Adva NETWORK SECURITY

Data Sheet

WCC-PCN-AES100GB

100Gbit/s 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
- **WCC-PCN-AES100GB 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
- **Compact footprint**
  Two-slot compact design enabling up to eight modules per 9RU shelf or one module per 1RU shelf
- **Multi-protocol support**
  The module supports 100GbE as well as OTN OTU-4 client services
- **Comprehensive monitoring capabilities**
  Fault and performance monitoring capabilities for both client as well as network interfaces
- **Designed for Adtran FSP 3000 platform**
  Extending widely applied open optical transport solution FSP 3000 with sophisticated ConnectGuard™ security features

Overview

The WCC-PCN-AES100GB is a DWDM transponder for the transport of encrypted 100GbE and OTU4 client services over optical networks. 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 WCC-PCN-AES100GB is a two-slot cryptographic WDM channel module with one 100Gbit/s client interface supporting QSFP28 pluggable transceivers and one 100Gbit/s network interface supporting CFP pluggable transceivers. The WCC-PCN-AES100GB implements cryptographic functions such as encryption, decryption, and random number generation. The aggregate 100Gbit/s 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 WCC-PCN-AES100GB 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 module ideal for the transport of sensitive information that must be protected from unauthorized access.

WCC-PCN-AES100GB

High-level technical specifications

General information

- 100Gbit/s transponder
- 2-slot module
- Pluggable transceivers
- Embedded control channels
- Typical power consumption including pluggable transceivers: 75W

Client and network ports

- Client port:
  - 1x QSFP28
  - Protocols supported: 100GbE and OTU4
- Network port:
  - 1x CFP network port
  - Tuneable DWDM interface

Environmental information

- SH9HU 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
- 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 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-10847”)
- 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)

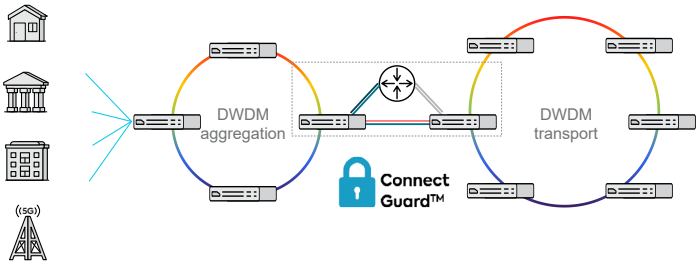
- FIPS 140-2 Level 2 certification
- Common Criteria (CC) certification (operating system level)

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