Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Prime Minister

Secretariat-General for National Defence and Security

French Network and Information Security Agency

Certification report ANSSI-CC-2017/01

ST33H768 secure microcontroller revision C, Firmware revision 5, with optional NesLib cryptographic library versions 4.1 and 4.1.1 and MIFARE4Mobile library version 2.1.0

Courtesy translation

Paris, 10 February 2017

Deputy General Director of the French Network
and Information Security Agency

Colonel Emmanuel GERMAIN
[SIGNED ORIGINAL]

SÉCURITÉ CERTIFICATION

Warning

The purpose of this report is to provide sponsors with a document enabling them to assess the security level of the product under the conditions of use or operation defined in this report for the evaluated version. This report also aims at providing 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 describes the 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 of the product by the French Network and Information Security Agency (ANSSI), and does not guarantee that the certified product is totally free of all exploitable vulnerabilities.

All correspondence concerning this report must 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

certification@ssi.gouv.fr

Certification report reference

ANSSI-CC-2017/01

Product name

ST33H768 secure microcontroller revision C, Firmware revision 5, with optional NesLib cryptographic library versions 4.1 and 4.1.1 and MIFARE4Mobile library version 2.1.0

Product reference/version

Maskset reference K8K0A, internal revision C,
firmware revision 5

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, 13106 Rousset, France

Sponsor

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

Evaluation facility

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

Mutual Recognition Agreements

CCRA

The product is recognized at level EAL2.

SOG-IS

Introduction

Certification

Certification for the security provided by information technology products and systems is governed by decree number 2002-535 of 18 April 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 certification procedures are available on the Internet site www.ssi.gouv.fr.

Table of contents

1. Product

1.1. Product overview

The evaluated product is the "ST33H768 secure microcontroller revision C, Firmware revision 5, with optional NesLib cryptographic library versions 4.1 and 4.1.1 and MIFARE4Mobile library version 2.1.0" developed by *STMICROELECTRONICS*.

The ST33H768 product derivatives included in this platform are defined by a number of hardware and software options configurable by the final customer. These options concern the non-volatile Flash memory size, the activation of the cryptographic coprocessors, library protection unit (LPU[1]), input/output interfaces, NesLib cryptographic library and MIFARE4Mobile library. This library may include the MIFARE® DESFire® EV1 or MIFARE® Classic® functionalities (the latter is out of the scope of this certification).

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 This card has many possible uses (secure identity documents as well as bank, pay TV, transport, health applications, 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. 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 access controls, 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;

[1] *Library Protection Unit*.

- Support for asymmetric key cryptography;
- Support for random number generation;
- The optional NesLib v4.1 and v4.1.1 cryptographic libraries offering RSA, SHA and ECC implementations as well as a secure service for generating prime numbers and RSA keys depending on the selected configuration;
- The optional MIFARE4Mobile library including the MIFARE® DESFire® EV1 functionality.

1.2.3. Architecture

The hardware architecture of the ST33H768 microcontroller is illustrated in figure 1.

