SECURITATEA ȘI AUTENTIFICAREA ÎN DOCUMENTELE DE CĂLĂTORIE CU CIP eMRTD: O ABORDARE INTEGRATĂ A TEHNOLOGIEI PKI ȘI DISPOZITIVELOR BIOMETRICE

SECURITY AND AUTHENTICATION IN TRAVEL DOCUMENTS WITH eMRTD CHIP: AN INTEGRATED APPROACH TO PKI TECHNOLOGY AND BIOMETRIC DEVICES

Subinspector de poliție Alexandru Florin MELINTE*

Rezumat: *Lucrarea explorează autentificarea documentelor de călătorie cu cip eMRTD în contextul creșterii călătoriilor internaționale și a cerințelor sporite de securitate. Tehnologia PKI și dispozitivele biometrice sunt esențiale pentru această autentificare, permițând verificarea rapidă și eficientă a identității călătorilor. Lucrarea analizează funcționarea acestor tehnologii și impactul lor asupra securității frontierelor, prevenției fraudei și protecției datelor personale*

Cuvinte cheie*: eMRTD, Tehnologia PKI, dispozitive biometrice, documente de călătorie pentru autentificare, securitate la frontieră, prevenirea fraudei, protecția datelor.*

Abstract: *The paper explores the authentication of travel documents with eMRTD chips in the context of increasing international travel and heightened security requirements. PKI technology and biometric devices are essential for this authentication, allowing for the quick and efficient verification of travelers' identities. The paper analyzes the functioning of these technologies and their impact on border security, fraud prevention, and data protection.*

Keywords: *eMRTD, PKI technology, biometric devices, travel document authentication, border security, fraud prevention, data protection.*

Într-o lume în care călătoriile internaționale sunt tot mai frecvente și securitatea devine o prioritate tot mai stringentă, autentificarea documentelor de călătorie cu cip eMRTD devine o temă deosebit de importantă și actuală. Ne putem imagina o scenă în care un călător trece prin controlul de securitate la un aeroport internațional, unde un ofițer îi scanează rapid pașaportul și îi verifică identitatea în câteva secunde. Această tehnologie este posibilă datorită implementării tehnologiei PKI și a dispozitivelor biometrice în documentele de călătorie, o abordare integrată care redefinește standardul în materie de securitate și autentificare. Prin intermediul acestui articol, se propune explorarea în profunzime această abordare integrată, înțelegerea funcționării tehnologiei PKI și cum sunt utilizate dispozitivele biometrice pentru a asigura o autentificare robustă și eficientă în documentele de călătorie cu cip eMRTD.

Voi analiza implicațiile acestei tehnologii în ceea ce privește securitatea frontierei, prevenirea fraudei și protecția datelor personale,

* Ministerul Afacerilor Interne, Direcția Generală pentru Comunicații și Tehnologia Informației, email: melinte.alexandru@myunap.net.

precum și impactul său asupra experienței călătorilor. Prin intermediul unor studii de caz și a unor exemple concrete, vom ilustra beneficiile și provocările acestei abordări, oferind cititorilor o viziune cuprinzătoare asupra acestui subiect de actualitate. Partea 10 a Documentului 9303[1] reprezintă o fereastră către lumea complexă a pașapoartelor electronice moderne și a necesității acestora pentru interoperabilitate globală. Această secțiune esențială definește Structura Logică a Datelor (LDS) pentru eMRTD-uri, punând bazele pentru o gestionare eficientă și securizată a informațiilor pe cipul contactless integrat. Partea 10 a Documentului 9303 stabilește standarde, identificând atât Elementele de Date obligatorii, cât și pe cele opționale, și oferind orientări clare pentru organizarea acestora pe cipul contactless. Prin intermediul acestui document, statele și integratorii au la dispoziție un cadru riguros pentru implementarea cipurilor contactless în documentele de călătorie electronice. Structura LDS definește nu numai elementele esențiale de date și structurile fișierelor, ci și profilurile aplicațiilor necesare pentru asigurarea interoperabilității globale. Ediția a opta a Documentului 9303 aduce o evoluție semnificativă, încorporând specificațiile pentru aplicații opționale precum Înregistrările de Călătorie și Biometricele Adiționale, extinzând astfel funcționalitatea pașapoartelor electronice dincolo de ceea ce era anterior posibil.

