Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Certification Report ANSSI-CC-2014/46

ST33G1M2 Secure microcontroller revision F, Firmware revision 9, with optional NesLib 4.1 cryptographic library and MIFARE® DESFire® EV1 library revision 3.7 or 3.8

Paris, July 21, 2014

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

certification.anssi@ssi.gouv.fr

Certification report reference

ANSSI-CC-2014/46

Product name

ST33G1M2 Secure microcontroller revision F, Firmware revision 9, with optional NesLib 4.1 cryptographic library and MIFARE® DESFire® EV1 library revision 3.7 or 3.8

Product reference

Reference maskset K8H0A, internal revision F, firmware revision 9

Protection profile conformity

[BSI_PP_0035-2007], version v1.0
Security IC Platform Protection Profile

Evaluation criteria and version

CC version 3.1 revision 4

Evaluation level

EAL5 Augmented
ALC_DVS.2 and AVA_VAN.5

Developer(s)

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

Sponsor

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

Evaluation facility

THALES (TCS – CNES)
18 avenue Edouard Belin, BPI1414, 31401 Toulouse Cedex 9, France

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 April, 18th 2002, modified. 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.

Contents

1. Product

1.1. Product overview

The evaluated product is the « ST33G1M2 Secure microcontroller revision F, Firmware revision 9, with optional NesLib 4.1 cryptographic library and MIFARE® DESFire® EV1 library revision 3.7 or 3.8 » developed by STMicroelectronics.

Product derivatives from ST33G1M2 included in this platform are defined by a number of hardware or software options configurable by the final customer. These options concern the non-volatile Flash memory size, the activation of the cryptographic coprocessors, library unit (LPU), input/output interfaces and MIFARE® technology libraries: MIFARE® DESFire® EV1 or MIFARE® Classic® (the latter is not part of the certification scope).

This microcontroller alone is not a product that can be used as such. It is designed to host one or more applications. It can be embedded in a plastic support to create a smartcard with multiple possible uses (secure identity documents, banking applications, pay-TV, transportation, health, etc.) depending on the embedded software applications. These software applications are not in the scope of this evaluation.

1.2. Product description

1.2.1. Introduction

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

This security target strictly complies with protection profile [BSI-PP-0035-2007]. Its compliance can be proven.

1.2.2. 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 (cf. [ST] in paragraph 3.1 "TOE overview" and [GUIDES]):

- physical information engraved on the chip's surface:
  - product identifier: **K8H0A** (major revision of the maskset corresponding to the ST33G1M2 platform) ;
  - Identification of the manufacturing site: **ST_4** (STMicroelectronics Rousset) or **ST_3** (STMicroelectronics Crolles) ;
- software information available in the chip's memory:
  - all the product's hardware and software identifiers can be obtained using the API and the method called "Get Product Information" as documented in the "Firmware User Manual" (cf. [GUIDES]). This API makes it possible to track all the actually configured options for each commercial derivative mainly via:

- the product identifier: the API returns the *Master ID*, which is the master product identifier (value **0061**h for the ST33G1M2) as well as the *Product ID*, which is the unique identifier of each of the products (value **00xx**h: to obtain the value of each commercial derivative, refer to [GUIDES]). For example, the ST33G1M2BP derivative (where all options are activated) will return the value 0061h for the *Master ID* and the value 006Dh for the *Product ID* ;
- Product revision: **46**h corresponds to the internal revision letter F of the product, which is the ASCII character coded in hexadecimal format written on one byte (see[GUIDES]) ;
- dedicated software identifiers:
  - **09**h: internal version of the firmware, hexadecimal value written on a byte (see [GUIDES]) ;
  - **22**h: version of the OST dedicated software, hexadecimal value written on a byte (see [GUIDES]) ;
- identifier of the MIFARE® technology library:
  - **0001**h or **0201**h: identifier of the embedded library package, hexadecimal value written on one byte (see [GUIDES]) ;

o information obtained with the order "NesLib_GetVersion":
- **1410**h: reference of cryptographic library NesLib version 4.1 (see [GUIDES] for the API description) ;

o information obtained with the order "DESFireAPI_LibraryGetVersion":
- **37**h or **38**h: references of MIFARE® DESFire® EV1 technology library revision 3.7 or 3.8 (see [GUIDES] for the API description).

