ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ

ΤΕΧΝΟΟΙΚΟΝΟΜΙΚΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΚΑΤΕΥΘΥΝΣΗ: ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΕ ΣΥΣΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΔΙΑΒΑΤΗΡΙΩΝ

Φοιτητής

Πέτρου Χαράλαμπος

Α.Μ 0925

ΕΠΙΒΛΕΨΗ: Λέκκας Δημήτριος

ΣΕΠΤΕΜΒΡΙΟΣ 2012

Πρόλογος

Τα ηλεκτρονικά διαβατήρια έχουν πλέον υιοθετηθεί παγκοσμίως ως το νέο μέσο ταυτοποίησης φυσικών προσώπων στους συνοριακούς ελέγχους μεταξύ των χωρών. Πρόκειται για υβριδικά έγγραφα τα οποία συνδυάζουν την παραδοσιακή μορφή με ενσωματωμένα ολοκληρωμένα κυκλώματα ικανά για αποθήκευση και επεξεργασία δεδομένων καθώς και κεραία για ασύρματη μετάδοση. Η νέα αυτή μορφή των διαβατηρίων έχει σκοπό να μειώσει δραστικά την πιθανότητα πλαστογραφίας και να αυξήσει σημαντικά την ευκολία αλλά και την αξιοπιστία των ελέγχων στα σημεία πρόσβασης χρησιμοποιώντας ασφαλή ψηφιακή αποθήκευση προσωπικών δεδομένων και πρωτόκολλα επικοινωνίας με τις μηχανές ανάγνωσης βασισμένα στην επιστήμη της κρυπτογραφίας. Παρόλα αυτά η επιλογή της τεχνολογίας RFID καθώς και η χρήση βιομετρικών στοιχείων τα οποία έχουν ήδη εισαχθεί από την δεύτερη γενιά των ηλεκτρονικών διαβατηρίων έχουν εγείρει αρκετά θέματα σχετικά με την διαφύλαξη της ιδιωτικότητας των κατόχων τους. Η σωστή αυθεντικοποίηση των τερματικών ανάγνωσης πριν την ικανότητα ανάγνωσης των ευαίσθητων προσωπικών δεδομένων από αυτά αποτελεί την λύση που εφαρμόζεται στις δύο τελευταίες γενιές. Η παρούσα εργασία αναλύει τους μηχανισμούς ασφάλειας όλων των γενιών διαβατηρίων και εστιάζει στην αδυναμία που φαίνεται να έχει απομείνει κατά την αυθεντικοποίηση των τερματικών ανάγνωσης. Παρουσιάζονται προτάσεις για την εξάλειψη της εν λόγω αδυναμίας από την βιβλιογραφία καθώς και δύο νέες προτάσεις προς την ίδια κατεύθυνση και αναλύονται ως προς την ασφάλεια τους.

Πίνακας Περιεχομένων

Λίστα Εικόνων

Εισαγωγή

Στην σημερινή εποχή όπου οι μετακινήσεις ανθρώπων μεταξύ χωρών γίνονται ολοένα και πιο συχνές έχει αρχίσει να διαφαίνεται η ανάγκη αντικατάστασης του παραδοσιακού τρόπου ταυτοποίησης φυσικών προσώπων με χρήση συμβατικών διαβατηρίων η οποία και στερείται του απαιτούμενου επιπέδου ασφάλειας. Τα νέα τεχνολογικά μέσα δίνουν την δυνατότητα σε αυτόν που τα κατέχει να πλαστογραφήσει τα παραδοσιακά έγγραφα με σχετική ευκολία και καθώς ο σημερινός έλεγχος βασίζεται στην υποκειμενική κρίση του ελεγκτή, να αλλάξει ταυτότητα και να δράσει ως κάποιος άλλος. Τα ηλεκτρονικά διαβατήρια αποτελούν μια νέα μορφή εγγράφων ταυτοποίησης η οποία έχει σκοπό να αυξήσει το επίπεδο ασφάλειας αποτρέποντας τέτοιους κινδύνους, ενισχύοντας την διαδικασία ελέγχου και διασφαλίζοντας την ακεραιότητα και αυθεντικότητα των εγγράφων. Οι τεχνολογίες που χρησιμοποιούνται είναι η υπολογιστική ισχύς, η οποία υπάρχει στο ολοκληρωμένο κύκλωμα το οποίο ενσωματώνουν τα νέα διαβατήρια, η τεχνολογία των RFIDs (ταυτοποίηση μέσω ραδιοσυχνοτήτων) δίνοντας την ικανότητα της ασύρματης επικοινωνίας με τις συσκευές ελέγχου (τερματικά ανάγνωσης) και φυσικά οι κρυπτογραφικές τεχνικές.

Δύο είναι τα κύρια θέματα προς επίλυση που αντιμετωπίζει η εφαρμογή των ηλεκτρονικών διαβατηρίων στην παρούσα φάση. Πρώτον, η ανάπτυξη μηχανισμών όσο το δυνατόν πιο ασφαλών όσον αφορά στην διασφάλιση της ιδιωτικότητας των κατόχων των νέων διαβατηρίων καθώς το νέο μέσο θα παρουσιάζει πλέον ευαίσθητα προσωπικά δεδομένα όπως βιομετρικά στοιχεία και δεύτερον η ανάπτυξη και εγκαθίδρυση μιας παγκόσμιας υποδομής δημόσιου κλειδιού η οποία είναι αναγκαία για να υποστηρίξει τόσο τους παραπάνω μηχανισμούς ασφάλειας όσο και τους μηχανισμούς αυθεντικοποίησης των ίδιων των διαβατηρίων.

Η παρούσα εργασία ασχολείται με τους μηχανισμούς ασφάλειας στις τρεις γενιές ηλεκτρονικών διαβατηρίων που ως τώρα έχουν παρουσιαστεί και εστιάζει στην κύρια αδυναμία που φαίνεται να έχει μείνει στην τρίτη γενιά, αυτήν της αδυναμίας ελέγχου των πιστοποιητικών των τερματικών συσκευών από πλευράς διαβατηρίου.

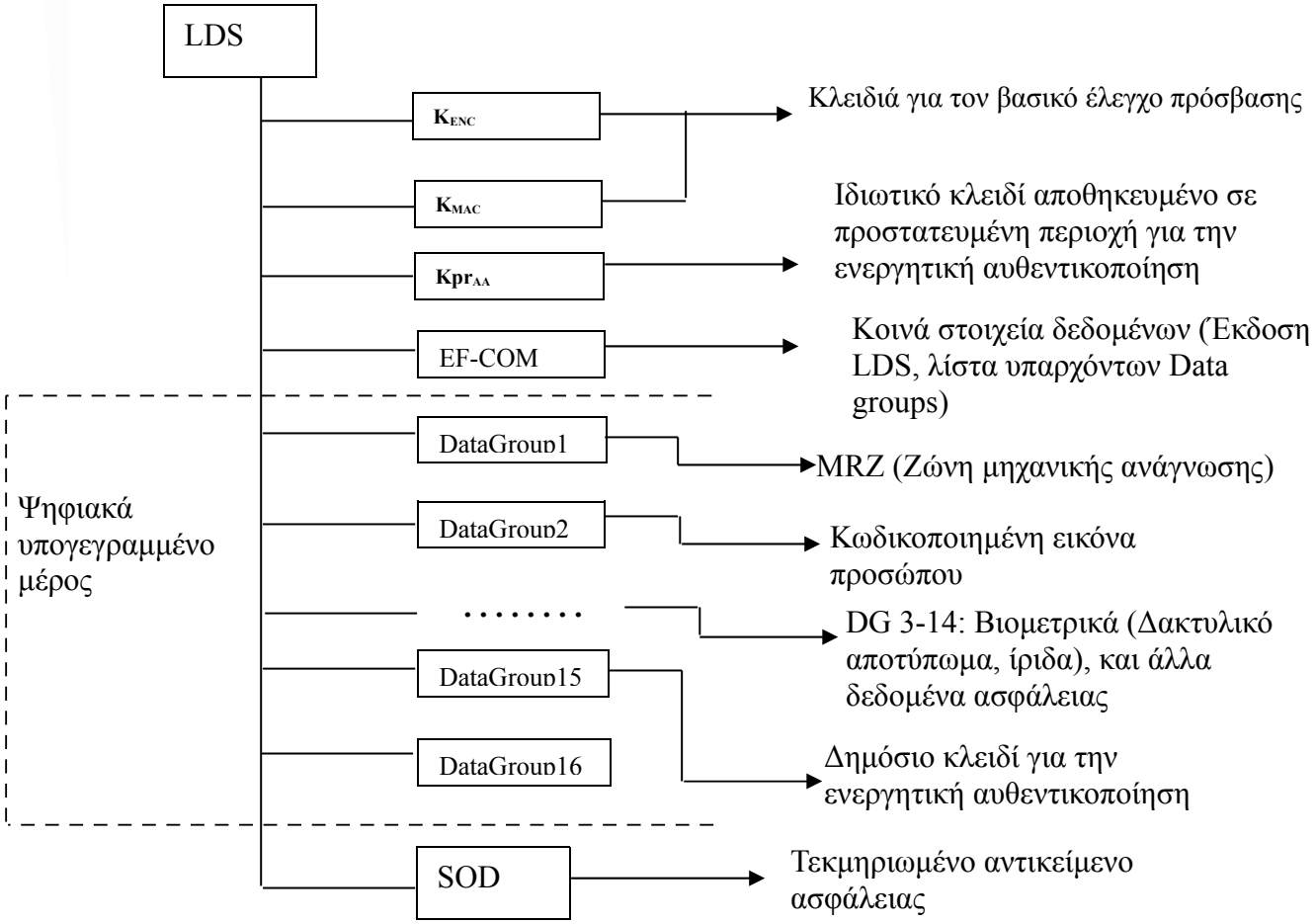
Στο πρώτο κεφάλαιο αναλύονται οι μηχανισμοί ασφάλειας σε κάθε γενιά διαβατηρίων και αναφέρονται οι λόγοι που οδήγησαν στην μετάβαση από την μία γενιά στην άλλη. Στο δεύτερο κεφάλαιο αναφέρεται το πρόβλημα ελέγχου των πιστοποιητικών και αναλύονται οι προτεινόμενες λύσεις που έχουν βρεθεί από την βιβλιογραφία. Τέλος στο τρίτο κεφάλαιο παρουσιάζονται δύο νέες προτάσεις και αναλύονται ως προς την ασφάλεια τους.

Κεφάλαιο 1 Μηχανισμοί Ασφάλειας ηλεκτρονικών Διαβατηρίων

.

1.1 Διαδικασίες Αυθεντικοποίησης ηλεκτρονικών Διαβατηρίων πρώτης γενιάς

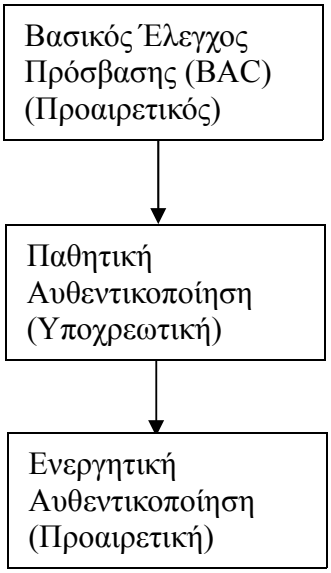
Το 2004 ο Διεθνής Οργανισμός Πολιτικής Αεροπορίας (ICAO) δημοσίευσε τις προδιαγραφές της λογικής δομής των δεδομένων που θα αποθηκεύονται σε ψηφιακή μορφή στο ολοκληρωμένο κύκλωμα που θα φέρουν τα διαβατήρια της πρώτης γενιάς προσπαθώντας έτσι να εξασφαλίσει την διαλειτουργικότητα μεταξύ των τερματικών ελέγχου και διαβατηρίων των διάφορων χωρών που θα υιοθετούσαν την νέα μορφή των διαβατηρίων. Σύμφωνα με τις προδιαγραφές υπάρχουν 16 ομάδες δεδομένων σε περιοχές προστατευμένες από εγγραφή, οι οποίες θα γράφονται μόνο κατά την φάση προσωποποίησης του διαβατηρίου. Οι ομάδες από 1 ως 15 θα πρέπει να υπογράφονται από την αρχή έκδοσης του διαβατηρίου και η υπογραφή θα αποθηκεύεται στην θέση SOD. Η λογική δομή των δεδομένων φαίνεται στο παρακάτω σχήμα:



Εικόνα 1 : Λογική δομή δεδομένων (LDS) ηλεκτρονικού διαβατηρίου

Την ίδια χρονιά η ICAO παρουσίασε τις προδιαγραφές των μηχανισμών ασφάλειας των ηλεκτρονικών διαβατηρίων πρώτης γενιάς εισάγοντας τρία πρωτόκολλα μεταξύ της επικοινωνίας ενός διαβατηρίου και ενός τερματικού ανάγνωσης· τον βασικό έλεγχο πρόσβασης, την παθητική αυθεντικοποίηση και την ενεργητική αυθεντικοποίηση.

Ο ρόλος του βασικού έλεγχου πρόσβασης είναι η έμμεση αυθεντικοποίηση του αναγνώστη και το επιτυγχάνει αυτό με το να απαιτείται οπτική επαφή της σελίδας δεδομένων του διαβατηρίου από το τερματικό ανάγνωσης. Η παθητική αυθεντικοποίηση ουσιαστικά εξασφαλίζει πως τα περιεχόμενα του διαβατηρίου είναι ακέραια και δεν έχουν αλλοιωθεί ενώ η ενεργητική αυθεντικοποίηση προστατεύει από το ενδεχόμενο της πλήρης κλωνοποίησης του διαβατηρίου από τρίτους. Στο παρακάτω σχήμα φαίνεται η σειρά με την οποία εφαρμόζονται τα τρία πρωτόκολλα κατά την διαδικασία αυθεντικοποίησης των διαβατηρίων πρώτης γενιάς από ένα τερματικό. Αρχικά εκτελείται ο βασικός έλεγχος πρόσβασης κατά τον οποίο εξάγονται και τα κλειδιά συνόδου, τα οποία θα χρησιμοποιηθούν για την κρυπτογράφηση και αυθεντικοποίηση όλης της περαιτέρω επικοινωνίας. Έπειτα εκτελείται η παθητική αυθεντικοποίηση, η οποία αποτελεί και τον μόνο υποχρεωτικό μηχανισμό ασφάλειας στα διαβατήρια πρώτης γενιάς και τέλος εκτελείται το πρωτόκολλο της ενεργητικής αυθεντικοποίησης.



Εικόνα 2: Στάδια αυθεντικοποίησης ηλεκτρονικών διαβατηρίων πρώτης γενιάς

Στα επόμενα τρία κεφάλαια θα παρουσιαστούν αναλυτικά τα παραπάνω πρωτόκολλα.

1.1.1 Βασικός έλεγχος πρόσβασης

Ο βασικός έλεγχος πρόσβασης ουσιαστικά εξασφαλίζει πως το τερματικό θα πρέπει να έχει φυσική πρόσβαση στο διαβατήριο και αυτό το επιτυγχάνει με το να απαιτείται οπτική ανάγνωση της σελίδας δεδομένων του διαβατηρίου για την εξαγωγή του κλειδιού αυθεντικοποίησης. Χρησιμοποιείται επίσης για την παραγωγή κλειδιών συνόδου με σκοπό την προστασία της εμπιστευτικότητας και της ακεραιότητας των δεδομένων που ανταλλάσσονται.
Αρχικά το τερματικό θα πρέπει να έρθει σε οπτική επαφή με το διαβατήριο και να αποθηκεύσει την πληροφορία που βρίσκεται στην MRZ περιοχή. Η πληροφορία MRZ είναι της μορφής:

P<CZESPECIMEN<<VZOR<<<<<<<<<<<<<<<<<<<<
99009054<4CZE6906229F16072996956220612<<<<74

Και βρίσκεται σε εμφανές μέρος στην σελίδα δεδομένων του διαβατηρίου όπως φαίνεται στο παρακάτω σχήμα:

Εικόνα 3: Ζώνη μηχανικής ανάγνωσης (MRZ) στην σελίδα δεδομένων ενός διαβατηρίου

Την πληροφορία MRZ την χρησιμοποιεί το τερματικό για να υπολογίσει το κλειδί αυθεντικοποίησης K_{MAC} και το κλειδί κρυπτογράφησης K_{ENC}. Τα κλειδιά αυτά θα χρησιμοποιηθούν για να προστατέψουν την ανταλλαγή πληροφορίας που χρειάζεται για να παραχθούν τα κλειδιά συνόδου με τα οποία θα προστατευτεί όλη η μετέπειτα επικοινωνία μεταξύ διαβατηρίου και τερματικού.
Ο υπολογισμός των K_{MAC}, K_{ENC} έχει ως εξής:
Από τα πεδία της MRZ που αφορούν τον αριθμό διαβατηρίου, την ημερομηνία γέννησης και την

ημερομηνία λήξης κατασκευάζεται η MRZ πληροφορία η οποία αποτελείται από 24 χαρακτήρες. Έπειτα εισάγεται η παραπάνω πληροφορία στον SHA-1 αλγόριθμο για να παραχθεί ένα hash 40 χαρακτήρων. Τα 16 πιο σημαντικά bytes αποτελούν το K_{SEED} το οποίο θα συνενωθεί με το byte 00000001 για την παραγωγή του K_{ENC} και με το byte 00000002 για την παραγωγή του K_{MAC}. (D_1 = K_{SEED} || 00000001, D_2 = K_{SEED} || 00000002). Έπειτα οι ποσότητες D_1 και D_2 θα περάσουν πάλι από τον SHA-1 και τα πρώτα 16 bytes θα αποτελέσουν τα κλειδιά KA_1 και KA_2 αντίστοιχα, ενώ τα 16 επόμενα bytes τα κλειδιά KB_1, KB_2. Τα κλειδιά αυτά τροποποιούνται έτσι ώστε να περιέχουν έγκυρα parity bits και τελικά τα K_{ENC} και K_{MAC} υπολογίζονται ως συνένωση των αντίστοιχων KA, KB. Η παραπάνω διαδικασία παρουσιάζεται και παρακάτω με την μορφή βημάτων:

Κατασκευή K_{ENC}	Κατασκευή K_{MAC}
1) Οπτική ανάγνωση MRZ	Οπτική ανάγνωση MRZ
2) Κατασκευή MRZ_info (40 χαρακτήρες)	Κατασκευή MRZ_info (40 χαρακτήρες)
3) $K_{SEED} = H_{SHA-1}$ (MRZ_info) (16 πιο σημαντικά bytes)	$K_{SEED} = H_{SHA-1}$ (MRZ_info) (16 πιο σημαντικά bytes)
4) K_{SEED} || 00000001 = D_1	K_{SEED} || 00000002 = D_2
5) $KA_1 = H_{SHA-1}(D_1)$ (Πρώτα 8 bytes) $KB_1 = H_{SHA-1}(D_1)$ (Επόμενα 8 bytes)	$KA_2 = H_{SHA-1}(D_2)$ (Πρώτα 8 bytes) $KB_2 = H_{SHA-1}(D_2)$ (Επόμενα 8 bytes)
6) Προσαρμογή των parity bits	Προσαρμογή των parity bits
7) $K_{ENC} = KA_1$ || KB_1	$K_{MAC} = KA_2$ || KB_2

Τα K_{ENC}, K_{MAC} υπολογίζονται στην πλευρά του τερματικού και υπάρχουν και στο διαβατήριο σε ασφαλή περιοχή μη αναγνώσιμη έτσι ώστε ο μόνος τρόπος εξαγωγής τους να είναι η οπτική ανάγνωση της MRZ περιοχής και οι παραπάνω μετασχηματισμοί.

Η προσαρμογή των parity bits γίνεται γιατί τα KA_1, KB_1, KA_2, KB_2 έχουν μήκος 64 bit και θα χρησιμοποιηθούν για κλειδιά στον αλγόριθμο DES ο οποίος δέχεται 54 bits και αγνοεί τα υπόλοιπα. Έτσι το τελευταίο bit από κάθε byte μπορεί να χρησιμοποιηθεί ως parity bit για να μπορεί να

ελεγχθεί η ακεραιότητα του κλειδιού.

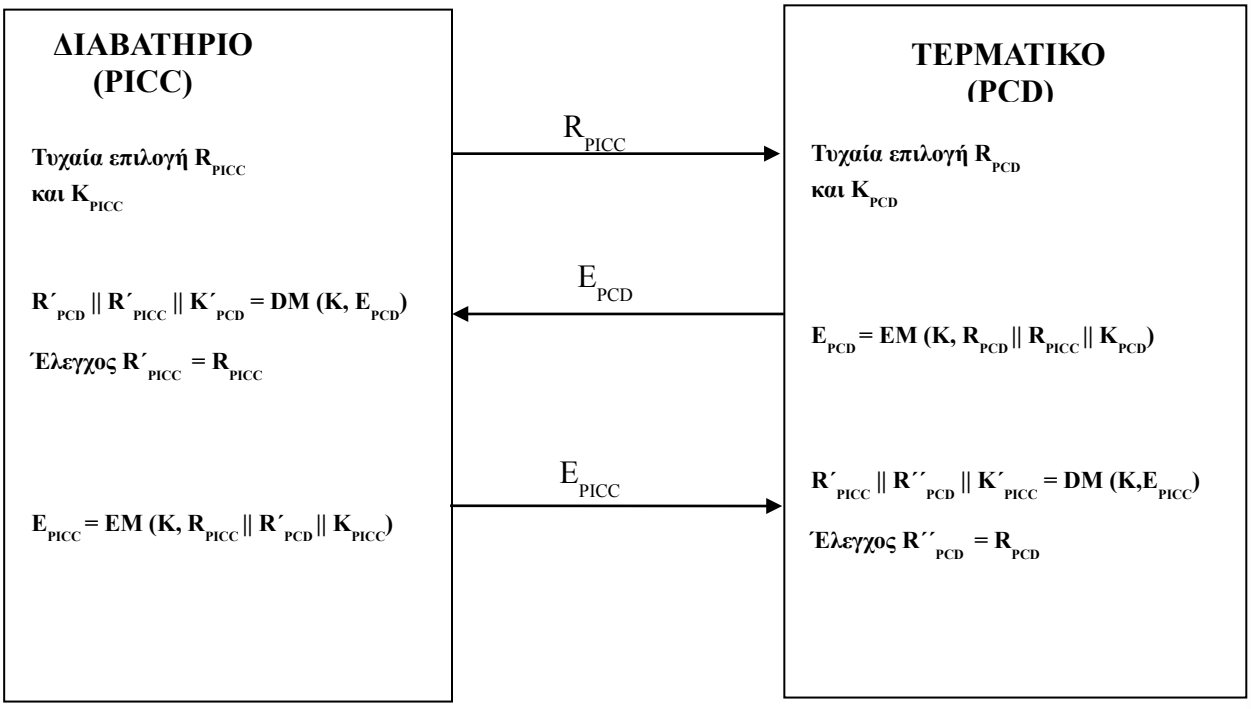
Η αυθεντικοποίηση και η δημιουργία των κλειδιών συνόδου KS_{ENC} και KS_{MAC} πραγματοποιείται με χρήση πρωτοκόλλου Πρόσκλησης-Απάντησης τριών περασμάτων. Η κρυπτογράφηση των μηνυμάτων βασίζεται στον αλγόριθμο 3DES, χρησιμοποιώντας μέθοδο αλυσιδωτής κρυπτογράφησης (CBC mode), μηδενικό IV και δύο κλειδιά (KA_1, KB_1). Για την αυθεντικοποίηση των μηνυμάτων χρησιμοποιείται ο MAC αλγόριθμος 3 κατά ISO/IEC 9797-1 με αλγόριθμο τμήματος DES και μηδενικό IV, ενώ η MAC τιμή υπολογίζεται πάνω στο κρυπτογραφημένο μήνυμα και συνενώνεται μ' αυτό κατά την αποστολή [βλέπε [1] ,annex E.4].

Στο παρακάτω σχήμα φαίνεται η ανταλλαγή των μηνυμάτων που πραγματοποιείται κατά τη διάρκεια του βασικού ελέγχου πρόσβασης. Για λόγους αναγνωσιμότητας ορίζεται η πράξη EM (K,S) για την κρυπτογράφηση και τον υπολογισμό της τιμής MAC ενός μηνύματος S ως εξής:

$$\mathbf{EM\ (K,\ S) = E\ (K_{ENC},\ S)\ ||\ MAC\ (K_{MAC},\ E\ (K_{ENC},\ S))}$$

όπου $\mathbf{K = \{\ K_{ENC}\ ,\ K_{MAC}\ \}}$

ενώ για την επαλήθευση και την αποκρυπτογράφηση του μηνύματος S ορίζεται η πράξη DM (K, C) έτσι ώστε: **DM (K, EM (K,S)) = S**



Εικόνα 4: Αυθεντικοποίηση και δημιουργία κλειδιών κατά τον βασικό έλεγχο πρόσβασης

Αρχικά το διαβατήριο επιλέγει με τυχαίο τρόπο το R_{PICC} (64 bit) και το K_{PICC} (128 bit) και στέλνει στο τερματικό το R_{PICC}.

Το τερματικό επιλέγει και αυτό με τυχαίο τρόπο τα R_{PCD} (64 bit) και το K_{PCD} (128 bit) και αφού λάβει το R_{PICC} στέλνει την κρυπτογραφημένη απάντηση E_{PCD} όπου $E_{PCD} = EM (K, R_{PCD} || R_{PICC} || K_{PCD})$ και $K = \{ K_{ENC} , K_{MAC} \}$.

Για τον υπολογισμό της τιμής MAC χρειάζεται σαν είσοδος και μια 64bit τιμή (SSD) η οποία υπολογίζεται ως η συνένωση των 4 πιο σημαντικών bytes του R_{PICC} και των 4 πιο σημαντικών bytes του R_{PCD} ($SSD = R_{PICC} || R_{PCD}$) [βλέπε [1] ,annex E.4.2]. Κάθε φορά και πριν την αποστολή ενός κρυπτογραφημένου μηνύματος μέσο της πράξης EM, για τον υπολογισμό της MAC η τιμή του SSD αυξάνεται κατά ένα.

Το διαβατήριο αποκρυπτογραφεί την απάντηση ($R'_{PCD} || R'_{PICC} || K'_{PCD} = DM (K,E_{PCD})$) και ελέγχει αν $R'_{PICC} = R_{PICC}$. Έπειτα στέλνει το κρυπτογραφημένο μήνυμα $E_{PICC} = EM (K, R_{PICC} || R'_{PCD} || K_{PICC})$

Το τερματικό αποκρυπτογραφεί το μήνυμα ($R'_{PICC} || R''_{PCD} || K'_{PICC} = DM (K,E_{PICC})$) και ελέγχει αν $R''_{PCD} = R_{PCD}$.

Τελικά διαβατήριο και τερματικό έχουν ανταλλάξει τα K_{PICC} και K_{PCD} με ασφαλή τρόπο χρησιμοποιώντας τα κλειδιά K_{ENC} , K_{MAC} και υπολογίζουν τα κλειδιά συνόδου KS_{ENC} και KS_{MAC} με τον ίδιο τρόπο που υπολογίστηκαν τα K_{ENC} , K_{MAC} από το K_{SEED} θεωρώντας πλέον ως K_{SEED} την τιμή: K_{PICC} XOR K_{PCD}. Από δω και πέρα όλη η επικοινωνία προστατεύεται με την μέθοδο *κρυπτογράφησε και μετά αυθεντικοποίησε* όπως και παραπάνω βάσει όμως πλέον των κλειδιών KS_{ENC} και KS_{MAC}.

1.1.2 Παθητική αυθεντικοποίηση

Η παθητική αυθεντικοποίηση είναι μια μέθοδος που βασίζεται στις ψηφιακές υπογραφές με σκοπό να αυθεντικοποίησει τα περιεχόμενα της λογικής δομής δεδομένων (LDS) του διαβατηρίου και να παρέχει έτσι προστασία έναντι σε προσπάθειες παραποίησης των δεδομένων αυτών.

Στην ομάδα δεδομένων 16 μέσα στην κάρτα βρίσκεται το *τεκμηριωμένο αντικείμενο ασφάλειας* (Document Security Object, SO_D). Πρόκειται για την ψηφιακή υπογραφή των δεδομένων από τις υπόλοιπες ομάδες η οποία δημιουργείται κατά την φάση της προσωποποίησης του διαβατηρίου από την Εκδίδουσα Αρχή (DS). Όλα τα δεδομένα έχοντας πρώτα περάσει από μια συνάρτηση κατακερματισμού κρυπτογραφούνται βάσει του ιδιωτικού κλειδιού του DS και αποθηκεύονται στην ομάδα 16. Το τερματικό ανάγνωσης πρέπει να έχει στην κατοχή του το ψηφιακό πιστοποιητικό του DS, το πιστοποιητικό της κρατικής αρχής πιστοποίησης (CSCA) η οποία πιστοποιεί τον DS και την αντίστοιχη λίστα ανάκλησης πιστοποιητικών. Έπειτα αφού έχει εξάγει όλα τα περιεχόμενα της LDS

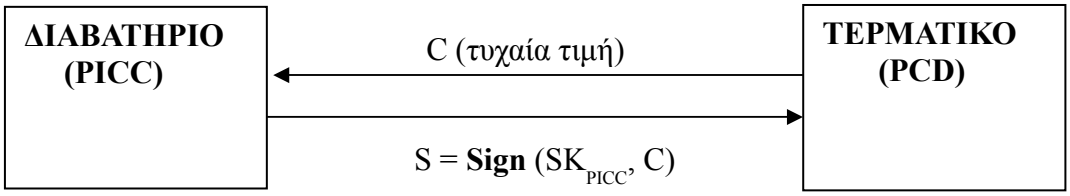
δομής, υπολογίζει την hash τιμή τους και την συγκρίνει με το SO_D (αφού πρώτα ελέγξει την εγκυρότητα του πιστοποιητικού του DS και μετά χρησιμοποιήσει το δημόσιο κλειδί του για να αποκρυπτογραφήσει το SO_D). Με αυτόν τον τρόπο ελέγχεται η ακεραιότητα και η αυθεντικότητα των ψηφιακών δεδομένων του διαβατηρίου.

Η παθητική αυθεντικοποίηση προστατεύει από το ενδεχόμενο παραποίησης των δεδομένων που βρίσκονται σε ψηφιακή μορφή μέσα στο ολοκληρωμένο κύκλωμα που φέρουν τα διαβατήρια, δεν προστατεύει όμως από το ενδεχόμενο αντικατάστασης του ολοκληρωμένου από κάποιο άλλο μέσα στο ίδιο το διαβατήριο όπως επίσης και από το ενδεχόμενο πλήρους κλωνοποίησης ενός διαβατηρίου. Η πρώτη απειλή αντιμετωπίζεται με το να αποθηκεύεται η MRZ πληροφορία και στην σελίδα δεδομένων των διαβατηρίων και σε ψηφιακή μορφή μέσα στην LDS δομή. Έτσι το τερματικό μπορεί να ελέγξει αν η πληροφορία που απέκτησε κατά τον βασικό έλεγχο πρόσβασης από την σελίδα δεδομένων ταιριάζει με την ψηφιακά αποθηκευμένη τιμή που λαμβάνει κατά την παθητική αυθεντικοποίηση και να αποτρέψει έτσι τον κίνδυνο της αντικατάστασης. Την δεύτερη απειλή έρχεται να αντιμετωπίσει η ενεργητική αυθεντικοποίηση. Όσον αφορά στην αναγκαία υποδομή δημοσίου κλειδιού και στις οντότητες πιστοποίησης CSCA και DS που την απαρτίζουν, αυτές θα αναλυθούν περισσότερο στο κεφάλαιο 1.4.

1.1.3 Ενεργητική αυθεντικοποίηση

Η ενεργητική αυθεντικοποίηση προστατεύει από το ενδεχόμενο των κλώνων χρησιμοποιώντας την τεχνική Πρόκλησης – Απάντησης (Challenge- response).

Στην ομάδα 15 περιέχεται ένα δημόσιο κλειδί, το οποίο προστατεύεται από το τεκμηριωμένο αντικείμενο ασφάλειας ως προς την ακεραιότητα του. Το τερματικό ανάγνωσης στέλνει μια τυχαία τιμή στην κάρτα (challenge) και το διαβατήριο απαντά υπογράφοντας την τιμή αυτή με το αντίστοιχο ιδιωτικό κλειδί το οποίο βρίσκεται σε προστατευμένο και μη αναγνώσιμο σημείο μέσα στο chip του διαβατηρίου. Με αυτόν τον τρόπο το τερματικό μπορεί να διαπιστώσει, χρησιμοποιώντας το δημόσιο κλειδί της ομάδας 15, ότι το διαβατήριο όντως κατέχει το συγκεκριμένο ιδιωτικό κλειδί και πως δεν πρόκειται για κλώνο.



SK_{PICC}: Ιδιωτικό κλειδί διαβατηρίου αποθηκευμένο σε μη προσβάσιμη περιοχή

Εικόνα 5: Ενεργητική Αυθεντικοποίηση

1.2 Διαδικασίες Αυθεντικοποίησης ηλεκτρονικών Διαβατηρίων δεύτερης γενιάς

Το 2006 η ομάδα εργασίας NTWG (New Technologies Working Group) του ICAO εγκρίνει τις καινούργιες προδιαγραφές για τα ηλεκτρονικά διαβατήρια διαμορφώνοντας έτσι την δεύτερη γενιά διαβατηρίων. Κύριος σκοπός της δεύτερης γενιάς είναι να καλύψει τις αδυναμίες του αρχικών μηχανισμών. Καταρχήν ο μηχανισμός του βασικού έλεγχου πρόσβασης γίνεται υποχρεωτικός και η ενεργητική αυθεντικοποίηση έχει αντικατασταθεί από ένα νέο πρωτόκολλο, την αυθεντικοποίηση CHIP. Επίσης εισάγονται ως υποχρεωτικά τα δευτερεύοντα βιομετρικά στοιχεία στο κύκλωμα των διαβατηρίων όπως η ίριδα και τα δακτυλικά αποτυπώματα με σκοπό την ενίσχυση της διαδικασίας της ταυτοποίησης. Τα βιομετρικά αυτά θεωρούνται ευαίσθητα προσωπικά δεδομένα και για την προστασία τους εισάγεται το πρωτόκολλο της αυθεντικοποίησης του τερματικού. Δημιουργείται δηλαδή για πρώτη φορά ο έλεγχος της εξουσιοδότησης που πρέπει να έχουν τα τερματικά ανάγνωσης έτσι ώστε να έχουν πρόσβαση σε ευαίσθητα δεδομένα.

