Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2011/28

ID-OneTM ePass v2.2 en configuration EAC sur composant NXP P5CD081V1A

Paris, le 26 août 2011

Le directeur général de l'agence nationale de la sécurité des systèmes d'information

[Original signé]

Patrick Pailloux

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2011/28

Nom du produit

ID-OneTM ePass v2.2 en configuration EAC sur composant NXP P5CD081V1A

Référence/version du produit

ID-OneTM ePass v2.2 en configuration EAC sur composant NXP P5CD081V1A version 2.2

Conformité à un profil de protection

[PP EAC], version 1.10

Machine Readable Travel Document with "ICAO Application", Extended Access Control

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeur(s)

Oberthur Technologies

71-73 rue des Hautes Pâtures,

92756 Nanterre, France

Oberthur Technologies

71-73 rue des Hautes Pâtures,

92756 Nanterre, France

22529 Hamburg, Allemagne

Commanditaire

Oberthur Technologies

71-73 rue des Hautes Pâtures,

92756 Nanterre, France

Centre d'évaluation

Serma Technologies

30 avenue Gustave Eiffel, 33608 Pessac, France

Tél : +33 (0)5 57 26 08 75, mél : e.francois@serma.com

Accords de reconnaissance applicables

CCRA **SOG-IS**

Le produit est reconnu au niveau EAL4.

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est le passeport électronique « ID-One™ ePass v2.2 en configuration EAC et AA sur composant NXP P5CD081 **»** développé par **Oberthur Technologies** sur un composant *NXP Semiconductors*.

Le produit évalué est de type « carte à puce » avec et sans contacts. Il implémente les fonctions de voyage électronique conformément aux spécifications de l'organisation de l'aviation civile internationale (OACI[1]). Ce produit est destiné à vérifier l'authenticité du document de voyage et à identifier son porteur lors d'un contrôle frontalier, à l'aide d'un système d'inspection.
Ce microcontrôleur et son logiciel embarqué ont vocation à être insérés dans la couverture des passeports traditionnels. Ils peuvent être intégrés sous forme de module ou d'*inlay*. Le produit final peut être un passeport, une carte plastique, etc.

1.2. Description du produit

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.
Cette cible de sécurité est conforme au profil de protection [PP EAC]. Il s'agit d'une conformité stricte.

1.2.1. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].
La version certifiée du produit est identifiable par les éléments suivants :

- nom commercial : ID-One™ ePass v2.2 en configuration EAC et AA sur composant NXP P5CD081
- référence du produit : *ePass V2.2 on NXP P5CD081*;
- référence du composant : P5CD081V1A ;
- code SAAAAR : 075021 ;
- code optionnel (*patch*) : 076151.

Ces informations peuvent être vérifiées par les données de traçabilités (CPLC[2]).

- un GET DATA de valeur 9F7F[3] pour les données de traçabilité de la ROM, dont les 13 premiers octets doivent être 9F 7F 2A 47 90 51 68 82 31 01 83 30 04 avec :
  - rappel des données du GET DATA : **9F 7F** ;
  - information sur la taille de la réponse : **2A** ;
  - fabricant du composant : **47 90** (NXP) ;
  - type du composant : **51 68** (P5CD081) ;

1 encore appelé ICAO pour *International Civil Aviation Organization*
2 *Card manager Production Life Cycle*.
3 En hexadécimal.

- identifiant du système d'exploitation : **82 31** (OBERTHUR OS) ;
- date de la version du système d'exploitation : **01 83** (183ème jour de 2010) ;
- version du système d'exploitation : **30 04**

- un GET DATA de valeur DF52[1] pour les données d'identification de la TOE, dont les 17 premiers octets doivent être DF 52 0C 59 01 00 07 50 21 30 37 36 31 35 31 90 00 avec :
  - rappel des données du GET DATA : **DF 52** ;
  - information sur la taille de la réponse : **0C** ;
  - numéro du masque : **59** ;
  - version du masque : **01** ;
  - *LDS configuration* : **00** ;
  - code SAAAAR du ROM code : **07 50 21** ;
  - code SAAAAR du code optionnel : **30 37 36 31 35 31**[2].

