PREMIER MINISTRE

Liberté
Égalité
Fraternité

Agence nationale de la sécurité
des systèmes d'information

Secrétariat général de la défense et de la sécurité nationale

Rapport de certification ANSSI-CC-2021/05

S3K250A / S3K232A / S3K212A 32-bit RISC Microcontroller for Smart Card with optional AT1 Secure Libraries including specific IC Dedicated software (version S3K250A_20201028)

Paris, le 1er février 2021

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

Guillaume POUPARD [ORIGINAL SIGNE]

SÉCURITÉ Ti 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-2021/05

Nom du produit

S3K250A / S3K232A / S3K212A 32-bit RISC Microcontroller for Smart Card with optional AT1 Secure Libraries including specific IC Dedicated software

Référence/version du produit

version S3K250A_20201028

Conformité à un profil de protection

Security IC Platform Protection Profile with Augmentation Packages, version 1.0

certifié BSI-CC-PP-0084-2014 le 19 février 2014

avec conformité aux packages :

"Authentication of the security IC"

"Loader dedicated for usage in Secured Environment only"

Critère d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeur

SAMSUNG ELECTRONICS Co., Ltd.

17 Floor, B-Tower, DSR building, Samsungjeonja-ro 1-1
Hwaseong-si, Gyeonggi-do
445-330 Corée du Sud

Commanditaire

SAMSUNG ELECTRONICS Co., Ltd.

17 Floor, B-Tower, DSR building, Samsungjeonja-ro 1-1
Hwaseong-si, Gyeonggi-do
445-330 Corée du Sud

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.

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

1.1 Présentation du produit

Le produit évalué est la famille de microcontrôleurs « S3K250A / S3K232A / S3K212A 32-bit RISC Microcontroller for Smart Card with optional AT1 Secure Libraries including specific IC Dedicated software, version S3K250A_20201028 » développée par SAMSUNG ELECTRONICS Co., Ltd.

Les trois microcontrôleurs ont le même *layout*. La seule différence entre ces microcontrôleurs est la taille logique de leur mémoire *Flash* : 250Ko pour le S3K250A, 232Ko pour le S3K232A et 212Ko pour le S3K212A.

Le microcontrôleur seul n'est pas un produit utilisable en tant que tel. Il est destiné à héberger une ou plusieurs applications. Il peut être inséré dans un support plastique pour constituer une carte à puce. Les usages possibles de cette carte sont multiples (documents d'identité sécurisés, applications bancaires, télévision à péage, transport, santé, etc.) en fonction des logiciels applicatifs qui seront embarqués. Ces logiciels ne font pas partie de la présente évaluation.

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 au profil de protection [PP0084], avec :
- le *package* « *authentication of the security IC* » ;
- le *package* « *loader dedicated for usage in secured environment only* ».

Du fait des exigences additionnelles de sécurité du produit, le logiciel peut être chargé en mémoire *Flash* après le point de livraison en environnement non-audité car le micro-circuit est auto-protégé et a la capacité de s'authentifier vis-à-vis de l'utilisateur.

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont :
- la protection en intégrité et en confidentialité des données utilisateur et des logiciels embarqués exécutés ou stockés dans les différentes mémoires de la TOE[1] ;
- la bonne exécution des services de sécurité fournis par la TOE aux logiciels embarqués ;
- le support au chiffrement cryptographique à clés symétriques ou asymétriques ;
- le support à la génération de nombres non prédictibles.

[1] *Target Of Evaluation – périmètre d'évaluation.*

1.2.3 *Architecture*

Le produit est constitué d'une partie matérielle et d'une partie logicielle, toutes deux décrites dans la cible de sécurité au chapitre 1.2 « *TOE Overview and TOE Description* ».

La partie matérielle comporte principalement :
- un processeur 32-bit (SC000 CPU[2]) avec *firewall* (MPU[3]) pour le contrôle d'accès ;
- des mémoires :
  - 19Ko de ROM (2Ko pour le *Samsung test mode*, 16Ko pour le *Boot loader*, 1Ko pour le *System API*) ;
  - 212K0 à 252Ko de *Flash*, en fonction du microcontrôleur considéré : S3K250A (250Ko), S3K232A (232Ko) et S3K212A (212Ko) ;
  - 8,5Ko de RAM (6Ko SRAM pour un usage général et 2,5Ko pour la Crypto RAM),
- des modules de sécurité : protection de la mémoire (MPU), génération d'horloge, surveillance et contrôle de la sécurité, gestion de l'alimentation, détection de fautes, etc. ;
- des modules fonctionnels : gestion des entrées / sorties en mode contact (SIO), générateur de nombres aléatoires –DTRNG[4], coprocesseurs cryptographiques DES et AES et accélérateur de calculs arithmétiques TORNADO™-T.

