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-2017/73

Microcontrôleur sécurisé ST33G1M2A1 révision H, Firmware révision 1.3.2, incluant optionnellement la bibliothèque cryptographique Neslib 6.0.3 et la bibliothèque SFM 1.0.7

Paris, le 18 décembre 2017

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ 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-2017/73

Nom du produit

Microcontrôleur sécurisé ST33G1M2A1 révision H, Firmware révision 1.3.2, incluant optionnellement la bibliothèque cryptographique Neslib 6.0.3 et la bibliothèque SFM 1.0.7

Référence/version du produit

Référence maskset K8H0A, révision interne H, firmware révision 1.3.2

Conformité à un profil de protection

Security IC Platform Protection Profile version v1.0

certifié BSI-CC-PP-0035-2007 le 23 août 2007

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeur

ST Microelectronics

190, avenue Celestin Coq, ZI de Rousset, 13106 Rousset, France

Commanditaire

ST Microelectronics

190, avenue Celestin Coq, ZI de Rousset, 13106 Rousset, France

Centre d'évaluation

THALES (TCS – 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 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 sécurisé ST33G1M2A1 révision H, Firmware révision 1.3.2, incluant optionnellement la bibliothèque cryptographique Neslib 6.0.3 et la bibliothèque SFM 1.0.7» développé par *ST MICROELECTRONICS*.

Les produits dérivés du ST33G1M2A1 sont définis par une série d'options matérielles ou logicielles configurables par le client final. Ces options concernent la taille mémoire non volatile (FLASH), la plage de température supportée (105°C, 125°C ou 150°C), la bibliothèque cryptographique Neslib et la bibliothèque SFM.

Les usages possibles de ce produit sont multiples (sécurisation d'une communication entre deux véhicules et/ou entre un véhicule et un serveur, système d'appel d'urgence *eCalls*, authentification et vérification de l'intégrité d'un module électronique, communication de machine à machine en environnement industriel, contrôle d'accès, transport, santé, électronique grand public, 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.

La cible de sécurité est conforme au profil de protection [PP0035].

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- l'initialisation de la plate-forme matérielle et des attributs ;
- la gestion sécurisée du cycle de vie ;
- l'intégrité logique du produit ;
- les tests du produit ;
- des contrôles d'accès aux mémoires dont un dédié à la bibliothèque embarquée ;
- la protection physique ;
- 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 au chiffrement cryptographique à clés asymétriques ;
- le support à la génération de nombres non prédictibles ;
- le service optionnel de bibliothèque SFM version 1.0.7 offrant des services de gestion de la mémoire FLASH assurant l'atomicité, l'endurance et la correction d'erreurs ;
- le service optionnel de bibliothèque cryptographique NesLib version 6.0.3 offrant, suivant la configuration choisie :
    - des implémentations RSA, ECC, SHA, DES et AES ;
    - un générateur de bits déterministe ;

- un service de génération sécurisée de nombres premiers et de clés RSA.

1.2.3. Architecture

L'architecture matérielle du microcontrôleur ST33G1M2A1 est illustrée par la figure 1.

