Using PSTN Encryption HC-2203 over BGAN

Version 1

3 September 2009

inmarsat.com/bgan

Contents

1 Overview

Inmarsat BGAN offers the same telephony services as its predecessor system GAN, namely Standard Voice (compressed), ISDN Data and the Audio 3.1kHz service which can be used for fax and data communication. Audio 3.1 kHz also enables digital PSTN telephony encryption.

Telephone and voice connections can be tapped. The risk increases even more when “quasi-open” satellite links are used which are generally easy to intercept. On BGAN links (radio transmission from and to the satellite) encryption takes place, however, it is only in the UMTS standard (Kasumi algorithm), which is not sufficient for high-security applications. In addition, this encryption may be switched off when technical problems arise on this link – which even further increases the risk of interception. Furthermore, if a fax is connected to the PSTN, the terrestrial portion of the connection is not protected!

1.1 PSTN encryption explained

In order to protect the entire transmission (i.e. from the BGAN link as well as the fixed network portion from the ground station to a recipient at headquarters, for example), reliable end-to-end encryption is required. This is available through PSTN Encryption HC-2203 from Crypto AG, which has been validated for BGAN and which is widely used throughout the telecommunications industry.

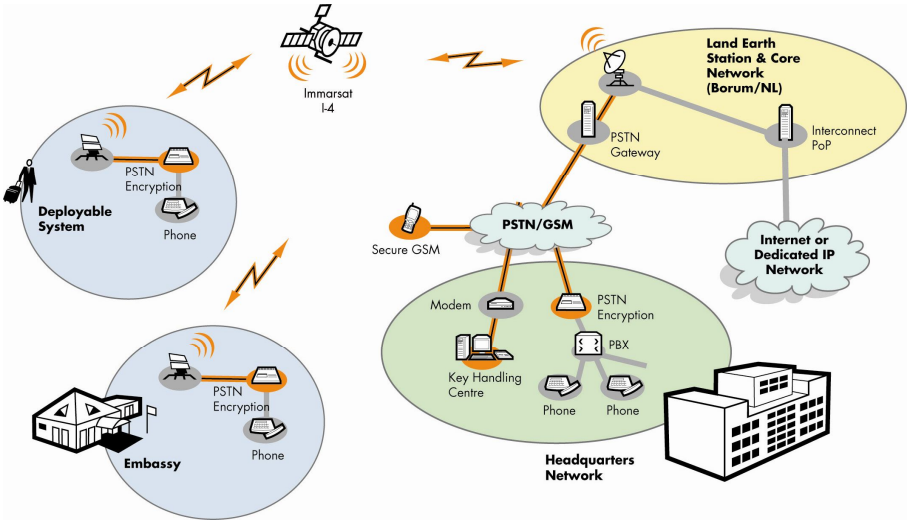
PSTN Encryption HC-2203 uses state-of-the-art modems that can cope with even the most difficult channel conditions and with up to two satellite hops (i.e. sat/sat connections). This ensures robust and secure telephone connections via BGAN links.

In addition to the PSTN Encryption unit, Crypto AG also offers a compatible unit for mobile networks (Secure GSM) which enables secure end-to-end telephony with GSM users. Crypto AG also offers an all-in-one solution in a portable case, containing a BGAN terminal, a telephone, and an encryption unit. Secure telephony via BGAN satellite is now a reality, even from remote areas.

2 Typical users

The security architecture implemented in all encryption solutions from Crypto AG (containing customer-specific algorithms and hardware-based encryption) is the perfect choice for users with highest security requirements. Typical user scenarios are:

- Governments/ministries involved in high-level negotiations, often requiring immediate access to secure telephone lines from practically any location abroad
- Diplomatic staff needing to establish a secure telephone connection when travelling without risk
- Border guards wanting to establish secure connection to the operations centre from remote areas, such as mountains, quickly and easily
- Ministries of the Interior wanting to correspond securely to all connected authorities
- A tap-proof satellite connection to the HQ, established from military vehicles within only a few seconds



The satellite terminal in the embassy might be a Thrane & Thrane EXPLORER 700, which HAS A detachable antenna that can be placed up to 100 m away from the modem and attached to a mast. The more sensitive modem is operated indoors.

