# Alcatel-Lucent

Alcatel-Lucent

1830 Photonic Service Switch (PSS)

Highly Secure Configurations for Encrypted Transport

PSS-32

PSS-16

PSS-4

FW Version: 1.3.1

## HW Versions:

PSS-32 – Chassis (WOMNW00ERB / 8DG59319AA 02), EC PSS-16/PSS-32 (8DG59241AD); 11QPEN4 (8DG61458AA); Filler Card (8DG-59418-AA)

PSS-16 – Chassis (WOM3P00CRC / 8DG59859AA 03), EC PSS-16/PSS-32 (8DG59241AD); 11QPEN4 (8DG61458AA); Filler Card (8DG-59418-AA)

PSS-4 – Chassis (WOCUATAUAB / 3KC12841AA 02), EC PSS-4 (3KC-12828-ABAC); 11QPEN4 (8DG61458AA); Filler Card (8DG-59418-AA)

# FIPS 140-2 Non-Proprietary Security Policy

# FIPS Security Level: 2

# Document Version: 1.03

# Table of Contents

# 1. Introduction

This document describes the rules for use of highly secure Alcatel-Lucent 1830 PSS configurations using 11QPEN4 card for high speed encryption transport when used in accordance with FIPS 140-2 level 2 requirements. Please see reference section for a full list of the FIPS 140-2 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 Multipexer (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 AES256 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.

## 1.1 Purpose

This document covers the secure operation of the 1830 PSS-32 and 1830 PSS-16 and 1830 PSS-4 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-4, PSS-16 and PSS-32 chassis. A subset of circuit packs supported is shown in Table 1a. For a complete set of circuit packs supported, please reference to the Alcatel-Lucent 1830 Photonic Service Switch Release 7.0 Product Information and Planning Guide. The set of circuit packs that were present in the validated configurations for FIPS approved mode are designated with an asterisk(*) in this same table. Power filters marked with “+” were not physically tested with the configuration but have been design analyzed to match the power filters that were physically present during the test.

***Table 1a – List of Circuit Packs***

| Circuit Card | | PSS-4 | PSS-16 | PSS-32 |
|---|---|---|---|---|
| **Acronym** | **Description** | | | |
| EC* | Equipment Controller - 16G flashcard | N/A | Y | Y |
| E4EC* | ED4 Equipment Controller | Y | N/A | N/A |
| 11STAR1 | 11G Single Port Tunable AnyRate (1 client) | Y | Y | Y |
| 11STAR1A | 11G Single Port Tunable AnyRate (1 client) -Yahara based | Y | Y | Y |
| 11STGE12 | 11G Single Port Tunable GBE Mux (12 clients) | Y | Y | Y |
| 11DPE12 | 11G Dual Port Tunable GBE Mux (12 clients) | Y | Y | Y |
| 11DPE12E | 11G Dual Port Pluggable GBE Mux (12 client) - enhanced (SyncE, Eth OAM) | Y | Y | Y |
| 11DPE12A | 11G Dual Port Pluggable GBE Mux (12 client) - ENH2 | Y | Y | Y |
| 11DPM12 | 11G Dual Pluggable 12-anyrate Mux OT | Y | Y | Y |
| 11QPA4 | 11G, Quad Port Any rate, 4 client | Y | Y | Y |
| 11QPA4A | 11G, Quad Port Any rate HARDENED, 4 client | Y | Y | Y |
| 11QPEN4* | 11G Quad Port Pluggable SAN Encryption (card with kit) | Y | Y | Y |
| 11QPE24 | Quad 11G/10GE + 24xGE/FE Interface Board | Y | Y | Y |
| 11STMM10 | 11G Single Port Tunable Multirate Mux (10 universal clients) | Y | Y | Y |
| 4DPA4 | MSC - 4G Dual Port Pluggable AnyRate (4 clients) | Y | Y | Y |
| 4DPA2 | MSC - 4G Dual Port Pluggable AnyRate (2 clients) | Y | Y | Y |
| 43STX4 | 40G Single Port Tunable MUX (4 clients) | N/A | Y | Y |
| 43STX4P | 40G Single Port Tunable MUX (4 clients, C-band, PDPSK) | N/A | Y | Y |
| 43SCX4 | 40G Single Port Tunable Mux Coherent (4 clients) | N/A | Y | Y |
| 43SCX4E | 40G Single Port Tunable Mux Coherent (4 client), 2 slot | N/A | Y | Y |
| 43STA1P | 40G Single Port Tunable AnyRate (1 client, PDPSK) | N/A | Y | Y |
| 43STA1PB | 40G Single Port Tunable Anyrate C-Band PDPSK Enhanced | N/A | Y | Y |
| 43SCA1 | 40G Single Port Tunable Anyrate Coherent 1-client A/D | N/A | Y | Y |
| 43SCGE1 | 40GbE SPT Coherent A/D (client CFP) | N/A | Y | Y |
| 43SCUP | 43G Single Port Tunable Coherent Uplink | N/A | Y | Y |
| 112SCX10 | 112SCX10 100G Mux, 10CL, Coherent | N/A | Y | Y |
| 112SNX10 | 112SNX10 100G Mux, 10CL, ER Coherent | N/A | Y | Y |
| 112SCA1 | 112SCA1 100G A/D, 1 CL, Coherent | N/A | Y | Y |
| 112SNA1 | 112SNA1 100G, A/D 1CL, ER Coherent | N/A | Y | Y |
| 112PDM11 | 112PDM11 100G Mux, 11CL, ODB | N/A | Y | Y |

| | | | | |
|---|---|---|---|---|
| 130SCX10 | 130SCX10 100G Mux, 10CL, SDFEC Coherent | N/A | Y | Y |
| PFDC20+ | PSS-32 DC Power Filter (20A) - PSS-32 | N/A | N/A | Y |
| PFDC20+ | PSS-32 DC Power Filter (20A) - w/voltage monitoring | N/A | N/A | Y |
| PFDC30+ | PSS-32 DC Power Filter (30A) - PSS-32 | N/A | N/A | Y |
| PFDC30+ | PSS-32 DC Power Filter (30A) - w/voltage monitoring | N/A | N/A | Y |
| PFDC50+ | PSS-32 DC Power Filter (50A) - PSS-32 | N/A | N/A | Y |
| PFDC50* | PSS-32 DC Power Filter (50A) - w/voltage monitoring | N/A | N/A | Y |
| PFDC60+ | PSS-32 DC Power Filter (60A) - PSS-32 | N/A | N/A | Y |
| PFDC60+ | PSS-32 DC Power Filter (60A) - w/voltage monitoring | N/A | N/A | Y |
| PFDC70+ | PSS-32 DC Power Filter (70A) - PSS-32 | N/A | N/A | Y |
| PFDC70+ | PSS-32 DC Power Filter (70A) - w/voltage monitoring | N/A | N/A | Y |
| PFDC20K* | PSS-16 DC Power Filter (20A) - PSS-32 | N/A | Y | N/A |
| PFDC20K+ | PSS-16 DC Power Filter (20A) - w/voltage monitoring | N/A | Y | N/A |
| PFDC35K+ | PSS-16 DC Power Filter (35A) - PSS-32 | N/A | Y | N/A |
| PFDC35K+ | PSS-16 DC Power Filter (35A) - w/voltage monitoring | N/A | Y | N/A |
| E4PFDCAK+ | ED 4 POWER FILTER(-48 VDC) with WT-HARDENED (with WT clock sub card) | Y | N/A | N/A |
| E4PFDCAK* | ED 4 POWER FILTER(-48 VDC) with WT EM-HARDENED (WT clock on PF mother card) | Y | N/A | N/A |
| E4PFDCBK+ | ED 4 POWER FILTER (+/-24 VDC) with WT-HARDENED | Y | N/A | N/A |
| E4PFACK+ | ED 4 POWER FILTER (AC) with WT-HARDENED | Y | N/A | N/A |

### 1.2.1 1830 PSS-32 Version tested

The module tested is shown in Figure 1b and consists of the items described in Table 1b.

***Figure 1b – 1830 PSS-32 Module Version Tested***

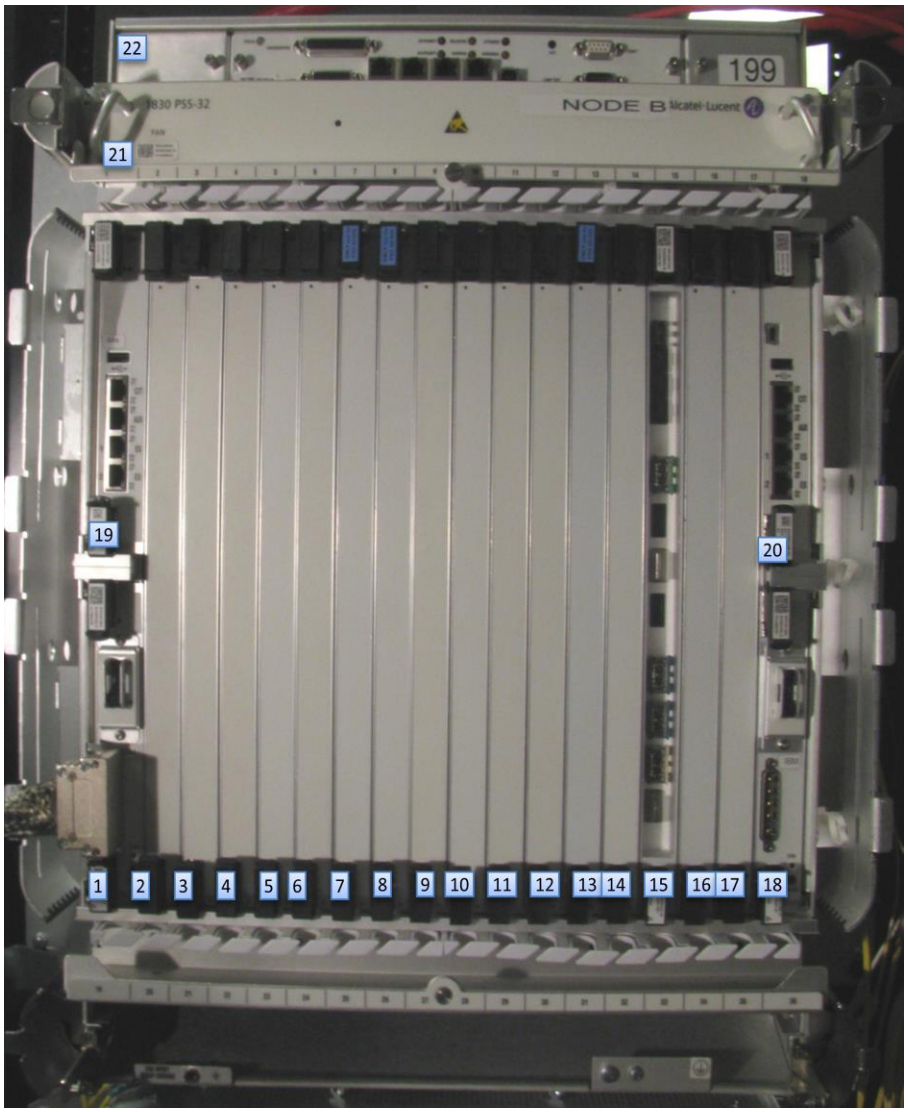


***Table 1b – 1830 PSS-32 Module Version Tested***

| Subcomponent | Description | Label in figure |
|---|---|---|
| EC PSS-16/PSS-32 | Equipment Controller (8DG59241AD) | 19, 20 |
| 11QPEN4 | Encryption card (8DG61458AA) | 15 |
| 10G MR XFP | Line XFP, 1310nm, medium reach, OTU2 | |
| 10GBASE-SR XFP | Client XFP short reach, 850nm, 10 GE | |
| 1AB396080001 | fVOA | |
| X8FCLC-L | XFP I-64.1/8.5GFC IT (8G FC XFP SM) | |
| X8FCSN-I | 8G FC XFP MM | |
| XL-64TU XFP | DWDM Tunable CT (50GHz 10G XFP) | |
| PF (-48V DC) PSS-32, 20A | Power Supply | 1, 18 |
| 8DG-59319-AAAB | CO shelf (part of FIPS KIT: 8DG-62677-AAAA) | |
| 8DG-59240-ABAA | PSS-32 User Panel (part of FIPS KIT: 8DG-62677-AAAA) | 22 |
| 8DG-6509-AAAA | Security Label Kit (part of FIPS KIT: 8DG-62677-AAAA) | |
| 8DG-61258-GAAA-TSZZA | Security Manual | |
| 8DG-59418-AA | Card Fillers | 2-14, 16, 17 |
| 8DG-59243-ABAA | High Capacity Fan (part of FIPS KIT: 8DG-62677-AAAA) | 21 |

### 1.2.2 1830 PSS-16 Version tested

The module tested is shown in Figure 1c and consists of the items described in Table 1c.

***Figure 1c– 1830 PSS-16 Module Version Tested***

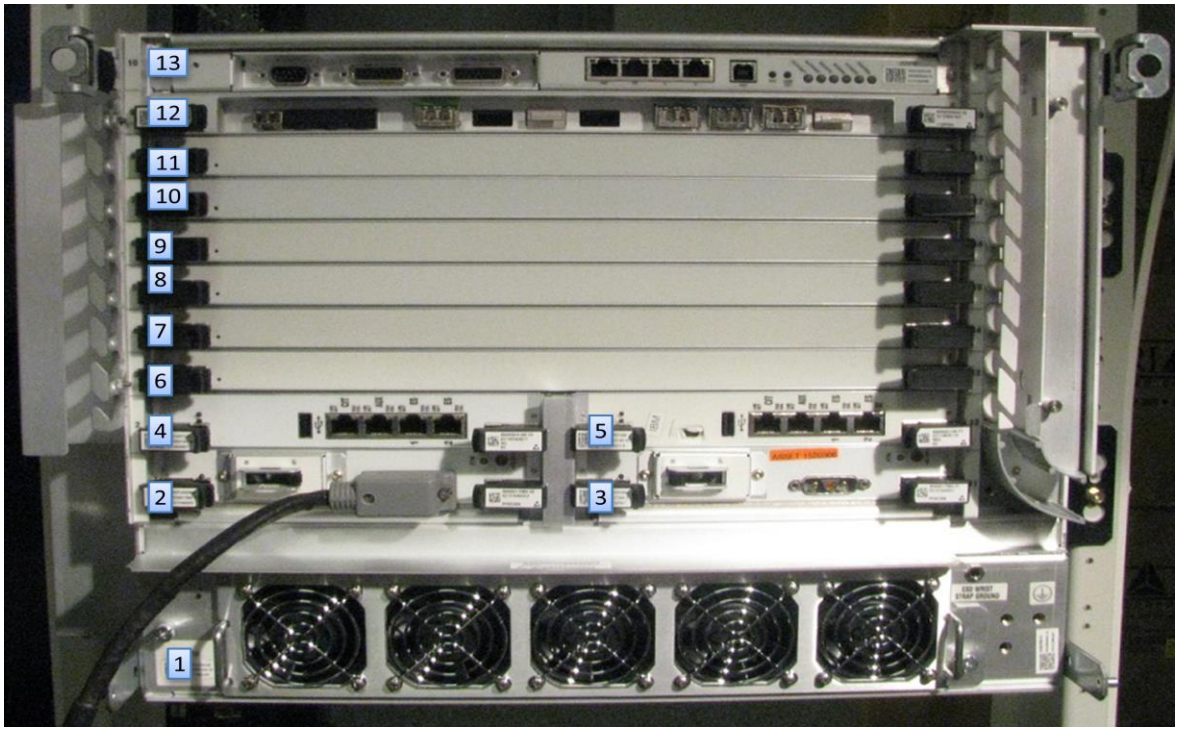



***Table 1c – 1830 PSS-16 Module Version Tested***

| Subcomponent | Description | Label in Figure |
|---|---|---|
| EC PSS-16/PSS-32 | Equipment Controller (8DG59241AD) | 4, 5 |
| 11QPEN4 | Encryption card (8DG61458AA) | 12 |
| 10G MR XFP | Line XFP, 1310nm, medium reach, OTU2 | |
| 10GBASE-SR XFP | Client XFP short reach, 850nm, 10 GE | |
| 1AB396080001 | fVOA | |
| X8FCLC-L | XFP I-64.1/8.5GFC IT (8G FC XFP SM) | |
| X8FCSN-I | 8G FC XFP MM | |
| XL-64TU XFP | DWDM Tunable CT (50GHz 10G XFP) | |
| PF (-48V DC) PSS-16, 20A | Power Supply | 2, 3 |
| 8DG-59859-AAAC | PSS-16 shelf (part of FIPS KIT: 8DG-62678-AAAA) | |
| 8DG-60094-AAAA | PSS-16 User Panel (part of FIPS KIT: 8DG-62678-AAAA) | 13 |
| 8DG-6509-AAAA | Security Label Kit (part of FIPS KIT: 8DG-62678-AAAA) | |

| | | |
|---|---|---|
| 8DG-61258-GAAA-TSZZA | Security Manual (part of FIPS KIT: 8DG-62678-AAAA) | |
| 8DG-59418-AA | Card Fillers | 6, 7, 8, 9, 10, 11 |
| 8DG-59912-AAAA | PSS16 Fan Tray (part of FIPS KIT: 8DG-62678-AAAA) | 1 |

### 1.2.3 1830 PSS-4 Version tested

The module tested is shown in Figure 1d and consists of the items described in Table 1d.

