόμοιος με το MS-DOS, υπάρχει ένα κύριο αρχείο (MF) που είναι όπως ο root directory. Κάτω από τη ρίζα, μπορούμε να έχουμε διαφορετικά αρχεία που καλούνται στοιχειώδη αρχεία (EFs). Μπορούμε επίσης να έχουμε τα διάφορους υποκαταλόγους που καλούνται αφοσιωμένα(dedicated) αρχεία (DFs). Κάτω από κάθε υποκατάλογο θα είναι τα στοιχειώδη αρχεία πάλι. Η κύρια διαφορά μιας δομής αρχείων των έξυπνων καρτών και μιας δομής αρχείων MS-DOS είναι ότι τα

αφιερωμένα αρχεία μπορούν επίσης να περιέχουν δεδομένα. Το σχήμα 8 παρουσιάζει τη λογική άποψη μιας δομής αρχείων των έξυπνων καρτών.



Σχήμα 8: Λογική Δομή Αρχείων μίας έξυπνης κάρτας

Στη τεχνολογία των έξυπνων καρτών, η ρίζα ή το κύριο αρχείο (MF), εκτός από το μέρος της επικεφαλίδας αποτελείται από τις επικεφαλίδες όλων των dedicated αρχείων και των στοιχειωδών αρχείων που περιέχουν το MF στη γονική ιεραρχία τους. Το dedicated αρχείο (DF) είναι μια λειτουργική ομαδοποίηση των αρχείων που αποτελούνται από τον εαυτό τους και όλα τα αρχεία που είναι άμεσα παιδιά του DF. Το στοιχειώδες αρχείο (EF) αποτελείται απλά από την επικεφαλίδα του και το σώμα που αποθηκεύει τα δεδομένα.

Οι τρόποι με τους οποίους τα δεδομένα διαχειρίζονται μέσα σε ένα αρχείο διαφέρουν και εξαρτώνται από τα διαφορετικά λειτουργικά συστήματα. Μερικά από αυτά μπορούν να διαχειριστούν τα δεδομένα απλά από την εξισορρόπηση και το μήκος, ενώ άλλα μπορούν να οργανώσουν τα δεδομένα στα σταθερά ή μεταβλητά μήκη των εγγραφών όπως το παγκόσμιο σύστημα για την κινητή επικοινωνία (GSM). Σε οποιαδήποτε περίπτωση, το αρχείο πρέπει να επιλεχτεί πριν εκτελεστεί οποιαδήποτε διαδικασία. Αυτό είναι ισοδύναμο με το άνοιγμα ενός αρχείου.

Έλεγχοι πρόσβασης

Οι λογικοί μηχανισμοί πρόσβασης και επιλογής ενεργοποιούνται αφότου παρέχεται η δύναμη στην κάρτα ενώ το κύριο αρχείο επιλέγεται αυτόματα. Η λειτουργία επιλογής επιτρέπει τη μετακίνηση γύρω από το δέντρο. Μπορεί να κατέρχεται με την επιλογή ενός EF ή DF, ή μπορεί να ανέρχεται με την επιλογή ενός MF ή DF. Η οριζόντια μετακίνηση μπορεί να γίνει με την επιλογή ενός EF από ένα άλλο EF, επίσης.

Μετά από την επιτυχία της επιλογής, η επικεφαλίδα του αρχείου μπορεί να ανακτηθεί και η οποία αποθηκεύει τις πληροφορίες για το αρχείο όπως ο αριθμός αναγνώρισης, η περιγραφή, οι τύποι, το μέγεθος, και τα λοιπά. Ιδιαίτερα, αποθηκεύει τις ιδιότητες του αρχείου που δηλώνει τους όρους πρόσβασης και την παρούσα κατάσταση. Η πρόσβαση των στοιχείων στο αρχείο εξαρτάται από το εάν εκείνοι οι όροι μπορούν να τηρηθούν ή όχι. Αυτό θα περιγραφεί στο ακόλουθο τμήμα.

Εν ολίγοις, η δομή αρχείων του λειτουργικού συστήματος των έξυπνων καρτών είναι παρόμοια με άλλα κοινά λειτουργικά συστήματα όπως το MS-DOS και το Unix. Εντούτοις, προκειμένου να παρασχεθεί ο μεγαλύτερος έλεγχος ασφάλειας, η ιδιότητα κάθε αρχείου ενισχύεται με την προσθήκη των όρων πρόσβασης και της θέσης αρχείων στην επικεφαλίδα του αρχείου. Επιπλέον, το κλείδωμα των αρχείων παρέχεται για να αποτρέψει την πρόσβαση στο αρχείο. Αυτοί οι μηχανισμοί και οι αλγόριθμοι ασφάλειας παρέχουν μια λογική προστασία της έξυπνης κάρτας.

2. Λειτουργικό σύστημα

Χαρακτηριστικά το λειτουργικό σύστημα του μικροεπεξεργαστή των έξυπνων καρτών μπορεί να χειρίζεται μόνο μερικές χιλιάδες bytes του κωδικοποιημένου προγράμματος. Το λειτουργικό σύστημα πρέπει να έχει ως στόχους :

- τη μετάδοση των δεδομένων μέσω της αμφίδρομης, τμηματικής τελικής διεπαφής
- τη φόρτωση, λειτουργία, και διαχείριση των εφαρμογών

- τον έλεγχος εκτέλεσης και την επεξεργασία των οδηγιών
- τη προστασία της πρόσβασης στα δεδομένα
- τη διαχείριση της μνήμης
- τη διαχείριση των αρχείων
- τη διαχείριση και εκτέλεση των κρυπτογραφικών αλγορίθμων

Σε αντίθεση με τα λειτουργικά συστήματα των προσωπικών υπολογιστών όπως το Unix, το DOS, και τα Windows, τα λειτουργικά συστήματα των έξυπνων καρτών δεν χαρακτηρίζουν τις διεπαφές με τον χρήστη ή τη δυνατότητα να έχουν πρόσβαση σε εξωτερικές περιφερειακές μονάδες ή στα μέσα απομνημόνευσης. Το μέγεθος τους είναι χαρακτηριστικά μεταξύ 3 και 24 Kbytes.

Επειδή ο χώρος της μνήμης των έξυπνων καρτών είναι αυστηρά περιορισμένος, δεν μπορούν να είναι γενικά εφαρμοσμένες σε όλες τις τυποποιημένες οδηγίες και τις δομές αρχείων, σε όλα τα λειτουργικά συστήματα των έξυπνων καρτών.

Υπάρχουν κυρίως δύο τύποι καρτών λειτουργικών συστημάτων. Ο ένας τύπος είναι η κάρτα OS που είναι η πιο οικονομικώς αποδοτική σε πολλές επιχειρήσεις, επειδή πληρώνετε μόνο για το μέγεθος και τις λειτουργίες που εσείς προσδιορίζετε. Αυτή η κλασική προσέγγιση μεταχειρίζεται τη κάθε κάρτα σαν μια ασφαλή συσκευή υπολογισμού και αποθήκευσης. Τα αρχεία και οι δικαιοδοσίες σε αυτά τα αρχεία είναι όλα τοποθετημένα από τον εκδότη εκ των προτέρων. Η μόνη πρόσβαση στις κάρτες θα είναι μέσω του λειτουργικού συστήματος. Τα δεδομένα διαβάζονται ή γράφονται στην κάρτα μέσω της δικαιοδοσίας που τίθεται μόνο από τους εκδότες. Το λειτουργικό σύστημα εκτελεί ένα σύνολο "εφαρμογών" όπως τη πιστοποίηση της ταυτότητας και τη κρυπτογράφηση, όπως ζητείται μέσω εντολών που στέλνονται στην κάρτα. Η CardLogix M.O.S.T. OS είναι ένα παράδειγμα αυτού του τύπου.

Η δεύτερη μεθοδολογία είναι η προσέγγιση του σκληρού δίσκου στα λειτουργικά συστήματα των καρτών. Η κάρτα είναι μια συσκευή υπολογισμού με έναν ενεργό διαχειριστή μνήμης που σας επιτρέπει να φορτώνεται

επάνω στη κάρτα συγκεκριμένες εφαρμογές και αρχεία. Το λειτουργικό σύστημα της κάρτας παρέχεται για την ενεργή κατανομή και διαχείριση των αρχείων. Έχει σχεδιαστεί για προγράμματα καρτών που έχουν μεγάλη αναμενόμενη διάρκεια ζωής του χρήστη (πάνω από 4 έτη). Η Java Card και η Microsoft Windows Card Os είναι παραδείγματα αυτής της προσέγγισης. Αυτές οι κάρτες έχουν πολύ μεγαλύτερο κίνδυνο, που οφείλεται στη ικανότητα τους να εισάγουν applets ή ιούς στην κάρτα.

Η έκδοση αυτών των καρτών αρχικά ήταν δαπανηρή, οφειλόμενη στην εκλέπτυνση του OS. Αυτές οι αρχιτεκτονικές καρτών χρειάζονται μεγαλύτερη μνήμη για τις μελλοντικές μη σχεδιασμένες βελτιώσεις και ένα πρόγραμμα μεγαλύτερης μνήμης για να φορτώνει τα applets. Επίσης, το κόστος υποδομής της ασφάλειας είναι πολύ πιο υψηλό για την διαχείριση οφειλόμενο στα πολλαπλά σημεία εισόδου στη λειτουργία του συστήματος των καρτών.

Τρία γενικά πρότυπα ανοικτών-OS καρτών περιλαμβάνουν:

- Microsoft-Windows® για τις έξυπνες κάρτες -χρησιμοποιούνται τα κοινά Microsoft Windows API
- Το Πολλαπλής εφαρμογής λειτουργικό σύστημα (MULTOS) -- που αναπτύχθηκε από την κοινοπραξία MAOSCO 1, για τις οικονομικές συναλλαγές με έμφαση στην ασφάλεια.
- Η τεχνολογία της Java στα Μικροσυστήματα Sun - παρέχεται για το φόρτωμα και το τρέξιμο των Java applets .

Τα προγράμματα που είναι παρόμοια με τα OS χρησιμοποιούν δικές τους λύσεις λογισμικού για τις συγκεκριμένες εφαρμογές που συνήθως αναπτύσσονται από τον κατασκευαστή των έξυπνων καρτών. Επειδή, ο υπεύθυνος ανάπτυξης πρέπει να μάθει έναν δικό του κώδικα, αρχικά το λογισμικό είναι δυσκολότερο να γραφθεί, αλλά μπορεί να παρέχει επιπλέον ασφάλεια από τους χάκερς .

Τα επαγγελματικά windows 2000 είναι η πρώτη εγγενή υποστήριξη των OS της Microsoft OS για τις έξυπνες κάρτες. Άλλα OSs απαιτούν πρό-

σθετη ενίσχυση οδηγών που παρέχεται από τον κατασκευαστή των συσκευών. Η εγγενής υποστήριξη των έξυπνων καρτών που παρέχεται από τα επαγγελματικά Windows 2000 περιλαμβάνει:

- οδηγούς αναγνωστών -υποστηρίζουν διάφορους αναγνώστες έξυπνων καρτών και απαιτούν μόνο ότι ο αναγνώστης θα συνδέεται με το σύστημα, το οποίο επιτρέπει σύνδεση στη πρίζα και εκτέλεση για την ανίχνευση και διαμόρφωση του αναγνώστη.
- PC/SC -- υποστηρίζει τη κάρτα PC/SC
- έτοιμη έξυπνη κάρτα -υποστηρίζει την άδεια εισόδου του PKI (Public Key Infrastructure-Υποδομή Δημοσίου Κλειδιού) στα δίκτυα.

Αν και τα επαγγελματικά Windows 2000 υποστηρίζουν τις έξυπνες κάρτες, που χρησιμοποιούνται για την άδεια εισόδου του PKI στο δίκτυο, ένας χρήστης χρειάζεται έναν πιστοποιημένο κεντρικό υπολογιστή και μια έξυπνη κάρτα, που διαμορφώνονται σύμφωνα με ένα πιστοποιητικό, προτού να μπορέσει να χρησιμοποιηθεί αυτή η λειτουργία. Ο πιστοποιημένος κεντρικός υπολογιστής ενεργεί όπως η αρχή πιστοποίησης, εκδίδοντας και επαληθεύοντας πιστοποιητικά που χρησιμοποιούνται στο δίκτυο. Αφού εγκατασταθεί και διαμορφωθεί το δίκτυο, ο χρήστης πρέπει να χρησιμοποιήσει την έξυπνη κάρτα για να εισαχθεί(log on) στο δίκτυο. Το Microsoft Outlook και ο Internet explorer παρέχουν, επίσης, υποστήριξη στις έξυπνες κάρτες. Οι έξυπνες κάρτες μπορούν να χρησιμοποιηθούν με το Outlook για να υπογράφουν ψηφιακά τα μηνύματα του ηλεκτρονικού ταχυδρομείου και για να στείλουν με ασφαλή μετάδοση το PKI. Μπορούν να χρησιμοποιηθούν με τον internet explorer για να ελέγχουν την πρόσβαση στα εξασφαλισμένα Web Sites .

3. Διακεκριμένες προδιαγραφές και πρότυπα έξυπνων καρτών

Η κοινή αρχιτεκτονική ασφάλειας δεδομένων(CDSA), αναπτύχθηκε από την Intel , για να παρέχει ένα ανοικτό, διαλειτουργικό, έκτατο και μια διασταυρωμένη πλατφόρμα πλαισίου λογισμικού που καθιστά τις πλατφόρμες των υπολογιστών ασφαλέστερες για όλες τις εφαρμογές συμπεριλαμβα-

νομένου του ηλεκτρονικού εμπορίου, τις επικοινωνίες, και το ψηφιακό περιεχόμενο. Οι προδιαγραφές του CDSA 2,0 υιοθετήθηκαν από την ανοικτή Ομάδα το Δεκέμβριο του 1997.

Τα ακόλουθα προκύπτουν σαν σημαντικά πρότυπα όσον αφορά την ένταξη των έξυπνων καρτών στον υπολογιστή και στις εφαρμογές ασφάλειας του δικτύου:

- ***PKCS#11: Πρότυπα Κρυπτογραφικών συμβολικών διεπαφών***

Αυτά τα πρότυπα καθορίζουν μια διεπαφή εφαρμογής προγραμματισμού (API)**, που καλείται Cryptoki, για συσκευές που κρατούν κρυπτογραφικές πληροφορίες και εκτελούν κρυπτογραφικές λειτουργίες. Η Cryptoki, αποφασισμένη ακολούθησε μια απλή προσέγγιση που βασιζόταν στο αντικείμενο με ένα κρυπτογραφικό κλειδί, εξετάζοντας τους στόχους της ανεξαρτησίας της τεχνολογίας (οποιοδήποτε είδος συσκευής) και τη διανομή των πόρων (πολλαπλές εφαρμογές που έχουν πρόσβαση σε πολλαπλές συσκευές). Τα πρότυπα δημιουργήθηκαν το 1994 από την RSA .

** *Το κρυπτογραφικό API της Microsoft (CryptoAPI)* παρέχει τις υπηρεσίες που επιτρέπουν στους υπεύθυνους ανάπτυξης εφαρμογών να προσθέσουν το σύστημα κρυπτογραφίας και το πιστοποιητικό που διαχειρίζεται τη λειτουργικότητα στις εφαρμογές Win32® . Οι εφαρμογές μπορούν να χρησιμοποιήσουν τις λειτουργίες μέσα στο CryptoAPI χωρίς να γνωρίζουν τίποτα για την βασική υλοποίηση, όπως γίνεται με μια εφαρμογή που μπορεί να χρησιμοποιήσει μια βιβλιοθήκη γραφικών χωρίς να γνωρίζει τίποτα για το ειδικό διαμορφωμένο υλικό γραφικών (graphics hardware).

- ***PC/SC***

Η ομάδα εργασίας του PC/Sc διαμορφώθηκε τον Μάιο του 1997. Δημιουργήθηκε για να αντιμετωπίσει τα κρίσιμα τεχνικά ζητήματα σχετικά με την ολοκλήρωση των έξυπνων καρτών με τα PC. Τα μέλη της ομάδας εργασίας PC/Sc συμπεριέλαβαν τα προσωπικά συστήματα συναλλαγής του Bull, τα Gemplus, τα Hewlett -Packard, την IBM, την MicrosoftCorp., τη Schlumberger, τα Siemens -Nixdorf Inc., τα Μικροσυστήματα Sun, τη Toshiba και την VeriFone. Η προδιαγραφή εξετάζει τους περιορισμούς στα

υπάρχοντα πρότυπα που περιπλέκουν την ολοκλήρωση των συσκευών ICC με το PC και αποτυγχάνουν να εξετάσουν επαρκώς τη διαλειτουργικότητα, από την πλευρά εφαρμογής των PC, μεταξύ των προϊόντων από πολλαπλούς προμηθευτές.

- ***OpenCard<Ανοικτή Κάρτα >***

Το OpenCard είναι ένα τυποποιημένο πλαίσιο που αναγγέλθηκε από τη διεθνή εταιρία μηχανών A.E. <International Business Machines Corporation, Inc>, τη Netscape, τη NCI, και τη Sun Microsystems Inc. Παρέχει λύσεις για τις διαλειτουργικές έξυπνες κάρτες πάνω σε πολλές πλατφόρμες υλικού και λογισμικού. Το πλαίσιο της OpenCard είναι ένα ανοικτό πρότυπο που παρέχει μια αρχιτεκτονική και ένα σύνολο από APIs που επιτρέπουν στους υπεύθυνους ανάπτυξης των εφαρμογών και στους φορείς παροχής υπηρεσιών να χτίσουν και να επεκτείνουν τις γνωστές λύσεις των έξυπνων καρτών σε οποιοδήποτε περιβάλλον που είναι συμμορφώσιμο με την Open Card. Αρχικά αναγγέλθηκε το 1997.

- ***JavaCard***

Η JavaCard API είναι μια προδιαγραφή που επιτρέπει την δυνατότητα εγγραφής μια φορά μόνο και τρέχει σε οποιοδήποτε περιβάλλον της Java, στις έξυπνες κάρτες και τις άλλες συσκευές, με περιορισμένη μνήμη. Η JavaCard API αναπτύχθηκε με τη συναίνεση των κύριων μελών της βιομηχανίας των έξυπνων καρτών και έχει υιοθετηθεί από περισσότερο από το 95% των κατασκευαστών της βιομηχανίας των έξυπνων καρτών, συμπεριλαμβανομένου του Bull/CP8 , του ημιαγωγού του Ντάλας, του De La Rue , του Geisecke & Devrient, του Gemplus, τις εσωτερικές τεχνολογίες, τη Motorola, τη Oberthur, τη Schlumberger, και τη Toshiba.

ΚΕΦΑΛΑΙΟ 5ο

ΑΝΑΓΝΩΣΤΕΣ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ

1. Εισαγωγικά στοιχεία

Συνήθως αναφερόμενοι στους "αναγνώστες έξυπνων καρτών", εννοούμε ότι όλα τα τερματικά των έξυπνων καρτών έχουν τη δυνατότητα, εξορισμού, να διαβάσουν και να γράψουν, εφ' όσον τους υποστηρίζει η έξυπνη κάρτα και οι κατάλληλοι όροι πρόσβασης έχουν τηρηθεί. Σε αντίθεση με τις έξυπνες κάρτες, οι οποίες έχουν όλες τους παρόμοια κατασκευή, οι αναγνώστες των έξυπνων καρτών έχουν παράγοντες ποικιλόμορφους με τα διάφορα επίπεδα μηχανικής και λογικής εκλέπτυνσης. Μερικά παραδείγματα περιλαμβάνουν: τον αναγνώστη που ενσωματώνεται σε μια μηχανή πώλησης, το φορητό αναγνώστη με τη λειτουργία συσσωρευτή με μια μικρή οθόνη LCD, τον αναγνώστη που ενσωματώνεται σε ένα κινητό τηλέφωνο GSM και τον αναγνώστη που συνδέεται με έναν προσωπικό υπολογιστή. Μηχανικά, οι αναγνώστες έχουν διάφορες επιλογές που συμπεριλαμβάνουν: το κατά πόσο ο χρήστης πρέπει να παρεμβάλει /αφαιρέσει την κάρτα του από τον αυτοματοποιημένο μηχανισμό εισαγωγής / εξαγωγής αποφεύγοντας, έτσι, τις διάφορες επαφές εναντίον των προσγειωμένων επαφών και των προβλέψεων για την είσοδο στην οθόνη και το πληκτρολόγιο. Ηλεκτρικά, ο αναγνώστης πρέπει να προσαρμοστεί με τα πρότυπα ISO /IEC 7816-3.

Οι επιλογές για τους αναγνώστες είναι πολυάριθμες. Πολλοί τύποι αναγνωστών είναι διαθέσιμοι άμεσα προς παραγγελία στη σημερινή αγορά και ο κάθε ένας έχει τα πλεονεκτήματα και τα μειονεκτήματά του.

2. Τεχνολογία Αναγνωστών έξυπνων καρτών

Οι αναγνώστες καρτών παρέχουν τη φυσική σύνδεση μεταξύ της έξυπνης κάρτας και του κεντρικού υπολογιστή(host). Το σχήμα 4 δείχνει ένα συνδυασμό πληκτρολογίου/ αναγνώστη καρτών. Ο κεντρικός υπολογιστής host μπορεί να είναι ένα PC ή μια αυτόνομη συσκευή. Ο αναγνώστης απελευθερώνει ισχύ, αρχικοποιεί την κάρτα, και ενεργεί ως μεσολαβητής μεταξύ της έξυπνης κάρτας και του κεντρικού υπολογιστή(host). Η ισχύς διανέμεται στην έξυπνη κάρτα μέσω μιας επαφής στην micromodule της επαφής των έξυπνων καρτών ή με την πρόκληση ρεύματος μέσω της κεραίας των ανέπαφων σχεδίων. Η αρχικοποίηση είναι ένα καθορισμένο πρωτόκολλο που πρέπει να εκτελούν όλες οι κάρτες. Όλοι οι αναγνώστες έξυπνων καρτών υποστηρίζουν την αρχικοποίηση οποιασδήποτε έξυπνης κάρτας, αλλά μπορούν να σταματήσουν να υποστηρίζουν την κάρτα με τη διακοπή του ηλεκτρικού ρεύματος.

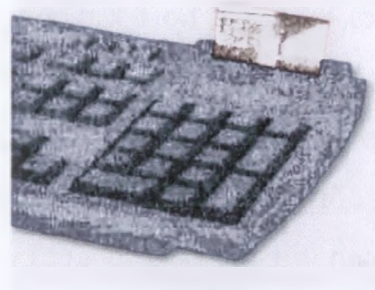


Figure 4. Smart-Card Reader

Σχήμα 9: Αναγνώστης έξυπνων καρτών

Ενημερότητα της κάρτας

Η όψη ενός αναγνώστη μιας έξυπνης κάρτας καλείται ενημερότητα κάρτας. Οι περισσότεροι αναγνώστες καρτών υποστηρίζουν και τις δύο επιλεγμένες όψεις:

- οι ενήμεροι αναγνώστες εμφανίζουν τη φυσική δομή καρτών και δρουν ως μεταφραστές μεταξύ του κεντρικού υπολογιστή (host) και της κάρτας. Οι κάρτες μνήμης απαιτούν την ενήμερη όψη, επειδή ο αναγνώστης πρέπει να ξέρει την ακριβή διεύθυνση για τα δεδομένα.
- Οι γενικοί αναγνώστες γνωρίζουν τη λογική δομή της κάρτας και περνούν τις εντολές από τον host κατ' ευθείαν στην κάρτα, χωρίς να αλλάζουν την εντολή. Οι κάρτες των μικροεπεξεργαστών χρησιμοποιούν τη γενική όψη, επειδή οι κάρτες έχουν δικό τους OS και λογική για να ερμηνεύουν τις εντολές.

3. Τύποι υλικού αναγνωστών

Οι συσκευές αναγνωστών έξυπνων καρτών είναι διαφανείς- ή αυτόνομοι – τύποι υλικού. Το υλικό διάφανου αναγνώστη, μερικές φορές απλά καλείτε αναγνώστης και απαιτεί έναν host για όλες τις ξεχωριστές λειτουργίες του, συμπεριλαμβανομένης και της αρχικοποίησης και της εφαρμογής. Αυτός ο τύπος υλικού δεν έχει καμία εσωτερική λογική, εκτός από έναν οδηγό γραμμών που ρυθμίζει το σήμα μεταξύ της κάρτας και του κεντρικού υπολογιστή host. Ένας διαφανής αναγνώστης είναι παρόμοιος με το modem ενός PC αφού ένας host καθοδηγεί τον αναγνώστη και την κάρτα. Αυτό απαιτεί περισσότερη υποστήριξη από το λογισμικό, το οποίο πρέπει να καταλάβει το ηλεκτρικό σχέδιο του αναγνώστη και πώς να επικοινωνεί με την κάρτα. Ο οδηγός πρέπει, επίσης, να έχει τη λογική για να υποστηρίξει την ενήμερη όψη για την επικοινωνία με τις κάρτες μνήμης.

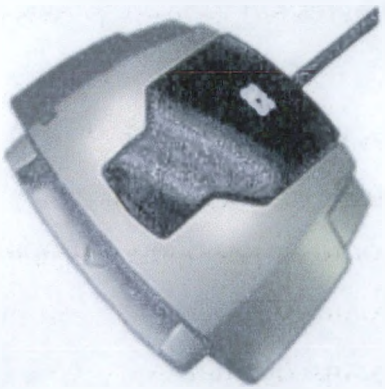
Το υλικό αυτόνομων αναγνωστών, που καλείτε μερικές φορές ως τερματικό, περιλαμβάνει όλη την λογική που απαιτείται για την αρχικοποίηση μιας κάρτας και για να ενεργήσει ως μεσολαβητής μεταξύ μιας κάρτας μνήμης και του host. Για παράδειγμα, ο host μπορεί να παραδώσει ένα μεγάλο πακέτο πληροφοριών στον αναγνώστη για να τις περάσει στην κάρτα μνήμης. Ο αναγνώστης πρέπει να ελέγξει το πακέτο και κάποιες φορές να το σπάσει σε δύο πακέτα, πριν στείλει τις πληροφορίες στην έξυπνη κάρτα.

Αυτό σημαίνει ότι ο host ενδιαφέρεται μόνο για την επικοινωνία στον αναγνώστη και όχι για την έξυπνη κάρτα.

Το OS καθορίζει όλες τις εντολές που καταλαβαίνει μια κάρτα μικροεπεξεργαστών, έτσι δεν είναι απαραίτητο να επέμβει ο αναγνώστης. Οι διαφανείς αναγνώστες απαιτούν περισσότερους οδηγούς απ' ότι ένας αυτόνομος εξοπλισμός, αλλά είναι φτηνότεροι για να κατασκευάσουν και ευκολότερο για να αλλάξουν. Οι αυτόνομοι αναγνώστες, αν και ακριβότεροι από τις διαφανείς συσκευές, έχουν γενικά σύνολα οδηγών που καθορίζουν την επικοινωνία μεταξύ ενός αναγνώστη και ενός κεντρικού υπολογιστή (host). Οι οδηγοί των καρτών μνήμης χτίζονται μέσα στη λογική, που καθιστά τη διαχείριση των οδηγών ευκολότερη, αλλά ο αναγνώστης μπορεί να θεωρηθεί ξεπερασμένος, εκτός και αν οι οδηγοί μπορούν να αναβαθμιστούν.

4. Υπάρχοντες αναγνώστες

- **ACR38U – Συσκευή ανάγνωσης έξυπνων καρτών**



Λεπτομερής περιγραφή:

Με τη συνεχόμενη εξέλιξη των προτύπων των προσωπικών υπολογιστών, ο αναγνώστης έξυπνων καρτών ACR38 είναι μία USB 2,0 πλήρης συσκευή ταχύτητας που σχεδιάζεται για χρήση σε περιβάλλον Η/Υ.

Η πιο πρόσφατη ενσάρκωση της σειράς αναγνωστών συνδυάζει ένα σύγχρονο σχέδιο με την πιο πρόσφατη τεχνολογία, και το καθιστά κατάλ-

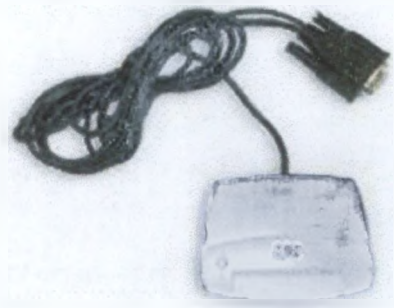
ληλη λύση για τις απαιτήσεις των περιβαλλόντων. Το ACR38 είναι ιδανικό για χρήση σε εφαρμογές στην ασφάλεια δικτύων και στα ηλεκτρονικά συστήματα πληρωμής καθώς επίσης και σε άλλες προηγμένες εφαρμογές έξυπνων καρτών.

