Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification DCSSI-2007/19

Java Card System de la carte Usimera Protect V1.0 sur le composant SLE88CFX4000P

Paris, le 17 septembre 2007,

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

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-2007/19

Nom du produit

Java Card System de la carte Usimera Protect V1.0 sur le composant SLE88CFX4000P

Référence/version de la carte

T1000230 Usimera Protect 128K crypto on Infineon
Version logiciel : 2.1

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_FSP.4, ADV_HLD.5, ADV_IMP.3, ADV_INT.3, ADV_LLD.2, ADV_RCR.3, ADV_SPM.3, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4

Développeur(s)

Gemalto

6 rue de la verrerie, 92197 Meudon, France

Commanditaire

Gemalto

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 le Java Card System inclus dans la carte Usimera Protect V1.0 développée par Gemalto ; cette carte avait déjà été certifiée au niveau EAL 4 augmenté des composants ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4 (voir détail en 2.2).

La carte Usimera Protect est destinée à être utilisée dans les systèmes GSM 2G et UMTS 3G, conformément aux spécifications ETSI relatives aux communications mobiles. En fonction du système dans lequel elle est intégrée, elle peut être utilisée comme carte SIM, USIM ou les deux. Cette carte peut également héberger des applets requérant des services de sécurité comme l'authentification à base des mécanismes DES/3DES.

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 s'inspire du profil de protection « Java Card System Protection Profile Collection, V1.0b, Configuration Standard 2.2 » (cf. [PP/JCS]).

1.2.1. Identification de la carte

Les éléments constitutifs de la carte Usimera Protect V1.0, dont son Java Card System, sont identifiés dans la liste de configuration [CONF].
La version de la carte Usimera Protect V1.0 est identifiable par les éléments suivants :

- référence produit : T1000230 Usimera Protect 128K crypto on Infineon ;
- version logiciel : 2.1 ;
- identifiant du composant : SLE88CFX4000P ;
- design step du composant : m8830 B17 ;
- bibliothèque logicielle du composant : PSL v0.50.23.

Ces éléments sont identifiables dans l'ATR de la carte (Answer to Reset), au sein des octets T9 à T11 (identifiant du composant : D0 00 3E) et T12 à 13 (identifiant du logiciel : 01 7D).

1.2.2. Services de sécurité du produit

Les services de sécurité évalués fournis par le produit sont :

- la gestion des transactions de la JCVM (machine virtuelle Java Card) ;
- la gestion de la valeur des attributs de sécurité suivants: applets résidentes, applets actives, et applets sélectionnées, et vérification de la cohérence du cycle de vie des applets ;
- le cloisonnement entre applets embarquées sur la carte à l'aide du pare-feu du JCRE (environnement d'exécution Java Card) ;
- la protection des fichiers CAP chargés ;
- la restriction de la possibilité de création de points d'entrée JCRE au JCRE ;

- la gestion du comportement des applications Java Card.

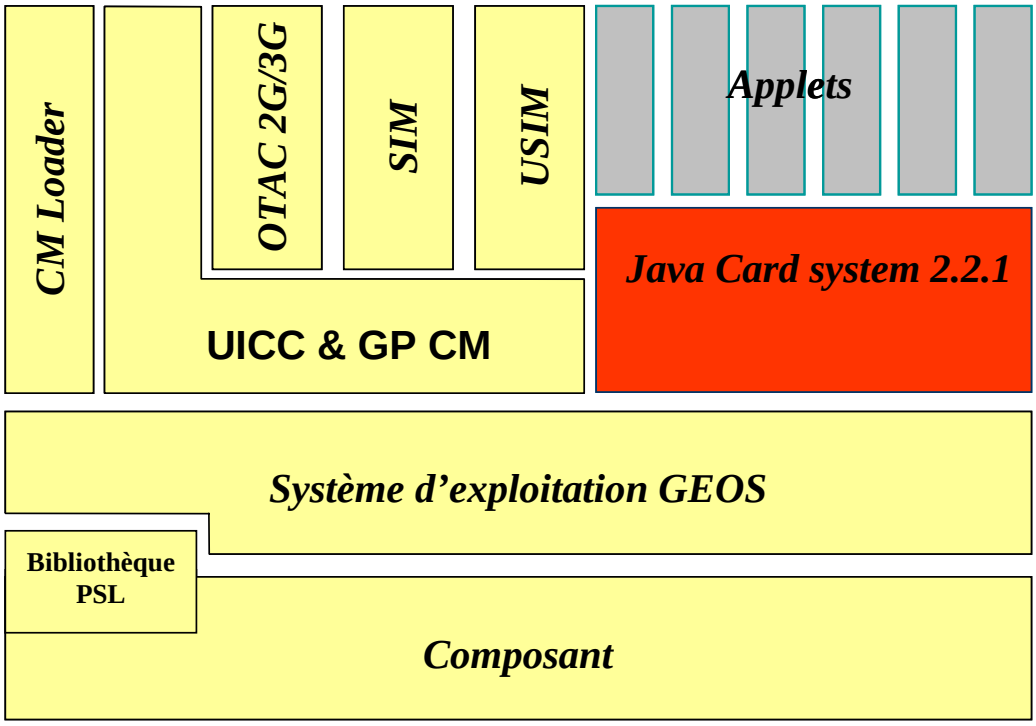
Ces services sont détaillés au chapitre 6.1de la cible de sécurité [ST] publique.

