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-2013/40

Virtual Machine of Multos M3 - G230M mask with AMD 113v4

Paris le 4 juillet 2013

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

[ORIGINAL SIGNE]

Patrick Pailloux

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-2013/40

Nom et version du produit

Virtual Machine of Multos M3
G230M mask with AMD 113v4

Conformité à un profil de protection

Néant

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 7

Développeurs

Multos International
Level 14, Tower B, Zenith Centre
821 Pacific Highway
Chatswood, NSW, Australia 2067

Trusted Labs
5 rue du Baillage
78000 Versailles, France

Commanditaire

Multos International
Level 14, Tower B, Zenith Centre
821 Pacific Highway
Chatswood, NSW, Australia 2067

Centre d'évaluation

THALES (TCS – CNES)
18 avenue Edouard Belin, BPI1414, 31401 Toulouse Cedex 9, France

Accords de reconnaissance applicables

CCRA

Le produit est reconnu au niveau EAL4.

SOG-IS

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

La cible d'évaluation est la fonctionnalité « *Virtual Machine of Multos M3 - G230M mask with AMD 113v4* » développée par Multos International et Trusted Labs.
Cette fonctionnalité fait partie du produit « Plateforme Multos M3 avec AMD 113v4 masquée sur composant SLE78CLX1600PM » développé par Multos International et Infineon, et certifié par l'ANSSI sous la référence [ANSSI-CC-2013/39].
Ce produit est de type « carte à puce » en mode contact, et en mode sans contact si l'interface Mifare est supportée par le composant. 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 nommé MEL (« *Multos Executable Language* [1] »).
Les applications en langage MEL sont interprétées par la machine virtuelle («*Virtual Machine »)* qui est l'objet de cette évaluation.

1.2. Description du produit

La cible de sécurité [ST] définit la fonctionnalité de sécurité évaluée et son environnement d'exploitation.

1.2.1. 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 « *1.3 TOE reference* » de la [ST].
L'identifiant du masque G230M (**0x77**) et la version du code correctif (**0113v004**) peuvent être obtenus respectivement par les commandes « GET MANUFACTURER DATA » et « GET CONFIGURATION DATA ».

1.2.2. Services de sécurité

Les services de sécurité fournis spécifiquement par la cible d'évaluation sont détaillés au chapitre « *7.1 Security Functionality* » de la [ST], ils sont résumés ci-après :

- gestion de la mémoire en fonction du cycle de vie (ouverture, chargement, création, sélection, dé-sélection, sortie, effacement) ;
- interprétation des primitives et instructions Multos appelées par les applications chargées ;
- gestion des interactions entre les applications chargées.

Les services de sécurité fournis par le produit « Plateforme Multos M3 avec AMD 113v4 masquée sur composant SLE78CLX1600PM » sont détaillés dans le rapport de certification [ANSSI-CC-2013/39].

[1] Langage Exécutable Multos.

1.2.3. Architecture

L'architecture du produit « Plateforme ID Motion V1 avec AMD 122v1 sur composants M7820 A11 », détaillée au chapitre « *1.5 TOE Description* » de la [ST], est illustrée par la figure 1.

Le produit est une carte à puce constituée :

- du composant SLE78CLX1600PM ;
- de la plateforme Multos M3 (masque G230M, identifiant 77) ;
- du code correctif, dit « *AMD* », en version 113v4 ;
- d'applications, en dehors du périmètre de cette évaluation, embarquées dans la mémoire du produit mais inactives dans la configuration évaluée.

