



Datum
18 april 2005

Ons kenmerk
BPR2005/54982

Onderdeel
DGKB/BPR

Inlichtingen
mw mr M. Gonzalez
T 070 361 3121
F

Uw kenmerk

Blad
1 van 7

Aantal bijlagen
2

Bezoekadres
Lange Vijverberg 11
2513 AC Den Haag

Postadres
Postbus 10451
2501 HL Den Haag

Internetadres
www.bprbzk.nl

De voorzitter van de Tweede Kamer der Staten-
Generaal
Binnenhof 4
2513 AA Den Haag

Onderwerp
Implementatie van de verordening van de
Europese Unie betreffende normen voor de
veiligheidskenmerken van en biometrische
gegevens in door de lidstaten afgegeven
reisdocumenten

Inleiding

Met deze brief wil ik u informeren over de wijze waarop de Nederlandse regering de verordening¹ van de Europese Unie (EU) betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten zal implementeren. In het verlengde hiervan rapporteer ik over de voortgang van de zogenaamde "biometrieproef". Tenslotte ga ik mede namens de minister van Justitie in op de vorming van een centrale registratie van biometrische gegevens, die ten grondslag ligt aan een informatie-infrastructuur die is aangekondigd in de brief van 24 januari 2005² inzake de bestrijding van terrorisme.

EU-verordening betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten (EU-verordening)

De verordening (als bijlage 1 bijgevoegd) heeft tot doel³ de paspoorten en overige reisdocumenten van de lidstaten van de Europese Unie beter te beveiligen tegen vervalsing en frauduleus gebruik. Hiertoe bepaalt artikel 1 van de verordening dat de door de lidstaten afgegeven paspoorten en andere reisdocumenten aan de minimum-veiligheidsnormen moeten voldoen die in de bijlage bij de verordening zijn vastgelegd. Daarnaast schrijft de verordening voor dat in deze documenten een opslagmedium wordt gebruikt dat een gezichtsopname bevat (de zogenaamde gelaatscan), terwijl daarin ook vingerafdrukken in een interoperabel formaat moeten worden opgenomen. Een uitzondering is gemaakt (artikel 1 lid 3) voor de documenten die een geldigheidsduur hebben van 12 maanden of korter.

¹ Verordening (EG) Nr. 2252/2004 van de Raad van 13 december 2004

² TK 2004-2005, 29 754 nr 5

³ TK 2003-2004, 22 111 nr 318



Datum
18 april 2005

Ons kenmerk
BPR2005/54982

Onderdeel
DGKB/BPR

Blad
2 van 7

Op 28 februari 2005 heeft de Europese Commissie een beschikking uitgevaardigd waarin zij de technische specificaties heeft vastgesteld voor de opslag van de biometrische kenmerken in de reisdocumenten van de lidstaten. Met de vaststelling van deze specificaties treedt de invoeringstermijn van 18 maanden in werking voor de invoering van de gelaatscan. Dit betekent dat de reisdocumenten van de lidstaten van de Europese Unie vóór 28 augustus 2006 een chip moeten bevatten met daarin de gelaatscan en de alfanumerieke gegevens die nu al zijn opgenomen in de machineleesbare strook van de documenten. De invoeringstermijn voor de vingerafdrukken (36 maanden) is nog niet in werking getreden. De uitwerking van de beveiliging van de vingerafdrukken in de chip is nog gaande. De Europese Commissie zal daaromtrent op een later moment nog een aanvullende beschikking treffen.

Over de financiering van de invoering van biometrie in de reisdocumenten zal ik de Tweede Kamer in de begroting voor 2006 nader informeren.

Technische implementatie van de verordening

Zoals uit de brieven van 19 december 2003⁴ en 5 oktober 2004⁵ aan uw Kamer kan worden afgeleid, is tot nu toe het voornemen geweest om de Nederlandse reisdocumenten te voorzien van zowel de gelaatscan als de vingerafdruk. De reden daarvoor is dat naar mijn mening de gelaatscan alleen onvoldoende is om zogenaamde look alike fraude te bestrijden. Met de vingerafdrukken (al dan niet in combinatie met de gelaatscan) kan dat wel.

Nu echter de technische specificaties voor de vingerafdrukken (nog) niet vastgesteld zijn door de Europese Commissie, zie ik mij genoodzaakt de biometrische kenmerken gefaseerd in te voeren. Zou ik dat niet doen, dan zou Nederland de invoeringstermijn voor de gelaatscan overschrijden.

De nu door mij voorziene gefaseerde invoering houdt in dat zo spoedig mogelijk in de Nederlandse reisdocumenten een chip wordt opgenomen waarin, conform de door de Europese Commissie vastgestelde specificaties, een gecomprimeerd beeldbestand van het gelaat van de houder van het reisdocument wordt opgeslagen. Over de beveiliging van de in de chip op te nemen gegevens heb ik u reeds in mijn brief van 29 november 2004⁶ geïnformeerd. Recapitulerend houdt de beveiliging in:

- dat de chip, nadat de chip is gepersonaliseerd, wordt gesloten. Daardoor kan er geen informatie meer aan de chip worden toegevoegd;
- het gebruik van een zogenaamde "Document Security Object"⁷. Dit is een digitale handtekening van de uitgevende instantie. De digitale handtekening maakt het mogelijk om de authenticiteit van de opgeslagen gegevens te verifiëren;

