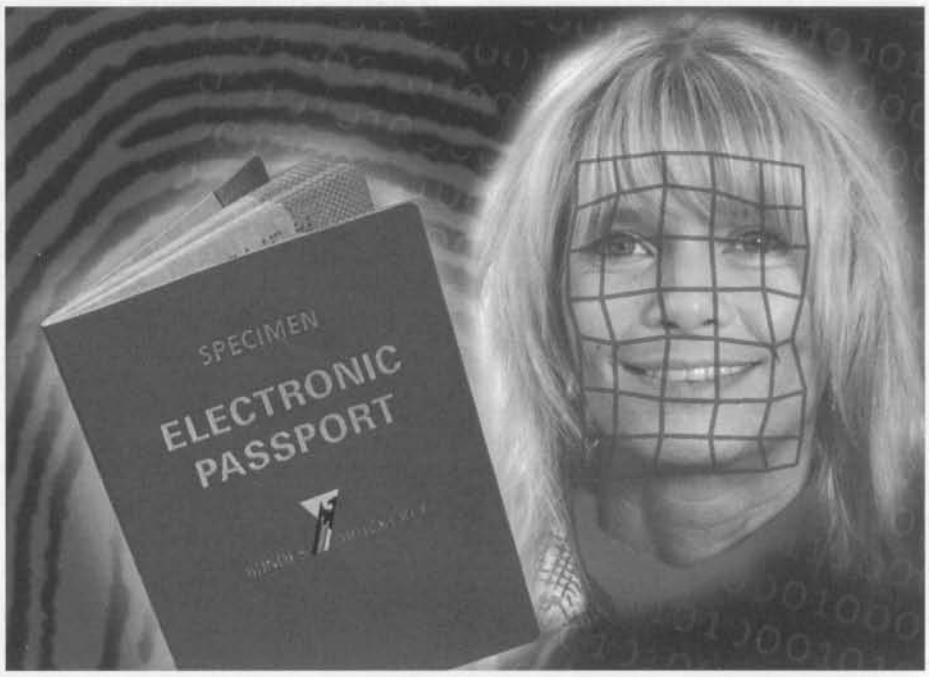
Ηλεκτρονικά διαβατήρια

Θα είναι σίγουρα ασφαλή;

Από τον Gerhard Schalk, της Philips Αυστρίας



Εάν το διαβατήριό σας λήγει μέσα στους επόμενους μήνες, το επόμενο διαβατήριο που θα πάρετε στα χέρια σας θα ανήκει στα ηλεκτρονικά διαβατήρια που μέσα στην φετινή χρονιά θεσπίζονται σε όλες τις χώρες της Ευρωπαϊκής Ένωσης. Τα ηλεκτρονικά διαβατήρια έχουν ενσωματωμένη μία ετικέτα RFID στην οποία έχουν καταχωρηθεί προσωπικές πληροφορίες, και την οποία οι υπάλληλοι ελέγχου θα μπορούν να διαβάσουν εξ' αποστάσεως. Ελπίζουμε βέβαια ότι μόνον οι αρμόδιοι θα έχουν πρόσβαση σε αυτή την ηλεκτρονική συνομιλία...

Σύμφωνα με τα σχέδια των αρμοδίων της Ε.Ε., η εφαρμογή του ηλεκτρονικού διαβατηρίου θα γίνει σταδιακά μέσα στους επόμενους μήνες, με καταληκτική ημερομηνία το τέλος Αυγούστου, όπου όλα τα παλαιού τύπου διαβατήρια αναμένεται να καταργηθούν. Κάτι ανάλογο ισχύει και για την Ελλάδα, και από τις αρχές Αυγούστου προβλέπεται να αρχίσει η έκδοση των ηλεκτρονικών διαβατηρίων, η σταδιακή εφαρμογή των οποίων θα διαρκέσει -πιθανόν- μέχρι το τέλος Σεπτεμβρίου οπότε και αναμένεται να καταργηθούν τα παλαιού τύπου διαβατήρια. Το ζήτημα των βιομετρικών δεδομένων, η προστασία αυτών και το ποιας μορφής ακριβώς προσωπική πληροφορία θα αποθηκεύεται στα ηλεκτρονικά διαβατήρια, έχει απασχολήσει σημαντικά πολύ κόσμο.

Τα ηλεκτρονικά λοιπόν διαβατήρια που έχουν αυτή τη στιγμή αρχίσει να εκδίδονται, περιλαμβάνουν την ίδια ακριβώς πληροφορία όσον αφορά τα προσωπικά δεδομένα με αυτή που είχαν και τα παλιά: όνομα, τόπος και ημερομηνία γέννησης, και μία εικόνα του κατόχου σε μορφή JPEG με μέγεθος 15 kByte. Εάν εξαιρέσουμε την εικόνα, όλα τα υπόλοιπα δεδομένα βρίσκονται ήδη σε μία ειδική περιοχή αναγνώσιμη από ειδικές συσκευές στους χώρους ελέγχου των τελωνείων, την καλούμενη "Μηχανικά Αναγνώσιμη Ζώνη" (Machine Readable Zone, MRZ). Από το 2007 και μετά, υπολογίζεται ότι στο διαβατήριο θα αποθηκεύεται και το δακτυλικό αποτύπωμα του δεξιού και αριστερού δείκτη.

