



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-2009/07

MultiApp ID Citizen 72K (Generic configuration)

*Composant S3CC91C masqué par la plateforme JC/GP
MultiApp v1.1 supportant l'applet de signature
électronique IAS Classic v3.0*

Paris, le 23 Avril 2009

*Le Directeur central de la sécurité des
systèmes d'information*
[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 présumées 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.gouv.fr

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification	DCSSI-2009/07	
Nom du produit	MultiApp ID Citizen 72K (Generic configuration)	
Référence/version du produit	Référence T1003982 Composant S3CC91C en révision 0, masqué par la plateforme JC/GP MultiApp en version 1.1, supportant l'applet de signature électronique IAS Classic version 3.0	
Conformité à un profil de protection	BSI-PP0005-2002: SSCD Type 2 Version 1.04 BSI-PP0006-2002: 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	
Développeurs	Gemalto La Vigie, Avenue du Jjubier Z.I. Athelia IV, 13705 La Ciotat, France	Samsung Electronics La Boursidière, RN186, Bat. Jura BP202, 92357 Le Plessis Robinson, France
Commanditaire	Gemalto La Vigie, Avenue du Jjubier Z.I. Athelia IV, 13705 La Ciotat, 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	6
1.1. PRESENTATION DU PRODUIT	6
1.2. DESCRIPTION DU PRODUIT EVALUE	6
1.2.1. <i>Identification du produit</i>	7
1.2.2. <i>Services de sécurité</i>	7
1.2.3. <i>Architecture</i>	7
1.2.4. <i>Cycle de vie</i>	8
1.2.5. <i>Configuration évaluée</i>	10
2. L’EVALUATION	12
2.1. REFERENTIELS D’EVALUATION	12
2.2. TRAVAUX D’EVALUATION	12
2.3. ANALYSE DE LA RESISTANCE DES MECANISMES CRYPTOGRAPHIQUES	12
3. LA CERTIFICATION	13
3.1. CONCLUSION	13
3.2. RESTRICTIONS D’USAGE.....	13
3.3. RECONNAISSANCE DU CERTIFICAT	13
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	13
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i>	14
ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT.....	15
ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	16
ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION	18

1. Le produit

1.1. Présentation du produit

Le produit évalué est la carte *MultiApp ID Citizen 72K*, dans sa configuration générique. La référence du produit est « IAS Classic v3.0 / MultiApp v1.1 T1003982 on S3CC91C rev.0 ». Cette carte à puce est destinée à être utilisée comme dispositif sécurisé de création de signature électronique (SSCD) de type 2 et 3.

Cette carte est constituée d'une part 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'autre part, une plateforme ouverte Java MultiApp version 1.1, développée par Gemalto conformément aux spécifications Java Card v2.2.1 et Global Platform v2.1, qui inclut un système d'exploitation, est embarquée sur le composant S3CC91C. Cette plateforme supporte plusieurs applets, elles-mêmes développées par Gemalto indépendamment du composant sous-jacent. Ces applets sont installées en ROM ou en EEPROM. En particulier, l'applet IAS Classic version 3.0, stockée en ROM, est l'applet principale du produit et fournit les services de signature électronique.

Le produit embarque plusieurs autres applets. Seule l'applet IAS Classic est instanciée. Le produit est alors diversifié suivant différentes configurations (cf. §1.2.5) combinant l'instanciabilité des autres applets. Une applet qui n'est pas instanciée, ni instanciable, est alors désactivée.

L'ensemble des applets instanciables n'est pas dans le périmètre de l'évaluation mais a néanmoins été pris en compte dans l'analyse de vulnérabilité.

La configuration (cf. §1.2.5) correspondant à la présente certification, ne définit comme instanciable que trois applets stockées en ROM : MPCOS, OATH et Biomatch C API & Cryptomanager. Les autres applets en ROM sont désactivées et il n'y a aucune applet en EEPROM.

