PREMIER MINISTRE

General Secretariat for Defence and National Security

French Network and Information Security Agency

Certification Report ANSSI-CC-2010/50

**SA33F1MD & SB33F1MD Secure
Microcontrollers, including cryptographic
library NesLib v3.0, in configuration SA or SB**

Paris, July 23th 2010

Courtesy Translation

SÉCURITÉ CERTIFICATION

Warning

This report is designed to provide sponsors with a document enabling them to assess the security level of a product under the conditions of use and operation defined in this report for the evaluated version. It is also designed to provide the potential purchaser of the product with the conditions under which he may operate or use the product so as to meet the conditions of use for which the product has been evaluated and certified; that is why this certification report must be read alongside the evaluated user and administration guidance, as well as with the product security target, which presents threats, environmental assumptions and the supposed conditions of use so that the user can judge for himself whether the product meets his needs in terms of security objectives.

Certification does not, however, constitute a recommendation product from ANSSI (French Network and Information Security Agency), and does not guarantee that the certified product is totally free of all exploitable vulnerabilities.

Any correspondence about this report has to be addressed to:

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information

51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP
France

certification.anssi@ssi.gouv.fr

Reproduction of this document without any change or cut is authorised.

Certification report reference	
ANSSI-CC-2010/50	
Product name	
SA33F1MD & SB33F1MD Secure Microcontrollers, including cryptographic library NesLib v3.0, in configuration SA or SB	
Product reference	
SA/B33F1M révision D (logiciel dédié AQC, maskset K8C0A, NesLib 3.0)	
Protection profile conformity	
BSI-PP-0035-2007 version 1.0 Security IC Platform Protection Profile v1.0, 15 June 2007	
Evaluation criteria and version	
Common Criteria version 3.1	
Evaluation level	
EAL 5 augmented **AVA DVS.2, AVA VAN.5**	
Developer	
STMicroelectronics **Smartcard IC division, 190 Avenue Célestin Coq, 13106 Rousset Cedex, France**	
Sponsor	
STMicroelectronics **Smartcard IC division, 190 Avenue Célestin Coq, 13106 Rousset Cedex, France**	
Evaluation facility	
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.	

Introduction

The Certification

Security certification for information technology products and systems is governed by decree number 2002-535 dated 18 April 2002 and published in the "Journal Officiel de la République Française". This decree stipulates that:

- The French Network and Information Security Agency draws up **certification reports**. These reports indicate the features of the proposed security targets. They may include any warnings that the authors feel the need to mention for security reasons. They may or may not be transmitted to third parties or made public, as the sponsors desire (article 7).

- The **certificates** issued by the Prime Minister certify that the copies of the products or systems submitted for evaluation fulfil the specified security features. They also certify that the evaluations have been carried out in compliance with applicable rules and standards, with the required degrees of skill and impartiality (article 8).

The procedures are available on the Internet site www.ssi.gouv.fr.

SA33F1MD & SB33F1MD Secure Microcontrollers,
including cryptographic library NesLib v3.0, in configuration
SA or SB   Certification report ANSSI-CC-2010/50

Content

1. Product

1.1. Presentation of the product

The evaluated products are the SA33F1M & SB33F1M secure microcontrollers revision D (dedicated software AQC, K8C0A mask set) developed by STMicroelectronics. These products include the cryptographic library Neslib in version v3.0, in SA configuration for SA33F1MD and in SB configuration for SB33F1MD. The hardware part and the dedicated software are identical to the ST33F1MD secure microcontroller certified under the reference ANSSI-CC-2010/49.

The SA33F1MD and SB33F1MD only differ by the SA or SB configuration of the Neslib cryptographic library in version v3.0. The SA Neslib configuration provides high-level routines to perform RSA and SHA operations, on top of that the SB configuration provides high-level routines to perform AES, ECC operations and a service of secure generation of prime numbers and RSA keys.

The microcontrollers aim to host one or several software applications and can be embedded in a plastic support to create a Smartcard with multiple possible usages (secure identity documents, banking, health card, pay-TV or transport applications…) depending on the Embedded Software applications. However, only the microcontroller is evaluated. The software applications are not in the scope of this evaluation.

1.2. Evaluated product description

The security target [ST] defines the evaluated product, its evaluated security functionalities and its operational environment.

This security target is compliant with [PP035] protection profile (strict compliance).

1.2.1. Product identification

The configuration list [CONF] identifies the product's constituent elements.