⁴ TK 2003-2004, 25764 nr 22

⁵ TK 2004-2005, 25764 nr 4

⁶ TK 2004-2005, 23 490 nr 350

⁷ ICAO-document: PKI for MRTD offering ICC Read-only Access (versie 1.1)





Datum
18 april 2005

Ons kenmerk
BPR2005/54982

Onderdeel
DGKB/BPR

Blad
3 van 7

- het gebruik van de zogenaamde "Actieve Authenticatie" tegen het kopiëren en vervalsen van de inhoud van de chip;
- het gebruik van een vorm van toegangscontrole (Basic Access Control) om het ongeoorloofd en ongemerkt uitlezen van de chip tegen te gaan;
- het gebruik van een versleutelde verbinding (Secure Messaging) tegen af luisteren/aftappen bij het uitlezen van de chip (door de uitleesapparatuur). Deze techniek zorgt er voor dat de communicatie tussen de chip en de reader versleuteld plaatsvindt.

Het is, gelet op de betekenis van de vingerafdrukken voor de bestrijding van look alike fraude, mijn voornemen om onmiddellijk na de vaststelling van de specificaties te starten met de invoering van de vingerafdrukken in de Nederlandse reisdocumenten. In dit verband wijs ik erop dat de in de chip opgeslagen vingerafdrukken nog extra beveiligd zullen worden door gebruik van "Extended Access Control". Deze techniek zorgt ervoor dat de vingerafdrukken alleen uitgelezen kunnen worden door daartoe geautoriseerde apparatuur van bevoegde instanties.

Juridische implementatie van de verordening

De Europese verordening beperkt zich tot het stellen van normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten. In de Paspoortwet zijn thans geen bepalingen opgenomen, die strijdig zijn met het gestelde in de verordening. In het licht van het feit dat de verordening rechtstreekse werking heeft, houdt dit in dat de invoering van de nieuwe normen in de Nederlandse reisdocumenten kan plaatsvinden zonder dat daarvoor aanpassing van de Paspoortwet noodzakelijk is.

Er dienen echter wel enkele aanvullende voorschriften te worden gegeven in verband met de administratieve procedures. Daarbij dient onderscheid te worden gemaakt tussen de invoering van de gelaatscan en de invoering van vingerafdrukken.

In de huidige generatie reisdocumenten is er sprake van het gebruik van een digitaal gescande foto van de aanvrager, die in het reisdocument wordt opgenomen in de vorm van enerzijds een met de houderpagina geïntegreerde fotoafbeelding en anderzijds een in die pagina aangebrachte imageperforatie. Dezelfde techniek wordt toegepast in de Nederlandse identiteitskaart. De opslag van de gegevens van de digitaal gescande foto in een chip, die vervolgens ook in de houderpagina wordt aangebracht, is in dit opzicht niet meer dan een derde variant om het reisdocument van een foto te voorzien. Aanpassing van de wet- en regelgeving is ook niet noodzakelijk om de gelaatscan in de reisdocumentenadministratie op te kunnen slaan. De gedigitaliseerde foto die bij de aanvraag wordt gemaakt is namelijk al in die administratie opgenomen.





Datum
18 april 2005

Ons kenmerk
BPR2005/54982

Onderdeel
DGKB/BPR

Blad
4 van 7

Voor de opnemings van vingerafdrukken geldt dat deze op basis van de Europese verordening kan plaatsvinden, zonder daarvoor de Paspoortwet te hoeven wijzigen. Niettemin is aanpassing van de Paspoortwet toch noodzakelijk om de vingerafdrukken ook in de reisdocumentenadministratie te kunnen opslaan en van daaruit te kunnen verstrekken bij verificatie. Voorts zullen de paspoortuitvoeringsregelingen moeten worden gewijzigd en onder andere bepalingen gaan bevatten die betrekking hebben op het afnemen van de vingerafdrukken bij de aanvraag van het reisdocument. De desbetreffende aanpassingen in de wet- en regelgeving zullen in gang worden gezet zodra de Europese Commissie de aanvullende specificaties voor de vingerafdrukken heeft vastgesteld.

De Europese verordening is van toepassing op door de lidstaten afgegeven paspoorten en reisdocumenten. Ingevolge artikel 2 van de Paspoortwet is de Nederlandse identiteitskaart een reisdocument van Nederland. Dit betekent dat de bepalingen in de verordening ook rechtstreeks gelden voor de Nederlandse identiteitskaart. Een afzonderlijke aanpassing van de Paspoortwet voor de invoering van de gelaatscan en vingerafdrukken in het model van de Nederlandse identiteitskaart is derhalve niet aan de orde.

Met uitzondering van de Nederlandse identiteitskaart zijn alle andere soorten Nederlandse reisdocumenten ingevolge artikel 2 van de Paspoortwet reisdocumenten van het Koninkrijk. De reisdocumenten van het Koninkrijk hebben overal hetzelfde model en worden door dezelfde producent in Nederland vervaardigd. De aanpassing van het model conform de Europese verordening betekent dat alle reisdocumenten van het Koninkrijk voorzien zullen gaan worden van een chip met gelaatscan en vingerafdrukken.

