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-2010/50

Microcontrôleurs sécurisés SA33F1MD et SB33F1MD incluant la bibliothèque cryptographique NesLib v3.0, en configuration SA ou SB

Paris, le 23 juillet 2010

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

Vice-amiral Michel Benedittini
[ORIGINAL SIGNE]

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-2010/50

Nom du produit

Microcontrôleurs sécurisés SA33F1MD et SB33F1MD incluant la bibliothèque cryptographique NesLib v3.0, en configuration SA ou SB

Référence/version du produit

SA33F1M révision D & SB33F1M révision D (logiciel dédié AQC, maskset K8C0A, bibliothèque cryptographique NesLib v3.0, en configuration SA ou SB)

Conformité à un profil de protection

BSI-PP-0035-2007 version 1.0

Critères d'évaluation et version

Critères Communs version 3.1 R3

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeur

STMicroelectronics

Secure Microcontrollers Division, 190 Avenue Célestin Coq, 13106 Rousset Cedex, France

Commanditaire

STMicroelectronics

Secure Microcontrollers Division, 190 Avenue Célestin Coq, 13106 Rousset Cedex, France

Centre d'évaluation

THALES - CEACI (T3S – CNES)

18 avenue Edouard Belin, BPI 1414, 31401 Toulouse Cedex 9, France

Tél : +33 (0)5 61 28 16 51, mél : nathalie.feyt@thalesgroup.com

Recognition arrangements

CCRA

SOG-IS

The product is recognised at EAL4 level.

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

Les produits évalués sont les microcontrôleurs sécurisés SA33F1M et SB33F1M en révision D (maskset major cut K8C0A, logiciel dédié AQC) développés par STMicroelectronics. Ils incluent la bibliothèque cryptographique NesLib version 3.0, en configuration SA pour le SA33F1MD et en configuration SB pour le SB33F1MD.

La partie matérielle et les logiciels dédiés sont identiques à ceux du ST33F1MD certifié sous la référence ANSSI-CC-2010/49.

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 (applications téléphoniques, bancaires, télévision à péage, ...) en fonction des logiciels applicatifs qui seront embarqués. Ces logiciels ne font pas partie de la présente évaluation.

1.2. Description du produit évalué

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

Cette cible de sécurité est strictement conforme au 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 K8C0DF ;
  - identifiant du logiciel dédié: AQC (séquence de boot & reset, autotest) ;
  - identifiant du site de production : ST_4 (Rousset) ;

- informations logiques disponibles dans la mémoire de la puce :
  - identifiant du produit : le produit dispose dans la zone OTP de deux octets de valeur 0000h pour le SA/SB33F1M tel que décrit dans la « Datasheet » (cf. [GUIDES]) ;
  - identifiant des logiciels dédiés : le Flash Loader fournit une API qui retourne la valeur 0007h pour identifier la séquence de boot & reset, le Flash Loader et les Flash drivers liés à la révision D du produit, ainsi qu'une méthode pour vérifier son intégrité tel que décrit dans le « Flash Loader Installation guide » (cf. [GUIDES]) ;

- référence de la bibliothèque cryptographique : NesLib fournit une API qui retourne la valeur 1300h pour identifier NesLib version 3.0 (configuration SA ou SB) tel que décrit dans son « User Manual » (cf [GUIDES]) ;
- la référence de la personnalisation et des données utilisateurs est également disponible au niveau d'octets de la zone OTP.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- l'initialisation de la plate-forme matérielle et de ces attributs ;
- la gestion sécurisée du cycle de vie ;
- l'intégrité logique du produit ;
- les autotests du produit ;
- la gestion des mémoires (firewall programmable) ;
- la protection physique ;
- la gestion des violations sécuritaires ;
- la non-observabilité ;
- 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 SA/SB33F1M sont constitués des éléments suivants :

- une partie matérielle composée :
  - d'un processeur ARM® SecurCore® SC300™ 32-bit RISC core ;
  - de mémoires :
    - 1280 Ko de mémoire Flash (avec contrôle d'intégrité) pour le stockage des programmes et des données ;
    - 30 Ko de mémoire RAM ;
    - de mémoire ROM pour le stockage des logiciels dédiés de test ;
  - de modules de sécurité :
    - unité de protection des mémoires (MPU) ;
    - générateur d'horloge ;
    - gestion de l'alimentation ;
    - surveillance et contrôle de la sécurité ;
    - contrôle d'intégrité des mémoires ;
    - détection de fautes ;
  - de modules fonctionnels :
    - trois compteurs 8-bits dont un configurable en watchdog ;
    - gestion des entrées/sorties selon les standards IART ISO 7816-3, SWP et optionnellement SPI ;
    - générateurs de nombres aléatoires (TRNG) ;
    - coprocesseur EDES pour le support des algorithmes DES ;
    - 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 entrée/sortie ;
  - des utilitaires de gestion du chargement de la mémoire NVM (Flash).
- une bibliothèque cryptographique (NesLib v3.0) fournissant des implémentations des fonctions cryptographiques RSA, SHA et un service (SKG) de génération sûre de nombres premiers et clés RSA en configuration SA, ou bien, RSA, SHA, AES, ECC et un service (SKG) de génération sûre de nombres premiers et clés RSA en configuration SB. Cette bibliothèque est incluse dans la cible de sécurité du produit. La bibliothèque est intégrée dans le code client, et est donc embarqué dans la mémoire NVM du produit.

