PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification DCSSI-2008/02

MultiApp ID SSCD - Microcontrôleur SLE66CX680PE-A13 masqué par le logiciel MultiApp ID v1.0 et correctif v3.1

Paris, le 13 février 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.pm.gouv.fr

Référence du rapport de certification

DCSSI-2008/02

Nom du produit

MultiApp ID SSCD - Microcontrôleur SLE66CX680PE-A13 masqué par le logiciel MultiApp ID v1.0 et correctif v3.1

Référence/version du produit

Version 1.0

Conformité à un profil de protection

PP/0304 JavaCard System Standard – JavaCard 2.1.1 configuration v1.0b, PP-SSCD type2 et PP-SSCD type3

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, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4

Développeur(s)

Gemalto SA

6 rue de la Verrerie, 92197 Meudon, France

Infineon Technologies AG

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

Commanditaire

Gemalto SA

6 rue de la Verrerie, 92197 Meudon, 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 « MultiApp ID SSCD - Microcontrôleur SLE66CX680PE-A13 masqué par le logiciel MultiApp ID v1.0 et correctif v3.1 » développée par Gemalto SA et Infineon Technologies AG.

Le produit est une carte à puce destinée à être utilisée dans le cadre de l'administration électronique. Cette carte fournit l'application Java Card MultiApp ID SSCD sur une plateforme Java Card certifiée en parallèle (Cf. DCSSI-2008/01). L'application MultiApp ID SSCD offre un ensemble de services de signature électronique répondant aux caractéristiques des dispositifs sécurisés de création de signature électronique.

1.2. Description du produit évalué

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 aux profils de protection « Secure Signature-Creation Device Type 2 » [PP0005] et « Secure Signature-Creation Device Type 3 » [PP0006].

La plateforme Java Card sur laquelle repose le produit, est conforme au profil de protection « Java Card Protection Profile Collection, v1.0b, Java Card 2.1.1 configuration » [PP0304].

Les applications chargées après la livraison au porteur, si elles respectent les procédures et recommandations des guides [GUIDES], ne remettent pas en cause la conformité de la cible de sécurité aux profils de protection SSCD types 2 [PP0005] et type 3 [PP0006].

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 :

- l'application MultiApp ID (« hardmask » en ROM) version 1.0,
- le correctif applicatif MultiApp ID (MultiApp ID corrective softmask #1) version 3.1,
- le microcontrôleur SLE66CX680PE-A13 avec RMS library version 2.5 et RSA2048 library version 1.4.

Ces informations peuvent être vérifiées par la commande « masktrack ». La valeur retournée est : « 53 91 05 00 01 31 00 00 00 00 ».

L'application SSCD certifiée peut être identifiée à l'aide son AID unique. Sa présence peut être vérifiée par la commande de sélection d'applications (« Select APDU ») ou en utilisant l'instruction « GetStatus » (valeur retournée : A0 00 00 00 30 49 41 53 31 30 31 50 6B 67).
Ces informations sont décrites dans les guides (cf. [GUIDES]).