Op 22 april 2002 is bij de Tweede Kamer het wetsvoorstel tot wijziging van de Paspoortwet, onder andere in verband met het toepassen van biometrie in reisdocumenten ingediend⁸. Op 10 juli 2002 heeft de Tweede Kamer het verslag met betrekking tot het wetsvoorstel vastgesteld⁹. De nota naar aanleiding van het verslag is niet uitgebracht. Enerzijds is dat het gevolg van politieke ontwikkelingen rond de invoering van biometrie op reisdocumenten in Europees en internationaal verband, die uiteindelijk hebben geleid tot de bovengenoemde Europese verordening. Anderzijds hebben technische ontwikkelingen geleid tot een aanpassing van biometrische technieken in reisdocumenten, met name binnen de ICAO. De technische specificaties die ICAO voor de gelaatscan heeft vastgesteld zijn, zoals hiervoor is vermeld, inmiddels overgenomen door de Europese Commissie. Door de hierboven genoemde ontwikkelingen is het in 2002 ingediende wetsvoorstel tot wijziging van de Paspoortwet inmiddels achterhaald. Daarom zal ik bevorderen dat genoemd wetsvoorstel zal worden ingetrokken.

⁸ TK 2001-2002, 28 342 (R 1719)

⁹ TK 2001-2002, 28 342 (R 1719), nr. 5.





Datum
18 april 2005

Ons kenmerk
BPR2005/54982

Onderdeel
DGKB/BPR

Blad
5 van 7

Biometrieproef

Van 28 augustus 2004 tot 28 februari 2005 is in zes gemeenten¹⁰ een proef gehouden waarbij burgers die een reisdocument komen aanvragen hebben kunnen meedoen aan een testtraject waarin een testreisdocument met biometrie werd aangevraagd. Van de deelnemers zijn twee vingerafdrukken en een gelaatscan opgenomen.

Deze gegevens zijn (versleuteld) gezonden naar de leverancier van de reisdocumenten die vervolgens een testdocument heeft geproduceerd voorzien van een chip met daarin de biometrische kenmerken (gelaatscan en vingerafdrukken). Het testdocument is gebruikt om de biometrische kenmerken te verifiëren.

De proef is goed verlopen. De zes gemeenten hebben met veel inzet en enthousiasme meegewerkt aan de proef. In totaal zijn 14.779 biometrische testdocumenten geproduceerd voor de proef. Gepland waren ca. 15.000 documenten.

De proef wordt thans geëvalueerd. In die evaluatie staan de volgende vragen centraal:

- Welke praktische gevolgen heeft invoering van biometrie op de reisdocumenten voor de uitgevende instanties van de reisdocumenten;
- Doen zich problemen/knelpunten voor (bijvoorbeeld ten aanzien van de bouwkundige voorzieningen, de beoordeling van de kwaliteit van de opgenomen biometrische kenmerken, etc).

De afronding van de evaluatie is begin mei 2005 gepland.

On line verificatie van de Nederlandse reisdocumenten

In de brief van 24 januari 2005 inzake de bestrijding van terrorisme is aangekondigd dat het kabinet een informatie-infrastructuur zal ontwikkelen om de identiteitsdocumenten die biometrische kenmerken gaan bevatten on line te kunnen verifiëren in de administratie van die documenten. Het gaat hierbij om de documenten die in Nederland op grond van de Wet op de identificatieplicht (WID) als identiteitsdocument zijn aangemerkt en die op grond van Europese regelgeving biometrische kenmerken gaan bevatten. In casu zijn dit de Nederlandse reisdocumenten en de vreemdelingendocumenten.

¹⁰ Apeldoorn, Almere, Eindhoven, Groningen, Rotterdam en Utrecht





Datum
18 april 2005

Ons kenmerk
BPR2005/54982

Onderdeel
DGKB/BPR

Blad
6 van 7

De on line verificatie van de documenten in de administratie van die documenten is noodzakelijk om (meer) zekerheid te kunnen krijgen omtrent de identiteit van de houder van het document en de betrouwbaarheid van het document. Het belang van deze controles is groot. In het kader van de bestrijding van terrorisme is het van het grootste belang dat voorkomen wordt dat terroristen de identiteit kunnen aannemen van andere personen en als gevolg daarvan onopgemerkt blijven. Daarnaast berokkent identiteitsfraude de samenleving in vele sectoren jaarlijks enkele miljoenen Euro's¹¹ aan financiële schade. Ook de bestrijding hiervan is voor het kabinet een prioriteit.

De on line verificatie die het kabinet voorstaat heeft belangrijke voordelen ten opzichte van de controles die nu mogelijk zijn. Nu kan on line alleen nagegaan worden of een document als vermist cq gestolen geregistreerd staat en derhalve niet in het maatschappelijk verkeer zou mogen voorkomen. In de toekomst zal ook on line geverifieerd kunnen worden of de gegevens die in het document staan overeenkomen met de gegevens die bij de aanvraag van het document in de administratie zijn opgeslagen. Tot die gegevens behoren ook de biometrische gegevens (gelaatscan en vingerafdruk). De meerwaarde van de verificatie van de biometrische gegevens in de administratie is er in gelegen dat daarmee een middel voorhanden is om manipulatie van die gegevens in het document te kunnen detecteren.

