5 Wahrheiten über Verschlüsselung zwischen Standorten und Rechenzentren

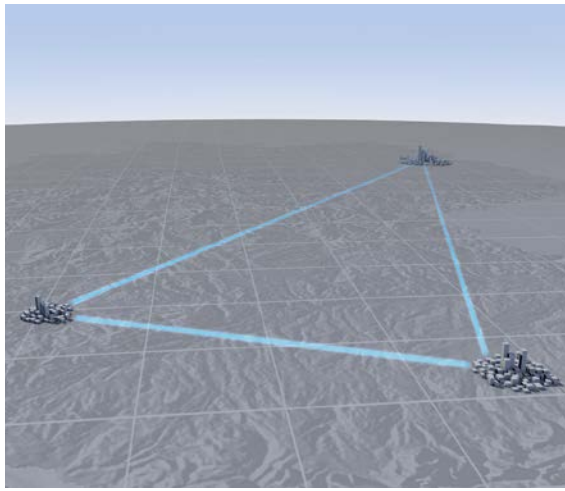
Stephan Lehmann
Dipl.-Betriebswirt, T.I.S.P.
Produktmanager
Tel. +49 (30) 6 58 84 - 265
stephan.lehmann@rohde-schwarz.com

ROHDE&SCHWARZ
Cybersecurity

Unser Tagesgeschäft basiert auf Kommunikation

Sicherheit ist erfolgsentscheidend

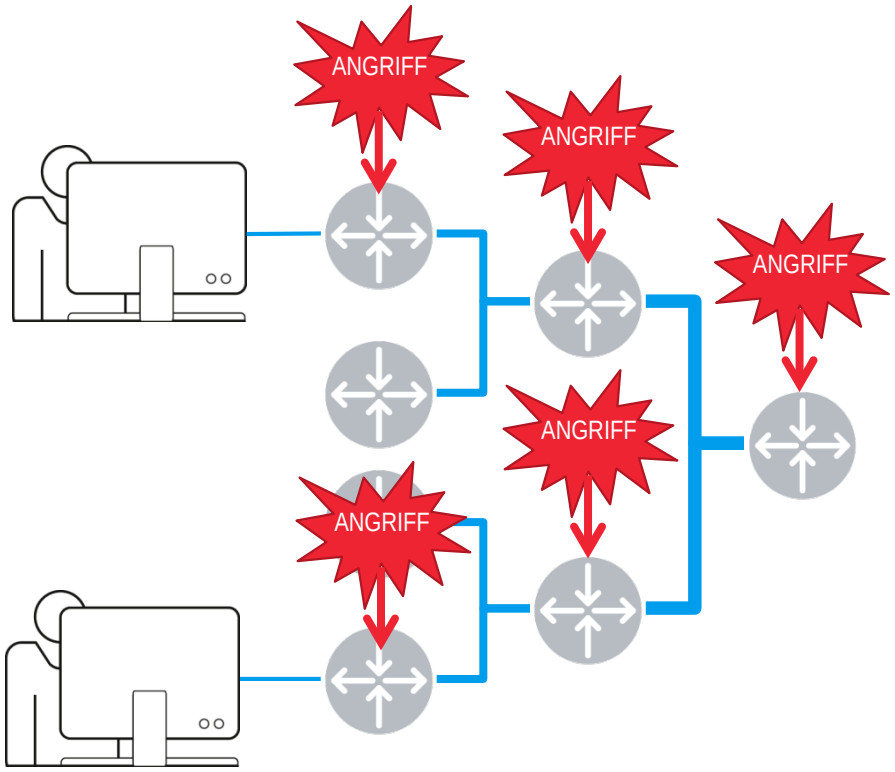
- Schnelle und sichere Kommunikation ermöglicht Wettbewerbsvorteile
  - Videokonferenzen
  - Desktop Sharing
  - VoIP Telefonie
  - Private Clouds und Big Data
- Ausgetauschte Daten sind strategisch, personenbezogen, oft unternehmenskritisch und meist vertraulich
- Akzeptanz der Lösung beim Anwender
  - Funktional und zeitsparend
  - Performant und verfügbar



