



*Liberté • Égalité • Fraternité*  
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale  
Agence nationale de la sécurité des systèmes d'information

## **Rapport de certification ANSSI-CC-2017/22**

### **IAS Classic V4.4 with MOC Server 1.1 on MultiApp V4**

*Paris, le 16 juin 2017*

*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](mailto:certification@ssi.gouv.fr)

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

Référence du rapport de certification

**ANSSI-CC-2017/22**

Nom du produit

**IAS Classic V4.4 with MOC Server 1.1 on MultiApp V4**

Référence/version du produit

**Version de l'application IAS : 4.4.0.A**  
**Version de l'application MOCA Server : 1.1.1.A**  
**Version plateforme Java Card MultiApp : 4.0**

Conformité aux profils 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 4**

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

**0Serma Safety & Security**  
14 rue Galilée, CS 10055, 33615 Pessac Cedex, France

Accords de reconnaissance applicables



**Le produit 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](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>Introduction</i> .....	6
1.2.2. <i>Services de sécurité</i> .....	6
1.2.3. <i>Architecture</i> .....	7
1.2.4. <i>Identification du produit</i> .....	7
1.2.5. <i>Cycle de vie</i> .....	8
1.2.6. <i>Configuration évaluée</i> .....	9
<b>2. L’EVALUATION .....</b>	<b>10</b>
2.1. REFERENTIELS D’EVALUATION .....	10
2.2. TRAVAUX D’EVALUATION .....	10
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI .....	10
2.4. ANALYSE DU GENERATEUR D’ALEAS .....	11
<b>3. LA CERTIFICATION .....</b>	<b>12</b>
3.1. CONCLUSION .....	12
3.2. RESTRICTIONS D’USAGE .....	12
3.3. RECONNAISSANCE DU CERTIFICAT .....	12
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i> .....	12
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i> .....	13
<b>ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT CCV3.1R4 .....</b>	<b>14</b>
<b>ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE .....</b>	<b>15</b>
<b>ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION .....</b>	<b>18</b>

# 1. Le produit

## 1.1. Présentation du produit

Le produit évalué est l'application « IAS Classic V4.4 with MOC Server 1.1 on MultiApp V4 » 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*)<sup>1</sup>.

## 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 de la plate-forme MultiApp V4.0 certifiée sous la référence [ANSSI-CC-2017/07] ;
- la génération de la donnée de création de signature (*Signature Creation Data* ou SCD) et de la donnée de vérification de signature (*Signature Verification Data* ou SVD) associée ;
- l'export de la donnée de vérification de signature (SVD) pour une création de certificat électronique ;
- l'import de la donnée de création de signature (SCD) et de la donnée de vérification de signature (SVD) associée ;
- la réception et le stockage du certificat électronique ;
- le passage de l'état non-opérationnel à l'état opérationnel ;
- la création de signature électronique via un canal de confiance ;
- l'authentification de l'administrateur ;
- l'authentification du signataire par un code PIN ou des données biométriques d'empreintes digitales.

---

<sup>1</sup> *Secure Signature Creation Device*.

### 1.2.3. Architecture

Le produit est constitué :

- du composant M7892 G12 ;
- d'un système d'exploitation sous forme d'une plateforme ouverte JavaCard MultiApp V4 dont l'interface de programmation (API) contient notamment le paquet propriétaire « *com.gemalto.javacardx.pace* » ;
- de l'applet « IAS Classic V4.4 » permettant à l'utilisateur de signer électroniquement des données ;
- de l'application « MOCA Server 1.1 » destinée à faire du *Match on Card*.

