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-2016/03

Application IAS V4.2.0.B sur la plateforme JavaCard ouverte MultiApp V3.1 masquée sur le composant P60D144PVA

(Version du patch : 1.3)

Paris, le 9 février 2016

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

Guillaume POUPARD
[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@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2016/03

Nom du produit

Application IAS V4.2.0.B sur la plateforme JavaCard ouverte MultiApp V3.1 masquée sur le composant P60D144PVA

Référence/version du produit

Version de l'application IAS : 4.2.0.B

Version de l'application MOCA Server : 1.0

Version de la plateforme Java Card MultiApp : 3.1 Version du patch : 1.3

Conformité à un profil de protection

Protection profiles for secure signature creation device – Part 2 : Device with key generation, version 2.0.1,
maintenu sous la référence [PP-SSCD-Part2].

Protection profiles for secure signature creation device – Part 3 : Device with key import, version 1.0.2,
certifié sous la référence [PP-SSCD-Part3].

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

Gemalto

6 rue de la Verrerie,
92197 Meudon cedex, France

NXP Semiconductors

Box 54 02 40,
D-22502 Hambourg, Allemagne

Commanditaire

Gemalto

6 rue de la Verrerie,
92197 Meudon cedex, France

Centre d'évaluation

Serma Technologies

14 rue Galilée, CS 10055, 33615 Pessac Cedex, France

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 à puce ouverte « MultiApp V3.1 » pouvant être en mode contact ou sans-contact. Le produit est développé par la société *GEMALTO* et embarqué sur le microcontrôleur P60D144PVA fabriqué par la société *NXP SEMICONDUCTORS*.

La cible d'évaluation est composée :
- de l'applet IAS Classic V4.2.0.B, qui permet à l'utilisateur de signer électroniquement des données ;
- de l'application « MOCA Server » version 1.0, qui permet de faire du *Match on Card* ;
- de la plateforme ouverte Java Card MultiApp V3.1, qui permet de charger des applets durant la phase opérationnelle. Cette plateforme est certifiée par ailleurs sous la référence [ANSSI-CC-2015/15].

D'autres applications, en dehors du périmètre de cette évaluation, sont embarquées dans la ROM du produit, notamment les applications natives eTravel EAC et SAC qui réalisent les fonctions de passeport électronique. Ces applications ne sont pas fonctionnelles dans ce produit. Bien qu'en dehors du périmètre de l'évaluation, ces applications ont été évaluées par ailleurs et leur présence a été prise en compte lors de l'évaluation, et notamment dans le cadre de la recherche de vulnérabilités.

1.2. Description du produit

1.2.1. Introduction

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

Cette cible de sécurité est strictement conforme aux profils de protection [PP-SSCD-Part2] et [PP-SSCD-Part3].

1.2.2. 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 présents dans la réponse que donne le produit suite à la commande GET DATA (voir [GUIDES]).

L'applet IAS est identifiable par les éléments présents dans la réponse que donne le produit suite à la commande GET DATA sur le CPLC :
- pour le tag '**C0**' on obtient la référence de l'applet : **49 41 53 20 43 6C 61 73 73 69 63 20 76 34** (IAS Classic v4) ;
- pour le tag '**C1**' on obtient la version de l'applet : **34 2E 32 2E 30 2E 42** (version 4.2.0.B).

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- ceux de la plateforme Java Card en configuration ouverte de la carte à puce MultiApp V3.1 certifiée sous la référence [ANSSI-CC-2015/15] ;
- l'authentification du signataire par un code PIN ou des données biométriques ;
- la génération des données de création et de vérification de signature ;
- l'import et le stockage des données de création de signature ;
- l'export des données de vérification de signature ;
- la création d'une signature électronique ;
- l'authentification de l'administrateur ;
- la protection en intégrité des données à signer ;
- la protection des communications à l'aide du mécanisme de *secure messaging*.

1.2.4. Architecture

Le produit est une carte à puce constituée :

- du composant P60D144PVA fabriqué par *NXP SEMICONDUCTORS* ;
- d'un système d'exploitation sous forme d'une plateforme ouverte Java Card MultiApp V3.1 dont l'interface de programmation (API) contient notamment le paquet propriétaire « *com.gemalto.javacardx.pace* » ;
- des applications natives passeport eTravel EAC et SAC, en dehors du périmètre de l'évaluation et non fonctionnelles ;
- de l'application « MOCA Server » destinée à faire du *Match on Card* ;
- de l'applet IAS Classic V4.2.0.B permettant à l'utilisateur de signer électroniquement des données.

