

ET

ET

ET



EUROOPA ÜHENDUSTE KOMISJON

Brüssel, 28/VI/2006

K(2006) 2909 lõplik

EI KUULU AVALDAMISELE

KOMISJONI OTSUS,

28/VI/2006,

millega nähakse ette liikmesriikides väljaantavate passide ja reisidokumentide turvaelementide ja biomeetria standardeid käsitlevad tehnilised kirjeldused

(Ainult tšehhi-, hollandi-, eesti-, soome-, prantsuse-, saksa-, kreeka-, ungari-, itaalia-, rootsi-, läti-, leedu-, malta-, poola-, portugali-, slovaki-, sloveeni- ja hispaaniakeelne tekst on autentsed)

KOMISJONI OTSUS,

28/VI/2006,

millega nähakse ette liikmesriikides väljaantavate passide ja reisidokumentide turvaelementide ja biomeetria standardeid käsitlevad tehnilised kirjeldused

(Ainult tšehhi-, hollandi-, eesti-, soome-, prantsuse-, saksa-, kreeka-, ungari-, itaalia-, rootsi-, läti-, leedu-, malta-, poola-, portugali-, slovaki-, sloveeni- ja hispaaniakeelne tekst on autentsed)

EUROOPA ÜHENDUSTE KOMISJON,

võttes arvesse Euroopa Ühenduse asutamislepingut,

võttes arvesse nõukogu 13. detsembri 2004. aasta määrust (EÜ) nr 2252/04¹ liikmesriikide poolt väljastatud passide ja reisidokumentide turvaelementide ja biomeetria standardite kohta, eriti selle artiklit 2,

ning arvestades järgmist:

- (1) 13. detsembri 2004. aasta määrusega (EÜ) nr 2252/04 nähakse ette üksnes sellised passide ja reisidokumentide üldised tehnilised kirjeldused, mis ei ole salastatud. Neile tuleb lisada täiendavad tehnilised kirjeldused, mis võivad jääda salajaseks.
- (2) Asjakohane on kehtestada kohustuslike sõrmejälgede salvestamise ja kaitse täiendavad tehnilised kirjeldused.
- (3) On otsustatud, et käesolevas otsuses sätestatud kirjeldusi ei hoita salajas, sest neis viidatakse peamiselt avalikult kättesaadavatele dokumentidele.
- (4) Käesoleva otsusega täiendatakse komisjoni 28. veebruari 2005. aasta otsust, millega nähakse ette liikmesriikides väljastatud passide ja reisidokumentide turvaelementide ja biomeetria standardeid käsitlevad tehnilised kirjeldused (C(2005) 409 (lõplik), millega sätestatakse näokujutise integreerimise tehnilised kirjeldused.
- (5) Selguse huvides on käesolevale otsuse lisas koondokument, millega sätestatakse komisjoni otsusega C(2005) 409 (lõplik) ja käesoleva otsusega kehtestatud tehnilised kirjeldused. Kõnealune tehniliste kirjelduste koondamine ei mõjuta määruses 2252/2004 sätestatud rakendamise tähtaegu.
- (6) Nõukogu 29. mai 2000. aasta otsuse 2000/365/EÜ (Suurbritannia ja Põhja-Iiri Ühendkuningriigi taotluse kohta osaleda teatavates Schengeni *acquis'* sätetes) kohaselt ei osalenud Ühendkuningriik kõnealuse määruse vastuvõtmisel, mistõttu see ei ole

¹ELT L 385, 29.12.2004, lk 1.

tema suhtes siduv ega kohaldatav, sest selles arendatakse edasi Schengeni *acquis'* sätteid. Seepärast ei ole Ühendkuningriik käesoleva otsuse adressaat.

