Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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-2009/56

Carte à puce Multiapp ID IAS ECC

Paris, le 17 février 2010

Le directeur général de l'agence nationale
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 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-2009/56

Nom du produit

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/version du produit

Version applet : v4.2.7.A
Version plate-forme Java Card Multiapp : v1.0
Version correctif : v1.2
Version microcontrôleur : V0B

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 3.1

Niveau d'évaluation

EAL 4 augmenté
ALC_DVS.2, AVA_VAN.5

Développeur(s)

Gemalto SA[1]
6 rue de la Verrerie
92197 Meudon, France

NXP Semiconductors GmbH[1]
Stresemannallee 101
D-22502 Hamburg, Germany

Commanditaire

Gemalto SA
6 rue de la Verrerie, 92197 Meudon, France

Centre d'évaluation

Serma Technologies
30 avenue Gustave Eiffel, 33608 Pessac, France
Tél : +33 (0)5 57 26 08 75, mél : e.francois@serma.com

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit est reconnu au niveau EAL4.

[1] : il s'agit des sites principaux.

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 :

- 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 à puce Multiapp ID IAS ECC, applet de signature v4.2.7.A chargée sur plate-forme Java Card Multiapp v1.0 avec correctif v1.2 masquée sur microcontrôleur NXP P5CD144 VOB**,** développée par Gemalto.

La TOE (*Target Of Evaluation* – cible d'évaluation) est une carte à puce destinée à être utilisée dans le cadre de l'administration électronique. Elle répond aux caractéristiques des dispositifs sécurisés de création de signature électronique (SSCD - *Secure Signature Creation Device*), dont les fonctionnalités applicatives sont offertes par l'application IAS ECC (*Identification Authentication Signature / European Citizen Card* - identification authentification signature / carte du citoyen européen) qui s'exécute sur la plateforme Java Card Multiapp.

L'application IAS ECC couvre les domaines de l'identité, de la signature électronique et du stockage de données et est compatible avec les spécifications E-sign (cf. [E-sign]).

Elle offre les deux principales fonctions attendues des produits SSCD type 2 et type 3 :

- génération de SCD / SVD (*Signature Creation Data / Signature Verification Data* – données de création de signature (la clé secrète) / données de vérification de signature (la clé publique)) ;
- création de signature.

1.2. Description du produit

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

Elle est strictement conforme[1] aux deux profils de protection [BSI-PP-0005-2002] - SSCD Type 2 - et [BSI-PP-0006-2002] - SSCD Type 3.

[1] Bien que les deux profils de protection [BSI-PP-0005-2002] - SSCD Type 2 - et [BSI-PP-0006-2002] - SSCD Type 3 ont été écrits en CCv2.1, qui ne spécifiaient pas (encore) la notion de conformité stricte (ou démontrable), on admet que la [ST], écrite suivant les CCv3.1, déclare une conformité stricte dans la mesure où elle reprend intégralement les exigences de ces deux profils de protection, moyennant une légère adaptation des critères CC qui est explicitée dans la [ST] au §2.4 PP REFINEMENTS.

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 :

Sujet concerné	*Configuration concernée*	*Origine*
Nom commercial	MultiApp ID IAS ECC	Gemalto
Label interne de la TOE	T1009875	Gemalto
Référence du microcontrôleur	P5CD144 VOB	NXP
Référence de la plate-forme	- Hardmask V1.0 (ref. MPH076) - Correctif V1.2	Gemalto
Référence de l'applet	Applet IAS ECC V4.2.7.A	Gemalto

Le logiciel embarqué dans la TOE peut être identifiée de façon unique au travers des données renvoyées par la commande *Get Data* (demande de données) :