1.2.3. Security services

The product provides the following main security services:
- Initialization of the hardware platform and attributes ;
- Secure management of the lifecycle ;
- Logical integrity of the product ;
- Tests of the product ;
- memory firewalls including one dedicated to embedded libraries ;
- Physical tampering protection ;
- Management of security violations ;
- Unobservability of sensitive data ;

- Secure loading and management of the Flash memory ;
- Support for symmetric key cryptography ;
- Support for asymmetric key cryptography ;
- Support for random number generation ;
- The optional NesLib v4.1 cryptographic library offering, depending on the selected configuration, RSA, SHA, and ECC implementations as well as a secure service for generating prime numbers and RSA keys ;
- The optional MIFARE® DESFire® EV1 interface.

1.2.4. Architecture

The hardware architecture of the ST33G1M2 microcontroller is illustrated in figure 1.
It is made up of:

- An ARM® SecurCore® SC000™ 32-bit RISC core processor ;
- Memories:
  - 384 to 1280 KB, configurable FLASH memory (with integrity check) with 128 KB granularity for the storage of data and dedicated test and memory-loading software (FLASH *loader*) ;
  - ROM for the storage of dedicated software ;
  - RAM ;
- functional modules: three 16-bit counters, among which one is configurable as a *watchdog*; an input/output management interface in Contact mode (IART ISO 7816-3), a serial peripheral interface (SPI)[1] and, optionally, a single-wire protocol (SWP) interface[2] ;
- security modules: memory protection unit (MPU[3]), memory protection unit dedicated to libraries (LPU), random number generator (TRNG), clock generator, security control and monitoring, power management, memory integrity control, fault detection ;
- Coprocessors:
  - EDES for supporting DES algorithms ;
  - AES for supporting AES algorithms ;
  - NESCRYPT with a dedicated RAM for supporting public key cryptographic algorithms.

In addition to these hardware components, the TOE also embeds:

- the software component dedicated (OST) to component startup (boot sequence) and microcontroller test (this software is stored in ROM and is no longer accessible once the TOE is in *Issuer* or *User* configuration) ;
- the software component dedicated (*firmware*) to Flash memory life cycle management, loading (*loader*) and interfacing with the application (*drivers*). This component is stored in ROM memory and in Flash memory.

[1] *Serial Peripheral Interface.*
[2] *Single Wire Protocol.*
[3] *Memory Protection Unit.*