- (7) Nõukogu 28. veebruari 2002. aasta otsuse 2002/192/EÜ (Iirimaa taotluse kohta osaleda teatavates Schengeni *acquis'* sätetes) kohaselt ei osalenud Iirimaa kõnealuse määruse vastuvõtmisel, mistõttu see ei ole tema suhtes siduv ega kohaldatav, sest selles arendatakse edasi Schengeni *acquis'* sätteid. Seepärast ei ole Iirimaa käesoleva otsuse adressaat.
- (8) Euroopa Liidu lepingule ja Euroopa Ühenduse asutamislepingule lisatud Taani seisukohta käsitleva protokollide artiklite 1 ja 2 kohaselt ei osalenud Taani kõnealuse määruse vastuvõtmisel, mistõttu see ei ole tema suhtes siduv ega kohaldatav. Kuna käesoleva otsuse eesmärk on täiendada Schengeni *acquis'*d vastavalt Euroopa Ühenduse asutamislepingu kolmanda osa IV jaotisele, on Taani teavitanud 6. juuni 2005. aasta kirjaga vastavalt nimetatud protokollide artiklile 5, et on selle oma siseriiklikku õigusesse ülevõtnud. Rahvusvaheline õigus kohustab Taanit rakendama käesoleva otsuse lisa. Seetõttu peaks Taani saama käesoleva otsuse koopia.
- (9) Islandi ja Norra puhul kujutab kõnealune määrus endast nende Schengeni *acquis'* sätete edasiarendamist Euroopa Liidu Nõukogu ning Islandi Vabariigi ja Norra Kuningriigi vahel sõlmitud lepingu tähenduses, mis käsitleb nimetatud kahe riigi ühinemist Schengeni *acquis'* sätete rakendamise, kohaldamise ja edasiarendamisega, mis on seotud nimetatud lepingu teatavaid rakenduseeskirju käsitleva nõukogu 17. mai 1999. aasta otsuse 1999/437/EÜ² artikli 1 punktis B osutatud valdkonnaga. Seepärast on käesolev komisjoni otsus Norra ja Islandi suhtes siduv.
- (10) Šveitsi puhul kujutab kõnealune määrus endast nende Schengeni *acquis'* sätete edasiarendamist Euroopa Liidu, Euroopa Ühenduse ja Šveitsi Konföderatsiooni vahel sõlmitud lepingu tähenduses, mis käsitleb Šveitsi ühinemist Schengeni *acquis'* sätete rakendamise, kohaldamise ja edasiarendamisega, mis on seotud nimetatud lepingule Euroopa Ühenduse nimel allakirjutamist ja selle teatavate sätete ajutist kohaldamist käsitleva nõukogu otsuse artikli 4 lõikes 1 osutatud valdkonnaga.
- (11) Käesolevas otsuses ettenähtud meetmed on kooskõlas määruse (EÜ) nr 1683/95 artikli 6 alusel loodud komitee arvamusega,

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

Artikkel 1

Liikmesriikides väljastatud passidesse ja reisidokumentidesse integreeritavate sõrmejälgede salvestamist ja kaitset käsitlevad tehnilised kirjeldused sätestatakse käesoleva otsuse lisa punktides 5, 6 ja 7.

² EÜT L 176, 10.7.1999, lk 31.

Artikkel 2

Liikmesriigid teevad käesoleva otsuse rakendamisel koostööd, eelkõige vahetades teavet kõikide tehniliste kirjelduste kohta.

Liikmesriigid saadavad väljaantavate passide ja reisidokumentide näidised komisjonile ja teistele liikmesriikidele. Samuti säilitavad liikmesriigid edaspidiste trükkide näidised ja hoiavad neid komisjonile ja teistele liikmesriikidele kättesaadavana.

Artikkel 3

Käesolev otsus on adresseeritud Belgia Kuningriigile, Tšehhi Vabariigile, Saksamaa Liitvabariigile, Eesti Vabariigile, Kreeka Vabariigile, Hispaania Kuningriigile, Prantsuse Vabariigile, Itaalia Vabariigile, Küprose Vabariigile, Läti Vabariigile, Leedu Vabariigile, Luksemburgi Suurhertsogiriigile, Ungari Vabariigile, Malta Vabariigile, Madalmaade Kuningriigile, Austria Vabariigile, Poola Vabariigile, Portugali Vabariigile, Sloveenia Vabariigile, Slovakkia Vabariigile, Soome Vabariigile ja Rootsi Kuningriigile.

