Техничко упутство

Напредни безбједносни механизми за машински читљиве путне исправе

2. Дио – Проширена контрола приступа Верзија 2 (EACv2), “Password Authenticated Connection Establishment” (PACE) и ограничена идентификација(RI)

Бања Лука, 01.03.2013. године

Садржај

1 Увод

Систем електронских докумената је развијен на бази докумената Њемачког института за информационе технологије и IDDEEA се захваљује на доступности докумената на званичним сајтовима BSI.

Овај дио техничког упутства обухвата електронске безбједносне механизме за електронске путне исправе описане у Doc 9303 дио 3 том 2 [4] за заштиту аутентичности (укључујући интегритет), оригиналност и поузданост података који су сачувани на радио фреквентном чипу уграђеном у путну исправу (MRTD чип).

Напомена: Уколико се захтијева усклађеност са ICAO Doc 9303 [3], [4], Basic Access Control/PACE и Extended Access Control у верзији 1 (који укључује аутентификацију чипа, верзија 1 и аутентификацију терминала верзија 1) се МОРАЈУ користити (види 1. дио овог техничког упутства).

1.1 Захтјеви за MRTD чипове и терминале

Ово техничко упутство дефинише захтјеве за имплементацију MRTD чипова и терминала. Док се MRTD чипови морају ускладити са захтјевима у складу са терминологијом описаном у одјељку 1.2, захтјеви за терминале се морају тумачити као смјернице, тј. интероперабилност MRTD чипа и терминала је загарантована ако је терминал усклађен са тим захтјевима, иначе ће интеракција са MRTD чипом бити неуспјешна или ће понашање MRTD чипа бити недефинисано. У принципу, MRTD чип не треба спроводити захтјеве везане за терминале осим ако је безбједност MRTD чипа директно нарушена.

1.2 Терминологија

Кључне ријечи “МОРА”, “НЕ МОРА”, “ЗАХТИЈЕВАНО”, БИЋЕ”, “ НЕЋЕ БИТИ”, “ТРЕБА”, “НЕ ТРЕБА”, “ПРЕПОРУЧЕНО”, “МОЖЕ”, и “ОПЦИОНАЛНО” у овом документу се могу тумачити као што је описано у RFC 2119 [1]. Кључна ријеч “УСЛОВНО” ће се тумачити на слиједећи начин:

УСЛОВНО: Употреба једне ставке зависи од употребе других ставки. Стога је даље квалификовано под којим условима је ставка ЗАХТИЈЕВАНА или ПРЕПОРУЧЕНА.

Када се користи у табелама (профилима), кључне ријечи су скраћене што је приказано у табели 1.

Кључна ријеч		Скраћеница
МОРА/БИЋЕ	ЗАХТИЈЕВАНО	M
НЕ МОРА/НЕЋЕ БИТИ	–	X
ТРЕБА	ПРЕПОРУЧЕНО	R
МОЖЕ	ОПЦИОНАЛНО	O
–	УСЛОВNO	C

Табела 1: кључне ријечи 1

2 MRTD апликације

У оквиру овог поглавља су набројане електронске апликације које се налазе у машински читљивим документима.

2.1 Апликације

Ова спецификација подржава три апликације: *еПасош*, *eID* и *еПотпис*.

2.1.1 еПасош апликација

еПасош апликација је описана у 1. дијелу овог техничког упутства. Издавалац MRTD имплементиране у складу са овим дијелом овог техничког упутства МОЖЕ дефинисати услове приступа другачије од оних у дијелу 1. ПРЕПОРУЧУЈЕ се да се захтијева Extended Access Control чак и за мање осјетљиве податке.

2.1.2 eID апликација

eID апликација је дефинисана у Прилогу А и захтијева да се овјери терминал на слиједећи начин:

- Да би писали на eID апликацију, MRTD чип ЋЕ захтијевати да се овјери терминал као терминал за аутентификацију са ауторизацијом за писање одговарајућих група података eID апликације.
- Да би очитавали са eID апликације, MRTD чип ЋЕ захтијевати да се овјери терминал као
    - Терминал за аутентификацију са ауторизацијом да се очитавају све групе података са eID апликације или као
    - Инспекцијски систем који подразумијева ауторизацију за очитавање свих група података eID апликације.

Да би се овјерио терминал као терминал за аутентификацију или инспекцијски систем, MORA се користити Процедура опште аутентификације (види Одјељак 2.4).

2.1.3 еПотпис апликација

Ова спецификација не захтијева усклађеност са одређеним стандардом, али захтијева да се терминал овјери на слиједећи начин:

- За инсталирање еПотпис апликације, MRTD чип ЋЕ захтијевати да се терминал овјери као терминал за аутентификацију са посебном ауторизацијом за инсталирање еПотпис апликације.
- За коришћење еПотпис апликације да би се направили потписи, MRTD ЋЕ захтијевати да се овјери терминал као териминал за потпис.

Да би се овјерио терминал као терминал за аутентификацију или терминал за потпис, MORA се користити Процедура опште аутентификације (види Одјељак 2.4).

2.2 Типови терминала

Ова спецификација обухвата три типа терминала: инспекцијски систем, терминали за аутентификацију и терминали за потпис.

2.2.1 Инспекцијски систем

Поред спецификација наведених у 1. дијелу овог техничког упутства, овај дио обухвата дефинисање проширеног инспекцијског система који подржава Општу процедуру аутентификације (види одјељак 2.4).