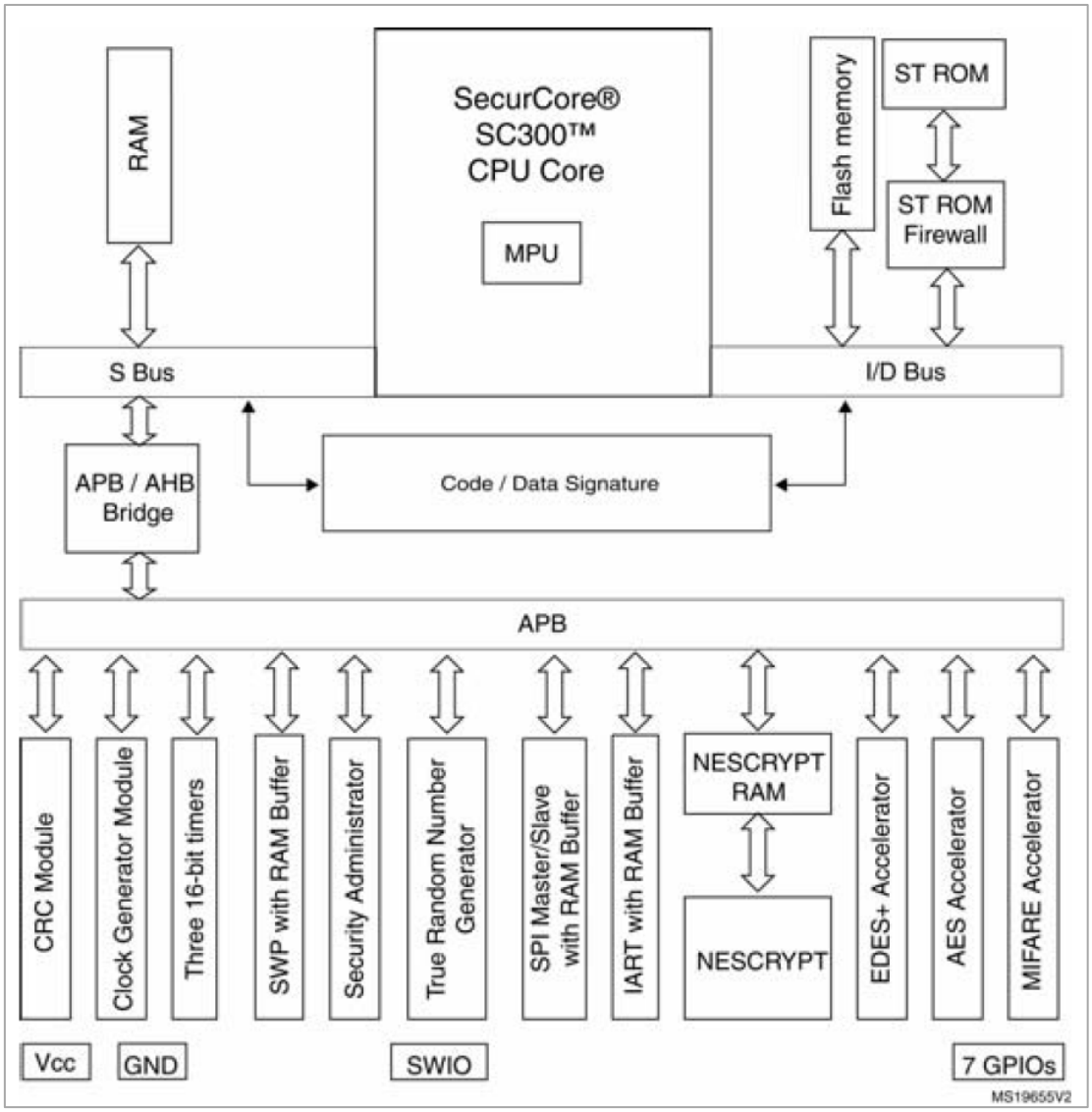


Figure 1 : Architecture

Elle est composée :

- d'un processeur « ARM® SecurCore® SC300™ 32-bit RISC core » ;
- de mémoires :
  - FLASH (avec contrôle d'intégrité) configurable de 384 Ko à 1280 Ko avec une granularité de 128 Ko pour le stockage des données et des logiciels dédiés de test et chargement de la mémoire (FLASH *loader*) ;
  - ROM pour le stockage des logiciels dédiés ;
  - RAM ;
- de modules fonctionnels : trois compteurs 16-bits dont un configurable en *watchdog*, un bloc de gestion des entrées/sorties en mode contact (IART ISO 7816-3), un bloc de

gestion d'interface série SPI[1] (fonctionnant en modes *Slave* et *Master*) et un bloc de gestion d'interface simple fil SWP[2] ;

- de modules de sécurité : une unité de protection des mémoires (MPU[3]), une unité de protection mémoire dédiée aux bibliothèques (LPU), un générateur de nombres aléatoires (TRNG), un générateur d'horloge, un module administrateur de la sécurité qui surveille et contrôle l'exécution de la politique de sécurité, une gestion de l'alimentation, un contrôle d'intégrité des mémoires, un mécanisme de détection de fautes ;
- de 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 cryptographiques à clé publique.

En plus de ces composants matériels, la TOE embarque également :

- le composant logiciel dédié (OST) au démarrage du composant (*boot sequence*) et au test du microcontrôleur (ce logiciel stocké en ROM n'est plus accessible une fois la TOE en configuration *Issuer* ou *User*) ;
- le composant logiciel dédié (*firmware*) à la gestion du cycle de vie et du chargement de la mémoire FLASH (*loader*) et à son interfaçage avec l'application (*drivers*). Ce composant est stocké en mémoire ROM et en mémoire FLASH.

De manière optionnelle, le client peut également choisir d'intégrer :

- la bibliothèque cryptographique NesLib version 6.0.3 fournissant les implémentations des fonctions cryptographiques décrites au chapitre 1.2.2. La bibliothèque NesLib est embarquée partiellement ou en totalité selon son besoin, avec le code client, dans la mémoire FLASH du produit ;
- la bibliothèque SFM version 1.0.7 (décrite au chapitre 1.2.2).