Brüssel, 28/VI/2006

Komisjoni nimel
Franco FRATTINI
komisjoni asepresident



Biomeetria kasutamine ELi passides

ELi passi tehniline kirjeldus

Komisjoni otsuse K (2006) 2909,
28/VI/2006, lisa

Sisukord

1	Kohaldamisala ja piirangud.....	3
2	Biomeetria	4
2.1	Esmane biomeetriline element - nägu	4
2.1.1	Vastavus standarditele.....	4
2.1.2	Tüüp	5
2.1.3	Vorming	5
2.1.4	Salvestamisnõuded	5
2.1.5	Muud küsimused.....	5
2.2	Teisene biomeetriline element - sõrmejäljed	5
2.2.1	Vastavus standarditele.....	5
2.2.2	Tüüp	6
2.2.3	Vorming ja kvaliteet.....	6
2.2.4	Salvestamisnõuded	6
3	Andmekandja (RF-kiibi struktuur).....	6
3.1	Vastavus standarditele.....	6
3.2	RF-liides	7
3.3	Salvestusmaht.....	7
4	Kiibi asetus elektroonilises passis (andmestruktuur)	7
4.1	Vastavus standarditele.....	7
4.2	Korrelatsioon trükitud andmetega.....	8
4.3	Kiibi loogiline andmestruktuur	8
5	Andmete turvalisuse ja terviklikkuse küsimused	8
5.1	Vastavus standarditele.....	8
5.2	Digitaalsete andmete turvalisus.....	8
5.3	Kontrollimenetlus.....	10
5.4	Passide avaliku võtme infrastruktuur	10
5.5	Kontrollisüsteemide avaliku võtme infrastruktuur.....	11
5.5.1	Sertifikaadi kehtivusaeg	11
5.5.2	Sertifitseerimine	11
5.5.3	Sertifitseerimispoliitika	12
6	Vastavushindamine	12
6.1	Vastavus standarditele.....	12
6.2	Funktsionaalsuse hindamine	13
6.3	Ühised hindamiskriteeriumid	13
7	Viited normidele.....	13

1 Kohaldamisala ja piirangud

Käesolevas dokumendis kirjeldatakse kiibipõhiste ELi passide lahendusi järgneva ELi dokumendi [1] alusel:

„Nõukogu määrus liikmesriikide väljastatud passide ja reisidokumentide turvaelementide ja biomeetria standardite kohta“

Käesoleva dokumendi aluseks on rahvusvahelised standardid, eelkõige ISO standardid ja masinloetavaid reisidokumente käsitlevad ICAO soovitusel, ning see sisaldab järgmist:

- Biomeetriliste tunnuste tehniline kirjeldus: nägu ja sõrmejäljed
- Andmekandja (kiip)
- Kiibi loogiline andmestruktuur
- Kiibile digitaalselt salvestatud andmete turvalisuse tehniline kirjeldus
- Kiibi ja rakenduste vastavushindamine
- RF-ühilduvus teiste elektrooniliste reisidokumentidega

Käesolevas dokumendis ei käsitleta järgnevat:

- Kiibi mehaanilise passi paigaldamise, vastupidavuse ja mehaaniliste katsetusprotseduuride tehniline kirjeldus.
- Kontrolli- või registreerimistoimingute standardoperatsioonide käsitlev tehniline kirjeldus.

2 Biomeetria

2.1 Esmane biomeetriline element - nägu

2.1.1 Vastavus standarditele

- ICAO NTWG, *Biometrics Deployment of Machine Readable Travel Documents* (Biomeetria kasutamine masinloetavates reisdokumentides), tehniline aruanne, versioon 2.0 (5. mai 2004) [3]
- ISO/IEC 19794-5:2005, *Biometric Data Interchange Formats – Part 5* (Biomeetriliste andmete andmevahetuse vormingud – 5. osa): Näokujutise andmed [4]

2.1.2 Tüüp

Näokujutis tuleb salvestada EESTVAATES PILDINA¹ vastavalt punktidele [3, 4].

2.1.3 Vorming

Näokujutis tuleb salvestada tihendatud PILDIFAILINA, mitte tootjapõhise mallina.

Kuigi nii JPEG- kui ka JPEG2000-tihendus on standardsed [3], soovitatakse ELi passi puhul JPEG2000-tihendust, sest selle abil tihendatud failid on väiksemad kui JPEG-tihendusega tihendatud failid.

