Nokia

Nokia 1830 Photonic Service Switch (PSS)

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2

Document Version: 2.21

Table of Contents

List of Figures

List of Tables

1. Introduction

This document describes the rules for use of the highly secure Nokia 1830 PSS configurations using 11QPEN4 card and S13X100E card for high speed encryption transport when used in accordance with FIPS 140-2 level 2 requirements. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module.

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 11QPEN4 is a full height, single-slot standalone card providing transport level encryption for interconnecting datacenters via optical fiber. The card supports OTU-2 line encryption with AES-256 that can be used to provide encryption of one or more pluggable client ports including 10 GE, OTU-2, 8G and 10G Fiber Channel client signals.

The S13X100E is a full height, single-slot standalone card providing transport level encryption for interconnecting datacenters via optical fiber. The card supports OTU-4 (100G) line encryption with AES-256 and HMAC-SHA-256 that can be used to provide encryption of one or more pluggable client ports including 10GE, 40GE and 100GE client signals.

1.1 Purpose

This document covers the secure operation of the 1830 PSS-32 and 1830 PSS-16II and 1830 PSS-8 Series including initialization, roles, and responsibilities of operating the product in a secure, FIPS 140-2 compliant manner.

1.2 Versions tested

The 1830 PSS products are very flexible and various circuit cards can be used in the slots provided by the PSS-8, PSS-16II and PSS-32 chassis. The subset of circuit packs used in the test configuration is shown below.
Use of circuit packs not tested under this validation will invalidate the FIPS certification.

HW Versions:
PSS-32

- Chassis (WOM4V10GRA / 8DG59319AB)
- 32EC2E Card(8DG63583AA)
- 11QPEN4(8DG60996AA)
- S13X100E (8DG63988AA)
- Filler Card(8DG59418AA)
- Security Label Kit (8DG-6509-AAAA)

PSS-16II

Chassis (WOMR300BRA / 3KC48960AC)
32EC2E Card (8DG63583AA)
11QPEN4(8DG60996AA)
S13X100E (8DG63988AA)
Filler Card(8DG59418AA)
Security Label Kit (8DG-6509-AAAA)

PSS-8

Chassis (WOMPU00CRA / 3KC48901AA)
8EC2E Card(3KC48910AA)
11QPEN4(8DG60996AA)
S13X100E (8DG63988AA)
Filler Card(8DG59418AA)
Security Label Kit (8DG-6509-AAAA)

Firmware Version:

PSS-32, PSS-16II, PSS-8

1830PSSECE-10.1-2

Document Versions:

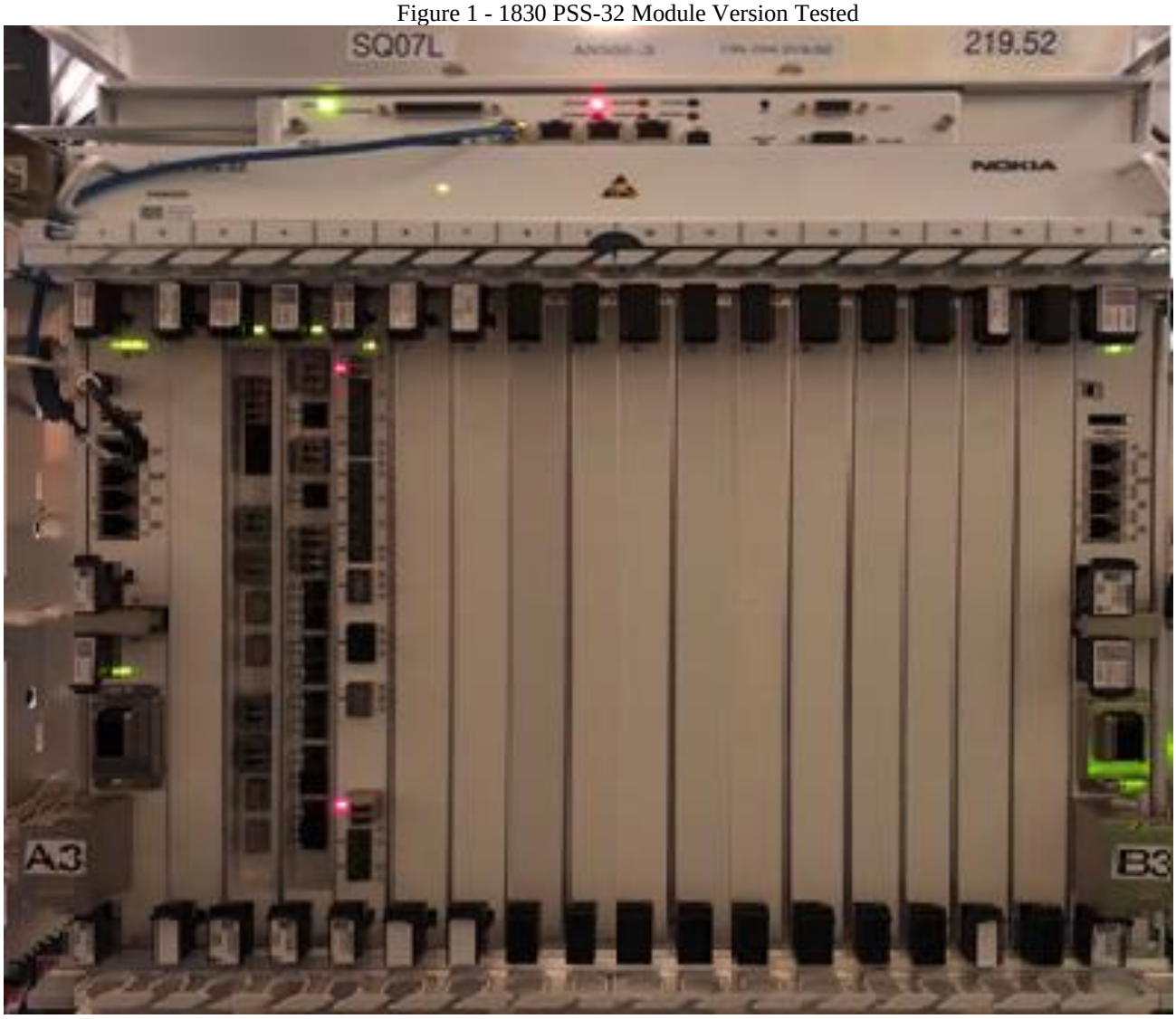
PSS-32, PSS-16II, PSS-8

1830 Photonic Service Switch (PSS) Release 10.1.2 Common Criteria User Guide (3KC-69646-KBCA-TSZZA)

1.2.1 1830 PSS-32 Version tested

The module tested is shown in Figure 1.

Figure 1 - 1830 PSS-32 Module Version Tested



1.2.2 1830 PSS-16II Version tested

The module tested is shown in Figure 2.

Figure 2 - 1830 PSS-16II Module Version Tested

1.2.3 1830 PSS-8 Version tested

The module tested is shown in Figure 3.

Figure 3 - 1830 PSS-8 Module Version Tested

2. 1830 PSS Cryptographic Module Overview

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 FIPS approved configurations of 1830 PSS consist of physically secured single shelf entities equipped with equipment controller cards and 11QPEN4 and/or S13X100E cards.

The cryptographic module is based on the encryption card 11QPEN4 and/or S13X100E installed on a single shelf version of an 1830 PSS with an Equipment Controller (32EC2E or 8EC2E).
Note, that an encrypted ODU4 path must have an S13X100E on both ends and an encrypted ODU2 path must have an 11QPEN4 on both ends. The S13X100Es and 11QPEN4s must use the same Firmware version (i.e. R10.1.2 in this case) and the same configuration (as described in chapter 3.) thus making the module bound to other modules within the same validation.
Other combinations do not work (this restriction includes equipment of other vendors).

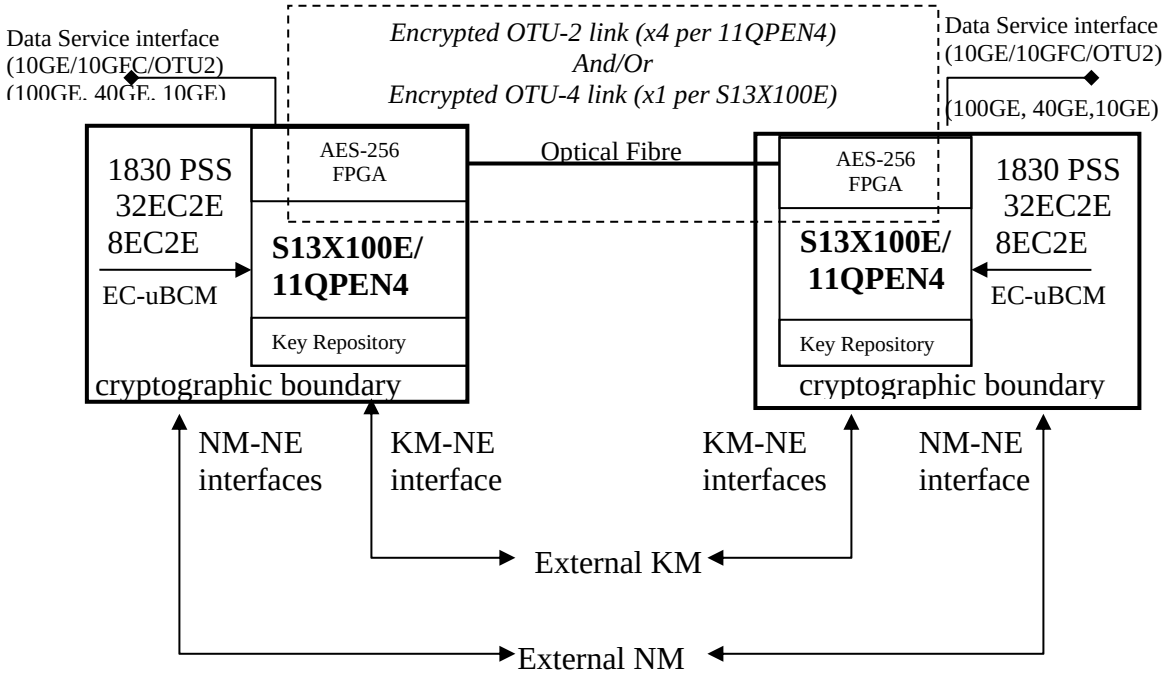


Figure 4 - Network Configuration of 1830 PSS-32/16-II/8

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 OTU2 client traffic for 11QPEN4) and (10x 10GE/OTU2,2x 40GE or 100GE/OTU4 for S13X100E) while in flight between data centers.

2.1 Cryptographic Module Specification

The cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2.

Section	Section Title	Security Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	3
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC	2
9	Self-Tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

Table 1 - Security Level Per FIPS 140-2 Section

All three of the PSS-32/PSS-16II/PSS-8 platforms are hardware modules with multi-chip standalone embodiments.

2.2 1830 Cryptographic Module Ports and Interface

FIPS 140-2 defines four logical interfaces:
• Data Input
• Data Output
• Control Input
• Status Output

2.2.1 PSS-32 Interfaces

Table 2 - FIPS 140-2 Logical Interface mapping for 1830 PSS-32

Panel	Physical Ports	Quantity	FIPS 140-2 Interface
User Panel (1) – See Figure 5 below			
	OAMP	1	Control Input – Status Output
	Craft(USB)	1	Control Input – Status Output
	Craft(DB-9)	1	Control Input – Status Output
Equipment Controller 32EC2E (2) – See Figure 8 below			
	CIT	2	Control Input – Status Output
11QPEN4 Encryption Card (up to 16) – See Figure 10 below			
	LEDs	9	Status Output
	L	4	Data Input and Data Output
	VA	4	Data Output
S13X100E Encryption Card (up to 15) – See Figure 11 below			
	LEDs	2	Status Output
	L	1	Data Input and Data Output
Filler Card (up to 16) – No Figure provided			
	n.a.	n.a.	No interfaces

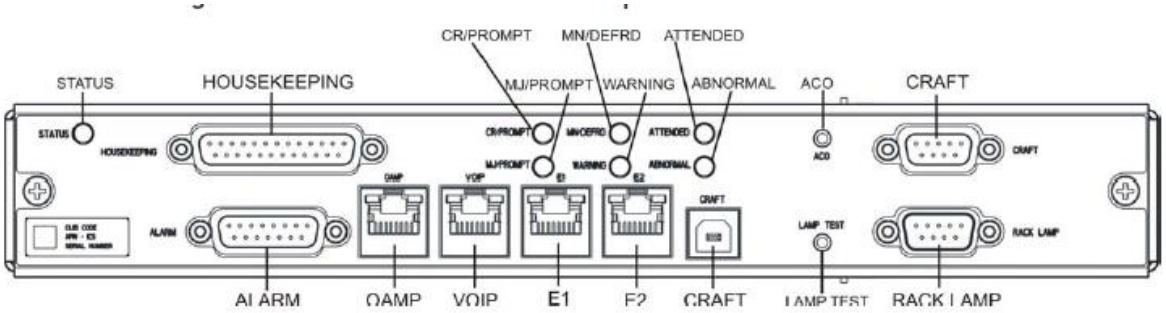


Figure 5 - PSS-32 User Panel - front view

2.2.2 PSS-16II Interfaces

Table 3- FIPS 140-2 Logical Interface mapping for 1830 PSS-16II

Panel	Physical Ports	Quantity	FIPS 140-2 Interface
User Panel (1) – See Figure 6 below			
	OAMP	1	Control Input – Status Output
	Craft	1	Control Input – Status Output
Equipment Controller 32EC2E (2) – See Figure 8 below			
	CIT	2	Control Input – Status Output
11QPEN4 Encryption Card (up to 8) – See Figure 10 below			
	LEDs	9	Status Output
	L	4	Data Input and Data Output
	VA	4	Data Output
S13X100E Encryption Card (up to 8) – See Figure 11 below			
	LEDs	2	Status Output
	L	1	Data Input and Data Output
Filler Card (up to 8) – No Figure provided			
	n.a.	n.a.	No interfaces

