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-2010/14

Plateforme MULTOS ML1, avec correctif AMD 0096v004, masquée sur deux variantes de composants Infineon SLE66CLX360PEM (variante produit ML1-36K-5F) et SLE66CLX800PEM (variante produit ML1-80K-63)

Paris, le 7 mai 2010

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-2010/14

Nom du produit

Plateforme MULTOS ML1, avec correctif AMD 0096v004, masquée sur deux variantes de composants Infineon SLE66CLX360PEM (variante produit ML1-36K-5F) et SLE66CLX800PEM (variante produit ML1-80K-63)

Référence/version du produit

Pour la variante ML1-36K-5F, l'identifiant composant est 5F
Pour la variante ML1-80K-63, l'identifiant composant est 63
La version du correctif de la plateforme est : AMD 0096v004

Conformité à un profil de protection

Néant

Critères d'évaluation et version

Critères Communs version 3.1

Niveau d'évaluation

EAL 4 augmenté

ALC_DVS.2, AVA_VAN.5

Développeur(s)

Multos International

Level 14, Zenith Tower B, 821 Pacific Highway, Chatswood NSW 2067, Sydney, Australia

Infineon Technologies AG

AIM CC SM PS, Am Campeon 1-12, 85579 Neubiberg, Germany

Commanditaire

Multos International

Level 14, Zenith Tower B, 821 Pacific Highway, Chatswood NSW 2067, Sydney, Australia

Centre d'évaluation

THALES - CEACI (T3S – CNES)

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

Tél : +33 (0)5 62 88 28 01 ou 18, mél : nathalie.feyt@thalesgroup.com

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, publié au Journal officiel de la République française. 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 MULTOS ML1, avec correctif AMD 0096v004, masquée sur deux variantes de composants Infineon SLE66CLX360PEM (variante produit ML1-36K-5F) et SLE66CLX800PEM (variante produit ML1-80K-63)**,** portant les identifiants composants respectivement 5F et 63, développée par Multos International.

La TOE (*Target Of Evaluation* – cible d'évaluation) est un système d'exploitation pour carte à puce. 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 MEL sont interprétées par le système d'exploitation Multos plutôt que compilées et exécutées par le processeur du composant sous-jacent.

1.2. Description du produit

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.

1.2.1. Identification du produit

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

Comme indiqué dans [ST], au §1.1, la version certifiée du produit est identifiable par les éléments suivants :

Variante du produit	*ML1-36K-5F*	*ML1-80K-63*	*Commande pour obtenir ces données*
Composant sous-jacent	SLE66CLX360PEM	SLE66CLX800PEM	
Identifiant composant	**5F**	**63**	GET MANUFACTURER DATA
Version du correctif de la plateforme	**0096v004**	**0096v004**	GET CONFIGURATION DATA

Ainsi, pour la variante du produit ML1-80K-63, on a les échanges suivants :

- données de la commande GET CONFIGURATION DATA envoyées à la carte :
  - 80 10 04 00 04
- données reçues de la carte :
  - **00 96** 0**0 04** 90 00
- données de la commande GET MANUFACTURER DATA envoyées à la carte :
  - 80 02 00 00 16
- données reçues de la carte :
  - 05 **63** 84 21 FF FF FF FF FF FF 1A 2B 3C 4D 5E 6F 00 20 00 FF 01 00 90 00