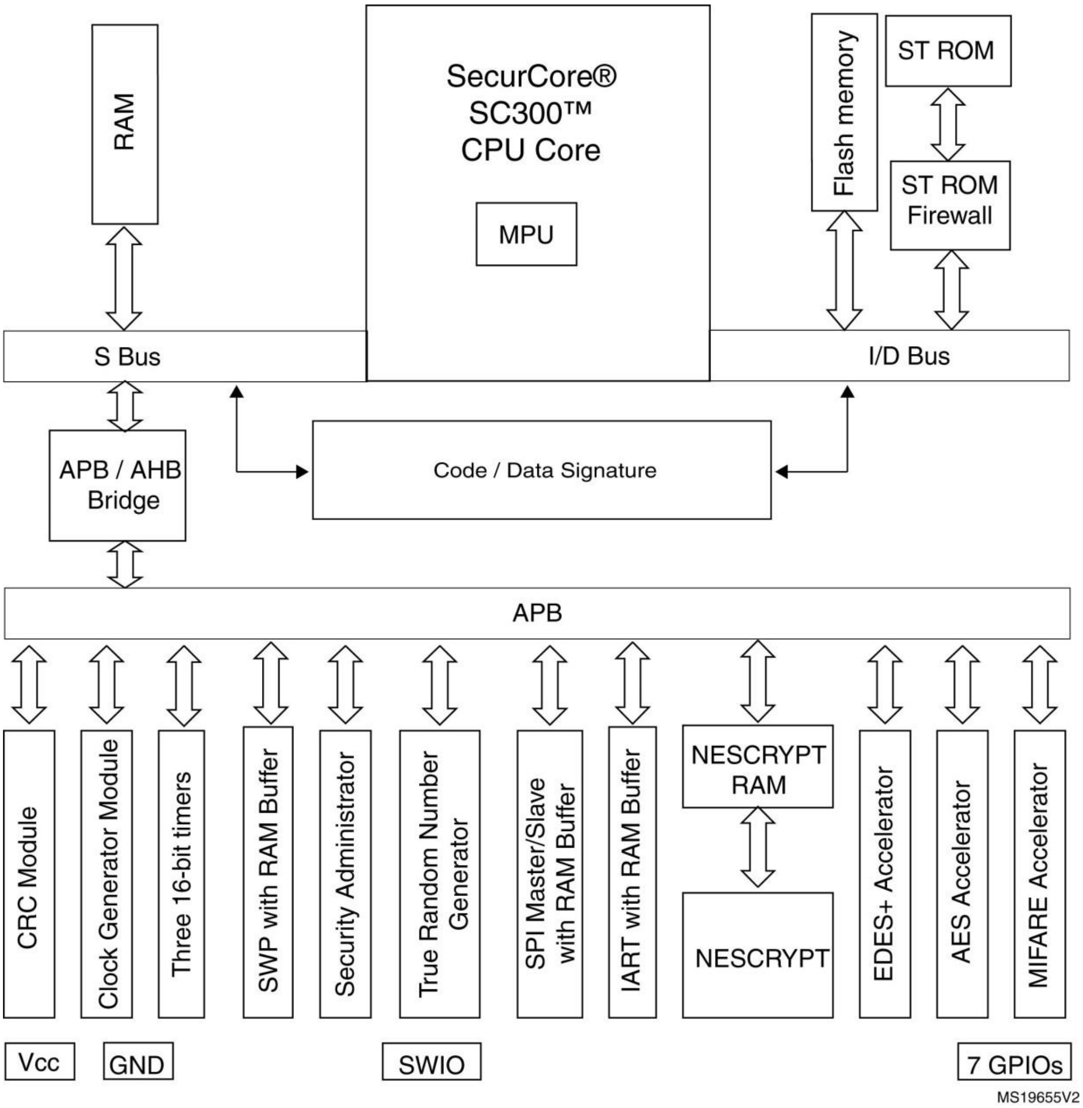

Figure 1: Architecture

It is made up of:

- an ARM® SecurCore® SC300™ 32-bit RISC core processor;
- Memories:
    - configurable 384 to 768 KB 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 storing dedicated software;
    - RAM;
- functional modules: three 16-bit timers, among which one is configurable as a *watchdog*, an input/output management block in contact mode (IART ISO 7816-3), a serial peripheral interface (SPI)[1] (operating in Slave and Master modes) 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 stored in ROM is no longer accessible once the TOE is in *Issuer* or *User*) configuration;
- The software component dedicated to the Flash memory lifecycle management (*firmware*), loading (*loader*) and interfacing with the application (*drivers*). This component is stored in ROM and Flash memory.

Optionally, the user can also choose to integrate a cryptographic library (NesLib version 4.1 or version 4.1.1) that supplies implementations of the cryptographic functions. Among these, the RSA, SHA and ECC functions, as well as a secure service for prime number and RSA key generation, and a determinist post-processing random number function, are included in the product evaluation. The NesLib library version 4.1 or version 4.1.1 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 MIFARE4Mobile library version 2.1.0. This library includes the MIFARE DESFire® EV1 and MIFARE® Classic functionalities. The MIFARE® Classic functionalities are out of the scope of this certification.

