PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2003/14

Plate-forme MULTOS I4C (1-1-1) incluant le patch AMD 0029v002 masquée sur SLE66CX322P/m1484 a24

Paris, le 4 décembre 2003

Le Directeur central de la sécurité des systèmes d'information

Henri Serres

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 terme d'objectifs de sécurité.
Toutefois, la certification ne constitue pas en soi une recommandation du produit par l'organisme de certification, et ne garantit pas que le produit certifié est totalement exempt de vulnérabilités exploitables.

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 :

- La direction centrale 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 selon les ITSEC et les Critères Communs sont publiques et disponibles en français sur le site Internet :

www.ssi.gouv.fr

Le site international concernant la certification selon les Critères Communs est accessible à l'adresse Internet :

www.commoncriteria.org

Accords de reconnaissance des certificats

L'**accord de reconnaissance** européen du SOG-IS de 1999 permet la reconnaissance entre les Etats signataires de l'accord[1], des certificats délivrés par leur autorité de certification. La reconnaissance mutuelle européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque :

La direction centrale de la sécurité des systèmes d'information passe aussi des **accords de reconnaissance** avec des organismes étrangers homologues ayant leur siège en dehors des Etats membres de la Communauté européenne. Ces accords peuvent prévoir que les certificats

[1] En avril 1999, les pays signataires de l'accord SOG-IS sont : le Royaume-Uni, l'Allemagne, la France, l'Espagne, l'Italie, le Suisse, les Pays-Bas, la Finlande, la Norvège, la Suède et le Portugal.

délivrés par la France sont reconnus par les Etats signataires. Ils peuvent prévoir aussi que les certificats délivrés par chaque partie sont reconnus par toutes les parties.

L'accord du Common Criteria Recognition Arrangement, permet la reconnaissance, par les pays signataires de l'accord[1], des certificats délivrés dans le cadre du schéma Critères Communs. La reconnaissance mutuelle s'applique au niveau EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque :

Les sites des organismes nationaux de certification des pays signataires de l'accord Common Criteria Recognition Arrangement sont :

Pays	Organisme certificateur	Site web
France	DCSSI	www.ssi.gouv.fr
Royaume-Uni	CESG	www.cesg.gov.uk
Allemagne	BSI	www.bsi.bund.de
Canada	CSE	www.cse-cst.gc.ca
Australie-Nouvelle Zélande	AISEP	www.dsd.gov.au/infosec
Etats-Unis	NIAP	www.niap.nist.gov

[1] En janvier 2003, les pays émetteurs de certificats signataires de l'accord sont : la France, l'Allemagne, le Royaume-Uni, les Etats-Unis, le Canada et l'Australie-Nouvelle Zélande ; les pays signataires de l'accord qui n'émettent pas de certificats sont : l'Espagne, la Finlande, la Grèce, Israël, l'Italie, la Norvège, les Pays-Bas, la Suède, l'Autriche et le Japon.

Table des matières

1. Le produit évalué

1.1. Identification du produit

Le produit évalué est la **plate-forme MULTOS I4C version 1-1-1 incluant le patch AMD 0029v002** développée par **Keycorp Limited** et **Infineon Technologies AG**, composée des éléments suivants :

Element	Version	Développeur
Keycorp MULTOS	I4C 1-1-1 (SIM-MM-0170 rev 1.0)	Keycorp Limited
Additional MULTOS Data	0029v002 (SIM-MM-0180 rev 2.0)	Keycorp Limited
Librairie RMS	0.6	Infineon Technologies AG
Micro-circuit SLE66CX322P	m1484 / a24	Infineon Technologies AG

La signification de l'identifiant (1-x-y) de la plate-forme est la suivante :

' I ' est pour le composant Infineon.
' 4 ' est pour la version des spécifications MULTOS.
' C ' est pour la version du système d'exploitation.
' 1 ' est pour la version de la ROM.
' x ' est pour le jeu de clé en ROM; 0 est pour le jeu de clés de la plate-forme de test et 1 est pour le jeu de clés de la plate-forme mise sur le terrain.
' x ' identifie les codelets en ROM. Un 0 signifie qu'il n'y a pas de codelet.

1.2. Le développeur

Keycorp Limited

67 Albert Avenue
Level 8
Chatswood
NSW2067
Australie

Infineon Technologies AG

Postfach 80 17 60
81617 München
Allemagne

1.3. Description du produit évalué

Le produit évalué est la plate-forme MULTOS I4C de Keycorp Limited. Elle permet le chargement sécurisé d'applications (chiffrées ou non), assurant ainsi l'authenticité et l'intégrité de celles-ci, et s'assure que les demandes d'effacement d'applet sont autorisées. De plus, elle s'assure qu'une application ne puisse pas perturber une autre application chargée sur la carte, et que le code et les données d'une application effacée ne soient plus accessibles.

1.3.1. Architecture

Le produit est constitué du système d'exploitation MULTOS développé par Keycorp Limited et du micro-circuit développé par Infineon Technologies AG. Le schéma suivant montre le périmètre du produit évalué.

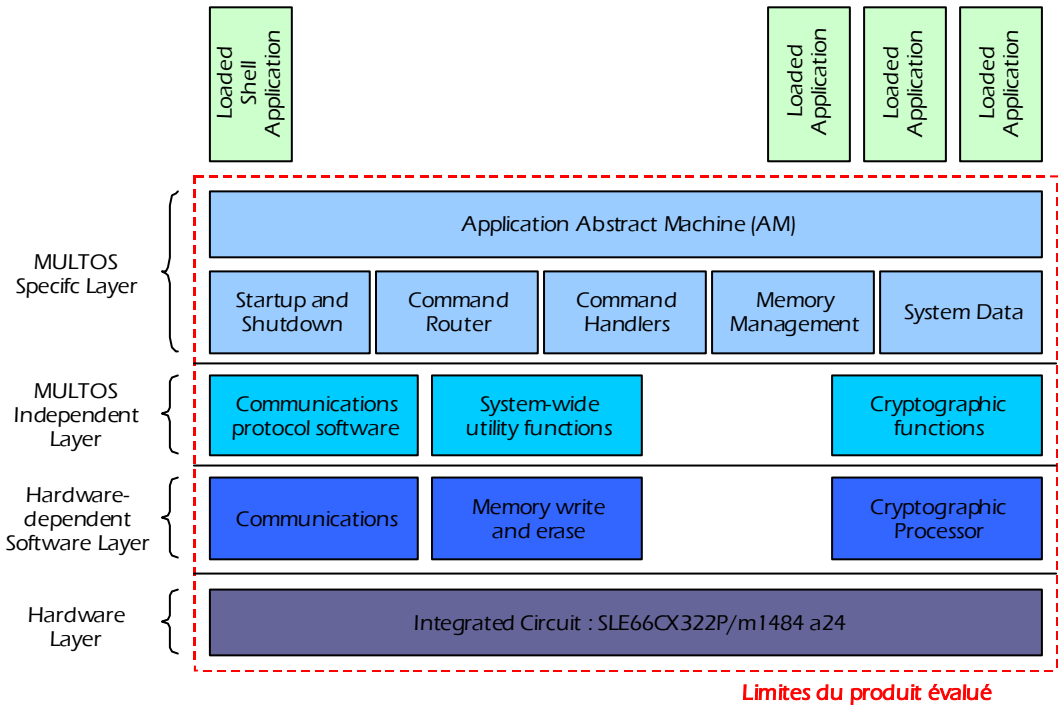

Figure 1 - Limites du produit évalué

Une description détaillée de l'architecture de l'application se trouve dans le document [HLD].