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

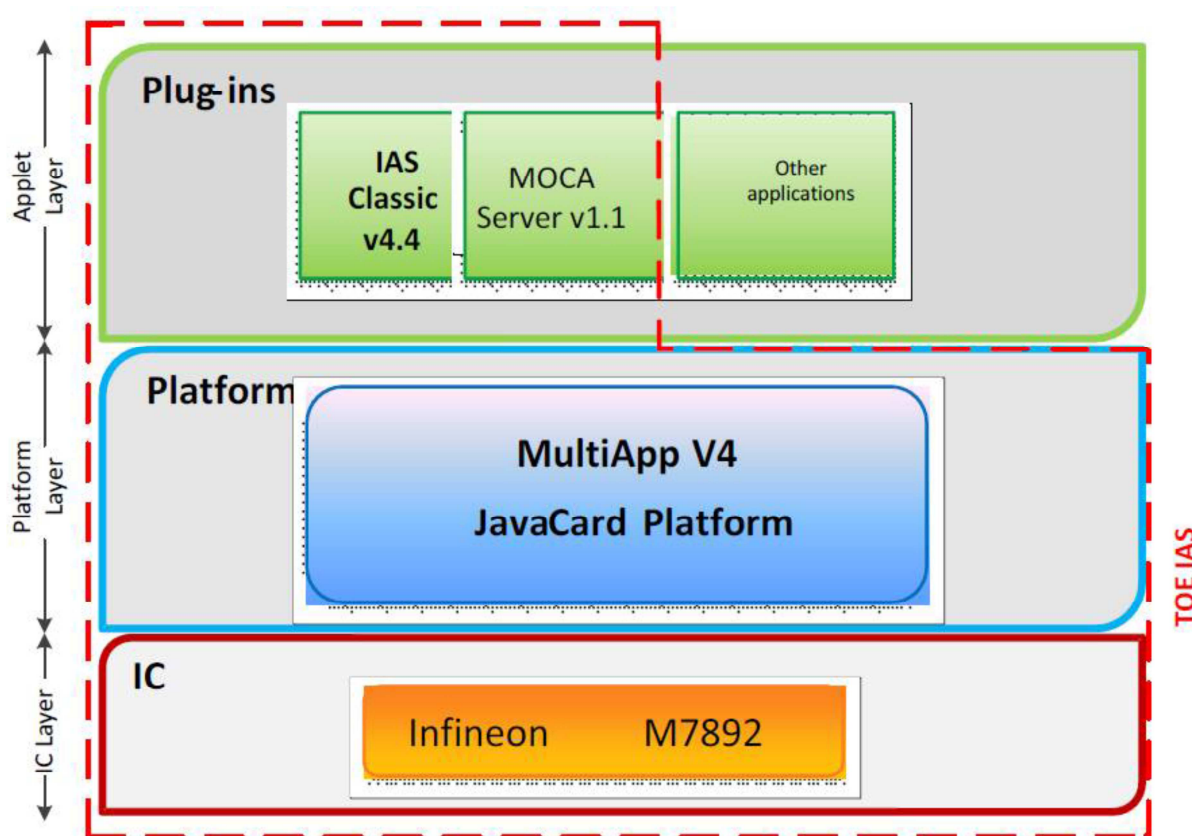


Figure 1 : Architecture du produit IAS Classic V4.4 with MOC Server 1.1 on MultiApp V4

Des applications Java en dehors du périmètre de cette évaluation peuvent être chargées sur la plate-forme JavaCard MultiApp V4. Toutes les applications qui sont chargées sur le produit 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 :
  - o le tag 'c0' 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) ;
  - o le tag 'c1' permet d'obtenir la version de l'applet IAS : **34 2E 34 2E 30 2E 41** (version 4.4.0.A).
  
- Identification de l'application MOC Server :
  - o le tag 'a0' 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) ;
  - o le tag 'a1' permet d'obtenir la version de l'application MOC Server : **31 2e 31 31 41** (version 1.1.1A).

