PREMIER 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-2021/35

S3NSN4V 32-bit RISC Microcontroller for Smart Card including specific IC Dedicated software (Référence : S3NSN4V_20210407)

Paris, le 13 juillet 2021

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-2021/35**
Nom du produit **S3NSN4V 32-bit RISC Microcontroller for Smart Card including specific IC Dedicated software**
Référence/version du produit **Référence : S3NSN4V_20210407**
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"*
Critère 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.

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 « S3NSN4V 32-bit RISC Microcontroller for Smart Card including specific IC Dedicated software, Référence : S3NSN4V_20210407 » 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 ;
- 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 des éléments suivants :
- une partie matérielle comprenant :
  - un processeur 32 bits « *RISC*[1] » ;
  - des mémoires :
    - 48 Ko de ROM ;
    - 55 Ko de RAM dont 5 Ko dédiés au coprocesseur arithmétique et 2 Ko de cache ;
    - 2000 Ko de FLASH ;
  - 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. ;

[1] *Reduced Instruction Set Computer* ou processeur à jeu d'instructions réduit.

- des modules fonctionnels : gestion des entrées / sorties en mode contact (UART, SWP et SPI), génération de nombres aléatoires – DTRNG (*Digital True Random Number Generator*[2]) 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.

- une partie logicielle composée :
  - des logiciels de test du microcontrôleur (*Test ROM code*) embarqués en mémoire ROM ; ces logiciels ne font pas partie de la TOE ;
  - de bibliothèques pour la génération de nombres aléatoires *DTRNG FRO M library*, versions : 2.0, 2.1, 3.2, 3.61, 4.0 ou C4.0 ;
  - du *Secure Boot Loader and system API*, version 1.4, permettant le chargement sécurisé du code 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 du tableau ci-après, détaillés dans la cible de sécurité [ST] au chapitre 1.2.2« TOE Definition ».

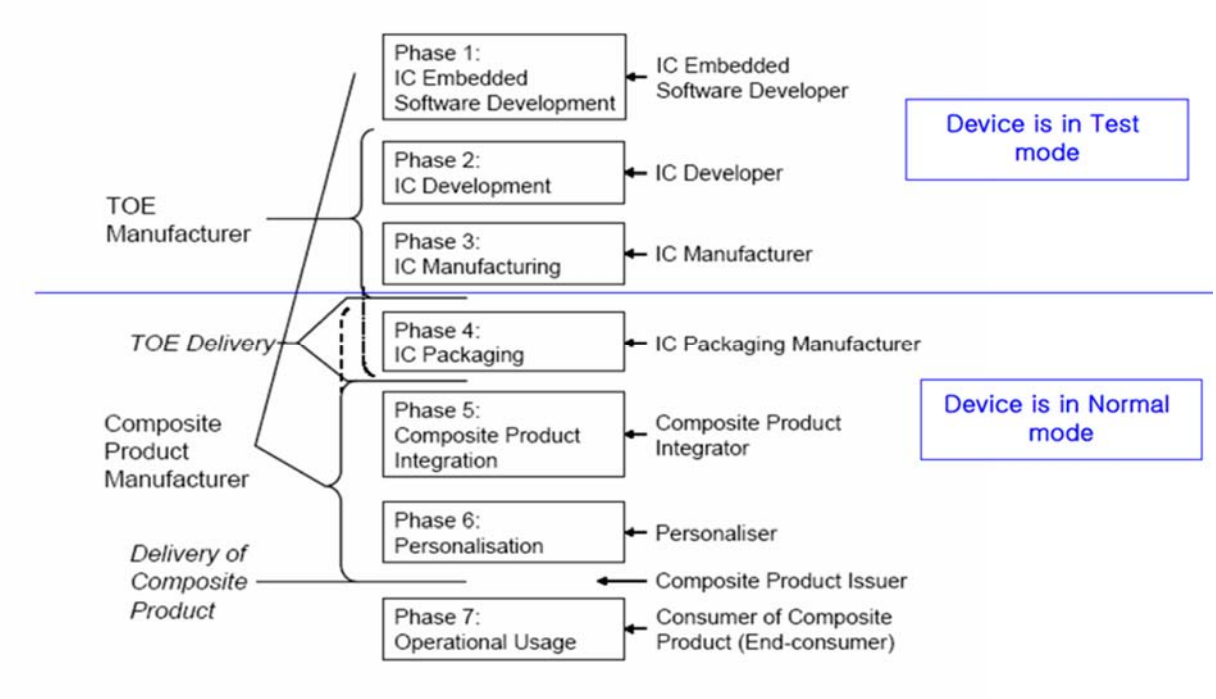
Eléments de configuration		Données d'identification lues
Identification du microcontrôleur	S3NSN4V	0x171C17041F
	Revision 0	0x00
Identification des logiciels embarqués	Test ROM Code version 1.0	0x10
	Secure Boot loader and system API version 1.4	0x14
Identification des bibliothèques	DTRNG FRO M library version 2.0	*0x0200*
	DTRNG FRO M library version 2.1	*0x0201*
	DTRNG FRO M library version 4.0	*0x0400*

