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-2012/38

Plateforme ID Motion V1 avec AMD 113v3 sur composants M7820 A11

(ID Motion V1 platform with AMD 113v3 embedded on M7820 A11 components)

Paris, le 21 décembre 2012

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

Patrick Pailloux
[ORIGINAL SIGNE]

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.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2012/38

Nom du produit

Plateforme ID Motion V1 avec AMD 113v3 sur composants M7820 A11

Référence/version du produit

Version du logiciel embarqué : Plateformes Multos 74 et 75
Version du code correctif : AMD 113v3
Variantes du composant M7820 A11 : Microcontrôleurs SLE78CLXxxxxP et SLE78CLXxxxxPM

Conformité à un profil de protection

Néant

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

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

THALES (TCS – CNES)

18 avenue Edouard Belin, BPI1414, 31401 Toulouse Cedex 9, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit est reconnu au niveau EAL4.

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 « Plateforme ID Motion V1 avec AMD 113v3 sur composants M7820 A11 » développée par Gemalto et Infineon. Les variantes des composants M7820 A11 utilisées sont les microcontrôleurs SLE78CLXxxxxP et SLE78CLXxxxxPM (cette dernière variante supporte une interface au standard Mifare).
La version de la plateforme est 75 pour le microcontrôleur SLE78CLXxxxxP et 74 pour le microcontrôleur SLE78CLXxxxxPM. La version du code correctif AMD (« *Additional Multos Data* » - dans la terminologie Multos) est 113v3 quelle que soit la variante du composant.
Le produit évalué est de type « carte à puce » avec et sans contact. Il est conçu de façon à ce que plusieurs applications puissent être chargées et exécutées de façon sécurisée sur la carte à puce. Ces applications sont écrites dans un langage, indépendant du composant sous-jacent, nommé MEL (« *Multos Executable Language* » – langage exécutable Multos). Les applications en langage MEL sont interprétées par le système d'exploitation Multos.

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. Elle s'inspire du profil de protection [PP/0010] certifié par l'ANSSI.

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 détaillés au chapitre « *1.1 Security Target Identification* » de la [ST] :

Variantes du composant	*SLE78CLxxxxPM (Interface Mifare)*	*SLE78CLxxxxP*	*Commande pour obtenir ces données*
Identification du composant	SLE78CLX1600PM SLE78CLX1440PM SLE78CLX800PM SLE78CLX480PM SLE78CLX360PM	SLE78CLX1600P SLE78CLX1440P SLE78CLX1280P SLE78CLX800P SLE78CLX480P SLE78CLX360P	
Identifiant du masque	G230M	G230	
Version de la plateforme	**0x74**	**0x75**	GET MANUFACTURER DATA
Version du code correctif (AMD)	**0113v003**	**0113v003**	GET CONFIGURATION DATA

Les variantes de composants prises en compte ici diffèrent uniquement par leur taille mémoire et par la présence ou non de l'interface Mifare.

1.2.3. Services de sécurité

Les services de sécurité fournis par le produit sont détaillés au chapitre « *7.1 Security Functionality* » de la [ST], ils sont résumés ci-après :

- le chargement d'applications ;
- la suppression d'applications ;
- la vérification de la signature des applications ;
- le déchiffrement des applications ;
- le chargement des données de contrôle MSM (*Multos Security Manager* – gestionnaire de sécurité Multos) ;
- l'écrasement des données critiques ;
- la gestion de l'exécution des applications ;
- la protection de la réinitialisation ;
- le contrôle d'intégrité des données sensibles de la plateforme (applications, clés internes…) ;
- l'autotest au démarrage et pendant l'initialisation ;
- la gestion des réactions aux tentatives de pénétration ;
- l'authentification de la carte.

1.2.4. Architecture

L'architecture du produit, détaillée au chapitre « *1.3.1 Product Description* » de la [ST], est illustrée par la figure 1.

Le produit est une carte à puce constituée :

- du composant M7820 A11 sous la forme d'une variante de microcontrôleur (voir liste plus haut au chapitre « 1.2.2 Identification du produit ») ;
- de la plateforme Multos « ID Motion V1 platform » avec l'OS Multos en version 75 pour les composants SLE78CLXxxxxP et 74 pour les composants SLE78CLXxxxxPM ;
- du code correctif, dit « *AMD* », en version 113v3.

D'autres applications, en dehors du périmètre de cette évaluation, sont embarquées dans la mémoire du produit mais ne sont pas actives dans la configuration évaluée.