***Figure 1d – 1830 PSS-4 Module Version Tested***

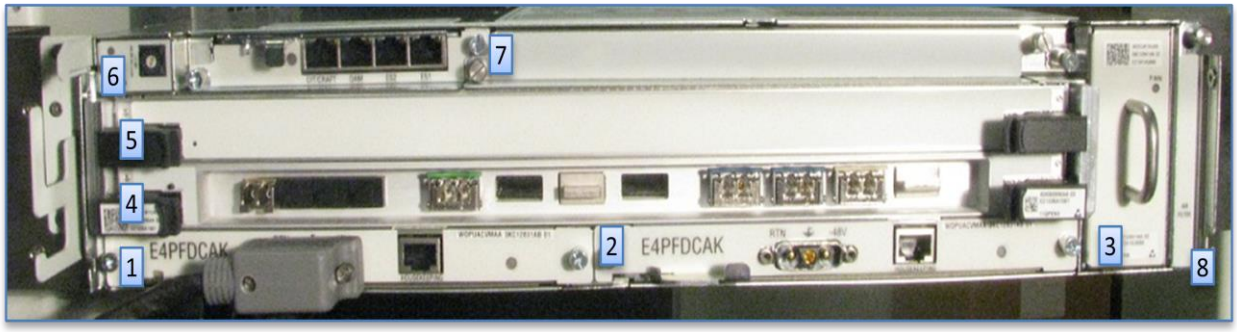



***Table 1d – 1830 PSS-4 Module Version Tested***

| Subcomponent | Description | Label in Figure |
|---|---|---|
| EC PSS-4 | EC4EC (3KC-12828-ABAC) | 6 |
| 11QPEN4 | Encryption card (8DG61458AA) | 4 |
| 10G MR XFP | Line XFP, 1310nm, medium reach, OTU2 | |
| 10GBASE-SR XFP | Client XFP short reach, 850nm, 10 GE | |
| 1AB396080001 | fVOA – fast Variable Optical Attenuator | |
| X8FCLC-L | XFP I-64.1/8.5GFC IT (8G FC XFP SM) | |
| X8FCSN-I | 8G FC XFP MM | |
| XL-64TU XFP | DWDM Tunable CT (50GHz 10G XFP) | |
| 3KC-13453-AAAA) | Shelf Kit for FIPS | 1, 2, 3, 8 |
| 3KC-13452-AAAA | PSS-4 FIPS Kit (Bracket and Air Baffle) | |
| 8DG-6509-AAAA | Security Label Kit (part of FIPS Kit: 3KC-13453-AAAA) | |
| 8DG-61258-GAAA-TSZZA | Security Manual (part of FIPS Kit: 3KC-13453-AAAA) | |
| 8DG-59418-AA | Full Slot Card Fillers (part of FIPS Kit: 3KC-13453-AAAA) | 5 |

# 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 cards.
The cryptographic module of Alcatel-Lucent Optical Encryption Solution is based on the encryption card 11QPEN4 installed on a single shelf version of a 1830 PSS with an Equipment Controller (EC). The cryptographic module consists of both hardware and software.

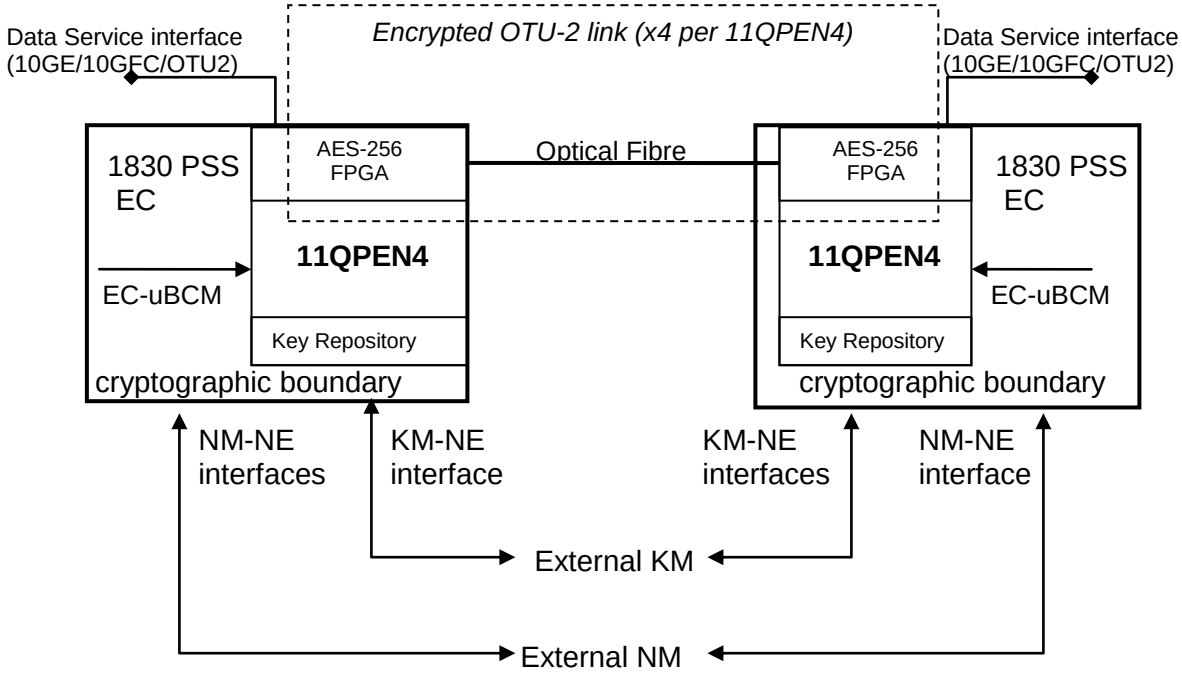



***Figure 1- Network Configuration of 1830 PSS-32/16/4***

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 while in flight between data centers. Each 11QPEN4 can be provisioned for up to 4 clients, each using its own facility optical fiber pair. The facility optical interfaces of the cryptographic module are normally equipped with DWDM XFPs so that they can be optically multiplexed by separate multi-shelf 1830 PSS system in order to minimize the number of actual fibers required between the two data center. These multi-shelf PSS systems are considered outside the boundary of the cryptographic module. This demarcation focuses the responsibility of the crypto officer functions (both for physical evidence and system logging) to the fewest number of shelves and components. The only "data" interfaces are the optical fiber interfaces on the faceplate of 11QPEN4 circuit packs. The NM-NE and KM-NE use the OAMP control/status interface to the module and use an encrypted AES256/SHA1 SNMPv3 link to ensure information is secure. The Key Manager (KM) is an operations system for managing encryption keys and security monitoring/logging of the services transmitted between cryptographic modules. The Photonic Manager (PhM) is an operations system for provisioning and monitoring parameters that are not Critical

Security Parameters(CSPs). (The PhM is also typically the operations system used by the multi-shelf PSS) The KM and the PhM are not part of the cryptographic module.

The PSS-32/PSS-16/PSS-4 shelves are a multiple-chip standalone cryptographic modules.

## 2.1 Required External Components

The cryptographic module requires the following external hardware and software in a datacenter or NOC environment.

| Datacenter Environment | Required | Purpose |
|---|---|---|
| SNMP Server | Yes | The SNMP server is a device that provides SNMPv3 functions with AuthPriv SHA1 authentication and AES256 encryption for the NM and KM. In this context a third party or an Alcatel-Lucent management product can be used. |

***Table 2: Required External Components***

## 2.2 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 3 - Security Level Per FIPS 140-2 Section***

All three of the PSS-32/PSS-16/PSS-4 platforms are hardware modules with multi-chip standalone embodiments. They are validated at overall Level 2 with section 3 validated at level 3.

## 2.3 1830 Cryptographic Module Ports and Interface

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

The only "data" interfaces that have encryption are the 11QPEN4. The OAMP is the primary status/control interface with encryption. The module features the following physical ports and LEDs: Each PSS-32/PSS-16/PSS 4 has slightly different interfaces and will be detailed below.

### 2.3.1 PSS-32 Interfaces

***Table 4- FIPS 140-2 Logical Interface mapping for 1830 PSS-32***

| Panel | Physical Ports | Quantity | FIPS 140-2 Interface |
|---|---|---|---|
| User Panel (1) – See Figure 2 below | | | |
| | OAMP | 1 | Control Input – Status Output |
| | Craft(USB) | 1 | Control Input – Status Output |
| | Craft(DB-9) | 1 | Control Input – Status Output |
| 11QPEN4 Encryption Card (up to 16) – See Figure 5 below | | | |
| | LEDs | 7 | Status Output |
| | VA | 4 | Data Input and Data Output |

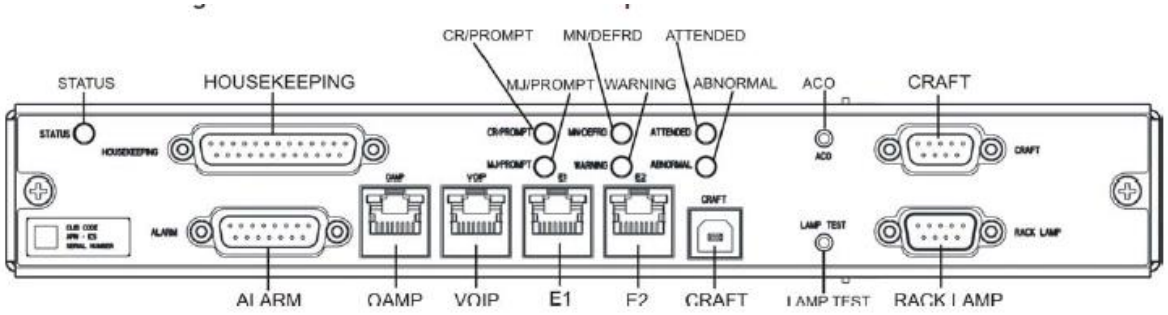



***Figure 2- PSS-32 User Panel - front view***

### 2.3.2 PSS-16 Interfaces

***Table 5- FIPS 140-2 Logical Interface mapping for 1830 PSS-16***

| Panel | Physical Ports | Quantity | FIPS 140-2 Interface |
|---|---|---|---|
| User Panel (1) – See Figure 3 below | | | |
| | OAMP | 1 | Control Input – Status Output |
| | Craft | 1 | Control Input – Status Output |
| 11QPEN4 Encryption Card (up to 3) – See Figure 5 below | | | |
| | LEDs | 6 | Status Output |
| | VA | 4 | Data Input and Data Output |

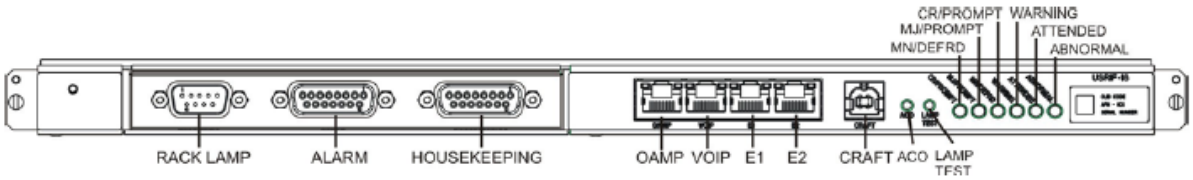



***Figure 3 - PSS-16 User Panel - front view***

### 2.3.3 PSS-4 Interfaces

***Table 6- FIPS 140-2 Logical Interface mapping for 1830 PSS-4***

| Panel | Physical Ports | Quantity | FIPS 140-2 Interface |
|---|---|---|---|
| User Panel (1) – See Figure 4 below | | | |
| | OAM | 1 | Control Input – Status Output |
| | Craft/CIT | 1 | Control Input – Status Output |
| 11QPEN4 Encryption Card (up to 1) – See Figure 5 | | | |
| | LEDs | 1 | Status Output |
| | VA | 4 | Data Input and Data Output |

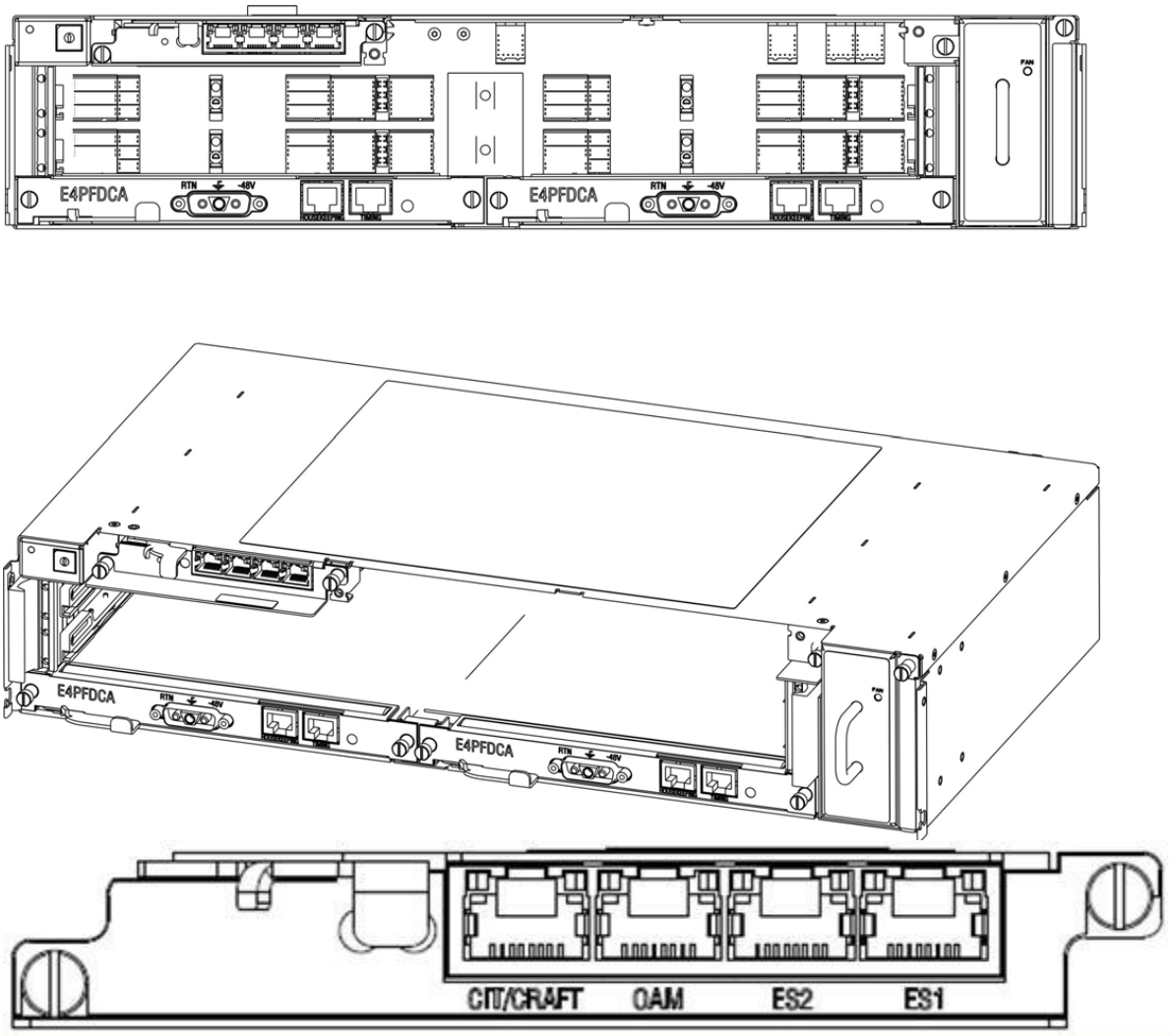



*Figure 4 - PSS-4 Shelf - front view and full shelf view and expanded view of E4EC Faceplate*

### 2.3.4 Equipment Controller PSS-16 and PSS-32

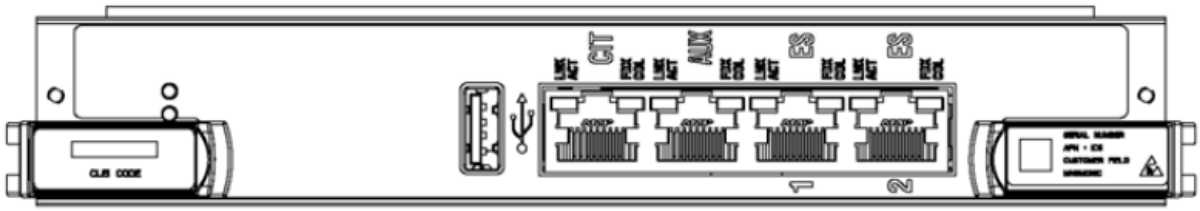



*Table 7 - FIPS 140-2 Logical Interface Mapping for Equipment Controller Card*

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

| | | |
|---|---|---|
| AUX | 1 | Not used in FIPS configuration |
| ES1 | 1 | Not used in FIPS configuration |
| ES2 | 1 | Not used in FIPS configuration |

### 2.3.5 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 5. 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).

