PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2006/08

Java Card Open Platform (référence T100921)

Paris, le 10 mai 2006.

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 le centre de certification, et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Synthèse

Rapport de certification 2006/08

Java Card Open Platform (référence T100921)

Développeurs : Axalto, Infineon

Critères Communs version 2.2

EAL4 Augmenté
(ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4)

conforme au profil de protection PP/0305

Commanditaire : Axalto

Centre d'évaluation : Serma Technologies

Les augmentations suivantes ne sont pas reconnues dans le cadre du CC RA :
ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4

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 publiques et disponibles en français sur le site Internet :
www.ssi.gouv.fr

Accords de reconnaissance des certificats

L'accord de reconnaissance européen du SOG-IS de 1999 permet la reconnaissance entre les Etats signataires de l'accord[1], des certificats délivrés par leur autorité de certification. La reconnaissance mutuelle 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 :

La direction centrale de la sécurité des systèmes d'information passe aussi des accords de reconnaissance avec des organismes étrangers homologues ayant leur siège en dehors des Etats membres de l'Union européenne. Ces accords peuvent prévoir que les certificats délivrés par la France sont reconnus par les Etats signataires. Ils peuvent prévoir aussi que les certificats délivrés par chaque partie sont reconnus par toutes les parties. (article 9 du décret 2002-535)
Ainsi, l'accord Common Criteria Recognition Arrangement permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance mutuelle 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] En avril 1999, les pays signataires de l'accord SOG-IS sont : le Royaume-Uni, l'Allemagne, la France, l'Espagne, l'Italie, la Suisse, les Pays-Bas, la Finlande, la Norvège, la Suède et le Portugal.
[2] En mai 2005, les pays émetteurs de certificats signataires de l'accord sont : la France, l'Allemagne, le Royaume-Uni, les Etats-Unis, le Canada, l'Australie-Nouvelle Zélande et le Japon ; les pays signataires de l'accord qui n'émettent pas de certificats sont : l'Autriche, l'Espagne, la Finlande, la Grèce, la Hongrie, Israël, l'Italie, la Norvège, les Pays-Bas, la Suède, la Turquie, la République Tchèque, Singapour et l'Inde.

Table des matières

1. Le produit évalué

1.1. Identification du produit

Le produit évalué est la carte Java Card Open Platform (référence T100921) développée par Axalto et Infineon. Ce produit est commercialisé sous deux noms différents : ICitizen Open v2 et Cyberflex Access 64k v3.

