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-2014/60

SC23Z018, SC23ZD12, SC23ZD08, SC23ZD04, SB23ZD18, SB23ZD12, SB23ZD08 and SB23ZD04 Secure microcontrollers with optional cryptographic library NesLib revision 3.1

Maskset K390A, internal revision H

Paris, October 21, 2014

Courtesy Translation

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 ANSSI (French Network and Information Security Agency), 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.anssi@ssi.gouv.fr

Reproduction of this document without any changes or editing is authorized.

Certification report reference

ANSSI-CC-2014/60

Product name

SC23Z018, SC23ZD12, SC23ZD08, SC23ZD04, SB23ZD18, SB23ZD12, SB23ZD08 and SB23ZD04 Secure microcontrollers with optional cryptographic library NesLib revision 3.1

Product reference/version

Maskset reference K390A, internal revision H

Protection profile conformity

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

Evaluation criteria and version

Common criteria version 3.1 revision 4

Evaluation level

EAL5 Augmented
ALC_DVS.2, AVA_VAN.5

Developer

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

Serma Technologies
14 rue Galilée, CS 10055, 33615 Pessac Cedex, France

Mutual Recognition Agreements

CCRA

SOG-IS

The product is recognized at level EAL4.

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 fulfill 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 products are the "SC23Z018, SC23ZD12, SC23ZD08, SC23ZD04, SB23ZD18, SB23ZD12, SB23ZD08 and SB23ZD04 Secure microcontrollers with optional NesLib cryptographic library revision 3.1, maskset reference K390A, internal revision H" developed by STMicroelectronics.

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 2.1 "TOE overview" and [GUIDES]):

- Information written on the microcontroller:
  - K390A: STMicroelectronics internal name of the ST23 family product, where the letter A identifies the major silicon revision letter:
  - YID: 3-digit code identifying the dedicated software also called the OST[1] (*Operating system for Test*);
  - UZU[2]: 3-digit code identifying the user software embedded in ROM in the case of this evaluation, it identifies the STMicroelectronics demonstration operating system called *Card Manager*. The Card Manager is not in the scope of this evaluation;
  - ST4: Identification of the manufacturing site (here, 4 corresponds to the STMicroelectronics site in Rousset, France);

[1]Dedicated operating system for the testing and maintenance of the TOE.
[2]This 3-digit code identifies the embedded software and is unique for each user as the embedded software is supplied by the customer to the sponsor for storage in the ROM. This 3-digit code included on all chips supplied to the customer will inevitably be different than the one appearing on the evaluated microcontrollers.

  - Identification, by a single letter, of the revision of each level of the manufacturing process corresponding to the sequence of masks ("Maskset") with internal revision H;
- information present in the OTP area ("One Time Programmable*") of the EEPROM*:
  - Identifier (see the table below) of SC23Zxxx/SB23ZDxx products, written on 2 bytes (see [GUIDES] for the EEPROM location);
  - *6Bh* : version of the OST dedicated software , hexadecimal value written on a byte (see [GUIDES] for the EEPROM location);
  - *48h: Product internal revision letter H, ASCII character coded in hexadecimal format written on 1 byte (see [GUIDES] for the EEPROM location)..*
- information returned by the cryptographic library (for SC23Zxxx products):
  - NesLib provides an API which returns the value 1310 to identify the NesLib version 3.1 (see [GUIDES]).

Commercial name	Product identifier	Non-volatile memory	NESCRYPT[1]
SC23Z018A	003Ah	18 Kbytes	Yes
SC23ZD12A	003Bh	12 Kbytes	Yes
SC23ZD08A	003Ch	8 Kbytes	Yes
SC23ZD04A	003Dh	4 Kbytes	Yes
SB23ZD18A	003Eh	18 Kbytes	No
SB23ZD12A	003Fh	12 Kbytes	No
SB23ZD08A	0040h	8 Kbytes	No
SB23ZD04A	0041h	4 Kbytes	No

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 firewall;
- Physical tampering protection;
- Management of security violations;
- Unobservability of sensitive data;
- Secure management of the EEPROM;
- Support for symmetric key cryptography;
- Support for asymmetric key cryptography;
- Support for random number generation;
- The NesLib V3.1 cryptographic library offering, depending on the selected configuration, RSA, SHA, AES, and ECC implementations as well as a secure service for generating prime numbers and RSA keys.