1.3.2. Cycle de vie

Le schéma Figure 2 représente toute l'infrastructure développée autour de MULTOS. Il met en avant tous les acteurs participant au développement d'une plate-forme MULTOS contenant des applications chargées ainsi que les transactions effectuées entre ces acteurs.
Les rôles dans l'infrastructure MULTOS sont les suivants :

- **MSM – MULTOS Security Manager :**
  Responsable sécurité MULTOS
  Il définit et supervise l'infrastructure de sécurité MULTOS, il fournit aussi les critères et services nécessaires aux autres acteurs présents dans l'infrastructure. Il représente par ailleurs l'Autorité de Certification pour cette infrastructure. Le *MSM* est unique dans toute l'infrastructure MULTOS et tous les autres acteurs doivent lui faire confiance.
- **MULTOS Implementor** (pour cette évaluation : **Keycorp**) **:**
  Développeur d'un système d'exploitation MULTOS
  Il représente une société développant un système d'exploitation MULTOS. Le MSM transmet une licence au *MULTOS Implementor*.
  Le *MULTOS Implementor* demande au *MSM* de transmettre les données de contrôle MSM (*MSM Control Data*) au *MCD manufacturer* ou bien au *MCD Issuer*.

- **IC (Integrated Circuit) Manufacturer** (pour cette évaluation : **Infineon**) **:**
  Fondeur
  Il fabrique le micro-circuit masqué par le système d'exploitation MULTOS. Il intègre aussi les clés dans la ROM du composant. Les clés et les données de sécurité sont fournies par le *MSM*. Le composant est ensuite transmis au *MCD Manufacturer*.
- **MCD (MULTOS Carrier Device) Manufacturer :**
  Encarteur et personnalisateur
  Il est chargé d'intégrer le composant masqué sur une carte plastique ainsi que d'inscrire sur la carte les informations nécessaires. En sortie de cette phase, la carte est initialisée. Cette phase n'est pas sécuritaire. Le *MCD Manufacturer* peut recevoir (comme l'*IC Manufacturer*) des données de contrôle MSM (*MSM control data*) de la part du *MSM* afin d'initialiser les MCD. C'est dans cette phase qu'est chargé le patch **AMD 0029v002**.

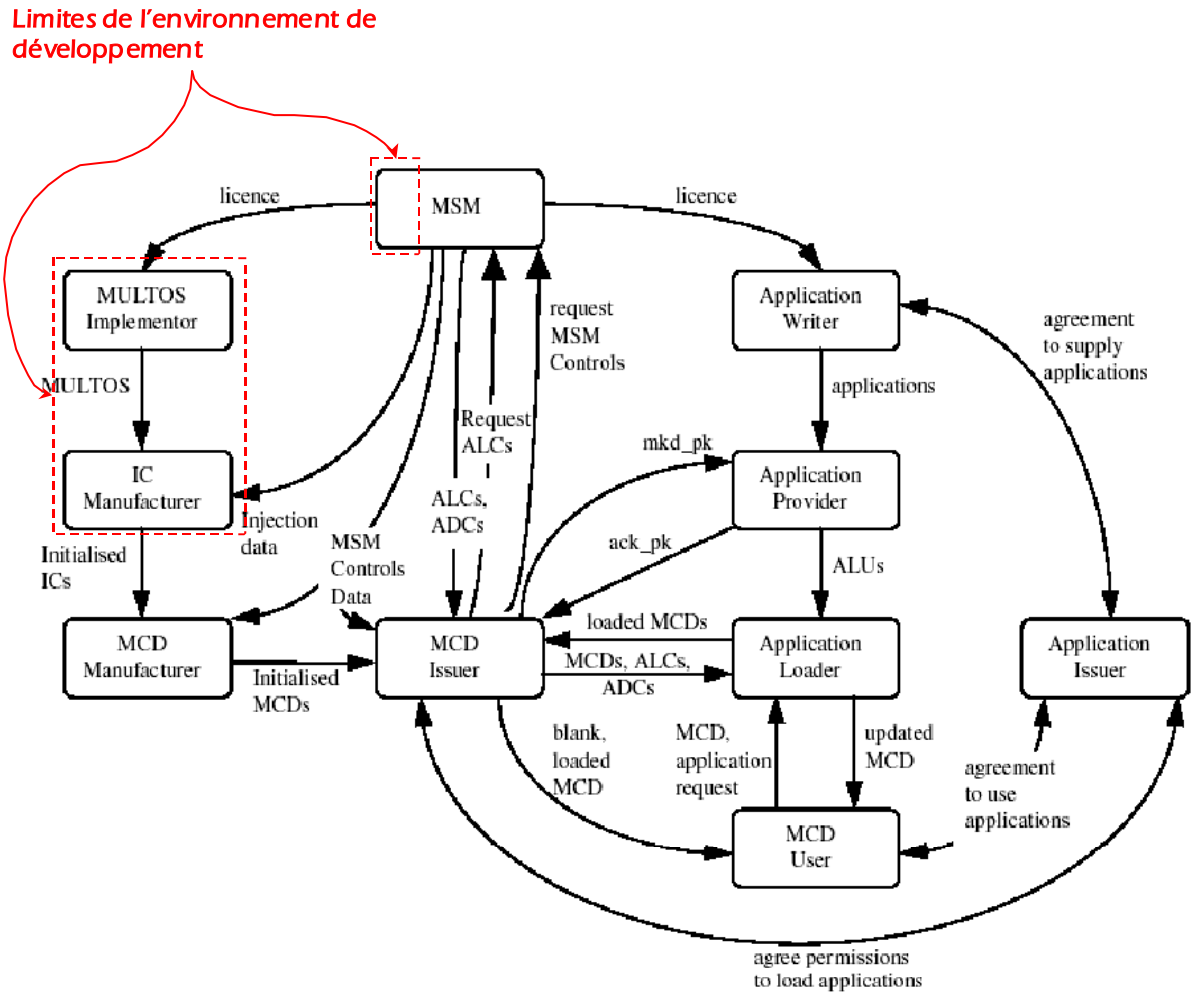

Figure 2 - Infrastructure MULTOS et limites de l'environnement de développement du produit

- **MCD Issuer :**
  Emetteur de cartes
  Il est chargé d'émettre les cartes (*MCD*). Il peut, comme le *MCD Manufacturer*, initialiser la carte avec les données de contrôle MSM transmises par le *MSM*.
- **Application writer :**
  Développeur d'applications fonctionnant sous environnement MULTOS
  Il développe des applications demandées par l'*Application Issuer*.
- **Application Issuer :**
  Commanditaire d'applications
  Il s'agit d'une société qui désire fournir une application à ses utilisateurs. L'*Application Issuer* convient avec un *MCD Issuer* que l'application peut être chargée sur les cartes de cet *MCD Issuer*.
- **Application Provider :**
  Fournisseur d'applications
  Il s'agit de l'organisme certifiant l'application à l'aide de sa clé publique et la chiffrant. Ce rôle peut être tenu par l'*Application writer*, l'*Application Issuer*, le *MCD Issuer* ou par tout autre organisme.
- **Application Loader :**
  Responsable du chargement d'applications
  Il réalise le chargement de l'application sur la carte.
- **MCD users :**
  Utilisateurs
  Ce sont les utilisateurs finaux des cartes émises.

