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-2010/59

MultiApp ID CIE/CNS

Applet de signature électronique CIE/CNS en version 1.0 sur plateforme JC/GP MultiApp v1.1 masquée sur composant SAMSUNG S3CC91C en révision 0

Paris, le 20 JUIN 2011

Le directeur général de l'agence nationale 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 l'agence nationale de la sécurité des systèmes d'information (ANSSI), 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 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-2010/59

Nom du produit

MultiApp ID CIE/CNS

Référence/version du produit

Référence T1003893

Applet de signature électronique CIE/CNS version 1.0 sur plateforme JC/GP MultiApp v1.1 masquée sur composant Composant S3CC91C en révision 0.

Conformité à un profil de protection

BSI-PP-0005-2002: SSCD Type 2 Version 1.04

BSI-PP-0006-2002: SSCD Type 3 Version 1.05

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

6 rue de la verrerie
92197 Meudon Cedex, France

Samsung Electronics

La Boursidière, RN186, Bat. Jura BP202,
92357 Le Plessis Robinson, France

Commanditaire

Gemalto

6 rue de la verrerie
92197 MEUDON Cedex, 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 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 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 CIE/CNS». Cette carte à puce est destinée à être utilisée comme dispositif sécurisé de création de signature électronique (SSCD) de types 2 et 3.

Cette carte est constituée :

- d'un microcontrôleur sécurisé S3CC91C en révision 0. Ce microcontrôleur RISC 16 bits, muni d'un co-processeur cryptographique TORNADO ainsi qu'une bibliothèque dédiée TORNADO RSA 3.5S, fabriqué par Samsung Electronics, a été certifié par le BSI en septembre 2007 [Certif_IC] suivant la référence BSI-DSZ-CC-0451-2007 ;
- d'un système d'exploitation comportant une plateforme Java Card MultiApp version 1.1, développée par Gemalto conformément aux spécifications Java Card v2.2.1 et Global Platform v2.1, le tout, embarqué sur le composant S3CC91C ;
- d'une applet CIE/CNS stockée en ROM fournissant des services de signature électronique ;
- d'autres applets développées par Gemalto sont installées en ROM. Ces applets ne font pas partie de la TOE mais leur présence a été prise en compte lors de l'analyse de vulnérabilités.

1.2. Description du produit

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 suivants :

« *Secure Signature-Creation Device Type 2 Version: 1.04* » de référence BSI-PP-0005-2002 (cf. [PP0005]) ;

« *Secure Signature-Creation Device Type 3 Version: 1.05* » de référence BSI-PP-0006-2002 (cf. [PP0006]).

1.2.1. Identification du produit

La version certifiée du produit est identifiable par les éléments constitutifs du produit qui sont identifiés dans la liste de configuration [CONF]. Ces éléments d'identification sont accessibles via les commandes suivantes :

- un GET DATA de valeur **0103**[1] dont les 12 octets utiles de la valeur retournée sont :

Rang	0	1	2	3	4	5	6	7	8	9	10	11
Valeur	B0	85	13	1E	02	50	42	50	00	C8	00	00

[1] en Héxadécimal

Les octets retournés ont la signification suivante :

Gemalto Family Name (0) : B0 pour Java Card ;
Gemalto OS Name (1) : 85 pour MultiApp ID v1.1 ;
Gemalto Mask Number (2) : 13 pour MSA081 ;
Gemalto Product Name, (3) : 1E pour CIE CNS configuration ;
Gemalto Flow version (4) : 02 ;
Gemalto filter set (5) : 50 pour Filter 01, version 5 ;
Chip Manufacturer (6-7) : 4250 pour Samsung ;
Chip version (8-9) : 00C8 pour S3CC91C ;
RFU (10-11) : 0000.

Les octets suivants (12 à 31) correspondent aux informations de personnalisations qui seront complétées lors de la personnalisation de la carte.

- un GET DATA de valeur 0104[1] qui donne les valeurs de traçabilité du masque :

Rang	0	1	2	3	4	5	6	7	8	9	10	11	12
Valeur	A1	00	78	24	0A	00	00	00	00	04	21	13	0A

[1]

Les octets retournés ont la signification suivante :

Référence PDM[2] de la puce (0-3) : A1007824 ;
Version PDM de la puce (4) : 0A ;
Référence PDM du *softmask* (5-7) : 000000[3] ;
Version PDM du *softmask* (8) : 00[3] ;
Référence PDM de l'applet (9-11) : 042113 pour S1042113 ;
Version PDM de l'applet : 0A pour version 1.0.

