COMMISSION DES COMMUNAUTÉS EUROPÉENNES

Bruxelles, le 28/VI/2006
C(2006) 2909 final

A NE PAS PUBLIER

DÉCISION DE LA COMMISSION

du 28/VI/2006

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

DÉCISION DE LA COMMISSION

du 28/VI/2006

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 allemande, espagnole, estonienne, finnoise, française, grecque, hongroise, italienne, lettone, lituanienne, maltaise, néerlandaise, polonaise, portugaise, slovaque, slovène, suédoise et tchèque 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 convient d'établir des spécifications techniques supplémentaires pour le stockage et la protection des empreintes digitales requises.

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

(4) La présente décision complète la décision de la Commission du 28 février 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 (C(2005) 409 final), qui établissait les spécifications techniques relatives à l'intégration de l'image de face.

(5) Par souci de clarté, un document consolidé, joint en annexe de la présente décision, présentant les spécifications techniques établies par la décision C(2005) 409 final de la Commission et par la présente décision, a été élaboré. Cette consolidation des spécifications techniques n'a pas d'incidence sur les délais de mise en œuvre fixés dans le règlement (CE) n° 2252/2004.

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

(6) 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 n'a pas pris 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.

(7) 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 n'a pas pris 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.

(8) 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 n'a pas pris 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, a notifié, par lettre du 6 juin 2005, la transposition de cet acquis dans son droit national. Il est donc soumis à l'obligation de droit international de mettre en œuvre l'annexe à la présente décision. Par conséquent, le Danemark doit recevoir un exemplaire de la présente décision.

(9) 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.

(10) 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.

(11) 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.

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

A ARRÊTÉ LA PRÉSENTE DÉCISION:

Article premier

Les spécifications techniques afférentes au stockage et à la protection des empreintes digitales devant être intégrées dans les passeports et les documents de voyage délivrés par les États membres sont présentées aux points 5, 6 et 7 de l'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 documents de voyage qu'il délivre. Chaque État membre s'engage également à conserver les spécimens des tirages ultérieurs et les tient à la disposition de la Commission et des autres États membres.

Article 3

Le Royaume de Belgique, la République tchèque, la République fédérale d'Allemagne, la République d'Estonie, la République hellénique, le Royaume d'Espagne, la République française, la République italienne, la République de Chypre, la République de Lettonie, la République de Lituanie, le Grand-duché de Luxembourg, la République de Hongrie, la République de Malte, le Royaume des Pays-Bas, la République d'Autriche, la République de Pologne, la République portugaise, la République de Slovénie, la République slovaque, République de Finlande, le Royaume de Suède sont destinataires de la présente décision.

Fait à Bruxelles, le 28/VI/2006

Par la Commission
Franco FRATTINI
Vice-président de la Commission

AMPLIATION CERTIFIEE CONFORME
Pour le Secrétaire général,

Jordi AYET PUIGARNAU
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/VI/2006 - C (2006) 2909

Table des matières

1 Champ d'application et limites 3
2 Biométrie 3
2.1 Élément biométrique principal – Image de face 3
2.1.1 Conformité aux normes 3
2.1.2 Type 4
2.1.3 Format 4
2.1.4 Volume de stockage 4
2.1.5 Autres questions 4
2.2 Élément biométrique secondaire – Empreintes digitales 4
2.2.1 Conformité aux normes 4
2.2.2 Type 5
2.2.3 Format et qualité 5
2.2.4 Volume de stockage 5
3 Support de stockage (architecture à puce RF) 5
3.1 Conformité aux normes 5
3.2 Interface RF 5
3.3 Capacité de stockage 5
4 Configuration de la puce du passeport électronique (structure des données) 6
4.1 Conformité aux normes 6
4.2 Corrélation avec les données imprimées 6
4.3 Structure des données logiques de la puce 6
5 Questions de sécurité et d'intégrité des données 6
5.1 Conformité aux normes 6
5.2 Sécurité des données numériques 6
5.3 Procédure d'inspection 8
5.4 Infrastructure à clé publique pour les passeports 8
5.5 Infrastructure à clé publique pour les systèmes de contrôle 8
5.5.1 Périodes de validité des certificats 8
5.5.2 Programmation des certificats 9
5.5.3 Politiques de certification 9
6 Évaluation de conformité 9
6.1 Conformité aux normes 9
6.2 Évaluation fonctionnelle 10
6.3 Évaluation par rapport aux Critères communs 10
7 Références normatives 10

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 et 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 19794-5:2005, Technologies de l'information - 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 aux normes [3 et 4].

2.1.3 Format

L'image de face doit être stockée comme FICHIER D'IMAGE compressé, 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 compressées JPEG.

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 2.1.2)

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 19794-4:2005, Technologies de l'information - Formats d'échange de données biométriques - Partie 4: Données d'image du doigt [5]
- ANSI/NIST-ITL 1-2000, Data Format for the Interchange of Fingerprint, Facial, Scarmark & Tattoo (SMT) Information; FBI: Wavelet Scalar Quantization (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 les formats d'image frontale complète (*full frontal image*) ou de *token image* arrêtés dans la dernière version de la norme ISO 19794-5.»

