

4TCC-PCN-32GU+AES100G-G

BSI-approved Layer 1 encrypted transport of 32GFC client services

Benefits

- Built-in cryptographic functions**
 No need for additional equipment or software
- BSI approval; CC-certified**
 BSI-VSA-10847 approval for the transport of classified data up to "VS-NfD" level; Common Criteria (CC) certification (operating system level)
- 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 per 9RU shelf respectively one module per 1RU shelf
- FEC for network and client interfaces**
 32GFC clients implement the mandatory FEC required in the Fibre Channel specifications for 32GFC
- Comprehensive monitoring capabilities**
 Multiple client and network port fault monitoring (FM) and performance monitoring (PM) capabilities
- Designed for Adtran FSP 3000 platform**
 Extending widely applied open optical transport solution FSP 3000 with sophisticated ConnectGuard™ security features

Overview

The 4TCC-PCN-32GU+AES100G-G is a muxponder that provides encrypted transport of up to three 32GFC client services on a single wavelength. With our robust and reliable ConnectGuard™ Layer 1 encryption technology, the 4TCC-PCN-32GU+AES100G-G satisfies the most stringent security demands, including being qualified by the German Federal Office for Information Security (BSI) for the transport of classified data up to VS-NfD level ("BSI-VSA-10847"). The channel card is fully compatible with Adtran FSP 3000 open optical transport platform.

The 4TCC-PCN-32GU+AES100G-G is a 100Gbit/s TDM channel module (muxponder) supporting three 32GFC client interfaces using the independent lanes of a single quad small form-factor pluggable (QSFP28) interface cage, and one OTU4/OTU4V network interface using a single CFP interface cage. If necessary, a breakout cable terminating in multiple optical connectors, each supporting a single optical lane (such as an MPO-to-LC breakout cable), might be used to connect to any client equipment that does not offer 32GFC interfaces on QSFP ports. The network 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 4TCC-PCN-32GU+AES100G-G modules against man-in-the-middle attacks. Our ConnectGuard™ Layer 1 encryption technology satisfies the strictest security standards such as FIPS 140-2. What's more it has achieved BSI approval for transport of classified data up to VS-NfD level. This makes it ideal for the transmission of sensitive information that must be protected from unauthorized access.



4TCC-PCN-32GU+AES100G-G

High-level technical specifications

General information

- Terminal multiplexer supporting three 32GFC independent client services
- Two-slot module
- Embedded communication channel (ECC)
- Typical power consumption with transceivers: 75W

Client and network ports

- Client interface:
 - 1x standard-compliant QSFP28 supporting three standard 32GFC interfaces
- Network interface:
 - 1x standard-compliant CFP transceiver (grey or colored)
 - Support of breakout cables

Environmental

- 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)

FM and PM monitoring

- Client interface:
 - Physical layer (PHYS), physical coding sublayer (PCS)
- Network interface:
 - Physical layer (PHYS), OTU section layer, encryption layer, ODU path layer, TCM layer, FEC PMs

ConnectGuard™ encryption

- Encryption of payload in accordance to AES-GCM with 256bit key
- Diffie-Hellman 4096 key exchange every minute
- Protection against modification
- Far-end authentication

Security certifications

- BSI approval for transport of classified data up to VS-NfD level (BSI-VSA-10847)
- Common Criteria (operating system level)

Applications in your network

Secure SAN DCI 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
- Most robust and reliable Layer 1 encryption on the market:
 - BSI approval for the transport of classified data up to VS-NfD level (BSI-VSA-10847)
 - Common Criteria certification (operating system level)
 - Adva Network Security is the only DWDM vendor that has achieved the BSI approval

