Tehničko uputstvo

Napredni sigurnosni mehanizmi za mašinski čitljive putne dokumente

Dio 3 – Opšte specifikacije

Banja Luka, 01.03.2013. godine

Sadržaj

1 Uvod

Ovaj dio Tehničkog uputstva sadrži opšte specifikacije koje obuhvataju, kako PKI koja se koristi za kontrolu pristupa, tako i mapiranje protokola za ASN.1 i APDU specifikacije za protokole definisane u dijelovima 1 i 2:

- Dio 1:
  - Autentifikacija terminala verzija 1
  - Autentifikacija čipa verzija 1
- Dio 2:
  - Password Authenticated Connection Establishment (PACE)
  - Autentifikacija čipa verzija 2
  - Autentifikacija terminala verzija 2
  - Ograničena identifikacija

Iako su specifikacije za PACEv2 u [10] kompatibilne sa specifikacijama u ovom dokumentu, molimo pogledajte [10] radi primjene PACE u skladu sa Dijelom 1.

Dokumenti kojima se primjenjuju samo protokoli opisani u dijelu 1 se u ovom uputstvu nazivaju „dokumenti Dijela 1“, dok se dokumenti kojima se primjenjuju protokoli iz Dijela 2 ili iz oba dijela nazivaju „dokumenti Dijela 2“.

1.1 Zahtjevi za čipove i terminale MRTD

Ovo tehničko uputstvo propisuje zahtjeve za primjene čipova i terminala MRTD. Dok čipovi MRTD moraju zadovoljavati te zahtjeve u skladu sa terminologijom koja je opisana u Odjeljku 1.2, zahtjeve za terminale treba posmatrati kao uputstva, tj. međuoperativnost čipova i terminala MRTD je zagarantovana jedino ukoliko terminal zadovoljava te zahtjeve, u suprotnom interakcija sa čipom MRTD će biti neuspješna ili će ponašanje čipa MRTD biti nedefinisano. U načelu, čip MRTD ne mora provoditi zahtjeve u vezi sa terminalima, osim ukoliko je neposredno ugrožena sigurnost čipa MRTD.

1.2 Terminologija

Ključne riječi „MORA“, „NE SMIJE“, „OBAVEZNO“, „ĆE“ „NEĆE“, „TREBA“, „NE TREBA“, „PREPORUČENO“, „MOŽE“ i „FAKULTATIVNO“ u ovom dokumentu treba tumačiti kako je opisano u RFC 2119 [2]. Ključnu riječ „USLOVNO“ treba tumačiti kako slijedi:

USLOVNO: Upotreba nekog predmeta zavisi od upotrebe drugih predmeta. Zato se dalje kvalifikuje pod kojim uslovima je predmet OBAVEZAN ili PREPORUČEN.

Kada se koriste u tabelama (profilima), ključne riječi se skraćuju, kako je prikazano u Tabeli 1.

Ključna riječ		Skrać.
MORA / ĆE	OBAVEZNO	m
NE SMIJE / NEĆE	–	x
TREBA	PREPORUČENO	r

MOŽE	FAKULTATIVNO	o
–	USLOVNO	c

Tabela 1: Ključne riječi

1.3 Skraćenice

Slijedeće skraćenice će biti korištene u ovoj specifikaciji.

Naziv	Skraćenica
Binarno kodirana cifra	BCD
Provjerljiv pomoću kartice	CV
Objekat sigurnosti kartice/čipa	SOC
Certifikaciono tijelo	CA
Identifikator čipa	ID PICC
Javni ključ za autentifikaciju čipa	PK PICC
Privatni ključ za autentifikaciju čipa	SK PICC
Državno certifikaciono tijelo (CA) za	CSCA
Državno certifikaciono tijelo (CA) za	CVCA
Certifikat državnog certifikacionog tijela (CA)	C.CVCA
Objekat sigurnosti dokumenta	SOD
Grupa podataka	DG
Verifikator dokumenata	DV
Certifikat verifikatora dokumenata	C.DV
Parametri domena	D
Privremeni privatni ključ	SK
Privremeni javni ključ	PK
Hash funkcija	H
Međunarodna organizacija za civilno	ICAO
Funkcija dogovora o ključu	KA
Funkcija izvođenja ključa	KDF
Logička struktura podataka	LDS
Mašinski čitljiva putna isprava	MRTD
Beskontaktni čip integrisanog kola	PICC
Beskontakni uređaj za povezivanje	PCD
Javni ključ za ograničenu identifikaciju	PK ID
Privatni ključ za ograničenu identifikaciju	SK ID
Javni ključ za sektor	PK Sector
Privatni ključ za sektor	SK Sector
Sektorski specifičan identifikator	IID Sector
Javni ključ za autentifikaciju terminala	PK PCD
Privatni ključ za autentiufikaciju terminala	SK PCD
Certifikat terminala	C.T

2 Infrastruktura javnih ključeva

Autentifikacija terminala zahtijeva od terminala da dokaže čipu MRTD da je ovlašten da pristupa osjetljivim podacima. Takav terminal je opremljen najmanje jednim *certifikatom terminala*, koji dekodira javni ključ i prava pristupa terminala, i odgovarajućim privatnim

ključem. Nakon što terminal dokaže da zna taj privatni ključ, čip MRTD odobrava terminalu pristup osjetljivim podacima kao što je naznačeno u certifikatu terminala.

PKI koja je neophodna za izdavanje i potvrđivanje certifikata terminala sastoji se od slijedećih cjelina:

1. Državna certifikaciona tijela za verifikaciju (CVCAs)
2. Verifikatori dokumenata (DVs)
3. Terminali

Ova PKI čini osnovu proširene kontrole pristupa. Prikazana je na Slici 1.

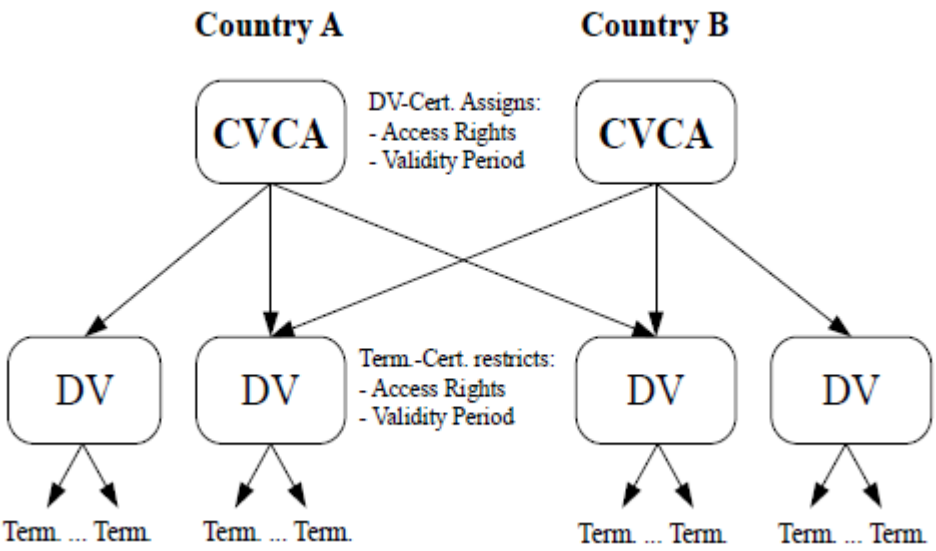
2.1 Državno certifikaciono tijelo za verifikaciju

Od svake države se zahtijeva da uspostavi jedno povjerljivo mjesto koje će izdavati certifikate verifikatora dokumenata: *Državno certifikaciono tijelo za verifikaciju* (CVCA). Zakonom o Agenciji za identifikacione dokumente, evidenciju i razmjenu podataka Bosne i Hercegovine (Službeni glasnik BiH 56/08) Agencija se praktično definiše kao CVCA u Bosni i Hercegovini.

Napomena: Državno certifikaciono tijelo za potpisivanje koje izdaje certifikate za potpisnike dokumenata (v. [8], [9]) i Državno certifikaciono tijelo za verifikaciju MOGU biti integrisani u jednu cjelinu, odnosno u Državno certifikaciono tijelo. Međutim, čak i u tom slučaju odvojeni parovi ključeva se MORAJU koristiti za različite uloge.

CVCA određuje prava pristupa nacionalnim čipovima MRTD za sve DV (tj. zvanične domaće DV, kao i za strane/komercijalne DV) izdavanjem certifikata za DV ovlaštene za pristup nekim osjetljivim podacima. Uslovi pod kojima CVCA odobrava DV pristup osjetljivim podacima su izvan okvira ovog dokumenta i TREBA da budu navedeni u politici certifikacije (v. Prilog C.5).

Certifikati verifikatora dokumenata MORAJU sadržati informacije kao što je ona o tome kojim podacima je određeni DV ovlašten da pristupa. Kako bi se umanjio potencijalni rizik koji mogu izazvati izgubljeni ili ukradeni terminali certifikati verifikatora dokumenata MORAJU imati kratak period važenja. Period važenja određuje CVCA koja izdaje certifikat po sopstvenom izboru i taj period važenja može biti različit u zavisnosti od verifikatora dokumenata kome se isti izdaje.



Slika 1: Infrastruktura javnih ključeva

*Strelice označavaju certifikaciju

2.2 Verifikatori dokumenata

Verifikator dokumenata (DV) je organizaciona jedinica koja upravlja grupom terminala (npr. terminali kojima rukuje granična policija neke države) na način da, između ostalog, izdaje certifikate terminala. Verifikator dokumenata je stoga CA koje je ovlašteno od strane barem nacionalnog CVCA da izdaje certifikate za svoje terminale. Certifikati terminala koje izda verifikator dokumenata obično preuzimaju i prava pristupa i period važenja certifikata verifikatora dokumenata, premda verfikator dokumenata MOŽE odlučiti da dalje **ograniči** prava pristupa ili period važenja u zavisnosti od terminala za koji je izdat certifikat.

Ukoliko verifikator dokumenata zahtijeva da njegovi terminali pristupaju osjetljivim podacima pohranjenim na čipu MRTD druge države, on MORA podnijeti zahtjev za DV certifikat koji izdaje CVCA odgovarajuće države. Verifikator dokumenata takođe MORA osigurati da se svi primljeni certifikati verifikatora dokumenata proslijede teminalima u okviru njegovog područja.

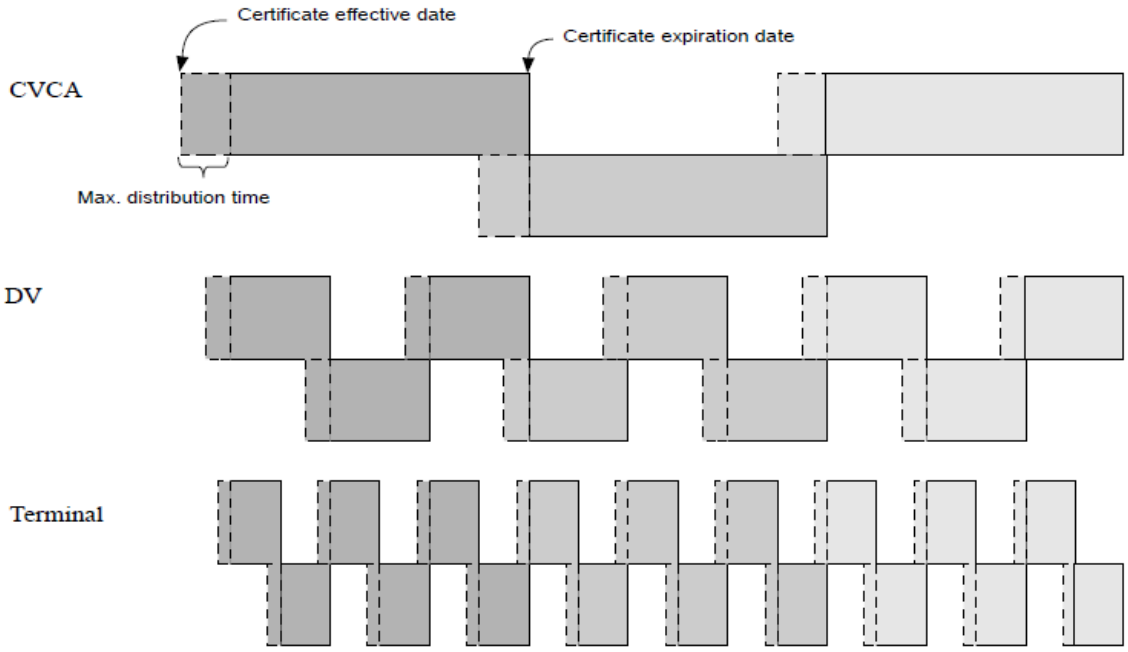
2.3 Certifikati provjerljivi pomoću kartice

CVCA povezujući certifikati, DV certifikati i certifikati terminala su certifikati koje treba da potvrdi čip MRTD. Zbog računarskih ograničenja tih čipova, certifikati MORAJU biti u formatu koji se može provjeriti karticom:

- Format i profil certifikata specifikovan u Prilogu C.1 ĆE biti korišteni.
- Algoritam potpisa, parametre domena i veličinu ključeva koji će biti korišteni određuje CVCA države koja izdaje, odnosno isti algoritam potpisa, parametri domena i veličine ključeva MORAJU biti upotrijebljeni u jednom lancu certifikata[1].

[1] Kao posljedica toga, verifikatori dokumenata i terminali će morati dobiti nekoliko parova ključeva.

- CVCA povezujući certifikati MOGU uključivati javni ključ koji odstupa od važećih parametara, odnosno CVCA MOŽE preći na novi algoritam potpisa, nove parametre domena ili veličinu ključeva.



Slika 2: Raspoređivanje certifikata

2.4 Raspoređivanje certifikata

Svaki certifikat MORA sadržati period važenja. Taj period važenja se identifikuje preko dva datuma, *datuma početka važenja certifikata* i *datuma isteka važenja certifikata.*

Datum početka važenja certifikata: Datum početka važenja certifikata ĆE biti datum generisanja certifikata.

Datum isteka važenja certifikata: Datum isteka važenja certifikata ĆE biti datum *nakon* koga ističe važenje certifikata. Njega po sopstvenom nahođenju može odrediti izdavač certifikata.

Prilikom generisanja certifikata, izdavač MORA pažljivo planirati promjene certifikata, pošto se MORA osigurati dovoljno vremena za prenošenje certifikata i uspostavljanje lanca certifikata. Očigledno, novi certifikat mora biti generisan prije isteka aktuelnog certifikata. Dobijeno *maksimalno vrijeme raspodjele* jednako je razlici datuma isteka starog certifikata i datuma početka važenja novog certifikata. Za upotrebu i distribuciju certifikata se PREPORUČUJU komunikacioni protokoli navedeni u TR-03129[4]. Raspoređivanje certifikata je prikazano na slici 2.

2.5 Potvrđivanje certifikata

Čip MRTD mora posjedovati lanac certifikata koji počinje sa povjerljivim mjestom pohranjenim u čipu MRTD, kako bi se moglo izvršiti potvrđivanje certifikata terminala.

Takva povjerljiva mjesta su manje ili više novi javni ključevi CVCA čipa MRTD. Početno/a povjerljivo/a mjesto/a ĆE biti sigurno pohranjeno/a u memoriji čipa MRTD u fazi proizvodnje ili (pred)personalizacije.

Pošto se par ključeva koji koristi CVCA tokom vremena mijenja, moraju se stvarati povezujući certifikati CVCA. Čip MRTD OBAVEZNO interno ažurira svoje/a povjerljivo/a mjesto/a u skladu sa važećim povezujućim certifikatima koje dobija.

Napomena: U skladu sa raspoređivanjem povezujućih certifikata CVCA (v. sliku 2), najviše dva povjerljiva mjesta po aplikaciji treba da budu pohranjena u čipu MRTD.

Čip MRDT MORA prihvatiti povezujući certifikat CVCA koji je istekao, ali NE SMIJE prihvatiti certifikat terminala ili DV koji je istekao. Čip MRTD ĆE koristiti svoj *tekući datum* kako bi se odredilo da li je certifikat istekao.

Tekući datum: Ukoliko čip MRTD ne posjeduje interni časovnik, tekući datum ĆE biti približno određen na način koji je opisan u nastavku. Tekući datum pohranjen u čipu MRTD u početku predstavlja datum (pred)personalizacije. Taj datum se zatim nezavisno približno određuje od strane čipa MRTD koristeći najnoviji datum početka važenja certifikata koji je sadržan u važećem povezujućem certifikatu CVCA, certifikatu DV ili *Ažuran certifikat terminala.*

Ažuran certifikat terminala: Certifikat terminala je ažuran ukoliko je čip MRTD povjerio izdavaču verifikatoru dokumenata da proizvodi certifikate terminala sa tačnim datumom početka važenja.

Terminal MOŽE poslati povezujuće certifikate CVCA, certifikate DV i certifikate terminala čipu MRTD kako bi se ažurirao tekući datum i povjerljivo mjesto pohranjeno u čipu MRTD čak i ukoliko terminal ne namjerava ili nije u stanju da nastavi autentifikaciju terminala.

Napomena: Čip MRTD potvrđuje samo da je certifikat *prividno* nov (tj. u odnosu na približno određen tekući datum).

2.5.1 Opšti postupak

Postupak potvrđivanja certifikata se sastoji od dva koraka:

1. **Provjera certifikata:** Potpis MORA biti važeći, te ukoliko se ne radi o povezujućem certifikatu CVCA, certifikat NE SMIJE biti istekao. Ukoliko je provjera neuspješna, postupak ĆE biti prekinut.
2. **Interno ažuriranje statusa:** Tekući datum MORA biti *ažuriran,* javni ključ i atributi (uključujući relevantne ekstenzije certifikata) MORAJU biti uvezeni, nova povjerljiva mjesta MORAJU biti *osposobljena*,povjerljiva mjesta koja su istekla MORAJU biti *onesposobljena* za provjeru certifikata DV.

Operacija *ažuriranja* tekućeg datuma i operacija *osposobljavanja* i *onesposobljavanja* povjerljivog mjesta MORA biti provedena kao atomska operacija.

Osposobljavanje povjerljivog mjesta: Novo povjerljivo mjesto ĆE biti dodato na spisak povjerljivih mjesta.

Onesposobljavanje povjerljivog mjesta: Povjerljiva mjesta koja su istekla NE SMIJU biti korištena za provjeru certifikata DV, ali MORAJU ostati upotrebljiva za provjeru povezujućeg certifkata CVCA. Onesposobljena povjerljiva mjesta MOGU biti izbrisana nakon uspješnog uvoza narednog povezujućeg certifikata.

2.5.2 Primjer postupka

Slijedeći postupak potvrđivanja, koji se navodi kao primjer, MOŽE se koristiti za potvrđivanje lanca certifikata. Čip MRTD provodi slijedeće korake za svaki dobijeni certifikat:

1. Čip MRTD provjerava potpis na certifikatu. Ukoliko je potpis neispravan, provjera će biti neuspješna.
2. Ukoliko certifikat nije povezujući certifikat CVCA, datum isteka važenja certifikata se upoređuje sa tekućim datumom čipa MRTD. Ukoliko je datum isteka važenja certifikata prije tekućeg datuma, provjera će biti neuspješna.
3. Certifikat je prihvaćen kao važeći i uvoze se javni ključ i atributi (uključujući relevantne ekstenzije certifikata) sadržani u certifikatu.

   a) Za CVCA, DV, i Ažuran certifikat terminala: Datum početka važenja certifikata se upoređuje sa tekućim datumom čipa MRTD. Ukoliko je tekući datum prije datuma početka važenja, tekući datum se ažurira na datum početka važenja.

   b) Za povezujući certifikat CVCA: Novi javni ključ CVCA se dodaje na spisak povjerljivih mjesta koji je sigurno pohranjen u memoriji čipa MRTD. Novo povjerljivo mjesto je time osposobljeno.

   c) Za certifikate DV ili terminala: Novi javni ključ DV ili terminala se privremeno uvozi radi potvrđivanja certifikata koje će uslijediti, odnosno radi autentifikacije terminala.

4. Povjerljiva mjesta koja su istekla, a koja su sigurno pohranjena u memoriji čipa MRTD su onesposobljena za potvrđivanje certifikata DV i mogu se ukoniti sa spiska povjerljivih mjesta.

2.6 Efektivna autorizacija

Svaki certifikat će sadržati *Certificate Holder Authorization Template* (v. Prilog C.1.5.) koji identifikuje tip terminala (v. Dio 1 i 2 ovog tehničkog uputstva) i određuje *relativnu autorizaciju* vlasnika certifikata koju dodjeljuje certifikaciono tijelo koje izdaje certifikat. Da bi se odredila *efektivna autorizacija* vlasnika certifikata čip MRTD MORA na nivou bita izračunati Bulovo „i“ relativne autorizacije koje je sadržano u certifikatu terminala, referentnom certifikatu verifikatora dokumenata i referentnom certifikatu CVCA.

2.6.1 Ograničena autorizacija (Samo dokumenti Dijela 2)

Efektivna autorizacija se dalje može ograničiti korištenjem Opšteg postupka autentifikacije (v. Dio 2 ovog theničkog uputstva). U tom slučaju terminal MORA naznačiti tip terminala i *ograničenu autorizaciju* (odnosno efektivnu autorizaciju koju zahtijeva terminal) kao dio PACE protokola. Za izračunavanje efektivne autorizacije čip MRTD ĆE uključiti ograničenu autorizaciju izračunavanjem Bulovog „i“ na nivou bita.

Napomena: Čip MRTD MORA potvrditi da su tip terminala naznačen u ograničenoj autorizaciji i tip terminala u relativnoj autorizaciji svakog certifikata u lancu certifikata jednaki. Ukoliko se otkrije neslaganje, čip MRTD ĆE vratiti prava pristupa na početne vrijednosti i ukazati na grešku (v. Prilog B.11.7.).

