Non-proprietary FIPS 140-2 Security Policy

Encryption Card
ADVA 9TCE-PCN-10GU+AES10G-F

ADVA Optical Networking SE

CONTENTS

1 Introduction 5

1.1 Purpose 6

1.2 References 7

2 Module 7

2.1 Overview 7
2.1.1 Typical application of FSP3000 system: 7
2.1.2 9TCE Encryption Card 8
2.1.3 Cryptographic Boundary 9

2.2 Module Specification 12

2.3 Security Level 13

2.4 Modes of Operation 13
2.4.1 How to Operate the Module in FIPS Approved Mode 15

3 Module Ports and Interfaces 15

4 Roles, Service and Authentication 15

4.1 Identification and Authentication Policy 15

4.2 Authentication Strength 16

4.3 Authenticated Services 16

4.4 Unauthenticated Services 17

5 Operational Environment 18

6 Cryptographic Key Management 18

7 EMI/EMC 20

8 Self-Tests 20

8.1 Power-On or on Demand Self-Tests 21

8.2 Conditional Self-Tests 22

8.3 Self-Test Failure Handling 23

9 Access Control Policy 23

10 Physical Security Policy 23

10.1 Physical Security Mechanisms 23

11 Security Rules 24

12 Mitigation of other Attacks Policy 24

13 Secure Operation 25

13.1 Installation, Initialization and Startup 25

13.2 General Tamper Seal Placement and Instructions 26

13.3 Types of Security Seals 27
13.3.1 Shelf 9 HU Placement Seals 27
13.3.2 Security Seal Label CFP 27
13.3.3 Security Twist Wire Seal 27

13.4 Security Seal Application Instruction 28
13.4.1 Security Seal Labels 28
13.4.2 Security Twist-Wire Seals 28
13.4.3 Shelf 1 HU Placement Seals SH1HU-HP/2DC and SH1HU-HP/E-TEMP/2DC 29
13.4.4 Sealing of SH1HU-R/PF 30
13.4.5 Sealing of SH7HU(-R) 32
13.4.6 Shelf 9 HU Placement Seals 33
13.4.7 Sealing of 9TCE-PCN-10GU+AES10G-F 34

13.5 Periodical Inspection 35

14 Definitions and Acronyms 36

FIGURES

Figure 1: 9TCE- based FSP 3000 Systems 6
Figure 2: Typical application of an ADVA FSP 3000 system 7
Figure 3: 9TCE encryption cards in FSP 3000 encryption solution 7
Figure 4: ADVA 9TCE-PCN-10GU+AES10G-F with backplane interface 8
Figure 5: 9TCE mounted in shelf SH9HU with red dotted line for Cryptographic Boundary 9
Figure 6: 9TCE mounted in shelf SH7HU (red dotted line indicating Cryptographic Boundary) 9
Figure 7: 9TCE mounted in shelf SH1HU (red dotted line indicating Cryptographic Boundary) 10
Figure 8: 9TCE top view with marked interfaces 10
Figure 9: 9TCE -front and back view 10
Figure 10: 9TCE left view 10
Figure 11: 9TCE right view 11
Figure 12: 9TCE bottom view 11

Figure 13: 9TCE card in multiple transponder mode 11
Figure 14: 9TCE card in single muxponder mode 12
Figure 15: 9TCE card in dual muxponder mode 12
Figure 16: Sealed ESD bag 25
Figure 17: Generic security seal label 27
Figure 18: Security seal label CFP 27
Figure 19: Security plastic wire coil-in seal package 27
Figure 20: Security plastic wire coil-in seal 27
Figure 21: Placement of seals on shelf 1 HU, top views 29
Figure 22: Placement seals, shelf 1 HU, placement 1 29
Figure 23: Placement seals, shelf 1 HU, placement 2 30
Figure 24: Placement seals, shelf 1 HU, placement 3 30
Figure 25: Placement seals, shelf 1 HU, placement 4 30
Figure 26: Placement of seals SH1HU-R/PF front-top view 31
Figure 27: Placement of seals SH1HU-R/PF front-bottom 31
Figure 28: Placement of seals SH1HU-R/PF left side positions 32
Figure 29: Placement of seals SH1HU-R/PF right side positions 32
Figure 30: Placement of seal SH1HU-R/PF right side position 32
Figure 31: Placement of seal SH7HU rear side 33
Figure 32: Placement of seal SH7HU (-R) rear side 33
Figure 33: Seals rear side shelf 9HU 34
Figure 34: Seals cover rear edge shelf 9 HU 34
Figure 35: Placement of twist seal in SH1HU configuration 35
Figure 36: Placement of twist seal in SH7HU and SH9HU configuration 35

TABLES

Table 1: Cryptographic module configurations 5
Table 2: Module validation security levels 13
Table 3: Cryptographic algorithms 14
Table 4: Cryptographic algorithms of the embedded module #2628 used by the cryptographic module 15
Table 5: Roles and required encryption identification and authentication 15
Table 6: Strength of authentication mechanisms 16
Table 7: Roles and services authenticated 17
Table 8: Roles and services unauthenticated 18
Table 9: Cryptographic key, CSP and PSP management 20
Table 10: Power-up self-tests 22
Table 11: Conditional tests 23
Table 12: Inspection/testing of physical security mechanisms 24
Table 13: Mitigation of other attacks 25
Table 14: Definition and acronyms 36

1 Introduction

This is the non-proprietary FIPS 140-2 Security Policy for the encryption card ADVA 9TCE-PCN-10GU+AES10G-F (also referred to as "9TCE" or as "9TCE encryption card" hereinafter). The cryptographic boundary of the module in the sense of FIPS 140-2 is the configured 9TCE encryption card within customer-chosen combinations of shelves with modular functionality and density. For clarity, the cryptographic module in the meaning of FIPS 140-2 consists of the 9TCE encryption card placed inside one of the shelves listed in table 1 below.

The module is a multiple-chip embedded cryptographic module that is covered with a commercial-grade metal cover that includes components equipped for physical security and assurance of opacity. They belong to the module in the sense of FIPS 140 and are located within the cryptographic boundary, but contribute exclusively to the physical security of the module.

The module is a part of the ADVA Fiber Service Platform (FSP) 3000 scalable optical data transport system. The module is a transponder for core telecommunication networks, and transports plaintext 10GbE or OUT-2 client-side data services to and from the encrypted network interface. The module performs key agreement and synchronization with a far-end network peer to support AES encryption of the network link.

The FIPS validation covers the following combinations of hardware and firmware of the 9TCE encryption card and either one of the listed shelves (firmware 191.4.8 contains some stability fixes, while the services and cryptographic functionality of the module stays the same as in 172.25.7; firmware versions for microcontroller part and FPGA part always correspond to each other one-to-one in a module, no mixing of versions is possible):

Component	Version	OE Processor	Part Number Hardware
Hardware: Encryption Card ADVA 9TCE-PCN-10GU+AES10G-F	HW B-1.01		1063707672-01 F7/9TCE-PCN-10GU+AES10G-F
Firmware: microcontroller part	172.25.7 / 191.4.8	Coldfire MCF5282	n/a
FPGA part	172.25.7 / 191.4.8	Xilinx Kintex UltraScale FPGA	n/a
Configured in one of the following shelves: 9HU shelf (SH9HU)	HW 2.01	n/a	1078700121 F7/SH9HU
7HU shelf (SH7HU)	HW 2.05	n/a	0078700101 F7/SH7HU
7HU shelf (SH7HU-R)	HW 2.05	n/a	0078700111 F7/SH7HU-R
1HU shelf (SH1HU-R/PF)	HW 1.01	n/a	1078700060-01 F7/SH1HU-R/PF
1HU shelf (SH1HU-HP/2DC)	HW 2.11	n/a	1078700144 F7/SH1HU-HP/2DC
1HU shelf (SH1HU-HP/E-TEMP/2DC)	HW 1.01	n/a	1078700145-01 F7/SH1HU-HP/E-TEMP/2DC
Tamper evident seals (delivery): SEAL/FIPS-GENERAL	n/a	n/a	1013700030-01
SEAL/FIPS-WIRE	n/a	n/a	1013700032-01
Tamper evident seals (ordered separately): SEAL/FIPS-GENERAL/5	n/a	n/a	BC00000738

Table 1: Cryptographic module configurations

Each of the module configurations has to be equipped to assure the opacity as required by FIPS 140-2 and the security as specified in Module and System Specification and User Documentation for approved operation. (Details in section 13, Secure Operation).

The module configuration within the shelf defines the Cryptographic Boundary. The shelf is part of the module, but contributes exclusively to the physical security, to ensure that the module is opaque within the visible spectrum. By tamper evident seals applied to 9TCE encryption card and shelf, tamper evidence is ensured for the module.

