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-2020/22

ST33G1M2 C01 including optional cryptographic library NesLib and optional technology MIFARE4Mobile

Paris, le 14 mai 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-2020/22

Nom du produit

ST33G1M2 C01 including optional cryptographic library NesLib and optional technology MIFARE4Mobile

Référence/version du produit

C01 avec

Version de la bibliothèque NesLib : 6.3.4

Version de la bibliothèque MIFARE4Mobile : 2.1.0

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

"Loader dedicated for usage in Secured Environment only"

Critères d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeur

STMicroelectronics

190 avenue Celestin Coq, Z.I. de Rousset, 13106 Rousset, France

Commanditaire

STMicroelectronics

190 avenue Celestin Coq, Z.I. de Rousset, 13106 Rousset, France

Centre d'évaluation

THALES / CNES

290 allée du Lac, 31670 Labège, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Ce certificat est reconnu au niveau EAL2.

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le directeur général de l'Agence national de la sécurité des systèmes d'information attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. LE PRODUIT 6

1.1. PRESENTATION DU PRODUIT 6
1.2. DESCRIPTION DU PRODUIT 6
1.2.1. Introduction 6
1.2.2. Services de sécurité 6
1.2.3. Architecture 7
1.2.4. Identification du produit 7
1.2.5. Cycle de vie 8
1.2.6. Configuration évaluée 8

2. L'EVALUATION 9

1.3. REFERENTIELS D'EVALUATION 9
1.4. TRAVAUX D'EVALUATION 9
1.5. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L'ANSSI 9
1.6. ANALYSE DU GENERATEUR D'ALEAS 9

3. LA CERTIFICATION 10

1.7. CONCLUSION 10
1.8. RESTRICTIONS D'USAGE 10
1.9. RECONNAISSANCE DU CERTIFICAT 10
1.9.1. Reconnaissance européenne (SOG-IS) 10
1.9.2. Reconnaissance internationale critères communs (CCRA) 10

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 sécurisé « ST33G1M2 C01 including optional cryptographic library NesLib and optional technology MIFARE4Mobile » développé par *STMICROELECTRONICS*.

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.

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*, les interfaces entrée/sortie, l'activation des crypto-processeurs, l'activation de l'unité de protection des librairies (LPU), la présence de la bibliothèque cryptographique *NesLib* et la présence de la bibliothèque MIFARE4Mobile. Ces configurations sont également décrites dans le document *Datasheet* (voir [GUIDES]).

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 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 sécurisés 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* v6.3.4 offrant, suivant la configuration choisie, les fonctionnalités DES, AES, RSA, ECC, SHA, DRBG et un service de génération sécurisée de nombres premiers et de clés RSA ;
- le service optionnel de bibliothèque MIFARE4Mobile v2.1.0 incluant les fonctionnalités MIFARE DESFire EV1 et MIFARE Classic.

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 paragraphe *TOE description*.

La partie matérielle comporte principalement :
- un processeur ARM SecurCore SC300 ;
- des mémoires non volatiles (ROM, *FLASH*) et volatile (RAM) ;
- des modules de sécurité : unité de protection des mémoires (MPU), unité de protection mémoire dédiée aux bibliothèques (LPU), générateur physique d'aléa (TRNG), générateur d'horloge, surveillance et contrôle de la sécurité, gestion de l'alimentation, contrôle d'intégrité des mémoires, détection de fautes ;
- des modules fonctionnels : bloc de gestion des entrées et des sortie en mode comptable (compatible avec le standard ISO 7816-3), bloc de gestion d'interface simple fil (SWP) avec une communication en champ proche (NFC) et bloc de gestion d'interface série (SPI) ;
- des coprocesseurs :
    - EDES+ pour le support des algorithmes DES ;
    - AES pour le support des algorithmes AES ;
    - NESCRYPT muni d'une RAM dédiée pour le support des algorithmes cryptographique à clé publique.

La partie logicielle est composée de :
- un logiciel dédié (OST) participant au démarrage du composant (*boot sequence*) et au test du microcontrôleur (ce logiciel stocké en ROM n'est plus accessible après la livraison de la TOE) ;
- 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 ;
- optionnellement, une bibliothèque MIFARE4Mobile incluant les fonctionnalités MIFARE DESFire EV1 et MIFARE Classic.

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 :

Eléments de configuration		Données d'identification
Identification du microcontrôleur	*IC Maskset name*	K8H0A
	IC version	F
	Master product identification number	0x0061 (ST33G1M2) 0x0105 (ST33I1M2)
Identification des logiciels embarqués	*Firmware version*	9 and A
	OST version	2.2
Identification des bibliothèques	*NesLib version*	6.3.4
	MIFARE4Mobile DesFire EV1 Id	0x00000004 or 0x00000504 (combined)
	MIFARE4Mobile version	2.1.0

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 [ST] au paragraphe *TOE life cycle*. Il est conforme au cycle de vie de sept phases décrit dans [PP0084].

