Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Certification Report ANSSI-CC-2013/25

ST31-K330A Secure microcontroller revision F for Dual mode version (contact and contactless) or contactless-only version, optionally including the NesLib cryptographic library revision 3.2

Paris, April 23rd, 2013

Courtesy Translation

SÉCURITÉ CERTIFICATION

Warning

This report is designed to provide sponsors with a document enabling them to assess the security level of a product under the conditions of use and operation defined in this report for the evaluated version. It is also designed to provide the potential purchaser of the product with the conditions under which he may operate or use the product so as to meet the conditions of use for which the product has been evaluated and certified; that is why this certification report must be read alongside the evaluated user and administration guidance, as well as with the product security target, which presents threats, environmental assumptions and the supposed conditions of use so that the user can judge for himself whether the product meets his needs in terms of security objectives.
Certification does not, however, constitute a recommendation product from ANSSI (French Network and Information Security Agency), and does not guarantee that the certified product is totally free of all exploitable vulnerabilities.

Any correspondence about this report has to be addressed to:

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP
France

certification.anssi@ssi.gouv.fr

Certification report reference

ANSSI-CC-2013/25

Product name

ST31-K330A Secure microcontroller revision F for Dual mode version (contact and contactless) or contactless-only version, optionally including the NesLib cryptographic library revision 3.2

Product reference

Maskset reference K330A , internal revision F

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

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 6
1.1. PRESENTATION OF THE PRODUCT 6
1.2. EVALUATED PRODUCT DESCRIPTION 6
1.2.1. Product identification 6
1.2.2. Security services 7
1.2.3. Architecture 7
1.2.4. Life cycle 9
1.2.5. Evaluated configuration 12
2. THE EVALUATION 13
2.1. EVALUATION REFERENTIAL 13
2.2. EVALUATION WORK 13
2.3. CRYPTOGRAPHIC MECHANISMS ROBUSTNESS ANALYSIS 13
2.4. RANDOM NUMBER GENERATOR ANALYSIS 13
3. CERTIFICATION 14
3.1. CONCLUSION 14
3.2. RESTRICTIONS 14
3.3. RECOGNITION OF THE CERTIFICATE 15
3.3.1. European recognition (SOG-IS) 15
3.3.2. International common criteria recognition (CCRA) 15
ANNEX 1. EVALUATION LEVEL OF THE PRODUCT 16
ANNEX 2. DOCUMENTARY REFERENCES FOR EVALUATED PRODUCT 17
ANNEX 3. REFERENCES ASSOCIATED TO THE CERTIFICATION 19

1. The product

1.1. Presentation of the product

The evaluated product is the “ST31-K330A Secure microcontroller revision F for Dual mode version (contact and contactless) or contactless-only version, optionally including the NesLib cryptographic library revision 3.2”, 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. 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 strictly complies with protection profile [BSI-PP-0035-2007]. Its compliance can be proven.

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 (cf. [ST] in paragraph 3.1 “TOE overview” and [GUIDES]):

- Information written on the microcontroller: :
  - K330A: STMicroelectronics internal name of the ST31 family product, the letter A identifies the major silicon revision number;
  - YGD: 3-digit code identifying the dedicated software also called the OST [1] ("*Operating System for Test*");
  - UZR[2]: 3-digit code 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;
  - 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") internal revision F;
- information present in the OTP area ("*One Time Programmable*") of the EEPROM:
  - *0033h*: "Master" identification number of the ST31-K330A product written on two bytes at addresses *0x0010000A-0Bh*;
  - *0059h*: "Child" identification number of the ST31-K330A product written on two bytes at addresses *0x0010000E-0Fh;*
  - *13h*: OST code version, hexadecimal value written on 1 byte at address *0x00100010h* ;
  - *46h*: Product internal revision letter F, ASCII characters (letters from A to Z) coded in hexadecimal format written on 1 byte at address *0x00100013h*.

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 firewall;
- Physical tampering protection;
- Management of security violations;
- Unobservability of sensitive data;
- Secure management of EEPROM;
- Support for symmetric key cryptography;
- Support for asymmetric key cryptography;
- Support for random number generation;
- The NesLib V3.2 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.

1.2.3. Architecture

The TOE hardware architecture is shown in Figure 1.
The ST31-K330A microcontroller consists of the following components:

- A hardware part with:
  - An ARM® SecurCore® SC000™ 32-bit RISC core processor;
  - Memories:
    - 52[1]/38/22/16 Kbytes of EEPROM (with integrity detection) for storing data;
    - 320 Kbytes of ROM for storing user applications;
    - 8 Kbytes of RAM;

[1] A commercial version with 40 Kbytes of EEPROM exists and is based on the 52-Kbyte product.

