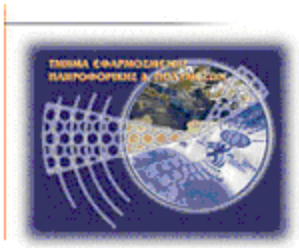
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών

Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων



Πτυχιακή εργασία

Ανάπτυξη ασφαλών εφαρμογών με τη χρήση έξυπνων καρτών

Παπαδέας Ν.Σ.Γ Δημήτριος ΑΜ 1272

Ηράκλειο 2008-2009

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος

Περίληψη

Η ακόλουθη πτυχιακή εργασία αποτελεί μία μελέτη των έξυπνων καρτών (Smart cards) σε ένα ευρύ περιβάλλον χρήσεων και εφαρμογών. Οι έξυπνες κάρτες αποτελούν ένα μέσο ενίσχυσης της ασφάλειας ενός ευρύτερου υπολογιστικού συστήματος ή δικτύου. Χρησιμοποιούνται είτε σε εμπορικές εφαρμογές είτε σε εφαρμογές ελέγχου πρόσβασης. Υπάρχουν διάφοροι τύποι καρτών όπως κάρτα επαφών (contact card) με ενσωματωμένο εξωτερικό chip ή ασύρματες κάρτες (wireless card) που υλοποιούν συναλλαγές από απόσταση μερικών δεκάδων εκατοστών. Οι περιστερές κάρτες έχουν δικό τους λειτουργικό σύστημα και σύστημα αρχείων. Η έξυπνη κάρτα Gemsafe, αποτελεί εμπορικό προϊόν της Gemplus-Gemalto, η οποία είναι η μεγαλύτερη εταιρία στην κατασκευή λογισμικού για κάρτες και συστημάτων ασφαλείας με smart cards. Η Gemsafe έχει το λειτουργικό σύστημα GPK και έχει μνήμη 16 Kilobytes και είναι πλήρως συμβατή με όλα τα προγράμματα της Gemalto. Οι αναγνώστες έξυπνων καρτών αποτελούν το υλικό τμήμα διασύνδεσης μεταξύ μίας κάρτας και ενός συστήματος. Ανάλογα με την περίπτωση υπάρχουν αναγνώστες για κάθε τύπο κάρτας. Οι GemSafe Libraries αποτελούν ένα πακέτο βιβλιοθηκών που υποστηρίζουν πολλές από τις πολύπλοκες συναλλαγές μεταξύ της κάρτας και του συστήματος, όπως επίσης πάνω σε αυτές τις βιβλιοθήκες έχουν αναπτυχθεί πολλά προγράμματα ελέγχου πρόσβασης και διαχείρισης καρτών. Επιπλέον οι GemSafe Libraries αποτελούν και μέσο επέκτασης της χρήσης μίας κάρτας λειτουργώντας ως διασυνδετικός κρίκος μεταξύ της κάρτας και τρίτων εφαρμογών όπως browsers και mail clients. Τέλος και η Java υποστηρίζει τον προγραμματισμό των καρτών και των εφαρμογών για κάρτες με τα Java card api και javax.smartcardio api αντίστοιχα, βοηθώντας σημαντικά και μειώνοντας αισθητά την πολυπλοκότητα και την δυσκολία ανάπτυξής μίας εφαρμογής σε κάρτα(ή για κάρτα) σε σχέση με την C++.

Abstract

The following thesis is a study of Smart cards in a wide range of uses and applications. Smart cards are a means of strengthening the security of a larger computer system or network. Smart cards are usually used in financial applications or access control applications. There are different types of cards like contact cards with an embedded chip or external wireless cards (wireless card) transactions carried out by a distance of some tens of centimeters. Most cards have their own operating and file system. Gemsafe smart card is a commercial product of Gemplus-Gemalto, which is the largest company in smart card manufacturing and software for security systems with smart cards. Gemsafe card has its own operating system GPK and has 16 Kilobytes of memory and is fully compatible with all Gemalto programs. Smart card readers are the main part of the hardware between a card and a system. There are many readers for each type of card. The GemSafe Libraries are a package of libraries that support many of the complex transactions between card and system, as well on these libraries have developed several programs to access control and card management. Furthermore GemSafe Libraries are also a way of extending the use of a card acting as a link between the interconnector and the third party card applications as browsers and mail clients. Finally, Java, programming language, supports card programming and card application development by developing Java card api and javax.smartcardio api respectively, helping significantly by reducing the complexity and difficulty in card applications development.

Ευχαριστίες

Με την ολοκλήρωση της πτυχιακής μου εργασίας, θα ήθελα να ευχαριστήσω όλους τους ανθρώπους οι οποίοι βοήθησαν στην περάτωση αυτής της εργασίας. Θα ήταν παράλειψη να μην αναφερθώ σε όλους εκείνους που μου συμπαραστάθηκαν σε αυτήν την προσπάθεια.

Κατά κύριο λόγω, θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου από το Τ.Ε.Ι Κρήτης Δρ. Μανιφάβα Χαράλαμπο, ο οποίος με υποστήριξε καθ' όλη τη διάρκεια της πτυχιακής εργασίας και μου εξασφάλισε την παροχή πλούσιας υλικοτεχνικής υποδομής, πολύτιμης για μια μελέτη όπως αυτή.

Θα ήθελα να ευχαριστήσω ιδιαίτερος τους γονείς μου, Γεώργιο-Νικηφόρο-Σταμάτη και Αγγελική για την εμπιστοσύνη και την υποστήριξη τους σε κάθε επιλογή μου.

Επίσης θα ήθελα να ευχαριστήσω τους Άρη Καράμ, Μιχάλιτσα Ευθυμίου, Αιμιλία Γρηγορακάκη, Οδυσσέα Παπαδέα , Ελένη Παπαδέα, Ιακωβίνα Καπινίαρη, Νικόλαο Παπαδόπουλο, Δημήτριο Παπαδάκη, Ιωάννη Κλωνάτο, Σταύρο Πασσά, Ευάγγελο Μάγγα, Ειρήνη τριγώνη, Σταυρόπουλο Κωνσταντίνο και Αργυρώ Παπαντωνάκη για την βοήθεια και την απεριόριστη ψυχολογική υποστήριξη και κατανόηση που μου παρείχαν όποτε αυτή χρειάστηκε.

Ηράκλειο, Φεβρουάριος 2009

Παπαδέας Ν.Σ.Γ Δημήτριος

Περιεχόμενα

Πίνακας εικόνων

Πίνακας πινάκων

1. Εισαγωγή

Τα τελευταία χρόνια η ασφάλεια των δεδομένων έχει γίνει ζωτικής σημασίας, τεράστια χρηματικά ποσά και προσωπικά δεδομένα έχουν χαθεί από επιθέσεις ή από κενά ασφαλείας σε κάποιο σύστημα. Το τραπεζικό σύστημα υποφέρει από απάτες αντιγραφής μαγνητικών καρτών χάνοντας εκατομμύρια δολάρια κάθε χρόνο, πολλές εταιρίες πληρώνουν πανάκριβα δύσχρηστα μέσα ελέγχου πρόσβασης είτε καταφεύγουν σε οικονομικές και όχι αποτελεσματικές λύσεις. Ένα αποτελεσματικό μέσο για την ενίσχυση των συστημάτων ασφαλείας αποτελούν οι smart cards, μια τεχνολογία που δεν είναι πρόσφατη αν σκεφτεί κάνεις ότι το αυτοματοποιημένο chip της κάρτας εφευρέθηκε από το γερμανό επιστήμονα Helmut Gröttrup και τον συνάδελφό του Jürgen Dethloff το 1968, όμως το δίπλωμα ευρεσιτεχνίας εκδόθηκε τελικά το 1982. Οι smart cards είναι ένα συνεχώς εξελισσόμενο υποσύστημα αναβάθμισης της ασφαλείας ενός ευρύτερου συστήματος με ενσωματωμένους διάφορους μηχανισμούς ασφαλείας ενώ παράλληλα οι smart cards εκ φύσεως είναι ασφαλέστερα μέσα από τις απλές μαγνητικές κάρτες.

1.1 Στόχος της εργασίας

Η εργασία που πραγματοποιήθηκε έχει σαν στόχο την μελέτη των έξυπνων καρτών σε ένα ευρύτερο περιβάλλον χρήσεων και εφαρμογών, ειδικότερα να εξετάζει τις έξυπνες κάρτες σαν εργαλείο ασφαλείας και τις δυνατότητες τους, το περιβάλλον τους και τα πρότυπα που τις αφορούν. Όπως επίσης την μελέτη του περιβάλλοντος ανάπτυξης εφαρμογών με έξυπνες κάρτες. Τα κύρια πεδία της μελέτης αυτής είναι:

- Η τεχνολογία των έξυπνων καρτών
- Η έξυπνη κάρτα Gemsafe και τα χαρακτηριστικά της
- Οι αναγνώστες έξυπνων καρτών
- Μια εμπορική εφαρμογή και οι δυνατότητες της
- Η χρήση των καρτών από ένα ευρύτερο περιβάλλον εφαρμογών
- Η ανάπτυξη μίας εφαρμογής.

1.2 Διάρθρωση της εργασίας

Η εργασία έχει την ακόλουθη δομή:

Αριθμός κεφαλαίου	Τίτλος	Σύντομη περιγραφή
1	Εισαγωγή	Στόχος και διάρθρωση εργασίας
2	Έξυπνες κάρτες	Παρουσίαση των έξυπνων καρτών, τύποι καρτών, προτερήματα μειονεκτήματα, operating systems, standards
3	Gamesafe smartcard	Μελέτη της Gemsafe κάρτας,του GPK OS, file structure, περιγραφή των communication commands
4	Smartcard readers	Εισαγωγή στους αναγνώστες καρτών και παρουσίαση δύο μοντέλων που μελετήθηκαν
5	Gamesafe software	Μελέτη των εφαρμογών διαχείρισης και χρήσης καρτών της Gemsafe
6	Χρήση από ξένες εφαρμογές	Παρουσίαση της δυνατότητας χρήσης των πιστοποιητικών των καρτών από τρίτα προγράμματα
7	Περιγραφή εφαρμογής card manager	Παρουσίαση της Java εφαρμογής διαχείρισης smartcard σε Data Base
8	Συμπεράσματα	Συμπεράσματα της εργασίας

2. Έξυπνη κάρτα (smart card)

Είναι μια κάρτα, η οποία μοιάζει εξωτερικά με τη γνωστή πιστωτική κάρτα. Εσωτερικά, όμως, διαφέρει σημαντικά από αυτήν. Η πιστωτική κάρτα είναι ένα απλό κομμάτι πλαστικού, στο οποίο έχει ενσωματωθεί μια μαγνητική ταινία(magnetic stripe), στην οποία είναι εγγεγραμμένα κάποια στοιχεία του χρήστη. Η έξυπνη κάρτα, αντίθετα, ενσωματώνει ένα μικροεπεξεργαστή, ο οποίος βρίσκεται κάτω από μια επαφή από χρυσό, προσαρμοσμένο στη μια πλευρά της. Η βασική διαφορά των δύο τύπων καρτών είναι ότι, ενώ τα δεδομένα στη μαγνητική ταινία είναι εύκολο να παραλλαχθούν ή και να διαγραφούν (ακόμη και τυχαία), αυτό δεν είναι δυνατό στην έξυπνη κάρτα, γιατί ο μικροεπεξεργαστής της δεν περιέχει δεδομένα για το χρήστη: Ο μικροεπεξεργαστής της κάρτας και ο υπολογιστής, με τον οποίο συνδέεται, επικοινωνούν πριν ο μικροεπεξεργαστής επιτρέψει την πρόσβαση στα δεδομένα που περιέχονται στη μνήμη της κάρτας. Με τον τρόπο αυτό αποτρέπεται η παραχάραξη των δεδομένων κι έτσι ο χρήστης διασφαλίζεται, αν η κάρτα του βρεθεί σε διαφορετικά από τα δικά του χέρια. Η τροφοδοσία της κάρτας με ενέργεια εξασφαλίζεται από τον αναγνώστη έξυπνης κάρτας (smart card reader), στον οποίο εισάγεται η κάρτα προκειμένου να χρησιμοποιηθεί. Αυτός μπορεί να επικοινωνήσει με κάποιο κεντρικό υπολογιστή, όπου υπάρχουν τα στοιχεία του χρήστη, προκειμένου να εξασφαλιστεί η πρόσβαση σε δεδομένα. Η μνήμη RAM μιας έξυπνης κάρτας έχει μέγεθος μέχρι 8 Kbytes, η μνήμη ROM μέχρι 384 Kbytes, η μνήμη PROM (προγραμματιζόμενη ROM) μέχρι 256 Kbytes. Ο μικροεπεξεργαστής είναι συνήθως 16 bytes, ενώ υποστηρίζει μικρή ομάδα εντολών (εξασφαλίζοντας μικρό μέγεθος), κυρίως αυτών που είναι απαραίτητες για την επικοινωνία με τον αναγνώστη καρτών / υπολογιστή και την κρυπτογράφηση των περιεχόμενων δεδομένων.

2.1 Βασικά χαρακτηριστικά

***Cost*:** Τυπικά το κόστος κυμαίνεται από $ 2.00 έως $ 10.00. Αυξήσεις του κόστους ανά κάρτα με τσιπ παρέχει μεγαλύτερη δυνατότητα αποθήκευσης και πιο πολύπλοκες ικανότητες. Το κόστος ανά κάρτα αυξομειώνεται αντιστρόφως ανάλογα με τον όγκο καρτών που έχουν παραγγελθεί.

***Reliability*:** Συνήθως οι προμηθευτές εγγυούνται από 10.000 έως 200.000 κύκλους ανάγνωσης / εγγραφής. Οι κάρτες που ισχυρίζονται ότι πληρούν τις προδιαγραφές του Διεθνούς Οργανισμού Τυποποίησης (ISO) πρέπει να επιτυγχάνουν τα αποτελέσματα των δοκιμών που καλύπτουν πτώση, κάμψη, τριβή, συμπυκνωμένου φορτίου, θερμοκρασίας, υγρασίας, στατικού ηλεκτρισμού, χημική επίθεση, φάσμα υπεριώδους, X-ray, και μαγνητικό πεδίο δοκιμών.

***Error Correction*:** Τα σύγχρονα Λειτουργικά Συστήματα Chip (COS) εκτελούν το δικό τους έλεγχο σφαλμάτων. Ο τερματικός σταθμός του λειτουργικού συστήματος θα πρέπει να ελέγχει τα δύο byte codes (SW) που επιστρέφει το COS μετά την εντολή που εκδίδεται από το τερματικό προς την κάρτα, σύμφωνα με το ISO 7816 Part 4[1] και

[1] Βλ. Κεφ. 2.10.1 ISO - International Standards Organization

τις αποκλειστικές του εντολές (proprietary commands). Ο τερματικός σταθμός λαμβάνει στη συνέχεια όλα τα απαραίτητα διορθωτικά μέτρα.

***Storage Capacity*:** EEPROM: 8K - 128K bit.

Σημείωση: Στην ορολογία των smart card, 1K σημαίνει χίλια bits και όχι χίλιοι 8-bit χαρακτήρες. Χίλια bits κανονικά θα αποθήκευαν 128 χαρακτήρες. Ωστόσο, με τις σύγχρονες τεχνικές συμπίεσης δεδομένων, η ποσότητα των δεδομένων που αποθηκεύονται στην smart card μπορεί να διευρυνθεί σημαντικά πέραν αυτής της βάσης μετάφρασης δεδομένων).

Ease of Use: Οι Smart cards είναι φιλικές προς το χρήστη ως προς την εύκολη διασύνδεση με την προβλεπόμενη εφαρμογή. Η χρήση της είναι ίδια με την γνωστή κάρτα μαγνητικής ταινίας ή τραπεζική κάρτα, αλλά είναι πολύ πιο ευέλικτή και ευπροσάρμοστη.

***Susceptibility*:** Οι Smart cards είναι ευπαθείς σε ζημιές στο τσιπ από σωματική κακοποίηση, αλλά πιο ανθεκτικές από της μαγνητικές κάρτες.

***Security*:** Οι Smart cards είναι υψηλής ασφάλειας. Οι πληροφορίες που αποθηκεύονται στο ολοκληρωμένο κύκλωμα είναι δύσκολο να διαταραχθούν ή να αντιγραφούν, σε αντίθεση με τις μαγνητικές κάρτες που η αποθήκευση των δεδομένων γίνεται στο εξωτερικό τμήμα της κάρτας και συνεπώς μπορούν εύκολα να αντιγραφούν. Επιπροσθέτως το chip του μικροεπεξεργαστή και επεξεργαστή των Smart card υποστηρίζει Co-DES, 3-DES, RSA ή πρότυπα ECC για κρυπτογράφηση, ταυτοποίηση ή επαλήθευση της ψηφιακής υπογραφής.

***First Time Read Rate*:** Το ISO 7816 οριοθετεί τον ρυθμό μετάδοσης των καρτών με επαφές στον ρυθμό μετάδοσης δεδομένων στα 9600 baud. Κάποια λειτουργικά συστήματα Chip (COS) επιτρέπουν αυξομείωση στην ταχύτητα μετάδοσης (baud). Μια καλά σχεδιασμένη εφαρμογή μπορεί συχνά να ολοκληρώσει μια συναλλαγή με την κάρτα σε ένα ή δύο δευτερόλεπτα. Η ταχύτητα αναγνώρισης της κάρτας είναι μεγάλη και συνεπώς η κάρτα αναγνωρίζεται και ταυτοποιείται σε ελάχιστο χρονικό διάστημα, όμως οι συναλλαγές συχνά περιέχουν και πολύπλοκα μπλοκ εντολών ή μεταφορές κάποιου όγκου δεδομένων που είναι πιο χρονοβόρες διαδικασίες από τις άπλες εντολές αναγνώρισης ή ταυτοποίησης όμως και πάλι το χρονικό διάστημα της συναλλαγής είναι μικρό. Η ταχύτητα περιορίζεται μόνο από τα σύγχρονα πρότυπα ISO εισόδου / εξόδου.

Proprietary Features: Αυτά είναι το Chip Operating System (COS) και τα εργαλεία ανάπτυξης του συστήματος.

***Processing Power*:** Οι κάρτες παλαιότερων εκδόσεων χρησιμοποιούσαν έναν 8-bit μικροελεγκτή clockable έως 16 MHz με ή χωρίς co-processor για υψηλής ταχύτητας κρυπτογράφηση. Η σημερινή τάση είναι προς τους προσαρμοσμένους ελεγκτές με 32-bit RISC επεξεργαστή στα 25 έως 32 MHz.

Power Source: Οι τιμές τάσης είναι 1.8, 3, ή 5 volt DC.

***Support Equipment Required for Most Host-based Operations*:** Τα μόνα που απαιτούνται είναι μια απλή συσκευή αποδοχής της κάρτας (δηλαδή, ένα τερματικό Card reader / writer) με ασύγχρονο ρολόι, μια σειριακή ή USB διασύνδεση, και μια πηγή ενέργειας των 5-volt. Για χαμηλό όγκο παραγγελιών, το κόστος ανά μονάδα των τερματικών σταθμών είναι περίπου $150. Το κόστος όμως μειώνεται σημαντικά με μεγαλύτερο όγκο παραγγελίας. Η πιο δαπανηρή εκδοχή των καρτών είναι οι ασύρματες συσκευές χειρός όπως τα τερματικά EFT / POS (εικόνα 1) που λειτουργούν με μπαταρία.

Εικόνα 1. EFT / POS συσκευή

2.2 Πλεονεκτήματα

Σε γενικές γραμμές οι Smartcards είναι ένα μέσο για την πραγματοποίηση επιχειρηματικών συναλλαγών σε ένα ευέλικτο, ασφαλές, τυποποιημένο τρόπο με ελάχιστη ανθρώπινη παρέμβαση. Επίσης οι Smart cards μπορούν να παρέχουν strong authentication για single sign-on ή enterprise single sign-on σε computers, laptops, data με encryption, enterprise resource planning πλατφόρμες όπως SAP(Special access program). Το βασικό πλεονέκτημα των έξυπνων καρτών, είναι η τριμελής ταυτοποίηση από το υλικό(hardware), τον χρήστη και τον κωδικό πρόσβασης. Το εύρος χρήσης τους είναι πάρα πολύ μεγάλο όπως και οι δυνατότητες τους. Τα προτερήματα των smartcard δεν θα αναφερθούν σε αυτό το σημείο, γιατί περιγράφονται αναλυτικά στα επόμενα κεφάλαια της εργασίας.

2.3 Μειονεκτήματα

Ένα πρόβλημα των έξυπνων καρτών μπορεί να είναι το ποσοστό αποτυχίας. Η πλαστική κάρτα στην οποία είναι ενσωματωμένο το τσιπ είναι αρκετά ευέλικτη, όμως όσο μεγαλύτερο είναι το chip, τόσο μεγαλύτερη είναι η πιθανότητα να σπάσει. Οι έξυπνες κάρτες συχνά βρίσκονται σε τσέπη ή σε πορτοφόλι - ένα αρκετά σκληρό περιβάλλον για μια κάρτα. Επιπλέον, τα τραπεζικά συστήματα, εμφανίζουν αδυναμία διαχείρισης του κόστους μετάβασης από μαγνητικές κάρτες σε smartcards αν και το κόστος αντικατάστασης των καρτών θα μπορούσε να υπερκαλυφθεί από την μείωση του κόστους της απάτης, η οποία μειώνεται αισθητά μετά από την μετάβαση σε smartcards. Χρησιμοποιώντας μια έξυπνη κάρτα για κάθε είδους συναλλαγές ενέχει κινδύνους για την ιδιωτική ζωή, διότι ένα τέτοιο σύστημα επιτρέπει στον επιχειρηματία – προμηθευτή της κάρτας και στις αρχές την παρακολούθηση της κατάστασης των ατόμων. Τέτοιες καταστάσεις μπορεί να είναι από πολύ ασήμαντες (πχ. τι πιστοποιητικά μεταφέρει ένας χρήστης) έως κρίσιμες και επικίνδυνες (πχ. την οικονομική του κατάσταση και την φυσική θέση του χρήστη). Οι έξυπνες κάρτες

είναι ο πιο ασφαλής τρόπος για client-side αναγνώριση και έλεγχο ταυτότητας (για παράδειγμα σε τραπεζικές εφαρμογές) όμως η ασφάλεια δεν είναι ποτέ 100% βέβαιη. Στο παράδειγμα του τραπεζικού τομέα, αν ένα PC έχει μολυνθεί με κάποιο είδος κακόβουλου λογισμικού (malware), το μοντέλο ασφαλείας είναι σπασμένο. Ένα κακόβουλο λογισμικό μπορεί να υπερισχύσει της επικοινωνίας και μέσω των εισροών του πληκτρολογίου και μέσω των εκροών της εφαρμογής όπως και μέσω της οθόνης. Αλλά και μεταξύ του χρήστη και της τραπεζικής εφαρμογής διαδικτύου (π.χ. Browser). Αυτή η υπερίσχυση θα είχε ως αποτέλεσμα την απαρατήρητη από τον χρήστη, τροποποίηση των συναλλαγών από το κακόβουλο λογισμικό. Υπάρχουν πολλά malwares με αυτή την ικανότητα (πχ. Trojan, Silentbanker). Ορισμένες τράπεζες συνδυάζουν μία έξυπνη κάρτα με ένα ασύρματο card reader για να αποφευχθεί αυτό το πρόβλημα. Ο πελάτης εισάγει μια πρόκληση(challenge) που έλαβε από την ιστοσελίδα της τράπεζας του, το PIN και το ποσό της συναλλαγής στον αναγνώστη καρτών, ο card reader επιστρέφει μία 8-ψηφία υπογραφή, αυτή η υπογραφή αντιγράφεται στο PC(σταθμό εργασίας ή ATM) και επιβεβαιώνεται από την τράπεζα. Η μέθοδος αυτή εμποδίζει ένα κακόβουλο λογισμικό να αλλάξει το ποσό της συναλλαγής. Εκτός από τα τεχνικά εμπόδια, επιπρόσθετο αρνητικό στοιχείο αποτελεί η έλλειψη προτύπων για την λειτουργικότητα και την ασφάλεια των smart card. Για να αντιμετωπιστεί αυτό το πρόβλημα ξεκίνησε το έργο ERIDANE (The Berlin Group[2]) για να ανάπτυξη της πρότασης: "Ενα νέο πλαίσιο για την λειτουργικότητα και την ασφάλεια των έξυπνων καρτών με έμφαση στον εξοπλισμό της αλληλεπίδρασης (POI)(a new functional and security framework for smart-card based Point of Interaction equipment)".

2.4 Παραγωγοί Smartcard

Οι κυριότεροι κατασκευαστές καρτών:

- Giesecke & Devrient GmbH - http://www.gdm.de/
- Bull - http://www.cp8.bull.net/products/prosca.htm
- Gemplus - http://www.gemplus.com/
- Hewlett-Packard - http://www.hp.com/
- Schlumberger - http://www.slb.com/smartcards/
- Solaic - http://www.winforms.phil.tu-bs.de
- Siemens Nixdorf - http://www.sni.de/
- IBM - http://www.ibm.com/
- Microsoft - http://www.microsoft.com/smartcard/

[2] http://www.berlin-group.org/

2.5 Κατασκευαστές Chip

Οι κυριότεροι κατασκευαστές ολοκληρωμένων κυκλωμάτων :

- SGS Thomson - http://us.st.com/stonline/
- Siemens - http://www.siemens.com/
- Motorola - http://www.mot.com/

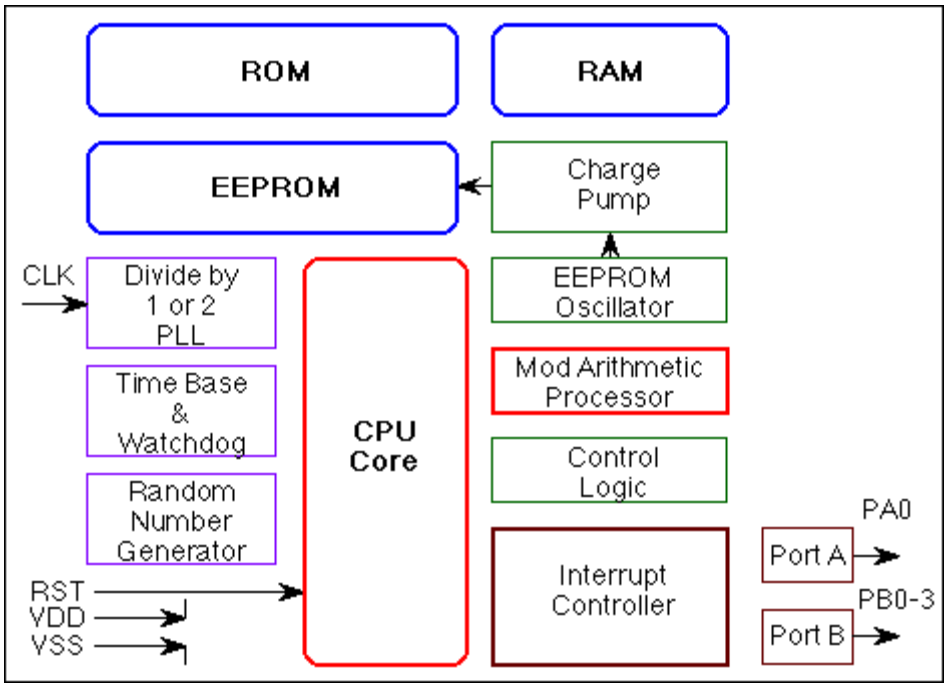
Εικόνα 2. Οι επαφές της κάρτας

Pin /contact	Pin	Περιγραφή
C1	Vcc	Τροφοδοσία της κάρτας
C2	RST	Χρήση ως reset signal
C3	CLK	Σήμα χρονισμού ή συγχρονισμού (προαιρετική χρήση από την κάρτα)
C4	*	
C5	GND	Γείωση
C6	Vpp	Είσοδος programming τάσης (προαιρετική χρήση από την κάρτα)
C7	I/O	Είσοδος / Έξοδος για τα σειριακά δεδομένα με το ολοκληρωμένο κύκλωμα της κάρτας
C8	*	

Πίνακας 1. Περιγραφή των επαφών της κάρτας

*Είτε χρησιμοποιούνται για εξειδικευμένες ενέργειες (όπως πχ. στο να σβήνουν όλα τα δεδομένα της κάρτας σε περίπτωση ανάγκης) είτε δεν χρησιμοποιούνται καθόλου. Ανάλογα με το πρότυπο που ακολουθεί ο προγραμματιστής της κάρτας και τον κατασκευαστή του chip.

Εικόνα 3. Η δομή του chip πάνω στην κάρτα



Εικόνα 4. Η αρχιτεκτονική ενός ολοκληρωμένου κυκλώματος μίας smart card με ενσωματωμένο μικροελεγκτή

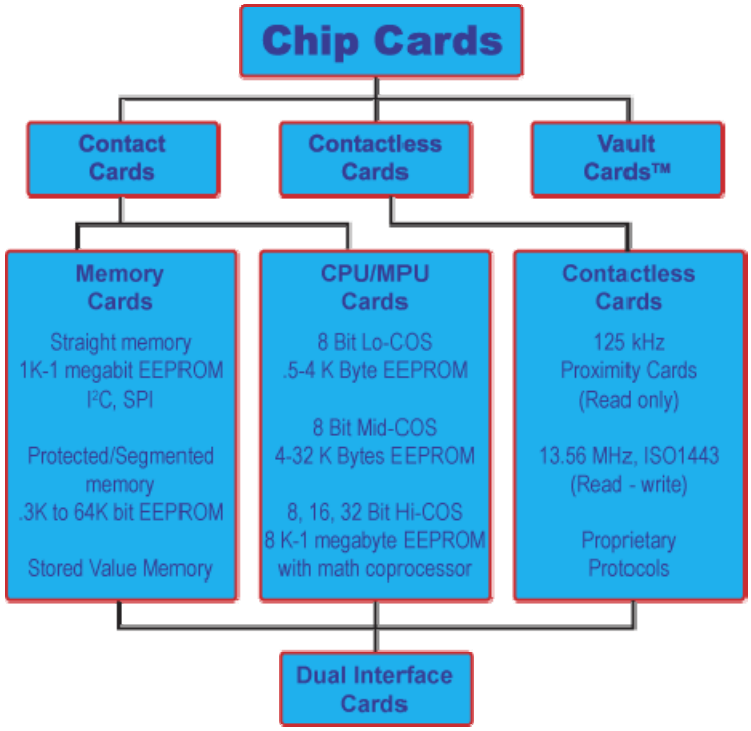
2.6 Οι Smartcards & οι άλλες τεχνολογίες

Τύπος κάρτας	Μεγίστη χωρητικότητα δεδομένων	Επεξεργαστική ισχύ	Κόστος ανά κάρτα	Κόστος τερματικού και διασύνδεσης
Magnetic Stripe Cards	140 bytes	None	$0.20 - $0.75	$750
Memory Cards	32 Gbytes	None	$1 - $250	$300
Processor (Smart) Cards	256KB EEPROM, 384KB ROM and 8KB static RAM	32-bit	$1-$20	$50-$500
Optical Memory Cards	4.9 Mbytes	None	$7 - $12	$3,500 - $4,000

Πίνακας 2. Συγκριτικός πίνακας καρτών

2.7 Τύποι Smart Cards

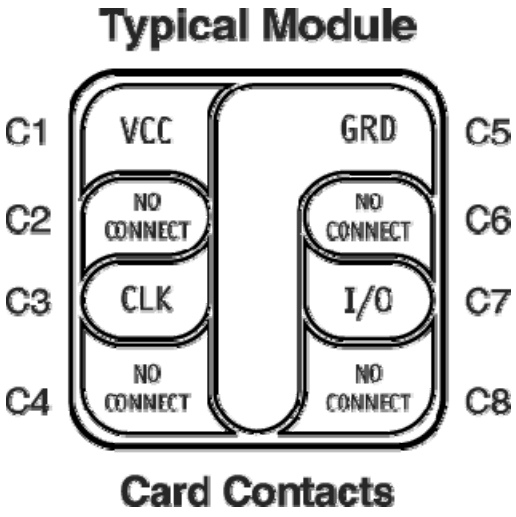
Οι Smart cards κατηγοριοποιούνται σε σχέση με: 1ον Τον τρόπο που η κάρτα διαβάζεται ή γράφεται, και 2ον Τον τύπο του κυκλώματος (chip) που υλοποιείται στην ενσωματώνεται στην κάρτα και τις δυνατότητες του.



Εικόνα 5. Γράφος κατηγοριοποίησης των smartcard

2.7.1 Κάρτες επαφών (Contact Cards)

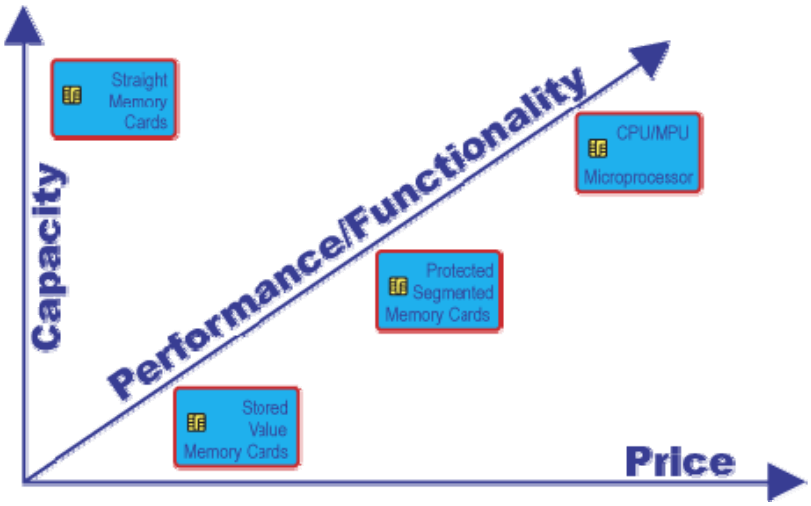
Είναι ο περισσότερο διαδεδομένος τύπος smart card. Κάρτα με ηλεκτρικές επαφές τοποθετημένες στο περίβλημα της, οι επαφές αυτές είναι τα σημεία επαφής με τον card reader όταν εισάγεται η κάρτα.



Εικόνα 6. Οι επαφές της κάρτας

Οι αυξημένες δυνατότητες επεξεργαστικής ισχύς, μνήμης και ευελιξίας είναι κάποια από τα προτερήματα των καρτών με επαφές. Οι κάρτες του τύπου αυτού, είναι αρκετά οικονομικές σε σχέση με τις δυνατότητες τους και πρέπει να επιλέγονται με γνώμονα το επιθυμητό επίπεδό ασφαλείας στα πλαίσια της λειτουργικότητας προς το κόστος. Όλες οι παραπάνω παράμετροι πρέπει να ζυγίζονται σε σχέση με τον κύκλο ζωής της κάρτας. Κατά μέσο όρο οι κάρτες συνήθως συνιστούν το 10 με 15% του συνολικού κόστους ενός συστήματος, με την υποδομή, ασφάλιση, εκπαίδευση και διαφήμισή να καταλαμβάνουν το υπόλοιπο 85%.

Το ακόλουθο σχήμα αναπαριστά μία γενική άποψη αντιστάθμισης συντελεστών Smart Card:



Εικόνα 7. Συσχέτιση συντελεστών των smart card

2.7.2 Κάρτες μνήμης (Memory Cards)

Οι κάρτες μνήμης δεν διαθέτουν εξελιγμένη επεξεργαστική ισχύ και δεν έχουν την δυνατότητα να διαχειριστούν δυναμικά τα αρχεία. Όλοι οι τύποι των καρτών μνήμης επικοινωνούν με τον card reader μέσω συγχρόνων πρωτοκόλλων. Οι διευθύνσεις ανάγνωσης από την κάρτα και εγγραφής στην κάρτα είναι προκαθορισμένες σε όλες τις κάρτες μνήμης. Υπάρχουν τρία είδη καρτών μνήμης:

- Straight
- Protected
- Stored Value

2.7.2.1 Straight Memory Cards

Οι κάρτες αυτού του τύπου, απλά αποθηκεύουν δεδομένα και δεν έχουν καμιά δυνατότητα επεξεργασίας δεδομένων. Αυτές οι κάρτες έχουν τον μικρότερο κόστος ανά bit για την μνήμη του χρήστη. Στην ουσία πρέπει να θεωρούνται ως data travelers από την στιγμή που δεν περιέχουν κανένα μηχανισμό ασφαλείας. Συνεπώς δεν μπορούν να ταυτοποιηθούν σε ένα σταθμό εργασίας από τον card reader παρά μόνο αν το σύστημα γνωρίζει όλους τους τύπους των καρτών που εισάγονται και τις έχει καταχρώμενες με βάση σειριακών αριθμών σε αντιστοίχηση με χρήστη. Τέλος οι κάρτες αυτές αντιγράφονται εύκολα σε βαθμό που να μην είναι με κανένα τρόπο διακριτές οι πλαστές από τις αυθεντικές.

2.7.2.2 Protected / Segmented Memory Cards

Οι κάρτες αυτού του τύπου έχουν μια ενσωματωμένη λογική ελέγχου πρόσβασης στην μνήμη της κάρτας. Θεωρούνται από τις πιο έφυες κάρτες όσο αφορά την αρχιτεκτονική τους. Οι κάρτες αυτές μπορούν να ρυθμιστούν σε κατάσταση ελεγχόμενης διαμόρφωσης δεδομένων (write protect) σε όλα ή μερικά από τα τμήματα της μνήμης. Αυτό επιτυγχάνεται με την χρήση password ή με κρυπτογραφία
Οι Segmented memory cards μπορούν να διαιρεθούν σε λογικά τμήματα προορισμένα για πολλαπλές χρήσεις. Τέλος οι κάρτες αυτές αντιγράφονται και πλαστογραφούνται δύσκολα από hackers αλλά σε τέτοιο βαθμό που να υπάρχει δυνατότητα διάκρισης των πλαστών από τις αυθεντικές.

2.7.2.3 Stored Value Memory Cards

Οι κάρτες αυτές είναι σχεδιασμένες για την αποθήκευση τιμών και δεδομένων ειδικού σκοπού. Οι κάρτες είναι είτε μιας χρήσης ή επαναφορτιζόμενες. Στις περισσότερες κάρτες αυτού του τύπου ενσωματώνονται μόνιμα μέτρα ασφαλείας κατά την κατασκευή τους. Τα μέτρα αυτά συμπεριλαμβάνουν κωδικούς κλειδιά και κυκλώματα τα οποία είναι κωδικοποιημένα μέσα στο hardware από τον κατασκευαστή. Η διάταξη της μνήμης σε αυτές τις συσκευές εγκαθίστανται ως ποσά μείωσης μιας μεταβλητής ή μετρητές. Αφήνοντας λίγη ή καθόλου μνήμη για οποιαδήποτε άλλη λειτουργία. Για απλές εφαρμογές όπως τηλεφωνικές κάρτες, το τσιπ έχει 60 ή 12 κελιά μνήμης για κάθε τηλεφωνική μονάδα. Ένα κελί μνήμης αδειάζει κάθε φορά που χρησιμοποιείται μια τηλεφωνική μονάδα. Όταν όλα τα κελιά μνήμης χρησιμοποιηθούν, η κάρτα

αχρηστεύεται και πετιέται. Η διαδικασία αυτή μπορεί να αναστραφεί στην περίπτωση των επαναφορτιζόμενων καρτών.

2.7.3 CPU/MPU Microprocessor Multifunction Cards

Αυτές οι κάρτες έχουν δυναμικές δυνατότητες επεξεργασίας δεδομένων. Ως Smart cards πολλών λειτουργιών αναθέτουν την μνήμη της κάρτας σε ανεξάρτητους τομείς ή αρχεία εξουσιοδοτημένα σε μια συγκεκριμένη λειτουργία ή εφαρμογή. Μέσα στην κάρτα υπάρχει ένας μικροεπεξεργαστής ή ένα τσιπ μικροελέγχου, το οποίο διευθύνει αυτόν τον καταμερισμό της μνήμης και την πρόσβαση των αρχείων. Αυτός ο τύπος του τσιπ είναι παρόμοιος με αυτά που βρίσκονται μέσα σε ηλεκτρονικούς υπολογιστές και όταν εγκαθίστανται σε μια smart card, διαχειρίζεται δεδομένα σε οργανωμένες δομές αρχείων, μέσω του λειτουργικού συστήματος της κάρτας. Σε αντίθεση με άλλα λειτουργικά συστήματα, αυτό το πρόγραμμα ελέγχει την πρόσβαση στη μνήμη του χειριστή πάνω στην κάρτα. Αυτή η δυνατότητα επιτρέπει διάφορες και πολλαπλές λειτουργίες ή διάφορες εφαρμογές να κατοικίσουν στην κάρτα, επιτρέποντας στις εταιρίες να εκδίδουν και να διατηρούν μια διαφορετικότητα στα προϊόντα τους μέσω της κάρτας. Για παράδειγμα μια χρεωστική κάρτα μπορεί επίσης να επιτρέπει πρόσβαση στα κτίρια ενός πανεπιστημίου. Οι CPU/MPU κάρτες ωφελούν τους χρήστες καθιστώντας τους ικανούς να προωθούν τα προϊόντα και υπηρεσίες τους μέσω τελευταίας τεχνολογίας συναλλαγών και τεχνολογία κρυπτογράφησης. Ειδικότερα, οι τεχνολογίες αυτές καθιστούν ασφαλή αναγνώριση των χρηστών και επιτρέπουν την ανανέωση των πληροφοριών χωρίς την αντικατάσταση των ήδη εγκατεστημένων αρχείων των καρτών, απλοποιούν τις αλλαγές του προγράμματος και τέλος μειώνουν το κόστος. Για το χρήστη της κάρτας, CPU/MPU σημαίνει μεγαλύτερη ευκολία και ασφάλεια, και τελικά, την εδραίωση των multi -cards που εξυπηρετούν πολλούς σκοπούς.

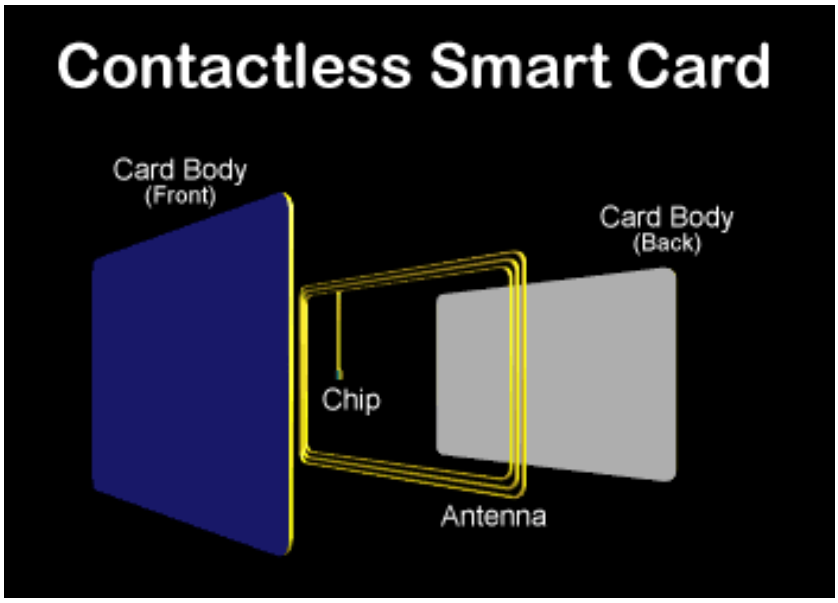
Υπάρχουν πολλά είδη chip σε αυτή την κατηγορία, συμπεριλαμβανομένων chip που υποστηρίζουν κρυπτογραφικές PKI[3] μεθόδους με on board μαθηματικούς co-processors ή τμήματα hardware με Java virtual machine.

2.7.4 Contactless Cards

Οι Contactless Cards είναι smart card που χρησιμοποιούν ραδιοφωνικές συχνότητες (RFID) για την επικοινωνία της κάρτας με τον αναγνώστη, χωρίς να χρειάζεται η εισαγωγή της κάρτας. Αντί αυτού η κάρτα για να διαβαστεί περνάει από την εξωτερική πλευρά του αναγνώστη. Οι τύποι Contactless Card περιλαμβάνουν άμεσες κάρτες που υλοποιούνται ως read-only για πρόσβαση κτιρίων. Τέτοιες κάρτες λειτουργούν με πολύ περιορισμένη μνήμη και επικοινωνούν στα 125 MHz. Οι πρώτες read & write contactless cards χρησιμοποιήθηκαν στις μεταφορές για ταχύτερες και οικονομικότερες φορτοεκφορτώσεις όπου η ασφάλεια δεν έπαιζε σημαντικό ρόλο. Επικοινωνούσαν στα 13.56 MHz και ήταν συμμορφωμένες κατά το πρότυπο ISO14443. Συχνά οι κάρτες αυτής της κατηγορίας είναι τύπου straight memory. Οι Contactless Cards κερδίζουν ολοένα και περισσότερο έδαφος ως κάρτες αγορών λόγο

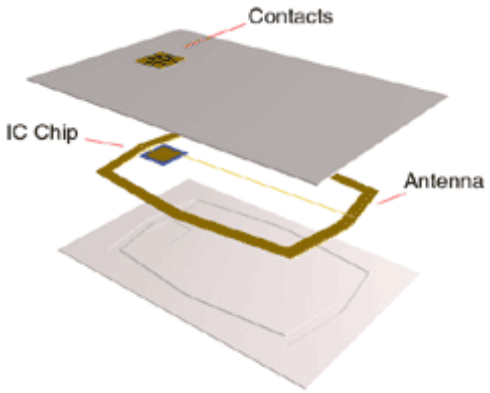
[3] Βλ. Παράρτημα

του χαμηλού κόστους επεξεργασίας σε συνδυασμό με ευκολία και ταχύτητα στις αγορές.



Εικόνα 8. Η δομή της ασύρματης κάρτας .

Ποικιλομορφίες της προδιαγραφής ISO14443 είναι A, B, και C, οι οποίες ορίζουν τα chips των διαφορετικών κατασκευαστών. A = Philips, B = Οποιοσδήποτε άλλος C = Sony chips. Οι Contactless card υστερούν σε περιεκτικότητα και δυνατότητες των κρυπτογραφικών μεθόδων και επεξεργαστική ισχύ σε σχέση με τις microprocessor cards. Τέλος η απόσταση για εφικτή επικοινωνία μεταξύ της κάρτας και του αναγνώστη είναι πολύ περιορισμένη.



Εικόνα 9. Combination Card

2.7.5 Combination Cards

Οι Combination Cards αποτελούν υβριδικές κάρτες που ενσωματώνουν και contact και contactless τεχνολογίες, μαζί στην ίδια κάρτα. Οι Combination Cards μπορούν επίσης να περιέχουν και δύο διαφορετικούς τύπους chip, σε αντίθεση με τις Dual-Interface card όπου ένα chip διαχειρίζεται και τις δύο λειτουργίες.

2.8 πλεονεκτήματα τύπων καρτών

2.8.1 Πλεονεκτήματα των Contactless cards:

- **Ταχύτητα:** Οι συναλλαγές με Contactless έχουν ταχύτερο συνολικό χρόνο συναλλαγής για τους χρήστες.

- **Άνεση**: Οι συναλλαγές με Contactless απαιτούν λιγότερη προσπάθεια από τους χρήστες - η παρουσία της κάρτας είναι αρκετή για να ολοκληρωθεί η συναλλαγή.

- **Χαμηλό κόστος συντήρησης**: Χωρίς τμήματα εκτεθειμένα στην φύση και την φυσική φθορά (πχ. τριβή επαφής), τα συστήματα contactless απαιτούν λιγότερη συντήρηση.

- **Έλξη των χρηστών:** Τα Contactless συστήματα μπορούν να ενσωματωθούν σε ένα μεγάλο φάσμα αντικειμένων εκτός από τις κάρτες, όπως ρολόγια, κλειδιά, δαχτυλίδια, κτλ. Η έλξη των χρηστών μπορεί να βελτιστοποιηθεί ανάλογα με την εφαρμογή και την αγορά που προορίζεται.

2.8.2 Πλεονεκτήματα των Microprocessor-based /contact cards:

- **Ασφάλεια**: Οι Microprocessor-based κάρτες συμμορφώνονται με τα κορυφαία πρότυπα ασφαλείας – DES, RSA και ECC.

- **Συνεργία μεταξύ των εφαρμογών:** Οι μικροεπεξεργαστές έχουν την ικανότητα να διαχειρίζονται πολλαπλές εφαρμογές στην ίδια κάρτα.

- **Ευκολία update**: Η υπολογιστική ισχύ ενός μικροεπεξεργαστή δίνει την δυνατότητα ενημέρωσης για τις κάρτες ακόμη και μετά την έναρξη λειτουργίας τους. Είτε προσθέτοντας μια νέα εφαρμογή, ή ενημέρωση μιας υπάρχουσας, οι χρήστες μπορούν να ανανεώσουν τις κάρτες ανά πάσα στιγμή μετά την διάθεση της ενημέρωσης .

2.9 Card Operating Systems COS

Οι δύο βασικότεροι τύποι λειτουργικών συστημάτων smart card είναι: Fixed File Structure και Dynamic Application System. Μία εξίσου σημαντική επιλογή με τον τύπο της κάρτας είναι το λειτουργικό της σύστημα. Επιλογή που πρέπει να γίνεται με βάση την εφαρμογή που προορίζεται η κάρτα.

2.9.1 Fixed File Structure

Η Fixed File ως δομή λειτουργικού συστήματος μεταχειρίζεται την κάρτα ως μία ασφαλείς υπολογιστική και αποθηκευτική συσκευή. Τα αρχεία και τα δικαιώματα προκαθορίζονται από τον κατασκευαστή. Αυτές οι προκαθορισμένες παράμετροι είναι οι ιδανικότερες και οικονομικότερες για την δεδομένη στιγμή της κατασκευής της κάρτας και δεν είναι τροποποιήσιμες στο μέλλον.

2.9.2. Dynamic Application System

Αυτός ο τύπος λειτουργικού συστήματος, που περιέχεται στις κάρτες MULTOS και στις JAVA cards, δίνει την δυνατότητα στους προγραμματιστές να αναπτύσσουν, να ελέγχουν και να εφαρμόζουν διαφορετικές εφαρμογές για την ίδια κάρτα. Οι εφαρμογές του Dynamic Application OS είναι σχετικά ανεξάρτητες και συνεπώς πιο εύκολα συντηρήσιμες και αναβαθμίσιμες. Ένα παράδειγμα Dynamic Application OS χρήσης είναι οι SIM cards για GSM όπου τα updates εγκαθίστανται δυναμικά και αυτόματα στην κάρτα.

2.10 Smart Card Standards

Τα smart card standards διατυπώνουν φυσικές ιδιότητες, χαρακτηριστικά επικοινωνίας και λειτουργούν ως πρότυπα-οδηγοί για εφαρμογές του ενσωματωμένου chip και των δεδομένων του. Σχεδόν όλα τα standards έχουν ως βάση το ISO 7816-1, 2 & 3. Οι προδιαγραφές που αναφέρονται στις εφαρμογές είναι αντικείμενο αντιπαράθεσης μεταξύ μεγάλων οργανισμών, όπου ο καθένας προτείνει τα δικά του πρότυπα. Στα ανοιχτά συστήματα καρτών πρέπει να επιτυγχάνεται διασυνδεσύμοτητα και αλλήλουποστιρίξη μεταξύ των συστημάτων σε πολλαπλά επίπεδα: **1).**Στην κάρτα ως σύστημα **2).**Στα τερματικά καρτών (card readers), **3).** Στα δίκτυα και **4).** Στα συστήματα κατασκευαστών καρτών. Η διασυνδεσύμοτητα και αλλήλουποστιρίξη στα ανοιχτά συστήμτα μπορεί μόνο να επιτρυχθεί με συμόρφώση στα διεθνή standards. Οι οργανισμοί πιστοποίησης που δραστηριοποπούνται στην θέσπιση standard για smart card. Οι ακόλουθοι οργανισμοί και standards είναι οι επικρατέστεροι στην κατασκευή smart card:

2.10.1 ISO - International Standards Organization [4]

Αυτός ο οργανισμός διευκολύνει την δημιουργία εθελοντικών standards μέσω μίας διαδικασίας που είναι προσβάσημη από όλους τους ενδιαφερομένους. Το ISO 7816 είναι διεθνή standard για Contact smart cards αλλά και για Contactless cards. Οποιοσδήποτε επιθυμεί να κατανοήσει την τεχνολογική δομή των smart cards οφείλει να εξοικειωθεί με τα πρότυπα ISO 7816 και 1443.

Περίληψη ISO 7816 – Αυτή είναι μια γενική επισκόπηση των προδιαγραφών που καλύπτει το ISO7816. Μερικά από αυτά είναι σε συνεχή εξέλιξη, ενώ άλλα είναι στάσιμα ή ακόμα και προσχέδια.

[4] http://www.iso.org/iso/home.htm

1. **ISO 7816-1:** Φυσικά χαρακτηριστικά, 1987: προδιαγράφει τις φυσικές διαστάσεις των contact smart cards και τις αντιστάσεις τους σε στατικό ηλεκτρισμό, ηλεκτρομαγνητική ακτινοβολία και μηχανικό στρες. Επίσης περιγράφει τις φυσικές αποστάσεις μίας μαγνητικής λωρίδας στην μαγνητική κάρτα.
2. **ISO 7816-2:** Αποστάσεις και τοποθεσίες των επαφών, 1988: προδιαγράφει την τοποθεσία, τους σκοπούς και τα ηλεκτρικά χαρακτηριστικά των μεταλλικών επαφών της κάρτας.
3. **ISO 7816-3:** Ηλεκτρικά σήματα και πρωτόκολλα επικοινωνίας, 1989: προδιαγράφει τις απαιτήσεις σε τάση και ρεύμα για τις επαφές όπως ορίζονται στο ISO 7816-2. Επίσης προδιαγράφει το ημιαμφίδρομο, ασύγχρονο πρωτόκολλο μεταφοράς χαρακτήρων (T=0). Τροποποίηση $1^{η}$:1992, τύπος πρωτόκολλου T=1, ημιαμφίδρομο, ασύγχρονο πρωτόκολλο μεταφοράς μπλοκ. Τροποποίηση $2^{η}$:1994, T=14: Αναθεωρείται η επιλογή του τύπου πρωτοκόλλου, ένα δυναμικό πρωτόκολλο συνδυασμός των T=0 και T=1.
4. **ISO 7816-4:** Ενδοβιομηχανικές εντολές για ανταλλαγή μηνυμάτων. Θεσπίζει ένα μπλοκ εντολών για CPU κάρτες, για να παρέχει πρόσβαση, ασφάλεια και μετάδοση στα δεδομένα της κάρτας. Συμπεριλαμβανόμενες σε αυτόν τον βασικό πύρινα, για παράδειγμα υπάρχουν οι εντολές read, write και update records.
5. **ISO 7816-5:** Αριθμητικό σύστημα και διαδικασίες καταχώρησης για Application Identifiers (AID): θέτονται τα standards για τους AID. Κάθε AID έχει δύο τμήματα. Το πρώτο είναι ο κατοχυρωμένος Application Provider Identifier (RID) μεγέθους πέντε bytes που είναι μοναδικός για κάθε κατασκευαστή. Το δεύτερο τμήμα είναι μεταβλητού μεγέθους πεδίου μέχρι 11 bytes έτσι ώστε το RIDs να μπορεί να χρησιμοποιηθεί για να αναγνώριση αντιστοιχών εφαρμογών.
6. **ISO 7816-6:** Ενδοβιομηχανικά (Inter-industry) στοιχεία δεδομένων: μεταφορά φυσικού επιπέδου, συναλλαγές δεδομένων, answer to reset και πρωτόκολλα επικοινωνίας. Οι προσδιορισμοί επιτρέπουν δύο πρωτόκολλα επικοινωνίας: το character protocol (T=0) ή το block protocol (T=1). Μία card μπορεί να υποστηρίζει ένα από τα δύο αλλά όχι και τα δύο (Σημείωση: Κάποιοι κατασκευαστές καρτών εμμένουν σε κανένα από τα δύο αυτά πρωτόκολλα και επιλέγουν το T=14.
7. **ISO 7816-7:** Ενδοβιομηχανικές (Inter-industry) εντολές για δομημένη Card Query Language (SCQL): Αυτό το κείμενο προδιαγραφών διαμορφώνει μια αφηρημένη άποψη για την SCQL database (SCQL = Structured Card Query Language βασισμένη σε SQL), και για τις συσχετιζόμενες Ενδοβιομηχανικές (inter-industry) enhanced commands.
8. **ISO 7816-8:** Εντολές λειτουργιών ασφαλείας: Το πρότυπο αυτό κωδικοποιεί τις εσωτερικές εντολές της κάρτας για λειτουργίες ασφαλείας.
9. **ISO 7816-9:** Εντολές για Card Management: προκαθορίζει μια περιγραφή και κωδικοποίηση του κύκλου ζωής των καρτών και των συσχετιζόμενων αντικειμένων, την περιγραφή και κωδικοποίηση των ιδιοτήτων των αντικειμένων, των μεθόδων, των εντολών, των στοιχείων των εντολών και γενικότερα όλες τις παραμέτρους και τους μηχανισμούς μια κάρτας.
10. **ISO 7816-10:** Ηλεκτρικά σήματα και answer to reset για synchronous cards: αυτό το κομμάτι του ISO 7816 καθορίζει την ισχύ και τις δομές των σημάτων καθώς επίσης την δομή του ATR μεταξύ του κυκλώματος και της

συγχρονισμένης δομής μεταφοράς και της διασύνδεσης με την τερματική συσκευή.

11. **ISO 7816-11:** Ταυτοποίηση χρηστών μέσω βιομετρικών μεθόδων. Σε ερευνητικό στάδιο.

2.10.2 FIPS (Federal Information Processing Standards) [5]

Ανεπτυγμένο από το Computer Security Division του National Institute of Standards and Technology (NIST). Τα FIPS standards είναι σχεδιασμένα να προστατεύουν τα ομοσπονδιακά αποκτήματα συμπεριλαμβανομένων υπολογιστικά και τηλεπικοινωνιακά συστήματα. Τα ακόλουθα FIPS standards εφαρμόζονται σε smart card τεχνολογίες και δίνουν έμφαση σε digital signature standards, υψηλού επιπέδου encryption standards, και απαιτήσεις security για κρυπτογραφικών λειτουργιών.

- **FIPS 140 (1-3):** Οι απαιτήσεις ασφάλειας που περιέχονται στο FIPS 140 (1-3) αφορούν πεδία σχετικά με την ασφαλή σχεδίαση και υλοποίηση κρυπτογραφικών λειτουργιών, ειδικότερα: ορισμός κρυπτογραφικών λειτουργιών, θύρες και διασυνδέσεις, ρόλοι, υπηρεσίες ,ταυτοποίηση, μοντέλο πεπερασμένης κατάστασης, φυσική ασφάλεια, λειτουργικά περιβάλλοντα, κρυπτογραφικά κλειδιά, ηλεκτρομαγνητική διασύνδεση και ηλεκτρομαγνητική συμβατότητα (EMI/EMC), αυτοέλεγχος, σχεδιασμός διασφάλισης και μετριασμός άλλων επιθέσεων.
- **FIPS 201:** Σε ερευνητικό στάδιο, αυτό το πρότυπο σκοπεύει να καλύψει τις προοπτικές πολύ-λειτουργικότητας των καρτών στο πεδίο συστημάτων διαχείρισης και ελέγχου ταυτότητας, για κυβερνητικούς σκοπούς(U.S. government).