2.6.2 Tumačenje (svi tipovi dokumenata)

Čip MRTD ĆE tumačiti efektivnu autorizaciju na slijedeći način:

- Efektivna uloga je CVCA:
  - Povezujući certifikat je izdalo državno CVCA.
  - Čip MRTD MORA ažurirati svoje interno povjerljivo mjesto, odnosno javni ključ i efektivnu autorizaciju.
  - Izdavač certifikata predstavlja povjerljiv izvor vremena i čip MRTD MORA ažurirati svoje tekuće vrijeme koristeći vrijeme početka važenja certifikata.
  - Čip MRTD NE SMIJE odobriti CVCA pristup osjetljivim podacima (tj. efektivnu autorizaciju TREBA zanemariti).
- Efektivna uloga je DV:
  - Certifikat je izdalo državno CVCA za ovlaštenog DV.
  - Izdavač certifikata predstavlja povjerljiv izvor vremena i čip MRTD MORA ažurirati svoje tekuće vrijeme koristeći vrijeme početka važenja certifikata.
  - Čip MRTD NE SMIJE odobriti DV pristup osjetljivim podacima (tj. efektivnu autorizaciju TREBA zanemariti).
- Efektivna uloga je Terminal:
  - Certifikat je izdao zvanični domaći ili strani, ili pak nezvanični DV.
  - Ukoliko certifikat predstavlja ispravan certifikat terminala (v. Odjeljak 2.5), tijelo koja ga je izdalo je povjerljiv izvor vremena i čip MRTD MORA ažurirati svoje tekuće vrijeme koristeći datum početka važenja certifikata.
  - Čip MRTD MORA autentifikovanom terminalu odobriti pristup osjetljivim podacima u skladu sa efektivnom autorizacijom.

Važeći certifikat terminala MORA biti prihvaćen kao ispravan od strane čipa MRTD ukoliko ga je izdao zvaničan domaći DV, a u suprotnom NE TREBA biti prihvaćen kao ispravan.

2.7 Sektor terminala za ograničenu identifikaciju

Terminalima se MORA naznačiti sektor terminala kako bi bila podržana ograničena identifikacija terminala. Sektor terminala ĆE biti sadržan u certifikatu terminala i shodno tome PREPORUČENO je da sektor terminala generiše verifikator dokumenata koji vrši certifikaciju. U svakom slučaju, sektor terminala NE SMIJE biti odabran od strane samog terminala.

Sektor terminala je uvijek javni ključ. On MOŽE biti izabran bilo nasumičnim odabirom sa nepoznatim privatnim ključem, kako bi se potpuno onemogućilo praćenje (u tom slučaju povezivanje sektorski specifičnih identifikatora između različitih sektora je računarski nemoguće) ili kao par ključeva kako bi se omogućio opoziv zasnovan na sektorski specifičnim identifikatorima.

2.7.1 Par ključeva za sektor

Par ključeva za sektor mora biti generisan od strane svih verifikatora dokumenata koji podržavaju sektorski specifičan opoziv čipova MRTD.

Svaki verifikator dokumenata ĆE provesti slijedeće korake za svaki od subordinisanih sektora:

1. Generisati novi par ključeva za sektor na osnovu javnog ključa sektora za opoziv.
2. Sigurno pohraniti privatni ključ za sektor (kod verifikatora dokumenata).
3. Uključiti javni ključ za sektor u svaki certifikat terminala za sve terminale koji pripadaju odgovarajućem sektoru.

Par ključeva sektora za opoziv ĆE biti genrisan od strane CVCA. CVCA MOŽE delegirati uslugu opoziva dobavljaču usluga.

2.7.2 Sektorski specifičan opoziv čipova MRTD

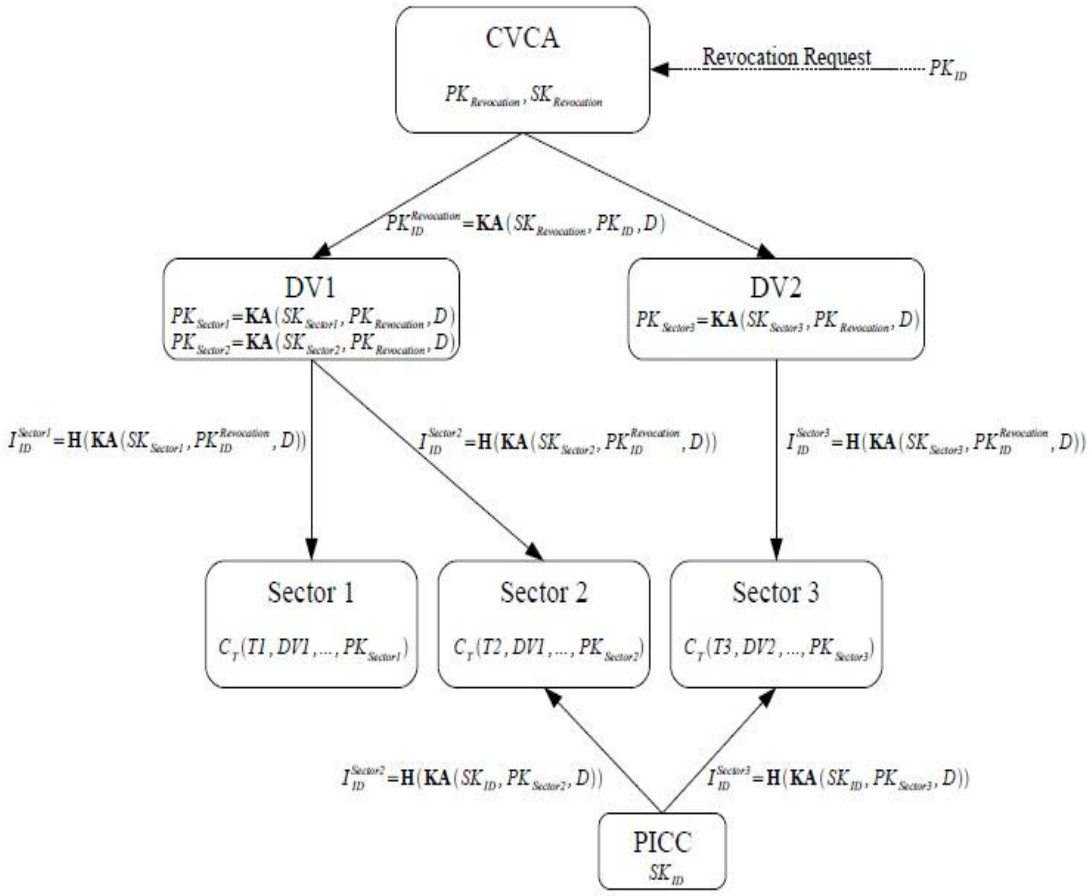
Par ključeva za ograničenu identifikaciju ĆE biti generisan prilikom (pred)personalizacije čipa MRTD. Privatni ključ ĆE biti pohranjen u čipu MRTD, javni ključ ĆE biti pohranjen u bazi podataka zajedno sa drugim podacima pomoću kojih se identifikuje nosilac MRTD.

Napomena: Generisanje para ključeva za ograničenu identifikaciju MOŽE biti provedeno u čipu MRTD ili eksterno. Par ključeva MORA biti izabran tako da bude jedinstven i MOŽE biti ili specifičan za čip ili za nosioca (tj. isti par ključeva će se koristiti za naredne čipove MRTD). Barem jedan par ključeva koji se koristi za ograničenu identifikaciju MORA biti specifičan za čip.

Da bi se opozvao čip MRTD, javni ključ čipa MRTD koji je specifičan za čip se pretražuje u bazi podataka i prenosi do CVCA. CVCA zatim transformiše javni ključ koristeći njegov privatni ključ sektora za opoziv. Transformisani javni ključ se zatim prenosi svim suborinisanim verifikatorima dokumenata. Svaki verifikator dokumenata izračunava sektorski specifične identifikatore koristeći privatne ključeve za sektor za sve subordinisane sektore terminala. Konačno, sektorski specifičan identifikator se prenosi do svih terminala odgovarajućeg sektora.

2.7.3 Generisanje lista opozvanih certifikata

CVCA objavljuje javni ključ sektora za opoziv $PK_{Revocation}$ i parametre domena D. Svaki verifikator dokumenata nasumice bira privatni ključ za sektor SK_{Sector} za svaki subordinisani sektor i izračunava javni ključ za sektor kao $PK_{Sector} = \mathbf{KA}(SK_{Sector}, PK_{Revocation}, D)$.



Slika 3: Opoziv

Da bi se opozvao čip MRTD upućuje se zahtjev CVCA za opoziv koji sadrži javni ključ za ograničenu identifikaciju PK_{ID}. Sektorski specifični identiteti se izračunavaju na slijedeći način:

1. CVCA izračunava $PK^{Revocation} = \mathbf{KA}(SK_{Revocation}, PK_{ID}, D)$ koristeći privatni ključ $SK_{Revocation}$ i javni ključ za ograničenu identifikaciju PK_{ID} koji je dobijen uz zahtjev za opoziv. Transformisani javni ključ $PK_{ID}^{Revocation}$ se proslijeđuje svim verifikatorima dokumenata.

2. Svaki verifikator dokumenata izračunava sektorski specifičan identifikator za sve subordinisane sektore. Za svaki sektor verifikator dokumenata izračunava

$$I_{ID}^{Sector} = H(KA(ID_{Sector}, PK_{ID}^{Revocation}, D))$$

koristeći odgovarajući privatni ključ za sektor SK_{Sector} i dobijeni javni ključ $PK_{ID}^{Revocation}$ čipa MRTD koji treba da bude opozvan. Sektorski specifičan identifikator I_{ID}^{Sector} se zatim proslijeđuje terminalima odgovarajućeg sektora.

2.7.4 Period važenja

Za razliku od para ključeva terminala (za autentifikaciju terminala), par ključeva za sektor je važeći dugo vremena i MORA se izabrati na odgovarajući način.

2.7.5

2.7.6 Migracija terminala

Kako bi se izvršila migracija terminala od jednog verifikatora dokumenata prema drugom verifikatoru dokumenata, par ključeva terminala za sektor MORA se na siguran način prenijeti do novog verifikatora dokumenata.

Napomena: Migracija terminala do novog verifikatora dokumenata nije moguća pod nadzorom drugog CVCA.

A. ASN.1 Specifikacije (Normativ)

Identifikatori objekta korišteni u slijedećim prilozima sadržani su u podstablu `bsi-de`:

```
bsi-de OBJECT IDENTIFIER ::= {
itu-t(0) identified-organization(4) etsi(0)
reserved(127) etsi-identified-organization(0) 7
}
```

A.1. Informacija o podržanim sigurnosnim protokolima

Struktura podataka ASN.1 `SecurityInfos` ĆE biti osigurana od strane čipa MRTD kako bi se naznačili podržani sigurnosni protokoli. Struktrura podataka je specificirana na slijedeći način:

```
SecurityInfos ::= SET OF SecurityInfo

SecurityInfo        ::= SEQUENCE {
protocol            OBJECT IDENTIFIER,
requiredData        ANY DEFINED BY protocol,
optionalData        ANY DEFINED BY protocol OPTIONAL
}
```

Elementi sadržani u `SecurityInfo` strukture podataka imaju slijedeće značenje:

- Identifikator objekta `protocol` identifikuje podržavani protokol.
- `requiredData` otvorenog tipa sadrži obavezne podatke specifične za protokol.
- `optionalData` otvorenog tipa sadrži fakultativne podatke specifične za protokol.

A.1.1. Podržani protokoli

Specifikacije ASN.1 za protokole sadržane u ovoj specifikaciji opisane su u nastavku teksta.

Napomena: Čipovi MRTD implementirani u skladu sa Verzijom 1.0.x ove specifikacije će osigurati samo `ChipAuthenticationPublicKeyInfo`.

U tom slučaju terminal TREBA da pretpostavi slijedeće:

- Čip MRTD podržava autentifikaciju čipa u verziji 1.
- Čip MRTD može podržavati autentifikaciju terminala u verziji 1.

Da bi se odredilo da li su osjetljivi podaci zaštićeni autentifikacijom terminala pohranjeni u čipu MRTD ili ne terminal može konsultovati objekat sigurnosti dokumenta i osnovni fajl EF.CVCA.

A.1.1.1. PACE

Da bi se ukazalo na podršku za PACE `SecurityInfos` može sadržati slijedeće stavke:

- MORA postojati najmanje jedan `PACEInfo` koji koristi standardizovan parametar domena.
- Za svaki podržani set eksplicitnih parametara domena MORA postojati `PACEDomainParameterInfo`

PACEInfo: Ova struktura podataka pruža detaljne informacije o primjeni PACE.

- Identifikator objekta `protocol` ĆE identifikovati algoritme koji će biti korišteni (tj. dogovor o ključu, simetrično šifrovanje i MAC).
- Integralna `version` ĆE identifikovati verziju protokola. Verzija 1 je zastarjela i PREPORUČENO je da se koristi samo verzija 2.
- Integralni `parameterId` se koristi da se naznači identifikator parametra domena. On MORA biti upotrijebljen ukoliko čip MRTD koristi standardizovane parametre domena (v. Tabelu 4) ili osigurava višestruke eksplicitne parametre domena za PACE.

```
id-PACE OBJECT IDENTIFIER ::= {
bsi-de protocols(2) smartcard(2) 4
}

id-PACE-DH-GM                          OBJECT IDENTIFIER ::= {id-PACE 1}
id-PACE-DH-GM-3DES-CBC-CBC             OBJECT IDENTIFIER ::= {id-PACE-DH-GM 1}
id-PACE-DH-GM-AES-CBC-CMAC-128         OBJECT IDENTIFIER ::= {id-PACE-DH-GM 2}
id-PACE-DH-GM-AES-CBC-CMAC-192         OBJECT IDENTIFIER ::= {id-PACE-DH-GM 3}
id-PACE-DH-GM-AES-CBC-CMAC-256         OBJECT IDENTIFIER ::= {id-PACE-DH-GM 4}

id-PACE-ECDH-GM                        OBJECT IDENTIFIER ::= {id-PACE 2}
id-PACE-ECDH-GM-3DES-CBC-CBC           OBJECT IDENTIFIER ::= {id-PACE-ECDH-GM 1}
id-PACE-ECDH-GM-AES-CBC-CMAC-128       OBJECT IDENTIFIER ::= {id-PACE-ECDH-GM 2}
id-PACE-ECDH-GM-AES-CBC-CMAC-192       OBJECT IDENTIFIER ::= {id-PACE-ECDH-GM 3}
id-PACE-ECDH-GM-AES-CBC-CMAC-256       OBJECT IDENTIFIER ::= {id-PACE-ECDH-GM 4}

id-PACE-DH-IM                          OBJECT IDENTIFIER ::= {id-PACE 3}
id-PACE-DH-IM-3DES-CBC-CBC             OBJECT IDENTIFIER ::= {id-PACE-DH-IM 1}
id-PACE-DH-IM-AES-CBC-CMAC-128         OBJECT IDENTIFIER ::= {id-PACE-DH-IM 2}
id-PACE-DH-IM-AES-CBC-CMAC-192         OBJECT IDENTIFIER ::= {id-PACE-DH-IM 3}
id-PACE-DH-IM-AES-CBC-CMAC-256         OBJECT IDENTIFIER ::= {id-PACE-DH-IM 4}

id-PACE-ECDH-IM                        OBJECT IDENTIFIER ::= {id-PACE 4}
id-PACE-ECDH-IM-3DES-CBC-CBC           OBJECT IDENTIFIER ::= {id-PACE-ECDH-IM 1}
id-PACE-ECDH-IM-AES-CBC-CMAC-128       OBJECT IDENTIFIER ::= {id-PACE-ECDH-IM 2}
id-PACE-ECDH-IM-AES-CBC-CMAC-192       OBJECT IDENTIFIER ::= {id-PACE-ECDH-IM 3}
id-PACE-ECDH-IM-AES-CBC-CMAC-256       OBJECT IDENTIFIER ::= {id-PACE-ECDH-IM 4}

PACEInfo ::= SEQUENCE {
protocol    OBJECT IDENTIFIER(
id-PACE-DH-GM-3DES-CBC-CBC |
id-PACE-DH-GM-AES-CBC-CMAC-128 |
id-PACE-DH-GM-AES-CBC-CMAC-192 |
id-PACE-DH-GM-AES-CBC-CMAC-256 |
id-PACE-ECDH-GM-3DES-CBC-CBC |
id-PACE-ECDH-GM-AES-CBC-CMAC-128 |
id-PACE-ECDH-GM-AES-CBC-CMAC-192 |
id-PACE-ECDH-GM-AES-CBC-CMAC-256 |
id-PACE-DH-IM-3DES-CBC-CBC |
id-PACE-DH-IM-AES-CBC-CMAC-128 |
id-PACE-DH-IM-AES-CBC-CMAC-192 |
id-PACE-DH-IM-AES-CBC-CMAC-256 |
id-PACE-ECDH-IM-3DES-CBC-CBC |
id-PACE-ECDH-IM-AES-CBC-CMAC-128 |
id-PACE-ECDH-IM-AES-CBC-CMAC-192 |
id-PACE-ECDH-IM-AES-CBC-CMAC-256),
version     INTEGER, -- TREBA biti 2
parameterId INTEGER OPTIONAL
}
```

PACEDomainParameterInfo: Ova struktura podataka osigurava jedan set eksplicitnih parametara domena za PACE za čip MRTD.

- Identifikator objekta `protocol` ĆE identifikovati tip parametara domena (tj.DH ili ECDH).
- Sekvenca `domainParameter` ĆE sadržati parametre domena.
- Integralni `parameterId` MOŽE biti korišten da se naznači lokalni identifikator parametra domena.

MORA se koristiti ukoliko čip MRTD osigurava višestruke eksplicitne parametre domena za PACE.

```
PACEDomainParameterInfo ::= SEQUENCE {
protocol    OBJECT IDENTIFIER(
id-PACE-DH-GM |
id-PACE-ECDH-GM |
id-PACE-DH-IM |
id-PACE-ECDH-IM),
domainParameter    AlgorithmIdentifier,
parameterId INTEGER OPTIONAL
}
```

A.1.1.2. Autentifikacija čipa

Da bi se ukazalo na podršku za autentifikaciju čipa `SecurityInfos` može sadržati slijedeće stavke:

- MORA postojati najmanje jedan `ChipAuthenticationPublicKeyInfo`.
- MORA postojati najmanje jedan `ChipAuthenticationInfo`.
- MORA postojati najmanje jedan `ChipAuthenticationDomainParameterInfo` za autentifikaciju čipa u verziji 2.

Ukoliko postoji više od jednog javnog ključa za autentifikaciju čipa, fakultativni `keyId` MORA biti upotrijebljen u sve tri strukture podataka kako bi se naznačio lokalni identifikator ključa. Svi javni ključevi MORAJU imati različite parametre domena.

ChipAuthenticationInfo: Ova struktura podataka pruža detaljne informacije o primjeni autentifikacije čipa.

- Identifikator objekta `protocol` ĆE identifikovati algoritme koji će biti korišteni (tj. dogovor o ključu, simetrično šifrovanje i MAC).
- Integralna `version` ĆE identifikovati verziju protokola. Trenutno su podržane verzije 1 i 2.
- Integralni `keyId` se MOŽE koristiti da se naznači lokalni identifikator ključa. On se MORA koristiti ukoliko čip MRTD osigurava više javnih ključeva za autentifikaciju čipa.

```
id-CA OBJECT IDENTIFIER ::= {
bsi-de protocols(2) smartcard(2) 3
}

id-CA-DH                        OBJECT IDENTIFIER ::= {id-CA 1}
id-CA-DH-3DES-CBC-CBC           OBJECT IDENTIFIER ::= {id-CA-DH 1}
id-CA-DH-AES-CBC-CMAC-128       OBJECT IDENTIFIER ::= {id-CA-DH 2}
id-CA-DH-AES-CBC-CMAC-192       OBJECT IDENTIFIER ::= {id-CA-DH 3}
```

```
id-CA-DH-AES-CBC-CMAC-256       OBJECT IDENTIFIER ::= {id-CA-DH 4}

id-CA-ECDH                      OBJECT IDENTIFIER ::= {id-CA 2}
id-CA-ECDH-3DES-CBC-CBC         OBJECT IDENTIFIER ::= {id-CA-ECDH 1}
id-CA-ECDH-AES-CBC-CMAC-128     OBJECT IDENTIFIER ::= {id-CA-ECDH 2}
id-CA-ECDH-AES-CBC-CMAC-192     OBJECT IDENTIFIER ::= {id-CA-ECDH 3}
id-CA-ECDH-AES-CBC-CMAC-256     OBJECT IDENTIFIER ::= {id-CA-ECDH 4}

ChipAuthenticationInfo ::= SEQUENCE {
protocol    OBJECT IDENTIFIER(
id-CA-DH-3DES-CBC-CBC |
id-CA-DH-AES-CBC-CMAC-128 |
id-CA-DH-AES-CBC-CMAC-192 |
id-CA-DH-AES-CBC-CMAC-256 |
id-CA-ECDH-3DES-CBC-CBC |
id-CA-ECDH-AES-CBC-CMAC-128 |
id-CA-ECDH-AES-CBC-CMAC-192 |
id-CA-ECDH-AES-CBC-CMAC-256),
version     INTEGER, -- MORA biti 1 za CAv1 ili 2 za CAv2
keyId INTEGER OPTIONAL
}
```

ChipAuthenticationDomainParameterInfo: Ova struktura podataka pruža jedan set eksplicitnih parametara domena za verziju 2 autentifikacije čipa za čip MRTD.