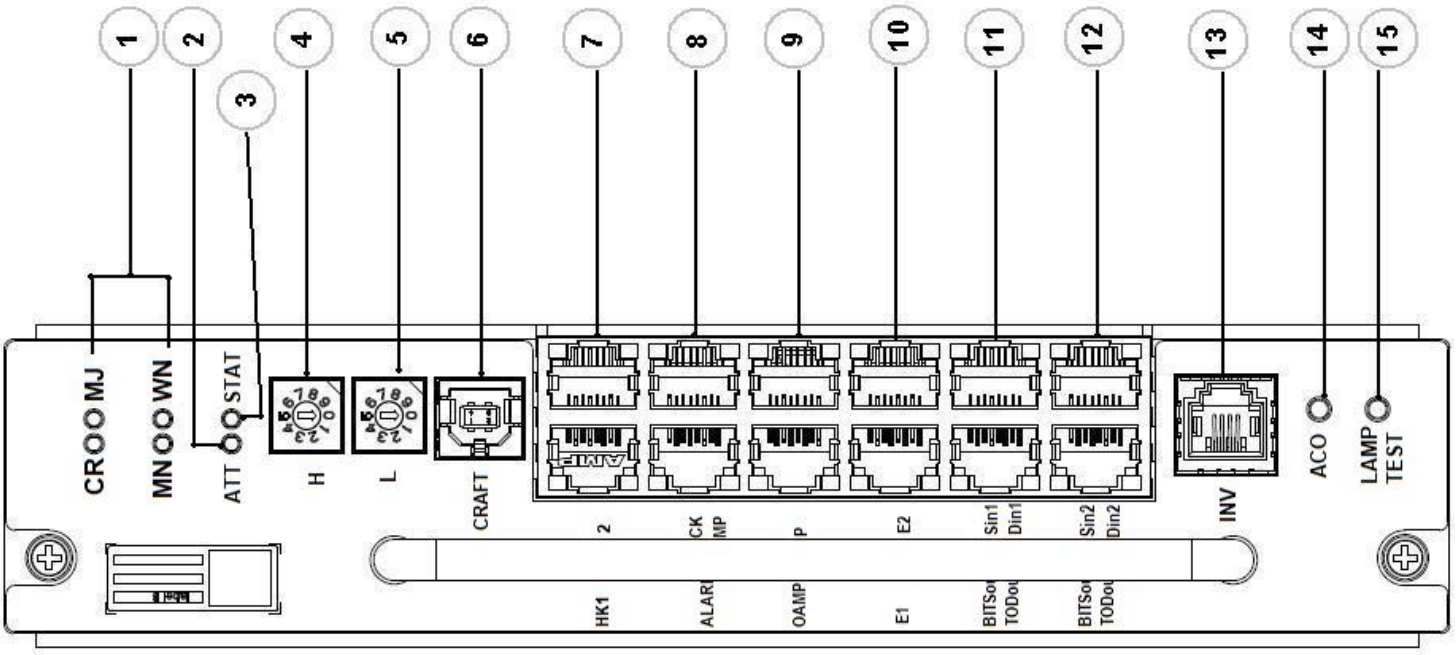


Figure 6 - PSS-16II User Panel - front view

1	LEDs “Alarms status”
2	LEDs “ATTENDED”
3	LEDs “STATUS”
4	2*Shelf-ID Rotary Shelf-ID Rotary "H"
5	Shelf-ID Rotary "L"
6	1* Type B USB interface Craft: Craft Port (USB signal)
7	“HOUSEKEEPING1” interface “HOUSEKEEPING2” interface
8	ALARM: RACK ALARM RACK LAMP
9	OAMP: OAMP (GbE) and its LED VOIP: VOIP and its LED
10	2*RJ-45 interface External LAN port and its LED E1 External LAN port and its LED E2
11	2*RJ-45 interface BITSin1 TODin1: BITS and 1pps and ToD IN1 BITSout1 TODout1: BITS and 1pps and ToD OUT1
12	2*RJ-45 interface BITSin2 TODin2: BITS and 1pps and ToD IN2 BITSout2 TODout2: BITS and 1pps and ToD OUT2
13	RJ-11 interface (INV): 1-wire connection to SFD44
14	Alarm cut-off button (ACO)

15	“LAMP TEST” button

Table 4 - Legend PSS-16II User Panel

2.2.3 PSS-8 Interfaces

Table 5 - FIPS 140-2 Logical Interface mapping for 1830 PSS-8

Panel	Physical Ports	Quantity	FIPS 140-2 Interface
Shelf Panel (1) – See Figure 7			
	OAMP	1	Control Input – Status Output
Equipment Controller 8EC2E (2) – See Figure 9			
	Craft	1	Control Input – Status Output
	CIT	1	Control Input – Status Output
11QPEN4 Encryption Card (up to 4) – See Figure 10			
	LEDs	9	Status Output
	L	4	Data Input and Data Output
	VA	4	Data Output
S13X100E Encryption Card (up to 4) – See Figure 11 below			
	LEDs	2	Status Output
	L	1	Data Input and Data Output
Filler Card (up to 4) – No Figure provided			
	n.a.	n.a.	No interfaces

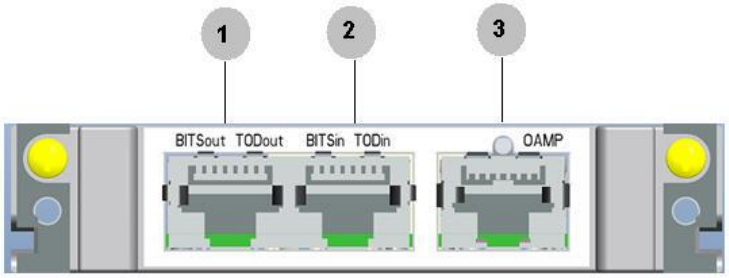


Figure 7 - PSS-8 Shelf Panel - front view

1	“BITS out and TOD out” RJ-45 interface
2	“BITS in and TOD in” RJ-45 interface
3	“OAMP” RJ-45 interface

Table 6 - Legend PSS-8 Shelf Panel

2.2.4 Equipment Controller PSS-16II and PSS-32

Table 7 - FIPS 140-2 Logical Interface Mapping for PSS-32/PSS-16II Equipment Controller Card

Physical Ports	Quantity	FIPS 140-2 Interface
LED	2	Status Output
CIT	1	Control Input – Status Output

AUX	1	Port disabled and cannot be used in FIPS configuration
ES1	1	Port enabled, but shall not be used in FIPS configuration
ES2	1	Port enabled, but shall not be used in FIPS configuration

The physical access to the AUX, ES1, ES2 is prevented by a faceplate which is secured by tamper labels (see Figure 28 for PSS-32 and Figure 19 for PSS-16II) if the module is in FIPS mode of operation. The AUX channel is disabled in the FIPS mode of operation and cannot be used. For ES1/ES2, non-usage of ES1/2 is by policy. The ES1/2 are unused in FIPS configurations and instead, the ports are used in non-FIPS multi-shelf configurations. They are, however, only used if the connected shelf is accepted to be a part of the NE. This requires provisioning actions that are prohibited by policy. CSPs are not accessible through ES1/2 and code cannot be loaded using ES1/2.

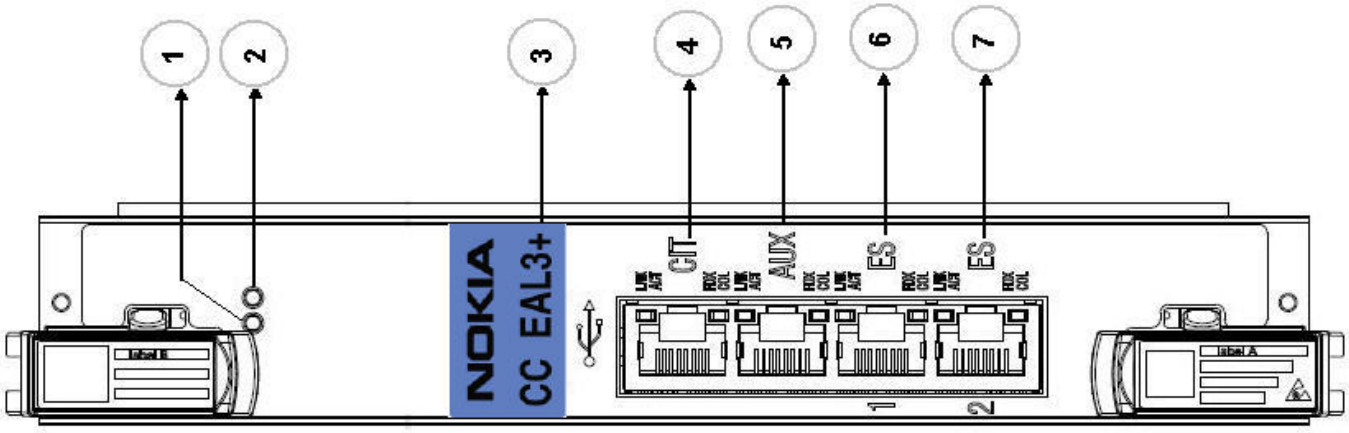


Figure 8 - PSS-32 and PSS-16II equipment controller 32EC2E Faceplate

1	LED “STATUS”
2	LED “EPS”
3	Interface that is not supported on 32EC2E (disabled by SW and covered by a seal)
4	“CIT” interface
5	“AUX” interface
6	“ES 1” interface
7	“ES 2” interface

Table 8 - Legend 32EC2E

2.2.5 Equipment Controller PSS-8

Table 9 - FIPS 140-2 Logical Interface Mapping for PSS-8 Equipment Controller Card

Physical Ports	Quantity	FIPS 140-2 Interface
LED	2	Status Output
CIT	1	Control Input – Status Output
CRAFT	1	Control Input – Status Output
ES1	1	Port enabled, but shall not be used in FIPS configuration
ES2	1	Port enabled, but shall not be used in FIPS configuration
RST	1	Control Input (EC reset)

The physical access to the ES1, ES2 is prevented by a faceplate which is secured by tamper labels (see Figure 18) if the module is in FIPS mode of operation. For ES1/ES2, non-usage of ES1/2 is by policy. The ES1/2 are unused in

FIPS configurations and instead, the ports are used in non-FIPS multi-shelf configurations. They are, however, only used if the connected shelf is accepted to be a part of the NE. This requires provisioning actions that are prohibited by policy. CSPs are not accessible through ES1/2 and code cannot be loaded using ES1/2.

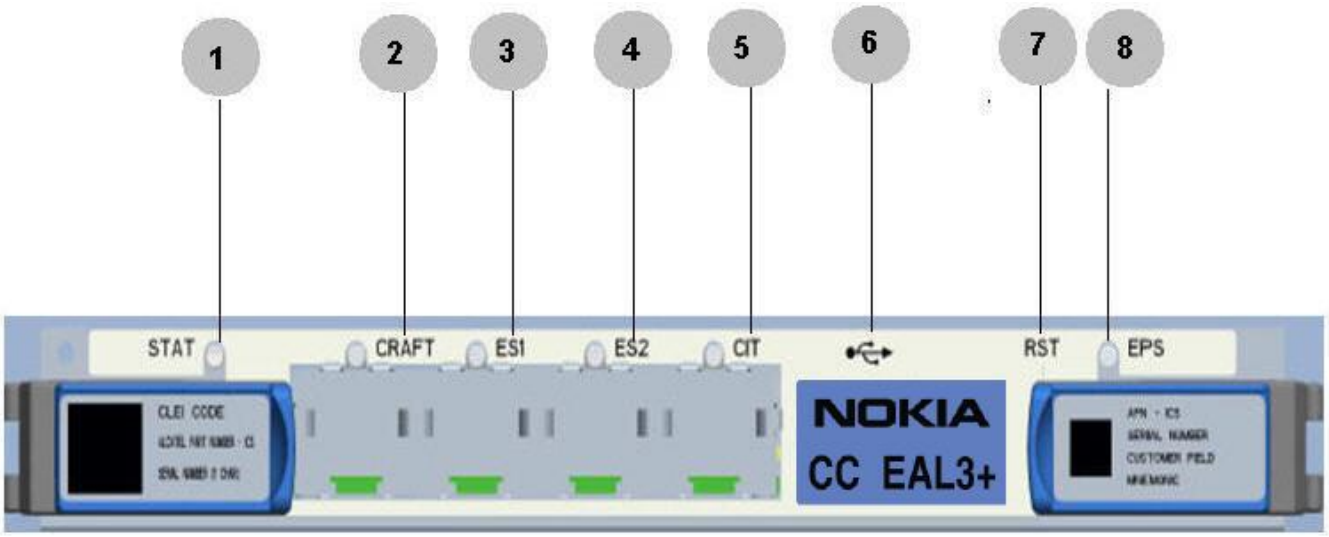


Figure 9 - PSS-8 equipment controller 8EC2E Faceplate

1	LED “STATUS”
2	“CRAFT” interface
3	“ES 1” interface
4	“ES 2” interface
5	“CIT” interface
6	Interface that is not supported on 8EC2E (disabled by SW and covered by a seal)
7	“RST” button
8	LED “EPS”

Table 10 - Legend 8EC2E

2.2.6 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, unencypted data in the form of Fibre Channel, Ethernet or OTU2 signals enter a client port and are encrypted and then transmitted out the assoicated 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).