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 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 la commande « Get Data ». Parmi les valeurs retournées, on trouve :

- Card Identity Data = B0 85 13 1C 01 04 42 50 00 C8 00 ;
- Gemalto Family Name: Java Card: B0h ;
- Gemalto OS Name: MultiApp ID v1.1: 85h ;
- Gemalto Mask Number: MSA081: 13h ;
- Gemalto Product Name: IAS CC configuration: 1Ch ;
- Gemalto Flow version: 01h ;
- Gemalto filter set: Filter 01, version 4: 04h ;
- Chip Manufacturer: Samsung: 4250h ;
- Chip version: S3CC91C: 00C8h ;

Les valeurs assignées à ces identifiants sont définies dans les guides utilisateurs et administrateurs du produit (Cf. [GUIDES]).

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’importation 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.

1.2.3. Architecture

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

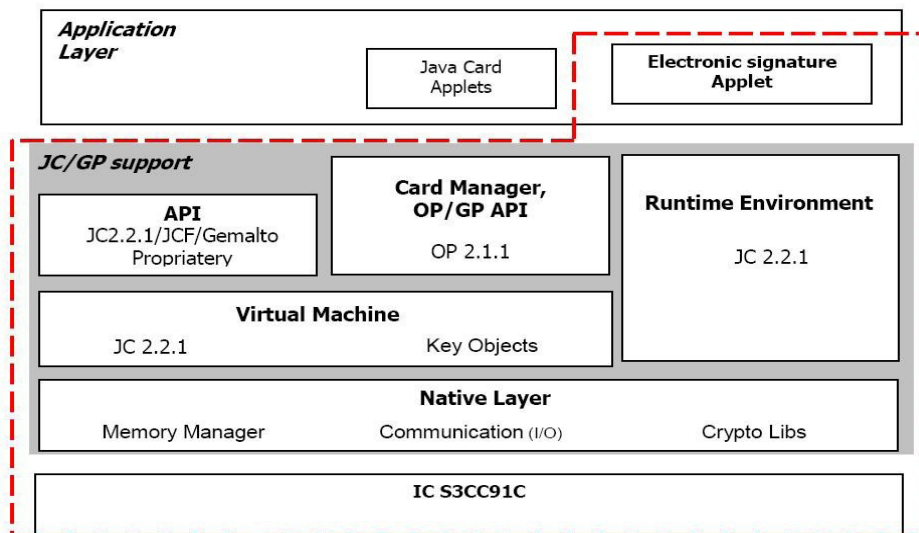


Figure 1 – Architecture du produit

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 ouverte JavaCard/GlobalPlatform : MultiApp, version 1.1, munie d'une JCVM ;
- de l'applet IAS Classic v3.0 de signature électronique avec ses données ;
- d'autres applets instanciables en dehors du périmètre de l'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 impliquées dans le développement sont les suivantes :

- Gemalto Meudon : site R&D pour le développement de l'OS, la plateforme Java Card, l'applet IAS Classic, puis la conception dédiée à la phase de pré-personnalisation ;
- Samsung Electronics Giheung (wafer line 6, Korea) pour la conception et fabrication de l'IC.

D'autres sites Gemalto interviennent lors des phases suivantes :

- Gemalto Gémenos et Pont-Audemer : sites de production (back-up) pour l'assemblage en micro-module ;
- Gemalto Vantaa et Gémenos : sites de production (backup) pour l'encartage et la phase de pré-personnalisation ;

Tous ces sites ont été audités (cf. §2.2) de manière à garantir la satisfaction de la famille d'exigences d'assurance ALC_DVS.

Les phases 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.

Phase 2 (Samsung Giheung¹) :

- 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*).

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).

Phase 4 (Gemalto Gémenos / Pont-Audemer) :

- assemblage des puces en micro-module.

Phase 5 (Gemalto Vantaa / Gémenos) :

- encartage (*packaging*) ;
- pré-personnalisation et chargement éventuel d'un patch en EEPROM.

Phase 6 (hors évaluation) :

- personnalisation.

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]).