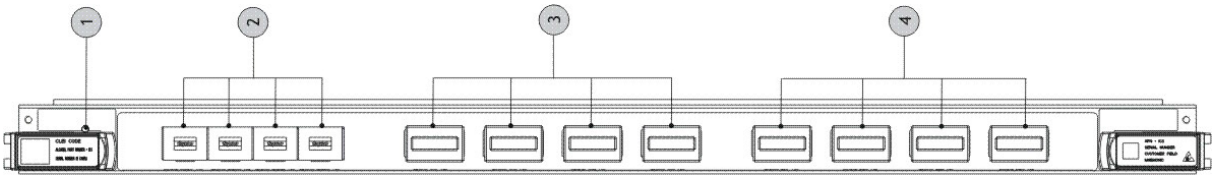



***Figure 5 - 11QPEN4 Encryption card***

**Legend:**

1 LEDs "STATUS"
2 "VA1" - "VA4" interfaces
3 "L1" - "L4" interfaces
4 "C1" - "C4" interfaces

**Note:**

***Table 8 - FIPS 140-2 Logical Interface Mapping for 11QPEN4 Card***

| Physical Ports | Quantity | FIPS 140-2 Interface |
|---|---|---|
| L1,L2,L3,L4 | 8 | Data Input – Data Output |
| C1,C2,C3,C4 | 8 | Data Input – Data Output |
| LEDs | 1 | Status |

## 2.4 Roles, Services, and Authentication

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

2) User Role which is referred to as ‘Crypto’

### 2.4.1 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 9 – Crypto Officer (Admin) Service Table

| Service | Operator | Description | Input | Output | Key\CSP Access (R\W\X) |
|---|---|---|---|---|---|
| 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<br>SNMPv3 Authentication Key – W<br>SNMPv3 Privacy Key - W |
| Commission the Module (Invoke FIPS mode) | 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 |
| Zeroize Keys | Admin | Zeroize keys and CSPs over SNMPv3 and CLI interfaces | Command and Parameters | Command Response | Crypto or User Password - W<br>SNMP Crypto (KM) or Admin (PhM) password - W<br>SNMPv3 Proxy Authentication Key - W<br>SNMPv3 Proxy Privacy Key – W<br>11QPEN4 Session Encryption |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | Key - W<br>11QPEN4 Session KAT Key - W |
| Session initiation | Admin | Initiate session with another module using AES keys. | Command and Parameters | Command Response | AES key - W |

### 2.4.2 User Role

A user is a non-Crypto Officer access to the system. The operator can be categorized based on their privilege: Administrator. A good principle in highly secure systems is restricted access and authentication. The expectation is a well-controlled number of operators would be assigned identity based Admin privileges to 1830 systems operating in FIPS mode. These services are all Approved services.

Table 10 – 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 |
| 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 |

| | | | | | |
|---|---|---|---|---|---|
| Zeroize Keys | Crypto | Zeroize keys and CSPs over SNMPv3 interfaces | Command and Parameters | Command Response | Crypto or User Password - W<br>SNMP Crypto (KM) or Admin (PhM) password - W<br>SNMPv3 Proxy Authentication Key - W<br>SNMPv3 Proxy Privacy Key – W<br>11QPEN4 Session Encryption Key - W<br>11QPEN4 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

### 2.4.3 Authentication

**Table 11 – Strengths of Authentication Mechanisms**

| Authentication Mechanism | Strength of Mechanism |
|---|---|
| Cyrpto Officer Admin and Crypto User password (CLI) | Minimum password length is 8 characters. There are 26 lower case plus 26 upper case plus 10 digits plus 14 special characters for a total of 76 characters. The minimum combinations that are possible are:<br>$76^8$ = 1,113,034,787,454,980.<br>After a failed login attempt, the system delays for 2 seconds prior to presenting the next login prompt Therefore, 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<br>1 : $76^8$ possible passwords / ((6 ×109 bits per minute) / 64 bits per password)]<br><br>1: 1,113,034,787,454,980 possible passwords / 31 passwords per minute)<br>1:172,305,160,258<br>or 1 in 172 billion, which is a smaller probability than 1 in 100,000 as required by FIPS 140-2 |
| Crypto Officer Admin and Crypto User password (SNMP) | The user login account for crypto user is created by the user manually at system turn up after the ”config admin ui” is set to FIPS. The password word can be entered from 12 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 password length of 12, the minimum combinations that are possible are 3.226E+21.<br>The fastest network connection supported by the module is 100 Mbps. Hence at most (100 ×106 × 60 = 6 × 109 =) 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<br>1 : $62^{12}$ possible passwords / ((6 ×109 bits per minute) / 64 bits per password)]<br>1: $3.226*10^{21}$ passwords / 93,750,000 passwords per minute) |

| | |
|---|---|
| | 1: 34,413,512,132,244, which is a smaller probability than 1:100,000 as required by FIPS 140-2 |

## 2.5 Physical security

### Overview

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

### Cryptographic boundary

The cryptographic boundary of the 1830 PSS shelves is different for each shelf type.

- For Alcatel-Lucent 1830 PSS-4, the cryptographic boundary configuration is defined as being the outer perimeter of the enclosure.
- For Alcatel-Lucent 1830 PSS-16, the cryptographic boundary configuration is defined as being the outer perimeter of the enclosure including the front cover.
- For Alcatel-Lucent 1830 PSS-32, the cryptographic boundary configuration is defined as the outer perimeter of the enclosure including the high-capacity fan unit and front cover.

### Physical security mechanisms

After the shelf has been configured to meet FIPS 140-2 Level 2 requirements, 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 1.2: “Install 11QPEN4” (p. 54) for detailed instructions on tamper-evident label placement.
- Provision the cryptographic module to operate in a FIPS mode. Refer to Procedure 1: “Provision the shelf for FIPS mode” (p. 47) for detailed instructions.
- EC cards are installed in EC slots and at least one 11QPEN4 pack is installed in
  - Alcatel-Lucent 1830 PSS-4 slot 7.
  - Alcatel-Lucent 1830 PSS-16 slots 7, and/or 8, and/or 9
  - Alcatel-Lucent 1830 PSS-32 slots 2–17
- all unpopulated slots are equipped with filler cards

### Tamper-evident labels

Tamper-evident labels shall be installed for the module to operate in a FIPS-approved mode of operation.

The following graphics illustrate a tamper-evident label.

Figure 8, "Tamper-evident label: intact" (p. 21) illustrates a tamper-evident label with no evidence of tampering.

**Figure 8 Tamper-evident label: intact**

Figure 9, "Tamper-evident label: broken (normal view)" (p. 22) illustrates a tamper-evident label that shows signs of tampering. Figure 10, "Tamper-evident label: broken (close-up view)" (p. 23) is a magnified view of the broken label. 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 9 Tamper-evident label: broken (normal view)**

Figure 10 Tamper-evident label: broken (close-up view)


### 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. If the label is not flat when affixed to the shelf, the barcode may not scan.

### Inspect labels

The Crypto Officer is also responsible for inspecting the tamper-evident labels on the shelves at least every 3 months. If any evidence of tampering is observed on the tamper-evident seals, the module shall be considered to be in a non-compliant state.

Upon such discovery, the Admin shall decommission the module and return to the vendor.

Detailed procedures on affixing labels for PSS-32, PSS-16 and PSS-4 are given in Appendix A.

## 2.6 Operational Environment

The operational environment is non-modifiable.

## 2.7 Cryptographic Key Management

For an algorithm implementation to be listed on a cryptographic module validation certificate as an Approved security function, the algorithm implementation shall meet all the requirements of FIPS 140-2 and shall successfully complete the cryptographic algorithm validation process.

Table 14– List of FIPS 140-2 Algorithms Certicates for 1830 PSS

| Algorithm | Alcatel-Lucent PSS-4 Crypto-SNMP Engine (EC) | Alcatel-Lucent PSS-32/16 Crypto-SNMP Engine (EC) | Alcatel-Lucent Crypto-OTU2 Engine (11QPEN4) |
|---|---|---|---|
| AES-256 in CFB128 Mode: CFB128 ( e/d; 256) | #2829 | #2830 | n/a |
| SHS-1 | #2370 | #2371 | n/a |
| CVL (SNMP) | #255 | #256 | n/a |
| AES-256 in CTR mode: CTR ( e; 256) | n/a | n/a | #2828 |

The module also uses the non-Approved but Allowed MD5 algorithm in the integrity test. The module also uses AES Certificates #2829 and #2830 to perform key wrapping.

Definition of CSPs Modes of Access
Table 15 defines the relationship between access to CSPs and the different module services.

Table 15 – List of Crypto Keys and CSPs

| CSP | CSP Type | Generation /Input | Output | Storage | Zeroization | Use |
|---|---|---|---|---|---|---|
| SNMP Crypto officer(Admin) or User (Crypto) password | Alpha-Numeric string | Entered into module at local console at initial provisioning | Never exits the module | Not stored-converted to Authenticaion and privacy keys | Zeroized when password is updated with a new one | Authentication |
| 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 password 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 password is updated with a new one | Used to encrypt during communication via SNMPv3 |
| 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 |
| 11QPEN4 Session 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 FPGA | Zeroized when new string is entered or when service is deleted | Used to authenticate traffic data connection |
| | | | | | | |

## 2.8 Self-Tests

The 1830 PSS-32/PSS-16/PSS-4 perform known answer tests and critical functions tests at power up. See table 16-18.

**Table 16 – Power-Up Known Answer Self-Tests PSS-32**

| 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/ECB. |
| AES Decrypt FPGA KAT (11QPEN4 cards) | Decrypt Known answer test for AES-256 CTR/ECB. |
| SHA KAT | Known answer test for SHA-1 |
| Firmware Integrity Test | All the cryptographic firmware modules are contained in rpm files in the compact flash on the EC card and are verified by MD5 checksum during the firmware startup. |

**Table 17 – Power-Up Known Answer Self-Tests PSS-16**

| 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/ECB. |
| AES Decrypt FPGA KAT (11QPEN4 cards) | Decrypt Known answer test for AES-256 CTR/ECB. |
| SHA KAT | Known answer test for SHA-1 |
| Firmware Integrity Test | All the cryptographic firmware modules are contained in rpm files in the compact flash on the EC card and are verified by MD5 checksum during the firmware startup |

**Table 18 – Power-Up Known Answer Self-Tests PSS-4**

| 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/ECB. |
| AES Decrypt FPGA KAT (11QPEN4 cards) | Decrypt Known answer test for AES-256 CTR/ECB. |
| SHA KAT | Known answer test for SHA-1 |

| | |
|---|---|
| Firmware Integrity Test | All the cryptographic firmware modules are contained in rpm files in the compact flash on the EC card and are verified by MD5 checksum during the firmware startup |

## 2.9 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 FIPS mode of operation

You shall place the module in FIPS mode with the admin user privilege.
To access the system with a admin user privilege, you must log into the CLI through a encrypted connection. Local CLI can be used to display FIPS UI and FIPS-Squelch settings.
For PSS-4 only: Install the PSS-4 FIPS Kit (bracket and air baffle)- (Refer to instructions Appendix A – Procedure 1)
For PSS-16 only: The 1830 PSS-16 module shall be mounted in an ANSI Bay Frame (for example KIT part #: 1AD139370001).
All subcomponents (11QPEN4 / filler cards) must be installed in the 1830 PSS shelf before the 1830 PSS is configured to operate in FIPS mode.

### 3.1.1 Configuring the 1830 PSS for FIPS operation

1. Verify the NE will come up with default values after loading factory load (TID=NE, OAMP IP address=0.0.0.0, Loopback IP address=172.16.1.1)
2. Connect a PC to the NE's CIT port and open WebUI. [WebUI and SSH is only used for initial provisioning from the local CIT port and are disabled in the last steps of initial provisioning.]
3. NE comes up with TID=NE, login using admin/admin
4. User is prompt to change TID or to initialize DB (do not initialize DB at this time).
5. Provision TID. DB invalid alarm will still be present.
6. Setup FTP server on PC and make sure the R7 NE software is already on the PC.
7. Login to NE again and provision the FTP server with the PC FTP server info.

   7a For PSS4 only: provision slot to be 11QPEN4

8. Upgrade the NE from factory load to R7 (audit, load, activate).
9. Clear the database (config database clear) – DBINVALID should clear
10. Commit the software.
11. Provision Loopback IP address – NE reboots
12. Provision OAMP IP address
13. Provision CN default route.

