Data Sheet

10TCE-PCN-16GU+AES100G

100Gbit/s muxponder 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
- **10TCE-PCN-16GU+AES100G certification variants**
  -F: FIPS 140-2 Level 2 homologated variant
  -BSI: BSI/EU/NATO-approved variant for classified data up to VS-V/restreint/restricted
- **Tamper-evident case**
  Hardware designed to avoid any unauthorized access or manipulation of security-sensitive components
- **High-density design**
  Two-slot compact design enabling up to eight modules (7 modules with BSI variant) per 9RU shelf or one module per 1RU shelf
- **Multi-service support**
  Support of any combination of client services, only limited by the maximum aggregated bandwidth (100Gbit/s)
- **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 10TCE-PCN-16GU+AES100G is a channel card that can multiplex/demultiplex up to 10 client interface signals of up to 16Gbit/s services onto/from an ITU-T-compliant wavelength for transport over an optical network. 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-V level. The channel card is fully compatible with Adtran's FSP 3000 open optical transport platform.

Our 10TCE-PCN-16GU+AES100G is an enterprise-type TDM channel module with ten SFP+ interface cages on the client side and a single CFP interface cage on the network side. The 10TCE-PCN-16GU+AES100G implements cryptographic functions such as key exchange, encryption, decryption and random number generation. The aggregate 100Gbit/s data stream is encrypted/decrypted using the Advanced Encryption Standard (AES). Our low-latency implementation makes this card a preferred choice for data center interconnections. Data encryption and the use of an endpoint authentication mechanism protect the network link between two communicating 10TCE-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 level 2 (-F variant). What's more, it has achieved BSI approval for transport of classified data up to VS-V level (-BSI variant). This makes this module ideal for the transport of sensitive information that must be protected from unauthorized access.

10TCE-PCN-16GU+AES100G

High-level technical specifications

General information

- Terminal multiplexer
- 2-slot module
- Pluggable transceivers:
  - Up to 10x SFP+ client interfaces
  - 1x CFP network interface
- Typical power consumption with SFP+ and CFP: 90W/91W/96W for standard-, FIPS- and BSI-variant

Client data rates supported

- 4GFC, 5G IB, 8GFC, 10GFC, 16GFC, STM-64/OC-192, 10 GbE WAN PHY, 10GbE LAN PHY, CE-LR, RoCE, 40GbE (4x 10GbE) and 100GbE (10x 10GbE)
- Any combination of client services allowed (up to the max aggregated bandwidth)

Environmental conditions

- SH9RU shelf: Telcordia SR-3580 level 3 (NEBS), ETSI EN 300 019-1-3 Class 3.1 (9RU) or 3.1e (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)

Protection switching

- 1+1 unidirectional revertive and non-revertive switching
- 1+1 bidirectional revertive and non-revertive switching
- Switching times <50ms
- Automatic protection switching (APS) channel per sub-aggregate service for client channel card protection

ConnectGuard™ encryption (standard variant)

- Encryption of payload according to AES-CTR with 256 bit key
- Diffie-Hellman 2048 bit key exchange every minute
- Protection against modification
- Far-end authentication via PACE or X.509
- Support of external key-exchange via QKD

Security certifications (standard variant)

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

ConnectGuard™ encryption (-BSI 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 via pairing

Security certifications (-BSI variant)

- BSI approval for transport of classified data up to VS-V level (BSI-VSA-10786 / BSI-VSA-10678)
- 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)

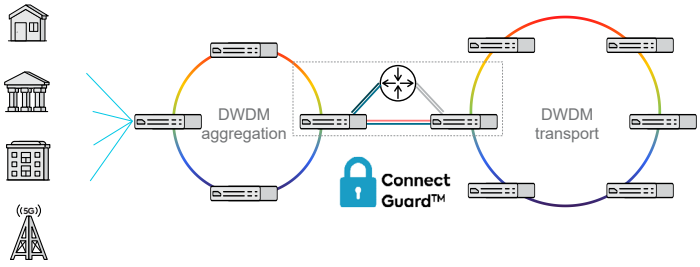
- FIPS 140-2 Level 2 certification
- Common Criteria (CC) certification (operating system level)

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
- Mutual authentication based on X.509 certificates
- Most robust and reliable Layer 1 encryption on the market:
  - BSI approval for the transport of classified data up to VS-V level (-BSI variant)
  - Adva Network Security is the only DWDM vendor that has achieved the 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