Adva
NETWORK SECURITY

Solution Brief

ConnectGuard™ security for optical networks

Quantum-safe encryption protects Layer 1 with operational simplicity

Highlights

- **Any protocol, any speed**
  Protocol-agnostic hardware-based encryption with lowest latency possible and 100% throughput
- **Protecting all layers at once**
  Encrypting data at the lowest layer protects data at higher layers as well
- **Certified and approved**
  Common Criteria and FIPS certified; approved for the transport of German-, EU- and NATO-classified data
- **Quantum-safe encryption**
  Combining Diffie-Hellman with newly developed McEliece cryptography for quantum-safe encryption
- **Fully integration into standard PKI**
  SCEP-based automation and manual operations
- **Ensemble Controller management suite**
  Separated security domains for operator and user

With the widespread adoption of cloud-based applications, more and more data is flowing outside the traditional enterprise perimeter. This means sensitive data is increasingly in danger from the growing threat of cyberattacks. Our ConnectGuard™ Layer 1 encryption, available on the FSP 3000 platform, secures data in motion with minimal operational effort and the highest levels of performance.

ConnectGuard™ security for optical networks

Data center interconnect and mission-critical network infrastructure with next-generation data security

Why Layer 1 encryption?

Encryption is the most effective way to secure communications over untrusted networks against unauthorized access. By encoding data at layer 1 it becomes unintelligible to anyone without permission to read it. What's more, encryption at Layer 1 protects data at all layers in the network stack, as any higher layers use the services of the layer below. As every bit transported at Layer 1 is encrypted, all data including management and control traffic is protected .

ConnectGuard™ security suite

Our innovative ConnectGuard™ optical encryption technology is available on the FSP 3000 platform. No additional hardware is required to protect data in motion. This ensures maximum performance at lowest cost and highest operational simplicity. With ultra-low latency and 100% throughput, our ConnectGuard™ optical encryption is protocol agnostic. It encrypts any type of customer service, e.g., Ethernet, Fiber Channel and OTN, in a fully transparent way. Encrypted data can be transported at 100Gbit/s and higher speeds.

ConnectGuard™ optical encryption uses the Advanced Encryption Standard and a 256-bit key (AES-256) to encrypt and protect data in motion. Diffie-Hellman key exchange for secure encryption key generation, with key rotation every minute, advanced physical security mechanisms, and a strictly separated encryption domain manager make the solution compliant to the most stringent regulatory requirements.

Compliant with regulatory requirements

With General Data Protection Regulation (GDPR) and other regulatory requirements in place, an increasing number of industry verticals such as the financial sector, healthcare, government agencies and military institutions, require maximum network security when transmitting sensitive information between data centers for disaster recovery and business continuity operations. Our FSP 3000 solutions with ConnectGuard™ optical encryption comply with the most stringent security standards, such as the US Federal Information Processing Standard FIPS 140-2, issued by the National Institute of Standards and Technology (NIST), (Certificate number #3952).

The FSP 3000 platform with ConnectGuard™ encryption technology has also been approved for the transmission of classified data by governmental institutions such as the German federal office for information security (BSI). As of today, the FSP 3000 is the only DWDM system that has BSI approval to be used for the transport of German-classified data up to Confidential ("VS-V") level. The approval also allows the use of ADVA FSP 3000 equipment for the transport of EU and NATO classified data. Now, government organizations can deploy the most robust security methods available in their transport infrastructure.

Quantum-safe encryption protects Layer 1 with operational simplicity

Full integration into PKI

Public key infrastructure (PKI) reduces security risks associated with business processes. It guarantees the security of electronic data in strategic areas, such as healthcare, finance or military. The FSP 3000 ConnectGuard™ technology uses the simple certificate enrollment protocol (SCEP) to integrate in existing PKI and obtain required certificates. Automated processes for complex and time-consuming tasks such as mutual authentication, key rotation or service provisioning, make the operation of our FSP 3000 encrypted connectivity simple. This significantly reduces operational complexity and operational costs.

High-level specifications

- Hardware-based, Layer 1 encryption
- Advanced encryption standard with 256-bit cryptographic key (AES-256)
- Diffie-Hellman 2048/3072/4096 bit dynamic key exchange every minute
- Key exchange configurable in ODU OH bytes
- FIPS (-F) certified and government (-G) approved channel cards variants
- Automated authentication between transponder modules or ports
- Automated key rotation though X.509 lifetime
- Automated certificate enrollment (SCEP) or manual operations
- NMS used for automated provisioning of secure services
- Built-in web server security with X.509 certificate

Future proof and quantum-safe

The advent of quantum computing with ultra-high processing power poses a major threat to data security. Traditional encryption technology is no longer sufficient to protect data against quantum-computer attacks. New quantum-safe techniques are required: PQC and QKD. Post quantum cryptography (PQC) uses algorithms that cannot be broken by quantum-computers. Quantum key distribution (QKD) uses quantum physics to secure information. Both methods are supported by FSP 3000.

Quantum computers are still under development. However, they already pose a thread today. Data encrypted with traditional algorithms could be stored and decrypted at a later point of time. Network operators and enterprises should start adapting their security measures now.

On July 2021 ADVA launched the first commercial solution offering fully encrypted services secured by PQC. Designed in accordance with the recommendations of leading bodies, the quantum-safe FSP 3000 transport solution relies on a hybrid key exchange system, combining PQC algorithms with classical encryption methods. Built for crypto-agility, the solution is ready for software updates in the future, ensuring it delivers the most robust network protection now and for decades to come.

Connect Guard™

"Our ConnectGuard™ encryption technology complies with the most stringent security standards"