1.3.3. Périmètre et limites du produit évalué

Le produit évalué est composé du système d'exploitation MULTOS version 1-1-1 incluant le patch AMD 0029v002, développé par Keycorp Limited, et du micro-circuit SLE66CX322P/m1484 a24 développé par Infineon Technologies AG.

1.4. Utilisation et administration

1.4.1. Utilisation

Les administrateurs sont (cf Figure 2) le *MULTOS Implementor*, l'*IC manufacturer*, le *MULTOS KMA*, le *MCD Manufacturer* et le *MCD Issuer*.

De manière générale, dans le cas d'une plate-forme, les utilisateurs de la plate-forme ne correspondent pas aux utilisateurs finaux, mais correspondent aux futurs développeurs d'applications pour cette plate-forme. Par conséquent, les utilisateurs dans le cas de ce produit sont (cf. Figure 2) l'*Application writer* (développeur d'une application), l'*Application Issuer* (commanditaire de l'application), l'*Application Provider* (le fournisseur de l'application), l'*Application Loader* (le responsable du chargement de l'application sur la plate-forme).

Dans le cas de l'utilisateur final (porteur de la carte à puce), la plate-forme MULTOS I4C n'offre pas réellement de fonctions de sécurité telles que définies par les Critères Communs. Toutefois, il est important de le rajouter dans ce paragraphe afin de montrer qu'il joue un rôle, pas nécessairement au niveau de la plate-forme MULTOS, mais plutôt au niveau des applications se trouvant chargées sur la plate-forme. Cet utilisateur aura en effet accès aux

fonctions de sécurité offertes par ces applications. Le *MCD user* (l'utilisateur final) est donc ajouté en dernier point.

Les fonctions et guides suivants sont accessibles pour ces différents utilisateurs :

- Application writer :
  Il développe des applications en respectant les recommandations se trouvant dans les guides [MDRM], [MIR] et [SGAD].
- Application Issuer :
  Il détermine les autorisations de chargement de l'application en s'aidant du guide [GMS].
- Application Provider :
  En respectant les recommandations du guide [GALU], il signe (électroniquement) l'application en vue du chargement, il génère les clés KTU (*Key Transformation Unit*) s'il souhaite que le code de l'application reste confidentiel et il chiffre les applications en utilisant ces clés.
- Application Loader :
  Le guide pour le responsable du chargement d'application est [GLDA]. Les fonctions qui lui sont offertes sont le chargement et l'effacement d'applications.
- MCD user :
  Les seules fonctionnalités accessibles à l'utilisateur final d'une carte à puce contenant la plate-forme MULTOS I4C, sont la demande du chargement d'une application et la demande de l'effacement d'une application [GMS].

1.4.2. Administration

Les administrateurs sont (cf Figure 2) le *MULTOS Implementor* (développeur d'un système d'exploitation MULTOS), l'*IC manufacturer* (le fondeur), le *MULTOS KMA* (, le *MCD Manufacturer* et le *MCD Issuer*.

Ces administrateurs ont pour fonctions :

- Implementor :
  Il vérifie que les *MCD* (MULTOS carrier device – plate-forme MULTOS) sont authentiques [MVP].
- IC manufacturer :
  Pour la génération du masque ROM complet, il injecte la clé *kck_pk* reçue du MSM [PGRI] et écrit en EEPROM les données de sécurité d'initialisation (MISA – MULTOS Intialisation Security Data) [IFD-MISA] et [MISA-HG].
- MULTOS KMA (Key Management Authority) :
  - Il génère les données de sécurité d'initialisation pour chaque plate-forme (MISA – MULTOS Intialisation Security Data) [MGKC] ;
  - Il gère les demandes de chargement de *MSM Control Data* [CA-PM], [MGKC] et [MSM-CDC] ;
  - Il gère les demandes de certificats, y compris les demandes d'utilisation de mécanismes cryptographiques robustes (cf § 3.10.5) [SSM] ;
  - Il gère les demandes et la livraison de clés *tkck* et *hm* [MKHD]. Ces clés sont décrites dans la cible de sécurité [ST] ;
  - Il vérifie que les *MCD* (MULTOS carrier device – plate-forme MULTOS) sont authentiques [MVP].

- MCD Manufacturer :
  Il vérifie que les *MCD* (MULTOS carrier device – plate-forme MULTOS) sont authentiques [MVP].
- MCD Issuer :
  - Il demande les certificats ALC/ADC [GMS] et [M-SPI] ;
  - Il demande l'enregistrement d'une application et son statut quant à l'utilisation ou non de mécanismes cryptographiques robustes (cf § 3.10.5) [GMS] et [M-SPI] ;
  - Il demande ([GMS] et [M-SPI]) et charge ([MCDL]) les données de contrôles MSM (*MSM control data*).

2. L'évaluation

2.1. Centre d'évaluation

CEACI (Thalès Microelectronics – CNES)

18 avenue Edouard Belin
31401 Toulouse Cedex 4

Téléphone : +33 (0)5 61 27 40 29

Adresse électronique : ceaci@cnes.fr

L'évaluation s'est déroulée de **décembre 2002** à **avril 2003**.

2.2. Commanditaire

Crédit Mutuel

6 rue Ventadour
75001 Paris
France

2.3. Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM], et à l'ensemble des interprétations finales listées dans les rapports d'évaluation.

2.4. Evaluation de la cible de sécurité

La cible de sécurité [ST] définit le produit évalué et son environnement d'exploitation.
Toutes les exigences fonctionnelles et d'assurance de la cible de sécurité sont extraites respectivement de la partie 2 et de la partie 3 des Critères Communs [CC].
La cible de sécurité répond aux exigences de la classe ASE.

