



## Ethernet Verschlüsselung

### atmedia Ethernet Verschlüsseler

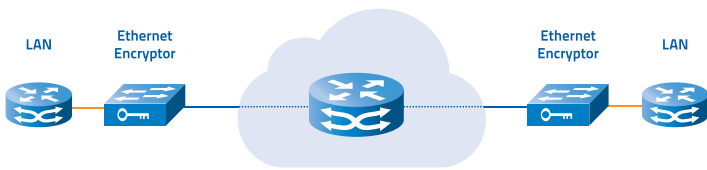
Im Bereich der Layer 2 Ethernet Netzwerke bieten immer mehr Netzwerkprovider ihren Kunden multipunkt-fähige WAN-Lösungen an. Technisch realisiert werden diese durch einfache Hub-and-Spoke oder leistungsfähige Carrier Ethernet bzw. Metro Ethernet bzw. VPLS Technologien. Für den Kunden stellen sich diese Lösungen als ein über mehrere Standorte verteiltes LAN dar, an das Ethernet Endgeräte direkt angeschlossen werden können. Im Gegensatz zu herkömmlichen Punkt-zu-Punkt Netzwerken ist die Trennung zwischen verschiedenen Nutzern seitens des Providers nur noch „virtuell“

- es besteht somit ein erhebliches Risiko, dass Netze verschiedener Kunden „vermischt“ werden, und Dritte unbefugten Zugriff auf das LAN erhalten.

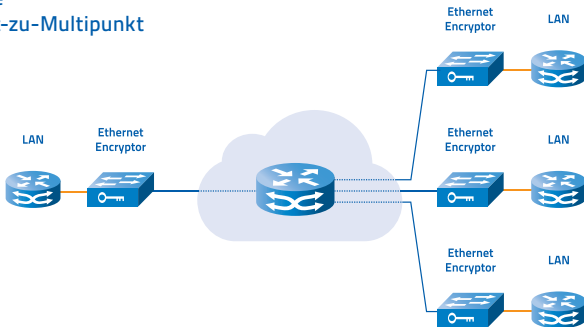
Der atmedia Ethernet Verschlüsseler schützt Ethernet Multipunkt Szenarien wirkungsvoll gegen Abhören und Manipulation. Das Gerät arbeitet transparent auf Netzwerk Layer 2 und unabhängig von eingesetzten Netzwerkprotokollen und Endgeräten. Eine Änderung der Netzwerk- Infrastruktur bzw. existierender Redundanzszenarien ist nicht erforderlich.

### Anwendungsszenarien

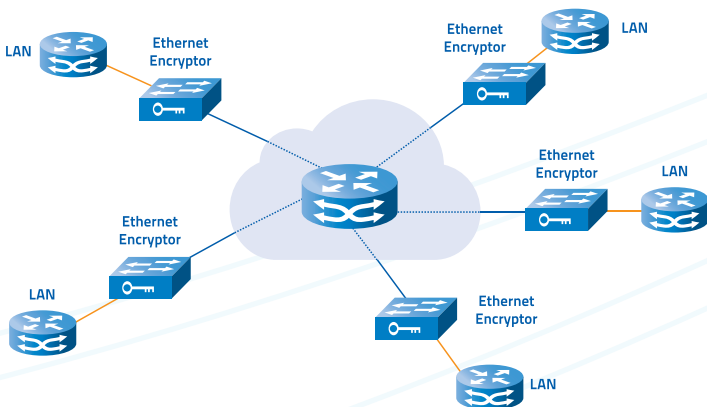
#### E-Line Punkt-zu-Punkt



#### E-Tree Punkt-zu-Multipunkt



#### E-Lan Multipunkt-zu-Multipunkt



### Highlights

- Stärkste verfügbare Crypto-Technologie (AES-GCM, ECC)
- Integritäts- und Replay-Schutz
- Voll-Duplex Verschlüsselung mit Leitungsgeschwindigkeit
- Transparent für VLAN, CoS, MPLS
- Interoperabel von 10M bis zu 10G
- Verschlüsselung von Unicast, Multicast und Broadcast Traffic
- Unabhängig von den verwendeten Endgeräten und Applikationen
- Keinerlei Änderung in der Netzwerk-Infrastruktur notwendig
- Sehr gut skalierbar
- Kein Einfluss auf vorhandene Redundanzszenarien
- Zugelassen für Verschlussachen durch das BSI



