Техничко упутство

Напредни безбједоносни механизми за машински читљиве путне документе

Дио 3 – Опште спецификације

Бања Лука, 01.03.2013. године

Садржај

1 Увод

Овај дио Техничког упутства садржи опште спецификације које обухватају, како PKI која се користи за контролу приступа, тако и мапирање протокола за ASN.1 и APDU спецификације за протоколе дефинисане у дијеловима 1 и 2:

- Дио1:
  - Аутентификација терминала верзија 1
  - Аутентификација чипа верзија 1
- Дио 2:
  - Password Authenticated Connection Establishment (PACE)
  - Аутентификација чипа верзија 2
  - Аутентификација терминала верзија 2
  - Ограничена идентификација

Иако су спецификације за PACEv2 у[10]компатибилне са спецификацијама у овом документу, молимо погледајте [10] ради примјене PACE у складу са Дијелом 1.

Документи којима се примјењују само протоколи описани у дијелу 1 се у овом упутству називају „документи Дијела 1“, док се документи којима се примјењују протоколи из Дијела 2 или из оба дијела називају „документи Дијела 2“.

1.1 Захтјеви за чипове и терминале MRTD

Ово техничко упутство прописује захтјеве за примјене чипова и терминала MRTD. Док чипови MRTD морају задовољавати те захтјеве у складу са терминологијом која је описана у Одјељку 1.2, захтјеве за терминале треба посматрати као упутства, тј. међуоперативност чипова и терминала MRTD је загарантована једино уколико терминал задовољава те захтјеве, у супротном интеракција са чипом MRTD ће бити неуспјешна или ће понашање чипа MRTD бити недефинисано. У начелу, чип MRTD не мора проводити захтјеве у вези са терминалима, осим уколико је непосредно угрожена безбједност чипа MRTD.

1.2 Терминологија

Кључне ријечи „МОРА“, „НЕ СМИЈЕ“, „ОБАВЕЗНО“, „ЋЕ“ „НЕЋЕ“, „ТРЕБА“, „НЕ ТРЕБА“, „ПРЕПОРУЧЕНО“, „МОЖЕ“ и „ФАКУЛТАТИВНО“ у овом документу треба тумачити како је описано у RFC 2119 [2]. Кључну ријеч „УСЛОВНО“ треба тумачити како слиједи:

УСЛОВНО:Употреба неког предмета зависи од употребе других предмета. Зато се даље квалификује под којим условима је предмет ОБАВЕЗАН или ПРЕПОРУЧЕН.

Када се користе у табелама (профилима), кључне ријечи се скраћују, како је приказано у Табели 1.

Кључна ријеч	Скраћ.

МОРА/ ЋЕ	ОБАВЕЗНО	м
НЕ СМИЈЕ / НЕЋЕ	–	х
ТРЕБА	ПРЕПОРУЧЕНО	r
МОЖЕ	ФАКУЛТАТИВНО	о
–	УСЛОВНО	с

Табела 1: Кључне ријечи

1.3 Скраћенице

Слиједеће скраћенице ће бити коришћене у овој спецификацији.

Назив	Скраћеница
Бинарно кодирана цифра	BCD
Провјерљив помоћу картице	CV
Објекат безбједности картице/чипа	SOC
Сертификационо тијело	CA
Идентификатор чипа	ID PICC
Јавни кључ за аутентификацију чипа	PK PICC
Приватни кључ за аутентификацију чипа	SK PICC
Државно сертификационо тијело (CA) за	CSCA
Државно сертификационо тијело (CA) за	CVCA
Сертификат државног сертификационог	C CVCA
Објекат безбједности документа	SO D
Група података	DG
Верификатор докумената	DV
Сертификат верификатора докумената	C DV
Параметри домена	D
Привремени приватни кључ	SK
Привремени јавни кључ	PK
Hash функција	H
Међународна организација за цивилно	ICAO
Функција договора о кључу	KA
Функција извођења кључа	KDF
Логичка структура података	LDS
Машински читљива путна исправа	MRTD
Бесконтактни чип интегрисаног кола	PICC
Бесконтакни уређај за повезивање	PCD
Јавни кључ за ограничену идентификацију	PK ID
Приватни кључ за ограничену	SK ID
Јавни кључ за сектор	PK Sector
Приватни кључ за сектор	SK Sector
Секторски специфичан идентификатор	ID Sector
Јавни кључ за аутентификацију терминала	PK PCD
Приватни кључ за аутентивфикацију	SK PCD
Сертификат терминала	C T

2 Инфраструктура јавних кључева

Аутентификација терминала захтијева од терминала да докаже чипу MRTD да је

овлаштен да приступа осјетљивим подацима. Такав терминал је опремљен најмање једним *цертификатом терминала*, који декодира јавни кључ и права приступа терминала, и одговарајућим приватним кључем. Након што терминал докаже да зна тај приватни кључ, чип MRTD одобрава терминалу приступ осјетљивим подацима као што је назначено у цертификату терминала.

PKI која је неопходна за издавање и потврђивање цертификата терминала састоји се од слиједећих цјелина:

1. Државна цертификациона тијела за верификацију (CVCAs)
2. Верификатори докумената (DVs)
3. Терминали

Ова PKI чини основу проширене контроле приступа. Приказана је на Слици 1.

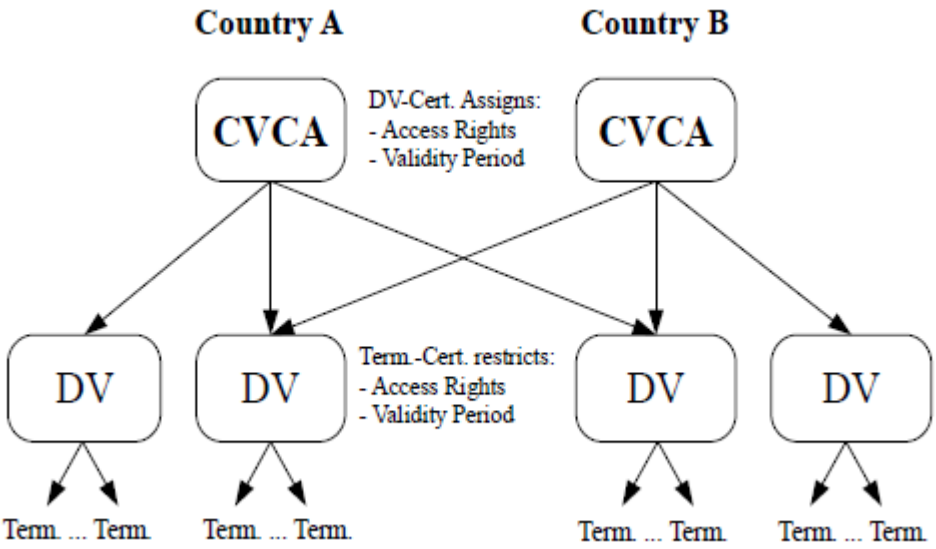
2.1 Државно цертификационо тијело за верификацију

Од сваке државе се захтијева да успостави једно повјерљиво мјесто које ће издавати цертификате верификатора докумената: *Државно цертификационо тијело за верификацију*(CVCA). Законом о Агенцији за идентификациона документа, евиденцију и размјену података Босне и Херцеговине (Службени глASNик БиХ 56/08) Агенција се практично дефинише као CVCA у Босни и Херцеговини.

Напомена: Државно цертификационо тијело за потписивањекоје издаје цертификате за потписнике докумената (в.[8],[9]) и Државно цертификационо тијело за верификацију МОГУ бити интегрисани у једну цјелину, односно у Државно цертификационо тијело.Међутим, чак и у том случају одвојени парови кључева се МОРАЈУ користити за различите улоге.

CVCA одређује права приступа националним чиповима MRTD за све DV (тј. званичне домаће DV, као и за стране/комерцијалне DV) издавањем цертификата за DV овлаштене за приступ неким осјетљивим подацима. Услови под којима CVCA одобрава DV приступ осјетљивим подацима су изван оквира овог документа и ТРЕБА да буду наведени у политици цертификације (в. Прилог Ц.5).

Цертификати верификатора докумената МОРАЈУ садржати информације као што је она о томе којим подацима је одређени DV овлаштен да приступа. Како би се умањио потенцијални ризик који могу изазвати изгубљени или украдени терминали цертификати верификатора докумената МОРАЈУ имати кратак период важења. Период важења одређује CVCA која издаје цертификат по сопственом избору и тај период важења може бити различит у зависности од верификатора докумената коме се исти издаје.



Слика 1: Инфраструктура јавних кључева

*Стрелице означавају цертификацију

2.2 Верификатори докумената

Верификатор докумената (DV) је организациона јединица која управља групом терминала (нпр. терминали којима рукује гранична полиција неке државе) на начин да, између осталог, издаје цертификате терминала. Верификатор докумената је стога CA које је овлаштено од стране барем националног CVCA да издаје цертификате за своје терминале. Цертификати терминала које изда верификатор докумената обично преузимају и права приступа и период важења цертификата верификатора докумената, премда верфикатор докумената МОЖЕ одлучити да даље **ограничи** права приступа или период важења у зависности од терминала за који је издат цертификат.

Уколико верификатор докумената захтијева да његови терминали приступају осјетљивим подацима похрањеним на чипу MRTD друге државе, он МОРА поднијети захтјев за DV цертификат који издаје CVCA одговарајуће државе. Верификатор докумената такође МОРА обезбиједити да се сви примљени цертификати верификатора докумената прослиједе теминалима у оквиру његовог подручја.

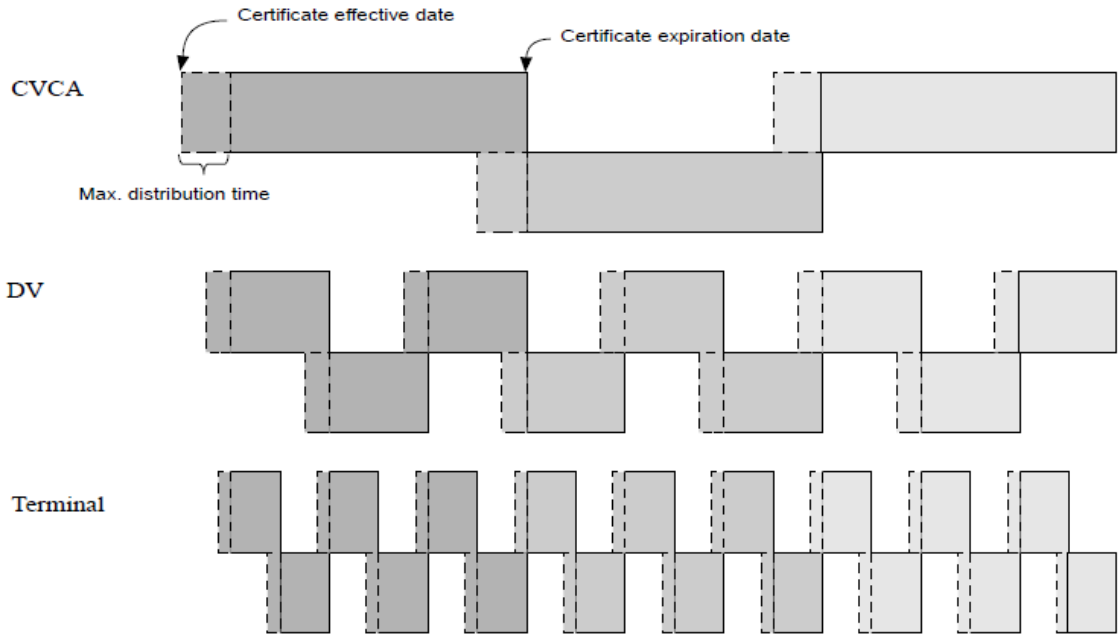
2.3 Цертификати провјерљиви помоћу картице

CVCA повезујући цертификати, DV цертификати и цертификати терминала су цертификати које треба да потврди чип MRTD. Због рачунарских ограничења тих чипова, цертификати МОРАЈУ бити у формату који се може провјерити картицом:

- Формат и профил цертификата спецификован у Прилогу Ц.1 ЋЕ бити кориштени.
- Алгоритам потписа, параметре домена и величину кључева који ће бити кориштени одређује CVCA државе која издаје, односно исти алгоритам потписа, параметри домена и величине кључева МОРАЈУ бити

употријебљени у једном ланцу цертификата[1].

- CVCA повезујући цертификати МОГУ укључивати јавни кључ који одступа од важећих параметара, односно CVCA МОЖЕ прећи на нови алгоритам потписа, нове параметре домена или величину кључева.



Слика 2: Распоређивање цертификата

2.4 Распоређивање цертификата

Сваки цертификат МОРА садржати период важења. Тај период важења се идентификује преко два датума, *датума почетка важења цертификата* и *датума истека важења цертификата.*

Датум почетка важења цертификата: Датум почетка важења цертификата ЋЕ бити датум генерисања цертификата.

Датум истека важења цертификата: Датум истека важења цертификата ЋЕ бити датум *након* кога истиче важење цертификата. Њега по сопственом нахођењу може одредити издавач цертификата.

Приликом генерисања цертификата, издавач МОРА пажљиво планирати промјене цертификата, пошто се МОРА обезбиједити довољно времена за преношењецертификата и успостављање ланца цертификата. Очигледно, нови цертификат мора бити генерисан прије истека актуелног цертификата. Добијено *максимално вријеме расподјеле* једнако је разлици датума истека старог цертификата и датума почетка важења новог цертификата. За употребу и дистрибуцију

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

цертификата се ПРЕПОРУЧУЈУ комуникациони протоколи наведени у TR-03129[4]. Распоређивање цертификата је приказано на слици 2.

2.5 Потврђивање цертификата

Чип MRTD мора посједовати ланац цертификата који почиње са повјерљивим мјестом похрањеним у чипу MRTD, како би се могло извршити потврђивање цертификата терминала. Таква повјерљива мјеста су мање или више нови јавни кључеви CVCA чипа MRTD. Почетно/а повјерљиво/а мјесто/а ЋЕ бити безбједно похрањено/а у меморији чипа MRTD у фази производње или (пред)персонализације.

Пошто се пар кључева који користи CVCA током времена мијења, морају се стварати повезујући цертификати CVCA. Чип MRTD ОБАВЕЗНО интерно ажурира своје/а повјерљиво/а мјесто/а у складу са важећим повезујућим цертификатима које добија.

Напомена:У складу са распоређивањемповезујућих цертификата CVCA (в. слику 2), највише два повјерљива мјеста по апликацији треба да буду похрањена у чипу MRTD.

Чип MRTD МОРА прихватити повезујући цертификат CVCA који је истекао, али НЕ СМИЈЕ прихватити цертификат терминала или DV који је истекао. Чип MRTD ЋЕ користити свој *текући датум* како би се одредило да ли је цертификат истекао.

Текући датум: Уколико чип MRTD не посједује интерни часовник, текући датум ЋЕ бити приближно одређен на начин који је описан у наставку. Текући датум похрањен у чипу MRTD у почетку представља датум (пред)персонализације. Тај датум се затим независно приближно одређује од стране чипа MRTD користећи најновији датум почетка важења цертификата који је садржан у важећем повезујућем цертификату CVCA, цертификату DV или *Ажуран цертификат терминала*.

Ажуран цертификат терминала: Цертификат терминала је ажуран уколико је чип MRTD повјерио издавачу верификатору докумената да производи цертификате терминала са тачним датумом почетка важења.

Терминал МОЖЕ послати повезујуће цертификате CVCA, цертификате DV и цертификате терминала чипу MRTD како би се ажурирао текући датум и повјерљиво мјесто похрањено у чипу MRTD чак и уколико терминал не намјерава или није у стању да настави аутентификацију терминала.

Напомена: Чип MRTD потврђује само да је цертификат *привидно* нов (тј. у односу на приближно одређен текући датум).

2.5.1 Општи поступак

Поступак потврђивања цертификата се састоји од два корака:

1. **Провјера цертификата:** Потпис МОРА бити важећи, те уколико се не ради о повезујућем цертификату CVCA, цертификат НЕ СМИЈЕ бити истекао. Уколико је провјера неуспјешна, поступак ЋЕ бити прекинут.
2. **Интерно ажурирање статуса:**Текући датум МОРА бити *ажуриран*, јавни кључ и атрибути (укључујући релевантне екстензије цертификата) МОРАЈУ бити увезени, нова повјерљива мјеста МОРАЈУ бити *оспособљена*,повјерљива мјеста која су истекла МОРАЈУ бити *онеспособљена* за провјеру цертификата DV.

Операција *ажурирања* текућег датума и операција *оспособљавања* и

онеспособљавања повјерљивог мјеста МОРА бити проведена као атомска операција.

Оспособљавање повјерљивог мјеста: Ново повјерљиво мјесто ЋЕ бити додато на списак повјерљивих мјеста.

Онеспособљавање повјерљивог мјеста: Повјерљива мјеста која су истекла НЕ СМИЈУ бити кориштена за провјеру цертификата DV, али МОРАЈУ остати употребљива за провјеру повезујућег цертифката CVCA. Онеспособљена повјерљива мјеста МОГУ бити избрисана након успјешног увоза наредног повезујућег цертификата.

