Tehničko uputstvo

Napredni sigurnosni mehanizmi za mašinski čitljive putne dokumente

2. Dio – Proširena kontrola pristupa Verzija 2 (EACv2), "Password Authenticated Connection Establishment" (PACE) i ograničena identifikacija(RI)

Banja Luka, 01.03.2013. godine

Sadržaj

1 Uvod

Sistem elektronskih dokumenata je razvijen na bazi dokumenata Njemčkog instituta za IT i IDDEEA se zahvaljuje na dostupnosti dokumenata na zvaničnim sajtovima BSI.

Ovaj dio tehničkog uputstva obuhvata elektronske sigurnosne mehanizme za elektronske putne dokumente opisane u Doc 9303 dio 3 tom 2 [4] za zaštitu autentičnosti (uključujući integritet), orginalnost i pouzdanost podataka koji su sačuvani na radio frekventnom čipu ugrađenom u putni dokument. (MRTD čip).

Napomena: Ukoliko se zahtjeva usklađenost sa ICAO Doc 9303 [3], [4], Basic Access Control/PACE i Ex- tended Access Control u verziji 1(koji uključuje autentifikaciju čipa, verzija 1 i autentifikaciju terminala verzija 1) se MORAJU koristiti (vidi 1.dio ovog tehničkog uputstva).

1.1 Zahtjevi za MRTD čipove i terminale

Ovo tehničko uputstvo definiše zahtjeve za implementaciju MRTD čipova i terminala. Dok se MRTD čipovi moraju uskladiti sa zahtjevima u skladu sa terminologijom opisanom u odjeljku 1.2, zahtjevi za terminale se moraju tumačiti kao smjernice, tj. interoperabilnost MRTD čipa i terminala je zagarantovani ako je terminal usklađen sa tim zahtjevima, inače će interakcija sa MRTD čipom biti neuspješna ili će ponašanje MRTD čipa biti nedefinisano. U principu, MRTD čip ne treba sprovoditi zahtjeve vezane za terminale osim ako je sigurnost MRTD čipa direktno narušena.

1.2 Terminologija

Ključne riječi “MORA”, “NE MORA”, “ZAHTJEVANO”, BIĆE”, “ NEĆE BITI”, “TREBA”, “NE TREBA”, “PREPORUČENO”, “MOŽE”, i “OPCIONALNO” u ovom dokumentu se mogu tumačiti kao što je opisano u RFC 2119 [1]. Ključna riječ “USLOVNO” će se tumačiti na sljedeći način:

USLOVNO: Upotreba jedne stavke zavisi od upotrebe drugih stavki. Stoga je dalje kvalifikovano pod kojim uslovima je stavka ZAHTJEVANA ili PREPORUČENA.

Kada se koristi u tabelama (profilima), ključne riječi su skraćena što je prikazano u tabeli 1.

Ključna riječ		Skraćenica
MORA/BIĆE	ZAHTJEVANO	M
NE MORA/NEĆE BITI	–	X
TREBA	PREPORUČENO	R
MOŽE	OPCIONALNO	O
–	USLOVNO	C

Tabela 1: ključne riječi 1

2 MRTD aplikacije

U okviru ovog poglavlja su nabrojane elektronske aplikacije koje se nalaze u mašinski čitljivim dokumentima.

2.1 Aplikacije

Ova specifikacija podržava tri aplikacije: *ePasoš*, *eID*, and *ePotpis*.

2.1.1 ePasoš aplikacija

ePasoš aplikacija je opisana u 1. dijelu ovog tehničkog uputstva. Izdavalac MRTD implementirane u skladu sa ovim dijelom ovog tehničkog uputstva MOŽE definisati uslove pristupa drugačije od onih

u dijelu 1. PREPORUČUJE se da se zahtjeva Extended Access Control čak i za manje osjetljive podatke.

2.1.2 eID aplikacija

eID aplikacija je definisana u Prilogu A i zahtjeva da se ovjeri terminal na sljedeći način:

- Da bi pisali na eID aplikaciju, MRTD chip ĆE zahtjevati da se ovjeri terminal kao terminal za autentifikaciju sa autorizacijom za pisanje odgovarajućih grupa podataka eID aplikacije.
- Da bi očitavali sa eID aplikacije, MRTD čip ĆE zahtjevati da se ovjeri terminal kao
  - Terminal za autentifikaciju sa autorizacijom da se očitavaju sve grupe podataka sa eID aplikacije ili kao
  - Inspekcijski sistem koji podrazumjeva autorizaciju za očitavanje svih grupa podataka eID aplikacije.

Da bi se ovjerio terminal kao terminal za autentifikaciju ili inspekcijski sistem, MORA se koristiti Procedura opšte autentifikacije (vidi Odjeljak 2.4).

2.1.3 ePotpis aplikacija

Ova specifikacija ne zahtjeva usklađenost sa određenim standardom, ali zahtjeva da se terminal ovjeri na sljedeći način:

- Za instaliranje ePotpis aplikacije, MRTD čip ĆE zahtjevati da se terminal ovjeri kao terminal za autentifikaciju sa posebnom autorizacijom za instaliranje ePotpis aplikacije.
- Za korištenje ePotpis aplikacije da bi se napravili potpisi, MRTD ĆE zahtjevati da se ovjeri terminal kao teriminal za potpis.

Da bi se ovjerio terminal kao terminal za autentifikaciju ili terminal za potpis, MORA se koristiti Procedura opšte autentifikacije (vidi Odjeljak 2.4).

2.2 Tipovi terminala

Ova specifikacija obuhvata tri tipa terminala: inspekcijski sistem, terminali za autentifikaciju i terminali za potpis.

2.2.1 Inspekcijski sistem

Pored specifikacija navedenih u 1. Dijelu ovog tehničkog uputstva, ovaj dio obuhvata definisanje proširenog inspekcijskog sistema koji podržava Opštu proceduru autentikacije (vidi odjeljak 2.4).

> *Napomena: U nastavku se inspekcijski sistem uvijek podrazumjeva kao prošireni inspekcijski sistem.*

2.2.2 Terminal za autentifikaciju

Terminal za autentifikaciju je terminal koji može da se koristi od strane institucija na nivou BiH (institucija nadležna za verifikaciju dokumenata) ili bilo koje druge organizacije (seslužbena / strana organizacija za verifikaciju dokumenata). MRTD čip ĆE zahtjevati da se terminal za autentifikaciju autentifikuje kako bi se prije pristupa utvrdila autentičnost u skladu sa važećom autorizacijom. Da bi se autentifikovao terminal kao terminal za autentifikaciju, MORA se koristiti Opšta procedura autentifikacije (vidi Odjeljak 2.4). Nivo autorizacije terminala za autentifikaciju ĆE BITI određen važećom autorizacijom izračunatom iz lanca certifikata.