- Identifikator objekta `protocol` ĆE identifikovati tip parametara domena (tj. DH ili ECDH).
- Sekvenca `domainParameter` ĆE sadržati parametre domena.
- Integralni `keyId` MOŽE biti korišten da se naznači lokalni identifikator ključa. On se MORA koristiti ukoliko čip MRTD osigurava više javnih ključeva za autentifikaciju čipa.

```
ChipAuthenticationDomainParameterInfo ::= SEQUENCE {
     protocol            OBJECT IDENTIFIER(id-CA-DH | id-CA-ECDH),
     domainParameter     AlgorithmIdentifier,
     keyId               INTEGER OPTIONAL
}
```

ChipAuthenticationPublicKeyInfo: Ova struktura podataka osigurava javni ključ za autentifikaciju čipa za čip MRTD.

- Identifikator objekta `protocol` ĆE identifikovati tip javnog ključa (tj. DH ili ECDH).
- Sekvenca `chipAuthenticationPublicKey` ĆE sadržati javni ključ u kodiranom obliku.
- Integralni `keyId` MOŽE biti korišten da se naznači lokalni identifikator ključa. On se MORA koristiti ukoliko čip MRTD osigurava više javnih ključeva za autentifikaciju čipa.

```
id-PK OBJECT IDENTIFIER ::= {
     bsi-de protocols(2) smartcard(2) 1
}

id-PK-DH                            OBJECT IDENTIFIER ::= {id-PK 1}
id-PK-ECDH                          OBJECT IDENTIFIER ::= {id-PK 2}
```

```
ChipAuthenticationPublicKeyInfo ::= SEQUENCE {
     protocol                        OBJECT IDENTIFIER(id-PK-DH |id-PK-ECDH),
     chipAuthenticationPublicKey     SubjectPublicKeyInfo,
     keyId                           INTEGER OPTIONAL
}
```

A.1.1.3. Autentifikacija terminala

Da bi se naznačila podrška za autentifikaciju terminala `SecurityInfos` može sadržati slijedeću stavku:

- TREBA da postoji najmanje jedan `TerminalAuthenticationInfo`.

TerminalAuthenticationInfo: Ova struktura podataka pruža detaljne informacije o implementaciji autentifikacije terminala.

- Identifikator objekta protocol ĆE identifikovati opšti protokol za autentifikaciju terminala, pošto se specifični protokol može promijeniti s vremenom.
- Integralni version ĆE identifikovati verziju protokola. Trenutno su podržane verzije 1 i 2.
- Sekvenca efCVCA se MOŽE koristiti u verziji 1 da se naznači (kratki) identifikator fajla za fajl EF.CVCA. Ona se MORA koristiti ukoliko se ne upotrebljava podrazumijevani (kratki) identifikator fajla.

```
id-TA OBJECT IDENTIFIER ::= {
     bsi-de protocols(2) smartcard(2) 2
}

id-TA-RSA                OBJECT IDENTIFIER ::= {id-TA 1}
id-TA-RSA-v1-5-SHA-1     OBJECT IDENTIFIER ::= {id-TA-RSA 1}
id-TA-RSA-v1-5-SHA-256   OBJECT IDENTIFIER ::= {id-TA-RSA 2}
id-TA-RSA-PSS-SHA-1      OBJECT IDENTIFIER ::= {id-TA-RSA 3}
id-TA-RSA-PSS-SHA-256    OBJECT IDENTIFIER ::= {id-TA-RSA 4}
id-TA-RSA-v1-5-SHA-512   OBJECT IDENTIFIER ::= {id-TA-RSA 5}
id-TA-RSA-PSS-SHA-512    OBJECT IDENTIFIER ::= {id-TA-RSA 6}

id-TA-ECDSA              OBJECT IDENTIFIER ::= {id-TA 2}
id-TA-ECDSA-SHA-1        OBJECT IDENTIFIER ::= {id-TA-ECDSA 1}
id-TA-ECDSA-SHA-224      OBJECT IDENTIFIER ::= {id-TA-ECDSA 2}
id-TA-ECDSA-SHA-256      OBJECT IDENTIFIER ::= {id-TA-ECDSA 3}
id-TA-ECDSA-SHA-384      OBJECT IDENTIFIER ::= {id-TA-ECDSA 4}
id-TA-ECDSA-SHA-512      OBJECT IDENTIFIER ::= {id-TA-ECDSA 5}

TerminalAuthenticationInfo ::= SEQUENCE {
     protocol            OBJECT IDENTIFIER(id-TA),
     version             INTEGER, -- MORA biti 1 za TAv1 ili 2 for TAv2
     efCVCA              FileID OPTIONAL – NE SMIJE SE koristiti za TAv2
}

FileID ::= SEQUENCE {
     fid    OCTET STRING (SIZE(2)),
     sfid OCTET STRING (SIZE(1)) OPTIONAL
}
```

A.1.1.4. Restricted Identification

Da bi se naznačila podrška za ograničenu identifikaciju `SecurityInfos` može sadržati

slijedeću stavku:

- MORA postojati Najmanje jedan `RestrictedIdentificationInfo`.
- MOŽE postojati najviše jedan RestrictedIdentificationDomainParameterInfo.

RestrictedIdentificationInfo: Ova struktura podataka pruža detaljne informacije o implementaciji ograničene identifikacije.

- Identifikator objekta protocol ĆE identifikovati algoritme koji će biti korišteni (tj. dogovor o ključu).
- Integralni version ĆE identifikovati verziju protokola. Trenutno je podržana samo verzija 1.
- Integralni keyId ĆE identifikovati privatni ključ koji će se koristiti.
- Bulov authorizedOnly ĆE indikovati da li je OBAVEZNA eksplicitna autorizacija da bi se koristio odgovarajući tajni ključ.
- Intagralni maxKeyLen se MOŽE koristiti da bi se naznačila maksimalna dužina podržanih ključeva specifičnih za sektor.

```
id-RI OBJECT IDENTIFIER ::= {
     bsi-de protocols(2) smartcard(2) 5
}

id-RI-DH           OBJECT IDENTIFIER ::= {id-RI 1}
id-RI-DH-SHA-1     OBJECT IDENTIFIER ::= {id-RI-DH 1}
id-RI-DH-SHA-224   OBJECT IDENTIFIER ::= {id-RI-DH 2}
id-RI-DH-SHA-256   OBJECT IDENTIFIER ::= {id-RI-DH 3}
id-RI-DH-SHA-384   OBJECT IDENTIFIER ::= {id-RI-DH 4}
id-RI-DH-SHA-512   OBJECT IDENTIFIER ::= {id-RI-DH 5}

id-RI-ECDH         OBJECT IDENTIFIER ::= {id-RI 2}
id-RI-ECDH-SHA-1   OBJECT IDENTIFIER ::= {id-RI-ECDH 1}
id-RI-ECDH-SHA-224 OBJECT IDENTIFIER ::= {id-RI-ECDH 2}
id-RI-ECDH-SHA-256 OBJECT IDENTIFIER ::= {id-RI-ECDH 3}
id-RI-ECDH-SHA-384 OBJECT IDENTIFIER ::= {id-RI-ECDH 4}
id-RI-ECDH-SHA-512 OBJECT IDENTIFIER ::= {id-RI-ECDH 5}

RestrictedIdentificationInfo ::= SEQUENCE {
     protocol      OBJECT IDENTIFIER(
                          id-RI-DH-SHA-1 |
                          id-RI-DH-SHA-224 |
                          id-RI-DH-SHA-256 |
                          id-RI-DH-SHA-384 |
                          id-RI-DH-SHA-512 |
                          id-RI-ECDH-SHA-1 |
                          id-RI-ECDH-SHA-224 |
                          id-RI-ECDH-SHA-256 |
                          id-RI-ECDH-SHA-384 |
                          id-RI-ECDH-SHA-512),
     params ProtocolParams,
     maxKeyLen     INTEGER OPTIONAL
}

ProtocolParams ::= SEQUENCE {
     version             INTEGER, -- MORA biti 1
     keyId               INTEGER,
     authorizedOnly      BOOLEAN
```

```
}
```

RestrictedIdentificationDomainParameterInfo: Ova struktura podataka osigurava set parametara domena koji su korišteni za generisanje javnog ključa PK_{ID} za opoziv čipa MRTD.

- Identifikator objekta `protocol` ĆE identifikovati tip parametara domena (tj. DH ili ECDH).
- Sekvenca `domainParameter` ĆE sadržati parametre domena.

```
RestrictedIdentificationDomainParameterInfo ::= SEQUENCE {
     protocol            OBJECT IDENTIFIER(id-RI-DH | id-RI-ECDH),
     domainParameter     AlgorithmIdentifier
}
```

A.1.1.5. CardInfoLocator (Samo dokumenti Dijela 2)

Da bi se osigurale informacije o mogućnostima i strukturi kartice `SecurityInfos` može sadržati slijedeću stavku:

- TREBA da postoji tačno jedan `CardInfoLocator`.

CardInfoLocator: Ova struktura podataka pruža detaljne informacije o tome gdje se preuzima CardInfo file [5].

- Niz `url` ĆE definisati lokaciju koja osigurava najnoviji CardInfo file za odgovarajući tip i verziju MRTD.
- Sekvenca `efCardInfo` MOŽE se koristiti da se naznači (kratki) identifikator fajla EF.CardInfo.

```
id-CI OBJECT IDENTIFIER ::= {
     bsi-de protocols(2) smartcard(2) 6
}

CardInfoLocator ::= SEQUENCE {
     protocol      OBJECT IDENTIFIER(id-CI),
     url           IA5String,
     efCardInfo    FileID OPTIONAL
}

FileID ::= SEQUENCE {
     fid    OCTET STRING (SIZE(2)),
     sfid   OCTET STRING (SIZE(1)) OPTIONAL
}
```

A.1.1.6. eIDSecurityInfo (Samo dokumenti Dijela 2)

Da bi se zaštitili podaci pohranjeni u eID aplikaciji `SecurityInfos` može sadržati slijedeću stavku:

- TREBA da postoji tačno jedan `eIDSecurityInfo`.

eIDSecurityInfo: Ova struktura podataka osigurava hash vrijednosti izabrane grupe podataka eID aplikacije.

- Sekvenca `eIDSecurityObject` ĆE definisati hash vrijednosti izabranih grupa

podataka

- Sekvenca `eIDVersionInfo` MOŽE se koristit da se identifikuje verzija eID-aplikacije.

```
id-eIDSecurity OBJECT IDENTIFIER ::= {
     bsi-de protocols(2) smartcard(2) 7
}

eIDSecurityInfo ::= SEQUENCE {
     protocol            OBJECT IDENTIFIER(id-eIDSecurity),
     eIDSecurityObject   EIDSecurityObject,
     eIDVersionInfo      EIDVersionInfo OPTIONAL
}

EIDSecurityObject ::= SEQUENCE {
     hashAlgorithm       AlgorithmIdentifier,
     dataGroupHashValues SEQUENCE OF DataGroupHash
}

DataGroupHash ::= SEQUENCE {
     dataGroupNumber     INTEGER,
     dataGroupHashValue  OCTET STRING
}

EIDVersionInfo ::= SEQUENCE {
     eIDVersion          PrintableString,
     unicodeVersion      PrintableString
}
```

A.1.1.7. PrivilegedTerminalInfo (samo dokumenti dijela 2)

Kako bi se dobile dodatne informacije o ključevima autentifikacije čipa ograničene privilegovanim terminalima, `SecurityInfos` mogu sadržavati sljedeći unos:

- Tačno jedan `PrivilegedTerminalInfo` MORA postojati ako su neki ključevi autentifikacije čipa dostupni samo privilegovanim terminalima.

PrivilegedTerminalInfo: Ova struktura podataka pruža `SecurityInfos` vezane za autentifikaciju čipa koristeći individualne ključeve čipa koji su dostupni samo privilegovanim terminalima.

- Set `PrivilegedTerminalInfo` ĆE obuhvatiti `SecurityInfos` prema ključevima autentifikacije čipa koji su dostupni samo privilegovanim terminalima.

```
id-PT OBJECT IDENTIFIER ::= {
     bsi-de protocols(2) smartcard(2) 8
}

PrivilegedTerminalInfo ::= SEQUENCE {
   protocol                    OBJECT IDENTIFIER(id-PT),
   privilegedTerminalInfos     SecurityInfos
}
```

A.1.1.8. Drugi protokoli

`SecurityInfos` MOGU sadržavati reference za protokole koji nisu sadržani u ovoj specifikaciji (uključujući aktivnu autentifikaciju i osnovnu kontrolu pristupa).

Naziv fajla	EF.CardAccess	EF.Card Security	EF.ChipSecurity
Fajl ID	0x011C	0x011D	0x011B
Kratki fajl ID	0x1C	0x1D	0x1B
Pristup očitavanja	UVIJEK	PACE (m) + TA[IS, AT, ST] (o)	PACE+TA[IS or *privileged* AT]
Pristup upisa	NIKADA	NIKADA	NIKADA
Veličina	promjenljivo	promjenljivo	promjenljivo
Sadržaj	DER kodirani SecurityInfos	DER kodirani SignedData	DER kodirani SignedData

Tabela 2 : Osnovni fajlovi pristup kartice, sigurnost kartice i sigurnost čipa

A.1.2. Memorija čipa

MRTD ĆE pružiti `SecurityInfos` u sljedećim transparentnim osnovnim fajlovima sadržanim u master fajlu (vidi tabelu 2):

- CardAccess (USLOVLJENO)

  ĆE biti ako je u čipu implementiran PACE, autentifikacija čipa verzija 2 i/ili autentifikacija terminal verzija 2. BIĆE čitljiv sa svih terminala.

- CardSecurity (USLOVLJENO)

  ĆE biti ako je čip implementirao autentifikaciju čipa verzija 2, autentifikacija terminal verzija 2 ili ograničenu identifikaciju. Pristup očitavanja CardSecurity ĆE biti ograničena terminalima koji su uspješno implementirali PACE i MOGU biti i dalje ograničeni autentifikovanim terminalima

- ChipSecurity (OPCIONALNO)

  Pristup očitavanja ChipSecurity ĆE biti ograničen autentifikovanim privilegovanim terminalima. Ako je taj opcionalni fajl dostupan, svi relevantni privatni `SecurityInfos` TREBAJU biti sačuvani na ChipSecurity i NE TREBAJU biti uključeni u CardSecurity.

Ako su PACE prema[10],autentifikacija terminala verzija 1 ili autentifikacija čipa implementirani, MRTD čip će osigurati `SecurityInfos` u elementarnom fajlu DG14 sadržanom u aplikaciji ePasoš.

A.1.2.1. CardAccess (USLOVLJENO)

Ako postoji, CardAccess će sadržavati relevantne `SecurityInfos` koje su potrebne za pristup aplikacijama:

- PACEInfo (ZAHTJEVANO)
- PACEDomainParameterInfo (USLOVLJENO)
  - Ova struktura (e) MORA postojati ako se koriste eksplicitni parametri domena.
- ChipAuthenticationInfo (USLOVLJENO)
  - Ova struktura MORA postojati ako je podržana autentifikacija čipa u verziji 2 i pristup očitavanja CardSecurity je ograničen autentifikovanim terminalima.
- ChipAuthenticationDomainParameterInfo (USLOVLJENO)
  - Ova struktura MORA postojati ako je podržana autentifikacija čipa u verziji 2 i pristup očitavanja CardSecurity je ograničen autentifikovanim terminalima.
- TerminalAuthenticationInfo (USLOVLJENO)
  - Ova struktura MORA postojati ako je podržana autentifikacija terminal u verziji 2.
- CardInfoLocator (PREPORUČENO)
- PrivilegedTerminalInfo (USLOVLJENO)
  - Ova struktura mora postojati ako neki su ključevi autentifikacije čipa u verziji 2 dostupni samo privilegovanim terminalima i pristup očitavanja CardSecurity je ograničen autentifikovanim terminalima.
  - Ova struktura ĆE obuhvatiti odgovarajuće `SecurityInfos`, odnosno za svaki ključ autentifikacije čipa koji je ograničen privilegovanim terminalima, ChipAuthenticationInfo i ChipAuthenticationDomainParameterInfo MORAJU biti uključeni tako da povezuju identifikator ključa.

A.1.2.2. CardSecurity (USLOVLJENO)

Ako postoji, fajl CardSecurity:

- ĆE sadržavati potpisan SecurityInfos koji MRTD čip podržava.
- ĆE sadržavati sve SecurityInfos sadržane u CardAccess osim PrivilegedTerminalInfo,
- ako su neki ključevi autentifikacije čipa verzija 2 dostupni samo privilegovanim terminalima a nijedan PrivilegedTerminalInfo nije sadržan u CardAccess, CardSecurity ĆE sadržavati PrivilegedTerminalInfo, koje obuhvataju odgovarajuće SecurityInfos,
- ĆE sadržavati odgovarajući ChipAuthenticationPublicKeyInfo za svaki ključ koji ChipAuthenticationInfo povezuje (isključujući ključeve povezane u

PrivilegedTerminalInfo).

Generisani specifični ključevi se TREBAJU koristiti umjesto ključeva individualnog čipa.

PREPORUČUJE se da se `eIDSecurityInfo` ne koristi u ovom fajlu.

A.1.2.3. ChipSecurity (OPCIONALNO)

Ako postoji, fajl CardSecurity ĆE sadržavati:

- potpisane `SecurityInfos` koje MRTD čip podržava,
- sve `SecurityInfos` sadržane u CardAccess, i
- odgovarajući ChipAuthenticationPublicKeyInfo za svaki ključ koji ChipAuthenticationInfo povezuje. Odgovarajući ChipAuthenticationPublicKeyInfo MORA takođe biti uključen u PrivilegedTerminalInfo. Svi ključevi povezani u PrivilegedTerminalInfo TREBAJU biti ključevi individualnog čipa.

PREPORUČENO je da se `eIDSecurityInfo` koristi kako bi osigurale hash-ove (statičnih) grupa podatak vezanih za lične podatke nosioca.

A.1.2.4. ePasoš DG14 (USLOVLJENO)

Ako čip implementira PACE prema [10], autentifikaciju terminala verzija 1 ili autentifikacija čipa verzija 1, MRTD čip ĆE takođe osigurati `SecurityInfos` u grupi podataka DG14 aplikacije ePasoš. PREPORUČENO je da DG14 i ChipSecurity (ako postoji) sadrže iste ključeve.

A.1.2.5. Format potpisa za CardSecurity i ChipSecurity

Fajlovi CardSecurity i ChipSecurity ĆE biti implementirane kao `SignedData` prema [7] sa tipom sadržaja `SecurityInfos`. Potpisnik dokumenta ĆE potpisati objekte sigurnosti. Certifikat potpisnika dokumenta MORA biti uključen u `SignedData`. Sljedeći identifikatori objekta ĆE se koristiti za identifikaciju tipa sadržaja:

```
id-SecurityObject OBJECT IDENTIFIER ::= {
     bsi-de applications(3) eID(2) 1
}
```

Struktura podataka SignedData je definisana u nastavku; više detalja se može pronaći u [7]:

```
SignedData ::= SEQUENCE{
     version CMSVersion,
     digestAlgorithms DigestAlgorithmIdentifiers,
     encapContentInfo EncapsulatedContentInfo,
     certificates [0] IMPLICIT CertificateSet OPTIONAL,
     crls [1] IMPLICIT RevocationInfoChoices OPTIONAL
     signerInfos SignerInfos
}

DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier
EncapsulatedContentInfo ::= SEQUENCE {
     eContentType ContentType,
     eContent [0] EXPLICIT OCTET STRING OPTIONAL
}
```

Algoritam / Format	DH	ECDH

Algoritam za dogovor ključeva	PKCS#3 [27]	ECKA [3]
X.509 Format javnog ključa	X9.42 [1]	ECC [3]
TLV Format javnog ključa	TLV, cf. Appendix D.3.2	TLV, cf. Appendix D.3.3
Kompresija javnog ključa	SHA-1 [23]	X-Coordinate
Potvrđivanje privremenog javnog ključa	RFC 2631 [26]	ECC [3]

Tabela 3: Algoritmi i formati za dogovor ključeva

```
ContentType ::= OBJECT IDENTIFIER SignerInfos ::= SET OF SignerInfo

SignerInfo ::= SEQUENCE {
      version CMSVersion,
      sid SignerIdentifier,
      digestAlgorithm DigestAlgorithmIdentifier,
      signatureAlgoritm SignatureAlgorithmIdentifier,
      signature SignatureValue
}
SignerIdentifier ::= CHOICE {
      issuerAndSerialNumber IssuerAndSerialNumber,
      subjectKeyIdentifier [0] SubjectKeyIdentifier
}

SignatureValue ::= OCTET STRING
```

A.2. Dogovor ključeva

PACE, autentifikacija čipa i ograničena identifikacija se baziraju na protokolima dogovora ključeva. Ovaj dodatak određuje opšte algoritme, formate i protokole.

A.2.1. Parametri domena

Sa izuzetkom parametra domena sadržanim u `PACEInfo`, svi parametric domena ĆE biti dani kao `AlgorithmIdentifier` , struktura podataka je definisana na sljedeći način; više detalja se može pronaći u [6]:

```
AlgorithmIdentifier ::= SEQUENCE {
      algorithm     OBJECT IDENTIFIER,
      parameters ANY DEFINED BY algorithm OPTIONAL
}
```

Sa `PACEInfo`, identifikacioni broj standardizovanih parametara domena opisanih u tabeli 4. ĆE biti direktno povezani. Eksplicitni parametri domena dobijeni iz `PACEDomainParameterInfo` NE SMIJU koristiti one identifikacione brojeve rezervisane za standardizovane parametre domena.

