Tehničko uputstvo

Napredni sigurnosni mehanizmi za mašinski čitljive putne dokumente

Dio 1 – Elektronski mašinski čitljivi putni dokumenti (eMRTD) sa BAC/PACEv2 i EACv1

Banja Luka, 01.03.2013. godine

Sadržaj

1 Uvod

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

Međunarodna organizacija civilne avijacije (ICAO) standardizuje mašinski čitljive putne dokumente u Dokumentu 9303 ICAO. Ovaj standard sastoji se iz tri dijela:

Dio 1: Mašinski čitljivi pasoši

• Poglavlje 1: Pasoši sa mašinski čitljivim podacima pohranjenim u format optički prepoznatljivih znakova

• Poglavlje 2: Specifikacije za elektronski osposobljene pasoše sa sposobnošću biometrijske identifikacije

Dio 2: Mašinski čitljive vize

Dio 3: Mašinski čitljivi zvanični putni dokumenti

• Poglavlje 1: Zvanični putni dokumenti sa mašinski čitljivim podacima pohranjenim u format optički prepoznatljivih znakova

• Poglavlje 2: Specifikacija elektronski osposobljenih zvaničnih putnih dokumenata sa sposobnošću biometrijske identifikacije

Ova tehnička smjernica uglavnom se fokusira i detaljnije opisuju sigurnosne mehanizme za elektronske putne dokumente opisane u Dokumentu 9303 Dio 1 Poglavlje 2 [2] i Dokument 9303, Dio 3 Poglavlje 2 [3] kako bi se zaštitila autentičnost (uključujući i integritet), originalnost i povjerljivost podataka pohranjenih na radiofrekvencijskom čipu ugrađenom u putni dokument. Ukratko, sigurnosni mehanizmi navedeni u [2], [3], [4] su: *pasivna autentikacija, aktivna autentikacija i kontrola pristupa (tj. osnovna kontrola pristupa-BAC i uspostavljanje veze preko autentikacije lozinkom-PACE), kako je dato u Tabeli 1.*

Mehanizam	Zaštita	Kriptografska tehnika
Pasivna autentikacija	Autentičnost	Digitalni potpis
Aktivna autentikacija	Originalnost	Upit-odgovor
Kontrola pristupa	Povjerljivost	Autentikacija & sigurni kanali

Tabela 1: Sigurnosni mehanizmi ICAO-a

Primjena aktivne autentikacije i kontrole pristupa je opcionog karaktera, dok je pasivna autentikacija obavezna. Iz toga direktno slijedi da se bez primjene ovih ili ekvivalentnih mehanizama, originalnost i povjerljivost pohranjenih podataka ne može garantovati. Ovo uputstvo je fokusirano na te aspekte i određuje dodatne mehanizme za autentikaciju i kontrolu pristupa koji su važni za siguran čip mašinski čitljivog putnog dokumenta.

1.1 Pasivna autentikacija

Aplikacija za elektronske pasoše ICAO-a u osnovi obuhvata 16 grupa podataka (DG1-DG16) i objekat sigurnosti dokumenta za pasivnu autentikaciju. Pregled korištenja ovih grupa podataka dat je u tabeli 3.

Za pasivnu autentikaciju koristi se digitalni potpis kako bi se izvršila autentikacija podataka pohranjenih u grupama podataka na čipu mašinski čitljivog putnog dokumenta. Taj potpis generiše potpisnik dokumenta (npr. proizvođač mašinski čitljivog putnog dokumenta) u fazi personalizacije čipa mašinski čitljivog putnog dokumenta putem elementa sigurnosti dokumenta koji sadrži heš vrijednosti svih grupa podataka pohranjenih na čipu. Za pojedinosti vezane za objekat sigurnosti dokumenta, potpisnike dokumenta i krovno certifikaciono tijelo za izdavanje elektronskih putnih dokumenata u državi, čitalac se upućuje na [2], [3].

Da bi se potvrdili podaci pohranjeni na čipu mašinski čitljivog putnog dokumenta putem pasivne autentikacije, terminal mora izvršiti slijedeće:

1. Očitati objekat sigurnosti dokumenta koji se nalazi u čipu mašinski čitljivog putnog dokumenta.
2. Preuzeti odgovarajući certifikat za potpisivanje dokumenata, pouzdan certifikat krovnog certifikacionog tijela za izdavanje elektronskih putnih dokumenata u državi, i odgovarajući spisak opozvanih certifikata.
3. Potvrditi certifikat potpisnika dokumenta i potpis elementa sigurnosti dokumenta
4. Proračunati heš vrijednosti grupa podataka koje se očitavaju i uporediti ih sa heš vrijednostima u elementu sigurnosti dokumenta.

Pasivna autentikacija omogućava terminalu da otkrije grupe podataka kojima se manipuliše, ali ne sprečava kloniranje čipova mašinski čitljivih putnih dokumenata, tj. kopiranje svih podataka pohranjenih na jednom čipu mašinski čitljivog putnog dokumenta na drugi.

1.2 Aktivna autentikacija

Aktivna autentikacija je digitalna karakteristika sigurnosti koja sprečava kloniranje uvođenjem para ključeva koji je jedinstven za svaki čip:

• Javni ključ je pohranjen u grupi podataka DG15 i samim tim zaštićen pasivnom autentikacijom.

• Odgovarajući privatni ključ pohranjen je u sigurnoj memoriji i može se koristiti samo unutar čipa mašinski čitljivog putnog dokumenta i ne može se očitati.

Na taj način, čip može dokazati poznavanje tog privatnog ključa putem protokola "izazov-odgovor", koji se naziva i aktivna autentikacija. U ovom protokolu čip mašinski čitljivog putnog dokumenta digitalno potpisuje izazov koji je terminal nasumično izabrao. Terminal prepoznaje da je čip putnog dokumenta autentičan ako, i samo ako je povratni potpis ispravan. Aktivna autentikacija predstavlja direktan protokol i veoma efikasno sprečava kloniranje, ali uvodi opasnost za privatnost: Semanitički upiti (vidi Dodatak B za diskusiju vezanu za Semantičke upite).

1.3 Kontrola pristupa

Kontrola pristupa nije potrebna samo zbog pitanja privatnosti, već umanjuje i rizik od pokušaja kloniranja. Čip koji se nalazi na mašinski čitljivom putnom dokumentu štiti pohranjene podatke od neovlašćenog pristupa kroz upotrebu odgovarajućih mehanizama za kontrolu pristupa kao što je opisano u nastavku:

• Manje osjetljivi podaci (npr. mašinski čitljiva zona, fotografija i drugi podaci koje je relativno lako pronaći iz drugih izvora) koji su potrebni za globalnu međuoperativnost graničnih prelaza zaštićeni su osnovnom kontrolom pristupa – BAC. Za bolje razumijevanje čitaoca, osnovna kontrola pristupa opisana je u Dodatku A.

