Nokia 1830 Photonic Service Switch (PSS) & Nokia 1830 Photonic Service Interconnect- Line (PSI-L)

FIPS 140-3 Non-Proprietary Security Policy
FIPS Security Level: 1
Document Version: 1.3 Last saved October 28, 2024 11:20

Table of Contents

List of Tables

List of Figures

Security Policy
October 28, 2024
Copyright 2021-2023 © Nokia
This document may be freely distributed whole and intact including this complete copyright notice
1.2
Page 4 of 65

Security Policy
October 28, 2024
Copyright 2021-2023 © Nokia
This document may be freely distributed whole and intact including this complete copyright notice
1.2
Page 5 of 65

1   General

This document describes the non-proprietary Cryptographic Module Security Policy for the Nokia 1830 Photonic Service Switch (PSS) & Nokia 1830 Photonic Service Interconnect- Line (PSI-L) for multi-shelf configurations. These are referenced in the document as PSS and PSI-8L.

This security policy provides the details for configuring and running these products in a FIPS-140-3 mode of operation and describes how the module meets the level 1 requirements of FIPS 140-3. Please see the references section for a full list of FIPS 140-3 requirements.

The security level of the individual areas is shown in the table below.

ISO/IEC 24759 Section 6.[Number Below]	FIPS 140-3 Section Title	Security Level
1	General	1
2	Cryptographic module specification	1
3	Cryptographic module interfaces	2
4	Roles, services, and authentication	3
5	Software/Firmware security	2
6	Operational environment	2
7	Physical security	1
8	Non-invasive security	N/A
9	Sensitive security parameter management	2
10	Self-tests	2
11	Life-cycle assurance	2
12	Mitigation of other attacks	N/A

Table 1 - Security Levels

2 Cryptographic module specification

For the purposes of FIPS 140-3, the 1830 is designated as a multi-chip standalone hardware cryptographic module.

2.1 Tested Platforms

The following platforms were tested for running the module in approved mode. They all share the same CPU, the Marvell MV78460, which does not contain a Processor Algorithm Accelerator (PAA).
Use of circuit packs not tested under this validation will invalidate the FIPS certification.

2.1.1 1830 PSS-32

Model	Hardware	Firmware Version	Distinguishing Features
1830 PSS-32	Chassis - WOM4V10GRA / 8DG59319AB	n/a	Card Holder
	32EC2 - 8DG63979AA	1830PSS ECN R23.3	Equipment Controller Card
	11QPEN4 - 8DG60996AA		10G Interface Card
	8P20 - 3KC49240AA		10G Interface Card
	S13X100E - 8DG63988AA		100G Interface Card
	Filler Card - 8DG59418AA	n/a	Empty Slot Blank
	Security Label Kit - 8DG-6509-AAAA	n/a	Tamper Labels

Table 2 – PSS-32 Cryptographic Module Test Configuration

2.1.2 1830 PSS-16II

Model	Hardware	Firmware Version	Distinguishing Features
1830 PSS 16II	Chassis - WOMR300BRA / 3KC48960AC	n/a	Card Holder
	32EC2 - 8DG63979AA	1830PSS ECN R23.3	Equipment Controller Card
	11QPEN4 - 8DG60996AA		10G Interface Card
	8P20 - 3KC49240AA		10G Interface Card
	S13X100E - 8DG63988AA		100G Interface Card
	Filler Card - 8DG59418AA	n/a	Empty Slot Blank
	Security Label Kit - 8DG-6509-AAAA	n/a	Tamper Labels

Table 3 - PSS-16II Cryptographic Module Test Configuration

Security Policy
October 28, 2024

Copyright 2021-2023 © Nokia

This document may be freely distributed whole and intact including this complete copyright notice

1.2

Page 8 of 65

2.1.3   1830 PSS-8

Model	Hardware	Firmware Version	Distinguishing Features
1830 PSS-8	Chassis - WOMPU00CRA / 3KC48901AA	n/a	Card Holder
	8EC2 - 3KC48820AA	1830PSS ECN R23.3	Equipment Controller Card
	11QPEN4 - 8DG60996AA		10G Interface Card
	8P20 - 3KC49240AA		10G Interface Card
	S13X100E - 8DG63988AA		100G Interface Card
	Filler Card - 8DG59418AA	n/a	Empty Slot Blank
	Security Label Kit - 8DG-6509-AAAA	n/a	Tamper Labels

Table 4 - PSS-8 Cryptographic Module Test Configuration

2.1.4   1830 PSS-24x

Model	Hardware	Firmware Version	Distinguishing Features
1830 PSS-24x	Chassis - WOMP410CRB / 3KC50378AA	n/a	Card Holder
	CEC2 - 3KC50335AA	1830PSS ECN R23.3	Equipment Controller Card
	MFC24X - 3KC50330AA		Multi-Function Card
	2UC400E - 3KC60522AA		100G Interface Card
	Filler Card – 3KC59819AC	n/a	Empty Slot Blank
	Security Label Kit - 8DG-6509-AAAA	n/a	Tamper Labels

Table 5 - PSS-24x Cryptographic Module Test Configuration

2.1.5   1830 PSS-8x

Model	Hardware	Firmware Version	Distinguishing Features
1830 PSS-8x	Chassis - 3TD00071AA	n/a	Card Holder
	XCEC8 – 3TD00030AA	1830PSS ECN R23.3	Equipment Controller Card
	XMFC - 3TD00014AA		Multi-Function Card
	Filler Card – 3TD00123AA	n/a	Empty Slot Blank
	Security Label Kit - 8DG6509AAAA	n/a	Tamper Labels

Table 6 – PSS-8x Cryptographic Module Test Configuration

2.1.6   1830 PSI-8L

Model	Hardware	Firmware Version	Distinguishing Features
1830 PSI-8L	Chassis - 3KC90291AA	n/a	Card Holder
	MEC2L - 3KC81775AC	1830PSS ECN R23.3	Equipment Controller Card
	PSILMFC - 3KC90213AA		Multi-Function Card

Security Policy
October 28, 2024

Copyright 2021-2023 © Nokia
This document may be freely distributed whole and intact including this complete copyright notice

1.2
Page 9 of 65

| | Filler Card - 8DG59418AA | | Empty Slot Blank |
| | Security Label Kit – 8DG-6509-AAAA | n/a | Tamper Labels |

Table 7 - PSI-8L Cryptographic Module Test Configuration

2.2 Algorithms
Nokia PSS-32/16II/8/24x PSI-8L SNMP-Engine

CAVP Cert.	Algorithm and Standard	Mode/Method	Description / Key Size / Key Strength	Use / Function
A2502	AES [FIPS 197] [SP 800-38A]	CFB128	Key Length: 256 bits	Symmetric Encryption and Decryption
A2502	HMAC [FIPS 198-1]	SHA-1, SHA2-256	Key Length: 160 bits, 256 bits	Keyed Hash
A2502	CVL [SP 800-135 Rev 1]	SNMP KDF Note: The SNMP protocols have not been reviewed or tested by the CAVP and CMVP	-	Key Derivation
A2502	KTS [SP 800-38F Rev 1]	SP 800-38A, FIPS 198-1, and SP 800-38F. KTS (key wrapping and unwrapping) per IG D.G.	Key Length: 256 bits Key Strength: 256 bits	Key establishment methodology provides 256 bits of encryption strength)
A2502	SHS [FIPS 180-4]	SHA-1, SHA-256	-	Message Digest

Table 8 - Approved Algorithms (Nokia SNMP-Engine)

The use of truncated HMAC-SHA-1-96 in SNMP protocol is compliant with IG.C.D.

Nokia openSSL

CAVP Cert.	Algorithm and Standard	Mode/Method	Description / Key Size / Key Strength	Use / Function
A3369	AES [FIPS 197] [SP 800-38A]	CBC, CTR	Key length: 128, 256 bits	Symmetric Encryption and Decryption
A3369	AES [FIPS 197] [SP 800-38A]	ECB	Key Length: 128 bits	Symmetric Encryption and Decryption Self-Test only
A3369	AES [SP 800-38D]	GCM	Key length: 128, 256 bits	Symmetric Encryption and Decryption
Vendor Affirmed	CKG [SP 800-133 Rev 1]	-	-	Symmetric key generation *Symmetric keys and generated seeds are*

CAVP Cert.	Algorithm and Standard	Mode/Method	Description / Key Size / Key Strength	Use / Function
				produced using unmodified output from the Approved DRBG.
A3369	CTR_DRBG [SP800-90A]	AES-256 Derivation Function Enabled No Prediction Resistance	256 bits	Random Number Generation
A3369	ECDSA [FIPS 186-4]	Key Pair Generation (PKG)	Curve: P-256, P-384, P-521	Asymmetric Key Generation
A3369	ECDSA [FIPS 186-4]	Public Key Validation (PKV)	Curve: P-256, P-384, P-521	Asymmetric Public Key Verification
A3369	ECDSA [FIPS 186-4]	Signature Generation	Curve: P-256, P-384, P-521	Digital Signature Verification
A3369	ECDSA [FIPS 186-4]	Signature Verification	Curve: P-256, P-384, P-521	Digital Signature Verification
A3369	HMAC [FIPS 198-1]	SHA-256, SHA-384, SHA-512	Key Length: 256 bits or greater	Keyed Hash
A3369	KAS-SSC [SP800-56A Rev 3]	KAS-ECC-SSC: Scheme: "Ephemeral Unified" with curve P-256, P-384, P-521 KAS-FFC-SSC: Scheme: "dhEphem" and domain parameter generation methods "ffdhe2048, MODP-4096, MODP-8192"	Domain Parameter Generation Methods: ffdhe2048, MODP-4096, MODP-8192	Shared Secret Computation ffdhe2048 self-test only
A3369	KAS [SP800-56A Rev 3]		KAS (ECC): P-256, P-384 and P-521 with SSH and TLS v1.2 KDF (SP800-135rev1)	KAS (KAS-SSC Cert. #A3369, CVL Cert. #A3369) As per IG D.F Scenario 2 path

NOKIA

CAVP Cert.	Algorithm and Standard	Mode/Method	Description / Key Size / Key Strength	Use / Function
			KAS (FFC): ffdhe2048, MODP-4096, and MODP-8192 with SSH KDF (SP800-135rev1)	(2), the CAVP testing is performed in which case it is split into (i) testing the computation of the shared secret, (ii) testing the key derivation function used in deriving the keying material as per SP800-135 Rev 1
A3369	KTS [SP 800-38F Rev 1]	AES (unauthenticated mode) with HMAC	Key Length: 128, 256 bits Key Strength: 128, 256 bits	Key transport (SSH, TLS) Key establishment methodology provides between 128 and 256 bits of encryption strength.
A3369	KTS [SP 800-38F Rev 1]	AES (authenticated mode)	Key Length: 128, 256 bits Key Strength: 128, 256 bits	Key Transport (SSH, TLS) Key establishment methodology provides between 128 and 256 bits of encryption strength.
A3369	CVL [SP 800-135 Rev 1]	SSH KDF, TLS KDF Note: The SSH, TLS protocols have not been reviewed or tested by the CAVP and CMVP	Cipher: AES-128, AES-256 Hash Algorithm: SHA2-256, SHA2-384, SHA2-512 TLS Version: v1.2 Hash	Key Derivation

CAVP Cert.	Algorithm and Standard	Mode/Method	Description / Key Size / Key Strength	Use / Function
			Algorithm: SHA2-256, SHA2-384	
A3369	RSA [FIPS 186-4]	-	Modulus: 2048, 3072, 4096	Asymmetric Key Generation
A3369	RSA [FIPS 186-4]	Signature Generation (PKCS#1 v1.5)	Modulus: 2048, 3072, 4096	Digital Signature Generation
A3369	RSA [FIPS 186-4]	Signature Verification (PKCS#1 v1.5)	Modulus: 1024, 2048, 3072, 4096	Digital Signature Verification
A3369	RSA [FIPS 186-4]	Signature Verification (PKCS PSS)	Modulus: 4096	Digital Signature Verification Self-test only
A3369	Safe Primes Key Generation [SP 800-133 Rev 1]	KeyGen for DH	Safe Prime Groups: ffdhe2048, MODP-4096, MODP-8192	Key Generation ffdhe2048 Self-test only
A3369	Safe Primes Key Verification [SP 800-133 Rev 1]	KeyVer for DH	Safe Prime Groups: MODP-4096, MODP-8192	Key Verification
A3369	SHS [FIPS 180-4]	SHA-1, SHA-256, SHA-384, SHA-512	N/A	Message Digest

Table 9 - Approved Algorithms (Nokia openSSL)

Nokia Jitter Entropy (JENT)

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) /Key Strength(s)	Use / Function
A3310	SHS [FIPS 180-4]	SHA3-256	256	Message Digest
Entropy Cert	**Algorithm and Standard**	**Mode/Method**	**Description / Key Size(s) /Key Strength(s)**	**Use / Function**
E26	Entropy [SP800-90B]	N/A (Algorithms covered by A3310)	N/A	Random Number Generation

Table 10 – Approved Algorithms (Nokia Jitter Entropy (JENT))

Rijndael AES256 CTR/GCM (Nokia Crypto-OTU2 Engine 11QPEN4)

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) /Key Strength(s)	Use / Function
A2537	AES [FIPS 197] [SP 800-38A]	CTR	Key length: 256 bits	Symmetric Encryption and Decryption
	AES [FIPS 197] [SP 800-38A]	ECB Encryption only	Key length: 256 bits	Symmetric Encryption
A2539	AES [SP 800-38D]	GCM	Key length: 256 bits	Symmetric Encryption and Decryption
	AES [FIPS 197] [SP 800-38A]	ECB Encryption only	Key length: 256 bits	Symmetric Encryption
A2538	AES [FIPS 197] [SP 800-38A]	CBC	Key length: 256 bits	Symmetric Encryption and Decryption
	HMAC [FIPS 198-1]	SHA2-256	256 bits	Keyed Hash
	SHS [FIPS 180-4]	SHA2-256	256 bits	Message Digest

Table 11 - Approved Algorithms (11QPEN4)

CRYPOTN (Nokia 100G using Microsemi, S13X100E, 2UC400E)

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) /Key Strength(s)	Use / Function
AES 3844 (S13X100E and 2UC400E)	AES [FIPS 197] [SP 800-38A]	CTR	Key length: 256 bits	Symmetric Encryption and Decryption
	AES [FIPS 197] [SP 800-38A]	ECB Encryption only	Key length: 256 bits	Symmetric Encryption
	AES [SP 800-38D]	GMAC	Key length: 256 bits	Symmetric Encryption and Decryption
A2415 (S13X100E), A2416 (2UC400E)	AES [FIPS 197] [SP 800-38A]	CBC	Key length: 256 bits	Symmetric Encryption and Decryption
	HMAC [FIPS 198-1]	SHA2-256	256 bits	Keyed Hash
	SHS [FIPS 180-4]	SHA2-256	256 bits	Message Digest

Table 12 - Approved Algorithms (S13X100E, 2UC400E)

CRYPOTN (Nokia 100G using Microsemi) uses HMAC-SHA256 (and the underlying SHA-256) for the authentication of the pack serial number, which is used to distinguish the two ends of the encryption section (certificate C1545).

