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-2013/44

Microcontrôleurs sécurisés
ST33F1M/1M0/896/768/640/512, SC33F1M0/896/768/640/512/384,
SM33F1M/1M0/896/768/640/512, SE33F1M/1M0/896/768/640/512,
SL33F1M/1M0/896/768/640/512, SP33F1M,
incluant le logiciel dédié révision D ou E et
optionnellement la bibliothèque cryptographique NesLib v3.0 ou v3.2

Version : *maskset* K8C0A, révision externe F, révision interne J

Paris, le 17 juin 2013

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

[Original signé]

Patrick Pailloux

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-2013/44

Nom du produit

Microcontrôleurs sécurisés ST33F1M/1M0/896/768/640/512, SC33F1M0/896/768/640/512/384, SM33F1M/1M0/896/768/640/512, SE33F1M/1M0/896/768/640/512, SL33F1M/1M0/896/768/640/512, SP33F1M, incluant le logiciel dédié révision D ou E et optionnellement la bibliothèque cryptographique NesLib v3.0 ou v3.2

Référence/version du produit

Version maskset K8C0A, révision externe F, révision interne J

Conformité à un profil de protection

[BSI_PP_0035], version V1.0
Security IC Platform Protection Profile

Critères d'évaluation et version

CC version 3.1 révision 3

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, 31401 Toulouse Cedex 9, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit est reconnu au niveau EAL4.

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 la famille de « Microcontrôleurs sécurisés ST33F1M/1M0/896/768/640/512, SC33F1M0/896/768/640/512/384, SM33F1M/1M0/896/768/640/512, SE33F1M/1M0/896/768/640/512, SL33F1M/1M0/896/768/640/512, SP33F1M, incluant le logiciel dédié révision D ou E et optionnellement la bibliothèque cryptographique NesLib v3.0 ou v3.2, référence ST33F1M, ST33F768, SC33F768, ST33F640, SC33F640, ST33F512, SC33F512 et SC33F384, en version maskset K8C0A, révision externe F, révision interne J », développée par STMicroelectronics.

Les dérivés Sx33Fxxx sont issus du même produit ST33F1M. Les parties matérielles et les logiciels dédiés sont strictement identiques. Ils ne diffèrent que par des restrictions de taille des mémoires ainsi que par la mise à disposition de l'interface SWP, selon le choix du client. Chacun de ces produits inclut optionnellement la bibliothèque cryptographique NesLib version v3.0 ou v3.2. Dans la suite du document, le produit et l'ensemble de ses dérivés sont désignés par Sx33Fxxx.

Les microcontrôleurs peuvent offrir une interface MIFARE Classic ou DESFire^{TM} EV0 hors cible de sécurité.

La partie matérielle et les logiciels dédiés des Sx33Fxxx sont des évolutions des Sx33Fxxx en version précédente (*maskset* K8C0A révision externe E, révision interne G), certifiés sous la référence [ANSSI-CC-2012/79] et maintenus sous la référence [ANSSI-CC-2012/79-M01].

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

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

La cible de sécurité est strictement conforme au profil de protection [BSI_PP_0035].

1.2.1. 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 :

- informations physiques gravées sur la surface de la puce :
  - identifiant de la puce : K8C0A (*maskset major cut*) ;
  - identifiant du site de production : ST_4 (Rousset) ou ST_2 (TSMC) ;

