Техничко упутство

Напредни сигурносни механизми за машински читљиве путне документе

Дио 1 – Електронски машински читљиви путни документи (eMRTD) sa BAC/PACEv2 i EACv1

Бања Лука, 01.03.2013. године

Sadržaj

1. Увод

Систем електронских докумената је развијен на бази докумената Њемчког института за IT и IDDEEA се захваљује на доступности докумената на званичним сајтовима BSI.

Међународна организација цивилне авијације (ICAO) стандардизује машински читљиве путне документе у Документу 9303 ICAO. Овај стандард састоји се из три дијела:

Дио 1: Машински читљиви пасоши

• Поглавље 1: Пасоши са машински читљивим подацима похрањеним у формат оптички препознатљивих знакова

• Поглавље 2: Спецификације за електронски оспособљене пасоше са способношћу биометријске идентификације

Дио 2: Машински читљиве визе

Дио 3: Машински читљиви званични путни документи

• Поглавље 1: Званични путни документи са машински читљивим подацима похрањеним у формат оптички препознатљивих знакова

• Поглавље 2: Спецификација електронски оспособљених званичних путних докумената са способношћу биометријске идентификације

Ова техничка смјерница углавном се фокусира и детаљније описују безбједносне механизме за електронске путне документе описане у Документу 9303 Дио 1 Поглавље 2 [2] и Документ 9303, Дио 3 Поглавље 2 [3] како би се заштитила аутентичност (укључујући и интегритет), оригиналност и повјерљивост података похрањених на радиофреквенцијском чипу уграђеном у путни документ. Укратко, безбиједносни механизми наведени у [2], [3], [4] су: пасивна аутентикација, активна аутентикација и контрола приступа (тј. основна контрола приступа - BAC и успостављање везе преко аутентикације лозинком-PACE), како је дато у Табели 1.

Механизам	Заштита	Криптографска техника
Пасивна	Аутентичнос	Дигитални потпис
Активна	Оргиналност	Упит-договор
Контрола приступа	Повјерљивос	Аутентификација и безбједни

Табела 1: Безбиједносни механизми ICAO-а

Примјена активне аутентикације и контроле приступа је опционог карактера, док је пасивна аутентикација обавезна. Из тога директно слиједи да се без примјене ових или еквивалентних механизама, оригиналност и повјерљивост похрањених података не може гарантовати. Ово упутство је фокусирано на те аспекте и одређује додатне

механизме за аутентикацију и контролу приступа који су важни за безбједан чип машински читљивог путног документа.

1.1 Пасивна аутентикација

Апликација за електронске пасоше ICAO-а у основи обухвата 16 група података (ДГ1-ДГ16) и објекат безбједности документа за пасивну аутентикацију. Преглед коришћења ових група података дат је у табели 3.

За пасивну аутентикацију користи се дигитални потпис како би се извршила аутентикација података похрањених у групама података на чипу машински читљивог путног документа. Тај потпис генерише потписник документа (нпр. произвођач машински читљивог путног документа) у фази персонализације чипа машински читљивог путног документа путем елемента безбједности документа који садржи хеш вриједности свих група података похрањених на чипу. За појединости везане за објекат безбједности документа, потписнике документа и кровно сертификационо тијело за издавање електронских путних докумената у држави, читалац се упућује на [2], [3].

Да би се потврдили подаци похрањени на чипу машински читљивог путног документа путем пасивне аутентикације, терминал мора извршити сљедеће:

1. Очитати објекат безбједности документа који се налази у чипу машински читљивог путног документа.
2. Преузети одговарајући сертификат за потписивање докумената, поуздан сертификат кровног сертификационог тијела за издавање електронских путних докумената у држави, и одговарајући списак опозваних сертификата.
3. Потврдити сертификат потписника документа и потпис елемента безбједности документа
4. Прорачунати хеш вриједности група података које се очитавају и упоредити их са хеш вриједностима у елементу безбједности документа.

Пасивна аутентикација омогућује терминалу да открије групе података којима се манипулише, али не спречава клонирање чипова машински читљивих путних докумената, тј. копирање свих података похрањених на једном чипу машински читљивог путног документа на други.

1.2 Активна аутентикација

А ктивна аутентикација је дигитална карактеристика безбједности која спречава клонирање увођењем пара кључева који је јединствен за сваки чип:

• Јавни кључ је похрањен у групи података ДГ15 и самим тим заштићен пасивном аутентикацијом.
• Одговарајући приватни кључ похрањен је у безбједној меморији и може се користити само унутар чипа машински читљивог путног документа и не може се очитати.

На тај начин, чип може доказати познавање тог приватног кључа путем протокола “изазов-одговор”, који се назива и активна аутентикација. У овом протоколу чип

машински читљивог путног документа дигитално потписује изазов који је терминал насумично изабрао. Терминал препознаје да је чип путног документа аутентичан ако, и само ако је повратни потпис исправан. Активна аутентикација представља директан протокол и веома ефикасно спречава клонирање, али уводи опасност за приватност: Семанитички упити (види Додатак Б за дискусију везану за Семантичке упите).

1.3 Контрола приступа

Контрола приступа није потребна само због питања приватности, већ умањује и ризик од покушаја клонирања. Чип који се налази на машински читљивом путном документу штити похрањене податке од неовлашћеног приступа кроз употребу одговарајућих механизама за контролу приступа као што је описано у наставку:

• Мање осјетљиви подаци (нпр. машински читљива зона, фотографија и други подаци које је релативно лако пронаћи из других извора) који су потребни за глобалну међуоперативност граничних прелаза заштићени су основном контролом приступа – BAC. За боље разумијевање читаоца, основна контрола приступа описана је у Додатку А.