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[2].

2.2.3 Format et qualité

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

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

L'algorithme de compression d'images WSQ DOIT être utilisé conformément à la norme [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 Documents, Technical Report, Version 2.0, 5 mai 2004 [3]
- ISO/IEC 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 aux normes [3, 7 et 8], l'interface RF de type A et l'interface RF de type B sont toutes deux considérées comme conformes à la norme de l'OACI.

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

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 (Machine Readable Zone - MRZ) du document et les données numériques de sécurisation du document (infrastructure à clé publique - ICP) doivent être stockées sur la puce avec les identifiants biométriques.

[2] Le format de stockage (CBEFF – Format commun d'échange de fichiers biométriques) mentionnera le doigt utilisé (index gauche, majeur droit, etc.) afin 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

- International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Doc 9303, Part 1 Machine Readable Passports, Draft Sixth Edition, 2006 [9]
- Instructions consulaires communes (ICC), 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 la norme [9], doivent correspondre aux données stockées numériquement dans la puce conformément à la norme [10].

4.3 Structure des données logiques de la puce

Conformément à la norme [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 la norme [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]
- Advanced Security Mechanisms for Machine Readable Travel Documents, Version 1.0, 2006 [13]

5.2 Sécurité des données numériques

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

N°	Sécurité	Remarques	Prescriptions d'utilisation
		N'empêche pas l'accès non autorisé. N'empêche pas l'écrémage.	
2a)	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. Ne prouve pas que le contenu de la LDS est authentique et non modifié. N'empêche pas l'interception des communications entre la puce et le système de contrôle.	FACULTATIF
b)	Authentification de la puce [13]	Prouve que le SO_D n'est pas une copie et a été lu sur la puce authentique. Prouve qu'il n'y a pas eu de substitution de la puce. Empêche l'interception des communications entre la puce et le système de contrôle.	Protection supplémentaire EXIGÉE pour toutes les données lors de l'introduction des données relatives aux empreintes digitales ou au plus tard 36 mois après l'adoption des spécifications techniques. Cette protection NE DOIT PAS être assurée par la puce, mais les systèmes de contrôle de l'UE DOIVENT utiliser ce mécanisme s'il est pris en charge par la puce.
3	Basic Access Control (contrôle d'accès de base) [11, 12]	Empêche l'écrémage. Réduit le risque d'interception des communications entre la puce et le système de contrôle (voir 2b)). N'empêche pas la copie exacte ou la substitution de la puce (requiert également la copie du document traditionnel).	EXIGÉ pour toutes les données
4	Authentification du terminal [13]	Empêche tout accès non autorisé aux données relatives aux empreintes digitales. Empêche l'écrémage des données relatives aux	Protection supplémentaire EXIGÉE pour les données relatives aux empreintes digitales

N°	Sécurité	Remarques	Prescriptions d'utilisation
		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).	

SO_D Document Security Object (SO_D). Cet objet est signé numériquement par l'État émetteur et contient une représentation hachée du contenu de la 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)

EAC Extended Access Control (contrôle d'accès étendu), soit, selon l'OACI, la combinaison de l'authentification de la puce et de l'authentification du terminal

5.3 Procédure d'inspection

Supprimé

5.4 Infrastructure à clé publique pour les passeports

Afin d'assurer l'intégrité et l'authenticité des données numériques stockées sur la puce, une infrastructure à clé publique (ICP) est introduite: chaque État membre DOIT mettre en place une seule *AC signataire nationale* faisant office de point de confiance national pour tous les États de réception et désigner au moins un *Signataire de documents* délivrant les passeports. De plus amples informations sur cette ICP (y compris les algorithmes de signature, les longueurs de clés et les périodes de validité) figurent dans la norme [11].
Chaque État membre DOIT communiquer à la Commission le nom et les coordonnées de l'organisation responsable du fonctionnement de l'*AC signataire nationale* et du ou des *Signataire(s) de documents*.

5.5 Infrastructure à clé publique pour les systèmes de contrôle

Pour éviter que des systèmes de contrôle non autorisés aient accès aux données relatives aux empreintes digitales, une autre ICP est introduite: chaque État membre DOIT mettre en place une seule *AC de vérification nationale* faisant office de point de confiance national pour les passeports délivrés par cet État membre et désigner au moins un *Vérificateur de documents* chargé de gérer un groupe de système de contrôle autorisés. De plus amples informations sur cette ICP figurent dans la norme [13].

Chaque État membre DOIT communiquer le nom et les coordonnées de l'organisation responsable du fonctionnement de l'*AC de vérification nationale* et du ou des *Vérificateur(s) de documents* à la Commission.