Η πληροφορία αυτή αποθηκεύεται με ψηφιακή μορφή σε μία μικροσκοπική ετικέτα τύπου RFID, η οποία ενσωματώνεται στο διαβατήριο. Υπάρχουν διάφοροι κατασκευαστές οι οποίοι παράγουν ανάλογες ετικέτες ασφάλειας, αλλά η P5CD072 που παράγεται από την Philips (ένα παράγωγο της οικογενείας "Smart MX Secure Smart Card Controller"), [1] είναι η πλέον διαδεδομένη στον χώρο και τα τρία τέταρτα περίπου των χωρών που εφαρμόζουν τα ηλεκτρονικά διαβατήρια επιλέγουν το ολοκληρωμένο της Philips. Ένας ανταγωνιστής της Philips είναι η Γερμανική εταιρεία Infineon με το ολοκληρωμένο SLE66CLX641 το οποίο χρησιμοποιείται σε ορισμένα Γερμανικά διαβατήρια. Σε πολλές πάντως περιπτώσεις, οι αρμόδιες αρχές συντάσσουν συμβόλαια με περισσότερους του ενός προμηθευτές, έτσι ώστε να έχουν εξασφαλισμένη και μία δεύτερη πηγή εξαρτημάτων. Η εν δυνάμει αγορά των συγκεκριμένων ολοκληρωμένων είναι τεράστια, και η Infineon υπολογίζει ότι μόνον στην Γερμανία και στην χρονιά αυτή, θα εκδοθούν περίπου 2,4 εκατομμύρια διαβατήρια Σε παγκόσμια κλίμακα, το συγκεκριμένο μέγεθος αναμένεται να φθάσει τα 125 εκατομμύρια.

Οι ελεγκτές των έξυπνων καρτών (Smart Card Controllers) με διασύνδεση προσέγγισης (χωρίς επαφές), είναι παρόμοιοι με τις ετικέτες RFID αλλά διαθέτουν ένα πολύ υψηλότερο βαθμό ασφάλειας, ανάλογο με αυτό των τραπεζικών καρτών που χρησιμοποιούν διασύνδεση με οκτώ επαφές. Η παραγωγή του λογισμικού για τα ολοκληρωμένα ελέγχεται με ιδιαίτερη αυστηρότητα από τις χώ-

ρες που ξεκινούν την χρήση του ηλεκτρονικού διαβατηρίου, όπως επίσης και οι προδιαγραφές των ίδιων των ολοκληρωμένων διαφυλάσσονται ως κόρη οφθαλμού και μόνον μία περίληψη των προδιαγραφών αυτών διατίθεται από τους κατασκευαστές.

Οι βασικές τεχνικές προδιαγραφές των ηλεκτρονικών διαβατηρίων δημιουργήθηκαν από τον Διεθνή Οργανισμό Πολιτικής Αεροπορίας (International Civil Aviation Organization, ICAO), ο οποίος αποτελεί μέλος της οικογενείας των οργανισμών των Ηνωμένων Εθνών. Στο κείμενο που παρήχθη προδιαγράφεται ένα ταξιδιωτικό διαβατήριο αναγνώσιμο από ειδικές συσκευές, και το διαβατήριο αυτό αναμένεται μάλιστα να εφαρμοστεί παγκοσμίως. Ολόκληρο το κείμενο με τις προδιαγραφές του ICAO διατίθεται ελεύθερα στον δικτυακό τόπο του ICAO [3]. Στο πρότυπο αυτό καθορίζεται η παγκόσμια δια-λειτουργικότητα των μηχανικά αναγνώσιμων ταξιδιωτικών εγγράφων.