- pour la partie plate-forme de la TOE, on obtient **B0 85 14 21 01 12 40 70 51 44 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00**, où
  - « **BO** » indique le nom de famille Gemalto du produit, ici, Java Card ;
  - « **85** » indique le nom de la plate-forme Gemalto, ici, MultiApp ID v1.0 ;
  - « **14** » indique le numéro du masque Gemalto, ici, MPH076 ;
  - « **21** » indique le nom du produit Gemalto, ici, la configuration IAS ECC ;
  - « **01** » indique la version du flux (script de pré-personnalisation) Gemalto ;
  - « 12 » indique la version du correctif, ici, v1.2 ;
  - « **40 70** » identifie le fabricant du microcontrôleur, ici, NXP ;
  - « **51 44** » identifie le composant, ici, P5CD144 ;
  - « **00 00** » sont des octets réservés pour un usage futur ;
  - le reste des octets à « **00** » sera renseigné par des données de fabrication et de personnalisation par les acteurs qui interviendront à ce moment du cycle de vie du produit ;
- pour la partie applet IAS ECC de la TOE, on obtient A0 0C **49 41 53 20 45 43 43 20 31 2E 30 31** A1 07 **34 2E 32 2E 37 2E 41**, où :
  - « **49 41 53 20 45 43 43 20 31 2E 30 31** » indique en ASCII (*American standard Code for Information Interchange* – code américain standardisé pour l'échange d'information) le label de l'applet (IAS ECC 1.01) ;
  - « **34 2E 32 2E 37 2E 41** » indique en ASCII la version de l'applet (4.2.7.A).

Ces informations permettent de tracer tous les éléments constitutifs de la TOE (microcontrôleur, masque, correctif et applet). Elles permettent d'identifier correctement et de façon unique la TOE. Elles ont pu être vérifiées sur les échantillons de la TOE reçus lors de l'évaluation.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont constitués :

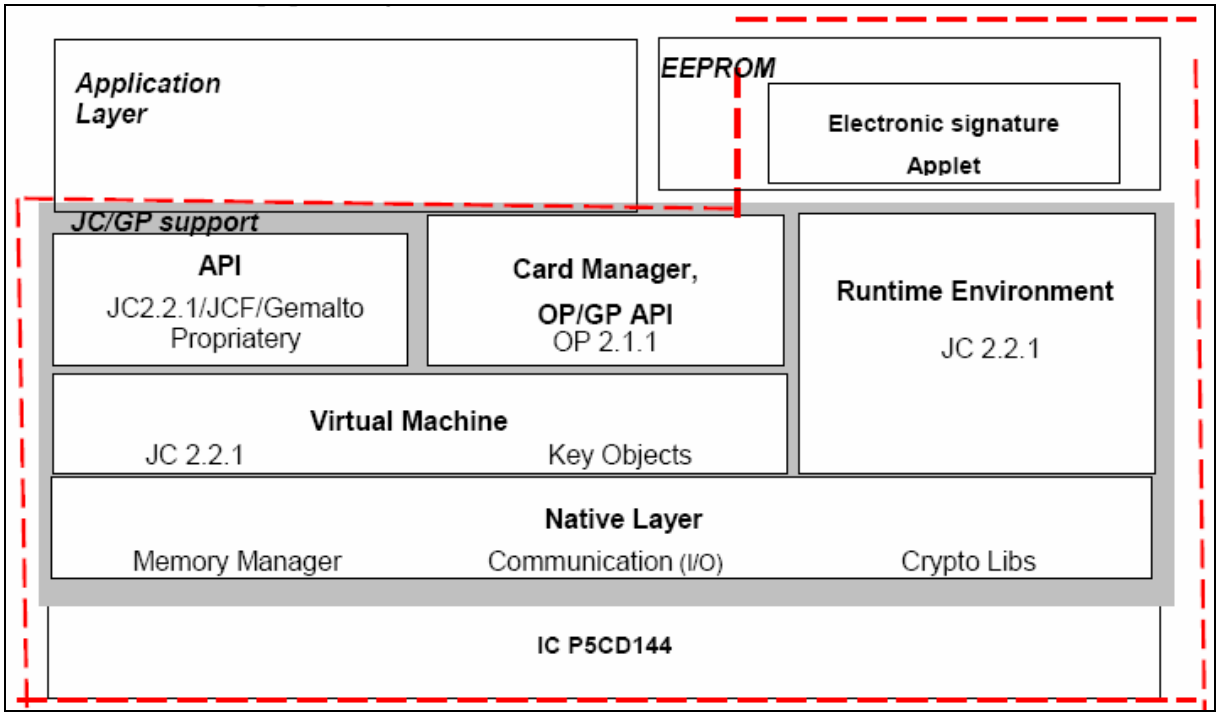
- de ceux fournis par la partie plate-forme de la TOE (détaillés dans [ST] au chapitre §7.1) :
  - protection contre les fuites par canaux auxiliaires pour protéger le RAD (*Reference Authentication Data* – données d'authentification de référence) et le SCD ;
  - protection des opérations de la carte (en particulier contrôle de cohérence des opérations en fonction du cycle de vie, gestion des alertes de sécurité levées par le microcontrôleur) ;
- de ceux fournis par l'applet IAS ECC de la TOE (détaillés dans [ST] au chapitre §7.2) :
  - gestion de l'authentification comme celle des différents utilisateurs (rôles) et lors de l'établissement des canaux sécurisés ;
  - gestion de la cryptographie comme la génération, la vérification et la destruction de clés ainsi que les opérations cryptographiques ;
  - contrôle de l'intégrité des données sensibles de l'utilisateur ainsi que celles devant être signées (DTBS – *Data To Be Signed*) ;
  - gestion des opérations et des contrôles d'accès ;
  - gestion des échanges sécurisés des données utilisateur.

