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-2016/23

Applet IAS Classic V3 sur plateforme Java Card ouverte MultiApp Essential V1.0 embarquée sur le composant M7793 A12 et G12

Paris, le 23 mai 2016

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ Ti CERTIFICATION

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-2016/23

Nom du produit

Applet IAS Classic V3 sur plateforme Java Card ouverte MultiApp Essential V1.0 embarquée sur le composant M7793 A12 et G12

Référence/version du produit

Version de l'application IAS Classic : 3.4.e
Version de la plateforme Java Card MultiApp Essential : 1.0

Conformité à un profil de protection

[PP-SSCD part 2], version 2.0.1 - PP for Secure Signature Creation Device – Part 2 : Device with key generation.

[PP-SSCD part 3], version 1.0.2 - PP for Secure Signature Creation Device – Part 3 : Device with key import.

[PP-SSCD part 4], version 1.0.1 - PP for Secure Signature Creation Device – Part 4 : Extension for device with key generation and trusted communication with certificate generation application.

[PP-SSCD part 5], version 1.0.1 - PP for Secure Signature Creation Device – Part 5 : Extension for device with key generation and trusted communication with signature creation application.

[PP-SSCD part 6], version 1.0.4 - PP for Secure Signature Creation Device – Part 6 : Extension for device with key import and trusted communication with signature creation application.

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,
92190 Meudon Cedex, France

Infineon

Am Campeon 1-12,
85579 Neubiberg, Allemagne

Commanditaire

Gemalto

6 rue de la Verrerie, 92190 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

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.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est la carte à puce composée de l'« Applet IAS Classic V3 sur plateforme Java Card ouverte MultiApp Essential V1.0 embarquée sur le composant M7793 A12 et G12 » développé par *GEMALTO* et *INFINEON*.

Le produit se présente sous la forme d'une carte à puce au format ISO 7816 fonctionnant en mode contact (standard ISO 7816-3) ; le microcontrôleur et la plateforme ouverte Java Card fournissent des services de sécurité aux applets, dont l'applet de signature électronique IAS Classic V3 embarquée sur la carte et objet de la présente évaluation.

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 part 2], version 2.0.1, [PP-SSCD part 3], version 1.0.2, [PP-SSCD part 4], version 1.0.1, [PP-SSCD part 5], version 1.0.1 et [PP-SSCD part 6], version 1.04.

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 suivants :

Elément de configuration	Valeur
Nom de la TOE	IAS Classic V3 on MultiApp Essential V1.0 on M7793 A12 and G12
Référence de la TOE (étiquette MKS)	IDApplets.IASEssential.Dev_011
Version de l'applet	33 2E 34 2E 65 (v3.4.e)
Date de compilation de l'applet	06/10/15
Identification du système d'exploitation (OS)	19 81
Date de production de l'OS	51 78 (i.e. 27/06/2015)
Version de l'OS	01 00
Fabriquant du microcontrôleur (IC)	40 90
Version de l'IC	72 27

La commande GET DATA utilisée avec les tags suivants permet d'identifier de manière unique la TOE :

- *Tag* DF 30 : version de l'applet ;
- *Tags* 01 03 et 9F 7F : identification de la plateforme.

Ainsi la réponse à la commande GET DATA avec le tag DF 30 est la suivante :

- DF 30 05 33 2E 34 2E 65 90 00,

où 33 2E 34 2E 65 désigne la version de l'applet (« 3.4.e »).
Toutes les applications qui étaient présentes dans la configuration du produit à la disposition de l'évaluateur sont identifiées ci-après par leurs noms et AID[1] :

- MOC applet v1.1 : 4D4F43415F436C69656E74 ;
- MOC server v1.1 : 4D4F43415F536572766572.

La commande GET STATUS permet à l'utilisateur du produit de vérifier quelles applications et quels packages sont installés dans le produit à sa disposition.

