PREMIÈRE 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-2019/57-R01

IDmove v4 on Infineon in EAC with PACE configuration with AA in option (OS Commercial Version : 0x 09 08 06 ; OS Unique Identifier : 0x DC 71)

Paris, le 18 Juillet 2023

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

Vincent STRUBEL

[ORIGINAL SIGNE]

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-2019/57-R01

Nom du produit

IDmove v4 on Infineon in EAC with PACE configuration with AA in option

Référence/version du produit

OS Commercial Version : 0x 09 08 06 ; OS Unique Identifier : 0x DC 71

Conformité à un profil de protection

Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE, Version 1.3.2

certifié BSI-CC-PP-0056-V2-2012-MA-02 le 5 décembre 2012

Machine Readable Travel Document using Standard Inspection Procedure with PACE, Version 1.01

certifié BSI-CC-PP-0068-V2-2011-MA-01 le 22 juillet 2014

Critère d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

IDEMIA
2 place Samuel de Champlain,
92400 Courbevoie, France

INFINEON TECHNOLOGIES AG
AIM CC SM PS – Am Campeon 1-12, 85579
Neubiberg, Allemagne

Commanditaire

IDEMIA
2 place Samuel de Champlain,
92400 Courbevoie, France

Centre d'évaluation

SERMA SAFETY & SECURITY
14 rue Galilée, CS 10071,
33608 Pessac Cedex, 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.ssi.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « *IDmove v4 on Infineon in EAC with PACE configuration with AA in option, OS Commercial Version : 0x 09 08 06 ; OS Unique Identifier : 0x DC 71* » développé par IDEMIA et INFINEON TECHNOLOGIES AG.

Il implémente les fonctions de document de voyage électronique conformément aux spécifications de l'organisation de l'aviation civile internationale (ICAO). Ce produit est destiné à permettre la vérification de l'authenticité du document de voyage et à identifier son porteur lors d'un contrôle frontalier, à l'aide d'un système d'inspection.

Ce microcontrôleur et son logiciel embarqué ont vocation à être insérés dans la couverture des passeports traditionnels, dans une *eCover* ou dans une *eDatapage*.

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.

Cette cible de sécurité est strictement conforme aux profils de protection [PP_EACv2] et [PP_PACE].

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont :

- la protection en intégrité des données du porteur stockées dans la carte : nations ou organisations émettrices, numéro du document de voyage, date d'expiration, nom du porteur, nationalité, date de naissance, sexe, portrait, autres données optionnelles, données biométriques additionnelles et autres données permettant de gérer la sécurité du document de voyage ;
- le contrôle d'accès aux données du porteur stockées dans la carte ;
- la protection, en intégrité et en confidentialité, des données lues à l'aide du mécanisme *Secure Messaging* ;
- l'authentification du microcontrôleur par le mécanisme optionnel *Active Authentication* (AA) ;
- le mécanisme *Extended Access Control* (EAC) d'authentification forte entre le microcontrôleur et le système d'inspection préalable à tout accès aux données biométriques, permettant l'établissement d'un canal sécurisé fort (*secure messaging*) ;
- le mécanisme *Password Authenticated Connection Establishment* (PACE) pour (1) l'authentification entre le microcontrôleur et le système d'inspection, et (2) l'établissement d'un canal sécurisé fort (*secure messaging*).

1.2.3 *Architecture*

Le produit est constitué, comme décrit au chapitre 2.3.1 de la cible :

- du microcontrôleur IFX_CCI_000005h H13, développé par INFINEON TECHNOLOGIES AG et certifié sous la référence [CER-IC] ;
- d'un module « BIOS » qui fournit les fonctionnalités pour la gestion des accès vers la couche applicative. Il fournit également les fonctions de gestion des exceptions et de communication ;
- d'une librairie cryptographique qui fournit à la couche applicative, les fonctions de sécurité cryptographique ;
- d'un module *Secure Messaging* qui fournit les fonctionnalités pour protéger en intégrité, authenticité et confidentialité les données permettant ainsi de disposer d'un moyen de communication sécurisée durant les phases de fabrication, de personnalisation et d'utilisation opérationnelle ;
- de *Resident Application* (RA), qui fournit un jeu de commandes complet qui permet la gestion de la carte dans sa phase opérationnelle ;
- de l'*Application Creation Engine* (ACRE), qui fournit un jeu de commandes complet utilisé pour pré-personnaliser la carte et ses applications ;
- de l'application *Machine Readable Travel Document* (MRTD), qui fournit un jeu de commandes complet qui permet la gestion des données MRTD durant la phase opérationnelle ;
- et d'un *boot* qui est en charge de gérer le démarrage des applications MRTD, RA et ACRE.

Tous ces éléments font partie de la cible d'évaluation (TOE).