1.2.4. Cycle de vie

Le cycle de vie du développement est résumé dans le schéma suivant :

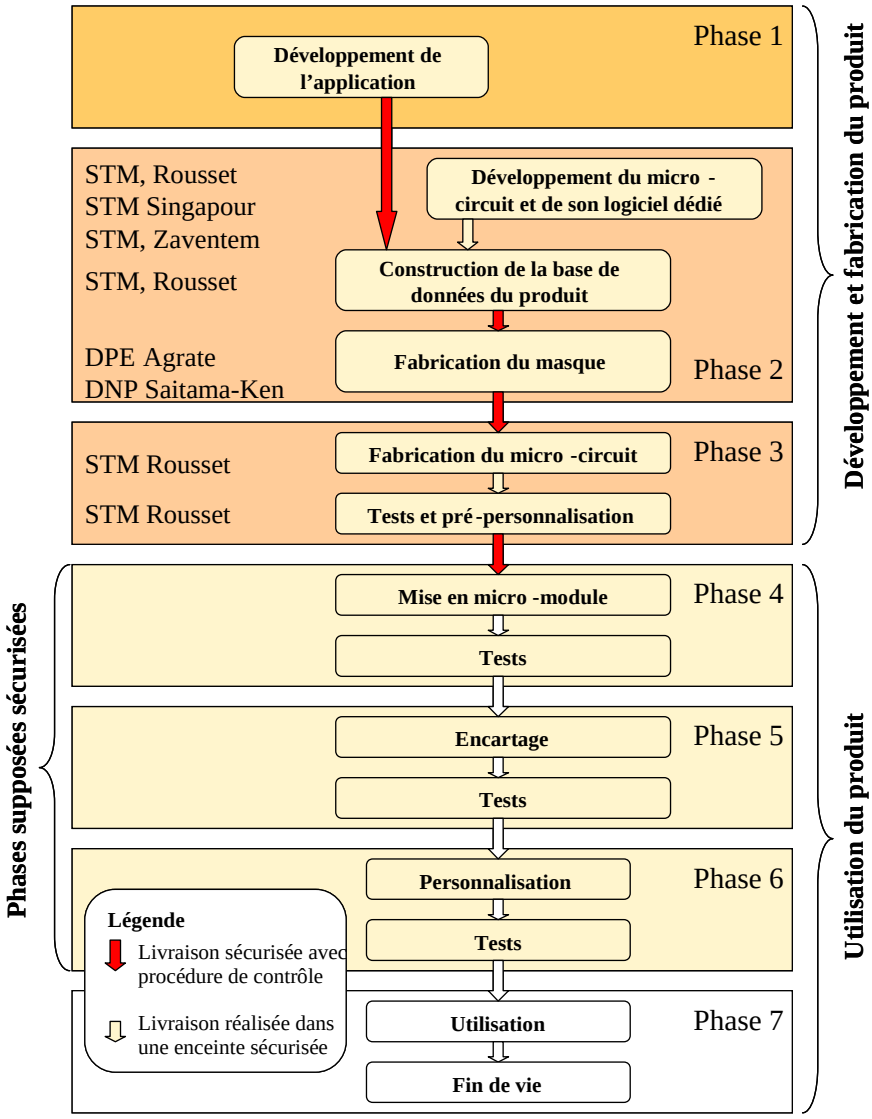

Figure 1 - Cycle de vie standard d'une carte à puce

Le produit est développé, intégré (préparation de la base de données du produit), fabriqué et testé par :

STMicroelectronics SAS

Secure Microcontroller Division
190 Avenue Célestin Coq, ZI de Rousset, BP2
13106 Rousset Cedex
France

Une partie du développement du produit est réalisée par :

STMicroelectronics Pte ltd

5A Serangoon North Avenue 5,
554574 Singapore.
Singapour

et par :

STMicroelectronics

Excelsiorlaan 44-46,
B-1930 Zaventem,
Belgique

Les réticules du produit sont fabriqués par :

DAI NIPPON PRINTING CO., LTD

2-2-1, Fukuoka, kamifukuoka-shi,
Saitama-Ken, 356-8507
Japon

et par :

DAI NIPPON PRINTING EUROPE

Via C. Olivetti, 2/A,
I-20041 Agrate Brianza,
Italie

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

- une 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 bloquée de manière irréversible lors du passage en configurations « Issuer » ou « User » ;
- une configuration « Issuer » 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 NVM.

  La configuration « Issuer » est bloquée de manière irréversible lors du passage en configuration « User » ;

- une configuration « User » 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.