**# System installation**

14. Install 11QPEN4s and Filler cards
15. Bring ES1 and ES2 state Down
16. Generate SSH keys [webUI] . [WebUI and SSH is only used for initial provisioning from the local CIT port and are disabled in the last steps of initial provisioning.]
17. config admin ui mode fips / [WebUI]
18. config general fips-squelching enable / [WebUI]

**# Disabling service user [CLI] / [WebUI]**

19. con admin users serviceAcc disabled

**# Create snmpv3 users, crypto user**

**20. Create snmpv3 user(nms)**

21. **Create snmpv3 crypto user**
22. Add to PhM
23. Add to KMT

**# PASSWORDS**

# Changing Admin password to FIPS compliant : [webUI]
# the “qweQWE123!@#” is an example password
24. qweQWE123!@#

**# Intrusion attempt handling [webUI]**

25. Administration -> Security -> System
26. Maximum Invalid Login Attempts: 5
27. Minimum wait after invalid login: 60

**# ACL Filters**

```
## Enable to make change in IP ACL
1. config acl_default snmpConfig enable


## Create BlockSsh
2. config acl_pattern BlockSsh
3. config acl_pattern BlockSsh action block
4. config acl_pattern BlockSsh ipProto TCP
5. config acl_pattern BlockSsh dstPort 22
```

```
## Create BlockHttps
6. config acl_pattern BlockHttps
7. config acl_pattern BlockHttps action block
8. config acl_pattern BlockHttps ipProto TCP
9. config acl_pattern BlockHttps dstPort 443


## Create BlockSsh5122
10. config acl_pattern BlockSsh5122
11. config acl_pattern BlockSsh5122 action block
12. config acl_pattern BlockSsh5122 ipProto TCP
13. config acl_pattern BlockSsh5122 dstPort 5122


## Create BlockNtp
14. config acl_pattern BlockNtp
15. config acl_pattern BlockNtp action block
16. config acl_pattern BlockNtp ipProto UDP
17. config acl_pattern BlockNtp dstPort 123


## Create BlockTcp3082 TL1 raw between OCS and NE ucmTL1
18. config acl_pattern BlockTcp3082
19. config acl_pattern BlockTcp3082 action block
20. config acl_pattern BlockTcp3082 ipProto TCP
21. config acl_pattern BlockTcp3082 dstPort 3082


## Create BlockTcp3083 TL1 telnet
22. config acl_pattern BlockTcp3083
23. config acl_pattern BlockTcp3083 action block
24. config acl_pattern BlockTcp3083 ipProto TCP
25. config acl_pattern BlockTcp3083 dstPort 3083


## Create dhcp server blocker.  request to a dhcp server
26. config acl_pattern BlockUdp67
27. config acl_pattern BlockUdp67 action block
28. config acl_pattern BlockUdp67 ipProto UDP
29. config acl_pattern BlockUdp67 dstPort 67


## Create Blockudp111 portmapper
30. config acl_pattern BlockUdp111
```

```
31. config acl_pattern BlockUdp111 action block
32. config acl_pattern BlockUdp111 ipProto UDP
33. config acl_pattern BlockUdp111 dstPort 111

## Create BlockTcp111 portmapper
34. config acl_pattern BlockTcp111
35. config acl_pattern BlockTcp111 action block
36. config acl_pattern BlockTcp111 ipProto TCP
37. config acl_pattern BlockTcp111 dstPort 111

## Create BlockUdp138 Netbios-dgm
38. config acl_pattern BlockUdp138
39. config acl_pattern BlockUdp138 action block
40. config acl_pattern BlockUdp138 ipProto UDP
41. config acl_pattern BlockUdp138 dstPort 138

## Create BlockTcp513 login,rsh
42. config acl_pattern BlockTcp513
43. config acl_pattern BlockTcp513 action block
44. config acl_pattern BlockTcp513 ipProto TCP
45. config acl_pattern BlockTcp513 dstPort 513

## Create BlockUdp514 syslog
46. config acl_pattern BlockUdp514
47. config acl_pattern BlockUdp514 action block
48. config acl_pattern BlockUdp514 ipProto UDP
49. config acl_pattern BlockUdp514 dstPort 514

## Create BlockTcp662 rpc.statd
50. config acl_pattern BlockTcp662
51. config acl_pattern BlockTcp662 action block
52. config acl_pattern BlockTcp662 ipProto TCP
53. config acl_pattern BlockTcp662 dstPort 662

## Create BlockUdp662 rpc.statd
54. config acl_pattern BlockUdp662
55. config acl_pattern BlockUdp662 action block
56. config acl_pattern BlockUdp662 ipProto UDP
```

```
57. config acl_pattern BlockUdp662 dstPort 662


## Create BlockTcp892 rpc.mount
58. config acl_pattern BlockTcp892
59. config acl_pattern BlockTcp892 action block
60. config acl_pattern BlockTcp892 ipProto TCP
61. config acl_pattern BlockTcp892 dstPort 892


## Create BlockUdp892 rpc.mount
62. config acl_pattern BlockUdp892
63. config acl_pattern BlockUdp892 action block
64. config acl_pattern BlockUdp892 ipProto UDP
65. config acl_pattern BlockUdp892 dstPort 892


## Create BlockUdp894 rpc.statd
66. config acl_pattern BlockUdp894
67. config acl_pattern BlockUdp894 action block
68. config acl_pattern BlockUdp894 ipProto UDP
69. config acl_pattern BlockUdp894 dstPort 894


## Create BlockUdp895 rpc.statd
70. config acl_pattern BlockUdp895
71. config acl_pattern BlockUdp895 action block
72. config acl_pattern BlockUdp895 ipProto UDP
73. config acl_pattern BlockUdp895 dstPort 895


## Create BlockTcp2049 rpc.nfsd
74. config acl_pattern BlockTcp2049
75. config acl_pattern BlockTcp2049 action block
76. config acl_pattern BlockTcp2049 ipProto TCP
77. config acl_pattern BlockTcp2049 dstPort 2049


## Create BlockUdp2049 nfs
78. config acl_pattern BlockUdp2049
79. config acl_pattern BlockUdp2049 action block
80. config acl_pattern BlockUdp2049 ipProto UDP
81. config acl_pattern BlockUdp2049 dstPort 2049
```

```
## Create BlockTcp2607 ospfd api
82. config acl_pattern BlockTcp2607
83. config acl_pattern BlockTcp2607 action block
84. config acl_pattern BlockTcp2607 ipProto TCP
85. config acl_pattern BlockTcp2607 dstPort 2607


## Create BlockUdp3084 TL1 multicast
86. config acl_pattern BlockUdp3084
87. config acl_pattern BlockUdp3084 action block
88. config acl_pattern BlockUdp3084 ipProto UDP
89. config acl_pattern BlockUdp3084 dstPort 3084


## Create BlockTcp7000 epic telnet
90. config acl_pattern BlockTcp7000
91. config acl_pattern BlockTcp7000 action block
92. config acl_pattern BlockTcp7000 ipProto TCP
93. config acl_pattern BlockTcp7000 dstPort 7000


## Create BlockTcp7162  epic TCP port
94. config acl_pattern BlockTcp7162
95. config acl_pattern BlockTcp7162 action block
96. config acl_pattern BlockTcp7162 ipProto TCP
97. config acl_pattern BlockTcp7162 dstPort 7162


## Create BlockTcp11222  sntp but no executable associated
98. config acl_pattern BlockTcp11222
99. config acl_pattern BlockTcp11222 action block
100.config acl_pattern BlockTcp11222 ipProto TCP
101.config acl_pattern BlockTcp11222 dstPort 11222


## Create BlockUdp50015 lom-inet
102.config acl_pattern BlockUdp50015
103.config acl_pattern BlockUdp50015 action block
104.config acl_pattern BlockUdp50015 ipProto UDP
105.config acl_pattern BlockUdp50015 dstPort 50015


## Create a filter for use in OampRx
106.config acl_filter FipsOampRx
```

```
107. config acl_filter FipsOampRx add pattern BlockSsh 1
108. config acl_filter FipsOampRx add pattern BlockHttps 2
109. config acl_filter FipsOampRx add pattern BlockSsh5122 3
110. config acl_filter FipsOampRx add pattern BlockNtp 4
111. config acl_filter FipsOampRx add pattern BlockTcp3082 5
112. config acl_filter FipsOampRx add pattern BlockTcp3083 6
113. config acl_filter FipsOampRx add pattern BlockUdp67 7
114. config acl_filter FipsOampRx add pattern BlockUdp111 8
115. config acl_filter FipsOampRx add pattern BlockTcp111 9
116. config acl_filter FipsOampRx add pattern BlockUdp138 10
117. config acl_filter FipsOampRx add pattern BlockTcp513 11
118. config acl_filter FipsOampRx add pattern BlockUdp514 12
119. config acl_filter FipsOampRx add pattern BlockTcp662 13
120. config acl_filter FipsOampRx add pattern BlockUdp662 14
121. config acl_filter FipsOampRx add pattern BlockTcp892 15
122. config acl_filter FipsOampRx add pattern BlockUdp892 16
123. config acl_filter FipsOampRx add pattern BlockUdp894 17
124. config acl_filter FipsOampRx add pattern BlockUdp895 18

125. config acl_filter FipsOampRx add pattern BlockTcp2049 23
126. config acl_filter FipsOampRx add pattern BlockUdp2049 24
127. config acl_filter FipsOampRx add pattern BlockTcp2607 25
128. config acl_filter FipsOampRx add pattern BlockUdp3084 26
129. config acl_filter FipsOampRx add pattern BlockTcp7000 27
130. config acl_filter FipsOampRx add pattern BlockTcp7162 28
131. config acl_filter FipsOampRx add pattern BlockTcp11222 29
132. config acl_filter FipsOampRx add pattern BlockUdp50015 30

## Also add back the original default pattern in fips mode at the highest
numbered entries
133. config acl_filter FipsOampRx add pattern SysPattern33 247
134. config acl_filter FipsOampRx add pattern SysPattern32 248
135. config acl_filter FipsOampRx add pattern SysPattern31 249
136. config acl_filter FipsOampRx add pattern SysPattern30 250
137. config acl_filter FipsOampRx add pattern SysPattern06 251
138. config acl_filter FipsOampRx add pattern SysPattern05 252
139. config acl_filter FipsOampRx add pattern SysPattern04 253
140. config acl_filter FipsOampRx add pattern SysPattern03 254
141. config acl_filter FipsOampRx add pattern SysPattern02 255
142. config acl_filter FipsOampRx add pattern SysPattern01 256
```

```
## Now remove the binding at oamp
// PSS32
143. config acl_port 1/40/oamp rx remove filter

// PSS16
144. config acl_port 1/10/oamp rx remove filter

// PSS4
145. config acl_port 1/1/oamp rx remove filter


// PSS32
146. config acl_port 1/40/oamp rx add filter FipsOampRx enabled

//PSS16
147. config acl_port 1/10/oamp rx add filter FipsOampRx enabled

//PSS4
148. config acl_port 1/1/oamp rx add filter FipsOampRx enabled


149. // Disable the edit of IP ACL

// User may not be able to execute this CLI command if the above execution
is performed at network interface related session
// such as ssh or webUI. The above rules are blocking https and ssh.
```

#Show ACL CLI commands

150. show acl_default
151. show acl_filter *
152. show acl_pattern *
153. show acl_port *
154. Admin account (Crypto-Officer role) to perform a show status
155. Setup optical service
156. install covers
157. install tamper-resistant seals (see procedure 2 in Appendix A)

### 3.1.2 Intrusion attempt handling

1830 PSS supports login intrusion attempt handling. After the maximum number of consecutive invalid login attempts for a session has been reached, the system records in the security log the IP address of the source along with the UID and an intrusion transient condition is reported. The paratemeter is settable between 0 and 15 with a default of 3.

### 3.1.3 Encryption

Encryption must be provisioned through the KMT over SNMPv3 connection. The Crypto Officer is responsible for provisioning encryption.

Follow procedure in 8DG-61258-GAAA-TUZZA Alcatel-Lucent 1830 Photonic Service Switch (PSS) Release 7.0 Key Management Tool (KMT) Administration Guide

### 3.1.4 Displaying FIPS mode and state

The following commands will display FIPS mode and state; If the 1830 PSS-32 is in FIPS approved mode when executed from the local CIT port as user (admin) during installation.
The command and output will be as shown here:
# show general detail
Name : NE180
System Description : System Description : Alcatel-Lucent 1830 PSS v7.0 SONET ADM NE
Description :
Location :
Contact :
S/W Version : 1830PSS-32-2.5-15
Current Date : 1970/01/01 01:06:14 (UTC)
System Up Time : 1 hours, 6 minutes, 39.87 seconds
Loopback IP Address: 172.16.1.3/32
EC Programmed Capacity: unknown
# show admin ui

UI: fips

# config general fips-squelching

Fips Squelch Mode is Enable.

Displaying FIPS mode and state from PhM is done on the following PhM Status Screens shown here in figures 10 and 11. PhM SNMPv2c is indicative that the the 1830 PSS is running in FIPS communication mode.

Figure 10 PhM Screen for Displaying FIPS Communination Mode (SNMPv2c)

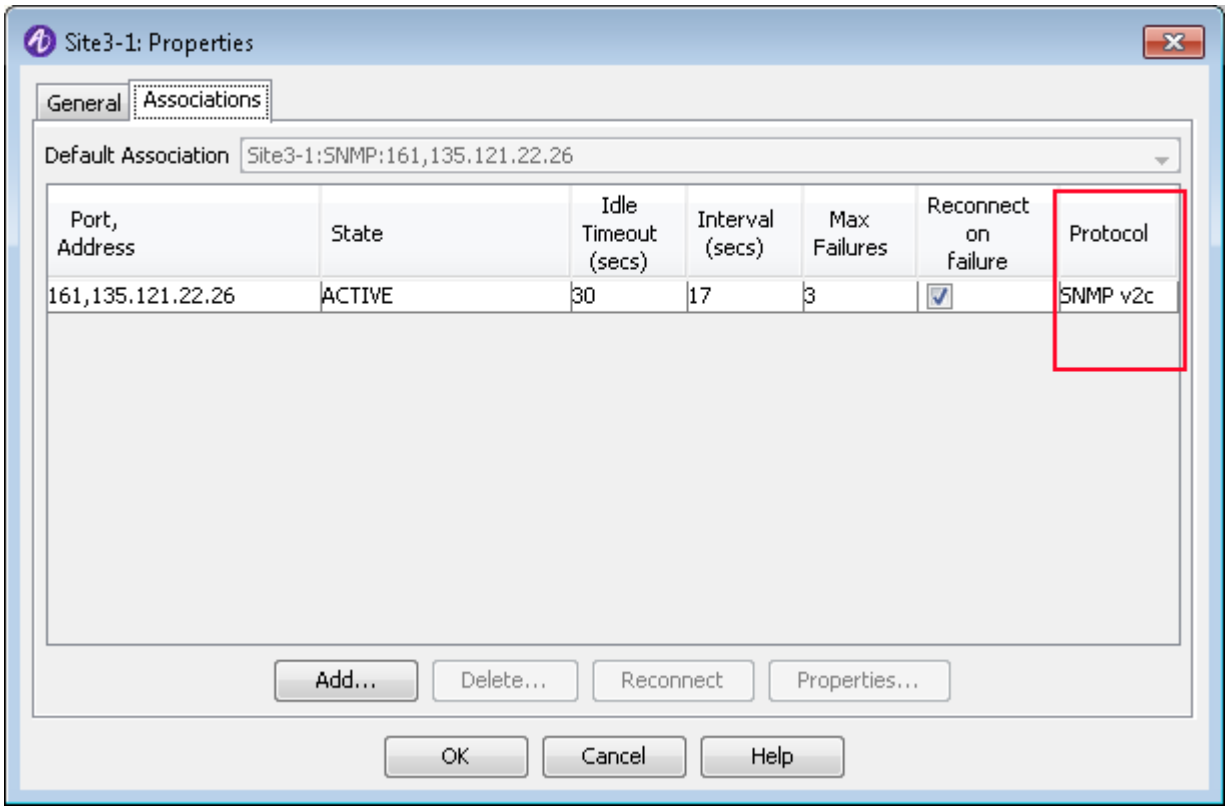
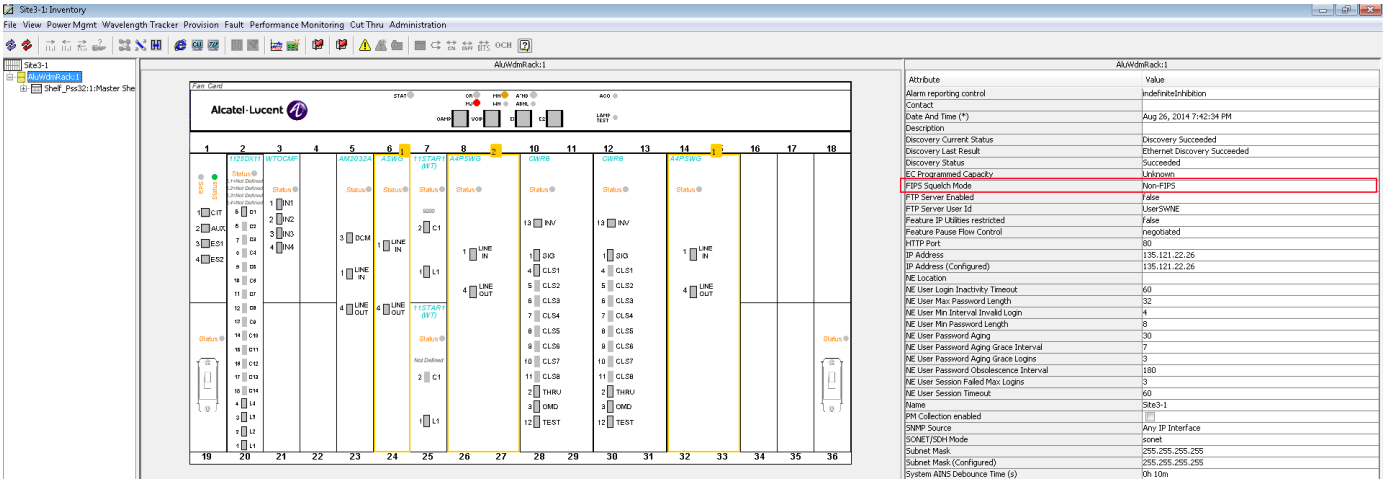



Figure 11 PhM Screen for Displaying FIPS Squelch Mode



### 3.1.5 Error States

Non-Recoverable Error State
An 1830 PSS-32/PSS-16/PSS-4 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-16/PSS-4 power-on and boot time self-tests

While an 1830 PSS-32/PSS-16/PSS-4 is in an Non-Recoverable Error state:
• All the 1830 PSS-32/PSS-16/PSS-4 transport slots all data output via the data output interfaces on the 1830 PSS-32/PSS-16/PSS-4 is inhibited
• A log is generated to notify the user about the reason which caused the node to transition to the error state.
Note: Do not attempt to do an upgrade if the 1830 PSS-32/PSS-16/PSS-4 is in the FIPS Error state. The 1830 PSS-32/PSS-16/PSS-4 cannot be considered as operating in a FIPS Approved mode of operation if an upgrade is performed while the 1830 PSS-32/PSS-16/PSS-4 is in the Error state.