2.2.3 Terminal za potpis

Terminal za potpis MORA biti odobren od strane nadležnog ovlaštenog organa ili certifikacijskog pružaoca usluga. MRTD čip ĆE zahtijevati da se terminal za potpis autentifikuje kako bi se prije pristupa utvrdila autentičnost u skladu sa važećom autorizacijom. Da bi se autentifikovao terminal kao terminal za potpis, MORA se koristiti Opšta procedura autentifikacije (vidi Odjeljak 2.4). Nivo autorizacije terminala za potpis ĆE BITI određen važećom autorizacijom izračunatom iz lanca certifikata.

2.2.4 Privilegovan terminal

MRTD čip MOŽE biti personalizovan tako da podržava i individualne čip i generički specifične ključeve za autentifikaciju čipa. U tom slučaju, MRTD ĆE ograničiti pristup individualnim čip ključevima na *privilegovane terminale.* MRTD čip MORA smatrati sljedeće terminale kao privilegovane terminale:

- Inspekcijski sistemi su uvijek privilegovani terminali.
- Terminali za autentifikaciju sa važećom autorizacijom „Privileged Terminal“ (3. Dio ovog tehničkog uputstva).

Terminali za potpis se nikad NEĆE smatrati privilegovanim terminalima.

2.3 Šifre

Osnovna i proširena kontrola pristupa moraju biti definisane da bi se dozvolilo nosiocu MRTD da kontroliše pristup aplikacijama implementiranim na bezkontaktnom MRTD čipu. Zbog ograničenja osnovne kontrole pristupa, ova specifikacija uvodi PACE kao sigurnosni i praktični mehanizam za ograničenje pristupa aplikacijama na osnovu znanja, tj. na osnovu šifri koje su ili odštampane na dokumentu ili poznate samo legitimnom nosiocu dokumenta.

Šifre podržane ovim dijelom tehničkog uputstva pored onih podržanih u 1.dijelu su:

PIN: Lični identifikacioni broj (PIN) je kratka tajna šifra koja ĆE BITI poznata jedino legitimnom nosiocu dokumenta.

PUK: Lični broj za deblokiranje (PUK) je duga tajna šifra koja ĆE BITI poznata jedino legitimnom nosiocu dokumenta.

2.3.1 PIN

PIN je kratka tajna korisnička šifra koja se koristi za pristup eID aplikaciji ili drugim aplikacijama. Upotreba PIN-a je ZAHTJEVANA za sve terminale za autentifikaciju, tj. jedino legitimni nosioc može dozvoliti terminalu za autentifikaciju da pristupi podacima na eID aplikaciji, osim ako terminal ima važeću autorizaciju za pristup podacima eID aplikacije sa CAN broj.

PIN je šifra koja se blokira, tj. PIN je povezan sa brojačem ponavljanja (RC) koji se smanjuje za svaku neuspješnu autentifikaciju. MRTD čip ĆE primijeniti sljedeću proceduru blokiranja kako bi se spriječilo odbijanje napada na servise:

RC = 0 MRTD čip ĆE *blokirati* PIN, tj. MRTD čip NE SMIJE prihvatiti dalje pokušaje autentifikacije koristeći blokirani PIN. Da bi se blokirani PIN *deblokirao* MORA se koristiti procedura deblokiranja kako bi se resetovao odgovarajući brojač ponavljanja i gdje je moguće, podesio novi PIN.

2.3.2 PUK

PUK je duga tajna korisnička šifra koja se koristi za pristup deblokiranim mehanizmima PIN-a i šiframa specifičnih aplikacija (npr. lokalni PIN ePotpis aplikacije).

PUK je šifra koja ne blokira, tj. MRTD čip NE SMIJE blokirati PUK nakon neuspješnih autentifikacija. Međutim, MOŽE povezati PUK sa brojačem korisnika koji se smanjuje sa svakom uspješnom autentifikacijom.

2.4 Procedura opšte autentifikacije

MRTD čip MORA ograničiti pristup eID aplikaciji i ePotpis aplikaciji terminalima koji su autentifikovani opštom procedurom autentifikacije kao proširenog inspekcijskog sistema, terminala za autentifikaciju i terminala za potpis u skladu sa važećom autorizacijom.

Pristup ePasoš aplikaciji MORA biti ograničen inspekcijskim sistemima,a procedurom opšte autentifikacije PREPORUČENO je zahtjevati da terminal bude autentifikovan kao prošireni inspekcijski sistem.

MRTD čip MORA podržavati reautentifikaciju terminala procedurom opšte autentifikacije nakon što je sesija (vidi odjeljak. „Sigurno slanje poruka“ u 3.dijelu ovog tehničkog uputstva pod definicijom „sesija“) završena i terminal je izabrao Master File.

Procedura opšte autentifikacije se sastoji od slijedećih koraka:

1. PACE **(ZAHTJEVANO)**

Terminal MORA navesti tip terminala i zahtjevana prava pristupa kao dio PACE-a. Ukoliko nije navedeno, MRTD čip MORA naknadno odbiti autentifikaciju terminala verzija 2 .

- Inspekcijski sistem ĆE koristiti CAN broj ili MRZ šifru.
- Terminal za autentifikaciju ĆE koristiti PKIN. MOŽE koristiti CAN broj ukoliko važeća autorizacija terminala odobro korištenje CAN broja („CAN broj dozvoljen).
- Terminal za potpis ĆE koristiti PIN; CAN broj ili PUK.

Ako je uspješno, MRTD čip poduzima slijedeće:

- POČEĆE sigurno slanje poruka.

OSIGURATI TRUST+POINTS za autentifikaciju teminala

2. Autentifikacija terminala verzija 2 (ZAHTJEVANO)

Kao dio terminala za autentifikaciju, terminal obavlja sljedeće:

- Terminal ĆE generisati privremeni javni ključ koji će se kasnije *koristiti* za autentifikaciju čipa. Terminal NE SMIJE koristiti neverifikovane domenske parametre za ovaj ključ, tj. jedino standardizovani parametri domena ili parametri domena terminala koji su sigurni mogu biti korišteni.
- Terminal ĆE autentifikovati generisani privremeni javni ključ.

Ukoliko je uspješno, MRTD čip obavlja sljedeće korake:

- ODOBRIĆE pristup očitavanju/pisanju grupi podataka u skladu sa pravima pristupa terminalima.
- OGRANIČIĆE ona prava pristupa Sigurnom slanju poruka koji je uspostavljen autentifikovanim privremenim javnim ključem (osim odgovarajući objekat sigurnosti).

3. Pasivna autentifikacija (ZAHTJEVANO)

Terminal obavlja sljedeće:

- Terminal ĆE očitavati i verifikovati odgovarajući sigurnosni objekat.
- Terminal ĆE uporediti nesigurne SecurityInfos očitane prije PACE-a sa sigurnim sadržajem objekta sigurnosti.

4. Autentifikacija čipa verzija 2 (ZAHTJEVANO)

MRTD čip ĆE resetovati sigurnu razmjenu poruka.