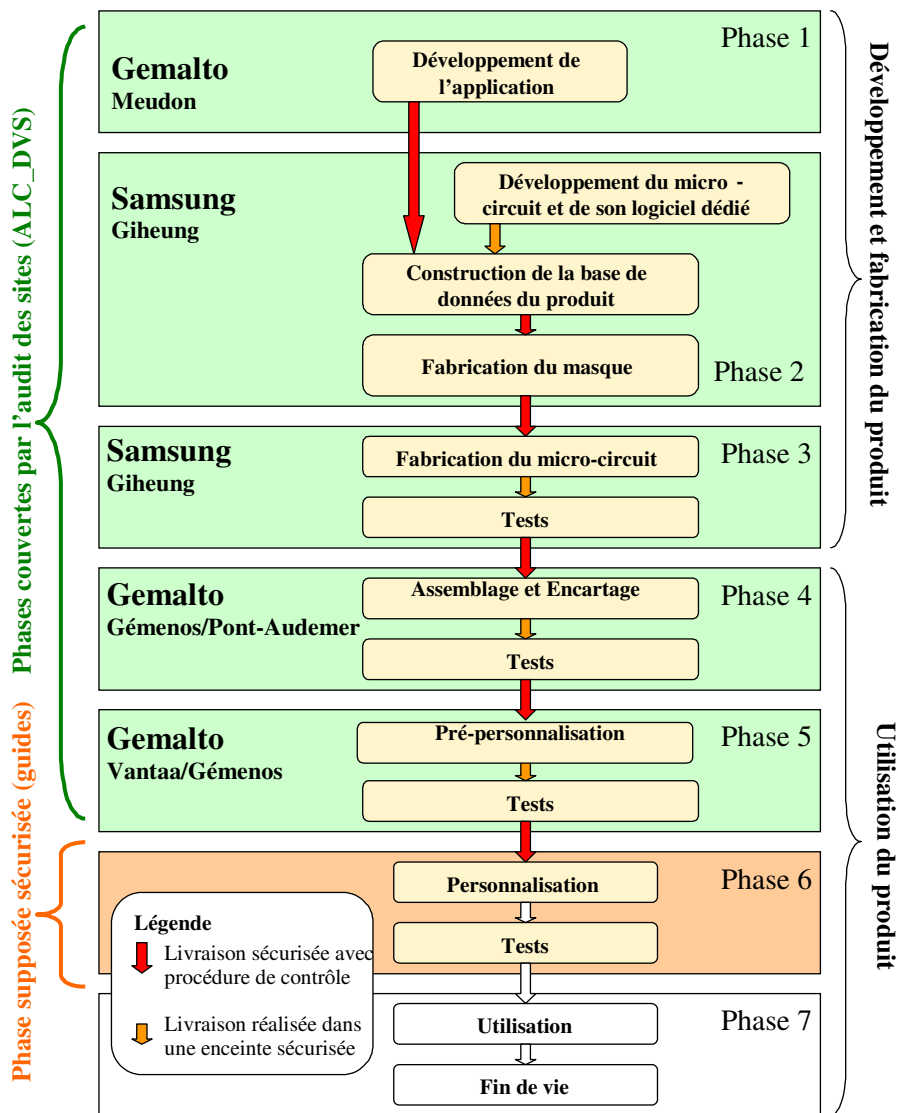


Figure 2 – Cycle de vie du produit

1.2.5. Configuration évaluée

La configuration évaluée, dite générique, est nommée *Generic configuration*. Cette configuration instancie l'applet IAS Classic et définit comme instanciable les trois applets MPCOS, OATH et Biomatch C API & Cryptomanager. Les autres applets en ROM sont désactivées et il n'y a aucune applet en EEPROM.

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 violations physiques ;
- implémentation de contre-mesures au sein de l'OS contre les attaques par observation ou injections de faute.

fonctionnalités de l'applet IAS Classic (SSCD2 & SSCD3) :

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

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 (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]).

L'évaluation s'appuie également sur des résultats déjà obtenus lors des évaluations ayant abouti aux certifications [2008/04] (produit similaire mais avec un autre composant HW et un autre OS) 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-IT.

