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-2012/77

ST23R160/80A/48A and ST23L160/80A/48A Secure microcontroller, optionally including the NesLib v3.1 cryptographic library

Maskset K2V0A, internal revision B

Paris, November 8th, 2012

Courtesy Translation

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-2012/77

Product name

ST23R160/80A/48A and ST23L160/80A/48A Secure microcontroller, optionally including the NesLib v3.1 cryptographic library.

Product reference

Maskset K2V0A, internal revision B

Protection profile conformity

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

Evaluation criteria and version

CC version 3.1 revision 3

Evaluation level

EAL6 Augmented
ALC_FLR.1

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

SERMA Technologies
30 Avenue Gustave Eiffel, 33608 Pessac Cedex, 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. The product

1.1. Presentation of the product

The evaluated products are the ST23R160/80/48A and ST23L160/80A/48A in internal revision B, developed by STMicroelectronics, including optionally the NesLib v3.1 cryptographic library.
The table below describes the different possible EEPROM memory sizes and possible interfaces for the variants of products:

Products	ST23R160	ST23R80A	ST23R48A	ST23L160	ST23L80A	ST23L48A
EEPROM Memory size	160K	80K	48K	160K	80K	48K
Interfaces	"Dual" Mode (contact and contactless)			Contact mode only		

Note: memory is still physically at size of 160 Ko but its capacity is restricted according to the variants.

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. The software applications are not in the scope of this evaluation.

1.2. Evaluated 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].

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 written on the microcontroller:

- K2V0A: STMicroelectronics internal name of the product, also called Maskset, the letter A identifies the major silicon revision number;
- AZB: reference identifying the dedicated software also called the OST [1] (Operating System for Test - dedicated operating system for boot sequence, tests and product maintenance);
- UZC[1]: reference identifying the user software embedded in User 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, refer §1.2.5;
- ST4: Identification of the Rousset manufacturing site.

Additional information is present in the OTP area (*One Time Programmable*) of the EEPROM memory (cf. [GUIDES]), in the following addresses:

Addresses	Item	ST23R160	ST23R80A	ST23R48A	ST23L160	ST23L80	ST23L48A
C007h C008h	Circuit	0019h	001Bh	001Ch	001Dh	001Eh	001Fh
C00Eh	OST Version	4Fh					
C011h	Internal revision	42h[2]					

The Neslib cryptographic library could be identified through the internal command "NesLib_GetVersion" that provides a value on 2 bytes (refer to [GUIDES]): "1310h" for NesLib version 3.1.

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;
- Test of the product;
- Memory management (firewall);
- Physical tampering protection;
- Management of security violations;
- Unobservability of sensitive data;

[1]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.
[2] ASCII code in hexadecimal of character B (internal revision of Maskset).

- Support for symmetric key cryptography;
- Support for asymmetric key cryptography;
- Support for random number generation;
- The 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 protected against side channel attacks.

1.2.4. Architecture

The ST23R160/80A/48A and ST23L160/80A/48A microcontroller consists of the following components:

- A hardware part with:
  - A 8/16-bit processor;
  - Memories:
    - 160/80/48 Kbytes (according to version including 128 bytes of OTP) EEPROM (with integrity detection) for storing data;
    - 390 Kbytes of ROM for storing user applications;
    - 6 Kbytes of RAM;
    - 20 Kbytes of ROM for storing the dedicated software (test software);
  - Security modules: Memory protection unit (MPU), clock generator, security control and monitoring, power management, memory integrity control, fault detection;
  - Functional modules: three 8-bit timers, input/output management function in contact mode (IART ISO 7816-3), a random number generator (TRNG), EDES coprocessor for supporting DES algorithms, AES coprocessor for supporting AES algorithms, NESCRYPT coprocessor with a dedicated 2Kbytes RAM for supporting public key cryptographic algorithms;
  - for ST23R160/80A/48A versions only, an ISO 14443 type B and B' radio frequency communication module;

- A part " dedicated software" in ROM which includes:
  - operating system for product test;
  - utilities for system and hardware/software interface management;

- A cryptographic library (Neslib v3.1) offering RSA, SHA, AES, and ECC cryptographic services, as well as a secure service for generating prime numbers and RSA keys protected against side channel attacks.

This library is fully part of the product security target. This library is linked with the Customer code, and so is embedded in the Customer ROM memory in the product.