2.10.3 EMV[6]

Οι εταιρίες Europay, MasterCard και Visa δημιούργησαν την EMV Company και ανέπτυξαν το "Integrated Circuit Card Specifications for Payment Systems". Αυτές οι προδιαγραφές σχετίζονται με το ISO7816 και θέτουν μια κοινή τεχνική βάση για συστήματα smart card και υλοποίηση συστήματος αποθηκευμένης τιμής. Οι προσδιορισμοί "Integrated Circuit Card Specifications for Payment Systems" μπορούν να αποκτηθούν από τις εταίρες Visa, MasterCard ή οποιοδήποτε μέλος της Europay τράπεζας.

[5] http://www.itl.nist.gov/

[6] http://www.emvco.com/

2.10.4 PC/SC [7]

Ένα standard για cards και readers, προτεινόμενο και υλοποιημένο από την Microsoft, το πρότυπο PC/SC. Η πρόταση αυτή εφαρμόζεται μόνο σε CPU cards. Που έχουν ενσωματωμένο το CryptoAPI, ένα πλαίσιο(framework) που υποστηρίζει πολλούς μηχανισμούς ασφαλείας για συστήματα και κάρτες. Το PC/SC είναι δικαίως το πιο διαδεδομένο πρότυπο διασύνδεσης για εφαρμογές for PC logon. Το πρότυπο αυτό είναι ένα σύνολο υψηλού επιπέδου αφηρημένων συνδετικών τμημάτων που επιτρέπουν συναλλαγές μεταξύ καρτών και μιας πληθώρας από αναγνώστες.

2.10.5 CEN (Comite' Europeen de Normalisation) και ETSI [8]

(European Telecommunications Standards Institute) είναι εστιασμένα στις τηλεπικοινωνίες, κυρίως GSM SIM για κινητά τηλέφωνα. Τα πρότυπα τους είναι τα GSM 11.11 και ETSI300045.

Εικόνα 10. Το logo της Cen

Εικόνα 11. Το logo της ETSI

[7] http://www.pcscworkgroup.com

[8] http://www.cen.eu *και www.**etsi**.org*

2.10.6 HIPAA [9]

Ο οργανισμός Health Insurance Portability and Accountability Act υιοθετεί τα διεθνή πρότυπα για την υλοποίηση ενός συστήματος ασφαλών ηλεκτρονικών συναλλαγών ιατρικών δεδομένων στις ΗΠΑ. Πολλά από τα χαρακτηριστικά ασφαλείας του επιπέδου που απαιτεί ο HIPAA, για λόγους ασφάλειας και προστασίας προσωπικών δεδομένων, υλοποιούνται σε ικανοποιητικό βαθμό για τις ανάγκες των προτύπων του οργανισμού.

Εικόνα 12. Το logo της HIPAA

IC Communications Standards – Ο οργανισμός σταμάτησε την λειτουργία του πολύ πριν τα chip ενσωματωθούν στις smart card. Η συνεισφορά του όμως ήταν σημαντική στα interfaces the I2C και SPI EEPROM.

2.11 Πρωτόκολλα μεταφοράς δεδομένων

Όνομα	Περιγραφή transmission protocol	Ορισμένο στο
T=0	Ασύγχρονο ημιαμφίδρομο επιπέδου byte	ISO/IEC 7816-3
T=1	Ασύγχρονο ημιαμφίδρομο επιπέδου block	ISO/IEC 7816-3
T=2	Δεσμευμένο για αμφίδρομές λειτουργίες	ISO/IEC 7816-3
T=3	Δεσμευμένο για αμφίδρομές λειτουργίες	ISO/IEC 7816-3
T=CL	APDU μεταφορά για contactless interface	ISO 14443[10]

[9] http://www.hipaa.org

[10] http://en.wikipedia.org/wiki/ISO_14443

Πίνακας 3. Πρωτόκολλο επικοινωνίας

Σημείωση: Αν η κάρτα δεν χρησιμοποιεί κανένα πρότυπο πρωτόκολλο μεταφοράς, αλλά χρησιμοποιεί ένα προσαρμοσμένο ή ιδιόκτητο πρωτόκολλο. Τότε το πρωτόκολλο επικοινωνίας που έχει ονομάζεται T=14.

2.11.1 Το πρωτόκολλο APDU (Application protocol data unit)

Μήνυμα APDU: ζευγάρι Command-response

Όνομα πεδίου	**Μέγεθος**	**Περιγραφή**	**Κωδικό**
Class byte	1	Class of instruction	CLA
Instruction byte	1	Instruction code	INS
Parameter bytes	2	Instruction parameters	P1-P2
Lc field	0, 1 ή 3	The Lc field fixes number Lc	-
Command data field	Lc	String of Lc bytes	-
Le field	0, 1, 2 ή 3	The Le field fixes number Le	-
Response data field	Lr	String of Lr bytes	
Status bytes	2	Command processing status	SW1-SW2

Πίνακας 4.Το πρωτόκολλο APDU

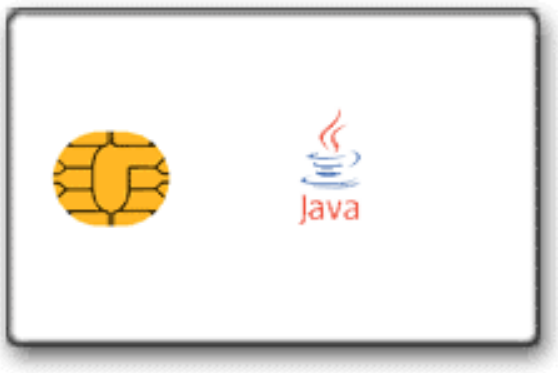
Το APDU (Application Protocol Data Unit) είναι μία επικοινωνιακή μονάδα μεταξύ της κάρτας και του card reader. Η δομή μιας εντολής APDU καθορίζεται από το πρότυπο ISO 7816. Υπάρχουν δύο κατηγορίες APDU: Η command APDUs και η response APDUs. Όπως υποδηλώνει το όνομα, η αρχική (command APDU) έχει αποσταλεί από τον αναγνώστη του δελτίου: περιλαμβάνει ένα υποχρεωτικό πεδίο (header) 5-byte και από το 0 έως το 255 τα byte των δεδομένων. Η τελευταία (response APDU) έχει αποσταλεί από την κάρτα προς τον αναγνώστη: θα περιέχει το υποχρεωτικό πεδίο κατάστασης (status word) 2-byte και από το 0 έως το 256 τα byte των δεδομένων.

2.12 Java card

Εικόνα 13. Το σήμα της Java Card

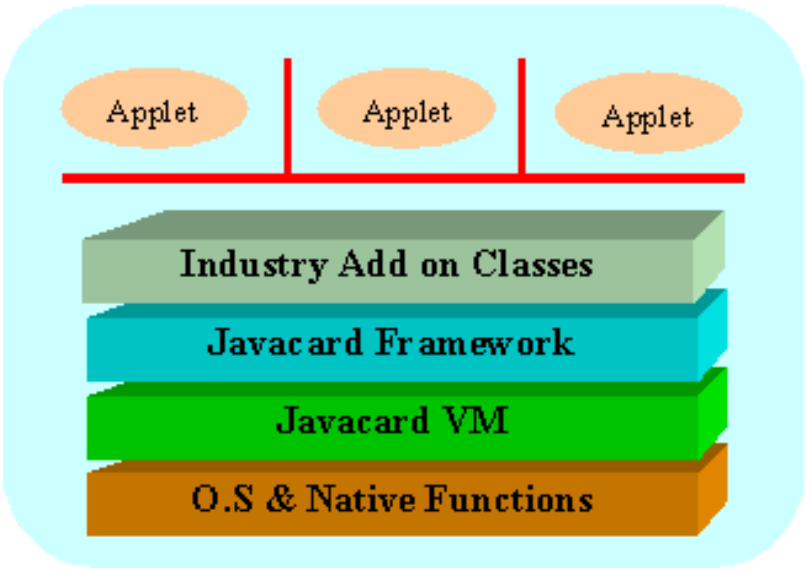
Java Card 3.0 - Το πρότυπο αυτό δημοσιεύτηκε από την Sun. Περιέχει πληροφορίες για την ανάπτυξη της Java Card virtual machine. Το πρότυπο Java Card Runtime Environment, το οποίο κατ' επέκταση προσδιορίζει την συμπεριφορά runtime για τις Java-based smart cards και τέλος το πρότυπο Java Card 3.0 περιγράφει αντίστοιχο API της Java για smart cards, το Java card API.

Η Java Card είναι ένα είδος smart card που έχει την ικανότητα να τρέχει προγράμματα Java.



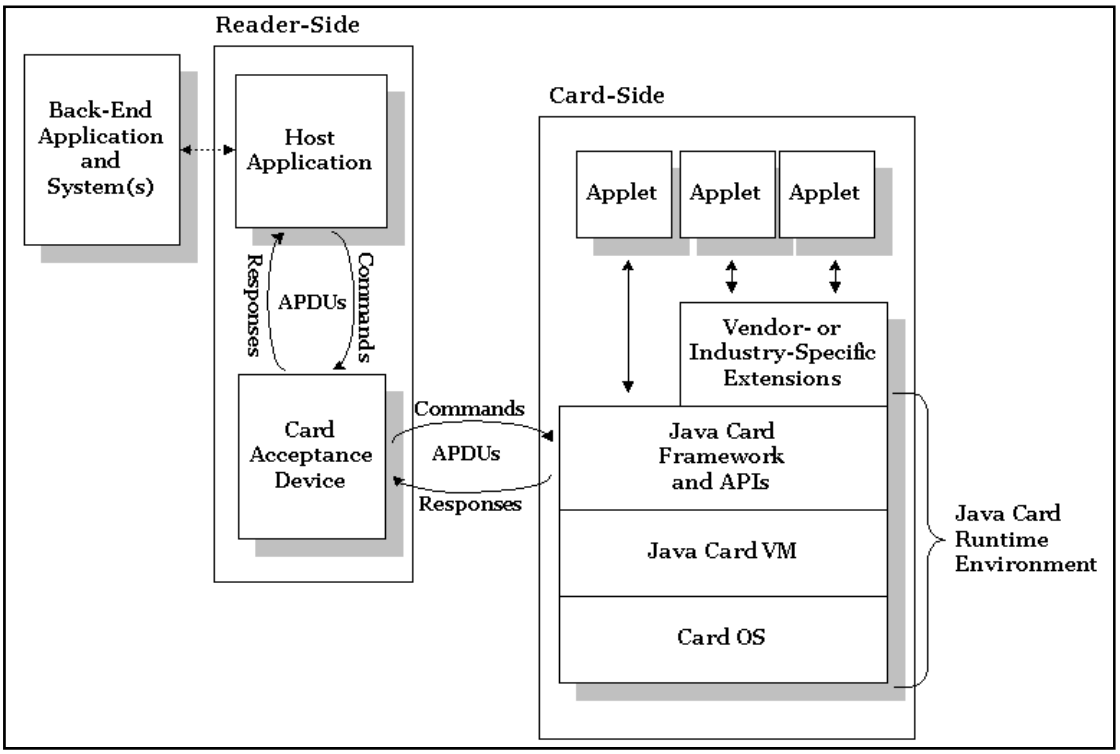
Εικόνα 14. Java Card

Η αρχιτεκτονική του συστήματος της Java Card παρουσιάζεται στο ακόλουθο σχήμα.



Εικόνα 15. Η αρχιτεκτονική της Java Card

Όπως φαίνεται από την Εικ. 15, το Java Card VM είναι ανεπτυγμένο στην κορυφή ενός συγκεκριμένου ενσωματωμένου κυκλώματος (IC) με ενσωματωμένη υλοποίηση λειτουργικού συστήματος. Το επίπεδο JVM αποκρύπτει την πολυπλοκότητα της τεχνολογικής δομής του κατασκευαστή με την χρήση απλής γλώσσας και system interface. Το Java Card framework προσδιορίζει ένα σύνολο από Application Programming Interface (API) κλάσεις για ανάπτυξη Java Card εφαρμογών και παρέχει υπηρεσίες συστήματος για αυτές τις εφαρμογές. Κάθε φορέας που χρησιμοποιεί Java Cards μπορεί να τις διαμορφώσει ανάλογα με τις ανάγκες του, υπάρχει δυνατότητα αναδιαμόρφωσης ακόμα και των system και security models. Η Java Card τεχνολογία δίνει την δυνατότητα στις smart cards και σε άλλες συσκευές με περιορισμένη μνήμη, να τρέχουν μικρές εφαρμογές, τα applet. Μία κάρτα μπορεί να έχει περισσότερα από ένα applet, διακρίνοντας τα με την χρήση του μοναδικού αναγνωριστικού *AID* (application identifier), όπως ορίζεται στο ISO 7816, part 5. Σημείωση οι smart cards δεν είναι προσωπικοί υπολογιστές. Έχουν περιορισμένη μνήμη και επεξεργαστική ισχύ. Οι χρήστες της Java Card 3.0 δεν πρέπει να θεωρούν το JC.30 ως μια μικρή έκδοση του JDK.



Εικόνα 16. Η αφηρημένη δομή επικοινωνίας ενός συστήματος με τον αναγνώστη του και με την Java card

2.12.1 Portability

Η Java Card τεχνολογία σκοπεύει στον προσδιορισμό ενός πρότυπου υπολογιστικού περιβάλλοντος για smart cards, όπου ίδια java card applets έχουν την δυνατότητα να τρέχουν σε διαφορετικές smart card, αντίστοιχη δυνατότητα των java applet που τρέχουν σε διαφορετικούς υπολογιστές. Όπως και στην Java, η δυνατότητα αυτή επιτυγχάνεται με τον συνδυασμό της εικονικής μηχανής της java card (jcvm) και μίας πολύ καλά ορισμένης runtime βιβλιοθήκης, η οποία διαχωρίζει το applet από τις διαφορές των καρτών. Παρ' όλα αυτά η φορητότητα παραμένει εξαρτημένη από θέματα όπως μέγεθος μνήμης, επιδόσεις, και υποστήριξη runtime (πχ. πρωτόκολλα επικοινωνίας ή αλγόριθμοι κρυπτογραφίας).

2.12.2 Security

Η τεχνολογία Java Card εξ' αρχής σχεδιάστηκε με σκοπό την διασφάλιση των ευαίσθητων πληροφοριών που είναι αποθηκευμένες σε smart card. Συνεπώς το πεδίο της ασφάλειας καλύπτεται από πολλές απόψεις.

- **Ενθυλάκωση δεδομένων (Data encapsulation).** Τα δεδομένα αποθηκεύονται μέσα στην εφαρμογή και οι Java Card εφαρμογές εκτελούνται σε ένα απομονωμένο περιβάλλον το (jcvm) ξεχωριστό από τα υποστρώματα λειτουργικό σύστημα και hardware.

- **Applet Firewall.** Οι διαφορετικές εφαρμογές είναι επίσης ξεχωριστές μεταξύ τους με την χρήση ενός applet firewall (τοίχος προστασίας) που περιορίζει και ελέγχει την πρόσβαση στα δεδομένα στοιχεία του κάθε applet.
- **Cryptography.** Υποστηρίζονται οι πιο ευρέως διαδεδομένοι αλγόριθμοι κρυπτογραφίας, όπως DES, 3DES, AES, RSA (συμπεριλαμβανομένης και της κρυπτογραφίας ελλειπτικής καμπύλης). Όπως επίσης υποστηρίζονται και άλλες κρυπτογραφικές υπηρεσίες του τύπου παραγωγή κλειδιού, υπογραφή και ανταλλαγή κλειδιού.
- **Applet.** Το applet είναι μια κατάσταση machine which επεξεργάζεται μόνο εντολές εισερχόμενων αιτήσεων και απαντάει στέλνοντας είτε δεδομένα είτε μήνυμα κατάστασης στην τερματική συσκευή.

Εικόνα 17. Η Java Card είναι υποσύνολο της Java

2.12.3 Java Card versus Java

Σε επίπεδο γλώσσας, η Java Card είναι ένα ακριβές υποσύνολο της Java : η δομή της Java Card υπάρχει πανομοιότυπη στην Java, και συμπεριφέρεται με τον ίδιο ακριβώς τρόπο. Η ιδιότητα αυτή υπόκειται στο γεγονός ότι τα Java Card προγράμματα γίνονται compile ως Java class αρχεία από Java compiler, χωρίς κάποια ειδική ρύθμιση. Παρ' όλα αυτά, πολλά χαρακτηριστικά της Java δεν υποστηρίζονται από την Java Card.

Για τις ανάγκες της εργασίας αυτής θα χρησιμοποιηθεί η GemSafe GPK1600 της εταιρίας Gemplus http://www.gemplus.com/ μέλος της GEMALTO http://www.gemalto.com/

3. Gamesafe GPK1600 smart card

Εικόνα 18. Η κάρτα GemSafe GPK1600

3.1 Βασικά χαρακτηριστικά

Η Gamesafe smart card είναι Cpu Contact card και αποτελεί προϊόν της Gemallto, είναι μία κάρτα χωριτικότητας 16k. Το λειτουργικό της σύστημα είναι το GPK.

- 16K EEPROM
- ISO 7816 -1/2/3/4
- RSA & 3DES algorithms
- Fast on board key generation

3.2 Εισαγωγή στο GPK

Η πολλαπλών επιπέδων εφαρμογή Gemplus Public Key (GPK) είναι ένα λειτουργικό σύστημα που υπηρετεί τους σκοπούς της ασφάλειας των δεδομένων, δίνοντας έμφαση στις ιδιαίτερα απαιτητικές ανάγκες των εφαρμογών των εμπορικών συναλλαγών.

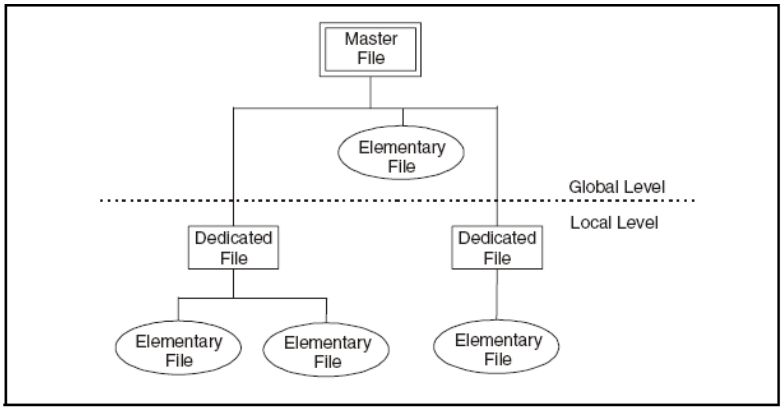
Το GPK περιλαμβάνει:

- Συμβατές δομές δεδομένων, εντολές και κώδικες επιστροφής σύμφωνα με το πρότυπο ISO 7816-4
- Ένα συμπληρωματικό σύνολο εντολών διαχείρισης και παραμετροποίησης της κάρτας , από τα διεθνή πρότυπα MPCOS-EMV
- Οι μέθοδοι πληρωμής, οι δομές δεδομένων και οι εντολές από τα διεθνή πρότυπα MPCOS-EMV, επιτρέπουν την λειτουργία της κάρτας ως ηλεκτρονικό πορτοφόλι (electronic purse)
- EMV-χαρακτηριστικά συμβατότητας
- Ο 3DES αλγόριθμος χρησιμοποιείται για ασφαλή αποστολή μηνυμάτων συμφώνα με το πρότυπο ISO 7816-4, αλλά και για κρυπτογράφηση και αποκρυπτογράφηση
- SSL 1,024-bit RSA υπογραφές
- RSA (up to 1,024 bits) υπογραφή/ αποκρυπτογράφηση (normal mode και CRT mode)
- Εξακρίβωση (verification) RSA (up to 1,024 bits)
- Υπογραφή και εξακρίβωση (verification): DSA

- Πάνω στην κάρτα (Onboard) παραγωγή κλειδιού RSA (512 and 1,024 bits)
- SHA-1 και MD5 αλγορίθμους για hashing
- Μηχανισμό παραγωγής τυχαίων αριθμών (8 bytes and 32 bytes)
- Padding με PKCS#1 version 1.5, ISO9796-2, ANSI X9.31

3.3 Δομή δεδομένων (Data Structure)

Το GPK βασίζεται σε συγκεκριμένο σύστημα αρχείων. Τα αρχεία οργανώνονται σε ιεραρχική δομή δύο επιπέδων. Το Κύριο αρχείο (Master File (MF)) είναι στην κορυφή της ιεραρχικής δομής του συστήματος αρχείων. Το MF μπορεί να περιέχει Στοιχειώδη αρχεία (Elementary Files(EFs)) αλλά και Ειδικού τύπου (Dedicated Files (DFs)). Τα DFs περιέχουν ομάδες από EFs, ενώ τα EFs περιέχουν data.



Εικόνα 19. Η δενδροειδής δομή του file system του GPK

- Global /local level

Το επίπεδο που σχηματίζεται από το Master File (MF) με τα Elementary Files (EF)s ακριβώς από κάτω του, αποκαλείται global level. Ενώ Το επίπεδο που σχηματίζεται από τα Dedicated Files (DF)s με τα EFs από κάτω τους αποκαλείται local level.

3.4 Σύνολο εντολών (Command Set)

Το λειτουργικό σύστημα GPK περιλαμβάνει:

- Εντολές διαχείρισης[11] (Administration commands), όπως δημιουργία αρχείου, εγγραφή και ανάγνωση δεδομένων από τα αρχεία της κάρτας
- Εντολές εμπορικών συναλλαγών[12] (Payment commands), όπως δημιουργία πορτοφολιού (purse), χρέωση πορτοφολιού .
- Εντολές Public Key, χρήση public key αλγόριθμους (RSA, DSA).

[11] Συνοπτική παρουσίαση στο κεφάλαιο 3.14 Administration Commands

[12] Συνοπτική παρουσίαση στο κεφάλαιο 3.15 Payment Commands

3.5 Διαχείριση πρόσβασης δεδομένων (Data Access Management)

Η πρόσβαση στα αρχεία του GPK μπορεί να προστατευθεί από μυστικούς κωδικούς. Οι μυστικοί κωδικοί αποθηκεύονται σε ειδικά EFs, που καλούνται secret code Elementary Files (EFsc). Το κάθε EFsc μπορεί να αποθηκεύσει μέχρι και οκτώ κωδικούς, αριθμώντας τους από 0 έως 7.

Το MF και κάθε DF μπορεί να έχει ένα EFsc. Οι Συνθήκες πρόσβασης (Access conditions) καθορίζουν το επίπεδο της προστασίας που χορηγείται σε κάθε αρχείο (όπως read or write, για παράδειγμα). Η κάρτα καθορίζει αν η πρόσβαση σε ένα αρχείο επιτρέπεται ή όχι , συγκρίνοντας τις τιμές ενός καταχωρητή εξουσιοδότησης με εκείνες που απαιτεί η συνθήκη πρόσβασης. Οι Συνθήκες πρόσβασης αποθηκεύονται στους περιγραφείς αρχείων (file descriptors) των DF και EF.

Οι οποίοι περιέχουν δύο τμήματα:

- Ένα σύνολο Συνθηκών πρόσβασης AC, που προκαθορίζει το επίπεδο προστασίας. Κάθε τύπος Συνθήκης πρόσβασης μπορεί να προστατεύεται μέχρι και από δύο μυστικούς κωδικούς. Επίσης το τμήμα αυτό περιέχει πληροφορίες σχετικά με το κρυπτογραφικό κλειδί που χρησιμοποιείται για την παραγωγή κλειδιών συνόδου για κάθε ασφαλή επικοινωνία με το αρχείο. Οι πληροφορίες αυτές είναι είτε global είτε local επίπεδο. Και είναι ένας τύπος ταυτότητας (Short File Identifier (SFI)) για το αρχείο κλειδιού.
- Μία αναφορά μυστικού κωδικού Συνθηκών πρόσβασης (AC Secret Code Reference) προδιαγράφει το επίπεδο (global or local) του αρχείου και το μέγεθος του μυστικού κωδικού.

Ασφαλή επικοινωνία (Secure messaging): είναι μια διεργασία κρυπτογράφησης που διασφαλίζει την μεταφορά δεδομένων στις GPK cards.

File Descriptor: Ένα στοιχείο που παράγεται κατά την δημιουργία του αρχείου και χρησιμοποιείται από το GPK για την διαχείριση αρχείων.

File Identifier: Τμήμα του file descriptor. Μια 2-byte τιμή που χρησιμοποιείται για την αναγνώριση αρχείου (MF, DF ή EF) μέσα σε φάκελο(directory). Τα πέντε least significant bits (lsb) είναι το **Short File Identifier(** SFI), το οποίο χρησιμοποιείται από συγκεκριμένες εντολές και μεθόδους για την αναγνώριση αρχείων.

3.6 Δομή των αρχείων (File Body Structure)

Στο σώμα ενός EF αρχείου αποθηκεύονται δεδομένα, οι GPK κάρτες μπορούν να αποθηκεύσουν έως τέσσερεις διαφορετικές δομές EF. Οι οποίες είναι :

3.6.1 Transparent Files

Ένα transparent file συντελείται από μια ακαθόριστη ακολουθία από bytes, που μπορεί να προσπελαστεί καθορίζοντας ένα σημείο σχετισμένο με την αρχή του EF.

3.6.2 Structured Files

Χωρίζονται στους ακολούθους τύπους αρχείων:

• Γραμμικά στατικά αρχεία (Linear fixed files)

• Γραμμικά δυναμικά αρχεία (Linear variable files)

• Κυκλικά- επαναλαμβανόμενα αρχεία (Cyclic files)

3.6.3 Linear fixed files

Ένα linear fixed file συντελείται από μια ακολουθία εξατομικευμένων αναγνωρίσιμων εγγραφών ιδίου μεγέθους . Το μέγεθος αυτό καθορίζεται κατά την δημιουργία του αρχείου και αποθηκεύεται στον περιγραφέα του αρχείου (file descriptor) . Οι εγγραφές αναφέρονται ως #1, #2, #3, ... ανάλογα με την σειρά δημιουργίας τους.

3.6.4 Linear variable files

Ένα linear variable file συντελείται από μια ακολουθία εξατομικευμένων αναγνωρίσιμων εγγραφών μεταβλητού μεγέθους. Οι εγγραφές αναφέρονται όπως και οι linear fixed. Τα αρχεία χειρίζονται από τη διεπαφή(interface) ως μια ακολουθία ανεξάρτητων εγγραφών.

3.6.5 Cyclic elementary files

Ένα cyclic EF συντελείται από μια ακολουθία εγγραφών ίδιου μεγέθους και αποθηκεύουν πληροφορίες με χρονολογική σειρά. Όταν όλες οι εγγραφές έχουν χρησιμοποιηθεί για αποθήκευση, τότε μια αναβάθμιση μίας εγγραφής κάνει overwrite την παλαιότερη εγγραφή. Ο μέγιστος αριθμός εγγραφών είναι 254. Τα αρχεία χειρίζονται από τη διεπαφή ως μια ακολουθία ανεξάρτητων εγγραφών. Το μέγεθος αυτό καθορίζεται κατά την δημιουργία του αρχείου και αποθηκεύεται στον περιγραφέα του αρχείου (file descriptor) . Οι εγγραφές αναφέρονται ως #1, #2, #3, ... αντιστρόφως ανάλογα με την σειρά δημιουργίας τους. Αυτό σημαίνει ότι η τελευταία εγγραφή θα αριθμείται ως #1, δηλαδή η τρέχουσα εγγραφή θα είναι πάντα το #1. Κατά την επιλογή ενός cyclic EF η τρέχουσα εγγραφή είναι επίσης #1.

3.7 Τύποι EF

Οι GPK cards μπορούν να αποθηκεύσουν έως εφτά διαφορετικούς EF τύπους :

3.7.1 Αρχεία πορτοφολιού (Purse files)

Το κάθε GPK purse file μπορεί να περιέχει μόνο ένα πορτοφόλι. Κάθε DF μπορεί να περιέχει μέχρι 32 purse files, τα οποία πρέπει να είναι τα πρώτα 32 αρχεία που δημιουργηθήκαν σε ένα DF.

3.7.2 Ενισχυμένα αρχεία πορτοφολιού (Enhanced purse files)

Τα GPK purses μπορούν να ενισχυθούν έτσι ώστε να μπορούν να περιέχουν επιπλέον μεθόδους. Τα Enhanced purse files περιέχουν ένα έξτρα πεδίο 5 θέσεων το οποίο μπορεί να χρησιμοποιηθεί για την προστασία της λειτουργίας **Credit**με ένα μυστικό κωδικό. Επίσης μπορεί να χρησιμοποιηθεί για την εξακρίβωση του ιεραρχικού επιπέδου των access conditions για τις λειτουργίες **Read Balance**, **Debit, και Credit** και έτσι αποφασίζεται εάν ο μυστικός κωδικός είναι από ένα global EFsc ή από ένα local EFsc.

3.7.3 3DES key files

Τα 3DES key files αποθηκεύουν κρυπτογραφικά κλειδιά που χρησιμοποιούνται σε όλες τις GPK κρυπτογραφικές συναρτήσεις. Το MF και κάθε DF μπορούν να αποθηκεύσουν περισσότερα από ένα 3DES key files.

Το GPK χρησιμοποιεί διαφορετικούς τύπους κρυπτογραφικών κλειδιών:

• **Administration keys** χρησιμοποιούνται για τον υπολογισμό των προσωρινών administration keys και για secure messaging.

• **Payment keys** χρησιμοποιούνται για εντολές πληρωμής (payment) commands όπως παραγωγή πιστοποιητικού συναλλαγής και για τον υπολογισμό των προσωρινών certification keys.

• **Log keys**

Χρησιμοποιούνται για να αρχικοποιήσουν μια συνεδρία συναλλαγών αλλά όχι για συνεδρία διαχείρισης (administration session), παρ' όλα αυτά όταν ένα κλειδί συνόδου εξάγεται από ένα log key μπορεί να χρησιμοποιηθεί για συνεδρία διαχείρισης (administration session) όπως secure messaging.

• **Signature keys**

Είναι payment keys προορισμένα για υπολογισμό υπογραφών (signatures).

• **Authentication keys**

Χρησιμοποιούνται για εντολές ταυτοποίησης και μόνο.

• **Public key files**

Ένα public key file είναι ένα γραμμικό μεταβλητό αρχείο. Μπορούν να κατασκευαστούν όσα public key files είναι απαραίτητο μέσα σε ένα DF. Οι εντολές PK crypto μπορούν να αναφέρονται σε ένα public key file από το SFI του. Ένα GPK, public key file μπορεί να περιέχει :

•Μέχρι ένα public key και ένα private key δημιουργημένα από key elements

• Πιστοποιητικά (Certificates), τα οποία θα είναι υπογραφές από ένα σετ κλειδιών από μία Certification Authority (CA).

Και τα public όπως και τα private key τα μπορούν να είναι είτε DSA key στοιχεία είτε RSA key στοιχεία. Τα DSA key στοιχεία έχουν κλειδί της τάξης μεγέθους των 512 bits ή 1,024 bits, ενώ τα RSA key στοιχεία έχουν μεγέθη 512, 768 ή 1,024 bits. Σε κάθε περίπτωση, ο συντελεστής ισούται με το μέγεθος του κλειδιού. Τα Private keys χρησιμοποιούνται από την κάρτα για εσωτερική ταυτοποίηση(internal authentication) ή υπογραφή συναλλαγών. Ενώ το τερματικό, για εξωτερική ταυτοποίηση(external authentication) και επιβεβαίωση των συναλλαγών της κάρτας. Επίσης το τερματικό επιβεβαιώνει ότι τα public keys της κάρτας έχουν πιστοποιηθεί από CA, μέσω του card certificate.

• Transaction manager files

Κάθε DF που περιέχει πορτοφόλι(purse file) πρέπει επίσης να περιέχει και ένα αρχείο διαχειριστή συναλλαγών (transaction manager file), με σκοπό να αναγνωρίζει κάθε εντολή payment.Το κάθε transaction manager file είναι transparent EF και έχει μέγεθος 8 bytes.Το MF και κάθε DF μπορούν να έχουν μόνο ένα transaction manager file.

Το transaction manager file περιέχει :

• Έναν μετρητή: Card Transaction Counter (CTC), μεγέθους 3byte, ο μετρητής αυτός αυξάνει κάθε φορά που μια payment transaction session ξεκινάει δηλαδή (κάθε φορά που η εντολή **Select Purse & Key** εκτελείται).

Ο CTC χρησιμοποιείται ως μεταβλητό στοιχείο σε cryptographic processing τύπου payment.

• Backup του CTC

Υλοποιείται με την χρήση ενός μηχανισμού backup.Ο μηχανισμός χρησιμοποιεί δύο καταχωρητές (current value και previous value) για να διατηρήσει την ακεραιότητα του μετρητή.

• Secret code files

Το secret code file είναι transparent EF. Τα MF και κάθε DF μπορούν να περιέχουν μέχρι ένα secret code Elementary File (EFsc). Μόνο το πρώτο secret code file που θα δημιουργηθεί σε ένα DF (ή στο MF) μπορεί να αναγνωριστεί από το operating system.Το κάθε secret code file μπορεί να αποθηκεύσει μέχρι και οκτώ μυστικούς κωδικούς, ταξινομημένους με διευθύνσεις, αριθμώντας τους από 0 έως 7. Ανάλογα με την σειρά που εμφανίζονται στο αρχείο. Ο κάθε κωδικός αποθηκεύεται σε οκτώ bytes. Τα τέσσερα πρώτα αντιστοιχούν στην επικεφαλίδα (header), τα οποία ακολουθούνται από μία τετραψήφια byte code value. Η επικεφαλίδα αποκλείει την ανάγνωση των δεδομένων με την χρήση της εντολής **Get Info.** Οι τιμές των μυστικών κωδικών είναι απροσπέλαστες από τον έξω κόσμο.

• Internal Application Data Files

Το Internal Application Data File (IADF) είναι ένα συγκεκριμένο αρχείο, το οποίο μπορεί να προσπελαστεί από το GPK με σκοπό την πρόσβαση σε πληροφορίες για ένα DF, μετά από την εκτέλεση της **Select command.** Το IADF επιτρέπει την υλοποίηση του File Control Information (FCI) να επιστρέφεται μετά από την επιλογή ενός DF, συμφώνα με τις προδιαγραφές της EMV (*EMV—IC Card Specifications for Payment Systems, Parts 1, 2, 3).* Το IADF είναι transparent file με συγκεκριμένη file descriptor byte(FDB) τιμή, και αναβαθμίζεται με την βοήθεια των εντολών **Update Binary και Write Binary**. Οι GPK cards προστατεύουν την πρόσβαση στα αρχεία με την χρήση μυστικών κωδικών ή μυστικών κλειδιών 3DES. Οι μυστικοί κωδικοί αποθηκεύονται στα secret code Elementary Files (EFsc). Όταν το τερματικό προσπαθεί να προσπελάσει τα αποθηκευμένα δεδομένα ενός EF, η card ελέγχει εάν τη συνθήκη EF access για να δει τα δικαιώματα πρόσβασης στο αρχείο, εάν είναι προστατευμένο από μυστικό κωδικό ή εάν ο τύπος πρόσβασης που επιχειρείται (**Update, Append / Write, Read**) επιτρέπεται. Εάν το αρχείο είναι προστατευμένο από μυστικό κωδικό, η card ελέγχει τον αντίστοιχο καταχωρητή ταυτοποίησης για να επιβεβαιώσει ότι ο μυστικός κωδικός είναι επιτυχώς και παρών.

3.8 Συνθήκες Πρόσβασης (Access conditions)

Οι Access conditions βρίσκονται στους descriptors των DF και EF. Περιέχουν δύο τμήματα:

3.8.1 AC group

• Ένα γκρουπ AC που καθορίζει το επίπεδο προστασίας.

Κάθε τύπος πρόσβασης (**Update, Append / Write, Read**) μπορεί να προστατεύεται το πολύ από δύο μυστικούς κωδικούς. Επίσης αυτό το τμήμα περιέχει πληροφορίες σχετικά με το 3DES key που χρησιμοποιείται για να παράγει session keys για κάθε secure messaging στο αρχείο. Οι πληροφορίες αυτές είναι το level (global ή local) και το Short File Identifier (SFI) για το key file. Το Group AC αποθηκεύεται σε ένα προκαθορισμένο τμήμα του file descriptor των DF ή EF.

3.8.2 AC Secret Code Reference

• Το AC Secret Code Reference αναφέρεται στο secret code file (global ή local) και στους secret code αριθμούς. Το AC Secret Code Reference αποθηκεύεται στο μεταβλητό τμήμα του file descriptor των DF ή EF. Access conditions προδιαγράφουν τα ακόλουθα:

• Οι μυστικοί κωδικοί πρέπει να υποβάλλονται πριν την χορήγηση της αδείας εισόδου σε ένα αρχείο.

• Το 3DES key file περιέχει το κλειδί που χρησιμοποιείται για secure messaging transactions με το αρχείο.

Οι Access conditions αρχικοποιούνται με την εντολή **Create File,** κατά την

δημιουργία ενός αρχείου. Μπορούν επίσης να είναι κλειδωμένες ή «τοποθετημένες ανάλογα με το επίπεδο »(localized) με την χρήση της εντολής **Freeze AC** σε κάθε στάδιο του κύκλου ζωής της κάρτας.

• Κλειδώνοντας μια access condition σημαίνει η ρύθμιση της στο 1 έτσι ώστε να αρνείται την πρόσβαση μόνιμα.

• Localizing μια access condition σημαίνει μετακίνηση του access condition key ή του secret code references από το MF EFKey και το EFsc files στα γονικά (parent) DF EFKey και EFsc files.

Group #	In a Dedicated File	In an Elementary File
1	**Create** sensitive files **Freeze AC** in sensitive files	**Update Binary** **Update Record**
2	**Create** data files **Freeze AC** in data files	**Write Binary** **Append Record**
3	Not used	**Read Binary** **Read Record**

Πίνακας 5. AC groups σε DF και EF

3.9 GPK Security

Το GPK περιλαμβάνει ένα σύνολο εντολών που υλοποιούν κρυπτογραφικές συναρτήσεις από ένα πλήρες σχήμα(ομάδα) εφαρμογών ασφαλείας : authentication, υπολογισμός του temporary key, παραγωγή Certificate, υπογραφές και secure messaging. Το temporary key είναι ένα κρυπτογραφικό κλειδί, που οι GPK κάρτες χρησιμοποιούν για κρυπτανάλυση (cryptographic processing). Όταν παράγεται ένα temporary key, τα κρυπτογραφικά χαρακτηριστικά μπορούν να χρησιμοποιηθούν. Αυτά είναι :

• Ταυτοποίηση μιας μεταφοράς εντολής διαχειριστή με την χρήση secure messaging.

• Συναλλαγές αυξημένης ασφάλειας με την χρήση κρυπτογραφημένων πιστοποιητικών.

3.10 Κρυπτογράφηση δημόσιου κλειδιού (Public Key Cryptography)

Το GPK περιλαμβάνει μια σειρά από εντολές που υλοποιούν κρυπτογράφηση δημόσιου κλειδιού. Μερικές από αυτές τις εντολές είναι : διαχείριση υπογραφής (manage signature), ταυτοποίηση και κρυπτογράφηση των κλειδιών (verification and the unwrapping of keys). Ένα κλειδί συνόδου κρυπτογραφείται με την χρήση αλγορίθμου δημοσίου κλειδιού και αποστέλλεται. Ο δέκτης αποκρυπτογραφεί το κλειδί με την χρήση τον ίδιο δημοσίου κλειδιού αλγόριθμο.

3.11 Επικοινωνία (Communication)

Οι GPK κάρτες στέλνουν και λαμβάνουν δεδομένα σύμφωνα με το πρωτόκολλο επικοινωνίας : T = 0 και δομή σύμφωνα με το 7816-3 standard. Επιπλέον, το GPK έχει δυνατότητα μεγίστης ταχύτητας μεταφοράς δεδομένων σε εισόδου /εξόδου διεργασίες. Η ταχύτητα αυτή μπορεί να προσαρμοστεί συμφώνα με τις ανάγκες του χρήστη με την βοήθεια της εντολής **Switch Speed.** Ο «διάλογος» μεταξύ συσκευής και κάρτας πραγματοποιείται σε βήματα, που ορίζονται ως εξής:

a. σύνδεση και ενεργοποίηση των επαφών από τη συσκευή

b. Reset της κάρτας

c. ανταπόκριση από την κάρτα με το σήμα Answer To Reset (ATR)

d. ανταλλαγή πληροφοριών μεταξύ κάρτας και συσκευής

e. απενεργοποίηση των επαφών από τη συσκευή (όταν η συναλλαγή έχει πραγματοποιηθεί ή έχει εντοπιστεί απομάκρυνση της κάρτας από τη συσκευή).

Σύμφωνα με το ISO7816 3.3 για το ATR υπάρχουν δυο τρόποι για μετάδοση της απάντησης:

Ασύγχρονη μετάδοση: Μεταδίδονται στην I/O line χαρακτήρες με ασύγχρονο ημιαμφίδρομο τρόπο. Κάθε χαρακτήρας είναι 8bit.

Συγχρονισμένη Μετάδοση: Μια σειρά από bits μεταδίδονται στην I/O line με ημιαμφίδρομο τρόπο και σε συγχρονισμό με το σήμα του ρολογιού CLK.

3.11.1 ATR :Το reset της κάρτας

1 – Θεωρείται ότι η εσωτερική κατάσταση της κάρτας δεν είναι γνωστή πριν από το reset.

2 – Για να είναι εφικτή οποιαδήποτε επικοινωνία της συσκευής με την κάρτα θα πρέπει να

οριστεί το RST σε μια κατάσταση που να δηλώνει ότι υπάρχει απάντηση στη γραμμή I/O.

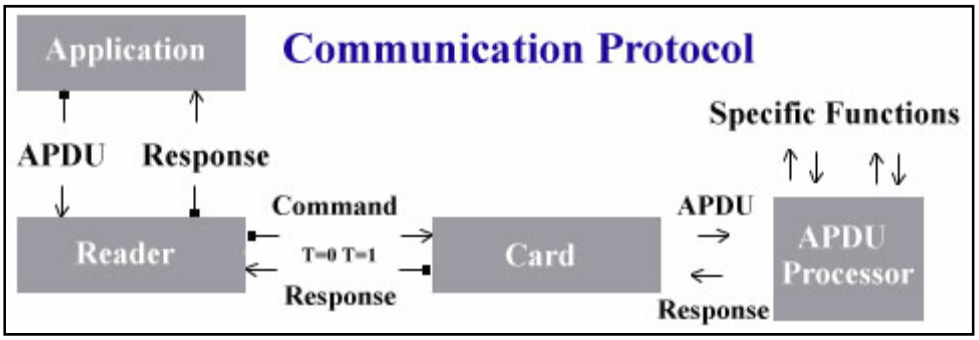
3 - Το RESET αρχίζει από τη συσκευή. Μέχρι το τέλος της ενεργοποίησης των επαφών, η κάρτα είναι έτοιμη για reset. Αφού ρυθμιστεί το σήμα του ρολογιού CLK και η I/O line, η κάρτα ύστερα από κάποιο χρονικό διάστημα (κύκλους του ρολογιού) πρέπει να επιστρέψει την απάντηση ATR. Αν μέσα στο προβλεπόμενο χρονικό διάστημα η κάρτα δεν επιστρέψει απάντηση τότε απενεργοποιούνται οι επαφές από τη συσκευή.

3.11.2 Answer to Reset σε ασύγχρονη μετάδοση

Ένας χαρακτήρας κατά την ασύγχρονη μετάδοση αποτελείται από τα παρακάτω 10 bits:

- Ένα bit εκκίνησης
- Οχτώ bits πληροφορίας (ba, bb, bc …bh)
- Ένα (δέκατο) bit bi που χρησιμοποιείται για τον έλεγχο άρτιας ισοτιμίας.

Σημειώνεται ότι η ισοτιμία είναι σωστή όταν το πλήθος των μονάδων είναι άρτιος αριθμός.



Εικόνα 20. Η δομή επικοινωνίας του APDU

Οι GPK cards δέχονται εντολές για κάθε μία από τις παρακάτω περιπτώσεις:

Case 1 - Χωρίς command ή response data. Η οποία στέλνεται ως ένα T = 0, ISO IN - TPDU με length = 0.
Case 2 - **S**hort format: χωρίς command data, αλλά με response data μεταξύ 1και 256 bytes. Η οποία στέλνεται ως ένα T = 0, ISO OUT -TPDU.
Case 3 - **S**hort format: command με data έως 255 bytes χωρίς response data. Η οποία στέλνεται ως ένα T = 0, ISO IN -TPDU.
Case 4 - **S**hort format: command data και response data έως 255 bytes. Η εντολή στέλνεται ως ένα T = 0, ISO IN -TPDU. Που όμως πρέπει να ακολουθείται από μία **Get Response** εντολή που να στέλνεται ως T = 0, ISO OUT- TPDU. Ο μηχανισμός Get Response είναι συμβατός με το ISO 7816-4 standard.

Command Format

GPK cards accept commands in the following format:

Header				Body		
CLA	INS	P1	P2	Lc	Parameters/Data	Le

Εικόνα 21. Η δομή των APDU εντολών που δέχεται το GPK

3.12 Πεδία κεφαλίδας (Header Fields)

Τα πεδία κεφαλίδας είναι υποχρεωτικά, και είναι τα εξής :

Field Name	Length	Description
CLA	1 byte	Instruction class. This can be any of the following values:
		00h ISO 7816-4/EMV compatible command
		04h ISO 7816-4/EMV compatible command with secure messaging
		80h Proprietary command
		84h Proprietary command with secure messaging
INS	1 byte	Instruction code. This is given with the command descriptions.
P1	1 byte	Parameter 1
P2	1 byte	Parameter 2

Πίνακας 6. Τα πεδία κεφαλής του APDU

3.13 Πεδία κορμού (Body Fields)

Το τμήμα κορμού είναι προαιρετικό και περιλαμβάνει τα εξής :

Field Name	Length	Description
Lc	1 byte	Data length
Data	n bytes	Command parameters or data
Le	1 byte	Expected length of data to be returned

Πίνακας 7.Τα πεδία κορμού του APDU

Response Format

Οι GPK κάρτες επιστρέφουν απαντήσεις στις εντολές στην ακόλουθη μορφή:

Body	Trailer
Data	SW1, SW2

Το σώμα (Body) είναι προαιρετικό και περιέχει τα δεδομένα που επιστρέφονται από την κάρτα

Το Trailer περιέχει τα εξής υποχρεωτικά πεδία:

• SW1: Status byte 1, που επιστρέφει το αποτέλεσμα της επεξεργασίας της εντολής

• SW2: Status byte 2, που επιστρέφει την επεξήγηση της επεξεργασίας της εντολής

3.14 Administration Commands

Το κεφάλαιο αυτό δίνει μια συνοπτική περιγραφή των administration εντολών. Αυτές περιλαμβάνουν ISO εντολές, όπως επίσης και ένα συμπληρωματικό σύνολο non-ISO εντολών που εκτελούν administration καθήκοντα (για παράδειγμα, η δημιουργία αρχείου). Ο ακόλουθος πίνακας (σελ. 37) δίνει μια σύντομη περίληψη των εν λόγω εντολών. Οι εντολές αυτές αποτελούν τον πυρήνα του GPK.

Cmd.	Full Name	Description
ApdRec	Append Record	Προσθέτει μία νέα εγγραφή σε ένα structured file.
CrtFile	Create File	Δημιουργεί ένα Elementary File (EF) ή ένα Dedicated File (DF).
ExtAut	External Authenticate	Προκαλεί τον έλεγχο ενός cryptogram που στέλνεται από τον έξω κόσμο στην κάρτα.
FreezeAC	Freeze Access Conditions	Κλειδώνει ή εντοπίζει την κατάσταση πρόσβασης σε ένα αρχείο.
GetChal	Get Challenge	Παράγει έναν 8-byte ή 32-byte τυχαίο αριθμό.
GetCSN	Get CSN	Επιστρέφει το Card Serial Number (CSN).
GetInfo	Get Info	Επιστρέφει διαφορές πληροφορίες για την κάρτα (όπως πχ. για τα αρχεία).
GetResp	Get Response	Ανακτά και διαγράφει τα δεδομένα που παρασκευάζονται από την κάρτα μνήμης RAM σε ανταπόκριση με την προηγούμενη εντολή.
IntAut	Internal Authenticate	Προκαλεί τον υπολογισμό ενός cryptogram της κάρτας να για έλεγχο από τον έξω κόσμο.
RdBin	Read Binary	Διαβάζει τα δεδομένα από ένα transparent EFs.
RdRec	Read Record	Διαβάζει τα δεδομένα από ένα structured file.
SelFil	Select File	Επιλέγει κάποιο EF ή κάποιο DF για χρήση σε συναλλαγή.
SelFk	Select File Key	Υπολογίζει ένα προσωρινό administration key και ένα cryptogram για ταυτοποίηση.
SetCard Status	Set Card Status	Ορίζει την εξατομικευμένη flag σε 1 μόλις η προσωποποίηση της κάρτας έχει ολοκληρωθεί και καθορίζει το μέγεθος των data units.
SetCod	Set Secret Code	Κάνει unblock ή αλλάζει έναν secret code.
SwtSpd	Switch Speed	Ρυθμίζει την κάρτα σε άλλη ταχύτητα.
UpdBin	Update Binary	Ενημερώνει τα data σε ένα EF.
UpdRec	Update Record	Ενημερώνει τα data σε ένα structured file.
Verify	Verify	Συγκρίνει την τιμή που υποβλήθηκε με τον μυστικό κωδικό αριθμό (0 έως 7) στο secret code file που σχετίζονται με την τρέχουσα επιλεγμένη DF.
WrBin	Write Binary	Γράφει δεδομένα σε ένα EF πραγματοποιώντας μια λογική OR μεταξύ της τρέχουσας τιμής της εγγράψιμης περιοχής και της τιμής που γράφεται στην περιοχή αυτή.

Πίνακας 8. Οι εντολές διαχείρισης του GPK

Όπου :

Cmd.: Είναι μια συντομογραφία του ονόματος της εντολής.

3.15 Payment Commands

Οι Payment Commands είναι εντολές που χρησιμοποιούνται για την εκτέλεση συναλλαγών στο GPK. Ο ακόλουθος πίνακας δίνει μια σύντομη περίληψη από αυτές τις εντολές:

Cmd.	Full Name	Description
CanDeb	Cancel Debit	Ακυρώνει την προηγούμενη χρέωση που εκτελείται από ένα τερματικό και προαιρετικά αντικαθιστά με μία νέα χρέωση.
Credit	Credit	Πιστώνει ένα purse.
Debit	Debit	Χρεώνει ένα purse.
RdBal	Read Balance	Διαβάζει την καθορισμένη τιμή ισορροπίας ενός purse.
SelP&K	Select Purse & Key	Επιλέγει το συγκεκριμένο purse και κλειδί, στη συνέχεια, δημιουργεί ένα νέο προσωρινό payment transaction key και ένα authentication cryptogram.
SetOpts	Set Options	Ορίζει την ακόλουθη Sign command επιλέγοντας μεταξύ : - χρήση τρέχουσας purse balance στον υπολογισμό του certificate .– Άδειασμα της RAM από όλες τις παραμέτρους μετά την εκτέλεση τη Sign command.
Sign	Sign	Δημιουργεί ένα πιστοποιητικό για την συναλλαγή που έχει προηγηθεί της εντολής.

Πίνακας 9. Οι payment εντολές του GPK

4. Smart card readers

Ο smart card reader είναι μια ηλεκτρονική συσκευή που διαβάζει smart cards, τροφοδοτεί το ενσωματωμένο κύκλωμα της smart card με ηλεκτρικό ρεύμα, λειτουργεί ως μέσο μετάδοσης δεδομένων από ένα σύστημα σε μία κάρτα υποστηρίζοντας τα ανάλογα πρωτόκολλα επικοινωνίας, ενώ κάποιοι reader έχουν αναβαθμίσιμο firmware. Υπάρχουν εξωτερικές και εσωτερικές υποδοχές card reader συσκευές. Όπως επίσης υπάρχουν laptops και πληκτρολόγια που έχουν ενσωματωμένο smart card reader. Η τιμή ποικίλει ανάλογα με τον αριθμό των reader που παραγγέλνονται όπως επίσης και από το μοντέλο παρ' όλα αυτά συνήθως κυμαίνεται σε χαμηλά επίπεδα, περίπου στα 10 - 20 €. Αρχικά οι smart card reader συνδέονταν με ένα σύστημα μόνο με σειριακή θύρα (Serial port) με αρκετά προβλήματα σε θέματα επικοινωνίας λόγω έλλειψης οδηγών διαχείρισης και χαμηλής ταχύτητας. Όμως με βάση τα πιο πρόσφατα πρότυπα PC/SC και CCID, έχουν αναπτυχθεί σύγχρονοι τρόποι επικοινωνίας μέσω USB συσκευών με ειδική κλάση συσκευής (device class) `0x0B`. Οι readers με αυτήν την κλάση δεν χρειάζονται οδηγούς (device drivers) διότι παρέχονται από τους κατασκευαστές λειτουργικών συστημάτων. Τέλος υπάρχουν και ασύρματοι readers που λειτουργούν με τα κοινά wireless πρότυπα (802.11) και φυσικά το κόστος είναι αρκετά υψηλότερο σε σχέση με έναν ενσύρματο reader.

4.1 PC USB-SL

Εικόνα 22. Ο PC USB-SL smart card reader

Όνομα μοντέλου	Πλαίσιο	Διαστάσεις
PC USB-SL	Slim Line	98 x 70 x 15 mm

4.1.1 PC USB-SL Applications

Ο PC USB-SL είναι ένας αναγνώστης καρτών (card reader), σχεδιασμένος για χρήση σε PC, ιδιαίτερα εύκολος και απλός στην χρήση.

Ο PC USB-SL υποστηρίζει:

- e-banking, electronic commerce
- Λειτουργίες ηλεκτρονικού πορτοφολιού (e-purse)
- Ασφαλή πρόσβαση σε υπολογιστή και ένα μεγάλο πλήθος μηχανισμών ασφαλείας

Προσφέρει δυνατότητες όπως :

- Έλεγχος πρόσβασης
- Ηλεκτρονικό εμπόριο
- Διαμόρφωση και προσαρμογή των καρτών
- Ανάπτυξη εφαρμογών για κάρτες

4.1.2 PC USB-SL Προτερήματα

Ο PC USB-SL αναλαμβάνει την διαχείριση της διασύνδεσης με την κάρτα, αφήνοντας μόνο την διαχείριση των σημαντικών λειτουργιών για τον κύριο υπολογιστή. Συμβατός με όλα τα λειτουργικά συστήματα και είναι συμβατός με κάθε USB type A, ανεξάρτητος από κάθε είδους περιορισμούς που σχετίζονται με θέματα τροφοδοσίας. Ο PC USB-SL είναι βασισμένος στα πρότυπα της Gemalto PC Core ® για hardware και λογισμικό (firmware), γεγονός που συνεπάγεται ότι ο PC USB-SL μπορεί να χειριστεί όλους τους τύπους έξυπνων καρτών, συμβατών με τα πρότυπα ISO7816 χωρίς προβλήματα συμβατότητας. Είναι φιλικό προς τον χρήστη και δεν απαιτεί ιδιαίτερες γνώσεις για την χρήση του, η εγκατάσταση του γίνεται εύκολα και σχεδόν αυτόματα. Τέλος, είναι συμβατός με όλα τα κύρια λειτουργικά περιβάλλοντα (Windows ® 98, 2000, Xp, Vista, Linux και MacOS). Ο PC USB-SL έχει επιτυχώς περάσει τον Microsoft Windows Hardware Quality Lab (WHQL) έλεγχο και είναι δικαιούχος για τον τίτλου "Designed for Microsoft Windows" για τα Windows 2000, Xp και Vista. Ο PC USB-SL είναι βασισμένος στο Gemcore Twin Pro IFM, το οποίο έχει λάβει το EMVCo letter of approval (# 11607 0103 400 20 LGA) και είναι συμπεριλαμβανημένο στις συσκευές υποστήριξης του EMV Level 1 συμμορφωμένο με το 4.0 device στο EMVCo[13]. Ο PC USB-SL είναι πλήρως συμμορφωμένος με τις Chip/Smart Card Interface Devices (CCID) rev 1.00 προδιαγραφές [14] Ώστε να δύναται να χρησιμοποιηθεί με τους Microsoft USB CCID τύπους οδηγού χρήσης (Class Driver) για Windows 2000, Xp, Server 2003 & Vista.

[13] http://www.emvco.com

[14] http://www.usb.org/developers/devclass_docs/ccid_classspec_1_00a.pdf

4.1.3 PC USB-SL Technical Specifications

Τα τεχνικά χαρακτηριστικά χωρίζονται στις παρακάτω κατηγορίες:

- Smart-card interface
- Θερμοκρασίες λειτουργίας/αποθήκευσης
- Electro-magnetic standards
- Security levels
- Standards/certifications
- Υποστηριζόμενα Λειτουργικά συστήματα
- API's

4.1.3.1 Smart-card interface

- Υποστήριξη ISO7816 Class A, B και C (5V, 3V, 1.8V)
- Υποστήριξη όλων των ISO7816 TA1 παραμέτρων (μέχρι και 344 Kbps)
- Διαβάζει και γράφει σε όλους τους ISO 7816-1,2,3,4 κάρτες μικροεπεξεργαστών (microprocessor cards), στα πρωτόκολλα T=0 και T=1
- Εντοπισμός Short circuit
- Ο connector της smart card είναι 8 σημείων επαφής (friction contacts) τοποθετημένους κατά ISO , εγγύηση για 100,000 κύκλους εισαγωγής, μηχανικά προσαρμοσμένος σύμφωνα με το EMV level 1.
- Υποστήριξη και διακοσμημένων smart cards.