CRYPOTN (Nokia 100G using Microsemi) uses AES-256-CTR combined with AES-GMAC to form a proprietary authenticated encryption function (GMAC+CTR). The authentication key is derived from the encryption key in exactly the same way that AES-GCM does and also all calculations are done in a GCM like manner. The only difference is that the length of the authentication and cipher text fields are transposed.

For CRYPOTN, the IV generation follows the rules of [FIPS 140-3 IG] section C.H (case 4):
The probability that the proprietary GMAC+CTR authenticated encryption function ever will be invoked with the same IV and the same key on two (or more) distinct sets of input data shall be no greater than 2^{-32} for 1830 PSS S13X100E and 2UC400E.
The following rules ensure that the construction of the IV, the keys and the Fixed Field used satisfy the above requirement.
- i.) By implementation, the Fixed Field for AtoZ direction is always different than the ZtoA direction.
- ii.) By implementation, the IV is composed of a Fixed Field and a running counter (Invocation Field) that starts at zero
- iii.) By implementation, authentication stops and new keys are required from the key management system if:
  - a. The modules power is lost and then restored (which would cause the IV to be reset)
  - b. Running counter reaches its maximum
- iv.) Therefore, since IV are only reused with different keys, as long as the probability of new keys being different than any previous used keys exceeds 2^{-32}, then the concatenation of the keys with the IV will also exceed 2^{-32}.

v.)   <u>By Policy</u>, the key management system (external to the module) always generates random 256-bit keys and the probability of the key manager ever generating the same key again shall be no greater than 2^{-32} during the system lifetime across all keys generated.

vi.)   <u>By Policy</u>, the key management system uses one newly generated key on one circuit per one key session time period. The key is used for both the AtoZ and the ZtoA directions of that circuit for that key session time period.

Table 13 - Non-Approved Algorithms Not Allowed in the Approved Mode of Operation

2.3 Module Description

The 1830 PSS is a scalable, next-generation Dense Wave Division Multiplexer (DWDM) platform that supports data center aggregation for Ethernet, Fiber Channel (FC) and other protocols. Multiprotocol services can then be dynamically and flexibly transported over metro and long-haul spans, using Tunable and Reconfigurable Optical Add-Drop Multiplexers (T-ROADMs) for optical wavelengths. The 1830 PSS enables transparent L2 Ethernet or FC and L3 IP services over the optical link.

The Nokia 1830 PSS-32 shelves provide increased network flexibility and operational automation through zero-touch, transparent photonic networking. Photonic networks use simplified and accelerated operations to transform wavelength division multiplexing (WDM) into true transport networking with advanced flexibility, performance, automation, and integration. Several Optical Add-Drop multiplexing (OADM) configurations are supported by components that provide optical filter routing, optical amplification, and support for interworking with optical signals originating on non-1830 PSS hardware.

The Nokia 1830 PSS-32s are closely related shelves that compose the Nokia 1830 PSS-32 multi-service multi-reach solution. They are scalable optical transport platforms that implement a converged platform solution for multi-service DWDM metro-area, long-haul, and Optical Transport Network (OTN) switching, and leading-edge flexibility with next generation optical and OTN capabilities.
The Nokia 1830 PSS-32 Central Office Shelf provides a 32-slot primarily DWDM platform.

Figure 1 - PSS-32 Shelf

The Nokia 1830 PSS-8 and PSS-16II are the new generation in the 1830 portfolio; it is future-oriented product to provide high capacity, high flexibility and high scalability. Integrated together with existing network management systems and engineering tools, both shelves provide operational automation through zero-touch, transparent photonic networking. These two new products are based on the platform that converges Lambda switching, OTN switching and packet switching in metro aggregation and core layers for service grooming and aggregation.
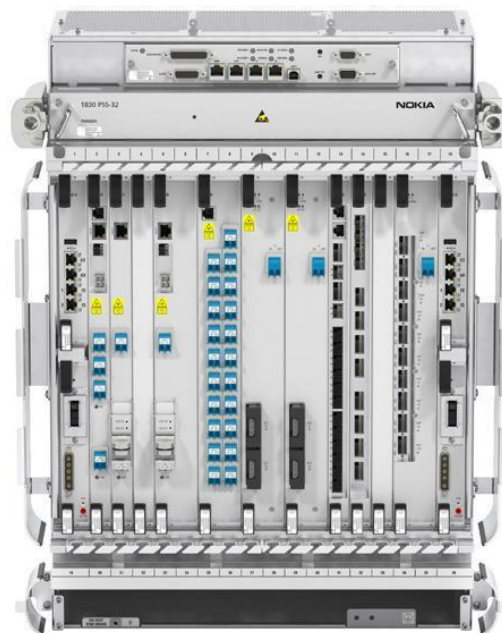
Figure 2 - PSS-16II Shelf

Figure 3 - PSS-8 Shelf

The 1830 PSS-24x is designed to address multilayer, multiservice, optical network scale and efficiency by delivering an industry leading level of optical transport network (OTN) and Ethernet switching. Capable of supporting up to 48 Tbps of OTN/Ethernet switching capacity in a single rack, terabit capable card slots and low system power utilization, the 1830 PSS-24x takes OTN/Ethernet grooming and protection to the next level of scale required to support efficient 100G, 200G, 400G, 500G and beyond wavelength transport.

Figure 4 - PSS-24x Shelf

The 1830 PSS-8x is optimized for both metro aggregation and metro core switching applications in optical transport networks (OTNs). It provides the flexibility and efficiency required to support an evolution to higher capacity services, enabling continued revenue streams as customers demand more bandwidth and enterprises move toward 10G, 100G, 200G and 400G connectivity.

With initial support for 1.6 Tb/s of electrical switching capacity and up to 4 Tb/s with latest switch fabric in a single 10RU shelf, 6.4 Tb/s per 300 mm rack the 1830 PSS-8x provides a small form factor high-capacity metro aggregation point.

Figure 5 - PSS-8x Shelf

1830 PSI-8L is a scalable and modular shelf that provides a DataCenter form factor compatible option to deploy Photonic Line configuration. As the industry has transitioned to data center-based applications, the shift has created a tremendous need for optical networks and bandwidth to interconnect data centers, as well as connect local data caching sites to their respective metro point-of-presence locations. While initial focus of data center solutions was on transponder shelves, need for flexibility and scalability of Photonic layer developed a need for appropriate photonic shelf. PSI-8L offers full compatibility to 1830 PSS current and future photonic cards.
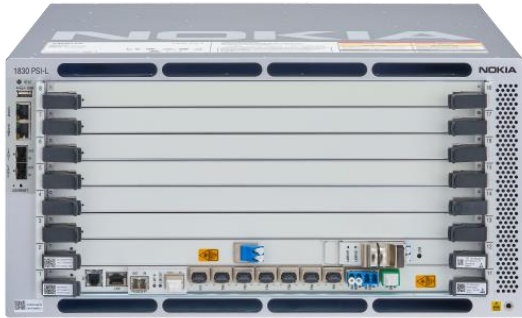
Figure 6 - PSI-8L Shelf

The approved configurations of 1830 PSS must meet stringent Physical, Logical and Operational requirements that are more restrictive than typical telecom or data center deployments. This use of 1830 PSS includes many different multi-shelf configurations with many different circuit pack types. The approved configurations of 1830 PSS consist of secured single shelf entities equipped with equipment controller cards and other cards (like 11QPEN4, S13X100E, 2UC400E) that are coupled into a multi-shelf system.

The multi-shelf system is controlled by a dedicated main shelf. The main shelf provides all the interfaces of the cryptographic boundary.
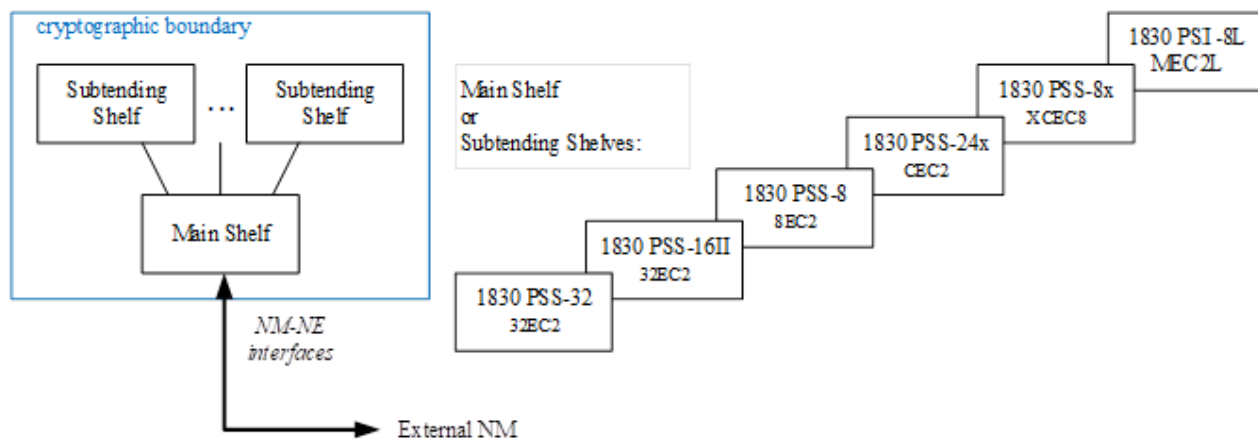
Figure 7 - Multi-Shelf Configuration

Each shelf type (PSS-32, PSS-16II, PSS-8, PSS-24x, PSS-8x and PSI-8L) can be used as main shelf or subtending shelf.

2.4 Block Diagram
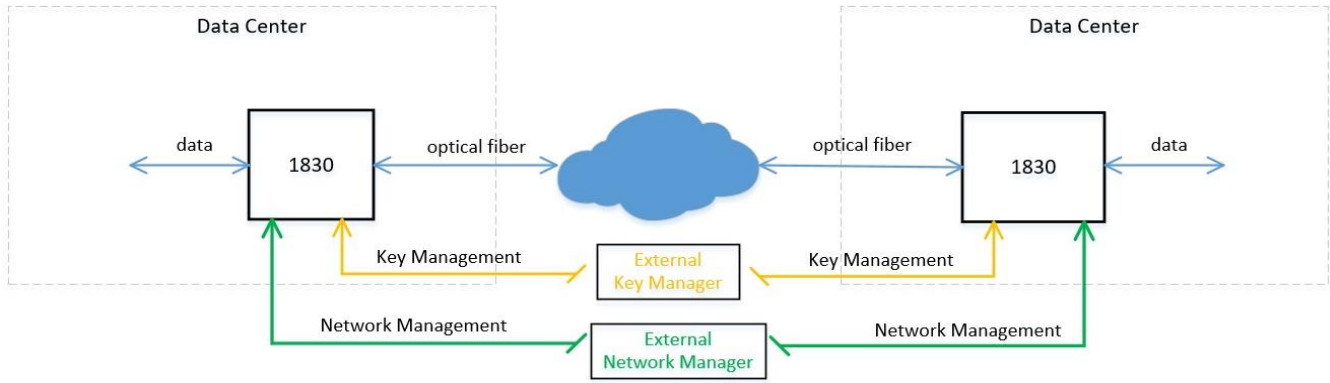
Figure 8 - 1830 PSS, 1830 PSI-8L Block Diagram

Security Policy
October 28, 2024

Copyright 2021-2023 © Nokia
This document may be freely distributed whole and intact including this complete copyright notice

1.2
Page 21 of 65

2.5 FIPS Configuration and Cryptographic Boundary

2.5.1 PSS-32/16II/8/24x/8x, PSI-8L

FIPS Configurations of 1830 PSS must meet stringent Physical, Logical and Operational requirements that are more restrictive than typical telecom or data center deployments. While the generalized use of 1830 PSS may normally include many different multi-shelf configurations with many different circuit pack types, the approved mode configurations of 1830 PSS consist of physically secured single shelf entities equipped with equipment controller cards and 11QPEN4, S13X100E, 2UC400E cards.

The cryptographic module is based on the encryption card 11QPEN4 and/or S13X100E or 2UC400E installed on a single shelf version of an 1830 PSS with an Equipment Controller (32EC2E, 8EC2E or CEC2).

The cryptographic modules are intended to be deployed at both ends of a transmit/receive pair of external optical fibers between two data centers to provide encryption of 10GE, 8G/10GFC and ODU2 client traffic (for 11QPEN4) and 10x 10GE/ODU2, 2x 40GE or 100GE/ODU4 (for S13X100E) and 4x ODU4 (for 2UC400E) while in flight between data centers.

Figure 9 - Network Configuration of 1830 PSS-32/16II/8/24x/8x, PSI-8L

Security Policy
October 28, 2024

1.2
Page 22 of 65

3 Cryptographic module interfaces

The module uses logical interfaces: Data Input, Data Output, Control Input, Status Output. The logical interface Control Output is not used by the module. The module does not output any command or control data used to control another module.

