PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification DCSSI-2009/02

Carte à puce jTOPv27-ASEv1 v1.0 : applet de signature électronique chargée sur la plate-forme JCLX80jTOP20ID masquée sur le composant SLE66CLX800PE

Paris, le 2 avril 2009

Le Directeur central 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 la Direction centrale de la sécurité des systèmes d'information (DCSSI), 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
Direction centrale 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

DCSSI-2009/02

Nom du produit

Carte à puce jTOPv27-ASEv1 v1.0 : applet de signature électronique chargée sur la plate-forme JCLX80jTOP20ID masquée sur le composant SLE66CLX800PE

Référence/version du produit

Version 1.0

Conformité à un profil de protection

Néant

Critères d'évaluation et version

Critères Communs version 2.3

conforme à la norme ISO 15408:2005

Niveau d'évaluation

EAL 4 augmenté

ADV_IMP.2, AVA_VLA.4

Développeur(s)

Trusted Labs
5 rue du Bailliage, 78000 VERSAILLES, FRANCE

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 Labs

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

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 :

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

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

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est la carte à puce jTOPv27-ASEv1 v1.0, version 1.0, développée par Trusted Labs. Il est constitué d'une applet de signature électronique chargée sur la plate-forme JCLX80jTOP20ID de Trusted Logic, elle-même masquée sur le composant SLE66CLX800PE d'Infineon technologies AG. Il est destiné à être utilisé dans le cadre d'applications de création de signature électronique.

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. Le résultat est un produit, une carte à puce, qui a été certifié (certificat [DCSSI-2008_43]) ;
- une deuxième composition entre l'applet de signature électronique et le produit précédemment certifié (nommé produit hôte par la suite).

1.2. Description du produit évalué

La cible de sécurité [ST] décrit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

Elle s'inspire du profil de protection BSI-PP-0006 pour les SSCD de type 3, mais elle ne réclame pas sa conformité (la validation des certificats n'est pas gérée par le produit par exemple).

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 :

Sujet concerné	***Configuration concernée***	***Origine***
Nom commercial	JCASE v1.0	Trusted Labs
Référence de la cible d'évaluation (label interne)	jTOPv27-ASEv1.0	Trusted Labs
Référence de la cible d'évaluation (label du composant)	SLE66CLX800PE	Infineon
Référence du système d'exploitation	Hardmask 1.0	Trusted Logic
Référence du masque logiciel (patch)	V1.4	Trusted Logic
Référence de l'applet	V1.0	Trusted Labs
Identifiant du composant	SLE66CLX800PE-m1581-e13/a14	Infineon

La partie 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 14 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 : 14 (1.4 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 GlobalPlatfom, va de OP_READY à TERMINATED).

La partie applet de la TOE peut être identifiée grâce au *tag* (étiquette) 51 renvoyée par l'instruction GET STATUS :

- 51 07 08 08 09 17 12 13 44 52 08 11 22 33 44 55 66 77 88 53 01 03 54 01 00 55 0056 00 90 00

Dans le champ valeur de ce *tag* 51 (constitué des 7 octets 08 08 09 17 12 13 44), on trouve la date (17 septembre 2008) et l'heure (12 h 13 min 44 sec) de génération de l'applet.

Ces informations (ATR et *tag* 51) 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 :