Μια αδυναμία της ενεργητικής αυθεντικοποίησης προκύπτει από το γεγονός πως κατά την εκτέλεση της το διαβατήριο ουσιαστικά υπογράφει τυχαίες τιμές χωρίς να γνωρίζει και να ελέγχει την σημασιολογία τους. Αυτό δίνει την δυνατότητα σε κρυπταναλυτικές επιθέσεις επιλεγμένου καθαρού μηνύματος (chosen plaintext attacks) να εκτελεστούν σε μια προσπάθεια εξαγωγής του ιδιωτικού κλειδιού του διαβατηρίου πράγμα εφικτό καθώς το πρωτόκολλο δεν απαιτεί αυθεντικοποιημένα τερματικά για να εκτελεστεί. Ο βασικός έλεγχος πρόσβασης μπορεί να περιορίζει τέτοιου είδους επιθέσεις αλλά δεν τις αποκλείει καθώς η MRZ πληροφορία ενός διαβατηρίου θα μπορούσε εύκολα να εξαχθεί όπως θα αναλυθεί και στο κεφάλαιο 1.3. Μία τεχνική που θα μπορούσε να εφαρμοστεί ώστε να αποφευχθεί ένα τέτοιο ενδεχόμενο είναι η σημασιολογία των προκλήσεων κατά την οποία το τερματικό παράγει την προς υπογραφή τιμή με έναν μη προβλέψιμο αλλά ελέγξιμο τρόπο. Όπως αναφέρεται και στο [2] τα τερματικά των διάφορων χωρών θα μπορούσαν να εφαρμόσουν τέτοιες τεχνικές και αντί της τυχαίας τιμής του C να στέλνουν στο διαβατήριο την τιμή:

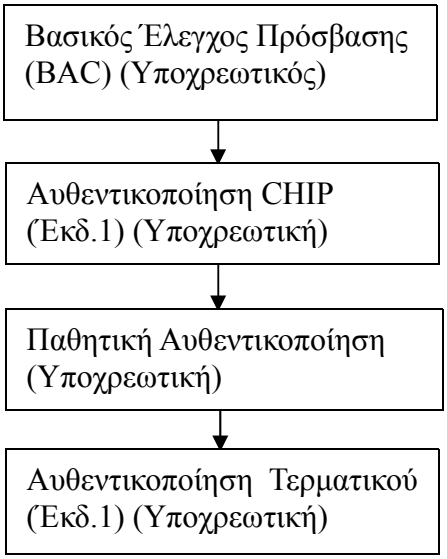
$$\mathbf{C = Sign\ (SK_{PCD},\ ID_{PICC} \parallel Ημέρα \parallel Ώρα \parallel Τοποθεσία)}$$

όπου SK_{PCD} είναι το ιδιωτικό κλειδί του τερματικού και ID_{PICC} το αναγνωριστικό του διαβατηρίου με σκοπό όχι μόνο την αντιμετώπιση της παραπάνω απειλής αλλά και για εσωτερική τους χρήση, όπως η εξακρίβωση πως ένα συγκεκριμένο άτομο έχει μεταναστεύσει. Με την εφαρμογή μιας τέτοιας τεχνικής το διαβατήριο θα μπορεί να εξακριβώσει ότι το τερματικό όντως δημιούργησε την πρόκληση και μόνο τότε να υπογράφει. Δημιουργείται όμως εδώ ένας νέος κίνδυνος σχετικά με την

ικανότητα εντοπισμού του στίγματος του διαβατηρίου από κάποιον κακόβουλο που παρακολουθεί την επικοινωνία κατά την διάρκεια της ενεργητικής αυθεντικοποίησης.

Η υιοθέτηση του πρωτοκόλλου CHIP αποφεύγει τέτοιου είδους προβλήματα και επιπλέον προσφέρει ισχυρά κλειδιά συνόδου τα οποία και χρησιμοποιούνται για την κρυπτογράφηση και αυθεντικοποίηση των μηνυμάτων της περαιτέρω επικοινωνίας. Εξαλείφεται έτσι και η αδυναμία που προκύπτει από τα χαμηλής εντροπίας κλειδιά του βασικού έλεγχου πρόσβασης, τουλάχιστον για την επικοινωνία που λαμβάνει χώρα από την εφαρμογή της CHIP αυθεντικοποίησης και μετά.

Τα βήματα που ακολουθούν τα διαβατήρια δεύτερης γενιάς κατά την διαδικασία της αυθεντικοποίησης με τις τερματικές συσκευές είναι τα εξής: Αρχικά εκτελείται ο βασικός έλεγχος πρόσβασης. Έπειτα ακολουθεί η αυθεντικοποίηση CHIP δημιουργώντας και τα κλειδιά συνόδου. Από κει και πέρα η επικοινωνία προστατεύεται από τα νέα κλειδιά. Ακολουθεί η παθητική αυθεντικοποίηση και τέλος εκτελείται η αυθεντικοποίηση του τερματικού. Μετά την επιτυχή λήξη της διαδικασίας το τερματικό μπορεί να αποκτήσει πρόσβαση στα δευτερεύοντα βιομετρικά του διαβατηρίου. Όλα τα στάδια είναι πλέον υποχρεωτικά.



Εικόνα 6: Στάδια αυθεντικοποίησης ηλεκτρονικών διαβατηρίων δεύτερης γενιάς

Τα παρακάτω δύο κεφάλαια παρουσιάζουν αναλυτικά τα πρωτόκολλα CHIP και αυθεντικοποίησης τερματικού.

1.2.1 Αυθεντικοποίηση CHIP (έκδοση 1)

Η αυθεντικοποίηση CHIP βασίζεται σε ένα στατικό ζευγάρι κλειδιών που υπάρχει μέσα στο κύκλωμα του διαβατηρίου. Το ιδιωτικό κλειδί είναι αποθηκευμένο σε ασφαλή χώρο προστατευμένο από ανάγνωση και εγγραφή, ενώ το δημόσιο κλειδί σε χώρο προστατευμένο από εγγραφή μόνο. Το ζευγάρι κλειδιών έχει παραχθεί και αποθηκευτεί κατά την διάρκεια της προσωποποίησης του

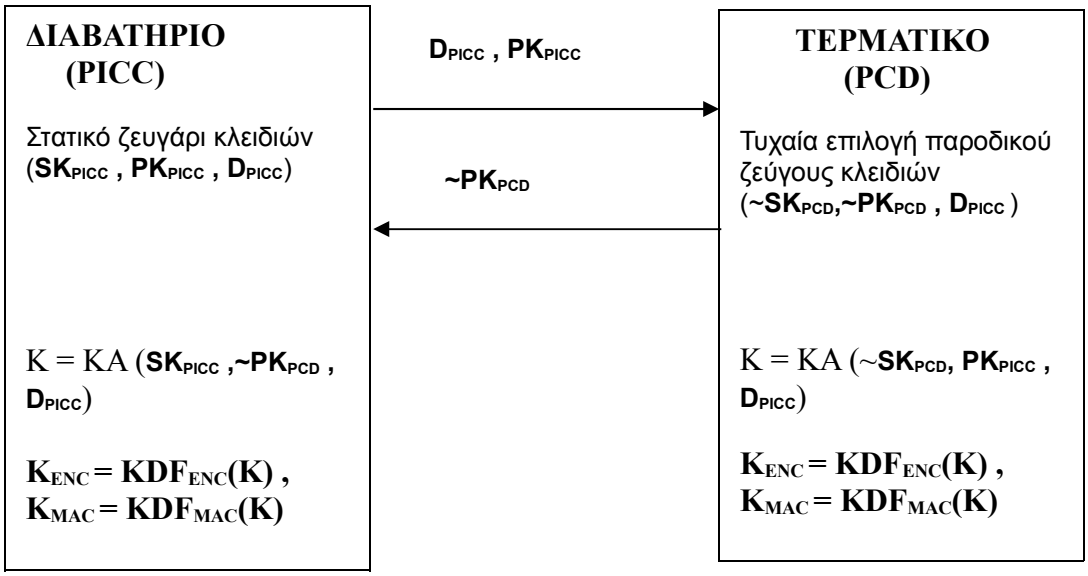
διαβατηρίου. Ουσιαστικά το ολοκληρωμένο κύκλωμα του διαβατηρίου εξασφαλίζει την αυθεντικότητα του, αποδεικνύοντας πως έχει στην κατοχή του το ιδιωτικό κλειδί.

Στην πρώτη έκδοση του πρωτοκόλλου η αυθεντικότητα του διαβατηρίου εξασφαλίζεται με έμμεσο τρόπο καθώς η πιστοποίηση της κατοχής του ιδιωτικού κλειδιού εξασφαλίζεται από την επιτυχή έκβαση της μετέπειτα επικοινωνίας, η οποία εξαρτάται από τα κλειδιά συνόδου $\mathbf{K_{ENC}}$, $\mathbf{K_{MAC}}$ που παράγονται.

Τα βήματα που εκτελούνται κατά την διάρκεια του πρωτοκόλλου είναι:

1. Το διαβατήριο στέλνει το δημόσιο κλειδί του ($\mathbf{PK_{PICC}}$) μαζί με τις δημόσιες παραμέτρους ($\mathbf{D_{PICC}}$) στο τερματικό.
2. Το τερματικό επιλέγει τυχαία ένα εφήμερο ζευγάρι κλειδιών ($\mathbf{\sim SK_{PCD}, \sim PK_{PCD}}$) και στέλνει το δημόσιο κλειδί του ($\mathbf{\sim PK_{PCD}}$) πίσω στο διαβατήριο.
3. Έπειτα από αυτήν την Diffie-Hellman ανταλλαγή των κλειδιών τα δύο μέρη υπολογίζουν το κοινό μυστικό **K .**
   ($\mathbf{K = KA(SK_{PICC}, PK_{PCD}, D_{PICC})}$ για το διαβατήριο και $\mathbf{K = KA(SK_{PCD}, PK_{PICC}, D_{PICC})}$ για το τερματικό)
4. Εξάγονται τα κλειδιά $\mathbf{K_{ENC}}$ και $\mathbf{K_{MAC}}$ και από τα δύο μέρη από τις σχέσεις:
   $\mathbf{K_{ENC} = KDF_{ENC}(K)}$, $\mathbf{K_{MAC} = KDF_{MAC}(K)}$ όπου η συνάρτηση εξαγωγής κλειδιού **KDF** είναι ουσιαστικά μία συνάρτηση κατακερματισμού.
5. Το διαβατήριο υπολογίζει επίσης την συμπιεσμένη μορφή του δημόσιου κλειδιού του τερματικού βάσει μιας συνάρτησης κατακερματισμού $\mathbf{Comp(\sim PK_{PCD})}$.
   (Η συνάρτηση **Comp** είναι ο SHA-1 αν πρόκειται για κλασική Diffie-Hellman ανταλλαγή, ενώ αν έχουμε Diffie-Hellman με χρήση ελλειπτικών καμπυλών (ECDH) είναι η χ συντεταγμένη του δημόσιου σημείου ECDH, δηλαδή ένα αλφαριθμητικό σταθερού μήκους $\log_{256}p$. Το $\mathbf{Comp(\sim PK_{PCD})}$ το αποθηκεύει προσωρινά το διαβατήριο γιατί θα το χρειαστεί αργότερα στο πρωτόκολλο αυθεντικοποίησης του τερματικού).

Το πρωτόκολλο παρουσιάζεται και σχηματικά στην παρακάτω εικόνα.



Εικόνα 7: Πρωτόκολλο αυθεντικοποίησης CHIP (Έκδοση 1)

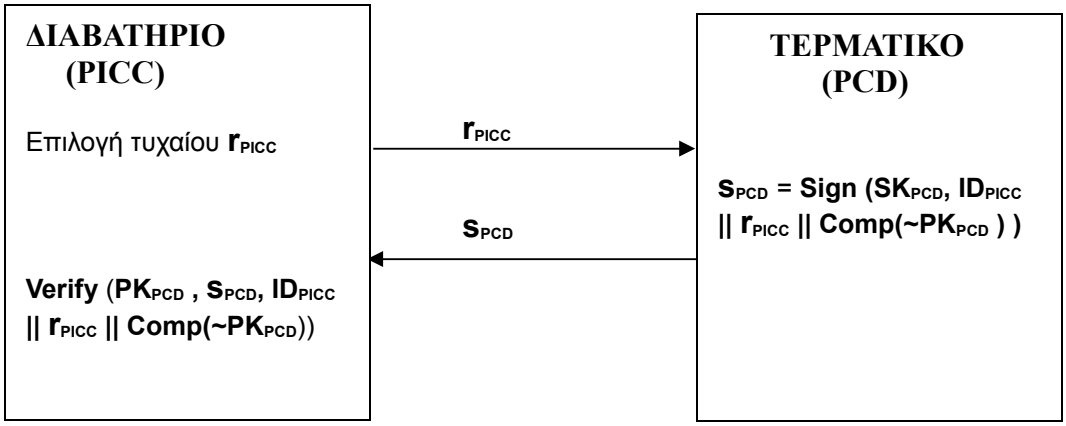
1.2.2 Αυθεντικοποίηση τερματικού (έκδοση 1)

Σκοπός της αυθεντικοποίησης τερματικού είναι να ελεγχθεί το τερματικό ως προς την εγκυρότητα και την αυθεντικότητα του και λειτουργεί ως ένας μηχανισμός ελέγχου πρόσβασης στα ευαίσθητα προσωπικά δεδομένα που είναι αποθηκευμένα στο κύκλωμα του διαβατηρίου. Για να το πετύχει αυτό χρησιμοποιεί ψηφιακά πιστοποιητικά και ένα πρωτόκολλο δύο μηνυμάτων. Αρχικά το ψηφιακό πιστοποιητικό του τερματικού μαζί με το πιστοποιητικό της οντότητας που το εξέδωσε μεταφέρονται από το τερματικό στο διαβατήριο. Το διαβατήριο κατά την φάση της προσωποποίησης έχει αποθηκευμένο το αυτό-υπογραφόμενο πιστοποιητικό της ριζικής αρχής πιστοποίησης και έτσι μπορεί να ελέγξει την εγκυρότητα των πιστοποιητικών που λαμβάνει από το τερματικό. Η υποδομή του δημοσίου κλειδιού που υποστηρίζει το πρωτόκολλο αυθεντικοποίησης τερματικού θα αναλυθεί εκτενώς στο κεφάλαιο 1.4.

Το βήματα που εκτελούνται στο πρωτόκολλο αυτό είναι τα εξής:

1. Αρχικά το διαβατήριο επιλέγει μια τυχαία τιμή $\mathbf{r_{PICC}}$ και την στέλνει στο τερματικό.
2. Το τερματικό υπογράφει τώρα την τιμή $\mathbf{ID_{PICC}} \,||\, \mathbf{r_{PICC}} \,||\, \mathbf{Comp(\sim PK_{PCD})}$.Το $\mathbf{ID_{PICC}}$ είναι το αναγνωριστικό του διαβατηρίου και στην πρώτη έκδοση του πρωτοκόλλου πρόκειται για την πληροφορία MRZ που έχει ανταλλαχθεί κατά τον βασικό έλεγχο του διαβατηρίου. Το $\mathbf{Comp(\sim PK_{PCD})}$ είναι η συμπιεσμένη μορφή του δημόσιου κλειδιού του τερματικού και έχει υπολογιστεί και μεταφερθεί και στα δύο μέρη κατά την αυθεντικοποίηση CHIP. Το τερματικό αφού υπογράψει, στέλνει την υπογραφή πίσω στο διαβατήριο.

3. Το διαβατήριο ελέγχει την υπογραφή χρησιμοποιώντας το δημόσιο κλειδί του τερματικού και ξεκλειδώνει ή όχι την πρόσβαση στα ευαίσθητα δεδομένα.



Εικόνα 8: Πρωτόκολλο Αυθεντικοποίησης Τερματικού (Έκδοση 1)

1.3 Διαδικασίες Αυθεντικοποίησης ηλεκτρονικών Διαβατηρίων τρίτης γενιάς

Το 2008 η Ομοσπονδιακή Υπηρεσία για την Ασφάλεια στην Πληροφορική της Γερμανίας (BSI) πρότεινε μια νέα στοίβα πρωτοκόλλων για τα διαβατήρια τρίτης γενιάς. Κύριος σκοπός ήταν η αντικατάσταση του βασικού ελέγχου πρόσβασης (BAC) με το πρωτόκολλο αυθεντικοποιημένης εγκατάστασης σύνδεσης με συνθηματικό (PACE).

Η αδυναμία του βασικού έλεγχου πρόσβασης έγκειται στα χαμηλής εντροπίας κλειδιά που παράγει καθώς αυτά εξάγονται από την MRZ πληροφορία του διαβατηρίου. Η MRZ πληροφορία ουσιαστικά απαρτίζεται από έναν σειριακό αριθμό 9 ψηφίων, την ημερομηνία γέννησης του κατόχου (6 ψηφία) και την ημερομηνία λήξης του διαβατηρίου (6 ψηφία) Όπως αναφέρει ο Δ. Λέκκας και ο Δ. Γκρίτζαλης στο [5] σε ένα υποθετικό σενάριο μιας χώρας 5 εκατομμυρίων κατοίκων με εκδιδόμενα διαβατήρια χρονικής διάρκειας 5 ετών για κάθε κάτοικο, η εντροπία θα μπορούσε προσεγγιστικά να υπολογιστεί ως εξής: Έχουμε 2980 διαφορετικές ημερομηνίες γέννησης με μια εκτίμηση για την ηλικία του κατόχου με απόκλιση ± 4 χρόνια και 1825 διαφορετικές ημερομηνίες λήξης για την πενταετία εγκυρότητας του διαβατηρίου. Με την υπόθεση πως ο αριθμός των εκδιδόμενων διαβατηρίων ανά ημέρα ακολουθεί ομοιόμορφη κατανομή και πως κάθε καινούργιο διαβατήριο λαμβάνει έναν αύξων σειριακό αριθμό έχουμε 2750 διαφορετικούς αριθμούς που μπορούν να συνδεθούν με μια συγκεκριμένη ημερομηνία λήξης. Λαμβάνοντας υπόψη και μια απόκλιση της τάξης του 30% η

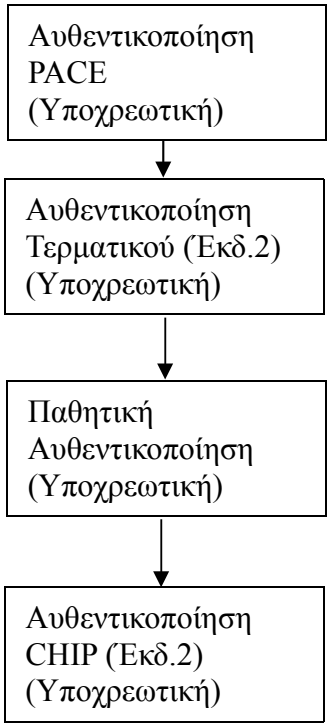
εντροπία για τον σειριακό αριθμό φτάνει τις 3540. Έτσι η συνολική εντροπία υπολογίζεται στα $2980 * 1825 * 3540 = 1.8 * 10^{10} \approx 2^{34}$ δηλαδή 34 bits.

Καθώς επίσης κάποια από τα πεδία στην MRZ μπορούν να εύκολα να προβλεφθούν κατά περίπτωση (όπως στην περίπτωση της ημερομηνίας γέννησης διπλωματικών προσώπων αφού η πληροφορία αυτή είναι δημοσίως γνωστή) η εντροπία των κλειδιών μπορεί να μειωθεί ακόμα περισσότερο. Έτσι τελικά προκύπτεί πως τα κλειδιά του βασικού έλεγχου πρόσβασης είναι αρκετά αδύναμα και θα μπορούσαν να σπάσουν με οποιοδήποτε συμβατικό σύστημα.

Ενώ τα ευαίσθητα βιομετρικά στοιχεία προστατεύονται από τον μηχανισμό της αυθεντικοποίησης του τερματικού, τα υπόλοιπα προσωπικά στοιχεία του διαβατηρίου εξαρτώνται άμεσα από το επίπεδο ασφάλειας που προσφέρει ο βασικός έλεγχος πρόσβασης. Το πρωτόκολλο PACE αναιρεί αυτόν τον κίνδυνο χρησιμοποιώντας ένα κοινό μυστικό το οποίο μοιράζονται τα δύο μέρη, το οποίο σε συνδυασμό με μια Diffie-Hellman ανταλλαγή κλειδιού παράγει κλειδιά υψηλής εντροπίας.

Επίσης οι νέες προδιαγραφές ανανεώνουν τα πρωτόκολλα CHIP και αυθεντικοποίησης τερματικού. Το πρωτόκολλο CHIP προσφέρει τώρα άμεση αυθεντικοποίηση των περιεχομένων του διαβατηρίου. Περαιτέρω τροποποιήσεις και στα δύο πρωτόκολλα αφορούν στην διατήρηση της λειτουργικότητας τους καθώς τώρα η σειρά με την οποία αυτά εκτελούνται έχει αλλάξει. Η αυθεντικοποίηση του τερματικού τώρα προηγείται της CHIP αυθεντικοποίησης.

Τα βήματα που εκτελούνται κατά την διαδικασία αυθεντικοποίησης στην τρίτη γενιά διαμορφώνεται τώρα ως εξής: Αρχικά εκτελείται ο έλεγχος PACE παράγοντας ισχυρά κλειδιά συνόδου τα οποία προστατεύουν την περαιτέρω επικοινωνία. Έπειτα εκτελείται η αυθεντικοποίηση του τερματικού για τον έλεγχο πρόσβασης στα ευαίσθητα βιομετρικά στοιχεία. Ακολουθεί η παθητική αυθεντικοποίηση και τέλος η αυθεντικοποίηση CHIP, η οποία επανεκκινεί την ασφαλή επικοινωνία δημιουργώντας νέα κλειδιά συνόδου.



Εικόνα 9: Στάδια αυθεντικοποίησης ηλεκτρονικών διαβατηρίων τρίτης γενιάς

Τα παρακάτω τρία κεφάλαια παρουσιάζουν αναλυτικά τα πρωτόκολλα της τρίτης γενιάς διαβατηρίων.

1.3.1 Πρωτόκολλο αυθεντικοποιημένης εγκατάστασης σύνδεσης με συνθηματικό (PACE)

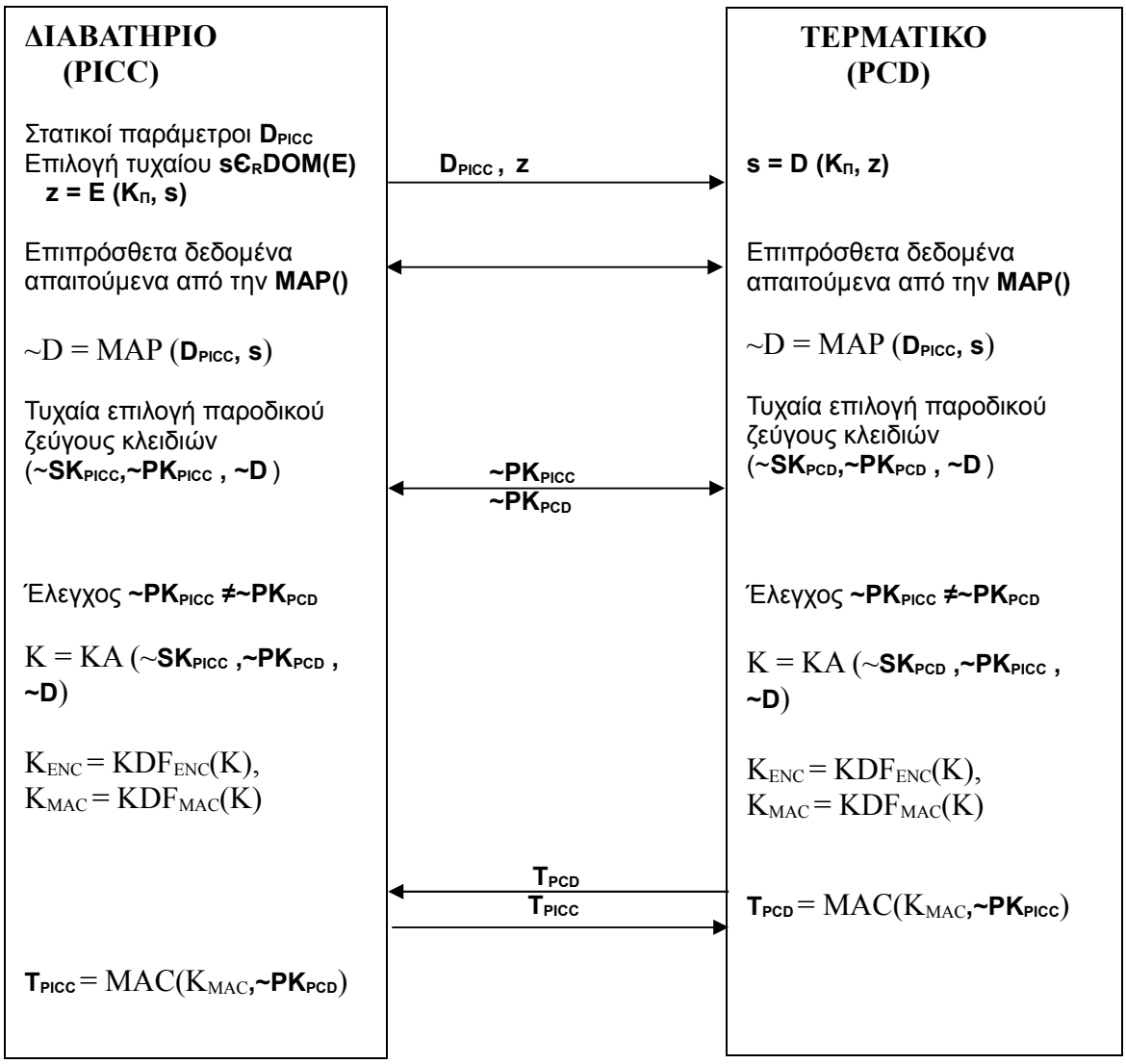
Η PACE αποτελεί μια εναλλακτική μέθοδο για τον βασικό έλεγχο πρόσβασης και ουσιαστικά αυθεντικοποιεί την σύνδεση μεταξύ διαβατηρίου και τερματικού κάνοντας χρήση ενός κοινού συνθηματικού **π**. Το συνθηματικό αυτό μπορεί να είναι η MRZ πληροφορία στην σελίδα δεδομένων του διαβατηρίου ή το CAN (αριθμός πρόσβασης της κάρτας). Το CAN μπορεί να είναι στατικό, οπότε θα βρίσκεται τυπωμένο πάνω στο διαβατήριο αλλά μπορεί να είναι και δυναμικό. Η δεύτερη περίπτωση θα υποστηρίζεται από διαβατήρια που χρησιμοποιούν χαμηλής ισχύος τεχνολογίες οθόνης, όπως η OLED ή το ηλεκτρονικό χαρτί. Σε αυτή την περίπτωση με την εκκίνηση του PACE το διαβατήριο θα επιλέγει τυχαία μια CAN τιμή και θα την προβάλει στην οθόνη. Σε όλες τις περιπτώσεις πάντως η PACE εξασφαλίζει πως το τερματικό για να συμμετέχει επιτυχώς θα πρέπει να έχει οπτική επαφή με το διαβατήριο όπως συνέβαινε και με τον βασικό έλεγχο πρόσβασης. Εδώ όμως ασχέτως από το μικρό μήκος των συνθηματικών τα κλειδιά συνόδου που παράγονται έχουν

υψηλή εντροπία.

Τα βήματα που εκτελούνται κατά την διάρκεια του PACE πρωτοκόλλου είναι τα εξής:

1. Αρχικά το διαβατήριο επιλέγει μια τυχαία τιμή **s** την οποία και κρυπτογραφεί με κλειδί το **Kπ** και την στέλνει στο τερματικό μαζί με τις δημόσιες παραμέτρους ($\mathbf{D_{PICC}}$) . Το **Kπ** προκύπτει από μια συνάρτηση εξαγωγής κλειδιού KDF έχοντας σαν είσοδο το συνθηματικό. **Kπ = KDF (π)**
2. Το τερματικό εξάγει την τιμή **s** με την βοήθεια του συνθηματικού.
3. Έπειτα διαβατήριο και τερματικό χρησιμοποιώντας μια συνάρτηση MAP και αφού έχουν ανταλλάξει επιπρόσθετα βοηθητικά δεδομένα για την λειτουργία της, παράγουν τις εφήμερες δημόσιες παραμέτρους **~D**. **(~D = MAP ($\mathbf{D_{PICC}}$, s))**. Για περισσότερες λεπτομέρειες για την MAP βλέπε παραγράφους A.3.4 ,A.3.5 από [2].
4. Το διαβατήριο και τερματικό αφού επιλέξουν τυχαία εφήμερα ζευγάρια κλειδιών (**~$\mathbf{SK_{PICC}}$**, **~$\mathbf{PK_{PICC}}$** και **~$\mathbf{SK_{PCD}}$,~$\mathbf{PK_{PCD}}$**) ανταλλάσσουν τα δημόσια κλειδιά τους.
5. Έπειτα από αυτήν την Diffie-Hellman ανταλλαγή των κλειδιών τα δύο μέρη υπολογίζουν το κοινό μυστικό **K** (αφού πρώτα ελέγξουν ότι τα δημόσια κλειδιά τους είναι διαφορετικά) (**K = KA**(**~$\mathbf{SK_{PICC}}$, ~$\mathbf{PK_{PCD}}$, ~D**) για το διαβατήριο και **K = KA**(**~$\mathbf{SK_{PCD}}$, ~$\mathbf{PK_{PICC}}$, ~D**) για το τερματικό)
6. Εξάγονται τα κλειδιά συνόδου $\mathbf{K_{ENC}}$ και $\mathbf{K_{MAC}}$ και από τα δύο μέρη από τις σχέσεις $\mathbf{K_{ENC}}$ = $\mathbf{KDF_{ENC}}$ **(K),** $\mathbf{K_{MAC}}$ = $\mathbf{KDF_{MAC}}$ **(K)** όπου η συνάρτηση εξαγωγής κλειδιού **KDF** είναι ουσιαστικά μία συνάρτηση κατακερματισμού. Για περισσότερες λεπτομέρειες για τις $\mathbf{KDF_{ENC}}$, $\mathbf{KDF_{MAC}}$ βλέπε παράγραφο A.2.3 από [2].

7. Τέλος ανταλλάσσονται και επικυρώνονται τα κουπόνια αυθεντικοποίησης $\mathbf{T_{PCD}}$,$\mathbf{T_{PICC}}$ όπου $\mathbf{T_{PCD}}$ = MAC(K_{MAC},**~$\mathbf{PK_{PICC}}$**) και $\mathbf{T_{PICC}}$ = MAC(K_{MAC},**~$\mathbf{PK_{PCD}}$**)



Εικόνα 10: Πρωτόκολλο PACE

1.3.2 Αυθεντικοποίηση τερματικού (έκδοση 2)

Στην δεύτερη έκδοση του πρωτοκόλλου το τερματικό ξεκινά την διαδικασία αφού το εφήμερο δημόσιο κλειδί του $\sim PK_{PCD}$ υπολογίζεται στο πρώτο βήμα από το τερματικό και έπειτα αποστέλλεται στο διαβατήριο.

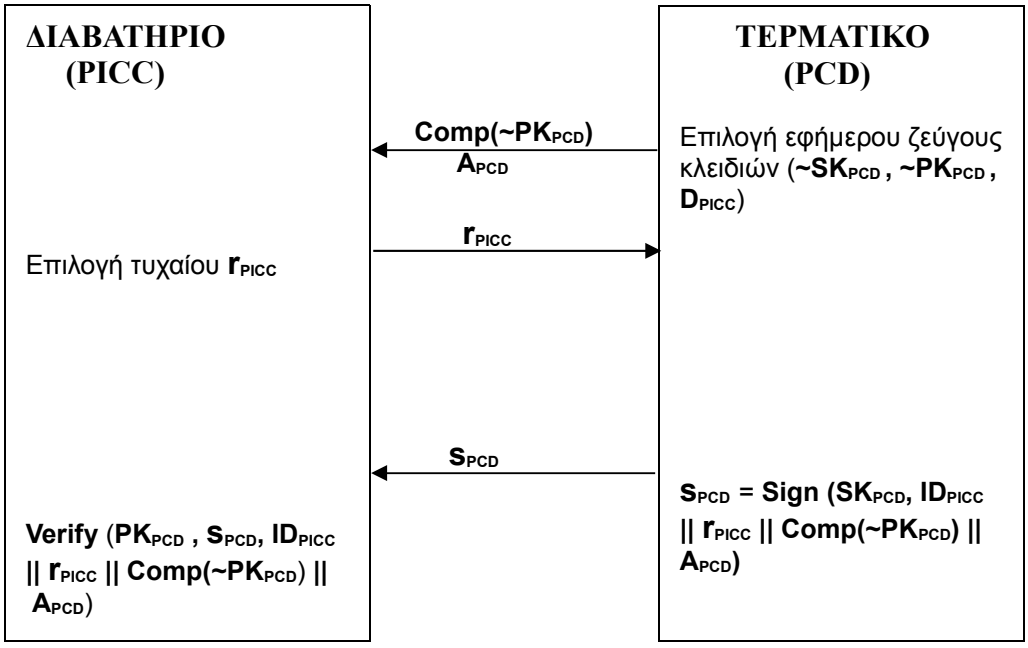
Αρχικά το ψηφιακό πιστοποιητικό του τερματικού μαζί με το πιστοποιητικό της οντότητας που το εξέδωσε μεταφέρονται από το τερματικό στο διαβατήριο. Το διαβατήριο ελέγχει την εγκυρότητα των πιστοποιητικών που λαμβάνει από το τερματικό εξάγει το στατικό δημόσιο κλειδί του τερματικού PK_{PCD} και το πρωτόκολλο ξεκινά.