1.2.2. Services de sécurité

Le produit met en œuvre les fonctions de sécurité requises au titre de la signature électronique et propose leur usage uniquement au travers de canaux de communication sécurisés. Le logiciel implémente la fonction de « dispositif sécurisé de création de signatures » (SSCD) qui permet la génération et l'import de données de création de signatures (SCD), de vérification de signatures (SVD) et la création de signatures électroniques qualifiées. Le produit protège les SCD et restreint leur usage aux seuls signataires autorisés.

[1] en Héxadécimal
[2] *Product Data Management*
[3] Ces données ne sont pas rentrées car elles sont disponibles via la commande précédente (GET DATA 0103)

1.2.3. Architecture

L'architecture du produit est résumée sur la figure 1 ci-dessous :

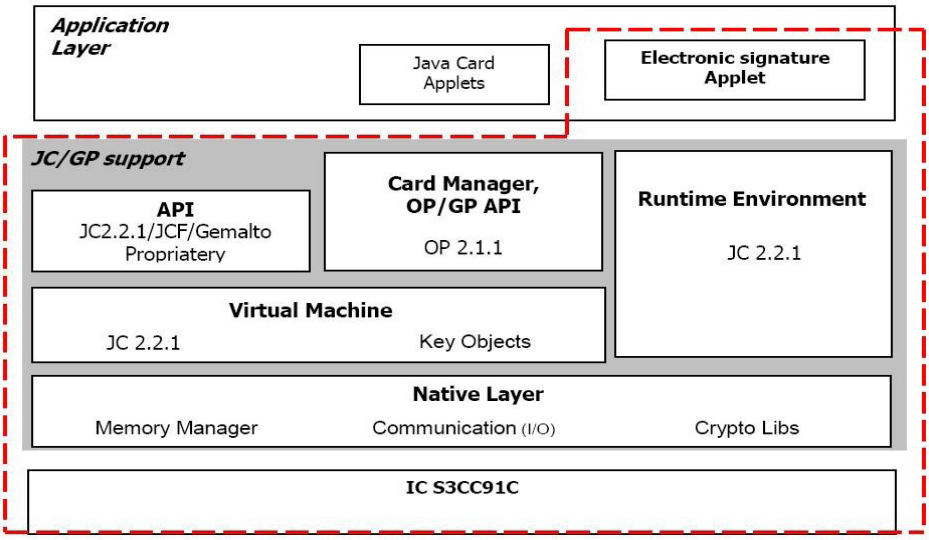

Figure 1 – Architecture du produit

Le produit est une carte à puce constituée :

- du composant S3CC91C rev. 0 avec sa bibliothèque logicielle cryptographique RSA Tornado 3.5S ;
- d'un OS sous forme d'une plateforme Java Card/GlobalPlatform : MultiApp, version 1.1, munie d'une JCVM[1] ;
- de l'applet CIE/CNS de signature électronique avec ses données.

Les autres applets instanciables ou non ne font pas partie de la cible d'évaluation (*TOE*) et sont donc en dehors du périmètre d'évaluation.

1.2.4. Cycle de vie

Le cycle de vie du produit est constitué de plusieurs phases qui s'opèrent sur différents sites des développeurs.

Les entités et transitions du processus de développement du produit qui s'inscrivent dans la cible d'évaluation peuvent être décrites comme suit (cf. figure 2) :

Phase 1 (Gemalto Meudon) :

- développement du logiciel embarqué (OS, plateforme Java Card, l'applet CIE/CNS) et conception dédiée à la phase de pré-personnalisation.

[1] Java Card Virtual Machine : machine virtuelle Java Card

Phase 2 (Samsung Giheung[1] - *wafer line 6, Korea*) :
- conception du circuit intégré et du logiciel dédié ;
- gestion du code client ;
- préparation des données pour les masques ;
- fabrication des masques.

Phase 3 (Samsung Giheung) :
- fabrication du micro-circuit ;
- tests ;
- polissage et sciage des galettes de silicium (wafers).

Phase 4 (Gemalto Gémenos / Pont-Audemer) :
- assemblage des puces en micromodules.

Phase 5 (Gemalto Vantaa / Gémenos) :
- encartage (packaging) ;
- pré-personnalisation et chargement éventuel d'un patch en EEPROM.

Phase 6 (**hors évaluation**) :
- personnalisation. A l'issue de cette phase, la carte est positionnée à l'état *OP_SECURED* interdisant le chargement de nouvelles applets.