1.2.3. Architecture de la carte

La carte Usimera Protect V1.0 est constituée :

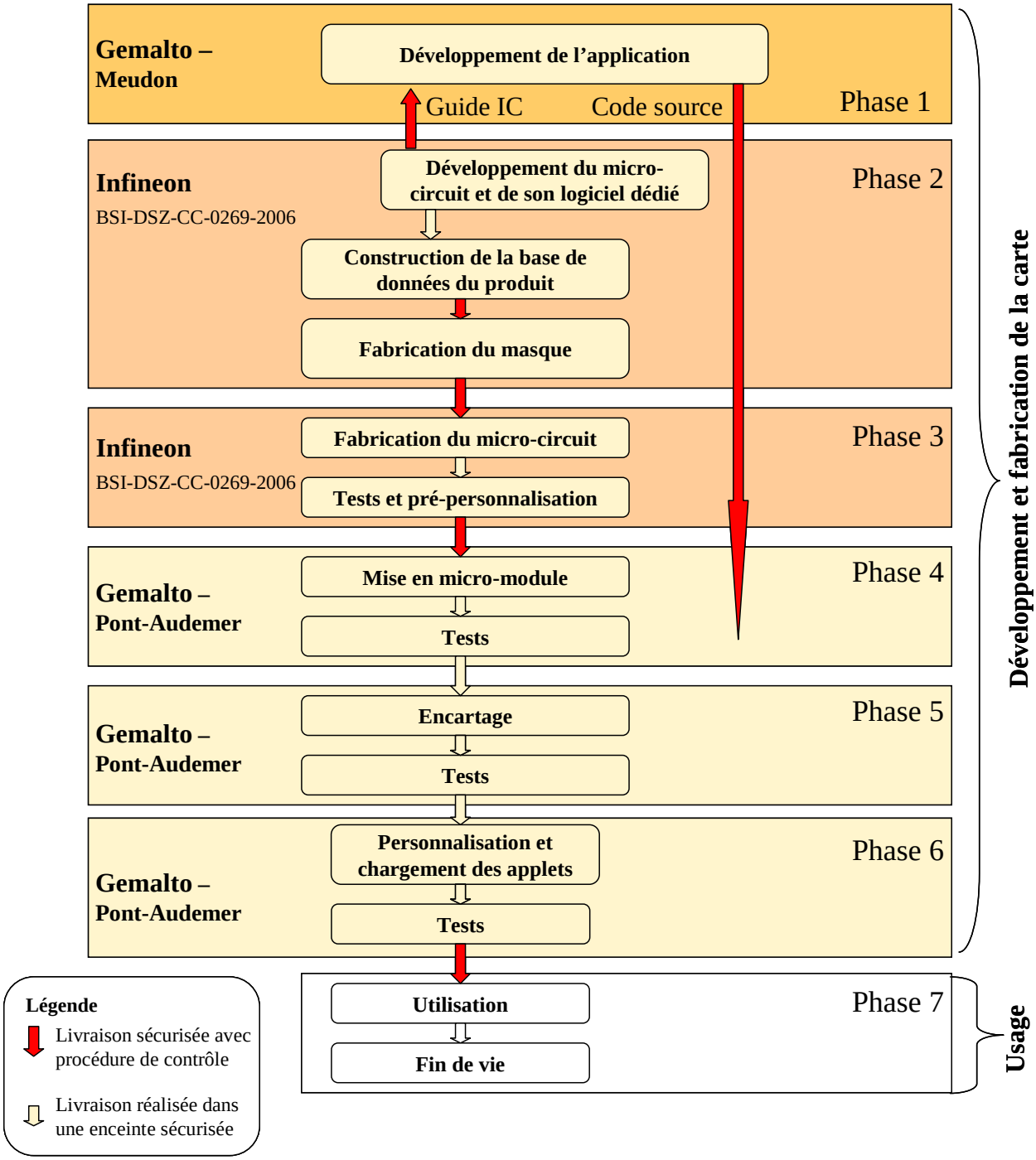
- du composant SLE88CFX4000P / m8830 B17 et sa bibliothèque logicielle cryptographique ;
- du système d'exploitation GEOS comprenant les fonctionnalités UICC ;
- du « Card Manager » et des fonctionnalités Open Platform ;
- d'une plate-forme Java Card comprenant les éléments JCRE 2.2.1, JCVM 2.2.1 et JCAPI 2.2.1 ;
- des applications SIM, USIM et OTA.