- informations logiques disponibles dans mémoire de la puce :
  - tous les identifiants matériels et logiciels du produit sont obtenus à partir d'une API et d'une méthode documentée dans le « ST32/33 System ROM User Manual » (voir [GUIDES]), accessible quelle que soit la configuration mise à disposition du client :
    - identifiant du produit : l'API retourne l'identifiant du produit maître (valeur **0000**h pour le ST33F1M) ainsi qu'un identifiant propre à chacun des produits dérivés tels que décrit dans le tableau ci-dessous repris de [GUIDES] ;
    - révision externe du produit (valeur **F** pour le ST33F1M révision F) ;
    - révision interne du produit (valeur **J**) ;
    - identifiant des logiciels dédiés : l'API retourne :
      - la valeur **0023**h pour identifier la séquence de boot & reset et l'autotest ;
      - la valeur **000D**h ou **000E**h pour identifier respectivement la révision D ou E du *Flash Loader* (incluant les *Flash Drivers*) liées à la révision F du produit ;
    - la référence de la personnalisation et des données utilisateurs ;
  - la référence de la bibliothèque cryptographique : NesLib fournit une API qui retourne la valeur **1300**h ou **1320h** pour identifier la NesLib version 3.0 ou 3.2 tel que décrit dans « ST33 Smartcard MCU NesLib User Manual » (voir [GUIDES]).

Nom commercial	Identifiant du produit (voir note)	Mémoire non volatile	Mémoire vive	SWP	MIFARE
ST33F1M	0000h	1.2 MOctets	30 KOctets	Oui	Non
SP33F1M	0000h	1.2 MOctets	30 KOctets	Oui	Oui
SM33F1M	002Bh	1.2 MOctets	30 KOctets	Oui	Oui
SE33F1M	002Bh	1.2 MOctets	30 KOctets	Oui	Oui
SL33F1M	002Bh	1.2 MOctets	30 KOctets	Oui	Oui
ST33F1M0	0034h	1 MOctets	30 KOctets	Oui	Non
SC33F1M0	0038h	1 MOctets	30 KOctets	Non	Non
SM33F1M0	0035h	1 MOctets	30 KOctets	Oui	Oui
SE33F1M0	0035h	1 MOctets	30 KOctets	Oui	Oui
SL33F1M0	0035h	1 MOctets	30 KOctets	Oui	Oui
ST33F896	0036h	896 KOctets	30 KOctets	Oui	Non
SC33F896	0039h	896 KOctets	30 KOctets	Non	Non
SM33F896	0037h	896 KOctets	30 KOctets	Oui	Oui
SE33F896	0037h	896 KOctets	30 KOctets	Oui	Oui
SL33F896	0037h	896 KOctets	30 KOctets	Oui	Oui
ST33F768	0026h	768 KOctets	24 KOctets	Oui	Non
SC33F768	0027h	768 KOctets	24 KOctets	Non	Non
SM33F768	002Ch	768 KOctets	24 KOctets	Oui	Oui
SE33F768	002Ch	768 KOctets	24 KOctets	Oui	Oui
SL33F768	002Ch	768 KOctets	24 KOctets	Oui	Oui
ST33F640	001Ah	640 KOctets	24 KOctets	Oui	Non

SC33F640	0025h	640 KOctets	24 KOctets	Non	Non
SM33F640	002Dh	640 KOctets	24 KOctets	Oui	Oui
SE33F640	002Dh	640 KOctets	24 KOctets	Oui	Oui
SL33F640	002Dh	640 KOctets	24 KOctets	Oui	Oui
ST33F512	0028h	512 KOctets	24 KOctets	Oui	Non
SC33F512	0029h	512 KOctets	24 KOctets	Non	Non
SM33F512	002Eh	512 KOctets	24 KOctets	Oui	Oui
SE33F512	002Eh	512 KOctets	24 KOctets	Oui	Oui
SL33F512	002Eh	512 KOctets	24 KOctets	Oui	Oui
SC33F384	002Ah	384 KOctets	24 KOctets	Non	Non

Tableau 1 : Récapitulatif des configurations

Note : Les dérivés préfixés par « SM », « SE » et « SL » qui ont le même suffixe ont le même numéro d'identification car il s'agit du même produit avec des contrats d'utilisation différents.