Human Interface

- Φωτοδίοδος (LED) ενός χρώματος (πράσινο)

Host Interface

- USB μέγιστη ταχύτητα (12 Mbps)
- Hubless
- Καλώδιο μήκους 1,5 μέτρα
- Σύνδεση USB type A
- Τροφοδοσία (Power supply) μέσω του USB port
- Τάση λειτουργίας (4.4 - 5.5)Volt

4.1.3.2 Θερμοκρασίες λειτουργίας/αποθήκευσης

- Λειτουργίας : +5°C / +55°C
- Αποθήκευσης : -25°C / +60°C

4.1.3.3 Electro-magnetic standards

- Europe: 89/336/CEE guideline
- EN 55022: 1994 Class B

- EN 50082-1: 1994
- EN 50081-1: 1992
- EN 61000-4-2: 1995
- EN 61000-4-3: 1997
- EN 61000-4-4: 1995
- Comply with EMC directive 89/336/EEC
- USA: FCC part 15 Class B

4.1.3.4 Security levels

- Europe: EN60950
- IEC950: 1991, Am,3: 1995
- USA: UL1950 third edition, dated July 28, 1995
- Canada: CSA950
- Συμμορφωμένο με την οδηγία χαμηλής τάσης 73/23/EEC

4.1.3.5 Standards/certifications

- ISO/IEC 7816-1,2,3,4: IC Cards με επαφές
- EMV level 1, EMV2000 version 4.0 για Gemcore Twin Pro IFM
- Microsoft Windows Hardware Quality Labs (WHQL), Windows Logo Program WLP 2.0
- USB 2.0 full speed
- CCID - Chip card Interface device 1.0
- Συμβατό ROHS
- WEEE marking

4.1.3.6 Υποστηριζόμενα Λειτουργικά συστήματα

- Windows 98, 98SE, Me, 2000, Xp, Vista 64 bits
- Windows Server 2003
- Windows Xp, Server & Vista 64 bits
- Linux Redhat WS3.0, WS4.0, Suse Professional 9.2, DEBIAN "Sarge"
- Win CE 4.1, 4.2, 5.0
- Mac OS X (10.3 and higher)

4.1.3.7 API's

- Microsoft PC/SC environment with associated drivers

4.2 Ο TEO BY XIRING: USB και PC/SC smart card reader της XIRING

Εικόνα 23. Ο smart card reader Teo by Xiring

4.2.1 Τεχνικά χαρακτηριστικά και πιστοποιητικά[15]

Ο Teo by XIRING είναι συμμορφούμενος με τα PC / SC & CCID, USB- smart card reader (class 1 reader). Προορίζεται να χρήση σε εφαρμογές όπου η εφαρμογή του υπολογιστή οδηγεί τον αναγνώστη σε διασύνδεση με την έξυπνη κάρτα (λειτουργεί επίσης με το Mac OS και σε περιβάλλον Linux).

[15] TEO BY XIRING V.2 – 01/06/2007 - http://www.infoestrutura.com.br/download/book_teo_by_xiring_eng.pdf

Host interface	• USB 2.0 (& USB 1.1) full speed (12Mbps)
Smart Card Interface	• ISO 7816 ; EMV 2000 Level 1 ; T=0, T=1 • Communication speed: Up to 420Kbps (depending on the card)
Supported smart cards	• ISO 7816 1-4 compliant microprocessor cards
Certifications	• USB 2.0 full speed (and USB 1.1) • EMV 2000 Level 1 • WHQL certified for Microsoft Windows 2000 & XP • Microsoft Windows Vista certified • CE • FCC Part 15 Class B • RoHS
Supported environments	• Windows 2000, XP, Vista (PC/SC & CCID compatible environments). • *NB: Teo by XIRING has been tested in MacOS X+ and Linux environments.*
Available drivers	• CCID Compliant (working with the CCID driver included in Win2K/XP)
Physical characteristics	• Size: 86x68x10 mm • Weight: Less than 65g • Cable: 1.4m
Other	• Working in 3 positions, thanks to the adjustable base (0°, 15°, 75°) • One high luminosity LED (red/green) • Dedicated area for your logo (via printed sticker) • Two double-side tapes to stick the product on a desk • Tech support: 2nd level support provided by eMail

Πίνακας 10. Τα χαρακτηριστικά του TEO BY XIRING

Ο Teo by XIRING είναι συμμορφωμένος με όλα τα απαραίτητα certificates:

CE Certification:

EMITECH

CERTIFICAT DE CONFORMITE

CERTIFICATE OF CONFORMITY

CC - 06 - 139

Suite aux essais effectués dans ses laboratoires, EMITECH certifie que l'équipement référencé ci-dessous est conforme aux normes :

Following tests performed in its laboratories, EMITECH declares that the equipment specified below complies with the standards:

EN 55022 : 1998 / A2 : 2003
EN 55024 : 1998 / A1 : 2001 / A2 : 2003

Comme l'atteste le procès-verbal d'essais / *As related in the tests report* : (n° RC-06-42060-1-A)

Désignation/*Brand name* : Smart card reader « TEO BY XIRING » / Lecteur de carte à puce « TEO BY XIRING »

Type/*Type*: XI-SMART VPC

Numéro de série/*Serial number* : XI6PA0047

Constructeur/*Manufacturer's name* :	XIRING
Adresse/*Manufacturer's address* :	*25, quai Gallieni* *92158 SURESNES* *FRANCE*
Essayé sur demande de/*Tested on request of* :	XIRING
Adresse :	25, quai Gallieni 92158 SURESNES FRANCE

Condition de validité du Certificat / *Validity requirements for this certificate:*

Cette attestation n'est valable que dans la mesure où l'équipement reste conforme aux normes applicables / *This attestation is only valid provided that the equipment continues to comply with the quoted specifications.*

Modification(s) de l'equipement durant les essais CEM/*Design modification(s) incorporated into the test:*

Not required

Ce certificat résulte d'essais effectués sur un exemplaire du produit, il n'implique pas une appréciation de l'ensemble de la fabrication des produits de série.

This certificate results of the tests done on one sample, it doesn't implicate a valuation of all manufactured equipments.

Laboratory EMITECH of Montigny-Le-Bretonneux and open area test site of AUNAINVILLE, le 23 November 2006

Pour EMITECH / Signed on behalf of EMITECH

Mimoun BENABDELKADER
Ingénieur d'affaires
Sales engineer

EMITECH ILE DE FRANCE - ATLANTIQUE - ANGOULEME - GRAND SUD - RHONE-ALPES eurocom

E-mail : commercial@emitech.fr - URL : www.emitech.fr

Groupe EMITECH - S.A. au capital de 490 000 € - R.C. VERSAILLES B 344 545 645 - APE 742 C

5. GemSafe Software

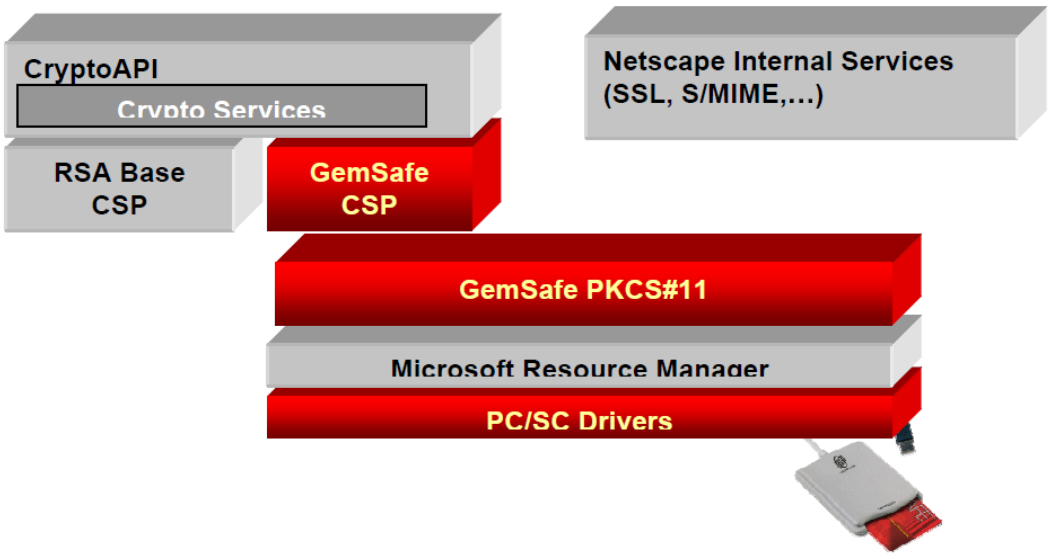
5.1 Εισαγωγή στις GemSafe Libraries

5.1.1 Τι είναι οι GemSafe Libraries;

Το Λογισμικό GemSafe Libraries είναι μία εφαρμογή κρυπτογραφικών βιβλιοθηκών βασισμένη σε smart cards, που δίνει την δυνατότητα σε άλλες εφαρμογές της χρήσης smart card cryptography σε ένα PKI περιβάλλον. Παρέχοντας έτσι μεγίστου επιπέδου ασφάλεια και φορητότητα. Το λογισμικό αυτό παρέχεται είτε ως συνοδευτικό μαζί με τις άλλες εφαρμογές της Gemalto είτε μπορεί να αγοραστεί ξεχωριστά. Σε καμία περίπτωση δεν είναι δωρεάν και δεν επιτρέπεται η διανομή του σε τρίτους. Η άδεια χρήσης του χορηγείται ανάλογα με την περίπτωση είτε σε μία εταιρία είτε σε κάποιο φυσικό πρόσωπο.

5.1.2 Αρχιτεκτονική GemSafe

Το Λογισμικό GemSafe είναι βασισμένο στα στάνταρ APIs: PKCS#11και CAPI[16], τα οποία εγκαθίστανται στο client PC, με σκοπό τρίτες εφαρμογές να έχουν πρόσβαση στις smart card, στις κρυπτογραφικές μεθόδους και στην ασφαλή αποθήκευση κλειδιών και πιστοποιητικών. Αναλαμβάνοντας την αλληλεπίδραση με τις κάρτες το Λογισμικό της GemSafe, αποκρύπτει την πολυπλοκότητα και παράλληλα επιτρέπει την ανεμπόδιστη εκμετάλλευση όλων των δυνατοτήτων των smart cards. Τέλος υποστηρίζει όλους τους συμβατούς PC/SC οδηγούς (drivers) αναγνωστών καρτών.



Εικόνα 24. Η αρχιτεκτονική δομή του λογισμικού της GemSafe

[16] PKCS#11και CAPI βλ. Παράρτημα

5.1.3 Προετοιμασία

• Απαιτήσεις συστήματος (System Requirements)

• Εγκατάσταση του λογισμικού GemSafe Libraries 4.2.0.

5.1.4 Απαιτήσεις συστήματος (System Requirements)

Λογισμικό : GemSafe Libraries 4.2.0.

5.1.4.1 Ελάχιστες απαιτήσεις Συστήματος

• 350 MB ελεύθερου χώρου στον σκληρό δίσκο

• Επεξεργαστή Pentium II 200 MHz ή νεότερο

• VGA κάρτα γραφικών που να υποστηρίζει τουλάχιστον 256 χρώματα

5.1.4.2 Λειτουργικά Συστήματα

Ο επόμενος πίνακας περιγράφει τα συμβατά λειτουργικά με την αντίστοιχη απαίτηση μνήμης που έχει το πρόγραμμα GemSafe Libraries 4.2.0

Operating System	RAM
Windows 98 SE	32MB
Windows ME	64MB
Windows NT 4.0 (SP6 or higher)	64MB
Windows 2000 Server	96MB
Windows 2000 Professional (with SP3 or SP4)	64MB
Windows XP Home (up to SP2)	64MB
Windows XP Professional (up to SP2)	64MB
Windows 2003 Server	138MB

Πίνακας 11. Υποστηριζόμενα λειτουργικά συστήματα

5.1.4.3 Περιφερειακά

Το GemSafe Libraries 4.2.0 απαιτεί τα παρακάτω περιφερειακά

- Μία ελεύθερη θήρα COM, USB ή PCMCIA.
- Έναν οδηγό CD ROM.

5.1.4.4 Υποστηριζόμενοι Card Readers

Οποιονδήποτε από τους ακόλουθους:

- GemPC Card for laptops
- GemPC400 for laptops.
- GemPC410 for desktops.
- GemPC430 designed for all workstations with a USB port (Windows 98, Me, 2000
- and XP)
- GemPC433 designed for all workstations with a USB port (Windows 98, Me, 2000
- and XP)
- GemPC Serial
- Gem e-Seal
- GemPC Twin Serial SL
- GemPC Twin USB SL
- GemPC Key

5.1.4.5 Υποστηριζόμενες Smart Cards

Οποιαδήποτε από τις ακόλουθες:

- GPK 16000, with GemSafe mapping
- GemSafe 16k (based on GPK 16000)
- GemSafe Xpresso 16k, 32k and 64k (based on GemXpresso Pro R3)
- GemSafe Xpresso 16k and 32k (based on GemXpresso Pro R3.2)
- GemXpresso 3.2 with GemSafe v1.11 applet and generic GemSafe mapping
- GemXpresso 3.2 with GemSafe v1.11 applet and Identrus mapping
- GPK v3.1 card with GemSafe generic mapping
- GPK v3.1 card with Identrus mapping
- GemXpresso 3 64K
- GemXpresso 3 32K with generic mapping

5.1.4.6 Υποστηριζόμενοι Browsers

Η πρόσβαση σε secure Web sites και η αποστολή secure e-mail μπορεί να επιτευχθεί μέσω του GemSafe Libraries 4.2.0, με οποιονδήποτε από τους ακόλουθους Web browsers:

- Microsoft Internet Explorer (IE) V 5.0 up to 7.0, που να υποστηρίζει SSL και secure E-mail.
- Netscape version 4.8 to 7.2, που να υποστηρίζει SSL και secure e-mail.
- Mozilla Firefox όλες οι version.

5.1.4.7 Υποστηριζόμενοι λογαριασμοί E-mail

Για την χρήση secure e-mail προγράμματος οι υποστηριζόμενοι λογαριασμοί είναι:

- Post Office Protocol (POP3) account.
- Internet Message Access Protocol (IMAP) compatible account.
- Mozilla Thunderbird όλες οι version.

5.1.5 Εγκατάσταση του λογισμικού GemSafe Libraries 4.2.0.

Σημειώσεις:

- Κατά την διάρκεια της εγκατάστασης στον reader δεν πρέπει να υπάρχει κάρτα.
- Η εγκατάσταση απαιτεί δικαιώματα διαχειριστή για να επιτευχθεί.
- Η εγκατάσταση του GemSafe Libraries 4.2.0 δεν διαγράφει αυτόματα παλαιότερες εκδόσεις από την GemSafe Libraries 3.0. Οι οποίες πρέπει να καταργηθούν από το σύστημα χειροκίνητα από τον χρήστη.

Εγκαθιστώντας τις GemSafe Libraries 4.2.0

Περιπτώσεις :

a) Μέσω δικτύου από τον διαχειριστή με remotely installation όπου ο χρήστης δεν χρειάζεται να επέμβει, απλά το λογισμικό ήδη βρίσκεται εγκατεστημένο στο σύστημα από τον διαχειριστή.

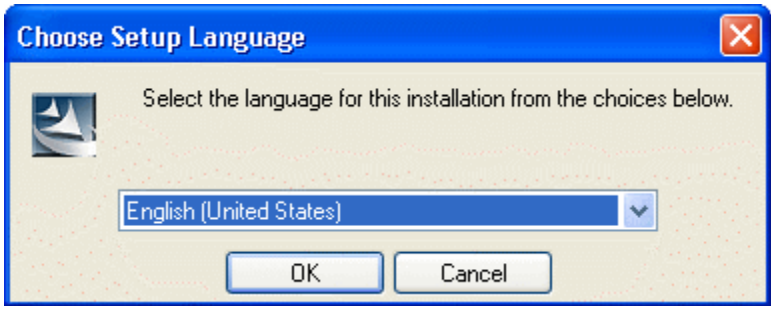
b) Μέσω CD-ROM που διανέμεται από τον διαχειριστή.

c) Μέσω δικτυακού τόπου, οπού ο διαχειριστής διαθέτει το installation program

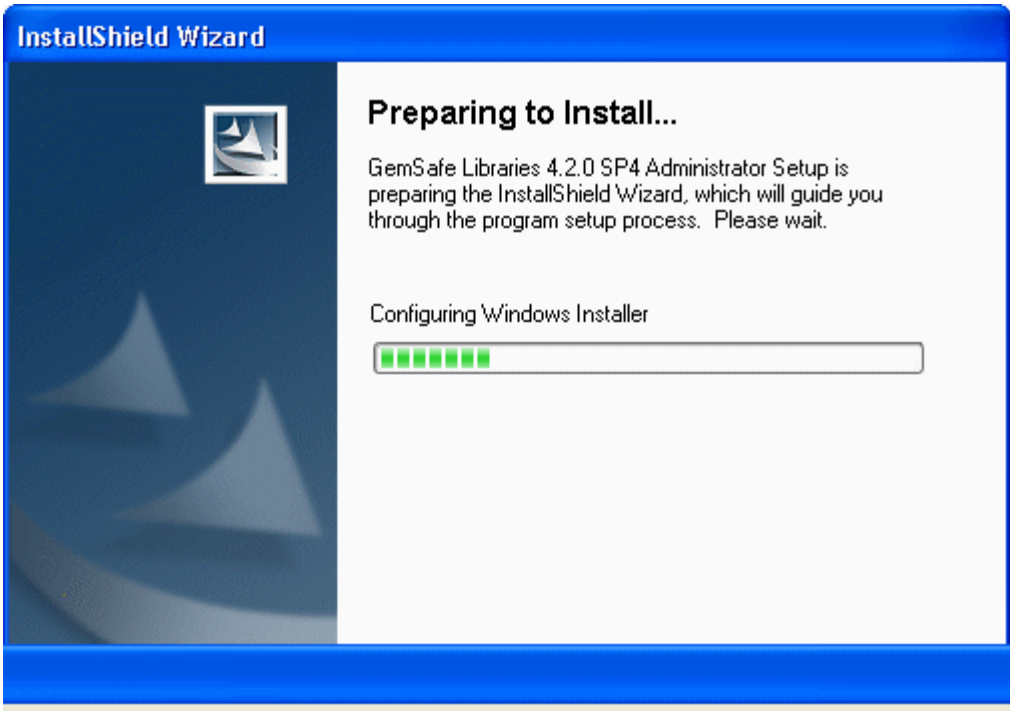
Για την εκκίνηση του installation του GemSafe Libraries, απαιτείται double-click στο **setup.exe** αρχείο:

Εικόνα 25. Το αρχείο εγκατάστασης

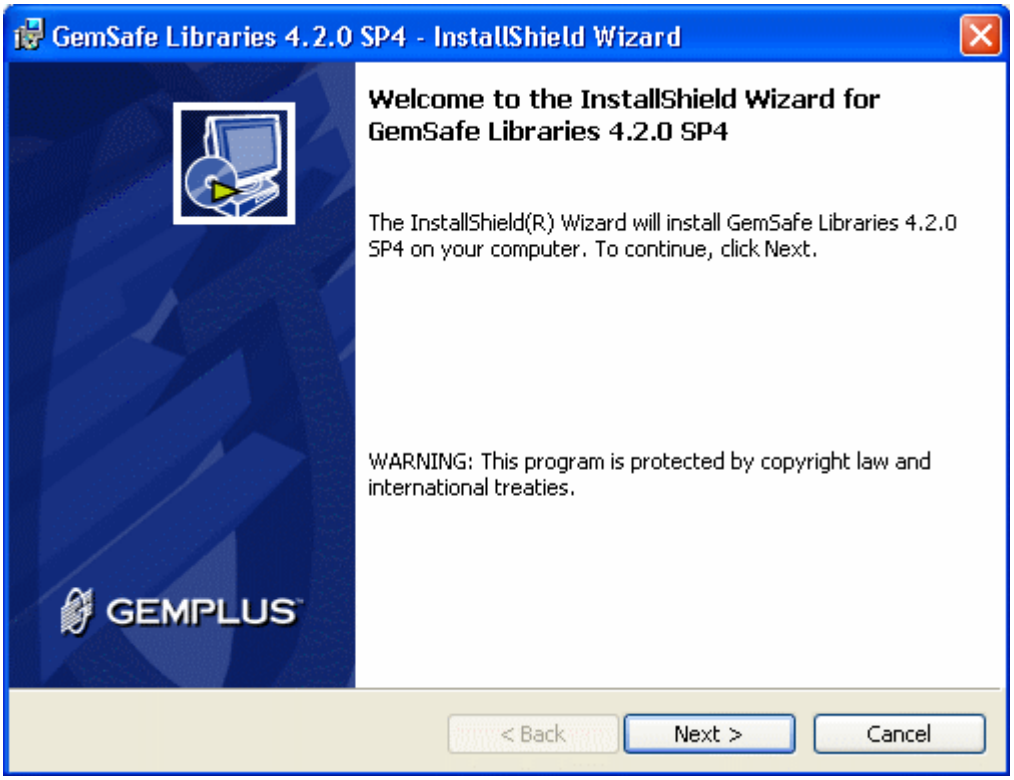
Ξεκινάει ένας **GemSafe Libraries InstallShield Wizard** με απλά βήματα καθοδηγείται η εγκατάσταση του λογισμικού, προετοιμάζοντας το πρόγραμμα ανάλογα με τις επιλογές του χρήστη



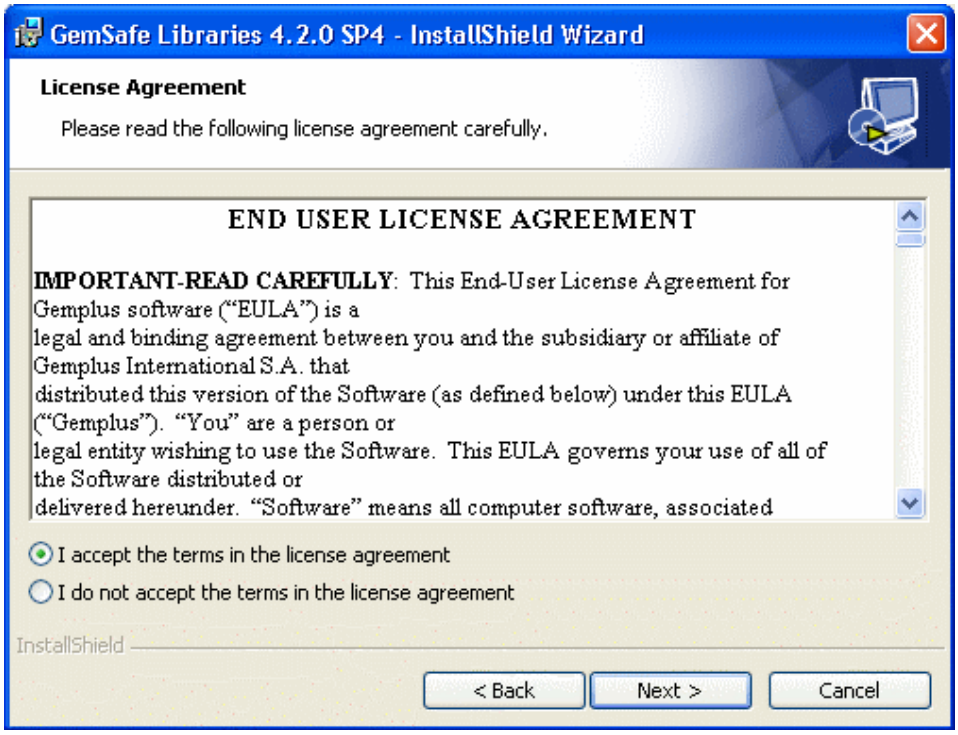
Εικόνα 26. Επιλογή γλώσσας



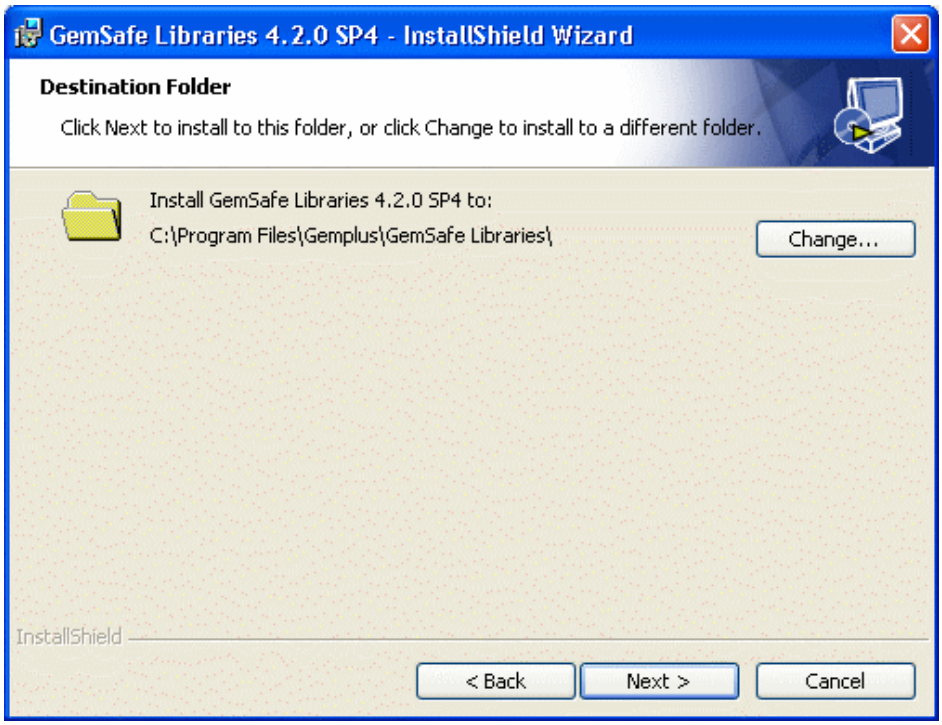
Εικόνα 27. Προετοιμασία εγκατάστασης



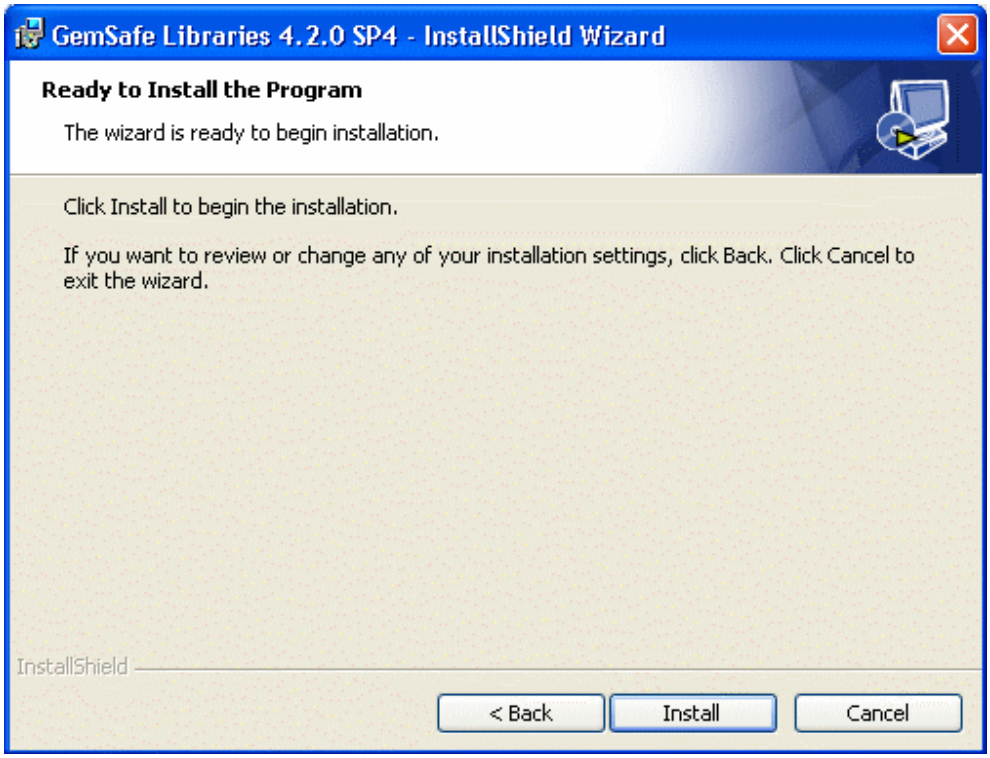
Εικόνα 28. Το Welcome παράθυρο



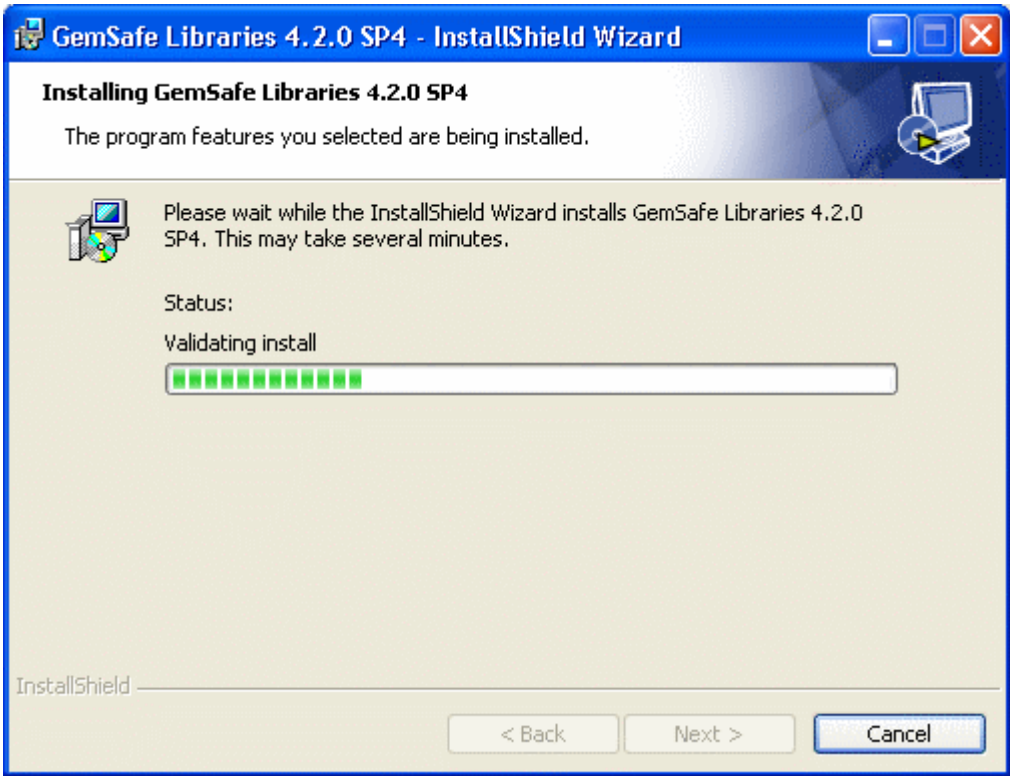
Εικόνα 29. Αδεία χρήσης του τελικού χρήστη



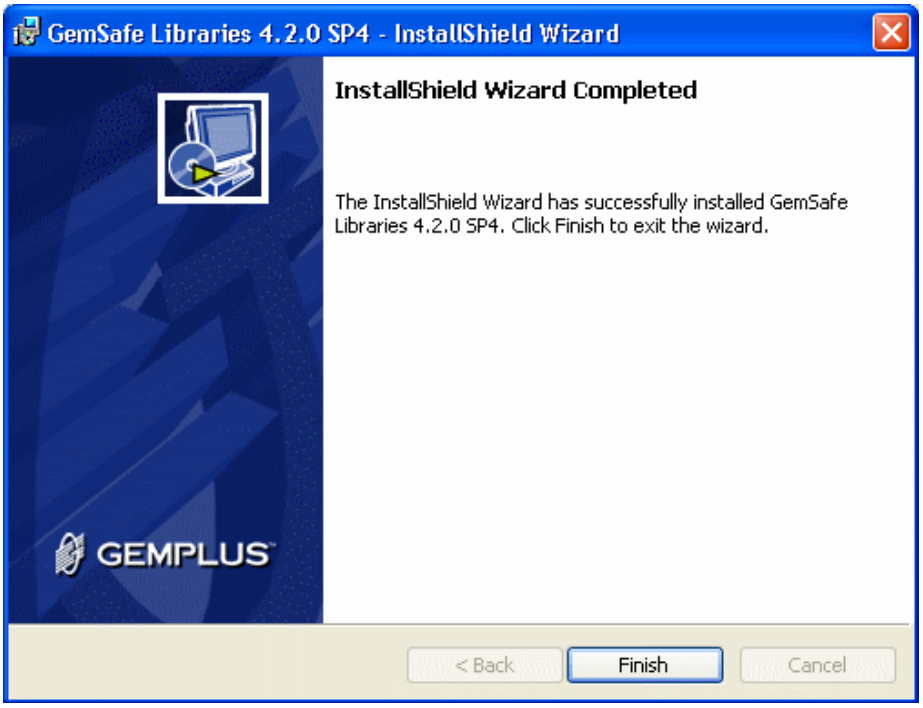
Εικόνα 30. Ορισμός φακέλου εγκατάστασης



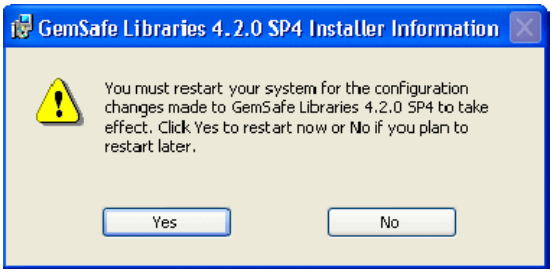
Εικόνα 31. Στάδιο έναρξης της εγκατάστασης



Εικόνα 32. Διαδικασία εγκατάστασης μέσω του InstallShield Wizard



Εικόνα 33. Επιτυχής εγκατάσταση του λογισμικού



Εικόνα 34. Απαιτείται επανεκκίνηση για να είναι διαθέσιμο το πρόγραμμα

Σημείωση:
Κατά την εγκατάσταση του Gemsafe Libraries 4.2.0 κόλλησε η εφαρμογή στο τελικό στάδιο. Στο λειτουργικό όμως υπήρχε το πρόγραμμα εγκατεστημένο. Κατά τις δοκιμές όμως χανόταν ο έλεγχος καθώς το interface έπαυε να ανταποκρίνεται, αυτό γινόταν κατά την τοποθέτηση της smart card μέσα στον reader και ενώ έπρεπε το πρόγραμμα να είναι σε θέση να φορτώνει τα δεδομένα της κάρτας δεν ανταποκρινόταν το γραφικό περιβάλλον. Πιθανότερη αιτία για το πρόβλημα αυτό ήταν κάποιο update των Windows XP που επηρέαζε τη Registry ή κάποια ασυμβατότητα της εφαρμογής με κάποιον οδηγό (driver) των Windows. Μετά από επικοινωνία με την Gemsafe και πολλές προσπάθειες σε διάφορα λειτουργικά, όλα up to date, δοκιμάζοντας μια προς μία όλες τις εκδόσεις-περιπτώσεων χρήστη-διαχειριστή σε συνδυασμό με τα tools που μου παρείχε η gemsafe support επετεύχθη η σωστή εγκατάσταση και εφαρμογή των δυνατοτήτων του Gemsafe Libraries 4.2.0 Administrator σε Windows XP, με μοναδικό up date το update driver of smart card reader.Το λειτουργικό για λόγους ευκολίας και ασφάλειας είναι guest στην virtual πλατφόρμα virtual box 1.5.0 σε host Ubuntu.

Για να τρέξει η εφαρμογή στο εικονικό περιβάλλον έπρεπε:

- ✓ Να υπάρχουν τα απαραίτητα αρχεία σε εικονικές μορφές δίσκων(.iso).
- ✓ Να υπάρχει δυνατότητα interface με USB, μέσω του host OS.
- ✓ Να είναι το μητρώο (Registry) των XP καθαρό.
- ✓ Να μην έχουν αναβαθμιστεί τα XP(up to date).

Product name	Versions	Uses cases and comments
Systems		
Windows	2000, XP, Vista , Server 2000/2003	Smart card logon, lock/unlock station
Web browsers		
Internet Explorer	v6 SP1, v7	Strong authentication with SSL
Netscape	v8.1	Strong authentication with SSL
Mozilla Firefox	v 1.5, v2,v 3	Strong authentication with SSL, PIN change, PKCS#12 file key injection
Emails		
Microsoft Outlook	2000/2003/2007, Express	Email signature and encryption
Lotus Notes	v 7.0	Email signature and encryption, email user authentication
Mozilla Thunderbird	v 1.5,v 2	Email signature and encryption
VPNs		
Check Point VPN-1	Secure Client NGX	X.509 certificate based authentication
Cisco VPN Client	v4.6	X.509 certificate based authentication
Microsoft VPN	Windows 2000 SP4, XP SP2, Vista	X.509 certificate based authentication
Certification Authorities		
Microsoft Windows CA	Server 2000/2003	Certificate enrolment and renewal
Entrust Entelligence	v7.1	Certificate enrolment and renewal
Idealx ID-PKI	v1.9	Certificate enrolment and renewal
Card Management Systems		
BellID Andis	v5.i	Certificate enrolment and renewal
Microsoft CLM	Beta 2	Certificate enrolment and renewal
Thin client and remote access		
Microsoft Terminal Services	Server 2003	Smart card logon
Wyse Thin Client	Windows CE 5.0	Smart card logon
Citrix Presentation Server	v4	Smart card logon
Office tools		
Microsoft office	2000, 2003, 2007	Documents signature and encryption, VB macros signing
Adobe Acrobat	v6, v7, v8, v9	Document encryption and signature
SUN Star Office	v8	Document signature
MSI Security Box	v6.1	Document signature
Open Office	v2.0	Document signature

Πίνακας 12. Περιπτώσεων-χρήσεων, οι εφαρμογές που είναι συμβατές με το λογισμικό της GemSafe.

5.2 GemSafe Toolbox

Εικόνα 35. Η εφαρμογή GemSafe Toolbox.

5.2.1 Περιγραφή της application

Το GemSafe Toolbox είναι μια πλατφόρμα υποστήριξης και διαχείρισης Smart card. Παρέχεται ένα φιλικό προς τον χρήστη περιβάλλον και ένα πλήθος δυνατοτήτων εκμετάλλευσης των προτερημάτων των Smart Card. Χρήση της κάρτας σε κάθε είδους λειτουργιά που παρέχεται από την εφαρμογή.

Επισκόπηση χαρακτηριστικών(data) κάρτας.

- Private and public data
- Αλγόριθμοι hash και κρυπτογράφησης
- Αλλαγή pin
- Απεμπλοκή pin
- Ορισμός πολιτικής pin(pin policy)
- Ορισμός βιβλιοθήκης
- Δημιουργία αρχείου βιβλιοθήκης
- Διαγνωστικός έλεγχος
- Reg tool

5.2.2 Επιλογές περιεχόμενων κάρτας

Ο χρήστης έχει δυνατότητα να επεξεργαστεί και να διαχειριστεί τα δεδομένα μίας κάρτας, πιο συγκεκριμένα ο χρήστης έχει δυνατότητες:

- Διαχείρισης πιστοποιητικών
- Διαχείρισης κωδικών pin

5.2.2.1 Ψηφιακά Πιστοποιητικά

Ορισμός:

Ένα ψηφιακό πιστοποιητικό είναι ένα κείμενο που λειτουργεί ως ψηφιακό διαβατήριο. Το κάθε πιστοποιητικό περιέχει το δημόσιο κλειδί του χρήστη και άλλες προσωπικές πληροφορίες για αυτόν και το πιστοποιητικό. Το πιο αποδεκτό παγκοσμίως standard για ψηφιακά πιστοποιητικά είναι αυτό που ορίστηκε ως *International Telecommunications Union standard ITU-T X.509*. Η πιο σύγχρονη έκδοση είναι η τρίτη έκδοση του X.509.

Ένα πιστοποιητικό X.509v3 περιλαμβάνει τα εξής δεδομένα:

- Αριθμό έκδοσης.
- Σειριακό αριθμό.
- Ταυτότητα αλγορίθμου υπογραφής .
- Όνομα εκδότη.
- Ημερομηνία λήξης
- Όνομα χρήστη.
- Πληροφορίες δημόσιου κλειδιού χρήστη.
- Μοναδικό αναγνωριστικό εκδότη.
- Μοναδικό αναγνωριστικό χρήστη.
- Επεκτάσεις.
- Υπογραφή των ανωτέρω πεδίων.

Για την διευκόλυνση των παραληπτών, είναι συνήθης τακτική, η επισύναψη του πιστοποιητικού σε κάθε secure e-mail που αποστέλλεται. Ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα, που περιέχεται μέσα στο πιστοποιητικό για να κρυπτογραφήσει το απαντητικό e-mail. Εάν δεν επισυναφτεί το πιστοποιητικό στο αρχικό mail, ο αποδέκτης θα πρέπει να το αποκτήσει από μία προσβάσιμη τοποθεσία, σε περίπτωση που επιθυμείται κρυπτογραφημένη απάντηση.

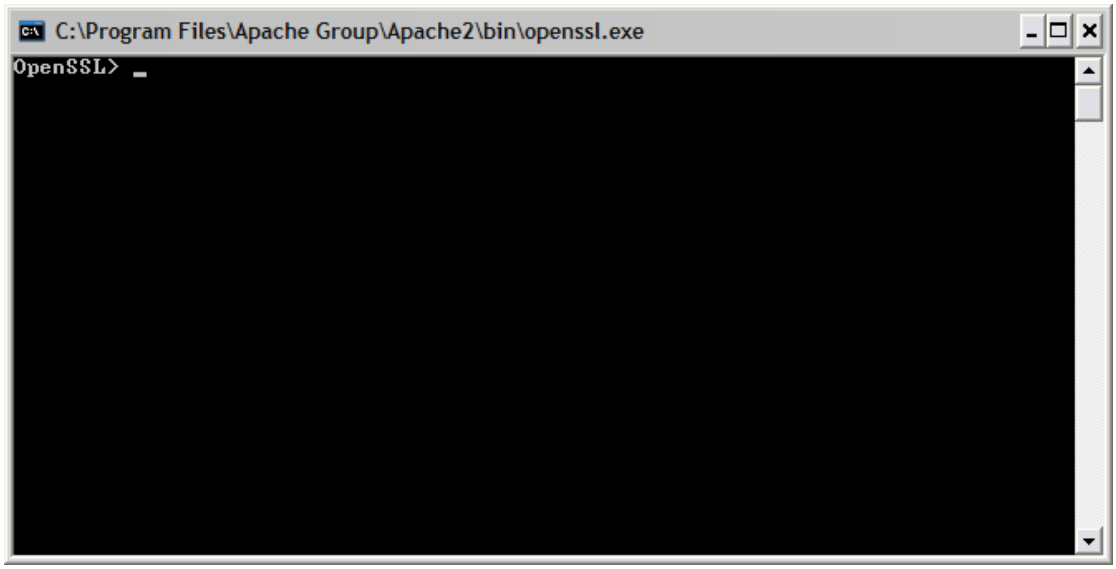
Παράδειγμα πιστοποιητικού :

```
Certificate:
  Data:
    Version: 1 (0x0)
    Serial Number: 7829 (0x1e95)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting
cc,
        OU=Certification Services Division,
        CN=Thawte Server CA/emailAddress=server-certs@thawte.com
    Validity
      Not Before: Jul 9 16:04:02 1998 GMT
      Not After : Jul 9 16:04:02 1999 GMT
    Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala,
        OU=FreeSoft,
CN=www.freesoft.org/emailAddress=baccala@freesoft.org
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
        Modulus (1024 bit):
          00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:
          33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:
          66:36:d0:8e:56:12:44:ba:75:eb:e8:1c:9c:5b:66:
          70:33:52:14:c9:ec:4f:91:51:70:39:de:53:85:17:
          16:94:6e:ee:f4:d5:6f:d5:ca:b3:47:5e:1b:0c:7b:
          c5:cc:2b:6b:c1:90:c3:16:31:0d:bf:7a:c7:47:77:
          8f:a0:21:c7:4c:d0:16:65:00:c1:0f:d7:b8:80:e3:
          d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8:
          e8:35:1c:9e:27:52:7e:41:8f
        Exponent: 65537 (0x10001)
  Signature Algorithm: md5WithRSAEncryption
    93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:
    92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
    ab:2f:4b:cf:0a:13:90:ee:2c:0e:43:03:be:f6:ea:8e:9c:67:
    d0:a2:40:03:f7:ef:6a:15:09:79:a9:46:ed:b7:16:1b:41:72:
    0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1:
    5a:de:9d:ea:63:cd:cb:cc:6d:5d:01:85:b5:6d:c8:f3:d9:f7:
    8f:0e:fc:ba:1f:34:e9:96:6e:6c:cf:f2:ef:9b:bf:de:b5:22:  68:9f
```

• Ένας Φορέας Πιστοποίησης **(CA)** είναι ένας έμπιστος οργανισμός που εκδίδει και διαχειρίζεται ψηφιακά πιστοποιητικά.

5.2.3 Διαχείριση Πιστοποιητικών

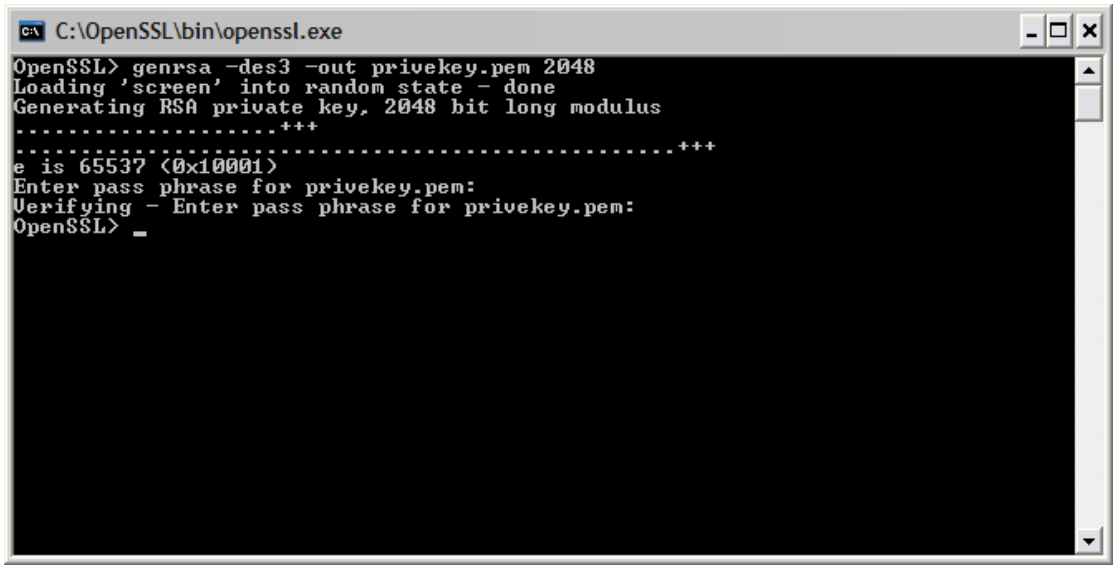
Δημιουργία πιστοποιήτικών με την βοήθεια του openssl:



Εικόνα 36. Το αρχικό command line μενού του openssl

Για την παραγωγή rsa key:

genrsa –des3* –out privekey.pem 2048 * aes256



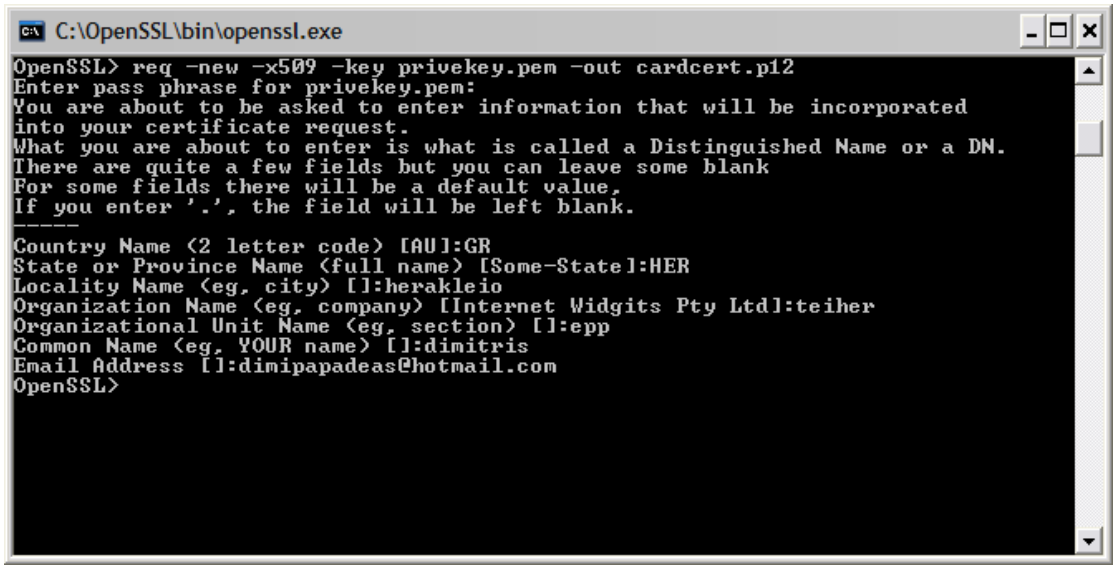
Εικόνα 37. Η εκτέλεση της εντολής παραγωγής κλειδιού

Το κλειδί που παρήχθη :

