Non-Proprietary FIPS 140-2 Security Policy

WCC-PCN-AES100GB-F Encryption Module with FSP 3000 Shelf

Firmware Version: 172.19.7 or 193.1.7

Document Version: 1.31
Date: June 2, 2021

ADVA Optical Networking SE
Fraunhoferstr. 9a
82152 Martinsried/Muenchen
Germany

Phone +49(0)89-890665-0
Fax +49(0)89-890665-699
http://www.adva.com/

CONTENTS

FIGURES

TABLES

1 Introduction

This document defines the security policy for the WCC-PCN-AES100GB-F Encryption Module with FSP 3000 Shelf. The module is a transponder for core telecommunication networks, and transports plaintext 100GbE or OTU4 client side data services to and from the encrypted network interface. The module performs key agreement and synchronization with a peer module at the far-end of an optical network to support AES encryption of the network link. The peer module is "the other party" in the terminology of [56Ar3].

The module is a configuration of the ADVA Fiber Service Platform (FSP) 3000 scalable optical data transport system. The encryption module is composed of a WCC-PCN-AES100GB-F card assembly installed in a customer-chosen ADVA FSP 3000 shelf, with one of the listed network interface transceivers in the card assembly's CFP receptacle. ADVA FSP 3000 shelves are available in various form factors to host customer-chosen combinations of modular functionality and density.

Table 1 "Cryptographic Module Configurations" shows module name, hardware part number, and hardware and firmware version numbers. Rows 8 through 15 list the CFP form factor pluggable network transceivers.

Table 1 Cryptographic Module Configurations

	Module	Description	HW P/N and version	FW version
1	WCC-PCN-AES100GB-F + F7/SH9HU	Card assembly in 9U shelf	Card: 1063700027-01 version C-1.02 Shelf: 1078700121 version 2.01	Card: 172.19.7 or 193.1.7 Shelf: N/A
2	WCC-PCN-AES100GB-F + F7/SH1HU-R/PF	Card assembly in 1U shelf with rear power access and pluggable fan unit	Card: 1063700027-01 version C-1.02 Shelf: 1078700060-01 version 1.01	Card: 172.19.7 or 193.1.7 Shelf: N/A
3	WCC-PCN-AES100GB-F + F7/SH1HU-HP/2DC	Card assembly in 1U shelf with DC input power	Card: 1063700027-01 version C-1.02 Shelf: 1078700144 version 2.11	Card: 172.19.7 or 193.1.7 Shelf: N/A
4	WCC-PCN-AES100GB-F + F7/SH1HU-HP/E-TEMP/2DC	Card assembly in 1U shelf with DC input and extended low temperature operation	Card: 1063700027-01 version C-1.02 Shelf: 1078700145-01 version 1.01	Card: 172.19.7 or 193.1.7 Shelf: N/A
5	-	General Purpose Tamper-Evident Seal	1013700030-01	N/A
6	-	CFP Tamper-Evident Seal	1013700031-01	N/A
7	-	Tamper-Evident Wire Seal	1013700032-01	N/A
8	CFP pluggable transceiver	CFP/112G/#DCTCG/SM/LC	1061700617-01	N/A
9	CFP pluggable transceiver	CFP/112G/#DCTCF/SM/LC	1061700618-01	N/A

	Module	Description	HW P/N and version	FW version
10	CFP pluggable transceiver	CFP/112G/#DCTCF/SM/LC	1061700618-02	N/A
11	CFP pluggable transceiver	CFP/112G/#DCTC/SM/LC	1061700619-01	N/A
12	CFP pluggable transceiver	CFP/112G/#DCTC/SM/LC	1061700619-02	N/A
13	CFP pluggable transceiver	CFP/112G/#DCTCR/SM/LC	1061700630-01	N/A
14	CFP pluggable transceiver	CFP/112G/#DCTCL/SM/LC	1061700634-01	N/A
15	CFP pluggable transceiver	CFP/112G/LR4/SM/LC	1061700655-02	N/A

The module is intended for use by US Federal agencies and other markets that require FIPS 140-2 validated encryption for network communications.

1.1 Security Level

See Table 2 for the FIPS 140-2 security levels for the module.

Table 2 Achieved Security Level by Requirement

Security Requirement	Security Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A
Overall	2

1.2 Module Description and Cryptographic Boundary

The cryptographic boundary is the metal case of the WCC-PCN-AES100GB-F card in conjunction with the enclosing ADVA shelf. The physical form of the module is shown in these figures:

- Figure 1 Cryptographic Boundary, WCC-PCN-AES100GB-F + F7/SH9HU
- Figure 2 Cryptographic Boundary, WCC-PCN-AES100GB-F + F7/SH1HU-R/PF
- Figure 3 Cryptographic Boundary, WCC-PCN-AES100GB-F + F7/SH1HU-HP/2DC
- Figure 4 Cryptographic Boundary, WCC-PCN-AES100GB-F + F7/SH1HU-HP/E-TEMP/2DC

The embodiment is a multi-chip embedded cryptographic module.

The module is shielded, with openings for cooling air flow. All sensitive components are enclosed by covers that are affixed with screws under tamper-evident seals.

In deployment, shelf slots are occupied by various card types or covered with blank panels to ensure proper cooling air flow. These other card types and blank panels are outside the cryptographic boundary, and include:

- Backplane connectors: Mates with the connectors J2 and J3 on the WCC-PCN-AES100GB-F Encryption Module
- Shelf fan assemblies
- Power-related components, such as pluggable power supply units