Το ολοκληρωμένο των έξυπνων καρτών

Ένα ελεγκτής έξυπνων καρτών είναι κατ' αρχήν ένας εξειδικευμένος τύπος μικροελεγκτή ο οποίος είναι σε θέση να αποθηκεύσει με ασφάλεια ευαίσθητες πληροφορίες, ενώ διαθέτει και ένα ενσωματωμένο συνεπεξεργαστή ο οποίος διευκολύνει τους απαραίτητους υπολογισμούς για την διαχείριση των κρυπτογραφημένων δεδομένων. Το Λειτουργικό Σύστημα της Κάρτας (Card Operating System, COS) αποθηκεύεται στην ROM και η ασφάλεια των δεδομένων αυτών είναι μέγιστη, με σκοπό την ορθή εκτέλεση της εφαρμογής (λογισμικού) και την αξιοπιστία των αποθηκευμένων δεδομένων. Το ολοκληρωμένο P5CD072 της έξυπνης κάρτας, είναι ένας ελεγκτής διπλής διασύνδεσης και υψηλής ασφαλείας με μνήμη 160 KByte ROM, 4,6 KByte RAM και 72 KByte EEPROM. Η διπλή διασύνδεση σημαίνει ότι το ολοκληρωμένο έχει δύο τρόπους επικοινωνίας με τον έξω κόσμο: είτε μέσω επαφών (σαν αυτές που έχουν οι έξυπνες πιστωτικές κάρτες), είτε χωρίς επαφές (προσέγγιση) όπου χρησιμοποιείται μία κεραία για να λάβει τροφοδοσία και να αποστείλει δεδομένα. Η Κεντρική Μονάδα Επεξεργασίας (CPU) διαθέτει ένα δείκτη δεδομένων (DPTR) 24 ψηφίων, ο οποίος είναι σε θέση να διευθυνσιοδοτήσει ένα μέγεθος μνήμης της τάξης των 16 Mbyte. Το σύνολο εντολών του επεξεργαστή είναι πλήρως συμβατό με αυτό του 8051, αλλά διαθέτει και κάποιες επιπρόσθετες εντολές, με σκοπό να επιτυγχάνει ταχύτερη διευθυνσιοδότηση μνήμης για τον κρυπτογραφικό συνεπεξεργαστή, μαζί με κάποιες ειδικές εντολές που υποστηρίζουν το Λειτουργικό σύστημα της έξυπνης κάρτας.

Η ανάπτυξη προγραμμάτων για την οικογένεια ελεγκτών "SmartMX" γίνεται με την βοήθεια ενός ειδικού assembler/compiler ο οποίος παράγεται από τον εξειδικευμένο οίκο ανάπτυξης λογισμικού Keil. Στην προσπάθεια βελτιστοποίησης του παραγόμενου κώδικα (μικρότερη χρήση μνήμης και υψηλότερη ταχύτητα εκτέλεσης), μέρος του λειτουργικού συστήματος ή ακόμη και ολόκληρο, εισάγονται στον συμβολομεταφραστή (assembler). Ο παραγόμενος κώδικας (πρόγραμμα), πριν "καεί" στην ROM, υποβάλλεται σε εξαντλητικές δοκιμές μέσω εξομοιωτών που παράγουν οι Keil ή Ashling.

Παρόμοια με τις μονάδες έξυπνων καρτών που προέρχονται από άλλους κατασκευαστές, τα φυλλάδια δεδομένων, οι σημειώσεις εφαρμογών, τα παραδείγματα ανάπτυξης κώδικα καθώς και τα εργαλεία ανάπτυξης δεν διατίθεται σε μη εξουσιοδοτημένα άτομα. Το μόνο που μπορεί κανείς να κατεβάσει από τον δικτυακό τόπο του κατασκευαστή, είναι μία μικρή φόρμα με τις προδιαγραφές [1].

Διασύνδεση χωρίς επαφές

Η έξυπνη κάρτα που χρησιμοποιείται στις πιστωτικές κάρτες, για να αποκαταστήσει επικοινωνία με το μηχάνημα της τράπεζας χρησιμοποιεί οκτώ ίχνη τα οποία αποτελούν τις επαφές για τα VDD, GND, IO1 έως IO3, CLK και RST. Το ηλεκτρονικό διαβατήριο από την άλλη δεν χρησιμοποιεί επαφές αλλά μία διασύνδεση προσέγγισης η οποία είναι συμβατή με το πρότυπο ISO/IEC14443.

Στην θέση των οκτώ επαφών που χρησιμοποιεί η πλειονότητα των έξυπνων καρτών της αγοράς, η Philips ανάπτυξε ένα μικροσκοπικό ολοκληρωμένο χωρίς επαφές (Σχήμα 1), το οποίο έχει πάχος μόλις 320 μm. Πρόκειται για μία στιβαρή μονάδα η οποία είναι αρκούντως μικρή για να "χωνευθεί" στο διαβατήριο. Επάνω στο ολοκληρωμένο υπάρχουν δύο ίχνη (τα LA και LB), στα οποία προσαρμόζεται η κεραία. Πριν τοποθετηθεί στο διαβατήριο (Σχήμα 2), το ολοκληρωμένο συνδέεται με την κεραία και το όλο σύστημα τοποθετείται σε ένα ειδικό φορέα.