Ook voor het aanvraag- en uitgifteproces van de Nederlandse reisdocumenten heeft het on line kunnen raadplegen van de administratie duidelijke meerwaarde. Het maakt het mogelijk om bij het verwerken van de aanvragen na te gaan of de aanvrager ook bij andere instanties een aanvraag voor een reisdocument heeft ingediend. Tevens krijgen de buitenlandse posten¹² en de paspoortverstrekende instanties in de Nederlandse Antillen en Aruba¹³ toegang tot de reisdocumentenadministratie om de gegevens omtrent eerdere aanvragen te kunnen raadplegen. Nu is die mogelijkheid er niet, omdat de reisdocumentenadministratie alleen decentraal wordt bijgehouden.

In de brief van 24 januari 2005 inzake de bestrijding van terrorisme is aangegeven dat de on line verificatie veronderstelt dat de administraties van de identiteitsdocumenten met biometrische kenmerken centraal zijn georganiseerd. Voor de vreemdelingendocumenten is dat reeds het geval. De reisdocumentenadministratie evenwel kent thans een decentrale opzet inhoudende dat de administratie zich bevindt bij de instanties die reisdocumenten uitgeven.

¹¹ Notitie fraude en financieel-economische criminaliteit: TK 2002-2003, 17050 nr 250

¹² In 2004 zijn door de buitenlandse posten 117.248 reisdocumenten uitgegeven. In dit aantal zijn de uitgegeven nooddocumenten niet inbegrepen

¹³ In 2004 zijn in de NA en Aruba 35.176 reisdocumenten uitgegeven. In dit aantal zijn de uitgegeven nooddocumenten niet inbegrepen





Datum
18 april 2005

Ons kenmerk
BPR2005/54982

Onderdeel
DGKB/BPR

Blad
7 van 7

Dat zijn de gemeenten, de Nederlandse ambassades en beroepsconsulaten in het buitenland, de Kabinetten van de Gouverneurs in de Nederlandse Antillen en Aruba, de gezaghebbers van de eilandgebieden in de Nederlandse Antillen en de daartoe aangewezen brigades van de Koninklijke Marechaussee.

Het voornemen was, zoals dat blijkt uit het wetsvoorstel uit 2002, om bij de invoering van biometrische gegevens in de Nederlandse reisdocumenten die gegevens ook op te nemen in de decentrale reisdocumentenadministratie. Gelet op de maatregelen die het kabinet noodzakelijk acht in het kader van de bestrijding van terrorisme en identiteitsfraude ben ik van plan het zuiver decentrale karakter van de reisdocumentenadministratie te wijzigen en tot centralisatie van de administratie over te gaan.

Dit zal in een separaat wetsvoorstel worden geregeld dat mede gebaseerd zal zijn op het beleidskader voor de bestrijding van identiteitsfraude waar de minister van Justitie thans aan werkt. Het wetsvoorstel zal naast de opzet van de administratie, ook de bescherming en de beveiliging van de administratie regelen, alsmede welke instanties toegang zullen krijgen tot deze administratie.

DE MINISTER VOOR BESTUURLIJKE VERNIEUWING EN
KONINKRIJKSRELATIES,

A. Pechtold



I

(Besluiten waarvan de publicatie voorwaarde is voor de toepassing)

VERORDENING (EG) Nr. 2252/2004 VAN DE RAAD

van 13 december 2004

betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten

DE RAAD VAN DE EUROPESE UNIE,

Gelet op het Verdrag tot oprichting van de Europese Gemeenschap, en met name op artikel 62, lid 2, onder a),

Gezien het voorstel van de Commissie⁽¹⁾,

Gezien het advies van het Europees Parlement⁽²⁾,

Overwegende hetgeen volgt:

- (1) De Europese Raad van Thessaloniki van 19 en 20 juni 2003 heeft bevestigd dat in de Europese Unie een coherente aanpak nodig is inzake het gebruik van biometrische identificatiemiddelen of biometrische gegevens in documenten voor onderdanen van derde landen, paspoorten voor EU-burgers en informatiesystemen (VIS en SIS II).
- (2) Bij een resolutie van de vertegenwoordigers van de regeringen van de lidstaten, in het kader van de Raad bijeen, van 17 oktober 2000 zijn minimumveiligheidsnormen voor paspoorten vastgesteld⁽³⁾. Deze resolutie dient nu door een communautaire maatregel te worden geactualiseerd om te komen tot betere geharmoniseerde veiligheidsnormen voor paspoorten en reisdocumenten ter bescherming tegen vervalsing. Tegelijkertijd moeten er biometrische identificatiemiddelen in het paspoort worden opgenomen, zodat een betrouwbaar verband kan worden gelegd tussen de rechtmatige houder en het document.
- (3) Met de harmonisatie van de veiligheidskenmerken en de integratie van biometrische identificatiemiddelen wordt, met het oog op toekomstige ontwikkelingen op Europees niveau, een belangrijke stap gezet naar het gebruik van nieuwe elementen die het reisdocument veiliger maken

en een betrouwbaarder verband tot stand brengen tussen de houder en het paspoort of reisdocument, hetgeen in belangrijke mate bijdraagt tot de bescherming ervan tegen frauduleus gebruik. Er moet rekening worden gehouden met de specificaties van de Internationale Burgerluchtvaartorganisatie (ICAO), met name die welke zijn opgenomen in document nr. 9303 betreffende machineleesbare reisdocumenten.