1.2.3. Architecture

Le produit est constitué :

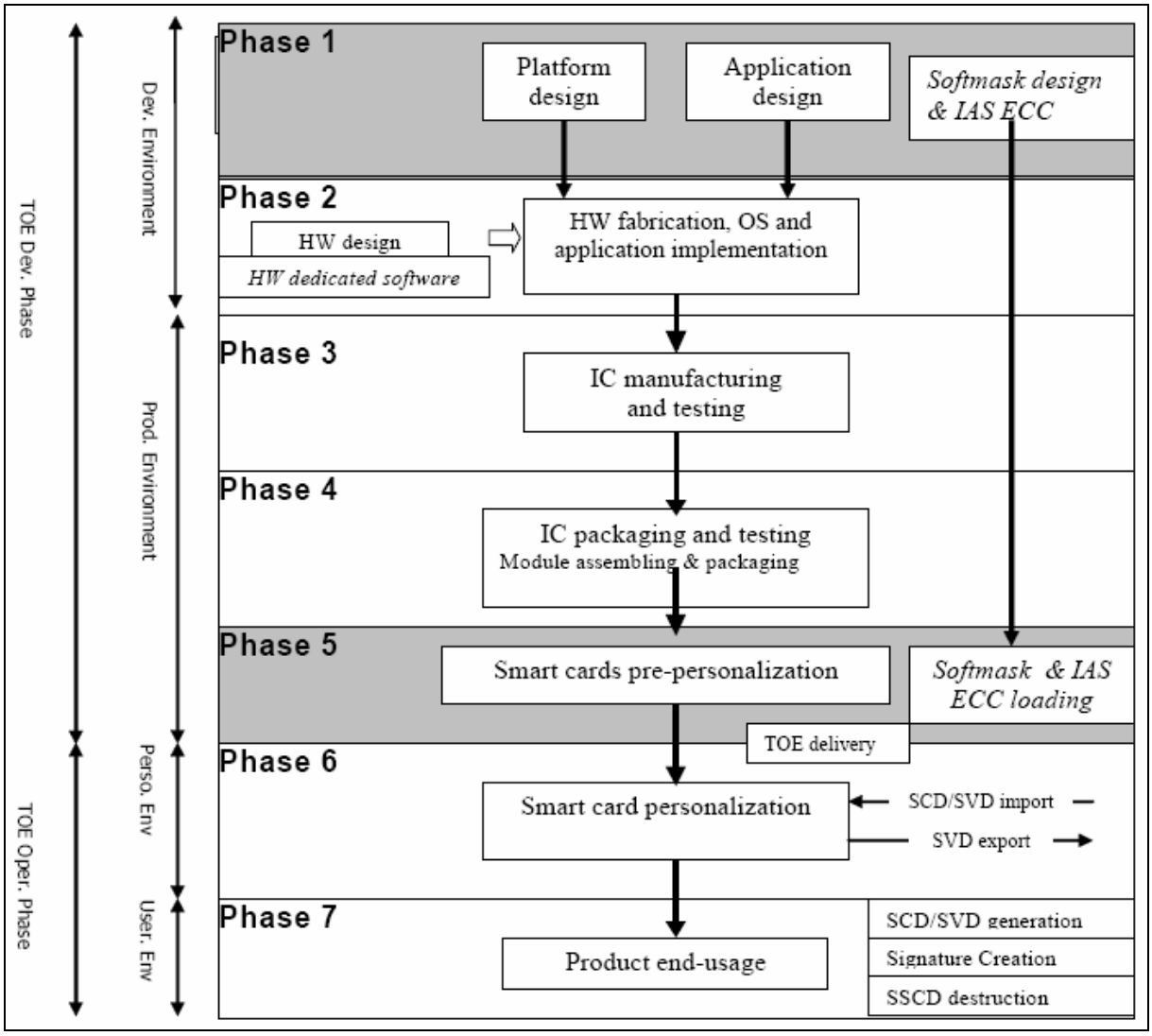
- d'une applet IAS ECC chargée en mémoire EEPROM ;
- d'un correctif (v1.2) de la plate-forme chargé en mémoire EEPROM ;
- d'une plate-forme Multiapp masquée en ROM ;
- d'un microcontrôleur.