L'architecture de cette carte est décrite dans la figure suivante (produit évalué en rouge) :



1.2.4. Cycle de vie

Le cycle de vie de la carte Usimera Protect V1.0 est le suivant :



Le développement des logiciels embarqués sur la carte Usimera Protect V1.0 a été réalisé sur le site suivant :

Gemalto Meudon

6 rue de la verrerie
92197 MEUDON
France

Le composant et sa bibliothèque logicielle cryptographique ont été développés par Infineon Technologies :

Infineon Technologies AG

CCM MTH, Postfach 80 09 49
D-81609 München,
Allemagne

La carte est fabriquée par Gemalto sur le site de Pont-Audemer :

Gemalto Pont-Audemer

Rue George Clémenceau,
27500 Pont-Audemer,
France

1.2.5. Configuration évaluée

Le certificat porte uniquement sur les fonctionnalités offertes par les services Java Card de la carte Usimera Protect V1.0.
En regard du cycle de vie, le produit évalué est inclus dans la carte personnalisée, en phase d'usage, avec les services de chargement d'applets de la plate-forme qui demeurent disponibles.

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, ont été utilisées.

2.2. Travaux d'évaluation

L'évaluation s'appuie sur les résultats d'évaluation du produit « Carte Usimera Protect : composant SLE88CFX4000P embarquant les applications SIM, USIM et OTA sur plate-forme ouverte Javacard (version 2.1) » certifié le 30 mars 2007 sous la référence 2007/08 [2007_08].

Cette évaluation a consisté à réévaluer le produit selon les plus hautes exigences des Critères Communs relatives au développement : les composants ADV retenus ici correspondent à ceux du niveau EAL7, qui nécessitent la mise en œuvre de méthodes formelles. La plupart des résultats relatifs aux autres composants d'assurance ont été obtenus lors de l'évaluation précédente. C'est le cas de l'analyse de vulnérabilités, qui a donc été menée sur la carte Usimera Protect V1.0 complète.

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 6 septembre 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 a été analysée par la DCSSI dans le cadre de l'évaluation précédente (voir [2007_08]). Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] et ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur.

3. La certification

3.1. Conclusion

L'évaluation, identifiée au chapitre 2 et décrite dans le rapport technique d'évaluation [RTE], a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises par 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 Java Card System, inclus dans la carte Usimera Protect V1.0 sur le composant SLE88CFX4000P, 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], notamment :

- pour les phases 1 à 6, les procédures adéquates doivent être mises en œuvre afin de maintenir l'intégrité et la confidentialité des biens de la TOE (OE.DEVELOPMENT) ;
- les applets chargées après délivrance de la carte ne doivent comporter aucune méthode native (OE.APPLET) ;
- tout byte-code doit être préalablement vérifié avant d'être chargé dans la carte, afin de garantir que le code est valide lors de son exécution (OE.VERIFICATION) ;
- toutes les applications présentes sur la carte avant sa délivrance doivent être conformes à la TOE de façon à assurer que les politiques et objectifs de sécurité décrits dans [ST] ne sont pas violés (OE.NATIVE.2) ;
- en cas de perte d'alimentation ou si la carte est retirée du lecteur pendant qu'une opération est en cours, la plateforme (SCP) doit autoriser la TOE à éventuellement achever correctment l'opération d'interruption ou à retourner dans un état sûr (OE.SCP.RECOVERY) ;
- la plateforme (SCP) doit fournir les fonctionnalités assurant le bon fonctionnement de la TSF (interdisant qu'elle soit contournée ou altérée) et contrôlant les accès aux informations propres à la TSF. Cette plateforme doit également fournir les services basiques, requis par l'environnement d'exécution pour réaliser les mécanismes de sécurité tels que les transactions atomiques, la gestion des objets persistants et transitoires, et les opérations cryptographiques
- la plateforme (SCP) doit posséder des mécanismes de sécurité au niveau de l'IC (OE.SCP.IC) ;
- le « card manager » doit contrôler l'accès aux fonctions de gestion de la carte telles que l'installation (excepté la phase de link), la mise à jour et la suppression d'applets. Il doit aussi implémenter la politique de l'émetteur de la carte (OE.CARD-MANAGEMENT) ;