> *Напомена: У наставку се инспекцијски систем увијек подразумијева као проширени инспекцијски систем.*

2.2.2 Терминал за аутентификацију

Терминал за аутентификацију је терминал који може да се користи од стране институција на нивоу БиХ (институција надлежна за верификацију докумената) или било које друге организације (сеслужбена / страна организација за верификацију докумената). MRTD чип ЋЕ захтијевати да се терминал за аутентификацију аутентификује како би се прије приступа утврдила аутентичност у складу са важећом ауторизацијом. Да би се аутентификовао терминал као терминал за аутентификацију, MORA се користити Општа процедура аутентификације (види Одјељак 2.4). Ниво ауторизације терминала за аутентификацију ЋЕ БИТИ одређен важећом ауторизацијом израчунатом из ланца цертификата.

2.2.3 Терминал за потпис

Терминал за потпис МОРА бити одобрен од стране надлежног овлаштеног органа или цертификацијског пружаоца услуга. MRTD чип ЋЕ захтијевати да се терминал за потпис аутентификује како би се прије приступа утврдила аутентичност у складу са важећом ауторизацијом. Да би се аутентификовао терминал као терминал за потпис, МОРА се користити Општа процедура аутентификације (види Одјељак 2.4). Ниво ауторизације терминала за потпис ЋЕ БИТИ одређен важећом ауторизацијом израчунатом из ланца цертификата.

2.2.4 Привилегован терминал

MRTD чип МОЖЕ бити персонализован тако да подржава и индивидуалне чип и генерички специфичне кључеве за аутентификацију чипа. У том случају, MRTD ЋЕ ограничити приступ индивидуалним чип кључевима на *привилеговане терминале.* MRTD чип МОРА сматрати слиједеће терминале као привилеговане терминале:

- Инспекцијски системи су увијек привилеговани терминали.
- Терминали за аутентификацију са важећом ауторизацијом „Privileged Terminal“ (3. Дио овог техничког упутства).

Терминали за потпис се никад НЕЋЕ сматрати привилегованим терминалима.

2.3 Шифре

Основна и проширена контрола приступа морају бити дефинисане да би се дозволило носиоцу MRTD да контролише приступ апликацијама имплементираним на бесконтактном MRTD чипу. Због ограничења основне контроле приступа, ова спецификација уводи PACE као сигурносни и практични механизам за ограничење приступа апликацијама на основу знања, тј. на основу шифри које су или одштампане на документу или познате само легитимном носиоцу документа.

Шифре подржане овим дијелом техничког упутства поред оних подржаних у 1. дијелу су:

PIN: Лични идентификациони број (PIN) је кратка тајна шифра која ЋЕ БИТИ позната једино легитимном носиоцу документа.

PUK: Лични број за деблокирање (PUK) је дуга тајна шифра која ЋЕ БИТИ позната једино легитимном носиоцу документа.

2.3.1 PIN

PIN је кратка тајна корисничка шифра која се користи за приступ eID апликацији или другим апликацијама. Употреба PIN-а је ЗАХТИЈЕВАНА за све терминале за аутентификацију, тј. једино легитимни носилац може дозволити терминалу за аутентификацију да приступи подацима на eID апликацији, осим ако терминал има важећу ауторизацију за приступ подацима eID апликације са CAN број.

PIN је шифра која се блокира, тј. PIN је повезан са бројачем понављања (RC) који се смањује за сваку неуспјешну аутентификацију. MRTD чип ЋЕ примијенити слиједећу процедуру блокирања како би се спријечило одбијање напада на сервисе:

RC = 0 MRTD чип ЋЕ *блокирати* PIN, тј. MRTD чип НЕ СМИЈЕ прихватити даље покушаје аутентификације користећи блокирани PIN. Да би се блокирани PIN *деблокирао* МОРА се користити процедура деблокирања како би се ресетовао одговарајући бројач понављања и гдје је могуће, подесио нови PIN.

2.3.2 PUK

PUK је дуга тајна корисничка шифра која се користи за приступ деблокираним механизмима PIN-а и шифрама специфичних апликација (нпр. локални PIN еПотпис апликације).

PUK је шифра која не блокира, тј. MRTD чип НЕ СМИЈЕ блокирати PUK након неуспјешних аутентификација. Међутим, МОЖЕ повезати PUK са бројачем корисника који се смањује са сваком успјешном аутентификацијом.

2.4 Процедура опште аутентификације

MRTD чип МОРА ограничити приступ eID апликацији и еПотпис апликацији терминалима који су аутентификовани општом процедуром аутентификације као проширеног инспекцијског система, терминала за аутентификацију и терминала за потпис у складу са важећом ауторизацијом.

Приступ еПасош апликацији МОРА бити ограничен инспекцијским системима, а процедуром опште аутентификације ПРЕПОРУЧЕНО је захтијевати да терминал буде аутентификован као проширени инспекцијски систем.

MRTD чип МОРА подржавати реаутентификацију терминала процедуром опште аутентификације након што је сесија (види одјељак. „Сигурно слање порука“ у 3. дијелу овог техничког упутства под дефиницијом „сесија“) завршена и терминал је изабрао Master File.

Процедура опште аутентификације се састоји од слиједећих корака:

1. PACE **(ЗАХТИЈЕВАНО)**

Терминал МОРА навести тип терминала и захтијевана права приступа као дио PACE-a. Уколико није наведено, MRTD чип МОРА накнадно одбити аутентификацију терминала верзија 2 .

- Инспекцијски систем ЋЕ користити CAN број или MRZ шифру.
- Терминал за аутентификацију ЋЕ користити PKIN. МОЖЕ користити CAN број уколико важећа ауторизација терминала одобро кориштење CAN броја („CAN број дозвољен).
- Терминал за потпис ЋЕ користити PIN; CAN број или PUK.

Ако је успјешно, MRTD чип предузима слиједеће:

- ПОЧЕЋЕ сигурно слање порука.

