COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN

Brussel, 28/II/2005
C(2005) 409 def

BESCHIKKING VAN DE COMMISSIE

van 28/II/2005

tot vaststelling van de technische specificaties in verband met de normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten

(Alleen de teksten in de Tsjechische, Nederlandse, Engelse, Estse, Finse, Franse, Duitse, Griekse, Hongaarse, Italiaanse, Zweedse, Letse, Litouwse, Maltese, Poolse, Portugese, Slowaakse, Sloveense en Spaanse taal zijn authentiek)

BESCHIKKING VAN DE COMMISSIE

van 28/II/2005

tot vaststelling van de technische specificaties in verband met de normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten

(Alleen de teksten in de Tsjechische, Nederlandse, Engelse, Estse, Finse, Franse, Duitse, Griekse, Hongaarse, Italiaanse, Zweedse, Letse, Litouwse, Maltese, Poolse, Portugese, Slowaakse, Sloveense en Spaanse taal zijn authentiek)

DE COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN,

Gelet op het Verdrag tot oprichting van de Europese Gemeenschap,

Gelet op Verordening (EG) 2252/04 van de Raad van 13 december 2004[1] betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten, en met name op artikel 2,

Overwegende hetgeen volgt:

(1) Verordening (EG) 2252/04 van 13 december 2004 behelst slechts de algemene en niet-geheime specificaties voor paspoorten en reisdocumenten. Deze dienen te worden aangevuld met bijkomende technische specificaties die geheim moeten blijven.

(2) Er is besloten dat de in deze beschikking vastgelegde specificaties niet geheim moeten worden gehouden, aangezien zij hoofdzakelijk verwijzen naar voor eenieder toegankelijke documenten.

(3) Overeenkomstig Besluit 2000/365/EG van de Raad van 29 mei 2000 betreffende het verzoek van het Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland deel te mogen nemen aan enkele van de bepalingen van het Schengenacquis, heeft het Verenigd Koninkrijk niet deelgenomen aan de vaststelling van de verordening en is deze niet bindend voor, noch van toepassing op het Verenigd Koninkrijk, aangezien zij een ontwikkeling vormt van de bepalingen van het Schengenacquis. Deze beschikking is derhalve niet tot het Verenigd Koninkrijk gericht.

(4) Overeenkomstig Besluit 2002/192/EG van de Raad van 28 februari 2002 betreffende het verzoek van Ierland deel te mogen nemen aan bepalingen van het Schengenacquis, heeft Ierland niet deelgenomen aan de vaststelling van de verordening en is deze niet

[1] PB L385 van 29 december 2004, blz. 1

bindend voor, noch van toepassing op Ierland, aangezien zij een ontwikkeling vormt van de bepalingen van het Schengacquis. Deze beschikking is derhalve niet tot Ierland gericht.

(5) Overeenkomstig de artikelen 1 en 2 van het Protocol betreffende de positie van Denemarken dat is gehecht aan het Verdrag betreffende de Europese Unie en het Verdrag tot oprichting van de Europese Gemeenschap, heeft Denemarken niet deelgenomen aan de vaststelling van de verordening en is deze derhalve niet bindend voor, noch van toepassing op Denemarken. Aangezien de verordening evenwel tot doel heeft het Schengenacquis te ontwikkelen krachtens de bepalingen van titel IV van het derde deel van het Verdrag tot oprichting van de Europese Gemeenschap, beslist Denemarken overeenkomstig artikel 5 van genoemd protocol binnen zes maanden nadat de Raad de verordening heeft vastgesteld, of het deze al dan niet in zijn nationale wetgeving zal omzetten. Deze beschikking is in dit geval ook tot Denemarken gericht.

