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-2018/24

IAS Classic V4.4.2 with MOC server v1.1 on MultiApp V4.0.1

Paris, le 11 juin 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 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

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

Référence du rapport de certification

ANSSI-CC-2018/24

Nom du produit

IAS Classic V4.4.2 with MOC server v1.1 on MultiApp V4.0.1

Référence/version du produit

Version de l'application IAS : 4.4.2

Version de l'application MOCA Server : 1.1

Version plateforme Java Card MultiApp : 4.0.1

Conformité à un profil de protection

Protection profiles for secure signature creation device :
Part 2: Device with key generation, v2.0.1, BSI-CC-PP-0059-2009-MA-01 ;
Part 3: Device with key import, v1.0.2, BSI-CC-PP-0075-2012 ;
Part 4: Extension for device with key generation and trusted communication with certificate generation application, v1.0.1, BSI-CC-PP-0071-2012 ;
Part 5: Extension for device with key generation and trusted communication with signature creation application, v1.0.1, BSI-CC-PP-0072-2012 ;
Part 6: Extension for device with key import and trusted communication with signature creation application, v1.0.4, BSI-CC-PP-0076-2013.

Critères d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

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

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

Commanditaire

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

Centre d'évaluation

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

Accords de reconnaissance applicables

CCRA

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

1.1. Présentation du produit

Le produit évalué est l'application « IAS Classic V4.4.2 with MOC server v1.1 on MultiApp V4.0.1 » développée par la société *GEMALTO* et embarquée sur le microcontrôleur M7892 G12 fabriqué par la société *INFINEON TECHNOLOGIES AG*.

Ce produit est destiné à être utilisé comme dispositif sécurisé de création de signature (SSCD)[1].

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 conforme aux profils de protection *Protection profiles for Secure Signature Creation Device* [PP-SSCD-Part2], [PP-SSCD-Part3], [PP-SSCD-Part4], [PP-SSCD-Part5] et [PP-SSCD-Part6].

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- ceux de la plateforme Java Card en configuration ouverte ou fermée de la plateforme MultiApp V4.0.1 certifiée sous la référence ANSSI-CC-2017/76 (voir [CER-PLF]) ;
- l'import de la donnée de création de signature SCD (*Signature Creation Data*) via un canal de confiance ;
- la génération *in-situ* des paires SCD / SVD (*Signature Verification Data*) ;
- la génération de signatures électroniques ;
- l'export de la donnée de vérification de signature (SVD) vers le CGA (*Certification Generation Application*) ;
- l'authentification du signataire par un code PIN ou des données biométriques d'empreintes digitales (BioPIN) ;
- l'authentification de l'administrateur (authentification mutuelle) ;
- l'intégrité des conditions d'accès aux données protégées SCD et RAD (*Reference Authentication Data*) ;
- l'intégrité des données à signer DTBS (*Data To Be Signed*) ;
- la protection en intégrité et en confidentialité, des données lues à l'aide du mécanisme de « *Secure Messaging* ».

1.2.3. Architecture

Le produit est constitué :

- du composant M7892 G12 précédemment certifié (voir [CER-IC]) ;

[1] *Secure Signature Creation Device.*

- de la plateforme Java Card MultiApp V4.0.1 précédemment certifié (voir [CER-PLF]) ;
- de l'application « IAS Classic V4.4.2 » mise à disposition de l'utilisateur pour lui permettre de signer électroniquement ses données ;
- de l'application « MOCA server V1.1 » utilisée pour réaliser du *Match On Card*.

