PREMIÈRE MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2022/34v2

ID-One Cosmo X embedding VITALE application (version 2.1.5)

Paris, le 19 Avril 2023

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

Emmanuel NAEGELEN

[ORIGINAL SIGNE]

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

AVERTISSEMENT

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2022/34v2

Nom du produit

ID-One Cosmo X embedding VITALE application

Référence/version du produit

version 2.1.5

Conformité à un profil de protection

Protection profiles for secure signature creation device:

Part 2 : Device with key generation, v2.01, BSI-CC-PP-0059-2009-MA-02 ;
Part 3 : Device with key import, v1.0.2, BSI-CC-PP-0075-2012-MA-01 ;
Part 4 : Extension for device with key generation and trusted communication with certificate generation application, v1.0.1, BSI-CC-PP-0071-2012-MA-01 ;
Part 5 : Extension for device with key generation and trusted communication with signature creation application, v1.0.1, BSI-CC-PP-0072-2012-MA-01 ;
Part 6 : Extension for device with key import and trusted communication with signature creation application, v1.0.4, BSI-CC-PP-0076-2013-MA-01.

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

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

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 7
1.2.3 Architecture 8
1.2.4 Identification du produit 8
1.2.5 Cycle de vie 9
1.2.6 Configuration évaluée 10
2 L'évaluation 11
2.1 Référentiels d'évaluation 11
2.2 Travaux d'évaluation 11
2.3 Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI 12
2.4 Analyse du générateur d'aléa 12
3 La certification 13
3.1 Conclusion 13
3.2 Restrictions d'usage 13
3.3 Reconnaissance du certificat 13
3.3.1 Reconnaissance européenne (SOG-IS) 13
3.3.2 Reconnaissance internationale critères communs (CCRA) 14
ANNEXE A. Références documentaires du produit évalué 15
ANNEXE B. Références liées à la certification 17

1 Le produit

1.1 Présentation du produit

Le produit évalué est « ID-One Cosmo X embedding VITALE application, version 2.1.5 » dont le logiciel embarqué est développé par IDEMIA, sur un microcontrôleur développé par INFINEON TECHNOLOGIES AG.
Ce produit offre des services de signature électronique (SSCD[1]) au travers des applications ADELE, VITALE1 et VITALE2, conformes aux profils de protection listés dans le paragraphe 1.2.1 ci-dessous.

Ce produit est destiné à être utilisé dans le cadre de l'application SESAM Vitale ainsi que pour des applications de signature électronique ; il est livré en configuration fermée et ne permet pas le chargement d'application en post-émission.

1.2 Description du produit

1.2.1 *Introduction*

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

Cette cible de sécurité est strictement conforme aux profils de protection [PP-SSCD-Part2], [PP-SSCD-Part3], [PP-SSCD-Part4], [PP-SSCD-Part5] et [PP-SSCD-Part6].

Cette certification correspond à une évaluation avec réduction de portée (voir [NOTE25]). Ici la réduction de portée correspond à la restriction de certaines et valeurs de PIN du périmètre d'évaluation. Les évolutions concernent ainsi essentiellement les guides du produit (voir [GUIDES]).

[1] *Secure Signature Creation Device.*

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont :

- la création de signature ou de sceau électronique ;
- la génération des clés de signature (c'est-à-dire la génération de la donnée de création de signature (SCD[2]) et de la donnée de vérification de signature (SVD[3]) associée) ;
- l'import des clés de signature (c'est-à-dire de la SCD et, optionnellement, de la SVD associée) ;
- l'export de clé publique (c'est-à-dire la SVD) ;
- l'établissement d'un canal de confiance pouvant permettre la création de signature électronique, l'import de la SCD ou l'export de la SVD dans un environnement non protégé ;
- l'authentification du porteur de carte basée sur la vérification d'un code PIN appelée également données d'authentification de référence (RAD[4]) ;
- le déblocage de la RAD.