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 ;
- la gestion des mémoires (firewall programmable) ;
- la protection physique ;
- la gestion des violations sécuritaires ;
- la non-observabilité des informations sensibles ;
- le chargement et la gestion sécurisés de la mémoire NVM (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 ;
- la bibliothèque cryptographique offrant, suivant la version et la configuration choisies, des implémentations RSA, SHA, AES, ECC et un service de génération sécurisée de nombres premiers et clés RSA.

De plus, hors cible de sécurité, le produit offre :
- les interfaces optionnelles MIFARE Classic ou DESFire™ EV0.

1.2.3. Architecture

Les microcontrôleurs Sx33Fxxx sont constitués des éléments suivants :

- une partie matérielle composée :
  - d'un processeur ARM® SecurCore® SC300™ 32-bit RISC core ;
  - de mémoires :
    - Flash (avec contrôle d'intégrité) pour le stockage des programmes et des données ;
    - RAM ;
    - ROM pour le stockage des logiciels dédiés de test ;

  - de modules de sécurité : unité de protection des mémoires (MPU), générateur d'horloge, surveillance et contrôle de la sécurité, gestion de l'alimentation, contrôle d'intégrité des mémoires, détection de fautes ;
  - de modules fonctionnels : 3 compteurs 8-bits dont un configurable en *watchdog*, un bloc de gestion des entrées/sorties en mode contact (IART ISO 7816-3), une interface SWP optionnelle (interface non disponible sur les microcontrôleurs SC33Fxxx), des générateurs de nombres aléatoires (TRNG), des coprocesseurs EDES pour le support des algorithmes DES et un coprocesseur NESCRYPT muni d'une RAM dédiée pour le support des algorithmes cryptographiques à clé publique ;
- une partie « logiciels dédiés » en ROM et NVM intégrant :
  - des logiciels de tests du microcontrôleur (autotest) ;
  - des utilitaires pour la gestion du système, de la mémoire NVM (Flash) et des interfaces hardware/software ;
  - des utilitaires de gestion du chargement de la mémoire NVM (Flash) ;
  - une interface optionnelle MIFARE Classic (hors cible de sécurité) ;
  - une interface optionnelle MIFARE DESFire™ EV0 (hors cible de sécurité).

De manière optionnelle, le client peut également choisir d'intégrer une bibliothèque cryptographique (NesLib v3.0 ou NesLib v3.2) fournissant des implémentations des fonctions cryptographiques RSA et SHA, RSA, SHA, AES, ECC et un service de génération sécurisée de nombres premiers et de clés RSA. Cette bibliothèque est incluse dans la cible de sécurité du produit et de chacun de ses dérivés. La bibliothèque est intégrée toute ou partie dans le code client selon son besoin, et est donc embarquée dans la mémoire NVM du produit.

1.2.4. Cycle de vie

Le cycle de vie du produit dans le cycle global du développement d'une carte à puce est résumé dans le schéma suivant :