Les transitions entre ces phases de développement conduisent au transfert de biens sensibles, logiques (données de conception, code source) ou physiques (échantillons de produit en cours de développement).

Les livraisons suivantes doivent alors être sécurisées :
- logiciel dédié et guide au développeur de l'application (en amont de la phase 1) ;
- code du logiciel embarqué au fabricant du microcontrôleur (entre phases 1 et 2) ;
- données requises par le fabricant des masques (durant la phase 2 : sous-traitance) ;
- masques au fabricant du microcontrôleur (entre phases 2 et 3) ;
- microcontrôleurs à l'assembleur et encarteur (entre phases 3 et 4) ;
- cartes au pré-personnalisateur (entre phases 4 et 5) ;
- cartes pré-personnalisées au personnalisateur (entre phases 5 et 6).

En regard du cycle de vie, le produit évalué est celui qui sort de la phase 5 de pré-personnalisation. Les phases suivantes sont couvertes par les guides du produit (cf. [GUIDES]).

[1] Samsung a éventuellement pu sous-traiter une ou plusieurs tâches comme la fabrication des masques. Les détails concernant le cycle de vie du composant Samsung S3CC91C, révision 0, se trouvent dans le rapport de certification du BSI (référence BSI-DSZ-CC-0451-2007).

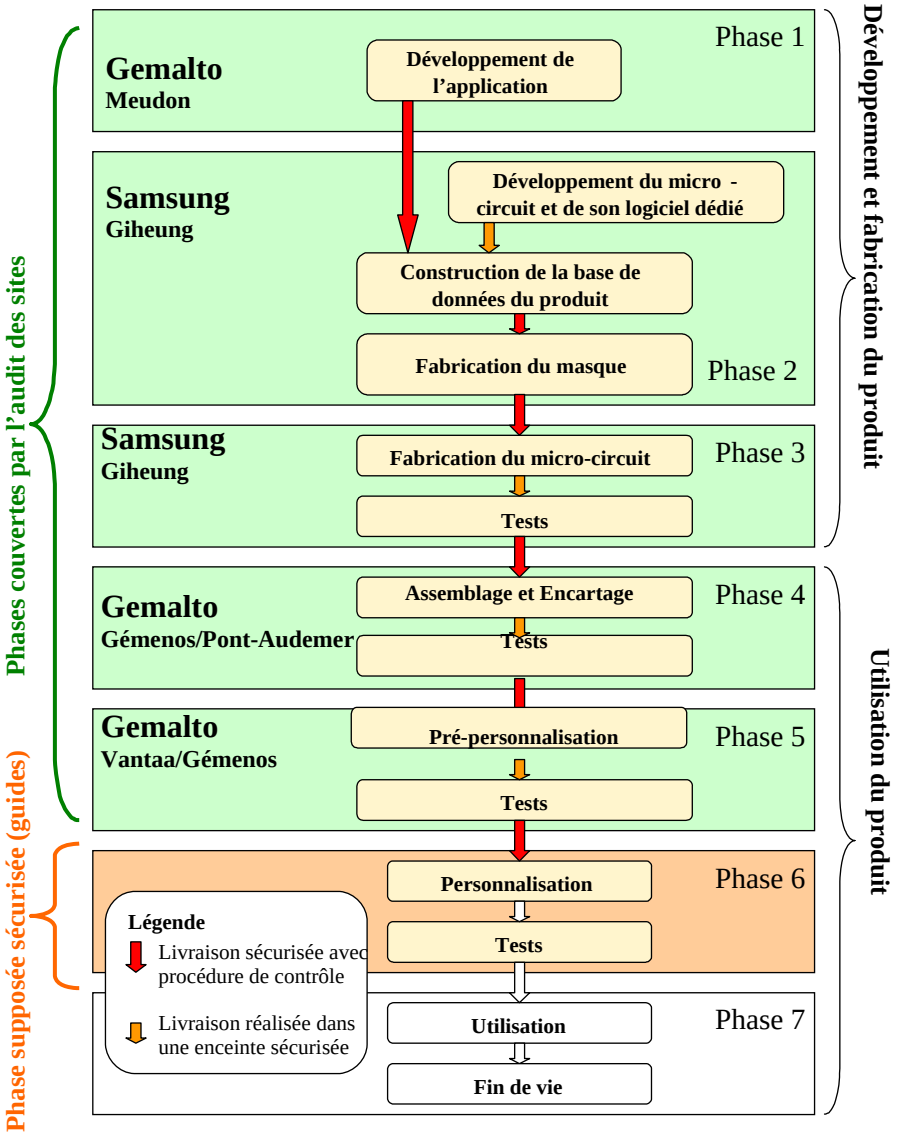

Figure 2 – Cycle de vie du produit

1.2.5. Configuration évaluée

Le certificat porte sur les fonctionnalités suivantes du produit :