ОБЕЗБИЈЕДИТИ TRUST+POINTS за аутентификацију терминала

2. Аутентификација терминала верзија 2

(ЗАХТИЈЕВАНО)

Као дио терминала за аутентификацију, терминал обавља слиједеће:

- Терминал ЋЕ генерисати привремени јавни кључ који ће се касније *користити* за аутентификацију чипа. Терминал НЕ СМИЈЕ користити неверификоване доменске параметре за овај кључ, тј. једино стандардизовани параметри домена или параметри домена терминала који су сигурни могу бити кориштени.
- Терминал ЋЕ аутентификовати генерисани привремени јавни кључ.

Уколико је успјешно, MRTD чип обавља слиједеће кораке:

- ОДОБРИЋЕ приступ очитавању/писању групи података у складу са правима приступа терминалима.
- ОГРАНИЧИЋЕ она права приступа Сигурном слању порука који је успостављен аутентификованим привременим јавним кључем (осим одговарајући објекат безбједности).

3. Пасивна аутентификација **(ЗАХТИЈЕВАНО)**

Терминал обавља слиједеће:

- Терминал ЋЕ очитавати и верификовати одговарајући безбједносни објекат.
- Терминал ЋЕ упоредити несигурне SecurityInfos очитане прије PACE-a са сигурним садржајем објекта безбједности.

4. Аутентификација чипа верзија 2
(ЗАХТИЈЕВАНО)

MRTD чип ЋЕ ресетовати сигурну размјену порука.

Терминал за аутентификацију може одабрати и користити апликацију(е) у складу са важећом ауторизацијом терминала.

Напомена: Терминал и MRTD чип МОРАЈУ користити успостављени безбједносни контекст (тј. сигурна размјена порука установљена аутентификацијом чипа) за сву даљу комуникацију.

2.4.1 Онлајн аутентификација

eID апликација се такође може користити онлајн, тј. MRTD чип и терминал за аутентификацију су повезани мрежом. У том случају разликујемо *локални терминал* и *удаљени терминал*:

Удаљени терминал: Удаљени терминал је ауторизован за приступ eID подацима. Он пружа локалном терминалу ланац цертификата аутентификације терминала и дигитални потпис креиран на упиту MRTD чипа са одговарајућим тајним кључем.

Локални терминал: Локални терминал повезује корисника са MRTD чипом и удаљеним терминалом али није ауторизован за приступ eID подацима. Ланац цертификата аутентификације терминала примљен од удаљеног терминала је приказан кориснику и само ако то корисник прихвата, локални терминал прослиједјује примљене цертификате MRTD чипу.

Напомена: Једино након аутентификације чипа када је успостављена сигурна end-to-end веза између MRTD чипа и удаљеног терминала, MRTD чип одобрава приступ eID подацима.

2.5 Управљање PIN-ом

PIN и CAN су једине шифре (коришћене за PACE) које се могу мијењати. PIN је једина шифра која може имати статусе суспендован и блокиран. Поред тога, PIN може имати статусе активиран и деактивиран. Преостале шифре (PUK и MRZ) су статичне и не могу блокирати. Детаљно коришћење шифри је појашњено у одјељку 2.3.

Управљање PIN-ом се састоји од слиједећих операција:

- Промјена CAN-а
- Промјена PIN-а
- Обнова PIN-а
- Деблокирање PIN-а
- Активирање PIN-а
- Деактивирање PIN-а

Мапирање механизмима управљања PINом као што су промијенити CAN, промијенити PIN, одблокирати PIN, активирати PIN, деактивирати PIN према директивама ISO 7816 су дата у 3. дијелу овог техничког упутства. Операција обновити PIN није мапирана према директиви ISO 7816 јер то имплицитно врши MRTD чип.

2.5.1 Неаутентификовани терминали

Терминал је *неаутентификован* прије успјешног завршавања аутентификације терминала. Неаутентификовани терминали могу обављати операције управљања PIN-ом како слиједи:

1. PACE (ЗАХТИЈЕВАНО)

Терминал НЕ ТРЕБА означавати врсту терминала и захтјевана права приступа ако терминал остаје неаутентификован. Терминал може изабрати CAN, PIN или PUK као шифру за PACE.

Уколико је успјешно, MRTD чип обавља слиједеће:

- ПОЧЕЋЕ сигурну размјену порука.
- Ако је PIN у функцији (тј. активиран, и није суспендован или блокиран) и ако је правилно употријебљен, MRTD чип обавља слиједеће:
  - ПОНИШИЋЕ број понављања PIN-а.
  - ОДОБРИЋЕ приступ слиједећем механизму управљања PIN-а : промјена PIN-а.
- Уколико је CAN правилно употријебљен:
  - Привремено ЋЕ обновити PIN.
- Уколико је PUK правилно употријебљен:
  - ОДОБРИЋЕ приступ слиједећем механизму управљања PIN-а: деблокирање PIN-а.
  - МОЖЕ одобрити приступ слјиедећем механизму управљања PIN-а: промјена PIN-а.

2. PACE са PIN-ом (ОПЦИОНАЛНО)

Овај корак се ЗАХТИЈЕВА у слиједећим случајевима:

- обнављање PIN-а.
- наставак процедуре за општу аутентификацију након управљања PIN-ом. У том случају терминал МОРА означити тип терминала (терминала за аутентификацију) и неопходна права приступа.1

Ако је PIN успјешно употријебљен и ако је функционалан и привремено обновљен, MRTD чип ће обавити слиједеће:

- Ако је PIN привремено обновљен, обновиће PIN.
- РЕСЕТОВАЋЕ бројач понављања PIN-а.
- ОДОБРИЋЕ приступ слиједећем механизму управљања PIN-а: промјена PIN-а.

[1] Углавном је то случај када се CAN користи да би се обновио PIN као дио процедуре за општу аутентификацију.

3. Управљање PIN-ом
(ОПЦИОНАЛНО)

Овај корак се ЗАХТИЈЕВА код промјене или деблокирања PIN-а.

