



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-2013/64

**Carte à puce SLJ 52 Gxx yyy AL : application
pour passeport électronique sur plateforme
jTOP INFv#46 masquée sur composants
Infineon SLE78CLX1600PM,
SLE78CLX800P et
SLE78CLX360PM**

Paris, le 18 novembre 2013

*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 présumées 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

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification

ANSSI-CC-2013/64

Nom du produit

Carte à puce SLJ 52 Gxx yyy AL : application pour passeport électronique sur plateforme jTOP INFv#46 masquée sur composants Infineon SLE78CLX1600PM, SLE78CLX800P et SLE78CLX360PM

Référence/version du produit

5.7

Conformité aux profils de protection

[PP EAC], version 1.10-2009

Common Criteria PP Machine Readable Travel Document with ICAO Application, Extended Access Control

[PP PACE], version 2-2011

Common Criteria PP Machine Readable Travel Document using Standard Inspection Procedure with PACE

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 4 augmenté
ALC_DVS.2, AVA_VAN.5

Développeur(s)

Trusted Logic SAS
6, rue de la Verrerie,
92197 Meudon, FRANCE

Infineon Technologies AG
AIM CC SM PS - Am Campeon 1-12 -
85579 Neubiberg, ALLEMAGNE

Commanditaire

Trusted Logic SAS
6, rue de la Verrerie,
92197 Meudon, FRANCE

Centre d'évaluation

Serma Technologies

14 rue Galilée – CS 10055, 33615 Pessac Cedex, FRANCE

Accords de reconnaissance applicables



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	6
1.1. PRESENTATION DU PRODUIT	6
1.2. DESCRIPTION DU PRODUIT	6
1.2.1. <i>Introduction</i>	6
1.2.2. <i>Identification du produit</i>	6
1.2.3. <i>Services de sécurité</i>	7
1.2.4. <i>Architecture</i>	8
1.2.5. <i>Cycle de vie</i>	8
1.2.6. <i>Configuration évaluée</i>	10
2. L’EVALUATION	11
2.1. REFERENTIELS D’EVALUATION	11
2.2. TRAVAUX D’EVALUATION	11
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI	11
2.4. ANALYSE DU GENERATEUR D’ALEAS	12
3. LA CERTIFICATION	13
3.1. CONCLUSION	13
3.2. RESTRICTIONS D’USAGE	13
3.3. RECONNAISSANCE DU CERTIFICAT	14
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	14
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i>	14
ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT	15
ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	16
ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION	18

1. Le produit

1.1. Présentation du produit

Le produit évalué est la carte à puce « SLJ 52 Gxx yyy AL, version 5.7 » développée par Trusted Logic et Infineon. Il est composé d'une application pour passeport électronique sur plateforme jTOP INFv#46 masquée sur composants Infineon SLE78CLX1600PM, SLE78CLX800P et SLE78CLX360PM.

La présente évaluation porte sur un produit en double composition :

- une première composition dont le résultat est la plate-forme « Java Trusted Open Platform (jTOP) INFv#46 masquée sur composants SLE78CLX1600PM, SLE78CLX800P et SLE78CLX360PM » et certifiée sous la référence [ANSSI-CC-2013/55]. 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 (ICAO) et les profils de protection *Extended Access Control* [PP EAC] et *Standard Inspection Procedure with PACE* [PP PACE].

1.2. Description du produit

1.2.1. Introduction

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 aux profils de protection [PP EAC] et [PP PACE]. Dans les deux cas, il s'agit d'une conformité stricte.

1.2.2. 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 de l'application	TL ICAO LDS – PACE/EAC on jTOP INFv#46
Version de l'application	5.7
Nom de la plateforme	jTOP INFv#46
Version de la plateforme	46.03
Intitulé dans le système de gestion des versions	TREL_INF_SLE78_GP22ID_V46_03

Configuration de la carte	0x7D:0x04:0x18:0x00:0x80:0x00:0x2A:0x04:0x00
Nom du composant	M7820 A11
Versions du composant	SLE78CLX1600PM, SLE78CLX800P et SLE78CLX360PM

Ces éléments sont obtenus après un ATR¹ ou en utilisant la commande Get Data (voir [GUIDES]).