[1] Description in chapter 1.2.4 Architecture.

1.2.4. Architecture

The TOE hardware architecture is shown in Figure 1.
The SC23Zxxx/SB23ZDxx microcontrollers include the following components:

- an 8/16-bit processor;
- memories:
  - 4/8/12/18 KB of EEPROM (with integrity check) for data storage;
  - 252 KB of ROM for user program storage;
  - 6 KB of RAM;
- Security modules: Memory protection unit (MPU), clock generator, security control and monitoring, power management, memory integrity control, fault detection;
- functional modules: three 8-bit counters, an input/output management function (IART ISO 7816-3 and I2C), a random number generator (TRNG);
- coprocessors:
  - EDES for supporting DES algorithms;
  - NESCRYPT with a dedicated RAM for supporting public key cryptographic algorithms (coprocessor only available for microcontrollers SC23Zxxx);

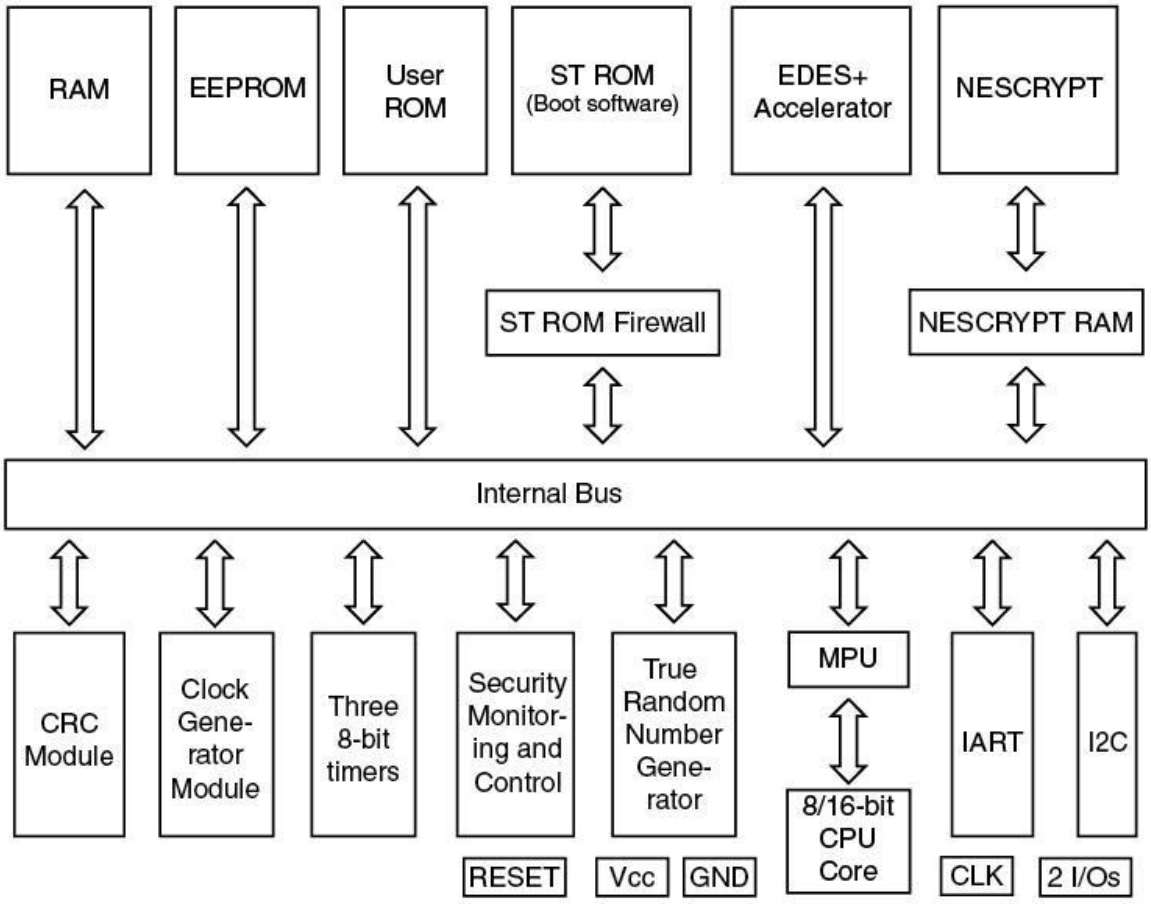

Figure 1: Architecture

The user can also choose to integrate a cryptographic library (NesLib v3.1) that supplies implementations of RSA, SHA, AES, and ECC cryptographic functions as well as a secure service for generating prime numbers and RSA keys. This library is included in the security target of the product and each of its derivatives. The library is partially or completely embedded according to requirements, with the customer code client, in the product ROM.

In addition to these hardware components and the cryptographic library, the TOE also embeds a dedicated operating system for test (OST) in the ROM.
The OST:

- starts the product ("Boot*");*
- provides commands for the testing and maintenance of the TOE;
- also controls the access to these functions when the TOE is in *Test* or User *configuration.*

This software component can no longer be accessed by the application embedded by the user of the TOE once it is configured for use in the field; i.e. the "end user" configuration.

1.2.5. Life cycle

The following figure illustrates the life cycle of the product in the global cycle of a smart card:

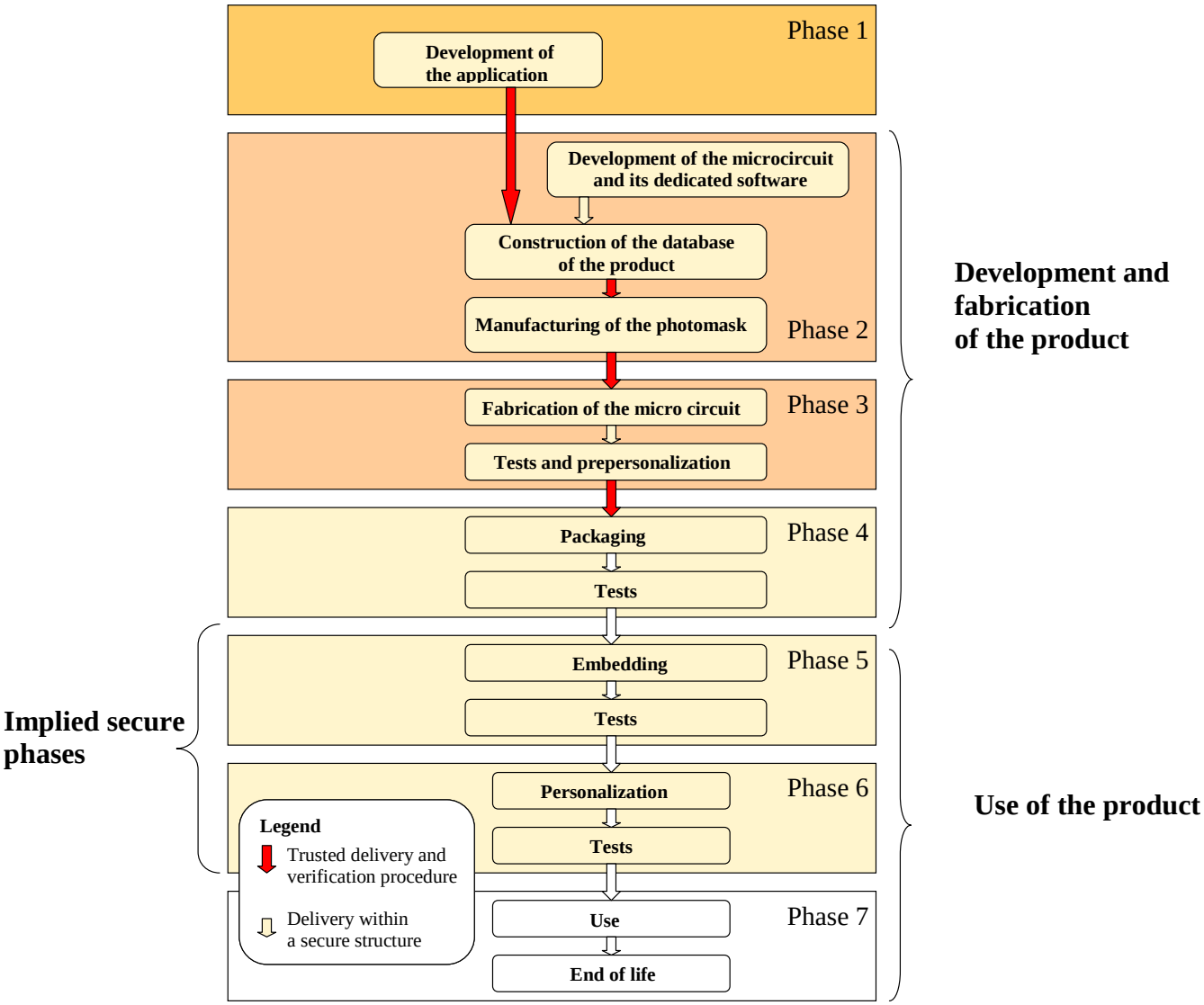

Figure 2: Life cycle

The product is developed at the following sites (Phases 2, 3 and 4):

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, Lamboekstraat 5, Building B, 3d Floor, 1831 Diegem/Machelem, 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	**STMicroelectronics** 629 Lorong 4/6 Toa Payoh 319521 Singapore Singapore
Global Foundries 60 Woodlands industrial park, D street 2 Singapore 738406 Singapore	**CMP Georges Charpak** 880 Avenue de Mimet 13542 Gardanne France
STS Microelectronics 101 Boulevard des Muriers BP97 20180 Bouskoura Marocco	**Smartflex** 27 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

For this evaluation, the evaluator considers the developer of the user software to be embedded in the microcontroller as the user of the product (there is no “administrator” defined in the product).

The product provides its own life cycle management system in the form of two operating configurations:

- "Test" configuration: at the end of the manufacturing phase, the microcontroller is tested using the test software included in ROM; the pre-personalization data can be loaded in EEPROM; this configuration is then irreversibly blocked when it switches to "User" configuration;
- "User" configuration: this mode consists of three sub-modes:
    - "Reduced test" mode that enables STMicroelectronics to perform several restricted tests;
    - "Diagnostics" mode: a part of the "Reduced test" 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.

1.2.6. Evaluated configuration

The certificate applies to the TOE defined in paragraph 1.2.1 in User configuration.
For the requirements of this evaluation, the samples of the TOE delivered to the evaluator have a "Card Manager" operating system embedded in the ROM. This OS is identified by the UZU 3-digit code and its purpose is to enable:

- interaction with the TOE through commands sent by the I/O
- loading test applications in EEPROM, or in RAM.

This "Card Manager" is not included in the scope of this evaluation.

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 [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 "SC23Z018, SC23ZD12, SC23ZD08, SC23ZD04, SB23ZD18, SB23ZD12, SB23ZD08 and SB23ZD04 Secure microcontrollers with optional NesLib cryptographic library revision 3.1, maskset K390A, internal revision C" certified on September 13, 2013 under the reference [ANSSI-CC-2013/61].

The evaluation technical report [RTE], delivered to ANSSI on the 23th of September 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.5 level.

2.4. Random number generator analysis

The evaluation facility evaluated the random number generator using the [AIS 31] methodology.
The generator achieved the class "P2 – High level".

