PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

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)

Paris, le 30 mars 2007

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-2007/08

Nom du produit

Carte Usimera Protect : composant SLE88CFX4000P embarquant les applications SIM, USIM et OTA sur plate-forme ouverte Javacard (version 2.1)

Référence/version du produit

Référence du produit : T1000230 Usimera Protect 128K crypto on Infineon
Version du code : 2.1

Conformité à un profil de protection

Java Card System Protection Profile Collection, V1.0b, Configuration Standard 2.2. Référence PP/0305

Critères d'évaluation et version

Critères Communs version 2.2

Niveau d'évaluation

EAL 4 augmenté

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

Développeurs

Gemalto

6 rue de la verrerie,
92197 Meudon, France

Infineon Technologies AG

St.-Martin-Straße 76,
81609 München, Allemagne

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 la carte Usimera Protect, constituée du composant SLE88CFX4000P / m8830 B17 avec sa bibliothèque logicielle PSL v0.50.23, développé par Infineon Technologies AG, et embarquant les applications SIM, USIM et OTA sur plate-forme ouverte Javacard, développées par Gemalto.
La référence du logiciel chargé en mémoire « flash » est « T1000230 Usimera Protect 128K crypto on Infineon » en version 2.1.

Cette carte 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. Ce produit 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 est conforme au profil de protection « Java Card System Protection Profile Collection, V1.0b, Configuration Standard 2.2 » (cf. [PP/JCS]).

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 :

- 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 du produit (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

Les principaux services de sécurité fournis par le produit sont décrits au chapitre 6.1 de la cible de sécurité publique (cf. [ST]). Ils sont rendus par le système d'exploitation, par les applications de communications GSM et UMTS, ainsi que par la plate-forme Javacard.

1.2.3. Architecture

Le produit est une carte à puce 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 du produit est résumée dans la figure suivante :