• Da bi se olakšala primjena, osnovna kontrola pristupa zasnovana je samo na simetričnoj kriptografiji, čime se jačina izvedenih sesijskih ključeva ograničava jačinom unosnih podataka, tj. odštampanom mašinski čitljivom zonom. Zbog toga se uvodi protokol – PACE (Uspostavljanje konekcije putem autentikacije lozinkom). Ovaj protokol zasnovan je na asimetričnoj kriptografiji i osigurava sesijske ključeve čija je jačina nezavisna od entropije unosnih podataka. Kada je u pitanju migracija, ICAO definiše i *dodatnu kontrolu pristupa* (vidi [4]), koja zahtijeva da pasoši kod kojih se primijenjuje PACE, primijenjuju i osnovnu kontrolu pristupa.

• Osjetljivi podaci (npr. otisak prsta i drugi podaci do kojih nije jednostavno doći iz drugih mnogobrojnih izvora) moraju biti dostupni samo ovlašćenim terminalima. Takvi podaci su dodatno zaštićeni i proširenom kontrolom pristupa.

Osnovna kontrola pristupa samo provjerava da li terminal ima fizički pristup putnim dokumentima tako što traži optičko očitanje mašinski čitljive zone. Proširena kontrola pristupa dodatno provjerava da li je terminal ovlašten da očitava osjetljive podatke. Prema tome, zahtijeva se stroga kontrola terminala. Međutim, proširena kontrola pristupa se ne traži pri globalnoj međuoperativnosti graničnih prelaza, ICAO još uvijek nije definisao ovaj protokol.

Uspostavljanje konekcije putem autentikacije lozinkom (PACE) koje se uvodi u ovoj specifikaciji može se koristiti kao sigurnija i pogodnija zamjena za osnovnu kontrolu pristupa.

1.4 Poboljšanja

U poređenju sa prethodnim verzijama BSI dokumenata, ova verzija obuhvata i slijedeća poboljšanja u oblasti pasoša:

• Integracija PACE u naprednu inspekcijsku proceduru.

• Ekstenzija sigurne razmjene poruka pri autentikaciji čipa na AES. U cijelom ovom dijelu Uputstva, PACE se odnosi na PACEv2 kao što je definisano u [4].

1.5 Uslovi za čipove i terminale mašinski čitljivih putnih dokumenata

U ovim Tehničkim smjernicama navedeni su uslovi za primjenu čipova i terminal mašinski čitljivih putnih dokumenata. Dok čipovi mašinski čitljivih dokumenata moraju ispunjavati uslove u skladu sa terminologijom opisanom u Dijelu 1.6,uslovi za terminale tumače se kao smjernice, tj. međuoperativnost čipa i terminal mašinski čitljivog putnog

dokumenta može se garantovati samo ukoliko terminal ispunjava te uslove, u suprotnom interakcija sa čipom će ili biti neuspješna ili će ponašanje čipa biti nedefinisano. U osnovi, čip mašinski čitljivog putnog dokumenta ne treba ispunjavati uslove vezane za terminale osim ako sigurnost čipa mašinski čitljivog putnog dokumenta nije direktno ugrožena.

1.6 Terminologija

Ključne riječi: "MORATI", "NE SMJETI", "TRAŽITI", "HTJETI", "NE HTJETI", "TREBATI, "NE TREBATI", "PREPORUČITI", "MOĆI", I "OPCIONO" u ovom dokumentu tumače se kao što je opisano u RFC 2119 [1]. Ključna riječ "USLOVLJENO" tumači se na sljedeći način:
USLOVLJENO: Upotreba jedne stavke zavisi od upotrebe drugih stavki. Stoga je dalje određeno
pod kojim uslovima se ta stavka TRAŽI ili PREPORUČUJE.

Kada se koriste u tabeli (profilima), ključne riječi se skraćuju kao što je navedeno u tabeli 2.

Ključna riječ		Skraćenic
MORATI/ HTJETI	TRAŽITI	m
NE SMJETI / NE HTJETI	–	x
TREBATI	PREPORUČITI	r
MOĆI	OPCIONO	o
–	USLOVLJENO	c

Tabela 2: Ključne riječi

2 Aplikacije za mašinski čitljive putne dokumente

U okviru ovog poglavlja se nalaze sistemi za mašinski čitljive putne dokumente

2.1 Aplikacija za elektronski pasoš

Aplikaciju za elektronski pasoš definisao je ICAO [2], [3], [4], [5]. Da biste očitali podatke iz aplikacije za elektronski pasoš, čip mašinski čitljivog putnog dokumenta TREBA zahtijevati da se izvrši autentikacija terminala kao inspekcijskog sistema. Različite autentikacijske procedure za aplikaciju za elektronski pasoš date su na slici 1.

2.2 Inspekcijski sistem

Inspekcijski sistem je službeni terminal kojim uvijek upravlja vladina organizacija (tj. domaći ili strani verifikator dokumenata). Čip mašinski čitljivog putnog dokumenta TREBA zahtijevati od inspekcijskog sistema da obavi svoju autentikaciju prije dodjele pristupa u skladu sa aktuelnom autorizacijom. Ovaj dio Tehničkog uputstva definiše dvije alternative za autentikaciju terminala kao inspekcijskog sistema: standardnu inspekcijsku proceduru i naprednu inspekcijsku proceduru.
Za očitanje aplikacije za elektronski pasoš koja zadovoljava ICAO standarde, MORA se koristiti standardna ili napredna inspekcijska procedura (uporedi Dio 2.4). U tome se ogleda razlika između *osnovnog inspekcijskog sistema* i *proširenog inspekcijskog sistema*.

• **Osnovni inspekcijski sistem:** Terminal koji koristi standardnu inspekcijsku proceduru kako bi obavio svoju autentikaciju na čipu mašinski čitljivog putnog dokumenta.

• **Prošireni inspekcijski sistem:** Terminal koji koristi procedure napredne inspekcije elektronskog pasoša.

Grupa podataka	Sadržaj	Očitati/ Ispisati	Obavezno/ Opciono	Kontrola pristupa BAC/PACE	EAC v1
DG1	Mašinski čitljiva zona	R	m	m	x
DG2	Biometrija: Lice	R	m	m	x
DG3	Biometrija: Prst	R	o	m	m
DG4	Biometrija: Zjenica oka	R	o	m	m
...		R	o	m	o
DG14	Sigurnosne informacije	R	c	m	x
DG15	Aktivna autentikacija	R	o	m	x
DG16	...	R	o	m	x
SO_D	Objekat sigurnosti dokumenta	R	m	m	x

DG14 je definisana i Dijelu 3. Skraćenice (o,c,r,m,x) date su u tabeli 2.