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 2.1 « TOE Identification » :

Eléments de configuration		Données d'identification lues
Identification du microcontrôleur ST33G1M2A1	*IC version H*	**48**h
	Master identification number ST33G1M2	**01BC**h
	IC maskset name	**K8H0A**
Identification des logiciels embarqués	*Firmware version : 1.3.2*	**010302**h
	OST version OST_3322	**0022**h
Identification des bibliothèques	*NesLib version 6.0.3*	**01060003**h
	SFM version 1.0.7	**00010007**h

[1] *Serial Peripheral Interface.*
[2] *Single Wire Protocol.*
[3] *Memory Protection Unit.*

Le nom du *maskset* **K8H0A** est donné dans [CONF] ; il peut être lu directement sur la surface du composant. Les autres éléments peuvent être vérifiés par appel à la méthode « Get Product Information ». La procédure d'identification est décrite dans le « *Firmware User Manual* », voir [GUIDES].

1.2.5. Cycle de vie

Le cycle de vie du produit est décrit dans [ST] ; il est conforme au cycle de vie de sept phases décrit dans [PP0035] :

Phase	*Name*	*Description*
1	*IC embedded software development*	*Security IC embedded software development specification of IC pre-personalisation requirements*
2	*IC development*	*IC design* *IC dedicated software development*
3	*IC manufacturing*	*Integration and photomask fabrication* *IC production* *IC testing* *Pre-personalisation*
4	*IC packaging*	*IC packaging (and testing)* *Pre-personalisation if necessary*
5	*Composition product integration*	*Composite product finishing process* *Composite product testing*
6	*Personalisation*	*Composite product personalisation* *Composite product testing*
7	*Operational usage*	*Composite product usage by its issuers and consumers*

Les phases suivantes ont été considérées pendant l'évaluation de ce produit :
- Phase 2 : développement ;
- Phase 3 : fabrication et test ;
- Phase 4 (optionnelle) : conditionnement et test final.

La TOE est délivrée, en fonction des besoins du client, après la phase 3 sous forme de *wafers* ou après la phase 4 sous le format du produit final.

Le produit gère son cycle de vie sous la forme de trois configurations :
- la configuration *Test*. A la fin de sa fabrication, le microcontrôleur est testé à l'aide du logiciel dédié OST présent en ROM. Cette configuration est ensuite bloquée de manière irréversible lors du passage en configuration *Issuer* ou *User* ;
- la configuration *Issuer* comprenant :
  - le mode *Final Test OS* : mode protégé permettant aux sites d'assemblage d'effectuer des tests restreints pour vérifier la qualité de l'assemblage, réservé à *ST MICROELECTRONICS* ;
  - le mode *Install* (ou *Flash loader*): mode protégé dédié à l'installation du loader, réservé à *ST MICROELECTRONICS* ;
  - le mode *User Emulation :* mode protégé permettant l'exécution d'une application chargée en mémoire FLASH ;
  - le mode *Diagnosic* : mode réservé à *ST MICROELECTRONICS*,
- la configuration *User* comprenant :

- le mode *User :* mode final d'utilisation du microcontrôleur qui fonctionne alors sous le contrôle du logiciel embarqué du composant ; le logiciel de test n'est plus accessible ; les utilisateurs finaux ne peuvent utiliser le microcontrôleur que dans cette configuration ;
- le mode *Diagnosic* : mode réservé à *ST MICROELECTRONICS*.

La configuration *Issuer* est bloquée de manière irréversible après le passage en configuration *User*. La TOE peut être livrée en configuration *Issuer* ou *User*. Le chargement de l'application par l'utilisateur en configuration *Issuer* doit être réalisé dans un environnement sécurisé.

Le produit a été développé sur les sites suivants :

