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-2011/07

Microcontrôleurs sécurisés ST33F1ME, ST33F768E, SC33F768E, ST33F640E, SC33F640E, ST33F512E, SC33F512E et SC33F384E incluant optionnellement la bibliothèque cryptographique NesLib v3.0

Paris, le 5 avril 2011

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

Patrick Pailloux
[Original signé]

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-2011/07

Nom du produit

Microcontrôleurs sécurisés ST33F1ME, ST33F768E, SC33F768E, ST33F640E, SC33F640E, ST33F512E, SC33F512E et SC33F384E incluant optionnellement la bibliothèque cryptographique NesLib v3.0

Référence/version du produit

Version E (logiciel dédié 0x000B et 0x000C, maskset K8C0A, bibliothèque cryptographique NesLib v3.0)

Conformité à un profil de protection

[PP0035], version V1.0

Security IC Platform Protection Profile

Critères d'évaluation et version

Critères Communs V3.1

Niveau d'évaluation

EAL5 Augmenté

ALC_DVS.2, AVA_VAN.5

Développeur(s)

STMicroelectronics

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

Commanditaire

STMicroelectronics

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

Centre d'évaluation

Thales T3S-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 ST33F1ME, ST33F768E, SC33F768E, ST33F640E, SC33F640E, ST33F512E, SC33F512E et SC33F384E incluant optionnellement la bibliothèque cryptographique NesLib v3.0 en version révision E (logiciel dédié 0x000B et 0x000C, *maskset* K8C0A, bibliothèque cryptographique NesLib v3.0) développé 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.

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 des ST33F1MD, SA33F1MD et SB33F1MD, certifiés sous les références ANSSI-CC-2010/49 et ANSSI-CC-2010/50.

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 ou l'élément sécurisé d'un téléphone portable. Les usages possibles de cette carte sont multiples (applications téléphonie/bancaires, télévision à péage, ...) en fonction des logiciels applicatifs qui sont 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 s'inspire du profil de protection [PP0035].

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 gravées sur la surface de la puce :
  - identifiant de la puce : K8C0A (*maskset major cut*) avec les niveaux de masques correspondant au *maskset* K8C0EG ;
  - identifiant du site de production : ST_4 (Rousset) ;

- informations logiques disponibles de la mémoire de la puce :
    - tous les identifiants matériels et logiciels du produits 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 **0000**h pour le ST33F1M) ainsi qu'un identifiant unique propre à chacun des produits dérivés tels que décrit dans la *Datasheet* (cf. [GUIDES]) ;
        - révision du produit (valeur **E** pour le ST33F1M revision E) ;
        - identifiant des logiciels dédiés : L'API qui retourne :
            - la valeur **0022**h pour identifier la séquence de boot & reset et l'autotest ;
            - la valeur **000B**h ou **000C**h pour identifier l'une des deux versions du *Flash Loader* (incluant les *Flash drivers*) liés à la révision E du produit, ;
              Une méthode pour vérifier l'intégrité de ces objets est décrite dans le « Flash Loader Installation guide » (cf. [GUIDES]) ;
        - 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 pour identifier la NesLib version 3.0 (configuration SA ou SB), tel que décrit dans son « User Manual » (cf [GUIDES]).

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 (SKG) de génération sûre de nombres premiers et clés RSA.

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 :
    - jusqu'à 1 280 Koctets de mémoire Flash (avec contrôle d'intégrité) sur le ST33F1M pour le stockage des programmes et des données ;
    - jusqu'à 30 Koctets de mémoire RAM sur le ST33F1M ;
    - de mémoire 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 de Ko 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).

De manière optionnelle, le client peut également choisir d'intégrer une bibliothèque cryptographique (NesLib v3.0) fournissant des implémentations des fonctions cryptographiques RSA et SHA, RSA, SHA, AES, ECC et un service (SKG) de génération sûre de nombres premiers et 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 développement est résumé dans le schéma suivant :

