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-PP-2010/07 du profil de protection « Java Card™ System Closed Configuration » (PP-JCS-Closed-v2.6 du 25 août 2010)

Paris, le 16 Dec. 10

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

[ORIGINAL SIGNE]

Avertissement

Ce rapport atteste la conformité de la version évaluée du profil de protection aux critères d'évaluation.
Un profil de protection est un document public qui définit, pour une catégorie de produits, un ensemble d'exigences et d'objectifs de sécurité, indépendants de leur technologie et de leur implémentation, qui satisfont les besoins de sécurité communs à un groupe d'utilisateurs.

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

Référence du rapport de certification **ANSSI-CC-PP-2010/07**
Nom du profil de protection ***Java Card™ System Closed Configuration***
Référence/version du profil de protection **PP-JCS-Closed-v2.6 du 25 août 2010**
Conformité à u profil de protection **Néant**
Critères d'évaluation et version **Critères Communs version 3.1, révision 3**
Niveau d'évaluation imposé par le PP **EAL 4 augmenté** **ALC_DVS.2, AVA_VAN.5**
Rédacteur(s) **Trusted Labs SAS** **5 rue du Bailliage, 78000 Versailles, France**
Commanditaire **SUN Microsystems, Inc** **4150 Network Circle, Santa Clara, CA 95054, USA**
Centre d'évaluation **Silicomp-AQL** **1 rue de la châtaigneraie, CS 51766, 35513 Cesson Sévigné Cedex, France** **Tél : +33 (0)2 99 12 50 00, mél : cesti@aql.fr**
Accords de reconnaissance applicables **CCRA** **SOG-IS**

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

Table des matières

1. Présentation du profil de protection

1.1. Identification du profil de protection

Titre : *Java Card™ System Protection Profile Open Configuration*
Référence, version : PP-JCS-Closed-v2.6
Date : 25 août 2010

1.2. Rédacteur

Ce profil de protection a été rédigé par Trusted Labs S.A.S pour le compte de Sun Microsystems, Inc :

Trusted Labs SAS

5 rue du Bailliage
78000 Versailles
France

Sun Microsystems, Inc

4150 Network Circle
Santa Clara, CA 95054
Etats Unis

1.3. Description du profil de protection

Ce [PP] répond au besoin de disposer d'un ensemble d'exigences de sécurité pour les plates-formes Java Card conformes aux versions 2.2.x et 3.0 Classic Edition des spécifications Java Card et ne supportant pas le téléchargement d'applets Java Card après émission de la carte (plates-formes dites « fermées »).

Ce [PP] remplace le profil de protection *Java Card System Minimal Configuration Version 1.0b Protection Profile* [PP-JCS], conforme aux Critères Communs v2.1, qui a été certifié par l'ANSSI sous la référence PP/0303 le 30 septembre 2003.

Ce [PP] requiert une conformité démontrable.

1.3.1. Généralités sur les plates-formes Java Card

La plate-forme Java Card

La plate-forme *Java Card* (JCP)[1]est constituée de la plate-forme du microcircuit (SCP)[2], du Système *Java Card* (JCS)[3] et de code natif s'exécutant au-dessus du SCP (cf. figure 1).
Le JCS est composé des éléments suivants : le Java Card Runtime Environment (JCRE), la

[1] *Java Card Platform.*
[2] *Smart Cart Platform.*
[3] *Java Card System.*

Java Card Virtual Machine (JCVM) et les API Java Card (JCAPI) (cf. figure 2).
Il permet à plusieurs applications (applets) d'être chargées sur une même carte à puce et assure l'interopérabilité de ces applications entre deux cartes à puce différentes (une même application peut fonctionnellement être exécutée sur deux plates-formes différentes).
En termes de sécurité, une plate-forme *Java Card* a pour principal objectif de contrer les accès ou les modifications non autorisées du code source des applications et des données sensibles (clés, code PIN, données biométriques, …).
Pour atteindre cet objectif, le JCS fournit des services de sécurité comme le mécanisme d'installation et d'effacement sécurisé, le mécanisme de « firewall », des API dédiés à la fourniture de services de sécurité, etc.

