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-2009/35

Carte à puce JCLXxxjTOPyyIDv2 : applet de passeport électronique chargée sur la plate-forme JCLX80jTOP20IDv2 masquée sur le composant SLE66CLX800PE

Paris, le29/01/2010

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

Patrick Pailloux
[ORIGINAL SIGNE]

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-2009/35

Nom du produit

Carte à puce JCLXxxjTOPyyIDv2 : applet de passeport électronique chargée sur la plate-forme JCLX80jTOP20IDv2 masquée sur le composant SLE66CLX800PE

Référence/version du produit

Version 3.0

Conformité à un profil de protection

[PP EAC]

Machine Readable Travel Document with „ICAO application", Extended Access Control v1.2, 19 November 2007

Critères d'évaluation et version

Critères Communs version 3.1

Niveau d'évaluation

EAL 4 augmenté

ALC_DVS.2, AVA_VAN.5

Développeur(s)

Trusted Logic

5 rue du Bailliage, 78000 Versailles, France

Infineon Technologies AG

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

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

Table des figures

1. Le produit

1.1. Présentation du produit

Le produit évalué est la carte à puce JCLXxxjTOPyyIDv2, version 3.0, développée par Trusted Logic et Infineon Technologies AG. Il est constitué d'une applet de passeport électronique chargée en ROM sur une plate-forme Java-Card, elle-même masquée sur un microcontrôleur sécurisé.

La présente évaluation porte sur un produit en double composition :

- une première composition dont le résultat est la plate-forme « Java Trusted Open Platform IFX#42 avec patch en version 2.0, masquée sur composants SLE66CLX800PE et SLE66CLX360PE », et certifiée sous la référence [ANSSI-CC-2009/34] (le produit résultant est appelé « produit hôte » dans la suite de ce document) ;
- une deuxième composition entre l'applet de passeport électronique et le produit hôte susmentionné.

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

1.2. Description du produit

La cible de sécurité [ST] (*Security Target)* 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 (cf. chapitre 1.2 [RTE]):

Sujet concerné	***Configuration concernée***	***Version***	***Origine***
Nom commercial de la TOE	JCLXxxjTOPyyIDv2	3.0	Trusted Logic
Autre dénomination de la TOE	TL ICAO LDS chargée sur jTOP ID platform	3.0	
Nom commercial de la plate-forme	jTOP ID Platform (JCLX80jTOP20ID)		Trusted Logic Infineon Technologies
Référence ROM	IFXv#42		Trusted Logic
Version du patch en EEPROM	2.0		
Nom du composant	SLE66CLX800PE		Infineon Technologies
Référence complète du composant	SLE66CLX800PE-m1581-e13/a14[1] SLE66CLX360PE-m1587-e13/a14		

Le fabricant décline, pour des raisons commerciales, différentes variantes de la configuration ci-dessus.
Ces variantes sont obtenues en initialisant différents paramètres correspondant à la taille mémoire, aux interfaces offertes et aux algorithmes cryptographiques autorisés ainsi qu'au type de passeport utilisé à partir de deux composants. Ces initialisations sont réalisées lors de la phase de fabrication.
Le nommage adopté par le fabricant pour ces variantes est **JC(L)(X)xxjTOPyyIDv2** dans lequel :

- « L » indique, s'il est présent, que l'interface sans contact est activée. La conformité au PP EAC oblige à ne considérer que la configuration « interface sans contact » activée.
- « X » indique, s'il est présent, que les algorithmes cryptographiques asymétriques sont activés ;
- « xx » indique la taille EEPROM qui peut être utilisée par le client final (maximum 80 Ko sur le composant SLE66CLX800PE et 36 Ko sur le composant SLE66CLX360PE) ;
- « yy » donne sur deux digits le type de passeport électronique utilisé :
    - 0x11 pour un passeport électronique supportant BAC & EAC sur une plateforme jTOP (*Java Trusted Open Platform)* fermée ne permettant pas le chargement d'une application ;
    - 0x31 pour un passeport électronique supportant BAC & EAC sur une plateforme jTOP.

Le produit certifié correspond donc au nommage suivant : **JCLXxxjTOPyyIDv2**.

[1] Les travaux d'évaluation ont été faits sur ce composant. L'évaluateur a considéré que ceux-ci pouvaient être généralisés au composant SLE66CLX360-m1587-e13/a14.

