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-2015/73

Plateforme Java Card MultiApp Essential v1.0, en configuration ouverte, sur le composant Infineon M7793 A12 ou G12

Paris, le 5 janvier 2016

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

[Original signé]
Guillaume POUPARD

SÉCURITÉ 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-2015/73

Nom du produit

Plateforme Java Card MultiApp Essential v1.0, en configuration ouverte, sur le composant Infineon M7793 A12 ou G12

Référence/version du produit

Version 1.0

Conformité à un profil de protection

Java Card System Protection Profile – Open Configuration [PP-JCS Open Configuration], version 3.0

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 Technologies

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 6

1.1. PRESENTATION DU PRODUIT 6
1.2. DESCRIPTION DU PRODUIT 6
1.2.1. Introduction 6
1.2.2. Identification du produit 6
1.2.3. Services de sécurité 7
1.2.4. Architecture 8
1.2.5. Cycle de vie 10
1.2.6. Configuration évaluée 12

2. L'EVALUATION 14

2.1. REFERENTIELS D'EVALUATION 14
2.2. TRAVAUX D'EVALUATION 14
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L'ANSSI 14
2.4. ANALYSE DU GENERATEUR D'ALEAS 15

3. LA CERTIFICATION 16

3.1. CONCLUSION 16
3.2. RESTRICTIONS D'USAGE 16
3.3. RECONNAISSANCE DU CERTIFICAT 17
3.3.1. Reconnaissance européenne (SOG-IS) 17
3.3.2. Reconnaissance internationale critères communs (CCRA) 17

ANNEXE 1. NIVEAU D'EVALUATION DU PRODUIT 18

ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE 19

ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION 20

1. Le produit

1.1. Présentation du produit

Le produit évalué est la « Plateforme Java Card MultiApp Essential v1.0, en configuration ouverte, sur le composant Infineon M7793 A12 ou G12 » développé par *GEMALTO* et *INFINEON*.
Le produit se présente sous la forme d'une carte à puce au format ISO 7816 et fonctionnant en mode contact (standard ISO 7816-3) ; la plateforme ouverte Java Card est destinée à fournir des services de sécurité aux applets qui seront installées et chargées sur la carte.

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 au profil de protection Java Card System Protection Profile – Open Configuration, version 3.0 [PP-JCS Open Configuration].

1.2.2. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version certifiée du produit est identifiable par les éléments présents dans la réponse donnée à la commande GET DATA avec le *tag* 9F 7F (voir [GUIDES]) :

40 90 72 27 19 81 51 78 01 00 51 35 a4 75 3a 01 88 29 40 82 51 35 12 93 51 35 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 90 00

Elément	Valeur
Fabricant du microcontrôleur	40 90
Version du microcontrôleur	72 27
Identifiant de l'OS	19 81
Date de production de l'OS	51 78
Version de l'OS	01 00

La commande GET DATA avec le *tag* 01 03 permet en outre d'obtenir les informations propriétaires *GEMALTO* suivantes (voir [GUIDES]) :

Nom de la famille	Java Card	B0
Nom du système d'exploitation	MutliApp Essential v1.0	8D
Numéro du masque	Conf. 1 – G240v1 (SLE77CFX2400PH)	51
	Conf. 2 – G275 (SLE77CLFX2400PH)[i]	52
	Conf. 3 – G275 (SLE77CLFX2400PH)[i]	54
Nom du produit	MutliApp Essential v1.0 – Conf. 1	4A
	MutliApp Essential v1.0 – Conf. 2[i]	4B
	MutliApp Essential v1.0 – Conf. 3[i]	4D
Configuration du produit	Configuration open platform	11
	Configuration open platform + IAS	31
Version du filtre	/	00
Fabricant du microcontrôleur	Infineon	40 90
Version du microcontrôleur	M7793 A12 et G12	72 27
	M7794 A12 et G12[i]	77 50

La principale différence entre le produit et la TOE[ii] (la plateforme) correspond aux applications chargées pré-émission sur cette carte à puce.
Aucune application n'était présente sur le produit à la disposition de l'évaluateur.