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 suivants, décrits dans le guide [AGD_PRE] :

- OS *commercial version* : 0x 09 08 06 ;
- OS *Unique Identifier* : 0x DC 71 ;
- *Chip type :*
  - ID1 : 0x 00 13,
  - ID2 : 0x XX XX pouvant prendre des valeurs différentes selon la configuration du microcontrôleur,
  - ID3 : 0x 00 00 ;
- *Design step* : 0x 07 0D (H13) ;
- IFX_CCI : 0x 00 00 05 ;
- *Firmware version identifier* : 0x 80 10 01 73.

Ces valeurs peuvent être vérifiées en utilisant la commande GET DATA avec le tag DF50 comme indiqué dans [AGD_PRE].

1.2.5 *Cycle de vie*

Les trois cycles de vie du produit sont décrits au chapitre 2.2.3de la cible de sécurité [ST].

Ils sont conformes au profil de protection [PP0084].

Les rapports des audits de sites effectués dans le schéma français et pouvant être réutilisés, hors certification de site, sont mentionnés dans [SITES].

1.2.6 *Configuration évaluée*

Le certificat porte sur les configurations suivantes :

- le mécanisme EAC (*Extended Access Control*) - incluant entre autre le mécanisme CA (*Chip Authentication*) - enrichi avec les fonctionnalités suivantes par rapport au [PP_EAC] : (1) génération de tout type de *secure messaging* à l'issue du CA (DES, AES-128, AES-192 et AES-256), et (2) exigence d'un niveau minimum de *secure messaging* préalablement configuré pour accéder aux données biométriques sensibles (iris, empreinte biométrique), afin de garantir un niveau de confidentialité adéquate ;
- le mécanisme PACE (*Password Authenticated Connection Establishment*) ;
- le mécanisme AA (*Active Authentication*) qui est optionnel et éventuellement désactivé ;
- le mécanisme CA (*Chip Authentication*) qui est optionnel et éventuellement désactivé ;
- les phases de pré-personnalisation et de personnalisation.

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_000005h H13 » au niveau EAL6 augmenté des composants ALC_FLR.1, conforme au profil de protection [PP0084]. Ce microcontrôleur a été certifié 29 avril 2022 sous la référence BSI-DSZ-CC-1110-V5-2022, 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 [RTE].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto]. 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.

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].

3.3 Reconnaissance du certificat

3.3.1 *Reconnaissance européenne (SOG-IS)*

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

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à 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 :

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

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[2] , 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 :

[2] 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 : - *IDmove v4 on Infineon in EAC with PACE configuration with AA in option – Security Target,* référence FQR 110 8954, version 8, 19 décembre 2022. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *IDmove v4 on Infineon in EAC with PACE configuration with AA in option – Public Security Target,* référence FQR 110 9127, version 6, 19 décembre 2022.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report QUANTUM-R1 Project,* référence QUANTUM_R1_ETR_1.2, 2 juin 2023.
[CONF]	Liste de configuration du produit : - *QUANTUM - Configuration List*, FQR 110 9030, Version 10, 24 février 2023.
[GUIDES]	Guide d'installation du produit : - [AGD_PRE] *IDmove v4 on Infineon MRTD/IDL Preparative Guidance Document*, FQR 110 8997, version 6, 19 décembre 2022. Guide d'utilisation du produit : - [AGD_OPE] *IDmove v4 on Infineon MRTD/IDL User Guidance Document,* FQR 110 8998, version 1, 31 mars 2019. Guide d'utilisation des mécanismes cryptographiques : - *Quantum QR Recommendations for Crypto Assessment Compatibility*, FQR 110 9040, version 3, 11 novembre 2022.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - IDEMIA-2022_GEN_v1.0 ; - [CRB] IDEMIA2022_CRB_STAR_v1.0 ; - [HAA] IDEMIA2021_Haarlem_STAR_v1.0 ; - [NOI-P] IDEMIA2021_NOI-D_STAR_v1.0 ; - [OST] IDEMIA-2021_OST_STAR_v1.0 ; - [PSC] IDEMIA2022_Pessac _STAR_v1.0 ; - [SZN] IDEMIA2020_SZN_STAR_v1.0 ; - [VTR] IDEMIA2021_VTR_STAR_v1.1.
[CER_IC]	Produit *Infineon Security Controller IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h H13 including the optional software libraries and dedicated firmware in several versions.* Certifié par le BSI *(Bundesamt für Sicherheit in der Informationstechnik)* sous la référence BSI-DSZ-CC-1110-V5-2022.
[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 EACv2]	*Protection Profile, Machine Readable Travel Document with "ICAO Application", Extended Access Control*, version 1.3.2, 5 décembre 2012. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) sous la référence BSI-CC-PP-0056-V2-2012-MA-02.
[PP PACE]	*Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE*, version 1.0.1, 22 juillet 2014. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) sous la référence BSI-CC-PP-0068-V2-2011-MA-01.

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.
[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.