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

Rapport de certification ANSSI-CC-2017/57

Logiciel embarqué dans le multiplexeur 9500 Microwave Packet Radio, version 07.01.0B avec sa carte CorEvo, version 34.09.00

Paris, le 05 octobre 2017

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ TI CERTIFICATION

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-2017/57

Nom du produit

Logiciel embarqué dans le multiplexeur 9500 Microwave Packet Radio, version 07.01.0B avec sa carte CorEvo, version 34.09.00

Référence/version du produit

Version 07.01.0B pour le multiplexeur version 34.09.00 pour la carte CorEvo

Conformité à un profil de protection

Aucune

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL 3 augmenté
ALC_FLR.3, AVA_VAN.3

Développeur(s)

NOKIA

Route de villejust, 91602 Nozay, France

Commanditaire

NOKIA

Route de villejust, 91602 Nozay, France

Centre d'évaluation

Amossys

4 bis allée du bâtiment, 35000 Rennes, France

Accords de reconnaissance applicables

CCRA

Ce certificat est reconnu au niveau EAL2 augmenté d'ALC_FLR.3.

SOG-IS

Ce certificat est reconnu au niveau EAL3 augmenté d'ALC_FLR.3.

Préface

La certification

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 Premier ministre 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 matières

1. LE PRODUIT 6

1.1. PRESENTATION DU PRODUIT 6
1.2. DESCRIPTION DU PRODUIT 6
1.2.1. Introduction 6
1.2.2. Services de sécurité 6
1.2.3. Architecture 6
1.2.4. Identification du produit 8
1.2.5. Cycle de vie 8
1.2.6. Configuration évaluée 9

2. L'EVALUATION 10

2.1. REFERENTIELS D'EVALUATION 10
2.2. TRAVAUX D'EVALUATION 10
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L'ANSSI 10
2.4. ANALYSE DU GENERATEUR D'ALEAS 10

3. LA CERTIFICATION 11

3.1. CONCLUSION 11
3.2. RESTRICTIONS D'USAGE 11
3.3. RECONNAISSANCE DU CERTIFICAT 12
3.3.1. Reconnaissance européenne (SOG-IS) 12
3.3.2. Reconnaissance internationale critères communs (CCRA) 12

ANNEXE 1. NIVEAU D'EVALUATION DU PRODUIT 13

ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE 14

ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION 15

1. Le produit

1.1. Présentation du produit

Le produit évalué est constitué du « logiciel embarqué dans le multiplexeur 9500 Microwave Packet Radio, version 07.01.0B avec sa carte CorEvo, version 34.09.00 » développé par *NOKIA*. Le produit est un multiplexeur pour les faisceaux hertziens numériques, il supporte les technologies PDH[1], SDH[2] et Ethernet afin de transformer le multiplexage temporel (TDM[3]) en « paquets Ethernet ». Le produit est une plateforme modulaire générique Ethernet (niveau 2+) adaptée pour la diffusion / réception sécurisée de données par voie hertzienne tels les réseaux 2G, 3G, 4G, HSDPA[4] et WiMAX vers les réseaux « Metro Ethernet[5] ».

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 :
- le chiffrement des paquets Ethernet au niveau de la couche 1 ;
- sa gestion sécurisée locale ou distante ;
- l'identification et l'authentification des utilisateurs ;
- la journalisation des *logs* ;
- la redondance.

1.2.3. Architecture

Le produit contient :
- la carte de chiffrement / déchiffrement installée dans un module MPT-HQAM situé à l'arrière de l'antenne (*Short Haul*) ou sur la carte MPT-HLS (*Long Haul*). Le chiffrement / déchiffrement AES-CTR 256 est effectué par un FPGA[6] ;
- le contrôleur d'équipement nommé CorEVo contenant un microSD[7]afin de sécuriser les échanges avec les éléments interfacés avec la TOE ;
- le *Microwave Service Switch* (MSS) connecté à la carte de chiffrement / déchiffrement via un câble Gigabit Ethernet ;

[1] *Plesiochronous Digital Hierarchy*.
[2] *Synchronous Digital Hierarchy.*
[3] *Time-Division Multiplexing.*
[4] *High Speed Downlink Packet Access* (3.5G, 3G+, H, turbo 3G) est un protocole de communication pour la téléphonie mobile.
[5] Réseau de télécommunications à haut débit basé sur le standard Ethernet qui permet de couvrir de larges zones géographiques.
[6] *Field Programmable Gate Array*.
[7] *Micro Secure Digital Card*.