Figure 1 Cryptographic Boundary, WCC-PCN-AES100GB-F + F7/SH9HU

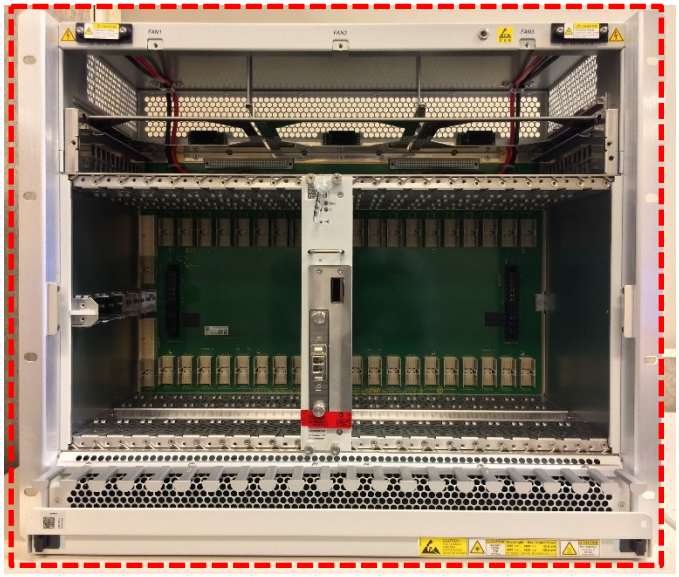


Figure 2 Cryptographic Boundary, WCC-PCN-AES100GB-F + F7/SH1HU-R/PF

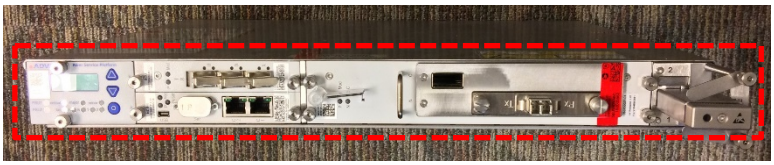


Figure 3 Cryptographic Boundary, WCC-PCN-AES100GB-F + F7/SH1HU-HP/2DC

Figure 4 Cryptographic Boundary, WCC-PCN-AES100GB-F + F7/SH1HU-HP/E-TEMP/2DC

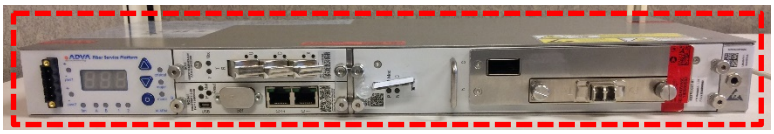


Figure 5 Top View, WCC-PCN-AES100GB-F Card

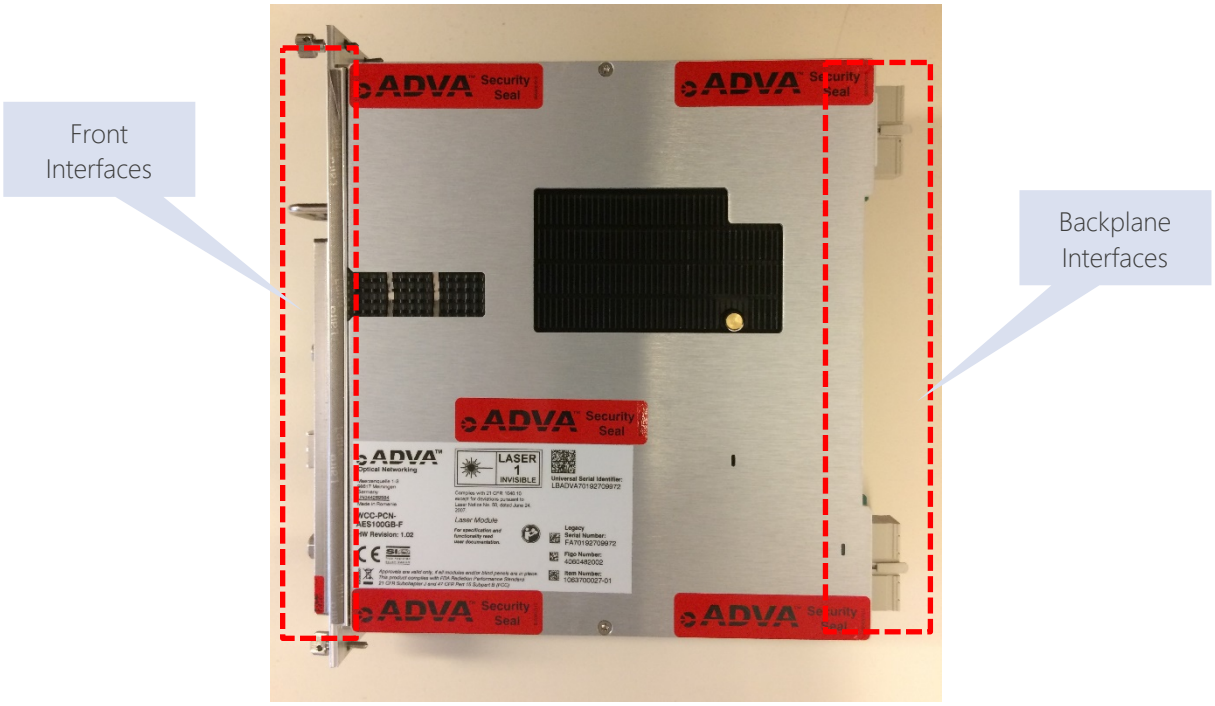


Figure 6 Bottom View, WCC-PCN-AES100GB-F Card

Figure 7 Front and Back View, WCC-PCN-AES100GB-F Card

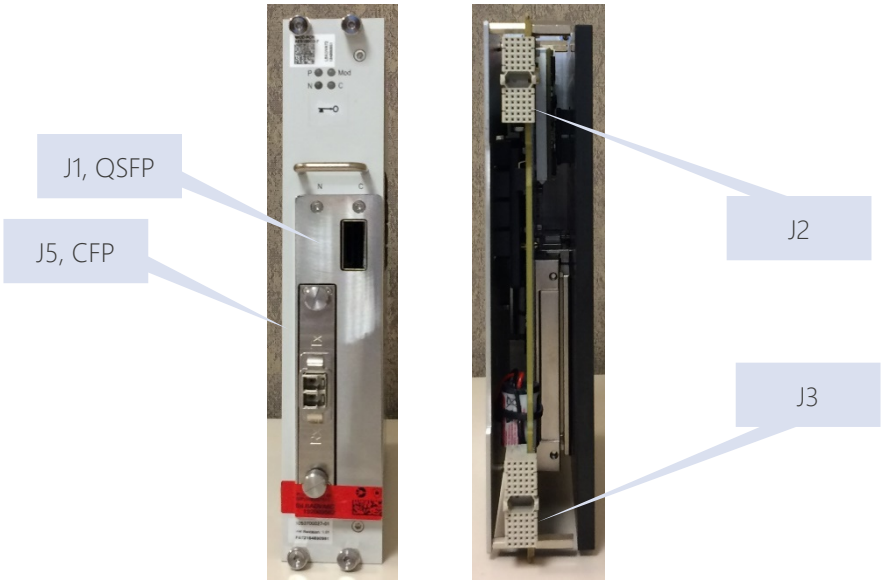


Figure 8 Left View, WCC-PCN-AES100GB-F Card

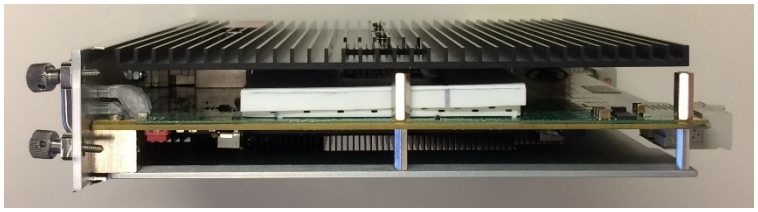
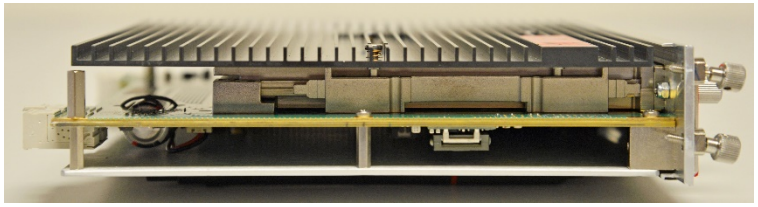


Figure 9 Right View, WCC-PCN-AES100GB-F Card



1.3 Module Ports and Interfaces

The module's ports and associated FIPS defined logical interface categories are listed in Table 3, and illustrated in Figure 10. The shelf backplane is outside the cryptographic boundary, and distributes electrical signals to and from the WCC-PCN-AES100GB-F card backplane connectors. Connector reference designators in the table correspond to labels on the WCC-PCN-AES100GB-F card. Signal directions are from the perspective of the WCC-PCN-AES100GB-F card. The optical network interface pins for received signals carry control inputs and encrypted data inputs. The optical network interface pins for transmitted signals carry status outputs and encrypted data outputs. The control and status information at the optical network interface is used for key agreement and synchronization with the far-end peer.

Table 3 Ports and Interfaces

Port	Description	Logical Interface Type
J2 and J3 power pins	Backplane connector, power and ground pins	Power
J3 control input pins	Backplane connector, interface to shelf control unit	Control in
J3 status output pins		Status out
J3 control/status bidirectional pins	Backplane connector, Ethernet to shelf control unit	Control in, status out
J1 pins for power	Front panel QSFP receptacle for client optical interface	Power
J1 pins for interrupt, presence		Control in
J1 pins for I2C		Control in, status out
J1 pins for reset, low power mode		Status out
J1 pins for receive signals		Data in
J1 pins for transmit signals		Data out
J5 pins for power	Front panel CFP receptacle for network optical interface	Power
J5 pins for control and status		Control in, status out
J5 pins for receive signals		Data in, control in
J5 pins for transmit signals		Data out, control out
LEDs	Front panel LED indicators	Status out

Figure 10 Ports and Interfaces

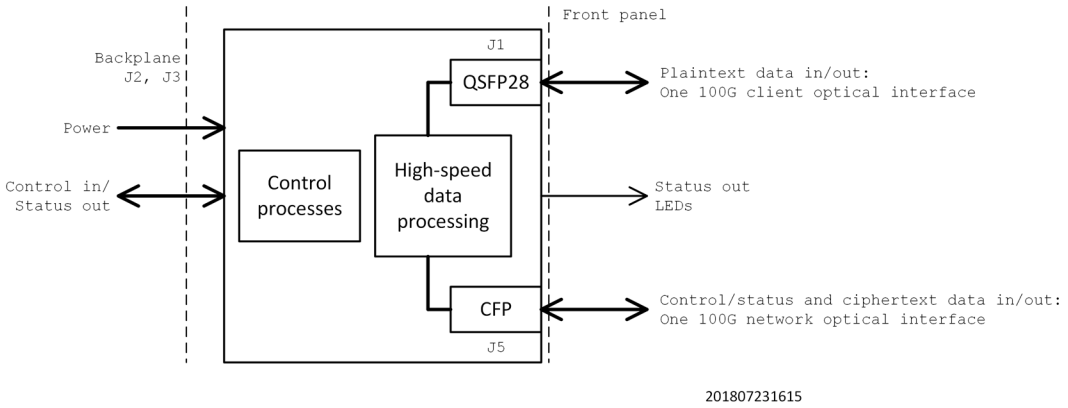
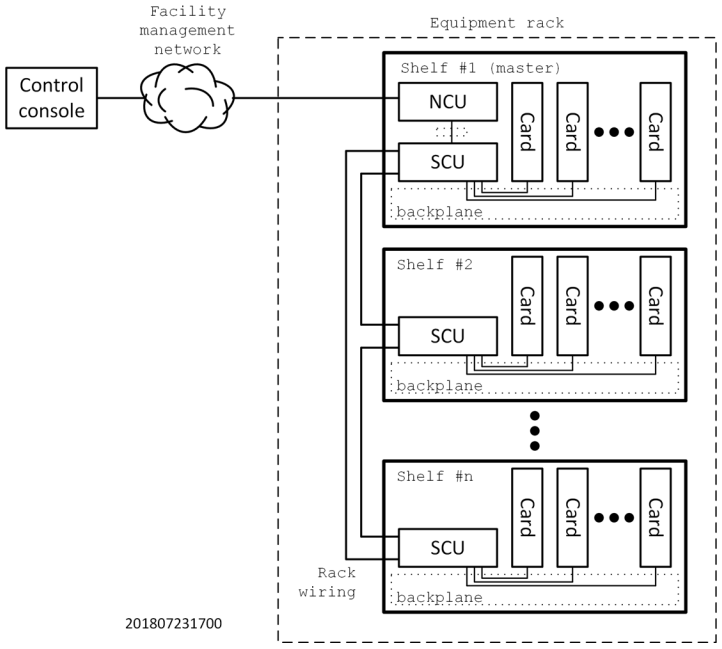


Figure 11 illustrates control of cards deployed in a shelf, and multiple shelves in an equipment rack. Each card's backplane control and status signals cross the cryptographic boundary to connect to a Shelf Control Unit (SCU) that is

outside the cryptographic module. Local rack wiring connects SCUs. One shelf includes a Network element Control Unit (NCU) that communicates with that shelf's SCU, and through the SCU to other shelves. The NCU is outside of the cryptographic boundary. The NCU and connected SCUs route messages through the facility's management network to a control console. The control console provides the user interface. The connection between the control console and the NCU is outside the cryptographic module and should be secured by the operator with SSH for text-based user interfaces, and HTTPS for browser user interfaces.

