PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification DCSSI-2008/43

Carte à puce JCLX80jTOP20ID : Java Trusted Open Platform sur composant SLE66CLX800PE

Paris, le 19 décembre 2008

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-2008/43

Nom du produit

Carte à puce JCLX80jTOP20ID :
Java Trusted Open Platform
sur composant SLE66CLX800PE

Référence/version du produit

IFXv#27_0.1, révision de code v1.4

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 5 augmenté

ALC_DVS.2, AVA_VLA.4

Développeur(s)

Trusted Logic SA

5, rue du Bailliage 78000 Versailles – France

Commanditaire

Trusted Logic SA

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 :

- 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 JCLX80jTOP20ID : Java Trusted Open Platform sur composant SLE66CLX800PE**,** version IFXv#27_0.1, révision de code v1.4 **»** développée par Trusted Logic SA.

C'est une carte à puce bi-mode (contact/sans contact) comportant une plate-forme d'exécution d'applets Java Card conforme aux spécifications Java Card 2.2.1 et VISA GlobalPlatform 2.1.1 - configuration 2 standard, masquée sur le composant SLE66CLX800PE d'Infineon Technologies. Le patch v1.4 est chargé en EEPROM (*Electrically Erasable Programmable Read only Memory* – mémoire programmable en lecture seule et électriquement effaçable).

1.2. Description du produit évalué

La cible de sécurité [ST] (*Security Target*) définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

La cible de sécurité s'inspire du profil de protection [JCSPP][1]. Comme le mécanisme RMI (*Remote Method Invocation* - méthode d'invocation à distance) et l'utilisation de plusieurs *Logical Channels* (canaux logiques) ne sont pas inclus dans le périmètre de l'évaluation, la conformité à ce profil de protection n'est pas réclamée.

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	JCLX80jTOP20ID	Trusted Logic
Référence de la cible d'évaluation (label interne)	jTOP v#27.01_1.4	Trusted Logic
Réference de la cible d'évaluation (label du composant)	SLE66CLX800PE	Infineon
Référence du logiciel	IFXv#27_0.1, révision de code v1.4	Trusted Logic
Identifiant du composant	SLE66CLX800PE-m1581-e13/a14	Infineon

[1] **[JCSPP] Java Card System Standard 2.2.1 Configuration Protection Profile, (« Standard 2.2.1 du Système Carte Java, Profil de Protection de la Configuration »)**
Version 1.0b, août 2003, enregistré et certifié par la DCSSI sous la référence PP/0305.

Des échantillons de la TOE (*Target of Evaluation* – cible d'évaluation) ont été fournis pour les besoins d'évaluation. La TOE peut être identifiée de manière unique par lecture des octets d'ATR (*Answer To Reset* - réponse à la mise sous tension) :

- 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 version du masque : 14 (1.4 est la version courante du logiciel).

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).

Ces informations permettent de tracer tous les éléments constitutifs de la TOE (composant, masque matériel, patch logiciel). Elles permettent d'identifier correctement et de façon unique la TOE. Elles ont pu être vérifiées sur les versions successives de la TOE reçues lors de l'évaluation.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- Card Management
  - Issuer Security Domain
    - OPEN
    - Card Content Management
      - Card Content Loading
      - Card Content Installation
      - Card Content Deletion
    - Life Cycle Management
    - Administration Commands Control
  - Secure Channels
    - Host Authentication
    - Message Integrity and Authentication
    - Message Data Confidentiality
    - Secure Channel Termination
  - Secure Channel Key Management
    - Session Key Generation
    - ISD Key Loading and Replacement
  - Cardholder Verification Management
    - Global CVM
- Runtime Environment
  - Application Reference Monitors
    - Java Card Firewall
    - Defensive Java Card Virtual Machine
  - Security countermeasures
    - Card Muting
    - Card Locking
    - Card Termination
  - Life Cycle Management

        - Clearing sensitive information
        - Booting Tests
    - Integrity
        - Atomic Transactions
    - Service Availability
        - Resource Quotas
    - Cryptography
        - Signature Generation and Verification
        - Encryption and Decryption
        - Message Digest Generation
        - Random Number Generation
    - Key Management
        - Key Generation
        - Key Agreement
        - Key Encryption
        - Key Integrity
        - Key Destruction
    - Cardholder Authentication
        - Cardholder Verification
        - PIN Value Integrity
- Integrated Circuit TSFs
    - Operating State Checking
    - Phase Management
    - Protection Against Snooping
    - Hardware Data Encryption
    - True Random Number Generation
    - Hardware Self Test
    - Notification of Physical Attack
    - Memory Management Unit
    - Cryptographic Support

