



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-2019/21
ST31H320 C01 including optional
cryptographic library NESLIB version 6.2.1

Paris, le 9 mai 2019

*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 présumées 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

La reproduction de ce document sans altération ni coupure est autorisée.

<i>Référence du rapport de certification</i> ANSSI-CC-2019/21
<i>Nom du produit</i> ST31H320 C01 including optional cryptographic library NESLIB version 6.2.1
<i>Référence/version du produit</i> C01
<i>Conformité à un profil de protection</i> Security IC Platform Protection Profile with Augmentation Packages, version 1.0, certifié BSI-CC-PP-0084-2014 le 19 février 2014 <i>avec conformité aux packages</i> “Loader dedicated for usage in Secured Environment only”
<i>Critères d'évaluation et version</i> Critères Communs version 3.1 révision 5
<i>Niveau d'évaluation</i> EAL 5 augmenté ADV_IMP.2, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.1, ALC_TAT.3, AVA_VAN.5
<i>Développeur</i> STMicroelectronics 190 avenue Celestin Coq, ZI de Rousset, 13106 Rousset, France
<i>Commanditaire</i> STMicroelectronics 190 avenue Celestin Coq, ZI de Rousset, 13106 Rousset, France
<i>Centre d'évaluation</i> Serma Safety & Security 14 rue Galilée, CS 10071, 33608 Pessac Cedex, France
<i>Accords de reconnaissance applicables</i>   Ce certificat est reconnu au niveau EAL2 augmenté de FLR.1.

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	6
1.1. PRESENTATION DU PRODUIT	6
1.2. DESCRIPTION DU PRODUIT	6
1.2.1. <i>Introduction</i>	6
1.2.2. <i>Services de sécurité</i>	6
1.2.3. <i>Architecture</i>	7
1.2.4. <i>Identification du produit</i>	7
1.2.5. <i>Cycle de vie</i>	7
1.2.6. <i>Configuration évaluée</i>	8
2. L’EVALUATION	9
2.1. REFERENTIELS D’EVALUATION	9
2.2. TRAVAUX D’EVALUATION	9
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI	9
2.4. ANALYSE DU GENERATEUR D’ALEAS	9
3. LA CERTIFICATION	10
3.1. CONCLUSION	10
3.2. RESTRICTIONS D’USAGE	10
3.3. RECONNAISSANCE DU CERTIFICAT	11
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	11
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i>	11
ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT	12
ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	13
ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION	16

1. Le produit

1.1. Présentation du produit

Le produit évalué est le microcontrôleur « ST31H320 C01 *with firmware* version 2.0.2 *including optional cryptographic library NESLIB* version 6.2.1 » développé par *STMICROELECTRONICS*.

Comme décrit dans la cible de sécurité [ST] au paragraphe *TOE overview*, ce produit se décline en différentes configurations selon la taille de mémoire non volatile *FLASH* et l'activation du coprocesseur cryptographique *NESCRYPT*. Ces configurations sont également décrites dans le document *Datasheet* (voir [GUIDES]).

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 « *loader dedicated for usage in secured environment only* ».

1.2.2. Services de sécurité

Les principaux services de sécurité évalués fournis par le produit sont :

- la protection physique ;
- l'initialisation de la plate-forme matérielle et des attributs ;
- la gestion sécurisée du cycle de vie ;
- l'intégrité logique du produit ;
- les contrôles d'accès aux mémoires ;
- la gestion des violations sécuritaires ;
- la non-observabilité des informations sensibles ;
- le chargement et la gestion de la mémoire *FLASH* ;
- le support au chiffrement cryptographique à clés symétriques ;
- le support à la génération de nombres non prédictibles ;
- le service optionnel de bibliothèque cryptographique *NESLIB* 6.2.1 offre les fonctionnalités DES, AES, RSA, SHA, ECC, DRBG, ainsi que la génération sécurisée de nombres premiers et de clés RSA.

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 paragraphe *TOE description*.

