



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-2013/55**

### **Plateforme jTOP INFv#46 masquée sur composants Infineon SLE78CLX1600PM, SLE78CLX800P et SLE78CLX360PM**

*Paris, le 7 août 2013*

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

Dominique Riban  
[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](mailto:certification.anssi@ssi.gouv.fr)

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

Référence du rapport de certification

**ANSSI-CC-2013/55**

Nom du produit

**Plateforme jTOP INFv#46 masquée sur composants  
Infineon SLE78CLX1600PM, SLE78CLX800P et  
SLE78CLX360PM**

Référence/version du produit

**Version 46.03**

Conformité à un profil de protection

**[PP JCS], version 3.0  
Java Card™ System  
Open Configuration Protection Profile**

Critères d'évaluation et version

**Critères Communs version 3.1 révision 3**

Niveau d'évaluation

**EAL 5 augmenté  
ALC\_DVS.2, AVA\_VAN.5**

Développeurs

**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  
30 avenue Gustave Eiffel, 33608 Pessac, 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](http://www.ssi.gouv.fr).



## Table des matières

<b>1. LE PRODUIT .....</b>	<b>6</b>
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> .....	7
1.2.5. <i>Cycle de vie</i> .....	8
1.2.6. <i>Configuration évaluée</i> .....	10
<b>2. L’EVALUATION .....</b>	<b>11</b>
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.....	11
<b>3. LA CERTIFICATION .....</b>	<b>13</b>
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
<b>ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT.....</b>	<b>15</b>
<b>ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE .....</b>	<b>16</b>
<b>ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION .....</b>	<b>18</b>

# 1. Le produit

## 1.1. Présentation du produit

Le produit évalué est la plateforme « Java Trusted Open Platform (jTOP) INFv#46 masquée sur composants SLE78CLX1600PM, SLE78CLX800P et SLE78CLX360PM » développée par Trusted Logic et Infineon.

Il s'agit d'une plateforme Java Card ouverte conçue de façon à ce que des applications sensibles (passport électronique, permis de conduire électronique, carte d'identité électronique, ...) puissent être chargées et exécutées de façon sécurisée.

Le produit est conforme aux spécifications *GlobalPlatform Card Specification* [GPCS], version 2.2.1 et plus particulièrement avec les spécifications *GlobalPlatform Card ID Configuration* [GPCS-ID], version 1.0.

## 1.2. Description du produit

### 1.2.1. Introduction

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 JCS]. Étant donné que cette version du profil de protection rend optionnelle l'utilisation du mécanisme RMI (*Remote Method Invocation* – méthode d'invocation à distance), non présent dans le produit, la conformité au PP est de type démontrable.

### 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 la TOE	jTOP INFv#46
Version de la TOE	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 ATR<sup>1</sup> ou en utilisant la commande Get Data (voir [GUIDES]).

<sup>1</sup> Answer to reset.



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

- **xx** correspond au type d'interface utilisés (contact / sans contact / *dual*, avec ou sans Mifare) ;
- **yyy** à la taille de la mémoire non volatile ;
- **z** au type d'application destiné à être chargé sur la plateforme.

### ***1.2.3. Services de sécurité***

Les principaux services de sécurité fournis par le produit sont :

- les services de sécurité au niveau du système d'exploitation :
  - o la gestion de l'exécution des applications ;
  - o le contrôle du flux d'exécution ;
  - o la gestion des états de la carte ;
  - o la gestion des accès mémoire ;
  - o la gestion de la confidentialité des mémoires ;
  - o le chargement de code sécurisé ;
  - o l'authentification du porteur de la carte ;
- les services de sécurité au niveau Java Card :
  - o la machine virtuelle défensive (JCVM – *Java Card Virtual Machine*) ;
  - o le pare-feu Java Card ;
  - o l'effacement sécurisé ;
- les services de sécurité au niveau GlobalPlatform :
  - o le gestionnaire de commandes ;
  - o le gestionnaire de cartes ;
  - o les canaux sécurisés ;
- les services cryptographiques :
  - o la génération de nombres aléatoires ;
  - o la génération de clés ;
  - o la gestion des clés ;
  - o la fourniture de mécanismes de chiffrement et de déchiffrement ;
  - o la fourniture de mécanismes de création et de vérification de signatures.