1.2. Développeurs

Axalto

36 rue de la Princesse
78431 Louveciennes Cedex
France

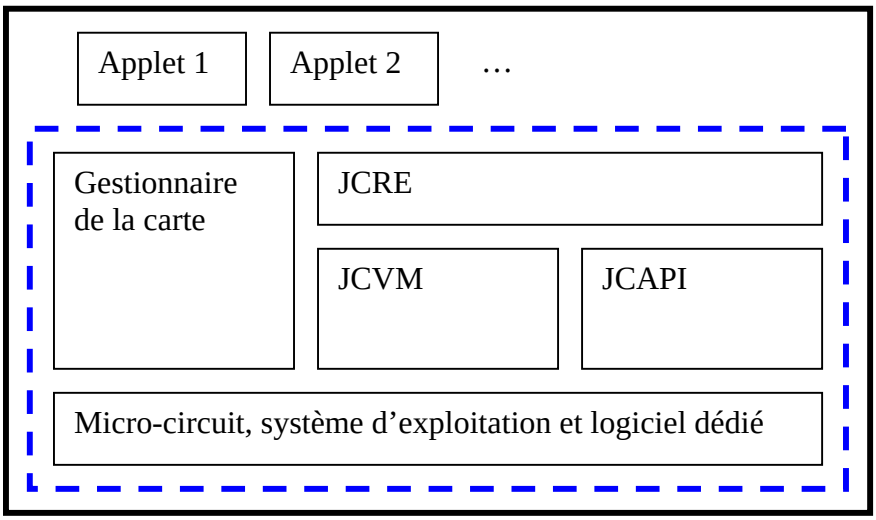
Infineon Technologies AG

Security & Chipcard ICs
P.O. Box 80 09 49
81609 München
Allemagne

1.3. Description du produit évalué

1.3.1. Architecture

Le produit est constitué du micro-circuit Infineon SLE66CX680PE/m1534a13 et de ses librairies, du système d'exploitation GEOS (Generic Operating System), du gestionnaire de la carte et de la plate-forme Java Card. La plate-forme Java Card comprend le JCRE (Java Card Runtime Environment), le JCVM (Java Card Virtual Machine) et le JCAPI (Java Card Application Programming Interface).



Limites de la cible d'évaluation
Limites de la carte

1.3.2. Cycle de vie

Le cycle de vie du produit est le suivant :

1. phase 1 : développement du masque (GEOS, JCVM) par Axalto ;
2. phase 2 : développement du micro-circuit par Infineon ;
3. phase 3 : fabrication du composant masqué et tests par Infineon ;
4. phase 4 : mise en micro-module, encartage et tests par Axalto ;
5. phase 5 : pré-personnalisation ;
6. phase 6 : personnalisation et gestion des applets (chargement, installation, suppression, extradition) par l'émetteur ;
7. phase 7 : utilisation et gestion des applets (chargement, installation, suppression, extradition) par l'émetteur et/ou le fournisseur de services.

1.3.3. Périmètre et limites du produit évalué

Le produit évalué comprend les éléments suivants :

- le micro-circuit Infineon SLE66CX680PE/m1534a13 ;
- la librairie RMS version 2.5 ;
- la librairie RSA2048 version 1.4 ;
- le ROM mask SB 147 ;
- le logiciel CENTAUR version 1.0.

Les éléments suivants ne font donc pas partie du périmètre d'évaluation :

- les applets chargées dans les phases de personnalisation et d'utilisation ;
- la carte plastique et ses attributs (hologrammes, bande magnétique, impressions diverses).

2. L'évaluation

2.1. Contexte

L'évaluation a été effectuée selon le schéma de composition défini dans le document [COMP]. La composition consiste à réaliser l'évaluation d'un composant masqué en évaluant d'une part le micro-circuit, et d'autre part la partie logicielle en vérifiant qu'aucune faiblesse n'est introduite par l'intégration du logiciel sur le micro-circuit.

Cette évaluation a été réalisée sur la base des résultats de l'évaluation du micro-circuit SLE66CX680PE/m1534a13 au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, conformément au profil de protection « Smartcard IC Platform Protection Profile » [PP/SSVG]. Ce micro-circuit a été certifié le 14 septembre 2005 sous la référence BSI-DSZ-CC-0322-2005 [RC_IC].

2.2. Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [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 et validées par la DCSSI ont été utilisées.

2.3. Commanditaire

Axalto

36 rue de la Princesse
78431 Louveciennes Cedex
France

2.4. Centre d'évaluation

Serma Technologies

30 avenue Gustave Eiffel
33608 Pessac
France

Téléphone : +33 (0)5 57 26 08 64

Adresse électronique : m.dus@serma.com

2.5. Rapport technique d'évaluation

L'évaluation s'est déroulée du 14 mars 2005 au 5 mai 2006.

Le rapport technique d'évaluation [RTE] détaille les travaux menés par l'évaluateur et présente les résultats obtenus. Les sections suivantes récapitulent les principaux aspects évalués.

2.6. Evaluation de la cible de sécurité

La cible de sécurité [ST] définit le produit évalué et son environnement d'exploitation.
Cette cible de sécurité est conforme au profil de protection PP/0305 [PP/0305].