Το βήματα που εκτελούνται στο πρωτόκολλο αυτό είναι τα εξής:

1. Το τερματικό επιλέγει ένα τυχαίο ζευγάρι εφήμερων κλειδιών ($\sim SK_{PCD}, \sim PK_{PCD}$) υπολογίζει

την συμπιεσμένη μορφή του δημόσιου κλειδιού του **Comp(~PK$_{PCD}$)** και την στέλνει στο διαβατήριο μαζί με κάποια βοηθητικά δεδομένα **A$_{PCD}$**. (τα βοηθητικά δεδομένα μπορεί να αποσταλούν, μπορεί και όχι και αφορούν σε υποστηρικτικά δεδομένα για κάποιες περαιτέρω λειτουργίες του τερματικού. Για περισσότερα βλέπε παράγραφο B.5 από [2].)

2. Το διαβατήριο επιλέγει μια τυχαία τιμή **r$_{PICC}$** και την στέλνει πίσω στο τερματικό.
3. Το τερματικό υπογράφει τώρα την τιμή **ID$_{PICC}$ || r$_{PICC}$ || Comp(~PK$_{PCD}$) || A$_{PCD}$** . Το **ID$_{PICC}$** είναι το αναγνωριστικό του διαβατηρίου και στην δεύτερη έκδοση του πρωτοκόλλου πρόκειται για την συμπιεσμένη μορφή του εφήμερου δημόσιου κλειδιού του διαβατηρίου **Comp(~PK$_{PICC}$)** που έχει παραχθεί και ανταλλαχθεί κατά την PACE. Το τερματικό αφού υπογράψει, στέλνει την υπογραφή πίσω στο διαβατήριο.
4. Το διαβατήριο ελέγχει την υπογραφή χρησιμοποιώντας το δημόσιο κλειδί του τερματικού και ξεκλειδώνει ή όχι την πρόσβαση στα ευαίσθητα δεδομένα.



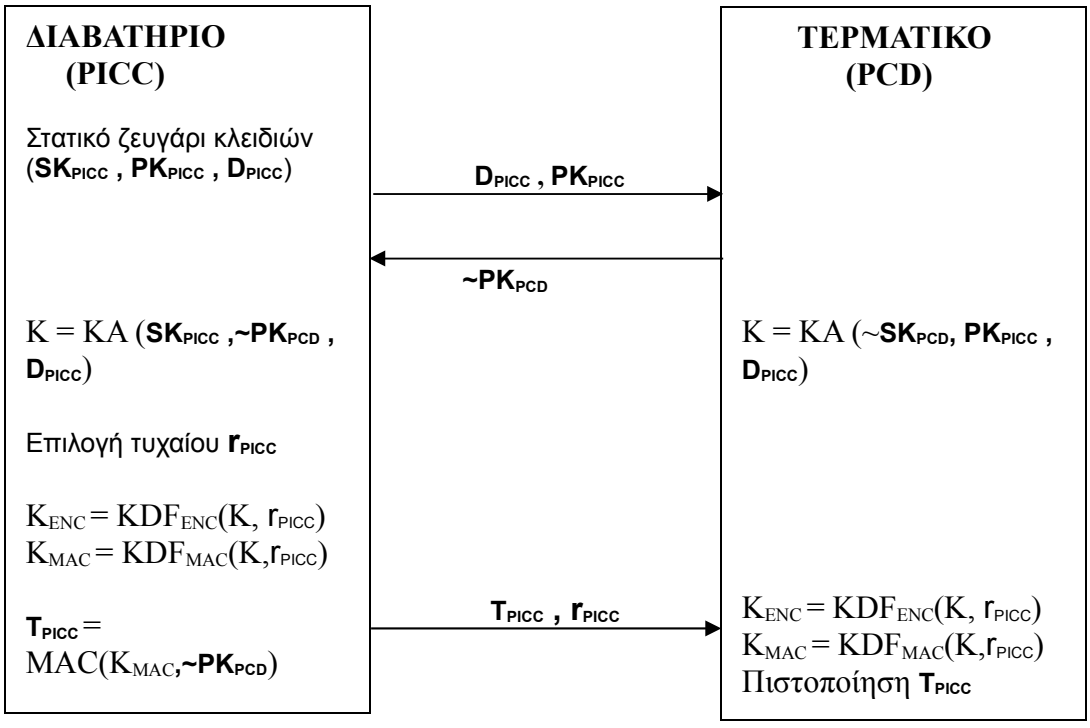
Εικόνα 11: Πρωτόκολλο Αυθεντικοποίησης Τερματικού (Έκδοση 2)

1.3.3 Αυθεντικοποίηση CHIP (έκδοση 2)

Στην δεύτερη έκδοση του πρωτοκόλλου CHIP εκτός του έμμεσου τρόπου αυθεντικοποίησης επιτυγχάνεται και άμεση αυθεντικοποίηση του διαβατηρίου με τον έλεγχο του κουπονιού αυθεντικοποίησης που αποστέλλεται στο τερματικό. Εδώ το πρωτόκολλο αυθεντικοποίησης του τερματικού θα πρέπει να έχει προηγηθεί καθώς το εφήμερο δημόσιο κλειδί **~PK$_{PCD}$** που παράγει θα χρησιμοποιηθεί στο παρόν πρωτόκολλο.

Τα βήματα που εκτελούνται κατά την διάρκεια του CHIP πρωτοκόλλου είναι τα εξής:

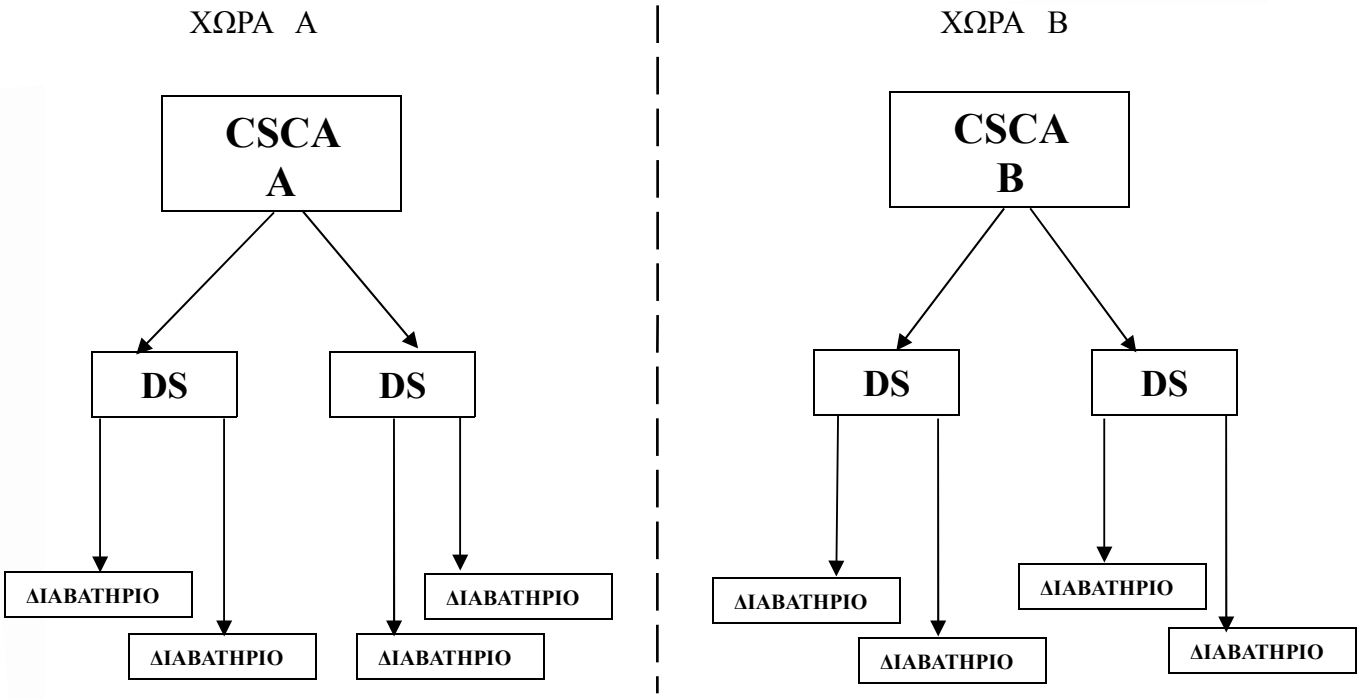
1. Το διαβατήριο στέλνει το δημόσιο κλειδί του (**PK_{PICC}**) μαζί με τις δημόσιες παραμέτρους (**D_{PICC}**) στο τερματικό.
2. Το τερματικό στέλνει το εφήμερο δημόσιο κλειδί του (**$\sim PK_{PCD}$**), το οποίο έχει υπολογιστεί κατά την διάρκεια του πρωτοκόλλου αυθεντικοποίησης τερματικού, πίσω στο διαβατήριο.
3. Το διαβατήριο υπολογίζει την συμπιεσμένη μορφή του κλειδιού του τερματικού **Comp($\sim PK_{PCD}$)** και την συγκρίνει με την τιμή που είχε λάβει από την αυθεντικοποίηση τερματικού.
4. Έπειτα από αυτήν την Diffie-Hellman ανταλλαγή των κλειδιών τα δύο μέρη υπολογίζουν το κοινό μυστικό **K .** (**$K = KA(SK_{PICC}, \sim PK_{PCD}, D_{PICC})$** για το διαβατήριο και **$K = KA(\sim SK_{PCD}, PK_{PICC}, D_{PICC})$** για το τερματικό)
5. Το διαβατήριο επιλέγει μια τυχαία τιμή **r_{PICC}** και εξάγει τα κλειδιά **K_{ENC}** και **K_{MAC}** από τις σχέσεις: **$K_{ENC} = KDF_{ENC}(K, r_{PICC})$, $K_{MAC} = KDF_{MAC}(K, r_{PICC})$**
6. Έπειτα το διαβατήριο υπολογίζει το κουπόνι αυθεντικοποίησης **T_{PICC}** του δημόσιου κλειδιού του τερματικού με την βοήθεια του κλειδιού **K_{MAC}** (**$T_{PICC} = MAC(K_{MAC}, \sim PK_{PCD})$**) και τον στέλνει στο τερματικό μαζί με την τιμή **r_{PICC}**.
7. Το τερματικό υπολογίζει τα κλειδιά συνόδου **K_{ENC}** και **K_{MAC}** από τις σχέσεις: **$K_{ENC} = KDF_{ENC}(K, r_{PICC})$, $K_{MAC} = KDF_{MAC}(K, r_{PICC})$** , ελέγχει το **$T_{PICC}$** με την βοήθεια του **$K_{MAC}$** και το διαβατήριο πιστοποιεί έτσι την αυθεντικότητα του.



Εικόνα 12: Πρωτόκολλο αυθεντικοποίησης CHIP (Έκδοση 2)

1.4 Υποδομή δημοσίου κλειδιού για τα ηλεκτρονικά διαβατήρια

Η παθητική αυθεντικοποίηση απαιτεί μια υποδομή δημοσίου κλειδιού έτσι ώστε να διασφαλιστεί ο έλεγχος της ψηφιακής υπογραφής που πιστοποιεί την αυθεντικότητα των δεδομένων που περιέχονται στην LDS δομή κάθε διαβατηρίου. Ενώ η υποδομή αυτή θα πρέπει να έχει παγκόσμια εμβέλεια δεν προτείνεται ,για λόγους εμπιστοσύνης, μια παγκόσμια ριζική αρχή πιστοποίησης η οποία θα μπορούσε να υπογράφει τα δεδομένα των διαβατηρίων όλων των χωρών. Αντί αυτής προτείνεται κάθε χώρα να υλοποιήσει την δικιά της υποδομή η οποία θα είναι εντελώς αυτόνομη και αποκλειστικά υπεύθυνη για την έκδοση των διαβατηρίων των πολιτών της. Έπειτα κάθε χώρα θα πρέπει να πρέπει να ενημερώνεται για τα δημόσια κλειδιά και τις λίστες ανάκλησης όλων των άλλων χωρών των οποίων τα διαβατήρια θα θέλει να ελέγξει και να ενημερώνει έγκαιρα τα εγχώρια τερματικά της με τις πιο πρόσφατες πληροφορίες για την επίτευξη του σωστού ελέγχου των διαβατηρίων. Η ICAO στο [1] ορίζει δύο οντότητες για τον σκοπό αυτό τις οποίες θα πρέπει να υλοποιήσει κάθε χώρα που θα θέλει να παράγει ηλεκτρονικά διαβατήρια. Την κρατική αρχή πιστοποίησης CSCA και τις αρχές έκδοσης διαβατηρίων DS. Η CSCA είναι η κεντρική οντότητα η οποία θα παράγει ζευγάρια ιδιωτικών-δημόσιων κλειδιών για κάθε αρχή έκδοσης DS. Το ιδιωτικό κλειδί θα πρέπει να φυλάσσεται με ασφάλεια εντός κάθε DS οντότητας ενώ το δημόσιο κλειδί θα έρχεται σε πιστοποιητικό (C_{DS}) υπογεγραμμένο από το ιδιωτικό κλειδί της CSCA. Το δημόσιο κλειδί της CSCA οντότητας θα περιέχεται σε αυτό-υπογραφόμενο πιστοποιητικό (C_{CSCA}) εκδιδόμενο από την ίδια. Κάθε DS θα είναι υπεύθυνη για την υπογραφή των δεδομένων των διαβατηρίων που βρίσκονται στην επικράτεια της κατά την φάση της προσωποποίησης με βάση το ιδιωτικό κλειδί που λαμβάνει από την κεντρική CSCA. Πρόκειται δηλαδή για μια υποδομή με ιεραρχία τριών επιπέδων όπως φαίνεται και στο παρακάτω σχήμα.



Εικόνα 13: Υποδομή δημοσίου κλειδιού για την αυθεντικοποίηση των διαβατηρίων

Όπως αναφέρεται στο [1] τα πιστοποιητικά των CSCA οντοτήτων θα πρέπει να διανέμονται μεταξύ των χωρών με ασφαλή τρόπο μέσω άλλων καναλιών επικοινωνίας (διπλωματικά μέσα) και θα πρέπει κάθε χώρα να εμπιστεύεται στο CSCA πιστοποιητικό μιας άλλης μέσω διαδικασιών οι οποίες είναι έξω από τα πλαίσια των προτάσεων της ICAO. Έπειτα κάθε χώρα θα πρέπει να ενημερώσει τα τερματικά της με τα εν λόγω πιστοποιητικά ώστε να τα καταστήσουν ικανά να ελέγξουν τα διαβατήρια και ένας ασφαλής τρόπος που θα μπορούσε αυτό να επιτευχθεί είναι μέσω δια-πιστοποίησης όπως αναφέρεται στο [5]. Στο σενάριο αυτό κάθε χώρα θα πρέπει να πρέπει να εκδίδει ένα δια-πιστοποιητικό το οποίο θα περιέχει όλα τα CSCA πιστοποιητικά, υπογεγραμμένα από το ιδιωτικό κλειδί της CSCA της ίδιας της χώρας, των χωρών που είναι πλέον έμπιστες και να το διανέμει στα τερματικά της.

Για τα πιστοποιητικά C_{DS} των αρχών έκδοσης αναφέρεται πως η ICAO θα διατηρεί έναν κατάλογο δημόσιων κλειδιών (PKD) ο οποίος θα είναι προσβάσιμος από όλες της συμμετέχουσες χώρες. Η ίδια η ICAO θα πρέπει να προμηθεύεται τα C_{CSCA} πιστοποιητικά από όλες τις χώρες έτσι ώστε να ελέγχει την εισαγωγή έγκυρων C_{DS} και αυτός ο κατάλογος θα αποτελεί τον κύριο μηχανισμό διανομής των C_{DS} πιστοποιητικών σε όλες τις χώρες. Επίσης προτείνεται τα διαβατήρια τα ίδια στην περιοχή SOD να περιέχουν και το C_{DS} πιστοποιητικό βάσει του οποίου εκδόθηκαν. Τέλος στον δημόσιο κατάλογο θα περιέχεται και η λίστα ανάκλησης των C_{DS} ως όμως ενός δευτερεύον τρόπου διανομής των λιστών καθώς ο κύριος τρόπος θα είναι μέσω διπλωματικών καναλιών επικοινωνίας.

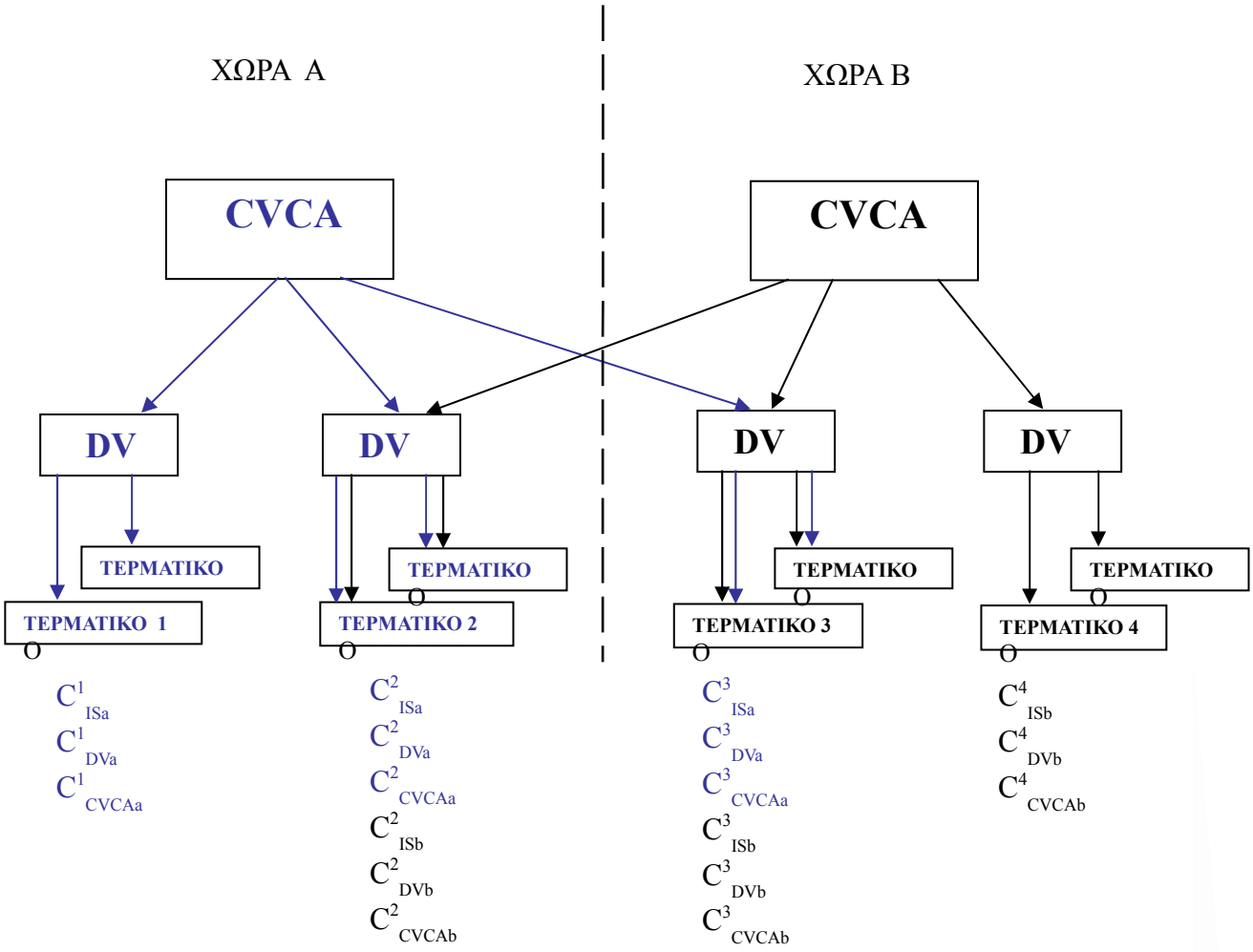
Με αυτό τον τρόπο οποιοσδήποτε έχει πρόσβαση στα δεδομένα των διαβατηρίων για να μπορεί να ελέγξει την αυθεντικότητα τους θα πρέπει πρώτα με κάποιον τρόπο να έχει αποκτήσει πρόσβαση στα C_{CSCA} πιστοποιητικά αφού αυτά δεν είναι προσβάσιμα μέσω του δημοσίου καταλόγου.

Τα πιστοποιητικά που αναφέρονται εδώ θα έρχονται με ημερομηνία λήξης. Η ICAO δίνει ως προτεινόμενη διάρκεια ζωής για τα C_{CSCA} τα 3 με 5 χρόνια ενώ για τα C_{DS} ως μέγιστη τιμή ορίζει τους 3 μήνες. Οι λίστες ανάκλησης θα πρέπει να εκδίδονται περιοδικά τουλάχιστον κάθε 90 μέρες από την κάθε χώρα με πιθανότητα έκτακτης έκδοσης όταν κάποιο περιστατικό υποκλοπής λάβει χώρα.

Με την εισαγωγή του πρωτοκόλλου αυθεντικοποίησης των τερματικών στην δεύτερη και τρίτη γενιά των διαβατηρίων δημιουργείται η ανάγκη μιας ακόμα υποδομής δημοσίου κλειδιού η οποία θα υποστηρίξει και αυτήν την διαδικασία αυθεντικοποίησης. Εδώ εισάγεται πάλι μια ιεραρχική υποδομή τριών επιπέδων. Η οντότητες που υλοποιούνται σε κάθε επίπεδο είναι οι Κρατικές Αρχές Πιστοποίησης (CVCA), οι Αρχές Πιστοποίησης Εγγράφων (DV) και τα τερματικά ανάγνωσης (IS). (Οι CVCA και οι CSCA οντότητες θα μπορούν σε κάθε χώρα να υλοποιηθούν ως μια ενιαία οντότητα CSCA/CVCA). Καταρχήν οποία χώρα θέλει να παράγει ηλεκτρονικά διαβατήρια δεύτερης και τρίτης γενιάς θα πρέπει να υλοποιήσει μια CVCA η οποία θα παράγει πιστοποιητικά για κάθε εγχώρια DV οντότητα αλλά και για κάθε αλλοδαπή DV οντότητα στις χώρες στις οποίες επιθυμεί τα διαβατήρια της να μπορούν να ελέγχονται. Οι DV οντότητες με τη σειρά τους αναλαμβάνουν να ελέγχουν μια ομάδα από εγχώρια τερματικά με το να εκδίδουν πιστοποιητικά για αυτά. Το κάθε διαβατήριο κατά την φάση της προσωποποίησης θα πρέπει να αποθηκεύει το δημόσιο κλειδί του CVCA της χώρας στην οποία ανήκει. Κατά την αυθεντικοποίηση ενός τερματικού από το διαβατήριο θα πρέπει στην αρχή του πρωτοκόλλου να διαβιβάζεται από το τερματικό προς το διαβατήριο μια αλυσίδα πιστοποιητικών η οποία θα ξεκινά από το CVCA πιστοποιητικό της χώρας που έκδωσε το διαβατήριο, το πιστοποιητικό του DV το οποίο έχει υπογράψει η CVCA της ίδιας χώρας και να καταλήγει στο πιστοποιητικό του τερματικού το οποίο έχει εκδοθεί από το αντίστοιχο DV. Το διαβατήριο έχοντας στην κατοχή του ως έμπιστο σημείο εκκίνησης το δημόσιο κλειδί του δικού του CVCA μπορεί και πιστοποιεί την εγκυρότητα των πιστοποιητικών που λαμβάνει και αυθεντικοποιεί έτσι το τερματικό. Κάθε DV οντότητα δηλαδή θα πρέπει να έχει πιστοποιηθεί από όσες χώρες θα ήθελε τα τερματικά της να μπορούν να ελέγξουν τα διαβατήρια και κάθε IS οντότητα με τη σειρά της θα πρέπει να κατέχει το ανάλογο αριθμό πιστοποιητικών εκδιδόμενων από την παραπάνω DV. Έτσι κατά τον έλεγχο των διαβατηρίων διαφορετικές αλυσίδες πιστοποιητικών διαβιβάζονται προς αυτό ανάλογα με το ποία χώρα έχει εκδώσει το συγκεκριμένο διαβατήριο.

Όλα τα παραπάνω πιστοποιητικά θα πρέπει να έχουν και αυτά μια ημερομηνία αρχής και μια ημερομηνία λήξης. Όταν περνάει η ημερομηνία λήξης τα πιστοποιητικά θα πρέπει φυσικά να ανανεώνονται. Ο τρόπος ανανέωσης των πιστοποιητικών μεταξύ των τριών παραπάνω οντοτήτων είναι θέμα της διαχείρισης πιστοποιητικών της υποδομής δημοσίου κλειδιού και δεν θα αναλυθεί στην παρούσα εργασία. Από την πλευρά των διαβατηρίων πάντως είναι θέμα της διαχείρισης να είναι πάντα ανανεωμένα τα πιστοποιητικά των DV και των τερματικών. Για τα πιστοποιητικά των κρατικών αρχών θα πρέπει να εκδίδονται από τις CVCA τα πιστοποιητικά σύνδεσης (CVCA Link Certificates) τα οποία θα μεταφέρονται κι αυτά μέσα στις αλυσίδες πιστοποιητικών προς τα διαβατήρια τα οποία αφού τα ελέγξουν με βάση το παλιό CVCA πιστοποιητικό θα πρέπει να τα αντικαθιστούν ως το νέο έμπιστο σημείο εκκίνησης. Προφανώς τα νέα πιστοποιητικά θα πρέπει να εκδίδονται πριν από την ημερομηνία λήξης των παλιών που πρόκειται να αντικαταστήσουν. Επίσης καθώς ανεβαίνουμε στην ιεραρχία της προτεινόμενης υποδομής ο χρόνος ζωής των αντίστοιχων πιστοποιητικών θα πρέπει να αυξάνει. Επειδή δεν υπάρχει κάποιος μηχανισμός ανάκλησης των πιστοποιητικών λόγω της φύσεως του συστήματος των διαβατηρίων (το διαβατήριο δεν μπορεί να έχει συνεχή πρόσβαση σε μια ενημερωμένη λίστα ανάκλησης), η έκδοση πιστοποιητικών με ημερομηνία λήξης αποτελεί μια μέθοδο περιορισμού του προβλήματος της κλοπής ιδιωτικών κλειδιών. Ρυθμίζοντας για παράδειγμα τον χρόνο ζωής των πιστοποιητικών των τερματικών όσο το δυνατόν πιο μικρό, περιορίζουμε την χρονική διάρκεια κατά την οποία ένα παραβιασμένο τερματικό μπορεί να λειτουργεί, επιβαρύνοντας όμως ταυτοχρόνως τους μηχανισμούς ανανέωσης. Μια ενδεικτική χρονική διάρκεια ζωής πιστοποιητικών είναι 1 με 30 μέρες για τα πιστοποιητικά των τερματικών, 2 εβδομάδες με 3 μήνες για αυτά των DV και 3 με 5 χρόνια για της CVCA.

Παρακάτω φαίνεται και σχηματικά η ιεραρχική δομή της υποδομής δημοσίου κλειδιού για την αυθεντικοποίηση των τερματικών.



Εικόνα 14: Υποδομή δημοσίου κλειδιού για την αυθεντικοποίηση των τερματικών στα ηλεκτρονικά διαβατήρια

Κεφάλαιο 2 Έλεγχος εγκυρότητας πιστοποιητικού τερματικού

2.1 Αδυναμία Ελέγχου

Ένα από τα κύρια προβλήματα που παραμένουν στα ηλεκτρονικά διαβατήρια τρίτης γενιάς είναι η αδυναμία του ελέγχου των πιστοποιητικών των τερματικών λόγω της έλλειψης εσωτερικού ρολογιού στα ολοκληρωμένα των διαβατηρίων. Καθώς το πιστοποιητικό του τερματικού περνάει στο διαβατήριο για να ελεγχθεί ως προς την εγκυρότητα του, ελέγχεται και η ημερομηνία λήξης του. Αφού όμως τα διαβατήρια στερούνται εσωτερικού ρολογιού ένας προσεγγιστικός έλεγχος εφαρμόζεται. Μέσα στο δεδομένα του διαβατηρίου υπάρχει ένα πεδίο για την τρέχουσα ώρα. Την

πρώτη φόρα το πεδίο αυτό ενημερώνεται κατά την φάση της προσωποποίησης. Καθώς το διαβατήριο περνάει από διαδοχικούς ελέγχους από τα τερματικά και στην περίπτωση επιτυχούς αυθεντικοποίησης το πεδίο ανανεώνει την τρέχουσα ώρα από την ημερομηνία αρχής του πιο πρόσφατου πιστοποιητικού που έχει λάβει. (συνήθως του πιστοποιητικού του ίδιου του τερματικού). Με αυτόν τον τρόπο το διαβατήριο κρατάει μια προσεγγιστική τιμή της τρέχουσας ώρας και ημερομηνίας το σφάλμα της οποίας αυξάνει ανάλογα με το χρονικό διάστημα το οποίο μεσολαβεί μεταξύ δύο διαδοχικών ελέγχων. Προκύπτει λοιπόν το πρόβλημα πως τα φυσικά πρόσωπα τα οποία δεν ταξιδεύουν συχνά να κατέχουν διαβατήρια με τρέχουσα ώρα ρυθμισμένη σε μεγάλη απόκλιση από την αληθινή, τα οποία ουσιαστικά δεν μπορούν να ελέγξουν την ημερομηνία των πιστοποιητικών των τερματικών. Αυτά τα διαβατήρια είναι αρκετά ευάλωτα σε επιθέσεις από παραβιασμένα τερματικά καθώς τους δίνουν την δυνατότητα να λειτουργούν για περισσότερο χρόνο από όσο θα όριζε το πιστοποιητικό τους.

Το πρόβλημα της σωστής ανανέωσης του χρόνου απαντάται σε όλα τα παθητικά RFID συστήματα λόγω της φύσης των συστημάτων αυτών. Τα δύο κύρια χαρακτηριστικά που καθιστούν την διαχείριση και λειτουργία των υποδομών δημοσίου κλειδιού σε αυτά ελλιπή, καθιστώντας έτσι τις τελικές συσκευές ευάλωτες σε επιθέσεις όπως η παραπάνω είναι η σποραδική συνδεσιμότητα των τελικών παθητικών συσκευών και η έλλειψη εσωτερικού ρολογιού σε αυτά.

Το πρόβλημα του εσωτερικού ρολογιού θα μπορούσε βέβαια να αντιμετωπιστεί με την υιοθέτηση ενεργών RFID κυκλωμάτων στα ηλεκτρονικά διαβατήρια τα οποία θα έχουν ενσωματωμένες μικρό-μπαταρίες δίνοντας έτσι την δυνατότητα ακριβής μέτρησης του χρόνου. Όπως αναφέρεται και στο [7] πρωτότυπα τέτοιων μπαταριών και μετρητών είναι ήδη έτοιμα προς ολοκλήρωση σε συστήματα ασύρματων έξυπνων καρτών. Παρόλα αυτά η διάρκεια ζωής σύμφωνα πάντα με το [7] (έτος έκδοσης 2010) παραμένει χαμηλή περίπου στα 3 χρόνια καθιστώντας την εφαρμογή τους προβληματική για διαβατήρια με επιθυμητή διάρκεια ζωής τα 10 χρόνια. Ακόμα κι αν η τεχνολογία επεκτείνει την διάρκεια στα επιθυμητά επίπεδα το κόστος μπορεί να αποτελέσει επίσης έναν ανασταλτικό παράγοντα εφαρμογής μιας τέτοιας λύσης. Στο παρακάτω κεφάλαιο αλλά και στην υπόλοιπη εργασία θα παρουσιαστούν και θα αναλυθούν προτάσεις σε μια προσπάθεια επίλυσης αυτού του προβλήματος θεωρώντας πως τα διαβατήρια θα συνεχίσουν να αποτελούν παθητικά κυκλώματα χωρίς καμία δυνατότητα εσωτερικής γνώσης της τρέχουσας ώρας.

2.2 Προτεινόμενες Λύσεις

Στην βιβλιογραφία αναφέρονται αρκετές προτάσεις εξάλειψης της παραπάνω αδυναμίας, χωρίς όμως καμία να δίνει οριστική λύση αφού όλες λίγο πολύ αφήνουν αναπάντητα ερωτήματα τα οποία και μένει να διερευνηθούν. Στα παρακάτω κεφάλαια παρουσιάζονται και σχολιάζονται πέντε

προτάσεις που επιχειρούν να δώσουν λύση στο πρόβλημα κάθε μία από μια διαφορετική οπτική γωνία. Η πρώτη χρησιμοποιεί εξυπηρετητές χρόνου η οποίες και αναλαμβάνουν να ενημερώσουν τα διαβατήρια με αξιόπιστο τρόπο. Η δεύτερη δίνει την δυνατότητα στον κάτοχο του διαβατηρίου να συμμετάσχει ενεργά στην διαδικασία αυθεντικοποίησης. Η τρίτη αφορά σε δύο νέα πρωτόκολλα τα οποία απαιτούν την συμμετοχή των DV οντοτήτων. Η τέταρτη προτείνει κρυπτογραφία βασισμένη σε ταυτότητες αντί της υποδομής δημοσίου κλειδιού και η τελευταία παρουσιάζει μια εναλλακτική του βασικού έλεγχου πρόσβασης και του πρωτοκόλλου αυθεντικοποίησης του τερματικού.