(6) Wat IJsland en Noorwegen betreft, vormt deze verordening een ontwikkeling van de bepalingen van het Schengenacquis zoals bedoeld in de door de Raad van de Europese Unie, de Republiek IJsland en het Koninkrijk Noorwegen gesloten overeenkomst inzake de wijze waarop deze twee staten worden betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis, vallend onder artikel 1, punt B, van Besluit 1999/437/EG van de Raad van 17 mei 1999 inzake bepaalde toepassingsbepalingen van die overeenkomst[2]. Deze beschikking van de Commissie is derhalve bindend voor Noorwegen en IJsland.

(7) Wat Zwitserland betreft, vormt de verordening een ontwikkeling van de bepalingen van het Schengenacquis zoals bedoeld in de Overeenkomst tussen de Europese Unie, de Europese Gemeenschap en de Zwitserse Bondsstaat inzake de wijze waarop Zwitserland wordt betrokken bij de uitvoering, de toepassing en de ontwikkeling van het Schengenacquis, vallend onder artikel 4, lid 1, van het besluit van de Raad inzake de onderteking namens de Europese Gemeenschap, en inzake de voorlopige toepassing van enkele bepalingen van die overeenkomst.

(8) De in deze beschikking beoogde maatregelen zijn in overeenstemming met het advies van het comité dat werd opgericht op grond van artikel 6 van Verordening (EG) 1683/95,

HEEFT DE VOLGENDE BESCHIKKING VASTGESTELD:

Artikel 1

De technische specificaties in verband met de normen voor de veiligheidskenmerken van en de biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten die de in Verordening (EG) 2252/04 vastgelegde specificaties aanvullen, worden vastgesteld overeenkomstig de bijlage bij deze beschikking.

---

[2] PB L176 van 10.7.1999, blz. 31.

Artikel 2

De lidstaten werken samen bij de uitvoering van deze beschikking, met name door informatie over alle technische specificaties uit te wisselen.

Elke lidstaat zendt de Commissie en de andere lidstaten een referentiespecimen toe van de door hem afgegeven paspoorten en reisdocumenten. Elke lidstaat houdt ook specimens van volgende drukoplagen bij en houdt deze ter beschikking van de Commissie en van de andere lidstaten.

Artikel 3

Deze beschikking is gericht tot België, Cyprus, Duitsland, Estland, Finland, Frankrijk, Griekenland, Italië, Letland, Litouwen, Luxemburg, Hongarije, Malta, Nederland, Oostenrijk, Polen, Portugal, Slovenië, Slowakije, Spanje, Tsjechië, Zweden.

Gedaan te Brussel, 28/II/2005

Voor de Commissie
Franco FRATTINI
Lid van de Commissie

VOOR GELIJKLUIDEND AFSCHRIFT
Voor de Secretaris – generaal,

Patricia BUGNOT
Directeur van de Griffie

Opneming van biometrische gegevens in EU-paspoorten

Specificaties voor EU-paspoorten

Bijlage bij de beschikking/het besluit van de Commissie van 28/II/2005 C(2005)409

Inhoud

1 Werkingssfeer en beperkingen

In dit document worden oplossingen voor EU-paspoorten met microchips voorgesteld op grond van het hierna genoemde EU-document [1]:

> *"Ontwerpverordening van de Raad betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten"*

Dit document is gebaseerd op internationale normen, in het bijzonder ISO-normen en aanbevelingen van de ICAO betreffende machineleesbare reisdocumenten. De volgende aspecten worden erin behandeld:

- specificaties voor biometrische identificatiemiddelen: gezichtsopname en vingerafdrukken
- opslagmedium (chip)
- logische gegevensstructuur op de chip
- specificaties voor de beveiliging van de digitaal op de chip opgeslagen gegevens
- beoordeling van de conformiteit van de chip en de toepassingen
- FR-compatibiliteit met andere elektronische reisdocumenten.

De volgende aspecten vallen buiten het bestek van dit document:

- specificaties voor de mechanische integratie van de chip in een paspoortboekje, duurzaamheid en mechanische testprocedures.
- specificaties voor de standaardwerkprocedures (Standard Operation Procedures – SOP's) voor de enrolment- of controleprocedure.