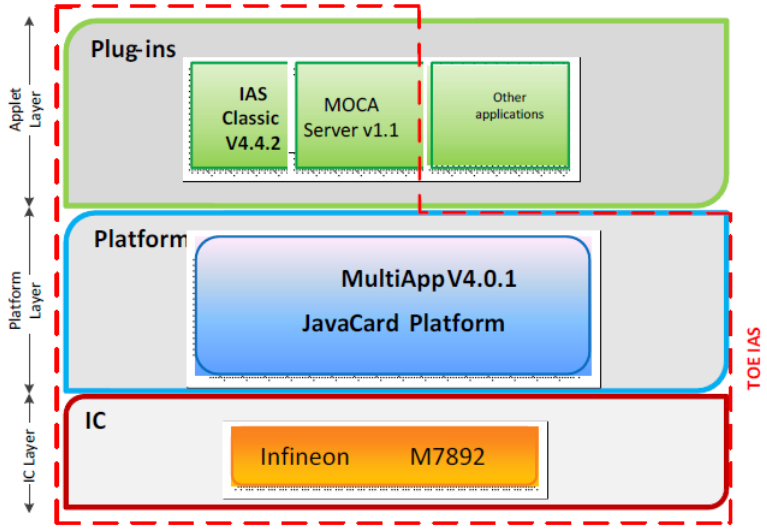

Figure 1 : Architecture du produit IAS Classic V4.4.2 with MOC server v1.1 on MultiApp V4.0.1

Le produit s'appuie sur la librairie cryptographique développée par *GEMALTO*.

Des applications Java en dehors du périmètre de cette évaluation peuvent être chargées sur la plate-forme JavaCard MultiApp V4.0.1, elles devront respecter les guides [PLF_BADR] et [PLF_SADR].

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 présents dans la réponse que donne le produit suite à la commande GET DATA sur le CPLC (voir [GUIDES]) :

- Identification de l'application IAS Classic :
  - le tag 'C**0**' permet d'obtenir la référence de l'applet IAS : **49 41 53 20 43 6C 61 73 73 69 63 20 76 34** (IAS Classic v4 en ASCII) ;
  - le tag '**C1**' permet d'obtenir la version de l'applet IAS : **34 2E 34 2E 32 2E 41** (version 4.4.2.A en ASCII).

- Identification de l'application MOC Server :
  - le tag 'A**0**' permet d'obtenir la référence de l'application MOC Server : **4D 4F 43 41 20 53 45 52 56 45 52 20 31 2E 31** (MOCA Server 1.1 en ASCII) ;
  - le tag '**A1**' permet d'obtenir la version de l'application MOC Server : **31 2E 31 2E 31 41** (version 1.1.1A en ASCII).

1.2.5. Cycle de vie

Le périmètre de l'évaluation se limite aux étapes 1 à 5 correspondant aux phases 1 et 2, respectivement phase de développement et phase de fabrication telles que décrites dans le profil de protection [PP-0084].

Le cycle de vie est décrit au chapitre 2.3.2 de la cible de sécurité [ST].

Les étapes 1 et 2 correspondent au développement du produit, plus précisément :

- au développement du logiciel embarqué : le logiciel dédié au composant *firmware*, le système d'exploitation, le système *JAVACARD*, la documentation, des *applets* et d'autres parties logicielles de la plateforme ;
- au développement du composant.

Les étapes 3 et 4 correspondent à la fabrication et au conditionnement (*packaging*) du composant.

L'étape 5 correspond au chargement du logiciel embarqué (hormis le *firmware* qui est déjà masqué durant l'étape 3) dans le composant. Il est à noter que le point de livraison, ou d'émission de la carte, est en sortie d'étape 5.

Les étapes 1 à 5 correspondent donc à la construction de la TOE. Elles ont été prises en compte dans la présente évaluation, avec, pour les étapes 2 et 3, une réutilisation des résultats de l'évaluation du composant. Les sites de développement et de fabrication du microcontrôleur sont détaillés dans le rapport de certification dont la référence est [CER-IC].

Le produit a été développé sur les sites suivants :

Gemalto Meudon 6 Rue de la Verrerie 92190 Meudon, France	Gemalto Singapore 12 Ayer Rajah Crescent Singapor 139941, Singapour
Gemalto Gémenos Avenue du Pic de Bretagne 13881 Gémenos, France	Gemalto La Ciotat Avenue du Jujubier, ZI Athelia IV 13705 La Ciotat, France
ATOS Paris (Aubervilliers / Croissy) 4 rue des Vieilles Vignes 77 183 Croissy-Beaubourg, France	ATOS Bydgoszcz – (ATOS Poland) Biznes Park, ul. Kraszewskiego 1 85-240 Bydgoszcz, Poland
Gemalto Barcelona Poligono lndustrial Llevant CL Llevant 12, 08150 Parets del Valles,Barcelona, Spain	Gemalto Montgomeryville 101 & 106 Park Drive Montgomeryville, PA 18 936 United States
Gemalto Curitiba Rodovia Dep. Leopoldo Jacomel, 13102 83323-410 Pinhais, PR Brazil	Gemalto Vantaa Myllynkivenkuja 4, Vantaa, Finland, FI-01620
Gemalto Tczew Ul. Skarszewska 2 33-110 Tczew, Poland	Gemalto Pont Audemer Z.l. Saint Ulfrant rue de Saint Ulkfrant 27500 Pont Audemer, France