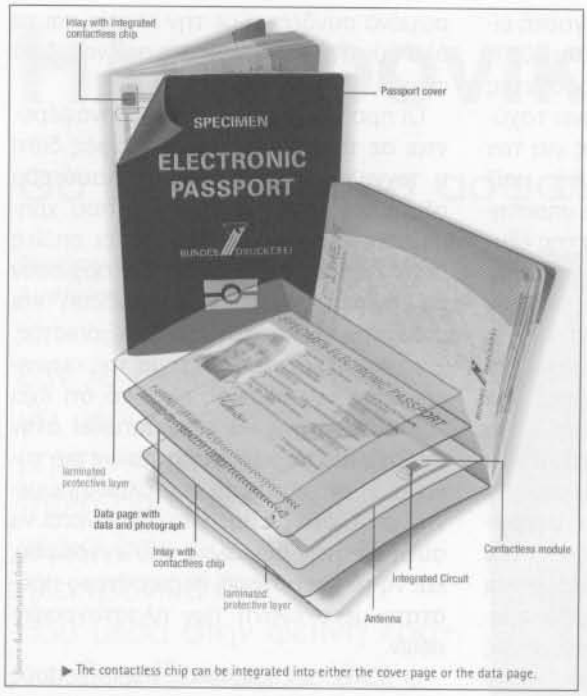
Οι προδιαγραφές του ICAO αναφέρονται σε τεχνολογία χωρίς επαφές διότι η τεχνολογία αυτή είναι περισσότερο αξιόπιστη από ένα σύστημα που χρησιμοποιεί μηχανικές επαφές, οι οποίες μετά από κάποια χρήση θα αρχίσουν να υποφέρουν από "κακή σύνδεση" και ενδέχεται να καταλήξουν αναξιόπιστες. Ένα επί πλέον πλεονέκτημα της συγκεκριμένης τεχνολογίας είναι το ότι έχει την δυνατότητα να ενσωματωθεί στην υπάρχουσα μορφή διαβατηρίων πιο εύκολα. Η ενσωμάτωση του ολοκληρωμένου μέσα στο διαβατήριο αναμένεται να αυξήσει στην ασφάλεια του εγγράφου, και να το καταστήσει περισσότερο προστατευμένο έναντι των πλαστογραφήσεων.

Ο ICAO δεν επιβάλλει περιορισμούς όσον αφορά το που θα πρέπει να τοποθετηθεί το ολοκληρωμένο, οπότε ανάλογα με την χώρα έκδοσης του διαβατηρίου μπορεί να το βρούμε ενσωματωμένο είτε σε κάποιο εσώφυλλο είτε στο εξώφυλλο αυτού.

Η επικοινωνία

Η τροφοδοσία και η μεταφορά δεδομένων στην έξυπνη κάρτα, γίνονται με τον ίδιο τρόπο που υλοποιούνται και στις κανονικές ετικέτες RFID, μέσω μίας κεραίας και ενός κυκλώματος αποκωδικοποίησης. Το πρότυπο ISO/IEC14443 καθορίζει την μεταφορά δεδομένων μεταξύ των καλούμενων "καρτών προσέγγισης" και της συσκευής ανάγνωσης. Η μέγιστη απόσταση της κάρτας από το σύστημα ανάγνωσης θα πρέπει να είναι 10 cm. Το συγκεκριμένο σημείο των προδιαγραφών (πέρα από το πρωτόκολλο επικοινωνίας) είναι πανομοιότυπο με το βιομηχανικό πρότυπο διασύνδεσης της Mifare® (Σχήμα 3). Η συσσωρευμένη εμπειρία που έχει αποκτηθεί από τα περισσότερα των 500 εκατομμυρίων συγκεκριμένων ολοκληρωμένων της Philips που βρίσκονται ήδη σε χρήση, εξασφαλίζει αν μη τι άλλο την αξιοπιστία της συγκεκριμένης μεθόδου μεταφοράς δεδομένων.

Πριν ξεκινήσει οποιαδήποτε επικοινωνία με την έξυπνη κάρτα, το τερματικό ανάγνωσης εκπέμπει ένα ηλεκτρο-μαγνητικό πεδίο υψηλής συχνότητας το οποίο ανιχνεύεται από οποιαδήποτε έξυπνη κάρτα βρεθεί στην περιοχή κάλυψης. Το φέρον στην συχνότητα των

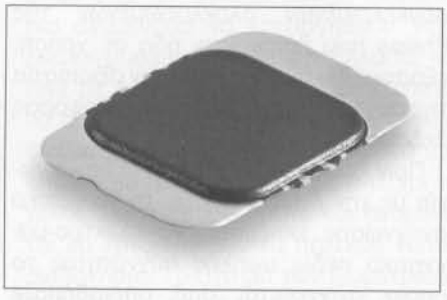


Σχήμα 1. Το ολοκληρωμένο και το πηνίο της κεραίας τοποθετούνται σε ένα ειδικό φύλλο. (φώτο: Bundesdruckerei [8]).

13,56 MHz επάγει ενέργεια στην έξυπνη κάρτα, η οποία στην συνέχεια αποθηκεύεται για να τροφοδοτήσει το ολοκληρωμένο. Η μέθοδος διαμόρφωσης του σήματος από την συσκευή ανάγνωσης προς το διαβατήριο είναι 100 % ASK (Amplitude Shift Keying), και η πληροφορία μεταφέρεται απλά ενεργοποιώντας και απενεργοποιώντας το φέρον. Η συγκεκριμένη μέθοδος διαμόρφωσης, μπορεί πολύ εύκολα και αξιόπιστα να αποκωδικοποιηθεί από την έξυπνη κάρτα που βρίσκεται στο διαβατήριο.

