ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΤΙΤΛΟΣ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΔΙΑΤΡΙΒΗΣ

“ΑΞΙΟΛΟΓΗΣΗ E-PASSPORT”

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΑΤΡΙΒΗ

ΟΝΟΜΑΤΕΠΩΝΥΜΟ: ΓΚΙΟΥΣΗ ΑΓΓΕΛΙΚΗ

ΑΡΙΘΜΟΣ ΜΗΤΡΩΟΥ: ΜΤΕ1206

ΕΠΙΒΛΕΠΩΝ: ΧΡΗΣΤΟΣ ΞΕΝΑΚΗΣ

ΠΕΙΡΑΙΑΣ 2015

Περιεχόμενα

ΠΕΡΙΛΗΨΗ

Τα ηλεκτρονικά διαβατήρια περιλαμβάνουν ανέπαφα τσιπ που αποθηκεύουν τα προσωπικά δεδομένα του κατόχου του διαβατηρίου, πληροφορίες σχετικά με το διαβατήριο και το ίδρυμα έκδοσης. Στην απλούστερη μορφή του ένα ηλεκτρονικό διαβατήριο περιέχει μόνο μια συλλογή από αρχεία μόνο για ανάγνωση, πιο προηγμένες παραλλαγές που μπορούν να περιλαμβάνουν εξελιγμένους κρυπτογραφικούς μηχανισμούς που προστατεύουν την ασφάλεια του εγγράφου ή / και της ιδιωτικής ζωής του κατόχου του διαβατηρίου. Αυτό το έγγραφο περιγράφει τα χαρακτηριστικά ασφαλείας των ηλεκτρονικών διαβατηρίων και συζητά την αποτελεσματικότητά τους. Τα ηλεκτρονικά διαβατήρια είναι βιομετρικά έγγραφα ταυτότητας τα οποία περιέχουν RFID ετικέτες και χρησιμοποιούνται κυρίως για την ασφάλεια των συνόρων. Ενσωματωμένες RFID ετικέτες μπορούν να αποθηκεύσουν δεδομένα, εκτελώντας υπολογισμούς χαμηλού κόστους και κρυπτογράφηση, και επικοινωνεί ασύρματα. Από το 2004, έχουμε δει την ανάπτυξη και την ευρεία εξάπλωση των τριών γενεών ηλεκτρονικών διαβατηρίων - Η Πρώτη Γενιά ICAO ePassport (2004), Extended Access Control ηλεκτρονικά διαβατήρια (2006), και τον εκτεταμένο έλεγχο πρόσβασης με κωδικό πιστοποίησης και Σύνδεση Ίδρυση (v2.1 EAC) ηλεκτρονικά διαβατήρια (2008). Σήμερα, πάνω από τριάντα εκατομμύρια ηλεκτρονικά διαβατήρια έχουν εκδοθεί σε όλο τον κόσμο. Στο έγγραφο αυτό, παρέχουμε μια εισαγωγική μελέτη των τεχνολογιών που εφαρμόζονται σε ηλεκτρονικά διαβατήρια - Βιομετρικά, RFID, και τις υποδομές δημόσιου κλειδιού? και στη συνέχεια συνεχίζουμε να αναλύσουμε τα πρωτόκολλα που εφαρμόζονται σε κάθε μία από τις τρεις γενιές ηλεκτρονικά διαβατήρια.

ΕΙΣΑΓΩΓΗ

Το διαβατήριο είναι μια κυβέρνηση που εκδίδει έγγραφο αναγνώρισης που αποδεικνύει ότι ο κάτοχος είναι πολίτης μιας συγκεκριμένης χώρας. Ανήκει υπό την προστασία του και επιτρέπεται να διεισδύσουν σε ξένες χώρες. Τα διαβατήρια πρέπει να είναι ανθεκτικά στην παραχάραξη, αλλά και διαθέσιμη για το πέρασμα από τον έλεγχο διαβατηρίων ο χρόνος είναι περιορισμένος. Αναγνώσιμα από μηχάνημα ταξιδιωτικών εγγράφων έχουν τη δυνατότητα να επιταχύνουν τη διαδικασία που διέρχεται από τον έλεγχο διαβατηρίων. Ο ICAO (Διεθνής Οργανισμός Πολιτικής Αεροπορίας - μια οργάνωση των Ηνωμένων Εθνών αρμόδιος για την πολιτική αεροπορία και διεθνή ταξίδια) έχουν ήδη τυποποιημένη την αποθήκευση ορισμένων δεδομένων διαβατηρίου σε δύο μηχανές επεξεργάσιμων γραμμών ήδη στη δεκαετία του 1980. Αυτή η ζώνη MRZ περιέχει τα βασικά στοιχεία σχετικά με το διαβατήριο και του κατόχου του (όνομα, επώνυμο, ημερομηνία γέννησης, ημερομηνία λήξης κλπ) και τυπώνεται σε μια τυποποιημένη γραμματοσειρά, έτσι ώστε να είναι αναγνώσιμα από μηχάνημα και να μπορούν να επεξεργάζονται τα συστήματα πληροφορικής.

Δεδομένου ότι το ποσό των δεδομένων που είναι αποθηκευμένα στο MRZ είναι μόνο πολύ μικρό και η μόνη «ασφάλεια» παράγοντας είναι το ψηφίο ελέγχου, νέοι τρόποι αποθήκευσης δεδομένων για την αυτοματοποιημένη επεξεργασία ερευνήθηκαν. Παρά το γεγονός ότι το ηλεκτρονικό μέρος του διαβατηρίου παραμένει προαιρετικό στο παγκόσμιο επίπεδο, κάποιες χώρες συμφώνησαν για την υποχρεωτική εισαγωγή των ηλεκτρονικών διαβατηρίων στα κράτη μέλη της ΕΕ. Τα δεδομένα σε ηλεκτρονικά διαβατήρια αποθηκεύονται ως στοιχειώδη αρχεία σε έναν φάκελο , μέχρι 16 αρχεία δεδομένων που ονομάζεται ως DG1 για DG16 .

Επίσης, ένα ηλεκτρονικό διαβατήριο έχει ενσωματωμένο ένα Radio Frequency Identification (RFID) που είναι ικανό για την κρυπτογραφική λειτουργικότητά. Η επιτυχής εφαρμογή των βιομετρικών δεδομένων και των τεχνολογιών RFID σε έγγραφα αποσκοπούν να ενισχύσουν την ασφάλεια των συνόρων με τη μείωση πλαστογραφίας και την ίδρυση χωρίς αμφιβολία ταυτότητας εγγράφων.

Η δυνατότητα RFID διαβατηρίων εγκρίθηκε για πρώτη φορά από τη Μαλαισία το 1998 . Ωστόσο, μέχρι το 2002, το εν λόγω διαβατήριο απέτυχε να διατηρήσει τις βασικές απαιτήσεις ασφάλειας δεδομένου ότι οι πληροφορίες κατόχου του

διαβατηρίου δεν ήταν κρυπτογραφημένα. Το μόνο μέτρο ασφάλειας που υλοποιήθηκε ήταν μια ψηφιακή υπογραφή σε όλα τα δεδομένα για να διασφαλιστεί ότι οι πληροφορίες δεν θα μπορούσαν να τροποποιηθούν από τους αντιπάλους. Αυτό ήταν σε μεγάλο βαθμό ανεπαρκής, δεδομένου ότι δεν εμπόδισε τα διαβατήρια από το να κλωνοποιηθούν, ή της παράνομης συλλογή δεδομένων μέσω skimming διαβατήριο.

Τέλος , ο Διεθνής Οργανισμός Πολιτικής Αεροπορίας εξέδωσε ένα σύνολο κατευθυντήριων γραμμών σχεδιασμού και προδιαγραφών πρωτοκόλλου για τα έθνη που επιθυμούν να εφαρμόσουν τη δυνατότητα RFID διαβατηρίων. Αυτό έγινε σε μια προσπάθεια για την τυποποίηση σχεδιασμού διαβατηρίων ενώ καθιστώντας τα πιο ασφαλή. Οι στόχοι της ασφάλειας των προδιαγραφών είναι: η εμπιστευτικότητα των δεδομένων, η ακεραιότητα δεδομένων, Data Authentication Προέλευσης, μη αποποίησης, ο αμοιβαίος έλεγχος ταυτότητας, και Key Integrity.

ΚΕΦΑΛΑΙΟ 1

1.1 ΔΙΑΒΑΤΗΡΙΟ

Το διαβατήριο είναι ταξιδιωτικό έγγραφο, που εκδίδεται από κρατική αρχή και χρησιμεύει για τη μετάβαση του κατόχου του σε χώρες του εξωτερικού και ως αποδεικτικό στοιχείο ταυτότητας και ιθαγένειας του κατόχου.

Υπάρχουν πολλοί διαφορετικοί τύποι διαβατηρίων, ανάμεσά τους το απλό διαβατήριο, το υπηρεσιακό διαβατήριο και το διπλωματικό διαβατήριο.

Πολλές χώρες εκδίδουν πλέον βιομετρικά διαβατήρια, που περιέχουν μικροτσίπ με ψηφιακή φωτογραφία του κατόχου ή/και δακτυλικά αποτυπώματα. Στην Ελλάδα, βιομετρικά διαβατήρια εκδίδονται ήδη από το 2006 με ψηφιακή φωτογραφία, από τα τέλη του Ιουνίου 2009 δε, περιέχουν και δακτυλικό αποτύπωμα του κατόχου.

Σήμερα, για να ταξιδέψει ένας πολίτης της Ευρωπαϊκής Ένωσης σε άλλη χώρα της Ε.Ε. αρκεί η αστυνομική ταυτότητα και δεν απαιτείται η έκδοση και κατοχή διαβατηρίου.

Εικόνα 1: Εξώφυλλο του ελληνικού διαβατηρίου

1.1.1 ΤΥΠΟΙ ΔΙΑΒΑΤΗΡΙΟΥ

Υπάρχει μια πρόχειρη τυποποίηση σε τύπους των διαβατηρίων σε όλο τον κόσμο , αν και τα είδη διαβατηρίου , τον αριθμό των σελίδων και οι ορισμοί μπορούν να διαφέρουν ανάλογα με τη χώρα .

Πλήρης διαβατήρια

• Διαβατήριο :(ονομάζεται επίσης τουριστικό διαβατήριο ή κανονικό διαβατήριο) : Η πιο κοινή μορφή του διαβατηρίου , που εκδόθηκε για τους πολίτες και άλλους υπηκόους . Μερικές φορές , τα παιδιά είναι νηολογημένα εντός διαβατήριο των γονέων , γεγονός που καθιστά ισοδύναμο με ένα οικογενειακό διαβατήριο .

• Επίσημο διαβατήριο: (ονομάζεται επίσης υπηρεσιακό διαβατήριο ή ειδικό διαβατήριο) : Εκδόθηκε σε δημοσίους υπαλλήλους για ταξίδια σχετίζονται με την εργασία , καθώς και τα εξαρτώμενα μέλη τους .

• Διπλωματικό διαβατήριο : Εκδόθηκε σε κυβερνητικούς αξιωματούχους και τα εξαρτώμενα μέλη τους για την εργασία που σχετίζονται με τα διεθνή ταξίδια . Τα περισσότερα άτομα με διπλωματική ασυλία φέρουν διπλωματικά διαβατήρια , αλλά ότι η ασυλία έρχεται μόνο όταν το προνόμιο του διπλωματικού καθεστώτος χορηγείται από τη χώρα στην οποία διπλωματική ιδιότητα ζητείται . Δεν υπονοείται από την κατοχή ενός διπλωματικού διαβατηρίου . Επιπλέον , έχει ένα διπλωματικό διαβατήριο δεν σημαίνει ταξίδια χωρίς βίζα . Κάτοχοι διπλωματικού διαβατηρίου πρέπει να συμμορφώνονται με τις ίδιες διαδικασίες όταν ταξιδεύετε σε μια ξένη χώρα, που απαιτούνται σε άλλους υπηκόους της χώρας του , εκτός αν είναι στη χώρα όπου έχουν παραχωρηθεί η διπλωματική ιδιότητα .

• Περιστασιακά , ένα διπλωματικό διαβατήριο μπορεί να δοθεί σε έναν ξένο πολίτη χωρίς διαβατήριο από τη δική του , όπως VIPs που έχουν εξοριστεί σε μια ξένη χώρα, όπως King Constantine II στην Ελλάδα .

• Διαβατήριο έκτακτης ανάγκης (που ονομάζεται επίσης την προσωρινή διαβατήριο): Εκδόθηκε σε άτομα των οποίων τα διαβατήρια χαθεί ή κλαπεί , χωρίς χρόνο για να το αντικαταστήσετε . Laissez - passer χρησιμοποιούνται για το σκοπό αυτό .

• Συλλογικό διαβατήριο : Εκδόθηκε σε καθορισμένες ομάδες για ταξίδια μαζί για συγκεκριμένους προορισμούς , όπως η ομάδα των παιδιών σχολικής ηλικίας σε μια σχολική εκδρομή .

• Οικογένεια διαβατηρίου : Εκδόθηκε σε μια ολόκληρη οικογένεια . Υπάρχει ένα κατόχου του διαβατηρίου , και μπορούν να ταξιδεύουν μόνοι ή με ένα ή περισσότερα άλλα μέλη της οικογένειας . Ένα μέλος της οικογένειας που δεν είναι ο κάτοχος του διαβατηρίου δεν μπορούν να χρησιμοποιήσουν το διαβατήριο για να ταξιδέψετε εκτός και αν συνοδεύονται από τον κάτοχο του διαβατηρίου.

1.2 ΗΛΕΚΤΡΟΝΙΚΟ ΔΙΑΒΑΤΗΡΙΟ

Το ηλεκτρονικό διαβατήριο είναι μια αντικατάσταση για το παραδοσιακό βιβλίο διαβατήριο που μπορούν να χρησιμοποιηθούν για ταξίδια και τη διέλευση των συνόρων σε παγκόσμιο επίπεδο . ePassports ακολουθούν πρότυπα που έχουν

καθοριστεί από τη Διεθνή Οργάνωση Πολιτικής Αεροπορίας και έχουν εκδοθεί από πολλές χώρες σε όλο τον κόσμο . Το ηλεκτρονικό διαβατήριο χρησιμοποιεί ασφαλή RF -enabled ανέπαφων τεχνολογία των έξυπνων καρτών για την προστασία των πολιτών προσωπικές πληροφορίες και να παρέχουν ισχυρή συνολική ασφάλεια για το έγγραφο διαβατηρίου .

Ένα e - Passport περιέχει ένα ηλεκτρονικό τσιπ . Το τσιπ διαθέτει τις ίδιες πληροφορίες που είναι τυπωμένες στη σελίδα δεδομένων του διαβατηρίου : το όνομα του κατόχου , την ημερομηνία γέννησης , και άλλες βιογραφικές πληροφορίες . Ένα e - Passport περιέχει επίσης ένα βιομετρικό αναγνωριστικό στοιχείο . Οι Ηνωμένες Πολιτείες απαιτεί ότι το τσιπ περιέχει μια ψηφιακή φωτογραφία του κατόχου . Όλα τα e - διαβατήρια που εκδίδονται από το Πρόγραμμα Απαλλαγής από Βίζα (VWP) χώρες και τις Ηνωμένες Πολιτείες έχουν τα χαρακτηριστικά ασφαλείας για να αποτρέπεται η μη εξουσιοδοτημένη ανάγνωση ή " skimming " των δεδομένων που αποθηκεύονται στο chip e - Passport .

Οι Ηνωμένες Πολιτείες απαιτούν οι ταξιδιώτες που εισέρχονται στις Ηνωμένες Πολιτείες στο πλαίσιο της Visa Waiver Program έχετε ένα e - Passport αν το διαβατήριό τους εκδόθηκε την ή μετά την 26 Οκτώβρη του 2006

Η διαδικασία ελέγχου για έναν κάτοχο e - Passport είναι το ίδιο με εκείνο για έναν κάτοχο μη -e - Passport . Όταν φθάνουν σε ΗΠΑ λιμένες εισόδου , οι κάτοχοι e - Passport θα πρέπει να κατευθύνεται από σήμανση ή το προσωπικό σχετικά με την κατάλληλη ΗΠΑ Τελωνείων και Προστασίας των Συνόρων περίπτερο στη χρήση.

Το Διαβατήριο χρησιμοποιεί μια εντελώς διαφορετική τεχνολογία RF - μια ετικέτα RFID που επιτρέπει πληροφορίες Κάρτα μοναδικό διαβατήριο για να διαβαστεί από μεγάλες αποστάσεις.

Όλα τα ηλεκτρονικά διαβατήρια το κοινό πρότυπο ICAO . Ωστόσο, οι χώρες εφαρμόζουν προγράμματα ePassport ανάλογα με τις ιδιαίτερες πολιτικές τους και μπορούν να εφαρμόσουν διαφορετικές επιλογές που ορίζεται στο πρότυπο . Αυτό οδηγεί σε διαφορές μεταξύ των εφαρμογών της χώρας ηλεκτρονικά διαβατήρια , ακόμη κι αν όλοι συμφωνούν με τις προδιαγραφές του ICAO .

Το ePassport παρέχει ο αξιωματικός προστασίας των συνόρων με ένα νέο εργαλείο για να βοηθήσει στον προσδιορισμό της ταυτότητας του παρουσιαστή με την προσθήκη της ηλεκτρονικής έκδοσης του εντύπου εγγράφου .

Με το νέο σχεδιασμό φυλλάδιο που το Στέιτ Ντιπάρτμεντ που εισάγονται με το ηλεκτρονικό διαβατήριο , νέες δυνατότητες εκτύπωσης , και ασφαλή μάρκες μικροελεγκτή ενσωματωθεί στο φυλλάδιο , η δυσκολία της πλαστογράφησης διαβατηρίων έχει αυξηθεί σημαντικά . ePassports περιλαμβάνουν πλέον ψηφιακές και φυσικές τεχνολογίες ασφαλείας που έχουν ενσωματωθεί μαζί για να παρέχουν σημαντικά υψηλότερα επίπεδα ασφάλειας . ePassports χρησιμοποιούν προηγμένες τεχνολογίες που εξασφαλίζουν ταυτότητες και νέες διαδικασίες σε ολόκληρη την αλυσίδα της εμπιστοσύνης - από την παραγωγή μέχρι τη χρήση του ePassport .

Τα μέτρα ασφαλείας που βρέθηκαν σε όλο το σύστημα ePassport , από την παραγωγή του το ίδιο το βιβλίο με τις πολιτικές και τις διαδικασίες που εφαρμόζονται στις συνοριακές διαβάσεις .

Κανείς έξω από την κυβέρνηση γνωρίζει το πλήρες " συνταγή " που περιλαμβάνει ειδικά χαρτιά , μελάνια , και τεχνικές κατασκευής . Το ενσωματωμένο chip είναι μια ασφαλής μικροελεγκτή με την προηγμένη κρυπτογραφία και ενσωματωμένους αισθητήρες για την ανίχνευση επιθέσεων .

Όταν το ηλεκτρονικό διαβατήριο εξατομικευμένη και εκδοθεί , τα στοιχεία που έχει γραφτεί για το τσιπ υπογράφεται από την εκδούσα αρχή , χρησιμοποιώντας τη χώρα τους βασικούς υπογραφή . (Αυτό είναι το ψηφιακό ισοδύναμο με σφραγίδα ενός δημόσιου συμβολαιογράφου πιστοποιεί ένα έγγραφο .) Μόλις κατασκευαστεί και εξατομικευμένη , δεν μπορούν να αλλάξουν .

Το ePassport έχει σχεδιαστεί για να διαβαστούν μόνο όταν είναι ανοικτή και μετά από μια επιτυχή ανάγνωση της μηχανικώς αναγνώσιμη ζώνη (MRZ) με αναγνώστη ePassport - ενεργοποιημένο .

Τελευταίο αλλά όχι λιγότερο σημαντικό , οι κυβερνήσεις , οι κατασκευαστές , οι εθνικές εκτυπωτές και το προσωπικό ελέγχου έχουν ενισχυθεί διαδικασίες κατασκευής διαβατήριο , την παράδοση και τον έλεγχό τους, για να δημιουργήσει μια ισχυρότερη αλυσίδα εμπιστοσύνης . Αυτές οι βελτιωμένες διαδικασίες προστατεύουν τους πολίτες από την κλοπή ταυτότητας και να εμποδίσουμε τους τρομοκράτες να αποκτήσουν επίσημα - αναζητούν διαβατήρια με πλαστές ταυτότητες.

Όποιος θέλει να κάνει ένα αντίγραφο ePassport θα πρέπει να έχουν το τσιπ , τα δεδομένα , και όλα τα στοιχεία παραγωγής και την τεχνογνωσία . Αλλά χωρίς το ιδιωτικό κρυπτογραφικό κλειδί κυβέρνηση πρέπει να υπογράφει ψηφιακά όλες τις

πληροφορίες , ο καθένας προσπαθεί να χρησιμοποιήσει ένα πλαστό διαβατήριο θα bestopped όταν ο έλεγχος κρυπτογραφία θα αποτύχει .

Όπως και με τις παραδοσιακές ταυτότητες ή διαβατήρια , είναι υψίστης σημασίας για την προστασία των δικών έγγραφα ταυτότητας σας . Έγγραφα ταυτότητας θα πρέπει ποτέ να αφήνονται αφύλακτα ή να περάσει σε κάποιον άλλο ... αν είναι ηλεκτρονικά ή παραδοσιακά ! Σήμερα , αν κάποιος χάνει ένα παραδοσιακό διαβατήριο , η ζημία πρέπει να αναφέρονται στις αρμόδιες αρχές . Το ίδιο ισχύει και αν χάσετε ένα ηλεκτρονικό διαβατήριο . Κατά τον έλεγχο των συνόρων , είναι πιο εύκολο να παρακολουθείτε πόσο τυχόν απολεσθέντος ή κλαπέντος ηλεκτρονικά διαβατήρια που χρησιμοποιούνται .