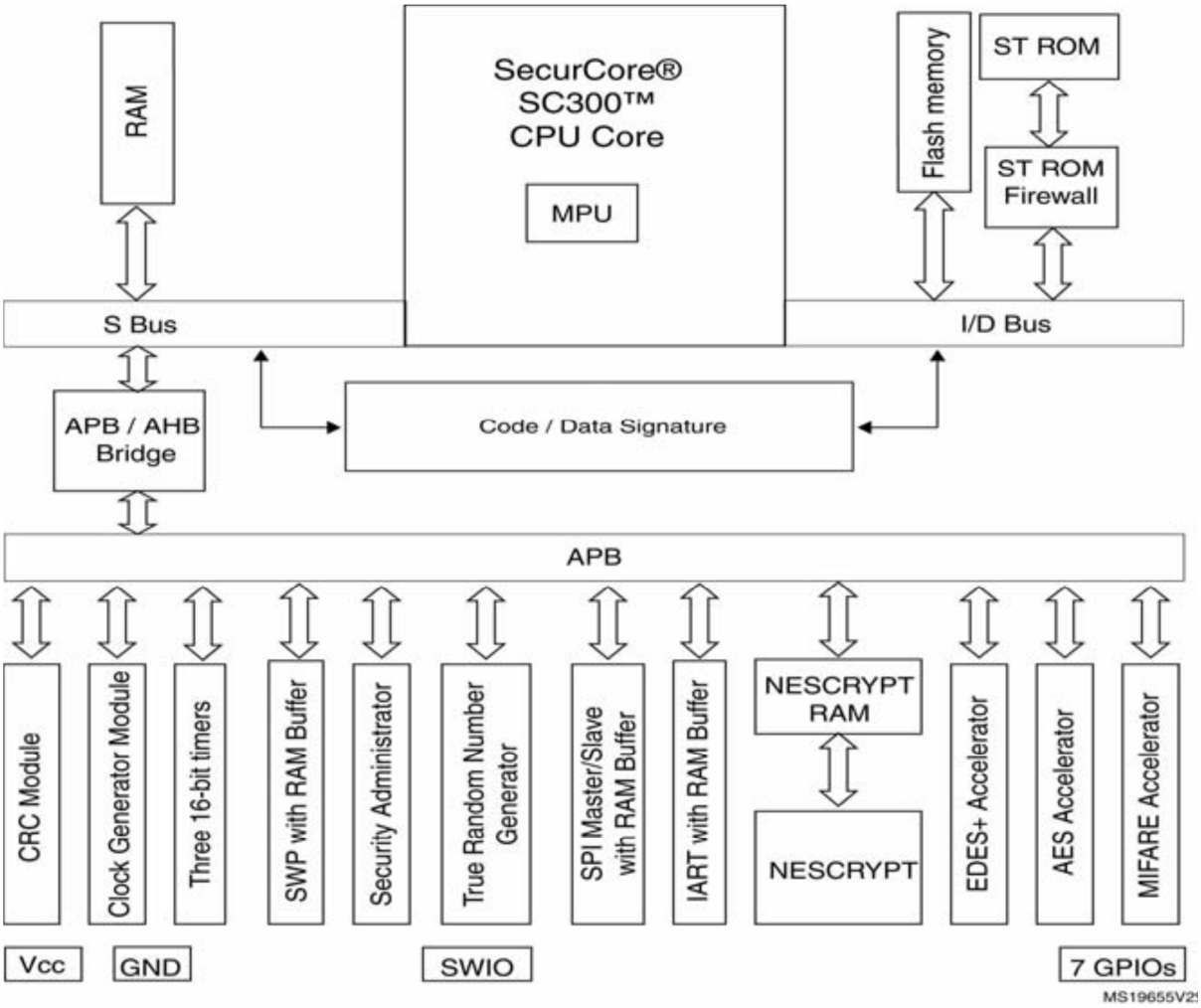

Figure 1: Architecture

Optionally, the user can also choose to integrate a cryptographic library (NesLib 4.1) that supplies implementations of cryptographic functions. Among these, RSA, SHA and ECC functions as well as a secure prime number and RSA key generator and a determinist post-processing random number function are included in the product evaluation target. The NesLib 4.1 library is embedded, either partially or totally as needed, with the client code in the non-volatile Flash memory of the product.

Optionally, the user can also choose to integrate the MIFARE® Classic library and/or MIFARE® DESFire® EV1 library version 3.7 or 3.8. The MIFARE® Classic library is outside of the scope of the certification. Only the MIFARE DESFire® EV1 library in both versions is included in the product evaluation target. According to needs, the client embeds the whole library or libraries in the product memory.

1.2.5. Life cycle

The life cycle of the product is described in the security target (see [ST]).

It includes the following sites for phase 2 (development), phase 3 (fabrication and test) and phase 4 (conditioning and final test):