MRTD чип ће обавити слиједеће:

- ДОЗВОЛИЋЕ терминалу да изврши слиједеће операције управљања PIN-ом:
  - Промјена PIN-а,ако терминал има приступ овој операцији.
  - Деблокирање PIN-а, ако терминал има приступ овој операцији.

Уколико је PUK повезан са бројачем корисника, он НЕ СМИЈЕ истећи а MRTD чип ЋЕ смањити бројач корисника или након успјешног извођења PACE протокола или након извршавања операције деблокирање PIN-а.

Напомена: Подршка за операцију промјена PIN-а управљања PIN-ом ако је кориштен PACE са PUK-ом је ОПЦИОНАЛНА а имплементација специфична.

2.5.2 Терминали за аутентификацију

Аутентификовани терминали са важећом ауторизацијом за управљање PIN-ом (види 3. дио овог техничког упутства) могу извршавати слиједеће операције управљања PIN-ом:

1. Процедура опште аутентификације
(ЗАХТИЈЕВАНО)

Ако је терминал аутентификован као терминал за аутентификацију са важећом ауторизацијом за управљање PIN-ом, MRTD чип врши слиједеће:

- ДОЗВОЛИЋЕ приступ механизмима управљања PIN-ом.

2. Управљање PIN-ом **(ЗАХТИЈЕВАНО)**

MRTD чип врши слиједеће:

- МОЖЕ дозволити терминалу обављање слиједећих операција управљања PIN-ом :
  - Промјена PIN-а
  - Промјена CAN-а
  - Деблокирање PIN-а
- МОРА дозволити терминалу обављање слиједећих операција управљања PIN-ом :
  - Активирање PIN-а
  - Деактивирање PIN-а

Напомена: Подршка за операцију управљања PIN-ом промјена PIN-а и промјена CAN-а је ОПЦИОНАЛНА а имплементација специфична.

2.6 MRTD-ови са екраном

Ако је MRTD чип опремљен екраном, MRTD чип ће користити екран на слиједећи начин:

- ПРИКАЗАЋЕ селектовану апликацију.
- Динамично ЋЕ изабрати и приказати CAN.
- ПРИКАЗАЋЕ идентификацију аутентификованог терминала и важећу ауторизацију.
- МОЖЕ приказати промјенљиве податке eID апликације, нпр. мјесто пребивалишта.

3 Спецификације протокола

У овом поглављу су наведени криптографски протоколи PACE, аутентификацију чипа и терминала преузимајући арбитрарну комуникацијску структуру. Мапирање према ISO 7816 наредби је дато у 3. дијелу овог техничког упутства.

3.1 Криптографски алгоритми и нотација

Протоколи који су извршени између двије стране: MRTD чип (PICC) и терминал (PCD). Табела 2. даје приказ коришћених парова кључева. Коришћене криптографске операције и нотације су наведене у наставку.

3.1.1 Хеш и компресивни алгоритми

Операције рачунања криптографског хеша и компресивног јавног кључа су описане на засебан алгоритамски начин.

3.1.1.1 Операције

- операција за рачунање хеша преко поруке *m* је означена са $\mathbf{H}(m)$.
- операција за рачунање компресоване репрезентације јавног кључа PK је означена са $\mathbf{Comp}(PK)$.

Протокол	MRTD Чип	Терминал	Напомена
PACE	$\widetilde{PK_{PICC}}$, $\widetilde{SK_{PICC}}$	$\widetilde{PK_{PCD}}$, $\widetilde{SK_{PCD}}$	Сви парови кључева су привремени парови кључева.
Аутентификација чипа	PK_{PICC}, SK_{PICC}	$\widetilde{PK_{PCD}}$, $\widetilde{SK_{PCD}}$	Пар кључева које терминал користи је привремени пар кључева различит од привременог PACE пара кључева.
Аутентификација терминала	PK_{CVCA}	PK_{PCD}, SK_{PCD}	MRTD чип верификује ланац цертификата запримљен од терминала користећи CVCA.
Ограничена идентификација	SK_{ID}	PK_{SECTOR}	MRTD чип НЕ ТРЕБА доставити јавни кључ PK_{ID}, терминал НЕ СМИЈЕ имати одговарајући приватни кључ SK_{Sector}. Кључеви PK_{ID} и SK_{Sector} су коришћени екстерно за генерисање опозивних листа.

Табле 2: преглед коришћених парова кључева

3.1.2 Алгоритми са симетричним кључем

Кључеви и операције за симетричну енкрипцију кључа и аутентификацију су описани на засебан алгоритамски начин.

3.1.2.1 Кључеви

Симетрични кључеви су изведени из заједничког тајног K и ОПЦИОНАЛНОГ r или из шифре π користећи функцију извођења кључа (DKF):

- Извођење кључа за енкрипцију порука је означено са $K_{Enc} = \mathbf{KDF_{Enc}}(K, [r])$.
- Извођење кључа за аутентификацију порука је означено са $K_{MAC} = \mathbf{KDF_{MAC}}(K, [r])$.
- Извођење кључа из шифре је означено са $K_{\pi} = \mathbf{KDF}_{\pi}(\pi)$.

3.1.2.2 Операције

Операције за енкрипцију и декрипцију порука су означене на слиједећи начин:

- Енкрипција текста који се шифрује *m* са кључем K_{Enc} је означено са $c = \mathbf{E}(K_{Enc}, m)$.
- Декрипција шифрованог текста *c* са кључем K_{Enc} је означено са $m = \mathbf{D}(K_{Enc}, c)$.

Операција за рачунање аутентификацијског кода *T* на поруци *m* са кључем K_{MAC} је означено са

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

3.1.3 Договор кључева

Кључеви и операције за договор кључева су описане на засебан алгоритамски начин. Мапирање према DH и ECDH се може пронаћи у 3. дијелу овог техничког упутства.

