



**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-2022/67

ACOS-IDv2.1 eMRTD (A) EAC/PACE Configuration (Version 2.1 eMRTD (A))

Paris, le 15 Décembre 2022

Le Directeur général adjoint de l'Agence
nationale de 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 présumées 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

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification	ANSSI-CC-2022/67	
Nom du produit	ACOS-IDv2.1 eMRTD (A) EAC/PACE Configuration	
Référence/version du produit	Version 2.1 eMRTD (A)	
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 1.0.1 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	EAL 5 augmenté ALC_DVS.2, AVA_VAN.5, ALC_FLR.1	
Développeurs	AUSTRIA CARD PLASTIKKARTEN UND AUSWEISSYSTEME GESELLSCHAFT M.B.H. Lamezanstrasse 4-8, 1230 Vienna, Autriche	INFINEON TECHNOLOGIES AG AIM CC SM PS – Am Campeon 1-12, 85579 Neubiberg, Allemagne
Commanditaire	AUSTRIA CARD PLASTIKKARTEN UND AUSWEISSYSTEME GESELLSCHAFT M.B.H. Lamezanstrasse 4-8, 1230 Vienna, Autriche	
Centre d'évaluation	SERMA SAFETY & SECURITY 14 rue Galilée – CS 10071 33608 PESSAC Cedex – FRANCE	
Accords de reconnaissance applicables	  <p>Ce certificat est reconnu au niveau EAL2 augmenté de FLR.1.</p>	

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.....	6
1.1	Présentation du produit.....	6
1.2	Description du produit.....	6
1.2.1	Introduction	6
1.2.2	Services de sécurité.....	6
1.2.3	Architecture	6
1.2.4	Identification du produit.....	7
1.2.5	Cycle de vie	7
1.2.6	Configuration évaluée	8
2	L'évaluation.....	9
2.1	Référentiels d'évaluation	9
2.2	Travaux d'évaluation	9
2.3	Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI.....	9
2.4	Analyse du générateur d'aléa.....	9
3	La certification	11
3.1	Conclusion.....	11
3.2	Restrictions d'usage	11
3.3	Reconnaissance du certificat.....	12
3.3.1	Reconnaissance européenne (SOG-IS).....	12
3.3.2	Reconnaissance internationale critères communs (CCRA).....	12
ANNEXE A.	Références documentaires du produit évalué	13
ANNEXE B.	Références liées à la certification	15

1 Le produit

1.1 Présentation du produit

Le produit évalué est « ACOS-IDv2.1 eMRTD (A) EAC/PACE Configuration, version 2.1 eMRTD (A) » développé par AUSTRIA CARD PLASTIKKARTEN UND AUSWEISSYSTEME GESELLSCHAFT M.B.H. et INFINEON TECHNOLOGIES AG.

Le produit évalué 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. 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 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 ;
- l'authentification du microcontrôleur par le mécanisme « *Active Authentication* » (AA) ou « *Chip Authentication* » (CA) ;
- l'authentification entre le document de voyage et le système d'inspection lors du contrôle aux frontières par le mécanisme « *Password Authenticated Connection Establishment* » (PACE) ;
- l'authentification entre le microcontrôleur et le système d'inspection lors du contrôle aux frontières par le mécanisme « *Extended Access Control* » (EAC) ;
- la protection, en intégrité et en confidentialité, à l'aide du mécanisme de « *Secure Messaging* », des données lues.

1.2.3 Architecture

Le produit est constitué :

- des microcontrôleurs « IFX_CCI_000005h H13 » (SLC52) et « IFX_CCI_000008h H13 » (SLC32) certifiés sous la référence [CER_IC] ;
- de l'*Operating System* natif « ACOS-IDv2.1 » incluant le code des applications configurées en eMRTD, implémentant les spécifications *Machine Readable Travel Document* (MRTD), avec les fonctionnalités EAC, PACE, CA et AA activées.

Une description plus précise se trouve au 2.4.2 de la cible de sécurité [ST].

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 2.2 « TOE reference » et au chapitre 5 « Identification » du guide [OPE_PRE].

Eléments de configuration		Origine
Nom de la TOE	ACOS-IDv2.1 eMRTD (A) EAC/PACE Configuration	AUSTRIA CARD
Version de la TOE	v2.1 eMRTD (A)	
Build number ¹	'CACD' pour l'IC SLC52GXX448 aa et SLC52GXX348 aa '83CE' pour l'IC SLC32GXX400 aa, SLC32GXX348 aa et SLC32PXX348 aa 'A323' pour l'IC SLC32GXX400 aa, SLC32GXX348 aa et SLC32PXX348 aa	
Réponse à l'ATR	'41 43 4F 53 2D 49 44 76 32 2E 31 20 30' pour 'ACOS-IDv2.1 0' en hexadécimal	

Les commandes nécessaires à la lecture de ces données sont décrites dans le guide du produit, voir [GUIDES].

1.2.5 Cycle de vie

Le cycle de vie du produit est présenté au chapitre 2.4.4 TOE Life-Cycle de la cible de sécurité [ST]. Il est décomposé en quatre phases conformes au profil de protection [PP0084].

Les phases 1 et 2 correspondent au développement du produit, plus précisément au développement du composant et du logiciel embarqué (*firmware*). Les phases 3 et 4 correspondent à la fabrication et au conditionnement (*packaging*) du produit. La phase 5 correspond au chargement du logiciel embarqué (hormis le *firmware* qui est déjà masqué en phase 2 dans le composant. Il est à noter que le point de livraison, ou d'émission de la carte, est en sortie de phase 2.

Les phases 1 à 5 correspondent donc à la construction de la TOE. Elles ont été prises en compte dans la présente évaluation, avec, pour la phase 2, une réutilisation des résultats de l'évaluation du composant. Le composant est développé et fabriqué par INFINEON TECHNOLOGIES AG. Les sites de développement et de fabrication du microcontrôleur sont détaillés dans le rapport de certification [CER_IC].

Le produit a été développé sur le site de Vienne, certifié par *Netherlands scheme for Certification in the Area of IT Security* (NSCIB).

Pour l'évaluation, l'évaluateur a considéré comme :

- administrateur du produit : les agents qui agissent au nom de l'Etat ou de l'organisation émettrice et qui personnalisent le MRTD² avec des données correspondant à l'identité de l'utilisateur ;

¹ XX et aa correspondent à plusieurs options, codés sur 2 *digit*/lettres, toutes combinaisons possibles.

² *Machine readable travel documents*.

- utilisateur du produit : le titulaire légitime du MRTD.

1.2.6 Configuration évaluée

Le certificat porte sur les configurations fermées identifiées au chapitre 1.2.4.

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 des microcontrôleurs « IFX_CCI_000005h H13 » et « IFX_CCI_000008h H13 », voir [CER_IC].

L'évaluation s'appuie sur les résultats d'évaluation des produits « ACOS-IDv2.0 eMRTD (B) EAC/PACE Configuration » certifié en janvier 2022 sous la référence ANSSI-CC-2022/07, voir [CER].

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 [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.

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 1.2 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'accord³, 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 signataires⁴, 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 :



³ La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

⁴ 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]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> - <i>Security Target - ACOS-IDv2.1 eMRTD (A) EAC/PACE Configuration</i>, référence <i>Security Target - ACOS-IDv2.1 eMRTD (A) EAC/PACE Configuration</i>, version 2.11, 23 mai 2022. <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> - <i>Security Target - ACOS-IDv2.1 eMRTD (A) EAC/PACE Configuration</i>, version 2.11 public, 23 mai 2022.
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> - <i>Evaluation Technical Report ACOS-ID Project</i>, référence <i>ACOSv2.1-eMRTD_ETR_v1.2</i>, version 1.2, 9 décembre 2022.
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"> - <i>Configuration_list_REL_ACOS-IDv2.1_01</i>, référence <i>configuration_list_REL_ACOS-IDv2.1_01</i>, version 01, 19 juillet 2022. - <i>Configuration_list_REL_ACOS-IDv2.1_eMRTD_CC-DOC_01</i>, référence <i>configuration_list_REL_ACOS-IDv2.1_eMRTD_CC-DOC_01</i>, version 01, 21 juillet 2022.
[GUIDES]	<p>Guide d'installation et d'administration du produit :</p> <ul style="list-style-type: none"> - <i>Preparation and Operational Manual - ACOS-IDv2.1 eMRTD, BAC and PACE/EAC Configuration</i>, référence <i>ACOS-ID eMRTDv2.0_AGD_PRE_OPE</i>, version 2.02, 23 mai 2022 ; - <i>ACOS-IDv2.0 Internal Operational Manual</i>, référence <i>ACOS-ID eMRTDv2.0_AGD_Internal</i>, version 1.2, 19 juillet 2021. <p>Guide d'utilisation du produit :</p> <ul style="list-style-type: none"> - <i>ACOS-ID User Manual</i>, version 2.13, 23 mars 2022.
[CER_IC]	<p><i>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</i></p> <p>Certifié par le BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>) le 29 avril 2022 sous la référence BSI-DSZ-CC-1110-V5-2022.</p>
[CER]	<p>Rapport de certification ANSSI-CC-2022/07 du produit « ACOS-IDv2.0 eMRTD (B) EAC/PACE Configuration (Version 2.0 eMRTD (B)) », 27 janvier 2022.</p>
[PP0084]	<p><i>Protection Profile, Security IC Platform Protection Profile with Augmentation Packages</i>, version 1.0, 13 janvier 2014.</p> <p>Certifié par le BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>) sous la référence BSI-PP-0084-2014.</p>
[PP EACv2]	<p><i>Protection Profile, Machine Readable Travel Document with "ICAO Application", Extended Access Control</i>, version 1.3.2, 5 décembre 2012.</p> <p>Maintenu par le BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>) sous la référence BSI-CC-PP-0056-V2-2012-MA-02.</p>

[PP PACE]	<p><i>Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE, version 1.0.1, 22 juillet 2014.</i></p> <p>Maintenu par le BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>) sous la référence BSI-CC-PP-0068-V2-2011-MA-01.</p>
-----------	---

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 4.0.
[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]	<i>Common Criteria for Information Technology Security Evaluation:</i> <ul style="list-style-type: none"> - <i>Part 1: Introduction and general model</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001 ; - <i>Part 2: Security functional components</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002 ; - <i>Part 3: Security assurance components</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	<i>Common Methodology for Information Technology Security Evaluation : Evaluation Methodology</i> , avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[JIWG IC] *	<i>Mandatory Technical Document – The Application of CC to Integrated Circuits</i> , version 3.0, février 2009.
[JIWG AP] *	<i>Mandatory Technical Document – Application of attack potential to smartcards and similar devices</i> , version 3.1, juin 2020.
[COMP] *	<i>Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices</i> , version 1.5.1, mai 2018.
[CCRA]	<i>Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security</i> , 2 juillet 2014.
[SOG-IS]	<i>Mutual Recognition Agreement of Information Technology Security Evaluation Certificates</i> , 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.