

WCC-PCN-AES100GB

100Gbit/s Transponder mit zertifizierter Layer 1 Verschlüsselung

Ihre Vorteile

- Integrierte Verschlüsselung**
 AES256-Verschlüsselung und paarweise Authentifizierung mit X.509-Zertifikaten, Schlüsselschnittstelle für QKD-Geräte und Common Criteria-zertifiziertes Betriebssystem
- WCC-PCN-AES100GB Zertifizierungsvarianten**
 -F: FIPS 140-2 Level 2 zugelassene Variante
 -G: BSI/EU/NATO-zugelassene Variante für Verschlusssachen bis VS-NfD/restreint/restricted
- Manipulationsgeschütztes Gehäuse**
 Hardwarefunktionen verhindern den unbefugten Zugriff auf oder die Manipulation von sicherheitsrelevanten Komponenten
- Kompaktes Design**
 Belegung von zwei Steckplätzen für bis zu acht Modulen pro 9HE-Baugruppenträger oder ein Modul im 1HE-Baugruppenträger
- Multi-Protokoll Unterstützung**
 Die Transponderkarte unterstützt anwendungsseitig eine 100GbE 100BASE-R und OTN OTU-4 Schnittstelle
- Umfassende Überwachungsfunktionen**
 Zahlreiche Funktionen zur Fehlerüberwachung (FM) und Performanceüberwachung (PM) an Anwender- und Netzschnittstellen
- Entwickelt für die Adtran FSP 3000 Plattform**
 Erweiterung der bewährten, offenen optischen Transportlösung FSP 3000 um leistungsfähige ConnectGuard™-Sicherheitsfunktionen

Überblick

Die WCC-PCN-AES100GB ist eine WDM-Transponderkarte für den Transport von verschlüsselten 100GbE- und OTU4-Diensten über optische Netze. Mit unserer robusten und zuverlässigen ConnectGuard™ Layer 1-Verschlüsselungstechnologie erfüllt dieses Modul die strengsten Sicherheitsanforderungen wie FIPS 140-2. Es ist außerdem vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für den Transport von Verschlusssachen bis zu VS-NfD zugelassen. Die Kanalkarte ist vollständig kompatibel mit der offenen optischen Transportplattform FSP 3000 von Adtran.

Die WCC-PCN-AES100GB ist eine kryptografische WDM-Kanalkarte für 2 Steckplätze mit einer anwendungsseitigen 100Gbit/s Schnittstelle für QSFP28 Steckmodule und einer netzseitigen 100Gbit/s Schnittstelle mit CFP-Steckmodul. Die WCC-PCN-AES100GB verfügt über kryptografische Funktionen wie Verschlüsselung, Entschlüsselung und Zufallszahlengenerierung. Der aggregierte 100Gbit/s Verkehr wird komplett mit dem Advanced Encryption Standard (AES) verschlüsselt/entschlüsselt. Die Datenverschlüsselung und der Einsatz eines Endpunkt-Authentifizierungsmechanismus schützen die Netzwerkverbindung zwischen zwei WCC-PCN-AES100GB-Karten vor Man-in-the-Middle-Angriffen. Unsere ConnectGuard™ Layer 1 Verschlüsselungstechnologie erfüllt die strengsten Sicherheitsstandards wie beispielsweise FIPS 140-2 (-F Variante). Darüber hinaus hat dieses Modul die BSI-Zulassung für die Übertragung von Verschlusssachen bis zur VS-NfD-Stufe erhalten (-G Variante). Damit ist diese Lösung ideal zum Schutz sensibler Informationen vor unbefugtem Zugriff geeignet.



WCC-PCN-AES100GB

Technische Spezifikationen auf einen Blick

Allgemeine Angaben

- 100Gbit/s Transponder
- Belegung von 2 Steckplätzen
- Steckbare Transceiver
- Integrierter Kanal für Steuerung
- Typische Verlustleistung mit steckbaren Transceivern: 75W

Schnittstellen

- Anwendungsseitig:
 - 1x QSFP28
 - Protokollunterstützung für 100GbE, 100GBaseR und OTU4
- Netzseitig:
 - 1xCFP Steckmodul
 - Durchstimmbare Wellenlänge