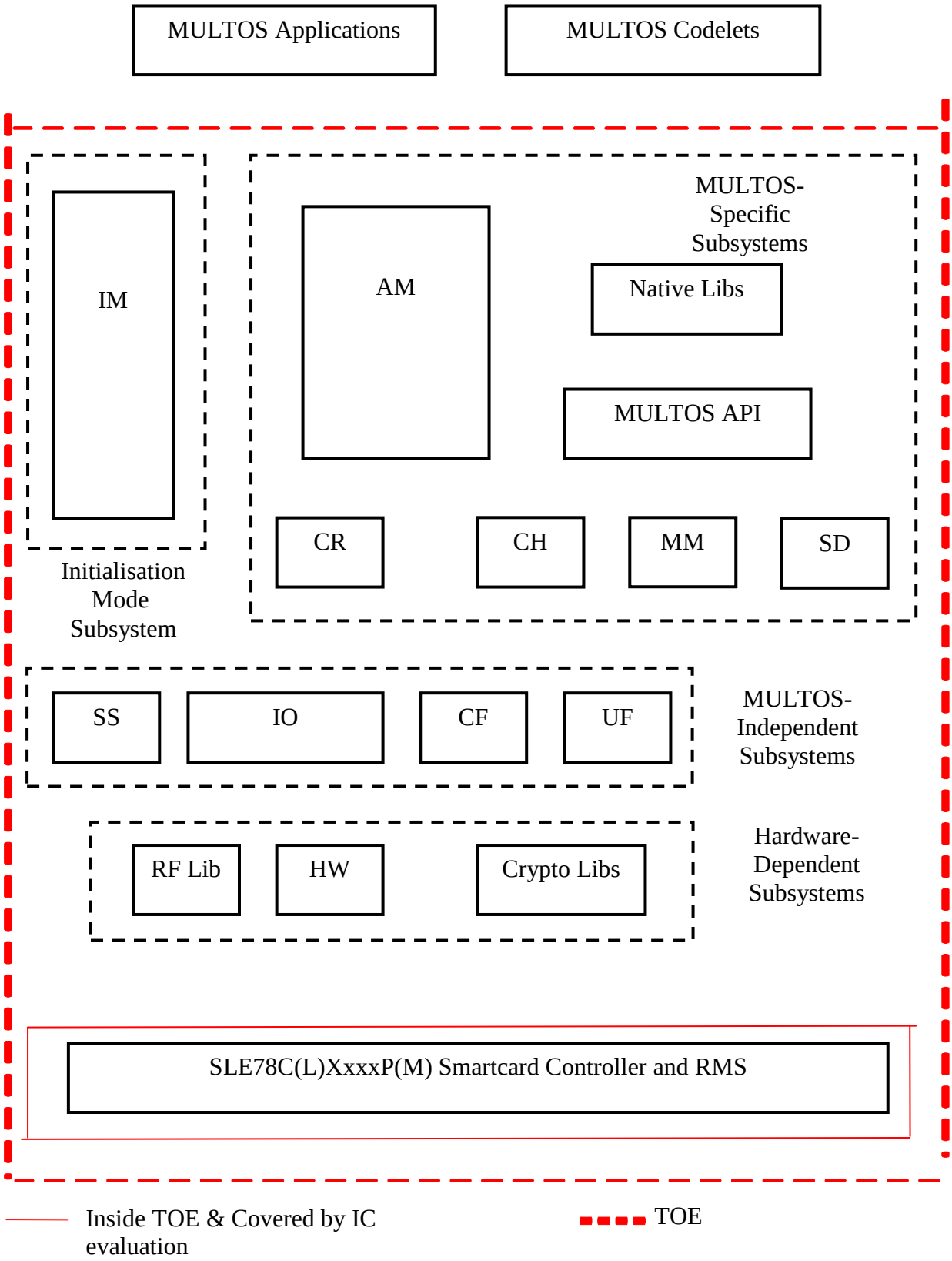

Figure 1: Architecture

1.2.5. Cycle de vie

Le cycle de vie du produit, détaillé au chapitre « *1.3.3 Smartcard Product Life Cycle* » de la [ST], est celui d'une carte à puce, il est illustré par la figure 2.

