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-2019/41

ID-One Cosmo v8.2 embedding VITALE application (Version 2.0.83)

Paris, le 25 octobre 2019

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

Emmanuel GERMAIN
[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-2019/41

Nom du produit

ID-One Cosmo v8.2 embedding VITALE application

Référence/version du produit

Version 2.0.83

Conformité à un profil de protection

Protection profiles for secure signature creation device

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

Critères d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 4 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

Idemia	NXP Semiconductors GmbH
2 place Samuel de Champlain,	**Troplowitzstrasse 20,**
92400 Courbevoie, France	**22529 Hamburg, 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 Premier ministre 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 la carte à puce « ID-One Cosmo v8.2 embedding VITALE application, Version 2.0.83 », disposant d'une interface contact, développée par *IDEMIA* et masquée sur le composant NXP P60D145 développé par *NXP SEMICONDUCTORS GMBH*.

Ce produit offre des services de signature électronique (SSCD[1]) aux travers des applications ADELE, VITALE1 et VITALE2, conformes aux profils de protections 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-issuance*.

1.2. Description du produit

1.2.1. Introduction

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

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].

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit et décrits dans les profils de protections 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.

[1] *Secure Signature Creation Device.*
[2] *Signature Creation Data*.
[3] *Signature Verification Data*.
[4] *Reference Authentication Data*.

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, chiffrage/déchiffrage de message émis, génération et vérification de MAC, échange de clé Diffie-Hellman, 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].

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 NXP P60D145 certifié sous la référence [CER-IC] ;
- de la plateforme *Java Card* ouverte « ID-One Cosmo V8.2 » certifiée sous la référence [CER-PTF] ;
- de l'*applet* de signature VITALE composée des applications ADELE, VITALE1 et VITALE2 contenant entre autres les fonctionnalités SSCD ;
- d'une application AIP (Application d'Initialisation et de Personnalisation), une application d'administration utilisée en phase de pré-personnalisation et de personnalisation et 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[1]).

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] et dans les [GUIDES].

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 les [GUIDES].

[1] *Target of Evaluation.*

Eléments de configuration		Origine
Nom / Version de la TOE	ID-One Cosmo v8.2 embedding VITALE application, version 2.0.83	*IDEMIA*
Identification de l'*applet* VITALE	« 56 49 » (identifiant de l'*applet*) « 91 07 » (date de version de l'*applet*) « 20 83 » (version de l'*applet*)	
Identification de la plateforme : ID-One Cosmo v8.2	« 82 31 » (plateforme) « 82 22 » (date de release) « 30 0E » (version)	
Identification du composant : NXP P60D145	« 47 90 » (fondeur) « 6B 48 » (type de composant)	*NXP SEMICONDUCTORS GMBH*

1.2.5. Cycle de vie

Le cycle de vie du produit est décrit au chapitre 4 de la cible de sécurité [ST] et résumé dans le tableau suivant :

Phase	Rôle	Sites ou acteurs	Couvert par
1	Développement du logiciel embarqué	Idemia Courbevoie et Meyreuil Sites audités dans le cadre de [CER-PTF]	ALC
2	Développement du microcontrôleur	Sites audités dans le cadre de [CER-IC]	ALC
3	Fabrication de l'IC et *packaging*	Sites audités dans le cadre de [CER-IC]	ALC
4	Chargement du logiciel	Idemia Noida et Vitré	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 d'*IDEMIA* (voir [SITES]) :

***IDEMIA* – Courbevoie** [CRB] 2, place Samuel de Champlain 92400 Courbevoie, France	***IDEMIA* – Vitré** [VIT] Avenue d'Helmstedt, BP 90308 35503 Vitré Cedex, France
***IDEMIA* – Noida** [NOI] Syscom India Private Limited Plot No. 60-61, NSEZ, Phase-II Dadri Road Noida-201305, Uttar Pradesh Inde	***IDEMIA* – Meyreuil** [MEY] Site ARTEPARC Route de la côte d'Azur 13590 Meyreuil, France

1.2.6. Configuration évaluée

Le certificat porte sur la configuration identifiée au paragraphe 1.2.4.

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 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 de l'application VITALE dans la plateforme déjà certifiée par ailleurs.

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

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 10 octobre 2019, 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 a été réalisée. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Afin que les mécanismes analysés soient conformes aux exigences du référentiel cryptographique de l'ANSSI ([REF]), les recommandations données au chapitre 8 du guide [PRE] doivent être respectées.

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.

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 (voir [CER-PTF]).

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 « ID-One Cosmo v8.2 embedding VITALE application, Version 2.0.83 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté 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].

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[1], 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].

