COMMISSION DES COMMUNAUTÉS EUROPÉENNES

Bruxelles, le 28/II/2005
C(2005)409 final

DÉCISION DE LA COMMISSION

du 28/II/2005

établissant les spécifications techniques afférentes aux normes pour les dispositifs de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres

Les textes en langues française,néerlandaise,tchèque,allemande,estonienne,grecque,espagnole,italienne,lettone ,lituanienne,hongroise,maltaise,polonaise,portugaise,slovène,slovaque,finnoise et suédoise sont les seuls faisant foi.

DÉCISION DE LA COMMISSION

du 28/II/2005

établissant les spécifications techniques afférentes aux normes pour les dispositifs de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres

Les textes en langues française,néerlandaise,tchèque,allemande,estonienne,grecque,espagnole,italienne,lettone ,lituanienne,hongroise,maltaise,polonaise,portugaise,slovène,slovaque,finnoise et suédoise sont les seuls faisant foi.

LA COMMISSION DES COMMUNAUTÉS EUROPÉENNES,

vu le traité instituant la Communauté européenne,

vu le règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004[1] établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, et notamment son article 2,

considérant ce qui suit:

(1) Le règlement (CE) n° 2252/2004 du 13 décembre 2004 n'établit que les spécifications techniques des passeports et des documents de voyage qui ont un caractère général et non secret. Celles-ci doivent être complétées par d'autres spécifications techniques qui peuvent rester secrètes.

(2) Il est convenu que les spécifications contenues dans la présente décision ne sont pas secrètes car elles portent essentiellement sur des documents publics.

(3) Conformément à la décision 2000/365/CE du Conseil du 29 mai 2000 relative à la demande du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord de participer à certaines dispositions de l'acquis de Schengen, le Royaume-Uni ne prend pas part à l'adoption du règlement et n'est donc pas lié par celui-ci ni soumis à son application, dans la mesure où il développe les dispositions de l'acquis de Schengen. Le Royaume-Uni n'est donc pas destinataire de la présente décision.

(4) Conformément à la décision 2002/192/CE du Conseil du 28 février 2002 relative à la demande de l'Irlande de participer à certaines dispositions de l'acquis de Schengen, l'Irlande ne prend pas part à l'adoption du règlement et n'est donc pas liée par celui-ci ni soumise à son application, dans la mesure où il développe les dispositions de l'acquis de Schengen. L'Irlande n'est donc pas destinataire de la présente décision.

[1] JO L 385 du 29 décembre 2004, p. 1.

(5) Conformément aux articles 1er et 2 du protocole sur la position du Danemark annexé au traité sur l'Union européenne et au traité instituant la Communauté européenne, le Danemark ne prend pas part à l'adoption du règlement et n'est donc pas lié par celui-ci ni soumis à son application. Toutefois, le règlement visant à développer l'acquis de Schengen en application des dispositions de la troisième partie, titre IV, du traité instituant la Communauté européenne, le Danemark, conformément à l'article 5 dudit protocole, décidera, dans un délai de six mois après que le Conseil aura arrêté ledit règlement, s'il le transpose ou non dans son droit national. Dans ce cas, le Danemark devient aussi destinataire de la présente décision.

(6) En ce qui concerne l'Islande et la Norvège, ce règlement constitue un développement des dispositions de l'acquis de Schengen au sens de l'accord conclu par le Conseil de l'Union européenne, la République d'Islande et le Royaume de Norvège sur l'association de ces deux États à la mise en œuvre, à l'application et au développement de l'acquis de Schengen, qui relève du domaine visé à l'article 1er, point B), de la décision 1999/437/CE du Conseil du 17 mai 1999 relative à certaines modalités d'application de cet accord[2]. La Norvège et l'Islande sont par conséquent liées par la présente décision de la Commission.

