

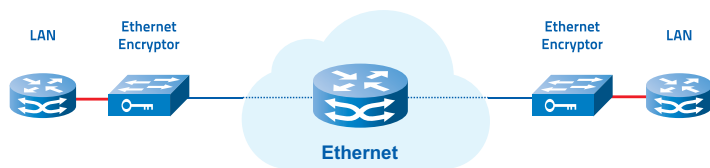
## High Assurance Ethernet and IP Encryption up to 100G

The **atmedia Encryptors** are safeguarding any layer 2 or layer 3 network communication reliably and without loss of quality. The area of application reaches from encryption of point-to-point connections to complex and large multipoint MPLS, VPLS or Metro Ethernet and storage networks. The systems are the first choice for the realization of highly available network scenarios where the communication between distributed sites or data centers has to be secured against interception and manipulation.

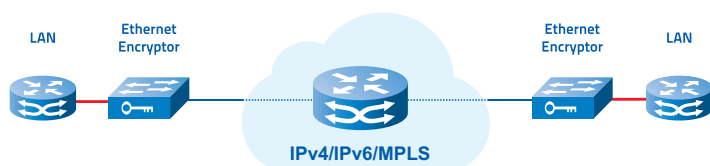
The atmedia Encryptors realize the network and encryption functionality with programmable FPGA hardware. All modules are completely developed and implemented by atmedia. A main feature is the encryption in combination with secure integrity protection for transmitted user data and network information (Ethernet and IP header). This protects the customer network against active and passive attacks since it realises a "perfect firewall".

### Application Scenarios

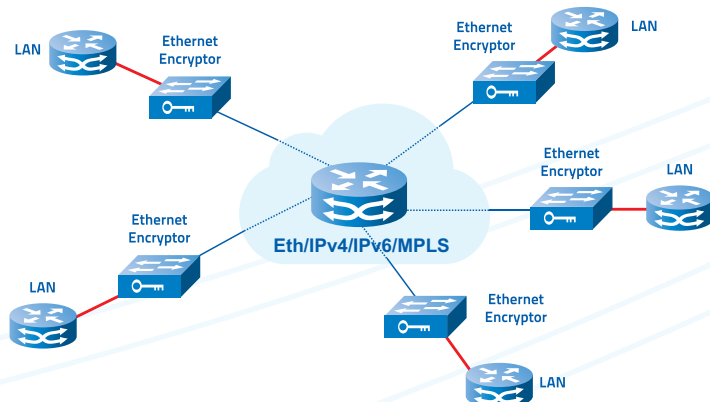
#### Ethernet interconnect via layer 2 or layer 1



#### Ethernet interconnect via layer 3 (IPv4 or IPv6 managed services)



#### Multipoint any-to-any interconnect via layer 3 or layer 2



### Highlights

- Strongest available crypto technology (AES256-GCM, 512bit ECC)
- Integrity- and Replay-Protection
- Lowest encryption overhead possible for secure operation
- "Perfect Firewall"
- Hardware-based random key generation
- Tamper resistant chassis
- IP-Tunnel via arbitrary IPv4 and IPv6 networks
- Traffic Flow Security (optional)
- No change of network design needed
- No impact on existing redundancy schemes
- Autonomous and maintenance free operation
- Approved by the German BSI for classified data (VS-NfD, EU Restrict, NATO restricted)
- Complete development by atmedia
- Made in Germany

## Technical Data

### atmedia Ethernet Encryptor

Models	
• A100MC (compact):	10M/100M throughput (RJ45 copper interfaces)
• A100M:	100M/1G throughput (RJ45 copper interfaces)
• A100MF:	100M/1G throughput (SFP Interfaces)
• A1G/A10G:	100M/1G/10G throughput (SFP/SFP+ interfaces)
• A4x10G:	4 * 1G/10G throughput (SFP/SFP+ interfaces)
• A40G:	10G/40G throughput (QSFP+ interfaces)
• A100G:	100G throughput (QSFP28 interfaces)

Performance
• Ethernet (Layer 2) und IP (Layer 3) encryption in point-to-point-, point-to-multipoint- or multipoint mode
• Multi tenant group encryption (max. 1000 peers)
• Real-time encryption in FPGA hardware
• Encryption independent of packet size and packet content
• Key changes without interruption of traffic
• Latency: 100M/100M compact < 50µs, 1G < 9µs, 10G/40G < 5µs

Network
• Compatible with E-Line, E-Tree, E-Lan, VPLS, VPWS and other Ethernet services
• Support of Jumbo frames
• IP-Tunnel mode: Layer 2 over IPv4 or IPv6 (IP or UDP) Throughput for small packets over 97% of link bandwidth
• Link Loss Carry Forward/Optical Loss Pass Through
• Traffic Flow Security mode prevents the identification, analysis and leakage of any data on the encrypted link.
• Protection against active attacks (Denial of Service) with hardware-based GCM packet filters
• Simple and secure IPv6 support
• Interoperable with network products of leading vendors

Options
• Wall mount kit, DIN-rail kit, 19" shelf for A100MC
• Rail extension kit for 19" mounting of A1G, A10G, A40G and A100G
• Optional licences for speed upgrades
• Optional licences for custom ECC, custom AES, TFS and IP

Crypto Technology
• AES-GCM(256 Bit) encryption with 64 or 128 Bit tag
• Integrity and replay protection with Galois Counter Mode (GCM)
• Key generation with hardware random source
• Key exchange with Diffie-Hellman ECC algorithm (DH-ECKAS)
• Compliant to the requirements of FIPS 140-2 L3 and CC EAL4
• Approved by the BSI for VS-NfD, NATO restricted and EU Restrict

Key Management
• Ad-hoc device authentication
• Tamper resistant key storage
• Built-in key server for the distribution of group keys
• Automatic time triggered change of master keys and group keys

System Management
• Configuration via serial console (RS-232/V.24) or Secure Shell (SSH) network access (out-of-band Ethernet RJ45 10/100/1000BT)
• Integrated monitoring of network status and operation
• Audit and event logging
• Remote monitoring via SNMP (V2c/V3 authpriv)
• Link monitoring with atmedia CryptMon

Hardware
• Operating temperature: 1°C - 40°C (A100MC: 50°C)
• Relative humidity: 10% - 85%, non condensing
• Chassis: 210mm x 220mm x 42mm (A100MC) 430mm x 230mm x 44mm (A100M) 430mm x 330mm x 44mm (1G/10G/40G/100G)
• Power supply: 12-30V DC, 90-240V AC, 7W (A100MC) 100-240V AC, 50-60Hz~, 11W (A100M) 100-240V AC, 50-60Hz~, 95W (1G/10G/40G/100G)
• Tamper resistant design

Conformity:
• CE (CB), FCC

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

Current firmware release: 3.3.2/3.3.3

Copyright © 2019 atmedia GmbH. All Rights Reserved. All trademarks mentioned in this document are the properties of their respective owners.