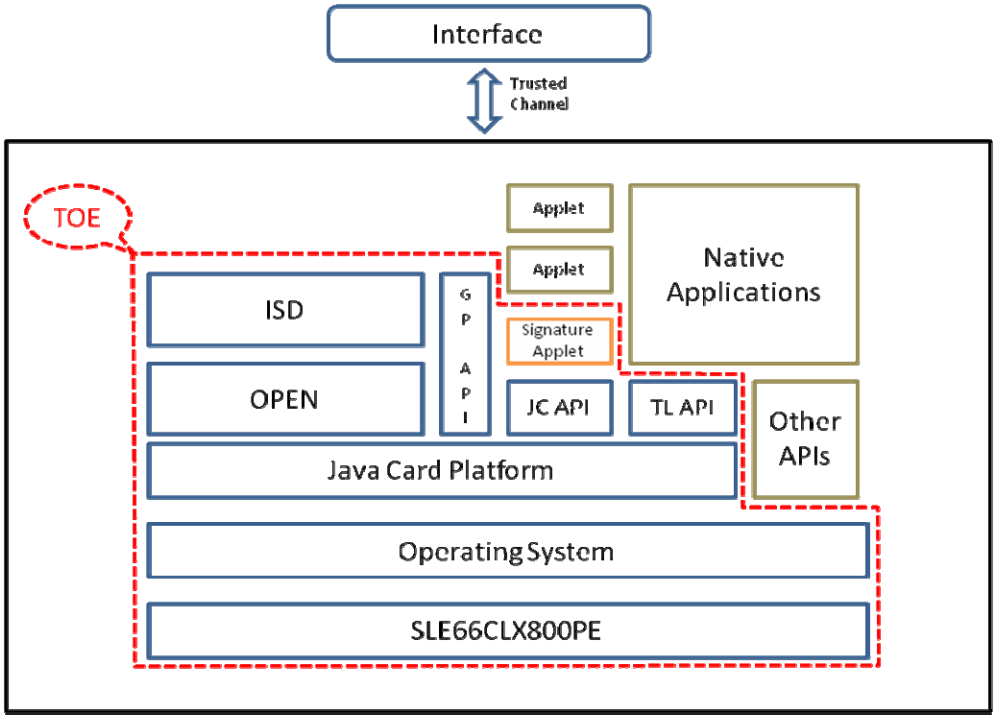
- de ceux fournis par la plate-forme (voir rapport de certification du certificat [DCSSI-2008_43]) :
- de ceux fournis l'applet :
  - *cryptographic keys generation* (génération de clés cryptographiques),
  - *public key export* (export de clé publique),
  - *signatory authentication* (authentification du signataire),
  - *electronic signature* (signature électronique),
  - *certificates storage* (stockage de certificats).

1.2.3. Architecture

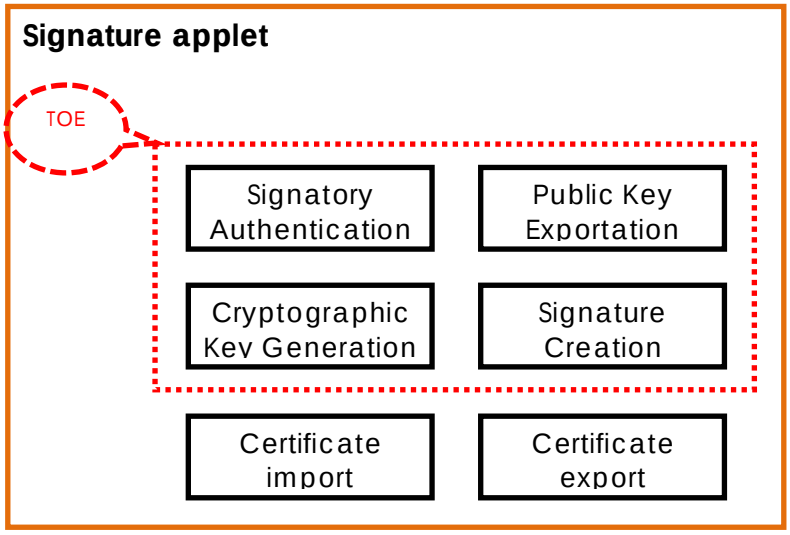
Le produit est constitué :

- d'une applet de signature électronique chargée en mémoire EEPROM (*Electrically Erasable Programmable Read Only Memory* – mémoire programmable en lecture seule et électriquement effaçable) ;
- d'un patch (v1.4) de la plate-forme, patch chargé en mémoire EEPROM ;
- d'une plate-forme masquée en ROM (*Read Only Memory* – mémoire en lecture seule) ;
- d'un composant.

Cette architecture peut être représentée de la façon suivante :



Concernant l'applet de signature, la figure ci-après identifie les éléments qui font partie de la TOE et ceux qui sont en dehors.