- Security modules: Memory protection unit (MPU), clock generator, security control and monitoring, power management, memory integrity control, fault detection;
- Functional modules: two 16-bit timers, input/output management function in Contact mode (IART ISO 7816-3), a random number generator (TRNG);
- Coprocessors:
  - EDES for supporting DES algorithms;
  - AES for supporting AES algorithms;
  - NESCRYPT with a dedicated RAM for supporting public key cryptographic algorithms;
- And ISO 14443 type A, B and B' radio frequency communication module compliant with PayPass™ specifications.

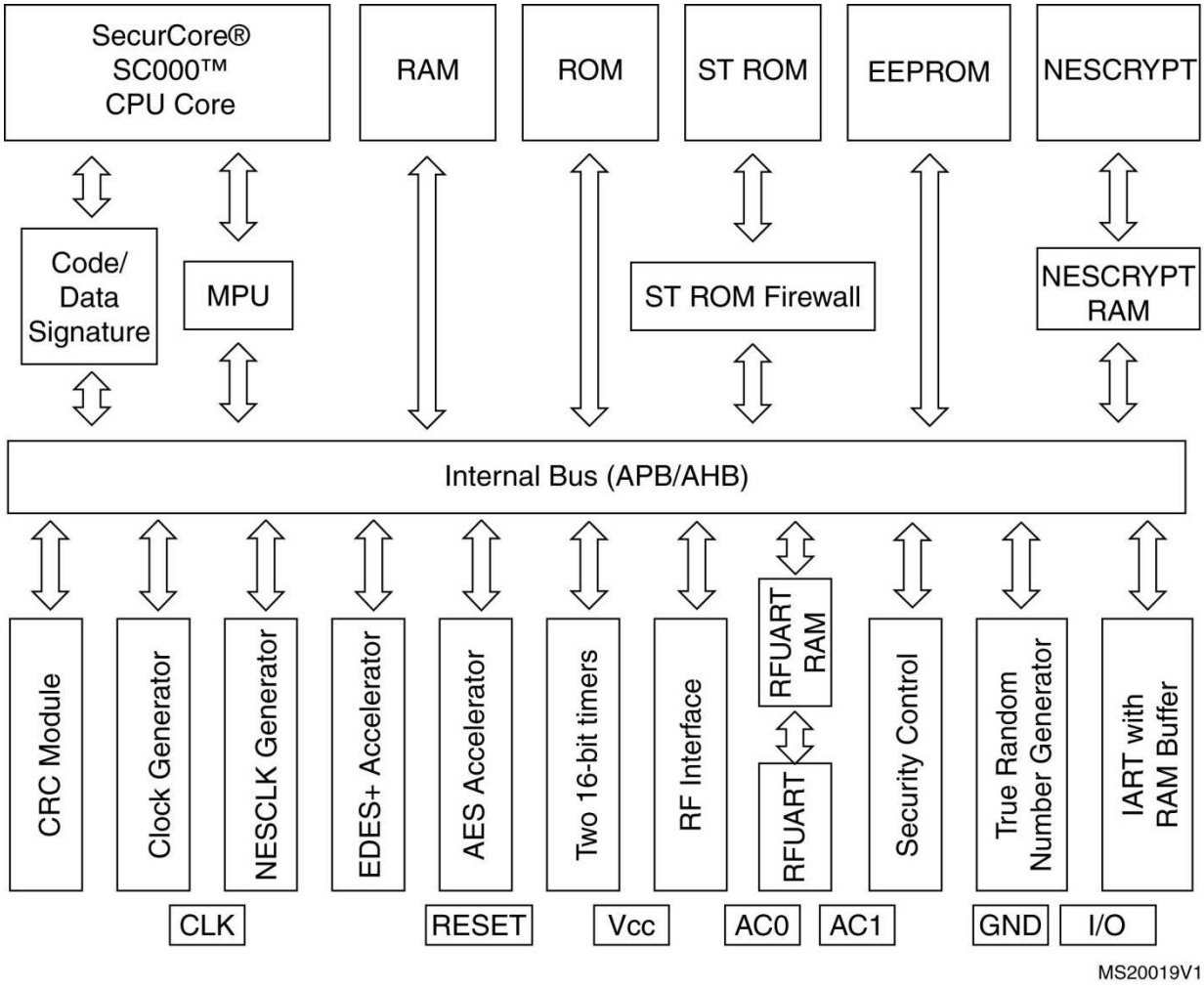

Figure 1: Architecture

Optionally, the user can also choose to integrate a cryptographic library (NesLib v3.2) 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's ROM.
In addition to these hardware components, the TOE also embeds in the ROM, a dedicated operating system for test (OST).
This software component:

- 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.