Figure 11 Card Connectivity to Control Console



1.4 Mode of Operation

The module operates in only a "FIPS Approved" mode. Only cryptographic functions that are FIPS-approved are applied. The module does not implement a bypass mode or a maintenance mode.

To verify that the module is in the approved mode of operation, use the "get version" feature of the "Respond to status requests" service to display the version of firmware components. Confirm that the displayed versions match those shown in Table 1 "Cryptographic Module Configurations". The tamper-evident seals shall be installed for the module to operate in the approved mode of operation.

2 Cryptographic Functionality

2.1 Algorithms and Protocols

The module implements the FIPS Approved cryptographic functions listed in Table 4 "Approved Algorithms". The module implements the Non-Approved but Allowed cryptographic functions listed in Table 5.

Table 4 Approved Algorithms

Cert. #	Algorithm	Mode	Description	Functions/caveats
C1459	AES [197]	CTR [38A]	Key size: 256	Encrypt, decrypt in FPGA
C1459		ECB [38A]	Key size: 256	Encrypt in FPGA
A1098, A1099		ECB [38A]	Key size: 128	Encrypt, decrypt in firmware
A1098, A1099		ECB [38A]	Key size: 256	Encrypt in firmware, decrypt tested but not used.
VA	CKG [IG D.12]	[133r2] Section 5.2 Asymmetric key establishment key generation using unmodified DRBG output		Key generation
		[133r2] Section 6.1 Direct symmetric key generation using unmodified DRBG output		
		[133r2] Section 6.2.1 Derivation of symmetric keys from a key agreement shared secret		
A1098, A1099	DRBG [90A]	CTR	Use_df, AES-256	Deterministic random bit generator
A1098, A1099	DSA [186]		L = 2048, N = 256	KeyGen. Tested, but not used.
A1098, A1099	safe-prime [56Ar3]		MODP-2048, MODP-3072, MODP-4096	KeyGen, KeyVer. MODP-2048 and MODP-3072 tested but not used
A1098, A1099	HMAC [198]	SHA-256	Key size: 160	Message authentication, KDF primitive
A1098, A1099	KAS [56Ar3]	FFC (party U, party V), KPG, Full	FC (p len = 2048, q len = 256), SHA-512, HMAC-SHA-256, Concat	Key agreement scheme provides 112 bits of encryption strength. Tested but not used.
A1098, A1099	KAS [56Ar3]	FFC (party U, party V), KPG, Full	p len = 4096, q len = 4096 SHA-512, HMAC-SHA-256, Concat	Key agreement scheme with safe primes provides 128 bits of encryption strength.
A1098, A1099	RSA [186]	PSS	n = 2048 SHA-256	Signature verification. Tested but not used.
			n = 3072 SHA-256 n = 4096 SHA-256	Signature verification
A1098, A1099	SHS [180]	SHA-256 SHA-512		Signature verification, message digest generation, password obfuscation.

Table 5 Non-Approved but Allowed Cryptographic Functions

Algorithm	Mode	Description	Functions/caveats
NDRNG	Non-Deterministic Random Number Generator		Seeds the DRBG for 256-bit security strength.

Table 6 Security-Relevant Protocols Used in FIPS Mode

Protocol	Description
None	

2.2 Critical Security Parameters

All CSPs used by the module are described in this section. All usage of these CSPs by the module (including all CSP lifecycle states) is described in Section 3.4 "Services". The isolation of CSPs from data outputs is illustrated in Figure 12.

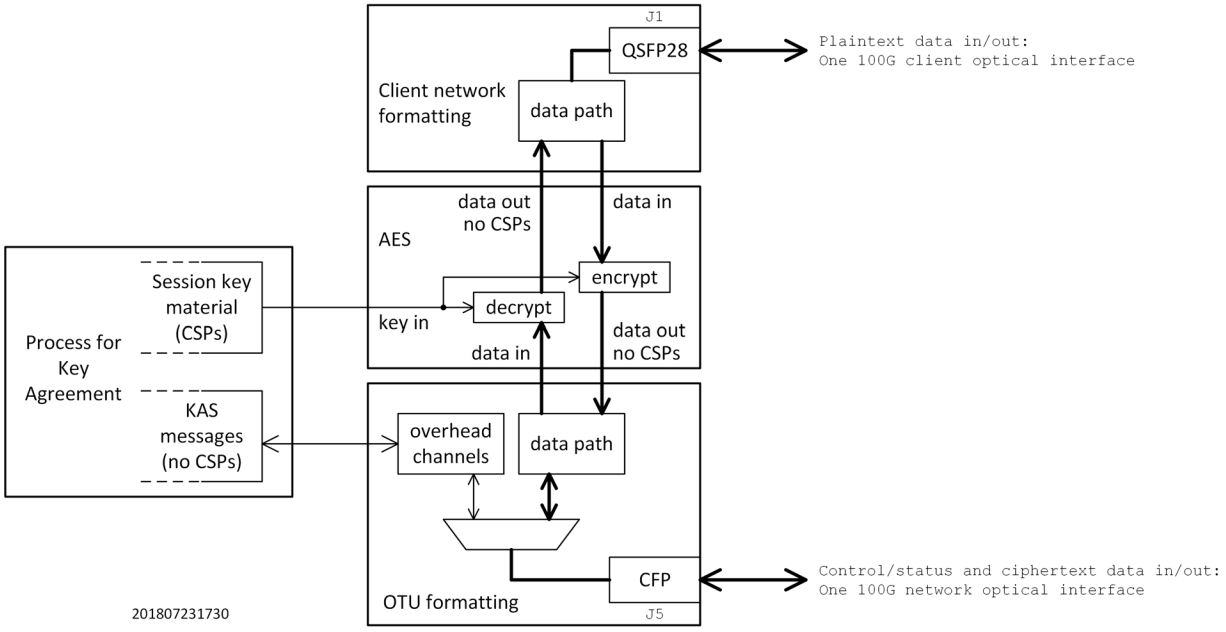
Table 7 Critical Security Parameters (CSPs)

CSP	Description/Usage
CO password	Used to check requests for service that require the crypto officer role (only a 256-bit hash is stored)
Static DH private key	Local static private key for the key agreement scheme [56Ar3] C(2e, 2s) (4096 bits)
Ephemeral DH private key	Local ephemeral private key for the key agreement scheme [56Ar3] C(2e, 2s) (4096 bits)
Session key material, current	Encryption key (256 bits)
	IV field of AES-256-CTR counter block (55 bits)
Session key material, next	Encryption key (256 bits)
	IV field of AES-256-CTR counter block (55 bits)
MacKey	Key-confirmation MAC key for HMAC-SHA-256 (160 bits) derived with session key material
Seed bits	Seed bits for firmware DRBG (384 bits per reseed) generated by internal entropy source
DRBG state	Internal state of CTR DRBG: V (128 bits) and Key (256 bits)
Storage extension key	128-bit key for access to nonvolatile secure storage in internal module and encryption of material stored in that module

Table 8 Public Keys

Public Key	Description/Usage
Static DH public key	Local static public key for the key agreement scheme [56Ar3] C (2e, 2s)
Ephemeral DH public key	Local ephemeral public key for the key agreement scheme [56Ar3] C (2e, 2s)
Other party static DH public key	Other party static public key for the key agreement scheme [56Ar3] C (2e, 2s) The value is stored upon confirmation by the crypto officer to trust the other party's public key
Other party ephemeral DH public key	Other party ephemeral public key for the key agreement scheme [56Ar3] C (2e, 2s)
Firmware authentication keys	List of 1 to 64 RSA public keys with modulus length of 3072 or 4096 bits to verify digital signature over incoming firmware image

Figure 12 CSP Isolation from Outputs



3 Roles, Authentication and Services

3.1 Assumption of Roles

The module supports three (3) distinct operator roles: authenticated User, authenticated Cryptographic Officer (CO), and unauthenticated role. The authenticated User connects via the optical interface's in-band overhead channels. The

Cryptographic Officer and unauthenticated role connect via the backplane. For backplane control messages, the cryptographic module enforces the separation of roles using password authentication of each CO command.