2 Biometrie

2.1 Primair biometrisch kenmerk – Gezicht

2.1.1 Overeenstemming met de normen

- ICAO NTWG, Biometrics Deployment of Machine Readable Travel Documents, Technical Report, Version 2.0, 5 mei 2004 [3]
- ISO/IEC FCD 19794-5: Biometric Data Interchange Formats – Part 5: Face Image Data [4]

2.1.2 Type

Er moet een FRONTALE OPNAME[1] van het gezicht worden opgeslagen, overeenkomstig [3, 4].

[1] In de ICAO-normen is het volgende vastgesteld: "Face biometric data interchange image recorded in Datagroup 2 [of the LDS] shall be derived from the passport photo used to create the displayed portrait printed on the data page of the Machine Readable Passport; and shall be encoded either according to type 2 (full frontal image) or type 3 (token image) formats set out in the latest version of ISO 19794 -5." ("In datagroep 2 [van de LDS – logische gegevensstructuur] vast-

2.1.3 Formaat

De gezichtsopname moet worden opgeslagen als een gecomprimeerd BEELDBESTAND, niet als een vendorspecifieke template.

Hoewel de JPEG- en de JPEG2000-compressie allebei in overeenstemming zijn met de normen [3], wordt JPEG2000 aanbevolen voor EU-paspoorten, omdat de bestanden in vergelijking met gecomprimeerde JPEG-afbeeldingen kleiner zijn[2].

2.1.4 Vereiste opslagcapaciteit

Nr.	Optie	Opmerking	Aanbeveling
1	JPEG-compressie	ongeveer 12-20 kilobyte per foto	
2	JPEG2000-compressie	ongeveer 6-10 kilobyte per foto	aanbevolen (zie 2.1.3)

2.1.5 Andere aspecten

- Er moeten richtsnoeren voor het maken van de foto's waarbij rekening wordt gehouden met de vereisten van de gelaatsherkenningstechnologie worden goedgekeurd overeenkomstig de ICAO-normen [3].

2.2 Secundair biometrisch kenmerk – Vingerafdrukken

2.2.1 Overeenstemming met de normen

- ICAO NTWG, Biometrics Deployment of Machine Readable Travel Documents, Technical Report, Version 2.0, 5 mei 2004 [3]
- ISO/IEC FCD 19794-4, Biometric Data Interchange Formats – Part 4: Finger Image Data [5]
- ISO/IEC FCD 19794-2, Biometric Data Interchange Formats – Part 2: Finger Minutiae Data [6]
- ANSI/NIST-ITL 1-2000 Standard "Data Format for the Interchange of Fingerprint, Facial, Scarmark & Tattoo (SMT) Information"; FBI: Wavelet Scalar Quantization (WSQ) [15]

gelegde afbeeldingen voor de biometrische gegevensuitwisseling moeten worden afgeleid van de pasfoto die wordt gebruikt voor de foto die wordt afgedrukt op de pagina met persoonsgegevens van het machineleesbare paspoort en moeten worden versleuteld overeenkomstig de formats van type 2 (volledig frontale opname) of type 3 (token image) die zijn vermeld in de laatste versie van ISO 19794-5.")

[2] Het commerciële gebruik van JPEG2000 kan éénmalige kosten voor SDK en support ten belope van 7 000 EUR ten gevolge hebben.

2.2.2 Type

De primaire vingerafdrukken die in het Europees paspoort moeten worden opgenomen, zijn:

PLATTE (NIET GEROLDE) AFDRUKKEN VAN DE LINKER- EN DE RECHTER-WIJSVINGER

Wanneer de kwaliteit van de vingerafdrukken van de wijsvingers ontoereikend is en/of in geval van verwonding van de wijsvingers moeten platte afdrukken van de middelvingers, ringvingers of duimen van goede kwaliteit worden opgenomen[3].

