



**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-2023/06**

ID-One COSMO X
(Codes SAAAAR : 093363 + patch 099E71;093364 +
patchs 099441 et 099E21;093366)

Paris, le 23 MAI 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 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-2023/06	
Nom du produit	ID-One COSMO X	
Référence/version du produit	Codes SAAAAR : 093363 + patch 099E71;093364 + patches 099441 et 099E21;093366	
Conformité à un profil de protection	Java Card System – Open Configuration Protection Profile, 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	EAL 5 augmenté ADV_TDS.5, ADV_INT.3, ADV_IMP.2, ATE_FUN.2, ATE_COV.3, ALC_CMC.5, ALC_DVS.2, ALC_FLR.1, ALC_TAT.3, 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	  <p>Ce certificat est reconnu au niveau EAL2 augmenté de ALC_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	7
1.2.4	Identification du produit.....	8
1.2.5	Cycle de vie	8
1.2.6	Configuration évaluée	9
2	L'évaluation.....	10
2.1	Référentiels d'évaluation	10
2.2	Travaux d'évaluation	10
2.3	Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI.....	10
2.4	Analyse du générateur d'aléa.....	11
3	La certification	12
3.1	Conclusion.....	12
3.2	Restrictions d'usage	12
3.3	Reconnaissance du certificat.....	13
3.3.1	Reconnaissance européenne (SOG-IS).....	13
3.3.2	Reconnaissance internationale critères communs (CCRA).....	13
ANNEXE A.	Références documentaires du produit évalué	14
ANNEXE B.	Références liées à la certification	16

1 Le produit

1.1 Présentation du produit

Le produit évalué est « ID-One COSMO X, Codes SAAAAR : 093363 + patch 099E71;093364 + patches 099441 et 099E21;093366 » dont le logiciel embarqué est développé par IDEMIA, sur un microcontrôleur développé par INFINEON TECHNOLOGIES AG.

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.

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 au profil de [PP JCS-O].

1.2.2 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 Feature of the TOE » et 8 « TOE Summary Specification ». Ils sont résumés ci-après :

- le chargement (avec vérification de signature DAP¹), l'installation, « l'extradition² » et la suppression d'occurrences d'applets ou de packages par le Card Manager ;
- l'identification et l'authentification de l'utilisateur du produit par le biais d'empreintes numériques (reconnaissance faciale ou empreinte digitale) par l'algorithme biométrique MOC ;
- l'établissement de connexion authentifiée par mot de passe (PACE) ;
- la suppression sécurisée de modules lors de la pré-personnalisation ou de la personnalisation avec le mécanisme FLEXICODE ;
- 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 ;

¹ Data Authentication Pattern.

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

- la protection du chargement d'applications pré-émission et post-émission ;
- l'isolation des applications entre contextes différents et la protection de la confidentialité et de l'intégrité des données applicatives entre les applications.

1.2.3 Architecture

Le périmètre d'évaluation (TOE³) est constitué, comme décrit aux chapitres 1.7 « *Product Architecture* » et 1.8 « *TOE Description* » de [ST] :

- du microcontrôleur SLC37, développé par INFINEON TECHNOLOGIES AG et certifié sous la référence [CER-IC] ;
- des parties logicielles suivantes, développées par IDEMIA et masquées en mémoire *flash* du composant :
 - o un système d'exploitation composé :
 - d'une interface entre les composants matériels et les composants natifs, nommée BIOS⁴ ;
 - de fonctionnalités cryptographiques ;
 - d'une machine virtuelle Java (JVM⁵) ;
 - d'un environnement d'exécution *Java Card* (JCRE⁶) ;
 - des interfaces de programmation d'application (API⁷) : *Java Card* et *Global Platform* ;
 - o un *dispatcher* nommé *Resident Application* et chargé de répartir les commandes envoyées à la carte vers les applications et modules correspondants ;
 - o 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 ou par un tiers ;
- une fonctionnalité appelée *JBox* destinée à embarquer une *Third Party Library* (TPL).

Les éventuels *patches* logiciels autres que ceux mentionnés dans ce rapport de certification, développés par IDEMIA et chargés en mémoire *flash* du composant, correspondants à de futures mises à jour du produit, ainsi que les futures applications chargées sur cette plateforme, sont hors du périmètre de cette évaluation.

Les applications qui seront chargées pré-émission et post-émission devront être vérifiées conformément aux contraintes listées dans la cible de sécurité [ST] au chapitre 1.7.3 « *TOE Guidance* ».