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la confidentialité et l'intégrité des clés cryptographiques et des données applicatives pendant l'exécution des opérations cryptographiques ;
- la confidentialité et l'intégrité des données d'authentification et des données applicatives pendant l'exécution des opérations d'authentification ;
- l'isolation des applications entre contextes différents et la confidentialité et l'intégrité des données applicatives entre les applications ;
- l'intégrité de l'exécution du code applicatif ;
- l'authentification du signataire par un code PIN ;
- 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.

1.2.4. Architecture

Le produit, présenté figure 1, est constitué des éléments suivants :

- des fonctionnalités matérielles du composant (CPU, RAM, ROM, EEPROM/FLASH, I/O, coprocesseurs cryptographiques) ;
- d'une partie native composée elle-même :
  - d'un gestionnaire de mémoire *Memory Manager* ;
  - d'un gestionnaire de communication *Communication* ;
  - de librairies cryptographiques *Crypto libs* ;
- d'un système Java Card (JCS : Java Card System) composé :
  - d'un environnement *runtime* (JCRE) ;
  - d'une machine virtuelle Java (VM) ;
  - d'une interface de programmation (Java API) ;
  - d'un gestionnaire d'applications (Card Manager) ;
- de l'application IAS Classic ;
- de l'application MOCA Server v1.1 ;
- de l'application MOCA Client v1.1.

Les applications déjà chargées dans le produit sont toutes identifiées dans le document [ST]. Bien que ces applications standards ne soient pas incluses dans le périmètre de l'évaluation, elles ont été prises en compte dans le processus d'évaluation conformément aux prescriptions de [OPEN]. En effet, ces applications standards ont été vérifiées conformément aux

[1] *Application Identifier.*

contraintes de développements d'applications décrites dans le rapport de certification [CER-PTF].

1.2.5. Cycle de vie

Le cycle de vie du produit peut être décliné de deux façons selon que la pré-personnalisation est réalisée sur module ou produit déjà encarté dans les locaux de *GEMALTO*.