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

1.2.4. 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]):

- information engraved on the component's surface:
    - product identifier: **K8K0A** (major revision of the *maskset* corresponding to the ST33H768 platform);
    - Identification of the manufacturing site: **ST_4** (STMicroelectronics Rousset), **ST_3** (STMicroelectronics Crolles), **ST_2** (TSMC);
    - version of the dedicated OST[1] software: **YQB**;
- 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* (see [GUIDES]). This API makes it possible to track all the actually configured options for each commercial derivative mainly via:
        - product identifier : the API returns the *Master ID* which is the master product identifier (value **0098**h for the ST33H768) product 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 ST33H768 derivative (where all options are activated) will return the value 0098h for the *Master ID* and the value 009Eh for the *Product ID*;
        - product revision: **43**h corresponds to the product's internal revision letter C, which is the ASCII character coded in hexadecimal format written on one byte (see [GUIDES]);
        - dedicated software identifiers:
            - **05**h : internal *firmware* version, hexadecimal value written on a byte (see [GUIDES]);
            - **22**h: version of the dedicated OST software; hexadecimal value written on a byte (see [GUIDES]);
    - information obtained with the "NesLib_GetVersion" command:
        - **1410**h: reference of the NesLib cryptographic library version 4.1;
        - **1411**h: reference of cryptographic library NesLib version 4.1.1 (see [GUIDES] for the API description);
    - information obtained with the "M4MAPI_LibraryGetVersion" command:
        - **020100**h: reference of the MIFARE4Mobile technology library revision 2.1.0 (see [GUIDES] for the API description).

1.2.5. Lifecycle

The product lifecycle is described in the security target (see [ST]).

[1] *Operating System for Test.*

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*** 12 rue Jules Horowitz BP217, 38019 Grenoble Cedex France
STMICROELECTRONICS 635 rue des lucioles 06560 Valbonne France	***STMICROELECTRONICS*** 10 rue de Jouanet ePark 35700 Rennes France
STMICROELECTRONICS Green Square Lambroekstraat 5, Building B, 3rd floor, 1831 Diegem/Machelen Belgium	***DAI NIPPON*** **Printing Europe** Via C. Olivetti 2/A I-20041 Agrate Brianza Italy
DAI NIPPON **Printing Co., Ltd** 2-2-1 Fukuoka Kamifukuoka-shi Saitama-Ken 356-8507 Japan	***STMICROELECTRONICS*** 629 Lorong 4/6 Toa Payoh 319521 Singapore Singapore
STS MICROELECTRONICS 16 Tao hua Rd. Futian free trade zone 518048 Shenzhen People's Republic of China	***TSMC*** Fab 2-5, Li-Hsin Rd. 6 Hsinchu science park Hsinchu 300-78 Taïwan République de Chine
TSMC Fab 14, 1-1 Nan Ke Rd Tainan science park, Tainan 741-44 Taïwan République de Chine	***SMARTFLEX*** UBI rd 4, MSL building #04-04 Singapore 408618 Singapore
STMICROELECTRONICS 850 rue Jean Monnet 38926 Crolles France	***NEDCARD*** Bijsterhuizen 25-29 6604 LM Wijchen The Netherlands

STMicroelectronics 9 Mountain Drive, LISP II, Brgy La Mesa Calamba, 4027 Philippines	***STMicroelectronics*** 101 Boulevard des Muriers BP97 20180 Bouskoura Morocco
STMicroelectronics 7 Loyang Drive Singapore 508938 Singapore	***Amkor*** ATP1, Km 22 East Service Rd. South superhighway Mantipula City 1771 Philippines
STMicroelectronics 18 Ang Mo Kio Industrial park 2, 569505 Singapore	***Amkor*** ATT1: 1F, No.1, Kao-Ping Sec, Chung-Feng Rd, Lungtan Township Taoyuan County 325, Taïwan People's Republic of China
STMicroelectronics Sdn. Bhd. Tanjong Agas Industrial area. P.o. Box 28, 84007 Muar, Johor Malaysia	**Stats ChipPac (SCS)** 5 Yishun St. 23, 768442 Singapore
Amkor ATP3/4, Science Avenue, Laguna technopark, Binan, Laguna, 4024 Philippines	***Stats ChipPac* (SCC)** 188 Huaxu Rd, Qingpu district, 201702 Shanghaï People's Republic of China
STMicroelectronics 7 Loyang Drive Singapore 508938 Singapore	***Stats ChipPac* (SCT)** No 176-5, 6 Lane Hualung Chun, Chiung Lin, 307 Hsinchu, Taïwan People's Republic of China
STMicroelectronics 5A Serangoon North Avenue 5 554574 Singapore Singapore	