2.5. Evaluation du produit

L'évaluation consiste à vérifier que le produit et sa documentation respectent les exigences fonctionnelles et d'assurance définies dans la cible de sécurité [ST].
L'évaluation de ce produit s'est appuyée sur le certificat du micro-circuit «Smart Card IC (Security Controller) SLE66CX322P with RSA 2048 / m1484a24, a27 and b14» émis par le BSI sous la référence BSI-DSZ-CC-0223-2003 [322P-A24]. Ce certificat atteste que le micro-circuit SLE66CX322P/m1484a24 atteint le niveau EAL 5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4 et qu'il est conforme au profil de protection référencé PP/BSI-0002 «Smartcard Integrated Circuit Protection Profile v2.0» [SSVG]. La validité de ce certificat est reconnue par le schéma français en vertu de l'accord de reconnaissance du SOG-IS [SOG-IS]. Le micro-circuit étant certifié par le schéma allemand, les travaux effectués dans le cadre de cette évaluation ont porté sur l'évaluation du masque et

sur son intégration sûre dans le micro-circuit conformément aux interprétations sur la composition d'un circuit intégré et d'un logiciel embarqué [JIL-Comp].
L'évaluation du produit s'est aussi appuyée sur l'évaluation selon les critères d'évaluation ITSEC du même système d'exploitation, masqué sur le composant SLE66CX320P. Cette précédente évaluation a donné lieu au certificat 2003/01 [2003/01].

2.5.1. Développement du produit

La classe d'assurance ADV – développement – définit les exigences de raffinement pas à pas des fonctions de sécurité du produit depuis ses spécifications globales dans la cible de sécurité [ST] jusqu'à l'implémentation. Chacune des représentations des fonctions de sécurité du produit qui résultent de ce processus fournit des informations qui aident l'évaluateur à déterminer si les exigences fonctionnelles du produit ont été satisfaites.
L'analyse des documents associés à la classe ADV montre que les exigences fonctionnelles sont correctement et complètement raffinées dans les différents niveaux de représentation du produit (spécifications fonctionnelles (FSP), sous-systèmes (HLD), modules (LLD) et implémentation (IMP)), jusqu'à l'implémentation de ses fonctions de sécurité.
Les documents fournis pour la classe ADV – développement – répondent aux exigences de la partie 3 des critères communs [CC] en terme de contenu et de présentation des éléments de preuve.

2.5.2. Documentation

Du point de vue de l'évaluation, les administrateurs sont le *MULTOS Implementor*, l'*IC manufacturer*, le *MULTOS KMA*, le *MCD Manufacturer* et le *MCD Issuer* (cf Figure 2). Les guides associés sont : [MVP], [PGRI], [IFD-MISA], [MISA-HG], [MGKC], [CA-PM], [MGKC], [MSM-CDC], [SSM], [MKHD], [MVP], [GMS] et [M-SPI].
Du point de vue de l'évaluation, les utilisateurs de la plate-forme ne correspondent pas aux utilisateurs finaux, mais correspondent aussi aux futurs développeurs d'applications pour cette plate-forme. Par conséquent, les utilisateurs dans le cas de ce produit sont (cf Figure 2) l'*Application writer* (développeur d'une application), l'*Application Issuer* (commanditaire de l'application), l'*Application Provider* (le fournisseur de l'application), l'*Application Loader* (le responsable du chargement de l'application sur la plate-forme). Les guides associés sont : [MDRM], [MIR], [SGAD], [GMS], [GALU], [GLDA].
Les guides utilisateur et administrateur répondent aux exigences de la partie 3 des critères communs [CC] en terme de contenu et de présentation des éléments de preuve.

2.5.3. Livraison et installation

La livraison est considérée après la fabrication par Infineon du composant masqué par le système d'exploitation. La livraison du composant [INFCD] a été vérifiée lors de son évaluation dont les résultats sont résumés dans le certificat émis par le BSI sous la référence BSI-DSZ-CC-0223-2003 [322P-A24].
La livraison du système d'exploitation vers Infineon est explicitée dans le document [OSDEL]. La livraison du patch (explicitée dans le document [OSDEL]) a fait l'objet d'une vérification lors de l'évaluation de la version précédente de la plate-forme [2003/01].
La procédure [OSDEL] de livraison est suffisante pour répondre aux exigences demandées : elle permet de connaître l'origine de la livraison et de détecter une modification du produit pendant la livraison.

L'installation du produit correspond d'une part à la phase de création du masque [PGRI] par le fondeur (Infineon) et la pré-personnalisation ([IFD-MISA] et [MISA-HG]). Le fondeur (*IC manufacturer*) doit en effet lors de la phase de création du masque ROM injecter les clés *kck_pk* et *hm* (fournis par le *MSM*). Une fois le composant masqué fabriqué, il écrit en EEPROM les données de sécurité (MISA).
La génération du produit consiste en la personnalisation [MCDL]. Le personnalisateur (*MCD manufacturer* ou MCD *Issuer*) doit charger les données de contrôle du MSM (*MSM control data*). Cette phase est essentielle pour rendre la plate-forme opérationnelle.
La phase de démarrage du produit consiste en l'alimentation de la carte, conformément à la norme ISO 7816-3.
Les procédures d'installation, de génération et de démarrage permettent d'obtenir une configuration sûre de l'application.
Les documents fournis pour la classe ADO – livraison et opération – répondent aux exigences de la partie 3 des critères communs 34 en terme de contenu et de présentation des éléments de preuve.

2.5.4. L'environnement de développement

Le développement du système d'exploitation se fait chez Keycorp Limited à Sidney (Australie). Sont développés le code source du système d'exploitation MULTOS et le code source du patch AMD 0029v002 (AMD – Additional MULTOS Data).
Le site de développement de Keycorp est situé :

Level 9, 67 Albert Avenue
Chatswood, N.S.W. 2067
Australie.

Les guides sont gérés par MAOSCO représenté par la société Mondex International Limited, à Londres (Royaume-Uni).
Le site de gestion des documents de Mondex International est situé :

47-53 Canon Street
London EC4M 55Q
Royaume-Uni

Les mesures de sécurité décrites dans les procédures fournissent le niveau nécessaire de protection pour maintenir la confidentialité et l'intégrité du produit évalué et de sa documentation.
La vérification de la mise en œuvre des procédures de développement et de gestion de configuration a été effectuée par un audit du site de Keycorp ci-dessus, lors de l'évaluation de la version précédente du système d'exploitation (plate-forme MULTOS version 1Q). Cette évaluation a donné lieu au certificat [2003/01].
Comme les guides sont gérés par Mondex International pour le compte de MAOSCO, le site de Mondex International a également été audité lors de la précédente évaluation.
La fabrication du composant est effectuée par Infineon Technologies AG en Allemagne.
Le système de gestion de configuration est utilisé conformément au plan de gestion de configuration.
La liste de configuration [LGC] identifie les éléments tracés par le système de gestion de configuration. Les éléments de configuration identifiés dans la liste de configuration sont maintenus par le système de gestion de configuration. Les procédures de génération de

l'application sont efficaces pour s'assurer que les bons éléments de configuration sont utilisés pour générer l'application.
Les documents fournis pour la classe ACM – gestion de la configuration – et ALC – support au cycle de vie – répondent aux exigences de la partie 3 des critères communs [CC] en terme de contenu et de présentation des éléments de preuve.

