PREMIER MINISTRE

Secrétariat général de la défense nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-2009/21

Carte à puce TL ICAO LDS

Paris, le 17 juillet 2009

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

Patrick Pailloux
[ORIGINAL SIGNE]

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 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.dcssi@sgdn.gouv.fr

Référence du rapport de certification

ANSSI-2009/21

Nom du produit

Carte à puce TL ICAO LDS : applet de passeport électronique chargée sur la plate-forme JCLX80jTOP20ID masquée sur le composant SLE66CLX800PE

Référence/version du produit

Version 2.0

Conformité à un profil de protection

[PP EAC]

Common Criteria Protection Profile - Machine Readable Travel Document with "ICAO Application", Extended Access Control

Critères d'évaluation et version

Critères Communs version 3.1

Niveau d'évaluation

EAL 4 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

Trusted Logic

5 rue du Bailliage, 78000 VERSAILLES, FRANCE

Infineon Technologies AG

AIM CC SM PS - Am Campeon 1-12 - 85579 Neubiberg, GERMANY

Commanditaire

Trusted Logic

5 rue du Bailliage, 78000 VERSAILLES, 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, publié au Journal officiel de la République française. 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 6

1.1. PRESENTATION DU PRODUIT 6
1.2. DESCRIPTION DU PRODUIT 6
1.2.1. Identification du produit 6
1.2.2. Services de sécurité 7
1.2.3. Architecture 8
1.2.4. Cycle de vie 8
1.2.5. Configuration évaluée 10

2. L'EVALUATION 11

2.1. REFERENTIELS D'EVALUATION 11
2.2. TRAVAUX D'EVALUATION 11
2.3. ANALYSE DE LA RESISTANCE DES MECANISMES CRYPTOGRAPHIQUES 11
2.4. ANALYSE DU GENERATEUR D'ALEAS 11

3. LA CERTIFICATION 12

3.1. CONCLUSION 12
3.2. RESTRICTIONS D'USAGE 12
3.3. RECONNAISSANCE DU CERTIFICAT 12
3.3.1. Reconnaissance européenne (SOG-IS) 12
3.3.2. Reconnaissance internationale critères communs (CCRA) 12

ANNEXE 1. NIVEAU D'EVALUATION DU PRODUIT 14

ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE 15

ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION 17

1. Le produit

1.1. Présentation du produit

Le produit évalué est la carte à puce TL ICAO LDS, version 2.0, développée par Trusted Logic. Il est constitué d'une applet de passeport électronique chargée sur la plate-forme JCLX80jTOP20ID de Trusted Logic, elle-même masquée sur le composant SLE66CLX800PE d'Infineon technologies AG.

La cible d'évaluation (TOE pour *Target Of Evaluation*) est le résultat d'une double composition :

- une première composition entre la plate-forme JCLX80jTOP20ID (système d'exploitation et plate-forme *Java Card Open*) et le composant SLE66CLX800PE d'Infineon Technologies, qui correspond à la carte à puce « JCLX80jTOP20ID : Java Trusted Open Platform sur composant SLE66CLX800PE », certifiée sous la référence [DCSSI-2008_43] (dans la suite de ce document, ce produit sera désigné par « produit hôte ») ;
- une deuxième composition entre l'applet de passeport électronique et le produit susmentionné, qui correspond au produit ici certifié.

Le produit implémente les fonctionnalités de document de voyage électronique telles que spécifiées par l'Organisation de l'Aviation Civile Internationale (cf. [OACI]) et le profil de protection *Extended Access Control* (cf [PP EAC]).

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 démontrable (voir l'argumentaire au paragraphe 2.1 de [ST]).

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 :

Eléments de gestion de configuration		**Origine**
Nom de la TOE	TL ICAO LDS	Trusted Logic
Version de la TOE	V2.0	
Nom de la plate-forme	jTop ID Platform (également dénommé JCLX80jTOP20ID)	
Référence ROM (label)	IFXv#27	
Référence patch (label)	V1.6	
Nom du circuit intégré	SLE66CLX800PE/360PE	

Eléments de gestion de configuration		Origine
Référence complète du circuit intégré	SLE66CLX800PE-m1581-e13/a14 & SLE66CLX800PE-m1587-e13/a14	Infineon Technnologies AG

La plate-forme de la TOE peut être identifiée de façon unique au travers des données de réponse à la mise sous tension (ATR pour *Answer To Reset*) :

- 3B FE 18 00 00 80 31 FE 45 80 31 80 66 40 90 A4 56 1B 16 83 XX 90 00 dans lesquels les octets historiques permettent d'identifier :
  - le fabricant du composant : 40 90 ;
  - le type du composant : A4 ;
  - le type du masque : 56 ;
  - la version du masque : 1B (version 27 de jTOP) ;
  - la révision du masque : 16 (1.6 est la version courante du patch).