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 *S3FV9RR - Chip Delivery Specification* (voir [GUIDES]).

1.2.5 *Cycle de vie*

Le cycle de vie du produit est le suivant :

[2] Générateur physique de nombres aléatoires.



Le produit a été développé sur les sites suivants :

Nom du Site	Adresse	Fonction
Hwasung Plant/ DSR Building	1, Samsungjeonja-ro, Hwasung-City, Gyeonggi-do, Corée du Sud	Phase 2 : *Smart Card Design Center*
Giheung Plant / SR3 building	San 24, Nongseo-Dong, Giheung-Gu, Yongin-City, Gyeonggi-Do 446-711, Corée du Sud	Phase 3 : *Test program developent*
Hwasung Plant/ NRD/MR2 Building	San #16, Banwol-Dong, Hwasung-City, Gyeonggi-Do, Corée du Sud	Phase 3 : *Mask Shop*
Giheung Plant/ Line S1	San 24, Nongseo-Dong, Giheung-Gu, Yongin-City, Gyeonggi-Do 446-711, Corée du Sud	Phase 3 : *Wafer Fabrication*
Giheung Plant/ Line 2		Phase 3 : *Inking / Giheung Wafer Stock*
Giheung Plant/ Line 1		Phase 3 : *Grinding*
Onyang Plant/ Warehouse	San #74, Buksoo-Ri, Baebang-Myun, Asan-City, Choongcheongnam-Do, Corée du Sud	Phase 4 : *Packing, Warehouse*
Onyang Plant/ Line 2		Phase 3&4 : *Stock, Grinding, Sawing, Packaging, Package Testing*
Onyang Plant/ Line 4		Phase 3&4 : *Grinding, Sawing, Packaging, Package Testing*
PKL Plant	493-3, Sungsung-Dong, Cheonan-City, Choongcheongnam-Do, Corée du Sud	Phase 3 : *External Mask Shop*

TOPPAN Plant	91, Wonjeok-ro 290 beon-gil,Sindun-myeon, Icheon-si, Gyeonggi-do, Corée du Sud	Phase 3 : External Mask Shop
HANAMICRON plant	#95-1 Wonnam-Li, Umbong-Myeon, Asan-City, Choongcheongnam-Do, Corée du Sud	Phase 3&4 : *Grinding, Sawing, Packaging, Package Testing*
Inesa Plant	No. 818 Jin Yu Road Jin Qiao Export Processing Zone Pudong, Shanghai, République populaire de Chine	Phase 3&4 : *Grinding, Sawing, COB*
		Phase 4 : *Packaging, Warehouse*
Eternal Plant	No.1755, Hong Mei South Road, Shanghai, République populaire de Chine	Phase 3&4 : *Sawing, COB*
		Phase 4 : *Packing, Warehouse*
TESNA Plant	450-2 Mogok-Dong, Pyeungtaek City, Gyeonggi, Corée du Sud	Phase 3 : Wafer *Testing, Pre-personalization*
ASE Korea	76, Saneopdanji-gil, Paju-si, Gyeonggi-do, Corée du Sud	Phase 3&4 : *Grinding, Sawing, SIP module assembly*
SFA Plant	30,2 gongda 7-gil, Seobukgu, Cheonansi, Choongcheongnam-Do, Corée du sud	Phase 4 : *IC Bumping*

