



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-2010/52**

**Carte à puce Multiapp ID IAS ECC wafer process :  
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**

*Paris, le 2 AOÛT 2010*

*Le directeur général adjoint de l'agence nationale  
de la sécurité des systèmes d'information*

Le vice-amiral Michel BENEDETTINI  
[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 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](mailto:certification.anssi@ssi.gouv.fr)

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

<i>Référence du rapport de certification</i> <p style="text-align: center;"><b>ANSSI-CC-2010/52</b></p>	
<i>Nom du produit</i> <p style="text-align: center;"><b>Carte à puce Multiapp ID IAS ECC wafer process :  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</b></p>	
<i>Référence/version du produit</i> <p style="text-align: center;"><b>Version applet : v4.2.7.A  Version plate-forme Java Card Multiapp : v1.0  Version correctif : v1.2  Version microcontrôleur : V0B</b></p>	
<i>Conformité à un profil de protection</i> <p style="text-align: center;"><b>[BSI-PP-0005-2002] : SSCD Type 2, version 1.04  [BSI-PP-0006-2002] : SSCD Type 3, version 1.05</b></p>	
<i>Critères d'évaluation et version</i> <p style="text-align: center;"><b>Critères Communs version 3.1</b></p>	
<i>Niveau d'évaluation</i> <p style="text-align: center;"><b>EAL 4 augmenté  ALC_DVS.2, AVA_VAN.5</b></p>	
<i>Développeurs</i> <p style="text-align: center;"><b>Gemalto SA<sup>1</sup>  6 rue de la Verrerie  92197 Meudon, France</b></p>	<p style="text-align: center;"><b>NXP Semiconductors GmbH<sup>1</sup>  Stresemannallee 101  D-22502 Hamburg, Germany</b></p>
<i>Commanditaire</i> <p style="text-align: center;"><b>Gemalto SA  6 rue de la Verrerie, 92197 Meudon, France</b></p>	
<i>Centre d'évaluation</i> <p style="text-align: center;"><b>Serma Technologies  30 avenue Gustave Eiffel, 33608 Pessac, France  Tél : +33 (0)5 57 26 08 75, mél : e.francois@serma.com</b></p>	
<i>Accords de reconnaissance applicables</i> <div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;"> <p><b>CCRA</b></p>  </div> <div style="text-align: center;"> <p><b>SOG-IS</b></p>  </div> </div> <p style="text-align: center;"><b>Le produit est reconnu au niveau EAL4.</b></p>	

<sup>1</sup> 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 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](http://www.ssi.gouv.fr).

# Table des matières

<b>1. LE PRODUIT .....</b>	<b>6</b>
1.1. PRESENTATION DU PRODUIT .....	6
1.2. DESCRIPTION DU PRODUIT .....	6
1.2.1. <i>Identification du produit</i> .....	7
1.2.2. <i>Services de sécurité</i> .....	8
1.2.3. <i>Architecture</i> .....	8
1.2.4. <i>Cycle de vie</i> .....	9
1.2.5. <i>Configuration évaluée</i> .....	11
<b>2. L’EVALUATION .....</b>	<b>12</b>
2.1. REFERENTIELS D’EVALUATION .....	12
2.2. TRAVAUX D’EVALUATION .....	12
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI .....	13
2.4. ANALYSE DU GENERATEUR D’ALEAS.....	13
<b>3. LA CERTIFICATION .....</b>	<b>14</b>
3.1. CONCLUSION .....	14
3.2. RESTRICTIONS D’USAGE.....	14
3.3. RECONNAISSANCE DU CERTIFICAT .....	15
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i> .....	15
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i> .....	15
<b>ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT.....</b>	<b>16</b>
<b>ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE .....</b>	<b>17</b>
<b>ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION .....</b>	<b>19</b>

# 1. Le produit

## 1.1. Présentation du produit

Le produit évalué est la « Carte à puce Multiapp ID IAS ECC wafer process, 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 et NXP.