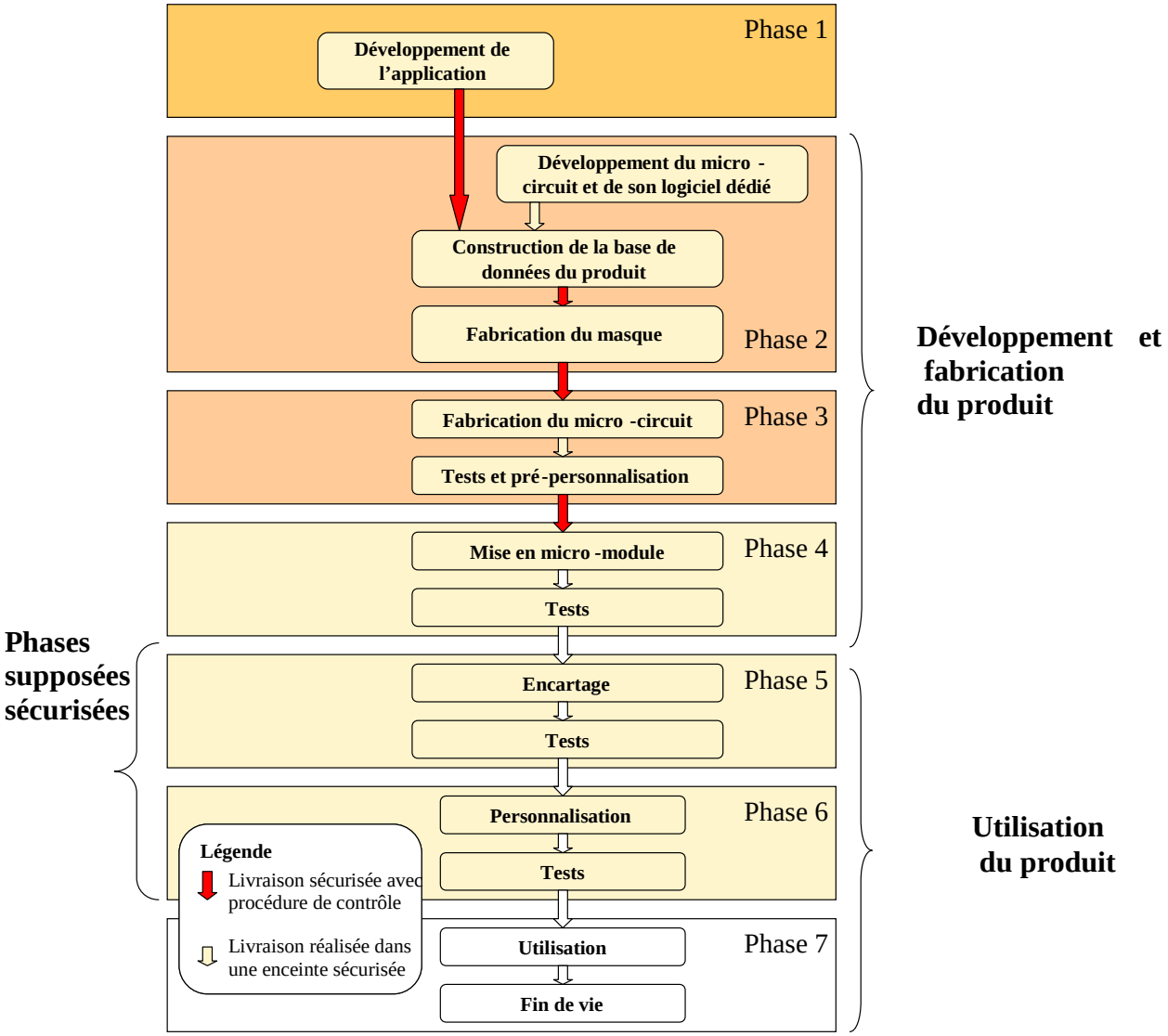

Figure 1 - Cycle de vie standard d'une carte à puce

Le produit a été développé sur les sites suivants :

STMicroelectronics SAS Smartcard IC division 190 Avenue Célestin Coq ZI de Rousset-Peynier 13106 Rousset Cedex France	**STMicroelectronics Pte ltd** 5A Serangoon North Avenue 5 554574 Singapour Singapour
STMicroelectronics Excelsiorlaan 44-46 B-1930 Zaventem Belgique	**STMicroelectronics** 629 Lorong 4/6 Toa Payoh 319521 Singapour Singapour
STMicrolectronics STMicroelectronics 850 rue Jean Monnet 38926 Crolles France	**STMicroelectronics** 7 Loyang drive 508938 Singapour Singapour
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
TSMC (TAIWAN) 1-1 Nan Ke N. Rd. Tainan science park Tainan 741_44 Taiwan, République de Chine	**TSMC (TAIWAN)** Li-Hsin Rd. 6 Hsinchu science park Hsinchu 300-78 Taiwan, République de Chine
STMicroelectronics 101 Boulevard des Muriers BP97 20 180 Casablanca Maroc	**STS Microelectronics** 16 Tao hua Rd. Futian free trade zone 518048 Shenzhen P.R. Chine
STMicrolectronics 9 Mountain Drive LISP II Brgy La mesa, 4027 Calamba, Philippines	**STMicrolectronics** Sdn. Bhd.Tanjong Agas industrial area. P.O. Box 28 84007 Muar, Johor, Malaisie
DISCO Hi-Tec Europe GmbH Liebigstrasse 8 D-85551 Kirchheim bei Munchen Allemagne	**NEDCARD** Bijsterhuizen 25-29 6604 LM Wijchen Pay-Bas