Χαρακτηριστικά γνωρίσματα του αναγνώστη ACR38:

- USB 2,0 πλήρης ταχύτητα διεπαφής στον Η/Υ με απλή δομή εντολών
- Διαβάζει και γράφει σε όλες τις κάρτες μικροεπεξεργαστών .
- Υποστηρίζει κάρτες μνήμης SLE 4418/28/32/42
- Υποστηρίζει τις πιο κοινές, βασισμένες στη μνήμη, έξυπνες κάρτες, συμπεριλαμβανομένου των καρτών 12C πρωτοκόλλου και των καρτών ασφαλής μνήμης.
- Σύντομη προστασία κυκλωμάτων
- Πιστοποιητικά προσαρμογής: ISO 7816-1/2/3, PC/SC, CE, FCC, MICROSOFT WHQL, EMV Certificated
- ISO7816-1/2/3 συμβατή διεπαφή έξυπνων καρτών
- Υποστήριξη PPS (πρωτόκολλο και επιλογή παραμέτρων) με 1743 – 305200 BPS στις έξυπνες κάρτες ανάγνωσης και γραψίματος
- RAM μεγέθους 768 bytes και ROM μεγέθους 16Kbytes
- Τυπικές εφαρμογές:
- Τραπεζικές εργασίες και αγορές από το σπίτι
- Ηλεκτρονικό εμπόριο
- Έλεγχος της ισορροπίας του ποσού επιβάρυνσης και της αξίας των ηλεκτρονικών πορτοφολιών
- Έλεγχος πρόσβασης στο δίκτυο
- Ψηφιακή υπογραφή
- Νομιμότητα και προωθήσεις
- Αποθηκευμένη αξία
- Ταυτοποίηση
- Επικόλληση ετικέτας
- Χώρος στάθμευσης και διόδια
- Στα On-line τυχερά παιχνίδια

Τεχνικές προδιαγραφές:	
Διεπαφή (Interface)	USB V2.0 πλήρης ταχύτητα
Voltage	Ρυθμισμένο 5V συνεχές ρεύμα
Υποστήριξη λειτουργικών συστημάτων	Windows 98, Me, 2000, και XP

- **ISO7816 τυποποιημένος σειριακός αναγνώστης και προγραμματιστής έξυπνων καρτών.**



Ταυτότητα προϊόντος : ACR3OS

Λεπτομερής περιγραφή:

Το ACR30 είναι ένας συμπαγής, πολύ αποδοτικός οικονομικά, ενιαίου τσιπ αναγνώστης έξυπνων καρτών που υποστηρίζει όλες τις MCU-βασισμένες στις έξυπνες κάρτες με T=0 ή T=1 πρωτόκολλα καθώς επίσης και τις δημοφιλείς κάρτες μνήμης στην αγορά. Υποστηρίζει όλες τις σημαντικές πλατφόρμες των Η/Υ. Όντας μια λύση single-chip έξυπνων καρτών, ο αναγνώστης αυτός των έξυπνων καρτών είναι μια από τις πιο οικονομικώς αποδοτικές λύσεις για το ηλεκτρονικό εμπόριο, την ασφάλεια των πληροφοριών, τον έλεγχο πρόσβασης, την ταυτοποίηση και άλλες εφαρμογές των έξυπνων καρτών. Είναι διαθέσιμο σήμερα στη σειριακή διεπαφή: ACR30S.

Αυτό είναι μια ιδανική λύση για την εύκολη ενσωμάτωση της πρόσβασης των έξυπνων καρτών σε οποιαδήποτε εφαρμογή. Η ενότητα διατηρεί τις πλήρεις λειτουργίες ενός αναγνώστη και συγγραφέα έξυπνων καρτών και μπορεί να ενσωματωθεί εύκολα στους κερματοδέκτες ,στους μετρητές χώρων στάθμευσης, στις μηχανές πώλησης, στα πλυντήρια, στις μηχανές τυχερών παιχνιδιών, στα ATM, στα περίπλοκα συστήματα ελέγχου πρόσβασης και σε πολλά άλλα.

Χαρακτηριστικά γνωρίσματα των σειριακών αναγνωστών έξυπνων καρτών ACR30:

- Συμμορφωμένος με το ISO 7816-1/2/3 και το PC/Sc
- Επικυρωμένος από τη CE, τη FCC, EMV και τη Microsoft WHQL
- Διαβάζει και γράφει σε ΟΛΕΣ τις έξυπνες κάρτες μικροελεγκτών
- Διαβάζει και γράφει στη δημοφιλή μνήμη των τύπων των έξυπνων καρτών στην αγορά:
  - Siemens
  - Atmel
  - STMicroelectronics
- Συμβατό σύστημα με τις περισσότερες πλατφόρμες Η/Υ: WINDOWS.95 ,98, Me, NT και 2000, Linux.

Τεχνικές προδιαγραφές:	
Διεπαφή	RS- 232 (σειριακή) ή σειριακή
Τάση ανεφοδιασμού(Voltage)	Ρυθμισμένο 5V συνεχές ρεύμα
Υποστήριξη λειτουργικών συστημάτων	WINDOWS.95 , 98, Me, NT και 2000, Linux

- **USB διεπαφή αναγνώστη και προγραμματιστής έξυπνων καρτών**

Ταυτότητα προϊόντος: ACR30U

Τεχνικές προδιαγραφές:	
Διεπαφή	(USB)
Τάση ανεφοδιασμού	Ρυθμισμένο 5V συνεχές ρεύμα
Πρότυπα / πιστοποιήσεις	ISO 7816-1/2/3, PC/SC, CE, FCC
Υποστήριξη λειτουργικών συστημάτων	WINDOWS.95 ,98, Me, NT και 2000, Linux

- **ACF30 σειριακός εύκαμπτων θέσεων αναγνώστης έξυπνων καρτών**

Το ACF30 είναι η ιδανική λύση για την εύκολη ένταξη στο περιβάλλον υπολογιστών γραφείου

Αναγνώστης και προγραμματιστής έξυπνων καρτών πληκτρολογίου

Διεπαφή αναγνωστών πληκτρολογίου και έξυπνων καρτών που ενσωματώνεται μέσα σε μια μονάδα.

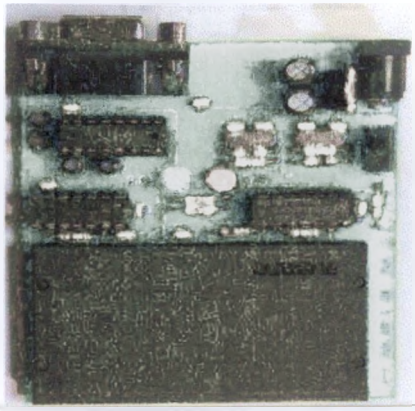
Ταυτότητα προϊόντων : ACK30S

Λεπτομερής περιγραφή:

Αυτό είναι μια ενσωματωμένη λύση έξυπνων καρτών για τις εφαρμογές PC/Sc. Ο αναγνώστης έξυπνων καρτών έχει ενσωματωμένες ηλεκτρονικές εφαρμογές σε ένα πληκτρολόγιο, που παρέχει μια τέλεια λύση στην υψηλή ασφάλεια έξυπνων καρτών. Αυτός ο αναγνώστης έξυπνων καρτών πληκτρολογίου είναι ιδανικός για τις εφαρμογές συμπεριλαμβανομένου: Τραπεζικές εργασίες Διαδικτύου, στην απευθείας σύνδεση με το χρηματιστήριο, εφαρμογή στις επιχειρήσεις Διαδικτύου που κάνουν εμπόριο, στις on-line αγορές, στην on-line ψυχαγωγία, όπως κινηματογράφος, χαρτοπαικτική λέσχη, παιχνίδια και πλήθος άλλων έξυπνων καρτών. Αυτός ο ισχυρός αναγνώστης έξυπνων καρτών πληκτρολογίου είναι διαθέσιμος σε δύο πρότυπα. ACK30S - ACR30 με τμηματική διεπαφή. Χαρακτηριστικά γνωρίσματα πληκτρολογίων: PS/2 διεπαφή με υποστήριξη 18 κλειδιών και 4 προγραμματίσημων κλειδιών.

Διπλού κρυστάλλου αναγνώστης / προγραμματιστής έξυπνων καρτών

Διπλού κρυστάλλου αναγνώστης / προγραμματιστής έξυπνων καρτών



Ταυτότητα προϊόντων :ISO 7816

Λεπτομερής περιγραφή:

Ο ISO 7816 διπλού κρυστάλλου προγραμματιστής έξυπνων καρτών έχει δυο κατασκευές στα κρύσταλλα, που επιτρέπουν το προγραμματισμό/ διάβασμα των έξυπνων καρτών σε δύο fequencies (3.57Mhz και 3.68Mhz). Ο προγραμματιστής έχει χτίσει στο διακόπτη και έτσι να γίνεται εύκολη η μεταστροφή μεταξύ των συχνοτήτων. Αυτός ο προγραμματιστής εργάζεται με τα δημοφιλή προγράμματα δωρεάν λογισμικού, όπως WinExplorer. Αυτός ο προγραμματιστής μπορεί να χρησιμοποιηθεί για να διαβάσει και να γράψει οποιαδήποτε έξυπνη κάρτα σύμφωνα με το ISO7816 σε 3,57 και 3,68 συχνότητες. Αυτός ο προγραμματιστής έξυπνων καρτών έρχεται με μια τμηματική παροχή καλωδίων και ηλεκτρικού ρεύματος για ευκολία.

Αυτοί οι προγραμματιστές έξυπνων καρτών χτίζονται επαγγελματικά και υποστηρίζονται με την εγγύηση επιστροφής χρημάτων εντός 6 μηνών. Εάν υπάρχει οποιοδήποτε πρόβλημα στους πρώτους 6 μήνες αποστέλλεται πίσω για ανταλλαγή.

ΚΕΦΑΛΑΙΟ 6ο

ΒΙΟΜΕΤΡΙΚΗ

1. Εισαγωγή - Γενικοί τρόποι επικύρωσης

Υπάρχουν διάφοροι τρόποι να επικυρωθεί ένα πρόσωπο ή μία πληροφορία για έναν υπολογιστή:

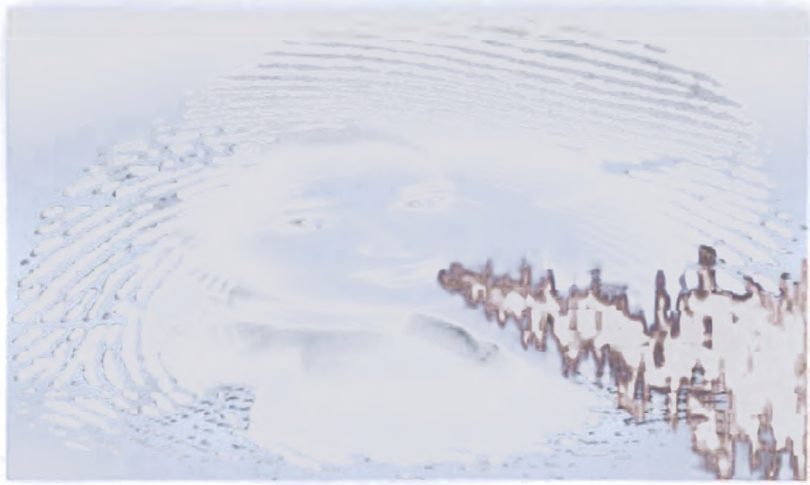
- **Κωδικός πρόσβασης** - η χρήση ενός ονόματος χρήστη και ενός κωδικού πρόσβασης παρέχει την πιο κοινή μορφή πιστοποίησης της ταυτότητας. Εισάγετε το όνομα και τον κωδικό πρόσβασής σας όταν προτρέπεται αυτό από τον υπολογιστή. Ο υπολογιστής ελέγχει το ζευγάρι σε ένα ασφαλές αρχείο για να τα επιβεβαιώσει. Εάν είτε το όνομα είτε ο κωδικός πρόσβασης δεν ταιριάζουν, δεν επιτρέπεστε η περαιτέρω πρόσβαση.

- **Κάρτες περασμάτων(Pass cards)** - αυτές οι κάρτες κυμαίνονται από μια απλή κάρτα με μια μαγνητική ταινία, παρόμοια με μια πιστωτική κάρτα, έως τις περίπλοκες έξυπνες κάρτες που έχουν ένα ενσωματωμένο τσιπ.

- **Ψηφιακές υπογραφές** - μια ψηφιακή υπογραφή είναι βασικά ένας τρόπος να εξασφαλιστεί ότι ένα ηλεκτρονικό έγγραφο (ηλεκτρονικό ταχυδρομείο, λογιστικό φύλλο, αρχείο κειμένου) είναι αυθεντικό. Τα πρότυπα ψηφιακών υπογραφών (DSS-Digital Signature Standard) είναι βασισμένα σε έναν τύπο μεθόδου κρυπτογράφησης με δημόσιο κλειδί, που χρησιμοποιεί τον Αλγόριθμο Ψηφιακών Υπογραφών (DSA-Digital Signature Algorithm). Ο DSS είναι η μορφή για τις ψηφιακές υπογραφές που έχει επικυρωθεί από την αμερικάνικη κυβέρνηση. Ο αλγόριθμος DSA αποτελείται

από ένα ιδιωτικό κλειδί, που είναι γνωστό μόνο από το δημιουργό του εγγράφου (ο υπογράφων), και ένα δημόσιο κλειδί. Το δημόσιο κλειδί έχει τέσσερα μέρη, για τα οποία μπορείτε να μάθετε περισσότερα σε αυτήν την σελίδα. Εάν τίποτα δεν αλλάζει στο έγγραφο αφότου συνδέεται με αυτό η ψηφιακή υπογραφή, αλλάζει την αξία με την οποία η ψηφιακή υπογραφή συγκρίνεται, δίνοντας την υπογραφή άκυρη.

Πρόσφατα, οι περιπλοκότερες μορφές της πιστοποίησης της ταυτότητας έχουν αρχίσει να εμφανίζονται στα συστήματα υπολογιστών σπιτιού και γραφείων. Τα περισσότερα από αυτά τα νέα συστήματα χρησιμοποιούν μια μορφή της βιομετρικής για την αυθεντικοποίηση. Η βιομετρική χρησιμοποιεί βιολογικές πληροφορίες για να επιβεβαιώσει την ταυτότητα.



Οι βιομετρικές λύσεις εμφανίζονται συνήθως. Δεν είναι μόνο ασφαλείς αλλά και δίνουν στο χρήστη την αίσθηση της ασφάλειας "υψηλής τεχνολογίας" που ενθαρρύνει την αποδοχή τους. Εντούτοις, οι βιομετρικές λύσεις έχουν και τα μειονεκτήματά τους. Ένα απ' αυτά είναι ότι η τεχνολογία είναι ακόμα νέα και μη αποδεδειγμένη. Υπάρχει επίσης το ερώτημα των ψεύτικων θετικών και των ψεύτικων αρνητικών. Καμία βιομετρική συσκευή δεν είναι100% ακριβής ώστε κάποιοι έγκυροι χρήστες να απορρίπτονται περιστασιακά (λανθασμένες αρνητικά) ή να επιτρέπεται σε μη έγκυρους χρήστες περιστασιακά (λανθασμένα θετικά). Και οι δύο περιπτώσεις θα μπορούσαν να υποστηριχτούν ή το αντίθετο, αλλά το πιο σημαντικό είναι ότι και οι δύο έχουν μειονεκτήματα. Κανένας δεν θέλει να αρνηθεί έναν εξουσιοδοτημένο χρήστη, ή ακόμα και να επιτρέψει την πρόσβαση σε έναν αναρμόδιο χρήστη είναι εξίσου απαράδεκτη. Ένας άλλος σημαντικός παράγοντας που αφήνεται συχνά έξω κατά τη συζήτηση των βιομετρικών λύσεων είναι ότι ενώ ένας χρήστης προσδιορίζεται μεμονωμένα, οι περισσότερες βιομετρικές λύσεις είναι ακόμα μόνο σχέδια πιστοποίησης ταυτότητας. Η ανίχνευση ενός δακτυλικού αποτυπώματος ή μια ανάλυση ρετίνας δεν είναι τίποτα περισσότερο από έναν μεγάλο μαθηματικό αριθμό που παράγεται από τα μοναδικά, αμετάβλητα βιολογικά χαρακτηριστικά που δημιουργούν έναν ισχυρό κωδικό πρόσβασης. Ακόμα μπορεί να υποβληθεί στην ίδια επαναλαμβανόμενη επίθεση που υποβάλλεται ένας κωδικός πρόσβασης. Εάν ένας χάκερ επρόκειτο να παρεμποδίσει αυτήν την μεταφορά και να λάβει αυτόν τον "κωδικό πρόσβασης" θα μπορούσε να χρησιμοποιηθεί στο μέλλον με την κακόβουλη πρόθεση. Ενώ μια βιομετρική λύση είναι ένας ισχυρός τρόπος να αποδείξει "ποιοι είστε," δεν εξετάζει "τι έχετε", κριτήρια που ταξινομούν τους δυο παράγοντες πιστοποίησης ταυτότητας. Από τη λήψη των μοναδικών χαρακτηριστικών των ατόμων, κάνει αυτήν την τεχνολογία να φανεί κάπως σαν το μεγάλο αδελφό της φύση. Στην πραγματικότητα, θα μπορούσε να υποστηριχτεί ότι ακόμα και με τις βιομετρικές λύσεις ένα κλειδί του υλικού θα πρέπει ακόμα να χρησιμοποιηθεί για να εξασφαλίσει ισχυρή πιστοποίηση της ταυ-

τότητας και ιδιωτικότητα. Αλλά ίσως η μεγαλύτερη πρόκληση που αντιμετωπίζει η βιομετρική είναι αυτή του κόστους. Από τώρα, οι βιομετρικές συσκευές δεν είναι οικονομικώς αποδοτικές.

Τα πλεονεκτήματα για τα οποία χρησιμοποιούμε ένα βιομετρικό για τον προσδιορισμό του είναι προφανή. Ο κάθε ένας από μας έχει ξεχάσει τον κωδικό πρόσβασής του και, σε μια προσπάθεια για να μην τον ξεχάσει την επόμενη φορά, είτε τον γράφει κάπου, ή επιλέγει έναν κωδικό που θα του είναι εύκολο να θυμηθεί. Στην ουσία έχουμε υπονομεύσει την ασφάλεια χάριν της ευκολίας. Η χρήση της βιομετρικής τα έχει αλλάξει όλα αυτά. Αντί να χρησιμοποιούμε ότι ξέρουμε για να αποδεικνύουμε ποιοι είμαστε, χρησιμοποιούμε κάποιο μοναδικό χαρακτηριστικό μας γνώρισμα όπως ένα δακτυλικό αποτύπωμα, αποτύπωση παλάμης(handprint) ή τον ήχο της φωνής μας.

Ένας κόσμος που αντικαθιστά μια δοκιμαστική μνήμη με έναν σαρωτή(scanner) δακτυλικών αποτυπωμάτων είναι ελκυστικός. Υπάρχουν διαθέσιμες πολυάριθμες συσκευές σήμερα που παρέχουν ασφαλή πρόσβαση που βασίζονται απλώς σε έναν βιομετρικό. Αν και αυτό είναι ένα βήμα προς τη σωστή κατεύθυνση, αυτό το έγγραφο κάνει το επιχείρημα αυτό να έχει περισσότερες ανάγκες απ' αυτές που μπορούν να γίνουν.

Για να κατανοήσετε το πρόβλημα, ας αρχίσουμε με το πώς ένα βιομετρικό, όπως ένα δακτυλικό αποτύπωμα, χρησιμοποιείται για να αποδείξει την ταυτότητά μας. Η διαδικασία αρχίζει από την παραγωγή ενός αντιγράφου, ή του πρότυπου, του δακτυλικού μας αποτυπώματός . Αυτό το πρότυπο πρέπει να καταχωρηθεί κάπου και να διατεθεί μόνο για τη σύγκριση με μια ζωντανή ανίχνευση του δακτυλικού μας αποτυπώματος . Για το που καταχωρείτε αυτό το πρότυπο είναι μια κρίσιμη ερώτηση. Θα μπορούσε να καταχωρηθεί σε κάθε μεμονωμένο σαρωτή δακτυλικών αποτυπωμάτων, αλλά για τις περισσότερες εφαρμογές αυτό δεν είναι ιδιαίτερα πρακτικό. Μια καλύτερη λύση είναι να καταχωρηθεί το πρότυπο σε κάποια κεντρική βάση δεδομένων. Τώρα ταιριάζοντας ένα ζωντανό δακτυλικό αποτύπωμα με όλα τα πρότυπα της βάσης δεδομένων μπορεί να προσδιορίσει ένα άτομο, ή, εάν το

όνομα του ατόμου παρέχεται με το ζωντανό δακτυλικό αποτύπωμα, η ταυτότητα μπορεί να επαληθευτεί αναζητώντας το πρότυπο, που συνδέεται με εκείνο το άτομο για να κάνει τη σύγκριση.

Όσο καλή και αν είναι αυτή η λύση, υποφέρει από πολλά μειονεκτήματα. Οι μεγάλες βάσεις δεδομένων μπορούν να είναι πολύ δαπανηρές για να παραχθούν και να διατηρηθούν και όταν βοηθούν τις βιομετρικές συσκευές μας είναι άχρηστες. Υπάρχει επίσης το ερώτημα ενός ατομικού δικαιώματος, του ελέγχου των προσωπικών βιομετρικών πληροφοριών. Σε λίγους από μας θα άρεσε να καταχωρούνται τα βιομετρικά μας πρότυπά σε διάφορες άγνωστες τοποθεσίες πέρα του ελέγχου μας. Η πιθανή κοινοποίηση αυτών των πληροφοριών σε αναρμόδια άτομα, όχι μόνο αυξάνει τα ερωτήματα της ατομικής ιδιωτικότητας αλλά και παρουσιάζει μια σοβαρή απειλή για την ασφάλεια. Χωρίς να μεταβούμε σε λεπτομέρειες, σκεφτόμαστε καθαρά μετριοπαθώς ότι όσο περισσότερη δυσκολία έχει ένας πιθανός αντίπαλος στη λήψη ενός νόμιμου βιομετρικού προτύπου, τόσο πιο ασφαλής είναι η διαδικασία προσδιορισμού. Η λύση μας σε αυτό το πρόβλημα είναι να καταχωρήσουμε το βιομετρικό πρότυπο σε ένα σημείο, το οποίο διαβάζεται από την ίδια συσκευή που συλλέγει και το ζωντανό βιομετρικό. Το Webster καθορίζει ένα σημείο ως "κάτι που εξυπηρετεί ως σημάδι της αρχής, ταυτότητας, γνησιότητας...". Εδώ το σημείο χρησιμοποιείται για να δέσει μια φυσική ιδιότητα (το βιομετρικός μας) με την ταυτότητά μας.

Το σημείο ανάγνωσης που αντιπροσωπεύεται από μια πλαστική κάρτα με ένα μπάλωμα PDF417 που θα το ονομάσουμε οπτική κάρτα, σημείο εγγραφής και ανάγνωσης που αντιπροσωπεύεται από μια κάρτα μνήμης, και ένα έξυπνο σημείο το οποίο αντιπροσωπεύεται από μια έξυπνη κάρτα. Χρησιμοποιώντας ένα από αυτά τα σημεία ο βιομετρικός /συμβολικός μας αναγνώστης μπορεί να συγκρίνει ένα ζωντανό βιομετρικό και ένα πρότυπο ενός προσώπου χωρίς να πρέπει να επικοινωνήσει ξανά με κάποια εξωτερική συσκευή. Η σύγκριση μπορεί να γίνει μέσα στον αναγνώστη. Ο σκοπός αυτού του εγγράφου είναι να δείξει πώς αυτά τα σημεία μπορούν να παρέχουν μια κατάλληλη, ασφαλή διαδικασία προσδιορισμού που

προστατεύει την ατομική ιδιωτικότητα. Για να το κάνουμε αυτό πρέπει αρχικά να αναθεωρήσουμε μερικά κρίσιμα γεγονότα για κάποιες σύγχρονες κρυπτογραφικές μεθόδους.

2. Βασικές κατηγορίες βιομετρικών μεθόδων:

Οι βιομετρικοί έλέγχοι διακρίνονται στις εξής δυο βασικές κατηγορίες:

- **Τεχνικές μέτρησης της συμπεριφοράς**. οι οποίες βασίζονται στη μέτρηση του τρόπου, με τον οποίο εκτελείται μια ενέργεια από το χρήστη (π.χ. ο τρόπος υπογραφής του ονόματος του, η ομιλίας μιας φράσης).
- **Φυσιομετρικές τεχνικές,** όπου φυσικά χαρακτηριστικά, όπως π,χ. το αποτύπωμα ή η μορφή του χεριού, αποτελούν αντικείμενο μέτρησης και σύγκρισης με κάποιο μοναδικό στοιχείο.

3. Βιομετρικά στοιχεία

Με το πέρασμα του χρόνου και την πρόοδο της τεχνολογίας, καθημερινά ερχόμαστε σε επαφή με επιτεύγματα, που παλιότερα αποτελούσαν πεδίο δράσης και αντικείμενο πόθου της επιστημονικής φαντασίας. Πόσοι άραγε από εμάς δεν θυμόμαστε τον Hal, τον υπολογιστή της Οδύσσειας 2001. Βασική του ικανότητα ήταν ότι μπορούσε να αναγνωρίσει τον ιδιοκτήτη του. Με τις νέες μεθόδους αναγνώρισης φυσικών χαρακτηριστικών, σε λίγο καιρό η εικόνα αυτή θα μας είναι οικεία και καθημερινή. Η αναγνώριση φυσικών χαρακτηριστικών (biometrics) είναι μια σειρά από αυτοματοποιημένες διεργασίες, οι οποίες αναγνωρίζουν ένα άτομο, αναλύοντας κάποια χαρακτηριστικά του. Τα κυριότερα χαρακτηριστικά που μετρώνται και αναγνωρίζονται είναι το πρόσωπο, τα δακτυλικά αποτυπώματα, η μορφολογία του χεριού, ο γραφικός χαρακτήρας, ο αμφιβληστροειδής του ματιού και η φωνή. Η πρώτη κατηγοριοποίηση που μπορούμε να κάνουμε έχει σχέση με το είδος των στοιχείων που χρησιμοποιούμε για την αναγνώριση ενός προσώπου. Παρατηρούμε ότι εκτός από την αναγνώριση φωνής, όλες οι υπόλοιπες μέθοδοι στηρίζονται στην αναγνώριση εικόνας.

α) Εξακρίβωση υπογραφής:

Οι αυτόματοι έλεγχοι υπογραφής αποτελούν μία φυσιολογική επέκταση μιας συνήθους διεργασίας, όπου καμία πολιτιστική αλλαγή δεν παρατηρείται. Ενώ ο ανθρώπινος παράγοντας ελέγχει κάθε φορά την τελική μορφή της υπογραφής, στον αυτόματο έλεγχο υπογραφής δίνεται μεγάλη έμφαση στη δυναμική αλλαγή της υπογραφής, δηλαδή στη σχετική ταχύτητα με την οποία σχεδιάζονται οι γραμμές και στη χρησιμοποιούμενη πίεση. Έτσι, η μέτρηση των παραμέτρων αυτών βοηθάει στη σύγκριση αποτελεσμάτων υπό διαφορετικές συνθήκες και ελαχιστοποιεί τις προσπάθειες πρόσβασης στο σύστημα.