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 signatures électroniques (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).

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 s'exécute sur la plateforme Java Card Multiapp.

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 privée) / 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<sup>1</sup> aux deux profils de protection [BSI-PP-0005-2002] - SSCD Type 2 - et [BSI-PP-0006-2002] - SSCD Type 3.

---

<sup>1</sup> 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 la 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 :

<i>Sujet concerné</i>	<i>Configuration concernée</i>	<i>Origine</i>
Nom commercial	MultiApp ID IAS ECC wafer process	Gemalto
Label interne de la TOE	T1015174	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 03 12 40 70 51 44 00**, où
  - « **B0** » 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 ;
  - « **03** » indique la version du flux Gemalto pour wafer process ;
  - « **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, c'est-à-dire 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 utilisés lors de l'évaluation.

### 1.2.2. Services de sécurité

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

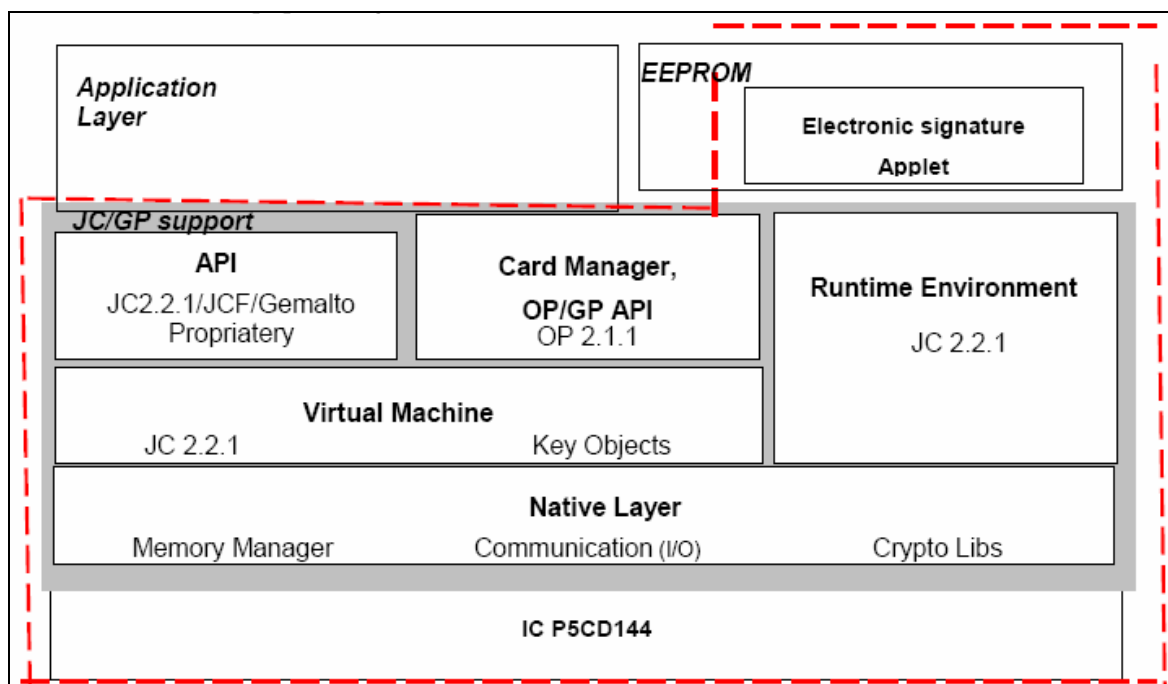
- ceux fournis par la partie plate-forme et microcontrôleur de la TOE (détaillés dans [ST] au chapitre §7.1) :
  - o protection contre les fuites par canaux auxiliaires pour protéger le RAD (*Reference Authentication Data* – données d’authentification de référence) et le SCD ;
  - o protection des opérations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

### 1.2.3. Architecture

Le produit est constitué par :