1.2.5. Cycle de vie

Le produit est proposé avec trois cycles de vie possibles qui sont explicités ci-après.

Pour chacun des cycles de vie, l'évaluation se limite aux étapes 1 à 5 correspondant aux phases 1 et 2, respectivement phase de développement et phase de fabrication.

Cycle de vie n° 1 : Initialisation du module sur le site de *GEMALTO* :

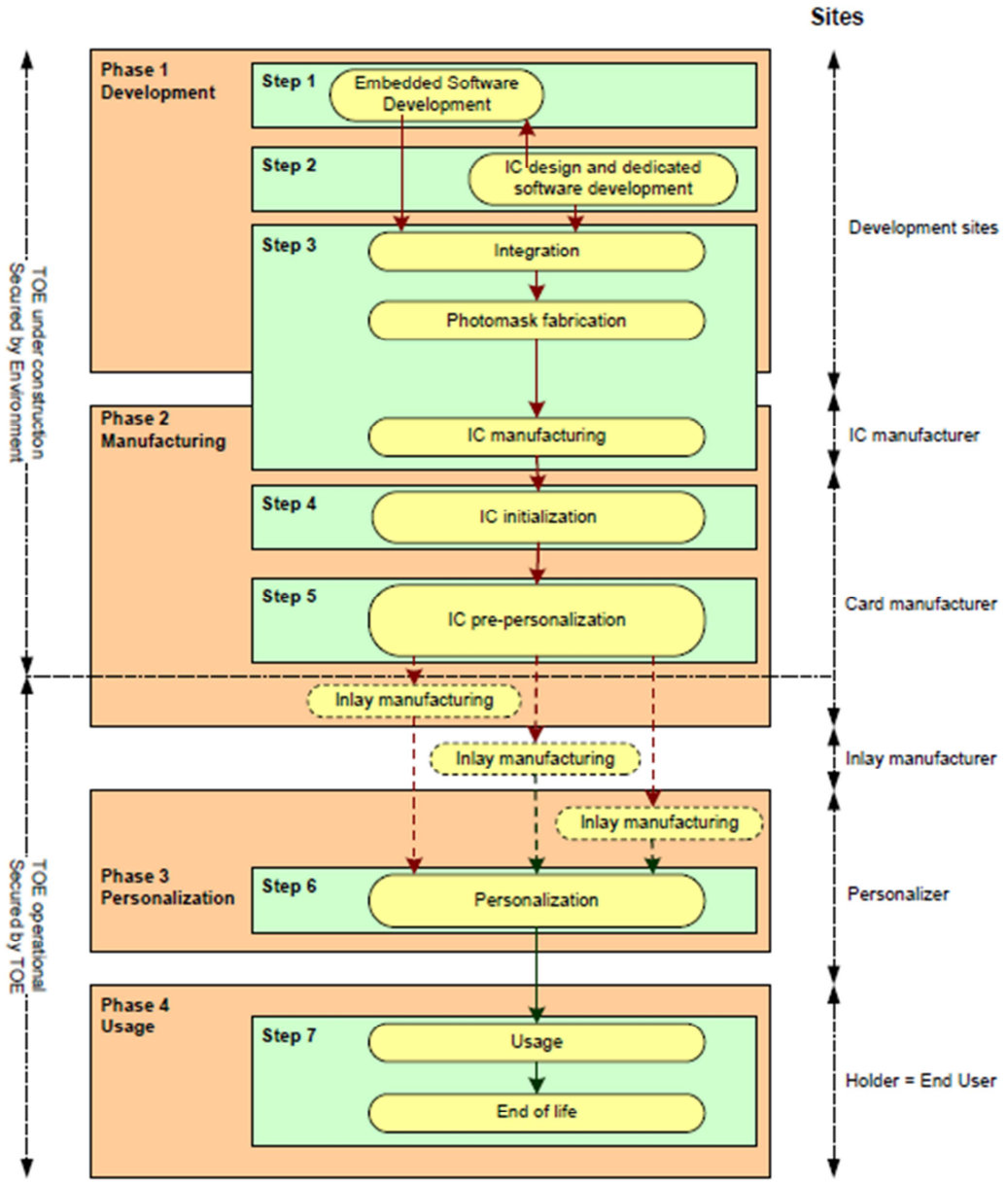

Figure 1 - Cycle de vie n° 1 : Initialisation du module sur le site de *GEMALTO*

Le cycle de vie n° 1 décrit le cycle de vie standard. Le module est fabriqué sur le site du fondeur. Il est ensuite envoyé sur le site de *GEMALTO* où il est initialisé et pré-personnalisé. Puis il est envoyé au personnalisateur, soit directement et dans ce cas le personnalisateur fabrique l'*inlay*, soit après que *GEMALTO* ait fabriqué l'*inlay*, soit après être passé par le fabricant d'*inlays* (autre que *GEMALTO*).