2.5.2 Примјер поступка

Слиједећи поступак потврђивања, који се наводи као примјер, МОЖЕ се користити за потврђивање ланца цертификата. Чип MRTD проводи слиједеће кораке за сваки добијени цертификат:

1. Чип MRTD провјерава потпис на цертификату. Уколико је потпис неисправан, провјера ће бити неуспјешна.
2. Уколико цертификат није повезујући цертификат CVCA, датум истека важења цертификата се упоређује са текућим датумом чипа MRTD. Уколико је датум истека важења цертификата прије текућег датума, провјера ће бити неуспјешна.
3. Цертификат је прихваћен као важећи и увозе се јавни кључ и атрибути (укључујући релевантне екстензије цертификата) садржани у цертификату.

   а)За CVCA, DV, и Ажуран цертификат терминала: Датум почетка важења цертификата се упоређује са текућим датумом чипа MRTD. Уколико је текући датум прије датума почетка важења, текући датум се ажурира на датум почетка важења.

   б)За повезујући цертификат CVCA: Нови јавни кључ CVCA се додаје на списак повјерљивих мјеста који је безбједно похрањен у меморији чипа MRTD. Ново повјерљиво мјесто је тиме оспособљено.

   ц)За цертификате DV или терминала: Нови јавни кључ DV или терминала се привремено увози ради потврђивања цертификата које ће услиједити, односно ради аутентификације терминала.
4. Повјерљива мјеста која су истекла, а која су безбједно похрањена у меморији чипа MRTD су онеспособљена за потврђивање цертификата DV и могу се уконити са списка повјерљивих мјеста.

2.6 Ефективна ауторизација

Сваки цертификат ће садржати *Certificate Holder Authorization Template* (в. ПрилогЦ.1.5.) који идентификује тип терминала (в. Дио1 и 2 овог техничког упутства) и одређује *релативну ауторизацију* влASНика цертификата коју додјељује цертификационо тијело које издаје цертификат. Да би се одредила *ефективна ауторизација* влASНика цертификата чип MRTD МОРА на нивоу бита израчунати Булово „и“ релативне ауторизације које је садржано у цертификату терминала, референтном цертификату верификатора докумената и референтном цертификату CVCA.

2.6.1 Ограничена ауторизација (Само документи Дијела 2)

Ефективна ауторизација се даље може ограничити коришћењем Општег поступка аутентификације (в. Дио 2 овог тхеничког упутства). У том случају терминал МОРА назначити тип терминала и *ограничену ауторизацију* (односно ефективну ауторизацију коју захтијева терминал) као дио PACE протокола. За израчунавање ефективне ауторизације чип MRTD ЋЕ укључити ограничену ауторизацију израчунавањем Буловог „и“ на нивоу бита.

Напомена:Чип MRTD МОРА потврдити да су тип терминала назначен у ограниченој ауторизацији и тип терминала у релативној ауторизацији сваког цертификата у ланцу цертификата једнаки. Уколико се открије неслагање, чип MRTD ЋЕ вратити права приступа на почетне вриједности и указати на грешку (в. Прилог Б.11.7.).

2.6.2 Тумачење (сви типови докумената)

Чип MRTD ЋЕ тумачити ефективну ауторизацију на слиједећи начин:

- Ефективна улога је CVCA:
  - Повезујући цертификат је издало државноCVCA.
  - Чип MRTD МОРА ажурирати своје интерно повјерљиво мјесто, односно јавни кључ и ефективну ауторизацију.
  - Издавач цертификата представља повјерљив извор времена и чип MRTD МОРА ажурирати своје текуће вријеме користећи вријеме почетка важења цертификата.
  - Чип MRTD НЕ СМИЈЕ одобрити CVCA приступ осјетљивим подацима (тј. ефективну ауторизацију ТРЕБА занемарити).
- Ефективна улога је DV:
  - Цертификат је издало државно CVCA за овлаштеног DV.
  - Издавач цертификата представља повјерљив извор времена и чип MRTD МОРА ажурирати своје текуће вријеме користећи вријеме почетка важења цертификата.
  - Чип MRTD НЕ СМИЈЕ одобрити DV приступ осјетљивим подацима (тј. ефективну ауторизацију ТРЕБА занемарити).
- Ефективна улога је Терминал:
  - Цертификат је издао званични домаћи или страни, или пак незванични DV.
  - Уколико цертификат представља исправан цертификат терминала (в. Одјељак 2.5), тијело која га је издало је повјерљив извор времена и чип MRTD МОРА ажурирати своје текуће вријеме користећи датум почетка важења цертификата.
  - Чип MRTD МОРА аутентификованом терминалу одобрити приступ осјетљивим подацима у складу са ефективном ауторизацијом.

Важећи цертификат терминала МОРА бити прихваћен као исправан од стране чипа MRTD уколико га је издао званичан домаћи DV, а у супротном НЕ ТРЕБА бити прихваћен као исправан.

2.7 Сектор терминала за ограничену идентификацију

Терминалима се МОРА назначити сектор терминала како би била подржана ограничена идентификација терминала. Сектор терминала ЋЕ бити садржан у цертификату терминала и сходно томе ПРЕПОРУЧЕНО је да сектор терминала генерише верификатор докумената који врши цертификацију. У сваком случају, сектор терминала НЕ СМИЈЕ бити одабран од стране самог терминала.

Сектор терминала је увијек јавни кључ. Он МОЖЕ бити изабран било насумичним одабиром са непознатим приватним кључем, како би се потпуно онемогућило праћење (у том случају повезивање секторски специфичних идентификатора између различитих сектора је рачунарски немогуће) или као пар кључева како би се омогућио опозив заснован на секторски специфичним идентификаторима.

2.7.1 Пар кључева за сектор

Пар кључева за сектор мора бити генерисан од стране свих верификатора докумената који подржавају секторски специфичан опозив чипова MRTD.

Сваки верификатор докумената ЋЕ провести слиједеће кораке за сваки од субординисаних сектора:

1. Генерисати нови пар кључева за сектор на основу јавног кључа сектора за опозив.
2. Безбједно похранити приватни кључ за сектор (код верификатора докумената).
3. Укључити јавни кључ за сектор у сваки цертификат терминала за све терминале који припадају одговарајућем сектору.

Пар кључева сектора за опозив ЋЕ бити генрисан од стране CVCA. CVCA МОЖЕ делегирати услугу опозива добављачу услуга.

2.7.2 Секторски специфичан опозив чипова MRTD

Пар кључева за ограничену идентификацију ЋЕ бити генерисан приликом (пред)персонализације чипа MRTD. Приватни кључ ЋЕ бити похрањен у чипу MRTD, јавни кључ ЋЕ бити похрањен у бази података заједно са другим подацима помоћу којих се идентификује носилац MRTD.

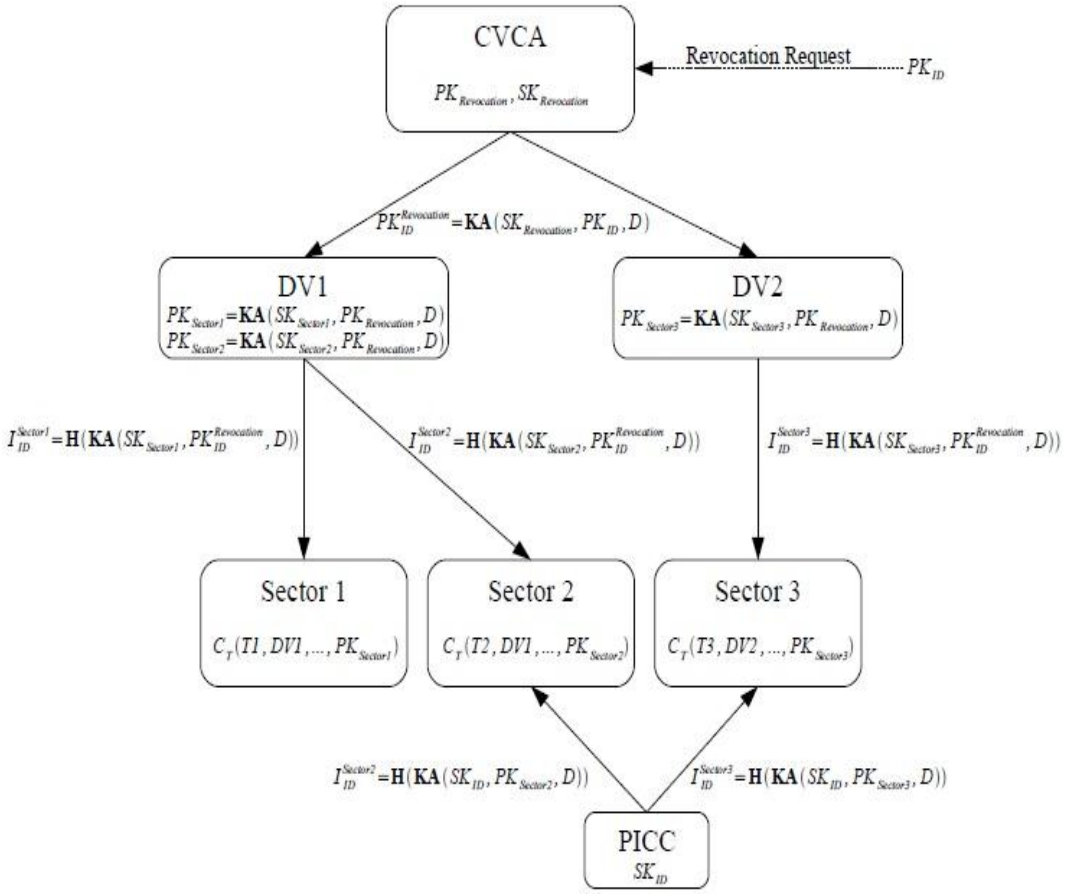
Напомена: Генерисање пара кључева за ограничену идентификацију МОЖЕ бити проведено у чипу MRTD или екстерно. Пар кључева МОРА бити изабран тако да буде јединствен и МОЖЕ бити или специфичан за чип или за носиоца (тј. исти пар кључева ће се користити за наредне чипове MRTD). Барем један пар кључева који се користи за ограничену идентификацију МОРА бити специфичан за чип.

Да би се опозвао чип MRTD, јавни кључ чипа MRTD који је специфичан за чип се претражује у бази података и преноси до CVCA. CVCA затим трансформише јавни кључ користећи његов приватни кључ сектора за опозив. Трансформисани јавни кључ се затим преноси свим суборинисаним верификаторима докумената. Сваки

верификатор докумената израчунава секторски специфичне идентификаторе користећи приватне кључеве за сектор за све субординисане секторе терминала. Коначно, секторски специфичан идентификатор се преноси до свих терминала одговарајућег сектора.

2.7.3 Генерисање листа опозваних цертификата

CVCA објављује јавни кључ сектора за опозив $PK_{Revocation}$ и параметре домена D. Сваки верификатор докумената насумице бира приватни кључ за сектор SK_{Sector} за сваки субординисани сектор и израчунава јавни кључ за сектор као PK_{Sector}=**КА** (SK_{Sector},$PK_{Revocation}$,D).



Слика 3: Опозив

Да би се опозвао чип MRTD упућује се захтјев CVCA за опозив који садржи јавни кључ за ограничену идентификацијуPK_{ID}. Секторски специфични идентитети се

израчунавају на слиједећи начин:

1. CVCA израчунава $PK^{Revocation} = \mathbf{KA}(SK_{Revocation}, PK\ ID, D)$ користећи приватни кључ $SK_{Revocation}$ и јавни кључ за ограничену идентификацију $PK\ ID$ који је добијен уз захтјев за опозив. Трансформисани јавни кључ *PK ID Revocation*се прослиједјује свим верификаторима докумената.

2. Сваки верификатор докумената израчунава секторски специфичан идентификатор за све субординисане секторе.За сваки сектор верификатор докумената израчунава

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

користећи одговарајући приватни кључ за сектор SK_{Sector}и добијени јавни кључ $PK_{ID}^{Revocation}$ чипа MRTD који треба да буде опозван. Секторски специфичан идентификатор I_{ID}^{Sector} се затим прослиједјује терминалима одговарајућег сектора.

2.7.4 Период важења

За разлику од пара кључева терминала (за аутентификацију терминала), пар кључева за сектор је важећи дуго времена и МОРА се изабрати на одговарајући начин.

2.7.5

2.7.6 Миграција терминала

Како би се извршила миграција терминала од једног верификатора докумената према другом верификатору докумената, пар кључева терминала за сектор МОРА се на безбједан начин пренијети до новог верификатора докумената.

Напомена: Миграција терминала до новог верификатора докумената није могућа под надзором другог CVCA.

A. ASN.1Спецификације (Норматив)

Идентификатори објекта кориштени у слиједећим прилозима садржани су у подстаблубси-де:

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

A.1. Информација о подржаним безбједносним протоколима

Структура података ASN.1 `SecurityInfos` ЋЕ бити обезбијеђена од стране чипа MRTD како би се назначили подржани безбједносни протоколи. Структрура података је специфицирана на слиједећи начин:

```
SecurityInfos ::= SET OF SecurityInfo

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

Елементи садржани у `SecurityInfos` структуре података имају слиједеће значење:

- Идентификатор објекта `protocol` идентификује подржавани протокол.
- `requiredData` отвореног типа садржи обавезне податке специфичне за протокол.
- `optionalData` отвореног типа садржи факултативне податке специфичне за протокол.

A.1.1. Подржани протоколи

Спецификације ASN.1за протоколе садржане у овој спецификацији описане су у наставку текста.

Напомена:Чипови MRTD имплементирани у складу са Верзијом 1.0.x ове спецификације ће обезбиједити само `ChipAuthenticationPublicKeyInfo`.

У том случају терминал ТРЕБА да претпостави слиједеће:

- Чип MRTD подржава аутентификацију чипа у верзији 1.
- Чип MRTD може подржавати аутентификацију терминала у верзији 1.

Да би се одредило да ли су осјетљиви подаци заштићени аутентификацијом терминала похрањени у чипу MRTD или не терминал може консултовати објекат безбједности документа и основни фајл EF.CVCA.

A.1.1.1. PACE

Да би се указало на подршку за PACE SecurityInfos може садржати слиједеће ставке:

- МОРА постојати најмање један `PACEInfo` који користи стандардизован параметар домена.
- За сваки подржани сет експлицитних параметара домена МОРА постојати `PACEDomainParameterInfo`

PACEInfo: Ова структура података пружа детаљне информације о примјени PACE.

- Идентификатор објекта `protocol` ЋЕ идентификовати алгоритме који ће бити кориштени (тј. договор о кључу, симетрично шифровање и MAC).
- Интегрална `version`ЋЕ идентификовати верзију протокола. Верзија 1 је застарјела и ПРЕПОРУЧЕНО је да се користи само верзија 2.
- Интегрални `parameterId`се користи да се назначи идентификатор параметра домена. Он МОРА бити употријебљен уколико чип MRTD користи стандардизоване параметре домена (в. Табелу 4) или обезбјеђује вишеструке експлицитне параметре домена за 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-CMAЦ-128         OBJECT IDENTIFIER ::= {id-PACE-DH-GM 2}
id-PACE-DH-GM-AES-CBC-CMAЦ-192         OBJECT IDENTIFIER ::= {id-PACE-DH-GM 3}
id-PACE-DH-GM-AES-CBC-CMAЦ-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-CMAЦ-128       OBJECT IDENTIFIER ::= {id-PACE-ECDH-GM 2}
id-PACE-ECDH-GM-AES-CBC-CMAЦ-192       OBJECT IDENTIFIER ::= {id-PACE-ECDH-GM 3}
id-PACE-ECDH-GM-AES-CBC-CMAЦ-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-CMAЦ-128         OBJECT IDENTIFIER ::= {id-PACE-DH-IM 2}
id-PACE-DH-IM-AES-CBC-CMAЦ-192         OBJECT IDENTIFIER ::= {id-PACE-DH-IM 3}
id-PACE-DH-IM-AES-CBC-CMAЦ-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-CMAЦ-128       OBJECT IDENTIFIER ::= {id-PACE-ECDH-IM 2}
id-PACE-ECDH-IM-AES-CBC-CMAЦ-192       OBJECT IDENTIFIER ::= {id-PACE-ECDH-IM 3}
id-PACE-ECDH-IM-AES-CBC-CMAЦ-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-CMAЦ-128 |
id-PACE-DH-GM-AES-CBC-CMAЦ-192 |
id-PACE-DH-GM-AES-CBC-CMAЦ-256 |
id-PACE-ECDH-GM-3DES-CBC-CBC |
id-PACE-ECDH-GM-AES-CBC-CMAЦ-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:Ова структура података обезбјеђује један сет експлицитних параметара домена за PACE за чип MRTD.

- Идентификатор објекта `protocol`ЋЕ идентификовати тип параметара домена(тј.DH или ECDH).
- Секвенца `domainParameter` ЋЕ садржати параметре домена.
- Интегрални `parameterId` МОЖЕ бити кориштен да се назначи локални идентификатор параметра домена.

МОРА се користити уколико чип MRTD обезбјеђује вишеструке експлицитне параметре домена за 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. Аутентификација чипа

Да би се указало на подршку за аутентификацију чипа `SecurityInfos` може садржати слиједеће ставке:

- МОРА постојати најмање један`ChipAuthenticationPublicKeyInfo`.
- МОРА постојати најмање један `ChipAuthenticationInfo`.
- МОРА постојати најмање један `ChipAuthenticationDomainParameterInfo`за аутентификацију чипа у верзији 2.

Уколико постоји више од једног јавног кључа за аутентификацију чипа, факултативни `keyId` МОРА бити употријебљен у све три структуре података како би се назначио локални идентификатор кључа. Сви јавни кључеви МОРАЈУ имати различите параметре домена.

ChipAuthenticationInfo:Ова структура података пружа детаљне информације о примјени аутентификације чипа.

- Идентификатор објекта `protocol`ЋЕ идентификовати алгоритме који ће бити кориштени (тј. договор о кључу, симетрично шифровање и MAC).
- Интегрална `version`ЋЕ идентификовати верзију протокола. Тренутно су

подржане верзије 1 и 2.

- Интегрални `keyId` се МОЖЕ користити да се назначи локални идентификатор кључа. Он се МОРА користити уколико чип MRTD обезбјеђује више јавних кључева за аутентификацију чипа.