Table 9 lists all operator roles supported by the module. The module does not support a maintenance role or bypass capability.

The module supports concurrent operators. Some commands that are honored only from the Cryptographic Officer role or from the unauthenticated role can execute without interrupting certain processes that are executed in the User role. See Section 3.5 "Concurrent Operations".

Each CO command is individually authenticated, and previous authentications are cleared at the conclusion of the command's operations.

Authentication data in the form of the CO password is protected from unauthorized disclosure, modification and substitution by physical access limitations to backplane signals within the system shelf. See Section 5.2 "Physical Inspection" for guidance on inspecting the shelf system that hosts the module. See Section 8 "Security Rules and Guidance" for recommendations on privacy measures for network links and user interface terminals that connect remotely to the system shelf.

The User authentication data is the static DH public key of the other party. The User authentication data is stored securely in the module to protect from unauthorized modification or substitution.

Table 9 Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
CO	Cryptographic Officer: Approve trust of other party public key, set policy values, enable User key agreement operations, commit firmware update, validate digital signature on new firmware image.	Role based	Password
User	User: Perform recurring key agreement operations to generate session keys for data encryption	Role based	Static DH public key
Unauthenticated	Unauthenticated: Request status indications, copy a firmware update image to standby memory, manage all non-cryptographic telecommunications functions, establish telecommunications operational states (e.g. "in service" or "disabled").	None	None

3.2 Authentication Methods

3.2.1 Cryptographic Officer Authentication

Authentication data accompanies each CO command.

The module enforces minimum password length of 10 characters and allows the characters to be chosen from the set of 95 ASCII printable characters. At least one character must be lower case, at least one must be upper case, and at least one must be a numeral. This allows at least 10 ^ 17 possible passwords. The probability that a random attempt will produce a successful guess of a randomly chosen password is less than one in 10^17, which is far less than one in 1,000,000.

After the module receives three consecutive CO commands with bad authentication data, the module enforces a 10-minute lock out during which incoming CO commands are discarded without examination. In a one-minute period, no more than three (3) attempts to guess an unknown password can occur. The probability that random attempts during a one-minute period will successfully authenticate is less than three in 10^17, which is far less than 1 in 100,000.

See Section 8 "Security Rules and Guidance" for recommendations on password selection.

3.2.2 User Authentication

The key agreement protocol conducted with the other party operates as a User process. Key agreement is authenticated with a static Diffie-Hellman key of the other party. The Cryptographic Officer provisions the module to trust the other party static DH public key.

The other party static DH public key is in a domain that has prime modulus length 4096 bits and order length 4095 bits. The other party static DH public key is used for key agreement in a C (2e, 2s) scheme that complies with [56Ar3]. This provides security strength of greater than 128 bits per Table 2 in [57p1r4].

The key agreement protocol runs automatically after the CO provisions trust of the other party and clears any policies or conditions that suspend automatic key agreement. The module limits the rate at which it will run a complete key agreement protocol exchange to one per minute. Since the key agreement scheme provides security strength greater than 128 bits, the probability that any single random attempt will succeed, or that attempts in a one-minute period will succeed, is much less than one in 1,000,000.

Successful key agreement is automatically followed by user data path encryption. The user data path is disconnected if the other party is not trusted and if there is no unexpired session key material. When the user data path is disconnected, user plaintext data streams are replaced with standard dummy patterns.

3.3 Authentication Description

Table 10 Authentication Description

Authentication Method	Probability	Justification
CO password	less than one in 1,000,000	Minimum length 10 characters from 95-symbol alphabet, requiring at least one lower case character, at least one upper case character, and one numeral, gives at least 10 ^ 17 possible passwords, which is greater than 1,000,000.
User static DH key	less than 1 / (2^128)	4096-bit Diffie-Hellman keys are in a domain with prime modulus of length 4096 bits and order of length 4095 bits. In the nomenclature of [57p1r4], this is L = 4096 and N = 4095. Section 5.6.1 and Table 2 of [57p1r4] indicate that L >= 3072 with N >= 256 provides security strength 128.
Digital signature on update code image	less than 1 / (2^112)	Updates to the firmware code image are authenticated by the module using the signature scheme RSASSA-PSS with SHA-256 and modulus lengths of at least 2048 bits. The initial values of trusted firmware authentication public keys are preloaded in manufacturing. Additions and deletions to the values of trusted firmware authentication public keys are delivered in update firmware code images. The signature scheme provides security strength 112 per Section 5.6.1, Table 2, and Table 3 of [57p1r4].

3.4 Services

All services implemented by the module are listed in Table 11 "Authenticated Services" and Table 12 "Unauthenticated Services". No CSP is output from the module by any service.

Table 11 Authenticated Services

Authenticated Service	Role	Description	Affected CSPs and Public Keys
Initialize	CO	Establish CO password and apply built-in default session key lifetime and event thresholds.	CO password Seed bits DRBG state Storage extension key
Reset	CO	Reset to factory state and zeroize all CSPs including CO password.	All CSPs and public keys except Fw auth key

Authenticated Service	Role	Description	Affected CSPs and Public Keys
Cold boot	CO	Reboot.	CO password Static DH public key Ephemeral DH private key Ephemeral DH public key Session key material MacKey Seed bits DRBG state Other party Eph DH pub key
Update firmware	CO	Control firmware update and mark which image is active.	CO password Static DH public key Ephemeral DH private key Ephemeral DH public key Session key material MacKey Seed bits DRBG state Other party Eph DH pub key Fw auth key
Run self-tests	CO	Perform power-on self-tests upon command.	CO password
Start pairing	CO	Remove trust of other party public key, delete old local static DH key pair, generate new local static DH key pair, and exchange static public info with other party.	CO password Seed bits DRBG state Static DH private key Static DH public key
Complete pairing	CO	Accept trust of other party static DH public key, and on success automatically begin the services "Key agreement" and "Encrypt network link".	CO password Static DH private key Static DH public key Other party static DH pub key Storage extension key
Set parameters	CO	Set session key lifetime, persistence of selected status indications, and thresholds for event counters that drive status indicators.	CO password
Clear event counters	CO	Clear counters of key agreement protocol errors, data path integrity check errors.	CO password

Authenticated Service	Role	Description	Affected CSPs and Public Keys
Change password	CO	Change CO password.	CO password
Key agreement	User	Perform key agreement with other party to periodically generate fresh session keys for data encryption.	Static DH private key Static DH public key MacKey Seed bits DRBG state Ephemeral DH private key Ephemeral DH public key Session key material Storage extension key Other party static DH pub key Other party eph DH pub key
Encrypt network link	User	Encrypt / decrypt bidirectional traffic at the network interface. In the absence of valid session key material, forward dummy replacement signals instead of encrypted and decrypted data.	Session key material
Validate new firmware	CO	Use a trusted public key embedded in the currently active image to validate the digital signature over a candidate new firmware image.	FW auth key

Table 12 Unauthenticated Services

Unauthenticated Service	Description	Affected CSPs
Reset upon uninstall	Reset to factory state and zeroize all CSPs including CO password upon removal of card from backplane.	All
Run power-on self-tests	Perform self-tests at power-up.	None
Respond to status requests	Provide status and alarm indications in response to request commands.	None
Indicate events and alarms	Send notifications and alarm indications at status outputs.	None
Copy firmware	Copy candidate firmware image to inactive memory area.	None

Table 13 "Security Parameters Access Rights within Services" defines the relationship between access to security parameters and the different module services. The modes of access shown in the table are defined as:

- G = Generate: The module generates the CSP.
- R = Read: The module reads the CSP for output.
- E = Execute: The module executes using the CSP.
- W = Write: The module writes the CSP to persistent storage.
- Z = Zeroize: The module zeroizes the CSP.

Table 13 Security Parameters Access Rights within Services

Service	CSPs and Public Keys													
	CO pw	Static DH private key	Static DH public key	Eph DH private key	Eph DH public key	Session key, current	Session key, next	MacKey	Seed bits	DRBG state	Storage extension key	Other party static DH public key	Other party Eph DH public key	Fw auth key
Initialize	W								G	G	GW			
Reset	EZ	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	
Cold boot	E		Z	Z	Z	Z	Z	Z	Z	Z			Z	
Update firmware	E		Z	Z	Z	Z	Z	Z	Z	Z			Z	W
Run self-tests	E													
Start pairing	E	GWE	GWE						GEZ	GE	E			
Complete pairing	E	E	R								E	WE		
Set parameters	E													
Clear event counters	E													
Change password	EW													
Reset upon uninstall	Z	Z	Z	Z	Z	Z	Z	Z			Z	Z	Z	
Run power-on self-tests														
Respond to status requests			R									R		R
Indicate events and alarms														
Key agreement		E	GR	GEZ	GR	G	G	GEZ	GEZ	GE	E	EZ	EZ	
Encrypt network link						E	E							

Service	CSPs and Public Keys													
	CO pw	Static DH private key	Static DH public key	Eph DH private key	Eph DH public key	Session key, current	Session key, next	MacKey	Seed bits	DRBG state	Storage extension key	Other party static DH public key	Other party Eph DH public key	Fw auth key
Copy firmware														
Validate new firmware														E

The services to indicate events and alarms do not interact with CSPs. The service to respond to status requests does not interact with CSPs.