Cycle de vie n° 2 : Initialisation du module sur le site du fondeur :

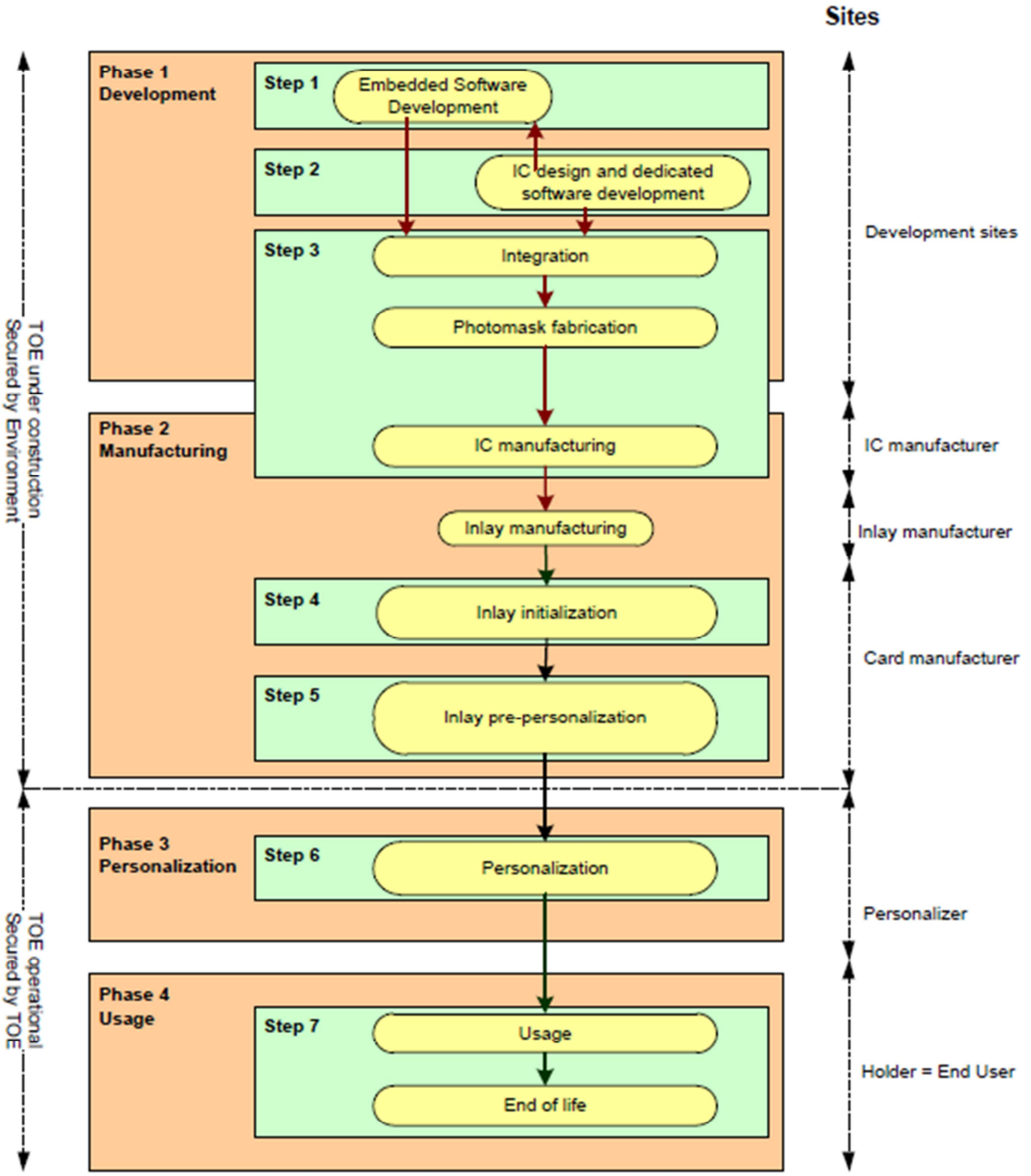

Figure 2 - Cycle de vie n° 2 : Initialisation du module sur le site du fondeur

Le cycle de vie n° 2 correspond au cas où le client souhaite recevoir les *wafers* directement du fondeur. Dans ce cas, l'initialisation et la pré-personnalisation, qui incluent des opérations sensibles telles que le chargement de patchs, sont réalisées sur le site du fondeur.

