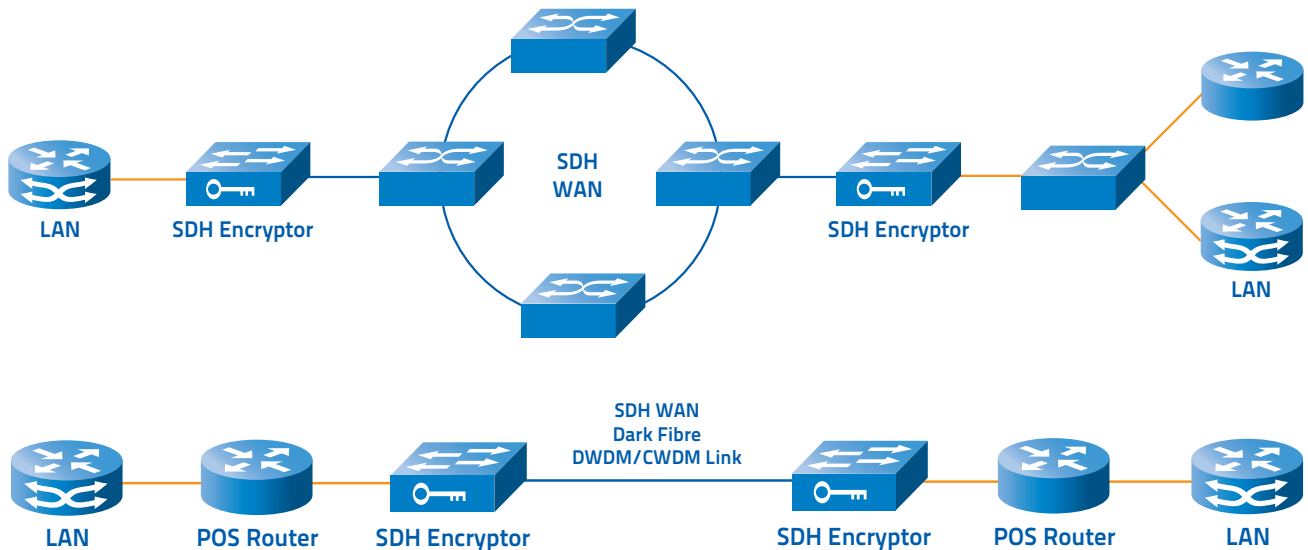# SONET/SDH Encryption

## atmedia SDH Encryptor

Modern high-speed networks are mostly based on the synchronous SONET/SDH technology. OC-3, OC-12 or OC-48 connections with transmission speeds from 155 mbps to 2.4 gbps are used in a more and more broadening area of application. Examples are interconnections between PBX devices, wire-, laser- or radio based SONET links for customer access and high speed router data exchange via Packet over SONET (POS). The atmedia SDH Encryptor is a protocol transparent encryption device for SONET/SDH links. The system encrypts OC3, OC12 and OC48 networks in realtime and without any loss of quality. Areas of application for the atmedia SONET Encryptor are network scenarios where standard SONET or SDH applications have to be reliably secured against tapping and manipulation. The atmedia SDH Encryptor simply adds VPN functionality to these networks.

## Application scenarios







## Highlights of the atmedia SDH Encryptor

- Strongest crypto technology available (AES-GCM, ECC)
- Full-Duplex real-time AES encryption at SDH transport level
- Encryption bandwidth from 155 mbps up to 2.4 gbps
- Simple integration into STM-1, STM-4 or STM-16 SONET/SDH networks (bump in the wire)
- Maintenance-free operation
- Transparent handling of SONET/SDH overheads and lead through of network clocks
- No impact on existing redundancy mechanisms
- Compliant to the requirements of FIPS 140-2 L3 and CC EAL4
- Certified for the transmission of classified data by the German BSI (restricted)

# Technical Data

## SDH Security

### Encryption Performance

- Line rate encryption of the C4/C4-4c/C4-16c container (path mode) or of the entire SONET link (line mode)
- Key change without interruption of traffic
- Latency per device: STM1: ≤ 0,016ms, STM4: ≤ 0,008ms, STM16: ≤ 0,002ms

### Key management

- Ad-hoc device authentication
- Tamper resistant key storage
- Automatic time triggered change of session keys
- Autonomous operation without external key management

### Netzwerk

- Compatible to SDH and SONET
- Transparent handling of SONET/SDH overheads
- 3R clock regeneration
- Optical Loss pass-through

### Line Interfaces

SFP-modules

SFP MM LC (62,5/125μ)

SFP SM LC (9/125μ) SR/IR/LR

SFP DWDM/CWDM

### Crypto Technology

- AES (256 bit) encryption with CBC block mode
- Key generation with hardware random source
- Key exchange with Diffie-Hellman ECC algorithm
- Compliant to the requirements of FIPS 140-2 L3 and CC EAL4
- Approved by the BSI for VS-NfD, NATO and EU restricted

### System management

- Configuration via serial console (RS-232/V.24) or SSH network (Ethernet RJ45-10/100BT) access
- Integrated monitoring of network status and operation
- Audit and event logging
- Remote monitoring via SNMP (V2c/V3)
- Link monitoring via atmedia CryptMon

### Hardware

Operating temperature: 1° C - 40° C

Relative humidity: 10% - 85%, non condensing

Network configurations: - STM-1/OC-3c (155.52 mbps)
- STM-4/OC-12c (622.08 mbps)
- STM-16/OC-48c (2.488 gbps)

Tamper resistant housing

482,6mm (19") 1RU chassis, H: 44mm, W: 430mm, D: 320mm

Redundant hot-swap PSU: 110-240V AC 50-60Hz or -48V DC, 90W

### Conformity

- CE, FCC

The atmedia systems and related documentation are subject to continuos improvement. Therefore atmedia reserves the right to change documentation without notice.