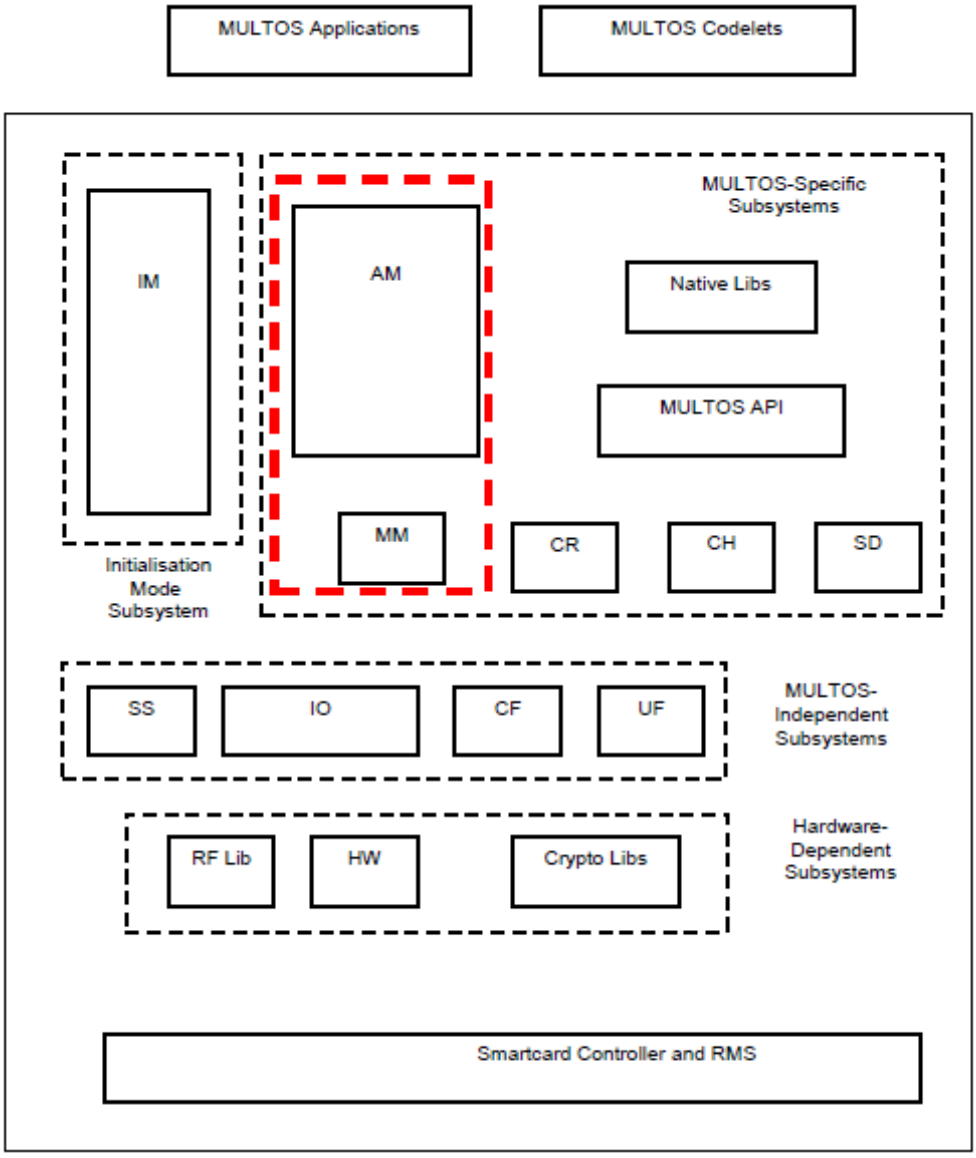

Figure 1: Architecture du produit

L'architecture du produit est composée des éléments suivants:

- composant SLE78CLX1600PM ;
- ensemble des sous-systèmes matériels (RF Lib , HW, Crypto Libs) ;
- ensemble des sous-systèmes indépendants Multos (SS, IO, CF, UF) ;
- ensemble des sous-systèmes d'initialisation (IM) ;
- ensemble des sous-systèmes spécifiques Multos (CR, CH, SD, Multos API, Native Libs, MM, AM) ;
- applications Multos chargées en ROM et en EEPROM (« *codelets* »).

La cible d'évaluation (ensemble défini en rouge sur la figure) est constituée des sous-systèmes:

- MM (« *Application Memory Manager* [1] ») qui gère la mémoire appartenant aux applications et fournit les services nécessaires au chargement, à l'exécution et à l'effacement de ces applications ;
- AM (« *Application Abstract Machine* [2] ») qui interprète et exécute les instructions des applications gérées par le MM.

La cible d'évaluation maintient une stricte séparation entre applications : chaque application ne peut accéder qu'à son propre espace mémoire (code et données) et ne peut obtenir un accès non-autorisé au code ou aux données d'une autre application.