La partie logicielle comporte principalement :
- des logiciels de test du microcontrôleur (*Test ROM code* version 1.0) embarqués en mémoire ROM ; ces logiciels ne font pas partie de la TOE ;
- de bibliothèques optionnelles pour la génération de nombres aléatoires (*DTRNG FRO* et *EHP DTRNG FRO libraries*) ;
- de bibliothèques optionnelles pour la cryptographie asymétrique (*AT1 Secure RSA/ECC/SHA Libraries*) ;
- un *Secure Boot loader* et un *System API*, permettant le chargement sécurisé du code utilisateur. Le code du *System API* fait partie de la TOE, mais pas en tant que TSF[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. Ces éléments peuvent être vérifiés par lecture des registres situés dans une zone spéciale de la mémoire spécifiée dans les [GUIDES], ou bien par appel à une fonction. La procédure d'identification est décrite dans le guide « *Chip Delivery Specification* » (voir [GUIDES]).

[2] *Central Processing Unit.*

[3] *iMemory Protection Unit.*

[4] *Digital True Random Number Generator* - générateur physique de nombres aléatoires.

[5] *TOE Security Functionality* – Fonctionnalité de sécurité de la TOE.

Eléments de configuration		Données d'identification lues
Révision matérielle, version 0		0x00
Identification des microcontrôleurs	S3K250A	0x140205000A
	S3K232A	0x140203020A
	S3K212A	0x140201020A
Identification des logiciels embarqués	*Test ROM code*, version 1.0 (hors TOE)	0x10
	Secure Boot loader and System API code, version 0.0	0x00
Identification des bibliothèques	*AT1 Secure RSA/ECC/SHA Library* v1.03 (optionnelle)	*0x312E3033*
	AT1 Secure RSA/ECC/SHA Library v2.01 (optionnelle)	*0x322E3031*
	AT1 Secure RSA/ECC/SHA Library v2.04 (optionnellel)	*0x322E3034*
	AT1 Secure RSA/ECC/SHA Library v2.05 (optionnelle)	*0X322E3035*
	DTRNG FRO Library v1.0 (optionnelle)	*0x0100*
	DTRNG FRO Library v2.0 (optionnelle pour la conformité AIS31)	*0x0200*
	DTRNG FRO Library v2.2 (optionnelle pour la conformité AIS31)	*0x0202*
	EHP DTRNG FRO Library v1.0 (optionnelle)	*0x0100*
	EHP DTRNG FRO Library v1.2 (optionnelle)	*0x0102*

1.2.5 *Cycle de vie*

Le cycle de vie du produit est décrit au chapitre 1.2.4 de [ST], il est conforme à celui décrit dans le [PP0084]. Le produit a été développé sur les sites décrits dans ce même chapitre.

Pour l'évaluation, l'évaluateur a considéré comme utilisateur du produit le développeur de l'application à embarquer dans le microcontrôleur.

1.2.6 *Configuration évaluée*

Le certificat porte sur les microcontrôleurs et les bibliothèques logicielles qu'ils embarquent tels que définis au chapitre 1.2.4. Toute autre application, y compris éventuellement les routines embarquées pour les besoins de l'évaluation, ne fait donc pas partie du périmètre de l'évaluation.

Au regard du cycle de vie mentionné au chapitre 1.2.4 de [ST], le produit évalué est celui obtenu à l'issue de la phase 3 lorsque le produit est livré sous forme de *wafer*, ou à l'issue de la phase 4 lorsque le produit est livré en boîtiers (micro-modules, etc.).

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 s'appuie sur les résultats d'évaluation de la famille de produits « S3K250A / S3K232A / S3K212A 32-bit RISC Microcontroller for Smart Card with optional AT1 Secure Libraries including specific IC Dedicated software, version S3K250A_20191028 » certifié le 18 décembre 2019 sous la référence ANSSI-CC-2019/61, voir [CER].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 30 septembre 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 a été réalisée conformément au référentiel technique de l'ANSSI [REF]. Les résultats obtenus sont mentionnés dans le rapport technique d'évaluation [RTE]. Les mécanismes analysés sont conformes aux exigences des référentiels cryptographiques de l'ANSSI. 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 produit embarque un générateur physique de nombres aléatoires, appelé DTRNG FRO, qui a fait l'objet d'une analyse par le CESTI.

Cette analyse n'a pas permis de mettre en évidence des biais statistiques bloquants. Ceci ne permet pas d'affirmer que les données générées soient réellement aléatoires mais assure que le générateur ne souffre pas de défauts majeurs de conception. Comme énoncé dans le document [REF], il est rappelé que, pour un usage cryptographique, la sortie d'un générateur matériel de nombres aléatoires doit impérativement subir un retraitement algorithmique de nature cryptographique, même si l'analyse du générateur physique d'aléas n'a pas révélé de faiblesse.

Le générateur de nombre aléatoire DTRNG FRO, utilisé comme indiqué dans [GUIDES] répond aux exigences PTG.2 de la méthodologie [AIS 31].

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 « S3K250A / S3K232A / S3K212A 32-bit RISC Microcontroller for Smart Card with optional AT1 Secure Libraries including specific IC Dedicated software, version S3K250A_20201028 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 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.