Le dernier octet précédant le mot d'état est variable, il dépend de l'état courant du cycle de vie de la carte (dans l'implémentation *Global Platfom*, va de OP_READY à TERMINATED).

L'applet de la TOE peut être identifiée grâce au *tag* (étiquette) 53 renvoyée lors de la sélection de l'application LDS :

- 6F 15 84 07 A0 00 00 02 47 10 01 A5 0A **53** 08 01 07 01 01 02 00 82 95.

Dans le champ valeur de ce *tag* 53 (constitué des 8 octets **01 07 01 01 02 00 82 95**), on trouve :

- la version des spécifications de LDS, soit 1.7 ;
- la version des spécifications de PKI, soit 1.1 ;
- la version de l'applet, soit 2.0 ;
- la date de génération de l'applet, soit 22 octobre 2008.

Ces informations (ATR et *tag* 53) permettent de tracer tous les éléments constitutifs de la TOE (composant, masque matériel, patch logiciel et applet). Elles permettent d'identifier correctement et de façon unique la TOE. Elles ont pu être vérifiées sur les échantillons de la TOE reçus lors de l'évaluation.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont constitués :

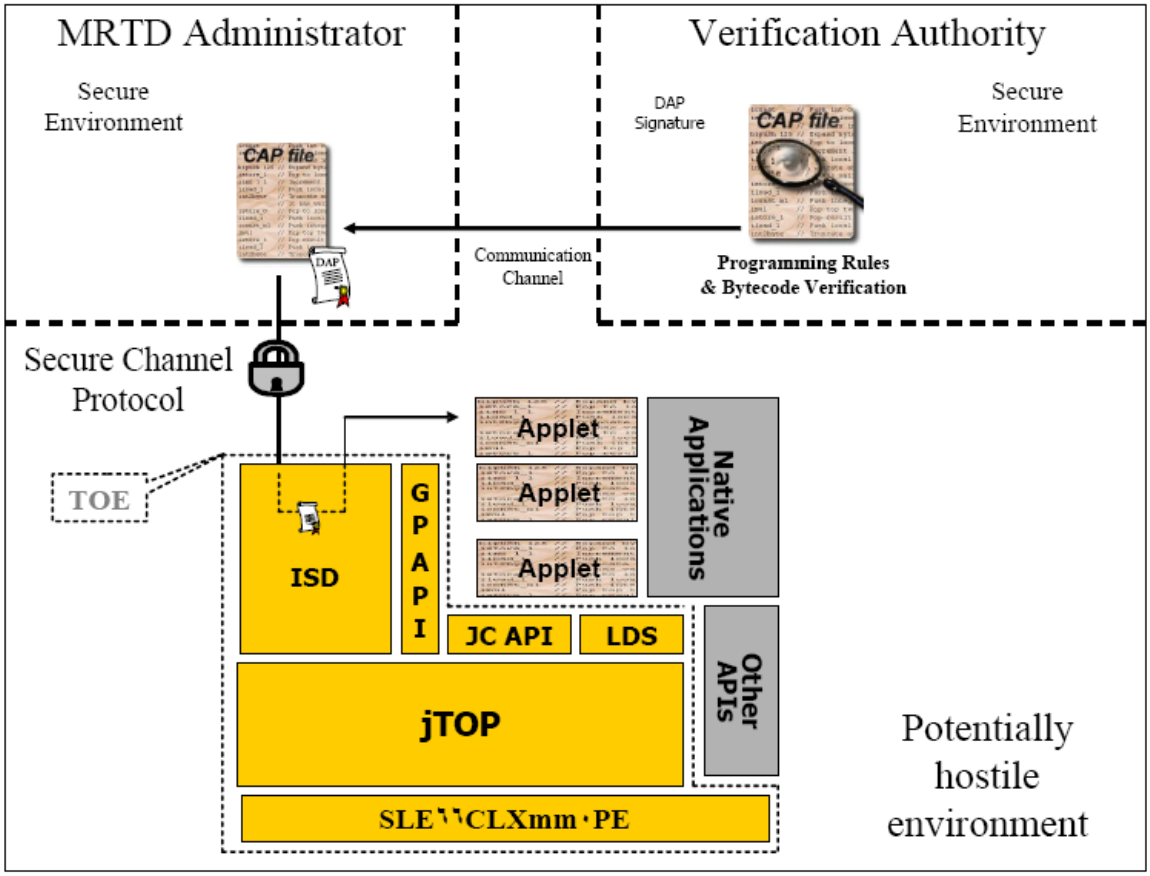
- de ceux fournis par la plate-forme (voir rapport de certification [DCSSI-2008_43]) :
- de ceux fournis par l'applet :
  - canal sécurisé avec un terminal de personnalisation ;
  - canal sécurisé avec un système d'inspection ;
  - protocole d'authentification basé sur le mécanisme *Basic Acces Control* (BAC) ;
  - *protocole Chip Authentication* ;
  - protocole *Active Authentication* ;
  - protocole *Terminal Authentication* ;
  - protocole *Personalization Authentication* ;
  - contrôle d'accès aux fichiers ;
  - anonymat du document de voyage électronique ;
- du contrôle de l'intégrité du *ByteCode*.

