PREMIER 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-2020/07-R01

Plateforme ID-One Cosmo V9.1 masquée sur le composant IFX SLC32 (Identification du matériel 092915)

Annule et remplace le rapport du 14 avril 2025

Paris, le 09 Mai 2025

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

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 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 Résumé

Référence du rapport de certification **ANSSI-CC-2020/07-R01**
Nom du produit **Plateforme ID-One Cosmo V9.1 masquée sur le composant IFX SLC32**
Référence/version du produit **Identification du matériel 092915**
Type de produit **Cartes à puce et dispositifs similaires**
Conformité à un profil de protection ***Java Card Protection Profile - Open Configuration, version 3.0.5*** certifié BSI-CC-PP-0099-2017 le 21 décembre 2017
Critère d'évaluation et version **Critères Communs version 3.1 révision 5**
Niveau d'évaluation **EAL5 augmenté** ALC_DVS.2, AVA_VAN.5, ALC_FLR.1
Référence du rapport d'évaluation *Evaluation Technical Report (full ETR) – PYRRHA-R01* référence LETI.CESTI.PYR.FULL.001 version 1.6 24 mars 2025.
Fonctionnalité de sécurité du produit voir 2.2.2 Services de sécurité
Exigences de configuration du produit voir 4.2 Restrictions d'usage
Hypothèses liées à l'environnement d'exploitation voir 4.2 Restrictions d'usage
Développeur **IDEMIA** 2 place Samuel de Champlain 92400 Courbevoie, France
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
augmenté de ALC_FLR.1.

SOG-IS

2 Le produit

2.1 Présentation du produit

Le produit évalué est « Plateforme ID-One Cosmo V9.1 masquée sur le composant IFX SLC32, Identification du matériel 092915 » développé par IDEMIA.

Le produit est destiné à héberger et exécuter une ou plusieurs applications, dites applets dans la terminologie *Java Card*. Ces applications peuvent revêtir un caractère sécuritaire différent (selon qu'elles soient « sensibles » ou « basiques ») et peuvent être chargées et instanciées avant ou après émission du produit.

2.2 Description du produit

2.2.1 *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-JCS].

2.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont détaillés dans la cible de sécurité [ST] aux chapitres 1.9 « *Major Security Features of the TOE* » et 8 « *TOE Summary Specification* ». Ils sont résumés ci-après :

- le chargement (avec vérification de signature DAP[1]), l'installation, « l'extradition[2] » et la suppression d'occurrences d'*applets* ou de *packages* par le *Card Manager* ;
- l'identification et l'authentification de l'utilisateur du produit ;
- la protection en confidentialité et en intégrité des données sensibles ;
- l'effacement sécurisé des données sensibles ;
- la mise à jour des données en mémoire persistante à travers un mécanisme de transactions atomiques ;
- des mécanismes de chiffrement, déchiffrement, signature et génération de nombres aléatoires ;
- la gestion des clés ;
- un mécanisme de pare-feu ;
- la gestion des exceptions ;
- la protection du chargement d'applications après émission ;

[1] *Data Authentication Pattern.*

[2] « L'extradition » permet à plusieurs applications de partager un domaine de sécurité dédié.

- l'isolation des applications entre contextes différents et la protection de la confidentialité et de l'intégrité des données applicatives entre les applications.

2.2.3 *Architecture*

Le périmètre d'évaluation *(TOE[3])* est constitué, comme décrit aux chapitres 1.7.1 « *Logical scope of the TOE* » et 1.8 « *TOE Description* » de la cible de sécurité [ST] :

- du microcontrôleur SLC32, développé par INFINEON TECHNOLOGIES AG et certifié sous la référence [CER_IC] ;
- des parties logicielles suivantes, développées par IDEMIA et masquées en FLASH :
  - un système d'exploitation composé :
    - d'une interface entre les composants matériels et les composants natifs, nommée BIOS[4] ;
    - de fonctionnalités cryptographiques ;
    - d'une machine virtuelle *Java (JVM[5])* ;
    - d'un environnement d'exécution *Java Card (JCRE[6])* ;
    - des interfaces de programmation d'application *(API[7])* : *Java Card* et Global Platform ;
  - un *dispatcher* nommé *Resident Application* et chargé de repartir les commandes envoyées à la carte vers les applications et modules correspondants ;
  - un gestionnaire d'applications (*Card Manager*) dont les fonctionnalités sont implémentées dans une *applet* dédiée du même nom ;
- d'un mécanisme de chargement de *patch* appelé JCVMPatch. Les *patches* sont développés et chargés en mémoire *flash* du composant par IDEMIA ;
- une fonctionnalité appelée JBox destiné à embarquer une *Third Party Library* (TPL).