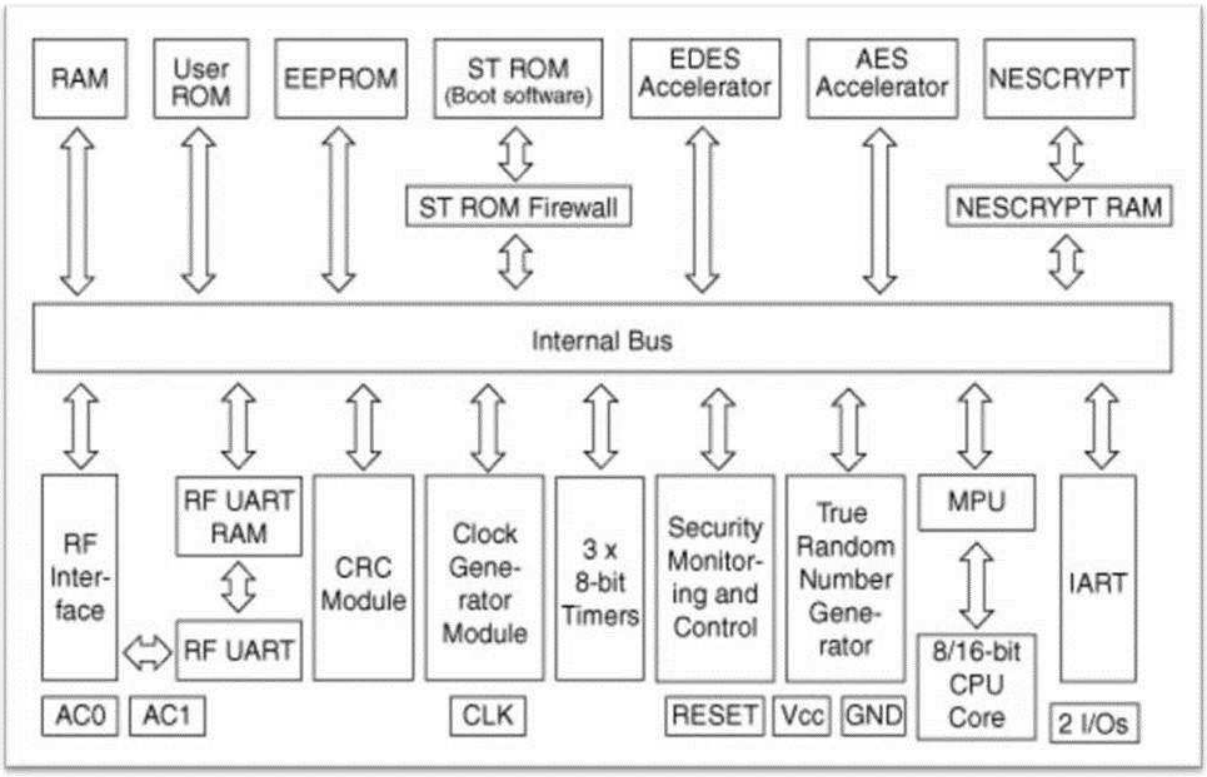

Figure 1. Architecture

1.2.5. Life cycle

The product life cycle is in line with the one described in [BSI-PP-0035-2007]. It is detailed in the chapters “2.3 TOE life cycle” and “2.4 TOE environment” of the [ST]. The different phases are illustrated in the following table:

Phase	***Name***	***Description***
1	Development of the embedded application	- Development of the user application
2	Development of the IC component	- Development of the component (hardware product) - Development of the dedicated software OST
3	Manufacturing of the IC component	- Manufacturing and integration of the photomask - Manufacturing of the component - Component Test - Conditioning - Pre-personalzation
4	Packaging of the component	- Packaging of component (and test)
5	Composite product integration	- finalizing Process of composite product - Conditioning of composite product - shipment of composite product
6	Personalization	- Personalization of composite product - Test of composite product
7	Use	- Use of composite product by end vendors and end users

Current evaluation covered phases 2, 3 and 4 of the life cycle.
Evaluation also covered delivery and check processes of the user application developed in phase 1, together with delivery process of the TOE to the entity in charge of the product packaging done in phase 4. The processes related to other phases are out of the scope of this evaluation.