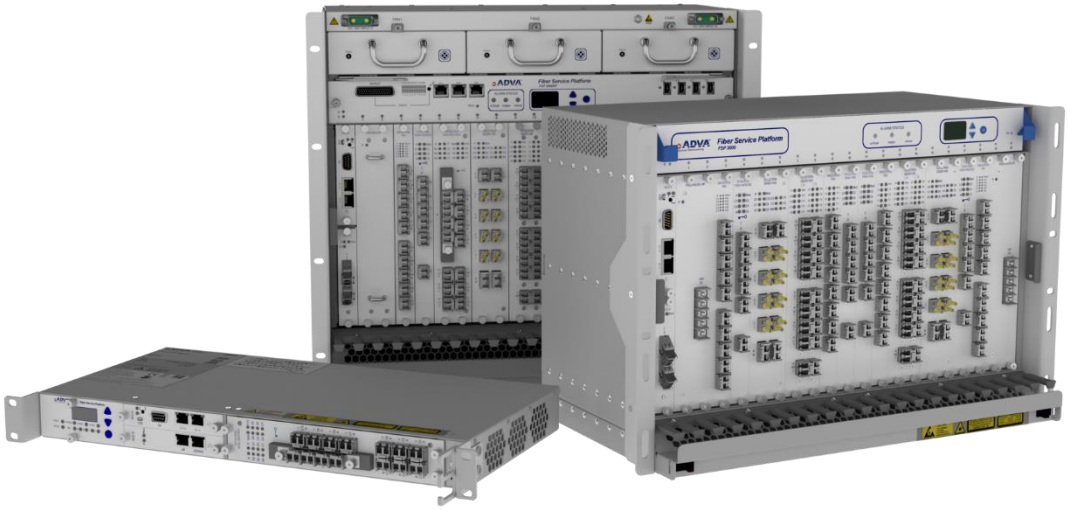

Figure 1: 9TCE- based FSP 3000 Systems

1.1 Purpose

This document was prepared as part of the FIPS 140-2 validation process.
This document describes, how the module meets the security requirements of FIPS 140-2. In addition, individuals and organizations receive instructions on how to use the product in a secure mode as approved by FIPS. The target group of this document is anyone who wants to use one of these products or wants to integrate it into a solution that meets the requirements of FIPS 140-2.

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 validation submission documentation is ADVA-proprietary and is releasable only under appropriate non-disclosure agreements.
For access to these product documents, please contact ADVA:

ADVA Optical Networking SE
Fraunhoferstr. 9a
82152 Martinsried/München
Germany
Phone +49(0)89-890665-0
Fax +49(0)89-890665-699
https://www.adva.com

1.2 References

This document describes, how the module meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2.

More details regarding FIPS 140-2 standards, qualification and the Cryptographic Module Validation Program (CMVP) are available on the NIST website, see https://csrc.nist.gov/projects/cryptographic-module-validation-program.

2 Module

2.1 Overview

2.1.1 Typical application of FSP3000 system:

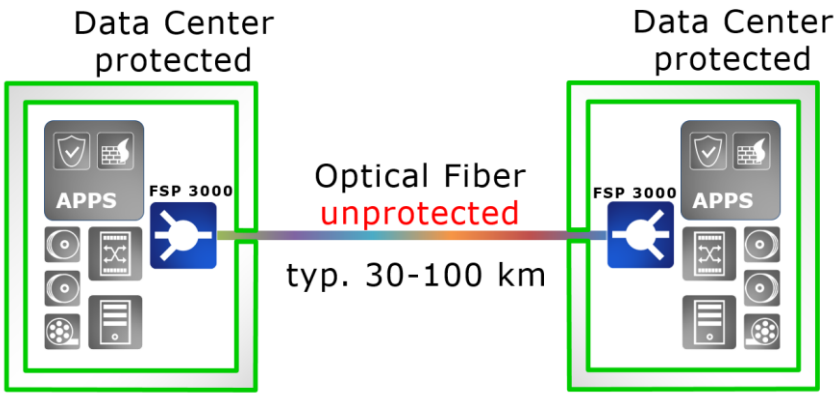

Figure 2: Typical application of an ADVA FSP 3000 system

In a typical application, the FSP 3000 containing the module is located in racks in a data center. The fiber connection between the data centers is completely owned by the user or a "service", which is sold by a service provider. The physical access to the equipment is controlled. Access is only granted to persons, which need to have access for restricted time. The access time is logged.

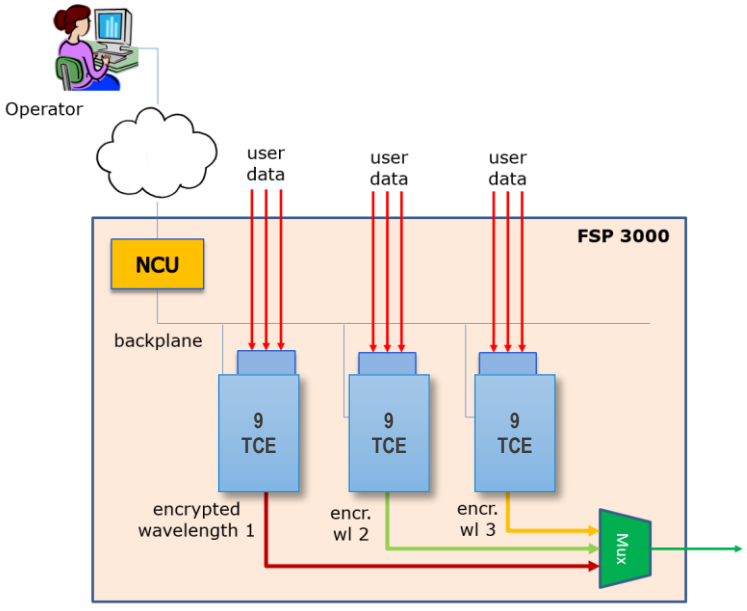

Figure 3: 9TCE encryption cards in FSP 3000 encryption solution

A typical encryption solution for the optical fiber connection with FSP 3000 consists of the following components: One or more FSP 3000 shelves including shelf controller, fan unit, power supply, and one network control unit (NCU) in the main shelf, multiple encryption cards and optical filters.
The 9TCE module interfaces supports up to ten SFP and SFP+ pluggable optics providing the optical-to-electrical conversion (and vice versa), collection of physical layer performance monitoring and alarm monitoring for each client service. The client interfaces support services with data rates ranging between 10Mbit/s (Ethernet) and 10.709Gbit/s (OTU2) while the network interfaces support data rates of 10.709Gbit/s (OTU2), 11.095Gbit/s (OTU2e) and 10.975Gbit/s (OTU2fc). This user data stream is encrypted, framed in OTU frames, protected with error correction codes and transmitted to the far-end side. The receiving side decrypts the data and sends it to the corresponding clients.

2.1.2 9TCE Encryption Card

The 9TCE-PCN-10GU+AES10G-F encryption card (abbreviated in this document as 9TCE) is a plug-in card for the FSP 3000 system. The 9TCE alone is implementing all logics/functionality as required by FIPS 140-2, yet the 9TCE alone is not the cryptographic module in the meaning of FIPS140-2. To satisfy the physical security requirements of FIPS 140-2 (mainly the opacity requirements), the 9TCE has to be mounted in one of the shelves as stated in the following section "Cryptographic Boundary" (see there for images of 9TCE and the corresponding shelves).

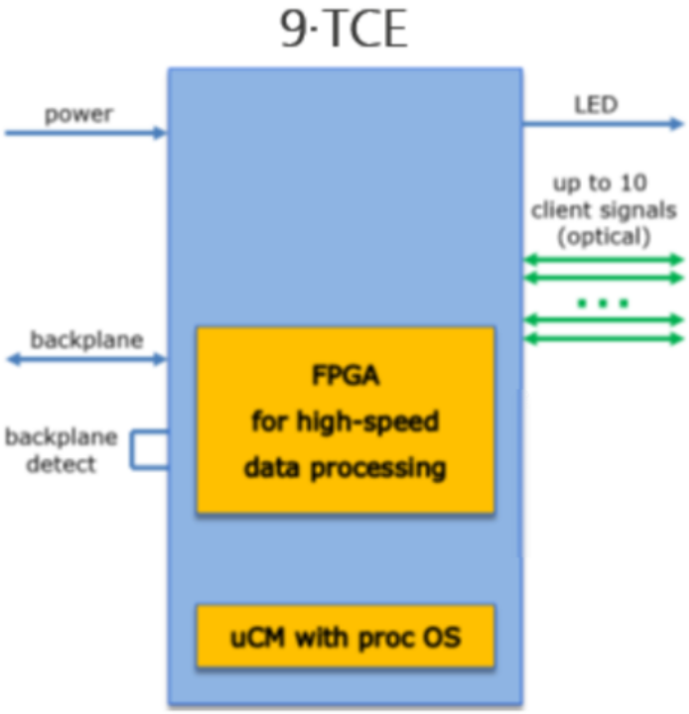

Figure 4: ADVA 9TCE-PCN-10GU+AES10G-F with backplane interface

The 9TCE shows its current status with LEDs on the front panel and NCU notifications. Please see Section 2.1.3 for pictures of the cryptographic module an the available shelves in can be operated in.

The NCU has contact to all modules, using the backplane with 100 Mbit/s Ethernet and VLANs. Please take note that the NCU is not part of the cryptographic module, it is an input/output device for the module only.

Furthermore, 9TCE contains an embedded cryptographic module, "StarSign Crypto-USB Token S powered by Sm@rtCafé Expert 7.0 Secure Element" by Giesecke+Devrient Mobile Security GmbH. This embedded module is a single-chip cryptographic module in a VQFN32 IC package, which is firmly integrated into the 9TCE using surface-mounting

technology (it is used as a seed source for 9TCE DRBG, compare CMVP cert. #2628 and corresponding security policy, and DRBG cert. #455).

2.1.3 Cryptographic Boundary

The Cryptographic Boundary is defined as the entire metal case of the 9TCE card include the outer range of the configured shelf, including all hardware, software and firmware encapsulated and tamper response detection within (as 9TCE contains the embedded cryptographic module, "StarSign Crypto-USB Token S powered by Sm@rtCafé Expert 7.0 Secure Element" by Giesecke+Devrient Mobile Security GmbH, this embedded module is also located inside the cryptographic boundary). The interfaces are all traces that cross the Cryptographic Boundary.