Tabela 3: Grupe podataka za aplikaciju za elektronski pasoš

Osnovni inspekcijski sistem ovlašten je samo za pristup manje osjetljivim podacima koji se nalaze u aplikaciji za elektronski pasoš koja zadovoljava standard ICAO-a. Nivo ovlaštenja proširenog inspekcijskog sistema ODREDIĆE se aktuelnom autorizacijom izračunatom iz lanca certifikata.

2.3 Lozinke

Da biste dozvolili nosiocu mašinski čitljivog putnog dokumenta da kontroliše pristup aplikacijama sprovedenim za beskontaktni čip, navedene su osnovna i proširena kontrola pristupa. Zbog ograničenja osnovne kontrole pristupa, ova specifikacija uvodi PACE kao siguran i praktičan mehanizam za ograničavanje pristupa aplikacijama na osnovu znanja, odnosno na osnovu lozinki koje su ili štampane na dokumentu ili su poznate samo legitimnom nosiocu dokumenta.
Dok osnovna kontrola pristupa podržava samo jednu "lozinku", tj simetričan ključ izveden iz mašinski čitljive zone, protokol PACE podržava više lozinki. Različite vrste lozinki koje se koriste u ovom dijelu specifikacije su:

CAN: Broj pristupne kartice (CAN) je kratka lozinka koja je odštampana ili prikazana na dokumentu. CAN predstavlja lozinku koja se ne može blokirati, odnosno čip na mašinski čitljivom putnom dokumentu NE SMIJE blokirati CAN ukoliko autentikacija ne uspije. CAN može biti statički (odštampan na dokumentu), polustatički (odštampan na naljepnici dokumenta) ili dinamički (nasumično ga odabere čip mašinski čitljivog putnog dokumenta i prikaže na samom dokumentu korišćenjem npr. elektronskog papira, OLED-a ili sličnih tehnologija).

MRZ: Lozinka za mašinski čitljivu zonu predstavlja statički tajni ključ koji ne može biti blokiran, a koji je izveden iz mašinski čitljive zone i može se koristiti i za PACE i za BAC.

Napomena: Budući da ovo Tehničko uputstvo ne preporučuje nikakvu određenu dužinu lozinki, svaka lozinka koja se ne može blokirati MORA sadržati dovoljnu entropiju ili mašinski čitljiv čip MORA primijeniti dodatne protivmjere za zaštitu od brutalnih udara. Protivmjere MOGU obuhvatiti odlaganja, ali NE SMIJU blokirati lozinke nakon neispravnih unošenja.

2.4 Inspekcijske procedure

Zavisno od toga da li je uređaj (odnosno, čip ili terminal mašinski čitljivog putnog dokumenta) u skladu sa ovom specifikacijom, uređaj nazivamo usklađenim ili neusklađenim. Zavisno od kombinacije terminala i čipa mašinski čitljivog putnog dokumenta, koristi se ili *standardna ili napredna inspekcijska procedura*:

• Neusklađeni inspekcijski sistem koristi standardnu inspekcijsku proceduru. Manje osjetljivi podaci pohranjeni na čipu MORAJU biti čitljivi na svakom neusklađenom inspekcijskom sistemu.

Inspekcijski sistem	Čip mašinski čitljivog putnog dokumenta	
	usklađeni	neusklađeni
usklađeni	napredni	standardni
neusklađeni	standardni	standardni

Tabela 4: Inspekcijske procedure

- Usklađeni inspekcijski sistem KORISTI naprednu inspekcijsku proceduru ukoliko je čip koji se nalazi na mašinski čitljivom dokumentu usklađen. U suprotnom, koristi se standardna inspekcijska procedura.

Tabela 4 daje pregled inspekcijskih procedura koje će se koristiti.

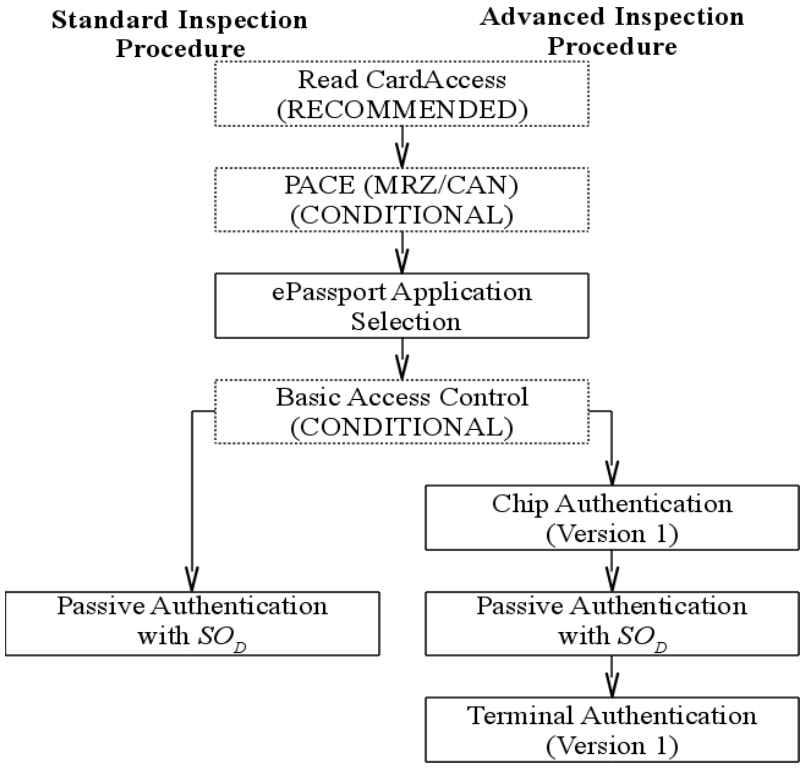
Terminal može koristiti ili standardnu inspekcijsku procedure za pristup manje osjetljivim podacima koji se nalaze u aplikaciji za elektronske pasoše ili naprednu inspekcijsku proceduru za pristup manje osjetljivim i osjetljivim podacima koji se nalaze u aplikaciji za elektronske pasoše.

Za standardnu inspekcijsku proceduru POTREBNO je da je mašinski čitljiva zona poznata terminalu (budući da se *osnovna kontrola pristupa* PREPORUČUJE za čipove mašinski čitljivih putnih dokumenata). Za naprednu ispekcijsku proceduru MORA biti poznata ili mašinski čitljiva zona ili CAN.