La livraison de la TOE peut s'effectuer :
- soit après la phase 3 si la TOE est livré sous forme de *wafer* ou de *dice* ;
- soit après la phase 4 si la TOE est livré sous forme de produit.

Les sites impliqués dans le cycle de vie du produit pour les phases 2, 3, et 4 sont listés dans la cible de sécurité (voir table 16 de [ST] et voir [SITES]).

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 la TOE définie au paragraphe 1.2.
Les configurations testées par l'évaluateur sont représentatives des différentes combinaisons commercialisées des différentes options matérielles et logicielles de la TOE (activation ou désactivation des coprocesseurs cryptographiques, de l'unité de protection des librairies, des interfaces d'entrées et de sorties).

2. L'évaluation

1.3. 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).

1.4. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 14 avril 2020, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

1.5. 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.

1.6. Analyse du générateur d'aléas

Le générateur de nombres aléatoires a fait l'objet d'une évaluation selon la méthodologie [AIS 31] et il répond aux exigences de la classe PTG.2.

Cette analyse n'a pas permis de mettre en évidence de biais statistiques bloquants pour un usage direct des sorties des générateurs. 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

1.7. 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 « ST33G1M2 et ST33I1M2, version C01 » 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.

1.8. 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 « ST33G1M2 et ST33I1M2, version C01 » 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 microcontrôleur 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].

1.9. Reconnaissance du certificat

1.9.1. 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 :

1.9.2. Reconnaissance internationale critères communs (CCRA)

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

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 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**	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	**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	1	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 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - ST33G1M2 C01 including optional cryptographic library NesLib and optional technology MIFARE4Mobile – Security Target, référence SMD_ST33G1M2_ST_19_001, version C01.3, octobre 2019. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - ST33G1M2 C01 including optional cryptographic library NesLib and optional technology MIFARE4Mobile – Security Target for composition, référence SMD_ST33G1M2_ST_19_002, version C01.3, octobre 2019.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report – Project : ASTIM / ST33G1M2 C01, référence ASTIM_ETR, version 5.0, 14 avril 2020. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - ASTIM / ST33G1M2 C01 – ETR LITE for composition, référence ASTIM_ETRLite, version 6.0, 20 avril 2020.
[CONF]	Listes de documentation et de configuration du produit : - ST33G1M2 C01 including optional cryptographic library NesLib, and optional technology MIFAER4Mobile – Configuration list, référence SMD_33G_CFGL_15_001, version 1.06 ; - NesLib 6.3.4 for ST33 Configuration List, référence SSS_NesLib_6.3.4_CFGL_19_001, version 01.01 ; - ASTIM – ST33G1M2 C01 Documentation report, référence SMD_K8H0_F_DR_19_001, version 1.2.
[GUIDES]	- ST33G1M2 ST33I1M2 datasheet Secure MCU with 32-bit ARM SecurCore SC300 – Datasheet, référence DS_ST33G_I, version 2 ; - ST33G1M2 platform : BP and BM specific product profiles – Technical note, référence TN_ST33G1M2_01, version 2.0 ; - ST33G1M2 platform : LS, LC and BS specific product profiles – Technical note, référence TN_ST33G1M2_02, version 2.0 ; - ST33G1M2 family extension : LS, LC and BS specific product profiles, référence TN_ST33G1M2_05, version 1.0 ; - ST33G1M2 family extension : BP and BM specific product profiles, référence TN_ST33G1M2_04, version 1.0 ; - ST33G1M2 : CMOS M10+ 80-nm technology die and wafer delivery description, référence DD_ST33G1M2, version 4.0 ; - ARM Cortex SC300 r0p0 Technical Reference Manual, référence ARM DDI 0337F, version F ;