În contextul dezvoltării pașapoartelor electronice, este crucial să înțelegem structura logică a datelor stocate pe cipul contactless al acestora. Conform specificațiilor de aplicare, selecția aplicației trebuie realizată utilizând un identificator de aplicație (AID), conform standardului ISO/IEC 7816-5." Schema de ordonare aleatorie permite înregistrarea datelor într-o ordine aparent aleatorie, dar care este consistentă cu capacitatea tehnologiei de extindere pentru a permite accesul direct la anumite elemente de date. Această abordare asigură eficiența și optimizarea facilității de utilizare pentru titularul legitim al pașaportului.

Pentru a garanta autenticitatea și integritatea datelor stocate pe cipul contactless al pașaportului, fiecare grup de date trebuie să fie reprezentat într-un obiect de autenticitate și integritate. Acest obiect este înregistrat într-un fișier separat (EF.SOD), iar utilizarea structurii de schimb biometric comun (CBEFF) poate oferi protecție suplimentară pentru detalii precum șabloanele biometrice. Pentru a asigura interoperabilitatea la nivel global, pașapoartele electronice trebuie să fie conforme cu standardele stricte stabilite de ISO/IEC 14443 și ISO/IEC 10373-6. Aceste standarde definesc cerințele esențiale pentru comunicarea și securitatea datelor pe cipurile contactless, precum și pentru testarea și certificarea acestora. Astfel, ele stabilesc baza pentru funcționarea corespunzătoare a pașapoartelor electronice și a cititoarelor acestora. Caracteristicile electrice și fizice ale pașapoartelor electronice sunt esențiale pentru o comunicare eficientă cu cititoarele și pentru o interacțiune fluentă între dispozitive. De exemplu,

[1] Machine Readable Travel Documents, disponibil la https://www.icao.int/-publications/Documents/9303_p10_cons_en.pdf, accesat la 23.04.2024.

conformitatea cu standardul ISO/IEC 14443-2 pentru interfața radiofrecvență și dimensiunile antenei conforme cu Clasa 1 din ISO/IEC 14443-1 asigură compatibilitatea și stabilitatea comunicațiilor între pașapoarte și cititoare. Protocolul de transmisie este o altă componentă critică a specificațiilor comune, Acesta trebuie să fie conform cu standardele ISO/IEC 14443, asigurând inițializarea corectă, anticoliziunea și transmiterea datelor în mod eficient. Suportul pentru protocoalele de transmisie Tip A sau Tip B este esențial pentru compatibilitatea cu diferite tipuri de cititoare. Odată selectate, aplicațiile de pe cipurile contactless necesită un set corespunzător de comenzi pentru a funcționa adecvat . De exemplu, comenzi precum SELECT și READ BINARY sunt esențiale pentru accesarea și citirea datelor stocate în cip. Implementarea corespunzătoare a acestor comenzi este vitală pentru gestionarea eficientă a informațiilor de călătorie și pentru asigurarea securității acestora.