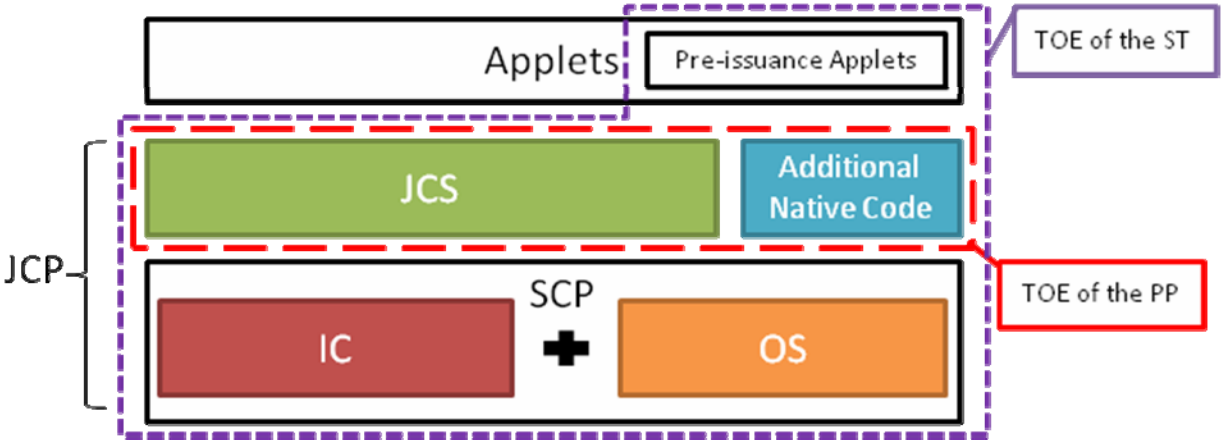

Figure 1 – Plate-forme Java Card (JCP)

Les applets

Les applications sont écrites en langage *Java Card*.
Les étapes de développement et de chargement d'une application sont les suivantes :

- développement du code source de l'application ;
- compilation du code source, qui devient un fichier class ;
- ce dernier fichier est traité par un convertisseur (converter), validant le code et générant un fichier *converted applet* (CAP) (l'équivalent d'un fichier class en programmation Java). Le fichier CAP contient une représentation binaire et exécutable des classes du paquetage (*package*, ensemble de *classes* et d'*interfaces*, représentant dans le contexte *Java Card*, soit une bibliothèque de fonctions utilisateur, soit une ou plusieurs applets) ;
- le fichier CAP est ensuite vérifié par un vérificateur de code (*bytecode verifier*, ie *off-card verifier*), avant d'être chargé de façon sécurisée (garantie de l'intégrité du fichier) sur la plate-forme ;
- le fichier est ensuite lié (*linked*) puis installé (*installed*). Pendant cette dernière phase, l'applet est enregistrée sur la carte par un numéro d'identification (AID – *Application IDentifier*) qui permettra d'identifier de manière unique l'instance de l'applet sur la carte (par exemple pour la sélection de l'applet, préalablement à son exécution).

L'exécution de l'applet est effectuée par l'interpréteur (*bytecode interpreter*) présent sur la carte.

1.3.2. Périmètre du profil de protection

La cible d'évaluation (TOE *Target Of Evaluation*) définie dans le profil de protection [PP] est constituée, comme précisé sur la figure 1, du JCS (*Java Card System*), conforme aux spécifications *Java Card Spécifications versions 2.2.x ou 3 Classic Edition*, ainsi que du code natif.
Elle est entièrement logicielle et ne contient aucune partie matérielle.
Comme précisé en §1.3.1, le JCS sert de support aux applets, et interagit avec le SCP et le gestionnaire de carte (*Card Manager*).

Néanmoins, toute évaluation de produit qui se voudrait conforme à ce [PP] devra prendre en compte l'ensemble des éléments de la plate-forme *Java Card*, comme représenté sur la figure 1 (TOE de la cible de sécurité).

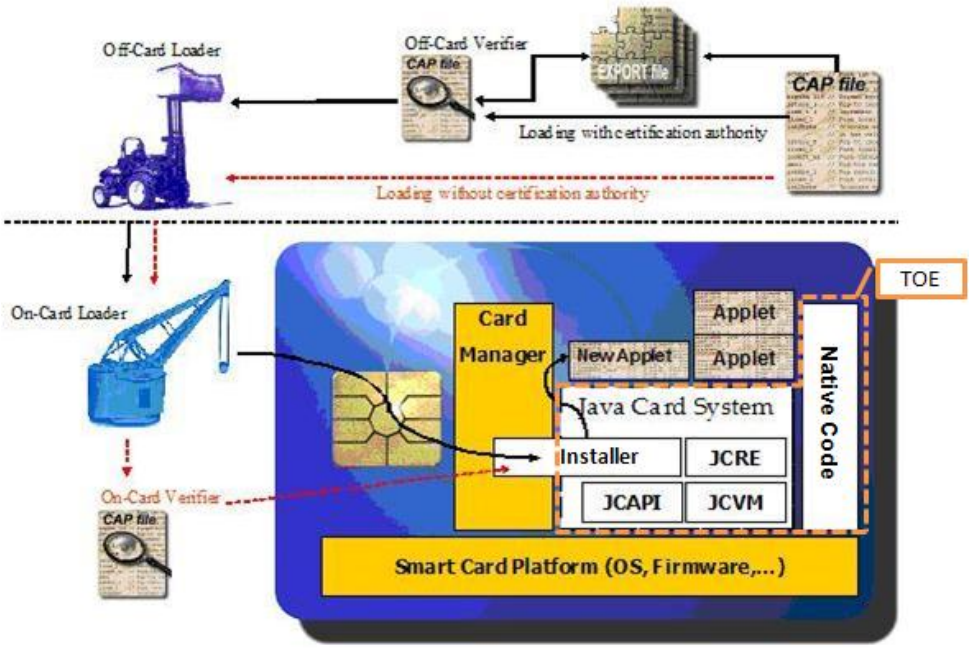

Figure 2 – Système Java Card et environnement d'installation

1.4. Exigences fonctionnelles

Les **exigences fonctionnelles de sécurité** définies par le profil de protection 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) ;
- Complete access control (FDP_ACC.2) ;
- Security attribute based access control (FDP_ACF.1) ;
- Subset information flow control (FDP_IFC.1) ;