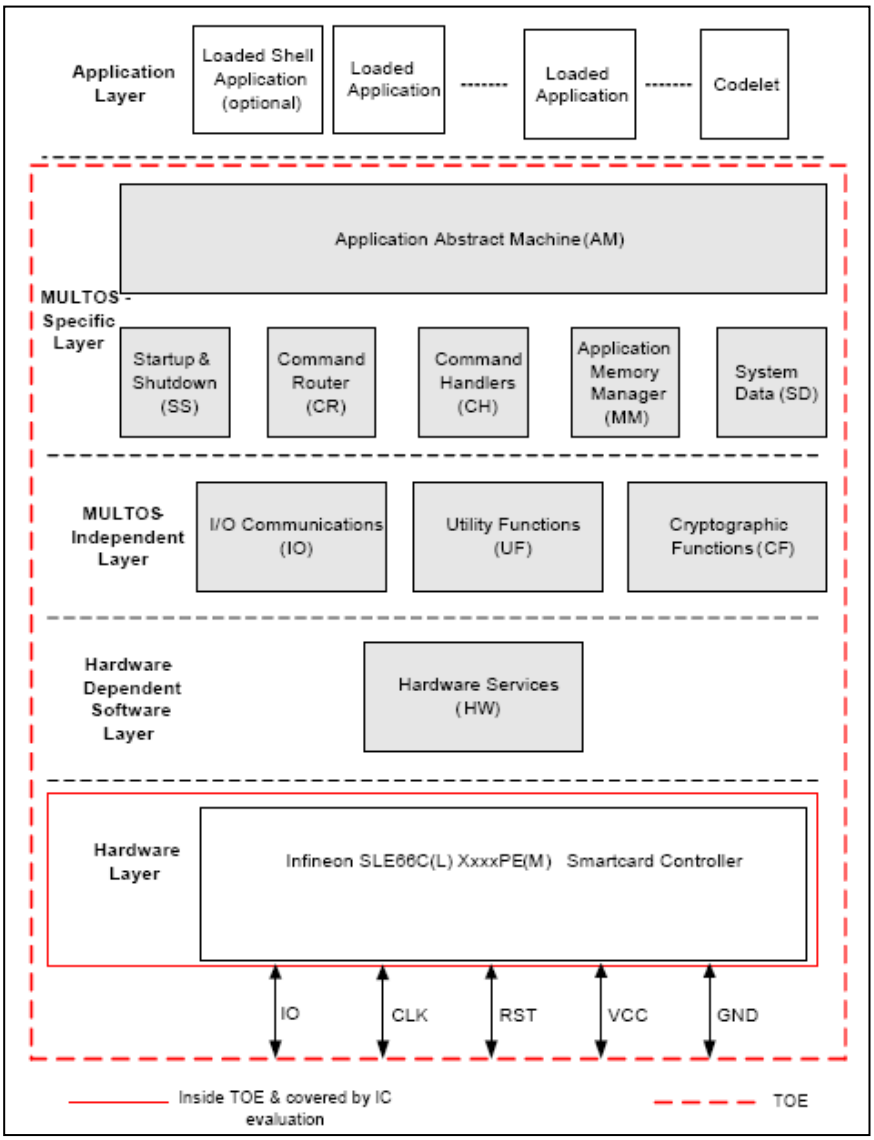
1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont (voir détail dans [ST] au §7.1) :

- chargement d'applications ;
- suppression d'applications ;
- vérification de la signature d'applications ;
- déchiffrement d'applications ;
- chargement des données de contrôle MSM (*Multos Security Manager* – gestionnaire de sécurité Multos) ;
- écrasement des données critiques ;
- protection de réinitialisation ;
- contrôle d'intégrité ;
- contrôle de validité au démarrage et initialisation ;
- décision logicielle face aux tentatives de pénétration ;
- authentification de la carte.

1.2.3. Architecture

La figure suivante donne une synthèse de l'architecture du produit (voir détail dans [ST] au §1.3.1) :



Le sous-système *Hardware Services(HW)* - services matériels – offre le service d'abstraction du matériel pour les échanges bas-niveau d'entrées/sorties et pour, entre autres, l'écriture dans la mémoire EEPROM du composant sous-jacent (couche *Hardware Layer* – couche matérielle).

Le sous-système *I/O Communications (IO)* implémente les protocoles de communication ISO/IEC 7816 et ISO/IEC 14443.

Le sous-système *Utility Functions (UF)* offre différentes fonctions utiles à l'ensemble des autres modules.

Le sous-système *Cryptographic Functions (CF)* offre des services cryptographiques tels que DES, aux modules des couches supérieures.

Le sous-système *Startup and Shutdown (SS)* est en charge du démarrage sécurisé du système d'exploitation Multos lorsque le composant sous-jacent est mis sous tension ; il est également en charge d'arrêter le système d'exploitation Multos lorsque ce dernier détecte un évènement anormal.