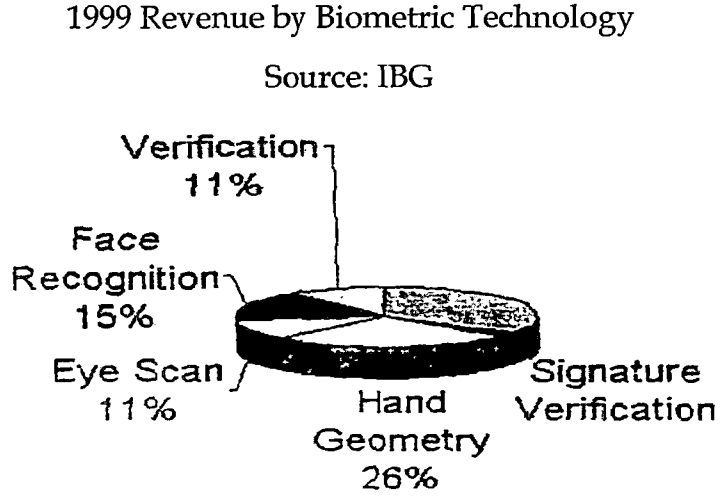
Η μέτρηση και αποθήκευση των δυναμικών στοιχείων μίας υπογραφής πραγματοποιείται με πλήθος μεθόδων, πολλές εκ των οποίων αποτελούν πρωτότυπα, όμως, όλες οι μετρήσεις γίνονται με χρήση ψηφιοποιημένης πλάκας ή ειδικής επιφάνειας. Όμως, όπως με όλα τα χαρακτηριστικά ανθρώπινης συμπεριφοράς, έτσι και οι υπογραφές επηρεάζονται από τη διάθεση του ελεγχόμενου χρήστη, το περιβάλλον και τις μεταβολές του, το μολύβι που χρησιμοποιείται ή το αντίστοιχο χαρτί , με αποτέλεσμα συχνά πολλοί άνθρωποι να διαθέτουν σύμφωνες υπογραφές. Με κατάλληλη ρύθμιση του συστήματος μπορούν να επιτευχθούν πολύ καλά αποτελέσματα για συχνούς χρήστες, αλλά και πάλι εμφανίζονται προβλήματα με τους χρήστες που απορρίπτονται από το σύστημα συχνά.

Η πλατφόρμα υπογραφής συνήθως έχει πολύ μικρό μέγεθος (περίπου 1 kb) γεγονός που καθιστά τη συγκεκριμένη τεχνική κατάλληλη για χρήση online ή με τη βοήθεια έξυπνης κάρτας. Επιπρόσθετο πλεονέκτημα των περισσότερων συστημάτων αναγνώρισης υπογραφής είναι ότι το αρχείο της υπογραφής εκλαμβάνεται και ως απόδειξη της πραγματοποιούμενης διεργασίας, δηλαδή επιτρέπεται με αυτόν τον τρόπο ο περιορισμός των συστημάτων που βασίζονται στη χρήση χαρτιού, όπως τα πιστωτικά μηχανήματα. Λόγω απλότητας και έλλειψης ιδιαίτερης αξιοπιστίας, η συγκεκριμένη μέθο-

δος τείνει να εκλείψει και να αντικατασταθεί από άλλες πιο σύγχρονες και αξιόπιστες μεθόδους .

β) Εξακρίβωση μέσω πληκτρολόγησης:

Χαρακτηριστικό της ανθρώπινης συμπεριφοράς μπορεί να αποτελεί και ο τρόπος πληκτρολόγησης του χρήστη και μάλιστα, ακόμα και επιδέξιοι δακτυλογράφοι αναγνωρίζονται με αυτόν τον τρόπο. Έτσι, παρέχεται ένας γρήγορος τρόπος αναγνώρισης των χρηστών του συστήματος ,χωρίς να απαιτείται καμία άλλη επιπρόσθετη διάταξη εισαγωγής δεδομένων ή διαδικασίας εγγραφής.



ΣΧΗΜΑ 10 : Βιομετρικές μεθόδοι & χρήση τους

Η συγκεκριμένη μέθοδος καθίσταται ελκυστική για εφαρμογές, όπως η προστασία ενός μικρού αριθμού χρηστών, οι οποίοι θεωρούνται σημαντικοί για το σύστημα. Παρόλο που οι εφαρμογές τέτοιων βιομετρικών στοιχείων θεωρούνται σχετικά περιορισμένες, η παραπάνω τεχνική κρίνεται ως ένα πολύ χρήσιμο εργαλείο στη βιομηχανία των υπολογιστικών συστημάτων ελέγχου πρόσβασης.

γ) Αναγνώριση φωνής

Τα συστήματα αναγνώρισης φωνής αποτελούν τα πιο συνηθισμένα σύγχρονα συστήματα, αλλά δυστυχώς δεν έχουν προσεγγίσει ακόμα τα επιθυμητά επίπεδα εφαρμογής σε εμπορικό περιβάλλον.

Η αναγνώριση φωνής αποτελεί μέρος της τεχνολογίας επεξεργασίας ομιλίας, η οποία παρουσιάζει ευρύτερη εφαρμογή σε πολλούς τομείς, ειδικά στη ψηφιακή τηλεφωνία και τηλεσυνδιάσκεψη, με τη βοήθεια φασματικής ανάλυσης και ειδικών αλγορίθμων, ανεπτυγμένων για υψηλής συχνότητας συμπίεση και ακριβή εμφάνιση της ομιλίας. Με τη χρήση των παραπάνω συστημάτων επιτρέπεται ένας πολύπλευρος έλεγχος, αφού ελέγχονται όχι μόνο ο λόγος του χρήστη, αλλά και ο τρόπος του λόγου. Επιπλέον, σε κάποιες εφαρμογές η χρήση τους συνεπάγεται και μικρό οικονομικό κόστος, λόγω της ύπαρξης ενός απλού ψηφιακού επεξεργαστή σημάτων (digital signal processor-DSP)αντί πολλών μικροφώνων.

Για να αναγνωρίσουμε ένα άτομο από τη φωνή του, χρησιμοποιούμε τα λεγόμενα "φωνητικά αποτυπώματα". Η ανθρώπινη φωνή δεν είναι ικανή να εκφέρει έναν τόνο κάθε φορά. Αντιθέτως παράγει συνεχόμενους βασικούς τόνους που δημιουργούν τη χροιά που ακούμε. Από όλα τα χαρακτηριστικά της ανθρώπινης φωνής τα σημαντικότερα είναι η συχνότητα και η ένταση. Η συχνότητα είναι η ταχύτητα με την οποία πάλλεται ο αέρας όταν μιλάμε, ενώ η ένταση είναι η δύναμη με την οποία εξέρχεται ο αέρας από το στόμα.

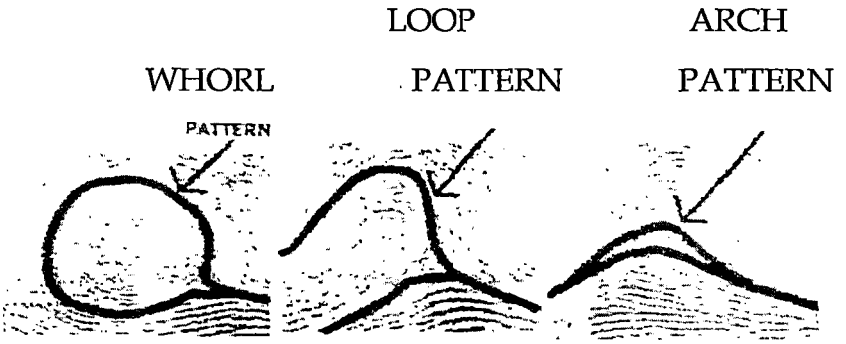
Το σύστημα που χρησιμοποιούμε για να κάνει την αναγνώριση, "εκπαιδεύεται" και "μαθαίνει" συγκεκριμένες λέξεις από συγκεκριμένο άτομο, φτιάχνοντας μια βάση φωνητικών δεδομένων και συγκρίνοντας, όταν χρειαστεί τη φωνή του. Αναλόγως με τον εξοπλισμό που διαθέτουμε, το ποσοστό επιτυχημένης αναγνώρισης μπορεί να είναι αρκετά υψηλό. Όμως υπάρχουν κάποιοι περιορισμοί και κάποιοι κανόνες που πρέπει να ακολουθούνται. Για παράδειγμα, οι λέξεις και οι φράσεις που θα χρησιμοποιηθούν πρέπει να είναι ακριβώς οι ίδιες.

4. Φυσιομετρικά στοιχεία

α) Αποτύπωμα δακτύλου-αντίχειρα:

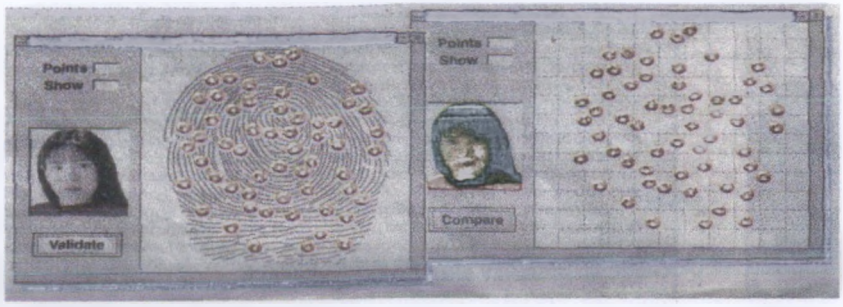
Χρησιμοποιείται κυρίως στο ηλεκτρονικό εμπόριο (e-commerce) ή σε εφαρμογές ασφάλειας δικτύων, δημόσιων υπηρεσιών και πρόσβασης προσώπων. Μολονότι υπάρχουν και άλλες ακριβείς μέθοδοι, η παραπάνω κρίνεται εξαιρετικά αξιόπιστη, με ευρεία απήχηση από τους χρήστες.

Τεχνολογία: Τα παραπάνω συστήματα μπορούν να απομονώσουν μία λεπτομερή μικρογραφία (minutiae) του αποτυπώματος ή ολόκληρη εικόνα του δαχτύλου. Ουσιαστικά, η μικρογραφία σχηματίζεται σε συντεταγμένες χ και ν και σε μία κατεύθυνση, ανάλυση πολύ συνηθισμένη. Η διαδικασία αυτή οδηγεί σε περιγράμματα περίπου 100 bytes, πολύ μικρότερα από τα αντίστοιχα μίας ολόκληρης εικόνας του δαχτύλου (500-1500 bytes).



ΣΧΗΜΑ 11: Χαρακτηριστικά αποτυπώματος δαχτύλου

Επειδή η επιφάνεια του δαχτύλου είναι πολύ μικρή και ο τρόπος καθημερινής ζωής ενδεχομένως να αλλοιώνει τα χαρακτηριστικά του, τα τελευταία χρόνια έχουν αναπτυχθεί διάφορες τεχνικές, οι οποίας παρέχουν την εικόνα με μεγαλύτερη ακρίβεια και ανάλυση. Οι σημαντικότερες από αυτές είναι: η οπτική τεχνική, η τεχνική σιλικόνης και υπερήχων.

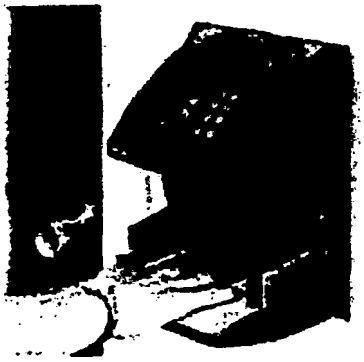


Προβλήματα-Κόστος: Τα προβλήματα ίων παραπάνω μεθόδων σχετίζονται με την αρμονία τους σε δημόσιες εφαρμογές, αφού περιπτώσεις όπως εργάτες ή φανατικοί καπνιστές χαρακτηρίζονται από αμυδρά αποτυπώματα, τα οποία δε μπορούν να αναλυθούν επαναληπτικά.

Από την άλλη μεριά, οι ηλεκτρονικές διατάξεις ανάγνωσης κοστολογούνται μεταξύ 600 και 1800 ΕΥΡΩ, όμως αναμένεται η επόμενη γενιά να καταστήσει ικανή τη χρήση ειδικά σχεδιασμένων αισθητήρων τύπου single-chip, οι οποίοι να απομονώνουν πληθώρα αντιτύπων του μεγέθους του δαχτύλου σε μορφή πίνακα, στοιχείο που θα συμβάλλει στη μείωση του κόστους, ενώ με εισαγωγή της χρήσης της τεχνολογίας σε καθημερινές εφαρμογές, το κόστος ίσως να υποβαθμιστεί ακόμα περισσότερο.

β) Εξέταση γεωμετρίας παλάμης(hand geometry)

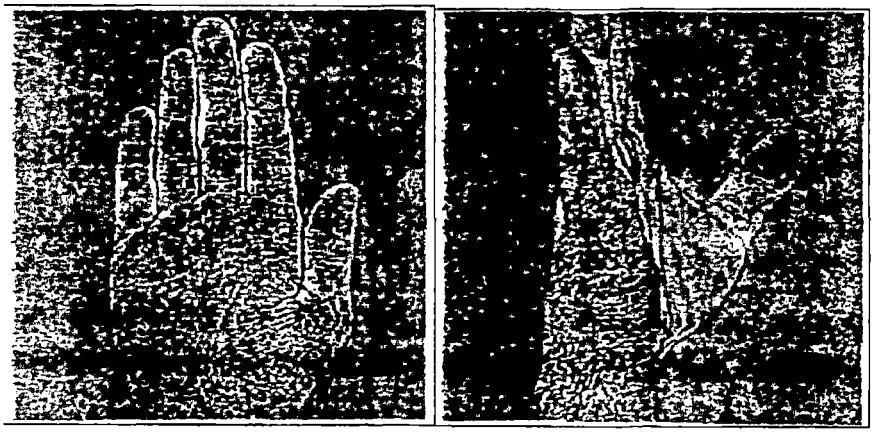
Η σάρωση παλάμης (handscan). γνωστή και σαν γεωμετρία παλάμης (hand geometry) αποτελεί την ευκολότερη μέθοδο και σημαντικότερη βιομετρική τεχνολογία ελέγχου πρόσβασης και αυθεντικοποίησης, ,αφού η παλάμη αποτελεί ένα μεγάλου μεγέθους ανθρώπινο χαρακτηριστικό, το οποίο μπορεί να τοποθετηθεί και να εξεταστεί με ακρίβεια σε κατάλληλο σύστημα (σχήμα 12).



ΣΧΗΜΑ 12 : Συσκευή ανάγνωσης γεωμετρίας παλάμης.

Η μέθοδος βασίζεται στην κατάλληλη τοποθέτηση και σάρωση της παλάμης όπου η εικόνα λαμβάνεται με τη βοήθεια κάμερας video και μετρώνται παράμετροι, όπως το ύψος των δαχτύλων, η απόσταση μεταξύ των αρθρώσεων κ.λ.π. παρέχοντας ένα περίγραμμα αναφοράς. Το μοντέλο αυτό μπορεί να είναι πάρα πολύ μικρό (συνήθως περίπου 10 dytes), γι' αυτό και κρίνεται ιδανική επιλογή για συστήματα χαμηλής έως και μεσαίας ασφάλειας(σχήμα 13).

Μάλιστα, η τελευταία γενιά τέτοιων συστημάτων χρησιμοποιήθηκε για έλεγχο πρόσβασης στο Ολυμπιακό χωριό των αθλητών στην Ατλάντα το 1996. σε ιδιωτικές εταιρείες, καθώς και στους χώρους επιβίβασης των επιβατών σε διάφορα αεροδρόμια των ΗΠΑ.

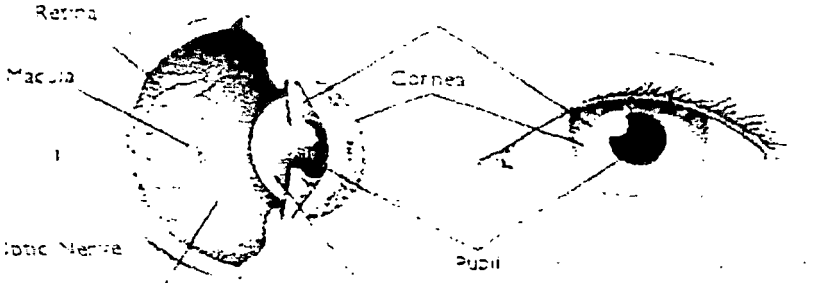


ΣΧΗΜΑ 13: Εικόνες με σάρωση γεωμετρίας παλάμης.

β) Σάρωση ρετίνας (Retinal scan)

Η σάρωση ρετίνας αποτελεί εξαιρετικά ακριβή και αξιόπιστη βιομετρική τεχνολογία, η οποία κρίνεται σαν η αποτελεσματικότερη επιλογή σε απαιτητικές περιστάσεις αυθεντικοποίησης.

Τεχνολογία: θεωρείται η δυσκολότερη σε χρήση τεχνολογία, αφού οι αναπαραστάσεις, του παρέχουν σι διατάξεις ανάγνωσης πάνω σε ειδικό φιλμ. πολλές φορές είναι εσφαλμένες: λόγω κυρίως αστάθειας του υποκειμένου. Μειονέκτημα της μεθόδου αποτελεί το γεγονός. ότι στην παρούσα φάση, απαιτείται η συνεργασία του χρήστη, ο οποίος θα πρέπει να είναι εξοικειωμένος με την τεχνολογία, ειδάλλως η μέτοηση θα αποτύχει δραματικά. Επιπρόσθετα, αρκετοί άνθρωποι δυσανασχετούν με την ιδέα της τοποθέτησης του οφθαλμού τους απέναντι από μία κάμερα, γεγονός που εκτόπισε τη μέθοδο σε καθημερινού τύπου εφαρμογές .



ΣΧΗΜΑ 14: Φυσιολογία οφθαλμού

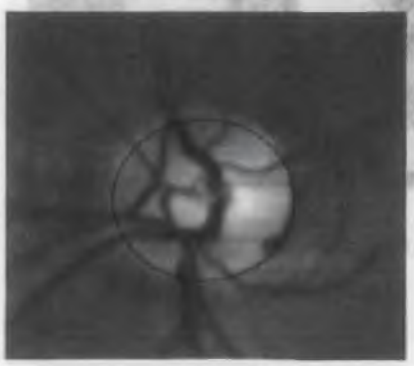
Καθώς ο χρήστης τοποθετεί τον οφθαλμό του στην διάταξη, ένα ειδικό φως πράσινου χρώματος διαπερνά τη ρετίνα, πραγματοποιώντας μετρήσεις σε περίπου 400 διαφορετικά σημεία. Συγκριτικά. η μέθοδος κρίνεται εξαιρετικά ακριβής, αφού χαρακτηριστικά κατά τη μέθοδο ανάκτησης δαχτυλικού αποτυπώματος μετρώνται μόλις 30-40 διακριτά σημεία. Τα παραγόμενα περιγράμματα έχουν πολύ μικρό μέγεθος (περίπου 35 bytes στα συνηθέστερα εμπορικά συστήματα), ενώ τα κριτήρια αξιοπιστίας ,χαρακτηρίζονται πολύ ικανοποιητικά.

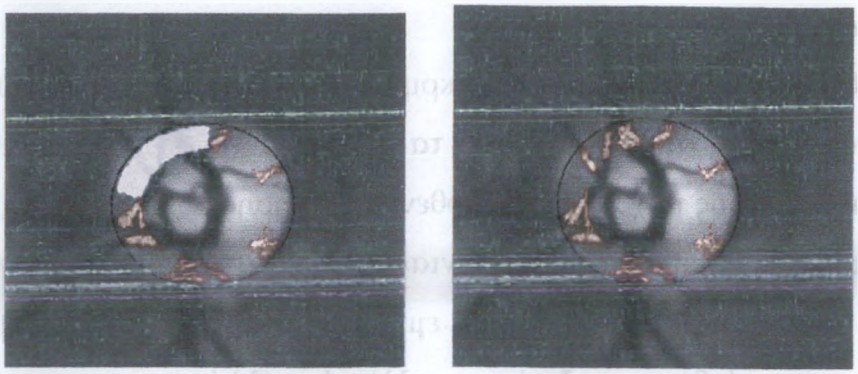
δ) Σάρωση ίριδος (Iris scan)

Η μέθοδος αυτή αποτελεί την ακριβέστερη και την πιο διαισθητική, τυγχάνοντας μεγάλης αποδοχής, αφού τα τελευταία χρόνια έχει αντικαταστήσει παραδοσιακούς μηχανισμούς αυθεντικοποίησης. όπως κωδικοί, προσωπικοί αριθμοί ή ακόμα και «κουπόνια». Η εφαρμογή τους συναντάται συνήθως σε περιπτώσεις ηλεκτρονικού εμπορίου(e-commerce), πρόσβασης σε δίκτυα, τερματικά διατραπεζικών συναλλαγών, αλλά και σε ιατρικά αρχεία ασθενών ή βάσεις δεδομένων.

Η μονάδα οπτικής αναγνώρισης του συστήματος Iris Access 3000 της εταιρείας LG Electronics. Διακρίνεται καθαρά ο φακός της κάμερας που πραγματοποιεί το image grabbing του ματιού.

Τεχνολογία: Η τεχνολογία που χρησιμοποιείται μετατρέπει όλα τα παραπάνω στοιχεία σε ένα κωδικό 512 byte, ο οποίος και αποτελεί το πλαίσιο αναφοράς (template) για οποιαδήποτε μελλοντική χρήση της μεθόδου. Ο όγκος των δεδομένων που αποθηκεύονται με τον παραπάνω τρόπο μπορεί να Φαντάζει πολύ μεγάλος σε σύγκριση πάντα με τις υπόλοιπες μεθόδους, όμως. οι πληροφορίες που λαμβάνονται κρίνονται ανεκτίμητες, αφού κάθε ίριδα υπολογίζεται ότι έχει 266 μοναδικά σημεία (spots) ενώ άλλα χαρακτηριστικά που εξετάζονται με βιομετρικές τεχνικές έχουν μόλις 13-60 σημεία.



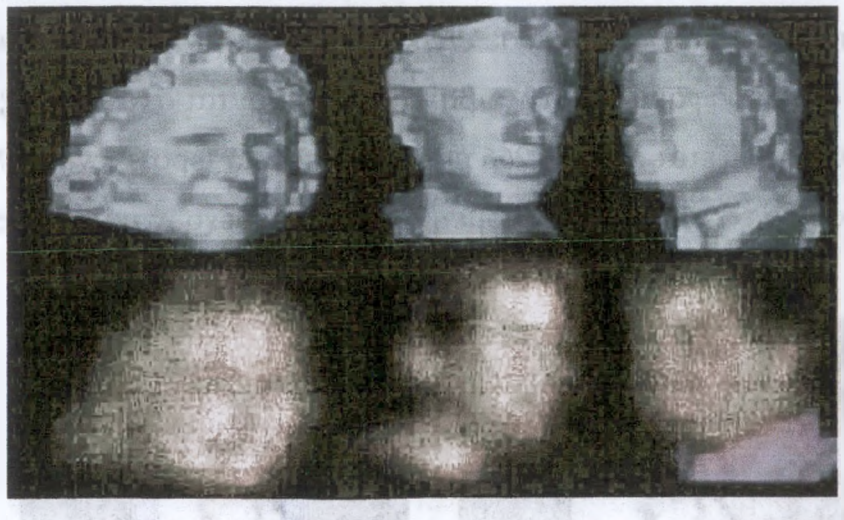


ΣΧΗΜΑ 15: Εικόνες σάρωσης ίριδος

Η παραπάνω μέθοδος αποτελεί την πιο σύγχρονη από όλες τις τεχνικές και έχει ήδη χρησιμοποιηθεί σε διάφορα σωφρονιστικά καταστήματα και στρατιωτικές υπηρεσίες των ΗΠΑ για έλεγχο πρόσβασης.

ε) Αναγνώριση προσώπου(facial recognition)

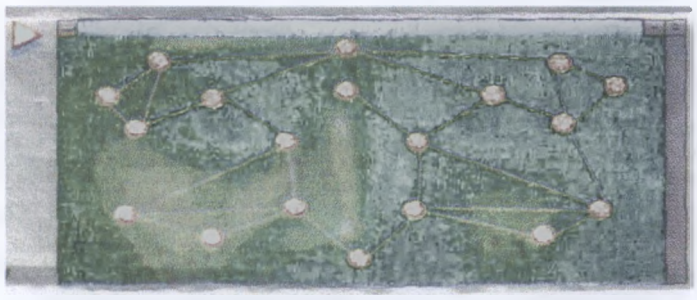
Η αναγνώριση προσώπου αποτελεί μία βιομετρική μέθοδος. ευρύτατα διαδεδομένη, ιδανική για ένα μεγάλο αριθμό εφαρμογών, όπως ελέγχου πρόσβασης σε υπολογιστές ή κτιριακά συγκροτήματα, τράπεζες πληροφοριών ή τερματικών μηχανημάτων, με χρήση διακριτών χαρακτηριστικών του ,προσώπου. (σχήμα 16).



Σχήμα 16: Παράδειγμα εικόνων αναγνώρισης προσώπου

Απαιτήσεις hardware: η παραπάνω τεχνολογία λειτουργεί αποτελεσματικά με μία συμβατική, video-PC camera ,απαιτώντας ελάχιστη ανάλυση 320 x 240pixels και 3-5 frames/sec. Ο συνδυασμός περισσότερων πλαισίων με υψηλότερη ανάλυση θα οδηγήσει σε καλύτερη εκτέλεση ελέγχων αυθεντικοποίησης και ταυτοποίησης. Οπωσδήποτε, η απόσταση της διάταξης μέτρησης από το υποκείμενο αποτελεί σημαντικό παράγοντα, που όμως εξαρτάται άμεσα από την ποιότητα της χρησιμοποιούμενης κάμερας και των δυνατοτήτων του συστήματος.

Συνήθως, το δείγμα λαμβάνεται κατά τη διεργασία εγγραφής (enrollment process). όπου αρκετές εικόνες του προσώπου του χρήστη λαμβάνονται μέσα σε χρονική περίοδο των 30 περίπου δευτερολέπτων. Οι εικόνες απεικονίζουν το χρήστη από διαφορετικές γωνίες και με διαφορετικές εκφράσεις προσώπου, με την ακρίβεια της εικόνας να εξαρτάται άμεσα από τον αριθμό των γωνιών και των εικόνων που λαμβάνονται συνολικά, Μετά τη διεργασία εγγραφής, εξάγονται κύρια χαρακτηριστικά της εικόνας, προκειμένου να συγκριθούν με το ήδη υπάρχον περίγραμμα αναφοράς, το οποίο σαν μέγεθος είναι πολύ μεγαλύτερο από την αντίστοιχη εικόνα. Συγκεκριμένα, ενώ τα χαρακτηριστικά ποιότητας μιας εικόνας προσώπου απαιτούν περίπου 150-300 kb, τα περιγράμματα αναφοράς είναι προσεγγιστικά 1300 bytes ή περίπου 1/100οστό του μεγέθους του αυθεντικού πλαισίου.



ΣΤ) Άλλες μεθόδοι

Θεωρητικά, οποιοσδήποτε μέρος του ανθρωπίνου σώματος ,μπορεί να χρησιμοποιηθεί ως βάση μέτρησης από κατάλληλο βιομετρικό σύστημα. Όμως. οι περισσότερες εμπορικές μορφές των συστημάτων αυτών επιστρώ-

νονται στα στοιχεία αυτά που είναι εύκολο να μετρηθούν και είναι περισσότερο αποδεκτά από το ευρύ κοινό.

Όμως, αναμφισβήτητα η υπέρτατη βιομετρική μέθοδος είναι η ανάλυση DNA., όπου μπορεί να ισχυριστεί με σιγουριά κάποιος ότι θα ποέπει να περάσουν δεκαετίες, προκειμένου η συγκεκριμένη τεχνική να χρησιμοποιείται για την αναγνώριση ταυτότητας σε εφαρμογές, όπως η αγορά σε ένα πολυκατάστημα ή η επιβίβαση σε κάποιο μεταφορικό μέσο.

5. Συνδυασμός της βιομετρικής και των συσκευών ανάγνωσης καρτών

Είναι σημαντικό να μελετήσουμε τη συσκευή ή τον αναγνώστη που θα διαβάζουν το σημείο και θα χειρίζονται τις μετρήσεις των βιομετρικών. Ένας βιομετρικός αναγνώστης στέλνει τις πληροφορίες άμεσα σε μια άλλη συσκευή, όπως σε ένα υπολογιστή, για τη σύγκριση τους με ένα προηγούμενο καταχωρημένο πρότυπο. Είναι πιθανό να υπάρχει ένας δεύτερος αναγνώστης που χειρίζεται το σημείο και στέλνει τις πληροφορίες που είναι καταχωρημένες σ 'αυτόν στον υπολογιστή. Υπάρχουν διάφορα προϊόντα στην αγορά σήμερα, που έχουν και συμβολικό και βιομετρικό αναγνώστη και στέλνουν πληροφορίες σε έναν υπολογιστή, όπου οι πληροφορίες του σημείου συγκρίνονται με τις πληροφορίες που προέρχονται από το βιομετρικό αναγνώστη. Μερικά από αυτά τα προϊόντα συνδυάζουν τους δύο αναγνώστες ενώ άλλα κρατούν τους δύο αναγνώστες χωριστούς. Αυτό δεν είναι και πολύ μεγάλη βελτίωση πάνω στη χρήση ενός μοναδικού βιομετρικού αναγνώστη, αφού ευαίσθητες βιομετρικές και άλλες πληροφορίες έχουν αφαιρεθεί από το σημείο και έτσι εκτίθονται σε κίνδυνο.