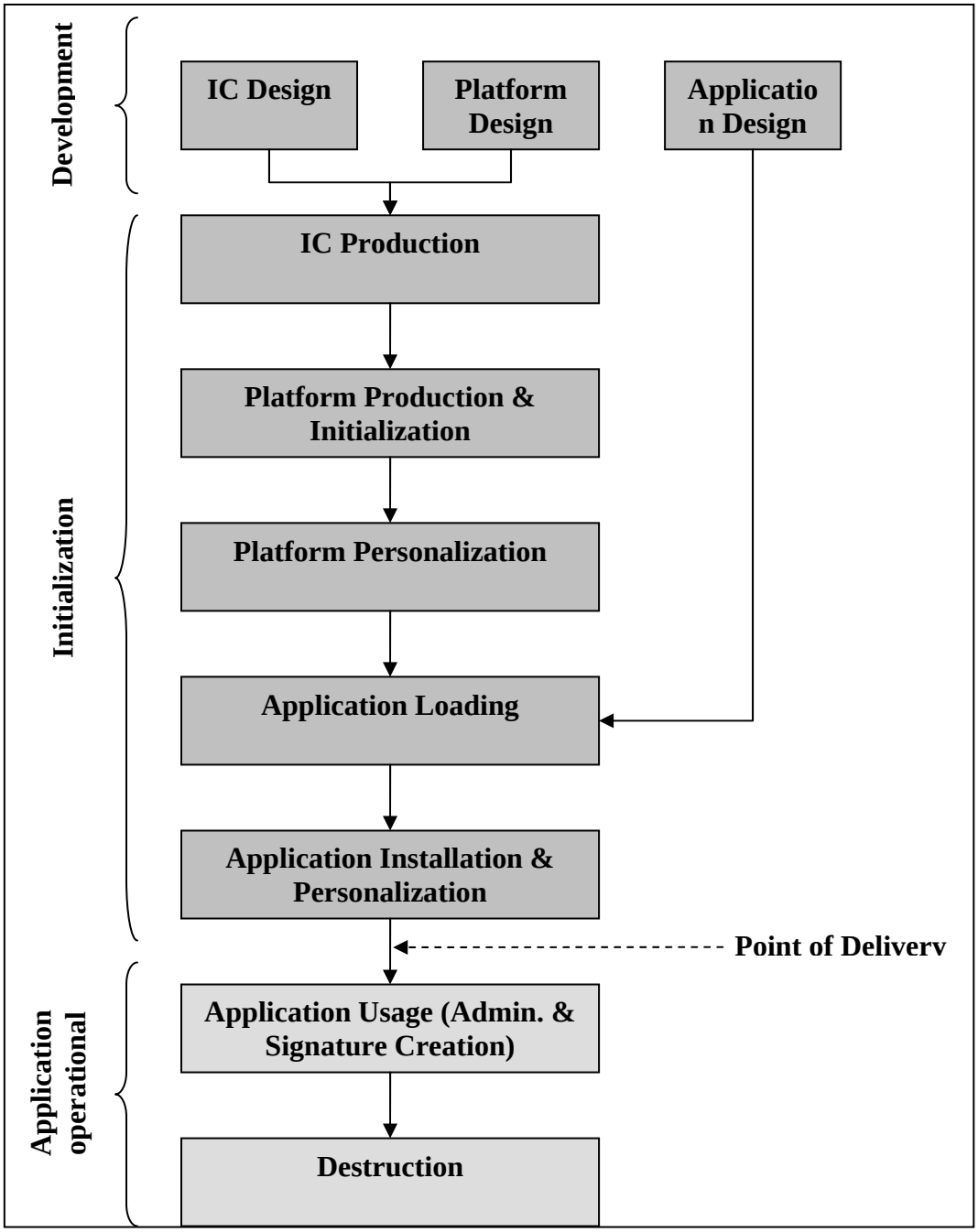
1.2.4. Cycle de vie

Le cycle de vie global de la TOE et celui particulier de l'applet sont décrits dans [ST].