Le produit est commercialisé sous plusieurs configurations dont le nom est SLJ 52 Gxx yyy AL, où

- **xx** correspond au type d'interface utilisé (contact / sans contact / *dual*, avec ou sans Mifare) ;
- **yyy** à la taille de la mémoire non volatile.

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- ceux fournis par l'applet, à savoir :
 - o la protection en intégrité et confidentialité des données ;
 - o l'authentification forte entre la carte et le système d'inspection ;
 - o le mécanisme *Active Authentication* ;
 - o le contrôle d'accès aux fichiers ;
- et ceux fournis par la plate-forme puisque cette dernière est maintenue dans un état ouvert (voir [ANSSI-CC-2013/55]).

¹ Answer to reset.

1.2.4. 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 :

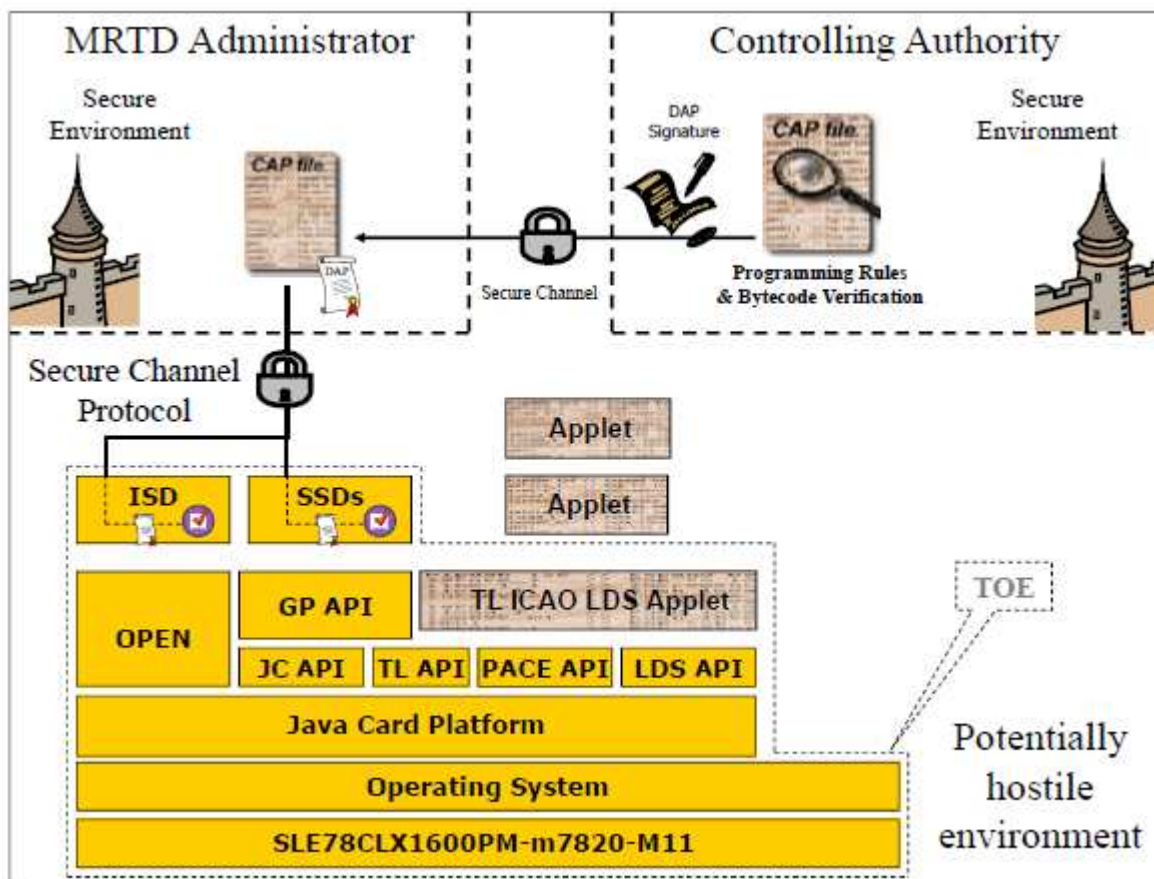


Figure 1

1.2.5. Cycle de vie

La figure 2 décrit le cycle de vie global du produit.