3.1.3.1 Кључеви

Слиједећи парови кључева се користе за PACE и аутентификацију чипова:

- За PACE, MRTD чип и терминал генеришу привремене Дифи-Хелман парове кључева на основу привремених домена параметара $\widetilde{D}$.
  - Привремени јавни кључ MRTD чипа је $\widetilde{PK_{PICC}}$, одговарајући тајни кључ је $\widetilde{SK_{PICC}}$.
  - Привремени јавни кључ терминала је $\widetilde{PK_{PCD}}$, одговарајући тајни кључ је $\widetilde{SK_{PCD}}$.
- За аутентификацију чипа, MRTD чип користи статичан Дифи-Хелман пар кључева и терминал генерише привремени јавни кључ на основу домена параметара DPICC MRTD чипа.
  - Привремени јавни кључ MRTD чипа је PK_{PICC}, одговарајући тајни кључ је SK_{PICC}.
  - Привремени јавни кључ терминала $\widetilde{PK_{PCD}}$, одговарајући тајни кључ је $\widetilde{SK_{PCD}}$.
  - Компресовани привремени јавни кључ терминала је означен са **Comp(**$\widetilde{PK_{PCD}}$).
- За ограничену идентификацију MRTD чип користи статични Diffie-Hellman пар кључева и терминали у оквиру сектора користе (скоро) статичан Дифи-Хелманпар кључева гдје је приватни кључ терминалу непознат.
  - Статични јавни кључ MRTD чипа је PK_{ID}, одговарајући тајни кључ је SK_{ID}.
  - Статични јавни кључ сектора је PK_{Sector}, одговарајући тајни кључ је SK_{Sector}.
  - Опозивни јавни кључ сектора је $PK_{Revocation}$, одговарајући тајни кључ је $SK_{Revocation}$.
  - Специфични секторски идентификатор је $I^{Sector.}$.

ПРЕПОРУЧЕНО је да MRTD чип тестира јавне кључеве добијене од терминала.

Напомена: Терминал ће морати користити различите привремене јавне кључеве за PACE и аутентификацију чипа. С обзиром на то да су привремени јавни кључеви у контексту специфични, користе се иста нотација.

3.1.3.2 Операције

Операције за генерисање заједничких јавних кључева K је означена са $K = \mathbf{KA}(SK, PK, D)$, гдје је SK (привремени или статични) тајни кључ, PK (привремени или статични) јавни кључ и D (привремени или статични) су параметри домена.

3.1.4 Потписи

Кључеви и операције за потписе су описани на засебан алгоритамски начин. Мапирање према RSA и ECDSA се може пронаћи у 3. дијелу овог техничког упутства.

3.1.4.1 Кључеви

За аутентификацију терминала се користе слиједећи пар кључева:

- Терминал има статичан пар кључева за аутентификацију. Јавни кључ је PK_{PCD}, одговарајући тајни кључ је SK_{PCD}.

3.1.4.2 Операције

Операције за потписивање и верификовање поруке су означене како слиједи:

- Потписивање поруке m са приватним кључем SK_{PCD} је означено са $s = \mathbf{Sign}(SK_{PCD}, m)$.
- Верификовање насталог потписа sса јавним кључем PK_{PCD} је означено са $\mathbf{Verify}(PK_{PCD}, s, m)$.

3.2 PACE

PACE протокол је шифром аутентификован Дифи-Хелманов протокол договора кључева који пружа сигурну комунуикацију и експлицитну аутентификацију MRTD чипа и терминала на основу шифре (MRTD чип и терминал дијеле исту шифру π).

Овај протокол успоставља сигурну размјену порука између MRTD чипа и терминала на основу слабе (кратке) шифре. PACE је алтернатива за основну контролу приступа (BAC), тј. омогућава да MRTD чип верификује да је терминал ауторизован за приступ сачуваним мање осјетљивим подацима али има двије предности:

- Јаки кључеви сесије су обезбијеђени независно од јачине шифре
- Ентропија шифре(и) кориштених за аутентификацију терминала може бити веома слаба (нпр. 6 цифара је у суштини довољно).

Напомена: Постоје двије верзије овог протокола које се разликују у контексту токена за аутентификацију. Привремени параметри домена генерисани у протоколу су дио токена за аутентификацију у верзији 1. Они су уклоњени у верзији 2 јер интегрисано мапирање назначено у [5] захтијева да привремени параметри домена остану тајни. Да би се користила PACE верзија 1 са интегрисаним мапирањем, MAC МОРА додатно заштитити повјерљивост поруке. Верзија 1 овог протокола је тако застарјела и ПРЕПОРУЧЕНО је користити верзију 2.

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

Слика 1: PACE

3.2.1 Спецификација протокола

Терминал и MRTD чип врше слиједеће кораке а поједностављена верзија је такође приказана на слици 1:

1. MRTD чип насумично и једнообразно бира једнократни случајни број (nonce) s, шифрује nonce број $z = E(K_\pi, s)$ гдје је $K_\varnothing = \mathbf{KDF_\pi}(\pi)$ изведено из заједничке шифре π, и шаље текст за енкрипцију z заједно са статичким параметрима домена D_{PICC} ка терминалу.
2. Терминал обнавља текст који се шифрује $s = \mathbf{D}(K_\pi, z)$ уз помоћ заједничке шифре π.
3. MRTD чип и терминал изводе слиједеће кораке:

   а) Они израчунавају привремене параметре домена $\tilde{D} = Map(D_{PICC}, s)$

   б) Они изводе анонимни Дифи-Хелманов договор кључева на основу привремених параметара домена и генеришу заједничке тајне

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

   ц) Током Дифи-Хелмановог договора кључева, свака страна ТРЕБА провјерити да се два јавна кључа $\widetilde{PK_{PICC}}$ и $\widetilde{PK_{PCD}}$ разликују.