Διαβάζοντας τις πληροφορίες που περιέχονται σε ένα ηλεκτρονικό διαβατήριο δεν είναι ούτε επίθεση , ούτε ένα ελάττωμα στην ασφάλεια . Ανάγνωση και αντιγραφή των ηλεκτρονικών δεδομένων σε ένα ηλεκτρονικό διαβατήριο δεν είναι απειλές και είναι ουσιαστικά το ίδιο με την ανάγνωση και φωτοτυπικό ένα παραδοσιακό χαρτί μόνο διαβατήριο που έχει ανοίξει . Τα νέα ηλεκτρονικά διαβατήρια σχεδιαστεί με πολλαπλά επίπεδα ασφάλειας . Το γεγονός ότι η έντυπη πληροφόρηση είναι μια ακριβή αντιστοιχία με την ψηφιακή προστατευόμενες ηλεκτρονικές πληροφορίες κάνει το νέο ePassport πολύ πιο ασφαλής και έναντι της απάτης .

Τα ηλεκτρονικά διαβατήρια σχεδιαστεί με πολλαπλά χαρακτηριστικά ασφαλείας .

Κατ 'αρχάς , ένα ηλεκτρονικό διαβατήριο είναι κατασκευασμένο από ειδικό χαρτί που ενσωματώνουν χαρακτηριστικά υψηλής εκτύπωση ασφαλείας . Με τον ίδιο σχεδόν τρόπο ότι τα χρήματα είναι τυπωμένο και παράγονται , αυτά τα εξελιγμένα χαρακτηριστικά που ενσωματώνονται σε ειδικό χαρτί και αναλώσιμα προστατεύονται από εξελιγμένα μέσα .

Εκτός από αυτά τα χαρακτηριστικά ασφαλείας φυσικής εκτύπωσης, ηλεκτρονικά διαβατήρια έχουν επίσης ένα μικρό , ενσωματωμένο ολοκληρωμένο κύκλωμα. Όταν δημιουργείται ένα ηλεκτρονικό διαβατήριο , οι ίδιες πληροφορίες είναι τόσο καλά τυπωμένα στο χαρτί και με ασφάλεια αποτυπωθεί στο chip . Οι πληροφορίες σχετικά με το chip είναι ψηφιακά υπογεγραμμένο από αρχή διαβατήριο της χώρας έκδοσης . (Αυτό είναι το ψηφιακό ισοδύναμο με σφραγίδα ενός δημόσιου συμβολαιογράφου πιστοποιεί ένα έγγραφο .)

Για την επιτυχή κλωνοποίηση ενός ePassport , ένας εγκληματίας θα πρέπει να αποκτήσουν τόσο το χαρτί της ασφάλειας και ένα κατάλληλο τσιπ . Η ποινική τότε θα πρέπει να δημιουργήσετε ένα πλήρες βιβλίο ePassport , ενσωματώσετε το τσιπ και να γράφουν τα ψηφιακά υπογεγραμμένα δεδομένα στο τσιπ - και να το κάνουμε αυτό με τέτοιο τρόπο ώστε το προκύπτον ePassport θα μοιάζουν αυθεντικά σε έναν παράγοντα διέλευσης των συνόρων . Ενώ αυτό είναι τεχνικώς εφικτό , θα ήταν εξαιρετικά δύσκολο να κάνει ένα ακριβές αντίγραφο ενός υπάρχοντος ePassport . Είναι επίσης σημαντικό να θυμόμαστε ότι η κλωνοποίηση ενός ePassport θα ισοδυναμούσε με κάποιον που χρησιμοποιεί ένα αντίγραφο του ePassport σας χωρίς γνώση σας . Για ePassport σας για να χρησιμοποιηθεί από κάποιον άλλο να αναλάβει την ταυτότητά σας , το άλλο πρόσωπο θα πρέπει να εξετάσουμε ακριβώς όπως σας . Για το λόγο αυτό , κλωνοποιημένα ηλεκτρονικά διαβατήρια δεν παρουσιάζουν υψηλό επίπεδο κινδύνου .

Στο παρελθόν , ήταν δυνατόν να αντικαταστήσει την φωτογραφία κολλημένο στο βιβλίο διαβατήριο και / ή να τροποποιήσουν τα δεδομένα εκτυπώνονται κάτω από το έλασμα . Με ένα ηλεκτρονικό διαβατήριο , οι προηγμένες τεχνικές που χρησιμοποιούνται για την εκτύπωση της σελίδας με τα στοιχεία και τα στοιχεία και τη φωτογραφία γράφεται επίσης με ηλεκτρονικά μέσα στο τσιπ . Έτσι , για κάποιον που θέλει να αλλάξει τα δεδομένα , το πρώτο εμπόδιο θα ήταν να αλλάξει με επιτυχία τις πληροφορίες και στα δύο μέρη , και να το πράξουν χωρίς να προσελκύσουν την προσοχή , ως αποτέλεσμα της αλλοίωσης προφανής .

Αλλά , ακόμα κι αν κάποιος ήταν σε θέση να εισαγάγει εναλλακτικές ή απατηλά στοιχεία για τον αντικαταστάτη του chip (όπως μερικοί χάκερ ισχυρίζονται) , το ψεύτικο ePassport δεν θα περάσει τον έλεγχο των συνόρων . Οποιαδήποτε αλλαγή στα δεδομένα ακυρώνει το ηλεκτρονικό διαβατήριο , δεδομένου ότι η ψηφιακή υπογραφή θα συμφωνεί πλέον με τις αποθηκευμένες πληροφορίες . Έτσι, το δεύτερο , και μεγαλύτερο , εμπόδιο θα δημιουργήσει τη σωστή ψηφιακή υπογραφή για να ταιριάζει με τα νέα δεδομένα . Οι περισσότερες αρχές διαβατήριο κλείδωμα των δεδομένων που αποθηκεύονται στο ePassport αφού έχει προγραμματιστεί έτσι ώστε να μην μπορούν να τροποποιηθούν τα δεδομένα . Στη συνέχεια, να υπογράψετε ψηφιακά τα δεδομένα με τη χώρα τους, την υπογραφή κλειδί, το οποίο είναι πολύ καλά προστατευμένο .

Το ηλεκτρονικό διαβατήριο δείχνει την εικόνα σας , το όνομά σας και άλλες πληροφορίες που να αποδεικνύουν ποιος είσαι? Η πληροφορία αυτή δεν έχει καμία χρήση , εκτός αν ο εισβολέας είναι πανομοιότυπα δίδυμα ή προσπαθεί σας (και καταφέρνει) να τροποποιήσει ορισμένες από τις πληροφορίες και την αξιοποίηση των παραγόμενων ePassport για κάποιον άλλο . Ένα αντίγραφο ePassport δεν είναι χρήσιμο σε ποινική ή απατεώνας . Τα στοιχεία του διαβατηρίου του τσιπ δεν μπορεί να αλλάξει χωρίς να έχει εντοπιστεί . Ένα αντίγραφο ePassport θα έχει καμία χρήση σε κανέναν άλλο , γιατί η εικόνα σας είναι πάνω στο τσιπ και τυπώνεται στο ePassport και ο απατεώνας δεν είναι εσύ . Αυτή η κατάσταση δεν είναι διαφορετική από μια απατεώνας προσπαθεί να χρησιμοποιήσει ένα χαμένο ή κλεμμένο διαβατήριο χαρτιού χωρίς μεταβολή . Το σύνολο του προγράμματος ePassport έχει σχεδιαστεί για να εξαλειφθεί ο κίνδυνος κάποιος αλλοίωση ή τη χρήση διαπιστευτηρίων διαβατήριο κάποιου άλλου , και οι μηχανισμοί ασφαλείας που στο έργο τόπο καλά .

Οι στόχοι του συνολικού προγράμματος ePassport ήταν να κάνει τα διαβατήρια σχεδόν αδύνατο να πλαστά και να αποτρέψει οποιονδήποτε άλλον εκτός από τον ιδιοκτήτη του διαβατηρίου από τη χρήση του ePassport . Το πρόγραμμα ePassport επιτυγχάνει τους στόχους αυτούς με δύο τρόπους

Πρώτον , οι πληροφορίες σχετικά με την τυπωμένη σελίδα , συμπεριλαμβανομένης της φωτογραφίας του κατόχου , αποθηκεύονται στο τσιπ και στη συνέχεια εμφανίζεται στην οθόνη κατά τον έλεγχο διαβατηρίων . Με τη σύγκριση της ψηφιακής πληροφορίας , το τυπωμένο διαβατήριο και το πρόσωπο , το προσωπικό ελέγχου διαβατηρίων μπορεί να επιβεβαιώσει ότι όλα είναι εντάξει . Θα δείτε αμέσως μια διαφορά αν κάποιος προσπαθεί να χρησιμοποιήσει ePassport πληροφορίες chip κάποιου άλλου .

Δεύτερον , οι πληροφορίες σχετικά με το chip είναι ψηφιακά υπογεγραμμένο από αρχή διαβατήριο της χώρας έκδοσης . Αυτό σημαίνει ότι, εάν οι πληροφορίες μεταβολές κατά οποιονδήποτε τρόπο μετά την ePassport έχει εκδοθεί, η μεταβολή θα πρέπει να ανιχνεύεται στον έλεγχο διαβατηρίων . Σημαίνει επίσης ότι οποιαδήποτε προσπάθεια να δημιουργήσει ένα ψεύτικο ePassport πιστοποίηση θα πρέπει να ανιχνεύεται .

Αν κάποιος ήταν να χρησιμοποιήσετε ένα αντίγραφο των δεδομένων σε ένα άλλο τσιπ ή συσκευή με μια διαφορετική σελίδα δεδομένων ή φωτογραφία , ο εξοπλισμός

σταθμό επιθεώρησης θα τονίσει τη διαφορά αυτή και να ειδοποιήσει τον επιθεωρητή . Αυτή η ηλεκτρονική πιστοποίηση έρχεται εκτός από την παραδοσιακή οπτική ελέγχους, οι οποίοι εξακολουθούν να διεξάγονται από τον επιθεωρητή . Ένα τσιπ ή τη συσκευή με ένα αντίγραφο των δεδομένων ePassport δεν θα λειτουργήσει με ένα διαφορετικό βιβλίο ePassport . Εκτός από τα προηγούμενα μέτρα ασφαλείας που περιγράφονται , τα πρόσθετα χαρακτηριστικά ασφαλείας πρόληψη του κινδύνου αυτού . ePassport δεδομένα προστατεύονται με μια τεχνική που ονομάζεται Basic Access Control (BAC) . Κατά τον έλεγχο των συνόρων , το ηλεκτρονικό διαβατήριο θα πρέπει να ανοιχθούν και τα κεφαλαία γράμματα τυπωμένο στο κάτω μέρος της σελίδας με τα στοιχεία (που ονομάζεται Μηχαναγνώσιμη Ζώνη , ή MRZ) , πρέπει να διαβάσετε πρώτα .

Τα περιεχόμενα του MRZ περιέχουν ένα κλειδί το οποίο χρησιμοποιείται για την πρόσβαση στο τσιπ? Το τσιπ επιτρέπεται μόνο για την επικοινωνία με τον αναγνώστη , αν ταιριάζουν τα κλειδιά . Τα δεδομένα MRZ δεν είναι απόρρητες πληροφορίες . Είναι απλά μια αναπαράσταση ορισμένων από τις τυπωμένες πληροφορίες σχετικά με την σελίδα δεδομένων. Τα δεδομένα MRZ επιτρέπει στους υπολογιστές να διαβάσει ηλεκτρονικά τις τυπωμένες πληροφορίες με ακρίβεια . Εάν οι πληροφορίες MRZ τυπωμένο στη σελίδα των στοιχείων δεν ταιριάζει με το κλειδί το τσιπ περιμένει , η επικοινωνία με το τσιπ ePassport δεν μπορεί να πραγματοποιηθεί και καμία ψηφιακή πληροφορία παρέχεται .

Το ePassport ενσωματώνει πολλαπλά στοιχεία ασφαλείας για να αποτρέψουν την ανάγνωση των δεδομένων προσωπικού χαρακτήρα χωρίς τη συγκατάθεση του πολίτη . Κατ 'αρχάς , μια ηλεκτρονική συσκευή ανάγνωσης πρέπει να ασκηθεί εντός τριών ιντσών της ePassport για να λειτουργήσει . Δεύτερον , ακόμη και αν ο αναγνώστης προσπαθεί να διαβάσει τα δεδομένα σε αυτή την κοντινή απόσταση , το ηλεκτρονικό διαβατήριο θα επιστρέψει μόνο ένα τυχαίο μοναδικό αναγνωριστικό (που αλλάζει με κάθε απόπειρα διαβάσει) με το αίτημα για την ePassport - μοναδική MRZ δεδομένα που είναι τυπωμένος στο εσωτερικό της το ηλεκτρονικό διαβατήριο . Η MRZ περιέχει πληροφορίες που πρέπει να χρησιμοποιείται από μια εξωτερική συσκευή για να σχηματίσουν το σωστό κωδικό πρόσβασης για να ξυπνήσει το διαβατήριο επάνω . Τρίτον , οι ΗΠΑ ePassport ενσωματώνει μια μεταλλική ασπίδα η οποία αποτρέπει την πρόσβαση στα δεδομένα , όταν το φυλλάδιο είναι κλειστό . Αυτά τα στοιχεία ασφαλείας να διασφαλίσει ότι το ηλεκτρονικό διαβατήριο θα πρέπει να διαβάζονται

μόνο όταν παρουσιασθεί , το φυλλάδιο άνοιξε , και η MRZ σαρώνονται από ένα σωστά ρυθμισμένο αναγνώστη.

Το ηλεκτρονικό διαβατήριο χρησιμοποιεί ένα untrackable, τυχαίο, μοναδικό αναγνωριστικό που αλλάζει κάθε φορά το ηλεκτρονικό διαβατήριο διαβάσει. Οποιαδήποτε δεδομένα μόνο από έναν συγκεκριμένο ePassport μπορούν να διαβαστούν μόνο μετά την πρώτη απόκτηση των δεδομένων ePassport MRZ που εκτυπώνεται στη σελίδα των στοιχείων φυλλάδιο και προσβάσιμη μόνο όταν το ηλεκτρονικό διαβατήριο φυσικά παρουσιάζεται σε έναν αναγνώστη (για παράδειγμα, σε ένα σημείο διέλευσης των συνόρων). Επιπλέον, οι ΗΠΑ ePassport ενσωματώνει μια μεταλλική θωράκιση RF που αποτρέπει την ανάγνωση του ePassport όταν το φυλλάδιο είναι κλειστό. Αυτά τα χαρακτηριστικά ασφαλείας χρησιμεύουν για να μπλοκάρουν αποτελεσματικά οποιαδήποτε παρακολούθηση.

1.2.1 ΟΦΕΛΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΔΙΑΒΑΤΗΡΙΟΥ

Τα οφέλη που προσφέρει ένα ηλεκτρονικό διαβατήριο είναι:

• ασφάλεια στον ταξιδιώτη ,

• προστασία κατά της κλοπής ταυτότητας ,

• προστασία της ιδιωτικής ζωής και

Υπάρχουν πολλαπλά επίπεδα ασφάλειας στο πλαίσιο της διαδικασίας e - Passport που αποφεύγονται οι επικαλύψεις .

1.3 ΒΙΟΜΕΤΡΙΚΟ ΔΙΑΒΑΤΗΡΙΟ

Ένα βιομετρικό διαβατήριο , είναι ένα διαβατήριο σε έντυπη και ηλεκτρονική μορφή που περιέχει βιομετρικά στοιχεία που μπορούν να χρησιμοποιηθούν για να πιστοποιήσουν την ταυτότητα των ταξιδιωτών. Χρησιμοποιεί μια έξυπνη κάρτα τεχνολογίας, συμπεριλαμβανομένου ενός μικροεπεξεργαστή τσιπ (τσιπ υπολογιστή) και την κεραία (τόσο για εξουσία στο τσιπ και επικοινωνίας) ενσωματωμένο στο μπροστινό ή πίσω κάλυμμα, ή το κέντρο της σελίδας, του διαβατηρίου. Τα χαρακτηριστικά εγγράφων και τσιπ τεκμηριώνονται στην Διεθνή Οργάνωση Πολιτικής Αεροπορίας 's (ICAO).

Τα σημερινά βιομετρικά συστήματα χρησιμοποιούνται για αυτό το είδος του συστήματος αναγνώρισης όπως αναγνώριση προσώπου, αναγνώριση δακτυλικών

αποτυπωμάτων και αναγνώρισης της ίριδας . Αυτά εγκρίθηκαν μετά την αξιολόγηση πολλών διαφορετικών ειδών των βιομετρικών στοιχείων, συμπεριλαμβανομένης της σάρωσης του αμφιβληστροειδούς . Ο ICAO ορίζει τις μορφές αρχείων και τα πρωτόκολλα επικοινωνίας που θα χρησιμοποιούνται στα διαβατήρια. Μόνο η ψηφιακή εικόνα (συνήθως σε μορφή JPEG ή JPEG2000 μορφή) είναι πραγματική και αποθηκεύεται στο τσιπ. Η σύγκριση των βιομετρικών στοιχείων γίνεται έξω από το κύκλωμα του διαβατηρίου από ηλεκτρονικά συστήματα ελέγχου των συνόρων.

1.4 Η ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ

Τα βιομετρικά διαβατήρια είναι εξοπλισμένα με μηχανισμούς προστασίας για την αποφυγή ή / και ανίχνευση επιθέσεων:

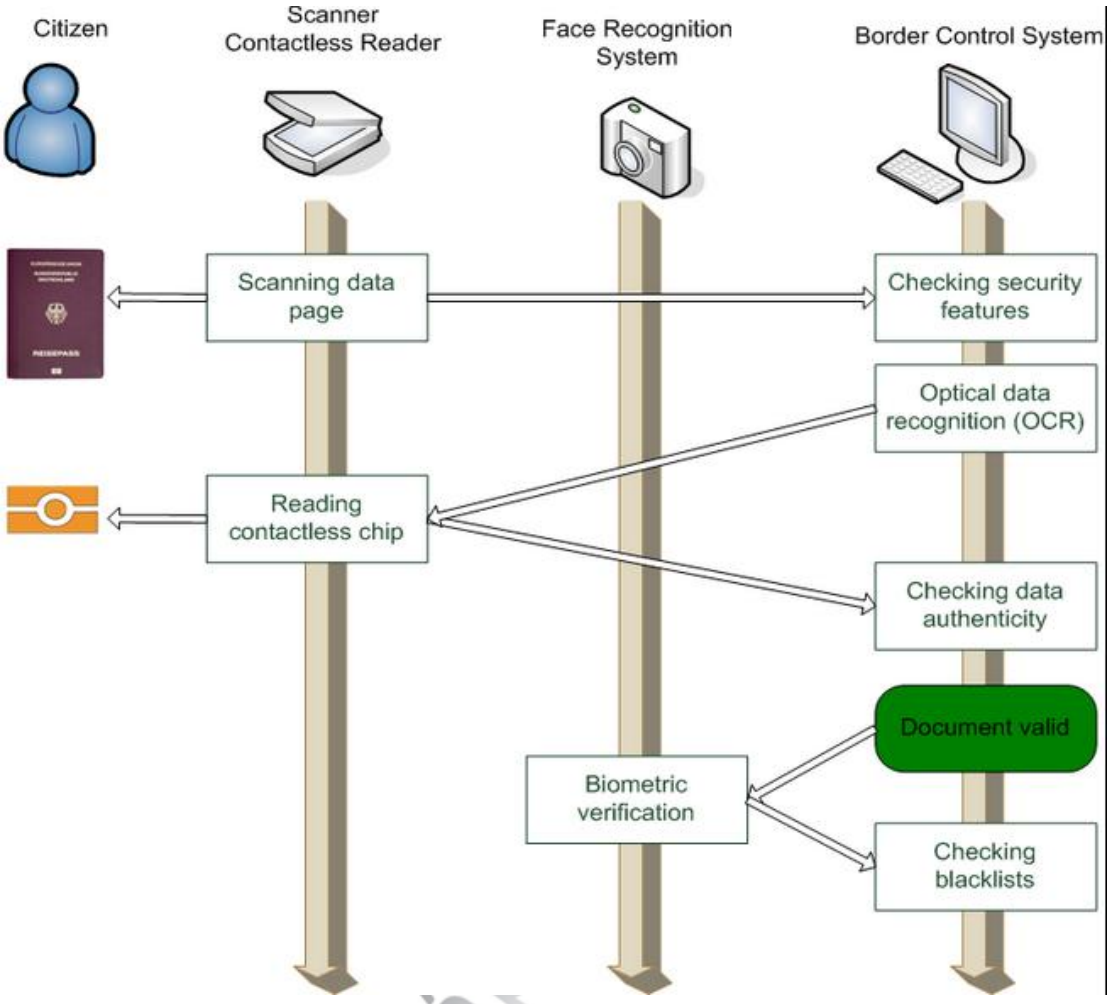
- *Μη ανιχνεύσιμα χαρακτηριστικά τσιπ.* Τυχαία τσιπ αναγνώρισης απαντά σε κάθε αίτημα με διαφορετικό αριθμό μαρκών. Αυτό αποτρέπει τον εντοπισμό των τσιπ διαβατηρίων. Χρησιμοποιώντας τυχαίους αριθμούς αναγνώρισης είναι προαιρετική.
- *Βασικός έλεγχος πρόσβασης (BAC).* BAC προστατεύει το κανάλι επικοινωνίας μεταξύ του τσιπ και τον αναγνώστη με την κρυπτογράφηση μεταδίδονται πληροφορίες. Πριν δεδομένα μπορούν να διαβαστούν από ένα τσιπ, ο αναγνώστης θα πρέπει να παρέχει ένα κλειδί, το οποίο προέρχεται από την Μηχαναγνώσιμη Ζώνη : η ημερομηνία γέννησης, την ημερομηνία λήξης και τον αριθμό του εγγράφου. Αν BAC χρησιμοποιείται, ένας εισβολέας δεν μπορεί (εύκολα) αφουγκράζομαι μεταφέρονται πληροφορίες χωρίς να γνωρίζει το σωστό κλειδί. Χρησιμοποιώντας ΠΑ είναι προαιρετική.
- *Παθητική ταυτότητας (PA).* PA αποτρέπει την τροποποίηση των δεδομένων chip του διαβατηρίου. Το τσιπ περιέχει ένα αρχείο (SOD) που αποθηκεύει τιμές κατακερματισμού όλων των αρχείων που είναι αποθηκευμένα στο τσιπ (εικόνα, τα δακτυλικά αποτυπώματα, κλπ) και μια ψηφιακή υπογραφή αυτών των hashes. Η ψηφιακή υπογραφή γίνεται χρησιμοποιώντας ένα κλειδί υπογραφής του εγγράφου που η ίδια έχει υπογραφεί από ένα κλειδί υπογραφής χώρα. Εάν ένα αρχείο στο τσιπ (π.χ. εικόνα) έχει αλλάξει, αυτό μπορεί να ανιχνευθεί, δεδομένου ότι η τιμή κατατεμαχισμού είναι εσφαλμένη. Οι αναγνώστες πρέπει να έχουν πρόσβαση σε όλα τα χρησιμοποιημένα δημόσια κλειδιά χώρα για να ελέγξει αν η

ψηφιακή υπογραφή δημιουργείται από μια αξιόπιστη χώρα. Χρησιμοποιώντας PA είναι υποχρεωτική.