Le sous-système *Command Router (CR)* pilote le module IO afin de recevoir les commandes, puis il transmet au module approprié pour leur traitement.

Le sous-système *Command Handlers (CH)* traite les commandes Multos reçues par les modules IO et CR.

Le sous-système *Application Memory Manager (MM)* gère la totalité de la mémoire appartenant aux applications MEL et aux « codelets » (code rassemblant des fonctions appelables par les applications) qui ont été chargés ; il offre également des services aux autres modules afin de permettre à ces applications d'être chargées, accédées et supprimées.

Le sous-système *System Data (SD)* gère les données du système d'exploitation Multos.

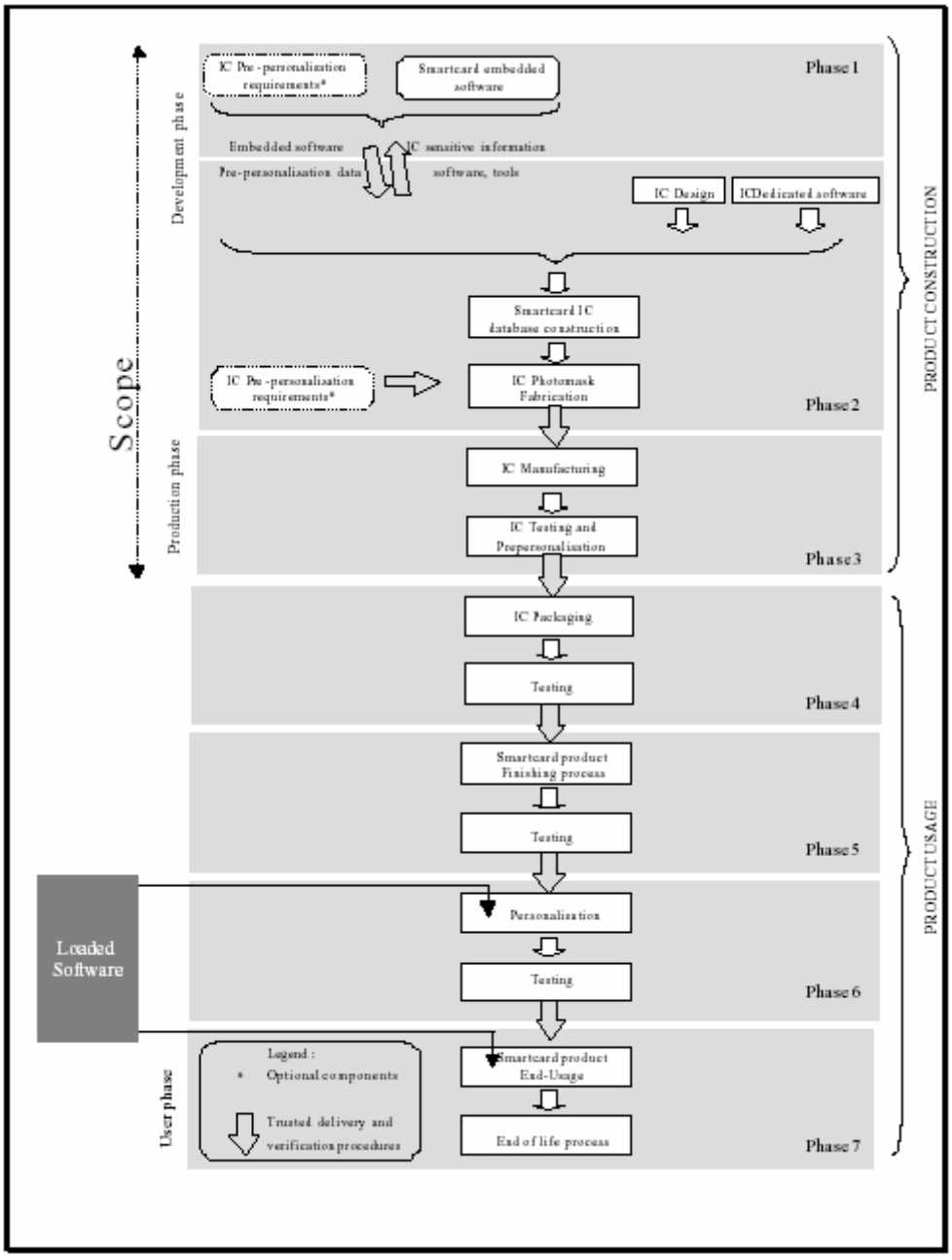
Le sous-système *Application Abstract Machine (AM)* exécute les applications MEL gérées par MM. Il constitue donc la machine virtuelle de Multos.