Les sites de développement et de fabrication du microcontrôleur sont identifiés dans le rapport de certification du composant (voir [CER-IC]).

Le guide [PLF_AGD_OPE] identifie également des recommandations relatives à la livraison des futures applications à charger via le système d'exploitation MultiApp V4.0.1 de cette carte.
Par ailleurs, les guides [PLF_BADR] et [PLF_SADR] décrivent les règles de développement des applications destinées à être chargées sur cette carte ; les guides [PLF_GTO_VA] et [PLF_THIRD_VA] décrivent les règles de vérification qui doivent être appliquées par l'autorité de vérification.

1.2.6. Configuration évaluée

Le certificat porte sur l'application « IAS Classic V4.4.2 intégrant l'application MOC Server 1.1 sur la plateforme ouverte Java Card MultiApp V4.0.1 » masquée sur le composant M7892 G12, telle que présentée au chapitre « 1.2.3 Architecture ».

Les plateformes Java Card utilisées dans le cadre de cette évaluation sont masquées sur le composant SLE78CLFX400**V**PHM issu du microcontrôleur M7892 G12.

La configuration ouverte du produit a été évaluée conformément à [OPEN] : ce produit correspond à une plateforme ouverte « cloisonnante ». Tout chargement de nouvelles applications doit être effectué conformément aux processus audités et doit répondre aux contraintes exposées au chapitre 3.2 du présent rapport de certification.

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 [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 sur la plateforme déjà certifiée par ailleurs [CER-PLF].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 22 mai 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 a été réalisée conformément au référentiel technique de l'ANSSI [REF]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY].

Certains mécanismes analysés ne sont pas conformes aux exigences du référentiel cryptographique de l'ANSSI ([REF]) notamment :

- l'utilisation de la clé de session S_ENC dans différents mécanismes de cryptographie liés aux protocoles SCP01 et SCP02 ;
- ceux mentionnés au paragraphe 3.6 de [AGD_PRE] si les recommandations mentionnées dans ce même paragraphe, ne sont pas scrupuleusement respectées.

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 [CER-IC]).

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 (voir [CER-PLF]).
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 « IAS Classic V4.4.2 with MOC server v1.1 on MultiApp V4.0.1 » masquée sur le composant M7892 G12 soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 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 applications chargées sur ce produit doivent respecter les contraintes de développement de la plateforme ([PLF_BADR] et [PLF_SADR]) ;
- les autorités de vérification doivent appliquer les guides [PLF_GTO_VA] et [PLF_THIRD_VA] ;
- la protection du chargement de toutes les applications sur ce produit doit être activée conformément aux indications de [PLF_AGD_PRE] ;
- l'utilisation du protocole SCP03 est à privilégier plutôt que les protocoles SCP01 et SCP02 qui sont déconseillés. Toutefois, si l'usage de l'un de ces deux derniers était rendu nécessaire, il est recommandé de le faire dans un environnement physiquement sécurisé et de chiffrer les données échangées (voir § 2.1.1 et 2.1.4 de [AGD_PRE_OPE]).

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 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 signataires[2], 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 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 V4.0.1: IAS EN Core & Extensions Security Target, référence D1433429, version 1.6, 4 mai 2018, *GEMALTO*. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - IAS Classic V4.4.2 with MOC Server 1.1 on MultiApp V4.0.1 Security Target Lite, reference D1433429, version 1.6p, *GEMALTO*.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report - CASSIDY-I Project, reference CASSIDY-I_ETR_v1.1 / 1.1, version 1.1, 22 mai 2018, *SERMA SAFETY & SECURITY*.
[ANA-CRY]	Cryptographic Mechanisms Evaluation Report CASSIDY-I Project, reference CASSIDY-I_IAS_cryptography_v1.2/1.2, version 1.2, 22 mai 2018, *SERMA SAFETY & SECURITY*.
[CONF]	Liste de configuration du produit : - MultiApp V4.0.1: ALC LIS document – IAS Classic v4.4.2, référence D1439244, version 1.5, 4 mai 2018, *GEMALTO*.