2.5.5. Tests fonctionnels

L'évaluateur a vérifié que toutes les fonctions de sécurité et les interfaces de la spécification fonctionnelle du produit sont reliées à au moins un test fonctionnel dans la documentation de test. Il a vérifié aussi que toutes les caractéristiques fonctionnelles de chaque fonction de sécurité, telles qu'elles sont décrites dans la conception de haut niveau [HLD], sont couvertes par les tests du développeur.
La version de la plate-forme utilisée pour les tests est MULTOS I4C 1-0-2, en effet ce sont les clés tests qui étaient chargées sur la plate-forme et le codelet chargé en ROM est celui utilisé pour les tests (codelet 2).

2.5.6. Estimation des vulnérabilités

Toutes les vulnérabilités identifiées par le développeur ont été vérifiées par une analyse complétée de tests. L'évaluateur conclut que les vulnérabilités identifiées par le développeur ont été correctement couvertes.
L'évaluateur a réalisé une analyse de vulnérabilité indépendante, dont les résultats ne montrent pas de vulnérabilités supplémentaires.
Comme pour les tests fonctionnels, la plate-forme utilisée pour l'estimation des vulnérabilité était MULTOS I4C 1-0-2.
Le produit dans son environnement d'exploitation est résistant à des attaquants disposant d'un potentiel d'attaque **élevé**.

3. Conclusions de l'évaluation

3.1. Rapport technique d'évaluation

Le rapport technique d'évaluation [RTE] décrit les résultats de l'évaluation du produit **plate-forme MULTOS I4C version 1-1-1 incluant le patch AMD 0029v002**.

3.2. Niveau d'évaluation

La plate-forme MULTOS I4C version 1-1-1 incluant le patch AMD 0029v002 a été évaluée selon les Critères Communs [CC] et sa méthodologie [CEM] au niveau **EAL4**[1] **augmenté des composants d'assurance suivants**, conformes à la partie 3 des Critères Communs :

Composants	Descriptions
ADV_IMP.2	Implementation of the TSF
ALC_DVS.2	Sufficiency of security measures
AVA_VLA.4	Highly resistant

Tableau 1 - Augmentations

Pour tous les composants, les verdicts suivants ont été émis :

Class ASE	Security Target evaluation	
ASE_DES.1	TOE description	Réussite
ASE_ENV.1	Security environment	Réussite
ASE_INT.1	ST introduction	Réussite
ASE_OBJ.1	Security objectives	Réussite
ASE_PPC.1	PP claims	Réussite
ASE_REQ.1	IT security requirements	Réussite
ASE_SRE.1	Explicitly stated IT security requirements	Réussite
ASE_TSS.1	Security Target, TOE summary specification	Réussite
Class ACM	**Configuration management**	
ACM_AUT.1	Partial CM automation	Réussite
ACM_CAP.4	Generation support and acceptance procedures	Réussite
ACM_SCP.2	Problem tracking CM coverage	Réussite
Class ADO	**Delivery and operation**	
ADO_DEL.2	Detection of modification	Réussite
ADO_IGS.1	Installation, generation, and start-up	Réussite

[1] Annexe 4 : tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans les Critères Communs [CC].

	procedures	
Class ADV	**Development**	
ADV_FSP.2	Fully defined external interfaces	Réussite
ADV_HLD.2	Security enforcing high-level design	Réussite
ADV_IMP.2	Implementation of the TSF	Réussite
ADV_LLD.1	Descriptive low-level design	Réussite
ADV_RCR.1	Informal correspondence demonstration	Réussite
ADV_SPM.1	Informal TOE security policy model	Réussite
Class AGD	**Guidance**	
AGD_ADM.1	Administrator guidance	Réussite
AGD_USR.1	User guidance	Réussite
Class ALC	**Life cycle support**	
ALC_DVS.2	Sufficiency of security measures	Réussite
ALC_LCD.1	Developer defined life-cycle model	Réussite
ALC_TAT.1	Well-defined development tools	Réussite
Class ATE	**Tests**	
ATE_COV.2	Analysis of coverage	Réussite
ATE_DPT.1	Testing: high-level design	Réussite
ATE_FUN.1	Functional testing	Réussite
ATE_IND.2	Independent testing - sample	Réussite
Class AVA	**Vulnerability assessment**	
AVA_MSU.2	Validation of analysis	Réussite
AVA_SOF.1	Strength of TOE security function evaluation	Réussite
AVA_VLA.4	Highly resistant	Réussite

Tableau 2 - Composants et verdicts associés

3.3. Exigences fonctionnelles

Le produit répond aux **exigences fonctionnelles de sécurité** [ST] suivantes[1] :

- Security Alarms (FAU_ARP.1)
- Potential violation analysis (FAU_SAA.1)
- Cryptographic key access (FCS_CKM.3)
- Cryptographic key destruction (FCS_CKM.4)
- Cryptographic operation (FCS_COP.1)
- Complete access control (FDP_ACC.2)
- Security attributes based access control (FDP_ACF.1)
- Basic data authentication (FDP_DAU.1)
- Export of user data without security attributes (FDP_ETC.1)

[1] Annexe 3 : tableau des exigences fonctionnelles de sécurité du produit évalué.

- Import of user data without security attributes (FDP_ITC.1)
- Subset residual information protection (FDP_RIP.1)
- Basic Rollback (FDP_ROL.1)
- Stored data integrity monitoring and action (FDP_SDI.2)
- Authentication failure handling (FIA_AFL.1)
- User attribute definition (FIA_ATD.1)
- Timing of authentication (FIA_UAU.1)
- Single-use authentication mechanisms (FIA_UAU.4)
- Timing of identification (FIA_UID.1)
- User-subject binding (FIA_USB.1)
- Management of security functions behaviour (FMT_MOF.1)
- Management of security attributes (FMT_MSA.1)
- Secure security attributes (FMT_MSA.2)
- Static attribute initialisation (FMT_MSA.3)
- Management of TOE security functions data (FMT_MTD.1)
- Management of limits on TSF data (FMT_MTD.2)
- Security roles (FMT_SMR.1)
- Unobservability (FPR_UNO.1)
- Failure with preservation of secure state (FPT_FLS.1)
- Resistance to physical attack (FPT_PHP.3)
- Function recovery (FPT_RCV.4)
- Non-bypassability of the TSP (FPT_RVM.1)
- TOE security functions domain separation (FPT_SEP.1)
- Inter-TSF basic TSF data consistency (FPT_TDC.1)
- TOE security functions testing (FPT_TST.1)
- Maximum quotas (FRU_RSA.1)

3.4. Résistance des fonctions

Seules les fonctions d'authentification ont fait l'objet d'une estimation du niveau de résistance.
Le niveau de résistance des fonctions de sécurité est jugé **élevé** (**SOF-High**).

3.5. Analyse des mécanismes cryptographiques

Les mécanismes cryptographiques de la plate-forme MULTOS I4C 1-1-1 sont identiques à ceux de la version précédente, la plate-forme MULTOS 1Q. Par conséquent les mécanismes n'ont pas de nouveau été analysés dans le cadre de l'évaluation de la plate-forme, les résultats de la plate-forme MULTOS 1Q pouvant s'appliquer à la plate-forme I4C 1-1-1.

3.6. Conformité à un profil de protection

(Sans objet)[1]

3.7. Reconnaissance européenne (SOG-IS)

Ce certificat a été émis dans les conditions de l'accord du SOG-IS. Les dispositions de cet accord nécessitent la fourniture de la cible de sécurité [ST].