• Да би се олакшала примјена, основна контрола приступа заснована је само на симетричној криптографији, чиме се јачина изведених сесијских кључева ограничава јачином уносних података, тј. одштампаном машински читљивом зоном. Због тога се уводи протокол – PACE (Успостављање конекције путем аутентикације лозинком). Овај протокол заснован је на асиметричној криптографији и обезбјеђује сесијске кључеве чија је јачина независна од ентропије уносних података. Када је у питању миграција, ICAO дефинише и додатну контролу приступа (види [4]), која захтијева да пасоши код којих се примијењује PACE, примијењују и основну контролу приступа.

• Осјетљиви подаци (нпр. отисак прста и други подаци до којих није једноставно доћи из других многобројних извора) морају бити доступни само овлашћеним терминалима. Такви подаци су додатно заштићени и проширеном контролом приступа.

Основна контрола приступа само провјерава да ли терминал има физички приступ путним документима тако што тражи оптичко очитање машински читљиве зоне. Проширена контрола приступа додатно провјерава да ли је терминал овлашћен да очитава осјетљиве податке. Према томе, захтијева се строга контрола терминала. Међутим, проширена контрола приступа се не тражи при глобалној међуоперативности граничних прелаза, ICAO још увијек није дефинисао овај протокол.

Успостављање конекције путем аутентикације лозинком (PACE) које се уводи у овој спецификацији може се користити као безбједнија и погоднија замјена за основну контролу приступа
.

1.4 Побољшања

У поређењу са претходним верзијама BSI докумената, ова верзија обухвата и сљедећа побољшања у области пасоша:

• Интеграција PACE у напредну инспекцијску процедуру.

• Екстензија безбједне размјене порука при аутентикацији чипа на AES. У цијелом овом дијелу Упутства, PACE се односи на PACEв2 као што је дефинисано у [4].

1.5 Услови за чипове и терминале машински читљивих путних докумената

У овим Техничким смјерницама наведени су услови за примјену чипова и терминал машински читљивих путних докумената. Док чипови машински читљивих докумената морају испуњавати услове у складу са терминологијом описаном у Дијелу 1.6,услови за терминале тумаче се као смјернице, тј. међуоперативност чипа и терминал машински читљивог путног документа може се гарантовати само уколико терминал испуњава те услове, у супротном интеракција са чипом ће или бити неуспјешна или ће понашање чипа бити недефинисано. У основи, чип машински читљивог путног документа не треба испуњавати услове везане за терминале осим ако безбједност чипа машински читљивог путног документа није директно угрожена.

1.6 Терминологија

К ључне ријечи: "МОРАТИ", "НЕ СМЈЕТИ", "ТРАЖИТИ", "ХТЈЕТИ", "НЕ ХТЈЕТИ", "ТРЕБАТИ, "НЕ ТРЕБАТИ", "ПРЕПОРУЧИТИ", "МОЋИ", И "ОПЦИОНО" у овом документу тумаче се као што је описано у РФЦ 2119 [1]. Кључна ријеч "УСЛОВЉЕНО" тумачи се на сљедећи начин:
УСЛОВЉЕНО: Употреба једне ставке зависи од употребе других ставки. Стога је даље одређено
под којим условима се та ставка ТРАЖИ или ПРЕПОРУЧУЈЕ.

Када се користе у табели (профилима), кључне ријечи се скраћују као што је наведено у табели 2.

Кључна ријеч		Skraćenic
МОРАТИ ХТЈЕТИ	ТРАЖИТИ	М
НЕ СМЈЕТИ НЕ ХТЈЕТИ	–	ц
ТРЕБАТИ	ПРЕПОРУЧИТИ	П
МОЋИ	ОПЦИОНО	О
–	УСЛОВЉЕНО	ц

Табела2. Кључне ријечи

2. Апликације за машински читљиве путне документе

У оквиру овог поглавља се налазе системи за машински читљиве путне документе

2.1 Апликација за елекронски пасош

Апликацију за електронски пасош дефинисао је ICAO [2], [3], [4], [5]. Да бисте очитали податке из апликације за електронски пасош, чип машински читљивог путног документа ТРЕБА захтијевати да се изврши аутентикација терминала као инспекцијског система. Различите аутентикацијске процедуре за апликацију за електронски пасош дате су на слици 1.

2.2 Инспекцијски систем

Инспекцијски сустем је службени терминал којим увијек управља владина организација (тј. домаћи или страни верификатор докумената). Чип машински читљивог путног документа ТРЕБА захтијевати од инспекцијског система да обави своју аутентикацију прије додјеле приступа у складу са актуелном ауторизацијом. Овај дио Техничког упутства дефинише двије алтернативе за аутентикацију терминала као инспекцијског система: стандардну инспекцијску процедуру и напредну инспекцијску процедуру.
За очитање апликације за електронски пасош која задовољава ИЦАО стандарде, МОРА се користити стандардна или напредна инспекцијска процедура (упореди Дио 2.4). У томе се огледа разлика између основног инспекцијског система и проширеног инспекцијског система.

• Основни инспекцијски систем: Терминал који користи стандардну инспекцијску процедуру како би обавио своју аутентикацију на чипу машински читљивог путног документа.

• Проширени инспекцијски систем: Терминал који користи процедуре напредне инспекције електронског пасоша.

Група података	Садржај	Очитати-исписат	Обавезно-опционио	Контрола приступа BAC/PACE	EAC v1
ДГ1	Машински читљива зона	Р	м	М	Ц
ДГ2	Биометриај лице	Р	М	М	ц
ДГ3	Биометрија-прст	Р	О	М	М
ДГ4	Биометрија-зјеница ока	Р	О	М	М
...		Р	О	М	О
ДГ14	Безбједоносне	Р	Ц	М	Ц
ДГ15	Активна аутентикација	Р	О	М	Ц
ДГ16	...	Р	О	М	Ц
CO_D	Објекат безбједности документа	Р	М	М	Ц

ДГ14 је дефинисана и Дијелу 3. Скраћенице (о,ц,р,м,х) дате су у табели 2.
Табела 3: Групе података за апликацију за електронски пасош

Основни инспекцијски систем овлашћен је само за приступ мање осјетљивим подацима који се налазе у апликацији за електронски пасош која задовољава стандард ИЦАО-а. Ниво овлашћења проширеног инспекцијског система ОДРЕДИЋЕ се актуелном ауторизацијом израчунатом из ланца сертификата.