A.2.1.1. Standardizovani parametri domena

Standardizovani parametri domena opisani u tabeli 4. se TREBAJU koristiti. Sljedeći identifikator objekta se TREBA koristiti da poveže standardizovane parametre domena u `AlgorithmIdentifier`:

```
standardizedDomainParameters OBJECT IDENTIFIER ::= {
      bsi-de algorithms(1) 2
}
```

Sa `AlgorithmIdentifier` ovaj identifikator objekta ĆE referencirati identifikacioni broj standardizovanog parametra domena kao u tabeli 4. kao `INTEGER`.

ID	Naziv	Veličina	Tip	Referenca
0	1024-bit MODP Group with 160-bit Prime Order	1024/160	GFP	[19]
1	2048-bit MODP Group with 224-bit Prime Order	2048/224	GFP	[19]
2	2048-bit MODP Group with 256-bit Prime Order	2048/256	GFP	[19]
3 – 7	RFU			
8	NIST P-192 (secp192r1)	192	ECP	[25], [19]
9	BrainpoolP192r1	192	ECP	[20]
10	NIST P-224 (secp224r1)*	224	ECP	[25], [19]
11	BrainpoolP224r1	224	ECP	[20]
12	NIST P-256 (secp256r1)	256	ECP	[25], [19]
13	BrainpoolP256r1	256	ECP	[20]
14	BrainpoolP320r1	320	ECP	[20]
15	NIST P-384 (secp384r1)	384	ECP	[25], [19]
16	BrainpoolP384r1	384	ECP	[20]
17	BrainpoolP512r1	512	ECP	[20]
18	NIST P-521 (secp521r1)	521	ECP	[25], [19]
19-	RFU			
* Ova kriva se ne može koristiti sa integrisanim mapiranjem.				

Tabela 4: Standardizovani parametri domena

A.2.1.2. Eksplicitni parametri domena

Eksplicitni parametri domena mogu biti sadržani u sljedećim strukturama:

- PACEDomainParameterInfo,
- ChipAuthenticationPublicKeyInfo,
- ChipAuthenticationDomainParameterInfo, i
- RestrictedIdentificationDomainParameterInfo

Identifikator objekta `dhpublicnumber` ili `ecPublicKey` za DH ili ECDH, svaki posebno, ĆE biti korišteni d povežu eksplicitne parameter domena u `AlgorithmIdentifier`:

```
dhpublicnumber OBJECT IDENTIFIER ::= {
     iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1
}
ecPublicKey OBJECT IDENTIFIER ::= {
     iso(1) member-body(2) us(840) ansi-x962(10045) keyType(2) 1
}
```

U slučaju eliptičnih kriva parametri domena MORAJU biti opisani eksplicitno u strukturi ECParameters, tj. NE SMIJU se koristiti pomenute krive i implicitni parametri domena.

A.2.1.3. PACE i autentifikacija čipa

MRTD čip MOŽE podržavati vise od jednog seta parametara domena (tj. čip može podržavati različite algoritme i/ili dužine kjluča) za PACE i autentifikaciju čipa verzija 1 i 2.

- Parametri domena sadržani u EF.CardAccess, tj. `PACEDomainParameterInfo` i `ChipAuthenticationDomainParameterInfo` (za autentifikaciju čipa verzija 2), su nezaštićeni i mogu biti nesigurni. Korištenje nesigurnih parametara domena može dovesti do napada, npr. korištenje nesigurnih parametara domena za PACE ĆE dovesti do obznanjivanje šifre.
- MRTD čipovi moraju podržavati najmanje jedan set standardizovanih parametara domena za PACE i autentifikaciju čipa verzija 2, ako su odgovarajući parametri implementirani kao sto je navedeno u tabeli 4.
- Terminali NE SMIJU koristiti neverfikovane parametre domena za PACE i autentifikaciju čipa verziju 2, tj. samo se koriste standardizovani parametri domena ili parametri domena koje eksplicitno terminal prepozna kao sigurne.
- Parametri domena sadržani u ChipAuthenticationDomainParameterInfo
- i `ChipAuthenticationPublicKeyInfo` su zaštićeni objektom sigurnosti.
- Autentifikacija čipa u verziji MORA osigurati najmanje jedan set eksplicitnih parametara domena.

A.2.1.4. Ograničena identifikacija

Parametri domena za ograničenu identifikaciju su definisani verifikatorom dokumenta i MORAJU se osigurati zajedno sa sektorskim javnim ključem u objektu podataka javnog ključa kao dio ograničene identifikacije (vidi prilog D.3 i B.4.1). Hash objekta podataka javnog ključa MORA biti sadržan u certifikatu terminal kao ekstenzija sektora terminala (vidi prilog C.3.2). MRTD čip MORA verifikovati sektorski javni ključ koristeći ekstenziju sektora terminala.

Šifra	Kodiranje
MRZ	SHA-1(Serial Number || Date of Birth || Date of Expiry)
CAN	Character String (cf. Appendix D.2.1.4)
PIN	Character String (cf. Appendix D.2.1.4)
PUK	Character String (cf. Appendix D.2.1.4)

Tabela 5: Kodiranje šifri

A.2.2. Privremeni javni ključevi („Ephemeral Public Keys“)

A.2.2.1. PACE i autentifikacija čipa

Terminal za generisanje privremenog javnog ključa za PACE i autentifikaciju čipa verzija 1 /2, svaka posebno, MORA koristiti parametre domena sadržane u `PACEInfo` ili `PACEDomainParameterInfo` i `ChipAuthenticationDomainParameterInfo` ili `ChipAuthenticationPublicKeyInfo`. Privremeni javni ključevi se moraju razmijeniti

kao proste vrijednosti javnog ključa. Više informacija o kodiranju se može pronaći u prilogu D.3.4.

Napomena: PREPORUČENA je validacija privremenih javnih ključeva. Za DH, validacija algoritma zahtjeva da MRTDF čip detaljnije poznaje parametre domena (tj. Raspored korištene podgrupe) nego što inače osigura PKCS#3.

A.2.2.2. Ograničena identifikacija

Privremeni javni ključevi se ne koriste za ograničenu identifikaciju.

A.2.2.3. Kompresija javnog ključa

Kompresovani privremeni javni ključ terminala **Comp** ($\widetilde{PK}_{PCD}$) kao što je zahtjevano za autentifikaciju terminala je definisan na sljedeći način:

- Za DH je kompresovani javni ključ SHA-1 hash DH javne vrijednosti, tj. oktetni niz fiksne dužine 20.
- Za ECDH kompresovani privremeni ključ je x-koordinata ECDH javne tačke, tj. oktetni niz fiksne dužine ($\log_{256} p$).

A.2.3. Funkcija izvođenja ključeva

Neka su $\mathbf{KDF}_{\mathbf{Enc}}(K,[r])=\mathbf{KDF}(K,[r],1)$, $\mathbf{KDF}_{\mathbf{MAC}}(K,[r])=\mathbf{KDF}(K,[r],2)$ funkcije izvođenja ključeva koje izvode ključeve za enkripciju iautentifikaciju, svaki posebno, iz zajedničke šifre K i opcionalnog broja *nonce* r.

Neka je $\mathbf{KDF}_{\pi}(\pi)=\mathbf{KDF}(f(\pi),3)$ funkcija izvođenja ključeva za izvođenje iz šifre π. Kodirenje šifre , tj.$K=f(\pi)$ je definisano u tebeli 5.

Funkcija izvođenja ključa $\mathbf{KDF}(K,[r],c)$, je definisana na sljedeći način:

Ulaz: Sljedeći ulazi su potrebni:

• zajednička tajna vrijednost K **(ZAHTJEVANO)**

• nonce broj r **(OPCIONALNO)**

• 32-bitni, big-endian integer counter c **(ZAHTJEVANO)**

Izlaz: Oktetni niz ključnih podataka.

Akcije: sljedeće akcije su izvršene:

1. ključni podatak=$\mathbf{H}(K\|r\|c)$
2. Izlaz oktetni niza ključnih podataka

Funkcija izvođenja ključa $\mathbf{KDF}(K,[r],c)$ zahtjeva odgovarajuću hash funkciju izvedenu od **H**(), tj. dužina u bitima hash funkcije ĆE biti interpretirana kao veća i jednaka dužina u bitima izvedenog ključa. Vrijednost hasha-a ĆE biti interpretirana kao big-endian bajt izlaz.

Nonce broj r se koristi samo za autentifikaciju čipa verzija 2.

Napomena: Zajednička tajna K je definisana kao oktetni niz. Ako je zajednička tajna generisana sa ECKA [3], x-koordinata generisane tačkeĆE se koristiti.

A.2.3.1. 3DES

Da bi se izveli 112-bitni 3DES [21] ključevi, hash funkcija SHA-1 [23] ĆE se koristiti i MORAJU se izvršiti sljedeći dodatni koraci:

- koristiti oktete 1 do 8 podataka ključa za formiranje podataka ključa A i okteta 9 do 16 podataka ključa B; nisu korišteni dodatni okteti,
- podesiti bitove pariteta podataka ključaA i ključa podatakaB za formiranje tačnih DES ključeva (OPCIONALNO).

A.2.3.2. AES

Da bi se izveli 128-bitni AES [22] ključevi, hash funkcija SHA-1 [23] ĆE se koristiti i MORAJU se izvršiti sljedeći dodatni koraci:

- koristiti oktete 1 do 16 podataka ključa; nisu korišteni dodatni okteti.

Da bi se izveli 192-bitni i 256-bitni AES [22] ključevi SHA-256 [23] ĆE se koristiti. Za 192-bitne AES ključeve MORAJU se izvršiti sljedeći dodatni koraci:

- koristiti oktete 1 do 24 podataka ključa; nisu korišteni dodatni okteti.

A.2.4. Token za autentifikaciju

Token za autentifikaciju korišten u PACE i autentifikaciji čipa verzija 2 ĆE biti izračunat preko objekta podataka javnog ključa (vidi prilog D.3) koji sadrži identifikator objekta korištenog protokola, tj. PACE ili autentifikacija čipa (kao što je naznačeno u MSE:Set AT, vidi prilog B.11.1), i preko zaprimljenog privremenog javnog ključa koristeći kod za autentifikaciju u ključ izveden iz dogovora ključeva.

A.2.4.1. 3DES

3DES [21] ĆE se koristiti u maloprodajni mode u skladu sa ISO/IEC 9797-1 [16] MAC algoritam 3 metod popunjavanja 2 sa blok šifrom DES i $IV = 0$.

A.2.4.2. AES

AES [22] ĆE se koristiti u CMAC modelu [24] sa MAC dužinom od 8 bajta.

A.3. PACE

A.3.1. PACE sa DH

Za PACE sa DH se MORAJU koristiti odgovarajući algoritmi i formati iz tabele A.2 i tabele 6.

OID	Mapiranje	Sim. šifra	Duž. ključa	Sigurna razmjena poruka	Token za aut.
id-PACE-DH-GM-3DES-CBC-CBC	Generic	3DES	112	CBC / CBC	CBC
id-PACE-DH-GM-AES-CBC-CMAC-128	Generic	AES	128	CBC / CMAC	CMAC
id-PACE-DH-GM-AES-CBC-CMAC-192	Generic	AES	192	CBC / CMAC	CMAC
id-PACE-DH-GM-AES-CBC-CMAC-256	Generic	AES	256	CBC / CMAC	CMAC

id-PACE-DH-IM-3DES-CBC-CBC	Integrated	3DES	112	CBC / CBC	CBC
id-PACE-DH-IM-AES-CBC-CMAC-128	Integrated	AES	128	CBC / CMAC	CMAC
id-PACE-DH-IM-AES-CBC-CMAC-192	Integrated	AES	192	CBC / CMAC	CMAC
id-PACE-DH-IM-AES-CBC-CMAC-256	Integrated	AES	256	CBC / CMAC	CMAC

Tabela 6: Identifikatori objekta za PACE sa DH

A.3.2. PACE sa ECDH

Za PACE sa ECDH se MORAJU koristiti odgovarajući algoritmi i formati iz tabele A.2 i tabele 7.

OID	Mapiranje	Sim. šifra	Duž. ključa	Sigurna razmjena poruka	Token za aut.
id-PACE-ECDH-GM-3DES-CBC-CBC	Generic	3DES	112	CBC / CBC	CBC
id-PACE-ECDH-GM-AES-CBC-CMAC-128	Generic	AES	128	CBC / CMAC	CMAC
id-PACE-ECDH-GM-AES-CBC-CMAC-192	Generic	AES	192	CBC / CMAC	CMAC
id-PACE-ECDH-GM-AES-CBC-CMAC-256	Generic	AES	256	CBC / CMAC	CMAC
id-PACE-ECDH-IM-3DES-CBC-CBC	Integrated	3DES	112	CBC / CBC	CBC
id-PACE-ECDH-IM-AES-CBC-CMAC-128	Integrated	AES	128	CBC / CMAC	CMAC
id-PACE-ECDH-IM-AES-CBC-CMAC-192	Integrated	AES	192	CBC / CMAC	CMAC
id-PACE-ECDH-IM-AES-CBC-CMAC-256	Integrated	AES	256	CBC / CMAC	CMAC

Tabela 7: Identifikatori objekta za PACE sa ECDH

A.3.3. Kodirani nonce broj

MRTD čip ĆE nasumično i jednoobrazno izabrati nonce broj $s \in \{0 \ldots 2^l - 1\}$ kao binarni bitni niz dužine l, gdje je l multiple blok veličine u bitima odgovarajuće blok šifre $\mathbf{E}()$ koju izabere MRTD čip.

- Nonce broj s ĆE biti kodiran u CBC modulu u skladu sa ISO 10116 [12] koristeći ključ $K_\pi = \mathbf{KDF}_\pi(\pi)$ izvedenu iz šifre π i $IV = 0$.
- Nonce broj s ĆE biti konvertovan u **nasumičan** generator koristeći specifičnu algoritamsku funkciju mapiranjaa **Map**.

Napomena: Postoji nekoliko različitih algoritama za implementiranje mapiranja nonce broja u privremene parametre domena. Trenutno, sva specifična mapiranja mapiraju nonce broj u privremeni generator. PREPORUČUJE SE implementacija mapiranja kao slučajno odabrana funkcija.

A.3.4. ECDH Mapiranje

Neka G i $\tilde{G}$ budu statički i privremeni

A.3.4.1. Generičko mapiranje

Funkcija **Map**: G↦ $\tilde{G}$ se definiše kao $\tilde{G}$= s· G+H, gdje je H∈ $\langle G \rangle$ je odabrano s.th $\log_G$ H je nepoznat. Tačka H ĆE biti izračunata anonimnim Diffie-Hellman dogovorom ključeva[3].

Napomena: Algoritam dogovora ključeva ECKA sprečava male podgrupne napade korištenjem kompatibilne kofaktor umnožavanja.

A.3.4.2. Integrisano mapiranje

Integrisano ECDH mapiranje je definisano sa ICAO [10].

A.3.5. DH Mapiranje

Neka g i $\tilde{g}$ budu statični i privremeni generator.

A.3.5.1. Generičko mapiranje

Funkcija **Map**: g↦ $\tilde{g}$ je definisana kao $\tilde{g} = g^s h$, gdje je $h \in \langle g \rangle$ izabran s.th. $\log_g h$ je nepoznat. Grupni element h ĆE biti izračunat anonimnim Diffie-Hellman dogovorom ključeva.

Napomena: Metod validacije javnog ključa koji je opisan u RFC 2631 [26] se MORA koristiti kako bi se spriječili mali podgrupni napadi.

A.3.5.2. Integrisano mapiranje

Integrisano DH mapiranje je definisano sa ICAO [10].

A.4. Autentifikacija čipa

A.4.1. Par ključeva za autentifikaciju čipa

Par(ovi) ključeva za autentifikaciju čipa MORAJU biti sačuvani na MRTD čipu.

- Privatni ključ ĆE biti sigurno sačuvan u memoriji MRTD čipu.
- Javni ključ ĆE biti osiguran kao `SubjectPublicKeyInfo` u strukturi `ChipAuthenticationPublicKeyInfo`.
- Parametri domena MOGU biti dodatno osigurani kao `AlgorithmIdentifier` strukturi `ChipAuthenticationDomainParameterInfo`.

Strukture podataka `SubjectPublicKeyInfo` i `AlgorithmIdentifier` su definisane na sljedeći način ; više detalja možete pronaći u [6]:

```
SubjectPublicKeyInfo ::= SEQUENCE {
     algorithm           AlgorithmIdentifier,
     subjectPublicKey    BIT STRING
}

AlgorithmIdentifier ::= SEQUENCE {
  algorithm       OBJECT IDENTIFIER,
  parameters      ANY DEFINED BY algorithm OPTIONAL
}
```

MRTD čip MOŽE podržavati više od jednog para ključeva za autentifikaciju čipa (tj. čip može podržavati različite algoritme i/ili dužine ključeva). U tom slučaju, lokalni

identifikator ključa MORA biti objavljen u odgovarajućim `ChipAuthenticationInfo`, `ChipAuthenticationPublicKeyInfo`, i `ChipAuthenticationDomainParameterInfo`.

A.4.2. Autentifikacija čipa sa DH

Za autentifikaciju čipa sa DH, određeni algoritmi i formati iz tabele A.2 i tabele 8 se MORAJU koristiti. Za autentifikaciju čipa verzija 1 PKCS#3 [27] se MORA koristiti umjesto X9.42 [1].

OID	Sim. šifra	Dužina ključa	Sigurna razmjena poruka	Token za aut.
id-CA-DH-3DES-CBC-CBC	3DES	112	CBC / CBC	CBC
id-CA-DH-AES-CBC-	AES	128	CBC / CMAC	CMAC
id-CA-DH-AES-CBC-	AES	192	CBC / CMAC	CMAC
id-CA-DH-AES-CBC-	AES	256	CBC / CMAC	CMAC

Tabela 8: Identifikatori objekta za autentifikaciju čipa sa DH

A.4.3. Autentifikacija čipa sa ECDH

Odgovarajući algoritmi i formati iz tabele A.2 i tabele 9 se MORAJU koristiti za autentifikaciju čipa sa ECDH

OID	Sim. šifra	Dužina ključa	Sigurna razmjena poruka	Token za aut.
id-CA-ECDH-3DES-CBC-CBC	3DES	112	CBC / CBC	CBC
id-CA-ECDH-AES-CBC-	AES	128	CBC / CMAC	CMAC
id-CA-ECDH-AES-CBC-	AES	192	CBC / CMAC	CMAC
id-CA-ECDH-AES-CBC-	AES	256	CBC / CMAC	CMAC

Tabela 9: Identifikatori objekta za autentifikaciju čipa sa ECDH

A.5. Ograničena identifikacija

A.5.1. MRTD čip privatnog ključa

Generisanje privatnog ključa SK_{ID} nije obuhvaćeno ovom specifikacijom. Ako je SK_{ID} generisan kao kodirani sekvencijalni brojač ili kao kodirani broj dokumenta, treća strana ĆE generisati i sigurno sačuvati tajni kodirani ključ.

2.7.7 A.5.2. Javni ključevi za sektor

Treća (provjerena) strana MORA generisati javne ključeve sektora.

- Ako treća strana MORA mora biti u mogućnosti da poveže sektorske specifične identifikatore po sektorima, onda ĆE treća strana generisati parove ključeva sektora i sačuvati sigurno privatne ključeve sektora.
- Ako treća strana NE MORA biti u mogućnosti da poveže sektorske specifične

identifikatore po sektorima, onda ĆE treća strana generisati parove ključeva sektora tako da su odgovarajući privatni ključevi nepoznati.

A.5.3. Ograničena identifikacija sa DH

Odgovarajući algoritmi i formati iz tabele A.2 i tabele 10 se MORAJU koristiti za ograničenu identifikaciju sa DH.

OID	Hash
id-RI-DH-SHA-1	SHA-1
id-RI-DH-SHA-224	SHA-224
id-RI-DH-SHA-256	SHA-256
id-RI-DH-SHA-384	SHA-384
id-RI-DH-SHA-512	SHA-512

Tabela 10: Identifikatori objekta za ograničenu identifikaciju sa DH

A.5.4. Ograničena identifikacija sa ECDH

Odgovarajući algoritmi i formati iz tabele A.2 i tabele 11 se MORAJU koristiti za ograničenu identifikaciju sa ECDH. Ulaz u hash funkciju ĆE biti x-koordinata tačke koji je ECKA[3] generisala.

OID	Hash
id-RI-ECDH-SHA-1	SHA-1
id-RI-ECDH-SHA-224	SHA-224
id-RI-ECDH-SHA-256	SHA-256
id-RI-ECDH-SHA-384	SHA-384
id-RI-ECDH-SHA-512	SHA-512

Tabela 11: Identifikatori objekta za ograničenu identifikaciju sa ECDH

2.8 A.6. Autentifikacija terminala

2.8.1 A.6.1. Reference javnog ključa

Javni ključevi koji se koriste za autentifikaciju terminala MORAJU biti sadržani u CV certifikatima u skladu sa profilom certifikata definisanom u prilogu C.1. svaki CV certifikat MORA sadržavati dvije reference javnog ključa, *referenca nosioca certifikata* i *referenca certifikacionog tijela*:

Referenca nosioca certifikata: Referenca nosioca certifikata je identifikator za javni ključ koji je osiguran u certifikatu koji ĆE se koristiti za referencu ovog javnog ključa.

Referenca certifikacionog tijela: Referenca certifikacionog tijela je referenca (eksternog) javnog ključa certifikacionog tijela koji ĆE se koristiti za verifikovanje potpisa certifikata.