Cycle de vie n° 3 : Initialisation sur *inlay* sur le site de *GEMALTO* :

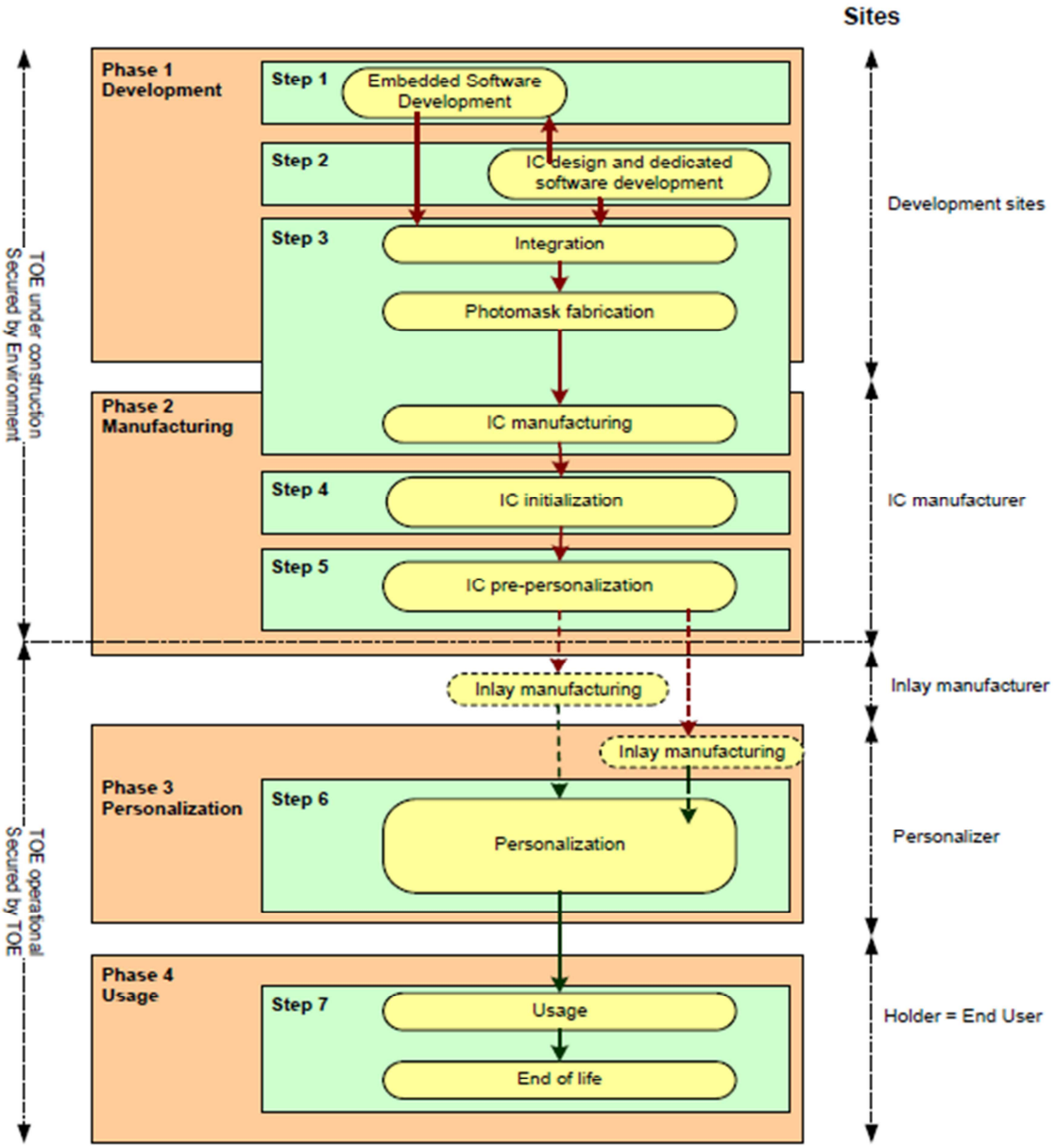

Figure 3 - Cycle de vie n° 3 : Initialisation sur *inlay* sur le site de *GEMALTO*

Le cycle de vie n° 3 correspond au cas où *GEMALTO* souhaite recevoir du fondeur des *inlays* plutôt que des modules. Dans ce cas, le fondeur envoie les *inlays* à *GEMALTO*.