```
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:Ова структура података пружа један сет експлицитних параметара домена за верзију 2 аутентификације чипа за чип MRTD.

- Идентификатор објекта `protocol`ЋЕ идентификовати тип параметара домена(тј.DH или ECDH).
- Секвенца `domainParameter` ЋЕ садржати параметре домена.
- Интегрални `keyId` МОЖЕ бити кориштен да се назначи локални идентификатор кључа. Он се МОРА користити уколико чип MRTD обезбјеђује више јавних кључева за аутентификацију чипа.

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

ChipAuthenticationPublicKeyInfo:Ова структура података обезбјеђује јавни кључ за аутентификацију чипа за чип MRTD.

- Идентификатор објекта `protocol`ЋЕ идентификовати тип јавног кључа (тј.DH или ECDH).
- Секвенца `chipAuthenticationPublicKey` ЋЕ садржати јавни кључ у кодираном облику.

- Интегралниkeyld МОЖЕ бити кориштен да се назначи локални идентификатор кључа. Он се МОРА користити уколико чип MRTD обезбјеђује више јавних кључева за аутентификацију чипа.

```
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.Аутентификација терминала

Да би се назначила подршка за аутентификацију терминала SecurityInfos може садржати слиједећу ставку:

- ТРЕБА да постоји најмање један TerminalAuthenticationInfo.

TerminalAuthenticationInfo:Ова структура података пружа детаљне информације о имплементацији аутентификације терминала.

- Идентификатор објекта protocol ЋЕ идентификовати општи протокол за аутентификацију терминала, пошто се специфични протокол може промијенити с временом.
- Интегрални version ЋЕ идентификовати верзију протокола. Тренутно су подржане верзије 1 и 2.
- Секвенца efCVCA се МОЖЕ користити у верзији 1 да се назначи (кратки) идентификатор фајла за фајл EF.CVCA. Она се МОРА користити уколико се не употребљава подразумијевани (кратки) идентификатор фајла.

```
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

Да би се назначила подршка за ограничену идентификацију `SecurityInfos` може садржати слиједећу ставку:

- МОРА постојати Најмање један `RestrictedIdentificationInfo`.
- МОЖЕ постојати највише један RestrictedIdentificationDomainParameterInfo.

RestrictedIdentificationInfo:Ова структура података пружа детаљне информације о имплементацији ограничене идентификације.

- Идентификатор објекта protocol ЋЕ идентификовати алгоритме који ће бити кориштени (тј. договор о кључу).
- Интегрални version ЋЕ идентификовати верзију протокола. Тренутно је подржана само верзија 1.
- Интегрални keyId ЋЕ идентификовати приватни кључ који ће се користити.
- Булов authorizedOnly ЋЕ индиковати да ли је ОБАВЕЗНА експлицитна ауторизација да би се користио одговарајући тајни кључ.
- Интагрални maxKeyLen се МОЖЕ користити да би се назначила максимална дужина подржаних кључева специфичних за сектор.

```
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:Ова структура података обезбјеђује сет параметара домена који су кориштени за генерисање јавног кључа *PK ID* за опозив чипа MRTD.

- Идентификатор објекта `protocol`ЋЕ идентификовати тип параметара домена (тј.DH или ECDH).
- Секвенца `domainParameter` ЋЕ садржати параметре домена.

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

A.1.1.5. CardInfoLocator(Само документи Дијела 2)

Да би се обезбиједиле информације о могућностима и структури картице`SecurityInfos` може садржати слиједећу ставку:

- ТРЕБА да постоји тачно један `CardInfoLocator`.

CardInfoLocator:Ова структура података пружа детаљне информације о томе гдје се преузима CardInfo file [5].

- Низ `url`ЋЕ дефинисати локацију која обезбјеђује најновији CardInfo file за одговарајући тип и верзију MRTD.
- Секвенца `efCardInfo` МОЖЕ се користити да се назначи (кратки) идентификатор фајла 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(Само документи Дијела 2)

Да би се заштитили подаци похрањени у eID апликацији `SecurityInfos` може садржати слиједећу ставку:

- ТРЕБА да постоји тачно један `eIDSecurityInfo`.

eIDSecurityInfo:Ова структура података обезбјеђује hash вриједности изабране групе података eID апликације.

- Секвенца `eIDSecurityObject` ЋЕ дефинисати hash вриједности изабраних група података
- Секвенца `eIDVersionInfo` МОЖЕ се користит да се идентификује верзија eID-апликације.

```
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 (само документи дијела 2)

Како би се добиле додатне информације о кључевима аутентификације чипа ограничене привилегованим терминалима, `SecurityInfos` могу садржавати сљедећи унос:

- Тачно један `PrivilegedTerminalInfo` МОРА постојати ако су неки кључеви аутентификације чипа доступни само привилегованим терминалима.

PrivilegedTerminalInfo : Ова структура података пружа `SecurityInfos` везане за аутентификацију чипа користећи индивидуалне кључеве чипа који су доступни само привилегованим терминалима.

- Сет `PrivilegedTerminalInfo` ЋЕ обухватити `SecurityInfos` према кључевима аутентификације чипа који су доступни само привилегованим терминалима.

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

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

A.1.1.8. Други протоколи

`SecurityInfos` МОГУ садржавати референце за протоколе који нису садржани у овој спецификацији (укључујући активну аутентификацију и основну контролу приступа).

Назив фајла	EF.CardAccess	EF.Card Security	EF.ChipSecurity
ФајлИД	0x011Ц	0x011Д	0x011Б
Кратки фајлИД	0x1Ц	0x1Д	0x1Б
Приступ очитавања	УВИЈЕК	PACE (m) + TA[IS, AT, ST] (o)	PACE+TA[IS or *privileged* AT]
Приступ уписа	НИКАДА	НИКАДА	НИКАДА
Величина	промјењиво	промјењиво	промјењиво
Садржај	DER кодирани SecurityInfos	DER кодирани SignedData	DER кодирани SignedData

Табела 2 : Основни фајлови приступ картице, сигурност картице и сигурност чипа

A.1.2. Меморија чипа

MRTD ЋЕ пружити `SecurityInfos` у сљедећим транспарентним основним фајловима садржаним у мастер фајлу (види табелу 2):

- CardAccess (УСЛОВЉЕНО)

  ЋЕ бити ако је у чипу имплементиран PACE, аутентификација чипа верзија 2 и/или аутентификација терминал верзија 2. БИЋЕ читљив са свих терминала.

- Card Security (УСЛОВЉЕНО)

  ЋЕ бити ако је чип имплементирао аутентификацију чипа верзија 2, аутентификација терминал верзија 2 или ограничену идентификацију. Приступ очитавања Card Security ЋЕ бити ограничена терминалима који су успјешно имплементирали PACE и МОГУ бити и даље ограничени аутентификованим терминалима

- ChipSecurity
  (ОПЦИОНАЛНО)

  Приступ очитавања ChipSecurity ЋЕ бити ограничен аутентификованим привилегованим терминалима. Ако је тај опционални фајл доступан, сви релевантни приватни `SecurityInfos` ТРЕБАЈУ бити сачувани на ChipSecurity и НЕ ТРЕБАЈУ бити укључени у Card Security.

Ако су PACE према[10],аутентификација терминала верзија 1 или аутентификација чипа имплементирани, MRTD чип ће обезбједити `SecurityInfos` у елементарном фајлу DG14 садржаном у апликацији еПасош.

A.1.2.1. CardAccess (УСЛОВЉЕНО)

Ако постоји, CardAccess ће садржавати релевантне `SecurityInfos` које су потребне за приступ апликацијама:

- PACEInfo (ЗАХТЈЕВАНО)
- PACEDomainParameterInfo (УСЛОВЉЕНО)
  - Ова структура (е) МОРА постојати ако се користе експлицитни параметри домена.
- ChipAuthenticationInfo (УСЛОВЉЕНО)
  - Ова структура МОРА постојати ако је подржана аутентификација чипа у верзији 2 и приступ очитавања Card Security је ограничен аутентификованим терминалима.
- ChipAuthenticationDomainParameterInfo (УСЛОВЉЕНО)
  - Ова структура МОРА постојати ако је подржана аутентификација чипа у верзији 2 и приступ очитавања Card Security је ограничен аутентификованим терминалима.
- TerminalAuthenticationInfo (УСЛОВЉЕНО)
  - Ова структура МОРА постојати ако је подржана аутентификација терминал у верзији 2.
- CardInfoLocator (ПРЕПОРУЧЕНО)
- PrivilegedTerminalInfo (УСЛОВЉЕНО)
  - Ова структура мора постојати ако неки су кључеви аутентификације чипа у верзији 2 доступни само привилегованим терминалима и приступ очитавања Card Security је ограничен аутентификованим терминалима.
  - Ова структура ЋЕ обухватити одговарајуће `SecurityInfos` , односно за сваки кључ аутентификације чипа који је ограничен привилегованим терминалима, ChipAuthenticationInfo и

ChipAuthenticationDomainParameterInfo МОРАЈУ бити укључени тако да повезују идентификатор кључа.

A.1.2.2. Card Security(УСЛОВЉЕНО)

Ако постоји, фајл Card Security:

- ЋЕ садржавати потписан SecurityInfos који MRTD чип подржава.
- ЋЕ садржавати све SecurityInfos садржане у CardAccess осим PrivilegedTerminalInfo ,
- ако су неки кључеви аутентификације чипа верзија 2 доступни само привилегованим терминалима а ниједан PrivilegedTerminalInfo није садржан у CardAccess, Card Security ЋЕ садржавати PrivilegedTerminalInfo, које обухватају одговарајуће SecurityInfos ,
- ЋЕ садржавати одговарајући ChipAuthenticationPublicKeyInfo за сваки кључ који ChipAuthenticationInfo повезује (искључујући кључеве повезане у PrivilegedTerminalInfo).

Генерисани специфични кључеви се ТРЕБАЈУ користити умјесто кључева индивидуалног чипа.

ПРЕПОРУЧУЈЕ се да се `eIDSecurityInfo` не користи у овом фајлу.

A.1.2.3. ChipSecurity(ОПЦИОНАЛНО)

Ако постоји, фајл Card Security ЋЕ садржавати:

- потписане `SecurityInfos` које MRTD чип подржава,
- све `SecurityInfos` садржане у CardAccess, и
- одговарајућиChipAuthenticationPublicKeyInfo за сваки кључ који ChipAuthenticationInfo повезује. Одговарајући ChipAuthenticationPublicKeyInfo МОРА такође бити укључен у PrivilegedTerminalInfo . Сви кључеви повезани у PrivilegedTerminalInfo ТРЕБАЈУ бити кључеви индивидуалног чипа.

ПРЕПОРУЧЕНО је да се `eIDSecurityInfo` користи како би обезбједиле hash -ове (статичних) група податак везаних за личне податке носиоца.

A.1.2.4. еПасош DG14 (УСЛОВЉЕНО)

Ако чип имплементира PACE према [10], аутентификацију терминала верзија 1 или аутентификација чипа верзија 1, MRTD чип ЋЕ такође обезбједити `SecurityInfos` у групи података DG 14 апликације еПасош. ПРЕПОРУЧЕНО је да DG14 и ChipSecurity (ако постоји) садрже исте кључеве.

A.1.2.5. Формат потписа за Card Securityи ChipSecurity

Фајлови Card Security и ChipSecurity ЋЕ бити имплементиране као `SignedData` према [7] са типом садржаја `SecurityInfos` . Потписник

документа ЋЕ потписати објекте безбједности. Цертификат потписника документа МОРА бити укључен у `SignedData`. Сљедећи идентификатори објекта ЋЕ се користити за идентификацију типа садржаја:

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

Структура податакаSignedData је дефинисана у наставку; више детаља се може пронаћи у [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
}
```

Алгоритам/ Формат	DH	ECDH
Алгоритам за договор кључева	PKCS#3 [27]	ECKA [3]
X.509Формат јавног кључа	X9.42 [1]	ECC [3]
TLV Формат јавног кључа	TLV, cf. Appendix D.3.2	TLV, cf. Appendix D.3.3
Компресија јавног кључа	SHA-1 [23]	X-Coordinate
Потврђивање привременог јавног кључа	RFC 2631 [26]	ECC [3]

Табела 3: Алгоритми и формати за договор кључева

```
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. Договор кључева

PACE, аутентификација чипа и ограничена идентификација се базирају на протоколима договора кључева. Овај додатак одређује опште алгоритме, формате и протоколе.

A.2.1. Параметри домена

Са изузетком параметра домена садржаним у `PACEInfo`, сви параметри домена ЋЕ бити дати као `AlgorithmIdentifier` , структура података је дефинисана на сљедећи начин; више детаља се може пронаћи у [6]:

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

Са `PACEInfo`, идентификациони број стандардизованих параметара домена описаних у табели 4. ЋЕ бити директно повезани. Експлицитни параметри домена добијени из `PACEDomainParameterInfo` НЕ СМИЈУ користити оне идентификационе бројеве резервисане за стандардизоване параметре домена.

A.2.1.1. Стандардизовани параметри домена

Стандардизовани параметри домена описани у табели 4. се ТРЕБАЈУ користити. Сљедећи идентификатор објекта се ТРЕБА користити да повеже стандардизоване параметре домена у `AlgorithmIdentifier`:

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

Са `AlgorithmIdentifier` овај идентификатор објекта ЋЕ референцирати идентификациони број стандардизованог параметра домена као у табели 4. као `INTEGER`.

ID	Назив	Величина	Ти	Референца
0	1024-bit MODP Group with 160-bit Prime Order	1024/160	GF	[19]
1	2048-bit MODP Group with 224-bit Prime Order	2048/224	GF	[19]
2	2048-bit MODP Group with 256-bit Prime Order	2048/256	GF	[19]
3 – 7	RFU			
8	NIST P-192 (secp192r1)	192	EC	[25], [19]
9	BrainpoolP192r1	192	EC	[20]
10	NIST P-224 (secp224r1)*	224	EC	[25], [19]
11	BrainpoolP224r1	224	EC	[20]
12	NIST P-256 (secp256r1)	256	EC	[25], [19]
13	BrainpoolP256r1	256	EC	[20]
14	BrainpoolP320r1	320	EC	[20]
15	NIST P-384 (secp384r1)	384	EC	[25], [19]
16	BrainpoolP384r1	384	EC	[20]
17	BrainpoolP512r1	512	EC	[20]
18	NIST P-521 (secp521r1)	521	EC	[25], [19]
19-	RFU			

* Ова крива се не може користити са интегрисаним мапирањем.