STMicroelectronics Secure MCU Division 190 Avenue Célestin Coq ZI de Rousset-Peynier 13106 Rousset Cedex France	**STMicroelectronics** 5A Serangoon North Avenue 5 554574 Singapore Singapore
STMicroelectronics 635 rue des lucioles 06560 Valbonne France	**STMicroelectronics** 12 rue Jules Horowitz BP217, 38019 Grenoble Cedex France
STMicroelectronics Green Square Lambroekstraat 5, Building B, 3rd floor, 1831 Diegem/Machelen Belgium	**STMicroelectronics** 10 rue de Jouanet ePark 35700 Rennes France
Dai Nippon Printing Co., Ltd 2-2-1 Fukuoka Kamifukuoka-shi Saitama-Ken 356-8507 Japan	**Dai Nippon Printing Europe** Via C. Olivetti 2/A I-20041 Agrate Brianza Italy
STS Microelectronics 16 Tao hua Rd. Futian free trade zone 518048 Shenzhen P.R. of China	**STS Microelectronics** 629 Lorong 4/6 Toa Payoh 319521 Singapore Singapore
TSMC Fab 14, 1-1 Nan Ke Rd Tainan science park, Tainan 741-44 Taïwan Republic of China	**TSMC** Fab 2-5, Li-Hsin Rd. 6 Hsinchu science park Hsinchu 300-78 Taïwan Republic of China
STS Microelectronics 850 rue Jean Monnet 38926 Crolles France	**Smartflex** UBI rd 4, MSL building #04-04 Singapore 408618 Singapore

STS Microelectronics 9 Mountain Drive, LISP II, Brgy La Mesa Calamba, 4027 Philippines	**Nedcard** Bijsterhuizen 25-29 6604 LM Wijchen The Netherlands
STS Microelectronics 7 Loyang Drive Singapore 508938 Singapore	**Disco HI-Tec Europe GmbH** Liebigstrasse 8, D-85551 Kirchheim bei München, Germany
STS Microelectronics 18 Ang Mo Kio Industrial park 2, 569505 Singapore	**STS Microelectronics** 101 Boulevard des Muriers BP97 20180 Bouskoura Marocco
STS Microelectronics Sdn. Bhd. Tanjong Agas Industrial area. P.o. Box 28, 84007 Muar, Johor Malaysia	**Amkor** ATP1, Km 22 East Service Rd. South superhighway Mantipula City 1771 Philippines
Amkor ATP3/4, Science Avenue, Laguna technopark, Binan, Laguna, 4024 Philippines	**Stats ChipPac (SCS)** 5 Yishun St. 23, 768442 Singapore
Stats ChipPac (SCT) No 176-5, 6 Lane Hualung Chun, Chiung Lin, 307 Hsinchu, Taïwan Republic of China	**Stats ChipPac (SCC)** 188 Huaxu Rd, Qingpu district, 201702 Shanghaï Popular Republic of China
STMicroelectronics 101 Boulevard des Muriers BP97 20 180 Casablanca Morocco	

For this evaluation, the evaluator considers the developer of the user software to be embedded in the microcontroller as the user of the product.

The product manages its life cycle in the form of three configurations:

- *Test* configuration: at the end of the manufacturing phase, the microcontroller is tested using the dedicated OST test software in ROM, this configuration is then irreversibly locked by changing the configuration to Issuer or User ;
- *Issuer* configuration: this configuration features five modes:

  - *Loader installation* mode: protected mode dedicated to the loader installation, reserved for STMicroelectronics ;
  - *Flash Loader* mode: protected mode giving access to the set of application-loading instructions or to the Flash memory data ;
  - *User Emulation* mode: protected mode used to execute an application loaded in FLASH memory ;
  - *Final Test OS* mode: protected mode used by the assembly sites to perform restricted tests to verify the assembly quality, reserved for STMicroelectronics;
  - *Diagnosis* mode: mode reserved for STMicroelectronics ;
- This Issuer configuration is then locked in an irreversible manner when the product switches to User configuration ;
- User configuration: this configuration features two modes:
  - *Diagnosis* mode: mode reserved for STMicroelectronics ;
  - *End User* mode: final user mode of the microcontroller that then operates under the control of the smartcard embedded software; the test software is no longer accessible; the end users can only use the microcontroller in this configuration ;
- The component may be delivered in the *Issuer* or *User* configuration ;
- In *Issuer* configuration, the user must load the application in a secure environment.

1.2.6. Evaluated configuration

The certificate concerns the TOE defined in paragraph 1.2.1 in User configuration.
The configurations tested by the evaluator are combinations of the different hardware and software options of the TOE (activation or deactivation of the cryptographic coprocessors, library protection unit, input/output interfaces and MIFARE® libraries).