   д) Они изводе кључеве сесије $K_{MAC} = \mathbf{KDF_{MAC}}(K)$ и $K_{Enc} = \mathbf{KDF_{Enc}}(K)$.

e) Они размјењују и верификују токене за $T_{PCD} = MAC(K_{MAC}, \widetilde{PK_{PICC}})$ и $T_{PICC} = MAC(K_{MAC}, \widetilde{PK_{PCD}})$

3.2.2 Статус безбједности

Уколико је PACE успјешно обављен онда је MRTD чип верификовао кориштену шифру. Сигурна размјена порука је започета коришћењем изведене сесије кључева K_{MAC} и K_{Enc}. MRTD чип НЕ СМИЈЕ прихватити више од једног извођења PACE-а у оквиру исте сесије (види одјељак „Сигурна размјена порука“ у 3. дијелу овог техничког упутства под дефиницијом „сесија“) осим ако се суспендовани PIN мора обновити коришћењем неаутентификованог терминала (види одјељак 2.5.1) са CAN бројем као шифром. У том случају, друго извођење PACE-а МОРА бити заштићено са сигурном размјеном података установљеном у првом извођењу. Уколико је друго извођење PACE-а било успјешно, MRTD чип је верификовао PIN. Сигурна размјена података је поново покренута коришћењем новоизведене сесије кључева K_{MAC} и K_{Enc}. У супротном, ако друго извођење PACE-а није било успјешно, сигурна размјена порука се наставља коришћењем претходно утврђених кључева сесије.

3.3 Аутентификација чипа верзија 2

Протокол аутентификације чипа је привремено – статични Дифи-Хелманов протокол договора кључева који пружа сигурну комуникацију и једносмјерну аутентификацију MRTD чипа.

Протокол у верзији 2 пружа експлицитну аутентификацију MRTD чипа верификовањем токена за аутентификацију и имплицитну аутентификацију сачуваних података извођењем сигурне размјене порука коришћењем нове сесије кључева.

3.3.1 Спецификација протокола

Терминал и MRTD чип врше слиједеће кораке а поједностављена верзија је такође приказана на слици 2.

У овој верзији аутентификација терминала се МОРА извршити прије аутентификације чипа, јер је привремени пар кључева ($\widetilde{SK_{PCD}}$, $\widetilde{PK_{PCD}}$, D) терминала генерисан као дио аутентификације терминала.

1. MRTD чип шаље свој статички Дифи-Хелман јавни кључ PK_{PICC} и параметре домена D_{PICC} терминалу.
2. Терминал шаље привремени јавни кључ $\widetilde{PK_{PCD}}$ ка MRTD чипу.
3. MRTD чип израчунава компресовани привремени јавни кључ терминала $\boldsymbol{Comp}(\widetilde{PK_{PCD}})$ и пореди са компресованим привременим јавним кључем добијеним у процесу аутентификације терминала.
4. MRTD чип и терминал рачунају слиједеће:
   a) Заједничку тајну $K = KA(SK_{PICC}, \widetilde{PK_{PCD}}, D) = KA(\widetilde{SK_{PCD}}, PK_{PICC}, D)$
5. MRTD чип насумично бира nonce број r_{PICC}, изводи кључеве сесије K_{MAC}=**KDF_{MAC}** (K, r_{PICC}) и K_{Enc}= **KDF_{Enc}** (K, r_{PICC}) за сигурну размјену порука од K и r_{PICC}, рачуна токен за аутентификацију и шаље r_{PICC} и T_{PICC}.
6. Терминал изводи кључеве сесије K_{MAC}=**KDF_{MAC}** (K, r_{PICC}) и K_{Enc}= **KDF_{Enc}** (K, r_{PICC}) за сигурну размјену порука од K и r_{PICC}, и верификује T_{PICC}.

Како би се верификовала аутентичност PK_{PICC} терминала, пасивна аутентификација ЋЕ бити изведена.

3.3.2 Статус безбједности

Уколико је аутентификација чипа успјешнио извршена, сигурно слање порука је поново покренуто коришћењем изведених кључева сесије K_{MAC} и K_{Enc}. У супротном, сигурно слање порука се наставља коришћењем претходно утврђених кључева сесије (PACE или BAC).

Напомена: Пасивна аутентификација се МОРА извршити у комбинацији са аутентификацијом чипа. Док се у верзији 1, пасивна аутентификација ТРЕБА извршити након аутентификације чипа коришћењем објекта безбједности документа или објекта безбједности чипа, у верзији 2 пасивна аутентификација се МОРА извршити прије аутентификације чипа коришћењем објекта безбједности документа или објекта безбједности чипа. Једино након успјешне валидације поменутог објекта безбједности, MRTD чип се може сматрати оргиналним.

3.4 Аутентификација терминала верзија 2

Протокол аутентификације терминала је протокол са два challenge-response покрета који пружа експлицитну једнообразну аутентификацију терминала.

Аутентификација терминала омогућава MRTD чипу да верификује да је терминал овлашћен за приступ осјетљивим подацима. Како терминал може приступати осјетљивим подацима и послије, сва даља комуникација МОРА бити одговарајуће заштићена. Стога, терминал за аутентификацију такође аутентификује привремени јавни кључ који терминал изабере и који ће се користити за подешавање сигурне размјене порука са аутентификацијом чипа верзија 2. MRTD чип мора повезати права приступа терминала сигурној размјени порука утврђеној аутентификованим привременим јавним кључевима терминала.

У овом протоколу ID_{PICC} је идентификатор MRTD чипа:

- Ако се користи BAC, ID_{PICC} је број документа MRTD чипа који се налази у MRZ укључујући контролну цифру.
- Ако се користи PACE ID_{PICC} се рачуна коришћењем привременог PACE јавног кључа, тј $IDD_{PICC} = Comp(\widetilde{PK_{PICC}})$

Напомена: Све поруке МОРАЈУ бити послане сигурном размјеном података на начин енкрипција па аутентификација коришћењем кључева сесије изведених из PACE у току аутентификације чипа.