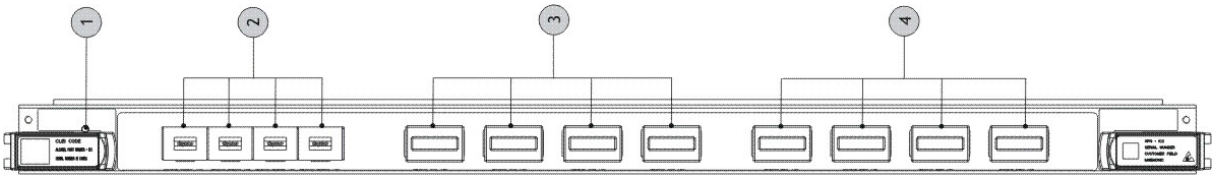


Figure 10 - 11QPEN4 Encryption card

Legend:
1 LEDs “STATUS”
2 “VA1”-“VA4” interfaces
3 “L1”-“L4” interfaces
4 “C1”-“C4” interfaces

Table 11 - FIPS 140-2 Logical Interface Mapping for 11QPEN4 Card

Physical Ports	Quantity	FIPS 140-2 Interface
L1,L2,L3,L4	4	Data Input – Data Output
VA1,VA2,VA3,VA4	4	Data Output
C1,C2,C3,C4	8	Data Input – Data Output
LEDs	13	Status Output

2.2.7 S13X100E

The S13X100E has

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

as shown in Figure 11. Each pluggable client interface transceiver and the fixed line side tranceiver provides an optical fiber interface for receive and an optical fiber interface for transmit. In the transmit direction, unencypted 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.

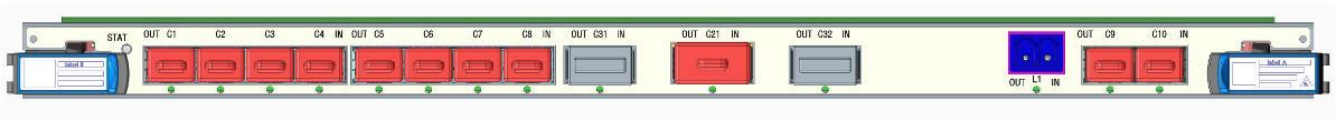


Figure 11 - S13X100E Encryption card

STAT	Card Status LED
C1…C10	Client XFP interfaces
C31, C32	Client QSFP interfaces
C21	Client CFP4 interface
L1	Line interface

Table 12 - Legend S13X100E

Table 13 - FIPS 140-2 Logical Interface Mapping for S13X100E Card

Physical Ports	Quantity	FIPS 140-2 Interface
L1	2	Data Input – Data Output
C1…C10,C21,C31,C32	26	Data Input – Data Output
LEDs	15	Status Output

2.2.8 Filler Card

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

Figure 12 - Filler Card

Physical Ports	Quantity	FIPS 140-2 Interface
none	Not applicable	Not applicable

Table 14 - FIPS 140-2 Logical Interface Mapping for Filler Card

2.3 Roles, Services, and Authentication

The module supports identity based authentication and the module supports two roles:
1) Crypto Officer Role which is referred to as 'Admin'
2) User Role which is referred to as 'Crypto'

2.3.1 Cryptographic Officer Role (Admin)

The Admin accesses the module via the SNMP and/or the Command Line Interface (CLI). 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.

Table 15 - Crypto Officer (Admin) Service Table

Service	Operator	Description	Input	Output	Key\CSP Access (W\X) (no keys have read access)
User Account Management	Admin	Manage user accounts, password complexity and user privileges via CLI interface	Commands and Parameters	Command Response	User Password – W, X
Change User Password	Admin	Change the User password for same account via CLI interface	Command	Command Response	User Password - W
SNMP Configuration and Management	Admin	Facilitates the user to manage SNMPv3 configurations via CLI interface	Command and Parameters	Command Response	User Password – X SNMPv3 Proxy Authentication Key – W SNMPv3 Proxy Privacy Key - W
Commission the Module	Admin	Commission the module by following the Security Policy guidelines via CLI interface	Commands and Parameters	Command Response	None
Perform Self-tests	Admin	Perform on-demand Power-up Self Tests by power cycling the cryptographic module	Commands	Command Response	None
Show Status	Admin	Allows operator to view status of the parameters associated with FIPS-Approved mode or not via SNMPv3 and CLI interfaces	Commands and Parameters	Command Response	User Password - X
Alarms Monitoring	Admin	Allows operator to view active alarms via SNMPv3 interfaces	Commands and Parameters	Command Response	User Password - X
Events Monitoring	Admin	Allows the user to view all logged events associated with their permissions via SNMPv3 interfaces	Commands and Parameters	Command Response	User Password - X
11QPEN4 Provision Equipment	Admin	Allows the user to provision and configure the 11QPEN4 cards via SNMPv3 interface	Commands and Parameters	Command Response	User Password - X
11QPEN4 Provision Facility	Admin	Allows the user to provision and configure the facility information associated with 11QPEN4 cards via SNMPv3 interface	Command and Parameters	Command Response	User Password - X
S13X100E Provision Equipment	Admin	Allows the user to provision and configure the S13X100E cards via SNMPv3 interface	Commands and Parameters	Command Response	User Password - X

Service	Operator	Description	Input	Output	Key\CSP Access (W\X) (no keys have read access)
S13X100E Provision Facility	Admin	Allows the user to provision and configure the facility information associated with S13X100E cards via SNMPv3 interface	Command and Parameters	Command Response	User Password - X
Zeroize Keys	Admin	Zeroize keys and CSPs over SNMPv3 and CLI interfaces	Command and Parameters	Command Response	Crypto or User Password - W SNMPv3 Crypto (KM) or Admin (NMS) password - W SNMPv3 Proxy Authentication Key - W SNMPv3 Proxy Privacy Key – W 11QPEN4 Session Encryption Key - W 11QPEN4 Session KAT Key – W S13X100E Session Encryption Key - W S13X100E Session KAT Key - W
Session initiation	Admin	Initiate session with another module using AES keys.	Command and Parameters	Command Response	AES key - W

2.3.2 User Role (Crypto)

The User 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 and 11QPEN4. Those transmission encryption functions cannot be provisioned by other roles. These services are all Approved services.

Table 16 - User (Crypto) Service Table

Service	Operator	Description	Input	Output	Key\CSP Access (R\W\X)
Change Crypto Password	Crypto	Change the Crypto password for same account	Command	Command Response	Crypto Password - W
Perform Self-tests	Crypto	Perform on-demand Power-up Self Tests by power cycling the cryptographic module	Remove and reestablish power to module	Status Response in logs	None
Alarms Monitoring	Crypto	Allows users to view active alarms via SNMPv3 interfaces	Commands and Parameters	Command Response	Crypto Password - X
Events Monitoring	Crypto	Allows the user to view all logged events associated with their permissions via SNMPv3 interfaces	Commands and Parameters	Command Response	Crypto Password - X
11QPEN4 Line Port WKAT Provisioning	Crypto	Allows the crypto user to provision and configure the WKAT via SNMPv3 interface	Commands and Parameters	Command Response	Crypto Password - X
11QPEN4 Line Port Encryption Key Provisioning	Crypto	Allows the crypto user to provision and switch the Encryption Key via SNMPv3 interface	Command and Parameters	Command Response	Crypto Password - X

Service	Operator	Description	Input	Output	Key\CSP Access (R\W\X)
11QPEN4 Line Port Encryption State Provisioning	Crypto	Allows the user to provision and configure the facility information associated with 11QPEN4 cards via SNMPv3	Command and Parameters	Command Response	Crypto Password - X
S13X100E Line Port WKAT Provisioning	Crypto	Allows the crypto user to provision and configure the WKAT via SNMPv3 interface	Commands and Parameters	Command Response	Crypto Password - X
S13X100E Line Port Encryption Key Provisioning	Crypto	Allows the crypto user to provision and switch the Encryption Key via SNMPv3 interface	Command and Parameters	Command Response	Crypto Password - X
S13X100E Line Port Encryption State Provisioning	Crypto	Allows the user to provision and configure the facility information associated with S13X100E cards via SNMPv3	Command and Parameters	Command Response	Crypto Password - X
Zeroize Keys	Crypto	Zeroize keys and CSPs over SNMPv3 interfaces	Command and Parameters	Command Response	User Password - W 11QPEN4 Session Encryption Key - W 11QPEN4 Session KAT Key – W S13X100E Session Encryption Key - W S13X100E Session KAT Key - W

R - indicates Read access W – indicates Write access
X – indicates the CSP is used within a security function or authentication mechanism

2.3.3 Authentication

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

Table 17 - Strengths of Authentication Mechanisms

Authentication Mechanism	PassKey / Password Rules	Strength of Mechanism
SNMPv3 user name and PassKey for 1830 SMS and NMS The user name should not be longer than 21 characters. The user name is a human readable string and no more that 21 characters in length, there are no additional SNMPv3 standards for user restrictions.	The PassKey can be from 27 to 32 characters, using upper and lower case letters and numeric digits 0–9. The PassKey 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 PassKey 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 PassKey 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 (100×10^6 × 60 = 6 × 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 PassKeys / ((6 ×10^9 bits per minute) / 64 bits per PassKey)), which is 1: 2,481E+48 possible PassKeys / 93,750,000 PassKeys per minute), which is 1: 2,646E+40, which is a smaller probability than 1:100,000 as required by FIPS 140-2. This provides a security strength of 160 bits (27 characters) to 190 bits (32 characters).
CLI user name and password User names 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) ○ ! (exclaimation 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 user name and the password must not have three consecutive identical characters.	(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 140-2.

2.4 Physical security

Overview

To operate in FIPS Approved mode the tamper-evident labels shall be installed as shown in Appendix A.

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

Physical security mechanisms

After the tamper seals have been applied to the module, the shelf cannot be accessed without indicating signs of tampering.

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

- Production-grade components and production-grade opaque enclosure with tamper-evident labels.
- Tamper-evident labels. Refer Procedure 1: “Install the tamper evident labels” for detailed instructions on tamper-evident label placement.
- Provision the cryptographic module to operate in a FIPS compliant mode. Refer to Procedure 1: “Provision 1830 PSS for FIPS 140-2 secured operation” for detailed instructions.
- all unpopulated slots are equipped with filler cards

Tamper-evident labels

Tamper-evident labels shall be installed (by the Crypto Officer (CO)) for the module to operate in a FIPS-approved mode of operation.

The following graphics illustrate a tamper-evident label.

Figure 13, “Tamper-evident label: intact” illustrates a tamper-evident label with no evidence of tampering.