Fonctionnalités de l'IC :

- génération de nombre aléatoire (DRNG) ;
- support cryptographique :
  - co-processeur TDES ;
  - co-processeur TORNADO (pour accélérer le RSA jusqu'à 2048 bits).
- bibliothèque RSA Tornado 3.5S (intégration optionnelle à la fabrication, non utilisée par Gemalto) ;
- interface ISO7816 ;
- protection mémoire (MPU) ;
- contrôle d'accès ;

- protection contre les émanations et les attaques par observation via des canaux cachés ;
- protection contre les violations des conditions environnementales ;
- non-réversibilité du mode test et mode normal.

Fonctionnalités de la plateforme Java Card :

- installation sécurisée des applications ;
- pare-feu (permet en outre d'assurer le cloisonnement des applications) ;
- contrôle d'intégrité des biens sensibles ;
- implémentation de la cryptographie (bibliothèque Gemalto pour RSA-1024 à 2048, RSA CRT, SHA-1 et SHA-256) ;
- gestion des clés ;
- communications sécurisées ;
- authentification ;
- gestion de la protection des biens sensibles contre les émanations et les attaques physiques ;
- implémentation de contre-mesures au sein de l'OS contre les attaques par observation ou injections de faute.

Fonctionnalités de l'applet CIE/CNS (SSCD2 & SSCD3) :

- gestion des authentifications ;
- gestion des opérations et contrôle d'accès :
  - création de signatures ;
  - génération de données de création et vérification de signatures ;
  - import et stockage de données de création de signatures ;
  - export de données de vérification de signatures.
- gestion de la cryptographie ;
- gestion de l'intégrité des données sensibles ;
- gestion des communications sécurisées.

Le produit évalué comporte des applications faisant partie de la TOE (décrites au §1.2.3) et d'autres hors TOE décrites ci-dessous :

- des applications installées sur le produit et instanciables :
  - MPCOS v3.8 développée par GEMALTO ;
  - OATH v2.10 développée par GEMALTO ;
  - PayPass MCHIP Select v2.7 développée par GEMALTO ;
  - Biomatch J API v3.0.1 1 Cryptomanager v2.0 développée par Precise Biometrics.
- des applications installées sur le produit mais qui ne sont pas instanciables (points d'entrée désactivés).

L'ensemble de ces applications a été pris en compte dans l'analyse de vulnérabilité.

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].
Pour les composants d'assurance supérieurs au niveau EAL4, des méthodes propres au centre d'évaluation, validées par l'ANSSI 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 (cf. [Certif_IC]).

Cette évaluation a ainsi pris en compte les résultats de l'évaluation (cf. [RTE_IC]) du microcontrôleur « S3CC91C, révision 0, avec bibliothèque RSA Tornado 3.5S » au niveau EAL4 augmenté des composants ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, conformément à sa cible de sécurité [ST_IC], basée sur le profil de protection de référence BSI-PP-0002-2001 [PP-0002]. Ce microcontrôleur a été certifié par le BSI le 10 septembre 2007 sous la référence BSI-DSZ-CC-0451-2007 (cf. [Certif_IC]).
Le niveau de résistance du microcontrôleur a été confirmé le 1er février 2011 dans le cadre du processus de surveillance.

L'évaluation s'appuie également sur des résultats déjà obtenus lors des évaluations ayant abouti aux certifications [2008/01] et [2009/56] (produits similaires mais avec un autre composant) et [2008-45] (passeport EAC). Une réutilisation des résultats a principalement été validée vis-à-vis de l'environnement de développement, du système de gestion de configuration et procédures de livraison, ainsi que des audits de sites de production réalisés par le même CESTI Serma Technologies et le CESTI allemand *TÜV Informationstechnik GmbH* (TÜV It).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 24 juin 2010, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques selon les référentiels techniques [REF-CRY] de l'ANSSI, n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA_VLA visé.

2.4. Analyse du générateur d'aléas

Le générateur d'aléas utilisé par le produit final est celui proposé par le produit hôte (voir rapport de certification du certificat composant (cf [CERTIF_IC]).

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 CIE/CNS 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 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [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 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puces et les dispositifs similaires, 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, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

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[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.