Les phases de conception et de développement du composant et de la plateforme sont couvertes par l'évaluation du composant (voir [BSI-DSZ-CC-0829-2012]) et de la plateforme (voir [ANSSI-CC-2013/55]).

¹ Fichier CAP.

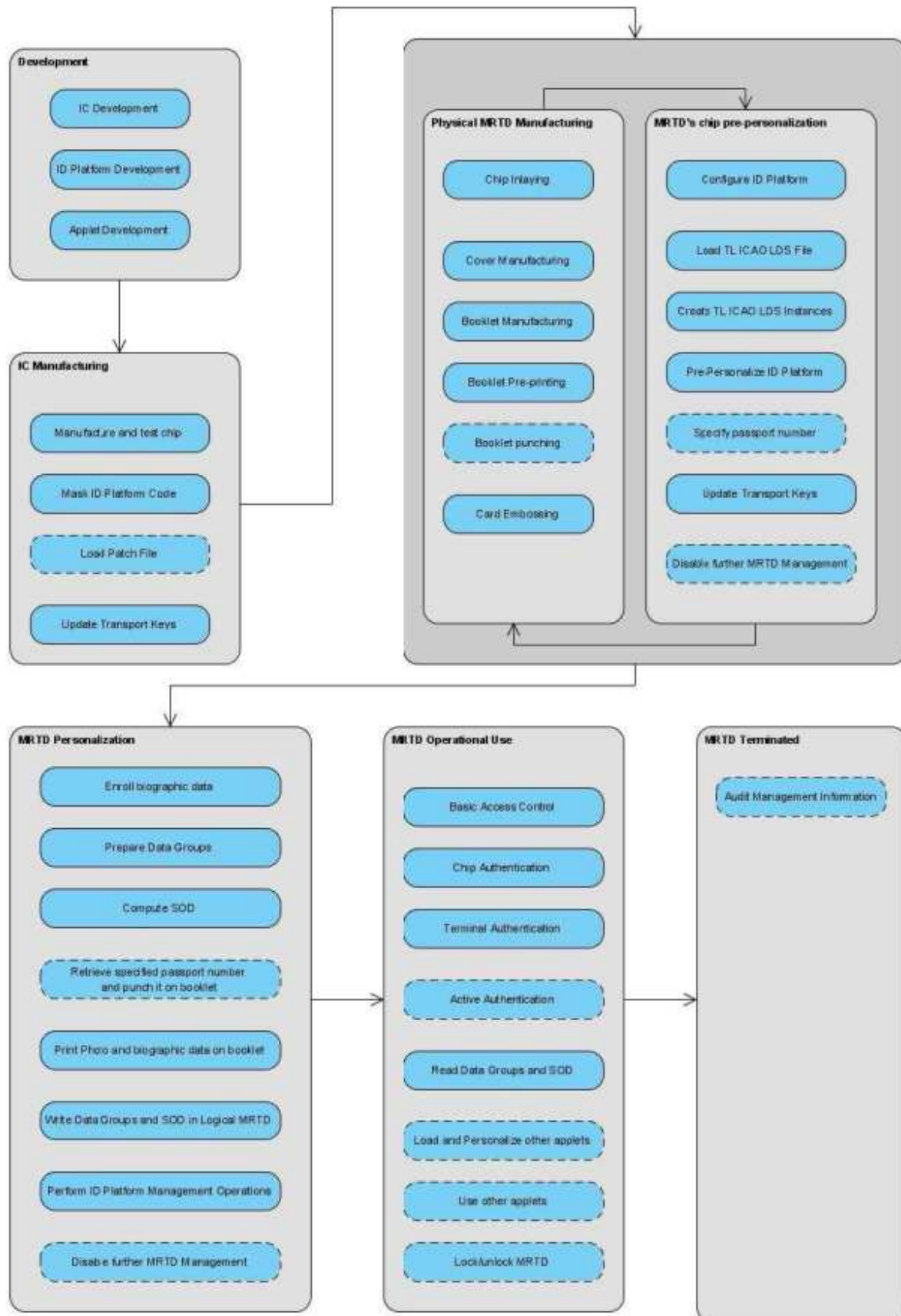


Figure 2

Le point de livraison de la TOE se situe entre le bloc « IC manufacturing » et le bloc général de fabrication du document de voyage.

Les fonctions de sécurité de la TOE sont évaluées dans la phase d'utilisation.

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

Trusted Logic SA
6 rue de la Verrerie
92190 Meudon
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.

1.2.6. Configuration évaluée

Le certificat porte sur l'application de passeport électronique sur la plateforme avec l'ensemble des API indiquées dans la figure 1.

Le produit a été évalué dans sa configuration passeport électronique avec l'interface contact (sans Mifare), il s'agit de la configuration **SLJ 52 GCA yyy AL**, qui comporte l'ensemble des services de sécurité offert par le produit.

La plateforme est laissée en configuration ouverte du produit et a donc été évaluée conformément à [NOTE.10] : ce produit correspond à une plateforme ouverte cloisonnante. Ainsi tout chargement de nouvelles applications conformes aux contraintes exposées au chapitre 3.2 et réalisé selon les processus audités ne remet pas en cause le présent rapport de certification.

Le CESTI a testé la plateforme masquée sur le composant M7820A11 dans ses configurations SLE78CLX1600PM, SLE78CLX800P et SLE78CLX360PM.

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 [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 [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

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 des évaluations de la plateforme et des composants.

