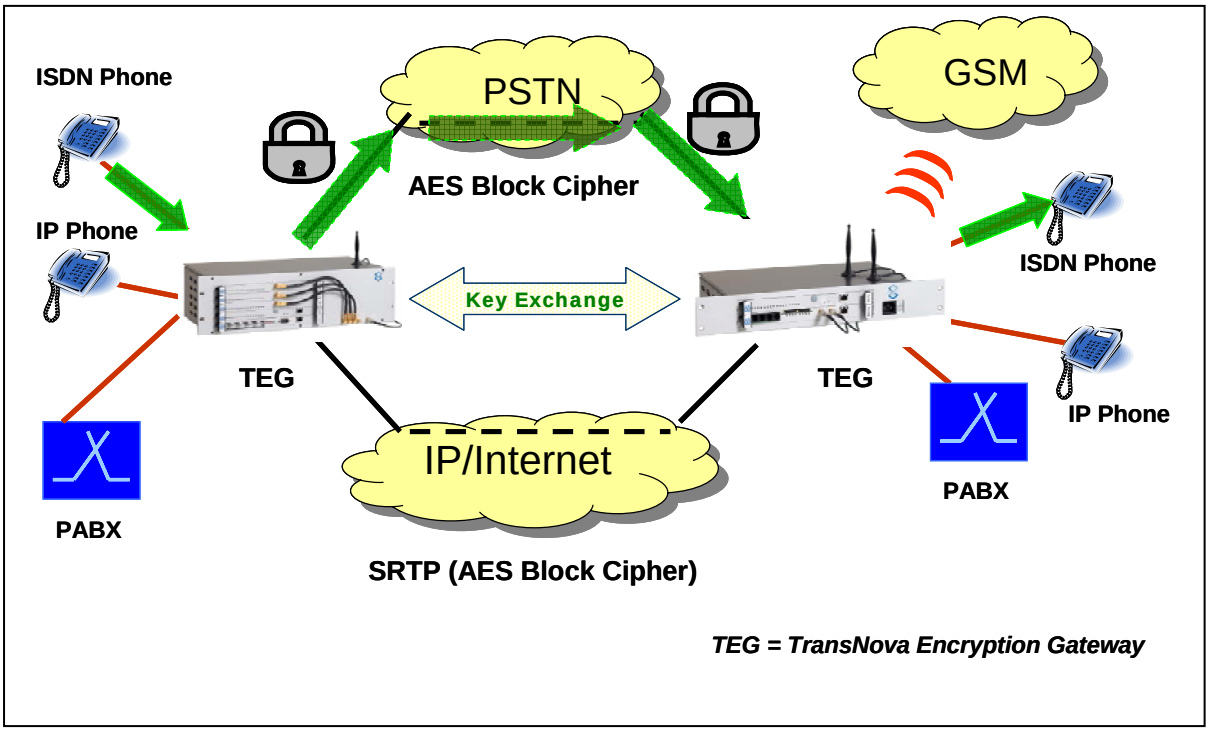
TEG (TransNova® Encryption Gateway)

Sichere Verschlüsselung in ISDN und IP Netzen



Problemstellung:

Die zunehmende Vernetzung der geschäftlichen und privaten Kommunikation bietet ideale Angriffspunkte für Mithörer und Spione und führt demzufolge zu einem drastischen Anstieg illegaler Angriffe auf Telefon– und Datennetze. Die Angriffe auf die vertraulichen Daten erfolgt dabei sowohl innerhalb der Unternehmen als auch außerhalb. Der wirtschaftliche Schaden, der durch das Ausspionieren von vertrauenswürdigen Daten und Telefongesprächen entsteht, ist sehr groß. Abhilfe kann hier nur durch eine Verschlüsselung der Daten und Telefongespräche geschaffen werden.

