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-2019/13

ST31G480 E01 including optional cryptographic library NESLIB v6.2.1, optional technologies MIFARE DESFire EV1 v4.8.12 and MIFARE Plus X v2.4.6

Paris, le 5 mars 2019

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

Emmanuel GERMAIN

[ORIGINAL SIGNE]

SÉCURITÉ Ti CERTIFICATION

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2019/13

Nom du produit

ST31G480 including optional cryptographic library NESLIB v6.2.1, optional technologies MIFARE DESFire EV1 v4.8.12 and MIFARE Plus X v2.4.6

Référence/version du produit

E01

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”

“Loader dedicated for usage by authorized users only”

Critères d’évaluation et version

Critères Communs version 3.1 révision 5

Niveau d’évaluation

EAL 5 augmenté

ADV_IMP.2, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.1, ALC_TAT.3, ASE_TSS.2, AVA_VAN.5

Développeur

STMicroelectronics

190 avenue Célestin Coq, ZI de Rousset, 13106 Rousset Cedex, France

Commanditaire

STMicroelectronics

190 avenue Célestin Coq, ZI de Rousset, 13106 Rousset Cedex, France

Centre d’évaluation

Serma Safety & Security

14 rue Galilée, CS 10071, 33608 Pessac Cedex, France

Accords de reconnaissance applicables

CCRA

SOG-IS

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

1.1. Présentation du produit

Le produit évalué est le microcontrôleur « ST31G480 E01 including optional cryptographic library NESLIB v6.2.1, optional technologies MIFARE DESFire EV1 v4.8.12 and MIFARE Plus X v2.4.6, including optional cryptographic library NESLIB and optional technologies MIFARE DESFire EV1 and MIFARE Plus X » 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*, l'activation des différentes interfaces de communication, l'adaptation aux types d'antennes, l'activation des ressources matérielles dédiées à MIFARE, 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 les packages « *loader dedicated for usage in secured environment only* » et « *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 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 au chiffrement cryptographique à clés asymétriques ;
- le support à la génération de nombres non prédictibles ;

- le service optionnel de bibliothèque cryptographique NesLib offrant des fonctionnalités RSA, SHA, ECC, DRBG, ainsi que la génération sécurisée de nombres premiers et de clés RSA ;
- la technologie (optionnelle) MIFARE DESFire EV1 ;
- la technologie (optionnelle) MIFARE Plus X.

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 mémoires utilisateur (volatile et non volatile) ;
- des modules de sécurité : unité de protection des mémoires (MPU), générateur d'horloge, surveillance et contrôle de la sécurité, contrôle d'intégrité ;
- des coprocesseurs cryptographiques pour accélérer les calculs AES, Triple DES et de cryptographie asymétrique ;
- un générateur physique d'aléa (TRNG).

La partie logicielle est composée de :

- le logiciel dédié au démarrage du produit (*boot sequence*) ;
- le système d'exploitation dédié aux tests (OST) ;
- le logiciel dédié au chargement d'application sur la *FLASH* ;
- les différents drivers nécessaires au développeur du logiciel embarqué ;
- l'ensemble de commandes hautement protégées dédiées à des diagnostics uniquement effectués par le développeur après authentification ;
- optionnellement, la bibliothèque cryptographique NesLib v6.2.1, offrant des services RSA (dont la génération de clés), courbes elliptiques, hachage, génération de nombres premiers, génération d'aléa déterministe (DRBG) ;
- optionnellement, les technologies MIFARE DESFire EV1 v4.8.12 et MIFARE Plus X v2.4.6.

1.2.4. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

Eléments de configuration		Données d'identification lues
Identification du microcontrôleur ST31G480 D01	*IC maskset name*	K8L0B
	IC version J	43
	Master identification number	00 B8
Identification des logiciels embarqués	*Firmware version 3.0.1*	03 00 01
	OST version 3.4	34
Identification des bibliothèques optionnelles	*NesLib version 6.2.1*	01 06 02 01
	MIFARE DESFire EV1 v4.8.12	04 08 0C 00
	MIFARE Plus X v2.4.6	02 04 06 00

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 manuel utilisateur « UM_ST31_FW », voir [GUIDES].