- *Ενεργός ταυτότητας (AA*). AA αποτρέπει την κλωνοποίηση των τσιπ διαβατηρίων. Το τσιπ περιέχει ένα ιδιωτικό κλειδί που δεν μπορεί να διαβάσει ή να αντιγραφεί, αλλά η ύπαρξή του μπορεί εύκολα να αποδειχθεί. Χρησιμοποιώντας AA είναι προαιρετική.
- *Επέκταση Ελέγχου Πρόσβασης (EAC).* EAC προσθέτει λειτουργικότητα να ελέγχουν τη γνησιότητα τόσο του τσιπ (chip ταυτότητας) και τον αναγνώστη (τερματικό ελέγχου ταυτότητας). Επιπλέον, χρησιμοποιεί ισχυρότερη κρυπτογράφηση από το BAC. EAC τυπικά χρησιμοποιείται για να προστατεύσει τα δακτυλικά αποτυπώματα και ίριδας σαρώσεις. Χρησιμοποιώντας EAC είναι προαιρετική. Στην EU, χρησιμοποιώντας EAC είναι υποχρεωτική για όλα τα έγγραφα που εκδίδονται ξεκινώντας 28, Ιουν, 2009.
- *Συμπληρωματικό Ελέγχου Πρόσβασης (SAC)* εισήχθη από τη ICAOτο 2009 για την αντιμετώπιση της BAC αδυναμίες. Εισήχθη ως συμπλήρωμα BAC (για τη διατήρηση της συμβατότητας), αλλά θα αντικαταστήσει στο μέλλον.
- *Θωράκιση του τσιπ.* Αυτό αποτρέπει τη μη εξουσιοδοτημένη ανάγνωση. Ορισμένες χώρες - συμπεριλαμβανομένης τουλάχιστον τις US - έχουν ενσωματώσει ένα πολύ λεπτό μεταλλικό πλέγμα στο εξώφυλλο του διαβατηρίου για να λειτουργήσει ως ασπίδα όταν το κάλυμμα του διαβατηρίου είναι κλειστό. Η χρήση της θωράκισης είναι προαιρετική.

1.5 ΔΙΑΔΙΚΑΣΙΑ ΕΛΕΓΧΟΥ

Μια τυπική ροή εργασιών ενός αυτόματου συστήματος ελέγχου των συνόρων:



Εικόνα 2: Διαδικασία Ελέγχου

1.6 ΧΩΡΕΣ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΕΙΤΑΙ ΤΟ ΒΙΟΜΕΤΡΙΚΟ ΔΙΑΒΑΤΗΡΙΟ

- Αυστρία
- Ευρωπαϊκή Ένωση
- Βέλγιο
- Βουλγαρία
- Κροατία
- Κύπρος
- Τσεχική Δημοκρατία .
- Δανία
- Εσθονία

- Φινλανδία
- Γαλλία
- Γερμανία
- Ελλάδα
- Ουγγαρία
- Ιρλανδία
- Ιταλία
- Λετονία
- Λιθουανία
- Λουξεμβούργο
- Μάλτα
- Ολλανδία
- Πολωνία
- Πορτογαλία
- Ρουμανία
- Σλοβακία
- Σλοβενία
- Ισπανία
- Σουηδία
- Ηνωμένο Βασίλειο
- Αλβανία
- Αργεντινή
- Αρμενία
- Αυστραλία
- Αζερμπαϊτζάν
- Βοσνία-Ερζεγοβίνη

- Βραζιλία
- Μπρουνέι
- Καναδάς
- Χιλή
- Λαϊκή Δημοκρατία της Κίνας
- Δομινικανή Δημοκρατία
- Αίγυπτος
- Γκαμπόν
- Γκάνα
- Χονγκ Κονγκ
- Ισλανδία
- Ινδία
- Ινδονησία
- Ιράν
- Ιράκ
- Ισραήλ
- Ιαπωνία
- Κοσσυφοπέδιο
- Μαλαισία
- Μαλδίβες
- Κυρίαρχο Στρατιωτικό Τάγμα της Μάλτας
- Μολδαβία
- Μαυροβούνιο
- Μαυριτανία
- Μαρόκο
- Νέα Ζηλανδία

- Νιγηρία
- Νορβηγία
- Πακιστάν
- Φιλιππίνες
- Κατάρ
- Η Ρωσική Ομοσπονδία
- Σαουδική Αραβία
- Σερβία
- Σιγκαπούρη
- Σομαλία
- Νότια Κορέα
- Νότιο Σουδάν
- Σουδάν
- Ελβετία
- Ταϊβάν
- Τατζικιστάν
- Ταϊλάνδη
- Τόγκο
- Τουρκία
- Τουρκμενιστάν
- Ουκρανία
- Ηνωμένα Αραβικά Εμιράτα
- Ηνωμένες Πολιτείες
- Ουζμπεκιστάν
- Βενεζουέλα

1.7 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΒΙΟΜΕΤΡΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Τα βιομετρικά χαρακτηριστικά συνιστούν βιολογικές ιδιότητες, πτυχές συμπεριφοράς, φυσιολογικά χαρακτηριστικά, προσωπικά γνωρίσματα ή επαναλαμβανόμενες κινήσεις. Τα γνωρίσματα και οι κινήσεις είναι και τα δύο μοναδικά για το άτομο και μετρήσιμα, ακόμη κι αν τα πρότυπα που χρησιμοποιούνται στην πράξη για την τεχνική μέτρησή τους εμπεριέχουν έναν ορισμένο βαθμό πιθανολογήσεως. Πρόκειται, δηλαδή, για μόνιμα γνωρίσματα ενός ανθρώπου, μέσω των οποίων είναι δυνατή η αναγνώριση ή επαλήθευση της ταυτότητάς του. Σε αυτά ανήκουν τα γενετικά δεδομένα (DNA), τα σωματικά χαρακτηριστικά (π.χ. δακτυλικά αποτυπώματα, ίριδα ματιού, γεωμετρία προσώπου) ή ακόμα και στοιχεία συμπεριφοράς (π.χ. τρόπος βαδίσματος ή πληκτρολογήσεως). Τα στοιχεία αυτά στο βαθμό που αποτελούν τμήμα της φυσιολογίας του ίδιου του ατόμου είναι αναλλοίωτα και ανά πάσα στιγμή διαθέσιμα.

Τα βιομετρικά συστήματα αναφέρονται στις αυτοματοποιημένες μεθόδους αναγνωρίσεως ενός προσώπου μέσω της χρήσεως των χαρακτηριστικών της φυσιολογίας ή της συμπεριφοράς. Σε αυτό το πλαίσιο, ένα βιομετρικό δείγμα συγκρίνεται με ένα βιομετρικό «πρότυπο», το οποίο αναφέρεται σε μια έκδοση ενός χαρακτηριστικού που κωδικοποιείται από έναν αλγόριθμο υπολογιστή, έτσι ώστε οι συγκρίσεις των καταχωρισμένων γνωρισμάτων να προσδιορίζουν επαρκώς το συγκεκριμένο άτομο. Τα βιομετρικά χαρακτηριστικά περιλαμβάνουν τεχνικές που χρησιμοποιούνται για τον εντοπισμό των ατόμων με βάση ένα συγκεκριμένο χαρακτηριστικό ή φυσικά χαρακτηριστικά μοναδικά για το άτομο. Κάθε ανθρώπινο χαρακτηριστικό της φυσιολογίας ή και της συμπεριφοράς μπορεί να χρησιμοποιηθεί ως βιομετρικό χαρακτηριστικό, εφ' όσον πληροί τις ακόλουθες προϋποθέσεις:

a. ***Καθολικότητα:*** κάθε άτομο πρέπει να έχει το χαρακτηριστικό.
b. ***Ο διακριτικός χαρακτήρας:*** κάθε δύο άτομα θα πρέπει να είναι αρκετά διαφορετικά από την άποψη των χαρακτηριστικών.
c. ***Μονιμότητα:*** το χαρακτηριστικό θα πρέπει να είναι επαρκώς αμετάβλητο για ένα χρονικό διάστημα.
d. ***Μετρησιμότητα:*** το χαρακτηριστικό μπορεί να μετρηθεί ποσοτικά

Τα βιομετρικά χαρακτηριστικά αξιολογούνται μέσα από μια ποικιλία παραγόντων, όπως η ακρίβεια της αναγνωρίσεως, η ταχύτητα, οι απαιτήσεις πόρων, οι επιπτώσεις

για τους χρήστες (το σύστημα βιομετρικών στοιχείων θα πρέπει να είναι σχετικά ακίνδυνο), η αποδοχή τους από τον πληθυσμό και η αντίστασή τους σε διάφορες δόλιες μεθόδους εξαγωγής λανθασμένων συμπερασμάτων. Σημαντική κατηγοριοποίηση των βιομετρικών συστημάτων αναφορικά με την κρίση περί νομιμότητας λειτουργίας τους είναι η διάκριση σε αυτά που αφήνουν ίχνη και σε αυτά που δεν αφήνουν και, ως εκ τούτου, σε αυτά που συλλέγονται εν γνώσει του υποκειμένου των δεδομένων και σε αυτά που συλλέγονται εν αγνοία του. Η συλλογή δακτυλικών αποτυπωμάτων μπορεί να λάβει χώρα εν αγνοία του προσώπου, στο οποίο αυτά αναφέρονται, σε αντίθεση με το βιομετρικό δεδομένο της ίριδας του ματιού. Οι νέες κάμερες με υψηλή ανάλυση επιτρέπουν με μια μόνο λήψη, την βιομετρική ανάλυση του προσώπου καθενός από τους χιλιάδες θεατές που ακολουθούν μια διαδήλωση ή βρίσκονται σε ένα στάδιο.

Τα συνηθέστερα βιομετρικά χαρακτηριστικά είναι τα ακόλουθα:

1.7.1 Εικόνα του προσώπου

Η εικόνα του προσώπου είναι το πιο ευρέως χρησιμοποιούμενο βιομετρικό χαρακτηριστικό. Πολλοί άνθρωποι παρουσιάζουν μια φωτογραφία ταυτότητάς τους σχεδόν σε καθημερινή βάση. Μέσω της χρήσεως βιομετρικών συστημάτων είναι δυνατό το συγκεκριμένο άτομο να ταιριάζει με την εικόνα του. Δυσκολία προσδιορισμού παρουσιάζεται, όταν η εικόνα του προσώπου έχει ληφθεί από μία δραστικά διαφορετική οπτική γωνία από την αποθηκευμένη εικόνα. Τίθεται επίσης το ερώτημα κατά πόσον το πρόσωπο παρέχει επαρκή βάση για την αναγνώριση ενός μεγάλου αριθμού των ταυτοτήτων, δεδομένων των φυσικών μεταβολών που υφίσταται κατά τη διάρκεια της διαδικασίας γηράνσεως ή των τεχνητών μεταβολών μέσω του μακιγιάζ ή της αλλαγής της κομμώσεως.

1.7.2 Υπογραφή

Είναι κοινώς αποδεκτό ότι η υπογραφή ενός ατόμου είναι μοναδική για αυτό. Τα βιομετρικά στοιχεία υπογραφής αποτελούν παράδειγμα νέων χρήσεων παραδοσιακών βιομετρικών τεχνολογιών. Ωστόσο, οι υπογραφές συνιστούν έκφανση ανθρώπινης συμπεριφοράς και μπορούν να αλλάξουν κατά τη διάρκεια μιας χρονικής περιόδου, καθώς επίσης και να επηρεάζονται από φυσικές και συναισθηματικές αλλαγές στο πρόσωπο. Επαγγελματίες πλαστογράφοι παραχαράκτες είναι σε θέση να αναπαράγουν υπογραφές δυνάμενες να ξεγελάσουν τα βιομετρικά συστήματα.

1.7.3 Δακτυλικά αποτυπώματα

Η αναγνώριση δακτυλικών αποτυπωμάτων συγκαταλέγεται μεταξύ των παλαιότερων, ευρύτερα μελετημένων και εκτενέστερα ανεπτυγμένων βιομετρικών συστημάτων. Συστήματα αναγνωρίσεως δακτυλικών αποτυπωμάτων χρησιμοποιούνται πολύ συχνά, λόγω της ακρίβειάς τους για τον εντοπισμό ενός ατόμου. Η μέθοδος της σαρώσεως δακτυλικών αποτυπωμάτων είναι επίσης εξαιρετικά προσιτή. Ωστόσο, οι μέθοδοι αναγνωρίσεως δακτυλικών αποτυπωμάτων δεν είναι πάντοτε αλάνθαστοι. Γενετικοί παράγοντες, η γήρανση, το περιβάλλον ή επαγγελματικοί λόγοι (π.χ. όσοι εκπονούν χειρωνακτική εργασία παρουσιάζουν πλήθος από κοψίματα και μώλωπες) δύνανται να μεταλλάσσουν συνεχώς τα δακτυλικά αποτυπώματά τους.

1.7.4 DNA (δεσοξυριβονουκλεϊκό οξύ)

Αυτό βρίσκεται στον πυρήνα των κυττάρων του κάθε ατόμου. Είναι μοναδικό για κάθε άτομο, με την εξαίρεση των πανομοιότυπων διδύμων που μοιράζονται το ίδιο DNA. Συνοδεύει τον άνθρωπο από τη στιγμή της γεννήσεώς του μέχρι το θάνατό του παραμένοντας αναλλοίωτο20, σε αντίθεση με τα δακτυλικά αποτυπώματα που αλλοιώνονται ή και εξαφανίζονται από τη χειρωνακτική εργασία, επεμβάσεις ή ασθένειες. Ένα από τα σημαντικότερα ζητήματα που σχετίζονται με τη δημιουργία βάσεων δεδομένων DNA είναι το γεγονός ότι τα γενετικά δεδομένα που προέρχονται από δείγματα DNA (γενετικούς τόπους) μπορούν να αποκαλύψουν - όχι άμεσα κατά τη φάση της συλλογής πληροφορίες σχετικά με την κατάσταση της υγείας, την προδιάθεση για ασθένειες ή την εθνοτική καταγωγή. Περαιτέρω, αξίζει να σημειωθεί ότι η πρώτη ύλη επί της οποίας γίνονται οι γενετικές αναλύσεις μπορεί εύκολα να διασπείρεται στο περιβάλλον χωρίς καν το άτομο να το αντιλαμβάνεται, και να μεταφέρεται στον τόπο του εγκλήματος με σκοπό τον αποπροσανατολισμό των ερευνών ή την ενοχοποίηση ή απενοχοποίηση συγκεκριμένων ατόμων. Με τον τρόπο αυτό, οι γενετικές πληροφορίες μπορεί να οδηγήσουν στην αντιμετώπιση ατόμων ως μη ισοτίμων μελών της κοινωνίας βάσει γενετικών διακρίσεων και γενετικού στιγματισμού. Για το λόγο αυτό, η δημιουργία βάσεων δεδομένων DNA ενέχει σημαντικό κίνδυνο για την ανθρώπινη αξιοπρέπεια και τα θεμελιώδη δικαιώματα. Η εξέταση του DNA συγκεκριμένου προσώπου, ώστε να διακριβωθεί η συμμετοχή του σε συγκεκριμένες εγκληματικές πράξεις ή και η συγκρότηση ειδικής τράπεζας όπου θα καταχωρίζεται το γενετικό αποτύπωμα ήδη καταδικασθέντων προσώπων μπορεί

να γίνουν αποδεκτά υπό την προϋπόθεση της ειδικής νομοθετικής ρυθμίσεως που προβλέπει μείζονες ουσιαστικές και διαδικαστικές εγγυήσεις. Ήδη το Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ) έχει αναγνωρίσει την επεξεργασία του γενετικού υλικού ως έναν από τους θεμιτούς περιορισμούς της πληροφοριακής αυτοδιαθέσεως του ατόμου. Βάσει τηςΣυνθήκης Prüm, γνωστής και ως "Schengen III", προβλέπεται η διακρατική συνεργασία για την άμεση πρόσβαση των κρατικών αρχών κάθε κράτους – μέλους σε όλες τις εθνικές βάσεις δεδομένων DNA και δακτυλικών αποτυπωμάτων με σκοπό τη διερεύνηση και καταστολή εγκλημάτων. Επίσης, βάσει της Αποφάσεως 2008/615/ΔΕΥ του Συμβουλίου της Ευρωπαϊκής Ενώσεως, «σχετικά με την αναβάθμιση της διασυνοριακής συνεργασίας, ιδίως όσον αφορά την καταπολέμηση της τρομοκρατίας και του διασυνοριακού εγκλήματος», με την οποία ολοκληρώθηκε η μεταφορά της Συνθήκης του Prüm στο κοινοτικό κεκτημένο και τέθηκε η νομική βάση για τη δημιουργία του μεγαλύτερου πανευρωπαϊκού δικτύου βάσεων δεδομένων των αστυνομικών αρχών, κάθε κράτος μέλος δεν δικαιούται απλώς, αλλά υποχρεούται πλέον να δημιουργήσει αρχεία DNA για τη διεύρυνση αξιόποινων πράξεων, ενώ έχει επιπλέον την υποχρέωση να παρέχει πρόσβαση στα άλλα κράτη μέλη για την αυτοματοποιημένη αναζήτηση γενετικών αποτυπωμάτων. Με την εν λόγω Απόφαση η χώρα μας ανέλαβε διεθνείς δεσμεύσεις αναφορικά με την υποχρέωση συστάσεως εθνικών αυτοματοποιημένων αρχείων DNA και τη μέσω αυτής διευκόλυνση της διασυνοριακής ανταλλαγής πληροφοριών για την πρόληψη και διερεύνηση αξιόποινων πράξεων. Συγκεκριμένα, με βάση το άρθρο 2 παρ. 1 α΄ της Αποφάσεως, η Ελλάδα ανέλαβε την υποχρέωση για την εντός τριών ετών σύσταση και τήρηση εθνικής βάσεως DNA καθώς και για την ανταλλαγή δεδομένων με άλλες εθνικές βάσεις προς το σκοπό της διερευνήσεως αξιόποινων πράξεων. Σύμφωνα με το άρθρο 7 της Αποφάσεως, η Ελλάδα ανέλαβε την υποχρέωση για παροχή νομικής συνδρομής μέσω της συλλογής και εξετάσεως κυτταρικού υλικού σχετικά με συγκεκριμένο και ευρισκόμενο στο έδαφός της πρόσωπο, εφόσον δεν υπάρχει ήδη διαθέσιμο το γενετικό του προφίλ στα εθνικά αρχεία.

Αναφορικά με τον τρόπο λήψεως του γενετικού υλικού, σύμφωνα με το άρθρο 5 της Συμβάσεως 108 του Συμβουλίου της Ευρώπης, όλες οι πληροφορίες πρέπει να αποκτώνται «κατά τρόπο έντιμο και νόμιμο». Περαιτέρω, σύμφωνα με την αρχή 4 της Συστάσεως R (92) 1, στις περιπτώσεις που το εθνικό δίκαιο επιτρέπει τη λήψη

γενετικού υλικού μπορεί να γίνεται και παρά την αντίθετη βούληση του ατόμου, χωρίς όμως να διευκρινίζεται εάν είναι θεμιτή η χρήση βίας για τη λήψη γενετικού υλικού ή εάν απλώς μπορεί να χρησιμοποιείται γενετικό υλικό που το άτομο διασπείρει στο περιβάλλον29. Το ζήτημα αυτό θίγεται στην παράγραφο 43 της αιτιολογικής εκθέσεως της Συστάσεως, σύμφωνα με την οποία για το ζήτημα της λήψεως θα αποφασίσει κάθε κράτος αυτοτελώς βάσει της αρχής της αναλογικότητας. Σύμφωνα με τη Γνώμη της Επιτροπής Βιοηθικής για τη συλλογή και διαχείριση των γενετικών δεδομένων30, η βίαιη αφαίρεση υλικών από το ανθρώπινο σώμα με σκοπό τη γενετική ανάλυση προσβάλλει σε κάθε περίπτωση την ανθρώπινη αξιοπρέπεια και δεν μπορεί να γίνει αποδεκτή.

1.7.5 Τρόπος πληκτρολογήσεως

Υποστηρίζεται ότι κάθε άτομο κτυπάει τα πλήκτρα σε ένα πληκτρολόγιο με μοναδικό τρόπο31 και, ως εκ τούτου, ο τρόπος πληκτρολογήσεως θα μπορούσε να μας προσφέρει πληροφορίες για την ταυτότητα του ατόμου. Ωστόσο, το χαρακτηριστικό αυτό απορρέει από τη συμπεριφορά του ατόμου και μπορεί να αλλάξει με την πάροδο του χρόνου.