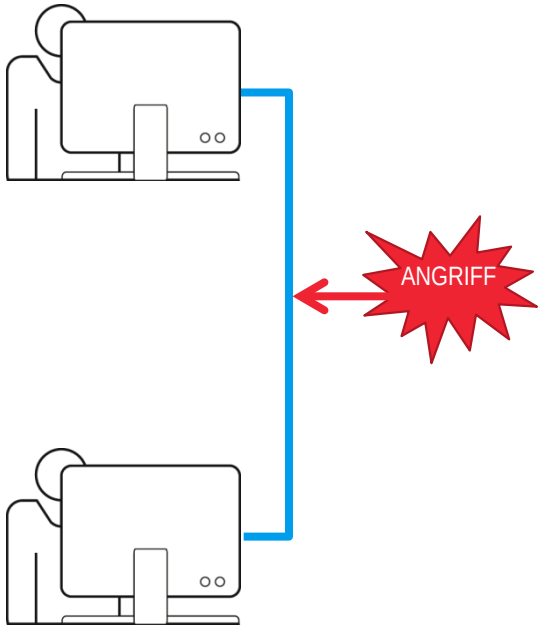
Kommunikation benötigt Ende-Ende-Sicherheit

Netzwerke und Standleitungen sind unsicher

Netzwerk-Knoten (Router/Switche) sind Angriffspunkte



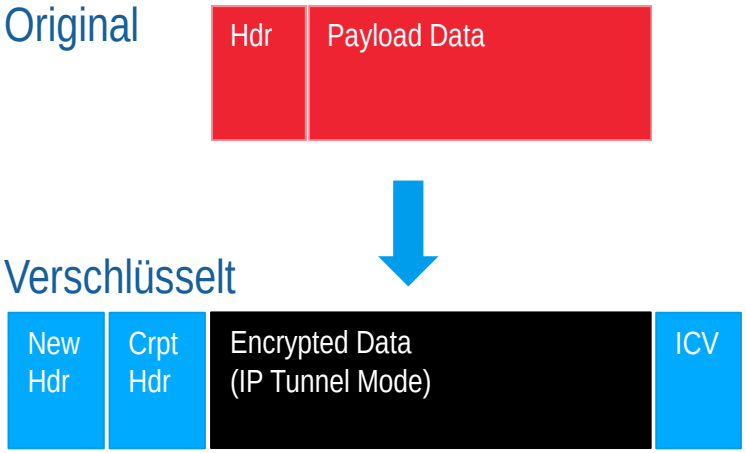
Standleitungen können angezapft werden



1. Wahrheit: Sicherheit erzeugt Overhead

So viel wie nötig, so wenig wie möglich

- Verschlüsselung benötigt Platz
  - neuer Header schützt vor Verkehrsflussanalysen und verdeckten Kanälen
  - Verschlüsselungsparameter
  - Authentisierung (ICV) für Manipulationsschutz
- Dieser „Overhead“ beeinflusst
  - Latenz und Jitter
  - Rahmen-/Paketgröße (MTU)
- Anforderung:
  - Konfigurierbarer Trade-Off zwischen Sicherheit und Overhead



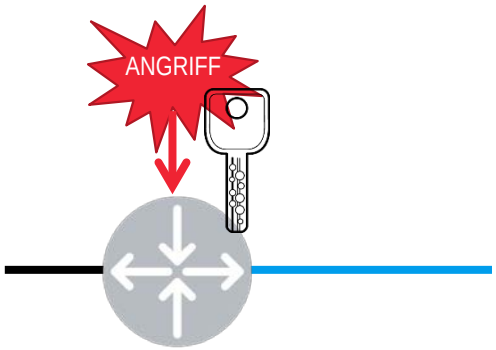
2. Wahrheit:
Integrierte Verschlüsselung ist weniger sicher

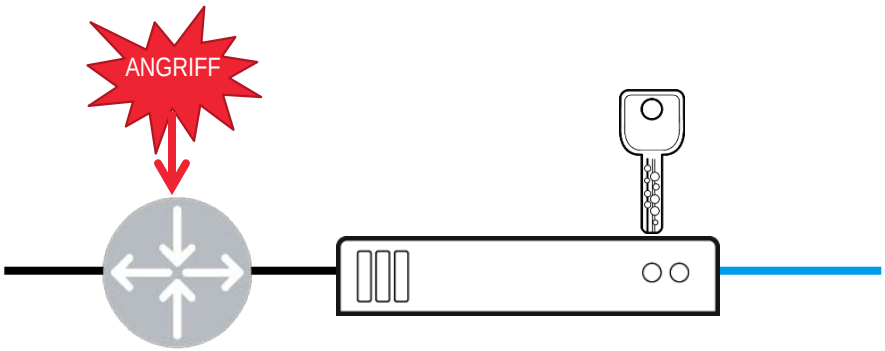
In Routern/Switchen eingebaute Verschlüsselung