Terminal za autentifikaciju može odabrati i koristiti aplikaciju(e) u skladu sa važećom autorizacijom terminala.

Napomena: Terminal i MRTD čip MORAJU koristiti uspostavljeni sigurnosni kontekst (tj. Sigurna razmjena poruka ustanovljena autentifikacijom čipa) za svu dalju komunikaciju.

2.4.1 Online autentifikacija

eID aplikacija se takođe može koristiti online, tj. MRTD čip i terminal za autentifikaciju su povezani mrežom. U tom slučaju razlikujemo *lokalni terminal* i *udaljeni terminal*:

Udaljeni terminal: Udaljeni terminal je autorizovan za pristup eID podacima. On pruža lokalnom terminalu lanac certifikata autentifikacije terminala i digitalni potpis kreiran na upitu MRTD čipa sa odgovarajućim tajnim ključem.

Lokalni terminal: Lokalni terminal povezuje korisnika sa MRTD čipom i udaljenim terminalom ali nije autorizovan za pristup eID podacima. Lanac certifikata autentifikacije terminala primljen od udaljenog terminala je prikazan korisniku i, samo ako to korisnik prihvata, lokalni terminal proslijeđuje primljene certifikate MRTD čipu.

Napomena: Jedino nakon autentifikacije čipa kada je uspostavljena sigurna end-to-end veza između MRTD čipa i udaljenog terminala, MRTD čip odobrava pristup eID podacima.

2.5 Upravljanje PIN-om

PIN i CAN su jedine šifre (korištene za PACE) koje se mogu mijenjati. PIN je jedina šifra koja može imati statuse suspendovan i blokiran. Pored toga, PIN može imati statuse aktiviran i deaktiviran. Preostale šifre (PUK i MRZ) su statične i ne mogu blokirati. Detaljno korištenje šifri je pojašnjeno u odjeljku 2.3.

Upravljanje PIN-om se sastoji od sljedećih operacija:

- Promjena CAN-a
- Promjena PIN-a
- Obnova PIN-a
- Deblokiranje PIN-a
- Aktiviranje PIN-a
- Deaktiviranje PIN-a

Mapiranje mehanizmima upravljanja PINom kao što su promijeniti CAN, promijeniti PIN, odblokirati PIN, aktivirati Pin, deaktivirati PIN prema direktivama ISO 7816 su data u 3.dijelu ovog tehničkog uputstva. Operacija obnoviti PIN nije mapirana prema direktivi ISO 7816 jer to implicitno vrši MRTD čip.

2.5.1 Neautentifikovani terminali

Terminal je *neautentifikovan* prije uspješnog završavanja autentifikacije terminala. Neautentifikovani terminali mogu obavljati operacije upravljanja PIN-om kako slijedi:

1. PACE **(ZAHTJEVANO)**

Terminal NE TREBA označavati vrstu terminala i zahtjevan prava pristupa ako terminal ostaje neautentifikovan. Terminal može izabrati CAN, PIN ili PUK kao šifru za PACE.

Ukoliko je uspješno, MRTD čip obavlja sljedeće:

- POČEĆE sigurnu razmjenu poruka.
- Ako je PIN u funkciji (tj. aktiviran, i nije suspendovan ili blokiran) i ako je pravilno upotrijebljen, MRTD čip obavlja sljedeće:
  - PONIŠIĆE broj ponavljanja PIN-a.
  - ODOBRIĆE pristup sljedećem mehanizmu upravljanja PIN-a : promjena PIN-a.
- Ukoliko je CAN pravilno upotrijebljen:
  - Privremeno ĆE obnoviti PIN.
- Ukoliko je PUK pravilno upotrijebljen:
  - ODOBRIĆE pristup sljedećem mehanizmu upravljanja PIN-a: deblokiranje PIN-a.
  - MOŽE odobriti pristup sljedećem mehanizmu upravljanja PIN-a: promjena PIN-a.

2. PACE sa PIN-om (OPCIONALNO)

Ovaj korak se ZAHTIJEVA u sljedećim slučajevima:

- obnavljanje PIN-a.
- nastavak procedure za opštu autentifikaciju nakon upravljanja PIN-om. U tom slučaju terminal MORA označiti tip terminala (terminala za autentifikaciju) i neophodna prava pristupa.1

Ako je PIN uspješno upotrijebljen i ako je funkcionalan i privremeno obnovljen, MRTD čip će obaviti sljedeće:

- Ako je PIN privremeno obnovljen, obnoviće PIN.
- RESETOVAĆE brojač ponavljanja PIN-a.
- ODOBRIĆE pristup sljedećem mehanizmu upravljanja PIN-a: promjena PIN-a.

3. Upravljanje PIN-om (OPCIONALNO)

Ovaj korak se ZAHTIJEVA kod promjene ili deblokiranja PIN-a.

MRTD čip će obaviti sljedeće:

- DOZVOLIĆE terminalu da izvrši sljedeće operacije upravljanja PIN-om:
  - Promjena PIN-a,ako terminal ima pristup ovoj operaciji.
  - Deblokiranje PIN-a, ako terminal ima pristup ovoj operaciji.

[1] Uglavnom je to slučaj kada se CAN koristi da bi se obnovio PIN kao dio procedure za opštu autentifikaciju.

Ukoliko je PUK povezan sa briojačem korisnika, on NE SMIJE isteći a MRTD čip ĆE smanjiti brojač korisnika ili nakon uspješnog izvođenja PACE protokola ili nakon izvršavanja operacije deblokiranje PIN-a.

Napomena: Podrška za operaciju promjena PIN-a upravljanja PIN-om ako je korišten PACE sa PUK-om je OPCIONALNA a implementacija specifična.

2.5.2 Terminali za autentifikaciju

Autentifikovani terminali sa važećom autorizacijom za upravljanje PIN-om (vidi 3.dio ovog tehničkog uputstva) mogu izvršavati sljedeće operacije upravljanja PIN-om:

1. **Procedura opšte autentifikacije**
   (ZAHTJEVANO)

   Ako je terminal autentifikovan kao terminal za autentifikaciju sa važećom autorizacijom za upravljanje PIN-om, MRTD čip vrši sljedeće:

   - DOZVOLIĆE pristup mehanizmima upravljanja PIN-om.

2. **Upravljanje PIN-om** **(ZAHTJEVANO)**

   MRTD čip vrši sljedeće:

   - MOŽE dozvoliti terminalu obavljanje sljedećih operacija upravljanja PIN-om :
     - Promjena PIN-a
     - Promjena CAN-a
     - Deblokiranje PIN-a
   - MORA dozvoliti terminalu obavljanje sljedećih operacija upravljanja PIN-om :
     - Aktiviranje PIN-a
     - Deaktiviranje PIN-a

Napomena: Podrška za operaciju upravljanja PIN-om promjena PIN-a i promjena CAN-a je OPCIONALNA a implementacija specifična.