Metoda de citire a datelor din pașaportul electronic poate fi realizată în două moduri: selectând fișierul electronic (EF) și apoi citind datele din EF-ul selectat, sau citind direct datele folosind identificatorul scurt al EF-ului. Suportul pentru identificatorul scurt al EF-ului este obligatoriu pentru pașaportul electronic. Prin urmare, este recomandat ca sistemul de inspecție să utilizeze identificatorul scurt al EF-ului pentru a asigura compatibilitatea și eficiența citirii datelor În contextul cerințelor extinse pentru suportul lungimii extinse (Extended Lc/Le), este important să subliniem că, în funcție de dimensiunea obiectelor criptografice, cum ar fi cheile publice sau semnăturile, trebuie utilizate APDU-uri (Application Protocol Data Units) cu câmpuri de lungime extinsă pentru a trimite aceste date către cipul eMRTD. Detaliile privind aceste câmpuri de lungime extinsă pot fi găsite în [ISO/IEC 7816-4] . Pentru cipurile eMRTD, suportul pentru câmpul de lungime extinsă este condiționat de algoritmele criptografice și dimensiunile cheilor selectate de statul emitent. Dacă acestea necesită utilizarea câmpului de lungime extinsă, cipurile eMRTD trebuie să ofere suport pentru aceasta, conform specificațiilor [ISO/IEC 7816-4]. Acest lucru trebuie indicat în ATS (Answer to Select) sau în EF.ATR/INFO (Elementary File Answer to Reset / Information). Pe de altă parte, pentru terminale, suportul pentru câmpul de lungime extinsă este obligatoriu. Un terminal ar trebui să verifice dacă suportul pentru acest câmp este indicat în ATS-ul sau ATR-ul cipului eMRTD înainte de a utiliza această opțiune. Este esențial ca terminalul să nu utilizeze câmpul de lungime extinsă pentru APDU-uri în afara comenzilor specificate, cu excepția situațiilor în care dimensiunile exacte ale bufferelor de intrare și ieșire ale cipului eMRTD sunt explicit indicate în ATS sau în EF.ATR/INFO. În plus, este important să menționăm și utilizarea lanțurilor de comenzi (Command Chaining) și gestionarea fișierelor EF mai mari de 32 767 de octeți. Aceste cerințe suplimentare și modalități de interacțiune sunt esențiale pentru asigurarea unui flux de date eficient și compatibil între cipurile eMRTD și terminalele utilizate în procesul de verificare și autentificare a pașapoartelor electronice.

Capacitatea de stocare a datelor pe cipul contactless este la discreția statului emitent, însă trebuie să fie de minim 32 kB conform specificațiilor. Această capacitate minimă este necesară pentru a stoca imaginea facială obligatorie, datele MRZ (Machine Readable Zone) și elementele necesare pentru securizarea datelor. Totuși, dacă se dorește stocarea unor imagini suplimentare, precum cele faciale, ale amprentelor digitale sau ale irisului, poate fi necesară o creștere semnificativă a capacității de stocare a datelor. Nu există o limită maximă specificată pentru capacitatea de stocare a datelor pe cipul contactless. Cu toate acestea, trebuie să se asigure că acesta poate stoca toate informațiile necesare și că are suficient spațiu pentru eventualele extinderi sau actualizări ale datelor. În cazul în care infrastructura PKI a unui stat nu este disponibilă pentru a semna datele eMRTD conform personalizării, iar emiterea documentului sau documentelor nu poate fi amânată, se recomandă ca cipul contactless LDS1 eMRTD să fie lăsat gol și blocat. Acest lucru ar trebui menționat printr-o notificare adecvată pe documentul eMRTD. Este important de subliniat că această situație este considerată a fi excepțională și trebuie gestionată în mod corespunzător pentru a asigura securitatea și integritatea datelor.

În documentul menționat[2], se evidențiază posibilitatea ca statele să valorifice capacitatea de stocare a documentelor de călătorie cu citire electronică (eMRTD) pentru a adăuga informații suplimentare, depășind astfel limitele definite global pentru interoperabilitate. Această abordare deschide calea către includerea detaliilor extinse în eMRTD-uri, precum certificatele de naștere sau datele biometrice pentru confirmarea identității. Ulterior, se conturează tranziția către ISO/IEC 39794 ca standard internațional pentru codificarea datelor biometrice, înlocuind versiunea anterioară, ISO/IEC 19794:2005. Această actualizare impune echipamentelor de citire a pașapoartelor să se adapteze noilor standarde până la o anumită data limită, pentru a asigura compatibilitatea și eficiența în procesul de verificare a identității. Pe de altă parte, în cadrul secțiunii dedicate structurii Logică de Date (LDS) pentru eMRTD-uri, se oferă o perspectivă asupra fișierului elementar EF.COM. Acesta nu numai că poate conține informații esențiale precum versiunea LDS și lista datelor disponibile în aplicație, dar servește și drept ancoră pentru interoperabilitate și eficiența pașapoartelor electronice în context global.