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

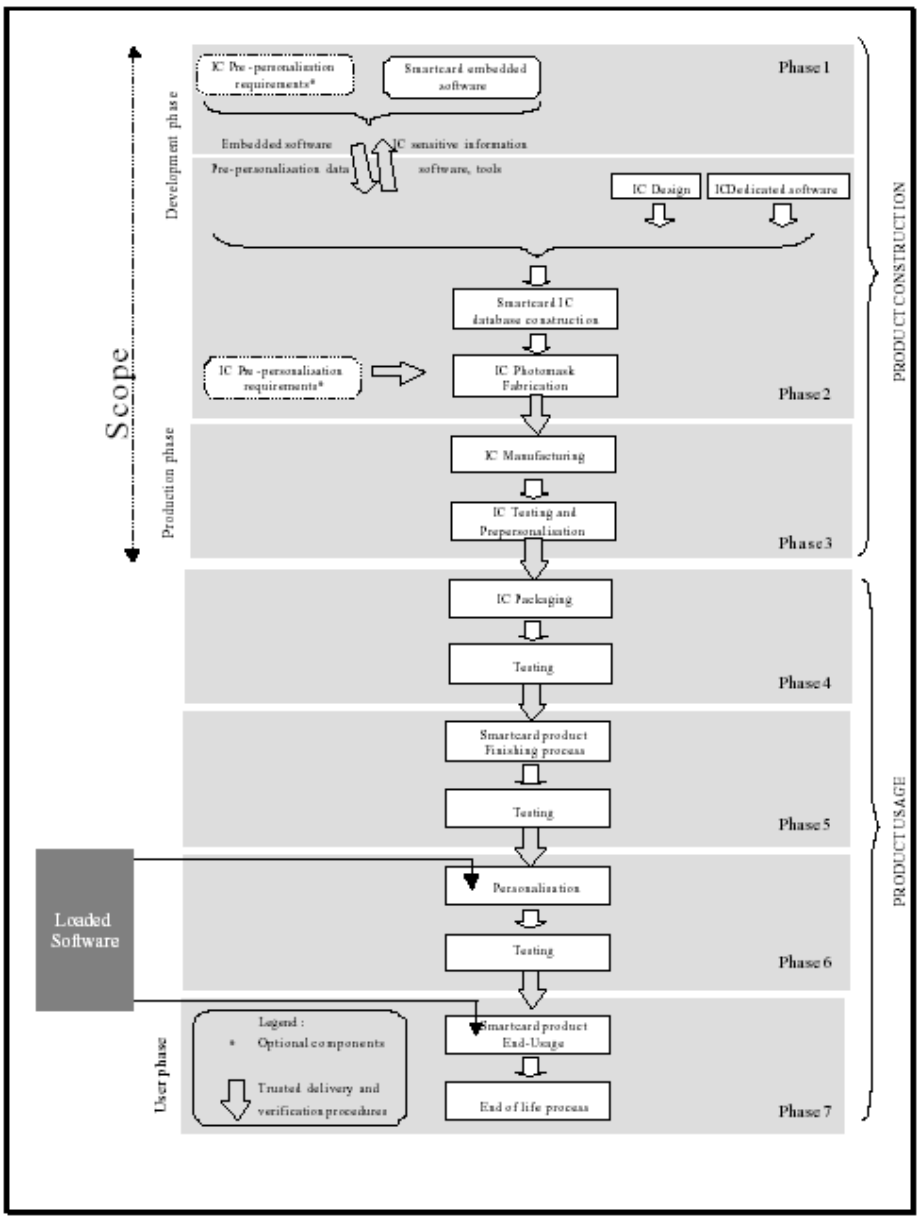

Figure 2: Cycle de vie

[1] Gestionnaire d'Applications Mémoire.
[2] Machine Abstraite d'Application.

Au regard du cycle de vie, le produit est évalué en sortie de la phase 3 du cycle de vie.

La cible d'évaluation a été développée durant les étapes 1 à 3 sur les sites suivants :

Multos international - Sydney

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

Trusted Labs - Versailles

5 rue du Baillage
78000 Versailles
France

Le produit a été développé et fabriqué par Multos international sur ses sites (voir [ANSSI-CC-2013/39]).

1.2.5. Configuration évaluée

Le certificat porte sur la configuration telle que présentée au chapitre « 1.2.3 Architecture ».

L'évaluateur a effectué ses tests sur la configuration suivante :

- masque G230M sur composant SLE78CLX1600PM avec librairie etravel.