The physical forms of the different shelves the cryptographic module can be operated in are shown in Figure 5 to Figure 7. Here the 9TCE encryption board is integrated to each available shelf listed in Table 1. Figure 8 to Figure 12 show the 9TCE encryption board

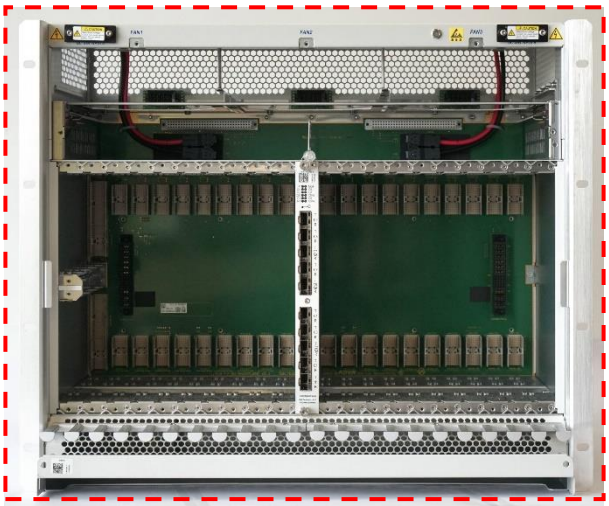

Figure 5: 9TCE mounted in shelf SH9HU with red dotted line for Cryptographic Boundary

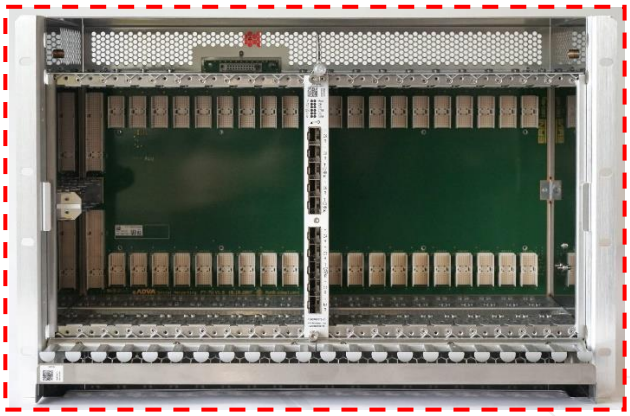

Figure 6: 9TCE mounted in shelf SH7HU (red dotted line indicating Cryptographic Boundary)

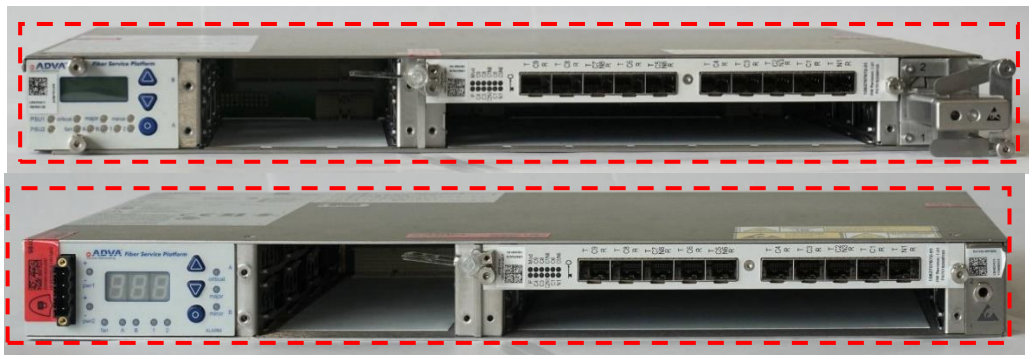

Figure 7: 9TCE mounted in shelf SH1HU (red dotted line indicating Cryptographic Boundary)

Figure 8: 9TCE top view with marked interfaces

Figure 9: 9TCE -front and back view

Figure 10: 9TCE left view

Figure 11: 9TCE right view

Figure 12: 9TCE bottom view

The primary purpose of the 9TCE encryption card is to secure data traffic over fiber-optical lines. The 9TCE encryption card supports multiple network interfaces and each interface runs independent encryption engines with independent management interface (configuration, fault, performance management). Encryption configuration and operation are managed individually per network port. There is only one Crypto Officer Password per 9TCE used to control all encryption related actions on any network port. . The 9TCE (as a whole, not the network ports individually) can be configured to "Transponder Mode" or "Muxponder Mode", and some of the ports can act either as client or as network depending on configuration. The following figure shows the 9TCE card in multi transponder mode with 4 client ports and 4 network ports.

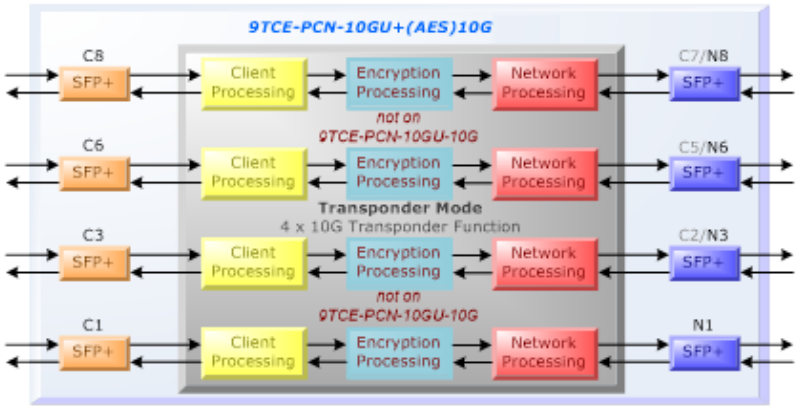

Figure 13: 9TCE card in multiple transponder mode

The following figure shows the 9TCE card in single muxponder mode with 9 client ports and 1 network port.

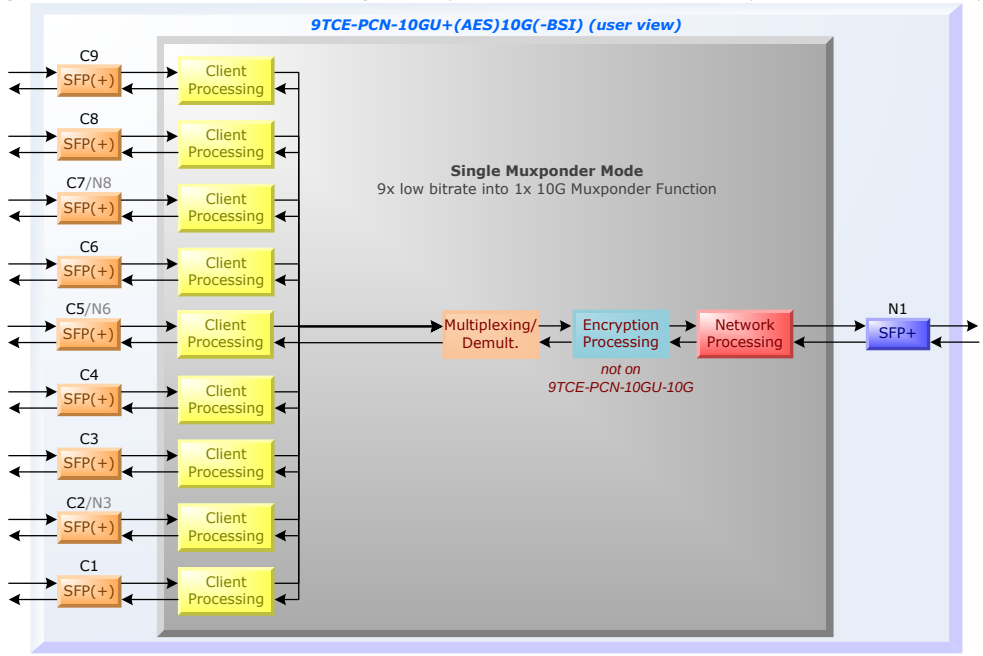

Figure 14: 9TCE card in single muxponder mode

The following figure shows the 9TCE card in dual muxponder mode with 8 client ports and 2 network port.

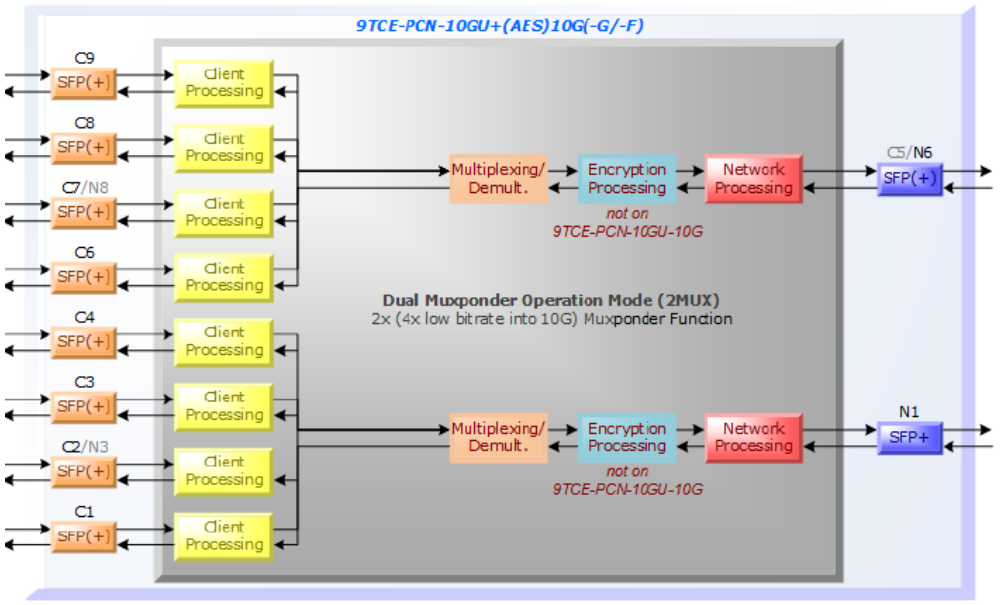

Figure 15: 9TCE card in dual muxponder mode

2.2 Module Specification

When placed inside one of the shelves listed in Table 1, the 9TCE card is shielded with metal on front, left and right side. It has openings at its top, bottom and back side, which are required for air flow and cooling. All sensitive components are inside the shielding. The cover is fixed with rivets to make it hard for an attacker to open and modify it. Figures 8 to 12 show the openings in the cover to allow air flow when 9TCE is mounted in a shelf. Electronic components of the 9TCE cannot be seen through these openings, when 9TCE is mounted in a shelf as given in table 1. The 9TCE cover and the layout of the PCB of 9TCE, in combination with the corresponding shelf, guarantee that sensitive components of 9TCE

(e.g., micro controller, FPGA, seed source, or IC used for password storage) are not reachable and that IC descriptions are not visible.