1.7.6 Ίριδα του ματιού

Η ίριδα είναι η χρωματιστή περιοχή του ματιού. Η οπτική υφή της διαμορφώνεται κατά τη διάρκεια της εμβρυϊκής αναπτύξεως και καθίσταται μόνιμη από την ηλικία των δύο ετών. Τα συστήματα ανιχνεύσεως ίριδας ήταν στο παρελθόν πολύπλοκα και ακριβά, ενώ τα νεότερα συστήματα είναι πιο προσιτά και φιλικά προς το χρήστη. Ιαπωνικές τράπεζες χρησιμοποιούν τη μέθοδο της σαρώσεως του αμφιβληστροειδούς (μίας διαδικασίας επαχθέστερης από τη σάρωση της ίριδας) για τις αυτόματες τραπεζικές συναλλαγές από τα μέσα της δεκαετίας του 199036. Περαιτέρω βιομετρικά χαρακτηριστικά είναι η δομή του προσώπου, η φωνή, αλλά και η γεωμετρία των χεριών, η μορφή των φλεβών, ο ιδιαίτερος τρόπος βαδίσματος ή ομιλίας

1.8 ΤΕΧΝΟΛΟΓΙΑ

1.8.1 Βασικά Τεχνολογίας

Η Ασφαλής ομάδα Mobile Solutions έχει τα προϊόντα που ταιριάζουν με την εφαρμογή ePassport στο χαρτοφυλάκιό της.

Αυτά περιλαμβάνουν:

- 16-bit ασφαλή προϊόντα ανέπαφων μικροελεγκτή
- 3ο μέρος του λογισμικού λειτουργικών
- 3rd Party Ψηφίδες

Μέσω της δημιουργίας στενών δικτύων αξίας των συνεργατών της, και ιδίως με τα μέλη της Silicon Trust, η Infineon μπορεί επίσης να φροντίσει για έναν πλούτο των τεχνολογικών απαιτήσεων καθώς και προσαρμοσμένες λύσεις ασφάλειας.

1.8.2 Τύποι chip

Ένα κοινό νήμα σε όλο αυτό το έγγραφο έχει η σημασία που δίνεται στο τσιπ. Λαμβάνοντας υπόψη το είδος των εφαρμογών που δημιουργείται τώρα, που συχνά απαιτούν κάτι περισσότερο από φορητές δυνατότητες αποθήκευσης δεδομένων, αλλά και την υπολογιστική δύναμη των προηγμένων τσιπ μικροελεγκτών, αυτό δεν αποτελεί έκπληξη.

Οι μάρκες που διατίθενται για ηλεκτρονικά διαβατήρια είναι ανέπαφα κρυπτογραφικά τσιπ που μπορεί να εκτελέσουν υπολογισμούς πολύπλοκης κρυπτογράφησης. Ανέπαφα ολοκληρωμένα κυκλώματα λειτουργούν μέσω των ηλεκτρομαγνητικών κυμάτων, τα οποία αποδεικνύονται τα προϊόντα της επιλογής για όλες τις εφαρμογές που απαιτούν εύκολη και βολική αναγνώριση του χρήστη, χωρίς την ανάγκη για σωματική επαφή του φυλλαδίου με μια συσκευή ανάγνωσης / εγγραφής. Είναι πολύ σημαντικό να αναφερθεί ότι η μετάδοση δεδομένων "over the air» δεν έχει καμία απολύτως επίπτωση στην προστασία της ιδιωτικής ζωής των δεδομένων, η οποία προστατεύεται από κρυπτογράφηση, όχι από τη διασύνδεση. Πολλές δημοσιεύσεις έχουν, δυστυχώς, δημιουργήσει την εντύπωση ότι χωρίς επαφή που πραγματοποιούν τα τσιπ είναι εύκολο να παρακολουθούνται ή να χειραγωγείται από μεγάλη απόσταση, το οποίο απλά δεν είναι αλήθεια. Αν και είναι δυνατόν να ανιχνευθεί η επικοινωνία μεταξύ ενός αναγνώστη και ενός τσιπ από απόσταση αρκετών μέτρων, αυτό δεν σημαίνει ότι κάποιος μπορεί να διαβάσει ή να χειριστεί δεδομένα, εάν χρησιμοποιείται κρυπτογράφηση.

1.8.3 Ελεγκτές Contactless

Ανέπαφοι ελεγκτές από την Infineon να υποστηρίξουν μια σειρά διεπαφών εγγύτητας για την παγκόσμια διαλειτουργικότητα. Οι σχεδιαστές μπορούν να επιλέξουν από ένα ευρύ φάσμα EEPROMs να αντανακλά τις ατομικές ανάγκες.

Η διπλή διεπαφή, ανεπαφικού ελεγκτή SLE 66CL160S ήταν η πρώτη του ελεγκτή κλάδου για την υποστήριξη των δύο ανέπαφων μεθόδων διαμόρφωσης για μετάδοση στο 13,56 MHz ζώνη ραδιοσυχνοτήτων, τύπου A και τύπου B, σε πλήρη συμμόρφωση με το πρότυπο ISO 14443.

Ο SLE 66CLX321P και ο SLE 66CLX641P βασίζονται στην πλατφόρμα 66P (βλέπε πίνακα 5). Αυτά τα ολοκληρωμένα κυκλώματα multi-mode υποστήριξης των βασικών τύπων διασύνδεσης εγγύτητας σε συνδυασμό με κορυφαίας απόδοσης και ασφάλειας, συμπεριλαμβανομένου του υλικού με βάση επιταχυντών DES, Ελλειπτικές Καμπύλες και RSA αλγορίθμους.

Για να συνεχιστεί αυτή η επιτυχημένη πορεία του προϊόντος, η Infineon εισήγαγε 66P ΕΝΙΣΧΥΜΕΝΗ οικογένειά με αυξημένη παράσταση, την ευκολία χρήσης, την ασφάλεια και την αποτελεσματικότητα του κόστους, το οποίο η εταιρεία πιστεύει ότι θα οδηγήσει σε ένα νέο πρότυπο 16-bit εφαρμογών έξυπνων καρτών.

Εξοπλισμένο με ένα εσωτερικό ρολόι τρέχει έως 33 MHz σε συνδυασμό με ένα αυτόματο σύστημα διαχείρισης ενέργειας, η σειρά 66PE θα προσφέρει τη μέγιστη απόδοση με το λογισμικό του χρήστη. Νέα προϊόντα που βασίζονται στην πλατφόρμα 66PE είναι υπό ανάπτυξη.

Πρόσθετα χαρακτηριστικά ασφαλείας, όπως αφρώδη κρυπτογράφηση λεωφορείου, ένα ενισχυμένο ρεύμα scrambler και ένα υλοποιημένο αυτόματο μηχανισμό αντι-σχίσιμο να σταθεροποιήσει τη θέση της Infineon Τεχνολογίας, ως κορυφαία εταιρεία στον κόσμο για τους ελεγκτές ασφαλείας.

1.8.4 Κρυπτογραφία ελεγκτών

Η Infineon προσφέρει μια σειρά από ενότητες ασφάλειας κρυπτογράφησης με 66s και 66P / οικογένειες 66PE / 88p.

- 1.100-bit Κρυπτογραφία κινητήρα: το ACE είναι ο αριθμητικός συνεπεξεργαστής για γρήγορο υπολογισμό της ασύμμετρου δημόσιου κλειδιού αλγορίθμων (π.χ. RSA). Είναι εξοπλισμένο με 700 bytes της RAM

- 1408-bit Κρυπτογραφία κινητήρα (Κρυπτογραφία @ 1408Bit): η Κρυπτογραφία @ 1408bit υποστηρίζει όλους τους ασύμμετρους αλγόριθμους που βασίζονται σε αριθμητικά υπόλοιπα, συμπεριλαμβανομένης της RSA, Ελλειπτικές Καμπύλες GF (p) και GF2n. Η μοναδική σχεδίαση του είναι η ταχύτερη μηχανή που το κάνει: να εκτελεί μια RSA 1024-bit υπογραφή με CRT (Κινέζικο Θεώρημα Υπολοίπων) σε μόλις 4 ms και μια υπογραφή 2048-bit _ μόνο 35 ms. Είναι εξοπλισμένο με 880 bytes της Crypto RAM και πρόγραμμα οδήγησης συσκευής του περιλαμβάνεται στο στρώμα υποστήριξη πλατφόρμας της οικογένειας 88
- DES (Data Encryption Standard) Επιταχυντής: ο επιταχυντής DES εκτελεί γρήγορα τους συμμετρικούς DES και Triple DES αλγόριθμους
- Ελλειπτική καμπύλη: η ελλειπτική καμπύλη πυρήνα υποστηρίζει πολλαπλασιασμό και πρόσθεση _ πεδίου Galois GF2n, n ≤ 191. ελλειπτικών καμπυλών GF (p) που υποστηρίζονται από την ACE
- AES (Advance Encryption Standard): ο αλγόριθμος AES υποστηρίζεται από εφαρμογές των σημειώσεων για ελεγκτές 66P / 88p

1.8.5 Η RSA 2048 Βιβλιοθήκη

Αυτή είναι μια ισχυρή, πολυ-λειτουργική βιβλιοθήκη Crypto για ελεγκτές η Infineon με SLE 66CXxxP / PE και SLE 66CLXxxP συνεπεξεργαστών / PE Crypto. Παρέχει αριθμητικές λειτουργίες για εύκολο προγραμματισμό του ACE. Περιλαμβάνει επίσης την πλήρη εφαρμογή RSA υπολογισμοί σημάδι, να ελέγχει και την παραγωγή κλειδιών. Υποστηρίζει έως 2.048 -bit μήκη κλειδιού. Ισχυρό SPA / DPA και DFA αντίμετρα παρέχονται επίσης με αυτήν τη βιβλιοθήκη. Στο πλαίσιο της αξιολόγησης της ασφάλειας οποιουδήποτε νέου ελεγκτή 66P / 66PE ξεκινώντας με το SLE 66CX322P, η RSA2048 βιβλιοθήκη έχει πιστοποιηθεί σύμφωνα με κοινά κριτήρια EAL-5 + (με BSI-PP-0002 προφίλ προστασίας).

ΚΕΦΑΛΑΙΟ 2

2.1 ΑΣΦΑΛΕΙΑ ΩΣ ΠΡΟΤΥΠΟ

Παρόλο που η ασφάλεια είναι υψίστης σημασίας, πρέπει να γίνει κατανοητό από την αρχή ότι το 100% ασφάλεια δεν είναι ποτέ δυνατόν. Ωστόσο, μια καλή προσέγγιση ασφάλειας θα εξασφαλίσει ότι τα χρήματα, ο χρόνος και η προσπάθεια που απαιτείται για να σπάσει ένα σύστημα που δεν θα άξιζε την πιθανή ανταμοιβή. Αυτό το εμπόδιο για να επιτεθούν, θα αποδυναμώσει την πάροδο του χρόνου, καθώς ανακαλύπτονται νέες μέθοδοι hacking, αλλά οι νέες τεχνικές ασφαλείας θα προκύψουν επίσης για να διασφαλιστεί η ασφάλεια του συστήματος που παραμένει τουλάχιστον ένα βήμα μπροστά από τις ικανότητες των hackers.

Πίσω από τα περισσότερα συστήματα ταυτοποίησης, όπως είναι το ηλεκτρονικό διαβατήριο, υπάρχει ένα σύστημα πληροφορικής, το οποίο θα εκτελεί λειτουργίες, όπως η αποθήκευση και επικυρώνει τις προσωπικές πληροφορίες των χρηστών. Υπάρχουν τέσσερα σημαντικά ζητήματα ασφάλειας που πρέπει να έχουν καλύψει τα συστήματα αυτά:

- *Ασφαλής Έλεγχος ταυτότητας* - εξασφαλίζει ότι μόνο οι νόμιμοι χρήστες μπορούν να έχουν πρόσβαση σε ορισμένα δεδομένα ή να εκτελέσουν συγκεκριμένες ενέργειες
- *Εμπιστευτικότητα των δεδομένων* - διασφαλίζει ότι τα προσωπικά ή ευαίσθητα δεδομένα προστατεύονται από μη νόμιμους χρήστες
- *Ακεραιότητα δεδομένων* - διασφαλίζει ότι τα δεδομένα δεν μεταβάλλονται σκόπιμα από μη νόμιμους χρήστες
- *Δεδομένα Διαθεσιμότητας* - διασφαλίζει ότι τα δεδομένα που διατίθενται με το σωστό άτομο, όποτε είναι απαραίτητο

Τα θέματα αυτά συνήθως επιτυγχάνονται με τη χρήση διαφορετικών μέτρων ασφαλείας. Για παράδειγμα, ο έλεγχος ταυτότητας μπορεί να επιτευχθεί με τη χρήση ενός κωδικού πρόσβασης, PIN ή βιομετρικά, όπως ένα δακτυλικό αποτύπωμα, ενώ η εμπιστευτικότητα μπορεί να διατηρηθεί με τη λήψη μέτρων κρυπτογράφησης.

Είναι λοιπόν σαφές ότι, ένα αποτελεσματικό σύστημα ασφαλείας δεν θα βασίζεται σε ένα ενιαίο μηχανισμό ασφάλειας. Μετά από όλα, αν η πόρτα σε ένα σπίτι έχει την πιο εκλεπτυσμένη κλειδαριά γνωστή για την ανθρωπότητα, αλλά οι μεντεσέδες του είναι

σκουριασμένο ή υπάρχει ένα παράθυρο που παραμείνει ανοικτό, τότε το μόνο ισχυρό μέτρο ασφαλείας θα παρακαμφθεί. Επιτυχής ασφάλεια θα δούμε σε ένα χαρτοφυλάκιο των μέτρων ασφαλείας για την εξασφάλιση του συνολικού συστήματος που μπορεί να διατηρούνται ασφαλείς από την επίθεση. Είναι καλύτερα αν αυτά τα μέτρα ασφάλειας είναι παρόμοιας δυσκολίας να ξεπεραστούν, καθώς το σημείο της επίθεσης κανονικά πάντα θα είναι στο πιο αδύναμο σημείο.

2.2 ΘΕΜΑΤΑ ΠΙΣΤΟΠΟΙΗΣΗΣ

Ο χρήστης οποιουδήποτε συστήματος ασφαλείας έχει κανονικά τρεις ερωτήσεις - είναι ασφαλές το σύστημα, πόσο ασφαλής είναι και πόσο κοστίζει; Για λίγο περισσότερο από μια δεκαετία οι εκδότες έχουν τη δυνατότητα να εξετάσουμε τις αξιολογήσεις ασφάλειας που διενεργούνται από ανεξάρτητους φορείς, όπως είναι οι κυβερνήσεις. Στην Ευρώπη, τα κριτήρια Πληροφορικής Αξιολόγησης Ασφάλειας (ITSEC) πρότυπα αναπτύχθηκαν και συμφωνήθηκαν από τη Γαλλία, τη Γερμανία, τις Κάτω Χώρες και το Ηνωμένο Βασίλειο το 1991. Εν τω μεταξύ, οι ΗΠΑ (Κριτήρια TCSEC -Trusted Υπολογιστικό Σύστημα Αξιολόγησης) και τον Καναδά (CTCPEC - καναδική αξιόπιστο υπολογιστή Προϊόν Κριτήρια Αξιολόγησης) είχαν αναπτύξει διαφορετικά πρότυπα. Πιο πρόσφατα Κοινά Κριτήρια πρότυπα (ISO / IEC 15408), όπως σε όλο τον κόσμο με τα ισχύοντα πρότυπα ασφάλειας, έχουν προκύψει οι οποίοι συγκεντρώνουν όλες αυτές τις πρωτοβουλίες για τη δημιουργία ενός συστήματος που έχει νόημα σε ένα ευρύτερο κοινό.

Το πλεονέκτημα της ύπαρξης ενός πιστοποιημένου προϊόντος, όπως μια έξυπνη κάρτα με τσιπ, είναι το υψηλό επίπεδο εμπιστοσύνης που προέρχεται από την ανεξάρτητη αξιολόγηση, ενώ αποδεικνύει ότι ο πωλητής του προϊόντος ήταν πρόθυμος να θέσει το προϊόν τους σε δοκιμασία.

ITSEC και κοινή πιστοποίησης κριτήρια έχουν αναλογική κλίμακα που μπορεί να ανατεθεί σε ένα συγκεκριμένο προϊόν, με _ κορυφή της κλίμακας είναι υψηλή ασφάλεια και το κάτω μέρος της κλίμακας που αντιπροσωπεύουν πολύ χαμηλά επίπεδα ασφάλειας. Σύμφωνα με τα συστήματα πιστοποίησης, κάθε ηλεκτρονικό προϊόν ή σύστημα που υποστηρίζει να έχουν την ικανότητα ασφάλειας μπορεί να αξιολογηθεί. Αυτό μπορεί να περιλαμβάνει μια σειρά από προϊόντα, όπως τα λειτουργικά συστήματα, συστήματα διαχείρισης βάσεων δεδομένων, αντιπυρικές ζώνες, τις έξυπνες κάρτες, και τα τσιπ στο επίκεντρο μιας έξυπνης κάρτας και το σύστημα PKI.

Στην πράξη, οι περισσότερες αξιολογήσεις συνήθως πραγματοποιούνται σε συστατικά στοιχεία του λογισμικού, αλλά το πεδίο αρχίζει να διευρυνθεί για να συμπεριλάβει

περισσότερα firmware και το υλικό. Στόχος της Infineon είναι να παρέχει την καλύτερη ασφάλεια διαθέσιμη για το υλικό - αποδειχθεί και πιστοποιηθεί. Τόσο ITSEC και τα κοινά κριτήρια παρέχουν μια αποτελεσματική διαδικασία για την αξιολόγηση ασφάλειας, αλλά τα κοινά κριτήρια αναμένεται να γίνουν το κυρίαρχο πρότυπο με το οποίο η ασφάλεια θα πρέπει να μετρηθεί. Πολυάριθμες ICs Infineon έχει απονεμηθεί ITSEC E4 Υψηλά πιστοποιητικά. Πολλές από τις τελευταίες αυτές, όπως το SLE 66CX322P, έχουν επίσης επιτύχει Κοινά Κριτήρια EAL5 + και η Infineon έχει δεσμευθεί να συνεχίσει αυτή τη στρατηγική για την επίτευξη αναγνωρισμένης πιστοποίησης ασφάλειας για ολοκληρωμένα κυκλώματα ασφάλειας.

2.3 ΣΕΝΑΡΙΑ ΕΠΙΘΕΣΗΣ

Ως ένα από τα βασικά συστατικά σε πολλά συστήματα αναγνώρισης, είναι σημαντικό ότι κάθε έξυπνη κάρτα με τσιπ είναι τόσο ασφαλές όσο το δυνατόν. Ασφάλεια αρχίζει με την ανάπτυξη προϊόντων, διαδικασιών παραγωγής και παράδοσης, όπου θα πρέπει να συσταθεί μια διαδρομή ελέγχου για κάθε μάρκα. Εξωτερικές επιθέσεις που μπορεί να είναι επεμβατικές ή μη επεμβατικές ανάλογα με τη μέθοδο που χρησιμοποιείται η επίθεση. Μια διεισδυτική επίθεση θα περιλαμβάνει τη φυσική παρέμβαση στη λειτουργία του τσιπ, ενώ μια μη επεμβατική διαδικασία θα μπορούσε, για παράδειγμα, περιλαμβάνουν την παρακολούθηση και ανάλυση της κατανάλωσης ηλεκτρικής ισχύος _ δεδομένου ότι οι διαφορετικές οδηγίες που πραγματοποιούνται.

2.3.1 Φυσική επίθεση

Η αντίστροφη μηχανική είναι μία πιθανή μέθοδος σωματικής επίθεσης ένας χάκερ θα μπορούσε να επιχειρήσει, σε μια προσπάθεια να δημιουργήσει μια παραποιημένη κάρτα, αν και τέτοιου είδους επιθέσεις ενδέχεται να είναι πολύ δαπανηρές. Τίποτα από χημικούς παράγοντες για να αφαιρέσουμε στρώματα στο τσιπ στον βομβαρδισμό ηλεκτρονίων να συμπεράνουμε ηλεκτρικό δυναμικό και δραστηριότητα σε ορισμένα σημεία είναι τα πιθανά σενάρια προσβολής.

2.4 ΗΛΕΚΤΡΙΚΗ ΑΣΦΑΛΕΙΑ

Μία άλλη μέθοδος ανοικτή για το δυνητικό χάκερ είναι να παρακολουθεί την κατανάλωση ρεύματος του τσιπ καθώς εκτελεί διάφορες οδηγίες. Αυτή η διαδικασία πρέπει να επαναληφθεί πολλές φορές χρησιμοποιώντας διαφορετικές τιμές εισόδου. Ηλεκτρικός θόρυβος θα πρέπει επίσης να υποβληθεί σε διαλογή έξω.

Οι κατασκευαστές τσιπ έχουν αναπτύξει διάφορα είδη καμουφλάζ κατά αυτόν τον τύπο επίθεσης, συμπεριλαμβανομένης της χρήσης των πρόσθετων παρεμβολών (άχυρο) ή την μείωση του θορύβου που δημιουργείται από το τσιπ, μέσω ειδικών κυκλωμάτων φιλτραρίσματος. Infineon εξαλείφει τη ρίζα του κακού αυτού του αποτελέσματος μέσω ειδικής μεθοδολογίας σχεδιασμού που εφαρμόζονται σε ζωτικά μέρη του τσιπ, όπως cryptocoprocessors.

2.5 ΚΩΔΙΚΟΣ BREAKING

Ένα κρίσιμο μέρος της ασφάλειας μιας έξυπνης κάρτας πηγάζει από τους αλγόριθμους που χρησιμοποιούνται για την κρυπτογράφηση των δεδομένων εντός της έξυπνης κάρτας. Η κύρια ευπάθεια έρχεται καθώς αυτά τα δεδομένα διέρχονται από την κάρτα σε έναν αναγνώστη όταν μια συναλλαγή λαμβάνει χώρα.