3.1 PSS-32 Interfaces

Physical port	Logical interface	Data that passes over port/interface
PSS-32 User Panel (1)		
OAMP (1)	OAMP interface	Control Input – Status Output
E1, E2 (2) (incl. LED)	Inter-Shelf LAN	Control Input – Status Output
Craft (USB) (1)	Craft Terminal	Control Input – Status Output
Craft (DB-9) (1)	Craft Terminal	Control Input – Status Output
Equipment Controller 32EC2 (2)		
CIT (2)	OAMP interface (local)	Control Input – Status Output
ES1, ES2	Inter-Shelf LAN	Control Input – Status Output
11QPEN4 Encryption Card (up to 16)		
LEDs (9)	Card, Transmission status	Status output
L (4)	Transmission	Data Input – Data Output
VA (4)	Transmission	Data Output
S13X100E Encryption Card (up to 15)		
LEDs (2)	Card, Transmission status	Status output
L (1)	Transmission	Data Input – Data Output
Filler Card (up to 16)		
n.a.	n.a.	No Interfaces

Table 14 - PSS-32 Ports and Interfaces

3.1.1 PSS-32 User Panel
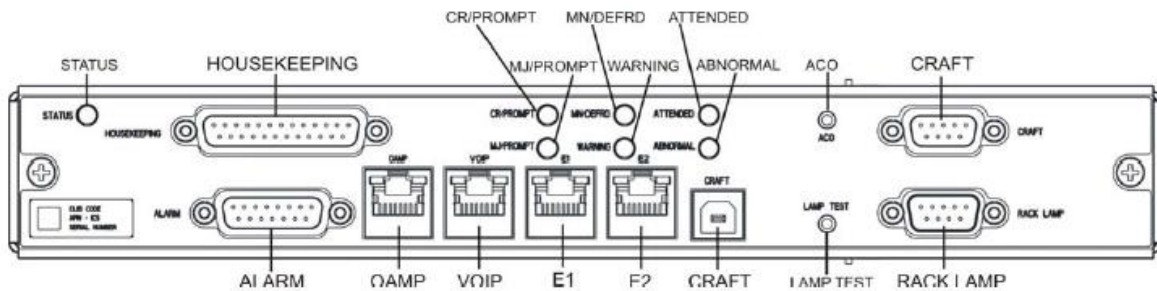
Figure 10 - PSS32 User Panel - front view

Physical port	Logical interface	Data that passes over port/interface
STATUS (1)	NE status LED	Status Output
HOUSEKEEPING (1)	Housekeeping	n.a. (shelf internal)
ALARM (1)	Rack Alarm	n.a. (shelf internal)
CR/PROMPT (1)	Critical Condition LED	Status Output
MJ/PROMPT (1)	Major Condition LED	Status Output
MN/DEFRD (1)	Minor Condition LED	Status Output
WARNING (1)	Warning Condition LED	Status Output
ATTENDED (1)	NE attended status LED	Status Output
ABNORMAL (1)	NE attended status LED	Status Output

Security Policy
October 28, 2024

Copyright 2021-2023 © Nokia
This document may be freely distributed whole and intact including this complete copyright notice

1.2
Page 23 of 65

Physical port	Logical interface	Data that passes over port/interface
OAMP (1) (incl. LED)	OAMP (GbE)	Control Input – Status Output
VOIP (1) (incl. LED)	Voice over IP	Data Input – Data Output
E1, E2 (2) (incl. LED)	Inter-Shelf LAN	Control Input – Status Output
CRAFT (1)	Type B USB interface Craft: Craft Port (USB signal)	Control Input – Status Output
ACO (1)	Alarm cut off button	Control Input
LAMP TEST (1)	Lamp test button	Control Input
CRAFT (Sub-D) (1)	(D-Sub DE-9) Debug Serial In/Out	Control Input – Status Output
RACK, LAMP (1)	Rack alarm, Rack Lamp	n.a. (shelf internal)

Table 15 - PSS-32 User Panel - Ports and Interfaces

3.2 PSS-16II Interfaces

Physical port	Logical interface	Data that passes over port/interface
PSS-16II User Panel (1)		
OAMP (1)	OAMP interface	Control Input – Status Output
E1, E2 (#10) (incl. LED)	Inter-Shelf LAN	Control Input – Status Output
Craft (USB) (1)	Craft Terminal	Control Input – Status Output
Craft (DB-9) (1)	Craft Terminal	Control Input – Status Output
Equipment Controller 32EC2 (2)		
CIT (2)	OAMP interface (local)	Control Input – Status Output
ES1, ES2	Inter-Shelf LAN	Control Input – Status Output
11QPEN4 Encryption Card (up to 16)		
LEDs (9)	Card, Transmission status	Status output
L (4)	Transmission	Data Input – Data Output
VA (4)	Transmission	Data Output
S13X100E Encryption Card (up to 15)		
LEDs (2)	Card, Transmission status	Status output
L (1)	Transmission	Data Input – Data Output
Filler Card (up to 16)		
n.a.	n.a.	No Interfaces

Table 16 - PSS-16II Ports and Interfaces

3.2.1 PSS-16II User Panel
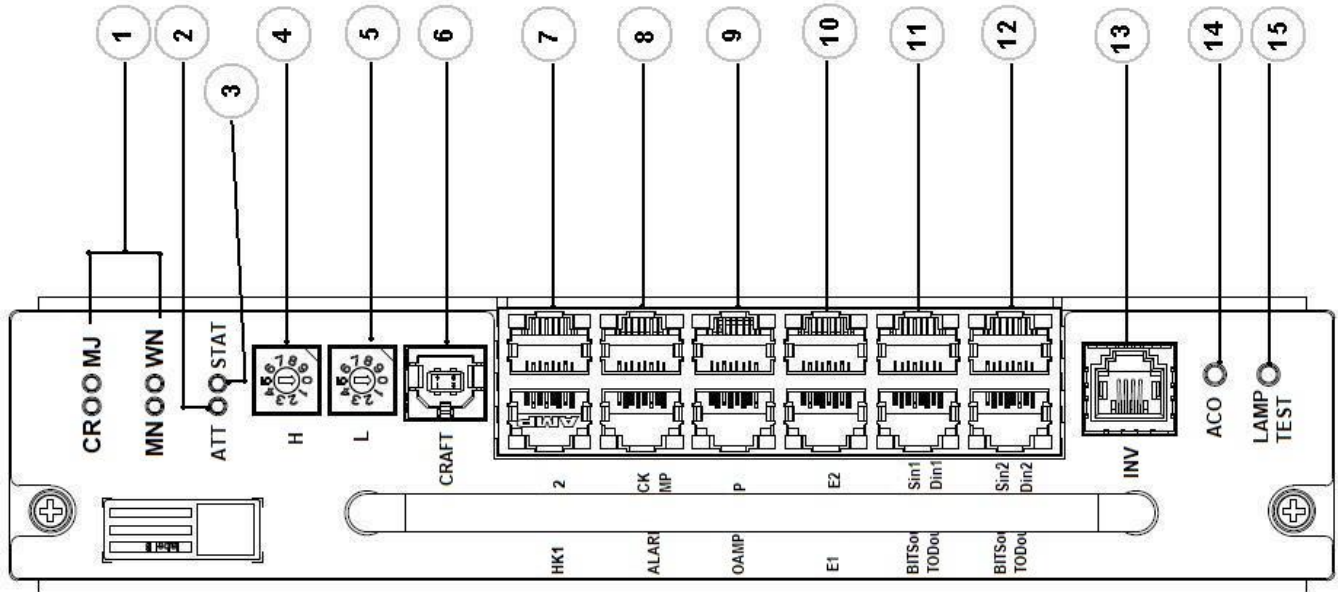
Figure 11 - PSS-16II User Panel - Ports and Interfaces

Physical port	Logical interface	Data that passes over port/interface
LEDs Alarm Status (4) (#1)	NE alarm status	Status Output
LED ATT (1) (#2)	NE attended status	Status Output
LED STAT (1) (#3)	NE status	Status Output
Shelf-ID Rotary H, L (2) (#4,5)	Shelf-ID configuration	Control Input
CRAFT (#6)	Type B USB interface Craft: Craft Port (USB signal)	Control Input – Status Output
HK1, HK2 (#7)	Housekeeping	n.a. (shelf internal)
RACK, LAMP (#8)	Rack alarm, Rack Lamp	n.a. (shelf internal)
OAMP (#9) (incl. LED)	OAMP (GbE)	Control Input – Status Output
VOIP (#9) (incl. LED)	Voice over IP	Data Input – Data Output
E1, E2 (#10) (incl. LED)	Inter-Shelf LAN	Control Input – Status Output
BITS out TOD out (#11)	Clock and timing	Data Output
BITS in TOD in (#11)	Clock and timing	Data Input
BITS out TOD out (#12)	Clock and timing	Data Output
BITS in TOD in (#12)	Clock and timing	Data Input
INV (#13)	1-wire connection to SFD44	n.a. (shelf internal)
ACO (#14)	Alarm cut off button	Control Input
LAMP TEST (#15)	Lamp test button	Control Input

Table 17 - PSS-16II User Panel - Ports and Interfaces

3.3 PSS-8 Interfaces

Physical port	Logical interface	Data that passes over port/interface
PSS-8 Shelf Panel (1)		
OAMP (1)	OAMP interface	Control Input – Status Output
Equipment Controller 8EC2 (2)		
Craft (1)	Craft Terminal	Control Input – Status Output
CIT (2)	OAMP interface (local)	Control Input – Status Output
ES1, ES2	Inter-Shelf LAN	Control Input – Status Output

11QPEN4 Encryption Card (up to 8)		
LEDs (9)	Card, Transmission status	Status output
L (4)	Transmission	Data Input – Data Output
VA (4)	Transmission	Data Output
S13X100E Encryption Card (up to 8)		
LEDs (2)	Card, Transmission status	Status output
L (1)	Transmission	Data Input – Data Output
Filler Card (up to 7)		
n.a.	n.a.	No Interfaces

Table 18 - PSS-8 Ports and Interfaces

3.3.1 PSS-8 Shelf Panel
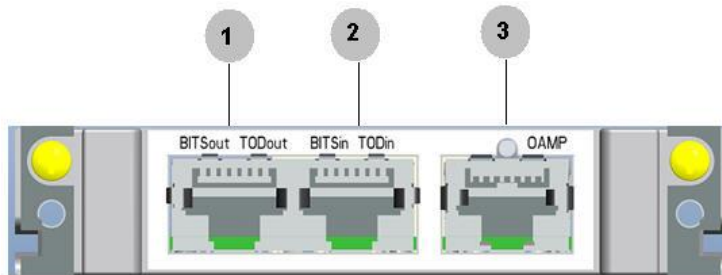
Figure 12 - PSS-8 Shelf Panel – Ports and Interfaces

Physical port	Logical interface	Data that passes over port/interface
BITS out TOD out (#1)	Clock and timing	Data Output
BITS in TOD in (#2)	Clock and timing	Data Input
OAMP (1) (#3)	OAMP interface	Control Input – Status Output

Table 19 - PSS-8 Shelf Panel - Ports and Interfaces

3.4 PSS-24x Interfaces

Physical port	Logical interface	Data that passes over port/interface
MFC24X (1)		
STAT (1)	NE status LED	Status Output
Shelf ID MSB, LSB (2)	Shelf ID Rotary Dials	Control Input
Equipment Controller CEC2 (2)		
STAT (1)	Card Status LED	Status Output
EPS (1)	EPS LED	Status Output
⚠ (1)	Alarm cut off button	Control Input
C, M, m, W (4)	Alarm Condition LED	Status Output
AT (1)	Attended LED	Status Output
AB (1)	Abnormal LED	Status Output
⬩⟵ (1)	Type B USB interface Craft: Craft Port (USB signal)	Control Input – Status Output
DLAN (1)	Debug LAN	Control Input – Status Output
DSER (1)	Debug Serial In/Out	Control Input – Status Output
DNR (1)	Do Not Remove LED	Status Output
CIT (1)	OAMP Management (local)	Control Input – Status Output
OAMP (1)	OAMP Management	Control Input – Status Output

E1 (1)	OAMP Management	Control Input – Status Output
ES1, ES2	Inter-Shelf LAN	Control Input – Status Output
R	Reset Button	Control Input
2UC400E Encryption Card (up to 24)		
STAT	Card status LED	Status Output
1, 2 LED (2)	Transmission status LED	Status output
1, 2 (2)	Line Interface	Data Input – Data Output
Filler Card (up to 23)		
n.a.	n.a.	No Interfaces

Table 20 - PSS-24x Ports and Interfaces

3.4.1 MFC24X
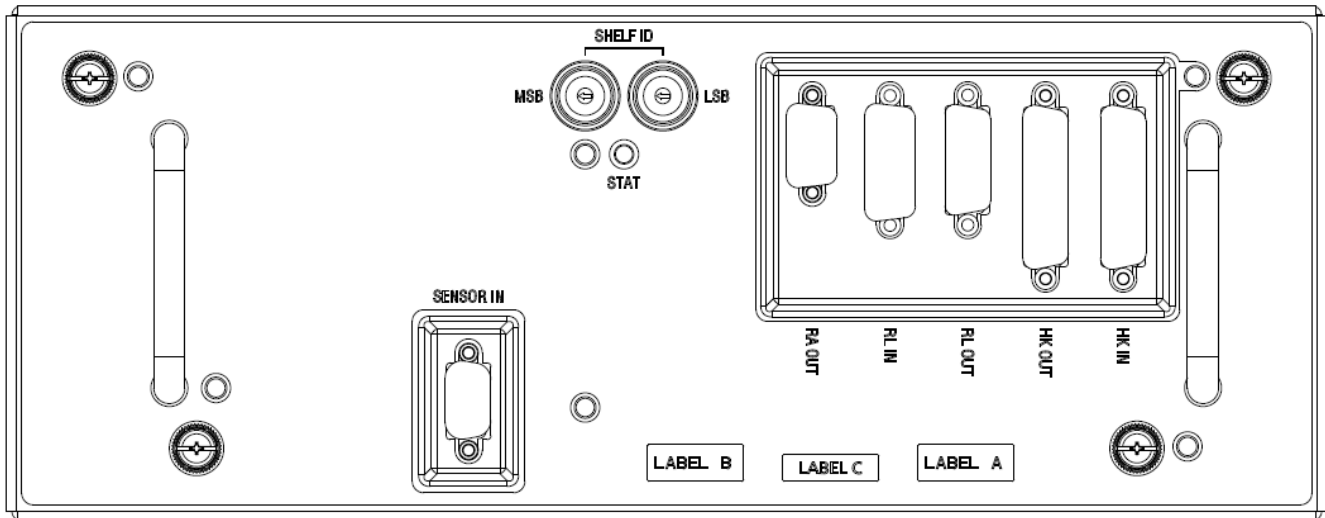
Figure 13 - PSS-24x MFC24X - Ports and Interfaces

Physical port	Logical interface	Data that passes over port/interface
STAT (1)	NE status LED	Status Output
Shelf ID MSB, LSB (2)	Shelf ID Rotary Dials	Control Input
HK IN, HK OUT (2)	Housekeeping	n.a. (shelf internal)
RA OUT, RL IN, RL OUT (3)	Rack alarm, Rack Lamp	n.a. (shelf internal)
SENSOR IN (1)	Interface to sensor card	n.a. (shelf internal)

Table 21 - MFC24x - Ports and Interfaces

3.5 PSS-8x Interfaces

Physical port	Logical interface	Data that passes over port/interface
XMFC (1)		
STAT (1)	NE status LED	Status Output
Shelf ID MSB, LSB (2)	Shelf ID Rotary Dials	Control Input
Equipment Controller XCEC8 (up to 2)		
STAT (1)	Card Status LED	Status Output
EPS (1)	EPS LED	Status Output
⚠ (1)	Alarm cut off button	Control Input
C (1)	Critical Condition LED	Status Output
M (1)	Major Condition LED	Status Output
m (1)	Minor Condition LED	Status Output

W (1)	Warning Condition LED	Status Output
AT (1)	Attended LED	Status Output
AB (1)	Abnormal LED	Status Output
⬦ (1)	Type B USB interface Craft: Craft Port (USB signal)	Control Input – Status Output
DLAN (1)	Debug LAN	Control Input – Status Output
DSER (1)	Debug Serial In/Out	Control Input – Status Output
DNR (1)	Do Not Remove LED	Status Output
CIT (1)	OAMP Management (local)	Control Input – Status Output
OAMP (1)	OAMP Management	Control Input – Status Output
ES1, ES2	Inter-Shelf LAN	Control Input – Status Output
R	Reset Button	Control Input
Filler Card (up to 7)		
n.a.	n.a.	No Interfaces

