



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-2013/13**

**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,  
Optional MIFARE DESFire™ EV1**  
Version : maskset K8C0A, revision externe E, revision interne G.

*Paris, le 06 mars 2013*

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

[Original signé]

Contre-amiral Dominique Riban





## 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 présumées 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](mailto:certification.anssi@ssi.gouv.fr)

La reproduction de ce document sans altération ni coupure est autorisée.



Référence du rapport de certification

**ANSSI-CC-2013/13**

Nom 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,  
Optional MIFARE DESFire™ EV1**

Référence/version du produit

**Version maskset K8C0A, revision externe E, revision interne G.**

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 3**

Niveau d'évaluation

**EAL5 Augmenté  
ALC\_DVS.2 et AVA\_VAN.5**

Développeur

**STMicroelectronics  
190 avenue Celestin Coq, ZI de Rousset, B.P. 2, 13106 Rousset, France**

Commanditaire

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

Centre d'évaluation

**Thalès (TCS-CNES)  
18 avenue Edouard Belin, 31401 Toulouse Cedex 9, France**

Accords de reconnaissance applicables



**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](http://www.ssi.gouv.fr).



## Table des matières

<b>1. LE PRODUIT .....</b>	<b>6</b>
1.1. PRÉSENTATION DU PRODUIT .....	6
1.2. DESCRIPTION DU PRODUIT .....	6
1.2.1. Identification du produit.....	6
1.2.2. Services de sécurité .....	8
1.2.3. Architecture.....	9
1.2.4. Cycle de vie .....	10
1.2.5. Configuration évaluée.....	13
<b>2. L'ÉVALUATION .....</b>	<b>14</b>
2.1. RÉFÉRENTIELS D'ÉVALUATION.....	14
2.2. TRAVAUX D'ÉVALUATION .....	14
2.3. COTATION DES MÉCANISMES CRYPTOGRAPHIQUES SELON LES RÉFÉRENTIELS TECHNIQUES DE L'ANSSI .....	14
2.4. ANALYSE DU GÉNÉRATEUR D'ALÉAS.....	14
<b>3. LA CERTIFICATION.....</b>	<b>15</b>
3.1. CONCLUSION.....	15
3.2. RESTRICTIONS D'USAGE.....	15
3.3. RECONNAISSANCE DU CERTIFICAT .....	16
3.3.1. Reconnaissance européenne (SOG-IS) .....	16
3.3.2. Reconnaissance internationale critères communs (CCRA) .....	16
<b>ANNEXE 1. NIVEAU D'ÉVALUATION DU PRODUIT.....</b>	<b>17</b>
<b>ANNEXE 2. RÉFÉRENCES DOCUMENTAIRES DU PRODUIT ÉVALUÉ .....</b>	<b>18</b>
<b>ANNEXE 3. RÉFÉRENCES LIÉES À LA CERTIFICATION .....</b>	<b>21</b>



# 1. Le produit

## 1.1. Présentation du produit

Le produit évalué est la famille de microcontrôleurs « 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, Optional MIFARE DESFire™ EV1 » en version *maskset* K8C0A, révision externe E, révision interne G, développée par STMicroelectronics.

Les dérivés Sx33Fxxx sont issus du même produit ST33F1ME. 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 3.0 ou version 3.2. De la même manière, le client peut choisir sur chacun des produits d'inclure optionnellement les bibliothèques de technologie MIFARE : MIFARE Classic ou MIFARE DESFire™ EV1.

Dans la suite du document, le produit et l'ensemble de ses dérivés sont désignés par Sx33Fxxx.

La partie matérielle et les logiciels dédiés des Sx33Fxxx sont des évolutions de la famille de microcontrôleurs ST33F1ME certifiés sous la référence ANSSI-CC-2012/79.

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\_0035-2007].