Καθώς και οι Data Encryption Standard (DES) αλγόριθμοι, οι έξυπνες κάρτες χρησιμοποιούν όλο και περισσότερο τα συστήματα υποδομής δημόσιου κλειδιού (PKI), οι οποίες συνήθως βασίζονται σε αλγορίθμους RSA, ωστόσο, ελλειπτικά η καμπύλη κρυπτογραφίας (ECC) είναι μια βιώσιμη εναλλακτική λύση και έχει το πλεονέκτημα ότι, για την ίδια δύναμη η ασφάλεια) χρειάζεται ένα μικρότερο κλειδί.

2.6 CONTACTLESS CHIP ΑΠΕΙΛΕΣ

Έχοντας υπόψη ότι το ηλεκτρονικό διαβατήριο θα χρησιμοποιήσει τα τσιπ ανέπαφων, είναι σημαντικό να κατανοήσουμε τις λεωφόρους της προσβολής που μπορεί να προκύψουν λόγω του γεγονότος ότι μία ραδιοσυχνότητα σύνδεση (RF) συμμετέχει. Μια ποικιλία των απειλών παρουσιάζονται παρακάτω.

Όπως ήταν αναμενόμενο, οι υποκλοπές είναι η πιο κοινή απειλή που αντιμετωπίζει ανέπαφες μάρκες. Είναι πιθανό ότι ένα άτομο μπορεί να παρακολουθήσει και να ακούσει την επικοινωνία μεταξύ του αναγνώστη και του τσιπ, χωρίς αρχές »ή τις γνώσεις κατόχου του διαβατηρίου.

Αν και δεν είναι υποχρεωτική στις προδιαγραφές ePassport, τα επιμέρους κράτη είναι σε θέση να προφυλαχθούν από αυτή με την εφαρμογή ενός μηχανισμού ελέγχου της πρόσβασης ώστε να αποτραπεί η αποκορύφωση και οι υποκλοπές δεδομένων. Εάν ένας τέτοιος μηχανισμός υποστηρίζεται, τότε ICAO λέει ότι τα περιεχόμενα του τσιπ θα πρέπει να διαβάζονται μόνο αφού ο κομιστής έχει πρόθυμα προσφέρει MRTD (Μηχαναγνώσιμη ταξιδιωτικού εγγράφου) τους για επιθεώρηση. Για να εξασφαλιστεί αυτό, ο επιθεωρητής διαβατήριο απαιτεί την ανάκτηση πληροφοριών που μπορούν να βρεθούν στην

Μηχαναγνώσιμη Ζώνη του διαβατηρίου (MRZ). Αυτό εκκινεί μία διαδικασία πρόκλησης-απόκρισης μεταξύ του αναγνώστη και του τσιπ, και μόλις επιβεβαιωθεί η ταυτότητα, το τσιπ κατόπιν απαιτεί να κρυπτογραφήσει το κανάλι επικοινωνίας μεταξύ της ίδιας και του αναγνώστη.

Άλλη μία συγκεκριμένη απειλή είναι γνωστή ως Grandmaster Chess επίθεση. Σε αυτήν την περίπτωση, η ομάδα MRTD παρουσιάστηκε από τον εισβολέα στο σύστημα ελέγχου να είναι εξοπλισμένο με ένα ειδικό τσιπ, το οποίο λειτουργεί ως υποκατάστατο για μια πραγματική τσιπ που βρίσκεται σε μια απομακρυσμένη θέση. Το τσιπ στη συνέχεια επικοινωνεί με τον εισβολέα, ο εισβολέας επικοινωνεί με άλλο εισβολέα, και ο άλλος επιτιθέμενος έχει πρόσβαση στο πραγματικό τσιπ. Τυπικά, το σύστημα ελέγχου δεν είναι σε θέση να παρατηρήσει ότι έχει επαληθεύσει ένα απομακρυσμένο τσιπ. Τεχνικά αυτή η επίθεση ήδη θα έχει ληφθεί, ιδίως όταν χρησιμοποιείται ενεργά η ταυτότητα, καθώς αυτό μπορεί να επιτρέψει μια αυτόματη σύγκριση μεταξύ του MRZ που αποθηκεύονται στο τσιπ και του MRZ που αναγράφεται στην σελίδα με τα στοιχεία του MRTD.

Ένα άλλο σενάριο επίθεσης που τίθεται σε συστήματα που χρησιμοποιούν παθητική ταυτότητα, η οποία δεν μπορεί να εμποδίσει την αντιγραφή των δεδομένων που είναι αποθηκευμένα στο τσιπ. Κατά συνέπεια, ένα γνήσιο τσιπ θα μπορούσε να αντικατασταθεί με ένα ψεύτικο τσιπ αποθήκευσης τα δεδομένα αντιγράφονται από το τσιπ του άλλου MRTD. Και πάλι ο ευκολότερος τρόπος γύρω από αυτό είναι να βεβαιωθείτε ότι τα δεδομένα που διαβάζονται από το τσιπ ταιριάζουν στην σελίδα με τα στοιχεία του MRTD .

2.7 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΑΣΦΑΛΕΙΑΣ

Περισσότερα από 50 χαρακτηριστικά ασφαλείας που εφαρμόζονται σήμερα σε ελεγκτές ασφάλειας της Infineon. Ορισμένες λειτουργίες ασφαλείας που βρέθηκαν σε ανέπαφες έξυπνες κάρτες ICs από Infineon Technologies περιλαμβάνουν:

- Αισθητήρας και φίλτρα για τον έλεγχο των συνθηκών λειτουργίας
- Κρυπτογράφηση Μνήμης της ROM, EEPROM και XRAM να αποτρέψει την ανάλυση της μνήμης
- Τα στοιχεία και η διεύθυνση κρυπτογράφησης σε μνήμες και λεωφορεία
- Μονάδα Διαχείρισης Μνήμης (MMU) για ασφαλείς Πολλαπλές εφαρμογές και την προστασία των δεδομένων
- Αφιερωμένη λογική του σχεδιασμού και του υλικού-μέτρων κατά αναλύσεων ισχύος
- Ιδιόκτητο σχέδιο για την ασφάλεια της CPU

- Αφιερωμένη συμμετρικές και ασύμμετρες συσκευές κρυπτο για γρήγορες και ασφαλείς κρυπτο πράξεις
- Η αληθινή γεννήτρια τυχαίων αριθμών για κρυπτογραφικούς σκοπούς και τα χαρακτηριστικά ασφαλείας του υλικού
- Ενεργή θωράκιση ενάντια σε κάθε είδους επεμβατικές επιθέσεις
- Προστασία από την οπτική επιθέσεων χρησιμοποιώντας αισθητήρες φωτός και αλγόριθμους κρυπτογράφησης μνήμης.

2.8 ΣΤΟΧΟΙ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΑΝΑΛΥΣΗ ΜΕΘΟΔΟΛΟΓΙΑΣ

Τα διαβατήρια χρησιμοποιούνται ως κύρια μορφή αναγνώρισης και λόγω της φύσης του περιεχομένου που είναι αποθηκευμένα στο τσιπ ενός e-διαβατήριου, είναι ζωτικής σημασίας ότι το έγγραφο είναι ανθεκτικό και διατηρεί επίσης το απόρρητο των δεδομένων. Εάν μια χώρα εφαρμόζει μόνο την υποχρεωτική απαίτηση ασφάλειας (PA), στη συνέχεια, την αυθεντικότητα και την ακεραιότητα. Αυτό δεν σημαίνει, ωστόσο, ότι αποτρέπει την αντιγραφή δεδομένων, αντικατάσταση τσιπ ή skimming και επίσης δεν εμποδίζει τη εξουσιοδοτημένη πρόσβαση στο e-διαβατήριο. Για μεγαλύτερη ασφάλεια ο ICAO συνιστά την εφαρμογή άλλων μηχανισμών ασφάλειας, όπως:

1. τον ενεργό έλεγχο ταυτότητας να αποτρέψει την αντιγραφή του SOD και τσιπ υποκατάστασης και
2. το πρωτόκολλο ελέγχου βασικής πρόσβασης για την πρόληψη και την αποκορύφωση υποκλοπών στην επικοινωνία μεταξύ του τσιπ e-διαβατήριου και του αναγνώστη.

Μέθοδος	**Οφέλη για την ασφάλεια**	**Ευπάθειες / Αδυναμίες**
Παθητικός έλεγχος ταυτότητας	Παρέχει την αυθεντικότητα, την ακεραιότητα και την SOD LDS	• Η αποτυχία να εντοπίσει την αντικατάσταση τσιπ. • Η αποτυχία για την πρόληψη κατά chip copy, μη εξουσιοδοτημένη πρόσβαση και skimming.

Ενεργός έλεγχο ταυτότητας	Εμποδίζει την επικάλυψη έναντι του SOD και την τροποποίηση τσιπ	την πολυπλοκότητα υλοποίησης, καθώς οι πόροι (μνήμη, CPU) είναι απαραίτητες.
Βασικός έλεγχος πρόσβασης	Εμποδίζει την αποκορύφωση και τις υποκλοπές	Η αποτυχία να εντοπιστεί το chip Αποτυχία για την πρόληψη έναντι αντιγραφής τσιπ. Πολυπλοκότητα υλοποίησης ως επιπλέον πόροι (μνήμη, CPU) που απαιτούνται.

Στην συνέχεια αναλύουμε τα πρωτόκολλα e-διαβατηρίων από την πρώτη αναγνώριση στόχων ασφαλείας τους. Υποθέτουμε ότι μια χώρα εφαρμόζει το υψηλότερο επίπεδο ασφάλειας:

1. *Εμπιστευτικότητα των δεδομένων:* Η εμπιστευτικότητα των δεδομένων εξασφαλίζει την προστασία της ιδιωτικής ζωής των στοιχείων του ηλεκτρονικού διαβατηρίου και την κρυπτογράφηση που είναι η κοινή τεχνική που παρέχει εμπιστευτικότητα. Στην περίπτωση του e-διαβατηρίου, η κρυπτογράφηση χρησιμοποιείται για να δημιουργήσει ένα ασφαλές κανάλι μεταξύ του αναγνώστη e-διαβατήριο και μικροτσίπ. Σημειώστε ότι τα κλειδιά κρυπτογράφησης που χρησιμοποιούνται για την κρυπτογράφηση, πρέπει να φυλάσσεται από μη εξουσιοδοτημένη πρόσβαση.
2. *Ακεραιότητα των δεδομένων:* η ακεραιότητα των δεδομένων αποτρέπει την παράνομη τροποποιήσεις των πληροφοριών που ανταλλάσσονται μεταξύ του αναγνώστη e-διαβατηρίου και μικροτσίπ. Επίσης ο DF, SOD και LDS πρέπει να είναι ασφαλής έναντι μη εξουσιοδοτημένων τροποποιήσεων, δηλαδή, οποιαδήποτε αλλοίωση δεδομένων πρέπει να είναι εύκολα ανιχνεύσιμη από το κέντρο της ασφάλειας των συνόρων.
3. *Προέλευση Δεδομένων ελέγχου ταυτότητας*: Ο έλεγχος ταυτότητας προέλευσης δεδομένων διασφαλίζουν ότι η πηγή της εκπομπής σε ένα πρωτόκολλο είναι

αυθεντικό, δηλαδή, τα στοιχεία σχετικά με το τσιπ θα πρέπει να συνδεθεί με πληροφορίες σχετικά με MRZ και στα δεδομένα που εμφανίζεται στη σελίδα στοιχείων κατόχου e-διαβατηρίου εξετάζεται επί του παρόντος από αξιωματικό ασφαλείας των συνόρων.

3. *Μη αποκήρυξη*: Μη αποκήρυξη παρέχει τη δυνατότητα να αποδειχθεί μια ενέργεια ή ένα γεγονός που έλαβε χώρα, έτσι ώστε οι συμμετέχοντες πρωτοκόλλου δεν μπορούν αργότερα να αρνηθούν τη μεταποίηση ότι τα δεδομένα Epassports έχουν πλεονέκτημα, όπως ο κομιστής e-διαβατηρίου θα είναι φυσικά παρών στο σημείο ελέγχου της ασφάλειας των συνόρων. Παρ 'όλα αυτά, θα ήταν σημαντικό να επιτευχθεί ένα αναμφισβήτητο ψηφιακό δεδομένο από το e-διαβατήριο για μελλοντική επεξεργασία.
4. *Αμοιβαίος έλεγχος ταυτότητας*: Η αμοιβαία πιστοποίηση είναι η διαδικασία κατά την οποία οι δύο συμμετέχοντες για να αποδείξουν την ταυτότητά τους ο ένας στον άλλο. Όπου ο αναγνώστης e-διαβατήριο πιστοποιεί ένα e-διαβατήριο, ο στόχος αυτός προστατεύει τον κάτοχο e-διαβατήριο, καθώς είναι ζωτικής σημασίας για ένα e-διαβατήριο για την εξακρίβωση της ταυτότητας του αναγνώστη epassport πριν δημοσιοποιήσουν οποιαδήποτε προσωπική πληροφορία. Αυτό αποτρέπει τη μη εξουσιοδοτημένη συσκευή ανάγνωσης epassport από τη λήψη βιομετρικών και προσωπικών στοιχείων από ένα e-διαβατήριο.
5. *Πιστοποιητικό Χειραγώγησης*: Το πιστοποιητικό ενεργεί ως διαβεβαίωση off-line από μια αξιόπιστη αρχή ότι το πιστοποιημένο δημόσιο κλειδί ανήκει πραγματικά στον κύριο που έχει στην κατοχή του αντίστοιχο μυστικό κλειδί. Ωστόσο, αυτό είναι η ευθύνη του πρωτοκόλλου για την επικύρωση ότι το αντίστοιχο μυστικό κλειδί είναι στην πραγματικότητα στην κατοχή του ο κύριος που διεκδικεί την ιδιοκτησία του δημόσιου κλειδιού. Ο αναγνώστης του διαβατηρίου θα πρέπει να έχει την εγγύηση ότι τα πιστοποιητικά που υποβλήθηκαν είναι έγκυρα και ταιριάζουν με τα δεδομένα σχετικά με το ηλεκτρονικό διαβατήριο. Ο ICAO έχει εφαρμόσει ένα PKI το οποίο θα ήταν για την αποθήκευση πιστοποιητικών υπογραφής από την έκδοση κρατικών και οργανισμούς.
6. *Κλειδί Freshness και Key Integrity*: Κλειδί Freshness και κλειδί ακεραιότητας προστατεύει από επιθέσεις αναπαραγωγής. Ο αναγνώστης e-διαβατηρίου πρέπει να έχουν ικανοποιητική απόδειξη ότι ένα nonce που παράγεται στα

πρωτόκολλα είναι "φρέσκα" και η ακεραιότητα του που προέρχεται το κλειδί συνόδου σώζεται. Και τα δύο μέρη θα πρέπει επίσης να έχουν αδιαμφισβήτητες αποδείξεις ότι η άλλη πλευρά έχει στην κατοχή του ένα έγκυρο κλειδί συνόδου. Κάθε προηγούμενο διακυβεύεται το κλειδί που θα πρέπει να ανιχνεύονται εύκολα και η εκτέλεση του πρωτοκόλλου θα πρέπει να τερματίσει.

7. *Προώθηση απορρήτου*: Προώθηση απορρήτου ασχολείται με την προστασία των πληροφοριών που δεν ήταν σε κίνδυνο, πριν χαθεί το κλειδί μακροπρόθεσμα. Σε ένα πρωτόκολλο e-διαβατηρίου, απώλεια κλειδιού συνόδου ή το πλήκτρο χρησιμοποιείται για να δημιουργήσει ένα κλειδί συνόδου (KENC και KMAC) δεν θα πρέπει να θέτουν σε κίνδυνο κάθε μελλοντική επικοινωνία.

2.8.1 Στόχοι Επιτιθέμενου

Ο στόχος του εισβολέα είναι να επιτευχθεί το τελικό αποτέλεσμα περιστατικού να αιτιολογεί την επίτευξη αυτού του στόχου για διάφορους λόγους (οικονομικούς, δημοσιότητα, πολιτική).

2.8.2 Δυνατότητες Επιτιθέμενου

Παρακάτω παραθέτουμε την εμπειρία, τις γνώσεις και τις ικανότητες που ένας εισβολέας θα μπορούσε να έχει, και οι οποίες παρέχουν τα συστατικά του προφίλ του εισβολέα. Ανεξάρτητα από αυτά, οι επιτιθέμενοι μπορούν να έχουν πρόσβαση σε ποικίλες ποσότητες:

- Ώρα
- Χρήματα
- Προθυμία αποδοχής ανίχνευσης της προσπάθειας (δηλαδή πιθανότητα ανίχνευσης της επίθεσης κατά τον έλεγχο των συνόρων).

2.8.3 Δυνατότητες χαμηλού κόστους

- Τα δεδομένα διαβατηρίου, αντιγράφονται από τα γνήσια e-διαβατήρια, με εξαίρεση τις πληροφορίες δακτυλικών αποτυπωμάτων.
- Δυνατότητα για να εισαγάγετε ένα ψεύτικο τσιπ σε ένα φυλλάδιο διαβατήριο, π.χ.

- πίσω από ένα αυτοκόλλητο θεώρησης?
- στο εξώφυλλο?
- σε ένα ψεύτικο κάλυμμα αντικατάστασης ανιχνεύσιμη μόνο σε πολύ στενή επιθεώρηση.

- Προγραμματιζόμενα έξυπνων καρτών ανέπαφων και η δυνατότητα αυτές να προγραμματιστούν.
- Ένα ζευγάρι των κλεμμένων ή αγοράσει γνήσια διαβατήρια.

2.8.4 Ικανότητες μεσαίου κόστους

- Λεπτομερή γνώση σχετικά με τους καταλόγους ελαττώματος.
- Δυνατότητα για να καταστρέψει τις μάρκες σε e-διαβατήρια άλλων ανθρώπων εξ αποστάσεως. Αυτό θα επιτρέψει σε έναν εισβολέα να απενεργοποιήσετε e-διαβατήριό του και να αναμιχθώ με τους άλλους ανθρώπους, οι οποίοι δεν λειτουργούν τόσο καλά.
- Η ικανότητα να εκτελέσει μια επίθεση άρνησης υπηρεσίας σε ένα σύστημα ελέγχου. Αυτό θα μπορούσε να γίνει με φυσικό ή μέσω προγραμματισμού (π.χ. ενεργοποίηση υπερχείλιση της στο λογισμικό σύστημα ελέγχου).
- Δυνατότητα να κάνουν τις βίαιες επιθέσεις στην BAC.
- Γνώσεις για τη μητρική OS και το ιδιοκτησιακό αρχικοποίησης και τις διαδικασίες εξατομίκευσης (ενδεχομένως χρειάζεται να χρησιμοποιήσει τα τσιπ κλεμμένων κενά).

2.8.5 Ικανότητες υψηλού κόστους

- Μεγάλος αριθμός των κλεμμένων ή αγόρασαν γνήσια διαβατήρια.
- Δυνατότητα για να εισαγάγετε ένα ψεύτικο τσιπ σε ένα φυλλάδιο διαβατήριο,
  - στην υπάρχουσα πραγματική κάλυψη?
  - στη σελίδα πλαστικοποιημένο διαβατήριο το οποίο είναι ουσιαστικά μη ανιχνεύσιμα, ακόμη και στη στενή επιθεώρηση.
- Τα δεδομένα διαβατηρίου, αντιγράφονται από τα γνήσια e-διαβατήρια, συμπεριλαμβανομένων των πληροφοριών των δακτυλικών αποτυπωμάτων.
- (Κλεμμένα ή αγοράζονται) κενά διαβατήρια. Το τσιπ μπορεί να είναι σε διαφορετικά στάδια της εκκίνησης.
- Η ικανότητα να παράγει υψηλής ποιότητας πλαστά βιβλιάρια διαβατήριο.

- Δυνατότητα για να ανακτήσετε ιδιωτικό Active ταυτότητας ή Chip Authentication κλειδιά από το κύκλωμα του διαβατηρίου με ανάλυση πλευρά καναλιών (π.χ. Διαφορικής Ανάλυσης ρεύματος).
- Εκ των έσω κατά τη διαδικασία έκδοσης.
- Πρόσβαση σε κλειδιά υπογραφής χώρα.
- Εκ των έσω κατά τον έλεγχο των συνόρων.
- Πρόσβαση στα πλήκτρα ελέγχου του συστήματος.
- Η δυνατότητα να εισάγετε πλαστά κλειδιά στα συστήματα ελέγχου.
- Η δυνατότητα να παρέμβει με τη λειτουργία των συστημάτων ελέγχου (π.χ. αλλάζοντας το λογισμικό του συστήματος ελέγχου).

2.8.6 Προφίλ Επιτιθέμενου

Οι διαφορετικοί εισβολείς μπορεί να είναι πρόθυμοι να δεχτούν ένα διαφορετικό επίπεδο κινδύνου. Για παράδειγμα, μια οικονομική πρόσφυγας μπορεί να είναι πρόθυμοι να αποδεχθούν μια πιθανότητα ανίχνευσης 50% (π.χ., προσπαθώντας να περάσει από μια πύλη για το ABC με τη ζωή μεγέθους φωτογραφία πριν από το πρόσωπό του), ενώ μια εγκληματική οργάνωση θα δεχθεί μια πολύ μικρότερη πιθανότητα ανίχνευσης και λύση να εφαρμοστεί προσεκτικά απάτη παρόμοιων (π.χ. να χρησιμοποιούν το επίσημο αλγόριθμο που ταιριάζουν εικόνα για να εντοπίσετε ένα άτομο που ταιριάζουν στη συνέχεια, αγοράζει / να κλέβει e-διαβατήριο του ατόμου). Η υπεράσπιση ενάντια των εισβολών οι οποίοι είναι πρόθυμοι να δεχτούν μεγάλη πιθανότητα ανίχνευσης γίνεται σταδιακά ακριβά. Τα προφίλ των εξής εισβολέων έχουν εντοπιστεί:

Ιδιώτες που σαν στόχο έχουν την διάβαση των συνόρων σημείο ελέγχου χωρίς να έχουν αναγνωριστεί σωστά (π.χ. με μια ψευδή ταυτότητα).

