

Hochsichere Ethernet und IP Verschlüsselung bis 100G

Die Verschlüsseler sichern alle Layer 2 und Layer 3 Netzwerkverbindungen zuverlässig und ohne Qualitätseinbußen. Das Einsatzgebiet erstreckt sich von der Verschlüsselung von Punkt-zu-Punkt Verbindungen bis hin zur Absicherung komplexer MPLS, VPLS, Metro Ethernet und Speicher Netze. Die Systeme eignen sich insbesondere für die Realisierung von hochverfügbaren Szenarien mit geringer Latenz, in denen die Kommunikation zwischen ganzen Standorten und Rechenzentren oder einzelnen Servern, TK-Anlagen, Terminal Systemen, Datenbanken oder Audio/Video Systemen geschützt werden muss.

Die Systeme realisieren die Netzwerk- und Verschlüsselungsfunktionalität mittels eigenentwickelter FPGA Hardware. Durch den AES-GCM Integritäts- und Replay-Schutz arbeiten die Geräte wie eine „perfekte Firewall“. Dieser Schutz gegen aktive Angriffe auf die Geräte und das Netzwerk ist unverzichtbar, da er in vielen sensiblen Anwendungen, wie z.B. in Steuer- und Überwachungssystemen, eine mindest ebenso wichtige Rolle spielt wie die eigentliche Verschlüsselung

Anwendungsszenarien

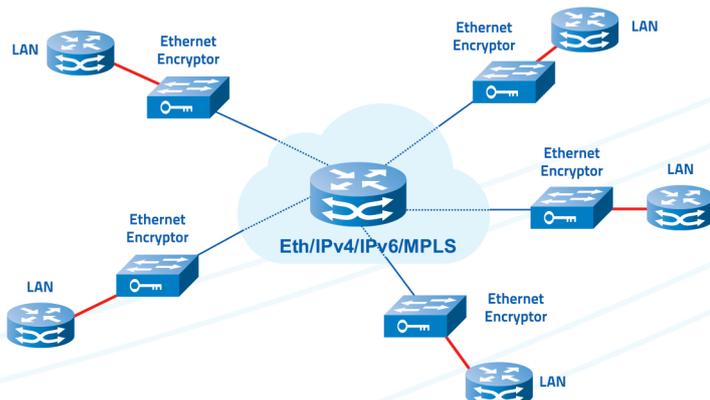
Ethernet Kopplung über Layer 2 oder Layer 1



Ethernet Kopplung über Layer 3 (IPv4 oder IPv6 Managed Services)



Multipunkt Vollvermaschung über Layer 3 oder Layer 2



Highlights

- Stärkste verfügbare Verschlüsselungstechnologie (AES256-GCM, 512Bit ECC)
- Integritäts- und Replay-Schutz
- Geringster Overhead bei sicherem Betrieb
- „perfekte Firewall“
- Hardware-Zufallszahlenerzeugung
- Manipulationsgeschütztes Gehäuse
- IP-Tunnel über beliebige IPv4 und IPv6 Netze
- Traffic Flow Security (optional)
- Keine Änderung der Infrastruktur notwendig
- Kein Einfluss auf vorhandene Redundanzszenarien
- Autonomer, wartungsfreier Betrieb
- Zugelassen für Verschlusssachen durch das BSI (VS-NfD, EU Restrint, NATO restricted)
- Made in Germany

