PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2018/35-R01

Plateforme IDMotion V2 (OS Multos V4.5.2, AMD version 0151v001)

Paris, le 23 Septembre 2024

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

Vincent STRUBEL

[ORIGINAL SIGNE]

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

AVERTISSEMENT

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CC-2018/35-R01**
Nom du produit **Plateforme IDMotion V2**
Référence/version du produit **OS Multos V4.5.2, AMD version 0151v001**
Conformité à un profil de protection **Néant**
Critère d'évaluation et version **Critères Communs version 3.1 révision 5**
Niveau d'évaluation **EAL5 augmenté** ALC_DVS.2, AVA_VAN.5
Développeur **THALES DIS FRANCE SAS** 6, rue de la Verrerie 92190 Meudon, France
Commanditaire **THALES DIS FRANCE SAS** 6, rue de la Verrerie 92190 Meudon, France
Centre d'évaluation **THALES / CNES** 290 allée du Lac, 31670 Labège, France
Accords de reconnaissance applicables **CCRA** Ce certificat est reconnu au niveau EAL2. **SOG-IS**

PREFACE

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 directeur général de l'Agence nationale de la sécurité des systèmes d'information 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.cyber.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est la « Plateforme IDMotion V2, OS Multos V4.5.2, AMD version 0151v001 » développé par THALES DIS FRANCE SAS.

Le produit évalué est de type « carte à puce » avec et sans contact. Il est conçu de façon à ce que plusieurs applications puissent être chargées et exécutées de façon sécurisée sur la carte à puce. Ces applications sont écrites dans un langage, indépendant du composant sous-jacent, nommé MEL[1]. Les applications en langage MEL sont interprétées par le système d'exploitation Multos.

1.2 Description du produit

1.2.1 *Introduction*

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

La cible de sécurité s'inspire du profil de protection [PP/0010].

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont décrits au chapitre 2.5 « *Target of evaluation description* » de la cible de sécurité [ST]. Ils comprennent notamment :

- le chargement d'applications ;
- la suppression d'applications ;
- la vérification de la signature des applications ;
- le déchiffrement des applications ;
- le chargement des données de contrôle MSM[2] ;
- l'écrasement des données critiques ;
- la gestion de l'exécution des applications ;
- la protection de la réinitialisation ;
- le contrôle d'intégrité des données sensibles de la plateforme (applications, clés internes…) ;
- l'autotest au démarrage et pendant l'initialisation ;
- la gestion des réactions aux tentatives de pénétration ;
- l'authentification de la carte ;
- la protection du chargement d'applications *post-issuance* ;
- l'isolation des applications entre contextes différents et la protection de la confidentialité et de l'intégrité des données applicatives entre les applications.

[1] *Multos Executable Language* - langage exécutable Multos.

[2] *Multos Security Manager* - gestionnaire de sécurité Multos.

1.2.3 *Architecture*

La TOE[3], comme décrit au chapitre 2.5.1 « *Product description* », est constituée des éléments suivants :

- du circuit intégré IFX_CCI_000014 développé et fabriqué par INFINEON TECHNOLOGIES AG ;
- du sous-système *hardware-dependent*, appelé *« drivers »* ;
- de la plateforme Multos avec sa machine virtuelle et ses API ;
- des primitives propriétaires incluant :
  - le module *Biometry Secure Messaging fileSystem* (inclus dans la TOE, mais hors TSF) ;
  - l'application ETravel EAC/PACE/BAC v2.4 chargée en Flash (hors TOE, mais faisant partie de l'image de la TOE) ;
  - l'application native GMF[4] v1.0 (hors TOE),
- des applications Multos chargées en NVM et exécutées par la machine virtuelle Multos (hors TOE) :
  - *Pin Server Application* (PSA) v0.2 ;
  - IAS Classic v4.4.1C ;
  - MOC client (MOCC) v1.0.2A.

Bien que ces applications ne soient pas incluses dans le périmètre de l'évaluation, elles ont été prises en compte dans le processus d'évaluation conformément aux prescriptions de [OPEN].

1.2.4 *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 du tableau ci-après, détaillés dans la cible de sécurité [ST] au chapitre 2.3 « *Security target identification* ».

Eléments de configuration		Origine
OS version Multos V4.5.2	« 000452 »	THALES DIS FRANCE SAS
Version du code correctif (AMD) IDMotion V2	« 0151001 »	
Build number 1.1.47	« 00010001002F »	
Identifiant de la plateforme	« 16 »	
Donnée d'identification du circuit intégré IFX_CCI_000014	« 00 00 14 »	INFINEON TECHNOLOGIES AG

Tableau 1 : Identification du produit

[3] *Target of Evaluation*

[4] *Global Master File*

Ces éléments peuvent être vérifiés par l'utilisation de la commande GET CONFIGURATION DATA. La procédure d'identification du produit est décrite dans le guide [MDRM].