Εσωτερικός παράνομος που σαν στόχος είναι η ενεργή αξιοποίηση εμπιστευτικών πρόσβασης στη διαδικασία έκδοσης για προσωπικό χρηματικό κέρδος (π.χ. από έναν αξιωματικό της αίτησης)

Οργανωμένες εγκληματικές και τρομοκρατικές οργανώσεις που σαν στόχος είναι η διάβαση των συνόρων σημείο ελέγχου χωρίς να έχουν αναγνωριστεί σωστά (π.χ. με μια ψεύτικη ταυτότητα). Αυτό θα μπορούσε να οδηγήσει στην εμπορία ανθρώπων ή εγκληματίες παράνομα πηγαίνουν στο εξωτερικό ή την είσοδο για να ξεφύγουν από την κράτηση.

Οι κυβερνήσεις που σαν στόχος είναι η διάβαση των συνόρων σημείο ελέγχου, που ανήκουν σε μια ξένη χώρα, χωρίς να έχουν αναγνωριστεί σωστά. (π.χ. με μια ψευδή ταυτότητα)

Hacker που σαν στόχος είναι η δημιουργία της δημοσιότητας σχετικά με τα θέματα ασφαλείας που σχετίζονται με e-διαβατήρια.

2.9 ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΚΑΙ ΒΙΟΜΕΤΡΙΚΑ ΔΙΑΒΑΤΗΡΙΑ

Σε μια παγκόσμια κοινωνία όπου το ηλεκτρονικό έγκλημα βρίσκεται σε άνθηση θα μπορέσουμε άραγε ποτέ να νιώσουμε απόλυτη ασφάλεια κλείνοντας τα ευαίσθητα προσωπικά μας δεδομένα σε ένα τσιπάκι το οποίο ενδεχομένως να γινόταν βορά στα αδηφάγα πλήκτρα των δεξιοτεχνών στους ηλεκτρονικούς υπολογιστές; Το σίγουρο είναι ότι το κύμα ψηφιακού εκσυγχρονισμού θα απλοποιήσει κατά πολύ την καθημερινότητά μας, απλοποιώντας τις μετακινήσεις μας σε ξένες χώρες και μεταμορφώνοντας άλλοτε χρονοβόρες διεργασίες σε αστραπιαίες διαδικασίες. Το θέμα είναι να υιοθετηθούν εις βάθος όλα τα απαιτούμενα μέτρα και συστήματα τα οποία πέρα από την ασφάλεια θα εγγυώνται τη σωστή λειτουργία του τεχνολογικά προηγμένου ενσωματωμένου συστήματος. Κατά την άποψη μου τα παρακάτω μέτρα μπορούν να οδηγήσουν προς αυτή την κατεύθυνση:

- *Ενημέρωση – Ειδοποίηση:* οι πολίτες πρέπει να ξέρουν πως και γιατί χρησιμοποιείται η τεχνολογία RFID καθώς επίσης ποίες πληροφορίες συλλέγονται και από ποιους. Θα πρέπει να χρησιμοποιούνται τυποποιημένα εικονίδια τα οποία θα «προδίδουν» την ύπαρξη και την χρήση ετικετών R.F.I.D.
- *Ανοιχτά Πρότυπα: επειδή τα R.FI.D.* συστήματα μπορούν να διαμορφωθούν με ποικίλους τρόπους, είναι πολύ σημαντικό ότι το κοινό έχει πρόσβαση στις πληροφορίες για τα πρότυπα σχεδίου σύμφωνα με τα οποία αυτά κατασκευάζονται. Οι πληροφορίες αυτές δεν πρέπει να περιοριστούν στις προοριζόμενες χρήσεις τους αλλά να διευκρινιστούν και οι μέγιστες δυνατότητες των συστημάτων αυτών. Οι πληροφορίες για τον κατασκευαστή του R.F.I.D. chip, του προμηθευτή συστήματος δεδομένων, κτλ. θα πρέπει να κοινοποιούνται , χωρίς να θίγεται η εθνική ασφάλεια, ώστε να μπορεί το ευρύ κοινό να αξιολογεί τις επιλογές σχεδίου και ολοκλήρωσης.

- *Επιλογή και Έλεγχος (Συγκατάθεση):* Όπου είναι δυνατόν, οι πολίτες πρέπει να έχουν την επιλογή να μην συμμετέχουν σε ένα πρόγραμμα που περιλαμβάνει τη χρήση της τεχνολογίας RFID για να καταγράψουν τις μετακινήσεις τους, διατηρώντας τα δικαιώματα και τα προνόμια (αλλά ίσως χάνοντας τα οφέλη ευκολίας) άλλων ατόμων που συμμετέχουν σε ένα πρόγραμμα που περιλαμβάνει την τεχνολογία R.F.I.D. Εάν η εθνική ασφάλεια στρέφεται ενάντια στο μεμονωμένο έλεγχο, ένα τέτοιο επιχείρημα πρέπει να δηλωθεί ρητά και η επιλογή να παρέχεται στο μέτρο όπου είναι δυνατό. Ίσως κάτω από τέτοιες περιστάσεις, η ειδοποίηση και η ενημέρωση θα ήταν απαραίτητες
- *Ασφάλεια δεδομένων:* Για να αποφευχθούν οι υποκλοπές θα πρέπει να εξασφαλιστεί το γεγονός ότι μόνο οι εξουσιοδοτημένοι αναγνώστες μπορούν να λάβουν τα σήματα από τις εξουσιοδοτημένες ετικέτες R.F.I.D. Τα στοιχεία πρέπει να κρυπτογραφηθούν στις ετικέτες, κατά τη μεταφορά, και στη βάση δεδομένων. Πρέπει να περιοριστούν προσεκτικά τα περιβάλλοντα στα οποία χρησιμοποιούνται οι ταυτότητες, και να σχεδιάζονται τα R.F.I.D. chips έτσι ώστε ποτέ να μην εμφανίζονται όμοια. Όπως με οποιοδήποτε πρόγραμμα βάσης δεδομένων, πρέπει να ληφθούν όλα τα κατάλληλα μέτρα για την ασφάλεια και την ακεραιότητα της βάσης δεδομένων.
- *Αποφυγή παρεκτρέπουσας χρήσης:* Τα στοιχεία που συλλέγονται από την τεχνολογία R.F.I.D. πρέπει να χρησιμοποιούνται μόνο για το δηλωμένο στόχο, καθώς επίσης να διατηρούνται μόνο καθ' όσο είναι απαραίτητο για να επιτευχθεί ο αρχικός στόχος για τον οποίο συλλέχθηκαν.
- *Εκστρατεία εκπαίδευσης:* η τεχνολογία RFID δεν είναι γνώριμη στο μεγαλύτερο μέρος του κοινού. Ο δημόσιος και ο ιδιωτικός τομέας επίσης στερείται της γνώσης για το πώς οι τεχνολογίες RFID λειτουργούν και πότε και πώς εφαρμόζονται καλύτερα. Κατά συνέπεια, υπάρχουν πολλοί άνθρωποι για τους οποίους η χρήση της τεχνολογίας RFID στα συστήματα ταυτότητας είναι δυσνόητη και απρόσιτη. Οι περισσότερες από τις ανησυχίες τους θα μπορούσαν να επιλυθούν εύκολα μέσω της εκπαίδευσης, με μια εκστρατεία εκπαίδευσης σχετικά με τη χρήση RFID, που περιλαμβάνει γιατί είναι απαραίτητη καθώς και πως προστατεύονται τα δικαιώματα τους.

ΚΕΦΑΛΑΙΟ 3

3.1 ΑΠΕΙΛΕΣ

Υπάρχουν πολλές απειλές μπορεί να επηρεάσει το εν λόγω σύστημα. Μερικές από αυτές τις απειλές είναι μεταξύ αναγνώστη και του διαβατηρίου ως skimming, ωτακουστή και η κλωνοποίηση. Επίσης υπάρχουν απειλές μεταξύ αναγνώστη και server που θα επικυρώσει τις πληροφορίες του ο κάτοχος διαβατηρίου. Στο προτεινόμενο πρωτότυπο Chip Authentication και Terminal ταυτότητας εφαρμόζονται για την αποφυγή των απειλών μεταξύ αναγνώστη και e-διαβατήριο, AES και έχει αναπτυχθεί για να υπερασπιστεί τις απειλές συστήματος μεταξύ του διακομιστή και του αναγνώστη.

3.1.1 Κοινές απειλές

Λόγω της ιδιωτικής ζωής της ευαίσθητης φύσης των δεδομένων e-διαβατηρίου και την ασύρματη τεχνολογία που χρησιμοποιείται, το ηλεκτρονικό διαβατήριο υπόκειται σε διάφορες απειλές για την ασφάλεια.

Λαθραία σάρωση: Οι κατευθυντήριες γραμμές του ICAO δεν απαιτούν έλεγχο πρόσβασης ή κρυπτογράφησης της επικοινωνίας RFID. Αυτό καθιστά το e-διαβατηρίου ευάλωτο σε μικρής εμβέλειας σάρωση του τσιπ RFID, το οποίο επιτρέπει την ανεπιθύμητη διαρροή ευαίσθητων πληροφοριών, όπως τα βιομετρικά δεδομένα.

Παράνομη παρακολούθηση: Το πρωτόκολλο RFID εκπέμπει ένα αναγνωριστικό για να αποφευχθεί η σύγκρουση κατά την επικοινωνία. Αν αυτό το αναγνωριστικό είναι μοναδικό, αυτό θα ταχτοποιεί κατιόν και την παρακολούθηση ενός συγκεκριμένου e-διαβατηρίου. Αυτό το αναγνωριστικό αποστέλλεται ακόμη και εάν ο έλεγχος της πρόσβασης έχει αναπτυχθεί.

Skimming και κλωνοποίηση: Όταν τα δεδομένα ενός RFID έχουν διαρρεύσει, αυτό θα μπορούσε να επιτρέψει σε χάκερ να κοινοποιήσουν το τσιπ RFID σε ένα νέο διαβατήριο. Επικυρώνει τα δεδομένα για το ίδιο που δεν είναι αρκετό για να το αποτρέψει αυτό.

Υποκλοπές: Μετά από ένα νόμιμο αναγνώστη διαβατηρίου παρέχεται πρόσβαση στα δεδομένα ηλεκτρονικού διαβατήριου, ευαίσθητα δεδομένα που μπορούν να διαρρεύσουν από υποκλοπές σχετικά με την ανακοίνωση.

3.1.2 Απειλές διακομιστή

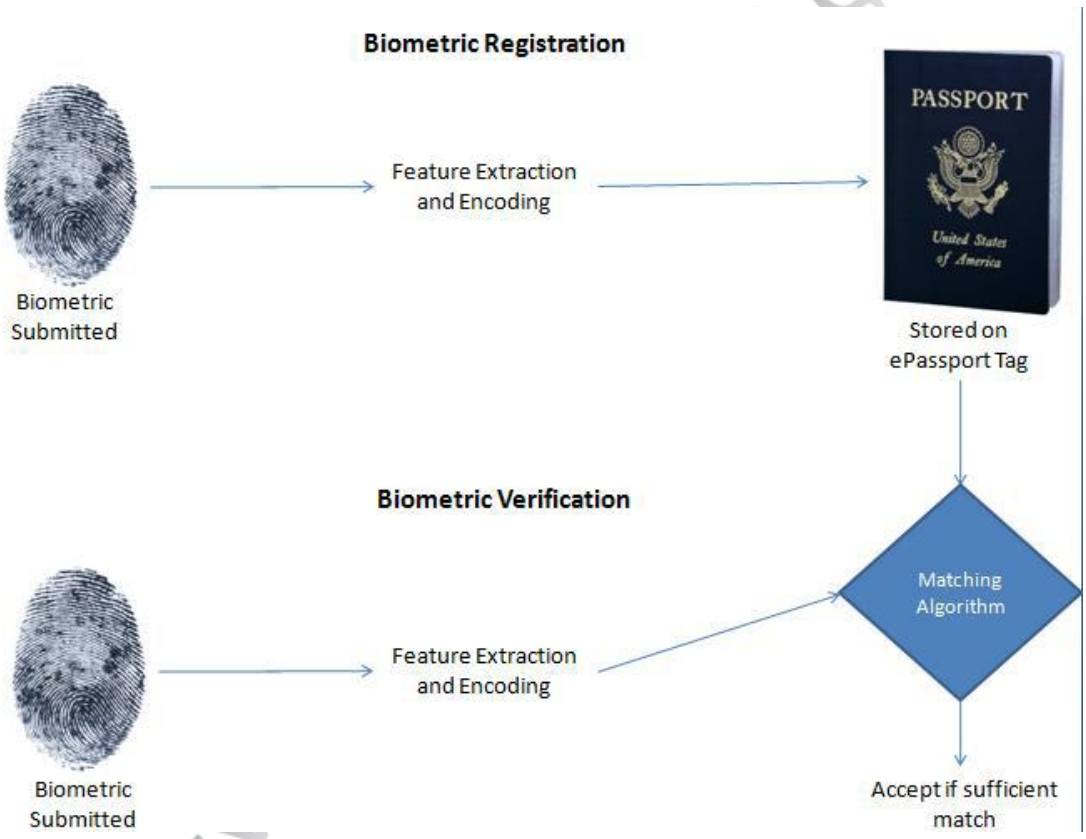
Server ασφάλεια είναι εξίσου σημαντική με την ασφάλεια των δικτύων, επειδή οι διακομιστές θα κατέχουν το μεγαλύτερο μέρος ή το σύνολο των πληροφοριών ταυτοποίησης. Εάν ένας διακομιστής έχει χαραχτεί, όλα τα περιεχόμενά της ενδέχεται να είναι διαθέσιμα για το cracker που έκλεψαν ή χειρίστηκαν κατά βούληση. Το δίκτυο μεταξύ του διακομιστή και του αναγνώστη είναι επίσης σημαντικό για την προστασία της ιδιωτικής ζωής και ασφάλειας των δεδομένων. Έτσι οι απειλές Server πρέπει να καλυφθούν για να αποφύγουν την απώλεια δεδομένων ή hacking του συστήματος.

ΚΕΦΑΛΑΙΟ 4

4.1 Τεχνολογίες ePassport

Τα ηλεκτρονικά διαβατήρια ενσωματώνουν τρεις τεχνολογίες για να συμβάλουν στην αντιμετώπιση των προβλημάτων ταυτότητας χρήστη και διαχείρισης της απάτης: Βιομετρικά στοιχεία, υποδομές δημόσιου κλειδιού (PKI), και το ραδιόφωνο (RFID). Σε αυτή την ενότητα θα δώσουμε μια σύντομη περιγραφή αυτών των τεχνολογιών.

4.1.1 Βιομετρικά στοιχεία



Εικόνα 3: Βιομετρικά στοιχεία

Ένα βιομετρικό στοιχείο είναι ένα φυσιολογικό χαρακτηριστικό ή της συμπεριφοράς που μπορεί να χρησιμοποιηθεί για τον εντοπισμό ή την εξακρίβωση της ταυτότητας ενός ατόμου. Βιομετρική ταυτότητα είναι η διαδικασία αναγνώρισης της γνησιότητας των ατόμων σε υπολογιστές που χρησιμοποιούν βιολογικά ή φυσιολογικά χαρακτηριστικά. Αυτή γίνεται γρήγορα η προτιμώμενη τεχνική για την ταυτοποίηση του χρήστη σε προσωπικές συσκευές, όπως κινητά τηλέφωνα, φορητούς υπολογιστές, κ.λπ. Αυτό μπορεί να αποδοθεί προς την αντίστασή τους στην πλαστογραφία. Συνήθως χρησιμοποιούνται τα βιομετρικά στοιχεία να περιλαμβάνουν πλάνα της

κεφαλής, τα δακτυλικά αποτυπώματα, παλάμη-εκτυπώσης, εικόνες της ίριδας θερμογραφήματα, η γεωμετρία των χεριών, του αμφιβληστροειδούς σαρώσεις, DNA, και φωνή. ηλεκτρονικά διαβατήρια ευνοούν τη χρήση των δακτυλικών αποτυπωμάτων ως το βασικό βιομετρικό. ? Η επιλογή του πιο αποδοτικούς βιομετρικών στοιχείων για μια εφαρμογή βασίζεται σε ορισμένα χαρακτηριστικά, όπως - καθολικότητα, Μοναδικότητα, Μονιμότητα, Performance, είσπραξης, της αποδοχής, και καταστρατήγησης.

Η Βιομετρική διαδικασία ελέγχου ταυτότητας για τα ηλεκτρονικά διαβατήρια περιλαμβάνει δύο διαδικασίες - εγγραφή και τον έλεγχο. Κατά τη φάση της καταχώρισης, ο αιτών ePassport καταγράφει βιομετρικών στοιχείων _ σε ασφαλή χώρο, υπό ανθρώπινη επίβλεψη. Ένα πρόγραμμα εξόρυξης χαρακτηριστικού χρησιμοποιείται για να κωδικοποιήσει αυτά τα βιομετρικών στοιχείων δεδομένων μετά την οποία είναι αποθηκευμένα στους χρήστες ePassport Tag. Για την ταυτοποίηση του χρήστη και επαλήθευσης της ταυτότητας σε ένα τερματικό ελέγχου, ο χρήστης γίνεται να παρέχει ένα δείγμα των βιομετρικών στοιχείων _. Ο ίδιος αλγόριθμος εξαγωγής χαρακτηριστικών χρησιμοποιείται για να κωδικοποιήσει το προσφάτως παρεχόμενο βιομετρικών στοιχείων. Ένας αλγόριθμος που ταιριάζει τρέχει στο τερματικό για να αποκτήσει τον βαθμό ομοιότητας μεταξύ του εγγεγραμμένου και παρέχει βιομετρικών στοιχείων. Εάν ο βαθμός ομοιότητας θεωρείται να είναι μεγαλύτερο από μία ορισμένη τιμή κατωφλίου, το βιομετρικό γίνεται αποδεκτό και η ταυτότητα του χρήστη επαληθευετε με επιτυχία. Δυστυχώς, χωρίς ανθρώπινη εποπτεία, δεν είναι πάντα δυνατό να ανιχνευθεί η χρήση προσθετικών στα βιομετρικά στοιχειά εγγραφής ή επαλήθευση σταδίων. Είναι εύκολο να δούμε ότι οι βιομετρικές επιθέσεις Χωρών θα γίνει πιο εύκολη να εκτελέσει όσο αυξάνεται η αυτοματοποίηση και η ανθρώπινη επίβλεψη των βιομετρικών στοιχείων διαδικασία μειώνεται.

4.1.2 Υποδομή Δημόσιου Κλειδιού (PKI)

Μια Υποδομή Δημοσίου Κλειδιού είναι απαραίτητη για τη διαδικασία του δημόσιου κλειδιού διανομής και ελέγχου ταυτότητας. Η Υποδομή Δημοσίου Κλειδιού για ηλεκτρονικά διαβατήρια παρέμεινε αμετάβλητη κατά τα τελευταία πέντε έτη. Τα βασικά στοιχεία του ePassport PKI είναι η χώρα Επαλήθευση αρχών Πιστοποίησης (CVCA) γνωστός και ως Χώρα Υπογραφή πιστοποιητικού Αρχές (CSCA), έγγραφο ελέγχου (DV), και συστημάτων ελέγχου (IS). Η Υποδομή Δημοσίου Κλειδιού

συνήθως έχει μια ιεραρχική δομή. Το ανώτατο όργανο επίπεδο σε κάθε χώρα λειτουργεί ως CSCA. Η CSCA δημιουργεί και αποθηκεύει ένα κλειδί ζεύγους (KPuCSCA? KPrCSCA). Το ιδιωτικό κλειδί της CSCA (KPrCSCA) χρησιμοποιείται για την υπογραφή κάθε εγγράφου πιστοποιητικό ελέγχου (DV) (από το δικό του και από άλλες χώρες). Υπάρχουν συνήθως πολλές ο επαληθευτής εγγράφου σε κάθε έθνος. Κάθε μία από αυτές ο επαληθευτής εγγράφου δημιουργεί και αποθηκεύει ένα κλειδί ζεύγους (KPuDV, KPrDV). Το ιδιωτικό κλειδί (KPrDV) του DV χρησιμοποιείται για την υπογραφή για κάθε σύστημα επιθεώρησης (Reader) (IS) πιστοποιητικό στον τομέα του και επίσης το στοιχείο δεδομένων ασφαλείας (SOD) του κάθε διαβατήριο που εκδίδει. Για να στείλετε e? Μερίδιο επαρκώς πιστοποιητικά DV από όλα τα έθνη, τα ICAO παρέχει ένα ευρετήριο κοινών κλειδιών (PKD). Η PKü θα αποθηκεύει μόνο τα πιστοποιητικά του συνόλου των εγγεγραμμένων DV _. Αυτός ο χώρος απόθεσης των πιστοποιητικών είναι διαθέσιμη σε κάθε έθνος και δεν διαβάζει προστατευόμενα. _ CRL(μπορεί επίσης να αποθηκευτεί στην ίδια PKD. Κάθε έθνος έχει την ευθύνη για την ενημέρωση χώρου αποθήκευσης του δημόσιου πιστοποιητικού και CRL κατά τη λήψη τους από τα PKD, μόλις γίνει αυτό, κάθε έθνος διανέμει τη νέα λήψη πληροφοριών για κάθε DV και είναι εντός της δικαιοδοσίας του.