Les microcontrôleurs de la famille « M7820 A11 » ont été évalués au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5, en conformité au profil de protection [PP-0035] et certifiés le 6 juin 2012 sous la référence [BSI-DSZ-CC-0829-2012].

La plateforme « Java Trusted Open Platform (jTOP) INFv#46 » a été évaluée au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5, en conformité au profil de protection [PP JCS] et certifiée le 7 août 2013 sous la référence [ANSSI-CC-2013/55].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 14 novembre 2013, 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 selon le référentiel technique de l'ANSSI [REF], n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA_VAN visé.

2.4. Analyse du générateur d'aléas

Le générateur de nombres aléatoires, de nature physique, utilisé par le produit final a été évalué dans le cadre de l'évaluation du microcontrôleur (voir [BSI-DSZ-CC-0829-2012]).

Par ailleurs, comme requis dans le référentiel cryptographique de l'ANSSI ([REF]), la sortie du générateur physique d'aléas subit un retraitement de nature cryptographique.

Les résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.5 visé.

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 SLJ 52 Gxx yyy AL : application pour passeport électronique sur plateforme jTOP INFv#46 masquée sur composants Infineon SLE78CLX1600PM, SLE78CLX800P et SLE78CLX360PM, version 4.7 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté des composants ALC_DVS.2 et AVA_VAN.5.

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], notamment :

- les développeurs d'applets complémentaires doivent appliquer le guide de développement d'applications « *Operational User Guidance* » ;
- les autorités de vérification doivent appliquer le guide « *jTOP Preparation Guide* ».

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'accord¹, 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 :