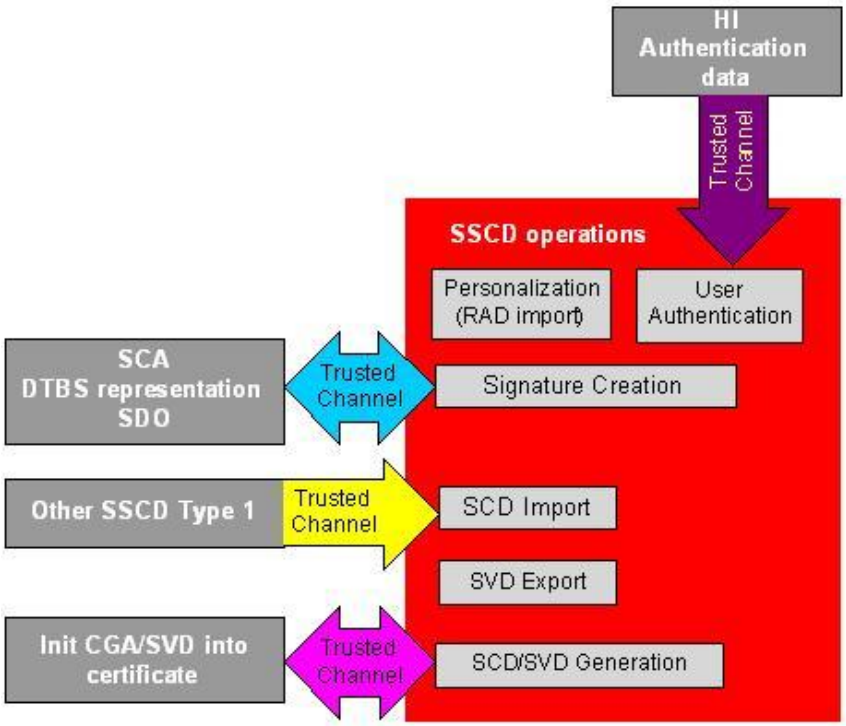
1.2.2. Services de sécurité

Les principaux services de sécurité fournis par l'application MultiApp ID sont :

- la génération des données de création de signatures électroniques (SCD) et de vérification de signatures électroniques (SVD) ;
- la gestion de la confidentialité de SCD (pas d'export possible) ;
- l'import de la paire SCD/SVD ;
- l'export de SVD ;
- la création de signatures ;
- l'administration des codes PIN ;
- l'authentification par code PIN du signataire ;
- l'authentification externe de l'administrateur ;
- la gestion d'un chemin de confiance avec un utilisateur (Human Interface HI).

Les principaux services de sécurité fournis par la plateforme Java Card sont :

- la gestion du cycle de vie de la carte et des applications ;
- des services d'administration des applications (chargement, installation, suppression) grâce au gestionnaire « GlobalPlatform Card Manager » et à l'utilisation de domaines de sécurité ;
- la gestion des clés de la plateforme « GlobalPlatform » ;
- la gestion des accès des applets aux interfaces de la plateforme (GlobalPlatform and Java Card 2.2.1 APIs et APIs propriétaires) ;
- l'isolation des applications (Java Card firewall).