2.3 Security Level

The module meets the overall requirements applicable to Level 2 security of FIPS 140-2. In section "Cryptographic Key Management" and "Design Assurance" level 3 is reached. The module has a 128-bit overall security strength.

Security Requirements Section	Level
Cryptographic Module Specification	2
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	2

Table 2: Module validation security levels

2.4 Modes of Operation

The module is designed to exclusively run in the Approved mode of operation. In this mode, the module supports the following FIPS-approved cryptographic algorithms (certificate numbers with prefix "C" belong to the firmware version 172.25.7, certificate numbers with prefix "A" belong to firmware version 191.4.8, no mixing of versions is possible in one module):

CAVP Cert	Algorithm	Standard(s)	Mode / Method	Key Lengths, Curves or Moduli	Use
#C667 for FW 172.25.7	AES	FIPS 197, SP 800-38A	CTR Encryption/ Decryption	256 bits	AES-CTR User Data Encryption/ Decryption on FPGA
#A887 for FW 191.4.8			ECB Encryption/ Decryption	256 bits	AES-CTR User Data Encryption/ Decryption on FPGA, see note below.
#C666 for FW 172.25.7 #A886 for FW 191.4.8	AES	FIPS 197, SP 800-38A	ECB Encryption/ Decryption	128 bits 256 bits	Secure Storage CTR_DRBG (in 9TCE firmware)
#C666 for FW 172.25.7 #A886 for FW 191.4.8	HMAC	FIPS 198-1	SHA-256	256-bit hash length	Key Confirmation according to SP 800-56Ar3 Sec. 6.1.1.5.3

#C666 for FW 172.25.7 #A886 for FW 191.4.8	SHS	FIPS 180-4	SHA-256, SHA-512	256-bit hash length 512-bit hash length	Secure Hash
#C666 for FW 172.25.7 #A886 for FW 191.4.8	DRBG	SP 800-90Ar1	CTR_DRBG	256 bits of strength	Deterministic Random Bit Generator (in 9TCE firmware)
#C666 for FW 172.25.7 #A886 for FW 191.4.8	RSA	FIPS 186-4	SHA-256 RSASSA-PKCS1-v1_5, RSASSA-PSS	4096 bits	Digital Signature verification
Vendor affirmed for FW 172.25.7	KAS	SP 800-56Ar3 (vendor affirmed per IG D.1-Rev3)	FFC (dhHybrid1, C(2e, 2s, FFC DH) Scheme) with One-Step Key Derivation using SHA-512 per SP 800-56Cr2	3072 bits	Key Establishment (key establishment methodology provides 128 bits of encryption strength)
#A886 for FW 191.4.8		SP 800-56Ar3			
#A886 for FW 191.4.8	Safe Primes Key Generation	SP 800-56Ar3	–	MODP-3072	Generation of DH key pairs (static and ephemeral key pairs) according to SP 800-56Ar3 Sec. 5.6.1.1.1 and 5.6.1.1.4 for use in the KAS
#A886 for FW 191.4.8	Safe Primes Key Verification	SP 800-56Ar3	–	MODP-3072	Used in the KAS for key validation according to SP 800-56Ar3 Sec. 5.6.2.3.1
Vendor affirmed	CKG	IG D.12	FFC (DH)	3072 bits	Generation of DH key pairs (static and ephemeral key pairs) according to SP 800-133r2 Sec. 5.2. W.r.t. SP 800-133r2 Sec. 4, no XOR is used.
Vendor affirmed	CKG	IG D.12	AES	128 bits	Generation of the storage extension key during module initialization. W.r.t. SP 800-133r2 Sec. 4, no XOR is used.

Table 3: Cryptographic algorithms

The following algorithms listed in the CAVP certificates referenced above are not used by the cryptographic module:

- AES-ECB of #C667 and #A887,
- DSA KeyGen (FIPS186-4) of #A886 (key generation for the KAS is done with safe primes).

Note regarding AES-CTR: In case of #A887, CAVP testing for AES-CTR was not available due to the way the counter is constructed and AES-ECB was tested instead. The module uses AES-CTR for user data encryption/decryption.

Note regarding KAS-SSC: Testing of SP800-56A in #C666 is used for vendor affirmation of SP800-56Ar3 following IG D.1-Rev3.

By verifying that the firmware version, identified using the 'Get Version' service, matches each of the validated firmware components versions listed in section 1, the operator can be assured that the module is running in the Approved mode. A SHA-256 hash value is included in the version information for unambiguous identification of the firmware of the module. Furthermore, no bypass mode and no maintenance mode are implemented in the module.

The following table identifies cryptographic algorithms implemented in the embedded module #2628 used by the cryptographic module.

CAVP Cert	Algorithm	Standard(s)	Mode / Method	Key Lengths, Curves or Moduli	Use
#455	DRBG	SP 800-90A	CTR_DRBG	256 bits of strength	Seeding of the cryptographic module's DRBG (see *Table 3*).

Table 4: Cryptographic algorithms of the embedded module #2628 used by the cryptographic module

The embedded module #2628 implements an NDRNG which is a non-approved function but allowed in the approved mode of operation. It is used to seed the DRBG of the embedded module. Besides that, the cryptographic module performs additional self-tests on the NDRNG output.

2.4.1 How to Operate the Module in FIPS Approved Mode

The module is operated in its Approved mode of operation, if instructions as given in section 13 are regarded, see:

13.1 Installation, Initialization and Startup
13.2 General Tamper Seal Placement and Instructions
13.3 Types of Security Seals
13.4 Security Seal Application Instruction
13.5 Periodical Inspection

3 Module Ports and Interfaces

The Module's physical interfaces (Figure 7) are the traces that cross the perimeter of the physical Cryptographic Boundary. The following logical interfaces are defined according to FIPS 140-2:

- Data input interface: receiving plaintext data from the local user or receive encrypted data from the far-end module via optical interfaces.
- Data output interface: send decrypted data to the local user or send encrypted data to the far-end module via optical interfaces.
- Control input interface: send control information to the module via backplane interface.
- Control input/output interface: A logical optical interface is used for key agreement and synchronization.
- Status output interface: get status information by management interface via backplane or by observing the LEDs in the front panel.
- Power input interface via backplane and output interface for SFP connector.

4 Roles, Service and Authentication

Crypto Officer is connected to the module via the backplane (using an NCU as input/output device). The User of the module (i.e. a remote module of the same type) is connected via optical link, using in-band channels for communication. The module also provides a couple of services without authentication and assuming Crypto Officer or User role.

The module supports concurrent operators only in terms of the Crypto Officer and the User (i.e. remote module) using the module at the same time, but both using disjoint sets of services over backplane or optical link, respectively.

4.1 Identification and Authentication Policy

The module supports two distinct roles with the following authentication:

Role	Type of Authentication	Authentication Data / CSP
User (U)	Role-based authentication with Pairing Token	Pairing token(s) (static DH Key)
Crypto- Officer (CO)	Role-based authentication with password	Crypto Officer password

Table 5: Roles and required encryption identification and authentication

A complete description of all the management and configuration capabilities can be found in the User Documentation.

4.2 Authentication Strength

Authentication	Authentication Data/Strength
Role based authentication with password	Minimum password length is 10 characters. Assuming random usage of 26 lower case letters, 26 upper case letters and 10 decimal digits, this makes a total of (26 + 26 + 10)^10 password combinations. After 3 failed password attempts, the CO account is locked for 10 minutes. In one minute, therefore only three attempts are possible. The probability of successfully authenticating to the module within one minute is 3/(26 + 26 + 10)^10, which is less than one in 100,000.
Role based authentication with Pairing token	Pairing token length is at least 3072 bit, this defines a strength of 128 bit at least. The probability for a successful random authentication attempt is therefore 1/2^128. After three failed attempts, the key agreement is locked and must be enabled by the CO. In one minute, therefore only three attempts are possible. The probability of successfully authenticating to the module within one minute is 3/(2^128), which is less than one in 100,000.