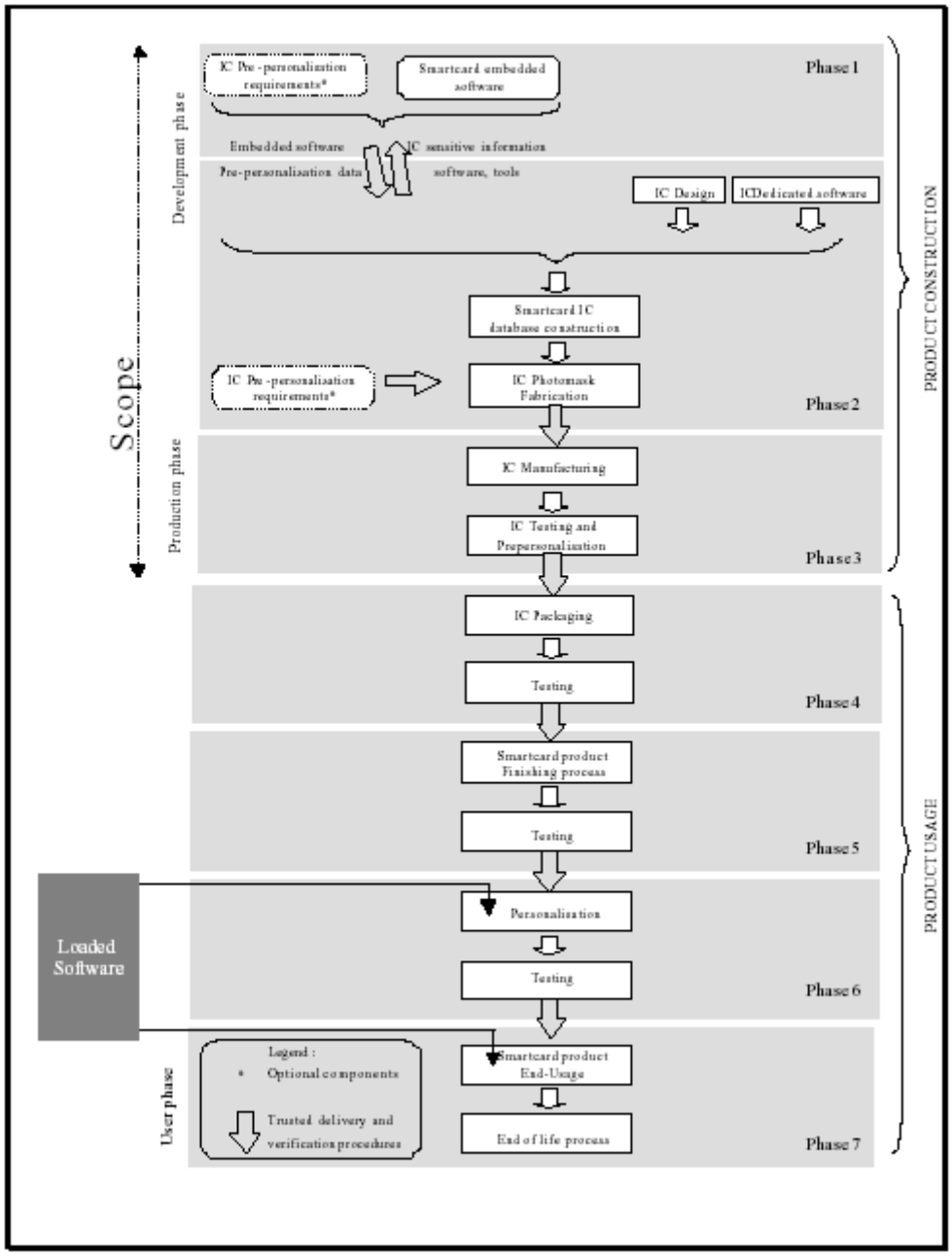

Figure 2: Cycle de vie

Le point de livraison est situé après l'étape 3. Les étapes 4, 5 et 6 ont été prises en compte durant l'évaluation au travers des guides (activités AGD). Les tests ont porté sur les fonctionnalités du produit disponibles aux étapes 4, 5, 6 et 7 (activités ATE et AVA).

Le produit a été développé et fabriqué durant les étapes 1 à 3 sur les sites suivants :

Gemalto - Meudon

6 Rue de la verrerie
92190 Meudon
France

Multos international - Sydney

Level 14, the Zenith - Tower B, 821 Pacific Highway
Chatswood NSW 2067
Australie

Gemalto - Vantaa

Turvalaaksonkaari 2
FI-01741 Vantaa
Finlande

Gemalto - Gemenos

Avenue du Pic de Bertagne
13881 Gémenos
France

Gemalto - Tczew

Ul. Skarszewska 2
83-110 Tczew
Pologne

Gemalto - Singapour

12 Ayer Rajah Crescent
Singapor 139941
Singapour

Le microcontrôleur a été développé et fabriqué par Infineon Technologies AG sur ses sites (voir [BSI-DSZ-CC-0813-2012]).