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- le contrôle d'accès en lecture et en écriture ;
- le mécanisme EAC ;
- le mécanisme de *secure messaging* ;
- l'authentification de l'agent de personnalisation ;
- l'authentification active (si activé) ;
- la protection physique.

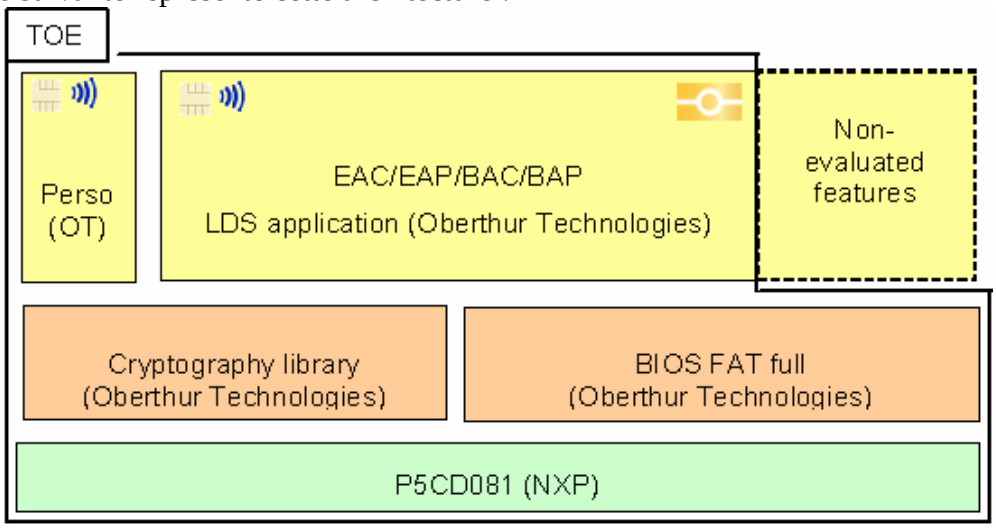
1.2.3. Architecture

Le produit est une carte à puce fermée constituée des éléments suivants :

- un microcontrôeur (P5CD081 de *NXP Semiconductors*) ;
- une application native « *BIOS FAT full* » donnant l'accès aux fonctionnalités du microcontrôleur ;
- une librairie cryptographique dédiée ;
- une application de personnalisation *Perso* ;
- l'application LDS[3] supportant les mécanismes EAC, EAP, BAC et BAP et dont certaines fonctionnalités ne font pas partie de la TOE. Leur présence a été, cependant, prise en compte lors de l'analyse de vulnérabilité :
  - *PACE generic* (mappage générique pour SAC, pace V2) ;
  - *PIN management* (gestion d'un PIN alphanumérique en tant que condition d'accès) ;
  - Biométrie (gestion d'un PIN biométrique en tant que condition d'accès).