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

 CR SA    13/05/28 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
```

## 3.2 Initialization of encryption keys

1830 PSS-32/PSS-16/PSS-4 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.
- Restarting the system or the 11QPEN4 when there are expired encryption keys. This action zeroizes all expired keys on the system or 11QPEN4.

Note: Disabling the administrative state of a port does not initialize the encryption key of the port.

## 3.3 Crypto Officer and User Guidance

### 3.3.1 Authentication modes

Local account authentication mode shall be provisioned for access to the 1830 PSS-32/PSS-16/PSS-4 when in FIPS mode. Administrator shall refrain from using RADIUS authentication.

### 3.3.2 Backups and restores

Backups and restores shall not to be performed in FIPS mode.

# 4. Abbreviations, Terminology and References

## 4.1 Abbreviations

| | |
|---|---|
| AES | Advanced Encryption Standard |
| AGD | Assurance Guidance Documents |
| ALC | Assurance Life Cycle |
| 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 |
| PhM | Photonic Manager |
| 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, May 2, 2012. http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf

# 5. APPENDIX A- Procedures consistent with Federal Information Processing Standards (FIPS) User Guide and Logbook 8DG-61258-GAAA-TSZZA Issue 1 October 2014

## Procedure 1: Install the PSS-4 FIPS Kit (bracket and air baffle)

### Purpose

The Alcatel-Lucent 1830 PSS-4 shelf requires a special bracket and air baffle to be FIPS compliant. The PSS-4 FIPS KIT (3KC-13452-AAAA) is listed in Table 1d, “Shelf Kit for FIPS-PSS-4, 3KC-13453-AAAA” (p. 6).

### Required equipment

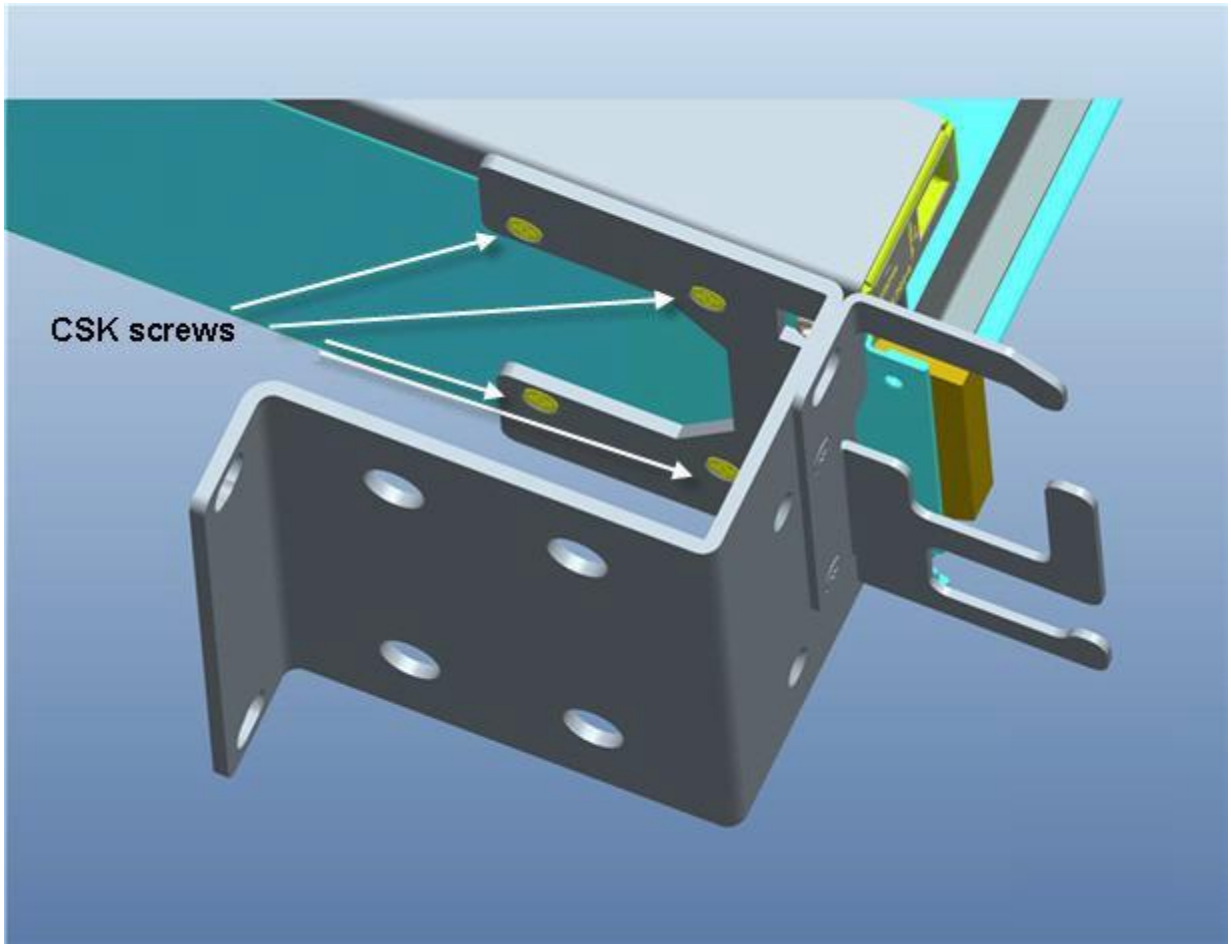
The following equipment is required to perform this procedure:

- PSS-4 FIPS KIT: 3KC-13452-AAAA. The kit includes:
  - PSS-4 FIPS bracket
  - PSS-4 FIPS air baffle
  - Six countersunk (CSK) M3x6 screws
  - Two PAN (Pan head) M2.5x6 screws
- ED 4 Shelf (Shelf, BP, Shelf ID, Dust Filter): 3KC-12960-AAAD

### Steps

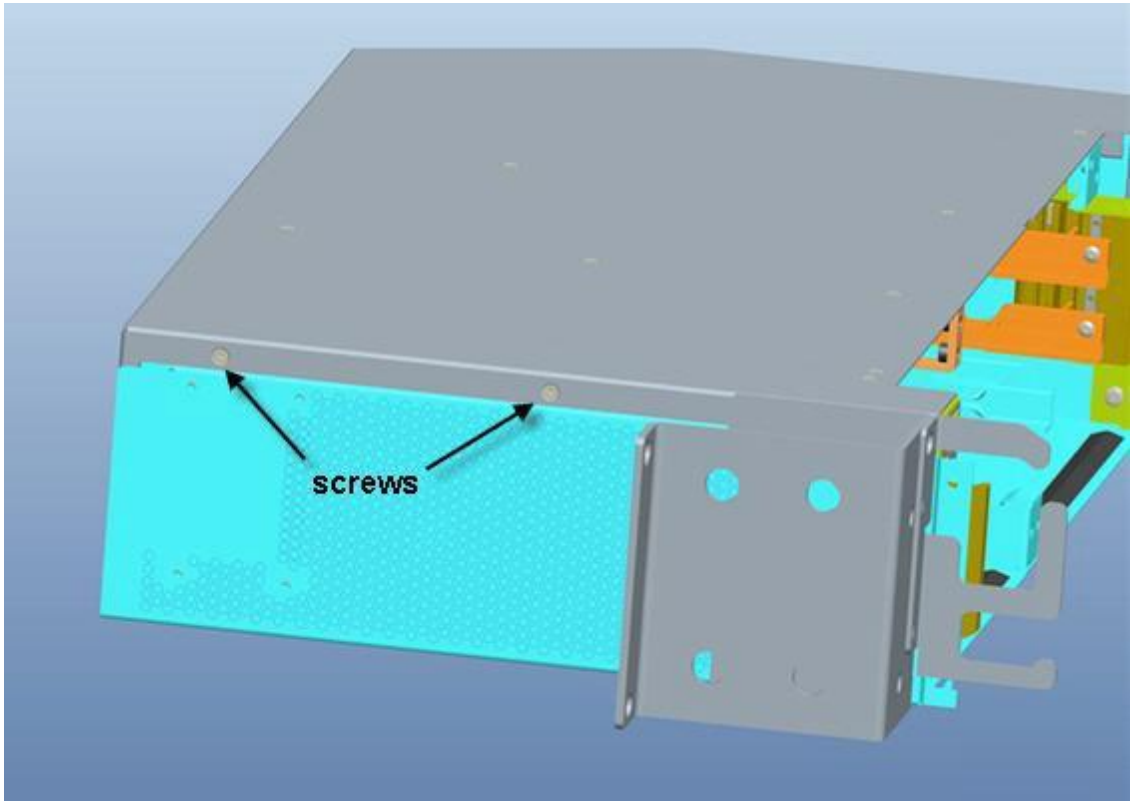
1 Attach the PSS-4 FIPS bracket to the Alcatel-Lucent 1830 PSS-4 shelf using four CSK screws.

Figure 11 PSS-4 FIPS bracket



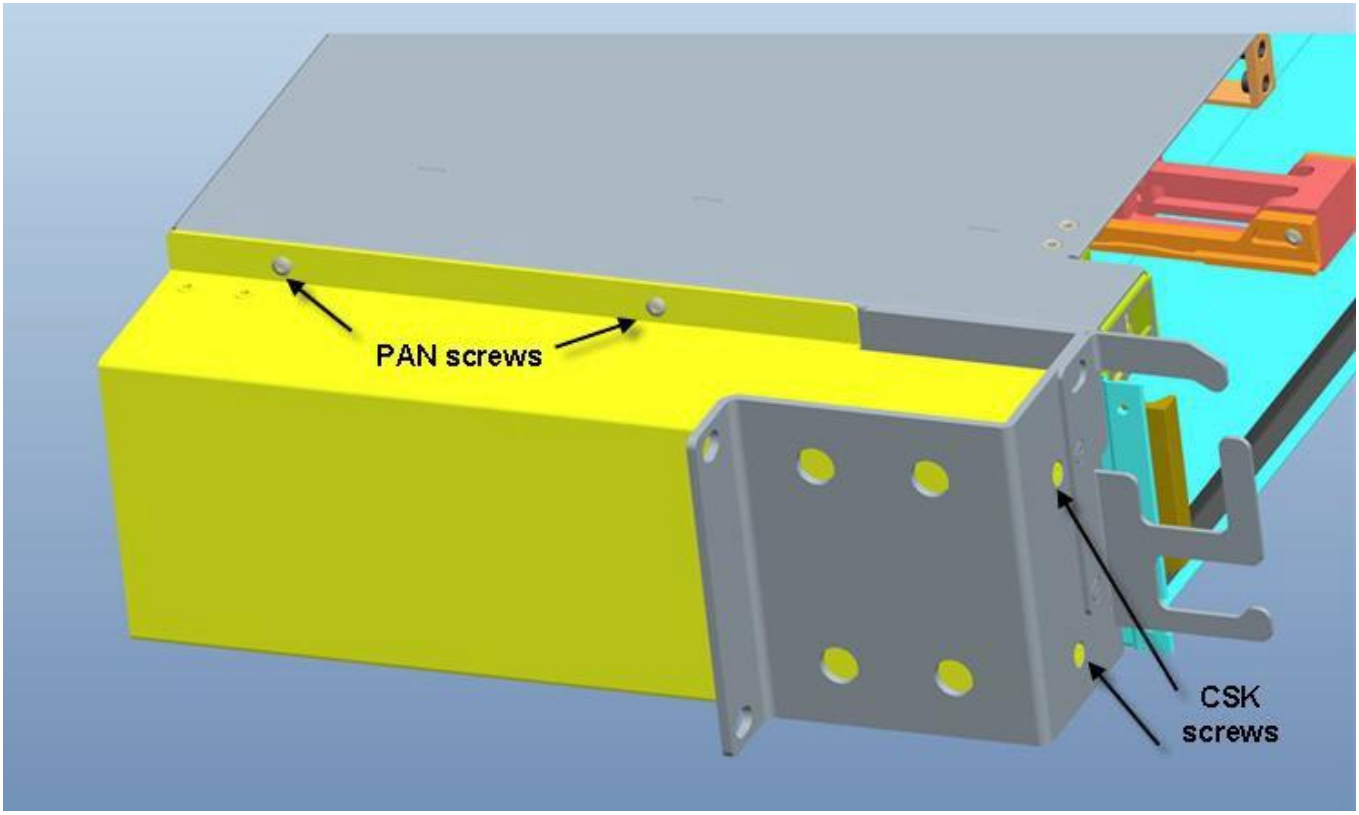

2 Remove the two screws on the Alcatel-Lucent 1830 PSS-4 shelf.

Figure 12 Alcatel-Lucent 1830 PSS-4 shelf screws




3 Install PSS-4 FIPS air baffle on the Alcatel-Lucent 1830 PSS-4 shelf using two CSK screws and two PAN screws.

Figure 13 PSS-4 FIPS air baffle




4 Refer to the *Alcatel-Lucent 1830 Photonic Service Switch 4 (PSS-4) Release 7.0 Installation and System Turn-Up Guide* and Procedure 3: "Provision the shelf for FIPS mode" (p. 55) to complete installation and FIPS mode provisioning.