Les éléments suivants sont hors périmètre de l'évaluation :

- le pare-feu du produit, puisque la [ST], au §3.4.3, prend comme hypothèse que les applications chargées chiffrent leurs données confidentielles (cf. A.USE_DATA) et ne contiennent pas de code sensible (A_USE_ALG) ;
- les primitives cryptographiques de la plateforme (APIs).

1.2.4. Cycle de vie

Le cycle de vie du produit est celui d'une carte à puce et est schématisé dans la figure suivante :



L'évaluation a couvert les phases 1 à 3. Le produit testé est celui livré à l'issue. Les autres phases sont couvertes par des guides qui ont été analysés pendant l'évaluation.

Le produit a été développé sur le site principal suivant :

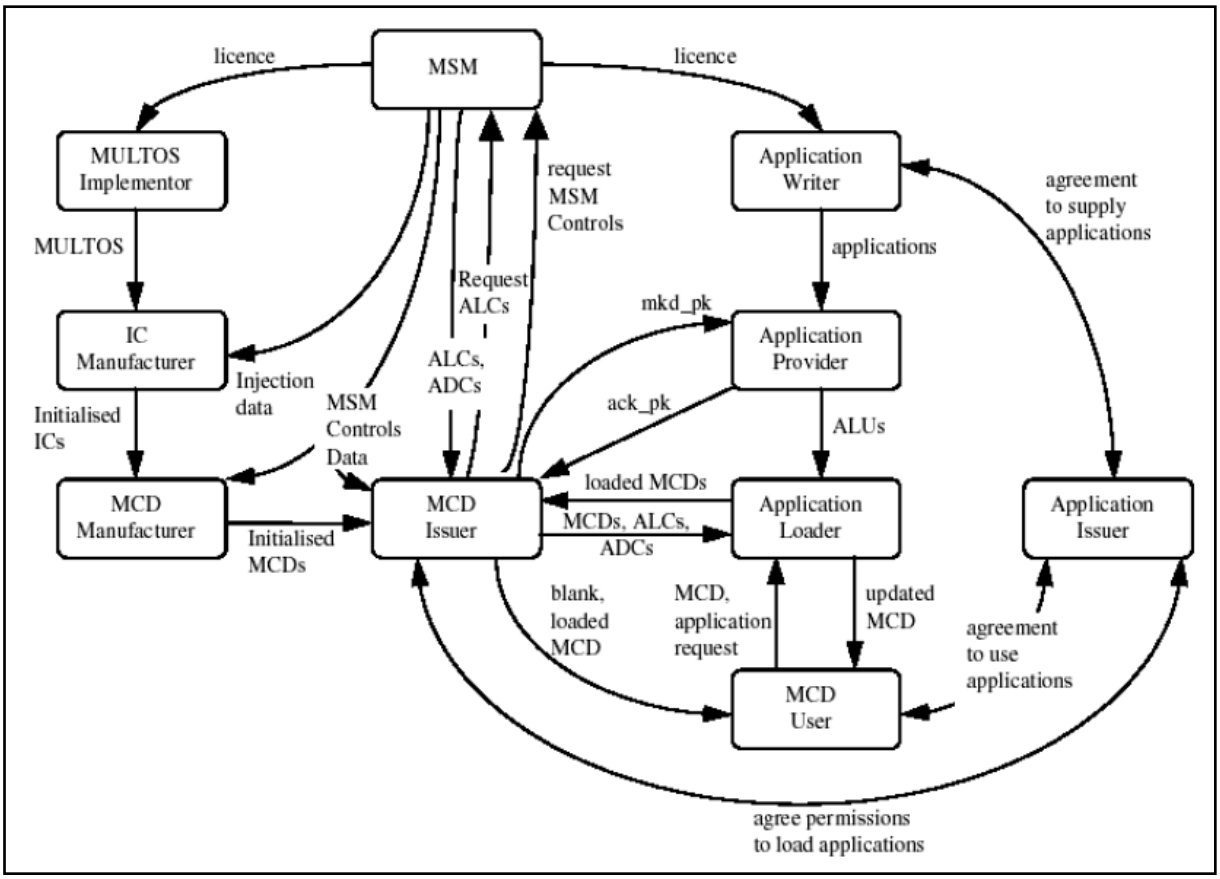
Multos International

Level 14, Zenith Tower B, 821 Pacific Highway
Chatswood NSW 2067, Sydney
Australia

Plus précisément, les sites du développeur du logiciel embarqué dans la carte, impliqués dans les phases 1 à 3, sont :

- le site de Sydney, en Australie (cf. ci-dessus), où l'essentiel des activités du développement de la TOE s'effectue (cf. phase 1 - développement du logiciel embarqué dans la carte) ;
- le reste des activités du développement de la TOE s'effectue à distance (en mode télétravail) depuis :
  - le Royaume-Unie(Royston) ;
  - l'Irlande (Waterford) ;
  - l'Australie (Lismore et Perth) ;
- le site de Warrington, au Royaume-Uni, où siège le KMA (*Key Management Authority* – autorité de gestion des clés) ;
- le site de Singapour, où siègent les responsables des activités des technologies de l'information qui pilotent les développements du produit.

Après la livraison de la TOE en phase 3, plusieurs acteurs sont impliqués (de la phase 4 à 7 du cycle de vie du produit) comme le montre synthétiquement le schéma suivant :



Les activités de ces différents acteurs (*Application Provider* - fournisseur d'applications, *MCD Manufacturer* – fabriquant du MCD (*Multos Carrier Device* – dispositif embarquant le système d'exploitation Multos), *MCD Issuer* – émetteur de MCD, etc.) sont encadrées par des guides fournis conjointement avec le produit.

Pour l'évaluation, l'évaluateur a considéré comme administrateurs du produit les rôles suivants (cf. [ST] au §1.3.6 pour plus de détails) :