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

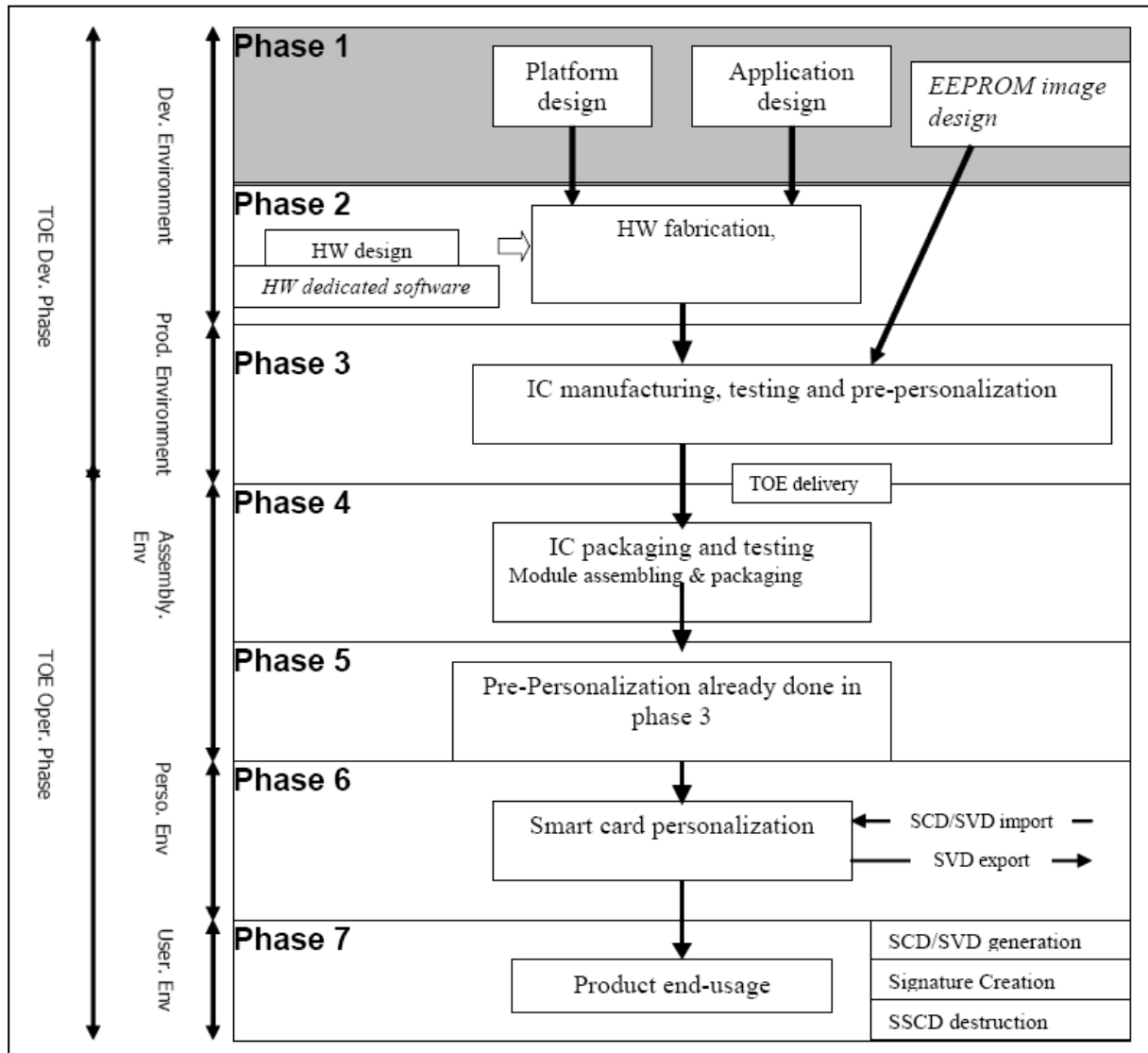
Cette architecture peut être représentée de la façon suivante :





### 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 3 (pré-personnalisation). Pour toutes les phases qui précèdent ce point de livraison, la TOE étant en construction, l’évaluateur a évalué les mesures d’assurance portant sur l’environnement de la TOE (pour les phases 2 et 3, l’évaluateur s’est appuyé sur les résultats obtenus lors de la certification du composant). Au-delà du point de livraison, l’évaluateur a évalué le produit et ses guides.

