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-2016/58

ST31G480 A02 including optional cryptographic library NESLIB and optional technologies MIFARE DESFire EV1 and MIFARE Plus X

Courtesy Translation

Paris, 25 August 2016

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 about 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-2016/58

Product name

ST31G480 A02 including optional cryptographic library NESLIB and optional technologies MIFARE DESFire EV1 and MIFARE Plus X

Product reference/version

A02

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

in compliance 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, ACL_DVS.2, ALC_FLR.1, ALC_TAT.3, ATE_COV.3, ATE_FUN.2, AVA_VAN.5, ASE_TSS.2

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 Safety & Security

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 writes 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. Product overview

The evaluated product is the "ST31G480 A02 including optional cryptographic library NESLIB and optional technologies MIFARE DESFire EV1 and MIFARE Plus X" 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, the activation of the various communication interfaces, the antenna tuning, the activation of the MIFARE-dedicated hardware resources, and the activation of the NESCRYPT cryptographic coprocessor . These configurations are also described in the *Datasheet* document (see [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 This card has many possible uses (secure identity documents as well as bank, pay TV, transport, health applications, etc.) depending on the embedded software applications. These software applications are not in the scope of this evaluation.

1.2. 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 is strictly compliant with 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*: K8L0B;
- *IC version*: H;
- *Master product identification number*: 00B8;
- *Firmware version*: 2.1.0;
- *OST version*: 3.4;
- (optional) *NesLib crypto library version*: 4.2.10;
- (optional) *MIFARE DESFire EV1 version*: 4.8.10;
- (optional) *MIFARE Plus X* version: 2.4.4;

All the values are available through the logic interfaces of the product, according to the methods and formats described in [GUIDES]. Moreover, "K8L0B ", the *IC Maskset name*, is etched on the surface of the component.

1.2.3. Security services

The product provides the following main security services:

- Physical tampering protection;
- Initialization of the hardware platform and attributes;
- Secure management of the lifecycle;
- Logical integrity of the product;
- memory firewalls;
- Management of security violations;
- Unobservability of sensitive data;
- loading and management of the *Flash* memory;
- Support for symmetric key cryptography;
- Support for asymmetric key cryptography;
- Support for random number generation;
- The optional service of a NesLib cryptographic library NesLib offering RSA, SHA and ECC implementation as well as the secure generation of prime numbers and RSA keys;
- the (optional) MIFARE DESFire EV1 technology;
- the (optional) MIFARE Plus X technology.

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:

- un processeur ARM SecurCore SC000;
- cryptographic coprocessors to accelerate AES, Triple DES and asymmetric cryptography calculations;
- a true random number generator (TRNG);
- (RAM, Flash) memories;
- Security modules: memory protection unit (MPU), clock generator, security control and monitoring, and memory integrity control;
- Functional modules: timers, input/output management in contact and contactless modes.

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 (including key generation), elliptic curve, hashing, prime number generation and deterministic random bit generation (DRBG) services.
- optionally, the MIFARE DESFire EV1 and MIFARE Plus X technologies.

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 user 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 *ADMIN*[1] configuration, the user must load the application in a secure environment.

1.2.6. Evaluated configuration

The certificate applies to the ST31G480 A02 product in the different configurations that are available (memory size and activated functionality, see §1.1 and [GUIDES]).

[1] Also called *ISSUER* in some Guides.

2. Evaluation

2.1. Evaluation reference frame

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.
For insurance 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 [JIWG 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 [RTE], delivered to the ANSSI on 25 July 2016, provides details on the work performed by the evaluation facility and certifies that all evaluation tasks are "**pass"**.

2.3. Rating of cryptographic mechanisms according to the ANSSI technical reference framework

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 [AIS31] methodology and it meets the requirements of the PTG.2 class.