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,8A94BBBB7F73A0A9

ZV1p/8+R5fne+VSBEideRI/zK9YYvCPxDpBpVboq4ISX3KZtc7IqhQPIplPoC3Rz
ah4IFRQvjo9BUPlzauyIyXJKLJZg8CjbQCjhwJi3XTTOofoqyS0S0VF7e5hcF/tP
hxiYA61BB32PuZQmDR6yDjVKkq4k01lessrpzNC124lW0asLKggviJEvdTYuwdcW
oCsPIAtwqbAmTOPkd/AOr65gZ8A9L1upj8pfHgB3uZhHZLLfTObFNocN2q1Ac+GJ
Qjc50b0jsKOR4OA/Djkqhp+eSaGsGZLXEWbdbonaBn2Ucaq0wraooLc/CTiVjSgV
NsE0D1GMp0PHt8b3mdINEkI61QtAM2jcGaZlPsWalzEeSH9lbwKp6ooUVduJoJ8H
tWLCRc2A/VV8Vlu5ViakN4br+GijCX/hoNU1D/rMGl1CCTWXYn5UbQfdV27YUWtk
WtbtFJfDAtv+PUiq2FH34H7pOB459D2sbtPD0VO5ODolZnbjbwCPM+9KqFuorbOs
F6W63TAyZwbMrhDxhnz/iL3lMUvUruQxR158JSYjkixmL6KNcxSPTWNyVAdCz4Fr
uoW5aouZjWMBXPXdGoCP68DDNTw83PM2ns7QCzaMeDM/AX4oraWeIujk+QNqBQen
1qmRDWkKaV5Da9fpyw1JfRPog1QjtjHS6D0zt/vyrlgqqA22viXVdjULkZ1oAiqG
uxetXiMHYZXmTLNRvp1GN1K/iH69+9Xo3giLir7MvcRdEIbUqXuC+Wz+XBlX68x4
3qlr+OV0nRU/0B+SHMMrMWyIFB1ivT0Ju6tW7AYKNkVRHQVhxa4OMbv75k1M2gbG
qjJlb8OM1bvEGmxbX7qHzcYocBkmf9glfw+0BpVMNvQJb8Ij6U8UHbL/NPFhVQ2s
Urgzz9LpIbu9RYSsImTMzDHoxda27NooACvmeK2ERe3JAhLCZDSW3fmtGC9/n3O+
ViYcNqfyJJI5nJLcSnsJMY2pqySjQ7TId/W4xwmqnH1/nj6TjyMCsZiV9Y56DZEN
18BhUfhNxZ3TK530hRYkpZXj6OTeBcKYGHN4zI7APGO7tnCc2bDREPhnWxOnPtVQ
Ta9UlC6FxM0LKHUup9gEurfedPNEY0LiE+38TcDHAHkW67BWKW+3o2K3DssCyxFx
6F/DpHR1Upg2C8+cUZlNTjl4KRFXVmo6jJRVdXfIwmWirPiaM01l4CaB8EKennHl
n6q/NsrtWlHOvwdDA9VC5qnUizVa7vvyNKppGQfjAsiT4rOIU+mTDQJvCKvGtQvS
gUpSiloEFVXRgulB1J+oY6+NcanzHk9qTsLT7LEF3sM06cON4owMUmCaoUMfWDVd
ooUnOLZHEfJpMD2DrAKlv6oDyoA80snrqvLX6kWxJtGWZUY/rDByGHYachRb4WQa
1XFSJi96dOn5sLCLQnQYHO80h6eYCIskAiR5VKKs1T6hARYwUGcpc7zoNwIezGm/
iauBNkskXwk25wsJnhbAFcZfuf84hdUz+I79q1tBye8jq8cTTBngzCieeMUWf8I+
PDIsCYrYjtGn7MEuE7vIEaEFGp9tIIv6lxTiIH62yLX+d7a6p3pj0Q==
-----END RSA PRIVATE KEY-----
```

Για την παραγωγή του πιστοποιητικού με την χρήση του κλειδιού που δημιουργήσαμε:



Εικόνα 38. Η εκτέλεση της εντολής παραγωγής πιστοποιητικού με το κλειδί privekey.pem που δημιουργήσαμε νωρίτερα

Εικόνα 39. Το κλειδί και το πιστοποιητικό

Το πιστοποιητικό που παρήχθη :

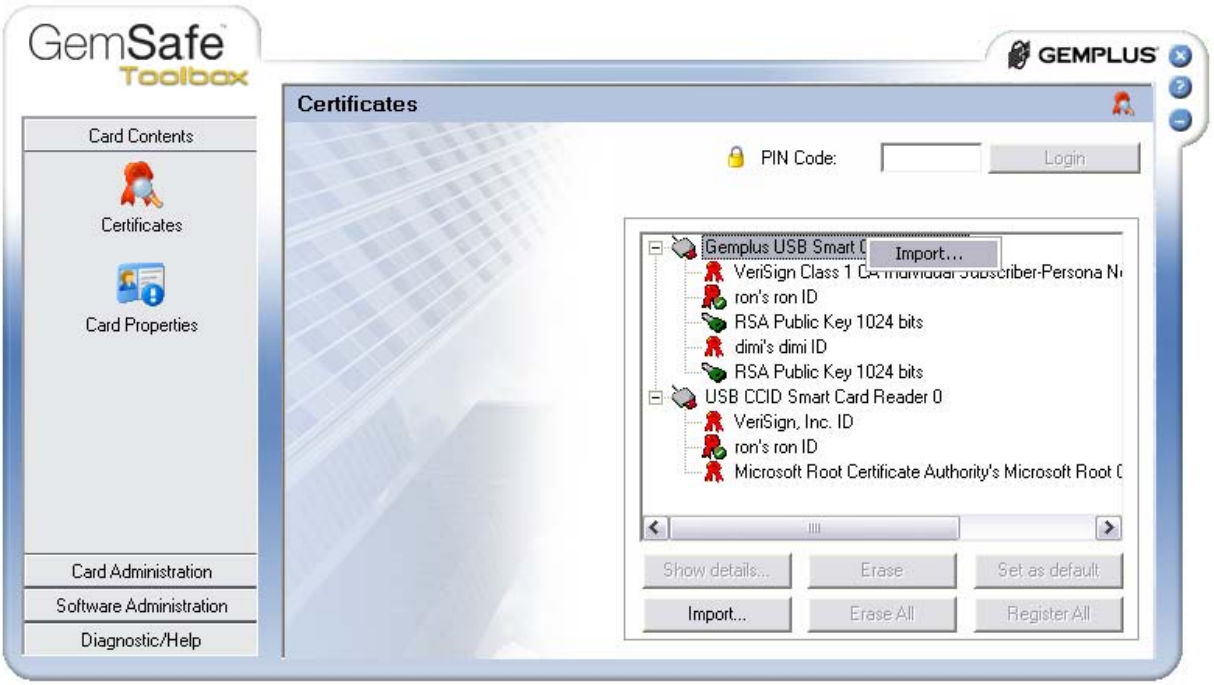
```
-----BEGIN CERTIFICATE-----
MIIEjDCCA3SgAwIBAgIJANfWlX/Xb/g5MA0GCSqGSIb3DQEBBQUAMIGKMQswCQYD
VQQGEwJHUjEMMAoGA1UECBMDSEVSMRIwEAYDVQQHEwloZXJha2xlaW8xDzANBgNV
BAoTBnRlaWhlcjEMMAoGA1UECxMDZXBwMREwDwYDVQQDEwhkaW1pdHJpczEnMCUG
CSqGSIb3DQEJARYYZGltaXBhcGFkZWFzQGhvdG1haWwuY29tMB4XDTA5MDExNzIz
MjcxMFoXDTA5MDIxNjIzMjcxMFowgYoxCzAJBgNVBAYTAkdSMQwwCgYDVQQIEwNI
RVIxEjAQBgNVBAcTCWhlcmFrbGVpbzEPMA0GA1UEChMGdGVpaGVyMQwwCgYDVQQL
EwNlcHAxETAPBgNVBAMTCGRpbWl0cmlzMScwJQYJKoZIhvcNAQkBFhhkaW1pcGFw
YWRlYXNAaG90bWFpbC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQDLpS5dayg9h4ZM4GaLKkxGuZc0ysd4XhYVkjYV+OVqwyJMbVleS+F622qvXyVA
BcJz0NVZBofX4AI4n1RViubRTX1J6jjMzgXnrjblhbGghm3UxAXJSEC8HPbhprQj
oTHr/yI7qXKrxIJnkzG5EafvaEW1h8XueDG2Ncx1x4ZmdPrtyTjp3jEb4kH7PxYM
P4pIqYcq1UMpTiPEaD04aYj7IVmmTEUaMw+ugMvTBnUIXd26CHZfE/S/HwiA1DZ/
TsEEY4aBrGc6Ga451/rWgQXXamEzN6OVA7VF9X/FsUJ2wVfDSg/yUX+g7cSx2uj5
ChWHOhDuOeT/Cgy22XoVat2TAgMBAAGjgfIwge8wHQYDVR0OBBYEFPZlSAsgYiWT
boGXFVEsPsUYtLO+MIG/BgNVHSMEgbcwgbSAFPZlSAsgYiWTboGXFVEsPsUYtLO+
oYGQpIGNMIGKMQswCQYDVQQGEwJHUjEMMAoGA1UECBMDSEVSMRIwEAYDVQQHEwlo
ZXJha2xlaW8xDzANBgNVBAoTBnRlaWhlcjEMMAoGA1UECxMDZXBwMREwDwYDVQQD
EwhkaW1pdHJpczEnMCUGCSqGSIb3DQEJARYYZGltaXBhcGFkZWFzQGhvdG1haWwu
Y29tggkA19aVf9dv+DkwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEA
MA4kTWSMWYUfTaczxtqiv8Segj4dYMNs8HR1gYD9rjgWLD3DsQkZiIQ/IPfjzmta
iMLaqkmD6C2PRJph6Js3DHO3zejKawe5SEnhZ69VLteUXqjgqYnhXF5oPivmZ4a3
YbB5Niur26NgD9smznhY2s2pHvX5yj3JfY4f3flid1IUBJ0BLELKIDJgRFsb4wBW
SQ4oIvOlLvl7cXIwhYpm34uHoeTck3hbwGaOm/WCQJhT6ulFvvLyNSi30tIdMjed
/Lz/8U/NOOvBFRx3i2z/O8bVVhFSggNc2gqkzOFRk4AuLvzBMeK9mxAWyhS5lUfS
UELsuI6Ezdts7Vtjmlhtyg==
-----END CERTIFICATE-----
```

5.2.3.1 Εισαγωγή / εξαγωγή πιστοποιητικών

Ανάλογα με τα δικαιώματα που έχουν παραχωρηθεί στον χρήστη, μπορεί να εισάγει και να εξάγει πιστοποιητικά στην κάρτα.

5.2.3.1a Εισαγωγή πιστοποιητικού (Import)

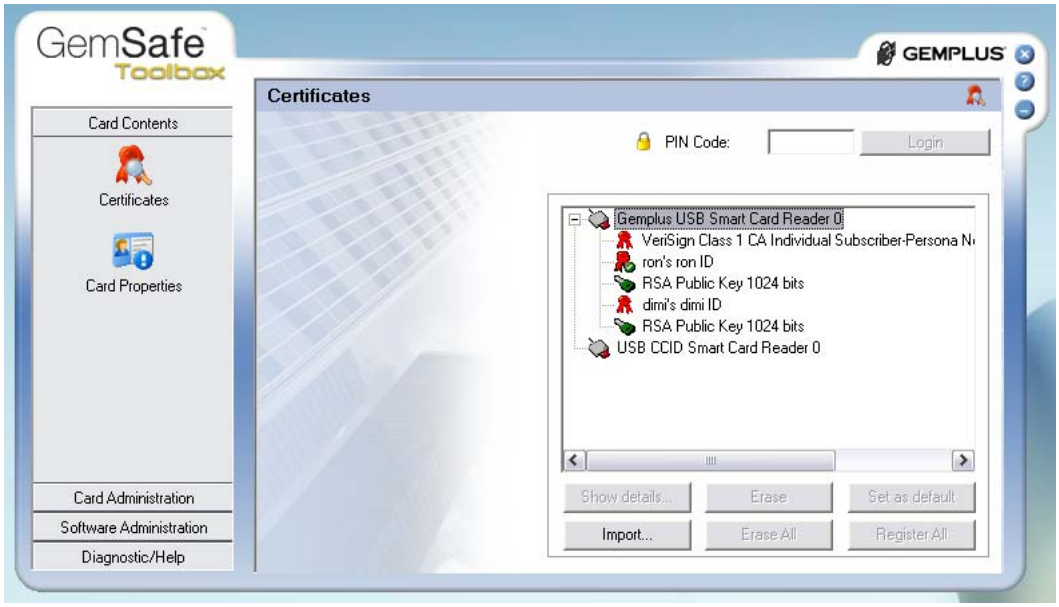
Επιλέγοντας τον smart card reader, ενεργοποιείται η επιλογή **Import** ή αλλιώς με δεξί κλικ πάνω στον reader, αναδύεται η επιλογή **Import.**



Εικόνα 40. Εισαγωγή πιστοποιητικών

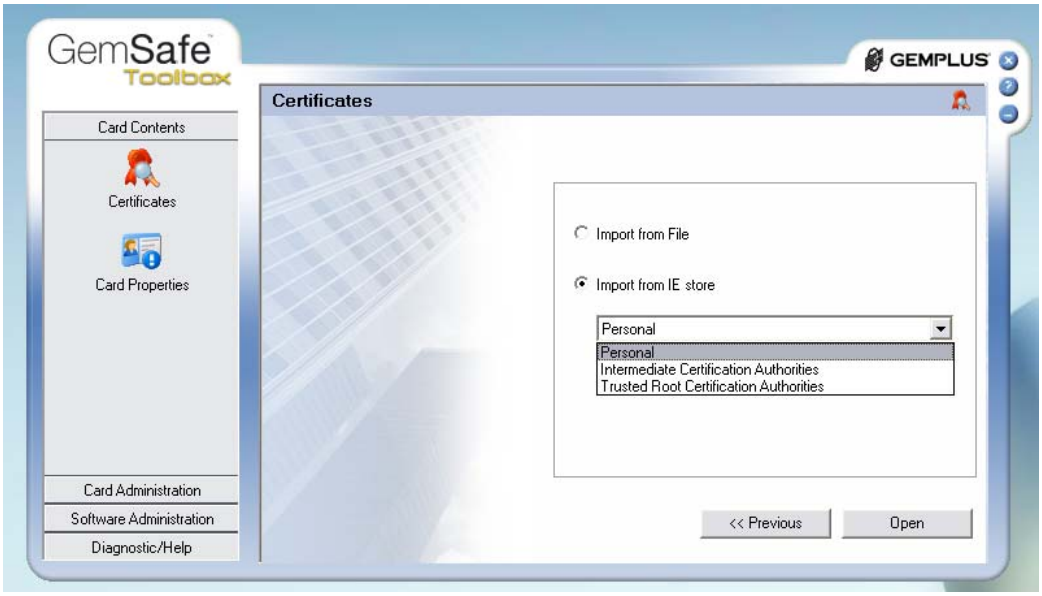
Ο χρήστης μπορεί να εισάγει πιστοποιητικό στην κάρτα χωρίς να χρειάζεται να έχει ταυτοποιηθεί, να έχει κάνει Log In. Εκτός από την περίπτωση που το πιστοποιητικό συνοδεύεται από ένα ζεύγος κλειδιών, οπού τότε πρέπει να έχει ταυτοποιηθεί με το σωστό PIN.

–Στις read-only cards δεν είναι δυνατή η εισαγωγή περεταίρω πιστοποιητικών.

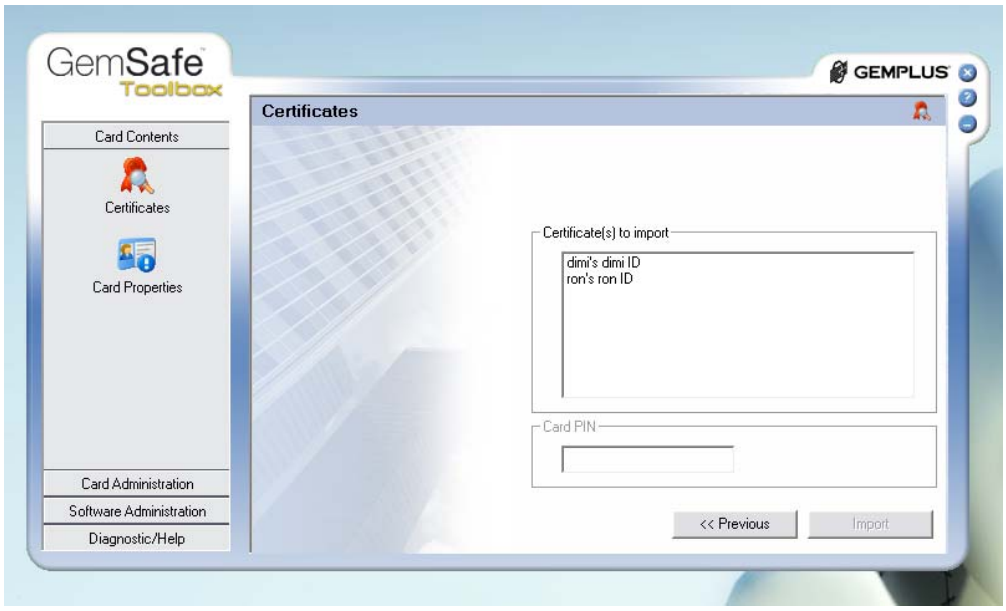


Εικόνα 41. Τα περιεχόμενα των καρτών στους CCID reader και Gemplus USB, όπως φαίνεται η κάρτα στον CCID είναι άδεια.

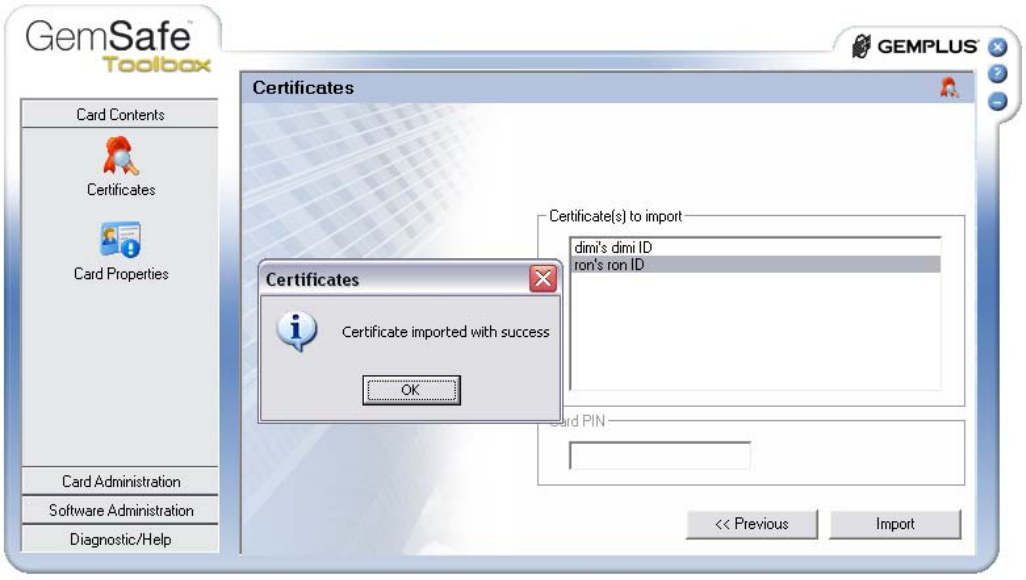
Μετά την επιλογή Import:



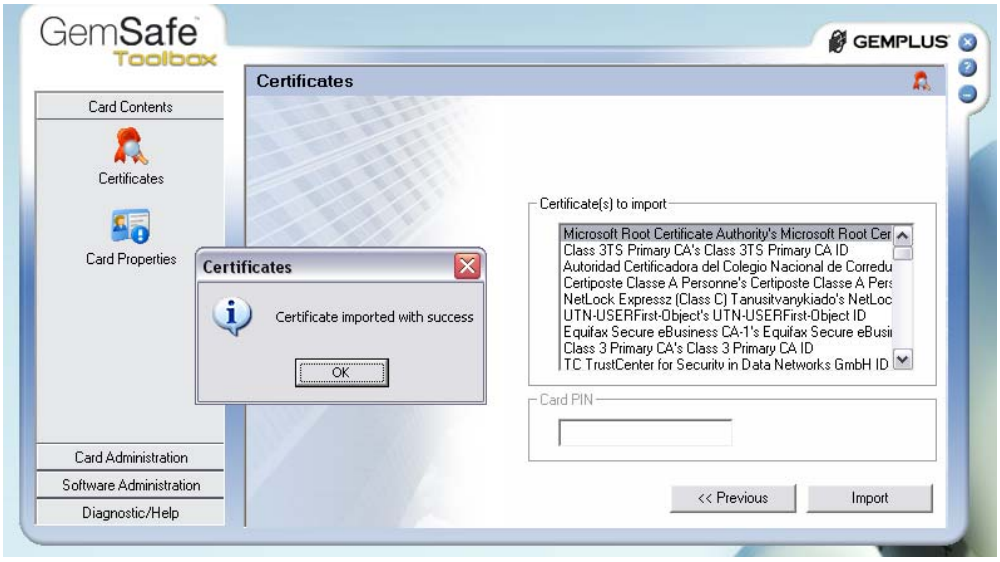
Εικόνα 42. Με την επιλογή Open, δίνεται η πρόσβαση στο αντίστοιχο πεδίο



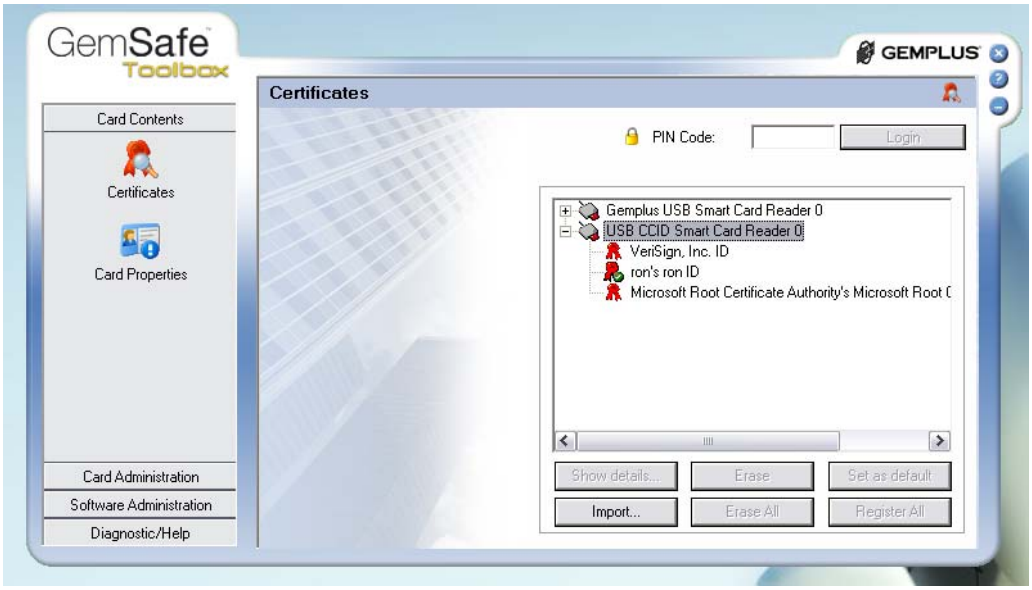
Εικόνα 43. Το personal πεδίο που είναι τα πιστοποιητικά που καταχώρησε ο χρήστης



Εικόνα 44. Η επιτυχής εισαγωγή του Personal ID

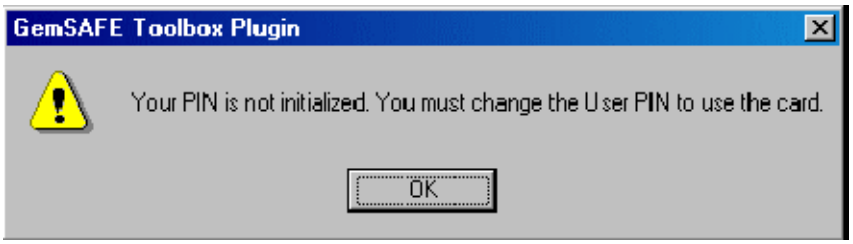


Εικόνα 45. Το Trusted root Certification Authorities πεδίο και η επιτυχής εισαγωγή του Microsoft root certificate



Εικόνα 46. Τα περιεχόμενα της κάρτας στον CCID reader μετά τις εισαγωγές

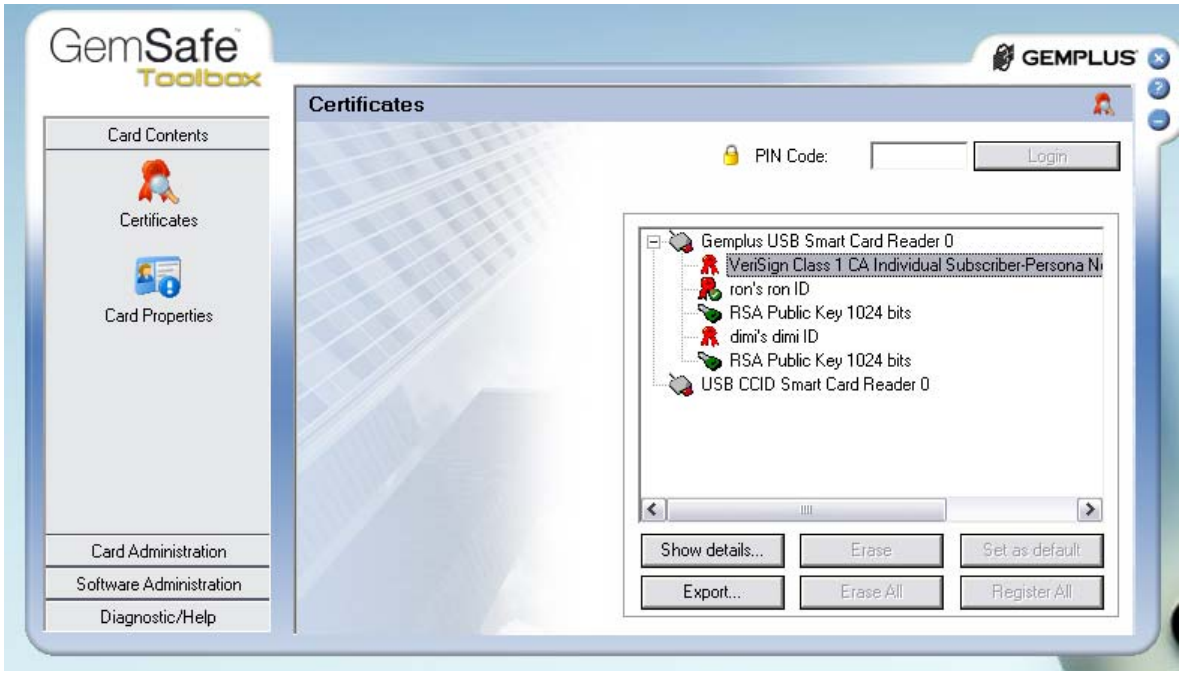
Δεν είναι επιτρεπτή η εισαγωγή πιστοποιητικών σε κάρτα που δεν έχει αρχικοποιημένο PIN, σε κάθε τέτοια προσπάθεια ο χρήστης λαμβάνει το σχετικό μήνυμα :



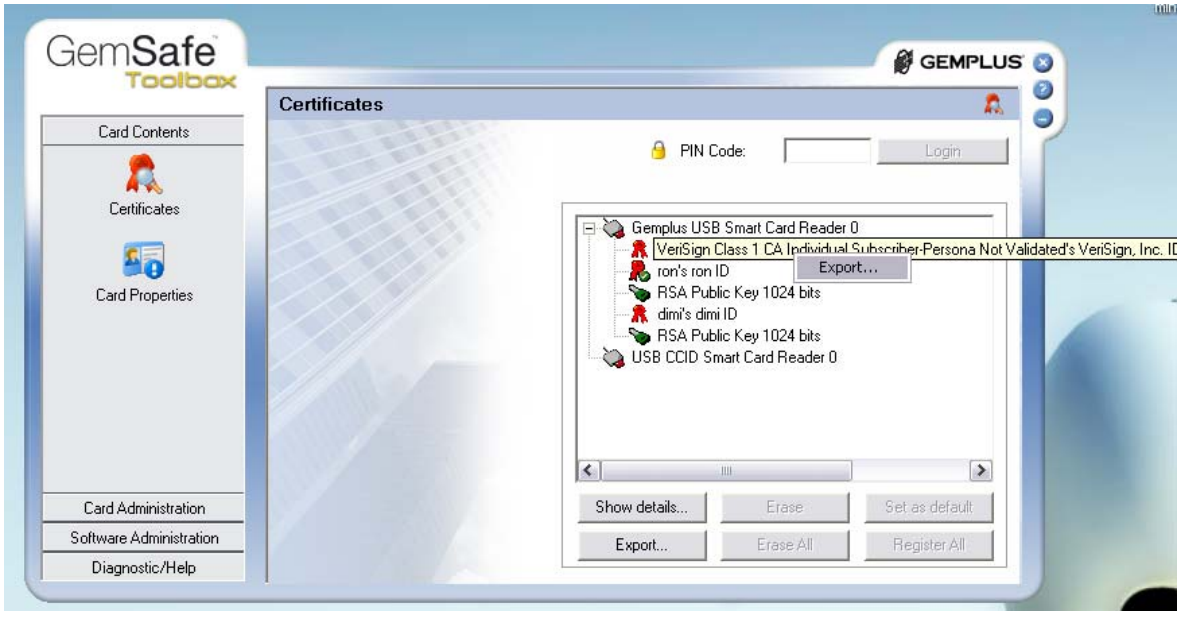
Εικόνα 47. Ειδοποίηση ότι η κάρτα δεν έχει αρχικοποιηθεί.

5.2.3.1b Εξαγωγή πιστοποιητικού (Export)

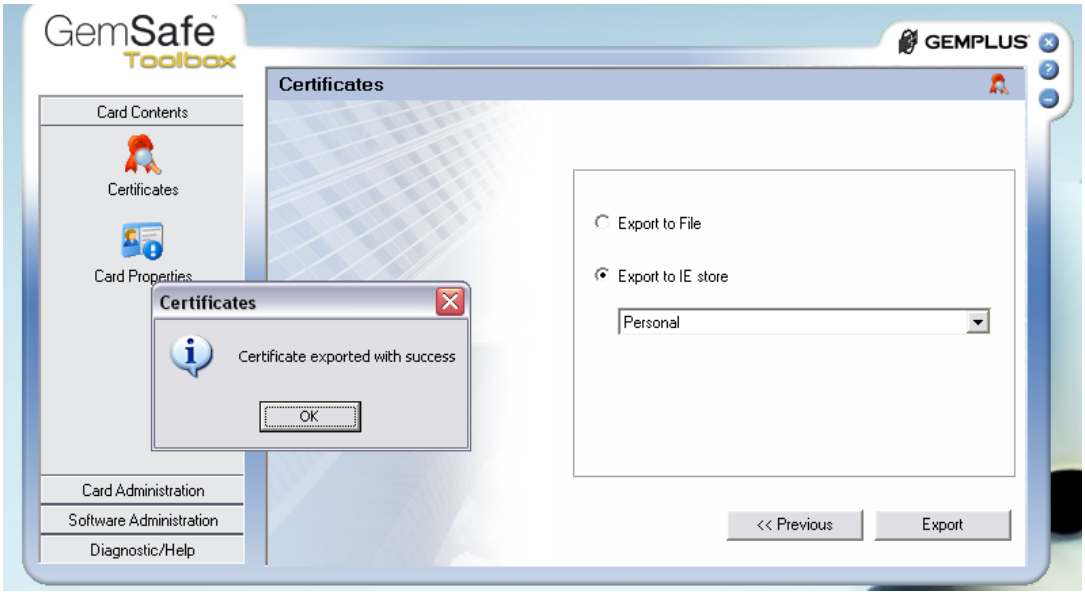
Για την εξαγωγή πιστοποιητικού, απλά επιλέγεται το πιστοποιητικό προς εξαγωγή και είτε με δεξί κλικ είτε από την επιλογή Export, προβάλλεται το μενού εξαγωγής και το πιστοποιητικό μπορεί να εξαχθεί στο IE store ή στον υπολογιστή με την μορφή αρχείου.



Εικόνα 48. Επιλέγεται το πιστοποιητικό προς εξαγωγή



Εικόνα 49. Με δεξί κλικ αναδύεται η επιλογή Export



Εικόνα 50. Η επιλογή Export στο πεδίο του IE store και η επιτυχής εξαγωγή στο Personal

Στην περίπτωση που επιλέγεται η εξαγωγή σε αρχείο(Export to File), αποθηκεύεται στο λειτουργικό με την μορφή .der αρχείου.

Εικόνα 51. Ένα πιστοποιητικό τύπου der

5.2.3.3 Ορίζοντας το Default πιστοποιητικό

Το Registration Tool αυτόματα καταχωρεί τα πιστοποιητικά της κάρτας στο IE cert store, χωρίς όμως να αντιγράφει τις πληροφορίες του πιστοποιητικού, απλά δημιουργεί ένα link μεταξύ του IE cert store και τις πληροφορίες πάνω στην κάρτα, για λόγους ασφαλείας. Ο ορισμός του Default πιστοποιητικού επιτρέπει στο χρήστη να καθορίσει πιστοποιητικό που θα επιλεγεί ως το προεπιλεγμένο πιστοποιητικό. Επιλέγοντας από τον κατάλογο των καταχωρημένων πιστοποιητικών.

Σημείωση: Το Default πιστοποιητικό είναι υποχρεωτικό για την χρήση του από τρίτες εφαρμογές[17], κυρίως από εφαρμογές της Microsoft.

[17]Κεφάλαιο 6. Χρήση των περιεχόμενων των Smart card από ξένες εφαρμογές

5.2.3.4 Καταχώρηση Πιστοποιητικών

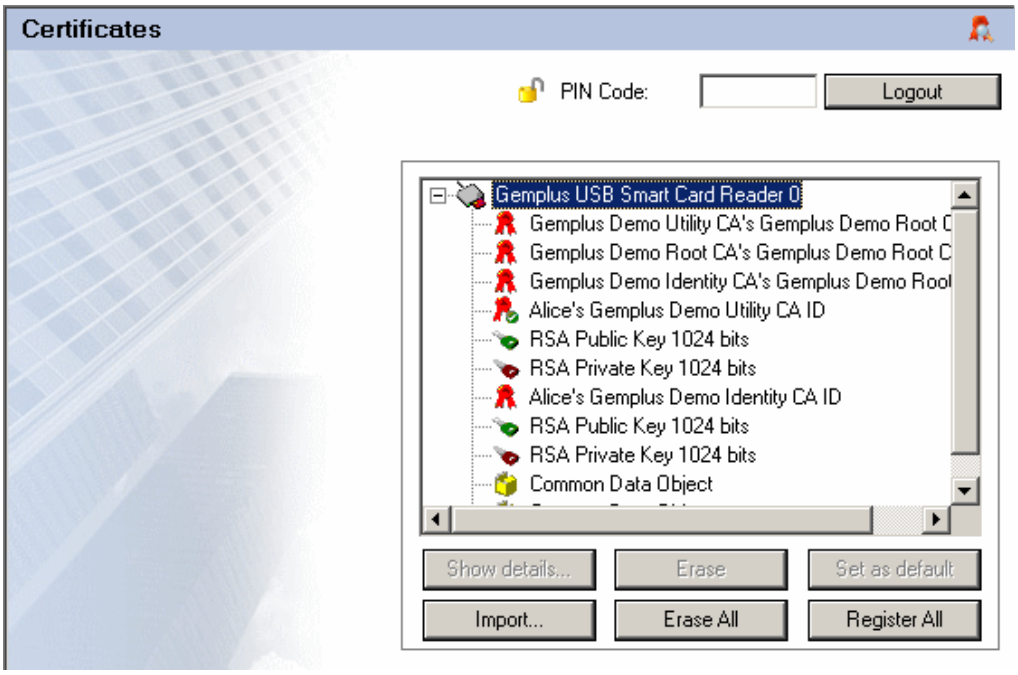
Τα πιστοποιητικά για να μπορούν να χρησιμοποιηθούν σε οποιαδήποτε περίπτωση, πρέπει να είναι καταχωρημένα (registered). Εάν για οποιονδήποτε λόγο δεν καταχωρηθούν αυτόματα τα πιστοποιητικά, ο χρήστης μπορεί να τα καταχωρήσει κατά βούληση με την βοήθεια του Toolbox Certificates Tool.

Για την χειροκίνητη καταχώρηση των πιστοποιητικών :

1. Μέσω του **Certificate Tool** και μετά την εισαγωγή του PIN.

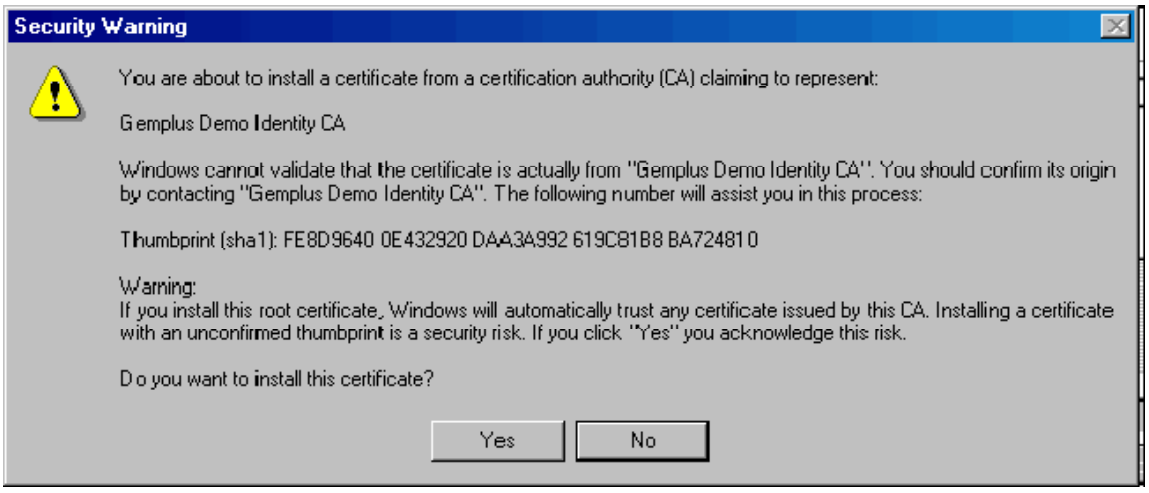
2. Click στο Card/Register Certificates.

Για να καταχωρηθούν όλα τα πιστοποιητικά επιλέγουμε τον αναγνώστη:  . Επιλέγοντας έτσι όλα τα PKCS#11 αντικείμενα που είναι αποθηκευμένα στην κάρτα, τότε έχουμε την δυνατότητα: register all certificates

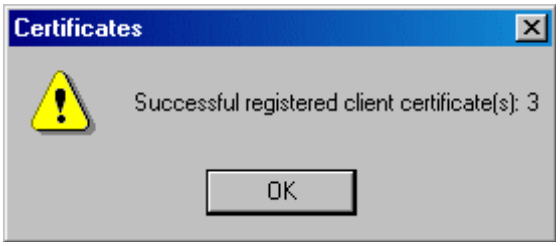


Εικόνα 52. Η επιλογή Register All είναι ενεργή μόνο όταν δεν έχουν καταχωρηθεί τα πιστοποιητικά

3. Με Click στο **Register All** τα Windows επιβεβαιώνουν την καταχώρηση με ένα σχετικό μήνυμα, συνοψίζοντας τα δεδομένα του πιστοποιητικού και ζητώντας τις απαιτούμενες επιβεβαιώσεις για τον φορέα πιστοποίησης (CA):



Εικόνα 53. Τέλος μετά την επιλογή του Yes, μήνυμα επιβεβαίωσης εμφανίζεται πληροφορώντας τον χρήστη τον αριθμό των πιστοποιητικών που καταχωρήθηκαν



Εικόνα 54. Τα πιστοποιητικά έχουν καταχωρηθεί

5.2.3.5 Διαγραφή πιστοποιητικών

Ο χρήστης μπορεί να διαγράψει όλα τα αντικείμενα που περιέχει η κάρτα, γενικότερα οποιοδήποτε αντικείμενο θεωρείται περιττό μπορεί να διαγραφεί με απώτερο όφελος την εξοικονόμηση χώρου για νέα αντικείμενα. Ανάλογα με την χωρητικότητα μίας κάρτας ένα κλειδί ή ένα πιστοποιητικό μπορεί να καταλαμβάνει είτε αμελητέο χώρο είτε σημαντικό τμήμα του αποθηκευτικού χώρου μίας κάρτας, ποσοστά της τάξης από 0-1 % σε κάρτες με μεγάλο αποθηκευτικό χώρο(128k), όμως οι περισσότερες κάρτες έχουν αποθηκευτικό χώρο της τάξης των 4 ή 8 ή 16 kilobytes. Με αποτέλεσμα ένα κλειδί (μεγέθους περίπου 1k) ή ένα πιστοποιητικό (μεγέθους 1-2 k) να καταλαμβάνουν μεγάλα τμήματα του αποθηκευτικού χώρου.

5.2.3.6 Διαγραφή όλων (Erase All)

Η επιλογή **Erase All** επιτρέπει στον χρηστή να διαγράψει όλα τα PKCS#11 αντικείμενα στην κάρτα (πιστοποιητικά, κλειδιά και δεδομένα).

Για την διαγραφή όλων των δεδομένων:

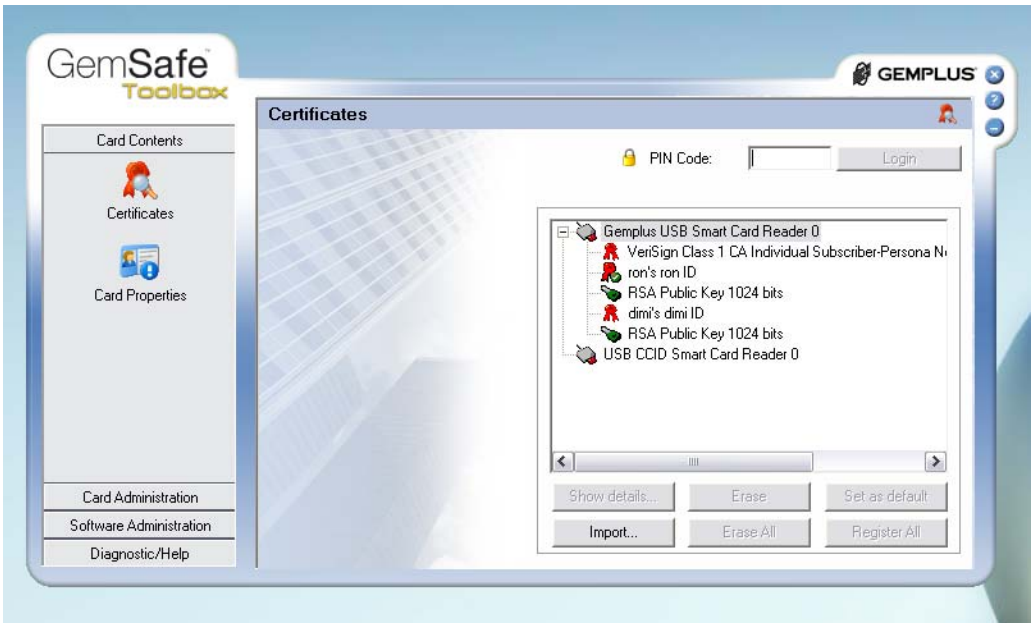
1. Εισαγωγή του Pin για Login

2.Επιλέγουμε τον card reader  , με αυτήν την κίνηση επιλέγονται όλα τα PKCS#11 αντικείμενα στην κάρτα

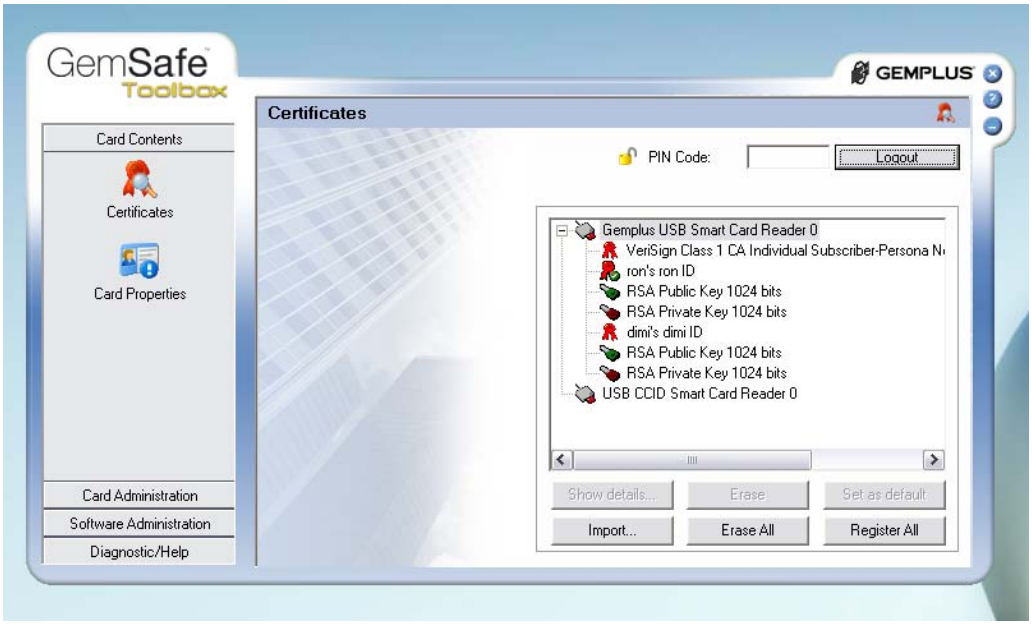
3. Επιλέγουμε **Erase All**, και όλα τα αντικείμενα PKCS#11 διαγράφονται από την κάρτα.

5.2.4 Περιεχόμενα κάρτας

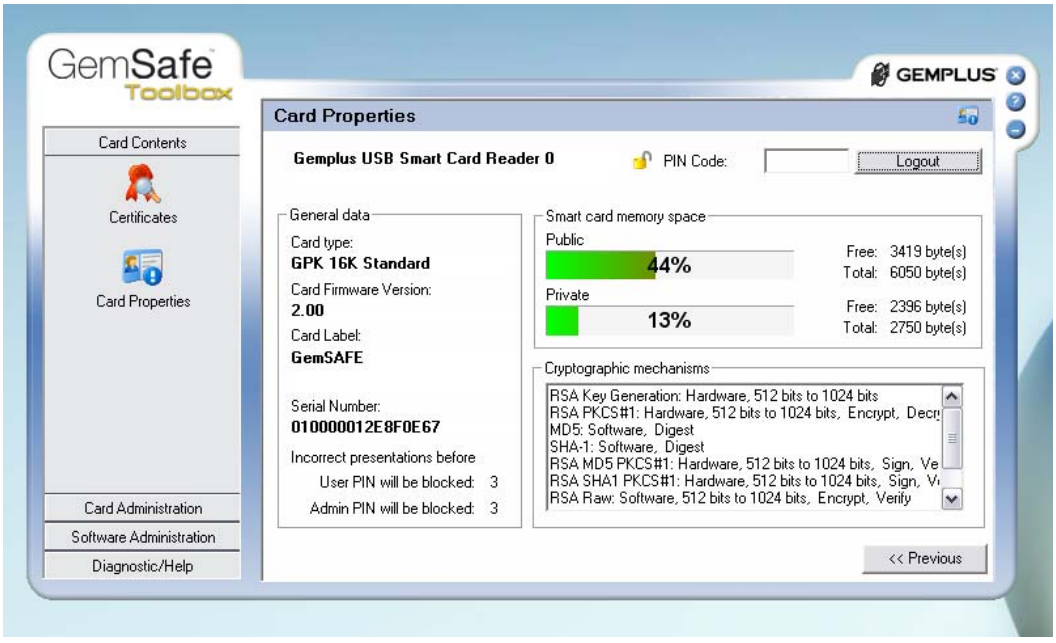
Στα περιεχόμενα της κάρτας υπάρχουν δύο πεδία, το public και το private. Στο public είναι όλα τα public keys, τα Ids τα οποία είναι τα περιεχόμενα στοιχεία των certificates, και τέλος στο public πεδίο είναι και το VeriSign της Certificate Authority(CA). Ενώ στο πεδίο private, όπου η πρόσβαση επιτρέπεται μετά την εισαγωγή του σωστού password(Μετά το login), υπάρχουν όπως είναι λογικό, τα private keys του χρήστη.



Εικόνα 55. Τα Public data της κάρτας που βρίσκεται στον Gemplus USB smart card Reader



Εικόνα 56. Μετά το login και τα Private data της κάρτας είναι διαθέσιμα



Εικόνα 57. Τα περιεχόμενα και η κατάσταση της κάρτας

	Πιστοποιητικό
	Default Πιστοποιητικό
	Εισαγμένο Δημόσιο Κλειδί
	On-board Δημόσιο Κλειδί [18]
	Εισαγμένο Ιδιωτικό Κλειδί
	On-board Ιδιωτικό Κλειδί
	Κοινό αντικείμενο δεδομένων

Πίνακας 13. Εικονίδια κλειδιών και πιστοποιητικών

5.2.5 Οι Αλγόριθμοι ασφαλείας της Gamsafe

Όνομα Αλγόριθμου	Εφαρμογή	Ιδιότητες
RSA Key Generation	Hardware	512 bits to 1024 bits
RSA PKCS#1	Hardware	512 bits to 1024 bits, Encrypt, Decrypt, Sign, Verify, Unwrap
MD5	Software	Digest
SHA-1	Software	Digest
RSA MD5 PKCS#1	Hardware	512 bits to 1024 bits, Sign, Verify
RSA SHA1 PKCS#1	Hardware	512 bits to 1024 bits, Sign, Verify
RSA Raw	Software	512 bits to 1024 bits, Encrypt, Verify
RSA 9796	Hardware	512 bits to 1024 bits, Sign, Verify

Πίνακας 14.Οι αλγόριθμοι hash και κρυπτογράφησης των Gemsafe καρτών [19]

[18] κλειδί παραγμένο από την κάρτα, πάνω στην κάρτα.

[19] Βλ Παράρτημα για τους όρους : RSA, MD5, SHA-1, PKCS#1, RSA 9796

5.2.6 Διαχείριση Pin

5.2.6.1 Pin

Ένα Pin (Personal Identification Number) είναι ένας προσωπικός κωδικός, που μπορεί να είναι μια ακολουθία αριθμών ή αλφαριθμητικών χαρακτήρων ή συνδυασμός αυτών, το Pin λειτουργεί σαν σύνθημα, password. Όταν το Pin μεταδίδεται σε ένα χρήστη καρτών πρέπει και να επαληθευθεί για να μπορεί να χρησιμοποιηθεί σε λειτουργίες ασφαλείας με την κάρτα, όπως η είσοδος στον σταθμό εργασίας ή η δημιουργία μίας ψηφιακής υπογραφής.

Default Gemsafe user pin: 1234

Default Gemsafe admin pin: 1234

5.2.6.2 Το Pin του χρήστη (user pin)

Το Pin του χρήστη μίας smart card μπορεί να είναι το αρχικό Pin που όρισε ο κατασκευαστής ή κάποιο άλλο που όρισε ο διαχειριστής . Το Pin του χρήστη πρέπει να είναι μοναδικό σε κάθε κάρτα και πρέπει να το γνωρίζει μόνο ο χρήστης. Εάν δίνεται η δυνατότητα από τον διαχειριστή, ο χρήστης οφείλει να αλλάξει το Pin μόλις το λάβει σε ένα που θα γνωρίζει μόνο αυτός. Επίσης ο διαχειριστής έχει την δυνατότητα να επιβάλει την αλλαγή του Pin κατά την πρώτη χρήση. Για την εκτέλεση μιας security operation ο χρήστης της κάρτας οφείλει να αποδείξει ότι γνωρίζει το Pin. Το λογισμικό που εφαρμόζει security operations συνήθως ζητάει από τον χρήστη να εισάγει το Pin.

• Στην περίπτωση της ψηφιακής υπογραφής, η επιτυχής εισαγωγή και επιβεβαίωση του Pin, αποδεικνύει ότι ο χρήστης είναι ο σωστός κάτοχος της κάρτας και του επιτρέπεται να υπογράψει με το επιλεγμένο κλειδί.

• Στην περίπτωση του network log on, ο χρήστης αποδεικνύει και ότι η κάρτα του είναι έγκυρη στο σύστημα αλλά και ότι αυτός σαν χρήστης του δικτύου, βρίσκεται όντος εκεί. Από την στιγμή που είναι ο μόνος που γνωρίζει το Pin, κανένας άλλος δεν θα μπορούσε να εισάγει το σωστό Pin.

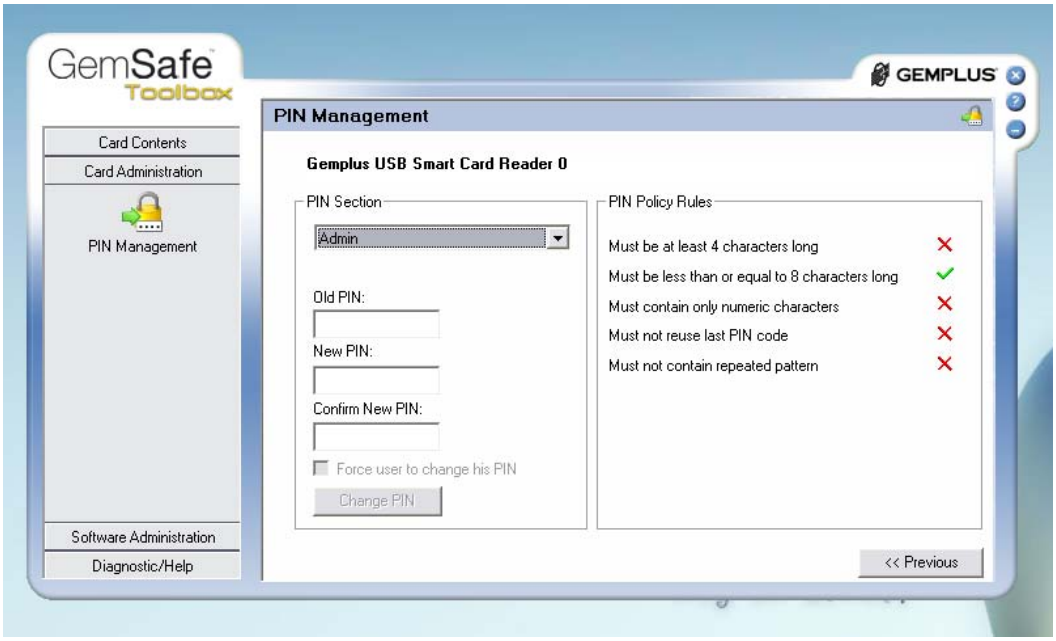
Σημείωση:
Εάν ο χρήστης ξεχάσει το Pin του, μετά από έναν προκαθορισμένο αριθμό αποτυχημένων προσπαθειών εισαγωγής του σωστού Pin, η κάρτα μπλοκάρει και ο χρήστης δεν μπορεί να την χρησιμοποιήσει για security operations. Τότε μόνο μία επιτυχής απεμπλοκή της κάρτας με την χρήση του administrator Pin, μπορεί να επαναφέρει την κάρτα στην αρχική της κατάσταση.

5.2.6.3 Το Pin του διαχειριστή (admin pin)

Το Pin του διαχειριστή είναι ένα άκρως σημαντικό τμήμα της ασφάλειας της κάρτας. Η γνώση αυτού του Pin, συνεπάγεται δυνατότητες αλλαγής του Pin του χρήστη, απεμπλοκή της κάρτας και κατά συνέπια απεριόριστη πρόσβαση στην κάρτα. Είναι πρωτίστης σημασίας οι διαχειριστές της κάρτας να διαφυλάξουν σε ασφαλές μέρος το Pin του διαχειριστή της ή των καρτών. Επίσης το Pin του διαχειριστή δεν πρέπει να γνωστοποιείται σε κανέναν ακόμα και στον ίδιο τον χρήστη της κάρτας, εκτός από περιπτώσεις που η πολιτική ασφάλειας το επιβάλει. Μετά από έναν προκαθορισμένο αριθμό αποτυχημένων προσπαθειών εισαγωγής του σωστού Pin του διαχειριστή, κάρτα μπλοκάρει και δεν μπορεί να χρησιμοποιηθεί ποτέ ξανά. Εκτός από την περίπτωση που προβλέπεται η υπό συνθήκες απεμπλοκή του Pin του διαχειριστή, από την πολιτική ασφαλείας.

5.2.6.4 Αλλαγή pin

Μέσω του Pin management control και της επιλογής change pin->next. Συμπληρώνοντας την φόρμα old pin- new pin- confirm pin, ανάλογα με την πολιτική Pin, γίνεται δεκτή ή όχι ή αλλαγή και επιλέγεται το change pin.



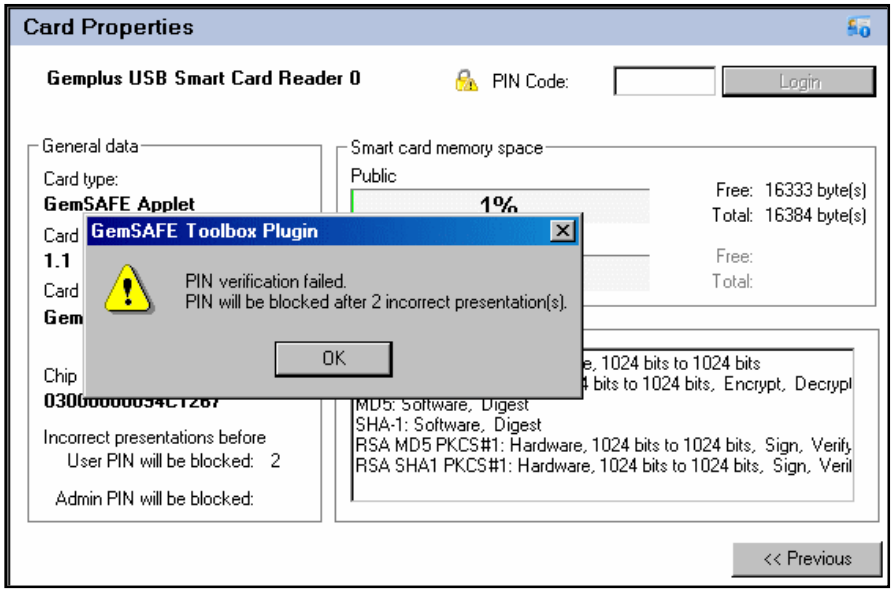
Εικόνα 58. Το menu αλλαγής του pin του χρήστη ή του διαχειριστή , ανάλογα με τα Pin Policy Rules (δεξιά) που έχουν οριστεί στην αντίστοιχή πολιτική

Εικόνα 59. Μήνυμα επιβεβαίωσης

5.2.6.5 Έλεγχος του μετρητή επικύρωσης του PIN (Ratification Counter)

Οι Smart cards προστατεύονται από επιθέσεις τύπου brute force με την χρήση του μηχανισμού μετρητή επικύρωσης. Μετά από έναν προκαθορισμένο αριθμό αποτυχημένων προσπαθειών εισαγωγής του σωστού Pin, η κάρτα μπλοκάρει. Ο μετρητής μειώνεται με κάθε λανθασμένη προσπάθεια μέχρι να γίνει μηδέν όπου και κλειδώνει η κάρτα, με κάθε επιτυχή προσπάθεια ο μετρητής ξαναπαίρνει την αρχική του τιμή. Ο Ratification Counter υποστηρίζεται από τελευταίας τεχνολογίας Smart Cards.

Για τον έλεγχο της τιμής του PIN ratification counter στην επιλογή Card Properties του Card Contents folder, επιλέγεται ο reader και **Next**.



Εικόνα 60. Μήνυμα ειδοποίησης εσφαλμένης εισαγωγής Pin

5.2.6.6 Απεμπλοκή pin / Unblock PIN (admin)

Η επιλογή απεμπλοκής της κάρτας (Unblock Card) επιτρέπει στον διαχειριστή ή τον χρήστη, την αναγνώριση και επιλογή της μπλοκαρισμένης κάρτας. Με την επιτυχή εισαγωγή του Admin Pin η κάρτα ξεμπλοκάρει και ορίζεται νέο PIN. Ο χρήστης για να μπορεί να ξεμπλοκάρει την κάρτα θα πρέπει:

1) Να του έχει παραχωρηθεί το αντίστοιχο permission από τον διαχειριστή.

2) Να γνωρίζει το Admin Pin της κάρτας του.

Συνήθως, η διαδικασία απεμπλοκής της κάρτας είναι στα καθήκοντα του διαχειριστή, λόγο της προσοχής που απαιτείται διότι εάν μπλοκάρει το Admin Pin η κάρτα δεν μπορεί να ξαναχρησιμοποιηθεί.
Σημείωση: Μερικές κάρτες επιτρέπουν την απεμπλοκή του Admin Pin, υπό προκαθορισμένες συνθήκες και διαδικασίες ανάλογα με την κάρτα και τον κατασκευαστή.

5.2.6.7 Εφαρμογή απομακρυσμένης απεμπλοκής

Η απομακρυσμένη απεμπλοκή της κάρτας νοείται ως την απεμπλοκή μίας μπλοκαρισμένης κάρτας από απόσταση, χωρίς να απαιτείται η επίσκεψη στον διαχειριστή. Η δυνατότητα αυτή απαιτεί την παραχώρηση του αντίστοιχου permission από τον διαχειριστή. Η εφαρμογή απομακρυσμένης απεμπλοκής απαιτεί υλοποίηση σε συνεργασία με την Gemplus, ανάλογα με το λογισμικό, τα πρότυπα και τις ανάγκες της εταιρίας.

Πιθανή εκδοχή:

1) Μια εφαρμογή αντιστοίχησης card serial number με random number σε μια βάση δεδομένων.

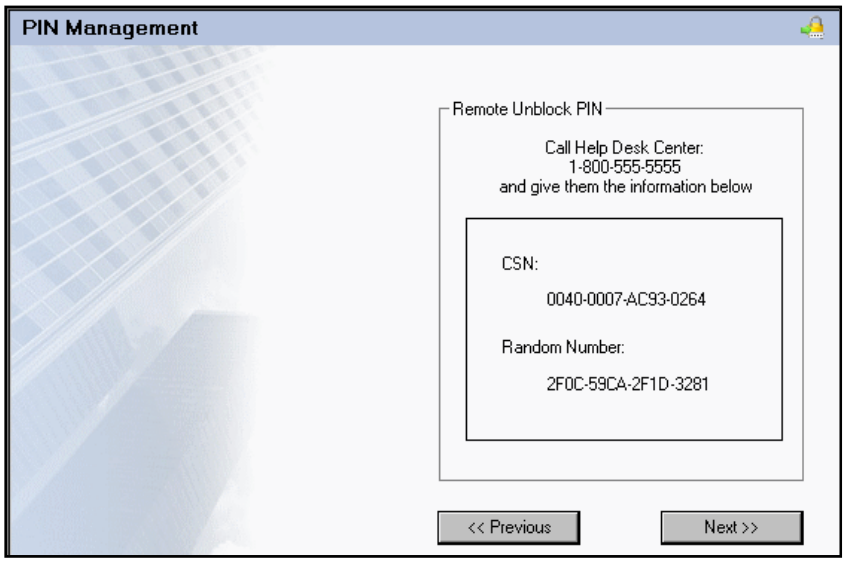
2) Η εφαρμογή παράγει μια κρυπτογραφημένη τιμή του αντίστοιχου Admin Pin κάθε κάρτας,

3) Ο χρήστης εισάγει μια κρυπτογραφημένη τιμή του Pin και επιβεβαιώνει την αλλαγή του Pin

4) Ο σειριακός αριθμός της κάρτας αποκρυπτογραφεί και επιβεβαιώνει την τιμή. Εάν το decrypted Admin Pin ισούται με το Admin Pin της κάρτας, ξεμπλοκάρει το Pin.

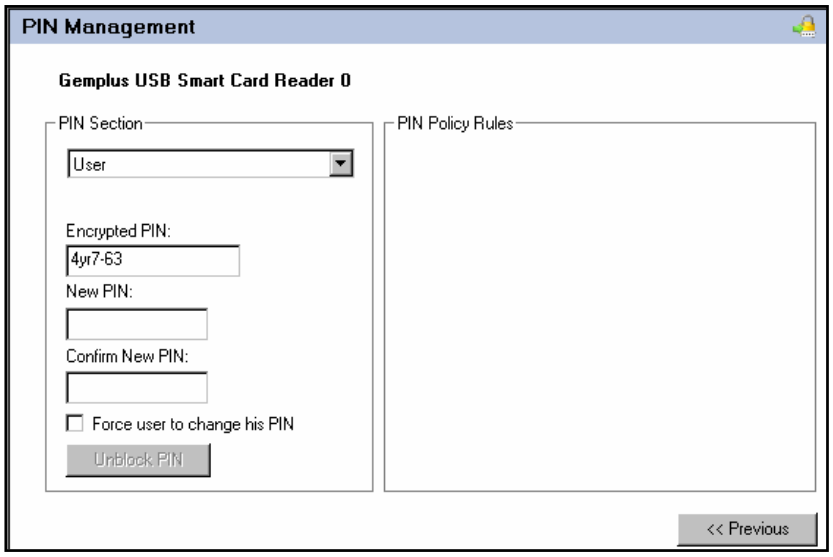
5.2.6.8 Απομακρυσμένη απεμπλοκή pin

1. Ο χρήστης εισάγει την blocked smart card στον smart card reader, επιλέγει το Pin Management tool  στον φάκελο Card Administration και την επιλογή Unblock Pin και Next.



Εικόνα 61. Απομακρυσμένη απεμπλοκή Pin

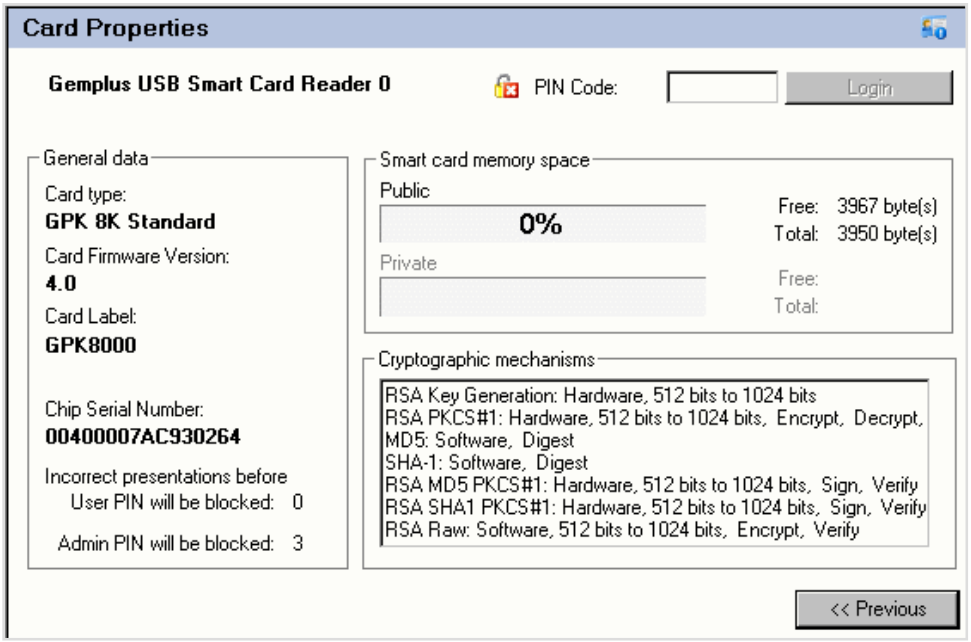
2.Ο χρήστης επικοινωνεί με το help desk, δίνοντας τον σειριακό αριθμό της κάρτας (card serial number (CSN)) και το random number. Το help desk με το CSN και το random number παράγει ένα encrypted Admin PIN.



Εικόνα 62. Αλλαγή κρυπτογραφημένου Pin

Με την επιλογή Next, αυτόματα το encrypted Admin Pin βρίσκεται στο σχετικό πεδίο.
Σημείωση**:** Με την επιλογή : Force user to change his Pin, ο χρήστης είναι υποχρεωμένος να αλλάξει το Pin ή όχι.

Ανάλογα με την πολιτική Pin, είτε ο user είτε ο administrator, μετά το login, μέσω του Pin management control και της επιλογής change pin -> next, συμπληρώνοντας την φόρμα Admin Pin- new Pin- confirm Pin, γίνεται δεκτή ή όχι ή αλλαγή και επιλέγεται το change pin.