Napomena: Kao što je opisano u Dijelu 1.1, pasivna autentikacija je kontinuiran proces koji zahtijeva izračunavanje heš vrijednosti svake grupe podataka koja se očita sa čipa, kao i njeno poređenje sa odgovarajućim heš vrijednostima elementa bezbjednosti dokumenta. Ovaj kontinuirani proces nije eksplicitno opisan, budući da se pretpostavlja da će biti primijenjen u narednim procedurama.

2.4.1 Otvaranje aplikacija za elektronski pasoš

Aplikacija za elektronski pasoš MORA biti otvorena kao dio standardne ili napredne inspekcijske procedure za elektronske pasoše. Otvaranje aplikacije za elektronske pasoše podrazumijeva odabir aplikacije za elektronski pasoš i izvršavanje kontrole pristupa kako to zahtijevaju čip koji se nalazi na mašinski čitljivom putnom dokumentu, odnosno, *osnovna kontrola pristupa* ili PACE.



Slika 1: Procedure za autentikaciju u aplikaciji za elektronski pasoš

Ukoliko čip koji se nalazi na mašinski čitljivom putnom dokumentu to zahtijeva, MORA se koristiti ili PACE ili *osnovna kontrola pristupa.* Ukoliko čip koji se nalazi na mašinski čitljivim putnim dokumentima podržava i PACE i *osnovnu kontrolu* pristupa, inspekcijski sistem TREBA koristiti PACE umjesto *osnovne kontrole pristupa.* Procedura otvaranja sastoji se od sljedećih koraka:

1. Čitanje CardAccess elementarne datoteke (PREPORUČUJE SE)

Terminal TREBA pokušati očitati elementarnu datoteku CardAccess kako bi se odredili parametri (odnosno, simetrične cifre, ključni algoritmi slaganja, parametri domena i mapiranje) koje podržava čip. Terminal može odabrati bilo koji od ovih parametara.
Ukoliko čitanje ove elementarne datoteke nije moguće, terminal TREBA pokušati očitati elektronski pasoš putem *osnovne kontrole pristupa.*

2. PACE (USLOVLJENO)

Ovaj korak se PREPORUČUJE ukoliko čip mašinski čitljivog dokumenta podržava PACE. Čip PRIHVATA sljedeće lozinke za PACE:

• mašinski čitljiva zona (podrška čipa mašinski čitljivog dokumenta se ZAHTIJEVA),
• CAN (podrška čipa mašinski čitljivog dokumenta je OPCIONA).

Ukoliko se obavi uspješno, čip mašinski čitljivog dokumenta radiće sljedeće:

- ZAPOČEĆE sigurnu razmjenu poruka.

- DODIJELIĆE pristup manje osjetljivim podacima (npr. DG1, DG2, DG14, DG15, itd. i elementu sigurnosti dokumenta).
- OGRANIČIĆE pristupna prava kako bi se zahtijevala sigurna razmjena podataka.

3. Odabrati aplikaciju za elektronski pasoš (ZAHTIJEVA SE)

4. Osnovna kontrola pristupa (USLOVLJENO)

Ovaj korak se ZAHTIJEVA ako kontrolu pristupa traži čip mašinski čitljivog putnog dokumenta, a PACE nije korišćen.

Ukoliko je kontrola uspješno obavljena, čip mašinski čitljivog dokumenta radiće sljedeće:

- ZAPOČEĆE sigurnu razmjenu poruka.
- DODIJELIĆE pristup grupi podataka DG14 (koja sadrži javni ključ za autentikaciju čipa).
- TREBA dodijeliti pristup manje osjetljivim podacima (npr. DG1, DG2, DG15, itd. i elementu sigurnosti dokumenta)[1].
- OGRANIČIĆE pristupna prava kako bi se zahtijevala sigurna razmjena podataka.

2.4.2 Standardna inspekcijska procedura

Standardna inspekcijska procedura može se koristiti za sve aplikacije za elektronski pasoš koje su usklađene sa ICAO standardima. Ako čip mašinski čitljivog putnog dokumenta podržava i PACE i *osnovnu kontrolu pristupa*, inspekcijski sistem ĆE KORISTITI PACE umjesto *osnovne kontrole pristupa.* Standardna inspekcijska kontrola sastoji se iz slijedećeg:

1. Otvaranje aplikacije elektronskog pasoša (ZAHTIJEVA SE)

2. Pasivna autentikacija (ZAHTIJEVA SE)

Terminal MORA očitati i potvrditi objekat sigurnosti dokumenta. Ukoliko je pristup kartici učitan, terminal UPOREĐUJE nesigurne informacije o sigurnosti koje su očitane putem pristupa kartici sa sigurnim sadržajem grupe podataka br. 14 (DG14).

3. Aktivna autentikacija (OPCIONO)

Ukoliko je to dostupno, terminal MOŽE očitati i potvrditi grupu podataka br. 15 (DG15) i izvršiti aktivnu autentikaciju.

4. Očitati i izvršiti autentikaciju podataka

[1] Za aplikaciju za elektronske pasoše koja je usklađena sa ICAO standardima, čip mašinski čitljivog dokumenta MORA dodijeliti pristup svim manje osjetljivim podacima. Ukoliko se ne zahtijeva usklađenost sa ICAO standardima, čip mašinski čitljivog dokumenta MOŽE odbiti pristup određenim grupama podataka dok se ne izvrši autentikacija čipa.

Terminal MOŽE očitati i potvrditi grupe podataka koje sadrže manje osjetljive podatke.

2.4.3 Napredna inspekcijska procedura

Procedura za naprednu inspekciju može se koristiti samo za aplikacije za elektronski pasoš koje su u skladu sa ICAO/EAC1. Napredna inspekcijska procedura sastoji se od sljedećeg:

1. Otvaranje aplikacije elektronskog pasoša (ZAHTIJEVA SE)

2. Autentikacija čipa Verzija 1 (ZAHTIJEVA SE)

Terminal OČITAVA grupu podataka (DG14) i obavlja autentikaciju čipa. Čip mašinski čitljivog putnog dokumenta radi sljedeće:

- ZAPOČINJE ponovnu sigurnu razmjenu poruka.
- DODIJELJUJE pristup manje osjetljivim grupama podataka (npr. DG1, DG2, DG15, itd.. i objekat sigurnosti dokumenta).
- OGRANIČAVA pristupna prava kako bi se tražila sigurna razmjena poruka koja se uspostavlja autentikacijom čipa.

3. Pasivna autentikacija (započeta) (ZAHTJEVA SE)

Terminal obavlja sljedeće:

- OČITAVA i POTVRĐUJE objekat sigurnosti dokumenta.
- POTVRĐUJE grupu podataka DG14. Ukoliko je očitan pristup kartici, terminal UPOREĐUJE nesigurne informacije o sigurnosti koje su očitane putem pristupa kartici sa sigurnim sadržajem grupe podataka (DG14).