De plus, le produit fournis aussi les mécanismes de sécurité décrits au chapitre 3.6 de la cible de sécurité [ST], à savoir :

- les mécanismes d'authentification (authentification du porteur de la carte, du mécanisme communiquant avec la carte afin d'établir un canal sécurisé, de l'administrateur de la TOE, authentification mutuelle avec l'entité communicante et authentification client/serveur) ;
- la cryptographie (génération de clés SCD/SVD ou de session, destruction de clés, authentification symétrique et asymétrique, création de signature, génération de nombres aléatoires, chiffrement/déchiffrement de message émis, génération et vérification de MAC, calcul de hash, calcul et vérification de certificat, chiffrement/déchiffrement de données) ;
- la gestion de clés (importation de SCD, génération de SCD, désactivation de SCD, création, extension ou modification de certificat, création de SVD, gestion des clés d'authentification) ;
- la gestion de PIN ;
- la gestion de canaux sécurisés ;
- le contrôle d'accès aux différentes données de l'*applet* ;
- le stockage des données ;
- l'intégrité et la confidentialité des données sensibles.

Les principaux services de sécurité de la plateforme sont décrits dans [CER-PTF].

[2] *Signature Creation Data*.

[3] *Signature Verification Data*.

[4] *Reference Authentication Data*.

1.2.3 *Architecture*

Le produit, dont l'architecture est détaillée aux chapitres 1 « *Introduction* » et 3 « *TOE Overview* » de la cible de sécurité [ST], est constitué :

- du microcontrôleur SLC37 ;
- de la plateforme *Java Card* ouverte « ID-One Cosmo X » ;
- de l'*applet* de signature VITALE composée des applications ADELE, VITALE1 et VITALE2 contenant entre autres les fonctionnalités SSCD[5] ;
- d'une application AIP (Application d'Initialisation et de Personnalisation), application d'administration utilisée en phase de pré-personnalisation et de personnalisation qui est inactive en phase « utilisation » ;
- d'un gestionnaire d'applications.

Parmi ces éléments, l'application AIP et le gestionnaire d'applications ne font pas partie de la cible d'évaluation (TOE[6]).

1.2.4 *Identification du produit*

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

La version certifiée du produit est identifiable par les éléments du tableau ci-après, détaillés dans la cible de sécurité [ST] au chapitre 1.2 « *TOE Reference* » et dans le guide [AGD_OPE] au chapitre 2 « Identification du produit ».

Eléments de configuration		Origine
Nom de la TOE	ID-One Cosmo X embedding VITALE application	IDEMIA
Identification de l'application VITALE	« 56 49 » (identifiant de l'applet) « 22 06 » (date de version de l'applet) « 21 05 » (version de l'applet en BCD) « 097523 » (SAAAAR code)	
Identification de la plateforme : ID-One Cosmo X	« 093364 » (SAAAAR code)	
Identification du microcontrôleur: SLC37	« 48 30 » (fondeur) « 49 15 » (type de composant)	INFINEON TECHNOLOGIES AG

Ces éléments peuvent être vérifiés par lecture des données CPLC de l'applet VITALE et de la plateforme, suivant la procédure d'identification décrite dans le guide [AGD_OPE] (voir [GUIDES]).

[5] *Secure Signature Creation Device.*

[6] *Target of Evaluation.*

1.2.5 *Cycle de vie*

Le cycle de vie du produit est décrit au chapitre 4 de la cible de sécurité [ST]. Il est décomposé en sept phases conformes au [PP0084] et présente 3 options selon le moment et le lieu de chargement des composants logiciels du produit :

- option 1 : plateforme et application sont chargées sur les sites INFINEON TECHNOLOGIES AG audités dans le cadre de [CER-IC] en phases 3 et 4 ;
- option 2 : la plateforme est chargée sur les sites audités dans le cadre de [CER-IC] et l'application sur les sites IDEMIA de Vitré et Noïda-P ;
- option 3 : plateforme et application sont chargées sur les sites IDEMIA de Vitré et Noïda-P.