3.8. Reconnaissance internationale (CC RA)

Ce certificat a été émis dans les conditions de l'accord du CC RA. Les dispositions de cet accord nécessitent la fourniture de la cible de sécurité [ST].
Les augmentations suivantes ne sont par reconnues dans le cadre du CC RA [CC RA] : ADV_IMP.2, ALC_DVS.2 et AVA_VLA.4 (Tableau 1).

3.9. Restrictions d'usage

La plate-forme MULTOS I4C 1-1-1 est soumise aux restrictions d'utilisation exprimées ci-dessous :

- La plate-forme doit être utilisée conformément à l'environnement d'utilisation prévu dans la cible de sécurité (§ 3.10) ;
- Les recommandations des guides de programmation des applications pour MULTOS doivent être impérativement respectées ;
- L'utilisateur de la plate-forme devra s'assurer que le correctif applicatif AMD 0029v002 est installé ;
- La clé publique (Application Provider's Asymetric Key) distribuée aux développeurs pour signer les applications à charger doit rester confidentielle.

Les résultats de l'évaluation ne sont valables que dans la configuration spécifiée dans le présent rapport de certification.

3.10. Objectifs de sécurité sur l'environnement

Les objectifs de sécurité suivants sont extraits de la cible de sécurité du produit [ST] :

3.10.1. Objectifs de sécurité sur la livraison du produit (phases 4 à 7)

- Les procédures de livraison doivent assurer la protection du composant masqué (protection matérielle et des informations du composant masqué) de manière à respecter les objectifs suivants : (O.DLV_PROTECT)
  - Non-divulgation des informations relevant de la sécurité ;
  - Identification des éléments livrés ;

[1] La cible de sécurité [ST] du produit ne revendique pas de conformité à un profil de protection.

- Règles de confidentialité (niveau de confidentialité, bordereau de livraison, accusé de réception) ;
- Protection physique pour prévenir à tout dommage physique ;
- Stockage sécurisé et procédures de stockage (incluant aussi les composants masqués rejetés) ;
- Traçabilité du composant masqué durant les livraisons (origine de la livraison et moyen d'expédition, accusés de réception, localisation du matériel et des informations) ;

- Des procédures doivent assurer que des actions correctives sont prises dans le cas d'opérations erronées durant une livraison (O.DLV_AUDIT) ;
- Des procédures doivent assurer que les personnes impliquées dans la livraison du composant masqué possèdent les connaissances suffisantes et ont suivi des formations afin de satisfaire aux exigences des procédures (O.DLV_RESP) ;

3.10.2. Objectifs de sécurité sur la livraison de la phase 1 à 4,5 et 6

- Les données de l'application doivent être livrées entre le développeur du logiciel embarqué et la mise en micro-module, ou l'encarteur, ou le personnalisateur de manière sécurisée, avec des procédures permettant de garantir l'intégrité et la confidentialité des données de l'application (O.DLV_DATA) ;

3.10.3. Objectifs de sécurité sur les phases 4 à 6

- Les tests appropriés des fonctionnalités du composant masqué doivent être effectués dans les phases 4 à 6. Durant toutes les phases de fabrication et de tests, des procédures de sécurité doivent être utilisées dans les phases 4, 5 et 6 pour garantir la confidentialité et l'intégrité du composant masqué et de ses données (O.TEST_OPERATE) ;

3.10.4. Objectifs de sécurité sur la phase 7

- Des protocoles et des procédures de communication sécurisées doivent être utilisés entre la carte à puce et le terminal (O.USE_DIAG) ;
- La documentation relative à la génération de certificats de chargement d'application (ALC – Application Load Certificate) pour les émetteurs de cartes doit indiquer que (O.CODE_HASH) :
  - si une application peut utiliser des mécanismes cryptographiques robustes, il est obligatoire de fournir un hash de l'application afin que le MSM puisse l'inclure dans l'en-tête de la clé de l'ALC ;
  - si une application ne peut pas utiliser de mécanismes cryptographiques robustes, il est alors fortement recommandé de fournir aussi un hash de l'application afin de l'inclure dans l'en-tête de la clé de l'ALC ;

3.10.5. Objectifs de sécurité sur le développement et le chargement des applications chargées

- Les fournisseurs d'applications chargées doivent (a) suivre les guides administrateur, (b) et fournir un canal de confiance lors de la livraison de l'application, afin de maintenir l'intégrité et la confidentialité de l'application et de garantir l'origine de la livraison de l'application (O.APPLI_DEV) ;

3.11. Synthèse des résultats

L'ensemble des travaux réalisés par le centre d'évaluation est accepté par le centre de certification qui atteste que la **plate-forme MULTOS I4C version 1-1-1 incluant le patch AMD 0029v002** identifiée au paragraphe 1.1 et décrite au paragraphe 1.3 du présent rapport **est conforme** aux exigences spécifiées dans la cible de sécurité [ST]. L'ensemble des travaux d'évaluation et les résultats de ces travaux sont décrits dans le rapport technique d'évaluation [RTE].

Annexe 1. Rapport de visite du site de Keycorp en Australie

Le site de développement de **Keycorp Limited situé 67 Albert Avenue Chatswood NSW2067, Australie** a fait l'objet d'une visite dans le cadre de l'évaluation de la version 1Q de la plate-forme MULTOS [2003/01].

Annexe 2. Analyse des mécanismes cryptographiques

Les mécanismes cryptographiques de la plate-forme MULTOS I4C 1-1-1 sont identiques à ceux de la version précédente, la plate-forme MULTOS 1Q. Par conséquent les mécanismes n'ont pas de nouveau été analysés dans le cadre de l'évaluation de la plate-forme, les résultats de la plate-forme MULTOS 1Q pouvant s'appliquer à la plate-forme I4C 1-1-1.

Annexe 3. Exigences fonctionnelles de sécurité du produit évalué

Attention : les descriptions des composants fonctionnels suivants sont donnés à titre indicatif. Seule une lecture attentive de la cible de sécurité [ST] peut apporter la description exacte des exigences fonctionnelles.