END OF STEPS

# Procedure 2: Install the tamper-evident labels

### Purpose

Use this procedure to provision to install the tamper-evident labels on a Alcatel-Lucent 1830 PSS-4, Alcatel-Lucent 1830 PSS-16, and Alcatel-Lucent 1830 PSS-32. Seal the systems only after you are sure that no additional provisioning/debugging is required. The tamper seals are provided in the Security Label Kit (8DG-6509-AAAA), which is a component of Shelf FIPS Kit: (3KC-13453-AAAA)

### Steps

1. When applying tamper-evident labels, ensure that the surface temperature to be sealed is be a **minimum** of +10°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 l**abels shall be cured for 24 hours.

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

- Procedure 2.1: “Install the tamper-evident labels on Alcatel-Lucent 1830 PSS-4” (p. 67)
- Procedure 2.2: “Install the tamper-evident labels on Alcatel-Lucent 1830 PSS-16” (p. 71)
- Procedure 2.3: “Install the tamper-evident labels on Alcatel-Lucent 1830 PSS-32” (p. 76)

END OF STEPS

# Procedure 2.1: Install the tamper-evident labels on Alcatel-Lucent 1830 PSS-4

### Purpose

Use this procedure to provision to install the tamper-evident labels on a Alcatel-Lucent 1830 PSS-4. Seal the system only after you are sure that no additional provisioning/debugging is required.

### Steps

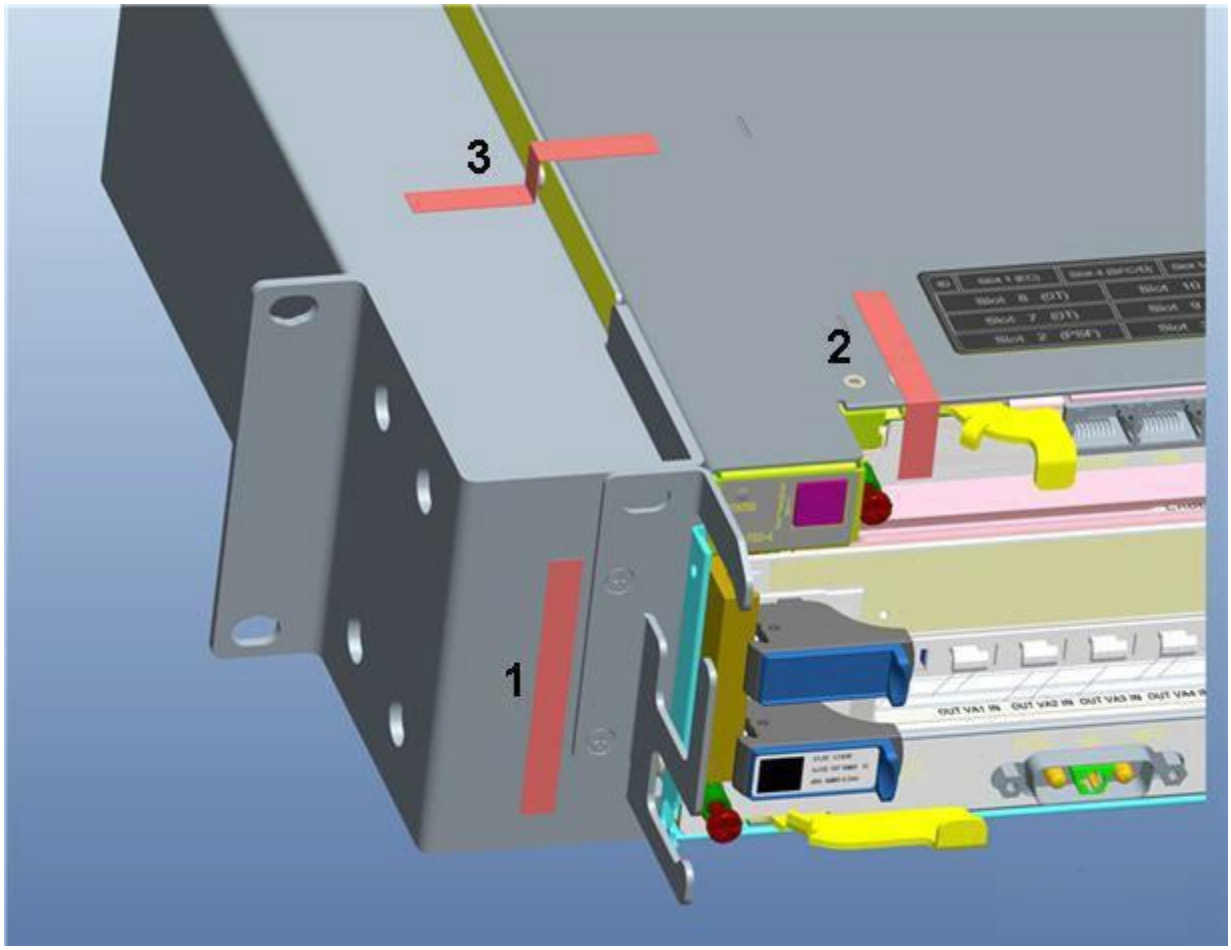
1 Install the 9 tamper-evident labels to seal the Alcatel-Lucent 1830 PSS-4 shelf.

**Table 28 Alcatel-Lucent 1830 PSS-4 shelf label locations**

| Location | Action | Reference |
|---|---|---|
| 1 | Place label 1 over the screws that affix the air baffle to the bracket. | Figure 11, "Left of Alcatel-Lucent 1830 PSS-4 shelf" (p. 68) |
| 2 | Place label 2 to seal EC pack. | |
| 3 | Place label 3 over the mounting screw that affixes the air baffle to the shelf. | |
| 4 | Place labels 4 and 5 to seal each of the two the power filters. | Figure 12, "Front of Alcatel-Lucent 1830 PSS-4 shelf" (p. 69) |
| 5 | | |
| 6 | Place label 6 to seal the fan tray and air filter. | |
| 7 | Place label 7 to seal the 11QPEN4 pack. | Figure 13, "11QPEN4 and blank pack in Alcatel-Lucent 1830 PSS-4 shelf" (p. 69) |
| 8 | Place label 8 to seal the blank pack. | |
| 9 | Place label 9 over the screw on the right side of the shelf. | Figure 14, "Right of Alcatel-Lucent 1830 PSS-4 shelf" (p. 70) |

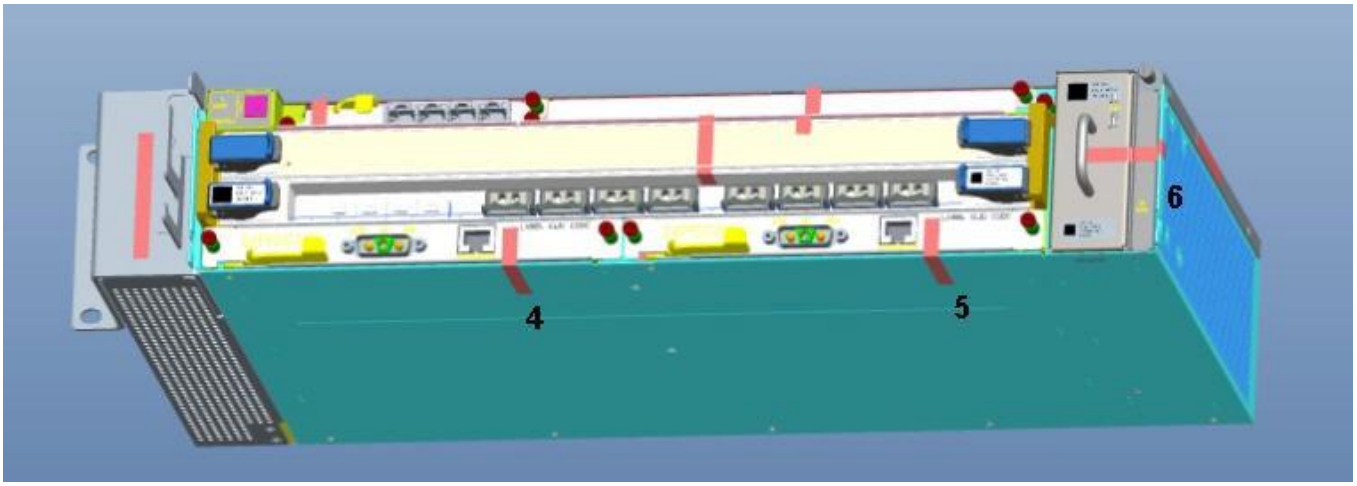
2 Place label 1 over the screws that affix the air baffle to the bracket. Place label 2 to seal EC pack. Place label 3 over the screw of the air baffle.

**Figure 11 Left of Alcatel-Lucent 1830 PSS-4 shelf**



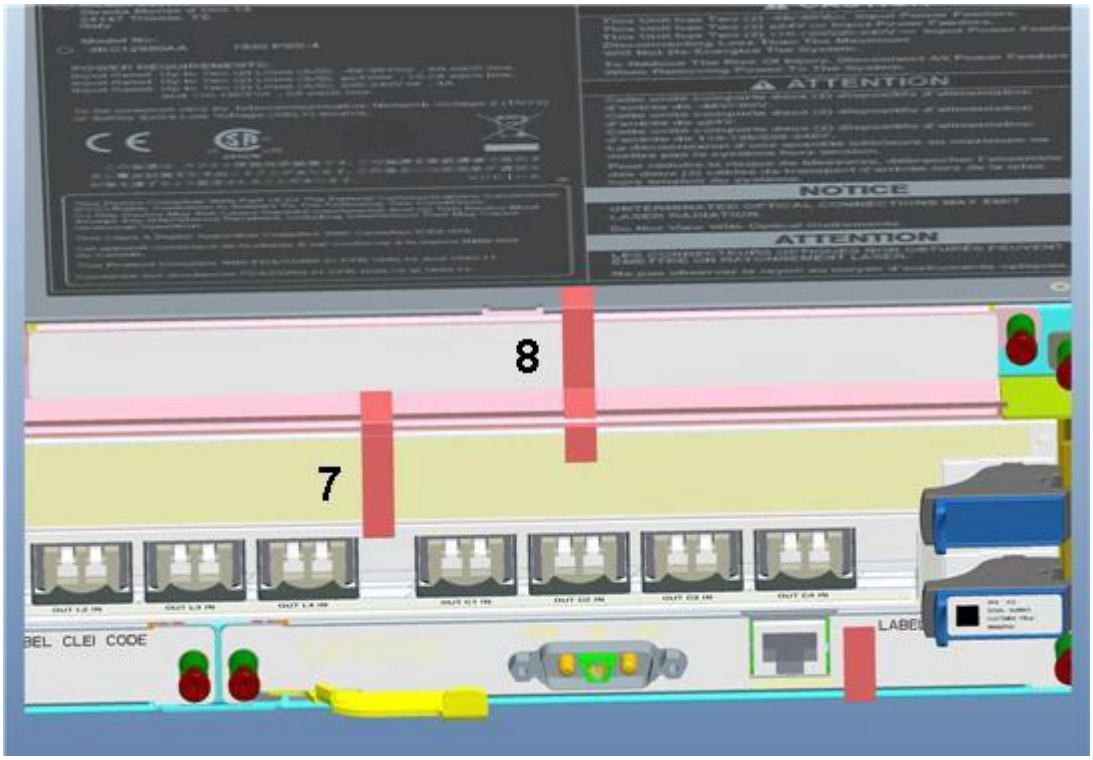

3 Place labels 4 and 5 to seal each of the two the power filters. Place label 6 to seal the fan tray and air filter.

