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-2015/59

ST31H320 A01 including optional cryptographic library NESLIB

COURTESY TRANSLATION

Paris, 28 December 2015

Le directeur général adjoint de l'agence nationale de la sécurité des systèmes d'information

Contre-amiral Dominique RIBAN
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Warning

This report is intended to provide people who request evaluations with a document to certify the level of security provided by the product under the usage or operating conditions defined in this report for the version which was evaluated. It is also intended to provide potential acquirers of the product with the conditions under which they may use the product to ensure that they meet the conditions for which the product was evaluated and certified; this is why the certification report must be read in conjunction with the evaluated usage and administration guides and with the product's security target which describes the pre-supposed threats, environmental hypotheses and usage conditions so that the user can judge whether the product is suitable for their needs in terms of security objectives.

The certification does not in itself constitute a product recommendation by the agence nationale de la sécurité des systèmes d'information (ANSSI) and does not guarantee that the certified product is completely free of vulnerabilities that can be exploited.

All correspondence relating to this report must be sent to:

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

certification@ssi.gouv.fr

Certification report reference

ANSSI-CC-2015/59

Product name

ST31H320 A01 including optional cryptographic library NESLIB

Product reference/version

A01

Protection profile conformity

Security IC Platform Protection Profile with Augmentation Packages, version 1.0,

certified by the BSI under reference BSI-CC-PP-0084-2014 o, 19 February 2014

with

"Package 1: Loader dedicated for usage in Secured Environment only"

Evaluation criteria and version

Common criteria version 3.1 revision 4

Evaluation level

EAL 5 augmented

ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.1, ALC_TAT.3, ATE_COV.3, ATE_FUN.2, AVA_VAN.5

Developer

STMicroelectronics

190 avenue Celestin Coq, ZI de Rousset, 13106 Rousset, France

Sponsor

STMicroelectronics

190 avenue Celestin Coq, ZI de Rousset, 13106 Rousset, France

Evaluation facility

Serma Technologies

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

Mutual Recognition Agreements

CCRA

SOG-IS

The product is recognized at level EAL2.

Foreword

Certification

Certification of the security provided by information technology products and systems is governed by amended decree 2002-535 of 18th April 2002. This decree indicates that:

- The agence nationale de la sécurité des systèmes d'information drafts the **certification reports**. These reports specify the characteristics of the security objectives proposed. They may contain any warnings that their authors consider are worth mentioning for security reasons. The people who order the reports may choose whether or not to communicate them to third parties or to make them public (article 7).
- The **certificates** awarded by the French Prime Minister certify that the individual product or system submitted for evaluation meets the specified security characteristics. They also certify that the evaluations were carried out according to current rules and standards, with the required levels of competence and impartiality (article 8).

The certification procedures are available on the website www.ssi.gouv.fr.

Table of contents

1. Product

1.1. Presentation of the product

The evaluated product is the secure microcontroller "*ST31H320 A01 including optional cryptographic library NESLIB*" developed by *STMICROELECTRONICS.*

As described in the security target [ST] in paragraph "*TOE overview*", this product has different configurations depending on the non-volatile *Flash* memory size, and the activation of the cryptographic coprocessor NESCRYPT. These configurations are also described in the *Datasheet* document (refer to [GUIDES]).

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. Description of the product

1.2.1. Introduction

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

This security target is strictly conformant to the protection profile [PP0084], with the package *"Loader dedicated for usage in a secure environment only"*.

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 (see [ST], "TOE identification" paragraph, and [GUIDES]):
- *IC Maskset name*: K8N0A
- *IC version*: C
- *Master product identification number*: 00DE
- *Firmware version*: 2.0.2
- *OST version*: 4.0
- (optional) *NesLib cryptographic library version*: 4.2.10

All the values are available through the logic interfaces of the product, according to the methods and formats described in [GUIDES]. In addition, "K8N0A", the *IC Maskset name* value, is etched on the surface of the component.

1.2.3. Security services

The product provides the following main security services:
- Physical tampering protection;
- Logical integrity of the product;

- Memory access control;
- Management of security violations;
- Unobservability of sensitive data;
- Flash memory loading and management;
- Support for symmetric key cryptography;
- Support for asymmetric key cryptography;
- Support for random number generation;
- The optional service of a NesLib v4.2 cryptographic library offering RSA, SHA and ECC implementation as well as the secure generation of prime numbers and RSA keys.

1.2.4. Architecture

This product is comprised of a hardware part and a software part, both described in the security target in paragraph *TOE description*.
The hardware part mainly consists of:

- a SecurCore® SC000™ ARM® processor;
- cryptographic coprocessors to accelerate AES, Triple DES and asymmetric cryptography calculations;
- a true random number generator (TRNG);
- memories (RAM and Flash);
- security modules: memory protection unit (MPU), clock generator, security control and monitoring, and data integrity control;
- functional modules: timers and input/output management in contact mode.

The software part is made up of:

- a dedicated software (OST), involved in the component startup (*boot sequence*);
- a dedicated software (*Firmware*) for Flash memory lifecycle management and loading(*Secure Flash loader*), and for interfacing with the application (*drivers*);
- optionally, a cryptographic library (NesLib) offering RSA services (including key generation), elliptic curve cryptography, hashing, prime number generation and deterministic random bit generation (DRBG).