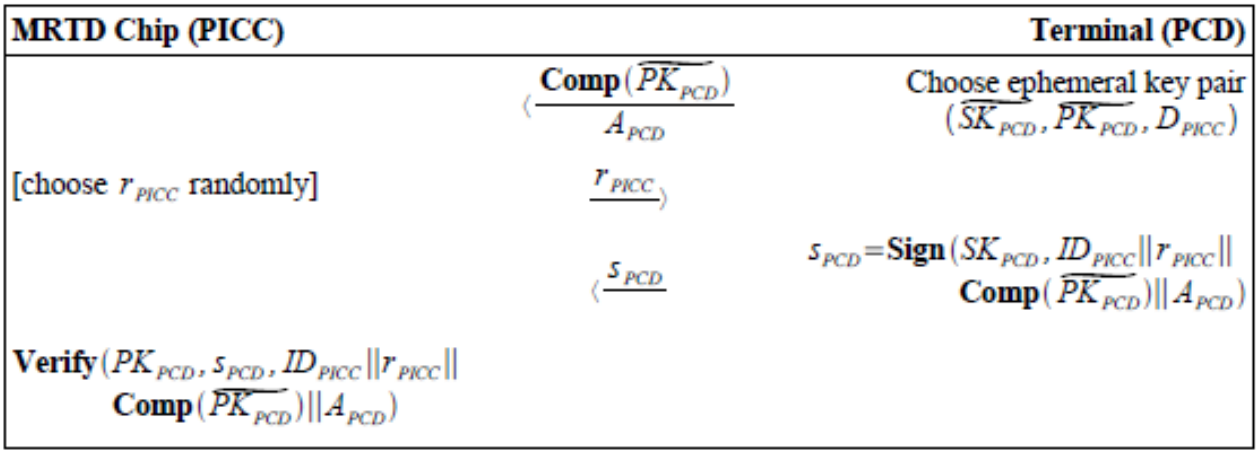


Figure 3: Terminal Authentication Version 2

3.4.1 Спецификација протокола

Терминал и MRTD чип врше слиједеће кораке а поједностављена верзија је такође приказана на слици 3.

1. Терминал шаље ланац цертификата MRTD чипу. Ланац почиње са цертификатом који се може провјерити са CVCA јавним кључем сачуваним на чипу и завршава се са цертификатом терминала.
2. MRTD чип верификује цертификате и изводи јавни кључ терминала PK_{PCD} .
3. Терминал

   а) генерише привремени Дифи-Хелманов пар кључева $(\widetilde{SK_{PCD}}, \widetilde{PK_{PCD}}, D)$ и шаље компресовани привремени јавни кључ $Comp(\widetilde{PK_{PKCD}})$ MRTD чипу, и

   б) може послати помоћне податке A_{PCD} MRTD чипу.

4. MRTD чип насумично бира challenge r_{PICC} и шаље га терминалу.
5. Терминал одговара потписом
   $$s_{PCD} = Sign(SK_{PCD}, ID_{PICC}||r_{PICC}||Comp(\widetilde{PK_{PICC}})||A_{PCD})$$
6. MRTD чип провјерава да је
   $$Verify(PK_{PCD}, ID_{PICC}||r_{PICC}||Comp(\widetilde{PK_{PCD}})||A_{PCD}) = true$$

Напомена: У верзији 1 аутентификација чипа се МОРА извршити прије аутентификације терминала, тј. $Comp(\widetilde{PK_{PKPCD}})$ се рачуна од MRTD чипа и терминала као дијела аутентификације чипа.

У верзији2 аутентификација чипа се МОРА извршити након аутентификације терминала. У том случају, $Comp(\widetilde{PK_{PKPCD}})$ се МОРА израчунати као дио аутентификације терминала. Поред тога, терминал МОЖЕ послати аутентификоване помоћне податке APCD MRTD чипу.

3.4.2 Статус безбједности

Ако је аутентификација терминала успјешно извршена, MRTD чип ЋЕ одобрити приступ сачуваним осјетљивим подацима у складу са важећом ауторизацијом терминала за аутентификацију. MRTD чип ЋЕ ипак ограничити права приступа терминала сигурној размјени порука утврђена аутентификованим привременим јавним кључем, тј. MRTD чип ЋЕ упоредити компресовану репрезентацију привременог јавног кључа терминала запримљеног као дио аутентификације терминала са компресованом репрезентацијом привременог јавног кључа добијеног од терминала као дио аутентификације чипа. MRTD чип НЕ СМИЈЕ прихватити више од једног извођења аутентификације терминала у оквиру исте сесије (види одјељак „Сигурна размјена порука“ у 3. дијелу овог техничког упутства под дефиницијом „сесија“).

Напомена: Аутентификација терминала не утиче на сигурну размјену порука. MRTD чип ЋЕ задржати сигурну размјену порука чак и ако је аутентификација терминала неуспјешна (осим ако се деси грешка код сигурне размјене порука)..

3.5 Ограничена идентификација

Протокол ограничене идентификације је статичан Дифи-Хелманов протокол договора кључева који генерише секторске специфичне идентификаторе MRTD чипа.

Ограничена идентификација пружа секторски специфичан идентификатор за MRTD са слиједећим својствима:

- У оквиру сваког сектора секторски специфичан идентификатор сваког MRTD чипа је јединствен.
- Између било која два сектора, рачунарски је неизводљиво повезати секторски специфичне идентификаторе било којег MRTD чипа[2].

Секторски специфични идентификатори се користи за идентификацију или поновну идентификацију MRTD чипа у оквиру сваког сектора. Аутентификација чипа и терминала MORA бити успјешно извршена прије употребе ограничене идентификације.

