Using the Omnisec 525 fax encryptor over BGAN

Version 2

6 June 2008

inmarsat.com/bgan

Contents

1 Overview

The Omnisec 525 Fax Encryptor is designed to ensure secure worldwide fax communications across your organization or enterprise. It can connect any G3/Super G3 standard fax machine and BGAN terminal or telephone line, allowing the sending and receiving fax messages simultaneously. It is also equipped with a Secure Mailbox, which can be set up to save incoming fax messages instead of printing them directly on the facsimile machine. This prevents the reading of confidential fax messages by unauthorized personnel.

This document provides recommendations on the use of the Omnisec 525 Fax Encryptor (called Omnisec 525 in this document) over the BGAN network. It explains the features and benefits of the fax encryptor, how to set up the Omnisec 525 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 525 offers the following main features over the BGAN network:

- Easy installation, operation and maintenance.
- The highest level of confidentiality, data integrity, authenticity, and non-repudiation of classified facsimile over BGAN or telephone lines.
- Automatic adaptation of connection speed up to V.34 (33.6kbps).
- Secure (encrypted) facsimile transmission over BGAN using the 3.1kHz service, and plain facsimile transmissions using the 4kHz service (if this option is enabled).
- Unique BGAN terminal to BGAN terminal mode (double sat hop) configuration.
- 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 525 is not supported on the EXPLORER 100/110, or the EXPLORER 300 terminal.

3 Benefits to BGAN users

The Omnisec 525 offers you the following main benefits:

- An exclusive Swiss-made facsimile
- A high level of security to ensure security for your worldwide fax communications over Inmarsat BGAN and over analog telephone lines (PSTN).
- High security against inadvertent plain transmissions.
- Omnicrypt™ Security Architecture (OSA), which satisfies highest government certification requirements and offers user-friendly secret key handling.
- The exchange of encrypted messages takes place without having to handle Security Modules and keys as the pin-protected Equipment Security Module (E-SM) is mechanically locked in the encryptor.
- Secret symmetric bilateral 256-bit Master Keys in the E-SM produce unique, short-lived 256-bit Session Keys, renewed for every communication and different for each partner.

Note It takes 40-60 Seconds to send a fax end to end depending on the amount of text and graphics. Approximately 20 seconds of this is introduced by the 525; this figure will double for a BGAN to BGAN call.

3.1 Security Architecture

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 525 after initially programming the Security Modules, and gives an example of an Omnisec 525 configuration.

4.1 Installation

a. Connect the RJ-11 socket LINE on the rear panel of the Omnisec 525 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.

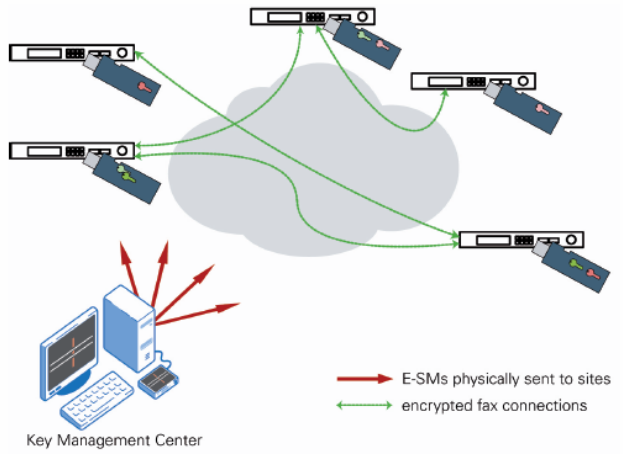
b. Insert the previously programmed Security Module (E-SM) into slot “SM A” of the encryptor and lock it permanently with the mechanical key.

c. Insert the universal power supply cable into the DC power socket on the rear panel of the Omnisec 525. The Omnisec 525 starts automatically and, on completion of the self-test of the line and fax interfaces, the display shows “SM CLOSED”. Enter the PIN to open the Security Module and the display shows “REDAY”.