Εικόνα 63. Μπλοκαρισμένη κάρτα

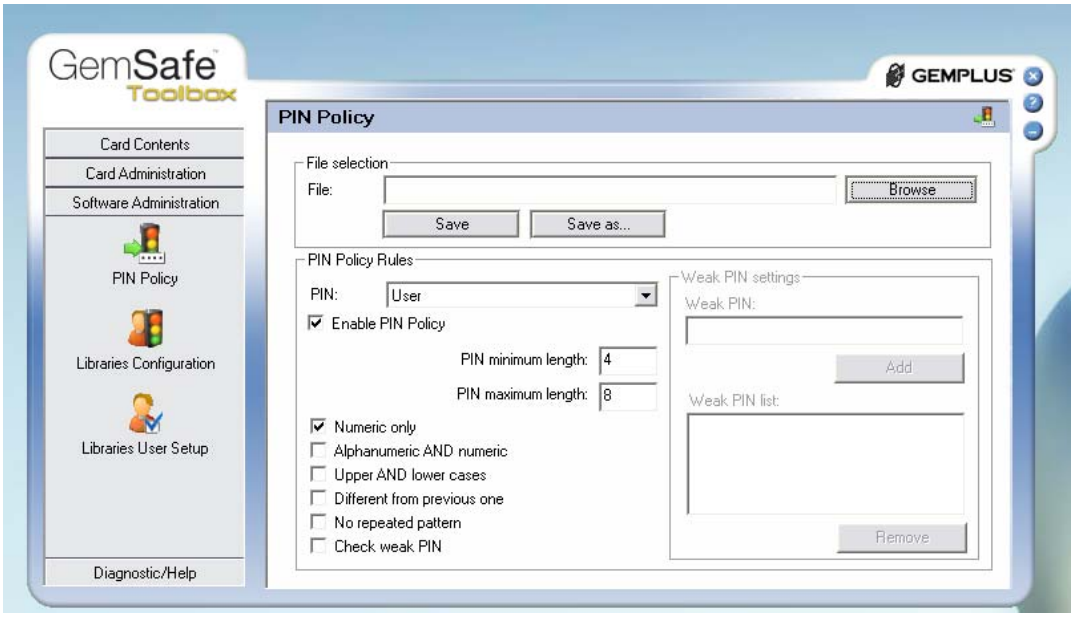
5.2.7 Διαμόρφωση βιβλιοθήκης

Οι βιβλιοθήκες αποτελούν ορισμό της συμπεριφοράς του χρήστη, είναι το σύνολο των δικαιωμάτων και δυνατοτήτων που έχει ένας χρήστης ή ένας διαχειριστής. Οι βιβλιοθήκες αποτελούν μια παράμετρο που ορίζεται διαφορετικά σε κάθε εφαρμογή και εταιρία ανάλογα με τις ανάγκες της εταιρίας και τα δικαιώματα πρόσβασης του κάθε χρήστη. Οι βιβλιοθήκες έχουν δύο κύριες δομές:

- πολιτική μυστικού κωδικού
- πολιτική βιβλιοθήκης του χρήστη

5.2.7.1 Ρύθμιση βιβλιοθήκης πολιτικής μυστικού κωδικού (pin policy)

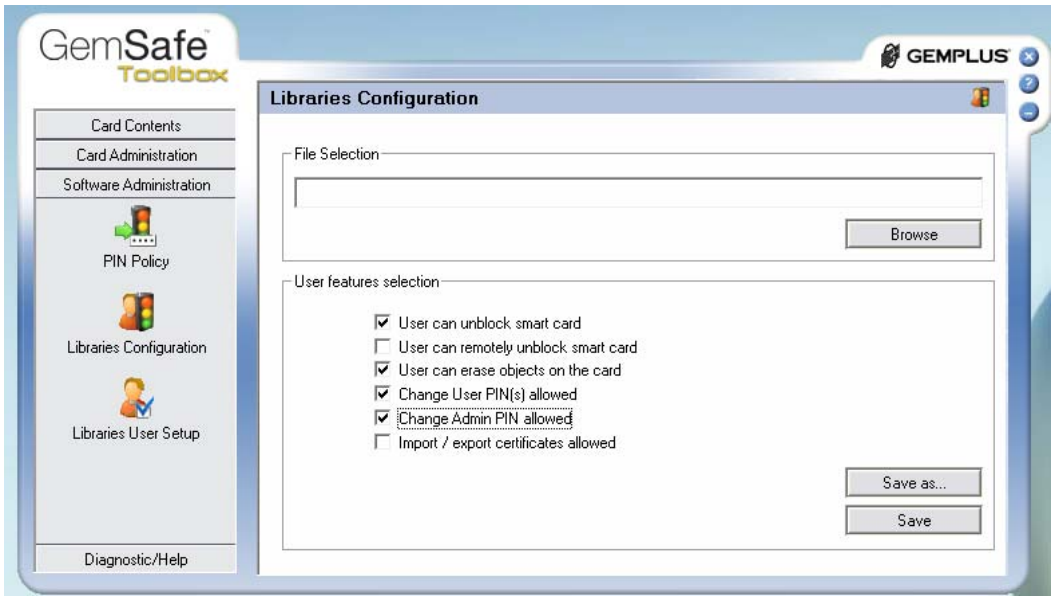
Με αυτήν την δυνατότητα, ο χρήστης ή ο διαχειριστής ορίζει τις διαφορές δομές και μορφές κατασκευής pin. Επιλέγεται ανάλογα, το pin να είναι: numeric only, Αλφαριθμητικό, Upper and Lower case, διαφορετικό από το προηγούμενο, αποτροπή χρήσης pattern και γίνεται έλεγχος weak pin ανάλογα με κάποια κριτήρια αδύναμων pin. Επίσης προκαθορίζεται το μέγεθος του Pin μεταξύ min και max length. Τέλος ο χρήστης αποθηκεύει τις ρυθμίσεις αυτές σε ένα αρχείο .ppc ενώ ταυτόχρονα δημιουργείται και ένα αρχείο Registry. Αυτή η διαδικασία δεν αλλάζει την πολιτική δημιουργίας pin.



Εικόνα 64. Το menu αλλαγής της Pin Policy για τον χρήστη ή τον διαχειριστή, ανάλογα με τις απαιτήσεις ασφαλείας της χρήσης για την οποία προορίζεται η κάρτα

5.2.7.2 Ρύθμιση πολιτικής βιβλιοθήκης του χρήστη

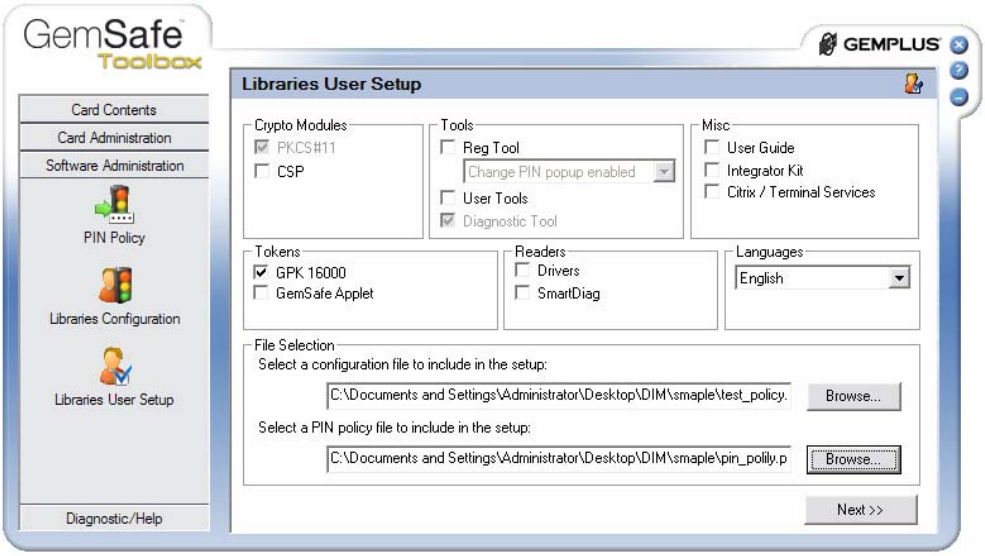
Με αυτήν την λειτουργία, ο διαχειριστής ορίζει μια δομή δυνατότητας αλληλεπίδρασης του χρήστη ή του διαχειριστή με το σύστημα. Επιλέγεται ανάλογα με τον σκοπό αλλά και την περίπτωση: Εάν ο user μπορεί να κάνει :unblock a card, able to change user or admin pin, remote unblock, user capability of importing - exporting deleting on a smart card. Τέλος ο διαχειριστής αποθηκεύει τις ρυθμίσεις αυτές σε ένα αρχείο .gls. Αυτή η διαδικασία δεν αλλάζει τις δυνατότητες αλληλεπίδρασης του χρήστη ή του διαχειριστή.



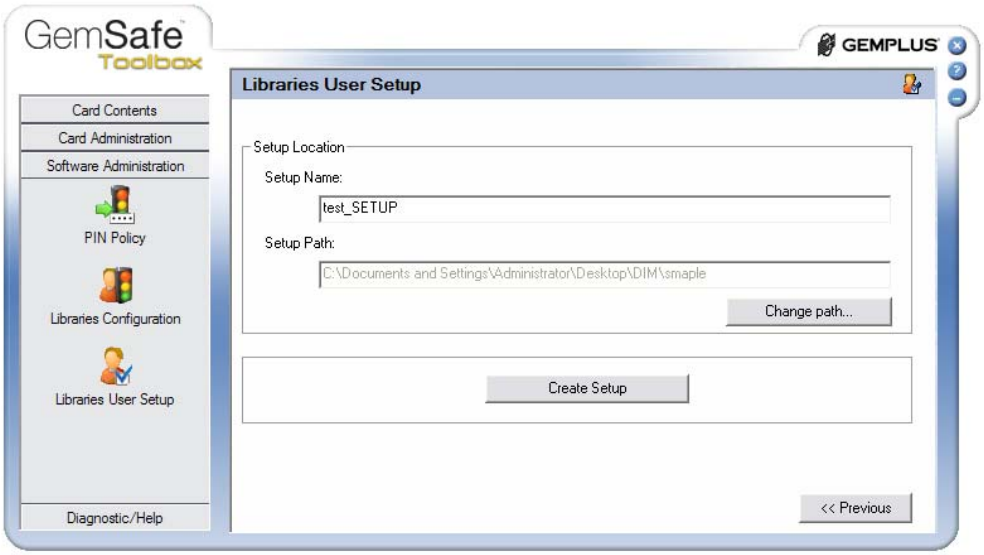
Εικόνα 65. Το menu ρύθμισης και αποθήκευσης ή επιλογής των αρχείων βιβλιοθήκης .gls

5.2.7.3 Δημιουργία αρχείου βιβλιοθήκης

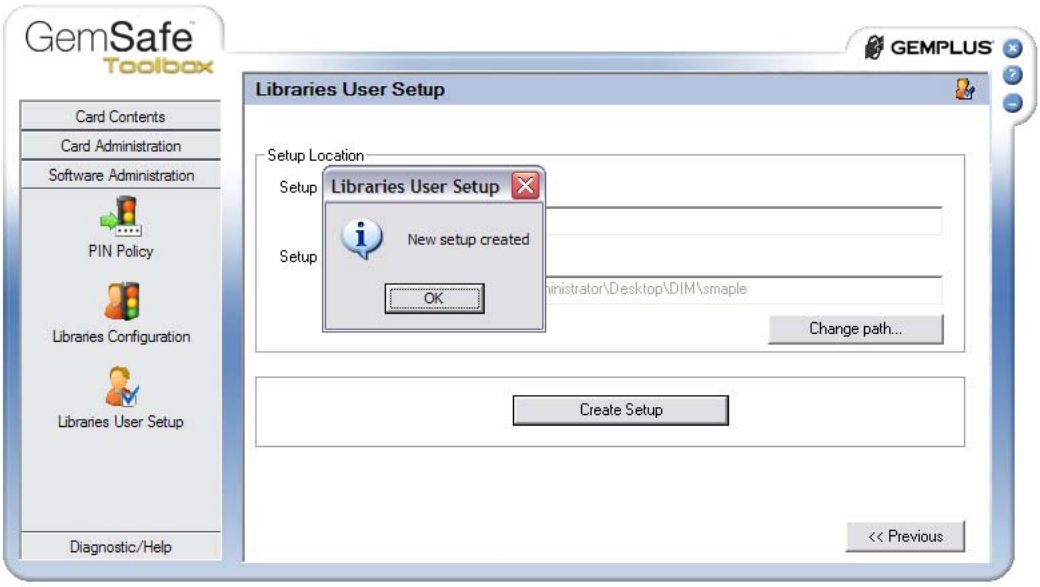
Μέσω της δυνατότητας αυτής, ο διαχειριστής μπορεί να ορίσει και να δημιουργήσει ένα αρχείο .exe το οποίο εγκαθιστά την πλήρως παραμετροποιημένη πολιτική συμπεριφορά του προγράμματος. Πιο συγκεκριμένα ο διαχειριστής επιλέγει ποιά: crypto modules, tools readers, tokens και languages. Καθώς επίσης επιλέγει pin policy και βιβλιοθήκη, επιλέγοντας τα αντίστοιχα αρχεία .ppc και .gls που έχει ο ίδιος ή κάποιος άλλος πράξει. Μετά τις επιλογές του αυτές παράγεται ένα αρχείο setup.exe που μπορεί να εγκατασταθεί σε οπουδήποτε pc που έχει είτε admin είτε user Gemsafe toolbox.



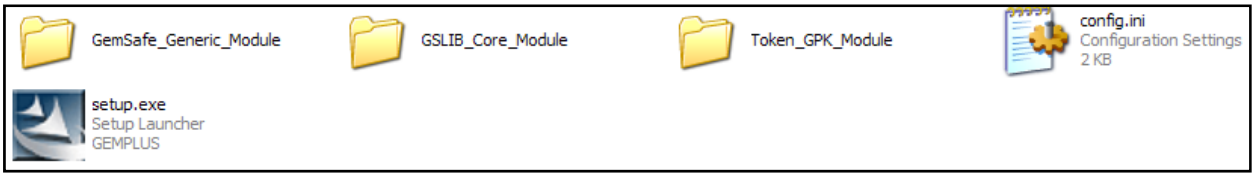
Εικόνα 66. Το menu ρύθμισης και δημιουργίας του αρχείου βιβλιοθήκης



Εικόνα 67. Ορισμός του ονόματος και της τοποθεσίας του test_SETUP φακέλου που περιέχει το setup.exe



Εικόνα 68. Επιτυχής δημιουργία του φακέλου test_SETUP



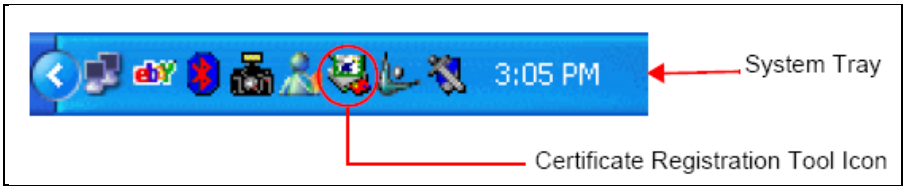
Εικόνα 69. Τα περιεχόμενα του αρχείου test_SETUP που παρήχθη

5.2.8 Έλεγχος και Βοήθεια

Η Gemalto παρέχει υποστήριξη πολλών επιπέδων στους χρήστες των Gemsafe libraries και κατ' επέκταση στους χρήστες του Gamsafe toolbox παρέχοντας το ιδιαίτερα χρήσιμο εργαλείο το Reg tool το οποίο καταχωρεί αυτόματα τα πιστοποιητικά της κάρτας. Επίσης παρέχονται το Diagnostic Tool και το SmartDiag τα οποία εξετάζουν κυρίως την κατάσταση των software και hardware της κάρτας και του υπολογιστή παρέχοντας την ανάλογη υποστήριξη όταν αυτό απαιτείται.

5.2.8.1 The certificate registration tool (Reg tool)

Το εργαλείο αυτό εάν είναι εγκατεστημένο, ανοίγει αυτόματα όταν ξεκινάνε τα Windows και ενεργοποιείται όταν εισάγεται η κάρτα στον reader. Το εργαλείο αυτό διαβάζει τα δεδομένα της κάρτας και δηλώνει (register) τα πιστοποιητικά στο ανάλογο Crypto Application Program Interface (CAPI). Η διαδικασία που ακολουθείται είναι η ίδια με την χειροκίνητη καταχώρηση, με μόνη διαφορά ότι το Reg tool ξεκινά αυτόματα.



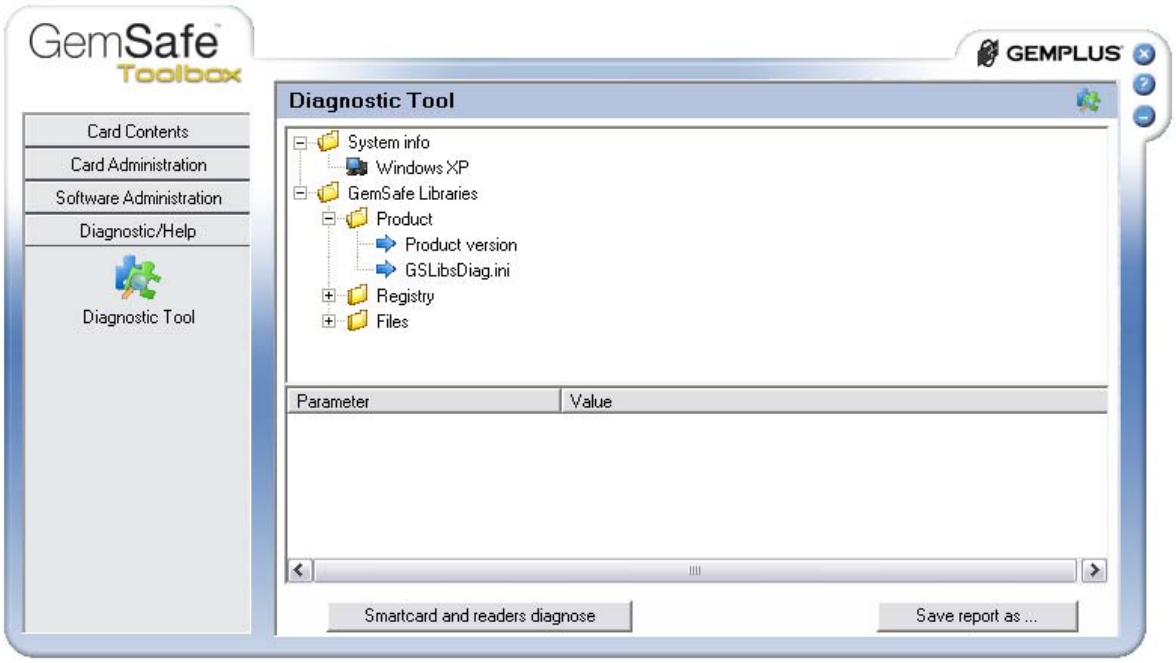
Εικόνα 70. Το Reg tool στο System Tray

Icon	Definition
	Certificate Registration Tool icon with no card inserted in the reader.
	Certificate Registration Tool icon with card inserted in the reader but no certificates on the card.
	Certicate Registration Tool icon with card inserted and registered certificate(s).

Εικόνα 71. Οι περιπτώσεις του Reg tool στο System Tray

5.2.8.2 Διαγνωστικός έλεγχος

Είναι ένας έλεγχος που κάνει το πρόγραμμα 1ον στον card reader και στην smart card και 2ον στον υπολογιστή. Για να επιβεβαιώσει πρώτα την καλή κατάσταση του reader και της κάρτας και αφετέρου να ελέγξει την δυνατότητα υποστήριξης του προγράμματος από τον υπολογιστή σε θέματα απαιτήσεων. Σε περίπτωση που κάτι δεν είναι εντάξει, ενημερώνεται ο χρήστης και δίνεται η δυνατότητα παραγωγής ενός report αρχείου το οποίο μπορεί να σταλεί στην Gemplus support για περεταίρω βοήθεια.



Εικόνα 72. Το menu δημιουργίας και αποθήκευσης Report

Επιλέγοντας το **Diagnostic Tool** ο χρήστης μπορεί να ελέγξει την κατάσταση του προγράμματος.

Το Diagnostic Tool παρέχει τα ακόλουθα:

- Πληροφορίες συστήματος
- Τιμές μητρώου και αρχεία του PKCS#11
- Πληροφορίες προϊόντος GemSafe Libraries
- Τιμές μητρώου για το GemSafe Libraries
- Κατάσταση των GemSafe Libraries αρχείων

Ο ακόλουθος πίνακας δείχνει τα εικονίδια του Diagnostic Tool με την περιγραφή τους.

Icon	Description
	The PC icon shows details about operating system of the GemSafe Libraries installation.
	A green magnifying glass icon shows that the registry item is stored and functioning correctly.
	A red magnifying glass icon indicates that the registry item is absent. In this case, you should remove the current installation of GemSafe Libraries and re-install it.
	A file icon with a green tick shows that the file or dll is installed and functioning correctly.
	A white cross on a red background indicates that the file does not correspond to a known version. In this case, you should reinstall GemSafe Libraries.
	A file icon with a question mark tick indicates that the file could not be read or is an unexpected version.
	A blue arrow indicates that more information is available.

Εικόνα 73. Περιγραφή των εικονιδίων

Για την παραγωγή status report επιλέγουμε **Report** > **Save as**. Από το **Save as** παράθυρο αποθηκεύεται σε .txt αρχείο στην τοποθεσία που επιλέγει ο χρήστης.

Ένα παράδειγμα Report :

GSLDiagnReport.txt [20]

5.2.8.3 Διάγνωση Smart Card και Reader

Υπάρχει η δυνατότητα να επισκόπησης των ιδιοτήτων της smart card και του smart card reader με την χρήση του SmartDiag Tool, μέσα από το Diagnostic Tool. Στο Diagnostic Tool, επιλέγοντας **Smart card and reader diagnose** ανοίγει το SmartDiag Tool

5.2.8.4 SmartDiag Tool

Το SmartDiag Tool επιβεβαιώνει την διαθεσιμότητα των ακόλουθων:

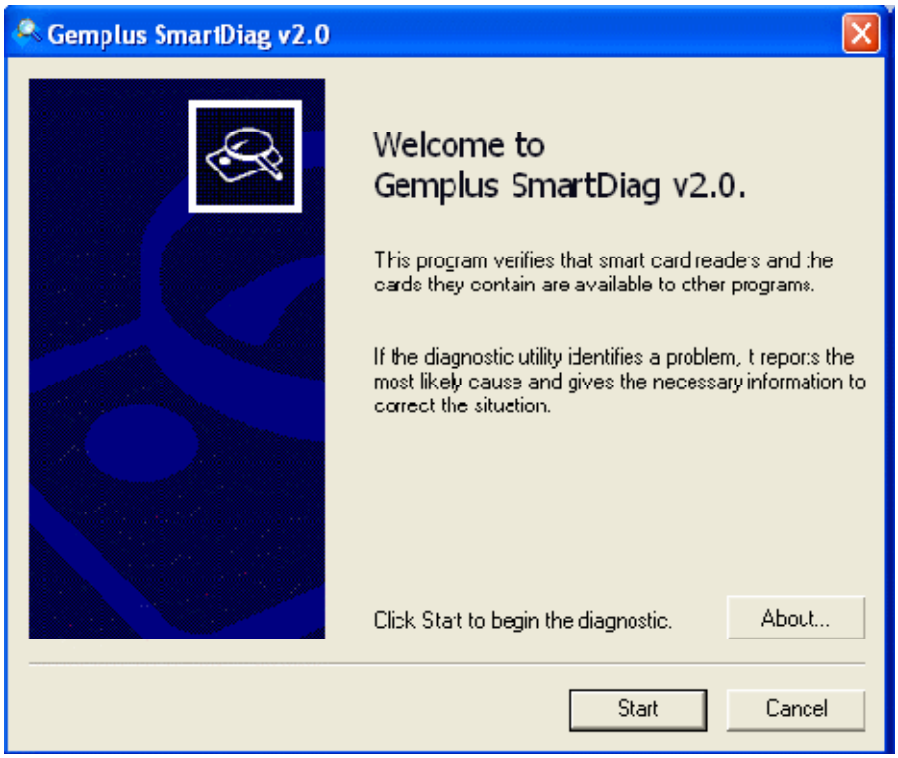
- Τα services του λειτουργικού συστήματος που συνεργάζονται με την κάρτα
- Τους Smart card readers
- Τις Smart cards

[20] Βλέπε Παράρτημα ΙΙ

Το tool αυτό επίσης αναφέρει οποιοδήποτε πρόβλημα software ή hardware και παρέχει πληροφορίες επίλυσης του.

5.2.8.5 Η εφαρμογή Gemplus SmartDiag v2.0

1) Ανοίγουμε το SmartDiag Tool μέσω του Diagnostic Tool, είτε μέσω του **Start/Programs/Gemplus/SmartDiag/SmartDiag v2.0,** έχουμε πρόσβαση στην εφαρμογή.

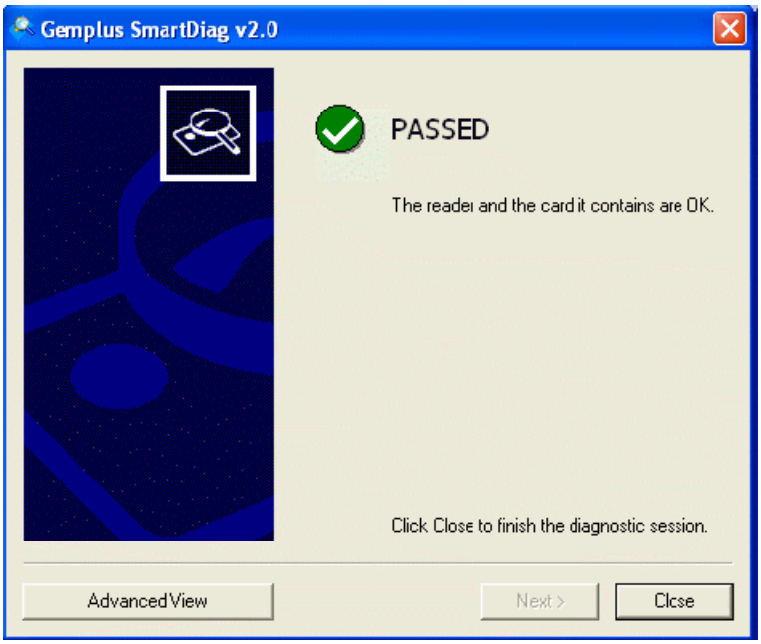


Εικόνα 74. Το Welcome παράθυρο, επιλέγοντας Start ξεκινάει η diagnostic session.

2. Το SmartDiag Tool ξεκινάει μία diagnostic session για να εξετάσει πιθανά προβλήματα με την εγκατάσταση του smart card reader ή της smart card που χρησιμοποιείται . Το αποτέλεσμα μπορεί να είναι ένα από τα ακόλουθα:

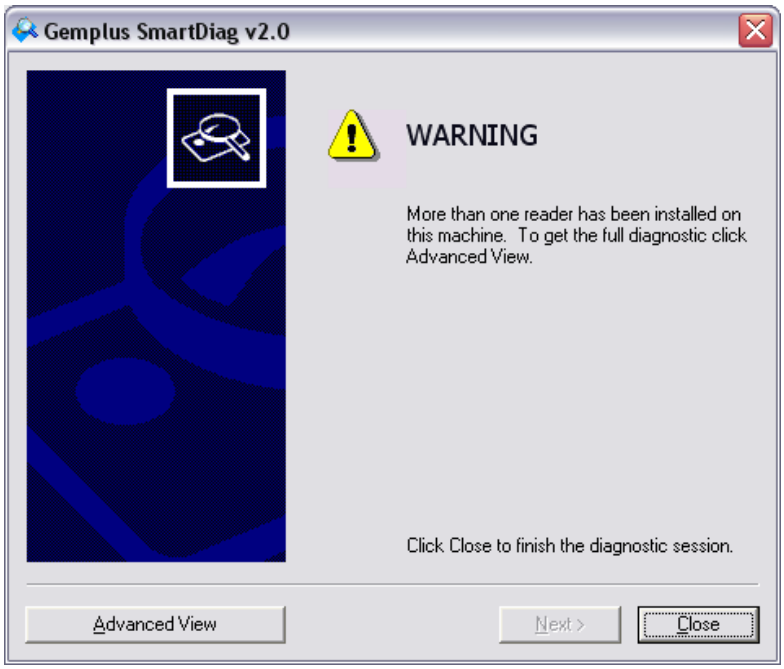
- Passed
- Failed
- Warning

3. Εάν όλα τα τμήματα είναι όπως πρέπει να είναι τότε εμφανίζεται:

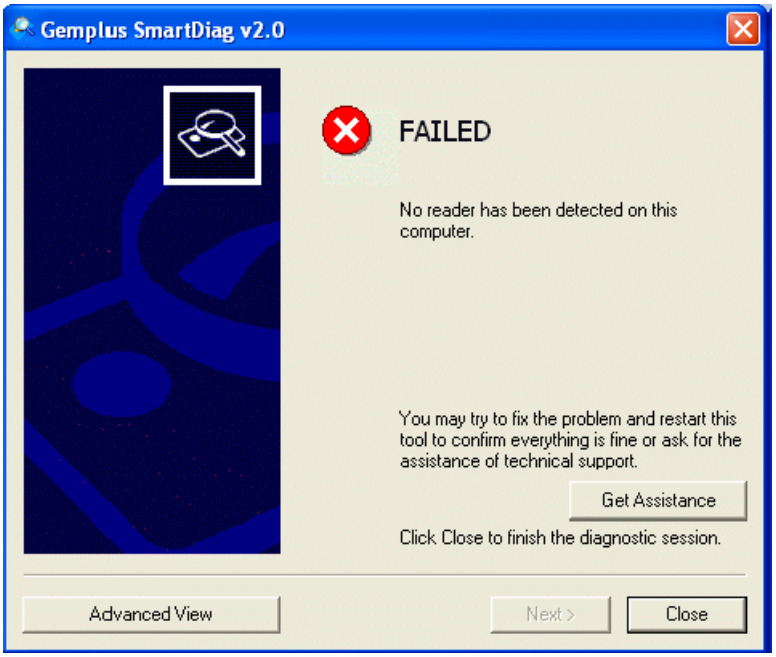


Εικόνα 75. Το παράθυρο επιτυχούς diagnostic session

Εάν το αποτέλεσμα είναι **Warning**, προτείνεται η επιλογή **Advanced View** για περεταίρω πληροφορίες

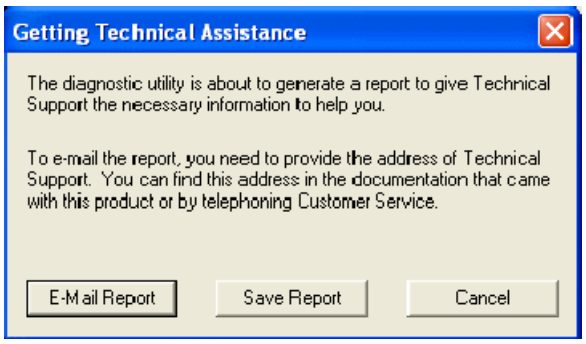


Εικόνα 76. Το παράθυρο diagnostic session με Warning αποτέλεσμα



Εικόνα 77. Το παράθυρο diagnostic session με FAILED αποτέλεσμα

Εάν το αποτέλεσμα είναι **FAILED**, με την επιλογή **Advanced View** ο χρήστης έχει πρόσβαση σε περεταίρω πληροφορίες όσο αφορά το πρόβλημα που έχει προκύψει. Και με την επιλογή **Get Assistance** παρέχεται στον χρήστη βοήθεια για την επίλυση του προβλήματος, ενώ σε περιπτώσεις που το πρόβλημα δεν λύνεται παροτρύνεται ο χρήστης να εγκαταστήσει το πρόγραμμα από την αρχή. Υπάρχουν πολλοί λόγοι να έχει αποτέλεσμα failed ένα diagnostic session, και αυτό συνήθως συμβαίνει όταν το πρόγραμμα δεν εκτελείται σωστά είτε για λόγους κατάστασης του υπολογιστή ή για λόγους προβληματικού Registry των Windows, είτε για λόγους κατεστραμμένης κάρτας.

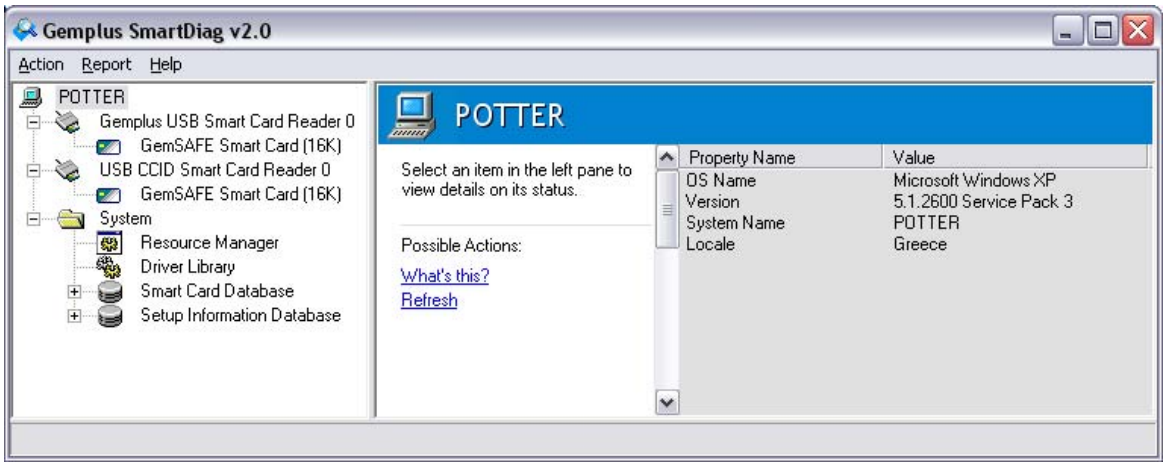


Εικόνα 78.Η παραπομπή Get Assistance

Η επιλογή **Advanced View** παρέχει περαιτέρω πληροφορίες για την κατάσταση του υποσυστήματος της κάρτας και τα προγράμματα διαχείρισης της. Ο σκοπός του Advanced View είναι το να παρέχει real-time περιγραφή της κατάστασης και εκτενή αναφορά των στοιχείων που σχετίζονται με την κάρτα. Αυτό μπορεί να φανεί ιδιαίτερα χρήσιμο, φανερώνοντας κρυφά ή low-level προβλήματα. Όπως επίσης μέσω

Advanced View αναγνωρίζονται οι εκδόσεις του λογισμικού και των hardware τμημάτων της smart card.

Παράδειγμα Advanced View:



Εικόνα 79. Το παράθυρο Advanced View

Τα περιεχόμενα του Advanced view είναι:

- Smart card readers και smart cards
- Services (συμβατότητα εφαρμογών, αναγνώριση reader)
- System (Resource Manager, driver library και Smart Card Database).

4. Για την παραγωγή report επιλέγεται **Report** > **Generate** και παράγεται το SmartDiag_Report.txt αρχείο στην επιλεγμένη τοποθεσία. Η SmartDiag_Report είναι πιο εκτενής αναφορά από την απλή GSLDiagnReport, παρέχοντας όλες τις απαραίτητες πληροφορίες που απαιτεί η τεχνική υποστήριξη. Στην περίπτωση που το αποτέλεσμα του ελέγχου είναι **Failed**, συνήθως το συνοδευτικό μήνυμα εξηγεί πλήρως την αιτία του προβλήματος . Επιπλέον είτε παρέχει την λύση είτε παραπέμπει στην **Get Assistance,** δυνατότητα επικοινωνίας με τεχνική υποστήριξη.

5.2.8.6 Τεχνική υποστήριξη

Στην περίπτωση που οι βοήθειες του SmartDiag Tool δεν επιλύουν τα προβλήματα που αντιμετωπίζει ο χρήστης, δίνεται η δυνατότητα της τεχνικής υποστήριξης από την GemSafe. Όπου ο χρήστης αποστέλλει την SmartDiag_Report, για πιο εξειδικευμένη και αποτελεσματική βοήθεια.

5.3 Windows Secure Logon

Το Windows Secure Logon (Interactive logon με smart card), είναι μια δυνατότητα επέκτασης της ασφαλείας ενός σταθμού εργασίας με τα πλεονεκτήματα των Smart card. Οι GemSafe Libraries υποστηρίζουν αυτήν την δυνατότητα υλοποιώντας την αυτόματα. Τα βήματα για να υλοποιηθεί το Interactive logon με smart card είναι απλά και δεν απαιτούν τις GemSafe Libraries.

5.3.0.1 Υλοποίηση του Interactive logon με smart card

Τα βήματα είναι τα εξής:

"Interactive logon: Require smart card" setting to control

Στην επιλογή των **Administrative tools** του Control panel επιλέγεται το **Local Security Policy**.

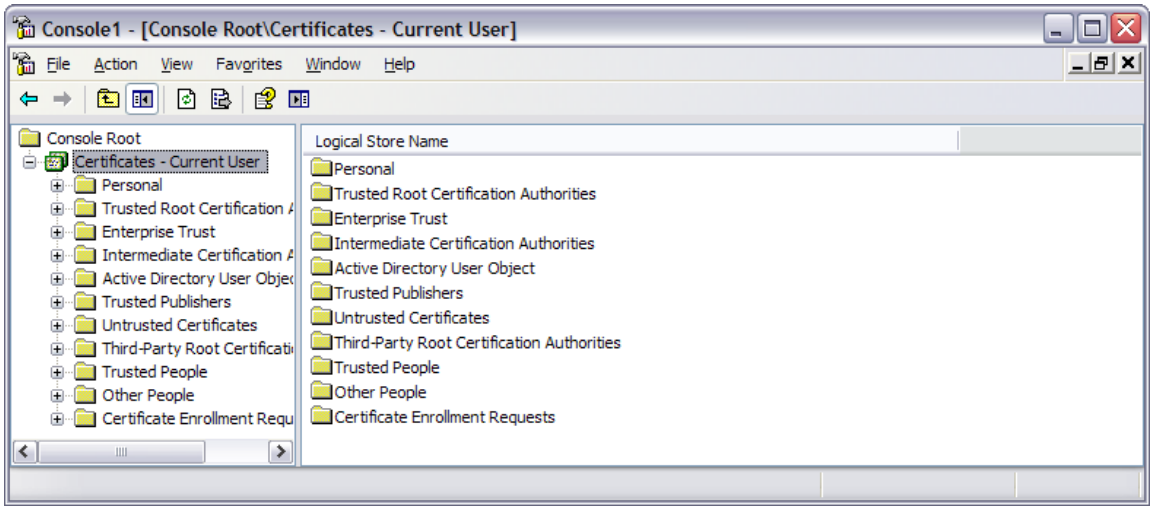
1. Ανοίγεται το **Local Policies**, και επιλέγεται **Security Options**.
2. Κάνοντας διπλό κλικ στο: **Interactive logon: Require smart card**.
3. Ο χρήστης έχει τις εξής επιλογές:

    - Για να καθοριστεί ότι οι χρήστες μπορούν να συνδεθούν με τον υπολογιστή μόνο με τη χρήση έξυπνων καρτών, επιλέγει **Enabled**.
    - Για να καθοριστεί ότι οι χρήστες μπορούν να συνδεθούν με τον υπολογιστή, χρησιμοποιώντας οποιαδήποτε μέθοδο, επιλέγει **Disabled**.

5.3.0.2 Προετοιμασία smart card certificate στο enrollment station[21]

1. Στο σύστημα που επιθυμεί ο χρήστης συνδέεται ως user ή administrator.
2. Στο **Start**, επιλέγεται **Run**, και εισάγεται η εντολή **mmc**.
3. Ανοίγει το Console root των Windows.
4. Στο **File** menu, επιλέγεται το **Add/Remove Snap-in** και **Add**.
5. Μέσα στο **Snap-in** μενού, κάνοντας διπλό κλικ στα **Certificates**.Όπου αναδύεται ένα μενού επιλογών όπου εκεί επιλέγεται το **My user account** και **Finish**.
6. Κάνοντας διπλό κλικ **Certificates - Current User** αναδύεται το console tree.
7. Από το console tree, επιλέγεται το **Personal,** Certificates – Current User/Personal.
8. Στο **Action** menu, ανοίγοντας το **All Tasks**, επιλέγεται το **Request New Certificate**.
9. Αμέσως ανοίγει ο Certificate Request Wizard, όπου ο οδηγός **Enrollment Agent** certificate καθοδηγεί τον χρήστη για την δημιουργία του πιστοποιητικού.
10. Όταν ολοκληρωθεί η διαδικασία επιλέγεται το **Install Certificate**.
11. Το πιστοποιητικό έχει καταχωρηθεί για ως πιστοποιητικό πρόσβασης των Windows για τον συγκεκριμένο χρήστη.

[21] Πηγή: http://technet.microsoft.com/en-us/library/cc781592.aspx



Εικόνα 80. .Το Console root των Windows XP με το certificate root

5.3.0.3 Ρύθμιση της smart card για user logon[22]

1. Στην σελίδα του **Smart Card Certificate Enrollment Station**, στον οδηγό **Certificate Template**, ο χρήστης μπορεί να επιλέξει από τα ακόλουθα:

    - Click **Smart Card Logon** εάν επιθυμεί να χρησιμοποιεί την κάρτα μόνο για logging στα Windows.
    - Click **Smart Card User** εάν επιθυμεί να χρησιμοποιεί την κάρτα και για υπογραφή e-mail σε συνδυασμό με το logging στα Windows.
2. Στο **Certification Authority**, επιλέγεται το όνομα της επιθυμητής CA για την καταχώρηση του πιστοποιητικού.
3. Στο **Cryptographic Service Provider**, επιλέγεται ο cryptographic service provider (CSP) από τους κατασκευαστές καρτών.
4. Στο**Administrator Signing Certificate**, επιλέγεται ο Enrollment Agent certificate, ο οποίος θα υπογράψει το enrollment request.
5. Στην επιλογή **User To Enroll**, επιλέγεται το **Select User**, όπου ορίζεται ο συγκεκριμένος χρήστης της κάρτας, και για την εκτέλεση click στο **Enroll**.
6. Όταν ζητηθεί από το σύστημα, τοποθετεί ο χρήστης την έξυπνη κάρτα στον card reader και επιλέγει **OK**. Μετά όταν ζητηθεί από το σύστημα, ο χρήστης πληκτρολογεί τον προσωπικό αριθμό αναγνώρισης (PIN) για την έξυπνη κάρτα.
7. Όταν το πιστοποιητικό που θα είναι εγκατεστημένο στην έξυπνη κάρτα, η ιστοσελίδα της CA θα σας δώσει τη δυνατότητα να προβάλλετε το πιστοποιητικό που έχει μόλις εγκατασταθεί.

5.3.1 Χρήση του Windows Secure Logon

[22] Πηγή: http://technet.microsoft.com/en-us/library/cc775842.aspx

Το Windows Secure Logon ενσωματώνεται τα Windows (2000, XP και VISTA). Με την χρήση smart card reader και μία card που περιέχει ένα certificate.

5.3.2 Δυνατότητες του Windows Secure Logon

- Log on και Log off στον σταθμό εργασίας.
- Lock του σταθμού εργασίας.
- Έλεγχος πρόσβασης σε επιλεγμένες εφαρμογές.

5.3.3 Log on με την χρήση Smart card

Παράδειγμα εισόδου στα Windows 2000 και XP με την χρήση smart card ανοίγοντας τα Windows. Το μήνυμα **Welcome to Windows** εμφανίζεται.

Εικόνα 81. Το παράθυρο Welcome των Windows 2000

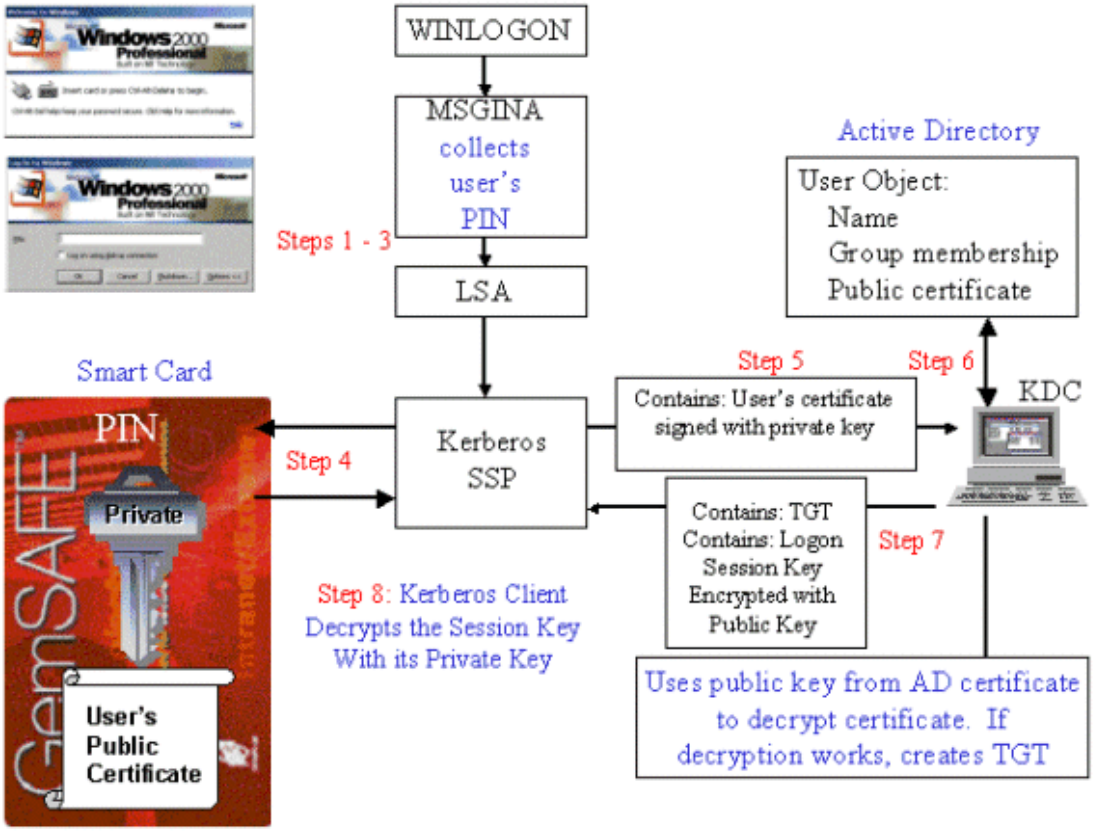
Εικόνα 82. Το παράθυρο Welcome των Windows XP

Εισάγοντας την κάρτα στον card reader αυτόματα ανοίγει το **Log On to Windows**

Εικόνα 83. Log On στα Windows 2000

Εισαγωγή Pin.

Εικόνα 84. Log On στα Windows XP



Εικόνα 85. Διαδικασία ενεργοποίησης smart card logon[23]

5.3.4 Lock του σταθμού εργασίας

Το Windows Secure Log On, παρέχει την δυνατότητα ενισχυμένου Lock του σταθμού εργασίας, υπό την έννοια ότι η διαδικασία του Lock γίνεται πολύ πιο γρήγορα, απλά με την εξαγωγή της κάρτας ο σταθμός εργασίας κλειδώνει. Ενώ το ίδιο απλά με τη εισαγωγή της κάρτας ο σταθμός εργασίας είναι και πάλι διαθέσιμος στον χρήστη.

[23] Πηγή : http://support.microsoft.com/kb/834875

Εικόνα 86. Το σχετικό μήνυμα ότι ο σταθμός εργασίας είναι κλειδωμένος

5.4 Η ασφάλεια των GemSafe Libraries

Τα Windows για να αλληλεπιδράσουν με τις smart cards και τους card readers χρησιμοποιούν την βιβλιοθήκη winscard.dll, η οποία εγκαθίσταται μέσω update μετά την πρώτη σύνδεση του υπολογιστή με κάποιον smart card reader. Η βιβλιοθήκη winscard.dll θα μπορούσε να χαρακτηριστεί ως ένα ευαίσθητο σημείο της επικοινωνίας ενός συστήματος με μία smart card. Μια τεχνική για να υποκλαπούν πολύτιμα δεδομένα (όπως πχ. το pin) από μία κάρτα είναι η παρακολούθηση της winscard.dll, με την παρακολούθηση μέσω ενός (hook) υποκλέπτονται οι εντολές APDU που μεταφέρουν όλα τα ευαίσθητα δεδομένα μαζί τους. Παράδειγμα τέτοιας υποκλοπής αποτελεί η εφαρμογή **apduview**[24], υλοποιώντας τα βήματα της ένας επιτιθέμενος αντιγράφει κάποια διαμορφωμένη έκδοσή της winscard.dll και ορίζει σε ποιο εκτελέσιμο θα τοποθετηθεί το hook. Με αυτόν τον τρόπο παράγεται ένα αρχείο κειμένου (winscard.txt) στο οποίο καταγράφονται όλες οι εντολές που εκτελούνται. Η επίθεση αυτή αντιμετωπίζεται με δύο τρόπους:

- Κρυπτογραφημένα δεδομένα

Ένα πρόγραμμα smart card μπορεί να σχεδιασμένο έτσι ώστε να κρυπτογραφούνται τα ευαίσθητα δεδομένα μέσα στην κάρτα και να αποκρυπτογραφούνται αφού ληφθούν από το πρόγραμμα του υπολογιστή και αντίστροφα, έτσι ώστε σε περίπτωση υποκλοπής τους να μην είναι εύκολη η ανάγνωση των ευαίσθητων πληροφοριών.

- Hash έλεγχος του εκτελέσιμου

Ένα πρόγραμμα smart card μπορεί να ελέγχει με διαφόρους τρόπους εάν το αρχικό εκτελέσιμο έχει υποστεί οποιαδήποτε μη επιθυμητή παρέμβαση ένας αποτελεσματικός τρόπος είναι και ο έλεγχος της hash σύνοψης του. Οι GamSafe Libraries ακολουθούν αυτήν την τακτική. Το εκτελέσιμο αναγνωρίζει ότι έχει

[24] *http://www.fernandes.org/apduview/index.html*

τροποποιηθεί σαν αρχείο όπως στην προκειμένη περίπτωση όπου έχει τοποθετηθεί το hook,και μπλοκάρει την λειτουργία του είτε εμφανίζοντας σχετικό μήνυμα και τερματίζοντας την λειτουργία του, είτε αναστέλλοντας όλες του της δράσεις όπως γίνεται και στο GamSafe toolbox, όπου απλά ο χρήστης δεν είχε την δυνατότητα να εκτελέσει καμία ενέργεια. Μετά την αφαίρεση του hook όλα λειτουργούν πάλι κανονικά.