### 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 en 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 :

<i>GEMALTO</i> Meudon 6, Rue de la Verrerie 92190 Meudon, France	<i>GEMALTO</i> Singapore 12, Ayer Rajah Crescent Singapor 139941, Singapour
<i>GEMALTO</i> Gémenos Avenue du Pic de Bertagne 13881 Gémenos, France	<i>GEMALTO</i> 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 Biznes Park, ul. Kraszewskiego 1 85-240 Bydgoszcz, POLAND
<i>GEMALTO</i> Barcelona Poligono Industrial Llevant CL Llevant 12, 08150 Parets del Valles, Barcelona Spain	<i>GEMALTO</i> Montgomeryville 101 & 106 Park Drive Montgomeryville, PA 18 936 United States
<i>GEMALTO</i> Curitiba Rodovia Dep. Leopoldo Jacomel, 13102 83323-410 Pinhais, PR Brazil	<i>GEMALTO</i> Vantaa Myllynkivenkuja 4, Vantaa, Finland, FI-01620
<i>GEMALTO</i> Tczew Ul. Skarszewska 2 33-110 Tczew, Pologne	<i>GEMALTO</i> Pont Audemer Z.I. Saint Ulfrant rue de Saint Ulkfrant 27500 Pont Audemer, France

Le guide [PLF\_AGD\_OPE] identifie des recommandations relatives à la livraison des futures applications à charger via le système d'exploitation MultiApp V4 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 intégrant l'application MOC Server 1.1 sur la plateforme ouverte Java Card MultiApp V4 masquée sur le composant M7892 G12, telle que présentée plus haut au chapitre « 1.2.3 Architecture » et personnalisée conformément à [AGD\_PRE].

## 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 [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 du microcontrôleur « 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) » au niveau EAL6 augmenté du composant ALC\_FLR.1 conforme au profil de protection [PP-0084]. Ce microcontrôleur a été certifié le 20 décembre 2016 sous la référence BSI-DSZ-CC-0891-V2-2016 (voir [CER-IC]).

L'évaluation s'appuie sur les résultats d'évaluation de la « Plateforme ouverte MultiApp V4.0 en configuration ouverte basée sur l'Operating System JLEP3 masquée sur le composant SLE78CLFX4000PH (M7892 G12) » certifiée le 8 mars 2017 sous la référence [ANSSI-CC-2017/07], conformément au profil de protection [PP JCS].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 30 mai 2017, 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].

Les mécanismes analysés sont conformes aux exigences des référentiels cryptographiques de l'ANSSI sous réserve de prendre en compte les recommandations se trouvant dans le manuel utilisateur [AGD\_OPE\_IAS].

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.

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 with MOC Server 1.1 on MultiApp V4 » 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 applications chargées sur ce produit doivent respecter les contraintes de développement de la plateforme (guides [PLF\_BADR] et [PLF\_SADR]) selon la sensibilité de l'application considérée ;
- 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].

### 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 lorsque les dépendances CC sont satisfaites. 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'Autriche, la Croatie, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, la Pologne, le Royaume-Uni et la Suède.



### 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>1</sup>, 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 :



---

<sup>1</sup> Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, l'Éthiopie, 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, le Qatar, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

## Annexe 1. Niveau d'évaluation du produit CCv3.1R4

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	
<b>ADV Développement</b>	ADV_ARC		1	1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	5	5	Complete semi-formal functional specification with additional error information
	ADV_IMP				1	1	2	2	1	1	Implementation representation of the TSF
	ADV_INT					2	3	3	2	2	Well-structured internals
	ADV_SPM						1	1			
	ADV_TDS		1	2	3	4	5	6	4	4	Semiformal modular design
<b>AGD Guides d'utilisation</b>	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
<b>ALC Support au cycle de vie</b>	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	5	5	Development tools 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	2	2	Compliance with implementation standards
<b>ASE Evaluation de la cible de sécurité</b>	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
<b>ATE Tests</b>	ATE_COV		1	2	2	2	3	3	2	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	3	3	Testing: modular design
	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
<b>AVA Estimation des vulnérabilités</b>	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>- MultiApp V4 : IAS EN Core &amp; Extensions, référence D1384185, version 1.3, 17 février 2017, <i>GEMALTO</i> ;</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>- Security Target Lite - MultiApp V4 : IAS EN Core &amp; Extensions, référence D1384185, version 1.3p, février 2017, <i>GEMALTO</i>.</li></ul>
[RTE]	<p>Rapport technique d'évaluation :</p> <p>Evaluation Technical Report – MINORIS IAS Project, référence MINORIS-IAS_ETR_v1.1, version 1.1, 10 mars 2017, <i>SERMA SAFETY &amp; SECURITY</i> ;</p>
[ANA-CRY]	<p>Cotation des mécanismes cryptographiques :</p> <p>Cryptographic Mechanisms Evaluation Report - MINORIS - IAS Project, v1.1, 30 mai 2017, <i>SERMA SAFETY &amp; SECURITY</i>.</p>
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"><li>- LIS: Configuration List for IAS, référence : D1403182–LIS-DOC-IAS-DOCUMENT, version 1.4 du 17 février 2017, <i>GEMALTO</i>.</li></ul>