There is a Deployable Secure BGAN Satellite Systems from Crypto AG which consists of an easily deployable case with integrated satellite communication, application and encryption equipment. The Deployable System uses an EXPLORER 500, which supports the Audio 3.1kHz service. This system has proven very reliable in terms of operation and availability.

3 Key features

- Highly secure, robust, digital telephony encryption of PSTN connections, tried and tested for use over BGAN satellite links
- Customer-specific algorithms and encryption processes in a tamper-proof hardware module
- Simple operation – change between plain and crypto at the push of a button
- Users do not need prior security knowledge
- Very good voice quality and recognition
- Encrypted data exchange via data port (e.g. via PCs)
- Simple key management in offline mode, e.g. through input on display or via Security Data Carrier, as well as online mode (Down Line Loading, DLL)
- State-of-the-art PSTN modem for difficult channel conditions and long round trip delays (up to 2.5 sec)
- Crypto AG manufactures all systems in compliance with quality assurance standard ISO 9001

4 Benefits to BGAN users

- Die cryptographic processes use a customer-specific algorithm which is not known or used by any third parties: The entire system is therefore logically impenetrable.
- The encryption processes are hardware-based in a tamper-proof security module – for every connection based on a random number a new unique session key is generated
- Unauthorised access to security data is not possible, as data never leaves the security module in plain mode
- The architecture provides enormous potential for flexible and customised use of the encryption to support the customer's security policy
- The end-user requires no security knowledge – the switch between plain and ciphered mode is via a simple push of a button
- Access can be protected by strong user authentication

5 Setting up

This section describes how to set up the HC-2203 unit and the BGAN terminals.

5.1 Setting up HC-2203 PSTN Encryption

There are no specific settings to enable HC-2203 for satellite communication, and the default settings are compatible with BGAN terminals. However, Crypto AG makes the following three recommendations:

- Recommended hardware parameters (jumper settings) **–** the line impedance of the phone/fax interface of the EXPLORER terminals is complex. Refer to the User Manual to check and, if necessary modify the required jumper setting (HPV) to complex line impedance.
- Recommended software parameter settings: Mode **-** set to **AUTOSELECT MAX 9600** (communication with a HC-24x3 is possible)
- Recommended software parameter settings: Transmit Level **-** set to **-7dB** (the RX level at the other end should be in the range -15dB to -25dB)

In case of connectivity problems, check the list of outgoing and incoming calls in the logs of the BGAN terminal and verify whether the required Audio 3.1kHz service was used (see sections 5.3 and 5.4 for details).

If the Audio 3.1 kHz settings are correct, use the built-in line monitor of the HC-2203 to assess the connections (refer to "Connectivity problems" in the User Manual).

If only calls from a PSTN cause problems (and satellite to PSTN works), then a media gateway may attempt to disable modem communication. Refer to the "Plain/Crypto Mode" chapter in the HC-2203 user manual for help in solving this.

5.2 About your BGAN SIM card subscription

Your SIM card must be provisioned for "Audio 3.1kHz". Define the connected 2-wire interface of the BGAN terminal to use "Audio 3.1kHz" for outgoing calls.