**Figure 12 Front of Alcatel-Lucent 1830 PSS-4 shelf**



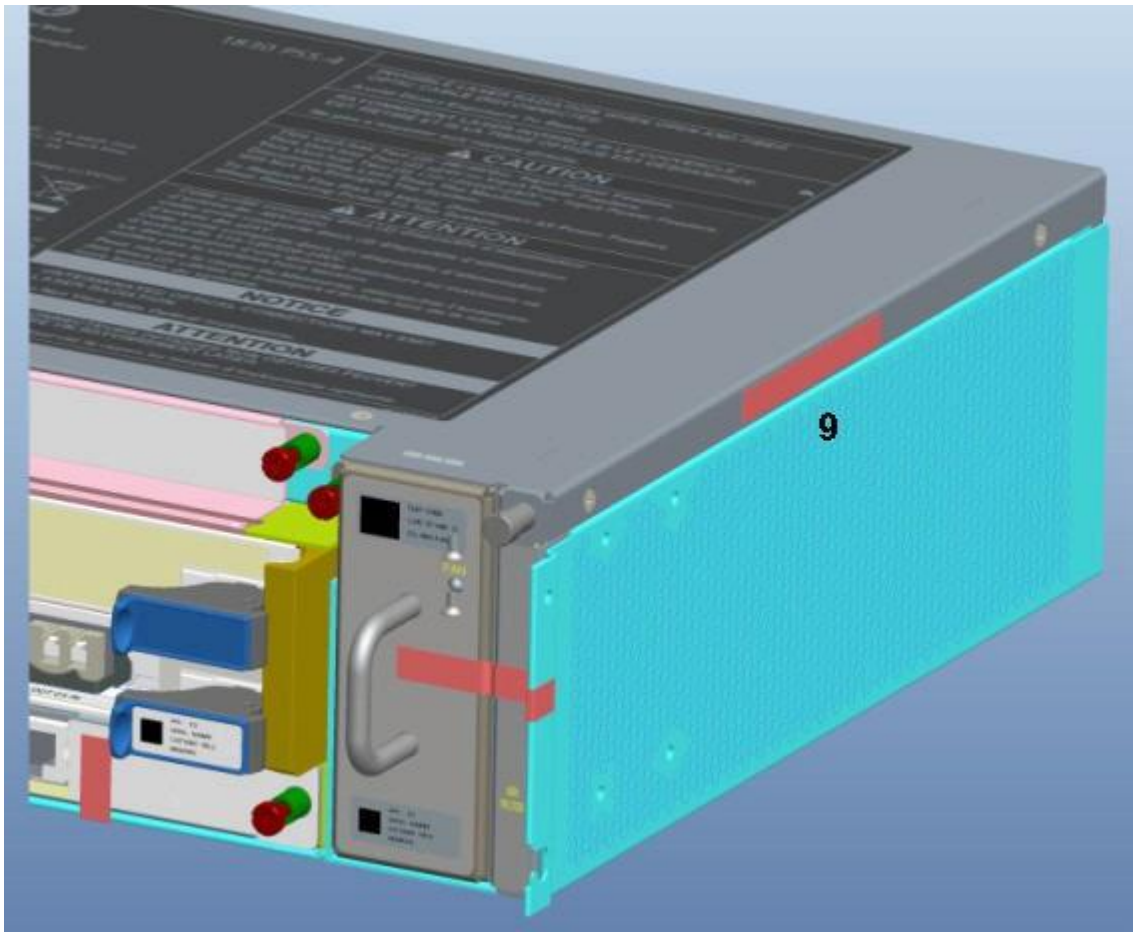

4 Place label 7 to seal the 11QPEN4 pack. Place label 8 to seal the blank pack.

Figure 13 11QPEN4 and blank pack in Alcatel-Lucent 1830 PSS-4 shelf




5 Place label 9 over the screw on the right side of the shelf.

**Figure 14 Right of Alcatel-Lucent 1830 PSS-4 shelf**




6 The crypotographic boundary of the Alcatel-Lucent 1830 PSS-4 shelf is now sealed

END OF STEPS

# Procedure 2.2: Install the tamper-evident labels on Alcatel-Lucent 1830 PSS-16

### Purpose

Use this procedure to provision to install the tamper-evident labels on a Alcatel-Lucent 1830 PSS-16. Seal the system only after you are sure that no additional provisioning/debugging is required.

### Steps

1 Install the 12 tamper-evident labels to seal the Alcatel-Lucent 1830 PSS-16 shelf.

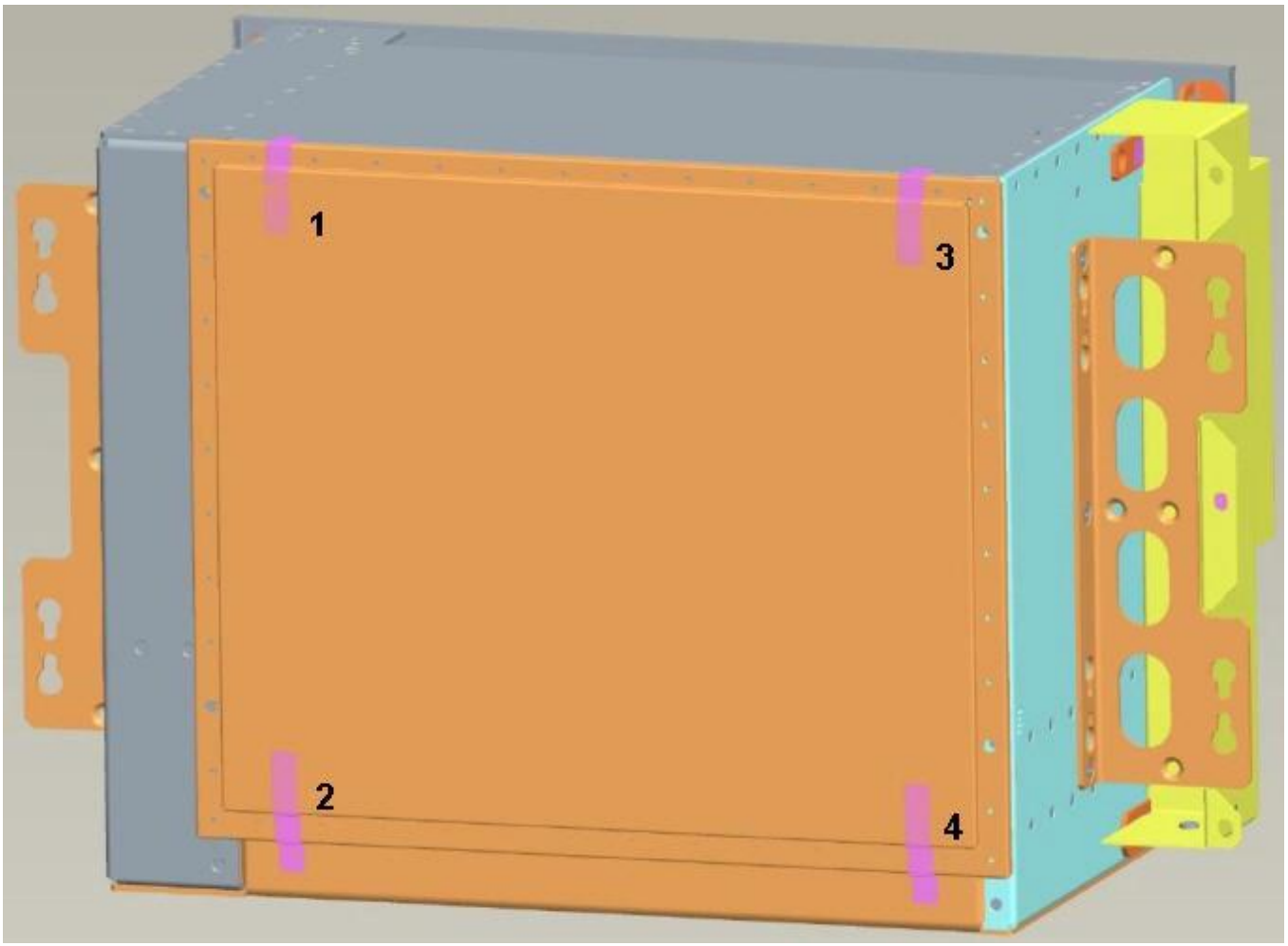
**Table 29 Alcatel-Lucent 1830 PSS-16 shelf label locations**

| Location | Action | Reference |
|---|---|---|
| 1 | Place labels 1–4 vertically over the 4 mounting screws that affix the rear cover to the shelf. | Figure 15, "Rear of Alcatel-Lucent 1830 PSS-16 shelf" (p. 72) |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | Place labels 5 and 6 over the 2 mounting screws that affix the shelf cover mounting brackets to the shelf. | Figure 16, "Right of Alcatel-Lucent 1830 PSS-16 shelf" (p. 73) |
| 6 | | |
| 7 | Place labels 7 and 8 over the 2 mounting screws that affix the air baffle to the shelf. | Figure 17, "Left of Alcatel-Lucent 1830 PSS-16 shelf" (p. 74) |
| 8 | | |
| 9 | Place labels 9 and 10 over the 2 mounting screws that affix the shelf cover mounting brackets to the shelf. | |
| 10 | | |
| 11 | Place labels 11 and 12 over the 2 | Figure 18, "Front of Alcatel-Lucent |

| | | |
|---|---|---|
| 12 | mounting screws that affix the front cover to the shelf. | 1830 PSS-16 shelf" (p. 75) |

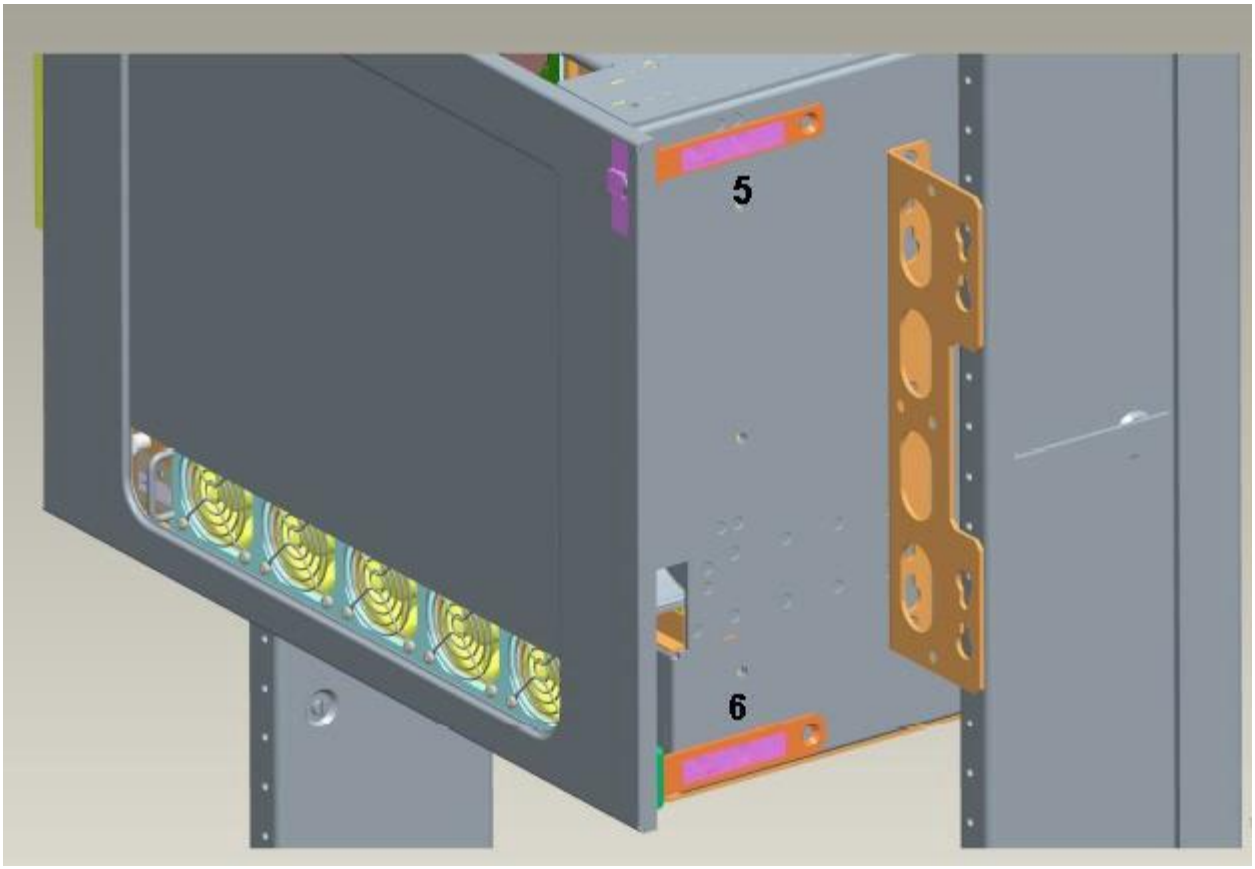
2 Place labels 1–4 vertically over the 4 mounting screws that affix the rear cover to the shelf.

**Figure 15 Rear of Alcatel-Lucent 1830 PSS-16 shelf**



3 Place labels 5 and 6 over the 2 mounting screws that affix the shelf cover mounting brackets to the shelf.

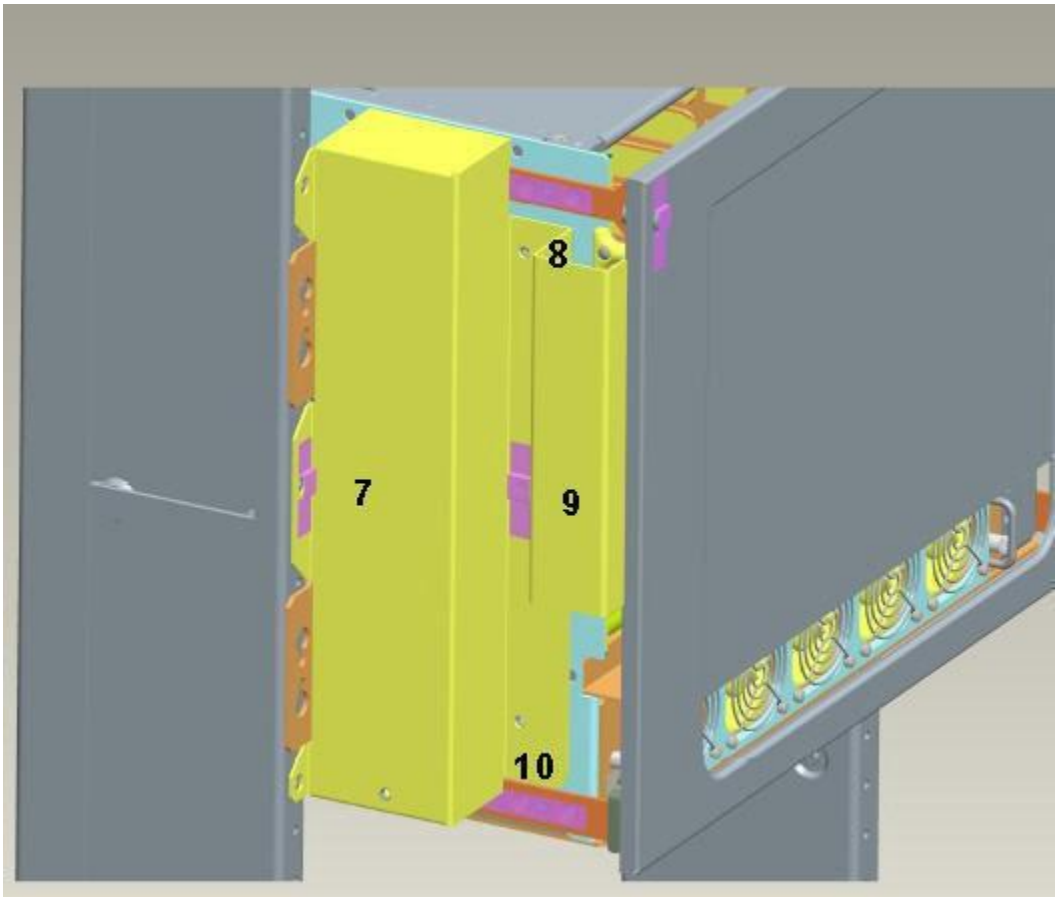
**Figure 16 Right of Alcatel-Lucent 1830 PSS-16 shelf**




4 Place labels 7 and 8 over the 2 mounting screws that affix the air baffle to the shelf.

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

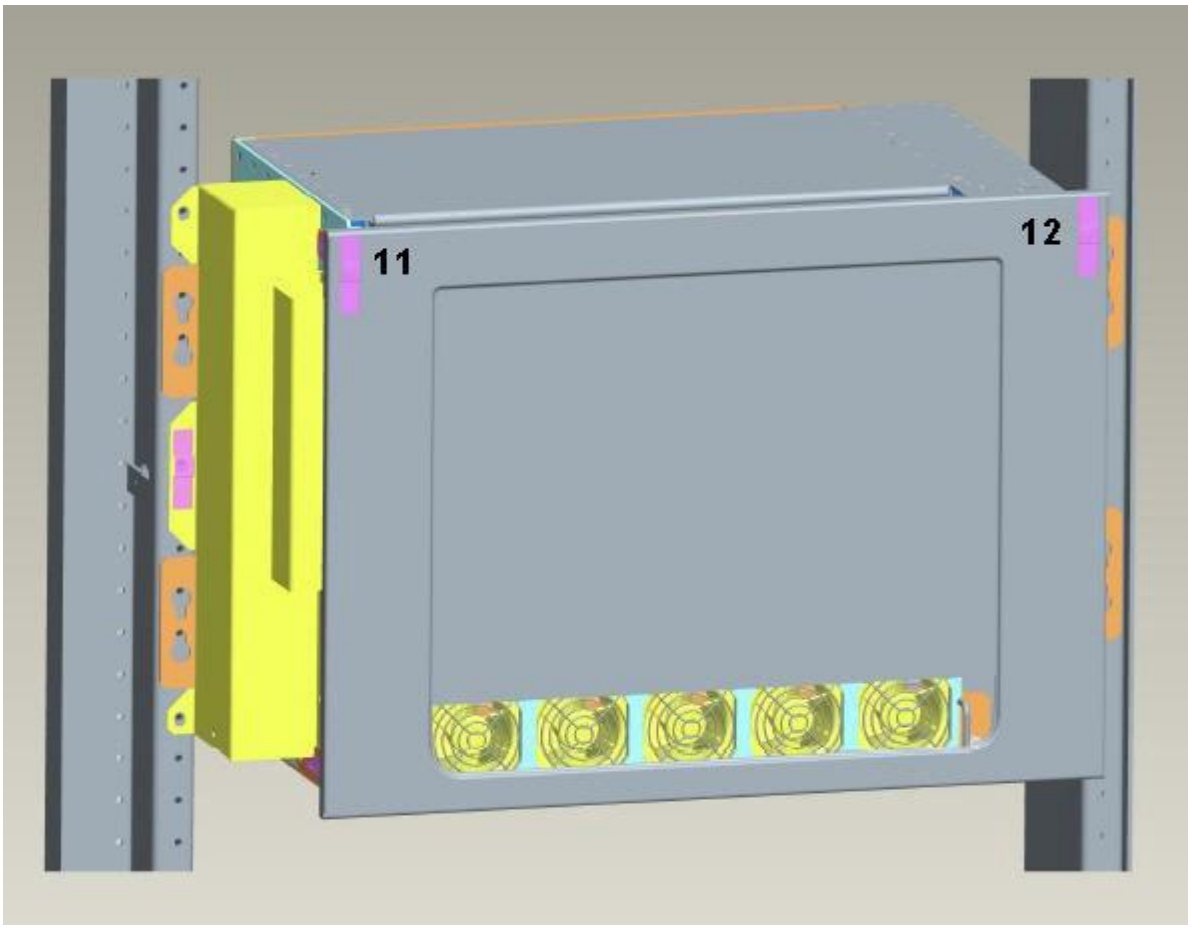
Figure 17 Left of Alcatel-Lucent 1830 PSS-16 shelf




**Note:** The yellow section is the exhaust baffle.

5 Place labels 11 and 12 over the 2 mounting screws that affix the front cover to the shelf.