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

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[1], 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 :

[1] La 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 4+	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	**4**	Complete functional specification
	ADV_IMP				1	1	2	2	**1**	Implementation representation of TSF
	ADV_INT					2	3	3		
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	**3**	Basic 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	**4**	Problem tracking 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	**1**	Well-defined development tools
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	**1**	Testing: basic 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 v8.2 embedding VITALE application, référence 2018_2000040096, version 1.6 du 09/10/2019, *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 v8.2 embedding VITALE application, référence 2019_2000043446, version 1.2 du 09/10/2019, *IDEMIA*.
[RTE]	Rapport technique d'évaluation : - Rapport technique d'évaluation RATEL, référence LETI.CESTI.RAT.RTE.A.001, version 1.2 du 10/10/2019, *CEA-LETI*.
[ANA-CRY]	Cotation des mécanismes cryptographiques – RATEL, référence LETI.CESTI.RAT.RT.005, version 1.0 du 14 février 2019, *CEA-LETI*.
[CONF]	Liste de configuration du produit : - Sesam-Vitale PCN-16-08, VITALE2 applet 2nd source – Software Release Sheet, référence 2018_2000035218, version 7.0 du 09/10/2019, *IDEMIA*.
[GUIDES]	Guide d'installation et d'administration du produit : - [PRE] Sesam-Vitale PCN-16-08, Guide d'utilisation, Manuel de Pré-Personnalisation - Personnalisation, référence 2018_2000035895, version 1.5 du 09/10/2019, *IDEMIA*. Guide d'utilisation du produit : - [OPE] Sesam-Vitale PCN-16-08, Guide d'utilisation, Manuel utilisateur, référence 2018_200035894, version 1.3 du 14/06/2019, *IDEMIA*.

[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - [CRB] o IDEMIA Development Environment ALC Class Evaluation Report (Generic Documentary activities), reference IDEMIA R&D site 2018_GEN_v1.1, version 1.1 du 19/06/2019, *SERMA SAFETY & SECURITY*. o Site Technical Audit Report - CRB, référence IDEMIA R&D site 2018_CRB_STAR_v1.3, version 1.3 du 26/06/2019, *SERMA SAFETY & SECURITY*. - [MEY] o Morpho MEYREUIL Site : 2017 Audit Report, reference LETI.CESTI.MOR.RAD.004, version 1.0 du 05/10/2017, *CEA-LETI*. - [NOI] o ALC Class Evaluation Report – IDEMIA 2019 Project, reference IDEMIA-2019_GEN_v1.1, version 1.1 du 19/07/2019, *SERMA SAFETY & SECURITY*. o Site Technical Audit Report 2019 – NOI-P, référence IDEMIA-2019_NOI-P_STAR_v1.1, version 1.1 du 19/07/2019, *SERMA SAFETY & SECURITY*. - [VIT] o Site Visit Lite Report – Vitré site audit, référence 17-0232_SVR-VTR_M_V1.0, version 1.0 du 17/01/2018, *SERMA SAFETY & SECURITY*.
[CER-PTF]	Rapport de certification ANSSI-CC-2019/28, Plateforme ID-One Cosmo v8.2 masquée sur le composant NXP P60D145. *Certifié par l'ANSSI le 19 juillet 2019 sous la référence ANSSI-CC-2019/28.*
[CER-IC]	Certification Report BSI-DSZ-CC-1059-2018 for NXP Secure Smart Card Controller P6022y VB* including IC Dedicated Software from NXP Semiconductors Germany GmbH. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 18 mai 2018, sous la référence BSI-DSZ-CC-1059-2018.*
[PP-SSCD-Part2]	Protection profiles for secure signature creation device – Part 2: Device with key generation, référence : prEN 14169-2:2012, version 2.0.1 datée du 23 janvier 2012. *Maintenu par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 21 février 2012 sous la référence BSI-CC-PP-0059-2009-MA-01.*
[PP-SSCD-Part3]	Protection profiles for secure signature creation device – Part 3: Device with key import, référence : prEN 14169-3:2012, version 1.0.2 datée du 24 juillet 2012. *Certifié par le BSI le 27 septembre 2012 sous la référence BSI-CC-PP-0075-2012.*

[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 14169-4:2012, version 1.0.1 datée du 14 novembre 2012. *Certifié par le BSI le 12 décembre 2012 sous la référence BSI-CC-PP-0071-2012.*
[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 14169-5:2012, version 1.0.1 datée du 14 novembre 2012. *Certifié par le BSI le 12 décembre 2012 sous la référence BSI-CC-PP-0072-2012.*
[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 14169-6:2013, version 1.0.4 datée du 3 avril 2013. *Certifié par le BSI le 16 avril 2013 sous la référence BSI-CC-PP-0076-2013.*
[PP JCS-O]	SUN Java Card System Protection Profile - Open Configuration, version 3.0. *Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2010/03-M01.*

Annexe 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 2.9, janvier 2013.
[COMP] *	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.5.1, mai 2018.
[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.
	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 2.00 du 8 juin 2012 annexée au Référentiel général de sécurité (RGS_B2), voir www.ssi.gouv.fr.
	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité (RGS_B3), 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.