5.5.1 Périodes de validité des certificats

La validité des certificats délivrés DOIT être comprise dans les limites suivantes:

Entité	Période de validité minimum	Période de validité maximum
Certificat de l'AC de vérification nationale	6 mois	3 ans
Certificat du Vérificateur de documents	2 semaines	3 mois
Certificat du système de contrôle	1 jour	1 mois

Ces délais peuvent être modifiés par le comité «article 6» en fonction des résultats des tests présentés par le Brussels Interoperability Group (BIG).

5.5.2 Programmation des certificats

Pour permettre de planifier la programmation des certificats, les délais de traitement et de distribution suivants DOIVENT être respectés. Les certificats de liaison destinés à l'AC de vérification nationale doivent être distribués au moins 14 jours avant l'expiration du certificat à remplacer.

Autorité de certification	Délai de traitement maximum (demande de certificat)	Délai de distribution maximum (certificat)
AC de vérification nationale	72 heures	24 heures
Vérificateur de documents	24 heures	48 heures

Ces délais peuvent être modifiés par le comité «article 6» en fonction des résultats des tests présentés par le BIG.

5.5.3 Politiques de certification

Le BIG établira une politique de certification commune dans un délai d'un an à compter de la décision de la Commission sur les spécifications techniques.

L'AC de vérification nationale de chaque État membre DOIT publier une politique de certification et peut établir un énoncé des pratiques de certification, conformément aux exigences fixées par le BIG, en indiquant notamment les conditions de délivrance des certificats destinés aux Vérificateurs de documents (étrangers). L'adoption de la politique de certification doit être notifiée à la Commission.

6 Évaluation de conformité

Un groupe de travail technique (le «Brussels Interoperability Group» ou BIG) sera mis sur pied [18] pour veiller à la conformité de l'interopérabilité des passeports aux présentes spécifications.

6.1 Conformité aux normes

- ICAO NTWG, RF Protocol and Application Test Standard for E-Passport; Parts 2&3 [19]
- ISO/IEC 7816-4, Cartes d'identification - Cartes à circuit intégré – Partie 4: Organisation, sécurité et commandes pour les échanges [12]

- ISO/IEC 7816-8, Cartes d'identification - Cartes à circuit intégré – Partie 8: Commandes pour des opérations de sécurité [20]
- Common Criteria Protection Profile for Machine Readable Travel Document with «ICAO Application», Basic Access Control, Version 1.0 [14]
- Common Criteria Protection Profile for Machine Readable Travel Document with «ICAO Application», Extended Access Control, Version 1.0 [17]

6.2 Évaluation fonctionnelle

L'évaluation fonctionnelle des puces MRTD DOIT être réalisée sur la base de la norme adéquate [19], actuellement en cours d'élaboration. D'autres cas types PEUVENT être définis par le BIG si la mise en œuvre de la norme [13] l'exige.

Chaque État membre DOIT charger un laboratoire d'essai (national) agréé de certifier la conformité fonctionnelle avec les normes adéquates sur toutes les couches ISO/OSI. Les certificats délivrés DOIVENT être notifiés à la Commission.

Couche ISO/OSI	Norme	Champ d'application
1-4	ISO 14443 [7]	Matériel informatique
6	ISO 7816 [12,20]	Logiciel (système d'exploitation)
7	Application OACI [10, 11]	Logiciel (application)

6.3 Évaluation par rapport aux Critères communs

Les puces de passeports DOIVENT être évaluées conformément au profil de protection adéquat fondé sur les Critères communs [14, 17].

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] Supprimée

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

[4] ISO/IEC FCD 19794-5:2005, Technologies de l'information - Formats d'échange de données biométriques - Partie 5: Données de l'image de face

[5] ISO/IEC 19794-4:2005, Technologies de l'information - Formats d'échange de données biométriques - Partie 4: Données d'image du doigt

[6] Supprimée

[7] ISO/IEC 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 avril 2003

[9] International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Doc 9303, Part 1 Machine Readable Passports, Draft Sixth

Edition, 2006

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

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

[12] ISO/IEC 7816-4:2005, Cartes d'identification - Cartes à circuit intégré – Partie 4: Organisation, sécurité et commandes pour les échanges

[13] Advanced Security Mechanisms for Machine Readable Travel Documents, Version 1.0, 2005

[14] Common Criteria Protection Profile for Machine Readable Travel Document with «ICAO Application», Basic Access Control, Version 1.0

http://www.bsi.bund.de/zertifiz/zert/reporte/PP0017b.pdf

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

www.itl.nist.gov/iad

[16] Supprimée

[17] Common Criteria Protection Profile for Machine Readable Travel Document with “ICAO Application”, Extended Access Control, Version 1.0

[18] Brussels Interoperability Group, mandat

[19] ICAO NTWG, RF Protocol and Application Test Standard for E-Passport; Parts 2&3

[20] ISO/IEC 7816-8:2004, Cartes d'identification - Cartes à circuit intégré – Partie 8: Commandes pour des opérations de sécurité