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.

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 GmbH**

Stresemannallee 101  
D-22502 Hamburg  
Allemagne

La phase de pré-personnalisation (déport de la phase 5 à la phase 3), incluse dans le wafer process, est également effectuée sur ces sites.

Pour l'évaluation, l'évaluateur a considéré :

- en tant qu'administrateur du produit :
  - o le personnalisateur (*Personalizer*) qui charge notamment les données de l'utilisateur final ;
  - o 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 ;
- en tant qu'utilisateur du produit :
  - o le porteur de la carte, qui est aussi le signataire dans le cadre de l'application de signature, et en tant que tel, 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 correspond à celle présentée au §1.2.3 Architecture, avec les précisions suivantes :

- le microcontrôleur NXP P5CD144 (VOB) est en configuration « à contact » ;
- seule la partie de la plate-forme Java Card MultiApp (v1.0) offrant les fonctionnalités Card Manager et GlobalPlatform permettant l'installation et le fonctionnement de l'applet de signature électronique (v4.2.7.A) a été évaluée (le reste de la plate-forme est hors périmètre de l'évaluation, la plate-forme est en mode fermée - au sens Java Card) ;
- l'applet de signature électronique (v4.2.7.A) est 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 ;

## 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] et à l'interprétation suivante :

- le composant d'assurance ATE\_DPT.2 est remplacé par le composant ATE\_DPT.1 au niveau EAL4 dans la révision 3 des CC version 3.1 (publiée après le démarrage de cette évaluation)

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 AP] et [COMP] 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 fait l'objet du certificat [BSI-DSZ-CC-0411-2007] délivré par le BSI, et maintenu en 2009 (cf. [BSI-DSZ-CC-0411-2007-MA-05]).

L'évaluation s'appuie sur les résultats de l'évaluation de la variante précédente du produit intitulée « 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 », certifiée par l'ANSSI (cf. [ANSSI-CC-2009\_56]). Les évolutions portent uniquement sur un changement du cycle de vie (déport de la phase 5 à la phase 3 : cf. plus haut au §1.2.4 Cycle de vie).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 26 avril 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] lors de la certification de la variante précédente du produit (cf. [ANSSI-CC-2009\_56]). Les mécanismes cryptographiques n'ayant pas changé dans le présent produit, les conclusions de la cotation précédente demeurent identiques (cf. §2.3 du [ANSSI-CC-2009\_56] et [ANA-CRY]).

Ces résultats ont été pris en compte dans l'analyse de vulnérabilités indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilités exploitables pour le niveau AVA\_VAN.5 visé.

### **2.4. Analyse du générateur d'aléas**

Le générateur d'aléas du produit a été analysé par l'ANSSI lors de la certification de la variante précédente du produit (cf. [ANSSI-CC-2009\_56]). Ce générateur d'aléas n'ayant pas changé dans le présent produit, les conclusions de l'analyse précédente demeurent identiques (cf. §2.4 du [ANSSI-CC-2009\_56]).

## 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 wafer process : 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 et NXP, 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 :

- l'usage des clés RSA de taille supérieure ou égale à 1 536 bits ;
- l'usage de 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 2010 permet la reconnaissance, par les pays signataires de l'accord<sup>1</sup>, 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 :



#### 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<sup>2</sup>, 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 :



---

<sup>1</sup> 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.

