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-2020/32

S3NSN4V 32-bit RISC Microcontroller for Smart Card with optional AE1 Secure RSA/SHA Library including specific IC Dedicated software (Revision 0)

Paris, le 26 juin 2020

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

Guillaume POUPARD
[ORIGINAL SIGNE]

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-2020/32

Nom du produit

S3NSN4V 32-bit RISC Microcontroller for Smart Card with optional AE1 Secure RSA/SHA Library including specific IC Dedicated software

Référence/version du produit

Référence S3NSN4V_20191220, revision 0

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"
"Loader dedicated for usage by authorized users only"

Critères d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 6 augmenté

ASE_TSS.2

Développeur

Samsung Electronics Co. Ltd.
17 Floor, B-Tower, 1-1, Samsungjeonja-ro
Hwaseong-si, Gyeonggi-do 445-330, Corée du Sud

Commanditaire

Samsung Electronics Co. Ltd.
17 Floor, B-Tower, 1-1, Samsungjeonja-ro
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 augmenté de FLR.2.

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 microcontrôleur « S3NSN4V 32-bit RISC Microcontroller for Smart Card with optional AE1 Secure RSA/SHA Library including specific IC Dedicated software, Revision 0 » développé par *SAMSUNG ELECTRONICS CO. LTD.*.

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* » ;
- le package « *loader dedicated for usage by authorized users only* ».

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.

1.2.3. Architecture

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

La partie matérielle comporte principalement :
- un processeur 32-bits « RISC[2] » ;
- des mémoires, dont :
  - 48 Ko de ROM,
  - 55 Ko de RAM dont 5 Ko dédiés au coprocesseur arithmétique et 2 Ko de cache,

[1] *Target Of Evaluation* ou périmètre de l'évaluation.
[2] *Reduced Instruction Set Computer* ou processeur à jeu d'instructions réduit.

  - 2000 Ko de FLASH ;
- des modules de contrôle : 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 (UART, SWP et SPI), génération de nombres aléatoires – DTRNG (*Digital True Random Number Generator*) et BPRNG (*Bilateral Pseudo-Random Number Generator*) à usage interne uniquement, coprocesseurs cryptographiques DES et AES et accélérateur de calculs arithmétiques TORNADO-E ;
- d'une puce NFC permettant de contrôler les communications sans contact à 13,56 MHz de fréquence ; cette puce ne fait pas partie de la TOE.

La partie logicielle est composée :
- des logiciels de test du microcontrôleur (*Test ROM code*) embarqués en mémoire ROM, ces logiciels ne font pas partie de la TOE ;
- d'une bibliothèque optionnelle pour la génération de nombres aléatoires (*DTRNG FRO M library*) ;
- d'une bibliothèque optionnelle de calcul cryptographique (*AE1 Secure RSA/SHA library*), qui utilise l'accélérateur TORNADO-E ;
- d'un *Secure Boot Loader* et d'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 service de sécurité évalué.

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 ci-après, détaillées dans la cible de sécurité [ST] au chapitre « *1.2.2 TOE Definition* » :

Eléments de configuration		Données d'identification lues
Identification du microcontrôleur S3NSN4V	*Référence S3NSN4V_20191220*	0x171C17041F
	Révision 0	0x00
Identification des logiciels embarqués	*Test ROM Code version 1.0*	0x10
	Secure Boot Loader & System API Code version 1.4	0x14
Identification des bibliothèques	*DTRNG FRO M library version 2.0 ou version 2.1*	0x0200 ou 0x0201
	AE1 Secure RSA/SHA library version 2.02	PKA_Lib_AE1_v2.02 (en ASCII)

Ces éléments peuvent être vérifiés par lecture des registres situés dans une zone spéciale de la mémoire ou bien par appel à une fonction comme spécifié dans les [GUIDES].

1.2.5. Cycle de vie

Le cycle de vie est décrit dans la cible de sécurité [ST] au chapitre « *1.2.4 TOE Life cycle* ». Il est conforme au cycle de vie décrit dans [PP0084].
Les points de livraison de la TOE considérés par cette évaluation sont situés :

- soit après la phase 3 ;
- soit après la phase 4.