- (4) Deze verordening gaat alleen over de harmonisatie van de veiligheidskenmerken, waaronder biometrische identificatiemiddelen, voor de paspoorten en reisdocumenten van de lidstaten. De aanwijzing van de autoriteiten en organisaties die toegang hebben tot de in het opslagmedium opgeslagen gegevens is een zaak van de nationale wetgeving, onder voorbehoud van bepalingen van het communautaire recht, het recht van de Europese Unie of van internationale overeenkomsten terzake.
- (5) Deze verordening behelst slechts de niet-geheime specificaties; deze dienen te worden aangevuld met bijkomende specificaties die geheim moeten blijven teneinde namaak en vervalsing te voorkomen. Dergelijke aanvullende technische specificaties moeten worden vastgesteld overeenkomstig Besluit 1999/468/EG van de Raad van 28 juni 1999 tot vaststelling van de voorwaarden voor de uitoefening van de aan de Commissie verleende uitvoeringsbevoegdheden⁽⁴⁾.
- (6) De Commissie dient te worden bijgestaan door het comité dat is ingesteld bij artikel 6 van Verordening (EG) nr. 1683/95 van de Raad van 29 mei 1995 betreffende de invoering van een uniform visummodel⁽⁵⁾.
- (7) Om te waarborgen dat de bedoelde informatie niet toegankelijk wordt voor meer personen dan noodzakelijk is, is het eveneens van wezenlijk belang dat elke lidstaat niet meer dan één organisatie aanwijst die verantwoordelijk is voor het aanmaken van paspoorten en reisdocumenten, waarbij het de lidstaten vrijstaat indien nodig van organisatie te veranderen; elke lidstaat dient om veiligheidsredenen de naam van de gekozen organisatie aan de Commissie en aan de andere lidstaten mee te delen.

⁽¹⁾ PB C 98 van 23.4.2004, blz. 39.

⁽²⁾ Advies uitgebracht op 2 december 2004 (nog niet gepubliceerd in het Publicatieblad).

⁽³⁾ PB C 310 van 28.10.2000, blz. 1.

⁽⁴⁾ PB L 184 van 17.7.1999, blz. 23.

⁽⁵⁾ PB L 164 van 14.7.1995, blz. 1. Verordening laatstelijk gewijzigd bij de Toetredingsakte van 2003.

- (8) Op de persoonsgegevens die in verband met paspoorten en reisdocumenten moeten worden verwerkt, is Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens⁽¹⁾ van toepassing. Er moet op worden toegezien dat in het paspoort geen andere informatie wordt opgenomen dan die welke wordt genoemd in deze verordening, in de bijlage bij deze verordening of in het reisdocument.
- (9) Overeenkomstig het evenredigheidsbeginsel is het voor het bereiken van de fundamentele doelstelling, namelijk de invoering van gemeenschappelijke veiligheidsnormen en interoperabele biometrische identificatiemiddelen, noodzakelijk en passend dat voorschriften worden vastgesteld voor alle lidstaten die de Schengenuitvoeringsovereenkomst van 14 juni 1985⁽²⁾ toepassen. Overeenkomstig artikel 5, derde alinea, van het Verdrag gaat deze verordening niet verder dan wat nodig is om de beoogde doelstellingen te verwezenlijken.
- (10) 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 aan het Verdrag tot oprichting van de Europese Gemeenschap, neemt Denemarken niet deel aan de aanneming van de verordening en is deze derhalve niet bindend voor, noch van toepassing op Denemarken. Aangezien deze 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.
- (11) Deze verordening vormt een ontwikkeling van de bepalingen van het Schengenacquis waaraan het Verenigd Koninkrijk niet deelneemt 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⁽³⁾; het Verenigd Koninkrijk neemt derhalve niet deel aan de aanneming van deze verordening en is hierdoor niet gebonden, noch onderworpen aan de toepassing ervan.
- (12) Deze verordening vormt een ontwikkeling van de bepalingen van het Schengenacquis waaraan Ierland niet deelneemt 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⁽⁴⁾. Ierland neemt derhalve niet deel aan de aanneming van deze verordening en is hierdoor niet gebonden, noch onderworpen aan de toepassing ervan.
- (13) 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⁽⁵⁾, vallend onder artikel 1, punt B, van Besluit 1999/437/EG van de Raad van 17 mei 1999 inzake bepaalde toepassingsbepalingen van die overeenkomst⁽⁶⁾.
- (14) Wat Zwitserland betreft, vormt deze 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⁽⁷⁾, vallend onder artikel 1, punt B, van Besluit 1999/437/EG van de Raad, in samenhang met artikel 4, lid 1, van de besluiten van de Raad van 25 oktober 2004 inzake de ondertekening namens de Europese Unie, inzake de ondertekening namens de Europese Gemeenschap, en inzake de voorlopige toepassing van enkele bepalingen van die overeenkomst⁽⁸⁾.