Табела 4: Стандардизовани параметри домена

A.2.1.2. Експлицитни параметри домена

Експлицитни параметри домена могу бити садржани у сљедећим структурама:

PACEDomainParameterInfo,

ChipAuthenticationPublicKeyInfo,

ChipAuthenticationDomainParameterInfo, i

RestrictedIdentificationDomainParameterInfo

Идентификатор објекта `dhpublicnumber` ili `ecPublicKey` за DH ili ECDH, сваки посебно, ЋЕ бити кориштени да повежу експлицитне параметер домена у `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
}
```

У случају елиптичних крива параметри домена МОРАЈУ бити описани експлицитно у структури ECParameters, тј. НЕ СМИЈУ се користити поменуте криве и имплицитни параметри домена.

A.2.1.3. PACE и аутентификација чипа

MRTD чип МОЖЕ подржавати више од једног сета параметара домена (тј. чип може подржавати различите алгоритме и/или дужине кључа) за PACE и аутентификацију чипа верзија 1 и 2.

Параметри домена садржани у EF.CardAccess, тј. `PACEDomainParameterInfo` и `ChipAuthenticationDomainParameterInfo` (за аутентификацију чипа верзија 2), су незаштићени и могу бити несигурни. Коришћење несигурних параметара домена може довести до напада, нпр. коришћење несигурних параметара домена за PACE ЋЕ довести до обзањивања шифре.

MRTD чипови морају подржавати најмање један сет стандардизованих параметара домена за PACE и аутентификацију чипа верзија 2, ако су одговарајући параметри имплементирани као сто је наведено у табели 4.

Терминали НЕ СМИЈУ користити неверификоване параметре домена за PACE и аутентификацију чипа верзију 2, тј. само се користе стандардизовани параметри домена или параметри домена које експлицитно терминал препозна као сигурне.

Параметри домена садржани у ChipAuthenticationDomainParameterInfo

и `ChipAuthenticationPublicKeyInfo` су заштићени објектом безбједности.

Аутентификација чипа у верзији МОРА обезбиједити најмање један сет експлицитних параметара домена

A.2.1.4. Ограничена идентификација

Параметри домена за ограничену идентификацију су дефинисани верификатором документа и МОРАЈУ се обезбиједити заједно са секторским јавним кључем у објекту података јавног кључа као дио ограничене идентификације (види прилог Д.3 і Б.4.1). Hash објекта података јавног кључа МОРА бити садржан у цертификату терминал као екстензија сектора терминала (види прилог Ц.3.2). MRTD чип МОРА верификовати секторски јавни кључ користећи екстензију сектора терминала.

Шифра	Кодирање
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)

Табела 5: Кодирање шифри

A.2.2. Привремени јавни кључеви („Ephemeral Public Keys“)

A.2.2.1. PACE и аутентификација чипа

Терминал за генерисање привременог јавног кључа за PACE и аутентификацију чипа верзија 1/2, свака посебно, МОРА користити параметре домена садржане у `PACEInfo` или `PACEDomainParameterInfo` и `ChipAuthenticationDomainParameterInfo` или `ChipAuthenticationPublicKeyInfo`. Привремени јавни кључеви се морају размијенити као просте вриједности јавног кључа. Више информација о кодирању се може пронаћи у прилогу Д.3.4.

Напомена: ПРЕПОРУЧЕНА је валидација привремених јавних кључева. За DH, валидација алгоритма захтјева да MRTDF чип детаљније познаје параметре домена (тј. Распоред кориштене подгрупе) него што иначе обезбиједи і PKCS#3.

A.2.2.2. Ограничена идентификација

Привремени јавни кључеви се не користе за ограничену идентификацију .

A.2.2.3. Компресија јавног кључа

Компресовани привремени јавни кључ терминала **Comp** ($\widetilde{PK}_{PCD}$) као што је захтјевано за аутентификацију терминала је дефинисан на сљедећи начин:

За DH је компресовани јавни кључ SHA-1 hash DH јавне вриједности, тј. октетни низ фиксне дужине 20.

За ECDH компресовани привремени кључ је x-координата ECDH јавне тачке, тј. октетни низ фиксне дужине ($\log_{256} p$).

A.2.3. Функција извођења кључева

Нека су $\mathbf{KDF}_{\mathbf{Enc}}(K,[r])=\mathbf{KDF}(K,[r],1)$, $\mathbf{KDF}_{\mathbf{MAC}}(K,[r])=\mathbf{KDF}(K,[r],2)$ функције извођења кључева које изводе кључеве за енкрипцију и

аутентификацију, сваки посебно, из заједничке шифре K и опционалног броја *nonce* r.

Нека је $\mathbf{KDF}_{\pi}(\pi)=\mathbf{KDF}(f(\pi),3)$ функција извођења кључева за извођење из шифре π. Кодирање шифре , tj.$K=f(\pi)$ је дефинисано у табели 5.

Функција извођења кључа $\mathbf{KDF}(K,[r],c)$, је дефинисана на сљедећи начин:

Улаз: Сљедећи улази су потребни:

- заједничка тајна вриједност K **(ЗАХТИЈЕВАНО)**
- nonce број r **(ОПЦИОНАЛНО)**
- 32-битни, big-endian integer counter c **(ЗАХТИЈЕВАНО)**

Излаз: Октетни низ кључних података.

Акције: сљедеће акције су извршене:

1. кључни податак=$\mathbf{H}(K\|r\|c)$
2. Излаз октетни низа кључних података

Функција извођења кључа $\mathbf{KDF}(K,[r],c)$ захтјева одговарајућу hash функцију изведену од **H** (), тј. дужина у битима hash функције ЋЕ бити интерпретирана као већа и једнака дужина у битима изведеног кључа. Вриједност hash-а ЋЕ бити интерпретирана као big-endian бајт излаз.

Nonce број r се користи само за аутентификацију чипа верзија 2.

Напомена: Заједничка тајна K је дефинисана као октетни низ. Ако је заједничка тајна генерисана са ECKA [3], x- координата генерисане тачке ЋЕ се користити.

A.2.3.1. 3DES

Да би се извели 112-битни 3DES [21] кључеви, hash фунцкија SHA-1 [23] ЋЕ се користити и МОРАЈУ се извршити сљедећи додатни кораци:

користити октете 1 до 8 података кључа за формирање података кључа А и октета 9 до 16 података кључа Б; нису кориштени додатни октети

подесити битове паритета података кључаА и кључа податакаБ за формирање тачних DES кључева (ОПЦИОНАЛНО).

A.2.3.2. AES

Да би се извели 128-битни AES [22] кључеви, hash функција SHA-1 [23] ЋЕ се користити и МОРАЈУ се извршити сљедећи додатни кораци:

користити октете 1 до 16 података кључа; нису кориштени додатни октети.

Да би се извели 192-битни и 256-битниAES [22] кључеви SHA-256 [23] ЋЕ се користити. За 192-битни AES кључеве МОРАЈУ се извршити сљедећи додатни кораци:

користити октете 1 до 24 података кључа; нису кориштени додатни октети.

A.2.4. Токен за аутентификацију

Токен за аутентификацију кориштен у PACE и аутентификацији чипа верзија 2 ЋЕ бити израчунат преко објекта података јавног кључа (види прилог Д.3) који садржи идентификатор објекта кориштеног протокола, тј. PACE или аутентификација чипа (као што је назначено у MSE:Set AT, vidi prilog Б.11.1), и преко запримљеног привременог јавног кључа користећи код за аутентификацију у кључ изведен из договора кључева.

A.2.4.1. 3DES

3DES [21] ЋЕ се користити у малопродајни mode у складу са ISO/IEC 9797-1 [16] MAC алгоритам 3 метод попуњавања 2 са блок шифром DES i $IV = 0$.

A.2.4.2. AES

AES [22] ЋЕ се користити у CMAC моделу [24] са MAC дужином 8 бајта.

A.3. PACE

A.3.1. PACE са DH

За PACE са DH се МОРАЈУ користити одговарајући алгоритми и формати из табеле A.2 и табеле 6.

OID	Мапирање	Сим. шифра	Дуж. кључа	Сигурна размјена порука	Токен за аут.
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

Табела 6: Идентификатори објекта за PACE са DH

A.3.2. PACE са ECDH

За PACE са ECDH се МОРАЈУ користити одговарајући алгоритми и формати из табеле A.2 и табеле 7.

OID	Мапирање	Сим. шифра	Дуж. кључа	Сигурна размјена порука	Токен за аут.
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

Табела 7: Идентификатори објекта за PACE са ECDH

A.3.3. Кодирани nonce број

MRTD чип ЋЕ насумично и једнообразно изабрати nonce broj $s \in \{0 \ldots 2^l - 1\}$ као бинарни битни низ дужине l, гдје је l multiple блок величине у битима одговарајуће блок шифре $\mathbf{E}()$ коју изабере MRTD чип.

Nonce број s ЋЕ бити кодиран у CBC модулу у складу са ISO 10116 [12] користећи кључ $K_\pi = \mathbf{KDF}_\pi(\pi)$ изведену из шифре π и $IV = 0$.

Nonce број s ЋЕ бити конвертован у насумичан генератор користећи специфичну алгоритамску функцију мапирања **Map**.

Напомена: Постоји неколико различитих алгоритама за имплементирање мапирања nonce броја у привремене параметре домена. Тренутно, сва специфична мапирања мапирају nonce број у привремени генератор. ПРЕПОРУЧУЈЕ СЕ имплементација мапирања као случајно одабрана функција.

A.3.4. ECDH Мапирање

Нека G и $\tilde{G}$ буду статички и привремени

A.3.4.1. Генеричко мапирање

Функција **Map** : G↦ $\tilde{G}$ се дефинише као $\tilde{G} = s \cdot G + H$, гдје је $H \in \langle G \rangle$ је одабран s.th $\log_G$ H је непознат. Тачка H ЋЕ бити израчуната анонимним Diffie-Hellman договором кључева [3].

Напомена: Алгоритам договора кључева ECKA спречава мале подгрупне нападе коришћењем компатибилне кофактор умножавања.

A.3.4.2. Интегрисано мапирање

Интегрисано ECDH мапирање је дефинисано са ICAO [10].

A.3.5. DH Мапирање

Нека g и $\tilde{g}$ буду статични и привремени генератор.

A.3.5.1. Генеричко мапирање

Функција **Map** : g↦ $\tilde{g}$ је дефинисана као $\tilde{g} = g^s h$, гдје је $h \in \langle g \rangle$ изабран s.th. $\log_g h$ је непознат. Групни елемент h ЋЕ бити израчунат анонимним Diffie-Hellman договором кључева.

Напомена: Метод валидације јавног кључа који је описан у RFC 2631 [26] се МОРА користити како би се спријечили мали подгрупни напади.

A.3.5.2. Интегрисано мапирање

Интегрисано DH мапирање је дефинисано са ICAO [10].

A.4. Аутентификација чипа

A.4.1. Пар кључева за аутентификацију чипа

Пар(ови) кључева за аутентификацију чипа МОРАЈУ бити сачувани на MRTD чипу.

Приватни кључ ЋЕ бити сигурно сачуван у меморији MRTD чипа.

Јавни кључ ЋЕ бити обезбјеђен као `SubjectPublicKeyInfo` у структури `ChipAuthenticationPublicKeyInfo`.

Параметри домена МОГУ бити додатно обезбјеђени као `AlgorithmIdentifier` структури `ChipAuthenticationDomainParameterInfo`.

Структуре података `SubjectPublicKeyInfo` и `AlgorithmIdentifier` s су дефинисане на сљедећи начин ; више детаља можете пронаћи у [6]:

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

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

MRTD чип МОЖЕ подржавати више од једног пара кључева за аутентификацију чипа (тј. чип може подржавати различите алгоритме и/или дужине кључева). У том случају, локални идентификатор кључа МОРА бити објављен у одговарајућим `ChipAuthenticationInfo`, `ChipAuthenticationPublicKeyInfo`, i `ChipAuthenticationDomainParameterInfo`.

A.4.2. Аутентификација чипа са DH

За аутентификацију чипа са DH, одређени алгоритми и формати из табеле A.2 и табеле 8 се МОРАЈУ користити. За аутентификацију чипа верзија 1 PKCS#3 [27] се МОРА користити умјесто X9.42 [1].

OID	Сим. шифр	Дужина кључа	Сигурна размјена порука	Токен за ауг.
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

Табела 8: Идентификатори објекта за аутентификацију чипа са DH

A.4.3. Аутентификација чипа са ECDH

Одговарајући алгоритми и формати из табеле A.2 и табеле 9 се МОРАЈУ користити за аутентификацију чипа са ECDH

OID	Сим. шифра	Дужина кључа	Сигурна размјена порука	Токен за аут.
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

Табела 9: Идентификатори објекта за аутентификацију чипа са ECDH

A.5. Ограничена идентификација

A.5.1. MRTD чип приватног кључа

Генерисање приватног кључа SK_{ID} није обухваћено овом спецификацијом. Ако је SK_{ID} генерисан као кодирани секвенцијални бројач или као кодирани број документа, трећа страна ЋЕ генерисати и сигурно сачувати тајни кодирани кључ.

A.5.2. Јавни кључеви за сектор

Трећа (провјерена) страна МОРА генерисати јавне кључеве сектора.

- Ако трећа страна МОРА мора бити у могућности да повеже секторске специфичне идентификаторе по секторима, онда ЋЕ трећа страна генерисати парове кључева сектора и сачувати сигурно приватне кључеве сектора.
- Ако трећа страна НЕ МОРА бити у могућности да повеже секторске специфичне идентификаторе по секторима, онда ЋЕ трећа страна генерисати парове кључева сектора тако да су одговарајући приватни кључеви непознати.

A.5.3. Ограничена идентификација са DH

Одговарајући алгоритми и формати из табеле А.2 и табеле 10 се МОРАЈУ користити за ограничену идентификацију са 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

Табела 10: Идентификатори објекта за ограничену идентификацију са DH

A.5.4. Ограничена идентификација са ECDH

Одговарајући алгоритми и формати из табеле А.2 и табеле 11 се МОРАЈУ користити за ограничену идентификацију са ECDH. Улаз у hash функцију ЋЕ бити x-координата тачке који је ЕСКА [3] генерисала.

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

Табела 11: Идентификатори објекта за ограничену идентификацију са ECDH

A.6. Аутентификација терминала

A.6.1. Референце јавног кључа

Јавни кључеви који се користе за аутентификацију терминала МОРАЈУ бити садржани у CV цертификатима у складу са профилом цертификата дефинисаном у прилогу Ц.1. сваки CV цертификат МОРА садржавати двије референце јавног кључа, референца носиоца цертификата и референца цертификационог тијела:

Референца носиоца цертификата: Референца носиоца цертификата је идентификатор за јавни кључ који је обезбјеђен у цертификату који ЋЕ се користити за референцу овог јавног кључа.

Референца цертификационог тијела: Референца цертификационог тијела је референца (екстерног) јавног кључа цертификационог тијела који ЋЕ се користити за верификовање потписа цертификата.

Напомена: Као посљедица референца цертификационог тијела садржаног у цертификату МОРА бити једнака референци носиоца цертификата у одговарајућем цертификату цертификационог тијела надлежног за издавање.

	Кодирање	Дужина
Позивни број	ISO 3166-1 ALPHA-2	2F
Мнемоника носиоца	ISO/IEC 8859-1	9V
Број секвенци	ISO/IEC 8859-1	5F
F: фиксна дужина (тачан број октета) V промјењива дужина (до одређеног броја октета)		

Табела 12: Референца носиоца цертификата

Референца носиоца цертификата ЋЕ се састојати од сљедећих увезаних елемената: позивни број, мнемоника носиоца, и редни број. Ови елементи се МОРАЈУ бирати у складу са табелом 12 и сљедећим правилима.

1. Код земље

Позив на број ЋЕ бити ISO 3166-1 ALPHA-2 број државе носиоца цертификата.

2. Мнемоника носиоца

Мнемоника носиоца ЋЕ бити бити додјељена као јединствен идентификатор како слиједи:

- CVCA ЋЕ додијелити мнемонику носиоца CVCA.

- Домаћи CVCA ЋЕ додијелити мнемонику носиоца DV.
- Надзорни DV ЋЕ додијелити мнемонику носиоца IS.

3. Број секвенци

Носилац цертификата ЋЕ додијелити број секвенци.

- Број секвенци МОРА бити нумерички или алфанумерички:

o нумерички број секвенци ЋЕ се састојати од знакова“0”...”9”.

o алфанумерички број секвенци ЋЕ се састојати од знакова“0”...”9” i “A”...”Z”.

- Број секвенци МОЖЕ почети са ISO 3166-1 ALPHA-2 позивним бројем надлежног органа за цертификацију, а преостала три знака ЋЕ бити алфанумерички број секвенци.
- Број секвенци МОЖЕ бити ресетован ако су сви доступни бројеви секвенци исцрпљени.

A.6.2. Импорт јавног кључа

Јавни кључеви који су увезени процедуром валидације цертификата (види одјељак 2.5) су или *трајно* или *привремено* сачувани на MRTD чипу. MRTD чип ТРЕБА да одбије импорт јавног кључа ако је референца носиоца цертификата већ позната чипу.

A.6.2.1. Трајни увоз

Јавни кључеви који су садржани у CVCA линк цертификатима ЋЕ бити трајно импортовани од стране MRTD чипа и МОРАЈУ бити сигурно сачувани на меморији MRTD чипа. Трајно импортован јавни кључи и његови метаподаци ЋЕ испунити сљедеће услове:

МОЖЕ бити замјењен *након истека* накнадним трајним импортованим кључем.

МОРА бити замјењен накнадним трајним увезеним кључем са истом референцом носиоца цертификата или импорт МОРА бити одбијен.

НЕ СМИЈЕ бити замјењен привременим импортованим јавним кључем.

Напомена: ПРЕПОРУЧУЈЕ се одбијање импорта јавног кључа ако је референца носиоца цертификата већ позната MRTD чипу.

Омогућавање и онемогућавање трајно импортованог јавног кључа мора бити atomic операција.

A.6.2.2. Привремени увоз

Јавне кључеве који су садржани у DV и цертификатима терминала ЋЕ привремено импортовати MRTD чип. Привремено импортован јавни кључ и његови метаподаци ЋЕ испунити сљедеће услове:

НЕЋЕ се моћи селектовати и користити након гашења MRTD чипа.

МОРА остати употребљив до завршетка замјене криптографске операције (tj. PSO:Verify Certificate ili External Authenticate).

МОЖЕ бити замјењен накнадним привременим импортованим јавним кључем.

Терминал НЕ СМИЈЕ користити било које друге привремено импортоване кључеве

осим оних који су посљедни импортовани.

Име фајла	EF.CVCA
ID фајл	0x011C (default)
Кратки фајл ID	0x1C (default)
Приступ очитавања	BAC *or* PACE (conditional to protocol support)
Приступ уписа	NEVER (internally updated only)
Величина	36 bytes (fixed) padded with octets of value 0x00
Садржај	[CARi][||CARi-1][||0x00..00]

Табела 5: Основни фајл EF.CVCA

A.6.2.3. Импортовани метаподаци

За сваки трајни или привремени импортовани јавни кључ, сљедећи додатни подаци који су садржани у цертификату (види одјељак Ц.1) МОРАЈУ бити сачувани:

Референца носиоца цертификата

Ауторизација носиоца цертификата (важећа рола и важећа ауторизација)

Датум ступања на снагу цертификата

Датум истека цертификата

Продужења цертификата (гдје је примјенљиво)

Рачунање ефикасне роле (CVCA, DV или терминал) и ефективна ауторизација носиоца цертификата је описана у одјељку 2.6.

Напомена: Формат сачуваних података функционише неовисно о систему и није садржана у овој спецификацији.

A.6.2.4. EF.CVCA

Подршка за основни фајл EF.CVCA је УСЛОВЉЕНА. Ако MRTD чип подржава аутентификацију терминала у верзији 1, мора урадити референце CVCA јавних кључева који одговарају за инспекцијске системе доступне у транспарентном основном фајлу EF.CVCA који је садржан у еПасош апликацији као што је дефинисано у табели 13.