2.1.4 Salvestamisnõuded

Nr	Võimalus	Märkus	Soovitus
1	JPEG-tihendus	umbes 12-20 kB/foto kohta	
2	JPEG2000-tihendus	umbes 6-10 kB/foto kohta	soovitatav (vaata 2.1.3)

2.1.5 Muud küsimused.

- Vastavalt ICAO standarditele tuleb vastu võtta fotografeerimise suunised (*Photograph Taking Guidelines*), milles võetakse arvesse näotuvastustehnoloogia nõudeid [3].

2.2 Teisene biomeetriline element - sõrmejäljed

2.2.1 Vastavus standarditele

- ICAO NTWG, *Biometrics Deployment of Machine Readable Travel Documents* (Biomeetria kasutamine masinloetavates reisidokumentides), tehniline aruanne, versioon 2.0 (5. mai 2004) [3]

¹ ICAO standardite kohaselt tuleb LDSi 2. andmerühma salvestatud näo biomeetriliste andmete andmevahetuspilt teha passipildist, mida on kasutatud masinloetava passi isikuandmete leheküljel kasutatud foto tegemiseks, ning see tuleb kodeerida kas ISO 19794-5 viimases versioonis esitletud *full frontal image* või *token image* vormingusse.

- ISO/IEC 19794-4:2005, Biomeetriliste andmete andmevahetuse vormid – 4. osa: Sõrme kujutise andmed [5]
- ANSI/NIST-ITL 1-2000 Standard “*Data Format for the Interchange of Fingerprint, Facial, Scarmark & Tattoo (SMT) Information* (Andmete salvestusviis sõrmejälgi, näojooni, arme ja tätoveeringuid puudutavate andmete vahetamiseks); FBI: *Wavelet Scalar Quantization (WSQ)* [15]

2.2.2 Tüüp

ELi passi lisatavad esmased sõrmejäljed on:

VASAKU JA PAREMA KÄE NIMETISSÕRME VAJUTUSJÄLJED.

Kui sõrmejälgede kvaliteet ei ole rahuldav ja/või nimetissõrmedel on vigastusi, tuleb võtta kvaliteetsed vajutamiseks võetud sõrmejäljed keskmistelt sõrmedelt, neljandatelt sõrmedelt või põialdelt.²

2.2.3 Vorming ja kvaliteet

Sõrmejäljed tuleb salvestada PILTIDENA vastavalt punktile [5].

Sõrmejälje kujutiste kvaliteet peab vastama punktidele [5] ja [15].

Faili suuruse vähendamiseks PEAB pildid tihendama WSQ-algoritmiga vastavalt punktile [15].

2.2.4 Salvestamisnõuded

SÕRMEJÄLJE KUJUTISTE kasutamine nõuab ligikaudu 12 – 15 kilobaiti sõrme kohta.

3 Andmekandja (RF-kiibi struktuur)

3.1 Vastavus standarditele

- ICAO NTWG, *Biometrics Deployment of Machine Readable Travel Documents* (Biomeetria kasutamine masinloetavates reisidokumentides), tehniline aruanne, versioon 2.0 (5. mai 2004) [3]

² Salvestamismeetod (CBEFF – *Common Biometric Exchange File Format*) salvestab kasutatud sõrmede tüübi (vasak nimetissõrm, parem keskmine sõrm jne.), tagamaks õige sõrme tõendamise.

- ISO/IEC FDIS 14443, *Identification cards - Contactless integrated circuit(s) cards - Proximity cards* (Isikutunnistused - Integraallülitusega kontaktivabad kaardid – Lähidistantskaardid) [7]
- ICAO NTWG, *Use of Contactless Integrated Circuits In Machine Readable Travel Documents* (Kontaktivaba integraallülituse kasutamine masinloetavates reisidokumentides), tehniline aruanne, versioon 3.1 (16. aprill 2003) [8]

3.2 RF-liides

Punktide [3, 7 ja 8] kohaselt peetakse nii A- kui ka B-tüüpi RF-liideseid ICAO standarditele vastavaks.

ICAO standarditele vastavad passid varustatakse A- või B-tüüpi RF-liidesega, mistõttu tuleb passide puhul piirikontrollisüsteemid kohandada mõlemale standardile.

3.3 Salvestusmaht

ICAO loogilise andmestruktuuri [10] kohaselt tuleb kiibile koos biomeetriliste tunnustega salvestada dokumendi masinloetava ala (MRZ) tähtnumbrilised andmed ja dokumendi digitaalsed turvaandmed (PKI).

