Adva NETWORK SECURITY

Data Sheet

# 9TCE-PCN-10GU+AES10G

Muxponder/quad-transponder with certified Layer 1 encryption

## Benefits

- **Built-in cryptographic functions**
  Featuring AES256 encryption, pair-wise authentication using X.509 certificates, key interface for QKD devices and Common Criteria certified operating system
- **9TCE-PCN-16GU+AES100G certification variants**
  -F: FIPS 140-2 Level 2 homologated variant
  -G: BSI/EU/NATO-approved variant for classified data up to VS-NfD/restreint/restricted
- **Tamper-evident case**
  Hardware designed to avoid any unauthorized access or manipulation of security-sensitive components
- **High-density design**
  10Gbit/s muxponder or quad-transponder with four independent transponders in just a 1-slot module
- **Multi-protocol ports**
  10 multi-protocol ports that can work as client or network ports in accordance with various operation modes
- **Comprehensive monitoring capabilities**
  Multiple fault and performance monitoring capabilities on the client and the network ports
- **Designed for Adtran FSP 3000 platform**
  Extending widely applied open optical transport solution FSP 3000 with sophisticated ConnectGuard™ security features

## Overview

**The 9TCE-PCN-16GU+AES100G is a channel card that can work as a 10Gbit/s multiplexer or quad-transponder with four independent transponders in just one card.** With our robust and reliable ConnectGuard™ Layer 1 encryption technology, this module satisfies the most stringent security demands such as FIPS 140-2. It is also qualified by the German Federal Office for Information Security (BSI) for the transport of classified data up to VS-NfD level. The channel card is fully compatible with Adtran's FSP 3000 open optical transport platform.

Our 9TCE-PCN-16GU+AES100G is an enterprise-type TDM channel module with 10 interface cages that can serve as either client or network ports depending on the application (muxponder or transponder). Moreover, it implements cryptographic functions such as encryption, decryption and random number generation. The network interface data stream is encrypted/decrypted using the Advanced Encryption Standard (AES). Data encryption and the use of an endpoint authentication mechanism protect the network link between two communicating 9TCE-PCN-16GU+AES100G modules against man-in-the-middle attacks. Our ConnectGuard™ Layer 1 encryption technology satisfies the strictest security standards such as FIPS 140-2 (-F variant). What's more, it has achieved BSI approval for transport of classified data up to VS-NfD level (-G variant). This makes this terminal ideal for the transmission of sensitive information that must be protected from unauthorized access.

# 9TCE-PCN-10GU+AES10G

## High-level technical specifications

### General information

- Two operation modes:
  - 10G terminal multiplexer
  - 10G quad-transponder
- 1-slot module
- 10x SFP/SFP+ cages for client port or network port use
- Typical power consumption fully equipped: 25W/35W (muxponder/transponder)

### Muxponder mode

- Nine client ports (SFP/SFP+) and one network port (SFP+)
- Up to nine client services multiplexed/ demultiplexed onto/from one 10Gbit/s ITU-T wavelength (OTU2)
- Client protocols supported: STM-4/OC12, GbE, STM-16/OC48 and electrical Ethernet E10-1000T

### Transponder mode

- Up to four independent transponders per card, each one with one client port (SFP/SFP+) and one network port (SFP+)
- Client protocols supported: 8GFC, STM-64/OC192, 10GbE LAN, CE-LR, RoCE, OTU-2

### Environmental conditions

- Telcordia SR-3580 level 3 (NEBS), ETSI EN 300 019-1-3 Class 3.1 (9RU)/3.1e (7RU, 1RU)
- Operating temperature: +5°C to +40°C / -40°C to +65°C with 1RU E-Temp+ shelf
- 5% to 85% relative humidity (non-condensing)

### ConnectGuard™ encryption (standard variant)

- Encryption of payload according to AES-CTR with 256 bit key
- Diffie-Hellman 4096 bit key exchange every minute
- Protection against modification
- Far-end authentication via pairing or X.509
- Support of external key-exchange via QKD

### Security certifications (standard variant)

- Common Criteria (CC) certification (operating system level)

### ConnectGuard™ encryption (-G variant)

- Encryption of payload according to AES-GCM with 256 bit key
- Diffie-Hellman 4096 bit key exchange every minute
- Post quantum based key exchange (PQC)
- Protection against modification
- Far-end authentication

### Security certifications (-G variant)

- BSI approval for transport of classified data up to VS-NfD level (“BSI-VSA-10788”)
- Common Criteria (CC) certification (operating system level)

### ConnectGuard™ encryption (-F variant)

- Encryption of payload according to AES-CTR with 256 bit key
- Diffie-Hellman 3072 bit key exchange every minute
- Protection against modification
- Far-end authentication via pairing

### Security certifications (-F variant)

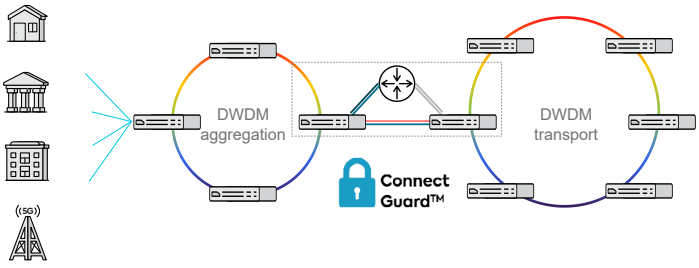
- FIPS 140-2 Level 2 certification
- Common Criteria (CC) certification (operating system level)

# Applications in your network

### Secure enterprise connectivity

- High-capacity transport of sensitive data over WDM metro network infrastructure
- Built-in Layer 1 encryption technology for robust protection of data in motion with 100% throughput and ultra-low latency
- Protocol-agnostic Layer 1 encryption protecting data at all layers in the network stack
- Post quantum based or external, quantum key distribution based key exchange
- Most robust and reliable Layer 1 encryption on the market:
  - BSI approval for the transport of classified data up to VS-NfD level (-G variant)
  - Adva Network Security is the only DWDM vendor that has achieved BSI approval
  - Common Criteria certification (operating system level)
  - FIPS 140-2 Level 2 certification (-F variant)

**Open optical transport network infrastructure from the optical edge to the core**




**Data center interconnect**