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 "SC23Z018, SC23ZD12, SC23ZD08, SC23ZD04, SB23ZD18, SB23ZD12, SB23ZD08 and SB23ZD04 Secure microcontrollers, optionally including the NesLib 3.1 cryptographic library, with maskset reference K390A, internal revision H" submitted to 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 SC23Z018, SC23ZD12, SC23ZD08, SC23ZD04, SB23ZD18, SB23ZD12, SB23ZD08 and SB23ZD04 Secure microcontrollers, optionally including the NesLib revision 3.1 cryptographic library 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. 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, 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. 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, 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:

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 life cycle	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

Annexe 2. Documentary references for evaluated product

[ST]	Reference security target for the evaluation : - *SC23Z018 and 7 derivative products with optional cryptographic library NESLIB 3.1 SECURITY TARGET*, reference: SMD_SC23Z018_ST_12_001_V02.07, version 2.07 of August 28, 2014, STMicroelectronics. For publication requirements, the following security target was provided and validated in the scope of this evaluation : - *SC23Z018 and 7 derivative products with optional NesLib3.1 Security Target - Public Version*, reference: SMD_SC23Z018_ST_13_001 Rev 01.07, of August 28, 2014, STMicroelectronics.
[RTE]	Evaluation technical report: - *Evaluation Technical Report POMEROL-2 Project,* reference: POMEROL_SC23Z018H_ETR_v1.1, version 1.1 of September 23, 2014, SERMA Technologies. For the composition evaluation needs for this microcontroller, a technical report on composition has been validated: - *ETR Lite for Composition SC23Z018 Project*, reference: SC23Z018H_ETRLiteComp_v1.1, version 1.1 of September 23, 2014, SERMA Technologies.
[CONF]	Configuration list: - SC23Z018 & Derivatives Configuration List, reference: SMD_SC23Z018_CFLG_14_001, version 1.0, STMicroelectronics. Documentation list: - SC23Z018 Evaluation Documentation Report rev2.03, reference: SMD_SC23Z018_DR_13_001, version v2.03, STMicroelectronics.

[GUIDES]	Product user guide: - *SC23Zxxx/SB23ZDxx Secure MCU with enhanced security, crypto-processor, 18-Kbyte EEPROM and I2C-bus Fast-mode slave interface – Datasheet*, reference: DS_SC23Z018, version 2, March 2014, STMicroelectronics; - *Application note SB23Z012/SC23Z018 and derivative devices security guidance*, reference: AN_SECU_Sx23Z0xx, version 4, September 5, 2014, STMicroelectronics ; - *User Manual – ST23 Secure MCUs NesLib 3.1 cryptographic library*, reference UM_23_NesLib_3.1, version 5, August 30, 2013, STMicroelectronics; - *Application Note, ST23Z secure microcontrollers power supply glitch detector characteristics*, reference AN_23Z_GLITCH, version 1, February 2013; - *ST23 – AIS31 Compliant Random Number user manual*, reference: UM_23_AIS31, revision 2, February 2013; - *ST23 – AIS31 Reference Implementation – Start-up, online and total failure tests – Application Note AN_23AIS31*, revision 2, September 2009.
[PP0035]	Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. *Certified by the BSI (Bundesamt für Sicherheit in der Informationstechnik) under reference BSI_PP_0035-2007.*
[ANSSI-CC-2013/61]	Secure microcontrollers SC23Z018, SC23ZD12, SC23ZD08, SC23ZD04, SB23ZD18, SB23ZD12, SB23ZD08 and SB23ZD04 with cryptographic library NesLib revision 3.1 in option. Certified by the ANSSI on September 13, 2013 under reference ANSSI-CC-2013/61.

Annexe 3. References associated with the certification

Decree 2002-535 of 18 April 2002 modified 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, ANSSI.
[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.
[COMP] *	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.2, January 2012.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, 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 2.03 of 21 February 2014 annexed to the General Security Reference Framework, see http://www.ssi.gouv.fr.
[AIS 31]	Functionality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25 September 2001, 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.