



**PREMIER
MINISTRE**

*Liberté
Égalité
Fraternité*

**Secrétariat général de la défense
et de la sécurité nationale**

Agence nationale de la sécurité
des systèmes d'information

Certification report ANSSI-CC-2021/31

**CN Series Encryptor
comprising of the models
CN4010/CN4020/CN6010/CN6140/CN9100/CN9120
running software version 5.0.2**

Paris, 7th July 2021

COURTESY TRANSLATION



WARNING

This report is intended to provide the sponsors with a document permitting to prove the security level offered by the product in the operation and utilisation conditions defined in this report for the evaluated version. It is also intended to provide the potential purchaser of the product with the conditions under which he can operate or use the product so as to be in the conditions of use for which the product has been assessed and certified; this is why this certification report should be read in conjunction with the evaluated user and administration guides as well as the product security target that describes the threats, the assumptions about the environment and the presupposed conditions of use so that the user can judge the suitability of the product for his needs in terms of safety objectives.



Certification does not in itself constitute a recommendation of the product by the National Information Systems Security Agency (ANSSI) and does not guarantee that the certified product is completely free from exploitable vulnerabilities.

All correspondence in relation to this report should 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

certification@ssi.gouv.fr

Reproduction of this document without alteration or cutting is authorized.

Reference of the certification report	ANSSI-CC-2021/31
Product name	CN Series Encryptor
Reference/product version	comprising of the models CN4010/CN4020/CN6010/CN6140/CN9100/CN9120 running software version 5.0.2
Compliance with a protection profile	N/A
Evaluation criteria and version	Common Criteria version 3.1 revision 5
Evaluation level	EAL 4 extended ALC_FLR.3
Developer	SENETAS 312 Kings Way, South Melbourne Victoria 3205 Australia
Sponsors	SENETAS 312 Kings Way, South Melbourne Victoria 3205 Australia
Evaluation centre	OPPIDA 4-6 avenue du vieil étang, Bâtiment B 78180 Montigny le Bretonneux, France
Applicable recognition agreements	  <p>This certificate is recognized at EAL2 level.</p>

PRÉFACE

The certification of security offered by information technology products and systems is governed by Decree 2002-535 of April 18, 2002, as amended. This decree indicates that:

- The National Information Systems Security Agency prepares certification reports. These reports specify the characteristics of the proposed security objectives. They may include any disclaimer that its editors feel is worth mentioning for safety reasons. They are, at the preference of the sponsors, communicated or not to third parties or made public (article 7) ;
- The certificates issued by the director general of the National Agency for the Security of Information Systems attest that the version of the products or systems submitted for evaluation meets the specified security characteristics. They also certify that the evaluations were carried out in accordance with the standards and regulations in force, with the required competence and impartiality (Article 8).

Certification procedures are available on the website www.ssi.gouv.fr.

TABLE OF CONTENT

1	The product.....	6
1.1	Product presentation	6
1.2	Product description.....	6
1.2.1	Introduction	6
1.2.2	Security services	6
1.2.3	Architecture	6
1.2.4	Product identification.....	6
1.2.5	Lifecycle	6
1.2.6	Configuration evaluated	6
2	The evaluation.....	8
2.1	Evaluation requirements.....	8
2.2	Evaluation work	8
2.3	Cryptographic mechanism analysis following the ANSSI technical requirements.....	8
2.4	Randomness generator analysis	8
3	The certification	9
3.1	Conclusion.....	9
3.2	Usage restrictions.....	9
3.3	Certificate recognition.....	9
3.3.1	European recognition (SOG-IS).....	9
3.3.2	Common Criteria international recognition (CCRA).....	10
ANNEXE A.	Product assessment level	11
ANNEXE B.	Documentary references of the evaluated product	12
ANNEXE C.	References related to certification	13

1 The product

1.1 Product presentation

The product evaluated is « CN Series Encryptor, comprising of the models CN4010/CN4020/CN6010/CN6140/CN9100/CN9120 running software version 5.0.2 » developed by SENETAS. The CN Series is a family of Ethernet network encryptors.

1.2 Product description

1.2.1 Introduction

The security target [ST] defines the product evaluated, its security functionality that has been evaluated and its utilisation environment.

1.2.2 Security services

The main security services offered by the product are described chapter 1.5.3 of the security target [ST].

1.2.3 Architecture

These devices share the same hardware architecture and the same software version (except the FPGA bitstream which differs from model to model).

A detailed description can be found chapter 1.4 of the security target.

1.2.4 Product identification

The TOE version (5.0.2) can be identified on different interfaces:

- On the LCD screen of the TOE ;
- In the command line interface accessible via SSH ;
- By using the Senetas proprietary management software CM7 (via SNMP) ;
- In the system audit logs.

1.2.5 Lifecycle

The lifecycle of the product is presented chapter 1.4.5 of the security target [ST].

1.2.6 Configuration evaluated

As the AES modes CTR and CFB don't offer integrity protection, the evaluation only covers AES-GCM mode.

