

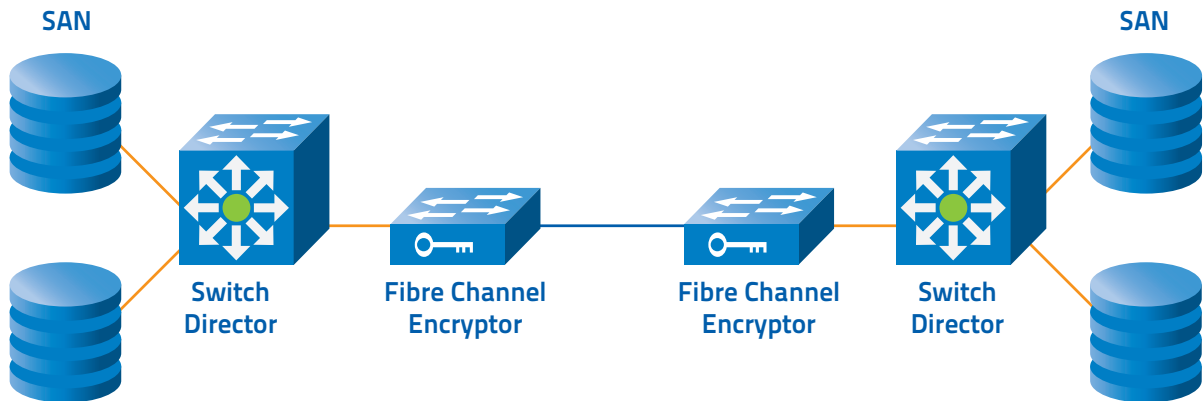
## Fibre Channel Encryption

### atmedia Fibre Channel Encryptor

Storage Area Networks are the backbones of today's computing infrastructure. Since they connect servers to their storage and backup systems, most sensitive data will be transferred over these networks. In a local environment, standard security measures like zoning and physical access restrictions might be sufficient. For a SAN that spreads over several distant locations however there exists a high risk of tapping and manipulation of most critical data. The SAN technology Fibre Channel is used for local storage connectivity as well as for connecting remote systems for business continuity scenar-

ios. A SAN extension can be easily realized by connecting several local Fibre Channel networks over Dark Fiber or WDM technology. The atmedia Fibre Channel Encryptor enables the protection of this distributed Fibre Channel SAN by a very simple integration into the existing Fibre Channel structure. It encrypts the payload between the switches and thus effectively prevents eavesdropping and manipulation of the valuable storage data. The hardware encryption works at network layer 2 and does not cause any measurable effect on SAN operation.

### Application scenario



### Highlights

- Strongest crypto-technology available (AES, ECC)
- Fibre Channel E-port encryption at line rate (1gbps/2gbps)
- No encryption overhead
- Network integration without any change of infrastructure (Bump in the wire)
- Maintenance-free operation
- Exchangeable SFP fibre optics



## Technical Data

### atmedia Fibre Channel Encryptor

<b>Performance</b>	<b>Crypto Technology</b>
<ul style="list-style-type: none"><li>▪ Real-time encryption of 1G/2G Fibre Channel E-Ports</li><li>▪ Full-duplex line-speed throughput independent of packet size</li><li>▪ Key changes without interruption of traffic</li><li>▪ Latency: <math>\leq 0,010</math>ms per device</li></ul>	<ul style="list-style-type: none"><li>▪ AES (256 bit) encryption with CBC block mode</li><li>▪ Key generation with hardware random source</li><li>▪ Key exchange with Diffie-Hellman ECC algorithm (DH-ECKAS)</li><li>▪ Compliant to the requirements of FIPS 140-2 L3 and CC EAL4</li></ul>
<b>Key Management</b>	<b>System Management</b>
<ul style="list-style-type: none"><li>▪ Ad-hoc device authentication</li><li>▪ Tamper resistant key storage</li><li>▪ Automatic time triggered change of master keys and group keys</li><li>▪ Autonomous operation without external key management</li></ul>	<ul style="list-style-type: none"><li>▪ Configuration via serial console (RS-232/V.24) or Secure Shell (SSH) network access (out-of-band Ethernet RJ45-10/100BT)</li><li>▪ Integrated monitoring of network status and operation</li><li>▪ Audit and event logging</li><li>▪ Syslog support</li><li>▪ Remote monitoring via SNMP (V2c/V3 authpriv)</li><li>▪ Link monitoring via ATMedia CryptMon</li></ul>
<b>Network</b>	<b>Hardware</b>
<ul style="list-style-type: none"><li>▪ Compatible to 1G/2G Fibre Channel E-Port</li><li>▪ E-Port / Inter Switch Link (ISL) Interface</li><li>▪ Optical Loss Pass-through</li></ul>	<p>Operating temperature: 1°C - 40°C</p> <p>Relative humidity: 10% - 85%, non condensing</p> <p>Chassis: 482,6mm (19") 1RU, H: 44mm, W: 430mm, D: 320mm</p> <p>Weight: 7kg</p> <p>Redundant Hot-Swap PSU: 110-240V AC 50-60Hz or -48V DC, 90W</p> <p>Tamper resistant design</p>
<b>Line Interfaces</b>	<b>Conformity</b>
SFP modules	<ul style="list-style-type: none"><li>▪ CE, FCC</li></ul>
SFP MM LC (62,5/125 $\mu$ )	
SFP SM LC (9/125 $\mu$ ) SR/IR/LR	
SFP DWDM/CWDM	

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