Овај фајл ЋЕ садржавати секвенцу објеката података (види прилог Д.2) референце цертификацијског тијела (CAR) одговарајућих за аутентификацију терминала.

Фајл ЋЕ садржавати највише два објекта података референце цертификацијског тијела.

Посљедња референца цертификацијског тијела ЋЕ бити први објекат података на овој листи.

Фајл МОРА бити попуњен са додатним октетима у вриједности 0x00.

Фајл EF.CVCA има идентификатор и кратки идентификатор фајла. Ако се задана вриједност не може користити, (кратки) идентификатор фајла ЋЕ бити дефинисан у ОПЦИОНАЛНОМ параметру `efCVCA` od `TerminalAuthenticationInfo`. Ако се `efCVCA` користи за означавање идентификатора фајла који ће се користити,

почетни фајл ће се поништити. Ако у `efCBCA` није понуђен кратки фајл, фајл EF.CBCA МОРА бити експлицитно одабран користећи дати идентификатор фајла.

A.6.3. Аутентификација терминала са RSA

За аутентификација терминала са RSA МОРАЈУ се користити сљедећи алгоритми и формати.

A.6.3.1. Алгоритам потписа

RSA [18], [28] као што је дефинисано у табели 14 ЋЕ се користити. Почетни параметри који ће се користити са RSA-PSS су дефинисани како слиједи:

Hash алгоритам: hash алгоритам је одабран у складу са табелом 14.

Algoritam генерисања маска: MGF1 [18], [28] користећи hash алгоритам.

Salt дужина: октетна дужина излаза одабраног hash алгоритма.

Trailer Field: 0xBS

A.6.3.2. Формат јавног кључа

TLB-формат [15] као што је описан у прилогу Д.3.1 ЋЕ се користити.

Идентификатор објекта ЋЕ се узети из табеле 14.

Дужина модула у битима ЋЕ бити 1024, 1280, 1536, 2048, ор 3072.

Дужина експоната у битима Ће бити највише 32.

A.6.4. Аутентификација терминала са ECDSA

За аутентификацију терминала са ECDSA МОРАЈУ се користити сљедећи алгоритми и формати.

OID	Потпис	Hash	Параметри
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

Табела 6: Идентификатори објекта за аутентификацију терминала са RSA

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

Табела 7: Идентификатори објекта за аутентификацију терминала са ECDSA

A.6.4.1. Алгоритам потписа

ECDSA са простим форматом потписа [3] као што је дефинисано у табели 15 ЋЕ се користити.

A.6.4.2. Формат јавног кључа

TLB формат [15] као што је описан у прилогу Д.3.3 ЋЕ се користити.

Идентификатор објекта ЋЕ се узети из табеле 15.

Дужина криве у битима ЋЕ износити 160, 192, 224, 256, 320, 384 ор 512.

Параметри домена ЋЕ бити у складу [3].

A.6.5. Аутентификовани помоћни подаци за аутентификацију терминала верзија 2

Коришћење помоћних података у аутентификацији терминала је УСЛОВЉЕНО. МОРА бити кориштено ако даље операције које извршава терминал захтијевају аутентификоване помоћне податке (детаљи се могу пронаћи у сљедећим одјељцима):

за старосну верификацију, терминал МОРА користити потребан датум рођења.

за верификацију важења документа, терминал МОРА користити тренутни датум.

за верификацију идентификационог броја општине, терминал МОРА користити (дијелове) идентификационог броја.

Аутентификовани помоћни подаци МОРАЈУ бити структурисани као што је дефинисано у табели 16:

аутентификација објекта података која садржи секвенцу дискреционих образаца података.

сваки дискрециони образац података садржи идентификатор објекта и објекат дискреционих података. Садржај објекта дискреционих података је дефинисан идентификатором објекта.

Тек након успјешне аутентификације терминала MRTD чип ЋЕ интерпретирати и направити доступним податке који су садржани у објекту дискреционих података за даље операције.

Напомена: уколико аутентификација објекта података садржи више од једног обрасца дискреционог податка са истим идентификатором објекта, подаци са посљедњег обрасца дискреционих података ЋЕ бити доступне за даље операције.

A.6.5.1. Идентификатор објекта

Сљедећи идентификатор објекта ЋЕ се користити за идентификацију аутентификованих помоћних података:

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

A.6.5.2. Старосна верификација

Сљедећи идентификатор објекта ЋЕ се користити за старосну верификацију:

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

Објекат дискреционих података ЋЕ садржавати датум рођења кодиран као `Date` (види дио 2) који терминал *захтијева*. MRTD чип ЋЕ упоредити сачуване датуме рођења са траженим датумом рођења. Старосна верификација је успјешна ако сачувани датум рођења није након траженог датумом рођења

Објекат података
Аутентификација
Образац дискреционих података
Идентификатор објекта
Дискрециони подаци
Образац дискреционих података
Идентификатор објекта
Дискрециони подаци
...

Табела 8: Аутентификовани помоћни подаци

A.6.5.3. Верификација важења документа

Сљедећи идентификатор објекта ЋЕ се користити за верификацију важења документа:

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

Објекат дискреционих података ЋЕ садржавати тренутни датум терминала кодиран као Date (види дио 2). MRTD чип ће упоредити сачуване датуме рока важења и тренутни датум. Верификација важења документа је успјешна ако сачувани датум рока важења није прије датог тренутног датума.

A.6.5.4. Верификација идентификационог броја општине

Сљедећи идентификатор објекта ЋЕ се користити за верификацију идентификационог броја општине:

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

Објекат дискреционих података ЋЕ садржавати (дијелове) идентификационог броја општине кодиране као `Octet•String` (види дио 2.). MRTD чип ЋЕ упоредити најљевије октете сачуваног идентификационог броја општине и пренесени (дио) тражени идентификациони број општине. Верификација идентификационог броја општине је успјешна ако су најљевији октети сачуваног идентификационог броја општине идентични пренесеним подацима.

Б. ISO 7816 Мапирање (Норматив)

У овом прилогу протоколи за PACE, аутентификацију чипа и аутентификацију терминала су мапирани према ISO 7816 ARDUs (јединице података апликативног протокола).

Б.1. PACE

Сљедећи низ команди ЋЕ се користити за имплементацију PACE. Сигурна размјена порука је УСЛОВЉЕНА. МОРА се користити за друго извршење PACE ако је протокол извршен два пута:

1. MSE:Set AT
2. General Authenticate

Објекти специфичних података протокола ЋЕ бити размјењени у ланцу General Authenticate команди што је приказано у наставку:

Korak	Опис	Подаци команди у протоколу		Подаци одговора у протоколу	
1.	Кодирани nonce број	-	одсутан	0x80	Кодирани nonce број
2.	Мапирање nonce број	0x81	Мапирање података	0x82	Мапирање података
3.	Извршавање договора кључева	0x83	Привремени јавни кључ	0x84	Привремени јавни кључ
4.	Заједничка аутентификација	0x85	Токен за аутентификацију	0x86 0x87	Токен за аутентификацију Референца цертификационог тијела (УСЛОВЉЕНО)

Референца(е) цертификационог тијела су ЗАХТЈЕВАНЕ ако се користи PACE са обрасцом ауторизације носиоца цертификата, тј. ако терминал за аутентификацију верзија 2 слиједи PACE. У том случају, објекат података 0x87 ЋЕ садржавати најновије референце цертификацијског тијела у односу на тип терминала назначен у обрасцу ауторизације носиоца цертификата. Објекат података 0x88 МОЖЕ садржавати претходне референце цертификацијског тијела.

Напомена: Параметри домена за PACE које чип подржава су доступни у EF.CardAc- cess (види прилог A.1.2.). Ако је подржано више од једног сета параметара домена, терминал МОРА одабрати параметре домена које ће се

користити у оквиру MSE:Set AT.

Б.1.1. Кодирни nonce број

Кодирани број (види прилог А.3.3) ЋЕ бити кодиран као октетни низ.

Б.1.2. Мапирање података

Измјењени податак је специфичан за кориштено мапирање.

Б.1.2.1. Генеричко мапирање

Привремени јавни кључеви (види прилог А.2.2 и прилог Д.3.4) ЋЕ бити кодирани као тачке елиптичке криве (ECDH) и непотписаног цијелог броја (DH).

Б.1.2.2. Интегрисано мапирање

Интегрисано мапирање је дефинисано са ICAO [10].

Б.1.3. Токен за аутентификацију

Токен за аутентификацију (види прилог А.2.4) ЋЕ бити кодиран као октетни низ.

Б.1.4. Референца цертификацијског тијела

MRTD чип ЋЕ вратити референце цертификацијског тијела *одговарајућих* CVCA јавних кључева који су сачувани на MRTD чипу:

референце МОРАЈУ бити динамичи изабране да одговарају типу терминала који PACE значи.

највише два објекта података референци цертификацијског тијела ЋЕ бити враћена.

најновије референце цертификацијског тијела ЋЕ бити садржане у објекту података 0x87.

Б.2. Аутентификација чипа

Сљедеће команда ЋЕ се користити при сигурној размјени порука за имплементацију аутентификацију чипа у верзији 1 са 3DES сигурном размјеном порука:

1. MSE:Set KAT

Напомена: MSE:Set KAT се НЕ СМИЈЕ користити за друге алгоритме osimid-CA-DH-3DES-CBC- CBC i id-CA-ECDH-3DES-CBC-CBC, тј. сигурна размјена порука је ограничена за 3DES.

Сљедећи низ команди ЋЕ се користити за сигурну размјену података

имплементирање аутентификације чипа у верзији 1 са AES и

имплементирање аутентификације чипа у верзији 1

Поред тога, овај низ се МОЖЕ користити за имплементацију аутентификације чипа у верзији 1 са 3DES:

1. MSE:Set AT
2. General Authenticate

Објекти специфичних података протокола ЋЕ се размјењивати са General Authenticate командом како је приказано у табели:

Корак	Опис	Подаци команди у протоколу		Подаци одговора у протоколу	
1.	Аутентификација чипа	0x80	Привремени јавни кључ	0x81 0x82	Нонце број Токен за аутентификацију

Напомена: Подршка података одговора у протоколу је УСЛОВЉЕНА: МОРА бити обезбјеђена за верзију 2 али НЕ СМИЈЕ за верзију 1.

Напомена: Јавни кључеви за аутентификацију чипа које чип подржава су доступни у објектима сигурности (види прилог А.1.2.). Ако је подржано више од једног јавног кључа, терминал МОРА одабрати одговарајући приватни кључ чипа који ће се користити у оквиру MSE:Set AT.

Б.2.1. Привремени јавни кључ

Привремени јавни кључеви (види прилог А.2.2 и Д.3.4) ЋЕ бити кодирани као елиптичке тачке криве (ECDH) или непотписан цијели број (DH).

Б.2.2. Nonce број

Nonce број ЋЕ бити кодиран као октетни низ дужине 8 октета.

Б.2.3. Токен за аутентификацију

Токен за аутентификацију (види прилог А.2.4) ЋЕ бити кодиран као октетни низ.

Б.3. Аутентификација терминала

Сљедећи низ команди ЋЕ се користити при сигурној размјени порука за имплементирање аутентификације терминала:

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

Кораци 1 и 2 се понављају за сваки CV цертификат који се треба верификовати (CVCA повезани цертификати, DV цертификати, цертификати терминала).

За аутентификацију терминала у верзији 2, MRTD чип МОРА додатно подржавати коришћење Get Challenge прије корака 1, тј. MRTD чип мора задржати генерисани изазов (challenge) након коришћења External Authenticate.

Б.4. Ограничена идентификација

Сљедећи низ команди ЋЕ се користити при сигурној размјени порука за имплементирање ограничене идентификације:

1. MSE:Set AT
2. General Authenticate

Објекти специфичних података протокола ЋЕ се размјењивати са Генерал Аутхентицате командом како је приказано у табели, а везане команде се НЕ СМИЈУ користити. МОРА се извршити најмање један корак:

Корак	Опис	Подаци команди у протоколу		Подаци одговора у протоколу	
1.	Ограничена идентификација (УСПОСТАВЉЕНО)	0xA0	1^{st} Јавни кључ сектора	0x81	1^{st} Специфични идентификатор сектора
2.	Ограничена идентификација	0xA2	2^{nd} Јавни кључ сектора	0x83	2^{nd} Специфични идентификатор сектора

Напомена: Приватни кључеви за ограничену идентификацију које чип подржава су назначени у одговарајућим објектима безбједности (види прилог А.1.2.). Ако се подржава више од једног приватног кључа, терминал МОРА одабрати приватни кључ који ће се користити у оквиру MSE:Set AT.

Б.4.1. Јавни кључ

Јавни кључ сектора PK_{Sector} ЋЕ бити кодиран као ојекат података јавног кључа без тага 0x7F49 (тј. 0x7F49 је замјењен са 0xA0/0xA2,сваки посебно) (види прилог Д.3), параметри домена МОРАЈУ бити укључени.

Б.4.2. Секторски специфичан идентификатор

Секторски специфичан идентификатор I_{ID}^{Sector} ЋЕ бити кодиран као октетни низ.

Б.5. Верификација помоћних података

Сљедећа команда ЋЕ се користити при сигурној размјени порука за имплементацију функције верификовања:

1. Verify

Сљедећи аутентификовани помоћни подаци се МОРАЈУ послати MRTD чипу као дио аутентификације терминала:

за старосну верификацију терминал МОРА послати тражени датум рођења.

за верификацију важења документа терминал МОРА послати тренутни датум

за верификацију идентификационог броја општине терминал МОРА послати (дио) идентификационог броја.

Б.6. Управљање PIN-ом

Б.6.1. Деблокирање или промјена PIN-а

Сљедећа команда ЋЕ се користити при сигурној размјени порука за имплементацију

деблокирање и/или промјену PIN-а:

1. Reset Retry Counter

   За подешавање новог PIN-а и ресетовања бројача понављања терминал ЋЕ користити Reset Retry Counter са новим подацима PIN-а.

   За ресетовање бројача понављања терминал ЋЕ користити Reset Retry Counter без података.

Коришћење команде ЋЕ бити ограничено ауторизованим терминалима: Прије коришћења ове команде, терминал се мора аутентификовати као терминал за аутентификацију са важећом ауторизацијом за управљање PIN-ом или коришћењем PACE са PUK/PIN.

Б.6.2. Активирање и деактивирање PIN-а

Сљедећа команда ЋЕ се користити при сигурној размјени порука за активирање PIN-а:

1. Activate

Сљедећа команда ЋЕ се користити при сигурној размјени порука за деактивирање PIN-а:

1. Deactivate

Коришћење ове команде је ограничено ауторизованим терминалима. Прије коришћења ове команде, терминал се мора аутентификовати као терминал за аутентификацију са важећом ауторизацијом за управљање PIN-ом

Б.7. Апликација еПотпис

Команде за инсталирање, ажурирање и коришћење апликације еПотпис нису обухваћене овом спецификацијом.

Б.8. Групе за очитавање података

APDU за одабир и очитавање EAC заштићених група података које је већ дефинисано са ICAO [8], [9] ЋЕ се користити (тј. Select File или Read Binary). У складу са ICAO спецификацијама, сваки неауторизован приступ EAC заштићеним групама података ЋЕ бити одбијен и MRTD чип МОРА одговорити са статусом у битима 0x6982 (“Сигурносни статус није задовољен”).

Б.9. Проширење

У зависности од величине криптографских објеката (нпр. јавни кључеви, потписи), МОРАЈУ се користити APDU са проширеним пољима за слање ових података MRTD чипу. Детаљније о проширењу види[13].

Б.9.1. MRTD чипови

Подршка проширења за MRTD чипове је УСЛОВЉЕНА. Ако су криптографски алгоритми и величине кључева одабрани од државе која врши издавање захтијевају коришћење проширења, MRTD чипови ЋЕ подржати та проширења. Ако MRTD чип подржава проширење, то МОРА бити назначено у ATR/ATS или у EF.ATR/INFO као што је дефинисано у[13].

Б.9.2. Терминали

Подршка проширења за терминале се ЗАХТИЈЕВА. Терминал ТРЕБА прије коришћења ове опције испитати да ли је подршка за проширење назначена у ATR/ATS or in EF.ATR/INFO MRTD чипа. Терминал НЕ СМИЈЕ користити проширења за APDU осим команди праћења, осим ако су тачне улазне и излазне величине меморија MRTD чипа експлицитно назначене у ATR/ATS или у EF.ATR/INFO.

PSO:Verify Certificate

MSE:Set KAT

General Authenticate

External Authenticate

Б.9.3. Грешке

MRTD чип ТРЕБА пријавити грешке наредбе са проширеном дужином кодом грешке 0x6700.

Б.10. Увезивање команди

Увезивање команди се користи само за команду General Authenticate. Детаљније о увезивању команди погледајте у [13].

Б.10.1. MRTD чипови

За MRT чипове, увезивање команди је ЗАХТИЈЕВАНО и подршка увезивања команди МОРА бити назначена у старим бајтовимА ATR/ATS или у EF.ATR/INFO као што је дефинисано у [13].

Б.10.2. Терминали

За терминале увезивање команди је ЗАХТИЈЕВАНО. Терминал прије уотребе ове опције ТРЕБА испитати да ли MRTD чип подржава увезивање команди.

Б.10.3. Грешке

Ако MRTD чип очекује крај увезивања, али прима команду која није означена као задња команда, MRTD чип ЋЕ назначити да задња команда у ланцу је очекивана са статусом у бајтима0x6883.

Б.11. APDU спецификације

У наставку су описане APDU коришћене за имплементацију протокола. MRTD чип ЋЕ имплементирати APDU као што је описано али МОЖЕ одступити од описа ако су APDU коришћене у другим контекстима.

Изостављен CLA бајт ЋЕ бити подешен за означавање сигурне размјене порука са аутентификованим заглављем, увезивањем команди и специфичним кодирањем апликација као што је захтијевано протоколима (види прилог Е.1).

Б.11.1. MSE:Set AT

Команда MSE:Set AT се користи за одабир и иницирање сљедећих протокола:

PACE, аутентификација чипа, аутентификација терминала и ограничена идентификација.

Команда			
INC	0x22	Управљање безбиједносним окружењем	
P1/P2	0xЦ1А4	PACE: Успоставити аутентикациони образац за узајамну аутентикацију.	
	0x41A4	Аутентикација чипа /ограничена идентификација: Поставити аутентикациони образац за интерну аутентикацију.	
Податак	0x80	Референце за криптографски механизам Одабрати идентификатор објекта протокола (само вриједност, Таг 0x06 је изостављен). Овај објекат података ЗАХТИЈЕВА се за све протоколе, осим за аутентикацију терминала у верзији 1. Референце за јавни/тајни кључ Овај објекат података ЗАХТИЈЕВА се за сљедеће протоколе:	УСЛОВЉЕНО