Figure 13 - Tamper-evident label: intact

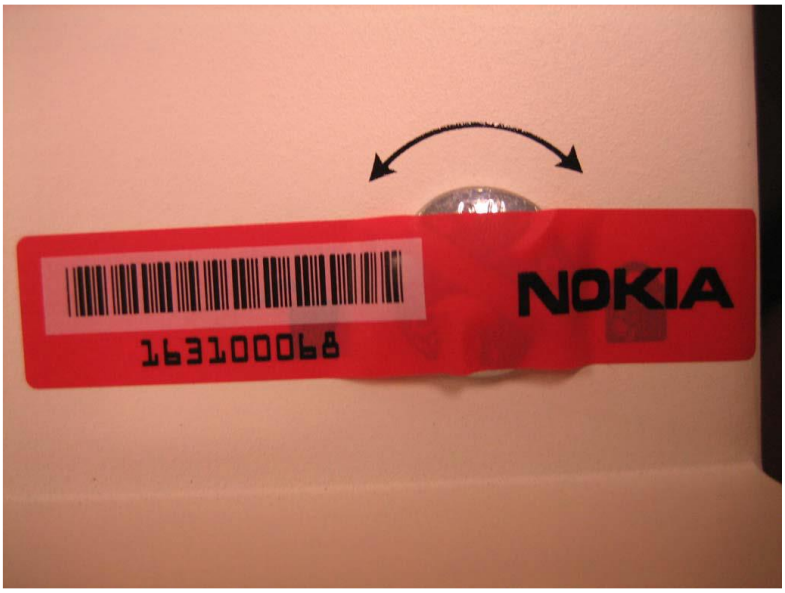
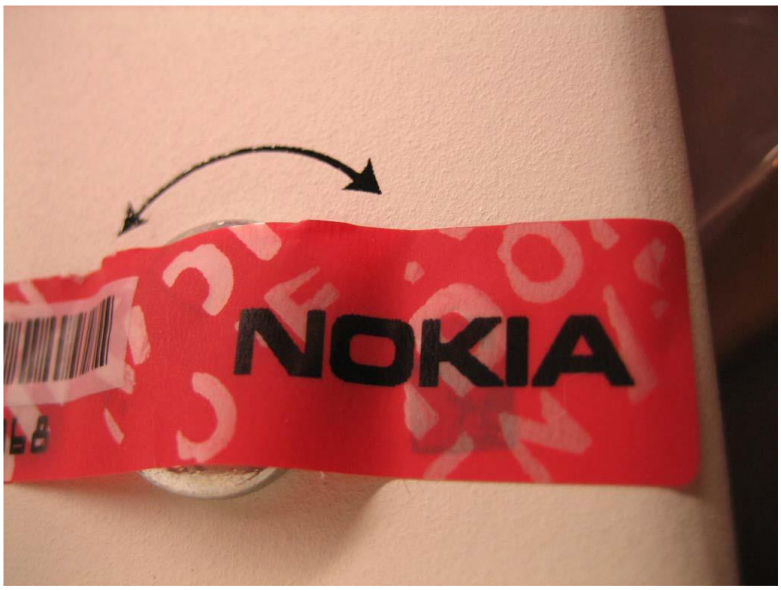


Figure 14, "Tamper-evident label: broken" illustrates a tamper-evident label that shows signs of tampering. Note the *VOID* markings on the solid red label. If any portion of the VOID marking is visible, the equipment is showing signs of potential tampering.

Figure 14 - Tamper-evident label: broken



Scan labels

The tamper-evident labels each have a unique serial number and a linear barcode. The linear barcodes can be scanned while still on the sheet.

Inspect labels

The Crypto Officer is also responsible for inspecting the tamper-evident labels on the shelves at least every 3 months.

Detailed procedures on affixing labels for PSS-32, PSS-16II and PSS-8 are given in Appendix A.

Broken tamper-evident labels

If a tamper-evident label is broken, then the respective module must be considered compromised and must not be used anymore.

2.5 Operational Environment

The module employs a non-modifiable operating environment. The firmware is executed by the module's Marvel Armada processor.
This operational environment of the module does not provide a general-purpose OS to the operator. The operational environment is not modifiable by the operator, and only the module's signed image can be executed. All firmware upgrades are digitally-signed, and a conditional self-test (RSA signature verification) is performed during each upgrade. If the signature test fails, the new firmware is ignored and the current firmware remains loaded.
Note: Only FIPS-validated firmware may be loaded to maintain the module's validation.

2.6 Cryptographic Key Management

The following table specifies the algorithms that were CAVP tested for the modules:

Table 18 - List of FIPS 140-2 Algorithms Certificates for 1830 PSS

Algorithm	Nokia PSS-8 and PSS-32/16II Crypto-SNMP Engine (EC)	Rijndael AES256 (Nokia Crypto-OTU2 Engine 11QPEN4)	CRYPOTN (Nokia 100G using Microsemi, S13X100E)	Nokia_File_Integrity_Check
AES-256 in CFB128 Mode: CFB128 (e/d; 256)	C882			
SHA-1	C882			
CVL (SNMP)	C882			
KTS (AES Cert. #C882 and HMAC Cert. #C882)	C882			
HMAC-SHA-1	C882			
HMAC-SHA256			C1545	
AES-256 in CTR Mode: CTR (e; 256)		C1144	AES 3844	
AES-256 GMAC Direction: Decrypt, Encrypt • Key Length: 256 • Tag Length: 128 • IV Length: 96 • AAD Length: 128			AES 3844	
SHA256			C1545	C1143

There are algorithms, modes, and keys that have been CAVs tested but not used by the module. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in this table are used by the module.

The module also uses HMAC (HMAC-SHA-1 (MAC:96)) Certificates C882 to perform key wrapping authentication in compliance to SP800-38F Revision 1 Transition (AES/TDES key wrapping). The module also uses AES (AES-256-CFB128) Certificates C882 to perform key wrapping encryption in compliance to SP800-38F Revision 1 Transition (AES/TDES key wrapping).

KTS (AES Cert. C882 and HMAC Cert. C882 establishment methodology provides 256 bits of encryption strength).

No parts of the SNMP protocol (under SNMP Cert. C882) other than the KDF has been tested by the CAVP and CMVP.

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 140-2 IG] section A.5 (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.
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.) By Policy, 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.) By Policy, 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.

The following table lists the keys and CSPs of the module:

Table 19 - List of Crypto Keys and CSPs

CSP	CSP Type	Generation /Input	Output	Storage	Zeroization	Use
SNMPv3 Crypto officer(Admin) or User (Crypto) PassKey	Alpha-Numeric string	Entered into module at local console at initial provisioning	Never exits the module	Not stored - converted to authentication and privacy keys	Zeroized when PassKey is updated with a new one	Used to generate authentication and encryption keys
SNMPv3 Crypto officer(Admin) or User (Crypto) Proxy Authentication Key	HMAC SHA-1-96 key	generated from SNMP authentication password and localized variables	Never exits the module	Stored within module in clear text in EC flash memory	Zeroized when PassKey is updated with a new one	Used to authenticate during communication via SNMPv3
SNMPv3 Crypto officer(Admin) or User (Crypto) Proxy Privacy Key	AES-256 key	generated from SNMP privacy password and localized variables	Never exits the module	Stored within module in cleartext in EC flash memory	Zeroized when PassKey is updated with a new one	Used to encrypt during communication via SNMPv3
SNMPv3 Crypto (KM) or Admin (NMS) PassKey	Alpha-Numeric string	Entered into module at local console at initial provisioning	Never exits the module	Not stored - converted to authentication and privacy keys	Zeroized when PassKey is updated with a new one	Used to generate authentication and encryption keys
11QPEN4 Session Encryption Key	AES-256 key	Imported across encrypted SNMPv3 link from KM	Never exits the module	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 Key	AES-256 key	Imported across encrypted SNMPv3 link from KM	Never exits the module	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	Imported across encrypted SNMPv3 link from KM	Exits the module in plaintext over secured SNMPv3 link	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 KAT key (WKAT Authentication String)	Hexadecimal Alpha-Numeric string	Imported across encrypted SNMPv3 link from KM	Exits the module in plaintext over secured SNMPv3 link	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

CSP	CSP Type	Generation /Input	Output	Storage	Zeroization	Use
S13X100E Session Authentication Key	AES-256 key	S13X100E Session Encryption Key is used	Never exits the module	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

2.7 Self-Tests

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

Table 20 - Power-Up Known Answer Self-Tests PSS-32/PSS-16II/PSS-8

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
Firmware Integrity Test	All the cryptographic firmware modules are contained in rpm files in the Main storage flash on the EC card and are verified by SHA256 checksum during the firmware startup.
HMAC-SHA256 KAT	Known answer test for HMAC-SHA256

2.8 Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks beyond the scope of FIPS 140-2 requirements.

3. Configuring the 1830 PSS for Secure Operation

This chapter describes how to configure the 1830 PSS for FIPS mode of operation.

3.1 Bringing the module into the FIPS mode of operation

In the following some actions must be executed

- Provision the module in general – chapter 3.1.1 to chapter 3.1.4
- Install the HW to be used – chapter 3.1.5
- Install tamper-evident labels – see APPENDIX A- Procedures for Installation of the FIPS Tamper Seals

3.1.1 Provision 1830 PSS for CC EAL3+ secured operation

3.1.1.1 Purpose

Perform these procedures to provision the shelf for CC EAL3+ secured operation.

3.1.1.2 Before you begin

1830 PSS can only be a CC EAL3+ certified configuration if the installed firmware is Release 10.1.2.
All subcomponents (11QPEN4, S13X100E, 11DPM12, and filler plates) must be installed in the 1830 PSS shelf before 1830 PSS is a CC EAL3+ certified configuration.
Refer to the following documents before performing this procedure

- *1830 Photonic Service Switch (PSS) Release 10.1 Command Line Interface Guide*
- *1830 Photonic Service Switch 8 (PSS-8) Release 10.1 Installation and System Turn-up Guide*
- *1830 Photonic Service Switch 16II (PSS-16II) Release 10.1 Installation and System Turn-up Guide*
- *1830 Photonic Service Switch 16/32 (PSS-16/PSS-32) Release 10.1 Installation and System Turn-up Guide*

3.1.1.3 Overview

1

Install the shelf with the required equipment.
Reference:
Refer to the appropriate document for your shelf type.

- *1830 Photonic Service Switch 8 (PSS-8) Release 10.1 Installation and System Turn-up Guide*
- *1830 Photonic Service Switch 16II (PSS-16II) Release 10.1 Installation and System Turn-up Guide*
- *1830 Photonic Service Switch 16/32 (PSS-16/PSS-32) Release 10.1 Installation and System Turn-up Guide*

Important! The equipment packaging is sealed with a “Void unless removed by end Customer” label. If the packaging label shows any evidence of tampering, DO NOT use the equipment.
Important! The USB port on each controller is covered by a blue tamper-evident label to prevent access to the port. If the label shows any evidence of tampering DO NOT use the card.
Note: The 8EC2E and 32EC2E equipment controller operate in fixed CC EAL3+ compliant mode (ANSSI mode). The operation mode cannot be changed. The ANSSI mode is compliant with the FIPS mode of operation.

2
Establish an initial connection to your NE.
Reference: 3.1.2 Connect to the NE using CRAFT port (p. 33)
3
Provision IP addresses, date/time, and commission the node.
Reference: 3.1.3 Provision IP addresses and date/time (p. 34)
4
Provision the user roles.
Reference: 3.1.4 Provision user roles (p. 35)
5
Install the cards.
Reference: 3.1.5 Install 11QPEN4, S13X100E, or 11DPM12 cards (p. 37)
6
Verify the Product Version.
An operator can verify that the validated firmware version is in operation by checking the Release Number displayed in response to the following CLI command: **show version**.
END OF STEPS

3.1.2 Connect to the NE using CRAFT port

3.1.2.1 Purpose

Locally connect to the NE, using a co-located PC with terminal SW (TERATERM or PUTTY), at the CRAFT port on the 8EC2E or 32EC2E cards with Baud Rate 38400, no parity, 8 data and 1 stop bits, no flow control.
Note: the use of SSH (and thus the use of a CIT LAN port) is avoided in 1830PSSECE-10.1-2 as the SSH is not part of this certification.
Note: as this is a direct local connection from PC to the NE no additional securing of this connection is needed.

3.1.2.2 Steps

1
If not already connected, connect one end of the CRAFT cable to the CRAFT port on the active 8EC2E or 32EC2E card (indicated by a green Active LED) on the shelf. Connect the other end of the cable to the serial port on your PC.
2
On your PC, open a terminal application with user name **CLI** (no password necessary) and initiate a CLI command session.
Result: The CLI interface opens, and the Username: prompt appears.
3
At the Username: prompt, type **admin** and **Enter**.
Result: The Password: prompt appears.
4

At the Password: prompt, type **admin** and **Enter**.
Result: The warning notice appears.
Note: After an invalid login, (for example, due to wrong password), the NE does not allow the next login immediately. The default waiting time is 4 seconds. After 3 consecutive failed attempts, the connection is terminated and will need to be re-established.
Reference: To provision the intrusion attempt handling parameters (minimum wait time between failed login attempts and the maximum number of invalid logins) refer to Step 7 in chapter 3.1.4.

5

Type **Y** and **Enter**.

END OF STEPS

3.1.3 Provision IP addresses and date/time

3.1.3.1 Purpose

Provision the IP addresses and the date/time of the NE.

3.1.3.2 User role

You must login to the NE using CLI with the user role of Administrator.

3.1.3.3 Steps

1

Provision Loopback IP address.
In CLI, enter **config interface loopback ip <ip>/<mask>** to set the IP address.
Confirm execution by typing **yes** after the command.
Result: The shelf will reboot.

2

When the controller LED is solid green, the shelf has completed rebooting. Reconnect to the NE.

3

Provision Control Network default route.
In CLI, enter **config cn routes default add <ip> <distance> <distribution mode>** to set the CN default route.

4

Provision OAMP IP address.

- For 1830 PSS-16II/1830 PSS-32: In CLI, enter the following commands:
  - **config interface usrpnl oamp ip <ip>/<mask>**
    Confirm execution by typing **yes** after the command.
  - **config interface usrpnl oamp st up**
- For 1830 PSS-8: In CLI, enter the following commands:
  - **config interface shfpnl oamp ip <ip>/<mask>**
    Confirm execution by typing **yes** after the command.
  - **config interface shfpnl oamp st up**

5

Provision current date and time on the shelf.