STATSChipPAC (Singapore) 5 Yishun St.23 768442 Singapour	**Smartflex Technologies** No 27 UBI rd 4 MSL building #04-04 408618 Singapour Singapour
AMKOR Technologies 119N. Science Avenue, Laguna Technopark, Binan 4024 Laguna, Philippines	**AMKOR Technologies** km 22 East Service road south superhighway 1771 Muntipula City, Philippines

Le produit comporte lui-même une gestion de son cycle de vie fonctionnel, prenant la forme de trois configurations d'utilisation :

- configuration « *Test* » : à la fin de sa fabrication, le microcontrôleur est testé à l'aide du logiciel de test présent en ROM. Les données de pré-personnalisation peuvent être chargées en NVM. Cette configuration est ensuite bloquée de manière irréversible lors du passage en configuration « *Issuer* » ou « *User* » ;
- configuration « *Issuer* » : mode comprenant quatre sous-modes :
  - mode « *Final Test OS*», permettant au site d'assemblage d'effectuer quelques tests restreints pour vérifier la qualité de l'assemblage ;
  - mode « *Diagnosis* » : sous-ensemble du mode « *Final Test OS* », réservé à STMicroelectronics ;
  - mode « *Flash Loader* » : mode protégé permettant d'effectuer le chargement de données ou d'une application en NVM ;
  - mode « *User Emulation* » : mode protégé lié au mode « *Flash Loader* » permettant d'émuler la configuration pour valider les applications chargées en Flash ;

  Les deux sous-modes « *Final Test* » et « *Diagnosis* » sont disponibles dès l'accès à la configuration « *Issuer* ». Les deux sous-modes « Flash Loader » et « *User Emulation* » sont protégés par une fonction d'authentification. La configuration « *Issuer* » est ensuite bloquée de manière irréversible lors du passage en configuration « *User* » ;
- configuration « *User* » : mode comprenant deux sous-modes :
  - mode « *Diagnosis* » : identique à celui de la configuration « *Issuer* », réservé à STMicroelectronics ;
  - mode « *End user* » : mode final d'utilisation du microcontrôleur qui fonctionne alors sous le contrôle du logiciel embarqué de la carte à puce. Le logiciel de test n'est plus accessible. Les utilisateurs finaux ne peuvent utiliser le microcontrôleur que dans cette configuration.

1.2.5. Configuration évaluée

Le certificat porte sur les configurations suivantes avec le masque version K8C0A révision externe E, révision interne G :

- ST33F1M/1M0/896/768/640/512 ;
- SC33F1M0/896/768/640/512/384 ;
- SM33F1M/1M0/896/768/640/512 ;
- SE33F1M/1M0/896/768/640/512 ;
- SL33F1M/1M0/896/768/640/512 ;

- SP33F1M.

Ces différentes références correspondent à un même circuit matériel dont :

- la taille de la mémoire flash et de la mémoire vive est bridée durant le test matériel du circuit ;
- l'interface *Single Wire Protocol (SWP)* est dégradée électriquement selon la configuration commerciale ;
- les interfaces MIFARE Classic ou DESFire sont présentes ou absentes.