2.3 Лозинке

Да бисте дозволили носиоцу машински читљивог путног документа да контролише приступ апликацијама спроведеним за бесконтактни чип, наведене су основна и проширена контрола приступа. Због ограничења основне контроле приступа, ова спецификација уводи PACE као сигуран и практичан механизам за ограничавање приступа апликацијама на основу знања, односно на основу лозинки које су или штампане на документу или су познате само легитимном носиоцу документа.
Док основна контрола приступа подржава само једну "лозинку", тј симетричан кључ изведен из машински читљиве зоне, протокол PACE подржава више лозинки. Различите врсте лозинки које се користе у овом дијелу спецификације су:

CAN: Број приступне картице (CAN) је кратка лозинка која је одштампана или приказана на документу. CAN представља лозинку која се не може блокирати, односно чип на машински читљивом путном документу НЕ СМИЈЕ блокирати CAN уколико аутентикација не успије. CAN може бити статички (одштампан на документу), полустатички (одштампан на наљепници документа) или динамички (насумично га одабере чип машински читљивог путног документа и прикаже на самом документу коришћењем нпр. електронског папира, OLED-а или сличних технологија).

MRZ: Лозинка за машински читљиву зону представља статички тајни кључ који не може бити блокиран, а који је изведен из машински читљиве зоне и може се користити и за PACE и за BAC.

Напомена: Будући да ово Техничко упутство не препоручује никакву одређену дужину лозинки, свака лозинка која се не може блокирати МОРА садржати довољну ентропију или машински читљив чип МОРА примијенити додатне противмјере за заштиту од бруталних удара. Противмјере МОГУ обухватити одлагања, али НЕ СМИЈУ блокирати лозинке након неисправних уношења.

2.4 Инспекцијске процедуре

. Зависно од тога да ли је уређај (односно, чип или терминал машински читљивог путног документа) у складу са овом спецификацијом, уређај називамо усклађеним или неусклађеним. Зависно од комбинације терминала и чипа машински читљивог путног документа, користи се или стандардна или напредна инспекцијска процедура:

• Неусклађени инспекцијски систем користи стандардну инспекцијску процедуру. Мање осјетљиви подаци похрањени на чипу МОРАЈУ бити читљиви на сваком неусклађеном инспекцијском систему

Инспекцијски систем	Чип машински читљивог путног	
	usklađeni	Неусклађени
Усклађени	Напредни	Стандардни
Неусклађени	стандардни	Стандардни

Табела 4: Инспекцијске процедуре

. • Усклађени инспекцијски систем КОРИСТИ напредну инспекцијску процедуру уколико је чип који се налази на машински читљивом документу усклађен. У супротном, користи се стандардна инспекцијска процедура.

Табела 4 даје преглед инспекцијских процедура које ће се користити.

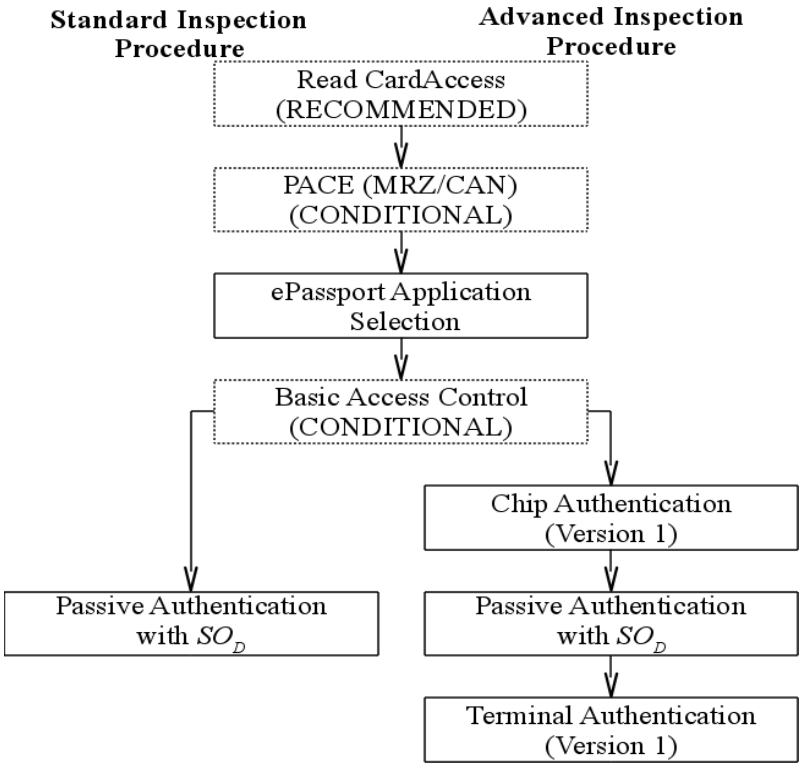
Терминал може користити или стандардну инспекцијску процедуре за приступ мање осјетљивим подацима који се налазе у апликацији за електронске пасоше или напредну инспекцијску процедуру за приступ мање осјетљивим и осјетљивим подацима који се налазе у апликацији за електронске пасоше.

За стандардну инспекцијску процедуру ПОТРЕБНО је да је машински читљива зона позната терминалу (будући да се основна контрола приступа ПРЕПОРУЧУЈЕ за чипове машински читљивих путних докумената). За напредну испекцијску процедуру МОРА бити позната или машински читљива зона или ЦАН.

