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-2020/67

iTrustee on Kirin 980
(Version 3.0)

Paris, le 30 juillet 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-2020/67

Nom du produit

iTrustee on Kirin 980

Référence/version du produit

Version 3.0

Conformité à un profil de protection

Trusted Execution Environement
Référence GPD_SPE_021, version 1.2.1

certifié ANSSI-CC-PP-2014/01-M01 le 13 décembre 2016

Critères d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 2 augmenté

AVA_TEE.2

Développeurs

Huawei Technologies France

18 quai du Point du Jour, 92659 Boulogne Billancourt Cedex

Huawei Central Software

Building Q27, No. 156 Beiqing Rd, Shi-Chuang-Ke-Ji-Shi-Fan-Yuan, Hai-Dian District, Beijing 100095 P.R.China

Hisilicon

No. 1599, Xinjinqiao Rd, Pudong Distrinct, Shanghai, 201206, P.R.China

Commanditaire

Huawei Technologies France

18 quai du Point du Jour, 92659 Boulogne Billancourt Cedex

Centre d'évaluation

THALES / CNES

290 allée du Lac, 31670 Labège, France

Accords de reconnaissance applicables

CCRA

Ce certificat est reconnu au niveau EAL2

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 national 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 le système d'exploitation « iTrustee on Kirin 980, Version 3.0 » développé par Huawei Technologies France

Ce produit est un environnement d'exécution de confiance (*Trusted Execution Environment* – TEE) pour des systèmes embarqués mettant en œuvre les spécifications de TEE de *GLOBALPLATFORM*. Il s'agit d'un environnement d'exécution isolé de tout autre environnement d'exécution, y compris l'environnement d'exécution du mobile (*Rich Execution Environment* – REE) et leurs applications qui sont exécutées dans ce REE.

Le TEE est capable d'exécuter des applications, appelées *Trusted Applications* (TA), ou applications de confiance, qui bénéficient d'un ensemble de services de sécurité tels que les communications sécurisées entre les *Client Applications* (CA)[1] et les TA, le stockage sécurisé des données, la gestion de clés et d'algorithmes cryptographiques, etc.

Le produit est destiné à être utilisé dans des téléphone portables *HUAWEI* de la gamme *MATE* et P pour offrir des services de sécurité mobiles tels que la gestion des droits numériques, le paiement mobile, ou encore l'authentification.

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 *Trusted Execution Environement*, référence GPD_SPE_021, version 1.2.1 [PP_TEE].

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la protection de la TOE qui inclut l'initialisation sécurisée du TEE pour garantir l'authenticité et l'intégrité de la TOE ;
- le stockage de confiance qui fournit la protection en confidentialité et intégrité de données des TA ;
- l'horodatage fiable qui peut être utilisé par les applications de confiance ;
- l'identification des utilisateurs et le contrôle d'accès pour restreindre l'accès des TA à certaines ressources;
- l'audit de sécurité pour détecter les potentielles violations de sécurité ;
- la protection de la TA pendant tout le cycle de vie ;
- la protection des communications entre les CA et les TA ;
- l'instanciation de sécurité du TEE grâce à un processus d'initialisation sécurisé ;

[1] Applications exécutées dans le REE.

- le support cryptographique pour les TA selon les spécifications de *GlobalPlatform Internal API* [GP_TEECore].

1.2.3. Architecture

Le périmètre de l'évaluation contient :

- le système d'exploitation iTrustee ;
- les *firmwares* pour le démarrage sécurisé (*Security Boot*) et *ARM Trusted Firmware* (ATF) ;
- les composants matériels suivants : RAM, les accélérateurs cryptographiques, le CPU, le ROM et l'OTP.

La figure 1 décrit l'architecture logiciel et *firmware* du produit.