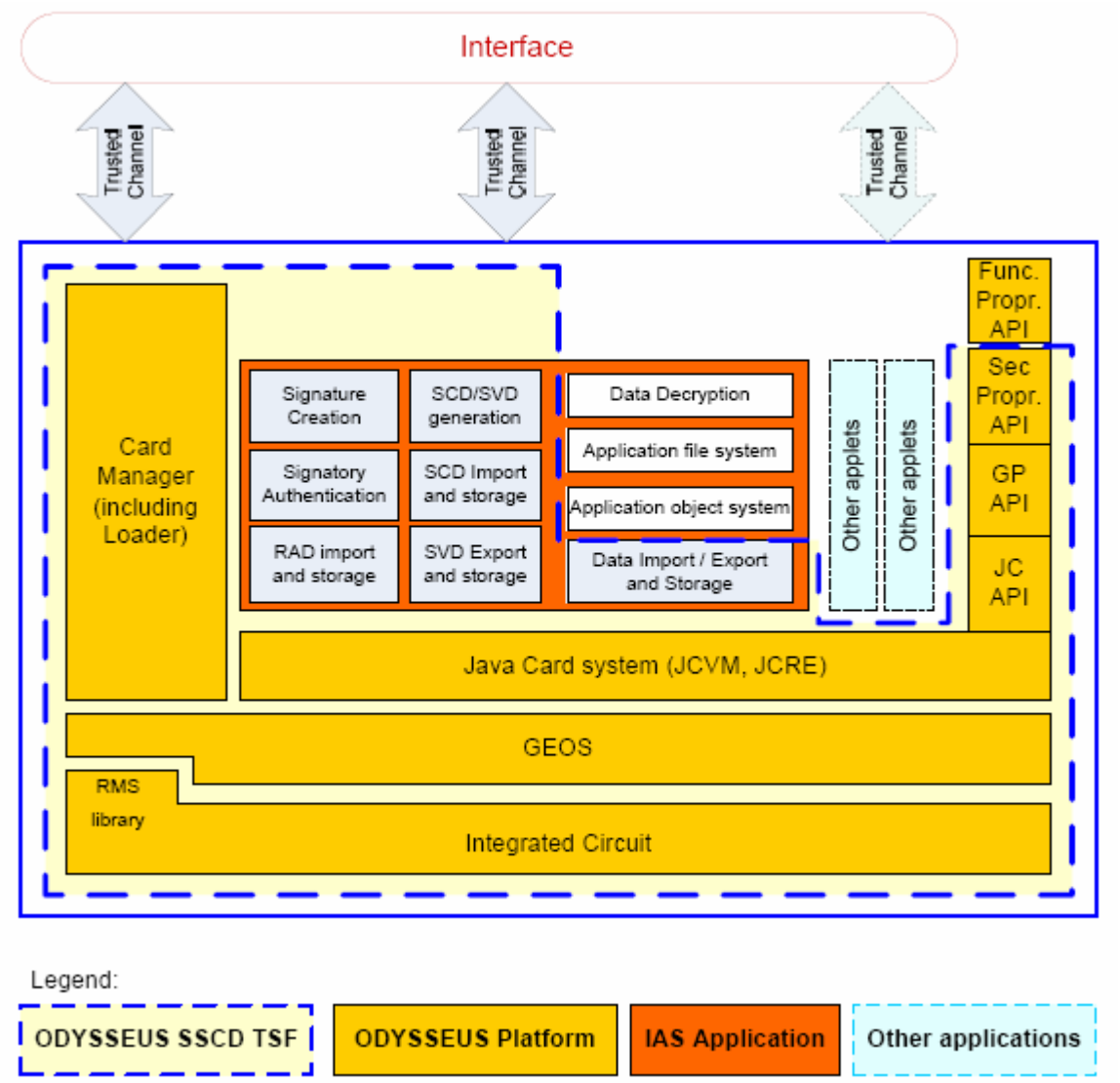
D'autres services présents dans la carte n'ont pas été évalués :

- l'authentification par Diffie-Helmann ;
- le déchiffrement symétrique ou asymétrique ;
- la vérification de certificat ;
- la gestion du système de fichier.