Τα δεδομένα από το διαβατήριο προς την συσκευή ανάγνωσης χρησιμοποιούν διαμόρφωση φόρτου με υπο-φέρον, όπου η συχνότητα του υπο-φέροντος είναι 847 kHz (13,56 MHz/16). Η διαμόρφωση του υπο-φέροντος επιτυγχάνεται μετάγοντας το εντός και εκτός. Η μεταφορά δεδομένων για τα διαβατήρια, είναι επί του παρόντος ορισμένη στα 106, 212 και 424 kbit/s. Όλες οι επικοινωνίες οργανώνονται υποχρεωτικά σε μία κατάσταση κύριου και εξαρτώμενου (master/slave), όπου η συσκευή ανάγνωσης έχει τον ρόλο του κύριου (master).

Στο IS014443 καθορίζεται η ισχύς του πεδίου η οποία πρέπει να είναι μεταξύ 1,5 A/m και 7,5 A/m. Με τις τιμές αυτές, σε μία κάρτα σε απόσταση 10 cm επάγεται μία ισχύς περίπου 5 mW, η οποία ισχύς χρησιμοποιείται για να ενεργοποιήσει την CPU και τον συνεπεξεργαστή του P5CD072.



Σχήμα 2. Ο ελεγκτής της έξυπνης κάρτας έχει πλάτος μόλις 0,32 mm. (Philips).

Το υλικό του ολοκληρωμένου

Στο Σχήμα 4 εικονίζεται το σχηματικό διάγραμμα του P5CT072, όπου μπορούμε να δούμε ότι περιλαμβάνονται και κάποια μπλοκ που δεν θα βλέπαμε σε ένα τυπικό μικροελεγκτή: η διασύνδεση RF, η Μονάδα διασύνδεσης χωρίς επαφές (Contact-less Interface Unit, CIU) και η γεννήτρια CRC16. Όλα τα προαναφερθέντα χρησιμοποιούνται για την χωρίς επαφές σειριακή επικοινωνία με το υλικό του αναγνώστη. Η CIU, είναι ένα ειδικό-χωρίς επαφές ISO 14443 UART.

Με την βοήθεια του εξειδικευμένου υλικού, ο συνεπεξεργαστής 3DES είναι σε θέση να κωδικοποιήσει ή απο-κωδικοποιήσει ένα μήνυμα 3DES μεγέθους 8 ψηφιολέξεων σε 25 μs. Ο συνεπεξεργαστής "FameXE PKI" είναι ένας ειδικός μαθηματικός συνεπεξεργαστής ο οποίος είναι βελτιστοποιημένος για να υπολογίζει μερικούς από τους πλέον δημοφιλείς αλγόριθμους ασύμμετρης κρυπτογράφησης, όπως οι RSA (Rivest, Shamir και Adleman) και ECC (Elliptic Curve Cryptography). Ο επεξεργαστής και ο συνεπεξεργαστής συνεργάζονται την ώρα που μεταφέρεται ο κρυπτογραφικός κώδικας, όπου ο επεξεργαστής είναι σε θέση να προετοιμάσει τους καταχωρητές για την αποθήκευση ενδιάμεσων τιμών που παράγονται από τον 32-μπιτο συνεπεξεργαστή κατά την διάρκεια των υπολογισμών. Κατά την διάρκεια επίσης των υπολογισμών αποκρυπτογράφησης του μηνύματος, χρησιμοποιείται και μία εξειδικευμένη ταχεία γεννήτρια τυχαίων αριθμών (RNG, Random Number Generator).

Η πρόσβαση στις μνήμες ROM, RAM και EEPROM επιτυγχάνεται από την μονάδα διαχείρισης μνήμης (Memory Management Unit, MMU). Με τον τρόπο αυτό επιτυγχάνεται η ανάπτυξη ενός τοίχους προστασίας (firewall) από υλικό (hardware), μεταξύ του πυρήνα του λειτουργικού συστήματος και όλων των υπολοίπων λειτουργιών του προγράμματος και της εφαρμογής. Ο επεξεργαστής υποστηρίζει δύο καταστάσεις λειτουργίας: ο μεν πυρήνας τρέχει σε "κατάσταση συστήματος" (system mode) και έχει απεριόριστη πρόσβαση στο υλικό, ενώ οι λειτουργίες που έχουν να κάνουν με την εφαρμογή όπως είναι οι ρουτίνες επικοινωνίας, το εσωτερικό σύστημα ενημέρωσης, οι υπολογισμοί κρυπτογράφησης ή οι λειτουργίες διαβατηρίου εκτελούνται σε "κατάσταση εφαρμογής" (application mode) και έχουν περιορισμένη πρόσβαση στις περιοχές μνήμης που τις αφορούν και καθόλου ή περιορισμένη πρόσβαση στο υλικό. Με τον τρόπο αυτό αποτρέπεται η πρόσβαση στην μνήμη και το υλικό από φυσικές παρεμβολές, παρείσακτο λογισμικό, ή ακόμη και από σφάλμα του λογισμικού.

Προστασία από Hacker

Χαρακτηριστικά ασφαλείας είναι ενσωματωμένα και στο υλικό του P5CT072. Υπάρχουν αισθητήρες που παρακολουθούν διαρκώς την τάση, την θερμοκρασία και τα όρια συχνοτήτων του ολοκληρωμένου, ενώ ένας αισθητήρας φωτός ανιχνεύει οποιεσδήποτε τεχνικές παραβίασης χρησιμοποιούν ισχυρό φωτισμό.

