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-2015/61

Microcontrôleur sécurisé ST33G1M2 révision F, Firmware révisions 9 et A, incluant optionnellement la bibliothèque cryptographique Neslib versions 4.1 et 4.1.1 et la bibliothèque MIFARE4Mobile ® 2.1.0

Paris, le 8 janvier 2016

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.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2015/61

Nom du produit

Microcontrôleur sécurisé ST33G1M2 révision F, Firmware révisions 9 et A, incluant optionnellement la bibliothèque cryptographique Neslib versions 4.1 et 4.1.1 et la bibliothèque MIFARE4Mobile ® 2.1.0

Référence/version du produit

Référence maskset K8H0A, révision interne F, firmware révisions 9 et A

Conformité à un profil de protection

[BSI_PP_0035-2007], version v1.0
Security IC Platform Protection Profile

Critères d'évaluation et version

CC version 3.1 révision 4

Niveau d'évaluation

EAL5 Augmenté
ALC_DVS.2 et AVA_VAN.5

Développeur

STMicroelectronics

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

Commanditaire

STMicroelectronics

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

Centre d'évaluation

THALES (TCS – CNES)

18 avenue Edouard Belin, BPI1414, 31401 Toulouse Cedex 9, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit 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 ST33G1M2 révision F, Firmware révisions 9 et A, incluant optionnellement la bibliothèque cryptographique Neslib versions 4.1 et 4.1.1 et la bibliothèque MIFARE4Mobile ® 2.1.0 » développé par STMicroelectronics.

Les produits dérivés du ST33G1M2 inclus dans cette plateforme sont définis par une série d'options matérielles ou logicielles configurables par le client final. Ces options concernent la taille de mémoire non volatile FLASH, l'activation des coprocesseurs cryptographiques, de l'unité de protection des librairies (LPU[1]), des interfaces entrées/sorties, de la bibliothèque cryptographique Neslib et de la bibliothèque MIFARE4Mobile. Cette bibliothèque peut inclure les fonctionnalités Mifare® DESFire® EV1 ou Mifare® Classic® (cette dernière ne faisant pas partie du périmètre de certification).

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,...) 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 [BSI_PP_0035-2007]. La conformité est démontrable.

1.2.2. 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 3.1 « TOE identification » et [GUIDES]) :

- informations inscrites physiquement sur la surface du composant :
  - identifiant du produit : **K8H0A** (révision majeure du *maskset* correspondant à la plateforme ST33G1M2) ;
  - identifiant du site de fabrication : **ST_4** (STMicroelectronics Rousset), **ST_3** (STMicroelectronics Crolles), **ST_2** (TSMC) ;
  - version du logiciel dédié OST[2] : **YJE** ;

[1] *Library Protection Unit.*
[2] *Operating System for Test.*

- informations logiques disponibles dans la mémoire de la puce :
    - tous les identifiants matériels et logiciels du produit sont obtenus à partir de l'API et de la méthode *Get Product Information* tel que documenté dans le *Firmware User Manual* (voir [GUIDES]). Cette API permet de tracer l'ensemble des options effectivement configurées pour chaque dérivé commercial avec principalement:
        - identifiant du produit : l'API retourne le *Master ID* qui est l'identifiant du produit maître (valeur **0061**h pour du produit ST33G1M2 et valeur **0105**h pour la version améliorée ST33I1M2 du produit ST33G1M2) ainsi que le *Product ID* qui est l'identifiant propre à chacun des produits (valeur **00xx**h : pour obtenir la valeur de chaque dérivé commercial, se reporter aux [GUIDES]). Par exemple, le dérivé ST33G1M2LC retournera la valeur 0061h pour le *Master ID* et la valeur 0069h pour le *Product ID* ;
        - révision du produit : **46**h correspondant à la lettre de révision F interne du produit, caractère ASCII codé en format hexadécimal écrite sur un octet (voir [GUIDES]) ;
        - identifiant des logiciels dédiés :
            - **22**h : version du logiciel dédié OST, valeur en hexadécimal écrite sur un octet (voir [GUIDES]) ;
            - **09**h ou **0A**h : version interne du *firmware*, valeur en hexadécimal écrite sur un octet (voir [GUIDES]) ;
            - **1410**h ou **1411**h: références respectives de la bibliothèque cryptographique NesLib en version 4.1 et en version 4.1.1 (voir [GUIDES]) ;
            - **00000004**h ou **00000504**h: références de la bibliothèque Mifare4Mobile incluant respectivement soit MIFARE® DESFire® EV1 soit la combinaison MIFARE® DESFire® EV1 et MIFARE® Classic® (voir [GUIDES]) ;