3.5 Concurrent Operations

These services do not allow any other service to run concurrently:

- Reset upon uninstall
- Run power-on self-tests
- Initialize
- Reset
- Cold boot
- Update firmware
- Run self-tests

The service "Encrypt network link" can operate concurrently with these in-operation services:

- Start pairing (if prior pairing and operations produced valid session key)
- Complete pairing (if prior pairing and operations produced valid session key)
- Key agreement
- Set parameters
- Clear event counters
- Change password
- Respond to status requests
- Indicate events and alarms
- Copy firmware
- Validate new firmware

4 Self-Tests

The module performs self-tests to ensure the proper operation of the module. Per FIPS 140-2 these are categorized as either power-on self-tests or conditional tests.

4.1 Power-on Self-Tests

Power-on self-tests are available on demand by power cycling the module, or by an authenticated command from the Cryptographic Officer. The module inhibits all data outputs while in the power-on self-test state.

The module performs the following algorithm known-answer tests (KATs) during power-on self-tests:

- RSASSA-PSS with SHA-256 signature verification with 3072-bit modulus
- Modular exponentiation for DH key agreement with 2048-bit operands
- CTR_DRBG SP 800-90A health tests for Instantiate, Reseed, and Generate functions
- SHA-256
- SHA-512
- AES-128 ECB encrypt and decrypt (firmware implementation)
- AES-256 ECB encrypt and decrypt (firmware implementation, decryption not used in subsequent operations)
- HMAC-SHA-256
- AES-256 ECB encrypt (FPGA implementation)

The module performs a firmware integrity test with SHA-256 over code in non-volatile memory.

All of the above tests must be completed successfully prior to any other use of cryptography or CSPs by the module. If any test fails, the module enters the power-on self-test error state and disables data output and cryptographic functions with CSPs. The front panel LEDs illuminate red to indicate error status. The power-on self-test error state can be cleared by a successful re-execution of the power-on self-tests.

Successful completion of power-on self-tests is indicated by yellow and green front panel LED illumination, as detailed in user documentation.

Status messages for power-on self-test success and failure are sent from the module over the backplane interface to the shelf control unit, which makes information available for display on local and remote user interfaces.

4.2 Conditional Tests

Conditional tests are performed when the related service operates.

The module performs the following conditional self-tests as indicated:

- Firmware load test via digital signature verification on candidate firmware update image (RSASSA-PSS with SHA-256 and modulus lengths of 2048, 3072, or 4096 bits)
- Seed source repetition count test on each output block (IG 9.8)
- Static and ephemeral DH private and public key pairwise consistency test on each key generation

4.3 Response to Conditional Test Failures

A failure of the firmware load test results in continued operation with the current firmware image and refusal to execute the failed candidate image.

The module enters a time-limited-encryption state in which further key agreement attempts are suspended upon failure of these conditional tests:

- seed sources, DRBG functions, or properties of internally generated DH keys
- repeated failures in shared secret verification

While in a time-limited-encryption state that suspends further key agreement, the module continues to supply network link encryption and decryption services with the current valid session key material until expiration of that material. In the absence of valid key material, the module replaces user data with dummy replacement data at the data output interfaces.

A front panel LED illuminates yellow to indicate suspended key agreement status, as detailed in user documentation. The suspended key agreement state can be cleared by an authenticated command from the Cryptographic Officer, or by successful execution of power-on self-tests.

Successful completion of conditional tests is indicated by green front panel LED illumination, as detailed in user documentation.

Status messages for conditional test failures, for key agreement success, and for firmware update status are sent from the module over the backplane interface to the shelf control unit, which makes information available for display on local and remote user interfaces.

5 Physical Security Policy

The module is designed for use in an ADVA FSP3000 shelf deployed in a typical data center or telecommunication equipment office. The facility should incorporate appropriate controls, including administrative policies and procedures, physical and environmental controls, information and data controls, software acquisition controls, and contingency planning. It is assumed that the facility's security controls restrict the equipment and time that an attacker can have at the module's location.

In addition to the above, the module itself has tamper-evident seals. Refer to Section 5.2 "Physical Inspection".

5.1 EMI/EMC

The module, when installed per this security policy, complies with the EMI/EMC requirements of 47 CFR FCC Part 15, Subpart B, Class A (Business use) equipment.

5.2 Physical Inspection

Table 14 Physical Security Inspection Guidelines

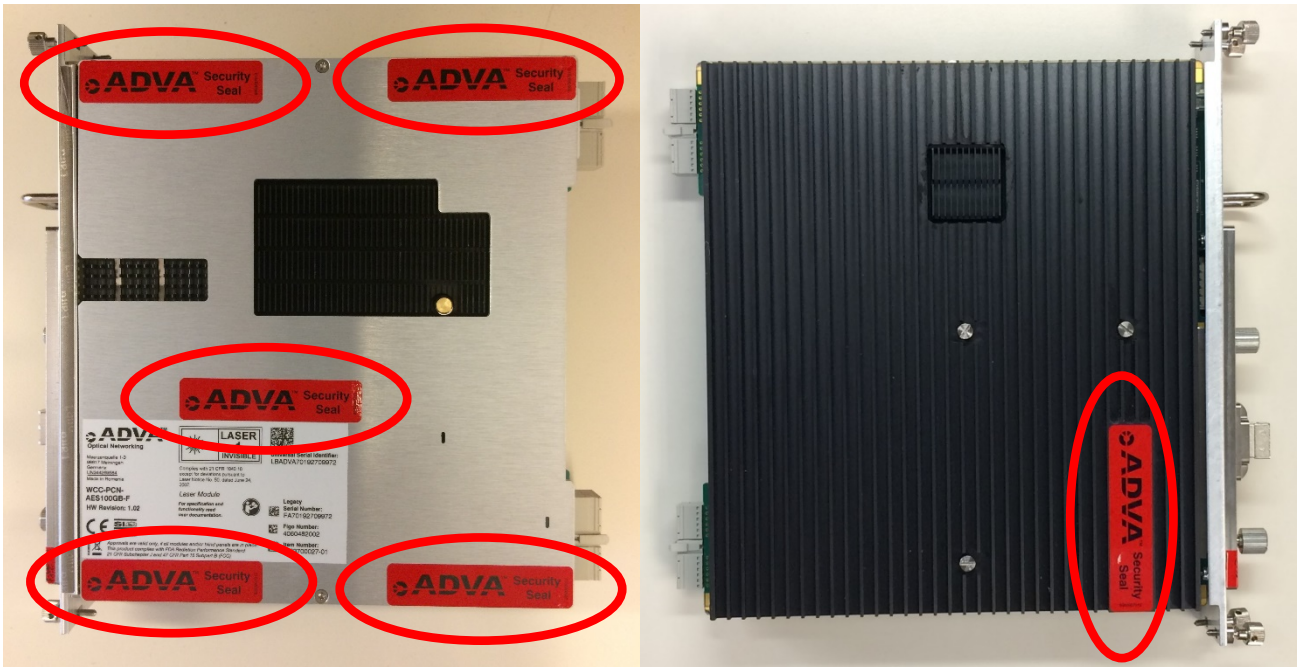
Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Factory-applied seals on shipping packaging, quantity one (1)	Upon initial receipt of card	Inspect the factory-applied seal on the card's shipping bag that protects the module from electrostatic discharge (ESD). Confirm that labeled hardware versions match the values in release notes and this security policy.
Factory-applied tamper-evident seals, quantity six (6)	Upon module installation and at any physical reconfiguration of hardware in the hosting shelf	Inspect factory-applied seals on card to confirm the card has not been tampered with since leaving the factory. Inspect connector pins to confirm no unauthorized connections have been added. Install card to its authorized position in the shelf.
CO-applied tamper-evident seals, quantity four (4) or six (6) seals on shelf depending on shelf type, quantity one (1) seal on CFP transceiver, and quantity one (1) wire seal	Monthly, or after any log event that indicates a card removal condition or absence of the CFP form factor pluggable subassembly	Apply and inspect seals to confirm that the card has not been moved from its authorized position in the shelf. Apply and inspect seals on front panel pluggable transceivers to confirm that the pluggable transceivers have not been removed to expose control inputs. Inspect seals on the shelf chassis to confirm that covers have not been removed to expose control inputs, such as CO password material on the backplane during Initialization. Monitor event logs for unexplained errors in key agreement or decryption services.

Figure 13 shows a factory-applied seal on the ESD-protective bag.

Figure 13 Tamper-Evident Seal on ESD bag

Figure 14 shows the six (6) factory-applied tamper-evident seals on the card assembly.