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 signataires², 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'Autriche, l'Espagne, la Finlande, la France, 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	1	Security architecture description	
	ADV_FSP	1	2	3	4	5	5	6	4	4	Complete functional specification	
	ADV_IMP				1	1	2	2	1	1	Implementation representation of the TSF	
	ADV_TDS		1	2	3	4	5	6	3	3	Basic modular design	
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance	
	AGD_PRE	1	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	4	Production support, acceptance procedures and automation	
	ALC_CMS	1	2	3	4	5	5	5	4	4	Problem tracking CM coverage	
	ALC_DEL		1	1	1	1	1	1	1	1	Delivery procedures	
	ALC_DVS			1	1	1	2	2	2	2	Sufficiency of security measures	
	ALC_FLR											
	ALC_LCD			1	1	1	1	2	1	1	Developer defined life-cycle model	
	ALC_TAT				1	2	3	3	1	1	Well defined development tools	
ASE Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1	1	1	Conformance claim	
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended component definition	
	ASE_INT	1	1	1	1	1	1	1	1	1	ST introduction	
	ASE_OBJ	1	2	2	2	2	2	2	2	2	Security objectives	
	ASE_REQ	1	2	2	2	2	2	2	2	2	Derived security requirements	
	ASE_SPD		1	1	1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	1	1	TOE summary specifications
ATE Tests	ATE_COV		1	2	2	2	3	3	2	2	Analysis of coverage	
	ATE_DPT			1	2	3	3	4	2	2	Testing: security enforcing modules	
	ATE_FUN		1	1	1	1	2	2	1	1	Functional testing	
	ATE_IND	1	2	2	2	2	2	3	2	2	Independent testing, -sample	
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	5	Advanced methodical vulnerability analysis	

Annexe 2. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation : TL ICAO LDS-PACE/EAC Security Target ; Référence : CP-2012-RT-767/1.7 ; Version : 1.7 du 04 novembre 2013.</p> <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : TL ICAO LDS-PACE/EAC Security Target - LITE ; Référence : CP-2012-RT-767 – LITE 1.0 ; Version : 1.0 du 12 novembre 2013.</p>
[RTE]	<p>Rapport technique d'évaluation : Evaluation Technical Report – Brontes Project ; Référence : BRONTES-ETR_v1.1 / 1.1 ; Version : 1.1 du 14 novembre 2013.</p>
[CONF]	<p>Configuration list (extraction from CVS) ; Référence : OURANOS_CONFIGURATION_ITEMS_20121122.TXT ; Daté du : 22 novembre 2012.</p>
[GUIDES]	<p>TL ICAO LDS-PACE/EAC Operation ; Référence : CP-2012-RT-770-1.2 ; Version : 1.2.</p> <p>TL ICAO LDS-PACE/EAC Preparation Guide ; Référence : CP-2012-RT-769-1.2 ; Version : 1.2.</p>
[PP-0035]	<p>Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.</i></p>
[PP JCS]	<p>Profil de protection "Java Card Protection Profile – Open Configuration", version 3.0 du 18 mai 2012. <i>Maintenu par l'ANSSI sous la référence ANSSI-CC-PP-2010/03-M01.</i></p>
[PP EAC]	<p>Protection Profile - Machine Readable Travel Document with "ICAO Application", Extended Access Control, version 1.10, 25 Mars 2009. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0056-2009.</i></p>
[PP PACE]	<p>Protection Profile - Machine Readable Travel Document using Standard Insepection Procedure with PACE, version 1.10, 25 Mars 2009. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0055-2009.</i></p>
[BSI-DSZ-CC-0829-2012]	<p>Certificat délivré par le BSI le 5 septembre 2012 pour le produit « Infineon smart card IC (Security Controller) M7820 A11 and M11</p>



	with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software ».
[ANSSI-CC-2013/55]	Certificat délivré par l'ANSSI le 7 août 2013 pour la Plateforme jTOP INFv#46 masquée sur composants Infineon SLE78CLX1600PM, SLE78CLX800P et SLE78CLX360PM.

Annexe 3. Références liées à la certification

<p>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.</p>	
[CER/P/01]	<p>Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.</p>
[CC]	<p>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.</p>
[CEM]	<p>Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.</p>
[JIWG AP]	<p>Mandatory Technical Document - Application of attack potential to smart-cards, JIWG, version 2.8, January 2012.</p>
[COMP]	<p>Joint Interpretation Library – Composite product evaluation for Smart Cards and similar devices, version 1.2, January 2012.</p>
[CC RA]	<p>Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.</p>
[SOG-IS]	<p>« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.</p>
[REF]	<p>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 (RGS_B_1), voir www.ssi.gouv.fr.</p>