Only devices conforming to the EN 60950-1:2005 safety standard may be connected to the Omnisec 525 (BGAN terminal, power supply, fax machine or a PC to the USB client connector on the rear panel).

Each Fax Encryptor 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

5.1 Selecting the mode

To set up the BGAN terminal for use with the Omnisec 525, you must first set up the Omnisec 525 has first to be set up to use Inmarsat BGAN connections either to any BGAN terminal or to any other PSTN network. To do this:

a. Login as Security Manager with the PIN of the E-SM.

b. In the main menu, choose **Device Properties > Line Interface > Load Country Profile > Inmarsat BGAN**.

c. Exit the menu. The Omnisec 525 is ready to send and receive facsimiles over your BGAN terminal.

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

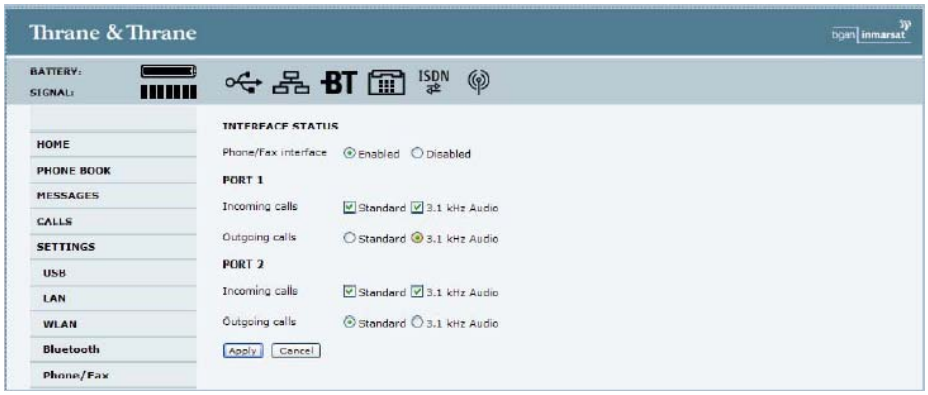
5.2 Setting up the EXPLORER 500 and EXPLORER 700

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:

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 port 2 to 3.1 kHz Audio for Incoming and Outgoing calls.

Note The EXPLORER 500 has only one port.

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

You are now ready to connect the Omnisec 525 to the terminal:

e. Connect the Omnisec 525 (LINE) to the EXPLORER 500 or EXPLORER 700 terminal's RJ-11 (phone/fax) port. On the EXPLORER 700, use port 2.

f. Connect the Group-3 fax-machine to the Omnisec 525 (FAX) plug on the unit's rear panel using the supplied RJ-11/RJ-11 cable.

Note the following:

- 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 8888#).
- To make a secure transmission from the HQ dial the 3.1 kHz Audio fax no. (AMS-ISDN5). Example: 00870 78 7654321