<p>[GUIDES]</p> <p>[AGD_PRE]</p> <p>[AGD_OPE_IAS]</p> <p>[PLF_BADR]</p> <p>[PLF_SADR]</p> <p>[PLF_GTO_VA]</p> <p>[PLF_THIRD_VA]</p> <p>[PLF_AGD_PRE]</p> <p>[PLF_AGD_OPE]</p>	<ul style="list-style-type: none"> <li>- MultiApp ID V4 Software AGD Document – IAS V4.4 Application, version 1.0, référence D1388754, 2 mars 2017, <i>GEMALTO</i> ;</li> <li>- Card Personalization Specification requirement for SSCD security evaluation IAS Classic v4.4, version 1.1, référence WG.RND.5.0026, 15 février 2017, <i>GEMALTO</i> ;</li> <li>- IAS Classic Applet V4.4, Reference Manual, référence D1387713D, 5 août 2016, <i>GEMALTO</i> ;</li> <li>- BioPIN Manager V2.0 – Reference Manual, référence D1290692B, 6 avril 2016, <i>GEMALTO</i> ;</li> <li>- Rules for applications on Multiapp certified product ; référence D1390963, version 1.1 de juin 2016, <i>GEMALTO</i> ;</li> <li>- Guidance for secure application development on Multiapp platforms, référence D1390326, version A01 de février 2016, <i>GEMALTO</i> ;</li> <li>- Verification process of <i>GEMALTO</i> non sensitive applet, référence D1390670, version A01 de février 2016, <i>GEMALTO</i> ;</li> <li>- Verification process of Third Party non sensitive applet, référence D1390671, version A01 de février 16, <i>GEMALTO</i> ;</li> <li>- MultiApp V4, Preparative Guide, référence D1390316, version 1.1 du 6 juin 2016, <i>GEMALTO</i> ;</li> <li>- MultiApp V4, Operational User Guide, référence D1390321, version 1.2 du 15 février 2017, <i>GEMALTO</i>.</li> </ul>
<p>[PP-SSCD-Part2]</p>	<p>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. <i>Maintenu par le BSI le 21 février 2012 sous la référence BSI-CC-PP-0059-2009-MA-01.</i></p>
<p>[PP-SSCD-Part3]</p>	<p>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. <i>Certifié par le BSI le 27 septembre 2012 sous la référence BSI-CC-PP-0075-2012.</i></p>



[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. <i>Certifié par le BSI le 12 décembre 2012 sous la référence BSI-CC-PP-0071-2012.</i>
[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. <i>Certifié par le BSI le 12 décembre 2012 sous la référence BSI-CC-PP-0072-2012.</i>
[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. <i>Certifié par le BSI le 16 avril 2013 sous la référence BSI-CC-PP-0076-2013.</i>
[PP JCS]	“Java Card Protection Profile – Open Configuration”, version 3.0, 18 mai 2012. <i>Maintenu par l’ANSSI sous la référence ANSSI-CC-PP-2010/03-M01.</i>
[PP-0084]	Protection Profile, Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13 janvier 2014. <i>Certifié par le BSI sous la référence BSI-PP-0084-2014.</i>
[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, du 20 décembre 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 de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : <ul style="list-style-type: none"> <li>- Part 1: Introduction and general model, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001 ;</li> <li>- Part 2: Security functional components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002 ;</li> <li>- Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.</li> </ul>
[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 <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a> .
	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 <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a> .
	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 <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a> .

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