2.2.3 Formaat en kwaliteit

De vingerafdrukken moeten als AFBEELDINGEN worden opgeslagen, overeenkomstig [5].

De kwaliteit van de vingerafdrukbeelden moet in overeenstemming zijn met [5] en [15].

Voor de compressie van de afbeeldingen gebruik worden gemaakt van de WSQ-algoritme overeenkomstig [15], teneinde de omvang van het bestand te verkleinen..

2.2.4 Opslagcapaciteit

Voor AFBEELDINGEN van vingerafdrukken is ongeveer 12–15 kilobyte per vinger vereist.

3 Opslagmedium (RF-chiparchitectuur)

3.1 Overeenstemming met de normen

- ICAO NTWG, Biometrics Deployment of Machine Readable Travel Document, Technical Report, Version 2.0, 5 mei 2004 [3]
- ISO/IEC FDIS 14443, Identification cards - Contactless integrated circuit(s) cards - Proximity cards [7]
- ICAO NTWG, Use of Contactless Integrated Circuits In Machine Readable Travel Documents, Technical Report, Version 3.1, 16 april 2003 [8]

3.2 RF-interface

Overeenkomstig [3,7,8] worden zowel de RF-interfaces van type A als die van type B in overeenstemming geacht met de ICAO-normen.

Paspoorten die aan de ICAO-normen voldoen, zullen zijn voorzien van RF-interfaces van type A en van type B, zodat de grenscontrolesystemen voor paspoorten en visa aan beide normen zullen moeten zijn aangepast.

3.3 Vereiste opslagcapaciteit

Overeenkomstig de logische gegevensstructuur van de ICAO [10] moeten de alfanumerieke gegevens van de machineleesbare strook (MRZ) van het document en de digitale documentbeveiligings-

[3] In het opslagformaat (CBEFF – Common Biometric Exchange File Format) wordt vastgelegd welke vinger is gebruikt (linkerwijsvinger, rechtermiddelvinger, enz.), teneinde te waarborgen dat de verificatie aan de hand van de juiste vinger gebeurt.

data (PKI: infrastructuur met publieke sleutel) samen met de biometrische identificatiegegevens op de chip worden opgeslagen.

De lidstaten moeten RF-chips gebruiken waarop alle overeenkomstig de EU-verordening [1] vereiste persoonsgegevens en biometrische kenmerken kunnen worden opgeslagen. Zie ook hoofdstuk 2.1.4 en 2.2.4.

Indien een lidstaat overeenkomstig de EU-verordening [1] andere gegevens op de chip wenst op te nemen, kan een grotere opslagcapaciteit nodig zijn.

4 Lay-out van de chip voor elektronische paspoorten (gegevensstructuur)

4.1 Overeenstemming met de normen

- ICAO Doc 9303, Part 1, Machine Readable Passports, Fifth Edition, 2003 [9]
- Gemeenschappelijke instructies aan de diplomatieke en consulaire beroepsposten (Common Consular Instructions - CCI), hoofdstuk VI, punt 4 en bijlage 10
- ICAO NTWG, Development of a Logical Data Structure – LDS for optional capacity expansion technologies, Technical Report, Revision 1.7, 18 mei 2004 [10]

4.2 Correlatie met gedrukte gegevens

De alfanumerieke gegevens die in de machineleesbare strook van het paspoort zijn gedrukt overeenkomstig [9], moeten correleren met de gegevens die digitaal in de chip zijn opgeslagen overeenkomstig [10].

4.3 Logische gegevensstructuur van de chip

Overeenkomstig [10].

5 Gegevensbeveiliging en -integriteit

Ter voorkoming van namaak wordt in het traditionele paspoort gebruik gemaakt van een aantal beveiligingselementen, zoals veiligheidsdruk en optisch variabele kenmerken (OVD) overeenkomstig [1]. De integriteit, authenticiteit en vertrouwelijkheid van de gegevens die digitaal in de chip van het paspoort zijn opgeslagen, moeten in gelijke mate worden gewaarborgd.