***ST MICROELECTRONICS* Rousset** 190 Avenue Célestin Coq ZI de Rousset-Peynier 13106 Rousset Cedex France	***ST MICROELECTRONICS* Grenoble** 12 rue Jules Horowitz BP 217 38019 Grenoble Cedex France	***ST MICROELECTRONICS* Sophia** 635 rue des lucioles 06560 Valbonne France
***ST MICROELECTRONICS* Rennes** 10 rue de Jouanet ePark 35700 Rennes, France	***ST MICROELECTRONICS* Zaventem** Green Square, Lambroekstraat 5 Building B, 3rd floor 1831 Diegem/Machelen Belgique	***ST MICROELECTRONICS* Crolles** 850 rue Jean Monnet 38926 Crolles France
***ST MICROELECTRONICS* Calamba** 9 Mountain Drive, LISP II, Brgy La Mesa Calamba, 4027 Philippines	***ST MICROELECTRONICS* Tao Payoh** 629 Lorong 4/6 Toa Payoh Singapore 319521 Singapour	***ST MICROELECTRONICS* Shenzhen** 16 Tao hua Rd. Futian free trade zone 518048 Shenzhen République Populaire de Chine
***STMICROELECTRONICS* Ang Mo Kio** 5A Serangoon N. Avenue 5, Singapore 554574 Singapour	***ST MICROELECTRONICS* Loyang** 7 Loyang Drive Singapore 508938 Singapour	***ST MICROELECTRONICS* Bouskoura** 101 Boulevard des Muriers BP97 20180 Bouskoura Maroc
***ST MICROELECTRONICS* Muar** Sdn. Bhd. Tanjong Agas Industrial area. P.o. Box 28, 84007 Muar, Johor Malaysie	***ST MICROELECTRONICS* Tunis** Cite Technologique des communications BP21,2088 La Gazelle Tunisie	***CMP* Gardanne** George Charpark 880 avenue de Mimet 13541 Gardanne France
TSMC Fab 2-5, 121 Park Avenue 3 Hsinchu science park Hsinchu 300-77 Taïwan République de Chine	***TSMC*** Fab 14, 1-1 Nan Ke Rd Tainan science park, Tainan 741-44 Taïwan République de Chine	***TSMC*** Fab 7 (server room only) Li-Hsin Rd.6, Hsinchu science park Hsinchu 300-78 Taïwan République de Chine

***DPE* Agrate** Via C. Olivetti 2/A I-20041 Agrate Italie	***DNP* Kamifukuoka** 2-2-1 Kami Fukuoka Fujimino-shi Saitama-Ken 356-8507 Japon	***AMKOR*** ATT1: 1F, N°1, Kao-Ping Sec, Chung-Feng Rd, Lungtan Township Taoyuan County 325, Taïwan Republique de Chine
AMKOR ATT3: 11 Guangfu road, Hsinchu Industrial Park, Hukou County Hsinchu 303 Taïwan Republique de Chine	***AMKOR*** ATP3/4, 119 N. Science Avenue, Laguna Technopark, Binan, Laguna, 4024 Philippines	***AMKOR*** ATP1, Km 22 East Service Rd. South superhighway Mantipula City 1771 Philippines
***STATS CHIPPAC* (SCT)** No 176-5, 6 Lane Hualung Chun, Chiung Lin, 307 Hsinchu, Taïwan Republique de Chine	***STATS CHIPPAC* (SCS)** 5 Yishun St. 23, Singapore 768442 Singapour	***SMARTFLEX*** 27 UBI rd 4, MSL building #04-01 Singapore 408618 Singapour

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

1.2.6. Configuration évaluée

Le certificat porte sur la TOE définie au paragraphe 1.2.1 en mode *Issuer* et *User*.
Les configurations testées par l'évaluateur sont des combinaisons des différentes options matérielles et logicielles de la TOE (activation ou désactivation des coprocesseurs cryptographiques, de l'unité de protection des librairies, des interfaces entrées/sorties, mise en œuvre des librairies optionnelles).

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [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 « Microcontrôleurs sécurisés ST33G1M2A et ST33G1M2M révision G, Firmware révision 1.3.2, incluant optionnellement la bibliothèque cryptographique Neslib 4.2.10 » certifié le 16 février 2017 sous la référence [CER-2017/02].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 30 octobre 2017, 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 visé.

2.4. Analyse du générateur d'aléas

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

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 « Microcontrôleur sécurisé ST33G1M2A1 révision H, Firmware révision 1.3.2, incluant optionnellement la bibliothèque cryptographique Neslib 6.0.3 et la bibliothèque SFM 1.0.7 » 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.