Напомена: Као што је описано у Дијелу 1.1, пасивна аутентикација је континуиран процес који захтијева израчунавање хеш вриједности сваке групе података која се очита са чипа, као и њено поређење са одговарајућим хеш вриједностима елемента безбједности документа. Овај континуирани процес није експлицитно описан, будући да се претпоставља да ће бити примијењен у наредним процедурама

2.4.1 Отварање апликација за електронски пасош

Апликација за електронски пасош МОРА бити отворена као дио стандардне или напредне инспекцијске процедуре за електронске пасоше. Отварање апликације за електронске пасоше подразумијева одабир апликације за електронски пасош и извршавање контроле приступа како то захтијевају чип који се налази на машински читљивом путном документу, односно, основна контрола приступа или PACE.



Слика 1: Процедуре за аутентикацију у апликацији за електронски пасош

Уколико чип који се налази на машински читљивом путном документу то захтијева, МОРА се користити или PACE или основна контрола приступа. Уколико чип који се налази на машински читљивим путним документима подржава и PACE и основну контролу приступа, инспекцијски систем ТРЕБА користити PACE умјесто основне контроле приступа. Процедура отварања састоји се од сљедећих корака:

1. Читање CardAccess елементарне датотеке (ПРЕПОРУЧУЈЕ СЕ)

Терминал ТРЕБА покушати очитати елементарну датотеку CardAccess како би се одредили параметри (односно, симетричне цифре, кључни алгоритми слагања, параметри домена и мапирање) које подржава чип. Терминал може одабрати било који од ових параметара.
Уколико читање ове елементарне датотеке није могуће, терминал ТРЕБА покушати очитати електронски пасош путем основне контроле приступа.

2. PACE (УСЛОВЉЕНО)

Овај корак се ПРЕПОРУЧУЈЕ уколико чип машински читљивог документа подржава PACE. Чип ПРИХВАТА сљедеће лозинке за PACE:

• машински читљива зона (подршка чипа машински читљивог документа се ЗАХТИЈЕВА),
• CAN (подршка чипа машински читљивог документа је ОПЦИОНА).

Уколико се обави успјешно, чип машински читљивог документа радиће сљедеће:
• ЗАПОЧЕЋЕ безбједну размјену порука.

- ДОДИЈЕЛИЋЕ приступ мање осјетљивим подацима (нпр. ДГ1, ДГ2, ДГ14, ДГ15, итд. и елементу безбједности документа).
- ОГРАНИЧИЋЕ приступна права како би се захтијевала безбједна размјена података.

3. Одабрати апликацију за електронски пасош (ЗАХТИЈЕВА СЕ)

4. Основна контрола приступа (УСЛОВЉЕНО)

Овај корак се ЗАХТИЈЕВА ако контролу приступа тражи чип машински читљивог путног документа, а PACE није коришћен.

Уколико је контрола успјешно обављена, чип машински читљивог документа радиће сљедеће:

- ЗАПОЧЕЋЕ безбједну размјену порука.
- ДОДИЈЕЛИЋЕ приступ групи података ДГ14 (која садржи јавни кључ за аутентикацију чипа).
- ТРЕБА додијелити приступ мање осјетљивим подацима (нпр. ДГ1, ДГ2, ДГ15, итд. и елементу безбједности документа) .
- ОГРАНИЧИЋЕ приступна права како би се захтијевала безбједна размјена података.

2.4.2 Стандардна инспекцијска процедура

. Стандардна инспекцијска процедура може се користити за све апликације за електронски пасош које су усклађене са ICAO стандардима. Ако чип машински читљивог путног документа подржава и ПАЦЕ и основну контролу приступа, инспекцијски систем ЋЕ КОРИСТИТИ ПАЦЕ умјесто основне контроле приступа. Стандардна инспекцијска контрола састоји се из сљедећег:

1. Отварање апликације електронског пасоша
(ЗАХТИЈЕВА СЕ)

2. Пасивна аутентикација
(ЗАХТИЈЕВА СЕ)

Терминал МОРА очитати и потврдити објекат безбједности документа. Уколико је приступ картици учитан, терминал УПОРЕЂУЈЕ несигурне информације о безбједности које су очитане путем приступа картици са безбједним садржајем групе података бр. 14 (ДГ14).

3. Активна аутентикација
(ОПЦИОНО)

Уколико је то доступно, терминал МОЖЕ очитати и потврдити групу података бр. 15 (ДГ15) и извршити активну аутентикацију.

4. Очитати и извршити аутентикацију података

Терминал МОЖЕ очитати и потврдити групе података које садрже мање осјетљиве податке

2.4.3 Напредна инспекцијска процедура

. Процедура за напредну инспекцију може се користити само за апликације за електронски пасош које су у складу са ICAO/EAC1. Напредна инспекцијска процедура састоји се од сљедећег:

1. Отварање апликације електронског пасоша
(ЗАХТИЈЕВА СЕ)

2. Аутентикација чипа Верзија 1
(ЗАХТИЈЕВА СЕ)

Терминал ОЧИТАВА групу података (ДГ14) и обавља аутентикацију чипа. Чип машински читљивог путног документа ради сљедеће:
• ЗАПОЧИЊЕ поновну безбједну размјену порука.
• ДОДИЈЕЉУЈЕ приступ мање осјетљивим групама података (нпр. ДГ1, ДГ2, ДГ15, итд.. и објекат безбједности документа).
• ОГРАНИЧАВА приступна права како би се тражила безбједна размјена порука која се успоставља аутентикацијом чипа.