³ Target Of Evaluation.

⁴ Basic Input/Output System.

⁵ Java Virtual Machine.

⁶ Java Card Runtime Environment.

⁷ Application Programming Interface.

1.2.4 Identification du produit

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

Les versions certifiées du produit, *release 3 patchée*, *release 4 patchée* et *release 6*, sont identifiables par les éléments du tableau ci-après, détaillés dans la cible de sécurité [ST] au chapitre 1.2 « *TOE Reference* ».

Éléments de configuration		Origine
Nom de la TOE	ID-One COSMO X	IDEMIA
Identification matérielle du produit (codes SAAAAR)	Release 3 avec un patch : 093363 et 099E71 Release 4 avec deux patches : 093364, 099441 et 099E21 Release 6 : 093366	
Identification de la plateforme	82 01 (numéro & version de masque)	
Identification du composant	49 (pour SLC37)	INFINEON TECHNOLOGIES AG

Ces éléments peuvent être vérifiés par l'utilisation de la commande GET DATA ou à la lecture de l'ATR. 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 qui seront chargées pré-émission et post-émission sur ce produit, et aux *patches* optionnels pouvant être installés en pré-personnalisation, personnalisation et en phase d'utilisation.

1.2.5 Cycle de vie

Les trois cycles de vie évalués du produit sont décrits au chapitre 1.11 « *Life-Cycle* » de la cible de sécurité [ST]. Ils sont décomposés en sept phases conformes au [PP0084].

	Phase	Acteur	Couvert par
Phase 1	Développement de la plateforme	IDEMIA	ALC
Phase 2	Développement du microcontrôleur	INFINEON TECHNOLOGIES AG	ALC
Phase 3	Fabrication du microcontrôleur	INFINEON TECHNOLOGIES AG	ALC
Phase 4	Conditionnement (<i>packaging</i>) du produit	IDEMIA	AGD_PRE
Phase 5	Pré-Personnalisation	IDEMIA	AGD_PRE
Phase 6	Personnalisation	Personnalisateur	AGD_PRE
Phase 7	Utilisation opérationnelle	Utilisateur final	AGD_OPE

Dans les deux premiers cycles de vie (voir Table 2 de [ST]), la livraison de la TOE s'opère à la fin de la phase 3. Après cette phase, la TOE est considérée comme auto-protégée.

Dans le troisième cycle de vie (voir Table 3 de [ST]), la livraison de la TOE s'opère à la fin de la phase 5. Après cette phase, la TOE est considérée comme auto-protégée.

Le produit a été développé sur les sites suivants (voir [SITES]) :

IDEMIA – Courbevoie [CRB] 2, place Samuel de Champlain 92400 Courbevoie, France	IDEMIA – Pessac [PSC] Bâtiment Elnath, 11 avenue de Canteranne, 33600 Pessac, France
IDEMIA – Vitré [VTR] Avenue d'Helmstedt BP 90308 35503 Vitré Cedex, France	IDEMIA – Shenzhen [SZN] 4F, Great wall technology building No 2, Kefa Rd Science and technology park, Nanshan district, Shenzhen, 518057, PR of China
IDEMIA – Haarlem [HAA] Oudeweg 32, 2031 CC Haarlem, The Netherlands	IDEMIA – Noida [NOI-D] Syscom India Private Limited PLOT-1A, sector 73, Noida Uttar Pradesh 201307, India
IDEMIA – Ostrava [OST] Jelinkova 1174/3A, 721 00 Ostrava-Svinov, Czech Republic	IDEMIA – Noida [NOI-P] Syscom India Private Limited Plot No 60-61, NSEZ, Phase II, Dadri Road, Noida-201305 Uttar Pradesh India

Les sites de développement et de fabrication du microcontrôleur sont couverts par le certificat [CER-IC].

Le produit permet le chargement d'applications en phase 3 (avant le point de livraison), en phase 5 (pré-émission) ou en phase 6 et 7 (post-émission).

Le guide [AGD-OPE] identifie les recommandations relatives à la livraison des futures applications à charger sur ce produit.

Par ailleurs, les guides [AGD-Dev_Sec], [AGD_JC] et [AGD_BIO] 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 « prépersonnalisateur », le « personnalisateur » et le *Card Manager*, et comme utilisateur du produit les développeurs des applications à charger sur la plateforme.

1.2.6 Configuration évaluée

Le certificat porte sur la configuration de la plateforme telle qu'elle est identifiée au paragraphe 1.2.4.

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.