### 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 :
  - o identifiant de la puce : K8C0A (*maskset major cut*) ;
  - o identifiant du site de production : ST\_4 (Rousset) ou ST\_2 (TSMC) ;



- informations logiques disponibles dans mémoire de la puce :
  - o 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 » (cf [GUIDES]), accessible quelle que soit la configuration mise à disposition du client :
    - identifiant du produit : l'API retourne l'identifiant du produit maître (valeur **0000h** 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 **E** pour le ST33F1M révision E) ;
    - révision interne du produit (valeur **G**) ;
    - identifiant des logiciels dédiés : l'API retourne :
      - la valeur **0022h** pour identifier la séquence de boot & reset et l'autotest ;
      - la valeur **000Dh** pour identifier la version du *Flash Loader* (incluant les *Flash Drivers*) liés à la révision E du produit ;
      - la référence de la personnalisation et des données utilisateurs ;
  - o la référence de la bibliothèque cryptographique : NesLib fournit une API qui retourne la valeur **1300h** pour identifier la NesLib version 3.0 ou **1320h** pour identifier la NesLib version 3.2, tel que décrit dans « ST33 Smartcard MCU NesLib User Manual » (cf [GUIDES]).
  - o La référence de la bibliothèque de technologie MIFARE : Chaque bibliothèque fournit une API qui retourne une valeur d'identification, telle que définie dans chacun des manuels d'utilisation respectifs. Concernant MIFARE DESFire™ EV1, l'API retourne la valeur 1.1.0 comme décrit dans le « User Manual: MIFARE DESFire™ EV1 Library 1.1 » (cf. [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 évalués 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 ;
- le service optionnel MIFARE DESFire™ EV1.

De plus, hors cible de sécurité, le produit offre le service optionnel MIFARE Classic.





### 1.2.3. Architecture

Les microcontrôleurs Sx33Fxxx sont constitués des éléments suivants :

- une partie matérielle composée :
  - o d'un processeur ARM® SecurCore® SC300™ 32-bit RISC core ;
  - o 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 ;
  - o 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 ;
  - o 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 :
  - o des logiciels de tests du microcontrôleur (autotest) ;
  - o des utilitaires pour la gestion du système, de la mémoire NVM (Flash) et des interfaces hardware/software ;
  - o des utilitaires de gestion du chargement de la mémoire NVM (Flash) ;
  - o une interface optionnelle MIFARE DESFire™ EV1 ;
  - o une interface optionnelle MIFARE Classic, 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 :