### ***1.2.4. Architecture***

Le produit est constitué des éléments suivants :

- du microcontrôleur, offrant les fonctionnalités matérielles (gestion de la mémoire et gestion des entrées/sorties), et sa bibliothèque cryptographique ;
- du système Java Card composé de :
  - o la machine virtuelle Java Card (JCVM) ;
  - o l'environnement d'exécution Java Card (JCRE) ;
  - o l'API Java Card (JCAPI) ;

- de diverses API :
  - o GlobalPlatform ;
  - o LDS (*Logical Data Structure* – API d'accès au système de fichier), définie dans [ST] comme ne fournissant pas de fonctions de sécurité ;
  - o PACE, définie dans [ST] comme ne fournissant pas de fonctions de sécurité ;
  - o API propriétaires Trusted Logic ;
- de plusieurs domaines de sécurité (développeur de la carte (ISD<sup>1</sup>) ou autre (SSD<sup>2</sup>)).

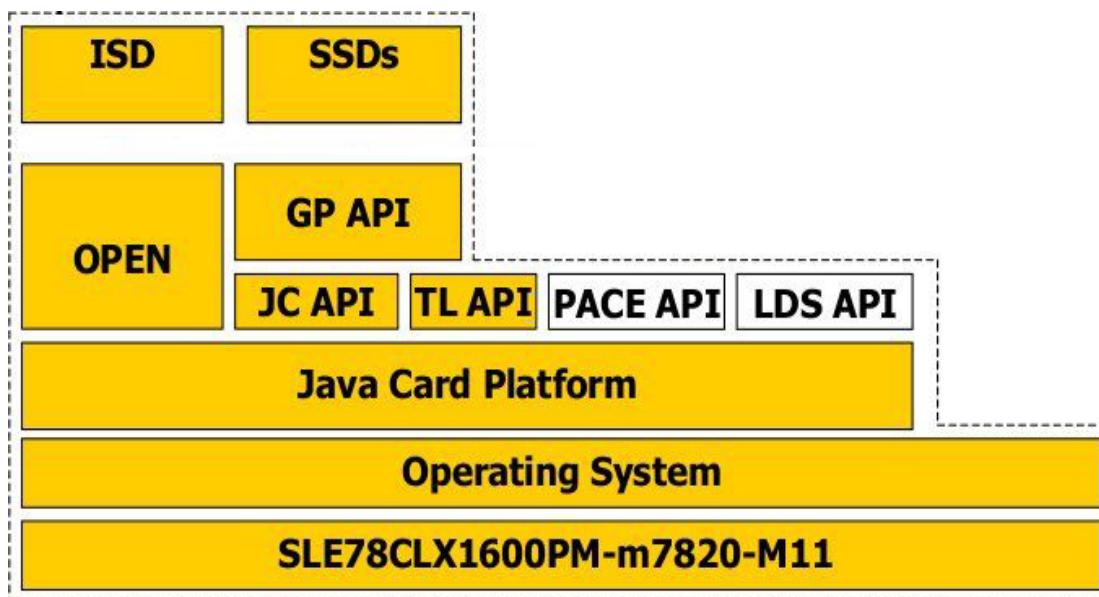


Figure 1 : Architecture de la plateforme

### 1.2.5. Cycle de vie

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

Les phases de conception (bloc « *IC & dedicated platform design* » et de fabrication (bloc « *IC Production* ») du composant sont couvertes par l'évaluation du composant (voir [BSI-DSZ-CC-0829-2012]).

Le périmètre de l'évaluation comprend les phases de conception et de développement du logiciel masqué. Cette phase est représentée dans la figure 2 par le bloc « *Platform design* ».

Les phases couvertes par l'évaluation correspondent à l'ensemble des phases jusqu'à ce que le produit atteigne l'état « *INITIALIZED Life Cycle State* » (voir figure 2). Les phases d'initialisation et de personnalisation de la plateforme ont été évaluées dans le cadre de l'évaluation du composant (voir [BSI-DSZ-CC-0829-2012]) et sont couvertes par les guides (voir [GUIDES]).

Les phases suivantes liées au chargement, à la gestion, à l'utilisation et à la suppression d'applications sont couvertes par les guides (voir [GUIDES]).

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

<sup>1</sup> Issuer security domain.

<sup>2</sup> Supplementary security domains.