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

- Door de lidstaten afgegeven paspoorten en reisdocumenten voldoen aan de in de bijlage vervatte minimumveiligheidsnormen.
- Voor deze paspoorten en reisdocumenten wordt een opslagmedium gebruikt dat een gezichtsoptname bevat. De lidstaten nemen ook vingerafdrukken in een interoperabel formaat op. De gegevens worden beveiligd en het opslagmedium heeft voldoende capaciteit en is voldoende geschikt om de integriteit, de authenticiteit en de vertrouwelijkheid van de gegevens te garanderen.
- Deze verordening is van toepassing op door de lidstaten afgegeven paspoorten en reisdocumenten. Zij is niet van toepassing op door de lidstaten aan hun onderdanen afgegeven identiteitskaarten of op tijdelijke paspoorten en reisdocumenten die een geldigheidsduur van 12 maanden of minder hebben.

⁽¹⁾ PB L 281 van 23.11.1995, blz. 31. Richtlijn laatstelijk gewijzigd bij Verordening (EG) nr. 1882/2003 (PB L 284 van 31.10.2003, blz. 1).

⁽²⁾ PB L 239 van 22.9.2000, blz. 19. Conventie laatstelijk gewijzigd bij Verordening (EG) nr. 871/2004 (PB L 162 van 30.4.2004, blz. 29).

⁽³⁾ PB L 131 van 1.6.2000, blz. 43.

⁽⁴⁾ PB L 64 van 7.3.2002, blz. 20.

⁽⁵⁾ PB L 176 van 10.7.1999, blz. 36.

⁽⁶⁾ PB L 176 van 10.7.1999, blz. 31.

⁽⁷⁾ Document 13054/04 van de Raad:

zie <http://register.consilium.eu.int>

⁽⁸⁾ Documenten 13464/04 en 13466/04 van de Raad:

zie <http://register.consilium.eu.int>

Artikel 2

Volgens de in artikel 5, lid 2, bedoelde procedure worden aanvullende technische specificaties voor het paspoort vastgesteld voor:

- a) aanvullende veiligheidskenmerken en -vereisten, met inbegrip van hogere normen ter voorkoming van vervalsing en namaak;
- b) technische specificaties betreffende het medium voor de opslag van de biometrische gegevens en de veiligheid ervan, zoals het voorkomen van ongeoorloofde toegang;
- c) kwaliteitseisen en gemeenschappelijke normen inzake gezichtsopname en vingerafdrukken.

Artikel 3

1. In overeenstemming met de procedure bedoeld in artikel 5, lid 2, kan worden besloten dat de in artikel 2 bedoelde specificaties geheim zijn en niet bekend worden gemaakt. Zij worden in dat geval uitsluitend verstrekt aan de door de lidstaten aangewezen organisaties die verantwoordelijk zijn voor het drukken en aan door een lidstaat of de Commissie naar behoren gemachtigde personen.

2. Elke lidstaat wijst één organisatie aan die voor het drukken van paspoorten en reisdocumenten verantwoordelijk is. De lidstaat deelt de naam van die organisatie mee aan de Commissie en aan de andere lidstaten. Twee of meer lidstaten kunnen daartoe een zelfde organisatie aanwijzen. Elke lidstaat is gerechtigd om van organisatie te veranderen. Hij stelt de Commissie en de andere lidstaten daarvan op de hoogte.

Artikel 4

1. Onverminderd de bepalingen betreffende de gegevensbescherming hebben de personen aan wie een paspoort of reisdocument wordt afgegeven, het recht de daarin vermelde persoonsgegevens te verifiëren en zo nodig te verzoeken dat deze worden gerectificeerd dan wel geschrapt.

2. Een paspoort of reisdocument bevat geen andere machineleesbare informatie dan die welke wordt genoemd in deze verordening of in de bijlage bij deze verordening dan wel door de lidstaat van afgifte overeenkomstig zijn nationale wetgeving in het paspoort wordt vermeld.

3. Voor de toepassing van deze verordening mogen de biometrische kenmerken in paspoorten en reisdocumenten alleen worden gebruikt voor het verifiëren van:

- a) de authenticiteit van het document;
- b) de identiteit van de houder door middel van direct beschikbare vergelijkbare kenmerken wanneer het overleggen van een paspoort of andere reisdocumenten wettelijk vereist is.

Artikel 5

1. De Commissie wordt bijgestaan door het bij artikel 6, lid 2, van Verordening (EG) nr. 1683/95 ingestelde comité.

2. Wanneer naar dit lid wordt verwezen, zijn de artikelen 5 en 7 van Besluit 1999/468/EG van toepassing.

De in artikel 5, lid 6, van Besluit 1999/468/EG bedoelde termijn wordt vastgesteld op twee maanden.

3. Het comité stelt zijn reglement van orde vast.

Artikel 6

Deze verordening treedt in werking op de twintigste dag volgende op die van haar bekendmaking in het *Publicatieblad van de Europese Unie*.

De lidstaten passen deze verordening toe:

- a) wat betreft de gezichtsopname: uiterlijk 18 maanden
 - b) wat betreft de vingerafdrukken: uiterlijk 36 maanden
- na de aanneming van de in artikel 2 bedoelde maatregelen. Reeds afgegeven paspoorten en reisdocumenten blijven evenwel geldig.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in de lidstaten overeenkomstig het Verdrag tot oprichting van de Europese Gemeenschap.

Gedaan te Brussel, 13 december 2004.

