



PREMIER MINISTRE

General Secretariat for Defence and National Security

French Network and Information Security Agency

Certification Report ANSSI-CC-2010/04

SA23YR18A and SB23YR18A Secure Microcontrollers, including the cryptographic library Neslib v2.0, in SA or SB configuration

Paris, April 19th 2010

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

certification.anssi@ssi.gouv.fr

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



| | |
|--|--|
| <i>Certification report reference</i> | ANSSI-CC-2010/04 |
| <i>Product name</i> | SA23YR18A and SB23YR18A Secure Microcontrollers |
| <i>Product reference</i> | SA23YR18 and SB23YR18 revision A (dedicated software ARC, K2N0ACA mask set), including the cryptographic library Neslib v2.0, in SA or SB configuration |
| <i>Protection profile conformity</i> | BSI-PP-0035-2007 version 1.0 Security IC Platform Protection Profile v1.0, 15 June 2007 |
| <i>Evaluation criteria and version</i> | Common Criteria version 3.1 |
| <i>Evaluation level</i> | EAL 5 augmented AVA DVS.2, AVA VAN.5 |
| <i>Developer</i> | STMicroelectronics Smartcard IC division, 190 Avenue Célestin Coq, 13106 Rousset Cedex, France |
| <i>Sponsor</i> | STMicroelectronics Smartcard IC division, 190 Avenue Célestin Coq, 13106 Rousset Cedex, France |
| <i>Evaluation facility</i> | Serma Technologies 30 avenue Gustave Eiffel, 33608 Pessac, France Phone: +33 (0)5 57 26 08 75, email : e.francois@serma.com |
| <i>Recognition arrangements</i> | <div style="display: flex; justify-content: space-around;"><div style="text-align: center;">CCRA </div><div style="text-align: center;">SOG-IS </div></div> <p>The product is recognised at EAL4 level.</p> |

Introduction

The Certification

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

- The French Network and Information Security Agency draws up **certification reports**. These reports indicate the features of the proposed security targets. They may include any warnings that the authors feel the need to mention for security reasons. They may or may not be transmitted to third parties or made public, as the sponsors desire (article 7).
- The **certificates** issued by the Prime Minister certify that the copies of the products or systems submitted for evaluation fulfil the specified security features. They also certify that the evaluations have been carried out in compliance with applicable rules and standards, with the required degrees of skill and impartiality (article 8).

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



Content

| | |
|--|-----------|
| 1. PRODUCT | 6 |
| 1.1. PRESENTATION OF THE PRODUCT..... | 6 |
| 1.2. EVALUATED PRODUCT DESCRIPTION | 6 |
| 1.2.1. <i>Product identification</i> | 6 |
| 1.2.2. <i>Security services</i> | 7 |
| 1.2.3. <i>Architecture</i> | 7 |
| 1.2.4. <i>Life cycle</i> | 8 |
| 1.2.5. <i>Evaluated configuration</i> | 10 |
| 2. EVALUATION | 11 |
| 2.1. EVALUATION REFERENTIAL | 11 |
| 2.2. EVALUATION WORK | 11 |
| 2.3. CRYPTOGRAPHIC MECHANISMS ROBUSTNESS ANALYSIS ACCORDING TO ANSSI TECHNICAL REFERENCE FRAME..... | 11 |
| 2.4. RANDOM NUMBER GENERATOR ANALYSIS | 11 |
| 3. CERTIFICATION..... | 12 |
| 3.1. CONCLUSION | 12 |
| 3.2. RESTRICTIONS OF USE..... | 12 |
| 3.3. RECOGNITION OF THE CERTIFICATE..... | 12 |
| 3.3.1. <i>European recognition (SOG-IS)</i> | 12 |
| 3.3.2. <i>International common criteria recognition (CCRA)</i> | 13 |
| ANNEX 1. EVALUATION LEVEL OF THE PRODUCT..... | 14 |
| ANNEX 2. EVALUATED PRODUCT REFERENCES..... | 15 |
| ANNEX 3. CERTIFICATION REFERENCES..... | 17 |

1. Product

1.1. Presentation of the product

The evaluated products are the SA23YR18A and SB23YR18A secure microcontrollers revision A (dedicated software ARC, K2N0ACA mask set) developed by STMicroelectronics. These products include the cryptographic library Neslib in version v2.0, in SA configuration for SA23YR18A and in SB configuration for SB23YR18A.