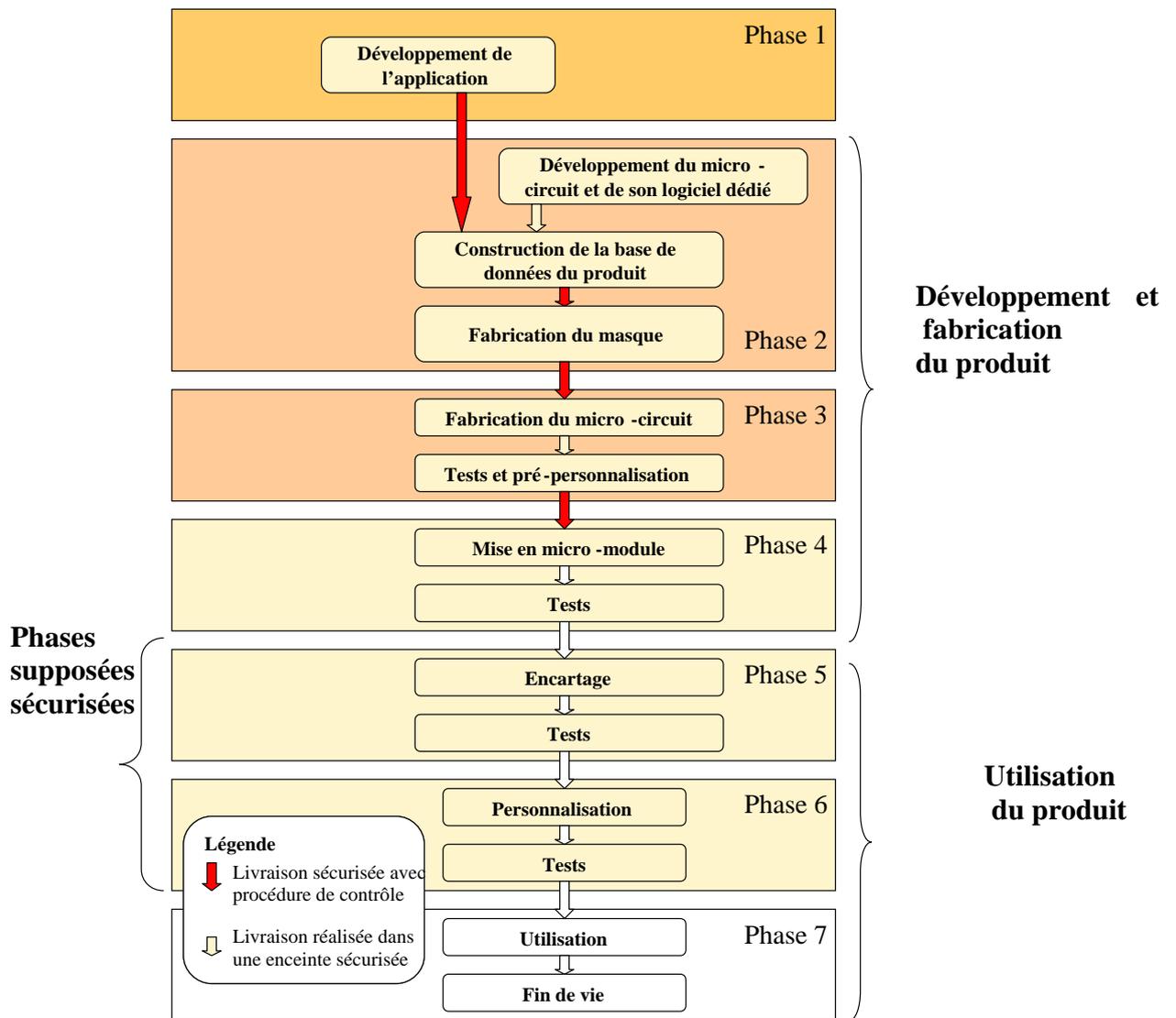


Figure 1 - Cycle de vie standard d'une carte à puce



Le développement du produit est réalisé sur les sites suivants (phases 2, 3 et 4) :

<p><b>STMicroelectronics SAS</b>          Smartcard IC division          190 Avenue Célestin Coq          ZI de Rousset-Peynier          13106 Rousset Cedex          France</p>	<p><b>STMicroelectronics Pte ltd</b>          5A Serangoon North Avenue 5          554574 Singapour          Singapour</p>
<p><b>STMicroelectronics</b>          Excelsiorlaan 44-46          B-1930 Zaventem          Belgique</p>	<p><b>STMicroelectronics</b>          629 Lorong 4/6 Toa Payoh          319521 Singapour          Singapour</p>
<p><b>STS Microelectronics</b>          16 Tao hua Rd.          Futian free trade zone          518048 Shenzhen          P.R. Chine</p>	<p><b>STMicroelectronics</b>          7 Loyang drive          508938 Singapour          Singapour</p>
<p><b>STMicroelectronics</b>          101 Boulevard des Muriers          BP97 20 180 Casablanca          Maroc</p>	<p><b>Smartflex Technologies</b>          No 27 UBI rd 4          MSL building #04-04          408618 Singapour          Singapour</p>
<p><b>TSMC</b>          1-1 Nan Ke N. Rd. Tainan science park,          Tainan 741-44,          Taiwan, République de Chine</p>	<p><b>TSMC</b>          Li-Hsin Rd. 6 Hsinchu science park,          Hsinchu 300-78,          Taiwan, République de Chine</p>
<p><b>Dai Nippon Printing Co., Ltd</b>          2-2-1 Fukuoka Kamifukuoka-shi          Saitama-Ken 356-8507          Japon</p>	<p><b>Dai Nippon Printing Europe</b>          Via C. Olivetti 2/A          I-20041 Agrate Brianza          Italie</p>
<p><b>DISCO Hi-Tec Europe GmbH</b>          Liebigstrasse 8          D-85551 Kirchheim bei Munchen          Allemagne</p>	<p><b>NEDCARD</b>          Bijsterhuizen 25-29          6604 LM Wijchen          Pay-Bas</p>
<p><b>STMicroelectronics</b>          850 rue Jean monnet          38926 Crolles          France</p>	<p><b>STMicroelectronics</b>          9 Mountain Drive, LISP II, Brgy La          Mesa          4027 Calamba          Philippines</p>