1.2.3. Architecture

Le produit est constitué :

- d'une applet de passeport électronique chargée en mémoire EEPROM ;
- d'un patch (v1.6) de la plate-forme chargé en mémoire EEPROM ;
- d'une plate-forme masquée en ROM ;
- d'un composant.

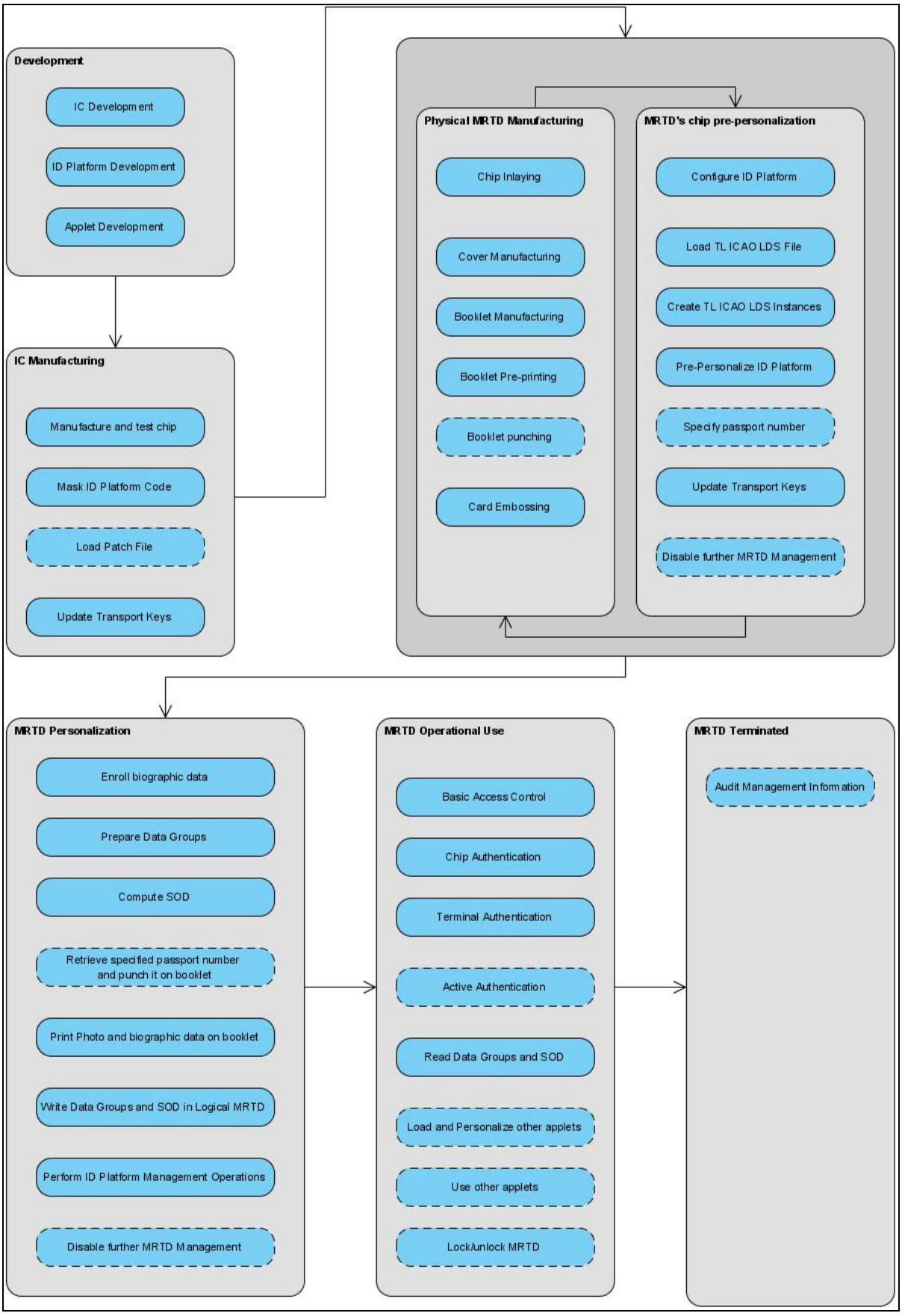
Cette architecture peut être représentée de la façon suivante :