Cette architecture peut être représentée de la façon suivante :



1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant (cf. [ST] au chapitre §1.4.3 *TOE life-cycle*) :



Comme le montre ce schéma, le point de livraison de la TOE (TOE *delivery*) s'effectue à la fin de la phase 5 (pré-personnalisation), après chargement du correctif de la plate-forme et de l'applet que son installation. Toutes les phases qui précèdent ce point de livraison ont été évaluées en considérant la TOE en construction, la phase 6 (personnalisation) a été évaluée sous couvert des guides, le produit évalué est celui utilisé en phase 7 (utilisation).

L'applet, la plate-forme et son correctif ont été développés (phase 1) sur le site de :

Gemalto Meudon

6 rue de la Verrerie
92197 Meudon,
France.

La pré-personnalisation (phase 5), durant laquelle le chargement de l'applet est effectué, ainsi que l'assemblage et le packaging (phase 4), ont été effectués sur les sites de Gemalto Gemenos et Vantaa, l'un étant le secours de l'autre :

Gemalto Gemenos

Avenue du Pic de Bretagne – BP 100
13881 Gémenos Cedex,
France.

Gemalto Vantaa

Turvalaaksonkaari 2 - P.O. Box 31
FI-01741 Vantaa,
Finlande

Le microcontrôleur a été développé et fabriqué par NXP sur ses sites (cf. [BSI-DSZ-CC-0411-2007-MA-04]), dont le principal est :

NXP Semiconductors GmbH1

Stresemannallee 101
D-22502 Hamburg
Allemagne

Pour l'évaluation, l'évaluateur a considéré :

- comme administrateur du produit :
  - le fabricant de la carte (*Smart Card product manufacturer*) : qui charge notamment l'applet et le correctif de la plate-forme ;
  - le personnalisateur (*Personalizer*) : qui charge notamment les données de l'utilisateur final ;
  - l'émetteur de la carte (*Card Issuer*) : typiquement une administration nationale, qui gère en particulier la personnalisation de la carte, et dans le cadre de l'application de la signature électronique, qui crée le PIN (*Personal Identification Number*) de l'utilisateur final et, le cas échéant, qui importe le premier SCD dans la TOE ;
- comme utilisateur du produit :
  - le porteur de la carte, qui est aussi le signataire dans le cadre de l'application de signature, et en tant que tel, qui pourra effectuer les opérations de signature électronique avec l'aide de son SCD, il pourra également détruire son SCD ou générer un nouveau couple de SCD/SVD. A la première utilisation, le signataire devra changer son code PIN. Un nouveau PIN est également nécessaire suite à la génération d'une nouvelle paire SCD/SVD.

Ces différents rôles sont détaillés dans la [ST] au chapitre §1.4.5 *The actors and roles*.