The TOE is always delivered in "End User" mode:
- either in wafer, possibly sawn, at the end of phase 3;
- or in a package at the end of phase 4.

The product is designed, developed, integrated (product data base preparation), manufactured and tested by:

STMicroelectronics SAS (Rousset/France),
SMD division, 190 Avenue Célestin Coq, ZI,
13106 Rousset Cedex,
France.

Part of the development is performed by:

STMicroelectronics Pte ltd (Ang Mo Kio/Singapore),
5A Serangoon North Avenue 5,
554574, Singapore,
Singapore.

STMicroelectronics (Zaventem/Belgium),
Excelsiorlaan 44-46,
B-1930 Zaventem,
Belgium.

Product can also be tested by:

STMicrolectronics (Toa Payoh/Singapore),
629 Lorong 4/6 Toa Payoh,
319521, Singapore,
Singapore.

Product masks are manufactured by:

DAI NIPPON PRINTING CO., LTD (DNP/Japan),
2-2-1, Fukuoka, kamifukuoka-shi,
Saitama-Ken, 356-8507,
Japan.

DAI NIPPON PRINTING EUROPE (DPE/Italy),
Via C. Olivetti, 2/A,
I-20041 Agrate Brianza,
Italy.

Product can be assembled in module or package by:

STMicroelectronics SA (Bouskoura/Morocco),
101, boulevard des Muriers BP 97,
20180, Bouskoura – Casablanca, Morocco.

SMARTFLEX TECHNOLOGIES (Singapore),
20, tampines St 92,
528875 Singapore,
Singapore.

NEDCARD BV (Netherland),
Bijsterhuizen 25-29,
6604 LM Wijchen,
Netherland.

Product can be sawn or back lapped by:

DISCO HI-Tec Europe GmbH (Germany),
Liebigstasse 8,
D-85551Kirchheim bei Munchen,
Germany.

STS Microelectronics (China),
16 Tao hua Rd., Futian free trade zone,
Shenzhen 518048,
P.R. China.

Product can be stored and shipped by the following sites:

STMicroelectronics SAS (Rousset/France),
SMD division, 190 Avenue Célestin Coq, ZI,
13106 Rousset Cedex,
France.

STMicroelectronics SA (Bouskoura/Marocco),
101, boulevard des Muriers BP 97,
20180, Bouskoura – Casablanca,
Morocco.

STMicroelectronics (Loyang, Singapore),
7 Loyang drive,
Singapore 508938,
Singapore.

For this evaluation, the evaluator considered 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 user configurations:

- “Test” configuration: at the end of the manufacturing phase, the microcontroller is tested using 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 in three sub-modes:
  - “Reduced test” mode that enables STMicroelectronics to perform several restricted tests;

- “Diagnosis” 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 above in section “1.2.4 Architecture” and configured in “User” mode.

For the requirements of this evaluation, the samples of the TOE delivered to the evaluator had a “Card Manager” operating system embedded in the ROM. This OS is identified by the UZC 3-digit code whose 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. The evaluation

2.1. Evaluation referential

The evaluation was carried out in compliance with the **Common Criteria version 3.1, revision 3** [CC] and the evaluation methods defined in the CEM manual [CEM].

For assurance 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 [CC AP] guides have been applied. In this way, the AVA_VAN level has been determined according to the rating scale of the [CC 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 uses results from following product evaluations:

- « Secure Microcontrollers SA23YR48/80B and SB23YR48/80B, including Cryptographic library NesLib v2.0 or v3.0, in configuration SA or SB » certified by ANSSI (see [ANSSI-CC-2010_02]);
- « Secure Microcontrollers SA23YR18A and SB23YR18A, including Cryptographic library Neslib V3.1 in configuration SA or SB » certified by ANSSI (see [ANSSI-CC-2011_06]).

The evaluation technical report [ETR], delivered to the ANSSI on 24th of September 2012, provides details on the work performed by the evaluation facility and certifies that all evaluation tasks are "**pass**".

2.3. Cryptographic mechanisms robustness analysis

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 "P2 – *SOF/High*".

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 "Secure microcontrollers ST23R160/80A/48A and ST23L160/80A/48A, optionally including the cryptographic library NesLib v3.1", submitted for evaluation fulfills the security features specified in its security target [ST] for the evaluation level EAL 6 augmented for ALC_FLR.1 component.