	0x83	• За PACE како би указао на лозинку која ће се користити: 0x01: MRZ 0x02: CAN 0x03: PIN 0x04: PUK • За аутентикацију терминала како би се одабрао јавни кључ терминала путем његовог кодираног назива у складу са ISO 8859-1. Референце за приватни кључ/референце за израчунавање сесијског кључа Овај објекат података ЗАХТИЈЕВА се за сљедеће протоколе (види Додатак А.2): • За PACE, да би се указало на идентификатор параметара домена који ће се користити уколико су параметри домена двосмислени, односно, постоји више од једног скупа параметара домена који су доступни за PACE.	УСЛОВЉЕНО
	0x84	• За аутентикацију чипа, да би се указало на идентификатор приватног кључа који ће се користити ако је приватни кључ двосмислен, односно постоји више од једног приватног кључа који су доступни за аутентикацију чипа.	УСЛОВЉЕНО

	~~0x67~~	~~Помоћни подаци чија се аутентикација извршава~~ Овај објекат података ЗАХТИЈЕВА се за аутентикацију терминала (верзија 2) уколико се користи верификација старости, важности документа или идентификационог броја општине)	~~УСЛОВЉЕНО~~
	0x91	Привремени јавни кључ Овај објекат података ЗАХТИЈЕВА се за аутентикацију терминала уколико је привремени јавни кључ $\widetilde{PK_{PCD}}$ непознат или двосмислен за чип MRTD-а када се извршава аутентикација терминала (односно, верзија 2). У овом случају компресовани привремени јавни кључ терминала **Comp**($\widetilde{PK_{PCD}}$) МОРА се послати чипу MRTD-а. Образац за ауторизацију носиоца сертификата	УСЛОВЉЕНО
Одговор			
Податак	–	Одсуство	

Статус бајтова	0x9000	Нормална операција Протокол је селектован и иницијализован.
	0x6A80	Нетачни параметри у пољима у којима се исписују команде • Алгоритми који нису подржани или чија је иницијализација неуспјешна. • Врста терминала на коју образац за ауторизацију носиоца сертификата указује није овлашћена за коришћење референтне лозинке (PACE).
	0x6A88	Референтни подаци нису пронађени Референтни подаци (односно, лозинка, приватни кључ, јавни кључ, параметри домена) нису доступни.
	0x63CH	Упозорење Одабрана је лозинка. X означава број преосталих покушаја верификације, ако нису једнаки иницијалној вриједности: X=1: Лозинка је обустављена. Лозинка се МОРА поновити. X=0: Лозинка је блокирана. Лозинка се мора деблокирати.
PACE		Упозорење Лозинка је деактивирана.
	0x6283 остало	Грешка која зависи од оперативног система Иницијализација протокола није успјела.
PACE		

Напомена:

- Неки оперативни системи прихватају одабир недоступног јавног кључа и враћају информацију о грешци само када се јавни кључ користи за одабрану сврху.
- Понављање и деблокирање лозинке захтијева експлицитно успостављање CAN-а или PUK-а коришћењем MSE:Set AT.

Б.11.2. General Authenticate

Команда General Authenticate користи се за извршавање сљедећих протокола: PACE-a, аутентикације чипа и ограничене идентификације.

Команда			
INS	0x86	General Authenticate	
P1/P2	0x0000	Кључеви и протокол су индиректно познати.	
Податак	0x7C	Динамичка аутентикација података Објекти података специфични за протокол	ЗАХТИЈЕВА СЕ
Одговор			
Податак	0x7C	Динамичка аутентикација података Објекти података специфични за протокол	ЗАХТИЈЕВА СЕ
Статус Bytes	0x9000	Нормална операција Протокол (корак) је био успјешан.	
	0x6300	Неуспјешна аутентикација Протокол (корак) је био неуспјешан.	
	0x63CH	Неуспјешна аутентикација Протокол (корак) је био неуспјешан. X означава број преосталих покушаја верификације: X=1: Лозинка је обустављена. Лозинка се МОРА поновити. X=0: Лозинка је блокирана. Лозинка се МОРА деблокирати.	
	0x6982	Безбиједносни статус није задовољен Терминал није овлашћен да извршава протокол (нпр. лозинка је блокирана, деактивирана или суспендована). Блокиран аутентикациони метод Лозинка је блокирана. Референтни подаци се не могу користити	

Напомена: Чип MRTD-a МОЖЕ указати на блокирану, деактивирану или суспендовану лозинку одговарајући са статусним бајтом 0x6982, умјесто статусних бајтова 0x6983, 0x6984, или 0x6985, датим редослиједом.

Б.11.3. MSE:Set KAT

Команда MSE:Set KAT користи се за верзију 1, аутентикације чипа са 3DES.

Команда			
INS	0x22	Управљање безбиједносним окружењем	
P1/P2	0x41A6	Успоставити образац за израчунавање слагања кључева.	
Податак	0x91 0x84	Привремени јавни кључ Привремени јавни кључ $\overline{PK}_{PCD}$ (види Додатак А.2) кодиран као читљива вриједност јавног кључа. Референце приватног кључа Овај објекат података ЗАХТИЈЕВА се уколико је приватни кључ двосмислен, односно, када је више од једног пара кључева на располагању за аутентикацију чипа (види Додатак А.1.1.2 и Додатак А.4.1).	ЗАХТИЈЕВА СЕ УСЛОВЉЕНО
Одговор			
Података	–	Одсуство	
Статусни бајтови	0x9000 0x6A80 остало	Нормална операција Операција усклађивања кључева извршена је успјешно. Изведени су нови сесијски кључеви. Нетачни параметри у пољима у којима се исписују команде Валидација привременог јавног кључа није успјешна. Претходно успостављени сесијски кључеви остају важећи. Грешка која зависи од оперативног система Претходно успостављени сесијски кључеви остају важећи.	

Б.11.4. MSE:Set DST

Команда MSE:Set DST користи се за успостављање верификације сертификата за аутентикацију терминала.

Команда		
INS	0x22	Управљање безбиједносним окружењем
P1/P2	0x81B6	Успостављање обрасца за дигитални потпис за верификацију.

Податак	0x83	Референце јавног кључа Кодирани назив јавног кључа који треба успоставити у складу са ISO 8859-1	ЗАХТИЈЕВА СЕ
Одговор			
Податак	–	Одсуство	
Статусни бајтови	0x9000 0x6A88 остало	Нормална операција Одабран је кључ за одређену намјену. Референтни подаци нису пронађени Одабир није успио јер јавни кључ није доступан.	

Напомена: Неки оперативни системи прихватају одабир недоступног јавног кључа и одговарају грешком само уколико се јавни кључ користи за одабрану намјену.

Б.11.5. PSO:Verify Certificate

Команда PSO:Verify Certificate користи се за верификацију и уношење сертификата за аутентикацију терминала.

Команда			
INS	0x2A	Извршити безбиједносну операцију	
P1/P2	0x00BE	Верификовати самоописиви сертификат.	
Податак	0x7F4E	Сертификационо тијело Сертификационо тијело које треба верификовати.	ЗАХТИЈЕВА СЕ ЗАХТИЈЕВА СЕ
Одговор			
Податак	–	Одсуство	
Статусни бајтови	0x9000	Нормална операција Валидација сертификата извршена је успјешно и јавни кључ је унесен. Грешка која зависи од оперативног система	

Б.11.6. Get Challenge

Команда Get Challenge користи се за извршавање аутентикације терминала.

Команда		
INS	0x84	Get Challenge
P1/P2	0x000	

Податак	–	Одсуство	
Le	0x08		ЗАХТИЈЕВА СЕ
Одговор			
Податак	r	8 насумичних бајтова.	
Статусни бајтови	0x9000	Нормална операција Грешка која зависи од оперативног система	

Б.11.7. External Authenticate

Команда External Authenticate користи се за извршавање аутентикације терминала.

Команда			
INS	0x82	External Authenticate	
P1/P2	0x000	Кључеви и алгоритми су индиректно познати.	
Податак		Терминал генерише потпис.	ЗАХТИЈЕВА СЕ
Одговор			
Податак	–	Одсуство	

Статусни бајтови	0x9000	Нормална операција Аутентикација обављена успјешно. Приступ групама података биће додијељен према важећим ауторизацијама одговарајућег верификованог сертификата.
	0x6300	Упозорење Верификација потписа неуспјешна.
	0x6982	Безбиједносни статус не задовољава Аутентикација неуспјешна јер тренутни ниво аутентикације терминала не дозвољава употребу аутентикације терминала (нпр. аутентикација терминала је већ извршена, итд.).
	0x6985	Услови коришћења нису задовољени
	остало	Врста терминала коју је одредио PACE не поклапа се са врстом терминала која се налази у ланцу сертификата. Грешка која зависи од оперативног система Неуспјешна аутентикација.

Б.11.8. Verify

Команда Verify користи се за верификацију помоћних података чија аутентикација се врши, односно, извршавање верификације старости, важности документа или верификације идентификационог броја општине.

Напомена: Због кодирања које је специфично за апликације, МОРА се користити класа инструкције *проприетару цласс*, односно, CLA=0x8C.

Команда			
INS	0x20	Verify	
P1/P2	0x800	Верификовати помоћне податке чија се аутентикација врши.	
Податак		Верификовати идентификатор објекта помоћних података.	ЗАХТИЈЕВА СЕ
Одговор			
Податак	–	Одсуство	

Статусни бајтови	0x9000	Нормална операција Верификација успјешна.
	0x6300	Верификација неуспјешна Верификација неуспјешна.
	0x6A88	Референтни подаци нису пронађени Референтни подаци нису пронађени.

Б.11.9. Reset Retry Counter

Команда Reset Retry Counter користи се за деблокирање или промјену PIN-а.

Команда			
INS	0x2C	Reset Retry Counter	
P1	0x02-0x03	Види доље	
P2		0x02: CAN 0x03: ПИН	
Податак		Поново успостављени подаци карактеристични за контекст, који зависе од P1: P1=0x02: new PIN/CAN P1=0x03: Absent	ЗАХТИЈЕВА СЕ
Одговор			
Податак	–	Одсуство	
Статусни бајтови	0x9000 0x6982 остало	Нормална операција Деблокирање или промјена PIN-а извршени успјешно. Безбиједносни статус не задовољава Терминал није овлашћен да изврши деблокирање или промјену ПИН-а.	

Напомена: Пошто је CAN лозинка која се не може блокирати, деблокирање CAN-а није неопходно. Међутим, чип MRTD-а МОЖЕ подржавати промјену PIN-а.

Б.11.10. Activate

Команда Activate користи се за подешавање PIN-а у активно стање.

Команда		
INS	0x44	Activate
P1	0x10	Активирање PIN-а преко параметра P2.
P2		0x03: PIN
Подата		Одсуство
Одговор		
Подата	–	Одсуство
Статусни бајтови	0x9000 0x6982 остало	Нормална операција PIN подешен у активно стање. Безбиједносни статус не задовољава Терминал није овлашћен за промјену статуса PIN-а.

Б.11.11. Deactivate

Команда Deactivate користи се за подешавање PIN-а у деактивирано стање.

Команда		
INS	0x04	Deactivate
P1	0x10	Деактивирање PIN-а преко параметра P2.
P2		0x03: PIN
Податак		Одсуство
Одговор		
Податак	–	Одсуство
Статусни бајтови	0x9000 0x6982 остало	Нормална операција PIN подешен у деактивирано стање. Безбиједносни статус не задовољава Терминал није овлашћен за промјену стања PIN-а.

Ц. CV сертификати (нормативно)

Ц.1. Профил сертификата

КОРИСТИТИ самоописиве сертификате који се верификују путем картице(ЦВ сертификат) у складу са стандардом ISO 7816 (види[13], [14], [15]) и профил сертификата назначен у табели 17. Појединости везане за кодирање објеката података који се користе у профилу сертификата можете пронаћи у Додатку Д.2.

Ц.1.1. Идентификатор профила сертификата

Идентификатор профила сертификата указује на верзију сертификата. Верзија 1, као што је назначено у табели 17, идентификује се вриједношћу 0.

Ц.1.2. Референце сертификационог тијела

Референце сертификационог тијела користе се за идентификацију јавног кључа који се користи за верификацију потписа сертификационог тијела (CVCA или DV). Референце сертификационог тијела МОРАЈУ бити исте као референце носиоца сертификата у одговарајућем сертификату сертификационог тијела (Линк сертификат CVCA или DV сертификат). Појединости везане за референце сертификационог тијела можете пронаћи у Додатку А.6.1.

Ц.1.3. Јавни кључ

Појединости везане за кодирање јавног кључа можете пронаћи у Додатку Д.3.

Објекат података	Серт
CV Сертификат	м
Сертификационо тијело	м
Идентификатор профила сертификата	м
Референце сертификационог тијела	м
Јавни кључ	м
Референце носиоца сертификата	м
Образац ауторизације за носиоца сертификата	м
Дан ступања на снагу сертификата	м
Дан престанка важности сертификата	м
Екстензије сертификата	о
Потпис	м

Табела 9: ЦВ Профил сертификата

Ц.1.4. Референце носиоца сертификата

Референце носиоца сертификата користе се за идентификацију јавног кључа који се налази на сертификату. Појединости које се односе на референцу носиоца сертификата можете пронаћи у Додатку А.6.1.

Ц.1.5. Образац ауторизације за носиоца сертификата

Рола и ауторизације носиоца сертификата КОДИРА се у обрасцу ауторизације за носиоца сертификата. Овај образац представља низ који се састоји од сљедећих објеката података:

1. Идентификатора објекта који одређује врсту терминала и формат обрасца.
2. Дискреционог објекта података који кодира релативну ауторизацију, односно ролу и ауторизацију носиоца сертификата у односу на сертификационо тијело.

Садржај и евалуација обрасца ауторизације за носиоца сертификата описани су у Додатку Ц.4.

Ц.1.6. Дан ступања на снагу/престанка важности сертификата

Указује се на период важности сертификата. Дан ступања на снагу сертификата МОРА бити дан генерисања сертификата.

Ц.1.7. Екстензије сертификата за аутентикацију терминала, верзија 2

Сертификати терминала за његову аутентикацију (види Додатак Ц.4.2.) МОГУ садржати екстензије како је дефинисано у Додатку Ц.3.

Ц.1.8. Потпис

Потпис на сертификату КРЕИРА се путем кодираног дијела сертификата (односно, обухватиће таг и дужину).Референце сертификационог тијела ИДЕНТИФИКУЈЕ јавни кључ који се користи за верификацију потписа.

Ц.2. Сертификациони захтјеви

Сертификациони захтјеви су скраћени CV сертификати који могу носити додатни потпис. ТРЕБА користити профил сертификационог захтјева назначен у табели 18. Појединости везане за кодирање објеката података који се користе у профилу сертификационог захтјева можете пронаћи у Додатку Д.2.

Ц.2.1. Идентификатор профила сертификата

Верзију профила идентификује идентификатор профила сертификата.Верзија 1 идентификује се вриједношћу 0како је дато у табели 18.

Ц.2.2. Референце сертификационог тијела

Референце сертификационог тијела ТРЕБА користити за информисање сертификационог тијела о приватном кључу који апликант **очекује** да ће се користити за потписивање сертификата. Уколико референце сертификационог тијела које су обухваћене захтјевом одступају од референци сертификационог тијела садржаног у издатом сертификату (односно, издати сертификат је потписан јавним кључем који апликант **не очекује**),одговарајући сертификат сертификационог тијела ТРЕБА, такође, доставити апликанту као одговор.

Појединости о референцама сертификационог тијела можете пронаћи у Додатку А.6.1.

Ц.2.3. Јавни кључ

Појединости везане за кодирање јавних кључева можете пронаћи у ДодаткуД.3.

Податакобјекта	Захт.
Аутентикација	ц
CV сертификат	м
Сертификационо тијело	м
Идентификатор профила сертификата	м
Референце сертификационог тијела	р
Јавни кључ	м
Референце носиоца сертификата	м
Екстензије сертификата	о
Потпис	м
Референце сертификационог тијела	ц
Потпис	ц

Табела 10: ЦВ профил сертификационог захтјева

Ц.2.4. Референце носиоца сертификата

Референца носиоца сертификата користи се за идентификацију јавног кључа који се налази у захтјеву и одговарајућег сертификата. Појединости везане за носиоца сертификата можете пронаћи у Додатку А.6.1.

Ц.2.5. Екстензије сертификата за аутентикацију терминала, верзија 2

Сертификациони захтјеви терминала за аутентикацију (види ДодатакЦ.4.2.)МОГУ садржати екстензије као што је дефинисано у ДодаткуЦ.3.

Ц.2.6. Потпис(-и)

Сертификациони захтјев може имати два потписа, *унутрашњи* и *вањски*:

Унутрашњипотпис
(ЗАХТЈЕВА СЕ)

Сертификационо тијело је самопотписиво, односно, ПОТРЕБНО је да се унутрашњи потпис може верификовати јавним кључем који се налази у сертификационом захтјеву. ПОТРЕБНО је да потпис буде креиран путем кодираног дијела сертификата (односно, да обухвати таг и дужину).

Вањскипотпис **(УСЛОВЉЕНО)**

- Потпис је ОПЦИОНИ ако субјекат аплицира за иницијални сертификат. У том случају захтјев МОЖЕ додатно потписати други субјекат којем пријемно сертификационо тијело то повјери (нпр. државно CVCA може извршити аутентикацију захтјева DV који је послат страном CVCA).
- Потпис се ЗАХТИЈЕВА уколико субјекат аплицира за додатни сертификат. У том случају, захтјев МОРА додатно потписати апликант користећи недавно генерисани пар кључева који је претходно регистрован код пријемног сертификационог тијела.

Уколико се користи вањски потпис, КОРИСТИ се објекат података за аутентикацију да би се смјестили сертификат CV (захтјев), референце сертификационог тијела и додатни потпис. Референце сертификационог тијела ИДЕНТИФИКУЈУ јавни кључ који се користи за верификацију додатног потписа. ПОТРЕБНО ЈЕ да потпис буде креиран увезивањем кодираног CV сертификата *и* кодиране референце сертификационог тијела (односно, да обухвати и таг и дужину).

Податакобјекта
Екстензије сертификата
Дискрециони образац за податке
Идентификатор објекта
Објекат података карактеристичан за контекст 1
...
Објекат података карактеристичан за контекстн
Дискрециони образац за податке
Идентификатор објекта
Објекат података карактеристичан за контекст 1
...
Објекат података карактеристичан за контекстм
...

Табела 11: Екстензије сертификата

Ц.3. Екстензије сертификата за аутентикацију терминала, верзија 2

Екстензија сертификата представља низ образаца са дискреционим подацима, гдје сваки образац са дискреционим подацима ТРЕБА садржати низ сљедећих објеката података приказаних и у табели 19:

1. Идентификатор објекта који одређује садржај и формат екстензије.
2. Један или више објеката података карактеристичних за контекст који садрже кодирану екстензију.

Сљедећи идентификатор објекта базе користи се за идентификовање екстензија сертификата дефинисаних у наставку:

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

Напомена:Процедура за валидацију сертификата описана у Дијелу 2.5.1 не узима у обзир екстензије сертификата. Због тога, екстензије не представљају критичне особине и чип MRTD-а НЕ СМИЈЕ одбити сертификат због непознатих екстензија. Непознате екстензије и екстензије које нису значајне за чип MRTD-а не треба импортовати.

Ц.3.1. Опис сертификата

За ову екстензију ТРЕБА користити сљедећи идентификатор објекта:

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

Сљедећи објекат података карактеристичан за контекст користи се за кодирање описа сертификата:

- 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
}
```