La plate-forme de la TOE peut être identifiée de façon unique au travers de la réponse à la mise sous tension ou de différentes commandes :

- les 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 16 2A 20 83 XX 90 00 dans lesquels les octets historiques permettent d'identifier :
  - le fabricant du composant : **40 90** ;
  - le type du composant : **A4** (pour SLE66CLX800PE)[1] ;
  - le type du masque : **16** ;
  - la version du masque : **2A** (version 42 de jTOP) ;
  - la révision du masque : **20** (2.0 est la version courante du patch).

  Le dernier octet précédant le mot d'état (90 00) est variable. Il dépend de l'état courant du cycle de vie de la carte (dans l'implémentation Global Platform [GPCS], va de OP_READY à TERMINATED).
- un GET DATA sur le *tag* (étiquette) 'DC' renvoie quant à lui la valeur du paramètre « NVRAM Size Lock », ce qui correspond à la taille de la zone EEPROM disponible pour la mémoire virtuelle ;
- un GET DATA sur le *tag* 'D0' renvoie la valeur du paramètre « Card Configuration », ce qui correspond à la valeur « 0x11 : carte fermée » ou « 0x31 : carte ouverte ».

L'applet de la TOE peut être identifiée grâce au *tag* 53 renvoyé 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 03 00 90 26 90 00.

Dans le champ valeur de ce *tag* 53 (constitué des 8 octets soulignés ci-dessus), on trouve :

- la version des spécifications de LDS, soit 01 07 pour 1.7 ;
- la version des spécifications de PKI, soit 01 01 pour 1.1 ;
- la version de l'applet, soit 03 00 pour 3.0 ;
- la date de génération de l'applet, soit 90 26 pour 26 janvier 2009[2].

Ces informations (ATR, tag DC, tag D0 et tag 53) permettent de tracer tous les éléments constitutifs de la TOE (composant, masque matériel, patch logiciel et applet). Les valeurs citées ci-dessus, conformes à celles utilisées dans [ST] et [CONF], permettent d'identifier de manière unique la TOE.

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 [ANSSI-CC-2009/34]) :
- de ceux fournis par l'applet, à savoir:
  - un canal sécurisé avec un terminal de personnalisation ;
  - un canal sécurisé avec un système d'inspection ;

[1] Ce serait **B6** pour le composant SLE66CLX360PE
[2] 9026 pour 26ème jour de l'année 2009

- le protocole d'authentification basé sur le mécanisme *Basic Access Control* (BAC) ;
- le protocole *Chip Authentication* ;
- le protocole *Active Authentication* ;
- le protocole *Terminal Authentication* ;
- le protocole *Personalization Authentication* ;
- le contrôle d'accès aux fichiers ;

- de la réalisation de l'anonymat du document de voyage électronique *MRTD Anonymity* ;
- du contrôle de l'intégrité du *ByteCode*.

1.2.3. Architecture

Le produit est constitué :

- d'une « applet »[1] de passeport électronique masquée en ROM ;
- d'un patch (v2.0) 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 :

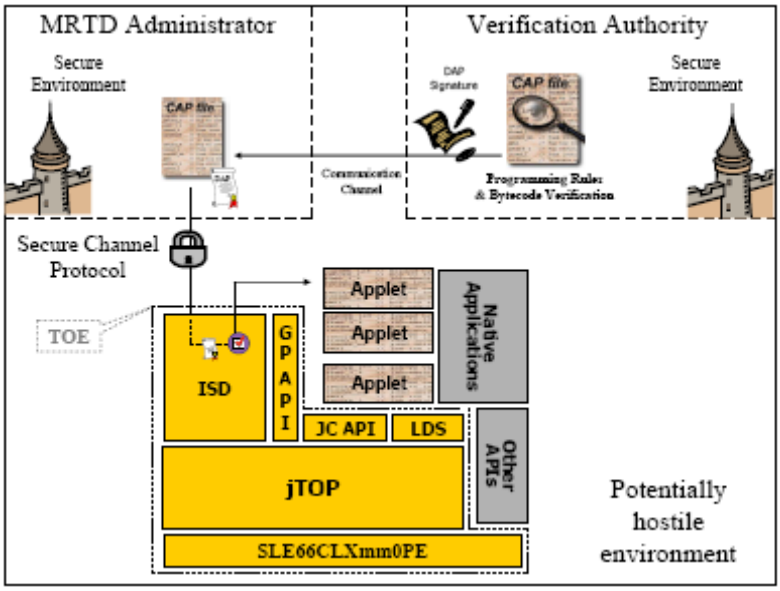

Figure 1 : Architecture du passeport de sécurité

[1] Fichier CAP

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 l'ANSSI [DCSSI-AN-9], notamment le chapitre relatif au cycle de vie, a été utilisé. Ainsi, le point de livraison de la TOE est remonté de la fin de la « fabrication du document de voyage », *MRTD Manufacturing*, (point de livraison indiqué dans le [PP EAC]) à la fin de la « fabrication du micro-circuit », *IC Manufacturing*, (point de livraison de la TOE).