Napomena: Kao posljedica referenca certifikacionog tijela sadržanog u certifikatu MORA biti jednaka referenci nosioca certifikata u odgovarajućem certifikatu certifikacionog tijela nadležnog za izdavanje

	Kodiranje	Dužina
Pozivni broj	ISO 3166-1 ALPHA-2	2F
Mnemonika nosioca	ISO/IEC 8859-1	9V
Broj sekvenci	ISO/IEC 8859-1	5F
F: fiksna dužina (tačan broj okteta) V: promjenljiva dužina (do određenog broja okteta)		

Tabela 12: Referenca nosioca certifikata

Referenca nosioca certifikata ĆE se sastojati od sljedećih uvezanih elemenata: *pozivni broj, mnemonika nosioca, i redni broj.* Ovi elementi se MORAJU birati u skladu sa tabelom 12 i sljedećim pravilima.

1. Kod zemlje

Poziv na broj ĆE biti ISO 3166-1 ALPHA-2 broj države nosioca certifikata.

2. Mnemonika nosioca

Mnemonika nosioca ĆE biti biti dodjeljena kao jedinstven identifikator kako slijedi:

- CVCA ĆE dodijeliti mnemoniku nosioca CVCA.
- Domaći CVCA ĆE dodijeliti mnemoniku nosioca DV.
- Nadzorni DV ĆE dodijeliti mnemoniku nosioca IS.

3. Broj sekvenci

Nosilac certifikata ĆE dodijeliti broj sekvenci.

- Broj sekvenci MORA biti numerički ili alfanumerički:
  - numerički broj sekvenci ĆE se sastojati od znakova“0”...”9”.
  - alfanumerički broj sekvenci ĆE se sastojati od znakova“0”...”9” i “A”...”Z”.
- Broj sekvenci MOŽE početi sa ISO 3166-1 ALPHA-2 pozivnim brojem nadležnog organa za certifikaciju, a preostala tri znaka ĆE biti alfanumerički broj sekvenci.
- Broj sekvenci MOŽE biti resetovan ako su svi dostupni brojevi sekvenci iscrpljeni.

A.6.2. Import javnog ključa

Javni ključevi koji su uvezeni procedurom validacije certifikata (vidi odjeljak 2.5) su ili *trajno* ili *privremeno* sačuvani na MRTD čipu. MRTD čip TREBA da odbije import javnog ključa ako je referenca nosioca certifikata već poznata čipu.

A.6.2.1. Trajni uvoz

Javni ključevi koji su sadržani u CVCA link certifikatima ĆE biti trajno importovani od strane MRTD čipa i MORAJU biti sigurno sačuvani na memoriji MRTD čipa. Trajno importovan javni ključi i njegovi metapodaci ĆE ispuniti sljedeće uslove:

- MOŽE biti zamjenjen *nakon isteka* naknadnim trajnim importovanim ključem.
- MORA biti zamjenjen naknadnim trajnim uvezenim ključem sa istom referencom

nosioca certifikata ili import MORA biti odbijen.

- NE SMIJE biti zamjenjen privremenim importovanim javnim ključem.

Napomena: PREPORUČUJE se odbijanje importa javnog ključa ako je referenca nosioca certifikata već poznata MRTD čipu.

Omogućavanje i onemogućavanje trajno importovanog javnog ključa mora biti atomic operacija.

A.6.2.2. Privremeni uvoz

Javne ključeve koji su sadržani u DV i certifikatima terminala ĆE privremeno importovati MRTD čip. Privremeno importovan javni ključ i njegovi metapodaci ĆE ispuniti sljedeće uslove:

- NEĆE se moći selektovati i koristiti nakon gašenja MRTD čipa.
- MORA ostati upotrebljiv do završetka zamjene kriptografske operacije (tj. PSO:Verify Certificate ili External Authenticate).
- MOŽE biti zamjenjen naknadnim privremenim importovanim javnim ključem.

Terminal NE SMIJE koristiti bilo koje druge privremeno importovane ključeve osim onih koji su posljedni importovani.

Ime fajla	EF.CVCA
ID fajl	0x011C (default)
Kratki fajl ID	0x1C (default)
Pristup očitavanja	BAC *or* PACE (conditional to protocol support)
Pristup upisa	NEVER (internally updated only)
Veličina	36 bytes (fixed) padded with octets of value 0x00
Sadržaj	[CARi][||CARi-1][||0x00..00]

Tabela 13: Osnovni fajl EF.CVCA

A.6.2.3. Importovani metapodaci

Za svaki trajni ili privremeni importovani javni ključ, sljedeći dodatni podaci koji su sadržani u certifikatu (vidi odjeljak C.1) MORAJU biti sačuvani:

- Referenca nosioca certifikata
- Autorizacija nosioca certifikata (važeća rola i važeća autorizacija)
- Datum stupanja na snagu certifikata
- Datum isteka certifikata
- Produženja certifikata (gdje je primjenljivo)

Računanje efikasne role (CVCA, DV ili terminal) i efektivna autorizacija nosioca certifikata je opisana u odjeljku 2.6.

Napomena: Format sačuvanih podataka funkcioniše neovisno o sistemu i nije sadržana u ovoj specifikaciji.

A.6.2.4. EF.CVCA

Podrška za osnovni fajl EF.CVCA je USLOVLJENA. Ako MRTD čip podržava autentifikaciju terminala u verziji 1, mora uraditi reference CVCA javnih ključeva koji odgovaraju za inspekcijske sisteme dostupne u transparentnom osnovnom fajlu EF.CVCA koji je sadržan u ePasoš aplikaciji kao što je definisano u tabeli 13.

Ovaj fajl ĆE sadržavati sekvencu objekata podataka(vidi prilog D.2) reference certifikacijskog tijela (CAR) odgovarajućih za autentifikaciju terminala.

- Fajl ĆE sadržavati najviše dva objekta podataka reference certifikacijskog tijela.
- Posljednja referenca certifikacijskog tijela ĆE biti prvi objekat podataka na ovoj listi.
- Fajl MORA biti popunjen sa dodatnim oktetima u vrijednosti 0x00.

Fajl EF.CVCA ima identifikator i kratki identifikator fajla. Ako se zadana vrijednost ne može koristiti, (kratki) identifikator fajla ĆE biti definisan u OPCIONALNOM parametru `efCVCA` od `TerminalAuthenticationInfo`. Ako se `efCVCA` koristi za označavanje identifikatora fajla koji će se koristiti, početni fajl će se poništiti. Ako u `efCVCA` nije ponuđen kratki fajl, fajl EF.CVCA MORA biti eksplicitno odabran koristeći dati identifikator fajla.

A.6.3. Autentifikacija terminala sa RSA

Za autentifikacija terminala sa RSA MORAJU se koristiti sljedeći algoritmi i formati.

A.6.3.1. Algoritam potpisa

RSA [18], [28] kao što je definisano u tabeli 14 ĆE se koristiti. Početni parametri koji će se koristiti sa RSA-PSS su definisani kako slijedi:

- Hash algoritam: hash algoritam je odabran u skladu sa tabelom 14.
- Algoritam generisanja maska: MGF1 [18], [28] koristeći hash algoritam.
- Salt dužina: oktetna dužina izlaza odabranog hash algoritma.
- Trailer Field: 0xBC

A.6.3.2. Format javnog ključa

TLV-format [15] kao što je opisan u prilogu D.3.1 ĆE se koristiti.

- Identifikator objekta ĆE se uzeti iz tabele 14.
- Dužina modula u bitima ĆE biti 1024, 1280, 1536, 2048, or 3072.
- Dužina eksponata u bitima Će biti najviše 32.

A.6.4. Autentifikacija terminala sa ECDSA

Za autentifikaciju terminala sa ECDSA MORAJU se koristiti sljedeći algoritmi i formati.

OID	Potpis	Hash	Parametri
id-TA-RSA-v1-5-SHA-1	RSASSA-PKCS1-v1_5	SHA-1	N/A

id-TA-RSA-v1-5-SHA-256	RSASSA-PKCS1-v1_5	SHA-256	N/A
id-TA-RSA-v1-5-SHA-512	RSASSA-PKCS1-v1_5	SHA-512	N/A
id-TA-RSA-PSS-SHA-1	RSASSA-PSS	SHA-1	default
id-TA-RSA-PSS-SHA-256	RSASSA-PSS	SHA-256	default
id-TA-RSA-PSS-SHA-512	RSASSA-PSS	SHA-512	default

Tabela 14: Identifikatori objekta za autentifikaciju terminala sa RSA

OID	Potpis	Hash
id-TA-ECDSA-SHA-1	ECDSA	SHA-1
id-TA-ECDSA-SHA-224	ECDSA	SHA-224
id-TA-ECDSA-SHA-256	ECDSA	SHA-256
id-TA-ECDSA-SHA-384	ECDSA	SHA-384
id-TA-ECDSA-SHA-512	ECDSA	SHA-512

Tabela 15: Identifikatori objekta za autentifikaciju terminala sa ECDSA

A.6.4.1. Algoritam potpisa

ECDSA sa prostim formatom potpisa [3] kao što je definisano u tabeli 15 ĆE se koristiti.

A.6.4.2. Format javnog ključa

TLV format [15] kao što je opisan u prilogu D.3.3 ĆE se koristiti.

- Identifikator objekta ĆE se uzeti iz tabele 15.
- Dužina krive u bitima ĆE iznositi 160, 192, 224, 256, 320, 384 or 512.
- Parametri domena ĆE biti u skladu [3].

A.6.5. Autentifikovani pomoćni podaci za autentifikaciju terminala verzija 2

Korištenje pomoćnih podataka u autentifikaciji terminala je USLOVLJENO. MORA biti korišteno ako dalje operacije koje izvršava terminal zahtijevaju autentifikovane pomoćne podatke (detalji se mogu pronaći u sljedećim odjeljcima):

- za starosnu verifikaciju, terminal MORA koristiti potreban datum rođenja.
- za verifikaciju važenja dokumenta, terminal MORA koristiti trenutni datum.
- za verifikaciju identifikacionog broja opštine, terminal MORA koristiti (dijelove) identifikacionog broja.

Autentifikovani pomoćni podaci MORAJU biti strukturisani kao što je definisano u tabeli 16:

- autentifikacija objekta podataka koja sadrži sekvencu diskrecionih obrazaca podataka.
- svaki diskrecioni obrazac podataka sadrži identifikator objekta i objekat diskrecionih podataka. Sadržaj objekta diskrecionih podataka je definisan identifikatorom objekta.

Tek nakon uspješne autentifikacije terminala MRTD čip ĆE interpretirati i napraviti dostupnim podatke koji su sadržani u objektu diskrecionih podataka za dalje operacije.

Napomena: ukoliko autentifikacija objekta podataka sadrži više od jednog obrasca diskrecionog podatka sa istim identifikatorom objekta, podaci sa posljednjeg obrasca diskrecionih podataka ĆE biti dostupne za dalje operacije.

A.6.5.1. Identifikator objekta

Sljedeći identifikator objekta ĆE se koristiti za identifikaciju autentifikovanih pomoćnih podataka:

```
id-AuxiliaryData OBJECT IDENTIFIER ::= {
     bsi-de applications(3) mrtd(1) 4
}
```

A.6.5.2. Starosna verifikacija

Sljedeći identifikator objekta ĆE se koristiti za starosnu verifikaciju:

```
id-DateOfBirth OBJECT IDENTIFIER ::= {id-AuxiliaryData 1}
```

Objekat diskrecionih podataka ĆE sadržavati datum rođenja kodiran kao `Date` (vidi dio 2) koji terminal *zahtijeva*. MRTD čip ĆE uporediti sačuvane datume rođenja sa traženim datumom rođenja. Starosna verifikacija je uspješna ako sačuvani datum rođenja nije nakon traženog datumom rođenja

Objekat podataka
Autentifikacija
Obrazac diskrecionih podataka
Identifikator objekta
Diskrecioni podaci
Obrazac diskrecionih podataka
Identifikator objekta
Diskrecioni podaci
...

Tabela 16: Autentifikovani pomoćni podaci

A.6.5.3. Verifikacija važenja dokumenta

Sljedeći identifikator objekta ĆE se koristiti za verifikaciju važenja dokumenta:

```
id-DateOfExpiry OBJECT IDENTIFIER ::= {id-AuxiliaryData 2}
```

Objekat diskrecionih podataka ĆE sadržavati trenutni datum terminala kodiran kao Date (vidi dio 2). MRTD čip će uporediti sačuvane datume roka važenja i trenutni datum. Verifikacija važenja dokumenta je uspješna ako sačuvani datum roka važenja nije prije datog trenutnog datuma.

A.6.5.4. Verifikacija identifikacionog broja opštine

Sljedeći identifikator objekta ĆE se koristiti za verifikaciju identifikacionog broja opštine:

```
id-CommunityID OBJECT IDENTIFIER ::= {id-AuxiliaryData 3}
```

Objekat diskrecionih podataka ĆE sadržavati (dijelove) identifikacionog broja opštine kodirane kao `Octet•String` (vidi dio 2.). MRTD čip ĆE uporediti najljevije oktete sačuvanog identifikacionog broja opštine i preneseni (dio) traženi identifikacioni broj opštine. Verifikacija identifikacionog broja opštine je uspješna ako su najljeviji okteti sačuvanog identifikacionog broja opštine identični prenesenim podacima.

B. ISO 7816 Mapiranje (Normativ)

U ovom prilogu protokoli za PACE, autentifikaciju čipa i autentifikaciju terminala su mapirani prema ISO 7816 APDUs (jedinice podataka aplikativnog protokola).

B.1. PACE

Sljedeći niz komandi ĆE se koristiti za implementaciju PACE. Sigurna razmjena poruka je USLOVLJENA. MORA se koristiti za drugo izvršenje PACE ako je protokol izvršen dva puta:

1. MSE:Set AT
2. General Authenticate

Objekti specifičnih podataka protokola ĆE biti razmjenjeni u lancu General Authenticate komandi što je prikazano u nastavku:

Korak	Opis	Podaci komandi u		Podaci odgovora u protokolu	
1.	Kodirani nonce	-	odsutan	0x80	Kodirani nonce
2.	Mapiranje nonce	0x81	Mapiranje	0x82	Mapiranje
3.	Izvršavanje dogovora ključeva	0x83	Privremeni javni ključ	0x84	Privremeni javni ključ
4.	Zajednička autentifikacija	0x85	Token za autentifikaciju	0x86 0x87	Token za autentifikaciju Referenca certifikacionog tijela (USLOVLJENO)

Referenca(e) certifikacionog tijela su ZAHTJEVANE ako se koristi PACE sa obrascom autorizacije nosioca certifikata, tj. ako terminal za autentifikaciju verzija 2 slijedi PACE. U tom slučaju, objekat podataka 0x87 ĆE sadržavati najnovije reference certifikacijskog tijela u odnosu na tip terminala naznačen u obrascu autorizacije nosioca certifikata. Objekat podataka 0x88 MOŽE sadržavati prethodne reference certifikacijskog tijela.

Napomena: Parametri domena za PACE koje čip podržava su dostupni u EF.CardAccess (vidi prilog A.1.2.). Ako je podržano više od jednog seta parametara domena, terminal MORA odabrati parametre domena koje će se koristiti u okviru MSE:Set AT.

B.1.1. Kodirni nonce broj

Kodirani broj (vidi prilog A.3.3) ĆE biti kodiran kao oktetni niz.

B.1.2. Mapiranje podataka

Izmjenjeni podatak je specifičan za korišteno mapiranje.

B.1.2.1. Generičko mapiranje

Privremeni javni ključevi (vidi prilog A.2.2 i prilog D.3.4) ĆE biti kodirani kao tačke eliptičke krive (ECDH) i nepotpisanog cijelog broja (DH).

B.1.2.2. Integrisano mapiranje

Integrisano mapiranje je definisano sa ICAO [10].

B.1.3. Token za autentifikaciju

Token za autentifikaciju (vidi prilog A.2.4) ĆE biti kodiran kao oktetni niz.

B.1.4. Referenca certifikacijskog tijela

MRTD čip ĆE vratiti reference certifikacijskog tijela *odgovarajućih* CVCA javnih ključeva koji su sačuvani na MRTD čipu:

- reference MORAJU biti dinamiči izabrane da odgovaraju tipu terminala koji PACE znači.
- najviše dva objekta podataka referenci certifikacijskog tijela ĆE biti vraćena.
- najnovije reference certifikacijskog tijela ĆE biti sadržane u objektu podataka 0x87.

B.2. Autentifikacija čipa

Sljedeće komanda ĆE se koristiti pri sigurnoj razmjeni poruka za implementaciju autentifikaciju čipa u verziji 1 sa 3DES sigurnom razmjenom poruka:

1. MSE:Set KAT

Napomena: MSE:Set KAT se NE SMIJE koristiti za druge algoritme osimid-CA-DH-3DES-CBC- CBC i id-CA-ECDH-3DES-CBC-CBC, tj. sigurna razmjena poruka je ograničena za 3DES.

Sljedeći niz komandi ĆE se koristiti za sigurnu razmjenu podataka

- implementiranje autentifikacije čipa u verziji 1 sa AES i
- implementiranje autentifikacije čipa u verziji 1

Pored toga, ovaj niz se MOŽE koristiti za implementaciju autentifikacije čipa u verziji 1 sa 3DES:

1. MSE:Set AT
2. General Authenticate

Objekti specifičnih podataka protokola ĆE se razmjenjivati sa General Authenticate komandom kako je prikazano u tabeli:

Korak	Opis	Podaci komandi u protokolu		Podaci odgovora u protokolu	
1.	Autentifikacija čipa	0x80	Privremeni javni ključ	0x81 0x82	Nonce broj Token za autentifikaciju

Napomena: Podrška podataka odgovora u protokolu je USLOVLJENA: MORA biti osigurana za verziju 2 ali NE SMIJE za verziju 1.

Napomena: Javni ključevi za autentifikaciju čipa koje čip podržava su dostupni u objektima sigurnosti (vidi prilog A.1.2.). Ako je podržano više od jednog javnog ključa, terminal MORA odabrati odgovarajući privatni ključ čipa koji će se koristiti u okviru MSE:Set AT.

B.2.1. Privremeni javni ključ

Privremeni javni ključevi (vidi prilog A.2.2 i D.3.4) ĆE biti kodirani kao eliptičke tačke krive (ECDH) ili nepotpisan cijeli broj (DH).

B.2.2. Nonce broj

Nonce broj ĆE biti kodiran kao oktetni niz dužine 8 okteta.

B.2.3. Token za autentifikaciju

Token za autentifikaciju (vidi prilog A.2.4) ĆE biti kodiran kao oktetni niz.

B.3. Autentifikacija terminala

Sljedeći niz komandi ĆE se koristiti pri sigurnoj razmjeni poruka za implementiranje autentifikacije terminala:

1. MSE:Set DST
2. PSO:Verify Certificate
3. MSE:Set AT
4. Get Challenge
5. External Authenticate

Koraci 1 i 2 se ponavljaju za svaki CV certifikat koji se treba verifikovati (CVCA povezani certifikati, DV certifikati, certifikati terminala).

Za autentifikaciju terminala u verziji 2, MRTD čip MORA dodatno podržavati korištenje Get Challenge prije koraka 1, tj. MRTD čip mora zadržati generisani izazov (challenge) nakon korištenja External Authenticate.

B.4. Ograničena identifikacija

Sljedeći niz komandi ĆE se koristiti pri sigurnoj razmjeni poruka za implementiranje ograničene identifikacije:

1. MSE:Set AT
2. General Authenticate

Objekti specifičnih podataka protokola ĆE se razmjenjivati sa General Authenticate komandom kako je prikazano u tabeli, a vezane komande se NE SMIJU koristiti. MORA se izvršiti najmanje jedan korak:

Korak	Opis	Podaci komandi u protokolu	Podaci odgovora u protokolu

1.	Ograničena identifikacija (USLOVLJENO)	0xA0	1st Javni ključ sektora	0x81	1st Specifični identifikator sektora
2.	Ograničena identifikacija (USLOVLJENO)	0xA2	2nd Javni ključ sektora	0x83	2nd Specifični identifikator sektora

Napomena: Privatni ključevi za ograničenu identifikaciju koje čip podržava su naznačeni u odgovarajućim objektima sigurnosti (vidi prilog A.1.2.). Ako se podržava više od jednog privatnog ključa, terminal MORA odabrati privatni ključ koji će se koristiti u okviru MSE:Set AT.

B.4.1. Javni ključ

Javni ključ sektora PK_{Sector} ĆE biti kodiran kao ojekat podataka javnog ključa bez taga 0x7F49 (tj. 0x7F49 je zamjenjen sa 0xA0/0xA2,svaki posebno) (vidi prilog D.3), parametri domena MORAJU biti uključeni.

B.4.2. Sektorski specifičan identifikator

Sektorski specifičan identifikator I_{ID}^{Sector}ĆE biti kodiran kao oktetni niz.

B.5. Verifikacija pomoćnih podataka

Sljedeća komanda ĆE se koristiti pri sigurnoj razmjeni poruka za implementaciju funkcije verifikovanja:

1. Verify

Sljedeći autentifikovani pomoćni podaci se MORAJU poslati MRTD čipu kao dio autentifikacije terminala:

- za starosnu verifikaciju terminal MORA poslati traženi datum rođenja.
- za verifikaciju važenja dokumenta terminal MORA poslati trenutni datum
- za verifikaciju identifikacionog broja opštine terminal MORA poslati (dio) identifikacionog broja.

B.6. Upravljanje PIN-om

B.6.1. Deblokiranje ili promjena PIN-a

Sljedeća komanda ĆE se koristiti pri sigurnoj razmjeni poruka za implementaciju deblokiranje i/ili promjenu PIN-a:

1. Reset Retry Counter

- Za podešavanje novog PIN-a i resetovanja brojača ponavljanja terminal ĆE koristiti Reset Retry Counter sa novim podacima PIN-a..
- Za resetovanje brojača ponavljanja terminal ĆE koristiti Reset Retry Counter bez podataka.