—Software Verschlüsselung mit AES
—Netz-Admin = Security-Admin
—Einfache Authentisierung mit Passwort
—Logische Separierung

Hochwertige Verschlüsselung durch dedizierte Appliance

+Hardware-Verschlüsselung mit AES256+
+Separates Security Management
+Starke 2-Faktor-Authentisierung mit Zertifikaten
+Physische Trennung verschlüsselter und unverschlüsselter Daten





3. Wahrheit: Sichere und schnelle Verschlüsselung benötigt spezialisierte Hardware

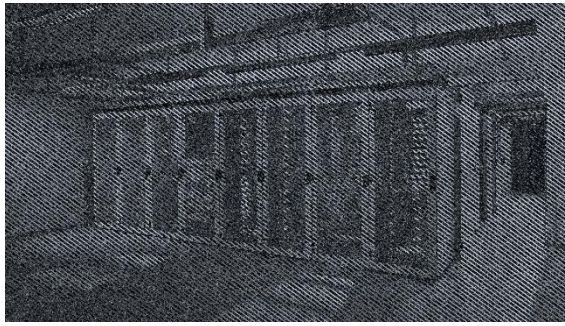
- Performance für Big Data und Echtzeitanwendungen
  - 10 Gbit/s = 10 Mrd. x „Licht an/aus“/s auf der Leitung
  - Verschlüsselung darf nicht der Flaschenhals sein
    - Schlüsselaushandlung (Elliptische Kurven)
    - Schlüsselerzeugung
    - Ver- und Entschlüsselung
  - Software benötigt Millisekunden
  - Hardware verschlüsselt in Mikrosekunden