La commande GET STATUS permet à l'utilisateur du produit de vérifier quelles applications et quels *packages* sont installés dans l'*Issuer Security Domain* sur le produit à sa disposition (voir également dans le document *MultiApp Essential Operating System Reference Manual* dans [GUIDES]).

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :
- l'initialisation du *Card Manager* et la gestion du cycle de vie de la carte ;
- le chargement et l'installation sécurisés d'applets via le *Card Manager* ;
- la suppression des applications sous le contrôle de l'*Issuer Security Domain* ;
- l'isolation des applications entre contextes différents et la protection de la confidentialité et de l'intégrité des données applicatives entre les applications ;
- l'exécution sécurisée du code applicatif à travers les API ;
- la gestion sécurisée des communications entre la carte et le terminal ;
- les services de base fournis par la plateforme :
    - la vérification de l'environnement d'exécution sur la base des informations fournies par le microcontrôleur ;
    - la vérification du cycle de vie ;
    - la protection des données d'authentification et des clés cryptographiques ;

[i] Cette configuration ne fait pas partie du périmètre de la présente évaluation.
[ii] *Target Of Evaluation* ou cible d'évaluation.

  - la génération de nombres aléatoires ;
  - la gestion des données sensibles et la sauvegarde ;
  - la gestion du contenu de la mémoire ;
  - le bon fonctionnement du mécanisme de pare-feu Java Card ;
- ainsi que les services offerts par le composant sous-jacent.

1.2.4. Architecture

L'architecture du produit dans son ensemble est illustrée sur la Figure 2 ; la TOE est la plateforme Java Card *MultiApp Essential* v1.0, embarquée sur le microprocesseur *INFINEON* M7793.

Elle se compose :

- des éléments matériels 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 ;
  - de bibliothèques cryptographiques ;
- 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 (API) incluant l'API standard Java Card et l'API propriétaire *GEMALTO* ;
  - d'un gestionnaire de *Security Domain* conforme aux spécifications Global Platform ;
  - d'un composant PACE[i] proposant une API pour l'authentification et le *secure messaging* PACE. Ce composant n'est pas activé sur le produit faisant l'objet de cette évaluation (il est activé uniquement sur le composant M7794 fonctionnant en mode sans contact ISO 14443)[ii].

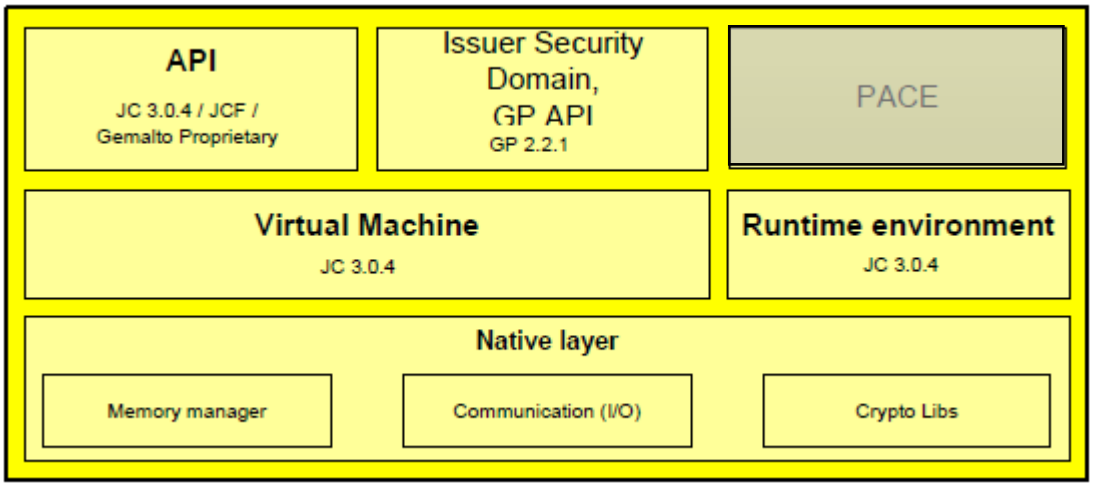

Figure 1 - Architecture de la TOE

[i] *Password Authenticated Connection Establishment*
[ii] Le produit embarqué sur le microcontrôleur M7794 fait l'objet d'une autre évaluation.