Pour les tâches d'évaluation de la cible de sécurité, les verdicts suivants ont été émis par l'évaluateur :

Classe ASE: Evaluation d'une cible de sécurité		**Verdicts**
ASE_DES.1	TOE description	Réussite
ASE_ENV.1	Security environment	Réussite
ASE_INT.1	ST introduction	Réussite
ASE_OBJ.1	Security objectives	Réussite
ASE_PPC.1	PP claims	Réussite
ASE_REQ.1	IT security requirements	Réussite
ASE_SRE.1	Explicitly stated IT security requirements	Réussite
ASE_TSS.1	Security Target, TOE summary specification	Réussite

2.7. Evaluation du produit

2.7.1. Les tâches d'évaluation

Les tâches d'évaluation réalisées correspondent au niveau d'évaluation EAL4[1] augmenté. Le tableau suivant précise les augmentations sélectionnées :

Composants d'assurance	
EAL4	Methodically designed, tested, and reviewed
+ ADV_IMP.2	Implementation of the TSF
+ ALC_DVS.2	Sufficiency of security measures
+ AVA_MSU.3	Analysis and testing for insecure state
+ AVA_VLA.4	Highly resistant

2.7.2. L'évaluation de l'environnement de développement

Le produit est développé sur le site de :

Axalto

36 rue de la Princesse
78431 Louveciennes Cedex
France

[1] Annexe 2 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].

L'évaluateur a analysé le plan de gestion de configuration fourni par le développeur qui précise l'utilisation du système de gestion de configuration. Le système permet de générer notamment la liste de configuration [CONF] qui identifie tous les éléments gérés par le système.

Des procédures de génération permettent par ailleurs de s'assurer que les bons éléments sont utilisés pour générer le produit évalué.

La vérification de l'application des procédures analysées a été effectuée lors d'une visite du site de Axalto à Louveciennes. (cf Annexe 1)

Pour les tâches d'évaluation liées à l'environnement de développement, les verdicts suivants ont été émis par l'évaluateur :

Classe ACM: Gestion de configuration		**Verdicts**
ACM_AUT.1	Partial CM automation	Réussite
ACM_CAP.4	Generation support and acceptance procedures	Réussite
ACM_SCP.2	Problem tracking CM coverage	Réussite
Classe ALC: Support au cycle de vie		**Verdicts**
ALC_DVS.2	Sufficiency of security measures	Réussite
ALC_LCD.1	Developer defined life-cycle model	Réussite
ALC_TAT.1	Well-defined development tools	Réussite

2.7.3. L'évaluation de la conception du produit

L'analyse des documents de conception a permis à l'évaluateur de s'assurer que les exigences fonctionnelles identifiées dans la cible de sécurité et listées ci-après sont correctement et complètement raffinées dans les niveaux suivants de représentation du produit : spécifications fonctionnelles (FSP), conception de haut-niveau (HLD), conception de bas-niveau (LLD), implémentation (IMP).

Les exigences fonctionnelles identifiées dans la cible de sécurité sont les suivantes :

- Security alarms (FAU_ARP.1) ;
- Cryptographic key generation (FCS_CKM.1) ;
- Cryptographic key distribution (FCS_CKM.2) ;
- Cryptographic key access (FCS_CKM.3) ;
- Cryptographic key destruction (FCS_CKM.4) ;
- Cryptographic operation (FCS_COP.1) ;
- Enforced proof of origin (FCO_NRO.2) ;
- Subset access control (FDP_ACC.1) ;
- Complete access control (FDP_ACC.2) ;
- Security attributes based access control (FDP_ACF.1) ;
- Subset information flow control (FDP_IFC.1) ;
- Complete information flow control (FDP_IFC.2) ;
- Simple security attributes (FDP_IFF.1) ;
- Import of user data with security attributes (FDP_ITC.2) ;
- Basic rollback (FDP_ROL.1) ;
- Subset residual information protection (FDP_RIP.1) ;
- Stored data integrity monitoring and action (FDP_SDI.2) ;