1.2.5. Cycle de vie

Le cycle de vie du produit est décrit dans la cible de sécurité (voir Table 3 de [ST] au chapitre 1.7) ; il est conforme au cycle de vie décrit dans [PP0084] et rappelé dans la table ci-après. Les sites impliqués dans le cycle de vie pour les phases 2, 3 et 4 sont indiqués dans la cible de sécurité (voir [ST] au chapitre 1.8, table 16 et [SITES]). Le produit est livré soit après la phase 3 sous forme de *wafers* (sciés ou non), soit après la phase 4 une fois packagé, en fonction de la demande du client. Il peut être livré configuré en mode administrateur ou utilisateur (voir chapitre 1.7 de la [ST]).

Phase	Nom	Description
1	Développement du logiciel embarqué sur le microcontrôleur	Développement du logiciel embarqué sur le microcontrôleur Spécification des exigences de pré-personnalisation du microcontrôleur
2	Développement du microcontrôleur	Design du microcontrôleur Développement des logiciels dédiés au fonctionnement du microcontrôleur
3	Fabrication et tests du microcontrôleur	Intégration et fabrication du masque photographique Fabrication du microcontrôleur Test du microcontrôleur Pré-personnalisation du microcontrôleur
4	Packaging du microcontrôleur	Packaging (et test) du microcontrôleur Pré-personnalisation (si nécessaire)
5	Processus de finalisation du produit	Processus de finalisation du produit de composition Test du produit de composition
6	Personnalisation du produit	Personnalisation du produit de composition Test du produit de composition
7	Utilisation finale du produit	Utilisation finale du produit de composition par son émetteur et ses consommateurs

Au regard du cycle de vie mentionné au chapitre 1.2.5, le produit évalué est celui obtenu à l'issue de la phase 3 lorsqu'il est livré sous forme de *wafer*, ou à l'issue de la phase 4 lorsqu'il est livré dans un packaging.

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 produit « ST31G480 D01 » dans les différentes configurations offertes, voir §1.2.4 ci-dessus et [GUIDES]. Toutes autres applications, y compris éventuellement les routines embarquées pour les besoins de l'évaluation, ne font 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 du produit ST31G480 D01, including optional cryptographic library NESLIB v6.2.1 and optional technologies MIFARE DESFire EV1 v4.8.12 and MIFARE Plus X v2.4.6 certifié en février 2019 sous la référence ANSSI-CC-2019/12, voir [CER-2019/12].
Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 28 janvier 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 « ST31G480 E01 including optional cryptographic library NESLIB v6.2.1, optional technologies MIFARE DESFire EV1 v4.8.12 and MIFARE Plus X v2.4.6 » 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, ASE_TSS.2, 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 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].

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 :

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[2], 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**	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	**2**	Well-structured internals
	ADV_SPM						1	1		
	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								**1**	Basic flaw remediation
	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	**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 : - ST31G480 E01 including optional cryptographic library NESLIB, and optional technologies MIFARE DESFire EV1 and MIFARE Plus X Security Target, référence SMD_ST31G480_ST_18_001, Révision E01.2, octobre 2018. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - ST31G480 E01 including optional cryptographic library NESLIB, and optional technologies MIFARE DESFire EV1 and MIFARE Plus X Security Target for composition, référence SMD_ST31G480_ST_18_002, Révision E01.2, décembre 2018.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report – ELIXIR4 project, référence Elixir4_ETR_v1.2, version 1.2, 27 février 2019, *SERMA SAFETY & SECURITY*. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - ETR Lite for Composition ELIXIR4 Project, référence Elixir4_ETR_v1.2_lite, version 1.2, 27 février 2019, *SERMA SAFETY & SECURITY*.
[CONF]	Liste de configuration du produit : - ST31 K8L0 Configuration List E01, référence SMD_ST31G480_J_CFGL_E01, version 2.0, 12 décembre 2018, STMicroelectronics ; - Neslib 6.2.1 for ST31G480 revJ configuration List, référence SSS_NESLIB_6.2.1_CFGL_18_002, version 1.0, 16 novembre 2018 ; - Mifare DESFire EV1 Library 4.8.12 on ST31G480 revH - configuration list, référence SSS_MIFARE_CFGL_17_002, version 01-00, 27 avril 2017 ; - Mifare PLus X library 2.4.6 on ST31G480 revH - configuration list, référence SSS_MIFARE_CFGL_17_001, version 01-00, 28 mars 2017.
[CER-2019/12]	Rapport de certification ANSSI-CC-2019/12, ST31G480 D01, including optional cryptographic library NESLIB and optional technologies MIFARE DESFire EV1 and MIFARE Plus X. *Certifié par l'ANSSI en février 2019 sous la référence ANSSI-CC-2019/12.*
[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.*