Figure 18 Front of Alcatel-Lucent 1830 PSS-16 shelf




6 The crypotographic boundary of the Alcatel-Lucent 1830 PSS-16 shelf is now sealed

END OF STEPS

# Procedure 2.3: Install the tamper-evident labels on Alcatel-Lucent 1830 PSS-32

### Purpose

Use this procedure to provision to install the tamper-evident labels. Seal the system only after you are sure that no additional provisioning/debugging is required.

### Steps

1 Install the 11 tamper-evident labels to seal the Alcatel-Lucent 1830 PSS-32 shelf.

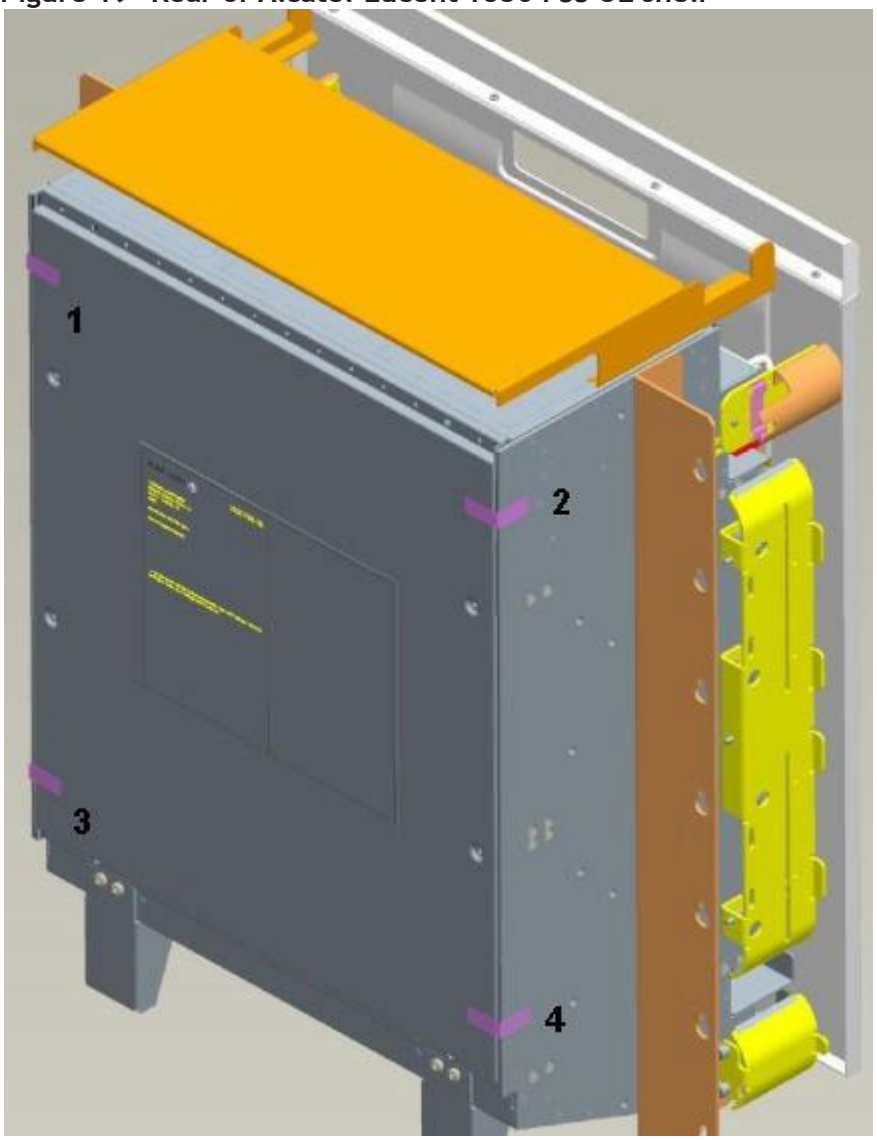
**Table 30 Alcatel-Lucent 1830 PSS-32 shelf label locations**

| Location | Action | Reference |
|---|---|---|
| 1 | Place labels 1–4 horizontally over the 4 mounting screws that affix the rear cover to the shelf. | Figure 19, "Rear of Alcatel-Lucent 1830 PSS-32 shelf" (p. 77) |
| 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 20, "Bottom of Alcatel-Lucent 1830 PSS-32 shelf" (p. 78)<br>Figure 21, "Close-up of location 5 and 6" (p. 79) |
| 6 | | |
| 7 | Place labels 7 and 8 over the 2 mounting screws that affix the top cover mounting brackets to the shelf. | Figure 22, "Left of Alcatel-Lucent 1830 PSS-32 shelf" (p. 80)<br>Figure 23, "Close-up of location 7" (p. 80) |
| 8 | | |
| 9 | Place labels 9 and 10 over the 2 mounting screws that affix the front cover to the shelf. | Figure 24, "Front of Alcatel-Lucent 1830 PSS-32 shelf" (p. 81) |
| 10 | | |

| | | |
|---|---|---|
| 11 | Place label 11 over one of the two screws that affix the top air exhaust to the shelf. | |

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

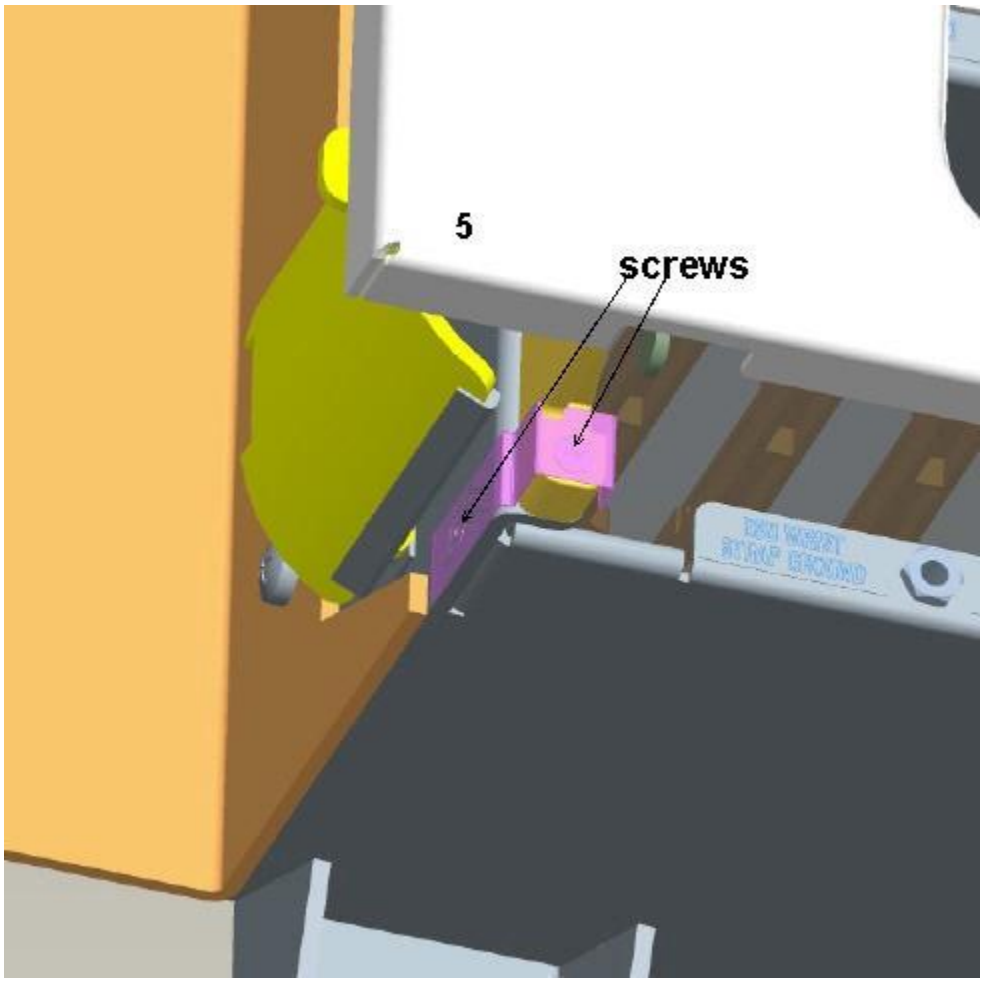
**Figure 19 Rear of Alcatel-Lucent 1830 PSS-32 shelf**



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 21, “Close-up of location 5 and 6” (p. 79) illustrates a close-up view of locations 5 and 6.

**Figure 21 Close-up of location 5 and 6**




4 Place labels 7 and 8 over the 2 mounting screws that affix the top cover mounting

brackets to the shelf. Figure 22, “Left of Alcatel-Lucent 1830 PSS-32 shelf” (p. 80) shows label 7 on the left side of the shelf. Label 8 should be placed on the right side of the shelf in the same position (not shown).

**Figure 22 Left of Alcatel-Lucent 1830 PSS-32 shelf**

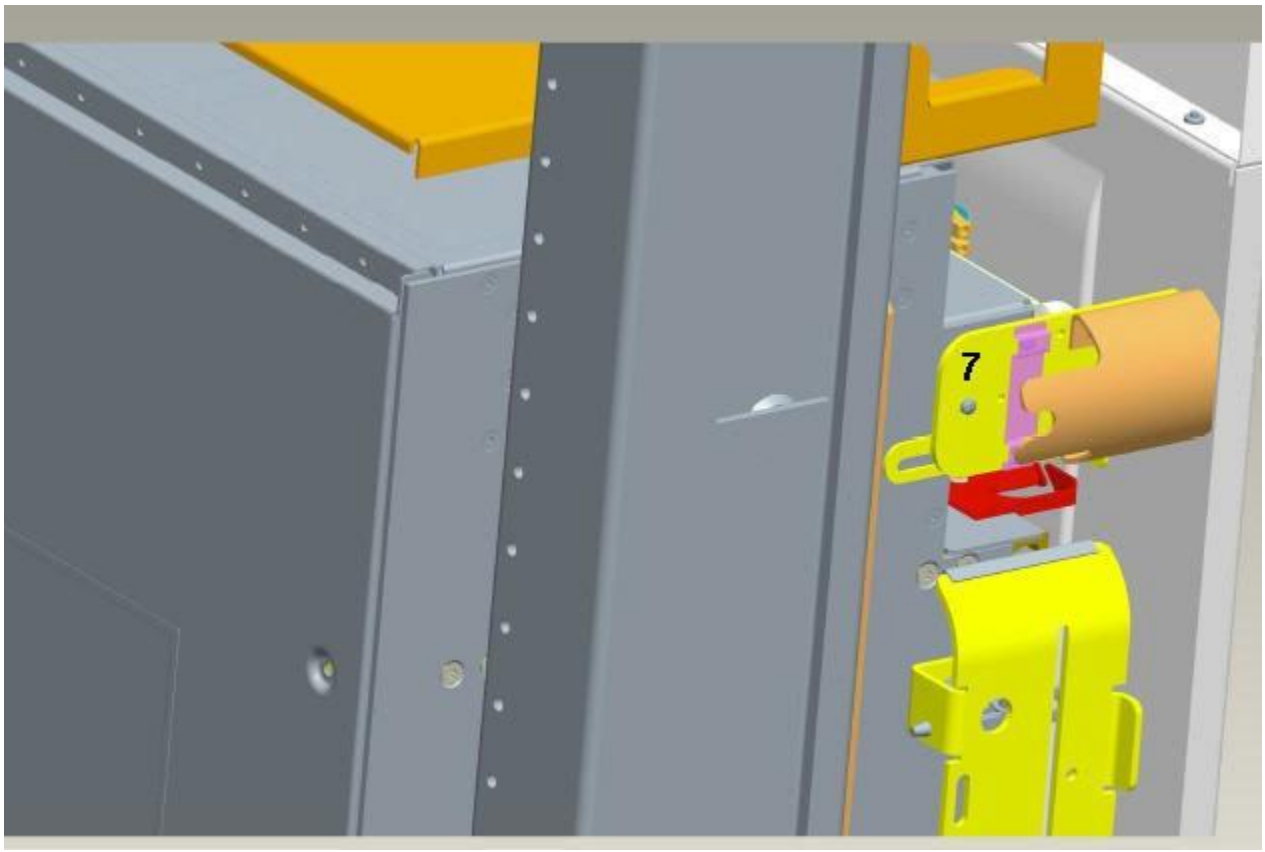
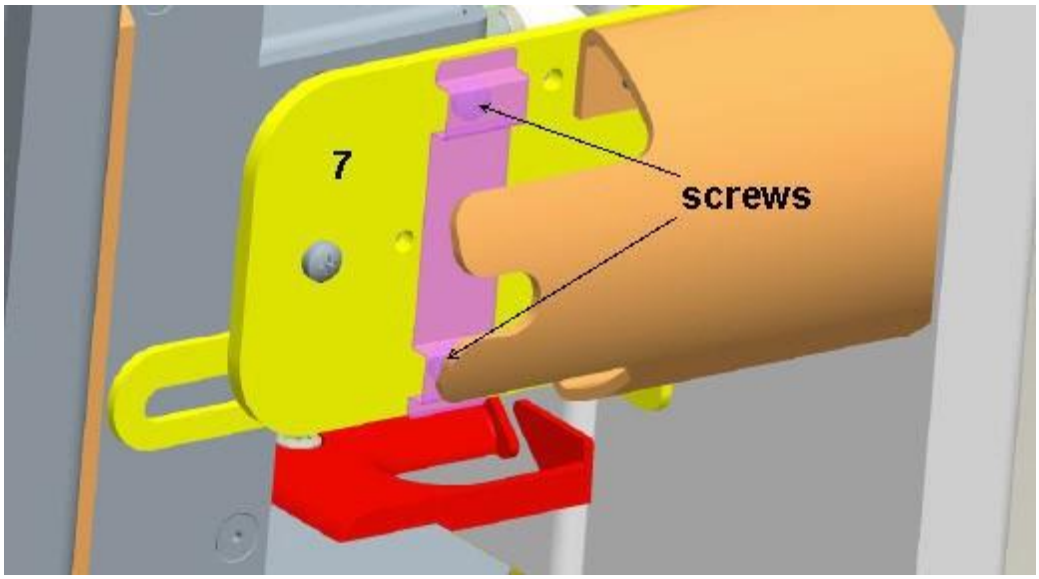


Figure 23 Close-up of location 7

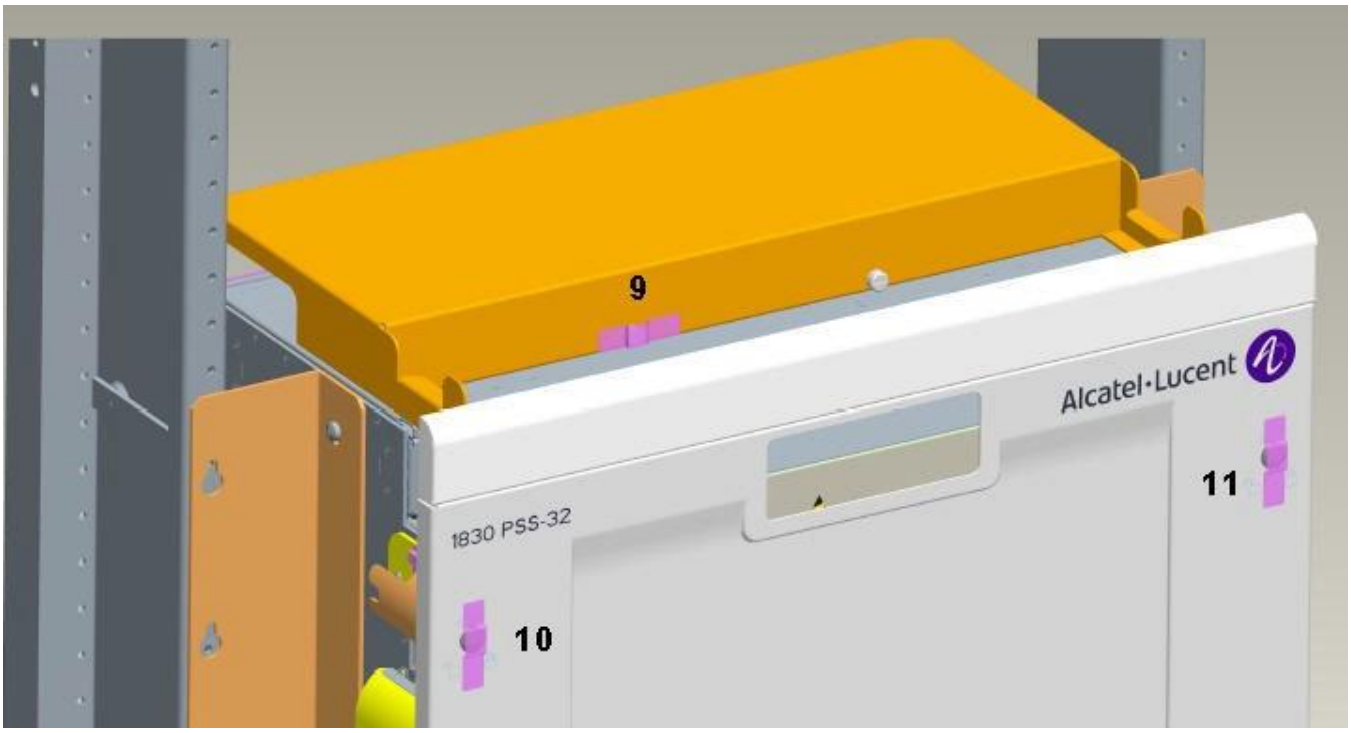



**Note:** Two of the three screws should be covered by the label.

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

Place label 11 over one of the two screws that affix the top air exhaust to the shelf.

Figure 24 Front of Alcatel-Lucent 1830 PSS-32 shelf




6 The crypotographic boundary of the Alcatel-Lucent 1830 PSS-32 shelf is now sealed.

END OF STEPS