În continuare, se adaugă o nouă dimensiune discuției privind structura Logică de Date (LDS) pentru documentele de călătorie cu citire electronică (eMRTD). Este important de precizat că fiecare eMRTD trebuie să includă un antet și o hartă a prezenței grupurilor de date, ceea ce permite statelor sau organizațiilor aprobate să localizeze și să decodeze diversele grupuri de date și elemente de date conținute în blocul de date înregistrat de statul sau organizația emitentă. Ulterior, se face o recomandare cu privire la utilizarea sistemelor de inspecție(IS) care se bazează pe fișierul EF.COM, sugerându-se modificarea acestora pentru a utiliza obiectul de securitate a

[2] Idem.

documentului SOD (Security object document). Această recomandare evidențiază necesitatea adaptării la noile standarde pentru a asigura o compatibilitate și securitate sporită în procesul de verificare a documentelor de călătorie. În ceea ce privește versiunile LDS și Unicode, precum și obiectul de securitate a documentului (SOD), se impune respectarea unor formate standardizate pentru a facilita interoperabilitatea și protecția datelor. În special, se subliniază importanța respectării setărilor de siguranță și a standardelor pentru a asigura integritatea și autenticitatea datelor stocate în eMRTD-uri. De asemenea, aici este important de menționat că în cadrul documentelor de călătorie cu citire electronica, triada CIA - Confidențialitate, Integritate și Disponibilitate - reprezintă o componentă fundamentală pentru asigurarea securității și protecției datelor. Confidențialitatea se referă la garantarea că informațiile personale stocate în documentele de călătorie sunt accesibile numai de către persoanele autorizate, reducând astfel riscul expunerii la fraudă sau utilizare neautorizată a datelor. Integritatea implică menținerea acurateței și autenticității datelor stocate în eMRTD, pentru a preveni modificările sau alterările neautorizate care ar putea afecta validitatea documentelor. Disponibilitatea se referă la asigurarea că datele sunt accesibile și utilizabile atunci când este necesar, garantând astfel că documentele de călătorie pot fi utilizate eficient și fără întârzieri în procesele de verificare și control la frontieră. Aceste adăugiri completează pe deplin înțelegerea necesității și a beneficiilor implementării unor standarde clare și actualizate în cadrul sistemelor de gestionare a documentelor de călătorie. Astfel, ulterior, vom discuta despre impactul acestor actualizări asupra procesului de călătorie și a securității în contextul internațional. Prin urmare, introducerea tehnologiilor avansate, cum ar fi sistemele de check-in online, verificarea biometrică și monitorizarea bagajelor în timp real, a simplificat și eficientizat experiența călătorilor. În același timp, măsurile de securitate au fost îmbunătățite prin utilizarea inteligenței artificiale și a partajării internaționale de informații, sporind protecția împotriva amenințărilor. Cu toate acestea, implementarea acestor tehnologii aduce provocări legate de costuri și confidențialitatea datelor, dar beneficiile în termeni de eficiență și siguranță sunt semnificative.

În continuare, voi aborda detalii care se referă la elementele de date care alcătuiesc Grupurile de Date 1 până la 16 din pașapoartele electronice. Fiecare grup de date (de la DG1 la DG16 (data groups)) este compus dintr-un număr de elemente de date obligatorii, opționale și condiționale. Ordinea specificată a elementelor de date trebuie respectată, iar fiecare grup de date trebuie stocat într-un fișier transparent EF, adresarea fișierelor EF făcându-se prin identificatorul EF scurt. Fișierele EF trebuie să aibă nume conform numărului n, EF.DGn, unde n reprezintă numărul grupului de date. În cadrul acestor grupuri de date, există informații obligatorii și opționale care formează structura generală a documentului. De exemplu, DG1 conține informații despre zona lizibilă de mașină (MRZ) a documentului, care trebuie să fie stocate conform unui template specific. Aceste informații

includ codul documentului, țara emitentă, numărul documentului, data nașterii, sexul, data expirării, naționalitatea și altele. De asemenea, voi discuta despre cum sunt stocate și codificate aceste elemente de date în funcție de formatul MRZ (TD1, TD2 sau TD3) și vom explora detaliile privind encodarea caracteristicilor biometrice, cum ar fi fotografia facială, conform standardelor ISO/IEC. Este important de menționat că în scopul interoperabilității internaționale, prima biometrie înregistrată în fiecare Grup de Date trebuie să fie codificată conform standardului ISO/IEC 19794-5.