The certified version of the product can be identified by the following elements:
- readable on the die :
  - o Die identification: K8C0A (Die name with HW major cut reference)
  - o Die mask set identification: all masks revision letters corresponding to K8C0DF mask set;
  - o Dedicated software identification: AQC (Boot sequence, embedded test software);
  - o Manufacturing site identification: ST 4 (Rousset);

- readable through the memory: two bytes in OTP allow identifying the product, dedicated SW, NesLib v3.0, personnalization & user data references, from a logical point of view, as described in the "Datasheet", "User Manual" and "Flash loader installation guide" (cf. [GUIDES]).

SA33F1MD & SB33F1MD Secure Microcontrollers,
including cryptographic library NesLib v3.0, in configuration
SA or SB   Certification report ANSSI-CC-2010/50

1.2.2. Security services

The product provides mainly the following security services:
- Initialisation of the hardware platform and its attributes;
- Secure handling of the life cycle;
- Logical integrity of the product;
- Test of the product;
- Memory management (firewall);
- Physical tampering protection;
- Security violation administrator;
- Unobservability;
- Secure Flash loading & management ;
- Symmetric Key Cryptography Support;
- Asymmetric Key Cryptography Support;
- Unpredictable number generation support;
- Cryptographic library providing, according to the configuration SA or SB, the implementation of the functions: RSA, SHA, AES, ECC and secure generation of prime numbers & RSA keys.

1.2.3. Architecture

The ST33F1MD microcontrollers are made up of:

- A Hardware part:
  - ARM® SecurCore® SC300™ 32-bit RISC core processing unit;
  - Memories:
    - 1280 Kbytes of Flash (with integrity control) for SW & data;
    - ROM for dedicated SW;
    - 30 Kbytes of RAM;
  - Security Modules: Memory protection unit (MPU), clock generator, security monitoring and control, power management, memory integrity control and fault detection;
  - Functional Modules: 3 8-bit timers, I/O management in contact mode (IART ISO 7816-3), SWP and optionally SPI, True Random Number Generator, EDES co-processor supporting DES algorithms and the NESCRYPT co-processor with a dedicated RAM supporting public key cryptographic algorithms.

- A dedicated software is embedded in ROM which comprises:
  - Microcontroller test software ("Auto test");
  - System, Interfaces, Flash memory & Flash loader management capabilities.

- A cryptographic library (NesLib v3.0) providing routines to perform RSA and SHA cryptographic operations, in configuration SA; or routines to perform RSA, SHA, AES , ECC, secure generation of prime numbers & RSA keys in SB configuration. This library is integrated by the Customer in his code, and is then embedded in the Flash.

1.2.4. Life cycle
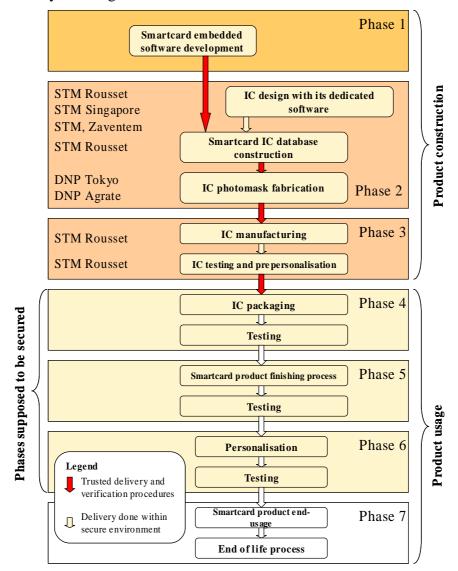
The product's life cycle is organised as follow:

Figure 1 – Life cycle of a smart card

SA33F1MD & SB33F1MD Secure Microcontrollers,
including cryptographic library NesLib v3.0, in configuration
SA or SB   Certification report ANSSI-CC-2010/50

The product is designed, prepared, manufactured and tested by:

STMicroelectronics SAS

Smartcard IC division
ZI de Rousset, BP2
13106 Rousset Cedex
France

A part of the design is realised by:

STMicroelectronics Pte Ltd

5A Serangoon North Avenue 5
554574 Singapore
Singapore

and by:

STMicroelectronics

Excelsiorlaan 44-46,
B-1930 Zaventem,
Belgium.

The photo masks of the product are manufactured by:

DAI NIPPON PRINTING CO., LTD

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

and by:

DAI NIPPON PRINTING EUROPE

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

The product manages itself the logical phases of its life cycle and can be in one of its three following configurations:

- "Test" configuration: at the end of IC manufacturing, the microcontroller is tested using the test software stored in ROM (called "Autotest") within the secure developer premises. Pre-personalization data can be loaded in the Flash. The product configuration is changed to "Issuer" or "User" before delivery to the next user, and the device cannot be reversed to the "test" configuration.