2.2.1 Εξυπηρετητές Χρόνου

Στο [7] οι Markus Ullmann και Matthias Vögeler προτείνουν δύο πρωτόκολλα ενημέρωσης χρόνου μεταξύ μιας ασύρματης έξυπνης κάρτας όπως είναι το διαβατήριο και ενός έμπιστου εξυπηρετητή χρόνου δίνοντας μια λύση στο πρόβλημα ανανέωσης της τρέχουσας ώρας του διαβατηρίου. Και στα δύο πρωτόκολλα το τερματικό ανάγνωσης απλά παίζει τον ρόλο του αναμεταδότη μεταξύ των εμπλεκομένων. Ο εξυπηρετητής χρόνου (TS) αναφέρεται ως έμπιστος καθώς κατέχει ένα ζευγάρι στατικών κλειδιών με το αντίστοιχο πιστοποιητικό υπογεγραμμένο από την CVCA. Το πιστοποιητικό αυτό μεταφέρεται στο διαβατήριο στην αρχή και των δύο πρωτοκόλλων. Επίσης και οι δύο περιπτώσεις βασίζονται σε κρυπτογραφία ελλειπτικών καμπυλών.

Το πρώτο πρωτόκολλο αναφέρεται ως πρωτόκολλο συγχρονισμού βασισμένο σε κώδικα αυθεντικοποίησης μηνυμάτων το οποίο αποτελεί μια Diffie-Hellmann ανταλλαγή για την δημιουργία ενός εφήμερου μυστικού σημείου K μιας ελλειπτικής καμπύλης παρέχοντας τελικά έμμεση αυθεντικοποίηση του TS. Η σφραγίδα του χρόνου μεταφέρεται χρησιμοποιώντας κώδικα αυθεντικοποίησης μηνύματος από τον TS στο διαβατήριο με κλειδιά που έχουν εξαχθεί από το κοινό μυστικό K. Πριν ξεκινήσει το πρωτόκολλο και τα δύο μέρη πρέπει να έχουν συμφωνήσει σε μια ελλειπτική καμπύλη E και σε ένα σημείο βάσης G.

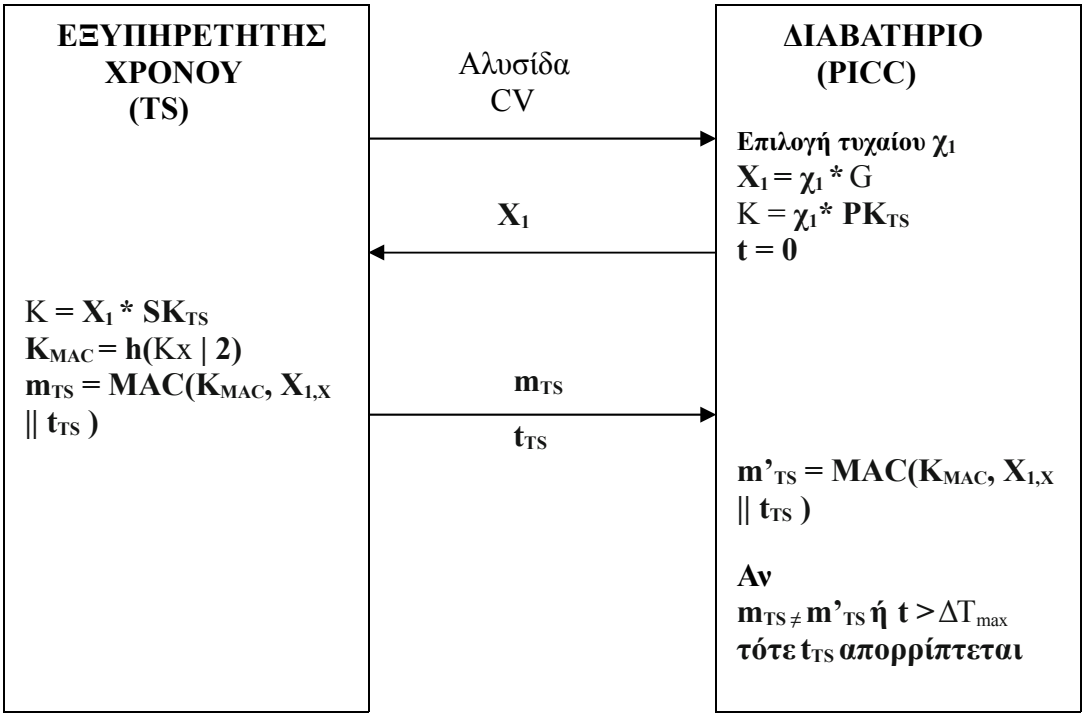
Έπειτα τα βήματα που ακολουθούνται είναι τα εξής:

1. Αρχικά το διαβατήριο επιλέγει τυχαία μία τιμή χ_1 **(** $\chi_1 \epsilon Z_n^*$**)** και παράγει ένα τυχαίο σημείο $\mathbf{X_1}$ της καμπύλης E έτσι ώστε $\mathbf{X_1 = \chi_1 *}$ G και υπολογίζει το κοινό μυστικό $K = \chi_1 * \mathbf{PK_{TS}}$ όπου $\mathbf{PK_{TS}}$ είναι το δημόσιο κλειδί του TS. Έπειτα ξεκινά έναν μετρητή **t** και στέλνει την τιμή $\mathbf{X_1}$ στον TS.
2. Ο TS υπολογίζει το K χρησιμοποιώντας το ιδιωτικό του κλειδί $\mathbf{SK_{TS}}$ από τη σχέση $K = \mathbf{X_1 * SK_{TS}}$ και αφού εξάγει το κλειδί αυθεντικοποίησης $\mathbf{K_{MAC}}$ $\mathbf{(K_{MAC} = h(Kx \mid 2))}$ υπολογίζει το $\mathbf{m_{TS}}$ από την σχέση $\mathbf{m_{TS} = MAC(K_{MAC}, X_{1,X} \| t_{TS})}$ όπου $\mathbf{t_{TS}}$ είναι η τρέχουσα ώρα του TS. Έπειτα στέλνει το $\mathbf{m_{TS}}$ και $\mathbf{t_{TS}}$ στο διαβατήριο.

3. Το διαβατήριο υπολογίζει την τιμή $\mathbf{MAC(K_{MAC}, X_{1,X} \| t_{TS})}$ και αν συμφωνεί με την ληφθείσα τιμή $\mathbf{m_{TS}}$ ενημερώνει την τρέχουσα του ώρα βάσει του $\mathbf{t_{TS}}$

Στο τρίτο βήμα ένας επιπρόσθετος έλεγχος λαμβάνει χώρα. Το διαβατήριο διατηρεί μέσα του μια τιμή ΔT_{max} . Αν ο μετρητής που ξεκίνησε μετά τους υπολογισμούς στο πρώτο βήμα ξεπεράσει το ΔT_{max} τότε το διαβατήριο απορρίπτει το $\mathbf{t_{TS}}$ που του έστειλε ο TS. Αυτό εξασφαλίζει πως η νέα ώρα που λαμβάνει από τον TS δεν θα έχει απόκλιση μεγαλύτερη από κάποιο προκαθορισμένο όριο απόκλισης καθώς από τον χρόνο που η οντότητα χρονοσήμανσης παίρνει ένα στιγμιότυπο της ώρας και μέχρι να κάνει τους απαραίτητους υπολογισμούς και το στιγμιότυπο να μεταφερθεί στο διαβατήριο και να πραγματοποιηθούν οι ανάλογοι υπολογισμοί από την πλευρά του διαβατηρίου περνάει ένα χρονικό διάστημα. Το χρονικό διάστημα αυτό αποτελεί μια αναπόφευκτη απόκλιση του $\mathbf{t_{TS}}$ από την πραγματική ώρα.

Το πρωτόκολλο παρουσιάζεται και σχηματικά παρακάτω. Στο σχήμα το τερματικό ανάγνωσης το οποίο και λειτουργεί ως απλός αναμεταδότης των μηνυμάτων έχει παραλειφθεί.



Εικόνα 15: Πρωτόκολλο συγχρονισμού βασισμένο σε κώδικα αυθεντικοποίησης μηνυμάτων

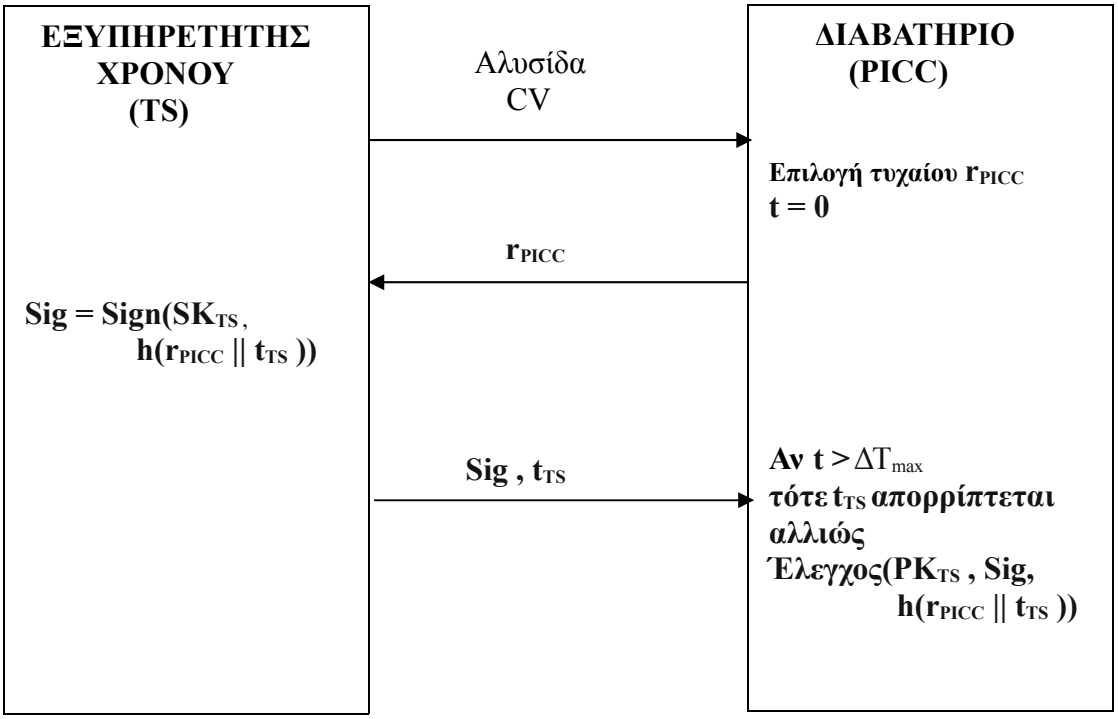
Το δεύτερο πρωτόκολλο είναι ένα πρωτόκολλο πρόκλησης-απάντησης δύο βημάτων το οποίο βασίζεται στις ψηφιακές υπογραφές και προσφέρει άμεση αυθεντικοποίηση της οντότητας χρονοσήμανσης. Εδώ ο TS ουσιαστικά λειτουργεί ως μια έμπιστη οντότητα χρονοσήμανσης που αντί να για κάποιο ψηφιακό έγγραφο βάζει την σφραγίδα του χρόνου σε μια τυχαία πρόκληση από το διαβατήριο.

Και εδώ διαβατήριο και TS θα πρέπει εκ των προτέρων να έχουν συμφωνήσει για την επιλογή της ελλειπτικής καμπύλης E και του βασικού σημείου G.

Τα βήματα κατά την διάρκεια εκτέλεσης του είναι τα εξής:

1. Αρχικά το διαβατήριο επιλέγει μια τυχαία τιμή $\mathbf{r_{PICC}}$ και αφού ξεκινήσει τον μετρητή **t** στέλνει την τιμή αυτή στον TS.
2. Ο TS αφού συνενώσει την τρέχουσα ώρα $\mathbf{t_{TS}}$ και την τυχαία τιμή $\mathbf{r_{PICC}}$ και περάσει την παραγόμενη τιμή από μια συνάρτηση κατακερματισμού, υπογράφει το αποτέλεσμα χρησιμοποιώντας τον αλγόριθμο DSA ελλειπτικών καμπυλών (ECDSA) και το ιδιωτικό του κλειδί $\mathbf{SK_{TS}}$. Έπειτα στέλνει πίσω στο διαβατήριο την ώρα $\mathbf{t_{TS}}$ μαζί με την ψηφιακή του υπογραφή.
3. Το διαβατήριο ελέγχει την υπογραφή του TS βάσει του δημόσιου κλειδιού του $\mathbf{PK_{TS}}$ και εφόσον ο μετρητής δεν έχει ξεπεράσει το ΔT_{max}, αποδέχεται την καινούργια ώρα.

Τα παραπάνω βήματα δίνονται και σχηματικά στο παρακάτω σχήμα.



Εικόνα 16: Πρωτόκολλο συγχρονισμού βασισμένο σε υπογραφές

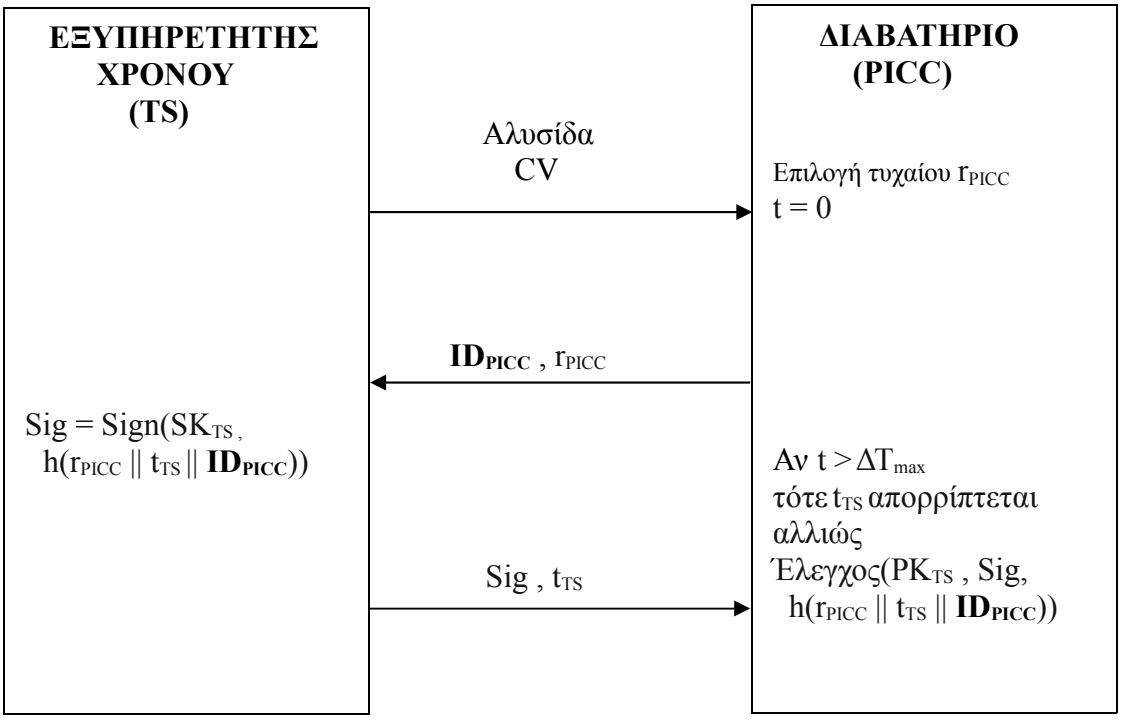
Παρατηρήσεις

Οι προτάσεις των Ullmann και Vögeler αφήνουν κάποια ανοιχτά θέματα τα οποία και χρήζουν περαιτέρω διερεύνησης ώστε η εμπλοκή των εξυπηρετητών χρόνου να θεωρηθεί ως ολοκληρωμένη λύση στο πρόβλημα του ελέγχου των πιστοποιητικών των τερματικών ανάγνωσης από τα ηλεκτρονικά διαβατήρια.

Καταρχήν προκύπτει το θέμα της διαχείρισης των πιστοποιητικών των TS. Δεν αναφέρεται πουθενά στην εργασία τους ποιος θα παράγει τα πιστοποιητικά των αυτών των οντοτήτων εκτός από το γεγονός πως το αναγκαίο ριζικό πιστοποιητικό για τον έλεγχο της CV αλυσίδας που θα μεταφέρεται στο διαβατήριο θα είναι το αυτό-υπογραφόμενο της CVCA οντότητας. Πιθανόν το έργο αυτό να πρέπει να το επωμιστούν οι DV οντότητες. Έπειτα δεν αναφέρεται αν θα υπάρχει μέθοδος ανάκλησης τέτοιων πιστοποιητικών αν αυτά υποκλαπούν και επίσης αν τα πιστοποιητικά αυτά θα περιέχουν με τη σειρά τους ημερομηνία αρχής και λήξης. Στην περίπτωση που θα έρχονται με ημερομηνία λήξης τότε πάλι τα διαβατήρια δεν έχουν κάποιον αξιόπιστο τρόπο να ελέγξουν αν τα πιστοποιητικά έχουν λήξει ή όχι αφού ακόμα δεν έχουν λάβει καμία ενημέρωση για την τρέχουσα ώρα. Το αρχικό πρόβλημα δηλαδή ουσιαστικά μετατίθεται από πρόβλημα ελέγχου των τερματικών σε πρόβλημα ελέγχου των οντοτήτων χρονοσήμανσης. Σίγουρα βέβαια η προσπάθεια μιας επίθεσης για να υποκλαπούν ιδιωτικά δεδομένα που περιέχονται στα διαβατήρια δυσχεραίνει καθώς τώρα θα πρέπει να αφορά σε συνδυασμένη παραβίαση και του τερματικού ανάγνωσης και της οντότητας χρονοσήμανσης, δεν παύει όμως να υφίσταται ακόμα ως απειλή.

Όσον αφορά τα προτεινόμενα πρωτόκολλα μια μικρή βελτίωση θα μπορούσε να υλοποιηθεί στο πρωτόκολλο συγχρονισμού βασισμένου σε ψηφιακές υπογραφές. Μία από τις απαιτήσεις ασφάλειας που υποτίθεται πως καλύπτει το εν λόγω πρωτόκολλο είναι η ανθεκτικότητα σε επιθέσεις πολλαπλής αποστολής (replay attacks). Παρόλα αυτά ένας επιτιθέμενος θα μπορούσε ακούγοντας το κανάλι επικοινωνίας μεταξύ διαβατηρίων και TS να μαζεύει ζευγάρια **(r_{PICC}, Sig)** και καθώς η συλλογή του θα αυξάνει μαζί θα αυξάνεται και η πιθανότητα κάποια στιγμή να ανιχνεύσει μία τιμή r_{PICC} την οποία έχει ήδη αποθηκεύσει. (Μια τέτοια συλλογή θα μπορούσε να αποκτηθεί ακόμα και με πλημμύρισμα του TS με τυχαίες τιμές από τον επιτιθέμενο). Τότε θα μπορούσε να παρέμβει στο κανάλι και να αποστείλει στο συγκεκριμένο διαβατήριο την αντίστοιχη υπογραφή **Sig** δίνοντας έτσι στο διαβατήριο μια παρελθούσα τιμή της τρέχουσας ώρας. Η υψηλή εντροπία του r_{PICC} υποτίθεται πως προστατεύει από ένα τέτοιο ενδεχόμενο άλλα μια μικρή τροποποίηση στο πρωτόκολλο θα μπορούσε να μειώσει δραματικά την πιθανότητα εμφάνισης του. Το κάθε διαβατήριο θα μπορούσε να στέλνει στο πρώτο βήμα του πρωτοκόλλου μαζί με το r_{PICC} και ένα αναγνωριστικό του διαβατηρίου ID_{PICC} . Η τιμή αυτή θα συνενώνεται μαζί με το r_{PICC} και το t_{TS}, πριν αυτά περάσουν στην συνάρτηση κατακερματισμού από την πλευρά του TS, παίρνοντας έτσι μέρος στην δημιουργία της υπογραφής. Το αναγνωριστικό ID_{PICC} θα μπορούσε να αποτελείται από τον αριθμό CAN του διαβατηρίου ή και την MRZ πληροφορία. Με αυτό τον τρόπο ο επιτιθέμενος μειώνει δραστικά την πιθανότητα που είχε να βρει ήδη αποθηκευμένο r_{PICC} και να εκτελέσει επιτυχώς την επίθεση καθώς τώρα η τυχαία τιμή r_{PICC} θα πρέπει να ανιχνευτεί δεύτερη φορά από το ίδιο διαβατήριο. Η εν λόγω τροποποίηση ουσιαστικά ενισχύει πρωτόκολλο αυτό έναντι στις επιθέσεις πολλαπλής αποστολής.

Η παρακάτω τροποποίηση φαίνεται και σχηματικά παρακάτω:



Εικόνα 17: Τροποποιημένο πρωτόκολλο συγχρονισμού βασισμένο σε υπογραφές

Τέλος σε καμία από τις παραπάνω δύο προτάσεις δεν διευκρινίζεται ο τρόπος τον οποίο χρησιμοποιεί ο TS για να μάθει την τρέχουσα ώρα. Μια αξιόπιστη πηγή χρόνου θα πρέπει να χρησιμοποιηθεί είτε με την μορφή ατομικού ρολογιού στο εσωτερικό του εξυπηρετητή είτε με χρήση του GPS πρωτοκόλλου είτε και μέσω αίτησης σε κάποιον NTP εξυπηρετητή. Η χρήση πάντως του τελευταίου αδημονεί κάποιους κινδύνους καθώς το πρωτόκολλο NTP δεν παρέχει μηχανισμούς ασφάλειας που να αποδεικνύουν πως η πηγή του χρόνου που χρησιμοποιήθηκε είναι αξιόπιστη.

2.2.2 Χειροκίνητος έλεγχος ημερομηνίας

Στο [6] οι Rishab Nithyanand et al προτείνουν μια λύση στο πρόβλημα δίνοντας στον κάτοχο του διαβατηρίου έναν ενεργό ρόλο κατά την διαδικασία ελέγχου. Η πρόταση τους περιλαμβάνει αλλαγές στην κατασκευή των διαβατηρίων τα οποία τώρα θα πρέπει να περιλαμβάνουν χαμηλής

ισχύος τεχνολογίες οθόνης, όπως η OLED ή το ηλεκτρονικό χαρτί, ικανές να παρουσιάσουν μια ημερομηνία έξι ψηφίων. Κατά την διαδικασία ελέγχου του πιστοποιητικού του τερματικού η ημερομηνία λήξης του θα παρουσιάζεται στην οθόνη του διαβατηρίου και ο κάτοχος του διαβατηρίου θα είναι αυτός που θα αποφασίζει αν θα δεχτεί την ημερομηνία ως έγκυρη ή όχι. Για να μπορέσει ο χρήστης να επέμβει στην διαδικασία ένα επιπλέον στοιχείο θα πρέπει να προστεθεί στο ηλεκτρονικό διαβατήριο έτσι ώστε αυτό να δέχεται την εντολή αποδοχής ή απόρριψης από αυτόν. Η κύρια πρόταση είναι πάλι κατασκευαστική με την εισαγωγή ενός κουμπιού πάνω στο διαβατήριο. Μια RFID ετικέτα με τα παραπάνω χαρακτηριστικά φαίνεται στο παρακάτω σχήμα:

Εικόνα 18: RFID ετικέτα με τεχνολογία οθόνης και κουμπιά

Εναλλακτικά των κουμπιών θα μπορούσαν να χρησιμοποιηθούν και κλουβιά Faraday τα οποία θα έκοβαν κάθε ασύρματη επικοινωνία του διαβατηρίου με εξωτερικές συσκευές όταν θα το επικάλυπταν πράγμα που θα μπορούσε εύκολα να επιτευχθεί με το να κλείσει απλώς κάποιος το κατάλληλα εξοπλισμένο διαβατήριο. Αναφέρεται επίσης και η λύση ενός διακόπτη ο οποίος θα αποσύνδεε κατά βούληση το κύκλωμα του διαβατηρίου με την κεραία του αλλά μάλλον απορρίπτεται λόγω της ευκολίας αστοχίας ενός τέτοιου μηχανικού μέσου.

Πέρα από τον έλεγχο για πιστοποιητικά που έχουν λήξει με φυσικό τρόπο οι Rishab Nithyanand et al αναφέρουν και την δυνατότητα να ελεγχθούν πιστοποιητικά που έχουν για κάποιο λόγω ανακληθεί. Εδώ υποτίθεται πως λίστες ανάκλησης, αφού έχουν πρώτα υπογραφεί από τις οντότητες CVCA, μεταφέρονται από το τερματικό προς το διαβατήριο για τον έλεγχο των πιστοποιητικών που έχουν ακυρωθεί λόγω κλοπής ιδιωτικών κλειδιών, παραβίασης των τερματικών συσκευών αλλά και για άλλους λόγους. Ενώ πριν το διαβατήριο δεν είχε κανέναν τρόπο να επικυρώσει το πόσο πρόσφατη είναι μια λίστα ανάκλησης, τώρα με την εμπλοκή του χρήστη αυτό γίνεται δυνατόν. Οι λίστες ανάκλησης περιέχουν μια λίστα με τους σειριακούς αριθμούς των πιστοποιητικών που έχουν ανακληθεί. Επίσης περιέχουν την ημερομηνία έκδοσης της λίστας (CRL_{ISS}) και την ημερομηνία της επόμενης ανανέωσης (CRL_{EXP}) καθώς οι λίστες αυτές θα πρέπει να ανανεώνονται σε τακτά χρονικά

διαστήματα. Η ημερομηνία CRL_{EXP} είναι αυτή που μπορεί τώρα να ελεγχθεί με έγκυρο τρόπο από τον κάτοχο του διαβατηρίου. Για να επιτευχθεί η διαδικασία ελέγχου που προτείνεται εδώ θα πρέπει επίσης το διαβατήριο να είναι εφοδιασμένο με έναν μετρητή αντίστροφης μέτρησης ο οποίος χρειάζεται για να ορίσει το χρονικό διάστημα αναμονής για ενδεχόμενη απόκριση από τον χρήστη. Στα παρακάτω βήματα αναλύεται η διαδικασία ελέγχου των πιστοποιητικών των τερματικών.

1. Αρχικά το διαβατήριο λαμβάνει το πιστοποιητικό του τερματικού ανάγνωσης CV μαζί με την λίστα ανάκλησης των πιστοποιητικών CRL.
2. Αν τα CV_{EXP} και CRL_{EXP} είναι μικρότερα από την τρέχουσα ώρα του διαβατηρίου και αν η CRL_{ISS} είναι μεγαλύτερη ή ίση με την CV_{EXP} τότε το διαβατήριο σταματά την διαδικασία.
3. Το διαβατήριο ελέγχει αν ο σειριακός αριθμός του πιστοποιητικού του τερματικού περιέχεται στην λίστα ανάκλησης και αν ναι τότε σταματά την διαδικασία.
4. Το διαβατήριο ελέγχει τις υπογραφές για το CV και την CRL. Αν η επαλήθευση αποτύχει η διαδικασία σταματά.
5. Αν η CRL_{ISS} ή η CV_{ISS} (όπου CV_{ISS} είναι η ημερομηνία έκδοσης του πιστοποιητικού του τερματικού) είναι ποιο πρόσφατη από την τρέχουσα ώρα του διαβατηρίου τότε αυτή ανανεώνεται με βάση την πιο πρόσφατη από τις δύο.
6. Το διαβατήριο εμφανίζει στην οθόνη του τη μικρότερη από τις CV_{EXP} και CRL_{EXP} και ξεκινά το αντίστροφο μετρητή. (Εδώ αναφέρεται σαν επαρκής χρόνος ρύθμισης του μετρητή τα δέκα δευτερόλεπτα.)
7. Ο κάτοχος του διαβατηρίου κοιτάει την οθόνη και εδώ υπάρχουν δύο παραλλαγές:

   Παραλλαγή Α:

   Αν η ημερομηνία στην οθόνη δεν είναι στο παρελθόν, τότε ο χρήστης δεν κάνει τίποτα και όταν ο μετρητής μηδενίσει η επικοινωνία μεταξύ αναγνώστη και διαβατηρίου συνεχίζεται κανονικά.

   Αλλιώς ο χρήστης πατάει το κουμπί (όσο ο μετρητής τρέχει ακόμα) ή απλώς κλείνει το διαβατήριο και η διαδικασία σταματά.

   Παραλλαγή Β:

   Αν η ημερομηνία στην οθόνη είναι στο μέλλον, ο χρήστης επεμβαίνει με τον ίδιο τρόπο και η επικοινωνία συνεχίζεται κανονικά.

   Αλλιώς ο χρήστης δεν κάνει τίποτα και όταν ο μετρητής μηδενίσει η διαδικασία σταματά από το διαβατήριο αυτή τη φορά.

Η παραλλαγή η οποία και τελικά προτείνεται είναι η δεύτερη καθώς για να συνεχιστεί η διαδικασία απαιτείται η άμεση ενέργεια του χρήστη, ενώ η απραξία του για οποιοδήποτε λόγο θεωρείται ως μη αποδοχή της ημερομηνίας.

Οι Nithyanand et al σε μια προσπάθεια εκτίμησης του ποσοστού του ανθρώπινου λάθους που εμπεριέχει η διαδικασία που προτείνουν, εκτέλεσαν πείραμα χρησιμοποιώντας 25 υποκείμενα. Οι ηλικίες των υποκειμένων κυμάνθηκαν από 18 ως 30 για το 68% και πάνω από 30 για το υπόλοιπο 32%. Το 80% επίσης κατείχε πανεπιστημιακή μόρφωση μιας και το πείραμα τους εκτελέστηκε σε πανεπιστημιακό χώρο. Τα υποκείμενα καλέστηκαν να συμμετέχουν στην διαδικασία αποδοχής ή απόρριψης ημερομηνιών σε σύστημα που προσομοίαζε το σύστημα διαβατηρίων και τερματικών ανάγνωσης με σκοπό να γίνει μια πρώτη εκτίμηση του κατά πόσο οι κάτοχοι των διαβατηρίων είναι ενήμεροι και μπορούν να κάνουν σωστό έλεγχο για την τρέχουσα ημερομηνία. Οι ημερομηνίες που εξετάστηκαν ήταν με +/- 1 , -3 , +7 , -29 και με -364 μέρες απόκλιση από την πραγματική, οι οποίες παρουσιάζονταν με τυχαίο τρόπο στα υποκείμενα. Τα αποτελέσματα τους παρουσιάζουν αρκετό ενδιαφέρων. Για λανθασμένες εκτιμήσεις όσον αφορά στην απόρριψη έγκυρης ημερομηνίας (false negatives) τα ποσοστά λάθους ήταν αρκετά χαμηλά με το υψηλότερο να φτάνει το 4%. Για λανθασμένες εκτιμήσεις όσον αφορά στην αποδοχή μη έγκυρης ημερομηνίας τα ποσοστό λάθους ήταν επίσης πολύ μικρά εκτός από την περίπτωση που η απόκλιση ήταν -365 μέρες όπου έφτασε το 40%. Αυτό δείχνει πως τα υποκείμενα ενώ ήταν αρκετά ικανά στην σωστή εκτίμηση της μέρας και του μήνα ,παρουσίαζαν χαμηλή ικανότητα σωστής εκτίμησης της χρονιάς.

Αξίζει επίσης να αναφερθεί πως στην συγκεκριμένη πρόταση παρουσιάζεται και μια μέθοδος βελτίωσης του προβλήματος χωρητικότητας που παρουσιάζουν οι λίστες ανάκλησης όταν ο αριθμός των πιστοποιητικών που έχουν ανακληθεί αυξάνει. Ενώ στις παραδοσιακές λίστες το μέγεθος της λίστας αυξάνει ανάλογα με τον αριθμό των πιστοποιητικών εδώ προτείνεται μια δομή λίστας με σταθερό μέγεθος. Η λίστα θα πρέπει να περιέχει τα ανακληθέντα πιστοποιητικά με αύξουσα σειρά βάσει του σειριακού τους αριθμού. Έπειτα η Αρχή η οποία θα υπογράφει την λίστα θα πρέπει να υπογράφει την κάθε εγγραφή στη λίστα ξεχωριστά με τέτοιο τρόπο ώστε η υπογραφή να συνδέει τον ένα σειριακό αριθμό με τον προηγούμενο. Έτσι η υπογραφή για την i εγγραφή στην λίστα παρουσιάζεται ως εξής:

$$\mathbf{Sign(i) = Sign(h(CRL_{ISS} \,||\, SN_i \,||\, SN_{i-1}))}$$

όπου $\mathbf{SN_i}$ είναι ο σειριακός αριθμός του πιστοποιητικού στην i εγγραφή.

Όταν το τερματικό στέλνει το πιστοποιητικό του στο διαβατήριο θα στέλνει μαζί και τις τιμές $\mathbf{Sign(i)}$, $\mathbf{CRL_{ISS}}$, $\mathbf{SN_i}$, $\mathbf{SN_{i-1}}$ έτσι ώστε ο δικός του σειριακός αριθμός να βρίσκεται μεταξύ των τιμών $\mathbf{SN_i}$ και $\mathbf{SN_{i-1}}$. Αντί δηλαδή να στείλει όλη την λίστα ανάκλησης στέλνει μόνο μια συγκεκριμένη εγγραφή της. Το διαβατήριο από την μεριά του αν επαληθεύσει την υπογραφή της εγγραφής της τροποποιημένης αυτής λίστας με επιτυχή τρόπο αυτό θα σημαίνει πως το πιστοποιητικό του τερματικού δεν μπορεί να βρίσκεται μέσα στην λίστα.

