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-2023/66

IDmove v5 on SCR404U in PACE configuration with AA and/or CA in option (OS Commercial Version : 0x098912;OS Unique Identifier : 0xB7BC0108 et E48C0108)

Paris, le 19 Janvier 2024

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-2023/66

Nom du produit

IDmove v5 on SCR404U in PACE configuration with AA and/or CA in option

Référence/version du produit

OS Commercial Version : 0x098912;OS Unique Identifier : 0xB7BC0108 et E48C0108

Conformité à un profil de protection

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

ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_TAT.3, ALC_FLR.3, ALC_DVS.2, ATE_COV.3, ATE_FUN.2, AVA_VAN.5

Développeurs

IDEMIA

2 place Samuel de Champlain,
92400 Courbevoie, France

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 augmenté de ALC_FLR.3.

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 « IDmove v5 on SCR404U in PACE configuration with AA and/or CA in option, OS Commercial Version : 0x098912;OS Unique Identifier : 0xB7BC0108 et E48C0108 » développé par IDEMIA.

Le produit est de type « carte à puce » pouvant être utilisé en modes avec et sans contact. 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 conforme au profil de protection [PP PACE].

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont détaillés dans la cible de sécurité [ST] au chapitre 2.2.1 « *Usage and Major Security features of the TOE* ». Ils sont résumés ci-après :

- 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 ;
- l'authentification du microcontrôleur par le mécanisme optionnel *Active Authentication* (AA) et/ou *Chip Authentication* (CA) ;
- la protection, en intégrité et en confidentialité, des données lues à l'aide du mécanisme *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*) ;
- un service de mise à jour optionnel du logiciel disponible durant la phase de vie du produit (pré-personnalisation, personnalisation et utilisateur) inspiré du profil de protection [PP0090].

1.2.3 *Architecture*

Le produit est constitué, comme décrit au chapitre 2.3.1 *« TOE architecture »* de la cible de sécurité [ST] :

- du microcontrôleur SCR404U, développé par IDEMIA 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 du tableau ci-après, détaillés dans la cible de sécurité [ST] au chapitre 2.1.2 « *TOE reference* ».

Eléments de configuration		Origine
OS *commercial version*	0x098912	IDEMIA
OS Unique Identifier (avec *CAM*)	0xB7BC0108	
OS Unique Identifier (sans CAM)	0xE48C0108	
IC type	0x2E (SCR404U)	
IC revision	0x02	
IC configuration	0x02	

Ces éléments peuvent être vérifiés en utilisant la commande GET DATA comme indiqué dans [AGD_PRE] au chapitre 3.

1.2.5 *Cycle de vie*

Les deux cycles de vie du produit sont décrits au chapitre 2.2.3 de 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 la configuration incluant :

- 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 « SCR404U », 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 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].

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 :

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 :

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

[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 v5 on SCR404U in PACE configuration with AA and/or CA in option – Security Target,* FQR 110 A0BE, version 4, 7 novembre 2023. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *IDmove v5 on SCR404U in PACE configuration with AA and/or CA in option – Public Security Target,* FQR 110 A0C2, version 6, 21 novembre 2023.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report PLANCK Project,* référence PLANCK_ETR_v1.2, version 1.2, 12 décembre 2023.
[CONF]	Liste de configuration du produit : *PLANCK configuration list*, FQR 110 9439, version 12, 30 novembre 2023.
[GUIDES]	Guide d'installation du produit : - [AGD_PRE] *IDmove v5 on SCR404U Preparative Guidance Document*, FQR 110 A110, version 5, 21 novembre 2023. Guide d'utilisation du produit : - [AGD_OPE] *IDmove v5 on SCR404U MRTD/IDL User Guidance Document,* FQR 110 A111, version 3, 9 novembre 2023. Guide cryptographique : - *PLANCK QR Recommendations for Crypto Assessment Compatibility*, FQR 110 A17E, version 1, 17 octobre 2023.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - IDEMIA2021_GEN_v1.0 ; - IDEMIA-2022_GEN_v1.0 ; - IDEMIA_2023_ALC_GEN_v1.0 ; - [CRB] IDEMIA2022_CRB_STAR_v1.0 ; - [HAA] IDEMIA2021_Haarlem_STAR_v1.0 ; - [MEY] IDEMIA2022_Meyreuil_STAR_v1.0 ; - [NOI-P] IDEMIA_2023_NOI-P_STAR_v1.0 ; - [OST] IDEMIA_2023_OST_STAR_v1.0 ; - [PSC] IDEMIA2022_Pessac _STAR_v1.0 ; - [SZN] IDEMIA_2023_SZN_STAR_v1.0 ; - [VTR] IDEMIA2021_VTR_STAR_v1.1 ; - [USG] USG1-4_STAR_V1.1.
[CER_IC]	Rapport de certification ANSSI-CC-2023/37 SCR404U (version B). Certifié par l'ANSSI sous la référence ANSSI-CC-2023/37.
[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 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.
[PP0090]	*Protection Profile, Machine Readable Electronic Documents - Optionales Nachladen (Optional Post-Emission Updates) [MR.ED-ON-PP]*, version 0.9.2, 18 août 2016. Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) sous la référence BSI-CC-PP-0090-2016.

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.