- Simple security attributes (FDP_IFF.1) ;
- Subset residual information protection (FDP_RIP.1) ;
- Basic rollback (FDP_ROL.1) ;
- Stored data integrity monitoring and action (FDP_SDI.2) ;
- User attribute definition (FIA_ATD.1) ;
- User identification before any action (FIA_UID.2) ;
- User-subject binding (FIA_USB.1) ;
- Management of TSF data (FMT_MTD.1) ;
- Secure TSF data (FMT_MTD.3) ;
- Management of security attributes (FMT_MSA.1) ;
- Secure security attributes (FMT_MSA.2) ;
- Static attribute initialisation (FMT_MSA.3) ;
- Specification of Management Functions (FMT_SMF.1) ;
- Security roles (FMT_SMR.1) ;
- Unobservability (FPR_UNO.1) ;
- Failure with preservation of secure state (FPT_FLS.1) ;
- Inter-TSF basic TSF data consistency (FPT_TDC.1) ;

Toutes les exigences fonctionnelles du profil de protection sont extraites de la partie 2 des Critères Communs [CC].

1.5. Exigences d'assurance

Le niveau d'assurance exigé par le profil de protection est le niveau **EAL4 augmenté des composants d'assurance suivants**[1] :

Composants	Descriptions
ALC_DVS.2	*Sufficiency of security measures*
AVA_VAN.5	*Advanced methodical vulnerability analysis*

Tableau 1 - Augmentations

Toutes les exigences d'assurance imposées par le profil de protection sont extraites de la partie 3 des Critères Communs [CC].

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

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

2.2. Commanditaire

Sun Microsystems, Inc

4150 Network Circle
Santa Clara, CA 95054
Etats Unis

2.3. Centre d'évaluation

Silicomp-AQL

1 rue de la châtaigneraie
CS 51766
F 35513 Cesson Sévigné Cedex
France

Téléphone : +33 (0)2 99 12 50 00

Adresse électronique : cesti@aql.fr

2.4. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 26 août 2010, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation relatives à la classe d'exigences d'assurance APE sont à « **réussite** ».
Conformément aux règles d'évaluation, les annexes du [PP] ne font pas partie du périmètre de l'évaluation.

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.

3.2. Recommandations et limitations d'usage

Toute évaluation d'un produit se réclamant conforme à ce [PP] devra inclure, comme précisé en figure 1, le système d'exploitation (OS) et le microcircuit (IC), distinguant ainsi la portée de l'évaluation du profil de protection (TOE du PP) de celle d'une cible de sécurité (TOE de la cible de sécurité). Ainsi, une cible de sécurité conforme à ce [PP] devra décliner les objectifs sur l'environnement du PP décrits ci-dessous en objectifs sur la TOE dans la cible :

- OE.SCP.IC ;
- OE.SCP.RECOVERY ;
- OE.SCP.SUPPORT.

3.3. Reconnaissance européenne (SOG-IS)

Ce rapport de certification 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[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E6 Elevé 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, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni, la Suède.

3.4. Reconnaissance internationale (CC RA)

Ce rapport de certification est émis dans les conditions de l'accord du CC RA [CC RA].

L'accord « Common Criteria Recognition Arrangement » 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, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 4+	Intitulé du composant
ADV Développement	ADV_ARC		**1**	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**4**	Complete functional application
	ADV_IMP				**1**	1	**2**	**2**	**1**	Implementation representation of the TSF
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**3**	Basic 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**	Problem tracking CM coverage
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**4**	Production support, acceptance procedures and automation
	ALC_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**2**	Sufficiency of security measures
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**1**	Well-defined development tools
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**	**1**	Testing: basic 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

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.	
[CPP/P/01]	Procédure CPP-P-01 Certification de profils de protection, 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.
[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.
[PP-JCS]	*JavaCard System Minimal Configuration, version 1.0b, Protection Profile, Août 2003*. Certifié par la DCSSI sous la référence PP/0303.
[PP]	Profil de Protection objet du présent rapport de certification : « *Java Card™ System Protection Profile Closed Configuration* », version 2.6 du 25 août 2010.
[RTE]	Evaluation Technical Report Java Card System – Open Configuration Référence : TDL003C3-RTE-02 version 2.1 du 26/08/2010