Sur la partie logicielle, le certificat porte sur le logiciel dédié révision D et E ainsi que sur la bibliothèque cryptographique Neslib v3.0 v3.2 (optionnellement choisie par le client).

Bien que les interfaces MIFARE Classic ou DESFire^{TM} EV0 soient hors cible de sécurité, elles ont été activées durant l'évaluation du produit.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1, révision 3** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

Pour répondre aux spécificités des cartes à puce, les guides [CC 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 « ST33F1M/1M0/896/768/640/512, SC33F1M0/896/768/640/512/384, SM33F1M/1M0/896/768/640/512, SE33F1M/1M0/896/768/640/512, SL33F1M/1M0/896/768/640/512, SP33F1M, With dedicated software revision D, Optional cryptographic library Neslib 3.0 or 3.2 » certifié le 12 novembre 2012 sous la référence [ANSSI-CC-2012/79] et maintenu sous la référence [ANSSI-CC-2012/79-M01].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 15 février 2013, 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

Le produit évalué offre les services cryptographiques suivants :

- support au chiffrement cryptographique à clés symétriques (EDES) ;
- support au chiffrement cryptographique à clés asymétriques (NESCRYPT) ;
- support à la génération de nombres non prédictibles (TRNG) ;
- support à l'utilisation des interfaces MIFARE Classic ou DESFire™ EV0.

Ces services ne peuvent cependant pas être analysés d'un point de vue cryptographique car ils ne concourent pas à la sécurité propre du produit ; leur résistance dépend de leur emploi par l'application.

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.
Le générateur atteint le niveau « P2 – *SOFHigh* ».

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 la famille de « Microcontrôleurs sécurisés ST33F1M/1M0/896/768/640/512, SC33F1M0/896/768/640/512/384, SM33F1M/1M0/896/768/640/512, SE33F1M/1M0/896/768/640/512, SL33F1M/1M0/896/768/640/512, SP33F1M, incluant le logiciel dédié révision D ou E et optionnellement la bibliothèque cryptographique NesLib v3.0 ou v3.2 , référence ST33F1M, ST33F768, SC33F768, ST33F640, SC33F640, ST33F512, SC33F512 et SC33F384, version maskset K8C0A, révision externe F, révision interne J » soumise 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 la famille de « Microcontrôleurs sécurisés ST33F1M/1M0/896/768/640/512, SC33F1M0/896/768/640/512/384, SM33F1M/1M0/896/768/640/512, SE33F1M/1M0/896/768/640/512, SL33F1M/1M0/896/768/640/512, SP33F1M, incluant le logiciel dédié révision D ou E et optionnellement la bibliothèque cryptographique NesLib v3.0 ou v3.2 » 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 spécifiés dans la cible de sécurité [ST] et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

Reconnaissance du certificat

Ce certificat fait l'objet d'une reconnaissance internationale.

3.2.1. 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 :

3.2.2. 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 EAL4 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, Singapour, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation du produit