1.2.3. Architecture

L'évaluation porte sur un produit en composition, une carte à puce complète composée d'un système d'exploitation, incluant :

- le système Java Card 2.2.1 (carte java 2.2.1), c'est à dire :
    - JCVM (*Java Card Virtual Machine* - machine virtuelle carte java) ;
    - JCRE (*Java Card Runtime Environment* - environnement d'exécution de la carte java) ;
    - et JCAPI (*Java Card Application Program Interface* - interface du programme d'application de la carte java) ;
- et VISA GlobalPlatform 2.1.1 - configuration 2.

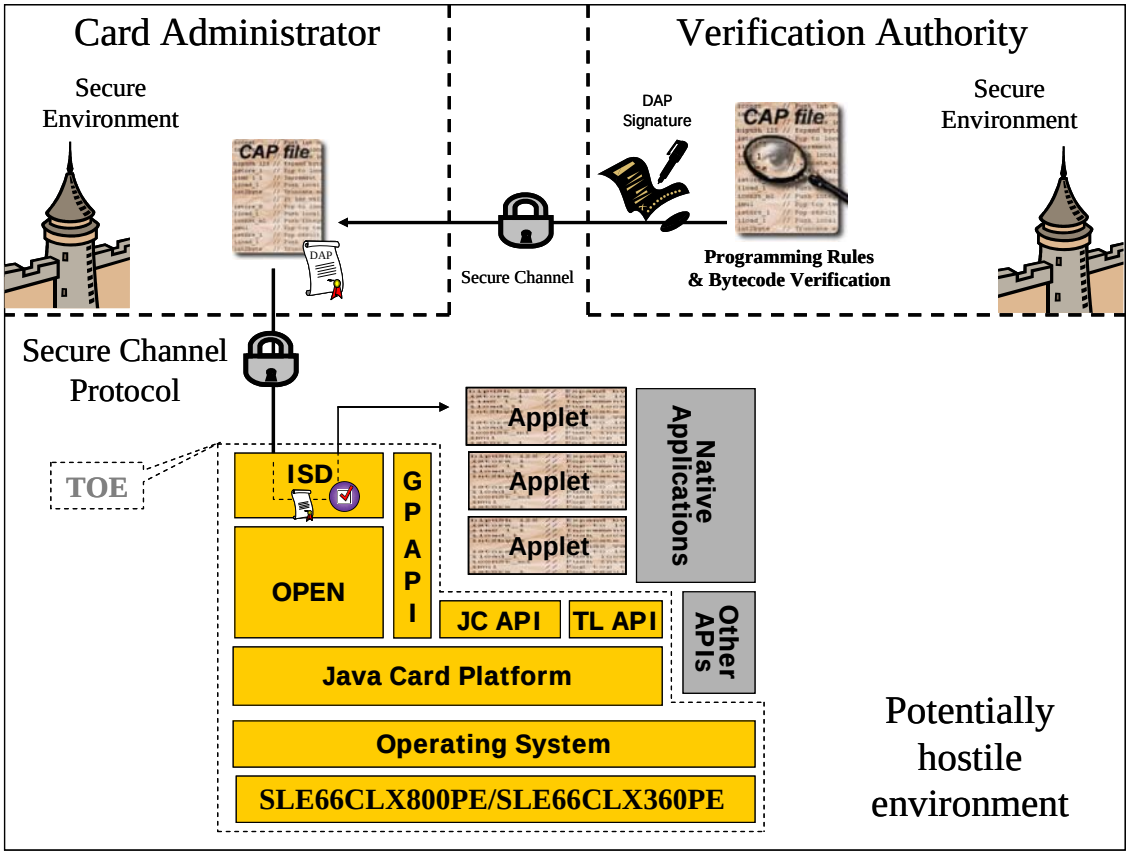
Le produit est masqué sur le microcontrôleur SLE66CLX800PE-m1581-e13/a14, qui a été certifié le 27 mai 2008 sous la référence BSI-DSZ-CC-0482[1].