Korišćenje komande ĆE biti ograničeno autorizovanim terminalima: Prije korištenja ove komande, terminal se mora autentifikovati kao terminal za autentifikaciju sa važećom autorizacijom za upravljanje PIN-om ili korištenjem PACE sa PUK/PIN.

B.6.2. Aktiviranje i deaktiviranje PIN-a

Sljedeća komanda ĆE se koristiti pri sigurnoj razmjeni poruka za aktiviranje PIN-a:

1. Activate

Sljedeća komanda ĆE se koristiti pri sigurnoj razmjeni poruka za deaktiviranje PIN-a:

1. Deactivate

Korištenje ove komande je ograničeno autorizovanim terminalima. Prije korištenja ove komande, terminal se mora autentifikovati kao terminal za autentifikaciju sa važećom autorizacijom za upravljanje PIN-om

B.7. Aplikacija ePotpis

Komande za instaliranje, ažuriranje i korištenje aplikacije ePotpis nisu obuhvaćene ovom specifikacijom.

B.8. Grupe za očitavanje podataka

APDU za odabir i očitavanje EAC zaštićenih grupa podataka koje je već definisano sa ICAO [8], [9] ĆE se koristiti (tj. Select File ili Read Binary). U skladu sa ICAO specifikacijama, svaki neautorizovan pristup EAC zaštićenim grupama podataka ĆE biti odbijen i MRTD čip MORA odgovoriti sa statusom u bitima 0x6982 (“Sigurnosni status nije zadovoljen”).

B.9. Proširenje

U zavisnosti od veličine kriptografskih objekata (npr. javni ključevi, potpisi), MORAJU se koristiti APDU sa proširenim poljima za slanje ovih podataka MRTD čipu. Detaljnije o proširenju vidi[13].

B.9.1. MRTD čipovi

Podrška proširenja za MRTD čipove je USLOVLJENA. Ako su kriptografski algoritmi i veličine ključeva odabrani od države koja vrši izdavanje zahtijevaju korištenje proširenja, MRTD čipovi ĆE podržati ta proširenja. Ako MRTD čip podržava proširenje, to MORA biti naznačeno u ATR/ATS ili u EF.ATR/INFO kao što je definisano u[13].

B.9.2. Terminali

Podrška proširenja za terminale se ZAHTIJEVA. Terminal TREBA prije korištenja ove opcije ispitati da li je podrška za proširenje naznačena u ATR/ATS or in EF.ATR/INFO MRTD čipa. Terminal NE SMIJE koristiti proširenja za APDU osim komandi praćenja, osim ako su tačne ulazne i izlazne veličine memorija MRTD čipa explicitno naznačene u ATR/ATS ili u EF.ATR/INFO.

- PSO:Verify Certificate
- MSE:Set KAT
- General Authenticate
- External Authenticate

B.9.3. Greške

MRTD čip TREBA prijaviti greške naredbe sa proširenom dužinom kodom greške 0x6700.

B.10. Uvezivanje komandi

Uvezivanje komandi se koristi samo za komandu General Authenticate. Detaljnije o uvezivanju komandi pogledajte u [13].

B.10.1. MRTD čipovi

Za MRT čipove, uvezivanje komandi je ZAHTIJEVANO i podrška uvezivanja komandi MORA biti naznačena u starim bajtovima ATR/ATS ili u EF.ATR/INFO kao što je definisano u [13].

B.10.2. Terminali

Za terminale uvezivanje komandi je ZAHTIJEVANO. Terminal prije uotrebe ove opcije TREBA ispitati da li MRTD čip podržava uvezivanje komandi.

B.10.3. Greške

Ako MRTD čip očekuje kraj uvezivanja, ali prima komandu koja nije označena kao zadnja komanda, MRTD čip ĆE naznačiti da zadnja komanda u lancu je očekivana sa statusom u bajtima0x6883.

B.11. APDU specifikacije

U nastavku su opisane APDU korištene za implementaciju protokola. MRTD čip ĆE implementirati APDU kao što je opisano ali MOŽE odstupiti od opisa ako su APDU korištene u drugim kontekstima.

Izostavljen CLA bajt ĆE biti podešen za označavanje sigurne razmjene poruka sa autentifikovanim zaglavljem, uvezivanjem komandi i specifičnim kodiranjem aplikacija kao što je zahtijevano protokolima (vidi prilog E.1).

B.11.1. MSE:Set AT

Komanda MSE:Set AT se koristi za odabir i iniciranje sljedećih protokola: PACE, autentifikacija čipa, autentifikacija terminala i ograničena identifikacija.

Komanda		
INS	0x22	Upravljanje sigurnosnim okruženjem
P1/P2	0xC1A4	PACE: Uspostaviti autentikacioni obrazac za uzajamnu autentikaciju.
	0x41A4	Autentikacija čipa /ograničena identifikacija: Postaviti autentikacioni obrazac za internu autentikaciju.

Podatak	0x80	Reference za kriptografski mehanizam Odabrati identifikator objekta protokola (samo vrijednost, Tag 0x06 je izostavljen). Ovaj objekat podataka ZAHTIJEVA se za sve protokole, osim za autentikaciju terminala u verziji 1.	USLOVLJENO
	0x83	Reference za javni/tajni ključ Ovaj objekat podataka ZAHTIJEVA se za sljedeće protokole: • Za PACE kako bi ukazao na lozinku koja će se koristiti: 0x01: MRZ 0x02: CAN 0x03: PIN 0x04: PUK • Za autentikaciju terminala kako bi se odabrao javni ključ terminala putem njegovog kodiranog naziva u skladu sa ISO 8859-1.	USLOVLJENO
	0x84	Reference za privatni ključ/reference za izračunavanje sesijskog ključa Ovaj objekat podataka ZAHTIJEVA se za sljedeće protokole (vidi Dodatak A.2): • Za PACE, da bi se ukazalo na identifikator parametara domena koji će se koristiti ukoliko su parametri domena dvosmisleni, odnosno, postoji više od jednog skupa parametara domena koji su dostupni za PACE. • Za autentikaciju čipa, da bi se ukazalo na identifikator privatnog ključa koji će se koristiti ako je privatni ključ dvosmislen, odnosno postoji više od	USLOVLJENO

	0x67	Pomoćni podaci čija se autentikacija izvršava	USLOVLJENO
	0x91	Ovaj objekat podataka ZAHTIJEVA se za autentikaciju terminala (verzija 2) ukoliko se koristi verifikacija starosti, važnosti dokumenta ili identifikacionog broja opštine) Privremeni javni ključ Ovaj objekat podataka ZAHTIJEVA se za autentikaciju terminala ukoliko je privremeni javni ključ $\widetilde{PK_{PCD}}$ nepoznat ili dvosmislen za čip MRTD-a kada se izvršava autentikacija terminala (odnosno, verzija 2). U ovom slučaju kompresovani privremeni javni ključ terminala **Comp**($\widetilde{PK_{PCD}}$) MORA se poslati čipu MRTD-a. Obrazac za autorizaciju nosioca sertifikata	USLOVLJENO
Odgovor			
Podata	–	Odsustvo	
Status bajtova	0x9000	Normalna operacija Protokol je selektovan i inicijalizovan.	
	0x6A80	Netačni parametri u poljima u kojima se ispisuju komande • Algoritmi koji nisu podržani ili čija je inicijalizacija neuspješna. • Vrsta terminala na koju obrazac za autorizaciju nosioca certifikata ukazuje nije ovlaštena za korištenje referentne lozinke (PACE).	
	0x6A88	Referentni podaci nisu pronađeni Referentni podaci (odnosno, lozinka, privatni ključ, javni ključ, parametri domena) nisu dostupni.	
	0x63CX	Upozorenje Odabrana je lozinka. X označava broj preostalih pokušaja verifikacije, ako nisu jednaki inicijalnoj vrijednosti: X=1: Lozinka je obustavljena. Lozinka se MORA ponoviti. X=0: Lozinka je blokirana. Lozinka se mora deblokirati.	

Napomena:

- Neki operativni sistemi prihvataju odabir nedostupnog javnog ključa i vraćaju informaciju o grešci samo kada se javni ključ koristi za odabranu svrhu.
- Ponavljanje i deblokiranje lozinke zahtijeva eksplicitno uspostavljanje CAN-a ili PUK-a korištenjem MSE:Set AT.

B.11.2. General Authenticate

Komanda General Authenticate koristi se za izvršavanje sljedećih protokola: PACE-a, autentikacije čipa i ograničene identifikacije.

Komanda			
INS	0x86	General Authenticate	
P1/P2	0x0000	Ključevi i protokol su indirektno poznati.	
Podatak	0x7C	Dinamička autentikacija podataka Objekti podataka specifični za protokol	ZAHTIJEVA SE
Odgovor			
Podatak	0x7C	Dinamička autentikacija podataka Objekti podataka specifični za protokol	ZAHTIJEVA SE
Status Bytes	0x9000	Normalna operacija Protokol (korak) je bio uspješan.	
	0x6300	Neuspješna autentikacija Protokol (korak) je bio neuspješan.	
	0x63C X	Neuspješna autentikacija Protokol (korak) je bio neuspješan. X označava broj preostalih pokušaja verifikacije: X=1: Lozinka je obustavljena. Lozinka se MORA ponoviti. X=0: Lozinka je blokirana. Lozinka se MORA deblokirati.	
	0x6982	Sigurnosni status nije zadovoljen Terminal nije ovlašten da izvršava protokol (npr. lozinka je blokirana, deaktivirana ili suspendovana). Blokiran autentikacioni metod Lozinka je blokirana. Referentni podaci se ne mogu koristiti Lozinka je deaktivirana.	

Napomena: Čip MRTD-a MOŽE ukazati na blokiranu, deaktiviranu ili suspendovanu lozinku odgovarajući sa statusnim bajtom 0x6982, umjesto statusnih bajtova 0x6983, 0x6984, ili 0x6985, datim redoslijedom.

B.11.3. MSE:Set KAT

Komanda MSE:Set KAT koristi se za verziju 1, autentikacije čipa sa 3DES.

Komanda			
INS	0x22	Upravljanje sigurnosnim okruženjem	
P1/P2	0x41A6	Uspostaviti obrazac za izračunavanje slaganja ključeva.	
Podatak	0x91	Privremeni javni ključ Privremeni javni ključ $\widetilde{PK}_{PCD}$ (vidi Dodatak A.2) kodiran kao čitljiva vrijednost javnog ključa.	ZAHTIJEVA SE USLOVLJENO
	0x84	Reference privatnog ključa Ovaj objekat podatka ZAHTIJEVA se ukoliko je privatni ključ dvosmislen, odnosno, kada je više od jednog para ključeva na raspolaganju za autentikaciju čipa (vidi Dodatak A.1.1.2 i Dodatak A.4.1).	
Odgovor			
Podatak	–	Odsustvo	
Statusni bajtovi	0x9000	Normalna operacija Operacija usklađivanja ključeva izvršena je uspješno. Izvedeni su novisesijski ključevi.	
	0x6A80	Netačni parametri u poljima u kojima se ispisuju komande Validacija privremenog javnog ključa nije uspješna. Prethodno uspostavljeni sesijski ključevi ostaju važeći.	
	ostalo	Greška koja zavisi od operativnog sistema Prethodno uspostavljeni sesijski ključevi ostaju važeći.	

B.11.4. MSE:Set DST

Komanda MSE:Set DST koristi se za uspostavljanje verifikacije certifikata za autentikaciju terminala.

Komanda			
INS	0x22	Upravljanje sigurnosnim okruženjem	
P1/P2	0x81B6	Uspostavljanje obrasca za digitalni potpis za verifikaciju.	
Podatak	0x83	Reference javnog ključa Kodirani naziv javnog ključa koji treba uspostaviti	ZAHTIJEVA SE
Odgovor			
Podatak	–	Odsustvo	

Statusni bajtovi	0x9000 0x6A88 ostalo	Normalna operacija Odabran je ključ za određenu namjenu. Referentni podaci nisu pronađeni Odabir nije uspio jer javni ključ nije dostupan.

Napomena: Neki operativni sistemi prihvataju odabir nedostupnog javnog ključa i odgovaraju greškom samo ukoliko se javni ključ koristi za odabranu namjenu.

B.11.5. PSO:Verify Certificate

Komanda PSO:Verify Certificate koristi se za verifikaciju i unošenje certifikata za autentikaciju terminala.

Komanda			
INS	0x2A	Izvršiti sigurnosnu operaciju	
P1/P2	0x00BE	Verifikovati samoopisivi certifikat.	
Podatak	0x7F4E	Certifikaciono tijelo Certifikaciono tijelo koje treba verifikovati.	ZAHTIJEVA SE ZAHTIJEVA SE
Odgovor			
Podat	–	Odsustvo	
Statusni bajtovi	0x9000	Normalna operacija Validacija certifikata izvršena je uspješno i javni ključ je unesen. Greška koja zavisi od operativnog sistema	

B.11.6. Get Challenge

Komanda Get Challenge koristi se za izvršavanje autentikacije terminala.

Komanda			
INS	0x84	Get Challenge	
P1/P2	0x0000		
Podata	–	Odsustvo	
Le	0x08		ZAHTIJEVA SE
Odgovor			
Podata	r_{PICC}	8 nasumičnih bajtova.	
Statusni	0x9000	Normalna operacija	

B.11.7. External Authenticate

Komanda External Authenticate koristi se za izvršavanje autentikacije terminala.

Komanda			
INS	0x82	External Authenticate	
P1/P2	0x0000	Ključevi i algoritmi su indirektno poznati.	
Podata		Terminal generiše potpis.	ZAHTIJEVA SE
Odgovor			
Podata	–	Odsustvo	
Statusni bajtovi	0x9000	Normalna operacija Autentikacija obavljena uspješno. Pristup grupama podataka biće dodijeljen prema važećim autorizacijama odgovarajućeg verifikovanog certifikata.	
	0x6300	Upozorenje Verifikacija potpisa neuspješna. Sigurnosni status ne zadovoljava	
	0x6982	Autentikacija neuspješna jer trenutni nivo autentikacije terminala ne dozvoljava upotrebu autentikacije terminala (npr. autentikacija terminala je već izvršena, itd.).	
	0x6985 ostalo	Uslovi korištenja nisu zadovoljeni Vrsta terminala koju je odredio PACE ne poklapa se sa vrstom terminala koja se nalazi u lancu certifikata.	

B.11.8. Verify

Komanda Verify koristi se za verifikaciju pomoćnih podataka čija autentikacija se vrši, odnosno, izvršavanje verifikacije starosti, važnosti dokumenta ili verifikacije identifikacionog broja opštine.

Napomena: Zbog kodiranja koje je specifično za aplikacije, MORA se koristiti klasa instrukcije *proprietary class*, odnosno, CLA=0x8C.

Komanda			
INS	0x20	Verify	
P1/P2	0x8000	Verifikovati pomoćne podatke čija se autentikacija vrši.	
Podata		Verifikovati identifikator objekta pomoćnih podataka.	ZAHTIJEVA SE
Odgovor			
Podata	–	Odsustvo	

Statusni bajtovi	0x9000	Normalna operacija Verifikacija uspješna.
	0x6300	Verifikacija neuspješna Verifikacija neuspješna.
	0x6A88 0x6982	Referentni podaci nisu pronađeni Referentni podaci nisu pronađeni.

B.11.9. Reset Retry Counter

Komanda Reset Retry Counter koristi se za deblokiranje ili promjenu PIN-a.

Komanda			
INS	0x2C	Reset Retry Counter	
P1	0x02- 0x03	Vidi dolje	
P2		0x02: CAN 0x03: PIN	
Podatak		Ponovo uspostavljeni podaci karakteristični za kontekst, koji zavise od P1: P1=0x02: new PIN/CAN	ZAHTIJEVA SE
Odgovor			
Podata	–	Odsustvo	
Statusni bajtovi	0x9000 0x6982 ostalo	Normalna operacija Deblokiranje ili promjena PIN-a izvršeni uspješno. Sigurnosni status ne zadovoljava Terminal nije ovlašten da izvrši deblokiranje ili promjenu PIN-a.	

Napomena: Pošto je CAN lozinka koja se ne može blokirati, deblokiranje CAN-a nije neophodno. Međutim, čip MRTD-a MOŽE podržavati promjenu PIN-a.

B.11.10. Activate

Komanda Activate koristi se za podešavanje PIN-a u aktivno stanje.

Komanda		
INS	0x44	Activate
P1	0x10	Aktiviranje PIN-a preko parametra P2.

P2		0x03: PIN
Podata		Odsustvo
Odgovor		
Podata	–	Odsustvo
Status ni bajtovi	0x9000 0x6982 ostalo	Normalna operacija PIN podešen u aktivno stanje. Sigurnosnt status ne zadovoljava Terminal nije ovlašćen za promjenu statusa PIN-a.

B.11.11. Deactivate

Komanda Deactivate koristi se za podešavanje PIN-a u deaktivirano stanje.

Komanda		
INS	0x04	Deactivate
P1	0x10	Deaktiviranje PIN-a preko parametra P2.
P2		0x03: PIN
Podata		Odsustvo
Odgovor		
Podata	–	Odsustvo
Status ni bajtovi	0x9000 0x6982 ostalo	Normalna operacija PIN podešen u deaktivirano stanje. Sigurnosni status ne zadovoljava Terminal nije ovlašten za promjenu stanja PIN-a.

C. CV certifikati (normativno)

C.1. Profil certifikata

KORISTITI samoopisive certifikate koji se verifikuju putem kartice (CV certifikat) u skladu sa standardom ISO 7816 (vidi [13], [14], [15]) i profil certifikata naznačen u tabeli 17. Pojedinosti vezane za kodiranje objekata podataka koji se koriste u profilu certifikata možete pronaći u Dodatku D.2.

C.1.1. Identifikator profila certifikata

Identifikator profila certifikata ukazuje na verziju certifikata. Verzija 1, kao što je

naznačeno u tabeli 17, identifikuje se vrijednošću 0.

C.1.2. Reference certifikacionog tijela

Reference certifikacionog tijela koriste se za identifikaciju javnog ključa koji se koristi za verifikaciju potpisa certifikacionog tijela (CVCA ili DV). Reference certifikacionog tijela MORAJU biti iste kao reference nosioca certifikata u odgovarajućem certifikatu certifikacionog tijela (Link certifikat CVCA ili DV certifikat). Pojedinosti vezane za reference certifikacionog tijela možete pronaći u Dodatku A.6.1.

C.1.3. Javni ključ

Pojedinosti vezane za kodiranje javnog ključa možete pronaći u Dodatku D.3.

Objekat podatka	Cert
CV Certifikat	m
Certifikaciono tijelo	m
Identifikator profila certifikata	m
Reference certifikacionog tijela	m
Javni ključ	m
Reference nosioca certifikata	m
Obrazac autorizacije za nosioca certifikata	m
Dan stupanja na snagu certifikata	m
Dan prestanka važnosti certifikata	m
Ekstenzije certifikata	o
Potpis	m

Tabela 17: CV Profil certifikata

C.1.4. Reference nosioca certifikata

Reference nosioca certifikata koriste se za identifikaciju javnog ključa koji se nalazi na certifikatu. Pojedinosti koje se odnose na referencu nosioca certifikata možete pronaći u Dodatku A.6.1.

C.1.5. Obrazac autorizacije za nosioca certifikata

Rola i autorizacije nosioca certifikata KODIRA se u obrascu autorizacije za nosioca certifikata. Ovaj obrazac predstavlja niz koji se sastoji od sljedećih objekata podataka:

1. Identifikatora objekta koji određuje vrstu terminala i format obrasca.
2. Diskrecioniog objekta podataka koji kodira relativnu autorizaciju, odnosno rolu i autorizaciju nosioca certifikata u odnosu na certifikaciono tijelo.

Sadržaj i evaluacija obrasca autorizacije za nosioca certifikata opisani su u Dodatku C.4.

C.1.6. Dan stupanja na snagu/prestanka važnosti certifikata

Ukazuje se na period važnosti certifikata. Dan stupanja na snagu certifikata MORA biti dan generisanja certifikata.

C.1.7. Ekstenzije certifikata za autentikaciju terminala, verzija 2

Certifikati terminala za njegovu autentikaciju (vidi Dodatak C.4.2.) MOGU sadržati ekstenzije kako je definisano u Dodatku C.3.

C.1.8. Potpis

Potpis na certifikatu KREIRA se putem kodiranog dijela certifikata (odnosno, obuhvatiće tag i dužinu). Reference certifikacionog tijela IDENTIFIKUJE javni ključ koji se koristi za verifikaciju potpisa.

C.2. Certifikacioni zahtjevi

Certifikacioni zahtjevi su skraćeni CV certifikati koji mogu nositi dodatni potpis. TREBA koristiti profil certifikacionog zahtjeva naznačen u tabeli 18. Pojedinosti vezane za kodiranje objekata podataka koji se koriste u profilu certifikacionog zahtjeva možete pronaći u Dodatku D.2.

C.2.1. Identifikator profila certifikata

Verziju profila identifikuje identifikator profila certifikata.Verzija 1 identifikuje se vrijednošću 0 kako je dato u tabeli 18.

C.2.2. Reference certifikacionog tijela

Reference certifikacionog tijela TREBA koristiti za informisanje certifikacionog tijela o privatnom ključu koji aplikant **očekuje** da će se koristiti za potpisivanje certifikata. Ukoliko reference certifikacionog tijela koje su obuhvaćene zahtjevom odstupaju od referenci certifikacionog tijela sadržanog u izdatom certifikatu (odnosno, izdati certifikat je potpisan javnim ključem koji aplikant **ne očekuje**), odgovarajući certifikat certifikacionog tijela TREBA, takođe, dostaviti aplikantu kao odgovor.

Pojedinosti o referencama certifikacionog tijela možete pronaći u Dodatku A.6.1.