Συχνά, αυτά τα προϊόντα κρυπτογραφούν τις πληροφορίες που έχουν σταλεί από το συμβολικό αναγνώστη στον υπολογιστή και μπορούν ακόμα και να κρυπτογραφήσουν το ζωντανό βιομετρικό που έχει σταλεί. Φυσικά, αυτό είναι το πιο σωστό πράγμα που μπορεί να κάνει κάτω απ' αυτές τις περιστάσεις, αλλά ευαίσθητες βιομετρικές πληροφορίες είναι ακόμα εκτεθειμένες στο λιγότερο ασφαλές περιβάλλον του υπολογιστή. Θεωρούμε ότι είναι

πολύ πιο επιθυμητό να επικρατήσει το βιομετρικό πρότυπο και σε όλες τις άλλες στιγμές να κρατήσει το πρότυπο μέσα στο σημείο. Με τον ίδιο τρόπο είναι ευκολότερο να εξασφαλιστούν οι πληροφορίες σε έναν αυτόνομο υπολογιστή παρά σε έναν υπολογιστή που συνδέεται με ένα δίκτυο, ειδικά το Διαδίκτυο.

6. Συνδυασμός βιομετρικών με έξυπνες κάρτες

Οι περισσότεροι από μας έχουν ακούσει για τις έξυπνες κάρτες, εκείνους τους μικρούς υπολογιστές που μεταφέρουμε τριγύρω με τις τσέπες μας που μεταμφιέζονται ως πιστωτικές κάρτες. Μπορούμε να έχουμε αναρωτηθεί τι τους κάνει τόσο ελκυστικούς. Σε αυτό το τμήμα θα έχουμε την ευκαιρία να δούμε πώς η υπολογιστική ισχύς της έξυπνης κάρτας μπορεί να μας δώσει μερικές εντυπωσιακές βελτιώσεις στην ασφάλεια και στη λειτουργία. Δεδομένου ότι έχουν γίνει δημοφιλέστερες, οι εφαρμογές των έξυπνων καρτών έχουν γραφτεί για την υγειονομική περίθαλψη, τις οικονομικές υπηρεσίες, τα ταξίδια ακόμα και για τα εμπιστευτικά προγράμματα. Όλα αυτά μπορούν να είναι διαθέσιμα προς χρήση από ένα ίδρυμα που αποφασίζει να χρησιμοποιήσει τις έξυπνες κάρτες ως συμβολικά τους. Εντούτοις, πρέπει να επισημανθεί ότι οι πολλαπλές εφαρμογές στις έξυπνες κάρτες μπορεί να προκαλέσουν μερικές ανησυχίες ασφάλειας.

Ακόμα, η μεταβλητότητα μιας έξυπνης κάρτας είναι ένα μεγάλο πλεονέκτημα. Για μας το πραγματικά μεγάλο πλεονέκτημα από τη χρησιμοποίηση μιας έξυπνης κάρτας είναι η αξιοπρόσεκτη βελτίωση στην ασφάλεια. Η κρυπτογράφηση που προστατεύει το βιομετρικό πρότυπο (και άλλες ευαίσθητες πληροφορίες) αποδυναμώθηκε από το γεγονός ότι το κλειδί αποκρυπτογράφησης έπρεπε να κρατηθεί από το κάθε αναγνώστη που αποδέχθηκε εκείνο το συμβολικό. Ο βιομετρικός/ συμβολικός αναγνώστης ήταν ικανός να αποκωδικοποιήσει και να επαληθεύσει ότι τα στοιχεία που περιλαμβάνονται ήταν αυθεντικά, αλλά το συμβολικό δεν έχει κανέναν τρόπο να επαληθεύσει ότι ο αναγνώστης που ζητά αυτές τις πληροφορίες ήταν νόμιμος.. Οι έξυπνες κάρτες έχουν την υπολογιστική ισχύ να επικυρώσουν το βιομε-

τρικό/ συμβολικό αναγνώστη προτού σταματήσουν την αποτίμηση των πληροφοριών. Αυτή η πιστοποίηση ταυτότητας χρησιμοποιεί όλα τα εργαλεία του δημόσιου κλειδιού και όταν γίνεται σωστά, προστατεύουμε τις ευαίσθητες πληροφορίες από την κοινοποίηση τους σε οποιαδήποτε αναρμόδια συσκευή.

Όπως προαναφέραμε, η έξυπνη κάρτα χαρακτηρίζεται από επεξεργασιακή και αποθηκευτική δυνατότητα, καθιστώντας τη μοναδική για πολύπλευρες εφαρμογές. Επιπρόσθετα, οι κατηγορίες καρτών στις οποίες χωρίζονται οι έξυπνες κάρτες καλύπτουν ένα ευρύ φάσμα εφαρμογών, όπου μπορεί να απαιτείται αυθεντικοποίηση ή αναγνώριση ταυτότητας του χρήστη με ακρίβεια. Έτσι. ο συνδυασμός μίας έξυπνης κάρτας με κάποια από τις παραπάνω βιομετρικές μεθόδους, προσδίδει μεγαλύτερη ασφάλεια και αξιοπιστία στο χρησιμοποιούμενο σύστημα. Συνήθως, τα περισσότερα συστήματα κάνουν χρήση κάποιας κάρτας σε συνδυασμό με μία τεχνική, όπου η ελάχιστη απαίτηση είναι η παροχή ενός προτύπου αναφοράς ή αριθμού ταυτότητας, τα οποία θα είναι αποθηκευμένα σε ένα κεντρικό σύστημα. Η αναγνώριση ταυτότητας του χρήστη σ' αυτές τις περιπτώσεις διευκολύνεται με τη χρήση μίας έξυπνης κάρτας, αφού η μεταφερσιμότητα του προτύπου επιτρέπει τη διενέργηση του ελέγχου από διάφορα τερματικά. Η έξυπνη κάρτα μπορεί να περιλαμβάνει πληροφορίες και δεδομένα για το χρήστη, που μπορούν να οδηγήσουν σε ακριβή έλεγχο της ταυτότητος του και ανάλογα ο χρήστης να αποκτήσει πρόσβαση ή όχι στην εφαρμογή που επιθυμεί.

Όμως, ακόμα και σε πολυπλοκότερες εφαρμογές, όπου απαιτείται υψηλός βαθμός ασφάλειας, οι απλές τεχνικές μπορούν να χρησιμεύσουν σαν το αρχικό και απλουστευμένο επίπεδο αυθεντικοποίησης η αναγνώρισης ταυτότητας, ενώ η χρήση συγχρόνων βιομετρικών μεθόδων σε συνδυασμό με τη χρήση μιας έξυπνης κάρτας να επιτρέπει το υψηλότερο παρεχόμενο από το σύστημα επίπεδο ασφαλείας, Με αυτόν τον τρόπο, διαχωρίζονται οι εφαρμογές στις οποίες έχει πρόσβαση ο χρήστης, προκειμένου να αποφεύγονται προσπάθειες εξαπάτησης ή αποδοχής άσχετων με τις πληροφορίες του συστήματος ατόμων .

Γιατί να μην κάνουμε τη σύγκριση του ζωντανού και βιομετρικού προτύπου πάνω στην ίδια την έξυπνη κάρτα; Ο λόγος είναι πολύ απλός. Εάν μια ενιαία έξυπνη κάρτα επρόκειτο να συμβιβαστεί από έναν αντίπαλο, έπειτα θα μπορούσε να χρησιμοποιηθεί για να κερδίσει την αναρμόδια πρόσβαση σε κάθε αναγνώστη που αρχικά εγκρίθηκε για να την πάρει. Αντιθέτως, εάν ένας βιομετρικός/ συμβολικός αναγνώστης συμβιβαστεί, έπειτα ο αντίπαλός μας θα αποκτήσει πρόσβαση μόνο σε οτιδήποτε ο αναγνώστης προστάτευε. Εν ολίγοις, είναι καλύτερο να αφεθεί η σύγκριση του ζωντανού και βιομετρικού προτύπου στον αναγνώστη .

Στη σύγκριση, τα περισσότερα άλλα βιομετρικά προϊόντα προσδιορισμού χρησιμοποιούν ένα συμβολικό για να μην πάρουν όλα τα πλεονεκτήματα του συμβολικού. Το βιομετρικό πρότυπο καταχωρείται στο σημείο, αλλά κινείται γύρω από διάφορες συναλλαγές. Το καλύτερο που θα μπορούσε να κάνει οποιαδήποτε από αυτές τις συσκευές θα ήταν να χρησιμοποιήσει ξεχωριστά το βιομετρικό σαρωτή για να συλλέξει το ζωντανό βιομετρικό και να το διαβιβάσει στον αναγνώστη των έξυπνων καρτών για τη σύγκριση του με το καταχωρημένο πρότυπο. Για να γίνει αυτό ασφαλώς, οι ζωντανές βιομετρικές πληροφορίες που διαβιβάστηκαν θα πρέπει να προστατευθούν χρησιμοποιώντας το ίδιο περίπλοκο πρωτόκολλο του δημόσιου κλειδιού, που χρησιμοποιήθηκε για να προστατεύσει τα μηνύματα που προήλθαν από τον ενσωματωμένο βιομετρικό /συμβολικό μας αναγνώστη. Αυτό στη συνέχεια, θα απαιτούσε έναν "έξυπνο" βιομετρικό αναγνώστη. Με άλλα λόγια, ο βιομετρικός αναγνώστης θα πρέπει να έχει την υπολογιστική δυνατότητα κάλυψης του ενσωματωμένου βιομετρικού/ συμβολικού μας αναγνώστη. Σε αυτή τη περίπτωση θα πρέπει, επίσης, να ενσωματώσουμε το βιομετρικό σαρωτή με το συμβολικό αναγνώστη και να κερδίσουμε με δόλο την πρόσθετη προστασία μιας ενιαίας μονάδας.

Περιληπτικά, η σύγχρονη τεχνολογία μας έχει παράσχει μια εύκολη, ασφαλή μέθοδο αναγνώρισης των ατόμων και ασφαλή πρόσβαση ενώ ταυτόχρονα προστατεύει την ιδιωτικότητα του ατόμου. Εάν οι ανάγκες της οργάνωσής σας, αυξήσουν την ασφάλεια της φυσικής πρόσβασής της, ή καλύ-

τερα τον έλεγχο πρόσβασης στους υπολογιστές και τα δίκτυα, θα υπάρχουν τώρα διάφορες οικονομικώς αποδοτικές λύσεις.

Συμπερασματικά, είναι εμφανές ότι δεν υπάρχει ιδανική επιλογή βιομετρικών συστημάτων, που να μπορούν να χρησιμοποιηθούν σε κάθε είδους εφαρμογή, αλλά η πληθώρα των βιομετρικών μεθόδων συνδυαζόμενη μάλιστα με μία έξυπνη κάρτα, παρέχει μεγαλύτερη ευελιξία στο χρήστη.

ΚΕΦΑΛΑΙΟ 7ο

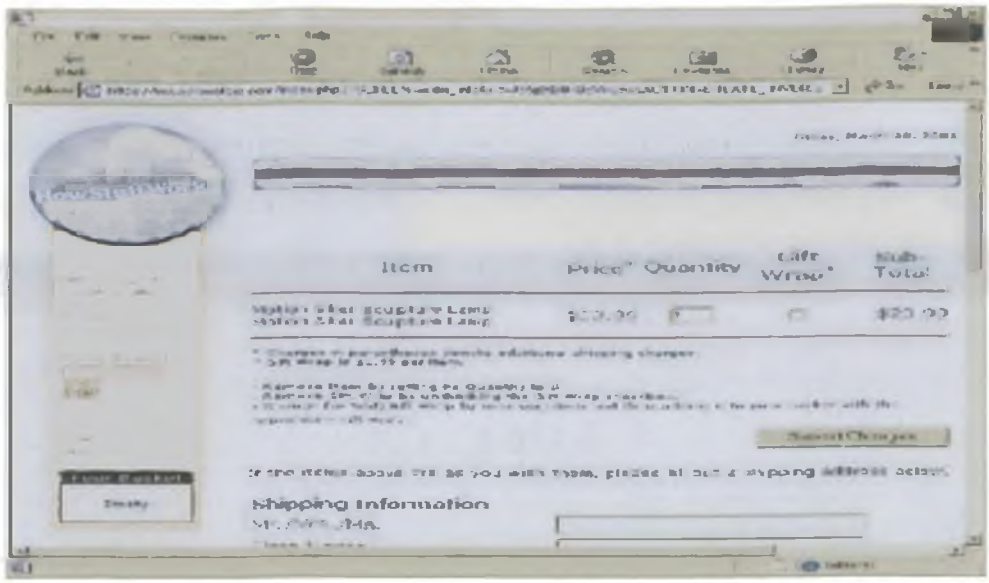
ΑΣΦΑΛΕΙΑ

1. Στοιχεία ασφάλειας

Η απίστευτη ανάπτυξη του Διαδικτύου έχει κινήσει το ενδιαφέρον των επιχειρήσεων και των καταναλωτών, καθώς και με την υπόσχεση της αλλαγής του τρόπου που ζούμε και εργαζόμαστε. Αλλά μια σημαντική ανησυχία είναι το πόσο ασφαλές είναι το Διαδίκτυο, ειδικά όταν στέλνονται ευαίσθητες πληροφορίες μέσω αυτού.

Υπάρχουν πολλές πληροφορίες που δεν θέλουμε να δουν άλλοι άνθρωποι, όπως:

- Πληροφορίες πιστωτικών καρτών
- Αριθμοί κοινωνικής ασφάλειας
- Ιδιωτική αλληλογραφία
- Προσωπικές πληροφορίες
- Ευαίσθητες πληροφορίες επιχειρήσεων
- Πληροφορίες τραπεζικών λογαριασμών .



Η ασφάλεια των πληροφοριών παρέχεται στους υπολογιστές και πέρα από το Διαδίκτυο με ποικίλες μεθόδους. Μια απλή αλλά ακριβής μέθοδος ασφάλειας είναι να κρατηθούν μόνο οι ευαίσθητες πληροφορίες στα μετακινούμενα μέσα αποθήκευσης, όπως τις δισκέτες. Αλλά οι δημοφιλέστερες μορφές ασφάλειας στηρίζονται στην κρυπτογράφηση όπου η διαδικασία της κωδικοποίησης των πληροφοριών γίνεται κατά τέτοιο τρόπο, ώστε μόνο το πρόσωπο (ή ο υπολογιστής) με το κλειδί μπορεί να τις αποκωδικοποιήσει.

2. Τι είναι ασφάλεια;

Η ασφάλεια, βασικά, είναι η προστασία κάτι πολύτιμου για να εξασφαλίσει ότι δεν θα κλαπεί, να χαθεί, ή να μεταβληθεί. Ο όρος "ασφάλεια στοιχείων" κατευθύνει μια εξαιρετικά ευρεία σειρά εφαρμογών και αγγίζει την καθημερινή ζωή όλων μας. Οι ανησυχίες σχετικά με την ασφάλεια των στοιχείων είναι έντονες κάθε στιγμή, ουσιαστικά σε κάθε συναλλαγή, οφειλόμενες στη αλματώδη πρόοδο της τεχνολογίας , από τους μετρητές χώρων στάθμευσης μέχρι την εθνική άμυνα.

Τα στοιχεία δημιουργούνται, ενημερώνονται, ανταλλάσσονται και καταχωρούνται μέσω των δικτύων. Ένα δίκτυο είναι οποιοδήποτε υπολογιστικό σύστημα όπου οι χρήστες είναι ιδιαίτερα αλληλεπιδραστικοί και αλληλοεξαρτώμενοι και εξ ορισμού, δεν είναι όλοι στην ίδια φυσική θέση. Σε

οποιοδήποτε δίκτυο, αφθονεί η ποικιλομορφία, από την άποψη των τύπων των στοιχείων αλλά και των τύπων των χρηστών . Γι' αυτό τον λόγο, ένα σύστημα ασφάλειας είναι σημαντικό να διατηρεί λειτουργίες υπολογισμού και δικτύων, να κρατά μυστικά τα ευαίσθητα στοιχεία ή να διατηρεί απλά την ασφάλεια των εργαζομένων. Οποιαδήποτε επιχείρηση μπορεί να παρέχει ένα παράδειγμα αυτών των πολλαπλών ανησυχιών ασφάλειας.

Η ασφάλεια πληροφοριών είναι μια εφαρμογή από μέτρα που εξασφαλίζουν την ασφάλεια και την ιδιωτικότητα των στοιχείων με τη διαχείριση της αποθήκευση τους και της διανομή τους. Η ασφάλεια πληροφοριών έχει τεχνικές και κοινωνικές επιπτώσεις. Η πρώτη, για να παρέχει μέτρα ασφάλειας εξετάζει απλά με την ερώτηση "πώς" και "πόσο" είναι το λογικό κόστος. Η δεύτερη επιτίθεται με το ζήτημα της ατομικής ελευθερίας, τις δημόσιες ανησυχίες, τα νομικά πρότυπα και πως τους καλύπτεται η ανάγκη για ιδιωτικότητα. Αυτή η συζήτηση καλύπτει μια σειρά από επιλογές που έχουν ξεδιπλωθεί από τους διευθυντές επιχειρήσεων, τους αρμόδιους για το σχεδιασμό συστημάτων και τους προγραμματιστές που θα συμβάλουν στην τελική στρατηγική ασφάλειας. Η τελική επιλογή στηρίζεται στο σχεδιαστή και τον εκδότη του συστήματος.

Στην εφαρμογή ενός συστήματος ασφάλειας, όλα τα δίκτυα δεδομένων εξετάζουν τα ακόλουθα βασικά στοιχεία:

1. **Υλικό:** συμπεριλαμβάνονται οι κεντρικοί υπολογιστές, οι εφεδρικές συσκευές μαζικής αποθήκευσης, τα κανάλια και οι γραμμές επικοινωνίας, τα συμβολικά υλικού (έξυπνες κάρτες) και απομακρυσμένες τοποθετημένες συσκευές (π.χ. αδύναμοι χρήστες ή συσκευές Διαδικτύου) που εξυπηρετούν ως μέσο διασύνδεσης μεταξύ των χρηστών και των υπολογιστών.
2. **Λογισμικό:** συμπεριλαμβάνονται τα λειτουργικά συστήματα, τα συστήματα διαχείρισης της βάσης δεδομένων, και η εφαρμογή προγραμμάτων επικοινωνίας και ασφάλειας.
3. **Δεδομένα:** συμπεριλαμβάνονται βάσεις δεδομένων που περιέχουν πληροφορίες σχετικές με τον πελάτη.

4. **Προσωπικό:** ενεργεί ως δημιουργός ή/ και χρήστης των δεδομένων, επαγγελματικό προσωπικό, προσωπικό γραφείου, διοικητικό προσωπικό και προσωπικό υπολογιστών.

3. Οι μηχανισμοί της ασφάλειας δεδομένων

Δουλεύοντας με τα πιο πάνω στοιχεία, λειτουργεί ένα αποτελεσματικό σύστημα ασφάλειας των δεδομένων με τους ακόλουθους βασικούς μηχανισμούς:

1. **Ακεραιότητα δεδομένων(integrity)**: αυτός ο μηχανισμός εξασφαλίζει ότι τα δεδομένα δεν θα χαθούν ή θα αλλοιωθούν όταν θα σταλούν σε σας(δηλ. Έχουν φτάσει άθικτα τα δεδομένα;).
2. **Πιστοποίηση ταυτότητας(authentication):** αυτό αποδεικνύει τις ταυτότητες των χρηστών ή του συστήματος. (Είναι σωστά τα δεδομένα και προέρχονται από το σωστό πρόσωπο;)
3. **Μη απαρνησιμότητα(Non-Repudiation):** απαγορεύει σε ένα οποιοδήποτε άτομο να απαρνηθεί τη συμμετοχή του στη δοσμένη συναλλαγή. (Μπορώ να επιβεβαιώσω την παραλαβή των στοιχείων και τη ταυτότητα του αποστολέα;)
4. **Εμπιστευτικότητα (confidentiality):** εξασφαλίζει πρόσβαση στα δεδομένα μόνο στους πομπούς και τους δέκτες. Αυτό γίνεται χαρακτηριστικά, με την υιοθέτηση μιας ή περισσότερων τεχνικών κρυπτογράφησης για την εξασφάλιση των δεδομένων σας. (Μπορώ να κρατήσω μυστικά αυτά τα δεδομένα;)
5. **Διαθεσιμότητα (availability):** τα συστήματα ασφαλείας καθίστανται άμεσα προσπελάσιμα σε κάθε εξουσιοδοτημένο χρήστη.
6. **Έγκριση και αποστολή:** μπορεί να τεθούν και να διαχειριστούν προνόμια πρόσβασης για πρόσθετους χρήστες και ομάδες. (Μπορώ να μοιραστώ ακίνδυνα αυτό τα δεδομένα εάν το επιλέξω;)
7. **Έλεγχος ασφάλειας και καταγραφή:** παρέχει ένα σταθερό όργανο παρακολούθησης και ένα ανιχνευτή λαθών της λειτουργίας του συστήματος ασφάλειας. (Μπορώ να ελέγξω ότι το σύστημα εργάζεται;)

8. **Διαχείριση :** επιτρέπει την διαχείριση του συστήματος ασφάλειάς σας. (Μπορώ να διαχειριστώ ενεργά το σύστημα;)

Πιστοποίηση ταυτότητας

Η πιστοποίηση ταυτότητας διαδραματίζει έναν κρίσιμο ρόλο στις διαδικασίες ασφάλειας, αφού επιθεωρεί, και μετά επιβεβαιώνει, τη καταλληλότητα της ταυτότητας των δεδομένων των ανθρώπων που λαμβάνουν μέρος σε μια συναλλαγή. Στην πιστοποίηση ταυτότητας, μια ψηφιακή υπογραφή ελέγχει τα δεδομένα στην αρχική τους σύνταξή με την παραγωγή μιας ταυτότητας που μπορεί να ελεγχθεί αμοιβαία από όλα τα συμβαλλόμενα μέρη που λαμβάνουν μέρος στη συναλλαγή. Ένας κρυπτογραφικός hash αλγόριθμος παράγει μια ψηφιακή υπογραφή.

Όλες οι πολιτικές ασφάλειας, οι κρυπτογραφημένες περίοδοι επικοινωνίας και οι ασφαλείς μεταφορές στοιχείων είναι ασήμαντης αξίας, εάν το βασικό σχέδιο πιστοποίησης ταυτότητας είναι αδύνατο. Σήμερα για παράδειγμα, τα αρχεία υγειονομικής περίθαλψης είναι προστατευμένα βασισμένος σε έναν συνδυασμό του ονόματος ενός προσώπου, διεύθυνσης, γένους, του SSN (κοινωνικός αριθμός ασφάλειας), τηλεφωνικού αριθμού, ασφαλιστικού αριθμού υγείας, ημερομηνίας γέννησης, εργοδότη και σχέσεων σε άλλα οικογενειακά μέλη. Αυτή η χρήση των προσωπικών πληροφοριών εμφανίζει την έλλειψη λάμψης προστασίας ιδιωτικότητας στη θέση σήμερα, ιδιαίτερα εάν παίρνουμε το εξεταζόμενο παράδειγμα του HIV όπου στα άτομα ανατίθεται ένας μοναδικός αριθμός για να βεβαιώσουν την ανωνυμία. Μια παρόμοια προσέγγιση πρέπει να ληφθεί για να προστατεύσει όλα τις συναλλαγές και τα ιατρικά αρχεία, έτσι, ώστε ένα πρόσωπο να μην μπορεί να ταιριάξει βασιζόμενο στις προσωπικές πληροφορίες τους.

Ο βασικός στόχος ενός βασισμένου στο υλικό σχεδίου πιστοποίησης ταυτότητας είναι να εξεταστεί αυτό το ζήτημα. Η βιομετρική, οι έξυπνα κάρτες και τα κλειδιά φαίνονται να είναι οι τρεις, πολύ συχνά συζητημένες προαιρετικές δυνατότητες στο χώρο πιστοποίησης ταυτότητας υλικού.

Ακεραιότητα δεδομένων

Αναφέρεται στη λειτουργία που ελέγχει τα χαρακτηριστικά ενός εγγράφου και μιας συναλλαγής. Τα χαρακτηριστικά και των δύο επιθεωρούνται και επιβεβαιώνονται για την ανάλογη και σωστή έγκριση. Η ακεραιότητα των δεδομένων επιτυγχάνεται με το ηλεκτρονικό σύστημα κρυπτογραφίας που προδιαγράφει μια μοναδική ταυτότητα στα δεδομένα, όπως ένα δακτυλικό αποτύπωμα. Οποιαδήποτε προσπάθεια να αλλαχτεί αυτή η ταυτότητα λαμβάνεται σήμα για την αλλαγή και σταματά οποιαδήποτε ενέργεια.

Μη αποδεκτικότητα

Αναφέρεται στη δυνατότητα μιας συναλλαγής να είναι μη αποδεκτή ή άκυρη με την ενσωμάτωση μιας ψηφιακής υπογραφής, που ένα τρίτο μέρος μπορεί να την επαληθεύσει ως σωστή. Παρόμοιο στην έννοια με το εγκεγραμμένο ηλεκτρονικό ταχυδρομείο, ο παραλήπτης διασκευαστής των δεδομένων, ελέγχει την ψηφιακή υπογραφή και τις συγκρίνει για να δει ότι ταιριάζουν.

Έλεγχος ασφάλειας και καταγραφή.

Αναφέρεται στην ανεξάρτητη εξέταση και στη καταγραφή αρχείων και δραστηριοτήτων για να εξασφαλίσει τη συμμόρφωση με τους καθιερωμένους ελέγχους, την πολιτική, και τις λειτουργικές διαδικασίες, προκειμένου να προτείνει οποιεσδήποτε υποδειγματικές αλλαγές στον έλεγχο, την πολιτική ή τις διαδικασίες.

Διαχείριση.

Πρόκειται για την επίβλεψη και το σχεδιασμό των στοιχείων και μηχανισμών που συζητιούνται πιο πάνω και πιο κάτω.

Εμπιστευτικότητα

Αφορά τη χρήση της κρυπτογράφησης προκειμένου να προστατευθούν οι πληροφορίες από την αναρμόδια κοινοποίηση τους. Το μη κωδικοποιημένο κείμενο είναι στραμμένο στο κρυπτογράφημα μέσω ενός αλγορίθμου, μετά αποκρυπτογραφείται πίσω στο πηγαίο κώδικα, χρησιμοποιώντας την ίδια μέθοδο.

Το σύστημα κρυπτογραφία είναι η μέθοδος μετατροπής των δεδομένων από μια ανθρώπινη αναγνώσιμη μορφή σε μια τροποποιημένη μορφή, και έπειτα πίσω στην αρχική αναγνώσιμη μορφή τους, για να καταστήσει δύσκολη την κάθε αναρμόδια πρόσβαση. Το σύστημα κρυπτογραφίας χρησιμοποιείται στους ακόλουθους τρόπους:

- εξασφαλίζει ιδιωτικότητα στα δεδομένα, με την κρυπτογράφηση τους.
- εξασφαλίζει ακεραιότητα στα δεδομένα, αναγνωρίζοντας εάν τα δεδομένα έχουν παραποιηθεί με έναν αναρμόδιο τρόπο .
- εξασφαλίζει μοναδικότητα στα δεδομένα, με τον έλεγχο ότι τα δεδομένα είναι "αυθεντικά", και όχι ένα "αντίγραφο" "του αυθεντικού". Ο πομπός συνδέει ένα μοναδικό προσδιοριστή με τα "αυθεντικά" δεδομένα. Αυτός ο μοναδικός προσδιοριστής, έπειτα, ελέγχεται από τον δέκτη των δεδομένων.

4. Έξυπνες κάρτες για την ασφάλεια των δεδομένων

Όπως ο εκδότη καρτών, πρέπει να καθορίσετε όλες τις παραμέτρους για την ασφάλεια της κάρτας και των δεδομένων της. Υπάρχουν δύο μέθοδοι που χρησιμοποιούν κάρτες για την ασφάλεια των δεδομένων του συστήματος, οι βασισμένοι στο κεντρικό υπολογιστή και οι βασισμένοι στη κάρτα.