[1] Ce certificat porte également sur le composant référencé SLE66CLX360PE-m1587-e13/a14 (se différenciant par une taille mémoire différente).

Le résultat de cette composition est une carte à puce de type plate-forme Java Card ouverte et sécurisée capable d'héberger des applications Java Card.

Les différentes opérations impliquées dans la gestion de ces applications sont accomplies conformément aux spécifications de VISA GlobalPlatform 2.1.1, configuration 2. Les opérations de gestion comprennent le téléchargement d'applications Java Card, leur installation, suppression, sélection en vue de leur exécution, la gestion du cycle de vie de la carte et des applications, et le partage d'un PIN (*Personal Identification Number* - code d'identification personnel) global commun à toutes les applications installées dans la carte.

Le schéma d'architecture global du produit est donné ci-après.



Les éléments suivants sont dans le périmètre de l'évaluation :

- Java Card 2.2.1 (excepté le RMI et les canaux logiques) ;
- VISA GlobalPlatform 2.1.1, configuration 2 ;
- des APIs Java Card propriétaires additionnelles (*util, security*) ;
- le cycle de vie de la TOE comprend les phases de conception et de développement du logiciel masqué. Les phases de conception et de fabrication du composant sont également couvertes en composition.

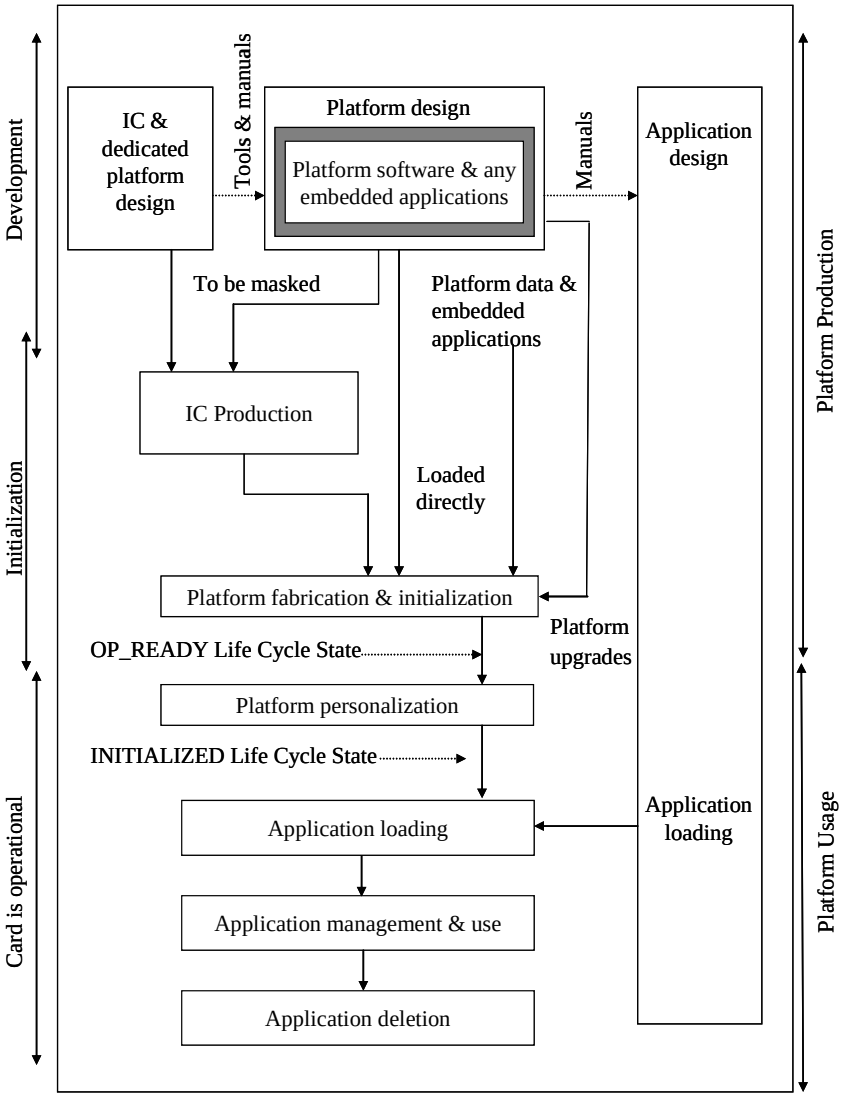
Les éléments suivants sont en dehors du périmètre de l'évaluation :

- le RMI ;
- les canaux logiques ;
- des APIs Java Card propriétaires additionnelles (*iso7816, math, sim*) ;
- toute application native qui pourrait être masquée dans le composant ;
- toute applet Java Card qui pourrait être chargée sur la plate-forme.