[GUIDES] : [AGD_PRE_OPE]	- MultiApp V4.0.1: AGD OPE and PRE document - IAS v4.4.2, version 1.3, référence D1438665, 12 avril 2018, *GEMALTO* ;
[AGD_PRE]	- Card Personalization Specification requirement for SSCD security evaluation IAS Classic v4.4, version 1.2, reference WG.RND.5.0026, 22 janvier 2018, *GEMALTO* ;
[AGD-OPE-IAS]	- IAS Classic Applet V4.4, Reference Manual, reference D1387713J, 26 septembre 2017, *GEMALTO* ; - BioPIN Manager V2.0 – Reference Manual, reference D1290692C, 26 octobre 2016, *GEMALTO* ; - IAS Classic Applets – Personalization Profiles Guides, reference D1203913G, 27 avril 2017, *GEMALTO* ;
[GUIDES_PLF] :	
[PLF_BADR]	- Rules for applications on Multiapp certified product ; référence D1390963, version 1.2 de novembre 2017, *GEMALTO* ;
[PLF_SADR]	- Guidance for secure application development on Multiapp platforms, référence D1390326, version A01 de février 2016, *GEMALTO* ;
[PLF_GTO_VA]	- Verification process of Gemalto non sensitive applet, référence D1390670, version A01 de février 2016, *GEMALTO* ;
[PLF_THIRD_VA]	- Verification process of Third Party non sensitive applet, référence D1390671, version A01 de février 2016, *GEMALTO* ;
[PLF_AGD_PRE]	- MultiApp V4.0.1 AGD_PRE document - Javacard Platform, référence D1431347, version 1.0 du 28 septembre 2017, *GEMALTO* ;
[PLF_AGD_OPE]	- MultiApp V4.0.1 Javacard Platform AGD_OPE document, référence D1432683, version 1.1 du 28 septembre 2017, *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-SSCD-Part4]	Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application, référence : prEN 14169-4:2012, version 1.0.1 datée du 14 novembre 2012. *Certifié par le BSI le 12 décembre 2012 sous la référence BSI-CC-PP-0071-2012.*
[PP-SSCD-Part5]	Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application, référence : prEN 14169-5:2012, version 1.0.1 datée du 14 novembre 2012. *Certifié par le BSI le 12 décembre 2012 sous la référence BSI-CC-PP-0072-2012.*
[PP-SSCD-Part6]	Protection profiles for secure signature creation device – Part 6: Extension for device with key import and trusted communication with signature creation application, référence : prEN 14169-6:2013, version 1.0.4 datée du 3 avril 2013. *Certifié par le BSI le 16 avril 2013 sous la référence BSI-CC-PP-0076-2013.*
[PP0084]	Protection Profile, Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13 janvier 2014. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0084-2014.*
[CER-PLF]	Plateforme JavaCard MultiApp V4.0.1 - PACE en configuration ouverte masquée sur le composant M7892 G12. *Certifiée par l'ANSSI le 18 décembre 2017 sous la référence ANSSI-CC-2017/76.*
[CER-IC]	Certification Report BSI-DSZ-CC-0891-V2-2016 for Infineon Security Controller M7892 Design Steps D11 and G12 with optional RSA2048/4096 v2.03.008, ECv2.03.008, SHA-2 v1.01 and Toolbox v2.03.008 libraries, symmetric crypto library v2.02.010 and with specific IC dedicated software (firmware) from Infineon Technologies AG. Certifié par le *BSI (Bundesamt für Sicherheit in der Informationstechnik)* le 20 décembre 2016, sous la référence BSI-DSZ-CC-0891-V2-2016.

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 : - 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 1.2, janvier 2012.
[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.

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