La figure suivante illustre l'architecture du produit ainsi que le périmètre de l'évaluation.

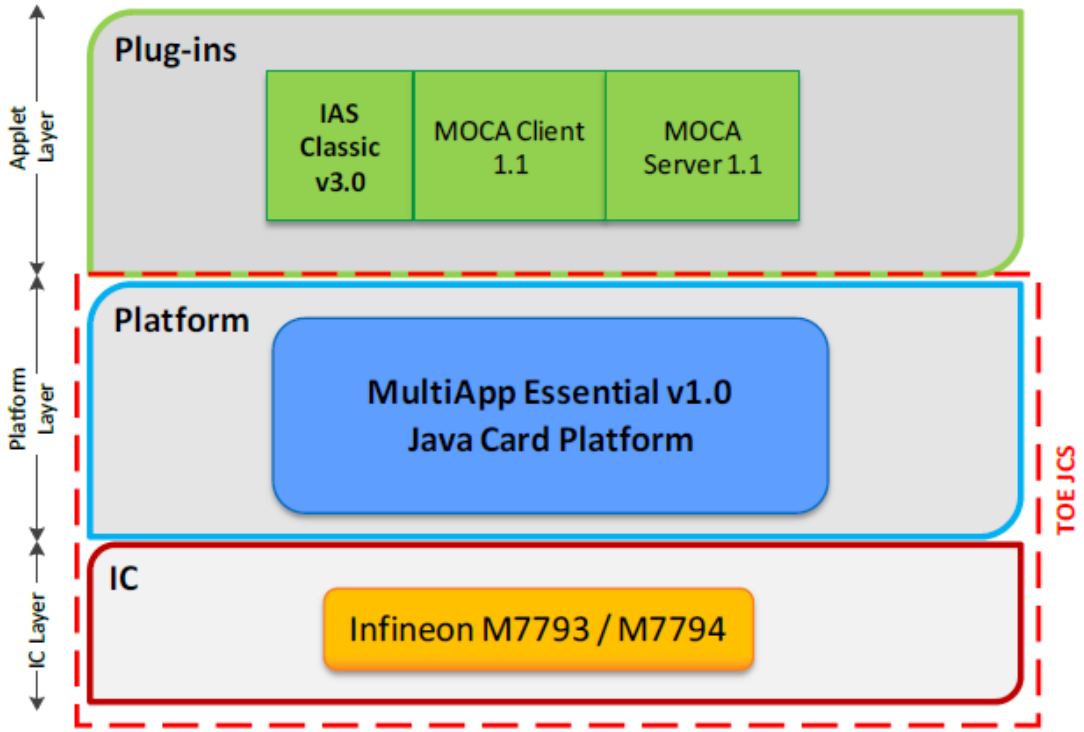

Figure 2 – Architecture du produit et périmètre de l'évaluation[i]

[i] Le présent rapport de certification ne couvre que le produit embarqué sur le composant M7793, bien que le code *GEMALTO* soit identique pour les deux microcontrôleurs. Le produit embarqué sur composant M7794 fait l'objet d'une autre évaluation.

1.2.5. Cycle de vie

Le cycle de vie du produit est celui décrit dans les figures suivantes. Il existe deux variantes selon que le composant embarquant la TOE est livré sous forme de modules ou déjà encarté sur le site *GEMALTO*.

