



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-2018/21
PPCA application v1.0.1.3 on MultiApp v4.0.1
Platform

Paris, le 15/05/2018

*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 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@ssi.gouv.fr

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

Référence du rapport de certification

ANSSI-CC-2018/21

Nom du produit

PPCA application v1.0.1.3 on MultiApp v4.0.1 Platform

Référence/version du produit

applet 1.0.1.3, platform 4.0.1

Conformité à un profil de protection

(aucune conformité à un profil de protection n'est réclamée)

Critères d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 4 augmenté
ALC_DVS.2, ATE_DPT.2, AVA_VAN.5

Développeurs

Gemalto
La Vigie, Avenue du Jujubier,
ZI Athelia IV, 13705 La Ciotat, France

INFINEON Technologies
AG
AIM CC SM PS – Am Campeon 1-12,
85579 Neubiberg, Allemagne

Commanditaire

Gemalto
La Vigie, Avenue du Jujubier,
ZI Athelia IV, 13705 La Ciotat, France

Centre d'évaluation

Serma Safety & Security
14 rue Galilée, CS 10055, 33615 Pessac Cedex, France

Accords de reconnaissance applicables



SOG-IS



Ce certificat est reconnu au niveau EAL2.

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	6
1.1. PRESENTATION DU PRODUIT	6
1.2. DESCRIPTION DU PRODUIT	6
1.2.1. <i>Introduction</i>	6
1.2.2. <i>Services de sécurité</i>	6
1.2.3. <i>Architecture</i>	6
1.2.4. <i>Identification du produit</i>	6
1.2.5. <i>Cycle de vie</i>	7
1.2.6. <i>Configuration évaluée</i>	7
2. L’EVALUATION	8
2.1. REFERENTIELS D’EVALUATION	8
2.2. TRAVAUX D’EVALUATION	8
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI	8
2.4. ANALYSE DU GENERATEUR D’ALEAS	8
3. LA CERTIFICATION	10
3.1. CONCLUSION	10
3.2. RESTRICTIONS D’USAGE	10
3.3. RECONNAISSANCE DU CERTIFICAT	11
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	11
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i>	11
ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT	12
ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	13
ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION	14

1. Le produit

1.1. Présentation du produit

Le produit évalué est la carte à puce « PPCA application v1.0.1.3 on MultiApp v4.0.1 Platform » développée par *GEMALTO* sur un microcontrôleur d'*INFINEON*.

Ce produit est destiné à être utilisé comme moyen d'authentification dans le cadre de services numériques.

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.

La cible de sécurité s'inspire du profil de protection [EAC2-PP]. Toutes les exigences de ce profil de protection sont revendiquées dans la cible de sécurité, à l'exception des exigences relatives au protocole « *Restricted Identification (RI)* ». Le produit implémente un protocole alternatif qui n'est pas celui spécifié par FIA_API.1.1/RI de [EAC2-PP] et qui n'est pas revendiqué comme service de sécurité dans cette évaluation.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- les services revendiqués lors de l'évaluation de la plateforme (voir [ANSSI-CC-2017/76]) ;
- les protocoles Terminal Authentication 2 et Chip Authentication 2 (voir [EAC2-PP]).

1.2.3. Architecture

Le produit est constitué d'une plateforme JavaCard et de plusieurs applets, dont une applet « PPCA ». Le rapport [ANSSI-CC-2017/76] décrit plus en détail l'architecture du produit.

L'applet PPCA et certains services de la plateforme n'ont pas été évalués au titre de [ANSSI-CC-2017/76] ; ils font l'objet de la présente évaluation.

1.2.4. 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 :

- la plateforme est identifiée par les premiers octets de la valeur *Tag Identity*, dont les valeurs attendues sont : B0 85 59 56 01 02 40 90 78 97. Les modalités pour lire *Tag Identity* sont décrites dans le guide de la plateforme (référéncé dans [ANSSI-CC-2017/76]).
- l'applet PPCA est identifiée par son nom « PPCA » et sa version « 1.0.1.3 ». Les modalités pour lire ces informations sont décrites dans le guide [REF-MAN] au chapitre « Checking the version of the PPCA applet ».

1.2.5. Cycle de vie

Le cycle de vie du produit est décrit au chapitre 3.5 de la cible de sécurité [ST].

Le produit a été développé sur les sites listés dans le rapport [ANSSI-CC-2017/76].

Les différents rôles d'utilisateur sont décrits au chapitre 3.6 de la cible de sécurité [ST].