The hardware part and the dedicated software are identical to the ST23YR18A secure microcontroller certified under the reference ANSSI-CC-2010/03.

The SA23YR18A and SB23YR18A only differ by the SA or SB configuration of the Neslib cryptographic library in version v2.0. The SA Neslib configuration provides high-level routines to perform RSA and SHA operations, on top of that the SB configuration provides high-level routines to perform AES and ECC operations.

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

1.2. Evaluated product description

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

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

1.2.1. Product identification

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

The certified version of the product can be identified by the following elements:

- Die identification: K2N0A (Die name with HW major cut reference) and all masks revision letters corresponding to K2N0ACA mask set;
- Cryptographic Library Reference: Neslib revision v2.0 (SA or SB configuration);
- Dedicated software identification: ARC (Boot sequence, embedded test software);
- Embedded software identification: UBS, this is the *Card Manager*, a reference Operating System, embedded in the *User ROM* of the samples which have been tested, for the evaluation needs only. The *Card Manager* is not part of the evaluation perimeter, cf §1.2.5;
- Manufacturing site identification: ST 4 (Rousset).



Identification elements are marked on the die and visible with a microscope. In addition, two bytes in OTP allow identifying the product from a logical point of view, as described in the “Datasheet” (cf. [GUIDES]). For Neslib Cryptographic library, Neslib provides an API in order to get the library revision, as described in the Neslib “User Manual” (cf. [GUIDES]).

1.2.2. Security services

The product provides mainly the following security services:

- Initialisation of the hardware platform and its attributes;
- Secure handling of the life cycle;
- Logical integrity of the product;
- Test of the product;
- Memory management (firewall);
- Physical tampering protection;
- Security violation administrator;
- Unobservability;
- Symmetric Key Cryptography Support;
- Asymmetric Key Cryptography Support;
- Unpredictable number generation support.
- A cryptographic library providing, depending on version and configuration used, high-level routines to perform RSA, SHA, AES , ECC operations.

1.2.3. Architecture

The SA/B23YR18A microcontrollers are made up of:

- A Hardware part:
 - An 8/16-bit central processing unit;
 - Memories:
 - 18 Kbytes of EEPROM (including 128 bytes of OTP) with integrity control, for program and data storage,
 - 230 Kbytes of ROM for user software,
 - 4 Kbytes of RAM,
 - 26 Kbytes of ROM for dedicated software;
 - Security Modules: Memory protection unit (MPU), clock generator, security monitoring and control, power management, memory integrity control and fault detection;
 - Functional Modules: 3 8-bit timers, I/O management in contact mode (IART ISO 7816-3), and contactless mode (RF UART ISO 14443-B), True Random Number Generator, EDES co-processor supporting DES algorithms and the NESCRYPT co-processor with a dedicated 2-Kbyte RAM supporting public key cryptographic algorithms.
- A dedicated software is embedded in ROM which comprises:
 - Microcontroller test software (“Auto test”);
 - System and Hardware/Software interface management capabilities.
- A cryptographic library (Neslib v2.0) providing routines to perform RSA and SHA cryptographic operations, in configuration SA; or routines to perform RSA, SHA, AES , ECC in SB configuration. This library is integrated by the Customer in his code, and is then embedded in the product User ROM.

1.2.4. Life cycle

The product's life cycle is organised as follow:

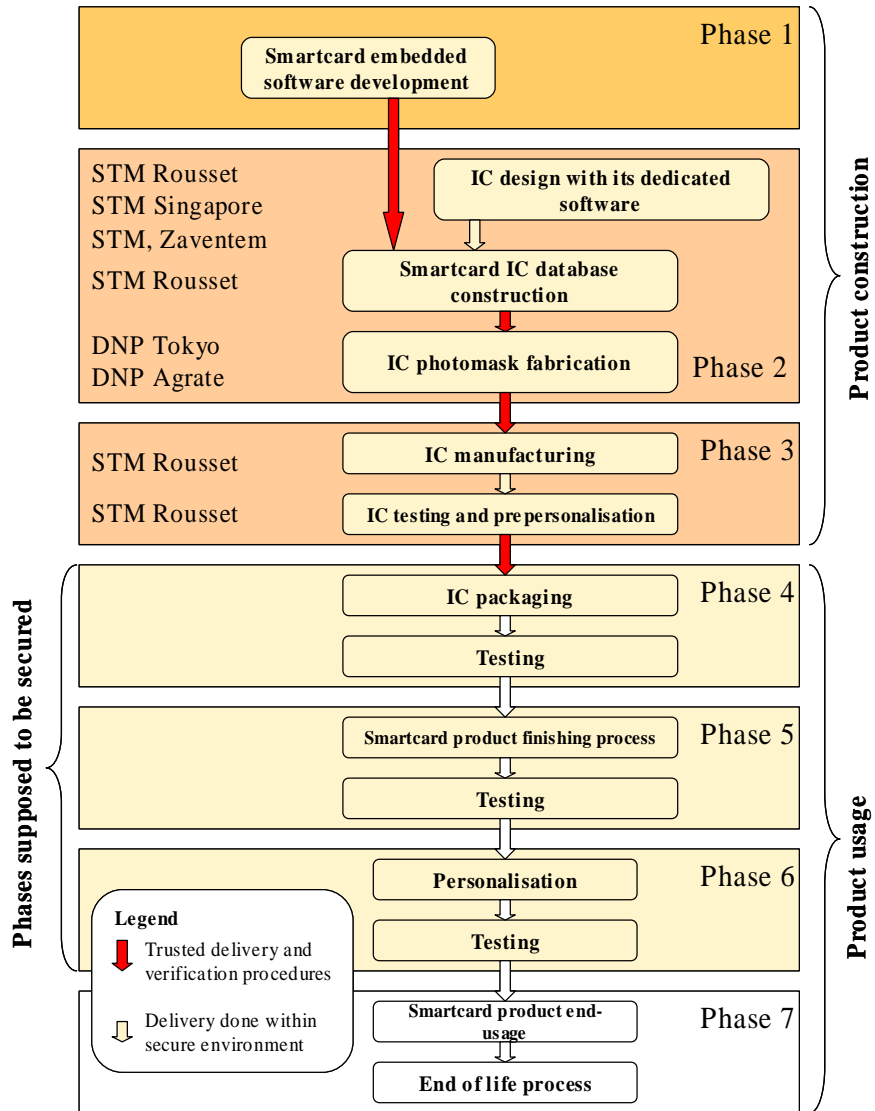


Figure 1 – Life cycle of a smart card

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

STMicroelectronics SAS

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



A part of the design is realised by:

STMicroelectronics Pte Ltd

5A Serangoon North Avenue 5
554574 Singapore
Singapore

and by:

STMicroelectronics

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

The photo masks of the product are manufactured by:

DAI NIPPON PRINTING CO., LTD

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

and by:

DAI NIPPON PRINTING EUROPE

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

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

- “Test” configuration: at the end of IC manufacturing, the microcontroller is tested using the test software stored in ROM (called “Autotest”) within the secure developer premises. Pre-personalization data can be loaded in the EEPROM. The product configuration is changed to “User” before delivery to the next user, and the device cannot be reversed to the “test” configuration.
- “User” configuration: final configuration of the product, including 3 modes:
 - “reduced test”, allowing STMicroelectronics to perform some reduced sets of test;
 - “diagnosis”, allowing even more limited operations, restricted to STMicroelectronics;
 - “end user”, final usage mode of the product, whose functionalities are driven exclusively by the Embedded Software. The developer test functionalities are unavailable. The end-users of the product can use it only under this mode.

1.2.5. Evaluated configuration

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

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

For the evaluation needs, the product SB23YR18A (with internal revision C), including the cryptographic library Neslib v2.0, were provided to the ITSEF with a dedicated evaluation software in a mode known as “open¹”.

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



2. Evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 3.1** [CC] and the Common Evaluation Methodology [CEM].

For assurance components above EAL4 level, the evaluation facility own evaluation methods, validated by ANSSI, have been used.

In order to meet the specificities of smart cards, the [CC IC] and [CC AP] guides have been applied.

2.2. Evaluation work

This evaluation is partially based on previous evaluation results of SB23YR80/48A product certified EAL5+ on December 2009 with the reference ANSSI-CC-2009/27.

The evaluation technical report [ETR], delivered to ANSSI on the 30th of September 2009, describes the work performed by the evaluation facility and assesses that all evaluation tasks are “pass”.

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

The evaluated product provides the following cryptographic support services:

- support for symmetric key cryptography (EDES) ;
- support for asymmetric key cryptography (NESCRIPT) ;
- support for random numbers generation (TRNG).

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

The SA/SB23YR18A products include also a cryptographic library Neslib v2.0. The quotation of the cryptographic mechanisms provided by this library, according to technical reference frame [REF-CRY], [REF-CLE] and [REF-AUT], has not been performed. Nevertheless, the evaluation did not reveal any vulnerability in design nor implementation for the targeted AVA_VAN level.