Table 22 - PSS-8x - Ports and Interfaces

3.5.1   XMFC
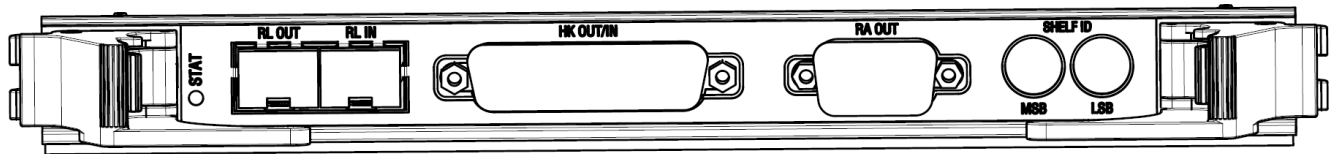
Figure 14 – XMFC - Ports and Interfaces

Physical port	Logical interface	Data that passes over port/interface
STAT (1)	NE status LED	Status Output
Shelf ID MSB, LSB (2)	Shelf ID Rotary Dials	Control Input
HK IN, HK OUT (2)	Housekeeping	n.a. (shelf internal)
RA OUT, RL IN, RL OUT (3)	Rack alarm, Rack Lamp	n.a. (shelf internal)

Table 23 – XMFC - Ports and Interfaces

3.6   PSI-8L Interfaces

Physical port	Logical interface	Data that passes over port/interface
PSI-8L Chassis (1)		
STAT LED (1)	Card status LED	Status output
OAMP (1)	OAMP interface	Control Input – Status Output
USB (1)	Type B USB interface Craft: Craft Port (USB signal)	Control Input – Status Output
CON (1)	Serial Debug	Control Input – Status Output
UID/RESET	Shelf Reset	Control Input
Equipment Controller MEC2L (up to 2)		
n.a.	n.a.	n.a.
PSILMFC (1)		
CON (1)	Serial Debug	Control Input – Status Output
CIT (1)	OAMP interface (local)	Control Input – Status Output
ES1, ES2	Inter-Shelf LAN	Control Input – Status Output
MEC 1 LED (1)	MEC 1 status LED	Status output
MEC 2 LED (1)	MEC 2 status LED	Status output

Filler Card (up to 4)		
n.a.	n.a.	No Interfaces

Table 24 – PSI-8L Ports and Interfaces

3.6.1   PSI-8L Chassis
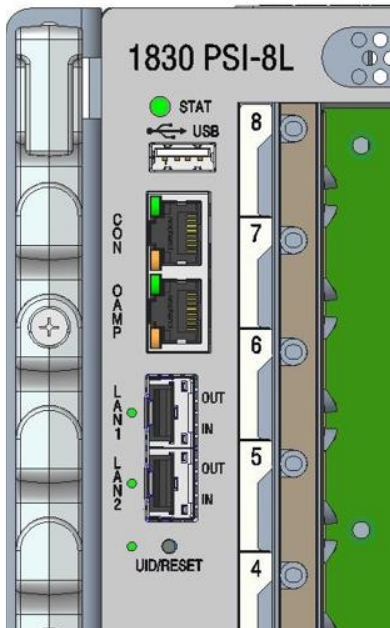
Figure 15 – PSI-8L Chassis (Front) - Ports and Interfaces

Physical port	Logical interface	Data that passes over port/interface
STAT LED (1)	Card status LED	Status output
OAMP (1)	OAMP interface	Control Input – Status Output
USB (1)	Type B USB interface Craft: Craft Port (USB signal)	Control Input – Status Output
CON (1)	Serial Debug	Control Input – Status Output
LAN1, LAN2	External IP equipment port	Port enabled, but shall not be used in FIPS configuration
UID/RESET	Shelf Reset	Control Input

Table 25 – PSI-8L Chassis - Ports and Interfaces

3.6.2   PSI-8L PSILMFC

Figure 16 - PSI-8L PSILMFC - Ports and Interfaces

Physical port	Logical interface	Data that passes over port/interface
INV	Inventory jack	Port disabled. Not used in this release.
CON (1)	Serial Debug	Control Input – Status Output
CIT (1)	OAMP interface (local)	Control Input – Status Output
ES1, ES2	Inter-Shelf LAN	Control Input – Status Output
LAN3, LAN4	External IP equipment port	Port enabled, but shall not be used in FIPS configuration

MEC 1 LED (1)	MEC 1 status LED	Status output
MEC 2 LED (1)	MEC 2 status LED	Status output

Table 26 - PSI-8L PSILMFC - Ports and Interfaces

3.7 Equipment Controller 32EC2 for PSS-32, PSS16II
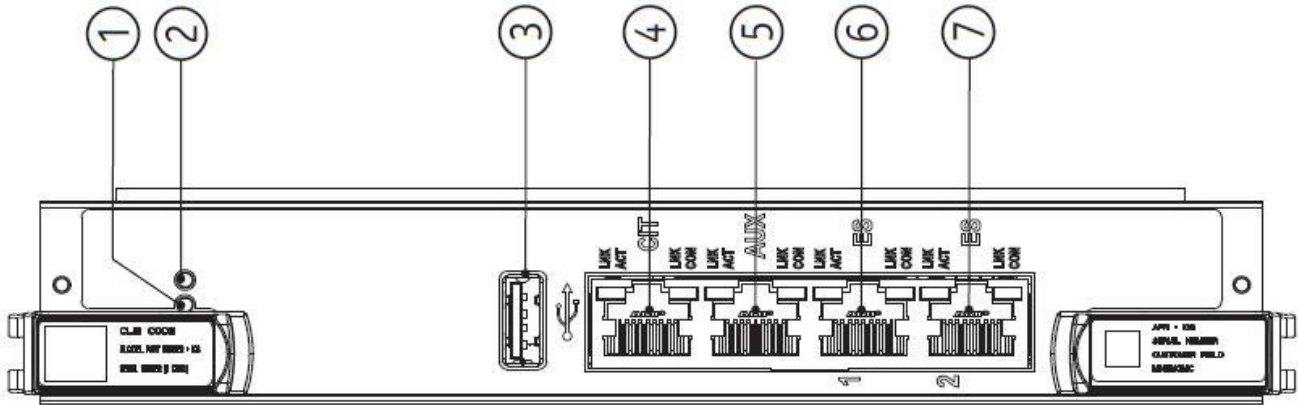
Figure 17 - 32EC2 - Ports and Interfaces

Physical port	Logical interface	Data that passes over port/interface
LED (#1)	LED status	Status Output
LED (#2)	LED EPS	Status Output
USB (#3)	USB	Control Input – Status Output
CIT (#4)	OAMP Management (local)	Control Input – Status Output
AUX (#5)		Port disabled and cannot be used in FIPS configuration
ES1, ES2 (#6,7)	Inter-Shelf LAN	Control Input – Status Output

Table 27 - 32EC2 - Ports and Interfaces

3.8 Equipment Controller 8EC2 for PSS-8
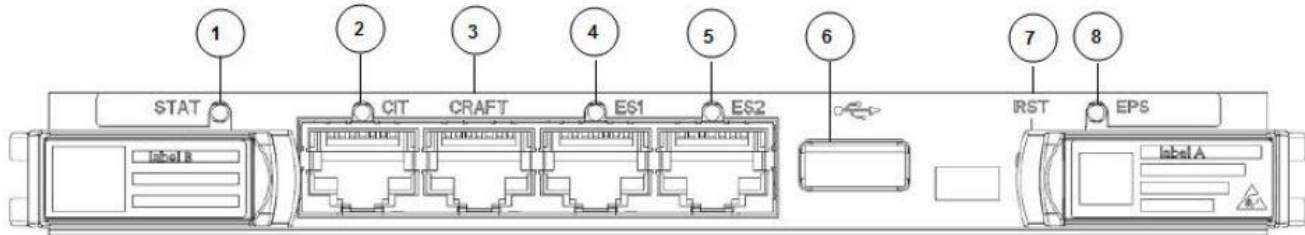
Figure 18 - 8EC2 - Ports and Interfaces

Physical port	Logical interface	Data that passes over port/interface
LED (#1)	LED status	Status Output
LED (#8)	LED EPS	Status Output
CRAFT (#3)	Craft Terminal	Control Input – Status Output
CIT (#2)	OAMP Management (local)	Control Input – Status Output
ES1, ES2 (#4,5)	Inter-Shelf LAN	Control Input – Status Output
USB (#6)	USB	Control Input – Status Output
RST (#7)	Reset button	Control Input

Table 28 - 8EC2 - Ports and Interfaces

3.9 Equipment Controller CEC2 for PSS-24x
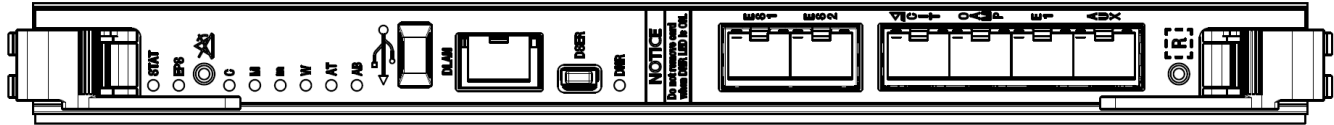
Figure 19 - CEC2 - Ports and Interfaces

Physical port	Logical interface	Data that passes over port/interface
STAT (1)	Card Status LED	Status Output
EPS (1)	EPS LED	Status Output
⚠ (1)	Alarm cut off button	Control Input
C (1)	Critical Condition LED	Status Output
M (1)	Major Condition LED	Status Output
m (1)	Minor Condition LED	Status Output
W (1)	Warning Condition LED	Status Output
AT (1)	Attended LED	Status Output
AB (1)	Abnormal LED	Status Output
⇆ (1)	Type B USB interface Craft: Craft Port (USB signal)	Control Input – Status Output
DLAN (1)	Debug LAN	Control Input – Status Output
DSER (1)	Debug Serial In/Out	Control Input – Status Output
DNR (1)	Do Not Remove LED	Status Output
ES1, ES2 (2)	Inter-Shelf LAN	Control Input – Status Output
CIT (1)	OAMP Management (local)	Control Input – Status Output
OAMP (1)	OAMP Management	Control Input – Status Output
E1 (1)	OAMP Management	Control Input – Status Output
AUX		Port enabled, but shall not be used in FIPS configuration
R	Reset Button	Control Input

Table 29 - CEC2 - Ports and Interfaces

3.10 Equipment Controller XCEC8 for PSS-8x
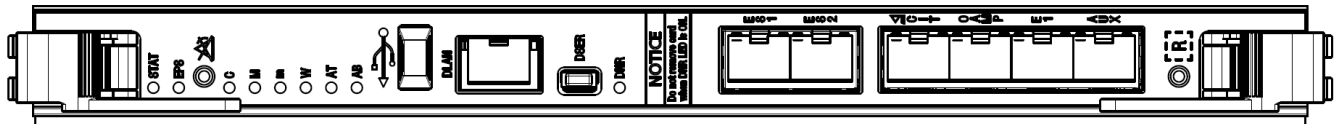
Figure 20 – XCEC8 - Ports and Interfaces

Physical port	Logical interface	Data that passes over port/interface
STAT (1)	Card Status LED	Status Output
EPS (1)	EPS LED	Status Output
⚠ (1)	Alarm cut off button	Control Input
C (1)	Critical Condition LED	Status Output
M (1)	Major Condition LED	Status Output
m (1)	Minor Condition LED	Status Output
W (1)	Warning Condition LED	Status Output
AT (1)	Attended LED	Status Output
AB (1)	Abnormal LED	Status Output
⇆ (1)	Type B USB interface Craft: Craft Port (USB signal)	Control Input – Status Output

DLAN (1)	Debug LAN	Control Input – Status Output
DSER (1)	Debug Serial In/Out	Control Input – Status Output
DNR (1)	Do Not Remove LED	Status Output
ES1, ES2 (2)	Inter-Shelf LAN	Control Input – Status Output
CIT (1)	OAMP Management (local)	Control Input – Status Output
OAMP (1)	OAMP Management	Control Input – Status Output
AUX		Port enabled, but shall not be used in FIPS configuration
R	Reset Button	Control Input

Table 30 - XCEC8 – Ports and Interfaces

3.11 11QPEN4

The 11QPEN4 has four pluggable client interfaces (C1, C2, C3, and C4), four pluggable line interfaces (L1, L2, L3 and L4) and four VOA sockets (VA1, VA2, VA3 and VA4) and a status LED as shown in Figure 10. The client and line interfaces are equipped with XFP transceivers. Each transceiver provides an optical fiber interface for receive and an optical fiber interface for transmit. Each line-client pair (L1-C1, L2-C2, L3-C3, L4-C4) provides an encrypted line port and the associated unencrypted client port. In the transmit direction, unencrypted data in the form of Fibre Channel, Ethernet or OTU2 signals enter a client port and are encrypted and then transmitted out the associated line port. In the receive direction, encrypted data is received on the Line Port and then decrypted and sent out the associated client port. The VOA sockets provide a means to optically attenuate the Line port signals- (They do not access or modify the content of the line port signals).
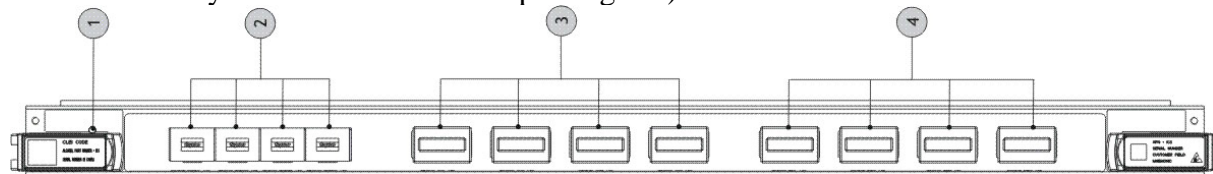
Figure 21 - 11QPEN4 - Ports and Interfaces

Physical port	Logical interface	Data that passes over port/interface
LED (#1)	LED status	Status Output
L1, L2, L3, L4 (4) (#2)	Transmission	Data Input – Data Output
VA1, VA2, VA3, VA4 (4) (#3)	Transmission	Data Output
C1, C2, C3, C4 (4) (#4)	Transmission	Data Input – Data Output
LEDs (12) (#2,3,4)	Transmission	Status Output

Table 31 - 11QPEN4 - Ports and Interfaces

3.12 S13X100E

The S13X100E has
- thirteen pluggable client interfaces
  - C1 … C10: SFP+ transceivers
  - C21: CFP4 transceiver
  - C31, C32: QSFP transceivers
- one fixed line interface
- a status LEDs for the card
- fourteen status LEDs (one for each interface)

Each pluggable client interface transceiver and the fixed line side transceiver provides an optical fiber interface for receive and an optical fiber interface for transmit. In the transmit direction, unencrypted data in the form of Ethernet, OTU2 or OTU4 signals enters the client ports, are multiplexed into one ODU4 signal and then encrypted and transmitted out the line port. In the receive direction, encrypted data is received on the Line Port and then decrypted and de-multiplexed and sent out the client ports.
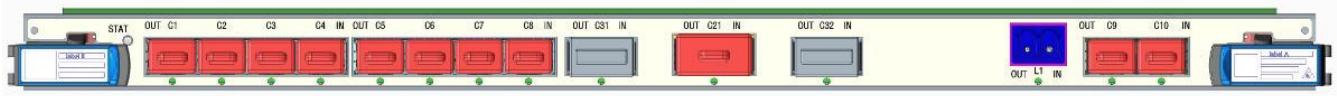
Figure 22 - S13X100E - Ports and Interfaces

Physical port	Logical interface	Data that passes over port/interface
LED STAT	LED status	Status Output
L1 (1)	Line Interface	Data Input – Data Output
C1..C10	Client XFP interfaces	Data Input – Data Output
C31..32	Client QSFP interfaces	Data Input – Data Output
C21	Client CFP4 interfaces	Data Input – Data Output

Table 32 - S13X100E - Ports and Interfaces

3.13 8P20
The 8P20 has

- eight client or line interfaces
- a status LEDs for the card
- eight status LEDs (one for each interface)

8P20 is a single-slot, half-height card supported in 1830 PSS-8/PSS-16II/PSS-32 shelves. It has six SFP and two SFP+ ports. It supports 8 sub-10G any-rate client ports in client/line configurations as a client tributary card in PSS-8/PSS-16II shelves, and it supports 6 sub-10G anyrate client ports with two line OTU2 SFP+ ports in the standalone muxponder configuration.