[GUIDES]	Guides du produit : - ST31G Platform - ST31G480 - Secure dual interface microcontroller with enhanced security and up to 480 Kbytes of Flash memory – Datasheet – production data, référence DS_ST31G480, revision 4, 13 avril 2018 ; - ARM Cortex SC000 Technical Reference Manual, référence ARM DDI 0456, issue A, septembre 2010 ; - ARMv6-M Architecture Reference Manual, référence ARM DDI 0419, issue C, septembre 2017 ; - User manual - ST31 Firmware V3, référence UM_ST31G_H_FWv3, révision 6, 28 février 2018 ; - ST31G480 Flash loader installation guide - User manual, référence UM_31G_FL, revision 2, février 2016 ; - NesLib 6.2 library - User manual, référence UM_NesLib_6.2, version 1.0, juin 2018 ; - ST31G and ST31H Secure MCU family - NesLib 6.2 security recommendations, référence AN_SECU_ST31G_H_NESLIB_6.2, version 4.0, octobre 2018 ; - Release note Neslib 6.2.1 for the ST31G and ST31H platforms, référence RN_ST31_NESLIB_6.2.1, version 2.0, 21 septembre 2018 ; - ST31G and ST31H Secure MCU platforms Security Guidance, référence AN_SECU_ST31G_H, révision 5, octobre 2018 ; - ST31G and ST31H - AIS31 Compliant Random Number User Manual, référence UM_31G_31H_AIS31, version 1.0, janvier 2015 ; - True Random Number Generator Description & Architecture, référence SMD_TRNG_TD_09_001, version 3.02, 27 novembre 2015 ; - ST31 - AIS31 Reference implementation - Startup online and total failure tests - Application Note, référence AN_31G_31H_AIS31, version 1, janvier 2015 ; - K8L ST31G480 AIS31 Characterization report, PEN_ST31G480_CR_14_005, v1.0, novembre 2014 ; - MIFARE DESFire EV1 library 4.8 for ST31G480 - User manual, référence UM_31_MFDF_EV1_4.8, version 4.0, février 2016 ; - MIFARE DESFire EV1 library 4.8.12 for ST31G480 - Appli note, référence AN_ST31G480_MFD_Lib, version 3.0, mars 2017 ; - MIFARE DESFIRE EV1 interface specification User manual, référence UM_Mifare_Desfire_EV1_Interface, version 5.0, mars 2017 ; - MIFARE Plus X library 2.4 for ST31G480 - User manual, référence UM_MIFARE_PLUS_X_2_4, version 5.0, décembre 2016 ; - MIFARE Plus X library 2.4.6 for ST31G480 - Appli note, référence AN_ST31G480_MFPX_Lib, revision 1, décembre 2016.

[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - 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 – ChipBond (JY & LH) Taiwan site audit, référence 17-0317_ChipBond_SVR-M_v1.0, version 1.0, 12 mars 2018 ; - 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.

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 2.9, janvier 2013.
[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.