C.2.3. Javni ključ

Pojedinosti vezane za kodiranje javnih ključeva možete pronaći u Dodatku D.3.

Podatak objekta	Zaht.
Autentikacija	c
CV certifikat	m
Certifikaciono tijelo	m
Identifikator profila certifikata	m
Reference certifikacionog tijela	r
Javni ključ	m
Reference nosioca certifikata	m
Ekstenzije certifikata	o
Potpis	m
Reference certifikacionog tijela	c

Potpis	c

Tabela 18: CV profil certifikacionog zahtjeva

C.2.4. Reference nosioca certifikata

Referenca nosioca certifikata koristi se za identifikaciju javnog ključa koji se nalazi u zahtjevu i odgovarajućeg certifikata. Pojedinosti vezane za nosioca certifikata možete pronaći u Dodatku A.6.1.

C.2.5. Ekstenzije certifikata za autentikaciju terminala, verzija 2

Certifikacioni zahtjevi terminala za autentikaciju (vidi Dodatak C.4.2.) MOGU sadržati ekstenzije kao što je definisano u Dodatku C.3.

C.2.6. Potpis(-i)

Certifikacioni zahtjev može imati dva potpisa, *unutrašnji* i *vanjski*:

Unutrašnji potpis **(ZAHTJEVA SE)**

Certifikaciono tijelo je samopotpisivo, odnosno, POTREBNO je da se unutrašnji potpis može verifikovati javnim ključem koji se nalazi u certifikacionom zahtjevu. POTREBNO je da potpis bude kreiran putem kodiranog dijela certifikata (odnosno, da obuhvati tag i dužinu).

Vanjski potpis **(USLOVLJENO)**

- Potpis je OPCIONI ako subjekat aplicira za inicijalni certifikat. U tom slučaju zahtjev MOŽE dodatno potpisati drugi subjekat kojem prijemno certifikaciono tijelo to povjeri (npr. državno CVCA može izvršiti autentikaciju zahtjeva DV koji je poslat stranom CVCA).
- Potpis se ZAHTIJEVA ukoliko subjekat aplicira za dodatni certifikat. U tom slučaju, zahtjev MORA dodatno potpisati aplikant koristeći nedavno generisani par ključeva koji je prethodno registrovan kod prijemnog certifikacionog tijela.

Ukoliko se koristi vanjski potpis, KORISTI se objekat podataka za autentikaciju da bi se smjestili certifikat CV (zahtjev), reference certifikacionog tijela i dodatni potpis. Reference certifikacionog tijela IDENTIFIKUJU javni ključ koji se koristi za verifikaciju dodatnog potpisa. POTREBNO JE da potpis bude kreiran uvezivanjem kodiranog CV certifikata *i* kodirane reference certifikacionog tijela (odnosno, da obuhvati i tag i dužinu).

Podatak objekta
Ekstenzije certifikata
Diskrecioni obrazac za podatke
Identifikator objekta
Objekat podataka karakterističan za kontekst 1
...
Objekat podataka karakterističan za kontekst n
Diskrecioni obrazac za podatke

Identifikator objekta
Objekat podataka karakterističan za kontekst 1
...
Objekat podataka karakterističan za kontekst m
...

Tabela 19: Ekstenzije certifikata

C.3. Ekstenzije certifikata za autentikaciju terminala, verzija 2

Ekstenzija certifikata predstavlja niz obrazaca sa diskrecionim podacima, gdje svaki obrazac sa diskrecionim podacima TREBA sadržati niz sljedećih objekata podataka prikazanih i u tabeli 19:

1. Identifikator objekta koji određuje sadržaj i format ekstenzije.
2. Jedan ili više objekata podataka karakterističnih za kontekst koji sadrže kodiranu ekstenziju.

Sljedeći identifikator objekta baze koristi se za identifikovanje ekstenzija certifikata definisanih u nastavku:

```
id-extensions OBJECT IDENTIFIER ::= {bsi-de applictions(3) mrtd(1) 3}
```

Napomena: Procedura za validaciju certifikata opisana u Dijelu 2.5.1 ne uzima u obzir ekstenzije certifikata. Zbog toga, ekstenzije ne predstavljaju kritične osobine i čip MRTD-a NE SMIJE odbiti certifikat zbog nepoznatih ekstenzija. Nepoznate ekstenzije i ekstenzije koje nisu značajne za čip MRTD-a ne treba importovati.

C.3.1. Opis certifikata

Za ovu ekstenziju TREBA koristiti sljedeći identifikator objekta:

```
id-description OBJECT IDENTIFIER ::= {id-extensions 1}
```

Sljedeći objekat podataka karakterističan za kontekst koristi se za kodiranje opisa certifikata:

- 0x80: Heš CertificateDescription

```
CertificateDescription ::= SEQUENCE {
     descriptionType     OBJECT IDENTIFIER,
     issuerName          [1] UTF8String,
     issuerURL           [2] PrintableString OPTIONAL,
     subjectName         [3] UTF8String,
     subjectURL          [4] PrintableString OPTIONAL,
     termsOfUsage        [5] ANY DEFINED BY descriptionType,
     redirectURL         [6] PrintableString OPTIONAL,
     commCertificates    [7] SET OF OCTET STRING OPTIONAL
}
```

Skup `commCertificates` MOŽE sadržati heš vrijednosti prihvatljivih certifikata X.509 udaljenog terminal. Heš funkciju koja se koristi DEFINIŠE heš funkcija kojom se potpisuju certifikati CV. Input za heš funkciju je odgovarajući certifikat DER-kodiran X.509 koji obuhvata i tag i dužinu. Heš funkciju koja se koristi za generisanje sadržaja ekstenzije DEFINIŠE heš funkcija za potpisivanje certifikata.

Napomena: Lokalni terminal koristi opis certifikata kao dio interakcije korisnika za onlajn autentikaciju udaljenog terminala (vidi Dio 2), a čip MRTD-a ga može ignorisati.

C.3.1.1. Format prostog teksta

Sljedeći identifikator objekta KORISTI se za identifikovanje uslova korištenja u formatu prostog teksta:

```
id-plainFormat OBJECT IDENTIFIER ::= {id-description 1}
PlainTermsOfUsage ::= UTF8String
```

2.8.1.1 C.3.1.2 Format HTML

Sljedeći identifikator objekta KORISTI se za identifikovanje uslova korištenja u formatu HTML:

```
id-htmlFormat OBJECT IDENTIFIER ::= {id-description 2}
HtmlTermsOfUsage ::= IA5String
```

2.8.1.2 C.3.1.3. Format PDF

Sljedeći identifikator objekta KORISTI se za identifikovanje uslova korištenja u formatu PDF [11]:

```
id-pdfFormat OBJECT IDENTIFIER ::= {id-description 3}
PdfTermsOfUsage ::= OCTET STRING
```

C.3.2. Sektor terminala

Sljedeći identifikator objekta KORISTI se za ovu ekstenziju:

```
id-sector OBJECT IDENTIFIER ::= {id-extensions 2}
```

Sljedeći objekti podataka karakteristični za kontekst koriste se za kodiranje sektora terminala:

- 0x80: Heš javnog ključa objekta podataka sektora 1 (vidi Dodatak D.3).
- 0x81: Heš javnog ključa objekta podataka sektora 2 (vidi Dodatak D.3).

Heš funkciju koja se koristi definisaće heš funkcija za potpisivanje certifikiata. Sam javni ključ nije obuhvaćen certifikatom i terminal ga MORA osigurati kao dio ograničene identifikacije.

Čip MRTD-a izračunava heš putem primljenog javnog ključa i poredi ga sa primljenim hešom.

Napomena: Tagovanje karakteristično za kontekst koristi se za javni ključ prilikom ograničene identifikacije (vidi Dodatak B.4.1). Čip MRTD-a MORA zamijeniti tagovanje karakteristično za kontekst 0xA0 tagovanjem karakterističnim za aplikaciju 0x7F49 prije izračunavanja heš vrijednosti.

C.4. Role i nivoi autorizacija

Sljedeći identifikator objekta KORISTI se za identifikaciju rola i nivoa autorizacije različitih vrsta terminala:

```
id-roles OBJECT IDENTIFIER ::= {bsi-de applications(3) mrtd(1) 2}
```

Napomena: Pristupna prava mogu biti proglašena *pravima rezervisanim za buduću*

upotrebu (RFU). Takva pristupna prava mogu biti dodijeljena u narednim verzijama ovog Tehničkog uputstva. Kao posljedica toga, čip MRTD-a koji je već izdat mora unijeti certifikate sa neočekivanom autorizacijom nosioca certifikata. Zahvaljujući proračunu pristupnih prava, opisanom u Dijelu 2.6, važeća autorizacija će uvijek ograničavati pristupna prava koja su čipu MRTD-a poznata u vrijeme personalizacije.

C.4.1. Inspekcijski sistemi

Sljedeći identifikator objekta KORISTI se za inspekcijske sisteme:

```
id-IS OBJECT IDENTIFIER ::= {id-roles 1}
```

Relativna autorizacija nosioca certifikata kodirana je jednim bajtom koji se tumači kao binarna raster mapa, što je predstavljeno u tabeli 20. Za više pojedinosti, ova bitmapa sadrži role i pristupna prava. Oboje zavise od autorizacija svih prethodnih certifikata u lancu.

7 6	5 4 3 2 1 0	Opis
x x	- - -	Rola
1 1	- - -	CVCA
1 0	- - -	DV (zvanični domaći)
0 1	- - -	DV (zvanični strani)
0 0	- - -	Inspekcijski sistemi
-	x x x x x x	Pristupna prava
-	x x x x - -	RFU
-	- - - - 1 -	Očitati pristup aplikaciji za elektronski pasoš: DG 4 (zjenica oka)
-	- - - - - 1	Očitati pristup aplikaciji za elektronski pasoš: DG 3 (otisak prsta)

Tabela 20: Autorizacije inspekcijskih sistema

Ovlašteni inspekcijski sistem uvijek će OČITATI pristup manje osjetljivim grupama podataka (npr. DG1, DG2, DG14) u aplikaciji za elektronski pasoš. Taj sistem bi, takođe, TREBAO očitati pristup svim grupama podataka aplikacije za elektronske lične karte.

C.4.2. Terminali za autentikaciju

Sljedeći identifikator objekta KORISTI se za terminale za autentikaciju:

```
id-AT OBJECT IDENTIFIER ::= {id-roles 2}
```

Relativne autorizacije nosioca certifikata kodirane su s pet bajtova koji se tumače kao binarna raster mapa kao što je prikazano u tabeli 21. Za više pojedinosti, ova bitmapa sadrži role i pristupna prava. Oboje zavise od autorizacija svih prethodnih certifikata u lancu.

Ovlašteni terminal za autentikaciju uvijek IMA pristup sljedećim funkcijama:

39 38	37 … 33	32 ... 29	28 ... 8	7 6 5 4 3 2 1 0	Opis
x x	- - -	- - -	- - -	- - - - - - - -	Rola
1 1	- - -	- - -	- - -	- - - - - - - -	CVCA
1 0	- - -	- - -	- - -	- - - - - - - -	DV (zvanični domaći)

0 1	- - -	- - -	- - -	- - - - - - - -	DV(nezvanični-zvanični/strani)
0 0	- - -	- - -	- - -	- - - - - - - -	Terminal za autentikaciju
	x x x	- - -	- - -	- - - - - - - -	Pristup pisanju (eLK)
- -	1 - -	- - -	- - -	- - - - - - - -	DG 17
- -	- ... -	- - -	- - -	- - - - - - - -	…
- -	- - 1	- - -	- - -	- - - - - - - -	DG 21
- -	- - -	x x x	- - -	- - - - - - - -	RFU: Pristup čitanju/pisanju
- -	- - -	- - -	x x x	- - - - - - - -	Pristup čitanju (eLK)
- -	- - -	- - -	1 - -	- - - - - - - -	DG 21
- -	- - -	- - -	- ... -	- - - - - - - -	…
- -	- - -	- - -	- - 1	- - - - - - - -	DG 1
	- - -	- - -	- - -	x x x x x x x x	Posebne funkcije
- -	- - -	- - -	- - -	1 - - - - - - -	Instalirati kvalifikovan certifikat
- -	- - -	- - -	- - -	- 1 - - - - - -	Instalirati certifikat
- -	- - -	- - -	- - -	- - 1 - - - - -	Upravljanje PIN-om
- -	- - -	- - -	- - -	- - - 1 - - - -	Dozvoljeni CAN
- -	- - -	- - -	- - -	- - - - 1 - - -	Privilegovani terminal
- -	- - -	- - -	- - -	- - - - - 1 - -	Ograničena identifikacija
- -	- - -	- - -	- - -	- - - - - - 1 -	Identifikacioni br. opštine
- -	- - -	- - -	- - -	- - - - - - - 1	Potvrda starosti

Tabela 21: Autorizacija terminala za autentikaciju

- Ograničena identifikacija osim ukoliko čip MRTD-a ne zahtijeva od terminala da bude ovlašten za korištenje funkcije (postavka `authorizedOnly` je aktivna, vidi Dodatak A.1.1.4)
- Verifikacija validnosti dokumenta

C.4.3. Terminali za potpisivanje

Sljedeći identifikator objekta KORISTI se za terminale za potpisivanje:

```
id-ST OBJECT IDENTIFIER ::= {id-roles 3}
```

Relativna autorizacija nosioca certifikata kodirana je jednim bajtom koji se tumači kao binarna raster mapa kao što je prikazano u tabeli 22. Za više pojedinosti, ova bitmapa sadrži role i pristupna prava. Oboje zavise od autorizacija svih prethodnih certifikata u lancu.

C.5. Certifikaciona politika

PREPORUČUJE SE da svako CVCA tijelo i svaki DV objavi certifikacionu politiku i/ili izjavu o certifikacionoj praksi.

C.5.1. Procedure

Certifikacionom politikom TREBA odrediti sljedeće procedure:

- Identifikacija subjekta, autentikacija i registracija;
- Apliciranje, izdavanje i distribucija certifikata;
- Oporavak od kvara ili ugrožavanja privatnosti,
- Revizija.

7 6	5 4 3 2 1 0	Opis
x x	- - - - - -	Role
1 1	- - - - - -	CVCA
1 0	- - - - - -	DV (Akreditaciono tijelo)
0 1	- - - - - -	DV (Provajder usluga certifikovanja)
0 0	- - - - - -	Terminal za potpisivanje
- -	x x x x x x	Pristupna prava (elektronski potpis)
- -	x x x x - -	RFU
- -	- - - - 1 -	Generisati kvalifikovan elektronski potpis
- -	- - - - - 1	Generisati elektronski potpis

Tabela 22: Autorizacija terminala za potpisivanje

C.5.2. Ograničenja korištenja

Certifikaciona politika TREBA odrediti ograničenja na uređajima koji se koriste za pohranjivanje/obradu odgovarajućih privatnih ključeva i ostalih osjetljivih (ličnih) podataka:

- Fizička i operativna sigurnost;
- Mehanizmi kontrole pristupa;
- Evaluacija i certifikacija (npr. zajednički kriteriji za zaštitu profila);
- Zaštita podataka.

D. DER kodiranje (normativ)

Istaknuta pravila kodiranja (DER) prema X.690 [17] KORISTE SE za kodiranje obje ASN. 1 strukture podataka i podataka objekta (karakteristične za aplikacije). Kodiranje rezultira strukturom tag-dužina-vrijednost (TLV), kao što slijedi:

Tag: oznaka kodirana u jednom ili dva okteta i ukazuje na sadržaj.

Dužina: Dužina kodirana kao nepotpisan cijeli broj (integer) u jednom, dva ili tri okteta rezultiraće maksimalnom dužinom od 65 535 okteta. KORISTI se minimalan broj okteta.

Vrijednost: Vrijednost je kodirana u nula ili više okteta.

D.1. ASN.1

Kodiranje struktura podataka definisano u ASN.1 sintaksi opisano je u X.690 [17].

D.2. Objekti podataka

Tabela 23 daje pregled tagova, dužina i vrijednosti objekta podataka koji se koriste u ovoj specifikaciji.

Napomena: Tag 0x7F4C još uvijek nije definisan u ISO/IEC 7816. Zahtijeva se alokacija.

Naziv	Tag	Dužina	Vrijednost	Komentar
Identifikator objekta	0x06	V	Identifikator objekta	–
Reference certifikacionog tijela	0x42	16V	Znakovni niz	Identifikuje javni ključ certifikacionog tijela koje je izdalo certifikat.
Diskrecioni podatak	0x53	V	Oktetni niz	Sadrži proizvoljne podatke.
Referenca nosioca certifikata	0x5F20	16V	Znakovni niz	Povezuje javni ključ koji se nalazi na certifikatu sa identifikatorom.
Dan prestanka važnosti certifikata	0x5F24	6F	Datum	Datum nakon kojeg certifikat prestaje važiti.
Dan stupanja na snagu certifikata	0x5F25	6F	Datum	Datum generisanja certifikata.
Identifikator profila certifikata	0x5F29	1F	Nepotpisan cijeli broj	Verzija certifikata i format zahtjeva za certifikatom.
Potpis	0x5F37	V	Oktetni niz	Digitalni potpis koji je izrađen preko asimetričnog kriptografskog algoritma.
Ekstenzije certifikata	0x65	V	Niz	Smješta ekstenzije certifikata.
Autentikacija	0x67	V	Niz	Sadrži objekte podataka koji se odnose na autentikaciju.
Obrazac diskrecionog podatka	0x73	V	Niz	Smješta proizvoljne objekte podataka.

CV certifikata	0x7F21	V	Niz	Smješta sam certifikat i njegov potpis.
Javni ključ	0x7F49	V	Niz	Smješta vrijednosti javnog ključa i parametara domena.
Obrazac za autorizaciju nosioca certifikata	0x7F4C	V	Niz	Kodira role nosioca certifikata (odnosno, CVCA, DV, terminala) i dodjeljuje pristupna prava za čitanje/pisanje.
Certifikat	0x7F4E	V	Niz	Smješta objekte podataka certifikata.
F: fiksna dužina (tačno određen broj okteta), V: Promjenljiva dužina do određenog broja okteta)				

Tabela 23: Pregled objekta podataka (sređenih prema tagovima)

D.2.1. Kodiranje vrijednosti

Osnovne vrste vrijednosti koje se koriste u ovoj specifikaciji su sljedeće: (nepotpisani) cijeli broj, tačke eliptične krive, datumi, znakovni nizovi, oktetni nizovi, identifikatori objekta i sekvence.

D.2.1.1. Nepotpisani cijeli brojevi

Svi cijeli brojevi koji se koriste u ovoj specifikaciji su nepotpisani cijeli brojevi. Nepotpisan cijeli broj KONVERTUJE se u oktetni niz putem binarne reprezentacije cijelog broja u formatu podataka u kojem je prvi dio najznačajniji (big-endian). KORISTI se minimalan broj okteta, odnosno NE SMIJU se koristiti vodeći okteti vrijednosti 0x00.

Napomena: Nasuprot tipu ASN.1, `INTEGER` je uvijek potpisan cijeli broj.

D.2.1.2. Tačke eliptične krive

Konverzija tačaka eliptične krive u oktetne tačke naznačena je u [3]. KORISTI SE nekompresovani format.

D.2.1.3. Datumi

Datum je kodiran sa 6 znakova $d_1|d_6$ u formatu GGMMDD korištenjem vremenske zone GMT. Konvertovan je u oktetni niz $o_1|o_6$ kodiranjem svakog znaka d_j u oktet o_j kao neupakovan binarno kodirani decimalni broj ($1 \leq j \leq 6$).

Godina GG kodirana je sa dva znaka i tumači se kao 20GG, odnosno, godina je data u rasponu od 2000 do 2099.

Šif.	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0																
1																
2	SP	!	"	#	$	%	&	’	(	)	*	+	,	-	.	/
3	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_

6	‘	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7	p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	
8																
9																
A	NB	¡	¢	£	¤	¥	¦	§	¨	©	ª	«	¬	SH	®	¯
B	□	±	²	³	´	µ	¶	·	¸	¹	º	»	¼	½	¾	¿
C	À	Á	Â	Ã	Ä	Å	Æ	Ç	È	É	Ê	Ë	Ì	Í	Î	Ï
D	Ð	Ñ	Ò	Ó	Ô	Õ	Ö	×	Ø	Ù	Ú	Û	Ü	Ý	Þ	ß
E	à	á	â	ã	Ä	å	æ	ç	è	é	ê	ë	ì	í	î	ï
F	ð	ñ	ò	ó	ô	õ	ö	÷	ø	ù	ú	û	ü	ý	þ	Ÿ
SP: Razmak, NBSP: Razmak bez prekida, SHY: Meka crtica																

Tabela 24: ISO/IEC 8859-1 Skup karaktera

D.2.1.4. Znakovni nizovi

Znakovni niz $c_1|c_n$ predstavlja spajanje n karaktera c_j pri čemu je $1 \leq j \leq n$. Potom se KONVERTUJE u oktetni niz $o_1|o_n$ pretvaranjem svakog znaka c_j u o_j korištenjem skupa karaktera iz ISO/IEC 8859-1. Skup karaktera možete pronaći u tabeli 24.

Šifre karaktera 0x00-0x1F i 0x7F-0x9F su nedodijeljene i NE SMIJU SE koristiti. Konverzija okteta u nedodijeljen znak REZULTIRAĆE greškom.

D.2.1.5. Oktetni nizovi

Oktetni niz $o_1|o_n$ predstavlja spajanje n okteta o_j pri čemu je $1 \leq j \leq n$. Svaki oktet o_j sastoji se od 8 bitova.