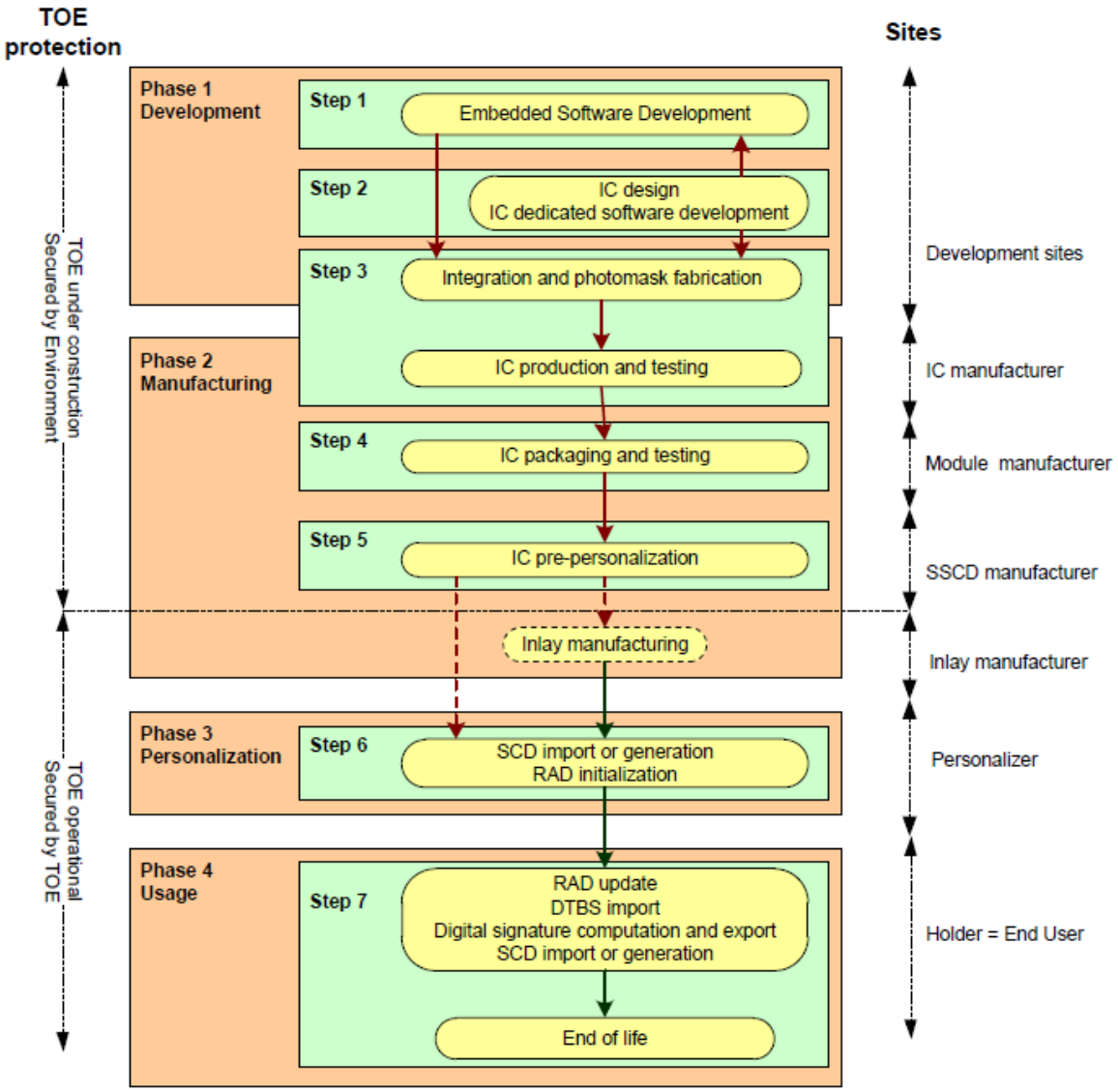

Figure 3 - Cycle de vie du produit – pré-personnalisation sur module sur site *GEMALTO*