- Data exchange integrity (FDP_UIT.1) ;
- User attribute definition (FIA_ATD.1) ;
- Timing of identification (FIA_UID.1) ;
- User identification before any action (FIA_UID.2) ;
- User-subject binding (FIA_USB.1) ;
- Management of security attributes (FMT_MSA.1) ;
- Secure security attributes (FMT_MSA.2) ;
- Static attribute initialisation (FMT_MSA.3) ;
- Management of TOE security functions data (FMT_MTD.1) ;
- Secure TSF data (FMT_MTD.3) ;
- Revocation (FMT_REV.1) ;
- Specification of management functions (FMT_SMF.1) ;
- Security management roles (FMT_SMR.1) ;
- Unobservability (FPR_UNO.1) ;
- Abstract machine testing (FPT_AMT.1) ;
- Failure with preservation of secure state (FPT_FLS.1) ;
- Resistance to physical attack (FPT_PHP.3) ;
- Automated recovery without undue loss (FPT_RCV.3) ;
- Function recovery (FPT_RCV.4) ;
- Non-bypassability of the TSP (FPT_RVM.1) ;
- TSF domain separation (FPT_SEP.1) ;
- Inter-TSF basic TSF data consistency (FPT_TDC.1) ;
- TSF testing (FPT_TST.1) ;
- Degraded fault tolerance (FRU_FLT.1) ;
- Maximum quotas (FRU_RSA.1) ;
- Inter-TSF trusted channel (FTP_ITC.1).

Pour les tâches d'évaluation liées à la conception du produit, les verdicts suivants ont été émis par l'évaluateur :

Classe ADV: Développement		**Verdicts**
ADV_SPM.1	Informal TOE security policy model	Réussite
ADV_FSP.2	Fully defined external interfaces	Réussite
ADV_HLD.2	Security enforcing high-level design	Réussite
ADV_LLD.1	Descriptive low-level design	Réussite
ADV_IMP.2	Implementation of the TSF	Réussite
ADV_RCR.1	Informal correspondence demonstration	Réussite

2.7.4. L'évaluation des procédures de livraison et d'installation

L'évaluateur a analysé les procédures de livraison du produit entre d'une part le site de fabrication du micro-circuit (Infineon) et le site de développement de la carte (Axalto) et d'autre part entre ce dernier site et le site de personnalisation de la carte.

Ces procédures permettent de connaître l'origine de la livraison et de détecter une modification du produit au cours de cette livraison.

L'installation du produit correspond aux phases d'encartage et de personnalisation (phases 4, 5 et 6). Les procédures analysées [INSTALL] permettent d'obtenir la configuration évaluée du produit.

Pour les tâches d'évaluation liées aux procédures de livraison et d'installation, les verdicts suivants ont été émis par l'évaluateur :

Classe ADO: Livraison et exploitation		Verdicts
ADO_DEL.2	Detection of modification	Réussite
ADO_IGS.1	Installation, generation, and start-up procedures	Réussite

2.7.5. L'évaluation de la documentation d'exploitation

Pour l'évaluation, l'évaluateur a considéré comme administrateurs du produit le personnalisateur, l'émetteur et le fournisseur de services et comme utilisateurs les utilisateurs finaux de la carte et les applets.

L'évaluateur a analysé les guides d'administration et d'utilisation [GUIDES] pour s'assurer qu'ils permettent d'exploiter le produit évalué d'une manière sécurisée.

Pour les tâches d'évaluation liées à la documentation d'exploitation, les verdicts suivants ont été émis par l'évaluateur :

Classe AGD: Guides		Verdicts
AGD_ADM.1	Administrator guidance	Réussite
AGD_USR.1	User guidance	Réussite

2.7.6. L'évaluation des tests fonctionnels

L'évaluateur a analysé la documentation des tests réalisés par le développeur pour s'assurer que toutes les fonctionnalités du produit listées dans la cible de sécurité ont bien été testées.

