R&S®Secure Gateway

End-to-end encryption for secure fax and voice communication

R&S®Secure Gateway provides secure end-to-end authentication and encryption for any fax device or analogue phone.

Protect your critical fax or voice communication from espionage and manipulation

Insufficient protection against eavesdropping and manipulation leads to loss of sensitive data and industrial espionage causing substantial damage. Telephone and facsimile services on connection-oriented networks – still the most widely deployed communication medium – are particularly exposed to attacks.

Therefore, it is essential to secure fax devices and phones in order to protect sensitive information from unauthorized access, espionage and sabotage.

R&S®Secure Gateway provides end-to-end authentication and encryption as a front-end device to any analogue fax machine or phone.

Performance without compromises

R&S®Secure Gateway works independently of the connected fax device or phone without reducing performance. In facsimile mode R&S®Secure Gateway acts as a store and forward device. The encrypted data is transmitted at full V.34 speed of 33,6 kbit/s over PSTN lines.

R&S®Secure Gateway supports analogue lines (PSTN) and IP transmission (Fax/Voice over IP). Operation over IP-network requires an IP-PBX that acts as a SIP-Server and manages registration of the R&S®Secure Gateways in the IP network.

ROHDE&SCHWARZ
Cybersecurity

Product Flyer | 02.00

Strong end-to-end encryption

A separate key Management Station provides for the generation and distribution of X.509 certificates. It creates an individual asymmetric long-term EC key with a key length of 384 bit directly on an USB-based tamper-proof smart card device (Crypto Token). This key is used solely for authentication. Thus, the private key never leaves the crypto token. The corresponding public key is signed by the Certification Authority generated on the Management Station. Resulting X.509 certificate as well as CA certificate are stored on the crypto token.

Each R&S®Secure Gateway is able to authenticate other devices by verifying if the signature comes from the CA created on the Management Station. Its respective counterpart can decrypt fax or voice message and verify its integrity. The symmetric key material for the line encryption is generated for each new fax or voice session by performing an Elliptic Curve Ephemeral Diffie-Hellman key exchange implemented as part of the Secure Communication Interoperability Protocol. A SHA512 hash function assures authenticity of certificate signatures. Data is encrypted with AES256 in Galois Counter Mode providing Authentication, Integrity and Confidentiality of transmitted data.

In IP mode, connection between R&S®Secure Gateway and the IP-PBX is secured by using TLS v1.2 with mutual authentication. Required certificates and necessary network configuration are generated on the Management Station. R&S®Secure Gateway employs Full Disk Encryption using keys generated on TPM v1.2.

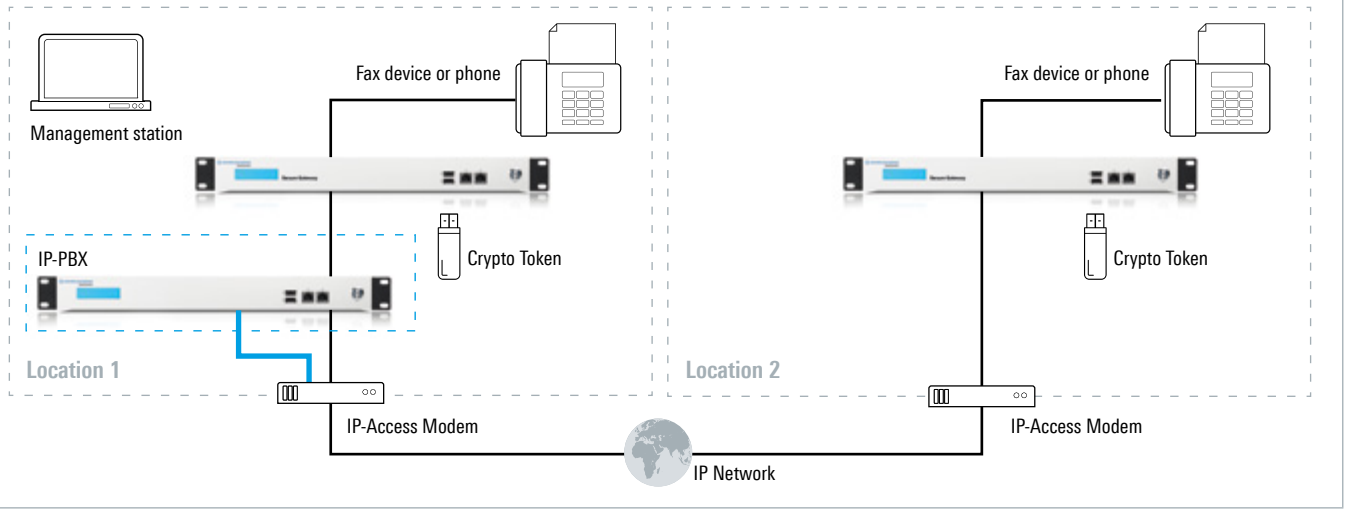
Features

Communication	▪ Fax transmission according to CCITT /ITU G3 recommendation ▪ V.34 modem supports up to 33,6 kBit/s ▪ encrypted communication over analogue lines PSTN) and Internet Protocol (IP)
Key exchange and perfect porward secrecy	ECDHE (secp384r1) implemented as part of the SCIP protocol
Symmetric encryption (AEAD)	AES256 GCM
Authentication	▪ ECDSA (secp384r1) ▪ X.509based certificates with SHA-512 signatures
Random key generation	▪ Hardware based random key generator (long term key) ▪ Built-in security module
Key management	Certification Authority / PKI supported management system

Specifications

Processing unit	
Dimensions	432 x 212 x 44 mm (19'', 1 HU)
Interfaces	1 x analogue line 1 x Ethernet 100BaseT
Storage	Internal Compact Flash Memory
Power supply	Internal 115 - 220V

System overview for secure voice & fax over IP



Rohde&Schwarz Cybersecurity GmbH
Muehldorfstrasse 15 | 81671 Munich, Germany
Info: +49 30 65884-222
Email: cybersecurity@rohde-schwarz.com
www.cybersecurity.rohde-schwarz.com

Rohde&Schwarz GmbH&Co. KG
www.rohde-schwarz.com

PD 5215.3691.32 | Version 02.00 | April 2018 (sch)
R&S®Secure Gateway
Data without tolerance limits is not binding | Subject to change

5215369132

5215.3691.32 02.00 PDP 1 en