1.2.6 *Configuration évaluée*

Le certificat porte sur les microcontrôleurs et les bibliothèques logicielles qu'ils embarquent tels que définis au 1.2.3. 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 détaillé au chapitre 1.2.5, 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 [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 du produit S3NSN4V 32-bit RISC Microcontroller for Smart Card with optional AE1 Secure RSA/SHA Library including specific IC Dedicated software certifié le 26 juin 2020 sous la référence ANSSI-CC-2020/32, voir [CER].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 29 mars 2021, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

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

La cotation des mécanismes cryptographiques a été réalisée. Afin que les mécanismes analysés soient conformes aux exigences du référentiel cryptographique de l'ANSSI ([REF]), les recommandations suivantes doivent être suivies :

- le triple-DES ne doit pas être utilisé après 2025 ;
- les bi-clés ne doivent être utilisées que dans un unique objectif fonctionnel.

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'aléa

Les produits embarquent un DTRNG, appelé DTRNG FRO M, incluant un retraitement qui a fait l'objet d'une analyse par le CESTI. Cette analyse n'a pas permis de mettre en évidence de 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 révélée de faiblesse.

Le générateur de nombres aléatoires a fait l'objet d'une évaluation selon la méthodologie [AIS 31] par le centre d'évaluation.

Le générateur atteint le niveau « PTG.2 ».

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 soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation visé.

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 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[3], 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].

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

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[4] , 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 :

[4] 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 produits évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - *S3NSN4V 32-bit RISC Microcontroller for Smart Card including specific IC Dedicated software, ST (Security Target), version 1.3*, 09/03/2021, SAMSUNG. 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 including specific IC Dedicated software, ST (Security Target) Lite, version 1.0*, 18/03/2021, SAMSUNG.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report (full ETR) – CAYUSE6-R - LETI.CESTI.CAY6R.FULL.001, version 1.0*, 19/03/2021, 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-R, LETI.CESTI.CAY6R.COMPO.001, version 1.0*, 19/03/2021, CEA-LETI.
[CONF]	Liste de configuration du produit : *Common Criteria Information Technology Security Evaluation – Cayuse6R – Configuration Management*, référence : Cayuse6R_ALC_CMC_CMS_V2.1, version 2.1, 19/03/2021, SAMSUNG.
[GUIDES]	Guide du produit : - *S3FV9RX HW DTRNG FRO M and DTRNG FRO M Library Application Note, version 1.13*, 09/03/2021, SAMSUNG ; - *S3FV9RX S3NSN4V HW DTRNG FRO M and DTRNG FRO M Library Application Note, version 1.3*, 09/03/2021 ; - S3FV9RX S3NSN4V HW DTRNG FRO M and DTRNG FRO M Library Application Note, version 3.0, 09/03/2021, SAMSUNG ; - S3NSN4V User's Manual, version 1.01, 02/12/2019, SAMSUNG ; - *Security Application Note for S3FV9RR/S3FV9RQ/S3FV9RP/S3FV9RK, S3NSN4V, version 1.0*, 21/10/2020 ; - S3NSN4V Chip Delivery Specification, version 1.01, décembre 2019, SAMSUNG ; - - Bootloader Specification for S3NSN4V, version 1.01, 02/12/2019, SAMSUNG ; - S3NSN4V System API Application Note, version 1.01, 04/12/2019, SAMSUNG ; - *SC300 Reference Manual, version 0.0*, 12/05/2014, SAMSUNG.
[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.
[CER]	*S3NSN4V 32-bit RISC Microcontroller for Smart Card with optional AE1 Secure RSA/SHA Library including specific IC Dedicated software (Revision 0)*

	Certifié le 26/06/2020 par l'ANSSI sous la référence ANSSI-CC-2020/32.

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]	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 and similar devices*, version 3.1, juin 2020.
[CCRA]	*Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security*, 2 juillet 2014.
[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.
[AIS31]	*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.