2.6 MRTD-ovi sa ekranom

Ako je MRTD čip opremljen ekranom, MRTD čip će koristiti ekran na sljedeći način:

- PRIKAZAĆE selektovanu aplikaciju.
- Dinamično ĆE izabrati i prikazati CAN.
- PRIKAZAĆE identifikaciju autentifikovanog terminala i važeću autorizaciju.
- MOŽE prikazati promjenljive podatke eID aplikacije, npr. mjesto prebivališta.

3 Specifikacije protokola

U ovom poglavlju su navedeni kriptografski protokoli PACE, autentifikaciju čipa i terminala preuzimajući arbitrarnu komunikacijsku strukturu.. Mapiranje prema ISO 7816 naredbi je dato u 3.dijelu ovog tehničkog uputstva.

3.1 Kriptografski algoritmi i notacija

Protokoli koji su izvršeni između dvije strane: MRTD čip (PICC) i terminal (PCD). Tabela 2 daje prikaz korištenih parova ključeva. Korištene kriptografske operacije i notacije su navedene u nastavku.

3.1.1 Hash i kompresivni algoritmi

Operacije računanja kriptografskog hash-a i kompresivnih javnog ključa su opisane na zaseban algoritamski način.

3.1.1.1 Operacije

- operacija za računanje hash-a preko poruke m je označena sa $\mathbf{H}(m)$.
- operacija za računanje kompresovane reprezentacije javnog ključa PK je označena sa $\mathbf{Comp}(PK)$.

Protokol	MRTD Čip	Terminal	Napomena
PACE	$\widetilde{PK_{PICC}}$, $\widetilde{SK_{PICC}}$	$\widetilde{PK_{PCD}}$, $\widetilde{SK_{PCD}}$	Svi parovi ključeva su privremeni parovi ključeva.
Autentifikacija čipa	PK_{PICC}, SK_{PICC}	$\widetilde{PK_{PCD}}$, $\widetilde{SK_{PCD}}$	Par ključeva koje terminal koristi je privremeni par ključeva različit od privremenog PACE para ključeva.
Autentifikacija terminala	PK_{CVCA}	PK_{PCD}, SK_{PCD}	MRTD čip verifikuje lanac certifikata zaprimljen od terminala koristeći CVCA.
Ograničena identifikacija	SK_{ID}	PK_{SECTOR}	MRTD čip NE TREBA dostaviti javni ključ PK_{ID}, terminal NE SMIJE imati odgovarajući privatni ključ SK_{Sector}. Ključevi PK_{ID} i SK_{Sector} su korišteni eksterno za generisanje opozivnih lista.

Table 2: pregled korištenih parova ključeva

3.1.2 Algoritmi sa simetričnim ključem

Ključevi i operacije za simetričnu enkripciju ključa i autentifikaciju su opisani na zaseban algoritamski način.

3.1.2.1 Ključevi

Simetrični ključevi su izvedeni iz zajedničkog tajnog K i OPCIONALNOG r ili iz šifre π koristeći funkciju izvođenja ključa (DKF):

- Izvođenje ključa za enkripciju poruka je označeno sa $K_{Enc} = \mathbf{KDF_{Enc}}(K, [r])$.
- Izvođenje ključa za autentifikaciju poruka je označeno sa $K_{MAC} = \mathbf{KDF_{MAC}}(K, [r])$.
- Izvođenje ključa iz šifre je označeno sa $K_{\pi} = \mathbf{KDF}_{\pi}(\pi)$.

3.1.2.2 Operacije

Operacije za enkripciju i dekripciju poruka su označene na sljedeći način:

- Enkripcija teksta koji se šifruje *m* sa ključem K_{Enc} je označeno sa $c = \mathbf{E}(K_{Enc}, m)$.
- Dekripcija šifrovaog teksta *c* sa ključem K_{Enc} je označeno sa $m = \mathbf{D}(K_{Enc}, c)$.

Operacija za računanje autentifikacijskog koda *T* na poruci *m* sa ključem K_{MAC} je označeno sa

$T = \mathbf{MAC}(K_{MAC}, m)$.

3.1.3 Dogovor ključeva

Ključevi i operacije za dogovor ključeva su opisane na zaseban algoritamski način. Mapiranje prema DH i ECDH se može pronaći u 3.dijelu ovog tehničkog uputstva.

3.1.3.1 Ključevi

Sljedeći parovi ključeva se korste za PACE i autentifikaciju čipova:

- Za PACE, MRTD čip i terminal generišu privremene Diffie-Hellman parove ključeva na osnovu privremenih domena parametara $\widetilde{D}$.
  - Privremeni javni ključ MRTD čipa je $\widetilde{PK_{PICC}}$, odgovarajući tajni ključ je $\widetilde{SK_{PICC}}$.
  - Privremeni javni ključ terminala je $\widetilde{PK_{PCD}}$, odgovarajući tajni ključ je $\widetilde{SK_{PCD}}$.
- Za autentifikaciju čipa, MRTD čip koristi s statičan Diffie-Hellman par ključeva i terminal generiše privremeni javni ključ na osnovu domena parametara DPICC MRTD čipa.
  - Privremeni javni ključ MRTD čipa je PK_{PICC}, odgovarajući tajni ključ je SK_{PICC}.
  - Privremeni javni ključ terminala $\widetilde{PK_{PCD}}$, odgovarajući tajni ključ je $\widetilde{SK_{PCD}}$.
  - Kompresovani privremeni javni ključ terminala je označen sa **Comp(**$\widetilde{PK_{PCD}}$).
- Za ograničenu identifikaciju MRTD čip koristi statični Diffie-Hellman par ključeva i terminali u okviru sektora koriste (skoro) statičan Diffie-Hellman par ključeva gdje je privatni ključ terminalu nepoznat.
  - Statični javni ključ MRTD čipa je PK_{ID}, odgovarajući tajni ključ je SK_{ID}.
  - Statični javni ključ sektora je PK_{Sector}, odgovarajući tajni ključ je SK_{Sector}.
  - Opozivni javni ključ sektora je $PK_{Revocation}$, odgovarajući tajni ključ je $SK_{Revocation}$.
  - Specifični sektorski identifikator je $I^{Sector.}$.

PREPORUČENO je da MRTD čip testira javne ključeve dobijene od terminala.

Napomena: Terminal će morati koristiti različite privremene javne ključeve za PACE i autentifikaciju čipa. Obzirom da su privremeni javni ključevi u kontekstu specifični, koriste se ista notacija.

3.1.3.2 Operacije

Operacije za generisanje zajedničkih javnih ključeva *K* je označena sa $K = \mathbf{KA}(SK, PK, D)$, gdje je *SK* (privremeni ili statični) tajni ključ, *PK* (privremeni ili statični) javni ključ i *D* (privremeni ili statični) su parametri domena.