Скуп `commCertificates` МОЖЕ садржати хеш вриједности прихватљивих сертификата X.509 удаљеног терминал. Хеш функцију која се користи ДЕФИНИШЕ хеш функција којом се потписују сертификати CV. Инпут за хеш функцију је одговарајући сертификат DER-кодиран X.509 који обухвата и таг и дужину. Хеш функцију која се користи за генерисање садржаја екстензије ДЕФИНИШЕ хеш функција за потписивање сертификата.

Напомена: Локални терминал користи опис сертификата као дио интеракције корисника за onlajn аутентикацију удаљеног терминала (види Дио 2), а чип MRTD-а га може игнорисати.

Ц.3.1.1. Формат простог текста

Сљедећи идентификатор објекта КОРИСТИ се за идентификовање услова кориштења у формату простог текста:

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

2.7.6.1 Ц.3.1.2Формат ХТМЛ

Сљедећи идентификатор објекта КОРИСТИ се за идентификовање услова кориштења у формату HTML:

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

2.7.6.2 Ц.3.1.3. Формат PDF

Сљедећи идентификатор објекта КОРИСТИ се за идентификовање услова кориштења у формату PDF[11]:

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

Ц.3.2. Сектор терминала

Сљедећи идентификатор објекта КОРИСТИ се за ову екстензију:

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

Сљедећи објекти података карактеристични за контекст користе се за кодирање сектора терминала:

- 0x80:Хеш јавног кључа објекта података сектора 1(види ДодатакД.3).
- 0x81:Хеш јавног кључа објекта података сектора 2(види ДодатакД.3).

Хеш функцију која се користи дефинисаће хеш функција за потписивање сертификиата. Сам јавни кључ није обухваћен сертификатом и терминал га МОРА обезбједити као дио ограничене идентификације.

Чип MRTD-а израчунава хеш путем примљеног јавног кључа и пореди га са примљеним хешом.

Напомена: Таговање карактеристично за контекст користи се за јавни кључ приликом ограничене идентификације(види Додатак Б.4.1). Чип MRTD-аМОРА замијенити таговање карактеристично за контекст 0xA0 таговањем карактеристичним за апликацију 0x7F49 прије израчунавања хеш вриједности.

Ц.4. Роле и нивои ауторизација

Сљедећи идентификатор објекта КОРИСТИ се за идентификацију рола и нивоа ауторизације различитих врста терминала:

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

Напомена: Приступна права могу бити проглашена *правима резервисаним за будућу употребу (RFU)*. Таква приступна права могу бити додијељена у наредним

верзијама овог Техничког упутства. Као посљедица тога, чип MRTD-а који је већ издат мора унијети сертификате са неочекиваном ауторизацијом носиоца сертификата. Захваљујући прорачуну приступних права, описаном у Дијелу 2.6, важећа ауторизација ће увијек ограничавати приступна права која су чипу MRTD-а позната у вријеме персонализације.

Ц.4.1. Инспекцијски системи

Сљедећи идентификатор објекта КОРИСТИ се за инспекцијске системе:

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

Релативна ауторизација носиоца сертификата кодирана је једним бајтом који се тумачи као бинарна растер мапа, што је представљено у табели 20. За више појединости, ова битмапа садржи роле и приступна права. Обоје зависе од ауторизација свих претходних сертификата у ланцу.

7 6	5 4 3 2 1 0	Опис
x x	- - -	Рола
1 1	- - -	CVCA
1 0	- - -	DV(званични домаћи)
0 1	- - -	DV(званични страни)
0 0	- - -	Инспекцијски системи
-	x x x x x x	Приступна права
-	x x x x - -	RFU
-	- - - - 1 -	Очитати приступ апликацији за електронски пасош:DG 4 (зјеница ока)
-	- - - - - 1	Очитати приступ апликацији за електронски пасош:DG 3 (отисак прста)

Табела 12: Ауторизације инспекцијских система

Овлашћени инспекцијски систем увијек ће ОЧИТАТИ приступ мање осјетљивим групама података (нпр.DG1,DG2,DG14) у апликацији за електронски пасош. Тај систем би, такође, ТРЕБАО очитати приступ свим групама података апликације за електронске личне карте.

Ц.4.2. Терминали за аутентикацију

Сљедећи идентификатор објекта КОРИСТИ се за терминале за аутентикацију:

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

Релативне ауторизације носиоца сертификата кодиране су с пет бајтова који се тумаче као бинарна растер мапа као што је приказано у табели 21. За више појединости, ова битмапа садржи роле и приступна права. Обоје зависе од ауторизација свих претходних сертификата у ланцу.

Овлашћени терминал за аутентикацију увијек ИМА приступ сљедећим функцијама:

39 38	37 … 33	32 ... 29	28 ... 8	76543210	Опис

x x	- - -	- - -	- - -	- - - - - - - -	Рола
11	- - -	- - -	- - -	- - - - - - - -	CVCA
1 0	- - -	- - -	- - -	- - - - - - - -	DV (званични домаћи)
01	- - -	- - -	- - -	- - - - - - - -	DV(незванични-званични/страни)
0 0	- - -	- - -	- - -	- - - - - - - -	Терминал за аутентикацију
	x x x	- - -	- - -	- - - - - - - -	Приступ писању (еЛК)
- -	1 - -	- - -	- - -	- - - - - - - -	DG 17
- -	- ... -	- - -	- - -	- - - - - - - -	…
- -	- - 1	- - -	- - -	- - - - - - - -	DG 21
- -	- - -	x x x	- - -	- - - - - - - -	RFU: Приступ читању/писању
- -	- - -	- - -	x x x	- - - - - - - -	Приступ читању(еЛК)
- -	- - -	- - -	1 - -	- - - - - - - -	DG 21
- -	- - -	- - -	- ... -	- - - - - - - -	…
- -	- - -	- - -	- - 1	- - - - - - - -	DG 1
	- - -	- - -	- - -	x x x x x x x x	Посебне функције
- -	- - -	- - -	- - -	1 - - - - - - -	Инсталирати квалификован сертификат
- -	- - -	- - -	- - -	- 1 - - - - - -	Инсталирати сертификат
- -	- - -	- - -	- - -	- - 1 - - - - -	Управљање ПИН-ом
- -	- - -	- - -	- - -	- - - 1 - - - -	Дозвољени ЦАН
- -	- - -	- - -	- - -	- - - - 1 - - -	Привилеговани терминал
- -	- - -	- - -	- - -	- - - - - 1 - -	Ограничена идентификација
- -	- - -	- - -	- - -	- - - - - - 1 -	Идентификациони бр.
- -	- - -	- - -	- - -	- - - - - - - 1	Потврда старости

Табела 13: Ауторизација терминала за аутентикацију

- Ограничена идентификација осим уколико чип MRTD-а не захтијева од терминала да буде овлашћен за коришћење функције (поставка `authorizedOnly` је активна, види ДодатакА.1.1.4)
- Верификација валидности документа

Ц.4.3. Терминали за потписивање

Сљедећи идентификатор објекта КОРИСТИ се за терминале за потписивање:

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

Релативна ауторизација носиоца сертификата кодирана је једним бајтом који се тумачи као бинарна растер мапа као што је приказано у табели 22. За више појединости, ова битмапа садржи роле и приступна права. Обоје зависе од ауторизација свих претходних сертификата у ланцу.

Ц.5. Сертификациона политика

ПРЕПОРУЧУЈЕ СЕ да свако CVCA тијело и сваки DV објави сертификациону политику и/или изјаву о сертификационој пракси.

Ц.5.1. Процедуре

Сертификационом политиком ТРЕБА одредити сљедеће процедуре:

- Идентификација субјекта, аутентикација и регистрација;
- Аплицирање, издавање и дистрибуција сертификата;
- Опоравак од квара или угрожавања приватности,
- Ревизија.

7 6	5 4 3 2 1 0	Опис
x x	------	Роле
1 1	- - - - - -	CVCA
1 0	- - - - - -	DV (Акредитационо тијело)
0 1	- - - - - -	DV (Провајдер услуга сертификовања)
0 0	- - - - - -	Терминал за потписивање
--	x x x x x x	Приступна права (електронски потпис)
- -	x x x x - -	RFU
- -	- - - - 1 -	Генерисати квалификован електронски
- -	- - - - - 1	Генерисати електронски потпис

Табела 14: Ауторизација терминала за потписивање

Ц.5.2. Ограничења коришћења

Сертификациона политика ТРЕБА одредити ограничења на уређајима који се користе за похрањивање/обраду одговарајућих приватних кључева и осталих осјетљивих (личних) података:

- Физичка и оперативна безбједност;
- Механизми контроле приступа;
- Евалуација и сертификација(нпр. заједнички критерији за заштиту профила);
- Заштита података.

Д. DER кодирање (норматив)

Истакнута правила кодирања (DER) према X.690 [17] КОРИСТЕ СЕ за кодирање обје ASN. 1 структуре података и података објекта (карактеристичне за апликације). Кодирање резултира структуром таг-дужина-вриједност (TLV), као што слиједи:

Таг: ознака кодирана у једном или два октета и указује на садржај.

Дужина: Дужина кодирана као непотписан цијели број (INTEGER) у једном, два или три октета резултираће максималном дужином од 65 535 октета. КОРИСТИ се минималан број октета.

Вриједност: Вриједност је кодирана у нула или више октета.

Д.1. ASN.1

Кодирање структура података дефинисано у ASN.1 синтакси описано је у X.690[17].

Д.2. Објекти података

Табела23 даје преглед тагова, дужина и вриједности објекта података који се користе у овој спецификацији.

Напомена: Tag 0x7F4C још увијек није дефинисан у ISO/IEC 7816. Захтијева се алокација.

Назив	Таг	Дужина	Вриједност	Коментар
Идентификатор објекта	0x06	V	Идентификатор објекта	–
Референце сертификационог тијела	0x42	16V	Знаковни низ	Идентификује јавни кључ сертификационог тијела које је издало сертификат.
Дискреционоподатак	0x53	V	Октетни низ	Садржи произвољне податке.
Референца носиоца сертификата	0x5F20	16V	Знаковни низ	Повезује јавни кључ који се налази на сертификату са идентификатором.
Дан престанка важности сертификата	0x5F24	6F	Датум	Датум након којег сертификат престаје важити.
Дан ступања на снагу сертификата	0x5F25	6F	Датум	Датум генерисања сертификата.
Идентификатор профила сертификата	0x5F29	1F	Непотписан цијели број	Верзија сертификата и формат захтјева за сертификатом.
Потпис	0x5F37	V	Октетни низ	Дигитални потпис који је израђен преко асиметричног криптографског алгоритма.

Екстензије сертификата	0x65	V	Низ	Смјешта екстензије сертификата.
Аутентикација	0x67	V	Низ	Садржи објекте података који се односе на аутентикацију.
Образац дискреционог податка	0x73	V	Низ	Смјешта произвољне објекте података.
CV сертификата	0x7F21	V	Низ	Смјешта сам сертификат и његов потпис.
Јавни кључ	0x7F49	V	Низ	Смјешта вриједности јавног кључа и параметара домена.
Образац за ауторизацију носиоца сертификата	0x7F4C	V	Низ	Кодира роле носиоца сертификата (односно,CVCA,DV, терминала) и додјељује приступна права за читање/писање.
Сертификат	0x7F4E	V	Низ	Смјешта објекте података сертификата.
F:фиксна дужина(тачно одређен број октета), V: Промјенљива дужина до одређеног броја октета)				

Табела 15: Преглед објекта података (сређених према таговима)

Д.2.1. Кодирање вриједности

Основне врсте вриједности које се користе у овој спецификацији су сљедеће: (непотписани) цијели број, тачке елиптичне криве, датуми, знаковни низови, октетни низови, идентификатори објекта и секвенце.

Д.2.1.1. Непотписани цијели бројеви

Сви цијели бројеви који се користе у овој спецификацији су непотписани цијели бројеви. Непотписан цијели број КОНВЕРТУЈЕ се у октетни низ путем бинарне репрезентације цијелог броја у формату података у којем је први дио најзначајнији (big-endian). КОРИСТИ се минималан број октета, односно НЕ СМИЈУ се користити водећи октети вриједности 0x00.

Напомена:Насупрот типу ASN.1, `INTEGER` је увијек потписан цијели број.

Д.2.1.2. Тачке елиптичне криве

Конверзија тачака елиптичне криве у октетне тачке назначена је у [3]. КОРИСТИ СЕ некомпресовани формат.

Д.2.1.3. Датуми

Датум је кодиран са 6 знакова $d_1|d_6$ у формату GGMMDD коришћењем временске зоне GMT. Конвертован је у октетни низ $o_1|o_6$ кодирањем сваког знака d_j у октет o_j као неупакован бинарно кодирани децимални број ($1 \leq j \leq 6$).

Година GG кодирана је са два знака и тумачи се као 20 GG, односно, година је дата у распону од 2000до2099.

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	Đ	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:Размак,NBSP: Размак без прекида,SHY:Мека цртица																

Табела 16: ISO/IEC 8859-1 Скуп карактера

Д.2.1.4. Знаковни низови

Знаковни низ $c_1|c_n$ представља спајање n карактера c_j при чему је $1 \le j \le n$. Потом се КОНВЕРТУЈЕ у октетни низ $o_1|o_n$ претварањем сваког знака c_j у o_j коришћењем скупа карактера из ISO/IEC 8859-1. Скуп карактера можете пронаћи у табели 24.