	- ARM Cortex M3 r2p0 Technical Reference Manual, ARM DDI 0337F3c, version F3c ; - ST33G1M2 Firmware user manual, référence UM_ST33G1M2_FW, version 14 ; - ST33G1M2 and derivatives Flash loader installation guide, référence UM_33G_FL, version 4.0 ; - ST33G and ST33H Firmware support for LPU regions – application note, référence AN_33G_33H_LPU, version 1 ; - ST33G and ST33H Secure MCU platforms – Securiy Guidance, référence AN_SECU_ST33, version 9 ; - ST33G and ST33H Power supply glitch detector characteristics – application note, référence AN_33_GLITCH, version 2 ; - ST33G and ST33H – AIS31 Compliant Random Number – User Manual, référence UM_33G_33H_AIS31, version 3 ; - ST33G and ST33H – AIS31 – Reference implementation : Start-up, on-line and total failure tests – Application note, référence AN_33G_33H_AIS31, version 1 ; - ST33 uniform timing application note, référence AN_33_UT, version 2 ; - NesLib cryptographic library NesLib 6.3 – User manual, référence UM_NesLib_6.3, version 4 ; - ST33G and ST33H secure MCU platforms – NesLib 6.3 security recommendations – Application note, référence AN_SECU_ST33G_H_NESLIB_6.3, version 5 ; - NesLib 6.3.4 for ST33G, ST33H and ST33I platforms – Release note, référence RN_ST33_NESLIB_6.3.4, version 2 ; - MIFARE4Mobile library 2.1 – User manual, référence UM_33_MIFARE4Mobile-2.1, version 5 ; - MIFARE4Mobile library 2.1.0 for ST33G1M2 – Application note, référence AN_ST33G1M2_M4M_Lib, version 1.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - ALC Class Evaluation Report - C15P0036 Project, référence C15P0036_ALC_GEN_V2.0, version 2.0, 11 juillet 2018 ; - 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 Report – STM 2020 Project, référence STM-2020_GEN_v1.1, version 1.1 20 novembre 2019 ; - Site Technical Audit Report - ATP1 & ATP3/4, référence STM_ATP1-3-4_STAR_v1.1, version 1.1, 13 mai 2019 ; - STMicroelectronics Development Environment Amkor Technology Taiwan 1 & 3 Site Technical Audit Report, reference STM2020_ATT1-3_STAR_v1.0, version 1.0, 6 janvier 2020 ; - Site Technical Audit Report - DNP, référence STM-DNP_STAR_v1.2, version 1.2, 27 mai 2019 ; - Site Technical Audit Report - DPE Agrate site audit, référence STM-DPE_STAR_v1.0, version 1.0, 5 juillet 2019 ;

	- Site Technical Audit Report - FEILIKS, référence STM_FEILIKS_STAR_v1.0, version 1.0, 24 avril 2019 ; - Site Technical Audit Report - Ang Mo Kio 1 Site Audit, référence STM2020_AMK1_STAR_V1.0, version 1.0, 26 novembre 2019 ; - Site Technical Audit Report TPY and AMK6, référence STM2020_TPY-AMK6_STAR_v1.0, version 1.0, 24 février 2020 ; - Site Technical Audit Report - STMicroelectronics Bouskoura Site Technical Audit Report, référence STM2020_BSK_STAR_v1.0, version 1.0, 27 décembre 2019 ; - Site Technical Audit Report STM Calamba, référence STM2020_CAL_STAR_v1.1, version 1.1, 10 janvier 2020 ; - Site Visit Lite Report – STM CROLLES site audit, référence STM_Crolles_SVR-M_v1.0, version 1.0, 18 juillet 2018 ; - Site Technical Audit Report – STM Rousset, référence STM2020_RST_STAR_v1.0, version 1.0, 5 février 2020 ; - Site Technical Audit Report - STM Grenoble, référence 18-0337_STM Grenoble_STAR_v1.0, version 1.0, 9 mai 2019 ; - Site Technical Audit Report - STM Ljubljana, référence STM_LJU_STAR_v1.0, version 1.0, 7 mars 2019 ; - Site Technical Audit Report - STMicroelectronics Loyang (LYG) Site Audit, référence STM2020_Loyang_STAR_v1.0, version 1.0, 21 novembre 2019 ; - Site Technical Audit Report - STM Rennes, référence STM_RNS_STAR_v1.0, version 1.0, 22 mai 2019 ; - Site Visit Lite Report – STS Shenzhen site audit, référence 17-0317_STS Shenzhen_SVR-M_v1.1, version 1.1, 14 décembre 2018 ; - Site Technical Audit Report - STM Sophia, référence STM_Sophia_STAR_v1.0, version 1.0, 28 décembre 2018 ; - Site Technical Audit Report - STM Tunis Site Audit, référence STM_TNS_STAR_v1.0, version 1.0, 5 septembre 2019 ; - Site Audit Technical Report - STM Zaventem site audit, référence STM_Zaventem_STAR_v1.0, version 1.0, 8 mars 2019 ; - Site Technical Audit Report - Winstek, référence STM_WIN_STAR_v1.1, version 1,1, 19 décembre 2018 ; - Site Technical Audti Report – JSCC, référence STM_JSCC_STAR_v1.0, version 1.0, 27 juin 2019 ; - Site Technical Audit Report – Smartflex, référence SMARTFLEX4_STAR_V1.0, version, 1.0, 8 août 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 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.
[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 (*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.