Le produit a été développé sur les sites suivants :

GEMALTO

Myllynkivenkuja 4
FI-01620 Vantaa
Finlande

GEMALTO

12 Ayer Rajah Crescent
Singapor 139941
Singapour

GEMALTO

6 Rue de la Verrerie
92190 Meudon
France

GEMALTO

Avenue du Pic de Bertagne
13881 Gémenos
France

GEMALTO

Avenue du Jujubier, ZI Athelia IV,
16705 La Ciotat
France

GEMALTO

Ul. Skarszewska 2
33-110 Tczew
Pologne

Le microcontrôleur est développé et fabriqué par *NXP SEMICONDUCTORS*. Les sites de développement et de fabrication du microcontrôleur sont détaillés dans le rapport de certification dont la référence est [BSI-DSZ-CC-0845-V2-2013].

Pour l'évaluation, l'évaluateur a considéré :

- comme administrateurs du produit :
  - le personnalisateur (étape 6) qui configure l'application IAS en chargeant les données de l'émetteur de la carte et du signataire ainsi que les secrets de l'application tels que les clés cryptographiques ;
  - l'émetteur de la carte (étape 7) qui procède aux opérations d'administration de la carte durant la phase opérationnelle ;
- comme utilisateur du produit le signataire (étape 7) qui fait appel à l'application IAS pour réaliser une opération de signature.

1.2.6. Configuration évaluée

Le certificat porte sur l'application IAS V4.2.0.B sur la plateforme ouverte Java Card masquée sur le composant P60D144PVA, telle que présentée plus haut au chapitre « 1.2.4 Architecture ».

Ce rapport de certification porte sur la configuration intégrant :

- le mécanisme *Match on Card*, fourni par l'application « MOCA Server », permettant l'authentification du porteur de la carte à l'aide d'empreinte digitale ;
- le mécanisme PACE (*Password authenticated Connection Establishment*), fourni par la plateforme, permettant l'authentification mutuelle entre la carte et le terminal par un mot de passe.

L'évaluateur a testé le produit sur le composant P60D144PVA.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [CC] et 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 [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

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 sur la plateforme déjà certifiée par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation de la « Plateforme Java Card en configuration ouverte de la carte à puce MultiApp v3.1 masquée sur le composant P60D144PVA patch 1.3 » au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5 conformément au profil de protection [PP JCS], le 31 août 2015, sous la référence [ANSSI-CC-2015/15].

L'évaluation s'appuie sur les résultats d'évaluation du produit « Application IAS V4.2.0.B sur la plateforme JavaCard ouverte MultiApp V3.1 masquée sur le composant P60D144PVA patch 1.3 » certifié le 28 septembre 2015 sous la référence [ANSSI-CC-2015/37].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 24 août 2015, 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 conformément aux référentiels techniques de l'ANSSI [REF].

Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] qui donne lieu aux conclusions suivantes :

- les mécanismes analysés sont conformes aux exigences des référentiels techniques de l'ANSSI ([REF]) sous réserve de prendre en compte les recommandations se trouvant dans les guides (voir [GUIDES]) ;
- la fonction de hachage SHA-1 ne doit pas être utilisée pour les applications de signature.

Quoi qu'il en soit, les résultats 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.

Dans le cadre du processus de qualification renforcée, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI. Ces résultats 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

Le générateur de nombres aléatoires, de nature physique, utilisé par le produit final a été évalué dans le cadre de l'évaluation du microcontrôleur (voir [BSI-DSZ-CC-0845-V2-2013]).

Par ailleurs, comme requis dans le référentiel cryptographique de l'ANSSI ([REF]), la sortie du générateur physique d'aléas subit un retraitement de nature cryptographique.

Les résultats 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.

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 « Application IAS v4.2.0.B sur la plateforme JavaCard ouverte MultiApp V3.1 masquée sur le composant P60D144PVA, patch 1.3 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5.

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, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- toutes les futures applications chargées sur ce produit (chargement *post-issuance*) doivent respectées les contraintes de développement de la plateforme (guides [AGD-Dev_Basic] et [AGD-Dev_Sec] selon la sensibilité de l'application considérée ;
- les autorités de vérification doivent appliquer le guide [AGD-OPE_VA].