(7) En ce qui concerne la Suisse, ce règlement constitue un développement des dispositions de l'acquis de Schengen au sens de l'accord signé par l'Union européenne, la Communauté européenne et la Confédération helvétique sur l'association de cet État à la mise en œuvre, à l'application et au développement de l'acquis de Schengen, qui relève du domaine visé à l'article 4, paragraphe 1, de la décision du Conseil relative à la signature de cet accord au nom de la Communauté européenne et à l'application transitoire de certaines dispositions de cet accord.

(8) Les mesures prévues par la présente décision sont conformes à l'avis du comité institué par l'article 6 du règlement (CE) n° 1683/95.

A ARRÊTÉ LA PRÉSENTE DÉCISION:

Article 1er

Les spécifications techniques afférentes aux normes pour les dispositifs de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, qui complètent celles établies par le règlement (CE) n° 2252/04, sont présentées en annexe de la présente décision.

Article 2

Les États membres coopèrent dans la mise en œuvre de la présente décision, notamment en échangeant des informations sur toutes les spécifications techniques.

Chaque État membre fait parvenir à la Commission et aux autres États membres un spécimen des passeports et des documents de voyage qu'il délivre. Chaque État membre s'engage

[2] JO L 176 du 10.7.1999, p. 31.

également à conserver les spécimens des tirages ultérieurs et les tient à la disposition de la Commission et des autres États membres.

Article 3

La Belgique, la République tchèque, l'Allemagne, l'Estonie, la Grèce, l'Espagne, la France, l'Italie, Chypre, la Lettonie, la Lituanie, le Luxembourg, la Hongrie, Malte, les Pays-Bas, l'Autriche, la Pologne, le Portugal, la Slovénie, la Slovaquie, la Finlande et la Suède sont destinataires de la présente décision.

Fait à Bruxelles, le 28/II/2005.

Par la Commission
Franco FRATTINI
Membre de la Commission

COMMISSION DES COMMUNAUTÉS EUROPÉENNES

AMPLIATION CERTIFIEE CONFORME
Pour le Secrétaire général,

Patricia BUGNOT
Directeur du Greffe

Intégration de données biométriques dans les passeports de l'UE

Spécifications du passeport européen

Annexe à la décision de la Commission du 28/II/2005 C(2005)409 final

Table des matières

1 Champ d'application et limites

Le présent document décrit différentes solutions pour les passeports européens à puce, sur la base du document [1] intitulé

> *«Règlement du Conseil établissant des normes pour les dispositifs de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres»*

Il se fonde sur des normes internationales, particulièrement les normes ISO et les recommandations de l'OACI sur les documents de voyage à lecture optique, et couvre les points suivants:

- Spécifications pour les identifiants biométriques: image de face et empreintes digitales
- Support de stockage (puce)
- Structure des données logiques sur la puce
- Spécifications pour la sécurité des données stockées numériquement sur la puce
- Évaluation de la conformité de la puce et des applications
- Compatibilité RF avec d'autres documents de voyage électroniques

Le présent document ne porte pas sur les éléments suivants :

- Spécifications pour l'insertion mécanique de la puce dans un livret de passeport, les procédures de tests de durabilité et de tests mécaniques.
- Spécifications relatives aux procédures opérationnelles standard (SOP) pour le processus d'inscription ou d'inspection.

2 Biométrie

2.1 Élément biométrique principal – Image de face

2.1.1 Conformité aux normes

- ICAO NTWG, Biometrics Deployment of Machine Readable Travel Documents, Technical Report, Version 2.0, 5 mai 2004 [3]
- ISO/IEC FCD 19794-5: Formats d'échange de données biométriques - Partie 5: Données de l'image de face [4]

2.1.2 Type

L'image de face doit être stockée comme IMAGE FRONTALE[1], conformément à [3, 4].

2.1.3 Format

L'image de face doit être stockée comme FICHIER D'IMAGE comprimé, et non pas sous un format spécifique propriétaire.

Bien que les compressions JPEG et JPEG2000 soient toutes deux conformes à la norme [3], la compression JPEG2000 est recommandée pour les passeports de l'UE parce qu'elle produit des fichiers moins volumineux que les images comprimées JPEG[2].