Ce cycle de vie est résumé dans le tableau suivant :

Phase	Rôle	Sites ou acteurs	Couvert par
1	Développement du logiciel embarqué	IDEMIA Courbevoie et Pessac Sites audités dans le cadre de [CER-PTF]	ALC
2	Développement du microcontrôleur	Sites audités dans le cadre de [CER-IC]	ALC
3	Fabrication du microcontrôleur et *packaging*	Voir options	ALC
4	Chargement du logiciel	Voir options	ALC
Point de livraison de la TOE			
5	Pré-personnalisation	Agent de fabrication	AGD_PRE
6	Personnalisation	Agent personnalisateur	AGD_PRE
7	Utilisation	Administrateur ou signataire	AGD_OPE

Le point de livraison de la TOE se situe en sortie de phase 4. 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 – Noida [NOI-P] Syscom India Private Limited Plot No 60-61, NSEZ, Phase II, Dadri Road, Noida-201305 Uttar Pradesh, India	**IDEMIA – Vitré [VTR]** Avenue d'Helmstedt BP 90308 35503 Vitré Cedex, France

Les sites de développement et de production du microcontrôleur et de la plateforme sont couverts par [CER-IC] et [CER-PTF].

Pour l'évaluation, l'évaluateur a considéré comme :

- administrateur du produit : les agents qui agissent au nom de l'Etat ou de l'organisation émettrice et qui personnalisent la carte avec des données de l'utilisateur final ;
- utilisateur du produit : le titulaire légitime de la carte.

NB : Dans le cadre particulier de cette certification, qui correspond à une évaluation avec réduction de portée, la validité des audits n'a pas été vérifiée.

1.2.6 *Configuration évaluée*

Le certificat porte sur la configuration identifiée au chapitre 1.2.4 du présent rapport.

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 s'appuie sur les résultats d'évaluation de ce même produit certifié le 23 Décembre 2022 sous la référence ANSSI-CC-2022/34, voir [CER]. Elle correspond à une évaluation avec réduction de portée suite à l'identification de vulnérabilité et prend en compte les travaux de réduction de portée de la plateforme [CER-PLF-D].

L'analyse de vulnérabilité de cette version du produit au regard des nouvelles attaques apparues depuis l'émission du certificat [CER] n'a pas été conduite dans le cadre de cette réévaluation partielle. Le niveau de résistance d'un produit certifié se dégrade au cours du temps. Seule une réévaluation ou une surveillance de cette version du produit permettrait de maintenir le niveau de confiance dans le temps.

Le CESTI en charge de l'évaluation initiale a émis un rapport d'analyse de réduction de portée (référence [RTE_part]) pour réévaluer les composants d'assurance impactés par l'évolution de la cible de sécurité du produit.

Le rapport technique d'analyse de réduction de portée [RTE_part], remis à l'ANSSI le 3 avril 2023, pour réévaluer les composants d'assurance ASE, ADV, ALC (hors audits), et ATE impactés par l'évolution de la cible de sécurité [ST] détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

Le rapport technique [RTE_init], remis à l'ANSSI le 9 décembre 2022 détaille les travaux initialement réalisés menés par le centre d'évaluation et atteste que la résistance du produit atteignait VAN.5 lors de son édition.

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 [ANSSI Crypto], la sortie du générateur physique d'aléa subit un retraitement de nature cryptographique.

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

3 La certification

3.1 Conclusion

Ce certificat atteste que le produit soumis à l'évaluation conformément à [NOTE25], répond aux caractéristiques de sécurité spécifiées dans la cible de sécurité [ST] pour le niveau d'évaluation visé à la date de certification initiale (voir [CER]). Pour rappel, les travaux d'analyse de la réduction de portée sont centrés sur l'impact de cette réduction de portée sur les tâches de conformité de l'évaluation initiale. La résistance globale du produit aux attaques de l'état de l'art n'a pas été mise à jour depuis la certification initiale.

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 le chapitre 8 du guide [AGD_PRE].