α) Σύστημα ασφάλειας βασισμένο στο κεντρικό υπολογιστή

Ένα σύστημα βασισμένο στο κεντρικό υπολογιστή επεξεργάζεται την κάρτα σαν ένα απλό κομιστή δεδομένων. Εξαιτίας αυτού , οι άμεσες κάρτες μνήμης μπορούν να χρησιμοποιηθούν πολύ επικερδώς, για πολλά συστή-

ματα. Όλη η προστασία των δεδομένων παρέχεται από τον κεντρικό υπολογιστή. Η κάρτα δεδομένων μπορεί να έχει κρυπτογραφηθεί αλλά η μεταφορά τους στον κεντρικό υπολογιστή μπορεί ακόμα να είναι ευαίσθητη σε επιθέσεις.

Μια κοινή μέθοδος αύξησης της ασφάλειας είναι να γραφτεί σ' ένα μην κρυπτογραφημένο κείμενο, ένα κλειδί που συνήθως περιέχει μια ημερομηνία ή/ και κατά τη διάρκεια κάποιας στιγμής μαζί με μια μυστική αναφορά σε ένα σύνολο κλειδιών στον κεντρικό υπολογιστή. Με αυτό το τρόπο κάθε μεταφορά είναι διαφορετική. Αλλά τα μέρη των κλειδιών βρίσκονται στη διάθεση των χάκερ που τα αναλύουν. Αυτή η ασφάλεια μπορεί να αυξηθεί με την χρήση των έξυπνων καρτών μνήμης που υιοθετούν έναν μηχανισμό κωδικού πρόσβασης για να αποτρέψουν κάποια αναρμόδια ανάγνωση των δεδομένων. Δυστυχώς οι κωδικοί πρόσβασης μπορούν να απορροφηθούν ανεμπόδιστα. Η πρόσβαση είναι έπειτα πιθανή και στη βασική μνήμη. Αυτές οι μεθοδολογίες χρησιμοποιούνται συχνά όταν ένα δίκτυο μπορεί να επεξεργασθεί μεθοδικά τα δεδομένα. Μπορεί να συγκρίνει τις τιμές και τη χρήση των καρτών και να παράγει έναν κατάλογο με τα προβλήματα των καρτών.

β) Σύστημα ασφαλείας βασισμένο στη κάρτα

Αυτά τα συστήματα είναι χαρακτηριστικοί μικροεπεξεργαστές που βασίζονται στη κάρτα. Μια κάρτα, ή ένα σύστημα που βασίζεται στο συμβολικό μεταχειρίζεται μια κάρτα σαν μια ενεργό συσκευή υπολογισμού. Η αλληλεπίδραση μεταξύ του κεντρικού υπολογιστή και της κάρτας μπορεί να είναι μια σειρά από βήματα που καθορίζουν εάν η κάρτα είναι εξουσιοδοτημένη για να χρησιμοποιηθεί στο σύστημα. Η διαδικασία ελέγχει επίσης εάν μπορεί να προσδιοριστεί ο χρήστης , να επικυρωθεί και εάν η κάρτα παρουσιάζει τα κατάλληλα αποδεικτικά για να διεξαχθεί μια συναλλαγή. Η ίδια η κάρτα μπορεί επίσης να απαιτεί το ίδιο πράγμα από τον κεντρικό υπολογιστή πριν προχωρήσει σε μια συναλλαγή. Η πρόσβαση σε συγκεκριμένες πληροφορίες της κάρτας ελέγχεται από Α) το εσωτερικό λειτουργικό

σύστημα της κάρτας Β) τις προετοιμασμένες δικαιοδοσίες που τίθενται από τον εκδότη καρτών σχετικά με τους όρους των αρχείων.

5. Παραδείγματα καρτών κρυπτογράφησης

Οι έξυπνες κάρτες είναι η αναδυόμενη τάση ταυτοποίησης που βασίζεται στα σημεία επειδή ενισχύουν τη δύναμη της ασφάλειας του κρυπτογραφημένου πακέτου του λογισμικού, όπως το SSL**. Με την προσθήκη της ασφάλειας των έξυπνων καρτών στο σύστημα σας, οι λειτουργίες ασφάλειας κρίσιμων αποστολών όπως το κλειδί αποθήκευσης, η κρυπτογράφηση του δημόσιου κλειδιού και οι ψηφιακές υπογραφές μετακινούνται από τον μη ασφαλή υπολογιστή σας και εκτελούνται στην ίδια την έξυπνη κάρτα με σημαντικά μεγαλύτερη ασφάλεια και φορητότητα. Είτε υιοθετείτε για να επικυρώσει τους χρήστες είτε για να ενδυναμώσει τη λειτουργικότητα των εφαρμογών, υπάρχει ένας αναγνώστης έξυπνων καρτών SSP ακριβώς κατάλληλος για το σύστημα σας.

Οι αναγνώστες έξυπνων καρτών SSP, που είναι συνδεδεμένοι με το Net Sign μπορούν να εκτελέσουν ποικίλες λειτουργίες, που κυμαίνονται από την έναρξη της αυτοματοποιημένης εφαρμογής, με την εισαγωγή των έξυπνων καρτών, μέχρι την αυτοματοποιημένη έξοδο από το σύστημα με την αφαίρεση των έξυπνων καρτών.

Οι λύσεις του SSP υποστηρίζουν τη βιομηχανία που ηγείται κάποιων ικανών έξυπνων καρτών RSA των1024 bit που σχεδιάστηκαν από τον Schlumberger, καθώς, επίσης, και άλλες κρυπτογραφικές έξυπνες κάρτες που είναι συμμορφώσιμες με τους αναγνώστες έξυπνων καρτών, σύμφωνα με τον διεθνή οργανισμό προτύπων (ISO 7816). Με την εξελιξιμότητα τόσο στη τιμή όσο και στην απόδοση, οι αναγνώστες SSP προσφέρουν ποικίλα επίπεδα ασφάλειας που οδηγούνται από τη μεμονωμένη ζήτηση των πελατών.

MONIKER

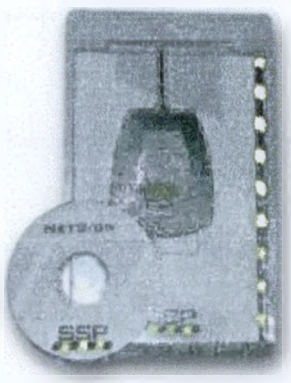
Η Moniker(FORTEZZA) crypto κάρτα παρέχει σημαντική απόδοση και αποθήκευση πιστοποιητικών/ κλειδιών σε ένα έμπιστο και εύχρηστο σημείο.

Σχεδιασμένο από την εθνική αντιπροσωπεία ασφάλειας (NSA) για να παραδώσει κρυπτογράφηση υψηλής απόδοσης και ψηφιακές υπηρεσίες χρησιμοποιώντας τα πρότυπα βιομηχανίας, το Moniker ενσωματώνει μια ολοκληρωμένη γεννήτρια τυχαίων αριθμών, ένα οριακό πραγματικού χρόνου ρολόι και μια αποθήκη μέχρι και 27 ψηφιακών πιστοποιητικών.

Η κάρτα Moniker παρέχει δυο ισχυρούς παράγοντες πιστοποίησης ταυτότητας(ταυτοποίησης-συθεντικοποίησης) από τις απαιτήσεις του χρήστη ή του διοικητή, προκειμένου να εισάγουν τον προσωπικό αριθμό αναγνώρισης τους(PIN). Η ασφάλεια ενισχύεται επειδή τα PINs κρυπτογραφούνται και καταχωρούνται στην κάρτα. Η crypto κάρτα Moniker αυτόματα "κλειδώνεται " μετά από κάποιο προκαθορισμένο αριθμό ανεπιτυχών προσπαθειών εισαγωγής του PIN των χρηστών, και όλο το ευαίσθητο περιεχόμενο των καρτών μηδενίζεται (σβήνεται) μετά από τις διαδοχικές ανεπιτυχείς προσπάθειες των διαχειριστών του PIN.

NetSign.

Τα επιχειρησιακά περιβάλλοντα Διαδικτύου αναγνωρίζουν την ζωτικής σημασίας ανάγκη να επικυρωθεί και να εξασφαλιστεί η ακεραιότητα των επιχειρησιακών συναλλαγών και επικοινωνιών. Αν οι επιχειρήσεις του



Διαδικτύου είναι χτισμένες επάνω σ' ένα ανοικτό δίκτυο, όπου οι επικοινωνίες περνούν απροστάτευτες, οι μεταφορές παρεμποδίζονται και οι συναλλαγές πλαστογραφούνται. Τότε αυτή η επιχείρηση θα είναι μια δαπανηρή επιχείρηση. Το SSP NetSign χρησιμοποιεί το Διαδίκτυο για τις επιχειρήσεις παρέχοντας ασφαλείς μεταφορές, προστασία των επικοινωνιών, προστασία των

συναλλαγών και την απόδειξη της ταυτότητας κάποιου σε ένα δικτυωμένο περιβάλλον.

Το SSP NetSign παραδίδει ένα έτοιμο προς χρήση πακέτο, το οποίο ενσωματώνει εύκολα τις έξυπνες κάρτες, οδηγώντας τα πακέτα των browsers και του ηλεκτρονικού ταχυδρομείου, για να εξασφαλίσει τις επικοινωνίες του Διαδικτύου, το εμπόριο, τη πρόσβαση στο ενδογενές/ εξωγενές δίκτυο (intranet/extranet), και να προστατεύσει τα desktops των χρηστών από την αναρμόδια πρόσβαση.

Οι κρίσιμης αποστολής λειτουργίες της ασφάλειας, όπως η αποθήκευση του ιδιωτικού κλειδιού και οι ψηφιακές υπογραφές, εκτελούνται στην έξυπνη κάρτα για μεγαλύτερη ασφάλεια. Το NetSign υποστηρίζει ένα ανοικτό σύστημα , που βασίζεται στα πλαίσια των προτύπων, για να παρέχει την ευελιξία που απαιτείται από τις οργανώσεις σήμερα.

** **Το SSL** είναι το ασφαλές στρώμα υποδοχής, το οποίο είναι ένα στρώμα πρωτοκόλλου που μπορεί να τοποθετηθεί μεταξύ ενός προσανατολισμένου προς τη σύνδεση, αξιόπιστου πρωτοκόλλου του στρώματος δικτύου (π.χ TCP/ IP) και του πρωτοκόλλου του στρώματος εφαρμογής (π.χ HTTP).

Η SSL επιτρέπει την ασφαλή επικοινωνία μεταξύ του πελάτη και κεντρικού υπολογιστή(server), με την άδεια της αμοιβαίας επικύρωσης, της ακεραιότητας και της κρυπτογράφησης για μυστικότητα. Το πρωτόκολλο σχεδιάζεται για να υποστηρίξει μια σειρά επιλογών για τους αλγόριθμους που χρησιμοποιούνται στο σύστημα κρυπτογράφησης. Αυτό επιτρέπει την επιλογή αλγορίθμων για τον συγκεκριμένο server καθώς επίσης, επιτρέπει στο πρωτόκολλο να εκμεταλλευτεί τους νέους αλγορίθμους.

Η SSL χρησιμοποιεί ένα συμβατικό αλγόριθμο του συστήματος κρυπτογράφησης(συμμετρικό σύστημα κρυπτογράφησης). Επιτρέπει στις εφαρμογές των πελατών να επικοινωνήσουν με τέτοιο τρόπο ώστε να μην μπορεί κάποιος να κρυφακούσει. Ο server επικυρώνεται πάντα ενώ οι πελάτες επικυρώνονται προαιρετικά.

6. Επικύρωση του κατόχου της κάρτας-PIN

6.1 Κωδικοί και αριθμοί PIN:

Η εισαγωγή και χρήση προσωπικών κωδικών ή αριθμών αποτελεί το συνηθέστερο τρόπο αυθεντικοποίησης και ταυτοποίησης ατόμων τα τελευταία χρόνια. Οι κωδικοί, όμως, αφενός μεν δεν συνίστανται για εφαρμογές υψηλής ασφαλείας, αφού πολύ συχνά οι χρήστες ξεχνάνε τον κωδικό τους ή τον γράφουνε σε χαρτί ή χρησιμοποιούν λέξεις, αφετέρου δε θεωρείται εύκολο να προβλεφθούν, με αποτέλεσμα να μειώνεται η αξιοπιστία και η ασφάλεια του συστήματος.

Καλύτερα αποτελέσματα επιφέρει ο συνδυασμός των κωδικών με κάποια μορφή κουπονιού (token) ή άλλης γεννήτριας τύπου πρόκλησης-απόκρισης (challenge-response). Όμως, και με αυτόν τον τρόπο, απομακρύνεται το μεγαλύτερο πλεονέκτημα που διαθέτουν οι κωδικοί, δηλαδή το χαμηλό οικονομικό κόστος, ενώ επιπλέον αποκλείεται η μοναδικότητα του κώδικα.

Από την άλλη μεριά, οι προσωπικοί αριθμοί ταυτοποίησης (Personal Identification Numbers-PINs) είναι ουσιαστικά μία απλή μορφή κωδικών, αφού συνήθως αποτελούνται από τέσσερα έως έξη ψηφία, τα οποία εισάγονται με τη βοήθεια κατάλληλου πληκτρολογίου. Μάλιστα, θεωρείται ότι οι χρήστες είναι περισσότερο εξοικειωμένοι με τη χρήση των παραπάνω κωδικών από τις τραπεζικές κάρτες, εφόσον οι παραπάνω κωδικοί εμφανίζουν περιορισμένο εύρος σφαλμάτων και απαιτούν απλή μορφή λογισμικού, χαρακτηριστικά δηλαδή που τα καθιστούν ευκολόχρηστα μέσα ταυτοποίησης σε βιομετρικά συστήματα.

Παρ' όλα αυτά, εμφανίζεται πληθώρα προβλημάτων στη χρήση τους λόγω δυσκολίας από πολλούς χρήστες στην απομνημόνευση των ψηφίων αυτών, ειδικά όταν χρησιμοποιούνται πολλές κάρτες με διαφορετικά PIN, ή ακόμα και στην αλλαγή του αριθμού PIN, με αποτέλεσμα και σ' αυτήν τη μέθοδο να μειώνεται η αξιοπιστία και η ασφάλεια που παρέχει το σύστημα. Γι' αυτό, και η χρήση τους στα τελευταία συστήματα που έχουν σχεδιασθεί, περιορίζεται σε δευτερεύοντα επίπεδα πρόσβασης των χρηστών στο σύ-

στημα, με καθοριστικό στάδιο την αναγνώριση της κάρτας από την αντίστοιχη διάταξη.

Οι έξυπνες κάρτες δε βασίζονται συνήθως σε κάποια ευφυή μέθοδο μεταφοράς κι αποθήκευσης των δεδομένων, αλλά τις περισσότερες φορές απαιτούν επαλήθευση του χρήστη. Η επιβεβαίωση της ταυτότητας του χρήστη συνήθως πραγματοποιείται με ξεχωριστή μέθοδο, όπως με την επαλήθευση προσωπικών λεπτομερειών του χρήστη διαφόρων βιομετρικών του στοιχείων ή απλά την εισαγωγή κάποιου προσωπικού αριθμού ταυτοποίησης <Personal Identification Number -PIN>.

Ενώ οι κατάλληλα σχεδιασμένες έξυπνες κάρτες δεν μπορούν στην πράξη να πλαστογραφηθούν, λίγη πρόοδος έχει σημειωθεί για να εξασφαλίσει ότι είναι ο αναγνωρισμένος κάτοχος κάρτας εκείνος που χρησιμοποιεί τη γνήσια κάρτα. Αυτό το πρόβλημα είναι ιδιαίτερα οξύ στον ηλεκτρονικό κόσμο, όπου οι καταναλωτές πραγματοποιούν συναλλαγές, όπου στα τερματικά των επιχειρήσεων δε υπάρχουν χειριστές ικανοί να διευθύνουν τις επαρκείς ρουτίνες επαλήθευσης.

Η πιο κοινή μέθοδος που χρησιμοποιείται για την επαλήθευση του κατόχου της κάρτας είναι αυτή τη στιγμή, να δοθεί στον κάτοχο ένα PIN (προσωπικός αριθμός αναγνώρισης) που πρέπει να θυμάται: ο κάτοχος κάρτας πρέπει να δακτυλογραφήσει το PIN μετά από κάθε αίτημα ή ίσως μόνο μια φορά ανά σύνοδο (π.χ. όταν παρεμβάλλεται η κάρτα στη συσκευή ανάγνωσης). Το PIN, εντούτοις, έχει διάφορα μειονεκτήματα, συμπεριλαμβανομένου του κινδύνου κλοπής ή κακής χρήσης. Η μόνη αληθινά αποτελεσματική μέθοδος επαλήθευσης του κατόχου κάρτας είναι η μέτρηση των φυσικών μοναδικών χαρακτηριστικών ενός ατομικού και ανίκανου για ψεύτικη απάντηση ή κατάχρηση.

6.2. Έλεγχος πρόσβασης

Το σύστημα ελέγχου της πρόσβασης στις έξυπνες κάρτες καλύπτει κυρίως την πρόσβαση των αρχείων. Κάθε αρχείο συνδέεται με μια επιγραφή που δείχνει τους όρους πρόσβασης ή τις απαιτήσεις του αρχείου και της πα-

ρούσας κατάστασης. Η θεμελιώδης αρχή του ελέγχου πρόσβασης είναι βασισμένη στη σωστή παρουσίαση των αριθμών PIN και της διαχείρισής τους.

6.2.1 Τα επίπεδα των όρων πρόσβασης

Πρώτιστα, οι όροι πρόσβασης ενός αρχείου μπορούν να καθοριστούν στα ακόλουθα πέντε επίπεδα. Μερικά από τα λειτουργικά συστήματα μπορούν να προσφέρουν περισσότερα από αυτά που εξαρτιόνται από την εφαρμογή που παρέχουν.

- Always (ALW): Η πρόσβαση του αρχείου μπορεί να εκτελεσθεί χωρίς κανένα περιορισμό.
- Επαλήθευση κατόχου κάρτας 1 (CHV1): Η πρόσβαση είναι δυνατή μόνο όταν η αξία CHV1 παρουσιάζεται έγκυρη.
- Επαλήθευση κατόχου κάρτας 2 (CHV2): Η πρόσβαση είναι δυνατή μόνο όταν παρουσιάζεται η αξία CHV2 έγκυρη.
- Administrative (ADM): Η κατανομή αυτών των επιπέδων και οι αντίστοιχες απαιτήσεις για την εκπλήρωσή τους είναι ευθύνη της κατάλληλης διοικητικής αρχής.
- Never (NEV): Η πρόσβαση του αρχείου είναι απαγορευμένη.

Αυτά τα επίπεδα προϋποθέσεων δεν είναι ιεραρχικά. Παραδείγματος χάριν, η σωστή παρουσίαση του CHV2 δεν σημαίνει ότι η πρόσβαση του αρχείου επιτρέπεται και η οποία απαιτεί την παρουσίαση CHV1. Κατά τη διάρκεια της λειτουργίας, οι αντίστοιχες απαιτήσεις πρέπει να ικανοποιηθούν πριν από την επιλογή του αρχείου. Παραδείγματος χάριν, η σωστή CHV1 αξία πρέπει να παρουσιαστεί εάν είναι όρος πρόσβασης ενός αρχείου.

6.2.2. Παρουσιάσεις PIN

Τα PIN αποθηκεύονται κανονικά στα ξεχωριστά στοιχειώδη αρχεία, το EFCHV1 και το EFCHV2 παραδείγματος χάριν. Η χρήση των όρων πρόσβασης σε εκείνα τα αρχεία μπορεί να αποτρέψει το PIN από την αλλαγή. Το PIN μπορεί να αλλάξει με την έκδοση της οδηγίας της PIN αλλαγής

μαζί με το νέο και το παλαιό PIN. Εντούτοις, για τα περισσότερα από τα λειτουργικά συστήματα έξυπνων καρτών, το αντίστοιχο PIN θα ακυρωθεί ή θα μπλοκαριστεί όταν ένας σταθερός αριθμός από άκυρα PINs παρουσιάζεται. Ο αριθμός των φορών ποικίλει στα διάφορα συστήματα.

Αυτήν τη στιγμή, όλα τα αρχεία θεωρούν ότι το PIN θα εμποδίσει την πρόσβαση. Η απελευθέρωση πραγματοποιείται με τη γνώση του σωστού PIN και με ένα συγκεκριμένο ξεμπλοκάρισμα του PIN που αποθηκεύεται στην κάρτα. Ακόμα, εάν ένα άκυρο ξεμπλοκάρισμα του PIN παρουσιάζεται και μέχρι έναν συγκεκριμένο αριθμό φορών, η απελευθέρωση του PIN, επίσης, εμποδίζεται. Κατόπιν και το PIN και το ξεμπλοκάρισμα του PIN θα ακυρωθεί και δε θα μπορεί πλέον να αποκατασταθεί. Αυτό καλείται αμετάκλητη παρεμπόδιση. Μερικά από τα συστήματα μπορούν ακόμη και να ακυρώσουν ολόκληρη την κάρτα προκειμένου να αποτραπούν οι περαιτέρω επιθέσεις.

6.2.3. Διαχείριση του PIN

Για να επιτύχουν την προστασία και το μπλοκάρισμα του PIN, δύο μετρητές πρέπει να εφαρμοστούν για κάθε έναν από τους αριθμούς επαλήθευσης του κατόχου της κάρτας (CHVs). Οι μετρητές αποτελούνται κατά τέτοιο τρόπο, ώστε οποιαδήποτε πιθανά λάθη, τα οποία θα μπορούσαν να έχουν επιπτώσεις στον έλεγχο της πρόσβασης στην κάρτα, να αποφευχθούν. Υπάρχουν τρία καθεστώτα στη διαχείριση του PIN που περιγράφονται κατωτέρω.

1. Το PIN έχει παρουσιαστεί:

Τα αρχεία ή οι λειτουργίες που διοργανώνουν την παρουσίαση του PIN ως προϋπόθεση ή όρο μπορούν να πραγματοποιηθούν. Κάθε φορά που παρουσιάζεται σωστά το PIN, ο μετρητής PIN θα επαναρυθμιστεί στο μέγιστο αριθμό δοκιμών, τρεις φορές παραδείγματος χάριν.

2. Το PIN δεν έχει παρουσιαστεί ή παρουσιάστηκε ανακριβώς:

Ο μετρητής PIN θα μειώνεται κατά ένα αφότου παρουσιαστεί κάθε ανακριβή PIN. Όλες οι διαδικασίες ή οι οδηγίες που απαιτούν την παρουσίαση του PIN θα ακυρωθούν. Εάν ο μετρητής PIN φθάσει στο μηδέν, η επόμενη παρουσίαση του PIN θα εμποδιστεί.

3. Το PIN εμποδίζεται:

Σε αυτό το σημείο, όλες οι διαδικασίες απαιτούν την παρουσίαση του PIN, ενώ, ακόμη και η ίδια η οδηγία παρουσίασης του PIN εμποδίζεται. Οι οδηγίες απελευθέρωσης του PIN πρέπει να πραγματοποιηθούν. Εάν παρουσιαστεί η σωστή απελευθέρωση του PIN, ο μετρητής PIN θα επαναρυθμιστεί στο μέγιστο αριθμό δοκιμών και θα υποστηριχτεί στο πρώτο καθεστώς. Εντούτοις, εάν παρουσιαστεί άκυρη απελευθέρωση του PIN, ο μετρητής PIN θα μειωθεί κατά ένα και όταν φθάσει στο μηδέν, το PIN δεν μπορεί να απελευθερωθεί ξανά.

Συνοψίζοντας, η δομή των αρχείων και ο έλεγχος της πρόσβασης που παρέχεται στις έξυπνες κάρτες και η αποθήκευση των δεδομένων στην κάρτα μπορούν να προστατευθούν είτε ατομικά, με τον καθορισμό των όρων πρόσβασης στην επικεφαλίδα κάθε αρχείου είτε ιεραρχικά με την ομαδοποίηση των αρχείων, στο πλαίσιο ενός ενιαίου dedicated αρχείου (DF), με τους όρους πρόσβασης που τίθενται σε αυτό. Επιπλέον, η αμετάκλητη παρεμπόδιση δίνει τη μέγιστη προστασία στην κάρτα έτσι ώστε η αυθαίρετη είσοδος να είναι αδύνατη.

7. Εξακρίβωση γνησιότητας και Ψηφιακές Υπογραφές

Στον πραγματικό κόσμο και πιο συγκεκριμένα στις τράπεζες, παρατηρούμε ότι οι άνθρωποι κάνουν διάκριση ανάμεσα στα πρωτότυπα και στα αντίγραφα Μια συμβατική υπογραφή χρησιμοποιείται ως γνωστόν για την απόδειξη της γνησιότητας ενός εγγράφου. Ειδικότερα, η υπογραφή αποτελεί μαρτυρία της εγκυρότητας του υπογεγραμμένου εγγράφου έτσι ώστε ο υπογράφων να μη μπορεί να το απαρνηθεί.

Στη σημερινή εποχή των δικτύων υπολογιστών, όπου πλήθος μηνυμάτων ανταλλάσσονται μεταξύ των οργανισμών καθίσταται αναγκαία

η χρησιμοποίηση ενός ηλεκτρονικού ισοδύναμου της συμβατικής υπογραφής, δηλαδή μιας ηλεκτρονικής υπογραφής . Έτσι, η ηλεκτρονική υπογραφή πρέπει να αποτελεί απόδειξη της προέλευσης, της γνησιότητας και της ακεραιότητας των ανταλλασσομένων μηνυμάτων.

Επιπλέον, η ηλεκτρονική υπογραφή πρέπει να δημιουργείται και να αναγνωρίζεται εύκολα και τέλος να πλαστογραφείται δύσκολα. Η ψηφιακή υπογραφή, ως ένα είδος ηλεκτρονικής υπογραφής, είναι μία συμβολοσειρά από bits και εξαρτάται από το μήνυμα που συνοδεύει.,Ο λόγος αυτής της εξάρτησης είναι η ευκολία απόσπασης και αντιγραφής συμβολοσειρών από τα μηνύματα που συνοδεύουν.

Πράγματι, όσο δύσκολη και αν είναι η διαδικασία δημιουργίας μιας ψηφιακής υπογραφής, εάν δεν συνδυάζεται κατάλληλα με το μήνυμα είναι εύκολη η προσθήκη της σε οποιοδήποτε άλλο μήνυμα. Η έννοια της, αρχικά, συζητήθηκε από τους Diffie και Hellman και από τότε έχουν προταθεί πολλά τέτοια συστήματα.

Υπάρχουν δύο γενικές κατηγορίες αλγορίθμων δημόσιου κλειδιού που μπορούν να χρησιμοποιηθούν για τη δημιουργία ψηφιακών υπογραφών. Η μία κατηγορία χρησιμοποιεί αλγορίθμους κρυπτογράφησης όπως ο RSA, ενώ η άλλη χρησιμοποιεί ιδιάζοντες αλγορίθμους υπογραφής χωρίς κρυπτογράφηση. Αντιπροσωπευτικός αλγόριθμος της δεύτερης κατηγορίας είναι ο DSA.

Οι ψηφιακές υπογραφές χρησιμοποιούνται για να επιβεβαιώσουν ότι ένα μήνυμα προέρχεται πραγματικά από τον ισχυριζόμενο αποστολέα .Μπορούν επίσης να χρησιμοποιηθούν timestamp στα έγγραφα: ένα εμπιστευμένο συμβαλλόμενο μέρος υπογράφει το έγγραφο και το timestamp του με το μυστικό κλειδί του /της, πιστοποιώντας κατά συνέπεια ότι το έγγραφο υπήρξε στο δηλωμένο χρόνο.