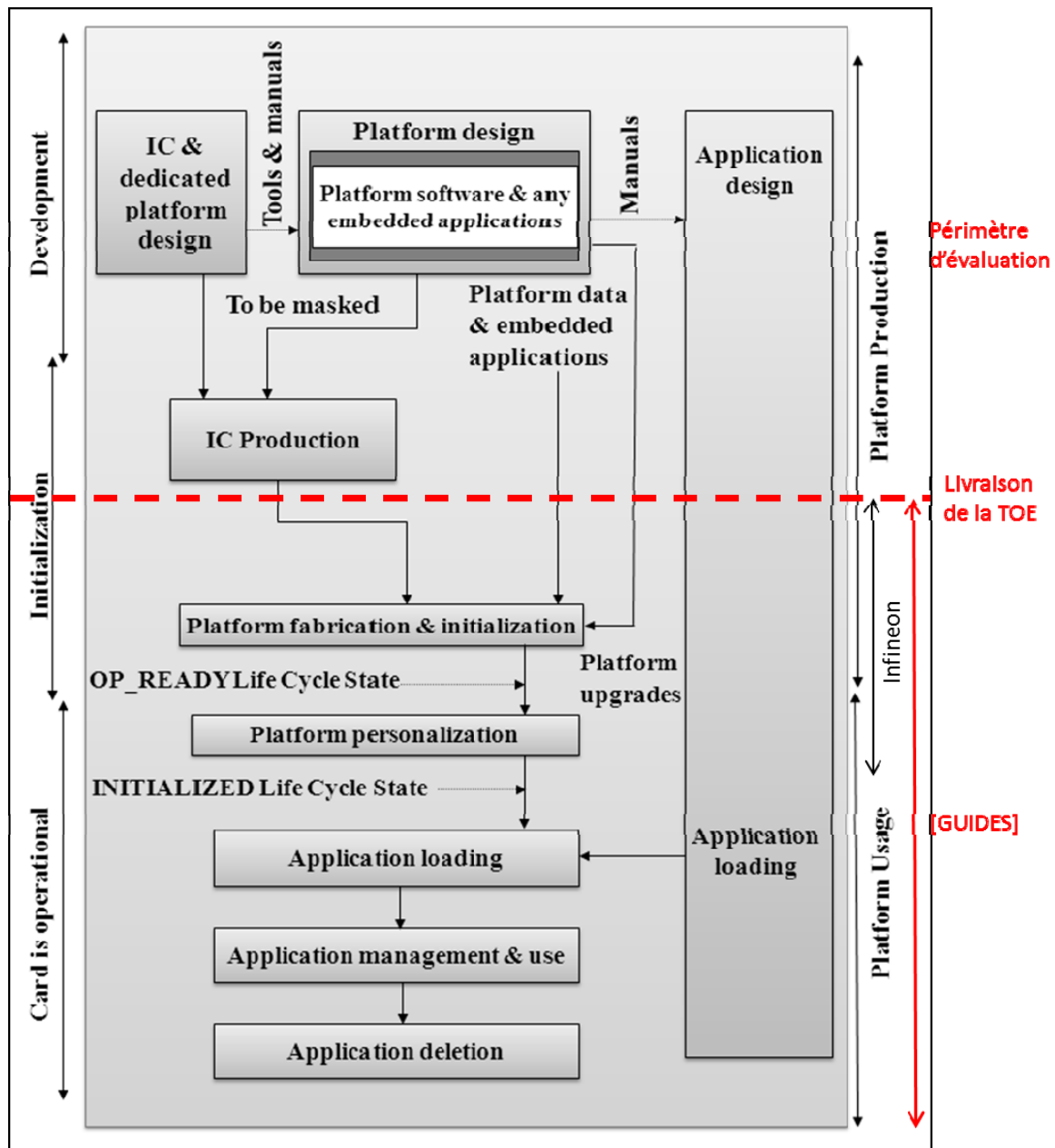


Figure 2 : Cycle de vie du produit

La plate-forme a été développée sur le site suivant :

**Trusted Logic SA**  
 6 rue de la Verrerie  
 92197 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

Une partie de la documentation a été rédigée sur le site de :

**Trusted Labs**

5 rue du Bailliage  
78000 Versailles  
France

Pour l'évaluation, l'évaluateur a considéré comme administrateur du produit le *Card Administrator* (administrateur de la carte) dont le rôle est défini dans [ST] et rappelé dans le guide d'administration du produit au chapitre Définitions (voir [GUIDES]).