Le produit est aussi composé des éléments hors *TOE* suivants, développés par IDEMIA :

- de potentiels *patchs* logiciels chargés en mémoire *flash* du composant, représentant des mises à jour du produit.

Bien qu'aucune application ne soit pas incluse dans le périmètre de l'évaluation, elles ont été prises en compte dans le processus d'évaluation conformément aux prescriptions de [OPEN]. En effet, les applications qui seront chargées *post*-émission devront être vérifiées conformément aux contraintes de développements d'applications décrites dans la cible de sécurité [ST] au chapitre 1.7.5 « *Applications* ».

[3] *Target Of Evaluation.*

[4] *Basic Input/Output System.*

[5] *Java Virtual Machine.*

[6] *Java Card Runtime Environnement.*

[7] *Application Programming Interface.*

2.2.4 *Identification du produit*

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

La version certifiée du produit est détaillée dans la cible de sécurité [ST] au chapitre 1.2 « *TOE Reference* » et dans [AGD-OPE] aux chapitres 2.1 « *Identification with tag 'DF52'* » et 2.2 « *Identification with tag 'DF50' (mask identification only)* ».

Ces éléments peuvent être vérifiés par l'utilisation de la commande GET DATA ou à la lecture de l'ATR[8]. La procédure d'identification du produit est décrite dans le guide [AGD_OPE].

La principale différence entre le produit et la *TOE* (la plateforme) correspond aux applications chargées pré-émission sur ce produit, et au *patch* optionnel pouvant être installé en pré-personnalisation, personnalisation et en phase d'utilisation.

2.2.5 *Cycle de vie*

Les trois cycles de vie du produit sont décrits au chapitre 1.11 « *Life-Cycle* » de la cible de sécurité [ST] ; ils sont conformes 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]. Suivant les étapes du cycle de vie, différents guides sont applicables, notamment :

- le guide [AGD-OPE] identifie les recommandations relatives à la livraison des futures applications à charger sur ce produit ;
- le guide [AGD-Dev_Sec] décrit les règles de développement des applications destinées à être chargées dans le produit selon leur niveau de sensibilité ;
- 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 « pré-personnalisateur », le « personnalisateur » et le *Card Manager*, et comme utilisateur du produit les développeurs des applications à charger sur la plateforme.

2.2.6 *Configuration évaluée*

Le certificat porte sur la configuration de la plateforme telle qu'elle est identifiée au paragraphe 2.2.4.

La configuration ouverte du produit a été évaluée conformément à [OPEN] : ce produit correspond à une plateforme ouverte cloisonnante. Ainsi tout chargement de nouvelles applications conformes aux contraintes exposées au chapitre 3.2 du présent rapport de certification ne remet pas en cause le présent rapport de certification lorsqu'il est réalisé selon les processus audités.

[8] *Answer To Reset.*

3 L'évaluation

3.1 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 et dispositifs similaires, 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).

3.2 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 « IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h in the design step H13 », 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** ».

3.3 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.

3.4 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.

4 La certification

4.1 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 (voir chapitre 1 Résumé).

Le certificat associé à ce rapport, référencé ANSSI-CC-2020/07-R01, a une date de délivrance identique à la date de signature de ce rapport et a une durée de validité de cinq ans à partir de cette date.

4.2 Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 2.2 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]. Notamment :

- toutes les futures applications chargées sur ce produit (chargement pré-émission et chargement post--émission) doivent respecter les contraintes de développement de la plateforme (guide [AGD-Dev_Sec]) ;
- les autorités de vérification doivent appliquer le guide [AGD-OPE] ;
- la protection du chargement de toutes les futures applications chargées sur ce produit (chargement pré-émission et post-émission) doit être activée conformément aux indications de [AGD_ALP].