3.1.4 Potpisi

Ključevi i operacije za potpise su opisani na zaseban algoritamski način. Mapiranje prema RSA i ECDSA se može pronaći u 3.dijelu ovog tehničkog uputstva.

3.1.4.1 Ključevi

Za autentifikaciju terminala se koriste sljedeći par ključeva:

- Terminal ima statičan par ključeva za autentifikaciju. Javni ključ je PK_{PCD},, odgovarajući tajni ključ je SK_{PCD}.

3.1.4.2 Operacije

Operacije za potpisivanje i verifikovanje poruke su označene kako slijedi:

- Potpisivanje poruke *m* sa privatnim ključem SK_{PCD} je označeno sa $s = \mathbf{Sign}(SK_{PCD}, m)$.
- Verifikovanje nastalog potpisa *s*sa javnim ključem PK_{PCD} je označeno sa $\mathbf{Verify}(\mathrm{PK}_{\mathrm{PCD}}, \mathrm{s}, \mathrm{m})$.

3.2 PACE

PACE protokol je šifrom autentifikovan Diffie-Hellmanov protokol dogovora ključeva koji pruža sigurnu komunuikaciju i eksplicitnu autentifikaciju MRTD čipa i terminala na osnovu šifre (MRTD čip i terminal dijele istu šifru π).

Ovaj protokol uspostavlja sigurnu razmjenu poruka između MRTD čipa i terminala na osnovu slabe (kratke) šifre. PACE je alternativa za osnovnu kontrolu pristupa (BAC), tj. omogućava da MRTD čip verifikuje da je terminal autorizovan za pristup sačuvanim manje osjetljivim podacima ali ima dvije prednosti:

- Jaki ključevi sesije su osigurani nezavisno od jačine šifre
- Entropija šifre(i) korištenih za autentifikaciju terminala može biti veoma slaba (npr. 6 cifri je u suštini dovoljno).

Napomena: Postoje dvije verzije ovog protokola koje se razlikuju u kontekstu tokena za autentifikaciju. Privremeni parametri domena generisani u protokolu su dio tokena za autentifikaciju u verziji 1. Oni su uklonjeni u verziji 2 jer integrisano mapiranje naznačeno u [5] zahtijeva da privremeni parametri domena ostanu tajni. Da bi se koristila PACE verzija 1 sa integrisanim mapiranjem, MAC MORA dodatno zaštititi povjerljivost poruke. Verzija 1 ovog protokola je tako zastarjela i PREPORUČENO je koristiti verziju 2.

MRTD Chip (PICC)		Terminal (PCD)
static domain parameters D_{PICC}		
choose random nonce $s \in_R Dom(E)$		
$z = \mathbf{E}(K_\pi, s)$	$\xrightarrow{D_{PICC}, z}$	$s = \mathbf{D}(K_\pi, z)$
additional data required for **Map**( )	$\langle - \rangle$	additional data required for **Map**( )
$\tilde{D} = \mathbf{Map}(D_{PICC}, s)$		$\tilde{D} = \mathbf{Map}(D_{PICC}, s)$
choose random ephemeral key pair $(\widetilde{SK_{PICC}}, \widetilde{PK_{PICC}}, \tilde{D})$		choose random ephemeral key pair $(\widetilde{SK_{PCD}}, \widetilde{PK_{PCD}}, \tilde{D})$
check that $\widetilde{PK_{PCD}} \neq \widetilde{PK_{PICC}}$	$\langle \widetilde{PK_{PCD}}, \widetilde{PK_{PICC}} \rangle$	check that $\widetilde{PK_{PICC}} \neq \widetilde{PK_{PCD}}$
$K = \mathbf{KA}(\widetilde{SK_{PICC}}, \widetilde{PK_{PCD}}, \tilde{D})$		$K = \mathbf{KA}(\widetilde{SK_{PCD}}, \widetilde{PK_{PICC}}, \tilde{D})$
	$\langle T_{PCD}$	$T_{PCD} = \mathbf{MAC}(K_{MAC}, \widetilde{PK_{PICC}})$
$T_{PICC} = \mathbf{MAC}(K_{MAC}, \widetilde{PK_{PCD}})$	$\xrightarrow{T_{PICC}}$	

Slika 1: PACE

3.2.1 Specifikacija protokola

Terminal i MRTD čip vrše sljedeće korake a pojednostavljena verzija je takođe prikazana na slici 1:

1. MRTD čip nasumično i jednoobrazno bira jednokratni slučajni broj (nonce) s, šifruje nonce broj z= $E(K_\pi, s)$ gdje je $K_\varnothing = \mathbf{KDF_\pi(\pi)}$ izvedeno iz zajedničke šifre π, i šalje tekst za enkripciju z zajedno sa statičkim parametrima domena D_{PICC} ka terminalu.
2. Terminal obnavlja tekst koji se šifruje $s = \mathbf{D}(K_\pi, z)$ uz pomoć zajedničke šifre π.
3. MRTD čip i terminal izvode sljedeće korake:

   a) Oni izračunavaju privremene parametre domena $\tilde{D} = Map(D_{PICC}, s)$

   b)Oni izvode anonimni Diffie-Hellmanov dogovor ključeva na osnovu privremenih parametara domena i generišu zajedničke tajne

$$K = KA(\widetilde{SK_{PICC}}, \widetilde{PK_{PCD}}, \tilde{D}) = KA(\widetilde{SK_{PCD}}, \widetilde{PK_{PICC}}, \tilde{D})$$

   c) Tokom Diffie-Hellmanovog dogovora ključeva, svaka strana TREBA provjeriti da se dva javna ključa $\widetilde{PK_{PICC}}$ i $\widetilde{PK_{PCD}}$ razlikuju.

   d) Oni izvode ključeve sesije $K_{MAC} = \mathbf{KDF_{MAC}}(K)$ and $K_{Enc} = \mathbf{KDF_{Enc}}(K)$.

e) Oni razmjenjuju i verifikuju tokene za $T_{PCD} = MAC(K_{MAC}, \widetilde{PK_{PICC}})$ i $T_{PICC} = MAC(K_{MAC}, \widetilde{PK_{PCD}})$

3.2.2 Status sigurnosti

Ukoliko je PACE uspješno obavljen onda je MRTD čip verifikovao korištenu šifru. Sigurna razmjena poruka je započeta korištenjem izvedene sesije ključeva K_{MAC} i K_{Enc}. MRTD čip NE SMIJE prihvatiti više od jednog izvođenja PACE-a u okviru iste sesije (vidi odjeljak „Sigurna razmjena poruka“ u 3.dijelu ovog tehničkog uputstva pod definicijom „sesija“) osim ako se suspendovani PIN mora obnoviti korištenjem neautentifikovanog terminala („vidi odjeljak 2.5.1) sa CAN brojem kao šifrom. U tom slučaju, drugo izvođenje PACE-a MORA biti zaštićeno sa sigurnom razmjenom podataka ustanovljenom u prvom izvođenju. Ukoliko je drugo izvođenje PACE-a bilo uspješno, MRTD čip je verifikovao PIN. Sigurna razmjena podataka je ponovo pokrenuta korištenjem novo izvedene sesije ključeva K_{MAC} i K_{Enc}. U suprotnom, ako drugo izvođenje PACE-a nije bilo uspješno, sigurna razmjena poruka se nastavlja korištenjem prethodno utvrđenih ključeva sesije.