Ce certificat donne une appréciation de la résistance produit « S3K250A / S3K232A / S3K212A 32-bit RISC Microcontroller for Smart Card with optional AT1 Secure Libraries including specific IC Dedicated software, version S3K250A_20201028 » à des attaques qui sont fortement génériques du fait de l'absence d'application spécifique embarquée. Par conséquent, la sécurité d'un produit complet construit sur le micro-circuit ne pourra être appréciée que par une évaluation du produit complet, laquelle pourra être réalisée en se basant sur les résultats de l'évaluation citée au chapitre 2.

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[6], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

3.3.2 *Reconnaissance internationale critères communs (CCRA)*

Ce certificat est émis dans les conditions de l'accord du CCRA [CCRA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[7] , 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 :

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

[7] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

ANNEXE A. 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**	*Semi formal 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	2	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 B. Références documentaires du produits évalué

[ST]	Cible de sécurité de référence pour l'évaluation : *Security Target S3K250A / S3K232A / S3K212A 32-bit RISC Microcontroller for Smart Card with optional AT1 Secure Libraries including specific IC Dedicated software, référence ST_Kootenai3R4_v4.1*, 24 septembre 2020. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : *Security Target Lite S3K250A / S3K232A / S3K212A 32-bit RISC Microcontroller for Smart Card with optional AT1 Secure Libraries including specific IC Dedicated software*, version 4.1, 28 septembre 2020.
[RTE]	Rapport technique d'évaluation : *Evaluation Technical Report (full ETR) – KOOTENAI3-R4, référence LETI.CESTI.KOO3R4.FULL.001-V1.0*, 30 septembre 2020. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : *Evaluation Technical Report (ETR for composition) KOOTENAI3-R4, référence LETI.CESTI.KOO3R4.COMPO.001-V1.0*, 30 septembre 2020.
[CONF]	Liste de configuration du produit : *Configuration Management, référence Kootenai3-R4_ALC_CMC_CMS_V5.0*, 28 septembre 2020.
[GUIDES]	*S3D350A/S3K170A/S3K250A HW DTRNG FRO and DTRNG FRO Library Application Note*, référence S3D350A_S3K170A_S3K250A_DTRNG_FRO_AN v1.42, 10 septembre 2020 ; *S3D350A/S3K170A/S3K250A HW DTRNG FRO and DTRNG FRO Library Application Note*, référence S3D350A_S3K170A_S3K250A_DTRNG_FRO_AN v1.62, 10 septembre 2020 ; *S3D350A/S3K170A/S3K250A HW DTRNG FRO and DTRNG FRO Library Application Note*, référence S3D350A_S3K170A_S3K250A_DTRNG_FRO_AN v2.0, 24 juillet 2019 ; *S3D350A/S3K170A/S3K250A HW DTRNG FRO and EHP DTRNG FRO Library Application Note*,référence S3D350A_S3K170A_S3K250A_EHP_DTRNG_FRO_AN_v1.42, 10 septembre 2020 ; *S3D350A/S3K170A/S3K250A HW DTRNG FRO and EHP DTRNG FRO Library Application Note*, référence S3D350A_S3K170A_S3K250A_DTRNG_FRO_AN_v2.0, 24 juillet 2019 ; *AT1 secure RSA/ECC Library API Manual,* référence AT1 RSA ECC Library API Manual v1.07, 30 janvier 2020 ; *AT1 secure RSA/ECC Library API Manual,* référence AT1 RSA ECC Library API Manual v2.04, 30 janvier 2020 ; *AT1 secure RSA/ECC Library API Manual,* référence AT1 RSA ECC Library API Manual v3.001, 10 septembre 2020 ; *AT1 secure RSA/ECC Library API Manual,* référence AT1 RSA ECC Library API Manual v3.01, 10 septembre 2020 ;

	S3D350A SERIES User's Manual, référence S3D350A Series_UM_REV0.94, 10 septembre 2019 ; *Security Application Note For S3D350A Family, S3K250A Family,S3K170A Family*, référence SAN_S3D350A_Series_v1.3, 21 août 2020 ; *S3K250A / S3K232A / S3K212A Chip Delivery Specification,* référence S3K250A Family_DV13, octobre 2019 ; *S3K350A SERIES Bootloader Specification,* référence S3D350A Series_ Bootloader_Specification_v1.5, 4 mars 2019 ; *S3D350A Families System API application note,* référence S3D350A Series_ AN09_SystemAPI_v0.91, 13 décembre 2018 ; *SC000 Reference Manual,* référence SC000_Reference_Manual v0.0, 13 octobre 2016.
[CER]	Rapport de certification ANSSI-CC-2019/61, S3K250A / S3K232A / S3K212A 32-bit RISC Microcontroller for Smart Card with optional AT1 Secure Libraries including specific IC Dedicated software, version S3K250A_20191028. Certifié le 18 décembre 2019.
[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 C. 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.
[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.
[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.
[AIS 31]	*A proposal for: Functionality classes for random number generators, AIS20/AIS31*, version 2.0, 18 Septembre 2011, BSI (*Bundesamt für Sicherheit in der Informationstechnik*).

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