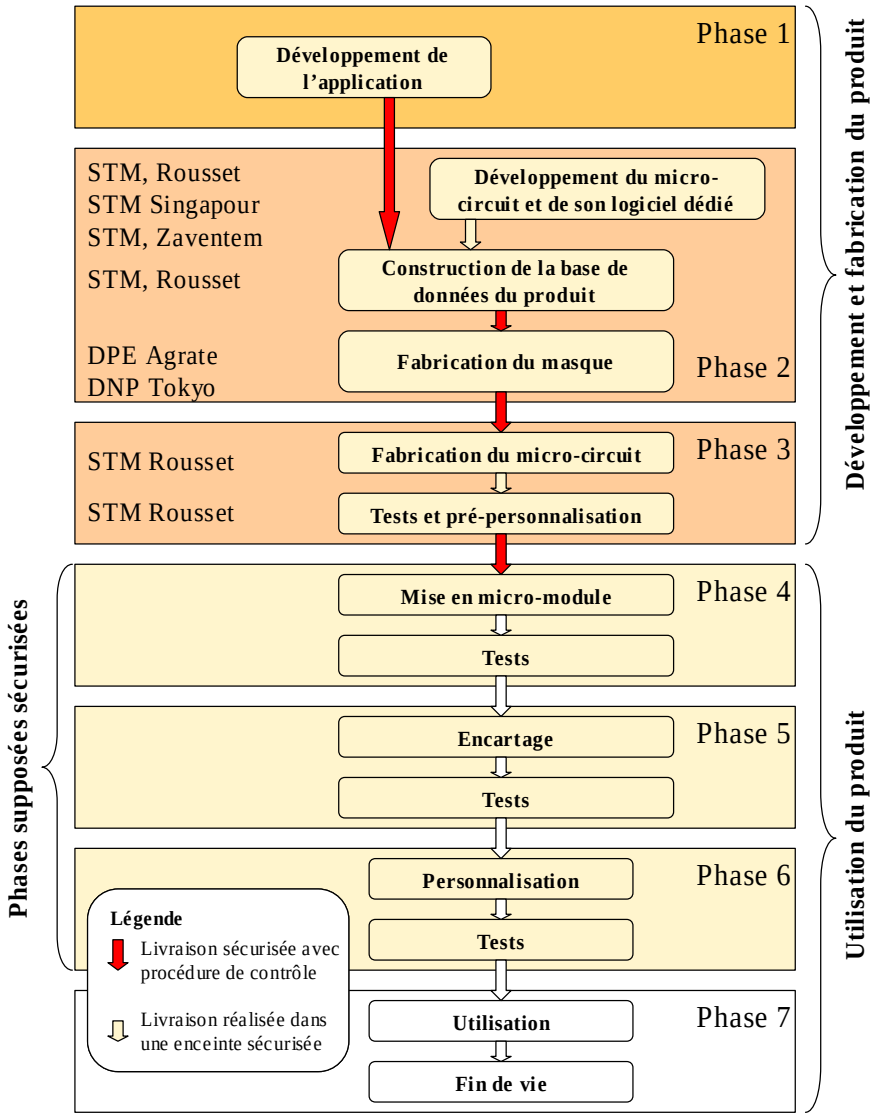

Figure 1 - Cycle de vie standard d'une carte à puce

Le produit a été développé sur les sites suivants :

STMicroelectronics SAS, Secure Microcontroller Division

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

STMicroelectronics

44-46 Excelsiorlaan
B-1930 Zaventem
Belgique

STMicroelectronics Pte ltd

5A Serangoon North Avenue 5
554574 Singapore
Singapour

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 », 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 :
Circuits ST33F1ME, ST33F768E, SC33F768E, ST33F640E, SC33F640E, ST33F512E, SC33F512E et SC33F384E avec le masque version K8C0.
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.
De même, l'interface *Single Wire Protocol (SWP)* est dégradée électriquement selon la configuration commerciale.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version V3.1, 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 [CC AP] ont été appliqués.

2.2. Travaux d'évaluation

L'évaluation s'appuie sur les résultats d'évaluation du produit Microcontrôleurs sécurisés SA33F1MD et SB33F1MD incluant la bibliothèque cryptographique NesLib v3.0, en configuration SA ou SB, certifié le 23 juillet 2010 sous la référence ANSSI-CC-2010/50 [ANSSI-CC-2010/50].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 7 février 2011, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques selon les référentiels techniques [REF-CRY], [REF-KEY] et [REF-AUT] n'a pas été réalisée par l'ANSSI. 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] par le laboratoire d'évaluation.
Le générateur atteint le niveau « P2 – *SOF High* ».

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 « Microcontrôleurs sécurisés ST33F1ME, ST33F768E, SC33F768E, ST33F640E, SC33F640E, ST33F512E, SC33F512E et SC33F384E incluant optionnellement la bibliothèque cryptographique NesLib v3.0 », version révision E (logiciel dédié 0x000B et 0x000C, maskset K8C0A, bibliothèque cryptographique NesLib v3.0) soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL5.