- "Issuer" configuration, including 4 modes:
  - mode « Final Test », allowing assembling site to perform restricted tests to check the quality of the assembling ;
  - mode « Diagnosis » : subset of the « Final Test OS », restricted to STMicroelectronics ;
  - mode « Flash Loader » : protected mode allowing data/application loading into the Flash ;

- ▪ mode « User Emulation » : protected mode related to the mode « Flash Loader » allowing to emulate the configuration for checking the applications loaded in Flash ;

The product configuration is changed to "User" before delivery to the next user, and the device cannot be reversed to the previous configurations.

- • "User" configuration: final configuration of the product, including 2 modes:
  - ▪ mode « Diagnosis », as the one in "Issuer" configuration, restricted to STMicroelectronics;
  - ▪ mode « End User », final usage mode of the product, whose functionalities are driven exclusively by the Embedded Software. The developer test functionalities are unavailable. The end-users of the product can use it only under this mode.

1.2.5. Evaluated configuration

This certification report presents the evaluation work related to the product and the dedicated software identified in §1.2.1. Any other embedded application, such as the embedded routines for evaluation purpose only, is not part of the evaluation perimeter.

Referring to the life-cycle, the evaluated product is the product that comes out the manufacturing, test and pre-personalization phase (phase 3).

For the evaluation needs, the products ST33F1MC & ST33F1MD, including the cryptographic library Neslib v3.0 (i.e. SA/B33F1MC & SA/B33F1MD), were provided to the ITSEF with a dedicated evaluation software in a mode known as "open[1]".

---

[1] mode that enables to load and execute a native code in Flash and also to disable the configurable security mechanisms.

SA33F1MD & SB33F1MD Secure Microcontrollers,
including cryptographic library NesLib v3.0, in configuration
SA or SB   Certification report ANSSI-CC-2010/50

2. Evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 3.1** [CC] and the Common Evaluation Methodology [CEM].
For assurance components above EAL4 level, the evaluation facility own evaluation methods, validated by ANSSI, have been used.
In order to meet the specificities of smart cards, the [CC IC] and [CC AP] guides have been applied.

2.2. Evaluation work

This evaluation is partially based on previous evaluation results of certified products from the ST23Y family.

The evaluation technical report [ETR], delivered to ANSSI on the 15th of June 2010, describes the work performed by the evaluation facility and assesses that all evaluation tasks are "**pass**".

2.3. Cryptographic mechanisms robustness analysis according to ANSSI technical reference frame

The evaluated product provides the following cryptographic support services:
- support for symmetric key cryptography (EDES) ;
- support for asymmetric key cryptography (NESCRYPT) ;
- support for random numbers generation (TRNG).

These services, however, cannot be analyzed in relation to the ANSSI technical reference frame [REF-CRY], [REF-CLE] and [REF-AUT] as they do not contribute to the inherent security of the product; their strength will depend on their use by the application embedded in the microcircuit.

The SA/SB33F1MD products include also a cryptographic library Neslib v3.0. The quotation of the cryptographic mechanisms provided by this library, according to technical reference frame [REF-CRY], [REF-CLE] and [REF-AUT], has not been performed. Nevertheless, the evaluation did not reveal any vulnerability in design nor implementation for the targeted AVA_VAN level.

2.4. Random number generator analysis

The evaluated product provides a hardware random number generator that has been evaluated according to the [AIS31] methodology by the evaluation facility: the generator reaches the class "P2 – *SOF-high*" according to [AIS31].

3. Certification

3.1. Conclusion

The evaluation was carried out according to the current rules and standards, with the required competency and impartiality as required for an accredited evaluation facility. All the work performed allows the release of a certificate in conformance with the decree 2002-535.

This certificate testifies that the secure microcontrollers SA/B33F1MD with NesLib 3.0 submitted for evaluation fulfil the security features specified in its security target [ST] for the evaluation level EAL5 augmented.

3.2. Restrictions of use

This certificate only applies on the products specified in chapter 1.2 of this certification report.

This certificate provides a resistance assessment of the SA/B33F1MD products to a set of attacks which remains generic due to the missing of any specific embedded application. Therefore, the security of a final product based on the evaluated microcontrollers would only be assessed through the final product evaluation, which could be performed using the results of current evaluation listed in Chapter 2.