Παρατηρήσεις

Η πρόταση του χειροκίνητου ελέγχου είναι μια εφικτή λύση στο πρόβλημα που δημιουργεί η ελλιπή γνώση της τρέχουσας ώρας στα ηλεκτρονικά διαβατήρια. Η προτεινόμενη τεχνολογία είναι έτοιμη και το κόστος δεν είναι απαγορευτικό. Όπως αναφέρεται και στο [6] το σημερινό κόστος (έτος δημοσίευσης της εργασίας το 2010) μιας RFID ετικέτας με τεχνολογίες οθόνης ηλεκτρονικού χαρτιού (ePaper) ενσωματωμένες και με δυνατότητα υποστήριξης υποδομής δημοσίου κλειδιού είναι γύρω στα 17 € σε ποσότητες των 100.000, με το κόστος να μειώνεται όσο η ποσότητα μεγαλώνει.

Παρόλα αυτά η εμπλοκή του ανθρώπινου παράγοντα αποτελεί ένα ισχυρό μειονέκτημα. Όπως και η ίδια η εργασία υποδεικνύει η μέθοδος είναι επιρρεπείς σε λάθη, το ποσοστό των οποίων για να εκτιμηθεί καλύτερα θα πρέπει να γίνουν περισσότερα και πιο εκτεταμένα πειράματα. Άλλωστε το δείγμα που αναφέρθηκε δεν μπορεί σε καμία περίπτωση να θεωρηθεί αντιπροσωπευτικό λόγω μικρού του μεγέθους αλλά και λόγω του υψηλού μορφωτικού επιπέδου των συμμετεχόντων. Σε κάθε περίπτωση σε μια πραγματική εφαρμογή όπως στα διαβατήρια τα αποτελέσματα μπορούν κάλλιστα να διαφέρουν σε σχέση με καλά οργανωμένα πειράματα. Επίσης δεν είναι και τόσο σίγουρο, αν και υποστηρίζεται στην εν λόγω εργασία μέσω των απαντήσεων των υποκειμένων που έλαβαν μέρος στα πειράματα αλλά και μέσω έρευνας μέσω του Διαδικτύου, πως μια τέτοια προσέγγιση θα γινόταν εύκολα αποδεκτή από το σύνολο των κατόχων διαβατηρίων χωρίς να προκαλέσει κάποιου είδους δυσαρέσκεια. Ανεξαρτήτως πάντως μιας ευρείας αποδοχής ή μη, το απρόβλεπτο της ανθρώπινης συμπεριφοράς και ο υποκειμενικός της χαρακτήρας την καθιστούν ακατάλληλη για να αποτελέσει ενεργό μέλος στις διαδικασίες ασφάλειας οποιουδήποτε συστήματος και κανονικά τέτοιου είδους λύσεις θα πρέπει να αποφεύγονται.

2.2.3 Ασφαλές πρωτόκολλο απευθείας σύνδεσης για ηλεκτρονικά διαβατήρια (OSEP)

Στο πρωτόκολλο OSEP οι DV οντότητες παίζουν ενεργό ρόλο στην αυθεντικοποίηση των τερματικών. Ονομάζεται πρωτόκολλο απευθείας σύνδεσης καθώς για την ομαλή του λειτουργία απαιτείται μια συνεχή συνδεσιμότητα μεταξύ τερματικών και DV. Εδώ η βασική ιδέα είναι πως τον ρόλο του ελέγχου της εγκυρότητας του πιστοποιητικού των τερματικών τον παίζει η οντότητα DV της χώρας που εξέδωσε το διαβατήριο. Έτσι το διαβατήριο απαλλάσσεται από το έργο του ελέγχου αυτού, τον οποίο δεν μπορεί ούτως ή άλλως να φέρει σε πέρας με αξιοπιστία καθώς στερείται εσωτερικού ρολογιού. Δύο εκδοχές έχουν βρεθεί για το πρωτόκολλο OSEP, η πρώτη στο [8] είναι και αυτή που συνέλαβε την ιδέα ενώ η δεύτερη στο [9] ουσιαστικά αποτελεί μια τροποποίηση της

πρώτης.

Στο [8] αν και η πρόταση των Vijayakrishnan Pasupathinathan et al αφορά στην αντικατάσταση όλων των πρωτοκόλλων της δεύτερης γενιάς ηλεκτρονικών διαβατηρίων, με τη λύση που παρουσιάζουν εξαλείφεται το πρόβλημα του έλεγχου των πιστοποιητικών των τερματικών από τα διαβατήρια, πρόβλημα το οποίο συνεχίζει να υφίσταται και στην τρίτη γενιά. Το πρωτόκολλο περιέχει δύο φάσεις: Την φάση της αυθεντικοποίησης του τερματικού και την φάση της αυθεντικοποίησης του διαβατηρίου. Προϋπόθεση για την εκτέλεση του πρωτοκόλλου είναι πως το στατικό δημόσιο κλειδί των διαβατηρίων καθώς και οι στατικές δημόσιες παράμετροι που θα χρησιμοποιηθούν να είναι πιστοποιημένα από τις αντίστοιχες οντότητες DV των χωρών που εξέδωσαν τα διαβατήρια ($CERT_{DV}(PK_{PICC})$, $CERT_{DV}(D_{PICC})$). Αν και δεν αναφέρεται κάπου στην πρόταση τους, αν υποθέσουμε πως οι οντότητες DV και DS είναι υλοποιημένες μαζί και πως ουσιαστικά αποτελούν μια ενιαία οντότητα τότε η πιστοποίηση αυτή μπορεί να γίνει κατά την φάση της προσωποποίησης των διαβατηρίων. Παρακάτω παρουσιάζονται αναλυτικά τα βήματα και των δύο φάσεων του πρωτοκόλλου.

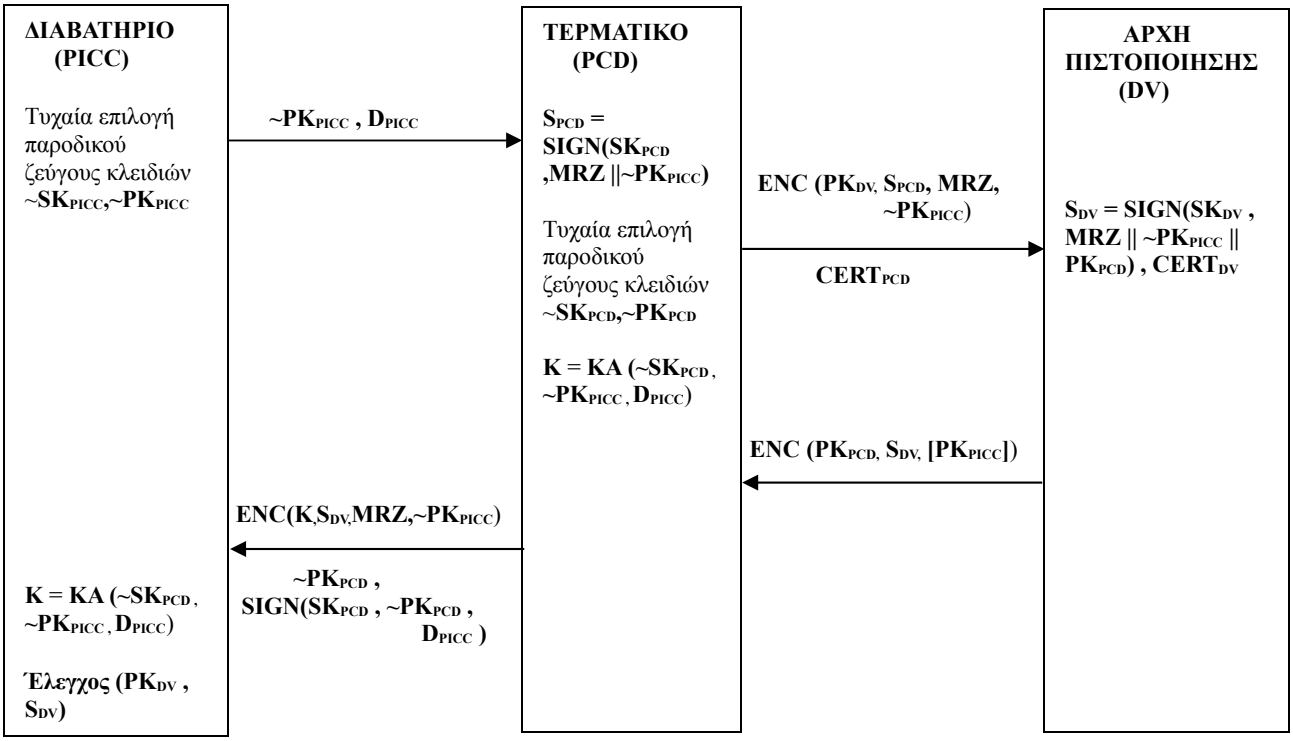
Πρώτη Φάση: Αυθεντικοποίηση του τερματικού

1. Αρχικά η πληροφορία MRZ διαβάζεται με οπτική ανάγνωση από το τερματικό και το πρωτόκολλο ξεκίνα από το τερματικό με την εντολή GET CHALLENGE προς το διαβατήριο
2. Το διαβατήριο παράγει ένα ζευγάρι εφήμερων κλειδιών (**$\sim SK_{PICC}$, $\sim PK_{PICC}$**) και στέλνει στο τερματικό του δημόσιο εφήμερο κλειδί του μαζί με τις δημόσιες παραμέτρους του **D_{PICC}**
3. Το τερματικό παράγει επίσης ένα ζευγάρι εφήμερων κλειδιών (**$\sim SK_{PCD}$, $\sim PK_{PCD}$**) και έπειτα υπογράφει με το στατικό ιδιωτικό του κλειδί **SK_{PCD}** την συνένωση των MRZ με το **$\sim PK_{PICC}$** παράγοντας την υπογραφή **S_{PCD} ($S_{PCD} = SIGN(SK_{PCD}$,MRZ || $\sim PK_{PICC})$)**. Έπειτα βρίσκει τον πλησιέστερο DV της χώρας που εξέδωσε το διαβατήριο του στέλνει την εξής πληροφορία: **S_{PCD}** , **$\sim PK_{PICC}$** , **MRZ** και το πιστοποιητικό του **$CERT_{PCD}$** αφού όμως τα τρία πρώτα τα έχει κρυπτογραφήσει με το δημόσιο κλειδί του **DV (PK_{DV})**
4. Ο DV αποκρυπτογραφεί τα **S_{PCD}** , **$\sim PK_{PICC}$** και **MRZ** με το ιδιωτικό του κλειδί **SK_{DV}** και αφού ελέγξει το πιστοποιητικό του τερματικού, δημιουργεί ένα υπογεγραμμένο μήνυμα για να πιστοποιήσει στο διαβατήριο την αυθεντικότητα του τερματικού. Το μήνυμα που υπογράφεται αποτελείται από την συνένωση των **MRZ , $\sim PK_{PICC}$** και του δημόσιου κλειδιού του τερματικού **PK_{PCD}**. Έπειτα στέλνει πίσω στο τερματικό την υπογραφή αυτή **S_{DV}** μαζί με το πιστοποιητικό του **$CERT_{DV}$** αφού πρώτα τα κρυπτογραφήσει με το ιδιωτικό κλειδί του τερματικού **SK_{PCD}** . Σε αυτό το σημείο αναφέρεται πως ο **DV** θα μπορούσε να

στείλει επιπλέον και μέσα στο κρυπτογραφημένο μήνυμα προς το τερματικό και το δημόσιο κλειδί του διαβατηρίου $\mathbf{PK_{PICC}}$ το οποίο και θα χρησιμοποιήσει στην δεύτερη φάση όταν θα αυθεντικοποιείται το διαβατήριο.

5. Το τερματικό αφού αποκρυπτογραφήσει το εισερχόμενο μήνυμα υπολογίζει το κοινό μυστικό **K** από το πρώτο μέρος της Diffie-Hellman ανταλλαγής που έγινε στο βήμα 2 ($\mathbf{K = KA\ (\sim SK_{PCD}\ ,\ \sim PK_{PICC}\ ,\ D_{PICC})}$) το οποίο θα χρησιμοποιηθεί από δω και πέρα ως το κλειδί συνόδου για την περαιτέρω επικοινωνία μεταξύ τερματικού και διαβατηρίου. Έπειτα στέλνει κρυπτογραφημένα με βάση το **K** τα $\mathbf{S_{DV}}$, **MRZ** και $\mathbf{\sim PK_{PICC}}$ μαζί με το $\mathbf{\sim PK_{PCD}}$ το οποίο και υπογράφει μαζί με τις δημόσιες παραμέτρους $\mathbf{D_{PICC}}$ με το στατικό του ιδιωτικό κλειδί $\mathbf{SK_{PCD}}$.
6. Το διαβατήριο υπολογίζει από την πλευρά του το κοινό κλειδί συνόδου **K** ($\mathbf{K = KA\ (\sim SK_{PICC}\ ,\ \sim PK_{PCD}\ ,\ D_{PICC})}$) με την βοήθεια του $\mathbf{\sim PK_{PCD}}$ και με αυτό αποκρυπτογραφεί τα $\mathbf{S_{DV}}$, **MRZ** και $\mathbf{\sim PK_{PICC}}$. Έπειτα ελέγχει την υπογραφή $\mathbf{S_{DV}}$ από που και λαμβάνει το $\mathbf{PK_{PCD}}$ με το οποίο ελέγχει την γνησιότητα του $\mathbf{\sim PK_{PCD}}$. Αν όλοι οι παραπάνω έλεγχοι περάσουν επιτυχώς το διαβατήριο αυθεντικοποιεί το τερματικό.

Παρακάτω φαίνεται και σχηματικά η πρώτη φάση του πρωτοκόλλου OSEP.

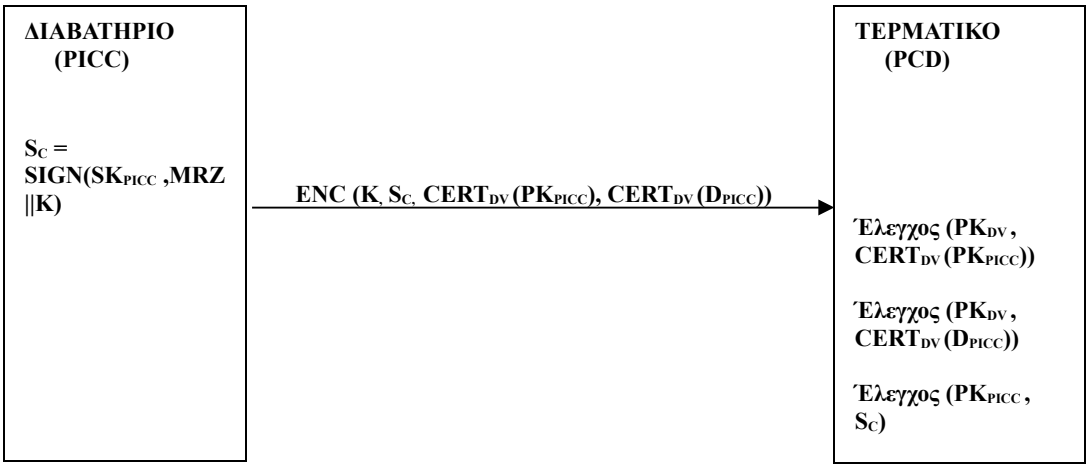


Εικόνα 19: Η αυθεντικοποίηση τερματικού στο Πρωτόκολλο OSEP

Δεύτερη Φάση: Αυθεντικοποίηση του διαβατηρίου

1. Το τερματικό ξεκινά την διαδικασία στέλνοντας στο διαβατήριο την εντολή INTERNAL AUTHENTICATE. Το διαβατήριο απαντά ως εξής: Πρώτα υπογράφει την συνένωση της MRZ πληροφορίας με το κλειδί συνόδου **K**. Έπειτα κρυπτογραφεί την υπογραφή Sc, το πιστοποιημένο από την DV οντότητα δημόσιο κλειδί του $CERT_{DV}(PK_{PICC})$ και το πιστοποιητικό των δημοσίων παραμέτρων του $CERT_{DV}(D_{PICC})$ χρησιμοποιώντας το κλειδί K και τα στέλνει πίσω στο τερματικό.
2. Το τερματικό αποκρυπτογραφεί το εισερχόμενο μήνυμα με το κλειδί συνόδου **K** και πιστοποιεί την υπογραφή Sc. Ελέγχει επίσης και τα δυο πιστοποιητικά και αν όλοι οι έλεγχοι περάσουν επιτυχώς το διαβατήριο αυθεντικοποιείται στο τερματικό.

Παρακάτω φαίνεται και σχηματικά η δεύτερη φάση του πρωτοκόλλου OSEP.



Εικόνα 20: Η αυθεντικοποίηση διαβατηρίου στο Πρωτόκολλο OSEP

Το OSEP έρχεται να αντικαταστήσει όλη τη στοίβα πρωτοκόλλων των διαβατηρίων δεύτερης γενιάς. Οι V. Pasupathinathan et al αναφέρουν πως το εν λόγω πρωτόκολλο επιτυγχάνει όλες τις απαιτήσεις ασφάλειας που πρέπει να πληρεί ένα σύστημα ελέγχου ηλεκτρονικών διαβατηρίων. Στην ανάλυση ασφάλειας αναφέρουν πως αποδεικνύουν την αυθεντικοποίηση μεταξύ διαβατηρίων και τερματικών (βλέπε [9] θεώρημα 2). Την εμπιστευτικότητα των δεδομένων την εξασφαλίζουν τα κλειδιά συνόδου που παράγονται κατά την Diffie-Hellman ανταλλαγή που πραγματοποιείται κατά την διάρκεια της αυθεντικοποίησης του τερματικού ενώ η ακεραιότητα εξασφαλίζεται με την χρήση των ψηφιακών υπογραφών. Επίσης αναφέρουν πως απλοποιούν αρκετά το θέμα της δια-πιστοποίησης που προκύπτει στην επίσημη εκδοχή της υποδομής δημοσίου κλειδιού για τα

διαβατήρια. Οι οντότητες DV δεν χρειάζεται πλέον να είναι πιστοποιημένες από τις ριζικές αρχές πιστοποίησης CVCA όλων των συμμετεχόντων χωρών, αφού ο έλεγχος θα γίνεται από την DV της χώρας του διαβατηρίου.

Μια παραλλαγή του OSEP πρωτοκόλλου αναφέρεται στο [9] από τους Mohamed Abid και Hossam Afifi. Στην παρουσίαση του πρωτοκόλλου παραπάνω δόθηκε η γενική μορφή της Diffie-Hellman ανταλλαγής για την παραγωγή του κλειδιού συνόδου. Ο V.Pasupathinathan στην εργασία του περιέγραψε την κλασσική DH ανταλλαγή δίνοντας όλες τις λεπτομέρειες για την επιλογή των δημοσίων παραμέτρων p,q,g καθώς και τον τρόπο παραγωγής των δημοσίων κλειδιών από τα ιδιωτικά, λεπτομέρειες που έχουν παραληφθεί παραπάνω χάριν γενίκευσης. Οι Abid και Afifi προτείνουν μια παραλλαγή μετατρέποντας την κλασσική DH σε DH με χρήση ελλειπτικών καμπυλών.

Οι ελλειπτικές καμπύλες είναι αρκετά ελκυστικές στην ασύμμετρη κρυπτογραφία καθώς προσφέρουν ίδιο βαθμό ασφάλειας χρησιμοποιώντας κλειδιά μικρότερου μήκους σε σχέση με μεθόδους όπως ο RSA αλγόριθμος ή η κλασσική DH. Με αυτόν τον τρόπο οι συσκευές επεξεργασίας που συμμετέχουν σε ένα ασύμμετρο κρυπτοσύστημα αποφορτίζονται από τις δύσκολες πράξεις ως ένα βαθμό και έτσι η επιλογή των ελλειπτικών καμπυλών γενικά προτιμάται ειδικά για συστήματα με χαμηλούς πόρους όπως είναι και η περίπτωση των ηλεκτρονικών διαβατηρίων.

Εδώ η πρόταση είναι η επιλογή της ελλειπτικής καμπύλης να βασιστεί σε βιομετρικά δεδομένα πράγμα που θα βοηθήσει αργότερα και στην ταυτοποίηση του κατόχου του διαβατηρίου. Με αυτόν τον τρόπο οι δημόσιες παράμετροι συσχετίζονται με την ταυτότητα του κατόχου και έτσι εξαλείφεται εντελώς η πιθανότητα δημιουργίας κοινών κλειδιών συνόδου από διαφορετικά διαβατήρια (στην περίπτωση που είχαν επιλεγεί κοινές δημόσιες παράμετροι για όλα τα διαβατήρια). Αναλυτικά αναφέρεται πως η ελλειπτική καμπύλη E που θα χρησιμοποιηθεί θα είναι της μορφής:

$$y^2 = x^3 + Ax + B \text{ όπου } 4A^3 + 27B^2 \neq 0$$

Οι εκδότες των διαβατηρίων (τον οποίο ρόλο θα παίζουν οι DV οντότητες) κατά την φάση προσωποποίησης αφού επιλέξουν έναν πρώτο αριθμό p, ένα σημείο P της καμπύλης E και τους συντελεστές A και B τα αποθηκεύουν σε μια βάση δεδομένων μαζί με ένα αναγνωριστικό ID του διαβατηρίου και ίσως μαζί με άλλες τιμές όπως όνομα κατόχου, φύλο κτλ. Έπειτα αφού υπογράψουν τις τιμές p, P, A, B τις περνάνε μαζί με το ID στην MRZ περιοχή του διαβατηρίου. Για τον υπολογισμό των A και B χρησιμοποιείται το δακτυλικό αποτύπωμα του κατόχου. Τα σημεία του αποτυπώματος (minutiae points) χωρίζονται σε 32 ομάδες και για την κάθε μια υπολογίζονται οι

μέσες τιμές για τα x και y. Έτσι καταλήγουν 32 σημεία $P_i(xi, yi)$. Το τελικό σημείο $P_0(x_0, y_0)$ υπολογίζεται από την συνένωση των xi, yi ($x_0 = x_1 \mid x_2 \ldots. \mid x_{32}$, $y_0 = y_1 \mid y_2 \ldots \mid y_{32}$). Τέλος αφού επιλεγεί η τιμή του A υπολογίζεται το B από τη σχέση:

$$B = y_0^2 - x_0^3 - Ax_0$$

Κάθε φορά που σε κάποιο σημείου ελέγχου των διαβατηρίων από τα τερματικά η τροποποιημένη έκδοση του πρωτοκόλλου OSEP τρέχει επιτυχώς και ξεκινά η φάση της ταυτοποίησης του κατόχου του διαβατηρίου ο κάτοχος θα πρέπει να δίνει το δακτυλικό του αποτύπωμα στο τερματικό. Το τερματικό τότε θα υπολογίζει με τη βοήθεια των A και p την ελλειπτική καμπύλη E και αν βρει το ίδιο B τότε ο κάτοχος θα ταυτοποιείται επιτυχώς.

Παρακάτω δίνεται ένας συγκριτικός πίνακας με τις δημόσιες παραμέτρους και τα εφήμερα κλειδιά των διαβατηρίων και των τερματικών και για τις δύο εκδοχές του OSEP πρωτοκόλλου

	OSEP με DH	OSEP με ECDH
$\sim PK_{PICC}$	**g^c mod p**	**c * P**
$\sim SK_{PICC}$	**c$\in$R** $1 \leq c \leq q - 1$	**c**
$\sim PK_{PCD}$	**g^{is} mod p**	**is * P**
$\sim SK_{PCD}$	**is$\in$R** $1 \leq is \leq q - 1$	**is**
K	**$g^{c * is}$ mod p**	**is * c * P**
D_{PICC}	**p** - πρώτος αριθμός (≥1024 bits) **q** - πρώτος αριθμός (159-160 bits) (q | (p - 1)) **g** – γεννήτορας τάξης q ($\forall i < q, g^i \neq 1 \bmod p$)	**P** - δημόσιο σημείο καμπύλης E **p** - πρώτος αριθμός **A , B** συντελεστές καμπύλης E Καμπύλη E: $y^2 = x^3 + Ax + B$

Εικόνα 21: Συγκριτικός πίνακας δημοσίων παραμέτρων και εφήμερων κλειδιών στο OSEP

Παρατηρήσεις

Το προτεινόμενο πρωτόκολλο και στις δύο εκδοχές του ουσιαστικά μετατοπίζει το πρόβλημα της αδυναμίας ελέγχου της ημερομηνίας λήξης των πιστοποιητικών των τερματικών στο πρόβλημα του ελέγχου των πιστοποιητικών των DV οντοτήτων. Πάλι τα διαβατήρια αδυνατούν να ελέγξουν τις ημερομηνίες λήξης αλλά αυτή τη φορά πρόκειται για τις DV οντότητες οι οποίες θεωρούνται πιο κεντρικές και πιο καλά προστατευμένες από τα τερματικά τα οποία πρέπει να είναι διεσπαρμένα σε κάθε σημείο ελέγχου διαβατηρίων. Η πιθανότητα παραβιασμένης DV είναι σίγουρα κατά πολύ μικρότερη από αυτήν ενός παραβιασμένου τερματικού οπότε και η παρούσα πρόταση αποτελεί αρκετά καλή λύση στο υπό μελέτη πρόβλημα καθώς επίσης μειώνει και τον φόρτο εργασίας στα

διαβατήρια στα οποία τώρα δεν χρειάζεται να διαβιβάζονται αλυσίδες πιστοποιητικών.

Το κύριο μειονέκτημα της έγκειται στην υπόθεση της διαρκούς συνδεσιμότητας μεταξύ DV και τερματικών. Όπως αναφέρεται και στο [8] για τον έλεγχο κάθε διαβατηρίου το τερματικό θα πρέπει να επικοινωνήσει με την πλησιέστερη DV της χώρας που ανήκει το διαβατήριο και αυτή θα μπορούσε να βρίσκεται στην αντίστοιχη πρεσβεία της κάθε χώρας μέσα στην χώρα εισόδου. Η DV στην πρεσβεία θα μπορούσε να είναι προμηθευμένη σε μη πραγματικό χρόνο με τις κατάλληλες πληροφορίες για τα διαβατήρια της χώρας που αντιπροσωπεύει έτσι ώστε να μπορεί να επιτελεί το έργο που της έχει ανατεθεί και αυτό δεν φαίνεται να αποτελεί κάποιο πρόβλημα. Η συνεχής συνδεσιμότητα όμως μεταξύ των DV των πρεσβειών με τα τερματικά της χώρας εισόδου απαιτεί ίσως αναδιανομή των τερματικών ανάγνωσης μέσα στη χώρα σε σημεία που είναι δυνατή μια τέτοια σύνδεση, πράγμα που μπορεί να είναι αρκετά δύσκολο για τερματικά που λειτουργούν για παράδειγμα σε απομακρυσμένους σταθμούς διεθνών τρένων.

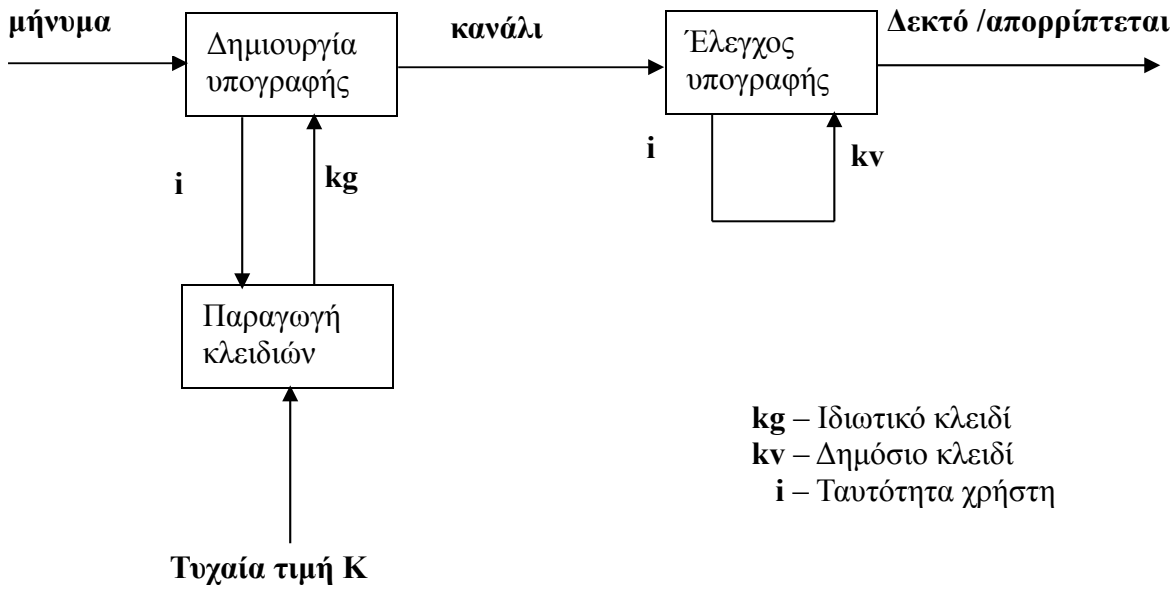
Τέλος στο θέμα της δια-πιστοποίησης πρέπει να σημειωθεί πως οι DV οντότητες που θα παίρνουν μέρος στην διαδικασία αν και θα ανήκουν στην ίδια χώρα με το υπό έλεγχο διαβατήριο θα καλούνται να ελέγξουν τερματικά άλλων χωρών τα οποία αν δεν έχουν πιστοποιητικά εκδιδόμενα από τις ίδιες τότε θα πρέπει με κάποιο τρόπο να έχουν πρόσβαση στα CVCA πιστοποιητικά όλων των χωρών.

2.2.4 Κρυπτογραφία βασισμένη σε Ταυτότητες (IBC)

Στο [10] προτείνεται μια εναλλακτική του εκτεταμένου έλεγχου πρόσβασης (της αυθεντικοποίησης του τερματικού) η οποία αντικαθιστά όλη την υποδομή δημοσίου κλειδιού με μια νέα υποδομή απαλλαγμένη από ψηφιακά πιστοποιητικά. Χωρίς χρήση πιστοποιητικών το πρόβλημα του έλεγχου εγκυρότητας τους εξαφανίζεται ενώ τα τερματικά εξακολουθούν να αυθεντικοποιούνται στα διαβατήρια πριν αυτά επιτρέψουν την πρόσβαση σε ευαίσθητα προσωπικά δεδομένα.

Η νέα υποδομή βασίζεται σε κρυπτογραφία βασισμένη σε ταυτότητες (IBC) και πρώτη φορά προτάθηκε από τον A. Shamir στο [11]. Η κύρια ιδέα της IBC είναι πως το ρόλο του δημόσιου κλειδιού δεν τον παίζει πλέον μια τυχαία επιλεγμένη τιμή ανεξάρτητη από τον κάτοχο του αλλά η ίδια η ταυτότητα του. Καθώς η ταυτότητα του κατόχου θεωρείται δημοσίως γνωστή δεν προκύπτει εδώ η ανάγκη αυθεντικοποίησης των δημοσίων κλειδιών και σύνδεσης τους με τον κάτοχο τους μέσω ενός πιστοποιητικού υπογεγραμμένου από μια τρίτη έμπιστη οντότητα. Την παραγωγή των ζευγαριών των κλειδιών την εκτελεί ένα έμπιστο κέντρο παραγωγής κλειδιών το οποίο έχοντας στην κατοχή του κάποιο μυστικό Κ μπορεί να παράγει από την ταυτότητα του χρήστη το ιδιωτικό του κλειδί και να του το παραδώσει κατά την εισαγωγή του στο σύστημα. Έπειτα το ίδιο το κέντρο δεν παίζει κανέναν ρόλο στην ασφαλή επικοινωνία μεταξύ των χρηστών και θα μπορούσε ακόμα

και να κλείσει. Στο επόμενο σχήμα φαίνεται το πλάνο ενεργειών για τις ψηφιακές υπογραφές με χρήση κρυπτογραφίας βασισμένης σε ταυτότητες όπως παρουσιάστηκε στην εργασία του Shamir.



Εικόνα 22: Πλάνο ενεργειών ψηφιακής υπογραφής με χρήση IBC

Η ασφάλεια αυτών των συστημάτων βασίζεται στο γεγονός πως μόνο το κέντρο παραγωγής κλειδιών μπορεί να παράγει τέτοια ζευγάρια έχοντας στην κατοχή του ένα μυστικό K και πως αυτό το μυστικό K φυλάσσεται από το κέντρο με ασφάλεια. Για να το πετύχει αυτό ο Shamir αναφέρει πως τέτοια συστήματα θα πρέπει να πληρούν δύο επιπλέον χαρακτηριστικά σε σχέση με τα κλασσικά συστήματα δημοσιών – ιδιωτικών κλειδιών: Πρώτων θα πρέπει με γνωστό το K να μπορεί εύκολα να υπολογιστεί ένας μεγάλος αριθμός ζευγαριών κλειδιών και δεύτερον η γνώση ενός συγκεκριμένου ζευγαριού παραγόμενου από κάποιο K δεν θα πρέπει να δίνει την δυνατότητα εξαγωγής του K.

