

Sirrix.CryptoGateway

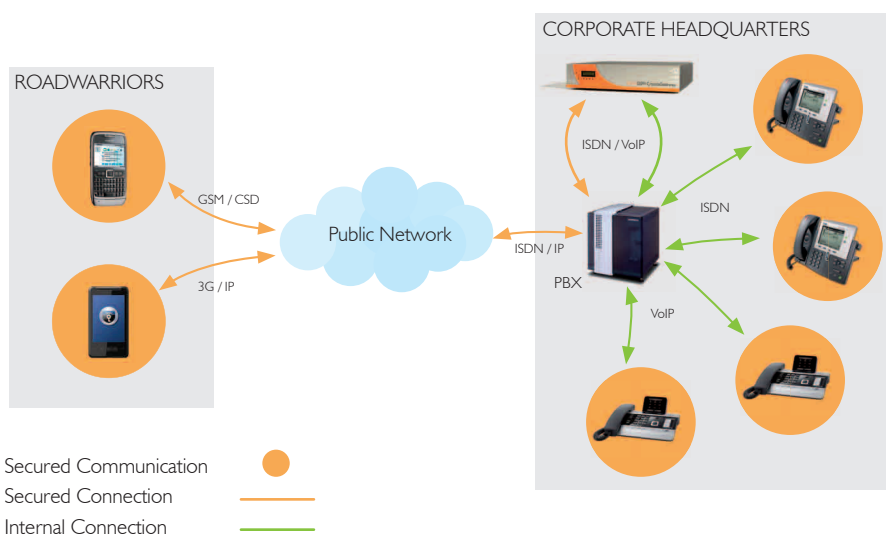
Secure encrypted mobile communication with VoIP- and ISDN based landline phones

Illegal wiretapping poses ever bigger risks to the confidentiality of voice communication, as the respective technical effort has even become less complex with the advent of Voice over IP (VoIP) and mobile networks. So-called IMSI-catchers are available on the market which fake a base station towards a mobile phone and can thus be used for a man-in-the-middle attack. Other attackers focus directly on the internal network of a mobile provider to catch many more calls as they pass the respective switches. This danger becomes especially very real when road warriors travel in less secure or trustworthy areas around the world.

Up to now, the market predominantly offered isolated stand-alone products for voice encryption in one single network that required identical, specialized end user devices. This has constrained the broad and easy use of such technology. Hence the Sirrix.CryptoGateway combines secure mobile communications with existing land line devices based on VoIP or ISDN technology. The CryptoGateway connects encrypted calls between secure mobile phones and any

standard phone set acting as an extension of a private branch exchange within an organisation. This ensures that outsiders are always faced with fully encrypted voice calls while at the same time ensuring that any extension within the organisation can be used to communi-

te with secure mobile phones. This effectively prevents unsecure connections via the mobile or public fixed telephone network.



All of an organisation's staff that needs to communicate confidential information can be equipped with a secured mobile phone for encrypted communications both mobile to mobile as well as mobile to headquarters back home. Users at headquarters can leverage their existing standard phone sets (VoIP, ISDN or analogue). Moreover, fully encrypted multi-party telephone conferences are possible as well.



Sirrix. CryptoGateway

- Seamless encryption between mobile and landline phones
- Secure Conferencing
- Up to 30 simultaneous Calls

Technical Specifications

Interfaces

- 4x ISDN basic rate interfaces
- alternatively 2x ISDN primary rate interfaces
- All ISDN channels can be configured as either encrypted for external or clear for internal communication
- alternatively 2x mobile ports (SIM-cards to be provided by customer)
- alternatively 2x analogue modem ports
- 1 x 1 Gbit/s VoIP port for SIP / RTP

Mobile Communication

- GSM Circuit Switched Mode (ISDN V.110 or analogue V.32 resp.)
- 3G IP connection mode
- optimized audio compression (CELP-Codec with 8 kHz)

Crypto function

- 4096 Bit Diffie-Hellmann key exchange
- 256 Bit encryption with AES and Twofish in counter mode
- Preshared key authentication
- FIPS 140-2 certified cryptokernel
- BOS-D compliant crypto chip

Conference function

- up to 30 simultaneous mobile encrypted calling/called parties
- up to 60 simultaneous internal calling/called parties
- several individual or conference calls in any mixture simultaneously possible

Models

CGW Entry
(I4/S4/M2/G2)

CGW BRI
(M)

CGW PRI
(E10/E20/E30)

System

CPU	1,6 GHz Intel Atom	2,66 GHz Intel Core i5 Quad	2,66 GHz Intel Core i5 Quad
RAM	2 GB	2 GB	4 GB
Persistent Storage	2 GB solid state disk	2x 250 GB Raid-1 hard disk	2x 250 GB Raid-1 hard disk
ISDN-Modul with HW-DSP	-	YES	YES
Dimensions	340 x 220 x 100 mm	425 x 390 x 90 mm	425 x 390 x 90 mm

External Interfaces (encrypted)

BRI-ports	- / 4 / - / -	4	-
PRI / E1-ports	-	-	2
Analogue ports (V.32)	- / - / 2 / -	-	-
GSM-ports	- / - / - / 2	-	-
Crypto channels	4 / 4 / 2 / 2	8	10 / 20 / 30
Ethernet port for VoIP	1 Gbit	1 Gbit	1 Gbit

Internal Interfaces (clear)

BRI-ports	- / 4 / - / -	4	-
PRI / E1-ports	-	-	2
Ethernet port for VoIP	1 Gbit	1 Gbit	1 Gbit

Features

Conferencing	up to 8 participants	up to 32 participants	up to 60 participants
Crypto channels retrofittable	-	-	up to 30
On-board TPM	Infineon 1.2	Infineon 1.2	Infineon 1.2
Ethernet port for management	100 Mbit	100 Mbit	100 Mbit