Figure 23 – 8P20 - Ports and Interfaces

Physical port	Logical interface	Data that passes over port/interface
STAT	Card status LED	Status Output
C1, C2, C3, C4, VA1/C5, VA2/C6, L1/C7, L1/C8 LED (8)	Transmission status LED	Status output
C1, C2, C3, C4, VA1/C5, VA2/C6, L1/C7, L1/C8 (8)	Client/Line Interface	Data Input – Data Output

Table 33 – 8P20 - Ports and Interfaces

3.14 2UC400E
The 2UC400E has

- two fixed line interfaces (1, 2)
- a status LEDs for the card
- two status LEDs (one for each interface)

The fixed line side transceivers provide an optical fiber interface for receive and an optical fiber interface for transmit. This card is used in a switching system, where the client-side signals are received from a backplane interface by the card. In the backplane-to-line direction, unencrypted data in the form of 100GE signals enters the client ports, is multiplexed into one ODU4 signal and then encrypted and transmitted out the line port. In the line-to-backplane direction, encrypted data is received on the Line Port and then decrypted and de-multiplexed and sent out the client ports.

Security Policy
October 28, 2024

Copyright 2021-2023 © Nokia
This document may be freely distributed whole and intact including this complete copyright notice

1.2
Page 33 of 65

Figure 24 – 2UC400E - Ports and Interfaces

Physical port	Logical interface	Data that passes over port/interface
STAT	Card status LED	Status Output
1, 2 LED (2)	Transmission status LED	Status output
1, 2 (2)	Line Interface	Data Input – Data Output

Table 34 – 2UC400E - Ports and Interfaces

3.15 MEC2L

The MEC2L has no interfaces. All needed interfaces (e.g. for OAMP) are accessible at the PSI-8L Chassis or PSILMFC.

Physical port	Logical interface	Data that passes over port/interface
n.a.	n.a.	No interfaces

Table 35 – MEC2L - Ports and Interfaces

3.16 Filler Card (PSS-32/16II/8/24x PSI-8L)

The Filler Card has no transmission functionality. Its main purpose is to guarantee the proper airflow for the cooling of the NE.

Figure 25 – PSS32-16II/8 Filler Card - Ports and Interfaces

Physical port	Logical interface	Data that passes over port/interface
n.a.	n.a.	No interfaces

Table 36 - Filler Card - Ports and Interfaces

Note: there are different physical filler cards for PSS-32/16II/8, for PSS-24x and for PSI-8L, but the properties of those cards are the same and are reflected in the table above.

4 Roles, services, and authentication

4.1 Roles

The module supports identity-based authentication and the module supports two roles:

- Crypto Officer Role which is referred to as 'Admin'
- User Role which is referred to as 'Crypto'

The Admin accesses the module via the SNMP and/or the Command Line Interface (CLI) and/or WebUI. This role provides all services that are necessary for initial installation of the module and management of the module. These services are all Approved services.

The Crypto accesses the module via the SNMP and/or the Command Line Interface (CLI). This role provides all services that are necessary for the provisioning and supervision of the transmission encryption function of the module for S13X100E, 11QPEN4 and 2UC400E. Those transmission encryption functions cannot be provisioned by other roles. These services are all Approved services.

Role	Type	Operator Type	Authentication Methods
Admin	Role	CO	SNMPv3 Authentication, CLI/WebUI Password
Crypto	Role	User	SNMPv3 Authentication, CLI Password

Table 37 - Roles, Service Commands, Input and Output

4.2 Services

Service	Description	Approved Security Functions	Keys And/or SSPs	Roles	Access rights to keys and/or SSPs	Indicator
Admin related Services						
User Account Management	Manage user accounts, password complexity and user privileges via CLI, WebUI interface	N/A	User Password (all accounts)	Admin	W	Log entry, Command execution returns success indicator
Change User Password	Change the User password for same account via CLI, Web UI interface	N/A	User Password	Admin	W	Log entry, Command execution returns success indicator
SNMP Configuration and Management	Manage SNMPv3 configurations via CLI, WebUI interface	AES-CFB128 Keyed Hash Message Authentication SNMPv3 Key Derivation KTS Secure Hash	SNMPv3 Passphrase SNMPv3 Authentication Key SNMPv3 Privacy Key	Admin	E, W	Log entry, Command execution returns success indicator
Key and Certificate Management	Manage Keys and Certificates (including Trust Anchors) via CLI, WebUI interface	RSA/ECDSA Key Pair Generation KTS Secure Hash	TLS Public Key TLS Private Key SSH Private Key SSH Public Key SNMP Certificate Fingerprint CA Public Key SSH User Public Key SFTP SSH User Private Key SFTP Server Public Host Key	Admin	G, E, R, W	Log entry, Command execution returns success indicator
Commission the Module	Commission the module by following the Security Policy guidelines via CLI interface	N/A	None	Admin	N/A	Log entry, Command execution returns success indicator

Service	Description	Approved Security Functions	Keys And/or SSPs	Roles	Access rights to keys and/or SSPs	Indicator
Perform Self-tests	Perform on-demand Power-up Self Tests by power cycling the cryptographic module	A3369, A2502, A3310, A2537, A2538, A2539, A2415, A2416, AES 3844	None	Admin	All ephemeral keys/CSPs – Z	Log entry
Show Status	Allows operator to view status of the parameters associated with FIPS-Approved mode via SNMPv3 and CLI interfaces	N/A	None	Admin	N/A	N/A
Alarms Monitoring	Allows operator to view active alarms via SNMPv3 interfaces	N/A	None	Admin	N/A	N/A
Events Monitoring	Allows the user to view all logged events associated with their permissions via SNMPv3 interfaces	N/A	None	Admin	N/A	N/A
11QPEN4 Provision Equipment	Allows the user to provision and configure the 11QPEN4 cards via SNMPv3 interface	N/A	None	Admin	N/A	N/A
11QPEN4 Provision Facility	Allows the user to provision and configure the facility information associated with 11QPEN4 cards via SNMPv3 interface	N/A	None	Admin	N/A	N/A
S13X100E Provision Equipment	Allows the user to provision and configure the S13X100E cards via SNMPv3 interface	N/A	None	Admin	N/A	N/A
S13X100E Provision Facility	Allows the user to provision and configure the facility information associated with S13X100E cards via SNMPv3 interface	N/A	None	Admin	N/A	N/A
Zeroize Keys	Zeroize keys and CSPs over SNMPv3 and CLI interfaces	N/A	SNMPv3 Passphrase SNMPv3 Authentication Key SNMPv3 Privacy Key 11QPEN4 Session Encryption Key 11QPEN4 Session KAT Key S13X100E Session Encryption Key S13X100E Session KAT Key	Admin	Z	Log entry, Command execution returns success indicator
Session initiation	Initiate session with another module using AES keys.	AES Encryption/Decryption Keyed Hash Message Authentication Secure Hash	11QPEN4 Session Encryption Key 11QPEN4 Session KAT Key S13X100E Session Encryption and Authentication Key S13X100E Session Communication Authentication Key S13X100E Session KAT Key 2UC400E Session Encryption Key 2UC400E Session KAT Key	Admin	E	Log entry, Command execution returns success indicator
Zeroize all SSPs	Zeroize all SSPs over CLI interface using Return-to-Factory command	N/A	All SSPs	Admin	Z	LED status indicator
Show version	Show the version of the module	N/A	None	Admin	N/A	N/A
Establish TLS session	Establish TLS session	AES-CBC, AES-GCM	CA Public Key TLS Public Key TLS Private Key	Admin	G, R, W, E	Log entry TLS session completes

Service	Description	Approved Security Functions	Keys And/or SSPs	Roles	Access rights to keys and/or SSPs	Indicator
		Encryption/Decryption Keyed Hash Message Authentication RSA Digital Signature Generation RSA Digital Signature Verification TLS 1.2 Key Derivation RSA Key Generation KAS-ECC-SSC Shared Secret Computation KTS Secure Hash Random Number Generation	ECDH Private Key Component ECDH Public Key Component ECDH Peer Public Key Component TLS Pre-Master Secret TLS Master Secret TLS Session Key TLS Authentication Key SNMPv3 Certificate Fingerprint Database Encryption Key AES GCM IV DRBG Seed Entropy Input String DRBG 'V' DRBG 'Key'			
Establish SSH session	Establish SSH session	AES-CTR, AES-GCM Encryption/Decryption Keyed Hash Message Authentication ECDSA Digital Signature Generation ECDSA Digital Signature Verification RSA Digital Signature Generation RSA Digital Signature Verification Key Derivation RSA/ECDSA Key Generation KAS-FCC-SSC Shared Secret Computation KAS-ECC-SSC Shared Secret Computation Secure Hash Random Number Generation	DH Public Key Component DH Private Key Component ECDH Public Key Component ECDH Private Key Component SSH Private Key SSH Public Key SSH Shared Secret SSH Session Key SSH Authentication Key SSH User Public Key SFTP SSH User Private Key SFTP Server Public Host Key Database Encryption Key AES GCM IV DRBG Seed Entropy Input String DRBG 'V' DRBG 'Key'	Admin	G, R, W, E	Log entry SSH session completes
Establish SNMPv3 session	Perform actions over SNMPv3	AES CFB128 Encryption/Decryption Keyed Hash Message Authentication KTS SNMPv3 KDF Secure Hash	SNMPv3 Authentication Key SNMPv3 Privacy Key SNMP Certificate Fingerprint	Admin	W, E	Log entry SNMPv3 session completes
Upgrade Application Firmware	Load FIPS validated application firmware	RSA Digital Signature Verification	Firmware Load Authentication Key	Admin	E	Log entry Show version confirmation
Crypto related Services						
Change Crypto Password	Change the Crypto password for same account	N/A	Crypto Password	Crypto	W	N/A

Service	Description	Approved Security Functions	Keys And/or SSPs	Roles	Access rights to keys and/or SSPs	Indicator
Perform Self-tests	Perform on-demand Power-up Self Tests by power cycling the cryptographic module	A3369, A2502, A3310, A2537, A2538, A2539, A2415, A2416, AES 3844	None	Crypto	All ephemeral keys/CSPs – Z	N/A
Alarms Monitoring	Allows users to view active alarms via SNMPv3 interfaces	N/A	None	Crypto	N/A	N/A
Events Monitoring	Allows the user to view all logged events associated with their permissions via SNMPv3 interfaces	N/A	None	Crypto	N/A	N/A
11QPEN4 Line Port WKAT Provisioning	Allows the crypto user to provision and configure the WKAT via SNMPv3 interface	KTS	11QPEN4 Session KAT key (WKAT Authentication String)	Crypto	W	Log entry, Command execution returns success indicator
11QPEN4 Line Port Encryption Key Provisioning	Allows the crypto user to provision and switch the Encryption Key via SNMPv3 interface	KTS	11QPEN4 Session Encryption Key	Crypto	W	Log entry, Command execution returns success indicator
11QPEN4 Line Port Encryption State Provisioning	Allows the user to provision and configure the facility information associated with 11QPEN4 cards via SNMPv3	N/A	None	Crypto	N/A	N/A
S13X100E Line Port WKAT Provisioning	Allows the crypto user to provision and configure the WKAT via SNMPv3 interface	KTS	S13X100E Session KAT key (WKAT Authentication String)	Crypto	W	Log entry, Command execution returns success indicator
S13X100E Line Port Encryption Key Provisioning	Allows the crypto user to provision and switch the Encryption Key via SNMPv3 interface	KTS	S13X100E Session Encryption and Authentication Key	Crypto	W	Log entry, Command execution returns success indicator
S13X100E Line Port Encryption State Provisioning	Allows the user to provision and configure the facility information associated with S13X100E cards via SNMPv3	N/A	None	Crypto	N/A	N/A
2UC400E Line Port WKAT Provisioning	Allows the crypto user to provision and configure the WKAT via SNMPv3 interface	KTS	2UC400E Session KAT key (WKAT Authentication String)	Crypto	W	Log entry, Command execution returns success indicator
2UC400E Line Port Encryption Key Provisioning	Allows the crypto user to provision and switch the Encryption Key via SNMPv3 interface	KTS	2UC400E Session Communication Authentication Key	Crypto	W	Log entry, Command execution returns success indicator
2UC400E Line Port Encryption State Provisioning	Allows the user to provision and configure the facility information associated with 2UC400E cards via SNMPv3	N/A	None	Crypto	N/A	Log entry, Command execution returns success indicator
Zeroize Keys	Zeroize keys and CSPs over SNMPv3 interfaces	N/A	SNMPv3 Passphrase SNMPv3 Authentication Key SNMPv3 Privacy Key 11QPEN4 Session Encryption Key 11QPEN4 Session KAT Key S13X100E Session Encryption Key S13X100E Session KAT Key	Crypto	Z	Log entry, Command execution returns success indicator

Table 38 - Approved Services

Access rights:

> G = Generate: The module generates or derives the SSP.
> R = Read: The SSP is read from the module (e.g. the SSP is output).
> W = Write: The SSP is updated, imported, or written to the module.

E = Execute: The module uses the SSP in performing a cryptographic operation.
Z = Zeroise: The module zeroises the SSP.