In CLI, enter:

1. **config gen timezone name <timezone>**.
2. **config general time <hour> <min> <sec>**.
3. **config general date <yyyy> <m> <d>**.
4. **show gen date** to verify your provisioning.

6

Do not enter **crypto key generate** to generate SSH keys.
As a side effect SSH cannot be used (especially not on CIT and OAMP LAN ports).

7

For 1830 PSS-8 only, enter the following CLI command **config general etr disable**.

END OF STEPS

3.1.4 Provision user roles

3.1.4.1 Purpose

Use this procedure to provision the following:

- User role (Administrator and Crypto) for CLI
- User role (Administrator and Crypto) for SNMPv3
- User role for Linux OS

3.1.4.2 Steps

1

In CLI, enter **config admin users add username crypto**.

2

Change the password for the admin account.
In CLI, enter:

- **config admin users edit service status disabled**
- **config admin users edit admin passwd**

3

Log out of the system and log in with the new password.

4

Provision the default timeout for the CLI user session as 15 minutes and the admin session as 0 minutes.
In CLI, enter:

- **config admin session timeout 15**
- **config admin users edit admin timeout 0**

5

Perform a warm reset on the shelf to execute the session timeout provisioning change in Step 4.
In CLI, enter **config admin resetne warm**
Result: WARNING! You are about to perform a warm system restart. Enter 'yes' to confirm, 'no' to cancel:

Enter **yes** to confirm that you want to restart the network element firmware.

6

Log in to system again.

7

Provision the number of invalid login attempts a CLI user is allowed before the CLI user is locked out and an Intrusion Attempt alarm raised.

Provision intrusion attempt handling parameters using the following CLI commands:

- **config admin session maxfailedlogins 5**
- **config admin session minwaitlogin 60**

Note: Users are locked out based on their originating address. Security logs record the originating address and connection type of invalid login attempts. Results of previous authentications are stored in volatile memory and cleared when the 1830 PSS shelf is powered off.

8

Create one SNMPv3 user as Administrator and one SNMPv3 user as Crypto.

In CLI, enter:

- **config admin snmpusers add omsuser administrator aes128md5**
- **config admin snmpusers add smsuser crypto aes256sha1**

Result: The newly created SNMP v3 user applies the same password for authentication and privacy. After new SNMP v3 user is added, you must edit the new user to change the Privacy Password.

9

Change the privacy password for the *omsuser* and the *smsuser*.

In CLI, enter:

- **config admin snmpusers edit omsuser privpasswd**
- **config admin snmpusers edit smsuser privpasswd**

Note: In this step the PassKey for SNMPv3 is set for the NM (omsuser) and KM (smsuser). Refer to chapter 2.3.3 for details.

10

Disable the default SNMP v3 user accounts.

In CLI, enter:

- **config admin snmpusers edit v3DefaultUser status disabled**
- **config admin snmpusers edit v3DftAdvUser status disabled**

11

Enable fips-squelching mode.

In CLI, enter **config general fips-squelching enable**

12

Change the maintenance (Linux OS) user passwords.

Note: The Linux OS users are for service and maintenance access only. Remember the passwords and share with service technicians if Linux OS access is necessary.

In CLI, enter:

- **config admin system maint1 credential**
- **config admin system maint2 credential**

Important! Wait 5 seconds before entering the next CLI command.

13

Verify that the maintenance (Linux OS) user passwords are correct.
In CLI, enter **config admin system status**
Result:

```
ANSSI-#2 config admin system status
User Password status
- - - - - - - - - - - - - - - - - -
maint1 Password OK
maint2 Password OK
```

14

Verify the current NE database synchronization status and control card activity states (active or inactive).
In CLI, enter **config redundancy detail**
Verify that the Inactive 8ECE2/32EC2E is ReadyTo Protect = Yes.
Result: Example:

```
Slot Type Activity ReadyTo
State Protect
-------------------------------------------
1/6 8EC2E Active -
1/12 8EC2E Inactive Yes
1/1 PF(cru) Active -
1/7 PF(cru) Inactive Yes
-------------------------------------------
```

15

Perform an EC side-switch.
In CLI, enter **config redundancy switch ec 1**
Result: WARNING: You are about to perform an activity switch. It is recommended that the databases be synchronized before performing an activity switch Enter 'yes' to confirm, 'no' to cancel.
Refer to Step 14.

16

Enter **yes** to confirm the activity switch.
Result: The system performs a warm reset.

END OF STEPS

3.1.5 Install 11QPEN4, S13X100E, or 11DPM12 cards

3.1.5.1 Steps

1

Install 11QPEN4, S13X100E, and 11DPM12 cards and verify that all unpopulated slots are equipped with filler plates.
Result: Allow the cards to boot.
Reference:
For related CLI commands, refer to *1830 Photonic Service Switch (PSS) Release 10.1 Command Line Interface Guide*:

- Part III: Card (core, OT, OTH) management, Chapter 6, "OT management commands".
  - 11QPEN4 interface commands
  - S13X100E interface commands
  - 11DPM12 interface commands
- Part V: Connection and protection management, Chapter 10, "Connection and protection management commands".
  - config interface topology
  - config odukxc
- *1830 Photonic Service Switch 8/16II/16/32 (PSS-8/PSS-16II/PSS-16/PSS-32) Release 10.1 User Provisioning Guide*

2
Set the Administrator passwords on 1830 SMS and NMS to be CC EAL3+ compliant.
Important! Never save passwords in your browser or 1830 SMS.
3
To add the NE to NMS, you must use an Administrator SNMPv3 user created in chapter 3.1.4.
Select snmpv3 option, AES256 encryption, and HMAC-SHA authentication.
4
To add the NE to 1830 SMS, you must use a Crypto SNMPv3 user created in chapter 3.1.4.
Select snmpv3 option, AES256 encryption, and SHA authentication.
5
Setup the service using CLI or 1830 SMS and NMS according to referenced documentation.
Result: The NE should be added to the NMS and discovered.
6
Verify that the service is up.
END OF STEPS

Note: Till this point CLI over serial interface is used. Now the NE is in the FIPS mode of operation. From then on CLI is not used anymore, but SNMPv3 is the means to access the NE.

3.2 Checking FIPS mode of operation

By default and by the steps shown in 3.1 the module is now in FIPS mode of operation. In addition the following checks should be done to make sure that UI mode and FIPS-squelching is correctly set.
Note: in FIPS compliant mode, the UI mode is displayed as "ANSSI".

3.2.1 Displaying FIPS mode and UI mode

The following commands will display FIPS mode and UI mode; If the 1830 PSS-32/16-II/8 is in FIPS approved mode when executed from the local CIT port as user (admin) after the steps to bring the module into the FIPS mode of operation.
The command and output will be as shown here:

```
ANSSI-3# show general detail
Name                    : ANSSI-3
System Description      : Nokia 1830 PSS v10.1 SONET ADM
Description :
Location :
Contact :
S/W Version             : 1830PSSECE-10.1-2
Current Date            : 2019/11/12 18:46:46 (UTC)
System Up Time          : 5 hours, 0 minutes, 35 seconds
Loopback IP Address     : 10.20.219.52/32

# show admin ui
UI: ANSSI

# config general fips-squelching
Fips Squelch Mode is Enable.
```

3.2.2 Error States

Non-Recoverable Error State
An 1830 PSS-32/PSS-16II/PSS-8 transitions to the Non-Recoverable Error state when one of the following conditions are met:
• Failure of any of the following tests:
– 1830 PSS-32/PSS-16II/PSS-8 power-on and boot time self-tests

While an 1830 PSS-32/PSS-16II/PSS-8 is in an Non-Recoverable Error state:
• All data output via the data output interfaces on the 1830 PSS-32/PSS-16II/PSS-8 is squelched (signal is replaced by a fixed traffic pattern).
• A log is generated to notify the user about the reason which caused the node to transition to the error state.
.

```
CR SA    13/05/24 00:13:27 ODU2     FIPSFAILURE         1/7/L1 In
   FIPS Selftest Squelch                                          11QPEN4
CR SA    13/05/24 00:13:27 ODU2     FIPSFAILURE         1/5/L1 In
   FIPS Selftest Squelch                                          S13X100E


 CR SA    13/05/28 21:07:40 EQPT     FIPSSWMISMATCH
1/2
   FIPS Software version mismatch                          Equipment Controller
```



```
CR SA    13/05/29 17:45:57 EQPT     AESFIPSFAILURE      1/2
  AES FIPS Failure                                      Equipment Controller
```

Note: the “FIPSSWMISMATCH” alarm log entry refers to a software version mismatch, where the terminology “software” is being used in the more generalized sense, but refers specifically to the module’s firmware. For clarity, please note that the alarm indicates a mismatch in the module’s firmware, version 1830PSSECE-10.1-2.

3.3 Zeroization

1830 PSS-32/PSS-16II/PSS-8 uses Advanced Encryption Standard (AES)-256 keys to encrypt client traffic over the WAN. Encryption keys are zeroized by any of the following actions, resulting in a loss of traffic:

- Zeroization of passwords and encryption keys are detailed in Table 15.
- Disabling encryption for a line port. This action zeroizes the encryption key for the port.
- Decommissioning the system. This action zeroizes all encryption keys on the system.
- Restoring provisioning data. This action zeroizes all encryption keys on the system.
- Deprovisioning (deleting) the 11QPEN4. This action zeroizes all encryption keys on the 11QPEN4.
- Deprovisioning (deleting) the S13X100E. This action zeroizes all encryption keys on the S13X100E.
- Restarting the system or the 11QPEN4 (or the S13X100E) when there are expired encryption keys. This action zeroizes all expired keys on the system or 11QPEN4 (or the S13X100E).

3.4 Crypto Officer and User Guidance

3.4.1 Interworking with other Modules

The Crypto Officer shall make sure that this module only interacts (for transmission encryption) with another module that is validated with the same certificate number.

3.4.2 Authentication modes

Local account authentication mode shall be provisioned for access to the 1830 PSS-32/PSS-16II/PSS-8 when in FIPS mode. RADIUS authentication is not used in FIPS mode.

3.4.3 Disabled Protocols

SSH and SFTP cannot be used in the approved mode of operation. These protocols did not undergo the full certification and are therefore disabled.

3.4.4 Non-Approved and Non-Allowed Cryptographic Algorithms (IG page 47, footnote 1)

The use of the SNMPv3 security option AES128/HMAC-MD5 provides a too weak security level and shall therefore not be used. Please refer to chapter 2.6 for the allowed SNMPv3 security options.

3.4.5 Backups and restores

Backups and restores shall not be performed in FIPS mode.

4. Abbreviations, Terminology and References

4.1 Abbreviations

Table 21 - Abbreviations

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

4.2 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document.

4.3 References

FIPS

[FIPS 140-2] FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001, CHANGE NOTICES (12-03-2002). http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[FIPS 140-2 DTR] Derived Test Requirements for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*, January 4, 2011 Draft. http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/fips1402DTR.pdf

[FIPS 140-2 IG] Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, October 23, 2019. http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf

5. APPENDIX A- Procedures for Installation of the FIPS Tamper Seals

Procedure 1: Install the tamper-evident labels

Purpose

Use this procedure to provision to install the tamper-evident labels on a Nokia 1830 PSS-8/16-II/32. The tamper seals are provided in the Security Label Kit (8DG-6509-AAAA).

Steps

1. When applying tamper-evident labels, ensure that the surface temperature to be sealed is be a **minimum** of +10°F and a maximum of +167°F.
2. Ensure that the surface to be sealed is dry. Moisture of any kind can cause a problem. Wipe the area with a clean paper towel.
3. Ensure that the surface to be sealed is clean. Wipe the area with a clean cloth or paper towel to remove any dust or other loose particles.
4. If there are possible chemical contaminants (oil, lubricants, release agents, etc), clean the surface with 100% iso-propyl alcohol. Wipe the alcohol dry with clean dry cloth or paper towel.

   Note: Avoid using rubbing alcohol; it can leave an oily coating that will interfere with adhesion of the label.
5. Installed tamper-evident labels shall be cured for 24 hours.

6 Proceed to the appropriate procedure to install the tamper-evident labels:

- Procedure 1.1: “Install the tamper-evident labels on Nokia 1830 PSS-8”
- Procedure 1.2: “Install the tamper-evident labels on Nokia 1830 PSS-16II”
- Procedure 1.3: “Install the tamper-evident labels on Nokia 1830 PSS-32”

END OF STEPS

Procedure 1.1: Install the tamper-evident labels on Nokia 1830 PSS-8

Purpose

Use this procedure to provision to install the tamper-evident labels on a Nokia 1830 PSS-8.

