Datenblatt

9TCE-PCN-10GU+AES10G

Muxponder/4-fach 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
- **9TCE-PCN-10GU+AES10G Zertifizierungs-varianten**
  -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**
  10Gbit/s Muxponder oder 4-fach-Transponder auf einer Schnittstellenkarte mit einfacher Breite
- **Multi-Protokoll-Schnittstellen**
  10 Multi-Protokoll-Schnittstellen können zum Anschluss von Anwendungen oder als netzseitige Ports verwendet werden
- **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 9TCE-PCN-10GU+AES10G ist eine Schnittstellenkarte, die als 10Gbit/s-Multiplexer oder als 4-fach Transponder eingesetzt werden kann. 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 offen optischen Transportplattform FSP 3000 von Adtran.

Unsere 9TCE-PCN-10GU+AES10G ist eine TDM-Multiplexkarte für Unternehmensnetze mit 10 Steckplätzen für Schnittstellenmodule, die je nach Einsatz als Muxponder oder Transponder entweder zum Anschluss von Anwendungen oder als netzseitige Ports verwendet werden können. Außerdem implementiert diese Karte kryptografische Funktionen wie Verschlüsselung, Entschlüsselung und Zufallszahlengenerierung. Der Verkehr auf der netzseitigen Schnittstelle wird komplett mit dem Advanced Encryption Standard (AES) verschlüsselt/entschlüsselt. Die Datenverschlüsselung und der Einsatz eines Endpunkt-Authentifizierungsmechanismus schützen die Netzwerkverbindung zwischen zwei 9TCE-PCN-10GU+AES10G Modulen 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.

9TCE-PCN-10GU+AES10G

Technische Spezifikationen auf einen Blick

Allgemeine Angaben

- Zwei Betriebsarten:
  - 10G Terminal-Multiplexer
  - 10G 4-fach Transponder
- Belegung eines Steckplatzes
- 10x SFP/SFP+ Steckplätze für Anwender- und netzseitige Schnittstellen
- Typische Leistungsaufnahme bei voller Bestückung: 25W/35W

Muxponder Betriebsart

- 9 Schnittstellen für Anwendungen (SFP/SFP+) and eine Netz-Schnittstelle (SFP+)
- Bis zu 9 Anwendungen werden in einer 10Gbit/s ITU-T Wellenlänge (OTU2) aggregiert
- Anwendungs-Schnittstellen: STM-4/OC12, GbE, STM-16/OC48 und elektrische Ethernet E10-1000T

Transponder Betriebsart

- Bis zu vier unabhängige Transponder pro Karte, mit jeweils einer Anwender-Schnittstelle (SFP/SFP+) und einer netzseitigen Schnittstelle (SFP+)
- Anwendungs-Schnittstellen: 8GFC, STM-64/OC192, 10GbE LAN, CE-LR, RoCE, OTU-2

Umgebungsbedingungen

- Telcordia SR-3580 level 3 (NEBS), ETSI EN 300 019-1-3 Class 3.1 (9RU)/3.1e (7RU, 1RU)
- Betriebstemperatur: +5°C bis +40°C / -40°C bis +65°C mit 1HE E-Temp+ Baugruppenträger
- 5% bis 85% relative Luftfeuchtigkeit (keine Betauung)

ConnectGuard™-Verschlüsselung (Standard Variante)

- Verschlüsselung der Nutzdaten mit AES-CTR und 256 Bit Schlüsseln
- Diffie-Hellman 2048 Bit Schlüsselaustausch jede Minute
- Schutz vor Manipulationen
- Authentifizierung der Gegenseite über 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-10788)
- 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)

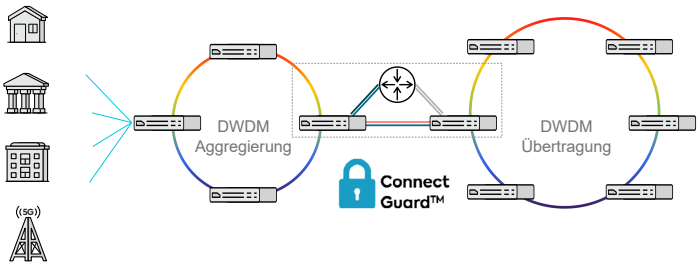
- FIPS 140-2 Level 2 Zertifizierung
- Common Criteria (CC) Zertifizierung (Betriebssystemebene)

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)

Offenes, optisches Transportnetz vom Zugangsbereich bis zum Backbone



Vernetzung von Rechenzentren

Verbindung von Hyperscale-Rechenzentren

Verbindung von Rechenzentren zur Sicherstellung der Geschäftskontinuität und Wiederherstellung nach Ausfällen

© August, 2024 Adva Network Security. Alle Rechte vorbehalten.
Änderungen ohne vorherige Ankündigung vorbehalten.