- le *Microwave Packet Transport* (MPT) qui est un émetteur / récepteur de radiodiffusion en mode *Ethernet packets*.

Suivant les besoins du client final, deux architectures différentes (*Short Haul et Long Haul*) sont possibles :

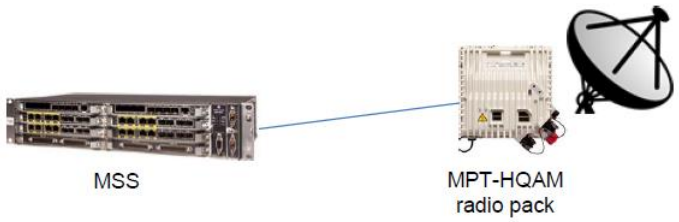

Figure 1-9500 Microwave Packet Radio dans une architecture *Short Haul*.

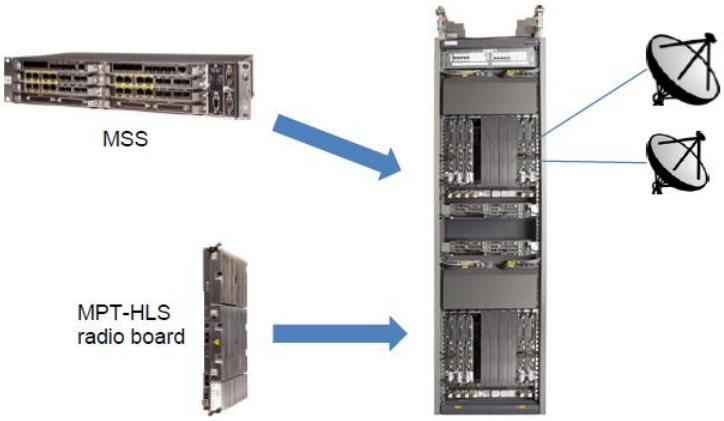

Figure 2 -9500 Microwave Packet Radio dans une architecture *Long Haul*.

Le périmètre physique de la TOE est le suivant :

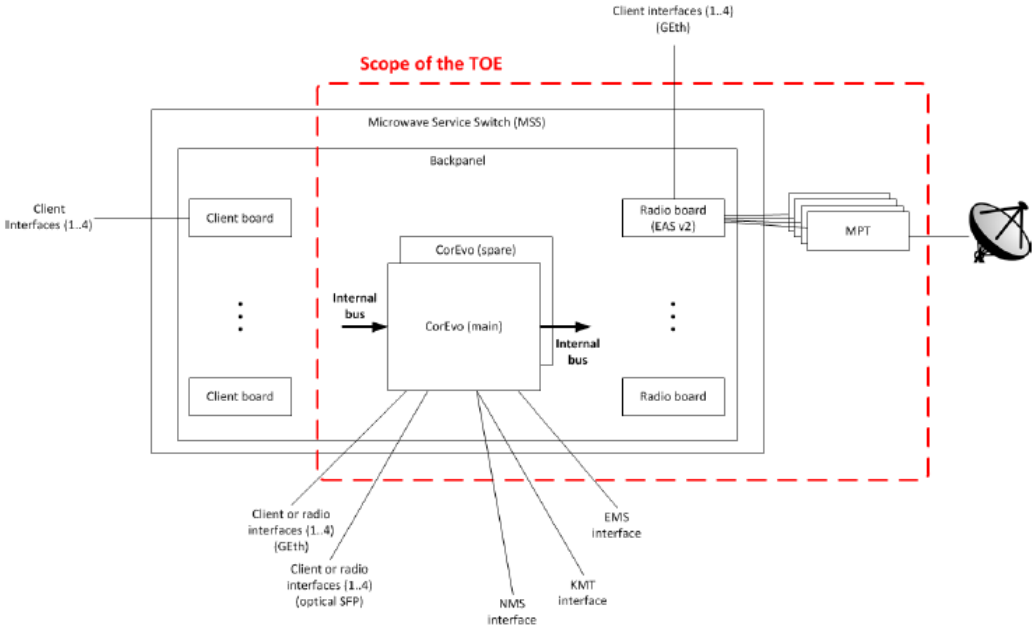

Figure 3 – Périmètre physique de la TOE.