Table 6: Strength of authentication mechanisms

4.3 Authenticated Services

The services for authorized operators (Crypto Officer (CO); User (U)) are listed below with access and use (r = read; w=write; x= execute) of CSPs. CSPs are erased on tamper detection, on zeroization command, on removal of module (further referred as 'erase of CSPs')

Service	Role	Description	Cryptographic Keys and CSPs	Type(s) of Access
Initial setup of module	CO	Set initial Crypto Officer password and set default crypto parameters Need: CO password Modify: CO password stored as SHA-256 protected in security chip	CO password	(w/x)
Start pairing	CO	Delete old pairing token and generate new pairing token Need: CO password Modify: local pairing token stored as DH private key protected in security chip	CO password pairing token	(w/x)
Accept fingerprint	CO	Establish pairing token Need: CO password stored as DH public key protected in security chip	CO password pairing token	(w/x)

Change CO password	CO	Change Crypto Officer password Need: CO password Change: CO password stored as SHA-256 protected in security chip	CO password	(w/x)
Allow firmware update	CO	Allow firmware update and set expected target revision.	CO password allow update target revision	(w/x)
Activate firmware update	CO	Activate new firmware revision located on standby image.	CO password	(x) (=new firmware version)
Cold start	CO	Cold start with current firmware image Required: Crypto Officer password	CO password	(x)
Configure session-key lifetime	CO	Established session-keys may be used for a limited time, even if key-agreement processes has failed.	CO password Key-lifetime	(r/w/x)
Initiate self-test	CO	Initiated Self-Test	CO password as defined in Self-test section 8	(x)
Reset key establishment failure counter	CO	Reset Counter	CO password Key establishment failure counter	(w/x)
Reset to factory-default ("Zeroize")	CO	Set module to well-defined initial state. Clear stored passwords (force zeroization)	CO password, all CSPs, all crypto parameters	(w/x)
key-establishment	U	Do key-establishment	Pairing token Session keys RBG	(r/w/x)
Link encrypt/ decrypt	U	encrypt/decrypt data	Session keys	(r/w/x)

Table 7: Roles and services authenticated

N.B. Firmware update is a two-step process. First, the new firmware is loaded into so-called standby image, i.e. the loading is performed, though the new firmware is not activated yet (even after a reset or power-cycle of the module). Only after the second step, in which the new firmware is explicitly activated by the CO, the former standby image becomes the active image (executed during subsequent power-ons of 9TCE). This allows pre-distribution of firmware updates to several copies of 9TCE, while cryptographic service is not affected at that time. The new firmware is then activated everywhere and all copies of 9TCE are restarted, ideally at the same time, to minimize downtime of the cryptographic services. In case of a firmware update performed, the resulting new configuration may no longer be validated (unless the 9TCE has been (re-) validated with new firmware version before).

4.4 Unauthenticated Services

The module provides a limited number of services for which the Crypto Officer or User is not required:

Service	Description	Input	Output
Self Test	Self-Test without command invocation (e.g. Power-On)	None	Status output
Status LED (Show Status)	Show Status LED without command invocation	None	Status information about the state of the encryption service and the self-test results.

Service	Description	Input	Output
Get Status (Show Status)	Get actual status information (e.g. serial number, HW revision, FW version and checksum, tamper, battery state, error state,)	Command Parameter	Response Actual status information
Send notification (Show Status)	Send notification to NCU	Event	Event information
Copy firmware	Copy firmware image to inactive FW memory of module ("standby image")	FW Image and Signature	Status of successful copy to module
Validate new firmware	Validate firmware approved signature	FW and signature Public keys running FW	Accept new FW or delete new FW image.

Table 8: Roles and services unauthenticated

5 Operational Environment

The FIPS 140-2 section 6 'Operational Environment requirements' are not applicable, because the module does not contain a modifiable operational environment.

To load new firmware image into the module, a firmware load test according to FIPS 140-2 is done. This requires the verification of a digital signature.

6 Cryptographic Key Management

The module uses a FIPS-Approved SP 800-90Ar1 CTR_DRBG to generate cryptographic FFC key pairs according to NIST SP 800-56Ar3. The randomness source used, implemented in the cryptographic module "StarSign Crypto-USB Token S powered by Sm@rtCafé Expert 7.0 Secure Element" by Giesecke+Devrient Mobile Security GmbH (referred to as "embedded module" in this SP), is an approved DRBG (compare CMVP cert. #2628 and DRBG cert. #455).

The 9TCE key management mechanisms, random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization is shown in the following section. Secrets and private key material (CSP) as well as public security parameters (PSPs) managed by the module will be zeroized as described in the following table:

CSP	CSP Type	Generation / Input	Output	Storage Location	Zeroization	Usage
CO Password	Password	CO / NCU	Never exits the module	Tamper protected in security chip as SHA-256 hash	Zeroization when tampered and per command.	Authenticate Crypto Officer Services
Storage extension key	128-bit AES key	Generation at initialization	Never exits the module	Tamper protected in security chip	Zeroization when tampered and per command.	128-bit key for access to nonvolatile secure storage in internal module and AES-ECB encryption of material stored in that module used for R/W of security chip data

Pairing token DH private static key (stored in security chip)	3072-bit DH key	The module's static key is generated internally req. by CO	Never exits the module	Tamper protected in security chip	Zeroization when tampered and per command.	Establishment of AES session key, Authentication
Pairing token DH private static key (stored in internal module)	3072-bit DH key	The module's static key is generated internally req. by CO	Never exits the module	Internal module (encrypted with Storage extension key)	Tamper protected by automated zeroization of the storage-extension key in the security chip. Zeroization per command.	Establishment of AES session key, Authentication
DH ephemeral private key	3072-bit DH key	The module's private key is generated internally	Never exits the module	RAM µCM	After key agreement.	Establishment of AES session key
Shared secret	Share secret as used in key agreement according to SP 800-56Ar3	Intermediate result of key-agreement process	Never exits the module	RAM µCM	After key agreement.	Establishment of AES session key
HMAC key	HMAC 160-bit key used in key confirmation according to SP 800-56Ar3	Intermediate result of key-agreement process	Never exits the module	RAM µCM	After key agreement.	Establishment of AES session key
AES key (and IV)	256-bit AES key (96-bit IV)	Result of key agreement process	Never exits the module	RAM µCM until send to FPGA	Zeroized in RAM µCM after the key was written to the FPGA. Tamper detection, every new key in FPGA or per command.	Session-key for encrypting user data
CTR_DRBG state	V and key values acc. to SP800-90Ar1, 256 bits each	CTR_DRBG state values as seeded and updated during DRBG usage	Internally used for DH private key generation using the CTR_DRBG. Do not exit the module.	µCm	Power cycle	Generate private DH keys. (for 1 of 4 ports) and Random delay values.
DRBG output/ CTR_DRBG seed	Seed, 384 bits	CTR_DRBG is seeded using output of DRBG of embedded module	Seed does not exit the module	Hardware (cert #2628)	Firmware (DRBG cert #2628)	DRBG of embedded module (DRBG cert. #455) used as seed source for CTR_DRBG
Firmware	SHA-256/ RSA-PSS-4096 signature	Generated by ADVA during firmware generation. Sent to module by NCU	SHA 256 exits the module for verification	Flash memory	Firmware update delete old image	Firmware update
PSP	**PSP Type**	**Generation / Input**	**Output**	**Storage Location**	**Zeroization**	**Usage**
Pairing token DH static public key (stored in security chip)	3072-bit DH key	The module's public key is generated internally	Public static key exits the module in key-establishment process	Security chip	Tamper protected in HW chip. Zeroization when tampered and per command.	Establish session key authentication

Pairing token DH static public key (stored in internal module)	3072-bit DH key	The module's public key is generated internally	Public static key exits the module in key-establishment process	Internal module (encrypted with Storage extension key)	Tamper protected by automated zeroization of the storage-extension key in the security chip. Zeroization per command.	Establish session key authentication
DH ephemeral public key	3072-bit DH key	The module's public key is generated internally	Public key exit the module in key-establishment process	RAM µCM send to far end µCM	After key agreement overwritten with zero.	Establish session key agreement
DH static public key of external device	3072-bit DH key	The public key is received as part of the key establishment process.	No output. Only the key fingerprint is sent to the management system for the pairing process.	Internal module (encrypted with Storage extension key)	Tamper protected by automated zeroization of the storage-extension key in the security chip. Zeroization per command. Zeroization when starting new pairing process.	Establish session key authentication
DH ephemeral public key of external device	3072-bit DH key	The public key is generated as part of the key establishment process.	No output.	RAM µCM	Zeroized after each key-agreement.	Establish session key authentication
Validation keys for new firmware	Set of public 4096-bit RSA keys	Generated by ADVA before firmware signature	Retrievable, no secret, but protected by digital signature	current/new firmware image	Never, but may be revoked by new firmware image	Firmware update, delete old image

Table 9: Cryptographic key, CSP and PSP management

N.B. The public and private static DH key is either stored in the security chip in plaintext or in encrypted form in the internal module. For the latter case, the storage extension key is used for key encryption. This storage extension key is stored in the security chip in plaintext. Whenever the security chip detects tampering, all keys in the security chip are zeroized. This storage extension is used in case multiple communication links are established (muxponder).

N.B. In the table above, "CTR_DRBG" denotes the deterministic random bit generator implemented in 9TCE firmware, whereas "DRBG" in the table above denotes the deterministic random bit generator implemented in the embedded module. The seed and state values of the DRBG of the embedded module have not been listed above, as these were CSPs already regarded during validation of the embedded module (compare cert. #2628 and corresponding security policy).

N.B. In case of a firmware update performed, the resulting new configuration may no longer be validated (unless the 9TCE has been (re-) validated with new firmware version before).

7 EMI/EMC

The Module is EMV Class A (business) compliant to the EMI/EMC requirements 47 CFR Part 15 Subpart B (FCC).

8 Self-Tests

The 9TCE performs power-up and conditional self-tests as required for FIPS 140-2 for verification of the integrity of firmware and operation of the implemented FIPS approved algorithms. The same self-tests can also be executed on demand.

Conditional self-tests run automatically when an applicable security function or operation is used.