En particulier, le *Card Administrator* est le représentant du *Card Issuer* (émetteur de la carte). Il a le contrôle du contenu de la carte, ainsi que de la gestion du cycle de vie de cette dernière. Durant la phase d'initialisation de la plate-forme, ce rôle est endossé par le *Card Enabler* (chargé d'habilitations de la carte). Durant la phase d'utilisation de la plate-forme, le *Card Administrator* peut verrouiller, déverrouiller, ou bloquer la carte, télécharger de nouvelles applets sur la carte, modifier les clés statiques de l'ISD ou récupérer des informations d'administration de la carte.

Par ailleurs, l'évaluateur a considéré comme utilisateurs du produit les *Application Developers* (développeurs d'applications) dont les responsabilités sont détaillées dans le guide d'utilisation du produit (voir [GUIDES]).

### ***1.2.6. Configuration évaluée***

Le certificat porte 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, il s'agit de la configuration **SLJ 52 GCA yyy DL**, qui comporte l'ensemble des services de sécurité offert par le produit.

La configuration ouverte du produit a 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 de l'évaluation des microcontrôleurs de la famille « M7820 A11 » au niveau EAL5 augmenté des composants ALC\_DVS.2 et AVA\_VAN.5, conforme au profil de protection [PP-0035] et certifié le 6 juin 2012 sous la référence [BSI-DSZ-CC-0829-2012].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 26 avril 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 « Plateforme jTOP INFv#46 masquée sur composants Infineon SLE78CLX1600PM, SLE78CLX800P et SLE78CLX360PM, version 46.03 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 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'applications 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'accord<sup>1</sup>, 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 signataires<sup>2</sup>, 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 :



---

<sup>1</sup> 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.

<sup>2</sup> 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_FLR									
	ALC_LCD			1	1	1	1	2	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	2	Compliance with implementation standards
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	1	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]	<p>Cible de sécurité de référence pour l'évaluation          JTOP INF#v46 (SLJ 52 Gxx yyy zL) – Security Target ;          Référence : CP-2011-RT-751-v.46-0.92 ;          Version : 0.92 du 14 février 2013.</p> <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :          Java Card Open Platform – Security Target-LITE ;          Référence : PU-2011-RT-751-v46-1.0-LITE ;          Version : 1.0 du 18 mai 2013.</p>
[RTE]	<p>Rapport technique d'évaluation :          Evaluation Technical Report – OURANOS Project ;          Référence : OURANOS-ETR_v1.0 ;          Version : 1.0 du 5 décembre 2012.</p> <p>Pour le besoin des évaluations en composition avec cette plateforme un rapport technique pour la composition a été validé :          ETR-lite for composition – ARGES Project ;          Référence : ARGES-ETR_Lite v1.0 ;          Version : 1.0 du 30 mai 2013.</p>
[CONF]	<p>Configuration list (extraction from CVS)          Référence : OURANOS_CONFIGURATION_ITEMS_20121122.TXT          Daté du : 22 novembre 2012.</p>
[GUIDES]	<p>jTOP INFv#46 (SLJ 52 Gxx yyy zL) - Operational User Guidance          Référence : CP-2011-RT-732-46          Version : 1.3</p> <p>jTOP INFv#46 (SLJ 52 Gxx yyy zL) – Preparative Procedures          Référence : CP-2011-RT-731-46          Version : 1.0</p> <p>jTOP Preparation Guide          Reference : CP-2011-RT-731-46-1.0          Version : 1.0</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>





[BSI-DSZ-CC-0829-2012]	Certificat délivré par le BSI le 5 septembre 2012 pour le produit « Infineon smart card IC (Security Controller) M7820 A11 and M11 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 ».
------------------------	---

### 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.
[JIWG AP]	Mandatory Technical Document - Application of attack potential to smart-cards, JIWG, version 2.8, January 2012.
[COMP]	Joint Interpretation Library – Composite product evaluation for Smart Cards and similar devices, version 1.2, January 2012.
[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]	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 <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a> .
[NOTE.10]	Joint Interpretation Library - Certification of « open » smart card products, version 1.1, February 2013.
[GPCS]	GlobalPlatform Card Specification, version 2.2.1, January 2011.
[GPCS-ID]	GlobalPlatform Card ID Configuration, version 1.0, December 2011.