Steps

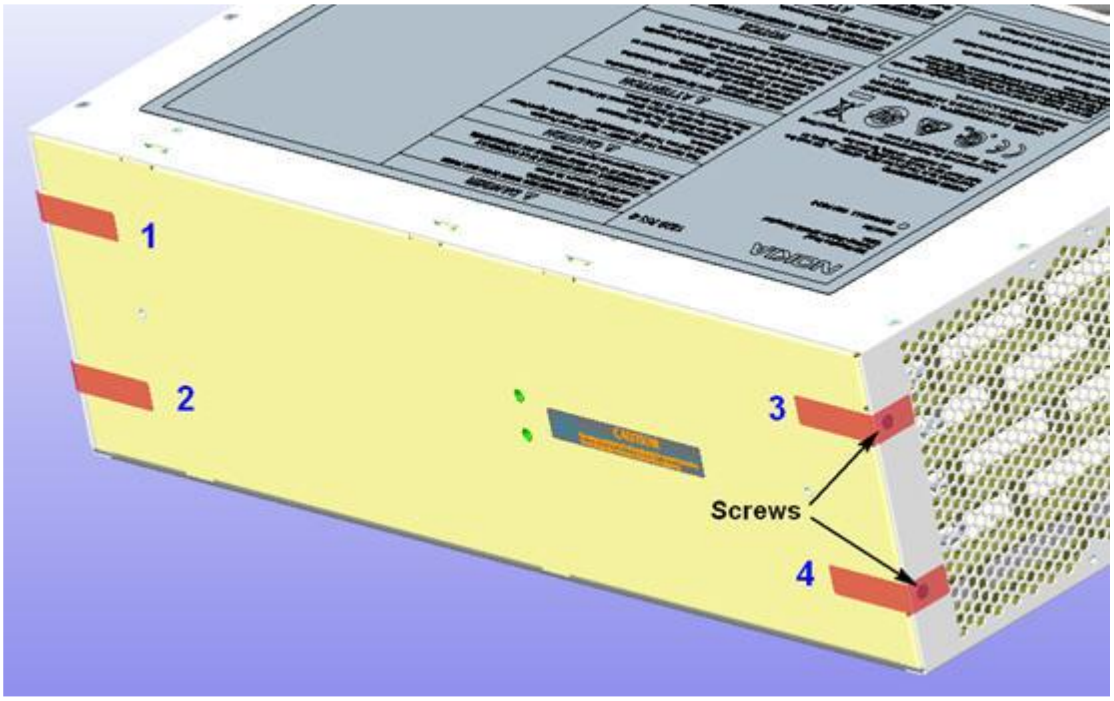
1 Install the 10 tamper-evident labels to seal the Nokia 1830 PSS-8 shelf.

Table 22 - Nokia 1830 PSS-8 shelf label locations

Location	Action	Reference
1	Place labels 1–4 horizontally over the 4 mounting screws that affix the rear cover to the shelf.	Figure 15, "Rear of an 1830 PSS-8 shelf"
2		
3		
4		
5	Place labels 5 and 6 over the top cover to wrap the faceplate latches on the controller.	Figure 16, "Top of an 1830 PSS-8 shelf "
6		
7	When the 1830 PSS-8 is installed in a 23" bay: Place label 7 and 8 vertically over the 2 mounting screws that affix the front cover adaptor to the shelf	Figure 17, "Left/Right of an 1830 PSS-8 shelf in a 23" bay"
8		
9	Place labels 9 and 10 over the 2 mounting screws that affix the front cover to the shelf.	Figure 18, "Front of an 1830 PSS-8 shelf"
10		

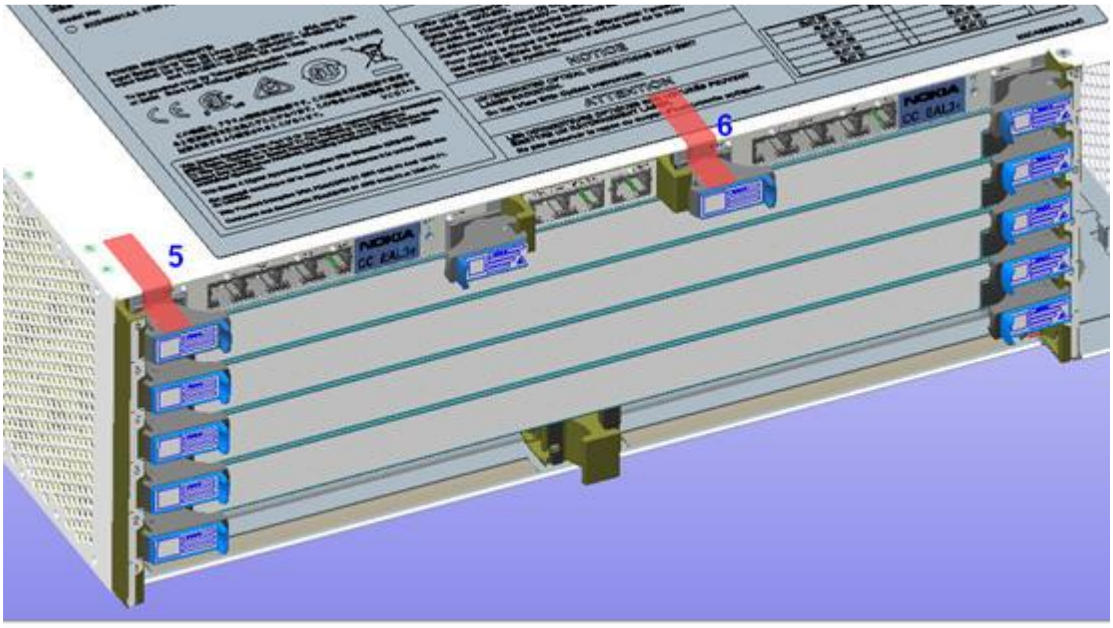
2 Place labels 1–4 horizontally over the 4 mounting screws that affix the rear cover to the shelf.

Figure 15 - Rear of an 1830 PSS-8 shelf



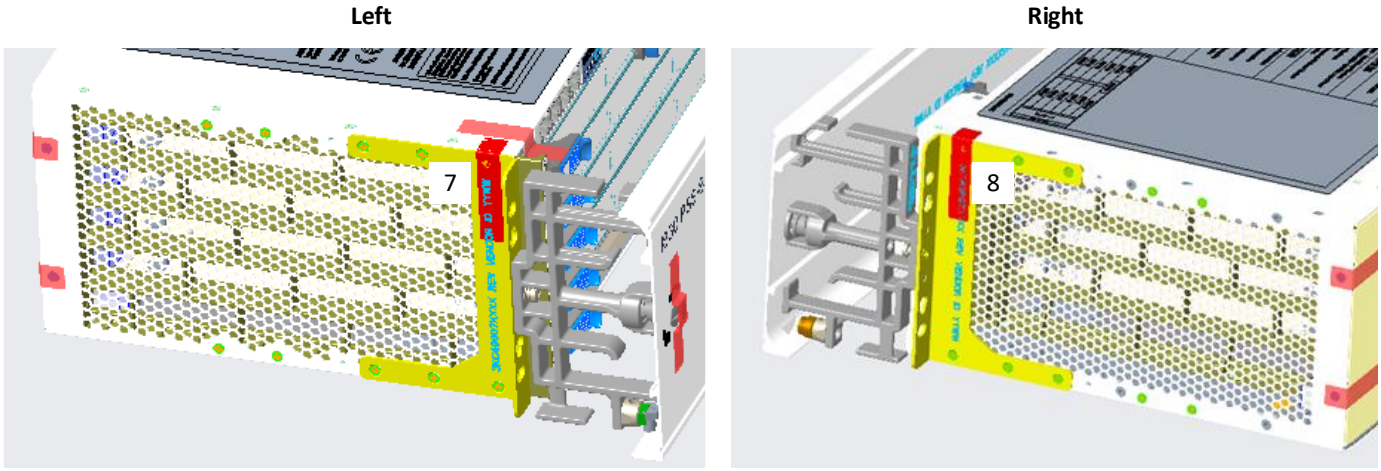
3 Place labels 5 and 6 over the over the top cover to wrap the faceplate latches.

Figure 16 - Top of an 1830 PSS-8 shelf



4 Place label 7 and 8 vertically over the 2 mounting screws that affix the front cover adaptor to the shelf.

Figure 17 - Left/Right of an 1830 PSS-8 shelf



5 Place labels 9 and 10 over the 2 mounting screws that affix the front cover to the shelf.

Figure 18 - Front of a 1830 PSS-8 shelf

6 The cryptographic boundary of the Nokia 1830 PSS-8 shelf is now sealed

END OF STEPS

Procedure 1.2: Install the tamper-evident labels on Nokia 1830 PSS-16II

Purpose

Use this procedure to provision to install the tamper-evident labels on a Nokia 1830 PSS-16II.

Steps

1 Install the 13 tamper-evident labels to seal the Nokia 1830 PSS-16II shelf.

Table 23 - Nokia 1830 PSS-16II shelf label locations

Location	Action	Reference
1	Place labels 1-5 horizontally over the 5 mounting screws that affix the rear cover to the shelf.	Figure 21, Rear of Nokia 1830 PSS-16II shelf
2		
3		
4		
5		
6	Place labels 6-7 vertically over the 2 mounting screws that affix the left bracket to the shelf.	Figure 22, Left of Nokia 1830 PSS-16II shelf
7		
8	Place labels 8 and 9 horizontally over the 2 mounting screws that affix the right bracket to the shelf.	Figure 23, Right of Nokia 1830 PSS-16II shelf
9		
10	Place labels 10 and 11 vertically over the 2 mounting screws that affix the front cover to the shelf. Place labels 12 and 13 vertically over the 2 mounting screws that affix the front cover to the fan tray.	Figure 24, Front of Nokia 1830 pss-16II shelf
11		
12		
13		