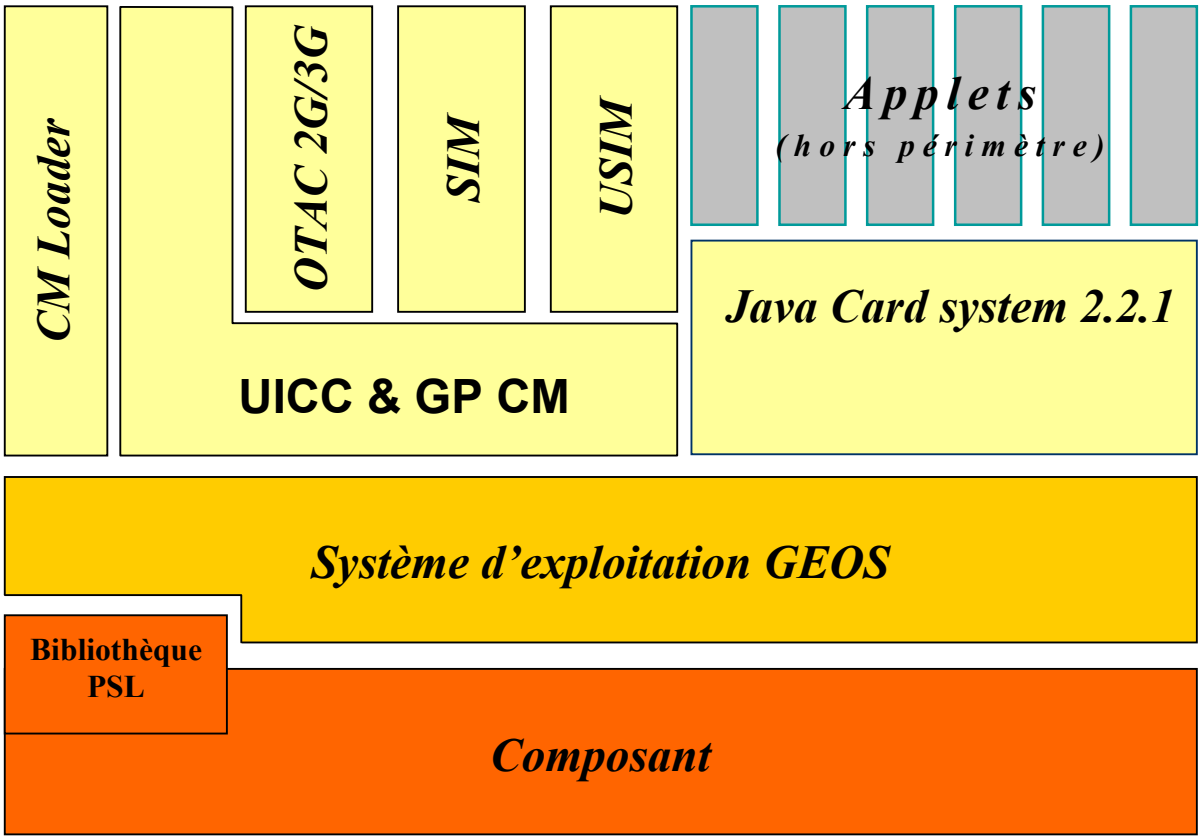

Figure 1 – Architecture du produit

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

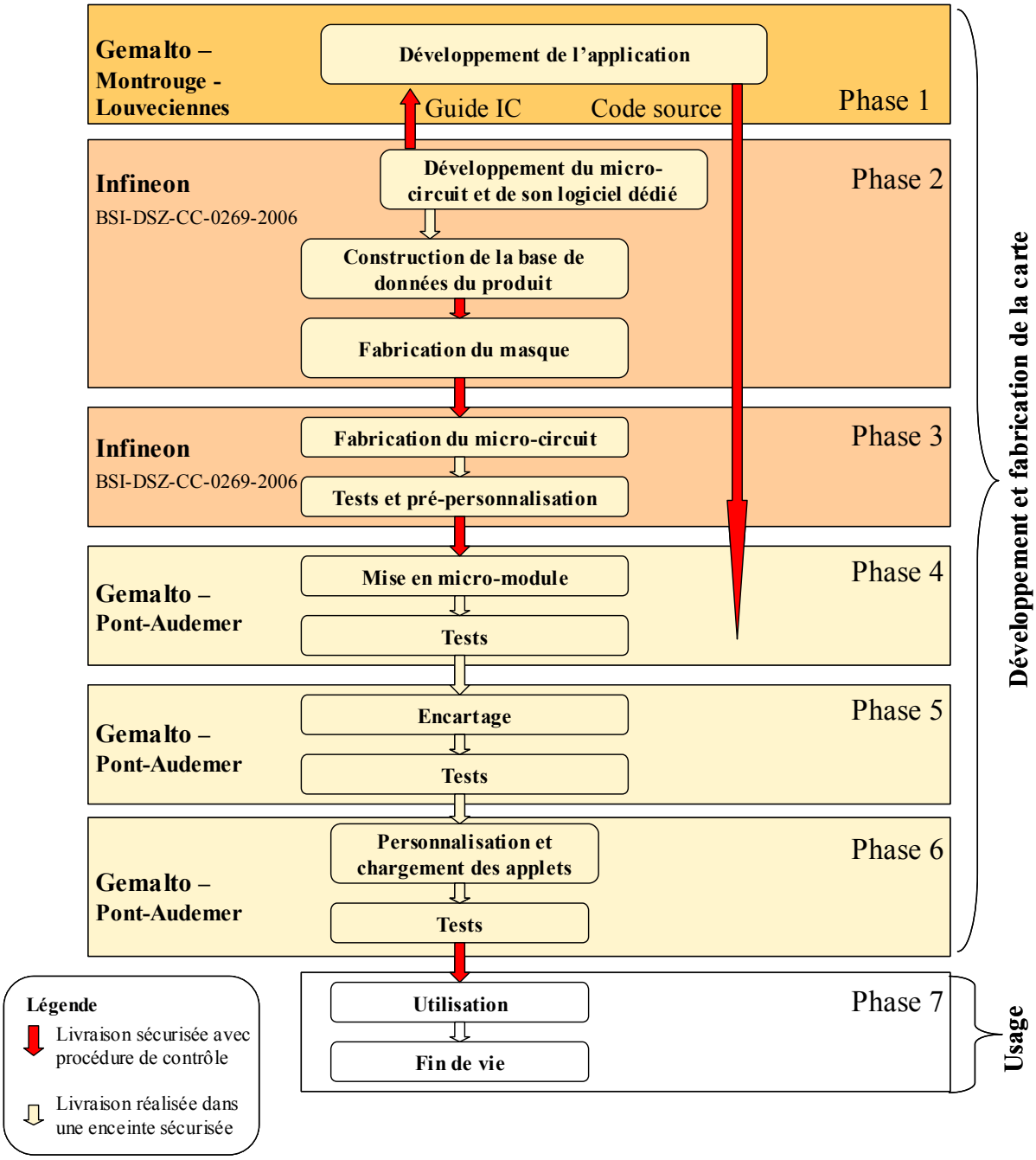

Figure 2 – Cycle de vie du produit

Le logiciel a été développé conjointement sur les sites de Gemalto à Montrouge et à Louveciennes :

Gemalto Montrouge

50 Av. Jean Jaurès,
92542 Montrouge Cedex,
France

Gemalto Louveciennes

36-38, rue de la princesse, BP 45
78431 Louveciennes Cedex
France

A la suite d'un déménagement, le site de développement de Gemalto se situe désormais à Meudon :

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 sur les fonctionnalités suivantes du produit :

- le composant et l'algorithme DES de sa bibliothèque logicielle cryptographique ;
- le système d'exploitation GEOS ;
- les fonctions d'authentification des applications SIM et USIM ;
- le chargement sécurisé offert par le « Card Manager » ;
- les services Java Card.