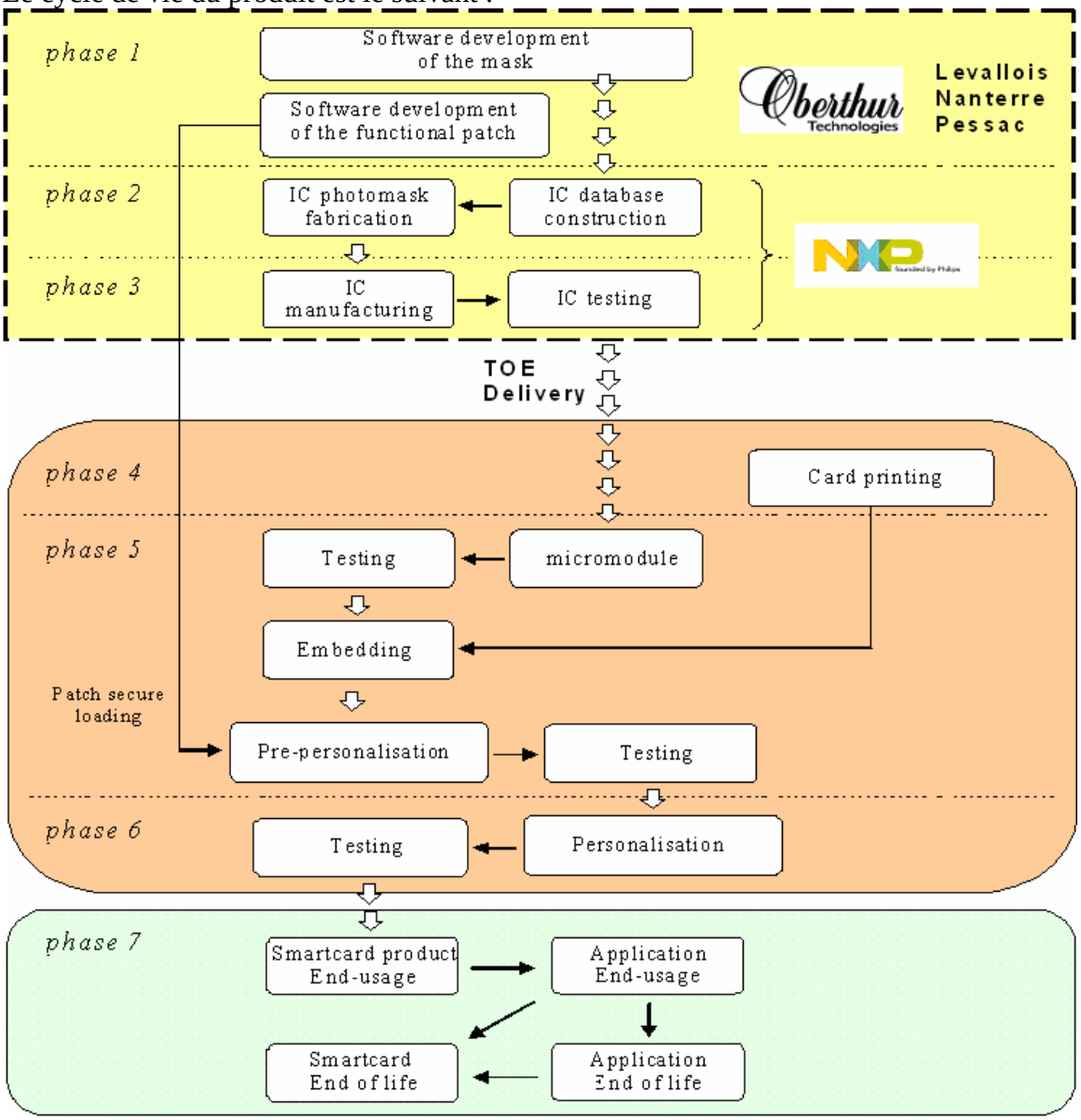
[1] En hexadécimal.
[2] code ASCII du code SAAAAR 076151 attendu.
[3] *Logical Data Structure*

La figure suivante représente cette architecture :



1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :



Le produit a été développé sur les sites suivants :

Oberthur Technologies – Site de Nanterre

71-73, rue des Hautes Pâtures
92726 Nanterre
France

Oberthur Technologies – Site de Levallois

50 quai Michelet
92300 Levallois-Perret
France

Oberthur Technologies – Site de Pessac
Parc Scientifique UNITEC 1
4 allée du Doyen Georges Brus – Porte 2
33600 Pessac
France

NXP Semiconductors
Stresemannallee 101
22529 Hambourg
Allemagne

1.2.5. Configuration évaluée

Le produit peut être personnalisé selon différentes configurations.
Le certificat porte sur la configuration suivante :

- mécanisme BAC activé ;
- mécanisme EAC activé ;
- mécanisme *active authenticate* activé (ECC ou RSA).

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 3** [CC] et à la méthodologie d'évaluation définie dans le manuel [CEM].
Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [CC IC] et [CC AP] ont été appliqués.

2.2. Travaux d'évaluation

L'évaluation en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel dans le microcontrôleur déjà certifié par ailleurs.
Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur « ***NXP Smart Card Controller P5CD081V1A*** » au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_VAN.5, ASE_TSS.2 conforme au profil de protection [PP]. Ce microcontrôleur a été certifié le 10 novembre 2009 sous la référence BSI-DSZ-CC-0555-2009.
Le niveau de résistance du microcontrôleur a été confirmé le 17 décembre 2010 dans le cadre du processus de surveillance.