Шифре карактера 0x00-0x1F и 0x7F-0x9F су недодијељене и НЕ СМИЈУ СЕ користити. Конверзија октета у недодијељен знак РЕЗУЛТИРАЋЕ грешком.

Д.2.1.5. Октетни низови

Октетни низ $o_1|o_n$ представља спајање n октета o_j при чему је $1 \le j \le n$. Сваки октет o_j састоји се од 8 битова.

Д.2.1.6. Идентификатори објекта

Идентификатор $i_1.i_2.|.i_n$ кодиран је као списак n непотписаних цијелих бројева i_j гдје је $1 \le j \le n$. Потом се КОНВЕРТУЈЕ у октетни низ $o_1|o_{n-1}$ коришћењем сљедеће процедуре:

1. Прва два цијела броја i_1 и i_2 упакована су у један цијели број i који се онда конвертује у октетни низ o_1. Вриједност u рачуна се на сљедећи начин:

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

2. Преостали цијели бројеви i_j директно се конвертују у октетне низове o_{j-1} гдје је $3 \leq j \leq n$. Више појединости о кодирању можете пронаћи у[17].

Напомена:Непотписани цијели бројеви кодирани су као октетни низови коришћењем формата у којем је први дио најважнији (big-endian) као што је описано у Додатку Д.2.1.1, међутим, користе се само битови 1-7 сваког октета. Бит 8 (крајњибит) постављен као један користи се да би се означило да тај октет не представља посљедњи октет у ланцу.

Д.2.1.7. Секвенце

Секвенца $D_1 | D_n$ представља ранг листун објеката података D_j гдје је $1 \leq j \leq n$. Секвенца се КОНВЕРТУЈЕ у повезан списак октетних низова $O_1 | O_n$ кодирањем сваког објекта податка D_j у октетни низ O_j путем DER-а.

Д.3. Објекат података јавног кључа

Објекат података јавног кључа садржи секвенце идентификатора објекта и неколико објеката података карактеристичних за контекст:

- Идентификатор објекта је карактеристичан за апликацију и односи се не само на формат јавног кључа (односно, објекти података карактеристични за контекст), већ и на његову употребу.
- Објекте података карактеристичне за контекст дефинише идентификатор објеката, а садрже вриједности јавног кључа и параметре домена.

Формат објеката података јавног кључа који се користи у овој спецификацији описан је у наставку.

Д.3.1. Јавни кључеви RSA

Објекти података садржани у јавном кључу RSA приказани су у табели 25. Редослијед објеката података је фиксан.

Објекат података	Скраће	Таг	Врста	ЦВСертифика
Идентификатор објекта		0x06	Идентификатор објекта	м
Сложенимодул	n	0x81	Непотписан цијели број	м
Јавни експонент	e	0x82	Непотписан цијели број	м

Табела 17: Јавни кључ RSA

Д.3.2. Јавни кључеви Диффие Хеллман

Објекти података који се налазе у јавном кључу DH приказани су у табели 26. Редослијед објеката података је фиксан.

Објекат података	Скраћ.	Таг	Врста
Идентификатор објекта		0x06	Идентификатор објекта
Прости модули	p	0x81	Непотписан цијели број
Редослијед подгрупа	q	0x82	Непотписан цијели број
Генератор	g	0x83	Непотписан цијели број
Јавна вриједност	y	0x84	Непотписан цијели број

Табела 18: Јавни кључ ДХ

Д.3.3. Јавни кључеви елиптичне криве

Објекти података садржани у јавном кључу елиптичне криве приказани су у табели 27. Редослијед објеката података је фиксан, УСЛОВЉЕНИ параметри домена МОРАЈУ бити или сви присутни, осим додатног фактора, или сви одсутни, како слиједи:

Објекат података	Скраћ.	Таг	Врста	CV Сертификат
Идентификатор објекта		0x06	Идентификатор	m
Прости модули	p	0x81	Непотписан цијели	c
Први коефицијент	a	0x82	Непотписан цијели	c
Други коефицијент	b	0x83	Непотписан цијели	c
Тачка у бази	G	0x84	Тачка елиптичне	c
Редослијед тачке у	r	0x85	Непотписан цијели	c
Јавна тачка	Y	0x86	Тачка елиптичне	m
Додатни фактор	f	0x87	Непотписан цијели	c

Табела 19: Јавни кључеви елиптичне криве

- CVCA линк сертификати МОГУ садржати параметре домена.
- ДВи сертификати терминала НЕ СМИЈУ садржати параметре домена. Параметри домена ДВ и јавни кључ терминала УЗИМАЈУ се из одговарајућих јавних кључева CVCA.
- Сертификациони захтјеви МОРАЈУ садржати параметре домена.

Д.3.4. Привремени јавни кључеви

Формат и параметри домена привремених јавних кључева већ су познати. Према томе, само основна вриједност јавног кључа, односно, јавна вриједност *y* за јавне кључеве Diffie-Hellman и јавну тачку *Y* за јавне кључеве елиптичне криве, користи се за преношење привременог јавног кључа у објекат података карактеристичан за контекст.

E. Безбједна размјена порука (Норматив)

Безбједна размјена порука пружа безбједан (односно, криптован и аутентикован) канал између терминала и чипа MRTD-а. Безбједна размјена порука може се успоставити аутентикацијом чипа, путем PACE-а или основне контроле приступа. Осигурани безбиједносни ниво, међутим, зависи од механизама који се користе за постављање безбједне размјене података.

Сесија започиње успостављањем безбједне размјене порука. Сесија се завршава само онда када се напусти безбједна размјена порука, нпр. слањем команде без кориштења безбједне размјене порука. У току сесије кључеви за безбједну размјену порука (односно они успостављени аутентикацијом чипа, путем PACE-а или основне контроле приступа) могу бити измијењени.

Напомена: Чип MRTD-а МОЖЕ индиректно одабрати *master fajl* кад се сесија заврши.

Будући да ово Упутство разматра само команду APDU са инструкцијом парних бајтова, Додатак Ф узима у обзир искључиво безбједну размјену порука за парове команда/одговор при чему команда APDU има паран INS бајт.

E.1. Структура порука у безбједној размјени APDU

Објекти података из безбједне размјене порука КОРИСТЕ се према табели 28, сљедећим редослиједом:

- [DO‘87’] [DO‘97’] DO‘8E’
- Одговор [DO‘87’] DO‘99’ DO‘8E’

Сви објекти података из безбједне размјене порука КОДИРАЈУ се у DER (види Додатак Д.2). Стварна вриједност Лц модификоваће се у Лц’ након примјене безбједне размјене порука. Уколико је потребно, одговарајући објекат података може се уврстити у APDU дио податка да би се пренијела оригинална вриједност Le. У заштићеној команди APDU, *нови le* бајт ПОДЕШЕН је на ‘00’.

Напомена:Безбједна размјена порука МОРА бити назначена коришћењем првог бајта идентификатора команде (class bajt) CLA = ‘XC’, са bitmask X, при чему бит 8 (подешен на 0) указује на класу инструкције *interindustry class*, а бит 5 (подешен на 1) указује на промјену команде.

E.1.1. Команда APDU

Према томе, команда ће уз примјену безбједне размјене порука ИМАТИ сљедећу структуру, зависно од стања одговарајуће несигурне команде:

Назив	Таг	Дужин	Команда	Одговор
Индикатор попуњавања садржаја којег прати криптограм	0x87	V	c	c

ЗаштићениЛе	0x97	2V	c	x
Статус обраде	0x99	2F	x	m
Криптографски контролни збир	0x8E	8F	m	M
Ф: фиксна дужина (тачан број октета), В: промјењива дужина (до броја октета)				

Табела 20: Употреба објеката података за безбједну размјеу порука

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. ОдговорAPDU

Одговор путем безбједне размјене порука ИМА сљедећу структуру, зависно од стања одговарајуће несигурне команде:

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. Попуњавање

Подаци које треба криптовати ПОПУЊАВАЈУ се у складу са ISO 7816-4 [13] коришћењем индикатора 0x01. За израчунавање криптографског контролног збира APDU попуњава се у складу са ISO 7816-4 [13].

Напомена: Пуњење се увијек обавља у овојници за безбједну размјену порука, а не преко основног криптографског алгоритма.

E.1.4. Примјери

Дата су три примјера на крају овог дијела:

- Слика 4 приказује трансформацију незаштићене команде APDU у заштићену

команду APDU у случају да су податак и/или Le доступни. Уколико ниједан податак није доступан, изоставити дио DO ’87’. Ако Le није доступно, изоставити дио DO’97’.

- Слика 5 приказује трансформацију незаштићене команде APDU у заштићену команду APDU у случају када податак и Ле нису доступни.
- Слика 6 приказује трансформацију незаштићеног одговора APDU у заштићени одговор APDU у случају када је податак доступан. Ако ниједан податак није доступан, изоставити дио ДО ’87’.

E.2. Криптографски алгоритми

Безбједна размјена порука заснована је или на 3DES -у[21] или AEc-у[22] на начин прво криптовање, па потом аутентикација, односно, податак је прво криптован, а након тога се форматиран криптован податак уноси у прорачуне за аутентикацију. Сесијски кључеви ИЗВОДЕ се преко PACE-а или аутентикације чипа коришћењем деривативне функције описане у Додатку A.2.3.

Напомена: Ако команда не садржи командне податке, не примјењује се никакво криптовање команде. Ако одговор не садржи податке који се односе на одговор, никакво криптовање се не примјењује на одговор.

E.2.1. 3 DES

3DES дефинисано је у[21].

E.2.1.1.3DES криптовање

За криптовање порука КОРИСТЕ се два кључа 3DES у CBC-моду у складу са ISO10116[12]са кључем *K Enc and IV* *0.*

E.2.1.2. 3DES аутентикација

За аутентикацију порука 3DES се КОРИСТИ у малопродајном моду рада у складу са ISO/IEC 9797-1 [16] MAC алгоритам 3 са блок шифром DES , кључ $K_{МАЦ}$ и $ИВ = 0$. Групу података чија аутентикација се извршава ТРЕБА додати на почетак путем бројача послатих секвенци.

E.2.2. AES

AES је дефинисан у[22].

E.2.2.1. AES Енкрипција

За криптовање порука AES КОРИСТИ CBC-мод у складу са ISO 10116 [12] са кључем

K Enc i IV **E** K Enc , SSC).

E.2.2.2.AES Аутентикација

За аутентикацију порука AES КОРИСТИСМАС-мод[24] са K_{MAC} са MAC дужином

од 8 бајтова. Групу података чија аутентикација се извршава ТРЕБА додати на почетак путем бројача послатих секвенци.

E.3. Бројач послатих секвенци

Непотписан цијели број КОРИСТИ се као бројач послатих секвенци (SSC). Величина бита SSC-а ЈЕДНАКА је величини блок шифре која је коришћена за безбједну размјену порука, односно, 64 бита за 3DES и 128 бита за AES.

SSC се ПОВЕЋА сваки пут прије генерисања команде или одговора APDU-а, односно, ако је почетна вриједност *x*, у сљедећој команди вриједност SSC је *x* +1. Вриједност SSC за први одговор је *x* +2.

Уколико дође до рестартовања безбједне размјене порука, SSC се користи на сљедећи начин:

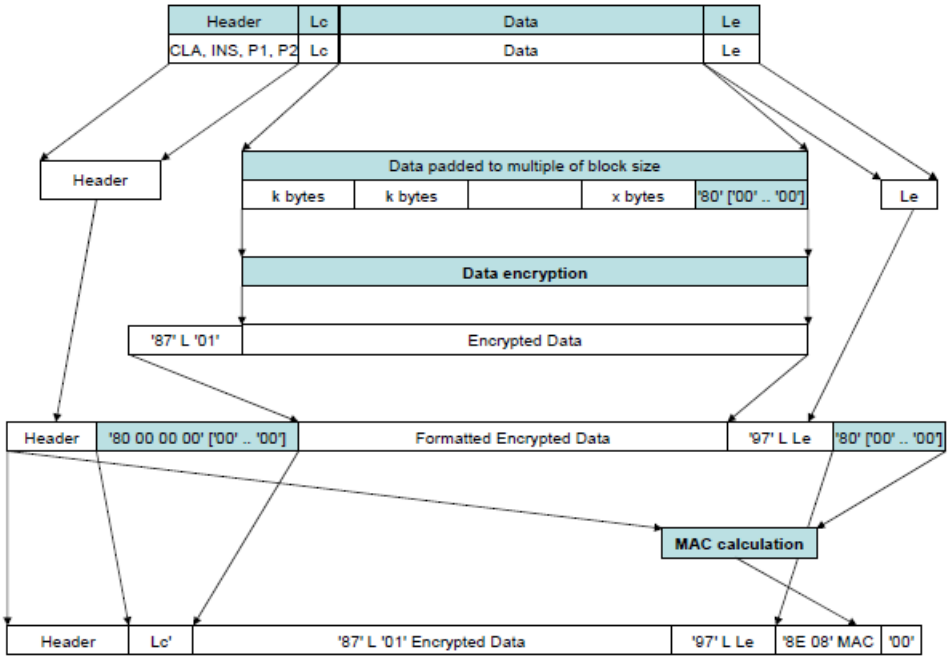
- Команде које се користе за слагање кључева заштићене су старим сесијским кључевима и старим SSC. Ово се нарочито односи на одговор посљедње команде која је коришћена за слагање сесијских кључева.
- Бројач послатих секвенци подешен је на своју нову почетну вриједност, односно у овој спецификацији SSC је подешен на 0.
- Нови сесијски кључеви и нови SSC користе се за заштиту наредних команди/одговора.

E.4. Грешке код безбједне размјене порука

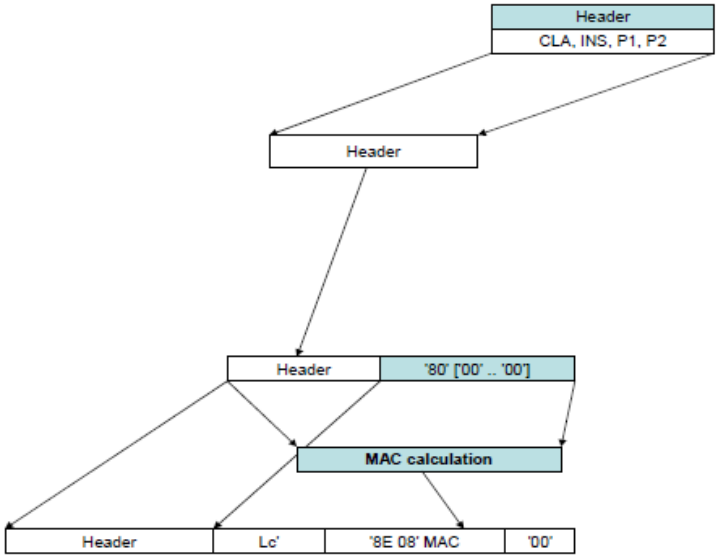
Чип MRTD-а МОРА напустити безбједну размјену података ако, и само ако, прими некодиран APDU или се појави грешка приликом безбједне размјене порука:

- Уколико недостају очекивани објекти података, чип MRTD-а ОДГОВАРА статусним бајтом 0x6987
- Уколико су очекивани објекти података нетачни, чип MRTD-а ОДГОВАРА статусним бајтом0x6988

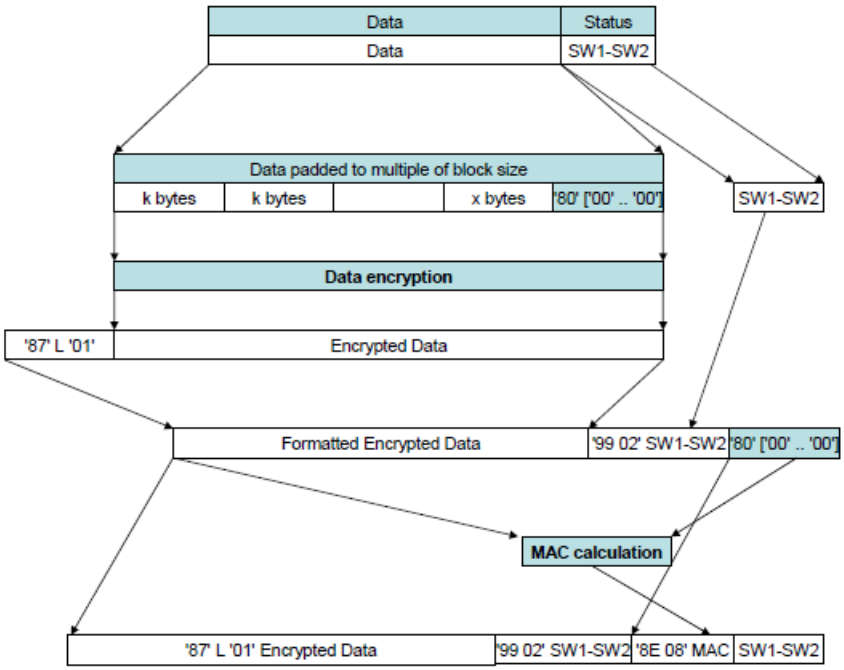
Уколико се напусти безбједна размјена порука, чип MRTD-а брише похрањене сесијске кључеве и успоставља почетне вриједности приступних права терминала.



Слика 4: Трансформација APDU команде



Слика 5: Трансформација APDU команде која не садрзи податке



Слика 6: Трансформација одговора на APDU команду

Литература

[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