4.3 Authentication

Role	Authentication Method	Authentication Strength
Admin	SNMPv3 Authentication	160 bit
	CLI/WebUI Authentication	160 bit
Crypto	SNMPv3 Authentication	160 bit
	CLI/WebUI Authentication	160 bit

Table 39 - Roles and Authentication

The cryptographic module only provides access to a user that assumes a role (Administrator or Crypto) and has a specific identity (username and a password). Users are required to follow password restrictions listed in the following table.

Authentication Mechanism	Keyword / Password Rules	Strength of Mechanism
SNMPv3 username and keyword for 1830 SMS and NMS The username should not be longer than 21 characters. The username is a human readable string and no more than 21 characters in length, there are no additional SNMPv3 standards for user restrictions.	The keyword can be from 27 to 32 characters, using upper- and lower-case letters and numeric digits 0–9. The keyword must be generated by a key generator (to guarantee the required randomness).	The SNMP v3 Crypto user is created by the user manually at system turn-up. The keyword can be entered from 27 to 32 characters, upper and lower letter case and numeric. There are 26 lower case plus 26 upper case plus 10 digits for a total of 62 characters: with a minimum keyword length of 27, the minimum combinations that are possible are 2,481E+48 or 62^{27}. The fastest network connection supported by the module is 100 Mbps. Hence at most ($100 \times 10^6 \times 60 = 6 \times 10^9$) = 6,000,000,000 bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is 1 : 62^{27} possible keywords / ((6×10^9 bits per minute) / 64 bits per keyword)), which is 1: 2,481E+48 possible keywords / 93,750,000 keywords per minute), which is 1: 2,646E+40, which is a smaller probability than 1:100,000 as required by FIPS 140-3.
CLI username and password Usernames are strings of 5 to 12 case-sensitive alphanumeric characters where the first character is an alphabetic character. The following special characters are also valid: • % (percent) • + (plus sign) • # (pound sign) • _ (underscore)	Minimum password length is 12 characters. There are 26 lower case plus 26 upper case plus 10 digits plus 14 special characters for a total of 76 characters. A password is a case-sensitive string of 12 to 32 alphanumeric characters having at least one of the following: • at least one lowercase alphabetic character • at least one uppercase alphabetic character • at least one numeric character • at least one special character The following special characters are valid: % (percent) + (plus sign) # (pound sign) _ (underscore)	(26 lower case + 26 upper case + 10 digits + 14 special characters) = 76 characters X a minimum password length of 12. 76^{12} = 37,133,262,473,195,501,387,776 After a failed login attempt, the system delays the next login prompt. With this delay, a maximum of 31 attempts can occur in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is 1: 37,133,262,473,195,501,387,776 possible passwords / 31 passwords per minute) = 1:1,197,847,176,554,693,593,154 which is a smaller probability than 1 in 100,000 as required by FIPS 140-3.

NOKIA

	! (exclamation mark) @ (at sign) $ (dollar sign) " (double quotation mark) & (ampersand) ' (apostrophe) ((left parenthesis)) (right parenthesis) (asterisk) . (period) The first character of the password can be any alphabetic, numeric, or a valid special character. The New Password cannot be the same as or the reverse of the associated username and the password must not have three consecutive identical characters.	

Table 40 - Strengths of Authentication Mechanisms

5   Software/Firmware security

A Nokia-Generic is the means to store software and firmware for a PSS-8/16II/32/24x/8x or PSI-8L system. The Nokia-Generic consists of a number of RPMs and each RPM contains a number of files.

5.1   Securing RPMs

Each RPM is protected in integrity and authentication (proof of origin) using a digital signature based on:

- SHA-512 [FIPS 180-4] for the hash function
- RSA-PSS [FIPS 186-4] with 4096-bits asymmetrical key for the signature calculation using a 512-bit salt (random value)

An RPM is checked when it is brought onto the module.

5.2   Securing Files

Each file is protected in integrity using an integrity check based on

- SHA-256 for the hash function

All files are checked a start-up of the module.

6 Operational environment

The operational environment is non-modifiable.

6.1 Operating System and Hardware Platforms

For the used Operating Systems and Hardware Platforms, please refer to chapter 2 "Cryptographic module specification".

6.2 Provision 1830 PSS and 1830 PSI-8L for FIPS 140-3 Secure Mode of Operation

To put the 1830 PSS or 1830 PSI-8L into the secure mode of operation use the procedure described in the respective "Installation and System Turn-Up Guide", in chapter "Security hardening guidelines for approved configurations" according to the following table:

Tested Platform	ITUG document to be used
PSS-32	[PSS-32 ITUG]
PSS-16II	[PSS-16II ITUG]
PSS-8	[PSS-8 ITUG]
PSS-24x	[PSS-24x ITUG]
PSS-8x	[PSS-8x ITUG]
PSI-8L	[PSI-8L ITUG]

Table 41 - Operational Environment - document reference for secure mode of operation

The steps needed to put the module in the secure mode of operation are shown in chapter 16.1.1 "Procedure: Provision for Approved Mode of Operation".

6.3 Approved Mode

When configured as specified in Section 16.1 of the Security Policy, the module supports only one mode of operation: the Approved mode.

7 Physical security

7.1 Overview

Physical security is provided compliant to FIPS 140-3 security level 1.

7.2 Physical boundary

The cryptographic boundary of the 1830 PSS shelves is

- PSS-8: Shelf and Shelf Cover and Shelf Panel
- PSS-16II, PSS-32: Shelf and Shelf Cover and User Panel
- PSS-24x (ETSI version): Rack (shelf is inside the rack)
- PSS-24x (ANSI variant): Shelf and Shelf Cover
- PSS-8x (ANSI variant): Shelf (can be with Shelf Cover)
- PSI-8L: Shelf

7.3 Physical Security Mechanisms

The multi-chip standalone cryptographic module includes the following physical security mechanisms:

- Production-grade components and production-grade opaque enclosure with tamper-evident labels.
- Provision the cryptographic module to operate in approved mode: refer to chapter 6.1 "Operating System and Hardware Platforms
- For the used Operating Systems and Hardware Platforms, please refer to chapter 2 "Cryptographic module specification".
- Provision 1830 PSS and 1830 PSI-8L for FIPS 140-3 Secure Mode of Operation" for detailed instructions.
- all unpopulated slots are equipped with filler cards

8 Non-invasive security

The module claims no non-invasive security techniques.

Security Policy
October 28, 2024   Copyright 2021-2023 © Nokia   1.2
Page 44 of 65

9 Sensitive security parameter management

List of SSPs:

Key/ SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import /Export	Establishment	Storage	Zeroisation	Use & related keys
SNMPv3 Passphrase	Minimum: 27 characters, 32 chars: 190 bits	N/A	N/A	Input in encrypted form via CLI or WebUI Never exits the module	AD/EE KTS	Plaintext in volatile memory	Reboot; power-cycle	Derivation of SNMPv3 privacy and authentication keys
SNMPv3 Privacy Key	256-bits	AES CFB128 Encryption/ Decryption A2502	N/A	Never exits the module	Derived internally using SNMP KDF	Local database cleartext	Zeroized when SNMPv3 passphrase is updated with a new one	Encrypting SNMPv3 packets
SNMPv3 Authentication Key	160-256 bits	Keyed-Hash Message Authentication A2502	N/A	Never exits the module	Derived internally using SNMP KDF	Local database cleartext	Zeroized when SNMPv3 passphrase is updated with a new one	Authenticating SNMPv3 packets
11QPEN4 Session Encryption Key (AES-256 key)	256-bits	AES-CTR, AES-GCM A2537, A2539	Imported across encrypted SNMPv3 link from KM	Imported Encrypted, no Export	AD/EE KTS	Stored in write only device registers in FPGA	Zeroized on module reset and key switches to new keys	Used to encrypt traffic data
S13X100E Session Encryption and Authentication Key (AES-256 key)	256-bits	AES-CTR, AES-GMAC AES 3844	Imported across encrypted SNMPv3 link from KM	Imported Encrypted, no Export	AD/EE KTS	Stored in write only device registers in FPGA	Zeroized on module reset and key switches to new keys	Used to encrypt traffic data
2UC400E Session Encryption Key (AES-256 key)	256-bits	AES-CTR, AES-GMAC AES 3844	Imported across encrypted SNMPv3 link from KM	Imported Encrypted, no Export	AD/EE KTS	Stored in write only device registers in FPGA	Zeroized on module reset and key switches to new keys	Used to encrypt traffic data
11QPEN4 Session KAT key (WKAT Authentication String) (Hexadecimal-Alpha-Numeric-String)	N/A	AES-ECB A2537, A2539	Imported across encrypted SNMPv3 link from KM	Exits the module in plaintext over secured SNMPv3 link	AD/EE KTS	Stored within module in plain text in EC flash memory and in ASIC	Zeroized when new string is entered or when service is deleted	Used to authenticate traffic data connection

Key/ SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import /Export	Establishment	Storage	Zeroisation	Use & related keys
S13X100E Session KAT key (WKAT Authentication String) (Hexadecimal-Alpha-Numeric-String)	N/A	AES-ECB AES 3844	Imported across encrypted SNMPv3 link from KM	Exits the module in plaintext over secured SNMPv3 link	AD/EE KTS	Stored within module in plain text in EC flash memory and in ASIC	Zeroized when new string is entered or when service is deleted	Used to authenticate traffic data connection
2UC400E Session KAT key (WKAT Authentication String) (Hexadecimal-Alpha-Numeric-String)	N/A	AES-ECB AES 3844	Imported across encrypted SNMPv3 link from KM	Exits the module in plaintext over secured SNMPv3 link	AD/EE KTS	Stored within module in plain text in EC flash memory and in ASIC	Zeroized when new string is entered or when service is deleted	Used to authenticate traffic data connection
S13X100E Session Communication Authentication Key (AES-256 key)	256-bits	HMAC-SHA2-256 A2415	S13X100E Session Encryption and Authentication Key is used	No Import, no Export	N/A	Stored AES-256 encrypted in module RAM	Zeroized on module reset and key switches to new keys	Used to authenticate (with HMAC-SHA256) information exchanged between modules
2UC400E Session Communication Authentication Key (AES-256 key)	256-bits	HMAC-SHA2-256 A24156	2UC400E Session Encryption Key is used	No Import, no Export	N/A	Stored AES-256 encrypted in module RAM	Zeroized on module reset and key switches to new keys	Used to authenticate (with HMAC-SHA256) information exchanged between modules
User Passwords	Minimum: 12 characters 32 chars= 199	N/A	Entered in module via CLI or Web UI	Entered Encrypted, no Export	N/A	Local database plaintext	Zeroized when password is updated with a new one Return-to-Factory Command	Authentication of Users
AES GCM IV	96-bit	AES-GCM A3369	Generated internally	Never exits the module	N/A	Plaintext in volatile memory	Reboot; power-cycle	IV for AES GCM
DH Private Key Component	112-200 bits	DH Shared Secret Computation A3369	Generated internally via Approved DRBG	Never exits the module	N/A	Plaintext in volatile memory	Reboot; power-cycle; session termination	Generation of SSH shared secrets

Key/ SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import /Export	Establishment	Storage	Zeroisation	Use & related keys
DH Public Key Component	112-200 bits	DH Shared Secret Computation A3369	[for the module] Generated internally via Approved DRBG	[for the module] Exits the module in plaintext form [for a peer] Input in plaintext form, never exits the module	N/A	Plaintext in volatile memory	Reboot; power-cycle; session termination	Generation of SSH shared secrets
ECDH Private Key Component	128-256 bits	ECDH Shared Secret Computation A3369	Generated internally via Approved DRBG	Never exits the module	N/A	Plaintext in volatile memory	Reboot; power-cycle; session termination	Generation of SSH and TLS shared secrets
ECDH Public Key Component	128-256 bits	ECDH Shared Secret Computation A3369	[for the module] Generated internally via Approved DRBG	[for the module] Exits the module in plaintext form [for a peer] Input in plaintext form, never exits the module	N/A	Plaintext in volatile memory	Reboot; power-cycle; session termination	Generation of SSH and TLS shared secrets
SSH User Public Key	112-150 bits (RSA) 128-256 bits (ECDSA)	ECDSA Signature Verification RSA Signature Verification A3369	N/A	Imported in Base64 encoded (PEM) file format via WebUI or CLI	AD/EE KTS	Local database AES-128 encrypted	Zeroized when key is updated with a new one Return-to-Factory command	Public key authentication (authorized key)
SFTP SSH User Private Key	112-150 bits (RSA) 128-256 bits (ECDSA)	ECDSA Signature Generation RSA Signature Generation A3369	N/A	Imported in Base64 encoded (PEM) file format via WebUI or CLI	AD/EE KTS	Local database AES-128 encrypted	Return-to-Factory command	Public key authentication to SFTP server (Identity key)

Key/ SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import /Export	Establishment	Storage	Zeroisation	Use & related keys
SFTP Server Public Host Key	112-150 bits (RSA) 128-256 bits (ECDSA)	ECDSA Signature Verification RSA Signature Verification A3369	N/A	[for the module] Imported in Base64 encoded (PEM) file format via WebUI or CLI [for a peer] Input in plaintext form as part of SSH session negotiation Never exits the module	AD/EE KTS	Local database cleartext	Return-to-Factory command	Authentication of SFTP server (known host key)
SSH Private Key	112-150 bits (RSA) 128-256 bits (ECDSA)	ECDSA/RSA Key Generation ECDSA Signature Generation RSA Signature Generation A3369	Generated internally via Approved DRBG	Never exits the module	N/A	Local database AES-128 encrypted	Return-to-Factory command	Authentication during SSH session negotiation
SSH Public key	112-150 bits (RSA) 128-256 bits (ECDSA)	ECDSA/RSA Key Generation ECDSA Signature Verification RSA Signature Verification A3369	[for the module] Generated internally via Approved DRBG	[for the module] Exits the module in plaintext form during SSH session negotiation Exported from module via CLI or WebUI (for install on client for host key authentication) [for a peer] Input in plaintext form as part of SSH session negotiation Never exits the module	N/A	Local database AES-128 encrypted	Return-to-Factory command	Authentication during SSH session negotiation

Security Policy
October 28, 2024

Copyright 2021-2023 © Nokia
This document may be freely distributed whole and intact including this complete copyright notice