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 8 janvier 2009, 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 Citizen 72K (Generic configuration)* 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] au chapitre 4.2 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 1999 permet la reconnaissance, par les pays signataires de l'accord², 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 :



² 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 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 signataires³, 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 :



³ 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

[2008/04]	Rapport de certification : <ul style="list-style-type: none"> - MultiApp ID CIE/CNS SSCD, Microcontrôleur SLE66CX680PE - A13 masqué par l'application CIE/CNS Référence : DCSSI-2008/04, 13 mars 2008, SGDN/DCSSI
[2008/45]	Rapport de certification : <ul style="list-style-type: none"> - Produits eTravel EAC version 1.1 (version 01 02) sur composants P5CD080 et P5CD144. Référence : DCSSI-2008/45, 18 décembre 2008, SGDN/DCSSI
[Certif_IC]	Rapport de certification : <ul style="list-style-type: none"> - S3CC91C, 16-Bit RISC Microcontroller for Smart Card, version 0. Référence : BSI-DSZ-CC-0451-2007 BSI
[RTE_IC]	ETR-Lite for composition : <ul style="list-style-type: none"> - ETR-LITE S3CC91C, Version 2.0, 28 Aug. 07, Tüv-IT / BSI
[ST_IC]	Cible de sécurité du microcontrôleur : <ul style="list-style-type: none"> - Security Target of S3CC91C 16-bit RISC Microcontroller for Smart Cards, Version 1.0, 9 Aug. 07, Samsung Electronics
[ST]	Cible de sécurité de référence de la plateforme pour l'évaluation : <ul style="list-style-type: none"> - Adriatic Platform Security Target, Version 1.5, ref. D1077228, 2008 Gemalto Cible de sécurité de référence de l'applet pour l'évaluation : <ul style="list-style-type: none"> - Adriatic IAS Classic Security Target, Generic Configuration Version 1.6, ref. D1077227_Generic, 2008 Gemalto
[RTE]	Rapport technique d'évaluation : <ul style="list-style-type: none"> - Evaluation Technical Report - Project: Adriatic IAS, Référence : ADRIATIC-IAS_ETR_v1.0 / 1.0, Serma Technologies

[CONF]	<p>La liste de configuration est constituée des documents suivants :</p> <ul style="list-style-type: none"> - Adriatic IAS Configuration List, Version 1.1, référence D1109385, Gemalto
[GUIDES]	<p>Guide d'administration et d'utilisation du produit :</p> <ul style="list-style-type: none"> - Platform Administrator's and user's guide, Version 1.2, référence D1077605, Gemalto - IAS Classic Administrator's and user's guide, Version 1.1, référence D1077604, Gemalto <p>Reference Manual :</p> <ul style="list-style-type: none"> - IAS Classic Applet v3, Reference Manual, Référence DOC116499E, Gemalto - MultiApp ID Combi and Derived Products, Reference Manual, Référence DOC116422A, Gemalto <p>Recommandations du composant S3CC91C :</p> <ul style="list-style-type: none"> - Application Note DRNG Software, Version 2.0, Samsung Electronics - Application Note RSA Crypto Library with TORNADO V3.5S, Version 1.10, Samsung Electronics - Security Application Note, S3CC91C, Version 1.2, Samsung Electronics
[PP0002]	Protection Profile - Smart Card IC Platform Version 1.0. <i>Certifié par le BSI sous la référence BSI-PP-0002-2001.</i>
[PP0005]	Protection Profile - Secure Signature-Creation Device Type 2, Version: 1.04, 25 July 2001. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0005-2002.</i>
[PP0006]	Protection Profile - Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001. <i>Certifié par le BSI sous la référence BSI-PP-0006-2002.</i>

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]	<p>Common Criteria for Information Technology Security Evaluation :</p> <p>Part 1: Introduction and general model, August 2005, version 2.3, ref CCMB-2005-08-001;</p> <p>Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002;</p> <p>Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003.</p> <p>Le contenu des Critères Communs version 2.3 est identique à celui de la Norme Internationale ISO/IEC 15408:2005.</p>
[CEM]	<p>Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004.</p> <p>Le contenu de la CEM version 2.3 est identique à celui de la Norme Internationale ISO/IEC 18045:2005.</p>
[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 de niveau de robustesse standard, version 1.10 du 19 décembre 2006, réf: 2741/SGDN/DCSSI/SDS/Crypto.



[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)
----------	---