3.3 Autentifikacija čipa verzija 2

Protokol autentifikacije čipa je privremeno – statični Diffie-Hellman protokol dogovora ključeva koji pruža sigurnu komunikaciju i jednosmjernu autentifikaciju MRTD čipa.

Protokol u verziji 2 pruža eksplicitnu autentifikaciju MRTD čipa verifikovanjem tokena za autentifikaciju i implicitnu autentifikaciju sačuvanih podataka izvođenjem sigurne razmjene poruka korištenjem nove sesije klkučeva.

3.3.1 Specifikacija protokola

Terminal i MRTD čip vrše sljedeće korake a pojednostavljena verzija je takođe prikazana na slici 2.

U ovoj verziji autentifikacija terminala se MORA izvršiti prije autentifikacije čipa, jer je privremeni par ključeva $(\widetilde{SK_{PCD}}, \widetilde{PK_{PCD}}, D)$ terminala generisan kao dio autentifikacije terminala.

1. MRTD čip šalje svoj statički Diffie-Hellman javni ključ PK_{PICC} i parametri domena D_{PICC} terminalu.
2. Terminal šalje privremeni javni ključ $\widetilde{PK_{PCD}}$ ka MRTD čipu.
3. MRTD čip izračunava kompresovani privremeni javni ključ terminala $\boldsymbol{Comp}(\widetilde{PK_{PCD}})$ i poredi sa kompresovanim privremenim javnim ključem dobijenim u procesu autentifikacije terminala.
4. MRTD čip i terminal računaju sljedeće:
   a) Zajedničku tajnu $K = KA(SK_{PICC}, \widetilde{PK_{PCD}}, D) = KA(\widetilde{SK_{PCD}}, PK_{PICC}, D)$
5. MRTD čip nasumično bira nonce broj r_{PICC}, izvodi ključeve sesije K_{MAC}=**KDF$_{MAC}$** (K, r_{PICC}) i K_{Enc}= **KDF$_{Enc}$** (K, r_{PICC}) za sigurnu razmjenu poruka od K i r_{PICC}, računa token za autentifikaciju i šalje r_{PICC} i T_{PICC}.
6. Terminal izvodi ključeve sesije K_{MAC}=**KDF$_{MAC}$** (K, r_{PICC}) i K_{Enc}= **KDF$_{Enc}$** (K, r_{PICC}) za sigurnu razmjenu poruka od K i r_{PICC}, i verifikuje T_{PICC}.

Kako bi se verifikovala autentičnost PK_{PICC} terminala, pasivna autentifikacija ĆE biti izvedena.

3.3.2 Status sigurnosti

Ukoliko je autentifikacija čipa uspješnio izvršena, sigurno slanje poruka je ponovo pokrenuto korištenjem izvedenih ključeva sesije K_{MAC} i K_{Enc}. U suprotnom, sigurno slanje poruka se nastavlja korištenjem prethodno utvrđenih ključeva sesije (PACE ili BAC).

Napomena: Pasivna autentifikacija se MORA izvršiti u kombinaciji sa autentifikacijom čipa. Dok se u verziji 1, pasivna autentifikacija TREBA izvršiti nakon autentifikacije čipa korištenjem objekta sigurnosti dokumenta ili objekta sigurnostii čipa, u verziji 2 pasivna autentifikacija se MORA izvršiti prije autentifikacije čipa korištenjem objekta sigurnosti dokumenta ili objekta sigurnosti čipa. Jedino nakon uspješne validacije pomenutog objekta sigurnosti, MRTD čip se može smatrati orginalnim.

3.4 Autentifikacija terminala verzija 2

Protokol autentifikacije terminala je protokol sa dva challenge-response pokreta koji pruža eksplicitnu jednoobraznu autentifikaciju terminala.

Autentifikacija terminala omogućava MRTD čipu da verifikuje da je terminal ovlašten za pristup osjetljivim podacima. Kako terminal može pristupati osjetljivim podacima i poslije, sva dalja komunikacija MORA biti odgovarajuće zaštićena. Stoga, terminal za autentifikaciju takođe autentifikuje privremeni javni ključ koji terminal izabere i koji će se koristiti za podešavanje sigurne razmjene poruka sa autentifikacijom čipa verzija 2. MRTD čip mora povezati prava pristupa terminala sigurnoj razmjeni poruka utvrđenoj autentifikovanim privremenim javnim ključevima terminala.

U ovom protokolu ID_{PICC} je identifikator MRTD čipa:

- Ako se koristi BAC, ID_{PICC} je broj dokumenta MRTD čipa koji se nalazi u MRZ uključujući kontrolnu cifru.
- Ako se koristi PACE ID_{PICC} se računa korištenjem privremenog PACE javnog ključa, tj $IDD_{PICC} = Comp(\widetilde{PK_{PICC}})$

Napomena: Sve poruke MORAJU biti poslane sa sigurnom razmjenom podata na način enkripcija pa autentifikacija korištenjem ključeva sesije izvedenih iz PACE u autentifikacije čipa.

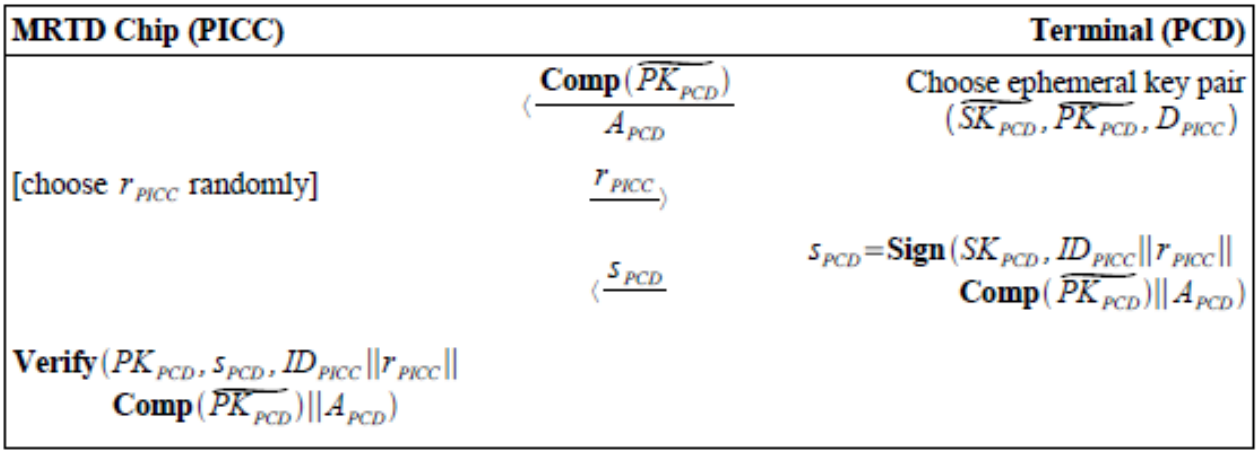


Figure 3: Terminal Authentication Version 2

3.4.1 Specifikacija protokola

Terminal i MRTD čip vrše sljedeće korake a pojednostavljena verzija je takođe prikazana na slici 3.