După studii aprofundate, am constatat că Grupul de Date 2 (DG2) constituie o componentă esențială pentru asigurarea interoperabilității biometrice la nivel global în documentele de călătorie. Acesta reprezintă o imagine a feței titularului, furnizând un element critic pentru confirmarea identității în sistemele de securitate și control la frontieră. Conform standardelor ISO/IEC, am identificat că utilizarea șablonului de grup pentru informații biometrice (BIT) cu șabloane BIT înglobate permite stocarea eficientă a mai multor șabloane biometrice într-o manieră armonioasă cu CBEFF. Pentru a asigura coerența și eficiența în stocarea și gestionarea acestor date, am recomandat codificarea conform standardului ISO/IEC 19794-5, facilitând astfel interoperabilitatea și aplicabilitatea internațională a informațiilor biometrice. De asemenea, am constatat că Grupul de Date 3 (DG3) reprezintă o opțiune facultativă, dar semnificativă, pentru statele membre care doresc să utilizeze recunoașterea amprentelor digitale ca tehnologie biometrică suplimentară în sprijinul confirmării identității asistate.

După investigații detaliate, am constatat că atât Grupul de Date 3 (DG3), cât și Grupul de Date 4 (DG4) reprezintă componente opționale, dar semnificative, ale documentelor de călătorie bazate pe tehnologia biometrică. DG3 este dedicat recunoașterii amprentelor digitale, în timp ce DG4 se concentrează pe utilizarea recunoașterii irisului.

Grupurile de Date 5 (DG5) până la 12 (DG12) sunt componente esențiale ale structurii logice de stocare a datelor în cipurile integrate ale documentelor de călătorie. DG5 este dedicat reprezentării portretelor vizuale, oferind un mecanism pentru confirmarea vizuală a titularului documentului. Pe de altă parte, DG6 este rezervat pentru utilizare viitoare, menținând flexibilitatea sistemelor de documente de călătorie în fața schimbărilor tehnologice. DG7 este destinat reprezentării semnăturilor sau semnelor obișnuite ale titularului, facilitând autentificarea documentului. La fel ca și DG6, DG8 și DG9 sunt rezervate pentru utilizare ulterioară, pregătind terenul pentru îmbunătățiri și extinderi viitoare ale funcționalității sistemelor de documente de călătorie. Pe de altă parte, DG10 este destinat reprezentării detaliilor substanțiale, iar DG11 și DG12 sunt dedicate adăugării de detalii personale suplimentare, contribuind la asigurarea autenticității și integrității procesului de identificare al călătorului.

În continuare, propun să discutăm despre LDS2 (Logical Data Structure 2), care reprezintă o extensie opțională și compatibilă cu LDS1 pentru cipurile eMRTD, care ar permite stocarea digitală și securizată a

informațiilor de călătorie, după ce documentul a fost emis. Această extensie extinde utilizarea eMRTD prin adăugarea de aplicații care ar putea permite stocarea digitală a datelor de călătorie (vize și ștampile de călătorie) și a altor informații care ar putea facilita călătoria titularului (biometrice suplimentare) pe durata valabilității sale. Folosirea completă a potențialului eMRTD prin „digitalizarea" restului datelor conținute în documente oferă o serie de beneficii de facilitare, în timp ce protejează documentul împotriva vulnerabilităților precum falsificarea, copierea și citirea sau scrierea neautorizată.

Aplicațiile suplimentare și opționale descrise ca fiind parte a LDS2 sunt: *Înregistrările de călătorie (ștampilele), vizele electronice,* sau alte biometrice suplimentare. În cadrul aplicației *înregistrărilor de călătorie,* stocarea înregistrărilor de intrare și ieșire din călătorie se face în două fișiere elementare separate, EF.EntryRecords și EF.ExitRecords, sub aplicația Înregistrărilor de Călătorie DF. Acestea au ambele o structură liniară cu înregistrări de dimensiuni variabile conform [ISO/IEC 7816-4]. De asemenea, certificatele semnatarului pentru Înregistrările de Călătorie sunt stocate într-un fișier elementar separat, EF.Certificates, având o structură liniară cu înregistrări de dimensiuni variabile. În cadrul aplicației *vizelor,* înregistrările de viză sunt stocate în fișierul elementar EF.VisaRecords, care are, de asemenea, o structură liniară cu înregistrări de dimensiuni variabile. Certificatele semnatarului pentru aceste înregistrări sunt stocate în EF.Certificates, sub aplicația Vizelor.