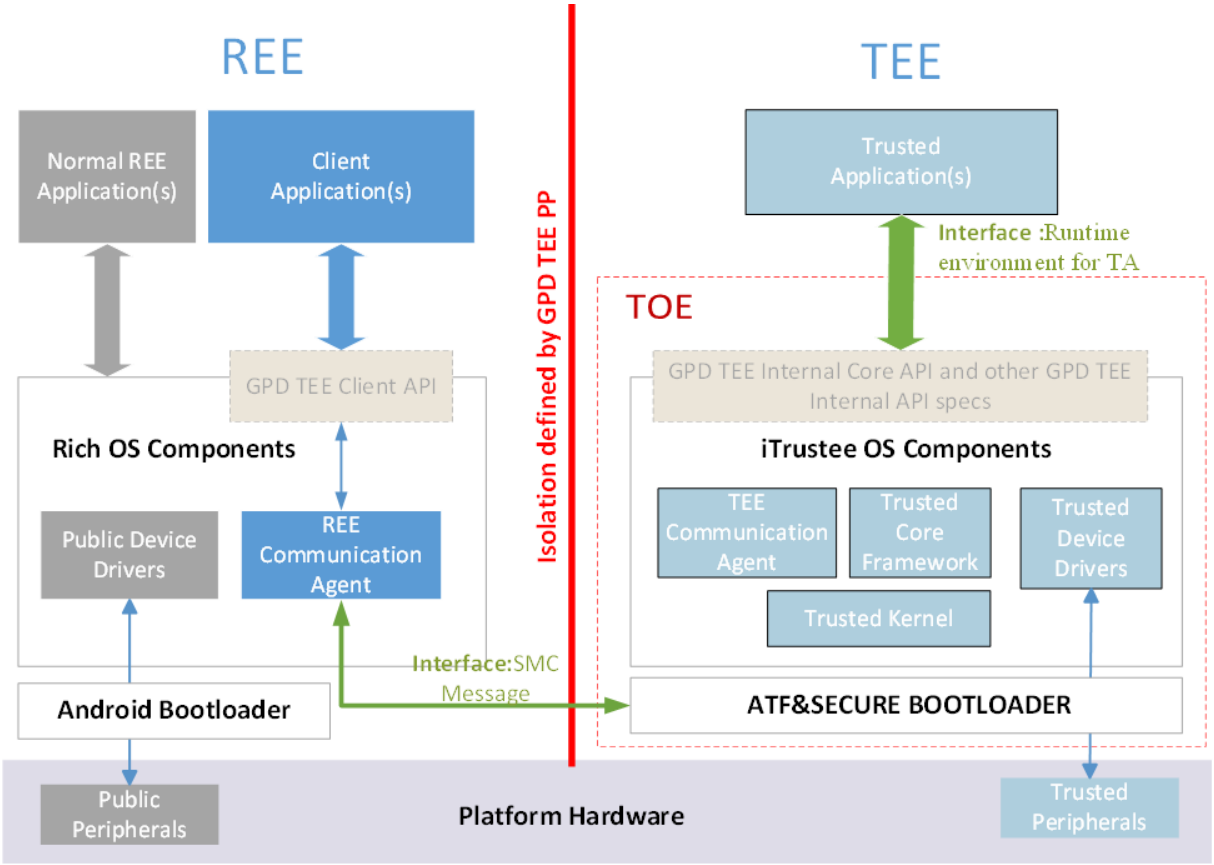

Figure 1 : Architecture logiciel et *firmware* du produit

La figure 2 décrit l'architecture matérielle du produit.