Liikmesriigid peavad kasutama asjakohase suurusega RF-kiipe, millele saab salvestada ELi õigusele vastavaid isikuandmeid ja biomeetrilisi tunnusjooni [1]. Vaata ka peatükke 2.1.4 ja 2.2.4.)

Kui liikmesriik soovib vastavalt ELi õigusele [1] lisada muid andmeid, võib osutada vajalikuks salvestusmahtu suurendada.

4 Kiibi asetus elektroonilises passis (andmestruktuur)

4.1 Vastavus standarditele

- Rahvusvahelise Tsiviillennunduse Organisatsioon (ICAO), *Machine Readable Travel Documents Doc 9303, Part 1 Machine Readable Passports* (Masinloetavad reisidokumendid), Doc 9303, 1. osa, Masinloetavad passid, 2006. aasta kuuenda väljaande projekt [9]
- Ühised konsulaarjuhised (CCI), VI peatüki punkt nr 4 ja lisa 10
- ICAO NTWG, *Development of a Logical Data Structure – LDS for optional capacity expansion technologies* (Loogilise andmestruktuuri arendus – LDS valikulistele mahtu suurendavatele tehnoloogiatele), tehniline aruanne, revisjon 1.7, 18. mai 2004 [10]

4.2 Korrelatsioon trükitud andmetega

Passi masinloetavale alale trükitud tähtnumbrilised andmed peavad punktile [9] vastavalt korreleeruma punkti [10] kohaselt kiibile digitaalselt salvestatud andmetega.

4.3 Kiibi loogiline andmestruktuur

Vastavalt punktile [10].

5 Andmete turvalisuse ja terviklikkuse küsimused

Tavapärasel passis on mitmeid võltsimisvastaseid meetmeid, kaasa arvatud punkti [1] kohased turvatrüki ja optiliselt muutuvad vahendid. Passi kiibile salvestatud andmete ühtsus, autentsus ja konfidentsiaalsus peavad olema võrdselt tagatud.

5.1 Vastavus standarditele

- ICAO NTWG, *PKI for Machine Readable Travel Documents Offering ICC Read-Only Access* (ICC kirjutuskaitsega PKI masinloetavates reisidokumentides), tehniline aruanne, versioon 1.1, 1. oktoober 2004 [11]
- *Advanced Security Mechanisms for Machine Readable Travel Documents*, (masinloetavate reisidokumentide turvamehhanismid) versioon 1.0, 2006 [13]

5.2 Digitaalsete andmete turvalisus

Nr	Turvalisus	Märkus	Kasutusviis
1	Passiivne tõendamine [11, 12]	Tõendab, et SO _D ja LDS sisu on autentne ja muutumatu. Ei välista täpse koopia tegemist ega kiibi vahetust. Ei välista loata kasutamist. Ei välista andmete lubamatut jäljendamist (skimming).	NÕUTAV kõikide andmete puhul (ICAO kohustuslik turvaelement)
2a)	Aktiivne tõendamine [11, 12]	Tõendab, et SO _D ei ole koopia, vaid on loetud autentselt kiibilt. Tõendab, et kiipi ei ole	VALIKULINE

Nr	Turvalisus	Märkus	Kasutusviis
		<p>vahetatud.</p> <p>Ei tõenda, et LDSi sisu on autentne ja vahetamata.</p> <p>Ei välista kiibi ja kontrollisüsteemi vahelise andmevahetuse pealtkuulamist</p>	
b)	<p>Kiibi tõendamine</p> <p>[13]</p>	<p>Tõendab, et SO_D ei ole koopia ja see on loetud autentselt kiibilt.</p> <p>Tõendab, et kiipi ei ole vahetatud.</p> <p>Välistab kiibi ja kontrollisüsteemi vahelise andmevahetuse pealtkuulamise</p>	<p>Lisakaitse NÕUTAV kõikide andmete puhul, kui sisestatakse sõrmejälgi või hiljemalt 36 kuud pärast tehniliste nõuete vastu võtmist. Kõnealust kaitset EI TOHI tagada kiip, kuid ELi kontrollisüsteemid PEAVAD seda mehhanismi kasutama, kui kiip seda võimaldab.</p>
3	<p>Põhiline ligipääsukontroll</p> <p>[11, 12]</p>	<p>Välistab andmete lubamatu jäljendamise (skimming).</p> <p>Vähendab kiibi ja kontrollisüsteemi vahelise andmevahetuse pealtkuulamise ohtu (vaata punkti 2b).</p> <p>Ei välista täpse koopia tegemist ega kiibi vahetust (nõuab ka tavapärase dokumendi kopeerimist).</p>	<p>NÕUTAV kõikide andmete puhul</p>

