PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2021/31

CNSeries Encryptor CN4010/CN4020/CN6010/CN6140/CN9100/CN9120 version 5.0.2

Paris, le 7 juillet 2021

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

Guillaume POUPARD

[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

AVERTISSEMENT

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

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

Référence du rapport de certification **ANSSI-CC-2021/31**
Nom du produit **CNSeries Encryptor**
Référence/version du produit **CN4010/CN4020/CN6010/CN6140/CN9100/CN9120 version 5.0.2**
Conformité à un profil de protection Sans objet
Critère d'évaluation et version **Critères Communs version 3.1 révision 5**
Niveau d'évaluation **EAL 4 augmenté** ALC_FLR.3
Développeur **SENETAS** 312 Kings Way, South Melbourne Victoria 3205 Australia
Commanditaire **SENETAS** 312 Kings Way, South Melbourne Victoria 3205 Australia
Centre d'évaluation **OPPIDA** 4-6 avenue du vieil étang, Bâtiment B 78180 Montigny le Bretonneux, France
Accords de reconnaissance applicables **CCRA** Ce certificat est reconnu au niveau EAL2. **SOG-IS**

PREFACE

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- l'Agence nationale de la sécurité des systèmes d'information élabore les rapports de certification. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7) ;
- les certificats délivrés par le directeur général de l'Agence nationale de la sécurité des systèmes d'information attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « CNSeries Encryptor, CN4010/CN4020/CN6010/CN6140/CN9100/CN9120 version 5.0.2 » développé par SENETAS. Il s'agit d'une gamme de chiffreurs réseau.

1.2 Description du produit

1.2.1 *Introduction*

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont décrits au 1.5.3 de la cible de sécurité [ST].

1.2.3 *Architecture*

Ces modèles partagent la même architecture matérielle et la même version de logiciel (à l'exception du *bitstream* FPGA qui diffère d'un produit à l'autre).
Une description plus précise se trouve au 1.4 de la cible de sécurité.

1.2.4 *Identification du produit*

La version de la TOE (5.0.2) peut être identifiée sur différentes interfaces :

- sur l'écran LCD de la TOE ;
- sur l'interface en ligne de commande accessible via SSH ;
- en utilisant le service de gestion propriétaire Senetas CM7 (via SNMP) ;
- dans les journaux d'audit système.

1.2.5 *Cycle de vie*

Le cycle de vie du produit est présenté au 1.4.5 de la cible de sécurité [ST].

1.2.6 *Configuration évaluée*

Les modes d'utilisation CTR et CFB n'offrant pas de protection en intégrité, l'évaluation ne porte que sur le mode AES-GCM.

Ainsi, les configurations évaluées du produit sont :

- CN4010 (matériel A4010B ; logiciel 5.0.2) en mode AES-GCM ;
- CN4020 (matériel A4020B ; logiciel 5.0.2) en mode AES-GCM ;
- CN6010 (matériel A6010B, A6011B ou A6012B ; logiciel 5.0.2) en mode AES-GCM ;
- CN6140 (matériel A6140B, A6141B ou A6142B ; logiciel 5.0.2) en mode AES-GCM :
    - en configuration 1G *single-port*,
    - en configuration 1G multi-port,
    - en configuration 10G *single-port*, et

Attention : le mode 10G multi-port n'est pas considéré dans le cadre de cette évaluation car il n'offre que de la confidentialité sans intégrité ;

- CN9100 (matériel A9100B, A9101B ou A9102B ; logiciel 5.0.2) en mode AES-GCM ;
- CN9120 (matériel A9120B, A9121B ou A9122B ; logiciel 5.0.2) en mode AES-GCM.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs version 3.1 révision 5 [CC], et à la méthodologie d'évaluation définie dans le manuel [CEM].

Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

2.2 Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le jour de sa finalisation par le CESTI (voir date en bibliographie), détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3 Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [ST]) ont fait l'objet d'une analyse conformément à la procédure [CRY/P/01] et les résultats ont été consignés dans le rapport [RTE].

Cette analyse a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Elles ont été prises en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le potentiel d'attaque visé.

L'utilisateur doit se référer aux [GUIDES] afin de configurer le produit de manière conforme au référentiel [ANSSI Crypto], pour les mécanismes cryptographiques qui le permettent.

2.4 Analyse du générateur d'aléa

Le générateur d'aléa utilisé par la TOE a fait l'objet d'une analyse conformément à la procédure [CRY/P/01] et les résultats ont été consignés dans le rapport [RTE].

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le potentiel d'attaque visé.

3 La certification

3.1 Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit « CNSeries Encryptor, CN4010/CN4020/CN6010/CN6140/CN9100/CN9120 version 5.0.2 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté du composant ALC_FLR.3.

3.2 Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

Comme précisé au paragraphe 1.2.6, les modes d'utilisation CTR et CFB n'offrent pas de protection en intégrité. Pour cette raison, l'évaluation ne porte que sur le mode AES-GCM.

L'utilisateur doit par ailleurs être conscient que le modèle de sécurité de la TOE ne définit pas de lien authentifié unique entre chaque paire de chiffreurs. **Un seul chiffreur compromis au sein du réseau a la capacité de compromettre les communications entre tous les chiffreurs du réseau** (voir chapitre 1.4.3.1 de [ST]).

Cela signifie par exemple que si l'utilisateur déploie un réseau commun pour ouvrir deux canaux vers des acteurs distincts, ces canaux ne seront pas protégés l'un de l'autre par la TOE : l'un de ces acteurs peut en effet utiliser son accès légitime pour espionner les communications entre l'utilisateur et l'autre acteur.

Ce risque n'étant, par construction, pas couvert par la TOE, il est de la responsabilité de l'utilisateur de le mitiger par des mesures organisationnelles. Il est donc impératif que l'utilisateur:

- s'assure du respect des objectifs de sécurité sur l'environnement d'exploitation tels que spécifiés dans la cible de sécurité [ST], et suive les recommandations se trouvant dans les guides fournis [GUIDES], **pour tous les chiffreurs appartenant au réseau** ;
- s'assure que les réseaux de chiffreurs ne sont établis **qu'entre des parties se faisant mutuellement confiance**.

3.3 Reconnaissance du certificat

3.3.1 *Reconnaissance européenne (SOG-IS)*

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

3.3.2 *Reconnaissance internationale critères communs (CCRA)*

Ce certificat est émis dans les conditions de l'accord du CCRA [CCRA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2] , des certificats Critères Communs.

La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL2 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[2] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

ANNEXE A. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 4+	Intitulé du composant
ADV Développement	ADV_ARC		1	1	1	1	1	1	**1**	*Security architecture description*
	ADV_FSP	1	2	3	4	5	5	6	**4**	*Complete functional specification*
	ADV_IMP				1	1	2	2	**1**	*Implementation representation of the TSF*
	ADV_INT					2	3	3		
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	**3**	*Basic modular design*
AGD Guides d'utilisation	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 au cycle de vie	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	**4**	*Problem tracking CM coverage*
	ALC_DEL		1	1	1	1	1	1	**1**	*Delivery procedures*
	ALC_DVS			1	1	1	2	2	**1**	*Identification of security measures*
	ALC_FLR								**3**	*Systematic flaw remediation*
	ALC_LCD			1	1	1	1	2	**1**	*Developer defined life-cycle model*
	ALC_TAT				1	2	3	3	**1**	*Well-defined development tools*
ASE Evaluation de la cible de sécurité	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	2	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 Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	**3**	*Focused vulnerability analysis*

ANNEXE B. Références documentaires du produits évalué

[ST]	Cible de sécurité de référence pour l'évaluation : • Senetas *CN Series Security Target, version 1.9*, 15 février 2021, SENETAS. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : • *Senetas CN* Series *Security Target, version 2.0*, 20 mai 2021, SENETAS.
[RTE]	*Evaluation Technical Report, OPPIDA/CESTI/CNSERIESENCRYPTOR/RTE, version 1.1*, 20 mai 2021, OPPIDA.
[GUIDES]	Liste des guides du produit : • Senetas CN Series Encryptor Preparative Procedures (AGD_PRE.1), version 1.8, 21 mai 2021, SENETAS ; • Senetas CN Series Encryptor Operational User Guidance (AGD_OPE.1), version 1.8, 21 mai 2021, SENETAS.

ANNEXE C. Références liées à la certification

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 ANSSI-CC-CER-P-01 Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, ANSSI.
[CRY/P/01]	Procédure ANSSI-CC-CRY-P01 Modalités pour la realisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, ANSSI.
[CC]	*Common Criteria for Information Technology Security Evaluation:* - *Part 1: Introduction and general model*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001; - *Part 2: Security functional components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002; - *Part 3: Security assurance components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	*Common Methodology for Information Technology Security Evaluation : Evaluation Methodology*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[CCRA]	*Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security*, 2 juillet 2014.
[SOG-IS]	*Mutual Recognition Agreement of Information Technology Security Evaluation Certificates*, version 3.0, 8 janvier 2010, Management Committee.
[ANSSI Crypto]	Guide des mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.04 du 1 janvier 2020, voir www.ssi.gouv.fr.