      informations obtenues avec la commande « NesLib_GetVersion » :
        - **9410**h : référence de la bibliothèque cryptographique NesLib version 4.1 ;
        - **9411**h : référence de la bibliothèque cryptographique NesLib version 4.1.1 (voir [GUIDES] pour la description de l'API) ;
    - informations obtenues avec la commande « M4MAPI_LibraryGetVersion » :
        - **020100**h : référence de la bibliothèque de technologie MIFARE4Mobile en révision 2.1.0 (voir [GUIDES] pour la description de l'API).

1.2.3. 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 aux bibliothèques embarquées ;
- 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 cryptographique NesLib v4.1 et v4.1.1 offrant, suivant la configuration choisie, des implémentations RSA, SHA, ECC et un service de génération sécurisée de nombres premiers et de clés RSA ;
- le service optionnel de bibliothèque MIFARE4Mobile incluant les fonctionnalités MIFARE® DESFire® EV1.

1.2.4. Architecture

L'architecture matérielle du microcontrôleur ST33G1M2 est illustrée par la figure 1.

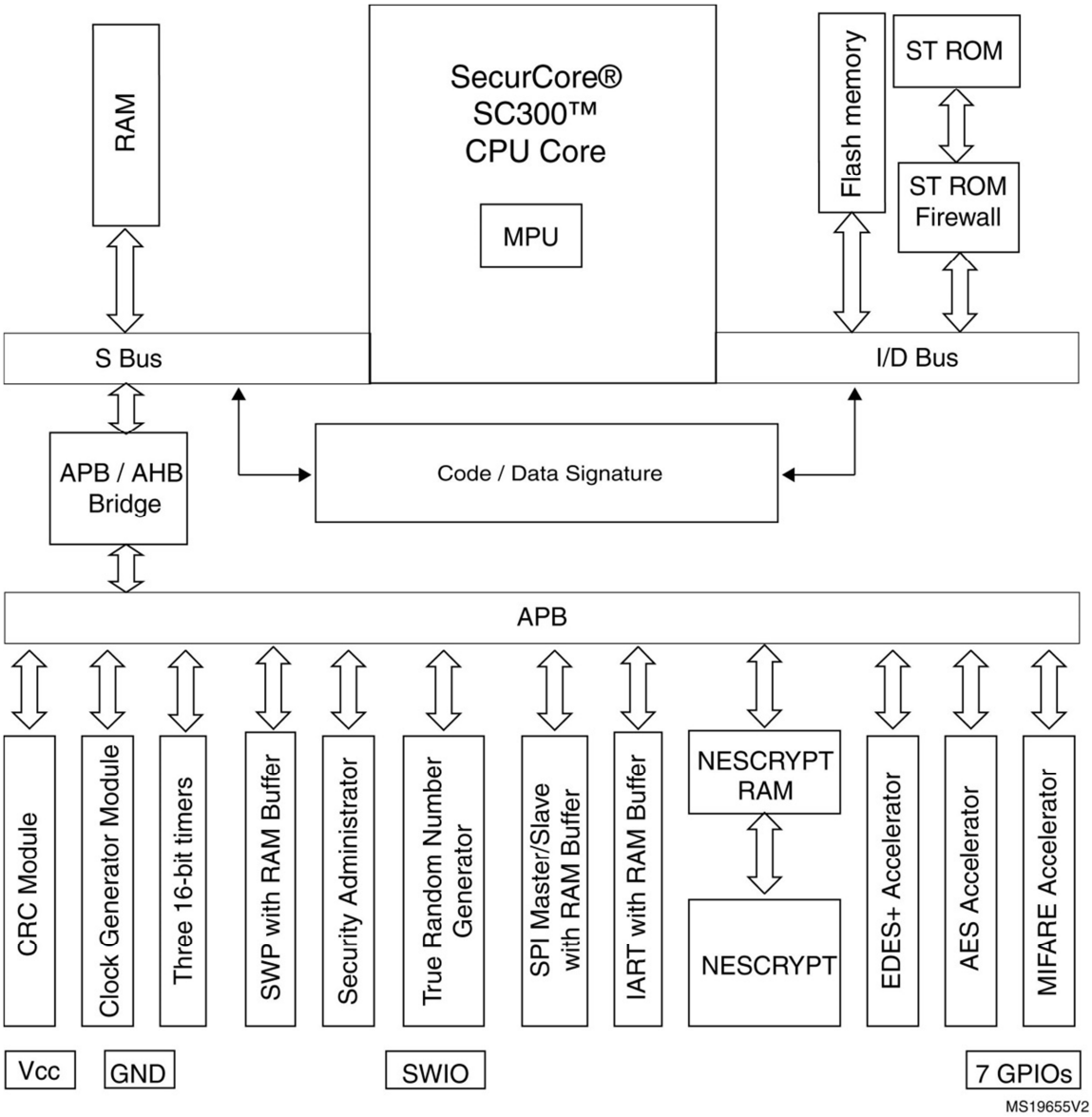

Figure 1: Architecture

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 optionnellement un bloc de gestion d'interface simple fil SWP[2] ;
- de modules de sécurité : unité de protection des mémoires (MPU[3]), unité de protection mémoire dédiée aux bibliothèques (LPU), un générateur de nombres aléatoires (TRNG), générateur d'horloge, surveillance et contrôle de la sécurité, gestion de l'alimentation, contrôle d'intégrité des mémoires, 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 une bibliothèque cryptographique (NesLib version 4.1 ou version 4.1.1) fournissant des implémentations des fonctions cryptographiques. Parmi celles-ci, les fonctions RSA, SHA, ECC, un service de génération sécurisée de nombres premiers et de clés RSA et un service de post-traitement déterministe des nombres aléatoires sont incluses dans la cible d'évaluation du produit. La bibliothèque Neslib version 4.1 ou version 4.1.1 est embarquée partiellement ou en totalité selon son besoin, avec le code client, dans la mémoire non volatile (FLASH) du produit.