Figure 14 Factory-Applied Tamper Seals on WCC-PCN-AES100GB-F Card



5.3 Cryptographic Officer-applied Tamper-Evident Seals

To provide assurance that module control inputs are connected only to authorized signals on the backplane and front panel pluggable transceivers, the Cryptographic Officer must apply four (4) or six (6) adhesive tamper-evident seals

(depending on shelf type) to the host shelf, one (1) adhesive tamper-evident seal on the installed pluggable CFP transceiver, and one (1) wire seal through cross-drilled mounting screws.

The Cryptographic Officer is responsible for securing and having control at all times of any unused seals, and for direct control and observation of module installation.

If tamper evidence is found on a seal and is not known to be due to authorized card installation and removal activities, the Cryptographic Officer should remove optical client data connections from the module and from the far-end peer module. The far-end peer module should be commanded to reset to its factory state to zeroize trust values and shared secrets. The module with tamper evidence should be replaced with a trusted unit, after which the optical client data connections at the local and far-end can be reconnected, and services resumed.

5.3.1 Types of Tamper-Evident Seals

5.3.1.1 General Purpose Tamper-Evident Seal

Figure 15 shows a general purpose tamper-evident seal for application at different positions on the shelf chassis and card. The general purpose tamper-evident seal is ADVA part number 1013700030-01. When applied to seams or over access points, the tamper-evident seal will show visible damage if parts forming a seam are displaced or if the seal is punctured or removed to provide access.

Figure 15 General Purpose Tamper-Evident Seal

5.3.1.2 CFP Tamper-Evident Seal

Figure 16 shows a tamper-evident seal for application to the CFP pluggable transceiver that is inserted at the card front panel to implement the network side optical to electrical interface. The CFP tamper-evident seal is ADVA part number 1013700031-01. If the pluggable CFP transceiver is removed from the module front panel, the tamper-evident seal will show visible damage.

Figure 16 CFP Tamper-Evident Seal

5.3.1.3 Tamper-Evident Wire Seal

Figure 17 shows a tamper-evident wire seal with a plastic body for application on mechanical assemblies that have security parts with aligned holes. The tamper-evident wire seal is ADVA part number 1013700032-01. When properly sealed, the wire is threaded through the aligned holes, and the seal or wire must be broken to disassemble the secured parts.

Figure 17 Tamper-Evident Wire Seal

5.3.2 Instructions for Applying Tamper-Evident Seals

For seals that adhere to surfaces:

- Handle seals with care.
- Do not touch the adhesive side.
- Before applying the seal, ensure the location for the application is clean, dry, and clear of any residue.
- Carefully align the seal in position before first contacting the application surface.
- Place the seal on the application surface and apply firm pressure to ensure adhesion.

Tamper evidence function is available immediately after seal application. The adhesive cures for up to 72 hours before it reaches complete stability.

For wire seals:

- Handle seals with care.
- Do not bend the seal handle.
- Feed the seal wire through the cross-holes in screws and chassis blocks according to user documentation for the combination of card and shelf chassis.
- Feed each seal wire end through one of the two cross-holes of the seal body until approximately 2 cm (1 inch) of wire passes through the seal body.

- Twist the seal handle clockwise until all seal wire is coiled completely into the seal body and the seal handle cannot be twisted further without breaking parts.
- Remove the seal handle by bending the handle toward the seal body.

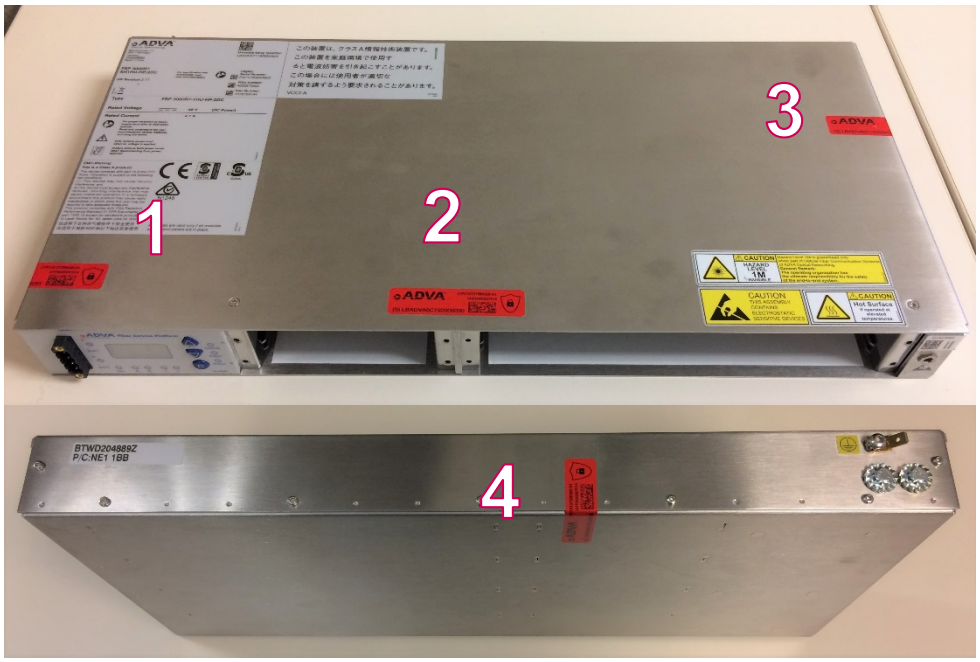
5.3.3 Seals on 1U Shelf with Front DC Power Access

The figures in this section show the locations of seals on the model F7/SH1HU-HP/2DC shelf and model F7/SH1HU-HP/E-TEMP/2DC shelf. The figures show locations of the general purpose tamper-evident seal, ADVA part number 1013700030-01.

Use four (4) seals on the 1U shelves with front DC power access. The seal locations are marked in Figure 18:

- Seal #1: at the top cover and side wall by the power supply.
- Seal #2: at the top cover near the center of the front panel area.
- Seal #3: at the top cover and side wall on the side opposite the power supply.
- Seal #4: at the bottom and rear surfaces near the center of the rear panel area.

Figure 18 Seal Locations on 1U Shelf with Front DC Power Access



See Figure 19 for a close-up view of seal #1's location on the 1U shelf with front DC power access. The seal must be placed on the top cover at the front left edge and must wrap onto the left side.

Figure 19 Detail of Seal #1 Location on 1U Shelf with Front DC Power Access

See Figure 20 for a close-up view of seal #2's location on the 1U shelf with front DC power access. The seal must be placed on the top cover near the center of the front panel area to cover the "Guarantee Void" label, which in turn covers the screw that holds the chassis card slot separator.

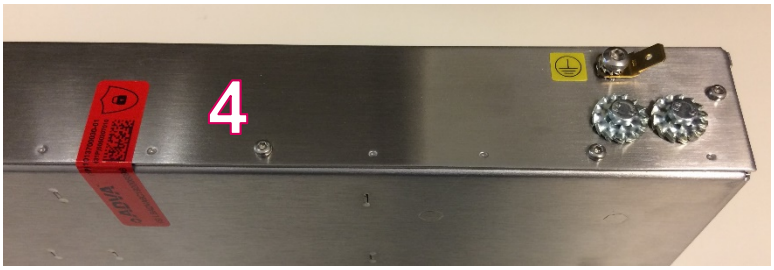
Figure 20 Detail of Seal #2 Location on 1U Shelf with Front DC Power Access

See Figure 21 for a close-up view of seal #3's location on the 1U shelf with front DC power access. The seal must be placed on the top cover near the middle of the right edge, about 2/5 of the way from the rear, and must wrap onto the right side between the air outlets.

Figure 21 Detail of Seal #3 Location on 1U Shelf with Front DC Power Access

See Figure 22 for a close-up view of seal #4's location on the 1U shelf with front DC power access. The seal must be placed on the bottom and rear surfaces near the center screw about 2 to 4 cm toward the ground lugs.

Figure 22 Detail of Seal #4 Location on 1U Shelf with Front DC Power Access



5.3.4 Seals on 1U Shelf with Rear Power Access

The figures in this section show the locations of seals on the model F7/SH1HU-R/PF shelf. The figures show locations of the general purpose tamper-evident seal, ADVA part number 1013700030-01.

Use six (6) seals on the 1U shelf with rear power access. Four (4) seal locations are marked in Figure 23 and two (2) seal locations are marked in Figure 24:

- Seal #1: at the top cover on the side with the power supply.
- Seal #2: at the top cover near the center of the front panel area.
- Seal #3: at the top cover on the side opposite the power supply near the front.
- Seal #4: at the top cover on the side opposite the power supply near the rear.

- Seal #5: at the bottom cover on the side opposite the power supply.
- Seal #6: at the bottom cover on the side with the power supply.