Les sites impliqués dans le cycle de vie du produit pour les phases 2 et 3 sont les suivants (voir aussi « *Table 1-1 Sites of the TOE life cycle* » de [ST] et voir [SITES]) :

Hwasung Plant (DSR & NRD Building) 1, Samsungjeonja-ro, Hwaseong-si, Gyeonggi-do, Corée du Sud	**Giheung Plant (SR3 building, lines 1, 2, 6 & S1)** San #24, Nongseo-Dong, Giheung-gu, Yongin-si, Gyeonggi-do, Corée du Sud
PKL Plant 493-3, Sungsung-Dong, Cheonan-City, Choongcheongnam-Do, Corée du Sud	**Onyang Plant (Warehouse, line 2, line 6)** 158 Baebang-ro, Baebang-eup, Asan-si, Chungcheongnam-do, Corée du Sud
HANA Micron Plant 77 Yeonamyulgeum-ro, Umbong-Myeon, Asan-Si, Chung-Nam, Corée du Sud	**TESNA Plant** 450-2 Mogok-Dong, Pyeungtaek-City, Gyeonggi, Corée du Sud
Inesa Plant No. 818 Jin Yu Road, Jin Qiao Export Processing Zone Pudong, Shanghai, Chine	**ASE Korea** 76, Sanupdanji-gil, Paju-si, Gyeonggi-do, Corée du Sud

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 le microcontrôleur et les bibliothèques logicielles optionnelles telles que définis aux chapitres 1.2.3 et 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.

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 des produits « S3FV9RR / S3FV9RQ / S3FV9RP / S3FV9RK 32-bit RISC Microcontroller for Smart Card with optional AE1 Secure RSA/SHA Library including specific IC Dedicated software, revision 0 or 1 » (voir [CER]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 15 mai 2020 détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

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

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

2.4. Analyse du générateur d'aléas

Le produit embarque un générateur physique de nombres aléatoires, appelé DTRNG FRO, qui a fait l'objet d'une analyse par le CESTI.

Les règles RègleArchiGVA-1 et RègleArchiGVA-2 ainsi que la recommandation RecomArchiGVA-1 de [REF] s'avèrent respectées, lorsque DTRNG FRO est utilisé comme indiqué dans le guide [DTRNG_Lib]. Le document [REF] impose, pour un usage cryptographique, que la sortie d'un générateur matériel de nombres aléatoires subisse un retraitement algorithmique de nature cryptographique ; ce retraitement n'est pas implémenté dans le produit et devra être développé par l'utilisateur le cas échéant.

Le générateur de nombre aléatoire DTRNG FRO, utilisé comme indiqué dans le guide [DTRNG_Lib], avec la librairie « DTRNG FRO M libray v2.1 », répond aux exigences PTG.2 de la méthodologie [AIS31].

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 « S3NSN4V 32-bit RISC Microcontroller for Smart Card with optional AE1 Secure RSA/SHA Library including specific IC Dedicated software, Revision 0 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 6 augmenté du composants ASE_TSS.2.

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 du produit « S3NSN4V 32-bit RISC Microcontroller for Smart Card with optional AE1 Secure RSA/SHA Library including specific IC Dedicated software, Revision 0 » 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[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 :

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

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].