1.2
Page 48 of 65

Key/ SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import /Export	Establishment	Storage	Zeroisation	Use & related keys
SSH Shared Secret	112-200 bits (FFC) 128-256 bits (ECC)	KAS-FFC-SSC, KAS-ECC-SSC Shared Secret Computation A3369	N/A	Never exits the module	KAS-FFC-SSC KAS-ECC-SSC Shared Secret Computation	Plaintext in volatile memory	Reboot; power-cycle; session termination	Derivation of the SSH Session Key and SSH Authentication Key
SSH Session Key	128-256 bits	AES-CTR AES-GCM Encryption/Decryption A3369	N/A	Never exits the module	SSH KDF used to derive keying material	Plaintext in volatile memory	Reboot; power-cycle; session termination	Encryption and decryption of SSH session packets
SSH Authentication Key	256-512 bits	Keyed-Hash Message Authentication A3369	N/A	Never exits the module	SSH KDF used to derive keying material	Plaintext in volatile memory	Reboot; power-cycle; session termination	Authentication of SSH session packets
CA Public Key	112-150 bits	RSA Signature Verification A3369	Generated externally	Imported in Base64 encoded (PEM) file format via WebUI or CLI	AD/EE KTS	Local database AES-128 encrypted	Zeroized when certificate is updated with a new one Return-to-Factory command	Verification of CA signatures
TLS Private Key	112-150 bits	RSA Key Generation/RSA Signature Generation A3369	Generated internally via Approved DRBG	Never exits the module		Local database AES-128 encrypted	Return-to-Factory command	TLS authentication
TLS Public Key	112-150 bits	RSA Key Generation/RSA Signature Verification A3369	[for the module] Generated internally via Approved DRBG	[for the module] Exits the module in plaintext form [for a peer] Input in plaintext form as part of TLS session negotiation Never exits the module		[for the module] Local database AES-128 encrypted [for a peer] Plaintext in volatile memory	Return-to-Factory command	TLS authentication 1024-bit RSA public keys are used for signature verification only
TLS Pre-Master Secret	128-256 bits	KAS-ECC-SSC Shared Secret Computation A3369	N/A	Never exits the module	Derived internally via KAS-ECC-SSC Shared Secret Computation	Plaintext in volatile memory	Reboot; power-cycle; upon completion of TLS Master Secret computation	Derivation of the TLS Master Secret

Key/ SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import /Export	Establishment	Storage	Zeroisation	Use & related keys
TLS Master Secret	128-256 bits	KAS-ECC-SSC Shared Secret Computation A3369	N/A	Never exits the module	Derived internally using the TLS Pre-Master Secret via TLS KDF	Plaintext in volatile memory	Reboot; power-cycle; session termination	Derivation of the TLS Session Key and TLS Authentication Key
TLS Session Key	128, 256	AES-CBC. AES-GCM Encryption/ Decryption A3369	N/A	Never exits the module	Derived internally using the TLS Master Secret via TLS KDF	Plaintext in volatile memory	Reboot; power-cycle; session termination	Encryption and decryption of TLS session packets
TLS Authentication Key	256-384 bits	Keyed-Hash Message Authentication A3369	N/A	Never exits the module	Derived internally using the TLS Master Secret via TLS KDF	Plaintext in volatile memory	Reboot; power-cycle; session termination	Authentication of TLS session packets
DRBG Seed	384 bits	Random number generation A3369	Entropy from ESV (Cert #26) approved platform noise source.	Never exits the module	N/A	Plaintext in volatile memory	Reboot; power-cycle	Random seed data drawn from Nokia Jitter Entropy(JENT) and used to seed an implementation of the NIST SP 800-90Ar1 CTR (AES) DRBG.
DRBG Key 256-bit AES key	256 bits	Random number generation A3369	Internal state generated using CTR_DRBG from [SP800-90Ar1].	Never exits the module	N/A	Plaintext in volatile memory	Reboot; power-cycle	32 bytes AES key stored in the RAM. Used in an implementation of the NIST SP 800-90Ar1 CTR (AES) DRBG.
DRBG V	128 bits	Random number generation A3369	Internal state generated using CTR_DRBG from [SP800-90Ar1].	Never exits the module	N/A	Plaintext in volatile memory	Reboot; power-cycle	Part of the secret state of the approved DRBG. The value is generated using the methods described in [SP800-90Ar1].

Key/ SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import /Export	Establishment	Storage	Zeroisation	Use & related keys
Entropy Input String	256 bits	Entropy Source for Random number generation E26	Generated internally	Never exits the module	N/A	Plaintext in volatile memory	Reboot; power-cycle	Random number generation
Firmware Load Authentication Key	N/A	RSA Digital Signature Verification A3369	N/A	N/A	N/A	Hardcoded/embedded in the application firmware image	N/A	Self-Test
SNMP Certificate Fingerprint	256-512 bits	Secure Hash A3369	N/A	Imported in hex format over CLI or WebUI	AD/EE KTS	Local database cleartext, certificate fingerprint only	Zeroized when certificate fingerprint is updated with a new one Return-to-Factory command	SNMPv3 user authentication for SNMP over TLS
Database Encryption Key	128-bit	AES-CBC A3369	N/A	N/A	N/A	Hardcoded/embedded in the application firmware image	Return-to-Factory Command	Encryption of SSPs in local database

Table 42 - SSPs

Note: all SSPs are zeroized via the Return-to-Factory CLI command.

Note: The AES-GCM IV is used in the TLS and SSH protocol. For TLS, the AES-GCM IV is internally generated deterministically in compliance with TLSv1.2 GCM cipher suites as specified in RFC 5288 and Section 8.2.1 of NIST SP 800-38D. Per RFC 5246, when the nonce_explicit part of the IV exhausts the maximum number of possible values for a given session key, the module will trigger a handshake to establish a new encryption key. The module is compatible with TLSv1.2 and supports acceptable GCM ciphersuites from Section 3.3.1 of SP 800- 52 Rev 2. For SSH, the AES GCM IV is constructed in compliance with the SSHv2 specification (RFCs 4252, 4253 and 5647) and only for use within the SSHv2 protocol.

RBG entropy sources:

Entropy sources	Minimum number of bits of entropy	Details
8EC2	256	JENT is used as entropy source
32EC2	256	JENT is used as entropy source
CEC2	256	JENT is used as entropy source
XCEC8	256	JENT is used as entropy source
MEC2L	256	JENT is used as entropy source

Table 43 - Non-Deterministic Random Number Generation Specification

10 Self-tests

The 1830 PSS-32/PSS-16II/PSS-8/24x and PSI-8L perform known answer tests and critical functions tests at power up.

Test	Description
AES Encrypt KAT	Encrypt Known answer test for AES-256 CFB-128.
AES Decrypt KAT	Decrypt Known answer test for AES-256 CFB-128.
AES Encrypt FPGA KAT (11QPEN4 cards)	Encrypt Known answer test for AES-256 CTR.
AES Decrypt FPGA KAT (11QPEN4 cards)	Decrypt Known answer test for AES-256 CTR.
AES Encrypt ASIC KAT (S13X100E cards)	Encrypt Known answer test for AES-256 GMAC.
AES Decrypt ASIC KAT (S13X100E cards)	Decrypt Known answer test for AES-256 GMAC.
SHA KAT	Known answer test for SHA-1
HMAC-SHA-1 KAT	Known answer test for HMAC-SHA-1
HMAC-SHA256 KAT	Known answer test for HMAC-SHA256
OpenSSL self-test (Nokia openSSL)	Details see below

Table 44 - Self-tests

Pre-Operational Self-Tests
- OpenSSL Integrity Test – using HMAC-SHA2-256
- Application Firmware Integrity Test – using error detection code (SHA2-256)

Conditional Cryptographic Algorithm Self-Tests (performed at power-up)
- OpenSSL library
  - AES encrypt KAT (ECB mode)
  - AES decrypt KAT (ECB mode)
  - AES GCM encrypt KAT
  - AES GCM decrypt KAT
  - CTR-based DRBG KAT
  - HMAC-SHA1, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512 KAT
  - ECDSA signature generation KAT OR ECDSA signature verification KAT
  - RSA signature generation KAT
  - RSA signature verification KAT
  - SNMPv3 KDF KAT
  - SSHv2 KDF KAT
  - TLS 1.2 KDF KAT
  - FFC DH shared secret KAT (2048)
  - ECDH shared secret KAT (P-256)

- Entropy Source library
  - SHA3-256 (entropy conditioning component)

HMAC KATs with SHA-1, SHA2-256, SHA2-384, and SHA2-512 utilize (and thus test) the full functionality of the SHA-1, SHA2-256, SHA2-384, and SHA2-512 algorithms; therefore, no independent KATs for SHA-1, SHA2-256, SHA2-384, and SHA2-512 implementations are required.

Conditional Self-Tests
- Firmware Load Test using RSA 4096 digital signature verification with SHA2-512
- Entropy RCT/APT
- ECDSA PCT
- RSA PCT
- DH/ECDH Key Assurances

Critical Functions Tests
- DRBG Health Checks (performed at power-up)

11 Life-cycle assurance

11.1 Delivery & Operation

Nokia delivers the module both physically and electronically.

The hardware is delivered physically via a trusted carrier. The box is sealed by PVC adhesive tape with identification labels. A tamper free tape is also applied. The box is then belted if required.

The software and guidance documentation are retrieved electronically from a web site.

Hardware and software items associated with the module are itemized by a unique Nokia Part Number (APN). In addition, each 1830 PSS or 1830 PSI-8L shelf can be ordered as a kit with the minimum required equipment for approved operation. The kit is also specified by a unique APN.

Final versions of 1830 PSS customer documentation are posted on the Nokia Support portal, a Nokia Extranet site for internal users and external customers with entitlement. If a customer document is re-issued, the re-issue is then posted on Nokia Support portal and the previous issue of the document removed.

11.2 Crypto Officer (Admin) Commisioning Guidance

The approved mode of operation has to be prepared by the Crypto Officer (Admin) by following the instructions in chapter 15 and chapter 16.

If the module starts up successfully, then the module has passed all self-tests (described in chapter 10) and is operating in the approved mode of operation

11.3 Decommissioning the module

When a zeroization of all SSPs is needed, because the module shall be decommissioned or taken out of the secured mode of operation, then the Return-to-Factory procedure can be used.

Please note, that this erases also all Firmware and thus leads to a need to send the equipment back to the factory before the next use. For details refer to chapter 16.4.

12 Mitigation of other attacks

The module has not been designed to mitigate any specific attacks beyond the scope of FIPS 140-3 requirements.

13 Acronyms

AES	Advanced Encryption Standard
AGD	Assurance Guidance Documents
ALC	Assurance Life Cycle
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CIA	Confidentiality, Integrity and Availability
CC	Common Criteria
CIT	Craft Interface Terminal
CLI	Command Line Interface
COE	Central Office Equipment
CPE	Customer Premises Equipment
CT	Commercial Temperature
DWDM	Dense Wavelength Division Multiplexing
EC	Equipment Controller
FC	Fibre Channel
GE	Gigabit Ethernet
KAT	Known Answer Test
KM	Key Manager
NE	Network Element
NM	Network Manager

NOC	Network Operations Center
OAMP	Operations, Administration, Maintenance and Provisoning
OTU	Optical Transport Unit
PP	Protection Profile
PSS	Photonic Service Switch
QPEN	Quad Pluggable ENcryption
RBAC	Role Based Access Control
RFS	Remote File Server
SFR	Security Functional Requirement
SNMP	Simple Network Manager Protocol
ST	Security Target
TOE	Target of Evaluation
T-ROADM	Tunable-Reconfigurable Optical Add/Drop Mulitplexer
TSF	TOE Security Functions
UID	User Identifier
VOA	Variable Optical Attenuator
VOIP	Voice over Internet Protocol
WKAT	Well Known Answer Test
XFP	eXtended Form-factor Pluggable

Table 45 - Acronyms

14 References

FIPS	
[FIPS 140-3]	FIPS PUB 140-3, *Security Requirements for Cryptographic Modules*
[FIPS 140-3 DTR]	Derived Test Requirements for FIPS PUB 140-3, *Security Requirements for Cryptographic Modules*
[FIPS 140-3 IG]	Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program
NIST	
[NIST800-38A]	Recommendation for Block Cipher Modes of Operation: Methods and Techniques - NIST Special Publication 800-38A
[NIST800-38D]	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC - NIST Special Publication 800-38D
[NIST800-38F]	Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping - NIST Special Publication 800-38F

15 Appendix A – Installing Tamper-evident labels

Installing tamper labels is not needed for FIPS 140-3 security level 1.

16 Guidance – System Configuration Procedures

16.1 Provisioning the 1830 PSS and 1830 PSI-8L

16.1.1 Procedure: Provision for Approved Mode of Operation

16.1.1.1 Overview

16.1.1.2 Purpose

This procedure describes how to configure the NE in order to comply with the Federal Information Processing Standards (FIPS) Publication 140-3 (Security Requirements for Cryptographic Modules), detailing the U.S and Canadian governments' requirements for cryptographic modules.

16.1.1.3 Preconditions

16.1.1.4 Communication environment

Important! Until the NE is secured by performing the steps described up to and including chapter **Error! Reference source not found.**,

it must not be connected to a LAN in order to avoid vulnerabilities.

For approved configuration, the NE must run an ECN software load.

When the NE is operational, the NE, along with the whole communication network, must be under restricted access. Internet access must be disabled, and access within the customer DCN must be restricted to selected systems, for example the NMS and computers of administrators.

The Gateway NE (GNE) does have a rudimentary firewall, but the PSS network should also be protected from network attacks, such as Denial of Service attacks or rogue packets. This protection is typically implemented at the DCN router that connects to the GNE. Additionally, IPSec tunneling between the DCN router and the management system(s) is recommended.

16.1.1.5 NE status

The NE is properly installed and running: The NE is physically assembled, and the software is installed. The NE has booted and can be accessed via CIT.

16.1.1.6 Environment security

Any equipment used to access the NE must be secured through the current state of the art security measures. This applies to computers that the 1830 PSS WebUI user interface or WS-NOC run on, but also, to the use of input devices for such computers.

Note: A *cordless* mouse or keyboard cannot be considered secure.

The OWASP (Open Web Application Security Project) community, among others, can provide the best practices in regard to this topic.

16.1.1.7 Communication with the NE

All communication from/to the Management System(s) can be secured using an IPSec tunnel. This is an additional security measure that is not required for most communication channels. The communication channels where this is mandatory, are explicitly shown in the respective chapters. Irrespective of the use of IPSec tunnel, secure protocols (SSH, SNMPv3, HTTPS, etc.) should be used to connect to the NE.

The IPSec tunnel is set up between the management system(s) and a DCN router placed next to the NE. From the DCN router to the NE, there is no IPSec tunnel possible, so this physical connection must be physically secured.

Note: The approved configuration allows secure communication protocols at the OAMP interface only.

16.1.1.8 General steps

16.1.1.9 Before you begin

Refer to the *1830 Photonic Service Switch (PSS) Release 22.12 Command Line Interface Guide* for more detailed information regarding the CLI commands used in this chapter.

16.1.1.10   Preparation

When the NE is connected to a DCN while the default user account passwords were not yet changed or ZTP enabled, and keys not set, the NE might be compromised.

Required steps:

1. Disconnect the NE from DCN, if the NE was connected to the DCN before.

2. If the security was already compromised (e.g., illegitimate user accounts were created), the system shall be reset to an initial status wiping out all configuration data. After this, restart the system turn-up procedure.