Egalement de manière optionnelle, le client peut choisir d'intégrer la bibliothèque MIFARE4Mobile en version 2.1.0. Cette bibliothèque inclut les fonctionnalités MIFARE DESFire® EV1 et MIFARE® Classic. Les fonctionnalités MIFARE® Classic sont en dehors du périmètre de certification.

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

Selon son besoin, le client embarque en totalité la ou les bibliothèques dans la mémoire du produit.

1.2.5. Cycle de vie

Le cycle de vie du produit est décrit dans la cible de sécurité (voir [ST]).
Il comprend les sites suivants pour la phase 2 (développement), la phase 3 (fabrication et test) et la phase 4 (conditionnement et test final):

STMicroelectronics Smartcard IC division 190 Avenue Célestin Coq ZI de Rousset-Peynier 13106 Rousset Cedex France	**STMicroelectronics** 5A Serangoon North Avenue 5 554574 Singapour Singapour
STMicroelectronics 635 rue des lucioles 06560 Valbonne France	**STMicroelectronics** 12 rue Jules Horowitz BP217, 38019 Grenoble Cedex France
STMicroelectronics Green Square Lambroekstraat 5, Building B, 3rd floor, 1831 Diegem/Machelen Belgique	**STMicroelectronics** 10 rue de Jouanet ePark 35700 Rennes France
Dai Nippon Printing Co., Ltd 2-2-1 Fukuoka Kamifukuoka-shi Saitama-Ken 356-8507 Japon	**Dai Nippon Printing Europe** Via C. Olivetti 2/A I-20041 Agrate Brianza Italie
STS Microelectronics 16 Tao hua Rd. Futian free trade zone 518048 Shenzhen République Populaire de Chine	**ST Microelectronics** 629 Lorong 4/6 Toa Payoh 319521 Singapour Singapour
TSMC Fab 14, 1-1 Nan Ke Rd Tainan science park, Tainan 741-44 Taïwan République de Chine	**TSMC** Fab 2-5, Li-Hsin Rd. 6 Hsinchu science park Hsinchu 300-78 Taïwan République de Chine