En plus de son interface avec la ou les antennes, la TOE dispose :
- d'une interface sécurisée d'administration à distance qui se connecte soit au système d'administration du réseau, soit à un outil de gestion de clés ;
- d'une interface de gestion locale ;
- de 1 à 23 interfaces pour des équipements « client » en fonction des configurations.

Le périmètre logique comprend l'intégralité de la TOE à l'exception :
- des protocoles SSH, SSL/TLS et SNMP qui sont actifs et peuvent être utilisés pour gérer la TOE. La cryptographie utilisée pour ces protocoles est hors du périmètre de l'évaluation ;
- le support TELNET ;
- le protocole d'authentification TACACS+ ;
- la gestion sécurisée locale ou distante.

Deux exemples d'architecture système sont donnés au paragraphe 1.4.2 de la cible de sécurité [ST].

1.2.4. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version certifiée du produit est identifiable de la manière suivante :
- pour l'administrateur, en utilisant la procédure décrite à la page 13 du guide d'installation « Certified Secure Mode » [GUIDE_ INSTALL]. L'administrateur a la possibilité de vérifier les *hash* obtenus avec ceux correspondant au produit certifié dont les valeurs sont indiquées à la page 14 du même guide ;
- pour l'utilisateur final, en utilisant les commandes décrites à la page 29 du guide utilisateur [GUIDE_UTIL].

1.2.5. Cycle de vie

Le cycle de vie du produit est le suivant :

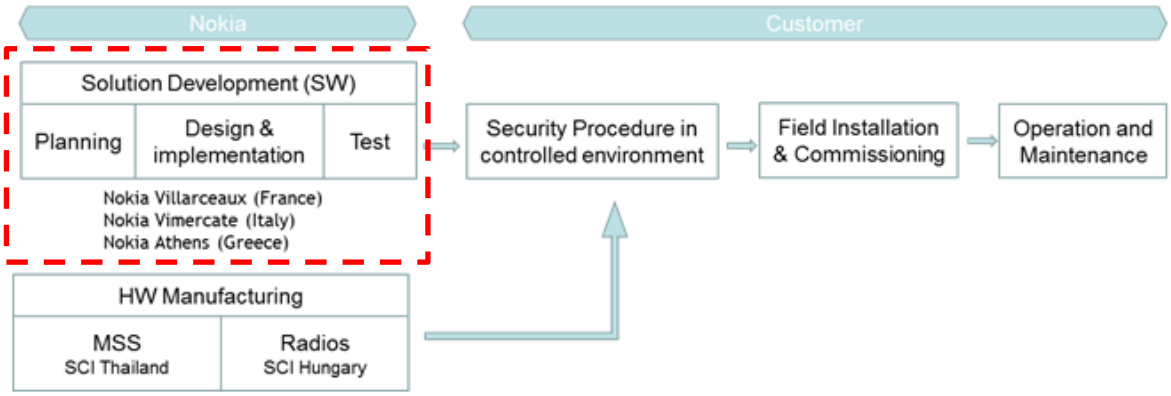

Figure 4 : Développement de la TOE.

Le produit a été développé sur les trois sites de *NOKIA* (encadré en rouge sur la figure ci-dessus). Ceux-ci ont été audités dans le cadre de cette évaluation. A noter que les activités de

développement de la cryptographie sont essentiellement assurées par le site de *NOKIA VILLARCEAUX*.

Noms des sites	Adresses des sites
Centre de Paris / Saclay (Villarceaux)	1, route de Villejust,91620 Nozay France
Via Energy Park	14 - 20871 Vimercate,MB Italy
AREVA building	14th km National Rd. Athinon Lamias, 14564 Nea Kifisia, Athens Greece

Pour l'évaluation, les rôles considérés sont :

- l'administrateur qui fournit les accès à tous les services nécessaires à l'installation initiale et à la gestion des éléments du réseau ;
- l'officier crypto qui administre les différentes clés cryptographiques. Il délivre tous les services nécessaires pour la gestion des fonctions et des paramètres de cryptographie.

1.2.6. Configuration évaluée

Le certificat porte sur « le logiciel embarqué dans le multiplexeur 9500 Microwave Packet Radio, version 07.01.0B avec sa carte CorEvo, version 34.09.00 ».

Les composants du système qui n'ont pas fait l'objet de l'évaluation (hors périmètre) sont les suivants :

- la plateforme matérielle du produit ;
- l'EMS[1] qui permet d'administrer et d'opérer la TOE via une interface d'administration locale ;
- le KMT[2] qui est entre autres, chargé de générer et distribuer les clés de session utilisées par la TOE ;
- le NMS[3] qui permet d'administrer et d'opérer la TOE via une interface d'administration distante.