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 "Secure microcontrollers ST23R160/80A/48A and ST23L160/80A/48A, optionally including the cryptographic library NesLib v3.1" 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 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 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, for smart cards and similar devices, up to ITSEC E6 High and CC EAL7 levels. The certificates that are recognized in the agreement scope 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 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 SOG-IS agreement are: Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and United Kingdom.

2 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

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 6+	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	**2**	Implementation representation of the TSF
	ADV_INT					**2**	**3**	**3**	**3**	Well-structured internals
	ADV_SPM						**1**	1	**1**	Formal TOE security policy model
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**5**	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	**5**	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								**1**	Basic flaw remediation
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**3**	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 components 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	**3**	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 : - ST23R160, ST23R80A, ST23R48A, ST23L160, ST23L80A, ST23L48A, all with optional cryptographic library NESLIB 3.1 Security Target, Reference : SMD_ST23xxxx_ST_10_001_V02.01, July 2011, STMicroelectronics. For publication requirements, the following security target was provided and validated in the scope of this evaluation : - ST23R160B, ST23R80AB, ST23R48AB, ST23L160B, ST23L80AB, ST23L48AB, all with optional cryptographic library NESLIB 3.1 Security Target - Public Version, Reference : SMD_ST23RLxxx_ST_11_001 Rev 01.00, July 2011, STMicroelectronics.
[ETR]	Evaluation technical report: - Evaluation Technical Report – STR160 Project, Reference: LAFITE_ST23R160B_ETR_v2.1/2.1, 24 septembre 2012, Serma Technologies. For composite evaluation requirements with this microcontroller, a technical report for composition has been validated: - ETR Lite for Composition – ST23R160 Project, Reference: LAFITE_ST23R160B_ETRLiteComp_v2.1/2., 24 septembre 2012, Serma Technologies.
[CONF]	Configuration list: - ST23R160, ST23R80A, ST23R48A, ST23L160, ST23L80A, ST23L48A products - Configuration list, Reference: SMD_ST23R160_CFGL_11_001 V02.00, STMicroelectronics. Documentation list: - ST23R160 (and derivatives) EAL6+ documentation report, Reference: SMD_ST23R160_DR_10_001 V1.1 STMicroelectronics.
[GUIDES]	Product user manuals: - ST23R160, ST23R80A, ST23R48A, ST23L160, ST23L80A, ST23L48A – Datasheet, Reference : DS_23R160 Rev 1.0, STMicroelectronics ; - ST23 Platform - Security Guidance, Reference : AN_SECU_23 Rev 9, STMicroelectronics ; - Application Note ST23Rxxx: recommendations for contactless operations, Reference: AN_23R160_RCMD_CL_Rev1, STMicroelectronics ; - User Manual of NesLib 3.1, Reference : UM_23_NesLib Rev 1, STMicroelectronics ; - ST23Rxxx/ST23Lxxx security guidance,

	Reference : AN_23R160_SECU Rev2, STMicroelectronics ; - ST23secure MCUs with AES NesLib security guidance, Reference : AN_23_AES_NesLib Rev1, STMicroelectronics ; - ST23R160 OST User Manual (full and reduced test configuration), Reference : PEN_ST23_UM_10_001, STMicroelectronics ; - ST23 AIS 31: Compliant Random Number – User Manual, Reference UM_23_AIS31, v2.0, STMicroelectronics ; - ST23 AIS 31: Reference Implementation - StartUp, Online and Total Failure Tests, Reference : AN_23_AIS31, v2.0, STMicroelectronics ;
[2010/02]	Certification report ANSSI-CC-2010/02, Secure Microcontrollers SA23YR48/80B and SB23YR48/80B, including cryptographic library NesLib v2.0 or v3.0, in configuration SA or SB, 10th of February 2010, ANSSI.
[2011/06]	Certification report ANSSI-CC-2011/06, Secure Microcontrollers SA23YR18A and SB23YR18A, including cryptographic library Neslib V3.1 in configuration SA or SB, 8th of September 2011, ANSSI.
[BSIPP0035]	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 to 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.
[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.
[JIWG AP]	Mandatory Technical Document - Application of attack potential to smart-cards, JIWG, version 2.8, January 2012.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, reference CCDB-2007-09-001 version 1.0, revision 1, September 2007.
[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 26 January 2010 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).