2. Evaluation

2.1. Evaluation referential

The evaluation was carried out in compliance with the **Common Criteria version 3.1, revision 4** [CC] and the evaluation methods defined in the CEM manual [CEM].

For insurance components not covered by the [CEM] manual, the evaluation facility's own evaluation methods, validated by the ANSSI, have been used.

In order to meet the specificities of smartcards, the [CC IC] and [CCDB AP] guides have been applied. In this way, the AVA_VAN level has been determined according to the rating scale of the [CCDB AP] guide. For the record, this rating scale is more stringent than the one defined by default in the standard method [CC] used for other product categories (software products, for example).

2.2. Evaluation work

The evaluation technical report [RTE], delivered to the ANSSI on July, 18, 2014, provides details on the work performed by the evaluation facility and certifies that all evaluation tasks are "**pass**".

2.3. Rating of cryptographic mechanisms according to the ANSSI technical reference framework

The rating of cryptographic mechanisms according to the ANSSI technical reference framework [REF] has not been carried out. Nonetheless, the evaluation has not detected any design or manufacturing vulnerabilities for the targeted AVA_VAN level.

2.4. Random number generator analysis

The evaluation facility evaluated the random number generator using the [AIS31] methodology.
The generator achieved the class PTG.2.

3. Certification

3.1. Conclusion

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

This certificate testifies that the "ST33G1M2 Secure microcontroller revision F, Firmware revision 9, optionally including the NesLib 4.1 cryptographic library and the MIFARE® DESFire® EV1 library revision 3.7 or 3.8" submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL 5 augmented for ALC_DVS.2 and AVA_VAN.5 components.

3.2. Restrictions

This certificate only applies to the product specified in section 1.2 of this certification report.

This certificate provides an assessment of the resistance of the "ST33G1M2 Secure microcontroller revision F, Firmware revision 9, optionally including the NesLib 4.1 cryptographic library and the MIFARE® DESFire® EV1 revision 3.7 or 3.8" to highly generic attacks due to the absence of a specific embedded application. Therefore, the security of a final product based on the evaluated microcontroller could only be assessed through a complete product evaluation, which could be performed on the basis of the evaluation results provided in section 2.

The user of the certified product must ensure compliance with the operational environmental security objectives specified in the security target [ST] and comply with the recommendations in the supplied guidance documents [GUIDES].

3.3. Recognition of the certificate

3.3.1. European recognition (SOG-IS)

This certificate is released in accordance with the provisions of the SOG-IS [SOG-IS].

The 2010 SOG-IS European recognition agreement allows the recognition, by signatory countries[1], of the ITSEC and Common Criteria certificates. The European recognition agreement, for smartcards and similar devices, is applicable up to level ITSEC E6 Elevated and CC EAL7. The certificates recognized in the scope of this agreement are released with the following marking:

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[2], of Common Criteria certificates. The mutual recognition is applicable up to the assurance components of the CC EAL4 level and also to the ALC_FLR family. The certificates recognized in the scope of this agreement are released with the following marking:

[1] The SOG-IS signatory countries are: Germany, Austria, Spain, Finland, France, Italy, Norway, the Netherlands, the United Kingdom and Sweden.

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

Annex 1. Evaluation level of the product

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+	Component name
ADV **Development**	ADV_ARC		**1**	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**5**	Complete semi-formal 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 User guidance	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**1**	1	1	1	1	1	1	**1**	Preparative procedures
ALC Life cycle support	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
	ALC_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**2**	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**2**	Compliance with implementation standards
ASE Evaluation of the security target	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claims
	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 specification
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**	Independent testing: sample
AVA Vulnerability assessment	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**5**	Advanced methodical vulnerability analysis