```
SCardTransmit (handle 0xEA010000):
 transmitted:
  80 CA 9F 7F 2D
 received:
  9F 7F 2A 00 15 00 04 32 31 12 99 32 30 02 79 00 01 08 57 00 A3 12
92 10 92 12
  93 10 92 03 34 10 94 00 00 01 00 00 00 00 00 00 00 00 00 90 00

SCardTransmit (handle 0xEA010000):
 transmitted:
  00 A4 04 00 08 A0 00 00 00 98 20 11 05
 received:
  61 21
```

Εικόνα 87. Παράδειγμα δύο υποκλεμμένων εντολών, η πρώτη έχει μεταφορά δεδομένων από την κάρτα ενώ η δεύτερη είναι μήνυμα επιβεβαίωσης.

6. Χρήση των περιεχόμενων των Smart card από ξένες εφαρμογές

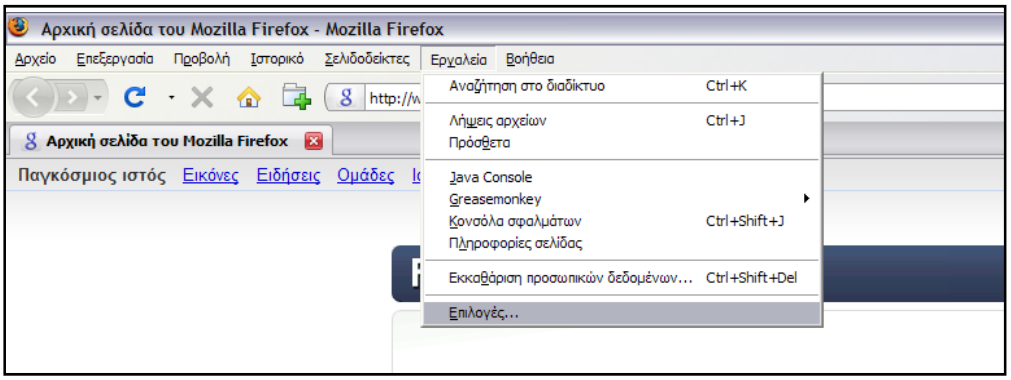
Οι Gemsafe libraries συνδυάζονται με την βιβλιοθήκη winscard.dll και παρέχουν διασύνδεση με τον Card Reader σαν συσκευή ασφαλείας στο λειτουργικό σύστημα. Όπως επίσης παρέχεται ελεγχόμενη πρόσβαση στα πιστοποιητικά που είναι καταχωρημένα στην κάρτα. Οι περιπτώσεις χρήσης των καρτών που θα εξεταστούν είναι με τον Mozilla Firefox και Mozilla Thunderbird ως συσκευή ασφαλείας και με Adobe Acrobat, το οποίο αναγνωρίζει αυτόματα (από το Reg tool) τα καταχωρημένα πιστοποιητικά.

6.0.1 Συσκευή ασφαλείας(security device).

Το Hardware ή το software που παρέχει κρυπτογραφικές υπηρεσίες όπως κρυπτογράφηση – αποκρυπτογράφηση και μπορεί να αποθηκεύει πιστοποιητικά και κλειδιά. Ένα hardware παράδειγμα αποτελεί η smart card ενώ software παράδειγμα αποτελεί ένας Certificate_Manager που παρέχει την δική του ενσωματωμένη ασφαλή διαχείριση δεδομένων. Κάθε τύπος συσκευής ασφαλείας είναι πάντα διαθέσιμος στο πρόγραμμα που τον διαχειρίζεται (πχ browser). Κάθε συσκευή ασφαλείας προστατεύεται από τον δικό της κωδικό ασφαλείας. Οι συσκευές ασφαλείας διαχειρίζονται από τις κρυπτογραφικές μονάδες (PKCS #11 module ή cryptographic module). Μία κρυπτογραφική μονάδα είναι ένα πρόγραμμα που διαχειρίζεται γενικότερα κρυπτογραφικές υπηρεσίες, παρέχοντας την διασύνδεση που χρειάζεται για να εξυπηρετούνται υπηρεσίες κάθε τύπου (software/hardware).

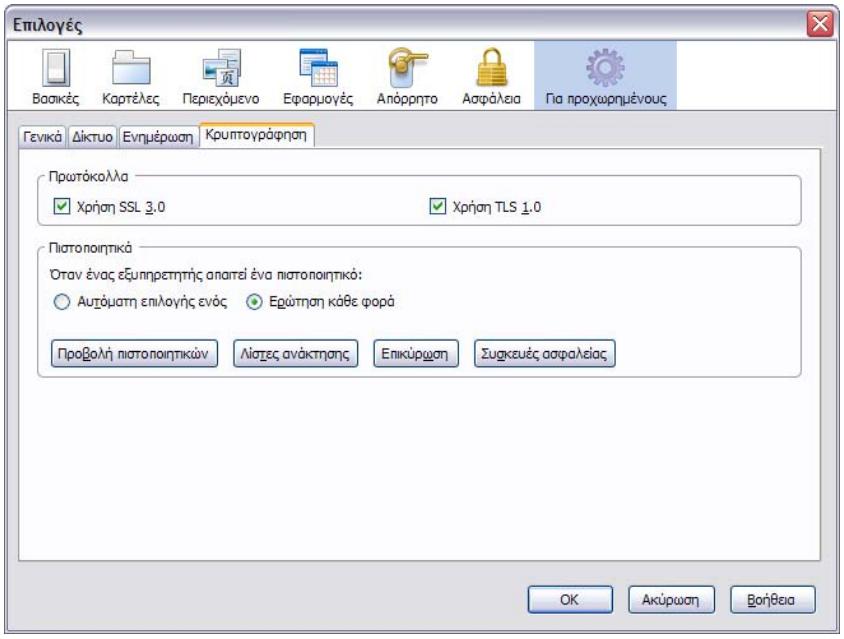
6.1 Mozilla Firefox

Για την εγκατάσταση μιας συσκευής ασφαλείας επιλέγεται το μενού ‘Επιλογές’ στην επιλογή ‘Εργαλεία’ του Mozilla Firefox:



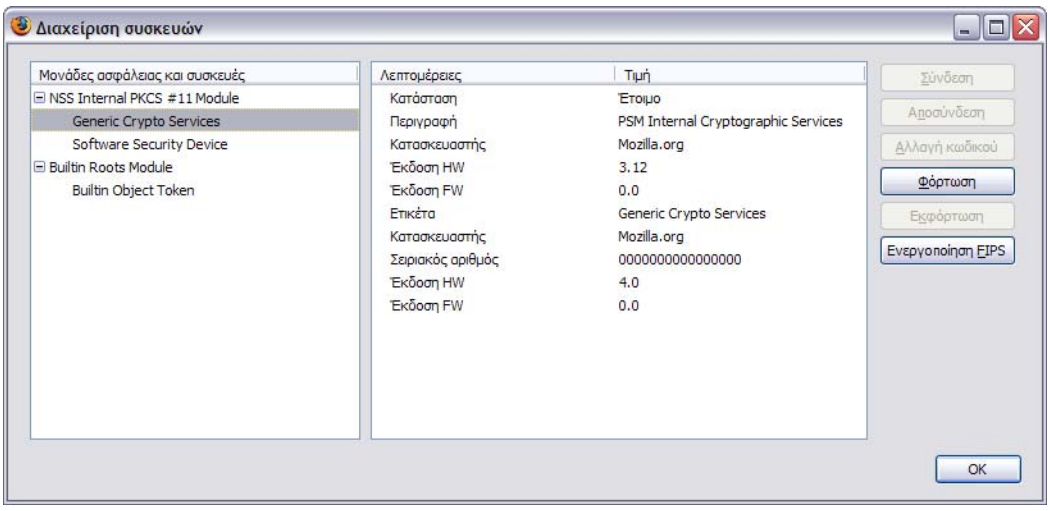
Εικόνα 88. Το εργαλείο Επιλογές

Εμφανίζεται το παράθυρο των επιλογών



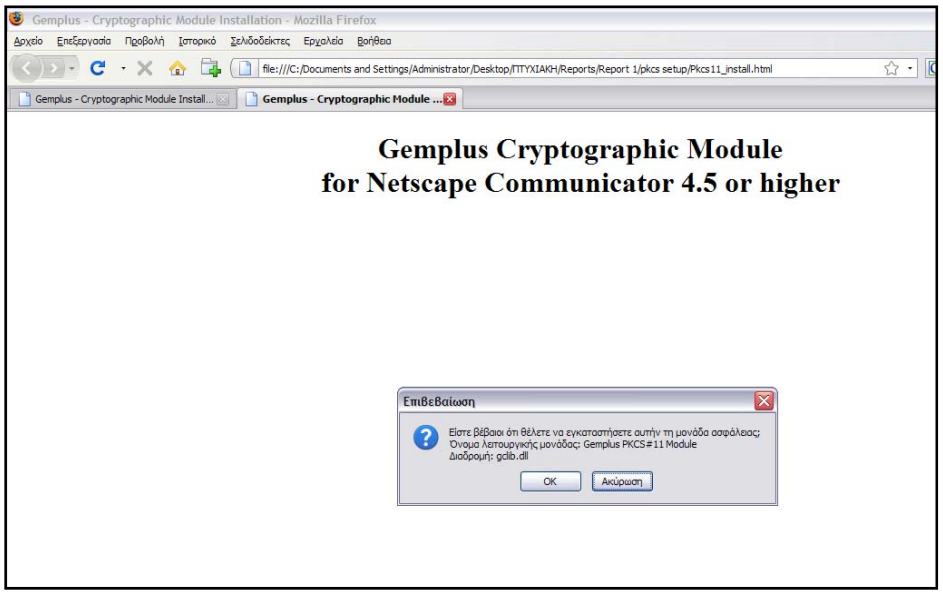
Εικόνα 89. Το παράθυρο των επιλογών

Όπου επιλέγεται το Συσκευές ασφαλείας και εμφανίζεται το παράθυρο της Διαχείρισης συσκευών, οπού είναι όλες οι καταχωρημένες κρυπτογραφικές μονάδες που χρησιμοποιεί ή μπορεί να χρησιμοποιήσει ο Firefox.



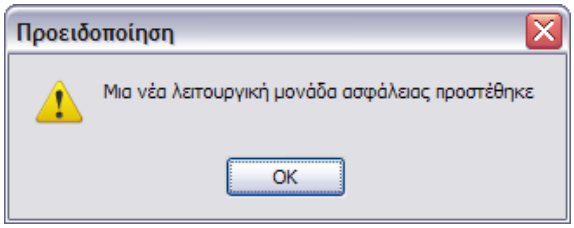
Εικόνα 90. Το παράθυρο της Διαχείρισης συσκευών

Για την εγκατάσταση του module στο σύστημα τρέχουμε το αρχείο Pkcs11_install.html που παρέχεται από την Gemsafe. Το αρχείο αυτό τρέχει ένα JavaScript κώδικα και προσθέτει την απαραίτητη κρυπτογραφική μονάδα



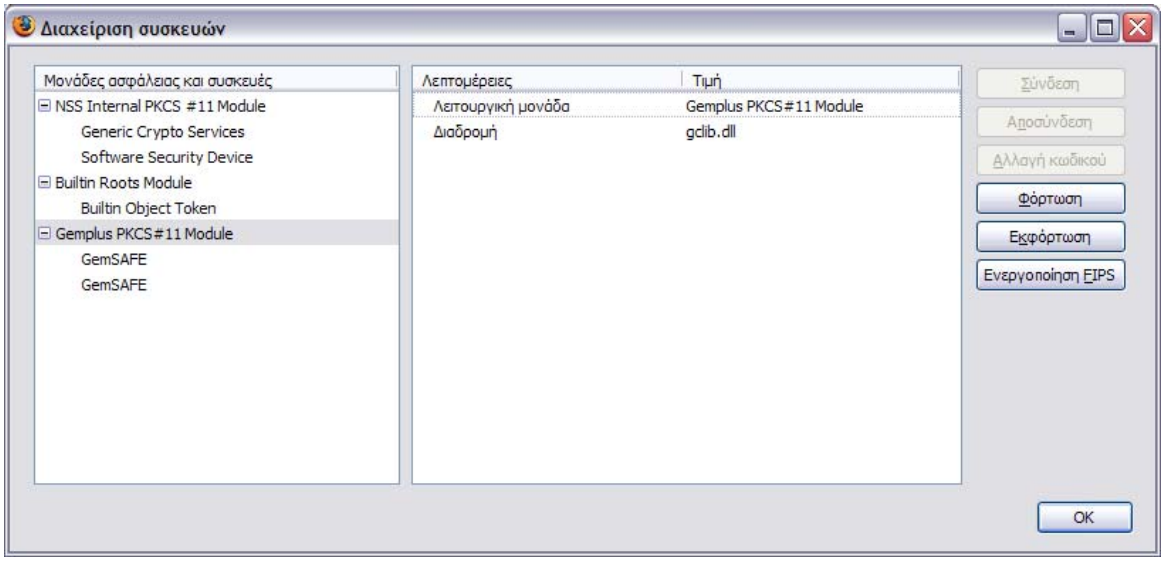
Εικόνα 91. Το αρχείο Pkcs11_install.html

Το αρχείο Pkcs11_install.html ανοίγει με τον Firefox, και ζητάει από τον χρήστη να επιβεβαιώσει την εγκατάσταση, και μετά την επιβεβαίωση του χρήστη εμφανίζεται το σχετικό μήνυμα της επιτυχούς εγκατάστασης.

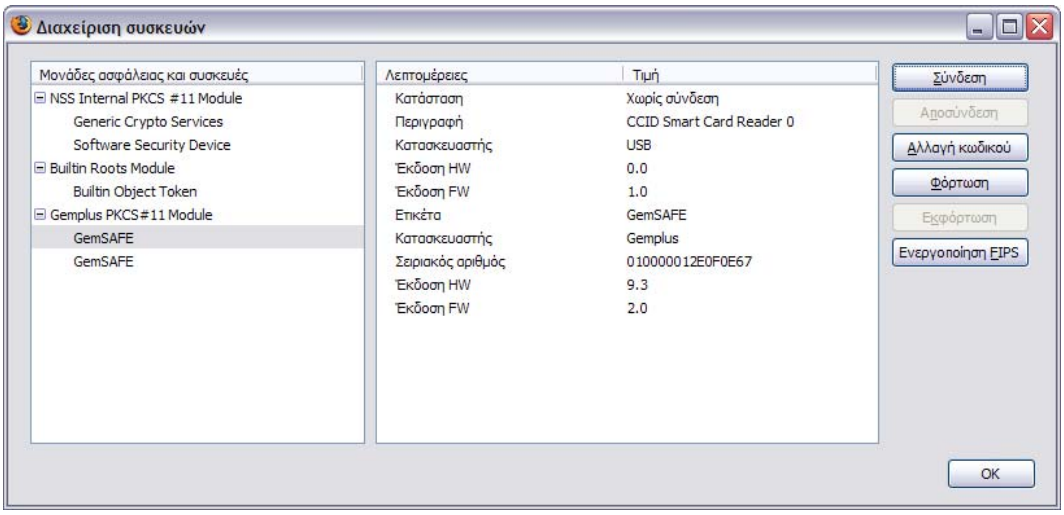


Εικόνα 92. Το μήνυμα επιτυχούς εγκατάστασης

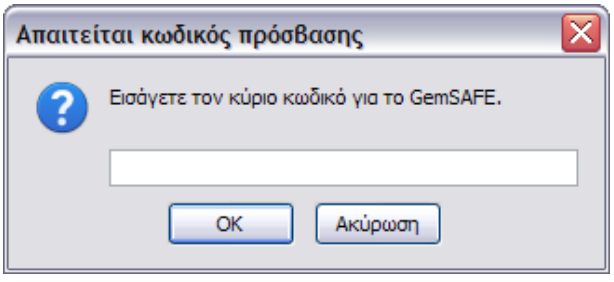
Στο μενού της διαχείρισης συσκευών υπάρχουν διαθέσιμες οι νέες κρυπτογραφικές μονάδες. Για να μπορούν να χρησιμοποιηθούν από τον browser πρέπει να έχουν φορτωθεί πρώτα. Αυτό γίνεται απλά μέσω της επιλογής Φόρτωση, οπού απλά ο χρήστης εισάγει τον κωδικό πρόσβασης της κάρτας. Και η φόρτωση της ή των κρυπτογραφικών μονάδων είναι επιτυχής.



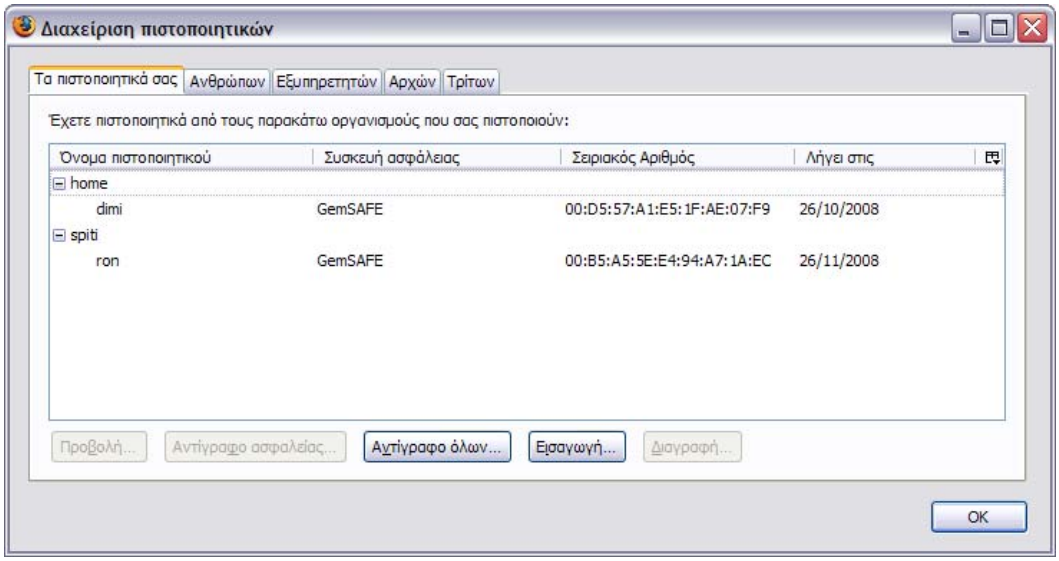
Εικόνα 93. Το παράθυρο της Διαχείρισης συσκευών με τις νέες προσθήκες, έχουμε 2 GemSafe modules, έναν για κάθε card reader που είναι συνδεμένος στο σύστημα



Εικόνα 94. Οι λεπτομέρειες της νέας κρυπτογραφικής μονάδας

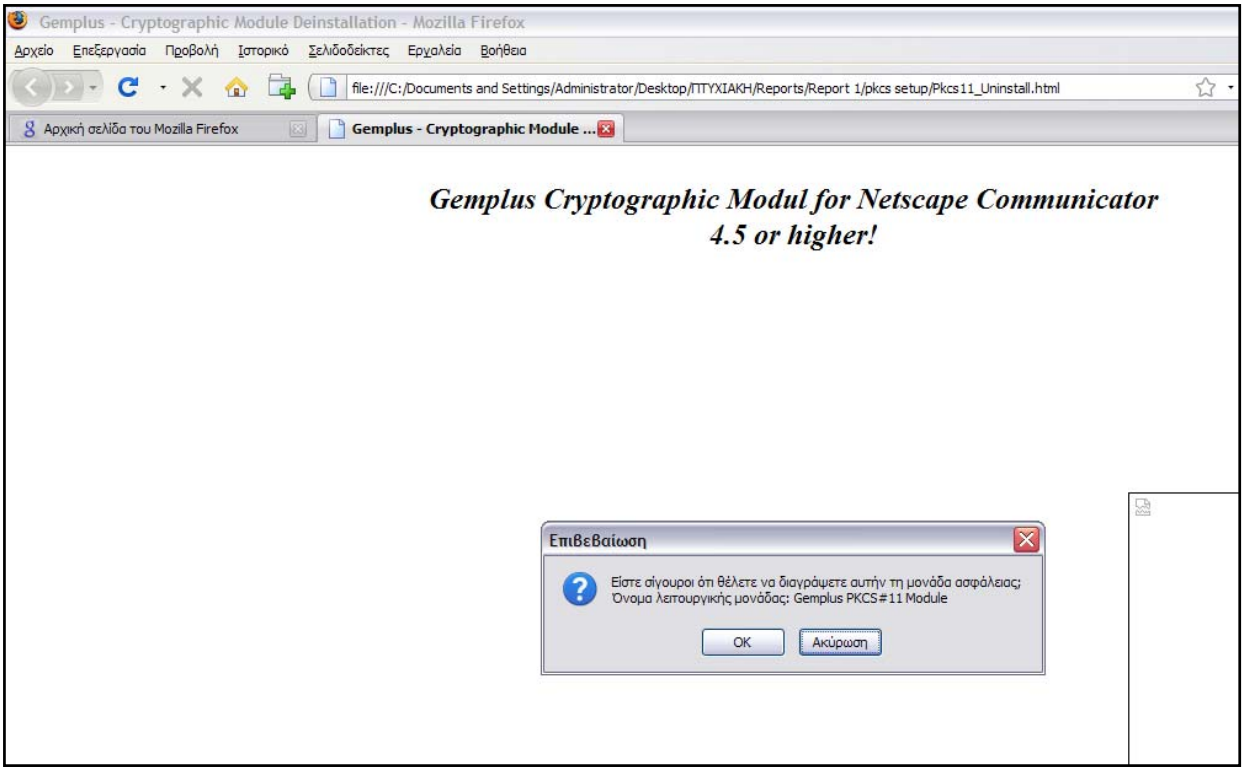


Εικόνα 95. Για την προβολή πιστοποιητικού απαιτείται εισαγωγή του κωδικού της κάρτας

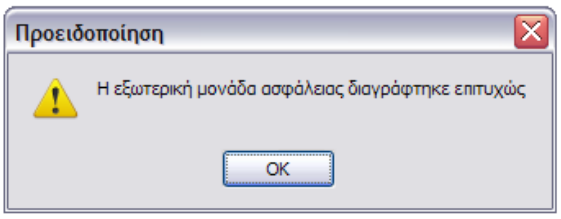


Εικόνα 96. Το μενού διαχείρισης πιστοποιητικών του χρήστη

Για την απεγκατάσταση του module από το σύστημα, αντίστοιχα τρέχουμε το αρχείο Pkcs11_Uninstall.html που επίσης παρέχεται από την Gemsafe. Το αρχείο αυτό τρέχει ένα JavaScript κώδικα που αφαιρεί την συγκεκριμένη κρυπτογραφική μονάδα



Εικόνα 97. Η διαγραφή της κρυπτογραφικής μονάδας



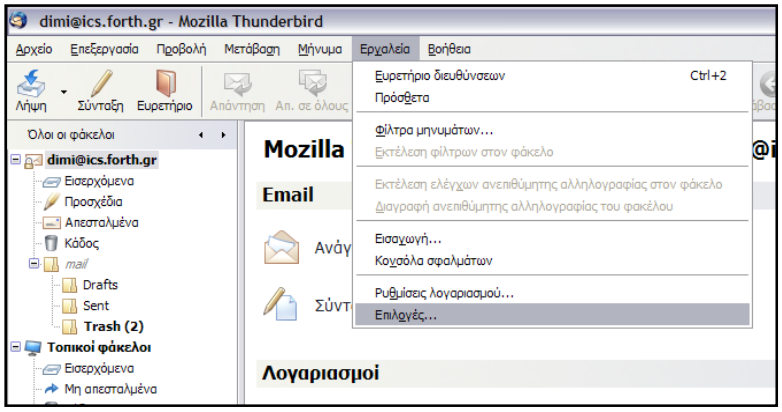
Εικόνα 98. Το μήνυμα επιτυχούς διαγραφής

6.2 Thunderbird

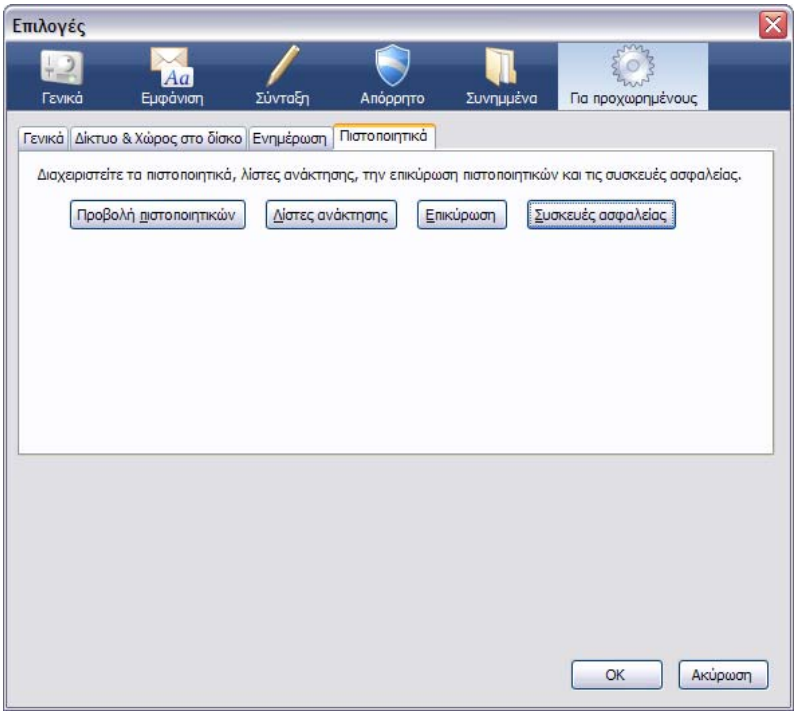
Το Mozilla Thunderbird, όπως και ο Firefox, έχει πρόσβαση στα πιστοποιητικά, που περιέχονται στην κάρτα για δύο χρήσεις, είτε για υπογραφή μηνύματος είτε για κρυπτογράφηση μηνύματος. Για να είναι τα πιστοποιητικά διαθέσιμα στον Thunderbird, ακολουθείται μια διαδικασία εγκατάστασης παρόμοια με αυτήν του Firefox. Με μόνη διαφορά ότι στην περίπτωση του Thunderbird η εγκατάσταση γίνεται χειροκίνητα. Εισάγοντας το όνομα μονάδας και το όνομα αρχείου μονάδας (αρχείο .dll)

Σημείωση: Το αρχείο gclib.dll είναι μία βιβλιοθήκη της Gamplus που περιέχει όλα τα απαραίτητα στοιχεία για την διασύνδεση των Gamsafe Libraries και των smart card με ξένες εφαρμογές όπως επίσης επιτρέπει σε ξένες εφαρμογές να υλοποιούν PKCS#11 κρυπτογραφία. Στην περίπτωση του Mozilla Firefox η χρήση του έγινε αυτόματα με την εκτέλεση του αρχείου Pkcs11_install.html, στην περίπτωση όμως του Thunderbird η διαδικασία αυτή πρέπει να γίνει χειροκίνητα.

Για την εγκατάσταση μιας συσκευής ασφαλείας επιλέγεται το μενού ‘Επιλογές’ στην επιλογή ‘Εργαλεία’ του Mozilla Thunderbird:

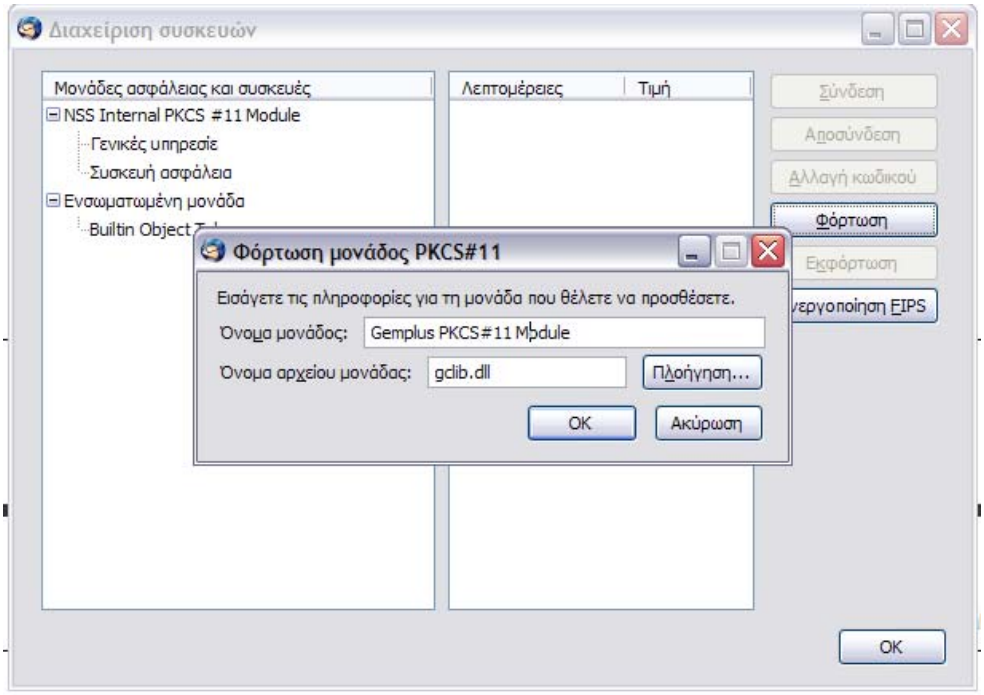


Εικόνα 99. Το εργαλείο Επιλογές του Mozilla Thunderbird

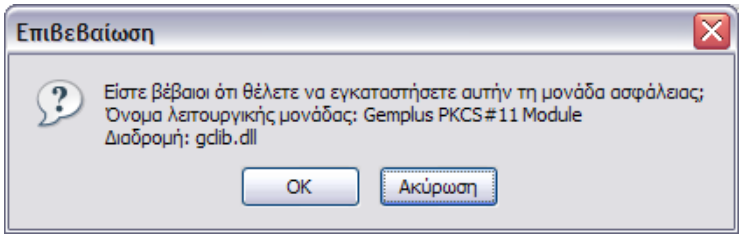


Εικόνα 100. Το παράθυρο επιλογών

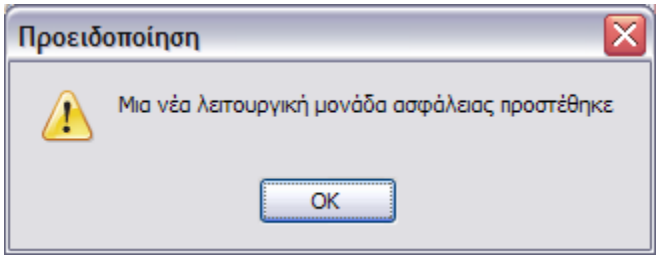
Όπου επιλέγεται το Συσκευές ασφαλείας και εμφανίζεται το παράθυρο της Διαχείρισης συσκευών, οπού είναι όλες οι καταχωρημένες κρυπτογραφικές μονάδες που χρησιμοποιεί ή μπορεί να χρησιμοποιήσει ο Thunderbird. Με την επιλογή Φόρτωση: δίνεται στον χρηστή η δυνατότητα να εισάγει χειροκίνητα μια κρυπτογραφική μονάδα:



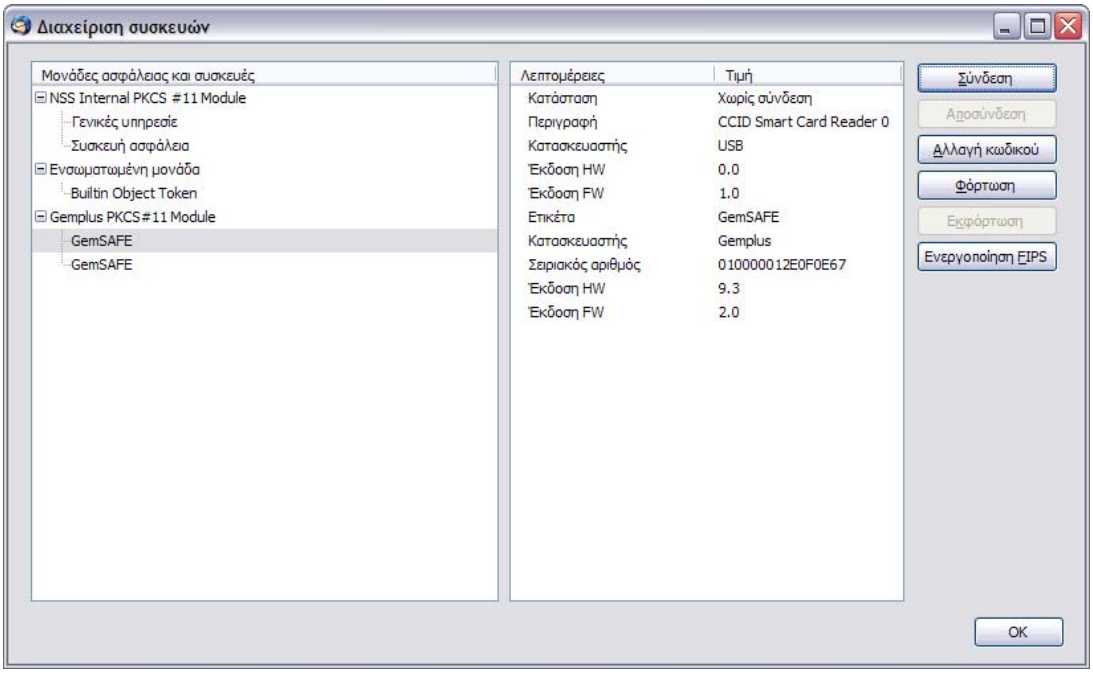
Εικόνα 101. Η φόρτωση της κρυπτογραφικής μονάδας



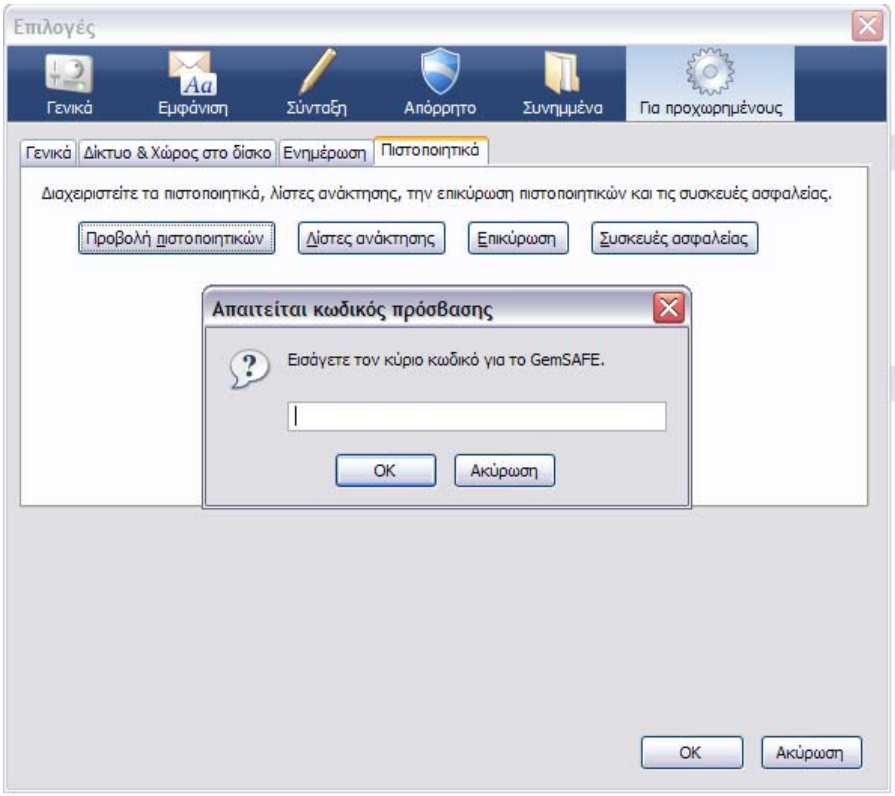
Εικόνα 102. Επιβεβαίωση φόρτωσης της κρυπτογραφικής μονάδας



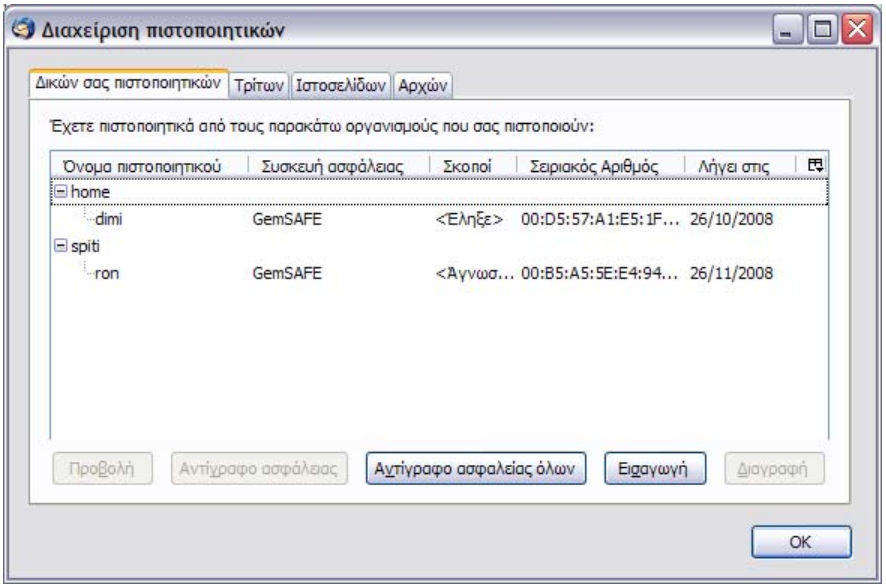
Εικόνα 103. Επιβεβαίωση εγκατάστασης



Εικόνα 104. Το παράθυρο διαχείρισης συσκευών με τις νέες μονάδες

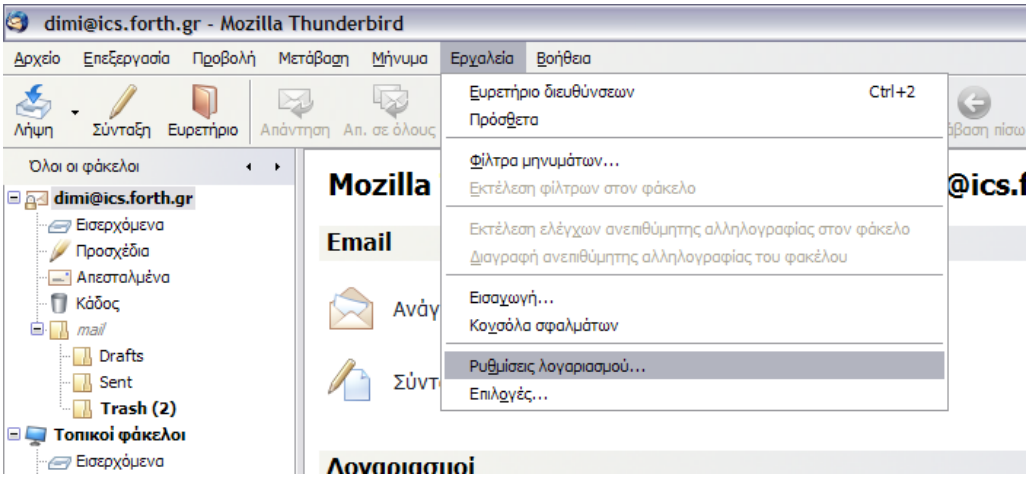


Εικόνα 105. Εισαγωγή κωδικού για να χορηγηθεί η πρόσβαση στα πιστοποιητικά της κάρτας



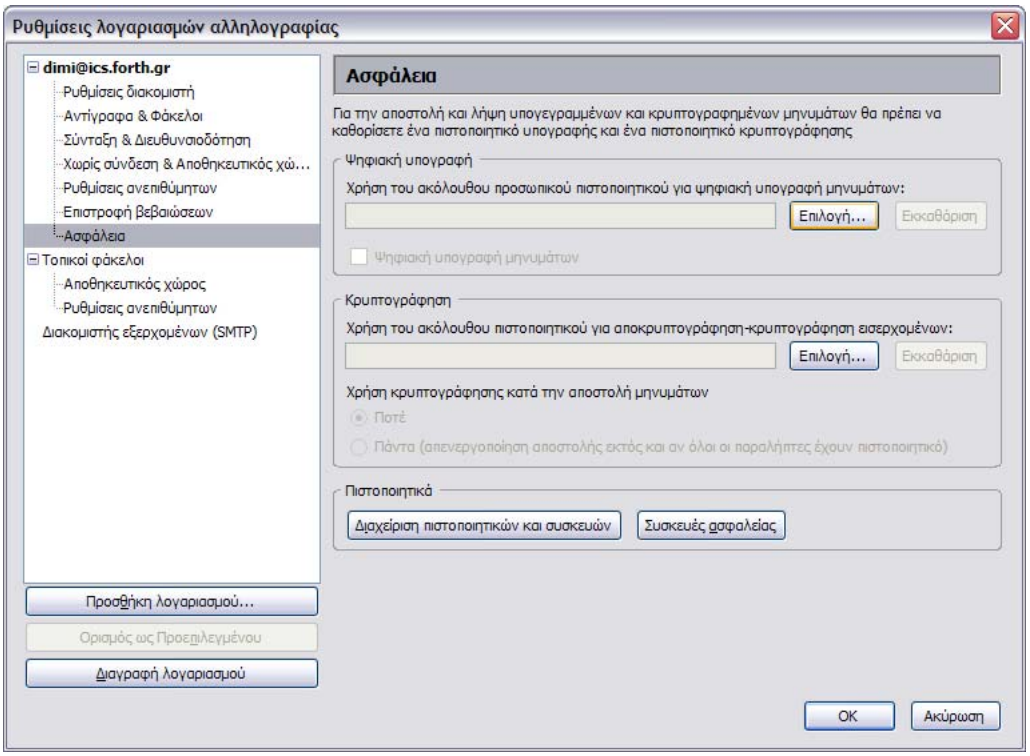
Εικόνα 106. Τα πιστοποιητικά της κάρτας

Για την χρήση των πιστοποιητικών απαιτείται η ρύθμιση του λογαριασμού:

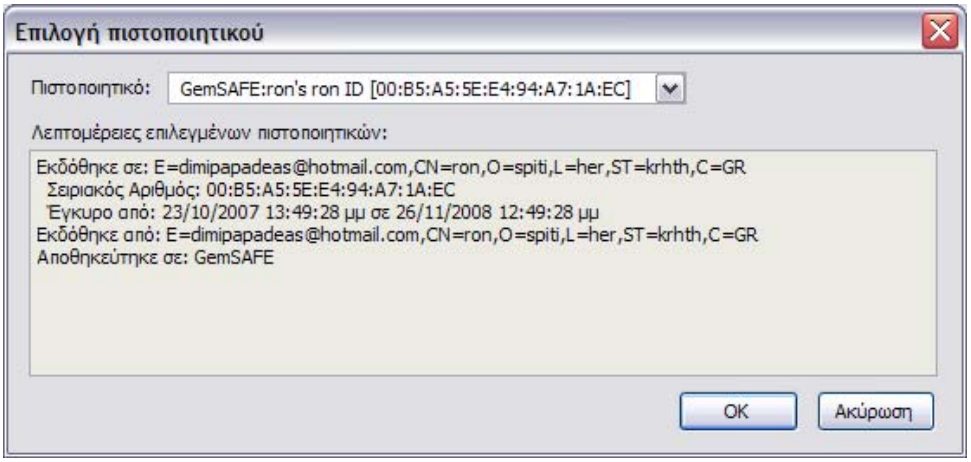


Εικόνα 107. Επιλογή ρύθμισης λογαριασμού

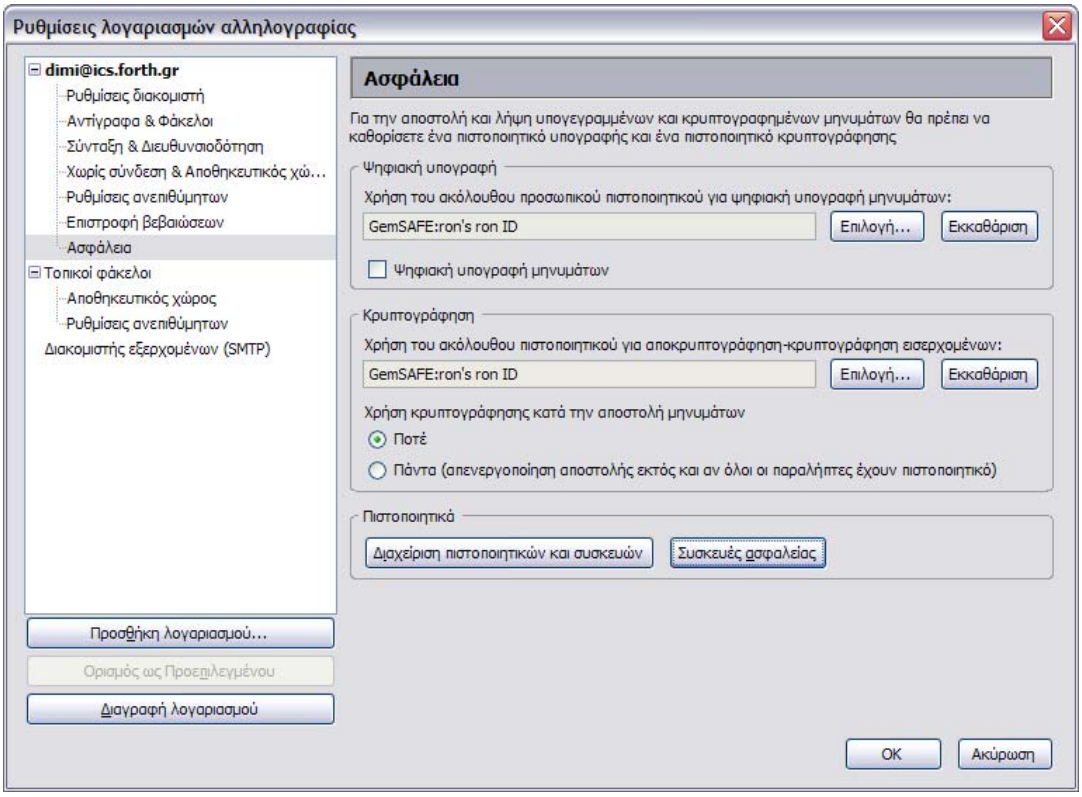
Ανάλογα με τις ανάγκες του, ο χρήστης δύναται να επιλέξει την χρήση των πιστοποιητικών του κάθε λογαριασμού, επιλέγει εάν τα πιστοποιητικά θα χρησιμοποιηθούν μόνο για κρυπτογράφηση ή μόνο για υπογραφή ή και για τα δύο:



Εικόνα 108. Το παράθυρο ρυθμίσεων του λογαριασμού στην κατηγορία της ασφάλειας, όπου επιλέγεται το πεδίο της χρήσης των πιστοποιητικών

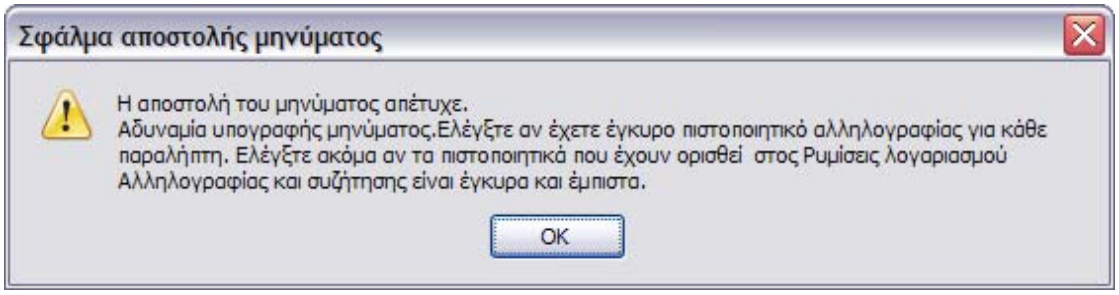


Εικόνα 109. Επιλογή του πιστοποιητικού της κάρτας



Εικόνα 110. Επιλεγμένα πιστοποιητικά

Σημείωση: Για την χρήση των πιστοποιητικών είτε για υπογραφή είτε για κρυπτογράφηση ο Thunderbird απαιτεί να είναι έγκυρα (να μην έχουν λήξει) τα πιστοποιητικά.



Εικόνα 111. Το Μήνυμα απέτυχε να αποσταλεί, διότι το πιστοποιητικό δεν είναι έμπιστο

6.3 Υπογράφοντας Adobe documents

Ψηφιακές υπογραφές

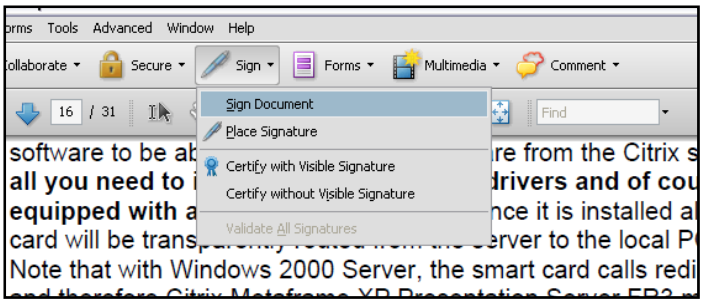
Μία ψηφιακή υπογραφή είναι ένα κομμάτι πληροφορίας που δημιουργείται με την χρήση των δεδομένων του μηνύματος και το private key του χρήστη. Οι ψηφιακές υπογραφές παρέχουν αυθεντικότητα (message authentication), ταυτοποίηση χρήστη και ακεραιότητα. Οι ψηφιακές υπογραφές δημιουργούνται από μαθηματικές ή από *hash* ή από private signing συναρτήσεις. Οι hash συναρτήσεις παράγουν μία σύνοψη του μηνύματος, μια συμπυκνωμένη έκδοση του αυθεντικού αρχείου. Η σύνοψη του μηνύματος κρυπτογραφείται με την χρήση του private key του αποστολέα, μετατρέποντας το σε ψηφιακή υπογραφή. Η ψηφιακή υπογραφή μπορεί να αποκρυπτογραφηθεί μόνο με την χρήση του δημόσιου κλειδιού του αποστολέα. Ο δέκτης του μηνύματος αποκρυπτογραφεί την ψηφιακή υπογραφή και συγκρίνει το αποτέλεσμα της με την *hash* σύνοψη του μηνύματος. Εάν οι δύο συνόψεις είναι ταυτόσημες, τότε το μήνυμα δεν παγιδεύτηκε συνεπώς είναι αυθεντικό.

6.3.1 Παράδειγμα ψηφιακής υπογραφής στο Adobe Acrobat pro

Η δυνατότητα της υπογραφής ενός αρχείου pdf έχει προβλεφθεί και υλοποιηθεί από τους σχεδιαστές των professional εκδόσεων του Adobe Acrobat. Με αποτέλεσμα η υπογραφή ενός αρχείου pdf να είναι μία πολύ απλή διαδικασία ακόμα και όταν υπογράφεται με πιστοποιητικά καταχωρημένα σε μια Smart card.

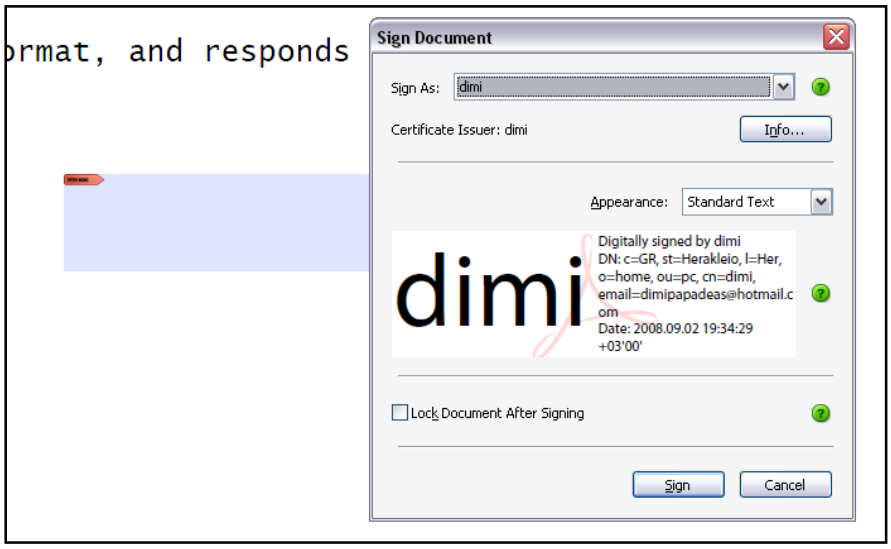
Τα βήματα για μία ψηφιακή υπογραφή είναι τα εξής:

1. Επιλέγεται το αρχείο pdf προς υπογραφή
2. Στην επιλογή Sign στο μενού επιλογών του Adobe Acrobat επιλέγεται το Sign Document



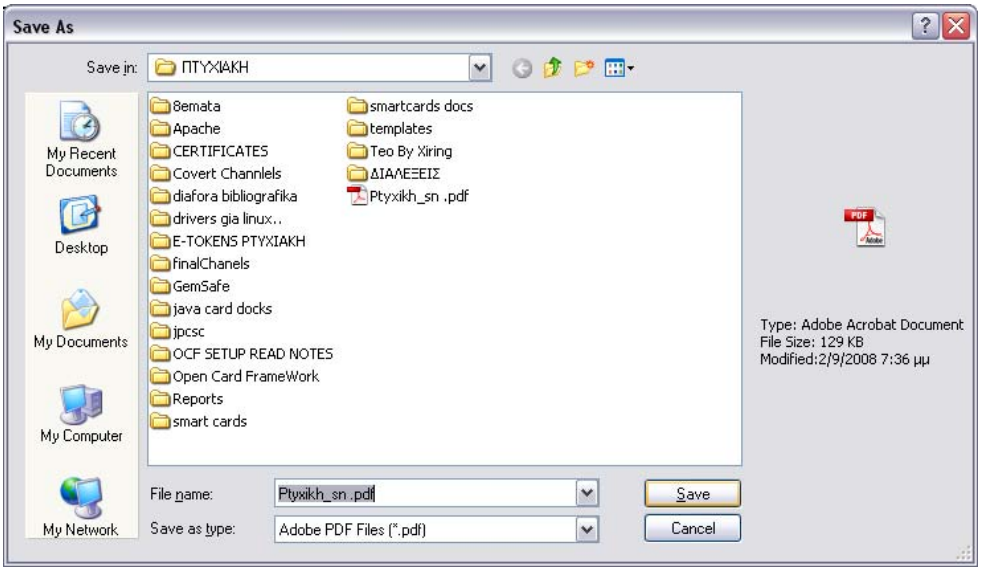
Εικόνα 112. Επιλογή υπογραφής

3. Επιλέγεται με τον κέρσορα μια περιοχή, για να τοποθετηθεί η υπογραφή εκεί
4. Μόλις επιλεχθεί η περιοχή αυτή, εμφανίζεται το μενού υπογραφής, με όλα τα πιστοποιητικά που αναγνωρίζει το λειτουργικό σύστημα, συμπεριλαμβανομένων και των καταχωρημένων πιστοποιητικών της κάρτας, χάρη στο Reg tool που τα έχει καταχωρήσει.



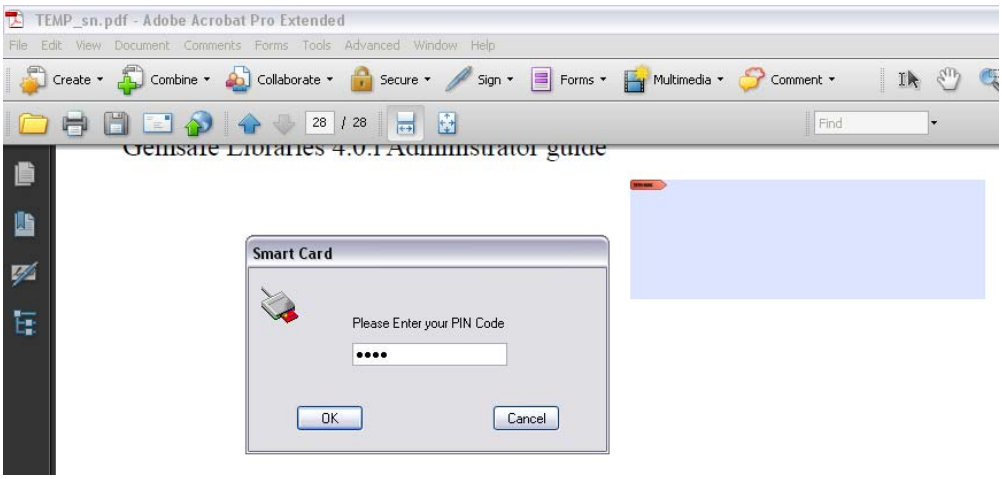
Εικόνα 113. Υπογραφή αρχείου

5. Επιλέγεται ο δημιουργός του πιστοποιητικού και προβάλλονται όλες οι δυνατότητες όπως το κλείδωμα και η δομή εμφάνισης της υπογραφής.
6. Αποθηκεύεται το υπογεγραμμένο αρχείο.



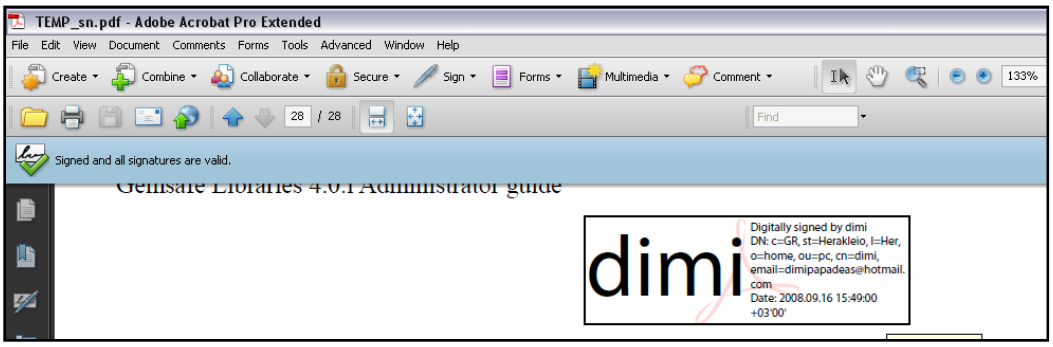
Εικόνα 114. Αποθήκευση υπογεγραμμένου αρχείου

7. Για να εκτελεστεί η αποθήκευση ο χρήστης υποχρεούται να εισάγει το Pin για να μπορέσει να χρησιμοποιήσει το πιστοποιητικό.



Εικόνα 115. Εισαγωγή Pin για την χρήση του πιστοποιητικού

8. Προβολή της υπογραφής :



Εικόνα 116. Επιβεβαίωση υπογραφής

9. Τέλος με κλίκ πάνω στην υπογραφή προβάλλεται και επιβεβαιώνεται η υπογραφή και η εγκυρότητα του πιστοποιητικού.

7. Περιγραφή εφαρμογής διαχείρισης καρτών

Η εφαρμογή Card Manager, είναι μία μικρή εφαρμογή ελέγχου πρόσβασης σε μια βάση δεδομένων, παραλληλίζοντας την χρήση της κάρτας με την απλή εισαγωγή όνομα χρήστη και κωδικού πρόσβασης. Η εφαρμογή εκμεταλλεύεται ελάχιστες από τις δυνατότητες ασφαλείας των smart card. Ο κύριος σκοπός της ανάπτυξης της εφαρμογής ήταν μια προσπάθεια εξοικείωσης με το προγραμματιστικό περιβάλλον στα πλαίσια της ανάπτυξης ασφαλών εφαρμογών με smartcard. Η υλοποίηση γίνε σε γλώσσα java στην πλατφόρμα NetBeans. Με την βοήθεια του API της java (v1.6) javax.smartcardio* .

7.1 Java™ Smart Card I/O API

Το Java Smart Card I/O API καθορίζεται από το πρότυπο JSR 268[25]. Το API είναι ένα Java API για επικοινωνία με Smart Cards χρησιμοποιώντας το πρότυπο ISO/IEC 7816-4 APDUs. Επιτρέποντας σε Java εφαρμογές να αλληλεπιδρούν με τις εφαρμογές που τρέχουν στις Smart Card, να αποθηκεύουν και να εξάγουν δεδομένα από τις smart cards.

7.2 Use cases

- ✓ Ανάγνωση Smart Card
- ✓ Έλεγχος κάρτας
- ✓ Ταυτοποίηση χρήστη και κάρτας
- ✓ Σύνδεση με βάση δεδομένων (java DB Derby)
- ✓ Αλληλεπίδραση με βάση δεδομένων (read, insert, update, delete)
- ✓ Καταχώρηση νέου χρηστή κάρτας (Cardholder[26])
- ✓ Υποτυπώδης διαχειριστής γεγονότων εισαγωγής και εξαγωγής Smart Card
- ✓ Αναγνώριση συνδεδεμένων Card reader
- ✓ Εναλλαγή default smart card reader

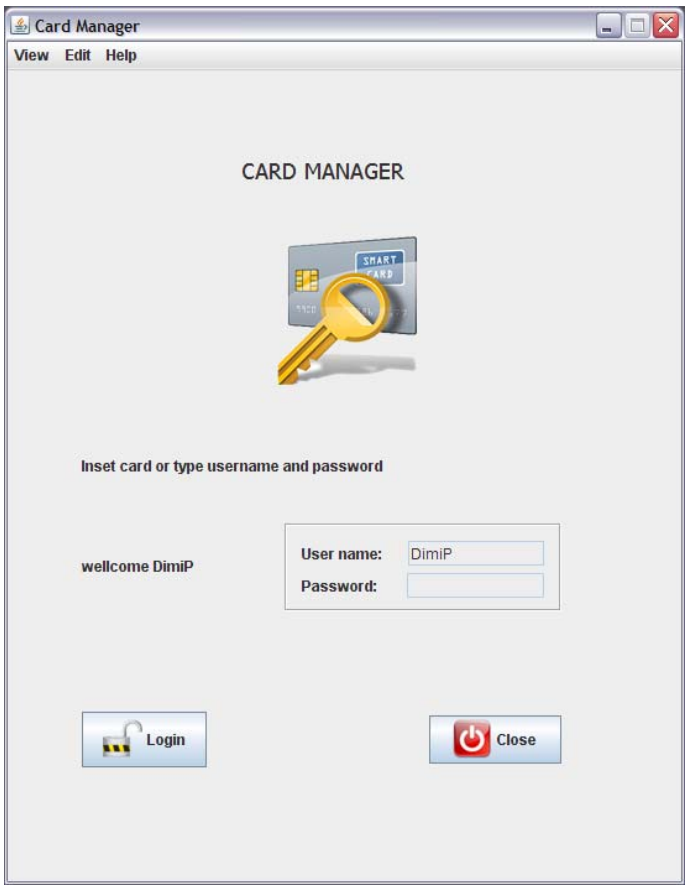
[25] http://jcp.org/en/jsr/detail?id=268

[26] Βλ. Παράρτημα

7.3 Προεπισκόπηση του Card manager

7.3.1 Access Control

Στο αρχικό μενού ο χρήστης έχει την δυνατότητα να εισέλθει (log in) στο σύστημα είτε με την χρήση της κάρτας είτε με την χρήση του κωδικού πρόσβασης. Για να είναι εφικτές αυτές οι δυνατότητες, πρέπει ο χρήστης να είναι κατοχυρωμένος στην βάση δεδομένων. Στην περίπτωση που δεν είναι κατοχυρωμένος ούτε ο χρήστης και συνεπώς ούτε η κάρτα του, υπάρχει η δυνατότητα να συνδεθεί κάποιος άλλος κατοχυρωμένος χρήστης είτε με τον κωδικό του είτε με την κάρτα του, και να καταχωρήσει τον καινούριο χρήστη και την κάρτα του. Γίνεται να καταχωρηθεί χρήστης χωρίς κάρτα αλλά όχι το αντίστροφο.



Εικόνα 117. Το αρχικό μενού με ταυτοποίηση χρήστη με μέσω της κάρτας.

Εικόνα 118. Το αρχικό μενού με άγνωστη κάρτα στον card reader, για να κατοχυρωθεί, πρέπει να εισαχθεί το username και τπ password ενός κατοχυρωμένου χρήστη.

Εικόνα 119. Το αρχικό μενού χωρίς κάρτα, για να γίνει το login πρέπει να εισαχθεί ή μια κατοχυρωμένη κάρτα είτε το username και τπ password ενός κατοχυρωμένου χρήστη.

7.3.2 Το κεντρικό μενού

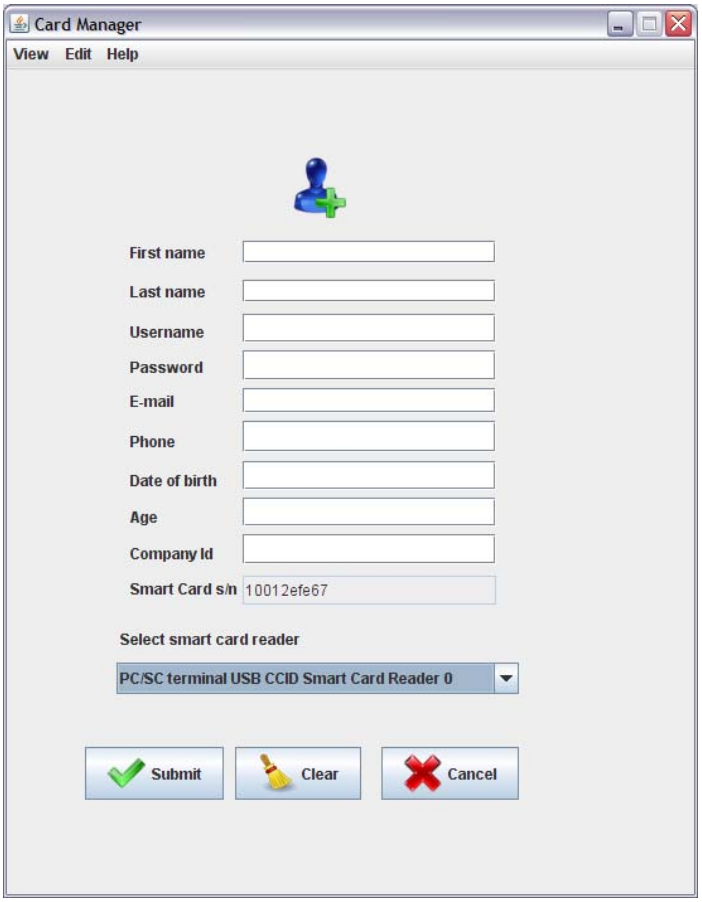
Στο κεντρικό μενού μπορεί να βρεθεί ο χρήστης μετά από μια επιτυχή ταυτοποίηση χρήστη, και την επιτυχή σύνδεση με την βάση δεδομένων. Από αυτό το μενού ο χρήστης μπορεί να πλοηγηθεί σε όλα τα υπό-μενού ενώ ενημερώνεται για τις στοιχειώδες πληροφορίες κατάστασης του συστήματος όπως τα ονόματα του ταυτοποιημένου και συνδεδεμένου χρήστη και της βάσης δεδομένων με την οποία έχει συνδεθεί το σύστημα.

Εικόνα 120. Το κεντρικό μενού με ταυτοποιημένο χρήστη

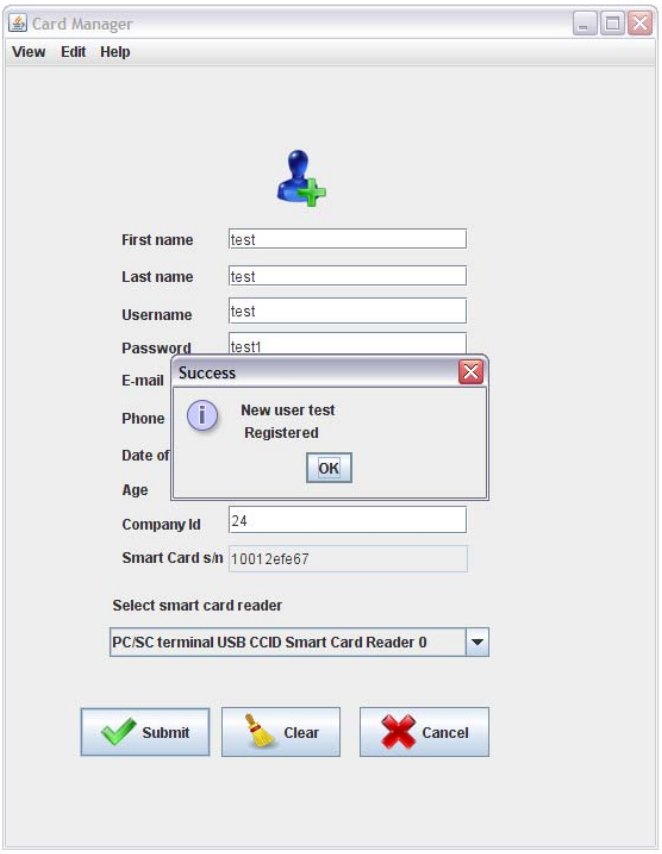
7.3.3 Το μενού καταχώρησης νέου χρήστη

Με την επιλογή 'New Cardholder' ένας κατοχυρωμένος, εγγεγραμμένος στην βάση δεδομένων, χρήστης έχει την δυνατότητα να κατοχυρώσει ένα νέο χρήστη με την

κάρτα του ή χωρίς. Κατά την εντολή καταχώρησης (Submit) γίνεται έλεγχος για κάθε παράληψη εισαγωγής κάποιου πεδίου, όπως επίσης και ο έλεγχος για την πιθανή εισαγωγή στοιχείων στα πεδία – κλειδιά με τιμή που ήδη είναι κατοχυρωμένη. Τα πεδία- κλειδιά πρέπει να έχουν μοναδικές τιμές. Τα πεδία αυτά είναι το username και το Company Id. Τέλος σε περίπτωση που ο χρηστής δεν διαθέτει κάρτα το πεδίο Card s/n στο οποίο βρίσκεται αυτόματα ο σειριακός αριθμός της κάρτας δεν καταχωρείται.



Εικόνα 121. Το μενού καταχώρησης νέου χρήστη στην βάση δεδομένων

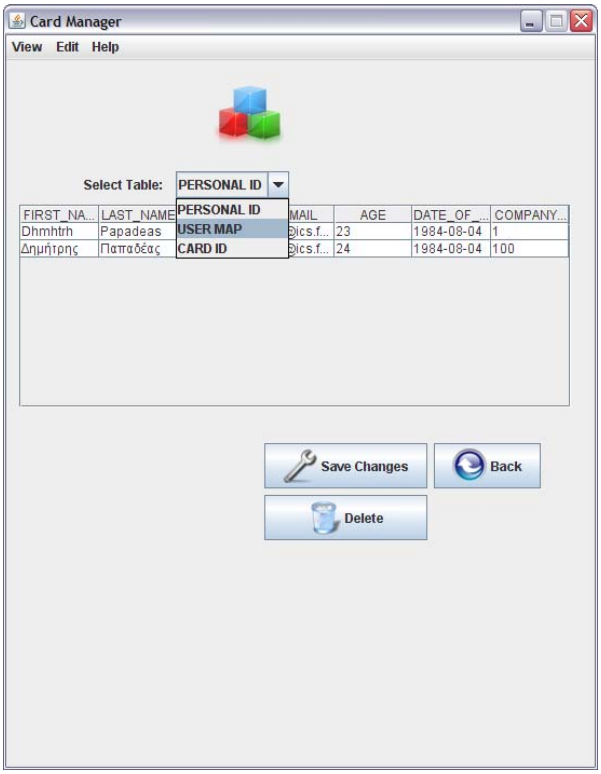


Εικόνα 122. Επιτυχής καταχώρηση του χρήστη test

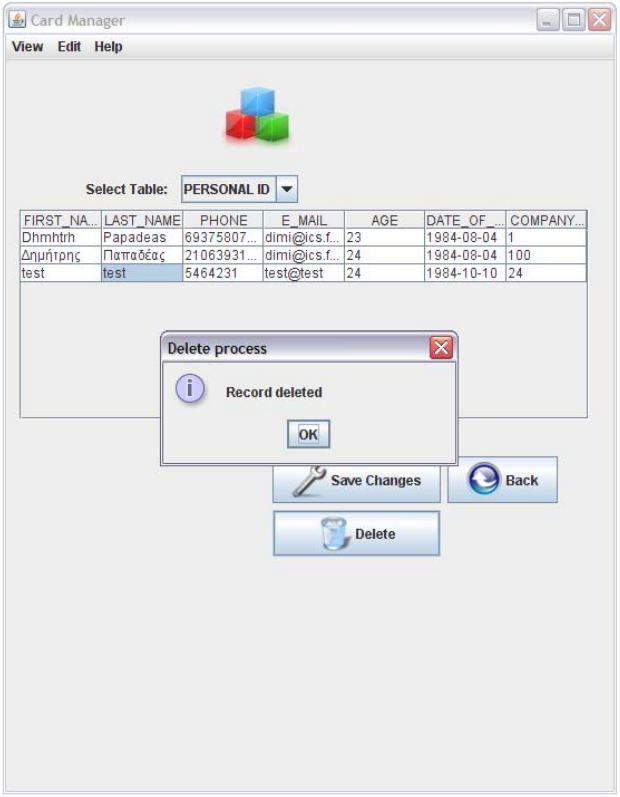
7.3.4 Η βάση δεδομένων

Η βάση δεδομένων αποτελείται από τρεις πινάκες τον PERSONAL ID, USER MAP και CARD ID. Ο PERSONAL ID περιέχει διαφορά προσωπικά στοιχεία του χρήστη, ο USER MAP είναι λειτουργικός πίνακας που συνδέει τους χρήστες με τα username τους και τέλος ο CARD ID , περιέχει τους κωδικούς και τους σειριακούς αριθμούς των καρτών. Η βάση δεδομένων είναι πλήρως υλοποιημένη στο σύστημα και οι χρήστες έχουν δυνατότητες τροποποίησης της ανάλογα με τις επιθυμίες τους.

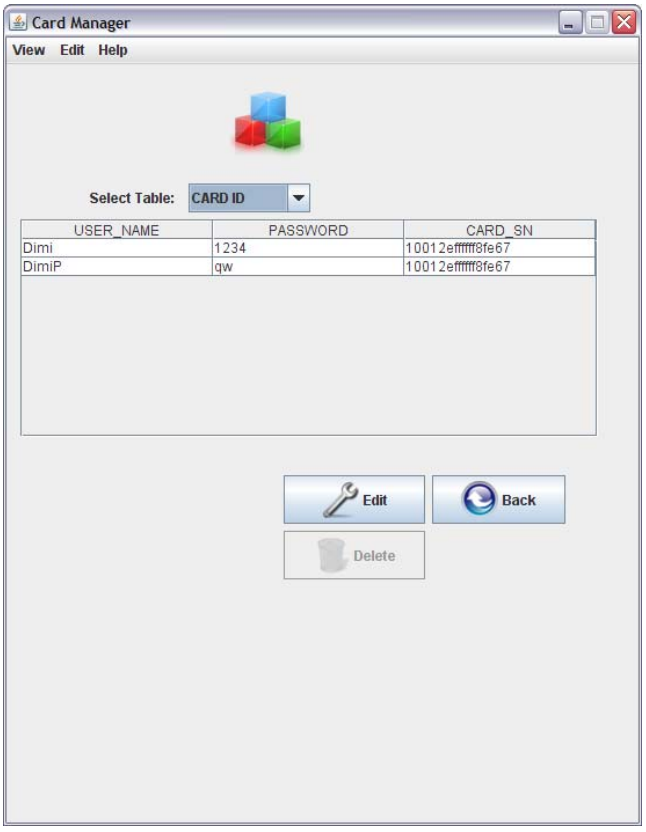
Σημείωση: Κανονικά θα έπρεπε το πεδίο card serial number (CARD_SN) να είναι primary key στον πίνακα CARD ID, για δική μας διευκόλυνση λόγο του περιορισμένου αριθμού καρτών σχεδιάστηκε να μην είναι private key το CARD_SN αλλά το USER_NAME , έτσι ώστε να έχουμε την δυνατότητα να καταχωρήσουμε πολλές εγγραφές.



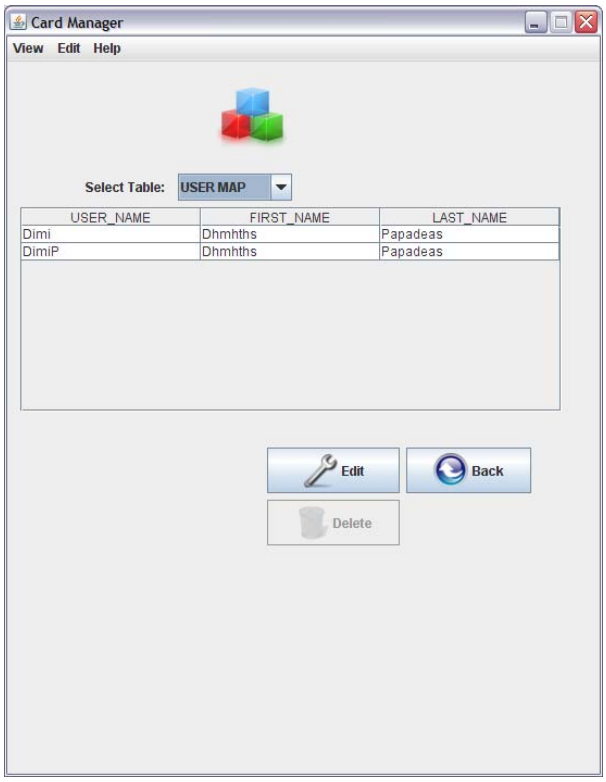
Εικόνα 123. Η επιλογή πίνακα της βάσης δεδομένων



Εικόνα 124. Επιτυχής διαγραφή εγγραφής



Εικόνα 125. Το πεδίο που αποθηκεύονται τα στοιχεία της κάρτας

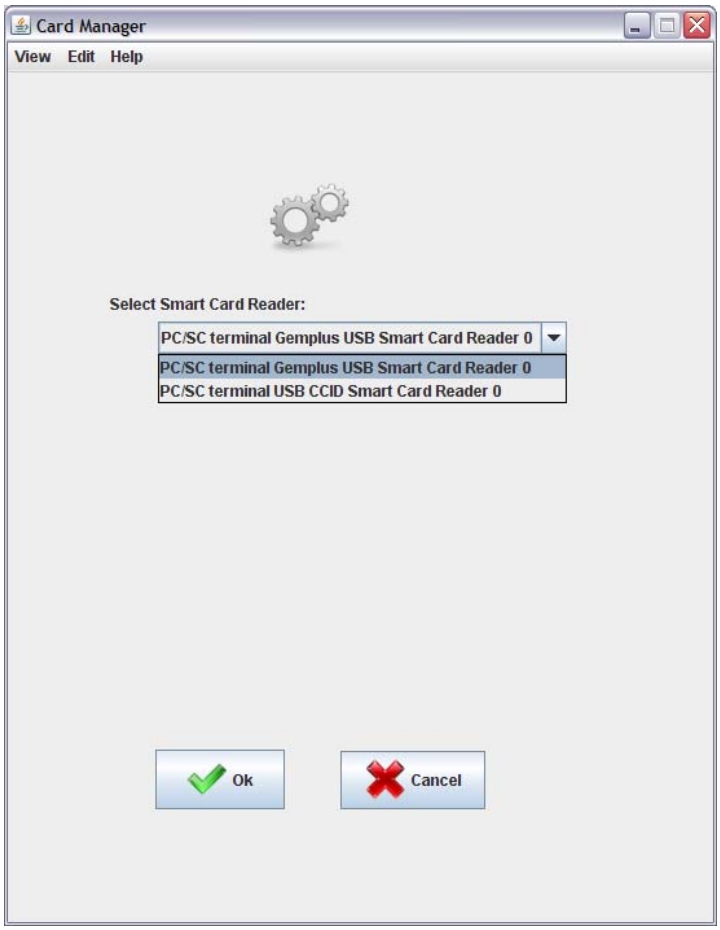


Εικόνα 126. Το πεδίο διασύνδεσης των χρηστών της βάσης δεδομένων με τις κάρτες

7.3.5 Το μενού επιλογών

Ο χρήστης μπορεί να επιλέξει δυναμικά τον default card reader ο οποίος είναι ο reader με τον οποίο επικοινωνεί το σύστημα. Το πρόγραμμα αυτόματα αναγνωρίζει όλους τους συνδεδεμένους card reader και θέτει ως default τον 1^{ο} που θα διαβάσει. Η δυνατότητα αλλαγής (switch) του default card reader, προσφέρει την ευελιξία καταχώρησης στην βάση διαφορετικών χρηστών με διαφορετικές κάρτες. Αυτό μπορεί να γίνει με 2 τρόπους.

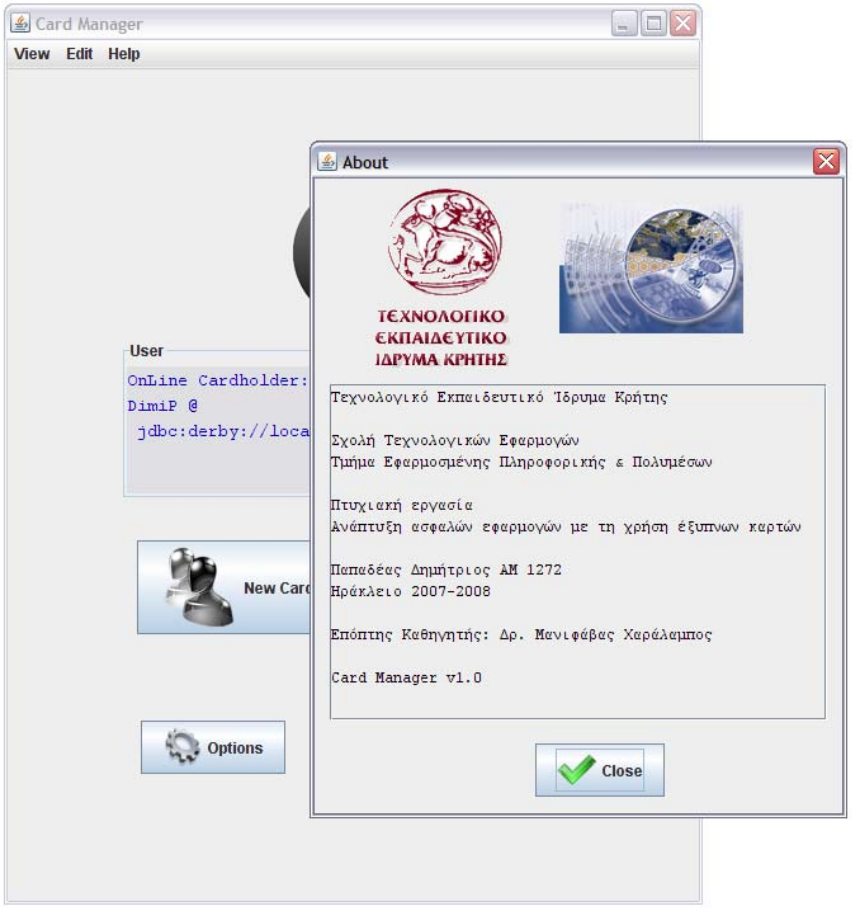
- Περίπτωση 1) Με πολλούς card reader:
  Σε αυτήν την περίπτωση ο διαχειριστής (ένας registered Cardholder) απλά συνδέεται από τον 1^{ο} reader και απλά κάνοντας switch στους άλλους card readers, διαβάζει την κάρτα του κάθε reader και καταχωρώντας τους αντίστοιχους νέους χρήστες.
- Περίπτωση 2) Με έναν card reader
  Σε αυτήν την περίπτωση ο διαχειριστής αφαιρεί την κάρτα του από τον card reader και εισάγει τη νέα κάρτα προς εγγραφή, αυτή η διαδικασία λειτουργεί υπό το authenticated session του διαχειριστή, του ατόμου που έκανε login και ξεκίνησε την διαδικασία εγγραφής



Εικόνα 127. Η προβολή των Smart card reader που είναι συνδεδεμένοι με τον σταθμό εργασίας και η επιλογή του default reader

7.3.6 Το μενού πληροφοριών

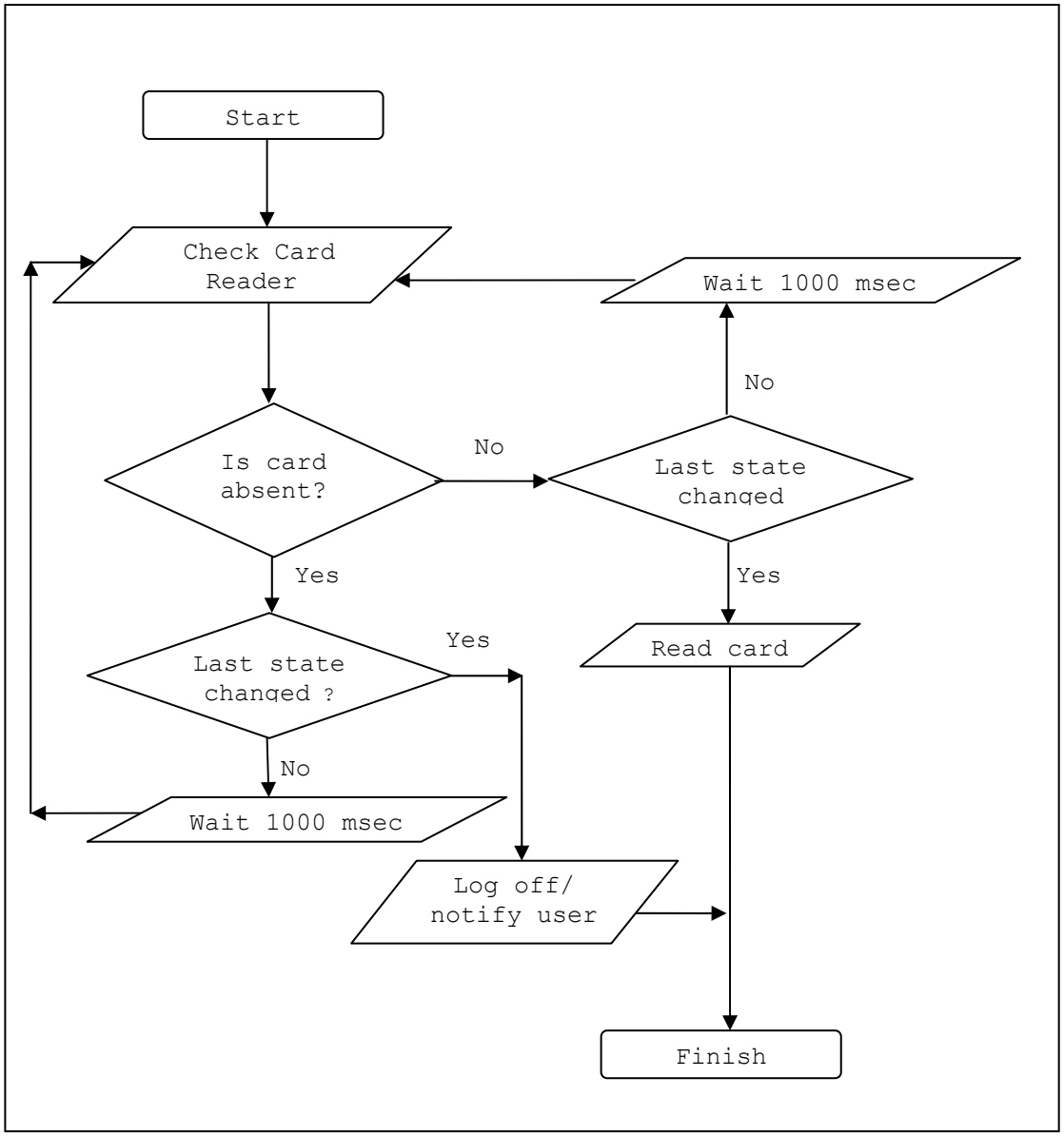
Το μενού πληροφοριών της εφαρμογής, που περιέχει διάφορα στοιχεία για τον κατασκευαστή και τους κατόχους των πνευματικών δικαιωμάτων της εφαρμογής.



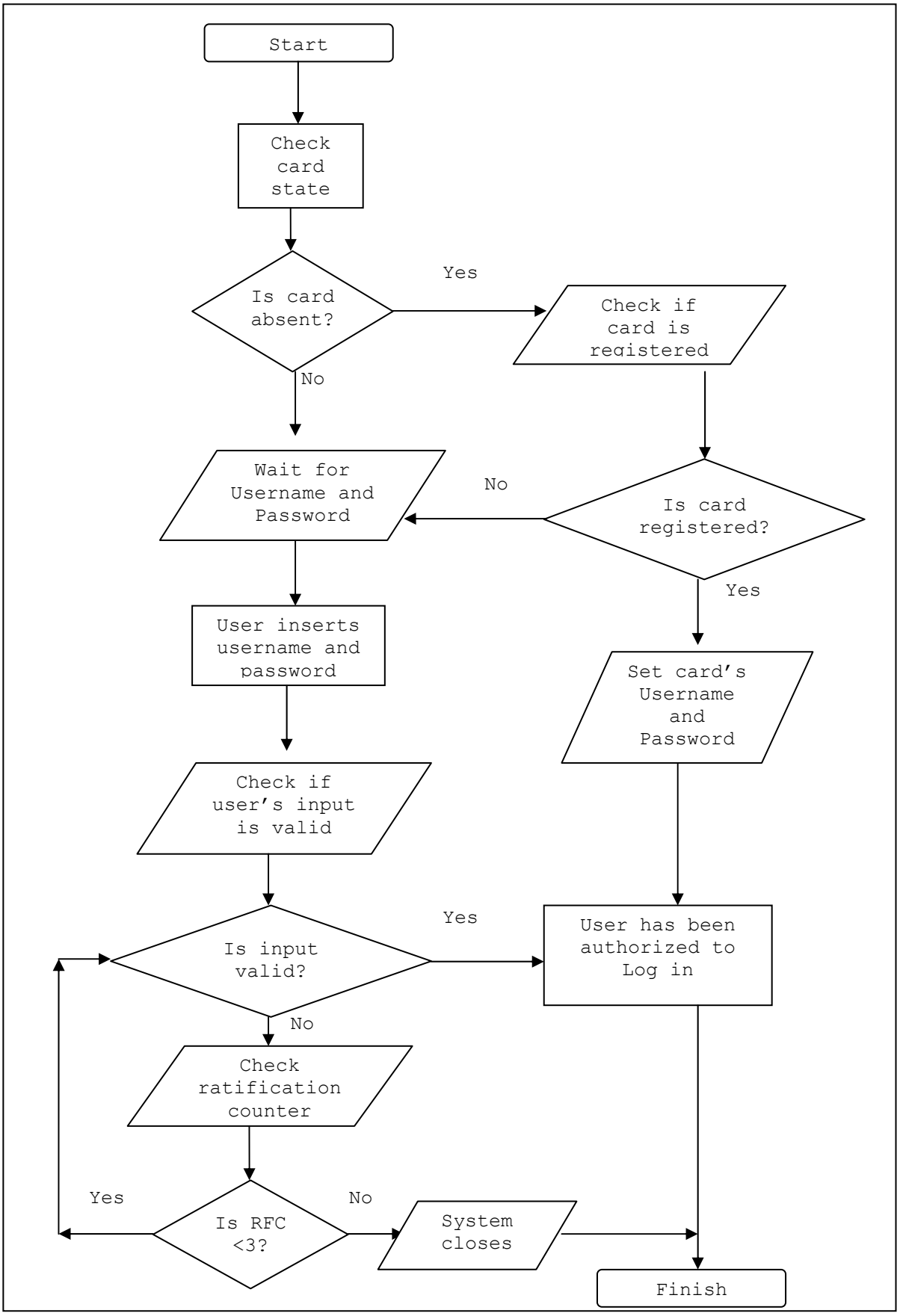
Εικόνα 128. Το μενού πληροφοριών

7.4 Flow Charts

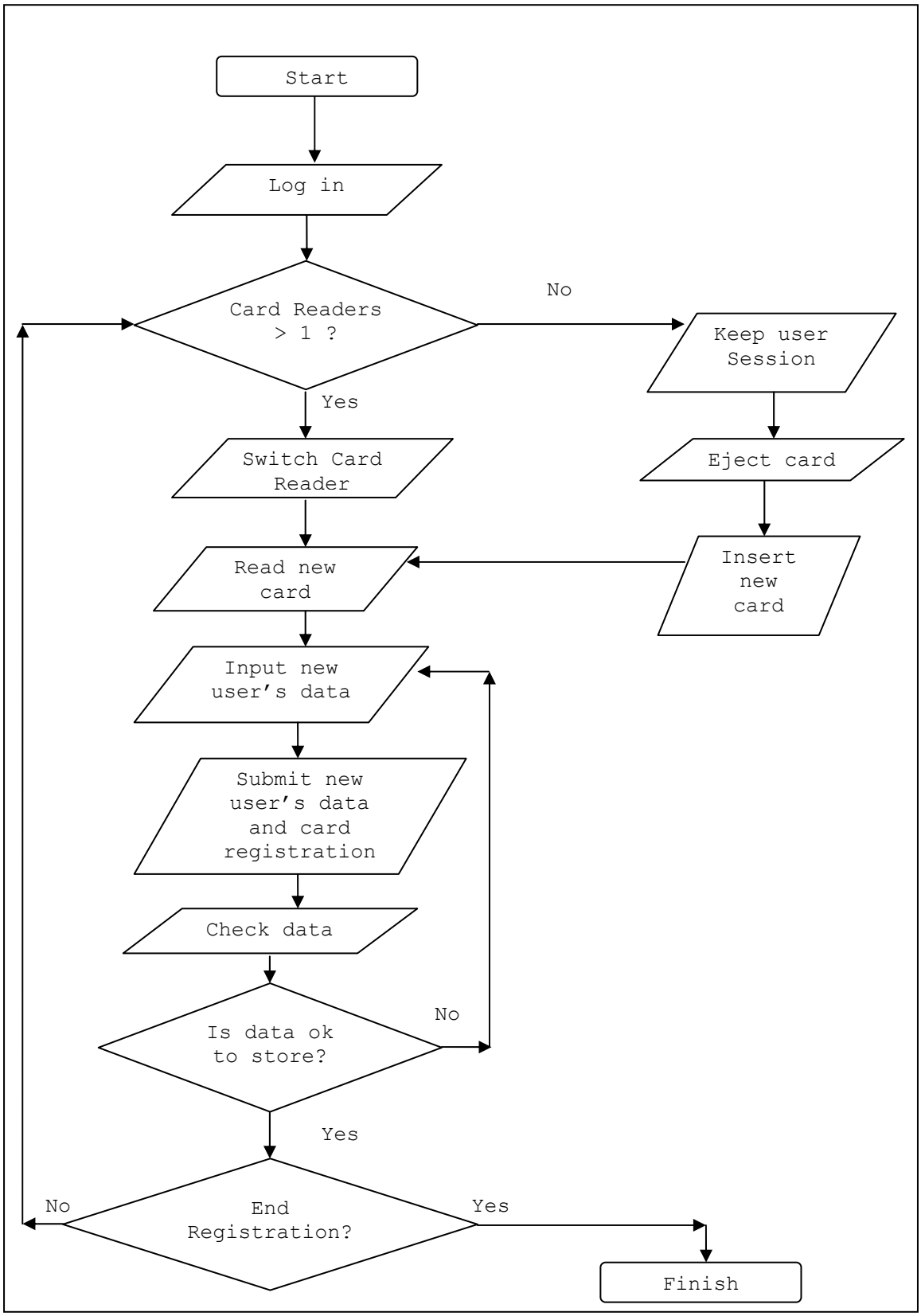
7.4.1 Card absence validation Thread



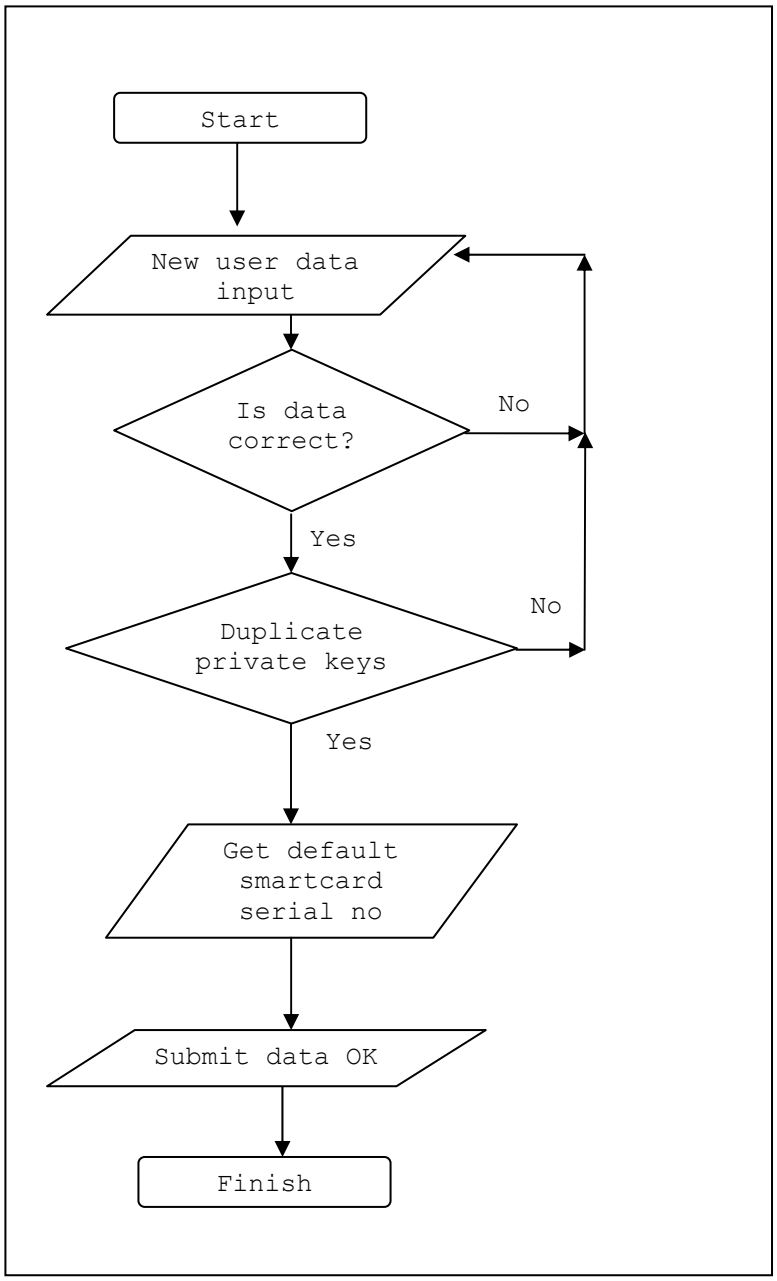
7.4.2 Log in flow chart



7.4.3 New User Registration



7.4.4 New User's Data Validation



8. Συμπεράσματα

Τελειώνοντας αυτή τη μελέτη μπορούμε να αναφερθούμε σε κάποια βασικά συμπεράσματα που προέκυψαν. Οι smart cards, είναι ένα εργαλείο υποστήριξης – αναβάθμισης ενός ευρύτερου συστήματος ασφαλείας είτε αυτό είναι τραπεζικό είτε σταθμός εργασίας είτε δίκτυο υπολογιστών. Το βέβαιο είναι ότι οι smart cards είναι αρκετά ασφαλείς και εκ φύσεως ενδυναμώνουν και την ασφάλεια του συστήματος που τις υιοθετεί. Σε αντίδραση στην αρχή του ότι "Κάθε σύστημα ασφαλείας είναι τόσο ασφαλές όσο ο πιο αδύναμος κρίκος του. (Συνήθως ο αδύνατος κρίκος είναι ο άνθρωπος)", οι smartcards δρουν με την φιλοσοφία του περιορισμού του σφάλματος του αδύνατου κρίκου, στην ουσία ενδυναμώνουν τον αδύναμο κρίκο. Αλλά σε καμία περίπτωση δεν θα μπορούσε να ισχύσει το ότι με την ενσωμάτωση των έξυπνων καρτών ένα σύστημα είναι 100% ασφαλές. Η ενσωμάτωση των έξυπνων καρτών σε ένα σύστημα δεν πρέπει να εστιάζεται στο κομμάτι της εφαρμογής και της υλοποίησης στο σύστημα, αλλά πρέπει να αντιμετωπίζει το σύστημα ως μία ξεχωριστή οντότητα, να ενσωματώνεται ως μία αλληλένδετη δομή του συστήματος, που επηρεάζει και να επηρεάζεται από κάθε παράμετρο του συστήματος.

Η σύγκριση με τις μαγνητικές κάρτες είναι περιττή, το επίπεδο δυνατοτήτων των μαγνητικών καρτών είναι πρωτόγονο σε σχέση με το επίπεδο των έξυπνων καρτών. Και όσον αφορά τα τραπεζικά συστήματα ασφαλείας σε καθολική μετάβαση σε χρήση των έξυπνων καρτών το κέρδος θα ήταν ανυπολόγιστο, πόσο μάλλον στην περίπτωση που θα υπήρχε πραγματικό ενδιαφέρον από τις τράπεζες για συνεισφορά σε περεταίρω έρευνα και ανάπτυξη των καρτών και των προτύπων τους.

- Οι αναγνώστες έξυπνων καρτών:
  Είναι αρκετά εξελιγμένοι οι σύγχρονοι card reader και η τιμή τους έχει μειωθεί αισθητά και είναι πλέον προσιτή.
- Μια εμπορική εφαρμογή:
  Οι GamSafe libraries αποτελούν μια ολοκληρωμένη εφαρμογή που καλύπτει πλήρως το πεδίο της διαχείρισης των έξυπνων καρτών.
- Οι 3^{ες} εφαρμογές:
  Η χρήση των καρτών από τρίτες εφαρμογές αποτελεί μια διαδικασία ιδιαίτερα ασφαλή και εύκολη.
- Η ανάπτυξη μίας εφαρμογής:
  Όσο αφορά το προγραμματιστικό περιβάλλον των έξυπνων καρτών, κυρίως λόγο της πολυπλοκότητας των προτύπων, η ανάπτυξη μίας εφαρμογής ή ο προγραμματισμός μίας κάρτας αποτελούν δύσκολα έργα για μικρές ομάδες ανάπτυξης. Αντιθέτως η χρήση από τον τελικό χρήστη (cardholder) μπορεί να είναι πολύ απλή και εύκολη, συναρτήσει πάντα με τις διαδικασίες που εκτελεί ο χρήστης. Αλλά συνήθως οι συναλλαγές και ο έλεγχος ταυτότητας είναι πολύ απλές διαδικασίες λόγω του ότι συνηθίζεται στα συστήματα έξυπνων καρτών να κρύβεται η πολυπλοκότητα από τον τελικό χρήστη.

Παράρτημα Ι

AES

Advanced Encryption Standard (AES), γνωστή και ως Rijndael. Ένα μπλοκ κρυπτογράφησης που έχει εγκριθεί ως ένα πρότυπο κρυπτογράφησης από την κυβέρνηση των ΗΠΑ.

Application programming interface (API)

Μία διασύνδεση πηγαίου κώδικα σε ένα σύστημα ηλεκτρονικού υπολογιστή ή σε μια βιβλιοθήκη προγραμμάτων, που παρέχεται προκειμένου να υποστηρίξει τα αιτήματα για τις υπηρεσίες που πρέπει να γίνουν από άλλα προγράμματα ηλεκτρονικών υπολογιστών, και / ή να καταστεί δυνατή η ανταλλαγή δεδομένων.

CA Certificate Authority

Είναι ένα νομικό πρόσωπο με την δικαιοδοσία και τις μεθόδους που να πιστοποιεί την ταυτότητα του ενός ή περισσοτέρων μερών σε μια ανταλλαγή (μία βασική λειτουργία σε κρυπτογραφικά συστήματα δημόσιου κλειδιού).

CCID

Η USB CCID (Chip / Smart Card Interface Devices) προδιαγραφή, ορίζει ένα πρότυπο πρωτόκολλο επικοινωνίας μεταξύ PC / SC smart card reader και υπολογιστή μέσω USB, επιτρέποντας με τον ίδιο οδηγό (device driver) να επικοινωνεί οποιοσδήποτε smart card reader που συμμορφώνεται με την προδιαγραφή CCID. Η επικοινωνιακή προσέγγιση αυτή του smartcard reader φέρνει μια απλοποιημένη Plug and Play εμπειρία στους χρήστες.

Card management system (CMS)

Το CMS είναι η διαχείριση ψηφιακής πιστοποίησης μίας έξυπνης κάρτα ή ενός token, λύση που χρησιμοποιείται για έκδοση, διαχείριση, διαμόρφωση και υποστήριξη και κρυπτογράφηση πιστοποιητικών PKI για εφαρμογές ταυτοποίησης σε έναν οργανισμό.

Card reader

Κάθε συσκευή που διαβάζει κωδικοποιημένες πληροφορίες από μια κάρτα, ένα token ή άλλη συσκευή ταυτοποίησης και επικοινωνεί με έναν κεντρικό υπολογιστή, όπως ένα πίνακα ελέγχου / επεξεργασίας δεδομένων ή για περαιτέρω ενέργειες.

Card serial number

Ένα αναγνωριστικό που είναι εγγυημένο ότι είναι μοναδικό μεταξύ όλων των αναγνωριστικών στοιχείων που χρησιμοποιούνται για ένα συγκεκριμένο σκοπό. Στις smartcards είναι συνήθως ένας μεγάλος δεκαεξαδικός σειριακός αριθμός.

Cardholder

Ένα φυσικό πρόσωπο στο οποίο έχει χορηγηθεί ή ανατεθεί μια κάρτα η οποία είναι υπό την κατοχή του. Η κάρτα πρέπει να έχει καταχωρηθεί σε κάποιο σύστημα με την ταυτότητα του κατόχου της έτσι ώστε να αντιστοιχίζεται ο κάτοχος με την κάρτα. Η αντιστοίχιση αυτή μπορεί να γίνεται ποικιλότροπος, ακόμα και μέσα στην κάρτα.

Challenge-Handshake Authentication Protocol (CHAP)

Το CHAP πιστοποιεί ένα χρήστη ή host δικτύου σε μια οντότητα πιστοποίησης που μπορεί να είναι πχ. ένας πάροχος πρόσβασης στο ιντερνέτ (ISP). Το πρωτόκολλο προσδιορίζεται από το RFC 1994: PPP Challenge Handshake Authentication Protocol (CHAP). Το CHAP είναι ένα scheme αυθεντικοποίησης που χρησιμοποιείται από Point to Point Protocol (PPP) servers για να πιστοποιήσει την ταυτότητα τον απομακρυσμένων χρηστών. Το CHAP περιοδικά επιβεβαιώνει την ταυτότητα του πελάτη με τη χρήση χειραψίας τριών δρόμων (three-way handshake). Αυτό πραγματοποιείται κατά τη διάρκεια εγκατάστασης της αρχικής σύνδεσης , και μπορεί πραγματοποιηθεί πάλι οποιαδήποτε άλλη στιγμή στο μέλλον. Η επιβεβαίωση βασίζεται σε ένα κοινό μυστικό (όπως για παράδειγμα ο κωδικός πρόσβασης του χρήστη).

1. έπειτα από την ολοκλήρωση της φάσης εγκαθίδρυσης σύνδεσης link establishment phase, ο authenticator αποστέλλει ένα "challenge" μήνυμα στον αποδέκτη (άλλο άκρο) peer.
2. Ο peer απαντά με μία τιμή που υπολογίζεται από μία one-way hash function, όπως το MD5 checksum hash.
3. Ο authenticator ελέγχει την απάντηση μέσω του δικού του υπολογισμού της αναμενόμενης τιμής hash. Αν οι τιμές ταιριάζουν, ο authenticator αναγνωρίζει την πιστοποίηση , αλλιώς τερματίζει τη σύνδεση.
4. κατά τυχαία χρονικά διαστήματα ο authenticator αποστέλλει νέο challenge στο peer και επαναλαμβάνει τα βήματα 1 έως 3.

Το πρωτόκολλο CHAP παρέχει προστασία εναντία σε επιθέσεις playback attack από το peer μέσω της χρήσης ενός incrementally changing identifier και μιας μεταβλητής challenge-value. Επίσης απαιτείται και ο πελάτης και ο server να γνωρίζουν το κείμενο του μυστικού παρ' όλο που δεν αποστέλλεται ποτέ μέσω δικτύου.

Checksum

Το άθροισμα ελέγχου, είναι υπολογιζόμενη τιμή που εξαρτάται από το περιεχόμενο ενός μηνύματος. Το άθροισμα ελέγχου μεταδίδεται με το μήνυμα. Το άλλο μέρος (ο αποδέκτης) μπορεί τότε να επαναϋπολογίσει το άθροισμα ελέγχου για την επαλήθευση ότι το μήνυμα δεν τροποποιήθηκε κατά τη διάρκεια της μετάδοσης του.

Chip

Ολοκληρωμένο κύκλωμα, ηλεκτρονικό εξάρτημα που εκτελεί την λογική, την επεξεργασία ή / και λειτουργίες της μνήμης. Chip είναι ένα ολοκληρωμένο κύκλωμα (επίσης γνωστό ως IC, μικροεπεξεργαστή, μικροτσίπ, τσιπ πυριτίου, ή τσιπ) είναι ένα

ηλεκτρονικό κύκλωμα μινιατούρα (που αποτελείται κυρίως από διατάξεις ημιαγωγών, καθώς και παθητικά στοιχεία) που έχει παραχθεί στην επιφάνεια από ένα λεπτό υπόστρωμα του ημι-αγώγιμου υλικού. Τα ολοκληρωμένα κυκλώματα χρησιμοποιούνται σε όλες σχεδόν τις ηλεκτρονικές συσκευές που χρησιμοποιούνται σήμερα και έχουν κάνει επανάσταση στον κόσμο της ηλεκτρονικής

Clipper chip

Ένα ανθεκτικό έναντι της παραποίησης VLSI chip σχεδιασμένο από την NSA για την κρυπτογράφηση φωνής επικοινωνιών. Είναι σύμφωνο με το πρότυπο Escrow Encryption Standard (EES) και εκτελεί τον αλγόριθμο κρυπτογράφησης Skipjack (Παλαμίδα).

Cryptanalysis

1) Η ανάλυση ενός κρυπτογραφικού συστήματος ή / και των εισροών και εκροών για την άντληση εμπιστευτικών μεταβλητών ή / και ευαίσθητων δεδομένων. 2) Οι δράσεις που πραγματοποιούνται για την μετατροπή κρυπτογραφημένων μηνυμάτων σε απλό κείμενο χωρίς τη γνώση του αρχικού κρυπταλγόριθμου και των κλειδιών που απασχολούνται στην κρυπτογράφηση.

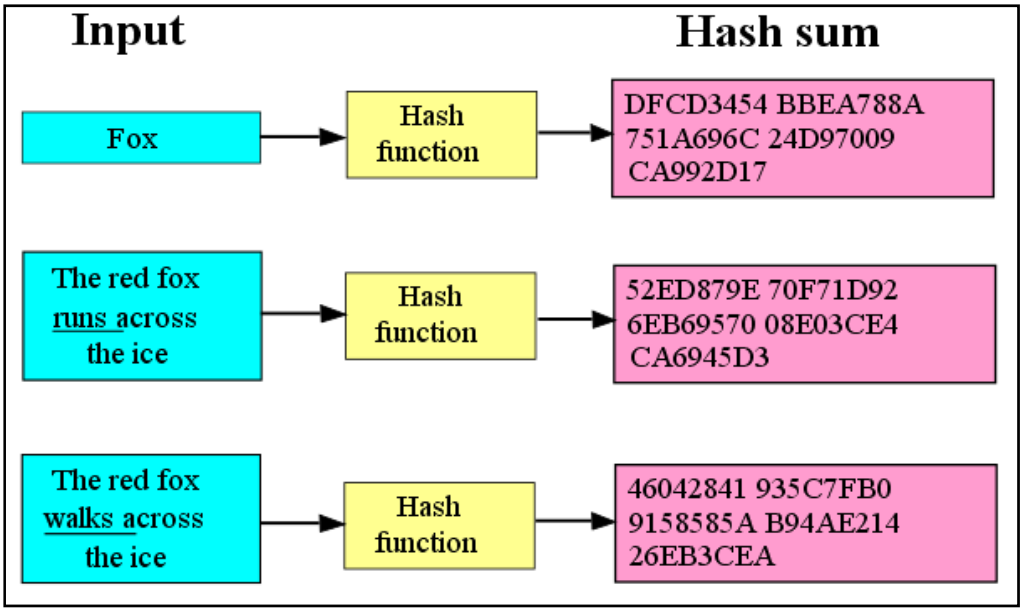
Crypto Application Program Interface (CAPI)

Το Capi είναι ένα api για συστήματα κρυπτογραφίας, είναι μια διεπαφή προγραμματισμού εφαρμογών, που περιλαμβάνεται σε διάφορα λειτουργικά συστήματα, που παρέχει υπηρεσίες για να μπορέσει να εξασφαλίσει την ανάπτυξη εφαρμογών Windows-based χρησιμοποιώντας κρυπτογράφηση. Είναι μια σειρά από δυναμικά συνδεδεμένες βιβλιοθήκες που παρέχει ένα αφηρημένο επίπεδο, το οποίο απομονώνει τους προγραμματιστές από τον κώδικα που χρησιμοποιείται για την κρυπτογράφηση των δεδομένων. Το CryptoAPI υποστηρίζει και ασύμμετρη και συμμετρική κρυπτογράφηση. Περιλαμβάνει τις λειτουργίες για κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων και για την πιστοποίηση της ταυτότητας με τη χρήση ψηφιακών πιστοποιητικών. Περιλαμβάνει επίσης μια σειρά κρυπτογραφικούς μηχανισμούς όπως πχ. γεννήτριες τυχαίων αριθμών. Το CryptoAPI συνεργάζεται με μια σειρά CSP (Cryptographic Service Providers) που είναι εγκατεστημένες στον υπολογιστή. Οι CSP είναι οι μονάδες που κάνουν την πραγματική δουλειά της κωδικοποίησης και αποκωδικοποίησης των δεδομένων κατά την εκτέλεση των κρυπτογραφικών λειτουργιών.

Cryptographic Hash Function

Στην κρυπτογραφία, μια κρυπτογραφική μέθοδος σύνοψης (hash function) είναι ένας μετασχηματισμός που μετατρέπει κάθε είσοδο σε προκαθορισμένου μεγέθους συμβολοσειρά (fixed-size string), η οποία αποκαλείται σύνοψη ή τιμή hash.Οι μέθοδοι σύνοψης (hash functions), με την δυνατότητα αυτή χρησιμοποιούνται σε ένα πλήθος υπολογιστικών σκοπών, συμπεριλαμβανομένης και της κρυπτογραφίας.Η τιμή του hash είναι μια συνοπτική αναπαράσταση του μηνύματος ή του κειμένου από το οποίο υπολογιστικέ. Οι κρυπτογραφικές hash functions χρησιμοποιούνται για ελέγχους ακεραιότητας μηνυμάτων και ψηφιακές υπογραφές σε ποικίλες εφαρμογές

στην ασφάλεια συστημάτων, όπως authentication και message integrity. Οι πιο διαδεδομένες hash functions είναι οι MD5 και SHA-1.



Εικόνα 129. Παραδείγματα μοναδικότητας Hash

Cryptography

Η επιστήμη που μελετά τις αρχές, τα μέσα και τις μεθόδους για την απόδοση απλού κειμένου σε ακατάληπτη κρυπτογραφημένη μορφή και αντίστροφα τη μετατροπή των κρυπτογραφημένων μηνυμάτων σε μορφή κατανοητή.

Cryptology

Η επιστήμη που ασχολείται με κρυφές, συγκεκαλυμμένες, ή κρυπτογραφημένες επικοινωνίες.

Data Encryption Standard (DES)

Ο αλγόριθμος κρυπτογράφησης DES είναι ένας κρυπτογραφικός αλγόριθμος για την προστασία των δεδομένων, που δημοσιεύθηκε από την Federal Information Processing Standard (FIPS). Ο DES εγκρίθηκε από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST), προορίζεται για δημόσια χρήση και την κυβέρνηση.

Encryption

Μία κρυπτογραφική διαδικασία με την οποία ένα κρυπτογραφημένο ευανάγνωστο μήνυμα είναι και να είναι δυσανάγνωστο σε όλους, εκτός από τον κάτοχο του κατάλληλου κρυπτογραφικό κλειδί.

Hooking

Στα πλαίσια του προγραμματισμού, το Hooking είναι μια τεχνική που χρησιμοποιεί άγκιστρα που να δημιουργούν τη λεγόμενη αλυσίδα διαδικασιών, όπως κάνει και ένα πρόγραμμα χειρισμού γεγονότων (event handler). Έτσι, μετά το γεγονός που συμβαίνει, ο έλεγχος της ροής της αλυσίδας ακολουθεί συγκεκριμένη σειρά. Το νέο hook καταχωρεί τη δική του διεύθυνση εξυπηρέτησης για το γεγονός και αναμένει να κληθεί ο αρχικός εξυπηρετητής σε κάποιο σημείο, συνήθως καλείται στο τέλος. Κάθε Hook είναι υποχρεωμένο να παραχωρεί την εκτέλεση στον προηγούμενο εξυπηρετητής, φτάνοντας τελικά στον αρχικά προεπιλεγμένο, σε κάθε άλλη περίπτωση η αλυσίδα έχει σπάσει. Αφαίρεση του Hook σημαίνει θέσπιση της αρχικής διαδικασίας στο πρόγραμμα χειρισμού (event handler). Το Hooking μπορεί να χρησιμοποιηθεί για πολλούς σκοπούς, συμπεριλαμβανομένης και της διόρθωσης σφαλμάτων και της παράτασης της αρχικής λειτουργικότητας. Μπορεί επίσης να χρησιμοποιείται καταχρηστικά με σκοπό το injection code (δυνητικά κακόβουλο) στον event handler - για παράδειγμα, τα rootkits προσπαθούν να κάνουν τους εαυτούς τους αόρατους παριστάνοντας την έξοδο από της κλήσεις του API που υπό κανονικές συνθήκες θα αποκαλύπτεται την ύπαρξή τους.

Intrusion

Κάθε δέσμη δράσεων που επιχειρεί να θέσει σε κίνδυνο την ακεραιότητα, την εμπιστευτικότητα ή τη διαθεσιμότητα ενός πόρου (υλικού και μη).

Intrusion Detection

Τεχνικές που αφορούν την προσπάθεια ανίχνευσης μιας εισβολής σε έναν υπολογιστή ή σε ένα δίκτυο, η ανίχνευση επιτυγχάνεται από την παρατήρηση των δράσεων, των αναφορών ασφάλειας ή τον έλεγχο δεδομένων. Η ανίχνευση διάρρηξης ή προσπάθειας διόρυξης γίνεται είτε χειροκίνητα, είτε μέσω ειδικών λογισμικών συστημάτων που λειτουργούν με αρχεία καταγραφής ή άλλες διαθέσιμες πληροφορίες σχετικά με το δίκτυο.

Key

Ένα σύμβολο ή ακολουθία συμβόλων (ή ηλεκτρική ή μηχανικών συσχετισμών συμβόλων), που εφαρμόζεται στο κείμενο για την κρυπτογράφηση ή αποκρυπτογράφηση.

OpenCard Framework

Το OpenCard Framework (OCF) παρέχει ένα Java API για την πρόσβαση τόσο σε card readers και για τις σχετικές εφαρμογές που είναι ενσωματωμένες σε έξυπνες κάρτες. Το OpenCard Framework είχε αρχικά οριστεί από την κοινοπραξία OpenCard, αλλά κυρίως από την IBM και Gemplus. Το έργο ολοκληρώθηκε με την έκδοση 1.2 της προδιαγραφής και υλοποίηση της αναφοράς από την IBM. Η κοινοπραξία διαλύθηκε και το OpenCard framework έμεινε σε αδρανή κατάσταση. Η

ιστοσελίδα ήταν ακόμα διαθέσιμη μέχρι και το 2007 αλλά είναι πλέον κλειστή. Το πρωτότυπο κώδικα μεταφέρθηκε στο SourceForge[27], αλλά ποτέ δεν υποστήριξε ενεργά.

PC/SC

Το PC/SC (Personal Computer/Smart Card) είναι μια προδιαγραφή για την επικοινωνία μεταξύ των προσωπικών υπολογιστών και των smart cards. Προσφέρει τη διαλειτουργικότητα των προϊόντων από διάφορους προμηθευτές καθορίζοντας ένα API (Application Programming Interface) για τη διαχείριση των card readers και την επικοινωνία με τους με τις κάρτες. Το PC / SC πρότυπο ορίζει τον τρόπο ενσωμάτωσης των card readers και smart card με το υπολογιστικό περιβάλλον και ορίζει το διαμερισμό των συσκευών διαχείρισης καρτών στις πολλαπλές εφαρμογές έξυπνων.

PC/SC Lite

Το Personal Computer/Smart Card Lite, είναι ανοιχτού κώδικα λογισμικό που υλοποίει το πρότυπο PC/SC για το Linux.

PKCS

Στην κρυπτογραφία, το **PKCS#1** είναι το πρώτο από μία οικογένεια standards που αποκαλούνται Public-Key Cryptography Standards (Πρότυπα κρυπτογράφησης δημοσίου κλειδιού), δημοσιευμένα από το RSA Laboratories. Προδιαγράφοντας τους βασικούς προσδιορισμούς και συστάσεις για την υλοποίηση του αλγορίθμου RSA για κρυπτογραφία δημόσιου κλειδιού. Καθορίζει τις μαθηματικές ιδιότητές του δημοσίου και του ιδιωτικού κλειδιού, primitive operations για encryption και υπογραφές, ασφαλή cryptographic schemes, και αναπαραστάσεις related ASN.1 syntax.

[27] http://sourceforge.net/

PKCS Standards Summary			
	Version	Name	Comments
PKCS #1	2.1	RSA Cryptography Standard	See RFC 3447. Defines the mathematical properties and format of RSA public and private keys (ASN.1-encoded in clear-text), and the basic algorithms and encoding/padding schemes for performing RSA encryption, decryption, and producing and verifying signatures.
PKCS #2	-	*Withdrawn*	No longer active. Covered RSA encryption of message digests, but was merged into PKCS #1.
PKCS #3	1.4	Diffie-Hellman Key Agreement Standard	A cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.
PKCS #4	-	*Withdrawn*	No longer active. Covered RSA key syntax, but was merged into PKCS #1.
PKCS #5	2.0	Password-based Encryption Standard	See RFC 2898 and PBKDF2.
PKCS #6	1.5	Extended-Certificate Syntax Standard	Defines extensions to the old v1 X.509 certificate specification. Obsoleted by v3 of the same.
PKCS #7	1.5	Cryptographic Message Syntax Standard	See RFC 2315. Used to sign and/or encrypt messages under a PKI. Used also for certificate dissemination (for instance as a response to a PKCS#10 message). Formed the basis for S/MIME, which is now based on RFC 3852, an updated Cryptographic Message Syntax Standard (CMS). Often used for single sign-on.
PKCS #8	1.2	Private-Key Information Syntax Standard.	Used to carry private certificate keypairs (encrypted or unencrypted).
PKCS #9	2.0	Selected Attribute Types	Defines selected attribute types for use in PKCS #6 extended certificates, PKCS #7 digitally signed messages, PKCS #8 private-key information, and PKCS #10 certificate-signing requests.
PKCS #10	1.7	Certification Request Standard	See RFC 2986. Format of messages sent to a certification authority to request certification of a public key. See certificate signing request.
PKCS #11	2.20	Cryptographic Token Interface (Cryptoki)	An API defining a generic interface to cryptographic tokens (see also Hardware Security Module). Often used for single sign-on and smartcard [1].
PKCS #12	1.0	Personal Information Exchange Syntax Standard	Defines a file format commonly used to store private keys with accompanying public key certificates, protected with a password-based symmetric key. PFX is a predecessor to PKCS#12. This is a container format that can contain multiple embedded objects, eg. multiple certificates. Usually protected/encrypted with a password. Can be used as a format for the Java key store. Can be used by Tomcat, but NOT by Apache.
PKCS #13	–	Elliptic Curve Cryptography Standard	(Under development.)
PKCS #14	–	Pseudo-random Number Generation	(Under development.)
PKCS #15	1.1	Cryptographic Token Information Format Standard	Defines a standard allowing users of cryptographic tokens to identify themselves to applications, independent of the application's Cryptoki implementation (PKCS #11) or other API. RSA has relinquished IC-card-related parts of this standard to ISO/IEC 7816-15 [2].

Εικόνα 130. Ο πίνακας των PKCS από την Wikipedia

Public Key Cryptography Standard #11 (PKCS#11)

Το πρότυπο αυτό καθορίζει την διασύνδεση με για κρυπτογραφικές διαδικασίες με συσκευές όπως token ή smart card.

Private Key Cryptography

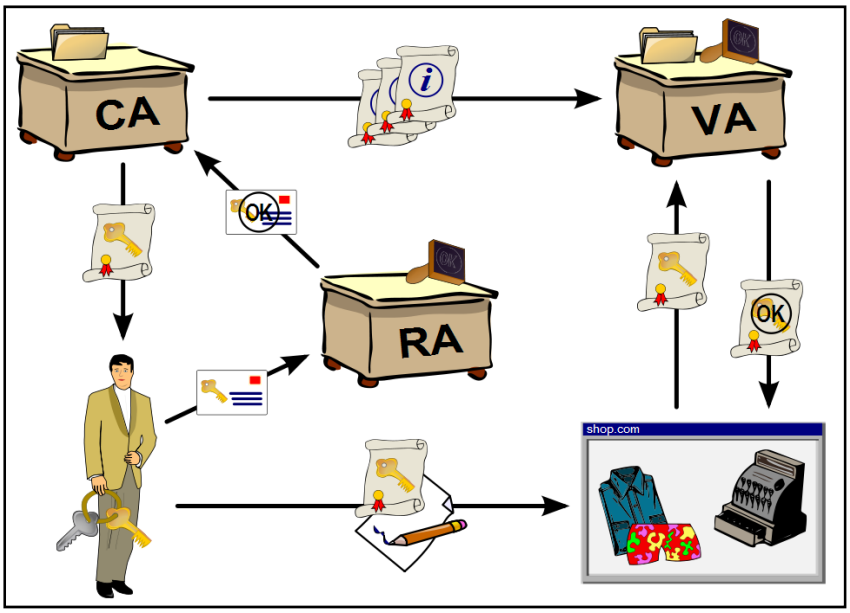
Η κρυπτογραφική μεθοδολογία με την οποία ο encryptor και ο decryptor χρησιμοποιούν το ίδιο κλειδί, το οποίο πρέπει να κρατηθεί μυστικό. Η μεθοδολογία αυτή συνήθως χρησιμοποιούνται μόνο από μια μικρή ομάδα.

Public Key Cryptography

Τύπος κρυπτογράφησης συμφώνα με τον την οποίο η διαδικασία κρυπτογράφησης είναι διαθέσιμη στο κοινό και απροστάτευτη, αλλά ένα μέρος της αποκρυπτογράφησης, το κλειδί προστατεύεται έτσι ώστε μόνο με τη γνώση και των δύο μερών της διαδικασίας της αποκρυπτογράφησης να είναι δυνατή η αποκρυπτογράφηση του κρυπτογραφημένου κείμενου.

Public Key Infrastructure (PKI)

Στην κρυπτογραφία, μια **PKI** είναι μια συμφωνία που δεσμεύει δημόσια κλειδιά με τις αντίστοιχες ταυτότητες χρηστών με μια αρχή έκδοσης πιστοποιητικών (certificate authority CA). Η ταυτότητα των χρηστών πρέπει να είναι μοναδική για κάθε CA. Η δέσμευση θεσπίζεται μέσω της καταγραφής και της διαδικασίας της έκδοσης, η οποία, ανάλογα με το επίπεδο αξιοπιστίας που έχει, δεσμεύεται να πραγματοποιείται από το λογισμικό σε CA, ή υπό την εποπτεία ανθρώπου. Ο ρόλος της **PKI** που εξασφαλίζει τη δέσμευση αυτή ονομάζεται Αρχή Εγγραφής (Registration Authority, RA). Για κάθε χρήστη, ταυτότητα του χρήστη, δημόσιο κλειδί, ή δεσμευτικό χαρακτήρα, όλοι οι όροι ισχύος και τα χαρακτηριστικά εισάγονται στο δημόσιο κλειδί των πιστοποιητικών που εκδίδονται από την CA. Ο όρος trusted third party (**TTP**)μπορεί επίσης να χρησιμοποιηθεί για μία certificate authority (**CA**). Ενώ ο όρος PKI κάποιες φορές εσφαλμένα χρησιμοποιείται υποδηλώνοντας κάποιους public key algorithms, οι οποίοι δεν απαιτούν CA για την δημιουργία τους.



Εικόνα 131.Υποδομή κρυπτογράφησης δημοσίου κλειδιού

RSA Algorithm

Ένας κρυπτογραφικός αλγόριθμος δημόσιου κλειδιού που βασίζεται στην υπόθεση ότι η παραγοντοποιήσει του προϊόντος των δύο μεγάλων πολυώνυμων (PRIMES) είναι δύσκολη.

RSA 9796 - ISO/IEC 9796-2:2002

Προδιαγράφει τρία ψηφιακά schemes παρέχοντας ανάκτηση του μηνύματος, δύο από τα οποία είναι ντετερμινιστικά (όχι τυχαία) ενώ το τρίτο είναι μη- αιτιοκρατικό (τυχαίο). Η ασφάλεια και των τριών schemes βασίζεται στην δυσκολία ανάλυσης των παραγόντων μεγάλων αριθμών. Και τα τρία schemes παρέχουν είτε ολική ανάκτηση

είτε μερική- τμηματική ανάκτηση του μηνύματος. Η μέθοδος παραγωγής κλειδιού για τα τρία signature schemes προκαθορίζεται στο ISO/IEC 9796.

Token

Ένα Token στα πλαίσια ασφάλειας, είναι ένα δείγμα hardware σαν έξυπνη κάρτα, αλλά θα μπορούσε επίσης να είναι ένα module λογισμικού σύνδεση σχεδιασμένο για να αλληλεπιδράει με ένα ειδικό hardware module, όπως μια έξυπνη κάρτα. Η ταυτοποίηση που βασίζεται σε Token προσφέρει αυξημένη ασφάλεια, επειδή η επιτυχία εξαρτάται από φυσικά αναγνωριστικά (πχ η έξυπνη κάρτα) και έναν προσωπικό αριθμό αναγνώρισης (PIN). Παράδειγμα Token αποτελεί η smart card όπως επίσης και το USB Token.

winscard.dll (Microsoft Smart Card Library)

Το αρχείο winscard.dll, απαιτείται από τα Windows, όταν χειρίζονται έξυπνες κάρτες και αναγνώστες έξυπνων καρτών. Οι έξυπνες κάρτες περιέχουν μικροεπεξεργαστές που περιέχουν κρυπτογραφημένες πληροφορίες για τον ιδιοκτήτη τους. Η ύπαρξη smart card reader σε ένα σύστημά απαιτεί την ύπαρξη της winscard.dll, διαφορετικά μπορεί να αφαιρεθεί.

Παράρτημα ΙΙ

GSLDiagnReport.txt