- Computer kennen keinen echten Zufall

- Physischer Manipulationsschutz

Original

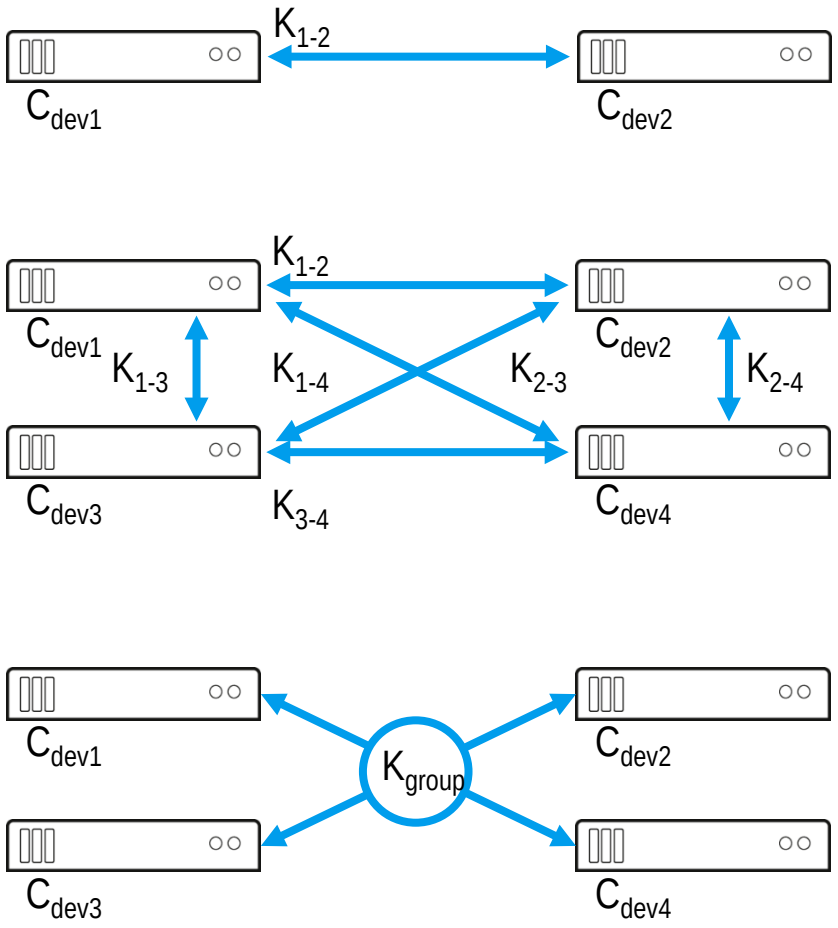
Schwache Verschlüsselung



Starke Verschlüsselung

4. Wahrheit: Schlüsselgenerierung und –Verwaltung wird schnell komplex

- Sicherheit basiert auf einer Vielzahl von Schlüsseln
  - Individuelle Geräte-Zertifikate (C_{dev}) zur Authentisierung und Schlüsselableitung
  - Sitzungsschlüssel (K_{1234}) zwischen zwei Kommunikationspartnern
  - Gruppenschlüssel (K_{group}) durch Key Server
- Anforderung:
  - Automatisiertes Schlüsselmanagement
  - Verzicht auf Single-Point-Of-Failure



5. Wahrheit: Nicht jede Zertifizierung garantiert das erforderliche Sicherheitslevel

- Security Compliance erfordert zertifizierte Lösungen
  - Datenschutz, TKG, GDPdU
  - BSI Grundschutz, Geheimschutz (VSA)
  - Basel II & III, Sarbanes-Oxley Act (SOX)

- Zertifizierung bestätigt definierte Schutzziele („Security Targets“)
  - Große Vielfalt (z. B. Common Criteria, FIPS, nationale Zulassungen)
  - Entspricht das Schutzziel dem Einsatzzweck?

- Qualitätskriterien für Zertifizierungen
  - Echte Zufallszahlen zur Schlüsselgenerierung
  - Regelmäßige Überprüfung der Kryptografie
  - Obligatorischer Manipulationsschutz

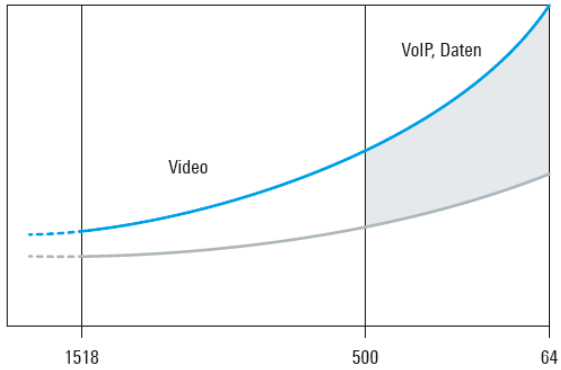
Benchmark für Verschlüsselungslösungen

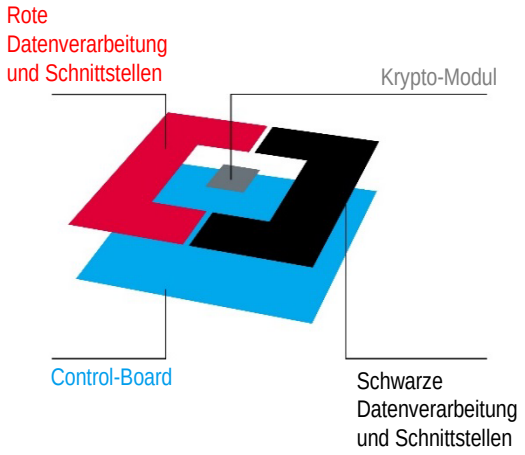
Sicherheit und Overhead?	• Konfigurierbarer Trade-Off zwischen Sicherheit und Overhead
Integrierte Verschlüsselung?	• Verschlüsselung von Netzwerkknoten (Router/Switche) trennen
Sicher und Performant?	• Spezialisierte Appliance mit gehärteten Krypto-Mechanismen
Schlüsselgenerierung und –Verwaltung?	• Automatisiertes und auditierbares Schlüsselmanagement
Zertifikat?	• Schutzziele für Einsatzzweck prüfen

Nächste Generation von Verschlüsselungsgeräten

R&S®SITLine ETH setzt neue Standards

Geringster Overhead	• Nur 5 Byte Overhead für GCM Transport (zzgl. 16 Byte Integrität)
Profi-Equipment	• Neueste kryptografische Methoden und Standards
Moderne Plattform-Architektur	• Saubere Rot-Schwarz-Trennung
Voll-Automatischer Krypto-Betrieb	• Selbstheilendes Management
Bestätigte Sicherheit	• BSI-Zulassung • CC EAL4+ Zertifizierung*





Leitungs- und Netzwerk-Verschlüsselung mit 40 Gbit/s

R&S®SITLine ETH40G

- 40 Gbit/s in nur einer Höheneinheit
- Maximale Bandbreiteneffizienz
- Geringste Latenz