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 6+	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	**2**	Complete mapping of the implementation representation of the TSF
	ADV_INT					2	3	3	**3**	Minimally complex internals
	ADV_SPM						1	1	**1**	Formal TOE security policy model
	ADV_TDS		1	2	3	4	5	6	**5**	Complete semiformal modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	**1**	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	1	2	3	4	4	5	5	**5**	Advanced support
	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	**3**	Compliance with implementation standards – all parts
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	**2**	TOE summary specification with architectural design summary
ATE Tests	ATE_COV		1	2	2	2	3	3	**3**	Rigorous analysis of coverage
	ATE_DPT			1	1	3	3	4	**3**	Testing: modular design
	ATE_FUN		1	1	1	1	2	2	**2**	Ordered 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 : - S3NSN4V 32-bit RISC Microcontroller for Smart Card with optional AE1 Secure RSA/SHA Livrary including specific IC Dedicated software, ST (Security Target), version 0.5, 4 décembre 2019, *SAMSUNG ELECTRONICS CO LTD.*. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - S3NSN4V 32-bit RISC Microcontroller for Smart Card with optional AE1 Secure RSA/SHA Livrary including specific IC Dedicated software, ST (Security Target) Lite, version 0.0, 11 décembre 2019, *SAMSUNG ELECTRONICS CO LTD.*.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report (full ETR) – CAYUSE6, référence LETI.CESTI.CAY6.FULL.001, version 1.1, 15 mai 2020, *CEA-LETI.* 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) – CAYUSE6, référence LETI.CESTI.CAY6.COMPO.001, version 1.1, 15 mai 2020, *CEA-LETI.*
[CONF]	Liste de configuration du produit : - Cayuse6 Configuration Management, version 1.1, 11 décembre 2019, *SAMSUNG ELECTRONICS CO LTD.*.
[GUIDES]	Guides du produit : - DTRNG FRO M Application Note, référence S3FV9RR_DTRNG_FRO_M_AN_v1.11, version 1.11 du 3 avril 2019, *SAMSUNG ELECTRONICS CO LTD.* ; - [DTRNG_LIB] S3FV9RX S3NSN4V HW DTRNG FRO M and DTRNG FRO M Library Application Note, S3FV9RR_S3NSN4V_DTRNG_FRO_M_AN_v1.2, version 1.2 du 1er novembre 2019, *SAMSUNG ELECTRONICS CO LTD.* ; - RSA/ECC Library API Manual, AE1_RSA_ECC_Librairy_API_Manual_v0.10, version 0.10 du 6 novembre 2019, *SAMSUNG ELECTRONICS CO LTD.* ; - S3NSN4V 32-bit CMOS Microcontroller for Smart Card User's Manual, S3NSN4V_UM_REV1.01, version 1.01 du 2 décembre 2019, *SAMSUNG ELECTRONICS CO LTD.* ; - Security Application Note for S3FV9RR / S3FV9RQ / S3FV9RP / S3FV9RK, S3NSN4V, référence SAN_S3FV9RR_S3NSN4V_v0.9, version 0.9 du 25 octobre 2019, *SAMSUNG ELECTRONICS CO LTD.* ;

	- S3NSN4V Chip Delivery Specification, référence DeliverySpec_S3NSN4V_Rev1.01, version 1.01 de décembre 2019, *SAMSUNG ELECTRONICS CO LTD.* ; - Bootloader Specification for S3NSN4V, référence S3NSN4V_TN02_Bootloader_Specification_v1.01, version 1.01 du 2 décembre 2019, *SAMSUNG ELECTRONICS CO LTD.* ; - S3NSN4V System API Application Note, référence S3NSN4V_AN01_SystemAPI_v1.01, version 1.01 du 4 décembre 2019, *SAMSUNG ELECTRONICS CO LTD.* ; - SC3NN Reference Manual, référence SC300_Reference_Manual_v0.0, version 0.0 du 12 mai 2014.
[CER]	S3FV9RR/S3FV9RQ/S3FV9RP/S3FV9RK 32-bit RISC Microcontroller for Smart Card with optional AE1 Secure RSA/SHA Library including specific IC Dedicated software (Revision 0 or 1). *Certifié par l'ANSSI le 19 octobre 2018 sous la référence ANSSI-CC-2018/40.*
[PP0084]	Protection Profile, Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13 janvier 2014. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0084-2014.*

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure ANSSI-CC-CER-P-01 Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : - Part 1: Introduction and general model, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001; - Part 2: Security functional components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002; - Part 3: Security assurance components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[JIWG IC] *	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, février 2009.
[JIWG AP] *	Mandatory Technical Document - Application of attack potential to smartcards, version 3.0, avril 2019.
[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.
[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.