```
GemSAFE Logon Diagnostic Report
01/23/09 15:18:48

================================================
System info
Windows XP
Name: Windows XP
Version: 5.1.2600
Information: Service Pack 3

================================================
================================================

Package Name:     GemSafe Libraries

.....................................
Product
Product version
Version: GemSafe Libraries 4.2.0-015 SP2 004
GSLibsDiag.ini
Location: C:\Program Files\Gemplus\Common\Diagnostic\GSLibsDiag.ini

.....................................
Registry
HKEY_LOCAL_MACHINE\SOFTWARE\Gemplus\GemSafe Libraries
InstallDir C:\Program Files\Gemplus\GemSafe Libraries Admin
HKEY_LOCAL_MACHINE\SOFTWARE\Gemplus\Cryptography\CSP
Pkcs#11Name      C:\Program      Files\Gemplus\GemSafe      Libraries
Admin\BIN\GCLIB.DLL
CryptoSign
C3C04C7CD82BCDE03D53196035FA685ABBA03F7209A170881BFED573B6FF012B11240
2481FCA31429336D1874098C7464C936FF24ED0F1788A7C706446E19D3F
ResourceFile      C:\Program      Files\Gemplus\GemSafe      Libraries
Admin\BIN\GUICore.DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Gemplus\Cryptography\Pkcs11\4.0
TokenCheckFreq 0
MaxSlot 10
BinPath C:\Program Files\Gemplus\GemSafe Libraries Admin\BIN
HKEY_LOCAL_MACHINE\SOFTWARE\Gemplus\Cryptography\Pkcs11\Token\PKCS#11
v2.01 - GemID/GemSAFE Applet Module
Name        C:\Program        Files\Gemplus\GemSafe        Libraries
Admin\BIN\pk2GemID.dll
Type dword:00000001
State dword:00000001
Signature
A6D9A92E46A1FBADE6F6F6BD99C7E2B2D01382DB3B658A097BDF12CB815F4FEE517B7
D552F6C58E297C967174B6DFC832EDB6C2138AB0FB4292AAA73D2E0FB4C
HKEY_LOCAL_MACHINE\SOFTWARE\Gemplus\Cryptography\Pkcs11\Token\PKCS#11
v2.01 - GPK Module
Name        C:\Program        Files\Gemplus\GemSafe        Libraries
Admin\BIN\pk2GPK16.dll
Type dword:00000001
State dword:00000001
Signature
2C680B840B26441013DFA7EEE09226868DB9B711933C23632E859A97504E700D75851
```

```
2EEBF2CCB01F5D84124F766F327E380950B9EDFF0CACACC7DBE3197A282
HKEY_LOCAL_MACHINE\SOFTWARE\Gemplus\Cryptography\RegTool
CSP Name Gemplus GemSAFE Card CSP
HKEY_LOCAL_MACHINE\SOFTWARE\Gemplus\Cryptography\SmartCards\GemSAFE
x509 Dictionary Name C:\Program Files\Gemplus\GemSafe Libraries
Admin\BIN\dict_002.bin
SignWithDER FALSE
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\
GemSAFE Smart Card (16K)
ATR 3BA70040008065A209000000
ATRMask FFFFFFFF00FFFFFFFF000000
Crypto Provider Gemplus GemSAFE Card CSP
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\
GemSAFE Smart Card (8K)
ATR 3BA70040008065A208000000
ATRMask FFFFFFFF00FFFFFFFF000000
Crypto Provider Gemplus GemSAFE Card CSP
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\
Gemplus GemSAFE Card CSP
Image Path C:\Program Files\Gemplus\GemSafe Libraries
Admin\BIN\GSafeCSP.dll
Type dword:00000001
Signature
9D63F448AC05D00596C722BD0628C8C0154236FAEE5E98EC3BBFB360B8A7DB585CA39
4014769B02856480FED7FE99788A4A8747F0E78B1DD10B9627445BA97E6ADDFC7C45F
DBB3DA63ABA6DF813C23A0C9CF0C4D4DBBDD0495B3C7AE96FD7EA338C67581067E718
14F8EE2645BB51548DD6C51ED7389C9669BD55E25E1F729750000000000000000000
SigInFile dword:00000000
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
RegTool "C:\Program Files\Gemplus\GemSafe Libraries
Admin\BIN\RegTool.exe"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\GemSAFE Card
Server
ImagePath C:\Program Files\Gemplus\GemSafe Libraries
Admin\BIN\GCardSrvNT.exe
Type dword:00000110
Start dword:00000002
ErrorControl dword:00000001
DisplayName GemSAFE Card Server
DependOnService SCardSvr
ObjectName LocalSystem
HKEY_LOCAL_MACHINE\SOFTWARE\Gemplus\Generic Tool
Plugin PIN Management C:\Program Files\Gemplus\GemSafe Libraries
Admin\BIN\PluginPINMngt.dll
HKEY_LOCAL_MACHINE\SOFTWARE\Gemplus\Generic Tool
Plugin Libraries Configuration C:\Program Files\Gemplus\GemSafe
Libraries Admin\BIN\PluginLibsConfig.dll
Plugin PIN Policy C:\Program Files\Gemplus\GemSafe Libraries
Admin\BIN\PluginPINPolicy.dll
HKEY_LOCAL_MACHINE\SOFTWARE\Gemplus\Generic Tool
Plugin Libraries CustomSetup C:\Program Files\Gemplus\GemSafe
Libraries Admin\BIN\PluginLibsCustomSetup.dll
HKEY_LOCAL_MACHINE\SOFTWARE\Gemplus\Generic Tool
Plugin Certificates C:\Program Files\Gemplus\GemSafe Libraries
Admin\BIN\PluginCertificates.dll
Plugin Information Card C:\Program Files\Gemplus\GemSafe Libraries
Admin\BIN\PluginInformationCard.dll
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\
GXPPro-R3.x MPCOS PTS
ATR 3b7a0000008065a20000000072d600
```

```
ATRMask ffff00ffffffffff00000000ffff00
Crypto Provider Gemplus GemSAFE Card CSP
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\
GXPPro-R3.x MPCOS
ATR 3b6a00008065a20000000072d600
ATRMask ffffffffffffff00000000ffff00
Crypto Provider Gemplus GemSAFE Card CSP
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\
GXPPro-R3.x STD PTS
ATR 3b7d00000080318065b08300000083009000
ATRMask ffff00ffffffffffffffff000000ffffffff
Crypto Provider Gemplus GemSAFE Card CSP
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\
GXPPro-R3.x STD
ATR 3b6d000080318065b08300000083009000
ATRMask ffffffffffffffffffff000000ffffffff
Crypto Provider Gemplus GemSAFE Card CSP
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\
GXPPro-R3.x FIPS PTS
ATR 3b7b0000008065b08300000083009000
ATRMask ffff00ffffffffffff000000ffffffff
Crypto Provider Gemplus GemSAFE Card CSP
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\
GXPPro-R3.x FIPS
ATR 3b6b00008065b08300000083009000
ATRMask ffffffffffffffff000000ffffffff
Crypto Provider Gemplus GemSAFE Card CSP
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\
GXPPro-R3.x MPCOS PTS T=1
ATR 3bfa000000813120438065a20000000072d60000
ATRMask ffff00ffffffffffffffff00000000ffff0000
Crypto Provider Gemplus GemSAFE Card CSP
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\
GXPPro-R3.x MPCOS T=1
ATR 3bea000081312043806 5a20000000072d60000
ATRMask ffffffffffffffffffffff00000000ffff0000
Crypto Provider Gemplus GemSAFE Card CSP
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\
GXPPro-R3.x STD PTS T=1
ATR 3bfd000000813120438031 8065b0830000008300900000
ATRMask ffff00ffffffffffffffffffffffff000000ffffff0000
Crypto Provider Gemplus GemSAFE Card CSP
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\
GXPPro-R3.x STD T=1
ATR 3bed000081312043803 18065b0830000008300900000
ATRMask ffffffffffffffffffffffffffff000000ffffff0000
Crypto Provider Gemplus GemSAFE Card CSP
.....................................
Files
PluginLibsConfig.dll
Name: PluginLibsConfig.dll
Location: C:\Program Files\Gemplus\GemSafe Libraries Admin\BIN
Description: Profile Generator DLL
Created: 11/16/04 10:55:18
Size: 733184 Bytes
Version: 1, 3, 4, 0
Hash: 345189A79684EF7BB0FEE6C97D0B441E6D688318
PluginPINPolicy.dll
Name: PluginPINPolicy.dll
Location: C:\Program Files\Gemplus\GemSafe Libraries Admin\BIN
```

```
Description: PIN Policy Plugin DLL
Created: 11/23/04 10:33:36
Size: 753664 Bytes
Version: 1, 2, 7, 0
Hash: 02F72BC66CAE894B1875AC5A5CFD1E000FE14B05
PluginPINMngt.dll
Name: PluginPINMngt.dll
Location: C:\Program Files\Gemplus\GemSafe Libraries Admin\BIN
Description: PIN Manager Plugin DLL
Created: 11/30/04 16:32:50
Size: 999424 Bytes
Version: 1, 3, 6, 0
Hash: 44206E8BECB206A8500D036FD093252E0DE478C0
GCardSrv.exe
Name: GCardSrv.exe
Location: C:\Program Files\Gemplus\GemSafe Libraries Admin\BIN
Description: GemSAFE Card Process
Created: 06/10/05 14:58:20
Size: 253952 Bytes
Version: 2, 1, 8, 2
Hash: 09CA835307EF4AA7A6666081A8F462B1CD4172FC
GCardSrvNT.exe
Name: GCardSrvNT.exe
Location: C:\Program Files\Gemplus\GemSafe Libraries Admin\BIN
Description: GemSAFE Card Server
Created: 06/01/05 10:17:14
Size: 118784 Bytes
Version: 2, 1, 8, 2
Hash: 04CF6E7F8D5E891189DF562BA8BBADFE595E7F6C
GCLIB.dll
Name: GCLIB.dll
Location: C:\Program Files\Gemplus\GemSafe Libraries Admin\BIN
Description: PKCS#11 v2.01 - Gemplus Cryptoki
Created: 06/01/05 10:10:04
Size: 200704 Bytes
Version: 5, 2, 0, 0
Hash: 26525AAAC4A4A9FCCC275ADD3FBD95FB505E372E
GSafeCsp.dll
Name: GSafeCsp.dll
Location: C:\Program Files\Gemplus\GemSafe Libraries Admin\BIN
Description: Gemplus GemSAFE Card CSP
Created: 05/30/05 18:42:10
Size: 237568 Bytes
Version: 4, 1, 1, 0
Hash: F2CE580E86EAC995E26F5F0D535739D5899B9424
GemPPM.dll
Name: GemPPM.dll
Location: C:\Program Files\Gemplus\GemSafe Libraries Admin\BIN
Description: GemPPM
Created: 11/23/04 10:32:02
Size: 241664 Bytes
Version: 2, 2, 4, 0
Hash: 4429CA477111E7E6DE4907B07E485D5B675DF2A7
GUICore.dll
Name: GUICore.dll
Location: C:\Program Files\Gemplus\GemSafe Libraries Admin\BIN
Description: GUICore DLL
Created: 03/07/05 16:00:28
Size: 221184 Bytes
Version: 1, 0, 8, 0
```

```
Hash: 58FBCE08D5888D87C31F0EF4F0281C9D7EEB9512
RegTool.exe
Name: RegTool.exe
Location: C:\Program Files\Gemplus\GemSafe Libraries Admin\BIN
Description: Certificate Registration Tool
Created: 06/08/05 14:49:00
Size: 40960 Bytes
Version: 2, 1, 3, 0
Hash: D0ABC40024668F6A4DD6B690FA3E9C6D7940A85A
pk2GemID.dll
Name: pk2GemID.dll
Location: C:\Program Files\Gemplus\GemSafe Libraries Admin\BIN
Description: PKCS#11 v2.01 - GemID/GemSAFE Applet Module
Created: 06/08/05 14:42:56
Size: 1761280 Bytes
Version: 3, 1, 5, 0
Hash: BEE952708D68D22976C59CC4E297D35CB5DE8B8F
pk2gpk16.dll
Name: pk2gpk16.dll
Location: C:\Program Files\Gemplus\GemSafe Libraries Admin\BIN
Description: PKCS#11 v2.01 - GPK Module
Created: 06/08/05 14:43:58
Size: 1101824 Bytes
Version: 7, 1, 3, 0
Hash: CCA1326547AF4FC37BFF0B32DA44DF5863E9FF21
PluginLibsCustomSetup.dll
Name: PluginLibsCustomSetup.dll
Location: C:\Program Files\Gemplus\GemSafe Libraries Admin\BIN
Description: Custom Setup Manager DLL for GemSAFE ToolBox
Created: 11/23/04 09:33:02
Size: 770048 Bytes
Version: 1, 1, 6, 0
Hash: 7BCFB4E6490BDBF4562363F651FB1F829812D8B7
PluginCertificates.dll
Name: PluginCertificates.dll
Location: C:\Program Files\Gemplus\GemSafe Libraries Admin\BIN
Description: Certificates PluginDLL
Created: 04/01/05 10:34:30
Size: 1007616 Bytes
Version: 1, 2, 0, 0
Hash: DD95A1A5DAAB66F2BBB185F0BBAE104CC2590A7C
PluginInformationCard.dll
Name: PluginInformationCard.dll
Location: C:\Program Files\Gemplus\GemSafe Libraries Admin\BIN
Description: Card Information Plugin DLL
Created: 11/30/04 16:30:30
Size: 798720 Bytes
Version: 1, 1, 5, 0
Hash: 7A4397A353E52C1E98F3ED06E87A6BF898F2176E
GemCNF.dll
Name: GemCNF.dll
Location: C:\Program Files\Gemplus\GemSafe Libraries Admin\BIN
Description: GemCNF
Created: 08/26/04 13:32:12
Size: 110592 Bytes
Version: 1, 0, 2, 0
Hash: 8B1F2D2D963164A8D14AB9C5D2391DF986C2DE84

================================================
<<<<<<<<<<<<<<<<<< End of report >>>>>>>>>>>>>>>>>>
```

Παράρτημα ΙΙΙ – Σύνοψη

ΑΝΑΠΤΥΞΗ ΑΣΦΑΛΩΝ ΕΦΑΡΜΟΓΩΝ ΜΕ ΤΗΝ ΧΡΗΣΗ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ

(ΠΕΡΙΛΗΨΗ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ)

Παπαδέας Ν.Σ.Γ Δημήτριος (ΑΜ 1272)

Τμήμα Εφαρμοσμένης Πληροφορικής και Πολυμέσων

ΣΤΕΦ / ΤΕΙ Κρήτης

Ηράκλειο, Κρήτη

E-mail: dimpapadeas@hotmail.com

Φεβρουάριος 2009

Επόπτης Καθηγητής: Μανιφάβας Χαράλαμπος (Επ. Καθηγητής)

1. Περίληψη

Η ακόλουθη πτυχιακή εργασία αποτελεί μία μελέτη των έξυπνων καρτών (Smart cards) σε ένα ευρύ περιβάλλον χρήσεων και εφαρμογών. Οι έξυπνες κάρτες αποτελούν ένα μέσο ενίσχυσης της ασφάλειας ενός ευρύτερου υπολογιστικού συστήματος ή δικτύου. Χρησιμοποιούνται είτε σε εμπορικές εφαρμογές είτε σε εφαρμογές ελέγχου πρόσβασης. Οι περιστερές κάρτες έχουν δικό τους λειτουργικό σύστημα και σύστημα αρχείων. Η έξυπνη κάρτα Gemsafe, αποτελεί εμπορικό προϊόν της Gemplus - Gemalto, η οποία είναι η μεγαλύτερη εταιρία στην κατασκευή λογισμικού για κάρτες και συστημάτων ασφαλείας με smart cards. Η Gemsafe έχει το λειτουργικό σύστημα GPK και είναι πλήρως συμβατή με όλα τα προγράμματα της Gemalto. Οι αναγνώστες έξυπνων καρτών αποτελούν το υλικό τμήμα διασύνδεσης μεταξύ μίας κάρτας και ενός συστήματος. Ανάλογα με την περίπτωση υπάρχουν αναγνώστες για κάθε τύπο κάρτας. Οι GemSafe Libraries αποτελούν ένα πακέτο βιβλιοθηκών που υποστηρίζουν πολλές από τις πολύπλοκες συναλλαγές μεταξύ της κάρτας και του συστήματος, όπως επίσης πάνω σε αυτές τις βιβλιοθήκες έχουν αναπτυχθεί πολλά προγράμματα ελέγχου πρόσβασης και διαχείρισης καρτών. Επιπλέον οι GemSafe Libraries αποτελούν και μέσο επέκτασης της χρήσης μίας κάρτας λειτουργώντας ως διασυνδετικός κρίκος μεταξύ της κάρτας και τρίτων εφαρμογών όπως browsers και mail clients. Τέλος και η Java υποστηρίζει τον προγραμματισμό των καρτών και των εφαρμογών για κάρτες με τα Java card api και javax.smartcardio api αντίστοιχα, βοηθώντας σημαντικά και μειώνοντας αισθητά την πολυπλοκότητα και την δυσκολία ανάπτυξής μίας εφαρμογής σε κάρτα(ή για κάρτα) σε σχέση με την C++.

2. Εισαγωγή

Τα τελευταία χρόνια η ασφάλεια των δεδομένων έχει γίνει ζωτικής σημασίας, τεράστια χρηματικά ποσά και προσωπικά δεδομένα έχουν χαθεί από επιθέσεις ή από κενά ασφαλείας σε κάποιο σύστημα. Το τραπεζικό σύστημα υποφέρει από απάτες αντιγραφής μαγνητικών καρτών χάνοντας εκατομμύρια δολάρια κάθε χρόνο, πολλές εταιρίες πληρώνουν πανάκριβα δύσχρηστα μέσα ελέγχου πρόσβασης είτε καταφεύγουν σε οικονομικές και όχι αποτελεσματικές λύσεις. Ένα αποτελεσματικό μέσο για την ενίσχυση των συστημάτων ασφαλείας αποτελούν οι smart cards, μια τεχνολογία που δεν είναι πρόσφατη αν σκεφτεί κάνεις ότι το αυτοματοποιημένο chip της κάρτας εφευρέθηκε από το γερμανό επιστήμονα Helmut Gröttrup και τον συνάδελφό του Jürgen Dethloff το 1968, όμως το δίπλωμα ευρεσιτεχνίας εκδόθηκε τελικά το 1982. Οι smart cards είναι ένα συνεχώς εξελισσόμενο υποσύστημα αναβάθμισης της ασφαλείας ενός ευρύτερου συστήματος με ενσωματωμένους διάφορους μηχανισμούς ασφαλείας ενώ παράλληλα οι smart cards εκ φύσεως είναι ασφαλέστερα μέσα από τις απλές μαγνητικές κάρτες.

3. Έξυπνη κάρτα (smart card)

Είναι μια κάρτα, η οποία μοιάζει εξωτερικά με τη γνωστή πιστωτική κάρτα. Εσωτερικά, όμως, διαφέρει σημαντικά από αυτήν. Η πιστωτική κάρτα είναι ένα απλό κομμάτι πλαστικού, στο οποίο έχει ενσωματωθεί μια μαγνητική ταινία(magnetic stripe), στην οποία είναι εγγεγραμμένα κάποια στοιχεία του χρήστη. Η έξυπνη κάρτα, αντίθετα, ενσωματώνει ένα μικροεπεξεργαστή, ο οποίος βρίσκεται κάτω από μια επαφή από χρυσό, προσαρμοσμένο στη μια πλευρά της. Η βασική διαφορά των δύο τύπων καρτών είναι ότι, ενώ τα δεδομένα στη μαγνητική ταινία είναι εύκολο να παραλλαχθούν ή και να διαγραφούν (ακόμη και τυχαία), αυτό δεν είναι δυνατό στην έξυπνη κάρτα, γιατί ο μικροεπεξεργαστής της δεν περιέχει δεδομένα για το χρήστη: Ο μικροεπεξεργαστής της κάρτας και ο υπολογιστής, με τον οποίο συνδέεται, επικοινωνούν πριν ο μικροεπεξεργαστής επιτρέψει την πρόσβαση στα δεδομένα που περιέχονται στη μνήμη της κάρτας. Με τον τρόπο αυτό αποτρέπεται η παραχάραξη των δεδομένων κι έτσι ο χρήστης διασφαλίζεται, αν η κάρτα του βρεθεί σε διαφορετικά από τα δικά του χέρια. Η τροφοδοσία της κάρτας με ενέργεια εξασφαλίζεται από τον αναγνώστη έξυπνης κάρτας (smart card reader), στον οποίο εισάγεται η κάρτα προκειμένου να χρησιμοποιηθεί. Αυτός μπορεί να επικοινωνήσει με κάποιο κεντρικό υπολογιστή, όπου υπάρχουν τα στοιχεία του χρήστη, προκειμένου να εξασφαλιστεί η πρόσβαση σε δεδομένα. Η μνήμη RAM μιας έξυπνης κάρτας έχει μέγεθος μέχρι 8 Kbytes, η μνήμη ROM μέχρι 384 Kbytes, η μνήμη PROM (προγραμματιζόμενη ROM) μέχρι 256 Kbytes. Ο μικροεπεξεργαστής είναι συνήθως 16 bytes, ενώ υποστηρίζει μικρή ομάδα εντολών (εξασφαλίζοντας μικρό μέγεθος), κυρίως αυτών που είναι απαραίτητες για την επικοινωνία με τον αναγνώστη καρτών / υπολογιστή και την κρυπτογράφηση των περιεχόμενων δεδομένων.

3.1 Smart card types

Οι κάρτες χωρίζονται σε κατηγορίες ανάλογα με τον τρόπο που η κάρτα διαβάζεται ή γράφεται ή ανάλογα με τον τύπο του κυκλώματος (chip) που υλοποιείται στην ενσωματώνεται στην κάρτα και τις δυνατότητες του. Στην πρώτη κατηγορία έχουμε τις Contact Cards που είναι ο περισσότερο διαδεδομένος τύπος smart card είναι κάρτα

με ηλεκτρικές επαφές τοποθετημένες στο περίβλημα της. Ο 2ος τύπος είναι οι Contactless Cards, οι οποίες είναι smart card που χρησιμοποιούν ραδιοφωνικές συχνότητες (RFID) για την επικοινωνία της κάρτας με τον αναγνώστη, χωρίς να χρειάζεται η εισαγωγή της κάρτας και ο τρίτος τύπος της κατηγορίας είναι οι Combination Cards που αποτελούν υβριδικές κάρτες που ενσωματώνουν και contact και contactless τεχνολογίες. Στην 2η κατηγορία, ανάλογα με τον τύπο του κυκλώματος έχουμε: τις Memory Cards, οι κάρτες αυτές δεν διαθέτουν εξελιγμένη επεξεργαστική ισχύ και δεν έχουν την δυνατότητα να διαχειριστούν δυναμικά τα αρχεία, οι Memory Cards χωρίζονται σε 3 υποκατηγορίες : Straight Memory Cards, Protected / Segmented Memory Cards και Stored Value Memory Cards. Ο 2ος τύπος των κατηγοριοποιημένων ανάλογα με το chip είναι οι CPU/MPU Microprocessor Multifunction Cards, αυτές οι κάρτες έχουν δυναμικές δυνατότητες επεξεργασίας δεδομένων. Ως Smart cards πολλών λειτουργιών αναθέτουν την μνήμη της κάρτας σε ανεξάρτητους τομείς ή αρχεία εξουσιοδοτημένα σε μια συγκεκριμένη λειτουργία ή εφαρμογή.

3.2 Smart card OS

Οι δύο βασικότεροι τύποι λειτουργικών συστημάτων smart card είναι: Fixed File όπου τα αρχεία και τα δικαιώματα προκαθορίζονται από τον κατασκευαστή, και ο Structure και Dynamic Application System όπου δίνεται η δυνατότητα στους προγραμματιστές να αναπτύσσουν, να ελέγχουν και να εφαρμόζουν διαφορετικές εφαρμογές για την ίδια κάρτα.

3.3 Smart Card Standards

Τα smart card standards διατυπώνουν φυσικές ιδιότητες, χαρακτηριστικά επικοινωνίας και προδιαγράφουν τις εφαρμογές του ενσωματωμένου chip και των δεδομένων του. Τα κυριότερα πρότυπα είναι το ISO 7816, με μία σειρά από εκδόσεις για πολλές περιπτώσεις των έξυπνων καρτών, το FIPS, που είναι σχεδιασμένο για την προστασία των ομοσπονδιακών αποκτημάτων συμπεριλαμβανομένων και των υπολογιστικών και τηλεπικοινωνιακών συστήματα. Το EMV, ένα πρότυπο ανεπτυγμένο από τις Europay, MasterCard και Visa με σκοπό την υποστήριξη του ISO7816. Το PC/SC, ένα standard για card readers, προτεινόμενο και υλοποιημένο από την Microsoft. Τα CEN και ETSI που εστιάζουν κυρίως στις sim κάρτες και τέλος το HIPAA που αφορά εφαρμογές του συστήματος υγείας.

4. Gamesafe smart card

Η Gamesafe smart card είναι Cpu Contact card και αποτελεί προϊόν της Gemallto, είναι μία κάρτα χωριτικότητας 16k. Το λειτουργικό της σύστημα είναι το GPK επίσης προϊόν της Gemalto. Το GPK (Gemplus Public Key) είναι ένα λειτουργικό σύστημα που υπηρετεί τους σκοπούς της ασφάλειας των δεδομένων, δίνοντας έμφαση στις ιδιαίτερα απαιτητικές ανάγκες των εφαρμογών των εμπορικών συναλλαγών.

Το GPK περιλαμβάνει

- File system global και local level
- Συμβατές δομές δεδομένων, εντολές και κώδικες επιστροφής σύμφωνα με το

πρότυπο (APDU) ISO 7816-4

- Ένα συμπληρωματικό σύνολο εντολών διαχείρισης και παραμετροποίησης της κάρτας , από τα διεθνή πρότυπα MPCOS-EMV
- Οι μέθοδοι πληρωμής, οι δομές δεδομένων και οι εντολές από τα διεθνή πρότυπα MPCOS-EMV, επιτρέπουν την λειτουργία της κάρτας ως ηλεκτρονικό πορτοφόλι (electronic purse)
- EMV-χαρακτηριστικά συμβατότητας
- Ο 3DES αλγόριθμος χρησιμοποιείται για ασφαλή αποστολή μηνυμάτων συμφώνα με το πρότυπο ISO 7816-4, αλλά και για κρυπτογράφηση και αποκρυπτογράφηση
- SSL 1,024-bit RSA υπογραφές
- RSA (up to 1,024 bits) υπογραφή/ αποκρυπτογράφηση (normal mode και CRT mode)
- Εξακρίβωση (verification) RSA (up to 1,024 bits)
- Υπογραφή και εξακρίβωση (verification): DSA
- Πάνω στην κάρτα (Onboard) παραγωγή κλειδιού RSA (512 and 1,024 bits)
- SHA-1 και MD5 αλγορίθμους για hashing
- Μηχανισμό παραγωγής τυχαίων αριθμών (8 bytes and 32 bytes)
- Padding με PKCS#1 version 1.5, ISO9796-2, ANSI X9.31

5. Smart card readers

Ο smart card reader είναι μια ηλεκτρονική συσκευή που διαβάζει smart cards, τροφοδοτεί το ενσωματωμένο κύκλωμα της smart card με ηλεκτρικό ρεύμα, λειτουργεί ως μέσο μετάδοσης δεδομένων από ένα σύστημα σε μία κάρτα υποστηρίζοντας τα ανάλογα πρωτόκολλα επικοινωνίας. Η τιμή ενός card reader ποικίλει ανάλογα με τον αριθμό των reader που παραγγέλνονται όπως επίσης και από το μοντέλο παρ' όλα αυτά συνήθως κυμαίνεται σε χαμηλά επίπεδα, περίπου στα 10 - 20 €. Αρχικά οι smart card reader συνδέονταν με ένα σύστημα μόνο με σειριακή θύρα (Serial port) με αρκετά προβλήματα σε θέματα επικοινωνίας λόγω έλλειψης οδηγών διαχείρισης και χαμηλής ταχύτητας. Όμως με βάση τα πιο πρόσφατα πρότυπα PC/SC και CCID, έχουν αναπτυχθεί σύγχρονοι τρόποι επικοινωνίας μέσω USB συσκευών.

6. GemSafe Libraries

Το Λογισμικό GemSafe Libraries είναι μία εφαρμογή κρυπτογραφικών βιβλιοθηκών βασισμένη σε smart cards, που δίνει την δυνατότητα σε άλλες εφαρμογές της χρήσης smart card cryptography σε ένα PKI περιβάλλον. Παρέχοντας έτσι μεγίστου επιπέδου ασφάλεια και φορητότητα. Το Λογισμικό της GemSafe είναι βασισμένο στα στάνταρ APIs: PKCS#11και CAPI, τα οποία εγκαθίστανται στο client PC, με σκοπό τρίτες εφαρμογές να έχουν πρόσβαση στις smart card, στις κρυπτογραφικές μεθόδους και στην ασφαλή αποθήκευση κλειδιών και πιστοποιητικών. Αναλαμβάνοντας την αλληλεπίδραση με τις κάρτες, επίσης αποκρύπτει την πολυπλοκότητα και παράλληλα επιτρέπει την ανεμπόδιστη εκμετάλλευση όλων των δυνατοτήτων των smart cards. Τέλος υποστηρίζει όλους τους συμβατούς PC/SC οδηγούς (drivers) αναγνωστών καρτών.

6.1 Gamsafe Toolbox

Το GemSafe Toolbox είναι μια πλατφόρμα υποστήριξης και διαχείρισης Smart card. Παρέχεται ένα φιλικό προς τον χρήστη περιβάλλον και ένα πλήθος δυνατοτήτων εκμετάλλευσης των προτερημάτων των Smart Card. Χρήση της κάρτας για διαχείριση πιστοποιητικών και κλειδιών, έλεγχος κατάστασης της κάρτας όπως επίσης δίνεται η δυνατότητα δημιουργίας και επεξεργασίας του προφίλ χρήσης του προγράμματος.

6.2 Gamsafe Log on

Το Windows Secure Logon (Interactive logon με smart card), είναι μια δυνατότητα επέκτασης της ασφαλείας ενός σταθμού εργασίας ενσωματώνοντας στον έλεγχο πρόσβασης- ταυτοποίηση χρήστη την χρήση smart card, κοινώς οι χρήστες κάνουν log in στα Windows με την χρήση της κάρτας τους και όχι με το pin τους. Οι GemSafe Libraries υποστηρίζουν αυτήν την δυνατότητα υλοποιώντας την αυτόματα.

7. Χρήση των περιεχόμενων των Smart card από ξένες εφαρμογές

Οι Gemsafe libraries συνδυάζονται με την βιβλιοθήκη winscard.dll και παρέχουν διασύνδεση με τον Card Reader σαν συσκευή ασφαλείας στο λειτουργικό σύστημα. Όπως επίσης παρέχεται ελεγχόμενη πρόσβαση στα πιστοποιητικά που είναι καταχωρημένα στην κάρτα. Οι περιπτώσεις χρήσης των καρτών που εξεταστήκαν είναι με τον Mozilla Firefox, ο Mozilla Thunderbird ως συσκευή ασφαλείας και με Adobe Acrobat, το οποίο αναγνωρίζει αυτόματα (από το Reg tool) τα καταχωρημένα πιστοποιητικά. Στον Thunderbird και στον Acrobat δίνεται η δυνατότητα υπογραφής και κρυπτογράφησης των e-mail και κειμένων αντίστοιχα.

8. Περιγραφή εφαρμογής διαχείρισης καρτών

Η εφαρμογή Card Manager, είναι μία μικρή εφαρμογή ελέγχου πρόσβασης σε μια βάση δεδομένων, παραλληλίζοντας την χρήση της κάρτας με την απλή εισαγωγή όνομα χρήστη και κωδικού πρόσβασης. Η εφαρμογή εκμεταλλεύεται ελάχιστες από τις δυνατότητες ασφαλείας των smart card. Ο κύριος σκοπός της ανάπτυξης της εφαρμογής ήταν μια προσπάθεια εξοικείωσης με το προγραμματιστικό περιβάλλον στα πλαίσια της ανάπτυξης ασφαλών εφαρμογών με smartcard. Η υλοποίηση γίνε σε γλώσσα java στην πλατφόρμα NetBeans. Με την βοήθεια του API της java (v1.6) javax.smartcardio*.

9. Συμπεράσματα

Οι smart cards, είναι ένα εργαλείο υποστήριξης – αναβάθμισης ενός ευρύτερου συστήματος ασφαλείας είτε αυτό είναι τραπεζικό είτε σταθμός εργασίας είτε δίκτυο υπολογιστών. Το βέβαιο είναι ότι οι smart cards είναι αρκετά ασφαλείς και εκ φύσεως ενδυναμώνουν και την ασφάλεια του συστήματος που τις υιοθετεί. Η σύγκριση με τις μαγνητικές κάρτες είναι περιττή, το επίπεδο δυνατοτήτων των μαγνητικών καρτών είναι πρωτόγονο σε σχέση με το επίπεδο των έξυπνων καρτών. Οι αναγνώστες έξυπνων καρτών:

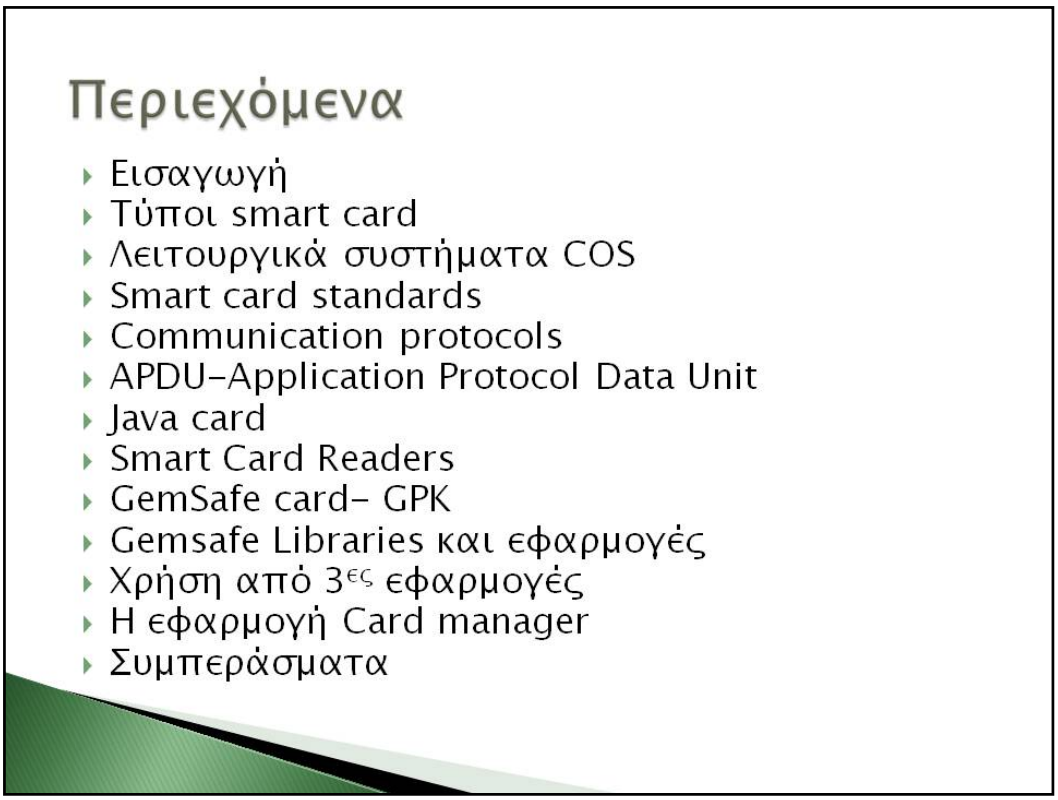
- Smart card reader
  Είναι αρκετά εξελιγμένοι οι σύγχρονοι card reader και η τιμή τους έχει μειωθεί

αισθητά και είναι πλέον προσιτή.

- Οι GamSafe libraries
  Αποτελούν μια ολοκληρωμένη εφαρμογή που καλύπτει πλήρως το πεδίο της διαχείρισης των έξυπνων καρτών.
- Οι 3^{ες} εφαρμογές:
  Η χρήση των καρτών από τρίτες εφαρμογές αποτελεί μια διαδικασία ιδιαίτερα ασφαλή και εύκολη.
- Η ανάπτυξη μίας εφαρμογής:

Όσο αφορά το προγραμματιστικό περιβάλλον των έξυπνων καρτών, κυρίως λόγο της πολυπλοκότητας των προτύπων, η ανάπτυξη μίας εφαρμογής ή ο προγραμματισμός μίας κάρτας αποτελούν δύσκολα έργα για μικρές ομάδες ανάπτυξης. Αντιθέτως η χρήση από τον τελικό χρήστη (cardholder) μπορεί να είναι πολύ απλή και εύκολη, συναρτήσει πάντα με τις διαδικασίες που εκτελεί ο χρήστης. Αλλά συνήθως οι συναλλαγές και ο έλεγχος ταυτότητας είναι πολύ απλές διαδικασίες λόγω του ότι συνηθίζεται στα συστήματα έξυπνων καρτών να κρύβεται η πολυπλοκότητα από τον τελικό χρήστη.

Παράρτημα IV – Παρουσίαση



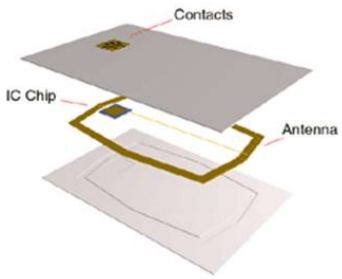
Εισαγωγή

- Ορισμός
- Βασικά χαρακτηριστικά
- Πλεονεκτήματα – μειονεκτήματα

Τύποι smart card

- Read –write
  1. Contact Cards
  2. Contactless Cards
  3. Combination Cards
- Chip

1. Memory Cards
   - Straight
   - Protected
   - Stored Value
2. CPU/MPU Microprocessor Multifunction Cards



Λειτουργικά συστήματα COS

- Fixed File Structure
- Dynamic Application System

Smart card standards

- ISO 7816
- FIPS
- EMV
- PC/SC
- CEN και ETSI
- HIPAA

Communication protocols

- Character protocol (T=0)
- Block protocol (T=1)
- Custom protocol (T=14)

APDU–Application Protocol Data Unit

Command Format

GPK cards accept commands in the following format:

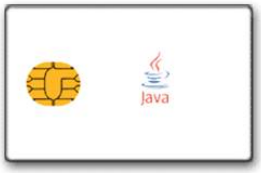
Header				Body		
CLA	INS	P1	P2	Lc	Parameters/Data	Le

Response Format

GPK cards return responses to commands in the following format:

Body	Trailer
Data	SW1, SW2

Java card



- Portability
- Security
- Java Card versus Java

Smart Card Readers

- Ορισμός
- Προδιαγραφές

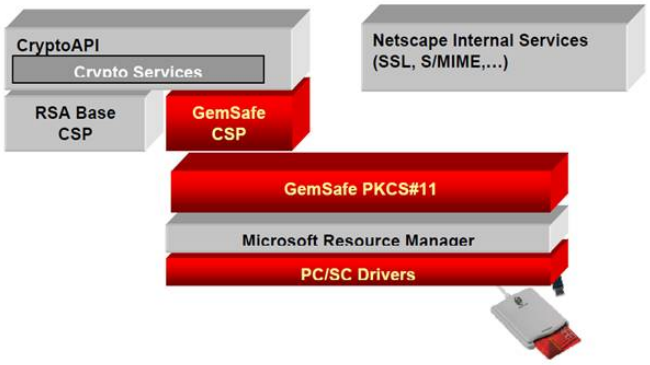
GemSafe card– GPK

- GamSafe Card

- GPK OS

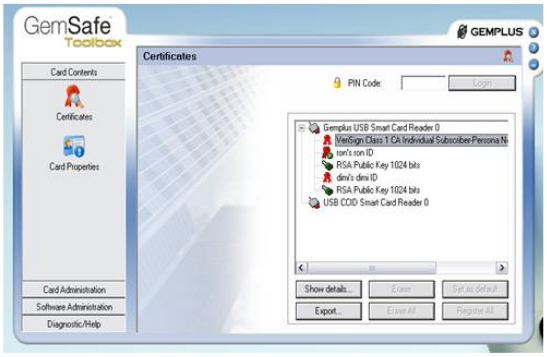
Gemsafe Libraries

- Libraries architecture



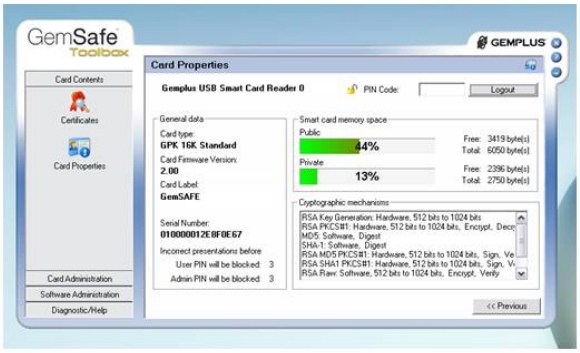
GemSafe Toolbox 1/5

- Certificates



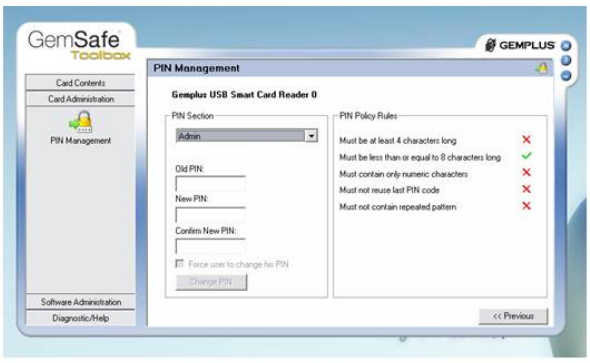
GemSafe Toolbox 2/5

- Card contents



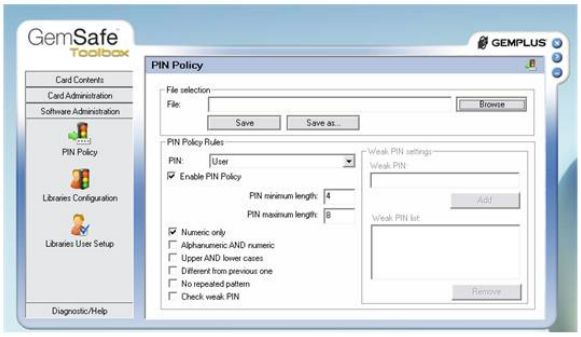
GemSafe Toolbox 3/5

- Pin administration



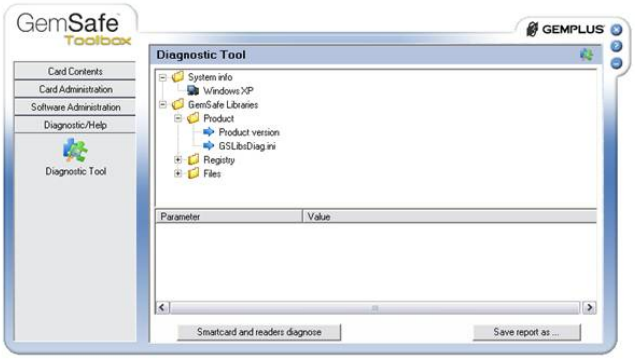
GemSafe Toolbox 4/5

- Pin Policy – Libraries configuration



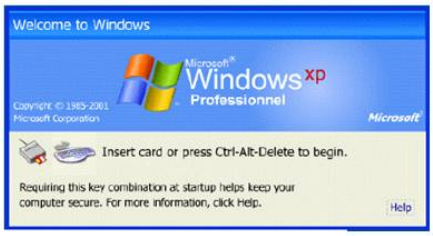
GemSafe Toolbox 5/5

- Diagnose and help



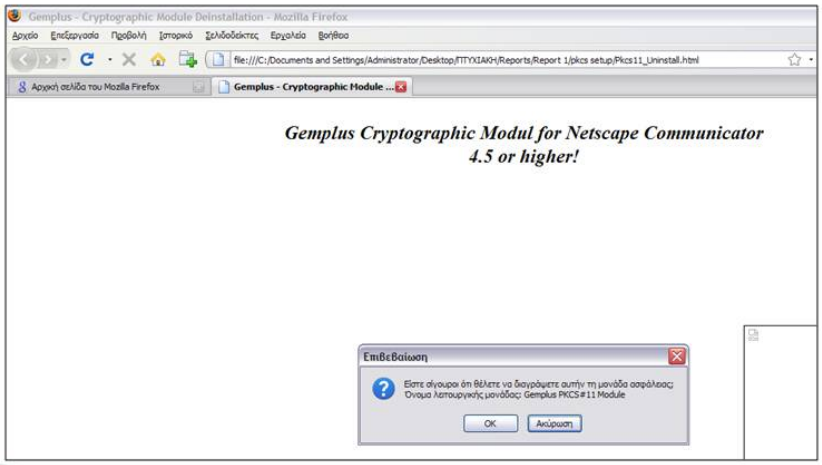
Windows secure Log on

- Interactive logon με smart card



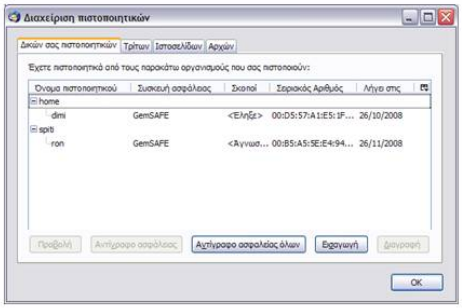
Χρήση από 3ες εφαρμογές 1/3

- Mozilla Firefox



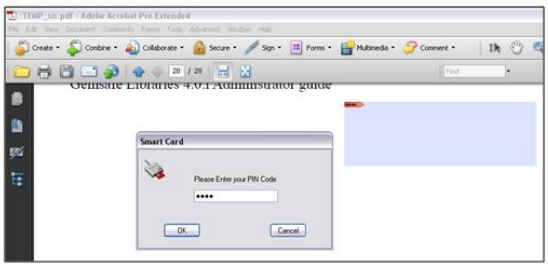
Χρήση από 3ες εφαρμογές 2/3

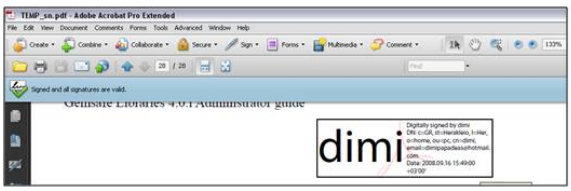
- Mozilla Thunderbird



Χρήση από 3ες εφαρμογές 3/3

- Adobe Acrobat





Η εφαρμογή Card manager 1/3

USE CASES:

- Ανάγνωση Smart Card
- Έλεγχος κάρτας
- Ταυτοποίηση χρήστη και κάρτας
- Αλληλεπίδραση με βάση δεδομένων(java DB Derby)
- Καταχώρηση νέου χρηστή κάρτας (Cardholder)
- Υποτυπώδης διαχειριστής γεγονότων εισαγωγής και εξαγωγής Smart Card
- Αναγνώριση συνδεδεμένων Card reader
- Εναλλαγή default smart card reader

Η εφαρμογή Card manager 2/3

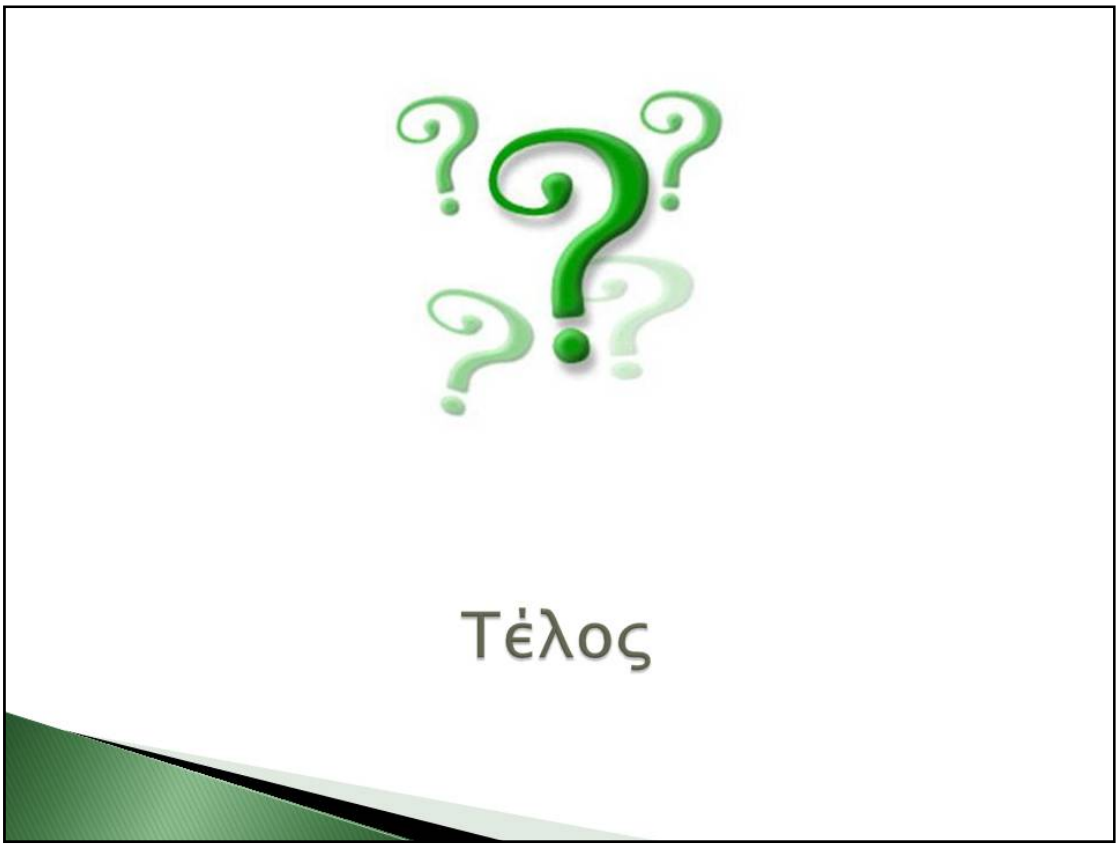
- User log in

Η εφαρμογή Card manager 3/3

- Main panel

Συμπεράσματα

- Smart Cards
- Smart Card Readers
- GamSafe libraries
- 3^{ες} εφαρμογές
- Η ανάπτυξη της εφαρμογής Card manager


Τέλος

Βιβλιογραφία

GPK16000 Reference Manual, GEMPLUS April 2001
GEMPLUS, B.P. 100, 13881 GEMENOS CEDEX, FRANCE.
Tel: +33 (0)4.42.36.50.00 Fax: +33 (0)4.42.36.50.90
Document Version 4.0
Document Reference: DPD05030D0

Gemsafe Libraries 4.0.i Administrator guide
GEMPLUS, B.P. 100, 13881 GEMENOS CEDEX, FRANCE.
Tel: +33 (0)4.42.36.50.00 Fax: +33 (0)4.42.36.50.90
Printed in France. Document Reference:DOC112108B
Document Version: 2.1
May 31 2005

Gemsafe Libraries 4.0.i user guide
GEMPLUS, B.P. 100, 13881 GEMENOS CEDEX, FRANCE.
Tel: +33 (0)4.42.36.50.00 Fax: +33 (0)4.42.36.50.90
Printed in France. Document Reference:DOC112110B
Document Version: 2.1
May 31 2005

Πλήρες Εγχειρίδιο της Java 6
Εκδόσεις Μ.Γκιούρδας 2002 - 2008, All rights reserved
Ζωοδόχου πηγής 74 –Τηλ. 210-3630219
106 81 Αθήνα, 10/2007
ISBN: 9605125382

Εισαγωγή στην Java 2. Ένας ολοκληρωμένος και εύχρηστος οδηγός της γλώσσας
Συγγραφέας: Λιακέας Γιώργος
Εκδότης: Κλειδάριθμος
Στουρνάρη 27Β
Αθήνα 106 82
ISBN: 960-209-625-X

JAVA - ΠΡΟΧΩΡΗΜΕΝΕΣ ΤΕΧΝΙΚΕΣ
Συγγραφέας: Τάνια Α. Κερκίρη
Εκδότης: Κλειδάριθμος
Στουρνάρη 27Β
Αθήνα 106 82
ISBN:960-209-900-3

Smart card - From Wikipedia, the free encyclopedia
http://en.wikipedia.org/wiki/Smart_card

Gemalto: the world leader in digital security
http://www.gemalto.com/

Smartcard Basics
http://www.smartcardbasics.com

Smart Card tutorial

http://www.ee.umanitoba.ca/~kinsner/whatsnew/tutorials/tu1999/smcards.html
http://www.smartcard.co.uk/tutorials/sct-itsc.pdf

The Berlin Group
http://www.berlin-group.org/

Smart Card Alliance
www.smartcardalliance.org/

RSA Laboratories
http://www.rsa.com/rsalabs/

The ISO 7816 - From Wikipedia, the free encyclopedia
http://en.wikipedia.org/wiki/ISO_7816

The ISO 7816 Smart Card Standard overview
http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816.aspx

ISO/IEC 7816 Part 4: Inter industry command for interchange
http://www.ttfn.net/techno/smartcards/iso7816_4.html

Mozilla.org Security Glossary
http://www.mozilla.org/projects/security/pki/psm/help_21/glossary.html#1028962

Apduview
http://www.fernandes.org/apduview/index.html

Οι κυριότεροι κατασκευαστές καρτών:

Giesecke & Devrient GmbH
http://www.gdm.de/

Bull
http://www.cp8.bull.net/products/prosca.htm

Gemplus
http://www.gemplus.com/

Hewlett-Packard
http://www.hp.com/

Schlumberger
http://www.slb.com/smartcards/
Solaic
http://www.winforms.phil.tu-bs.de

Siemens Nixdorf
http://www.sni.de/

IBM
http://www.ibm.com/

Microsoft
http://www.microsoft.com/smartcard/

Οι κυριότεροι κατασκευαστές ολοκληρωμένων κυκλωμάτων :

SGS Thomson
http://us.st.com/stonline/

Siemens
http://www.siemens.com/

Motorola
http://www.mot.com/

EMVCo
http://www.emvco.com

FIPS (Federal Information Processing Standards
http://www.itl.nist.gov/

PC/SC Workgroup
http://www.pcscworkgroup.com

ISO
http://www.iso.org/iso/home.htm

Comite' Europeen de Normalisation
http://www.cen.eu

European Telecommunications Standards Institute
www.etsi.org

Health Insurance Portability and Accountability Act
http://www.hipaa.org

Java™ Smart Card I/O API, Package javax.smartcardio description
http://java.sun.com/javase/6/docs/jre/api/security/smartcardio/spec/javax/smartcardio/package-summary.html

Java™ Smart Card I/O API
http://jcp.org/en/jsr/detail?id=268

Netbeans IDE
www.**netbeans**.org/

Eclipse IDE

http://www.eclipse.org/

Java card - From Wikipedia, the free encyclopedia
http://en.wikipedia.org/wiki/Java_Card

Java card - sun
http://java.sun.com/javacard/

Java Card
http://www.javasoft.com/javacard

TEO BY XIRING V.2 – 01/06/2007
http://www.infoestrutura.com.br/download/book_teo_by_xiring_eng.pdf