Höchste Performance

- Sitzungsschlüssel mit hoher Entropie
- Starke 2-Faktor-Authentisierung durch Passwort und Token
- Manipulationsresistente Geräte

Wirksame Verschlüsselung

- 100 Watt Nennleistung, 90% Wirkungsgrad
- Weniger Strom und weniger Abwärme
- Optimiert für Kaltgangseinhausungen

Green IT

- 99,9975% Verfügbarkeit (höchste MTBF)
- Im Betrieb wechselbare Netzteile, Lüfter und Batterien
- Automatischer Krypto-Betrieb

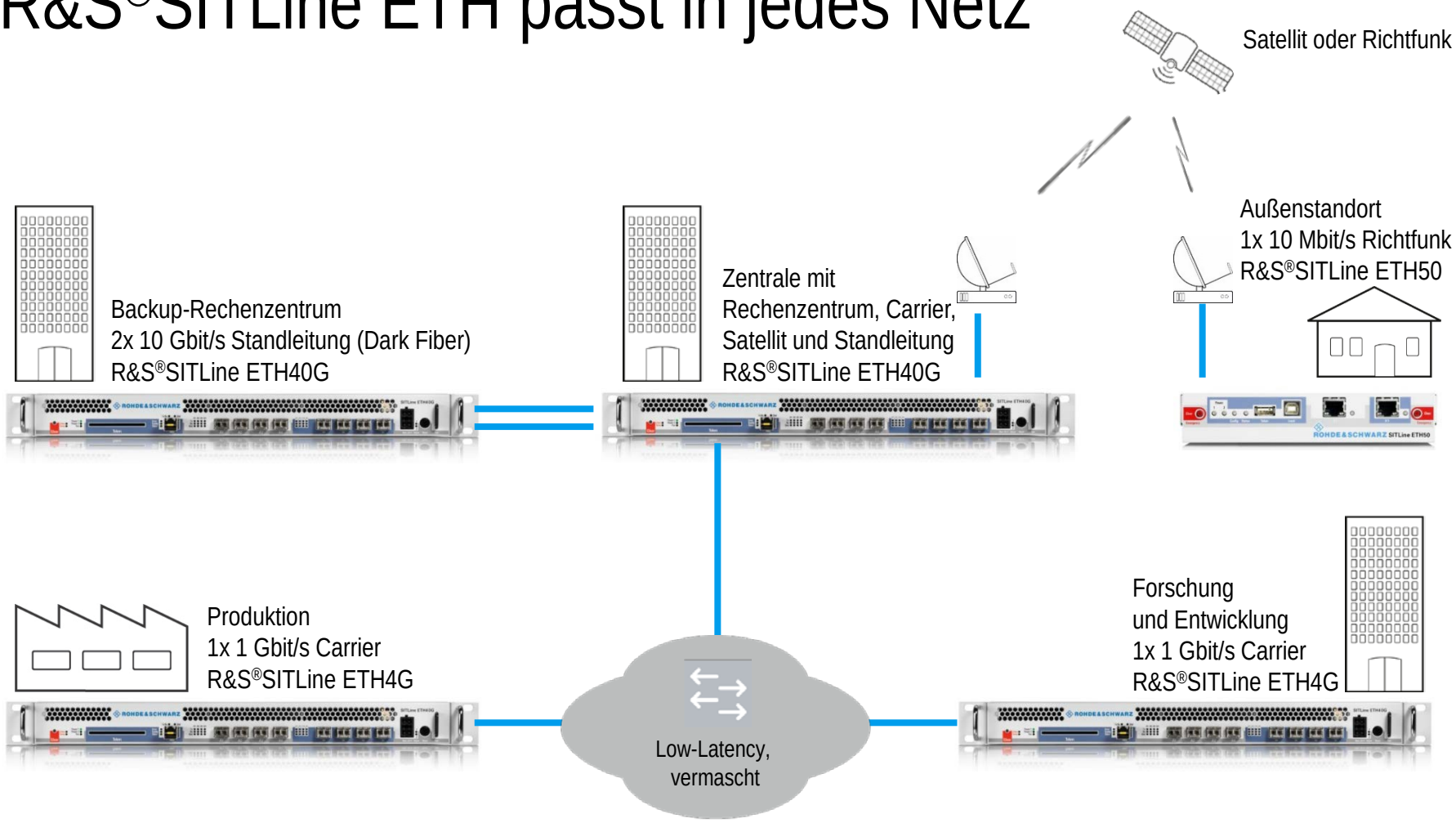
24x7 serienmäßig

DEUTSCHER RECHENZENTRUMSPREIS 2015

DEEP TECH AWARD 2015

Ethernet-Verschlüsselung für alle Bandbreiten

R&S®SITLine ETH passt in jedes Netz



Mehr Infos?