ST Microelectronics 850 rue Jean Monnet 38926 Crolles France	**Smartflex** UBI rd 4, MSL building #04-04 Singapore 408618 Singapour
ST Microelectronics 9 Mountain Drive, LISP II, Brgy La Mesa Calamba, 4027 Philippines	**Nedcard** Bijsterhuizen 25-29 6604 LM Wijchen Pays-Bas
ST Microelectronics 7 Loyang Drive Singapore 508938 Singapour	**Disco HI-Tec Europe GmbH** Liebigstrasse 8, D-85551 Kirchheim bei München, Allemagne
ST Microelectronics 18 Ang Mo Kio Industrial park 2, 569505 Singapour	**ST Microelectronics** 101 Boulevard des Muriers BP97 20180 Bouskoura Maroc
ST Microelectronics Sdn. Bhd. Tanjong Agas Industrial area. P.o. Box 28, 84007 Muar, Johor Malaysie	**Amkor** ATP1, Km 22 East Service Rd. South superhighway Mantipula City 1771 Philippines
Amkor ATP3/4, Science Avenue, Laguna technopark, Binan, Laguna, 4024 Philippines	**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 303 Hsinchu, Taïwan Republique de Chine	**Stats ChipPac (SCS)** 5 Yishun St. 23, 768442 Singapour
Stats ChipPac (SCT) No 176-5, 6 Lane Hualung Chun, Chiung Lin, 307 Hsinchu, Taïwan Republique de Chine	**Stats ChipPac (SCC)** 188 Huaxu Rd, Qingpu district, 201702 Shanghaï République Populaire de Chine

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

Le produit gère son cycle de vie sous la forme de trois configurations :

- configuration *Test* : à 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* ;
- configuration *Issuer :* cette configuration comprend cinq modes :
  - mode *Loader installation* : mode protégé dédié à l'installation du loader, réservé à STMicroelectronics ;
  - mode *Flash Loader :* mode protégé donnant accès au jeu d'instruction de chargement de l'application ou de données en mémoire FLASH ;
  - mode *User Emulation :* mode protégé permettant l'exécution d'une application chargée en mémoire FLASH ;
  - 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 STMicroelectronics ;
  - mode *Diagnosis* : mode réservé à STMicroelectronics ;

  Cette configuration *Issuer* est ensuite bloquée de manière irréversible lors du passage en configuration *User ;*
- configuration *User :* cette configuration comprend deux modes :
  - mode *Diagnosis :* mode réservé à STMicroelectronics ;
  - mode *End 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 composant peut être livré en configurations *Issuer* ou *User*.
Le chargement de l'application par l'utilisateur en configuration *Issuer* doit être réalisé dans un environnement sécurisé.

1.2.6. Configuration évaluée

Le certificat porte sur la TOE définie au paragraphe 1.2.1 en configuration *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).

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 [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 « Microcontrôleur sécurisé ST33H768 révision C, Firmware révision 4, incluant optionnellement la bibliothèque cryptographique Neslib version 4.1 et version 4.1.1 » certifié le 15 septembre 2015 sous la référence [CER-2015/36].
Le rapport technique d'évaluation [RTE] remis à l'ANSSI le 17 septembre 2015 et son annexe [MAINT] remise à l'ANSSI le 9 décembre 2015, détaillent les travaux menés par le centre d'évaluation et attestent 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 vulnérabilités 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] 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

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 ST33G1M2 révision F, Firmware révisions 9 et A, incluant optionnellement la bibliothèque cryptographique Neslib versions 4.1 et 4.1.1 et la bibliothèque MIFARE4Mobile ® 2.1.0 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL5 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 ST33G1M2 révision F, Firmware révisions 9 et A, incluant optionnellement la bibliothèque cryptographique Neslib versions 4.1 et 4.1.1 et la bibliothèque MIFARE4Mobile ® 2.1.0 » 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. 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] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

[2] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, la Suède et la Turquie.