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 « Microcontrôleurs sécurisés ST33F1ME, ST33F768E, SC33F768E, ST33F640E, SC33F640E, ST33F512E, SC33F512E et SC33F384E incluant optionnellement la bibliothèque cryptographique NesLib v3.0 » 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 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[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 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'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

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 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 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 procedure
ALC Support au cycle de vie	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
	ADO_DEL		**1**	1	**1**	1	1	**1**	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**2**	**Sufficiency of security measures**
	ALC_FLR								**1**	**Basic flaw remediation**
	ALC_LCD			1	**1**	**1**	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**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**	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**	Independant 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 : - SB33F1M SECURITY TARGET référence SMD_ST33F1M_ST_09_001, version v01.01 du 3 mars 2010 éditée par STMicroelectronics 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 1 du 28 octobre 2010 éditée par STMicroelectronics
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report – ST33F1ME, ST33F768E, SC33F768E, ST33F640E, SC33F640E, ST33F512E, SC33F512E & SC33F384E, all with optional Neslib 3.0, Référence : SQ2_ETR_v5.0, Thales Security & Solutions & Services - Evaluation Technical Report lite – ST33F1ME, ST33F768E, SC33F768E, ST33F640E, SC33F640E, ST33F512E, SC33F512E & SC33F384E, all with optional Neslib 3.0, Référence : SQ2_ETR_lite_v3.0, Thales Security & Solutions & Services
[CONF]	Liste de configuration des produits : - ST33F1ME & Derivatives Configuration list, Référence : SMD_33F_CFGL_10_001 v01.00, STMicroelectronics, - NesLib v3.0 on ST33F1M Configuration List, Référence : Neslib_3.0_CFGL_09_001 v01.01, STMicroelectronics, - Impact Analysis Report – Sx33Fxxx rev E (Annex A - Configuration list update) Référence : SMD_33F_SIA_10_001 v01.01, STMicroelectronics, Liste de la documentation : - ST33F1M and Derivatives (including Neslib 3.0) - Documentation report, Référence : SMD_ST33F1M_DR_10_001 v01.00 STMicroelectronics.

[GUIDES]	Les guides d'utilisation du produit sont constitués des documents suivants : - ST33F1M Smartcard MCU and derivatives with ARM SecurCore SC300 CPU - Datasheet, Référence : DS_33F1M Rev 0.7, STMicroelectronics - ST33F1M Die Description, Référence : DD_33F1M Rev 4, STMicroelectronics - ST33F640/SC33F640 Die Description, Référence : DD_33F640 Rev 1, STMicroelectronics - NesLib 3.0 cryptographic library user manual, Référence : UM_33_NesLib_3_0 Rev 4, STMicroelectronics - ST33 Platform - Security Guidance, Référence : AN_SECU_33 Rev 3, STMicroelectronics - ST32/33 System ROM User Manual, Référence : UM_32_33_SysROM Rev 22, STMicroelectronics - ARM® Cortex ™ SC300 r0p0 Technical Reference Manual Référence : ARM DDI 0337F Rev F, ARM - ARM® SC300 r0p0 - SecurCore Technical Reference Manual Référence : supp_ARM_DDI_0337_supp1A Rev A, ARM - ARM® Cortex™ M3 r2p0 Technical Reference Manual Référence : ARM DDI 0337 Rev F3c, ARM - ST33F1M Uniform Timing Application Note, Référence : AN_33F1M_UT Rev 1, STMicroelectronics - ST33 - AIS31 Compliant Random Number user manual Référence : UM_33_AIS31 Rev 1, STMicroelectronics - ST33 - AIS31 Reference Implementation: Start-up, On-line and Total Failure Tests Application Note Référence : AN_33_AIS31 Rev 1, STMicroelectronics - ST33F1M and Derivatives Flash Loader Installation Guide Référence : UM_33F1M_FL Rev 3, STMicroelectronics - Errata Sheet: ST33F1M Flash loader Installation Guide (applicable only for System ROM 0x000B) - Référence : ES_33F1M_FL Rev 2, STMicroelectronics

[ANSSI-CC-2010/50]	Réévaluation du produit Microcontrôleurs sécurisés SA33F1MD et SB33F1MD incluant la bibliothèque cryptographique NesLib v3.0, en configuration SA ou SB certifié le 23 juillet 2010 sous la référence ANSSI-CC-2010/50.
[PP EAC]	Protection Profile - Machine Readable Travel Document with "ICAO Application", Extended Access Control, version 1.10, 25 Mars 2009. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0056-2009*
[PP0035]	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.
[JIL]	ITSEC Joint Interpretation Library, version 2.0.
[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.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2009-03-001 version 2.7 revision 1, March 2009.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, reference CCDB-2007-09-001 version 1.0, revision 1, September 2007.
[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-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010, voir www.ssi.gouv.fr

[REF-KEY]	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008, voir www.ssi.gouv.fr
[REF-AUT]	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010, voir www.ssi.gouv.fr
[AIS 34]	Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004, BSI (Bundesamt für Sicherheit in der Informationstechnik)
[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)