1.2.6. Configuration évaluée

Le certificat porte sur la configuration telle que présentée au chapitre « 1.2.4 Architecture ».

L'évaluateur a effectué ses tests sur les différentes configurations suivantes :

- masque G230M sur composant SLE78CLX1600PM (version de la plateforme : 0x74, version du code correctif : 0113v003) ;
- masque G230 sur composant SLE78CLX1600P (version de la plateforme : 0x75, version du code correctif : 0113v003).

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 3** [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM] et à la note [ANSSI-CC-NOTE.10].

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 [CC IC] et [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [CC 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 intitulé « *Infineon smart card IC (Security Controller) M7820 A11 with optional RSA2048/4096 v1.02.008, EC v1.02.008, SHA-2 v1.01 and Toolbox v1.02.008 libraries and with specific IC dedicated software* » au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5, conforme au profil de protection [BSI-PP-0035-2007]. Ce microcontrôleur a été certifié par le BSI (voir [BSI-DSZ-CC-0813-2012]) le 6 juin 2012.

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 9 novembre 2012, 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 visé.

2.4. Analyse du générateur d'aléas

Le générateur d'aléas du produit était en dehors du périmètre de l'évaluation et n'a pas été analysé.

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 ID Motion V1 avec AMD 113v3 sur composants M7820 A11», 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.

Ce certificat donne une appréciation de la résistance du produit « Plateforme ID Motion V1 avec AMD 113v3 sur composants M7820 A11», à des attaques génériques du fait de l'absence d'application spécifique embarquée. Ces attaques ont été menées, entre autres, avec le chargement d'applications malveillantes conçues pour les besoins de test par l'évaluateur.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'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 EAL4 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, Singapour, 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 : - ID Motion V1 Security target, référence ST_D184441, version 1.6.2, 12 juillet 2012, Gemalto. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - ID Motion V1 Security target, référence ST_D184441-Pub, 12 juillet 2012, Gemalto.
[RTE]	Rapport technique d'évaluation : - Evaluation technical report - Project: PODESTAT, référence POD_ETR, version 1.3r2b, 9 novembre 2012, THALES (TCS – CNES). Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - Evaluation technical report lite - Project: PODESTAT, référence POD_ETR Lite, version 113_2.0, 16 novembre 2012, THALES (TCS – CNES).
[CONF]	Liste de configuration du produit : - Manufacturing Data Pack, référence MI-DP-0182, version 1.1, Gemalto.
[GUIDES]	Guide de préparation du produit : - Keycorp MULTOS - Mask Verification Procedure, référence SIM-PR-0012, version 1.2, Multos. Guide d'opération du produit : - Enablement, référence MAO-DOC-HOW-002, version 1.0, Multos. - MULTOS Developer's Reference Manual, référence MAO-DOC-TEC-006, version 1.46, Multos. - Guide to Loading and Deleting Applications - GLDA, référence MAO-DOC-TEC-008, version 2.21, Multos. - Guide to Generating Application Load Units - GALU, référence MAO-DOC-TEC-009, version 2.52, Multos. - Security Guidance for MULTOS Application Developers, référence MI-MA-0031, version 1.5, Multos.

[BSI-PP-0035-2007]	Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.*
[BSI-DSZ-CC-0813-2012]	Certificat BSI délivré le 6 juin 2012 pour le produit : « *Infineon smart card IC (Security Controller) M7820 A11 with optional RSA2048/4096 v1.02.008, EC v1.02.008, SHA-2 v1.01 and Toolbox v1.02.008 libraries and with specific IC dedicated software* »
[PP/0010]	Certificat ANSSI délivré en janvier 2001 pour le profil de protection Smart Card IC with Multi-Application Secure Platform Version 2.0.
[ANSSI-CC-NOTE.10]	Note d'application : « Certification d'applications sur plateformes ouvertes cloisonnantes ». 16 décembre 2010, ANSSI.

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, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2009-03-002 version 3.0, revision 1, March 2009.
[JIWG AP]	Mandatory Technical Document - Application of attack potential to smart-cards, JIWG, version 2.8, January 2012.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, reference CCDB-2007-09-001 version 1.0, revision 1, September 2007.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.
[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 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité, voir http://www.ssi.gouv.fr.