Figure 19 - Tamper labels front overall

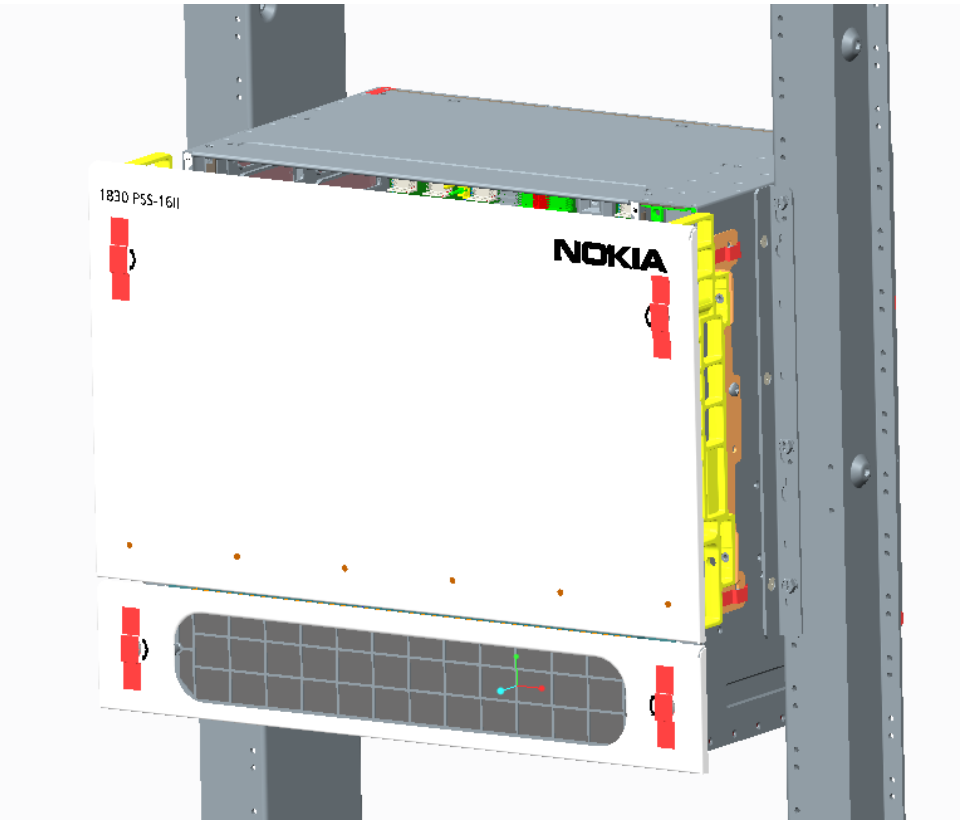
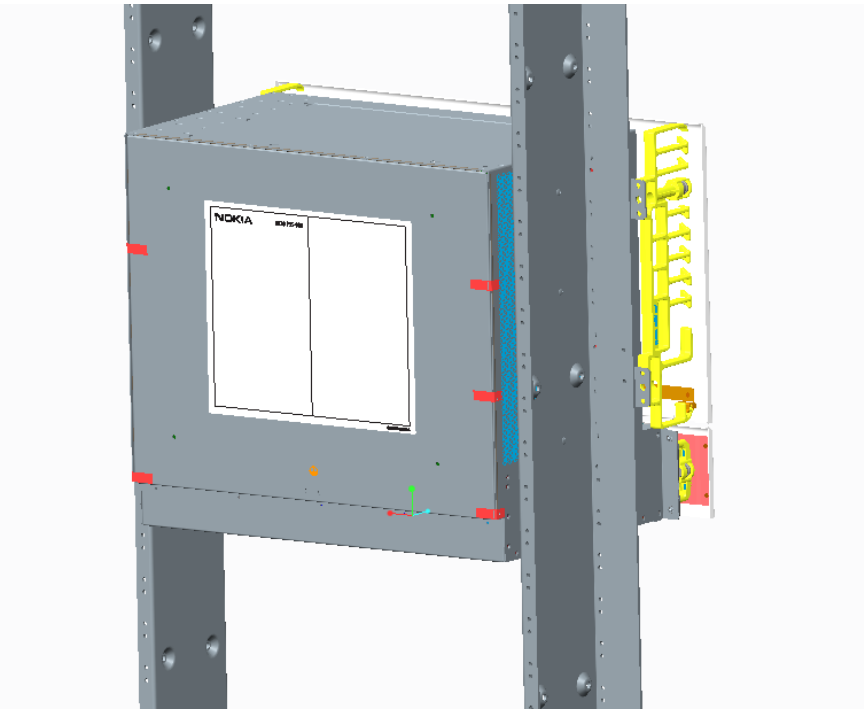
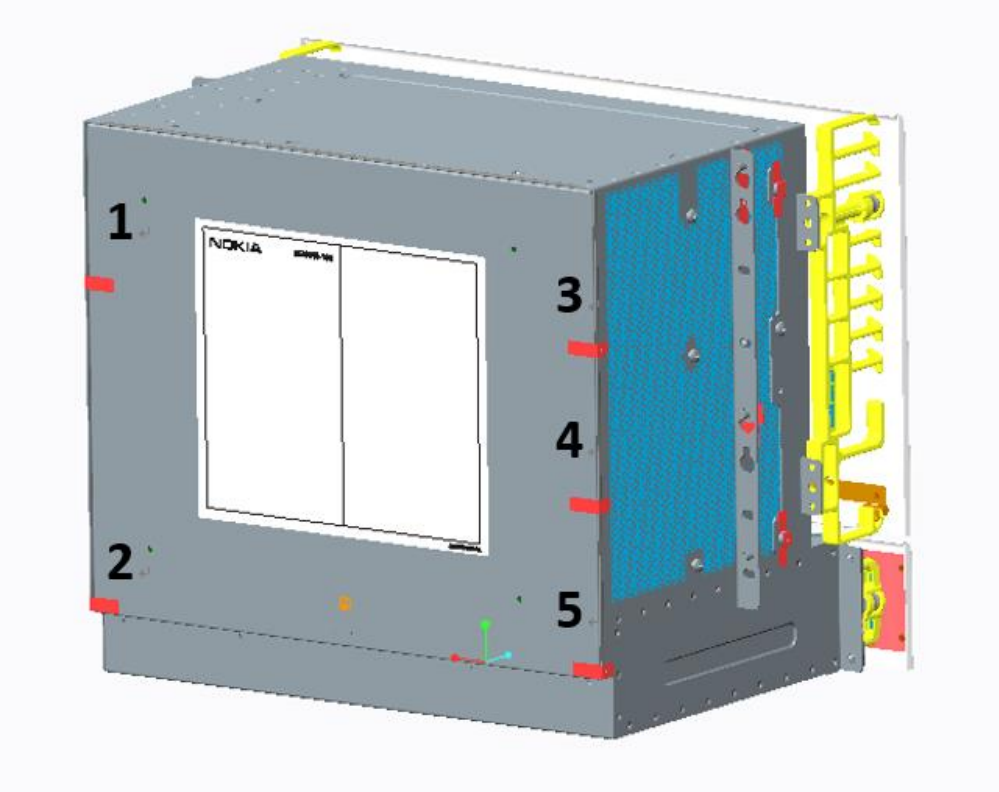


Figure 20 - Tamper labels rear overall



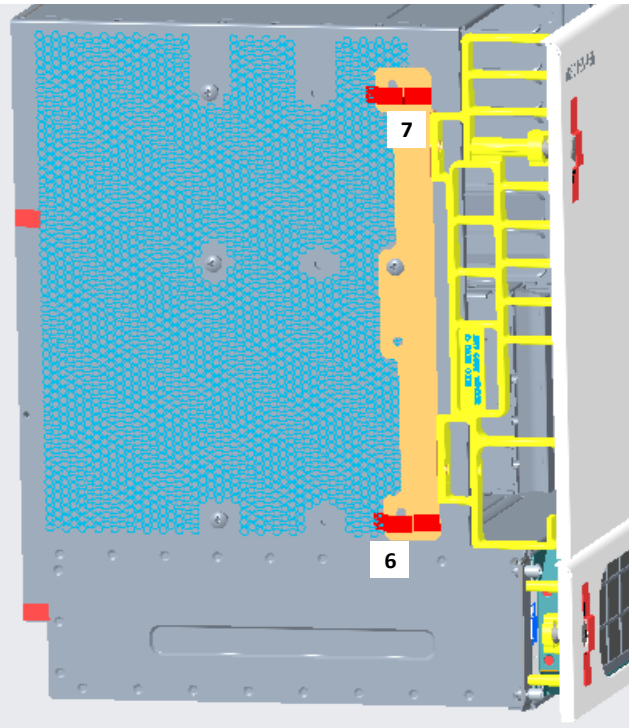
2 Place labels 1–5 vertically over the 5 mounting screws that affix the rear cover to the shelf.

Figure 21 - Rear of Nokia 1830 PSS-16II shelf



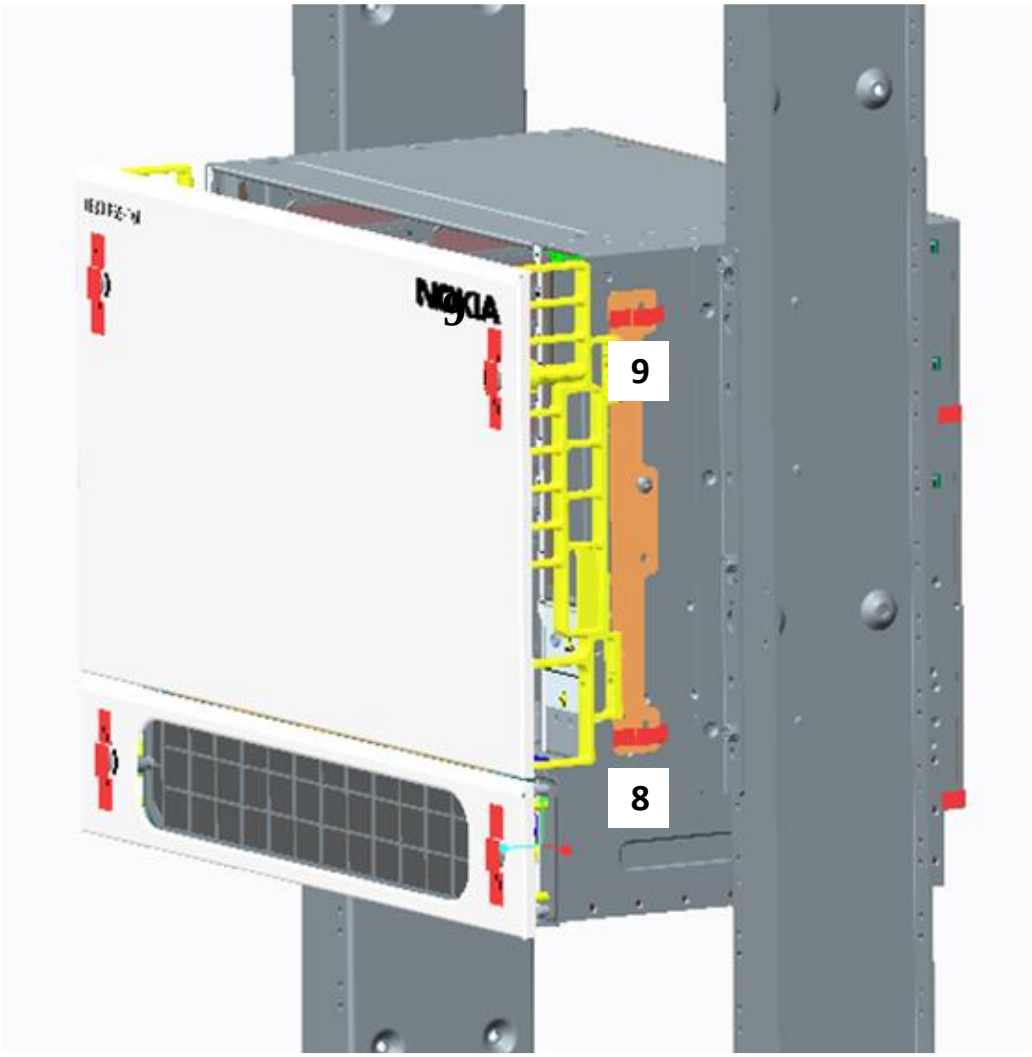
3 Place labels 6 to 7 vertically over the 2 mounting screws that affix the left bracket to the shelf.

Figure 22 - Left of Nokia 1830 PSS-16II shelf



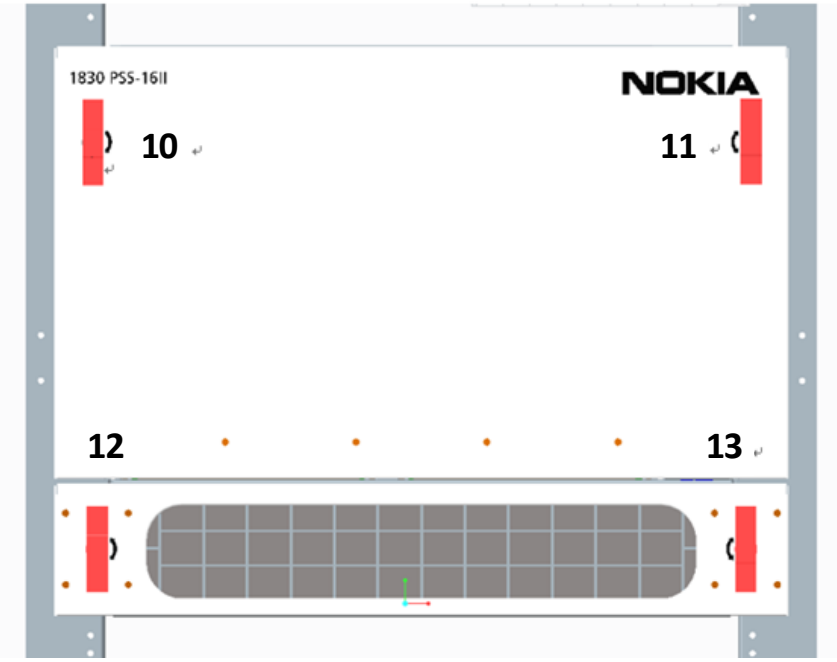
4 Place labels 8 and 9 horizontally over the 2 mounting screws that affix the right bracket to the shelf.

Figure 23 - Right of Nokia 1830 PSS-16II shelf



5 Place labels 10 and 11 vertically over the 2 mounting screws that affix the front cover to the shelf. Place labels 12 and 13 vertically over the 2 mounting screws that affix the front cover to the fan tray.

Figure 24 - Front of Nokia 1830 PSS-16II shelf



6 The cryptographic boundary of the Nokia 1830 PSS-16II shelf is now sealed

END OF STEPS

Procedure 1.3: Install the tamper-evident labels on Nokia 1830 PSS-32

Purpose

Use this procedure to provision to install the tamper-evident labels.