Les étapes entre ces deux points (Fabrication « physique » du document de voyage *Physical MRTD Manufacturing* et la pré-personnalisation de la puce du document de voyage, *MRTD's chip pre-personalization*, dans le schéma ci-dessous) étant couvertes par des guides [GUIDES].

Légende figure 2:

Livraison sécurisée avec procédure de contrôle

Livraison dans une enceinte sécurisée

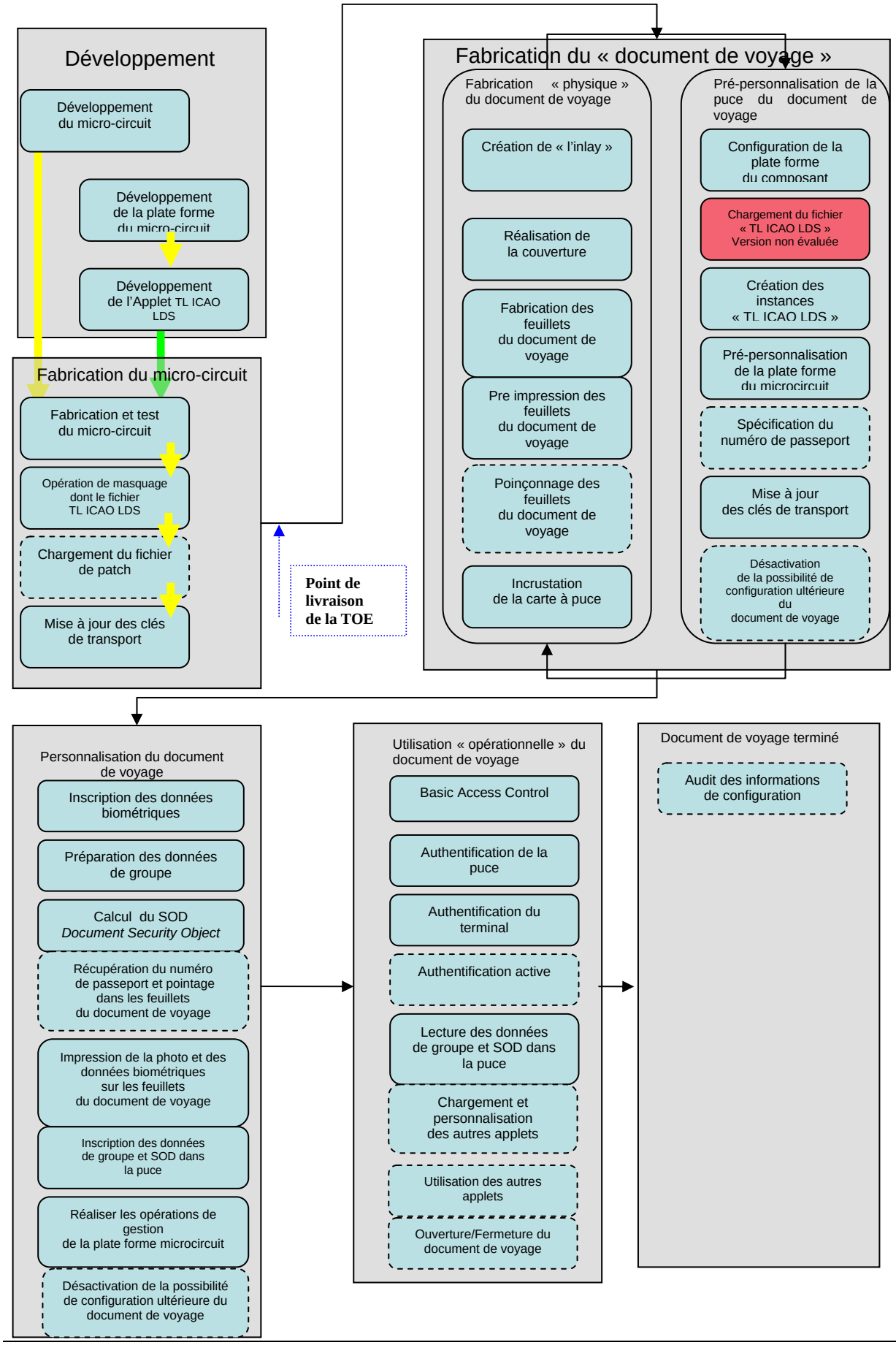

Figure 2 : Cycle de vie du document de voyage électronique

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
Allemagne

Par ailleurs, pour l'évaluation, l'évaluateur a considéré comme :

- administrateurs du produit : les nations ou organisations émettrices du passeport ;
- utilisateurs du produit : le porteur du passeport, l'officier de contrôle aux frontières et le système d'inspection

1.2.5. Configuration évaluée

L'évaluation a couvert les deux mécanismes BAC[1] et EAC qui peuvent utiliser des algorithmes basés sur RSA ou ECC, ainsi que l'*Active Authentication* basé sur RSA CRT.