8.1 Power-On or on Demand Self-Tests

Power-on self-tests run automatically after the device powers up with no further input or action of an operator. The module inhibits all data outputs while is in the self-test state.
The module enter approved mode only when all self-tests are successfully passed otherwise the module enters the error state.
The module uses cryptographic algorithm known-answer tests (KAT) to test for each FIPS 140-2-approved cryptographic functions (encryption, decryption, authentication, and random number generation) implemented on the module.

Function tested	Used for	Self-Test	State when fail
AES-ECB encryption / decryption on microcontroller (uCM) #C666 / #A886	Pseudo random number generation Data encryption and decryption in ECB mode for secure storage of CSPs	Known answer test	Error
AES-ECB encryption on FPGA #C667 / #A887	Data encryption in CTR mode	Known answer test	Error
DRBG of embedded module #455	Random number generation	Power-on self-test as implemented in embedded module (validated under CMVP cert. #2628), SP 800-90B test, Chi-square test	Error
CTR_DRBG #C666 / #A886	Random number generation	SP .800-90Ar1 health tests (KAT for instantiate, reseed, and generate functions), Chi-square test	Error
SHA-256 hash on uCM #C666 / #A886	Password hash generation Digital signature on FW Image	Known answer test	Error
SHA-512 hash on uCM #C666 / #A886	Key-derivation function	Known answer test	Error
HMAC-SHA-256 #C666 / #A886	Key-confirmation	Known answer test	Error
DH #C666 / #A886	Used for key agreement	Known answer test per IG D.8: Shared Secret Computation KAT -> FPGA expt mod KAT	Error

		Key Derivation Function (KDF) KAT -> SHA512 KAT	
RSA-3072 #C666 / #A886	Used for firmware signature and verification	Known answer test	Error
Firmware	FW Checksum CRC 32	Known answer test	Error

Table 10: Power-up self-tests

8.2 Conditional Self-Tests

The module implements the following conditional self-tests.

Function	Used for	Test	State when fail	Test is triggered...
Generate static or ephemeral DH key pair (Safe Primes Key Generation) #A886	Key-agreement	Full public-key validation (Safe Primes Key Verification)	Error	For each new generated static or ephemeral key pair
Generate static DH key pair #A886	Key agreement	Perform shared secret computation with a temporary, randomly selected key pair and verify common result	Retry	For each new generated static key pair
Received static or ephemeral DH public key #A886	Key-agreement	Full public-key validation (Safe Primes Key Verification) Check failed three times	>= 3 then Limited encryption Retry (wait for next scheduled key agreement)	For each new public DH key received
Key confirmation #C666 / #A886	Key agreement	HMAC check failed three times	>= 3 then Limited encryption Retry (wait for next scheduled key agreement)	For each key-agreement
DRBG of embedded module #455	Random number generation	Self-test as implemented in embedded module (validated under CMVP cert. #2628), SP 800-90B test, Chi-square test	Error and mitigation to Limited encryption	Internally in the embedded module (#2628)

Function	Used for	Test	State when fail	Test is triggered...
CTR_DRBG #C666 / #A886	Random number generation	SP 800-90Ar1 health tests, Chi-square test	Error and mitigation to Limited encryption	For each new generated random number
CSPs storage in secure IC	Authentication	CRC checksum verification	Error	When CSPs are stored in the secure IC
Firmware Signature #C666 / #A886	Firmware update signature verification	Firmware load test (RSA 4096 signature verification)	Stay in current image	When the software/firmware update functionality is requested.

Table 11: Conditional tests

N.B. In case of a firmware update performed, the resulting new configuration may no longer be validated (unless the 9TCE has been (re-) validated with new firmware version before).

8.3 Self-Test Failure Handling

On power-on or at any time on demand a self-test can be executed. If this test fails, the module goes into "Error State" and disables cryptographic functions with CSPs, only status information is available.

On failed conditional tests the module may enter either "Error State" or "Limited encryption", depending on the cause of failure (see table 10 above). In case of 'Limited encryption', encrypted data transmission continues until the configured session-key lifetime is reached.

In error state the module LED illuminate red. Forced self-test on demand or power-cycle may return the module to normal operation. State changes are logged.

9 Access Control Policy

An access control policy to the module shall be established by the CO in a manner, to prevent unauthorized access to information and services

10 Physical Security Policy

10.1 Physical Security Mechanisms

It is assumed that the cryptographic module, i.e. the 9TCE mounted in one of the shelves as listed in table 1, is used in a protected environment, where an attacker has only limited time and equipment (FIPS 140-2, security level 2).

The Crypto Officer is responsible for secure configuration, management and changes for setting up the module to the FIPS Approved mode.

Physical Security Mechanisms	Recommended Frequency of Inspection / Test	Inspection / Test Guidance Details
Seals protecting against opening of the metal shield without leaving visible damages.	First after initial installation and seal placement. Later every time when the module was potentially accessed by unauthorized people, e.g. during cleaning or maintenance.	Visual inspection by the CO of entire metal shield and all seals for damages and signs of removal or tampering. Includes verification of the seal serial numbers.

Table 12: Inspection/testing of physical security mechanisms

11 Security Rules

Summarized, the 9TCE was designed to enforce the following security rules:

- The module grants no access to any cryptographic services without successful (role-based) operator authentication.
- New authentication to the module is required after a power-cycle.
- The module provides two distinct operator roles. The role 'User' (i.e., a remote module of the same type) is authenticated via a Pairing Token. The role 'User' shall use the approved cryptographic function of the module.
- The role 'Crypto Officer' is authenticated via a password. Only the 'Crypto Officer' is allowed to change security-related values.
- The module performs power-on and conditional self-tests. The Crypto Officer is able to start/restart self-tests on demand.
- Data output and status output never contain any CSPs or sensitive data. Data output is inhibited during self-test, zeroization and in error states.
- The module does not support manual key entry.
- The module does not support a maintenance role/interface.
- The module does not implement a bypass capability.

12 Mitigation of other Attacks Policy

The module implements the following mechanisms to mitigate attacks beyond the requirements of FIPS 140-2 as stated in section 2.3.

Other Attack	Mitigation Mechanism	Specific Limitations
Removal of 9TCE encryption card from the shelf	A security chip with non-imprinting key memory with high-speed erase is used for storing critical security parameters. After a tamper event, this memory is actively erased, using a battery. One tamper input of the security chip is connected to the backplane of the FSP 3000 shelf. When the module is removed from the shelf, the security chip is actively erased (independently of the shelf's power-supply).	None

Other Attack	Mitigation Mechanism	Specific Limitations
Opening the 9TCE encryption card case	A tamper input of the security chip is connected to the cover of the encryption card with a mechanical switch, which deletes the security parameters when the cover is opened (independently of the shelf's power-supply).	None
Out-of-range operational conditions	The security chip is programmed to delete the security parameters on abnormal temperature (less than -26°C or more than +90°C) or abnormal voltage or oscillator operation.	None
Timing analysis on DH	To avoid leakage of potential side-channel information due to key-dependent calculation times in DH, each modExp calculation is followed by a random delay time in the same range as a complete modExp calculation takes.	None

Table 13: Mitigation of other attacks

13 Secure Operation

The following sections describe how to place and keep the module in FIPS-Approved mode of operation.

13.1 Installation, Initialization and Startup

After receiving the module, the Crypto Officer shall first inspect the delivered module:

- Check packaging and inspect the shipping box
- The transport seals must not be damaged
- Are there scratches or deformations on the metal case?
- Have tamper evident seal been provided, too?
- Order SEAL/FIPS-KIT-SHELF for sealing the shelf with order number in table1.

The ESD bag or the transport box of the encryption card is sealed so that the customer can check for modifications.

Figure 16: Sealed ESD bag

The hardware version of 9TCE received has to match the validated hardware version according to table 1. The 9TCE must be inserted in an approved configuration of FSP 3000 shelf, also as listed in table 1

Seals have to be applied as stated in sections 13.2ff. hereinafter.

After powering on the shelf including 9TCE, automatic power up self-tests are executed without any operator actions necessary.

The Crypto Officer must have a valid admin, provision or crypto account on the Network Control Unit (NCU), which acts as an input/output device for the 9TCE. Either a web browser or an SSH client must be used to login to the NCU.

Check firmware version (see User Documentation how to use the 'Get Version' service). If the firmware version should not match the validated firmware version as stated in table 1, install a validated firmware version before proceeding.

The Crypto Officer must select their module and must set the Crypto Officer password. The default Crypto Officer Password and the complexity rules can be found in the user manual. The new Crypto Officer password must differ from the default password.

For the following steps should be done for up to four ports, an optical connection to the far-end module is required (e.g. cables must be plugged in the right ports, optical wavelength and protocol must have been provisioned. See details in user guides).

In the next step the Crypto Officer must start the pairing process on the local and remote encryption cards. The button is shown in the NCU user interface. The action must be confirmed with the Crypto Officer's password. The fingerprint of the new local authentication token (local static DH public key) is shown.

When the optical connection is available, near-end and far-end module communicate via an in-band channel. The NCU user interface displays the fingerprint of the far-end authentication token (remote static DH public key) beside the fingerprint of the local module.

The NCU user interface of the far-end side displays the same fingerprints in the opposite order.
When the fingerprints of both sides are correct, the Crypto Officer accepts the fingerprints by pressing the accept buttons on both sides. These decisions are stored persistently and must be confirmed with the Crypto Officer's passwords on both sides.

When both sides have accepted their authentication tokens, the automatic key agreement starts and an encrypted traffic will start soon.

Before the first session key has been established, also during self-test, error state or after zeroization, any data output is inhibited.