4.1.3 Radio Frequency Identification

RFID είναι μια ασύρματη τεχνολογία που χρησιμοποιείται για την επικοινωνία μεταξύ ενός Tag και ένα συστήματος ελέγχου που ονομάζεται Reader. Κατά τη διάρκεια των τελευταίων ετών, η τεχνολογία RFID έχει μια περιοχή μεγάλης διαμάχης μετά την εφαρμογή ορισμένων μεγάλων καταστημάτων διανομής όπως η Benetton CRL(Ιταλία) και το μετρό Μέλλον Κατάστημα CRL(Γερμανία) για λόγους που δεν γνωστοποιήθηκαν. Από τότε έχουν υπάρξει σημαντικές διαμαρτυρίες και ακόμα και μποϊκοτάζ των προϊόντων από τους ακτιβιστές της ιδιωτικής ζωής που φοβούνται ότι αυτές οι ετικέτες RFID που χρησιμοποιούνται για δραστηριότητες όπως η συμπεριφορά των χαρακτηριστικών και των πελατών παρακολούθησης [27]. Μερικές από τις σημαντικότερες απειλές που πρέπει να αντιμετωπιστούν κατά την εφαρμογή της τεχνολογίας RFID σε ευαίσθητα πεδία όπως η διεθνής ασφάλεια είναι σάρωση, παρακολούθηση, Υποκλοπές, και Κλωνοποίηση .ie είναι σημαντικό ότι ένας αντίπαλος δεν είναι σε θέση να κάνει τα εξής:

- Διαβάστε δεδομένα από την ετικέτα χωρίς τη συγκατάθεση του κατόχου του διαβατηρίου.
- Παρακολουθούν τις κινήσεις του κατόχου του διαβατηρίου.
- Λαθρακρόαση νόμιμων αλληλεπιδράσεων.
- Δημιουργήστε μια νέα ετικέτα που μπορεί να συνδεθεί σε ένα διαβατήριο.

RFID αποτελείται από τρία υποσυστήματα: Ετικέτες, αναγνώστες και κεραίες. Ετικέτες RFID μπορεί να είναι ένας από τους τρεις τύπους: ενεργός, ημι-ενερός ή παθητικός. Οι ενεργές ετικέτες είναι εκείνες οι οποίες λειτουργούν με μπαταρία, ενώ παθητικές ετικέτες έχουν μπαταρίες και χρησιμοποιούν την εξουσία που λαμβάνονται από τα ραδιοσήματα από τους αναγνώστες RFID να λειτουργούν. Οι αναγνώστες RFID λειτουργούν σε ένα ευρύ φάσμα συχνοτήτων, τη δύναμη, και κυμαίνεται ανάγνωση? αυτά τα χαρακτηριστικά που ορίζονται από την εφαρμογή. Οι κεραίες συνήθως είναι ενσωματωμένες στο RFID Reader και κάρτα RFID.

4.2 Πρότυπη προδιαγραφή ePassport

Το ePassport έχει ενσωματωμένο σε αυτό μια ετικέτα RFID η οποία είναι ικανή για κρυπτογραφικους υπολογισμών και είναι παθητική στη φύση. Παθητικές ετικέτες RFID επιλέχθηκαν λόγω του χαμηλού τους κόστους, υψηλής πιστότητας, και η σύντομη ανάγνωση απο σειρές. Το σύστημα RFID υλοποιείται σε ηλεκτρονικά διαβατήρια που ακολουθούν το πρότυπο ISO 14443, το οποίο καθορίζει τη χρήση του 13.56MHz ραδιοσυχνοτήτων για την επικοινωνία. Τα φυσικά χαρακτηριστικά του ePassport Ετικέτες που ορίζεται από το πρότυπο ISO 7810 ID-3, η οποία καθορίζει ένα Tag μεγέθους 125 χιλιοστά x 88 χιλιοστά. Αυτές οι ετικέτες RFID έχουν μια κεραία που χτίστηκε γύρω τους. ePassport Ετικέτες έχουν μεταξύ 32-144 kilobyte της μνήμης EEPROM ενσωματωμένο σε αυτά. Σε αυτή τη μνήμη που αποθηκεύουμε 16 ομάδες δεδομένων που κυμαίνονται από DG1 - DG 16. Αυτές οι 16 ομάδες αποθηκεύουν πληροφορίες, όπως δεδομένα που βρίσκονται στην Μηχαναγνώσιμη Ζώνη CRL(MRZ) του διαβατηρίου, εξάγεται βιομετρικά χαρακτηριστικά, τα δημόσια κλειδιά και άλλα στοιχεία δεδομένων. Από ePassport συστήματα RFID λειτουργούν σε 13.56MHz CRL(HF), το σχεδιασμό κεραιών βρόχου ή διπόλου που μπορούν να χρησιμοποιηθούν σε έξυπνες κάρτες και τα ηλεκτρονικά διαβατήρια δεν είναι δυνατόν, αντί να χρησιμοποιούμε τις ιδιότητες της επαγωγικής σύζευξης για μετάδοση σήματος μεταξύ RFID ετικετών και των αναγνωστών. Υπάρχουν πολλές

άλλες προκλήσεις που πρέπει να αντιμετωπιστούν και κατά το σχεδιασμό των συστημάτων RFID χρησιμοποιώντας παθητικές HF ετικέτες.

ΚΕΦΑΛΑΙΟ 5

5.1 ΠΡΩΤΗ ΓΕΝΝΙΑ E-PASSPORT

Το 2004, ο Διεθνής Οργανισμός Πολιτικής Αεροπορίας (ICAO), δημοσίευσε μια σειρά από κατευθυντήριες γραμμές (Doc 9303) που επρόκειτο να ακολουθηθεί ως πρότυπο ePassport ντε φάκτο. Η προεπιλογή για τα υποχρεωτικά βιομετρικά στοιχεία που θα χρησιμοποιηθούν είναι το headshot του ατόμου, και άλλα επιτρεπόμενα για τη χρήση βιομετρικών στοιχείων που είναι τα δακτυλικά αποτυπώματα και εικόνες της ίριδας. Υπάρχουν τρία πρωτόκολλα κρυπτογράφησης που περιγράφονται στην πρώτη γενιά προδιαγραφές ICAO για να εξασφαλιστεί η ορθότητα δεδομένων και της ιδιωτικής ζωής. Αυτές είναι παθητική ταυτότητα, Βασικός έλεγχος πρόσβασης, και Active ταυτότητα.

5.1.1 Παθητική ταυτότητα

Πιστοποίηση Η παθητική είναι το μόνο υποχρεωτικό πρωτόκολλο κρυπτογράφησης στην περιγραφή της πρώτης γενιάς ICAO. Πρωταρχικός στόχος της είναι να επιτρέψει τον αναγνώστη να βεβαιωθείτε ότι τα δεδομένα στο ηλεκτρονικό διαβατήριο είναι αυθεντικά. Το σύστημα αυτό είναι γνωστό ως παθητική ταυτότητα, δεδομένου ότι η ετικέτα δεν εκτελεί καμία επεξεργασία και μόνο συμμετέχουν παθητικά στο πρωτόκολλο. Πρέπει να σημειωθεί ότι η παθητική ταυτότητα δεν δεσμεύει το tag σε ένα δηλαδή διαβατήριο μπορούμε απλώς να αποδείξει ότι τα στοιχεία που αναγράφονται στην ετικέτα είναι σωστά, δεν είναι το αυθεντικότητα της ίδιας της ετικέτας CRL(δεν μπορεί να ανιχνεύσει την κλωνοποίηση) Το Σύστημα Ελέγχου retreives του πιστοποιητικού του ελεγκτή εγγράφου έκδοσης, χρησιμοποιούν το δημόσιο κλειδί από το πιστοποιητικό αυτό ελεγκτής της ψηφιακής υπογραφής που χρησιμοποιείται για την υπογραφή των δεδομένων στο LDS. Μόλις καθοριστεί η εγκυρότητα της υπογραφής, ο αναγνώστης υπολογίζει το hash του καθενός από αυτά τα στοιχεία δεδομένων και τα συγκρίνει με τις κωδικοποιημένες τιμές που αποθηκεύονται στο SOD.

5.1.2 Ενεργή Πιστοποίηση

Η Ενεργή Πιστοποίηση είναι ένα προαιρετικό πρωτόκολλο στις ICAO προδιαγραφές πρώτης γενιάς. Χρησιμοποιώντας ένα απλό μηχανισμό πρόκλησης-απόκρισης, στοχεύει να εντοπίσει αν η ετικέτα θα αντικατασταθεί ή κλωνοποιηθεί. Αν η Ενεργή

Πιστοποίηση υποστηρίζεται, η ετικέτα για το ηλεκτρονικό διαβατήριο αποθηκεύει ένα δημόσιο κλειδί CRL(KPuAA) στην ομάδα δεδομένων 15 και κατακερματισμού της εκπροσώπησης στο SOD. Το αντίστοιχο ιδιωτικό κλειδί CRL(KPrAA) είναι αποθηκευμένο στο ασφαλές τμήμα της μνήμης του Tag. Προκειμένου για την ετικέτα, για να διαπιστωθεί η γνησιότητά του, οφείλει να αποδείξει στον αναγνώστη ότι το ΔΙΑΤΗΡΕΙ αυτό το ιδιωτικό κλειδί.

1. Ο αναγνώστης στέλνει μια τυχαία 64 σειρά δυαδικών ψηφίων CRL(R) στην ετικέτα.
2. Τα σημάδια Tag σε αυτήν τη συμβολοσειρά χρησιμοποιούν το πλήκτρο KPrAA και στέλνει αυτή την υπογραφή προς τον αναγνώστη.
3. Ο αναγνώστης αποκτά το δημόσιο κλειδί KPuAA που αποθηκεύεται στην ομάδα δεδομένων 15.
4. Ο αναγνώστης επαληθευτών της ορθότητας του υπογεγραμμένου string χρησιμοποιεί τις γνώσεις του R και KPuAA.

5.1.3 Βασικός έλεγχος πρόσβασης

Βασικός έλεγχος πρόσβασης CRL(BAC) είναι ένα προαιρετικό πρωτόκολλο που προσπαθεί να εξασφαλίσει ότι οι αναγνώστες μόνο με φυσική πρόσβαση στο διαβατήριο μπορούν να διαβάσουν δεδομένα των πινακίδων. Όταν ένας αναγνώστης προσπαθεί να ανιχνεύσει την BAC ενεργοποιημένη του ePassport, εμπλέκεται σε ένα πρωτόκολλο το οποίο απαιτεί από τον αναγνώστη να αποδείξει τις γνώσεις του σε ένα ζεύγος μυστικών κλειδιών CRL(ονομάζονται `πλήκτρα πρόσβασης») που προκύπτουν από τα στοιχεία του μηχανήματος αναγνώσιμης ζώνης CRL(MRZ) του διαβατήριου. Από αυτά τα κλειδιά, ένα κλειδί συνόδου που χρησιμοποιείται για την ασφαλή ανταλλαγή μηνυμάτων επιτυγχάνεται. Τα πλήκτρα πρόσβασης CRL(KENC? KMAC) προέρχονται από διαθέσιμα στο MRZ ακόλουθα δεδομένα: Ο αριθμός διαβατηρίου CRL(έγγραφο αριθ), ημερομηνία γέννησης του κατόχου του διαβατηρίου CRL(DOB), ισχύει μέχρι την ημερομηνία του διαβατηρίου CRL(DOE), 3 Έλεγχος ψηφία (C).

K_{seed} = 128msb(SHA - 1(DocNo||DOB||DOE||C))

K_{ENC} = 128msb(SHA - 1(K_{seed}||1))

K_{MAC} = 128msb(SHA -ν1(K_{seed}||2))

Ο αναγνώστης θα μπει τώρα σε ένα μηχανισμό πρόκλησης-απάντησης CRL(που περιγράφεται παρακάτω) για να αποδείξουν την κατοχή κλειδιών πρόσβασης και να αποκομίσουν ένα κλειδί συνόδου.

1. Η ετικέτα δημιουργεί και στέλνει στο αναγνώστη μια σειρά 64 bit CRL(R_T).

2. Ο αναγνώστης δέχεται R_T και δημιουργεί δύο τυχαίες 64 ακολουθίες δυαδικών ψηφίων CRL(R_R, K_R).

3. Ο αναγνώστης κρυπτογραφεί τώρα $R_R||R_T||K_R$ χρησιμοποιώντας τον αλγόριθμο 3-DES και το κλειδί K_{ENC}.

4. Ο αναγνώστης υπολογίζει τώρα στο MAC τη κρυπτογράφηση που χρησιμοποιούν ANSI MAC με στο κλειδί K_{MAC}.

5. Ο αναγνώστης στέλνει το κρυπτογράφημα και στο MAC στην ετικέτα.

6. Η ετικέτα ελέγχει στο MAC, αποκρυπτογραφεί το κρυπτογράφημα. Είναι επαληθευτές της ορθότητας των τελών ταξινόμησης και, στη συνέχεια, εξάγει K_R.

7. Η ετικέτα δημιουργεί μια άλλη 64 bit τυχαία σειρά K_T.

8. Η ετικέτα κρυπτογραφεί τώρα $R_T||R_R||K_T$ χρησιμοποιώντας τον αλγόριθμο 3-DES και K_{ENC}.

9. Η ετικέτα υπολογίζει τώρα στο MAC τη κρυπτογράφηση που χρησιμοποιούν ANSI MAC με στο κλειδί K_{MAC}.

10. Η ετικέτα στέλνει το κρυπτογράφημα και στο MAC προς τον αναγνώστη.

11. Ο αναγνώστης ελέγχει την MAC, αποκρυπτογραφεί το κρυπτογράφημα. Είναι επαληθευτής της ορθότητας R_R και, στη συνέχεια, εξάγει το K_T.

12. Τόσο η αναγνώστη και η ετικέτα υπολογίζουν το κλειδί περιόδου σποράς (K_{seed}) ως $K_T K_R$

Τώρα και τα δύο μέρη δημιουργούν ένα νέο κλειδί κρυπτογράφησης περιόδου K_E και μια συνεδρία MAC κλειδί K_M, όπως φαίνεται παρακάτω.

$K_E = 128msb(SHA - 1(K_{seed}||1))$

$K_M = 128msb(SHA - 1(K_{seed}||2))$

Από αυτό το σημείο και κάθε επικοινωνία εξασφαλίζεται με τη χρήση της παραπάνω κρυπτογράφησης και τα κλειδιά της MAC.

5.2 Δεύτερης γενιάς ηλεκτρονικά διαβατήρια

Το 2006 ένα νέο σύνολο προτύπων για τα ηλεκτρονικά διαβατήρια που ονομάζονται εκτενής έλεγχος πρόσβασης εγκρίθηκε από τις Τεχνολογίες Νέα Ομάδα Εργασίας (NTWG), το οποίο βασίστηκε στην πρόταση για ηλεκτρονικό διαβατήριο τυποποίηση από την Ευρωπαϊκή Ένωση. Ο πρωταρχικός στόχος των EAC ήταν η πληρέστερη Tag Reader και ταυτότητας πρωτόκολλα. Αποσκοπούσε επίσης να προωθήσει την εφαρμογή των δευτερογενών βιομετρικών στοιχείων για πρόσθετη ασφάλεια. Σε αυτή την ενότητα θα περιγράψουμε το τσιπ ταυτότητας και Terminal ταυτότητας πρωτόκολλα και μερικά από τα AWS που δεν μετριάζεται από την ίδρυσή της. Για την επίτευξη αμοιβαίας επαλήθευσης ταυτότητας, η EAC πρόταση εισήγαγε δύο νέα πρωτόκολλα που ονομάζονται Chip Authentication και Terminal ταυτότητας. Αυτά χρησιμοποιούνται για να συμπληρώσουν το πρωτόκολλο Παθητικής ταυτότητας, το πρωτόκολλο βασικού έλεγχου πρόσβασης και, ενδεχομένως, το Active πρωτόκολλο ελέγχου ταυτότητας που περιγράφεται στην προδιαγραφή ePassport πρώτης γενιάς του ICAO.

5.2.1 Τσιπ ελέγχου ταυτότητας

Το πρωτόκολλο τσιπ έλεγχο ταυτότητας είναι υποχρεωτικό πρωτόκολλο στις προδιαγραφές EAC. Έχει ως στόχο να αντικαταστήσει Active έλεγχο ταυτότητας ως μηχανισμό για την ανίχνευση κλωνοποιημένων ηλεκτρονικών διαβατήριων. Αν το τσιπ έλεγχο ταυτότητας εκτελείται με επιτυχία θεσπίζει ένα νέο ζευγάρι των κλειδιών κρυπτογράφησης και MAC για την αντικατάσταση BAC που προέρχονται κλειδιά συνόδου και την ασφαλή ανταλλαγή μηνυμάτων. Αυτό επιτυγχάνεται με τη χρήση του στατικού Diffie-Hellman πρωτοκόλλου συμφωνίας κλειδιού. Σημειώστε ότι το ηλεκτρονικό διαβατήριο Tag έχει ήδη ένα δημόσιο κλειδί τσιπ έλεγχο ταυτότητας και ιδιωτικό κλειδί. Η διαδικασία των τσιπ έλεγχο ταυτότητας περιγράφεται παρακάτω.

1. Η ετικέτα στέλνει TKPuCA προς τον αναγνώστη μαζί με τους Diffie-Hellman κλειδί παραμέτρων της σύμβασης (D).
2. Ο αναγνώστης επαληθεύει την ορθότητα του κλειδιού που λαμβάνεται με τη χρήση Παθητικής έλεγχο ταυτότητας.
3. Ο αναγνώστης χρησιμοποιεί τα δεδομένα στο D για να δημιουργήσει το δικό του ζεύγος δημόσιου και ιδιωτικού κλειδιού (RKPuCA, RKPrCA).

4. Ο αναγνώστης στέλνει το δημόσιο κλειδί που παράγεται RKPuCA στην ετικέτα.
5. Η Reader και Tag μπορεί τώρα να δημιουργήσει ένα νέο κλειδί σπόρων (Kseed) χρησιμοποιώντας αυτό το κοινόχρηστο πληροφορίες.
6. Το νέο κρυπτογράφησης και τα κλειδιά της MAC

5.2.2 Τερματικό ελέγχου ταυτότητας

Το πρωτόκολλο τερματικού ελέγχου ταυτότητας είναι ένα πρωτόκολλο που εκτελείται μόνο εάν απαιτείται πρόσβαση στα πιο ευαίσθητα δεδομένα (δευτερογενών βιομετρικών στοιχείων). Πρόκειται για έναν μηχανισμό απόκρισης πρόκλησης που επιτρέπει την ετικέτα για να επικυρώσετε τη συσκευή ανάγνωσης που χρησιμοποιείται στο τσιπ ελέγχου ταυτότητας. Ο αναγνώστης αποδεικνύει στην ετικέτα με τη χρήση ψηφιακής πιστοποίησης, ότι έχει εγκριθεί από το σπίτι και να επισκεφθείτε το έθνος να διαβάσετε ePassport Ετικέτες. Η διαδικασία του Terminal ελέγχου ταυτότητας περιγράφεται παρακάτω.

1. Ο αναγνώστης στέλνει το Tag ένα πιστοποιητικό ελέγχου του συστήματος (το οποίο ελήφθη από την τοπική DV) και το πιστοποιητικό του DV (που ελήφθη από την CVCA).
2. Η ετικέτα επιθεωρεί τα πιστοποιητικά και εξάγει το δημόσιο κλειδί ($RKPu_{TA}$) του αναγνώστη από το πιστοποιητικό ελέγχου του συστήματος.
3. Η ετικέτα δημιουργεί μια τυχαία χορδή (R) και το στέλνει στον αναγνώστη.
4. Ο αναγνώστης υπολογίζει το hash του RKPuCA που προέρχονται από το πρωτόκολλο τσιπ ελέγχου ταυτότητας.
5. Ο αναγνώστης υπογράφει το μήνυμα (R||SHA-1 (RKPuCA)) με το ιδιωτικό κλειδί του (RKPrTA).
6. Η ετικέτα επαληθευτών την ορθότητα των R και RKPuCA χρησιμοποιώντας το πλήκτρο RKPuTA και παρέχει πρόσβαση σε δευτερεύουσα βιομετρικά στοιχεία αναλόγως.

5.3 Τρίτη γενιά ηλεκτρονικά διαβατήρια

Στα τέλη του 2008, η Ομοσπονδιακή Υπηρεσία Ασφάλειας Πληροφοριών (BSI - Γερμανία) κυκλοφόρησε ένα έγγραφο το οποίο περιγράφει νέους μηχανισμούς ασφαλείας για ηλεκτρονικά διαβατήρια. Σε αυτή την ενότητα θα περιγράψουμε αυτά

τα πρωτόκολλα ηλεκτρονικών διαβατήριών τρίτης γενιάς. Ενώ αυτή η συγγραφή κατιόν είναι κατάλληλο για ESIGN, ηλεκτρονικών ταυτοτήτων και ePassport εφαρμογές, θα την περιγράψουμε μόνο για relevence του σε ηλεκτρονικών διαβατήριών. Η προδιαγραφή τρίτης γενιάς εισάγει ένα νέο πρωτόκολλο που ονομάζεται PACE. Εκτός από την PACE, τα πρωτόκολλα τερματικού ελέγχου ταυτότητας και τσιπ ελέγχου ταυτότητας επίσης ενημερώθηκαν. Ο ρυθμός (Κωδικός Authenticated Connenction Ίδρυση) πρωτοκόλλου εισάγεται ως αντικατάσταση του μηχανισμού βασικού έλεγχου πρόσβασης.

5.3.1 Κωδικός σύνδεσης με έλεγχο ταυτότητας Ίδρυσης (PACE)

Το PACE αντικαθιστά το πρωτόκολλο βασικού έλεγχου πρόσβασης, ως μηχανισμός που επιτρέπει σε μια ετικέτα για να βεβαιωθείτε ότι ο αναγνώστης έχει εξουσιοδοτημένη πρόσβαση στο ηλεκτρονικό διαβατήριο. Η ετικέτα και τον Reader μοιράζονται ένα κοινό κωδικό (π) το οποίο χρησιμοποιείται σε συνδυασμό με τον Diffie-Hellman πρωτόκολλο συμφωνίας κλειδιού για να παρέχει ένα ισχυρό κλειδί συνόδου. Η όλη διαδικασία περιγράφεται παρακάτω.