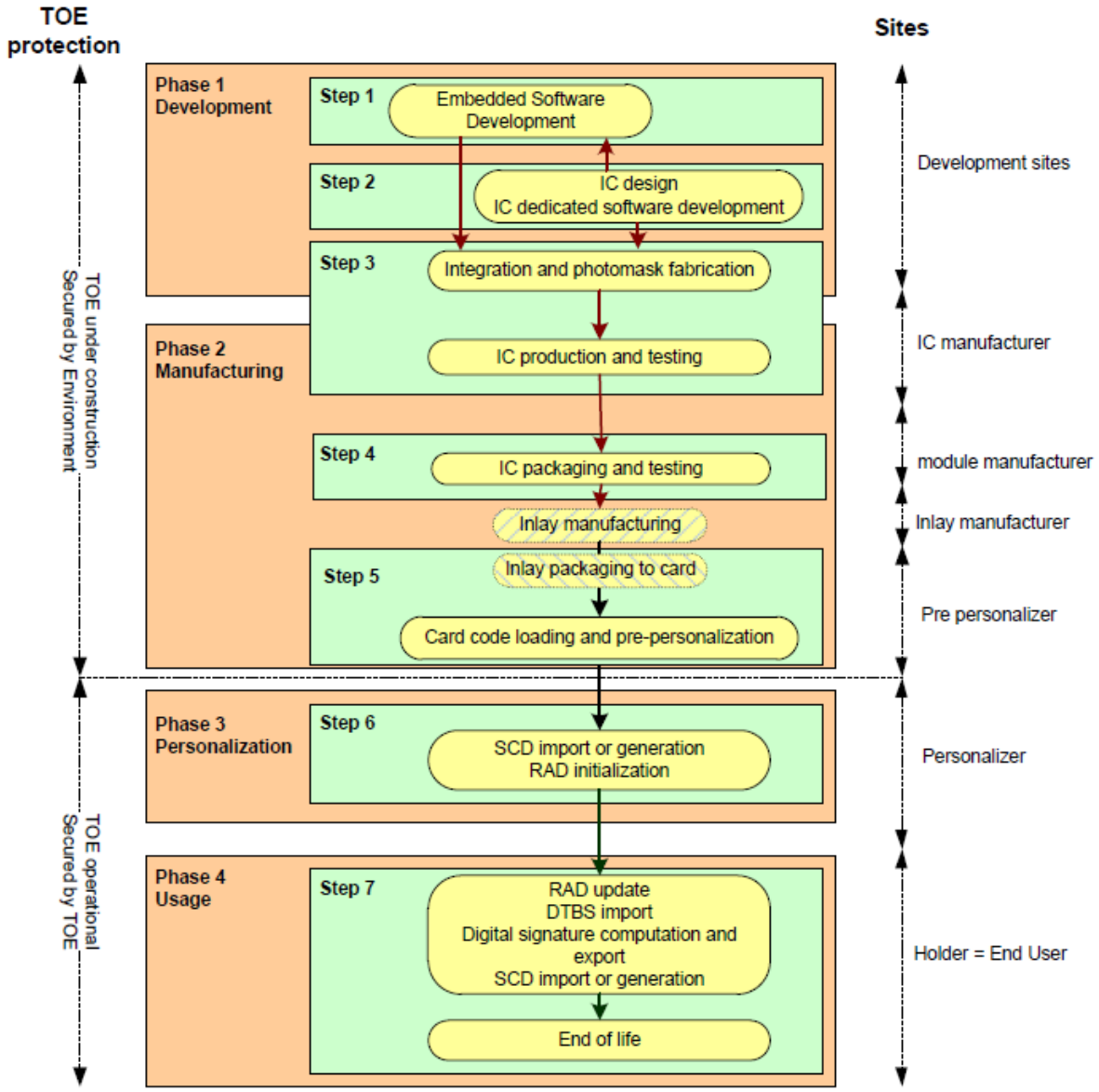

Figure 4 - Cycle de vie du produit - pré-personnalisation sur module encarté sur site *GEMALTO*

La présente évaluation couvre les phases 1 à 5 au titre de la classe ALC.
Les phases 6 et 7 sont couvertes par les guides (classe AGD).