1.2.4. Cycle de vie

Comme précisé précédemment, le périmètre d´évaluation comprend les phases de conception et de développement du logiciel masqué (la phase de conception et de fabrication du composant étant couverte par l'évaluation du composant). C'est le bloc qui est intitulé « Platform design » dans la figure suivante qui représente tout le cycle de vie dans laquelle la cible d'évaluation s'inscrit.

Les phases d'initialisation et de personnalisation de la plate-forme sont en dehors du périmètre de l'évaluation. Les fonctions de sécurité de la TOE sont évaluées dans la Phase d´Utilisation (état SECURED du cycle de vie GlobalPlatform).



Le produit a été développé sur le site suivant :

Trusted Logic SA

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 [ADM] dans le chapitre Définitions.

En particulier, il est le représentant du *Card Issuer* (émetteur de la carte). Il a le contrôle total 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 terminer la carte, télécharger de nouvelles applets sur la carte, modifier les clés statiques de l'ISD (*Issuer Security Domain* - domaine de sécurité de l'émetteur) ou récupérer des informations d'administration de la carte.

Par ailleurs, l'évaluateur a considéré comme utilisateur du produit les *Application Developers* (développeurs d'applications) dont les responsabilités sont détaillées dans [USR].

1.2.5. Configuration évaluée

Le certificat porte sur la plate-forme Java Card seule, telle que présentée plus haut au paragraphe 1.2.3 Architecture, et configurée conformément au guide de personnalisation (Cf. [GUIDES]).

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 SDR], [CC IC], [CC AM], [CC AP], [COMP] des Critères Communs 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 microcontrôleur déjà certifié par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4 et conformément au profil de protection [PP0002].

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 9 décembre 2008, 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 a été analysée par la DCSSI. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] et donnent lieu aux conclusions suivantes : certains des mécanismes analysés n'atteignent pas le niveau standard défini dans le référentiel cryptographique de la DCSSI (Cf. [REF-CRY]).

L´analyse a identifié des faiblesses théoriques dans certains des mécanismes étudiés. Quoi qu'il en soit, 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 VLA visé.

2.4. Analyse du générateur d'aléas

Le produit dispose de deux générateurs de nombres aléatoires (notés SMRNG et APRNG).

Tous deux utilisent le TRNG (*True Randon Number Generator* - générateur matériel de nombres aléatoires) fourni par le composant. Ce TRNG a fait l'objet d'une évaluation selon la méthodologie [AIS 31]. Il atteint le niveau *Class P2 level High* lorsqu'il est utilisé en respectant les recommandations spécifiques décrites au chapitre 2 du [AN_RNG].

Le SMRNG est destiné aux seuls besoins du système d'exploitation. Les sorties de SMRNG ne sont pas disponibles ni pour les applications, ni pour l'utilisateur final de la carte, et ne sont pas utilisées pour des applications cryptographiques. L'analyse de SMRNG par la DCSSI s'est donc arrêtée lors de et à ce constat.

L'APRNG est destiné aux applications. Plus précisément, les données aléatoires générées, combinaison de TRNG et d'un post-traitement cryptographique, sont utilisées pour :

- la génération des clés ;
- compléter les données de certains protocoles ;
- les données aléatoires fournies par la classe RandomData (JavaCarD API).

L'APRNG a fait l'objet d'une analyse par la DCSSI qui indique qu'il est de niveau de robustesse standard.

En effet, cette analyse n'a pas permis de mettre en évidence de biais statistiques bloquant pour un usage direct des sorties des générateurs. Ceci ne permet pas d'affirmer que les données générées soient réellement aléatoires mais assure que le générateur ne souffre pas de défauts majeurs de conception. Comme énoncé dans le document [REF-CRY], il est rappelé que, pour un usage cryptographique, la sortie d'un générateur matériel de nombres aléatoires doit impérativement subir un retraitement algorithmique de nature cryptographique, même si l'analyse du générateur physique d'aléa n'a pas révélé de faiblesse.