Nr	Turvalisus	Märkus	Kasutusviis
4	Terminali tõendamine [13]	Välistab loata ligipääsu sõrmejälgedele. Välistab sõrmejälgede lubamatu jäljendamise (skimming). Nõuab täiendavat võtmehaldust. Ei välista täpse koopia tegemist ega kiibi vahetust (nõuab ka tavapärase dokumendi kopeerimist).	Lisakaitse NÕUTAV sõrmejälgede puhul

SO_D *Document Security Object* (dokumendi turvaobjekt). Väljaandjariik kirjutab objektile alla digitaalselt ning objekt sisaldab räsikoodina LDS-sisu.

LDS *Logical Data Structure* (loogiline andmestruktuur)

MRTD *Machine Readable Travel Document* (masinloetav reisidokument)

MRZ *Machine Readable Zone* (masinloetav ala)

EAC *Extended Access Control* (Laiendatud ligipääsukontroll), mis on ICAO standardi kohaselt kombinatsioon kiibi tõendamisest ja terminali tõendamisest.

5.3 Kontrollimenetlus

Välja jäetud

5.4 Passide avaliku võtme infrastruktuur

Kiibil salvestatud digitaalsete andmete terviklikkuse ja autentsuse kindlustamiseks kasutatakse PKId. Iga liikmesriik PEAB määrama ainult ühe riikliku allakirjutava sertifitseerimisasutuse (*Country Signing CA*), keda vastuvõtavad riigid usaldavad ja vähemalt ühe passe väljaandva dokumendi allakirjutaja (*Document Signer*). PKI infrastruktuuri üksikasjad (sealhulgas allkirja algoritmid, võtme pikkused ja kehtivusperioodid) on nimetatud punktis [11].

Iga liikmesriik PEAB komisjonile teatama riikliku allakirjutava sertifitseerimisasutuse (*Country Signing CA*) ja dokumendi allakirjutaja(te) (*Document Signer*) tegevuse eest vastutava organisatsiooni kontaktandmed.

5.5 Kontrollisüsteemide avaliku võtme infrastruktuur

Vältimaks volitamata kontrollisüsteemide kaudu juurdepääsu sõrmejälgedele, on kasutusele võetud täiendav PKI: iga liikmesriik PEAB määrama ainult ühe riikliku tõendava sertifitseerimisasutuse (*Country Verifying CA*), kes on kõnealuse liikmesriigi väljaantud passide suhtes usaldusväärne, ja vähemalt ühe volitatud kontrollisüsteemide rühma haldava dokumentide tõendaja (*Document Verifier*). Kõnealuse PKI infrastruktuuride üksikasjad on toodud punktis [13].

Iga liikmesriik PEAB komisjonile teatama riikliku tõendava sertifitseerimisasutuse (*Country Verifying CA*) ja dokumentide tõendaja(te) (*Document Verifier*) tegevuse eest vastutava organisatsiooni kontaktandmed.

5.5.1 Sertifikaadi kehtivusaeg

Väljastatud sertifikaatide kehtivusaeg PEAB mahtuma järgmiste tähtaegade sisse:

Üksus	Minimaalne kehtivusaeg	Maksimaalne kehtivusaeg
Riikliku tõendava sertifitseerimisasutuse sertifikaat (<i>Country Verifying CA Certificate</i>)	6 kuud	3 aastat
Dokumendi tõendaja sertifikaat (<i>Document Verifier Certificate</i>)	2 nädalat	3 kuud
Kontrollisüsteemi sertifikaat	1 päev	1 kuu

Kõnealuseid tähiseid võib muuta artikli 6 alusel loodud komitee vastavalt BIGi töörühma esitatud testi tulemustele.