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 of 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

Références documentaires du produit évalué

[2008/01]	Rapport de certification : Plateforme Java Card MultiApp ID, Microcontrôleur SLE66CX680PE - A13 masqué par le logiciel MultiApp ID v.1.0, Référence : DCSSI-2008/01, 13 février 2008, SGDN/DCSSI.
[2008/45]	Rapport de certification : Produits eTravel EAC version 1.1 (version 01 02) sur composants P5CD080 et P5CD144, Référence : DCSSI-2008/45, 18 décembre 2008, SGDN/DCSSI.
[2009/56]	Rapport de certification : Carte à puce Multiapp ID IAS ECC : applet de signature v4.2.7.A chargée sur la plate-forme Java Card Multiapp v1.0 avec correctif v1.2 masquée sur microcontrôleur NXP P5CD144 VOB, Référence : ANSSI-CC-2009/56, 17 février 2010, SGDSN/ANSSI.
[Certif_IC]	Rapport de certification : S3CC91C, *16-Bit RISC Microcontroller for Smart Card, version 0,* Référence : BSI-DSZ-CC-0451-2007, 10 septembre 2007, BSI.
[RTE_IC]	*ETR-Lite for composition (initial)* : ETR-LITE S3CC91C, Version 2.0, 28 août 2007, Tüv-IT / BSI ; *ETR-Lite for composition* : ETR-LITE S3CC91C, Version 4.0, 25 janvier 2011, Tüv-IT / BSI.
[ST_IC]	Cible de sécurité du microcontrôleur : *Security Target of S3CC91C 16-bit RISC Microcontroller for Smart Cards*, Version 1.0, 9 août 2007, Samsung Electronics.
[ST]	Cible de sécurité de référence de la plateforme pour l'évaluation : *Adriatic Platform Security Target*, Version 1.5, ref. D1077228, 19 novembre 2008, Gemalto ;

	Cible de sécurité de référence de l'applet pour l'évaluation : Adriatic-CIE Security Target, Version 1.8, ref. D1077254, 7 avril 2011, Gemalto ; Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : MultiApp ID CIE/CNS Security Target, Creation from evaluated ST (V1.8), 7 avril 2011, Gemalto.
[RTE]	Rapport technique d'évaluation : *Evaluation Technical Report – ADRIATIC-CIE Project*, Référence : ADRIATIC-CIE_ETR_v1.0 / 1.0, 24 juin 2010, Serma Technologies. *External Note* – ADRIATIC-CIE Project, Référence : ADRIATIC-C_NOTE_06_v1.0, 8 avril 2011, Serma Technologies.
[CONF]	La liste de configuration est constituée des documents suivants : Adriatic-CIE LIS : Configuration List, Version 1.1, référence D1167178, 21 juin 2010, Gemalto.
[GUIDES]	Guide d'administration et d'utilisation du produit : - ADRIATIC-CIE Administrator Guide, Version 1.6, référence D1081609, 3 juin 2010, Gemalto ; - ADRIATIC-CIE User Guide, Version 1.3, référence D1081421, 3 juin 2010, Gemalto. Manuels de référence : - Personalization manual – CIE Italy Step 2 applet, Version 0.8, référence D1068730, 26 juin 2010, Gemalto ; - Software requirement specification of CIE/CNS, Version B22, référence D1063806, 26 juin 2010, Gemalto ; Recommandations du composant S3CC91C : - Application Note DRNG Software, Version 2.0, 13 décembre 2007, Samsung Electronics ; - Application Note RSA Crypto Library with TORNADO V3.5S, Version 1.10, 21 juin 2007, Samsung Electronics ; - Security Application Note, S3CC91C, Version 1.3, Samsung Electronics.
[PP0002]	*Protection Profile - Smart Card IC Platform Version 1.0, 11 July 2001*.

	Certifié par le BSI *(Bundesamt für Sicherheit in der Informationstechnik)* sous la référence BSI-PP-0002-2001.
[PP0005]	*Protection Profile - Secure Signature-Creation Device Type 2, Version: 1.04, 25 July 2001*. Certifié par le BSI *(Bundesamt für Sicherheit in der Informationstechnik)* sous la référence BSI-PP-0005-2002.
[PP0006]	*Protection Profile - Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001*. Certifié par le BSI *(Bundesamt für Sicherheit in der Informationstechnik)* sous la référence BSI-PP-0006-2002.

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-2008-04-001 version 2.5 revision 1, April 2008.
[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.
[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010, voir www.ssi.gouv.fr
[AIS 34]	Application Notes and Interpretation of the Scheme - Evaluation

	Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004, BSI (Bundesamt für Sicherheit in der Informationstechnik)