5.1 Overeenstemming met de normen

- ICAO NTWG, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Technical Report, Version 1.1, 1 oktober 2004 [11]
- ISO/IEC 7816-4, Identifications cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange [12]
- Access Control for Machine Readable Travel Documents, Preliminary Draft, 2004 [13]
- CWA 14890-1:2004, Application Interface for smart cards used as Secure Signature Creation Devices , Part 1 - Basic requirements, Version 1.09 rev2 [16]

5.2 Beveiliging van digitale gegevens

Nr.	Beveiliging	Opmerking	Gebruik

Nr.	Beveiliging	Opmerking	Gebruik
1	Passieve authenticatie [11, 12]	Bewijst dat de inhoud van het SO_D en de LDS authentiek is en niet is gewijzigd. Voorkomt een exacte kopie of vervanging van de chip niet. Voorkomt ongeoorloofde toegang niet. Voorkomt "skimming" (het ongeoorloofd kopiëren van gegevens) niet.	NOODZAKELIJK voor alle gegevens (verplicht veiligheidselement van de ICAO)
2	Actieve authenticatie [11, 12]	Bewijst dat het SO_D geen kopie is, maar van de authentieke chip is gelezen. Bewijst dat de chip niet is vervangen. Vereist processorchips.	FACULTATIEF
3	Basic Access Control (eenvoudige toegangscontrole) [11, 12, 16]	Voorkomt skimming. Voorkomt eavesdropping (ongeoorloofd afluisteren) van de communicatie tussen het MRTD (machineleesbare reisdocument) en het controlesysteem (wanneer gebruikt voor het creëren van een versleuteld kanaal). Voorkomt een exacte kopie of vervanging van de chip niet (vereist ook het kopiëren van het traditionele document). Vereist processorchips.	NOODZAKELIJK voor alle gegevens
4	Extended Access Control (uitgebreide toegangscontrole) [11, 12, 13]	Voorkomt ongeoorloofde toegang tot vingerafdrukgegevens. Voorkomt skimming van vingerafdrukgegevens. Vereist aanvullend sleutelmanagement. Voorkomt een exacte kopie of vervanging van de chip niet (vereist ook het kopiëren van het traditionele document). Vereist processorchips.	Aanvullende bescherming NOODZAKELIJK voor vingerafdrukgegevens

SO_D Document Security Object (SO_D). Dit object wordt door de staat van afgifte digitaal ondertekend en bevat de representatie van de LDS-inhoud in hash-code.

LDS	Logical Data Structure (logische gegevensstructuur)
MRTD	Machine Readable Travel Document (machineleesbaar reisdocument)
MRZ	Machine Readable Zone (machineleesbare strook, machineleesbare zone)

De specificaties inzake de uitgebreide toegangscontrole (Extended Access Control) en de PKI zullen in een afzonderlijk besluit van de Commissie worden behandeld.

5.3 Veiligheidsinfrastructuur

Teneinde de integriteit en de authenticiteit van de op de chip opgeslagen digitale gegevens te waarborgen, wordt een "vlakke" infrastructuur met publieke sleutel (PKI) ingevoerd.

Country Signing CA Certificate:

- Door de CA (certificatieautoriteit) van het ondertekenende land zelf ondertekend en afgegeven certificaat van het hoogste niveau dat als een teken van betrouwbaarheid geldt voor de ontvangende staat.
- De "Country Signing CA Private Key" (private sleutel van de CA van het ondertekenende land) wordt gebruikt om de "Document Signer Certificates" te ondertekenen.
- "Country Signing CA Certificates" (certificaten van de CA van het ondertekenende land) moeten initieel via "diplomatieke weg" worden toegezonden. Een latere update via elektronische weg moet worden gespecificeerd.