1.2.5. Lifecycle

The product lifecycle is described in the security target (see [ST]); it is compliant with the 7-phase lifecycle described in [PP0084].

The sites involved in the lifecycle for phases 2, 3 and 4 are indicated in the security target (see Table 16 in [ST]).

For this evaluation, the evaluator considers the developer of the software to be embedded in the microcontroller as the user of the product.

In the security target, the developer has chosen the compliance with "*Package 1: loader dedicated for usage in a secure environment only*" of protection profile [PP0084]. In *Issuer*[1] configuration, the user must load the application in a secure environment.

[1] Also called *ADMIN* in several STMicroelectronics documents, including the security target.

1.2.6. Evaluated configuration

The certificate applies to the ST31H320 A01 product in the different configurations that are available (memory sizes, NESCRYPT activation, see §1.1 and [GUIDES]).

2. Evaluation

2.1. Evaluation reference bases

The evaluation was carried out according to **Common Criteria version 3.1 revision 4** [CC], and the evaluation methodology defined in the CEM manual [CEM].
For the assurance components which are not covered by the [CEM] manual, methods specific to the evaluation centre and validated by the ANSSI were used.

The guides [JIWG IC] and [JIWG AP] were applied to meet the specifics of the smart cards. So, the AVA_VAN level was determined according to the rating scale in the guide [JIWG AP]. Remember that this rating scale is more demanding than the scale defined by default in the standard method [CC], used for the other product categories (software products, for example).

2.2. Evaluation work

The evaluation technical report [RTE], delivered to the ANSSI on 18 December 2015, provides details on the work performed by the evaluation facility and certifies that all evaluation tasks are "**pass**".

2.3. Cryptographic mechanisms rating according to the ANSSI's technical reference bases

The rating of cryptographic mechanisms according to the ANSSI technical reference framework [REF] has not been carried out. Nonetheless, the evaluation has not detected any design or manufacturing vulnerabilities for the targeted AVA_VAN.5 level.

2.4. Random number generator analysis

The evaluation facility evaluated the random number generator using the [AIS 31] methodology and it satisfies the requirements of the PTG.2 class.

The analysis did not put in evidence any statistic bias forbidding the direct use of the generator outputs. This is not sufficient to state that the generated data are really random, but it ascertains that the generator does not have major design defects. As stipulated in the [REF] document, it is reminded that, for a cryptographic usage, the hardware random number generator output must be submitted to a cryptographic reprocessing even if the analysis of the physical random number generator has revealed no weaknesses.

3. Certification

3.1. Conclusion

The evaluation was carried out according to current rules and standards with the levels of competence and impartiality required for an approved evaluation centre. All of the evaluation work carried out enables a certificate to be issued according to decree 2002-535.

This certificate confirms that the evaluated "ST31H320 A01 product including the optional cryptographic library NESLIB" meets the security characteristics specified in its security target [ST] for the evaluation level EAL 5 augmented for the ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.1, ALC_TAT.3, ATE_COV.3, ATE_FUN.2 and AVA_VAN.5 components.

3.2. Usage restrictions

This certificate relates to the product specified in chapter 1.2 of this certification report.

This certificate provides an assessment of the resistance of "ST31H320 A01 including the optional cryptographic library NESLIB" to highly generic attacks due to the absence of a specific embedded application. Consequently, the security of a full product built on the micro-circuit may only be assessed by evaluating the full product; this evaluation may be carried out based on the results of the evaluation mentioned in chapter 2.

The user of the certified product must ensure that the security objectives are met within the operating environment, as specified in the security target [ST] and follow the recommendations in the guides provided [GUIDES].

3.3. Certificate recognition

3.3.1. European recognition (SOG-IS)

This certificate is issued under the conditions of the SOG-IS agreement [SOG-IS].

The 2010 SOG-IS European recognition agreement enables recognition of the ITSEC and Common Criteria certificates by the countries which have signed the agreement[2]. For smart cards and similar mechanisms, European recognition applies up to ITSEC E6 High and CC EAL7 level. The certificates that are recognised in the context of this agreement are issued with the following mark:

3.3.2. International Common Criteria Recognition (CCRA)

This certificate is issued under the conditions of the CCRA agreement [CC RA].

The "Common Criteria Recognition Arrangement" enables recognition of the Common Criteria certificates by the signatory countries[3].
Recognition applies to CC EAL2 level assurance components and the ALC_FLR family. The certificates that are recognised in the context of this agreement are issued with the following mark:

[2] The countries that have signed the SOG-IS agreement are: Germany, Austria, Spain, Finland, France, Italy, Norway, the Netherlands, the United Kingdom and Sweden.

[3] The following countries have signed the CCRA agreement: Germany, Australia, Austria, Canada, Denmark, Spain, the United States of America, Finland, France, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, Norway, New Zealand, Pakistan, the Netherlands, the Republic of Korea, the Czech Republic, the United Kingdom, Sweden and Turkey.

