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-2023/27

CombICAO Applet v3 on ID-One Cosmo X (EAC with PACE Configuration) (SAAAAR : 203742)

Paris, le 21 Juin 2023

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

Emmanuel NAEGELEN

[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-2023/27

Nom du produit

CombICAO Applet v3 on ID-One Cosmo X (EAC with PACE Configuration)

Référence/version du produit

SAAAAR : 203742

Conformité à un profil de protection

Machine Readable Travel Document with "ICAO Application", Extended Access Control
version 1.3.2, BSI-CC-PP-0056-V2-2012-MA02
Machine Readable Travel Document using Standard Inspection Procedure with PACE,
version 1.0.1, BSI-CC-PP-0068-V2-2011-MA-01

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

CEA - LETI
17 avenue des martyrs,
38054 Grenoble Cedex 9, 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 « CombICAO Applet v3 on ID-One Cosmo X (EAC with PACE Configuration), SAAAAR : 203742 » développé par IDEMIA, sur un microcontrôleur développé par INFINEON.

Le produit évalué est de type « carte à puce » pouvant être utilisé en deux 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*. Le produit final peut prendre différentes formes, de carte ou de module.

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 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 décrits dans la cible de sécurité [ST] à la section « *TOE usage and major security features of the TOE* ».

1.2.3 *Architecture*

Le produit est constitué :

- de la plateforme ouverte *JavaCard* « ID-One Cosmo X » embarquée sur un microcontrôleur SLC37 ;
- de l'*applet* « CombICAO Applet v3 » chargée sur cette plateforme.

Il n'y a aucune autre *known applet* au sens de [OPEN].

1.2.4 *Identification du produit*

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

La procédure d'identification est décrite au chapitre 4 du guide AGD_PRE (voir [GUIDES]).
La version certifiée du produit correspond aux valeurs attendues décrites dans la cible de sécurité [ST] au chapitre 1.2 « *TOE Reference* ».

1.2.5 *Cycle de vie*

Le cycle de vie du produit, présenté au chapitre 4 de la cible de sécurité [ST], présente différentes options selon le moment et le lieu de chargement des composants logiciels du produit.

Il est conforme à celui décrit dans [PP0084]. Les rapports des audits de sites effectués dans le schéma français et pouvant être réutilisés, hors certification de site, sont mentionnés dans [SITES].

Les sites de développement et de production du microcontrôleur et de la plateforme sont couverts par [CER_IC] et [CER_PLF].

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

Par ailleurs, les guides [AGD_JC], [AGD_BIO] et [AGD-Dev_Sec] décrivent les règles de développement des applications destinées à être chargées sur cette carte ; le guide [AGD_ALP] décrit les règles de vérification qui doivent être appliquées par l'autorité de vérification.

Pour l'évaluation, l'évaluateur a considéré comme administrateur du produit : le personnaliseur, le gestionnaire de la carte chargé de l'administration de la carte, et comme utilisateur du produit : l'utilisateur du produit final sur le terrain.

1.2.6 *Configuration évaluée*

Le certificat porte sur la configuration avec les mécanismes *Extended Access Control* (EAC) et *Password Authenticated Connection Establishment* (PACE), telle que décrite par la cible de sécurité [ST] (voir en particulier les premiers paragraphes du chapitre 3.2) et les [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 de l'*applet* sur la plateforme déjà certifiée par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation de la plateforme « ID-One Cosmo X » (voir [CER-PLF]).

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.

L'utilisateur doit se référer aux [GUIDES] afin de configurer le produit de manière conforme au référentiel [ANSSI Crypto], pour les mécanismes cryptographiques qui le permettent.

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 1.2du 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 : - *Security Target CombICAO Applet v3 on ID-One Cosmo X (EAC with PACE configuration)*, FQR 550 0224 Ed 8, 28 mars 2023. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *CombICAO Applet v3 on ID-One Cosmo X (EAC with PACE configuration) Public Security Target*, FQR 550 0285 Ed 4, 28 mars 2023.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report* - HYPERION-H, LETI.CESTI.HYPH.FULL.001 - V3.2, 26 mai 2023.
[ANA_CRY]	Cotation des mécanismes cryptographiques HYPERION-N_X, LETI.CESTI.HYPX.RT.001-v1.0, 1 décembre 2021.
[CONF]	*CombICAO Applet V3 Configuration List*, FQR 220 1642 Ed 9, 17 avril 2023.
[GUIDES]	- *CombICAO Applet V3 on ID-One Cosmo X* – AGD_PRE, FQR 220 1640 Ed 4, 11 janvier 2023 ; - *CombICAO Applet V3 on ID-One Cosmo X* – AGD_OPE, FQR 220 1641 Ed 4, 11 janvier 2023 ; - *CombICAO Applet V3, Recommendations for Compatibility with QR*, FQR 220 1646 Ed 1, 1 décembre 2021 ; - [AGD_OPE] *ID-One Cosmo X Reference Guide*, référence FQR 110 9563, version 13, 15/03/2023 ; - [AGD-Dev_Sec] *ID-One Cosmo X on SLC37 Applet Security Recommendations*, référence FQR 110 9572, version 7, 21/03/2023 ; [AGD_JC] *ID-One Cosmo X Java Doc*, référence FQR 110 9616, version 4, 17/01/2022 ; - [AGD_BIO] *BIOMETRY ON ID-ONE COSMOX (SLC 37)*, référence FQR 110 9598, version 2, 02/02/21 ; - [AGD_ALP] *ID-One Cosmo X Application Loading Protection Guidance*, référence FQR 110 9603, version 3, 05/05/2021.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - IDEMIA2022_GEN_v1.0 ; - IDEMIA2021_GEN_v1.0 ; - IDEMIA2020_CRB_STAR_v1.1 ; - [JKT] IDEMIA2021_JKT_STAR_V1.1 ; - [MNL] IDEMIA2020_MNL_STAR_V1.0 ; - IDEMIA2020_Haarlem_STAR_v1.0 ; - IDEMIA2021_NOI-P_STAR_v1.0 ; - IDEMIA2022_Pessac_STAR_v1.0 ; - IDEMIA2021_VTR_STAR_v1.1 ; - IDEMIA-2020_SZN_STAR_v1.0 ; - IDEMIA-2021_OST_STAR_v1.0 ; - IDEMIA2021_NOI-D_STAR_v1.0.

[CER_IC]	*Certification Report BSI-DSZ-CC-1107-V3-2022 for IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh design step T11 with firmware 80.306.16.0 & 80.306.16.1, optional NRG SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib v01.30.0564, optional SCL v2.15.000 and v2.11.003, optional ACL v3.33.003 and v3.02.000, optional RCL v1.10.007, optional HCL v1.13.002 and guidance* Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 16 mai 2022.
[CER-PLF]	Rapport de certification ANSSI-CC-2023/06, ID-One COSMO X (Codes SAAAAR : 093363 + patch 099E71 ; 093364 + patchs 099441 et 099E21 ; 093366).
[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-MA02.
[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.
[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.