2.4. Random number generator analysis

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

3. Certification

3.1. Conclusion

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

This certificate testifies that the SA23YR18A and SB23YR18A secure microcontrollers, including the cryptographic library Neslib v2.0 in SA or SB configuration, submitted for evaluation fulfil the security features specified in its security target [ST] for the evaluation level EAL5 augmented.

3.2. Restrictions of use

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

This certificate provides a resistance assessment of the SA23YR18A and SB23YR18A products to a set of attacks which remains generic due to the missing of any specific embedded application. Therefore, the security of a final product based on the evaluated microcontrollers would only be assessed through the final product evaluation, which could be performed using the results of current evaluation listed in Chapter 2.

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

3.3. Recognition of the certificate

3.3.1. European recognition (SOG-IS)

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

The European recognition agreement made by SOG-IS in 1999 allows recognition from signatory states of the agreement¹, of ITSEC and Common Criteria certificates. The European recognition is applicable up to ITSEC E6 and CC EAL7 levels. The certificates that are recognized in such scope are released with the following marking:



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



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 countries¹, of the Common Criteria certificates. The mutual recognition is applicable up to the assurance components of CC EAL4 level and also to ALC_FLR family. The certificates that are recognized in the agreement scope are released with the following marking:



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

Annex 1. Evaluation level of the product

| Classe | Famille | Composants par niveau d'assurance | | | | | | | Niveau d'assurance retenu pour le produit | | |
|---|---------|-----------------------------------|-------|-------|-------|-------|-------|-------|---|-----------------------|--|
| | | EAL 1 | EAL 2 | EAL 3 | EAL 4 | EAL 5 | EAL 6 | EAL 7 | EAL 5+ | Intitulé du composant | |
| ADV Développement | ADV_ARC | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Security architecture description |
| | ADV_FSP | 1 | 2 | 3 | 4 | 5 | 5 | 6 | 5 | 5 | Complete semiformal functional specification with additional error information |
| | ADV_IMP | | | | 1 | 1 | 2 | 2 | 1 | 1 | Implementation representation of the TSF |
| | ADV_INT | | | | | 2 | 3 | 3 | 2 | 2 | Well-structured internals |
| | ADV_SPM | | | | | | 1 | 1 | | | |
| | ADV_TDS | | 1 | 2 | 3 | 4 | 5 | 6 | 4 | 4 | Semiformal modular design |
| AGD Guides d'utilisation | AGD_OPE | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Operational user guidance |
| | AGD_PRE | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Preparative procedure |
| ALC Support au cycle de vie | ALC_CMC | 1 | 2 | 3 | 4 | 4 | 5 | 5 | 4 | 4 | Production support, acceptance procedures and automation |
| | ALC_CMS | 1 | 2 | 3 | 4 | 5 | 5 | 5 | 5 | 5 | Development tools CM coverage |
| | ADO_DEL | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Delivery procedures |
| | ALC_DVS | | | 1 | 1 | 1 | 2 | 2 | 2 | 2 | Sufficiency of security measures |
| | ALC_FLR | | | | | | | | | | |
| | ALC_LCD | | | 1 | 1 | 1 | 1 | 2 | 1 | 1 | Developer defined life-cycle model |
| | ALC_TAT | | | | 1 | 2 | 3 | 3 | 2 | 2 | Compliance with implementation standards |
| ASE Evaluation de la cible de sécurité | ASE_CCL | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Conformance claim |
| | ASE_ECD | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Extended component definition |
| | ASE_INT | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | ST introduction |
| | ASE_OBJ | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | Security objectives |
| | ASE_REQ | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | Derived security requirements |
| | ASE_SPD | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Security problem definition |
| | ASE_TSS | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | TOE summary specifications |
| ATE Tests | ATE_COV | | 1 | 2 | 2 | 2 | 3 | 3 | 2 | 2 | Analysis of coverage |
| | ATE_DPT | | | 1 | 2 | 3 | 3 | 4 | 3 | 3 | Testing: modular design |
| | ATE_FUN | | 1 | 1 | 1 | 1 | 2 | 2 | 1 | 1 | Functional testing |
| | ATE_IND | 1 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | Independant testing, sample |
| AVA Estimation des vulnérabilités | AVA_VAN | 1 | 2 | 2 | 3 | 4 | 5 | 5 | 5 | 5 | Advanced methodical vulnerability analysis |