Document Signer Certificate:

- De "Document Signer Private Key" (private sleutel van de ondertekenaar van het document) wordt gebruikt om Document Security Objects te ondertekenen.
- "Document Signer Certificates" (certificaten van de ondertekenaar van het document), die in iedere staat door een nationale Document Signing Authority (autoriteit voor het ondertekenen van documenten) worden verstrekt, MOETEN worden opgeslagen op de chip in het paspoort.

De relatie tussen de certificaten voor de elektronische paspoorten en de elektronische visa:

De lidstaten zullen naar alle waarschijnlijkheid elektronische paspoorten en elektronische visa afgeven die voldoen aan de ICAO-normen.

- De lidstaten wordt aanbevolen hetzelfde "Country Signing CA Certificate" te gebruiken voor de paspoorten en de visa.
- Ten gevolge van de gedecentraliseerde personalisering van de visa zullen de "Document Signer Certificates" voor visa verschillen van die voor paspoorten. Er moeten verschillende benamingen voor de "Document Signer Certificates" voor visa en voor die voor elektronische paspoorten worden ingevoerd, om deze van elkaar te onderscheiden.

Voor nadere gegevens, zie [11].

6 Conformiteitsbeoordeling

Er zal worden beoordeeld of de reisdocumenten met biometrische gegevens in overstemming zijn met [14].

Er zullen beschermingsprofielen voor reisdocumenten met biometrische gegevens worden ontwikkeld.

7 Referentiedocumenten

[1] "Verordening (EG) nr. 2252/2004 van de Raad betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten"

[2] "Voorstel voor een verordening van de Raad tot wijziging van Verordening (EG) nr. 1683/95 betreffende de invoering van een uniform visummodel"
"Voorstel voor een verordening van de Raad tot wijziging van Verordening (EG) nr. 1030/2002 betreffende de invoering van een uniform model voor verblijfstitels voor onderdanen van derde landen"
EU-document 14969/1/03 REV1, 21 november 2003

[3] ICAO NTWG, Biometrics Deployment of Machine Readable Travel Documents, Technical Report, Version 2.0, 5 mei 2004 [ICAO Bio]

[4] ISO/IEC FCD 19794-5: Biometric Data Interchange Formats – Part 5: Face Image Data

[5] ISO/IEC FCD 19794-4, Biometric Data Interchange Formats – Part 4: Finger Image Data

[6] ISO/IEC FCD 19794-2, Biometric Data Interchange Formats – Part 2: Finger Minutiae Data

[7] ISO/IEC FDIS 14443, Identification cards – Contactless integrated circuit(s) cards - Proximity cards

[8] ICAO NTWG, Use of Contactless Integrated Circuits In Machine Readable Travel Documents, Technical Report, Version 3.1, 16 april 2003

[9] ICAO Doc 9303, Part 1, Machine Readable Passports, Fifth Edition, 2003

[10] ICAO NTWG, Development of a Logical Data Structure – LDS for optional capacity expansion technologies, Technical Report, Revision 1.7, 18 mei 2004

[11] ICAO NTWG, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Technical Report, Version 1.1, 1 oktober 2004

[12] ISO/IEC 7816-4, Identifications cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange

[13] Access Control for Machine Readable Travel Documents, Preliminary Draft, 2004

[14] Gemeenschappelijke criteria

[15] ANSI/NIST-ITL 1-2000 Standard "Data Format for the Interchange of Fingerprint, Facial, Scarmark & Tattoo (SMT) Information"
FBI: Wavelet Scalar Quantization (WSQ)

www.itl.nist.gov/iad

[16] CWA 14890-1:2004, Application Interface for smart cards used as Secure Signature Creation Devices , Part 1 - Basic requirements, Version 1.09 rev2
http://www.uninfo.polito.it/ws_esign/docs.htm