Class FAU	**Security audit**
Security audit automatic response	
FAU_ARP.1	*Security alarms* Le produit doit entreprendre des actions (spécifiées dans la cible de sécurité [ST]) dans le cas où une violation potentielle de la sécurité est détectée.
Security audit analysis	
FAU_SAA.1	*Potential violation analysis* Le produit doit implémenter un seuil de détection élémentaire, défini selon une règle fixée (spécifiée dans la cible de sécurité [ST]).
Class FCS	**Cryptographic support**
Cryptographic key management	
FCS_CKM.3	*Cryptographic key access* Les accès aux clés cryptographiques doivent être effectués conformément à une méthode d'accès spécifiée qui peut être basée sur une norme identifiée. Les paramètres de cette exigence sont spécifiés dans la cible de sécurité [ST].
FCS_CKM.4	*Cryptographic key destruction* Le produit doit détruire les clés cryptographiques conformément à une méthode de destruction spécifiée qui peut être basée sur une norme identifiée. Les paramètres de cette exigence sont spécifiés dans la cible de sécurité [ST].
Cryptographic operation	
FCS_COP.1	*Cryptographic operation* Le produit doit exécuter des opérations cryptographiques conformément à un algorithme spécifié et des clés cryptographiques dont les tailles peuvent prendre plusieurs valeurs spécifiées. L'algorithme et les tailles des clés cryptographiques spécifiés peuvent être basés sur une norme identifiée (spécifiés dans la cible de sécurité [ST]).
Class FDP	**User data protection**
Access control policy	
FDP_ACC.2	*Complete access control* Chaque règle de contrôle d'accès identifiée doit s'appliquer à toutes les opérations sur les sujets et objets couverts par cette règle. De plus tous les objets et toutes les opérations doivent être couverts par au moins une règle de contrôle d'accès identifiée.
Access control functions	
FDP_ACF.1	*Security attribute based access control* Le produit doit mettre en œuvre des accès basés sur des attributs de sécurité

	et des groupes d'attributs désignés. Il peut aussi offrir l'aptitude d'autoriser ou de refuser explicitement l'accès à un objet sur la base d'attributs de sécurité.
Data authentication	
FDP_DAU.1	*Basic data authentication* Le produit doit être capable de garantir l'authenticité des informations contenues dans des objets spécifiés dans la cible de sécurité [ST] (e.g. des documents).
Export to outside TSF control	
FDP_ETC.1	*Export of user data without security attributes* Le produit doit appliquer les règles de sécurité appropriées lors de l'exportation de données de l'utilisateur à l'extérieur. Les données de l'utilisateur exportées par cette fonction sont exportées sans les attributs de sécurité qui leur sont associés.
Import from outside TSF control	
FDP_ITC.1	*Import of user data without security attributes* Les attributs de sécurité doivent représenter correctement les données de l'utilisateur et doivent être fournis séparément de l'objet.
Residual information protection	
FDP_RIP.1	*Subset residual information protection* Le produit doit garantir que toutes les informations résiduelles contenues dans n'importe quelle ressource ne sont pas disponibles pour un sous-ensemble défini des objets lors de l'allocation ou de la désallocation de la ressource.
Rollback	
FDP_ROL.1	*Basic rollback* Le produit doit pouvoir annuler un certain nombre d'opérations effectuées sur des objets.
Stored data integrity	
FDP_SDI.2	*Stored data integrity monitoring and action* Le produit doit contrôler les données des utilisateurs stockées pour rechercher des erreurs d'intégrité identifiées et entreprendre des actions (spécifiées dans la cible de sécurité [ST]) suite à une détection d'erreur.
Class FIA	**Identification and authentication**
Authentication failures	
FIA_AFL.1	*Authentication failure handling* Le produit doit être capable d'arrêter le processus d'établissement d'une session après un nombre spécifié de tentatives d'authentification infructueuses d'un utilisateur. Il doit aussi, après la clôture du processus d'établissement d'une session, être capable de désactiver le compte de l'utilisateur ou le point d'entrée (e.g. station de travail) à partir duquel les tentatives ont été faites jusqu'à ce qu'une condition définie par un administrateur se réalise.
User attribute definition	
FIA_ATD.1	*User attribute definition* Les attributs de sécurité spécifiés dans la cible de sécurité [ST] doivent être maintenus individuellement pour chaque utilisateur.
User authentication	

FIA_UAU.1	*Timing of authentication* Le produit autorise un utilisateur à exécuter certaines actions, spécifiées dans la cible de sécurité [ST], avant que son identité ne soit authentifiée.
FIA_UAU.4	*Single-use authentication mechanisms* Le mécanisme d'authentification doit fonctionner avec des données d'authentification à usage unique.
User identification	
FIA_UID.1	*Timing of identification* Le produit autorise les utilisateurs à exécuter certaines actions, identifiées dans la cible de sécurité [ST], avant d'être identifiés.
User-subject binding	
FIA_USB.1	*User-subject binding* La relation entre les attributs de sécurité de l'utilisateur et un sujet agissant pour le compte de cet utilisateur doit être maintenue.
Class FMT	**Security management**
Management of functions in TSF	
FMT_MOF.1	*Management of security functions behaviour* Le produit doit limiter la capacité à gérer le comportement des fonctions de sécurité du produit à des utilisateurs autorisés (spécifiés dans la cible de sécurité [ST]).
Management of security attributes	
FMT_MSA.1	*Management of security attributes* Les utilisateurs autorisés doivent pouvoir gérer les attributs de sécurité spécifiés.
FMT_MSA.2	*Secure security attributes* Le produit doit garantir que les valeurs assignées aux attributs de sécurité sont valides par rapport à l'état sûr.
FMT_MSA.3	*Static attribute initialisation* Le produit doit garantir que les valeurs par défaut des attributs de sécurité sont soit de nature permissive soit de nature restrictive.
Management of TSF data	
FMT_MTD.1	*Management of TSF data* Les utilisateurs autorisés peuvent gérer les données des fonctions de sécurité du produit.
FMT_MTD.2	*Management of limits on TSF data* Ce composant spécifie l'action à entreprendre lorsque les valeurs limites des données sont atteintes ou dépassées.
Security management roles	
FMT_SMR.1	*Security roles* Les rôles relatifs à la sécurité que le produit reconnaît doivent être identifiés et associés à des utilisateurs (spécifiées dans la cible de sécurité [ST]).
Class FPR	**Privacy**
Unobservability	
FPR_UNO.1	*Unobservability* Le produit n'autorise pas certains utilisateurs (spécifiées dans la cible de sécurité [ST]) à déterminer si certaines opérations (spécifiées dans la cible

	de sécurité [ST]) sont en cours d'exécution.
Class FPT	**Protection of the TSF**
Fail secure	
FPT_FLS.1	*Failure with preservation of secure state* Le produit doit préserver un état sûr dans le cas de défaillances identifiées.
TSF physical protection	
FPT_PHP.3	*Resistance to physical attack* Le produit doit empêcher ou résister à certaines intrusion physique (spécifiées dans la cible de sécurité [ST]) sur certaines parties du produit (spécifiées dans la cible de sécurité [ST]).
Trusted recovery	
FPT_RCV.4	*Function recovery* La reprise au niveau de fonctions de sécurité identifiées (dans la cible de sécurité [ST]) doit être garantie, en garantissant soit la réussite finale, soit un retour des données dans un état sûr.
Reference mediation	
FPT_RVM.1	*Non-bypassability of the TSP* Les règles de sécurité du produit ne doivent pas pouvoir être contournées.
Domain separation	
FPT_SEP.1	*TSF domain separation* Le produit doit offrir un domaine protégé et distinct pour les fonctions de sécurité du produit et procurer une séparation entre sujets.
Inter-TSF TSF data consistency	
FPT_TDC.1	*Inter-TSF basic TSF data consistency* Le produit doit offrir la capacité de garantir la cohérence des attributs lors des échanges avec un autre produit de confiance.
TSF self test	
FPT_TST.1	*TSF testing* Le produit doit effectuer des tests permettant de s'assurer de son fonctionnement correct. Ces tests peuvent être effectués au démarrage, de façon périodique, à la demande d'un utilisateur autorisé ou quand d'autres conditions sont remplies. Le produit doit aussi permettre aux utilisateurs autorisés de contrôler l'intégrité de données du produit et du code exécutable.
Class FRU	*Resource utilisation*
Resource allocation	
FRU_RSA.1	*Maximum quotas* Le produit doit garantir, à l'aide de mécanismes de quotas, que les utilisateurs et les sujets ne monopoliseront pas une ressource contrôlée.

