Certification Report ANSSI-CC-2014/94

ST31-K330A Secure microcontroller revision H for Dual mode version (contact and contactless) or contactless only version, with optional NesLib cryptographic library v3.2, MIFARE® DESFire® EV1 library v2.2 and MIFARE Plus®-S library v1.3

Paris, 5 January 2015

Courtesy Translation

SÉCURITÉ
CERTIFICATION
Ti

Certification report ANSSI-CC-2014/94

ST31-K330A Secure microcontroller revision H for Dual
mode version (contact and contactless) or contactless only
version

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

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

ANSSI-CC-CER-F-07EN.008

ST31-K330A Secure microcontroller revision H for Dual
mode version (contact and contactless) or contactless only
version

Certification report ANSSI-CC-2014/94

Certification report reference

ANSSI-CC-2014/94

Product name

ST31-K330A Secure microcontroller revision H for Dual mode version (contact and contactless) or contactless only version, with optional NesLib cryptographic library v3.2, MIFARE® DESFire® EV1 library v2.2 and MIFARE Plus®-S library v1.3

Product reference

K330A maskset reference, 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

EAL 5 augmented
ALC_DVS.2, ASE_TSS.2, 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
14 rue Galilée, CS 10055, 33615 Pessac Cedex, France

Recognition arrangements

CCRA   SOG-IS

The product is recognised at EAL4 level.

Certification report ANSSI-CC-2014/94

ST31-K330A Secure microcontroller revision H for Dual mode version (contact and contactless) or contactless only version

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.

ST31-K330A Secure microcontroller revision H for Dual
mode version (contact and contactless) or contactless only
version   Certification report ANSSI-CC-2014/94

Contents

Certification report ANSSI-CC-2014/94

ST31-K330A Secure microcontroller revision H for Dual mode version (contact and contactless) or contactless only version

1. The product

1.1. Presentation of the product

The evaluated product is the "ST31-K330A Secure microcontroller revision H for Dual mode version (contact and contactless) or contactless only version**,** with optional NesLib cryptographic library v3.2, MIFARE® DESFire® EV1 library v2.2 and MIFARE Plus®-S library v1.3" 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. 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]. 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] paragraph 2.1 "TOE identification" and [GUIDES]):
- Information written on the microcontroller:
    - K330A: STMicroelectronics internal name of the product from the ST31 family, where the letter A identifies the major revision of the silicon;
    - YGE: 3-digit code identifying the dedicated software also called the OST[1] (Operating system for Test);
    - UZZ[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;

---

[1] Dedicated operating system for the testing and maintenance of the TOE.
[2] This 3-digit code identifies the embedded software, which is unique for each customer. This 3-digit code present on all chips supplied to a customer will therefore be different from the one appearing on the evaluated microcontrollers.

ST31-K330A Secure microcontroller revision H for Dual
mode version (contact and contactless) or contactless only
version   Certification report ANSSI-CC-2014/94

- ST4: Identification of the manufacturing site (here, 4 corresponds to the STMicroelectronics Rousset site);
- Identification, by a single letter, of the revision of each level of the manufacturing process corresponding to the sequence of masks ("Maskset") internal revision H;
- information present in the OTP area ("One Time Programmable") of the EEPROM:
  - *0033h*: Master identification number of the ST31-K330A product written on 2 bytes (see [GUIDES] for the EEPROM location);
  - *0059h*: Child identification number of the ST31-K330A product written on 2 bytes (see [GUIDES] for the EEPROM location). The 0059h value corresponds to the commercial version MR31Z052H. To obtain the exact value of the Child identification number for each commercial version, refer to [GUIDES];
  - *14h*: version of the OST code, hexadecimal value written on 1 byte (see [GUIDES] for the EEPROM location);
  - *48h*: internal revision letter H of the product, ASCII character coded in hexadecimal format written on 1 byte (see [GUIDES] for the EEPROM location);
- information returned by the libraries:
  - *1320h*: reference of the NesLib cryptographic library version 3.2 (see "ST31 NesLib cryptographic library User manual" for the API description);
  - *2210h*: reference of the MIFARE technology library (see "User Manual: MIFARE DESFire EV1 Library 2.2" for the API description);
  - *1300h*: reference of the MIFARE technology library (see "User Manual: MIFARE Plus-S Library 1.3 for ST31-K330" for the API description).

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;
- Access control to the MIFARE DESFire EV1and MIFARE Plus-S libraries;
- 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 optional cryptographic library NesLib version 3.2 offering, depending on the selected configuration, RSA, SHA and ECC implementations as well as a secure service for generating prime numbers and RSA keys;
- The optional MIFARE DESFire EV1 library version 2.2;
- The optional MIFARE Plus-S library version 1.3.

1.2.4.   Architecture

The hardware architecture of the ST31-K330A microcontroller is illustrated in figure 1.
It consists of:

ST31-K330A Secure microcontroller revision H for Dual mode version (contact and contactless) or contactless only version

Certification report ANSSI-CC-2014/94

- An ARM® SecurCore® SC000™ 32-bit RISC core processor;
- Memories:
  - 52^1/38/22/16 KB of EEPROM (with integrity check) for data storage;
  - A ROM partitioned into two distinct areas: a 24 KB area reserved for STMicroelectronics and a 320 KB user area;
  - 8 KB of RAM;
- security modules: memory protection units (MPU), memory protection unit dedicated to libraries (LPU), random number generator (TRNG), 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);
- Co-processors:
  - EDES for supporting DES algorithms;
  - AES for supporting AES algorithms;
  - NESCRYPT with a dedicated RAM for supporting public key cryptographic algorithms;
- an ISO 14443 type A, B and B' radio frequency communication module compliant with PayPass™ specifications.

---

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

ST31-K330A Secure microcontroller revision H for Dual
mode version (contact and contactless) or contactless only
version   Certification report ANSSI-CC-2014/94
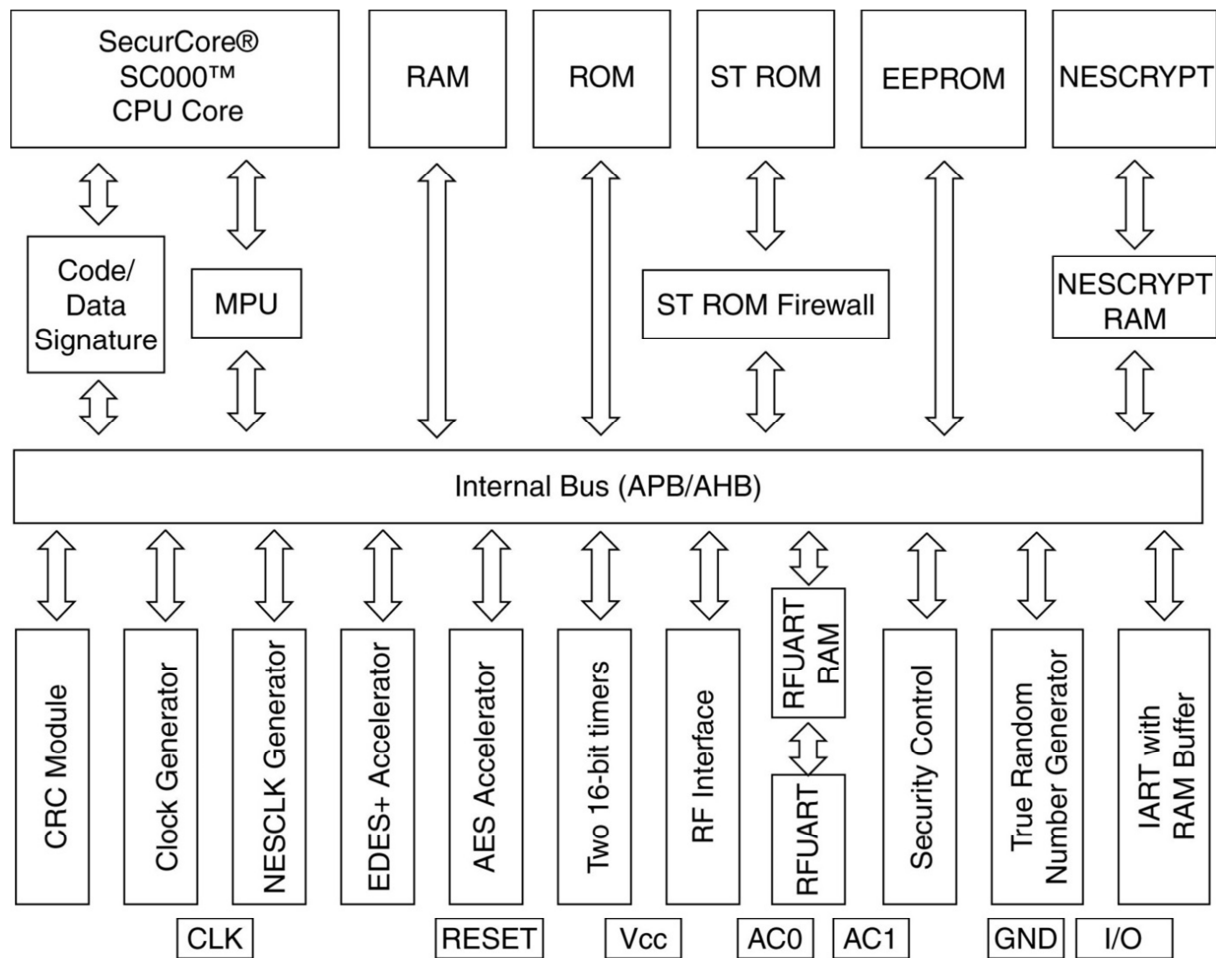

Figure 1: Architecture

Optionally, the user can also choose to integrate a cryptographic library (NesLib version 3.2) providing 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.

Optionally, the user can also choose to integrate the MIFARE DESFire EV1 library version 2.2 or the MIFARE Plus-S library version 1.3. This library is included in the product security target and is fully embedded in the product ROM.

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

The OST:
-   ensure the start of the product ("Boot");
-   provides commands for the testing and maintenance of the TOE;
-   also ensures the access control to these functions when the TOE is in Test or User configuration.

This software component can no longer be accessed by the embedded application once the TOE is configured for use in the field (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:

Certification report ANSSI-CC-2014/94

ST31-K330A Secure microcontroller revision H for Dual mode version (contact and contactless) or contactless only version
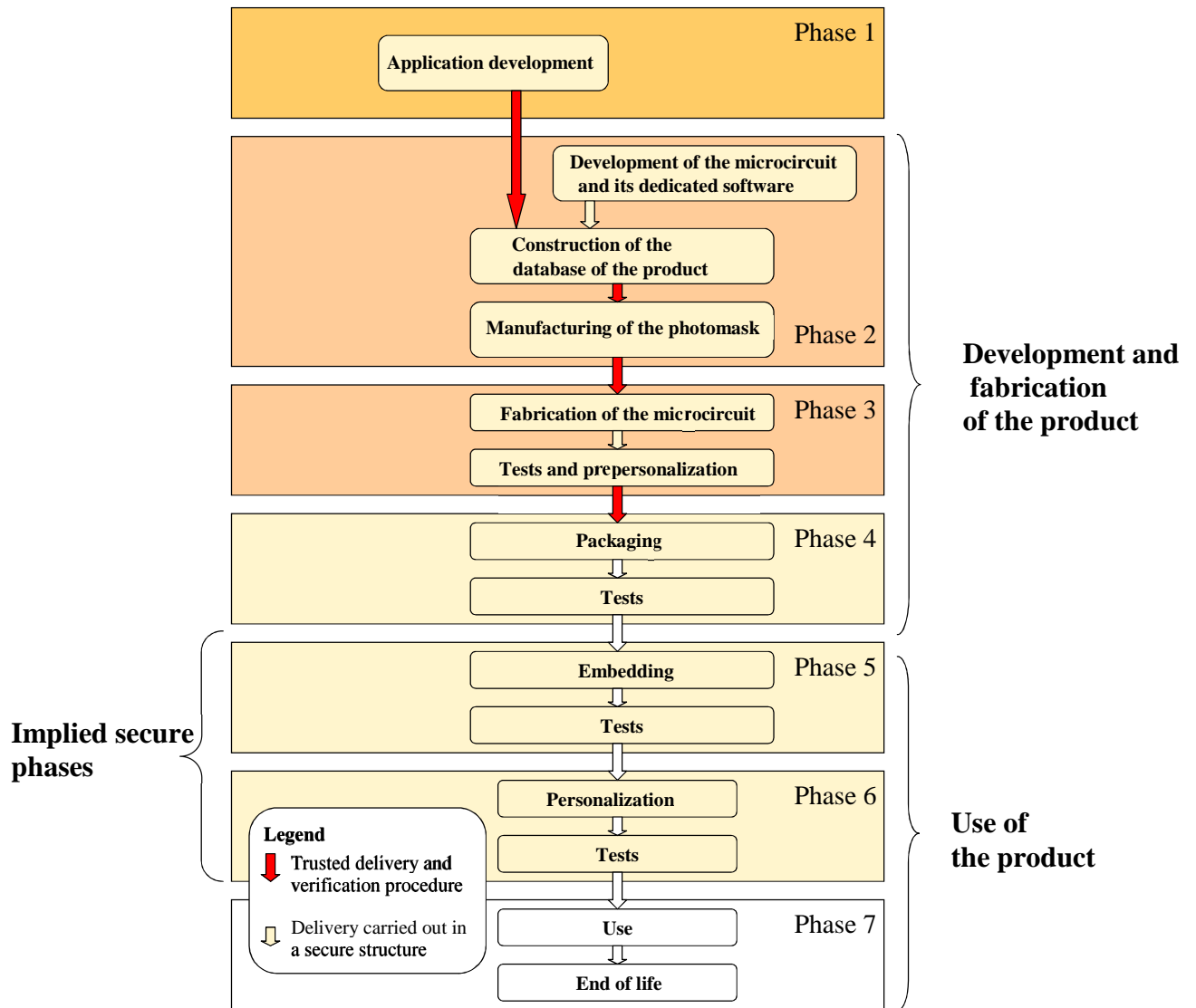

Figure 2: Life cycle

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

STMicroelectronics	STMicroelectronics
Smartcard IC Division 190 Avenue Célestin Coq ZI de Rousset-Peynier 13106 Rousset Cedex France	5A Serangoon North Avenue 5 554574 Singapore Singapore

ST31-K330A Secure microcontroller revision H for Dual mode version (contact and contactless) or contactless only version

Certification report ANSSI-CC-2014/94

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 China	**STMicroelectronics** 629 Lorong 4/6 Toa Payoh 319521 Singapor Singapore
Dai Nippon Printing Co., Ltd 2-2-1 KAMI-FUKUOKA, Fujimino-shi Saitama 356-8507 Japan	**Dai Nippon Printing Europe** Via C. Olivetti 2/A I-20041 Agrate Italy
CMP Georges Charpak 880 Avenue de Mimet 13542 Gardanne France	**Smartflex** N°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
STMicroelectronics 635 route des lucioles 06560 Valbonne France	**STMicroelectronics** 12 rue Jules Horowitz, BP 217 38019 Grenoble Cedex France
STMicroelectronics 10 rue de Jouanet, ePark 35700 Rennes France	**STMicroelectronics** 850 rue Jean Monet 38926 Crolles France
STMicroelectronics 18 Ang M0 Kio Industrial park 2 56950 Singapore Singapore	

Certification report ANSSI-CC-2014/94

ST31-K330A Secure microcontroller revision H for Dual mode version (contact and contactless) or contactless only version

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 operation 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 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 UZZ 3-digit code and its purpose is to enable:
- interaction with the TOE through commands sent by the I/O;
- loading of test applications in EEPROM, or in RAM.

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

ST31-K330A Secure microcontroller revision H for Dual
mode version (contact and contactless) or contactless only
version   Certification report ANSSI-CC-2014/94

2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 3.1 revision 4** [CC], with the Common Evaluation Methodology [CEM].
For assurance components which are not covered by [CEM] manual, the evaluation facility own evaluation methods, validated by ANSSI, have been used.

In order to meet the specificities of smart cards, the [JIWG IC] and [JIWG AP] guides have been applied. Thus the reached AVA_VAN level has been determined according to the rating table of the [JIWG AP] guide that is more demanding than the default one defined in [CC] used for other types of products (software products for example).

2.2. Evaluation work

The evaluation relies on the evaluation results of the "ST31-K330A Secure microcontroller revision F for the Dual mode version (contact and contactless) or the contactless only version, with optional NesLib cryptographic library revision 3.2 and MIFARE DESFire EV1 library revision 2.2"certified the 4th December 2013 under the reference [ANSSI-CC-2013/66].

The evaluation technical report [ETR], delivered to ANSSI the 18th December 2014, provides details on the work performed by the evaluation facility and assesses that all evaluation tasks are "**pass**".

2.3. Cryptographic mechanisms robustness analysis

The robustness of cryptographic mechanisms has not been analysed according to the ANSSI reference [REF]. 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 random number generator was evaluated by using the [AIS31] methodology.
The generator achieved the class "P2 – *SOF/High*".

Certification report ANSSI-CC-2014/94

ST31-K330A Secure microcontroller revision H for Dual mode version (contact and contactless) or contactless only version

3. Certification

3.1. Conclusion

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

This certificate testifies that the product "ST31-K330A Secure microcontroller revision H for Dual mode version (contact and contactless) or contactless only version, with optional NesLib cryptographic library v3.2, MIFARE® DESFire® EV1 library v2.2 and MIFARE Plus®-S library v1.3", submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL 5 augmented for ALC_DVS.2, ASE_TSS.2 and AVA_VAN.5 components.

3.2. Restrictions

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

This certificate provides a resistance assessment of the product "ST31-K330A Secure microcontroller revision H for Dual mode version (contact and contactless) or contactless only version, with optional NesLib cryptographic library v3.2, MIFARE® DESFire® EV1 library v2.2 and MIFARE Plus®-S library v1.3" product 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 microcontroller would only be assessed through the final product evaluation, which could be performed on the basis of the current evaluation results.

The user of the certified product shall respect the security objectives for the operational environment, as specified in the security target [ST], and shall respect the recommendations in the guidance [GUIDES].

ST31-K330A Secure microcontroller revision H for Dual
mode version (contact and contactless) or contactless only
version   Certification report ANSSI-CC-2014/94

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.

Certification report ANSSI-CC-2014/94

ST31-K330A Secure microcontroller revision H for Dual mode version (contact and contactless) or contactless only version

Annex 1. Evaluation level of the product [CCv3.1R4]

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+	Name of the component
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 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 Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	**1**	Extended component definition
	ASE_INT	1	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	1	**2**	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	1	**2**	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		**1**	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	**2**	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

ST31-K330A Secure microcontroller revision H for Dual
mode version (contact and contactless) or contactless only
version   Certification report ANSSI-CC-2014/94

AVA Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5	5	Advanced methodical vulnerability analysis

Certification report ANSSI-CC-2014/94

ST31-K330A Secure microcontroller revision H for Dual mode version (contact and contactless) or contactless only version

Annex 2. Evaluated product references

[ST]	Reference security target for the evaluation : - ST31-K330A version H (dual or contactless mode only) with optional library NesLib 3.2, and optional technology MIFARE® DESFire® EV1 2.2 and optional technology MIFARE® Plus® S 1.3 SECURITY TARGET, 10 June 2014, reference SMD_MR31Zxxx_ST_13_001_V02.01, version 2.01. For publication requirements, the following security target was provided and validated in the scope of this evaluation : - ST31-K330A version H (dual or contactless mode only) with optional library NesLib3.2 and optional technology MIFARE® DESFire® EV1 2.2 and optional technology MIFARE® Plus® 1.3 Security Target – Public Version, 12 December 2014, reference SMD_MR31Zxxx_ST_13_002, version 2.02.
[ETR]	Technical report of the evaluation: - Evaluation Technical Report CHABLIS-2 Project, 18 December 2014, reference CHABLIS-2_ETR_v2.1/2.1, version 2.1. For the composition evaluation needs for this microcontroller, a technical report on composition has been validated: - ETR Lite for Composition ST31-K330A Project, 18 December 2014, reference CHABLIS-2_ETRLiteComp_ v2.1/2.1, version 2.1.
[CONF]	Configuration list: - ST31-K330A - Configuration list, reference SMD_ST31-K330A_H_CFGL_14_001, version v1.0, 6 June 2014. Documentation list: - ST31-K330 Evaluation Documentation Report, 6, November 2014, reference SMD_ST31-K330_DR_12_001, version v4.1.

ST31-K330A Secure microcontroller revision H for Dual mode version (contact and contactless) or contactless only version

Certification report ANSSI-CC-2014/94

[GUIDES]	Product user guide: - ARM SC000 Technical Reference Manual - R0P0, September 2010, reference ARM DDI 0456, revision A; - ARM v6-M Architecture Reference Manual, September 2010, reference ARM DDI 0419, revision C; - ST31 - AIS31 Compliant Random Number user manual, February 2013, reference UM_31_AIS31, revision 2; - ST31 - AIS31 Reference implementation - Startup, online and total failure tests - Application Note, February 2013, reference AN_31_AIS31, revision 2; - ST31 - K330 Platform (Sx31Zxxx,Mx31Zxxx) - Datasheet, 3 June 2014, reference DS_ST31Z052, revision 4; - ST31 - K330 Platform - Die description, 2 June 2014, reference DD_31Z052, revision 4; - Application note – ST31-K330 security guidance, 5 September 2014, reference AN_SECU_ST31-K330, revision 4; - ST31 NesLib cryptographic library - User manual, 24 April 2014, reference UM_31_NESLIB_3.2, revision 7; - ST31-K330 and ST33-K8H0 secure microcontrollers - Power supply glitch detector characteristics, March 2013, reference AN_31_GLITCH, revision 2; - Application note - ST31-K330 Dual interface secure microcontrollers - Recommendations for contactless operations, 28 July 2014, reference AN_31_RCMD, revision 2; - MIFARE DESFire EV1 library 2.2 - user manual, February 2013, reference UM_MIFARE_DESFire_EV1_2.2, revision 2; - MIFARE DESFire EV1 interface specification User manual, 8 October 2013, reference UM_MIFARE_DESFire_EV1_Interface, revision 1; - MIFARE Plus S library 1.3 for ST31-K330 – User manual, 16 May 2014, reference UM_31_MIFARE_PLUS_S-1.3.0, revision 1; - MIFARE Plus S interface specification, October 2013, reference UM_MIFARE_PLUS_S, revision 1.
[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.*

Certification report ANSSI-CC-2014/94

ST31-K330A Secure microcontroller revision H for Dual
mode version (contact and contactless) or contactless only
version

Annex 3. Certification references

	Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, 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, révision 4, ref CCMB-2012-09-004.
[JIWG IC] *	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, February 2009.
[JIWG AP] *	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, January 2013.
[CC RA]	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, July 2, 2014.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.
[AIS 34]	Application Notes and Interpretation of the Scheme (AIS) – Evaluation Methodology for CC Assurance Classes for EAL5+ (CC v2.3 &CC v3.1) and EAL6 (CC v3.1), AIS34, version 3, 3 September 2009, BSI (Bundesamt für Sicherheit in der Informationstechnik).
[AIS 31]	Functionnality 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; the support equivalent CCRA document applies to the frame of the mutual recognition agreement of the CCRA.