The Crypto Officer may change other security parameter settings but the default settings are secure.

Place the seals as described below.

13.2 General Tamper Seal Placement and Instructions

The Crypto Officer is responsible for

- Securing and having control at all times of any unused seals

- Direct control and observation of any changes to the module such as reconfigurations where the tamper-evident seals or security appliances are removed or installed to ensure the security of the module is maintained during such changes and the module is returned to a FIPS Approved state.

13.3 Types of Security Seals

13.3.1 Shelf 9 HU Placement Seals

Multipurpose security seal label for application at different positions on chassis' and modules.

Figure 17: Generic security seal label

13.3.2 Security Seal Label CFP

Special security seal label for application at installed CFPs at the front plate of module.

Figure 18: Security seal label CFP

13.3.3 Security Twist Wire Seal

Security seal which consists of a plastic body and a wire for application on module and pluggable interfaces which are designed with cross-holes and other facilities for feeding-through of wire in a way which prevents removal from hosting entity if the seal is installed.

Figure 19: Security plastic wire coil-in seal package

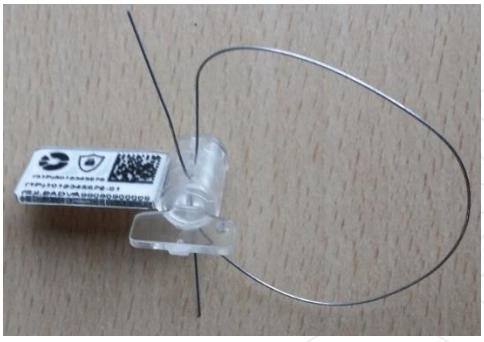

Figure 20: Security plastic wire coil-in seal

13.4 Security Seal Application Instruction

FIPS compliant operation requires closing and sealing of chassis and modules of FSP 3000.
The following seals must be used for FIPS compliant sealing.

The following FIPS seals are part of the 9TCE delivery:

- 1013700030-01 SEAL/FIPS-GENERAL seal label
- 1013700032-01 SEAL/FIPS-WIRE plastic wire coil-in seal

The SEAL/FIPS-KIT-SHELF must be ordered separately:

- BC00000738 SEAL/FIPS-GENERAL/5 it contains 5 x 1013700030-01 seals.

The seals are equipped with a tamper-evidence functionality. After applying each seal, any attempt to remove the seal causes visible damage of the seal. Each seal is serialized. The serial number is available on the seal as text and as 2D code (DataMatrix). The 2D code is readable with most contemporary bar code scanners and by use of smartphone apps. Each seal comes with a counterfoil (or stub) for documentation purpose.

After applying a seal, the Crypto Officer have to place the counterfoil/stub in their documentation for registration of the serial numbers of the applied seals. The registered serial numbers of the seals in Crypto Officer's documentation can be used for checking and identifying seals on the products during Crypto Officer's audit of products in FIPS compliant mode of operation.

13.4.1 Security Seal Labels

For all seal label applications, the Crypto Officer shall observe the following instructions:

- Handle the seals with care.
- Do not touch the adhesive side.
- Before applying a 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. Any re-seating of a seal label may cause tamper evidence.
- Place the seal on the application surface by use of transfer foil and apply firm pressure to ensure adhesion
- Remove transfer foil gently and press the seal to application surface again

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

13.4.2 Security Twist-Wire Seals

These seals shall be applied to the different products as described in the following sections. The plastic wire coil-in seal consists of a plastic seal body, a metal wire. Attached to the seal body is a white label with a counterfoil/stub.

For all twist-wire seal applications, the Crypto Officer shall observe the following instructions:

- Handle the seals with care.
- Do not bend seal handle.
- Remove the unattached part of the white label including the counterfoil/stub (leaving the white label on the flag of seal body)
- Feed both ends of wire through the both parallel holes in the seal body until approx. 1 cm (approx. 1/2 inch) of the wire left the other side of the holes
- Twist the seal body handle gently clockwise until the wire is tightly coiled into the seal body

- Break away the seal handle finally

13.4.3 Shelf 1 HU Placement Seals SH1HU-HP/2DC and SH1HU-HP/E-TEMP/2DC

The figures in this section show the placement of four labels on the covers of the 1 SH1HU-HP/2DC and SH1HU-HP/E-TEMP/2DC shelves. It is crucial that labels are placed correctly, to make sure that a shelf also provides appropriate tamper evidence. Without proper placement of seals on a shelf, covers of the shelf may be partly dismounted without tamper evidence, resulting in undetectable physical access to the 9TCE card inside.

For FIPS compliant operation, the SH1HU-R/PF chassis has to be sealed with four seal labels of type

1013700030-01 SEAL/FIPS-GENERAL

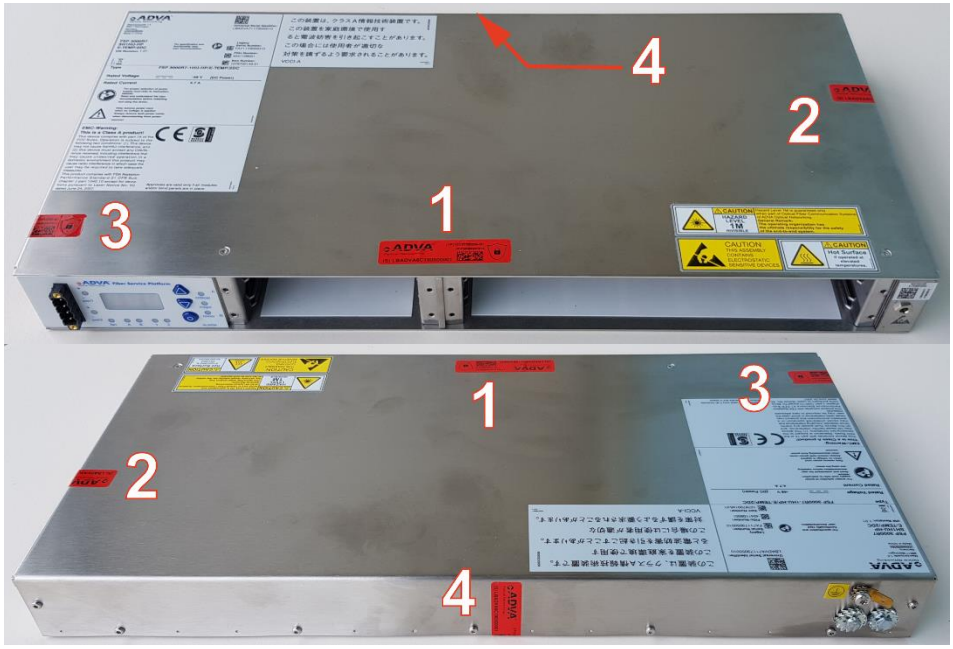

Figure 21: Placement of seals on shelf 1 HU, top views

Figure 22: Placement seals, shelf 1 HU, placement 1

One seal label must be placed at top cover covering the screw of module slot separation (and 'Guarantee void' label) (1).

Figure 23: Placement seals, shelf 1 HU, placement 2

One seal label must be placed at right upper edge at two fifth from right side, bridging from top plate to side plate avoiding the left side air outlet (2).

Figure 24: Placement seals, shelf 1 HU, placement 3

One seal label must be placed at left upper edge near the front, bridging from top plate to side plate between the fan opening and the pair of holes for fastening optional rack handles (3).

Figure 25: Placement seals, shelf 1 HU, placement 4

One seal label must be placed at the rear bottom edge, bridging from the rear plate to the bottom plate at a position to the side of the center rear screw toward the ground lugs (4).

13.4.4 Sealing of SH1HU-R/PF

The figures in this section show the placement of seals on the front and rear covers of the 1 SH1HU-R/PF shelf. It is crucial that labels are placed correctly, to make sure that a shelf also provides appropriate tamper evidence. Without proper placement of seals on a shelf, covers of the shelf may be partly dismounted without tamper evidence, resulting in undetectable physical access to the 9TCE card inside.

For FIPS compliant operation, the SH1HU-R/PF chassis has to be sealed with six seal labels of type

1013700030-01 SEAL/FIPS-GENERAL.

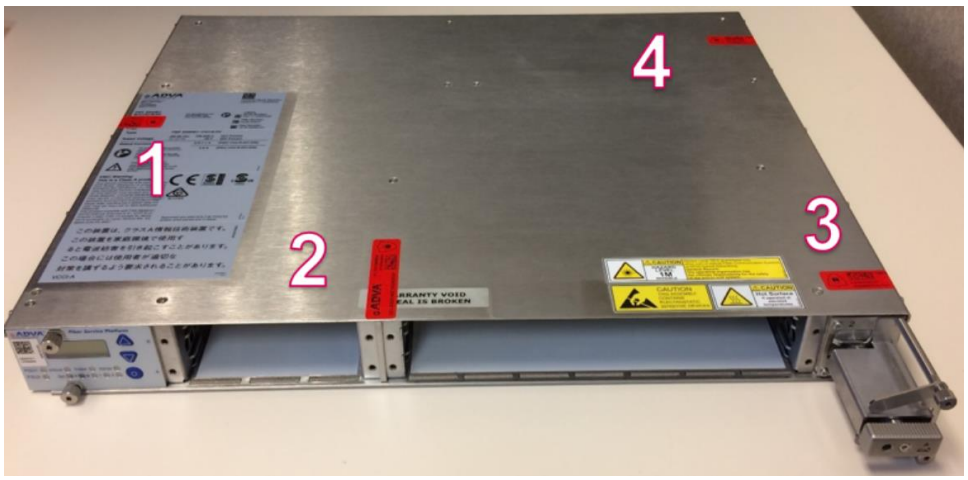

Figure 26: Placement of seals SH1HU-R/PF front-top view

One seal label must be placed at left upper edge in 2/5 from rear side bridging from top plate to side plate avoiding the left side air outlet (1).

