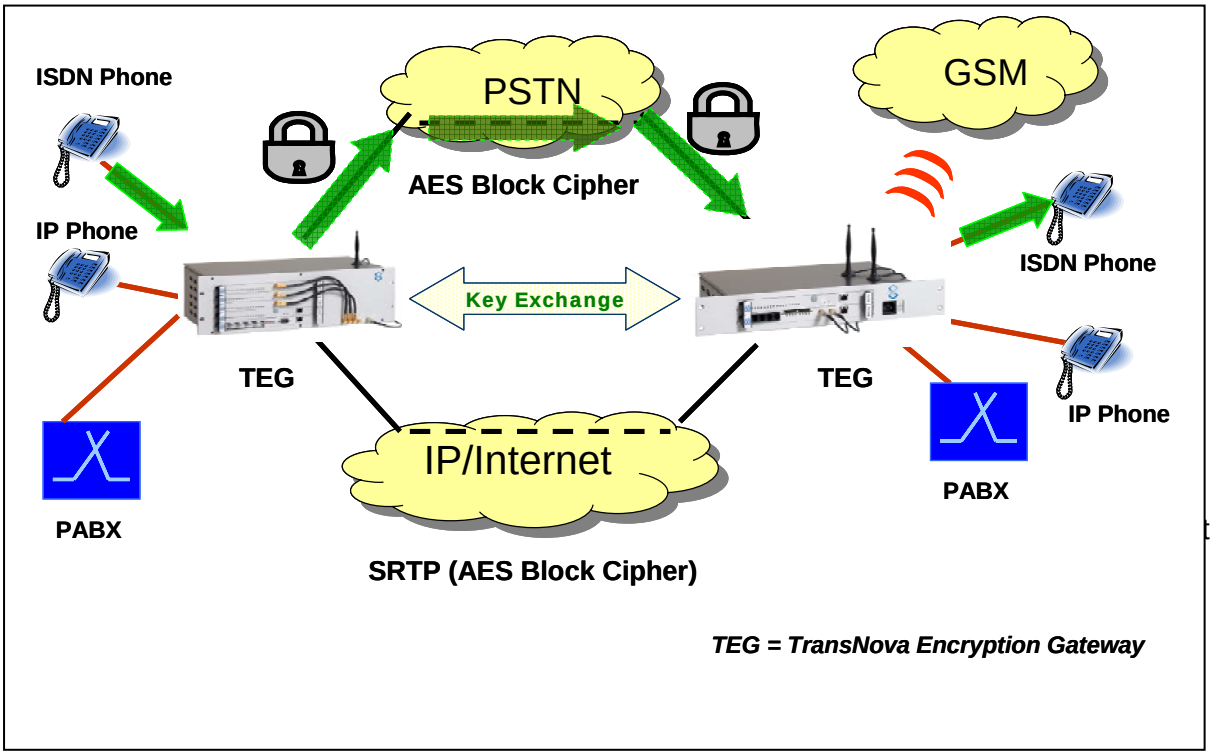
TEG (TransNova® Encryption Gateway)

Secure Encryption in the ISDN and IP Networks



Encryption and Key Exchange

The encryption is accomplished to the AES coding procedure, which was internationally standardized and recognized by the NIST (National Institute of Standards and Technology) in the USA as particularly safe.
Here it concerns a symmetrical block coding in such a way specified with firm block size of 128 bits and variable key size of 128, 192 and/or. 256 bits.
The AES coding algorithm is characterised both by a very high security and by a very high efficiency, which makes very short turn-around times possible.
The asymmetrical key exchange takes place on the Diffie Hellman (DH) procedure according to the Multimedia Internet Keying standard (MIKEY, RFC 3830). Both procedures are regarded as extremely safe.
The use of RSA for the asymmetrical key exchange with Public key infrastructures can be used as per requirement.

TransNova® Encryption Gateway offers greatest possible flexibility

The TransNova® Encryption gateway (TEG) accomplishes the encryption within the hardware, this is the reason that very short working times can be ensured.
With the standardized interfaces, both S2M (PRI) and individual telephones can be connected. In the TEG both ISDN connections, and IP connections (SRTP) can be encrypted with AES.

NovaTec Kommunikationstechnik GmbH
Technologiepark 9 * D-33100 Paderborn
www.novatec.de
info@novatec.de
Phone: +49 (0) 5251-1589-610
Fax: +49 (0) 5251-1589-611

The encryption can take place both for defined extensions and/or target called numbers with a configurable call numbering plan, or via placing a free-definable number combination (prefix) in front.

The TransNova Encryption gateway is available both as a separate system, which can be integrated into the existing enterprise network by simple insertion in the existing ISDN or IP connection, or as an additional module, which can be brought into already existing systems of the TransNova family (TMG, TNM).

Summary:

Applications

- Encryption of speech and data connections.
- Encryption of Video Conferencing.

Customers

- Small, Middle and Large Enterprises
- Carrier
- SOHO, Home Office with connection to the company headquarters

Encryption

- AES (Advanced Encryption Standard) with firm Block sizes (128 Bit) and variable Key lengths from 128, 192 and 256 Bit.
- Different variants for SRTP.

Computation of the test reports - Hashing (HMAC etc.)

- Algorithims: SHA-1, SHA-2 etc.

Key Exchange

- Asymmetrical Key Exchange: Diffie-Hellman (DH) for „Pre-Shared Key“, RSA for „Public Key“ etc.
- Protocol Expiration: MIKEY (with usual modifications).

Flexibility

- Encryption for individual BRI as also for PRI with 30 B Channels.
- Encryption on the basis of the extensions and/or target numbers (call numbering plan) or individually by placing a configurable number combination in front (Prefix)
- Encryption Gateway available as an individual unit or as a module for already existing products in the TransNova Product Family.