D.2.1.6. Identifikatori objekta

Identifikator $i_1.i_2.|.i_n$ kodiran je kao spisak n nepotpisanih cijelih brojeva i_j gdje je $1 \leq j \leq n$. Potom se KONVERTUJE u oktetni niz $o_1|o_{n-1}$ korišćenjem sljedeće procedure:

1. Prva dva cijela broja i_1 i i_2 upakovana su u jedan cijeli broj *i* koji se onda konvertuje u oktetni niz o_1. Vrijednost *i* računa se na sljedeći način:

$$i = i_1 \cdot 40 + i_2$$

2. Preostali cijeli brojevi i_j direktno se konvertuju u oktetne nizove o_{j-1} gdje je $3 \leq j \leq n$. Više pojedinosti o kodiranju možete pronaći u [17].

Napomena: Nepotpisani cijeli brojevi kodirani su kao oktetni nizovi korištenjem formata u kojem je prvi dio najvažniji (big-endian) kao što je opisano u Dodatku D.2.1.1, međutim, koriste se samo bitovi 1-7 svakog okteta. Bit 8 (krajnji bit) postavljen kao jedan koristi se da bi se označilo da taj oktet ne predstavlja posljednji oktet u lancu.

D.2.1.7. Sekvence

Sekvenca $D_1 \mid D_n$ predstavlja rang listu n objekata podataka D_j gdje je $1 \leq j \leq n$. Sekvenca se KONVERTUJE u povezan spisak oktetnih nizova $O_1 \mid O_n$ kodiranjem svakog objekta podatka D_j u oktetni niz O_j putem DER-a.

D.3. Objekat podataka javnog ključa

Objekat podataka javnog ključa sadrži sekvence identifikatora objekta i nekoliko objekata podataka karakterističnih za kontekst:

- Identifikator objekta je karakterističan za aplikaciju i odnosi se ne samo na format javnog ključa (odnosno, objekti podataka karakteristični za kontekst), već i na njegovu upotrebu.
- Objekte podataka karakteristične za kontekst definiše identifikator objekata, a sadrže vrijednosti javnog ključa i parametre domena.

Format objekata podataka javnog ključa koji se koristi u ovoj specifikaciji opisan je u nastavku.

D.3.1. Javni ključevi RSA

Objekti podataka sadržani u javnom ključu RSA prikazani su u tabeli 25. Redoslijed objekata podataka je fiksan.

Objekat podataka	Skraće	Ta	Vrsta	CV Certifikat
Identifikator objekta		0x06	Identifikator objekta	m
Složeni modul	n	0x81	Nepotpisan cijeli broj	m
Javni eksponent	e	0x82	Nepotpisan cijeli broj	m

Tabela 25: Javni ključ RSA

D.3.2. Javni ključevi Diffie Hellman

Objekti podataka koji se nalaze u javnom ključu DH prikazani su u tabeli 26. Redoslijed objekata podataka je fiksan.

Objekat podataka	Skrać.	Tag	Vrsta
Identifikator objekta		0x06	Identifikator objekta
Prosti moduli	p	0x81	Nepotpisan cijeli broj

Redoslijed podgrupa	q	0x82	Nepotpisan cijeli broj
Generator	g	0x83	Nepotpisan cijeli broj
Javna vrijednost	y	0x84	Nepotpisan cijeli broj

Tabela 26: Javni ključ DH

D.3.3. Javni ključevi eliptične krive

Objekti podataka sadržani u javnom ključu eliptične krive prikazani su u tabeli 27. Redoslijed objekata podataka je fiksan, USLOVLJENI parametri domena MORAJU biti ili svi prisutni, osim dodatnog faktora, ili svi odsutni, kako slijedi:

Objekat podataka	Skrać.	Tag	Vrsta	CV Certifikat
Identifikator objekta		0x06	Identifikator objekta	m
Prosti moduli	p	0x81	Nepotpisan cijeli broj	c
Prvi koeficijent	a	0x82	Nepotpisan cijeli broj	c
Drugi koeficijent	b	0x83	Nepotpisan cijeli broj	c
Tačka u bazi	G	0x84	Tačka eliptične krive	c
Redoslijed tačke u	r	0x85	Nepotpisan cijeli broj	c
Javna tačka	Y	0x86	Tačka eliptične krive	m
Dodatni faktor	f	0x87	Nepotpisan cijeli broj	c

Tabela 27: Javni ključevi eliptične krive

- CVCA link certifikati MOGU sadržati parametre domena.
- DV i certifikati terminala NE SMIJU sadržati parametre domena. Parametri domena DV i javni ključ terminala UZIMAJU se iz odgovarajućih javnih ključeva CVCA.
- Certifikacioni zahtjevi MORAJU sadržati parametre domena.

D.3.4. Privremeni javni ključevi

Format i parametri domena privremenih javnih ključeva već su poznati. Prema tome, samo osnovna vrijednost javnog ključa, odnosno, javna vrijednost *y* za javne ključeve Diffie-Hellman i javnu tačku *Y* za javne ključeve eliptične krive, koristi se za prenošenje privremenog javnog ključa u objekat podataka karakterističan za kontekst.

E. Sigurna razmjena poruka (Normativ)

Sigurna razmjena poruka pruža siguran (odnosno, kriptovan i autentikovan) kanal između terminala i čipa MRTD-a. Sigurna razmjena poruka može se uspostaviti autentikacijom čipa, putem PACE-a ili osnovne kontrole pristupa. Osigurani sigurnosni nivo, međutim, zavisi od mehanizama koji se koriste za postavljanje sigurne razmjene podataka.

Sesija započinje uspostavljanjem sigurne razmjene poruka. Sesija se završava samo onda kada se napusti sigurna razmjena poruka, npr. slanjem komande bez korištenja sigurne razmjene poruka. U toku sesije ključevi za sigurnu razmjenu poruka (odnosno oni uspostavljeni autentikacijom čipa, putem PACE-a ili osnovne kontrole pristupa) mogu biti izmijenjeni.

Napomena: Čip MRTD-a MOŽE indirektno odabrati *master fajl* kad se sesija završi.

Budući da ovo Uputstvo razmatra samo komandu APDU sa instrukcijom parnih bajtova, Dodatak F uzima u obzir isključivo sigurnu razmjenu poruka za parove komanda/odgovor pri čemu komanda APDU ima paran INS bajt.

E.1. Struktura poruka u sigurnoj razmjeni APDU

Objekti podataka iz sigurne razmjene poruka KORISTE se prema tabeli 28, sljedećim redoslijedom:

- Komanda APDU: [DO‘87’] [DO‘97’] DO‘8E’
- Odgovor APDU: [DO‘87’] DO‘99’ DO‘8E’

Svi objekti podataka iz sigurne razmjene poruka KODIRAJU se u DER (vidi Dodatak D.2). Stvarna vrijednost Lc modifikovaće se u Lc’ nakon primjene sigurne razmjene poruka. Ukoliko je potrebno, odgovarajući objekat podataka može se uvrstiti u APDU dio podatka da bi se prenijela originalna vrijednost Le. U zaštićenoj komandi APDU, *novi Le* bajt PODEŠEN je na ‘00’.

Napomena: Sigurna razmjena poruka MORA biti naznačena korištenjem prvog bajta identifikatora komande (class bajt) CLA = ‘XC’, sa bitmask X, pri čemu bit 8 (podešen na 0) ukazuje na klasu instrukcije *interindustry class*, a bit 5 (podešen na 1) ukazuje na promjenu komande.

E.1.1. Komanda APDU

Prema tome, komanda će uz primjenu sigurne razmjene poruka IMATI sljedeću strukturu, zavisno od stanja odgovarajuće nesigurne komande:

Naziv	Tag	Dužina	Komanda	Odgovor
Indikator popunjavanja sadržaja kojeg prati kriptogram	0x87	V	c	c
Zaštićeni Le	0x97	2V	c	x
Status obrade	0x99	2F	x	m
Kriptografski kontrolni zbir	0x8E	8F	m	M
F: fiksna dužina (tačan broj okteta), V: promjenjiva dužina (do broja okteta)				

Tabela 28: Upotreba objekata podataka za sigurnu razmjeu poruka

Case 1: CH || Lc' || DO'8E'|| new Le

Case 2: CH || Lc' || DO'97' || DO'8E' || new Le

Case 3: CH || Lc' || DO'87' || DO'8E' || new Le

Case 4: CH || Lc' || DO'87' || DO'97' || DO'8E' || new Le sa CH: Command Header (CLA INS P1 P2)

E.1.2. Odgovor APDU

Odgovor putem sigurne razmjene poruka IMA sljedeću strukturu, zavisno od stanja odgovarajuće nesigurne komande:

Case 1: DO'99' || DO'8E' || SW1SW2

Case 2: DO'87' || DO'99' || DO'8E' || SW1SW2

Case 3: DO'99' || DO'8E' || SW1SW2

Case 4: DO'87' || DO'99' || DO'8E' || SW1SW2

E.1.3. Popunjavanje

Podaci koje treba kriptovati POPUNJAVAJU se u skladu sa ISO 7816-4 [13] korištenjem indikatora 0x01. Za izračunavanje kriptografskog kontrolnog zbira APDU popunjava se u skladu sa ISO 7816-4 [13].

Napomena: Punjenje se uvijek obavlja u ovojnici za sigurnu razmjenu poruka, a ne preko osnovnog kriptografskog algoritma.

E.1.4. Primjeri

Data su tri primjera na kraju ovog dijela:

- Slika 4 prikazuje transformaciju nezaštićene komande APDU u zaštićenu komandu APDU u slučaju da su podatak i/ili Le dostupni. Ukoliko nijedan podatak nije dostupan, izostaviti dio DO '87'. Ako Le nije dostupno, izostaviti dio DO'97'.
- Slika 5 prikazuje transformaciju nezaštićene komande APDU u zaštićenu komandu APDU u slučaju kada podatak i Le nisu dostupni.
- Slika 6 prikazuje transformaciju nezaštićenog odgovora APDU u zaštićeni odgovor APDU u slučaju kada je podatak dostupan. Ako nijedan podatak nije dostupan,

izostaviti dio DO ’87’.

E.2. Kriptografski algoritmi

Sigurna razmjena poruka zasnovana je ili na 3DES-u [21] ili AES-u [22] na način prvo kriptovanje, pa potom autentikacija, odnosno, podatak je prvo kriptovan, a nakon toga se formatiran kriptovan podatak unosi u proračune za autentikaciju. Sesijski ključevi IZVODE se preko PACE-a ili autentikacije čipa korištenjem derivativne funkcije opisane u Dodatku A.2.3.

Napomena: Ako komanda ne sadrži komandne podatke, ne primjenjuje se nikakvo kriptovanje komande. Ako odgovor ne sadrži podatke koji se odnose na odgovor, nikakvo kriptovanje se ne primjenjuje na odgovor.

E.2.1. 3DES

3DES definisano je u [21].

E.2.1.1. 3DES kriptovanje

Za kriptovanje poruka KORISTE se dva ključa 3DES u CBC-modu u skladu sa ISO 10116 [12] sa ključem K_{Enc} and $IV = 0$.

E.2.1.2. 3DES autentikacija

Za autentikaciju poruka 3DES se KORISTI u maloprodajnom modu rada u skladu sa ISO/IEC 9797-1 [16] MAC algoritam 3 sa blok šifrom DES, ključ K_{MAC} i $IV = 0$. Grupu podataka čija autentikacija se izvršava TREBA dodati na početak putem brojača poslatih sekvenci.

E.2.2. AES

AES je definisan u [22].

E.2.2.1. AES Enkripcija

Za kriptovanje poruka AES KORISTI CBC-mod u skladu sa ISO 10116 [12] sa ključem

K_{Enc} i $IV = \mathbf{E}(K_{Enc}, SSC)$.

E.2.2.2. AES Autentikacija

Za autentikaciju poruka AES KORISTI CMAC-mod [24] sa K_{MAC} sa MAC dužinom od 8 bajtova. Grupu podataka čija autentikacija se izvršava TREBA dodati na početak putem brojača poslatih sekvenci.

E.3. Brojač poslatih sekvenci

Nepotpisan cijeli broj KORISTI se kao brojač poslatih sekvenci (SSC). Veličina bita SSC-a JEDNAKA je veličini blok šifre koja je korištena za sigurnu razmjenu poruka, odnosno, 64 bita za 3DES i 128 bita za AES.

SSC se POVEĆA svaki put prije generisanja komande ili odgovora APDU-a, odnosno, ako je početna vrijednost x, u sljedećoj komandi vrijednost SSC je $x+1$. Vrijednost SSC za prvi odgovor je $x+2$.

Ukoliko dođe do restartovanja sigurne razmjene poruka, SSC se koristi na sljedeći način:

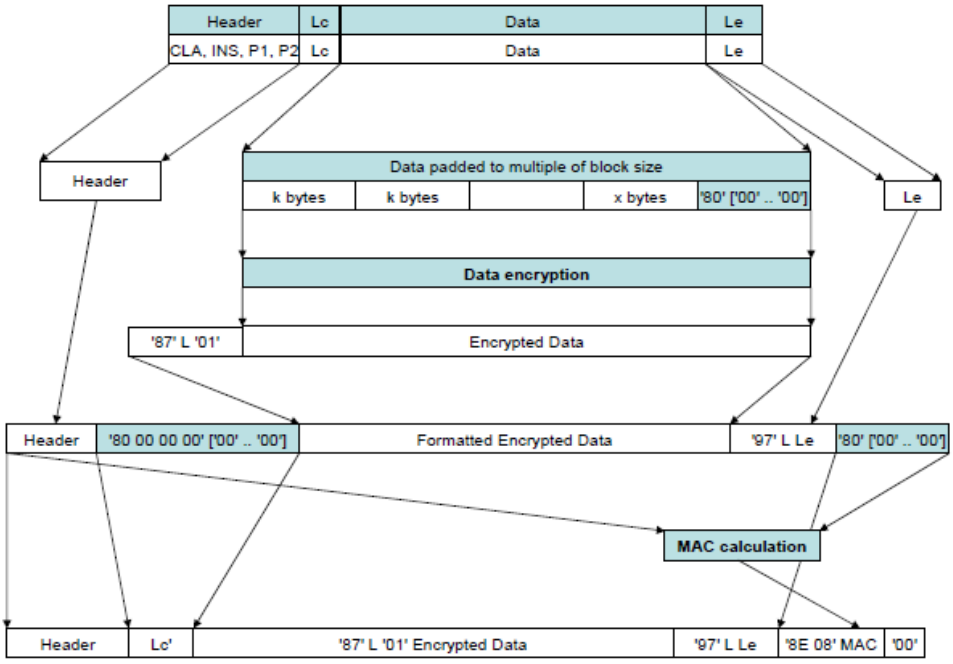
- Komande koje se koriste za slaganje ključeva zaštićene su starim sesijskim ključevima i starim SSC. Ovo se naročito odnosi na odgovor posljednje komande koja je korištena za slaganje sesijskih ključeva.
- Brojač poslatih sekvenci podešen je na svoju novu početnu vrijednost, odnosno u ovoj specifikaciji SSC je podešen na 0.
- Novi sesijski ključevi i novi SSC koriste se za zaštitu narednih komandi/odgovora.

E.4. Greške kod sigurne razmjene poruka

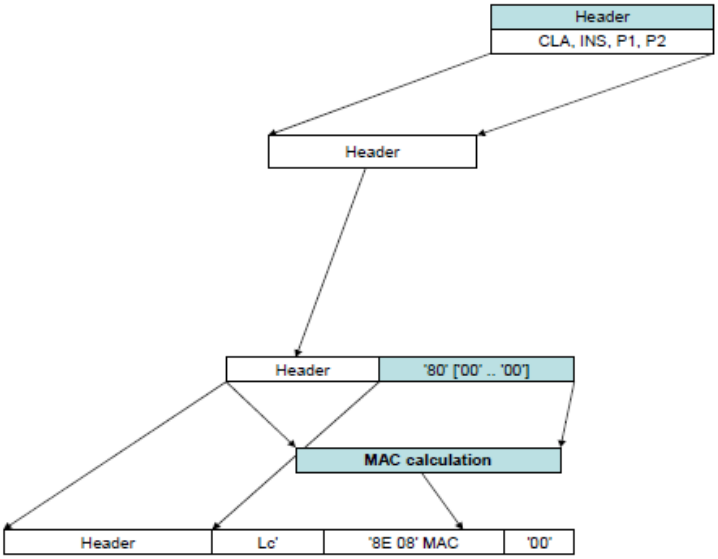
Čip MRTD-a MORA napustiti sigurnu razmjenu podataka ako, i samo ako, primi nekodiran APDU ili se pojavi greška prilikom sigurne razmjene poruka:

- Ukoliko nedostaju očekivani objekti podataka, čip MRTD-a ODGOVARA statusnim bajtom 0x6987
- Ukoliko su očekivani objekti podataka netačni, čip MRTD-a ODGOVARA statusnim bajtom 0x6988

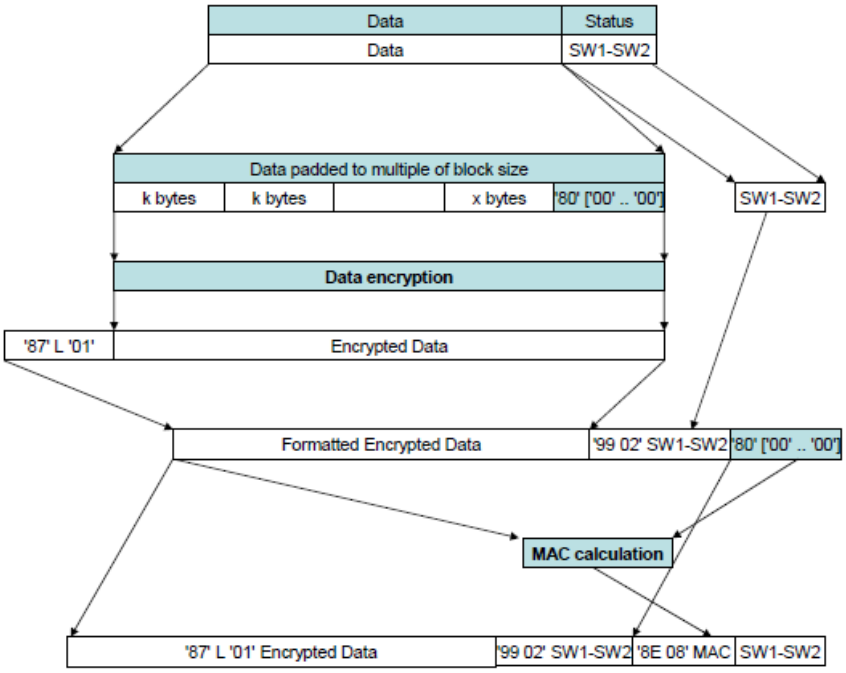
Ukoliko se napusti sigurna razmjena poruka, čip MRTD-a briše pohranjene sesijske ključeve i uspostavlja početne vrijednosti pristupnih prava terminala.



Slika 4: Transformacija APDU komande



Slika 5: Transformacija APDU komande koja ne sadrzi podatke



Slika 6: Transformacija odgovora na APDU komandu

Literatura

[1] ANSI. Public key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography, ANSI X9.42-2000,

1999

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

2119, 1997

[3] BSI. Elliptic Curve Cryptography (ECC) Version 1.11, TR-03111, 2009

[4] BSI. PKIs for Machine Readable Travel Documents – Protocols for the Management of Certificates and CRLs, TR-03129, 2009

[5] BSI. eCard-API-Framework - ISO24727-3 Interface Version 1.1.1, TR-03112-4,

2011

[6] Cooper, David; Santesson, Stefan; Farrell, Stephen; Boeyen, Sharon; Housley, Russell and Polk, Tim. Internet X.509 public key infrastructure - certificate and certificate revocation list (CRL) profile, RFC 5280, 2008

[7] Housley, Russel. Cryptographic message syntax (CMS), RFC 5652, 2009

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

[9] 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

[10] ICAO. Supplemental Access Control for Machine Readable Travel Documents, Technical Report, 2010

[11] ISO 32000-1:2008. Document management − Portable document format − Part 1: PDF 1.7, 2008

[12] ISO/IEC 10116:2006. Information technology − Security techniques − Modes of operation for an n-bit block cipher, 2006

[13] ISO/IEC 7816-4:2005. Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange, 2005

[14] ISO/IEC 7816-6:2004. Identification cards – Integrated circuit cards – Part 6: Interindustry data elements for interchange, 2004

[15] ISO/IEC 7816-8:2004. Identification cards – Integrated circuit cards – Part 8: Commands for security operations, 2004

[16] ISO/IEC 9797-1:1999. Information technology − Security techniques − Message

Authentication Codes (MACs) − Part 1: Mechanisms using a block cipher, 1999

[17] 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

[18] Jonsson, Jakob and Kaliski, Burt. Public-key cryptography standards (PKCS)#1: RSA cryptography specifications version 2.1, RFC 3447, 2003

[19] Lepinski, Matt; Kent, Stephen. Additional Diffie-Hellman Groups for Use with

IETF Standards, RFC 5114, 2008

[20] Lochter, Manfred; Merkle, Johannes. Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, RFC 5639, 2010

[21] NIST. Data Encryption Standard (DES), FIPS PUB 46-3, 1999

[22] NIST. Specification for the Advanced Encryption Standard (AES), FIPS PUB

197, 2001

[23] NIST. Secure hash standard (and Change Notice to include SHA-224), FIPS PUB

180-2, 2002

[24] NIST. Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, 2005

[25] NIST. Digital Signature Standard (DSS), FIPS 186-3, 2009

[26] Rescorla, Eric. Diffie-Hellman key agreement method, RFC 2631, 1999

[27] RSA Laboratories. PKCS#3: Diffie-Hellman key-agreement standard, RSA Laboratories Technical Note, 1993

[28] RSA Laboratories. PKCS#1 v2.1: RSA cryptography standard, RSA Laboratories Technical Note, 2002