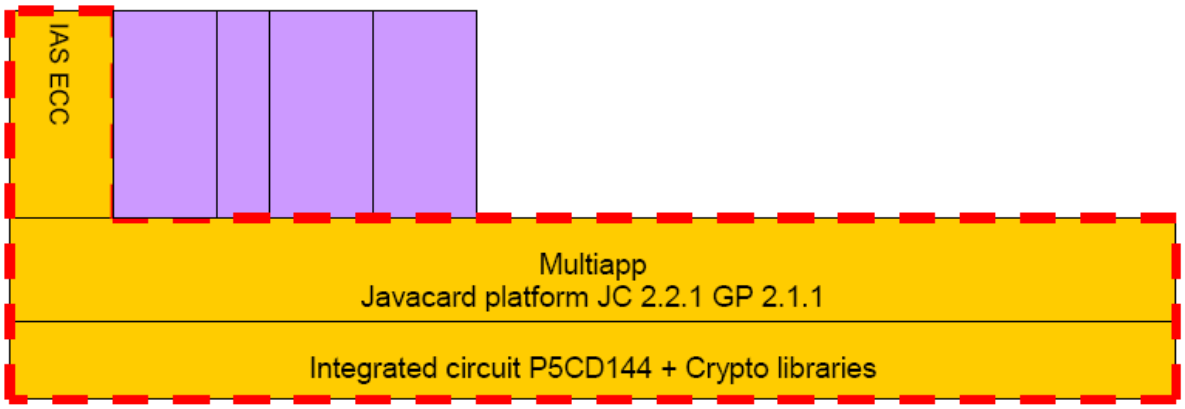
1.2.5. Configuration évaluée

La configuration considérée pour l'évaluation est la carte à puce constituée du microcontrôleur NXP P5CD144 (VOB), en configuration « à contact », et du logiciel embarqué comprenant :

- la partie de plate-forme Java Card MultiApp (v1.0) offrant les fonctionnalités Card Manager et GlobalPlatform (le reste est hors périmètre de l'évaluation) ;
- le correctif de la plate-forme (v1.2) ;
- l'applet de signature électronique (v4.2.7.A) instanciée et activée.

Le masque de la carte peut comporter d'autres applications en ROM (*Read Only Memory*). Celles-ci ne font pas partie du périmètre de l'évaluation et sont désactivées dans cette configuration.

Le schéma ci-après récapitule ces points et montre, en ligne pointillée, le périmètre inclus dans l'évaluation :



2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1** [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [CC IC] et [CC AP] ont été appliqués.

2.2. Travaux d'évaluation

L'évaluation en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel dans le microcontrôleur déjà certifié par ailleurs.
Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur NXP P5CD144V0B au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, conforme au profil de protection [BSI-PP-0002-2001]. Ce microcontrôleur a été maintenu par le BSI (cf. [BSI-DSZ-CC-0411-2007-MA-04]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 6 janvier 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 a été réalisée par l'ANSSI conformément à son référentiel technique [REF-CRY]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY].

Les mécanismes analysés sont conformes aux exigences du référentiel cryptographique de l'ANSSI (cf. [REF-CRY]) sous réserve du complet respect des guides (cf. [GUIDES]. En particulier, en vue de la qualification[1] du produit, ces [GUIDES] demandent d'utiliser des clés RSA de taille supérieure ou égale à 1 536 bits et d'utiliser l'algorithme SHA-256.

L'évaluation de l'implémentation cryptographique réalisée par l'évaluateur répond aux exigences du processus de qualification[1] au niveau renforcé.

Les résultats de ces analyses ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.5 visé.

2.4. Analyse du générateur d'aléas

Ce générateur a fait l'objet d'une analyse par l'ANSSI.

C'est un générateur physique couplé avec un mécanisme de retraitement cryptographique. Ce mécanisme est reconnu de niveau standard selon le référentiel cryptographique de l'ANSSI (cf. [REF-CRY]).

Concernant le générateur physique, comme il n'est pas accessible depuis la TOE, l'évaluateur n'a pas pu effectuer d'analyses statistiques. Toutefois, l'évaluateur du microcontrôleur indique en avoir effectué lors de l'évaluation qui a conduit à la certification du microcontrôleur.