Voor de Raad
De voorzitter
B. R. BOT

BIJLAGE

MINIMUMVEILIGHEIDSNORMEN VOOR DOOR DE LIDSTATEN AFGEGEVEN PASPOORTEN EN REISDOCUMENTEN

Inleiding

In deze bijlage wordt het minimumveiligheidsniveau vastgesteld dat vereist is voor paspoorten en reisdocumenten van de lidstaten. De bepalingen van de bijlage hebben in eerste instantie betrekking op de pagina met persoonsgegevens. De generieke veiligheidskenmerken gelden ook voor de andere delen van de paspoorten.

De pagina met persoonsgegevens kan uit verschillende basismaterialen bestaan. In de bijlage wordt het minimumveiligheidsniveau aangegeven voor het specifieke materiaal dat wordt gebruikt.

1. Materiaal

Het papier dat gebruikt wordt voor de delen van het paspoort of reisdocument waarop persoonsgegevens of andere gegevens worden vermeld, dient te voldoen aan de volgende minimumvereisten:

- geen optische witmakers,
- tweetonig watermerk,
- veiligheidsreagenten tegen chemische radering,
- veiligheidsvezels (deels zichtbaar en deels fluorescerend onder UV-belichting, of onzichtbaar en fluorescerend in tenminste twee kleuren),
- onder UV-belichting fluorescerende planchetten strekken tot aanbeveling (verplicht voor stickers),
- het gebruik van een veiligheidsdraad strekt tot aanbeveling.

Indien de pagina met persoonsgegevens als sticker is uitgevoerd, is een watermerk in het daarvoor gebruikte papier niet vereist. In het papier van de schutbladen van het paspoort is evenmin een watermerk vereist. Op de schutbladen is het gebruik van veiligheidsreagenten uitsluitend vereist indien daarop gegevens worden vermeld.

Binddraad moet worden beveiligd zodat het niet kan worden vervangen.

Indien een voor de vermelding van persoonsgegevens in het paspoort ingevoegde kaart geheel uit synthetisch basismateriaal bestaat, kunnen de voor paspoortpapier bruikbare echtheidskenmerken doorgaans niet worden aangebracht. Bij gebruik van stickers en kaarten moeten de ontbrekende echtheidskenmerken worden gecompenseerd door druktechnische maatregelen, door een antikopieerbeveiliging, of door een in de punten 3, 4 of 5 beschreven techniek, die verder gaan dan de hiernavolgende minimumnormen.

2. Pagina met persoonsgegevens

Het paspoort bevat een machineleesbare pagina met persoonsgegevens die beantwoordt aan de specificaties inzake machineleesbare paspoorten in ICAO-document nr. 9303 betreffende machineleesbare paspoorten (deel 1); de wijze van afgifte daarvan moet met die specificaties stroken.

De afbeelding van de houder wordt eveneens op de pagina met persoonsgegevens aangebracht en mag niet worden gekleefd, maar dient in het materiaal van deze pagina te worden geïntegreerd met behulp van een in punt 5 beschreven personaliseringstechniek.

De persoonsgegevens moeten worden aangebracht op de pagina achter de titelpagina van het paspoort. Op de schutbladen van het paspoort mogen niet langer persoonsgegevens worden aangebracht.

De grafische vormgeving (lay-out) van de pagina met persoonsgegevens moet van die van de overige paspoortpagina's onderscheiden kunnen worden.

3. Druktechnieken

De volgende druktechnieken worden gebruikt:

A. Ondergrondbedrukking:

- tweekleurige guilloches of gelijkwaardige structuren,
- iriseffect, zo mogelijk fluorescerend,
- onder UV-belichting fluorescerende opdruk,
- motieven die een efficiënte bescherming bieden tegen namaak en tegen vervalsing (vooral op de pagina met persoonsgegevens), naar keuze met microprint,
- op paspoortpagina's van papier en op stickers moet inkt met reagenten worden gebruikt,
- indien het papier van het paspoort goed beveiligd is tegen pogingen tot vervalsing, is het gebruik van inkt met reagenten facultatief.

B. Formulierendruk:

Met geïntegreerde microprint (indien niet reeds in de ondergrondbedrukking aanwezig).

C. Nummering:

Op alle pagina's in het paspoort moet een uniek documentnummer worden gedrukt (zo mogelijk met een speciaal type cijfers c.q. letters en met onder UV-belichting fluorescerende inkt), of geperforeerd of, bij paspoortkaarten, geïntegreerd met gebruikmaking van dezelfde techniek als voor de persoonsgegevens. Aanbevolen wordt ervoor te zorgen dat het unieke documentnummer bij paspoortkaarten aan beide zijden van het document zichtbaar is. Wanneer voor de vermelding van persoonsgegevens een sticker wordt gebruikt, moet het unieke documentnummer worden gedrukt met fluorescerende inkt en is een speciaal type cijfers of letters verplicht.

Wanneer voor de vermelding van de persoonsgegevens een sticker of een niet-gelamineerde houderpagina wordt gebruikt, wordt daarop bovendien plaatdruk met latent beeldeffect, microprint, inkt met optisch variabele eigenschappen en een DOVID (diffractive optically variable image device) gebruikt. Op paspoortkaarten die geheel uit synthetisch basismateriaal bestaan, worden eveneens aanvullende optisch variabele veiligheidskenmerken gebruikt, en wel minstens door het gebruik van een DOVID of gelijkwaardige procédé.