- *Multos Security Manager (MSM)* (le gestionnaire de sécurité Multos) ;
- *Multos Implementor* (celui qui implémente une version particulière de Multos) ;
- *Integrated Circuit (IC) Manufacturer* (le fabricant du composant) ;
- *Multos Carrier Device (MCD) Manufacturer* (le fabricant du MCD) ;
- *Multos Carrier Device (MCD) Issuer* (l'émetteur du MCD) ;

et comme utilisateurs du produit les rôles suivants (cf. [ST] au §1.3.6 pour plus de détails) :

- *Application Writer* (le développeur de l'application) ;
- *Application Issuer* (l'émetteur de l'application) ;
- *Application Provider* (le fournisseur de l'application) ;
- *Application Loader* (celui qui charge l'application dans le MCD) ;
- *MCD User* (l'utilisateur final du MCD).

1.2.5. Configuration évaluée

Le certificat porte sur les deux variantes ML1-36K-5F et ML1-80K-63 du produit. Ces variantes sont identifiées au §1.2.1 Identification du produit.

La configuration évaluée pour la ML1-80K-63 était basée sur le KMA « par défaut », c'est-à-dire avec des clés de test ; en effet, au moment de l'évaluation, le KMA de cette variante n'était pas défini.

En revanche, le KMA pour la variante ML1-36K-5F étant défini au moment de l'évaluation, l'évaluateur a pu le prendre en compte.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [CC IC] et [CC AP] ont été appliqués.

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 SLE66CLX360PEM/m1588-a14 et SLE66CLX800PEM/m1580-a14 4, au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, conforme au profil de protection [PP0002] ; ce microcontrôleur a été certifié puis maintenu par le BSI (cf. [BSI-DSZ-CC-0482-2008-MA-05]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 2 avril 2010, 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

L'ANSSI n'a pas réalisé la cotation des mécanismes cryptographiques selon ses référentiels techniques. 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 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 la plateforme MULTOS ML1, avec correctif AMD 0096v004, masquée sur deux variantes de composants Infineon SLE66CLX360PEM (variante produit ML1-36K-5F) et SLE66CLX800PEM (variante produit ML1-80K-63)**,** portant les identifiants composants respectivement 5F et 63, soumise à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté.