[1] Le processus de qualification d'un produit de sécurité, utilisé dans le schéma français, est décrit sur le site de l'ANSSI (cf. http://www.ssi.gouv.fr/site_article39.html)

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 évalué, carte à puce Multiapp ID IAS ECC, applet de signature v4.2.7.A chargée sur plate-forme Java Card Multiapp v1.0 avec correctif v1.2 masquée sur microcontrôleur NXP P5CD144 VOB**,** développée par Gemalto, 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], en particulier, pour être conforme aux exigences de la qualification du produit :

- d'utiliser des clés RSA de taille supérieure ou égale à 1 536 bits ;
- d'utiliser l'algorithme SHA-256.

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 1999 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Espagne, la Finlande, la France, la Grèce, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

[2] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, 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
ADV Développement	ADV_ARC		**1**	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**4**	**Complete functional specification**
	ADV_IMP				**1**	1	**2**	2	**1**	Implementation representation of the TSF
	ADV_INT					**2**	**3**	3		
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**3**	Basic modular design
AGD Guides d'utilisation	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**1**	1	1	1	1	1	1	**1**	Preparative procedure
ALC Support au cycle de vie	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Production support, acceptance procedures and automation
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**4**	Problem tracking CM coverage
	ADO_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**2**	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**1**	Well defined development tools
ASE Security Target Evaluation	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claim
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended component definition
	ASE_INT	**1**	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	**1**	**2**	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	**1**	**2**	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		**1**	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	**1**	1	1	1	1	1	1	**1**	TOE summary specifications
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**3**	3	**4**	**1**	Testing: security enforcing modules
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independant testing, sample
AVA Estimation des vulnérabilités	AVA_VAN	**1**	**2**	**2**	**3**	**4**	**5**	5	**5**	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - MISTRAL Security Target v1.9, D1111555 Gemalto. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - MultiApp ID IAS ECC - Security Target Jan 6, 2010 Gemalto.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report - MISTRAL Project MISTRAL_ETR_v1.1 / 1.1 Serma Technologies.
[ANA-CRY]	Rapport d'analyse cryptographique de l'ANSSI : Cotation de mécanismes cryptographiques - Qualification MISTRAL, N°2356/SGDN/ANSSI/DR, 22/09/2009.
[CONF]	Liste de configuration - LIS: Configuration List – MISTRAL D1132920, V1.5, 06/01/2010 Gemalto.
[GUIDES]	Guide d'initialisation du produit : - Card Initialization Specification for MultiApp ID v1.0: MPH076 for IAS ECC products D1088720, v1.5 Gemalto. Guide de préparation : - Preparative procedure D1116279, v1.1 Gemalto. Guide d'administration du produit : - Card Personalization Specification requirement for SSCD security evaluation IASECCv4_002_CPS_Req_For_CC_Evaluation, v1.1 Gemalto. Guide d'utilisation du produit : - IAS-ECC Operational user guidance D1115162, v1.1 Gemalto.

[BSI-PP-0005-2002]	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-0005-2002T.*
[BSI-PP-0006-2002]	Protection Profile — Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001. *Certifié par le BSI sous la référence BSI-PP-0006-2002T.*
[BSI-PP-0002-2001]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0002-2001.*
[E-sign]	Application Interface for Smart Cards used as Secure Signature Creation Device CEN/ISSS WS/E-Sign Draft CWA Group K part 1 – Basic requirements. Version 1, Release 9 (17th September 2003) Application Interface for Smart Cards used as Secure Signature Creation Device CEN/ISSS WS/E-Sign Draft CWA Group K part 2 – Additional services. Version 0, Release:19 (12th December 2003)
[BSI-DSZ-CC-0411-2007-MA-04]	Rapport de maintenance BSI délivré le 7 juillet 2009 pour les produits *NXP Smart Card Controller P5CD144V0B, P5CN144V0B and P5CC144V0B each with specific IC Dedicated Software*

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, September 2006, version 3.1, revision 1, ref CCMB-2006-09-001; Part 2: Security functional components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-002; Part 3: Security assurance components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2007, version 3.1, révision 2, ref CCMB-2007-09-004.
[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 1.11 du 24 octobre 2008, voir www.ssi.gouv.fr