Annexe 4. Niveaux d'assurance prédéfinis IS 15408 ou CC

Classe	Famille	Composants par niveau d'assurance						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Classe ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Classe ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Classe ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	**3**
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Classe AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Classe ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Classe ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Classe AVA Estimation des vulnérabilités	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Annexe 5. Références documentaires du produit évalué

[2003/01]	Rapport de certification 2003/01 Plate-forme MULTOS 4.06 version 1Q (composant SLE66CX320P / m1421B25 masqué par MULTOS 4.06 release 1Q + AMD 0030v001) Janvier 2003 Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI)
[322P-A24]	Certification Report Smart Card IC (Security Controller) SLE66CX322P with RSA 2048 / m1484a24, A27 and B14 Référence BSI-DSZ-CC-0223-2003 Bundesamt für Sicherheit in der Informationstechnik
[CA-PM]	MULTOS CA Process Map Reference PM-06 Version 5.0 Octobre 2001 Mondex International
[GALU]	Guide to Generating Application Load Units Reference MAO-DOC-REF-009 Version 2.51 Décembre 2002 MAOSCO
[GLDA]	Guide to Loading and Deleting Applications Reference MAO-DOC-REF-008 Version 2.20 Janvier 2000 MAOSCO
[GMS]	A Guide to the MULTOS Scheme Reference MAO-DOC-REF-003 Version 2.00 Mars 2000 MAOSCO
[HLD]	Keycorp MULTOS High Level Design Specification Reference SIM-SP-0181 Version 1.0 17 mars 2003 Keycorp Limited
[IFD-MISA]	IFD-MISA Interface Specifcation Reference MAOS-GKC-DEV-030 Version 2.0 Février 2001

	MAOSCO
[INFCD]	SLE66CX322P / m1484 Delivery Reference Delivery_10 Version 1.0 Infineon
[JIL-Comp]	Les guides pour la composition sont : ▪ ETR-lite for composition version 1.0 mars 2002 Joint Interpretation Library ▪ ETR-lite for composition : Annex A, Composite smartcard evaluation : Recommended best practice version 1.2 mars 2002 Joint Interpretation Library
[LGC]	La liste de configuration pour les documents est : ▪ Configuration List of MAOSCO documentation Version 1.0 14 mars 2003 Mondex International Celle pour le système d'exploitation MULTOS I4C : ▪ Manufacturing Data Pack Reference SIM-DP-0091 Version 1.2 Keycorp Et celle pour le patch AMD 0029v002 : ▪ Manufacturing Data Pack Reference SIM-DP-0092 Version 1.1 Keycorp
[MCDL]	Enablement / MSM Controls data Loading Reference mao-doc-tbl-004 Version 3 Mai 1999 MAOSCO
[MDRM]	MULTOS Developers Reference Manual Reference MAO-DOC-REF-006 Version 1.40 December 2001 MAOSCO

[MGKC]	MGKC MULTOS Management Procedures Reference MXI-MGKC-PRO-004 Version 5.0 Mai 2002 Mondex International
[MIR]	MULTOS Implementation Report Reference MAO-DOC-REF-010 Version 1.23 July 2002 MAOSCO
[MISA-HG]	MISA Handling Guidelines Reference MAOS-GKC-DEV-032 Version 3.0 Février 2001 MAOSCO
[MKHD]	MULTOS TKCK & HM Preparation & Despatch Reference mxi-ca-mops-002 Version 1.0 Avril 2001 Mondex International
[MSM-CDC]	Produce MSM Controls Data Checklist Reference CH-06 Version 10.0 Mars 2003 Mondex International
[M-SPI]	M-SPI 4.0 User Guide Reference MAOS-GKC-DEV-020 Version 4.02 Mondex International
[MVP]	KEYCORP MULTOS Mask Verification Procedure Reference SIM-PR-0012 Version 1.0 Keycorp
[OSDEL]	Keycorp MULTOS – Delivery Process Reference SIM-IN-0003 Version 3.0 Avril 2002 Keycorp
[PGRI]	Security Procedures for Generating the Keycorp / Infineon MULTOS 4 ROM Image Reference maos-gkc-ops-007 Version 2-0

	Octobre 2000 Mondex International
[RTE]	Evaluation Technical Report Référence EX3_RTE Version 1.0L 29 avril 2003 CEACI Erratum to the Evaluation Technical Report Référence EX3_ERR_01 Version 1.0 21 octobre 2003 CEACI
[SGAD]	Security Guidance for Application Developers Reference SIM-MA-0031 Version 1.1 May 2002 Keycorp Limited
[SSM]	Security Manager Procedures Reference SSM-PRO-001 Version 4.0 Octobre 2002 Mondex International
[SSVG]	Profil de protection «Smartcard Integrated Circuit Protection Profile v2.0» Référence BSI-PP-0002 Bundesamt für Sicherheit in der Informationstechnik
[ST]	Keycorp MULTOS Common Criteria Security Target Reference SIM-SP-0167 Version 2.1 18 mars 2003 Keycorp Limited

Annexe 6. 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.	
Décret 2001-272 du 30 mars 2001- Décret pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.	
[CC]	Critères Communs pour l'évaluation de la sécurité des technologies de l'information: ▪ Part 1: Introduction and general model, august 1999, version 2.1, ref CCIMB-99-031 ; ▪ Part 2: Security functional requirements, august 1999, version 2.1, ref CCIMB-99-032 ; ▪ Part 3: Security assurance requirements, august 1999, version 2.1, réf: CCIMB-99-033.
[CEM]	Méthodologie d'évaluation de la sécurité des technologies de l'information: ▪ Part 2: Evaluation Methodology, august 1999, version 1.0, ref CEM- 99/045.
[IS 15408]	Norme IS/IEC 15408 :1999, comportant 3 documents : ▪ IS 15408–1: (Part 1) Introduction and general model ; ▪ IS 15408–2: (Part 2) Security functional requirements ; ▪ IS 15408–3: (Part 3) Security assurance requirements ;
[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 2.0, April 1999, Management Committee of Agreement Group.
[MQ]	Manuel qualité du centre de certification Référence SGDN/DCSSI/SDR/MQ.01 Version 1.0 SGDN/DCSSI
[CER/P/01]	Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information Référence CER/P/01.1 Version 1 SGDN/DCSSI

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat Général de la Défense Nationale
Direction Centrale de la Sécurité des Systèmes d'Information
Bureau certification
51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr