Using the Omnisec 222 secure telephone over BGAN

Version 2

6 June 2008

inmarsat.com/bgan

Contents

1 Overview

The Omnisec 222 Secure Telephone Encryptor is a powerful, flexible and adaptable voice encryption system. It has two independent telephone interfaces with both OFDM modem and standard analog modem on each line. This allows the connection of any internal caller to an external partner over a PBX, using an encrypted Inmarsat BGAN 3.1Khz channel (or an unencrypted channel, if you choose). You will notice a remarkably short delay of only ~10 seconds when entering encrypted mode, due to the deployment of modems using OFDM modulation.

This document provides recommendations on the use of the Omnisec 222 Secure Telephone Encryptor (called Omnisec 222 in this document) over the BGAN network. It explains the features and benefits of the telephone, how to set up the Omnisec 222 for use over BGAN, the equipment needed, and the set up required for use with BGAN.

1.1 Typical Users

- Government agencies
- Military and Defense organizations
- Police and Security Forces
- Oil, gas and mining organizations
- Bank, Finance and Multinational Corporations

2 Key Features

The Omnisec 222 offers the following main features over the BGAN network:

- The telephone can be used as both a standard telephone or as a Secure Telephone Encryptor. Secure (encrypted) voice calls use the 3.1kHz service and standard calls use the 4kbps service.
- If connected over one BGAN terminal (Fixnet), the Omnisec 222 uses the unique fast synchronization of its OFDM mode when entering encrypted mode. In BGAN to BGAN connections, it uses standard V.32 mode.
- You can either connect the Ominsec 222 to the RJ-11 port of a Thrane & Thrane EXPLORER 500 or EXPLORER 700 terminal, or via a terminal adapter to the ISDN port of a Hughes 9201 terminal.

  Note The Omnisec 222 is not supported on the EXPLORER 100/110, or the EXPLORER 300 terminal.

- The second line of the Omnisec 222 can be used to forward a voice call to any ordinary telephone inside or outside your organization.

3 Benefits to BGAN users

The Omnisec 222 offers you the following main benefits:

- A convenient-to-use Swiss-made telephone.
- A high level of security, protecting your worldwide voice communications over Inmarsat BGAN and analog telephone lines (PSTN).
- Support for both secure (encrypted) and clear (unencrypted) communications.
- Two independent telephone interfaces, enabling a variety of advanced tasks, such as alternating between a plain and an encrypted conversation, or connecting an internal caller to an external partner over an encrypted link.
- Support on both interfaces either for Omnisec's unique OFDM/QAM modem technology at 2400, 4800 or 7200 bps, or standard V modem technology at 2400 (V.22bis), 4800 (V.32) or 9600 bps (V.34) resulting in excellent voice quality and perfect speaker recognition.
- Sophisticated modern telephone functions, such as redialing, a call register, a phonebook, and programmable keys for speed dialing.

3.1 Security Architecture

The multi-barrier OmnicryptTM Security Architecture raises digital voice encryption to the highest level of security. Secret symmetric bilateral 256-bit Master Keys generate short-lived 256-bit Session Keys, which are used for encrypting the communications.

Efficient and flexible key management is assured either:

- For small networks, by means of the Built-in Key Equipment (BIKE) utility.
- For larger networks, by means of the Key Management Center application Omnisec 711, with the Security Module Programmer Omnisec 704.

Online expansion (new station added) or 'pruning' (stations deleted from a network) of existing networks is made possible by the Key Download feature of the Station Manager application Omnisec 741, which also enables firmware updates.

3.2 Security Module

The unique 256-bit Master Keys for each pair of participating sites are generated from a random "white noise" source within the device or the key management utility. The Security Module Programmer 704 is highly sophisticated and tamper-proof.

Every connection produces a unique 256-bit Session Key (used once and only once), based on the corresponding Master Key. Nobody has access to the decryption keys (Master or Session), and they can't be read out of the Security Modules.

4 Setting up - hardware

This section describes how to set up BGAN for use with Omnisec 222 after initially programming the Security Modules, and gives an example of an Omnisec 222 configuration.

Installation

a. Connect the handset to the RJ-22 socket on the left-hand panel of the Omnisec 222.

b. Connect the RJ-11 socket LINE-1 on the rear panel of the Omnisec 222 to the RJ-11 port of an EXPLORER 500 or EXPLORER 700 terminal, or via a terminal adapter to the ISDN port of the Hughes 9201 terminal.

c. Insert the universal power supply cable into the DC power socket on the rear panel of the Omnisec 222. The Omnisec 222 starts automatically and on completion of the self-test the telephone shows the main screen.

d. Insert the previously programmed Security Module (E-SM) on the right-hand panel of the Omnisec 222, type in the PIN code of the SM and lock it permanently with the mechanical key.

It is important to understand the difference between clear mode and cipher (encrypted) mode calls:

- Clear mode calls - non-encrypted, insecure calls with any partner to any kind of telephone.
- Cipher mode calls - encrypted calls with a partner who also has an Omnisec 222 Secure Telephone and corresponding Master Keys in their Security Module (E-SM).

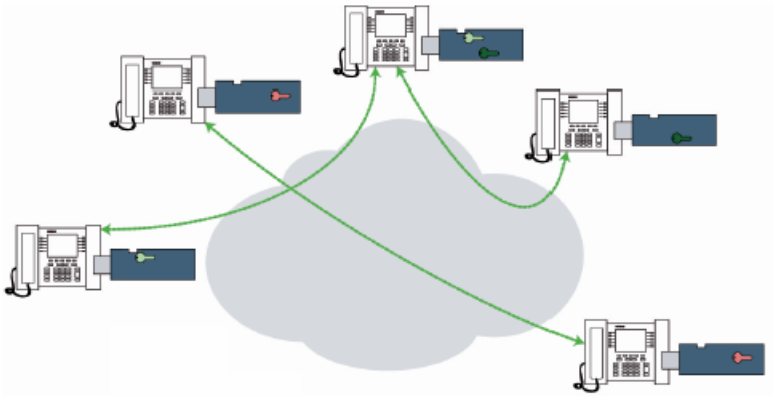
Note If the Omnisec 222 is connected via a PBX, this PBX should be set to pass all incoming and outgoing DTMF tones. These tones are used by two Omnisec 222s to exchange configuration parameters during call initialization.

Only devices conforming to the EN 60950-1:2005 safety standard may be connected to the Omnisec 222 (handset, power supply or a PC to the USB client connector on the rear panel).

Each Secure Telephone participating in a secure network owns a Security Module (E-SM). Each SM has three centrally controlled properties, defined by the Network Security Manager during an initialization process at the Network Management site:

- It belongs to a specific network
- It belongs to one or more user groups for which it possesses a 256-Bit Master Key.
- It may or may not support AKA (Authenticated Key Agreement).

5 Setting up – software



Selecting the mode

To set up the BGAN terminal for use with the Omnisec 222 (Version 1.25), you must first set up the Omnisec 222 for use in either BGAN to fixnet mode (which can use any analog network), or BGAN to BGAN mode: (which must have a BGAN terminal at both ends of the link).

- BGAN to Fixnet - Press the soft key [Menu], choose [Setup] and [Phone settings] and then select [Country] = BGAN
- BGAN to BGAN - Press the soft key [Menu], choose [Setup] and [Phone settings] and then [Country] = BGAN to BGAN

The new settings will take effect after rebooting (power off and on again).

The next step depends on whether you are using an EXPLORER terminal, or the Hughes 9201 terminal.

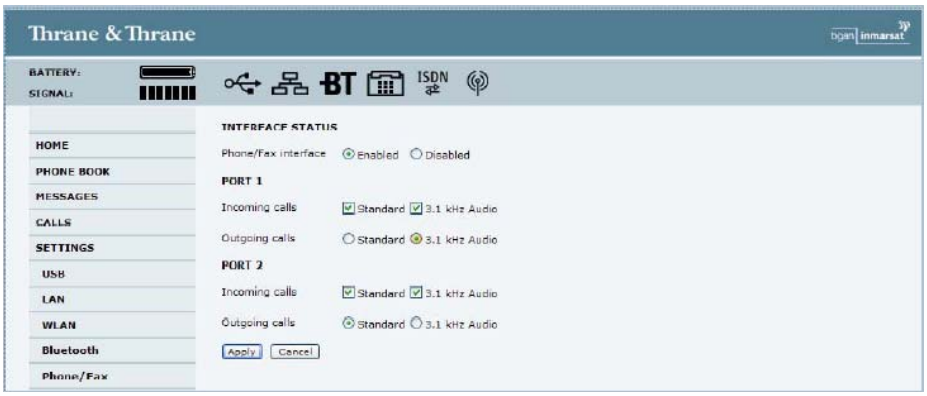
5.1 Setting up the EXPLORER 500 and EXPLORER 700

The EXPLORER 500 and EXPLORER 700 BGAN terminals can be configured to use the 3.1kHz audio service by default. 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 4k Audio mode.

To configure the EXPLORER terminal to use the 3.1 kHz audio service by default (for secure calls):

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 the Phone/Fax port to which the Omnisec 222 is connected to 3.1 kHz Audio for Outgoing calls.

