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-2020/20

MS6003
(Rev C)

Paris, April 16th, 2020

COURTESY TRANSLATION

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-2020/20

Product name

MS6003

Product reference/version

Rev C

Conformity with a protection profile

Security IC Platform Protection Profile with Augmentation Packages

BSI-CC-PP-0084-2014, version 1.0

Conformity with packages

"Authentication of the security IC"
"Loader dedicated for usage in Secured Environment only"
"Loader dedicated for usage by authorized users only"

Evaluation criteria and version

Common Criteria version 3.1 revision 5

Evaluation level

EAL 5 augmented

ALC_DVS.2, AVA_VAN.5

Developer(s)

WISeKey

Arteparc Bachasson, bat A, Rue de la carrière de Bachasson, CS70025
13590 Meyreuil, France

Request made by

WISeKey

Arteparc Bachasson, bat A, Rue de la carrière de Bachasson, CS70025
13590 Meyreuil, France

Evaluation centre

CEA - LETI

17 rue des martyrs, 38054 Grenoble Cedex 9, France

Applicable recognition agreements

CCRA	SOG-IS
This certificate is recognised at EAL2 level	

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. The product

1.1. Presentation of the product

The product evaluated is “MS6003, Rev C” developed by WISeKey.

The microcontroller on its own is not a product that may be used in its current state. It is intended to host one or more applications. It may be inserted into a plastic support to constitute a smart card. This card has multiple uses (secure identity documents, banking applications, subscription television, transport, health, etc.) depending on the application software embedded in it. These software are not part of this evaluation.

1.2. Description of the product

1.2.1. Introduction

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

This security target complies with the protection profile [PP0084] with*:*

- Package “authentication of the security IC”
- Package” loader dedicated for usage in secured environment only”
- Package “loader dedicated for usage by authorized users only”

1.2.2. Security services

The main security services provided by the product are:

- Those of the ARM Secure Core SC300 (Privileged/Unprivileged modes, NMI, ...);
- MPU;
- Protection by voltage, frequency, temperature and glitch detectors;
- Protection by Active Shield, Light detector, mirroring of registers;
- Protection by frequency divisor and dummy operations;
- Support of symmetric and asymmetric cryptography;
- Protection against code loading (secure bootloader)

1.2.3. Architecture

The product is composed of hardware and software parts, both described in the security target [ST] in paragraph 1.4.2 TOE Definition.
The hardware part mainly contains:

- ARM SecureCore SC300 Processor;
- Cryptographic accelerators;
- Physical random generator;
- Volatile and non-volatile memories;
- Communication controllers.

The software part contains:

- Cryptographic library *Crypto Software Toolbox*;
- Wear levelling library;
- Optional *Secure Bootloader* software.

1.2.4. Product identification

The product's components are identified in the configuration list [CONF].

The certified product version may be identified by the following elements:
- Table 1 (hardware and software elements) of the security target [ST]
- Table 2 (document elements) of the security target [ST]

1.2.5. Life cycle

The product life cycle is described in the security target [ST]; it is compliant with the 7 phases life cycle described in [PP0084]. The main life cycle sites considered in the evaluation are described in the Table 3 of the security target [ST].

For the evaluation, the evaluator has considered as product user the developer of an application to be loaded in the TOE.

1.2.6. Evaluated configuration

The certificate relates to the product MS6003 rev C referenced in Table 1 and Table 2 of the security target [ST] with the configurations available at the delivery points defined in the life cycle.

2. Evaluation

2.1. Evaluation reference bases

The evaluation was carried out according to **Common Criteria version 3.1 revision 5** [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

This evaluation took into account the results of the evaluation on the microcontroller "MS6001 revision E". This microcontroller was certified on 29th January 2018 under the reference [ANSSI-CC-2018/02].

The evaluation technical report [ETR], which was delivered to the ANSSI on 16th March 2020, details the work carried out by the evaluation centre and certifies that all the evaluation tasks are rated as "pass**"**.

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

The cryptographic mechanisms were not rated according to the ANSSI's technical reference base [REF]. Nevertheless, the evaluation did not highlight any design or construction vulnerabilities for the targeted AVA_VAN.5 level.

2.4. Random Number Generator analysis

The random number generator is evaluated according to the methodology [AIS 31]. The generator reaches level "PTG.2"class.

In addition, in order to comply with the ANSSI's cryptographic reference base [REF], the output of the physical random number generator must be subjected to cryptographic reprocessing, even though no weakness was found in the physical generator.

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 product “MS6003, rev C” submitted for evaluation meets the security characteristics specified in its security target [ST] for the evaluation level of the AVA_VAN.5 and ALC_DVS.2 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 MS6003 rev C product's resistance to attacks which are highly generic due to the lack 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[1]. 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[2].

Recognition applies to CC EAL4 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:

1 The list of signatory countries of the SOG-IS agreement is available on the website www.sogis.org.

2 The list of signatory countries of the CCRA arrangement is available on the website www.commoncriteriaportal.org..

Appendix 1. Product evaluation level

Class	Family	Components by assurance level							Assurance level selected for the product	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 5+	Component title
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 guides	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 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 estimation	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**5**	Advanced methodical vulnerability analysis

Appendix 2. Documentary references for the product evaluated

[ST]	Reference security target for the evaluation: - Sirocco-C Security Target, version 1.5, 10th march 2020, WISEKEY For publication requirements, the following security target has been supplied and validated in the context of this evaluation: - MS6003 Security Target-Lite, TPG0235A, 10th march 2020, WISEKEY.
[RTE]	Technical evaluation report: - Evaluation Technical Report (full ETR) –SIRROCO-C, LETI.CESTI.SIR.FULL.001-V1.0, 16th March 2020, LETI For the composition evaluation requirements with this microcontroller, a technical report for the composition has been validated: - Evaluation Technical Report (ETR for composition) – SIRROCO-C, LETI.CESTI.SIR.COMPO.001-V1.0, 16 mars 2020, LETI.
[CONF]	Product configuration list: - SIROCCO Manufacturing Configuration List, v1.0, 3rd May 2019, - Sirocco Development Tools Configuration List, v1.0, 4th March 2019, - Wear Leveling Library Configuration List, v1.0, 17th June 2016, - Wear Leveling Library Software Development Tools Configuration List, rev B, 17th June 2016, - Toolbox 4.x Development Tools, rev B, 22nd January 2016, - Secure BootLoader Transport MS6xxx Software Development Tools Configuration List, rev 1, 22nd October 2019, - SIROCCO delivery list, v1.0, 10th March 2020.
[GUIDES]	*See Table 2 of the security target [ST]*
[SITES]	Report of Document analysis and site audit for reuse: - Wisekey Development Environment ALC Class Evaluation Report (Generic documentary activities), WISEKEY-2019_ALC_GEN_v1.0, 25th July 2019, Serma Safety & Security, - Site Technical Audit Report Wisekey Meyreuil, WISEKEY-2018_STAR_v1.0, 20th December 2018, Serma Safety & Security.
[PP0084]	Protection Profile, Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13rd January 2014. Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under reference BSI-PP-0084-2014

[ANSSI-CC-2018/02]	Rapport de certification ANSSI-CC-2018/02, Microcontrôleur MS6001 révision E embarquant la bibliothèque cryptographique Toolbox version 06.04.01.07 et la bibliothèque Wear Levelling version 06.03.02.02, 29th January 2018.

Appendix 3. References linked to certification

Amended decree No. 2002-535 of 18th April 2002 relating to the evaluation and certification of the security provided by information technology products and systems.	
[CER/P/01]	CER-P-01 procedure 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, April 2017, version 3.1, revision 5, ref CCMB-2017-04-001; Part 2: Security functional components, April 2017, version 3.1, revision 5, ref CCMB-2017-04-002; Part 3: Security assurance components, April 2017, version 3.1, revision 5, ref CCMB-2017-04-003.
[CEM]	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, April 2017, version 3.1, revision 5, ref CCMB-2017-04-004.
[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 smart cards, version 3.0, April 2019.
[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, 8th January 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21st February 2014 annexée au Référentiel général de sécurité (RGS_B1), www.ssi.gouv.fr.
[AIS 31]	A proposal for: Functionality classes for random number generators, AIS20/AIS31, version 2.0, 18th September 2011, BSI (Bundesamt für Sicherheit in der Informationstechnik).

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