



PSTN Encryption HC-2203

The telephone is probably the most often tapped means of communication in the world. When you talk with someone on the phone, the confidentiality of the information you communicate is not guaranteed. You can consistently eliminate this information risk by using End-to-End Encryption (i.e. from phone set to phone set). The PSTN Encryption HC-2203 from Crypto AG is the world's simplest and most reliable high-security solution for this purpose.

The PSTN Encryption HC-2203 is virtually a plug-and-play application. Simply connect the unit between your phone set and phone socket and you can call from then on at the press of a button to anyone else with the same setup, anywhere in the world. There is no need for you to be concerned about the transmission network through which your call is routed provided the whole connection is transparent to data modem signals (as in conventional PSTN networks). The system is even robust enough to tolerate up to two satellite hops in each direction of the connection. However in case of difficult network conditions there are many hardware and software settings (e.g. signal levels, operating modes) available and a built-in monitor tool e.g. to assess the signal quality on the line. These features allow you to fine tune the unit to the network requirements.

A special remote control feature allows a secretary to setup a call, and switch this through to the VIP only after the connection has been established in cipher mode. The same setup is also used to allow a small local user group to share a unit.

The PSTN Encryption unit is compatible with all types of analogue telephone. The encryption does not interfere with audio quality or speaker identification. If you

also operate Secure GSM telephones from Crypto AG in your network, inter-network compatibility is assured, end-to-end. In other words, you can phone these cell users without fear of your call being tapped. The built-in modem offers you the additional option of encrypted data communication. The cryptographic Security Architecture of Crypto AG provides the best protection for your confidential information. Digital encryption is performed in a separate tamper-proof hardware encryption module, where information and security data cannot be read-out mechanically or electrically. The cipher key for your current call is chosen and calculated automatically in one of three possible methods. Each focuses on different operational or security requirements: The classic direct symmetrical, the derived symmetrical or the asymmetrical call key methods.

The central Key Handling Centre KHC-2000 is available to you for key distribution (online or offline) and for the management of all security parameters. With this centre, you can also set up crypto-groups with authorisation to interact. They can be overlapping and/or hierarchical, as required by your organisational structure.

Key features

- Digital desktop end-to-end cipher unit for your high-security worldwide telephone communications in PSTN networks with transition capability to GSM networks
- Practically no degradation of audio quality and speaker identification
- Robust protection of voice and data communication even in networks with reduced or special transmission quality (e.g. SatCom)
- Simple installation by merely connecting the unit between your phone set and phone socket
- Simple operation; encryption at the press of a button
- Encryption is performed in a tamper-proof hardware module with secret algorithms profiled by your security manager
- Supports other security elements such as emergency clear and blacklist factory reset
- Finely scalable key distribution concept (online/offline) for convenient security management regardless of network size
- Compatible with Secure GSM HC-24x3

General data

Voice quality aspects

- Good speaker recognition
- Immune to background noise
- Supports various bitrates
- Independent of language
- Quality not affected by male or female voice

Operation modes

Voice:

- Plain (bypassed)
- Encrypted voice full duplex (2400...9600 bps)

Data:

- Transparent data channel 2400...19200 bps with RTS/CTS

User interface

Keyboard:

- 4 x 3 numeric/alphanumeric keys
- 1 plain/Crypto control key
- 2 cursor and 2 softkeys

Display:

- Backlit LCD 4 lines x 20 characters
- 3 status LED

Transmission principle

- Line modems: V.34, V.32bis, V.22bis
- Modem speeds: 2400...19200 bps
- Synchronisation time: 15 sec typ.

Types of networks

- Classical PSTN
- Leased line
- Military tactical area network (conditional)
- Satellite network (2 hops)

Provided channel is a transparent.

Line interface

- Connector: RJ-11

Line impedance:

- Complex: 200 ohm + 820 ohm/115nF
- Real: 600 ohm

Bandwidth:

- 390...3200 Hz (nominal)
- 500...2400 Hz (minimal)
- Transmit level: -9...-21 dBm
- Receive level range: 0...-46 dBm

Phone interface

- Connector: RJ-11
- Line impedance: 600 ohm

Data interface

- Configuration: RS-232, DCE, 25 S
- Speed: 2400...57'600 bps
- Mode: asynchron 8N1

Auxiliary interface

- Software update

Safety

- EN 60950

Power supply

- 10...36 V dc

Power consumption

- Max. 15 VA

Reliability

- MTBF: 100,000 hrs
- MTTR < 1,5 hrs

Dimensions

- 220 x 215 x 70 mm L/W/H

Weight

- 1.98 kg
(incl. batteries, without AC power supply)

Test

- Permanent built-in selftest
- Security monitor

Cryptographic data

Algorithm

- HCA-480, customer-specific cipher algorithm
- Customer managed profiling of algorithm by CMP with variety > 10⁵⁰⁶

Key calculation method

- Symmetric direct, derived
- Asymmetric

Key variety

- Communication key (CK) variety: 2¹²⁸
- Key stream period: > 10²⁸ years

Key memory

- 999 communication keys

Access protection

- Tamper-proof security module
- Password protection

Management

- Online downline loading of communication keys, blacklist and security parameters from Key Handling Centre KHC-2000
- Cloning with smart card
- Manual key management via keyboard

Clear functions

- User clear for communication keys
- Emergency clear
(powered by internal battery)
- Remote clear via blacklist
- Factory reset

Environmental data

- Operating temperature: -10 °C...+50 °C
- Storage temperature: -25 °C...+70 °C
- Humidity: 95 % (RH) at +50 °C
- Vibration: 1 g effective, 10...500 Hz (random)
- Shock: 15g, 6 ms

Approvals

- Marking: CE (European conformity)
- Safety: EN 60950
- Quality assurance: ISO 9001:2000
- Telecommunications: CTR 21 incl. all advisory notes

Accessories/options

- AC power supply: 90...264 Vac
- Data cables: data transfer cable (optional)

Telephony Systems