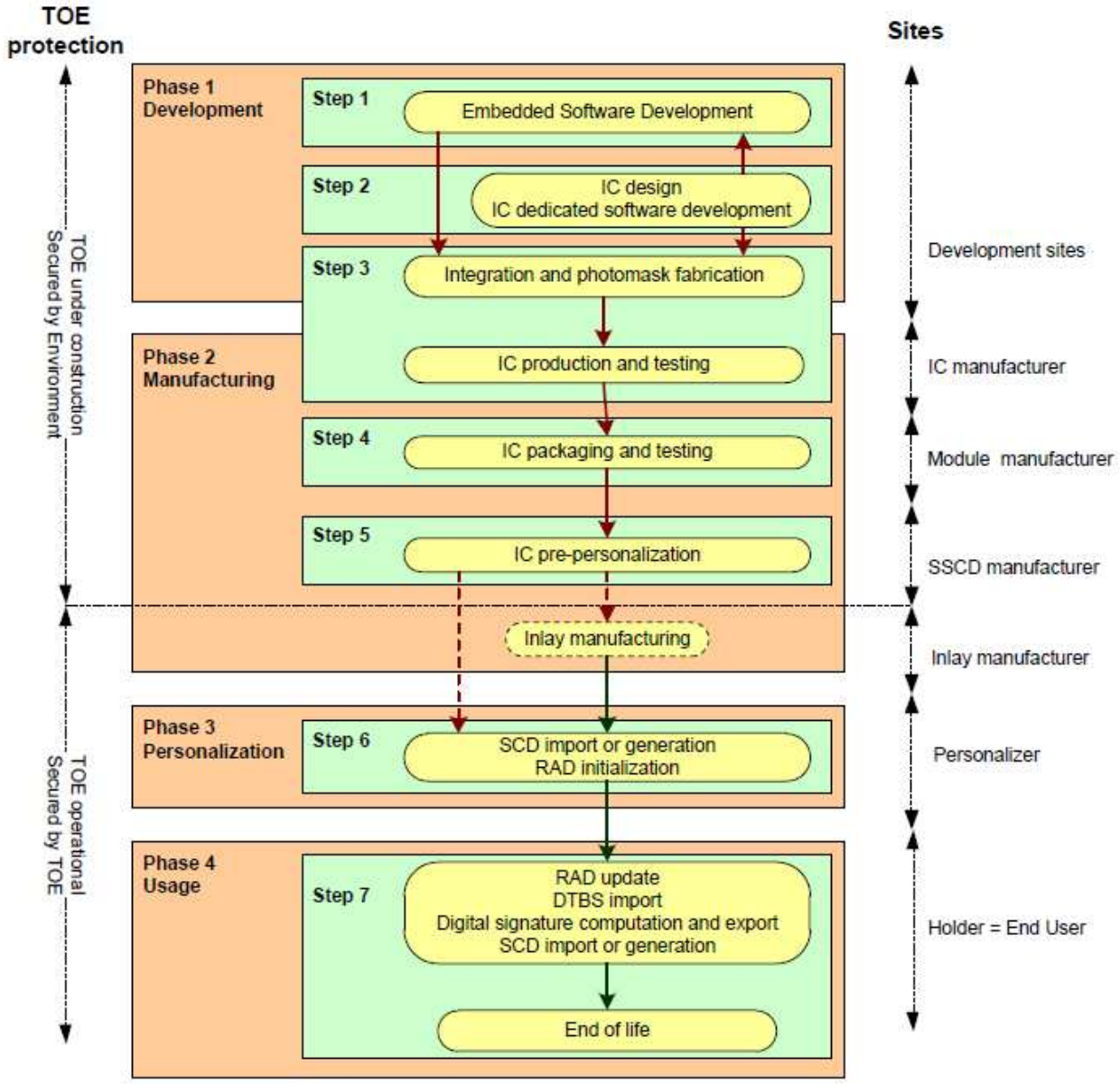

Figure 1 - Pré-personnalisation sur module

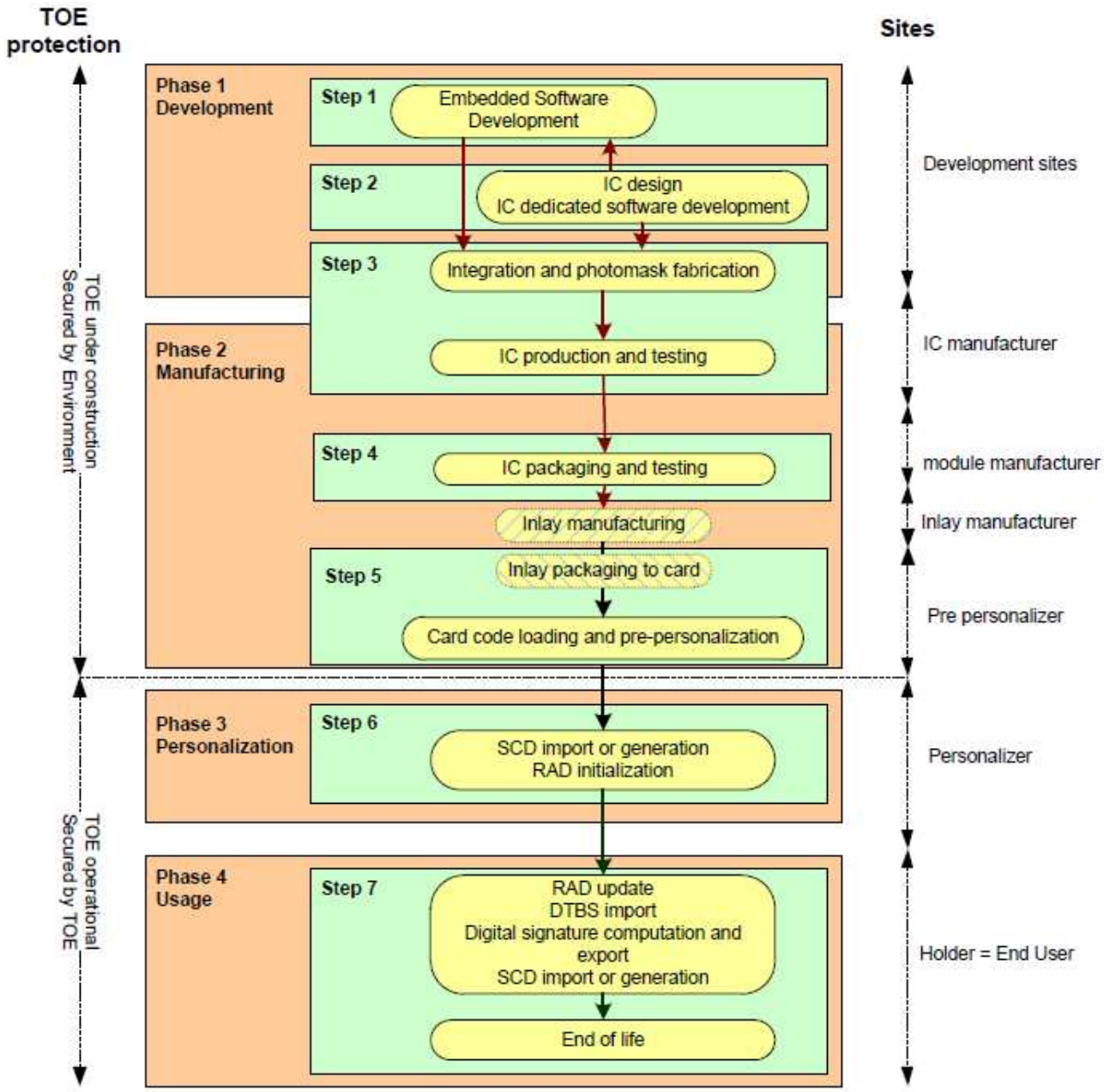

Figure 2 - pré-personnalisation sur produit encarté

Le produit a été développé sur le site suivant :

GEMALTO **Meudon** (Phase 1)

6 rue de la Verrerie
92190 Meudon
France

GEMALTO **Singapore** (Phase 1, 4 & 5)

12 Ayer Rajah Crescent
Singapore 139941
(Singapour)

GEMALTO **Gémenos** (Phase 4 & 5)

Avenue du Pic de Bertagne
13881 Gemenos
France

GEMALTO **Tczew** (Phase 5)

ul. Skarszewska 2
33-110 Tczew
Pologne

GEMALTO **Vantaa** (Phase 5)

Myllynkivenkuja 4
Vantaa, Finland FI-01620
(Finlande)

Ces sites ont fait l'objet d'audits selon le référentiel d'exigences [MSSR]. Certains audits n'ont pas été réalisés spécifiquement pour cette évaluation, mais dans le cadre de campagnes annuelles ou biennales d'audits des sites du développeur ; les résultats ont pu être réutilisés en suivant la méthodologie et les exigences définies dans [NOTE 17].

Le composant sur lequel la plateforme Java Card est embarquée a été développé sur les sites d'*INFINEON*, audités au titre de la certification du microcontrôleur (voir [CER IC]).

Le guide [AGD-OPE] identifie également des recommandations relatives à la livraison des futures applications à charger sur cette carte.
Par ailleurs, les guides [AGD-Dev_Basic] et [AGD-Dev_Sec] décrivent les règles de développement des applications destinées à être chargées sur cette carte ; le guide [AGD-OPE-VA] décrit les règles de vérification qui doivent être appliquées par l'autorité de vérification.

1.2.6. Configuration évaluée

Le certificat porte sur la configuration identifiée au 1.2.4.
L'applet évaluée est celle embarquée avec la plateforme Java Card sur le composant M7793 (mode contact uniquement).

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 au chapitre 3.2 du présent rapport de certification et réalisé selon les processus audités ne remet pas en cause le présent rapport de certification.

Toutes les applications identifiées dans [ST] ont été vérifiées conformément aux contraintes décrites dans [AGD-OPE_VA].