L'évaluateur a également réalisé des tests fonctionnels pour s'assurer, de manière indépendante, du fonctionnement correct du produit évalué. L'évaluateur a réalisé ses tests fonctionnels indépendants sur des cartes identifiées au paragraphe 1.1 et en utilisant un émulateur du micro-circuit fourni par Infineon.

Pour les tâches d'évaluation liées aux tests fonctionnels, les verdicts suivants ont été émis par l'évaluateur :

Classe ATE: Tests		Verdicts
ATE_COV.2	Analysis of coverage	Réussite
ATE_DPT.1	Testing: high-level design	Réussite
ATE_FUN.1	Functional testing	Réussite
ATE_IND.2	Independent testing - sample	Réussite

2.7.7. L'évaluation des vulnérabilités

L'évaluateur s'est assuré que la documentation fournie avec le produit [INSTALL] [GUIDES] est suffisamment claire pour éviter des erreurs d'exploitation qui pourraient mener à un état non sûr du produit.

Seules la fonction de ratification du PIN a fait l'objet d'une estimation du niveau de résistance intrinsèque. Le niveau de résistance de ces fonctions est jugé élevé.

En s'appuyant sur une analyse de vulnérabilités réalisée par le développeur et sur toutes les informations qui lui ont été livrées dans le cadre de l'évaluation, l'évaluateur a réalisé sa propre analyse indépendante pour estimer les vulnérabilités potentielles du produit. Cette analyse a été complétée par des tests sur des cartes identifiées au paragraphe 1.1.

L'analyse réalisée par l'évaluateur n'a pas permis de démontrer l'existence de vulnérabilités exploitables pour le niveau visé. Le produit peut donc être considéré comme résistant à des attaques de niveau élevé.

Pour les tâches d'évaluation liées aux vulnérabilités, les verdicts suivants ont été émis par l'évaluateur :

Classe AVA : Estimation des vulnérabilités		**Verdicts**
AVA_MSU.3	Analysis and testing for insecure state	Réussite
AVA_SOF.1	Strength of TOE security function evaluation	Réussite
AVA_VLA.4	Highly resistant	Réussite

2.7.8. L'analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques a été analysée par la DCSSI. Les résultats obtenus ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur.

Le produit évalué offre en outre plusieurs services cryptographiques. Ces services ne peuvent cependant pas être analysés d'un point de vue cryptographique car ils ne concourent pas à la sécurité propre du produit ; leur résistance dépend de leur emploi par l'application embarquée sur le produit.

2.7.9. L'analyse du générateur d'aléas

Le produit évalué offre un générateur d'aléas qui peuvent être utilisés par le logiciel embarqué. Ce générateur a fait l'objet d'une analyse par la DCSSI.

Cette analyse n'a pas permis de mettre en évidence de biais statistiques élémentaires. Ceci ne permet pas de dire que les données générées sont réellement aléatoires mais assure que le générateur ne souffre pas de défaut majeur de conception.

3. La certification

3.1. Conclusions

L'ensemble des travaux réalisés par le centre d'évaluation et décrits dans le rapport technique d'évaluation [RTE] permet la délivrance d'un certificat conformément au décret 2002-535.
Ce certificat atteste que l'exemplaire du produit soumis à évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST]. Il atteste également que l'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises. (Art. 8 du décret 2002-535)

3.2. Restrictions d'usage

Les conclusions de l'évaluation ne sont valables que pour le produit spécifié au chapitre 1 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation résumés ci-dessous et suivre les recommandations se trouvant dans les guides fournis [INSTALL] [GUIDES] :

- les applets chargées après l'émission de la carte ne doivent pas contenir de méthodes natives ;
- les codes opération doivent être vérifiés afin d'en vérifier leur validité avant d'être chargé.

3.3. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

3.4. Reconnaissance internationale (CC RA)

Ce certificat est émis dans les conditions de l'accord du CC RA [CC RA]. Toutefois, les augmentations suivantes n'entrent pas dans le cadre de l'accord : ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4.

