



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-2017/58

**Logiciel embarqué dans les équipements
NOKIA 1830 Photonic Service Switch en
configuration PSS/32 et PSS/8 version 9.1.0,
build 14.28-40**

Paris, le 9 octobre 2017

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

Guillaume POUPARD
[ORIGINAL SIGNE]



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 présumées 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

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification	ANSSI-CC-2017/58				
Nom du produit	Logiciel embarqué dans les équipements NOKIA 1830 Photonic Service Switch en configuration PSS/32 et PSS/8				
Référence/version du produit	Version 9.1.0, build 14.28-40				
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	<table border="0"><tr><td style="text-align: center;">CCRA </td><td style="text-align: center;">SOG-IS </td></tr><tr><td style="text-align: center;">Le produit est reconnu au niveau EAL2 augmenté d'ALC_FLR.3.</td><td style="text-align: center;">Le produit est reconnu au niveau EAL3 augmenté d'ALC_FLR.3</td></tr></table>	CCRA 	SOG-IS 	Le produit est reconnu au niveau EAL2 augmenté d'ALC_FLR.3.	Le produit est reconnu au niveau EAL3 augmenté d'ALC_FLR.3
CCRA 	SOG-IS 				
Le produit est reconnu au niveau EAL2 augmenté d'ALC_FLR.3.	Le produit 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	7
1.2.5. Cycle de vie	7
1.2.6. Configuration évaluée	8
2. L’EVALUATION	9
2.1. REFERENTIELS D’EVALUATION	9
2.2. TRAVAUX D’EVALUATION	9
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI	9
2.4. ANALYSE DU GENERATEUR D’ALEAS	9
3. LA CERTIFICATION	10
3.1. CONCLUSION	10
3.2. RESTRICTIONS D’USAGE	10
3.3. RECONNAISSANCE DU CERTIFICAT	11
3.3.1. Reconnaissance européenne (SOG-IS)	11
3.3.2. Reconnaissance internationale critères communs (CCRA)	11
ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT	12
ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	13
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 les équipements NOKIA 1830 Photonic Service Switch en configuration PSS/32 et PSS/8 version 9.1.0, build 14.28-40 » développé par *NOKIA*. Le produit 1830 PSS¹ est une plateforme DWDM² évolutive qui permet d'agréger différents protocoles tels que *fibres channel*³, *Ethernet* ou autres.

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* ;
- son autotest ;
- la gestion des alarmes.

1.2.3. Architecture

Le produit contient :

- la carte 11QPEN4 (*Quad Port Encryption Transponder*) permettant d'effectuer le chiffrement AES-CTR 256 à partir d'un FPGA⁴ ;
- le contrôleur d'équipement contenant un microSD⁵ afin de sécuriser les échanges avec les éléments interfacés avec la TOE ;
- la carte 11DPM12 (*Multiplexer*) qui n'implémente pas de fonctions de sécurité mais qui permet de réaliser les fonctions de multiplexage de différents protocoles.

¹ *Photonic Service Switch*.

² *Dense Wavelength Division Multiplexing* est une technologie de multiplexage optique utilisée pour augmenter la largeur de bande sur une même fibre optique en multiplexant simultanément plusieurs signaux de longueur d'onde différente.

³ Protocole défini par la norme ANSI X3T11 pour le haut débit (Gigabit).

⁴ *Field programmable Gate Array*.

⁵ *Micro Secure Digital Card*.



La gamme 1830 PSS se décline en deux produits, 1830PSS-8 et 1830PSS-32 suivant le nombre de cartes électroniques admissibles dans le *rack*. Le 1830 PSS est donc commercialisé dans deux châssis différents :

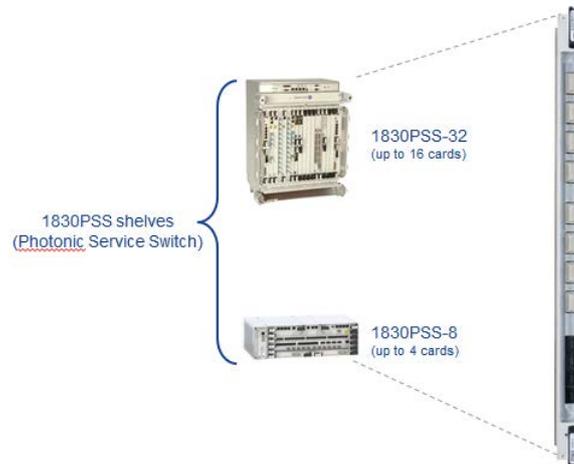


Figure 1 : Gamme de produits

Les périmètres physique et logique sont décrits au paragraphe 1.5 de la [ST].

1.2.4. Identification du produit

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

La version évaluée du produit peut être vérifiée à partir de son empreinte MD5 ou SHA 256 en respectant la procédure décrite au paragraphe 18 du guide « 1830 Photonic Service Switch (PSS) Release 9.1.0 - Common Criteria User Guide » (voir [GUIDES]).

1.2.5. Cycle de vie

Le produit a été développé sur les trois sites mentionnés ci-après. Ceux-ci ont tous été audités dans le cadre de cette évaluation.