3. Пасивна аутентикација (започета)
(ЗАХТЈЕВА СЕ)

Терминал обавља сљедеће:

• ОЧИТАВА и ПОТВРЂУЈЕ објекат безбједности документа.
• ПОТВРЂУЈЕ групу података ДГ14. Уколико је очитан приступ картици, терминал УПОРЕЂУЈЕ несигурне информације о безбједности које су очитане путем приступа картици са безбједним садржајем групе података (ДГ14).

4. Активна аутентикација
(ОПЦИОНО)

Уколико је то доступно, терминал МОЖЕ очитати и потврдити групу података (ДГ15) и извршити активну аутентикацију.

5. Аутентикација терминала Верзија 1 (УСЛОВЉЕНО)

Овај корак се ЗАХТИЈЕВА за приступ осјетљивим подацима електронског пасоша. Уколико се обави успјешно, чип машински читљивог путног документа ради сљедеће:
• ДОДЈЕЉУЈЕ додатни приступ групама података према приступним правима за терминал.
• ОГРАНИЧАВА сва приступна права како би се тражила безбједна размјена порука која се успоставља аутентикацијом чипа и коришћењем краткотрајног јавног кључа чија се аутентикација обавља путем аутентикације терминала.

6. Очитавање и аутентикација података
Терминал МОЖЕ очитати и потврдити групе података у складу са приступним правима за терминал

3. Спецификације протокола

У овом поглављу криптографски протоколи за PACE, аутентикацију чипа и терминала одређени су под претпоставком произвољне комуникационе инфраструктуре. Мапирање за команде ISO 7816 дато је у поглављу 3 ових Техничких смјерница.

3.1 Криптографски алгоритми и симболи

Протоколи се извршавају између двије стране: чипа машински читљивог путног документа (PICC) и терминала (PCD). Табела 5 даје преглед коришћених парова кључева. Коришћене су сљедеће криптографске операције и симболи.

3.1.1 Компресиони и хеш алгоритми

Операције за израчунавање криптографског хеша и компресије јавног кључа описани су на алгоритамски независан начин.

3.1.1.1 Операције

• Операција за израчунавање хеша преко поруке m означена је као **H**(*m*).
• Операција за израчунавање компресоване слике јавног кључа означена је као **Comp**(*PK*).

3.1.2 Симетрични алгоритми кључа

Кључеви и операције за симетричну енкрипцију и аутентикацију кључева описани су на алгоритамски независан начин.

3.1.2.1 Кључеви

Симетрични кључеви изводе се из заједничког тајног K и ОПЦИОНОГ произвољног и једном употријебљеног p или из лозинке π коришћењем функције за извођење кључева (КДФ):
• Извођење кључа за енкрипцију порука означено је са $K_{Enc} = \mathbf{KDF}_{\mathbf{Enc}}(K, [r])$.
• Извођење кључа за аутентикацију поруке означено је као $K_{MAC} = \mathbf{KDF}_{\mathbf{MAC}}(K, [r])$.

Протокол	MRTD чип	Терминал	Напомена
Аутентикација чипа	PK_{PICC}, SK_{PICC}	$\widetilde{PK_{PCD}}$, $\widetilde{SK_{PCD}}$	Пар кључева који користи терминал представља тренутни пар кључева који се разликује од тренутног пара кључева за PACE.
Аутентикација терминала	PK_{CVCA}	PK_{PCD}, SK_{PCD}	Чип машински читљивог путног документа потврђује ланац сертификата које прими терминал коришћењем јавног кључа CVCA.

Табела 5: Преглед парова кључева који су употријебљени

3.1.2.2 Кључеви

За аутентикацију чипа, чип машински читљивог путног документа користи статички Diffie-Hellman пар кључева, а терминал генерише тренутни пар кључева на основу параметара статичког домена чипа машински читљивог путног документа D_{PICC}.

- Статички јавни кључ чипа машински читљивог путног документа је PK_{PICC}, а одговарајући приватни кључ је SK_{PICC}.
- Тренутни јавни кључ терминала је $\widetilde{PK}_{PCD}$, а одговарајући приватни кључ је $\widetilde{SK}_{PCD}$.
- Компресовани тренутни јавни кључ терминала означен је као **Comp** ($\widetilde{PK}_{PCD}$).

ПРЕПОРУЧУЈЕ СЕ да чип машински читљивог путног документа потврђује јавне кључеве које прими од терминала.

3.1.2.3 Операције

Операција за генерисање заједничког тајног кључа K означена је као K = KA □ SK , PK , D □, гдје је SK (тренутни или статички) тајни кључ, PK је (тренутни или статички) јавни кључ, а D су (тренутни или статички) параметри домена.

3.1.3 Потписи

Кључеви и операције за потписе описани су на алгоритамски независан начин. Мапирање за RSA i ECDSA дато је у поглављу 3 овог Техничког упутства.

3.1.3.1 Кључеви

Терминал за аутентикацију користи сљедећи кључ:

• Терминал има статички пар кључева за аутентикацију. Јавни кључ је PK_{PCD}, а одговарајући приватни кључ је SK_{PCD}.

3.1.3.2 Операције

Операције за потписивање и потврђивање порука одређене су на сљедећи начин:

• Потписивање поруке m приватним кључем SK_{PCD} s=**Sign** (SK_{PCD}, m).

• Потврђивање резултирајућег потписа с јавним **кључем** PK_{PCD} одређено је преко **Verify(**PK_{PCD},s,m) .

3.2 Основна контрола приступа

Основна контрола приступа објашњена је у [2]. За додатно информисање, спецификација и дискусија о ограничењима дати су у Додатку A.

3.3 PACE

Протокол PACE представља лозинком аутентификован Diffie-Hellman протокол за слагање кључева који пружа безбједну комуникацију и експлицитну аутентикацију засновану на чипу и терминалу машински читљивог документа (односно, чип и терминал машински читљивог документа дијеле исту лозинку).