<sup>2</sup> 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	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	4	4	Complete functional specification
	ADV_IMP				1	1	2	2	1	1	Implementation representation of the TSF
	ADV_INT					2	3	3			
	ADV_SPM						1	1			
	ADV_TDS		1	2	3	4	5	6	3	3	Basic modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	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	4	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	4	4	Problem tracking CM coverage
	ADO_DEL		1	1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	2	Sufficiency of security measures
	ALC_FLR										
	ALC_LCD			1	1	1	1	2	1	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	1	1	Well defined development tools
ASE Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1	1	1	Conformance claim
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended component definition
	ASE_INT	1	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	1	TOE summary specifications
ATE Tests	ATE_COV		1	2	2	2	3	3	2	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	1	1	Testing: basic design
	ATE_FUN		1	1	1	1	2	2	1	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	Independant testing, sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	5	Advanced methodical vulnerability analysis



## Annexe 2. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> <li>- MISTRAL2 Security Target v1.1, D1152705 Gemalto.</li> </ul> <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> <li>- MultiApp ID IAS ECC – Wafer process - Security Target July 21, 2010 Gemalto.</li> </ul>
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> <li>- Evaluation Technical Report – MISTRAL2 Project MISTRAL2_ETR_v1.0 / 1.0 Serma Technologies.</li> </ul>
[CONF]	<p>Liste de configuration</p> <ul style="list-style-type: none"> <li>- LIS: Configuration List – MISTRAL2 D1154428, V1.0, 18/01/2010 Gemalto.</li> </ul>
[GUIDES]	<p>Guide utilisateur opérationnel du produit :</p> <ul style="list-style-type: none"> <li>- IAS-ECC Operational user guidance D1153719, v1.0 Gemalto.</li> </ul> <p>Guide utilisateur pour la diversification du filtre de validation :</p> <ul style="list-style-type: none"> <li>- User Guide to execute Diversification filter validation USG001R20044_DiversificationFilter, v1.2 Gemalto.</li> </ul> <p>Guide de préparation :</p> <ul style="list-style-type: none"> <li>- Preparative procedure – MISTRAL2 D1153820, v1.1 Gemalto.</li> </ul>
[BSI-PP-0005-2002]	<p>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-0005-2002T.</i></p>
[BSI-PP-0006-2002]	<p>Protection Profile — Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001. <i>Certifié par le BSI sous la référence BSI-PP-0006-2002T.</i></p>
[BSI-PP-0002-2001]	<p>Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0002-2001.</i></p>
[E-sign]	<p>Application Interface for Smart Cards used as Secure Signature Creation Device CEN/ISSS WS/E-Sign Draft CWA Group K part 1 – Basic</p>

	<p>requirements. Version 1, Release 9 (17th September 2003)</p> <p>Application Interface for Smart Cards used as Secure Signature Creation Device</p> <p>CEN/ISSS WS/E-Sign Draft CWA Group K part 2 – Additional services. Version 0, Release:19 (12th December 2003)</p>
[BSI-DSZ-CC-0411-2007]	<p>Certificat BSI délivré le 5 juillet 2007 pour les produits <i>NXP Secure Smart Card Controller P5CD144V0B, P5CN144V0B and P5CC144V0B each with specific IC Dedicated Software.</i></p>
[BSI-DSZ-CC-0411-2007-MA-05]	<p>Rapport de maintenance BSI délivré le 6 novembre 2009 pour les produits <i>NXP Smart Card Controller P5CD144V0B, P5CN144V0B and P5CC144V0B each with specific IC Dedicated Software</i></p>
[ANA-CRY]	<p>Rapport d'analyse cryptographique de l'ANSSI : Cotation de mécanismes cryptographiques - Qualification MISTRAL, N°2356/SGDN/ANSSI/DR, 22/09/2009.</p>
[ANSSI-CC-2009_56]	<p>Certificat ANSSI délivré le 17 février 2009 sous le titre : 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.</p>

### 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-2009-03-001 version 2.7 revision 1, March 2009.
[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 3.0, 8 Janvier 2010, Management Committee.
[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.11 du 24 octobre 2008, voir <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a>