Note The EXPLORER 500 has only one port.

d. Click on **Apply** to save the settings.

Note the following:

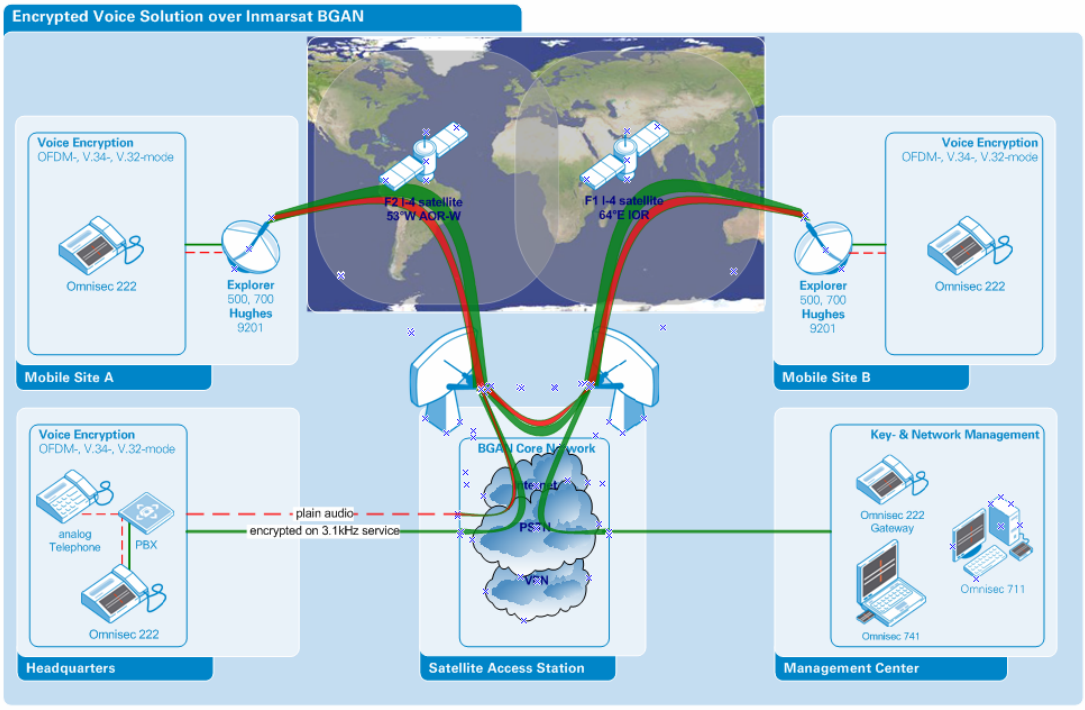
- After changing the default service to the 3.1 kHz Audio, you can initiate a low-cost Standard Voice call (not secure) by entering 1* in front of the number dialed. All other calls default to 3.1 kHz audio.
- To make a secure call to Headquarters (HQ), dial out using 3.1 kHz audio and enter hash (#) after the phone number (for example, 0045 3955 8800#).

- To make a standard low-cost call to HQ, prefix the phone number with 1*, AND enter a hash (#) after the phone number, for example: 1*0045 3955 8800#

5.2 Setting up the Hughes 9201

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.

5.3 Omnisec 222 over BGAN: End-To-End Solution Diagram



- Headquarters to Mobile Site A: Plain (un-encrypted) call using 4kbps audio service.
- Headquarters to Mobile Site A: Secure (encrypted) call using 3.1kHz audio service (remarkably short delay when entering encrypted mode (OFDM mode)).
- Mobile Site A to Mobile Site B: Plain call using 4kbps audio service.
- Mobile Site A to Mobile Site B: Secure (encrypted) call using 3.1kHz audio service (standard delay when entering encrypted mode (V.32 mode)).

Equipment Needed

Typical example:

- At least two Omnisec 222 Secure Telephone Encryptors, with Security Modules
- EXPLORER 500 or EXPLORER 700 BGAN terminals, or Hughes 9201 BGAN terminal with terminal adapter.

6 BGAN Customisation

The Omnisec 222 Secure Telephone Encryptor Version 1.25 (and higher) has been customized for use with BGAN. Choose the appropriate BGAN setup within the country profile.

7 Further details and support

Inmarsat Contact

Customer_Care@inmarsat.com

Omnisec AG Contact:

E-Mail: bgan@omnisec.ch

Web site: http://www.omnisec.ch/222

Postal address : Rietstrasse 14

CH-8108 Daellikon, Switzerland

Telephone: +41 44 847 67 11