2.1.4 Volume de stockage

N°	Option	Remarque	Recommandation
1	compression JPEG	env. 12-20 Ko par photo	
2	compression JPEG2000	env. 6-10 Ko par photo	recommandé (voir 2.1.3)

2.1.5 Autres questions

- Les instructions pour la prise de photos tenant compte des exigences de la technologie de reconnaissance de l'image de face sont à établir conformément aux normes de l'OACI [3]

2.2 Élément biométrique secondaire – Empreintes digitales

2.2.1 Conformité aux normes

- ICAO NTWG, Biometrics Deployment of Machine Readable Travel Documents, Technical Report, Version 2.0, 5 mai 2004 [3]
- ISO/IEC FCD 19794-4, Formats d'échange de données biométriques - Partie 4: Données d'image du doigt [5]
- ISO/IEC FCD 19794-2, Formats d'échange de données biométriques - Partie 2: Données du point caractéristique du doigt [6]
- Norme pour l'échange des informations concernant les empreintes, portraits, cicatrices et tatouages (ANSI/ NIST-ITL 1-2000); FBI: Théorie mathématique des ondelettes (WSQ) [15]

[1] Conformément aux normes de l'OACI, «L'image de la face selon le format d'échange de données biométriques, enregistrée dans le groupe de données 2 (de la structure des données logiques) sera dérivée de la photo de passeport utilisée pour créer l'image imprimée sur la page comportant les données du passeport à lecture optique, et sera encodée selon le format de type 2 (image de face complète) ou le format de type 3 (token image) arrêtés dans la dernière version de la norme ISO 19794-5.»

[2] L'utilisation commerciale de JPEG2000 peut représenter un forfait de près de 7 000 euros pour le SDK et le suivi.

2.2.2 Type

Les empreintes digitales principales à intégrer dans le passeport européen sont les

EMPREINTES À PLAT DE L'INDEX GAUCHE ET DE L'INDEX DROIT

Si la qualité des empreintes digitales laisse à désirer et/ou si les index présentent des blessures, il faudra prendre l'empreinte à plat, de bonne qualité, des majeurs, des annulaires ou des pouces[3].

2.2.3 Format et qualité

Les empreintes digitales seront stockées comme IMAGES, conformément à [5].

La qualité des images des empreintes digitales sera conforme à [5] et à [15].

L'algorithme de compression d'images WSQ DOIT être utilisé conformément à [15] afin de réduire la taille du fichier.

2.2.4 Volume de stockage

L'utilisation d'IMAGES d'empreintes digitales requiert 12 à 15 Ko environ par doigt.

3 Support de stockage (architecture à puce RF)

3.1 Conformité aux normes

- ICAO NTWG, Biometrics Deployment of Machine Readable Travel Document, Technical Report, Version 2.0, 5 mai 2004 [3]
- ISO/IEC FDIS 14443, Cartes d'identification - Cartes à circuit intégré – Cartes de proximité [7]
- ICAO NTWG, Use of Contactless Integrated Circuits In Machine Readable Travel Documents, Technical Report, Version 3.1, 16 avril 2003 [8]

3.2 Interface RF

Conformément à [3, 7, 8], l'interface RF de type A et l'interface RF de type B sont toutes deux considérées conformes à la norme de l'OACI.

Les passeports répondant aux exigences de l'OACI seront équipés des deux interfaces de type A et de type B, ce qui implique que les systèmes d'inspection aux frontières devront pouvoir utiliser les deux normes pour les passeports et les visas.

3.3 Capacité de stockage

Conformément à la structure des données logiques de l'OACI [10], les données alphanumériques de la zone de lecture optique (MRZ) du document et les données numériques de sécurisation du document (ICP – infrastructure à clé publique) doivent être stockées sur la puce avec les identifiants biométriques.

[3] Le format de stockage (CBEFF – cadre commun pour les formats d'échange de données biométriques) mentionnera le doigt utilisé (index gauche, majeur droit, etc.) pour faire en sorte que le doigt correct soit vérifié.