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[7], 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 :

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

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[8] , 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 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 X embedding VITALE application*, référence FQR 110 9935, version 4, 07/03/2023. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *Public Security Target ID-One Cosmo X embedding VITALE application*, référence FQR 110 9936, version 4, 07/03/2023.
[RTE_init]	Rapport technique d'évaluation : - *Evaluation Technical report THERIA-X, référence LETI.CESTI.THX.FULL.001, version 1.1, 09/12/2022.*
[RTE_part]	Rapport technique d'évaluation : - *Evaluation Technical report THERIA-X*, référence LETI.CESTI.THX.FULL.001, version 2.0, 03/04/2023.
[ANA_CRY]	Cotation des mécanismes cryptographiques THERIA-X, référence LETI.CESTI.THX.RT.002, version v1.0, 30/09/2022.
[CONF]	Liste de configuration du produit : *Vitale2 on Cosmo X Configuration List*, référence FQR 110 A137, version 5, 29/03/2023.
[GUIDES]	Guide d'installation et d'administration du produit : - [AGD_PRE] Manuel de Pré-Personnalisation - Personnalisation, référence FQR 110 9916, version 3, 03/03/2023. Guide d'utilisation du produit : - [AGD_OPE] Manuel utilisateur VITALE2 applet COSMO X, référence FQR 110 9917, version 2, 03/03/2023.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - IDEMIA2020_GEN_v1.0 ; - IDEMIA2021_GEN_v1.0 ; - IDEMIA2020_CRB_STAR_v1.1 ; - IDEMIA2021_NOI-P_STAR_v1.0 ; - IDEMIA2020_PSC_STAR_v1.0 ; - IDEMIA2021_VTR_STAR_v1.1.
[CER]	Rapport de certification ANSSI-CC-2022/34, ID-One Cosmo X embedding VITALE application (version 2.1.5), 23 Décembre 2022.

[CER-IC]	*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.* Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 16 mai 2022.
[CER-PTF]	Rapport de certification ANSSI-CC-2021/29, ID-One Cosmo X (Code SAAAAR : 093363). Certifié par l'ANSSI le 5 juillet 2021 sous la référence ANSSI-CC-2021/29.
[CER-PLF-D]	Rapport de certification ANSSI-CC-2021/29-S01v2, ID-One Cosmo X (R3 : 093363 ; R4 : 093364 ; R4 patché : 093364 + patch 099441). Certifié par l'ANSSI sous la référence ANSSI-CC-2021/29-S01v2.
[PP-SSCD-Part2]	*Protection profiles for secure signature creation device – Part 2: Device with key generation*, référence : prEN 419211-2:2013, version 2.0.1 datée du 18 mai 2013. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 30 juin 2016 sous la référence BSI-CC-PP-0059-2009-MA-02.
[PP-SSCD-Part3]	*Protection profiles for secure signature creation device – Part 3: Device with key import*, référence : prEN 419211-3:2013, version 1.0.2 datée du 14 septembre 2013. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 30 juin 2016 sous la référence BSI-CC-PP-0075-2012-MA-01.
[PP-SSCD-Part4]	*Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application*, référence : prEN 419211-4:2013, version 1.0.1 datée du 12 octobre 2013. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 30 juin 2016 sous la référence BSI-CC-PP-0071-2012-MA-01.
[PP-SSCD-Part5]	*Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application*, référence : prEN 419211-5:2013, version 1.0.1 datée du 12 octobre 2013. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 30 juin 2016 sous la référence BSI-CC-PP-0072-2012-MA-01.
[PP-SSCD-Part6]	*Protection profiles for secure signature creation device – Part 6: Extension for device with key import and trusted communication with signature creation application*, référence : prEN 419211-6:2014, version 1.0.4 datée du 25 juillet 2014. Maintenu par le BSI le 30 juin 2016 sous la référence BSI-CC-PP-0076-2013-MA-01.
[PP0084]	*Protection Profile, Security IC Platform Protection Profile with Augmentation Packages*, version 1.0, 13 janvier 2014. Certifié par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) sous la référence BSI-PP-0084-2014.

ANNEXE B. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER-P-01]	Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, référence ANSSI-CC-CER-P-01, version 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 3.1, juin 2020.
[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.