## Technische Daten

### atmedia Ethernet Verschlüsseler

<p><b>Leistungsdaten</b></p> <ul style="list-style-type: none"> <li>▪ Punkt-zu-Punkt-, Punkt-zu-Multipunkt- oder Multipunkt-Verschlüsselung</li> <li>▪ Mandantenfähige Gruppenverschlüsselung (max. 1000 Peers)</li> <li>▪ Echtzeit Verschlüsselung der Ethernet Payload (IEEE 802.3)</li> <li>▪ Durchsatz unabhängig von der Paketgröße</li> <li>▪ Schlüsselwechsel ohne Unterbrechung des Links</li> <li>▪ Latenz: 100M: ≤ 0,040ms, 1G ≤ 0,008ms, 10G: ≤ 0,004ms je Gerät</li> </ul>	<p><b>Verschlüsselungstechnologie</b></p> <ul style="list-style-type: none"> <li>▪ AES-GCM oder AES-CBC (256 Bit) Verschlüsselungsverfahren</li> <li>▪ Integritäts- und Replay-Schutz über Galois Counter Modus (GCM)</li> <li>▪ Schlüsselerzeugung durch Hardware Zufallszahlengenerator</li> <li>▪ Schlüsselaustausch über Diffie-Hellman ECC Verfahren (DH-ECKAS)</li> <li>▪ Konform zu den Anforderungen von FIPS 140-2 L3 und CC EAL4</li> <li>▪ Zugelassen vom BSI für VS-NfD, NATO restricted und EU restrint</li> </ul>
<p><b>Schlüsselmanagement</b></p> <ul style="list-style-type: none"> <li>▪ Ad-hoc Authentisierung zum Registrieren von Gegenstellen</li> <li>▪ Manipulationsgeschützte Schlüsselspeicherung</li> <li>▪ Built-in Schlüsselservers zur Verteilung der Gruppenschlüssel</li> <li>▪ Automatischer Wechsel der Verbindungsschlüssel nach konfigurierbarem Zeitintervall</li> </ul>	<p><b>Systemmanagement</b></p> <ul style="list-style-type: none"> <li>▪ Konfiguration über serielle Konsole (RS-232/V.24) oder Secure Shell (SSH) Netzwerkzugang (Out-of-Band Ethernet RJ45-10/100BT)</li> <li>▪ Integrierte Leitungs- und Betriebsüberwachung</li> <li>▪ Audit und Event Logging</li> <li>▪ Abfrage des Betriebszustandes über SNMP (V2c/V3 authpriv)</li> <li>▪ Überwachung des Linksstatus mittels atmedia CryptMon</li> </ul>
<p><b>Netzwerk</b></p> <ul style="list-style-type: none"> <li>▪ Kompatibel mit E-Line, E-Tree, E-Lan, VPLS, VPWS und anderen Ethernet Services</li> <li>▪ Unterstützung von Jumbo Frames</li> <li>▪ Transparent bzgl. VLAN (auch Q-in-Q), CoS, MPLS, Fibre Channel over Ethernet (FCoE)</li> <li>▪ Optical Loss pass-through (Link Loss Carry Forward)</li> </ul>	<p><b>Hardware</b></p> <p>Arbeitstemperatur: 1°C - 40°C</p> <p>Luftfeuchtigkeit: 10% - 85%, nicht kondensierend</p> <p>10M / 100M: 482,6mm (19") 1HE, H: 44mm, B: 430mm, T: 230mm, G: 4kg Redundante Stromversorgung: 110-240V AC 50-60Hz, 11W</p> <p>1G: 482,6mm (19") 1HE, H: 44mm, B: 430mm, T: 320mm, G: 7kg Redundante Hot-Swap Stromversorgung 110-240V AC 50-60Hz oder -48V DC, 90W</p> <p>10G: 482,6mm (19") 2HE, H: 88mm, B: 430mm, T: 370mm, G: 10kg Redundante Hot-Swap Stromversorgung 110-240V AC 50-60Hz oder -48V DC, 115W</p> <p>Gehäuse: Tamper resistentes Design</p>
<p><b>Line Interfaces</b></p> <p>10 M: 10Base-T TP RJ45 Full-Duplex</p> <p>100 M: 10/100Base-T TP RJ45 Full-Duplex</p> <p>1 G: SFP-Module</p> <p>1000Base-T SFP TP RJ45</p> <p>1000Base-X SFP MM LC (62,5/125µ)</p> <p>1000Base-X SFP SM LC (9/125µ) SR/IR/LR</p> <p>1000Base-X SFP DWDM/CWDM</p> <p>10 G: XFP-Module</p> <p>10GBase-R XFP MM LC (62,5/125µ)</p> <p>10GBase-R XFP SM LC (9/125µ) SR/IR/LR</p> <p>10GBase-R XFP DWDM/CWDM, tunable DWDM</p>	<p><b>Konformität</b></p> <ul style="list-style-type: none"> <li>▪ CE, FCC</li> </ul>

Die atmedia Systeme sowie die zugehörige Dokumentation werden ständig auf dem neuesten Stand der Technik gehalten. atmedia behält sich daher vor, entsprechende Änderungen jederzeit und ohne vorherige Ankündigung durchzuführen.