[1] *Equipment Management System*.
[2] *Key Management Tool*.
[3] *Network Management System*.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [CC], et à la méthodologie d'évaluation définie dans le manuel CEM [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 14 septembre 2017, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

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

La cotation des mécanismes cryptographiques a été réalisée conformément au référentiel technique de l'ANSSI [REF]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Les mécanismes analysés sont conformes aux exigences des référentiels cryptographiques de l'ANSSI. Les résultats ont été pris 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 niveau AVA_VAN.3 visé.

Dans le cadre du processus de qualification standard, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI [EXP-CRY]. Ces résultats ont été pris 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 niveau AVA_VAN.3 visé.

2.4. Analyse du générateur d'aléas

Le produit ne comporte pas de générateur d'aléas entrant dans le périmètre d'évaluation.

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 logiciel embarqué dans le multiplexeur 9500 Microwave Packet Radio, version 07.01.0B avec sa carte CorEvo, version 34.09.00 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 3 augmenté des composants ALC_FLR.3 et AVA_VAN.3.

3.2. Restrictions d'usage

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

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations mentionnées dans les guides fournis [GUIDE_INSTALL] et [GUIDE_UTIL]. L'utilisateur devra notamment :

- paramétrer le multiplexeur 9500 MSS pour qu'il puisse fonctionner en *secure mode* ;
- s'assurer que les clés générées répondent aux recommandations de l'ANSSI ;
- localiser le produit dans une zone sécurisée afin de prévenir toute manipulation non autorisée ;
- s'assurer que l'usage de la TOE respecte les hypothèses formulées dans la [ST] notamment A_PROTECTION et A_MNGT_EQPT_PROTECTION ;
- s'assurer que les objectifs de sécurité pour l'environnement de la TOE sont remplis notamment OE_MNGT_NETWORK ;
- s'assurer que les mots de passe respectent les règles préconisées à la page 67 du guide d'installation « Certified Secure Mode » [GUIDE_ INSTALL].

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 jusqu'au niveau ITSEC E3 Elémentaire et CC EAL4 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

3.3.2. Reconnaissance internationale critères communs (CCRA)

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

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 :

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

Annexe 1. 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 3+	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**	**3**	Functional specification with complete summary
	ADV_IMP				**1**	1	**2**	2		
	ADV_INT					**2**	**3**	3		
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**2**	Architectural 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	**3**	Authorisation controls
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**3**	Implementation representation 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		
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**	1	**3**	3	**4**	**1**	Testing: basic 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 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Security Target 9500 Microwave Packet Radio, reference 3DB19413AAAADTZZA, version 0.16, 19 septembre 2017, *NOKIA*.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical report, référence ETR-LAPLACE-1.01, 14 septembre 2017, *AMOSSYS*.
[EXP-CRY]	Expertise des mécanismes cryptographiques, référence CRY-LAPLACE-1.01, 1er août 2017, *AMOSSYS*.
[ANA-CRY]	Expertise des mécanismes cryptographiques, référence CRY-LAPLACE-1.01, 1er août 2017, *AMOSSYS*.
[CONF]	Liste de configuration du produit : - ALC documentation, NOKIA 9500 MPR, référence 3DB19413AAAADPZZA, version 08, 5 septembre 2017, *NOKIA*.
[GUIDE_ INSTALL]	Guides d'installation du produit : - Certified Secure Mode – Software Erase and Reload for radios and µSD manual, reference 3DB 19419SDAATQZZA, version 1, avril 2017, *NOKIA* ; - Hardware Installation and Replacement Manual, référence 3DB19285ADAATQZZA, version 1, *NOKIA*.
[GUIDE_ UTIL]	Guide d'utilisation du produit : - Certified Secure Mode – User Manuel, référence 3DB19420SDAATQZZA, version 1, septembre 2017, *NOKIA*.

Annexe 3. 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.
[CC]	Common Criteria for Information Technology Security Evaluation : - Part 1: Introduction and general model, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001; - Part 2: Security functional components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002; - Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[CC RA]	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.
[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), voir www.ssi.gouv.fr.
	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 2.00 du 8 juin 2012 annexée au Référentiel général de sécurité (RGS_B2), voir www.ssi.gouv.fr.
	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité (RGS_B3), voir www.ssi.gouv.fr.