FSP 3000 ConnectGuard™ Optical

Combining secure Layer 1 encryption with operational simplicity

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™ Optical Layer 1 encryption secures data in motion at line speeds up to 600Gbit/s with minimal operational effort and the highest levels of performance.

Why Layer 1 encryption?

Encryption is the most effective way to increase the level of security and safeguard external network connections against unauthorized access. What's more, encryption at Layer 1 protects data at all layers in the network stack, as everything must flow through the connectivity layer before going anywhere else. As every bit transported at Layer 1 is encrypted, there is no information left behind.

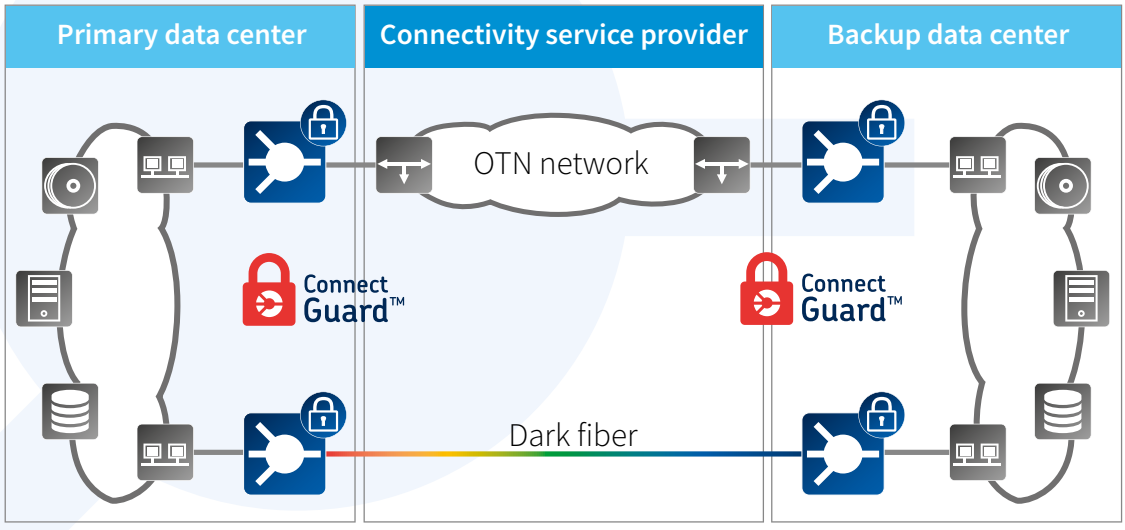
ADVA ConnectGuard™ security suite

Our innovative ConnectGuard™ Optical technology available on the FSP 3000 platform, is the safest method to protect information and guarantee data integrity with the highest performance. It delivers maximum efficiency at ultra-low latency and line speeds in excess of 100Gbit/s. What's more, it carries a wide variety of protocols including Ethernet, Fiber Channel, Infiniband and OTN.

ADVA ConnectGuard™ Optical network encryption provides a transparent, wire-speed service using Advanced Encryption Standard (AES-256) for maximum data security. Dynamic Diffie-Hellman key exchange for secure encryption key generation, with key rotation every minute, and a strictly separated encryption domain manager make the solution compliant to the most stringent regulatory requirements.

Your benefits

- **Any protocol, any speed**
  Protocol-agnostic hardware-based encryption with lowest latency possible and 100% throughput
- **Full data protection**
  Encryption at the lowest layer; protecting data at higher layers as well
- **Certified and approved**
  Approved by governmental institutions for the transport of classified data
- **Fully integration into standard public key infrastructure (PKI)**
  SCEP-based automation and manual operations
- **Ensemble ConnectGuard™ Director**
  Strictly separated encryption domain manager
- **Ease of use**
  Automated procedures for authentication, services creation and regular key generation.



Compliant with regulatory requirements

With General Data Protection Regulation (GDPR) and other regulatory requirements taking effect in 2018, an increasing number of industry verticals such as the financial sector, healthcare, government agencies and military institutions, require maximum network security when transmitting private information between data centers for disaster recovery and business continuity operations. Our FSP 3000 ConnectGuard™ Optical solution complies 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).

Our 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-VSA-10034). It's the first platform that supports Fiber Channel encryption at line speeds of up to 100Gbit/s to achieve BSI-approved status. Now, government organizations can deploy the most robust security methods available in their transport infrastructure. Data that requires restricted clearance, including EU and NATO communication, can be encrypted at the lowest network layer on streams of 100Gbit/s capacity and beyond.

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. Our FSP 3000 ConnectGuard™ technology has been engineered to work in this environment, where an efficient and secure interworking with third-party solutions is required. 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.

Connect Guard™

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

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
- SCEP-based automation and manual operations
- NMS used for automated provisioning of secure services
- Built-in web server security with X.509 certificate

Future-proof solution

The advent of quantum computing will be a game changer for every industry and will have a huge impact on data security: traditional encryption technology is no longer sufficient to ensure data in this environment. New cryptographic algorithms and new secure communication methods, such as post quantum cryptography (PQC) and quantum key distribution (QKD), are currently under development. ADVA, in cooperation with major partners and customers, is participating in the development of these new technologies. Successful demos have already taken place, such as the world-first 100G quantum-safe transport over 2800km in a unique joint demo with some of Europe's leading national research and education networks (NRENs).

For more information please visit us at www.oscilloquartz.com

ADVA™