<b>AMKOR Technologies ATP 3/4</b> 119N. Science Avenue, Laguna Technopark, Binan 4024 Laguna Philippines	<b>AMKOR Technologies ATP1</b> km 22 East Service road south superhighway 1771 Muntipula City Philippines
<b>STATSCHIP PAK</b> 5 Yishun St.23 768442 Singapour Singapour	<b>STMicroelectronics</b> Sdn, Bhd Tanjong Agas industrial area, P.O. Box 28 84007 Muar, Johor Malaisie

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 :
  - o mode « *Final Test* », permettant au site d'assemblage d'effectuer quelques tests restreints pour vérifier la qualité de l'assemblage ;
  - o mode « *Diagnosis* » : sous-ensemble du mode « *Final Test OS* », réservé à STMMicroelectronics ;
  - o mode « *Flash Loader* » : mode protégé permettant d'effectuer le chargement de données ou d'une application en NVM ;
  - o 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 :
  - o mode « *Diagnosis* » : identique à celui de la configuration « *Issuer* », réservé à STMMicroelectronics ;
  - o 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™ EV1 sont présentes ou absentes.



## 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].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 21 décembre 2012, 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™ EV1.

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 « 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, Optional MIFARE DESFire™ EV1, *maskset* K8C0A, révision externe E, révision interne G. », soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans la 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 « 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, Optional MIFARE DESFire™ EV1, *maskset* K8C0A, révision externe E, révision interne G » 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].



### 3.3. Reconnaissance du certificat

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

##### 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<sup>1</sup>, 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<sup>2</sup>, 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 :



<sup>1</sup> 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.

<sup>2</sup> 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
<b>ADV Development</b>	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
<b>AGD Guidance</b>	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
<b>ALC Life-cycle support</b>	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
<b>ASE Security target evaluation</b>	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
<b>ATE Tests</b>	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
<b>AVA Vulnerability assessment</b>	AVA_VAN	1	2	2	3	4	5	5	5	Advanced methodical vulnerability analysis



## Annexe 2. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> <li>- 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, product revision E, with optional cryptographic library Neslib 3.0 or 3.2, with optional technology MIFARE DESFire™ EV1 SECURITY TARGET référence SMD_SM33Fxxx_ST_11_001, version 01.03 du 20 décembre 2012.</li> </ul> <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> <li>- 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, product revision E, with optional cryptographic library Neslib 3.0 or 3.2, with optional technology MIFARE DESFire™ EV1 SECURITY TARGET - PUBLIC VERSION référence SMD_SM33Fxxx_ST_12_001, version 01.02 du 20 décembre 2012.</li> </ul>
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> <li>- SEQUOIA2C Evaluation technical report référence SQ2_ETR, version v2.0 du 19 octobre 2012 ;</li> <li>- SEQUOIA2BC MFC14 Evaluation technical report référence SQ2BCM1_ETR, version v1.0 du 21 décembre 2012.</li> </ul> <p>Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé :</p> <ul style="list-style-type: none"> <li>- SEQUOIA2C Evaluation technical report lite référence SEQ2C_ETR Lite, version v1.0 du 16 novembre 2012.</li> </ul>
[CONF]	<ul style="list-style-type: none"> <li>- ST33F1M and Derivatives (including Neslib 3.0 &amp; 3.2) - Documentation report référence SMD_ST33F1M_DR_12_001, version 1.2 du 16 mai 2012 ;</li> <li>- ST33F1M and DERIVATIVES with EV1 CONFIGURATION LIST référence SMD_33F_CFGL_12_002, version 01.01 du 26 avril 2012 ;</li> <li>- MIFARE DESFireEV1 Library 1.1 on ST33F1M: Configuration List référence SSS_MFDFEV1_1.1_CFGL_12_001, version 01.01 du 09 octobre 2012.</li> </ul>