Class	Family	Components by assurance level							Assurance level of the product	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 5+	Name of the component
ADV Development	ADV_ARC		**1**	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**5**	Complete semiformal 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 Guidance	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**1**	1	1	1	1	1	1	**1**	Preparative procedure
ALC Life-cycle support	ALC_CMC		**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 Security target evaluation	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claim
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended component 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 specifications
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	2	**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 Vulnerability assessment	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 : - SB33F1M SECURITY TARGET référence SMD_ST33F1M_ST_09_001, version v03.01 de décembre 2012. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - ST33F1ME + 7 derivatives with optional Neslib Security Target - Public version référence SMD_Sx33Fxxx_ST_10_002, version 3.01 de décembre 2012.
[RTE]	Rapport technique d'évaluation : - SEQUOIA3 A/B Evaluation technical report référence SEQ3AB_ETR, version v1.0 du 15 février 2013. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - SEQUOIA2 Evaluation technical report lite référence SQ2_ETR Lite, version 15 février 2013.
[CONF]	Liste de configuration : - ST33F1MF and Derivatives Configuration List (DSW rev D and rev E, MIFARE Classic and MIFARE DESFire EV0) référence SMD_33F_CFGL_13_002, version v01.00 du 30 avril 2013.
[GUIDES]	Guides du produit : - ST33F1M Smartcard MCU and derivatives with ARM SecurCore SC300 CPU - Datasheet, Référence : DS_33F1M Rev 2.0 ; - ST33F1M Die Description, Référence : DD_33F1M Rev 5; - ST33F640/SC33F640 Die Description, Référence : DD_33F640 Rev 1 ; - NesLib 3.0 cryptographic library user manual, Référence : UM_33_NesLib_3_0 Rev 5 ; - NesLib 3.2 cryptographic library user manual, Référence : UM_33_NesLib_3_2 Rev 2 ; - ST33 Platform - Security Guidance, Référence : AN_SECU_33 Rev 3 ; - ST32/33 System ROM User Manual, Référence : UM_32_33_SysROM Rev 29 ; - User manual: MIFARE Classic Software library revision 1.4.0 référence UM_MIFARE_CLASSIC, version v5; - User Manual MIFARE DESFire EV0 software Library version v1.2 réf UM_MIFARE_DESFIRE_EV0-1.2 rev4 - ARM® Cortex ™ SC300 r0p0 Technical Reference Manual

	Référence : ARM DDI 0337F Rev F ; - ARM® SC300 r0p0 - SecurCore Technical Reference Manual Référence : supp_ARM_DDI_0337_supp1A Rev A ; - ARM® Cortex™ M3 r2p0 Technical Reference Manual Référence : ARM DDI 0337 Rev F3c ; - ST33F1M Uniform Timing Application Note, Référence : AN_33F1M_UT Rev 1 ; - ST33 - AIS31 Compliant Random Number user manual Référence : UM_33_AIS31 Rev 1 ; - ST33 - AIS31 Reference Implementation: Start-up, On-line and Total Failure Tests Application Note Référence : AN_33_AIS31 Rev 1 ; - ST33F1M and Derivatives Flash Loader Installation Guide Référence : UM_33F1M_FL Rev 5.
[ANSSI-CC-2012/79]	Rapport de certification : - ST33F1M/1M0/896/768/640/512, SC33F1M0/896/768/640/512/384, SM33F1M/1M0/896/768/640/512, SE33F1M/1M0/896/768/640/512, SL33F1M/1M0/896/768/640/512, SP33F1M, With dedicated software revision D, Optional cryptographic library Neslib 3.0 or 3.2, référence ANSSI-CC-2012/79 du 12 novembre 2012.
[ANSSI-CC-2012/79-M01]	Rapport de maintenance : - ST33F1M/1M0/896/768/640/512, SC33F1M0/896/768/640/512/384, SM33F1M0/896/768/640/512/384, SE33F1M0/896/768/640/512/384, SL33F1M0/896/768/640/512/384, SP33F1M, With dedicated software revision D, Optional cryptographic library Neslib 3.0 or 3.2, référence ANSSI-CC-2012/79-M01 du 8 avril 2013.
[BSI_PP_0035]	Protection Profile - Security IC Platform Protection Profile, version V1.0 du 15 juin 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI_PP_0035.*

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, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2009-03-002 version 3.0, revision 1, March 2009.
[JIWG AP]	Mandatory Technical Document - Application of attack potential to smart-cards, JIWG, version 2.8, January 2012.
[COMP]	Joint Interpretation Library – Composite product evaluation for Smart Cards and similar devices, version 1.2, Jaunuary 2012.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.
[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 (RGS_B_1), voir www.ssi.gouv.fr.
[AIS 31]	Functionnality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25 September 2001, BSI (Bundesamt für Sicherheit in der Informationstechnik).