1.2.4. Cycle de vie

Le cycle de vie du produit est décrit dans [ST] au paragraphe 3.3.

La note d'application n°9 publiée par la DCSSI (cf. [DCSSI-NA-9]), et particulièrement le chapitre relatif au cycle de vie, a été utilisée. Ainsi, le point de livraison de la TOE est remonté de la fin *MRTD Manufacturing* (point de livraison indiqué dans le [PP EAC]) à la fin de *IC Manufacturing* (point de livraison de la TOE), les étapes entre ces deux points (cf. *Physical MRTD Manufacturing* et *MRTD's pre-personalization* dans le schéma ci-dessous) étant couvertes par des guides (cf. [GUIDE]).



NB : Les pavés en pointillés représentent des actions optionnelles.

L'applet et la plate-forme ont été développées sur le site de :

Trusted Logic SA

5 rue du Bailliage
78000 VERSAILLES
FRANCE

Le composant a été développé sur le site de :

INFINEON TECHNOLOGIES AG

AIM CC SM PS
Am Campeon 1-12
85579 Neubiberg
GERMANY

Les utilisateurs et les administrateurs du produit hôte (voir rapport de certification du certificat [DCSSI-2008_43]) sont également utilisateurs et administrateurs du produit final.

Par ailleurs, pour l'évaluation, l'évaluateur a considéré comme :
- administrateurs du produit, les nations émettrices du passeport ;
- utilisateurs du produit, le porteur du passeport ainsi que l'officier de contrôle aux frontières et le système d'inspection qui interviennent en phase d'utilisation du produit.

1.2.5. Configuration évaluée

L'évaluation a couvert les deux mécanismes BAC et EAC qui peuvent utiliser les algorithmes RSA ou ECC et le protocole *Active Authentication.*

Le protocole *Chip Authentication* ne peut se faire qu'avec l'algorithme ECC (ECDH), tandis que le protocole *Active Authentication*, lorsque activé, ne peut se faire qu'avec l'algorithme RSA CRT.

De plus, étant donné que le produit est constitué d'une plate-forme *Java Card* ouverte, le produit peut être chargé avec d'autre(s) applet(s). Toutes les configurations sont couvertes dans le périmètre de l'évaluation.

Le certificat porte sur la configuration suivante du produit :
- état personnalisé de la plate-forme et de l'applet ;
- état GP INITIALIZED pour la carte ;
- état SELECTABLE pour l'applet.

Enfin, dans un mode d'utilisation spécifique du document de voyage, l'agent de personnalisation a la possibilité de désactiver toute future action de gestion de la carte (au sens *Global Platform*), afin que la plate-forme reste dans un mode natif (c'est-à-dire dans lequel l'*Issuer Security Domain* ne peut plus être sélectionné).