5.5.2 Sertifitseerimine

Sertifitseerimise kavandamisel PEAB järgima järgmisi töötlemis- ja jaotamisaegu. Riikliku tõendava sertifitseerimisasutuse (*Country Verifying CA*) ühendussertifikaadid TULEB laiali jaotada vähemalt 14 päeva enne asendatava sertifikaadi kehtivusaja lõppemist.

Sertifitseerimisasutus	Maksimaalne töötlemisaeg (sertifitseerimistaotlus)	Maksimaalne jaotamisaeg (sertifikaat)
Riiklik tõendav sertifitseerimisasutus (<i>Country Verifying CA</i>)	72 tundi	24 tundi
Dokumendi tõendaja (<i>Document Verifier</i>)	24 tundi	48 tundi

Kõnealuseid tähiseid võib muuta artikli 6 alusel loodud komitee vastavalt BIGi töörühma esitatud testi tulemustele.

5.5.3 Sertifitseerimispoliitika

BIGi töörühm töötab aasta jooksul pärast komisjoni otsust tehniliste kirjelduste kohta välja ühise sertifitseerimispoliitika.

Iga liikmesriigi riiklik tõendav sertifitseerimisasutus (*Country Verifying CA*) AVALIKUSTAB sertifitseerimispoliitika ning võib vastavalt BIGi töörühma nõuetele kehtestada sertifitseerimispraktika eeskirja, mis näitab eelkõige, millistel tingimustel antakse välja (välisriigi) dokumendi tõendaja sertifikaat. Komisjoni teavitatakse sertifitseerimispoliitika vastuvõtmisest.

6 Vastavushindamine

Käesoleva kirjeldusega ühilduvate passide koostalitlusvõime tagamiseks luuakse tehniline töörühm (“Brussels Interoperability Group”, BIG) [punkt 18].

6.1 Vastavus standarditele

- ICAO NTWG, *RF Protocol and Application Test Standard for E-Passport*, (RF-protokoll ja e-passide taotluse teststandard), 2. ja 3. osa [19]
- ISO/IEC 7816-4, *Identifications cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange* (Isikutunnistused – Integraallülitusega kaardid – 4. osa: Andmevahetuse korraldus, turvalisus ja käsud) [12]
- ISO/IEC 7816-8, *Identifications cards – Integrated circuit cards – Part 8: Commands for security operations* (Isikutunnistused – Integraallülitusega kaardid – 8. osa: Turvaoperatsioonide käsud [20]

- *Common Criteria Protection Profile for Machine Readable Travel Document with “ICAO Application”, Basic Access Control*, (ICAO rakendusega masinloetavate reisidokumentide kaitseprofiili üldised kriteeriumid, põhiline ligipääsukontroll), versioon 1.0 [14]
- *Common Criteria Protection Profile for Machine Readable Travel Document with “ICAO Application”, Extended Access Control*, (ICAO rakendusega masinloetavate reisidokumentide kaitseprofiili üldised kriteeriumid, laiendatud ligipääsukontroll), versioon 1.0) [17]

6.2 Funktsionaalsuse hindamine

MRTD-kiipide funktsionaalsuse hindamisel PEAB kasutama asjakohaseid standardeid, mis on praegu väljatöötamisel. BIGi töörühm VÕIB kindlaks määrata dokumendi [13] rakendamiseks vajalikud täiendavad testid.

Iga liikmesriik PEAB ISO/OSI kõigi tasemete asjakohaste standardite funktsionaalse ühilduvuse kinnitamiseks sõlmima lepingu akrediteeritud (riikliku) testlaboriga. Väljastatud sertifikaatidest TULEB komisjonile teatada.

ISO/OSI tase	Standard	Kohaldamisala
1-4	ISO 14443 [7]	Riistvara
6	ISO 7816 [12,20]	Tarkvara (OS)
7	ICAO rakendus [10,11,]	Tarkvara (rakendus)

6.3 Ühised hindamiskriteeriumid

Passikiipe PEAB hindama vastavalt asjakohastele kaitseprofiili üldistele kriteeriumitele [14, 17].

7 Viited normidele

- [1] „Nõukogu määrus (EÜ) nr 2252/2004 liikmesriikide väljastatud passide ja reisidokumentide turvaelementide ja biomeetria standardite kohta“
- [2] välja jäetud
- [3] ICAO NTWG, *Biometrics Deployment of Machine Readable Travel Documents* (Biomeetria kasutamine masinloetavates reisidokumentides), tehniline raport, versioon 2.0 (5. mai 2004) [ICAO Bio]
- [4] ISO/IEC FCD 19794-5, *Biometric Data Interchange Formats – Part 5: Face Image Data*, (Biomeetriliste andmete andmevahetuse vormid – 5. osa:

- Näokujutise andmed)
- [5] ISO/IEC 19794-4:2005, *Biometric Data Interchange Formats – Part 4: Finger Image Data* (Biomeetriliste andmete andmevahetuse vormid – 4. osa: Sõrmekujutise andmed)
- [6] välja jäetud
- [7] ISO/IEC 14443 *Identification cards – Contactless integrated circuit(s) cards – Proximity cards* (Isikutunnistused – Integraallülitusega kontaktivabad kaardid – Lähidistantskaardid)
- [8] ICAO NTWG, *Use of Contactless Integrated Circuits In Machine Readable Travel Documents* (Kontaktivaba integraallülituse kasutamine masinloetavates reisidokumentides), tehniline raport, versioon 3.1 (16. aprill 2003)
- [9] Rahvusvahelise Tsiviillennunduse Organisatsioon (ICAO), *Machine Readable Travel Documents Doc 9303, Part 1 Machine Readable Passports* (Masinloetavad reisidokumendid), Doc 9303, 1. osa, masinloetavad passid, 2006. aasta kuuenda väljaande projekt [9]
- [10] ICAO NTWG, *Development of a Logical Data Structure – LDS for optional capacity expansion technologies* (Loogilise andmestruktuuri arendus – LDS valikuliselt mahtu suurendavatele tehnoloogiatele), tehniline raport, revisjon 1.7, (18. mai 2004)
- [11] ICAO NTWG, *PKI for Machine Readable Travel Documents Offering ICC Read-Only Access* (ICC-kirjutuskaitsega PKI masinloetavates reisidokumentides), tehniline raport, versioon 1.1, 1. oktoober 2004
- [12] ISO/IEC 7816-4:2005, *Identifications cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange* (Isikutunnistused – Integraallülitusega kaardid – 4. osa: Andmevahetuse korraldus, turvalisus ja käsud)
- [13] *Advanced Security Mechanisms for Machine Readable Travel Documents* (masinloetavate reisidokumentide täiendatud turvamehhanismid), versioon 1.0, 2005
- [14] *Common Criteria Protection Profile for Machine Readable Travel Document with “ICAO Application”, Basic Access Control*, (ICAO rakendusega

- masinloetavate reisidokumentide kaitseprofili üldised kriteeriumid, põhiline ligipääsukontroll), versioon 1.0)
<http://www.bsi.bund.de/zertifiz/zert/reporte/PP0017b.pdf>
- [15] ANSI/NIST-ITL 1-2000 *Standard “Data Format for the Interchange of Fingerprint, Facial, Scarmark & Tattoo (SMT) Information* (Andmete salvestusviis sõrmejälgi, näojooni, arme ja tätoveeringuid käsitlevate andmete vahetamiseks)
FBI: Wavelet Scalar Quantization (WSQ)
www.itl.nist.gov/iad
- [16] välja jäetud
- [17] *Common Criteria Protection Profile for Machine Readable Travel Document with “ICAO Application”, Basic Access Control*, (ICAO rakendusega masinloetavate reisidokumentide kaitseprofili üldised kriteeriumid, põhiline ligipääsukontroll), versioon 1.0)
- [18] *Brussels Interoperability Group, Terms of Reference*, Brüsseli koostalitlusvõime töörühm, reglement
- [19] ICAO NTWG, *RF Protocol and Application Test Standard for E-Passport; Parts 2&3*, (RF protokoll ja e-passide taotluse teststandard), 2. ja 3. osa),
- [20] ISO/IEC 7816-8:2004, *Identifications cards – Integrated circuit cards – Part 8: Commands for security operations* (Isikutunnistused – Integraallülitusega kaardid – 8. osa: Turvaoperatsioonide käsud)