Umgebungsbedingungen

- SH9HU: Telcordia SR-3580 Level 3 (NEBS), ETSI EN 300 019-1-3 Class 3.1 (9RU) or 3.1e (1RU)
- Betriebstemperatur: +5°C bis +40°C / -40°C bis +65°C mit IHE E-Temp+ Baugruppenträger
- 5% bis 85% relative Luftfeuchtigkeit (keine Betauung)

Ersatzschaltung

- 1+1 unidirektionales revertives und nicht-revertives Schalten
- Umschaltzeiten <50ms
- Automatische Umschaltung zum Schutz anwendungsseitiger Schnittstellen

ConnectGuard™-Verschlüsselung (Standard Variante)

- Verschlüsselung der Nutzdaten mit AES-CTR und 256 Bit Schlüsseln
- Diffie-Hellman 4096 Bit Schlüsselaustausch jede Minute
- Schutz vor Manipulationen
- Authentifizierung der Gegenseite über PACE oder X.509
- Unterstützung des externen Schlüsselaustauschs über QKD

Sicherheitszertifizierungen (Standard Variante)

- Common Criteria (CC) Zertifizierung (Betriebssystemebene)

ConnectGuard™-Verschlüsselung (-G Variante)

- Verschlüsselung der Nutzdaten mit AES-GCM und 256 Bit Schlüsseln
- Diffie-Hellman 4096 Bit Schlüsselaustausch jede Minute
- Quanten-sicherer Schlüsselaustausch mit PQC
- Schutz vor Manipulationen
- Authentifizierung der Gegenseite über Pairing

Sicherheitszertifizierungen (-G Variante)

- BSI-Zulassung für den Transport von Verschlusssachen bis zu VS-NfD (BSI-VSA-10847)
- Common Criteria (CC) Zertifizierung (Betriebssystemebene)

ConnectGuard™-Verschlüsselung (-F Variante)

- Verschlüsselung der Nutzdaten mit AES-CTR und 256 Bit Schlüsseln
- Diffie-Hellman 3072 Bit Schlüsselaustausch jede Minute
- Schutz vor Manipulationen
- Authentifizierung der Gegenseite über Pairing

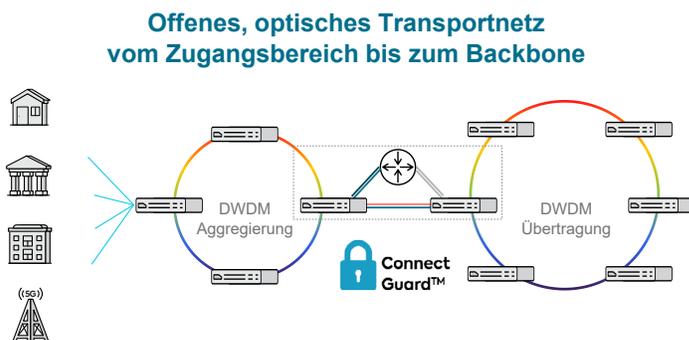
Sicherheitszertifizierungen (-F Variante)

- FIPS 140-2 Level 2 Zertifizierung
- Common Criteria (CC) Zertifizierung (Betriebssystemebene)

Anwendungen im Netz

Sichere SAN DCI-Verbindungen im Unternehmensnetz

- Hochgeschwindigkeits-Übertragung von sensiblen Daten über ein WDM-Metro-Netz
- Integrierte Layer 1-Verschlüsselung für zuverlässigen Schutz von Daten im Transportnetz mit 100 % Durchsatz und extrem niedriger Latenzzeit
- Protokollunabhängige Verschlüsselung auf Netzschicht 1 (Layer 1) schützt alle darüber liegenden Netzschichten
- Post-Quantum-Kryptografie (PQC) oder quantenbasierter Austausch von Schlüsseln (QKD)
- Wechselseitige Authentifizierung auf der Basis von X.509-Zertifikaten
- Die robusteste und zuverlässigste Layer 1-Verschlüsselung auf dem Markt:
 - BSI-Zulassung für den Transport von Verschlusssachen bis zu VS-NfD (-G Variante)
 - Adva Network Security ist der einzige DWDM-Anbieter, der die BSI-Zulassung erhalten hat
 - Common Criteria-Zertifizierung (Betriebssystemebene)
 - FIPS 140-2 Level 2 Zertifizierung (-F Variante)



Vernetzung von Rechenzentren