4. Aktivna autentikacija (OPCIONO)

Ukoliko je to dostupno, terminal MOŽE očitati i potvrditi grupu podataka (DG15) i izvršiti aktivnu autentikaciju.

5. Autentikacija terminala Verzija 1 (USLOVLJENO)

Ovaj korak se ZAHTIJEVA za pristup osjetljivim podacima elektronskog pasoša. Ukoliko se obavi uspješno, čip mašinski čitljivog putnog dokumenta radi sljedeće:

- DODJELJUJE dodatni pristup grupama podataka prema pristupnim pravima za terminal.
- OGRANIČAVA sva pristupna prava kako bi se tražila si razmjena poruka koja se uspostavlja autentikacijom čipa i korišćenjem kratkotrajnog javnog ključa čija se autentikacija obavlja putem autentikacije terminala.

6. Očitavanje i autentikacija podataka
Terminal MOŽE očitati i potvrditi grupe podataka u skladu sa pristupnim pravima za terminal.

3 Specifikacije protokola

U ovom poglavlju kriptografski protokoli za PACE, autentikaciju čipa i terminala određeni su pod pretpostavkom proizvoljne komunikacione infrastrukture. Mapiranje za komande ISO 7816 dato je u poglavlju 3 ovih Tehničkih smjernica.

3.1 Kriptografski algoritmi i simboli

Protokoli se izvršavaju između dvije strane: čipa mašinski čitljivog putnog dokumenta (PICC) i terminala (PCD). Tabela 5 daje pregled korištenih parova ključeva. Korištene su slijedeće kriptografske operacije i simboli.

3.1.1 Kompresioni i heš algoritmi

Operacije za izračunavanje kriptografskog heša i kompresije javnog ključa opisani su na algoritamski nezavisan način.

3.1.1.1 Operacije

• Operacija za izračunavanje heša preko poruke m označena je kao $\mathbf{H}(m)$.
• Operacija za izračunavanje kompresovane slike javnog ključa označena je kao $\mathbf{Comp}(PK)$.

3.1.2 Simetrični algoritmi ključa

Ključevi i operacije za simetričnu enkripciju i autentikaciju ključeva opisani su na algoritamski nezavisan način.

3.1.2.1 Ključevi

Simetrični ključevi izvode se iz zajedničkog tajnog K i OPCIONOG proizvoljnog i jednom upotrijebljenog r ili iz lozinke π korištenjem funkcije za izvođenje ključeva (KDF):
• Izvođenje ključa za enkripciju poruka označeno je sa $K_{Enc} = \mathbf{KDF_{Enc}}(K, [r])$.
• Izvođenje ključa za autentikaciju poruke označeno je kao $K_{MAC} = \mathbf{KDF_{MAC}}(K, [r])$.

Protokol	MRTD čip	Terminal	Napomena
Autentikacija čipa	PK_{PICC}, SK_{PICC}	$\widetilde{PK_{PCD}}$, $\widetilde{SK_{PCD}}$	Par ključeva koji koristi terminal predstavlja trenutni par ključeva koji se razlikuje od trenutnog para ključeva za PACE.
Autentikacija terminala	PK_{CVCA}	PK_{PCD}, SK_{PCD}	Čip mašinski čitljivog putnog dokumenta potvrđuje lanac certifikata koje primi terminal korištenjem javnog ključa CVCA.

Tabela 5: Pregled parova ključeva koji su upotrijebljeni

3.1.2.2 Ključevi

Za autentikaciju čipa, čip mašinski čitljivog putnog dokumenta koristi statički Diffie-Hellman par ključeva, a terminal generiše trenutni par ključeva na osnovu parametara statičkog domena čipa mašinski čitljivog putnog dokumenta D_{PICC}.

- Statički javni ključ čipa mašinski čitljivog putnog dokumenta je PK_{PICC}, a

odgovarajući privatni ključ je SK_{PICC}.

- Trenutni javni ključ terminala je $\widetilde{PK}_{PCD}$, a odgovarajući privatni ključ je $\widetilde{SK}_{PCD}$.
- Kompresovani trenutni javni ključ terminala označen je kao **Comp** ($\widetilde{PK}_{PCD}$).

PREPORUČUJE SE da čip mašinski čitljivog putnog dokumenta potvrđuje javne ključeve koje primi od terminala.

3.1.2.3 Operacije

Operacija za generisanje zajedničkog tajnog ključa K označena je kao $K = \mathbf{KA}(SK, PK, D)$, gdje je SK (trenutni ili statički) tajni ključ, PK je (trenutni ili statički) javni ključ, a D su (trenutni ili statički) parametri domena.

3.1.3 Potpisi

Ključevi i operacije za potpise opisani su na algoritamski nezavisan način. Mapiranje za RSA i ECDSA dato je u poglavlju 3 ovog Tehničkog uputstva.

3.1.3.1 Ključevi

Terminal za autentikaciju koristi slijedeći ključ:

• Terminal ima statički par ključeva za autentikaciju. Javni ključ je PK_{PCD}, a odgovarajući privatni ključ je SK_{PCD}.

3.1.3.2 Operacije

Operacije za potpisivanje i potvrđivanje poruka određene su na slijedeći način:

• Potpisivanje poruke m privatnim ključem SK_{PCD} određeno je preko s=**Sign** (SK_{PCD}, m).

• Potvrđivanje rezultirajućeg potpisa s javnim ključem PK_{PCD} određeno je preko **Verify**(PK_{PCD},s,m) .

3.2 Osnovna kontrola pristupa

Osnovna kontrola pristupa objašnjena je u [2]. Za dodatno informisanje, specifikacija i diskusija o ograničenjima dati su u Dodatku A.

3.3 PACE

Protokol PACE predstavlja lozinkom autentifikovan Diffie-Hellman protokol za slaganje ključeva koji pruža sigurnu komunikaciju i eksplicitnu autentikaciju zasnovanu na čipu i terminalu mašinski čitljivog dokumenta (odnosno, čip i terminal mašinski čitljivog dokumenta dijele istu lozinku).
Protokol uspostavlja sigurnu razmjenu poruka između čipa i terminala mašinski čitljivog putnog dokumenta, koja je zasnovana na slabim (kratkim) lozinkama. PACE predstavlja alternativu osnovnoj kontroli pristupa, odnosno, omogućava čipu mašinski čitljivog putnog dokumenta da potvrdi da je terminal ovlašten da pristupi pohranjenim manje osjetljivim podacima, ali ima i dvije prednosti:

• Jaki sesijski ključevi osigurani su nezavisno od jačine lozinke.

• Entropija lozinki koje se koriste za autentikaciju terminal može biti veoma niska (npr. 6 znakova je u suštini dovoljno).

PACE je objašnjen u poglavlju [4]. Za dodatne informacije, pogledajte i poglavlje 3 ovog Tehničkog uputstva.

3.4 Autentikacija čipa, verzija 1

Protokol za autentikaciju čipa predstavlja kratkotrajan statički Diffie-Hellman protokol za slaganje ključeva koji osigurava sigurnu komunikaciju i jednostranu autentikaciju čipa mašinski čitljivog putnog dokumenta.
Protokol uspostavlja sigurnu razmjenu poruku između čipa i terminala mašinski čitljivog putnog dokumenta zasnovanog na statičkom paru ključeva pohranjenom u čipu mašinski čitljivog dokumenta. Autentikacija čipa predstavlja alternativu opcionoj aktivnoj autentikaciji ICAO-a, odnosno, omogućuje terminalu da potvrdi da je čip mašinski čitljivog putnog dokumenta autentičan, i ima dvije prednosti nad originalnim protokolom:

• Spriječeni su semantički upiti, budući da transkripte koje proizvede ovaj protokol nije moguće prenositi.
• Pored autentikacije čipa mašinski čitljivog putnog dokumenta, ovaj protokol osigurava i jake sesijske ključeve. Detalji vezani za semantičke upite opisani su u Dodatku B.

Protokol u svojoj verziji 1 putem sigurne razmjene poruka pruža implicitnu autentikaciju, kako samog čipa, tako i podataka pohranjenih na njemu uz upotrebu novih sesijskih ključeva.

3.4.1 Specifikacija protokola

Slijedeće korake obavljaju terminal i čip mašinski čitljivog putnog dokumenta. Pojednostavljena verzija prikazana je na slici 2.

1. Čip mašinski čitljivog putnog dokumenta šalje terminalu svoj statički Diffie-Hellman javni ključ PK_{PICC}, i parametar domena D_{PICC}.
2. Terminal generiše kratkotrajni Diffie-Hellman par ključeva $(\widetilde{SK}_{PCD}, \widetilde{PK}_{PCD}, D_{PICC})$ i šalje čipu mašinski čitljivog putnog dokumenta kratkotrajni javni ključ $\widetilde{PK}_{PCD}$.
3. I čip i terminal mašinski čitljivog putnog dokumenta izračunavaju slijedeće:
   a) Zajednički tajni $K = \mathbf{KA}(SK_{PICC}, \widetilde{PK}_{PCD}, D_{PICC}) = \mathbf{KA}(\widetilde{SK}_{PCD}, PK_{PICC}, D_{PICC})$
   b) Sesijske ključeve $K_{MAC} = \mathbf{KDF}_{MAC}(K)$ i $K_{Enc} = \mathbf{KDF}_{Enc}(K)$ izvedene iz K za sigurnu razmjenu poruka.
   c) Kompresovani kratkotrajni javni ključ terminala **Comp** $(\widetilde{PK}_{PCD})$ za autentikaciju terminala.

Terminal IZVRŠAVA pasivnu autentikaciju kako bi potvrdio autentičnost PK_{PICC}.

3.4.2 Sigurnosni status

Ako je autentikacija čipa obavljena uspješno, sigurna razmjena podataka započinje ponovo

korištenjem izvedenih sesijskih ključeva K_{MAC} i K_{Enc}. U suprotnom, sigurna razmjena podataka nastavlja se korištenjem prethodno uspostavljenih sesijskih ključeva (putem PACE-a ili osnovne kontrole pristupa).

Napomena: Pasivna autentikacija MORA se obaviti u kombinaciji sa autentikacijom čipa. Samo nakon uspješne validacije odgovarajućeg elementa sigurnosti, čip mašinski čitljivog putnog dokumenta može se smatrati autentičnim.

Čip mašinski čitljivog putnog dokumenta (PICC)	Terminal (PCD)
Statički par ključeva (SK_{PICC}, PK_{PICC}, D_{PICC}) PK PICC D PICC ‹$\widetilde{PK_{PCD}}$ K =**KA** (SK $_{PICC}$, $\widetilde{PK_{PCD}}$, D $_{PICC}$)	Odabrati nasumičan kratkotrajni par ključeva ($\widetilde{SK_{PCD}}$, $\widetilde{PK_{PCD}}$, D $_{PICC}$) K =**KA** ($\widetilde{SK_{PCD}}$, PK $_{PICC}$, D $_{PICC}$)

Slika 2: Autentikacija čipa Verzija 1

Specifikacija protokola 3

Čip mašinski čitljivog putnog dokumenta (PICC)	Terminal (PCD)
Odabrati nasumično r_{PICC} $\underline{r_{PICC}}$ ‹Spcd **Potvrditi (** PK $_{PCD}$, s $_{PCD}$, ID $_{PICC}$ ||r $_{PICC}$ ||**Comp**($\widetilde{PK_{PCD}}$))	s $_{PCD}$ =**Sign** ($\widetilde{SK\ PCD}$, $\widetilde{ID\ PICC}$ ||r $_{PICC}$||Comp PKpcd

3.5 Autentikacija terminala verzija 1

Protokol za autentikaciju terminala predstavlja protokol izazov-odgovor iz dva poteza koji omogućava eksplicitnu jednostranu autentikaciju terminala.

Ovaj protokol omogućava čipu mašinski čitljivog putnog dokumenta da potvrdi da li je terminal ovlašten da pristupi osjetljivim podacima. Budući da terminal može naknadno pristupiti osjetljivim podacima, sva dalja komunikacija MORA se zaštititi na odgovarajući način. Prema tome, autentikacijom terminala obavlja se i autentikacija kratkotrajnog javnog ključa koji terminal odabere, a koji je korišten za uspostavljanje sigurne razmjene poruka kod autentikacije čipa. Čip mašinski čitljivog dokumenta MORA uvezati pristupna prava terminala za sigurnu razmjenu poruka uspostavljenu putem autentičnog kratkotrajnog javnog ključa terminala.
U ovom protokolu ID_{PICC} predstavlja identifikator čipa mašinski čitljivog putnog dokumenta:

- Ukoliko se koristi *osnovna kontrola pristupa*, ID_{PICC} je broj dokumenta čipa mašinski čitljivog putnog dokumenta koji se nalazi u mašinski čitljivoj zoni

uključujući i kontrolni znak.

• Ako se koristi PACE, ID_{PICC} se izračunava korištenjem kratkotrajnog javnog ključa čipa mašinski čitljivog putnog dokumenta za PACE, odnosno ID_{PICC} =**Comp** ($\widetilde{PK_{PICC}}$). Ovo se naziva *dinamičko uvezivanje.*

Obratite pažnju da su neke države izdale mašinski čitljive putne dokumente korištenjem *statičkog uvezivanja* za kombinovanje PACE-a i autentikacije terminala, gdje ID_{PICC} predstavlja:

• broj dokumenta čipa mašinski čitljivog putnog dokumenta koji se nalazi u mašinski čitljivoj zoni uključujući i kontrolni znak, ako je mašinski čitljiva zona upotrijebljena kao lozinka za PACE, ili

• CAN, ako je CAN upotrijebljen kao lozinka.

Ukoliko je autentikacija terminala putem dinamičkog uvezivanja neuspješna, inspekcijski sistemi TREBA da pokušaju pristupiti dokumentu putem statičkog uvezivanja. Statičko uvezivanje se NE SMIJE koristiti kod novoizdatih dokumenata.

Napomena: Sve poruke MORAJU se prenijeti putem sigurne razmjene poruka, tako da se prvo izvrši enkripcija, a potom autentikacija korištenjem sesijskih ključeva izvedenih putem *osnovne kontrole pristupa* ili PACE-a.

3.5.1 Specifikacija protokola

Terminal i čip mašinski čitljivog putnog dokumenta obavljaju sljedeće korake, a pojednostavljena verzija predstavljena je na slici 3.

1. Terminal šalje lanac certifikata čipu mašinski čitljivog putnog dokumenta. Lanac počinje certifikatom koji se može potvrditi putem javnog ključa CVCA pohranjenog na čipu i završava sa certifikatom terminala.
2. Čip mašinski čitljivog putnog dokumenta potvrđuje certifikate i izvodi javni ključ terminala PK_{PCD}.
3. Čip mašinski čitljivog putnog dokumenta nasumično bira izazov r_{PICC} i šalje ga terminalu.
4. Terminal odgovara potpisom
   s_{PCD}=**Sign** (SK_{PCD}, ID_{PICC}||r_{PICC}||**Comp** ($\widetilde{PK_{PCD}}$)) .
5. 5. Čip mašinski čitljivog putnog dokumenta provjerava da li je
   Verify (PK_{PCD}, s_{PCD}, ID_{PICC}||r_{PICC}||**Comp** ($\widetilde{PK_{PCD}}$))= ISTINITO .

Napomena: U verziji 1, autentikacija čipa se MORA obaviti prije autentikacije terminala, odnosno **Comp** (PK_{PCD}) izračunava i čip i terminal mašinski čitljivog putnog dokumenta kao dio autentikacije čipa.

3.5.2 Sigurnosni status

Ukoliko je autentikacija terminala uspješno obavljena, čip mašinski čitljivog putnog dokumenta DODIJELJUJE pristup pohranjenim osjetljivim podacima u skladu sa važećim ovlašćenjem terminala za koji se vrši autentikacija. Međutim, čip mašinski čitljivog putnog dokumenta OGRANIČAVA pristupna prava terminala za sigurnu razmjenu poruka uspostavljenu preko autentičnog kratkotrajnog javnog ključa, odnosno, čip mašinski čitljivog putnog dokumenta UPOREĐUJE kompresovanu sliku kratkotrajnog javnog

ključa terminala primljenu kao dio procesa autentikacije terminala sa kompresovanom slikom kratkotrajnog javnog ključa koju terminal osigurava kao dio procesa autentikacije čipa. Čip mašinski čitljivog putnog dokumenta NE SMIJE prihvatiti više od jednog izvršenja autentikacije terminala u okviru iste sesije (vidi Poglavlje "Sigurna razmjena poruka" u dijelu 3 ovog Tehničkog uputstva koje se odnosi na definiciju "sesije").

Napomena: Autentikacija terminala ne utiče na sigurnu razmjenu poruka. Čip mašinski čitljivog putnog dokumenta ČUVA sigurnu razmjenu poruka, čak i u slučaju da se autentikacija terminala ne obavi uspješno (osim ukoliko se ne pojavi greška vezana za sigurnu razmjenu poruka).

A. OSNOVNA KONTROLA PRISTUPA (Informativno)

Protokol za *osnovnu kontrolu pristupa* određuje ICAO [2], [3]. *Osnovna kontrola pristupa* provjerava da li terminal ima fizički pristup stranici sa podacima mašinski čitljivog putnog dokumenta. Ovo se obavlja tako što se od terminala traži da izvede ključ za autentikaciju iz *optički* čitljive mašinski čitljive zone putnog dokumenta. Protokol za *osnovnu kontrolu pristupa* zasnovan je na Standardu ISO/IEC 11770-2 [6] koji se odnosi na mehanizam za uspostavljanje ključa 6. Ovaj protokol se koristi i za generisanje sesijskih ključeva koji se upotrebljavaju za zaštitu povjerljivosti (i integriteta) podataka koji se prenose.

A.1. Osnovni pristupni ključevi dokumenta

Ključeve za osnovni pristup dokumentu KB_{Enc} i KB_{MAC} pohranjene na radiofrekvencijskom čipu u sigurnoj memoriji, mora izvesti terminal iz mašinski čitljive zone putnog dokumenta prije pristupanja radiofrekvencijskom čipu. Prema tome, terminal optički očita mašinski čitljivu zonu i generiše ključeve za osnovni pristup dokumentu primjenom ICAO KDF [2], [3] na najznačajnijih 16 bajta SHA-1 [7] heša nekih polja mašinski čitljive zone. Budući da je optičko očitavanje mašinski čitljive zone sklono greškama, za generisanje osnovnih pristupnih ključeva koriste se samo polja zaštićena kontrolnim znakovima: broj dokumenta, datum rođenja i datum važenja. Posljedica toga je da autentikacioni ključ ima relativno nisku entropiju. Stvarna entropija uglavnom zavisi od vrste broja dokumenta. Za putne dokumente koji važe 10 godina, **maksimalna** jačina autentikacionog ključa je približno:

- 56 bita za numerički broj dokumenta ($365^2 \cdot 10^{12}$ mogućnosti)
- 73 bita za alfanumerički broj dokumenta ($365^2 \cdot 36^9 \cdot 10^3$ mogućnosti)

Ova procjena, naročito u drugom slučaju, zahtijeva da se broj dokumenta bira nasumice i na jedinstven način. Zavisno od nivoa znanja napadača, stvarna entropija ključeva za osnovni pristup dokumentu može biti niža, npr. ako napadač poznaje sve brojeve dokumenata koji su u upotrebi ili je u mogućnosti da odredi vezu između broja dokumenta i datuma prestanka važnosti dokumenta.
Uzmemo li u obzir da je u prvom slučaju maksimalna entropija (56 Bit) relativno niska, moguće je izračunavanje autentikacionog ključa iz praćene sesije. S druge strane, to i dalje zahtijeva više truda nego da se isti (manje osjetljivi) podaci dobiju iz drugih izvora.