- l'environnement TI ainsi que la plateforme doivent assurer l'exécution continue et correcte de ses fonctionnalités (OE.OPERATE) ;
- l'environnement TI (le « card manager ») doit contrôler la disponibilité des ressources pour les applications (OE.RESOURCES) ;
- l'environnement TI (le « card manager ») doit assurer que la réallocation de blocs mémoire pour la zone d'exécution de la JCVM ne divulgue pas d'informations qui étaient préalablement stockées dans ce bloc (OE.REALLOCATION) ;
- le seul moyen que l'environnement TI doit fournir aux applications pour exécuter du code natif est l'invocation d'API Java Card standards ou propriétaires (OE.NATIVE) ;
- le « card manager » doit assurer que tout conteneur d'informations partagées par les applications (tels que le buffer d'entrées/sorties ou une variable globale publique de l'API) est toujours purgé après l'exécution d'une application (OE.SHRD_VAR_CONFID) ;
- la plateforme (SCP) doit fournir des moyens sûrs de chiffrer les données sensibles des applications (OE.CIPHER) ;
- la plateforme (SCP) doit fournir des moyens sûrs de gestion des clés cryptographiques (OE.KEY-MNGT) ;
- l'environnement TI doit fournir des moyens sûrs de gestion des objets PIN (OE.PIN-MNGT) ;
- l'environnement TI doit fournir des moyens pour restreindre les accès distants des lecteurs aux services implémentés par l'applet de la carte (OE.REMOTE) ;
- le « card manager » doit assurer la protection du chargement des packages (OE.LOAD) ;
- le « deletion manager » doit assurer la protection de l'effacement des applets et des packages (OE.DELETION) ;
- l'environnement TI doit assurer que la suppression d'objets ne rompt pas les références aux objets (OE.OBJ-DELETION).

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 Portugal, le Royaume-Uni, la Suède et la Suisse.

3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat 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, la Corée du Sud, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Nouvelle-Zélande, la Norvège, 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**	**4**	Formal functional specification
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**	**5**	Formal high-level design
	ADV_IMP				**1**	**2**	**3**	3	**3**	Structured implementation of the TSF
	ADV_INT					**1**	**2**	**3**	**3**	Minimisation of complexity
	ADV_LLD				**1**	1	**2**	2	**2**	Semiformal low-level design
	ADV_RCR	**1**	1	1	1	**2**	2	**3**	**3**	Formal 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**	**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**	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

[ST]	Cible de sécurité de référence pour l'évaluation : - Formal Assurance on the JavaCard Virtual Machine embedded in Usimera Protect - Security Target, référence: D1031392, révision 1.3, septembre 2007 Pour les besoins de publication la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Formal Assurance on the JavaCard Virtual Machine embedded in Usimera Protect - Security Target – Public Version, référence: D1031392, révision. 1.3, septembre 2007
[RTE]	Rapport technique d'évaluation : - SIMEOS EXTENDED project Evaluation Technical Report, reference SIMEOSEXT_ETR_V1.1.fm, version 1.1 du 21/08/07 (diffusé le 06/09/07)
[CONF]	Simeos Configuration List, référence : D1021043, version 3.3, juillet 2007
[GUIDES]	- Installation, Generation and Start-up - Pre-personalization Procedure, référence : IGS_D1021046, revision 1.0 - USimera Protect Volume 1 - User Guide, référence : D1019543, révision 2.0 - USimera Protect Volume 2 - Administrator Guide, référence : D1019545, révision 2.0 - JCVM 2.2: User Manual Applets Development Guide, référence : AGD_D1016741, révision 0.5
[PP/JCS]	Java Card System Protection Profile Collection, V1.0b, Configuration Standard 2.2. *Certifié par la DCSSSI sous la référence PP/0305.*
[2007_08]	Rapport de certification DCSSI-2007/08 - Carte Usimera Protect : composant SLE88CFX4000P embarquant les applications SIM, USIM et OTA sur plate-forme ouverte Javacard (version 2.1), 30 mars 2007, SGDN/DCSSI
[ANA-CRY]	Cotation de mécanismes cryptographiques, Projet SIMEOS, Référence : N° 294/SGDN/DCSSI/SDS/Crypto du 12 février 2007

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 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.