La principale différence entre le produit et la TOE correspond aux applications chargées pré-émission sur ce produit. Toutes les applications qui étaient présentes dans la configuration du produit à la disposition de l'évaluateur sont identifiées dans le tableau ci-après.

Nom, version de l'application	**Identification**	**Nom du *codelet***
IAS classic v4.4.1C	0x00B8	IASClassic.app,Codelet
MOC client v1.0.2A	0x00B9	MOCClient.app,Codelet
PSA v0.2	0x00B7	PSACodelet.app,Codelet

Tableau 2 : Applications chargées sur le produit

La commande *GET CONFIGURATION DATA* (Codelets) permet à l'utilisateur du produit de vérifier quelles applications sont installées dans le produit à sa disposition.

1.2.5 *Cycle de vie*

Le cycle de vie du produit est décrit au chapitre 2.5.4 *« Smartcard Product Life Cycle »* de la cible de sécurité [ST] ; il est conforme à celui décrit dans [PP0084], à l'exception du point de livraison qui s'effectue à la fin de la phase 5. Les rapports des audits de sites effectués dans le schéma français et pouvant être réutilisés, hors certification de site, sont mentionnés dans [SITES].

Les phases 1 à 5 correspondent à la construction de la TOE. Elles ont été prises en compte dans la présente évaluation, avec, pour les phases 2 et 3, une réutilisation des résultats de l'évaluation du composant, voir [CR_IC]. Aucune procédure de *patching* n'est possible après la phase 5.

La phase 6 correspond à la personnalisation du produit. La phase 7 correspond quant à elle à la phase opérationnelle du produit. Ces phases sont couvertes par des recommandations sécuritaires (voir [GUIDES]).

Le guide [GALU] identifie également des recommandations relatives à la livraison des futures applications à charger sur cette carte.

Par ailleurs, les guides [SGAD] et [MDRM] décrivent les règles de développement des applications destinées à être chargées sur cette carte.

1.2.6 *Configuration évaluée*

Le certificat porte sur la configuration telle que présentée par le Tableau 1 : Identification du produit.

La configuration ouverte du produit a été évaluée conformément à [OPEN] : ce produit correspond à une plateforme ouverte cloisonnante. Ainsi tout chargement de nouvelles applications conformes aux contraintes exposées au chapitre 3.2 du présent rapport de certification ne remet pas en cause le présent rapport de certification lorsqu'il est réalisé selon les processus audités.

Toutes les applications identifiées dans le Tableau 2 ont été vérifiées conformément aux contraintes décrites dans [GUIDES].

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC], et à la méthodologie d'évaluation définie dans le manuel [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 [JIWG IC] et [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

2.2 Travaux d'évaluation

L'évaluation en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel dans le microcontrôleur déjà certifié par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur « IFX_CCI_000014h », voir [CER_IC].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le jour de sa finalisation par le CESTI (voir date en bibliographie), détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

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

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [ST]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [ANA_CRY].

Cette analyse a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Elles ont été prises en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

2.4 Analyse du générateur d'aléa

Le générateur de nombres aléatoires, de nature physique, utilisé par le produit final a été évalué dans le cadre de l'évaluation du microcontrôleur (voir [CER_IC]).

Par ailleurs, comme requis dans le référentiel [ANSSI Crypto], la sortie du générateur physique d'aléa subit un retraitement de nature cryptographique.

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

3 La certification

3.1 Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation visé.

3.2 Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

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

- toutes les futures applications chargées sur ce produit (chargement post-émission) doivent respecter les contraintes de développement de la plateforme (guides [SGAD] et [AGD-MDRM]) ;
- pour le chargement de futures applications sur le produit, ces dernières devront appliquer la procédure de vérification ([SGAD], [GALU] et [VP]) ;
- la protection du chargement de toutes les futures applications chargées sur ce produit (chargement post-émission) doit être activée conformément aux indications de [GDLA] ;
- la protection du chargement de toutes les applications chargées pré-émission doit être activée conformément aux indications de [GDLA].

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[5], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

3.3.2 *Reconnaissance internationale critères communs (CCRA)*

Ce certificat est émis dans les conditions de l'accord du CCRA [CCRA].