This analysis did not put in evidence any statistic bias forbidding the direct use of the generator outputs. This analysis 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 imperatively be submitted to a cryptographic algorithm 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 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 evaluated product, "ST31G480 A02 including optional cryptographic library NESLIB and optional technologies MIFARE DESFire EV1 and MIFARE Plus X" meets the security characteristics specified in its security target [ST] for the EAL 5 augmented evaluation level of the ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ACL_DVS.2, ALC_FLR.1, ALC_TAT.3, ATE_COV.3, ATE_FUN.2, AVA_VAN.5 and ASE_TSS.2 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 product resistance 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. Certificate recognition

3.3.1. European recognition agreement (SOG-IS)

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

The 2010 SOG-IS European recognition agreement allows the recognition by signatory countries[1] of the ITSEC and Common Criteria certificates. The European recognition agreement, for smartcards and similar devices, is applicable up to level ITSEC E6 Elevated and CC EAL7. The certificates recognized in the scope of this agreement are released with the following marking:

3.3.2. Common Criteria Recognition Arrangement (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 Common Criteria certificates.
The mutual recognition is applicable up to the assurance components of the CC EAL2 level and also to the ALC_FLR family.
The certificates recognized in the scope of this agreement are released with the following marking:

[1] The following countries have signed the SOG-IS agreement: Germany, Austria, Spain, Finland, France, Italy, Norway, the Netherlands, the United Kingdom and Sweden.
[2] 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 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 with architectural design summary
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]	Reference security target for the evaluation : - ST31G480 A02 including optional cryptographic library NESLIB, and optional technologies MIFARE DESFire EV1 and MIFARE Plus X Security Target, SMD_ST31G480_ST_14_001 Rev A02.4, June 2016, STMicroelectronics. For publication requirements, the following security target was provided and validated in the scope of this evaluation: - ST31G480 A02 including optional cryptographic library NESLIB, and optional technologies MIFARE DESFire EV1 and MIFARE Plus X Security Target for composition, SMD_ST31G480_ST_14_002 Rev A02.4, June 2016, STMicroelectronics
[RTE]	Technical report of the evaluation: - Evaluation Technical Report ELIXIR ST Project, ELIXIR_ST_ETR_v1.1 / 1.1, 22 July 2016, Serma Safety & Security. For the composition evaluation needs for this microcontroller, a technical report on composition has been validated: - ETR Lite for Composition ELIXIR ST Project, Elixir_ST_ETRliteComp_v1.1 / 1.1, 22 July 2016, Serma Safety & Security.
[CONF]	Product configuration list: - ST31 – K8L0 Configuration List, ST31G480_H_68pF_CFGL_16_001 Rev 1.0, 21 March 2016, STMicroelectronics; - ST31 – K8L0 Configuration List, ST31G480_H_20pF_CFGL_16_001 Rev 1.0, 21 March 2016, STMicroelectronics;

[GUIDES]	- ST31G platform ST31G480, Datasheet – preliminary data, DS_ST31G480 Rev 0.12, March 2016, 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 3, March 2016, STMicroelectronics; - ST31 firmware, User manual, UM_ST31_FW Rev 9, March 2016, 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 4, January 2016 STMicroelectronics; - ST31G480 Flash memory loader installation guide, User manual, UM_31G_FL Rev2, February 2016, 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; - MIFARE DESFire EV1 library 4.8 for ST31G480 secure microcontrollers, User manual, UM_31_MFDF_EV1_4.8 Rev 4, February 2016, STMicroelectronics; - MIFARE DESFire EV1 library 4.8.10 for ST31G480 – Application note, AN_ST31G480_MFD_Lib Rev 1.0, STMicroelectronics; - MIFARE DESFire EV1 Interface Specification, User manual, UM_Mifare_Desfire_EV1_Interface, Rev 4.0, April 2016, STMicroelectronics; - MIFARE Plus X library 2.4 for ST31G480- User manual, UM_MIFARE_PLUS_X_2_4 Rev 4, February 2016, 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, referenceCCMB-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]	Cryptographic mechanisms – Rules and recommendations concerning the choice and configuration of cryptographic mechanisms, Version 2.03 of 21 February 2014 annexed to the General Security Reference Framework (RGS_B1), see http://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 equivalent CCRA support document applies.