Για να πετύχει αυτές τις συνθήκες ο Shamir στην υλοποίηση του χρησιμοποιεί μια παραλλαγή του αλγορίθμου RSA. Συγκεκριμένα ως δημόσιες παράμετροι επιλέγονται οι n, e και f όπου:

n – Το γινόμενο δύο μεγάλων πρώτων αριθμών p, q

e – Μεγάλος πρώτος σχετικά πρώτος με $\varphi(n)$ ($\varphi(n) = (p-1)(q-1)$)

f – Συνάρτηση κατακερματισμού

Το μυστικό K θεωρείται εδώ η γνώση των αριθμών p, q. Τα ζευγάρια κλειδιών παράγονται ως εξής:

i – Το δημόσιο κλειδί και ταυτόχρονα η ταυτότητα του χρήστη

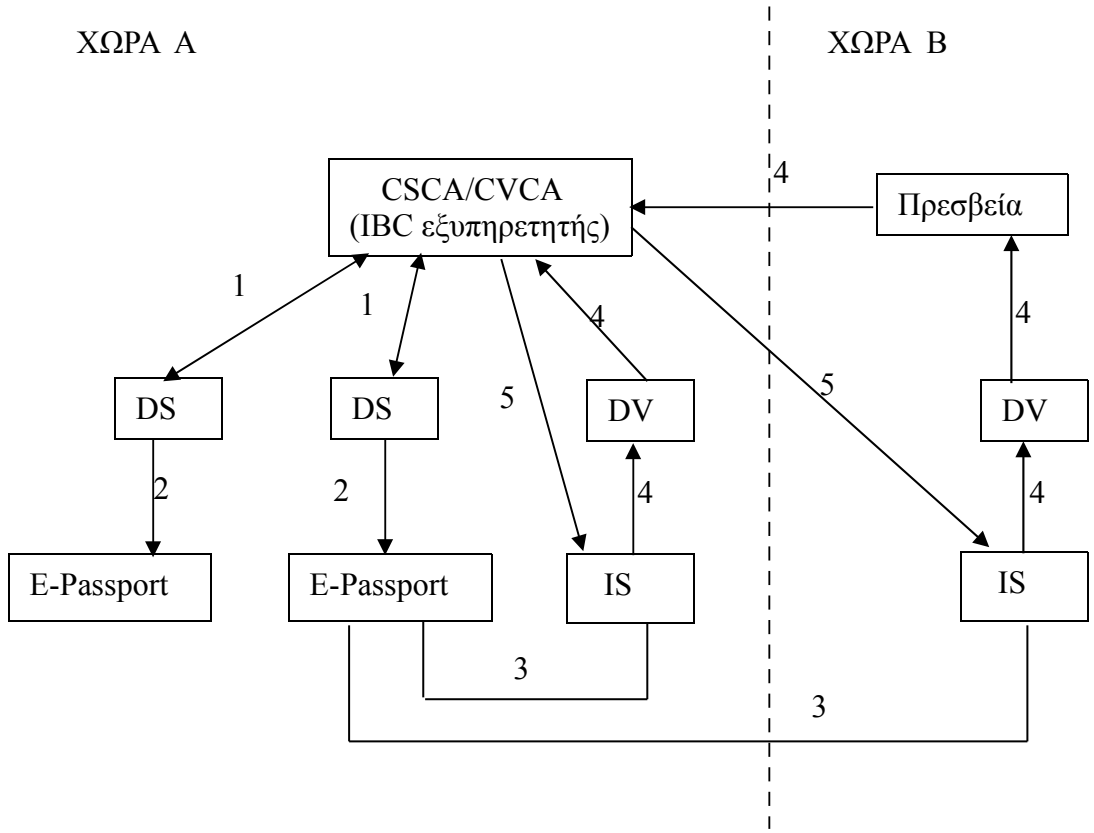
q – Το ιδιωτικό κλειδί έτσι ώστε $q^e = i \pmod n$

Το κέντρο γνωρίζοντας τα p και q μπορεί εύκολα να υπολογίσει τα ζευγάρια των ιδιωτικών και των δημόσιων κλειδιών. Ο κάθε χρήστης δεν μπορεί να υπολογίσει το K λόγω της δυσκολίας της παραγοντοποίησης μεγάλων πρώτων αριθμών ενώ τα ιδιωτικά κλειδιά προστατεύονται από το πρόβλημα υπολογισμού διακριτών λογαρίθμων. Για την παραγωγή και τον έλεγχο της υπογραφής ακολουθούνται τα εξής βήματα: Ο υπογράφων υπολογίζει για κάποιο τυχαίο r την τιμή $t = r^e \pmod n$ και την τιμή s όπου $s = q \cdot r^{f(t, m)}$ όπου m είναι το μήνυμα προς υπογραφή. Έπειτα στέλνει τα t και s μαζί με το μήνυμα m. Για τον έλεγχο της υπογραφής απλώς ελέγχεται ότι ισχύει η σχέση :
$s^e = i \cdot t^{f(t, m)}$ (συνθήκη ελέγχου υπογραφής).
Τέλος λόγω της ιδιότητας του ομομορφισμού του αλγορίθμου RSA προτείνεται η ταυτότητα i να μην εκλαμβάνεται απευθείας από το χαρακτηριστικό γνώρισμα του κατόχου (όπως είναι το όνομα, η διεύθυνση κ.α.) αλλά να περνάει πρώτα από μια συνάρτηση κατακερματισμού η έξοδος της οποίας να παράγει την πραγματική τιμή του i.
Κρυπτοσυστήματα σαν αυτό που αναλύθηκε παραπάνω έχουν το προτέρημα πως δεν χρειάζονται κανάλι επικοινωνίας για την διανομή των δημόσιων κλειδιών αλλά παρουσιάζουν το ελάττωμα πως μια κεντρική οντότητα γνωρίζει τα ιδιωτικά κλειδιά όλων των χρηστών και ως αποτέλεσμα έχουν περιορισμένες εφαρμογές.

Οι C.H. Li , X.F. Zhang, H. Jin, W. Xiang στο [10] προσαρμόζουν την παραπάνω ιδέα στα ηλεκτρονικά διαβατήρια αντικαθιστώντας το πρωτόκολλο αυθεντικοποίησης τερματικού με ένα νέο πρωτόκολλο αυθεντικοποίησης βασισμένο σε κρυπτογραφία βασισμένη σε ταυτότητες. Στην νέα υποστηρικτική υποδομή δημοσίων κλειδιών που προτείνουν η κρατική αρχή πιστοποίησης CSCA/CVCA ουσιαστικά δρα ως μια έμπιστη οντότητα παραγωγής IBC κλειδιών ενσωματώνοντας έναν IBC εξυπηρετητή. Κατά την προσωποποίηση των διαβατηρίων και έπειτα από αίτηση από τις DS οντότητες προς τον IDC εξυπηρετητή διαβιβάζονται στο διαβατήριο το ζευγάρι του ιδιωτικού και δημόσιου κλειδιού, οι δημόσιες παράμετροι και μια λίστα ανάκλησης. Το ιδιωτικό κλειδί S_{ID_ISSUER} θα αποθηκευτεί σε ασφαλές μέρος εντός του διαβατηρίου ενώ οι υπόλοιπες πληροφορίες μπορούν να αποθηκευτούν στην DG13 ομάδα δεδομένων. Το κάθε τερματικό επίσης θα πρέπει να στέλνει μια αίτηση στην CVCA της χώρας της οποίας τα διαβατήρια θα θέλει να ελέγξει με δικαίωμα εκτεταμένης πρόσβασης. Η αίτηση αυτή θα περνάει μέσω των DV οντοτήτων και στην περίπτωση που έχουμε αλλοδαπή DV τότε εμπλεκόμενη στην διαδικασία θα είναι και η ανάλογη πρεσβεία. Έπειτα η CVCA αρχή θα πρέπει να στείλει μέσω ενός καναλιού ασφαλούς επικοινωνίας το ζευγάρι των IBC κλειδιών μαζί με τις δημόσιες παραμέτρους στο τερματικό. Το ιδιωτικό κλειδί ως ευαίσθητη πληροφορία αναφέρεται πως θα αποθηκεύεται σε μια έξυπνη κάρτα σε ασφαλές σημείο η οποία θα είναι ενσωματωμένη στο τερματικό. Διαβατήρια και τερματικά θα μπορούν τώρα να τρέξουν το νέο πρωτόκολλο αυθεντικοποίησης στην μεταξύ τους

επικοινωνία και να καθορίζουν το επιτρεπόμενο είδος πρόσβασης.

Η υποδομή αυτή περιγράφεται και στο παρακάτω σχήμα:



1: Αίτηση / Εξουσιοδότηση
2: Προσωποποίηση
3: Αυθεντικοποίηση
4: Αίτηση
5: Εξουσιοδότηση

Εικόνα 23: Υποδομή EAC με χρήση IBC

Για την υλοποίηση τους οι .H. Li , X.F. Zhang, H. Jin, W. Xiang χρησιμοποίησαν ελλειπτικές καμπύλες και γεννήτριες διγραμμικών απεικονίσεων βασίζοντας έτσι την ασφάλεια του συστήματος τους στα BDH και ECDLP προβλήματα. Η παραγωγή των δημόσιων παραμέτρων από τον IBC εξυπηρετητή εκτελείται μόνο μια φορά στην αρχή λειτουργίας του και περιλαμβάνει και την επιλογή του κύριου κλειδιού **S.** Η αποκλειστική γνώση του **S** καθιστά την CVCA ως την μοναδική οντότητα που μπορεί να παράγει ζευγάρια IBC κλειδιών και έτσι το κλειδί αυτό θα πρέπει να φυλάσσεται με ασφαλή τρόπο.

Οι δημόσιες παράμετροι παρουσιάζονται στον παρακάτω πίνακα:

G_1	Κυκλική ομάδα με γεννήτορα P τάξης q (προσθετική)
G_2	Κυκλική ομάδα με γεννήτορα P τάξης q (πολλαπλασιαστική)
ê	Διγραμμική απεικόνιση ê : G_1 x $G_1 \rightarrow G_2$
P	Σημείο ελλειπτικής καμπύλης
q	Μεγάλος πρώτος αριθμός
P_{Pub}	S x P (όπου S το κύριο κλειδί SϵZ*q)
H	Συνάρτηση κατακερματισμού H:{0,1}* $\rightarrow G_1$

Εικόνα 24: Δημόσιες παράμετροι στην IBC υποδομή

Η πληροφορία που αποθηκεύεται στα τερματικά είναι η ταυτότητα (ID_IS) του τερματικού, το αναγνωριστικό (ISSUER) της χώρας που εξουσιοδοτεί το τερματικό, η ημερομηνία λήξης EXP των κλειδιών του τερματικού, οι δημόσιες παράμετροι (PAPA) και το ιδιωτικό κλειδί του τερματικού. Τα κλειδιά υπολογίζονται ως εξής:

Δημόσιο κλειδί τερματικού: $Q_{ID\_RECEIVER} = H$ (ID_Receiver)

όπου ID_Receiver = ID_IS || ISSUER || EXP

Ιδιωτικό κλειδί τερματικού: $S_{ID\_RECEIVER} = S \cdot Q_{ID\_RECEIVER}$

Η πληροφορία που αποθηκεύεται στα διαβατήρια κατά την φάση της προσωποποίησης είναι οι δημόσιες παράμετροι , το αναγνωριστικό (ID_ISSUER) της DS οντότητας που έκδωσε το διαβατήριο και η λίστα ανάκλησης η οποία έχει τη μορφή CRL = ID_IS || EXP_{NEW} όπου το EXP_{NEW} είναι η νέα ημερομηνία λήξης για τα τερματικά που θα ανακληθούν. Τα κλειδιά έχουν την εξής μορφή:

Δημόσιο κλειδί διαβατηρίου: $Q_{ID\_ISSUER} = H$ (ID_ISSUER)

Ιδιωτικό κλειδί διαβατηρίου: $S_{ID\_ISSUER} = S \cdot Q_{ID\_ISSUER}$

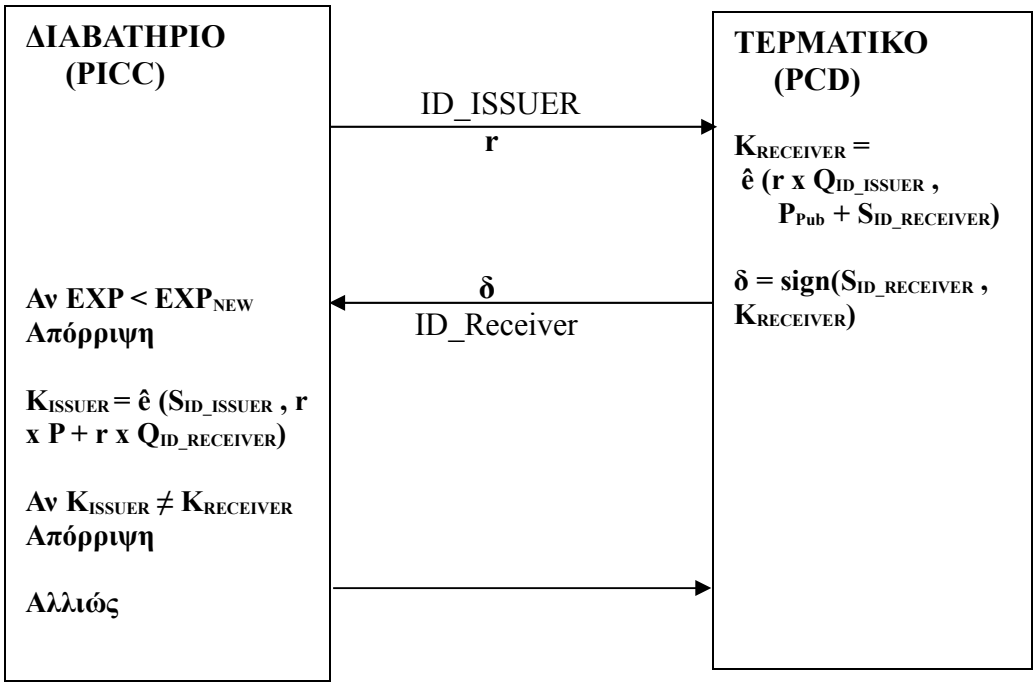
Η ημερομηνία λήξης εδώ δεν έχει το νόημα της φυσικής λήξης των κλειδιών των τερματικών αλλά έναν τρόπο να ελεγχθούν τα τερματικά που για κάποιο λόγο έχουν ανακληθεί. Σε περίπτωση ανάκλησης τα τερματικά θα πρέπει να αιτηθούν νέων κλειδιών από τις αντίστοιχες CVCA όπου και θα αποκτήσουν νέα ταυτότητα ID_Receiver = ID_IS || ISSUER || EXP_{NEW} . Κατά τη διάρκεια του πρωτοκόλλου αυθεντικοποίησης το διαβατήριο θα πρέπει να ελέγχει την ημερομηνία λήξης του τερματικού από την ταυτότητα του και αν αυτή είναι πριν την ημερομηνία που έχει στην λίστα

ανάκλησης για αυτό τότε θα πρέπει να θεωρεί πως το συγκεκριμένο τερματικό έχει ανακληθεί. Στην περίπτωση επιτυχούς αυθεντικοποίησης η λίστα ανάκλησης θα μπορεί να ενημερώνεται από το τερματικό προς το διαβατήριο.

Τα βήματα που εκτελούνται στο νέο πρωτόκολλο αυθεντικοποίησης είναι τα εξής:

1. Το διαβατήριο επιλέγει μια τυχαία τιμή **r** και την στέλνει στο τερματικό μαζί με την ταυτότητα (ID_ISSUER) της DS οντότητας που το εξέδωσε.
2. Το τερματικό υπολογίζει την τιμή $K_{RECEIVER}$ από τη σχέση: $K_{RECEIVER} = \hat{e} (r \times Q_{ID\_ISSUER} , P_{Pub} + S_{ID\_RECEIVER})$ και υπογράφει την τιμή αυτή με το ιδιωτικό του κλειδί $S_{ID\_RECEIVER}$. Έπειτα στέλνει την υπογραφή του **δ** μαζί με την τιμή ID_Receiver πίσω στο διαβατήριο.
3. Το διαβατήριο ελέγχει την τιμή EXP και αν είναι πριν την EXP_{NEW} μέσα στην λίστα ανάκλησης σταματά την διαδικασία. Στην άλλη περίπτωση υπολογίζει την τιμή K_{ISSUER} από την σχέση: $K_{ISSUER} = \hat{e} (S_{ID\_ISSUER} , r \times P + r \times Q_{ID\_RECEIVER})$. Έπειτα αποκρυπτογραφεί την υπογραφή **δ** με βάση το δημόσιο κλειδί του τερματικού $Q_{ID\_RECEIVER}$ από όπου ανακτά το $K_{RECEIVER}$ και ελέγχει αν $K_{ISSUER} = K_{RECEIVER}$. Αν ισχύει τότε ξεκλειδώνει την πρόσβαση για το τερματικό.

Το πρωτόκολλο φαίνεται και σχηματικά παρακάτω.



Εικόνα 25: Πρωτόκολλο Αυθεντικοποίησης κατά IBC - EAC

Η ισότητα $K_{ISSUER} = K_{RECEIVER}$ προκύπτει από ιδιότητα της θεωρίας ομάδων καθώς ισχύει:

$K_{RECEIVER} = \hat{e}\ (r \times Q_{ID\_ISSUER}\ ,\ P_{Pub} + S_{ID\_RECEIVER}) = \hat{e}\ (r \times Q_{ID\_ISSUER}\ ,\ S \times P + S \times Q_{ID\_RECEIVER}) =$

$\hat{e}\ (S \times Q_{ID\_ISSUER}\ ,\ r \times P + r \times Q_{ID\_RECEIVER}) = \hat{e}\ (S_{ID\_ISSUER}\ ,\ r \times P + r \times Q_{ID\_RECEIVER}) = K_{ISSUER}$

Παρατηρήσεις

Η παραπάνω πρόταση όντως αποφεύγει το πρόβλημα του ελέγχου των πιστοποιητικών των τερματικών που προκύπτει από τον προσεγγιστικό τρόπο υπολογισμού της τρέχουσας ώρας από πλευράς διαβατηρίων παρουσιάζοντας ένα νέο πρωτόκολλο αυθεντικοποίησης τερματικών μαζί με μια εναλλακτική υποδομή δημοσίου κλειδιού. Όπως αναφέρουν και οι συγγραφείς η νέα αυτή υποδομή παρουσιάζει επίσης αρκετά χαμηλότερο διαχειριστικό κόστος σε σχέση με την κλασσική και τα ίδια τα διαβατήρια μειώνουν κατά ένα μεγάλο μέρος τον επεξεργαστικό φόρτο εργασίας καθώς δεν θα χρειάζεται πλέον να ελέγχουν αλυσίδες πιστοποιητικών στην επικοινωνία τους με τα τερματικά. Παρόλα αυτά η συγκεκριμένη πρόταση παρουσιάζει αρκετά μειονεκτήματα.

Καταρχήν η ανάκληση των τερματικών η οποία εισήχθηκε για να αντιμετωπίσει την πιθανότητα της διέρευσης των ιδιωτικών κλειδιών τους δεν φαίνεται να λύνει ουσιαστικά το πρόβλημα. Όπως αναφέρεται, οι τιμές ημερομηνίας λήξης (EXP) αποτελούν πλέον μέρος της κρυπτογραφικής διαδικασίας καθιστώντας έτσι όποια προσπάθεια παραποίησης τους άμεσα αντιληπτή καθώς ο έλεγχος στο τελευταίο βήμα του πρωτοκόλλου αναπόφευκτα θα αποτύχει. Ενώ αυτός ο ισχυρισμός είναι σωστός το πρόβλημα με τις λίστες ανάκλησης βρίσκεται αλλού. Τίποτα δεν μπορεί να εξασφαλίσει πως τα διαβατήρια θα έχουν αποθηκευμένες τις πιο πρόσφατες λίστες ανάκλησης. Έτσι όταν κάποιο διαβατήριο με παλιά λίστα ανάκλησης τύχει να ελεγχθεί από κάποιο τερματικό που έχει ανακληθεί αλλά σε χρόνο από τον οποίο και πέρα ο κάτοχος του δεν έτυχε να ταξιδέψει δεν θα έχει τρόπο να καταλάβει πως το τερματικό δεν είναι έγκυρο.

Ένα επίσης πρόβλημα είναι πως η παραπάνω λύση προϋποθέτει την γνώση όλων των τερματικών ελέγχου κατά την φάση της προσωποποίησης των διαβατηρίων. Αυτό το επιβάλει η λίστα ανάκλησης που πρέπει να αποθηκευτεί στο διαβατήριο όταν αυτό εκδοθεί από της DS οντότητες η οποία έχει εγγραφές της μορφής $ID\_IS \parallel EXP_{NEW}$. Το γεγονός αυτό καθιστά το όλο σύστημα μη επεκτάσιμο καθώς για να εισαχθεί ένα νέο τερματικό ελέγχου θα πρέπει να ενημερωθούν όλα τα διαβατήρια με την καινούργια εγγραφή στην λίστα ανάκλησης τους. Το συγκεκριμένο πρόβλημα, αν και επισημαίνεται στο [10] , δεν αναλύεται επαρκώς ούτε προτείνεται κάποιος τρόπος επίλυσης του.

Τέλος δεν προβλέπεται μια πιθανή υποκλοπή στο κύριο κλειδί του IBC εξυπηρετητή. Σε αντίθεση με την κλασσική υποδομή δημόσιου κλειδιού όπου τα πιστοποιητικά των CVCA έχουν και αυτά ημερομηνία λήξης εδώ το κύριο κλειδί S και οι δημόσιες παράμετροι παραμένουν τα ίδια καθόλη

τη διάρκεια λειτουργίας του συστήματος. Σε περίπτωση υποκλοπής του S το σύστημα δεν παρουσιάζει καμία ευελιξία καθώς θα πρέπει να εκκινήσει πάλι από την αρχή με ενημέρωση των στοιχείων αυθεντικοποίησης σε όλα τα διαβατήρια και σε όλα τα τερματικά για να συνεχίσει να λειτουργεί με ασφαλή τρόπο.

2.2.5 Εξυπηρετητές κλειδιών πρόσβασης

Στο [12] οι Pablo Najera, Francisco Moyano και Javier Lopez ερευνούν τις αδυναμίες των διαβατηρίων δεύτερης γενιάς και προτείνουν μια εναλλακτική του βασικού έλεγχου πρόσβασης και της αυθεντικοποίησης τερματικού. Αν και η πρόταση τους αφορά κυρίως στην επίλυση των προβλημάτων που δημιουργούν τα στατικά και χαμηλής εντροπίας κλειδιά του BAC, πράγμα που διορθώνεται στην τρίτη γενιά με την υιοθέτηση του πρωτοκόλλου PACE, ταυτόχρονα δίνουν και λύση στο πρόβλημα του ελέγχου των πιστοποιητικών των τερματικών το οποίο παραμένει και στην τρίτη γενιά. Οι συγγραφείς αναφέρονται στην πρόταση τους σαν μια εναλλακτική γενικά για συστήματα που διαχειρίζονται ηλεκτρονικά έγγραφα υβριδικής μορφής (εννοώντας έγγραφα βασισμένα σε χαρτί αλλά και με ικανότητα διαχείρισης της ψηφιακής πληροφορίας). Τα ηλεκτρονικά διαβατήρια ανήκουν σε αυτή την κατηγορία και όπως υποστηρίζουν η πρόταση τους μπορεί να εφαρμοστεί και σε αυτά και για αυτό το λόγο παρουσιάζεται εδώ.

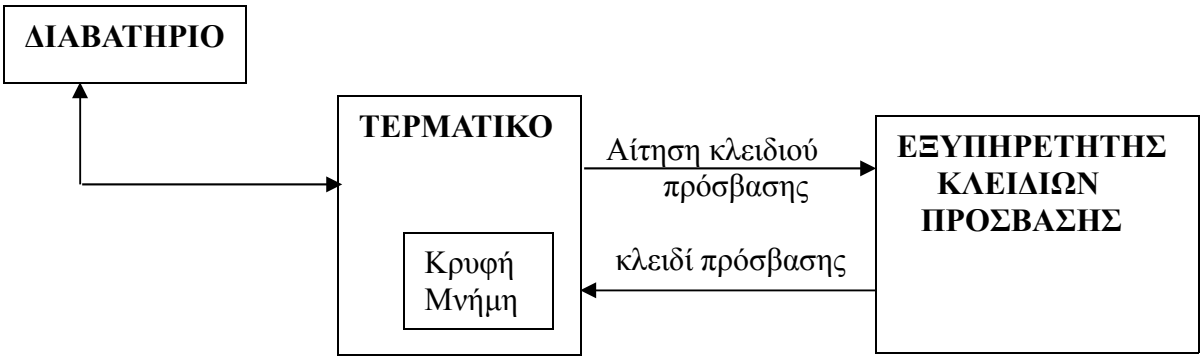
Η βασική ιδέα είναι να τροποποιηθεί ο βασικός έλεγχος πρόσβασης έτσι ώστε το K_{SEED} να μην προέρχεται από την MRZ περιοχή του διαβατηρίου αλλά από κάποια τρίτη έμπιστη οντότητα, τον εξυπηρετητή κλειδιών πρόσβασης. Όταν το διαβατήριο ελέγχεται από το τερματικό, το τερματικό θα πρέπει να επικοινωνεί με τον εξυπηρετητή από όπου θα ζητά το K_{SEED} για το συγκεκριμένο διαβατήριο. Για να μπορέσει να αποκτήσει αυτήν την πληροφορία θα πρέπει πρώτα να αυθεντικοποιηθεί στον εξυπηρετητή και με αυτόν τον τρόπο μετά την επιτυχή έκβαση του βασικού έλεγχου πρόσβασης το διαβατήριο μπορεί να γνωρίζει πως το τερματικό είναι έγκυρο και πως μπορεί να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα καθιστώντας έτσι το πρωτόκολλο αυθεντικοποίησης τερματικού μη αναγκαίο. Η αυθεντικοποίηση του τερματικού από τον εξυπηρετητή μπορεί να γίνει χωρίς κανένα πρόβλημα καθώς δεν υπάρχουν πλέον οι περιορισμοί των διαβατηρίων όπως η προσεγγιστική γνώση της τρέχουσας ώρας.

Για να το πετύχουν αυτό οι συγγραφείς προτείνουν πως από την MRZ περιοχή των διαβατηρίων δεν θα εξάγεται το ίδιο το K_{SEED} αλλά ένας δείκτης σε αυτό έτσι ώστε με μια αίτηση από το τερματικό να μπορεί να βρεθεί το αντίστοιχο K_{SEED} από την βάση δεδομένων στον εξυπηρετητή. Αρχικά το K_{SEED} το οποίο θα είναι αποθηκευμένο στο διαβατήριο και στον εξυπηρετητή θα έχει δημιουργηθεί με τυχαίο τρόπο έτσι ώστε να μην παρουσιάζει καμία σύνδεση με πληροφορίες ενδεικτικές για το διαβατήριο όπως η ημερομηνία γέννησης κτλ. Με αυτό τον τρόπο η εντροπία

μπορεί να αυξηθεί μέχρι και 128 bits. Επίσης δίνεται η δυνατότητα δυναμικών κλειδιών στον βασικό έλεγχο πρόσβασης με το να μπορεί το τερματικό να ζητήσει από τον εξυπηρετητή την δημιουργία καινούργιου K_{SEED} για έναν συγκεκριμένο δείκτη το οποίο και θα παράγεται σε πραγματικό χρόνο επίσης με τυχαίο τρόπο και θα επιστρέφεται στο τερματικό και έπειτα θα ανανεώνεται και στο διαβατήριο. Για την ανάγκη της συνεχούς σύνδεσης των τερματικών με τον εξυπηρετητή κλειδιών πρόσβασης αναφέρεται πως θα μπορούσε να υλοποιηθεί ένας αριθμός από εξυπηρετητές δίνοντας έτσι την δυνατότητα στα τερματικά να επιλέγουν αυτόν που μπορούν τη δεδομένη στιγμή να συνδεθούν. Την πληροφορία των διαθέσιμων εξυπηρετητών θα μπορούσε να την παρέχει το ίδιο το διαβατήριο στα τερματικά ή κάποια άλλη τρίτη οντότητα θα μπορούσε να παρέχει στα τερματικά την λίστα με τα κατάλληλα URLs. Επίσης μια κρυφή μνήμη θα μπορούσε να υλοποιηθεί στα τερματικά στην οποία θα αποθηκεύονται τα K_{SEED} μετά από ενημέρωση από τους εξυπηρετητές για μελλοντική χρήση με σκοπό να μειωθεί η συχνότητα επικοινωνίας με αυτούς. Έτσι τελικά τα βήματα που εκτελούνται κατά τον έλεγχο των διαβατηρίων από τα τερματικά διαμορφώνονται ως εξής:

1. Αρχικά το τερματικό διαβάζει από την MRZ περιοχή του διαβατηρίου τον δείκτη για το K_{SEED}
2. Το τερματικό ψάχνει στην κρυφή μνήμη για το αντίστοιχο $K_{SEED.}$ Αν το βρει το πρωτόκολλο του βασικού έλεγχου πρόσβασης συνεχίζεται με βάση αυτό το $K_{SEED.}$ Αν όχι τότε ψάχνει τον πρώτο διαθέσιμο εξυπηρετητή κλειδιών πρόσβασης. Όταν τον βρει αυθεντικοποιείται σε αυτόν και αφού εγκαταστήσει ένα ασφαλές κανάλι επικοινωνίας του στέλνει τον δείκτη για το $K_{SEED.}$
3. Ο εξυπηρετητής βρίσκει στην βάση του το K_{SEED} και το επιστρέφει στο τερματικό.
4. Το τερματικό αφού αποθηκεύσει το K_{SEED} στην κρυφή μνήμη του ολοκληρώνει τον βασικό έλεγχο πρόσβασης με το διαβατήριο με βάση αυτό.

Η παραγωγή καινούργιων K_{SEED} αποφασίζεται από πολιτικές ασφάλειας με τις οποίες ενημερώνονται τα τερματικά από τους εξυπηρετητές κλειδιών πρόσβασης. Στις πολιτικές αυτές καθορίζεται η διάρκεια χρήσης των K_{SEED}, αν αυτά θα αποθηκεύονται στην κρυφή μνήμη κ.α. Αν για το συγκεκριμένο διαβατήριο το τερματικό αποφασίσει πως το K_{SEED} πρέπει να ανανεωθεί τότε θα πρέπει να ζητήσει από τον εξυπηρετητή την παραγωγή νέου K_{SEED}. Ο εξυπηρετητής θα το παράγει και αφού το αποθηκεύσει θα πρέπει να το στείλει στο τερματικό από όπου θα ενημερωθεί και το διαβατήριο. Αν και δεν αναφέρεται στο [12] υπονοείται πως η μεταφορά του νέου K_{SEED} προς το διαβατήριο θα πρέπει να γίνει μεσω ασφαλής επικοινωνίας η οποία θα έχει εγκατασταθεί με βάση την προηγούμενη K_{SEED} τιμή.



Εικόνα 26: Αρχιτεκτονική υποδομής κλειδιών πρόσβασης

Οι απαιτήσεις ασφάλειας μιας τέτοιας λύσης όπως αναφέρουν και οι συγγραφείς είναι η εμπιστευτικότητα και η ακεραιότητα των κλειδιών στους εξυπηρετητές, η ακεραιότητα των κλειδιών στην κρυφή μνήμη των τερματικών, η κρυπτογραφημένη επικοινωνία μεταξύ τερματικών και εξυπηρετητών και φυσικά η αυθεντικοποίηση των πρώτων στους δεύτερους η οποία θα πρέπει να υλοποιηθεί με χρήση ψηφιακών πιστοποιητικών.

Παρατηρήσεις

Η ασφάλεια της συγκεκριμένης πρότασης εστιάζεται στους εξυπηρετητές κλειδιών πρόσβασης. Για την εφαρμογή της στα ηλεκτρονικά διαβατήρια θα πρέπει να υλοποιηθεί ένας σημαντικός αριθμός εξυπηρετητών ώστε να ικανοποιηθεί η συνθήκη της απευθείας σύνδεσης με όλα τα τερματικά. Καθώς ο κάθε εξυπηρετητής θα πρέπει να κατέχει τις τιμές των K_{SEED} για όλα τα διαβατήρια το διαχειριστικό πρόβλημα του συγχρονισμού μεταξύ τους επιβαρύνεται αρκετά.

Επίσης δεν αναφέρεται το γεγονός πως και οι εξυπηρετητές θα πρέπει να αυθεντικοποιούνται στα τερματικά καθώς έχει συμπεριληφθεί η δυνατότητα παραγωγής νέων κλειδιών από αυτούς. Χωρίς αμοιβαία αυθεντικοποίηση θα μπορούσε οποιοσδήποτε να παράγει K_{SEED} και να γεμίσει τα διαβατήρια με λανθασμένες τιμές σε μια προσπάθεια DoS επίθεσης ή ακόμα χειρότερα δίνοντας την δυνατότητα για μη εξουσιοδοτημένη πρόσβαση στα δεδομένα των διαβατηρίων. Αυτό βέβαια δεν αποτελεί πρόβλημα για την παραπάνω εναλλακτική καθώς η αμοιβαία αυθεντικοποίηση μπορεί να συμπεριληφθεί στην πρόταση.

Το κυριότερο μειονέκτημα όμως αποτελεί η απόκριση του συστήματος σε μια ενδεχόμενη παραβίαση κάποιου από τους εξυπηρετητές. Δεν φαίνεται να έχει προβλεφθεί ένα τέτοιο σενάριο σύμφωνα με το οποίο όλα τα κλειδιά των διαβατηρίων θα είχαν παραβιαστεί και θα έπρεπε όλα τα διαβατήρια με κάποιο τρόπο να ανακαλεστούν και να αλλάξουν τις τιμές των K_{SEED} τους εσωτερικά.

Κεφάλαιο 3 Προτάσεις

Στα παρακάτω κεφάλαια παρουσιάζονται και αναλύονται δύο νέες προτάσεις που αφορούν στην επίλυση του προβλήματος που προκύπτει από την ελλιπή γνώση της τρέχουσας ώρας από πλευράς διαβατηρίων. Η πρώτη αφορά στην τροποποίηση του πρωτοκόλλου αυθεντικοποίησης τερματικών όπως παρουσιάζεται στα διαβατήρια τρίτης γενιάς και βασίζεται στην ίδια προσέγγιση που έχει γίνει και στο OSEP πρωτόκολλο ενώ στην δεύτερη εισάγεται μια επιπλέον διαδικασία πριν τον έλεγχο των διαβατηρίων από τα τερματικά κατά την οποία τα διαβατήρια ανανεώνουν σε μεταξύ τους επικοινωνία τις τιμές της τρέχουσας ώρας και πιθανές λίστες ανάκλησης.