Κάποιες επί πλέον δικλείδες ασφαλείας παρέχουν προστασία έναντι παραβιάσεων (cracking) του κώδικα, μέσω "Απλής Ανάλυσης Ισχύος" (Simple Power Analysis, SPA) ή "Διαφορικής Ανάλυσης Ισχύος (Differential Power Analysis, DPA). Οι συγκεκριμένες τεχνικές παραβίασης βασίζονται στο γεγονός ότι όταν μία πύλη CMOS εντός του ολοκληρωμένου μετάγεται από το 0 στο 1 αντλεί διαφορετικό ρεύμα απ' ότι εάν μεταγόταν από το 1 στο 0. Με την βοήθεια λοιπόν ενός παλμογράφου και με ανάλυση των σημάτων είναι δυνατόν να σχηματιστεί το "προφίλ ρεύματος" ενός μη προστατευμένου κυκλώματος , απ' όπου μπορεί κανείς να αντλήσει πληροφορίες σχετικά με τα κωδικοποιημένα δεδομένα. Για

Μπορούν τα προσωπικά δεδομένα να κλαπούν;

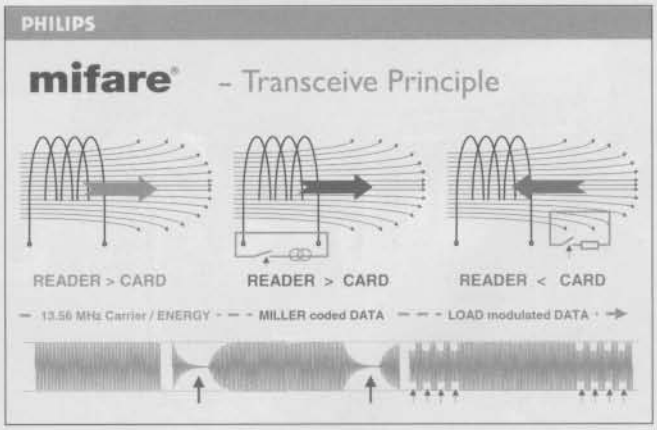
Στην αγορά έχουν ήδη αρχίσει να κυκλοφορούν ειδικά προστατευτικά καλύμματα για διαβατήρια [5], τα οποία είναι συνήθως κατασκευασμένα από αλουμίνιο και σκοπό έχουν την προστασία του διαβατηρίου από ενδεχόμενη λαθραία ανάγνωση της ετικέτας RFID. Τα συγκεκριμένα καλύμματα μπορεί να δείχνουν όμορφα και να διατηρούν το διαβατήριο σε άψογη κατάσταση, αλλά τελικά ο πραγματικός τους σκοπός είναι άλλος. Όσο το διαβατήριο είναι κλειστό, προστατεύεται και από ένα επί πλέον σύστημα, το Βασικό Σύστημα Ελέγχου (Basic Access Control, BAC) το οποίο αποτρέπει την ανάγνωση πριν ξεκινήσει η ανάγνωση δεδομένων από την ετικέτα, οι υπάλληλοι του τελωνείου είναι υποχρεωμένοι να ανοίξουν το διαβατήριο και να διαβάσουν με ένα οπτικό σαρωτή τις πληροφορίες που είναι αποθηκευμένες στην ειδική περιοχή MRZ. Κάποιες από τις πληροφορίες αυτές στην συνέχεια κωδικοποιούνται για να παραχθεί ένα κλειδί γνησιότητας, το οποίο αποστέλλεται προς την ετικέτα RFID για να την ενημερώσει ότι βρίσκεται στην περιοχή ενός εξουσιοδοτημένου γραφείου ελέγχου, οπότε και ελευθερώνεται η επικοινωνία της συσκευής ανάγνωσης με την κάρτα. Το γραφείο ελέγχου διαβατηρίων λοιπόν χρειάζεται εκτός από την συσκευή RFID και ένα οπτικό σαρωτή ο οποίος διαβάζει την "Μηχανικά Αναγνώσιμη Ζώνη" (Machine Readable Zone, MRZ). Το συγκεκριμένο σύστημα είναι προφανώς πιο ασφαλές από ένα απλό σειριακό αριθμό συνδεδεμένο με το διαβατήριο, όπως για παράδειγμα ο γνωστός αριθμός PIN της πιστωτικής μας κάρτας όπου αρκεί η καταχώριση του αριθμού για να επικυρωθεί μία εμπορική πράξη.

Μόλις αποκατασταθεί η επικοινωνία με την κάρτα, αρχίζει η ανταλλαγή πληροφοριών και τα δεδομένα κωδικοποιούνται με ένα τριπλό σύστημα DES (το μήκος του κλειδιού είναι 112 ψηφία) [4]. Το συγκεκριμένο σύστημα εξασφαλίζει ένα ικανοποιητικό επίπεδο ασφαλείας στην ανταλλαγή δεδομένων και αποτρέπει την υποκλοπή αυτών. Στην ανταλλαγή δεδομένων περιλαμβάνονται και κάποιες κωδικές λέξεις (checksum), οι οποίες αποτρέπουν την μη εξουσιοδοτημένη πρόσβαση στα δεδομένα.