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1** [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM].
Pour les composants d'assurance qui ne seraient pas couverts par [CEM], des méthodes propres au centre d'évaluation et validées par la DCSSI 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 de l'applet dans le produit hôte certifié par ailleurs (certificat [DCSSI-2008_43]).
Cette évaluation a ainsi pris en compte les résultats de l'évaluation du produit hôte, effectuée par le même évaluateur, au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_VLA.4.

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 31 mars 2009, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques n'a pas été analysée par la DCSSI.

2.4. Analyse du générateur d'aléas

Le générateur d'aléas utilisé par le produit final est celui offert par le produit hôte (voir rapport de certification du certificat [DCSSI-2008_43]).

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 « Carte à puce TL ICAO LDS : applet de passeport électronique chargée sur la plate-forme JCLX80jTOP20ID masquée sur le composant SLE66CLX800PE, Version 2.0» soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 0 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation spécifiés dans la cible de sécurité [ST] au paragraphe 5.2 et suivre les recommandations se trouvant dans les guides fournis [GUIDES]. Notamment, il devra s'assurer que l'autorité de vérification vérifie que toute applet chargée sur la plate-forme, conjointement à celle du passeport électronique, respecte bien l'exigence d'anonymat exigée par le [PP EAC].

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 1999 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

3.3.2. Reconnaissance internationale critères communs (CCRA)

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

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

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, la République de Corée, le Pakistan, les Pays-Bas, 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 4+	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**	**4**	Complete functional specification
	ADV_IMP				**1**	1	**2**	2	**1**	Implementation representation of the TSF
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**3**	Basic 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 procedure
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	**4**	Problem tracking CM coverage
	ADO_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**2**	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**1**	Well defined development tools
ASE Security Target Evaluation	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claim
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended component 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 specifications
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	**2**	**3**	3	**4**	**2**	Testing: security enforcing modules
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independant 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 : - TL ICAO LDS EAC Security Target référence CP-2008-RT-432, version 1.3 Trusted logic Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - TL ICAO LDS EAC Security Target Lite référence PU-2009-RT-356, version 1.3 Trusted logic
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report - IRIS project référence IRIS_ETR_v1.0, version 1.0 Serma Technologies
[CONF]	Liste de configuration du produit - TF4C Software Configuration Management Plan référence CP-2007-RT-017, version 1.3 Trusted logic - TL ICAO LDS Software Configuration Management Plan référence CP-2008-RT-679, version 1.1 Trusted logic - Configuration List (IRIS files) référence IRIS_DELIVERY_SERMA_ALCCMS_200930330 Trusted logic
[GUIDES]	Guide de préparation du produit : - TL ICAO LDS Preparation Guide référence CP-2008-RT-727, version 1.3 Trusted logic Guide d'utilisation du produit : - TL ICAO LDS Operation Guide référence CP-2008-RT-740, version 1.1 Trusted logic
[PP BAC]	Protection Profile - Machine Readable Travel Document with ICAO Application, Basic Access Control, version 1.0, 18 August 2005. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0017*
[PP EAC]	Protection Profile - Machine Readable Travel Document with ICAO Application, Extended Access Control, version 1.2 du 19 November 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0026*

[OACI]	ICAO Doc 9303, Sixth Edition, 2007
[DCSSI-2008_43]	Certificat DCSSI délivré le 19 décembre 2008 pour le produit carte à puce JCLX80jTOP20ID : Java Trusted Open Platform sur composant SLE66CLX800PE *Certifiée par la DCSSI sous la référence DCSSI-2008_43*

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 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, September 2006, version 3.1, revision 1, ref CCMB-2006-09-001; Part 2: Security functional components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-002; Part 3: Security assurance components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2007, version 3.1, révision 2, ref CCMB-2007-09-004.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2006-04-003 version 2.0, revision 1, April 2006.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2008-04-001 version 2.5 revision 1, April 2008.
[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 2.0, April 1999, Management Committee of Agreement Group.
[DCSSI-AN-9]	Note d'application E-passport : utilisation du profil de protection EAC référence NOTE/09.1, 2415/SGDN/DCSSI/SDR, 24 octobre 2008 SGDN/DCSSI