The following command resets the system:
```
config admin factory-reset
2. From the serial console of the active EC cryptographic module, access CLI as the
default administrator 'admin'.  Set the NE TID."
3. From the serial console of the active EC, login to CLI as default administrator
'admin'.
Execute the following CLI command to set the OAMP IP address.
config interface usrpnl oamp ip <ipaddress/mask>
```

16.1.1.11   Configuration access: CIT

```
Required steps must be executed using a locally connected Craft Interface Terminal
(CIT) in order
to avoid interference from DCN before the NE is secured.
```

16.1.1.12   NE keys

```
NE keys and certificates must be generated.
```
Required steps:
```
1. Generate an SSH key.
crypto key generate all
2. Generate an SSL key (note: SSL means really TLS).
crypto sslkey generate keytype rsa keylen 2048
```

```
3. Get and install a signed TLS X.509v3 certificate. Refer to chapter 16.1.1.13
for more detailed information.
Note: When the NE is security hardened it can be connected to the LAN.
Note: Please refer to the User Provisioning Guide for more information.
```

16.1.1.13   Signed SSL/TLS X.509v3 certificate

In section **Error! Reference source not found.**, an SSL/TLS key was generated.
Create a signed X.509v3 certificate for the NE based on this SSL/TLS key.
Required steps:
Create a signed X.509v3 certificate and load it onto the NE.
Use the following commands:
1. Generate a CSR (Certificate Signing Request):

config sslcsr generate

2. Provision Subject Alternative Names (SAN) if SAN authentication/server authentication is
required on the peer.

config sslcsr san {add | delete} {<ip-address> |<domain>}

3. Upload the CSR to a file server:

**config software server transfer < ip address of server:
example 135.104.252.100>**

config software server transfer protocol sftp

**config software server transfer userid < user-id-for-
server>**

**config software server transfer root <example path:
/home/sw1/ SAN8CSR.csr>**

config software server transfer detail

config software server transfer load sslnecsr

4. Create the certificate by signing the CSR by an external CA (Certificate Authority).
5. Download the signed certificate to the NE:

config software server transfer protocol sftp

**config software server transfer userid < user-id-for-
server>**

**config software server transfer root <example path:
/home/sw1/ SAN8certificate.pem>**

```
config software server transfer load sslomscsr
```
6. Install downloaded certificate:
```
config sslcert yes
```
Be sure to install the NE root certificate on any clients connecting to the WebUI
Note: Please refer to the *User Provisioning Guide* for more information.

16.1.1.14 Secure mode
In order to enforce secure (encrypted) protocols, the NE must be set to secure mode.
Required step:
1. Set NE to secure mode via CLI:
```
config admin ui mode encrypted
```

16.1.1.15 User and account administration for NE management
16.1.1.16 TL1, CLI, WebUI, NETCONF/gRPC
System security settings
The following settings are **required** to help enforce better security.
```
config admin session maxfailedlogins 5
config admin authentication local password minlength 12
config admin session timeout 15
config admin maxsession 1
config admin minwaitlogin 15
```
Default local accounts
At the time of NE deployment, there are two default accounts: admin and service.
admin: The admin account is used to initially configure the NE. This includes creation of additional accounts to manage the NE.
service: The service account is used by Nokia service personnel to install the NE and perform maintenance activities.
Required steps:
1. Change the default admin password.
config admin users edit admin passwd
2. Create a non-default account with administrative privileges to be used instead of the default admin account. For example, to create a user named "adminjoe" with administrative privileges, use the following command:
config admin users add adminjoe administrator
Note: Should you lose the new password, or disable the users, no maintenance access to the system will be available in case of emergency.
It is recommended to always create new users with Administrative privilege for periodic work, and to disable the default user permanently.
Recommended steps:
1. Disable the default admin account.
    config admin users edit admin status disabled
2. Disable the default service account.
    config admin users edit service status disabled

16.1.1.17 SNMP
The following steps must be executed regardless if the NE is to be managed using SNMP or not.
Accounts for SNMP are maintained by the NE.
Internal accounts
Important! The SNMP user accounts **v3IntComDefUser** is used for internal purposes. It must not be changed or removed.
Default accounts
At the time of NE deployment, there are two default accounts: **v3DefaultUser** and **v3DftAdvUser**.
Required steps:
1. Disable default accounts：
```
config admin snmpusers edit v3DftAdvUser status disabled
config admin snmpusers edit v3DefaultUser status disabled
```
Other predefined accounts
If the NE was connected to a DCN before it was secured, other accounts might have been created.

If other accounts than the default accounts are present, then those accounts must be deleted unless there is a clear and acceptable reason for them to be there.

Required step:

1. Check for additional accounts and delete all non-default accounts (unless they are legitimate).

User-defined accounts

Required steps:

1. Create SNMP accounts as needed for accessing management systems.

2. Configure security options and passwords in alignment with accessing management systems.

WS-NOC related accounts

WS-NOC connection is not required. If WS-NOC is used, one SNMP user account is needed for the WS-NOC to manage the NE. The WS-NOC account is an SNMPv3 user.

Required steps:

1. Create an SNMPv3 user with the following commands:

```
config admin snmpusers add newnfmuser120 admin aes256sha256
config admin snmpusers edit newnfmuser120 privpasswd
```

16.1.1.18　Open Agent

The Open Agent provides the NETCONF/gRPC interface and is disabled by default. If the Open Agent is enabled, disable it.

Required step:

1. If it was enabled, use the following command to disable Open Agent:

```
config general openagent disabled
```

16.1.1.19　ZTP (Zero Touch Provisioning)

By default, ZTP is enabled. Disable ZTP mode.

Required step:

1. Disable ZTP via an Admin CLI account:

```
config admin ztp disable
```

16.1.1.20　FIPS squelching

Enable fips-squelching mode.

Required step:

1. In CLI, enter:

```
config general fips-squelching enable
```

16.1.1.21　Maintenance accounts

Accounts for maintenance are maintained by the NE. Those accounts are to be distinguished from TL1/CLI/WebUI, SNMP, or GMPLS CP accounts.

Default accounts

At the time of NE deployment, there are two default accounts: **maint1** and **maint2**. The default status is that they are disabled.

Required steps:

1. Disable remote access to **maint1** if it is enabled.

```
config admin system maint1 disable
```

2. Change the default passwords.

Use an Admin CLI account to change the passwords of **maint1** and **maint2**:

```
config admin system maint1 <password>
config admin system maint2 <password>
```

Note: Passwords must available when required for action by service personnel and kept in a safe area.

Recommended step:

1. Disable remote access to **maint2** if it is enabled.

maint2 has less access rights than **maint1** and could be used for remote access while remote access for **maint1**is disabled. Still, the disabling of remote access to **maint2** is recommended.

To disable the remote access to **maint2**, use an Admin CLI account to execute:

16.1.1.22　`config admin system maint2 disable`Disable local serial console

The local serial console can be used for local maintenance actions. For the login the maint1 user

will be used. It is required that it is either managed by the autostate feature [see 16.1.1.28] or permanently disabled. To disable it, execute the following command:

```
config admin system maint1 localdisable
```
Note: If all management protocols at the OAMP interface and remote maintenance logins
have failed or are disabled, then no maintenance access is possible anymore - neither remote nor local.
If the local serial console is enabled, it will be notified by the standing condition MAINT-ALLOWEDLOCAL. The default severity is NR (not reported). It appears in the condition list and logs only. If the severity shall be increased to MJ (major), CR (critical) or WR (warning), then it is automatically present in the alarm list because the FIPS status of the NE is violated in case it is open.

16.1.1.23 Remote access is now safe

16.1.1.24 Precondition

The required steps described in the preceding sections of the security hardening guidelines were executed. This means that the NE is now hardened to a degree that it is safe to connect to a general network.

16.1.1.25 Allow remote access to the NE

The next steps can be done using any management access type that has a secure connection. Configuration access via remote access is now safe, and you may connect to a LAN now.
Note: The DCN is secured, using IP ACL throughout the DCN (see DCN Guide for concepts and instructions).

16.1.1.26 Physical security

16.1.1.27 Introduction

The NE must be in a secure network; see chapter 16.1.1.4. In addition, the communication channel in and out of the NE must be restricted.

16.1.1.28 Customer LAN ports, Embedded Communication Channel (ECC)

Recommended steps:

1. Assign IP Address to OAMP port of TOE:

```
config interface mfc shelf/slot/oamp <ip address for the
TOE>
```

```
config cn routes default add <ip address for DHCP server>
```

16.1.1.29 Services

16.1.1.30 Introduction

The following services should only be enabled if they are used. If they are not used, they should be disabled.
The following services are covered by this document: NTP, Radius, TACACS+, SWNE, Installation from USB Stick, SFTP Client, OSPF, Syslog, SNMP Traps, GMPLS CP, ZTP.

16.1.1.31 NTP with authentication

To authenticate the NTP server(s), a key must be provisioned per NTP server used.
Required steps:
1. Establish an authentication key on each NTP server.
2. Provision each NE receiving time from that server with the authentication key.
Note: The length of the NTP Key must be at least 12 characters and the NTP Key hash type must be SHA-1 (Secure Hash Algorithm 1), not MD5 (Message-digest algorithm).

16.1.1.32 SWNE

For approved configuration, SWNE functionality must be disabled.
NEs can be in a server or in a client role.
Required step:
Disable the SWNE functionality:
1. Execute the following command:
```
config general ftpserver disable
```
Note: In case of a software update, SWNE functionality must be enabled temporarily.

16.1.1.33 Installation from USB stick

For approved configuration, use of USB ports is prohibited. The USB ports are therefore sealed and shall not be used.

Security Policy
October 28, 2024

Copyright 2021-2023 © Nokia

This document may be freely distributed whole and intact including this complete copyright notice

1.2

Page 61 of 65

16.1.1.34　Bluetooth access
The NE can be accessed via bluetooth using a bluetooth dongle. For approved
configuration, access via bluetooth must be disabled.
Required step:
1. Execute the following command to disable it:

16.1.1.35　`config interface BT state down`SFTP client
1. Provision key-based authentication which supports mutual authentication for SFTP file
transfers.
The following file transfers support this:
• SW download
```
config software server
```
• Software dynamic download
```
config software dynamic refreshserver
```
• Data backup & restore
```
config database server ip <ip address of server: example
135.104.252.100>
config database server protocol sftp
config database server userid <user-id-for-server>
config database path <example path: /home/sw1/ajayoka/DB>
```
• **Log file transfer**
```
config transferlog server ip <ip address of server: example
192.168.219.170 >
    config transferlog server protocol SFTP
    config transferlog server userid crypto
  prompted for <password>
    config transferlog server port 22
    config transferlog path /home/crypto
```
•
• Syslog file transfer
```
config admin transfersyslog server
```

• System Trust anchor installation file transfer
```
config keystore system trustanchor
```

Note: The parameters are always the same, but the commands differ. The configuration must
be done for all used services.
2. Provision the server and the user credentials on the server.[use server documentation]
3. Once the provisioning is complete, mutual authentication is available for SFTP.
Required steps:
1. Enable SFTP only if needed.
2. The recommended password length for the password used for the SFTP server login as a client
is 12 characters. Alternatively, use key based authentication.

16.1.1.36　SNMP traps
Required step:
1. Set the SNMP trap destination(s) for 1830 SMS.
```
config snmpserver trapdest add <snmp-server-name> <ip
address of server> 1500 3 v3 0 smsuser256
```

16.1.1.37　TLS
1. Use TLS 1.2:
```
config admin security tls tls-system version max 1.2
config admin security tls tls-system version min 1.2
config admin security commit
```

Security Policy
October 28, 2024
Copyright 2021-2023 © Nokia
This document may be freely distributed whole and intact including this complete copyright notice
1.2
Page 62 of 65

16.2 Periodically Check Log Files

The NE stores information in various log files. This log files should be periodically checked.

Recommended step:

1. Check log files periodically for anomalies.

Show logs all

16.3 On-demand Self-test

A FIPS self-test can be initiated by power cycling the system. (This action will impact service until system fully boots up.)

After starting, verify the status of the self-test.

FIPSSFMISMATCH or AESFIPSFAILURE conditions must not appear.

show condition

16.4 • De-Provisioning the 1830 PSS and 1830 PSI-8L

16.4.1 Procedure: Zeroization of All SSPs

16.4.1.1 Overview

16.4.1.1.1 Purpose

This procedure describes how to zeroize all SSPs to comply with the Federal Information Processing Standards (FIPS) Publication 140-3 (Security Requirements for Cryptographic Modules), detailing the U.S and Canadian governments' requirements for cryptographic modules.

16.4.1.2 Initiate SSP Zeroization

All SSPs are zeroized when the module executes the command to return it to factory. Administrator privilege is needed to execute this command.

Required steps:

1. initiate Return-to-Factory:

```
config admin return-to-factory
```

16.4.1.3 Finish SSP Zeroization

Zeroizing all SSPs in the module takes some time, so the operator must wait for the internal steps to complete. The Zeroization process is considered completed once all controllers show their LED in Solid Red.

Required steps:

1. Wait for all controller card LEDs to show solid red.

16.5 Additional Guidance

In additional to direct guidance provided in this security policy, additional detailed guidance is available to registered customers from Nokia documentation web site at documentation.nokia.com.

Nokia Guidance	
[PSS-32 ITUG]	**1830 Photonic Service Switch (PSS-32) Release 22.12 Installation and System Turn-Up Guide** Issue Date: 2022/12/22 | Issue: 1 | Document: 3KC-71311-PBAA-TJZZA
[PSS-16II ITUG]	**1830 Photonic Service Switch (PSS-16II) Release 22.12 Installation and System Turn-Up Guide** Issue Date: 2022/12/22 | Issue: 1 | Document: 3KC-71311-PBAA-SMZZA
[PSS-8 ITUG]	**1830 Photonic Service Switch (PSS-8) Release 22.12 Installation and System Turn-Up Guide** Issue Date: 2022/12/22 | Issue: 1 | Document: 3KC-71311-PBAA-SLZZA
[PSS-24x ITUG]	**1830 Photonic Service Switch (PSS-24x) Release 22.12 Installation and System Turn-Up Guide** Issue Date: 2022/12/22 | Issue: 1 | Document: 3KC-71311-PBAA-SJZZA
[PSS-8x ITUG]	**1830 Photonic Service Switch (PSS-8x) Release 22.12 Installation and System Turn-Up Guide** Issue Date: 2022/12/22 | Issue: 1 | Document: 3KC-71311-PBAA-SKZZA
[PSI-8L ITUG]	**1830 Photonic Service Switch (PSI-4L/PSI-8L) Release 22.12 Installation and System Turn-Up Guide** Issue Date: 2022/12/22 | Issue: 1 | Document: 3KC-71311-PBAA-TLZZA

Note: the ITUG documents of R22.12 are valid for R23.3 as well.