Напомена: У зависности од хеш функције која се користи за креирање секторског специфичног идентификатора, могу се десити хеш колизије.

3.5.1 Спецификације протокола

Терминал и MRTD чип изводе слиједеће кораке, а поједностављена верзија је приказана на слици 4.

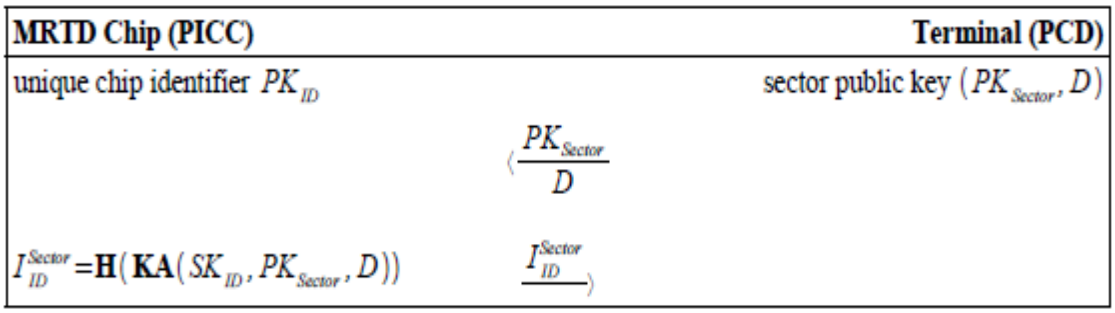
1. Терминал шаље статични секторски јавни кључ PK_{Sector}, и параметре домена D MRTD чипу. .

[2] Засвисно од генерације сектора повјерљива трећа страна може или не може повезати секторске идентификаторе између сектора.

2. MRTD чип верификује PK_{Sector}, рачуна и шаље свој секторски специфичан идентификатор $I_{ID}^{Sector} = H(KA(SK_{ID}, PK_{Sector}, D))$ терминалу.

3. Терминал провјера да ли је примљени секторски специфичан идентификатор I^{Sector}_{ID} је на листи опозивних идентификатора сектора добијених од верификатора документа.

Ограничена идентификација ЋЕ се користити само након што је аутентификација терминала и



чипа успјешно извршена. Једино је тада загарантована аутентичност јавног кључа сектора PK_{Sector} Sector секторског специфичног идентификатора $ISector_{ID.}$

У зависности од генерисања сектора, повјерена трећа страна може или не може бити у могућности да повеже секторске идентификаторе у оквиру сектора.

> *Напомена: MRTD чип МОРА верификовати јавни кључ сектора коришћењем наставка терминала сектора (види 3. дио овог техничког упутства) садржаном у цертификату терминала.*

3.5.2 Статус безбједности

Ограничена идентификација не утиче на статус безбједности MRTD чипа.

A. eID апликација (Нормативно)

A.1. eID апликација

eID апликација се састоји од 21 групе података (DG1 - DG21) које садрже личне податке. Преглед групе података је приказан у табели 3.

DG	Content	FID	SFID	ASN.1 type	R/W	Access
DG1	Врста документа	0x0101	0x01	Врста документа	R	PACE + TA + CA
DG2	Земља издавања	0x0102	0x02	Земља издавања	R	PACE + TA + CA
DG3	Рок важења	0x0103	0x03	Рок важења	R	PACE + TA + CA
DG4	Лично име	0x0104	0x04	Лично име	R	PACE + TA + CA
DG5	Презиме	0x0105	0x05	Презиме	R	PACE + TA + CA
DG6	Вјероисповијест	0x0106	0x06	Умјетничко име	R	PACE + TA + CA
DG7	Академска титула	0x0107	0x07	Академска титула	R	PACE + TA + CA
DG8	Датум рођења	0x0108	0x08	Датум рођења	R	PACE + TA + CA
DG9	Мјесто рођења	0x0109	0x09	Мјесто рођења	R	PACE + TA + CA
DG10	Националност	0x010A	0x0A	Националност	R	PACE + TA + CA
DG11	Пол	0x010B	0x0B	Пол	R	PACE + TA + CA
DG12	Опционални подаци	0x010C	0x0C	Опционални подаци	R	PACE + TA + CA
DG13	--	0x010D	0x0D	RFU	R	PACE + TA + CA
DG14	--	0x010E	0x0E	RFU	R	PACE + TA + CA
DG15	--	0x010F	0x0F	RFU	R	PACE + TA + CA
DG16	--	0x0110	0x10	RFU	R	PACE + TA + CA
DG17	Мјесто пребивалишта	0x0111	0x11	Мјесто пребивалишта	R/W	PACE + TA + CA
DG18	Број општине	0x0112	0x12	Број општине	R/W	PACE + TA + CA
DG19	Дозвола боравка I	0x0113	0x13	Дозвола боравка I	R/W	PACE + TA + CA
DG20	Дозвола боравка II	0x0114	0x14	Дозвола боравка II	R/W	PACE + TA + CA
DG21	Опционални подаци	0x0115	0x15	Опционални подаци	R/W	PACE + TA + CA

Табела 3: Групе података на eID апликацији

A.1.1. Application Identifier

eID апликација ЋЕ бити идентификована стандардним идентификатором апликације 0xE80704007F00070302 који се заснива на слиједећим објектима идентификатора:

id-eID OBJECT IDENTIFIER ::= {

bsi-de applications(3) 2

}

A.2. ASN.1 Дефиниција

Свака елементарна датотека садржи ASN.1- структуру дефинисану у наставку. Подаци се декодирају према истакнутим правилима декодирања (DER) дефинисаним у [6].

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

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

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

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

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

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

4 Библиографија

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

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

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

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

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

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

[7] Други дио техничког Упутства за MRTD BSI