3.1 Αυθεντικοποίηση τερματικού με απευθείας σύνδεση

Η πρόταση αυτή βασίζεται στην ίδια προσέγγιση που έγινε και στο πρωτόκολλο OSEP με τη διαφορά πως τα πρωτόκολλα CHIP, PACE και αυτό της παθητικής αυθεντικοποίησης παραμένουν ίδια. Αυτό που αλλάζει είναι το πρωτόκολλο αυθεντικοποίησης του τερματικού το οποίο τώρα περιλαμβάνει και τις DV οντότητες και στις δύο εκδοχές του.

Στο πρωτόκολλο για το αυθεντικοποίηση του τερματικού ουσιαστικά το τερματικό λαμβάνει μια τυχαία τιμή από το διαβατήριο και τη στέλνει πίσω υπογεγραμμένη. Το διαβατήριο πιστοποιεί την υπογραφή έχοντας το πιστοποιητικό του τερματικού. Για το λόγο αυτό στην αρχή του πρωτοκόλλου το τερματικό δίνει στο διαβατήριο την αλυσίδα πιστοποιητικών δηλαδή το δικό του πιστοποιητικό και το πιστοποιητικό της DV οντότητας. Το διαβατήριο, το οποίο από την φάση της προσωποποίησης έχει μέσα του το αυτό-υπογραφόμενο πιστοποιητικό της κρατικής αρχής πιστοποίησης (CVCA), ελέγχει την εγκυρότητα του DV πιστοποιητικού, και έπειτα βάσει αυτού ελέγχει την εγκυρότητα του πιστοποιητικού του τερματικού. Όπως έχει ήδη αναλυθεί και σε προηγούμενο κεφάλαιο το πρωτόκολλο έρχεται σε δύο εκδόσεις όπου η μόνη ουσιαστικά διαφορά αφορά το εφήμερο δημόσιο κλειδί του τερματικού **(~PK_{PCD})**. Στην έκδοση 1 το κλειδί έχει παραχθεί και ανταλλαχθεί κατά την φάση του CHIP πρωτοκόλλου, ενώ στην έκδοση 2 το κλειδί παράγεται και ανταλλάσσεται κατά την διάρκεια του πρωτοκόλλου αυθεντικοποίησης του τερματικού για να χρησιμοποιηθεί αργότερα από το CHIP. (Η έκδοση 2 προηγείται της αυθεντικοποίησης CHIP ενώ η έκδοση 1 έπεται)

Η λογική της παραλλαγής των δυο εκδόσεων είναι πως την τυχαία αυτή τιμή την υπογράφει τώρα η DV οντότητα της οποίας το πιστοποιητικό θεωρείται πως είναι έγκυρο και δεν έχει λήξει. Για να πάρει το διαβατήριο την υπογραφή της θα πρέπει το τερματικό να προωθήσει την τυχαία τιμή προς την DV και για πάρει πίσω την υπογραφή θα πρέπει πρώτα να αυθεντικοποιηθεί σε αυτόν. Με αυτό τον τρόπο η DV οντότητα κάνει τώρα τον έλεγχο του πιστοποιητικού του τερματικού για

λογαριασμό του διαβατηρίου. Με το επιτυχή έλεγχο της υπογραφής που κάνει το διαβατήριο στην DV ουσιαστικά εξασφαλίζει πως και το τερματικό έχει έγκυρο πιστοποιητικό.

Η υλοποίηση του πρωτοκόλλου έγινε με βάσει το παρακάτω σκεπτικό:

- Η τροποποίηση του πρωτοκόλλου να είναι όσο το δυνατόν μικρότερη.
- Όλες οι υπογραφές να γίνονται πάνω σε τυχαίες τιμές που προέρχονται και από τις δύο μεριές για να διατηρηθεί κάποιο επίπεδο ασφάλειας ([14] chapter 3.2)

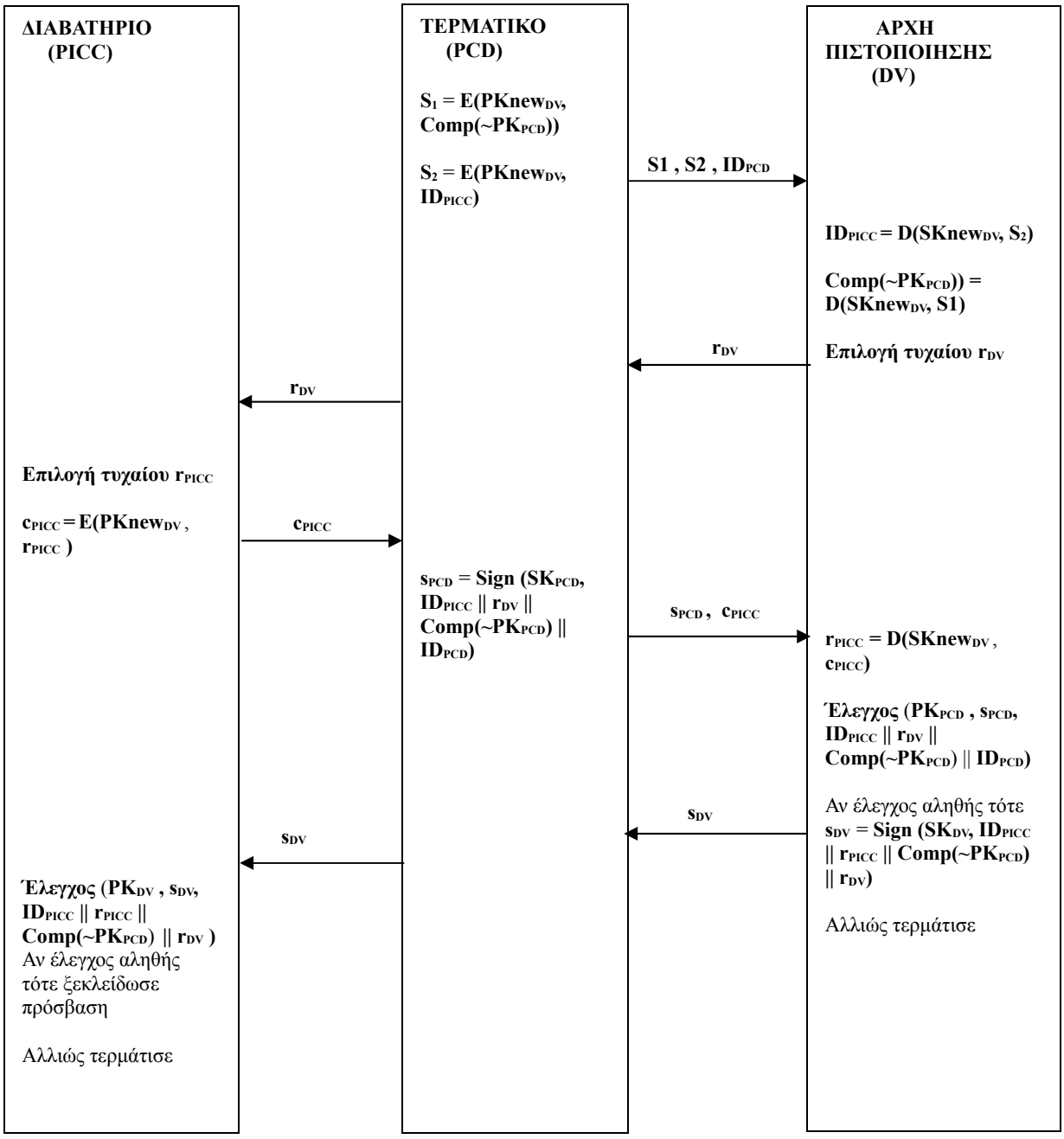
Επίσης επειδή κάποιες τιμές που θα ανταλλαχθούν στην διεπαφή μεταξύ του τερματικού και της DV είναι κρίσιμες για την ασφάλεια των άλλων μηχανισμών ασφάλειας των διαβατηρίων (όπως π.χ το $\sim PK_{PCD}$) θα πρέπει να προστατευτούν. Γι' αυτό γίνεται η εισαγωγή ενός νέου ζευγαριού κλειδιών της DV (PK_{newDV} , SK_{newDV}) όπου το SK_{newDV} είναι το ιδιωτικό κλειδί και το κρατάει η DV ενώ το PK_{newDV} είναι το δημόσιο κλειδί και έρχεται σαν επιπρόσθετο κλειδί στο πιστοποιητικό της DV (ίσως σε κάποιο πεδίο επέκτασης). Τα νέα κλειδιά χρησιμοποιούνται για τον παραπάνω λόγο αντί των κλειδιών για την υπογραφή για να μειωθεί το ρίσκο του συστήματος σε περίπτωση διέρευσης των κλειδιών. ([15] Remark 10.40)

Τα βήματα που εκτελούνται στην τροποποίηση της πρώτης έκδοσης του πρωτοκόλλου της αυθεντικοποίησης του τερματικού είναι τα εξής:

1. Αρχικά το τερματικό (PCD) κρυπτογραφεί τα ID_{PICC} και $Comp(\sim PK_{PCD})$ με το δημόσιο κλειδί της DV οντότητας PK_{newDV} , παράγει τα S_1 και S_2 και τα στέλνει στην DV μαζί με το ID_{PCD} (αναγνωριστικό του τερματικού).
2. Η DV εξάγει τα ID_{PICC} και $Comp(\sim PK_{PCD})$ χρησιμοποιώντας το ιδιωτικό της κλειδί SK_{newDV} και επιλέγει μια τυχαία τιμή r_{DV} την οποία και στέλνει στο τερματικό.
3. Το τερματικό προωθεί το r_{DV} στο διαβατήριο.
4. Το διαβατήριο επιλέγει μια τυχαία τιμή r_{PICC} την κρυπτογραφεί με το PK_{newDV} παράγοντας το c_{PICC} και το στέλνει στο τερματικό.
5. Το τερματικό παράγει το hash των $ID_{PICC} \| r_{DV} \| Comp(\sim PK_{PCD}) \| ID_{PCD}$ και το υπογράφει με το ιδιωτικό του κλειδί SK_{PCD}. Έπειτα στέλνει την υπογραφή s_{PCD} μαζί με το c_{PICC} στην DV.
6. Η DV εξάγει το το r_{PICC} και έχοντας το ID_{PCD} βρίσκει στην βάση του το έγκυρο πιστοποιητικό του τερματικού. Έπειτα από το δημόσιο κλειδί PK_{PCD} του πιστοποιητικού πιστοποιεί την υπογραφή που έλαβε.
7. Η DV υπογράφει τώρα το hash του $ID_{PICC} \| r_{PICC} \| Comp(\sim PK_{PCD}) \| r_{DV}$ και στέλνει την δικιά του υπογραφή πίσω στο τερματικό. Σε περίπτωση που η πιστοποίηση του τερματικού αποτύχει για οποιοδήποτε λόγο τότε η διαδικασία σταματά
8. Το τερματικό προωθεί την υπογραφή στο διαβατήριο.
9. Το διαβατήριο πιστοποιεί την υπογραφή της DV χρησιμοποιώντας το δημόσιο κλειδί της

DV από το πιστοποιητικό που είχε λάβει στην αρχική φάση του πρωτοκόλλου. Σε περίπτωση επιτυχίας το τερματικό αυθεντικοποιείται έμμεσα και αποκτά πρόσβαση στα ευαίσθητα δεδομένα του διαβατηρίου ,ενώ σε περίπτωση αποτυχίας η διαδικασία σταματά και η πρόσβαση απαγορεύεται.

Παρακάτω δίνεται και σχηματικά η πρώτη έκδοση του πρωτοκόλλου:

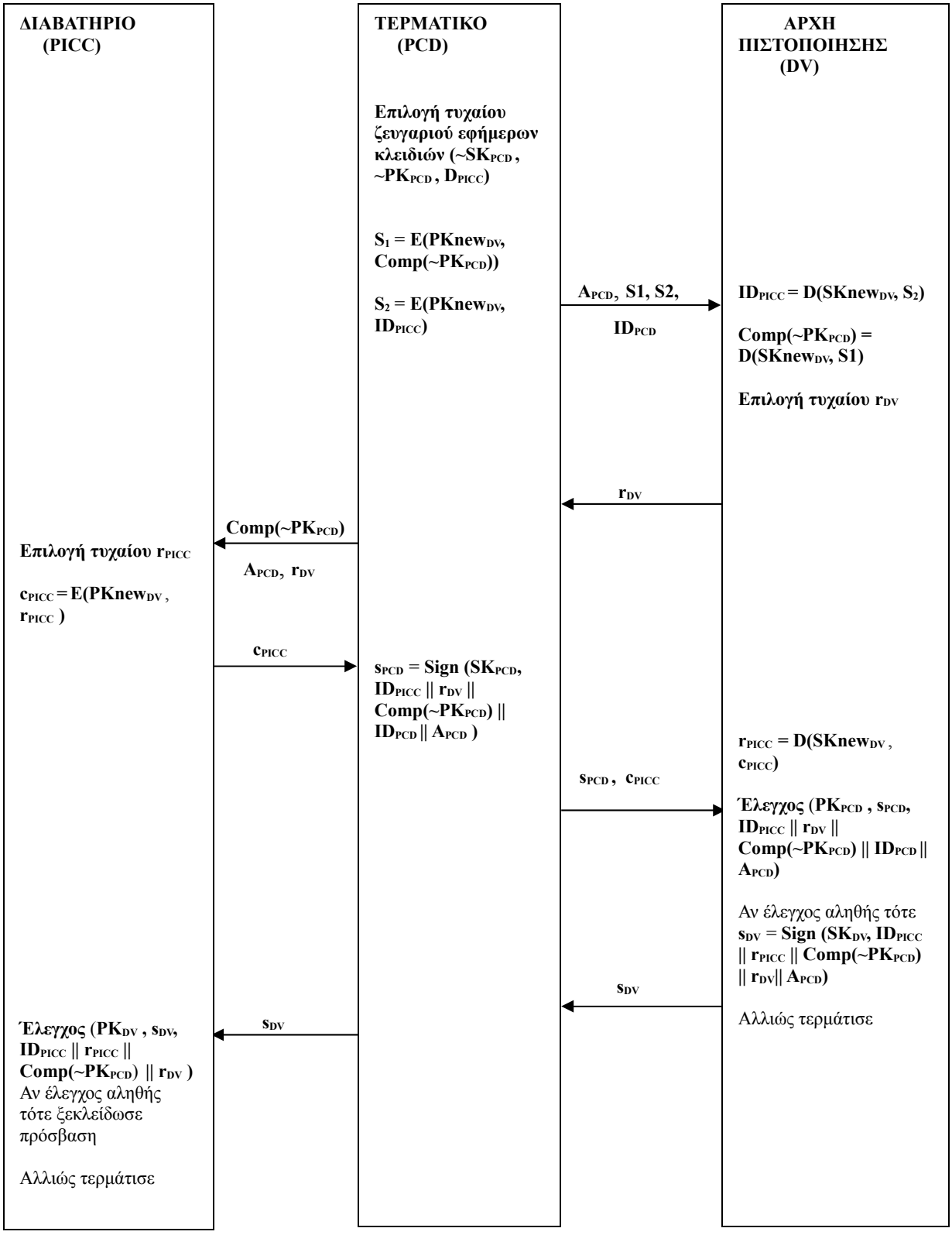


Εικόνα 27: Αυθεντικοποίηση τερματικού με απευθείας σύνδεση (Έκδοση 1)

Παρακάτω παρουσιάζονται τα βήματα που εκτελούνται στην τροποποίηση της δεύτερης έκδοσης του πρωτοκόλλου της αυθεντικοποίησης του τερματικού:

1. Αρχικά το τερματικό (PCD) επιλέγει ένα παροδικό ζευγάρι κλειδιών ($\sim SK_{PCD}$, $\sim PK_{PCD}$, D_{PICC}). Έπειτα κρυπτογραφεί τα ID_{PICC} και $Comp(\sim PK_{PCD})$ με το δημόσιο κλειδί της DV οντότητας PK_{newDV}, παράγει τα S_1 και S_2 και τα στέλνει στην DV μαζί με το ID_{PCD} (αναγνωριστικό του τερματικού) και τα βοηθητικά δεδομένα A_{PCD}
2. Η DV εξάγει τα ID_{PICC} και $Comp(\sim PK_{PCD})$ χρησιμοποιώντας το ιδιωτικό του κλειδί SK_{newDV} και επιλέγει μια τυχαία τιμή r_{DV} την οποία και στέλνει στο τερματικό
3. Το τερματικό προωθεί το r_{DV} στο διαβατήριο μαζί με τα $Comp(\sim PK_{PCD})$ και A_{PCD}
4. Το διαβατήριο επιλέγει μια τυχαία τιμή r_{PICC} την κρυπτογραφεί με το PK_{newDV} παράγοντας το c_{PICC} και το στέλνει στο τερματικό
5. Το τερματικό παράγει το hash των $ID_{PICC} \| r_{DV} \| Comp(\sim PK_{PCD}) \| ID_{PCD}$ και το υπογράφει με το ιδιωτικό του κλειδί SK_{PCD}. Έπειτα στέλνει την υπογραφή s_{PCD} μαζί με το c_{PICC} στην DV.
6. Η DV εξάγει το το r_{PICC} και έχοντας το ID_{PCD} βρίσκει στην βάση του το έγκυρο πιστοποιητικό του PCD. Έπειτα από το δημόσιο κλειδί PK_{PCD} του πιστοποιητικού πιστοποιεί την υπογραφή που έλαβε.
7. Η DV υπογράφει τώρα το hash του $ID_{PICC} \| r_{PICC} \| Comp(\sim PK_{PCD}) \| r_{DV}$ και στέλνει την δικιά του υπογραφή πίσω στο τερματικό. Σε περίπτωση που η πιστοποίηση του τερματικού αποτύχει για οποιοδήποτε λόγο τότε η διαδικασία σταματά.
8. Το τερματικό προωθεί την υπογραφή στο διαβατήριο.
9. Το διαβατήριο πιστοποιεί την υπογραφή της DV χρησιμοποιώντας το δημόσιο κλειδί της DV από το πιστοποιητικό που είχε λάβει στην αρχική φάση του πρωτοκόλλου. Σε περίπτωση επιτυχίας το τερματικό αυθεντικοποιείται έμμεσα και αποκτά πρόσβαση στα ευαίσθητα δεδομένα του διαβατηρίου ,ενώ σε περίπτωση αποτυχίας η διαδικασία σταματά και η πρόσβαση απαγορεύεται.

Παρακάτω δίνεται και σχηματικά η δεύτερη έκδοση του πρωτοκόλλου:



Εικόνα 28: Αυθεντικοποίηση τερματικού με απευθείας σύνδεση (Έκδοση 2)

Το πλεονέκτημα της παραπάνω πρότασης αφορά κυρίως στην εξάλειψη του προβλήματος της αδυναμίας των διαβατηρίων να ελέγξουν την ημερομηνία λήξης των πιστοποιητικών των τερματικών. Επίσης το πιστοποιητικό του τερματικού δεν χρειάζεται πλέον να φτάσει στο διαβατήριο. Έτσι το διαβατήριο αποφορτίζεται από το έργο του ελέγχου εγκυρότητας του πιστοποιητικού του τερματικού κατά την αρχική φάση του πρωτοκόλλου (επιφορτίζεται βέβαια με μια πράξη κρυπτογράφησης της τυχαίας πρόκλησης $\mathbf{r_{PICC}}$).

Όσον αφορά στις αδυναμίες μπορεί να λεχθεί πως εν λόγω πρόταση κληρονομεί όλα τα μειονεκτήματα που προκύπτουν από την προσέγγιση της απευθείας σύνδεσης τα οποία και έχουν επισημανθεί στο OSEP πρωτόκολλο καθώς επίσης και στο μειονέκτημα που προκύπτει από την δυνατότητα DoS επίθεσης στις DV οντότητες.

3.2 Πρωτόκολλα ανανέωσης στοιχείων μεταξύ διαβατηρίων

Η κύρια ιδέα για την υλοποίηση αυτών των πρωτοκόλλων είναι πως τα διαβατήρια πριν περάσουν από τον έλεγχο των τερματικών θα μπορούν να ανταλλάσσουν κάποια στοιχεία μεταξύ τους με σκοπό να ανανεώσουν τις τιμές τους με τις πιο πρόσφατες. Τα στοιχεία αυτά θα είναι είτε η τρέχουσα ώρα είτε οι λίστες ανάκλησης με σκοπό να μειωθεί η πιθανότητα λανθασμένης αυθεντικοποίησης των τερματικών από τα διαβατήρια των κατόχων που έχουν να ταξιδέψουν πολύ καιρό. Για το λόγο αυτό μια νέα διαδικασία θα πρέπει να εισαχθεί στους σταθμούς ελέγχου των διαβατηρίων κατά την οποία οι κάτοχοι θα φέρουν τα διαβατήρια σε μεταξύ τους επικοινωνία έτσι ώστε να ενημερωθούν όλα με τα στοιχεία του πιο πρόσφατου ταξιδιώτη. Η διαδικασία αυτή της ανανέωσης ενώ θα μπορούσε να είναι προαιρετική, προτείνεται να έχει υποχρεωτικό χαρακτήρα καθώς στην πρώτη περίπτωση οι συχνοί ταξιδιώτες οι οποίοι και κατέχουν τα πιο πρόσφατα δεδομένα πιθανόν να απουσίαζαν καθιστώντας την όλη λογική προβληματική. Παρακάτω δίνονται δύο λύσεις σε αυτή τη φιλοσοφία, με την πρώτη να ανανεώνει τις λίστες ανάκλησης και την δεύτερη να ανανεώνει την τρέχουσα ώρα των διαβατηρίων. Παρουσιάζεται επίσης η δομή του δικτύου μέσα από το οποίο θα επικοινωνήσουν τα διαβατήρια καθώς και ο τρόπος εγκαθίδρυσης ενός ασφαλούς καναλιού για την επικοινωνία μεταξύ τους.

Για λόγους που θα αναλυθούν και παρακάτω τα διαβατήρια που θα συμμετέχουν στην διαδικασία την κάθε φορά θα πρέπει να έχουν την ίδια χώρα έκδοσης, περιορίζοντας έτσι τους πιθανούς υποψήφιους σε κάποιο σταθμό αναχώρησης μειώνοντας και την πιθανότητα εύρεσης κάποιου διαβατηρίου με αρκετά πρόσφατα δεδομένα. Προτείνεται η διαδικασία αυτή να λαμβάνει χώρα σε σταθμούς εξόδου των χωρών αποκλειστικά για τους κάτοχους των διαβατηρίων των αντίστοιχων χωρών με το σκεπτικό πως στην περίπτωση αυτή έχουμε μεγάλο δείγμα από κατάλληλα για την

διαδικασία διαβατήρια και λόγω της υπόθεσης πως το μεγαλύτερο διάστημα παραμονής σε ένα σημείο για κάποιο διαβατήριο είναι η χώρα έκδοσης του.

3.2.1 Ανανέωση λιστών ανάκλησης

Το στοιχείο που ανταλλάσσεται εδώ στην επικοινωνία μεταξύ των διαβατηρίων είναι οι λίστες ανάκλησης και ουσιαστικά πρόκειται για την πρόταση που παρουσιάζεται στο [13] σε μια προσπάθεια εφαρμογής της στα ηλεκτρονικά διαβατήρια.

Οι Matei Ciobanu Morogan και Sead Muftic στο [13] ασχολούνται με το πρόβλημα διαχείρισης πιστοποιητικών σε ad hoc δίκτυα που βασίζονται σε υποδομές δημόσιων κλειδιών. Στην προσπάθεια να λύσουν το πρόβλημα της αδυναμίας συνεχούς σύνδεσης των κόμβων ενός ad hoc δικτύου με την PKI υποδομή εισάγουν δύο διαδικασίες διαχείρισης των λιστών ανάκλησης πιστοποιητικών. Κατά την πρώτη οι κόμβοι του συστήματος όταν αποκτούν σύνδεση με τις οντότητες πιστοποίησης CA ενημερώνονται για τη λίστα ανάκλησης ακολουθώντας τα εξής βήματα:

1. Ο κόμβος στέλνει μια αίτηση για την ενημερωμένη λίστα ανάκλησης από την CA.
2. Η CA περνάει την λίστα ανάκλησης από μια συνάρτηση κατακερματισμού (Hash (CRL)), δημιουργεί μια χρονοσφραγίδα και υπογράφει και τις δύο τιμές με μια υπογραφή. Έπειτα στέλνει πίσω στον κόμβο και τις δύο τιμές μαζί με την ψηφιακή υπογραφή.
3. Ο κόμβος αφού πιστοποιήσει την υπογραφή ελέγχει αν η τιμή κατακερματισμού της δικιά του λίστας ταιριάζει με αυτήν που έλαβε. Αν προκύψει πως οι λίστες είναι ίδιες τότε σταματά αλλιώς συνεχίζει ζητώντας την λίστα από την CA.
4. Η CA υπογράφει την λίστα μαζί με την χρονοσφραγίδα και στέλνει την λίστα, την χρονοσφραγίδα και την υπογραφή πίσω στον κόμβο.

Η δεύτερη διαδικασία αφορά στην επικοινωνία μεταξύ των κόμβων του συστήματος. Έστω πως ο κόμβος Α θέλει να ανανεώσει την λίστα ανάκλησης που κατέχει και υποθέτει πως ο κόμβος Β έχει μια πιο ενημερωμένη λίστα. Τα βήματα που εκτελούνται είναι τα εξής:

1. Ο Α στέλνει στον Β την τιμή κατακερματισμού της λίστας ανάκλησης που έχει αποθηκευμένη μαζί με την μέγιστη ηλικία αυτής της λίστας.
2. Αν ο Β έχει μια πιο πρόσφατη λίστα τότε συγκρίνει τις τιμές κατακερματισμού της λίστας που έλαβε με την δικιά του και αν είναι ίδιες τότε επιστρέφει την τιμή αυτή μαζί με την χρονοσφραγίδα της λίστας που κατέχει υπογεγραμμένες από την CA (επιστρέφει δηλαδή ότι

είχε λάβει στην πρώτη φάση στο βήμα 2). Σε περίπτωση που οι λίστες είναι διαφορετικές επιστρέφει επίσης και την ίδια τη λίστα υπογεγραμμένη μαζί με την χρονοσφραγίδα της (ότι είχε λάβει στο βήμα 4 της πρώτης φάσης).

3. Σε περίπτωση που ο κόμβος Α δεν γνωρίζει το δημόσιο κλειδί της CA τότε ζητά από τον Β το πιστοποιητικό της CA που έχει χρησιμοποιήσει.
4. Ο Β στέλνει πίσω το πιστοποιητικό της CA.(αν ζητηθεί)
5. Ο Α μπορεί τώρα να ελέγξει τις υπογραφές και ανανεώνει την λίστα ανάκλησης εσωτερικά.

Επίσης οι Morogan και Muftic αναφέρουν πως η δεύτερη διαδικασία θα μπορούσε να τροποποιηθεί για να συμπεριλάβει μια ομάδα από κόμβους. Αρχικά όλοι οι κόμβοι θα πρέπει να διαπιστώσουν ποιος κόμβος κατέχει την πιο πρόσφατη λίστα. Έτσι σε ένα αρχικό στάδιο όλοι οι κόμβοι θα πρέπει να ανταλλάξουν την hash τιμή της λίστας που κατέχουν μαζί την χρονοσφραγίδα της υπογεγραμμένες από την CA και έπειτα αφού διαπιστώσουν ποια είναι η πιο πρόσφατη να ζητήσουν από τον κατάλληλο κόμβο την συγκεκριμένη λίστα.

Με αυτό τον τρόπο επιτυγχάνεται η ενημέρωση των λιστών ανάκλησης των κόμβων όταν αυτοί εκτός σύνδεσης. Στο παραπάνω σενάριο έχει υποτεθεί πως η υποδομή δημοσίου κλειδιού αποτελείται από αρχές πιστοποίησης CA οι οποίες έχουν όλες πιστοποιηθεί από μια ριζική αρχή πιστοποίησης TCA της οποίας το πιστοποιητικό κατέχουν όλοι οι κόμβοι του συστήματος.

Για την προσαρμογή των παραπάνω διαδικασιών στα ηλεκτρονικά διαβατήρια προκύπτει ο εξής περιορισμός: Η ανανέωση των διαβατηρίων μπορεί να γίνει μόνο μεταξύ διαβατηρίων που έχουν εκδοθεί από την ίδια κρατική αρχή πιστοποίησης CVCA. Αυτό προκύπτει από την δομή της υποδομής δημοσίου κλειδιού και το γεγονός πως κάθε διαβατήριο μπορεί να ελέγχει μόνο πιστοποιητικά που έχουν ως ριζική αρχή πιστοποίησης την ίδια χώρα έκδοσης του διαβατηρίου. Για κάθε διαβατήριο μια διαφορετική αλυσίδα πιστοποιητικών παίρνει μέρος κατά την αυθεντικοποίηση των τερματικών με κάθε τερματικό να κατέχει τόσες αλυσίδες όσες και οι χώρες που θέλει να ελέγχει. (βλέπε εικόνα 14).

Με την ανανέωση των λιστών ανάκλησης κατά την επικοινωνία μεταξύ εγχώριων διαβατηρίων η λύση του προβλήματος παραμένει βέβαια προσεγγιστική. Παρόλα αυτά το σφάλμα στον έλεγχο των πιστοποιητικών μειώνεται αισθητά και ειδικά στην περίπτωση των σπάνιων ταξιδιωτών καθώς υπάρχει μεγάλη πιθανότητα μετά την διαδικασία της ανανέωσης η ανανεωμένη λίστα να προέρχεται από κάποιον κάτοχο διαβατηρίου που έχει ταξιδέψει ξανά αρκετά πρόσφατα.

Εδώ οι λίστες ανάκλησης θα πρέπει να μεταφέρονται στα διαβατήρια από τα τερματικά μετά από

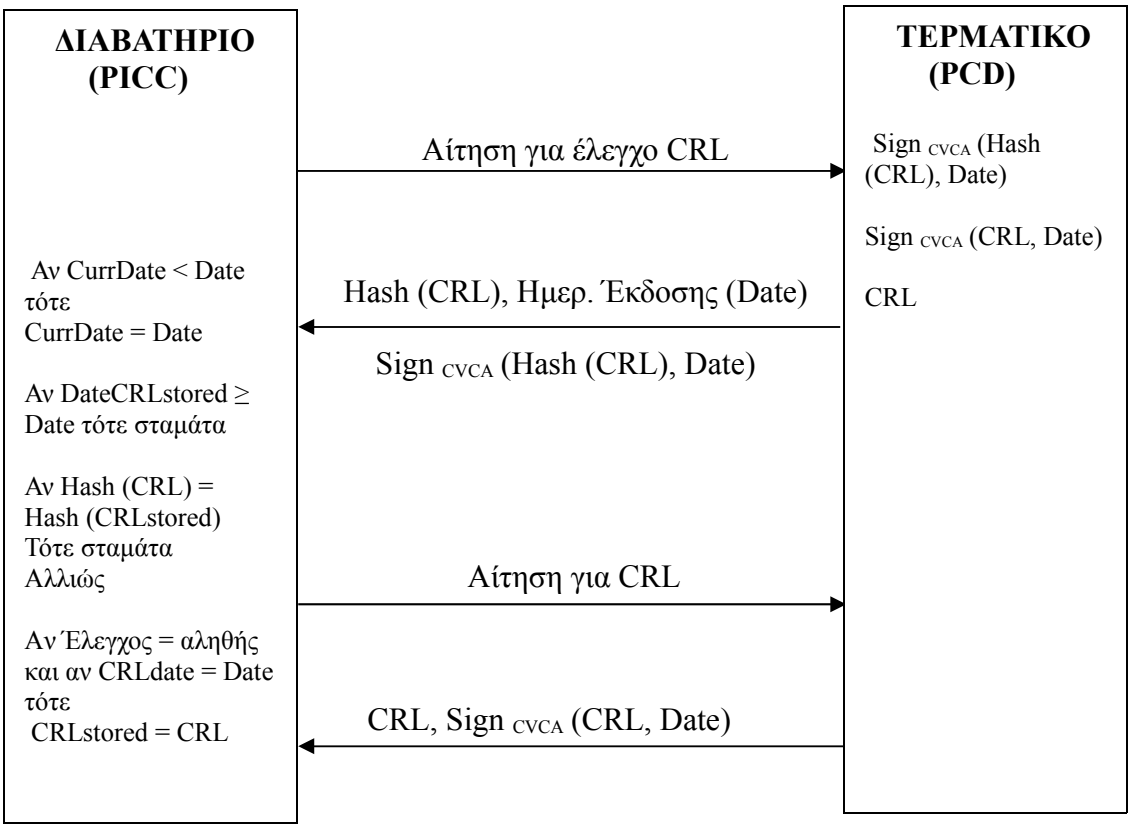
την επιτυχή έκβαση και της αυθεντικοποίησης τερματικού και μέσα από το ασφαλές κανάλι επικοινωνίας που έχει ήδη εγκατασταθεί. Κάθε χώρα θα διαχειρίζεται την δικιά της λίστα για τα όλα τα τερματικά εγχώρια ή μη για τα οποία εκδίδει πιστοποιητικά και θα πρέπει να τα ενημερώνει με την ανανεωμένη λίστα σε τακτά χρονικά διαστήματα ή και νωρίτερα σε περίπτωση παραβίασης τερματικού το οποίο και θα πρέπει να ανακληθεί στέλνοντας πάντα μαζί και τις εξής τιμές: την υπογραφή στην τιμή κατακερματισμού της λίστας μαζί με την ημερομηνία έκδοσης της λίστας (**Sign (**Hash (CRL) || date**)**) και την υπογραφή στην ίδια την λίστα μαζί με την τιμή της ημερομηνίας έκδοσης της (**Sign (**CRL || date**)**). Εδώ το ρόλο της χρονοσφραγίδας τον παίζει η ημερομηνία έκδοσης της λίστας. Στην λύση στο [13] η χρονοσφραγίδα είχε το νόημα της ώρας που η λίστα μεταφέρθηκε στον κόμβο από την CA μετά από αίτηση του ίδιου του κόμβου. Εδώ θεωρείται πως οι CVCA δεν δέχονται αιτήσεις αλλά πως όλη η υποδομή είναι σχεδιασμένη έτσι ώστε οι νέες λίστες να διαμοιράζονται στα τερματικά σε αρκετά μικρό χρονικό διάστημα από την στιγμή έκδοσης τους. Για την μεταφορά των λιστών ανάκλησης από τα τερματικά προς τα διαβατήρια αρχικά θα στέλνεται η hash τιμή της λίστας μαζί με την ημερομηνία έκδοσης και την υπογραφή **Sign (**Hash (CRL) || date**)** και αν έπειτα ζητηθεί θα στέλνεται η ίδια η λίστα μαζί με την τιμή **Sign (**CRL || date**)**. Ο λόγος που η επιπλέον πληροφορία της ημερομηνία έκδοσης θα πρέπει να στέλνεται ξεχωριστά στην πρώτη φάση βασίζεται στην εξής λογική: Η λίστα δεν χρειάζεται να μεταφέρεται ολόκληρη κάθε φορά από τα τερματικά προς τα διαβατήρια αλλά μόνο αν υπάρχει ανάγκη αντικατάστασης αυτής από μια καινούργια. Έτσι όπως και στην πρόταση στο [13] θα πρέπει να μπορεί να ελέγχεται η περίπτωση της ύπαρξης μιας διαφορετικής και πιο πρόσφατης λίστας μέσα στο τερματικό από αυτήν μέσα στο διαβατήριο χωρίς την μεταφορά της λίστας. Έτσι μετά από κάθε επιτυχή έκβαση του πρωτοκόλλου αυθεντικοποίησης τερματικού η παρακάτω επικοινωνία θα πρέπει να συντελείται.