Les recommandations du chapitre « 2.3 Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI » du présent rapport devront également être mises en œuvre.

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 :

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.
Pour les évaluations enregistrées avant septembre 2014, 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'Autriche, l'Espagne, la Finlande, la France, 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, 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 5+	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**	**5**	Complete semi-formal functional specification with additional error information
	ADV_IMP				**1**	1	**2**	2	**1**	Implementation representation of the TSF
	ADV_INT					**2**	**3**	3	**2**	Well-structured internals
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**4**	Semiformal 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 procedures
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	**5**	Development tools CM coverage
	ALC_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	**2**	Compliance with implementation standards
ASE Evaluation de la cible de sécurité	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended components 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 specification
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**3**	3	**4**	**3**	Testing: modular 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_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 : - MultiApp V31 Delphes31 : IAS EN Security Target, version 1.1, référence : D1296544, 10 février 2015, Gemalto. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Security Target Lite MultiAppV3.1 IAS Classic V4.2 EN, version 1.1p, référence : D1296544, juin 2015, Gemalto.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report DELPHES31 Project, version 1.0, référence : DELPHES31_ETR_IAS_CORE-144K_v1.0, 24 août 2015, Serma Technologies.
[ANA-CRY]	Cryptographic Mechanisms Evaluation Report DELPHES 31 – IAS Project, version : 1.0, référence DELPHES31_IAS_cryptography_v1.0, 19 février 2014, Serma Technologies.
[CONF]	Liste de configuration du produit : - LIS : Configuration List for IAS Classic 4.2, version 1.0, référence : D1327264, 16 avril 2014, Gemalto.
[GUIDES]	Guide générique : - MultiApp ID V31 Software AGD Document – IAS V42 Application, version 1.0, référence D1326533, 8 avril 2014, Gemalto. Guide d'administration du produit : - IAS Classic Applet V4.2, Reference Manual, référence : D1307695A, 23 octobre 2013, Gemalto ; - BioPIN Manager V2.0 – Reference Manual, référence : D1290692A, 17 juin 2013, Gemalto. Guide de personalisation : - Card Personalization Specification requirement for SSCD security evaluation IAS Classic v4.2, version 1.0, référence : IACv42_001-CPS_Req_For_CC_Evaluation, 27 septembre 2013, Gemalto.
[PP-SSCD-Part2]	Protection profiles for secure signature creation device – Part 2: Device with key generation, référence : prEN 14169-2:2012, version 2.0.1 datée du 23 janvier 2012. *Maintenu par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 21 février 2012 sous la référence BSI-CC-PP-0059-2009-MA-01*.

[PP-SSCD-Part3]	Protection profiles for secure signature creation device – Part 3: Device with key import, référence : prEN 14169-3:2012, version 1.0.2 datée du 24 juillet 2012. *Certifié par le BSI le 27 septembre 2012 sous la référence BSI-CC-PP-0075-2012.*
[PP JCS]	"Java Card Protection Profile – Open Configuration", version 3.0, 18 mai 2012. *Maintenu par l'ANSSI sous la référence ANSSI-CC-PP-2010/03-M01*.
[BSI-DSZ-CC-0845-V2-2013]	NXP Secure Smart Card Controller P60x144/080PVA/PVA(Y) with IC Dedicated Software FW5.0. *Certifié par le BSI le 19 décembre 2013 sous la référence BSI-DSZ-CC-0845-V2-2013.*
[ANSSI-CC-2015/15]	Plateforme Java Card en configuration ouverte de la carte à puce MultiApp V3.1 masquée sur le composant P60D144PVA patch 1.3. *Certifié par l'ANSSI le 31 août 2015 sous la référence ANSSI-CC-2015/15.*
[ANSSI-CC-2015/37]	Application IAS V4.2.0.B sur la plateforme JavaCard ouverte MultiApp V3.1 masquée sur le composant P60D144PVA patch 1.3. *Certifié par l'ANSSI le 28 septembre 2015 sous la référence ANSSI-CC-2015/37.*

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié 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, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001; Part 2: Security functional components, Septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002; Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[JIWG IC] *	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, février 2009.
[JIWG AP] *	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, janvier 2013.
[COMP] *	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.2, janvier 2012.
[CC RA]	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 janvier 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.
	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 2.00 du 8 juin 2012 annexée au Référentiel général de sécurité (RGS_B2), voir www.ssi.gouv.fr.

	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité (RGS_B3), voir www.ssi.gouv.fr.

*Document du SOG-IS ; dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.