Pentru a asigura interoperabilitatea și performanța corespunzătoare a eMRTD-urilor, este esențial să se țină cont de specificațiile tehnice detaliate. De exemplu, dimensiunea și poziționarea antenei sunt la latitudinea statului emitent, cu diverse opțiuni pentru plasarea cipului și a antenei în structura documentului. Este recomandat ca eMRTD-urile să respecte specificațiile Clasei 1 conform [ISO/IEC 18745-2].

eMRTD-urile trebuie să suporte anumite rate de biți obligatorii, precum 106 kbit/s și 424 kbit/s, dar pot oferi și suport opțional pentru rate de biți mai mari. De asemenea, se recomandă utilizarea unui identificator unic aleatoriu (UID (Unique Identifier)[3] /PUPI (Pseudo-Unique PICC Identifier)[4] pentru a spori confidențialitatea și pentru a reduce riscul de urmărire.

Pentru a asigura conformitatea și eficiența în utilizarea e-MRTD-urilor, sistemele de inspecție trebuie să îndeplinească specificații tehnice riguroase. Aceste sisteme trebuie să aibă un volum de operare adecvat conform specificațiilor ISO/IEC 18745-2 și să utilizeze forme de undă corespunzătoare pentru comunicarea magnetică. De asemenea, intensitatea câmpului magnetic trebuie să fie de cel puțin 2 A/m pentru sistemele de tip 1, 2 și 3, respectiv 1,5 A/m pentru sistemele de tip M. Secvențele de interogare trebuie să asigure o detecție rapidă și eficientă a eMRTD-urilor,

[3] Este un cod unic, fie fix, fie generat aleatoriu, care identifică în mod specific un eMRTD.
[4] Este un identificator care funcționează similar cu UID, dar este proiectat să fie unic doar într-un anumit context sau pentru o anumită perioadă de timp.

incluzând un semnal nemodulat de 10 ms înainte de orice comandă REQA/WUPA (Request A/Wake-Up A)[5] sau REQB/WUPB (Request B/Wake-Up B)[6]. Sistemele de inspecție trebuie să suporte rate de biți obligatorii de 106 kbit/s și 424 kbit/s în ambele direcții, cu opțiunea de a suporta rate de până la 27.12 Mbit/s. Suportul pentru distorsiuni electromagnetice (EMD) nu este obligatoriu, dar poate îmbunătăți comunicarea contactless. Sistemele trebuie să fie compatibile cu cel puțin clasa 1 de antene și, opțional, cu clasele 2 și 3. De asemenea, este recomandat ca aceste sisteme să funcționeze în intervalul de temperatură de -10°C până la 50°C și să fie capabile să gestioneze multiple eMRTD-uri sau alte carduri contactless simultan, utilizând algoritmi și mecanisme de recuperare a erorilor.

În final, articolul a desfășurat o panoramă detaliată a sistemului de securitate și gestiune a datelor din documentele de călătorie electronice. De la standardele tehnice precum LDS și LDSSecurityObject, până la exemple practice de comenzi și proceduri specifice, am explorat esența complexă a acestui domeniu crucial pentru securitatea și eficiența călătoriilor internaționale. Cu tehnologia în continuă evoluție și cerințele de securitate tot mai stricte, acest domeniu rămâne în centrul inovației și al eforturilor noastre de a facilita o experiență de călătorie.

BIBLIOGRAFIE

Machine Readable Travel Documents, disponibil la https://www.icao.int/-publications/Documents/9303_p10_cons_en.pdf.

[5] Folosite pentru dispozitivele de tip A, REQA inițiază interogarea, iar WUPA trezește dispozitivele din modul de așteptare.

[6] Folosite pentru dispozitivele de tip B, REQB inițiază interogarea, iar WUPB trezește dispozitivele din modul de așteptare.