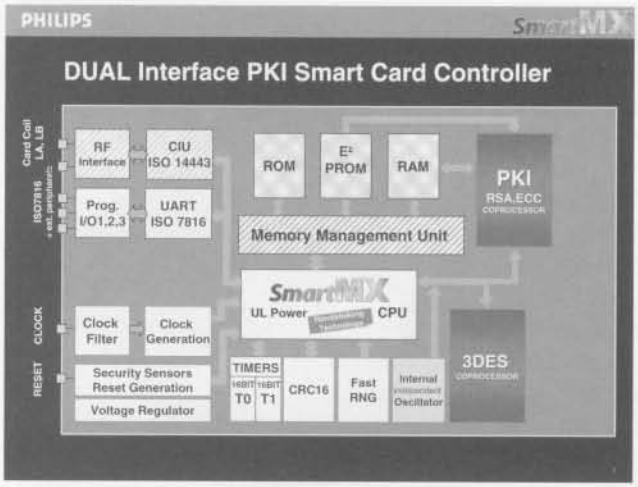
Από το 2007 αναμένεται στο σύνολο των προσωπικών δεδομένων που αποθηκεύονται στο διαβατήριο, να εισαχθούν και τα δακτυλικά αποτυπώματα. Αυτή η επί πλέον πληροφορία θα προστατεύεται από ένα αυξημένο επίπεδο ελέγχου πρόσβασης, το οποίο αναφέρεται ως "Εκτεταμένος Ελεγχος Πρόσβασης" (Extended Access Control, EAC). Το συγκεκριμένο σύστημα χρησιμοποιεί κρυπτογράφηση με δημόσια κλειδιά, μέσω των οποίων αναγνωρίζεται το κάθε σημείο ελέγχου και υπάρχει η δυνατότητα περιορισμού των προσωπικών δεδομένων τα οποία το κάθε σημείο ελέγχου είναι σε θέση να διαβάσει. Οι κατά τόπους λοιπόν αρχές έκδοσης διαβατηρίων θα χρησιμοποιούν το σύστημα EAC για να ελέγξουν το ποσοστό της πληροφορίας που μπορεί να αναγνώσει ένα σύστημα ελέγχου διαβατηρίων το οποίο για παράδειγμα βρίσκεται σε κάποια υπερατλαντική χώρα.

να αντιμετωπιστούν οι παρεμβάσεις αυτής της μορφής, το ολοκληρωμένο είναι σχεδιασμένο με τέτοιο τρόπο ώστε να αντλεί σταθερό ρεύμα ανεξάρτητα της εσωτερικής ροής δεδομένων, ενώ ταυτόχρονα ο επεξεργαστής και ο συνεπεξεργαστής εκτελούν "τυφλούς" υπολογισμούς με σκοπό να αυξήσουν την φαινόμενη "τυχαιότητα" της δραστηριότητας του επεξεργαστή.

Και η ίδια όμως η έξυπνη κάρτα είναι σχεδιασμένη με στόχο την αποτροπή μη εξουσιοδοτημένης ανάγνωσης ή διαχείρισης των δεδομένων. Τα μέρη του επεξεργαστή μέσα στο ολοκληρωμένο P5CT072 είναι κατανεμημένα με την τεχνική "glue logic", έτσι ώστε να μην είναι δυνατός ο εντοπισμός μίας μόνον περιοχής που να αποτελεί την CPU ή τον δίαυλο του συστήματος, ενώ τα διάφορα μέρη είναι μοιρασμένα γύρω από το ολοκληρωμένο με μία φαινομενικά ανοργάνωτη διάταξη. Με παρόμοιο τρόπο οι γραμμές διευθύνσεων, δεδομένων και ελέγχου προς τις ROM, EEPROM και RAM είναι ανακατεμένες έτσι ώστε οι περιοχές διευθύνσεων να μην είναι συνεχής αλλά να εμφανίζονται με τυχαίο τρόπο. Η περιοχή δηλαδή μνήμης 1001 δεν είναι απαραίτητο να έπεται της διεύθυνσης 1000. Η διάταξη αυτή παρέχει κάποια προστασία έναντι απλών προσπαθειών λήψης αντιγράφων της μνήμης. Κάθε φορά που το ολοκληρωμένο εκτελεί επανατοποθέτηση της μνήμης κατά την εκκίνηση, οι



Σχήμα 3. Η επικοινωνία μεταξύ του συστήματος ανάγνωσης και της έξυπνης κάρτας, βάσει της αρχής της Mifare. Κατά την ανάγνωση η κάρτα διαμορφώνει το σήμα του συστήματος φορτίζοντας το κύκλωμα συντονισμού. (Philips).