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 spécifiés dans la cible de sécurité [ST] et suivre les recommandations se trouvant dans les guides fournis [GUIDES]. En particulier, au cas où une évaluation selon les [CC] d'une application en composition sur cette plateforme serait envisagée, il est recommandé de :

- charger l'application sur cette plateforme de manière signée et chiffrée ;
- s'assurer que l'application chargée ne contient pas de code sensible ;
- s'assurer que l'application chargée encrypte ses données confidentielles ;
- vérifier le périmètre de la future TOE devant être pris en considération, dans la mesure où la TOE actuelle est un sous-ensemble du produit complet puisque, par exemple, les primitives cryptographiques de la plateforme (APIs) ne sont pas dans le périmètre du produit évalué ici.

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 the 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 procedure
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
	ADO_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 Security Target Evaluation	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claim
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended component 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 specifications
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	**2**	**3**	3	**4**	**2**	Testing: security enforcing modules
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independant 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 : - MULTOS M1 - Common Criteria - Security Target, référence MI-SP-0327, version 1.3, Multos International.
[RTE]	Rapport technique d'évaluation : - Evaluation technical report - Project: FORTE, référence : FOR_ETR, version: 3.0, 02/04/2010, Thales-CEACI.
[CONF]	Liste de configuration : - Manufacturing data pack 3 référence : MI-DP-0154, version 7.0 Multos International.
[GUIDES]	Guide d'administration du produit : - Delivery process, référence : MI-IN-0003, version : 2.0 Multos International; - Enablement, référence : MAO-DOC-HOW-002, version: 1.00, Multos International ; - Guide to generating ALU, référence : mao-doc-ref-009, version: 2.51, Multos International ; - Guide to loading and deleting applications, référence : MAO-DOC-REF-008, version: 2.20, Multos International ; - Mask Verification Procedure, référence : SIM-PR-0012, version : 1-2, Multos International ; - Mask Verification Procedure MI-PR-0012 v.1.0, référence : MI-PR-0012, version : 1.0 Multos International ; - MISA Handling Guidelines référence : maos-gkc-dev-032, version : 3-0 Multos International ; - MULTOS KMA File Interface Formats, référence : maos-gkc-spc-002/1, version : 6-0, Multos International ; - Security guidance for multos application developpers 5, référence : MI-MA-0031, version : 1.4, Multos International ; Guide d'utilisation du produit : - StepServer & StepXpress Manual, référence : StepServer & StepXpress Manual, Multos International ;

[PP0002]	*Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001*. Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0002-2001.
[PP/0010]	Certificat ANSSI délivré en janvier 2001 pour le profil de protection *Smart Card IC with Multi-Application Secure Platform Version 2.0*
[BSI-DSZ-CC-0482-2008-MA-05]	Rapport de maintenance BSI délivré le 15 avril 2009 pour *Infineon Smart Card IC (Security Controller)SLE66CLX800PE / m1581-e13/a14, **SLE66CLX800PEM / m1580-e13/a14**, SLE66CLX800PES / m1582-e13/a14, SLE66CX800PE / m1599-e13/a14, SLE66CLX360PE / m1587-e13/a14, **SLE66CLX360PEM / m1588-e13/a14**, SLE66CLX360PES / m1589-e13/a14, SLE66CLX180PE /m2080-a14, SLE66CLX180PEM / m2081-a14, SLE66CLX120PE / m2082-a14, SLE66CLX120PEM / m2083-a14 all with optional libraries RSA V1.5 and ECC V1.1 and all with specific IC dedicated software*.

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 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, September 2006, version 3.1, revision 1, ref CCMB-2006-09-001; Part 2: Security functional components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-002; Part 3: Security assurance components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2007, version 3.1, révision 2, ref CCMB-2007-09-004.
[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.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2009-03-001 version 2.7 revision 1, March 2009.
[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.