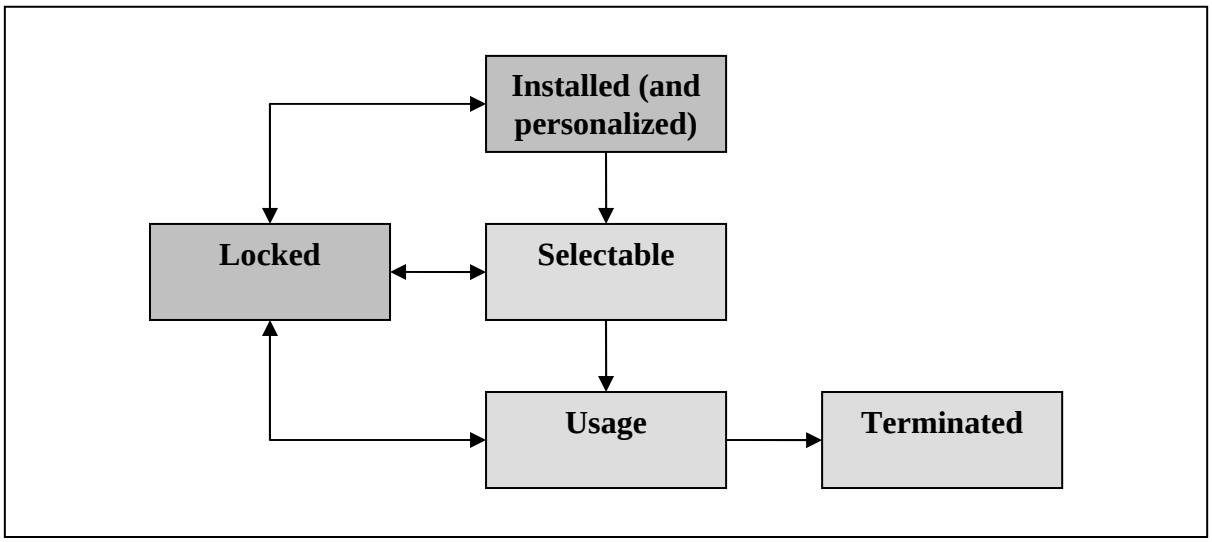
Le cycle de vie global de la TOE comprend toutes les étapes de design jusqu'à la fin de la phase de personnalisation, ainsi que toutes les étapes de la phase de fabrication du composant.

La plate-forme est masquée par le fabricant du composant qui l'initialise et la délivre au fabricant de carte ; ce dernier effectue la fabrication de la carte, personnalise la plate-forme, charge l'applet, installe cette dernière et la personnalise.

La figure suivante donne une illustration de ce cycle de vie global :



Le cycle de vie particulier de l'applet seule est illustré dans la figure suivante :



L'applet a été développée sur le site de :

Trusted Labs
5 rue du Bailliage
78000 VERSAILLES
FRANCE

La plate-forme a été développée 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 administrateurs du produit hôte (voir rapport de certification du certificat [DCSSI-2008_43]) sont également utilisateurs et administrateurs du produit final présent.

Les acteurs suivants peuvent interagir avec l'applet :

- *Card Administrator* (administrateur de la carte) : il est également celui de l'application de signature, il gère l'applet et effectue les requêtes de génération de clés à la carte ;
- *Signatory* (signataire et porteur de la carte) : il utilise l'application de signature électronique pour signer les messages qu'il a approuvés ;
- *ASE Application Provider* (fournisseur de l'application ASE) : c'est le développeur de l'applet ;
- *Service Provider* (fournisseur de service) : il peut demander au porteur de la carte de signer les messages afin d'obtenir son approbation ;
- *Application Integrator* (intégrateur d'application) : il charge et installe l'applet sur la plate-forme de la carte, la personnalise avec :
    - un code PIN (*Personal Identification Number* - code porteur),
    - une clé partagée pour le *Card Administrator*,
    - une clé partagée pour le *Service Provider*,
    - un numéro de série.