Les États membres sont tenus d'utiliser des puces RF d'une dimension suffisante pour contenir les données personnelles et les caractéristiques biométriques conformément au règlement de l'UE [1]. Voir aussi les sections 2.1.4 et 2.2.4.

Si, conformément au règlement de l'UE [1], un État membre souhaite ajouter d'autres données, une capacité de stockage supplémentaire pourra s'avérer nécessaire.

4 Configuration de la puce du passeport électronique (structure des données)

4.1 Conformité aux normes

- ICAO Doc 9303, Part 1, Machine Readable Passports, Cinquième édition, 2003 [9]
- Instructions consulaires communes (CCI), chapitre VI n° 4 et annexe 10
- ICAO NTWG, Development of a Logical Data Structure – LDS for optional capacity expansion technologies, Technical Report, Revision 1.7, 18 mai 2004 [10]

4.2 Corrélation avec les données imprimées

Les données alphanumériques, imprimées dans la zone de lecture optique du passeport conformément à [9], doivent correspondre aux données stockées numériquement dans la puce conformément à [10].

4.3 Structure des données logiques de la puce

Conformément à [10].

5 Questions de sécurité et d'intégrité des données

Le document de passeport traditionnel contient un certain nombre de dispositifs destinés à empêcher la contrefaçon, dont des dispositifs d'impression sécurisée et des marques optiquement variables conformément à [1]. Il convient de veiller semblablement à l'intégrité, à l'authenticité et à la confidentialité des données stockées numériquement sur la puce du passeport.

5.1 Conformité aux normes

- ICAO NTWG, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Technical Report, Version 1.1, 1er octobre 2004 [11]
- ISO/IEC 7816-4, Cartes d'identification - Cartes à circuit intégré – Partie 4: Organisation, sécurité et commandes pour les échanges [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 Sécurité des données numériques

N°	Sécurité	Remarque	Utilisation
1	Authentification passive [11, 12]	Prouve que le contenu du SO_D et du LDS est authentique et non modifié. N'empêche pas la copie	EXIGÉ pour toutes les données (critère de sécurité obligatoire de l'OACI)

N°	Sécurité	Remarque	Utilisation
		exacte ou la substitution de la puce. N'empêche pas l'accès non autorisé. N'empêche pas l'écrémage.	
2	Authentification active [11, 12]	Prouve que le SO_D n'est pas une copie mais a été lu sur la puce authentique. Prouve qu'il n'y a pas eu de substitution de la puce. Demande une puce microprocesseur.	FACULTATIF
3	Basic Access Control (contrôle d'accès de base) [11, 12, 16]	Empêche l'écrémage. Empêche l'interception illicite des communications entre les MRTD (documents de voyages à lecture optique) et le système de contrôle (en cas d'utilisation dans un canal de communication crypté). N'empêche pas la copie exacte ou la substitution de la puce (requiert également la copie du document traditionnel). Demande une puce microprocesseur.	EXIGÉ pour toutes les données
4	Extended Access Control (contrôle d'accès étendu) [11, 12, 13]	Empêche tout accès non autorisé aux données relatives aux empreintes digitales. Empêche l'écrémage des données relatives aux empreintes digitales. Demande une gestion supplémentaire des clés. N'empêche pas la copie exacte ou la substitution de la puce (requiert également la copie du document traditionnel). Demande une puce microprocesseur.	Protection supplémentaire EXIGÉE pour les données relatives aux empreintes digitales

SO_D Document Security Object (SO_D). Cet objet est signé numériquement par l'État émetteur et contient une représentation en hachage du contenu de la structure des données (LDS).

LDS Logical Data Structure/Structure des données logiques

MRTD Machine Readable Travel Document/Document de voyage à lecture optique

MRZ Machine Readable Zone/Zone de lecture optique

Les spécifications concernant le contrôle d'accès étendu et l'ICP seront arrêtées dans une autre décision de la Commission.