<p>[GUIDES]</p>	<ul style="list-style-type: none"> <li>- ST33F1M Smartcard MCU and derivatives with ARM SecurCore SC300 CPU - Datasheet référence DS_ST33F1M, version 2 du 02 mars 2012 ;</li> <li>- ST33F1M Smartcard MCU and derivatives with ARM SecurCore SC300 CPU - Datasheet référence DS_ST33F1M, version 2 du 02 mars 2012 ;</li> <li>- ST33F1M: 90nm CMOS M10 Flash technology die description référence DD_33F1M, version 5 du 25 mai 2011 ;</li> <li>- ARM Cortex SC300 r0p0 Technical Reference Manual référence ARM DDI 0337F, version F du 18 février 2010 ;</li> <li>- ARM SC300 r0p0 - SecurCore Technical Reference Manual Supplement 1A référence supp_ARM_DDI_0337_supp1A, version A du 18 février 2010 ;</li> <li>- ARM Cortex M3 r2p0 Technical Reference Manual référence ARM DDI 0337 F3c, version F3c du 18 février 2010 ;</li> <li>- ST33F1M Uniform Timing référence AN_33F1M_UT, version 1 du 10 juin 2010 ;</li> <li>- ST33F1M Flash loader installation guide référence UM_33F1M_FL, version 5 du 26 septembre 2012 ;</li> <li>- ST33 Smartcard MCU NesLib 3.0 cryptographic library user manual référence UM_33_NesLib_3.0, version 5 du 13 avril 2012 ;</li> <li>- ST33 Secure microcontrollers NesLib 3.2 cryptographic library user manual référence UM_33_NESLIB_3.2, version 2 du 12 avril 2012 ;</li> <li>- ST33 platform Security guidance - 3 référence AN_SECU_33, version 3 du 18 novembre 2010 ;</li> <li>- User Manual: MIFARE Classic library 1.3 référence UM_MIFARE_CLASSIC, version 4 du 21 mai 2012 ;</li> <li>- User Manual: MIFARE Classic library 1.4 référence UM_MIFARE_CLASSIC, version 5 du 11 décembre 2012 ;</li> <li>- User Manual: MIFARE DESFire™ EV1 Library 1.1 référence UM_MIFARE_DESFire_EV1, version 2 du 27 septembre 2012 ;</li> <li>- Resource sharing on ST33F1M devices - Application Note référence AN_MFD FEV1_F1M, version 2 du 13 décembre 2012 ;</li> <li>- ST33 - AIS31 Compliant Random Number user manual - 1 référence UM_33_AIS31, version 1 du 19 février 2010.</li> </ul>
<p>[ANSSI-CC-2012/79]</p>	<p>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, Version : maskset K8C0A, revision externe E, revision interne G.  <i>Certifié le 12 novembre 2012 sous la référence ANSSI-CC-2012/79</i></p>



[BSI_PP_0035-2007]	Protection Profile - Security IC Platform Protection Profile, version v1.0 du 15 juin 2007. <i>Certifié par Certification sous la référence BSI_PP_0035-2007.</i>
--------------------	---



### 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, January 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.
[AIS 31]	Functionality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25 September 2001, BSI (Bundesamt für Sicherheit in der Informationstechnik).