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], au document [METHODES-FORMELLES], aux notes [ANSSI-CC-NOTE.10] et [ANSSI-CC-NOTE.12].

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 [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 s'appuie sur les résultats d'évaluation du produit « Plateforme Multos M3 avec AMD 113v4 masquée sur composant SLE78CLX1600PM » certifié le 12 juin 2013 sous la référence ANSSI-CC-2013/39 ([ANSSI-CC-2013/39]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 10 avril 2013, 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

Le produit ne comporte pas de mécanismes cryptographiques entrant dans le périmètre d'évaluation.

2.4. Analyse du générateur d'aléas

Le produit ne comporte pas de générateur d'aléas entrant dans le périmètre d'évaluation.

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 la fonctionnalité *« Virtual Machine of Multos M3 - G230M mask with AMD 113v4 »* soumise à l'évaluation répond aux caractéristiques de sécurité spécifiées dans la cible de sécurité [ST] pour le niveau d'évaluation EAL 7.

3.2. Restrictions d'usage

Ce certificat porte sur la fonctionnalité « *Virtual Machine of Multos M3 - G230M mask with AMD 113v4* » spécifiée au chapitre 1.2 du présent rapport de certification. Il donne une appréciation de la résistance de cette fonctionnalité à des attaques qui sont fortement génériques du fait de l'absence d'application spécifique embarquée.

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 :

[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.

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[1], 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 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 7	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**	**6**	Complete semi-formal functional specification with additional formal specification
	ADV_IMP				**1**	1	**2**	2	**2**	Complete mapping of the implementation representation of the TSF
	ADV_INT					**2**	**3**	3	**3**	Minimally complex internals
	ADV_SPM						**1**	1	**1**	Formal TOE security policy model
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**6**	Complete semiformal modular design with formal high-level design presentation
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	**5**	Advanced support
	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**	**2**	Measurable life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**3**	Compliance with implementation standards – all parts
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	**3**	Rigorous analysis of coverage
	ATE_DPT			**1**	1	**3**	3	**4**	**4**	Testing: implementation representation
	ATE_FUN		**1**	1	1	1	**2**	2	**2**	Ordered functional testing

	ATE_IND	**1**	**2**	2	2	2	2	**3**	**3**	Independent testing - complete
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 : - Multos M3 Virtual Machine Security target, référence MI-SP-0473, version 1.0, 27/02/2013, Multos international. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Multos M3 Virtual Machine Public Security target, référence MI-SP-0477, version 1.0, 27/02/2013, Multos international.
[RTE]	Rapport technique d'évaluation : - Evaluation technical report - Project: PMI_EAL7, référence PMI_EAL7_ETR, version 1.0, 10/04/2013, THALES (TCS – CNES).
[CONF]	Listes de configuration du produit : - Manufacturing Data Pack, référence MI-DP-0092, version 1.2, Multos International. - VM EAL7 Certification Manufacturing Data Pack, référence MI-DP-0209, version 1.0, Multos International.
[GUIDES]	Guide de préparation du produit : - Keycorp MULTOS - Mask Verification Procedure, référence SIM-PR-0012, version 1.2, Multos. Guides d'opération du produit : - 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. - Security Guidance for MULTOS Application Developers, référence MI-MA-0031, version 1.5, Multos.
[ANSSI-CC-2013/39]	Certificat ANSSI délivré le 12 juin 2013 : « Plateforme Multos M3 avec AMD 113v4 masquée sur composant SLE78CLX1600PM » sous la référence ANSSI-CC-2013/39.

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.
[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.
[ANSSI-CC-NOTE.10]	Note d'application : « Certification d'applications sur plateformes ouvertes cloisonnantes », 16 décembre 2010, référence ANSSI-CC-NOTE/10.0, voir http://www.ssi.gouv.fr.
[ANSSI-CC-NOTE.12]	« Note d'application - Modélisation formelle des politiques de sécurité d'une cible d'évaluation », 25 mars 2008, référence ANSSI-CC-NOTE/12.1, voir http://www.ssi.gouv.fr.
[METHODES-FORMELLES]	« Remarques relatives à l'emploi des méthodes formelles (déductives) en sécurité des systèmes d'information », 14 avril 2008, Eric Jaeger, voir http://www.ssi.gouv.fr.