4. Beveiliging tegen kopiëren

Op de pagina met persoonsgegevens wordt een optisch variabel kenmerk (OVD) of ander gelijkwaardig kenmerk gebruikt dat hetzelfde niveau van identificatie en beveiliging biedt als het kenmerk dat momenteel in het uniforme visummodel wordt gebruikt; dit kenmerk dient de vorm aan te nemen van diffractieve structuren die naar gelang van de invalshoek variëren (DOVID), geïntegreerd in de warm of anderszins gelamineerde (zo dun mogelijke) folie of toegepast als OVD-overlay, dan wel op een sticker of niet-gelamineerde houderpagina, als gemetalliseerd of gedeeltelijk gedemetalliseerd OVD (met plaatdruk bedrukt) of een gelijkwaardig kenmerk.

Het OVD moet in het document worden geïntegreerd als onderdeel van een gelaagde structuur die een doeltreffende bescherming biedt tegen namaak en vervalsing. In een papieren document moet het OVD over een zo groot mogelijke oppervlakte worden geïntegreerd in de warm of anderszins gelamineerde (zo dun mogelijke) folie of toegepast als OVD-folie, zoals beschreven in punt 5. In een document uit synthetisch basismateriaal moet het OVD over een zo groot mogelijke oppervlakte in de gelaagde structuur van de kaart worden geïntegreerd.

Voor een synthetische kaart die wordt gepersonaliseerd door middel van lasergravure met daarin opgenomen een optisch variabel met laser geïntegreerd kenmerk, moet het diffractieve OVD, ten minste in de vorm van een gepositioneerd en gemetalliseerd of transparant DOVID, worden gebruikt om een betere bescherming tegen reproductie te bieden.

Indien een pagina met persoonsgegevens bestaat uit synthetisch basismateriaal met een papieren kern, moet het diffractieve OVD, ten minste in de vorm van een gepositioneerd en gemetalliseerd of transparant DOVID, worden gebruikt om een betere bescherming tegen reproductie te bieden.

5. Personaliseringstechniek

Om te verzekeren dat de in het paspoort vermelde gegevens voldoende zijn beveiligd tegen namaak of vervalsing, worden de persoonsgegevens, waartoe de afbeelding van de houder, diens handtekening en de belangrijkste afgiftegegevens behoren, geïntegreerd in het basismateriaal van het document. Traditionele methodes om foto's te bevestigen worden niet meer gebruikt.

De volgende personaliseringstechnieken kunnen worden gebruikt:

- laserdruk,
- thermotransferprocédé,
- inktjetdruk,
- fotografisch procédé,
- lasergravure, waarbij de kaartlagen met de veiligheidskenmerken doeltreffend worden gepenetreerd.

Om ervoor te zorgen dat de persoonsgegevens afdoende beveiligd zijn tegen pogingen tot vervalsing, wordt bij laserdruk-, thermotransfer- en fotografische personaliseringstechnieken een warm of anderszins gelamineerde (zo dun mogelijke) folie met een antikopieerbeveiliging gebruikt.

De reisdocumenten van de EU-lidstaten moeten machineleesbaar zijn. De pagina met persoonsgegevens moet volgens ICAO-document nr. 9303, deel 1, worden opgemaakt en de wijze van invullen moet voldoen aan de in dat document opgenomen voorschriften voor machineleesbare documenten.



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 2004¹ 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

¹PB 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 overeenkomst². 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 ondertekening 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



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	3
2	Biometrie	3
2.1	Primair biometrisch kenmerk – Gezicht	3
2.1.1	Overeenstemming met de normen	3
2.1.2	Type	3
2.1.3	Formaat	4
2.1.4	Vereiste opslagcapaciteit	4
2.1.5	Andere aspecten	4
2.2	Secundair biometrisch kenmerk – Vingerafdrukken	4
2.2.1	Overeenstemming met de normen	4
2.2.2	Type	5
2.2.3	Formaat en kwaliteit	5
2.2.4	Opslagcapaciteit	5
3	Opslagmedium (RF-chiparchitectuur)	5
3.1	Overeenstemming met de normen	5
3.2	RF-interface	5
3.3	Vereiste opslagcapaciteit	5
4	Lay-out van de chip voor elektronische paspoorten (gegevensstructuur)	6
4.1	Overeenstemming met de normen	6
4.2	Correlatie met gedrukte gegevens	6
4.3	Logische gegevensstructuur van de chip	6
5	Gegevensbeveiliging en -integriteit	6
5.1	Overeenstemming met de normen	6
5.2	Beveiliging van digitale gegevens	6
5.3	Veiligheidsinfrastructuur	8
6	Conformiteitsbeoordeling	8
7	Referentiedocumenten	10

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 OPNAME¹ 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 gezichtsofopname 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 zijn².

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 opgenomen³.

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 beroepsposen (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
-----	-------------	-----------	---------

EU-paspoort - Specificaties

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 (ongoorloofd af luisteren) 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 (SOD). 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 veiligheidsskenmerken 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 verblijfsti-tels 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 Im-age 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 Tra-vel 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 ca-pacity 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: Or-ganization, 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 Finger-print, 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 Signa-ture Creation Devices , Part 1 - Basic requirements, Version 1.09 rev2
http://www.uninfo.polito.it/ws_esign/docs.htm