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 « Microcontrôleur sécurisé ST33G1M2A1 révision H, Firmware révision 1.3.2, incluant optionnellement la bibliothèque cryptographique Neslib 6.0.3 et la bibliothèque SFM 1.0.7 » à des attaques qui sont fortement génériques du fait de l'absence d'application spécifique embarquée. Par conséquent, la sécurité d'un produit complet construit sur le micro-circuit ne pourra être appréciée que par une évaluation du produit complet, laquelle pourra être réalisée en se basant sur les résultats de l'évaluation citée au chapitre 2.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

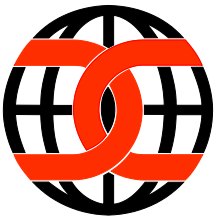
Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puces 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	**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 : - « ST33G platform ST33G1M2A1 maskset K8H0A version H, with firmware revision 1.3.2, optional cryptographic library NesLib 6.0.3, and optional library SFM 1.0.7 - Security target », référence SMD_ST33G_ST_16_001, révision 1.03, 27/10/2017. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - « ST33G platform ST33G1M2A1 maskset K8H0A version H, with firmware revision 1.3.2, optional cryptographic library NesLib 6.0.3, and optional library SFM 1.0.7 - Security target for composition », référence SMD_ST33G_ST_16_002, révision 1.03, 27/10/2017.
[RTE]	Rapport technique d'évaluation : - « Evaluation Technical Report - Project LATOUR AM2 », référence LATAM2_ETR, révision 3.0, 30/10/2017. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - « Evaluation Technical Report for composition evaluation Project LATOUR AM2 », référence LATAM2_ETRLite, révision 4.0, 08/12/2017.
[CONF]	Listes de configuration du produit : - « ST33G1M2A1 & derivatives (HW revH, FW 1.3.2, opt NesLib 6.0/SFM 1.0) – CFG LIST », référence SMD_33G_CFGL_16_002, révision 1.01, 07/07/2017 ; - « NesLib 6.0.3 for ST33 Configuration List », référence SSS_NesLib603ST33_CFGL_17_001, révision 1.0, 30/06/2017 ; - « Storekeeper Library 1.0 on ST33G1M2A1 rev. H Configuration List », référence SSS_STOREKEEPER_CFGL_17_001, révision 1.0, 27/04/2017. Liste de la documentation : - « ST33G1M2A, ST33G1M2M and derivatives CC EAL 5+ Project Evaluation (HW rev H, Firmware 1.3.2 and optional NesLib 6.0 / SFM 1.0) – Documentation report », référence SMD_ST33G1M2AM_DR_16_002, révision 1.03, 27/10/2017.

[GUIDES]	Guides d'utilisation du produit : - « Datasheet : ST33G1M2A - Automotive-grade secure MCU with 32-bit ARM SecurCore SC300 CPU and high-density Flash memory », référence DS_ST33G1M2A, révision 1.0, février 2017 ; - « Application note : ST33G and ST33h Secure MCU platforms Security guidance », référence AN_SECU_ST33, révision 5.0, février 2017 ; - « Application note : ST33G and ST33H – AIS Reference importation : Start-up, on-line and total failure tests », référence AN_33G_33H_AIS31, révision 1.0, octobre 2013 ; - « User manual : ST33G and ST33H – AIS31 Compliant Random Number », référence UM_33G_33H_AIS31, version 3.0, octobre 2015 ; - « Cortex-M3 SC300 revision r0p0 Technical Reference Manuel », référence ARM_DDI_0037, révision F ; - « User manual : ST33G1m2A/ST33G1M2M firmware », référence UM_ST33G1M2A_M_FW, révision 6.0, mai 2017 ; - « User manual : Flash memory loader installation guide for the ST33G1m2A and ST33G1M2M platforms », référence UM_33GA_FL, révision 3.0, août 2016 ; - « User manual : NesLib cryptographic library NesLib 6.0 », référence UM_NESLIB_6.0, révision 2.0, mars 2017 ; - « Application note : ST33 Secure MCU platforms NesLib 6.0 security recommandations », référence AN_SECU_ST33_NESLIB_6.0, révision 1.0, mars 2017 ; - « Application note : StoreKeeper library 1.0 Security recommandations », référence AN_SECU_StoreKeeper, révision 1.0, janvier 2017 ; - « User manual : StoreKeeper v1.0 », référence UM_StoreKeeper, révision 3.0, novembre 2016 ; - « User manual : Blackbox project – Developeur Kit system overview », référence OPE_UG_09_001, révision 2.02, août 2013 ; - « Datasheet : BlackBox – ST BlackBox interface », référence DS_BLACKBOX, révision 2, octobre 2012.
[CER-2017/02]	Rapport de certification ANSSI-CC-2017/02 « Microcontrôleurs sécurisés ST33G1M2A et ST33G1M2M révision G, Firmware révision 1.3.2, incluant optionnellement la bibliothèque cryptographique Neslib 4.2.10 » émis le 16 février 2017, ANSSI
[PP0035]	Protection Profile, Security IC Platform Protection Profile, version 1.0, juin 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.*

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, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001; - Part 2: Security functional components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002; - Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[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 September 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.