Besuchen Sie Rohde & Schwarz in Halle 6/G16

- Rohde & Schwarz Application Notes
  - Ethernet-Standleitungen
  - Rechenzentrumsanbindung
  - Leitungs- und Netzwerk- Verschlüsselung mit 40 Gbit/s
- Evaluationshilfe für Ethernet-Verschlüsseler
  - Erschienen auf www.inside-it.ch
- Internetworking Perspectives
  - Web Blog von Ivan Pepelnjak
  - http://blog.ipspace.net/

Starke Ende-zu-Ende-Verschlüsselung für Ethernet-Standleitungen

R&S®SITLine ETH schützt ohne Durchsatzeinbußen gegen Abhören und Manipulieren.

Zur Bewältigung der an allen Standorten wachsenden Informationsflut ist eine hoch performante Kommunikationsinfrastruktur erforderlich. Zugleich sollen die übertragenen Daten gegen Manipulation und Abhören durch unautorisierte Dritte geschützt werden. Dies erfordert eine starke Ende-zu-Ende-Verschlüsselung, die jedoch die Leistungsfähigkeit des Netzwerks nicht einschränken darf. Die Verschlüsselung muss sich mit Sicherheitsmanagement, Durchsatz und Verfügbarkeit nahtlos in die vorhandene WAN-Infrastruktur integrieren. Ausserdem muss sie mit knappen IT-Budgets zu betreiben sein.

Ethernet-Standleitungen – die wirtschaftlichste Lösung für steigende Datenmengen

Ethernet-Standleitungen sind eine leistungsstarke und kostengünstige Technologie, um verteilte Standorte mit 100 Mbit/s, 1 Gbit/s oder sogar 10 Gbit/s in das Backbone einzubinden. Große Distanzen werden mit minimaler Latenz überbrückt, so als ob die Niederlassung am Etagen-Switch der Zentrale angeschlossen wäre. Davon profitieren Anwender und Administratoren gleichermaßen: Applikationen können mit Echtzeitzugriff zentral und kostengünstig als Private Cloud angeboten werden. Die hohe Sprach- und Bildqualität abhörsicherer Videokonferenzen motiviert jeden einzelnen Mitarbeiter und sichert die Akzeptanz dieser Technologie. Auch bandbreiten- und latenzsensitive Backup-Szenarien sind auf einfache Weise möglich.

R&S®SITLine ETH schützt Ihre Daten – hoch performant und zugelassen

R&S®SITLine ETH verschlüsselt komplette Ethernet-Standleitungen oder einzelne VLANs, ohne die Übertragungsleistung merklich zu beeinflussen. Zur Verschlüsselung mit AES256 erzeugt R&S®SITLine ETH unvorhersagbare Schlüssel. Der Zufallszahlengenerator wurde nach Common Criteria Stufe EAL4+ zertifiziert. Die zusätzliche, zertifikatsbasierte Authentisierung der R&S®SITLine ETH-Geräte unterbindet wirksam sogenannte Man-in-the-Middle-Angriffe. R&S®SITLine ETH ist vom Bundesamt für Sicherheit in der Informationstechnik (BSI) geprüft und zugelassen.

Ihre Anforderung

In hart umkämpften Märkten werden Wettbewerbsvorteile nur durch schnelle und zielgerichtete Kommunikation errungen. Videokonferenzen und Private-Cloud-Anwendungen ermöglichen den Austausch geschäftskritischer Informationen und sichern die schnelle Reaktionsfähigkeit von Organisationen. Insbesondere Unternehmen mit geografisch verteilten Standorten stellt dies vor eine Herausforderung.

You act. We protect.
Rohde&Schwarz SIT:
Verschlüsselung und IT-Sicherheit.

ROHDE&SCHWARZ

Sichere Kommunikation
Application Card | 01.01
Starke Ende-zu-Ende-Verschlüsselung für Ethernet-Standleitungen

Echtzeit-Ethernet-Verschlüsselung mit 40 Gbit/s
R&S®SITLine ETH