5.3 Infrastructure de sécurité

Afin d'assurer l'intégrité et l'authenticité des données numériques stockées sur la puce, une ICP «plate» est insérée.

Certificat de l'autorité de certification (AC) du pays:

- Le certificat du niveau le plus élevé, signé et émis par l'AC du pays, est le point de confiance pour l'État de réception.
- La clé privée délivrée par l'AC du pays est utilisée pour signer les certificats du signataire du document.
- Les certificats de l'AC du pays doivent dans un premier temps être distribués par les canaux diplomatiques. La mise à jour ultérieure par voie électronique doit être spécifiée.

Certificat du signataire du document:

- La clé privée du signataire du document est utilisée pour signer les DSO (Document Security Objects).
- Les certificats de signature des documents, générés par chaque État au sein d'une autorité nationale de signature de documents, DOIVENT être stockés dans les puces des passeports.

Liens entre les certificats des passeports électroniques et des visas électroniques:

Les États membres émettront très probablement des passeports électroniques et des visas électroniques conformes aux directives de l'OACI.

- Il est recommandé d'utiliser le même certificat de l'autorité de certification du pays pour les passeports et les visas.
- Les certificats du signataire des documents ne seront pas les mêmes pour les visas et les passeports à cause de la personnalisation décentralisée des documents de visas. Une convention pour le libellé devra être arrêtée afin de faire une distinction entre les certificats des signataires de documents pour les visas et les certificats des signataires de documents pour les passeports électroniques.

Pour plus de détails, voir [11].

6 Évaluation de conformité

La conformité au sens de [14] des documents de voyage porteurs de données biométriques fera l'objet d'une évaluation

Des profils de protection seront mis au point pour les documents de voyage porteurs de données biométriques.

7 Références normatives

[1] «Règlement (CE) n° 2252/2004 du Conseil établissant des normes pour les dispositifs de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres»

[2] «Projet de règlement du Conseil modifiant le règlement (CE) n° 1683/95 établissant un modèle type de visa»
«Projet de règlement du Conseil modifiant le règlement (CE) n° 1030/2002 établissant un modèle uniforme de titre de séjour pour les ressortissants de pays tiers»
Document UE 14969/1/03 REV1, 21 novembre 2003

[3] ICAO NTWG, Biometrics Deployment of Machine Readable Travel Documents, Technical Report, Version 2.0, 05 May 2004 [ICAO Bio]

[4] ISO/IEC FCD 19794-5: Technologies de l'information - Formats d'échange de données biométriques - Partie 5: Données de l'image de face

[5] ISO/IEC FCD 19794-4: Technologies de l'information - Formats d'échange de données biométriques - Partie 4: Données d'image du doigt

[6] ISO/IEC FCD 19794-2: Technologies de l'information - Formats d'échange de données biométriques - Partie 2: Données du point caractéristique du doigt

[7] ISO/IEC FDIS 14443: Cartes d'identification - Cartes à circuit intégré – Cartes de proximité

[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 May 2004

[11] ICAO NTWG, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Technical Report, Version 1.1, October 01, 2004

[12] ISO/IEC 7816-4, Cartes d'identification - Cartes à circuit intégré – Partie 4: Organisation, sécurité et commandes pour les échanges

[13] Access Control for Machine Readable Travel Documents, Preliminary Draft, 2004/Contrôle de l'accès aux documents de voyage lisibles à la machine, version provisoire, 2004

[14] Critères communs

[15] ANSI/NIST-ITL 1-2000 Standard "Data Format for the Interchange of Fingerprint, Facial, Scarmark & Tattoo (SMT) Information"/Norme pour l'échange des informations concernant les empreintes, portraits, cicatrices et tatouages (ANSI/NIST-ITL 1-2000)
FBI: Wavelet Scalar Quantization (WSQ)/Théorie mathématique des ondelettes
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/Interface /Interface d'application pour cartes à puces utilisées comme dispositifs sécurisés de création de signa-

ture, partie 1 : exigences essentielles.