La partie matérielle comporte principalement :

- un processeur ARM SecurCore SC000 ;
- des coprocesseurs cryptographiques pour accélérer les calculs AES, Triple DES (EDES+) et de cryptographie asymétrique (*NESCRYPT*)¹ ;
- un générateur physique d'aléa (TRNG) ;
- des mémoires non volatiles (ROM, Flash) et volatile (SRAM) ;
- des modules de sécurité : unité de protection des mémoires (MPU), générateur d'horloge, surveillance et contrôle de la sécurité, contrôle d'intégrité ;
- des modules fonctionnels : compteurs, gestion des entrées/sorties en mode contact.

La partie logicielle est composée de :

- un logiciel dédié (OST), participant au démarrage du composant (*boot sequence*) ;
- un logiciel dédié (*firmware*), assurant la gestion du cycle de vie, le chargement de la mémoire Flash (*Secure Flash loader*), et l'interfaçage avec l'application (*drivers*) ;
- optionnellement, une bibliothèque cryptographique (*NESLIB*), offrant des services RSA (dont la génération de clés), courbes elliptiques, hachage, génération de nombres premiers, génération d'aléas déterministes (DRBG), DES et AES.

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 (voir [ST] au paragraphe « TOE identification » et [GUIDES]) :

- *IC Maskset name* : K8N0A ;
- *IC version* : D ;
- *Master product identification number* : 00DE ;
- *Firmware version* : 2.0.2 ;
- *OST version* : 4.0 ;
- (optionnel) *NESLIB crypto library version* : 6.2.1

Toutes ces valeurs sont disponibles à travers les interfaces logiques du produit, selon les méthodes et formats décrits dans [GUIDES].

1.2.5. Cycle de vie

Le cycle de vie du produit est décrit dans la cible de sécurité (voir [ST]) ; il est conforme au cycle de vie de 7 phases décrit dans [PP0084]. Les sites impliqués dans le cycle de vie pour les phases 2, 3 et 4 sont indiqués dans la cible de sécurité (voir table 16 de [ST]).

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

¹ Les fonctions de sécurité évaluées de NESCRYPT (NExt Step CRYPTography) utilisent l'API de NesLib : l'utilisation de NESCRYPT sans NesLib sort donc du cadre de ce certificat.

1.2.6. Configuration évaluée

Le certificat porte sur le produit « ST31H320 C01 *including optional cryptographic library NESLIB version 6.2.1* » dans les différentes configurations offertes (tailles mémoire, activation *NESCRYPT*), voir [ST]§1.5 et [GUIDES].

Les fonctionnalités de *NESCRYPT* ont été évaluées à travers la bibliothèque cryptographique *NESLIB*.

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 [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 « *ST31H320 A02 including optional cryptographic library NESLIB* » maintenu le 20 avril 2016 sous la référence ANSSI-CC-2015/59-M01 [R-M01]. La principale amélioration apportée à la TOE, est la mise à jour de la *NESLIB*.

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 29 avril 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 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 générateur de nombres aléatoires a fait l'objet d'une évaluation selon la méthodologie [AIS31] et il répond aux exigences de la classe PTG.2.

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 révélé de faiblesse.

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 « *ST31H320 C01 including optional cryptographic library NESLIB version 6.2.1* » 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 ADV_IMP.2, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.1, ALC_TAT.3 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 du produit « *ST31H320 C01 including optional cryptographic library NESLIB version 6.2.1* » 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'accord¹, 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].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires², 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 SOG-IS est disponible sur le site web de l'accord : www.sogis.org.