5.3 Setting up the Hughes 9201

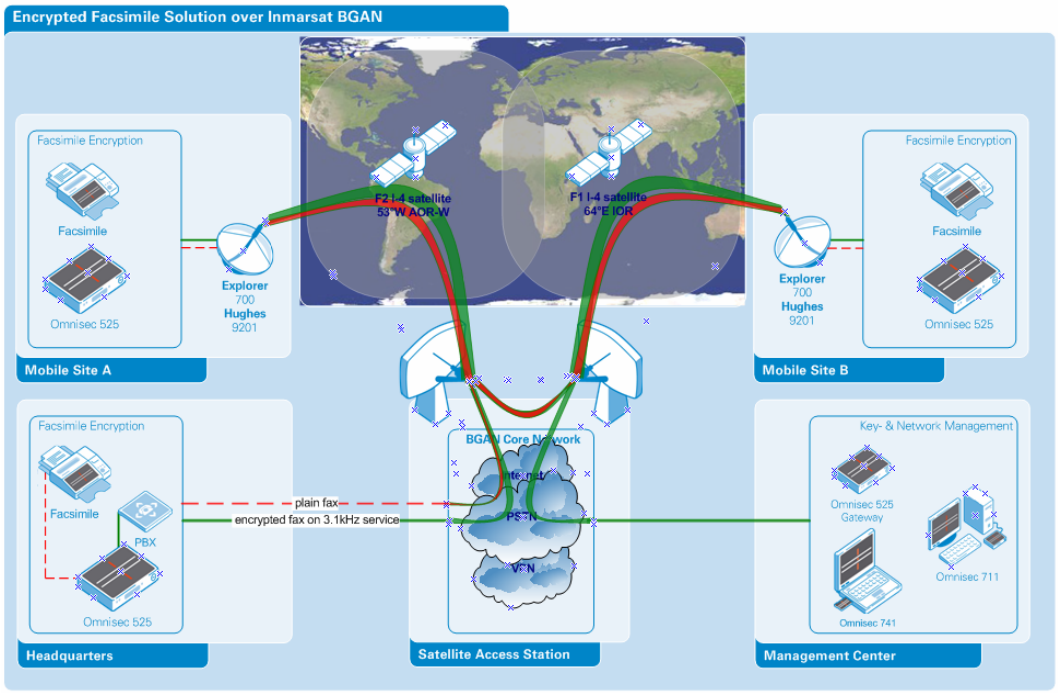
The Hughes 9201 uses a terminal adapter, and therefore the terminal adapter must be configured with the correct MSN numbers. By default the HNS terminal uses MSN 2 for the 3.1KHz audio service. To confirm this, click on Terminal > ISDN interface in BGAN LaunchPad.

You are now ready to connect the Omnisec 525 to the terminal:

a. Connect the Omnisec 525 (LINE) to the Hughes 9201 terminal's phone/fax port.

b. Connect the Group-3 fax-machine to the Omnisec 525 (FAX) plug on the unit's rear panel using the supplied RJ-11/RJ-11 cable.

5.4 Omnisec 525 over BGAN: End-To-End Solution Diagram



- Headquarters to Mobile Site A: Secure (encrypted) facsimile using 3.1kHz service
- Mobile Site A to Mobile Site B: Secure (encrypted) facsimile using 3.1kHz service

Equipment Needed

Typical example:

- At least two Omnisec 525 Fax Encryptors with Security Modules
- EXPLORER 500 or EXPLORER 700 BGAN terminal, or Hughes 9201 BGAN terminal with terminal adapter

6 BGAN Customisation

The Omnisec 525 Fax Encryptor Version 1.25 (and higher) has been customized for use with BGAN. Choose the appropriate BGAN setup within the country profile.

7 Hints and tips

The following are best practice hints and tips to ensure you get the most from Omnisec 525 over BGAN:

- Plain transmit and plain receive can be enabled or disabled. If both are disabled, the Omnisec 525 will not allow any plain messages to be sent or received.
- If you do not want fax messages to be left unattended on the fax machine, enable the Secure Mailbox on the Omnisec 525. This stores up to 500 pages of any incoming fax message encrypted in this mailbox.
- The call Routing Table enables you to restrict the exchange of encrypted faxes by explicitly allowing or blocking specific telephone numbers. For example the entry 0041* will block all faxes to Switzerland.
- An encrypted facsimile transmission can only be made by enabling the Omnisec 525's non-transparent mode. In general fax calls which are routed over VoIP (Voice over IP) gateways at telecom providers are likely to use a non-transparent channel. This means that standard facsimile procedures cannot be applied due the fact that the gateways may change all data which is not specified in the T.30 standard.

8 Further details and support

Inmarsat Contact

Customer_Care@inmarsat.com

Omnisec AG Contact

E-Mail: bgan@omnisec.ch

Web site: http://www.omnisec.ch/525

Postal address: Rietstrasse 14
CH-8108 Daellikon, Switzerland

Telephone: +41 44 847 67 11