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 JCLX80jTOP20ID : Java Trusted Open Platform sur composant SLE66CLX800PE**,** version IFXv#27_0.1, révision de code v1.4 **»** soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 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 spécifiés dans la cible de sécurité [ST] et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

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 :

[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.

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* (accord de reconnaissance Critères Communs) 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, 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 5+	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	**3**	Development tools 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**	**3**	Semiformal functional specification
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**	**3**	Semiformal high-level design
	ADV_IMP				**1**	**2**	**3**	3	**2**	Implementation of the TSF
	ADV_INT					**1**	**2**	**3**	**1**	Modularity
	ADV_LLD				**1**	1	**2**	2	**1**	Descriptive low-level design
	ADV_RCR	**1**	1	1	1	**2**	2	**3**	**2**	Semiformal correspondence demonstration
	ADV_SPM				**1**	**3**	3	3	**3**	Formal 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	**2**	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD				**1**	**2**	2	**3**	**2**	Standardised life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**2**	Compliance with implementation standards
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**2**	2	**3**	**2**	Testing: low-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	**1**	Covert channel analysis
	AVA_MSU			**1**	**2**	2	**3**	3	**2**	Analysis and testing of insecure states
	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

[ST]	Cible de sécurité de référence pour l'évaluation : • JCLX80jTOP20ID/JCLX36jTOP20ID - Security Target - version 1.8 (la référence Développeur est CP-2006-RT-389) Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : • JCLX80jTOP20ID/JCLX36jTOP20ID - Security Target Lite - version 1.4 (la référence Développeur est CP-2007-RT-075)
[RTE]	Rapport technique d'évaluation : • Evaluation Technical Report - ALCAZAR project, ALCAZAR_ETR_v1.1 Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : • ETR-LITE FOR COMPOSITION (ETR-LITE), v1.0, 2008.03.11, (la référence Développeur est 0482_ETRcomp_080311_v1) o SLE66CLX800PE / m1581-e13/a14 o SLE66CLX800PEM / m1580-e13/a14 o SLE66CLX800PES / m1582-e13/a14 o SLE66CX800PE / m1599-e13/a14 o SLE66CLX360PE / m1587-e13/a14 o SLE66CLX360PEM / m1588-e13/a14 o SLE66CLX360PES / m1589-e13/a14 o SLE66CLX180PE / m2080-a14 o SLE66CLX180PEM / m2081-a14 o SLE66CLX120PE / m2082-a14 o SLE66CLX120PEM / m2083-a14 o all optional with RSA2048 V1.5 and ECC V1.1 Certification ID: 8103819623 / BSI-DSZ-CC-0482
[ANA-CRY]	Cotation de mécanismes cryptographiques, 847/SGDN/DCSSI/SDS/Crypto, 18/04/2008
[CONF]	Plan de gestion de la configuration du logiciel (référence [ACM] dans [RTE]): • JCLX80jTOP20ID Software Configuration Management Plan - version 1.2 (la référence Développeur est CP-2007-RT-017) Liste de configuration (référence [LIS] dans [RTE]) : • Configuration list - version 0.5 (la référence Développeur est CVS-Files-Versions.txt /CVS-Repositories-Architectures.txt / SVN-Files-Versions.txt)

[GUIDES]	Guide d'administration du produit (référence [ADM] dans [RTE]) : • JCLX80jTOP20ID Administration Guide, version 1.2 (la référence Développeur est CP-2007-RT-165) Guide d'utilisation du produit (référence [USR] dans [RTE]) : • JCLX80jTOP20ID Common Criteria User Guide, version 1.1, (la référence Développeur est CP-2007-RT-166)
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0002-2001.
[AN_RNG]	Application Note : Security & Chip Card Ics SLE 66CxxxP and SLE 66CxxxPE Testing the Random Number Generator non-AIS-31 and AIS-31 compliant, version 11.2004 (la référence Développeur est CAN_SLE66CxxxP_PE_RNG_2004_11)

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.
[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.
[REF-CRY]	Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, version 1.10 du 19 décembre 2006, réf: 2741/SGDN/DCSSI/SDS/Crypto.

[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)
[AIS 31]	Functionnality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25 September 2001, BSI (Bundesamt für Sicherheit in der Informationstechnik)