Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2020/08

Plateforme ID-One Cosmo V9.2 masquée sur le composant IFX SLC52 Identification du matériel 093772

Paris, le 9 avril 2020

Le directeur général de l'agence nationale de la sécurité des systèmes d'information

Guillaume POUPARD
[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-2020/08

Nom du produit

Plateforme ID-One Cosmo V9.2 masquée sur le composant IFX SLC52

Référence/version du produit

Identification du matériel : 093772

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

Critères d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, 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

CCRA

SOG-IS

Ce certificat est reconnu au niveau EAL2.

Préface

La certification

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 matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est « Plateforme ID-One Cosmo V9.2 masquée sur le composant IFX SLC52, Identification du matériel 093772 ». Elle est développée par *IDEMIA* et embarquée sur le microcontrôleur développé et fabriqué par *INFINEON TECHNOLOGIES AG*.

Ce produit est une plateforme ouverte *Java Card* conforme à la spécification émise par *Global Platform*, contact et/ou sans contact, destinée à accueillir les *applets* de l'utilisateur pré-émission et/ou post-émission, et à leur fournir les services de sécurité détaillés dans la cible de sécurité [ST].

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 protection [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 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 *post-issuance* ;
- l'isolation des applications entre contextes différents et la protection de la confidentialité et de l'intégrité des données applicatives entre les applications.

1*Data Authentication Pattern.*
2« L'extradition » permet à plusieurs applications de partager un domaine de sécurité dédié.

1.2.3. Architecture

Le périmètre d'évaluation (TOE[3]) est constitué, comme décrit aux chapitres 1.7.1 et 1.8 de [ST]) :

- du microcontrôleur SLC52, 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 :
    - 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 nouvelle 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-issuance* devront être vérifiées conformément aux contraintes de développements d'applications décrites dans la cible de sécurité [ST] au chapitre 1.7.5.

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 [ST] aux chapitres 1.2 « *TOE Reference* » et dans [AGD-OPE] aux annexes B.1 et B.2.

3 *Target Of Evaluation.*
4 *Basic Input/Output System.*
5 *Java Virtual Machine.*
6 *Java Card Runtime Environnement.*
7 *Application Programming Interface.*

Eléments de configuration		Origine
Nom de la TOE	ID-ONE COSMO V9.2	*IDEMIA*
Identification matérielle du produit	09 37 72 (code SAAAAR) 09 02 00 00 00 00 (version commerciale)	
Identification de la plateforme	5B 02 (numéro & version de masque)	
Identification du composant	13 (pour SLC52)	*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].

Par exemple :

- l'identification du produit « 09 37 72 » peut être lue dans la réponse ATR « 3B DB 96 00 80 B1 FE 45 1F 83 00 31 C1 64 **09 37 72** 13 00 90 00 » ;
- les données d'identification du composant « 13 » et de la plateforme « 5B 02 » peuvent être lues dans la réponse à la commande GET DATA avec le tag « DF 52 » (*subTag* « 01 » pour le composant et « 03 » pour la plateforme).

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.

1.2.5. Cycle de vie

Les trois cycles de vie du produit sont décrits au chapitre 1.11 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 (*packaging*) 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, elle 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, elle 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-P] 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	

Le microcontrôleur est développé et fabriqué par *INFINEON TECHNOLOGIES AG*. Les sites de développement et de fabrication de ce microcontrôleur sont détaillés dans le rapport de certification [CER-IC].

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.

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 version 3.1 révision 5** [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 le microcontrôleur déjà certifié par ailleurs.
Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur « Infineon Security Controller IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h H13 including the products from the second production line and optional software packages: Flash Loader, Asymmetric Crypto Library, Symmetric Cryptographic Library, Hardware Support Layer, Hash Crypto Library, Mifare Compatible Software, and CIPURSE Crypto Library » au niveau EAL6 augmenté du composant ALC.FLR.1, conforme au profil de protection [PP0084]. Ce microcontrôleur a été certifié le 18 juin 2019 sous la référence BSI-DSZ-CC-1110-V2-2019, voir [CER_IC].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 13 mars 2020, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques selon le référentiel technique de l'ANSSI [REF] n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilité de conception et de construction pour le niveau AVA_VAN.5 visé.

2.4. Analyse du générateur d'aléas

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 « Plateforme ID-One Cosmo V9.2 masquée sur le composant IFX SLC52, Identification du matériel 093772 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation des composants ALC_DVS.2 et AVA_VAN.5.

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 *post-issuance*) doivent respecter les contraintes de développement de la plateforme (guides [AGD-Dev_Sec]) selon la sensibilité de l'application considérées ;
- les autorités de vérification doivent appliquer le guide [AGD-OPE] ;
- la protection du chargement de toutes les futures applications chargées sur ce produit (chargement *post-issuance*) 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'accord[8], 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 [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[9], 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 :