Οι ψηφιακές υπογραφές, επίσης, χρησιμοποιούνται για να πιστοποιήσουν ότι ένα δημόσιο κλειδί ανήκει σε ένα ιδιαίτερο πρόσωπο. Αυτό, γίνεται υπογράφοντας με το συνδυασμό του κλειδιού και τις πληροφορίες για τον ιδιοκτήτη του από ένα εμπιστευμένο κλειδί. Ο λόγος για

εμπιστοσύνη στο κλειδί μπορεί πάλι να είναι ότι υπογράφηκε από ένα άλλο εμπιστευμένο κλειδί. Τελικά, κάποιο κλειδί πρέπει να είναι η ρίζα της ιεραρχίας της εμπιστευτικότητας (δηλαδή δεν εμπιστεύεται επειδή υπογράφηκε από κάποιο, αλλά επειδή θεωρείτε a priori ότι το κλειδί μπορεί να εμπιστευθεί). Σε μια συγκεντρωτική υποδομή κλειδιών υπάρχουν πολύ λίγες ρίζες στο δίκτυο εμπιστοσύνης (π.χ., εμπιστευμένες κυβερνητικές αντιπροσωπείες, τέτοιες ρίζες καλούνται επίσης αρχές πιστοποίησης). Σε μια κατανεμημένη υποδομή δεν χρειάζεται να είναι οποιεσδήποτε παγκοσμίως αποδεκτές ρίζες και κάθε συμβαλλόμενο μέρος μπορεί να έχει διαφορετικές εμπιστευμένες ρίζες (τέτοιες, όπως, του κλειδιού του συμβαλλόμενου μέρους και οποιωνδήποτε κλειδιών που υπογράφονται από αυτό).

Μια ψηφιακή υπογραφή ενός αυθαίρετου εγγράφου δημιουργείται χαρακτηριστικά με τον υπολογισμό μιας ταξινόμησης (σύνοψης) μηνυμάτων από το έγγραφο και τη σύνδεση της με τις πληροφορίες για τον υπογράφοντα, ένα timestamp, κ.λ.π. Η προκύπτουσα σειρά κρυπτογραφείται, έπειτα, χρησιμοποιώντας το ιδιωτικό κλειδί του υπογράφοντος και ένα κατάλληλο αλγόριθμο. Το προκύπτων κρυπτογραφημένο block των bits είναι η υπογραφή. Διανέμεται, συχνά, μαζί με τις πληροφορίες για το δημόσιο κλειδί που χρησιμοποιήθηκε για να το υπογράψει. Για να ελέγξει μια υπογραφή, ο λαμβάνων πρώτα αποφασίζει εάν εμπιστεύεται ότι το κλειδί ανήκει στο πρόσωπο που υποτίθεται ότι ανήκει και αποκρυπτογραφεί, έπειτα, την υπογραφή χρησιμοποιώντας το δημόσιο κλειδί του προσώπου. Εάν η υπογραφή αποκρυπτογραφεί κατάλληλα και οι πληροφορίες αντιστοιχούν σε αυτές του μηνύματος (κατάλληλη αφομοίωση μηνυμάτων κ.λ.π.), η υπογραφή γίνεται αποδεκτή. Διάφορες μέθοδοι για τις ψηφιακές υπογραφές είναι διαθέσιμες.

Τελευταία στην Αμερική έχει προταθεί από την NSA (National Security Agency) το σύστημα Captstone που συνδυάζει τα χαρακτηριστικά του Clipper Chip και την ψηφιακή υπογραφή με DSA και είναι ένα πολλαπλό κρυπτογραφικό σύστημα. Αυτό, μπορεί να χρησιμοποιηθεί για κρυπτο-

γράφηση με δημόσιο κλειδί, για ψηφιακή υπογραφή και για ανταλλαγές κλειδιών .

ΚΕΦΑΛΑΙΟ 8ο

ΚΡΥΠΤΟΓΡΑΦΙΑ

1. Εισαγωγικά στοιχεία

Οι άνθρωποι εννοούν διαφορετικά πράγματα όταν μιλούν για τη κρυπτογραφία.. Η ισχυρή κρυπτογράφηση είναι ένα είδος κρυπτογράφησης που μπορεί να χρησιμοποιηθεί για να προστατεύσει πληροφορίες πραγματικής αξίας για οργανωμένους εγκληματίες, πολυεθνικές εταιρίες και σημαντικές κυβερνήσεις. Η ισχυρή κρυπτογράφηση χρησιμοποιείται μόνο στις στρατιωτικές επιχειρήσεις. Εντούτοις, στην κοινωνία των πληροφοριών έχει γίνει ένα από τα βασικά εργαλεία για τη μυστικότητα και την εμπιστευτικότητα.

Καθώς κινούμαστε σε μια κοινωνία πληροφοριών, τα τεχνολογικά μέσα για τη παγκόσμια επιτήρηση εκατομμυρίων ανθρώπων διατίθενται στις κυβερνήσεις. Η κρυπτογραφία έχει γίνει ένα από τα κύρια εργαλεία για την ιδιωτικότητα, την εμπιστοσύνη, τον έλεγχο πρόσβασης, τις ηλεκτρονικές πληρωμές, την εταιρική ασφάλεια, και σε αμέτρητους άλλους τομείς.

Το σύστημα της κρυπτογραφίας δεν είναι πλέον ένα στρατιωτικό αντικείμενο που δεν πρέπει να μπερδευτεί. Είναι καιρός να απομυθοποιηθεί το σύστημα της κρυπτογραφίας και να αξιοποιηθούν πλήρως τα πλεονεκτήματα που επιτρέπει στη σύγχρονη κοινωνία.

2. Βασική ορολογία

Στην κρυπτογραφική ορολογία, το μήνυμα καλείται plaintext (κείμενο μη κωδικοποιημένο) ή cleartext. Η κωδικοποίηση του περιεχομένου του μηνύματος κατά τέτοιο τρόπο, ώστε να υποκρύπτεται το περιεχόμενό του από τους ξένους, καλείται κρυπτογράφηση. Το κρυπτογραφημένο μήνυμα καλείται ciphertext (κρυπτογραφημένο κείμενο). Η διαδικασία αποκατάστασης του plaintext από το ciphertext καλείται αποκρυπτογράφηση. Η κρυπτογράφηση και η αποκρυπτογράφηση χρησιμοποιούν συνήθως ένα κλειδί και η μέθοδος κωδικοποίησης είναι τέτοια που η αποκρυπτογράφηση μπορεί να εκτελεσθεί μόνο με τη γνώση του κατάλληλου κλειδιού.

Κρυπτογραφία είναι η τέχνη ή η επιστήμη της διατήρησης των μηνυμάτων μυστικών. Η κρυπτανάλυση είναι η τέχνη του σπασίματος των ciphers, δηλ. η ανάκτηση του plaintext χωρίς τη γνώση του κατάλληλου κλειδιού. Οι άνθρωποι που κάνουν τη κρυπτογραφία είναι οι cryptographers (κρυπτογράφοι), και οι επαγγελματίες της κρυπτανάλυσης είναι οι cryptanalysts (κρυπταναλυτές).

Η κρυπτογραφία εξετάζει όλες τις πτυχές της ασφάλειας των μηνυμάτων, της αυθεντικοποίησης, των ψηφιακών υπογραφών, των ηλεκτρονικών χρημάτων και άλλων εφαρμογών. Η κρυπτολογία είναι ο κλάδος των μαθηματικών που μελετά τα μαθηματικά θεμέλια των κρυπτογραφικών μεθόδων.

3. Βασικοί κρυπτογραφικοί αλγόριθμοι

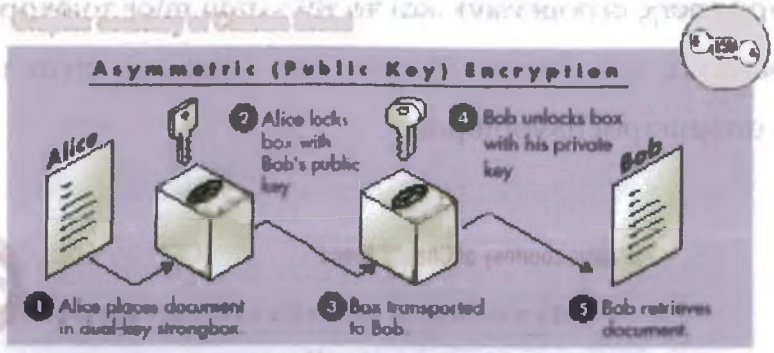
Μια μέθοδος κρυπτογράφησης και αποκρυπτογράφησης καλείται cipher. Μερικές κρυπτογραφικές μέθοδοι στηρίζονται στη μυστικότητα των αλγορίθμων, όπου τέτοιοι αλγόριθμοι είναι μόνο ιστορικού ενδιαφέροντος και δεν είναι επαρκείς για τις πραγματικές ανάγκες. Όλοι οι σύγχρονοι αλγόριθμοι χρησιμοποιούν ένα κλειδί για να ελέγξουν την κρυπτογράφηση και την αποκρυπτογράφηση. Ένα μήνυμα μπορεί να αποκρυπτογραφηθεί μόνο εάν το κλειδί ταιριάζει με το κλειδί κρυπτογράφησης. Το κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση μπορεί να είναι διαφορετικό

από το κλειδί κρυπτογράφησης, αλλά για τους περισσότερους αλγορίθμους είναι το ίδιο.

Υπάρχουν δύο κατηγορίες αλγορίθμων βασισμένων στα κλειδιά, οι συμμετρικοί (ή μυστικού κλειδιού) και οι ασύμμετροι (ή δημόσιου κλειδιού) αλγορίθμων. Η διαφορά είναι ότι οι συμμετρικοί αλγόριθμοι χρησιμοποιούν το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση (ή το κλειδί αποκρυπτογράφησης παράγεται εύκολα από το κλειδί κρυπτογράφησης), ενώ οι ασύμμετροι αλγόριθμοι χρησιμοποιούν διαφορετικό κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση και το κλειδί αποκρυπτογράφησης δεν μπορεί να προέλθει από το κλειδί κρυπτογράφησης.

Οι συμμετρικοί αλγόριθμοι μπορούν να διαιρεθούν στα ciphers ρευμάτων (stream ciphers) και στα ciphers φραγμών(ciphers block). Τα Ciphers ρευμάτων μπορούν να κρυπτογραφήσουν ένα ενιαίο κομμάτι του plaintext σε ένα διάστημα, ενώ τα ciphers φραγμών παίρνουν διάφορα κομμάτια (των 64 bit στα σύγχρονα ciphers), και τα κρυπτογραφούν ως ενιαία μονάδα.

Τα ασύμμετρα ciphers (που αποκαλούνται επίσης αλγόριθμοι δημόσιων κλειδιών ή γενικά κρυπτογραφία δημόσιου κλειδιού) επιτρέπουν στο κλειδί κρυπτογράφησης να είναι δημόσιο (μπορεί ακόμη και να δημοσιευθεί σε μια εφημερίδα), επιτρέποντας σε καθένα να κρυπτογραφήσει με το κλειδί, ενώ μόνο ο κατάλληλος παραλήπτης (που ξέρει το κλειδί αποκρυπτογράφησης) μπορεί να αποκρυπτογραφήσει το μήνυμα. Το κλειδί κρυπτογράφησης καλείται επίσης δημόσιο κλειδί και το κλειδί αποκρυπτογράφησης ιδιωτικό ή μυστικό κλειδί.



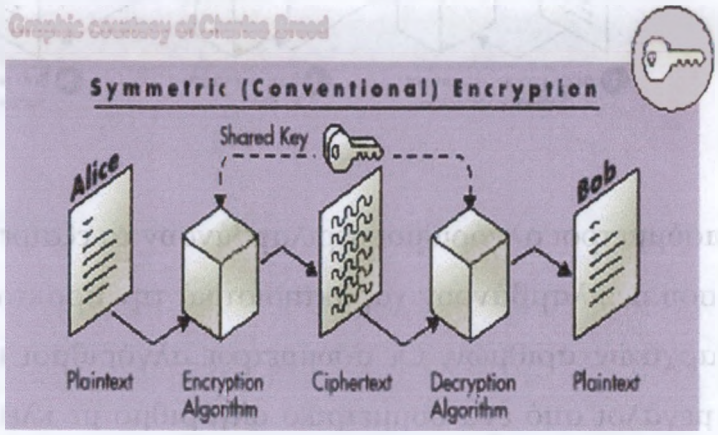
Οι ασύμμετροι αλγόριθμοι περιλαμβάνουν τα εξαιρετικά σύνθετα μαθηματικά που περιλαμβάνουν χαρακτηριστικά την πρακτόρευση των μεγάλων πρωταρχικών αριθμών. Οι ασύμμετροι αλγόριθμοι είναι χαρακτηριστικά πιο μεγάλοι από ένα συμμετρικό αλγόριθμο με κλειδί σύντομου μήκους. Αλλά λόγω της πολυπλοκότητάς τους, χρησιμοποιούνται στην υπογραφή ενός μηνύματος ή ενός πιστοποιητικού. Συνήθως δεν χρησιμοποιούνται για τη μεταφορά των κρυπτογραφημένων δεδομένων.

Οι σύγχρονοι κρυπτογραφικοί αλγόριθμοι δεν μπορούν πραγματικά να εκτελεσθούν από τους ανθρώπους. Οι ισχυροί κρυπτογραφικοί αλγόριθμοι έχουν ως σκοπό να εκτελεσθούν από υπολογιστές ή ειδικευμένες συσκευές Hardware. Στις περισσότερες εφαρμογές, η κρυπτογραφία γίνεται στο λογισμικό των υπολογιστών, ενώ πολυάριθμα κρυπτογραφικά πακέτα λογισμικού είναι διαθέσιμα.

Γενικά, οι συμμετρικοί αλγόριθμοι εκτελούνται γρηγορότερα σε έναν υπολογιστή απ' ότι οι ασύμμετροι. Στην πράξη χρησιμοποιούνται συχνά μαζί, έτσι ώστε ένας αλγόριθμος δημόσιου κλειδιού να χρησιμοποιείται για να κρυπτογραφήσει ένα τυχαίο κλειδί κρυπτογράφησης. Το τυχαίο κλειδί χρησιμοποιείται για να κρυπτογραφήσει το πραγματικό μήνυμα, χρησιμοποιώντας έναν συμμετρικό αλγόριθμο.

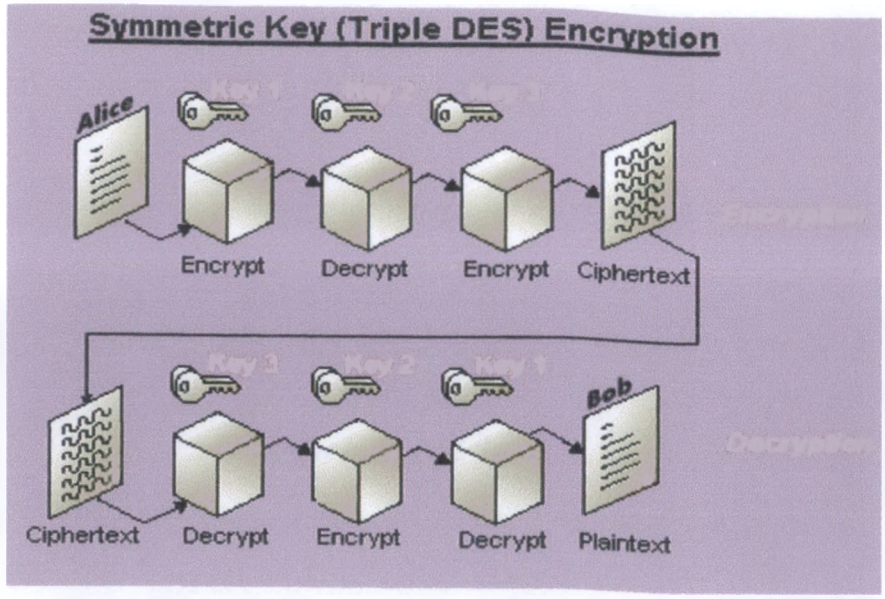
Πολλοί καλοί κρυπτογραφικοί αλγόριθμοι είναι ευρέως και δημόσια διαθέσιμοι σε οποιοδήποτε σημαντικό βιβλιοπωλείο, επιστημονική βιβλιοθήκη, ή γραφείο διπλωμάτων ευρεσιτεχνίας, και στο Διαδίκτυο. Οι γνωστές συμμετρικές λειτουργίες, που περιλαμβάνουν το DES (πρότυπο

κρυπτογράφησης δεδομένων) και το RSA ,που πήρε το όνομα του από τους τρεις εφευρέτες του (Rivest, Shamir, και Adleman), είναι πιθανών οι πιο γνωστοί ασύμμετροι αλγόριθμοι.



DES και RSA

Το πρότυπο κρυπτογράφησης δεδομένων (DES) εφευρέθηκε από την εταιρία της IBM στη δεκαετία του '70. Κατά τη διάρκεια της διαδικασίας να γίνει ένας πρότυπος αλγόριθμος, τροποποιήθηκε σύμφωνα με τις υποδείξεις της εθνικής αντιπροσωπείας ασφάλειας (NSA). Ο αλγόριθμος έχει μελετηθεί από κρυπτογράφους για σχεδόν 20 έτη. Κατά τη διάρκεια αυτής της περιόδου, δεν έχει δημοσιευθεί καμία μέθοδος που να περιγράφει έναν τρόπο παραβίασης του αλγόριθμου, εκτός από τις τεχνικές ζωτικής παραβίασης. Ο DES έχει ένα κλειδί 56-δυαδικών ψηφίων. Ο Τριπλός-DES είναι μια μέθοδος που χρησιμοποιεί το DES για να παρέχει πρόσθετη ασφάλεια. Ο τριπλός-DES μπορεί να γίνει με δύο ή με τρία κλειδιά. Δεδομένου ότι ο αλγόριθμος εκτελεί μια ακολουθία κρυπτογράφησης-αποκρυπτογράφησης -κρυπτογράφησης , αυτό καλείται μερικές φορές τρόπος EDE. Αυτό το διάγραμμα δείχνει ένα τριπλό- DES με τη μέθοδο των τριών κλειδιών που χρησιμοποιείται για την κρυπτογράφηση:



Η ψηφιακή υπογραφή κατά RSA καθώς και η επαλήθευση της, υποστηρίζονται από μία επιλογή μήκους κλειδιών 512, 768, ή 1024 bit. Οι αλγόριθμοι αυτοί τυπικά χρησιμοποιούν το θεώρημα Chinese Remainder Theorem (CRT), για να επιταχύνουν την διαδικασία. Ακόμη και με την χρήση κλειδιού μήκους 1024 bit, ο εκτιμώμενος χρόνος εκτέλεσης της ψηφιακής υπογραφής είναι τυπικά κάτω από ένα δευτερόλεπτο. Συνήθως το αρχείο EEPROM περιέχει το ιδιωτικό κλειδί το οποίο είναι σχεδιασμένο έτσι ώστε το ευαίσθητο βασικό υλικό να μην εγκαταλείπει ποτέ το τσιπ. Το ιδιωτικό κλειδί δεν μπορεί να εξαχθεί σαν πληροφορία από το ολοκληρωμένο κύκλωμα. κι ούτε ο καρτούχος έχει πρόσβαση σε αυτό.

Αν και οι έξυπνες κάρτες έχουν τη δυνατότητα να δημιουργούν ζεύγη κλειδιών RSA, η συγκεκριμένη διαδικασία είναι συνήθως αρκετά χρονοβόρα.. Συγκεκριμένα, ο τυπικός χρόνος δημιουργίας ενός ζεύγους κλειδιών RSA 1024 bit,κυμαίνεται από 8 δευτερόλεπτα έως και 30. Μεγαλύτεροι χρόνοι παραβιάζουν τις προδιαγραφές κατά ISO για την διάρκεια των επικοινωνιών, γι'αυτό και ειδικευμένο λογισμικό που ελέγχει τέτοιες λειτουργίες, ή κατάλληλες συσκευές, είναι κατά καιρούς απαραίτητο. Επιπρόσθετα, η ποιότητα των κλειδιών που δημιουργούνται είναι πιθανά χαμηλή, λόγω της έλλειψης υπολογιστικής ισχύος του ολοκληρωμένου κυκλώματος της κάρτας που είναι πιθανό να έχει δημιουργήσει ένα σχετικά εύκολο-τυχαίο -αριθμό

που με τη σειρά του θα έχει σαν αποτέλεσμα αδύναμους αλγορίθμους, από πλευράς ασφάλειας.

4. Παράδειγμα Κρυπτογράφησης

Κρυπτογράφηση

Ο Harry θέλει να στείλει μια έκθεση της επιχείρησης στην οποία εργάζεται σε μια συνάδελφο του, έτσι αυτός:

- παράγει ένα κλειδί περιόδου επικοινωνίας
- κρυπτογραφεί την έκθεση της επιχείρησης χρησιμοποιώντας το κλειδί περιόδου επικοινωνίας και ένα συμμετρικό αλγόριθμο
- λαμβάνει το δημόσιο κλειδί της Sally από την αρχή πιστοποίησης
- συνδέει την ψηφιακή υπογραφή με την κρυπτογραφημένη έκθεση της επιχείρησης
- κρυπτογραφεί τη συνδυασμένη ψηφιακή υπογραφή/ κρυπτογραφημένη έκθεση της επιχείρησης χρησιμοποιώντας το δημόσιο κλειδί της Sally
- κρυπτογραφεί το κλειδί περιόδου επικοινωνίας χρησιμοποιώντας το δημόσιο κλειδί της Sally, παράγοντας ένα ψηφιακό φάκελο
- μεταφέρει το πακέτο με τη κρυπτογραφημένη ψηφιακή υπογραφή /κρυπτογραφημένη έκθεση της επιχείρησης στη Sally.
- Μεταφέρει το ψηφιακό φάκελο στη Sally.

Αποκρυπτογράφηση.

Η Sally λαμβάνει το πακέτο με τη ψηφιακή υπογραφή/ κρυπτογραφημένη έκθεση της επιχείρησης και τον ψηφιακό φάκελο, έτσι αυτή:

- αποκρυπτογραφεί το πακέτο με την ψηφιακή υπογραφή/ κρυπτογραφημένη έκθεση της επιχείρησης χρησιμοποιώντας το ιδιωτικό της κλειδί
- αποκρυπτογραφεί τον ψηφιακό φάκελο χρησιμοποιώντας το ιδιωτικό της κλειδί για να ανακτήσει το κλειδί περιόδου επικοινωνίας.

- αποκρυπτογραφεί την κρυπτογραφημένη έκθεση της επιχείρησης χρησιμοποιώντας το κλειδί περιόδου επικοινωνίας
- τρέχει την έκθεση μέσω μιας λειτουργίας αφομοίωσης για να λάβει μια hash αξία.
- λαμβάνει το δημόσιο κλειδί του Harry από την αρχή πιστοποίησης αποκρυπτογραφεί την ψηφιακή υπογραφή χρησιμοποιώντας το δημόσιο κλειδί του Harry για να πάρει την παραγόμενη hash αξία του Harry.
- συγκρίνει την παραγόμενη hash αξία του Harry με την δική της παραγόμενη hash αξία.

Εάν η Sally αποκρυπτογραφήσει επιτυχώς την ψηφιακή υπογραφή χρησιμοποιώντας το δημόσιο κλειδί του Harry, μπορεί να είναι βέβαιη ότι η εμπιστευτική έκθεση της επιχείρησης προήλθε από το Harry. Εάν ταιριάζουν επίσης οι δύο hash αξίες που παράγονται από την έκθεση, η Sally έχει μια εγγύηση ότι η έκθεση είναι άθικτη.

ΚΕΦΑΛΑΙΟ 9ο

ΥΠΟΚΛΟΠΗ

1. Εισαγωγή

Αν και αυξάνονται οι αριθμοί, οι καταναλωτές ακόμα δεν χρησιμοποιούν τις πιστωτικές τους κάρτες στο Διαδίκτυο, τόσο, όσο, θα ήθελαν οι e-tailers (ηλεκτρονικοί λιανοπωλητές). Γι' αυτό πολλοί έμποροι του Διαδικτύου<cyber-merchants> συνεχίζουν να προσφέρουν μια ατελή σειρά παραγγελιών, έτσι, ώστε οι αγοραστές να έχουν την επιλογή να αποσύρουν την παραγγελία τους. Η αγορά μέσω του Διαδικτύου<cyber-shopping> μπορεί να είναι πιο βολική -- και μερικοί άνθρωποι κάνουν όλες τις αγορές τους on-line -- αλλά η απάτη των πιστωτικών καρτών είναι πάντα μια απειλή και στο κόσμο του Διαδίκτυο και στον πραγματικό κόσμο. Οι χάκερς έχουν βρει τρόπους για να κλέβουν αριθμούς πιστωτικών καρτών από τα web-sites.

Για να επεξηγήσει τη σημασία μιας ικανής ασφάλειας, ένας δημοσιογράφος του δικτύου της Tv, προειδοποίησε ότι μια πιθανή απώλεια της ασφάλειας σε μια περιοχή του Ιστού στο Διαδίκτυο, θα ήταν σε θέση να αποκτήσουν πρόσβαση στα αρχεία περίπου 1.500 πελάτες, στα οποία θα περιλαμβάνονται τα πάντα, από τους αριθμούς πιστωτικών καρτών και τα αρχεία πληρωμών μέχρι και λεπτομερή σχόλια για τους πελάτες.

Μερικοί e- tailers κατηγορούν την απροθυμία του καταναλωτή για την ανικανότητα του κυβερνοχώρου να αποκτήσει τη μορφή της προσωπικής επαφής που παίρνει ένας αγοραστής, όταν κοιτάζει με τα μάτια του τον έμπορο ενός καταστήματος. Οι εμπειρογνώμονες λένε ότι αυτό το είδος ενθαρρυντικού επιπέδου , θα ενισχυθεί όταν οι απευθείας σύνδεσης μέθοδοι

πληρωμής και τα μέτρα ασφάλεια τυποποιηθούν σύμφωνα με τις λιανικές βιομηχανίες και τις βιομηχανίες ταχυδρομικών παραγγελιών.

Ενώ, οι επιχειρήσεις του Διαδικτύου έχουν αναλάβει τις ευθύνες τους προς τους κατόχους των πιστωτικών καρτών, για τις παραβιάσεις ασφάλειας και τις προκύπτουσες απώλειες , παραμένει το πρόβλημα των ανθρώπων που χρησιμοποιούν κλεμμένες πιστωτικές κάρτες για να κάνουν τις αγορές τους στο Διαδίκτυο. Και ενώ οι άδικες ή ψευδείς ραδιουργίες από τις επιχειρήσεις πιστωτικών καρτών δε λαμβάνονται σαν δεδομένες, συμβαίνουν. Τα καλά νέα είναι ότι οι καταναλωτές προστατεύονται από το νόμο, σε περίπτωση απάτης πιστωτικών καρτών.

Θα πρέπει να αποδίδεται προσοχή κατά την ολοκλήρωση της εφαρμογής της πιστωτικής κάρτας. Μερικά είδη εφαρμογών παρέχουν τώρα ένα κουτί με το οποίο μπορεί να ελεγχθεί αν επιτρέπεται ή απαγορεύετε τη πώληση των πληροφοριών του χρήστη στο κατάλογο αποστολής. Ο χρήστης μπορεί, επίσης, να προστατευθεί αποσύροντας το όνομά του από τον ηλεκτρονικό ταχυδρομικό κατάλογο του πιστωτικού γραφείου<credit bureaus mailing lists>.

Όταν θα γράφει σε αυτές τις επιχειρήσεις, θα περιλαμβάνει το πλήρες όνομα του, τις παραλλαγές του ονόματος του και την ηλεκτρονική διεύθυνση αποστολής του, τον αριθμό κοινωνικών ασφαλίσεως του και την υπογραφή του. Πρέπει, να δηλώνεται σαφώς ότι απαιτείται να αφαιρεθεί το όνομά σας από τους ηλεκτρονικούς ταχυδρομικούς καταλόγου.

Η εξασφάλιση των δικτύων, οδήγησε στη δημοτικότητα των λύσεων ασφάλειας της περιμέτρου των δικτύων, όπως τα firewall, τα αντιβιοτικά λογισμικά και τα συστήματα ανίχνευσης τυχόν εισβολών. Αυτά τα προϊόντα στοχεύουν να περιορίσουν τους τύπους εφαρμογών ώστε να μπορούν να διαπεράσουν τα σύνορα δικτύων και να επεκταθούν σε ασφαλής ζώνες. Στις περισσότερες περιπτώσεις, αυτά τα προϊόντα περιόρισαν την κυκλοφορία στις διάφορες ιστοσελίδες και το ηλεκτρονικό ταχυδρομείο. Αν και δεν είναι σίγουρο, αυτές οι λύσεις εργάστηκαν καλά για την εξασφάλιση των δικτύων από εξωτερικές επιθέσεις - και συνεχίζουν σήμερα για να παρέχουν ένα ακέ-

ραιο συστατικό μιας λύσης για πιο ολοκληρωμένη IT ασφάλεια μιας επιχείρησης. Παρα το γεγονός ότι ο αριθμός των επιθέσεων στις εφαρμογές συνεχίζει να αυξάνεται, οι επιχειρήσεις απαιτούν:

- εξασφάλιση πρόσβασης στις αναδυόμενες εφαρμογές, όπως ροή βίντεο και άμεσα μηνύματα
- απομάκρυνση της πρόσβασης για τις εφαρμογές των συνεργατών, πελατών και των προμηθευτών μέσω ενός ειδικού δικτύου
- εξασφάλιση της πρόσβασης στις εφαρμογές και τους πόρους των δικτύων από οποιοδήποτε δημόσιο ή ιδιωτικό δίκτυο.