De plus, étant donné que le produit est constitué d'une plate-forme *Java Card* ouverte, le produit peut être chargé, lors de la pré-personnalisation du document de voyage, avec d'autres applets répondant aux critères de conformité tirés des politiques de sécurité présentées dans la cible de sécurité du produit hôte (cf. P.VERIFICATION et P.MRTD-TRACEABILITY dans [ST]).

Toutes les configurations sont couvertes dans le périmètre de l'évaluation.

Ces configurations sont complètement définies durant la phase de personnalisation faisant suite au processus ***EMV Command Personalization*** basé sur les spécifications *GlobalPlatform* [GPCS].

Le certificat porte sur la configuration suivante du produit :

- la plate-forme et l'applet sont personnalisées ;
- la carte est dans l'état GP_SECURED ;
- l'applet est dans l'état SELECTABLE.

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 *GlobalPlatform*[2]*).*

[1] Conformément à la note d'application n° 9 publiée par l'ANSSI [DCSSI-AN-9] et particulièrement le chapitre relatif à la résistance du mécanisme BAC.
[2] 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] et à la méthodologie d'évaluation définie dans le manuel CEM *Evaluation Methodology* [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 AP] et [COMP] 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 produit hôte déjà certifié par ailleurs [ANSSI-CC-2009/34].

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 (CC 2.3).

Le rapport technique d'évaluation, remis à l'ANSSI le 9 juillet 2009 [RTE] 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

A la demande du commanditaire, la cotation des mécanismes cryptographiques selon le référentiel technique [REF_CRY] n'a pas été réalisée par l'ANSSI. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception ni de construction pour le niveau AVA_VAN visé.

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 [ANSSI-CC-2009/34]).

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 JCLXxxjTOPyyIDv2 : applet de passeport électronique chargée sur la plate-forme JCLX80jTOP20IDv2 masquée sur le composant SLE66CLX800PE » 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 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 qui ont été spécifiés dans la cible de sécurité [ST] et suivre les recommandations se trouvant dans les guides fournis [GUIDES]. Notamment, il devra s'assurer que l'autorité de vérification (Figure 1) 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].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2], 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 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.
[2] 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 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
	ALC_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 1.7 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-2008-RT-432-1.7-LITE Trusted logic
[RTE]	Rapport technique d'évaluation : – Evaluation Technical Report ICARIOS project reference ICARIOS_ETR_V1.0, version 1.0 Serma Technologies
[GPCS]	GlobalPlatform 2.1.1 Card Specification (March 2003) GlobalPlatform
[CONF]	Liste de configuration du produit – Java Trusted Open Platform Software Configuration Management Plan Référence CP-2007-RT-017, version 1.4 Trusted Logic – TL ICAO LDS Software Configuration Management Plan Référence CP-2009-RT-186, version 1.0 Trusted Logic – Configuration Liste (ICARIOS files) ICARIOS_DELIVERY_SERMA_ALCCMS_20090709 Trusted Logic
[GUIDES]	Guide de préparation du produit : – TL ICAO LDS Preparation Guide Référence : CP-2008-RT-727 V1.7 Trusted Logic Guide d'utilisation du produit : – TL ICAO LDS Operation Guide Référence : CP-2008-RT-740 V1.2 Trusted Logic
[PP EAC]	Protection Profile - Machine Readable Travel Document with « ICAO Application », Extended Access Control, version 1.2 du 19 ovembre 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0026-2006-MA-01*
[OACI]	ICAO Doc 9303, Sixth Edition, 2006

[ANSSI-CC-2009/34]	Certificat ANSSI : – délivré le 27 octobre 2009 – pour le produit « carte à puce JCLX80jTOP20ID : Java Trusted Open Platform IFX#v42, avec patch en version 2.0, masquée sur composants SLE66CLX800PE et SLE66CLX360PE » – sous la référence ANSSI-CC-2009/34

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, revision 2, ref CCMB-2007-09-004.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2009-03-001 version 2.7, Mars 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.
[CCRA]	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
[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.11 du 24 octobre 2008, voir www.ssi.gouv.fr