1.2.3. Architecture

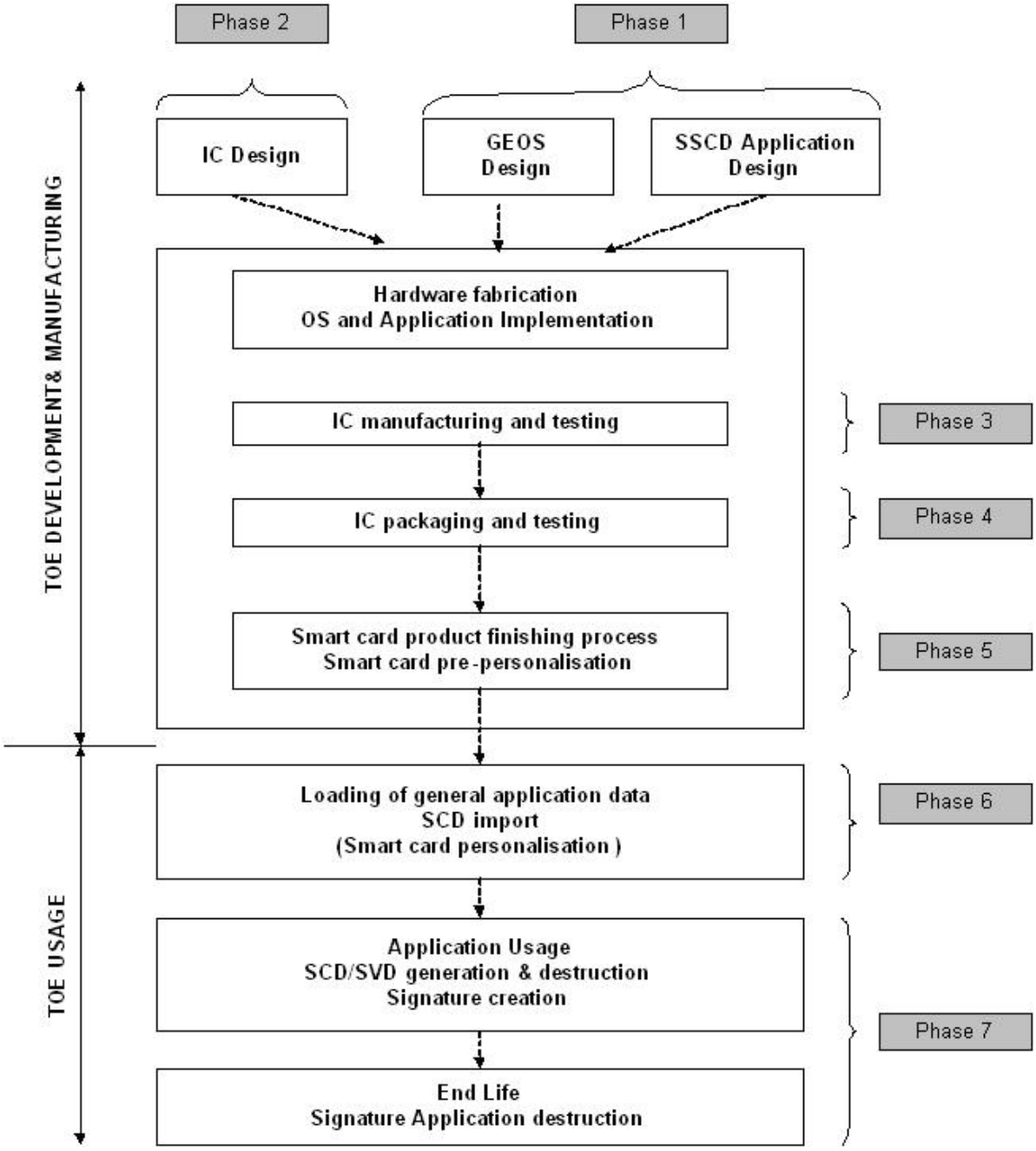
Le produit est constitué :

- du microcontrôleur et ses librairies ;
- du système d'exploitation GEOS ;
- du « Card manager » incluant le « loader » ;
- du « Java Card System » ;
- et de l'application « SSCD » MultiApp ID.



1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :



Le produit a été développé sur les sites suivants :

Gemalto Meudon site R&D

6 rue de la Verrerie
92197 Meudon,
France.

Gemalto Gémenos – site de production

Avenue du Pic de Bretagne,
13 881 Gémenos,
France.

Gemalto Orléans – site de production

Avenue de la Pomme de Pin,
45590 Saint Cyr en val,
France.

INFINEON Technologies AG

Postfach 80 09 49,
D-81609 München,
Allemagne.

Pour l'évaluation, l'évaluateur a considéré comme « administrateurs du produit » le « personnalisateur » de la carte et l'émetteur de la carte (« Card Issuer ») et comme « utilisateur du produit » le signataire, détenteur de la carte à puce. Ces rôles sont détaillés dans la cible de sécurité [ST].

1.2.5. Configuration évaluée

Le certificat porte sur la plateforme Javacard avec l'application MultiApp ID seule. L'application doit être 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] et 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 du logiciel dans le microcontrôleur déjà certifié par ailleurs.
Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur « SLE66CX680PE - m1534-A13 with RSA2048 V1.4 & specific IC dedicated software » au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, conforme au profil de protection [PP0002]. Ce microcontrôleur a été certifié le 14 septembre 2005 sous la référence BSI-DSZ-CC-0322.

Le niveau de résistance du microcontrôleur a été confirmé le 11 octobre 2006 dans le cadre du processus de surveillance.

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 11 décembre 2007, 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.

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 « MultiApp ID SSCD - Microcontrôleur SLE66CX680PE-A13 masqué par le logiciel MultiApp ID v1.0 et correctif v3.1» 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 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].