8La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.
9La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 5+	Intitulé du composant
ADV Développement	ADV_ARC		1	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	**5**	Complete semi-formal functional specification with additional error information
	ADV_IMP				1	1	2	2	**1**	Implementation representation of the TSF
	ADV_INT					2	3	3	**2**	Well-structured internals
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	**4**	Semiformal modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	**1**	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	1	2	3	4	4	5	5	**4**	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	**5**	Development tools CM coverage
	ALC_DEL		1	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			1	1	1	2	2	**2**	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD			1	1	1	1	2	**1**	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	**2**	Compliance with implementation standards
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	**1**	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	**1**	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	**2**	Analysis of coverage
	ATE_DPT			1	1	3	3	4	**3**	Testing: modular design
	ATE_FUN		1	1	1	1	2	2	**1**	Functional testing
	ATE_IND	1	2	2	2	2	2	3	**2**	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	**5**	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Security Target ID-One COSMO v9.2, référence FQR 110 9277, version 6, 10/02/2020, *IDEMIA*. 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 V9.2, référence FQR 110 9443, version 4, 10/02/2020, *IDEMIA*.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report – DEUCALION, référence LETI.CESTI.DEU.FULL.001, version 1.3, 13/03/2020, *CEA-LETI*.
[CONF]	Liste de configuration du produit : - ID-One Cosmo v9.2 Configuration List, FQR 110 9296, version 5, 11/02/2020, *IDEMIA*.
[GUIDES]	Guide d'installation, d'administration et d'utilisation du produit : - [AGD_PRE] ID-One Cosmo V9.2 Pre-Perso Guide, référence FQR 110 9289 version 3, 27/01/2020, *IDEMIA* ; - Platform Flash Image Generation, référence FQR 110 9402 version 1, 27/11/2019, *IDEMIA* ; - OS Secure Acceptance Process, référence FQR 110 8921, version 1, 24/09/2018, *IDEMIA* ; - [AGD_OPE] ID-One Cosmo V9.2 Reference Guide, référence FQR 110 9290, version 3, 27/01/2020, *IDEMIA* ; - JCVM_PATCH, référence FQR 110 8805, version 2, 23/08/2019, *IDEMIA* ; - ID-One Cosmo V9.2 - Javadoc, référence FQR 110 9299, version 1, *IDEMIA* ; - JBox SW Configuration, référence FQR 110 9273, version 1, 17/07/19, *IDEMIA*. Guide de développement d'applications sécurisées : - [AGD-Dev_Sec] ID-One Cosmo v9.2 Applet Security Recommandations, référence FQR 110 9291, version 2, 13/01/2020, *IDEMIA* ; - [AGD_ALP] ID-One Cosmo v9.2 Application Loading Protection Guidance, référence FQR 110 9292, version 1, 31/07/2019, *IDEMIA*.

[SITES]	Rapports d'analyse documentaire : - IDEMIA Development Environment ALC Class Evaluation Report (Generic Documentary activities), référence IDEMIA R&D site 2018_GEN_v1.1, 19/06/2019, *SERMA SAFETY & SECURITY ;* - IDEMIA Haarlem Development Environment - ALC Class Evaluation Report (Generic Documentary activities), référence SITE_IDEMIA_HAARLEM_ALC_GEN_v1.0, 24/08/2019, *SERMA SAFETY & SECURITY ;* - IDEMIA Development Environment - ALC Class Evaluation Report (Generic Documentary activities), référence IDEMIA-2019_GEN_v1.0, 24/04/2019, *SERMA SAFETY & SECURITY* ; - IDEMIA Development Environment - ALC Class Evaluation Report (Generic Documentary activities), référence IDEMIA-2019_GEN_v1.1, 1/07/2019, *SERMA SAFETY & SECURITY*. Rapports d'audit de site pour la réutilisation : - [CRB] Site Technical Audit Report CRB, référence IDEMIA R&D site 2018_CRB_STAR_v1.3, 26/06/2019, *SERMA SAFETY & SECURITY* ; - [HAA] Site Technical Audit Report IDEMIA Haarlem, référence SITE_IDEMIA_HAARLEM_STAR_v1.1, 03/01/2019, *SERMA SAFETY & SECURITY* ; - [PSC] Site Technical Audit Report PSC, référence IDEMIA R&D site 2018_PSC_STAR_v1.2, 18/12/2019, *SERMA SAFETY & SECURITY* ; - [VTR] Site Technical Audit Report IDEMIA Vitré, référence IDEMIA-2019_VTR_STAR_v1.1, 8/01/2020, *SERMA SAFETY & SECURITY* ; - [SZN] Site Technical Audit Report IDEMIA Shenzhen, référence IDEMIA-2019_SZN_STAR_v1.0, 08/11/2019, *SERMA SAFETY & SECURITY* ; - [OST] Site Technical Audit Report OST, référence IDEMIA-2019_OST_STAR_v1.0, 24/06/2019, *SERMA SAFETY & SECURITY* ; - [NOI] Site Technical Audit Report 2019 NOI-P, référence IDEMIA-2019_NOIP_STAR_v1.1, 17/07/2019, *SERMA SAFETY & SECURITY*.

[CER-IC]	Certification Report BSI-DSZ-CC-1110-V2-2019 for Infineon Security Controller IFX_CCI_000003h,000005h, 000008h, 00000Ch, 000013h, 000014h,000015h, 00001Ch, 00001Dh, 000021h, 000022h H13 including the products from the second production line and optional software packages: Flash Loader, Asymmetric Crypto Library, Symmetric Cryptographic Library, Hardware Support Layer, Hash Crypto Library, Mifare Compatible Software, and CIPURSE™ Crypto Library. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 18 juin 2019, sous la référence BSI-DSZ-CC-1110-V2-2019*.
[PP JCS-O]	Java Card System Protection Profile - Open Configuration, version 3.0.5, Décembre 2017. *Certifié par l'ANSSI sous la référence ANSSI-CC-PP-0099-2017*.
[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 3. 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]	Procédure ANSSI-CC-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, ANSSI.
[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, version 3.0, avril 2019.
[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.
[CC RA]	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.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.

*Document du SOG-IS ; dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.