Figure 23 Seal Locations on Top of 1U Shelf with Rear Power Access

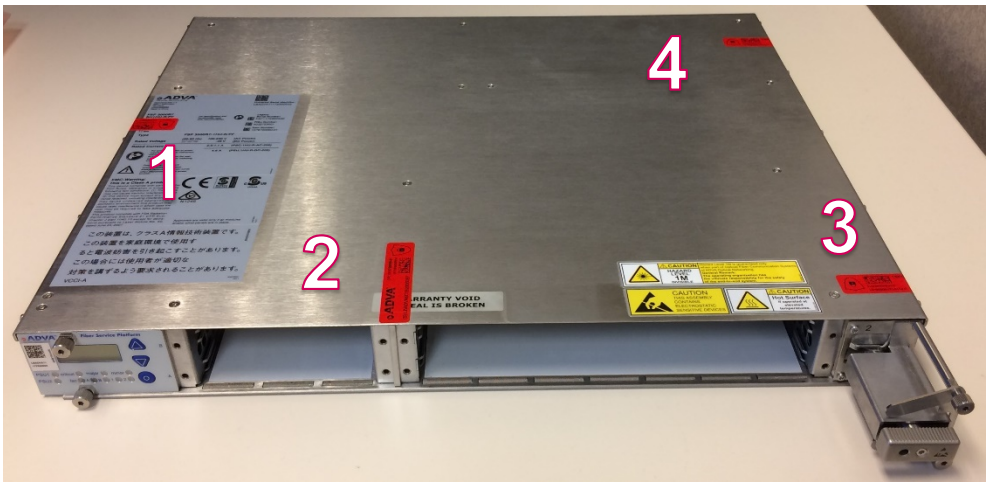
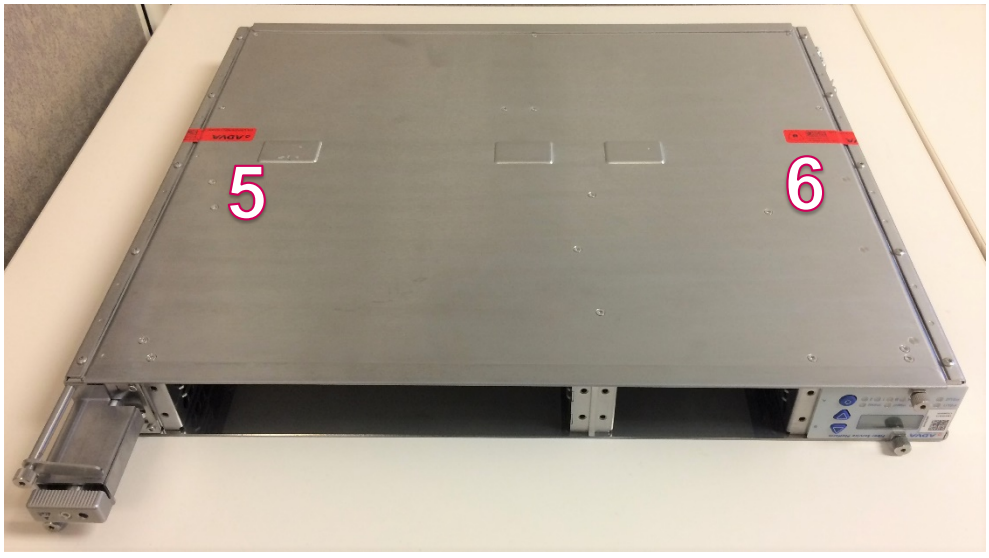


Figure 24 Seal Locations on Bottom of 1U Shelf with Rear Power Access



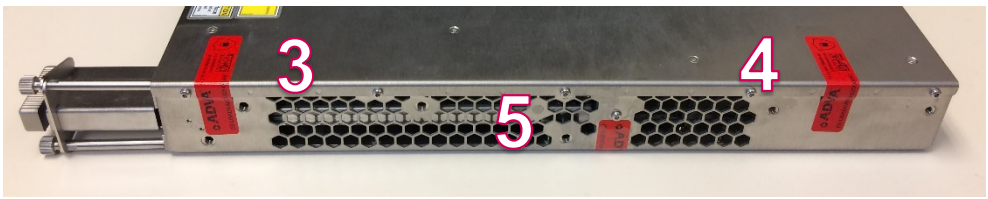
See Figure 25 for a close-up view of locations for seal #1 and seal #6 on the 1U shelf with rear power access. Seal #1 must be placed on the top cover near the middle of the left edge and must wrap onto the left side between the air

outlets. Seal #6 must be placed on the bottom cover near the middle of the left edge and must wrap onto the left side between the air outlets.

Figure 25 Detail of Seal #1 and #6 Locations on 1U Shelf with Rear Power Access

See Figure 26 for a close-up view of locations for seals #3, #4, and #5 on the 1U shelf with rear power access. Seal #3 must be placed on the top cover near the front of the right edge and must wrap onto the right side in front of the air outlets. Seal #4 must be placed on the top cover near the rear of the right edge and must wrap onto the right side behind the air outlets. Seal #5 must be placed on the bottom cover near the middle of the right edge and must wrap onto the right side between the air outlets.

Figure 26 Detail of Seal #3, #4, and #5 Locations on 1U Shelf with Rear Power Access



See Figure 27 for a close-up view of seal #2's location on the 1U shelf with rear power access. The seal must be placed on the top cover near the center of the front panel area to cover the "Warranty Void" label, which in turn covers the

screw that holds the chassis card slot separator. (Note: The white "Warranty Void" label shown in Figure 27 is not a tamper-evident seal.)

Figure 27 Detail of Seal #2 Location on 1U Shelf with Rear Power Access

5.3.5 Seals on 9U Shelf

The figures in this section show the locations of seals on the model F7/SH9HU shelf. The figures show locations of the general purpose tamper-evident seal, ADVA part number 1013700030-01.

Use four (4) seals on the 9U shelf.

Two (2) seal locations on the top of the shelf are marked in Figure 28:

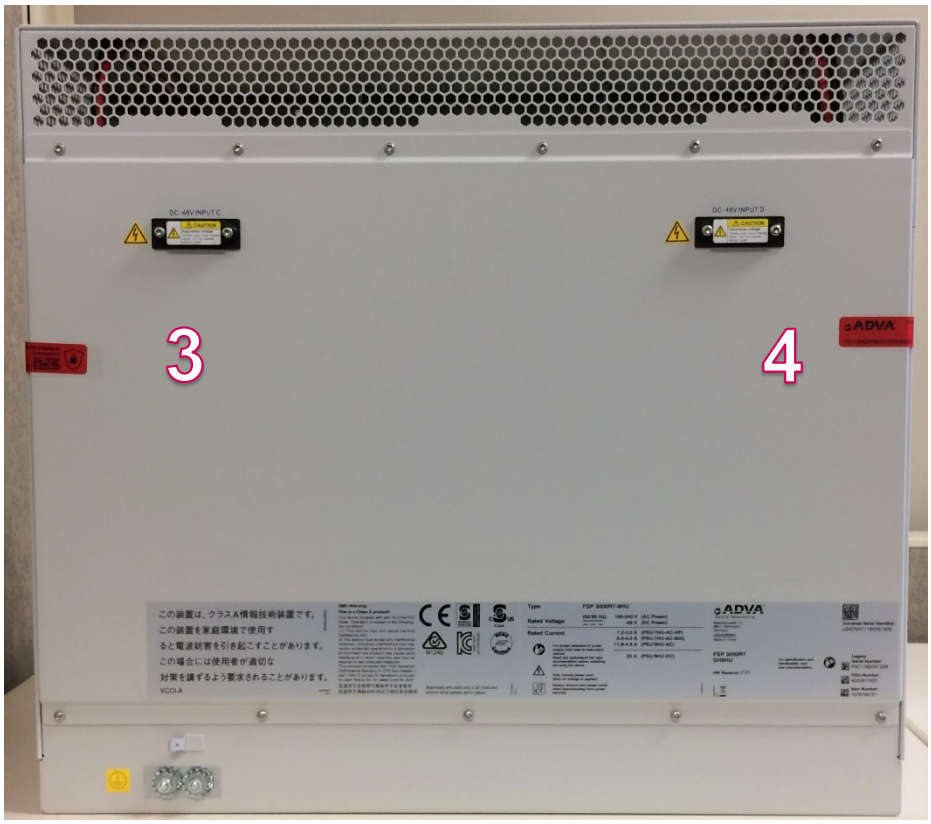
- Seal #1: at the rear edge of the chassis top surface, covering the second screw from the left edge.
- Seal #2: at the rear edge of the chassis top surface, covering the second screw from the right edge.

Figure 28 Seal Locations on Top of 9U Shelf

Two (2) seal locations on the rear of the shelf are marked in Figure 29:

- Seal #3: at the left side (as viewed from the rear) at about 2/3 the height of the removable rear cover, wrapped around the edge to adhere to the rear and left covers.
- Seal #4: at the top about 1/3 of the chassis width from the left side (as viewed from the rear), wrapped around the edge to adhere to the rear and top covers.

Figure 29 Seal Locations on Rear of 9U Shelf



5.3.6 Seals on Card Secured to Transceivers and Shelf

The figures in this section show the locations of seals on the WCC-PCN-AES100GB-F card.

Figure 30 shows the location of the CFP tamper-evident seal, ADVA part number 1013700031-01, on the CFP form factor network interface transceiver.