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 ST33G1M2 Maskset K8H0A version F with firmware revision 9 and A, optional cryptographic library Neslib 4.1 and 4.1.1, and optional technology MIFARE4Mobile® 2.1.0, Security Target, référence SMD_ST33G_ST_14_003, revision 1.03, October 2015. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - ST33G platform ST33G1M2 Maskset K8H0A version F with firmware revision 9 and A, optional cryptographic library Neslib 4.1 and 4.1.1, and optional technology MIFARE4Mobile® 2.1.0, Security Target for composition, référence SMD_ST33G_ST_15_001, revision v1.02, October 2015.
[RTE]	Rapports technique d'évaluation : - Evaluation technical report Project LATOURM, référence LATM_ETR, version v1.0 du 17 septembre 2015 ; - Evaluation technical report for composite evaluation Project LATOURM, référence Maint_LAT_ETR Lite, version v1.0 du 12 décembre 2015.
[MAINT]	Annexe au rapport technique d'évaluation : - Evaluation technical report for IAR pre-analysis Project ST33 référence MAINT_LAT_ETR, version v1.0 du 9 décembre 2015.
[CONF]	Liste de configuration : - ST33G1M2 rev F & derivatives (incl. Firmware rev 9 and rev A, optional NesLib v4.1 & v4.1.1, MIFARE4Mobile v2.1.0) CONFIGURATION LIST, référence SMD_33G_CFGL_15_001, revision 1.1, October 2015. Liste de la documentation : ST33G1M2 rev F & derivatives (incl. Firmware rev 9 and rev A, optional NesLib v4.1 & v4.1.1, MIFARE4Mobile v2.1.0) DOCUMENTATION REPORT, référence SMD_ST33G1M2_DR_15_001, revision 1.02, October 2015.
[GUIDES]	Guides d'utilisation du produit : - ST33G Platform - ST33G1M2: Secure MCU with 32-bit ARM® SecurCore® SC300™ CPU - and high density Flash memory – Datasheet, reference: DS_33G1M2, revision 6, May 2015 ; - ST33G1M2 platform: BP and BM specific product profiles – Technical note, reference TN_ST33G1M2_01, revision 2, June 2015 ; - ST33G1M2 platform: LS, LC and BS specific product profiles –

	Technical note, reference TN_ST33G1M2_02, revision 2, June 2015; - ST33G1M2 family extension – Technical note, reference TN_ST33G1M2_03, revision 1, July 2015 ; - ST33GIM2 family extension: BP and BM specific product profiles – Technical note, reference TN_ST33G1M2_04, revision 1, July 2015 ; - ST33G1M2 family extension: LS, LC and BS specific product profiles – Technical note, reference TN_ST33G1M2_05, revision 1, July 2015 ; - ST33 uniform timing application note, reference: AN_33_UT revision 2, November 2013 ; - ST33G1M2 and derivatives Flash loader installation guide - User manual, reference UM_33G_FL, revision 4, August 2015 ; - ST33G1M2 Firmware User Manual, reference UM_ST33G1M2_FW, revision 8, August 2015 ; - ST33G and ST33H Security Guidance, reference: AN_SECU_ST33, revision 3.0, March 2015 ; - ST33G and ST33H - AIS31 Compliant Random Number user manual, reference UM_33G_33H_AIS31, revision 2, February 2014; - ST33G and ST33H - AIS31 Reference implementation - Startup, online and total failure tests - Application Note, reference AN_33G_33H_AIS31, revision 1, October 2013 ; - NesLib 4.1 and 4.1.1 for ST33 Secure MCUs cryptographic library User manual, reference UM_33_NESLIB_4, revision 4, January 2015; - ST33 Secure MCU family NesLib 4.1 and NesLib4.1.1 security recommendations, reference AN_SECU_33_NESLIB_4, revision 7, April 2015 ; - MIFARE4Mobile® Library 2.1 – User Manual, reference UM_MIFARE4Mobile-2.1, revision 5, June 2015 ; - MIFARE4Mobile® Library 2.1 for ST33G1M2 – Application note, reference AN_ST33G1M2_M4M_Lib, revision 1, June 2015.
[CER-2015/36]	Rapport de certification ANSSI-CC-2015/36 « Microcontrôleur sécurisé ST33H768 révision C, Firmware révision 4, incluant optionnellement la bibliothèque cryptographique Neslib version 4.1 et version 4.1.1 », émis le 15 septembre 2015, ANSSI.
[BSI_PP_0035-2007]	Protection Profile - Security IC Platform Protection Profile, version v1.0 du 15 juin 2007. *Certifié par le BSI sous la référence BSI_PP_0035-2007.*

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 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 CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, September 2012, version 3.1, revision 4, ref CCMB-2012-09-001; Part 2: Security functional components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-002; Part 3: Security assurance components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2012, version 3.1, révision 4, ref 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 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité, voir http://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.