Noms des sites	Adresses des sites
Nokia - Ottawa, Canada	600 March Road, Ottawa, Ontario CANADA K2K 2T6
Nokia Murray Hills	600-700 Mountain Avenue, Murray Hill, NJ 07974 USA
Flextronic Manufacturing S.R.I.	Strada al Monte d'Oro 14, 34147 Trieste (TS), ITALIE

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 les équipements NOKIA 1830 Photonic Service Switch en configuration PSS/32 et PSS/8 version 9.1.0, build 14.28-40 ».

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'EMS¹ qui permet d'administrer et d'opérer la TOE via une interface d'administration locale ;
- le KMT² qui est entre autres, chargé de générer et distribuer les clés de session utilisées par la TOE ;
- le NMS³ 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 25 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 les équipements NOKIA 1830 Photonic Service Switch en configuration PSS/32 et PSS/8 version 9.1.0, build 14.28-40 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL3 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 se trouvant dans les guides fournis (voir [GUIDES]).

L'utilisateur devra notamment :

- 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, A_MNGT_NETWORK, A_ADMIN et A_MNGT_EQPT_PROTECTION ;
- s'assurer que les mots de passe respectent les règles préconisées dans les [GUIDES].

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'accord¹, 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 signataires², 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	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	3	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	2	Architectural design
AGD Guides d'utilisation	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 Support au cycle de vie	ALC_CMC	1	2	3	4	4	5	5	3	3	Authorisation controls
	ALC_CMS	1	2	3	4	5	5	5	3	3	Implementation representation 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	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	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	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	2	2	Analysis of coverage
	ATE_DPT			1	2	3	3	4	1	1	Testing : basic design
	ATE_FUN		1	1	1	1	2	2	1	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	3	3	Focused vulnerability analysis



Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : <ul style="list-style-type: none">- Nokia 1830 Photonic Service Switch, version 0.24, 27 septembre 2017, <i>NOKIA</i>.
[RTE]	Rapport technique d'évaluation : <ul style="list-style-type: none">- Evaluation Technical Report, référence ETR-ARAGO-1.01, version 1.01, 25 septembre 2017, <i>AMOSSYS</i>.
[EXP-CRY]	Expertise des mécanismes cryptographiques, référence CRY-ARAGO-1.00, version 1.00, 31 juillet 2017, <i>AMOSSYS</i> .
[ANA-CRY]	Expertise des mécanismes cryptographiques, référence CRY-ARAGO-1.00, version 1.00, 31 juillet 2017, <i>AMOSSYS</i> .
[CONF]	Liste de configuration du produit : <ul style="list-style-type: none">- Nokia 1830 PSS R9.1.0 Life-Cycle Support Documentation, version 1.1, 22 septembre 2017, <i>NOKIA</i>.- Nokia ANSSI SW 1830PSSECE-9.1-0 rpms checksum, référence 3KC-69624-AAAA, version 1.03, 8 septembre 2017, <i>NOKIA</i>.

[GUIDES]	<p>Guide d'installation du produit :</p> <ul style="list-style-type: none">1830 Photonic Service Switch 8 (PSS-8) Release 9.1 Installation and System Turn-Up Guide, référence 8DG-63269-JBAA-SLZZA, version 1, février 2017, <i>NOKIA</i>.- 1830 Photonic Service Switch 16/32 (PSS-16/PSS-32) Release 9.1 - Installation and System Turn-Up Guide, référence 8DG-63269-JBAA-TJZZA, version 1, février 2017, <i>NOKIA</i>.- 1830 Security Management Server Release 1.1 – Installation Guide, référence 3KC-68205-BBAA-TIZZA, version 1, mars 2017, <i>NOKIA</i>.- 1830 Photonic Service Switch (PSS) Release 9.1 – User Provisioning Guide, référence 8DG-63269-JBAA-TCZZA, version 2, février 2017, <i>NOKIA</i>. <p>Guide d'administration du produit :</p> <ul style="list-style-type: none">- 1830 Photonic Service Switch (PSS) Release 9.1 - Command Line Interface Guide, référence 8DG-63269-JBAA-THZZA, version 1, février 2017, <i>NOKIA</i>.- 1830 Photonic Service Switch 832 (PSS-8PSS-32) Release 9.1.0 ECE Customer Release Notes, référence 3KC-69632-AAAA, version 1, mars 2017, <i>NOKIA</i>.- 1830 PSS Release 9.1 - Maintenance and Trouble-Clearing Guide, référence 8DG-63269-JBAA-TMZZA, version 3, février 2017, <i>NOKIA</i>.- 1830 Photonic Service Switch (PSS) Release 9.1.0 - Common Criteria User Guide, référence 8DG-63269-JBAA-TSZZA, version 3, septembre 2017, <i>NOKIA</i>.- 1830 Security Management Server Release 1.1 – User Guide, référence 3KC-68205-BBAA-TVZZA, version 2, septembre 2017, <i>NOKIA</i>.- 1830 Security Management Server Release 1.1 – Administrator Guide, référence 3KC-68205-BBAA-TUZZA, version 2, septembre 2017, <i>NOKIA</i>.- 1830 Security Management Server Release 1.1 – Customer Release Notes, référence 3KC-68214-AAAA, version 1, mars 2017, <i>NOKIA</i>.- 1830 Photonic Service Switch (PSS) 9.1 - Quick Reference Guide, référence 8DG-63269-JBAA-TNZZA, version 1, février 2017, <i>NOKIA</i>.
----------	---



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 .