Figure 30 Seal Location on CFP Transceiver in Card

Figure 31 shows the location of the tamper-evident wire seal, ADVA part number 1013700032-01. The wire is threaded through the cross-drilled top mounting screws that secure the card in the 9U shelf.

Figure 31 Wire Seal Placement through Top Cross-Drilled Mounting Screws on Card in 9U Shelf

When the WCC-PCN-AES100GB-F card is installed in a 1U chassis, the two cross-drilled mounting screws that are supplied at the bottom front position of the card must be moved to secure the neighboring cards or blank panels. This

allows a single wire seal to secure all the slots on the 1U shelf. The red arrow in Figure 32 shows the repositioning of two cross-drilled screws, and the green arrow shows the repositioning of conventional screws.

Figure 32 Cross-Drilled Card Mounting Screw Positions on 1U Shelf

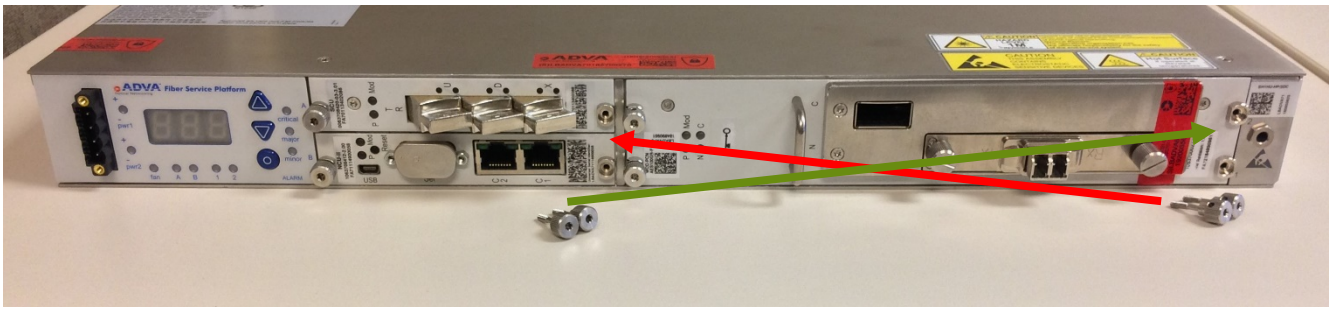


Figure 33 shows the position of the tamper-evident wire seal, ADVA part number 1013700032-01. Close-up detail is shown in Figure 34. The wire is threaded through the four (4) cross-drilled screws at the front center of the shelf. One cross-drilled screw secures each of the two (2) blank panels or cards on the left side of the shelf, and two (2) cross-drilled screws secure the WCC-PCN-AES100GB-F card.

Figure 33 Wire Seal Placement through Four (4) Cross-Drilled Mounting Screws on Card in 1U Shelf

Figure 34 Wire Seal Placement Detail in 1U Shelf

6 Operational Environment

The module has a non-modifiable operational environment under the FIPS 140-2 definitions. The module includes a firmware load service to support necessary updates. New firmware is only activated if the Cryptographic Officer authorizes installation of the matching firmware version and the module successfully verifies a digital signature over the firmware image. The module is FIPS-validated only when running firmware that has been validated on the module through the FIPS 140-2 CMVP.

7 Mitigation of Other Attacks Policy

This section is not applicable. The module does not claim to mitigate any other attacks.

8 Security Rules and Guidance

This section documents the security rules for operation of the module to implement the security requirements of FIPS 140-2.

1. The module provides two (2) distinct authenticated operator roles: User and Cryptographic Officer, and an unauthenticated role.
2. The module provides role-based authentication: password for Cryptographic Officer commands which affect security and static Diffie-Hellman authentication for User operations.
3. The module clears previous authentications at the completion of each authenticated command and on power cycle.
4. An operator does not have access to any cryptographic services prior to assuming an authorized role.
5. The module allows the operator to initiate power-on self-tests by power cycling the module or by issuing an authenticated Cryptographic Officer command.
6. Power-on self-tests do not require any operator action.
7. Data outputs are inhibited during self-tests, zeroization, and error states. Data outputs are not connected to key generation processes. Data outputs do not contain CSPs.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. Zeroization performed by the reset and firmware update services operates on all CSPs.
10. The module supports the "Encrypt network link" User service concurrently with some in-operation services (see Section 3.5 "Concurrent Operations").
11. The module does not support a maintenance interface or role, or a bypass mode.

12. The module does not support manual key entry.
13. The module interfaces with the ADVA NCU and ADVA SCU via the shelf backplane for control and status input/output. The module interfaces with industry standard optical transponders for input/output of client and network data.
14. The module does not enter or output plaintext CSPs; the CO password is entered as a hash value.
15. The module does not output intermediate key values.
16. The operator must apply the tamper seals as indicated in Section 5.3 "Cryptographic Officer-applied Tamper-Evident Seals".
17. The Cryptographic Officer must select a password with a value that is robust against human and machine guessing, for instance by using an entropy-seeded password generator program.
18. When changing the password from its factory-default value, the Cryptographic Officer should confirm that the shelf backplane and local rack wiring has not been tampered with by an attacker, and that the communication links for the user interface do not reveal plaintext contents of password change commands.
19. The module automatically starts the "Encrypt network link" service and automatically reruns the "Key agreement" service in the User role after the Cryptographic Officer has accepted trust of the other party cryptographic credentials.

9 References and Definitions

Table 15 References

Reference	Full Specification Name
[38A]	Morris Dworkin, *Recommendation for Block Cipher Modes of Operation - Methods and Techniques*, NIST Special Publication 800-38A, December 2001. U.S. Department of Commerce, National Institute of Standards and Technology.
[56Ar3]	Elaine Barker, Lily Chen, Allen Roginsky, Apostol Vassilev and Richard Davis, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, NIST Special Publication 800-56A Revision 3, April 2018. U.S. Department of Commerce, National Institute of Standards and Technology.
[57p1r4]	Elaine Barker, *Recommendation for Key Management, Part 1: General*, NIST Special Publication 800-57 Part 1 Revision 4, January 2016. U.S. Department of Commerce, National Institute of Standards and Technology.

Reference	Full Specification Name
[90A]	Elaine Barker and John Kelsey, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, NIST Special Publication 800-90A Revision 1, June 2015. U.S. Department of Commerce, National Institute of Standards and Technology.
[133r2]	Elaine Barker, Allen Roginsky, and Richard Davis, *Recommendation for Cryptographic Key Generation*, NIST Special Publication 800-133 Revision 2, June 2020. U.S. Department of Commerce, National Institute of Standards and Technology.
[140]	*FIPS PUB 140-2 Security Requirements for Cryptographic Modules*, May 25, 2001. U.S. Department of Commerce, National Institute of Standards and Technology.
[180]	*FIPS PUB 180-4 Secure Hash Standard (SHS)*, August 2015. U.S. Department of Commerce, National Institute of Standards and Technology.
[186]	*FIPS PUB 186-4, Digital Signature Standard (DSS)*, July 2013. U.S. Department of Commerce, National Institute of Standards and Technology.
[197]	*Federal Information Processing Standards Publication 197 Specification for the Advanced Encryption Standard (AES)*, November 26, 2001. U.S. Department of Commerce, National Institute of Standards and Technology.
[198]	*FIPS PUB 198-1 The Keyed-Hash Message Authentication Code (HMAC)*, July 2008. U.S. Department of Commerce, National Institute of Standards and Technology.
[IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*, August 28, 2020. National Institute of Standards and Technology, Canadian Centre for Cyber Security.
[RFC 3447]	Jakob Jonsson and Burt Kaliski, *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1*, Internet Society Request for Comments 3447, February 2003.

Table 16 Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard (see [197])
CFP	C Form-factor Pluggable transceiver interface
CKG	Cryptographic Key Generation
CMVP	Cryptographic Module Validation Program
CO	Cryptographic Officer

Acronym	Definition
CSP	Critical Security Parameter
CTR	Counter mode of block cipher operation (see [38A])
DLC	Discrete Logarithm Cryptography
DRBG	Deterministic Random Bit Generator (see [90A])
FC	Name for an FFC parameter-size set (see Table 1 in [56Ar3])
FFC	Finite Field Cryptography
HMAC	Hashed Message Authentication Code (see [198])
HTTPS	Hypertext Transfer Protocol for Secure Communication
KAS	Key Agreement Scheme
KAT	Known Answer Test
KDF	Key Derivation Function
KPG	Key Pair Generation
NCU	ADVA Network element Control Unit
OTU4	Signaling format specified in ITU-T Recommendation G.709
PSS	Probabilistic Signature Scheme (see [186] and [RFC 3447])
QSFP	Quad Small Form-factor Pluggable transceiver interface
RSA	Rivest Shamir Adleman cryptosystem (see [186])
SCU	ADVA Shelf Control Unit
SHA	Secure Hash Algorithm (see [180])
SHS	Secure Hash Standard (see [180])
SSH	Secure Shell
VA	Vendor Affirmed (see Section A.3 of [IG])