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM] et aux interprétations suivantes :

- *Certification of « open » smart cards products*, version 1.1, 4 février 2013, Joint Interpretation Library ([OPEN]) ;
- *Composite product evaluation for Smart Cards and similar devices*, version 1.4, août 2015, Joint Interpretation Library ([COMP]) ;
- *Minimum site security requirements*, version 1.1, juillet 2013, Joint Interpretation Library ([MSSR]).

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 [CER-PTF]

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 28 janvier 2016, 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 vulnérabilités de conception et de construction 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 « Applet IAS Classic V3 sur plateforme Java Card ouverte MultiApp Essential V1.0 embarquée sur le composant M7793 A12 et 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 futures applications chargées sur ce produit (chargement *post-issuance*) doivent respecter 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].

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.
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] 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 4+	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**	**4**	Complete functional specification
	ADV_IMP				**1**	1	**2**	2	**1**	Implementation representation of TSF
	ADV_INT					**2**	**3**	3		
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**3**	Basic 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	**4**	Problem tracking 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	**1**	Well-defined development tools
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**	**1**	Testing: basic 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 Essential IAS V1 Security Target*, référence : D1341165_93, version 1.0, 15 janvier 2016. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *MultiApp Essential IAS V1 Security Target*, référence : D1341165_93, version : 1.2p, 15 janvier 2016.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report - TULUM project, référence : TULUM-IAS-93_ETR_V1.0, version 1.0, *SERMA* Safety & Security.
[CONF]	Liste de configuration du produit : - LIS: Configuration List for IASClassicV3 on M7793, référence : D1379977_LIS_DOC_IASClassicV3 on M7793.xlsx, version 1.1, *GEMALTO*.
[GUIDES]	[AGD-PRE] Guides d'installation du produit : - *MultiApp Essential V1.0 Software AGD document – IAS Classic V3 Application*, référence : D1354335, version 1.0, *GEMALTO* ; - *Card Personalization Specification requirement for SSCD security evaluation IAS Classic v3*, référence : WG.RND.5.0026, version 1.0, *GEMALTO*; [AGD-OPE] Guides d'utilisation : - *IAS Classic Applet V3 Reference Manual*, référence : D1204099H, version du 21 janvier 2015 ; - [AGD-Dev_Sec] *Guidance for secure application development on Multiapp Essential platforms*, référence : D1349727, version A00, GEMALTO. - [AGD-Dev_Basic] *Rules for applications on Multiapp Essential certified product*, référence : D1349720, version A01, GEMALTO. [AGD-OPE_VA] Mesures pour le chargement d'applications : - *Verification process of Gemalto non sensitive applet loaded in pre-issuance*, référence : D1350374, version A00, GEMALTO; - *Verification process of Third Party non sensitive applet loaded in pre-issuance*, référence : D1350548, version A00, GEMALTO.
[CER-IC]	*Infineon Technologies Security Controller M7793 A12 and G12 with optional RSA2048/4096 v1.02.010 or v1.02.013 or v2.00.002, EC v1.02.010 or v1.02.013 or v2.00.002 and Toolbox v1.02.010 or v1.02.013 or v2.00.002 libraries and with specific IC-dedicated software*, certifié par le BSI sous la référence : BSI-DSZ-CC-0926-2014.

[CER-2015/73]	Plateforme Java Card MultiApp Essential v1.0, en configuration ouverte, sur le composant Infineon M7793 A12 ou G12, certifié sous la référence ANSSI-CC-2015/73 le 5 janvier 2016.
[PP-SSCD-Part 2]	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 le 21 février 2012 sous la référence BSI-CC-PP-0059-2009-MA-01.*
[PP-SSCD-Part 3]	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-Part 4]	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-Part 5]	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-Part 6]	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.*
[PP0035]	Protection Profile, Security IC Platform Protection Profile, version 1.0, juin 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.*

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.
[OPEN]	*Certification of « open » smart cards products*, version 1.1, 4 février 2013, Joint Interpretation Library.
[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.

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