1.2.5. Configuration évaluée

Le certificat porte sur la configuration telle que définie au paragraphe §1.2.3. Architecture, en ayant le produit dans l'état :

- personnalisé pour la plate-forme et l'applet,
- GP INITIALIZED pour la carte,
- SELECTABLE pour l'applet.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 2.3** [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

Pour les composants d'assurance supérieurs au niveau EAL4, des méthodes propres au centre d'évaluation, validées par la DCSSI et compatibles avec le document [AIS 34], 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, effectuée par le même évaluateur, du produit hôte au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_VLA.4.

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 4 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 jTOPv27-ASEv1 v1.0 : applet de signature électronique chargée sur la plate-forme JCLX80jTOP20ID masquée sur le composant SLE66CLX800PE, de version 1.0, 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 décrit 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 spécifiés dans la cible de sécurité [ST] au chapitre §5.2 et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

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
ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2	**1**	Partial CM automation
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Configuration support and acceptance procedures
	ACM_SCP			**1**	**2**	**3**	3	3	**2**	Problem tracking CM coverage
ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**	**2**	Detection of modification
	ADO_IGS	**1**	1	1	1	1	1	1	**1**	Installation, generation and start-up procedures
ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**	**2**	Fully defined external interfaces
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**	**2**	Security enforcing high-level design
	ADV_IMP				**1**	**2**	**3**	3	**2**	Implementation of the TSF
	ADV_INT					**1**	**2**	**3**		
	ADV_LLD				**1**	1	**2**	2	**1**	Descriptive low-level design
	ADV_RCR	**1**	1	1	1	**2**	2	**3**	**1**	Informal correspondence demonstration
	ADV_SPM				**1**	**3**	3	3	**1**	Informal TOE security policy model
AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1	**1**	Administrator guidance
	AGD_USR	**1**	1	1	1	1	1	1	**1**	User guidance
ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2	**1**	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD				**1**	**2**	2	**3**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**1**	Well-defined development tools
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**2**	2	**3**	**1**	Testing: high-level 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_CCA					**1**	**2**	2		
	AVA_MSU			**1**	**2**	2	**3**	3	**2**	Validation of analysis
	AVA_SOF		**1**	1	1	1	1	1	**1**	Strength of TOE security function evaluation
	AVA_VLA		**1**	1	**2**	**3**	**4**	4	**4**	Highly resistant

Annexe 2. Références documentaires du produit évalué

[DCSSI-2008_43]	Certificat DCSSI délivré le 19 décembre 2008 pour le produit carte à puce JCLX80jTOP20ID : Java Trusted Open Platform sur composant SLE66CLX800PE
[ST]	Cible de sécurité de référence pour l'évaluation : • jTOPv27-ASEv1 - Security Target - version 1.4 - CP-2008-RT-356
[RTE]	Rapport technique d'évaluation : • Evaluation Technical Report - ESCARPE Project - ESCARPE_ETR_v1.1 / 1.1 Pour les besoins d'évaluation en composition de l'applet avec la plate-forme, les documents suivants ont été pris en compte : • Evaluation Technical Report - ALCAZAR Project - ALCAZAR_ETR_v1.1, version 1.1 (rapport établi par le même évaluateur) ; • jTOPv27-ASEv1 - Composite Design Compliance - version 1.0 - CP-2008-RT-556
[CONF]	• JTOPv27 - ASEv1 - Configuration management plan - version 1.1 - CP-2008-RT-361 • Escarpe files - Escarpe files.txt
[GUIDES]	Guide d'administration du produit : • jTOPv27 - ASEv1 - Administration Guide - version 1.3 - CP-2008-RT-357 Guide d'utilisation du produit : • jTOPv27 - ASEv1 - User Guide - version 1.3 - CP-2008-RT-358

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, August 2005, version 2.3, ref CCMB-2005-08-001; Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002; Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003. Le contenu des Critères Communs version 2.3 est identique à celui de la Norme Internationale ISO/IEC 15408:2005.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. Le contenu de la CEM version 2.3 est identique à celui de la Norme Internationale ISO/IEC 18045:2005.
[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.
[AIS 34]	Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004, BSI (Bundesamt für Sicherheit in der Informationstechnik)