L'accord « *Common Criteria Recognition Arrangement* » permet la reconnaissance, par les pays signataires[6] , des certificats Critères Communs.

La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL2 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[5] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

[6] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

ANNEXE A. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - *IDMotion V2 Platform Security Target*, référence ST_D1172991, version 2.5, 25 avril 2024. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *IDMotion V2 Platform Security Target public version*, référence ST_D1172991_P, version 2.0.
[RTE]	Rapport technique d'évaluation : - *Evaluation technical report BOLERO_A*, référence BOLA_2023_ETR_1, version 1.3, 19 août 2024.
[ANA_CRY]	*Analysis of Cryptographic Mechanisms BOLERO_A*, référence BOLA_2023_CRY, version 1.3, 19 août 2024.
[CONF]	Liste de configuration du produit : *BOLERO_A: ALC LIS CC document*, référence *BOLERO_A_Deliverables*, version 1.5, 25 avril 2024.
[GUIDES]	Guide d'installation du produit : - [AGD_PRE] *AGD_PRE ID MOTION V2 Platform*, référence D1598745, version 1.3, 11 août 2023. Guide d'administration et d'utilisation du produit : - [AGD_OPE] *AGD_OPE ID MOTION V2 Platform,* référence D1600741, version 1.3 ; - [ENA] *Multos Enablement*, référence MAO-DOC-TEC-101, version 1.4 ; - [GLDA] *MULTOS - GLDA, Guide to Loading and Deleting*, référence MAO-DOC-TEC-008, version 2.29 ; - [MDRM] *MULTOS - MDRM, Multos Developer's Reference Manual*, référence MAO-DOC-TEC-006, version 1.59 ; - *Card Initialization Specification Multos ID Motion V2*, référence CIS_Multos_ID_Motion_V2, version A02.0 ; - [SGAD] *MULTOS - Security Guidance for MULTOS Application Developers*, référence MI-MA-0031, version 2.0 ; - [GALU] *Multos GALU, Guide to Generating Application Load Units*, référence MAO-DOC-TEC-009, version 2.9 ; - [VP] *MULTOS - Mask Verification Procedure*, référence MI-PR-0012, version 1.1.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - DISGEN21_ALC_GEN_v1.0 ; - DISGEN22_ALC_GEN_v1.1 ; - DISGEN23_ALC_GEN_v1.0 ;

	- [CBA] DISGEN23_CUR_STAR_v1.0 ; - [MDN] DISGEN21_MDN_STAR_v1.1 ; - [SGP] DISGEN22_SGP_STAR_v1.0 ; - [GEM] DISGEN22_GEM_STAR_v1.0 ; - [VAN] DISGEN21_VAN_STAR_v1.0 ; - [TCZ] DISGEN23_TCZ_STAR_v1.0 ; - [CHA] DISGEN22_CHA_STAR_v1.0 ; - [PAU] DISGEN22_PAU_STAR_v1.0.
[CER_IC]	*Infineon Security Controller IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h in the design step H13 and including optional software libraries and dedicated firmware in several versions* Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 9 septembre 2022 sous la référence BSI-DSZ-CC-1110-V5-2022-MA-01.
[PP0084]	*Protection Profile, Security IC Platform Protection Profile with Augmentation Packages*, version 1.0, 13 janvier 2014. Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) sous la référence BSI-PP-0084-2014.
[PP/0010]	*Protection Profile Smart Card Integrated Circuit With Multi-Application Secure Platform*, version 2.0, novembre 2000. Certifié par l'ANSSI sous la référence PP/0010.

ANNEXE B. 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]	Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, référence ANSSI-CC-CER-P-01, version 5.0.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1.
[CC]	*Common Criteria for Information Technology Security Evaluation:* - *Part 1 : Introduction and general model*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001 ; - *Part 2 : Security functional components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002 ; - *Part 3 : Security assurance components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	*Common Methodology for Information Technology Security Evaluation : Evaluation Methodology*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[JIWG IC] *	*Mandatory Technical Document – The Application of CC to Integrated Circuits*, version 3.0, février 2009.
[JIWG AP] *	*Mandatory Technical Document – Application of attack potential to smartcards and similar devices*, version 3.2, novembre 2022.
[COMP] *	*Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices*, version 1.5.1, mai 2018.
[OPEN]	*Certification of « Open » smart card products*, version 1.1 (*for trial use*), 4 février 2013.
[CCRA]	*Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security*, 2 juillet 2014.
[SOG-IS]	*Mutual Recognition Agreement of Information Technology Security Evaluation Certificates*, version 3.0, 8 janvier 2010, Management Committee.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.

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