Протокол успоставља безбједну размјену порука између чипа и терминала машински читљивог путног документа, која је заснована на слабим (кратким) лозинкама. PACE представља алтернативу основној контроли приступа, односно, омогућава чипу машински читљивог путног документа да потврди да је терминал овлашћен да приступи похрањеним мање осјетљивим подацима, али има и двије предности:

• Јаки сесијски кључеви обезбјеђени су независно од јачине лозинке.

• Ентропија лозинки које се користе за аутентикацију терминал може бити веома ниска (нпр. 6 знакова је у суштини довољно).

PACE је објашњен у поглављу [4]. За додатне информације, погледајте и поглавље 3 овог Техничког упутства.

3.4 Аутентикација чипа, верзија 1

Протокол за аутентикацију чипа представља краткотрајан статички Diffie-Hellman протокол за слагање кључева који обезбјеђује безбједну комуникацију и једнострану аутентикацију чипа машински читљивог путног документа.
Протокол успоставља безбједну размјену поруку између чипа и терминала машински читљивог путног документа заснованог на статичком пару кључева похрањеном у чипу машински читљивог документа. Аутентикација чипа представља алтернативу опционој активној аутентикацији ICAO-а, односно, омогућује терминалу да потврди да је чип машински читљивог путног документа аутентичан, и има двије предности над оригиналним протоколом:

• Спријечени су семантички упити, будући да транскрипте које произведе овај протокол није могуће преносити.
• Поред аутентикације чипа машински читљивог путног документа, овај протокол обезбјеђује и јаке сесијске кључеве. Детаљи везани за семантичке упите описани су у Додатку Б.

Протокол у својој верзији 1 путем безбједне размјене порука пружа имплицитну аутентикацију, како самог чипа, тако и података похрањених на њему уз употребу нових сесијских кључева.

3.4.1 Спецификација протокола

Сљедеће кораке обављају терминал и чип машински читљивог путног документа. Поједностављена верзија приказана је на слици 2.

1. Чип машински читљивог путног документа шаље терминалу свој статички Diffie-Hellman јавни кључ PK_{PICC}, и параметар домена D_{PICC}.
2. Терминал генерише краткотрајни Diffie-Hellman пар кључева ($\widetilde{SK_{PCD}}, \widetilde{PK_{PCD}}$, D_{PICC}) и шаље чипу машински читљивог путног документа краткотрајни јавни кључ $\widetilde{PK_{PCD}}$.
3. И чип и терминал машински читљивог путног документа израчунавају сљедеће:

a) Заједнички тајни K =**KA** (SK $_{PICC}$, $\widetilde{PK}_{PCD}$, D$_{PICC}$)=**KA** ($\widetilde{SK}_{PCD}$, PK $_{PICC}$, D$_{PICC}$)
b) Сесијске кључеве K_{MAC} =**KDF** $_{MAC}$ (K) и K_{Enc} =**KDF** $_{Enc}$ (K) изведене из K за безбједну размјену порука.
c) Компресовани краткотрајни јавни кључ терминала **Comp (**$\widetilde{PK}_{PCD}$**)** за аутентикацију терминала.

Терминал ИЗВРШАВА пасивну аутентикацију како би потврдио аутентичност PK_{PICC}.

3.4.2 Безбиједносни статус

Ако је аутентикација чипа обављена успјешно, безбједна размјена података започиње поново коришћењем изведених сесијских кључева K_{MAC} i K_{Enc}. У супротном, безбједна размјена података наставља се коришћењем претходно успостављених сесијских кључева (путем PACE-a или основне контроле приступа).

Напомена: Пасивна аутентикација МОРА се обавити у комбинацији са аутентикацијом чипа. Само након успјешне валидације одговарајућег елемента безбједности, чип машински читљивог путног документа може се сматрати аутентичним.

Чип машински читљивог путног документа (PICC)	Терминал (PCD)
Статички пар кључева (SK_{PICC}, PK_{PICC}, D_{PICC}) PK PICC D PICC —————— 〈$\widetilde{PK}_{PCD}$ K =**KA** (SK $_{PICC}$, $\widetilde{PK}_{PCD}$, D $_{PICC}$)	Одабрати насумичан краткотрајни пар кључева ($\widetilde{SK}_{PCD}$, $\widetilde{PK}_{PCD}$, D $_{PICC}$) K =**KA** ($\widetilde{SK}_{PCD}$, PK $_{PICC}$, D $_{PICC}$)

Слика 2: Аутентикација чипа Верзија 1

Спецификација протокола 3

Чип машински читљивог путног документа (PICC)	Терминал (PCD)
Одабрани насумично r_{PICC} $\underline{r_{PICC}}$ 〈Spcd **Потврдити (** 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 Аутентикација терминала верзија 1

Протокол за аутентикацију терминала представља протокол изазов-одговор из два

потеза који омогућује експлицитну једнострану аутентикацију терминала.

Овај протокол омогућава чипу машински читљивог путног документа да потврди да ли је терминал овлашћен да приступи осјетљивим подацима. Будући да терминал може накнадно приступити осјетљивим подацима, сва даља комуникација МОРА се заштитити на одговарајући начин. Према томе, аутентикацијом терминала обавља се и аутентикација краткотрајног јавног кључа који терминал одабере, а који је коришћен за успостављање безбједне размјене порука код аутентикације чипа. Чип машински читљивог документа МОРА увезати приступна права терминала за безбједну размјену порука успостављену путем аутентичног краткотрајног јавног кључа терминала.
У овом протоколу ID_{PICC} представља идентификатор чипа машински читљивог путног документа:

- Уколико се користи *основна контрола приступа*, ID_{PICC} је број документа чипа машински читљивог путног документа који се налази у машински читљивој зони укључујући и контролни знак.
- Ако се користи PACE, ID_{PICC} се израчунава коришћењем краткотрајног јавног кључа чипа машински читљивог путног документа за PACE, односно ID_{PICC}=**Comp** ($\widetilde{PK_{PICC}}$). Ово се назива *динамичко увезивање.*

Обратите пажњу да су неке државе издале машински читљиве путне документе коришћењем *статичког увезивања* за комбиновање PACE-a и аутентикације терминала, гдје ID_{PICC} представља:

- број документа чипа машински читљивог путног документа који се налази у машински читљивој зони укључујући и контролни знак, ако је машински читљива зона употријебљена као лозинка за PACE, или
- CAN, ako je CAN употријебљен као лозинка.

Уколико је аутентикација терминала путем динамичког увезивања неуспјешна, инспекцијски системи ТРЕБА да покушају приступити документу путем статичког увезивања. Статичко увезивање се НЕ СМИЈЕ користити код новоиздатих докумената.

Напомена: Све поруке МОРАЈУ се пренијети путем безбједне размјене порука, тако да се прво изврши енкрипција, а потом аутентикација коришћењем сесијских кључева изведених путем *основне контроле приступа* или PACE-a.

3.5.1 Спецификација протокола

Терминал и чип машински читљивог путног документа обављају сљедеће кораке, а поједностављена верзија представљена је на слици 3.

1. Терминал шаље ланац сертификата чипу машински читљивог путног документа. Ланац почиње сертификатом који се може потврдити путем јавног кључа CVCA похрањеног на чипу и завршава са сертификатом терминала.
2. Чип машински читљивог путног документа потврђује сертификате и изводи јавни кључ терминала PK_{PCD}.

3. Чип машински читљивог путног документа насумично бира изазов r_{PICC} и шаље га терминалу.
4. Терминал одговара потписом
$$s_{PCD} = \textbf{Sign}\ (SK_{PCD}, ID_{PICC} || r_{PICC} || \textbf{Comp}\ (\widetilde{PK_{PCD}}))\ .$$
5. 5. Чип машински читљивог путног документа провјерава да ли је
Verify (PK_{PCD}, s_{PCD}, ID_{PICC} ||r_{PICC} ||**Comp** $(\widetilde{PK_{PCD}})$)= ИСТИНИТО .

Напомена: У верзији 1, аутентикација чипа се МОРА обавити прије аутентикације терминала, односно **Comp** (PK_{PCD}) израчунава и чип и терминал машински читљивог путног документа као дио аутентикације чипа.

3.5.2 Безбиједносни статус

Уколико је аутентикација терминала успјешно обављена, чип машински читљивог путног документа ДОДИЈЕЉУЈЕ приступ похрањеним осјетљивим подацима у складу са важећим овлашћењем терминала за који се врши аутентикација. Међутим, чип машински читљивог путног документа ОГРАНИЧАВА приступна права терминала за безбједну размјену порука успостављену преко аутентичног краткотрајног јавног кључа, односно, чип машински читљивог путног документа УПОРЕЂУЈЕ компресовану слику краткотрајног јавног кључа терминала примљену као дио процеса аутентикације терминала са компресованом сликом краткотрајног јавног кључа коју терминал обезбјеђује као дио процеса аутентикације чипа. Чип машински читљивог путног документа НЕ СМИЈЕ прихватити више од једног извршења аутентикације терминала у оквиру исте сесије (види Поглавље “Безбједна размјена порука” у дијелу 3 овог Техничког упутства које се односи на дефиницију “сесије”).

Напомена: Аутентикација терминала не утиче на безбједну размјену порука. Чип машински читљивог путног документа ЧУВА безбједну размјену порука, чак и у случају да се аутентикација терминала не обави успјешно (осим уколико се не појави грешка везана за безбједну размјену порука).

A. ОСНОВНА КОНТРОЛА ПРИСТУПА (Информативно)

Протокол за *основну контролу приступа* одређује ICAO [2], [3]. *Основна контрола приступа* провјерава да ли терминал има физички приступ страници са подацима машински читљивог путног документа. Ово се обавља тако што се од терминала тражи да изведе кључ за аутентикацију из *оптички* читљиве машински читљиве зоне путног документа. Протокол за *основну контролу приступа* заснован је на Стандарду ISO/IEC 11770-2 [6] који се односи на механизам за успостављање кључа 6. Овај протокол се користи и за генерисање сесијских кључева који се употребљавају за заштиту повјерљивости (и интегритета) података који се преносе.

A.1. Основни приступни кључеви документа

Кључеве за основни приступ документу KB_{Enc} и KB_{MAC} похрањене на радиофреквенцијском чипу у безбједној меморији, мора извести терминал из машински читљиве зоне путног документа прије приступања радиофреквенцијском чипу. Према томе, терминал оптички очита машински читљиву зону и генерише кључеве за основни приступ документу примјеном ICAO KDF [2], [3] на најзначајнијих 16 бајта SHA-1 [7] хеша неких поља машински читљиве зоне. Будући да је оптичко очитавање машински читљиве зоне склоно грешкама, за генерисање основних приступних кључева користе се само поља заштићена контролним знаковима: број документа, датум рођења и датум важења. Посљедица тога је да аутентикациони кључ има релативно ниску ентропију. Стварна ентропија углавном зависи од врсте броја документа. За путне документе који важе 10 година, **максимална** јачина аутентикационог кључа је приближно:

- 56 бита за нумерички број документа ($365^2 \cdot 10^{12}$ могућности)
- 73 бита за алфанумерички број документа ($365^2 \cdot 36^9 \cdot 10^3$ могућности)

Ова процјена, нарочито у другом случају, захтијева да се број документа бира насумице и на јединствен начин. Зависно од нивоа знања нападача, стварна ентропија кључева за основни приступ документу може бити нижа, нпр. ако нападач познаје све бројеве докумената који су у употреби или је у могућности да одреди везу између броја документа и датума престанка важности документа.
Узмемо ли у обзир да је у првом случају максимална ентропија (56 Bit) релативно ниска, могуће је израчунавање аутентикационог кључа из праћене сесије. С друге стране, то и даље захтијева више труда него да се исти (мање осјетљиви) подаци добију из других извора.

A.2. Спецификација протокола

Основна контрола приступа приказана је на слици 4. Ради бољег очитавања, енкрипција и аутентикација
порука комбинују се у јединствену аутентикациону основну функцију енкрипције:

$$\mathbf{EM}(K, S) = \mathbf{E}(KB_{Enc}, S) \,||\, \mathbf{MAC}(K_{MAC}, \mathbf{E}(KB_{Enc}, S)), \text{ где је } K = \{KB_{Enc}, KB_{MAC}\}.$$

Одговарајућа операција **DM** (*K, C*) дефинисана је аналогно, односно као верификација и декрипција.

1. Чип машински читљивог путног документа шаље терминалу једнократно r

r_{PICC} .

2. Терминал шаље чипу машински читљивог путног документа криптовани изазов $e_{PCD} = \mathbf{EM}(K, r_{PCD}||r_{PICC}||K_{PCD})$, гдје је r_{PICC} једнократна употреба чипа машински читљивог документа, r_{PCD} представља насумично одабрану једнократну употребу терминала, а K_{PCD} представља материјал кључа за генерисање сесијских кључева.

3. Чип машински читљивог путног документа обавља сљедеће:

a) Дешифрује примљени изазов у $r_{PCD}||r_{PICC}||K_{PCD} = \mathbf{DM}(K, e_{PCD})$ и потврђује да је $r'_{PICC} = r_{PICC}$

b) Шаље одговор у виду криптованог изазова $e_{PICC} = \mathbf{EM}(K, r_{PICC}||r_{PCD}||K_{PICC})$, гдје је

c) r_{PICC} једнократна употреба чипа машински читљивог путног документа, а K_{PICC} представља материјал кључа за генерисање сесијских кључева.

4. Терминал дешифрује криптовани изазов у $r_{PICC}||r_{PCD}||K_{PICC} = \mathbf{DM}(K, e_{PICC})$ и потврђује да је $r''_{PCD} = r_{PCD}$.

5. Након успјешне аутентикације, сва даља комуникација МОРА се заштитити путем безбједне размјене порука, тако да се прво изврши енкрипција, а потом аутентикација коришћењем сесијских кључева K_{Enc} and K_{MAC} изведених у складу са [2], [3] заједничке master тајне $K_{Master} = K_{PICC} \oplus K_{PCD}$ и бројача слања секвенци изведеног из r_{PICC} and r_{PCD}.

Б. Семантички упити (Информативно)

Размотримо потпис заснован на протоколу упит-одговор између чипа и терминала машински читљивог путног документа, гдје чип жели доказати познавање свог приватног кључа SK_{PICC}:

1. Терминал шаље чипу машински читљивог путног документа насумично одабран упит c.

2. Чип машински читљивог путног документа одговара потписом $s = \mathbf{Sign}(SK_{PICC}, c)$.

Будући да се ради о веома једноставном и ефикасном протколу, чип машински читљивог путног документа у ствари потписује поруку c без познавања самог семантичког садржаја поруке. Пошто потписи пружају преносив доказ аутентичности, било које треће лице, у принципу, може бити увјерено да је чип машински читљивог путног документа заиста потписао ту поруку.

Иако c треба бити насумичан низ битова, терминал може генерисати тај низ битова на непредвидив начин који је могуће (јавно) верификовати, нпр. допустити да SK_{PCD} буде приватни кључ терминала и да $c = \mathbf{Sign}(SK_{PCD}, ID_{PICC} \| \text{Date} \| \text{Time} \| \text{Location})$ буде упит генерисан коришћењем шеме потписа са могућношћу опоравка поруке. Потпис гарантује да је терминал заиста генерисао овај упит. Захваљујући преносивости потписа терминала, било које треће лице које има повјерења у терминал и познаје одговарајући јавни кључ PK_{PCD} може провјерити путем верификације овог потписа да ли је упит исправно креиран. Осим тога, захваљујући преносивости потписа чипа машински читљивог путног документа на упит, треће лице може закључити да је тврдња постала истинита: чип машински читљивог путног документа заиста је у одређено вријеме, одређеног дана био на одређеној локацији.

Позитивна страна је да државе могу користити семантички упит за своју интерну употребу, нпр. да докажу да је одређена особа заиста имигрирала. Док је негативна страна то што се овакви докази могу злоупотријебити за праћење људи. Злоупотреба је могућа због тога што активна аутентикација није ограничена само на овлашћене терминале. Најгори сценарио били би чипови машински читљивих путних докумената који пружају активну аутентикацију без основне контроле приступа. У том случају, могао би се успоставити веома моћан систем праћења тако што би се безбједни модули хардвера смјестили на истакнута мјеста. Резултирајући логови не могу се фалсификовати захваљујући потпису. Основна контрола приступа умањује овај проблем у одређеној мјери, будући да је неопходна интеракција са носиоцем документа. Ипак, проблем и даље остаје, али је ограничен на мјеста гдје се путни документ носиоца свакако очитава, нпр. авиокомпаније, хотели, итд.

Можда изгледа да је, нарочито када је у питању бесконтактни сценарио, упит могуће пратити и поново употријебити у неко друго вријеме, на другом мјесту или локацији и тако учинити доказ у најмању руку непоузданим. Будући да је праћење упита технички могуће, аргумент, ипак, није ваљан. Претпоставка је да се ради о терминалу за који се може вјеровати да исправно производи упите и за који се

вјерује да је провјерио идентитет чипа машински читљивог путног документа прије него што је започео процес активне аутентикације. Стога, праћени упит ће садржати идентитет другачији од идентитета онога који доказује и потписује упит.