Steps

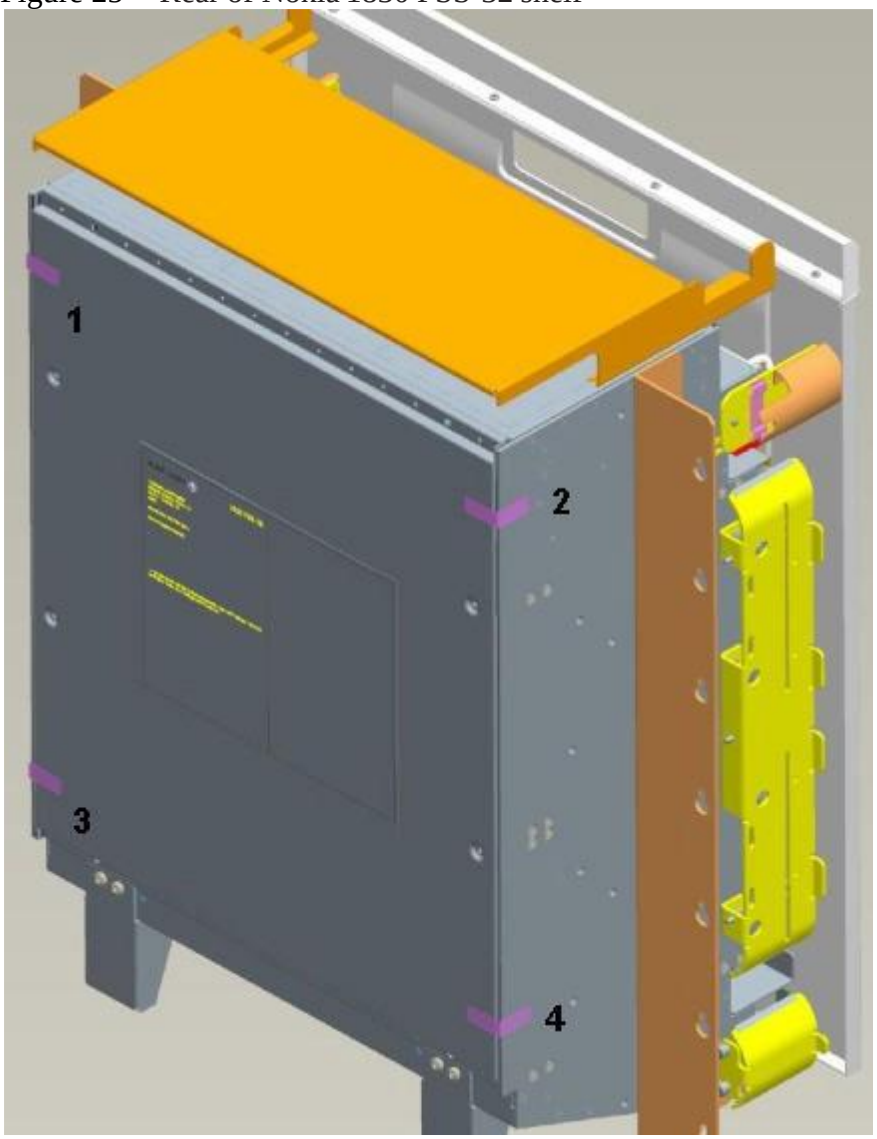
1 Install the 9 tamper-evident labels to seal the Nokia 1830 PSS-32 shelf.

Table 24 - Nokia 1830 PSS-32 shelf label locations

Location	Action	Reference
1	Place labels 1–4 horizontally over the 4 mounting screws that affix the rear cover to the shelf.	Figure 25, "Rear of Nokia 1830 PSS-32 shelf"
2		
3		
4		
5	Wrap labels 5 and 6 around each of the 2 mounting screws that affix the bottom shelf cover mounting bracket to the shelf.	Figure 26, "Close-up of location 5" Figure *27*, "Close-up of location 6"
6		
7	Place label 7 over one of the two screws that affix the top air exhaust to the shelf.	Figure 28, "Front of Nokia 1830 PSS-32 shelf"
8	Place labels 8 and 9 over the 2 mounting screws that affix the front cover to the shelf.	
9		

2 Place labels 1–4 horizontally over the 4 mounting screws that affix the rear cover to the shelf.

Figure 25 - Rear of Nokia 1830 PSS-32 shelf



3 Wrap labels 5 and 6 around each of the 2 mounting screws that affix the bottom shelf cover mounting bracket to the shelf.

Figure 26, "Close-up of location 5" illustrates a close-up view of locations 5.

Figure 26 - Close-up of location 5

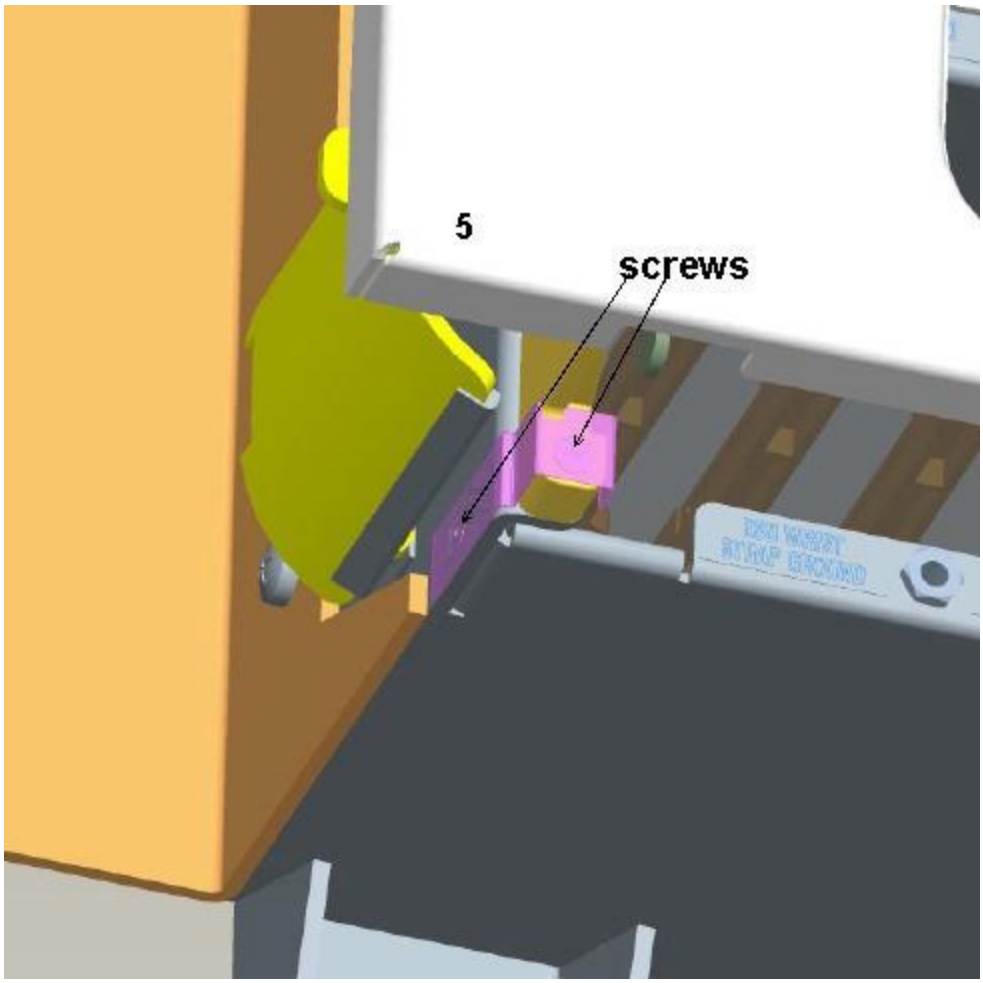
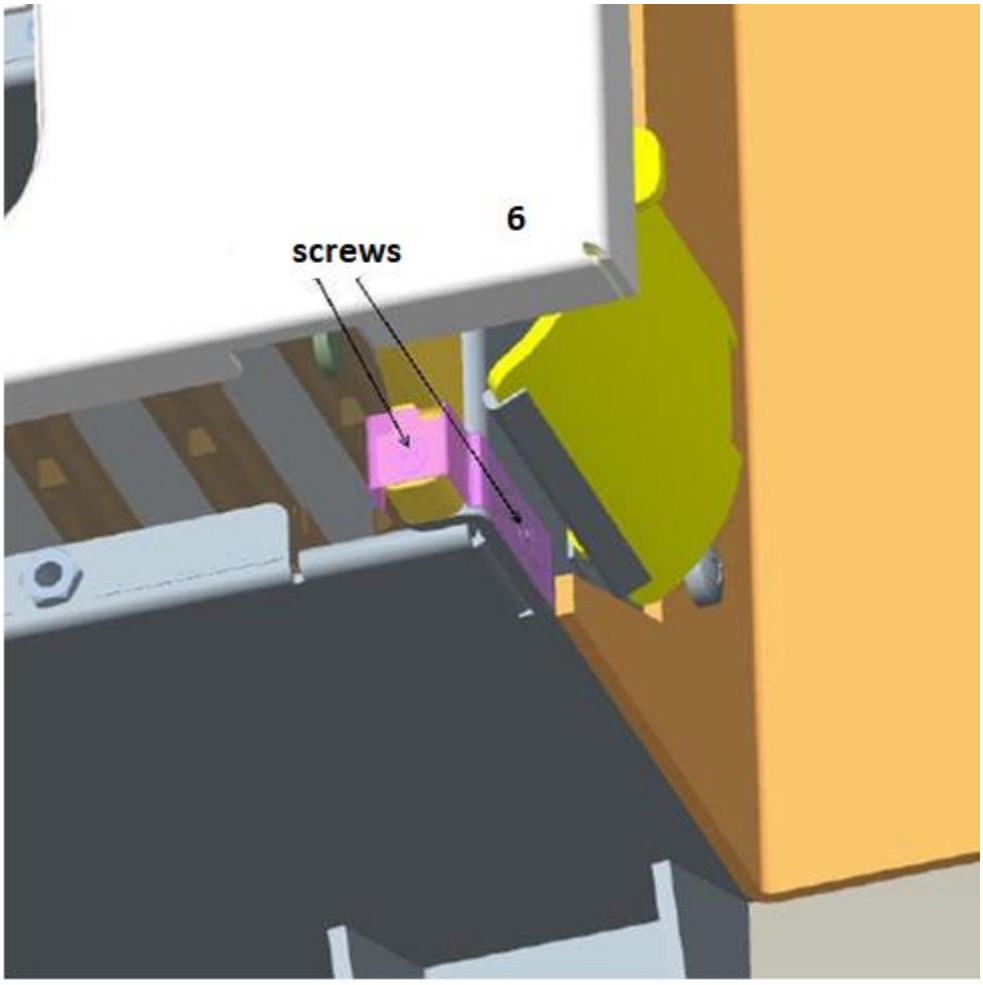


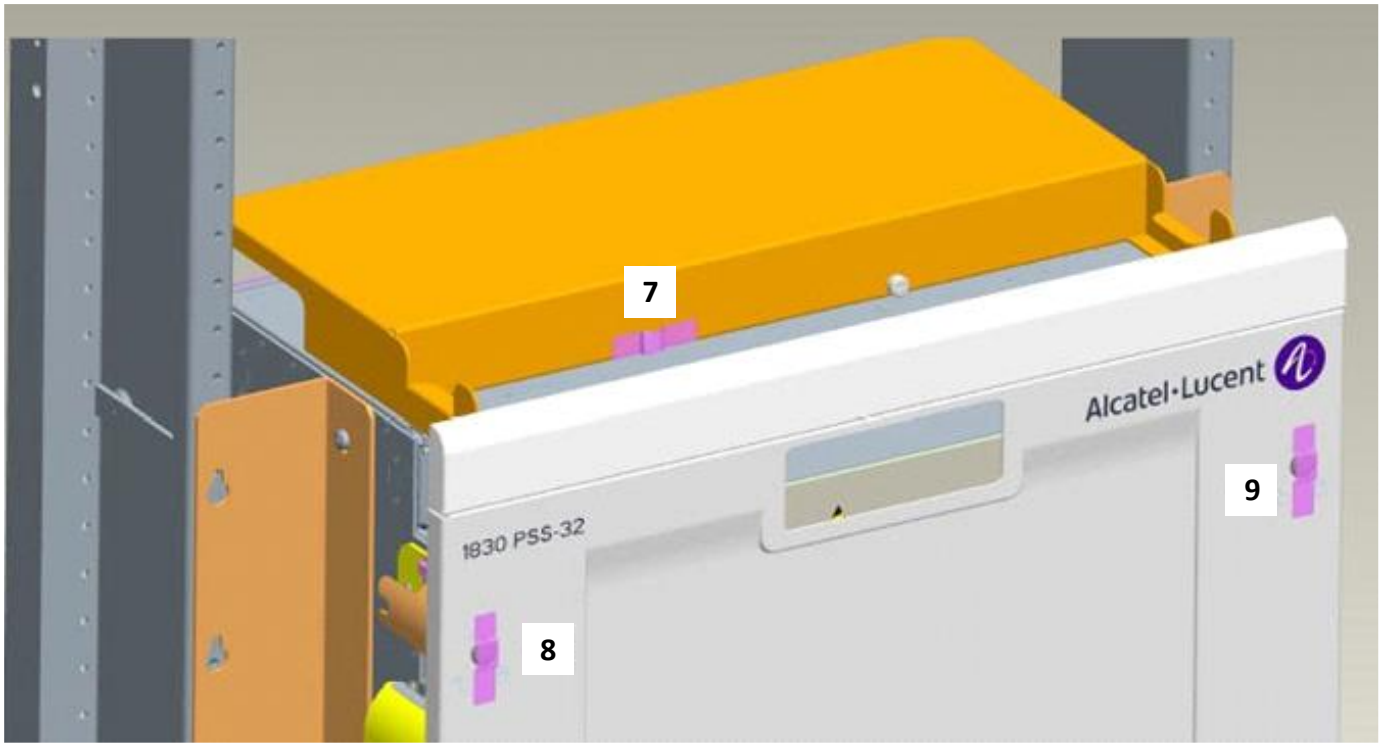
Figure 27, "Close-up of location 6" illustrates a close-up view of locations 6.

Figure 27 - Close-up of location 6



4 Place label 7 over one of the two screws that affix the top air exhaust to the shelf. Place labels 8 and 9 over the 2 mounting screws that affix the front cover to the shelf.

Figure 28 - Front of Nokia 1830 PSS-32 shelf



5 The cryptographic boundary of the Nokia 1830 PSS-32 shelf is now sealed.

END OF STEPS