² 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 5+	Intitulé du composant			
ADV Développement	ADV_ARC		1	1	1	1	1	1	1	1	Security architecture description		
	ADV_FSP	1	2	3	4	5	5	6	5	5	Complete semi-formal functional specification with additional error information		
	ADV_IMP				1	1	2	2	2	2	Complete mapping of the implementation representation of the TSF		
	ADV_INT					2	3	3	2	2	Well-structured internals		
	ADV_SPM						1	1					
	ADV_TDS		1	2	3	4	5	6	5	5	Complete semiformal modular design		
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance		
	AGD_PRE	1	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	5	Advanced support		
	ALC_CMS	1	2	3	4	5	5	5	5	5	Development tools CM coverage		
	ALC_DEL		1	1	1	1	1	1	1	1	Delivery procedures		
	ALC_DVS			1	1	1	2	2	2	2	Sufficiency of security measures		
	ALC_FLR									1	1	Basic flaw remediation	
	ALC_LCD			1	1	1	1	2	1	1	1	Developer defined life-cycle model	
	ALC_TAT				1	2	3	3	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	1	1	Conformance claims	
	ASE_ECD	1	1	1	1	1	1	1	1	1	1	Extended components definition	
	ASE_INT	1	1	1	1	1	1	1	1	1	1	ST introduction	
	ASE_OBJ	1	2	2	2	2	2	2	2	2	2	Security objectives	
	ASE_REQ	1	2	2	2	2	2	2	2	2	2	Derived security requirements	
	ASE_SPD		1	1	1	1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	2	2	2	Analysis of coverage	
	ATE_DPT			1	1	3	3	4	3	3	3	3	Testing: modular design
	ATE_FUN		1	1	1	1	2	2	1	1	1	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	2	2	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	5	5	5	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none">- ST31H320 C01 including optional cryptographic library NESLIB, Security Target, référence SMD_ST31H320_ST_17_001 Rev C01.3, octobre 2018, <i>STMICROELECTRONICS</i>. <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none">- ST31H320 C01 including optional cryptographic library NESLIB, Security Target for composition, référence SMD_ST31H320_ST_17_002 Rev C01.3, octobre 2018, <i>STMICROELECTRONICS</i>.
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none">- Evaluation Technical Report – Loupiac3 project, référence Loupiac3_ETR_v1.4, version 1.4, 29 avril 2019, <i>SERMA SAFETY & SECURITY</i>. <p>Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé :</p> <ul style="list-style-type: none">- ETR Lite for Composition – Loupiac3 project, référence Loupiac3_ETR-Lite_v1.4, version 1.4, 29 avril 2019, <i>SERMA SAFETY & SECURITY</i>.
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none">- ST31 – K8N0 Configuration list – C01, référence SMD_ST31H320_D_CFGL_C01, version 1.1, 17 octobre 2018, <i>STMICROELECTRONICS</i> ;- NesLib 6.2.1 for ST31H320 Configuration List, référence SSS_NESLIB_6.2.1_CFGL_18_002, version 01-00, 16/10/2018, <i>STMICROELECTRONICS</i>.

[GUIDES]	<ul style="list-style-type: none">- ST31H platform ST31H320, Datasheet – production data, référence DS_ST31H320 Rev 2, 29 janvier 2016, <i>STMICROELECTRONICS</i> ;- ARM Cortex SC000 Technical Reference Manual, référence ARM_DDI_0456 Rev A, septembre 2010, <i>ARM</i> ;- ARMv6-M Architecture Reference Manual, référence ARM_DDI_0419 Rev C, septembre 2010, <i>ARM</i> ;- User manual, ST31 firmware, référence UM_ST31_FW Rev 9, mars 2016, <i>STMICROELECTRONICS</i> ;- User manual, ST31H320 Flash memory loader, installation guide, référence UM_31H_FL Rev 3, juillet 2015, <i>STMICROELECTRONICS</i> ;- User manual, UM_NesLib_6.2, référence UM_NesLib_6.2-Rev1.0, juin 2018, <i>STMICROELECTRONICS</i> ;- Application note, ST31G and ST31H secure MCU platforms NesLib 6.2 security recommendations, référence AN_SECU_ST31G_H_NESLIB_6.2 Rev4.0, octobre 2018, <i>STMICROELECTRONICS</i> ;- Release note, NesLib 6.2.1 for ST31G and ST31H platforms, reference RN_ST31_NESLIB_6.2.1 – Rev 2.0, octobre 2018, <i>STMICROELECTRONICS</i> ;- ST31H and ST31H Secure MCU platforms Security Guidance, référence AN_SECU_ST31G_H, version 5, juin 2018, <i>STMICROELECTRONICS</i> ;- User manual, ST31G and ST31H – AIS31 Compliant Random Number, référence UM_31G_31H_AIS31 Rev1, janvier 2015, <i>STMICROELECTRONICS</i> ;- Application note, ST31G and ST31H – AIS31 reference implementation: start-up, on-line and total failure tests, référence AN_31G_31H_AIS31 Rev 1, janvier 2015, <i>STMICROELECTRONICS</i>.
----------	--