Technische Daten

Ethernet Verschlüsseler

Gerätetypen	Verschlüsselungstechnologie
<ul style="list-style-type: none">• A100MC (compact): 10M/100M Durchsatz mit RJ45 Kupfer Interfaces• A100M: 100M/1G Durchsatz mit RJ45 Kupfer Interfaces• A100MF: 100M/1G Durchsatz mit SFP Interfaces• A1G/A10G: 100M/1G/10G mit SFP/SFP+ Interfaces• A4x10G: 4 * 1G/10G mit SFP/SFP+ Interfaces• A40G: 10G/40G mit QSFP+ Interfaces• A100G: 100G mit QSFP28 Interfaces	<ul style="list-style-type: none">• AES-GCM (256 Bit) Verschlüsselungsverfahren (64/128 Bit Tag)• Integritäts- und Replay-Schutz über Galois Counter Modus (GCM)• Schlüsselerzeugung durch Hardware Zufallszahlengenerator• Schlüsselaustausch über Diffie-Hellman ECC (DH-ECKAS)• Konform zu den Anforderungen von FIPS 140-2 L3 und CC EAL4• Zugelassen vom BSI für VS-NfD, NATO restricted und EU Restrict
Leistungsdaten	Schlüsselmanagement
<ul style="list-style-type: none">• Ethernet (Layer 2) und IP (Layer 3) Verschlüsselung im Punkt-zu-Punkt-, Punkt-zu-Multipunkt- oder Multipunkt-Modus• Mandantenfähige Gruppenverschlüsselung (max. 1000 Peers)• Echtzeit Verschlüsselung in FPGA Hardware• Durchsatz unabhängig von der Paketgröße• Schlüsselwechsel ohne Unterbrechung des Links• Latenz: 100M/100M compact < 50µs, 1G < 9µs, 10G/40G/100G < 5µs	<ul style="list-style-type: none">• Ad-hoc Authentisierung zum Registrieren von Gegenstellen• Manipulationsgeschützte Schlüsselspeicherung• Built-in Schlüsselservers zur Verteilung der Gruppenschlüssel• Automatischer Wechsel der Verbindungsschlüssel nach konfigurierbarem Zeitintervall
Netzwerk	Systemmanagement
<ul style="list-style-type: none">• Kompatibel mit E-Line, E-Tree, E-Lan, VPLS, VPWS und anderen Ethernet Services• Unterstützung von Jumbo Frames• IP-Tunnel Modus: Layer 2 über IPv4 oder IPv6 (IP oder UDP) Durchsatz bei kleinen Paketen über 97% der Netzbandbreite• Link Loss Carry Forward/Optical Loss Pass Through• Traffic Flow Security Modus verhindert das Erkennen und die Analyse der verschlüsselten Kommunikation• Schutz gegen aktive Angriffe (Denial of Service) durch hardware-basierte Paketfilterung• Einfache und sichere IPv6 Unterstützung• Interoperabel zu verbreiteten Netzwerkprodukten	<ul style="list-style-type: none">• Konfiguration über serielle Konsole (RS-232/V.24) oder Secure Shell (SSH) Netzwerkzugang (Out-of-Band Ethernet RJ45-10/100/1000BT)• Integrierte Leitungs- und Betriebsüberwachung• Audit und Event Logging• Abfrage des Betriebszustandes über SNMP (V2c/V3 authpriv)• Überwachung des Linkstatus mittels atmedia CryptMon
Optionen	Hardware
<ul style="list-style-type: none">• Wandhalterung, DIN-Schienen Halterung, 19" Boden für A100MC• Verlängerungsset 19" Einbau für A1G, A10G, A4x10G, A40G, A100G• Optionale Lizenzen für höhere Verschlüsselungsleistungen• Optionale Lizenzen für custom ECC, custom AES, TFS und IP	<ul style="list-style-type: none">• Arbeitstemperatur: 1°C - 40°C (A100MC: 50°C)• Luftfeuchtigkeit: 10% - 85%, nicht kondensierend• Gehäuse: 210mm x 220mm x 42mm (A100MC) 430mm x 230mm x 44mm (A100M) 430mm x 330mm x 44mm (1G/10G/40G/100G)• Stromversorgung: 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 resistentes Design
	Konformität
	<ul style="list-style-type: none">• CE (CB), FCC

Die Systeme sowie die zugehörige Dokumentation werden ständig auf dem neuesten Stand der Technik gehalten.