Σχήμα 4. Σχηματικό διάγραμμα του ελεγκτή της έξυπνης κάρτας (Philips).

διευθύνσεις των περιοχών της μνήμης RAM αναδιατάσσονται, με αποτέλεσμα μία κυψέλη μνήμης να μην αφορά την ίδια με προηγούμενα διεύθυνση. Το επίπεδο ασφαλείας που παρέχουν τα συγκεκριμένα ολοκληρωμένα έξυπνων καρτών (όπως επίσης και διαβατηρίων) εξαρτώνται από την απόλυτη ακεραιότητα της διαδικασίας κατασκευής του υλικού των ολοκληρωμένων και την σύνθεση των ίδιων των διαβατηρίων.

Έφτασε η ώρα του Μεγάλου Αδελφού;

Κατά την διαδικασία κατασκευής του κάθε ολοκληρωμένου RFID καθώς και των χωρίς επαφές ολοκληρωμένων των έξυπνων καρτών, μέσα στην EEPROM αποθηκεύεται ένας μοναδικός αριθμός ταυτοποίησης (Unique Identification number, UID). Στην περίπτωση όπου εντός του πεδίου ανίχνευσης του συστήματος ανάγνωσης καρτών παρουσιάζονται περισσότερες της μίας κάρτες, ο UID επιτρέπει στο σύστημα να ταυτοποιήσει την κάθε κάρτα χωριστά. Η επικοινωνία λοιπόν με την κάθε κάρτα μπορεί να γίνει επιλεκτική, και με τον τρόπο αυτό αποφεύγονται τυχόν συγκρούσεις στην ανταλλαγή δεδομένων (Anti-collision protection). Σε ένα διαβατήριο όμως, ο UID θα μπορούσε να συνδεθεί άμεσα με τον κάτοχό του. Ο συσχετισμός αυτός έχει απαγορευτεί για όλα τα Ευρωπαϊκά διαβατήρια και αντ' αυτού παράγεται ένας τυχαίος αριθμός UID, ο οποίος έχει ισχύ αντίστοιχη με την ισχύ του διαβατηρίου.

Τα νέα ηλεκτρονικά διαβατήρια μπορούν να καταστήσουν τους τελωνειακούς υπαλλήλους, εικόνες από το παρελθόν. Αυτό νομίζουν μερικοί.

Το λειτουργικό σύστημα

Το λογισμικό εφαρμογής και το λειτουργικό σύστημα για τα Γερμανικά διαβατήρια έχουν αναπτυχθεί από την T-Systems, μία θυγατρική της Telekom. Το βασικό λειτουργικό σύστημα χωρίζεται στις παρακάτω κατηγορίες: επικοινωνία μέσω της διασύνδεσης χωρίς επαφές, εντολές ελέγχου του προγράμματος, διαχείριση αρχείων και εφαρμογή κρυπτογραφικών αλγορίθμων για δεδομένα και ασφάλεια.

Το σύστημα αρχειοθέτησης των έξυπνων καρτών είναι οργανωμένο με ένα τρόπο παρόμοιο με αυτό των αρχείων DOS σε ένα PC. Τα αρχεία αποθηκεύονται στο EEPROM της έξυπνης κάρτας και περιέχουν όλες τις προσωπικές πληροφορίες. Αφού αποθηκευτούν στην EEPROM, το λειτουργικό σύστημα φροντίζει ώστε να μην επιτραπεί καμία πλέον απόπειρα επανεγγραφής των συγκεκριμένων δεδομένων.

Όσον αφορά το ηλεκτρονικό διαβατήριο, ο ICAO έχει καθορίσει κάποια περαιτέρω χαρακτηριστικά ασφαλείας. Η ασφάλεια και αυθεντικότητα των αποθηκευμένων δεδομένων προστατεύεται από μία μοναδική ψηφιακή υπογραφή, η αναδομημένη τιμή της οποίας [4] αποθηκεύεται σε ένα ειδικό αρχείο στην μνήμη. Η εν λόγω ψηφιακή υπογραφή βεβαιώνει ότι τα δεδομένα κωδικοποιήθηκαν από κάποια έγκυρη υπηρεσία και δεν έχουν τροποποιηθεί. Η κάθε υπηρεσία που έχει δικαίωμα έκδοσης διαβατηρίων κατέχει μία εξουσιοδότηση μέσω ενός ψηφιακού κλειδιού εκχωρημένου από τον ICAO. Με τον τρόπο αυτό εξασφαλίζεται ότι η γνησιότητα των δεδομένων που βρίσκονται στο ολοκληρωμένο είναι δυνατόν να επιβεβαιωθεί από την ψηφιακή υπογραφή που εκδίδεται μόνον από την αντίστοιχη αρχή έκδοσης διαβατηρίων.

(060010-1)

Σύνδεσμοι στο διαδίκτυο

[1] www.semiconductors.com/products/identification/
[2] www.infineon.com/security_and_chipcard_ics
[3] www.icao.int/mrtd/download/technical.cfm
[4] http://www.wikipedia.org
[5] https://shop.foebud.org/
[6] www.bundesdruckerei.de