Lösung: TEG (TransNova® Encryption Gateway)

Zur Lösung dieses Sicherheitsproblems wurde aus der erprobten TransNova® Produktfamilie das TransNova Encryption Gateway TEG entwickelt, das eine sichere Ende-zu-Ende Verschlüsselung sowohl für ISDN-Verbindungen als auch für Verbindungen über IP herstellt. Hierbei können sowohl einzelne S_0 (BRI) Verbindungen als auch S_{2M} (PRI) mit 30 B-Kanälen verschlüsselt werden.

Verschlüsselung und Schlüsseltausch

Die Verschlüsselung wird nach dem AES Verschlüsselungsverfahren durchgeführt, das international standardisiert und von der NIST (National Institute of Standards and Technology) in den USA als besonders sicher anerkannt wurde. Hierbei handelt es sich um eine so genannte symmetrische Blockverschlüsselung mit fester Blockgröße von 128 Bit und variabler Schlüsselgröße von 128, 192 bzw. 256 Bit.
Der AES Verschlüsselungsalgorithmus zeichnet sich sowohl durch eine sehr hohe Sicherheit als auch durch eine sehr hohe Leistungsfähigkeit aus, was sehr kurze Durchlaufzeiten

ermöglicht. Der asymmetrische Schlüsseltausch erfolgt nach dem Diffie-Hellman (DH) Verfahren entsprechend dem Multimedia Internet Keying Standard (MIKEY, RFC 3830). Beide Verfahren werden als extrem sichere Prozeduren angesehen. Die Nutzung von RSA für den asymmetrischen Schlüsseltausch mit Public Key Infrastrukturen ist nach Bedarf vorgesehen.

TransNova® Encryption Gateway bietet größtmögliche Flexibilität

Das TransNova® Encryption Gateway (TEG) führt die Verschlüsselung in der Hardware durch, weshalb sehr kurze Verarbeitungszeiten gewährleistet werden können. Durch die genormten Schnittstellen können sowohl Nebenstellen mit S_{2M} (PRI) als auch einzelne Telefone angeschlossen werden. Im TEG können sowohl ISDN Verbindungen, als auch IP Verbindungen (SRTP) mit AES verschlüsselt werden. Die Verschlüsselung kann sowohl für bestimmte Quell- bzw. Zielrufnummern nach einem konfigurierbaren Rufnummernplan, oder aber durch Voranstellen einer freidefinierbaren Zifferkombination (Präfix) erfolgen.

Das TransNova Encryption Gateway ist sowohl als Einzelsystem verfügbar, das in das bestehende Unternehmensnetz durch einfaches Dazwischenschalten in die bestehende ISDN oder IP Verbindung integriert werden kann, als auch als zusätzliches Modul, welches in schon bestehende Systeme der TransNova Familie (TMG,TMN) eingebracht werden kann.

Zusammenfassung:

Anwendungen
- Verschlüsselung von Sprach- und Datenverbindungen.
- Verschlüsselung von Videokonferenzen.

Kunden
- Kleine, mittlere und große Unternehmen
- Carrier
- SOHO, Home Office mit Anbindung an die Unternehmenszentrale

Verschlüsselung
- AES (Advanced Encryption Standard) mit fester Blocklänge (128 Bit) und variabler Schlüssellänge von 128, 192 und 256 Bit.
- Verschiedene Varianten für SRTP.

Berechnung der Prüfnachrichten - Hashing (HMAC usw.)
- Algorithmen: SHA-1, SHA-2 usw.

Schlüsseltausch
- Asymmetrischer Schlüsseltausch: Diffie-Hellman (DH) für „Pre-Shared Key“, RSA für „Public Key“ usw.
- Protokollablauf: MIKEY (mit gängigen Modifikationen).

Flexibilität
- Verschlüsselung für einzelne S_0 / BRI wie auch für S_{2m} / PRI mit 30 B-Kanälen.
- Verschlüsselung anhand der Quell- bzw. Zielrufnummer (Rufnummernplan) oder individuell durch das Voranstellen einer konfigurierbaren Zifferkombination.
- Encryption Gateway als Einzelgerät oder innerhalb der TransNova Produktfamilie als Einzelmodul einsetzbar.