1. Terminal šalje lanac certifikata MRTD čipu. Lanac počinje sa certifikatom koji se može provjeriti sa CVCA javnim ključem sačuvanim na čipu i završava se sa certifikatom terminala.
2. MRTD čip verifikuje certifikate i izvodi javni ključ terminala PK_{PCD} .
3. Terminal

   a) generiše privremeni Diffie-Hellmanov par ključeva $(\widetilde{SK_{PCD}},\ \widetilde{PK_{PCD}},\ D)$ i šalje kompresovani privremeni javni ključ $Comp(\widetilde{PK_{PKCD}})$ MRTD čipu, i

   b) može poslati pomoćne podatke A_{PCD} MRTD čipu.

4. MRTD čip nasumično bira challenge r_{PICC} i šalje ga terminalu.
5. Terminal odgovara sa potpisom
   $$s_{PCD} = Sign(SK_{PCD}, ID_{PICC}||r_{PICC}||Comp(\widetilde{PK_{PICC}})||A_{PCD})$$
6. MRTD čip provjerava da je
   $$Verify(PK_{PCD}, ID_{PICC}||r_{PICC}||Comp(\widetilde{PK_{PCD}})||A_{PCD}) = true$$

Napomena: U verziji 1 autentifikacija čipa se MORA izvršiti prije autentifikacije terminala, tj

$Comp(\widetilde{PK_{PKPCD}})$ se računa od MRTD čipa i terminala kao dijela autentifikacije čipa.

U verziji2 autentifikacija čipa se MORA izvršiti nakon autentifikacije terminala. U tom slučaju,

$Comp(\widetilde{PK_{PKPCD}})$ se MORA izračunati kao dio autentifikacije terminala. Pored toga, terminal MOŽE poslati autentifikovane pomoćne podatke APCD MRTD čipu.

3.4.2 Status sigurnosti

Ako je autentifikacija terminala uspješno izvršena, MRTD čip ĆE odobriti pristup sačuvanim osjetljivim podacima u skladu sa važećom autorizacijom terminala za autentifikaciju. MRTD čip CE ipak ograničiti prava pristupa terminala sigurnoj razmjeni poruka utvrđena autentifikovanim privremenim javnim ključem, tj. MRTD čip ĆE uporediti kompresovanu reprezentaciju privremenog javnog ključa terminala zaprimljenog kao dio autentifikacije terminala sa kompresovanom reprezentacijom privremenog javnog ključa dobijenog od terminala kao dio autentifikacije čipa. MRTD čip NE SMIJE prihvatiti više od jednog izvođenja autentifikacije terminala u okviru iste sesije (vidi odjeljak „Sigurna razmjena poruka“ u 3.dijelu ovog tehničkog uputstva pod definicijom „sesija“).

Napomena: Autentifikacija terminala ne utiče na sigurnu razmjenu poruka. MRTD čip ĆE zadržati sigurnu razmjenu poruka čak i ako je autentifikacija terminala neuspješna (osim ako se desi greška kod sigurne razmjene poruka)..

3.5 Ograničena identifikacija

Protokol ograničene identifikacije je statičan Diffie-Hellmanov protokol dogovora ključeva koji generiše sektorske specifične identifikatore MRTD čipa.

Ograničena identifikacija pruža sektorski specifičan identifikator za MRTD sa sljedećim svojstvima:

- U okviru svakog sektora sektorski specifičan identifikator svakog MRTD čipa je jedinstven.
- Između bilo koja dva sektora, računarski je neizvodljivo povezati sektorski specifične identifikatore bilo kojeg MRTD čipa[2].

Sektorski specifični identifikatori se koristi za identifikaciju ili ponovnu identifikaciju MRTD čipa u okviru svakog sektora. Autentifikacija čipa i terminala MORA biti uspješno izvršena prije upotrebe ograničene identifikacije.

Napomena: U zavisnosti od hash funkcije koja se koristi za kreiranje sektorskog specifičnog identifikatora, mogu se desiti hash kolizije.

3.5.1 Specifikacije protokola

Terminal i MRTD čip izvode sljedeće korake, a pojednostavljena verzija je prikazana na slici 4.

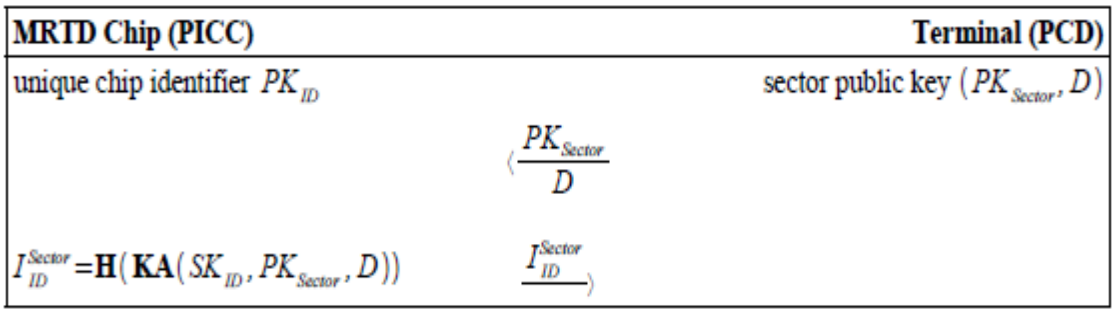
1. Terminal šalje statični sektorski javni ključ PK_{Sector}, i parametre domena D MRTD čipu. .

2. MRTD čip verifikuje PK_{Sector}, računa i šalje svoj sektorski specifičan identifikator $I_{ID}^{Sector} = H(KA(SK_{ID}, PK_{Sector}, D))$ terminalu.

[2] Zasvisno od generacije sektora povjerljiva treća strana može ili ne može povezati sektorske identifikatore između sektora.

3. Terminal provjera da li je primljeni sektorski specifičan identifikator I^{Sector}_{ID} je na slisti opozivnih identifikatora sektora dobijenih od verifikatora dokumenta.