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 du microcontrôleur « *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* », 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** ».

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 potentiel d'attaque 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 potentiel d'attaque 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], notamment :

- toutes les futures applications chargées sur ce produit (chargement pré-émission et post-émission) doivent respecter les contraintes de développement de la plateforme (guides [AGD_JC], [AGD_BIO] et [AGD-Dev_Sec]) selon la sensibilité de l'application considérée ;
- 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].

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'accord⁸, 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 signataires⁹, 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 :



⁸ La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

⁹ 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 ID-ONE COSMO X</i>, référence FQR 110 9792, version 4, 23/03/2023. <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 Lite ID-ONE COSMO X</i>, référence FQR 110 A19A, version 2, 23/03/2023.
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none">- <i>Evaluation Technical Report – HERA</i>, référence LETI.CESTI.HER.FULL.001, version 1.4, 19/04/2023. <p>Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé :</p> <ul style="list-style-type: none">- <i>Evaluation Technical Report (ETR for composition) – HERA</i>, référence LETI.CESTI.HER.COMPO.001, version 1.4, 19/04/2023.
[ANA_CRY]	<p>Cotation des mécanismes cryptographiques ZEUS, référence LETI.CESTI.ZEU.RT.009 – V2.3, version 2.3, 21/06/2021.</p>
[CONF]	<p>Liste de configuration du produit : <i>Id-One Cosmo X Configuration List</i>, référence FQR 110 9619, version 11, 21/03/2023.</p>
[GUIDES]	<p>Guides d'installation, d'administration et d'utilisation du produit :</p> <ul style="list-style-type: none">- [AGD_PRE] <i>ID-One Cosmo X Pre-Perso Guide</i>, référence FQR 110 9562, version 13, 15/03/2023 ;- <i>JBox Software Configuration</i>, référence FQR 110 9273, version 2, 26/01/2021 ;- <i>Platform Flash Image Generation</i>, référence FQR 110 9402, version 1, 27/11/2019 ;- <i>JCVM PATCH</i>, référence FQR 110 8805, version 4, 23/12/2020 ;- [AGD_OPE] <i>ID-One Cosmo X Reference Guide</i>, référence FQR 110 9563, version 13, 15/03/2023 ;- <i>SECURE ACCEPTANCE PROCESS</i>, référence FQR 110 8921, version 1, 24/09/2018 ;- <i>GLOBAL PRIVACY FRAMEWORK</i>, référence FQR 110 9567, version 3, 25/11/2021. <p>Guides de développement des applications :</p> <ul style="list-style-type: none">- [AGD_ALP] <i>ID-One Cosmo X Application Loading Protection Guidance</i>, référence FQR 110 9603, version 3, 05/05/2021 ;- [AGD-Dev_Sec] <i>ID-One Cosmo X on SLC37 Applet Security Recommendations</i>, référence FQR 110 9572, version 7, 21/03/2023 ;- [AGD_JC] <i>ID-One Cosmo X Java Doc</i>, référence FQR 110 9616, version 4, 17/01/2022 ;- [AGD_BIO] <i>BIOMETRY ON ID-ONE COSMOX (SLC 37)</i>, référence FQR 110 9598, version 2, 02/02/21.

	<p>Guide cryptographique : <i>ID-One Cosmo X Cryptographic French Conformance Guidance</i>, référence FQR 110 9745, version 7, 21/03/2023.</p>
[SITES]	<p>Rapports d'analyse documentaire et d'audit de site pour la réutilisation :</p> <ul style="list-style-type: none"> - IDEMIA2022_GEN_v1.0 ; - IDEMIA2021_GEN_v1.0 ; - IDEMIA2020_CRB_STAR_v1.1 ; - 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]	<p><i>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</i> Certifié par le BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>) le 16 mai 2022.</p>
[PP JCS-O]	<p><i>Java Card System Protection Profile - Open Configuration</i>, version 3.0.5, 21 décembre 2017. Certifié par le BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>) sous la référence BSI-CC-PP-0099-2017.</p>
[PP0084]	<p><i>Protection Profile, Security IC Platform Protection Profile with Augmentation Packages</i>, version 1.0, 13 janvier 2014. Certifié par le BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>) sous la référence BSI-PP-0084-2014.</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 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.
[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 3.2, novembre 2022.
[COMP] *	<i>Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices</i> , version 1.5.1, mai 2018.
[OPEN]	<i>Certification of « Open » smart card products</i> , version 1.1 (for trial use), 4 février 2013.
[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.