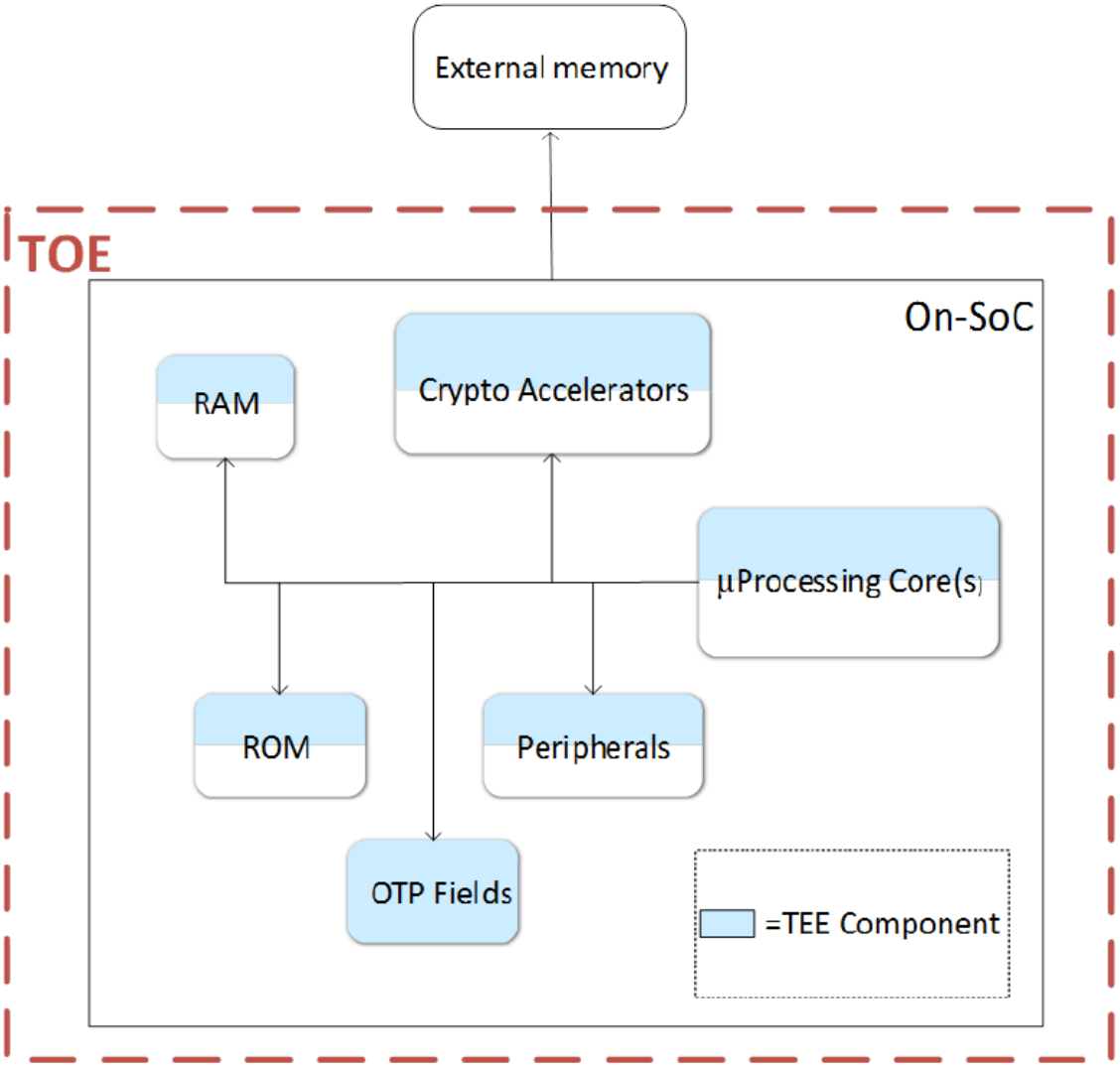

Figure 2 : Architecture matériel du produit

Les éléments ci-dessous ne sont pas dans le périmètre de l'évaluation :

- les applications de confiance ;
- l'environnement d'exécution du mobile, le REE ;
- les applications de l'utilisateur.

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 suivants :

Composant	Version	Développeur
Huawei iTrustee V3.0 on Kirin 980	3.0	*HUAWEI TECHNOLOGIES CO., LTD*
SoC	Kirin 980	*HISILICON*
ATF binary	1.0 MD5 Hash : b105cc4d51511f4b4290f48e2c782aab	*ARM/* *HISILICON*
iTrustee binary	3.0 MD5 Hash: 79d5fd6ea04d43134e12dd94218fc612	*HUAWEI TECHNOLOGIES CO., LTD*
Boot code	1.0 MD5 Hash: 2561c3f407199abcb18633155df398ad	*HISILICON*

La version de ces éléments peut être vérifiée de deux façons différentes :

- en consultant les journaux TEE au démarrage à l'aide de la commande `tlogcat` de REE ;
- en appelant l'API TEE_EXT_GetPlatformVersionInfo à partir d'une TA.