1.2.5. Configuration évaluée

Ce rapport de certification présente les travaux d'évaluation relatifs au microcontrôleur, aux logiciels dédiés et à la bibliothèque cryptographique, identifiés au §1.2.1. Toute autre application éventuellement embarquée, notamment les routines embarquées pour les besoins de l'évaluation, ne font donc pas partie du périmètre d'évaluation.
En regard du cycle de vie, le produit évalué est le produit qui sort de la phase de fabrication, tests et pré-personnalisation (phase 3).
Pour les besoins de l'évaluation, les microcontrôleurs ST33F1MC et ST33F1MD munis de la NesLib v3.0 (qui correspondent aux SA/SB33F1MC et SA/SB33F1MD), ont été fournis au centre d'évaluation, avec un système d'exploitation logiciel dédié, dans un mode dit « ouvert[1] »

[1] Mode permettant de charger et d'exécuter du code natif en NVM et de déconnecter les mécanismes sécuritaires paramétrables.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].
Pour les composants d'assurance supérieurs au niveau EAL4, des méthodes propres au centre d'évaluation, validées par l'ANSSI, ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [CC IC] et [CC AP] ont été appliqués.

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 15 juin 2010, 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 de support cryptographiques suivants :
- support au chiffrement cryptographique à clés symétriques (EDES) ;
- support au chiffrement cryptographique à clés symétriques (NESCRYPT) ;
- support à la génération de nombres non prédictibles (TRNG).

Ces services ne peuvent cependant pas être analysés vis-à-vis des référentiels techniques de l'ANSSI [REF-CRY], [REF_CLE] et [REF-AUT], car ils ne concourent pas à la sécurité propre du produit : leur résistance dépendra de leur emploi par l'application embarquée sur le microcircuit.

Les produits SA/SB33F1MD contiennent également une bibliothèque cryptographique NesLib v3.0. La cotation des mécanismes cryptographiques offerts par cette bibliothèque, selon les référentiels techniques [REF-CRY], [REF_CLE] et [REF-AUT] n'a pas été réalisée par l'ANSSI. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception, ni de construction pour le niveau AVA_VAN visé.

2.4. Analyse du générateur d'aléas

Le générateur de nombres aléatoires, de nature physique, a fait l'objet d'une évaluation selon la méthodologie [AIS 31] par le centre d'évaluation. Le générateur est de classe « P2 – *SOF-high* » selon l'[AIS31].

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 les microcontrôleurs sécurisés SA33F1MD et SB33F1MD, incluant la bibliothèque cryptographique NesLib version 3.0, en configuration SA ou SB, soumis à l'évaluation répondent aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 augmenté.

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 des microcontrôleurs sécurisés SA33F1MD et SB33F1MD 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] au chapitre 5.2 et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

3.3. Reconnaissance du certificate

3.3.1. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord 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.

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Espagne, la Finlande, la France, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

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 de l'accord[1], 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 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_SB33F1M_ST_09_001 v01.01, STMicroelectronics. Pour les besoins de publication, les cibles de sécurité suivantes ont été fournies et validées dans le cadre de cette évaluation : - SA/SB33F1MD Security Target - Public Version, Référence : SMD_Sx33F1M_ST_10_001 v01.00, STMicroelectronics.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report, Référence : SQA_ETR_v1.0, Thales Security & Solutions & Services. Rapport technique d'évaluation public : - Evaluation Technical Report Lite for Composition, Référence : SQA_ETR_LITE_v1.0, Thales Security & Solutions & Services.
[CONF]	Liste de configuration des produits : - ST/SA/SB33F1M products - Configuration list, Référence : SMD_33F1M_CFGL_10_002 v01.00, STMicroelectronics ; - NesLib v3.0 on ST33F1M Configuration List, Référence : Neslib_3.0_CFGL_09_001 v01.01, STMicroelectronics. Liste de la documentation : - ST/SA/SB33F1M documentation report, Référence : SMD_ST33F1M_DR_09_001 v01.01 STMicroelectronics.
[GUIDES]	Les guides d'utilisation du produit sont constitués des documents suivants : - ST33F1M Smartcard MCU with ARM SecurCore SC300 CPU and 1.25 Mbyte Flash Memory -. Datasheet, Référence : DS_33F1M Rev 0.5, STMicroelectronics ; - ST33F1M Die Description, Référence : DD_33F1M Rev 4, 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 2, STMicroelectronics ; - ST32/33 System ROM User Manual, Référence : UM_32_33_SysROM Rev 15, 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 Flash Loader Installation Guide, Référence : UM_33F1M_FL Rev 1, STMicroelectronics.
[PP0035]	Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.*

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure 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.
[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, Feb 2009.
[REF-CRY]	Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, version 1.20 du 26 janvier 2010, voir www.ssi.gouv.fr
[REF-CLE]	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
[AIS31]	Functionnality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25 September 2001, BSI (Bundesamt für Sicherheit in der Informationstechnik)