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 lifecycle 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 the following modes:
    - *Final Test OS* mode: protected mode used by the assembly sites to perform restricted tests to verify the assembly quality, reserved for *STMICROELECTRONICS*;
    - *Install* mode (or *Flash loader*): protected mode dedicated to the loader installation, reserved for *STMICROELECTRONICS*;
    - User Emulation mode: protected mode used to execute an application loaded in Flash memory;
    - *Diagnosis* modes (*reduced* or *extended*) : modes 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 the following modes:
    - *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;
    - *Diagnosis* modes (*reduced* or *extended*) : modes reserved for *STMICROELECTRONICS*.

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 applies to the TOE defined in section 1.2.1 in *User* configuration.
The configurations tested by the assessor are combinations of the different hardware and software options of the TOE (activation or deactivation of the cryptographic coprocessors, library protection unit and input/output interfaces).

2. Evaluation

2.1. Evaluation reference frame

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 [JIWG IC] and [JIWG AP] guides have been applied. In this way, the AVA_VAN level has been determined according to the rating scale of the [JIWG 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 is based on the evaluation results of the product: "ST33H768 secure microcontroller revision C, Firmware revision 4, with optional NesLib cryptographic library version 4.1 and version 4.1.1" certified on 15 September 2015 under the reference [CER-2015/36] and maintained on 17 March 2016 under the reference [MAIN-2015/36].
The evaluation technical report [RTE], delivered to the ANSSI on 30 September 2016, details 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 [AIS 31] methodology and found that it meets the requirements of the PTG.2 class.
This analysis did not put in evidence any statistic bias forbidding the direct use of the generator outputs. This analysis is not sufficient to state that the generated data are really random, but it ascertains that the generator does not have major design defects. As stipulated in the [REF] document, it is reminded that, for a cryptographic usage, the hardware random number generator output must imperatively be submitted to a cryptographic algorithm reprocessing even if the analysis of the physical random number generator has revealed no weaknesses.

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 work performed permits the release of a certificate in compliance with the decree 2002-535.

This certificate testifies that the "ST33H768 secure microcontroller revision C, Firmware revision 5, with optional NesLib cryptographic library versions 4.1 and 4.1.1 and MIFARE4Mobile library version 2.1.0", which was submitted for evaluation, fulfils the security features specified in the security target [ST] for evaluation level EAL5 augmented for ALC_DVS.2 and AVA_VAN.5 components.

3.2. Usage 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 "ST33H768 secure microcontroller revision C, Firmware revision 5, with optional NesLib cryptographic library versions 4.1 and 4.1.1 and MIFARE4Mobile library version 2.1.0" 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 current evaluation results provided in section 2.

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

3.3. Certificate recognition

3.3.1. European recognition agreement (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 when the CC requirements are satisfied. The certificates recognized in the scope of this agreement are released with the following marking:

INFORMATION TECHNOLOGY SECURITY
SOGIS
IT SECURITY CERTIFIED
MUTUAL RECOGNITION AGREEMENT

3.3.2. Common Criteria Recognition Arrangement (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 following countries have signed the SOG-IS agreement: Germany, Austria, Spain, Finland, France, Italy, Norway, the Netherlands, the United Kingdom and Sweden.

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

Annexe 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 Support to lifecycle	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 lifecycle 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 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