Des objectifs de sécurité sur l'environnement issus du profil de protection PP SSCD type 2 [PP0005] concernent les aspects suivants :

- la correspondance entre SVD et SCD (OE.SCD_SVD_Corresp) ;
- le transfert sécurisé de SCD entre SSCD (OE.SCD_Transfer) ;
- l'unicité des données de création de signature (OE.SCD_Unique).

Des objectifs de sécurité sur l'environnement issus des profils de protection PP SSCD type 2 [PP0005] et PP SSCD type 3 [PP0006] concernent les aspects suivants :

- la génération de certificats qualifiés (OE.CGA_Qcert) ;
- la vérification de l'authenticité de la SVD par la CGA (OE.SVD_Auth_CGA) ;
- la protection des VAD (OE.HI_VAD) ;
- les données devant être signées (OE.SCA_Data_Intend).

Un objectif de sécurité sur l'environnement (OE.Key_Mngt) concerne la gestion sûre des clés. Il précise que les environnements de l'application de création de signatures (SCA) et l'application de génération de certificats CGA doivent protéger la confidentialité des clés utilisées pour les communications sécurisées entre la carte et ces applications (SCA et CGA).

Des objectifs de sécurité sur l'environnement liés à la plateforme concernent les aspects suivants :

- des procédures doivent être employées pour couvrir les besoins de confidentialité et d'intégrité des biens de la carte jusqu'à la phase de personnalisation (phase 6), (OE.DEVELOPMENT) ;
- les applets chargées après la livraison au porteur ne doivent pas contenir de méthodes natives (OE.APPLET) ;

• tout code (« byte-code ») d'applet doit être vérifié avant chargement, afin de garantir son exécution (OE.VERIFICATION).

Il est recommandé de vérifier l'identification de l'applet certifiée de signature selon la procédure prévue par les guides (Cf. [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 :

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[2], 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 SOG-IS sont : l'Allemagne, l'Espagne, la Finlande, la France, la Grèce, l'Italie, la Norvège, les Pays-Bas, le Portugal, le Royaume-Uni, la Suède et la Suisse.

[2] 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 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	**2**	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	**3**	Analysis and testing for 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 : - ODYSSEUS SSCD Security Target Version 1.4 issued September 21st, 2007, réf. : D1049311. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - ODYSSEUS SSCD Security Target (Public version) Version 1.6 issued January 24th, 2008, réf. : D1049311.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report - ODYSSEUS Project réf.: ODYSSEUS_ETR_V1.1 - ADDENDUM au Rapport Technique d'Evaluation ODYSSEUS_ETR_V1.1 réf. : ODYSSEUS_REP_04_V1.0
[CONF]	ODYSSEUS Configuration List v1.3 réf. : D1050209.
[GUIDES]	Guide d'installation du produit : - ODYSSEUS Installation, Generation & Startup procedure, v1.0, réf. : D1050210 Guide d'administration du produit : - Administrator Manual, v0.6, réf. : ADM_D1050012 - ODYSSEUS SSCD Personalization, v1.02, réf. : PER_D1051441 Guide d'utilisation du produit : - ODYSSEUS Platform User Manual, v0.5 réf. : USR_D1050014
[PP0304]	JavaCard System Standard - Protection Profile Collection, JavaCard 2.1.1 configuration v1.0b, August 2003. Certifié par la DCSSI sous la référence PP/0304.
[PP0005]	Protection Profile — Secure Signature-Creation Device Type 2, Version: 1.04, 25 July 2001. *Certifié par le BSI sous la référence BSI-PP-0005-2002T.*
[PP0006]	Protection Profile — Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001. *Certifié par le BSI sous la référence BSI-PP-0006-2002T.*
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certifié par le BSI sous la référence BSI-PP-0002-2001.*

Il est à noter que le nom « ODYSSEUS » présent dans certains documents correspond à « MultiApp ID SSCD» et identifie l'évaluation.

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-2007-04-001 version 2.3, revision 1, April 2007.
[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.
[AIS 34]	Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004, Bundesamt für Sicherheit in der Informationstechnik.