1.2.4. Life cycle

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

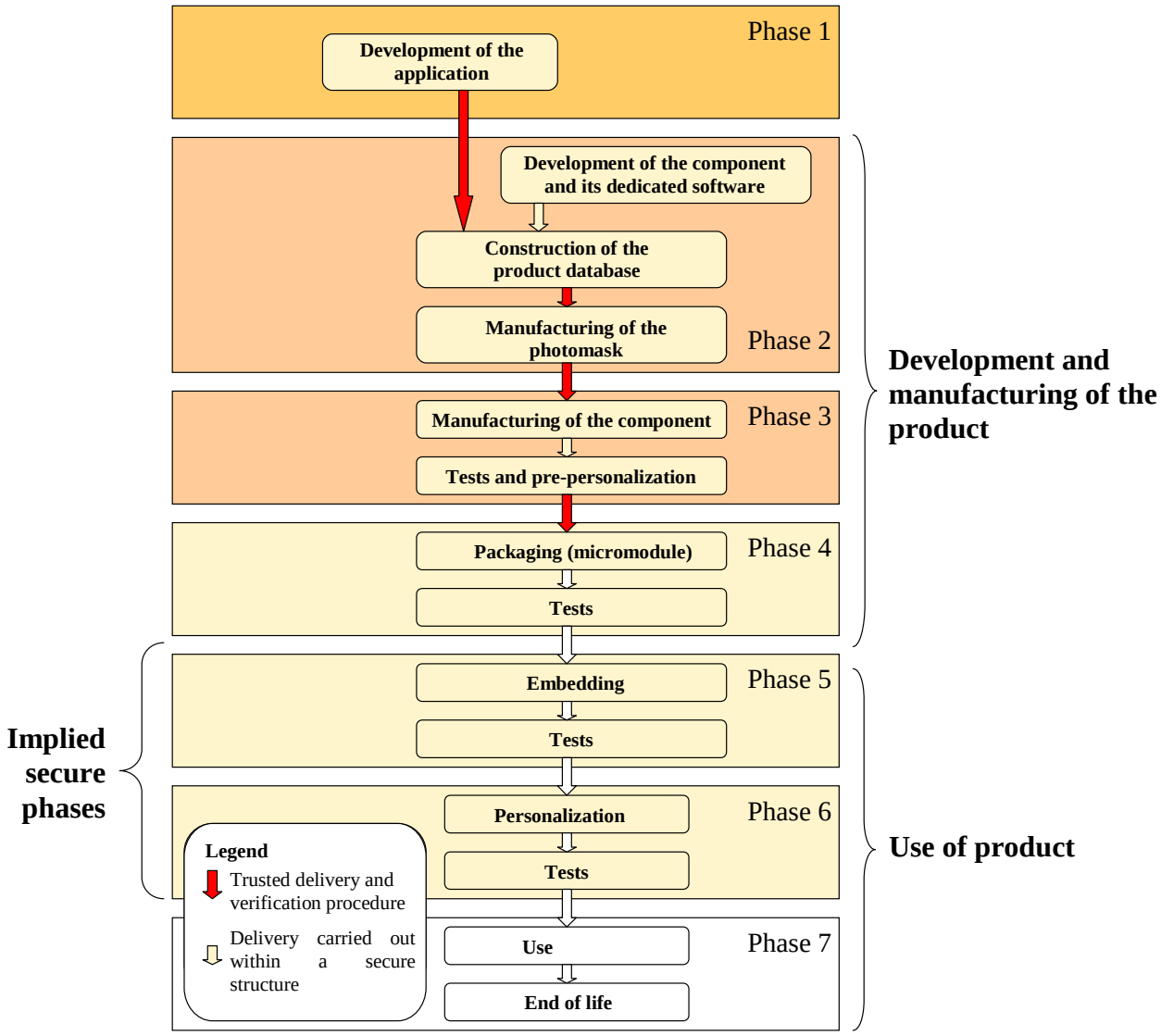

Figure 2: Life cycle

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 Singapour Singapour

STMicroelectronics Green Square, Lamboekstraat 5, Building B, 3d Floor, 1831 Diegem/Machelem, Belgium	**STMicroelectronics** 101 Boulevard des Muriers BP97 20 180 Casablanca Morocco
STS Microelectronics 16 Tao hua Rd. Futian free trade zone 518048 Shenzhen P.R. of China	**STMicroelectronics** 629 Lorong 4/6 Toa Payoh 319521 Singapour Singapour
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
CMP Georges Charpak 880 Avenue de Mimet 13542 Gardanne France	**Smartflex** 20, Tampines Street 92 Singapore 528875 Singapour
STS Microelectronics 9 Mountain Drive, LISP II, Brgy La Mesa Calamba, 4027 Philippines	**Netcard** Bijsterhuizen 25-29 6604 LM Wijchen The Netherlands
STS Microelectronics 7 Loyang Drive Singapore 508938 Singapour	**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 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.

1.2.5. Evaluated configuration

The certificate applies to the TOE defined in section 1.2.1 and configured in “User” mode.
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 UZR 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 4** [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 [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 technical report [ETR], delivered to the ANSSI on 17 April 2013, 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 "ST31-K330A Secure microcontroller revision F for Dual mode version (contact and contactless) or contactless-only version, optionally including the NesLib cryptographic library revision 3.2", submitted for evaluation fulfills 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 "ST31-K330A Secure microcontroller revision F for Dual mode version (contact and contactless) or contactless-only version, optionally including the Neslib cryptographic library revision 3.2" 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 5+	Component name
ADV Development	ADV_ARC		**1**	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**5**	Complete semi-formal functional specification with additional error information
	ADV_IMP				**1**	1	**2**	2	**1**	Implementation representation of the TSF
	ADV_INT					**2**	**3**	**3**	**2**	**Well-structured internals**
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**4**	Semiformal modular design
AGD User guidance	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**1**	1	1	1	1	1	1	**1**	Preparative procedures
ALC Life cycle support	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Production support, acceptance procedures and automation
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**5**	Development tools CM coverage
	ALC_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**2**	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**2**	Compliance with implementation standards
ASE Evaluation of the security target	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended 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	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**3**	3	**4**	**3**	Testing: modular design
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independent testing: sample
AVA Vulnerability assessment	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**5**	Advanced methodical vulnerability analysis

Annex 2. Documentary references for evaluated product

[ST]	Reference security target for the evaluation : - ST31 - K330A version F (dual or contactless mode only) with optional cryptographic library NesLib 3.2 – Security Target, reference SMD_SR31Zxxx_ST_13_001, version v1.03, 26 March 2013. For publication requirements, the following security target was provided and validated in the scope of this evaluation : - ST31 - K330A version F (dual or contactless mode only) with optional cryptographic library NesLib 3.2 – Public Security Target, reference SMD_SR31Zxxx_ST_13_002, version v1.0, 26 March 2013.
[RTE]	Evaluation technical report: - Full Evaluation technical report for Project CHABLIS reference: CHABLIS_ETR, version v1.1 of 17 April 2013 ; - ST31-K330A project: Lite evaluation technical report Reference: ST31-K330A-ETRLiteComp_v1.1, version v1.1, 19 April 2013.
[CONF]	Configuration list: - ST31-K330A - Configuration list Reference SMD_ST31-K330A_F_CFGL_13_001, version v1.0, 12 March 2013. Documentation list: - ST31-K330 Evaluation Documentation Report Reference: SMD_ST31-K330_DR_12_001, version v1.0, 3 April 2013.
[GUIDES]	Product user manuals: - ARM SC000 Technical Reference Manual, reference: ARM DDI 0456 version A, September 2010; - ARM v6-M Architecture Reference Manual, reference: ARM DDI 0419, version C, September 2010; - ST31 - K330 platform - Sx31Zxxx, Mx31Zxxx - Secure dual interface microcontroller with enhanced security and up to 52 Kbytes of EEPROM – Datasheet, reference: DS_SR31Z052, revision 1.0, February 2013; - ST31 - K330 platform 90nm F10 CMOS die description, reference: DD_31Z052, revision 2, June 2012; - ST31 - K330 Security guidance, reference: AN_SECU_ST31_K330, revision 1.0, April 2013; - ST31 - AIS31 Compliant Random Number user manual, reference: UM_31_AIS31, revision 2, February 2013; - ST31 - AIS31 Reference implementation - Startup, online and total failure tests - Application Note AN_31_AIS31, revision 2,

	February 2013; - ST31 NesLib cryptographic library User manual, reference UM_31_NESLIB_3.2, revision 3, March 2013; - Application Note - Recommendations for use of EEPROM and code signature in ST31-K330 secure microcontrollers, reference AN_31_EEPROM, revision 1, February 2013; - ST31-K330 and ST33-K8H0 secure microcontrollers – Power supply glitch detector characteristics, reference: AN_31_GLITCH version 2, March 2013; - Application note - ST31-K330 Dual Interface Secure MCUs - Recommendations for contactless operations, reference: AN_31_RCMD version 1, February 2013.
[BSI_PP_0035-2007]	Protection Profile - Security IC Platform Protection Profile, version v1.0 of 15 June 2007. *Certified by the BSI under reference BSI_PP_0035-2007.*

Annex 3. References associated 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.
[CCDB AP]	CCDB-2012-04-002 - Application of attack potential to smart-cards, version 2.8, April 2012.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.
[SOG-IS]	"Mutual Recognition Agreement of Information Technology Security Evaluation Certificates", version 3.0, 8 January 2010, Management Committee.
[REF]	Cryptographic mechanisms – Rules and recommendations concerning the choice and configuration of cryptographic mechanisms, Version 1.20 of 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).