Annexe 2. Documentary references for evaluated product

[ST]	Reference security target for the evaluation : - ST33H768 platform maskset K8K0A version C with firmware revision 5, optional cryptographic library NesLib 4.1 and 4.1.1 and optional technology MIFARE4Mobile® 2.1.0 – Security Target, reference SMD_ST33H_ST_16_001, revision 1.03, September 2016. For publication needs, the following security target was provided and validated in the scope of this evaluation: - ST33H768 platform maskset K8K0A version C with firmware revision 5, optional cryptographic library NesLib 4.1 and 4.1.1 and optional technology MIFARE4Mobile® 2.1.0 – Security Target for composition, reference SMD_ST33H_ST_16_002, revision v1.00, September 2016.
[RTE]	Evaluation technical reports: - Evaluation technical report Project: ST33H768 with M4M, reference LAT2M_ETR, version v1.0 of 30 September 2016; - Evaluation technical report for composite evaluation Project: ST33H768 with M4M, reference LAT2M_ETRLite, version v1.0 of 2 December 2016.
[CONF]	Configuration list: - ST33H768 rev C & derivatives (incl. Firmware rev 5, Optional NesLib 4.1 and 4.1.1, MIFARE4Mobile v2.1.0) CONFIGURATION LIST, reference SMD_ST33H_CFGL_16_001, revision 1.02, September 2016. Documentation list: - ST33H768 rev C & derivatives (incl. Firmware rev 5, opt. NesLib 4.1 and 4.1.1, opt. MIFARE4Mobile v2.1.0) DOCUMENTATION REPORT, reference SMD_ST33H768_DR_14_001, revision 1.06, September 2016.
[GUIDES]	Product user guides: - ST33H Platform - ST33H768: Secure MCU with 32-bit ARM® SecurCore® SC300TM CPU - and high density Flash memory – Datasheet, reference: DS_ST33H768, revision 4, April 2015; - ST33H768: BP and BM specific product profiles – Technical note, reference TN_ST33H768_01, revision 1, April 2015; - ST33H768: LS, LC and BS specific product profiles – Technical note, reference TN_ ST33H768_02, revision 1, April 2015; - ST33H768: CMOS M10+ 80 nm technology die and wafer delivery description, reference DD_ST33H768, revision 2, March 2014; - ST33 uniform timing application note, reference: AN_33_UT revision 2, November 2013;

	- ST33H768 Firmware User manual, reference UM_ST33H768_FW, revision 5, May 2015; - ST33G and ST33H Security Guidance, reference AN_SECU_ST33, revision 5.0, February 2016; - ST33G and ST33H Power supply glitch detector characteristics - Application note, reference AN_33_GLITCH, revision 2.0, January 2014; - ST33G and ST33H - AIS31 Compliant Random Number user manual, reference UM_33G_33H_AIS31, revision 3, October 2015; - ST33G and ST33H - AIS31 Reference implementation - Startup, online and total failure tests - Application note, reference AN_33G_33H_AIS31, revision 1, October 2013; - ST33 ARM Execute-only memory support for SecurCore SC300 devices - Application note, reference AN_33_EXE, revision 2, November 2014; - ST33 NesLib Library User manual, NesLib 4.1 and 4.1.1 for ST33 Secure MCUs, reference UM_33_NESLIB_4, revision 4, December 2014; - NesLib 4.1 for ST33 – Limitations versus NesLib 4.1.1, reference TN_ST33G_NesLib4.1, revision 4, July 2015; - ST33 Secure MCU family NesLib 4.1 and NesLib 4.1.1 security recommendations, reference AN_SECU_33_NESLIB_4, revision 7, April 2015; - ST33H and derivatives – Flash loader installation guide, reference UM_33H_FL_v4, revision 4, August 2015; - MIFARE4Mobile® library 2.1 – User manual, reference UM_MIFARE4Mobile-2.1, revision 5, June 2015; - MIFARE4Mobile® Library 2.1 for ST33G1M2 – Application note, reference AN_ST33G1M2_M4M_Lib, revision 1, June 2015.
[CER-2015/36]	Certification report ANSSI-CC-2015/36 "ST33H768 secure microcontroller revision C, Firmware revision 4, with optional NesLib cryptographic library version 4.1 and version 4.1.1", released on 15 September 2015, ANSSI.
[MAIN-2015/36]	Maintenance report ANSSI-CC-2015_36_M01 "ST33H768 secure microcontroller revision C, Firmware revisions 4 and 5, with optional NesLib cryptographic library version 4.1 and version 4.1.1", released on 17 March 2016, ANSSI.
[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.

Annexe 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.
[JIWG IC] *	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, February 2009.
[JIWG AP] *	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, January 2013.
[CC RA]	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 July 2014.
[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).

*Document of the SOG-IS; in the frame of the mutual recognition agreement of the CCRA, the support equivalent CCRA document applies.