Σαφώς, η ασφάλεια δικτύων δεν είναι αρκετή για να προστατεύσει τις εφαρμογές και δεν είναι αρκετά εύκαμπτη ώστε να επιτρέψει στις επιχειρήσεις να παραδώσουν την πρόσβαση στις εφαρμογές που ζητούν οι χρήστες. Προσπάθειες έχουν γίνει μέσω της συναρμολόγησης διάφορων συστατικών, αλλά το γεγονός παραμένει ότι η ασφάλεια των δικτύων εξασφαλίζει τα δίκτυα, όχι τις εφαρμογές. Η εφαρμογή ασφάλειας αναπτύχθηκε για να παρέχει στις επιχειρήσεις ένα πρόσθετο επίπεδο ασφάλειας, το οποίο παρέχει υποστήριξη στη γενική ασφάλειά.

2. Λειτουργίες ασφάλειας

Σε ένα υψηλό επίπεδο, η ασφάλεια εφαρμογής πρέπει να εκτελέσει τρεις λειτουργίες:

- Μεγιστοποίηση της διαθεσιμότητας των εφαρμογών: καθιερώνετε μια σύνδεση από οποιαδήποτε εφαρμογή σε οποιοδήποτε έμπιστο χρήστη που διαχειρίζεται τις πολυπλοκότητες και τους κινδύνους ασφάλειας στα σύνορα των δικτύων και καθιστά την εφαρμογή διαθέσιμη στους χρήστες – σε οποιοδήποτε δίκτυο κι αν βρίσκονται.
- Διαχείριση της πρόσβασης της εφαρμογής: η εγγύτητα των χρηστών και η εμπιστευτικότητα των δεδομένων μέσω της πιστοποίησης της ταυτότητας και του ελέγχου πρόσβασης γίνεται μόλις μια εφαρμογή είναι διαθέσιμη στους χρήστες – σε οποιοδήποτε δίκτυο κι αν βρίσκονται.

- Εξασφάλιση της ιδιωτικότητας της κυκλοφορίας των δεδομένων της εφαρμογής: κρυπτογραφεί το ρεύμα των δεδομένων της εφαρμογής για να εξασφαλιστεί η ακεραιότητα των στοιχείων, δεδομένου ότι διαπερνούν τα δημόσια ή/ και ιδιωτικά δίκτυα και παρέχεται η δυνατότητα αναγραφής και κάλυψης της εφαρμογής.

Οι εφαρμογές ασφαλείας , μαζί με την εγκατεστημένη ασφάλεια δικτύων, παρέχουν το καλύτερο και στους δύο κόσμους: μέγιστη ασφάλεια με τη μέγιστη πρόσβαση της εφαρμογής.

3. Οι επιθέσεις στις έξυπνες κάρτες

Μία έξυπνη κάρτα φαίνεται να είναι ένα ανώτερο εργαλείο για την ασφάλεια των συστημάτων και παρέχει μια θέση για ασφαλή αποθήκευση. Ένα από τα χαρακτηριστικά γνωρίσματα ασφάλειας που παρέχονται από τα περισσότερα λειτουργικά συστήματα έξυπνων καρτών είναι οι κρυπτογραφικές ευκολίες. Παρέχουν την κρυπτογράφηση και την αποκρυπτογράφηση των στοιχείων για την κάρτα και μερικοί από αυτούς μπορούν ακόμη και να χρησιμοποιηθούν για να παράγουν τα κρυπτογραφικά κλειδιά.

Το μυστικό του κρυπτογραφικού αλγορίθμου, τα κλειδιά που αποθηκεύονται και ο έλεγχος πρόσβασης μέσα στην έξυπνη κάρτα, γίνονται οι στόχοι των επιτιθέμενων. Σήμερα, πολλές επιχειρήσεις και κρυπτογράφοι απαιτούν να είναι σε θέση να σπάσουν την έξυπνη κάρτα και τον μικροελεγκτή της. Μερικοί από αυτούς, επιτίθονται στην κάρτα φυσικά ,ενώ άλλοι αποδεικνύουν την επιτυχία τους με μαθηματικές θεωρίες.

α) Λογικές επιθέσεις

Εφόσον, όλο το υλικό του κλειδιού μιας έξυπνης κάρτας αποθηκεύεται στην ηλεκτρικά εξαλείψιμη προγραμματίσημη μνήμη μόνο για ανάγνωση (EEPROM), και εξαιτίας του γεγονότος ότι οι EEPROM εγγεγραμμένες διαδικασίες μπορούν να επηρεαστούν από τις ασυνήθιστες τάσεις και θερμοκρασίες, οι πληροφορίες μπορούν να παγιδευτούν με την αύξηση ή τη ρίψη της παρεχόμενης τάσης στο μικροελεγκτή. Στην έκθεση της "αντίστα-

σης πλαστογραφήσεων - μια προειδοποιητική σημείωση" από το Ross και το Markus (1996), διάφορα παραδείγματα επίθεσης των έξυπνων καρτών με τη ρύθμιση της τάσης παρέχονται.

Παραδείγματος χάριν, μια ευρέως γνωστή επίθεση του μικροελεγκτή PIC16C84 είναι ότι η ασφάλεια των bits του ελεγκτή μπορεί να είναι σαφής με το σβήσιμο της μνήμης, με την αύξηση της τάσης VCC σε VPP - 0.5V. Μια επίθεση στον επεξεργαστή ασφάλειας DS5000 είναι ένα άλλο παράδειγμα. Μια σύντομη πτώση της τάσης μπορεί να απελευθερώσει την κλειδαριά ασφάλειας και μερικές φορές χωρίς να σβήσει τα μυστικά δεδομένα.

Για αυτούς τους λόγους, μερικοί επεξεργαστές ασφάλειας εφάρμοσαν τους αισθητήρες που θα προκαλέσουν έναν συναγερμό όταν υπάρχουν οποιεσδήποτε περιβαλλοντικές αλλαγές. Εντούτοις, αυτά τα είδη αισθητήρων προκαλούν πάντα ψεύτικο συναγερμό λόγω των διακυμάνσεων όταν τροφοδοτείται η κάρτα και το κύκλωμα είναι εγκαθιδρυμένο. Επομένως αυτό το σχέδιο δεν χρησιμοποιείται συχνά

β) Φυσικές επιθέσεις

Οι φυσικές επιθέσεις είναι χαρακτηριστικές. Προτού να μπορέσει να εκτελεσθεί αυτό το είδος επίθεσης, το τσιπ κυκλωμάτων πρέπει να αφαιρεθεί από την πλαστική κάρτα. Αυτό μπορεί να γίνει με την απλή χρησιμοποίηση ενός αιχμηρού μαχαιριού για να κόψει μακριά το πλαστικό, πίσω από το τσιπ έως ότου η κόλλα γίνει ορατή. Έπειτα η κόλλα μπορεί να διαλυθεί με την προσθήκη μερικών σταγόνων νιτρικού οξέος (> 98% HNO 3). Το οξύ και η ρητίνη μπορούν να πλυθούν με το τίναγμα της κάρτας με ασετόν, έως ότου εκτεθεί πλήρως η επιφάνεια πυριτίου. Τελικά το τσιπ μπορεί να εξεταστεί και να δεχτεί επίθεση άμεσα.

Στο εργαστήριο Cavendish στο Cambridge, μια τεχνική αναπτύσσεται για την αντίστροφη εφαρμοσμένη μηχανική στα τσιπ κυκλωμάτων. Το σχεδιάγραμμα και η λειτουργία του τσιπ μπορούν να προσδιοριστούν χρησιμοποιώντας εκείνη την τεχνική. Κατόπιν, μια άλλη τεχνική που αναπτύσσεται από την IBM μπορεί να χρησιμοποιηθεί για να παρακολουθεί τη λει-

τουργία του τσιπ. Κατά συνέπεια, το μυστικό του μπορεί να αποκαλυφθεί πλήρως.

Εκτός από αυτό, υπάρχουν πολλοί διαφορετικοί τρόποι για να εκτελεσθούν οι φυσικές επιθέσεις. Παραδείγματος χάριν, εξαλείφοντας τη κλειδαριά ασφάλειας των bit με τη συγκέντρωση των UV ακτινών στο EPROM, εξετάζοντας τη λειτουργία του κυκλώματος με τη χρησιμοποίηση των μικροαναλυτών ή τη χρησιμοποίηση των μικροσκοπίων κοπτών λέιζερ για την εξερεύνηση του τσιπ κ.λ.π. Εντούτοις, αυτά τα είδη επιθέσεων είναι διαθέσιμα μόνο στα καλά χρηματοδοτημένα εργαστήρια, δεδομένου ότι οι δαπάνες που συνδέονται είναι αρκετά υψηλές.

4. Επιθέσεις στα κρυπτογραφικά συστήματα (Κρυπτανάλυση)

Η κρυπτανάλυση είναι η τέχνη της αποκρυπτογράφησης των κρυπτογραφημένων επικοινωνιών χωρίς τη γνώση των κατάλληλων κλειδιών. Υπάρχουν πολλές τεχνικές κρυπτανάλυσης. Μερικές από τις σημαντικότερες περιγράφονται παρακάτω:

- **Επίθεση μόνο στο Ciphertext (Ciphertext-only attack)**: Αυτή είναι η κατάσταση, κατά την οποία ο επιτιθέμενος δεν γνωρίζει τίποτα για το περιεχόμενο του μηνύματος και πρέπει να εργαστεί από το ciphertext μόνο. Στην πράξη, είναι δυνατόν, αρκετά συχνά να γίνουν εικασίες για το plaintext, δεδομένου ότι πολλοί τύποι μηνυμάτων έχουν καθορίσει τις επικεφαλίδες. Ακόμη και οι συνηθισμένες επιστολές και τα έγγραφα αρχίζουν με έναν πολύ προβλέψιμο τρόπο. Είναι, επίσης, δυνατό να υποτεθεί ότι κάποιο block κρυπτογραφημάτων περιέχει μια κοινή λέξη.

- **Επίθεση με γνωστό plaintext (Known-plaintext attack)**: Ο επιτιθέμενος ξέρει ή μπορεί να υποθέσει το plaintext για μερικά μέρη του κρυπτογραφήματος (ciphertext). Ο στόχος είναι να αποκρυπτογραφηθεί το υπόλοιπο του block του κρυπτογραφημένου κειμένου χρησιμοποιώντας αυτές τις πληροφορίες. Αυτό, μπορεί να γίνει με τον καθορισμό του κλειδιού που χρησιμοποιείται για την κρυπτογράφηση των δεδομένων ή μέσω κάποιου συντομότερου δρόμου.

- **Επιλεγμένη plaintext επίθεση (chosen-plaintext attack):** Ο επιτιθέμενος είναι σε θέση να έχει οποιοδήποτε κείμενο θέλει κρυπτογραφημένο με ένα άγνωστο κλειδί. Ο στόχος είναι να καθοριστεί το κλειδί που χρησιμοποιείται για την κρυπτογράφηση. Μερικές μέθοδοι κρυπτογράφησης, ιδιαίτερα η RSA, είναι εξαιρετικά ευπαθής στις επιλεγμένες plaintext επιθέσεις. Όταν τέτοιοι αλγόριθμοι χρησιμοποιούνται, ιδιαίτερη προσοχή πρέπει να δοθεί στη σχεδίαση ολόκληρου του συστήματος, έτσι ώστε ένας επιτιθέμενος να μη μπορεί ποτέ να έχει επιλεγμένη plaintext κρυπτογράφηση.

- **Man-in-the-middle attack:** Αυτή η επίθεση σχετίζεται με την κρυπτογραφική επικοινωνία και τα βασικά πρωτόκολλα ανταλλαγής. Η ιδέα είναι ότι όταν δύο συμβαλλόμενα μέρη ανταλλάζουν κλειδιά για ασφαλή επικοινωνία, ένας αντίπαλος μπαίνει μεταξύ των συμβαλλόμενων μερών στη γραμμή επικοινωνίας. Ο αντίπαλος εκτελεί, έπειτα, μια χωριστή ανταλλαγή κλειδιών με κάθε μέρος. Τα συμβαλλόμενα μέρη θα καταλήξουν στη χρησιμοποίηση διαφορετικού κλειδιού, κάθε ένα από τα οποία είναι γνωστά στον αντίπαλο. Ο αντίπαλος θα αποκρυπτογραφήσει, έπειτα, οποιαδήποτε επικοινωνία με το κατάλληλο κλειδί και θα τις κρυπτογραφήσει με το άλλο κλειδί για την αποστολή του στο άλλο συμβαλλόμενο μέρος. Τα συμβαλλόμενα μέρη θα σκεφτούν ότι επικοινωνούν ασφαλώς, αλλά στην πραγματικότητα ο αντίπαλος ακούει τα πάντα.

Ένας τρόπος για να αποτραπούν οι man-in-the-middle επιθέσεις είναι ότι και οι δύο πλευρές υπολογίζουν μια κρυπτογραφική hash λειτουργία ανταλλαγής των κλειδιών (ή τουλάχιστον των κλειδιών κρυπτογράφησης), την υπογράφουν χρησιμοποιώντας έναν αλγόριθμο ψηφιακής υπογραφής και στέλνουν την υπογραφή στην άλλη πλευρά. Ο παραλήπτης έπειτα ελέγχει ότι η υπογραφή προήλθε από το άλλο επιθυμητό συμβαλλόμενο μέρος και ότι η hash λειτουργία στην υπογραφή ταιριάζει με αυτό που υπολόγισαν τοπικά.

- **Επίθεση συγχρονισμού (Timing attack):** Αυτή η πολύ πρόσφατη επίθεση βασίζεται στις επανειλημμένες μετρήσεις των ακριβή χρόνων εκτέλεσης των αρθρωτών διαδικασιών εκθετοποίησης.

Υπάρχουν πολλές άλλες κρυπτογραφικές επιθέσεις και τεχνικές κρυπτανάλυσης. Εντούτοις, αυτές είναι πιθανώς οι σημαντικότερες για ένα σχεδιαστή πρακτικών συστημάτων. Καθένας που συλλογίζεται να σχεδιάσει έναν νέο αλγόριθμο κρυπτογράφησης, πρέπει να έχει μια βαθύτερη κατανόηση αυτών των ζητημάτων.

5. Προστασία της διαδικασίας

Λόγω της δύναμης του υπολογισμού μιας έξυπνης κάρτας, είναι δυνατό να επιτευχθούν off-line συναλλαγές και οι επαληθεύσεις. Παραδείγματος χάριν, μια έξυπνη κάρτα και μια συσκευή-αποδέκτης καρτών (CAD) μπορούν να προσδιορίσουν η μια την άλλη με τη χρήση της αμοιβαίας ενεργού μεθόδου επικύρωσης(αυθεντικοποίησης) . Επιπλέον, τα δεδομένα και οι κώδικες που αποθηκεύονται στην κάρτα κρυπτογραφούνται από τον κατασκευαστή των τσιπ με τη χρήση της υπολογιστικής κρυπτογράφησης, η οποία καθιστά το τσιπ κυκλωμάτων σχεδόν αδύνατο να πλαστοποιηθεί.

Σήμερα, οι έξυπνες κάρτες χρησιμοποιούνται σε διάφορους τομείς επειδή μπορούν να χρησιμοποιηθούν μαζί με άλλες τεχνολογίες, όπως οι ασύμμετροι κρυπτογραφικοί αλγόριθμοι και ο προσδιορισμός της βιομετρικής, για να παρέχουν τις ιδιαίτερα σίγουρες και έμπιστες εφαρμογές. Αυτό το τμήμα συζητά τρεις ιδιαίτερες περιοχές όπου καταδεικνύονται πώς τα διαφορετικά συστήματα μπορούν να χρησιμοποιήσουν τις έξυπνες κάρτες για να ενισχύσουν την ασφάλεια τους.

5.1 Προσδιορισμός των εγγράφων

Τα παραδοσιακά έγραφα που βασίζονται στο προσδιορισμό της ταυτότητας, όπως η κάρτα προσδιορισμού, οι άδειες, τα διαβατήρια/visa, και τα λοιπά, θεωρούνται πάντα αναξιόπιστα. Όλα είναι εύκολο να πλαστοποιηθούν και να αντιγραφούν. Ιδιαίτερα με τη σημερινή τεχνολογία, η υψηλής ποιότητα έγχρωμη φωτοτυπία , οι εκτυπωτές, και τα scanner προσεγγίζονται και αποκτούνται εύκολα, και κατά συνέπεια τα υψηλής ποιότητας

ψευδή έγγραφα μπορούν να παραχθούν εύκολα. Αυτό καθιστά την επιθεώρηση των εγγράφων όλο και περισσότερο δύσκολη.

Η έξυπνη κάρτα είναι πιθανώς η καλύτερη λύση για αυτό το πρόβλημα. Οι τυπωμένες πληροφορίες και οι φωτογραφίες μπορούν να ψηφιοποιηθούν και να αποθηκευτούν στην κάρτα. Με την οργάνωση των προϋποθέσεων προσπέλασης και του κωδικού πρόσβασης στα αρχεία, μόνο τα εξουσιοδοτημένα πρόσωπα ή αρχές, όπως οι κυβερνητικές υπηρεσίες, επιτρέπεται να έχουν πρόσβαση στις πληροφορίες. Επιπλέον, μαζί με την τεχνολογία της βιομετρικής, οι βιομετρικές πληροφορίες του κατόχου της κάρτας μπορούν να τοποθετηθούν στην κάρτα, έτσι ώστε η έξυπνη κάρτα να μπορεί να συνεργαστεί με τον ανιχνευτή βιομετρικών για να προσδιορίσει ή να ελέγξει εάν η κάρτα ανήκει στον κάτοχο ή όχι. Αυτό βελτιώνει σημαντικά την αξιοπιστία του εγγράφου που φέρει η έξυπνη κάρτα .

Οι διαδικασίες λειτουργίας θα μπορούσαν να είναι παρόμοιες με το παραδοσιακό έγγραφο που βασίζεται στο σύστημα της ταυτοποίησης. Εντούτοις, αντί της επαλήθευσης των εγγράφων από την εξέταση ενός λειτουργικού ελέγχου, μια συσκευή-αποδέκτης καρτών θα χρησιμοποιηθεί. Η συσκευή που περιέχει τους εξουσιοδοτημένους κωδικούς και τα PIN μπορεί να ξεκλειδώσει το αρχείο και να ανακτήσει τις πληροφορίες του ιδιοκτήτη για επαλήθευση. Στην περίπτωση όπου χρησιμοποιείται η βιομετρική, ο χρήστης μπορεί να επικυρωθεί με την τοποθέτηση του απαραίτητου μέρους του σώματός του επάνω σε έναν αναγνώστη βιομετρικής, τα στοιχεία που συλλέγονται από τον αναγνώστη μπορούν να χρησιμοποιηθούν για να συγκριθούν με αυτά της κάρτας.

Σήμερα, πολλές οργανώσεις ή κυβερνήσεις σε διάφορες χώρες έχουν ήδη ξεκινήσει την έρευνα για αυτά τα θέματα. Παραδείγματος χάριν, πολλές αερογραμμές σκοπεύουν να αναπτύξουν τα ηλεκτρονικά εισιτήριά με τη χρησιμοποίηση των έξυπνων καρτών, οι οποίες συνεργάζονται με το απαρχαιωμένο σύστημα σε μερικά αεροδρόμια. Μία έξυπνη κάρτα αποθηκεύει τυπικά τις λεπτομέρειες πτήσης του επιβάτη όπως το όνομα, τον αριθμό του καθίσματος, τον αριθμό πτήσης, λεπτομέρειες αποσκευών και τα λοιπά.

Αυτό βοηθά να ελέγξει τον επιβάτη κατά την άφιξή του και να προσδιορίσει τον ιδιοκτήτη των αποσκευών σε περίπτωση χαμένων ή αζήτητων αποσκευών. Πιο σημαντικά, το σύστημα μπορεί να βοηθήσει στην ταυτοποίηση των εγκληματιών και των τρομοκρατών.

Εν περιλήψη, αναμένεται ότι η χρησιμοποίηση των έξυπνων καρτών ως έγγραφο(τεκμήριο) ταυτοποίησης θα είναι η μελλοντική τάση που θα αντικαταστήσει τα παραδοσιακά σε χαρτί πιστοποιητικά. Οι πληροφορίες που αποθηκεύονται στην κάρτα για τον ιδιοκτήτη θα αυξάνονται και θα γίνονται όλο και περισσότερο ευαίσθητα. Επομένως, το τρέχον σύστημα ελέγχου πρόσβασης βασισμένο στην παρουσίαση του PIN μπορεί να μην είναι αρκετά ασφαλές. Προτείνεται ότι το λειτουργικό σύστημα καρτών πρέπει να συνεργαστεί με κάποιους αλγορίθμους επικύρωσης για να προστατεύσει όλα τα αρχεία ή ακόμα και ολόκληρο το σύστημα.

5.2 Έλεγχος πρόσβασης στο λειτουργικό σύστημα

Ο έλεγχος πρόσβασης είναι μια από τις σημαντικές χρήσεις των έξυπνων καρτών. Υπάρχει, επίσης, ένα κίνητρο πίσω από την ανάπτυξη της έξυπνης κάρτας. Σε αυτό το τμήμα, συζητάμε πώς να ελέγξουμε την πρόσβαση ενός λειτουργικού συστήματος σε έναν προσωπικό υπολογιστή με τη χρησιμοποίηση μιας έξυπνης κάρτας.

Οι προσωπικοί υπολογιστές έχουν έλλειψη από τη προστασία ασφάλειας στο σύστημά τους, ειδικά οι περιοχές συστήματος, όπως ο τομέας εκκίνησης ενός σκληρού δίσκου ή μιας δισκέτας. Επιτρέπεται να τροποποιηθούν από τον καθέναν χωρίς οποιαδήποτε προστασία, πράγμα το οποίο προκαλεί τη δυνατότητα μόλυνσης από ιούς. Στις μέρες μας, ένας προσωπικός υπολογιστής είναι αρκετά ισχυρός για να πάρει τη θέση των μίνι υπολογιστών για να ενεργήσει ως κεντρικός υπολογιστής δικτύων, αλλά η μοναδικού χρήστη φύση της δεν έχει αλλάξει και αυτό έχει κάνει το πρόβλημα σοβαρότερο.

Ένα ενδεικτικό σύστημα ακεραιότητας της έναρξης (Bits) εισάγεται από τον Paul και τη Lance οι οποίοι χρησιμοποιούν την τεχνολογία των έξυπνων καρτών για να προστατεύσουν το λειτουργικό σύστημα. Η βασική

ιδέα είναι ότι ο host υπολογιστής τίθεται σε έναρξη πραγματικά από μια έξυπνη κάρτα ή επιθυμεί τις κρίσιμες πληροφορίες από την κάρτα για να ολοκληρώσει την ακολουθία έναρξης, έτσι ώστε, ακόμα κι αν ένας εισβολέας μπορεί να κερδίσει τη φυσική πρόσβαση στο υλικό, είναι αδύνατο να εγγυηθεί την ακεραιότητα του συστήματος.

Η έξυπνη κάρτα διαμορφώνεται για να ζητήσει την επικύρωση χρηστών πριν από την πρόσβαση στα στοιχεία. Κατά τη διάρκεια έναρξης του συστήματος, δύο επικυρώσεις πρέπει να εκτελεσθούν πριν από την ολοκλήρωση της ακολουθίας έναρξης. Πρώτα, ο χρήστης επικυρώνεται από την έξυπνη κάρτα με τη βοήθεια ενός κωδικού πρόσβασης. Έπειτα, ο host επικυρώνει την κάρτα με την ανάγνωση του κοινού μυστικού από την κάρτα. Αφού ταιριάζουν και τα δύο, ο host διαβάζει τις πληροφορίες έναρξης από την έξυπνη κάρτα και ολοκληρώνει η ακολουθία έναρξης. Κατόπιν το PC λειτουργεί κανονικά.

Η έξυπνη κάρτα μπορεί, επίσης, να αποθηκεύσει το άθροισμα ελέγχου των κρίσιμων δεδομένων και των εκτελέσιμων προγραμμάτων. Είναι αποτελεσματικό ενάντια στους ιούς, η επικύρωση της ακεραιότητας αρχείων παρά η ανίχνευση για τις γνωστές υπογραφές των ιών. Γενικά, η χρήση της έξυπνης κάρτας ενίσχυσε την ασφάλεια του υπολογιστή με τη χρησιμοποίηση των έμφυτων ασφαλών ικανοτήτων αποθήκευσης και επεξεργασίας.

ΚΕΦΑΛΑΙΟ 10ο

ΣΥΜΠΕΡΑΣΜΑΤΑ

1. Διαδικασία ολοκλήρωσης της Έξυπνης Κάρτας

Κάθε κάρτα από την αρχή της δημιουργίας της έως και το τέλος ζωής της ακολουθούνται τα εξής βήματα:

1. Πρόσβαση στην κάρτα με τη χρήση του αρχικού της transport κλειδιού.
2. Δημιουργία των αρχικών δομών πληροφορίας.
3. Αποθήκευση των ιδιωτικών RSA κλειδιών στην κάρτα.
4. Αποθήκευση των αντίστοιχων δημοσίων κλειδιών.
5. Δημιουργία τυχαίου κωδικού PIN για τη χρήση της κάρτα στην Υ.Δ.Κ.
6. Κρυπτογράφηση του PIN με το δημόσιο κλειδί της αρχής πιστοποίησης.
7. Αποθήκευση στη κάρτα του κρυπτογραφημένου PIN.
8. Η κάρτα τίθεται σε «usage mode»
9. Έλεγχος των λειτουργιών της κάρτας με την ανάγνωση
10. Power off της κάρτας

2. Εξασφάλιση πληροφοριών & φυσικών στοιχείων

Εκτός από την ασφάλεια των πληροφοριών, οι έξυπνες κάρτες επιτυγχάνουν μεγαλύτερη φυσική ασφάλεια των υπηρεσιών και του εξοπλισμού, επειδή η κάρτα περιορίζει την πρόσβαση σε όλους, εκτός από τον εξουσιοδοτημένο χρήστη(ες). Το ηλεκτρονικό ταχυδρομείο και τα PCs έχουν πλέον εξοικειωθεί με τις έξυπνες κάρτες. Οι πληροφορίες και η ψυχαγωγία παραδίδονται μέσω του σπιτιού ή του PC. Η κατοίκον παράδοση των υπηρεσιών

κρυπτογραφείται και αποκρυπτογραφείται ανάλογα με τη πρόσβαση των συνδρομητών. Οι ψηφιακές τηλεοπτικές ασύρματες μεταδόσεις αποδέχονται τις έξυπνες κάρτες ως ηλεκτρονικά κλειδιά για την προστασία. Οι έξυπνες κάρτες μπορούν, επίσης, να ενεργήσουν ως κλειδιά στη τοποθέτηση των μηχανών για τον ευαίσθητο εργαστηριακό εξοπλισμό και τους διανομείς των φαρμάκων, εργαλείων, των καρτών βιβλιοθήκης, των συλλόγων υγειονομικού εξοπλισμού κ.λ.π....

2.1. Ηλεκτρονικό εμπόριο

Οι έξυπνες κάρτες το καθιστούν εύκολο για τους καταναλωτές, την ασφαλή καταχώρηση των πληροφοριών και των μετρητών για τις αγορές. Τα πλεονεκτήματα που παρέχουν στους καταναλωτές είναι:

- η κάρτα μπορεί να φέρει κάποιο προσωπικό λογαριασμό, πληροφορίες εκτίμησης και αγοραστικές προτιμήσεις που μπορούν να προσεγγιστούν με ένα χτύπημα του ποντικιού αντί να συμπληρώνουν(filling out) φόρμες.
- οι κάρτες μπορούν να διαχειριστούν και να ελέγξουν τις δαπάνες, με τα αυτόματα όρια και τις αναφορικές εκθέσεις.
- Με τα συστήματα POS και τη κάρτα που ενεργεί ως ασφαλής κεντρικός χώρος κατάθεσης πόντων ή ανταμοιβών, τα προγράμματα πίστης του Διαδικτύου(loyalty programs) μπορούν να επεκταθούν σε πολλαπλούς προμηθευτές.
- "οι μικροπληρωμές " - πληρώνουν το ονομαστικό κόστος χωρίς την αμοιβή της συναλλαγής που συνδέεται με τις πιστωτικές κάρτες ή για ποσά που είναι πάρα πολύ μικρά για μετρητά.