4.4 Reconnaissance du certificat

4.4.1 *Reconnaissance européenne (SOG-IS)*

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

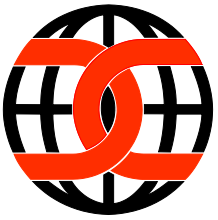
L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[9], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

4.4.2 *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[10] , 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 :



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

[10] 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 ID-One Cosmo v9.1*, référence FQR 110 9246, version 13, 17 décembre 2024. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *Security Target Lite ID-One Cosmo v9.1*, référence FQR 110 9395, version 9, 17 décembre 2024.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report (full ETR) – PYRRHA-R01*, référence LETI.CESTI.PYR.FULL.001, version 1.6, 24 mars 2025. Pour le besoin des évaluations en composition avec ce produit un rapport technique pour la composition a été validé : - *Evaluation Technical Report : ETR for composition - PYRRHA-R01*, référence LETI.CESTI.PYR.COMPO.001, version 1.5, 24 avril 2025.
[ANA_CRY]	Cotation des mécanismes cryptographiques PYRRHA-R01 & DEUCALION-R01, référence LETI.CESTI.DEU.RT.010- V1.0, version 1.0, 21 janvier 2025.
[CONF]	Liste de configuration du produit : - *ID-One Cosmo v9.1 Configuration List*, FQR 110 9295, version 8, 18 décembre 2024.
[GUIDES]	Guide d'installation, d'administration et d'utilisation du produit : - [AGD_PRE] *ID-One Cosmo V9.1 Biometry Pre-Perso Guide*, référence FQR 110 9208, version 9, 1er décembre 2021 ; - *Platform Flash Image Generation*, référence FQR 110 9402, version 1, 27 novembre 2019 ; - *OS Secure Acceptance Process*, référence FQR 110 8921, version 1, 24 septembre 2018 ; - [AGD_OPE] *ID-One Cosmo V9.1 Biometry Reference Guide*, référence FQR 110 9200, 8, 16 mars 2022 ; - *ID-One Cosmo V9.1 platform - Javadoc*, référence FQR 110 9242, version 1 ; - *JCVM_PATCH*, référence FQR 110 8805, version 2, 23 août 2019. Guide de développement d'applications sécurisées : - [AGD-Dev_Sec] *ID-One Cosmo v9.1 Biometry Applet Security Recommandations*, référence FQR 110 9237, version 3, 10 janvier 2022 ; - [AGD_ALP] *ID-One Cosmo v9.1 Biometry Application Loading Protection Guidance*, référence FQR 110 9238, version 1, 9 octobre 2019.

	Guide cryptographique : - *ID-One Cosmo 9.1 and 9.2 Cryptographic Guidance*, référence FQR 110 A3ED, version 1, 6 décembre 2024 ; - *ID-One Cosmo 9.1 and 9.2 Cryptographic French Conformance Guidance*, référence FQR 110 A3E9, version 1, 6 décembre 2024.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - IDEMIA_2024_ALC_GEN_v1.0 ; - IDEMIA2022_CRB_STAR_v1.0 ; - IDEMIA-2024_Haarlem_STAR_v1.0 ; - IDEMIA_2023_NOI-P_STAR_v1.0 ; - IDEMIA2022_Pessac_STAR_v1.0 ; - IDEMIA_2023_VTR_STAR_v1.1 ; - IDEMIA_2024_SZN_STAR_v1.0 ; - IDEMIA_2023-OST_STAR_v1.0 ; - IDEMIA_2023_NOI-D_STAR_v1.0.
[CER_IC]	*Certification Report BSI-DSZ-CC-1110-V7-2024 for Infineon Security Controller IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h in the design step H13 from Infineon Technologies AG*. Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 30 septembre 2024, sous la référence BSI-DSZ-CC-1110- V7-2024.
[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-JCS]	*Java CardProtection Profile - Open Configuration*, version 3.0.5. Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) sous la référence BSI-PP-0099-2017.

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, 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 3.2.1, février 2024.
[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.