1. Το διαβατήριο στέλνει μια αίτηση για τον έλεγχο της λίστας ανάκλησης
2. Το τερματικό στέλνει στο διαβατήριο την τιμή κατακερματισμού της λίστας, την ημερομηνία έκδοσης της και την υπογραφή της CVCA για τις δύο αυτές τιμές.
3. Το διαβατήριο αφού πιστοποιήσει την υπογραφή της CVCA ελέγχει αν η λίστα που κατέχει είναι πιο πρόσφατη από αυτήν του τερματικού και αν αυτό ισχύει η διαδικασία σταματά. Έπειτα συγκρίνει τις τιμές κατακερματισμού της λίστας που έλαβε με την δικιά του και αν είναι ίδιες πάλι σταματά. Αν καμία από τις παραπάνω περιπτώσεις δεν ισχύει τότε ζητά από το τερματικό την ανανεωμένη λίστα. Επίσης αν η ημερομηνία έκδοσης της λίστας είναι μεταγενέστερη της τρέχουσας ώρας του διαβατηρίου, τότε ανανεώνεται και η τρέχουσα ώρα.
4. Το τερματικό στέλνει στο διαβατήριο την λίστα μαζί με την υπογραφή της CVCA στην

λίστα και την ημερομηνία έκδοσης.

5. Το διαβατήριο πιστοποιεί την υπογραφή της CVCA χρησιμοποιώντας της ημερομηνία έκδοσης που αναγράφεται στην λίστα και ελέγχοντας πως πρόκειται για την ίδια ημερομηνία που έλαβε στο βήμα 3 και ανανεώνει την λίστα ανάκλησης του εσωτερικά.

Τα βήματα αυτά παρουσιάζονται και σχηματικά παρακάτω:



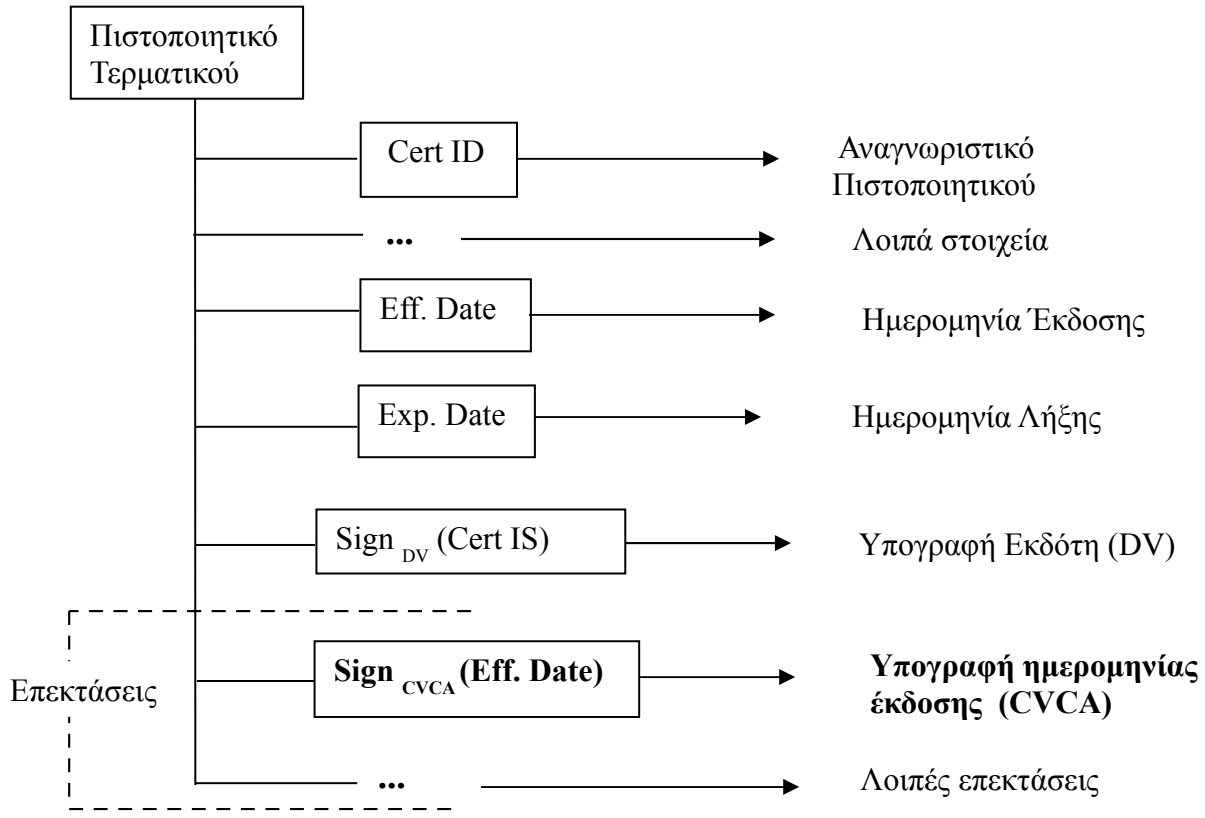
Εικόνα 29: Πρωτόκολλο μεταφοράς λίστας ανάκλησης σε διαβατήριο από τερματικό

Το ότι το πρωτόκολλο δεν σταματά αν η τρέχουσα ώρα του διαβατηρίου είναι μεταγενέστερη της ημερομηνίας έκδοσης της λίστας ανάκλησης δικαιολογείται από το γεγονός πως η τρέχουσα ώρα είτε θα περιέχει την ημερομηνία έκδοσης μιας λίστας ανάκλησης από προηγούμενο έλεγχο, είτε την ημερομηνία έκδοσης του πιστοποιητικού κάποιου τερματικού από προηγούμενο έλεγχο είτε την ημερομηνία έκδοσης του πιστοποιητικού του τερματικού σε αυτόν τον έλεγχο. Εκτός από την πρώτη περίπτωση οι υπόλοιπες δεν συσχετίζονται με το αν το τερματικό έχει πιο πρόσφατη λίστα ανάκλησης από το διαβατήριο. Ειδικά για την τελευταία περίπτωση ισχύει πως το πιστοποιητικό του τερματικού θα είναι μεταγενέστερο της λίστας ανάκλησης που περιέχεται στο τερματικό στο χρονικό διάστημα που μεσολαβεί μεταξύ της έκδοσης του πιστοποιητικού και της επόμενης ανανέωσης της λίστας ανάκλησης.

Η διαδικασία και το πρωτόκολλο επικοινωνίας μεταξύ των διαβατηρίων θα αναλυθεί σε παρακάτω κεφάλαιο στο οποίο περιγράφεται και το προτεινόμενο δίκτυο πρόσβασης.

3.2.2 Ανανέωση τρέχουσας ώρας

Αντί της ανταλλαγής των λιστών ανάκλησης το διαβατήρια θα μπορούσαν να ανανεώνουν την τιμή της τρέχουσας ώρας σε μεταξύ τους επικοινωνία. Για το σκοπό αυτό θα πρέπει η ημερομηνία έκδοσης των πιστοποιητικών των τερματικών (η οποία έχει αντικαταστήσει την τρέχουσα ώρα στα διαβατήρια από το τελευταίο τερματικό που πέρασαν) να έρχεται και αυτή με την υπογραφή του CVCA. Έτσι θα πρέπει να προστεθεί διαδικασία όπου κατά την παραγωγή ενός πιστοποιητικού τερματικού από την DV οντότητα να ζητείται από το αντίστοιχο CVCA να υπογράφει η ημερομηνία έκδοσης του πιστοποιητικού. Η υπογραφή αυτή θα μπορούσε να μπαίνει σε κάποιο πεδίο επέκτασης του πιστοποιητικού του τερματικού και θα αποθηκεύεται στα διαβατήρια με την μεταφορά της αλυσίδας πιστοποιητικών προς σε αυτά κατά την αρχική φάση του πρωτοκόλλου αυθεντικοποίησης του τερματικού. Η νέα τροποποιημένη μορφή των πιστοποιητικών των τερματικών φαίνεται στο παρακάτω σχήμα.



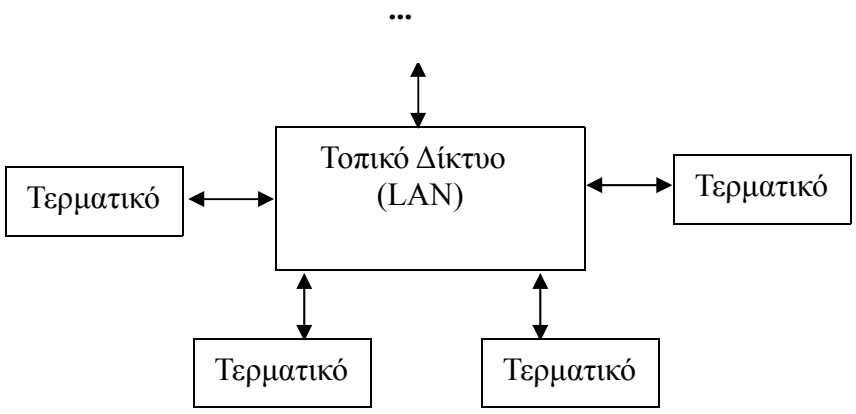
Εικόνα 30: Τροποποιημένο πιστοποιητικό τερματικών

Τώρα τα διαβατήρια αποθηκεύοντας εκτός της τρέχουσας ώρας και την υπογραφή της ριζικής αρχής πιστοποίησης (CVCA) για αυτήν μπορούν να ανταλλάξουν το στοιχείο αυτό με αξιόπιστο τρόπο σε μεταξύ τους επικοινωνία όπως θα αναλυθεί στο παρακάτω κεφάλαιο.

Ένα από τα πλεονεκτήματα αυτής της πρότασης έναντι αυτής που παρουσιάστηκε στο προηγούμενο κεφάλαιο είναι ότι καθιστά εφαρμόσιμες προτάσεις για την διαχείριση των λιστών ανάκλησης όπως αυτή που παρουσιάστηκε στο κεφάλαιο 2.2.2

3.2.3 Δίκτυο πρόσβασης

Για την επικοινωνία μεταξύ των διαβατηρίων προτείνεται η εγκατάσταση στους σταθμούς αναχώρησης ενός Ethernet τοπικού δικτύου με το οποίο θα συνδέονται τερματικά ανάγνωσης όπως φαίνεται και στο παρακάτω σχήμα.



Εικόνα 31: Τοπικό δίκτυο πρόσβασης για την ανανέωση των στοιχείων

Τα διαβατήρια θα εισέρχονται στα τερματικά του δικτύου αυτού τα οποία και θα λειτουργούν ως μη αυθεντικοποιημένα τερματικά. Για να δοθεί στα διαβατήρια άδεια πρόσβασης στο τοπικό δίκτυο από τα τερματικά η τυπική διαδικασία ελέγχου θα πρέπει να εκτελείται όπως αυτή περιγράφεται στο [2] (Εικόνα 3.1) με τα πρωτόκολλα PACE και της παθητικής αυθεντικοποίησης να έχουν πλέον υποχρεωτικό χαρακτήρα.

Σε πρώτη φάση θα πρέπει να αποφασίζεται πιο από τα διαβατήρια έχει το πιο πρόσφατο στοιχείο

(**Element**). Για την ανανέωση των λιστών ανάκλησης αυτό που αρχικά θα ανταλλάσσεται είναι η τιμή κατακερματισμού της λίστας, η ημερομηνία έκδοσης της λίστας και η υπογραφή και των δύο από την CVCA οντότητα ενώ για την ανανέωση της τρέχουσας ώρας θα ανταλλάσσεται είναι η τρέχουσα ώρα και η υπογραφή της CVCA για αυτήν.

Ανανέωση λίστας ανάκλησης:

Element = Hash (CRL), Eff. Date (CRL), Sign $_{CVCA}$ (Hash (CRL), Eff. Date (CRL))

Ανανέωση τρέχουσας ώρας:

Element = Current_Time , Sign $_{CVCA}$ (Current_Time)

Για την ενημέρωση όλων των διαβατηρίων με το πιο πρόσφατο στοιχείο η εξής διαδικασία θα ακολουθείται σε ένα υποθετικό δίκτυο n- τερματικών:

1. Κάθε διαβατήριο που θα περνά επιτυχώς την τυπική διαδικασία ελέγχου θα στέλνει στο τερματικό το δικό του Element.
2. Κάθε τερματικό λαμβάνοντας το Element θα το στέλνει στο δίκτυο προς όλους τους προορισμούς μέσω ενός μηνύματος εκπομπής (broadcast message).
3. Κάθε τερματικό θα λαμβάνει μηνύματα από το δίκτυο και έπειτα θα στέλνει όλα τα Elements που περιέχουν πίσω στα διαβατήρια.

   Κάθε διαβατήριο θα πρέπει να ξεχωρίσει το πιο πρόσφατο από όλα τα Elements (συμπεριλαμβανομένου και του δικού του) και αφού το ελέγξει ως προς την εγκυρότητα του να το αποθηκεύσει ως το νέο Element. Για την περίπτωση που έχουμε ανανέωση της τρέχουσας ώρας το πρωτόκολλο εδώ σταματά. Για την περίπτωση της ανανέωσης λίστας ανάκλησης το διαβατήριο που έχει την πιο πρόσφατη λίστα θα πρέπει να στείλει πίσω στο τερματικό την τιμή: **New_CRL = CRL**, **Eff. Date (CRL), Sign $_{CVCA}$ ((CRL), Eff. Date (CRL))** (τα υπόλοιπα βήματα αφορούν μόνο στην περίπτωση των λιστών ανάκλησης).
4. Το τερματικό μόλις λάβει την **New_CRL** θα πρέπει να την στείλει στο δίκτυο προς όλα τα τερματικό μεσώ πάλι ενός broadcast μηνύματος.
5. Τα διαβατήρια αφού λάβουν το **New_CRL** από τα τερματικά τους πιστοποιούν την εγκυρότητα της υπογραφής, ελέγχουν πως οι ημερομηνίες έκδοσης μεταξύ Element και New_CRL ταιριάζουν και ανανεώνουν την λίστα ανάκλησης τους.

3.2.4 Εγκαθίδρυση ασφαλούς καναλιού

Λόγω της κρισιμότητας στην ασφάλεια της υποδομής δημοσίου κλειδιού που κατέχει η μυστικότητα του ιδιωτικού κλειδιού των κρατικών αρχών πιστοποίησης CVCA και λόγω του γεγονότος πως μέσα στο δίκτυο πρόσβασης θα κυκλοφορούν πολλά ζευγάρια καθαρών -κρυπτογραφημένων μηνυμάτων (plaintext – ciphertext pairs) δημιουργημένα από αυτό το κλειδί προτείνεται ως επιπλέον μηχανισμός ασφάλειας (πέραν του έλεγχου πρόσβασης στο δίκτυο) η εγκαθίδρυση ενός ασφαλούς καναλιού επικοινωνίας μεταξύ των διαβατηρίων πριν ξεκινήσουν να ανταλλάσσονται τα στοιχεία ανανέωσης. Με αυτόν τον τρόπο περιορίζεται η πιθανότητα επιτυχών επιθέσεων κρυπτανάλυσης στο ιδιωτικό κλειδί των CVCA οντοτήτων οι οποίες θα μπορούσαν να είναι δυνατές αν υπάρχει η δυνατότητα μεγάλης συλλογής τέτοιων ζευγαριών.

Για το λόγο αυτό προτείνεται στην αρχή της επικοινωνίας να εκτελείται από τα διαβατήρια που απόκτησαν πρόσβαση στο δίκτυο μια Diffie Hellman ανταλλαγή ενός κλειδιού με το οποίο θα κρυπτογραφείται η επικοινωνία μέσα στο τοπικό δίκτυο.

Η DH ανταλλαγή θα πρέπει να είναι πολλαπλών συμμετεχόντων και παρακάτω δίνεται ο τρόπος υλοποίησης της όπως έχει παρουσιαστεί και στο [13] (κεφάλαιο 22.1) αλλά προσαρμοσμένος για λειτουργία σε ένα τοπικό δίκτυο το οποίο δίνει την δυνατότητα για μηνύματα εκπομπής. Η ανάλυση εδώ θα παρουσιαστεί για τρία διαβατήρια και έπειτα σχολιαστεί και η γενίκευση της και για την περίπτωση N διαβατηρίων.

Αρχικά όλα τα διαβατήρια της ίδιας χώρας θα πρέπει να έχουν τις ίδιες δημόσιες παραμέτρους **n** και **g** οι οποίες μπορούν να εισαχθούν κατά την φάση της προσωποποίησης. Αφού και τα τρία διαβατήρια (A, B, C) αποκτήσουν πρόσβαση στο δίκτυο τα επόμενα βήματα εκτελούνται:

1. Κάθε τερματικό ζητά από τα διαβατήρια τις δημόσιες τιμές για την DH ανταλλαγή.
2. Αφού τα διαβατήρια A, B και C επιλέξουν τυχαίους μεγάλους πρώτους αριθμούς **a, b, c**, υπολογίζουν αντιστοίχως τις τιμές $\mathbf{g^a \bmod n}$, $\mathbf{g^b \bmod n}$, $\mathbf{g^c \bmod n}$ και τις στέλνουν πίσω στα τερματικά.
3. Κάθε τερματικό εκπέμπει στο δίκτυο την τιμή που έλαβε και αφού λάβει τις αντίστοιχες τιμές από τα άλλα τερματικά τις στέλνει πίσω στο δικό του διαβατήριο.

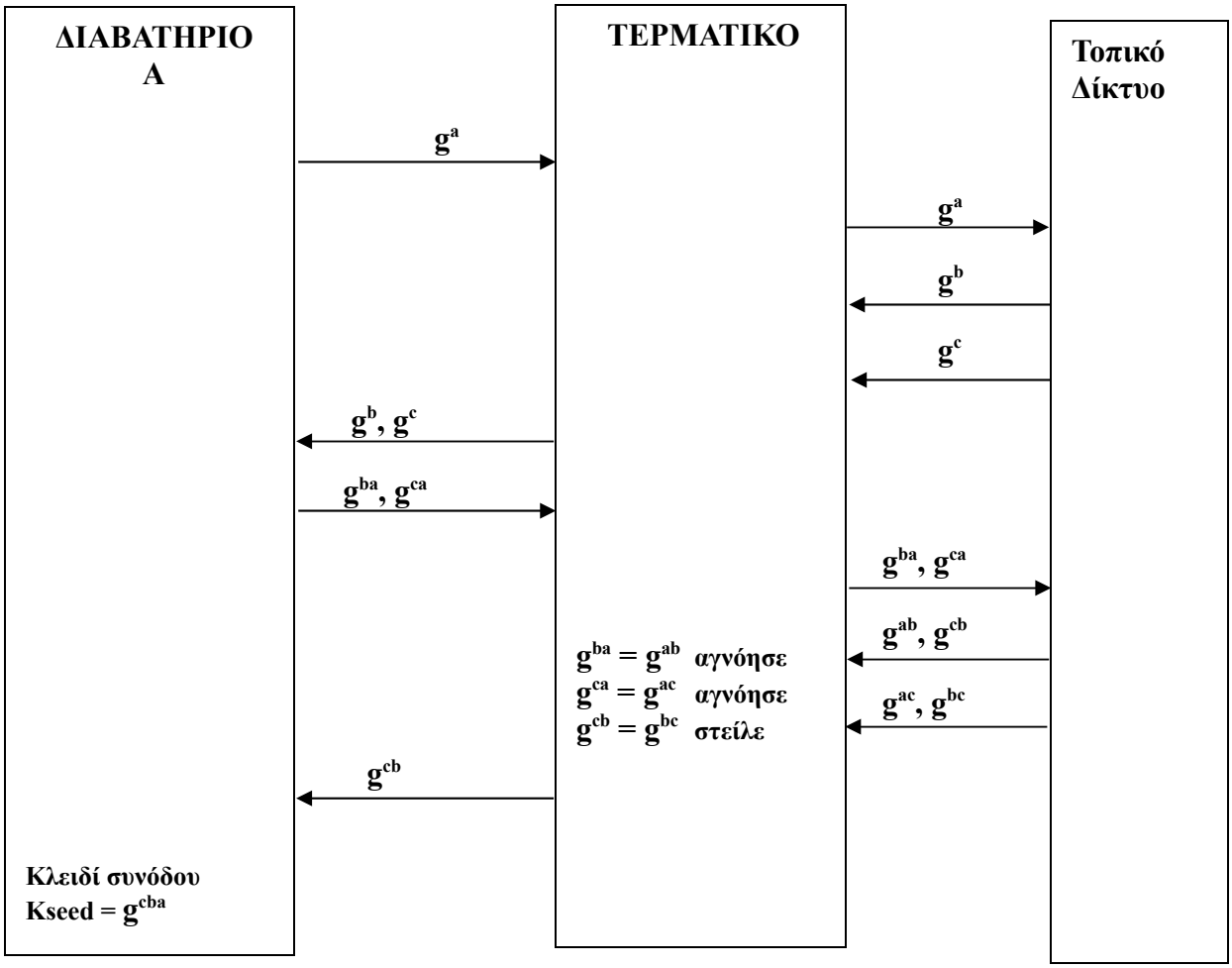
Από δω και πέρα θα αναφέρομαι μόνο στο διαβατήριο A και θα εννοείται πως τα αντίστοιχα βήματα εκτελούνται και για τα διαβατήρια B και C.

4. Το διαβατήριο A υπολογίζει τις τιμές $\mathbf{g^{ba} \bmod n}$ και $\mathbf{g^{ca} \bmod n}$ και τις στέλνει στο τερματικό.
5. Το τερματικό εκπέμπει τις τιμές προς το δίκτυο και λαμβάνει από τα άλλα διαβατήρια τις

τιμές: $\mathbf{g^{ab}\ mod\ n}$, $\mathbf{g^{cb}\ mod\ n}$, $\mathbf{g^{ac}\ mod\ n}$, $\mathbf{g^{bc}\ mod\ n}$. Το τερματικό διαγράφει τώρα από τις τιμές που έλαβε αυτές που είναι ίδιες με αυτές που μόλις έστειλε ($\mathbf{g^{ab} = g^{ba}}$ και $\mathbf{g^{ac} = g^{ca}}$) και αφού διαπιστώσει πως $\mathbf{g^{cb} = g^{bc}}$ στέλνει μόνο την μία τιμή πίσω στο διαβατήριο.

6. Το διαβατήριο Α μόλις λάβει το $\mathbf{g^{cb}}$ υπολογίζει το κλειδί συνόδου ως το $\mathbf{g^{cba}}$ ($\mathbf{K_{ΣΥΝΟΔΟΥ} = g^{cba}}$)

Παρακάτω παρουσιάζονται και σχηματικά τα βήματα που εκτελούνται για την δημιουργία του κλειδιού συνόδου από την πλευρά του διαβατηρίου Α και για τρεις συμμετέχοντες.



Εικόνα 32: DH ανταλλαγή κλειδιού στο τοπικό δίκτυο με τρεις συμμετέχοντες

Γενικά το κάθε διαβατήριο θα αποθηκεύει το κλειδί συνόδου αφού λάβει μία μόνο τιμή από το τερματικό και αφού την υψώσει στο δύναμη που του υπαγορεύει η μυστική του τιμή. Σε κάθε άλλη περίπτωση θα επενεργεί με τον ίδιο τρόπο στις τιμές που λαμβάνει από το τερματικό και θα στέλνει τα αποτελέσματα πίσω σε αυτό μέχρι να λάβει μία μόνο τιμή. Για τρία διαβατήρια συμμετέχοντα έχουμε πως το κάθε ένα θα πρέπει να εκτελέσει 4 εκθετικές πράξεις και να ανταλλάξει 4 μηνύματα

με το αντίστοιχο τερματικό. Γενικά προκύπτει πως για N διαβατήρια ο αριθμός των εκθετικών πράξεων που απαιτούνται είναι 2^{N-1} ενώ ο αριθμός των μηνυμάτων που πρέπει να ανταλλαχθούν μεταξύ διαβατηρίου και τερματικού είναι 2(N - 1). Περαιτέρω βελτιώσεις ως προς τον αριθμό των εκθετικών πράξεων από πλευράς διαβατηρίων θεωρούνται έξω από τα πλαίσια αυτής της εργασίας.

Η λύση που προτείνεται εδώ για την εγκαθίδρυση ασφαλούς καναλιού επικοινωνίας μεταξύ των διαβατηρίων προστατεύει την ανταλλαγή των στοιχείων ανανέωσης από κάποιον που ενδεχομένως να μπορεί να έχει πρόσβαση στα δεδομένα που κυκλοφορούν στο τοπικό αυτό δίκτυο, δεν προστατεύει όμως από την απειλή κάποιου παραβιασμένου τερματικού πρόσβασης στο δίκτυο καθώς η DH ανταλλαγή είναι επιρρεπής σε επιθέσεις τύπου άνθρωπος-στη-μέση (Man in the Middle attacks).

Επίσης η συνολική πρόταση των πρωτοκόλλων ανανέωσης στοιχείων όπως παρουσιάστηκε για τα ηλεκτρονικά διαβατήρια παρουσιάζει ένα σημαντικό μειονέκτημα ως προς την υλοποίηση της. Λόγω της ανάγκης για αυξημένη πιθανότητα συμμετοχής τουλάχιστον ενός συχνού ταξιδιώτη ώστε να έχουμε ικανοποιητικά αποτελέσματα προκύπτει πως η καινούργια διαδικασία στους σταθμούς αναχώρησης θα πρέπει να έχει υποχρεωτικό χαρακτήρα και πως θα πρέπει να υπάρχει ένας ελάχιστος αριθμός συμμετεχόντων ώστε το πρωτόκολλο ανταλλαγής να ξεκινά. Προκύπτει άρα το θέμα του πόση θα είναι η αναμονή στα σημεία ανανέωσης ώστε να μαζευτεί ο κατάλληλος αριθμός διαβατηρίων αφού το πρωτόκολλο απαιτεί συμμετοχή διαβατηρίων σε πραγματικό χρόνο καθώς επίσης και το τι θα συμβεί αν δεν μαζευτεί ο κατάλληλος αριθμός συμμετεχόντων.

Συμπεράσματα

Τα ηλεκτρονικά διαβατήρια έρχονται να αντικαταστήσουν τον παραδοσιακά έγγραφα προσφέροντας ισχυρούς μηχανισμούς έναντι στις πλαστογραφήσεις και ενισχύοντας την διαδικασία της ταυτοποίησης των φυσικών προσώπων. Η χρήση βιομετρικών στοιχείων έχει καταστήσει άμεση την ανάγκη επιπρόσθετων μηχανισμών ασφάλειας όσον αφορά στην ιδιωτικότητα των κατόχων των νέων εγγράφων. Η αυθεντικοποίηση των τερματικών ανάγνωσης ώστε να ελέγχεται η πρόσβαση στα ευαίσθητα προσωπικά δεδομένα είναι η λύση που έχει αυτή τη στιγμή υλοποιηθεί. Ύστερα από συνεχείς τροποποιήσεις στα πρωτόκολλα ασφάλειας βρισκόμαστε πλέον στην τρίτη γενιά ηλεκτρονικών διαβατηρίων με μια όμως αδυναμία να παραμένει: τα διαβατήρια λόγω έλλειψης εσωτερικού ρολογιού δεν μπορούν να ελέγξουν ικανοποιητικά τα πιστοποιητικά των τερματικών ανάγνωσης ως προς την ημερομηνία λήξης τους.

Αρκετές προτάσεις από την βιβλιογραφία έχουν βρεθεί στα πλαίσια αυτής της εργασίας που

αφορούν στην επίλυση του εν λόγω προβλήματος. Η πρώτη εισάγει την οντότητα του εξυπηρετητή χρόνου σε μια προσπάθεια να ανανεώσουν τα διαβατήρια την τρέχουσα τους ώρα. Η δεύτερη δίνει κατασκευαστική λύση επιτρέποντας στον κάτοχο του διαβατηρίου να ελέγξει αυτός τις ημερομηνίες. Η τρίτη προτείνει το πρωτόκολλο OSEP με την ενεργή συμμετοχή των DV οντοτήτων. Η τέταρτη χρησιμοποιεί κρυπτογραφία βασισμένη σε ταυτότητες και η τελευταία εισάγει τους διαχειριστές κλειδιών πρόσβασης. Όλες οι παραπάνω προτάσεις αναλύονται ως προς πληρότητα τους και εντοπίζονται οι όποιες αδυναμίες τους.

Επίσης δύο νέες προτάσεις παρουσιάζονται με την πρώτη να ακολουθεί την ίδια φιλοσοφία με το OSEP και την δεύτερη να παρουσιάζει έναν τρόπο μείωσης του σφάλματος προσέγγισης της τρέχουσας ώρας εισάγοντας μια καινούργια διαδικασία και ένα πρωτόκολλο μεταξύ των διαβατηρίων.

Προς το παρόν το πρόβλημα υπάρχει και έχει αναγνωριστεί από πληθώρα αναφορών από την βιβλιογραφία. Μέχρι τα διαβατήρια να λειτουργήσουν ως ενεργές RFID συσκευές με ικανότητα μέτρησης του χρόνου κάποια λύση θα πρέπει να βρεθεί πιθανότατα σε μια νέα γενιά ηλεκτρονικών διαβατηρίων.

Αναφορές

[1] (ICAO) PKI for Machine Readable Travel Documents offering ICC Read-Only Access October 01, 2004

[2] (BSI) Advanced Security Mechanisms forMachine Readable Travel Documents,Technical Guideline TR-03110, 2010

[3] Rishab Nithyanand, "A Survey on the Evolution of Cryptographic Protocols in ePassports" University of California – Irvine 2009

[4] Anshuman Sinha, "A survey of system security in contactless electronic passports", International Journal of Critical Infrastructure Protection Volume 4, Issues 3-4, December 2011, Pages 154-164

[5] Dimitrios Lekkas, Dimitris Gritzalis, "e-Passports as a means towards the first World-Wide Public Key Infrastructure", in Proceedings: 4th European PKI Workshop (EuroPKI) Mallorca, Spain, Lecture Notes in Computer Science (LNCS), Vol. 4582, Springer (2007)

[6] Rishab Nithyanand, Gene Tsudik, and Ersin Uzun , "Readers Behaving Badly Reader Revocation in PKI-Based RFID Systems", Computer Security – ESORICS 2010 Lecture Notes in Computer Science, 2010, Volume 6345/2010, 19-36

[7] Markus Ullmann and Matthias Vögeler, "Contactless Security Token Enhanced Security by Using New Hardware Features in Cryptographic-Based Security Mechanisms" from "Towards Hardware-Intrinsic Security Information" Security and Cryptography, 2010, Part 5, 259-279, chapter 4.4

[8] Vijayakrishnan Pasupathinathan, "An on-line secure e-passport protocol", ISPEC'08 Proceedings of the 4th international conference on Information security practice and experience, Pages 14-28

[9] Abid, M., Afifi, H.: Secure e-passport protocol using elliptic curve diffie-hellman key agreement protocol. In: 4th International Conference on Information Assurance and Security. (2008)

[10] C.H. Li , X.F. Zhang, H. Jin, W. Xiang, "E-passport EAC scheme based on Identity-Based Cryptography", Information Processing Letters 111 (2010) 26–30

[11] A. Shamir, "Identity-Based Cryptosystems and signature schemes", in: Proceedings of CRYPTO 84, in: Lecture Notes in Comput. Sci., vol. 196, Springer-Verlag, Berlin, 1984, pp. 47–53.

[12] Pablo Najera, Francisco Moyano, Javier Lopez, "Security Mechanisms and Access Control Infrastructure for e-Passports and General Purpose e-Documents", Journal of Universal Computer Science, vol. 15, no. 5 (2009), 970-991

[13] Matei Ciobanu Morogan, Sead Muftic, “Certificate Management in Ad Hoc Networks”, Applications and the Internet Workshops, 27-31 Jan. 2003, 337 - 341

[14] Bruce Schneier, “Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C”, Jan. 1996

[15] A. Menezes, P. VanOorschot, S. Vanstone, “Handbook of Applied Cryptography”, Aug. 1996