Ograničena identifikacija ĆE se koristiti samo nakon što je autentifikacija terminala i čipa uspješno



izvršena. Jedino je tada zagarantovana autentičnost javnog ključa sektora PK_{Sector}

Sector sektorskog specifičnog identifikatora $ISector_{ID.}$

U zavisnosti od generisanja sektora, povjerena treća strana može ili ne može biti u mogućnosti da poveže sektorske identifikatore u okviru sektora.

Napomena: MRTD čip MORA verifikovati javni ključ sektora korištenjem nastavka terminala sektora (vidi 3.dio ovog tehničkog uputstva) sadržanom u certifikatu terminala.

3.5.2 Status sigurnosti

Ograničena identifikacija ne utiče na status sigurnosti MRTD čipa.

A. eID aplikacija (Normativno)

A.1. eID aplikacija

eID aplikacija se sastoji od 21 grupe podataka (DG1 - DG21) koje sadrže lične podatke. Pregled grupe podataka je prikazanau tebeli 3.

DG	Content	FID	SFID	ASN.1 type	R/W	Access
DG1	Vrsta dokumenta	0x0101	0x01	Vrsta dokumenta	R	PACE + TA + CA
DG2	Zemlja izdavanja	0x0102	0x02	Zemlja izdavanja	R	PACE + TA + CA
DG3	Rok važenja	0x0103	0x03	Rok važenja	R	PACE + TA + CA
DG4	Lično ime	0x0104	0x04	Lično ime	R	PACE + TA + CA
DG5	Prezime	0x0105	0x05	Prezime	R	PACE + TA + CA
DG6	Vjeroispovjest	0x0106	0x06	Umjetničko ime	R	PACE + TA + CA
DG7	Akademska titula	0x0107	0x07	Akademska titula	R	PACE + TA + CA
DG8	Datum rođenja	0x0108	0x08	Datum rođenja	R	PACE + TA + CA
DG9	Mjesto rođenja	0x0109	0x09	Mjesto rođenja	R	PACE + TA + CA
DG10	Nacionalnost	0x010A	0x0A	Nacionalnost	R	PACE + TA + CA
DG11	Pol	0x010B	0x0B	Pol	R	PACE + TA + CA
DG12	Opcionalni podaci	0x010C	0x0C	Opcionalni podaci	R	PACE + TA + CA
DG13	--	0x010D	0x0D	RFU	R	PACE + TA + CA
DG14	--	0x010E	0x0E	RFU	R	PACE + TA + CA
DG15	--	0x010F	0x0F	RFU	R	PACE + TA + CA
DG16	--	0x0110	0x10	RFU	R	PACE + TA + CA
DG17	Mjesto prebivalište	0x0111	0x11	Mjesto prebivalište	R/W	PACE + TA + CA
DG18	Broj opštine	0x0112	0x12	Broj opštine	R/W	PACE + TA + CA
DG19	Dozvola boravka I	0x0113	0x13	Dozvola boravka I	R/W	PACE + TA + CA
DG20	Dozvola boravka II	0x0114	0x14	Dozvola boravka II	R/W	PACE + TA + CA
DG21	Opcionalni podaci	0x0115	0x15	Opcionalni podaci RW	R/W	PACE + TA + CA

Tabela 3: Grupe podataka na eID aplikaciji

A.1.1. Application Identifier

eID aplikacija ĆE biti identifikovana sa standardnim identifikatorom aplikacije 0xE80704007F00070302 koji se zasnima na sljedećim objektima identifikatora:

id-eID OBJECT IDENTIFIER ::= {

bsi-de applications(3) 2

}

A.2. ASN.1 Definicija

Svaka elementarna datoteka sadrži ASN.1- strukuru definisanu u nastavku. Podaci se dekodiraju prema istaknutim pravilima dekodiranja (DER) definisanim u [6].

```
DocumentType        ::= [APPLICATION 1] ICAOString (SIZE (2))
IssuingState        ::= [APPLICATION 2] ICAOCountry
DateOfExpiry        ::= [APPLICATION 3]     Date
GivenNames          ::= [APPLICATION 4]     UTF8String
FamilyNames         ::= [APPLICATION 5]     UTF8String
ArtisticName        ::= [APPLICATION 6]     UTF8String
AcademicTitle       ::= [APPLICATION 7]     UTF8String
DateOfBirth         ::= [APPLICATION 8]
Date PlaceOfBirth   ::= [APPLICATION 9]     GeneralPlace
Nationality         ::= [APPLICATION 10] ICAOCountry
Sex                 ::= [APPLICATION 11] ICAOSex
OptionalDataR       ::= [APPLICATION 12] SET OF OptionalData
PlaceOfResidence    ::= [APPLICATION 17] GeneralPlace
CommunityID         ::= [APPLICATION 18] OCTET STRING
ResidencePermitI    ::= [APPLICATION 19] Text
ResidencePermitII   ::= [APPLICATION 20] Text
OptionalDataRW      ::= [APPLICATION 21] SET OF OptionalData
ICAOString          ::= PrintableString (FROM ("A".. "Z" | " "))
ICAOCountry         ::= ICAOString (SIZE (1|3))        -- ICAO country code ICAO
Sex                 ::= PrintableString (FROM ("M"|"F"|" "))
Date                ::= NumericString (SIZE (8)) -- YYYYMMDD

Place ::= SEQUENCE {
        street   [10] UTF8String OPTIONAL,
```

```
        city      [11] UTF8String,
        state     [12] UTF8String OPTIONAL,
        country[13] ICAOCountry,
        zipcode[14] PrintableString OPTIONAL
}

GeneralPlace ::= CHOICE {
        structuredPlace          Place
        freetextPlace [1] UTF8String
        noPlaceInfo      [2] UTF8String
}

Text ::= CHOICE {
        uncompressed [1] UTF8String
        compressed      [2] OCTET STRING
        -- contains a DEFLATE-compressed UTF8String (cf. [2] for details on
        -- the compression algorithm)
}

OptionalData ::= SEQUENCE {
        type OBJECT IDENTIFIER,
        data ANY DEFINED BY type OPTIONAL
}
```

4 Bibliografija

[1] Bradner, Scott. Key words for use in RFCs to indicate requirement levels, RFC 2119, 1997

[2] Deutsch, Peter. DEFLATE compressed data format specification version 1.3., RFC 1951, 1996

[3] ICAO, Machine Readable Travel Documents - Part 1: Machine Readable Passport, Specifications for electronically enabled passports with biometric identification capabilities, ICAO Doc 9303, 2006

[4] ICAO, Machine Readable Travel Documents - Part 3: Machine Readable Official Travel Documents, Specifications for electronically enabled official travel documents with biometric identification capabilities, ICAO Doc 9303, 2008

[5] ICAO. Supplemental Access Control for Machine Readable Travel Documents, Technical Report, 2009

[6] ITU-T. Information Technology – ASN.1 encoding rules: Specification of Basic Encoding Rules(BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), X.690, 2002

[7] Drugi dio tehničkog Uputstva za MRTD BSI