Le chargement des applications post-émission est réalisé une fois le produit sur le terrain dans les mains de l'utilisateur final.

Le produit a été développé sur les sites suivants :

***GEMALTO* Meudon**

6 rue de la Verrerie
92190 Meudon
France

***GEMALTO* Tczew**

ul. Skarszewska 2
33-110 Tczew
Pologne

***GEMALTO* Singapore**

12 Ayer Rajah Crescent
Singapore 139941
(Singapour)

***GEMALTO* Vantaa**

Myllynkivenkuja 4
Vantaa, Finland FI-01620
(Finlande)

***GEMALTO* Gémenos**

Avenue du Pic de Bertagne
13881 Gemenos
France

***GEMALTO* Curitiba**

Rodovia Dep. Leopoldo Jacomel, 13102
83323-410 – Pinhais – PR
Brésil

***GEMALTO* La Ciotat**

La Vigie – Avenue du Jujubier
13705 La Ciotat Cedex
France

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 suivies par le *card issuer*, qui joue le rôle d'autorité de vérification.

1.2.6. Configuration évaluée

Le certificat porte sur la configuration identifiée au 1.2.4.
La plateforme évaluée est celle embarquée 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.
Toutes les applications devant être chargées sur la carte doivent faire l'objet de vérifications conformément aux règles 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 du microcontrôleur M7793 (A12 et G12) au niveau EAL5 augmenté des composants ALC_DVS.2, et AVA_VAN.5, conforme au profil de protection [PP0035]. Ce microcontrôleur a été certifié le 4 avril 2014 sous la référence [CER-IC].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 4 décembre 2015, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

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

La cotation des mécanismes cryptographiques 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 « Plateforme Java Card MultiApp Essential v1.0, en configuration ouverte, sur le composant Infineon M7793 A12 ou 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 pre-émission et post-émission) doivent respecter les contraintes de développement de la plateforme (guides [AGD-Dev_Basic] et [AGD-Dev_Sec] selon la sensibilité de l'application considérées) ; le chargement des applications relève de la responsabilité du *card issuer* ;
- le *card issuer*, qui joue le rôle d'autorité de vérification, doit également appliquer le guide [AGD-OPE_VA] pour les opérations de vérification.

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 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 Essential: JCS Security Target on M7793*, référence : D1341162-93, version 1.4, *GEMALTO*. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *MultiApp Essential on M7793 Security Target Lite*, référence : D1341162-93, version 1.4p, *GEMALTO*.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report TULUM Project*, référence : TULUM-JCS-93_ETR_v1.1, version 1.1, *SERMA TECHNOLOGIES*.
[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.
[CONF]	Liste de configuration du produit : - LIS: Configuration List for platform, référence : D1369532, version 1.0, *GEMALTO* ; - D1366815_LIS_DOC_PLF93, version 1.4, *GEMALTO*.
[GUIDES]	[AGD-PRE] Guide d'administration du produit : - *MultiApp Essential AGD_PRE document - Javacard Platform*, référence D1352259, version 1.0, *GEMALTO*. [AGD-OPE] Guide d'utilisation du produit : - *MultiApp Essential V1 Software, AGD_OPE document – Javacard Platform*, référence : D1353174, version 1.4, *GEMALTO*. - *MultiApp Essential Operating System Reference Manual*, référence : D1352558B, version B, *GEMALTO*. - [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*.
[PP-JCS Open Configuration]	*Java Card System Protection Profile – Open Configuration*, version 3.0, certifié sous la référence : ANSSI-PP-2010-03M01, mai 2012.

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 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.
[NOTE 17]	Note d'application – Réutilisation des composants d'assurance ALC, version 1.0, 5 mai 2015.
[MSSR]	*JIL – Minimum Site Security Requirements*, version 1.1, Juillet 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.

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