En regard du cycle de vie, le produit évalué est 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 2.2** [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 [AIS34] ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [CCIC] et [CCAP] 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 « SLE88CFX4000P » 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 23 mars 2006 sous la référence BSI-DSZ-CC-0269-2006. Une version maintenue a été validée au titre de la « continuité de l'assurance » le 28 février 2007 sous la référence : BSI-DSZ-CC-0269-2006-MA-02.

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 28 mars 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. 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.

L'analyse cryptographique a révélé que les tailles de clés de certains algorithmes ne permettent pas d'atteindre le niveau standard du référentiel cryptographique de la DCSSI (cf. [REF-CRY]). Ces limitations sont dues aux spécifications GSM et ne sont pas sous le contrôle du développeur. Les vulnérabilités résultantes sont de nature système et ne sont pas spécifiques au produit lui-même. C'est le cas en particulier pour l'authentification du réseau 2G. En revanche, le service d'authentification 3G atteint bien le niveau standard du référentiel cryptographique de la DCSSI (cf. [REF-CRY]).

2.4. Analyse du générateur d'aléas

La plate-forme offre deux générateurs d'aléas (un matériel, et un logiciel) qui peuvent être utilisés par les développeurs d'applet.

Le générateur matériel a fait l'objet d'une évaluation AIS31 (cf. [AIS31]) dans le cadre de la certification du composant (cf. BSI-DSZ-CC-0269-2006). Le centre d'évaluation a néanmoins effectué une analyse complémentaire. Cette analyse n'a pas permis de mettre en évidence de biais statistiques bloquant pour un usage direct de la sortie du générateur. Ceci ne permet pas d'affirmer que les données générées soient réellement aléatoires mais assure que le générateur matériel 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.

Le générateur logiciel consiste en un retraitement logiciel des aléas issus du générateur matériel précédemment évoqué. Le mécanisme de retraitement n'atteint pas le niveau standard de la DCSSI (cf. [REF-CRY]). Pour un usage cryptographique, la sortie de ce générateur de nombres aléatoires doit donc également subir un retraitement algorithmique de nature cryptographique qui atteigne le niveau standard.

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 produit « Carte Usimera Protect : composant SLE88CFX4000P embarquant les applications SIM, USIM et OTA sur plate-forme ouverte Javacard (version 2.1) » 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], notamment :

- Pour les services mobiles :
  - L'opérateur du système GSM/UMTS doit appliquer des mesures de protection forte en confidentialité pour les clés d'administration GSM/UMTS, afin qu'elles puissent être utilisées à des fins d'authentification ;
- Pour la Javacard :
  - Les applets chargées après délivrance de la carte ne doivent comporter aucune méthode native ;
  - 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.
  - Les développeurs d'applets doivent prendre en compte les recommandations relatives à l'usage des générateurs de nombres aléatoires évoquées au §2.4 du présent rapport.

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 CC RA [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 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**	**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**	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 : - Usimera Protect - Security Target, Référence : D1019540 rev. 5.0, Gemalto Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Usimera Protect Security Target – Public version, Référence : D1019540 rev. 5.0 Gemalto
[RTE]	Evaluation Technical Report - SIMEOS platform (EAL4+ evaluation), Référence : SIMEOS_ETR_V1.1 Serma Technologies
[ANA-CRY]	Cotation de mécanismes cryptographiques, Projet SIMEOS, Référence : N° 294/SGDN/DCSSI/SDS/Crypto du 12 février 2007
[CONF]	Simeos Configuration List, Référence : D1021043 v2.3 Gemalto
[GUIDES]	- Installation, Generation and Start-up - Pre-personalization Procedure, Référence : IGS_D1021046 v1.0, Gemalto - USimera Protect Volume 1 - User Guide, Référence : D1019543 revision 2.0, Gemalto - USimera Protect Volume 2 - Administrator Guide, Référence : D1019545 revision 2.0, gemalto - JCVM 2.2: User Manual Applets Development Guide, Référence : AGD_D1016741 revision 0.5, Gemalto
[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.*
[PP/JCS]	Java Card System Protection Profile Collection, V1.0b, Configuration Standard 2.2. *Certifié par la DCSSSI sous la référence PP/0305.*

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, 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.
[CCSUP]	Common Criteria Supporting Document – Rationale for Smart cards and similar devices, version 1.1, June 2006.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, version 2.0, April 2006.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, version 2.1, April 2006.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - ETR-lite for composition, Version 1.3, April 2006.
[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.
[AIS31]	Functionnality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25 September 2001, Bundesamt für Sicherheit in der Informationstechnik

[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