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-2022/64

ACOS-IDv2.1 SSCD (A) CB-Comm (Version 2.1 SSCD (A))

Paris, le 15 Décembre 2022

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

Emmanuel NAEGELEN

[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

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-2022/64

Nom du produit

ACOS-IDv2.1 SSCD (A) CB-Comm

Référence/version du produit

Version 2.1 SSCD (A)

Conformité à un profil de protection

Protection profiles for secure signature creation device:

Part 2 : Device with key generation, v2.0.1, BSI-CC-PP-0059-2009-MA-02 ;
Part 3 : Device with key import, v1.0.2, BSI-CC-PP-0075-2012-MA-01 ;
Part 4 : Extension for device with key generation and trusted communication with certificate generation application, v1.0.1, BSI-CC-PP-0071-2012-MA-01.

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

CCRA

Ce certificat est reconnu au niveau EAL2 augmenté de FLR.1.

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 « ACOS-IDv2.1 SSCD (A) CB-Comm, Version 2.1 SSCD (A) » développé par AUSTRIA CARD PLASTIKKARTEN UND AUSWEISSYSTEME GESELLSCHAFT M.B.H. et INFINEON TECHNOLOGIES AG.

Ce produit, de type « carte à puce », est destiné à être utilisé comme dispositif sécurisé de création de signature (SSCD[1]). Il peut être utilisé dans différents types de documents (carte d'identité, permis de conduire, carte d'entreprise, passeport, etc.) disposant d'interfaces avec et/ou sans contact.

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 *Protection profiles for Secure Signature Creation Device* [PP-SSCD-Part2], [PP-SSCD-Part3] et [PP-SSCD-Part4].

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont :

- la création de signature ou de sceau électronique dans un environnement où la sécurité repose sur des mesures organisationnelles ;
- la génération des clés de signature (c'est-à-dire la génération de la donnée de création de signature (SCD[2]) et de la donnée de vérification de signature (SVD[3]) associée ;
- l'import des clés de signature (c'est-à-dire de la SCD et, optionnellement, de la SVD associée) ;
- l'export de clé publique (c'est-à-dire la SVD) vers le CGA[4] ;
- l'authentification du signataire par un code PIN ou des données biométriques d'empreintes digitales (*BioPIN*) ;
- l'authentification de l'administrateur (authentification mutuelle) ;
- l'intégrité des conditions d'accès aux données protégées SCD et RAD[5] ;
- l'intégrité des données à signer DTBS[6] ou une unique représentation de ces données (DTBS/R[7]) et la vérification des données d'authentification d'utilisateurs (VAD[8]), optionnellement à travers un canal sécurisé avec SCA[9] ;
- la protection en intégrité et en confidentialité, des données lues à l'aide du mécanisme de « *Secure Messaging*».

[1] *Secure Signature Creation Device.*

[2] *Signature Creation Data.*

[3] *Signature Verification Data.*

[4] *Certification Generation Application.*

[5] *Reference Authentication Data.*

[6] *Data To Be Signed.*

[7] *Unique Representation of DTBS.*

[8] *Verification Authentication Data.*

[9] *Signature Creation Application.*

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 de l'application de création de signature configurée en SSCD, implémentant les spécifications *Secure Signature Creation Device*.

Une description plus précise se trouve au 2.3.3 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 5.1 « *Identification* » du guide [OPE_PRE].

Eléments de configuration		Origine
Nom de la TOE	ACOS-IDv2.1 SSCD (A) CB-Comm	AUSTRIA CARD
Version de la TOE	v2.1 SSSD (A)	
Build number[10]	'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 2.3.4 « *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].

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

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 de la carte ;
- utilisateur du produit : les signataires qui font appel à l'application SSCD pour réaliser une opération de signature.

1.2.6 *Configuration évaluée*

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

L'évaluateur a testé le produit configuré avec les configurations A, B et C définies dans le guide [OPE_PRE], le numéro de *build* étant '8C1D'. Ces résultats s'appliquent également pour les composants « IFX_CCI_000005h H13 » et « IFX_CCI_000008h H13 » (certifiés sous la même référence [CER_IC]).

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 du produit « ACOS-IDv2.0 SSCD (A) CB-Comm » certifié en juin 2022 sous la référence ANSSI-CC-2022/19, 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'accord[11], 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[12] , 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 :

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

[12] 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 - ACOS-IDv2.1 SSCD (A) CB-Comm*, version 2.11, 23 mai 2022. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *Security Target - ACOS-IDv2.1 SSCD (A) CB-Comm*, version 2.11 public, 23 mai 2022.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report ACOS-IDv2.1 SSCD Project*, référence ACOS-IDv2.1_SSCD_ETR_v1.2, version 1.2, 9 décembre 2022.
[CONF]	Liste de configuration du produit : - *Configuration_list_REL_ACOS-IDv2.1_01*, référence configuration_list_REL_ACOS-IDv2.1_01, version 01, 19 juillet 2022. - *Configuration_list_REL_ACOS-IDv2.1_SSCD_CC-DOC_01*, référence configuration_list_REL_ACOS-IDv2.1_SSCD_CC-DOC_01, version 01, 21 juillet 2022.
[GUIDES]	Guide d'installation et d'administration du produit : - *Preparation and Operational Manual - ACOS-IDv2.1 SSCD (A)*, référence ACOS-IDv2.1_SSCD_AGD_PRE_OPE, version 2.02, 23 mai 2022 ; - *ACOS-IDv2.0 Internal Operational Manual*, référence ACOS-ID eMRTDv2.0_AGD_Internal, version 1.2, 19 juillet 2021. Guide d'utilisation du produit : - *ACOS-ID User Manual*, version 2.13, 23 mars 2022.
[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 from Infineon Technologies AG* Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 29 avril 2021 sous la référence BSI-DSZ-CC-1110-V5-2022.
[CER]	Rapport de certification ANSSI-CC-2022/19 du produit « ACOS-IDv2.0 SSCD (A) CB-Comm (v2.0 SSCD (A)) », 7 juin 2022.
[PP-SSCD-Part2]	*Protection profiles for secure signature creation device – Part 2: Device with key generation*, référence : prEN 419211-2:2013, version 2.0.1 datée du 18 mai 2013. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 30 juin 2016 sous la référence BSI-CC-PP-0059-2009-MA-02.
[PP-SSCD-Part3]	*Protection profiles for secure signature creation device – Part 3: Device with key import*, référence : prEN 419211-3:2013, version 1.0.2 datée du 14 septembre 2013. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 30 juin 2016 sous la référence BSI-CC-PP-0075-2012-MA-01.

[PP-SSCD-Part4]	*Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application*, référence : prEN 419211-4:2013, version 1.0.1 datée du 12 octobre 2013. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 30 juin 2016 sous la référence BSI-CC-PP-0071-2012-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.

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]	*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 3.1, juin 2020.
[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.