[SITES]	<p>Rapports d'analyse documentaire et d'audit de site pour la réutilisation :</p> <ul style="list-style-type: none"> - ALC Class Evaluation Report – STM Project, référence STM_GEN_v1.0, version 1.0, 18 octobre 2018 ; - ALC Class Evaluation Report – STM Project, référence STM_GEN_v2.0, version 2.0, 21 décembre 2018 ; - ALC Class Evaluation Lite Report – C15P0036 Project, référence C15P0036_GEN_Lite_V1.0, version 1.0, 2 juin 2016 ; - ALC Class Evaluation Report – C15P0036 Project, référence C15P0036_ALC_GEN_V2.0, version 2.0, 11 juillet 2018 ; - Site Technical Audit Report – STM Sophia, référence STM_Sophia_STAR_v1.0, version 1.0, 28 décembre 2018 ; - Site Technical Audit Report – Site SMARTFLEX3, référence SiteSMARTFLEX3_STAR_v1.0, version 1.0, 29 septembre 2018 ; - Site Visit Lite Report – STM ROUSSET site audit, référence 17-0317_STM-ROUSSET_SVR-M_v1.1, version 1.1, 20 juillet 2018 ; - Site Visit Lite Report – Bouskoura site audit, référence 17-0317_BSK_SVR-M_v1.0, version 1.0, 18 janvier 2018 ; - Site Visit Lite Report – STM CROLLES site audit, référence STM_Crolles_SVR-M_v1.0, version 1.0, 18 juillet 2018 ; - Site Visit Lite Report – STM Zaventem site audit, référence 16-0227-STM-ZAV_SVR-M_v1.0, version 1.0, 14 juin 2017 ; - Site Visit Lite Report – STM Rennes site audit, 16-0227-STM-RNS_SVR-M_v1.0, version 1.0, 20 juillet 2017 ; - Site Visit Lite Report – STM Grenoble, 16-0227_STGrenoble_SVR-M_v1.0, version 1.0, 13 septembre 2017 ; - Sites Visit Report Lite – STM AMK1, Loyang & Calamba site audits, référence 17-0317-STM_SVR-M_v1.0, version 1.0, 20 décembre 2017 ; - Site Visit Lite Report – DPE site audit, référence 17_0317_SVR-DPE-M_v1.0, version 1.0, 21 décembre 2017 ; - Site Visit Lite Report – Toa Payoh site audit, référence 17-0317_TPY_SVR_-M_v1.0, version 1.0, 12 mars 2018 ; - Site Visit Lite Report – STM Tunis site audit, référence 16-0227-STM-TNS_SVR-M_v1.0, version 1.0, 20 octobre 2017 ; - Site Visit Lite Report – STS Shenzhen site audit, référence 17-0317_STS Shenzhen_SVR-M_v1.1, version 1.1, 14 décembre 2018 ; - Site Visit Report Lite – ATP site audit, référence 16-0227_STM-ATP_SVR-M_v1.0, version 1.0, 26 octobre 2017 ; - Site Visit Lite Report – FEILIKS site audit, référence 17-0317_FEILIKS_SVR-M_v1.0, version 1.0, 25 juillet 2018 ; - Site Technical Audit Report – DNP, référence STM-DNP_STAR_v1.0, version 1.0, 19 novembre 2018.
[PP0084]	<p>Protection Profile, Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13 janvier 2014. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0084-2014.</i></p>
[R-M01]	<p>Rapport de maintenance ANSSI-CC-2015/59-M01, ST31H320 A02 including optional cryptographic library NESLIB, 20 avril 2016.</p>

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 : <ul style="list-style-type: none"> - 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 .
[AIS 31]	A proposal for: Functionality classes for random number generators, AIS20/AIS31, version 2.0, 18 Septembre 2011, BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>).

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