Thus, the product configurations evaluated are:

- CN4010 (hardware A4010B ; software 5.0.2) in AES-GCM mode ;
- CN4020 (hardware A4020B ; software 5.0.2) in AES-GCM mode ;
- CN6010 (hardware A6010B, A6011B or A6012B ; software 5.0.2) in AES-GCM mode ;
- CN6140 (hardware A6140B, A6141B or A6142B ; software 5.0.2) in AES-GCM mode
 - In 1G single-port configuration,
 - In 1G multi-port configuration,

- In 10G single-port configuration, and
- In 10G multi-port configuration ;

Note: The 10G Multi-port configuration is not considered in this evaluation because it only offers confidentiality without integrity (it does not support AES-GCM mode, it only supports AES-CTR mode);

- CN9100 (hardware A9100B, A9101B or A9102B; software 5.0.2) in mode AES-GCM;
- CN9120 (hardware A9120B, A9121B or A9122B; software 5.0.2) in mode AES-GCM.

2 The evaluation

2.1 Evaluation requirements

The evaluation has been performed according to the Common Criteria version 3.1 revision 5 [CC], and to the evaluation methodology defined in the manual [CEM].

For the assurance components which are not covered by the manual [CEM], some dedicated methods have been used by the evaluation centre and validated by ANSSI.

2.2 Evaluation work

The technical report of evaluation [RTE], given to ANSSI the day of its finalisation by the CESTI (see date in bibliography), details the work done by the centre of evaluation and acknowledges that all evaluation tasks are « **success** ».

2.3 Cryptographic mechanism analysis following the ANSSI technical requirements

The cryptographic mechanisms implemented by the product security functions (see [ST]) have been analysed according to the procedure [CRY/P/01] and the results have been added to the report [RTE].

This analysis has identified some non-conformity with the requirements [ANSSI Crypto]. They have been taken into account in the independent vulnerability analysis performed by the evaluator and have been deemed not to demonstrate any exploitable vulnerability for the targeted attack surface.

The user must refer to [GUIDES] in order to configure the product to be conformed to the requirements [ANSSI Crypto], for the allowed cryptographic mechanisms.

2.4 Randomness generator analysis

The randomness generator used by the TOE has been analysed according to the procedure [CRY/P/01] and the results have been added to the report [RTE].

The independent vulnerability analysis performed by the evaluator did not expose any exploitable vulnerabilities for the targeted attack surface.

3 The certification

3.1 Conclusion

The evaluation has been done according to the actual standards and regulations, with the competence and impartiality required of a licensed evaluation centre. The entire evaluation work realised permits the delivery of the certificate according to the Decree 2002-535.

The certificate attests that the product « CN Series Encryptor, comprising of the models CN4010/CN4020/CN6010/CN6140/CN9100/CN9120 running software version 5.0.2 » under evaluation meets the security requirements specified in the security target [ST] for the level EAL4+ evaluation augmented using the ALC_FLR.3 component.

3.2 Usage restrictions

This certificate covers the product specified in chapter 1.2 of the present certification report.

As mentioned in section 1.2.6, the AES modes CTR and CFB don't offer integrity protection: therefore, the evaluation only covers the AES-GCM mode.

The user must be aware that the security model of the TOE does not define a unique authenticated link between each pair of encryptors. **A single encryptor, if compromised, can therefore compromise all the communications between the other encryptors on the same network** (see chapter 1.4.3.1 of [ST]).

It means for instance that if a user uses a common network to implement two channels with two different actors, those two channels will not be protected from one another by the TOE: one of those actors may use their legitimate access to eavesdrop communications between the user and the other actor.

By design, this threat is not addressed by the TOE; it is therefore up to the user to mitigate it through organizational measures. The user must:

- Ensure that security objectives as defined in [ST] are met, and follow the recommendations defined in [GUIDES], **for all encryptors present on their network;**
- Ensure that encryptor networks are deployed **only between actors that trust each other.**

3.3 Certificate recognition

3.3.1 European recognition (SOG-IS)

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

The SOG-IS European recognition agreement of 2010 allows the recognition, by the agreement signatory countries¹, of the ITSEC and Common Criteria certificates. The European recognition applies, for smart cards and similar devices, up to ITSEC level E6 extended and CC EAL7 when CC dependencies are met. Certificates recognized under this agreement are issued with the following mark:

¹ The list of signatory countries of the SOG-IS agreement is available on the agreement's website: www.sogis.eu.



3.3.2 *Common Criteria international recognition (CCRA)*

This certificate is issued in the CCRA agreement conditions [CCRA].

The agreement « Common Criteria Recognition Arrangement » allows the recognition, by the agreement signatory countries², of the Common Criteria certificates.

The recognition applies up to the assurance components of CC level EAL2 and the family ALC_FLR. Certificates recognized under this agreement are issued with the following mark:



² The list of signatory countries of the CCRA agreement is available on the agreement's website: www.commoncriteriaportal.org.

ANNEXE A. Product assessment level

Class	Family	Component per insurance level							Insurance level retained for this product			
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 4+	Component title		
ADV Development	ADV_ARC		1	1	1	1	1	1	1	1	Security architecture description	
	ADV_FSP	1	2	3	4	5	5	6	4	4	Complete functional specification	
	ADV_IMP				1	1	2	2	1	1	Implementation representation of the TSF	
	ADV_INT					2	3	3				
	ADV_SPM						1	1				
	ADV_TDS		1	2	3	4	5	6	3	3	Basic modular design	
AGD Utilisation guides	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance	
	AGD_PRE	1	1	1	1	1	1	1	1	1	Preparative procedures	
ALC Lifecycle support	ALC_CMC	1	2	3	4	4	5	5	4	4	Production support, acceptance procedures and automation	
	ALC_CMS	1	2	3	4	5	5	5	4	4	Problem tracking CM coverage	
	ALC_DEL		1	1	1	1	1	1	1	1	Delivery procedures	
	ALC_DVS			1	1	1	2	2	1	1	Identification of security measures	
	ALC_FLR									3	3	Systematic flaw remediation
	ALC_LCD			1	1	1	1	2	1	1	1	Developer defined life-cycle model
ALC_TAT				1	2	3	3	1	1	1	Well-defined development tools	
ASE Security target evaluation	ASE_CCL	1	1	1	1	1	1	1	1	1	Conformance claims	
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended components definition	
	ASE_INT	1	1	1	1	1	1	1	1	1	ST introduction	
	ASE_OBJ	1	2	2	2	2	2	2	2	2	Security objectives	
	ASE_REQ	1	2	2	2	2	2	2	2	2	Derived security requirements	
	ASE_SPD		1	1	1	1	1	1	1	1	1	Security problem definition
ASE_TSS	1	1	1	1	1	1	1	1	1	1	TOE summary specification	
ATE Tests	ATE_COV		1	2	2	2	3	3	2	2	2	Analysis of coverage
	ATE_DPT			1	2	3	3	4	3	3	3	Testing: modular design
	ATE_FUN		1	1	1	1	2	2	1	1	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	2	Independent testing: sample
AVA Vulnerabilities assessment	AVA_VAN	1	2	2	3	4	5	5	3	3	3	Focused vulnerability analysis

ANNEXE B. Documentary references of the evaluated product

[ST]	Security Target reference for evaluation : <ul style="list-style-type: none">• Senetas <i>CN Series Security Target, version 1.9</i>, 15th February 2021, SENETAS. For publication requirements, the following security target has been provided and validated for this evaluation :• <i>Senetas CN Series Security Target, version 2.0</i>, 20th May 2021, SENETAS.
[RTE]	<i>Evaluation Technical Report, OPPIDA/CESTI/CNSERIESENCRYPTOR/RTE, version 1.1</i> , 20 th May 2021, OPPIDA.
[GUIDES]	List of product guides : <ul style="list-style-type: none">• Senetas CN Series Encryptor Preparative Procedures (AGD_PRE.1), version 1.8, 21st May 2021, SENETAS ;• Senetas CN Series Encryptor Operational User Guidance (AGD_OPE.1), version 1.8, 21st May 2021, SENETAS.

ANNEXE C. References related to certification

Decree 2002-535 of the 18 th April 2002 amended relating to the assessment and certification of the security offered by information technology products and systems.	
[CER/P/01]	Procedure ANSSI-CC-CER-P-01 Common criteria certification of the security offered by products, information technology systems, sites or protection profiles, ANSSI.
[CRY/P/01]	Procedure ANSSI-CC-CRY-P01 Methods for carrying out cryptographic analyses and evaluations of random number generators, ANSSI.
[CC]	<p><i>Common Criteria for Information Technology Security Evaluation:</i></p> <ul style="list-style-type: none"> - <i>Part 1: Introduction and general model</i>, April 2017, version 3.1, revision 5, reference CCMB-2017-04-001; - <i>Part 2: Security functional components</i>, April 2017, version 3.1, revision 5, reference CCMB-2017-04-002; - <i>Part 3: Security assurance components</i>, April 2017, version 3.1, revision 5, reference CCMB-2017-04-003.
[CEM]	<i>Common Methodology for Information Technology Security Evaluation : Evaluation Methodology</i> , April 2017, version 3.1, revision 5, reference CCMB-2017-04-004.
[CCRA]	<i>Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security</i> , 2 nd July 2014.
[SOG-IS]	<i>Mutual Recognition Agreement of Information Technology Security Evaluation Certificates</i> , version 3.0, 8 th January 2010, Management Committee.
[ANSSI Crypto]	Guide to cryptographic mechanisms - Rules and recommendations concerning the choice and sizing of cryptographic mechanisms, version 2.04 of the 1 st January 2020, see www.ssi.gouv.fr .

* SOG-IS document; under the CCRA recognition agreement, the equivalent CCRA support document applies.