Annexe 1. Evaluation level of the product

Class	Family	Components by assurance level							Assurance level of the product	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 5+	Component name
ADV Development	ADV_ARC		1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	5	Complete semi-formal functional specification with additional error information
	ADV_IMP				1	1	2	2	2	Complete mapping of the implementation representation of the TSF
	ADV_INT					2	3	3	3	Minimally complex internals
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	5	Complete semiformal modular design
AGD User guidance	AGD_OPE	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	1	Preparative procedures
ALC Support to lifecycle	ALC_CMC	1	2	3	4	4	5	5	5	Advanced support
	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 lifecycle model
	ALC_TAT				1	2	3	3	3	Compliance with implementation standards - all parts
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 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	Rigorous analysis of coverage
	ATE_DPT			1	1	3	3	4	3	Testing: modular design
	ATE_FUN		1	1	1	1	2	2	2	Ordered functional testing
	ATE_IND	1	2	2	2	2	2	3	2	Independent testing: sample
AVA Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5	5	Advanced methodical vulnerability analysis

Annexe 2. Documentary references for evaluated product

[ST]	Security target for the evaluation : ST31H320 A01 including optional cryptographic library NESLIB, Security Target, SMD_ST31H320_ST_14_001 Rev A01.5, December 2015, STMicroelectronics. For publication requirements, the following security target was provided and validated in the scope of this evaluation : ST31H320 A01 including optional cryptographic library NESLIB, Security Target for composition, SMD_ST31H320_ST_14_002 Rev A01.5, December 2015, STMicroelectronics.
[RTE]	Technical report of the evaluation: Evaluation Technical Report LOUPIAC Project, LOUPIAC_ETR_v1.2, 18 December 2015, Serma Technologies. For the composition evaluation needs for this microcontroller, a technical report for composition has been validated: ETR Lite for Composition LOUPIAC Project, LOUPIAC_ETRliteComp_v1.2, 18 December 2015, Serma Technologies.
[CONF]	Product configuration list : - ST31 – K8N0 Configuration List, SMD_ST31H310_C_CFGL_15_003 Rev 1.0, 15 December 2015, STMicroelectronics; - NesLib 4.2.10 for ST31 on ST31H320 configuration list, SSS_Neslib4210ST31_H320_CFGL_15_001, July 2015, STMicroelectronics.

[GUIDES]	- ST31H platform ST31H320, Datasheet – preliminary data, DS_ST31H320 Rev 0.4, August 2015, STMicroelectronics; - ARM Cortex SC000 Technical Reference Manual, ARM_DDI_0456 Rev A, September 2010, ARM; - ARMv6-M Architecture Reference Manual, ARM_DDI_0419 Rev C, September 2010, ARM; - ST31G and ST31H Secure MCU platforms, Security guidance, AN_SECU_ST31G_H Rev 2, November 2015, STMicroelectronics; - ST31 firmware, User manual, UM_ST31_FW Rev 5, August 2015, STMicroelectronics; - NesLib 4.2 library, User manual, UM_NESLIB_4.2 Rev 1.0, July 2015, STMicroelectronics; - ST31G and ST31H Secure MCU platforms NesLib 4.2 security recommendations, AN_SECU_ST31_NESLIB_4.2 Rev1, August 2015, STMicroelectronics; - NesLib 4.2.10 for ST31 platforms, release note, RN_ST31_NESLIB_4.2.10 Rev 1, August 2015, STMicroelectronics; - ST31H320 Flash memory loader installation guide, User manual, UM_31H_FL Rev 3, July 2015, STMicroelectronics; - ST31G and ST31H - AIS31 Compliant Random Number - User Manual, UM_31G_31H_AIS31 Rev 1.0, January 2015, STMicroelectronics; - ST31 - AIS31 Reference implementation - Startup, online and total failure tests - Application Note, AN_31_AIS31 Rev 2, February 2013, STMicroelectronics.
[PP0084]	Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13 January 2014. *Certified by the BSI (Bundesamt für Sicherheit in der Informationstechnik) under reference BSI-CC-PP-0084-2014.*

Annexe 3. References associated with the certification

Decree 2002-535 of 18 April 2002 modified related to the evaluation and certification of the security provided by the information technology products and systems.	
[CER/P/01]	Procedure CER/P/01 Certification of the security provided by information technology products and systems, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, September 2012, version 3.1, revision 4, reference CCMB-2012-09-001; Part 2: Security functional components, September 2012, version 3.1, revision 4, reference CCMB-2012-09-002; Part 3: Security assurance components, September 2012, version 3.1, revision 4, reference CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, September2012, version 3.1, revision 4, reference 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, 2 July 2014.
[SOG-IS]	“Mutual Recognition Agreement of Information Technology Security Evaluation Certificates”, version 3.0, 8 January 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), see www.ssi.gouv.fr.
[AIS 31]	A proposal for: Functionality classes for random number generators, AIS20/AIS31, version 2.0, 18 September 2011, BSI (Bundesamt für Sicherheit in der Informationstechnik).

*Document of the SOG-IS; in the frame of the mutual recognition agreement of the CCRA, the support equivalent CCRA document applies.