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 18/08/201l, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques a été réalisée conformément aux référentiels techniques de l'ANSSI [REF-CRY], [REF-KEY] et [REF-AUT]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Il en ressort que pour assurer la conformité aux référentiels techniques de l'ANSSI décrits ci-dessus, les recommandations suivantes devront être suivies lors de la personnalisation du produit :

- la taille des clés RSA et de groupe DH devront être d'au moins 2048 bits ;
- la taille de groupe ECDH et de clé ECDSA devront être d'au moins 200 bits (256 bits recommandés).

2.4. Analyse du générateur d'aléas

Le générateur d'aléas utilisé par le produit final est celui proposé par le produit hôte et a été évalué dans le cadre de l'évaluation BSI-DSZ-CC-0555-2009.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit « ID-One™ ePass v2.2 en configuration EAC et AA sur composant NXP P5CD081 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 augmenté.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].
L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[1], des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 5+	Intitulé du composant
ADV Développement	ADV_ARC		**1**	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**5**	Complete semi-formal functional specification with additional error information
	ADV_IMP				**1**	1	**2**	2	**1**	Implementation representation of the TSF
	ADV_INT					**2**	**3**	3	**2**	Well-structured internals
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**4**	Semiformal modular design
AGD Guides d'utilisation	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**1**	1	1	1	1	1	1	**1**	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Production support, acceptance procedures and automation
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**5**	Development tools CM coverage
	ALC_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**2**	Sufficiency of security measures
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**2**	Compliance with implementation
ASE Evaluation de la cible de sécurité	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended components definition
	ASE_INT	**1**	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	**1**	**2**	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	**1**	**2**	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		**1**	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	**1**	1	1	1	1	1	1	**1**	TOE summary specification
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	**2**	**3**	3	**4**	**3**	Testing modular Design
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**5**	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - *HERMES Security Target EAC, reference: FQR 110 5142, Issue 2 , 18th july 2011,* Oberthur Technologies. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *ID One ePass V2.2 on NXP In EAC configuration with AA, reference : FQR 110 5770,* Ed 1, Oberthur Technologies.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report – HERMES Project, reference: HERMES_ETR_v1.1/1.1, 18th august 2011,* Serma Technologies.
[ANA-CRY]	Cotation des mécanismes cryptographiques, référence : 894/ANSSI/ACE du 1er avril 2011, ANSSI.
[CONF]	Liste de configuration - *Configuration list, reference FQR 110 5644, version 2, 12th august 2011,* Oberthur Technologies ; - *ePass v2.2 on NXP P5CD081 PRODUCT GENERATION DESCRIPTION, reference 075021 00 PGD, version 1-AA, 12th july 2011,* Oberthur Technologies ; - *Optional Code r1.0 for ePass V2.2 on P5CD081, reference 076151 00 PGD* 27th january 2011, Oberthur Technologies.
[GUIDES]	- *HERMES Guidance, reference: FQR 110 5575, Issue 1, 10th february 2011,* Oberthur Technologies ; - *HERMES Administration and Personnalization Guidance document, reference: FQR 110 5358, Issue 1, 6h september 2010,* Oberthur Technologies.
[PP EAC]	*Protection Profile - Machine Readable Travel Document with "ICAO Application", Extended Access Control, version 1.10,* 25 Mars 2009. Certifié par le BSI. *(Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0055-2009.*
[PP]	Security IC Protection Profile, version 1.0, 23rd august 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0035-2007.*

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.
[CC]	*Common Criteria for Information Technology Security Evaluation :* *Part 1: Introduction and general model,* *July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001;* *Part 2: Security functional components,* *July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002;* *Part 3: Security assurance components,* *July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.*
[CEM]	*Common Methodology for Information Technology Security Evaluation : Evaluation Methodology,* *July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.*
[CC IC]	*Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2009-03-002 version 3.0, revision 1, March 2009.*
[CC AP]	*Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2009-03-001 version 2.7 revision 1, March 2009.*
[COMP]	*Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, reference CCDB-2007-09-001 version 1.0, revision 1, September 2007.*
[CC RA]	*Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.*
[SOG-IS]	*« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0,* 8 Janvier 2010*, Management Committee.*
[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr
[REF-KEY]	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr

[REF-AUT]	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr