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-2019/43-R01

Application CPS2ter, adossée à l'application IAS ECC v1.3, en composition sur la plateforme ID-One Cosmo v8.2 (Code SAAAAR Applet : 0708312; Code SAAAAR Patch : 093072)

Paris, le 04 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-2019/43-R01

Nom du produit

Application CPS2ter, adossée à l'application IAS ECC v1.3, en composition sur la plateforme ID-One Cosmo v8.2

Référence/version du produit

Code SAAAAR Applet : 0708312; Code SAAAAR Patch : 093072

Conformité à un profil de protection

Néant

Critère d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL4 augmenté
ALC_DVS.2, AVA_VAN.5

Développeurs

IDEMIA
2 place Samuel de Champlain,
92400 Courbevoie, France

NXP SEMICONDUCTORS GMBH
Troplowitzstrasse 20,
22529 Hamburg, Allemagne

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 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 7
1.2.4 Identification du produit 7
1.2.5 Cycle de vie 7
1.2.6 Configuration évaluée 7
2 L'évaluation 8
2.1 Référentiels d'évaluation 8
2.2 Travaux d'évaluation 8
2.3 Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI 8
2.4 Analyse du générateur d'aléa 9
3 La certification 10
3.1 Conclusion 10
3.2 Restrictions d'usage 10
3.3 Reconnaissance du certificat 11
3.3.1 Reconnaissance européenne (SOG-IS) 11
3.3.2 Reconnaissance internationale critères communs (CCRA) 11
ANNEXE A. Références documentaires du produit évalué 12
ANNEXE B. Références liées à la certification 14

1 Le produit

1.1 Présentation du produit

Le produit évalué est l'« Application CPS2ter, adossée à l'application IAS ECC v1.3, en composition sur la plateforme ID-One Cosmo v8.2, Code SAAAAR Applet : 0708312; Code SAAAAR Patch : 093072 » développé par IDEMIA et masqué sur le composant NXP P60D145 développé par NXP SEMICONDUCTORS GMBH.

Ce produit est une carte à puce disposant d'une interface contact et d'une interface sans contact qui propose les services IAS et CPS2ter sur le même microcontrôleur. Le but est de permettre une transition de la technologie CPS2ter actuellement utilisée par l'Agence des Systèmes d'Information Partagés de Santé (ASIP Santé) vers la technologie CPS3 basée sur le standard IAS.

Ainsi ce produit est destiné à être utilisé comme dispositif de stockage sécurisé de données médicales avec accès à des services distants sensibles. Il est livré en configuration fermée et ne permet pas le chargement d'application en *post-issuance*.

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.

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit et décrits dans [ST] sont :

- l'import de code PIN et de clés ;
- l'authentification via le code PIN de l'utilisateur ;
- l'export de données de l'utilisateur ;
- la génération de nombre aléatoire ;
- la vérification de l'authenticité des commandes entrantes via un cryptogramme, appelée « PRO mode » ;
- l'authentification externe d'entités distantes pour l'accès aux données de l'utilisateur ;
- la personnalisation sécurisée via un canal de confiance.

1.2.3 *Architecture*

Le produit, dont l'architecture est décrite au chapitre 2 de la cible de sécurité [ST], est constitué :

- du microcontrôleur NXP P60D145 certifié sous la référence [CER-IC] ;
- de la plateforme *Java Card* ouverte « ID-One Cosmo V8.2 » .(code SAAAR 091121), surveillée sous la référence [SUR-PTF], avec le *patch* optionnel « R1.0 *Appli Deselection before DESFire* » .(code SAAAR 093072) ;
- de l'application « IAS ECC v2 version 1.3 » en configuration #1, #2, #3 ou #4 (code SAAAR 077234), surveillées sous les références ANSSI-CC-2019/33-S01, ANSSI-CC-2019/34-S01, ANSSI-CC-2019/35-S01 et ANSSI-CC-2019/36-S01 (voir [SUR-IAS]), fonctionnant à travers les interfaces contact et sans contact ;
- de l'application « CPS2ter, version 1.12 » (.code SAAAR 0708312), fonctionnant seulement via l'interface contact, avec le patch « *R2.0 GIP-CPS supporting SCP03* » (code SAAAR 093072.

Tous ces éléments font partie de la cible d'évaluation (TOE[1]).

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 3 « *Identification of the product* » du guide [AGD_PRE].

La version certifiée du produit correspond aux valeurs attendues décrites au chapitre 1.2 « *TOE reference* » de la cible de sécurité [ST].

1.2.5 *Cycle de vie*

Le cycle de vie du produit est décrit au chapitre 2.3 « *TOE product life cycle* » de [ST].

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 le produit tel que décrit au paragraphe 1.2.3.

[1] *Target of Evaluation.*

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 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 la plateforme déjà certifiée par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation de la plateforme « Plateforme ID-One Cosmo v8.2 masquée sur le composant NXP P60D145 » au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5, conforme au profil de protection [PP JCS-O]. Cette plateforme a été certifiée le 19 juillet 2019 sous la référence ANSSI-CC-2019/28 (voir [CER-PTF]).

Le niveau de résistance de cette plateforme a été confirmé le 17 novembre 2022 dans le cadre du processus de surveillance, voir [SUR-PTF].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 2 mai 2023, 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 cryptographique de l'ANSSI [REF], la sortie du générateur physique d'aléas subit un retraitement de nature cryptographique.

Les résultats ont été pris 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 AVA_VAN.5 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[2], 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[3] , 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 SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

[3] 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 CPS2ter Application on* ID-One Cosmo v8.2, référence FQR 110 9044, version 6.0, 07/04/23. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *Security Target Lite CPS2ter Application on ID-One Cosmo v8.2*, référence FQR 110 9201, version 3, 07/04/23.
[RTE]	Rapport technique d'évaluation : - LAKSHMI-R1, Rapport Technique d'Evaluation, référence LETI.CESTI.LAK.ETR.001, version 2.0, 24/04/2023.
[ANA_CRY]	Cotation des mécanismes cryptographiques, référence LAKSHMI, LETI.CESTI.LAK.RT.07, version 1.0, 24/04/2023. .
[CONF]	Liste de configuration du produit : - *LAKSHMI Configuration List*, référence FQR 110 9090, version 3, 07/04/23.
[GUIDES]	Guide d'installation et d'administration du produit : - [AGD_PRE] *GIP-CPS on ID-One Cosmo v8.2 – AGD_PRE – Pre-Personalization Guide*, référence 110 8975, version 3, 03/10/2019. Guide d'utilisation du produit : - *GIP-CPS on ID-One Cosmo v8.2 – AGD_OPE – Reference Guide*, référence FQR 110 8976, version 2, 19/04/23 ; - *CPS3ter Java Applet – SOFTWARE REQUIREMENTS SPECIFICATIONS*, référence 070837 00 SRS, version 7-AA, 31/01/2019 ; - *Optional code R1.0 GIP-CPS suppporting SCP03*, référence FQR 110 9105, version 2, 02/04/2019. Guides d'installation, d'administration et de développement d'applications sécurisées sur la plateforme : - *ID-One Cosmo V8.2 Pre-Perso Guide*, référence FQR 110 8875 version 9, 02/06/2020 ; - *ID-One Cosmo V8.2 Reference Guide*, référence FQR 110 8885, version 8, 02/06/2020 ; - *ID-One Cosmo V8.2 on P60D145 - Applet Security Recommandations*, référence FQR 110 8963, version 4, 18/03/2019 ; - *ID-One Cosmo V8.1-n Application Loading Protection Guidance*, référence FQR 110 8001, version 2, 11/02/2022 ; - *Optional code R1.0 Appli Deselection before DESFire*, référence FQR 110 9106, version 2, 02/04/2019.

[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - IDEMIA2022_GEN_v1.0 ; - IDEMIA2022_CRB_STAR__v1.0 ; - IDEMIA2022_Pessac_STAR_v1.0.
[CER-IC]	*Certification Report for NXP Secure Smart Card Controller P6022y VB* including IC Dedicated Software*, référence BSI-DSZ-CC-1059-V4-2021, 24/06/2021.
[CER-PTF]	Rapport de certification de la « Plateforme ID-One Cosmo v8.2 masquée sur le composant NXP P60D145 », référence ANSSI-CC-2019/28, 19/07/2019.
[SUR-PTF]	Rapport **de** surveillance de la « Plateforme ID-One Cosmo v8.2 masquée sur le composant NXP P60D145 », référence ANSSI-CC-2019/28-S01, 17/11/2022.
[SUR-IAS]	Rapports de surveillance: - « IAS ECC V2, version 1.3 en configuration #1 sur la plateforme ID-One Cosmo v8.2 », référence ANSSI-CC-2019/33-S01, 17/11/2022 ; - « IAS ECC V2, version 1.3 en configuration #2 sur la plateforme ID-One Cosmo v8.2 », référence ANSSI-CC-2019/34-S01, 17/11/2022 ; - « IAS ECC V2, version 1.3 en configuration #3 sur la plateforme ID-One Cosmo v8.2 », référence ANSSI-CC-2019/35-S01, 17/11/2022 ; - « IAS ECC V2, version 1.3 en configuration #4 sur la plateforme ID-One Cosmo v8.2 », référence ANSSI-CC-2019/36-S01, 17/11/2022.
[PP JCS-O]	SUN Java Card System Protection Profile - Open Configuration, version 3.0. Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2010/03- M01.

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 3.0, juillet 2020.
[COMP] *	*Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices*, version 1.5, octobre 2017.
[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.