Annex 2. Evaluated product references

| | |
|----------|--|
| [ST] | <p>Reference security target for the evaluation:</p> <ul style="list-style-type: none"> - SB23YR18 Security Target, Reference : SMD_SB23YR18_ST_09_001, v01.00, STMicroelectronics <p>For the needs of publication, the following security target has been provided and validated in the evaluation:</p> <ul style="list-style-type: none"> - SA/SB23YR18 Security Target - Public Version, Reference : SMD_SB23YR18_ST_09_002, v02.00, STMicroelectronics |
| [ETR] | <p>Evaluation technical report :</p> <ul style="list-style-type: none"> - Evaluation Technical Report - LAFITE Project, Reference : LAFITE-SB23YR18A_ETR_v1.0 / 1.0, Septembre 2009,Serma Technologies <p>For the needs of composite evaluation with this microcontroller a technical report for composition has been validated:</p> <ul style="list-style-type: none"> - ETR Lite for Composition – LAFITE project, Reference: LAFITE_SB23YR18A_ETRLiteComp_v1.0/ 1.0, Serma Technologies |
| [CONF] | <p>Products configuration list:</p> <ul style="list-style-type: none"> - Configuration list, Reference : SMD_SB23YR18_CFGL_09_001 rev 1.0, STMicroelectronics <p>List of the delivered materials:</p> <ul style="list-style-type: none"> - Documentation report, Reference : SMD_SB23YR18_DR_09_001_v1.4, STMicroelectronics <p>Neslib v2.0 library configuration list:</p> <ul style="list-style-type: none"> - Neslib 2.0 configuration list Reference : NesLib_2.0_CFGL_09_005_V01.01 STMicroelectronics |
| [GUIDES] | <p>The product user guidance documentation is the following:</p> <ul style="list-style-type: none"> - ST23YR18 Datasheet, Reference : DS_23YR18 Rev 0.3, STMicroelectronics - ST23YR18 : Recommendations for contactless operation, Reference : AN_23YR18_RCMD Rev 3, STMicroelectronics |

| | |
|----------|---|
| | <ul style="list-style-type: none">- ST23 Platform - Security Guidance, Reference : AN_SECU_23 Rev 7, STMicroelectronics- ST21/23 programming manual Reference : PM_21_23/0709 Rev 1, STMicroelectronics- User Manual of Neslib 2.0 library, Reference : UM_NesLib_2.0 Rev 2, STMicroelectronics- NesLib 2.0: using the dispatcher on ST23YR18 UBS, Reference : PTD_NesLib_TN_09_008_v01.00, STMicroelectronics- ST23 AIS31 Compliant Random Number User Manual, Référence : UM_23_AIS31 Rev 1, STMicroelectronics- ST23 AIS31 Tests reference implementation user manual, Référence : AN_23_AIS31 Rev1, STMicroelectronics |
| [PP0035] | Security IC Platform Protection Profile Version 1.0 June 2007. <i>Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0035-2007.</i> |



Annex 3. Certification references

| | |
|--|---|
| Decree number 2002-535 dated 18 th April 2002 related to the security evaluations and certifications for information technology products and systems. | |
| [CER/P/01] | Procedure CER/P/01 - Certification of the security provided by IT products and systems, DCSSI. |
| [CC] | Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, September 2006, version 3.1, revision 1, ref CCMB-2006-09-001, Part 2: Security functional components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-002, Part 3: Security assurance components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-003. |
| [CEM] | Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2007, version 3.1, ref CCMB-2007-09-004, revision 2. |
| [CC IC] | Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2006-04-003 version 2.0, revision 1, April 2006. |
| [CC AP] | Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2009-03-001 version 2.7 revision 1, March 2009. |
| [REF-CRY] | Cryptographic mechanisms - Rules and recommendations about the choice and parameters sizes of cryptographic mechanisms, version 1.11, 24 th of October 2008, see www.ssi.gouv.fr |
| [REF-CLE] | Cryptographic keys management - Rules and recommendations about management of keys used in cryptographic mechanisms, version 1.10, 24 th of October 2008, see www.ssi.gouv.fr |
| [REF-AUT] | Authentication - Rules and recommendations about authentication mechanisms with standard level robustness, v0.13 12 th of April 2007, No. 729/SGDN/DCSSI/SDS |
| [AIS31] | Functionality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25/09/2001, Bundesamt für Sicherheit in der Informationstechnik (BSI) |