1.2.6. Configuration évaluée

La configuration ouverte du produit a été évaluée conformément à [OPEN] : ce produit correspond à une plateforme ouverte cloisonnante. Ainsi tout chargement de nouvelles applications conformes aux contraintes exposées dans le rapport [ANSSI-CC-2017/76] ne remet pas en cause le présent rapport de certification lorsqu'il est réalisé selon les processus audités.

Les différentes configurations (*Feature Flag*, voir [ANSSI-CC-2017/76]) offertes par le produit sont couvertes par l'évaluation.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 5** [CC], et à la méthodologie d'évaluation définie dans le manuel [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 [JIWG 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 dans le microcontrôleur déjà certifié par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation de la « Plateforme Javacard MultiApp V4.0.1- PACE en configuration ouverte masquée sur le composant M7892 G12 » au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5, conforme au profil de protection [PP-JC]. Cette plateforme a été certifiée le 18 décembre 2017 sous la référence [ANSSI-CC-2017/76]. Le microcontrôleur a été certifié le 20 décembre 2016 sous la référence BSI-DSZ-CC-0891-V2-2016 et la plateforme n'utilise pas les services de génération de nombre premiers des bibliothèques de ce microcontrôleur.

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 20 avril 2018, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

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

La cotation des mécanismes cryptographiques selon le référentiel technique de l'ANSSI [REF] n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilité de conception et de construction pour le niveau AVA_VAN.5 visé.

2.4. Analyse du générateur d'aléas

Le produit comporte un générateur de pseudo-aléa qui a fait l'objet d'une évaluation selon la méthodologie [AIS20/31], il répond aux exigences DRG.4, comme revendiqué dans la cible de sécurité de la plateforme.

Comme énoncé dans le document [REF], les aléas générés subissent effectivement un retraitement algorithmique 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 «PPCA application v1.0.1.3 on MultiApp v4.0.1 Platform » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté des composants ALC_DVS.2, ATE_DPT.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].

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'accord¹, des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. 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 signataires², des certificats Critères Communs.

La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL2 ainsi qu'à la famille ALC_FLR.

Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



¹ La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.

² La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

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 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 procedures
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
	ALC_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 Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended components 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 specification
ATE Tests	ATE_COV		1	2	2	2	3	3	2	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	2	2	Testing: security enforcing modules
	ATE_FUN		1	1	1	1	2	2	1	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	Independent 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"> - PPCA application on MultiApp V4.0.1 Platform Security Target, D1432617 v1.5, 18 avril 2018. <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"> - PPCA application on MultiApp V4.0.1 Platform Security Target Public version, D1432617 v1.5p, 18 avril 2018.
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> - Evaluation Technical Report, REMBRANDT Project, REMBRANDT_ETR_v1.1, 20 avril 2018, <i>SERMA</i>.
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"> - PPCA 1.0 application on MultiApp V4.0.1 Platform – Documentation list, v1.6, 18 avril 2018, <i>GEMALTO</i> ; - PPCA 1.0 application – Code configuration list, checkpoint 1.15, 2 février 2018.
[GUIDES] [REF-MAN] [ADG-Top]	<p>Polymorphic Pseudonym Card Application V1.0, Reference Manual, D1430671D, 25 janvier 2018, <i>GEMALTO</i> ;</p> <p>PPCA 1.0 application on MultiApp V4.0.1 Platform, AGD top-level document, D1447007 Rev 1.2, avril 2018, <i>GEMALTO</i>.</p> <p>(Voir également [GUIDES] de [ANSSI-CC-2017/76])</p>
[ANSSI-CC-2017/76]	<p>Rapport de certification ANSSI-CC-2017/76, Plateforme JavaCard MultiApp V4.0.1 – PACE en configuration ouverte masquée sur le composant M7892 G12, 18 décembre 2017.</p>
[PP-JC]	<p>Java Card System Protection Profile - Open Configuration, version 3.0. Profil de protection certifié par l'ANSSI le 25 juin 2010 et maintenu le 29 mai 2012 sous la référence ANSSI-CC-PP-2010/03-M01.</p>
[EAC2-PP]	<p>Electronic Document implementing Extended Access Control Version 2 defined in BSI TR-03110, version 1.01. <i>Certifié le 13 juillet 2015 par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0086-2015.</i></p>

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 ANSSI-CC-CER-P-01 Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : <ul style="list-style-type: none"> - Part 1: Introduction and general model, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001; - Part 2: Security functional components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002; - Part 3: Security assurance components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[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 1.4, août 2015.
[OPEN]	Certification of « Open » smart card products, version 1.1 (for trial use), 4 février 2013.
[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 .
[AIS2031]	A proposal for: Functionality classes for random number generators, AIS20/AIS31, version 2.0, 18 Septembre 2011, BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>).

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