The user of the certified product shall respect the operational environmental security objectives specified in the security target [ST] chapter 5.2 and shall respect the recommendations in the guidance [GUIDES].

3.3. Recognition of the certificate

3.3.1. European recognition (SOG-IS)

This certificate is issued in accordance with the provisions of the SOG-IS agreement [SOG-IS]. The European recognition agreement made by SOG-IS in 2010 allows recognition from signatory states of the agreement[1], of ITSEC and Common Criteria certificates. The European recognition is applicable up to ITSEC E6 and CC EAL7 levels. The certificates that are recognized in such scope are released with the following marking:

---

1 The signatory countries of the SOG-IS agreement are: Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and United Kingdom.

SA33F1MD & SB33F1MD Secure Microcontrollers,
including cryptographic library NesLib v3.0, in configuration
SA or SB   Certification report ANSSI-CC-2010/50

3.3.2. International common criteria recognition (CCRA)

This certificate is released in accordance with the provisions of the CCRA [CC RA].

The Common Criteria Recognition Arrangement allows the recognition, by signatory countries[1], of the Common Criteria certificates. The mutual recognition is applicable up to the assurance components of CC EAL4 level and also to ALC_FLR family. The certificates that are recognized in the agreement scope are released with the following marking:

---

1 The signatory countries of the CCRA arrangement are: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, the Republic of Korea, Malaysia, Netherlands, New-Zealand, Norway, Pakistan, Singapore, Spain, Sweden, Turkey, the United Kingdom and the United States of America.

Annex 1. Evaluation level of the product

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	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Production support, acceptance procedures and automation
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**5**	Development tools CM coverage
	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									
	ALC_LCD			1	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**2**	Compliance with implementation standards
ASE Evaluation de la cible de sécurité	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance 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**	Independant testing, sample

AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	Advanced methodical vulnerability analysis

Annex 2. Evaluated product references

[ST]	Reference security target for the evaluation:
	   - SB33F1M Security Target,
	     Référence : SMD_SB33F1M_ST_09_001 v01.01,
	     STMicroelectronics.
	
	For the needs of publication, the following security target has been provided and validated in the evaluation:
	     SA/SB33F1MD Security Target - Public Version,
	     Référence : SMD_Sx33F1M_ST_10_001 v01.00,
	     STMicroelectronics.

[ETR]	Evaluation technical report :
	   - Evaluation Technical Report - SEQUOIA Project,
	     Référence : SQA_ETR_v1.0,
	     Thales Security & Solutions & Services.
	
	For the needs of composite evaluation with this microcontroller a technical report for composition has been validated:
	   - Evaluation Technical Report Lite for Composition,
	     Référence : SQA_ETR_LITE_v1.0,
	     Thales Security & Solutions & Services.

[CONF]	Products configuration list:
	   - 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.
	
	List of the delivered materials:
	   - ST/SA/SB33F1M documentation report,
	     Référence : SMD_ST33F1M_DR_09_001 v01.01,
	     STMicroelectronics

[GUIDES]	The product user guidance documentation is the following:
	   - 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 ;

SA33F1MD & SB33F1MD Secure Microcontrollers,
including cryptographic library NesLib v3.0, in configuration
SA or SB   Certification report ANSSI-CC-2010/50

	- 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]	Security IC Platform Protection Profile Version 1.0 June 2007. *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0035-2007.*

Annex 3. Certification references

Decree number 2002-535 dated 18th April 2002 related to the security evaluations and certifications for information technology products and systems.	
[CER/P/01]	Procedure CER/P/01 - Certification of the security provided by IT products and systems, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, September 2006, version 3.1, revision 1, ref CCMB-2006-09-001, Part 2: Security functional components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-002, Part 3: Security assurance components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2007, version 3.1, ref CCMB-2007-09-004, revision 2.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2006-04-003 version 2.0, revision 1, April 2006.
[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.
[REF-CRY]	Cryptographic mechanisms - Rules and recommendations about the choice and parameters sizes of cryptographic mechanisms, version 1.11, 24th of October 2008, see www.ssi.gouv.fr
[REF-CLE]	Cryptographic keys management - Rules and recommendations about management of keys used in cryptographic mechanisms, version 1.10, 24th of October 2008, see www.ssi.gouv.fr
[REF-AUT]	Authentication - Rules and recommendations about authentication mechanisms with standard level robustness, v0.13 12th of April 2007, No. 729/SGDN/DCSSI/SDS
[AIS31]	Functionality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25/09/2001, Bundesamt für Sicherheit in der Informationstechnik (BSI)