Annex 2. Documentary references for evaluated product

[ST]	Reference security target for the evaluation : - ST33G1M2 platform version F with firmware revision 9, optional cryptographic library NesLib 4.1 and optional technology MIFARE® DESFire® EV1 3.7 & 3.8 – Security Target, reference SMD_ST33G_ST_13_001, revision 3.02, May 2014. For publication needs, the following security target was provided and validated in the scope of this evaluation: - ST33G1M2 platform version F with firmware revision 9, optional cryptographic library NesLib 4.1 and optional technology MIFARE® DESFire® EV1 3.7 & 3.8 – Security Target, reference SMD_ST33G_ST_13_002, revision v2.03, June 2014.
[RTE]	Evaluation technical report: - Evaluation technical report Project LATOUR reference LAT_ETR, version v2.0 du 18 juillet 2014 ; - Evaluation technical report Project Lite LATOUR reference LAT_ETR Lite, version v2.0 du 18 juillet 2014.
[CONF]	Configuration list: - ST33G1M2 rev F & derivatives (incl. Firmware rev 9, NesLib v4.1, MIFARE Classic v1.3, MIFARE® DESFire® EV1 v3.7 & v3.8) CONFIGURATION LIST, reference SMD_33G_CFGL_13_001, revision 1.0, June 2014. Documentation list: ST33G1M2 rev F & derivatives (incl. Firmware rev 9, NesLib v4.1, MIFARE Classic v1.3, MIFARE® DESFire® EV1 v3.7 & v3.8) DOC REPORT, reference SMD_ST33G1M2_DR_13_001, revision 1.04, July 2014.
[GUIDES]	Product user manuals: - ST33G Platform - ST33G1M2: Secure MCU with 32-bit ARM® SecurCore® SC300™ CPU - and high density Flash memory – Datasheet, reference: DS_33G1M2, revision 3, May 2014 ; - ST33 uniform timing application note, reference: AN_33_UT revision 2, November 2013 ; - ST33G1M2 Firmware User Manual, reference UM_ST33G1M2_FW, revision 6, May 2014 ; - ST33G and ST33H Security Guidance, reference: AN_SECU_ST33, revision 1.0, February 2014 ; - ST33G and ST33H - AIS31 Compliant Random Number user manual, reference UM_33G_33H_AIS31, revision 2, February 2014 ; - ST33G and ST33H - AIS31 Reference implementation - Startup,

	online and total failure tests - Application Note, reference AN_33G_33H_AIS31, revision 1, October 2013 ; - NesLib 4.1 for ST33 Secure MCUs cryptographic library User manual, reference UM_33_NESLIB_4, revision 3, February 2014 ; - ST33 Secure MCU family NesLib 4.1 security recommendations, reference AN_SECU_33_NESLIB_4, revision 5, April 2014 ; - MIFARE® DESFire® EV1 Library 3.7 for ST33G1M2 Secure MCUs – User Manual, reference UM_MIFARE_DESFire-EV1-3.7, revision 2, February 2013 ; - MIFARE® DESFire® EV1 Library 3.8 for ST33G1M2 Secure MCUs – User Manual, reference UM_MIFARE_DESFire-EV1-3.8, revision 1, April 2013.
[BSI-PP-0035-2007]	Protection Profile - Security IC Platform Protection Profile, version v1.0 of 15 June 2007. *Certified by the BSI under reference BSI_PP_0035-2007.*

Annex 3. References associated with the certification

Decree 2002-535 of 18 April 2002 related to the evaluation and certification of the security provided by the information technology products and systems.	
[CER/P/01]	Procedure CER/P/01 Certification of the security provided by information technology products and systems, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, September 2012, version 3.1, revision 4, ref CCMB-2012-09-001; Part 2: Security functional components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-002; Part 3: Security assurance components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, September 2012, version 3.1, revision 4, ref CCMB-2012-09-004.
[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.
[CCDB AP]	CCDB-2012-04-002 - Application of attack potential to smart-cards, version 2.8, April 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 January 2010, Management Committee.
[REF]	Cryptographic mechanisms – Rules and recommendations concerning the choice and configuration of cryptographic mechanisms, version 1.20 of January 26, 2010 annexed to the General Security Reference Framework, see http://www.ssi.gouv.fr.
[AIS 31]	A proposal for: Functionality classes for random number generators, AIS20/AIS31, version 2.0, 18 September 2011, BSI (Bundesamt für Sicherheit in der Informationstechnik).