1.2.5. Cycle de vie

Le cycle de vie du produit est divisé en cinq phases :

- Phase 1 : Conception du logiciel, *firmware* et matériel ;
- Phase 2 : Fabrication du SoC ;
- Phase 3 : Intégration des logiciels ;
- Phase 4 : Fabrication des appareils ;
- Phase 5 : Utilisation finale.

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

Huawei Central Software Beijing China	**Huawei Hisilicon** Shanghai China
Huawei Mobile Department Shanghai China	**TSMC Limited** Taiwan China
ASE Technology Co., Ltd Taiwan China	**SPIL Co., Ltd** Taiwan China
Huawei Machine Co., Ltd Dongguan China	**Shenzhen FuTaiHong Precision Industry Co., Ltd** Shenzhen China

Pour l'évaluation, l'évaluateur a considéré comme utilisateur du produit les développeurs de TA et CA.

1.2.6. Configuration évaluée

Le certificat porte sur le produit tel que décrit au paragraphe « 1.2.4 Identification du produit », configuré conformément au guide de personnalisation (cf. [GUIDES]).

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 TEE, l’annexe A du [PP_TEE] a été appliquée. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation de cette annexe. 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

Le rapport technique d’évaluation [RTE], remis à l’ANSSI le 11 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_TEE.2 visé.

2.4. Analyse du générateur d’aléas

Le générateur d’aléas du produit était en dehors du périmètre de l’évaluation et n’a pas été analysé. La sortie du générateur a fait l’objet d’une analyse se basant sur le référentiel [NIST SP 800-90A], conformément à la cible de sécurité. 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_TEE.2 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 « iTrustee on Kirin 980, Version 3.0» soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 2 augmenté du composant AVA_TEE.2.

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 jusqu'au niveau ITSEC E3 Elémentaire et CC EAL4 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 [CCv3.1R5]

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 2+	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	**2**	Security-enforcing functional specification
	ADV_IMP				1	1	2	2		
	ADV_INT					2	3	3		
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	**1**	Basic 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	**2**	Use of a CM system
	ALC_CMS	1	2	3	4	5	5	5	**2**	Parts of the TOE CM coverage
	ALC_DEL		1	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			1	1	1	2	2		
	ALC_FLR									
	ALC_LCD			1	1	1	1	2		
	ALC_TAT				1	2	3	3		
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	**1**	Evidence of coverage
	ATE_DPT			1	2	3	3	4		
	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	**2**	Vulnerability analysis
	AVA_TEE		2						**2**	TEE vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Huawei iTrustee V3.0 on Kirin 980 Security Target, version 1.9, 7/11/2019. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Huawei iTrustee V3.0 on Kirin 980 Security Target, version 1.9, 7/11/2019.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report Project : ROSE, référence Rose_ETR, version 2.0, 11/03/2020.
[CONF]	Liste de configuration du produit : - Huawei iTrustee V3.0 on Kirin 980 ALC, version 1.0
[GUIDES]	Guide d'installation du produit : - [AGD_PRE]: Huawei iTrustee V3.0 on Kirin 980 Preparative Procedures for User, version 1.6, 29/04/2019. Guide d'utilisation du produit : - [AGD_OPE]: Huawei iTrustee V3.0 on Kirin 980 Operational User Guidance, version 1.2, 16/03/2019 ;
[PP_TEE]	Protection Profile, Trusted Execution Environment, référence GPD_SPE_021, version 1.2, 5 janvier 2015. *Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2014/01*.
	Protection Profile, Trusted Execution Environment, référence GPD_SPE_021, version 1.2.1, 13 décembre 2016. *Maintenu par l'ANSSI sous la référence ANSSI-CC-PP-2014/01-M01*.
[GP_TEECore]	GlobalPlatform Technology TEE Internal Core API Specification, référence GPD_SPE_010, version 1.2, 05/2019.

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.
[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.
[NIST SP 800-90A]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators, NIST SP 800-90A, janvier 2012