5.3 Setting up the EXPLORER 500/527 and EXPLORER 700

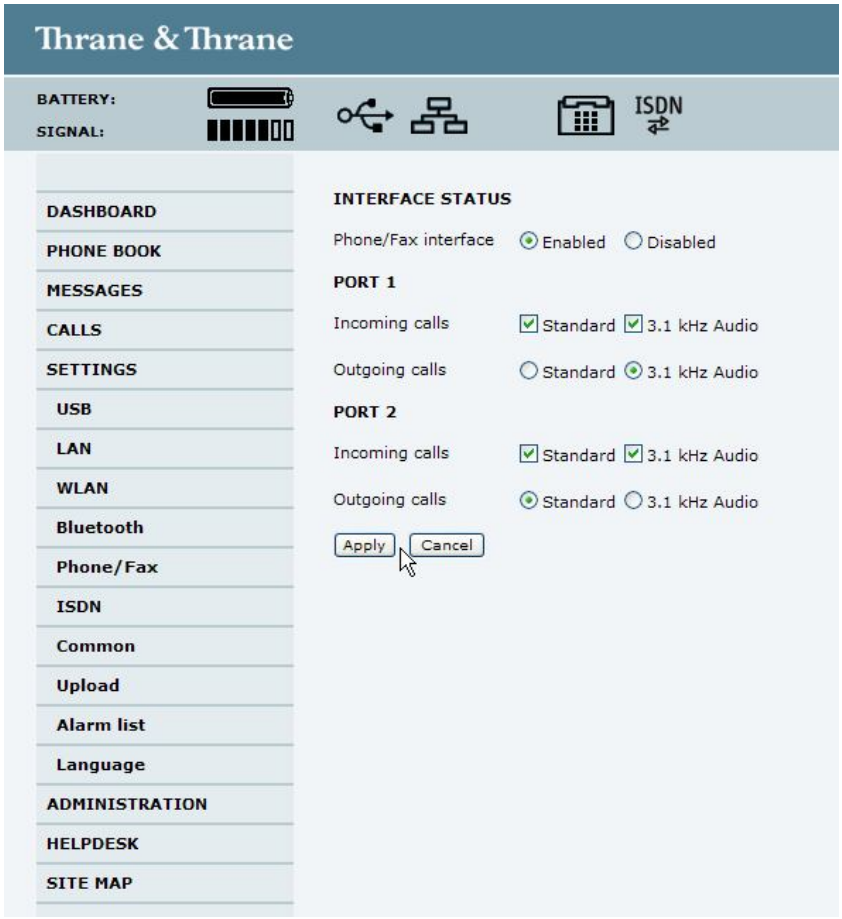
The Thrane & Thrane EXPLORER 500, EXPLORER 527 and EXPLORER 700 BGAN terminals can be configured to use the 3.1kHz audio service by default for outgoing calls (for incoming calls, the terminals are set to accept only the audio 3.1kHz and Standard service, enabling fax and plain phone communication). This means that you do not have to press **2*** in front of the number to select

this 3.1kHz service. In 3.1kHz mode, non-encrypted voice calls are possible but at a higher cost than on the standard voice mode or require a preselection of **1*** (prior to the subscriber number) to use the cheaper standard voice mode.

To configure the EXPLORER terminal to use the 3.1 kHz audio service by default:

a. With your computer connected to the EXPLORER terminal, open the Thrane & Thrane web interface by typing **191.168.0.1** into a web browser.

b. Click on **SETTINGS**, then click on **Phone/Fax**. The following screen displays:



c. Set Phone/Fax **3.1 kHz Audio** and **Standard** for incoming calls and **3.1 kHz Audio** for outgoing calls.

Note: The EXPLORER 500 has only one port. On the EXPLORER 700, set **Port 2** to 3.1 kHz Audio.

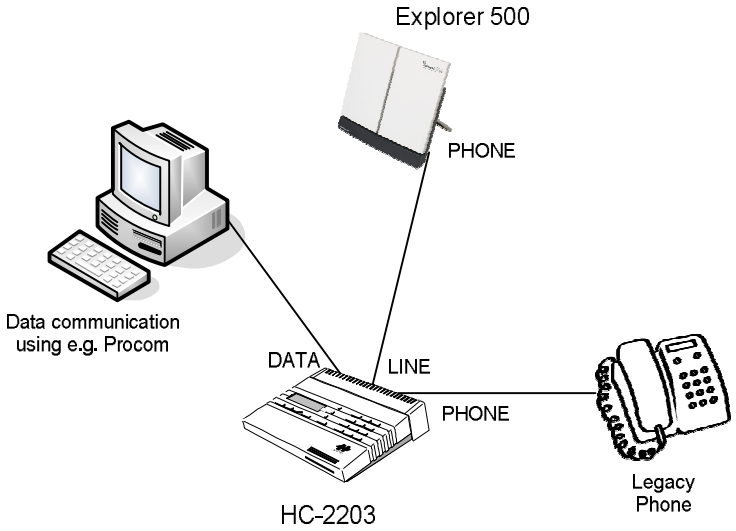
d. Click on **Apply** to save the settings. You are now ready to connect the HC-2203 to the terminal:

e. Connect HC-2203 (LINE) to the EXPLORER 500 or EXPLORER 700 terminal's RJ-11 (phone/fax) port. On the EXPLORER 700, use port 1

f. Connect the phone to the HC-223 (PHONE) plug on the unit's rear panel using the supplied RJ-11/RJ-11 cable.

Notes:

- For FleetBroadband, use the same setting for terminals FB250 and FB500
- To make a secure call to Headquarters (HQ), dial out enter hash (#) after the phone number as a delimitter (for example, 0044 3456 5389#)
- Check the HC-2203 preset in respect of cipher or plain mode; The green Cipher LED must be on.
- To select the Audio 3.1kHz BGAN service, you must use the assigned subscriber number for this service. It is a different number from the standard voice service number.



5.4 Setting up the Hughes 9201 or Hughes 9250 terminal

The Hughes 9201 uses a terminal adapter, and therefore the terminal adapter must be configured with the correct MSN numbers. By default the HNS terminal uses MSN 2 for the 3.1KHz audio service. To confirm this, click on **Terminal > ISDN interface** in BGAN LaunchPad.

You are now ready to connect the HC-2203 to the terminal:

a. Connect the HC-2203 (LINE) to the Hughes 9201 terminal's phone/fax port.

b. Connect the Phone to the HC-2203 (FAX) plug on the unit's rear panel using the supplied RJ-1 1/RJ-1 1 cable.

6 Technical specifications

For PSTN networks with varying performance, select modems with variable bit rates and modulation types as they can adapt automatically to the conditions (2400 ... 19200 bps, V.32/V.32, V.34), thus enabling robust connections. PSTN Encryption HC-2203 has been designed for these specifications and can provide robust encrypted connections. Nowadays, all PSTN networks no longer support PSTN V-Modem communication unconditionally, especially when so-called media gateways are involved (i.e. when PSTN connections are routed over IP-based networks or backbones).

HC-2203 is compatible with the BGAN satellite terminals and with virtually all commercially available PSTN telephones (analogue). PSTN Encryption HC-2203 is also compatible with Secure

GSM C-24x3 from Crypto AG, enabling direct secure telephone connections between BGAN terminals and from BGAN terminals to GSM or PSTN users and vice versa.

The encrypted connection is established manually or automatically in the background. Plain operation is always possible, but can also be disabled. The encryption unit is simply installed by connecting a cable to the telephone and to the telephony jack of the satellite terminal.

7 General data

Category	Details
Operation mode	Voice: Plain (bypassed) / Encrypted voice full duplex (2400...9600 bps) Data: Transparent data channel 2400...19200 bps with RTS/CTS
Interfaces	Keyboard: 4 x 3 numeric/alphanumeric keys, 1 plain/crypto control key, 2 cursor and 2 soft keys 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 network	Classical PSTN Leased line Military tactical area network (conditional) Satellite network (2 hops) Provided channel is a transparent.
Telephony systems	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: - 7...-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: asynchronous 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
Weight	1.98 kg (incl. batteries, without AC power supply)

8 Further details and support

Inmarsat Contact
customer_care@inmarsat.com

Crypto AG Contact

E-Mail: support@crypto.ch
Web site: www.crypto.ch

Crypto AG
P.O. Box 460
CH-6301 Zug
Switzerland

Tel. +41 41 749 77 22
Fax +41 41 741 22 72