1. Η ετικέτα κρυπτογραφεί ένα τυχαίο nonce (s) χρησιμοποιώντας το κλειδί K_π .Εδώ, K_π είναι SHA-1 (π||3).
2. Η ετικέτα στέλνει το κρυπτογραφημένο nonce και στο Diffie Hellman το κλειδί συμφωνίας παραμέτρων του στατικού πεδίου (D) προς τον αναγνώστη.
3. Ο αναγνώστης χρησιμοποιεί το κοινό κωδικό (π) για να ανακτήσει την κρυπτογραφημένη nonce (s).
4. Η ετικέτα και ο Αναγνώστης υπολογίζει το Diffie-Hellman εφήμερο τις βασικές παραμέτρους τομέα (D ') με το πλήκτρο D και s.
5. Η ετικέτα δημιουργεί ένα ζεύγος κλειδιών δίνεται από την ($PACEKPr_T$, $PACEKPu_T$) και στέλνει $PACEKPu_T$.
6. Το Reader δημιουργεί το ζεύγος κλειδιών ($PACEKPr_R$, $PACEKPu_R$) και στέλνει $PACEKPu_R$.
7. Η Reader και Tag έχουν πλέον αρκετές κοινές πληροφορίες για να δημιουργήσει ένα κλειδί σπόρων (K_{seed}).
8. Η Reader και Tag τώρα αντλούν συνεδρία κλειδιών K_{ENC} και K_{MAC}
9. Ο αναγνώστης υπολογίζει ένα διακριτικό ταυτότητας:
   T_R = MAC (K_M, ($PACEKPu_T$, D ')) και το στέλνει στον Tag για επαλήθευση.

10. Η ετικέτα υπολογίζει ένα διακριτικό ταυτότητας:

T_T = MAC (K_M, (PACEKPu$_R$, D ')) και το στέλνει στον αναγνώστη για επαλήθευση.

Τύποι των κωδικών πρόσβασης Ο καθορισμός της προδιαγραφής επιτρέπει δύο τύπους κωδικών πρόσβασης για χρήση με ηλεκτρονικά διαβατήρια. Αυτά είναι CAN και MRZ κωδικούς πρόσβασης. Ο αριθμός πρόσβασης της κάρτας (CAN) μπορεί να είναι ένας μικρός στατικός ή δυναμικός κωδικό πρόσβασης. Εάν η CAN είναι στατική, αυτό απλώς αναγράφεται στο διαβατήριο. Αν είναι δυναμική, η ετικέτα που επιλέγει τυχαία και την εμφανίζει στο διαβατήριο χρήση τεχνολογιών χαμηλής επίδειξη δύναμης, όπως OLED ή ePaper. Ο κωδικός πρόσβασης MRZ είναι ένα συμμετρικό κλειδί στατικού τύπου που προέρχεται από τον MRZ του ηλεκτρονικού διαβατηρίου.

5.3.2 Τερματικό ελέγχου ταυτότητας έκδοση 2

Στις νέες προδιαγραφές, τερματικού ελέγχου ταυτότητας πρέπει να εκτελούνται Πριν από τον τσιπ ελέγχου ταυτότητας. Ο σκοπός του πρωτοκόλλου τερματικού ελέγχου ταυτότητας είναι να επιτρέψει στην ετικέτα για να επικυρώσετε στον αναγνώστη, πριν επιτρέψει την πρόσβαση σε πολύ ευαίσθητες βιομετρικές πληροφορίες. Υπάρχουν αρκετές τροποποιήσεις στο πρωτόκολλο τερματικού ελέγχου ταυτότητας η οποία περιγράφεται παρακάτω.

1. Ο αναγνώστης στέλνει την ετικέτα μιας αλυσίδας πιστοποιητικών που αρχίζει με την βεβαίωση της τοπικής DV και τελειώνει με τον πιστοποιητικό έλεγχο του συστήματος.
2. Η ετικέτα επαληθεύει την αυθεντικότητα των εν λόγω πιστοποιητικών μέσω δημόσιο το κλειδί CVCA.
3. Η ετικέτα εξάγει πλέον το δημόσιο κλειδί αναγνωστών (RPuK).
4. Ο αναγνώστης παράγει ένα ζεύγος εφήμερου κλειδιού Diffie-Hellman: ($RPrK_{TA}$, $RPuK_{TA}$) χρησιμοποιώντας τις παραμέτρους τομέα (D).
5. Ο αναγνώστης στέλνει το δακτυλικό αποτύπωμα του δημόσιου κλειδιού (Comp ($RPuK_{TA}$)) και ορισμένα βοηθητικά στοιχεία (ATA) στην ετικέτα.
6. Η ετικέτα στέλνει μια τυχαία πρόκληση (R) προς τον αναγνώστη.
7. Ο αναγνώστης χρησιμοποιώντας το ιδιωτικό κλειδί RPrK υπογράφει το string (ID_{TA}||R||Comp ($RPuK_{TA}$) ||A_{TA}) και το στέλνει στην ετικέτα.

8. Η ετικέτα επαληθεύει την ορθότητα της υπογραφής και το string χρησιμοποιώντας το δημόσιο κλειδί (RPuK) και άλλων γνωστών παραμέτρων.

5.3.3 Τσιπ ελέγχου ταυτότητας Έκδοση 2

Το πρωτόκολλο Τσιπ ελέγχου ταυτότητας στη νέα προδιαγραφή εκτελείται μόνο μετά την εκτέλεση του πρωτοκόλλου τερματικού ελέγχου ταυτότητας. Αυτή είναι μια αναγκαιότητα, δεδομένου ότι το πρωτόκολλο Τσιπ απαιτεί το εφήμερο ζεύγος κλειδιών Diffie-Hellman ($RPrK_{TA}$, $RPuK_{TA}$), η οποία δημιουργήθηκε κατά τη φάση τερματικού. Το πρωτόκολλο Τσιπ περιγράφεται παρακάτω.

1. Η ετικέτα στέλνει στον Αναγνώστη το δημόσιο κλειδί του (TPu_K).
2. Ο αναγνώστης στέλνει το εφήμερο κλειδί $RPuK_{TA}$ που έχει δημοσιοποιηθεί και έχει παραχθεί κατά τη διάρκεια ελέγχου ταυτότητας τερματικού στην ετικέτα.
3. Η ετικέτα υπολογίζει το αποτύπωμα των αναγνωστών δημόσιου κλειδιού, όπως: Comp ($RPuK_{TA}$) χρησιμοποιώντας το δημόσιο κλειδί που μόλις έλαβε και στα βοηθητικά δεδομένα (A_{TA}). Συγκρίνει αυτό το αναγνωριστικό με εκείνο που ελήφθη στο τελικό στάδιο ελέγχου ταυτότητας.
4. Το Tag Αναγνώστης και έχουν αρκετές κοινές πληροφορίες για να απορρέουν ένα κλειδί σπόρων (K_{seed}).
5. Η ετικέτα δημιουργεί μια τυχαία nonce (R). Τα κλειδιά συνόδου υπολογίζονται ως K_{MAC} = SHA-1 ($K_{seed}||R||2$) και K_{Enc} = SHA-1 ($K_{seed}||R||1$).
6. Η ετικέτα υπολογίζει τώρα το διακριτικό ταυτότητας: T_T = MAC (K_{MAC} ($RPuK_{TA}$, D)). Η ετικέτα στέλνει R και T_T προς τον αναγνώστη.
7. Ο αναγνώστης χρησιμοποιεί R για να αντλήσει τα κλειδιά συνόδου από K_{seed}. Στη συνέχεια, επαληθεύει στον T_T ταυτότητας κουπόνι.

5.4 Ατέλειες στην Προδιαγραφή πρώτης γενιάς

BAC και Ενεργός έλεγχος ταυτότητας δεν είναι υποχρεωτικό. Τα καθεστώτα BAC και Active έλεγχος ταυτότητας είναι προαιρετικές σε αυτές τις προδιαγραφές. Εάν αυτά τα πρωτόκολλα δεν εφαρμόζονται σε συνδυασμό με την τεχνολογία RFID, οι κάτοχοι ePassport καθίσταται περισσότερο ευάλωτα στους αντιπάλους (από το κανονικό τους κατόχους διαβατηρίου). Αυτό επειδή είναι εύκολο να ξαφρίσει δεδομένα από την ετικέτα χωρίς τη γνώση των κατόχων αν BAC είναι άτομα με ειδικές ανάγκες και τα

νέα διαβατήρια να μπορούν να κατασκευαστούν χρησιμοποιώντας αυτά τα δεδομένα, εάν ο Active έλεγχος ταυτότητας είναι απενεργοποιημένος. Στα κανονικά διαβατήρια, δεν υπάρχει Tag που μπορεί να είναι αποκορυφωμένο από απόσταση και ως εκ τούτου την κλωνοποίηση του διαβατηρίου απαιτεί φυσική πρόσβαση στο ίδιο το έγγραφο.

Αδυναμία των BAC Κλειδιών Πρόσβασης Η BAC είναι το μόνο πρωτόκολλο που αποσκοπούν στην προστασία των κατόχων ePassport από αποκορύφωση και υποκλοπές επιθέσεις. Δυστυχώς, η ασφάλεια ολόκληρου του πρωτοκόλλου του βασίζεται στην εντροπία των δύο κλειδιών πρόσβασης που προέρχονται από στοιχεία δεδομένων σχετικά με την MRZ των ePassport. Ενώ η εντροπία αυτών των πλήκτρων πρόσβασης είναι 56 bits στο μέγιστο, τα περισσότερα από αυτά bits είναι εύκολα guessable. Για παράδειγμα, η εντροπία Ημερομηνίας Γέννησης τομέα μπορεί να μειωθεί σε μεγάλο βαθμό για τους διπλωμάτες και αξιωματούχους (από την ημερομηνία γέννησής τους είναι στη διάθεση του κοινού). Πολλές επιθέσεις σε ολλανδικά και γερμανικά πλήκτρα πρόσβασης ePassport έχουν δείξει ότι η εντροπία των πλήκτρων πρόσβασης BAC μπορεί να μειωθεί σε 25-35 κομμάτια. Είναι προφανές ότι αυτό δεν παρέχει καμία πραγματική ασφάλεια. Μόλις ο αντίπαλος παίρνει αυτά τα πλήκτρα, θα είναι σε θέση να διαβάσει και να παρακολουθήσει την ετικέτα καθ 'όλη τη διάρκεια ζωής του ePassport.

Η έλλειψη πρόσβασης Κανόνων Οι προδιαγραφές ePassport πρώτης γενιάς του ICAO δεν έχει ειδικούς κανόνες πρόσβασης για τα δευτεροβάθμια βιομετρικά στοιχεία, όπως δακτυλικά αποτυπώματα και την εικόνα της ίριδας που θεωρούνται πιο ευαίσθητα από άλλες προσβάσιμες πληροφορίες. Αυτή η έλλειψη κανόνων πρόσβασης καθιστά δυνατή για τα μέρη να αποκτήσουν πρόσβαση σε πληροφορίες που είναι πολύ ιδιωτικες και είναι σαφές ότι δεν χρειάζονται. Για παράδειγμα, είναι εύκολο για το ξενοδοχείο ρεσεψιονίστ, γραφεία ενοικίασης αυτοκινήτων, και άλλοι οργανισμοί όπου τα διαβατήρια που χρησιμοποιούνται συχνά για την αναγνώριση, να έχουν πρόσβαση και να αποθηκεύουν τις ευαίσθητες πληροφορίες που δεν θα πρέπει να έχουν.

5.5 Λάθη στις δεύτερης γενιάς προδιαγραφών

Η εξάρτηση από τις προδιαγραφές BAC Η EAC εξακολουθούν να εξαρτώνται από το πρωτόκολλο βασικού έλεγχου πρόσβασης για την προστασία των βιογραφικών στοιχείων και headshot του κατόχου ePassport. Το πρωτόκολλο BAC βασίζεται σε πληροφορίες διαθέσιμες για MRZ του διαβατηρίου και έχει την εντροπία μέχρι 56 bits.

Ευάλωτη σε επιθέσεις από τη στιγμή που Ισχύει τους αναγνώστες ePassport Tags είναι παθητική στη φύση και ως εκ τούτου δεν έχουν ρολόγια, αυτό σημαίνει ότι κάνουν εκτιμήσεις για την τρέχουσα ημερομηνία βασίζεται μόνο στις πληροφορίες που έλαβε από τους αναγνώστες την τελευταία φορά που είχαν ενεργοποιηθεί. Αυτό σημαίνει ότι είναι δυνατό για τους αναγνώστες με λήξη πιστοποιήσεων για να διαβάσετε τα περιεχόμενα ενός ePassport Tag αν η ημερομηνία του ePassport Tag δεν είχε ενημερωθεί για μεγάλο χρονικό διάστημα

Η ευπάθεια σε επιθέσεις άρνησης υπηρεσίας, αφού το πρωτόκολλο τερματικού ελέγχου ταυτότητας εκτελείται μόνο μετά το πρωτόκολλο Τσιπ ελέγχου ταυτότητας στη διαδικασία EAC λειτουργίας, είναι δυνατόν για ένα κακόβουλο Reader για να κατακλύσουν την ετικέτα με μη έγκυρα πιστοποιητικά. Δεδομένου ότι η ετικέτα έχει πολύ περιορισμένη μνήμη, αυτό θα προκαλέσει την ετικέτα για να σταματήσει να λειτουργεί, όπως απαιτείται

5.6 Οι ελλιπής προδιαγραφές τρίτης γενιάς

Η προδιαγραφή ePassport τρίτης γενιάς φαίνεται να έχουν μετριαστεί όλα, αλλά ένα από τα προβλήματα που υπήρχαν στις προηγούμενες γενιές.

Ευάλωτη σε επιθέσεις από τη στιγμή που Ισχύει τους αναγνώστες ePassport Tags είναι παθητική στη φύση και ως εκ τούτου δεν έχουν ρολόγια, αυτό σημαίνει ότι κάνουν εκτιμήσεις για την τρέχουσα ημερομηνία βασίζεται μόνο στις πληροφορίες που έλαβε από τους αναγνώστες _ τελευταία φορά που ήταν ενεργή. Αυτό σημαίνει ότι είναι δυνατό για τους αναγνώστες με λήξη πιστο ποιητικών για να διαβάσετε τα περιεχόμενα ενός ePassport Tag εάν η ημερομηνία για το ηλεκτρονικό διαβατήριο AG δεν είχε ενημερωθεί για μεγάλο χρονικό διάστημα.

ΣΥΜΠΕΡΑΣΜΑ

Η παθητική ταυτότητα εξασφάλισης της γνησιότητας των δεδομένων που αποθηκεύονται σε ηλεκτρονικά διαβατήρια είναι ένα σαφές όφελος για την ασφάλεια από ηλεκτρονικού μέρους διαβατηρίου. Αλλά μπορεί να είναι αποτελεσματική μόνο αν η χώρα υπογράφει πιστοποιητικά CA και είναι διαθέσιμα σε όλα τα συστήματα ελέγχου.

Ενώ η BAC μπορεί να αποτρέψει τα βασικά skimming, χαμηλής εντροπίας του κλειδιού ταυτότητας αποτελεί σημαντική αδυναμία της. Οι προσπάθειες για να συμπεριλάβει το προαιρετικό πεδίο δεδομένων από τη μηχανικώς αναγνώσιμη ζώνη στο βασικό υπολογισμό απορρίφθηκαν από την ICAO, ώστε να μην σπάσει η διαλειτουργικότητα με τα υπάρχοντα συστήματα. Ο μόνος τρόπος για να βελτιωθεί η αντοχή του BAC είναι η χρήση τυχαίων αριθμών αλφαριθμητικών εγγράφων. Ορισμένες χώρες έχουν ήδη αλλάξει την πολιτική αριθμοδότησης τους, προκειμένου να κάνουν τις επιθέσεις εναντίον BAC δυσκολότερη. Αν ανησυχείτε ότι ένας εισβολέας θα μπορούσε να επικοινωνήσει με το διαβατήριό χωρίς τις γνώσεις σας και είτε να προσπαθήσει να σπάσει το BAC ή τουλάχιστον υποθέτω κάποιες πληροφορίες σχετικά με το τσιπ, μόλις αποθηκεύσετε το διαβατήριό σας σε ένα κάλυμμα προστασίας το οποίο είναι ευρέως διαθέσιμο.

Ενεργός κλωνοποίηση διαβατηρίων ταυτότητας πρόληψης υλοποιείται από ένα εκπληκτικά μικρό αριθμό χωρών. Η κλωνοποίηση μπορεί επίσης να προληφθεί με ταυτότητα τσιπ, το οποίο αποτελεί μέρος της EAC και θα υλοποιηθούν στη δεύτερη γενιά διαβατηρίων της EU. EAC είναι επίσης σε θέση να προστατεύσει τα δακτυλικά αποτυπώματα και εικόνες της ίριδας που είναι αποθηκευμένα σε DG3 / 4 από μη εξουσιοδοτημένη ανάγνωση. Το κλειδί για τη διαχείριση πίσω από αυτό είναι, ωστόσο, δεν είναι ασήμαντο - κυρίως από την οργανωτική άποψη. Και παρόλο που το DV και IS πιστοποιητικά θα έχουν μικρή ισχύ για να περιορίσουν τη χρήση των κλεμμένων συστημάτων ελέγχου, αυτό θα είναι αποτελεσματικό μόνο για τα διαβατήρια των συχνών ταξιδιωτών

Η πρώτη προδιαγραφή γενιάς ePassport αν και ακόμα η χρήση σε πολλές χώρες έχει πάρα πολλούς κινδύνους για την ασφάλεια και την εφαρμογή του δεν συνιστάται. Τα εκτεταμένα πρωτόκολλα ελέγχου πρόσβασης εισάγουν την έννοια της αμοιβαίας επαλήθευσης ταυτότητας μεταξύ της ετικέτας και του αναγνώστη και αυτό βοηθά στη

μείωση του κινδύνου από επιθέσεις skimming. Ωστόσο, μια αιτία ανησυχίας είναι η εξάρτησή της από τα βασικά πλήκτρα ελέγχου πρόσβασης που είναι γνωστό ότι είναι ανασφαλής. Ενώ η διεύθυνση προδιαγραφών ePassport τρίτης γενιάς σχεδόν σε κάθε ανησυχία ασφάλειας έθεσε από την πρώτη και δεύτερη γενιάς προδιαγραφές, ότι έχουν λήξει τερματικά προβλήματος εξακολουθούν να είναι μια σημαντική αιτία για ανησυχία, ειδικά για τα ηλεκτρονικά διαβατήρια σπανίως χρησιμοποιούνται. Έχουμε περιγράψει τις τρεις γενιές προδιαγραφών ePassport μαζί με τις επιχειρησιακές τους διαδικασίες και αναλύσαμε τις αδυναμίες.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. A Survey on the Evolution of Cryptographic Protocols in ePassports, Rishab Nithyanand
2. An Overview of Electronic Passport Security Features**,** Zdeněk Říha**,** Faculty of Informatics, Masaryk University, Botanická 68A, 602 00 Brno, Czech Republic
3. DESIGN AND IMPLEMENTATION OF E-PASSPORT SCHEME USING CRYPTOGRAPHIC ALGORITHM ALONG WITH MULTIMODAL BIOMETRICS TECHNOLOGY, V.K. Narendira Kumar and B. Srinivasan, International Journal of Advanced Information Technology (IJAIT) Vol. 1, No. 6, December 2011
4. Leveraging the e-passport PKI to achieve interoperable security for e-government cross border services, Dimitrios Lekkas and Dimitrios Zissis
5. A better time approximation scheme for e-passports , Charalampos Petrou, Christoforos Ntantogian, Christos Xenakis
6. Biometrics and their use in e-passports, Ben Schouten , Bart Jacobs
7. Formal Security Analysis of Australian E-passport Implementation, Vijayakrishnan P Josef Pieprzyk Huaxiong Wang
8. Security Analysis of Australian and E.U. E-passport Implementation, Vijayakrishnan Pasupathinathan and Josef Pieprzyk, Department of Computing, Macquarie University, New South Wales, Australia 2109
9. Technical analysis of security mechanisms used in RFID E-passport, related threats, security and privacy issues, Shah Sheetal, Los Angeles, CA, USA
10. Security and Privacy Issues in E-passports, Ari Juels, David Molnary, and David Wagnerz
11. Operational and Technical security of Electronic Passports ,Warsaw, July 2011
12. Technical analysis of security mechanisms used in RFID E-passport, related threats, security and privacy issues, Shah Sheetal, Viterbi School of Engineering, University of Southern California, Los Angeles, CA, USA
13. Implementation of an Improved Secure System Detection for E-passport by using EPC RFID Tags, A. Baith Mohamed, Ayman Abdel-Hamid, Kareem Youssri Mohamed, World Academy of Science, Engineering and Technology 36 2009

14. A Note on the Relay Attacks on e-passports? The Case of Czech e-passports, Martin Hlavac and Tomas Rosa

15. Moving to the third generation of electronic passports, A new dimension in electronic passport security with Supplemental Access Control (SAC) (gemalto)

16. Βιομετρικές μέθοδοι και προστασία ιδιωτικότητας: Σκέψεις με αφορμή την απόφαση ΔΕΕ Michael Schwarz κατά κρατιδίου Bochum (C-291/2012)*, Φερενίκη Παναγοπούλου-*Κουντατζή***, Δρ. Ν. (Humboldt), Μ.Δ.Ε. (Παν. Αθηνών), M.P.H. (Harvard

Ιστοσελίδες

1. http://en.wikipedia.org/wiki/Passport
2. http://www.dhs.gov/e-passports
3. http://en.wikipedia.org/wiki/Biometric_passport
4. www.smartcardalliance.org (ePassport Frequently Asked Questions, A Smart Card Alliance Identity Council Publication, Publication Date: March 2009, Publication Number: IC-09001)
5. https://www.passports.gov.au/web/epassport.aspx
6. http://passport.gc.ca/eppt/photos.aspx?lang=eng
7. http://www.passport.gov.gr/el/
8. http://www.passport.gov.gr/npc-periexomeno/npc-periexomeno/viometrika-xaraktiristika-diavatiriou.html
9. http://www.icao.int/Pages/default.aspx
10. http://europa.eu/index_el.htm

ΕΙΚΟΝΕΣ