Annexe 1. Visite du site de développement de la société Axalto à Louveciennes

Le site de développement de la société Axalto situé à Louveciennes, a fait l'objet d'une visite par l'évaluateur le 8 novembre 2005 pour s'assurer de l'application des procédures de gestion de configuration, de support au cycle de vie et de livraison, pour le produit Java Card Open Platform (référence T100921).

Ces procédures ont été fournies et analysées dans le cadre des tâches d'évaluation suivantes :

- ACM_AUT.1 et ACM_CAP.4 ;
- ALC_DVS.2 ;
- ADO_DEL.2.

Un rapport de visite [Visite] a été émis par l'évaluateur.

Annexe 2. Niveaux d'assurance prédéfinis EAL

Classe	Famille	Composants par niveau d'assurance						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Classe ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Classe ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Classe ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	**3**
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Classe AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Classe ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Classe ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Classe AVA Estimation des vulnérabilités	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Annexe 3. Références documentaires du produit évalué

[CONF]	CENTAUR Platform: Configuration List, référence LIS_D1022401, révision 1.2 du 3 mai 2006.
[GUIDES]	• CENTAUR platform : Administrator manual, référence AGD_D1018916, révision 1.2. • CENTAUR platform : User manual, référence AGD_D1018917, révision 1.5. • FU Manage Java CardTM 2.2.1 API, référence LVRDSTG033085, révision 1.5. • FU Manage VOP2.0.1' Java API, référence MRD06STG013025, révision 1.2. • FU Manage GP2.1.1 Java API, référence LVRDSTG033080, révision 1.1. • FU Manage Java API Extensions, référence LVRDSTG053110, révision 1.0. • FU Manage ISO SM Java API, référence LVRDSTG043102, révision 1.0. • FU Manage File System Java API, référence LRD13STG053004, révision 1.0.
[INSTALL]	Centaur Installation, Generation and Start-up, référence IGS_D1022420, révision 1.0.
[RTE]	Evaluation Technical Report – Centaur platform, référence CENTAUR_ETR_V1.1.fm du 02/05/06.
[ST]	• CENTAUR Platform: Security Target, référence D_1018903, révision 1.5 du 4 mai 2006. • CENTAUR JAVACARD OPEN PLATFORM – ICitizen Open v2 – Cyberflex Access 64k v3, référence ST_D1018903.
[Visite]	Evaluation report – Classes ACM, ADO, ALC, Annex A, référence CENTAUR_ACM-ALC-ADO_v2.0.fm du 2 février 2006.
[PP/JCS]	Profil de protection « JavaCard System Standard 2.2 Configuration », version 1.0b, référence PP/0305.
[PP/SSVG]	Profil de protection « Smartcard Integrated Circuit Protection Profile V1.0 », référence BSI-PP-0002.
[RC_IC]	Rapport de certification « Infineon Smart Card IC (Security Controller) SLE66CX680PE/m1534a13 and SLE66CX360PE/m1536a13 both with RSA 2048 V1.4 and specific IC Dedicated Software », référence BSI-DSZ-CC-0322-2005 du 14 septembre 2005.

Annexe 4. 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, January 2004, version 2.2, ref CCIMB-2004-01-001; Part 2: Security functional requirements, January 2004, version 2.2, ref CCIMB-2004-01-002; Part 3: Security assurance requirements, January 2004, version 2.2, ref CCIMB-2004-01-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, January 2004, version 2.2, ref CCIMB-2004-01-004.
[CC IC]	Common Criteria supporting documentation - The Application of CC to Integrated Circuits, version 1.2, July 2000.
[CC AP]	Common Criteria supporting documentation - Application of attack potential to smart-cards, version 1.1, July 2002.
[COMP]	Common Criteria supporting documentation – ETR-lite for composition: Annex A - Composite smartcard evaluation : Recommended best practice, Version 1.2, March 2002.
[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.

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.pm.gouv.fr