A.2. Specifikacija protokola

Osnovna kontrola pristupa prikazana je na slici 4. Radi boljeg očitavanja, enkripcija i autentikacija
poruka kombinuju se u jedinstvenu autentikacionu osnovnu funkciju enkripcije:

$\mathbf{EM}(K, S) = \mathbf{E}(KB_{Enc}, S) \,||\, \mathbf{MAC}(K_{MAC}, \mathbf{E}(KB_{Enc}, S))$, gdje je $K = \{KB_{Enc}, KB_{MAC}\}$.

Odgovarajuća operacija **DM** (*K, C*) definisana je analogno, odnosno kao verifikacija i dekripcija.

1. Čip mašinski čitljivog putnog dokumenta šalje terminalu jednokratno r_{PICC} .
2. Terminal šalje čipu mašinski čitljivog putnog dokumenta kriptovani izazov $e_{PCD} = \mathbf{EM}(K, r_{PCD} || r_{PICC} || K_{PCD})$, gdje je r_{PICC} jednokratna upotreba čipa mašinski čitljivog dokumenta, r_{PCD} predstavlja nasumično odabranu jednokratnu

upotrebu terminala, a K_{PCD} predstavlja materijal ključa za generisanje sesijskih ključeva.

3. Čip mašinski čitljivog putnog dokumenta obavlja sljedeće:

a) Dešifruje primljeni izazov u $r_{PCD}||r_{PICC}||K_{PCD} = \mathbf{DM}(K, e_{PCD})$ i potvrđuje da je $r'_{PICC} = r_{PICC}$

b) b) Šalje odgovor u vidu kriptovanog izazova $e_{PICC} = \mathbf{EM}(K, r_{PICC}||r_{PCD}||K_{PICC})$, gdje je

c) r_{PICC} jednokratna upotreba čipa mašinski čitljivog putnog dokumenta, a K_{PICC} predstavlja materijal ključa za generisanje sesijskih ključeva.

4. Terminal dešifruje kriptovani izazov u $r_{PICC}||r_{PCD}||K_{PICC} = \mathbf{DM}(K, e_{PICC})$ i potvrđuje da je $r''_{PCD} = r_{PCD}$.

5. Nakon uspješne autentikacije, sva dalja komunikacija MORA se zaštititi putem sigurne razmjene poruka, tako da se prvo izvrši enkripcija, a potom autentikacija korištenjem sesijskih ključeva K_{Enc} and K_{MAC} izvedenih u skladu sa [2], [3] zajedničke master tajne $K_{Master} = K_{PICC} \oplus K_{PCD}$ i brojača slanja sekvenci izvedenog iz r_{PICC} and r_{PCD}.

B. Semantički upiti (Informativno)

Razmotrimo potpis zasnovan na protokolu upit-odgovor između čipa i terminala mašinski čitljivog putnog dokumenta, gdje čip želi dokazati poznavanje svog privatnog ključa SK_{PICC}:

1. Terminal šalje čipu mašinski čitljivog putnog dokumenta nasumično odabran upit c.

2. Čip mašinski čitljivog putnog dokumenta odgovara potpisom s=**Sign** (SK_{PICC}, c) .

Budući da se radi o veoma jednostavnom i efikasnom protkolu, čip mašinski čitljivog putnog dokumenta u stvari potpisuje poruku c bez poznavanja samog semantičkog sadržaja poruke. Pošto potpisi pružaju prenosiv dokaz autentičnosti, bilo koje treće lice, u principu, može biti uvjereno da je čip mašinski čitljivog putnog dokumenta zaista potpisao tu poruku.

Iako c treba biti nasumičan niz bitova, terminal može generisati taj niz bitova na nepredvidiv način koji je moguće (javno) verifikovati, npr. dopustiti da SK_{PCD} bude privatni ključ terminala i da c=**Sign** (SK_{PCD} , ID_{PICC} ||Date||Time||Location) bude upit generisan korištenjem šeme potpisa sa mogućnošću oporavka poruke. Potpis garantuje da je terminal zaista generisao ovaj upit. Zahvaljujući prenosivosti potpisa terminala, bilo koje treće lice koje ima povjerenja u terminal i poznaje odgovarajući javni ključ PK_{PCD} može provjeriti putem verifikacije ovog potpisa da li je upit ispravno kreiran. Osim toga, zahvaljujući prenosivosti potpisa čipa mašinski čitljivog putnog dokumenta na upit, treće lice može zaključiti da je tvrdnja postala istinita: čip mašinski čitljivog putnog dokumenta zaista je u određeno vrijeme, određenog dana bio na određenoj lokaciji.

Pozitivna strana je da države mogu koristiti semantički upit za svoju internu upotrebu, npr. da dokažu da je određena osoba zaista imigrirala. Dok je negativna strana to što se ovakvi dokazi mogu zloupotrijebiti za praćenje ljudi. Zloupotreba je moguća zbog toga što aktivna autentikacija nije ograničena samo na ovlašćene terminale. Najgori scenario bili bi čipovi mašinski čitljivih putnih dokumenata koji pružaju aktivnu autentikaciju bez osnovne kontrole pristupa. U tom slučaju, mogao bi se uspostaviti veoma moćan sistem praćenja tako što bi se sigurni moduli hardvera smjestili na istaknuta mjesta. Rezultirajući logovi ne mogu se falsifikovati zahvaljujući potpisu. Osnovna kontrola pristupa umanjuje ovaj problem u određenoj mjeri, budući da je neophodna interakcija sa nosiocem dokumenta. Ipak, problem i dalje ostaje, ali je ograničen na mjesta gdje se putni dokument nosioca svakako očitava, npr. aviokompanije, hoteli, itd.

Možda izgleda da je, naročito kada je u pitanju beskontaktni scenario, upit moguće pratiti i ponovo upotrijebiti u neko drugo vrijeme, na drugom mjestu ili lokaciji i tako učiniti dokaz u najmanju ruku nepouzdanim. Budući da je praćenje upita tehnički moguće, argument, ipak, nije valjan. Pretpostavka je da se radi o terminalu za koji se može vjerovati da ispravno proizvodi upite i za koji se vjeruje da je provjerio identitet čipa mašinski čitljivog putnog dokumenta prije nego što je započeo proces aktivne autentikacije. Stoga, praćeni upit će sadržati identitet drugačiji od identiteta onoga koji dokazuje i potpisuje upit.