One seal label must be placed at top cover next to front 2/5 from left covering the screw of module slot separation and the 'WARRANTY VOID' label orthogonally (2).

One seal label must be placed label at the top cover on the side opposite the power supply near the front. (3).

One seal label must be placed label at the top cover on the side opposite the power supply near the rear. (4).

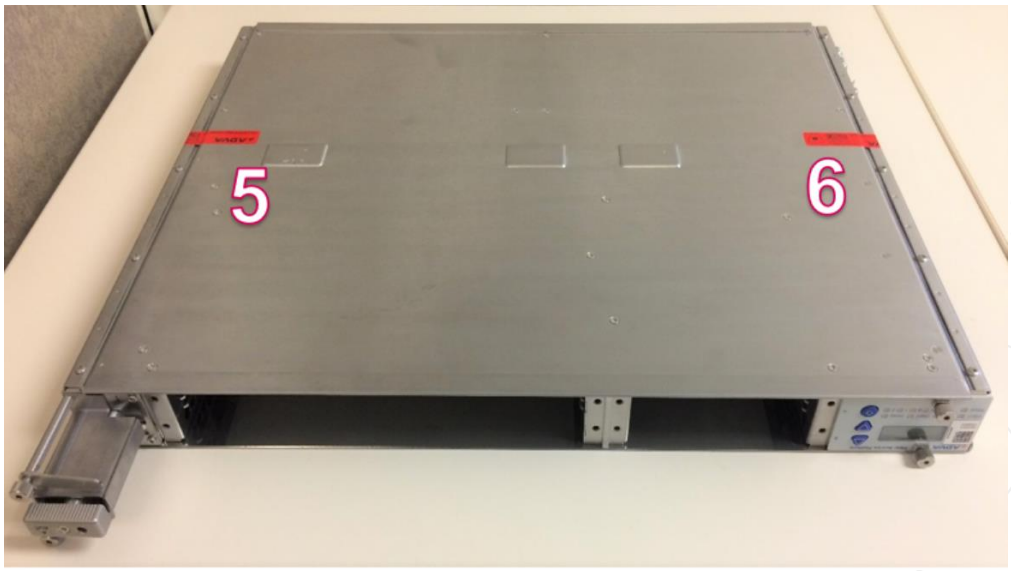

Figure 27: Placement of seals SH1HU-R/PF front-bottom

One seal label must be placed at right lower edge in 2/5 from rear side bridging from bottom plate to the left side plate avoiding the left side air outlet (5).

One seal label must be placed at left lower edge in 2/5 from rear side bridging from bottom plate to the right-side plate avoiding the left side air outlet (6).

Figure 28: Placement of seals SH1HU-R/PF left side positions

Figure 29: Placement of seals SH1HU-R/PF right side positions

Figure 30: Placement of seal SH1HU-R/PF right side position

13.4.5 Sealing of SH7HU(-R)

The figures in this section show the placement of seals on the front and rear covers of the 7HU module configuration. It is crucial that labels are placed correctly, to make sure that a shelf also provides appropriate tamper evidence. Without proper placement of seals on a shelf, covers of the shelf may be partly dismounted without tamper evidence, resulting in undetectable physical access to the 9TCE card inside.

For FIPS compliant operation, the SH7HU chassis and the SH7HU-R chassis have to be sealed seal labels of type

1013700030-01	SEAL/FIPS-GENERAL

Figure 31: Placement of seal SH7HU rear side

Place one seal label at left of the screw of removable rear cover bridging the top plate and the rear side cover lid (1),

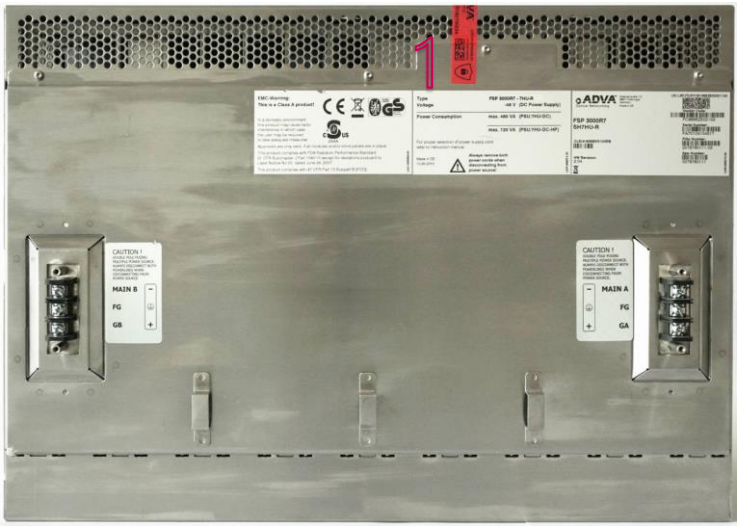

Figure 32: Placement of seal SH7HU (-R) rear side

Place one seal label at left of the screw of removable rear cover bridging the top plate and the rear side cover lid (1).

13.4.6 Shelf 9 HU Placement Seals

The figures in this section show the placement of seals on the front and rear covers of the 9 HU module configuration. It is crucial that labels are placed correctly, to make sure that a shelf also provides appropriate tamper evidence. Without proper placement of seals on a shelf, covers of the shelf may be partly dismounted without tamper evidence, resulting in undetectable physical access to the 9TCE card inside.

For FIPS compliant operation, the SH9HU chassis has to be sealed with seal labels of type

1013700030-01 SEAL/FIPS-GENERAL.

Use four seal labels for sealing as shown below. (Note: Pictures illustrate seal positions only)

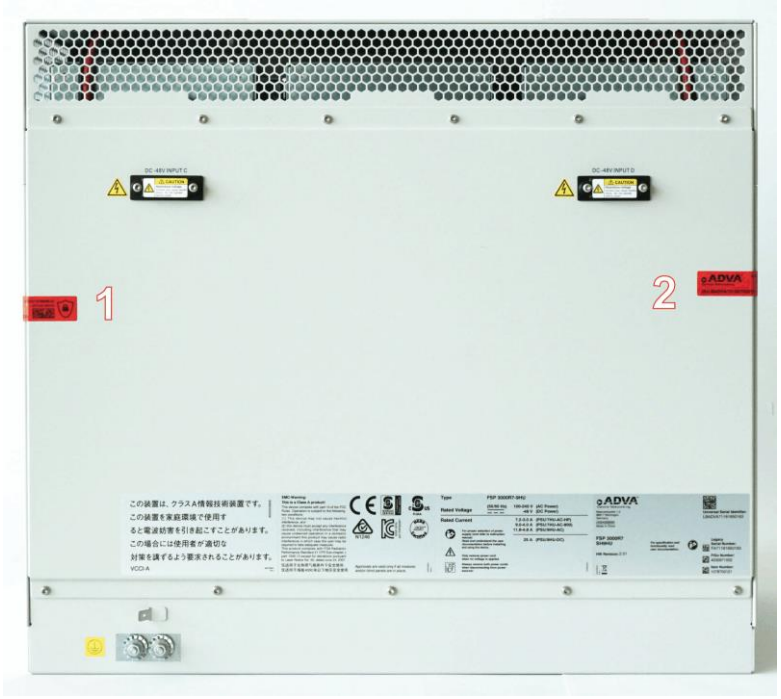

Figure 33: Seals rear side shelf 9HU

Place one seal label at left edge in 2/3 of height of removable rear cover (1).

Place one seal label at right edge in 2/3 of height of removable rear cover (2).

Figure 34: Seals cover rear edge shelf 9 HU

Place one seal label at rear edge of chassis top covering the second screw (counted from left side edge) (3).

Place one seal label at rear edge of chassis top covering the second screw (counted from right side edge) (4).

13.4.7 Sealing of 9TCE-PCN-10GU+AES10G-F

For FIPS compliant operation, the 9TCE-PCN-10GU+AES10G-F module has to be sealed with one seal of type

1013700032-01 SEAL/FIPS-WIRE plastic wire coil-in seal

Figure 35: Placement of twist seal in SH1HU configuration

Figure 36: Placement of twist seal in SH7HU and SH9HU configuration

The twist wire seal must be placed as shown above.
The wire must be fed through the holes of the four screws and through the two holes of the seal body.
The wire must be coiled in completely and the handle of the seal must be removed.

13.5 Periodical Inspection

ADVA recommends to inspect the system visually in a periodical manner to secure no injury or tampering. Also inspect the log files, especially check unsuccessful key agreements or login attempts.

14 Definitions and Acronyms

Term	Definition
AES	Advanced Encryption Standard
CTR	Counter Mode (mode of AES encryption)
CSP	Critical Security Parameter
CFP	C form-factor pluggable (Optical Transceiver)
DH	Diffie-Hellman (key-establishment algorithm)
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book (mode of AES encryption)
FCC	Federal Communications Commission independent agency of the United States government
FFC	Finite Field Cryptography (used e.g. for Diffie-Hellman key-establishment)
FPGA	Field Programmable Gate Array
FIPS	Federal Information Processing Standard
IV	Initialization Vector
KDF	Key Derivation Function
NCU	Network Control Unit
NIST	National Institute of Standards and Technology
PCB	Print Circuit Board
RBG	Random Bit Generator
RSA	Rivest, Shamir, Adleman (public-key algorithm for digital signatures)
SHA	Secure Hash Algorithm
uCM	micro Controller Module

Table 14: Definition and acronyms