2.2. Προσωπική χρηματοδότηση

Καθώς οι τράπεζες εισάγουν τον ανταγωνισμό στις πρόσφατα ανοιγμένες αγορές όπως τις μεσιτικές αμοιβές από τις επενδύσεις, εξασφαλίζουν τις συναλλαγές μέσω των έξυπνων καρτών μ' ένα αυξανόμενο ποσοστό. Αυτό σημαίνει ότι:

- Θα βελτιώσει την υπηρεσία πελατών. Οι πελάτες μπορούν να χρησιμοποιούν ασφαλισμένα τις έξυπνες κάρτες για γρήγορες, εικοσιτετράωρες ηλεκτρονικές μεταφορές κεφαλαίων μέσω του Διαδικτύου.
- το κόστος μειώνεται: οι συναλλαγές που κανονικά θα απαιτούσαν χρόνο και γραφική εργασία ενός τραπεζικού υπαλλήλου, μπορούν να ρυθμιστούν ηλεκτρονικά από τον πελάτη με μια έξυπνη κάρτα.

2.3. *Η υγειονομική περίθαλψη*

Η έκρηξη των δεδομένων της υγειονομικής περίθαλψης φέρνει νέες προκλήσεις στην αποδοτικότερη φροντίδα των ασθενών και την ιδιωτικότητα τους. Οι έξυπνες κάρτες λύνουν και τις προκλήσεις με την ασφαλή αποθήκευση και την διανομή των πάντων από τα στοιχεία έκτακτης ανάγκης μέχρι τη κατάσταση ωφελημάτων τους.

- γρήγορη ταυτοποίηση των ασθενών και βελτιωμένη θεραπεία
- ένας εύκολος τρόπος μεταφοράς των δεδομένων μεταξύ των συστημάτων ή σε περιοχές χωρίς συστήματα
- μείωση του κόστους συντήρησης αρχείων.

2.4. *Τηλεργασία και εταιρική ασφάλεια των δικτύων*

Τα δίκτυα Intranet μεταξύ των επιχειρήσεων και τα ιδεατά ιδιωτικά δίκτυα "VPNs" ενισχύονται με την χρήση των έξυπνων καρτών. Οι χρήστες μπορούν να επικυρωθούν και να εγκριθούν για να έχουν πρόσβαση σε συγκεκριμένες πληροφορίες που βασίζονται στα πρωτοποθετημένα προνόμια. Πρόσθετες εφαρμογές κυμαίνονται από το ασφαλές ηλεκτρονικό ταχυδρομείο μέχρι το ηλεκτρονικό εμπόριο.

2.5. *Πανεπιστημιούπολη Badging και πρόσβαση*

Οι επιχειρήσεις και τα πανεπιστήμια όλων των τύπων χρειάζονται απλές κάρτες ταυτότητας για όλους τους υπαλλήλους και τους σπουδαστές. Στους περισσότερους από αυτούς τους ανθρώπους τους χορηγείται επίσης πρόσβαση σε κάποια δεδομένα, εξοπλισμό και τμήματα, σύμφωνα με τη

θέση που κατέχουν. Οι πολλαπλής λειτουργίας, έξυπνες κάρτες που βασίζονται στο μικροεπεξεργαστή ενσωματώνουν την ταυτότητα με τα προνόμια πρόσβασης και καταχωρούν, επίσης, κάποια αξία για χρήση της στις διάφορες περιοχές, όπως τις καφετέριες και τα καταστήματα.

Ο σκοπός της τεχνολογίας των έξυπνων καρτών είναι να παράσχουν στη συζήτηση για τη τεχνολογία, τις εφαρμογές και τα ζητήματα που συνδέθηκαν με τις έξυπνες κάρτες. Θα μπορεί να εξυπηρετήσει ως στοιχείο συμπεριφοράς για τους ανθρώπους ώστε:

- Να δεσμεύσει τη συμμετοχή στη συζήτηση για ζητήματα τεχνικής και δημόσιας πολιτικής συμπεριλαμβανομένης της ασφάλειας, της ιδιωτικότητας, του νομικού, ρυθμιστικού και οικονομικού αντίκτυπου των εφαρμογών των έξυπνων καρτών.
- Να εκπαιδεύσει και να ενημερώσει τους υπόλοιπους σχετικά με τη δυνατότητες ,αδυναμίες και τη γενική χρήση των έξυπνων καρτών.
- να μοιραστεί τις ιδέες, τις πληροφορίες και συγκεκριμένες εμπειρίες για τις έξυπνες κάρτες.

3. Λόγοι χρήσης - Πλεονεκτήματα έξυπνων καρτών

Όπως είναι εμφανές από τα παραπάνω, η νέα τεχνολογία καρτών, η οποία σταδιακά εισάγεται σε κάθε δραστηριότητα της καθημερινότητας, διευκολύνει τους κατόχους της, αφού χαρακτηρίζεται από πληθώρα στοιχείων σε σύγκριση με τις παλαιότερες γενιές. Συγκεκριμένα, η χρήση τέτοιων καρτών δικαιολογείται από τους εξής λόγους:

1. Ταυτοποίηση &. ανθεντικοποίηση του χρήστη: Τα παραπάνω επιτυγχάνονται εύκολα χάρη στην πληθώρα ασφαλιστικών κλειδιών που μπορεί να διαθέτει μία έξυπνη κάρτα.
2. Παροχή μεγαλύτερης ασφάλειας: Οι κάρτες smart χαρακτηρίζονται από ικανότητα προστασίας των δεδομένων τους από ενδεχόμενες απάτες ή καταστροφές, χάρη σε ποικίλες μεθόδους. Η παρεχόμενη ασφάλεια μπορεί να είναι πολυεπίπεδη με ύπαρξη ανάλογου αριθμού ασφαλιστικών κλειδιών (π.χ. PIN), τα οποία και να επιτρέπουν την πρόσβαση σε αντί-

στοιχες εφαρμογές του δικτύου που χρησιμοποιείται. Εναλλακτικά, εφόσον ο μικροεπεξεργαστής είναι ενσωματωμένος στη κάρτα, η παραβίαση της είναι αδύνατη χωρίς την καταστροφή του - σε αντίθεση με τις κάρτες τύπου magnetic stripe , οι οποίες περιέχουν τα δεδομένα στο εξωτερικό της κάρτας, με αποτέλεσμα την εύκολη αντιγραφή τους. Επιπλέον, πολλές εφαρμογές που απευθύνονται για smart cards αποτρέπουν την παρακολούθηση της πρόσβασης από άλλα άτομα, τα οποία δεν έχουν την αρμοδιότητα. Τέλος, η απουσία ρευστού χρήματος από έξυπνες κάρτες (smart cards), που χρησιμοποιούνται για τραπεζικές συναλλαγές εξαλείφει τον κίνδυνο οποιασδήποτε κλοπής χρημάτων από τον κάτοχο της κάρτας.

3. Δυνατότητα υλοποίησης διαφορετικών εφαρμογών(multi-application): οι κάρτες τύπου smart εκτελούν πολλαπλές και διαφορετικές εφαρμογές με απίστευτη απλότητα-αντίθετα με τις άλλες κάρτες- λόγω κυρίως της κενότητας αποθήκευσης κι επεξεργασίας των δεδομένων που διαθέτουν.
4. Απλοποίηση διαδικασιών: Εφαρμογές της καθημερινότητας μπορούν να πραγματοποιηθούν εξαιρετικά απλά με χρήση έξυπνων καρτών, όπως προπληρωμένες κάρτες διοδίων, κάρτες μεταφοράς ή συγκοινωνιών.
5. Μείωση κόστους διαδικασιών: Η μείωση του κόστους που επιφέρει η χρήση τους, όπως κόστος προσωπικού, διαχείρισης εγγράφων, χρονικό κόστος κ.λ.π επιβάλλει την ευρύτερη χρήση των έξυπνων καρτών.
6. Μεταφερσιμότητα: Το μικρό μέγεθος των παραπάνω καρτών, σε συνδυασμό με τις πολύπλοκες εφαρμογές σης οποίες χρησιμοποιούνται, καθιστά ιδιαίτερα ευκολόχρηστη την τεχνολογία των παραπάνω καρτών.

4. Μειονεκτήματα - Προβλήματα

Τα πλεονεκτήματα των smart cards είναι πολυάριθμα κι εμφανή σε κάθε εφαρμογή που χρησιμοποιούνται. Από την άλλη, όμως, μεριά αναμφισβήτητα οι έξυπνες κάρτες χαρακτηρίζονται από ολιγάριθμα μεν, αλλά κυριότατα μειονεκτήματα, όπως:

1. Εμπιστευτικότητα: Το σημαντικότερο θέμα στη χρήση καρτών αποτελεί η προστασία της εμπιστευτικότητας (confidentiality) των δεδομένων που είναι αποθηκευμένα στην κάρτα, καθώς κι ο περιορισμός της πρόσβασης σε αυτά. Μάλιστα, πολλά προγράμματα για την ανάκτηση δεδομένων προϋποθέτουν την ύπαρξη ενός φορητού τερματικού (π.χ. σε μία επίσκεψη του ιατρού στο σπίτι ή κατά τη διάρκεια γρήγορης επιθεώρησης της κατάστασης των ασθενών από τον ιατρό σε ένα νοσοκομείο).
2. Διάθεση πληροφορίας: Ένα άλλο πρόβλημα που εμφανίζεται σε όλες σχεδόν τις εφαρμογές των έξυπνων καρτών είναι η ύπαρξη αμφιβολιών από το κοινό, καθώς πολλοί άνθρωποι θεωρούν απαραίτητη την κατανόηση όλων των πληροφοριών που υπάρχουν στο αρχείο τους, ενώ παράλληλα επιθυμούν να ελέγχουν τα άτομα που βλέπουν τις πληροφορίες. Τα παραπάνω συνήθως είναι μη εφικτά, αφού οι πληροφορίες είναι αποθηκευμένες με κωδικούς ή λέξεις κλειδιά, στοιχεία τα οποία δεν είναι κατανοητά.
3. Ασυμβατότητα εφαρμογών: Παράγοντα ιδιαίτερα σημαντικό, για την ανάπτυξη των εφαρμογών έξυπνων καρτών αποτελεί η μη συμβατότητα των καρτών σε κάποια συστήματα. Αυτό συμβαίνει, γιατί αν και έχουν δημιουργηθεί κάποια πρότυπα, οι διάφοροι οργανισμοί χρησιμοποιούν διαφορετικά συστήματα υπολογιστών, σχεδιασμένα να πληρούν συγκεκριμένες απαιτήσεις. Ως επακόλουθο, παρατηρούνται τεράστια κενά στην αλυσίδα των υπηρεσιών και κρίνεται αναγκαία η παρέλευση αρκετού χρόνου, ώσπου να υπάρξει ομοιομορφία σε όλα τα συστήματα που χρησιμοποιούνται.
4. Ομοιομορφία δεδομένων: Είναι γεγονός, ότι δε μπορούν να εισαχθούν όλες οι πληροφορίες σε μία κάρτα με την ίδια μορφή. Πολλές φορές, είναι αναγκαία η αποθήκευση κι άλλων επιπρόσθετων δεδομένων, όπως κειμένων ή εικόνων, τα οποία θεωρούνται πολλές φορές άκρως σημαντικά.
5. Καταστροφή - απώλεια κάρτας: Στις περιπτώσεις αυτές, συνήθως λαμβάνει χώρα η επανακατασκευή της κάρτας, με λεπτομερή εξέταση των προ-

σωπικών δεδομένων του εξουσιοδοτημένου χρήστη. Επειδή, όμως, κάποιες φορές η παραπάνω λύση είναι ανέφικτη, συνήθως διενεργείται αντιγραφή των αρχείων του χρήστη από το σύστημα σε άλλο αρχείο, προκειμένου να καλυφθούν οι περιπτώσεις απώλειας ή καταστροφής.

6. Υψηλό οικονομικό κόστος κατασκευής, το οποίο εμποδίζει κατά κάποιο τρόπο την ευρύτερη χρήση των έξυπνων καρτών στις πολυπλοκότερες εφαρμογές.
7. Αδυναμία αποθήκευσης μεγάλου όγκου δεδομένων, όπως για παράδειγμα ιατρικών εικόνων ή λεπτομερών στοιχείων για το χρήστη, που διευκολύνουν τη χρήση των καρτών αυτών.
8. Δυσκολία επιβολής κοινά αποδεκτών τεχνολογικών προτύπων, καθώς πριν την ευρεία χρησιμοποίηση των παραπάνω καρτών, οι δημόσιοι κι ιδιωτικοί τομείς θα πρέπει να εγκρίνουν κι εγκαθιδρύσουν ένα συγκεκριμένο τεχνολογικό πρότυπο. Η δυσκολία υλοποίησης των παραπάνω επιβαρύνεται από τη πολλαπλή χρήση τους σε διαφορετικές γεωγραφικές περιοχές, οι οποίες χαρακτηρίζονται από ιδιαιτερότητες και διαφορετικά πρότυπα.
9. Ανάγκη ύπαρξης περιφερειακών συστημάτων ανάγνωσης έξυπνων καρτών, γεγονός που δυσχεραίνει την ευρύτερη χρήση των καρτών, λόγω υπερβολικής αύξησης του κόστους λειτουργίας.
10. Υψηλό αρχικό κόστος υποδομής, αφού η κοινωνία έχει εμπιστευτεί τις προηγούμενες τεχνολογίες καρτών για πολλά χρόνια κι είναι εξαιρετικά δύσκολο να προσαρμοστούν οι χρήστες σε τόσο σύντομο χρονικό διάστημα. Οπωσδήποτε, η παραπάνω δυσκολία εντείνεται λόγω και του αρχικά υψηλού οικονομικού κόστους, όμως όπως κάθε νέα τεχνολογία θεωρείται λογική η μείωση του κόστους κατασκευής της στο άμεσο μέλλον.

Μέθοδοι προστασίας-Πληροφορίες γενικής χρήσης

✖ υπογράψτε την κάρτα σας -- μόλις την λάβετε

✖ όταν χρησιμοποιείτε την κάρτα σας στο ATM, εισάγετε το PIN σας κατά τέτοιο τρόπο, ώστε, κανένας να μη μπορεί να απομνημονεύσει εύκολα τις πληκτρολογήσεις σας.

✖ μην αφήνετε την απόδειξη σας πίσω στο ATM.

✖ Το PIN και ο αριθμός λογαριασμού σας από μια πεταμένη απόδειξη, θα μπορούσε να σας καταστήσει ευάλωτους στην απάτη πιστωτικών καρτών. Επίσης, μην πετάτε την κατάσταση λογαριασμού της πιστωτικής σας κάρτας, αποδείξεις ή αντίγραφα, χωρίς πρώτα να τα αχρηστεύσετε!

✖ ποτέ να μην δίνεται τον αριθμό της πιστωτικής σας κάρτας μέσω τηλεφώνου εκτός αν εσείς αρχίσατε την κλήση. Ακόμα και αν καλέσατε έναν νόμιμο έμπορο (όπως μια επιχείρηση ηλεκτρονικών ταχυδρομικών παραγγελιών), ποτέ να μην δώσετε τον αριθμό της κάρτας σας προς τα έξω μέσω ενός ασύρματου τηλεφώνου. Ασύρματοι σαρωτές που κρυφακούνε αυτές τις συνομιλίες είναι διαθέσιμοι για λίγες εκατοντάδες ευρώ σε οποιοδήποτε κατάστημα ηλεκτονικών και η φωνή σας μπορεί να ληφθεί από κάποιον, από πολύ μεγαλύτερη απόσταση απ' ότι τη μέγιστη χρήσιμη εμβέλεια του ασύρματου τηλεφώνου σας. Ένα κοινό scam είναι όταν κάποιος σας καλεί "πίσω" , αφού υποβάλετε μια παραγγελία ,ισχυριζόμενος ότι είναι από μέρους του έμπορου και σας λεει ότι υπήρξε ένα πρόβλημα με τον αριθμό της κάρτας σας -- θα σας πείραζε να του τον ξαναδίνατε; Το καλύτερο πράγμα που θα κάνατε θα ήταν να ζητήσετε ένα όνομα επαφής και να τηλεφωνήσετε πίσω στον έμπορο, στον αριθμό που είχατε χρησιμοποιήσει αρχικά.

✖ αγνοήστε οποιαδήποτε προσφορά πιστωτικών καρτών που απαιτούν να δώσετε μπροστά προκαταβολή ή αποτυγχάνουν να αποκαλύψουν την ταυτότητα του εκδότη των καρτών.

✖ Σιγουρευτείτε ότι πήρατε πίσω την κάρτα σας αφότου κάνετε μια αγορά (μια συνήθεια που πρέπει να ακολουθείτε είναι να αφήνετε το πορτοφόλι σας ανοικτό στο χέρι σας έως ότου πάρετε πίσω την κάρτα σας). Επίσης, σιγουρευτείτε ότι σχίζετε προσωπικά οποιεσδήποτε άχρηστες ή ακυρωμένες λανθασμένες πωλήσεις.

✖ πάντα να κρατάτε ένα κατάλογο με τις πιστωτικές σας κάρτες, τους αριθμούς των πιστωτικών σας καρτών και τον αριθμό ατέλειας τους σε περίπτωση που κλαπεί η κάρτα σας ή χαθεί

✖ ελέγχεται τη μηνιαία κατάσταση των πιστωτικών σας καρτών για να βεβαιωθείτε ότι όλα τα έξοδα είναι δικά σας και ειδοποιήστε αμέσως τον εκδότη των καρτών αν υπάρχουν λάθη ή αναρμόδια έξοδα.

ΕΠΙΛΟΓΟΣ

Κάποιοι τύποι προβλημάτων που μπορούν να αποτελέσουν μια απειλή για το ενεργητικό του συστήματος των έξυπνων καρτών περιλαμβάνουν:

- ακατάλληλους για τη ασφάλεια κωδικούς πρόσβασης (γράφοντας τους κάτω, διαμοιράζονται).
- Τα προσδιορισμένα PINs και οι μηχανισμοί αντικατάστασης
- εξουσιοδοτημένες υπηρεσίες πιστοποίησης ταυτότητας
- φτωχή καταμερισμός των δεδομένων
- φυσική ασφάλεια (η φυσική αφαίρεση ή η καταστροφή του υλικού υπολογισμού σας).

Ζούμε σε έναν κόσμο γρήγορης τεχνικής αλλαγής.. Η διαβίβαση της συμβατότητας και η διασυνοριακή και διασταύρωση της διαλειτουργικότητας του σχεδίου είναι όλο και περισσότερο δύσκολο να διατηρηθεί στα πλαίσια της γρήγορης ανάπτυξης της τεχνολογίας των τσιπ. Το EEPROM μπορεί να δώσει λύση στη γρηγορότερη και μακροβιώσιμη μνήμη. Η τάση για την ισχύ των έξυπνων καρτών μειώνεται σχεδόν ετησίως. Οι τεχνολογίες ασφάλειας απαιτούν την πάντα γρηγορότερη δύναμη επεξεργασίας. Αυτό το περιβάλλον καθιστά εξαιρετικά δύσκολη τη βέβαιη ανάπτυξη, την απόκτηση και την επέκταση των έξυπνων καρτών που για να υποστηρίξουν οποιαδήποτε λογική επιχειρησιακή περίπτωση, πρέπει να θεωρηθούν ως μακροπρόθεσμα σημεία.

Τα τσιπ έξυπνων καρτών είναι το ουσιαστικό λειτουργικό συστατικό των έξυπνων καρτών και αυτό εμφανίζεται, επίσης, στην επικάλυψη εκτός από τις κάρτες μεγέθους πιστωτικής, στα πλαστικά σημεία. Οι SIMs (Ενότητες Ταυτοτήτων Συνδρομητών, που υλοποιούνται αρχικά με απλή, ενιαία

εφαρμογή των τσιπ των έξυπνων καρτών) με ένα μικρότερο φυσικό σχήμα ενσωματώνεται ήδη σε όλες τις GSM τηλεφωνικές συσκευές και οι νέες εξελίξεις ενσωματώνουν τα έξυπνα τσιπ μέσα σε ποικίλες άλλες συσκευές όπως τα PDAs και τα ρολόγια καρπού.

Υπάρχουν, επίσης, εμπορικές εξελίξεις που επιδιώκουν να τοποθετήσουν το ηλεκτρονικό πορτοφόλι και άλλες παρόμοιες ευκολίες μέσα σε περιβάλλον λογισμικού σε PCs και κεντρικούς υπολογιστές, που προλαμβάνουν την ανάγκη για την επέκταση των έξυπνων καρτών. Μένει να φανεί ποια από αυτές τις πρωτοβουλίες λογισμικού θα ακμάσει, ιδιαίτερα αφού είναι δύσκολο να εξασφαλιστεί η ασφάλειά τους.

Η φυσική και λογική δομή μιας έξυπνης κάρτας και του αντίστοιχου ελέγχου πρόσβασης ασφάλειας έχει συζητηθεί σε αυτό το άρθρο. Θεωρείται ότι οι έξυπνες κάρτες προσφέρουν περισσότερη ασφάλεια και εμπιστευτικότητα από τα άλλα είδη αποθήκευσης πληροφοριών ή συναλλαγής. Επιπλέον, οι εφαρμογές των έξυπνων καρτών καταδεικνύουν ότι μία έξυπνη κάρτα είναι μια από τις καλύτερες λύσεις για να παρέχει και να ενισχύσει στο σύστημα την ασφάλεια και την ακεραιότητα.

Στο τέλος του εγγράφου, μια επισκόπηση των τεχνικών επίθεσης στην έξυπνη κάρτα συζητείται, επίσης. Η ύπαρξη αυτών των επιθέσεων δεν σημαίνει ότι μια έξυπνη κάρτα είναι ανασφαλής. Είναι σημαντικό να συνειδητοποιήσουμε ότι οι επιθέσεις ενάντια σε οποιαδήποτε ασφαλή συστήματα δεν είναι καινούργιες ή μοναδικές. Οποιαδήποτε συστήματα ή τεχνολογίες που ισχυρίζονται 100% ασφάλεια είναι αναξιόπιστα. Η κύρια εκτίμηση του καθορισμού εάν ένα σύστημα είναι ασφαλές ή όχι εξαρτάται από το εάν το επίπεδο ασφάλειας μπορεί να καλύψει την απαίτηση του συστήματος.

Επιπλέον, οι δαπάνες που συνδέονται για να σπάσουν το σύστημα είναι πολύ μεγαλύτερες από ότι είναι το κόστος του ίδιου του συστήματος ή πρέπει να σπαταληθούν αρκετά έτη υπολογισμού της δύναμης προκειμένου να σπάσει σε μια ενιαία συναλλαγή. Καθώς η τεχνολογία προχωράει γρήγορα, οι κατασκευαστές αναπροσαρμόζονται και ενισχύουν τα προϊόντα τους συνεχώς. Τέλος, συνάγεται το συμπέρασμα ότι οι έξυπνες κάρτες είναι

πραγματικά ασφαλής συσκευές. Είναι μια ασφαλής θέση για να αποθηκευτούν πολύτιμες πληροφορίες όπως τα ιδιωτικά κλειδιά, οι αριθμοί λογαριασμών, πολύτιμα προσωπικά στοιχεία, όπως πληροφορίες βιομετρικής.

Οι έξυπνες κάρτες αποτελούν, επίσης, ένα ασφαλές σημείο για να εκτελεστούν οι off-line διαδικασίες, τέτοιες όπως τα δημόσια ή ιδιωτικά κλειδιά κρυπτογράφησης και αποκρυπτογράφησης. Οι έξυπνες κάρτες αποτελούν ένα στοιχείο στη επίλυση του προβλήματος της ασφάλειας στο σύγχρονο κόσμο.

Οι έξυπνες κάρτες έγιναν σημαντικά και χρήσιμα εργαλεία της ασφάλειας για τη χρήση τους στο περιβάλλον του PC. Αυτές οι απλές, αλλά και ισχυρές συσκευές μπορούν να προγραμματιστούν για να παρέχουν κάποιο βαθμό ασφαλείας στις διάφορες σχετικές εργασίες, που κυμαίνονται από την ταυτοποίηση των χρηστών μέχρι και την εξασφαλισμένη μεταφορά μέσω του δικτύου. Οι νέες έξυπνες κάρτες JAVA και PC/SC παρέχουν σχεδόν απεριόριστες δυνατότητες για τις εφαρμογές του PC. Με τα επαγγελματικά Microsoft Windows 2000 παρέχεται εγγενής υποστήριξη και αναμένεται να ακολουθήσουν κι' άλλα Oss. Η τεχνολογία των έξυπνων καρτών ενδέχεται να γίνει ένα επικρατέστερο εργαλείο στη βιομηχανία των υπολογιστών.

ΒΙΒΛΙΟΓΡΑΦΙΑ-ΙΣΤΟΣΕΛΙΔΕΣ

Εισαγωγή

ΒΙΒΛΙΑ

1)Ντούσκος Π.: Η επιστημονική τεχνική πρόοδος στον σύγχρονο κόσμο, Εκδόσεις Gutenberg ,Αθήνα 1996

2)Σημειώσεις Πληροφορική και Κοινωνία, Μαυρομμάτης Ελευθέριου

Συστήματα ηλεκτρονικών πληρωμών

Ιστοσελίδες

http://www.noesis.se/ed/cmiedd10.htm

http://www.noesis.se/ed/cmiedd20.htm

http://www.noesis.se/ed/cmiedd30.htm

http://www.noesis.se/ed/cmiedd40.htm

http://www.howstuffworks.com

Ορισμός, χρήση και εφαρμογές

ΒΙΒΛΙΑ

Schnorr C.P., Efficient Signature Generation for Smart Cards, Journal of Cryptology

Ιστοσελίδες

http://www.howstuffworks.com

Λογισμικό έξυπνων καρτών

ΒΙΒΛΙΑ

Schnorr C.P., Efficient Signature Generation for Smart Cards, Journal of Cryptology

Ιστοσελίδες

http://www.howstuffworks.com

Αναγνώστες έξυπνων καρτών

ΒΙΒΛΙΑ

Schnorr C.P., Efficient Signature Generation for Smart Cards, Journal of Cryptology

Βιομετρική

Σημειώσεις από πανεπιστήμιο Πάτρας, Μαράντης Διονύσιος

Ιστοσελίδες

http://www.ram.com

Ασφάλεια

ΒΙΒΛΙΑ

Digital signature standard (DSS, Announced in Federal Register)

Γκρίτζαλης Δ. , Ασφάλεια Πληροφοριακών Συστημάτων σε περιβάλλοντα Υψηλής ευπάθειας. Διδακτορική διατριβή ,Πανεπιστήμιο Αιγαίου, Μάιος 1994

Οι τεχνολογίες πληροφορικής στο ελληνικό τραπεζικό σύστημα , Μελέτη της ΕΠΥ, Φεβρουάριος 1994

Β. Χρυσικόπουλος: Σημειώσεις από το μάθημα Ασφάλεια Πληροφοριακών Συστημάτων.

Communications-Interworking - Of The ACM

Κρυπτογραφία

ΒΙΒΛΙΑ

1)Schneier B. , Applied Cryptography: Protocols, algorithms and source code in C, Wiley, 1994.

2)Davida G., Desmedt Y, Matt B, Defending Systems against Viruses throw Cryptographic Authentication

3)Γκρίτζαλης Δ. , Ασφάλεια Πληροφοριακών Συστημάτων σε περιβάλλοντα Υψηλής ευπάθειας. Διδακτορική διατριβή ,Πανεπιστήμιο Αιγαίου, Μάιος 1994

Communications-Interworking - Of The ACM

4)DE JORGE , W.. and Chaum, D.:"Some Variations in RSA signatures and Their Security ." in Advances in Cryptology-CRYPTO 1986 Proeedings, Odlyzko, A.M. (Ed.), New York: Springer Verlag, 1987

Υποκλοπή

ΒΙΒΛΙΑ

1)Γκρίτζαλης Δ. , Ασφάλεια Πληροφοριακών Συστημάτων σε περιβάλλοντα Υψηλής ευπάθειας. Διδακτορική διατριβή ,Πανεπιστήμιο Αιγαίου, Μάιος 1994

2) R. Moses ,"A European Standard for Risk Analysis", in Proceedings, 10th World Conference on Computer Security, Audit and Control, Elsevier Advanced Technology, 1993